Chương I Tổng quan

1.1. Giới thiệu các thiết bị mạng LAN.

1.1.1. Định nghĩa

Mạng cục bộ (Local Area Network – LAN) là mạng nằm trong một phạm vi hẹp với chu vi nhỏ hơn vài chục km, nó thường là sở hữu của một số cơ quan, tổ chức nào đó. Ví dụ mạng trong trường học, nhà máy…

Công nghệ LAN được sử dụng rộng rãi nhất hiện nay là Ethernet. Nó đạt được sự cân bằng giữa tốc độ, giá cả, dễ cài đặt, và khả năng hỗ trợ. Khoảng 80% các mạng LAN đã cài đặt dùng Ethernet.

Chuẩn Ethernet được định nghĩa bởi viện kỹ thuật điện và điện tử (IEEE) Hoa Kỳ trong chỉ tiêu thường biết đến dưới mã hiệu IEEE802.3.

1.1.2. Phương tiện Ethernet và cấu trúc liên kết(Topology):

Cáp đồng trục là phương tiện LAN đầu tiên được dùng trong cấu trúc liên kết tuyến (bus topology). Trong cấu hình này cáp đồng trục tạo thành một tuyến đơn gắn với tất cả các trạm. Tuy nhiên ngày nay cấu trúc này rất ít được ử dụng.

Một cấu trúc khác gọi là cấu trúc liên kết hình sao thì mạnh hơn. Trong cấu trúc liên kết hình sao, mỗi trạm được gắn vào một dây hệ trung tâm (HUB) bởi một đoạn cáp xoắn riêng biệt. Mỗi đầu cáp gắn với các NIC của các trạm và đầu kia gắn với cổng các HUB đặt trong khoang dây tại trung tâm

Có thể xây dựng mạng Ethernet sử dụng các phương tiện khác nhau: Cáp dây xoắn, cáp đòng trục, cáp quang.

1.1.2.1. Cấu trúc kết nối Bus.

- **Dùng cáp đồng trục.**

Cáp đồng trục dùng làm đường truyền chung cho toàn mạng. Đường truyền chung trong mạng được gọi là bus. Mọi nút mạng được gắn vào

đường bus đó. ở hai đầu của đoạn cáp có thiết bị gọi là terminal để chánh phản hồi ngược lại của tín hiệu.

Dùng cáp béo RG8: Để gsứn nút mạng vào bus phải có thiết bị tranceiver để nhận các bít từ cạc mạng ra sau đó chuyển thnhf xung (tín hiệu phù hợp để chạy trên dây cáp)

Dùng cáp gầy: Không sử dung tranceiver mà gắn ngay trên NIC. Sử dụng một số các thiết bị đầu cuối (connecter) hình chữ T hai đầu nối với BNC, một đaauf nối với đầu ra của NIC, ta thấy kết nối đơn giản hơn.

Nhược điểm của cấu trúc bus:

♣ Khi đoạn cáp bị đứt tại một điểm bất kỳ sẻ làm ngưng trệ giao thông trên toàn bộ mạng do khi bị đứt đoạn cáp bị chia thành hai phần do đó sẽ thiếu mất một terminal, tín hiệu truyển đi sẽ bị phản xạ trở lại.

♣ Khi số lượng nút mạng khá lớn sẽ gây khó khăn trong việc phát hiện các sự cố trên đường cáp.

♣ Không thuận lợi cho việc nâng cấp mạng.

♣ Tốc độ tối đa là 10 Mbps.

Dùng đôi xoắn

Phương thức truyền tín hiệu trên các đồng trục là không cân bằng dó đó ta sử dụng hai sợi đây có hiệu điện thể ngược nhau xoắn vào nhau để làm cho pha ngược nhau. Gọi là cáp đối xoắn.

Cáp đôi xoắn chia 2 loại:

♣ STP (Shielded Twisted Pair): Có thêm một lớp bọc bằng kim loại xung quanh các cặp dây để tăng cường khả năng chống nhiễu, do đó loại cáp này được áp dụng trong môi trương có khả năng chống nhiễu cao

♣ UTP (Unshielded TP): Sau các cặp dây đến ngay lớp bảo vệ, không có lớp bọc kim loại xung quanh, do đó nó được áp dụng trong các môi trường thông thường

Dùng cáp quang

Tín hiệu được truyền dưới dạng tia sáng nên ít bị ảnh hưởng của nhiễu, từ tính, độ suy hao không lớn.

Được chế tạo từ các sợi thuỷ tinh nhỏ do đó chi phí cao, rất phức tạp cho việc sửa chữa bởi các thiết bị rất tinh vi.

Cấu tạo gồm 3 lớp:

♣ Lõi thuỷ tinh

♣ Lớp vạtt liệu chống khúc xạ

♣ Lớp vỏ bảo vệ

Tín hiệu truyền dưới dạng tia sáng trên lớp thuỷ tinh, có lớp khúc xạ làm cho tín hiệu bị suy hao ít do đó truyền trên đường truyền dài được.

Chia cáp quang thành 2 loại:

♣ Single Mode: Cho phép tia sáng truyền qua nó theo chiều song song với trục nằm ngang.

♣ Multi Mode: Cho phép ánh sáng truyền trên nó theo hướng bất kỳ.

Truyền dùng cáp quang tốc đọ rất cao

1.1.2.2. Cấu trúc kết nối Star.

Có thể dùng cáp đôi xoắn hoặc dùng cáp quang

 Thiết bị Oullet (Wall place):

Oullet là một loại ổ cắm, thay vì nối từ HUB đến các nút mạng ta nối từ HUB đến các Outlet rồi từ đó nối đến các nút mạng.

Dùng Oullet tăng tính linh động, dễ di chuyển đến các nút mạng mà không ảnh hưởng nhiều đến các nút mạng khác.

 Thiết bị Patch Panel và Cross Connect:

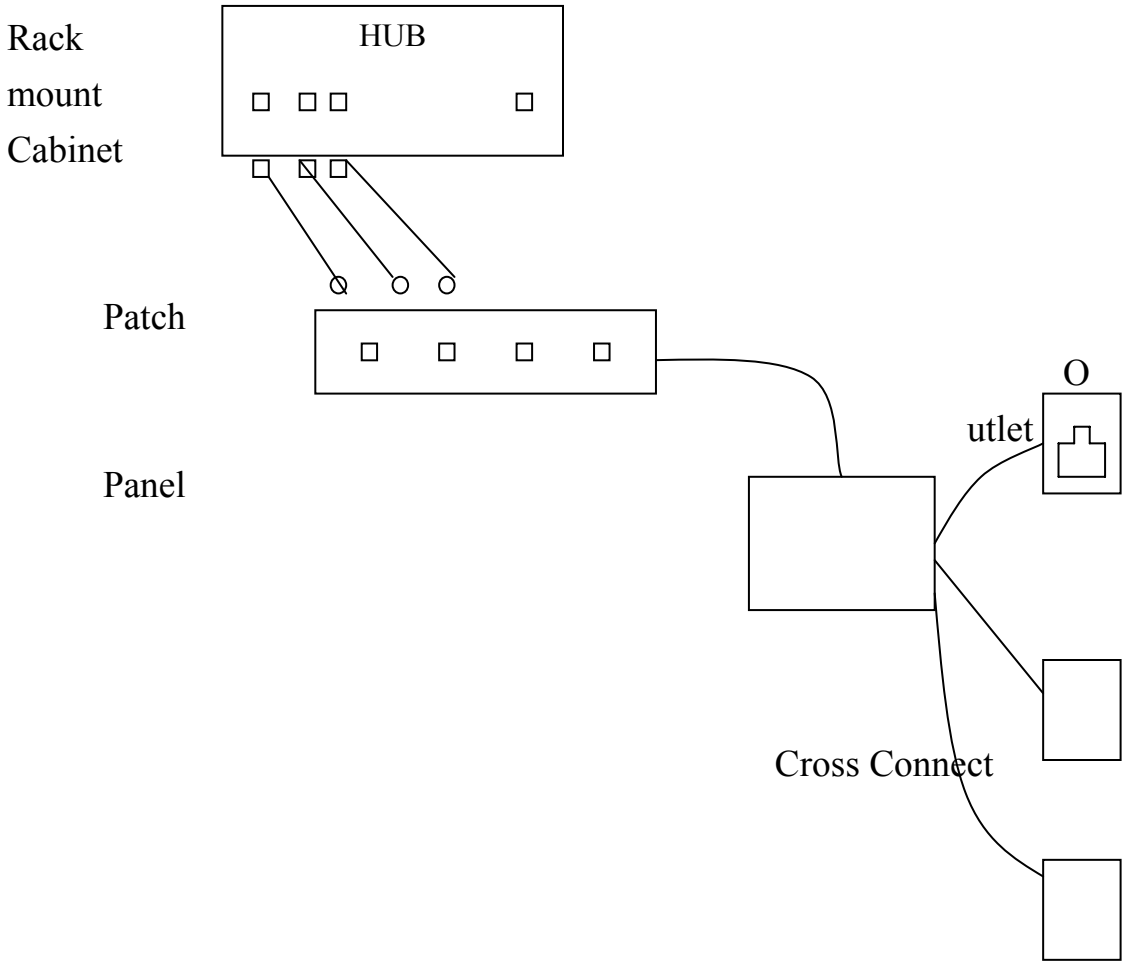
Patch Panel như cái bảng cắm dây, dùng outlet, khi số nút mạng tăng lên nhiều khó xử lý khi đó ta dùng thiết bị Patch Panel

Patch Panel có các cổng TP để nối với các HUB.

Khi ta nối các HUB/Bridge với nhau ta dùng Cross cable (cáp chéo), đây là loạ cáp truyền một đầu, nhận một đầu.

Số lượng HUB kết nối giữa 2 nút mạng <= 4

Không nối vòng tròn các HUB với nhau.



Đặc điểm của cấu trúc Star:

♣ Một đoạn bị đứt không ảnh hưởng đến toàn mạng

♣ Việc tăng thêm số lượng nút mạng dễ dàng, không ảnh hưởng đến giao thông trên mạng.

♣ Việc nâng cao tốc độ có thể làm được

1.1.2.3. Cấu trúc kết nối Ring.

Cấu hình mạng ring nối các máy tính trên một vòng cáp. Không có đầu nào bị hở. Tín hiệu truyền đi theo một chiều và đi qua từng máy tính. Khác với cấu hình bus thụ động, mỗi máy tính đóng vai trò như một bộ chuyển tiếp, khuyếch đại tín hiệu và gửi nó đến máy tính tiếp theo. Do tín

hiệu đi qua từng máy nên sự hỏng hóc của một máy ảnh hưởng đến toàn mạng.

1.2. Giới thiệu các thiết bị mạng WAN

1.2.1. Định nghĩa.

Mạng diện rộng (Wide Area Network - WAN) là hệ thống kết nối các mạng cục bộ nằm ở xa nhau. Ví dụ kết nối các điểm trong một thành phố, giữa các thành phố…

1.2.2. Thiết bị Gateway

Các Gateway được thiét kế để nối các loại mạng khác nhau về cơ bản .Chúng thực hiện điều đó bằng cách dịnh các thông điệp từ một định dạng này sang một định dạng khác .

Các Gateway thường được dùng để nối một mạng với một máy tính chính hoặc với một máy tính mini. Nếu bạn không có một máy tính chính hoặc máy tính mini,có lẽ bạn không cần Gateway .

+Các Gateway là cần thiết vì các nhà sản xuất máy tính dùng các thiết kế độc quyền trong mạng.Nếu các nhà sản xuất máy tính chịu nói chuyện với nhau 20 năm trước thì ngày nay chúng ta đã không phải dùng các Gateway để cho các mạng nói chuyện với nhau.

1.2.3. Thiết bị Router

Thiết bị Router tương tự như một Bridge siêu thông minh cho các mạng thực sự lớn. Các Bridge biết địa chỉ của tất cả các máy tính ở các máy tính kết nối đến nó và có thể gửi chuyển tiếp các thông điệp theo đúng địa chỉ. Nhưng các Router còn biết nhiều hơn về mạng. Một Router không những chỉ biết địa chỉ của tất cả các máy tính mà còn biết các Bridge và Router khác ở trên mạng và có thể quyết định lộ trình có hiệu quả nhất để gửi mỗi thông điệp của mạng.

Một trong những thủ thuật hay nhất mà các Router có thể thực hiện là nghe ngóng trên toàn mạng để xem các phần khác nhau của mạng

bận rộn như thế nào.Nếu một phần nào đó của mạng bị bận, Router có thể quyết định gửi tiếp một thông điệp bằng cách dùng một đường ít bận hơn.

1.3. So sánh sự Bridge và Switch

Bạn có thể nghĩ về các Switch như là Bridge có nhiều cổng. Switch là một phần cứng cơ sở, điều đó có nghĩa là chúng sử dụng các địa chỉ MAC từ các Card kết nối của các máy chủ để lọc được một mạng xác định. Bạn cần phải nhớ cách mà các Switch sử dụng các mạch tích hợp ứng dụng đặc biệt để xây dựng và lưu trữ các bảng lựa chọn.

Tuy nhiên, có một số điểm khác nhau giữa các Bridge và các Switch điều này bạn sẽ nhận thấy ở các tính chất sau:

+> Để tạo ra các quyết định lựa chọn, các Bridge sử dụng phần mềm còn các Switch sử dụng phần cứng.

+> Mỗi Bridge chỉ có một cây bao trùm trong khi đó mỗi Switch có thể có nhiều cây bao trùm.

+> Các Bridge có số cổng cực đại là 16, trong khi đó các Switch có thể có hàng trăm cổng.

Mặc dù bridge và switch có nhiều tính năng tương tự nhau nhưng chúng vẫn có nhiều điểm khác biệt. Switch nhanh hơn nhiều so với bridge bởi vì chúng chuyển đổi bằng phần cứng so với cách chuyển đổi bằng phần mềm của bridge, switch có khả năng kết nối các mạng có băng thông khác nhau ví dụ có thể kết nối hai mạng cục bộ ethernet 10Mbps và mạng 100Mbps với nhau. Switch có mật độ cổng cao hơn so với bridge. Một số cung cấp kiểu hoạt động cut-through switching làm giảm thời gian trễ trong mạng trong khi đó bridge chỉ cung cấp chế độ store-and-forward switching. Cuối cùng switch làm giảm thiểu sự đụng độ trên các đoạn của mạng bởi vì chúng cung cấp băng thông dành riêng cho các đoạn.

Chương II Hoạt động của Ethernet bridge và switch

2.1. Giới thiệu về mạng Ethernet

Phần này giới thiệu về kiến trúc mạng Ethernet và trình bày khái quát về các chức năng, đặc tính, và những thành phần chủ yếu của kiến trúc mạng Ethernet.

♣ Tổng quan về Ethernet

Kiến trúc mạng kết hợp các tiêu chuẩn, cấu hình và giao thức để tạo thành mạng làm việc. Phần này mô tả kiến trúc mạng Ethernet.

♣ Nguồn gốc của Ethernet

Vào cuối thập niên 60, trường đại học Hawall phát triển một mạng diện rộng (WAN) (gọi là ALOHA). Hẳn các bạn còn nhớ, mạng diện rộng (WAN) chính là cục bộ (LAN) mở rộng qua một địa hình rộng hơn. Trường đại học có một địa hình rộng lớn và họ cần nối kết những máy tính nằm rải rác khắp khu vực trường. Một trong những đặc điểm quan trọng của mạng mà họ đã thiết kế là việc sử dụng CSMA/CD làm phương pháp truy nhập.

Mạng sơ khai này đặt nền tảng cho cấu trúc mạng Ethernet ngày nay. Vào năm 1972. Robert Metcalfe và David boggs phát minh ra sơ đồ đường cáp và lược đồ truyền dữ liệu ở trung tâm nghiên cứu Palo Alto của Xerox (Xerox Palo Alto Research) Center – PARC). và đưa ra sản phẩm Ethernet đầu tiên vào năm 1975. Phiên bản Ethernet đầu tiên được thiết kế như một hệ thống 2.94 Mbps để nối hơn 100 máy tính vào sợi cáp dài 1 km.

Xerox Ethernet thành công đến mức tập đoàn và Digital Equipment đã thảo ra tiêu chuẩn Ethernet 10 Mbps. Ngày nay, đó là quy cách kĩ thuật mô tả phương pháp nối và dùng chung cáp cho máy tính và hệ thống dữ liệu.

Quy cách kỹ thuật Ethernet có cùng chức năng như tầng Phicical và tâng Data Link trong OSI. Thiết kế này là cơ sở cho quy cách kĩ thuật 802.3 của IEEE.

♣ Các đặc tính của Ethernet

Hiện nay Ethernet là kiến trúc mạng phổ biến nhất: kiến trúc dải gốc (Baseband Architecture) này dùng cấu hình bus thường dùng ở tốc độ 10 Mbps và dựa vào CSMA\CD để điều chỉnh lưu thông trên đường cáp chính.

Môi trường Ethernet mạng tính thụ động, có nghĩa nó lấy năng lượng từ máy tính và vì vậy sẽ không ngừng hoạt động trừ khi phương tiện nối bị cắt đứt hoặc bị kết thúc không đúng cách.

♣ **Những đặc điểm cơ bản của Ethernet**

Danh sách sau tóm tắt các đặc tính của Ethernet

Cấu hình truyền thông	bus đường thẳng
Cấu hình khác	star bus
Kiểu kiến trúc	dải gốc (Baseband)
Phương pháp truy nhập	CSMA\CD
Quy tắc truy nhập	IEEE 802.3
Vận tộc chuyền	10 Mbps hoặc 100 Mbps
Loại cáp	cáp đông trục, cáp mảnh,các UTP

♣ **Dạng thức khung trong Ethernet**

Ethernet chia dữ liệu thành nhiều gói có dạng thức khác với gói dụng trong mạng khác. Ethernet chia dữ liệu thành nhiều khung (frame). Khung là khói thông tin được truyền như một đơn vị duy nhất. Khung trong Ethernet có thể dài tự 64 byte đến 1518 byte, nhưng bản thân Ethernet đã sử dụng ít nhất 18 byte nên dữ liệu trong một khung Ethernet có thể dài từ 46 byte đến 1500 byte mỗi khung đền có chứa thông tin điều khiển và tuân theo cùng một cách cơ bản. Lấy ví dụ, khung Ethernet II (dùng cho TCP\IP) đượng truyền qua mạng với các thành phần sau:

Trường khung	Mô tả
Đầu	Đánh dấu điểm bắt đầu khung
Đích và nguồn	Địa chỉ nguồi và địa chỉ đích
Kiểu	Được dùng để nhận diện giao

	thức tầng Network (IP hay IPX)
Mã kiểm tra CRC	Trường kiểm tra lỗi nhằm các định liệu có phải khung đã đến mà không bị hư hại hay không

Mẫu khung Ethernet II

♣ Giới thiệu cấu hình 10BaseT

Vào năm 1990, uỷ ban IEEE ban hành quy cách kỹ thuật 802.3 dành cho việc chạy Ethernet trên dây xoắn đôi. 10BaseT(10 Mbps,dải gốc, trên cáp xoắn đôi) là mạng Ethernet điển hình dùng cáp xoắn đôi trần (UTP), nhưng cáp xoắn đôi có bọc (STP) cũng dùng được mà không làm thay đổi thông số nào của 10BaseT.

Đa số mạng loại này được lập cấu hình theo dạng star (hình sao) nhưng bên trong dùng hệ thống truyền tín hiệu bus giống như các cấu hình Ethernet khác. Hub của mạng 10BaseT đóng vai trò như bộ truyền tiếp đa cổng (multiport repeater) và thường được đặt ở nơi bắc dây trong nhà. Mỗi mày tính có hai cặp dây dẫn – một cặp dùng để nhận dữ liệu và cặp kia dùng truyền dữ liệu.

Chiều dài tối đa của một phân đoạn 10BaseT là 100m (328 feet). Có thể dùng bộ chuyển tiếp để nối thêm chiều dài nay. Chiều dài cáp tối đa giữa các máy tính là 2.5m. Một mạng cục bộ 10BaseT sẽ phục vụ cho 1024 máy tính. Hình 12.4 minh hoạ những lợi điểm của sơ đồ đi dây hình sao trong giải pháp 10BaseT. Cáp UTP có khả năng truyền dữ liệu ở tốc độ 10 Mbps. Rất dễ dời chuyển và thay đổi máy tính bằng cách di chuyển dây tiếp dẫn mô dun trong bảng phân phối. Khác với mạng bus Ethernet truyền thống. Các

thiếu bị khác trên mạng không bị ảnh hưởng do sự thay đổi trên bảng phân phối.

Bảng phần phối nên được kiểm tra ở những tốc độ cao hơn 10 Mbps. Hub mới nhất có thể cung câp nối kết chao các đoạn cáp Ethernet cả mảnh lẫn dày. Với kiểu lắp đặt này, cũng dễ dàng chuyển đổi từ cáp Ethernet dày sang cáp 10BaseT bằng cách gắn một máy thu phát 10BaseT nhỏ vào cổng AUI của CARD mạng bất kì.

Tóm tắt cấp hình 10BaseT

Phân mục	Ghi chú
Cáp	Cáp UTP hạng 3.4 hoặc 5
Bộ nối	RJ-45 ở các đầu cáp
Máy thu phát	Mỗi máy tính cần một cái: một số card có máy thu phát cài sẵn
Khoảng cách từ máy thu phát tới Hub	Tối đa 100m
Cáp chính cho hub	Cáp đồng trục hoặc cáp quang nối với mạng cục bộ lớn hơn
Tổng số máy tính cho mỗi mạng cục bộ không có thành phần nối	Theo quy cách kĩ thuật là 1024 máy

♣ Cân nhắc hiệu suất mạng

Ethernet có thể sử dụng một vài giao thưc truyền thông, trong đó có TCP/IP, vốn hoạt động hiệu quả trong môi trường UNIX. Điều này khiến cho Ethernet được ưa chuộng trong các cộng đồng khoa học và học đường.

♣ Phân đoạn

Hiệu xuất thi hành của Ethernet có thể được cải thiện bằng cách chia một đoạn cáp nối đầy thiết bị thành hai đoạn cáp nối it thiết bị hơn và nối hai đoạn cáp này bằng một bridge hoặc router. Việc này làm giảm lưu lượng truyền thông trên mỗi đoạn cáp. Do có ít mày tính truyền

dữ liệu nên đoạn cáp hơn, do đó thời gian truy nhập xẽ nhanh hơn. Phân đoạn là một giải pháp lý tưởng trong trường hợp mạng kết hợp thêm nhiều người dùng mới hoặc ứng dụng trong giải thông cao, chẳng hặn chương trình cơ sở dữ liệu và chương trình Video đang đượng cài thêm vào mạng.

♣ Hệ điều hành mạng

Ethernet sẽ làm việc tốt với các hệ điều hành phổ biến như sau:

- Microft Windows 95
- Microft Windows NT Workstation
- Microft Windows NT Server
- Microft LAN Manager
- Microft Windows for Workgroups
- Novell NetWare
- IBM LAN Server
- AppleShare

2.2. Ethernet switch và bridge

2.2.1. Hoạt động của Switch và Bridge.

2.2.1.1. Cơ bản về Switch và Bridge

Bridge và switch là các thiết bị truyền dữ liệu hoạt động chủ yếu ở tầng 2 theo mô hình OSI. Bởi vậy chúng được xem là các thiết bị tầng Data-link.

Bridge được thương mại hoá vào đầu những năm 1980. Khi đó bridge kết nối và cho phép truyền các gói dữ liệu giữa các mạng giống nhau. Gần đây, các bridge kết nối các mạng khác nhau đang được phát triển và chuẩn hoá.

Nhiều kiểu bridge đã chứng tỏ được tầm quan trọng của chúng với vai trò là các thiết bị kết nối mạng. Transparent bridging (Bridge trong suốt) sử dụng chủ yếu trong môi trường Ethernet trong lúc đó source-route bridging lại sử dụng chủ yếu trong môi trường Token-ring. Translational bridging cung cấp sự chuyển đổi định dạng dữ liệu và nguyên tắc truyền giữa các phương tiện truyền khác nhau (chủ yếu là giưa ethernet và Token-Ring).

Cuối cùng, source-route transparent bridging kết hợp giải thuật của transparent bridging và source-route bridging để cho phép truyền trong môi trường có cả Ethernet và Token-Ring.

Ngày nay, kỹ thuật switching đã nổi lên là sự phát triển của kỹ thuật bridging và thừa kế các tính năng và ứng dụng của chúng. Kỹ thuật switching thống trị các ứng dụng mà trước đâu sử dụng kỹ thuật bridging. Hiệu năng cao hơn, mật độ cổng cao hơn, giá tính cho một cổng thấp hơn và mềm dẻo hơn đóng vai trò to lớn giúp cho switching vượt trội so với bridging và trở thành công nghệ thay thế bridge.

Tổng quan về các thiết bị tầng liên kết

Quá trình bridging và switching xảy ra ở tầng liên kết, tầng điều khiển luồng dữ liệu, xử lý lỗi truyền thông, cung cấp địa chỉ vật lý và kiểm soát truy cập đường truyền. Bridges cung cấp các chức năng này băng cách sử dụng nhiều giao thức của tầng liên kết mà chúng hiện thực hoá các giải thuật kiểm soát luồng dữ liệu, xử lý lỗi, đánh địa chỉ và truy cập đường truyền. Các giao thức tầng liên kết phổ biến nhất là Ethernet, Token-Ring và FDDI.

Các thiết bị Bridge và switch không phải là các thiết bị phức tạp. Chúng phân tích các gói dữ liệu đến, quyết định có chuyển tiếp gói dữ liệu đó không dựa vào các thông tin có trong gói dữ liệu đó và chuyển tiếp gói dữ liệu đó nếu cần. Trong một số trường hợp, ví dụ như source-route bridging, các gói dữ liệu được chuyển tiếp cùng mội lúc tới đích.

Tính trong suốt của đối với các giao thức tầng cao hơn là các ưu điểm lớn nhất của bridging và switching. Bởi cai hai thiết bị này đều làm việc ở tầng liên kết, chúng không kiểm tra thông tin của các tầng cao hơn. Điều này có nghĩa là chúng làm cho việc truyền thông nhanh hơn so với bất kỳ giao thức ở tầng network nào. Thông thường, bridge không chuyển các giao thức giao vận AppleTalk, DECNet, TCP/IP, XNS giữa hai hay nhiều mạng.

Bridge có khả năng chọn các gói dữ liệu dựa trên các trường của tầng 2. Ví dụ, một bridge có thể được lập trình để loại bỏ (không chuyển tiếp) tất cả các gói dữ liệu từ một mạng nào đấy.Bởi vì các của tầng liên kết dữ liệu có các liên kết với các tầng trên, bridge có thể lựa chọ dựa trên các tham số

này. Hơn nữa, việc lựa chọn có thể rất có ích trong việc hạn chế các gói tin multicast.

Bằng cách chia nhỏ các một mạng lớn thành các phần nhỏ, bridge và switch đưa lại nhiều lợi ích. Bởi vì chỉ một phần các gói tin được chuyển tiếp, bridge và switch làm giảm khối lượng truyền thông của các thiết bị trên tất cả các đoạn được kết nối. Bridge và switch đóng vai trò như là một Firewall đối với một số lỗi có nguy cơ phá huỷ mạng và điều tiết truyền thông giữa một số lượng lớn các thiết bị hơn là cung cấp chỉ một mạng cục bộ nối tới bridge. Bridge và switch mở rộng phạm vi của mạng cục bộ, cho phép kết nối các thiết bị ở khoảng cách xa mà trước đây không cho phép.

2.2.1.2. Ethernet Bridge/Swich

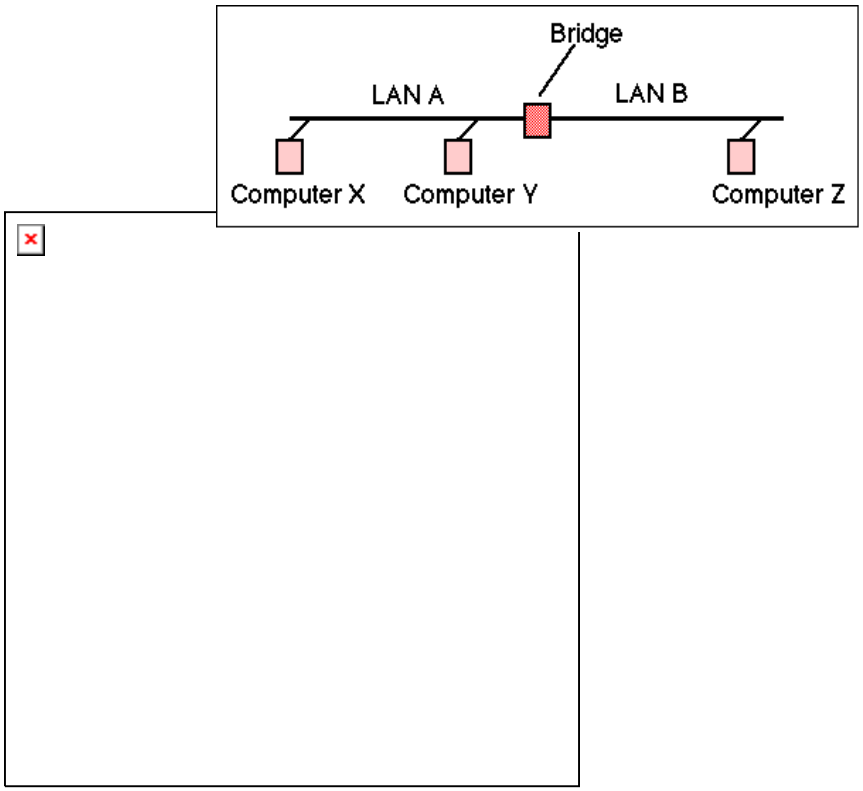
Bridge là thiết bị kết nối của mạng LAN, nó hoạt động ở tầng 2 (Data Link) của mô hình OSI 7 tầng. Nó cũng được sử dụng để kết nối 2 mạng LAN (A,B), để xây dựng lên một mạng LAN rộng hơn. Bridge cũng có thể chọn đường giữa 2 mạng LAN và có thể tạo lên một cách hợp lý, có hiệu lực trong việc chia công việc lớn từ một mạng LAN thành một nhóm công việc nhỏ hơn định vị trên các mạng LAN nhỏ khác nhau. Bridge đươc đưa ra đầu tiên là bởi IEEE 802.1D (1990) và sau đó là bởi ISO (1993).

Định dạng của PDUs tại tầng này trong Ethernet LAN là định nghĩa về khuôn dạng Ethernet frame (giống như MAC - Medium Access Control). Nó bao gồm 6 byte địa chỉ và 1 byte protocol ID / length field

Trường địa chỉ cho phép frame gửi một trạm hay nhiều trạm. Giao thức MAC sẽ chịu trách nhiệm cho việc chuyển đổi trung gian và dự đoán sự sai lạc trong việc hoặc là truyền nhận trung gian, hoặc là tại các trạm thu phát nơi cần đến của việc truyền nhận trung gian

♣ Hoạt động của Bridge

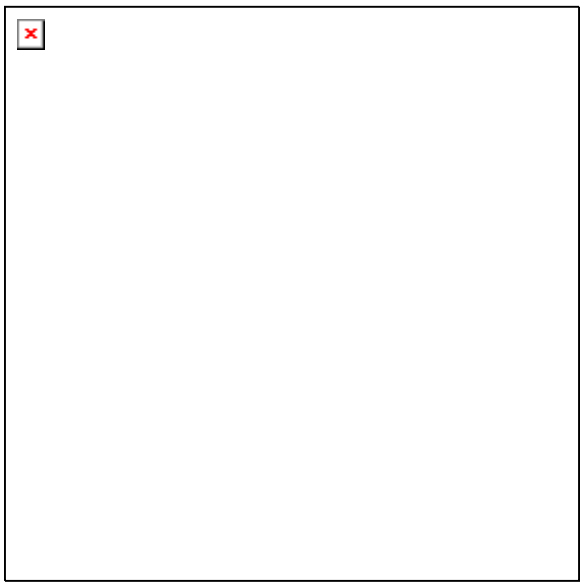
Bridge đơn giản và hay được sử dụng là Transparent Bridge, Bridge có thể forward (truyền và nhận) frame từ một mạng LAN này (ví dụ LAN A) tới một mạng LAN khác (ví dụ LAN B). Rõ ràng là Bridge có thể forward tất cả frame, về phần này nó khá giống như là repeater. Việc forwarded frames sẽ rất nhanh chóng nếu Bridge cần forwarded frames từ mạng LAN này đến mạng LAN khác. Để làm được điều này Bridge có cơ chế học (learn) ở tất cả các mát tính được kết nối trong mạng LAN. Thông thường đó là cơ chế học địa chỉ.

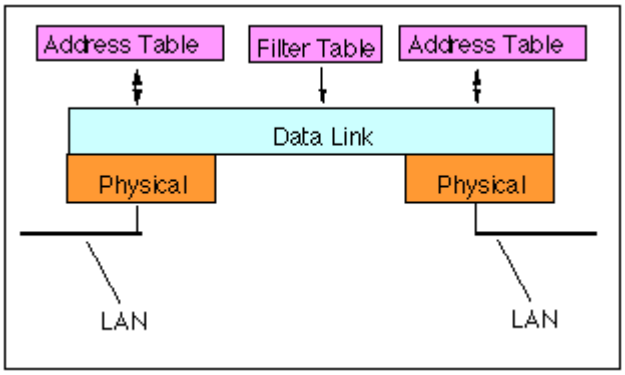


Một bridge nối hai mạng LAN (A và B)

Để học địa chỉ đã được sử dụng, các cổng (ports) – là phần giao diện của Bridge gần nhất sẽ liên kết tới, Bridge quan sát phần header của Ethernet frames khi nó nhận được. Ví dụ như địa chỉ nguồn MAC của mỗi frame nó nhận được, và nó cập nhật vào ngay cổng nơi mà nó nhận được frame. Bridge có thể học địa chỉ phụ thuộc vào các máy tính liên kất đến các máy tính tên mỗi cổng của nó. Điều này gọi là "learning". Như hình vẽ trên có 3 máy tính X,Y,Z, giả thiết ràng mỗi máy tính đều gửi các frame đến các máy tính khác. Địa chỉ nguồn của X,Y sẽ được quan sát bởi mạng A, trong khi

địa chỉ của máy tính Z lại được theo dõi bởi mạng B





Một bridge lưu trữ các địa chỉ phần cứng được quan sát từ các frame nhận được bởi mỗi cổng và sử dụng thông tin này để học các frame cần thiết phải truyền tiếp bởi bridge

Bridge có thể lưu trữ địa chỉ phần cứng học được từ frame nó nhận về trong giao diện giao tiếp và nó sử dụng thông tin này để dùng cho các frame cần forward đến Bridge

Địa chỉ học được được lưu trư trên bảng địa chỉ giao diện của mỗi cổng. Mỗi lần bảng này được gọi đến Bridge sẽ kiểm tra địa chỉ đích của tất cả các frame mà nó nhận được, sau đó nó kiểm tra tất cả các bảng giao diện

trên tất cả các cổng. Nếu frame nào có địa chỉ trùng với địa chỉ trong bảng (một gói với địa chỉ nguồn chỉ đến địa chỉ đích hiện tại). Có 3 khả năng có thể xảy ra:

Nếu địa chỉ không tìm thấy, không có frame nào được nhận ở nguồn. Địa chỉ nguồn có thể không tồn tại, hoặc không có frame nào sử dụng địa chỉ này vì không có trong bảng (địa chỉ cũng có thể bị xoá bởi bridge bởi địa chỉ này lâu ngày không được sử dụng). Bridge không biết cổng cần forward tiếp frame này, do đó nó sẽ gửi ra các cổng khác trừ cái cổng mà nó đã nhận được frame này. Điều này gọi là flooding

Nếu địa chỉ được tìm thấy ở bảng giao diện và địa chỉ này phù hợp với địa chỉ ở cổng nó nhận được thì frame này sẽ không được gửi đi nữa (nó có thể đã được nhận rồi)

Nếu địa chỉ được tìm thấy ở bảng giao diện và địa chỉ này không phù hợp với địa chỉ ở cổng nó nhận được frame thì Bridge sẽ forward frame này tới cổng phù hợp với địa chỉ đó.

Gói thông tin với nguồn của X và đích của Y được nhận và huỷ bỏ khi máy tính Y kết nối trực tiếp tới LAN A, noi mà gói thông tin từ X với đích của Z forward tới mạng B bởi Bridge .

♣ Broadcast and Multicast

Bridge forward broadcast frame ra ngoài tất cả các cổng ngoại trừ cổng nơi mà nó nhận được frame. Hành động thông thường cho multicast frame giống như broadcast frame. Điều này rất thuận lợi vì Bridge có thể multicast frame tới từng phần của mạng cần nhận gói dữ liệu thôi. Một số Bridge thực hiện extra processing để điều khiển sự quá tải của multicast frames

♣ Quản lý bảng giao diện(Managing the Interface Tables)

Bridge thực hiện quản lý bảng giao diện bằng cấu trúc dữ liệu phần mềm hay sử dụng hay sử dụng chip bộ nhớ địa chỉ nội dung (Contents Addressable Memory (CAM)). Trong cả hai trường hợp kích thước của bảng

phải được định nghĩa và luôn luôn bắt buộc 1000's - 10 000's lần vào. Trong mạng LAN lớn điều này có thể được giới hạn.

Để kiểm soát các bảng nhỏ hất hết các Bridge duy trì cơ chế kiểm tra các địa chỉ được sử dụng nhiều gânf đây nhất. Địa chỉ nào không được sử dụng hay sử dụng cách đây quá xa mà không thấy sử dụng lại sẽ bị xoá đi. Điều này có thể ảnh hưởng đến các địa chỉ không được sử dung thường xuyên ở một nút mạng. Còn địa chỉ khi được sử dụng lại, trước khi frame được nhận từ nguồn, nó sẽ ,yêu cầu frame xuất hiện trên tất cả các cổng

Sự lợi ích của việc xoá các địa chỉ cũ là bảng giao diện của Bridge sẽ chỉ ghi địa chỉ MAC. Nếu NIC ngường việc gửi địa chỉ sẽ bị xoá khỏi bảng. Nếu sau đó NIC kết nối lại, nối vào sẽ được phục hồi nhưng kết nối đến cổng khác, nối vào khác sẽ được tạo tương ứng với địa chỉ cần đến. Bridge luôn luôn cập nhật bảng địa chi giao diện cho mỗi địa chỉ nguồn trong khi nhận frame MAC, do đó thậm chí nếu máy tính thay đổi điểm kết nối, hay kết nối lần đầu tiên Bridge sẽ cập nhật lại ngay khi có kết nối đến.

♣ Filter Tables

Trong một số Bridge, phần điều khiển của hệ thống có thể lờ đi việc forwarding thông thường bởi việc chèn vào các đường đi trong bảng lọc để hạn chế việc forwarding giữa các nhóm khác nhau (ví dụ đảm bảo sự an toàn cho các trường hợp đặc biệt của địa chỉ MAC). Bảng lọc chứa danh sách địa chỉ nguồn hay địa chỉ đích. Frame mà được phép thoả mãn các lối đi (entries) trong bảng lọc (filter table) sẽ được forward tới các cổng một cách rõ ràng.

2.2.2. Các công nghệ Switching.

Switch là thiết bị sử dụng để ghép nối với các nút mạng, Switch có khả năng Multiprocessor, mỗi cổng điều khiển bằng một processor nên có thể chuyển tiếp dữ liệu cho nhiều cổng do đó nhờ có Switch mạng máy tính có khả năng tăng tốc độ lên.

2.2.2.1. Layer 2 LAN Switching

Switch hoạt động ở tầng Datalink do đó nó có thể tiếp nhận và xử lý các Frame. Bạn có thể nghĩ về các Switch như là Bridge có nhiều cổng. Trong chương 1, đã đề cặp đến Switch là một phần cứng cơ sở, điều đó có nghĩa là chúng sử dụng các địa chỉ MAC từ các Card kết nối của các máy chủ để lọc được một mạng xác định. Bạn cần phải nhớ cách mà các Switch sử dụng các mạch tích hợp ứng dụng đặc biệt để xây dựng và lưu trữ các bảng lựa chọn.

Bạn không thể ra ngoài và mua một Bridge, nhưng để hiểu các Bridge được thiết kế và lưu trữ như thế nào là cả vấn đề quan trọng bởi vì các Switch hai lớp thực hiện dưới một hình thức như nhau.

Ba chức năng thay đổi tại lớp hai

Sự thay đổi tại lớp hai có ba chức năng khác nhau :

Quá trình học địa chỉ :

Các Bridge và các Switch ở lớp hai nhớ lại địa chỉ nguồn của mỗi frame được thu và đưa nó vào một cơ sở dữ liệu có tên là MAC.

Quyết định chuyển / lựa chọn :

Khi một frame được thu , switch kiểm tra địa chỉ nơi đến của frame đó và cổng ra ở trong cơ sở dữ liệu MAC.

Thoát khỏi vòng lặp:

Nếu có nhiều sự kết nối giữa các Switch được thiết lập để tăng độ dư thừa cho mạng thì có thể xuất hiện các vòng lặp trên mạng. STP được sử dụng để kết thúc các vòng lặp này mà vẫn đảm bảo được tính dư thừa của mạng.

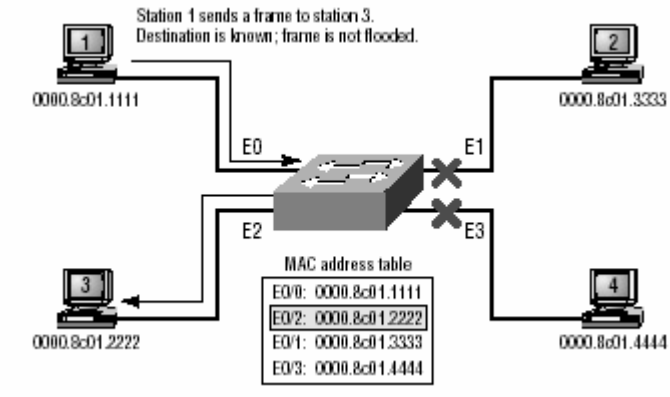
Các chức năng vừa trình bày ở trên sẽ được thảo luận một cách chi tiết ở những phần tiếp theo:

Quá trình học địa chỉ :

Các Switch ở lớp hai có nhiệm vụ ghi nhận địa chỉ. Khi một Switch được hoạt động, bảng lựa chọn Mac là rỗng. Khi một thiết bị truyền và một frame được nhận ở trên cổng kết nối thí Switch sẽ lấy địa chỉ nguồn và vị trí của frame này trong bảng lựa chọn MAC. Nó nhớ lại vị trí cổng tương ứng

với từng thiết bị được xác định. Khi không biết được vị trí của thiết bị đích cần truyền thì Switch không lựa chọn và frame này được truyền đi trên toàn mạng.

Nếu một thiết bị trả lời và truyền một frame trở lại thì Switch sẽ lấy địa chỉ nguồn từ frame này, đặt địa chỉ MAC vào trong cơ sở dữ liệu và kết hợp địa chỉ đó với cổng thu frame. Bởi vì Switch bây giờ có hai địa chỉ MAC trong bảng lựa chọn nên các thiết bị này có thể tạo ra được các liên kết điểm - điểm và các frame này chỉ được truyền đi giữa hai thiết bị mà thôi. Đây là một chức năng hơn hẳn của các Switch ở lớp hai so với các Hub. ở trong mạng Hub tất cả các Frame được truyền đi tới tất cả các cổng ở mọi thời điểm.



Hình 4.1 : Chỉ ra các thủ tục xây dựng cơ sở dữ liệu MAC.

Trong hình vẽ này ta thấy có bốn máy chủ cùng kết nối với Switch, Khi bắt đầu làm việc Switch này không có gì trong bảng địa chỉ MAC. Hình vẽ chỉ ra bảng lựa chọn MAC của Switch này khi từng máy đã kết nối với nó.Các bước sau sẽ chỉ ra cách cập nhật bảng này :

(1) : Trạm 1 gửi một frame tới trạm 3.

Địa chỉ MAC của trạm 1 là : 0000.8c01.1111. Địa chỉ MAC của trạm 2 là : 0000.8c01. 2222.

(2) : Switch sẽ thu frame này trên thiết bị ghép tương thích Ethernet 0/0. Và đặt địa chỉ nguồn vào trong bảng địa chỉ MAC.

(3) : Bởi vì địa chỉ đích không ở trong cơ sở dữ liệu MAC nên frame này sẽ được truyền tới tất cả các cổng kết nối.

(4) : Trạm 3 thu được frame đó và gửi trả lời lại trạm1. Switch sẽ thu frame này trên thiết bị ghép tương thích Ethernet 0/2. Và đặt địa chỉ nguồn của nó vào trong cơ sở dữ liệu Mac.

(5) : Trạm 1 và trạm 3 sẽ tạo ra kết nối điểm - điểm và hai trạm này sẽ thu các frame. Trạm 2 và trạm 4 sẽ không được biết gì về các frame này.

Nếu hai thiết bị không thể trao đổi thông tin với Switch trong khoảng thời gian xác định, khi đó Switch sẽ kích hoạt tất cả các đầu vào từ cơ sở dữ liệu để dữ cho cơ sở dữ liệu đó có khả năng như hiện tại.

Quyết định chuyển tiếp/ loc

Switch hai lớp cũng sử dụng bảng lọc địa chỉ MAC để chuyển tiếp và lọc các frame nhận được trên switch. Khi một frame đến một switch, địa chỉ vật lý đích được so sánh với các địa chỉ trong cơ sở dữ liệu địa chỉ MAC chuyển tiếp/lọc. Nếu địa chỉ vật lý được biết, có trong cơ sở dữ liệu, frame được gửi ra đúng cổng yêu cầu. Switch không đẩy frame ra bất cứ cổng nào ngoại trừ cổng đích.

Nếu địa chỉ đích phần cứng không được liết kê trong cơ sở dữ liệu MAC, frame được gửi đến tất cả các cổng hoạt động ngoại trừ cổng trên đó frame được nhận. Nếu một thiết bị chả lời broadcast, cơ sở dữ liệu MAC được cập nhật với cổng thiết bị đó.

Các frame Multicast và Broadcast

Nhớ lại rằng các switch hai lớp chuyển tiết tấp cả các *broadcast.* Quyết định chuyển tiếp hoặc lọc không sử dụng trong tình huống broadcast bởi vì các frame boadcast và multicast không có một địa chỉ phần cứng đích cụ thể.

Địa chỉ nguồn sẽ luôn luôn là địa chỉ phần cứng của thiết bị phát frame , và địa chỉ nơi đến hoặc sẽ là toàn số 1 (broadcast), hoặc nó sẽ là một sự kết hợp của địa chỉ mạng hoặc địa chỉ subnet được chỉ rõ và các số

1 cho địa chỉ host (multicast). Ví dụ, một broadcast và multicast biểu điễn bằng các số nhị phân được chỉ ra trong Bảng 4.2.

Bảng 4.2

	Binary	Decimal
Broadcast	11111111.11111111.11111111.11111	255.255.255.255
Multicast	10101100.00010000.11111111.11111	172.16.255.255

Dù chúng tôi đã đưa cho cho bạn một ví dụ về một địa chỉ multicast, thuật ngữ multicast thường sử dụng với cái nhìn tới những nhóm multicast sử dụng vùng địa chỉ IP lớp D.

Chú ý rằng broadcast tất cả các bits bằng 1 còn multicast thì không. Cả hai đều là một loại broadcast, chỉ có điều multicast gửi frame cho duy nhất một mạng hoặc mạng con nhất định và tất cả host bên trong mạng hoặc mạng mạng con đó, trong khi mà một broadcast gửi frame cho tất cả các mạng và tất cả các host.

Khi một switch nhận các loại frame này, các frame nhanh chóng được chuyển tiếp tới tất cả các cổng tích cực của switch (chế độ mặc định). Để các broadcasts và multicasts được chuyển tiếp tới các cổng xác định, bạn tạo ra các LANs , điều này không được đề cập trong tài liệu này.

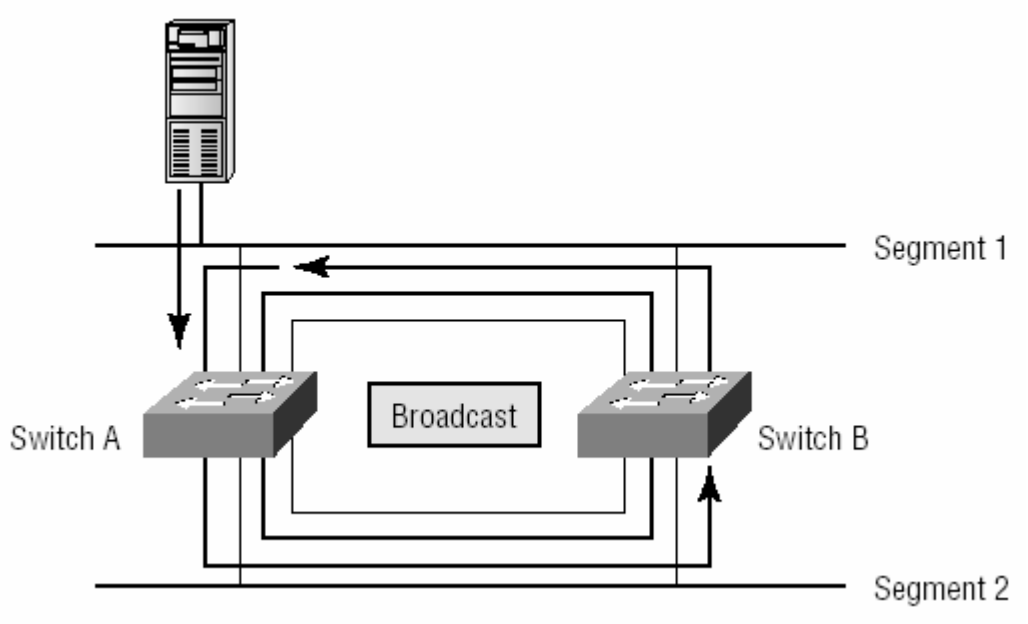
Vòng lặp tránh lỗi

Cuối cùng, switch hai lớp có trách nhiệm vòng tránh lỗi. Sẽ là một ý tưởng tốt khi sử dụng những mối liên kết thừa giữa những các switch. Chúng giúp khắc phục các lỗi mạng do một mối liên kết lỗi. Những mối liên kết thừa mặc dù có ích vô cùng, nhưng chúng gây ra nhiều vấn đề hơn hơn

chúng giải quyết. Trong những mục sau, chúng ta sẽ bàn luận về vài vấn đề nghiêm túc nhất:

- Các cơn bão Broadcast
- Nhiều frame được copy
- Đa vòng lặp

Các hệ thống broadcast



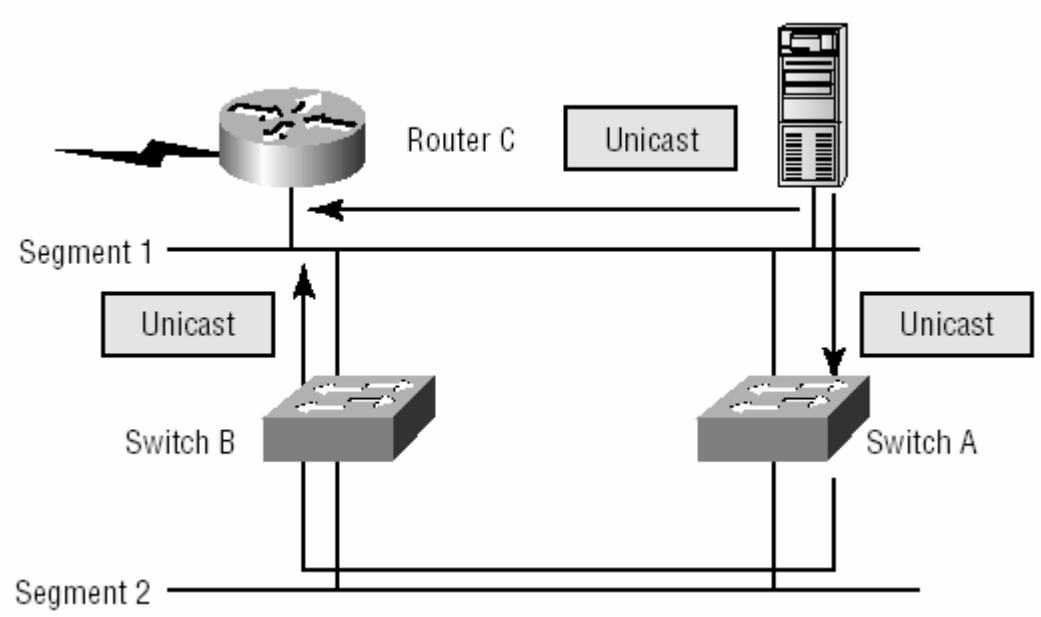
Nếu không có sự phối hợp vòng tránh phù hợp, thì các switch sẽ làm ngập lụt vĩnh viễn khắp các liên kết mạng bởi các broadcast. Điều này đôi khi được biện dẫn như một cơn bão broadcast. Hình 4.2 chỉ ra bằng cách nào một broadcast có thể được truyền lan khắp cả mạng.

Hình 1 Cơn bão broadcast

Nhiều frame được copy

Vấn đề khác là một thiết bị có thể nhận nhiều bản copy của cùng một frame bởi vì frame có thể đến từ các đoạn khác nhau cùng lúc. Hình 4.3 chỉ ra bằng cách nào nhiều frame có thể đến từ nhiều đoạn đồng thời.

Hình 2 Nhiều frame được copy



Bảng lọc địa chỉ MAC sẽ lúng túng về nơi một thiết bị được định vị bởi vì switch có thể nhận frame của hơn một mối liên kết. Có thể nói rằng switch không thể chuyển tiếp một frame được bởi vì nó cập nhật triền miên bảng lọc địa chỉ MAC với các vùng địa chỉ phần cứng nguồn được xác định .

Nhiều vòng lặp

Một trong những vấn đề lớn nhất là nhiều vòng phát sinh khắp nơi một liên kết mạng. Cái này có nghĩa rằng những vòng lặp có thể xuất hiện bên trong những vòng khác. Nếu một cơn bão broadcast khi đó xuất hiện, thì mạng không có khả năng thực hiện đóng chuyển gói. Để giải quyết ba vấn đề này, giao thức Spanning Tree ra đời.

2.2.2.2. Layer 3 Switching.

Sự khác nhau duy nhất giữa một layer 3 switch và một router là cách người quản trị tạo ra sự thực hiện vật lý. Các router ruyền thống sử dụng các bộ vi xử lý để tạo các quyết định có chuyển tiếp hay không và các switch thực hiện việc chuyển tiếp dữ liệu chỉ dựa trên phần cứng. Tuy nhiên, một vài router truyền thống có thể có các chức năng phần cứng khác như là trong một vài loại của kiểu higher-end. Các layer 3 switch có thể được đặt ở bất cứ nơi nào trong mạng bởi vì chúng điều khiển sự lưu thông hiệu năng cao của mạng LAN và giá cả hợp lý hơn để thay thế cho router.

Layer 3 Switching là chuyển tiếp gói tất cả dựa trên phần cứng, và tất cả các gói chuyển tiếp được thực hiện bởi phần cứng ASICs. Layer 3 Switch thực sự là không khác nhau về chức năng so với một router truyền thống và thực hiện cùng các chức năng được liệt kê sau đây:

- Xác định đường đi dựa trên địa chỉ lôgic
- Chạy kiểm tra lỗi tầng 3 (chỉ trên header)
- Sử dụng Time To Live (TTL)
- Xử lý và trả lời bất cứ thông tin lựa chọn nào
- Có thể cập nhật giao thức quản lý mạng đơn giản (Simple Network Management Protocol-SNMP) trong đó quản lý dựa trên thông tin (Management Infomation Base-MIB)
- Cung cấp sự an toàn, bảo mật

Các lợi ích của layer 3 switching gồm có:

- Chuyển tiếp gói dựa trên phần cứng
- Chuyển tiếp gói hiệu năng cao
- High-speed scalability
- Độ trễ nhỏ
- Giá thành của mỗi cổng nhỏ
- Flow accounting
- An toàn, an ninh
- Chất lượng phục vụ (QoS)

2.2.2.3. Layer 4 Switching.

Layer 4 Switching được coi như là công nghệ layer 3 switching dựa trên phần cứng và cũng có thể coi là ứng dụng (ví dụ như là Telnet hoặc FTP). Layer 4 Switching cung cấp thêm sự dẫn đường hơn tầng 3 bằng cách sử dụng số hiệu cổng được tìm thấy trong header tầng Transport để quyết định chọn đường đi. Những số hiệu cổng này được tìm thấy trong Request for Comment (RFC) 1700 và tham khảo các giao thức tầng cao hơn, chương trình và các ứng dụng.

Thông tin tầng 4 được sử dụng để trợ giúp việc quyết định chọn đường đi cho hầu hết các loại. Ví dụ như các danh sách truy nhập mở rộng có thể được lọc dựa trên các số hiệu cổng tầng 4. Một ví dụ khác là tính toán thông tin được lấy bởi switching NetFlow trong các router higher-end của Cisco.

Lợi ích lớn nhất của layer 4 switching đó là người quản trị mạng có thể cấu hình một layer 4 switch để ưu tiên lưu thông dữ liệu bởi ứng dụng, có nghĩa là chất lượng phục vụ (QoS) có thể được xác định đối với mỗi một người dùng. Ví dụ như một số người dùng có thể được xác định như là một nhóm video và có nhiều quyền ưu tiên, hoặc băng thông dựa trên sự đòi hỏi để thực hiện videoconferencing.

Tuy nhiên, người dùng có thể là thành phần của rất nhiều nhóm và chạy rất nhiều ứng dụng, các layer 4 switch phải có thể cung cấp một bảng lọc rất lớn hoặc khoảng thời gian trả lời sẽ trải qua. Bảng lọc này phải to hơn nhiều so với bảng của switch layer 2 hoặc layer 3. Layer 2 Switch có thể chỉ có bảng lọc lớn bằng số người dùng kết nối vào mạng, có thể thậm chí là ít hơn nếu một vài trung tâm được thực hiện với cơ cấu chuyển mạch. Tuy nhiên, một layer 4 switch có thể có 5 hoặc 6 đầu vào cho mỗi một thiết bị kết nối vào mạng! Nếu layer 4 switch không có bảng lọc bao gồm tất cả các thông tin, switch sẽ không thể tạo ra các kết quả với tốc độ cao.

2.2.2.4. Multi-Layer Switching (MLS).

Multi-Layer Switching kết hợp các công nghệ của layer 2, 3 và 4 switching và cung cấp high-speed scalability với độ trễ nhỏ. Nó hoàn thành sự kết hợp này cho ra tốc độ cao với độ trễ nhỏ bằng cách sử dụng các bảng lọc rất lớn dựa trên tiêu chuẩn thiết kế của người quản trị mạng.

Multi-Layer Switching có thể tạo ra lưu thông với tốc độ lớn và cũng cung cấp khả năng dẫn đường tầng 3 là cái có thể loại bỏ khả năng thắt cổ chai cho các router mạng. Công nghệ này dựa trên ý kiến một đường đi, nhiều chuyển mạch.

Multi-Layer Switching có thể tạo ra quyết định đường đi/chuyển mạch dựa trên những điều sau:

- Địa chỉ MAC nguồn/đích trong frame Data Link
- Địa chỉ IP nguồn/đích trong header tầng Network
- Giao thức trong header tầng Network
- Số hiệu cổng nguồn/đích trong header tầng Transport

Không có sự khác nhau nào trong việc thể hiện giữa switch tầng 3 và tầng 4 bởi việc quyết định đường đi/chuyển mạch là đều dựa trên phần cứng.

2.3. Transparent bridging

2.3.1. Cơ sở.

Các bridge trong suốt được phát triển đầu tiên tại Công ty Thiết bị Số (Digital Equipment Corporation) vào đầu những năm 1980. Công ty Digital đã đệ trình công trình này tới Viện những kỹ sư Điện tử và Điện (IEEE), viện này xác nhập công trình này vào trong tiêu chuẩn IEEE 802.1. Các bridge trong suốt rất phổ biến trong Ethernet hoặc những mạng theo chuẩn IEEE 802.3. Chương này cung cấp một tổng quan về cách thức tiến hành giao thông của các bridge trong suốt và các thành phần giao thức.

Các bridge trong suốt có tên như vậy bởi vì bộ dạng và sự hoạt động của chúng là trong suốt đối với hệ thống các host. Khi các bridge trong suốt được bật lên, chúng học cấu hình (topology) của mạng bởi việc phân

Host address	Network number
15	1
17	1
12	2
13	2
18	1
9	1
14	3
.	.
.	.
.	.

S13754

tích địa chỉ nguồn của của các frame được gửi đến từ tất cả các mạng mà bridge được gắn vào đó. Nếu, cho ví dụ, một bridge thấy một khung đến trên Line 1 từ một Host A , bridge kết luận Host A có thể được tìm thấy qua mạng bằng việc kết nối tới Line 1. Qua quá trình này, bridge trong suốt xây dựng một bảng , như hình vẽ:

Cấu hình 26-1: Các bridge trong suốt xây dựng một bảng xác định rằng một host có thể truy cập

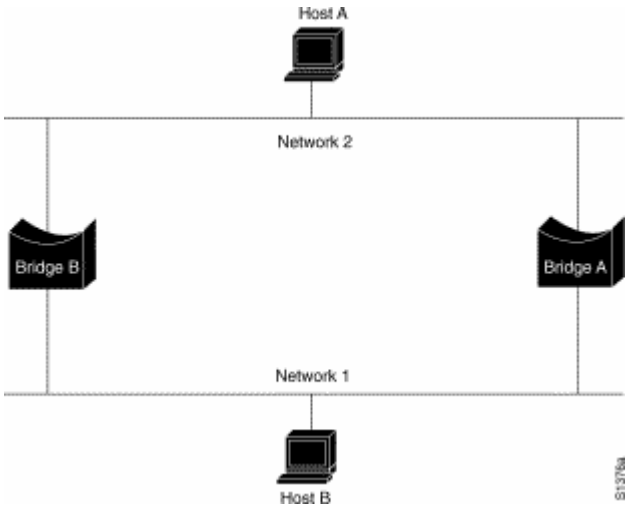
Bridge sử dụng bảng của nó như cơ sở để truyền tiếp. Khi một khung nhận được từ một trong các cổng của bridge, bridge xem địa chỉ nơi đến của khung trong bảng nội tại của nó. Nếu bảng chứa liên hệ giữa địa chỉ nơi đến và bất kỳ cổng nào của bridge ngoài cổng trên đó khung nhận được, thì khung được đẩy tới cổng đó. Nếu không có mối liên hệ nào được tìm thấy, thì khung được đẩy tới tất cả các cổng trừ cổng mà frame đó được nhân. Các Broadcast và Multicast cũng hoạt động tương tự theo cách này.

Các bridge trong suốt cô lập rất thành công giao thông trong đoạn, do đó giảm bớt giao thông trên mỗi đoạn riêng lẻ. Điều này thông thường cải thiện thời gian trễ của mạng, như được nhìn thấy bởi người dùng. Giới hạn giao thông được giảm bớt và thời trễ của mạng được cải thiện phụ thuộc vào mật độ giao thông trong đoạn liên, cũng như số lượng truyền thông của các Broadcast và Multicast.

Không có một nghi thức bridge - bridge, giải thuật Bridge - trong suốt không thể thực hiện được khi tồn tại nhiều đường nôi, nối các bridge, và các mạng cục bộ (LANs) giữa bất kỳ hai mạng LANs nào trong liên kết mạng. Hình 26.2 minh hoạ một vòng bridge như vậy.

Giả thiết Host A gửi một frame cho Host B. Cả hai bridge nhận frame và kết luận chính xác Host A trên mạng 2. Không may, sau đó Host B nhận hai bản "frame copy" của Host A , cả hai bridge lần nữa sẽ nhận khung trên các cổng, nối với mạng 1, của chúng vì tất cả các Host nhận tất cả thông điệp dạng broadcast. Trong vài trường hợp, các bridge sẽ thay đổi các bảng bên trong của chúng để xác định rằng Host A thuộc về Mạng 1. Như vậy

thì, khi Host B trả lời cho frame của Host A, cả hai bridge sẽ nhận rồi sau đó thả các trả lời bởi vì các bảng của chúng sẽ xác định rằng nơi đến (Host A) là trên cùng đoạn mạng như frame nguồn.



Hình 26 2 : các vòng bridge dẫn đến chuyển tiếp không và học trong trong môi trường bridge trong suốt không chính xác.

2.3.2. Các vòng bridge

Ngoài những vấn đề kết nối cơ bản, sự tăng nhanh của những thông báo broadcast trong các mạng với những vòng đại diện một vấn đề mạng nghiêm túc tiềm tàng. Xem lại Hình 26 2 lần nữa, giả thiết frame ban đầu của Host A là một broadcast. Cả hai bridge sẽ tiếp tục chuyển tiếp các frame, sử dụng tất cả dải thông của mạng và khóa sự truyền thông của các gói khác trên cả hai đoạn.

Một cấu hình (topology) với các vòng , như được chỉ ra trong Hình 26 2, có thể rất hữu ích cũng như có hại tiềm tàng. Một vòng ngụ ý rằng sự tồn tại nhiều đường dẫn xuyên qua liên kết mạng, và một mạng với nhiều đường từ nguồn tới đích có thể tăng thêm tính chịu đựng lỗi mạng qua đó cải thiện tính linh hoạt của tôpô.

Chương III Hoạt động của Token Ring Bridge và Switch

3.1. Giới thiệu về mạng Token Ring

IBM giới thiệu phiên bản Tocken Ring vào năm 1994 như một phần trong giải pháp và khả năng nối kết dành cho toàn bộ máy tính và môi trường máy tính của IBM, bao gồm:

- Máy tính cá nhân
- Máy tính tầm chung
- Mainframe và môi trường kiến trúc mạng hệ thống
- Mục tiêu của phiên bản Token Ring là thực hiện một cấu trúc đi dây đơn giản, dùng cáp xoắn đôi nối máy tính vào mạng thông qua ổ cắm điện trên tường và có đường dây chính tập trung ở một nơi.

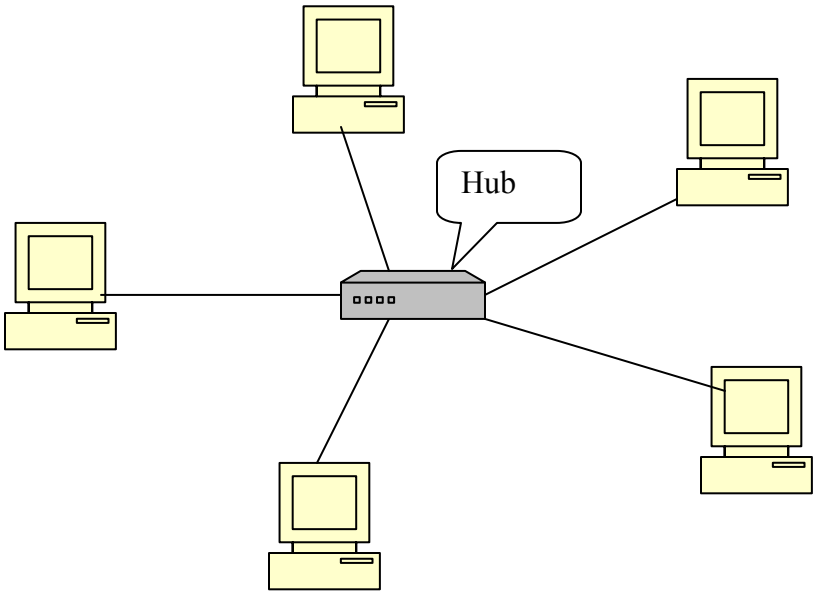
Vào năm 1985, kiến trúc Token Ring của IBM trở thành tiêu chuẩn của ANSI/IEEE.

Các đặc tính của Token Ring

Mạng Token Ring là một ứng dụng thực tế của tiêu chuẩn IEEE 808.2. Chính phương pháp truy nhập vòng chuyền thẻ bài, chứ không phải sơ đồ cáp, phải phân biệt mạng Token Ring với các mạng khác.

Kiến trúc

Kiến trúc mạng Token Ring điển hình bắt đầu với vòng vật lý. Tuy nhiên, trong ứng dụng thực tế của IBM, vòng cáp hình sao (Star Ring), các máy tính trên mạng được nối với một hub trung tâm. Vòng logic biểu thị đường đi của thẻ bài (token) giữa 2 máy tính. Vòng cáp vất lý trong thực tế nằm trong hub. Người dùng là thành phần của vòng, nhưng họ lại nối kết với vòng qua hub.



Hình 3.1.1 Vòng logic sô đồ dây dẫn trên thên thực tế lại chạy qua hub

Bặc điểm cơ bản của Token Ring

Mạng Token Ring có những đặc tính sau:

- Cấu hình star ring
- Phương pháp truy nhập: chuyển thẻ bài (token passing)
- Cáp UTP và STP (IBM Loại 1, 2 và 3)
- Tốc độ truyền 4 Mbps và 16 Mbps
- Truyền dải rộng
- Quy cách ký thuật 802.5

Dạng thức khung

Hình 3.1.2 minh hoạ dạng thức cơ bản của khung dữ liệu Token Ring. Khích thước các trường trong Hình 13.2 không đại diện cho kích thước trường trong khung thất. Trường dữ liệu chiếm phần lớn khung.

Giới hạn đầu	Điều khiển truy nhập	Điều khiển khung	Địa chỉ đích	Địa chỉ nguồn	**Dữ liệu**	CRC	Giới	Trạng thái khung

Hình 3.1.2

Hình 2 Khung dữ liệu Token Ring

Trường	Mô tả
Giới hạn đầu	Cho biết vị trí bắt đầu khung
Điều khiển truy nhập	Chó biết mức ưu tiên của khung và cho biết nó là thẻ bài hay khung dữ liệu
Điều khiển khung	Hoặc chưa thông tin Media Access Control cho mọi máy tính hoặc chứa thông tin " trạm cuối" cho chỉ một máy tính
Địa chỉ nguồn	Cho biết máy tính nào đã gởi khung
Địa chỉ đích	Chó biết địa chỉ máy tính sẻ nhậ khung
Thông tin chính, tức tín hiệu	Dữ liệu gởi
Chuỗi kiểm khung	Thông tin kiểm tra lỗi CRC
Giới hạn cuối	Cho biết vị trí kết thúc khung
Trạng thái khung	Chó biết khung có được thừa nhận, sao chép hay không và cho biết có đại chỉ đích hay không.

Phương pháp vần hành của vòng chuyển thẻ bài

Khi máy tính đầu tiên trong mạng Token Ring đăng nhập mạng tạo ra một thẻ bài (Token) thẻ bài này du ngoạn quanh vòng, thăm do từng máy tính một cho đến khi có một máy tính phát tín hiệu cho biết nó muốn truyền dữ liệu và giành quyền điều khiển thẻ bài. Thẻ bài là một luông bít định sẵn, cho phép máy tính đặt dữ liệu lên cáp mạng. Máy tính có thể không truyền dữ liệu lên cáp trừ khi nó đạt được quyền sở hữu thẻ bài. Trong khi thẻ bài đăng bị sở hữu bởi một máy tính, những máy tính khác không thể tiến hành truyền dữ liệu. Sau khi lấy được thẻ bài máy tính gửi một khung dữ liệu lên mạng. Khung này tiếp tục chuyển quanh vòng rồi dừng lại tại máy tính có địa chỉ khớp với địa chỉ đích trên khung.

Máy tính đích sao chép khung dữ liệu sang vùng nhớ đêm của nó rồi đánh dấu vào trường trạng thái của khung để thông báo rằng dữ liệu đã được tiếp nhân. Khung dữ liệu lại theo vòng quay trở về máy gửi, tại đây cuộc

truyền được xác nhận là thành công. Máy gửi sẽ loại bỏ khung dữ liệu ra khỏi vòng và gửi lên vòng một thẻ bài mới.

Mỗi lần chỉ có một thẻ bài hoạt động trên mạng và thẻ bài chỉ xoay vòng theo một chiều. Chuyển thẻ bài mang tính quyết định, có nghĩa là máy tính không thể truy cập mạng như nó vẫy có thể truy nhập trong môi trường CSMA/CD. Nếu thẻ bài có sẵn, máy tính có thể sử dụng thẻ bài để gửi dữ liệu. Mối máy tính đóng vai chò như một bộ chuyển tiếp một chiều, tái tạo thẻ bài và chuyển nó đi.

Giám sát hệ thống

Máy tính đầu tiên đăng nhập mạng được hệ thống Token Ring phân công giám sát hoạt động của mạng. Bộ giám sát này kiểm tra nhằm đảm bảo khung dữ liệu được truyền- nhận đúng nơi, đúng chỗ, bằng cách kiểm tra để tìm xem có khung dữ liệu nào luân chuyển từ một vòng trở lên và đảm bảo mỗi lần chỉ có một thẻ bài trên mạng.

Nhận biết máy tính

Khi một máy tính mới đăng nhập, hệ thông Token Ring kết nạp máy tính đó để nó trở thành một phần của vòng. Thủ tục kết nạp bao gồm:

- Kiểm tra xem có địa chỉ trùng nhau không
- Thông báo cho các máy tính khác trên mạng biết về sự hiện điên của máy tính mới.

Các thành phần phần cứng

- Hub
- Đường cáp
- Cáp nối tạm
- Bộ nối
- Bộ lọc phương tiện

Bảng phân phối

- Bộ chuyển tiếp
- Card mạng
- Cáp quang

3.2. Token Ring switch và bridge

3.2.1. Tổng quan Token Ring Switching

Tại sao các khách hàng lại chuyển sang switch. Ngày nay, các kiến trúc liên mạng chia sẻ phương tiện hub và router đang tiến hóa, bao gồm những công nghệ mới và các khả năng mới đầy hiệu quả. Những người quản

trị mạng ngày càng đòi hỏi triển khai mạng có tính co giãn, đầy mềm dẻo sẽ điều tiết các yêu cầu ngày càng lớn về băng thông, sự ổn định và có thể quản lý, trong khi đó tối thiểu hóa các chi phí tài chính đối với cơ sở hạ tầng mạng. Từ những yêu cầu đó, ngàng công nghiệp mạng đang tiến hóa về phía các kiến trúc mạng mới: đó là liên mạng có chuyển mạch.

Các liên mạng có chuyển mạch tích hợp các thiết bị switch vào các mạng chia sẻ phương tiện để tối ưu hóa lợi ích của cả routing và switching. Các LAN switch được thêm vào để tăng thêm băng thông và làm giảm sự tắc nghẽn trên các hub chia sẻ phương tiện hiện có, trong khi những công nghệ backbone mới như là ATM (Asynchronous Transfer Mode) switching và ATM router, cung cấp các băng thông backbone tuyệt vời hơn có thể đáp ứng các yêu cầu của các dịch vụ đòi hỏi chuyển dữ liệu tốc độ cao qua.

Hỗu hết các nhà thiết kế mạng hiện nay bắt đầu tích hợp các thiết bị switching vào trong các mạng chia sẻ phương tiện hiện có của họ để đạt được các mục đích sau:

- Tăng cường băng thông có thể cho mỗi người dùng, làm giảm bớt sự tắc nghẽn trong mạng chia sẻ phương tiện của họ.

Tốc độ các bộ vi xử lý tăng theo số mũ, ưu điểm của các ứng dụng và các tệp cần nhiều băng thông, và sự mở rộng của số lượng người dùng thách thức khả năng của các mạng chia sẻ phương tiện hiện hành để cung cấp băng thông đủ cho mỗi người sử dụng và thiết bị trên mạng.

- Việc điều khiển các mạng VLAN bằng cách tổ chức các người dùng mạng vào các nhóm làm việc lôgic độc lập với các giao thức vật lý của hệ thống kết nối các hub, để giảm giá của việc di chuyển, thêm vào, thay đổi và cải thiện tính mềm dẻo của hệ thống mạng.
- Triển khai các ứng dụng đa phương tiện nổi bật trên các nền tảng chuyển mạch và các công nghệ khác nhau, làm cho chúng có thể phục vụ một số lượng lớn các người dùng.
- Cung cấp một con đường tiến hóa suôn sẻ tới các giải pháp chuyển mạch hiệu năng cao như là ATM

Người sử dụng trên các mạng LAN chia sẻ thì phải chia sẻ là tranh giành băng thông. Khi một người sử dụng riêng biệt yêu cầu và sử dụng một lượng lớn băng thông thì phần còn lại không còn đáp ứng được cho các người dùng khác trên mạng LAN. Khi yêu cầu về băng thông vượt quá khả năng có thể, các người dùng bị buộc phải đợi do đó làm trễ việc lưu thông và xử lý. Như là một kết quả, số lượng người sử dụng mà một mạng LAN đơn lẻ có thể hỗ trợ là bị giới hạn bởi những yêu cầu về băng thông của những người sử dụng đó.

LAN switching:

- Thay thế cho multiple-bridged LAN
- Cung cấp các kiểu multiple bridging:
  - Transparent bridging
  - Source-route bridging
  - Source-route transparent bridging
  - Source-route switching
- Cung cấp khả năng truyền qua tốc độ cao và độ trễ thấp
- Giảm broadcast (VLAN)
- Hỗ trợ multi-layer switching (tùy chọn)

Rất nhiều người kết hợp LAN switching với Ethernet switching. Ethernet switching truyền thống đã cung cấp nhiều khả năng khá mạnh. Cả switch Ethernet và Token Ring cung cấp nhiều ưu điểm.

Một cấu hình LAN điển hình được tạo lập theo cơ sở hạ tầng vật lý nó đang kết nối với. Các người dùng được phân nhóm dựa theo vị trí của họ trong mối quan hệ với hub họ kết nối với và cách để cáp có thể truyền trong hệ thống đường dây. Sự phân đoạn nói chung được cung cấp bởi router liên kết mỗi hub chia sẻ với nhau. Kiểu của phân đoạn không phân loại các người dùng theo nhóm làm việc kết hợp của họ hoặc yêu cầu về băng thông.

Bởi vì các switch cũng có thể hỗ trợ chế độ multiple bridging, như là transparent bridging (TB), source-route bridging (SRB) hoặc là source-route transparent bridging (SRT), một switch đơn lẻ có thể được sử dụng để thay thế một multiple-bridged LAN.

Các vấn đề kết hợp với các mạng LAN chia sẻ và sự nổi bật của các switch đang gây ra sự thay đổi các cấu hình của mạng LAN truyền thống bằng các cấu hình liên mạng VLAN chuyển mạch. Các cấu hình VLAN chuyển mạch thay đổi các cấu hình LAN theo các cách sau đây:

- Các switch thay thế các hub đầu cuối trong hệ thống đường dây kết nối mạng. Các switch là dễ dàng cài đặt với một sự thay đổi nhỏ hoặc thậm chí là không thay đổi về cáp và có thể hoàn toàn thay thế một hub chia sẻ với mỗi cổng phục vụ cho mỗi người dùng.
- Các VLAN được tạo lập để cung cấp các dịch vụ phân đoạn mà truyền thống được cung cấp bởi các router trong các cấu hình LAN. Một VLAN là một mạng chuyển mạch đó là phân đoạn lôgic bởi các chức năng, các nhóm dự án, hoặc các ứng dụng mà không quan tâm tới vị trí vật lý của người dùng. Mỗi cổng switch có thể được ấn định cho một VLAN. Các cổng trong một VLAN chia sẻ các broadcast. Các cổng không thuộc VLAN đó không chia sẻ các broadcast này. Giảm broadcast sẽ cải thiện toàn bộ hiệu năng của mạng.

- Truyền thông giữa các VLAN được cung cấp bởi routing tầng 3 của mô hình OSI.

Các cấu hình VLAN tập hợp các người dùng bởi sự kết hợp lôgic hơn là vị trí vật lý.

Trong liên mạng có chuyển mạch, các VLAN cung cấp sự phân đoạn và tổ chức mềm dẻo. Sử dụng công nghệ VLAN, bạn có thể phân loại các cổng switch và các người sử dụng kết nối vào chúng vào các truyền thông xác định lôgic thú vị như sau:

- Các bạn đồng nghiệp trong cùng một phòng
- Nhóm sản xuất chức năng chéo nhau
- Các nhóm người sử dụng khác nhau chia sẻ ứng dụng hoặc phần mềm giống nhau (như là các người dùng Lotus Note)

Bạn có thể phân loại các cổng và các người dùng thành các nhóm truyền thông thú vị trong một switch đơn lẻ hoặc trên các switch được kết nối. Bằng cách phân loại các cổng và người dùng cùng với nhau thông qua các switch multiple, các VLAN có thể mở rộng cơ sở hạ tầng xây dựng đơn lẻ, xây dựng liên kết, hoặc thậm chí là các mạng diện rộng (WAN). Các VLAN loại bỏ các ràng buộc vật lý của các truyền thông nhóm làm việc.

Tùy chọn, một switch LAN có thể cung cấp multilayer switching. Về cơ bản, điều này có nghĩa là LAN switch cung cấp một chức năng định hướng (Layer 3 Switching) thêm vào bridging (Layer 2 Switching).

Tại sao sử dụng switch Token Ring:

Một switch Token Ring hoạt động như là một bridge nhiều cổng và cung cấp:

- Các chế độ multiple bridging
- Tốc độ chuyển qua nhanh và độ trễ nhỏ
- Phân đoạn với các VLAN

Đơn giản nhất, một switch Token Ring là một bridge LAN nhiều cổng. Một switch Token Ring nói chung cung cấp chuyển mạch với độ trễ nhỏ và hỗ trợ VLAN.

Phương thức truyền thống để kết nối các phân đoạn Token Ring là sử dụng một bridge source-routing (SRB). Ví dụ như các bridge thường xuyên được sử dụng để nối các vòng nhóm làm việc với vòng backbone. Tuy nhiên, sự khởi tạo của bridge có thể làm giảm đáng kể hiệu năng tại các máy

trạm của người dùng. Các vấn đề hơn nữa có thể được giới thiệu bằng cách tập hợp lưu thông trên vòng backbone.

Để duy trì hiệu năng và tránh tràn vòng backbone, bạn có thể định vị các server trên cùng một vòng như là một nhóm làm việc cần phải truy nhập đến server. Tuy nhiên, việc phân tán các server ở khắp nơi trên mạng là cho chúng khó có thể sao lưu, quản trị và bảo đảm hơn là nếu chúng được định vị trên vòng backbone. Phân tán các server cũng giới hạn số lượng các server mà các máy trạm riêng biệt có thể truy nhập.

Các router backbone có thể cung cấp sự chuyển qua tốt hơn so với các bridge và có thể liên kết một số lượng lớn các vòng mà không trở thành quá tải. Các router cung cấp cả chức năng bridging và routing giữa các vòng và đã phức tạp hóa kỹ thuật điều khiển broadcast. Các kỹ thuật này trở nên ngày càng quan trọng khi số lượng các thiết bị trên mạng tăng lên.

Trở ngại chủ yếu của việc sử dụng router như là một backbone là mối quan hệ giữa giá thành cao tính cho một cổng và thực tế rằng lượng chuyển tiếp nói chung không tăng khi các cổng được thêm vào. Một switch Token Ring được thiết kế để cung cấp sự chuyển qua với tốc độ dây dẫn mà không cần quan tâm đến số lượng cổng trên switch. Thêm vào đó, Catalyst 3900 Token Ring switch có thể được cấu hình để cung cấp độ trễ rất nhỏ giữa các cổng Token Ring bằng cách sử dụng cut-through switching.

Khi là cục bộ, một Token Ring switch cung cấp giá thành nhỏ cho mỗi cổng và có thể có độ trễ nhỏ giữa các liên trạm hơn là router. Thêm vào đó, một switch có thể được sử dụng để đính trực tiếp một số lượng lớn các client hoặc server bởi vậy thay thể sự tập trung

Nói chung, một switch Token Ring được sử dụng cùng chung với một router, cung cấp khả năng kết nối cao giữa các phân đoạn Token Ring trong khi vẫn có điều khiển broadcast và kết nối diện rộng được cung cấp bởi router.

Các chế độ bridging:

Transparent Bridging	Switch based on table lookup of destination MAC address. Parallel paths eliminated via IEEE spanning tree
Source-Route Bridging	Switch decision based upon next hop in Routing Information Field (RIF)
Source-Route Transparent Bridging	Frames with no RIF transparently bridged. Frames with RIFs source-route bridged
Source-Route Translational Bridging	Source-routed frames converted to transparent bridge frames and vice versa
Source-Route Switching	All ports have same ring number. Switch learns MAC addresses of attached stations and source-routing information for stations behind source-route bridges

Có năm chế độ nói chung trong các mạng LAN hiện nay:

Transparent Bridging:

Transparent Bridging đầu tiên được sử dụng trong mạng LAN Ethernet (mặc dù nó thường xuyên được sử dụng trong mạng LAN Token Ring với giao thức IPX, khi khách hàng không muốn cài đặt modul Novell ROUTE.COM)

Source-Route Bridging:

Source-Route Bridging (SRB) là phương thức của bridging được phát triển bởi IBM cho những người dùng trong mạng Token Ring. Với SRB, chủ yếu đường đi tới đích là được xác định trước, trong thời gian thực, ưu tiên việc gửi dữ liệu.

Source-Route Transparent Bridging:

Source-Route Transparent Bridging dùng cả các công nghệ của SRB và transparent bridging trong một thiết bị. Các bridge SRT thực hiện SRB và transparent bridging trong cùng thời gian, một gói cho mỗi lần chuyển.

SRT sử dụng cho các mạng trộn Ethernet và Token Ring trên đó một vài trạm thực hiện source-routing còn một vài trạm thì không. Mạng Token Ring có thể được cấu hình với các giao thức source-route bridge như là SNA và NetBIOS, và các giao thức khác transparent bridge phổ biến nhất là Novell IPX.

Source-Route Translational Bridging:

Source-Route Translational Bridging được sử dụng để chuyển giữa Ethernet và Token Ring, cũng như giữa FDDI và Token Ring.

Source-Route Switching:

Trong Source-Route Switching, switch học và chuyển tiếp các frame dựa trên mô tả source route cho các trạm mà là một hoặc nhiều chặng source-route bridge. Một mô tả đường đi là một phần của trường thông tin định hướng (Routing Infomation Field-RIF) mà xác định một chặng đơn lẻ. Nó được định nghĩa như là một số hiệu vòng, số hiệu bridge.

Khi một source-routed frame đến switch, switch sẽ học mô tả đường đi cho chặng gần nhất đối với switch. Các frame nhận được từ các cổng khác với cùng chặng tiếp theo của mô tả đường đi xác định từ đích của chúng, sẽ được chuyển tiếp đến cổng tương ứng với chặng gần nhất vừa xác định ở trên.

Source-Route Bridging:

Tìm kiếm chặng tiếp theo

Switch quyết định dựa trên chặng tiếp theo trong RIF:

- All Routes Explorers (ARE) cho việc phát hiện đường
- Spanning Tree Explorers (STE) cho lược đồ dữ liệu
- IBM Spanning Tree cho STE frame

Source-Route Bridging (SRB) là phương thức nguyên thuỷ của bridging mà IBM cung cấp cùng với Token Ring. Một Source-Route Bridge tạo tất cả các quyết định chuyển tiếp dựa trên trường thông tin định hướng (Routing Infomation Field-RIF). Nó không nhớ hoặc tìm kiếm các địa chỉ MAC. Bởi vậy, frame không có RIF sẽ không được chuyển tiếp.

Với SRB, mỗi cổng trên switch được ấn định một số hiệu vòng và bản thân switch cũng được ấn định một hoặc nhiều số hiệu bridge. Thông tin này được sử dụng để xây dựng các RIF và để tìm kiếm từ đó xác định khi chuyển tiếp một frame.

Các Source-Route Bridge sử dụng giao thức IBM Spanning-Tree để loại ra các bản sao đường đi. Giao thức IBM Spanning-Tree khác so với giao thức IEEE Spanning-Tree. Nếu switch hỗ trợ SRB, nó cũng có thể hỗ trợ giao thức IBM Spanning-Tree.

Client hoặc server hỗ trợ source routing nói chung sẽ gửi một frame thăm dò để xác định đường đi đến địa chỉ đích. Có hai kiểu frame thăm dò: All Routes Explorers (ARE) và Spanning Tree Explorers (STE). Tất cả các bridge sao chép các frame ARE và thêm thông tin định hướng của chúng. Chỉ các bridge ở trạng thái chuyển tiếp trong spanning tree mới sao chép các frame STE và thêm thông tin định hướng của chúng. Các frame ARE được sử dụng để tìm đường khi các frame ARE vượt qua tất cả các con đường giữa hai thiết bị. Frame STE được sử dụng để gửi lược đồ dữ liệu khi spanning tree chắc chắn rằng chỉ có một bản sao của mỗi frame được gửi tới mỗi vòng.

Source-route Transparent Bridging:

Tìm kiếm địa chỉ MAC và chặng tiếp theo trong RIF

Kết hợp Transparent và Source-route Bridging:

- Các frame không có RIF là transparently bridged

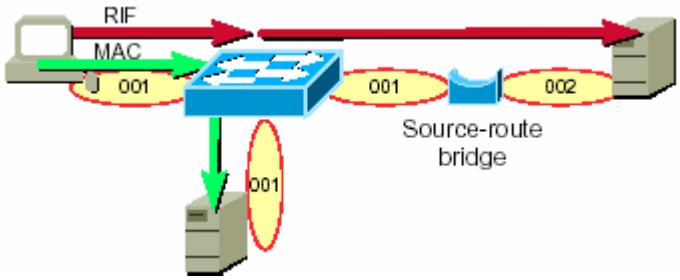
- Các frame có RIF là source-route bridged
- Giao thức IEEE Spanning Tree cho transparent và STE frame

Source-route Transparent Bridging (SRT) là một chuẩn IEEE kết hợp Source-route Bridging và Transparent Bridging. Một bridge SRT chuyển tiếp frame không có RIF dựa trên địa chỉ MAC đích. Frame có RIF được chuyển tiếp dựa trên RIF.

Một vài giao thức như là SNA đầu tiên cố gắng để thiết lập một kết nối sử dụng một frame không có RIF. Trong trường hợp SNA, frame thử nghiệm này sẽ được gửi để xem đích có thuộc cùng một vòng với nguồn không. Nếu frame thử nghiệm không trả lời, thì một ARE test frame với RIF sẽ được gửi. Nếu SRT bridging được sử dụng, frame thử nghiệm đầu tiên không có RIF sẽ được chuyển tiếp thông qua bridge tới đích. Đích sẽ trả lời, và đường đi spanning tree thông qua các bridge sẽ được sử dụng. Mặc dù đường đi này hoạt động, nó vẫn có thể gây rắc rối. Mạng có thể được cấu hình với backbone song song với mục đích lưu thông sẽ được phân tán trên cả hai đường. Điều này sẽ hoạt động tốt nếu source-routing được sử dụng. Tuy nhiên, nếu đường đi spanning tree được sử dụng, thì chỉ có một trong hai backbone được sử dụng để chuyển lưu thông. Backbone còn lại sẽ không được sử dụng trừ phi có lỗi.

Một vấn đề khác là cách sử dụng các bản sao của địa chỉ MAC của gateway SNA. SNA yêu cầu người dùng nhập vào địa chỉ MAC của gateway đích, như là 3745 Token Ring interface coupler (TIC). Để ngăn cản khách hàng phải nhập địa chỉ sao lưu trong trường hợp gateway lỗi, rất nhiều người thiết kế mạng SNA đặt một gateway khác trên một vòng khác với cùng địa chỉ MAC. Điều này sẽ làm việc với source-routing và cho phép tự động phục hồi gateway lỗi. Tuy nhiên, SRT không chấp nhận cùng một địa chỉ MAC trên hai vòng khác nhau.

Source-Route Switching:



- Phân đoạn siêu nhỏ cho các người dùng đầu cuối có nhiều băng thông hơn trong khi duy trì số hiệu vòng
- Switch học các địa chỉ MAC của các trạm kết nối vào các cổng

- Switch học thông tin source-routing cho các trạm trên phía các source-route bridge

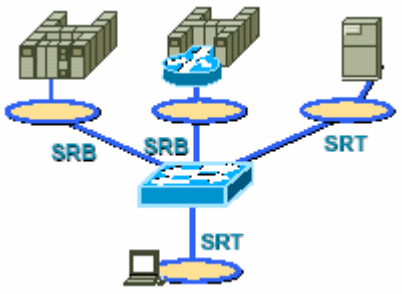
Vì transparent bridging chuẩn không hỗ trợ thông tin source-routing, một chế độ bridging mới, được gọi là source-route switching, đã được tạo ra. Source-route switching chuyển những các frame không chứa đựng thông tin định hướng, theo cùng cách mà transparent bridging làm. Tất cả các vòng mà là source-route switched có cùng số hiệu vòng, và switch học các địa chỉ MAC của những bộ tiếp hợp trên những vòng này.

Ngoài việc học những địa chỉ MAC, switch cũng học những mô tả đường đi. Khi một source-route frame vào switch, switch học mô tả đường đi cho chặng ngắn nhất tới switch. Các switch sâu đó với cùng chặng kế tiếp mô tả đường đi được chuyển tiếp tới cổng với source-route bridge chính xác.

Điều này có hai lợi ích. Trước hết, switch không cần học những địa chỉ MAC của những thiết bị trên phía khác của một source-route bridge, từ đó giảm bớt nhiều số lượng những địa chỉ MAC mà switch phải giữ vững. Thứ hai, switch có thể hỗ trợ các đường đi source-routing song song bằng việc gửi frame tới source-route bridge chính xác.

Trong khi một switch hỗ trợ source-route switching duy nhất có thể được sử dụng tới vi mô phân đoạn một Token Ring hiện hữu trong một mạng source-route bridge, nó không thể sử dụng để thay thế source-route bridge hiện hữu mà không có renumbering các vòng hiện hữu.

Chế độ Bridging cho từng cổng



Ngoài việc hỗ trợ một số lượng lớn các kiểu switching, một Token Ring switch cần phải cũng hỗ trợ những đặc tính mạng hiện hữu. Có hai đặc tính g đặc biệt mà phải được xem xét :

Hỗ trợ các bản sao TIC

Sự hỗ trợ những giao thức (như IPX) cái mà có thể không sử dụng source-routing

Nhiều người dùng SNA với FEPs đã sử dụng một đặc tính gọi là hỗ trợ bản sao TIC, nơi mà multiple Token Ring coupler trên FEP có thể có cùng địa chỉ MAC đó (mặc dù trên những vòng khác nhau). Điều này cung cấp phiên thiết lập lại sử dụng địa chỉ MAC xen kẽ.

Nhiều người dùng IPX chọn transparently bridge lưu thông IPX, hơn là cài đặt thêm đặc tính ROUTE.COM được yêu cầu với source-route bridge lưu thông IPX.

Bởi vậy, SRT switching được yêu cầu đối với lưu thông IPX, và SRB được yêu cầu cho hỗ trợ bản sao TIC. SRT không hỗ trợ những địa chỉ MAC bản sao bởi vì nó không hỗ trợ IBM Spaning Tree hoặc những đường đi song song. Khả năng định nghĩa chế độ switch bởi cổng cho phép hỗ trợ bản sao TIC sẽ được sử dụng trên FEP cổng trong khi lưu thông IPX được gửi chỉ trên những cổng hỗ trợ SRT.

3.2.2. Các phương thức hoạt động của Tokenring Switch

Cũng giống như đối với ethernet switch và bridge, Token Ring switch và bridge cũng có ba kiểu hoạt động chính:

Store-and-forward

Với phương thức hoạt động này, switch nhận toàn bộ gói tin và lưu vào buffer của nó và thực hiện kiểm tra CRC. Bởi vì nó phải nhận toàn bộ gói tin thì mới chuyển tiếp do đó thời gian trễ lớn và biến đổi theo độ dài của gói tin.

Ví dụ đối với một gói tin 4k, truyền trên một mạng 16Mbps thì thì thời gian nhận của nó là 2048 micro giây có nghĩa là hơn 2ms. Thời gian này không phải là lớn nhưng trong một mạng có nhiều bridge switch thì thời gian trễ trên mạng có thể lớn nhất là đối với các giao thức phải chờ việc báo nhận thì mới gửi tiếp được gói tin sau. Điều này làm ảnh hưởng đến hiệu năng của mạng

Cut-through (Real Time)

Theo phương thức này, switch không copy toàn bộ gói tin mà chỉ copy một phần gói tin (từ 20 đến 60 byte) vào buffer của nó. Sau đó nó thực hiện các công việc cần thiết để chuyển tiếp gói tin tới các cổng cần thiết.

Phương thức này làm giảm thời gian trễ nhỏ (cỡ 30 micro giây) trên các switch bởi vì nó chuyển tiếp gói tin đi ngay.

Đối với phương thức này vấn đề quan trọng là :

Cổng để chuyển tiếp gói tin phải sẵn sàng tại thời điểm đó. Trong một mạng có mật độ truyền lớn thì nhiều gói tin phải đợi trước khi được truyền đi. Điều này làm cho mạng mất đi tính tin cậy mà lại không đạt được hiệu quả về tốc độ.

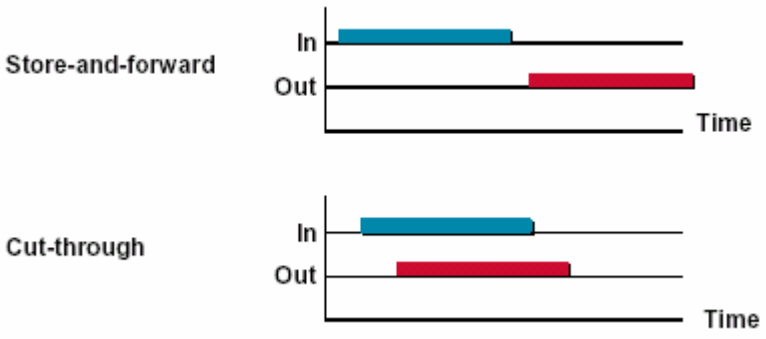
Hai cổng này phải có cùng tốc độ, nếu các cổng không cùng tốc độ thì ta không thể sử dụng phương pháp này.

Không có các kiểm tra lỗi nên các gói tin bị lỗi vẫn được chuyển tiếp đi. Điều này làm tổn phí băng thông của mạng vì việc truyền các gói tin đó là vô ích.

Adaptive cut-through:

Đây là cách kết hợp của phương pháp cut-though và store-and-forward. Switch có thể tự động chuyển giữa hai chế độ này dựa trên một ngưỡng tỉ lệ lỗi do người dùng đặt ra. Ban đầu mạng khởi động ở chế độ cut-through nhưng sau đó nếu tỉ lệ gói tin bị lỗi lớn hơn một ngưỡng nào đó thì cổng đó lại tự động chuyển về kiểu store-and-forward.

So sánh thời gian trễ của hai phương thức cut-through và store-and-forward



3.3. Source-route bridging

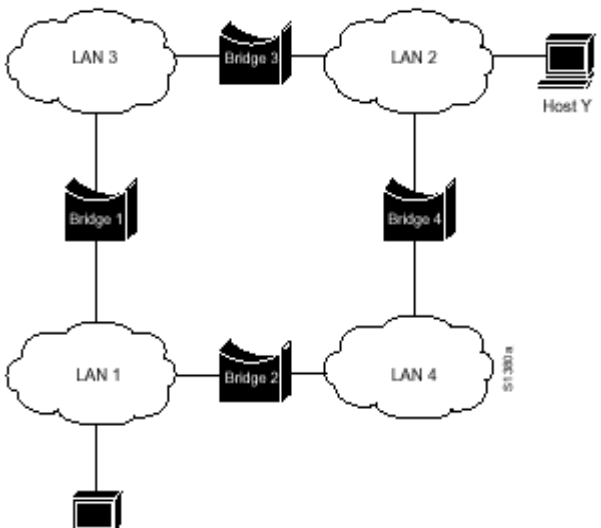
3.3.1. Phần cơ sở

Giải thuật bắc cầu giữa lộ trình và nguồn được phát triển bởi hãng IBM, và được đề nghị với tổ chức IEEE đưa thành chuẩn IEEE 802.5, chuẩn này là cách để nối các mạng LAN với nhau. Từ sự đề nghị đầu tiên đó, IBM đã đưa ra một chuẩn nối mới tới tổ chức IEEE 802 đó là : Giải pháp nối trong suốt giữa lộ trình và nguồn (SRT- the source-route transparent bridging solution). Sự bắc cầu trong suốt giữa lộ trình và nguồn loại bỏ toàn bộ SRB, và đưa ra hai kiểu nối các mạng LAN đó là : Trong suốt và Trong suốt đường đi - nguồn. Mặc dù sự bắc cầu SRT đã có được những hỗ trợ nhất định nhưng các kiểu hoạt động SRB vẫn được thực hiện trên một phạm vi rộng. Phần này trình bày về giải thuật gửi frame SRB cơ bản và miêu tả cá trường của frame SRB.

3.3.2. Giải thuật SRB .

SRBs có tên như vậy bởi vì nơi gửi sẽ đưa toàn bộ thông tin từ nguồn đến đích vào Frame mà nó truyền đi trên toàn mạng LAN. SRBs cất và gử các frame này dựa vào đường đi xác định xuất hiện trong một trường riêng ở trong frame. Hình 25-1 minh hoạ mạng SRB cụ thể.

Trong hình 25-1, Hot X muốn gửi một frame tới Hot Y. ban đầu Hot X không biết Hot Y có cùng trong một mạng LAN hay không. Để xác định điều này, Hot X sẽ gửi một Frame kiểm tra, nếu frame đó quay trở về Hot X mà vẫn



không xác định được vị trí của Hot Y, điều đó có nghĩa là Hot Y ở một mạng LAN khác và đó là vấn đề mà Hot X cần phải biết.

Để xác định một cách chính xác vị trí của Hot Y (Trong trương hợp Hot Y nằm ở một mạng Lan khác), Hot X phải gửi đi một "Frame thăm dò". Mỗi bridge thu "frame thăm dò" này (Trong ví dụ : Bridge 1 và Bridge 2) và copy frame đó tới tất cả các cổng ra của nó. Thông tin về đường đi sẽ được cộng thêm vào frame khi chúng đi qua một mạng con. Khi "frame thăm dò" của Hot X tới Hot Y, Hot Y gửi trả lời tới từng Hot riêng biệt và sử dụng toàn bộ thông tin về đường đi. Khi nhận được tất cả các frame trả lời Hot X sẽ xác điịnh đường đi tốt nhất.

Trong hình vẽ 25-1, đưa ra hai đường đi chính như sau :

☞ LAN 1 → Bridge 1 → LAN 3 → Bridge 3 → LAN 2

☞ LAN 1 → Bridge 2 → LAN 4 → Bridge 4 → LAN 2

Hot 1 phải chọn một trong hai đường đi ở trên. Chuẩn IEEE 802.5 không có một quy định cụ thể nào để phục vụ cho Hot X chọn đường, nhưng nó có một số những gợi ý như sau:

☞ Frame đầu tiên được thu.

☞ Trả lời có chặng đường ngắn nhất

☞ Trả lời với kích thước frame nhỏ nhất.

☞ Sự kết hợp của các chuẩn trước.

Trong hầu hết tất cả các trường hợp đường đi nằm trong frame đầu tiên được thu.

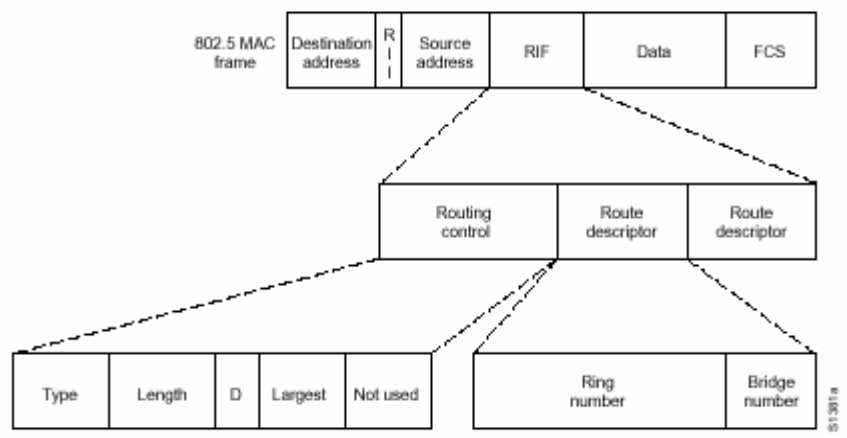
Sau khi đường đi được chọn, nó được đưa vào trường thông tin đường đi (RIF - Routing Information Field) của các frame gửi tới Hot Y. Trường thông tin

tìm đường chỉ nằm trong các frame gửi tới các mạng LAN khác. Các thông tin về đường đi ở trong frame được xác định bằng cách dặt bit quan trọng nhất trong trường địa chỉ nguồn(Source Address field), gọi là bit chỉ báo thông tin về đường (RII).

3.3.3. Định dạng Frame

Trường thông tin về đường đi được minh hoạ cụ thể trong hình25-2, nó gồm có hai trường chính : Trường điều khiển đường và trường đánh dấu đường (*Routing Control* and *Routing Descriptor*). Các trường này được miêu tả một cách tổng quát như sau :

(hình 25 -2)



Hình 25-2 : RIF trong các frame để gửi tới tất cả các mạng LAN (chuẩn IEEE 802.5)

Trường điều khiển đường

Bao gồm bốn trường nhỏ sau : Type, Length, D bit, frame lớn nhất.

☞ Trường Type : Gồm ba kiểu điều khiển đường có thể thực hiện được :

Đường riêng biệt (Specifically routed) : ĐƯợc sử dụng khi nút nguồn cung cấp đường đi xác định trong phần đầu của RIF. Các Bridge gửi frame này bằng cách sử dụng các trường xác định đường đi.

Thăm dò tất cả các đường (All paths explorer): Được sử dụng để tìm các điểm ở xa. Đường đi này được chọn khi frame này đi qua từng mạng. Các Bridge thêm các thông tin : số Bridge, số vòng vào frame khi nó được gửi đi (Bridge cũng cộng số vòng đầu tiên của vòng đầu tiên). Nơi đích đến nhận nhiều frame cũng như nhiều đường đi tới đích.

Thăm dò cây tổng thể (Spanning - tree explorer) : Được sử dụng để tìm cây ở xa. Chỉ những Bridge ở trong cây tổng thể gửi các frame này thì mới thêm số kết nối và số vòng liên kết vào trong frame khi nó được gửi đi. Kiểu thăm dò cây tổng thể đã làm giảm số lượng các frame được gửi đi trong tiến trình tìm kiếm.

☞ Trường Length : Xác định tổng độ dài của RIF (tính theo byte). Trường này có phạm vi từ 2 byte đến 30 byte.

☞ Trường bit D : Xác định và điều khiển hướng truyền của frame (truyền đi và truyền ngược lại). Trường bit D có tác dụng hoặc là các Bridge đọc số vòng, số bridge kết nối trong bộ phận chỉ đường từ phải qua trái (trong trường hợp gửi đi) hoặc là từ trái sang phải trong trường hợp truyền ngược lại.

☞ Trường quy định về fích thước cực đại của frame : Xác định kích thước cực đại của một frame mà bộ phận chỉ đường còn có thể kiểm soát được. Nơi gửi có thể đặt kích thước cực đại cho frame mà nó truyền đi, nhưng các Bridge có thể giảm kích thước này xuống nếu như nó không có khả năng truyền các frame có kích thước lớn như vậy.

Trường đánh dấu đường

Mỗi trường đánh dấu đường bao gồm hai trường nhỏ:

☞ Số vòng (12 bit) : Gán giá trị duy nhất trong từng mạng được kết nối .

☞ Số lượng bridge (4 bit): Gán giá trị theo số lượng vòng. Số này không phải là duy nhất trừ khi nó song song với Bridge khác mà Bridge này nối với hai mạng vòng.

Những đường đi đang xen kẽ liên tục các bridge và các vòng. Một trường thông tin về đường (RIF) có thể chứa nhiều hơn một trường đánh dấu đường. Chuẩn IEEE xác định số lượng cực đại của trường đánh dấu đường là 14 (có cựu đại 13 bridge hoặc hop bởi vì số bridge cuối cùng luôn bằng 0).

Ngày nay , IBM chỉ rõ số lượng cực đại của trường đánh dấu đường là 8 (7 bridge hoặc đoạn nối). Tất cả công nghệ Bridge đều theo cách thực hiện của IBM.

Mới đây những phần mềm kết nối của IBM kết hợp với các adapter của mạng LAN mới được hỗ trợ 13 hop.

3.3.4. Miêu tả một số chức năng cơ bản của việc nối giữa đường đi và nguồn

Để truyền được những gói dữ liệu giữa các mạng vòng thì nơi gửi phải biết được đường tới đích. Đầu tiên nơi gửi dùng "frame kiểm tra" để xác định xem đích cần đến có thuộc cùng một mạng nhỏ hay không. Nếu đích cần xác định đó thuộc cùng một mạng bridge không cần phải sử dụng. Trong trường hợp ngược lại(đích đó nằm ngoài mạng cục bộ), nơi gửi sẽ gửi ra mạng ngoài một frame có tên là "frame thăm dò", frame này sẽ được truyền tới tất cả các Bridge, các Bridge sẽ cộng thông tin về đường đi vào trong frame này và gửi chúng tới tất cả các cổng. Vì vậy đường đ tới đích sẽ được ghi nhận. Đích cần xác định sẽ gửi lại tất cả các frame mà nó thu được. Nơi gửi sau khi nhận được các frame trả lời sẽ chọn ra đường đi tới đích. Có một số tiêu chuẩn chính trong việc chọn đường đó là : thứ tự các frame đến, số lượng của các đoạn tới đích, MTU cực đại dọc theo đường đi hoặc là kết hợp các tiêu chuẩn trên. Trong Frame còn có một bit gọi là RII(Routing Information Indicator Chỉ báo thông tin về đường đi). Nó là bit quan trọng

nhất được đặt trong địa chỉ MAC của nguồn(nơi gửi) và nó được đặt bởi nơi gửi.

Chương IV Hoạt động của RSTB

Phần này mô tả hỗ trợ bridge là chuyển đổi SourceRoute-Transparent Bridge. Nó bao gồm các mục sau:

- Giới thiệu về SR-TB
- Cho phép SR-TB
- Chuyển đổi SR-TB hoạt động như thế nào
- SR-TB và Frame Relay

4.1. Giới thiệu về chuyển đổi SR-TB:

Chuyển đổi Source Route-Transparent Bridge (SR-TB) kết nối các mạng sử dụng source route bridge (hay mạng source route) và transparent bridge (hay mạng transparent bridge). Nó kết nối hai mạng một cách trong suốt. Các máy trạm trong cả hai mạng không nhận thấy sự tồn tại của bridge SR-TB. Bất cứ một máy trạm trong mạng kết hợp thì cũng xuất hiện trong chính mạng của nó.

Source routing có hiệu lực trong kiểuSRT, giữa source routing Token Ring gần kề. Các bridge chỉ source-route không thể cùng tồn tại với các bridge SRT là cái kết nối các mạng LAN Ethernet và Token Ring. Bởi vì một nút đầu cuối Token Ring cần truyền thông với một nút Ethernet thì nó phải được cấu hình để bỏ qua RIF. Nhưng nếu nút đầu cuối được cấu hình để bỏ qua RIF thì nó không thể truyền thông qua các bridge source routing bình thường vì các bridge này đòi hỏi RIF.

SR-TB thực hiện chức năng này bằng cách chuyển các frame từ mạng transparent bridging sang các frame source routing trước khi chuyển tiếp chúng tới mạng source routing. Bridge thực hiện điều này bằng cách duy trì một cơ sở dữ liệu địa chỉ của các máy trạm đầu cuối, mỗi cái với RIF tương ứng trong mạng source routing. Nó cũng điều khiển việc phát hiện đường đi thay mặt các máy trạm đầu cuối hiện diện trong mạng transparent bridging.

Nó sử dụng cơ chế phát hiện đường để tìm đường đến máy trạm đích trong mạng source routing. Nó gửi địa chỉ các frame tới vùng điểm đích chưa biết trong khuôn dạng STE (Spanning Tree Exporer).

SR-TB có thể điều khiển ba kiểu spanning tree sau:

- Spanning tree hình thành bởi một mạng transparent bridge
- Spanning tree hình thành bởi một mạng source routing bridge
- Một spanning tree đặc biệt của tất cả các bridge SR-TB

Mục tiếp theo thảo luận chi tiết hoạt động của SR-TB

4.2. Cho phép SR-TB.

Những thông tin sau phác thảo các bước khởi tạo yêu cầu để cho phép các lựa chọn SR-TB bridge được đưa ra bởi ASRT bridge:

- **Enable bridge**: Cho phép bridging trên tất cả các ghép nối LAN. Bạn cũng có thể bao gồm các ghép nối WAN (các đường nối tiếp) bằng cách sử dụng câu lệnh add port.
- **Disable transparent** *port #* Làm mất hiệu lực transparent bridging trên các ghép nối.
- **Enable source-routing** *port#segment#[bridge#]* Cho phép source routing đối với những cổng được đưa ra ở trên. Khi source routing là cho phép trên nhiều hơn hai cổng, một số hiệu phân đoạn thêm vào được yêu cầu để ấn định một phân đoạn ảo bên trong cần thiết cho cấu hình 1:N SRB
- **Enable sr-tb-conversion** *segment#.* Cho phép chuyển đổi các frame source-route sang các frame transparent và ngược lại. Bạn cũng phải ấn định một số hiệu phân đoạn mạng và kích cỡ MTU mạng để miêu tả hầu hết mạng transparent bridging (Ethernet/FDDI)

Sau khi hoàn thành các thủ tục được miêu tả ở trên, bạn có thể vào danh sách các bridge để hiển thị cấu hình của bridge hiện hành. Điều này cho phép bạn thẩm tra và kiểm soát cấu hình của mình.

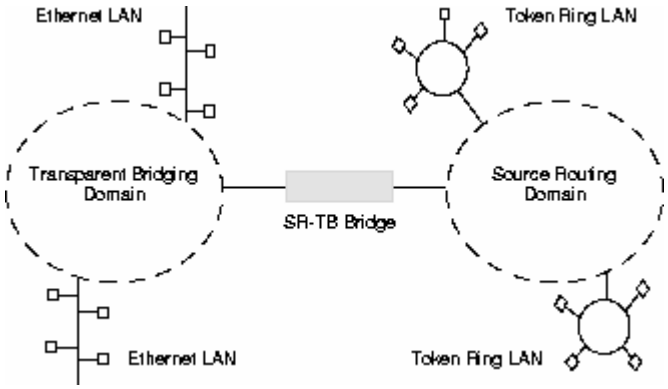
Nếu bạn muốn thay đổi cấu hình, xem thêm phần các câu lệnh bridge để biết chi tiết. Sau khi bạn đã kết thúc việc thay đổi cấu hình, khởi động lại router để cấu hình mới có thể có hiệu lực.

4.3. Chuyển đổi SR-TB hoạt động như thế nào.

Trong kết nối SR-TB, một mạng được phân vùng thành hai hoặc nhiều mạng riêng biệt. Mỗi mạng được tạo bởi một tập hợp các phân đoạn LAN kết nối bằng các bridge, tất cả hoạt động dưới cùng một phương thức kết nối chung. Điều này cho phép các mạng được tạo bởi hai kiểu mạng sau:

- Source routing
- Transparent bridging

Hình 14 chỉ ra một ví dụ của các mạng như vậy. Với các mạng riêng biệt, mỗi một source routing có một single-route broadcast topology tạo lập cho các bridge của nó. Chỉ các bridge thuộc source routing spanning tree đó là được chỉ định để chuyển tiếp các single-route broadcast frame. Trong trường hợp này, các frame mang các chỉ báo single-route broadcast được định hướng tới tất cả các phân đoạn của mạng source routing.



Hình 14: Bridge SR-TB kết nối hai mạng

4.4. Các hoạt động cụ thể của Source Routing và Transparent Bridging

SR-TB là một thiết bị hai cổng với giao diện MAC ấn định cho phân đoạn LAN bên phía source routing và một cái khác ấn định cho phân

đoạn LAN bên phía transparent bridging. Mỗi máy trạm đầu cuối đọc lớp MAC tương ứng với phân doạn LAN của nó.

Bên phía kết nối với transparent, SR-TB hoạt động tương tự như các transparent bridge khác. Nó giữ một bảng các địa chỉ của các máy trạm mà nó biết là các máy trạm transparent bridging. Nó tiến hành các giao thức liên kết bridge cần thiết để tạo lập và duy trì spanning tree mạng khi có nhiều hơn một SR-TB kết nối các mạng khác nhau.

SR-TB chuyển tiếp một frame nhận được từ máy trạm transparent bridging của nó tới bên source routing chỉ khi nó không tìm thấy địa chỉ đích của frame trong bảng địa chỉ bên phía transparent bridging.

Bên phía kết nối với source routing, SR-TB kết hợp các chức năng của một source routing bridge và một máy trạm đầu cuối source routing theo một cách cụ thể. Như là một máy trạm đầu cuối source routing, nó duy trì một sự kết hợp của các địa chỉ đích và thông tin định hướng. Nó cũng truyền thông như là một máy trạm đầu cuối với các ứng dụng trong bridge của bản thân nó (ví dụ như quản lý mạng) hoặc như là một vật trung gian giữa các máy trạm bên phía kết nối transparent.

SR-TB chuyển tiếp một frame nhận được từ máy trạm transparent bridging của nó tới bên source routing của bridge chỉ khi nó không tìm được địa chỉ đích của frame trong bảng địa chỉ ở bên phía kết nối transparent của nó. Các frame được truyền bằng cách kết hợp các máy trạm source routing mang thông tin định hướng của bridge với bridge, nếu những thông tin đó bridge biết và có chứa đựng.

Là một bridge source routing, SR-TB tham gia vào xử lý phát hiện đường đi và vào việc định hướng các frame đã mang thông tin định hướng. Đường đi được chọn lựa là độc nhất với SR-TB bao gồm số hiệu LAN của mạng LAN riêng trên phía source routing của nó và số hiệu bridge của riêng nó.

SR-TB cũng duy trì một số hiệu LAN đơn lẻ đại diện cho tất cả các mạng LAN trên phía kết nối transparent. Nó xử lý mỗi trường hợp nhận và chuyển tiếp các frame khác nhau được mô tả trong bảng sau:

Bảng quyết định của bridge SR-TB:

Kiểu frame nhận được	Hành động của SR-TB
Các frame không định hướng nhận được từ các máy trạm source routing	Không sao chép hoặc chuyển tiếp các frame mang thông tin định hướng
All-routes broadcast frame nhận được từ các máy trạm source routing	Sao chép các frame và thiết lập các bit A và C của chỉ báo broadcast trong frame được lặp. Nếu địa chỉ đích là nằm trong bảng kết nối transparent, chuyển tiếp các frame không có thông tin định hướng trên mạng kết nối transparent. Mặt khác, không chuyển tiếp frame.
Single-route broadcast frame nhận được từ các máy trạm source routing. Bridge được chỉ định là single-route broadcast bridge	Sao chép các frame và thiết lập các bit A và C của chỉ báo broadcast, loại bỏ các thông tin định hướng của frame, và chuyển tiếp các thông tin đã được sửa đổi tới phía kết nối transparent. Thêm vào số hiệu bridge của nó để lưu trữ trường thông tin định hướng và số hiệu LAN cho phía kết nối transparent. Thay đổi chỉ báo broadcast thành non-broadcast, bổ sung bit D, và lưu trữ thông tin định hướng này cho địa chỉ nguồn của frame.
Non-broadcast frame nhận được từ các máy trạm source routing.	Nếu frame mang đường đi cụ thể, bridge sẽ xem xét thông tin định hướng. Nếu SR-TB là một phần của đường đi và xuất hiện giữa số hiệu LAN

	cho phía source routing và số hiệu LAN cho phía transparent bridge thì sao chép frame và thiết lập bit A và C trong frame được lặp Chuyển tiếp frame tới phía kết nối transparent không có các thông tin định hướng. Nếu SR-TB chưa có một đường đi cố định cho địa chỉ nguồn, lưu trữ một bản sao chép của thông tin dẫn đường, bổ sung bit D và cất giữ thông tin định hướng đã được lưu trữ cho địa chỉ nguồn của frame.
Frame nhận được từ phía kết nối transparent	Để chuyển tiếp frame tới phía source routing, đầu tiên phải xác định xem nó có kết hợp thông tin định hướng với địa chỉ nguồn chứa đựng trong frame không . Nếu có, thêm thông tin định hướng vào frame, đặt RII thành 1, và xếp hàng các frame để truyền về phía source routing. Nếu không, thêm một trường điều khiển định hướng vào frame gồm có một chỉ báo cho single-route broadcast và hai đường đi định rõ trong đó bao gồm 'hai số hiệu' LAN và số hiệu bridge của riêng nó.

4.5. SR-TB Bridging -Các ví dụ

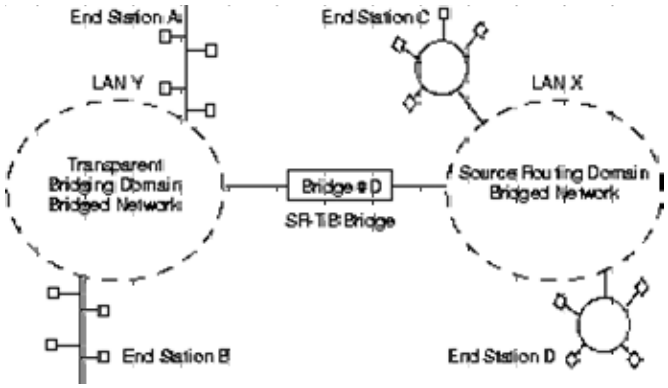
SR - TB kết nối các miền sử dụng source routing với các miền sử dụng transparent bridging bởi liên kết các miền với nhau một cách trong

suốt. Trong thời gian hoạt động, các trạm trong cả hai miền không ý thức được sự tồn tại của SR - TB. Từ điểm nhìn của máy trạm cuối, bất kỳ trạm nào trên mạng được kết hợp có vẻ trong miền của chính mình.

Những mục sau cung cấp những ví dụ đặc tả mô phỏng cách thức frame được truyền tiếp đi trong khi SR - TB " hoạt động". Hình vẽ cung cấp thông tin được liệt kê dưới đây để bổ trợ cho các tình huống được mô tả ở mỗi phần.

- D là số cầu của bridge
- X là số mạng LAN phía mạng LAN sử dụng source routing
- Y là số mạng LAN phía mạng LAN sử dụng transparent bridging
- A, B, C, Và D là những nhà ga kết thúc

Hình 14 SR - TB Bridging các ví dụ



Ví dụ 1 Frame chuyển từ trạm A tới trạm B

Khi SR - TB nhận một khung với địa chỉ nguồn là trạm cuối A và địa chỉ đích là trạm B, nó đặt địa chỉ của trạm cuối A vào trong bảng phía transparent bridging của nó. Bảng này chứa đựng địa chỉ của những trạm được biết là thuộc phía transparent bridging của bridge. Đây là hoạt động bình thường cho transparent bridging.

Nếu địa chỉ của trạm cuối B không có trong trong bảng địa chỉ phía transparent bridging và không tồn tại trong bảng địa chỉ phía source routing, SR - TB không biết sự định vị của trạm cuối. Trong trường hợp này, SR - TB truyền tiếp frame về phía source routing như một broadcast loại

source routing với yêu cầu không quay trở lại truyến đường đã đi qua. Bất kỳ frame nào của trạm cuối B gửi đi (không chủ ý tới nơi đến của nó) thì địa chỉ của nó sẽ được thêm vào bảng địa chỉ transparent bridging. Điều này ngăn ngừa các frame có địa chỉ là trạm cuối B trong tương lai được truyển tiếp về phía source routing.

Ví dụ 2: Frame gửi từ trạm cuối A tới trạm cuối C

Trong ví dụ này, địa chỉ của trạm cuối A được sử lý giống như trong ví dụ trước đây. Một khi địa chỉ của trạm cuối C không tồn tại trong bảng địa transparent bridge, SR - TB sẽ truyển tiếp frame về phía source routing.

Sau đó bridge tìm kiếm địa chỉ của trạm cuối C trong bảng địa source routingcủa nó. Bảng này chứa đựng tất cả các địa chỉ được biết và thông tin lộ trình liên quan cho những trạm về phía source routing của bridge. Nếu địa chỉ của C có trong bảng source routing, bridge sẽ truyển tiếp frame bằng cách sử dụng thông tin lộ trình trong bảng địa chỉ. Nếu địa chỉ của C không có trong bảng source routing (hoặc nếu nó xuất hiện nhưng có thông tin lộ trình vô giá trị), bridge sẽ truyển tiếp frame về phía phía source routing như một broadcast với yêu cầu không trả lại tuyên đường trở về.

Khi trạm cuối C nhận được frame này, nó nhập địa chỉ của trạm cuối A vào trong bảng source routing cùng với phương hướng ngược lại của tuyến đường xây dựng từ SR - TB bridge và dánh dấu nó là một mục vào tạm thời. Sau đó khi trạm cuối C cố gắng gửi một frame cho trạm cuối A, nó sử dụng tuyến đường đặc biệt này, và vì tuyến đường được đánh dấu tạm thời, nó gửi frame như một non-broadcast với yêu cầu tìm đường trở về.

Khi nào frame trả lời đến, SR - TB truyển tiếp nó về phía transparent bridge mà không có thông tin lộ trình nhưng đặt tuyến đường tới trạm cuối C vào trong bảng trọn đường nguồn như một tuyến đường tạm thời. Hơn nữa điều này khiến thực thể quản lý mạng (SMT) gửi một khung tìm đường với một thiết lập broadcast cho tất cả các tuyến đượng trở lại trạm

C. Điều này cho phép trạm cuối C chọn tuyến đượng tối ưu cho các frame có địa chỉ tới trạm cuối A, sau đó lộ trình này được đặt vào bảng trọn đường source như một tuyến đường lâu dài.

Ví dụ 3: Frame gửi từ trạm cuối C tới trạm cuối D

Nếu frame được gửi như những non-broadcast và vượt qua đoạn tới SR - TB bridge nào được gắn vào, bridge kiểm tra RII được sắp xếp theo trình tự chọn đường (mạng LAN X Tới Bridge Q tới mạng LAN Y). Nó không thể tìm thấy thứ tự và như vậy không truyển tiếp frame.

Nếu frame được gửi như một broadcast single-route, bridge vứt bỏ frame nếu nó đã biết rằng trạm cuối D ở phía source routing. Nếu nó không biết điều đó, nó truyển tiếp frame về phía transparent bridging (trừ thông tin lộ trình), và thêm thông tin lộ trình Q vào Y. Cuối cùng, nó lưu thông tin lộ trình cho trạm cuối C như một tuyến đường tạm thời trong bảng lộ trọn đường source routing với một chỉ báo non-broadcast và bit hướng được bổ sung.

Nếu frame được gửi như một all - routes broadcast , SR - TB loại bỏ frame (vì địa chỉ của trạm cuối D không có mặt trong bảng địa chỉ tramsparent bridging) và chắc chắn rằng địa chỉ của trạm cuối C có trong bảng source routing.

Ví dụ 4: Frame gửi từ trạm cuối C tới trạm cuối A

Nếu frame được gửi non-broadcast, SR - TB kiểm tra RII để sắp sếp thứ tự đường đi (X Tới Q tới Y). Khi nó tìm thấy đường đi, nó chuyển tiếp frame về phía transparent bridging. Nó cũng lưu lại thông tin chọn đường cho trạm cuối C.

Nếu khung được gửi như single- route broadcast, SR - TB chuyển tiếp nó (Số trừ Thông tin lộ trình) tới phía transparent bridging và thêm thông tin tuyến đường Q vào Y. Nó cũng thiết lập thông báo non-broadcast, bổ dung bit hướng, và thêm thông tuyến đường đối cho địa chỉ tram cuối C trong bảng tuyến đường của source routing của nó. Nếu lối vào

tạm thời cho trạm cối C đã tồn tại trong bảng tuyến đường source routing table, thì SR - TB sẽ cập nhật thông chọn đường.

Nếu frame được gửi như một all-routes broadcast, SR - TB sẽ loại bỏ frame này, nhưng chắc chắn rằng địa chỉ của trạm cuối C tồi tại trong bảng source routing.

4.6. Ứng dụng của SR-TB (Mixed-Media Bridging.)

4.6.1. Cơ sở

Bridge trong suốt (transparent bridges) được sử dụng chủ yếu trong mạng Ethernet còn source route bridge lại được sử dụng chủ yếu trong mạng TokenRing. Cả hai loại bridge này rất phổ biến, bởi vậy vấn đề đặt ra là có phương thức nào để kết nối trực tiếp các bridge này lại với nhau không. Có nhiều cách giải quyết cho vấn đề này.

Translational bridging: cung cấp một giải pháp rẻ tiền cho nhiều vấn đề trong đó có cả việc kết nối giữa các transparent bridge và source-route bridge. Phương pháp này xuất hiện lần đầu tiên vào cuối những năm 80 nhưng không được các tổ chức tiêu chuẩn ủng hộ. Do đó, nhiều vấn đề của nó vẫn tồn tại đối với người thực hiện nó.

Những năm 90, IBM giải quyết được một số yếu kém của tranlational bridging và giới thiệu phương thức kết hợp chúng (source - route transparent bridging - SRT). SRT có thể chuyển tiếp dữ liệu cho cả các net sử dụng transparent bridge va source route bridge và tạo ra spanning tree cho cả transparent bridge, bởi vậy cho phép các trạm của từng loại có thể giao tiếp với các trạm cùng loại trong các mạng có cấu trúc bất kỳ. SRT được định nghĩa trong phụ lục C của chuẩn IEE 802.1d.

Cuối cùng mục đích của kết nối các transparent bridge va SRB là cho phép các nút mạng của hai loại mạng trên giao tiếp với nhau.

4.6.2. Các vấn đề nảy sinh.

Có nhiều vấn đề cần giải quyết khi các nút mạng của Ethernet/transparent bridge giao tiếp với các nút mạng TokenRing/SRB. Sau đây là các vấn đề chủ yếu:

Thứ tự bit không thống nhất: Mặc dù cả Ethernet va TokenRing đều cung cấp địa chỉ MAC 48 bit, nhưng cách biểu diễn bên trong của các địa chỉ này không giống nhau. Trong dòng tuần tự các bit được truyền đi, TokenRing coi bit đầu tiên nhận được là bit cao nhất của byte trong khi đó Ethernet lại coi đó là bit thấp nhất của byte.

Các địa chỉ MAc bị nhúng vào dữ liệu: Trong một số trường hợp, địa chỉ MAC lại được chuyển trong phần dữ liệu của gói tin. Giáo thức phân giải địa chỉ (address Resolution Protocol - ARP) rất thông dụng trong mạng TCP/IP là một ví dụ, nó đặt địa chỉ MAC trong phần dữ liệu của gói dữ liệu tầng liên kết dữ liệu (Data - link). Chuyển đổi các địa chỉ xuất hiện trong phần dữ liệu của gói như vậy là rất khó khăn bởi vì nó phải dùng vào từng trường hợp cụ thể.

Kích thước cực đại của các khối dữ liệu không giống nhau: Kích thước gói dữ liệu cực đại của Ethernet là vào khoảng 1500 byte trong khi đó TokenRing có kích thước gói dữ liệu cực đại lớn hơn nhiều. Bởi vì các bridge không có khả năng phân nhỏ hay kết hợp các gói dữ liệu có kích thước lớn hơn kích thước tối đa của mạng đó sẽ bị huỷ bỏ.

Xử lý các bit trạng thái: TokenRing có 3 bit trạng thái của gói: A, C va E. Mục đích của các bit này là xác định nơi nhận đã nhận được gói này chưa (bit A), đã copy gói này chưa (C) và gói có bị lỗi không (bit E). Ethernet không có các bit nào cho nên vấn đề đặt ra là giải quyết các bit này như thế nào. Điều đó là vấn đề của người sản xuất Ethernet - TokenRing bridge.

Xử lý các chức năng chỉ có trong TokenRing: Một số bit trong gói của TokenRing không có các bit tương ứng trong Ethernet. Ví dụ: trong Ethernet không có cơ chế ưu tiên trong khi TokenRing thì có. Một số bit trong gói dữ liệu của TokenRing phải bỏ đi khi chuyển sang gói tin Ethernet như token bit, monitor bit và các bit dự trữ.

Xử lý các gói tin thăm dò: Các transparent bridge không biết sẽ phải làm gì đối với các gói tin thăm dò của SRB. Transparent bridge nhận biết cấu trúc mạng qua việc phân tích các gói tin nhận được. Chúng không biết các quá trình tìm đường của SRB.

Xử lý hướng thông tin dẫn đường(Routing Information Field - RIF) trong gói tin TokenRing. SRB đặt các thông tin dẫn đường trong trường RIF. Các transparent bridge không có các trường tương tự, và các thông tin này là khác lạ đối với transparent bridge.

Các thuật toán STP không giống nhau: Transparent bridging và SRB đều sử dụng các thuật toán cây bao trùm tuy nhiên các thuật toán được áp dụng lại khác nhau.

Xử lý các gói thông tin không có thông tin dẫn đường: SRB yêu cầu các gói tin trong mạng đều chứa thông tin dẫn đường. Khi một gói tin không có trường RIF (bao gồm các gói tin báo thay đổi cấu trúc topo mạng và cấu hình của transparent bridge cũng như các gói tin địa chỉ MAC gửi từ mạng transparent bridging) tới một SRB bridge đều bị bỏ qua.

4.6.3. Translational bridging

Bởi vì không có sự chuẩn hoá nào trong việc giao tiếp giữa hai phương thức truyền khác nhau, không có sự cài đặt cửa translation bridging nào được gọi là đúng đắn. Sau đây là một số phương pháp thông dụng đã được sử dụng:

Các bridge dịch sắp xếp lại các bit của địa chỉ nguồn và đích khi dịch một gói tin dạng Ethernet sang TokenRing và ngược lại. Vấn đề các địa chỉ MAC bị nhúng trong dữ liệu được giải quyết bằng cách lập trình cho bridge kiểm tra các loại địa chỉ khác nhau nhưng giải pháp này phải thích nghi với các địa chỉ MAC mới. Một số giải pháp của translational bridging chỉ kiểm tra một số địa chỉ nhúng thông dụng nhất. Nếu các phần mềm thực hiện các translational bridging chạy trên một router nhiều giao thức, thì router sẽ dẫn đường cho các giao thức này và giải quyết toàn bộ vấn đề.

Trường TRF có một trường con chỉ ra rằng kích thước lớn nhất có thể chấp nhận của SRB. Bridge dịch khi đó sẽ gửi các gói từ transparent bridge to SRB đặt kích thước gói tin cực đại là kích thước cực đại của Ethernet. Một số trạm không thể xử lý được trường này và trong trường hợp để gói tin bị huỷ bỏ bởi Translational bridging.

Các bit thể hiện các chức năng TokenRing ma không có trong Ethernet sẽ bị vứt bỏ bởi bridge. Ví dụ các bit thể hiện ưu tiên, dự trữ và giám sát (trong byte điều khiển truy nhập (access –control byte) bị loại bỏ. Các bit thể hiện trạng thái của TokenRing có nhiều cách xử lý khác nhau tuỳ vào các nhà sản xuất. Một số bridge loại bỏ các bit này, một số khác sẽ thiết lập bit C (để thể hiện frame đã được copy) nhưng không thiết lập bit A (để thể hiện nơi nhận ra địa chỉ này). Trong trường hợp trước, nút TokenRing gửi xác định được gói dữ liệu nó gửi đi có bị mất hay không, Cách làm này thể hiện cơ chế tin cậy và có thể có thêm cơ chế theo dõi các gói tin bị mất mà các cơ chế này tốt hơn là cài đặt ở tầng 4 của mô hình CSI. Cách tiếp cận thứ hai thể hiện thiết lập bit C để theo dõi các gói tin nhưng không thiết lập bit A vi bridge không phải là đích cuối cùng.

Translational bridging có thể tạo ra một gateway mềm giữa hai mạng. Đối với SRB, Translational bridging có một chỉ số vòng và số bridge cho riêng nó và nó giống như một SRB bình thường. Chỉ số vòng trong trường hợp này thể hiện toàn bộ mạng transparent bridging. Đối với mạng transparent - bridging lại là một transparent bridge.

Khi chuyển từ mạng SRB sang mạng transparent bridging, các thông tin SRB bị loại bỏ RIF thường lưu lại để sử dụng cho việc gửi lại sau đó. Khi truyền ngược lại, từ transparent - bridging sang SRB, bridge dịch kiểm tra xem gói đó là gửi cho một nút xác định hay multicast. Nếu là multicast hay broadcast nó gửi gói đó như là một gói tin thăm dò spanning tree. Nếu nó có

địa chỉ duy nhất bridge dịch tìm địa chỉ này trong bảng lưu thông tin dẫn đường. Nếu có nó địa chỉ đó được thêm vào gói tin, nếu ngược lại nó được gửi như là gói tin thăm dò spanning tree. Bởi vì hai cây bao trùm không giống nhau, nhiều đường đi giữa mạng SRB va transparent bridging thường là không thể được.

Khi chuyển giữa IEE 803.3 và TokenRing, địa chỉ đích và nguồn (DASA), điểm truy ccập dịch vụ (service - access point SAP), điều khiển kết nối logic (Logical - Link Control - LLC) được chuyển sang các trường tương ứng của gói kết quả. Thứ tự bit của SA và DA được sắp xếp lại. Khi chuyển từ IEE 802.3 sang TokenRing, trường độ dài của gói tin IEE 802.3 bị bỏ đi. Byte điều khiển truy nhập vá RIF bị loại bỏ. RIF có thể lưu ở bridge cho các sử dụng sau này.

Khi chuyển đỏi từ Ethernet sang TokenRing, địa chỉ đích, nguồn, kiểu và dữ liệu được chuyển sang các trường tương ứng của gói tin đích và DASA được sắp xếp lại RIF, SAP, LLC và mã người bán bị loại bỏ khi chuyển từ TokenRing sang Ethernet. Khi chuyển từ Ethernet sang TokenRing không có thông tin nào bị laọi bỏ.

4.6.4. Source - Route Transparent Bridging.

SRT kết hợp các thuật toán của transparent briding và SRB. SRT sử dụng bit chỉ định thông tin dẫn đường (routing information indicator - RII) để phân biệt gói tin sử dụng SRB và gói tin transparent bridging. Nếu bit RII là 1, RIF sẽ có mặt trong gói tin và bridge sử dụng SRB. Nếu RII là 0, RII không có mặt, và bridge sử dụng transparent bridging.

Với một bridge dịch, SRT bridge không phải là giải pháp hoàn hảo cho việc kết nối các mạng tính chất khác nhau. SRT bridge vẫn phải xử lý các vấn đề không tương thích giữa mạng Ethernet/TokenRing đã nêu ra ở trên. SRT yêu cầu các nâng cấp phần cứng của SRB để cho phếp chúng xử lý các gói tin phức tạp hơn. Ngoài ra cần phải có các nâng cấp về phần mềm, hơn nữa trong môi trường có SRT bridge, transparent bridge, và SRB, source route việc lựa chọn giữa SRT và SRB là có thể. Các đường đi được chọn có khả năng không tốt như là đối với môi trường chỉ có transparent bridge. Cuối cùng, mạng vừa có SRB và SRT bridging làm mất đi các tính năng của SRT, do đó người sử dụng không muốn chuyển sang SRT khi chúng còn đắt. SRT bridging chỉ sử dụng để kết nối hai mạng có kiến trúc khác nhau, giữa SRD và transparent bridging.

Chương V Spanning Tree Protocol (STP)

5.1. Hoạt động của giao thức Spanning Tree.

Giao thức này áp dụng cho cả Switch và Bridge, bây giờ ta đi xem xét các hoạt động của giao thức Spanning Tree:

Khi các thiết bị Switch/Bridge tham gia vào mạng nó sẽ sử dụng một gói dữ liệu BPDU (Bridge Protocol Data Unit) để trao đổi thông tin với nhau nhằm:

Xác định Switch/Bridge nào được coi là gốc (Root Switch/Bridge)

Trên các Switch/Bridge không phải là gốc (NonRoot Switch/Bridge) nó phải xác định ra Root Port – đây là cổng mà nó sẽ kết nối đến

Root Switch/Bridge theo đường ngắn nhất, trong một Bridge/S chỉ có một Root Port

Xác định trạng thái của các cổng là Forward hay Block:

√ Forward là trạng thái truyền nhận dữ liệu bình thường

Block là trạng thái không truyền nhận dữ liệu

Trong một gói dữ liệu của Bridge/Switch sử dụng BPDU mang các thông tin sau:

Root Bridge's ID: là MAC address của Bridge/Switch đó, MAC address là duy nhất nên Root Bridge's ID là duy nhất.

Bridge ID được sử dụng đểv xác định Root Bridge trong mạng và xác định Root Port. Bridge ID dài 8 bytes bao gồm priority và MAC address của Bridge/Switch.

Priority: đây là mưc ưu tiên của thiết bị Bridge/Switch, thường ban đầu priority của Bridge/Switch như nhau (coi =1), khi cần thiết sẽ thay đổi, MAC address hầu như không thay đổi được.

Priority trên tất cả các Bridge/Switch dùng phiên bản IEEE STP mặc định là 32768.

Cost

Send Bridge's ID: số hiệu của Bridge gửi trên gói BPDU, mục đích của chỉ số này là để cho nút nhận khi nhận được BPDU nó sẽ xác định được là BPDU được gửi từ đâu.

Mỗi cổng trên Bridge/Switch được gán cho một giá nhất định, tuỳ thuộc vào tốc độ của cổng

Ví dụ:

Port Speed	Cost
100Mbps	100
100Mbps	19
1Gbps	4
10Gbps	2

5.1.1. Quá trình lựa chọn Root Bridge

Các switch và bridge có sử dụng giao thức STP trao đổi thông tin với nhau bằng các gói **dữ liệu giao thức bridge** (Bridge Protocol Data Units - BPDU). Các BPDU được sử dụng để gửi các thông tin cấu hình tới tất cả các bridge khác. Định danh của từng thiết bị bridge được gửi tới các bridge khác qua các BPDU.

Định danh bridge được sử dụng để xác định bridge gốc của mạng và các cổng gốc. Định danh của bridge dài 8 byte bao gồm mức ưu tiên và địa chỉ MAC của thiết bị đó. Mức ưu tiên mặc định của các thiết bị theo chuẩn IEEE STP là 32768.

- Khi Bridge/Switch tham gia vào mạng bao giờ nó cũng tự coi nó là Root Bridge, đồng thời nó tạo ra BPDU trong đó Root Bridge's ID trỏ đến Mac Address của nó, sau quá trình này nó gửi BPDU đến tất cả các cổng khác của nó, Cost của BPDU ban đầu bằng 0
- Trong quá trình lựa chọn nếu Bridge/Switch nhận được một BPDU mô tả về một ứng cử viên khác tốt hơn (mục đích là chọn lại Root Bridge vì ban đầu Bridge/Switch tự coi Root Bridge là chính nó) dựa vào 2 yếu tố:
  1. Priority: Bridge/Switch nào có priority thấp hơn thì tốt hơn
  2. ID : Ban đầu Priority của tất cả Bridge/Switch là bằng nhau, khi nhận được Bridge/Switch nào có ID bé nhất thì tốt nhất.

Nếu Bridge/Switch có cùng giá trị priority, thì MAC address dùng để xác định cái nào co chỉ số ID thấp nhất .

Ví dụ, nếu 2 Bridge/Switch A, B cả hai cùng sử dụng priority mặc định là 32768. Nếu MAC address của Bridge/Switch A là 0000.0C00.1111.1111 và Nếu MAC address của Bridge/Switch B là 0000.0C00.2222.2222 và thì Bridge/Switch A sẽ được chọn là Root Bridge.

Các BPDU được gửi đi một lần trong 2 giây. Điều này gây nên một tổn phí khá lớn nhưng ta phải chú ý rằng gói tin này chỉ có đến layer 2 không có các thông tin của layer 3. Sau đây là một ví dụ của một gói tin BPDU:

Flag: 0x80 802.3
Status: 0x00
Packet length: 64
802.3 header
Destination: 01:80:c2:00:00:00
Source: 00:b0:64:75:6b:c3
LLC length: 38
802.2 Logical Link Control (LLC) header
Dest. SAP: 0x42 802.1 Bridge Spanning Tree
Source SAP: 0x42 802.1 Bridge Spanning Tree
Command: 0x03 Unnumbered information
802.1 - Bridge Spanning Tree
Protocol Identifier: 0
Protocol Version ID: 0
Message Type: 0 Configuration Message
Flag: %00000000
Root Priority/ID: 0x8000 / 00:b0:64:75:6b:c0
Cost of Path to root: 0x00000000 (0)
Bridge Priority/ID 0x80 / 00:b0:64:75:6b:c0
Port Priority/ID 0x80 / 0x03
Message Age: 0/256 seconds (0 giây)
Maximum Age: 5120/256 (20 giây)
Hello time: 512/256 (2 giây)

Forward Delay; 3840/256 (15 giây)
Extra bytes (thêm vào cho đủ): 00 00 00 00 00 00 00 00
Frame Check Sequence: 0x2e006400

Xem xét giá của đường đi từ bridge này đến gốc: trong trường hợp này là bằng không bởi vì bridge này tự xem nó là nút gốc. Trong Frame trên ta thấy có chỉ ra các thời gian của BPDU, các khoảng thời gian này được sử dụng để ngăn ngừa sự lặp các gói tin. Bởi vì các gói tin này chỉ có thể tồn tại trong một khoảng thời gian nhất định. Các BPDU rất dễ bị trễ do chiều dài của gói thông tin, các quá trình xử lý của switch, băng thông và các vấn đề tối ưu. Điều này có thể dẫn đến một mạng không tin cậy bởi vì có thể đưa đến việc các gói tin bị quẩn khi các gói tin BPDU không đến đúng lúc. STP sử dụng đồng hồ để bắt các cổng phải chờ các thông tin cấu hình đúng.

Trong gói tin được phân tích ở trên, thời gian Hello là 2 giây, thời gian bắt đầu xây dựng lại cây là 20 giây, và thời gian trễ là 15 giây.

Khi nhận được ứng cử viên tốt hơn nó sẽ dừng ngay việc loan truyền các thông tin về Root Bridge hiện thời mà nó chuyển sang loan truyền thông tin về Root Bridge mới . Kết quả của quá trình này là ta chọn được Bridge/Switch có ID và priority bé nhất.

5.1.2. Lựa chọn Root Port

Sau khi đã chọn được Bridge gốc, tất cả các các switch phải trở thành các cành của nút gốc. Mỗi switch nhận các BPDU trên các cổng hoạt động, và nếu có nhiều hơn một BPDU nhận được thì nó nhận ra rằng nó đang có các kết nối dư thừa nối đến gốc. Switch phải chọn ra một cổng làm cổng gốc và cho các cổng khác vào trạng thái block.

Để chọn ra cổng gốc, ta sử dụng các thông tin về tổn phí tới gốc. Tổn phí của STP được tính là tổng các tổn phí dựa trên băng thông của các kết nối mà bridge sử dụng để kết nối tới gốc.

Bảng sau đây các tổn phí đối với các mạng Ethernet khác nhau:

Tốc độ	IEEE mới	IEEE ban

		đầu
10Gbps	2	1
1Gbps	4	1
100Mbps	19	10
10Mbps	100	100

Khi các tổn phí của các kết nối đến gốc đã được xác định, switch sẽ xác định cổng nào có chi phí thấp nhất. Cổng đó được chọn làm cổng gốc còn các cổng khác chuyển sang chế độ Block. Nếu có các cổng có cùng chi phí thì cổng có số hiệu cổng thấp nhất được chọn làm cổng gốc.

Ban đầu Bridge/Switch coi cổng nào gửi cho nó BPDU đầu tiên là Root Port. Khi nhận được BPDU tiếp mô tả về Root Bridge nó sẽ làm như sau:

Lấy cost hiện thời cộng với cost của cổng mà nó nhận được BPDU:

New Cost = Cost + Cost (Port)

Sau đó Bridge/Switch xem giá trị New Cost có bé hơn giá trị Cost mà nó đang sử dụng để nối đến Root Bridge không?

+ Nếu nhỏ hơn nó coi cổng mà nó nhận được BPDU là Root Port

+ Nếu không nhỏ hơn nó không xem xét nữa

Tính xong New Cost Bridge/Switch phải gửi BPDU đến tất cả các cổng khác không phải là Root Port .

Tóm lại Root Port phụ thuộc vào Cost của các cổng

5.1.3. Các trạng thái của cổng

Một cổng của switch hoặc bridge sử dụng STP chuyển đổi giữa 4 trạng thái sau:

♣ *Blocking:* Không chuyển các gói dữ liệu, nhận các BPDU. Tất cả các cổng sẽ mặc định là ở trạng thái block khi switch được bật lên.

♣ *Listening:* Nhận các BPDU để đảm bảo không có các vòng lặp trên mạng trước khi chuyển các gói tin.

♣ *Learning:* Nhận các địa chỉ MAC và xây dựng các bảng lọc nhưng không chuyển tiếp các Frame.

♣ *Forwarding:* Cổng có thể gửi và nhận dữ liệu. Một cổng không bao giờ được đặt vào trạng thái này trừ khi không có các kết nối thừa hoặc cổng đó xác nhận được là nó có con đường đi tới gốc.

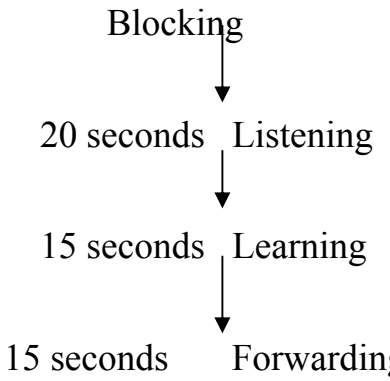
Một người quản trị hệ thống có thể đặt cổng về trạng thái không sẵn sàng, hoặc nếu cổng xảy ra lỗi, thì switch cũng có thể chuyển cổng về trạng thái không sẵn sàng.

Nói chung, các cổng của switch ở một trong hai trạng thái là blocking hoặc forwarding. Một cổng forwarding là một cổng được xác định là có giá trị (cost) nhỏ nhất đối với bridge gốc. Tuy nhiên, nếu kiến trúc mạng thay đổi do các liên kết sai, hoặc người quản trị thêm một switch mới vào mạng, các cổng trên một chuyển mạch sẽ ở trạng thái lắng nghe và cập nhật.

Các cổng blocking được sử dụng để ngăn việc lặp vòng. Khi một switch xác định được đường đi tốt nhất đến bridge gốc, tất cả các cổng khác sẽ được đặt ở trạng thái blocking. Các cổng bị blocking sẽ vẫn nhận được các gói BPDU (Bridge Protocol Data Unit).

Nếu một switch xác định rằng một cổng bị block bây giờ nên chuyển thành cổng được chỉ định, nó sẽ trở lại trạng thái listen. Nó sẽ kiểm tra tất cả các gói BPDU nhận được để chắc chắn rằng sẽ không tạo ra một vòng lặp khi cổng đó chuyển sang trạng thái forwarding.

Hình 4.5 chỉ ra thời gian ngầm định trong STP và các hành động trong STP:



Total = 50 seconds

Chú ý thời gian từ blocking đến forwarding. Blocking đến listening là 20 giây. Listening đến learning là 15 giây. Learning đến forwarding là 15 giây và tổng cộng là 50 giây. Tuy nhiên, switch có thể chuyển thành không sẵn sàng nếu cổng ngừng hoạt động hoặc cổng bị lỗi.

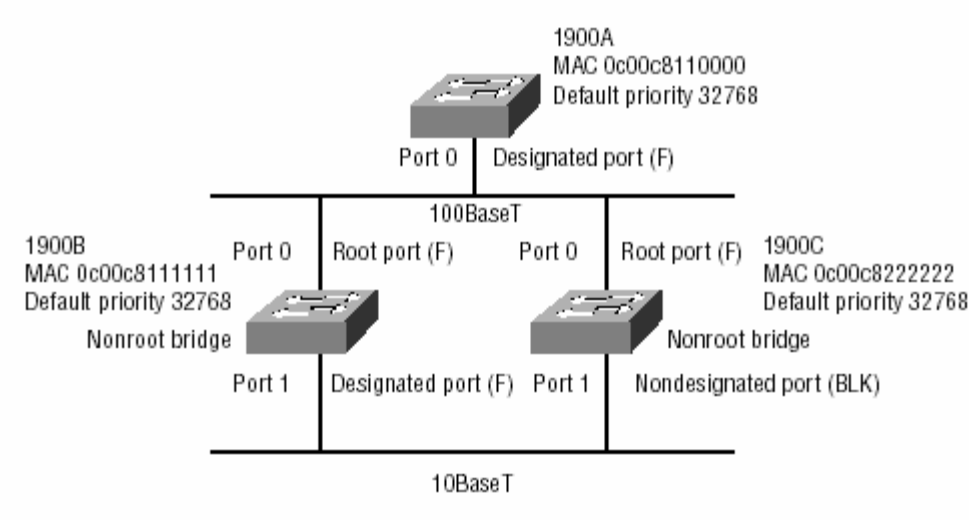
5.1.4. Sự hội tụ.

Sự hội tụ xảy ra khi các bridge và các switch chuyển tiếp tới trạng thái blocking hoặc forwarding. Không có dữ liệu được chuyển tiếp trong suốt thời gian này. Sự hội tụ là rất quan trọng trong việc chắc chắn rằng tất cả các thiết bị có cùng cơ sở dữ liệu.

Vấn đề của sự hội tụ đó là khoảng thời gian được sử dụng cho tất cả các thiết bị để có thể cập nhật. Trước khi dữ liệu bắt đầu được chuyển tiếp, tất cả các thiết bị phải được cập nhật. Thời gian thường được sử dụng để chuyển từ trạng thái blocking sang trạng thái forwarding là 50 giây. Thay đổi thời gian ngầm định STP là không được khuyên dùng, nhưng thời gian cũng có thể được điều chỉnh nếu điều đó cần thiết. Thời gian cần để chuyển một cổng từ trạng thái listening tới trạng thái learning hoặc từ trạng thái learning tới trạng thái forwarding được gọi là trễ chuyển tiếp.

5.2. Ví dụ cây spanning

Trong hình 4.6, ba switch có cùng mức độ ưu tiên là 32768. Tuy nhiên, cần chú ý tới địa chỉ MAC của mỗi switch. Bằng cách xem xét độ ưu tiên và địa chỉ MAC của mỗi một switch, chúng ta có thể xác định được bridge gốc.



Bởi vì 1900A có địa chỉ MAC thấp nhất và cả ba switch có cùng độ ưu tiên ngầm định nên 1900A sẽ là bridge gốc.

Để xác định cổng gốc (root port) trên 1900B và 1900C, chúng ta cần xem xét cost của các đường kết nối các switch này đến bridge gốc, từ đó chọn ra root port là cổng mà qua đó bridge hiện thời sẽ kết nối đến bridge gốc theo một con đường có cost là bé nhất. Vì đường kết nối từ cả hai switch này đến switch gốc là từ cổng 0 và sử dụng đường kết nối 100Mbps, đây là đường có cost là tốt nhất và vì vậy cổng gốc trên cả hai switch đều là cổng 0.

Sử dụng bridgeID để xác định các cổng được chỉ định trên các swich. Bridge gốc luôn luôn có tất cả các cổng là được chỉ định. Tuy nhiên, 1900B và 1900C có cùng một cost để đến được bridge gốc, cổng được chỉ định sẽ là trên switch 1900B bởi vì nó có bridgeID là nhỏ hơn. Bởi vì 1900B đã được xác định là có cổng được chỉ định, switch 1900C sẽ đặt cổng 1 của nó ở trạng thái blocking để ngăn chặn bất cứ một vòng lặp mạng nào có thể xảy ra.

Các phương thức của switch ở mạng LAN:

Các LAN switch được sử dụng để forward hoặc lọc các frame dựa trên phần cứng của chúng. Tuy nhiên, có ba phương thức khác nhau để chuyển tiếp hoặc lọc các frame. Mỗi phương thức có những ưu điểm và nhược điểm và vì vậy hiểu rõ sự khác nhau của các phương thức của LAN switch sẽ giúp chúng ta có những quyết định sáng suốt khi lựa chọn phương thức phù hợp.

Switch có ba phương thức sau:

Lưu trữ và chuyển tiếp (Store-and-Forward): Với chế độ lưu trữ và chuyển tiếp, switch sẽ nhận toàn bộ frame dữ liệu vào trong buffer, kiểm tra CRC (cyclic redundance check) được thực hiện, sau đó địa chỉ đích mới được tìm kiếm trong bảng MAC.

Cut-through: Với chế độ cut-through, switch sẽ đợi cho đến khi nhận được địa chỉ đích và sau đó tìm kiếm ngay trong bảng MAC.

FragmentFree: FragmentFree là chế độ ngầm định đối với switch Catalyst 1900, đôi khi nó được xem như là chế độ cut-through được sửa đổi. Nó kiểm tra 64 byte đầu tiên của frame (bởi vì có thể xảy ra xung đột) trước khi chuyển tiếp frame.

Store-and-forward

Phương thức store-and-forward là một trong ba kiểu chính của các chuyển mạch mạng LAN. Với phương thức hoạt động này, switch nhận toàn bộ gói tin và lưu vào buffer của nó và thực hiện kiểm tra CRC. Bởi vì nó phải nhận toàn bộ gói tin thì mới chuyển tiếp do đó thời gian trễ lớn và biến đổi theo độ dài của gói tin.

Gói tin sẽ bị loại bỏ nếu nó bị lỗi CRC, có kích thước quá nhỏ (nhỏ hơn 64 byte) hay quá lớn (lớn hơn 1518 byte kể cả CRC). Khi gói tin không bị lỗi thì switch sẽ xem xem địa chỉ MAC của đích trong bảng thông tin dẫn đường để chuyển tiếp gói tin đến cổng cần thiết.

Cut-through (Real Time)

Theo phương thức này, switch chỉ copy phần địa chỉ đích (6 byte tiếp theo phần preamble) vào buffer của nó. Tiếp đó nó xem địa chỉ này có trong bảng thông tin dẫn đường để chuyển tiếp gói tin tới các cổng cần thiết. Phương thức này làm giảm thời gian trễ trên các switch bởi vì nó chuyển tiếp gói tin đi ngay khi nó nhận được địa chỉ và xác định được cổng để chuyển gói tin đến.

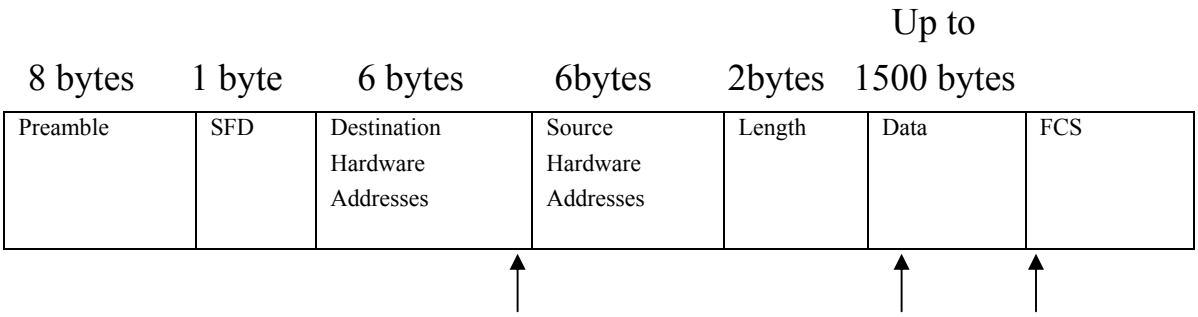
Một số switch có thể thiết lập để thực hiện chuyển gói tin theo phương thức cut-through cho các cổng khi xác suất lỗi không vượt quá đến một ngưỡng do người dùng định ra. Khi vượt quá xác suất lỗi đó các cổng đó được tự động chuyển về phương thức store-and-forward để không truyền các gói tin bị lỗi.

FragmentFree(Modified cut-through)

Đây là phương thức được cải tiến từ phương thức cut-through. Trong phương thức này switch sẽ chờ để nhận xong cửa sổ xung đột (collision window) dài 64 byte rồi mới chuyển tiếp gói tin. Cơ sở để áp dụng cách tiếp cận này là nếu một gói tin bị lỗi thì nó thường xảy ra trong 64 byte đầu tiên. FragmentFree cung cấp cách kiểm tra lỗi tốt hơn so với phương thức cut-through và cũng không gây ra trễ lớn như là store-and-forward.

Hình 4.7 minh họa những điểm khác nhau tại đó các chế độ switch xảy ra trong một frame. Các chế độ khác nhau sẽ được thảo luận chi tiết trong các mục sau.

Hình 4.7: Các chế độ switch khác nhau trong một frame


Up to
8 bytes
1 byte
6 bytes
6bytes
2bytes
1500 bytes
Preamble
SFD
Destination Hardware Addresses
Source Hardware Addresses
Length
Data
FCS
Cut-through: the error checking
FragmentFree: check for collision
Store-and--forward

THIẾT BỊ MẠNG

Biên soạn:
ThS. Tô Nguyễn Nhật Quang

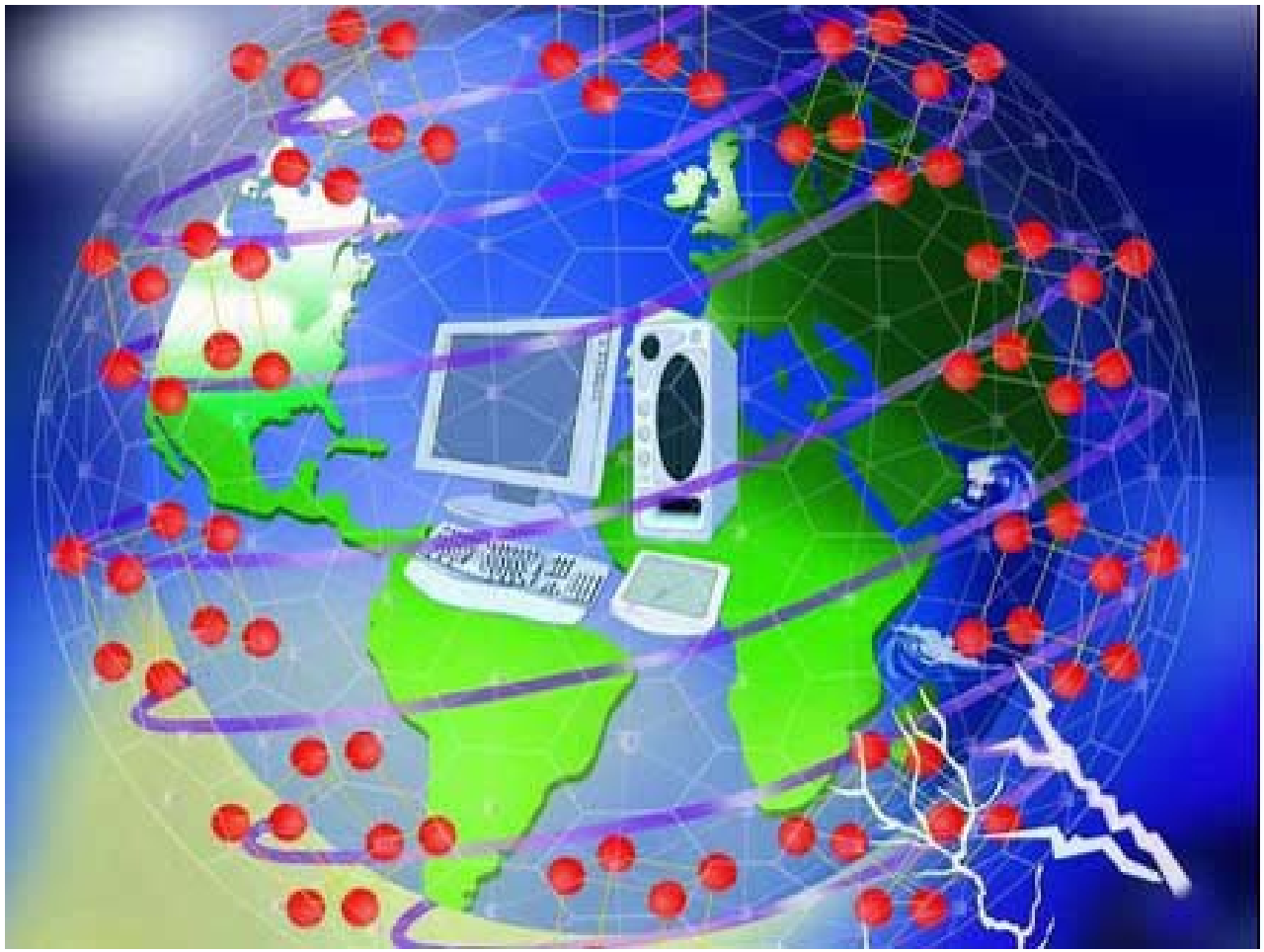
NỘI DUNG MÔN HỌC

Chương 1: Cơ bản về Networking (S3 – S35)
Chương 2: Môi trường và thiết bị truyền dẫn (S36 – S59)
Chương 3: Thiết bị liên kết mạng (S60 – S93)
Chương 4: Router (S94 – S172)
Chương 5: Switch (S173 – S316)
Chương 6: Các giao thức định tuyến (S317 – S380)
Chương 7: Access Control List - ACL (S381 – S420)
Chương 8: Network Access Translation (S421 – S442)
Chương 9: Các công nghệ WAN (S443 – S460)

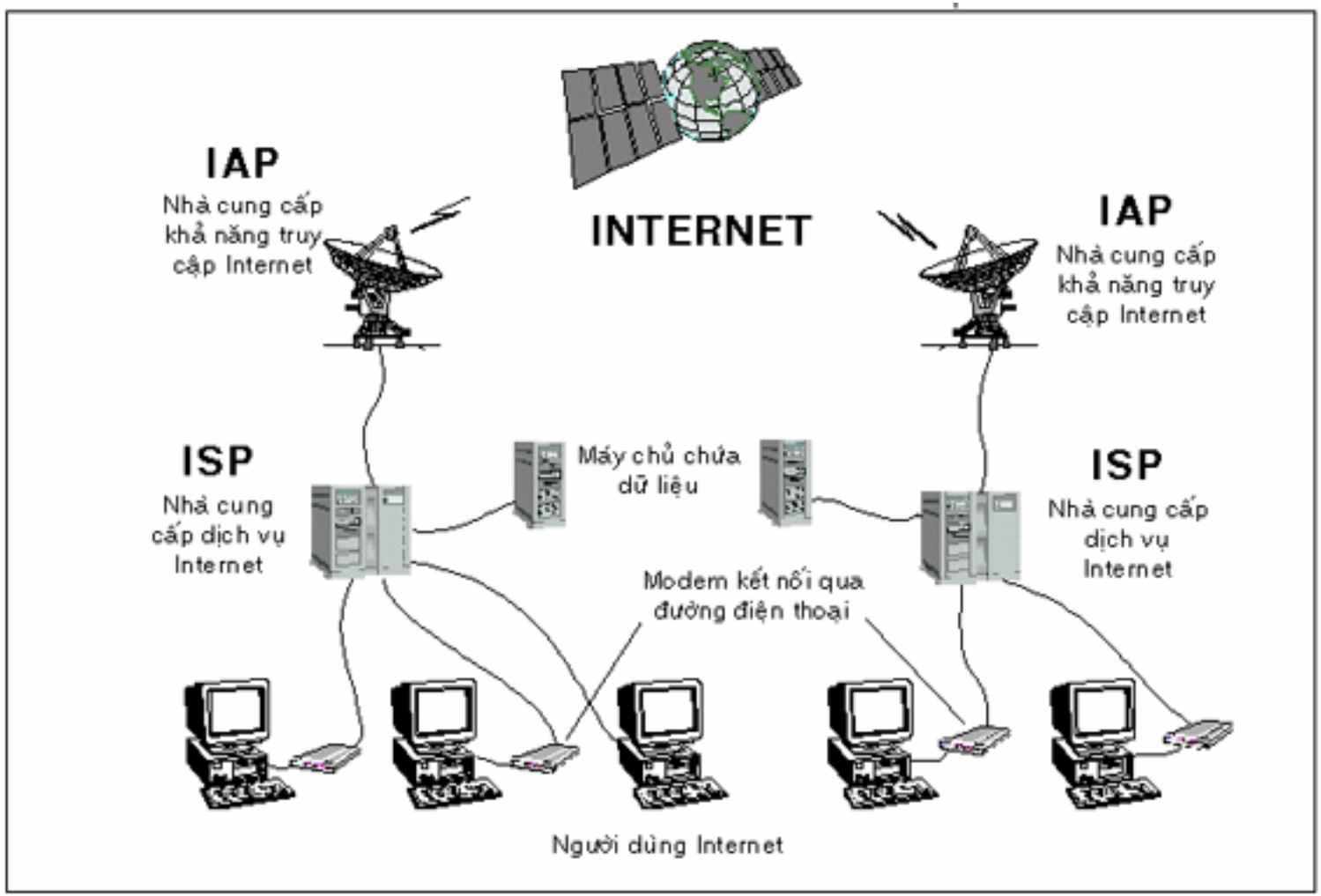
CƠ BẢN VỀ NETWORKING

- Nhu cầu kết nối Internet
- Các ký hiệu (icons) thường dùng
- Lược đồ mạng
- Phân loại mạng
- Mô hình OSI và TCP/IP
- Các hệ thống số
- Địa chỉ IP

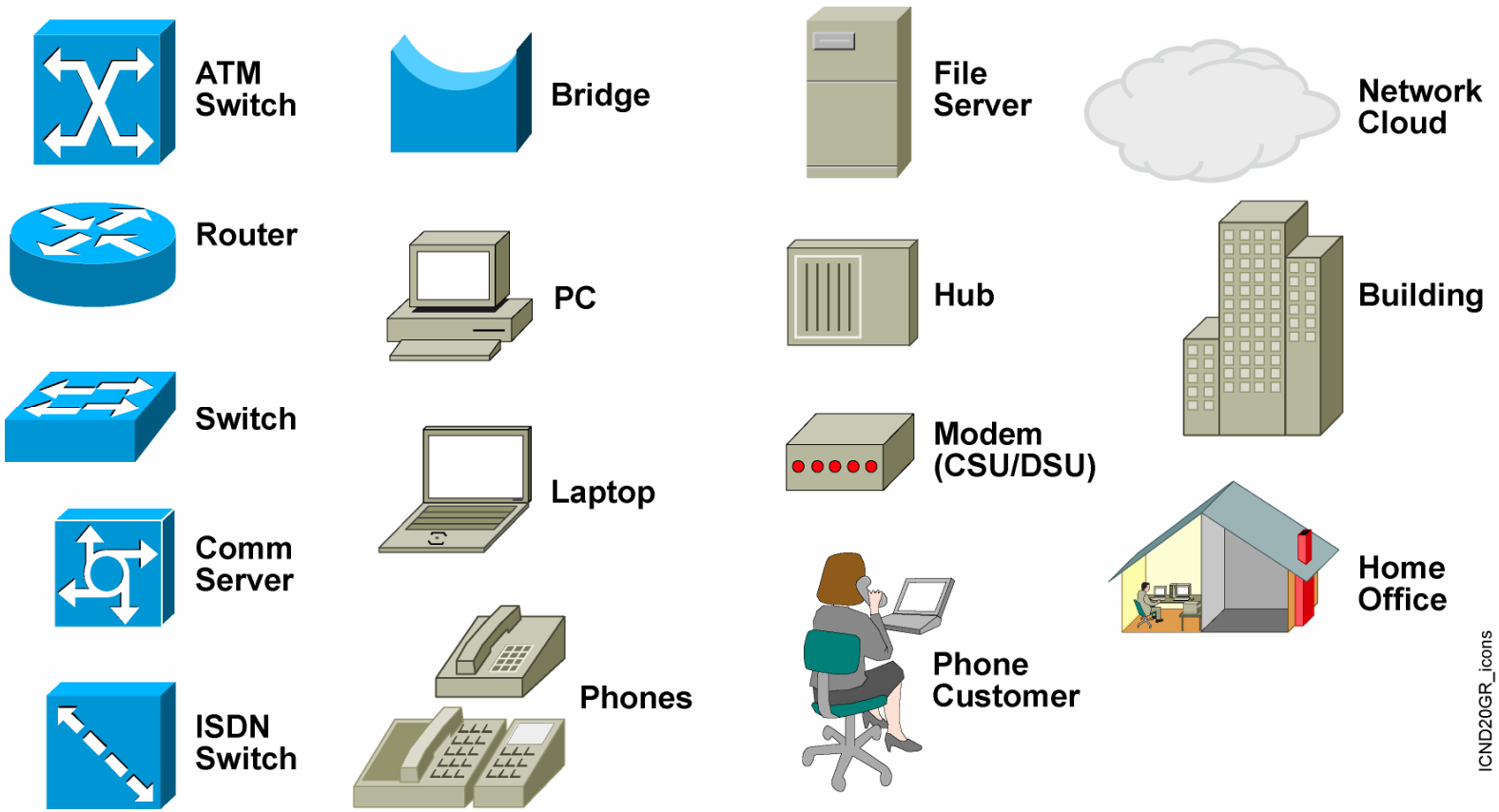
Nhu cầu kết nối Internet



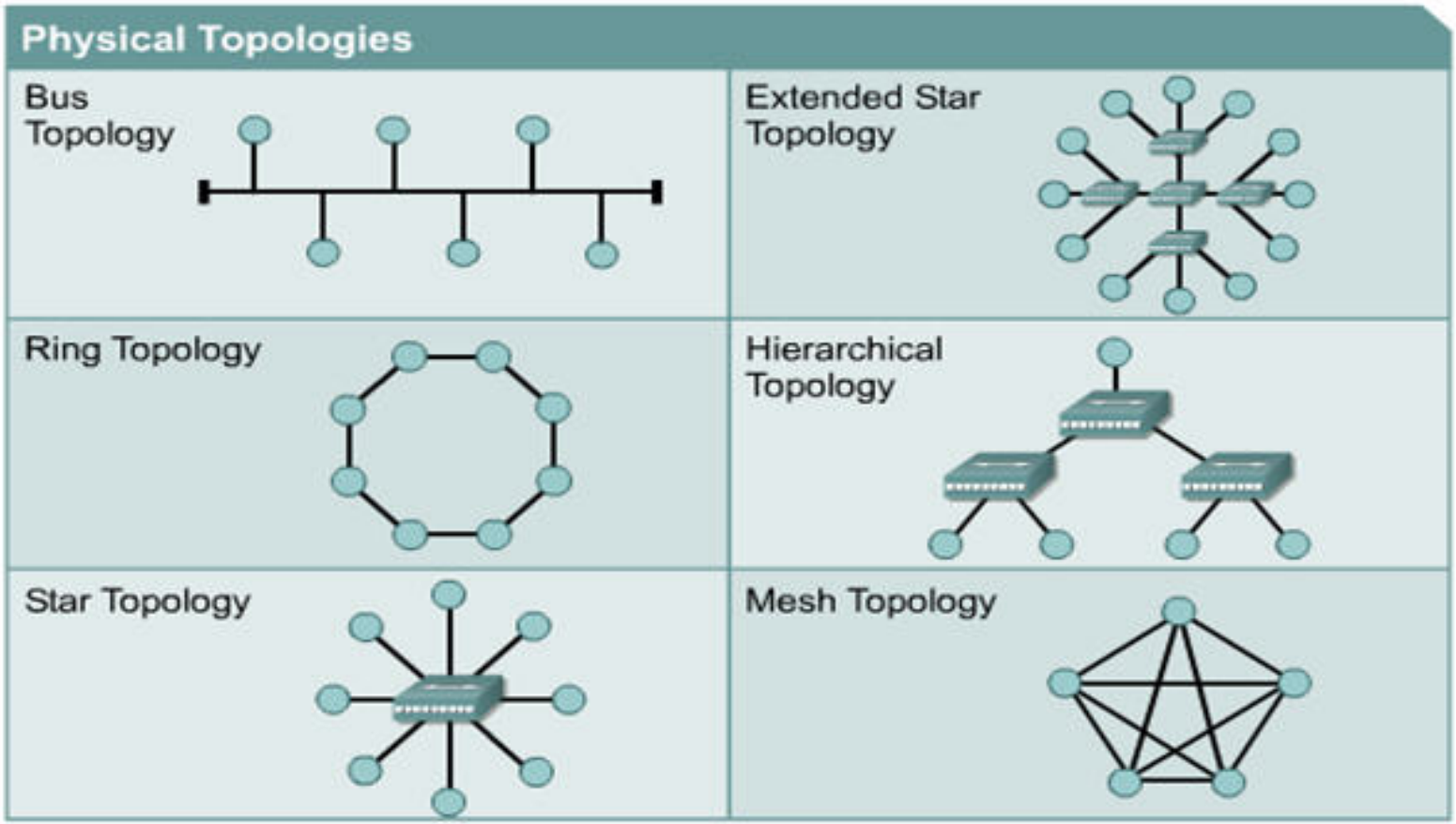
Nhu cầu kết nối Internet



Các ký hiệu thường dùng



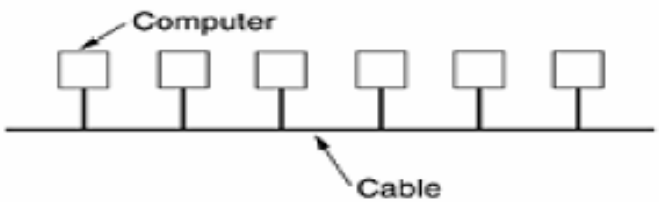
Lược đồ mạng (Network topology)



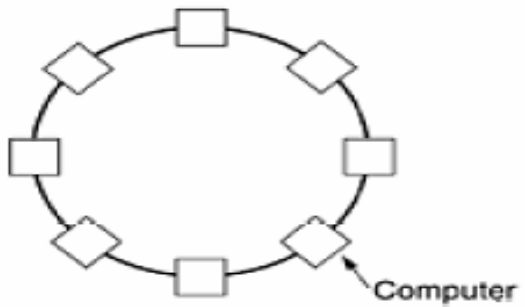
Phân loại mạng

Mạng cục bộ (Local Area Networks - LANs)

- Có giới hạn về địa lý
- Tốc độ truyền dữ liệu cao
- Do một tổ chức quản lý
- Sử dụng kỹ thuật Ethernet hoặc Token Ring
- Các thiết bị thường dùng trong mạng là Repeater, Brigde, Hub, Switch, Router.



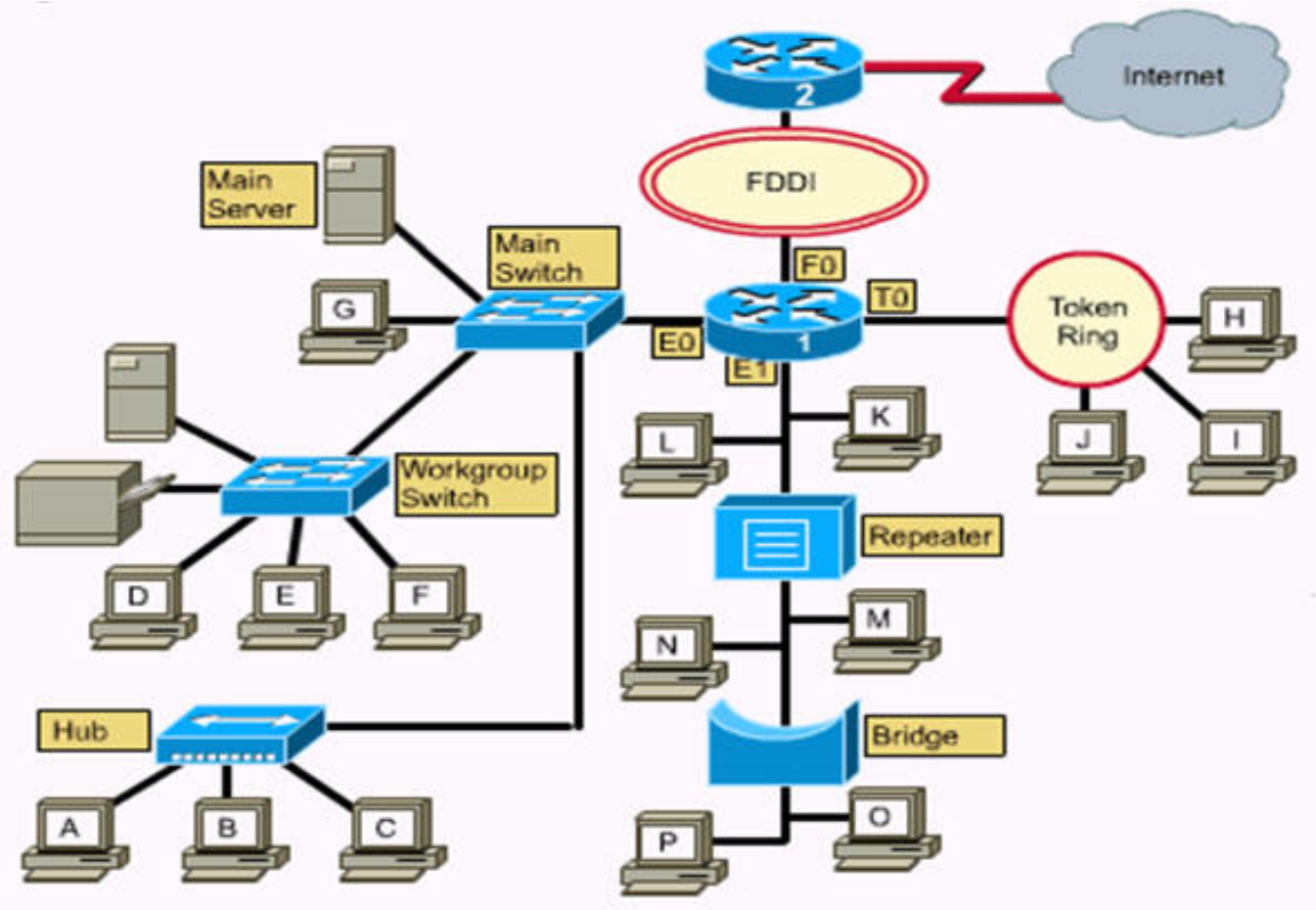
802.3 Ethernet



802.5 Token Ring

Phân loại mạng

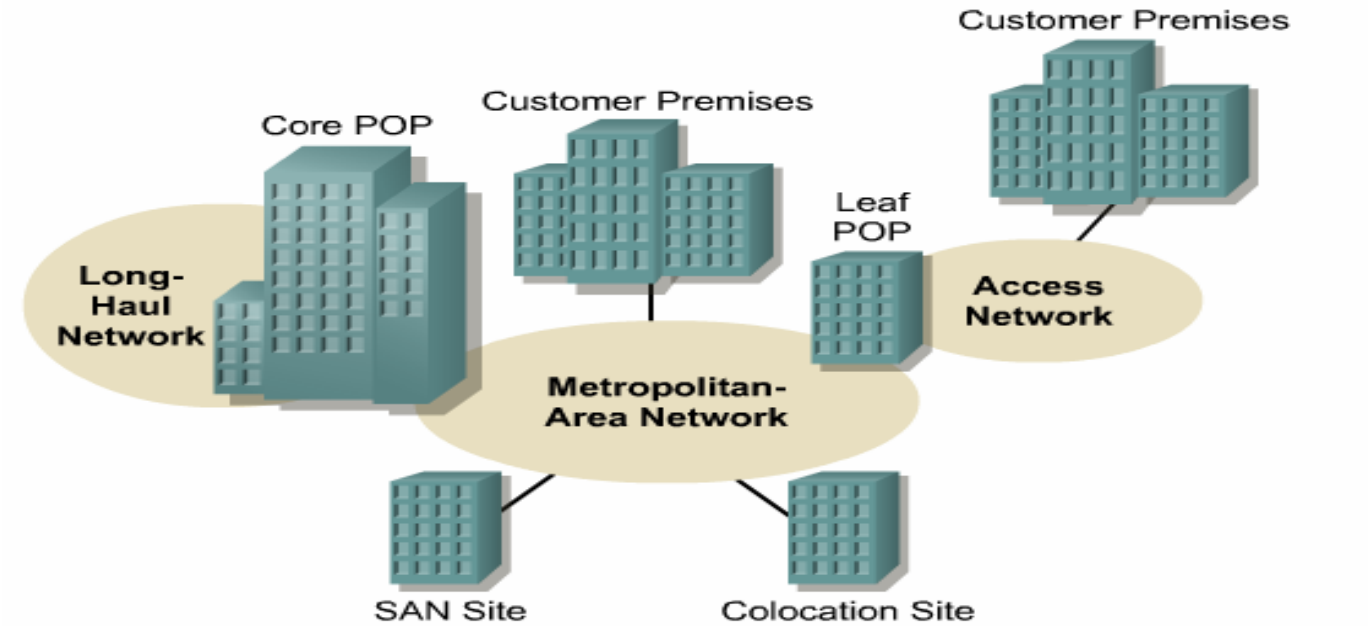
Mạng cục bộ (Local Area Networks - LANs)



Phân loại mạng

Mạng thành phố (Metropolitan Area Network - MANs)

- Có kích thước vùng địa lý lớn hơn LAN
- Do một tổ chức quản lý
- Thường dùng cáp đồng trục hoặc cáp quang

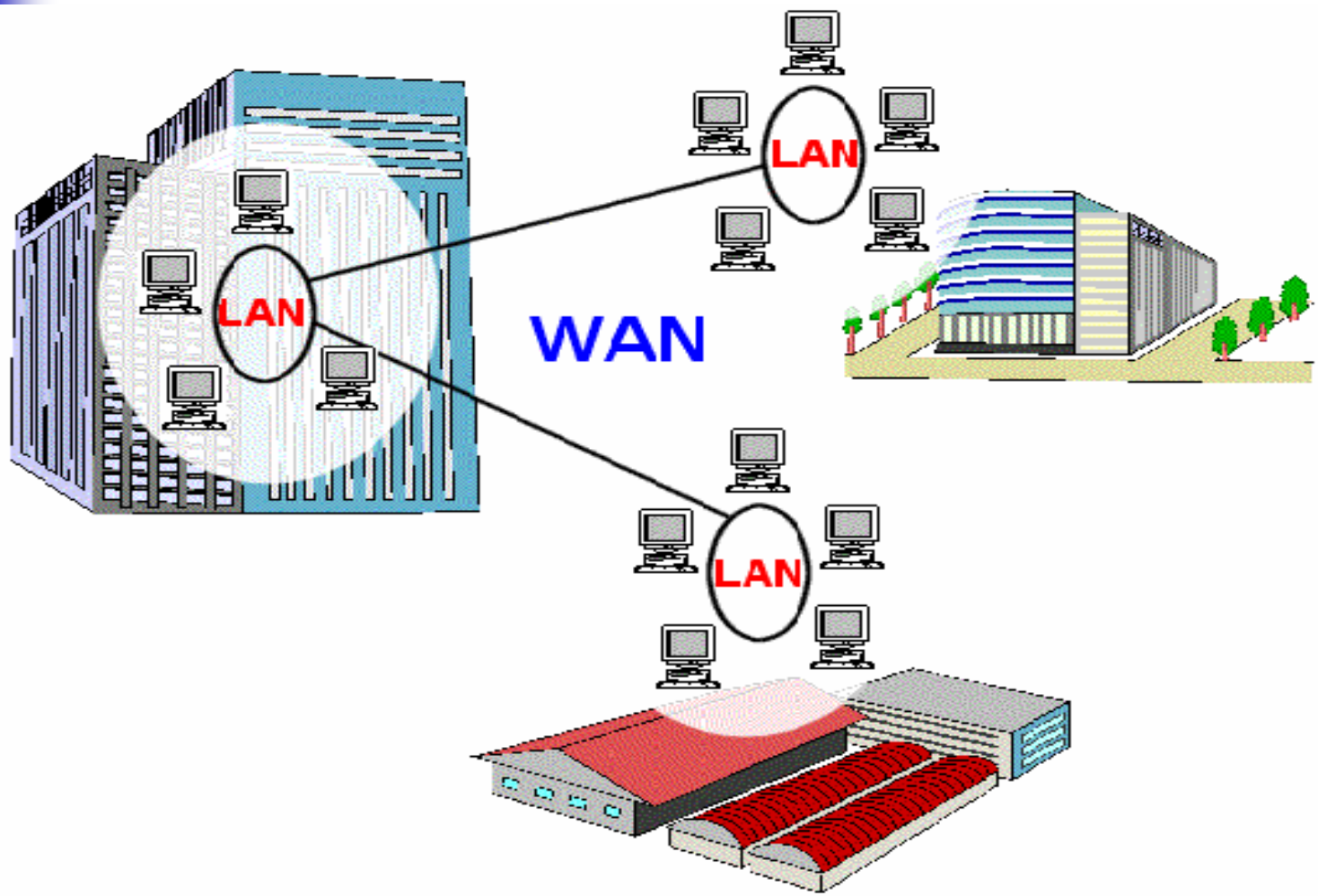


Phân loại mạng
Mạng diện rộng (Wide Area Networks - WANs)

- Là sự kết nối nhiều LAN
- Không có giới hạn về địa lý
- Tốc độ truyền dữ liệu thấp
- Do nhiều tổ chức quản lý
- Sử dụng các kỹ thuật Modem, ISDN, DSL, Frame Relay, ATM

Phân loại mạng

Mạng diện rộng (Wide Area Networks - WANs)



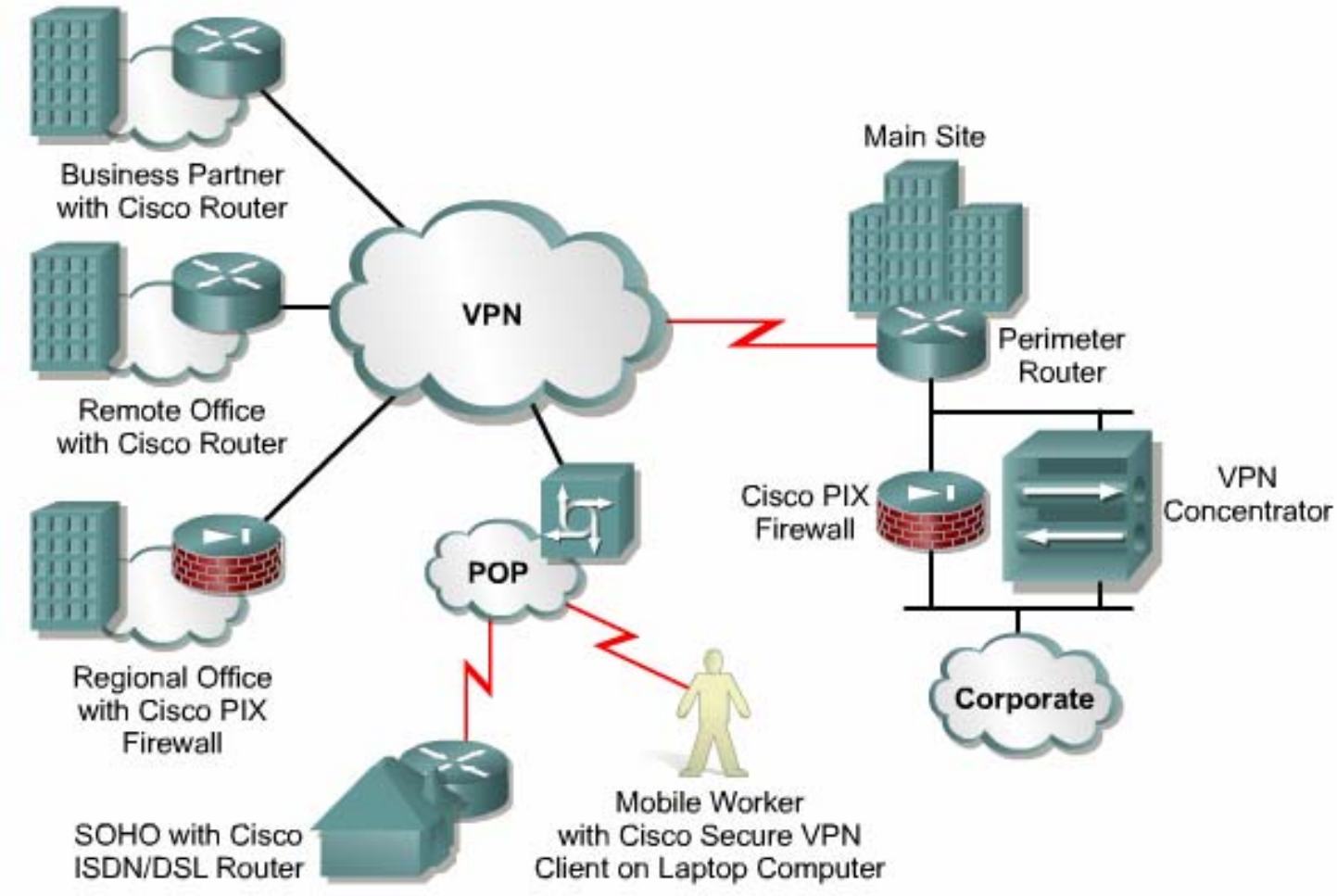
Phân loại mạng
Mạng không dây (Wireless Networking)

- Do tổ chức IEEE xây dựng và được tổ chức Wi-fi Alliance đưa vào sử dụng trên toàn thế giới.
- Có 3 tiêu chuẩn: chuẩn 802.11a, chuẩn 802.11b, chuẩn 802.11g (sử dụng phổ biến ở thị trường Việt Nam).
- Thiết bị cho mạng không dây gồm 2 loại: card mạng không dây và bộ tiếp sóng/điểm truy cập (Access Point - AP).

Phân loại mạng
Mạng không dây (Wireless Networking)

Phân loại mạng

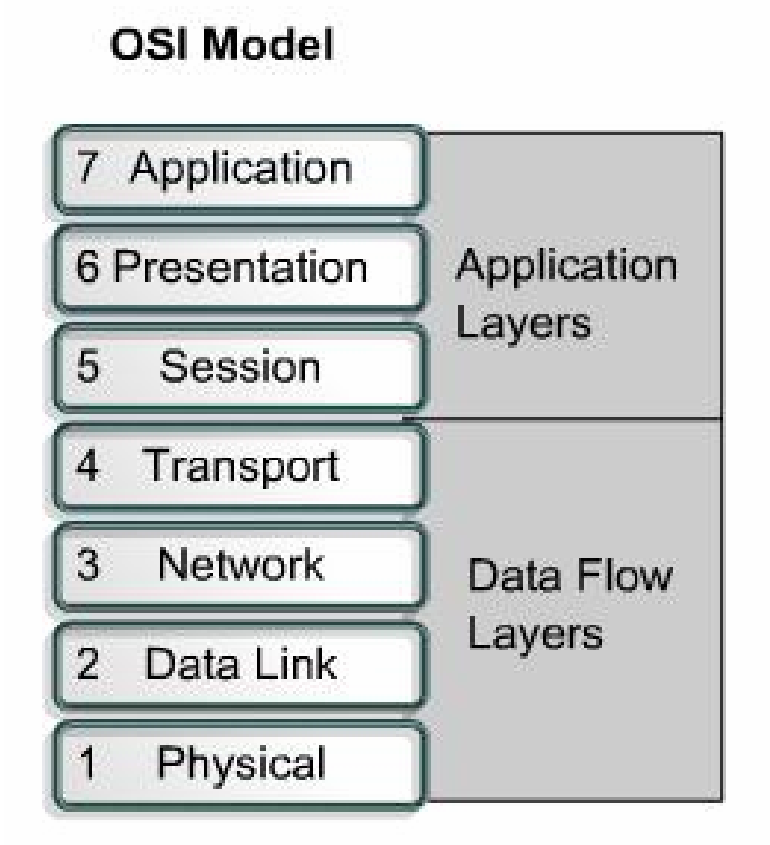
Mạng riêng ảo (Virtual Private Networks - VPNs)



Mô hình OSI và TCP/IP

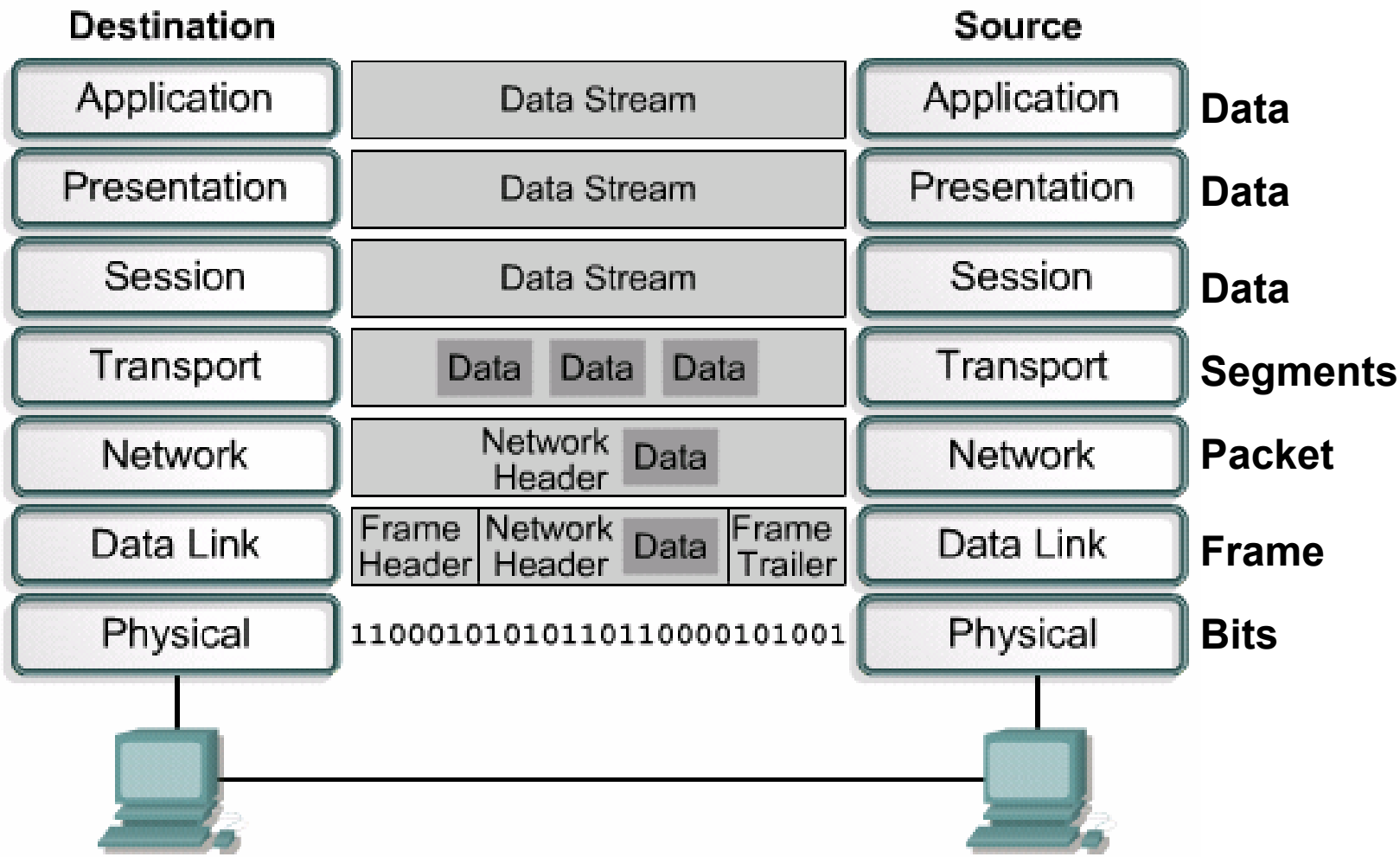
Mô hình OSI (Open Systems Interconnection)

- Lý do hình thành: Sự gia tăng mạnh mẽ về số lượng và kích thước mạng dẫn đến hiện tượng bất tương thích giữa các mạng.
- Ưu điểm của mô hình OSI:
  - Giảm độ phức tạp
  - Chuẩn hóa các giao tiếp
  - Đảm bảo liên kết hoạt động
  - Đơn giản việc dạy và học



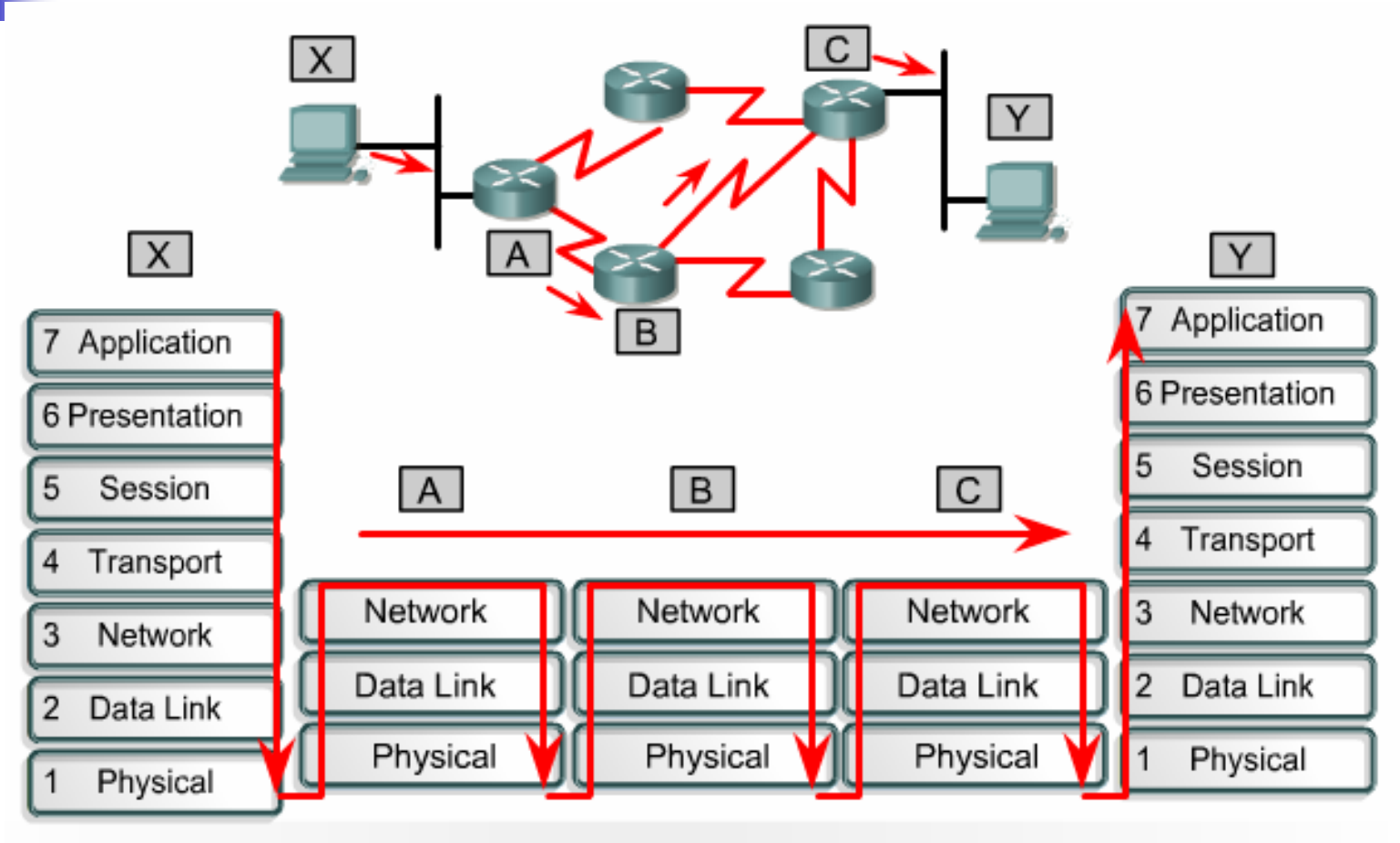
Mô hình OSI và TCP/IP

Đóng gói dữ liệu trong mô hình OSI



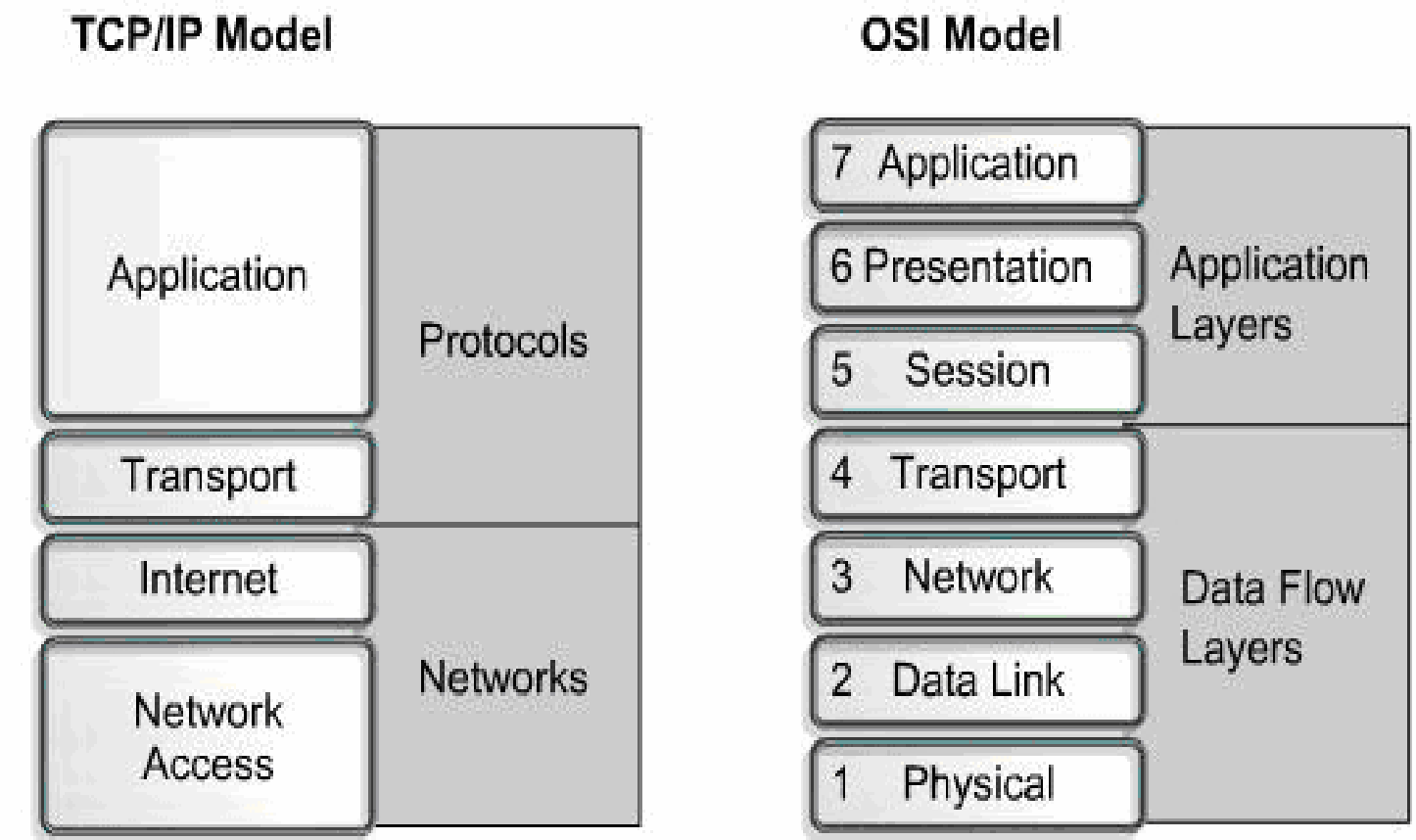
Mô hình OSI và TCP/IP

Dòng dữ liệu trên mạng trong mô hình OSI



Mô hình OSI và TCP/IP

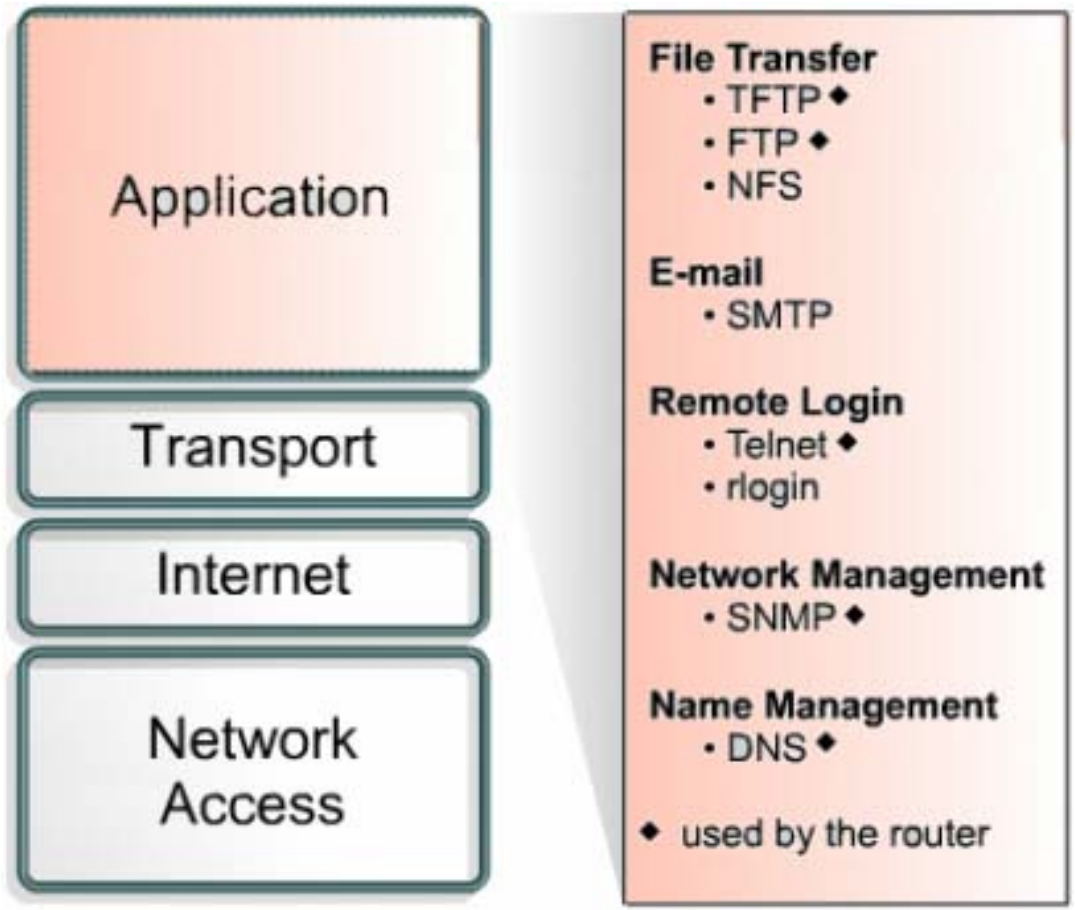
Mô hình TCP/IP



Mô hình OSI và TCP/IP

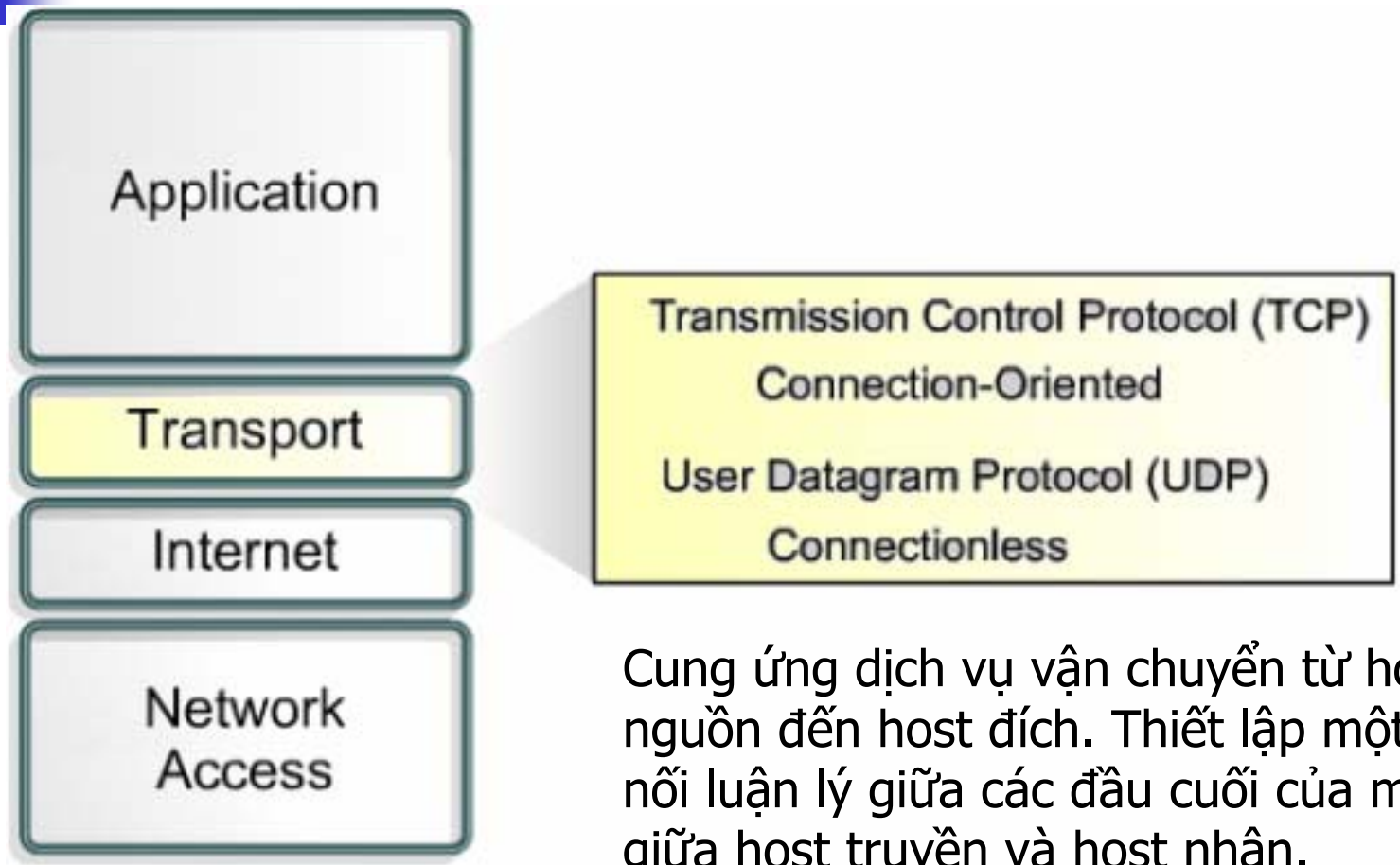
Mô hình TCP/IP – Lớp Ứng dụng

Kiểm soát các giao thức lớp cao, các chủ đề về trình bày, biểu diễn thông tin, mã hóa và điều khiển hội thoại. Đặc tả cho các ứng dụng phổ biến.



Mô hình OSI và TCP/IP

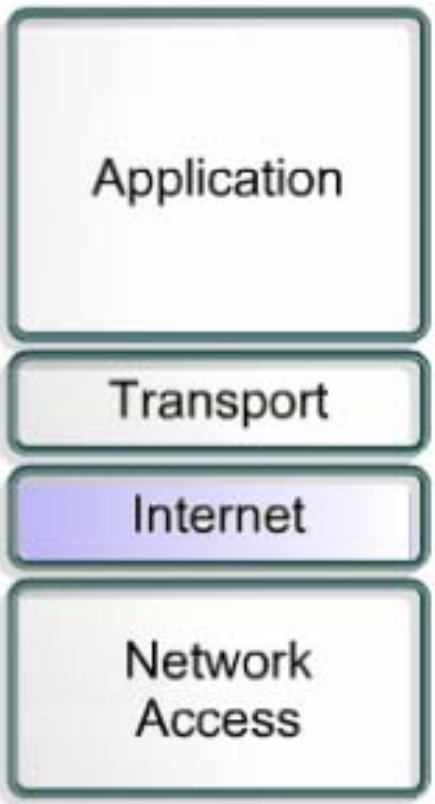
Mô hình TCP/IP – Lớp Vận chuyển



Cung ứng dịch vụ vận chuyển từ host nguồn đến host đích. Thiết lập một cầu nối luận lý giữa các đầu cuối của mạng, giữa host truyền và host nhận.

Mô hình OSI và TCP/IP

Mô hình TCP/IP – Lớp Internet

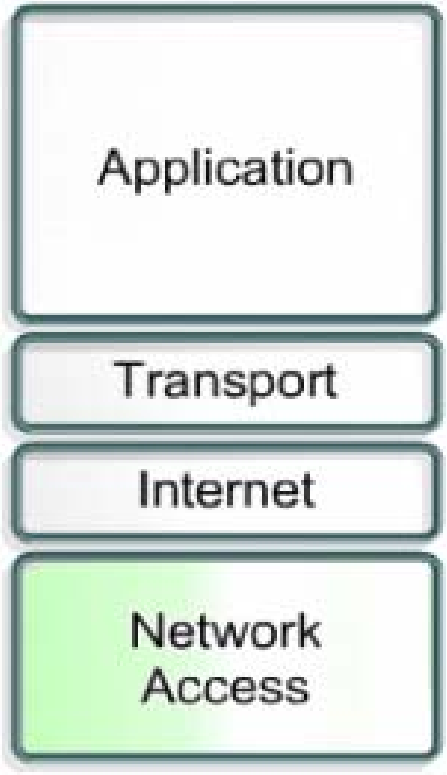


Mục đích của lớp Internet là chọn đường đi tốt nhất xuyên qua mạng cho các gói dữ liệu di chuyển tới đích. Giao thức chính của lớp này là Internet Protocol (IP).

- Internet Protocol (IP)
- Internet Control Message Protocol (ICMP)
- Address Resolution Protocol (ARP)
- Reverse Address Resolution Protocol (RARP)

Mô hình OSI và TCP/IP

Mô hình TCP/IP – Lớp Truy nhập mạng

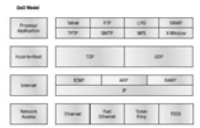


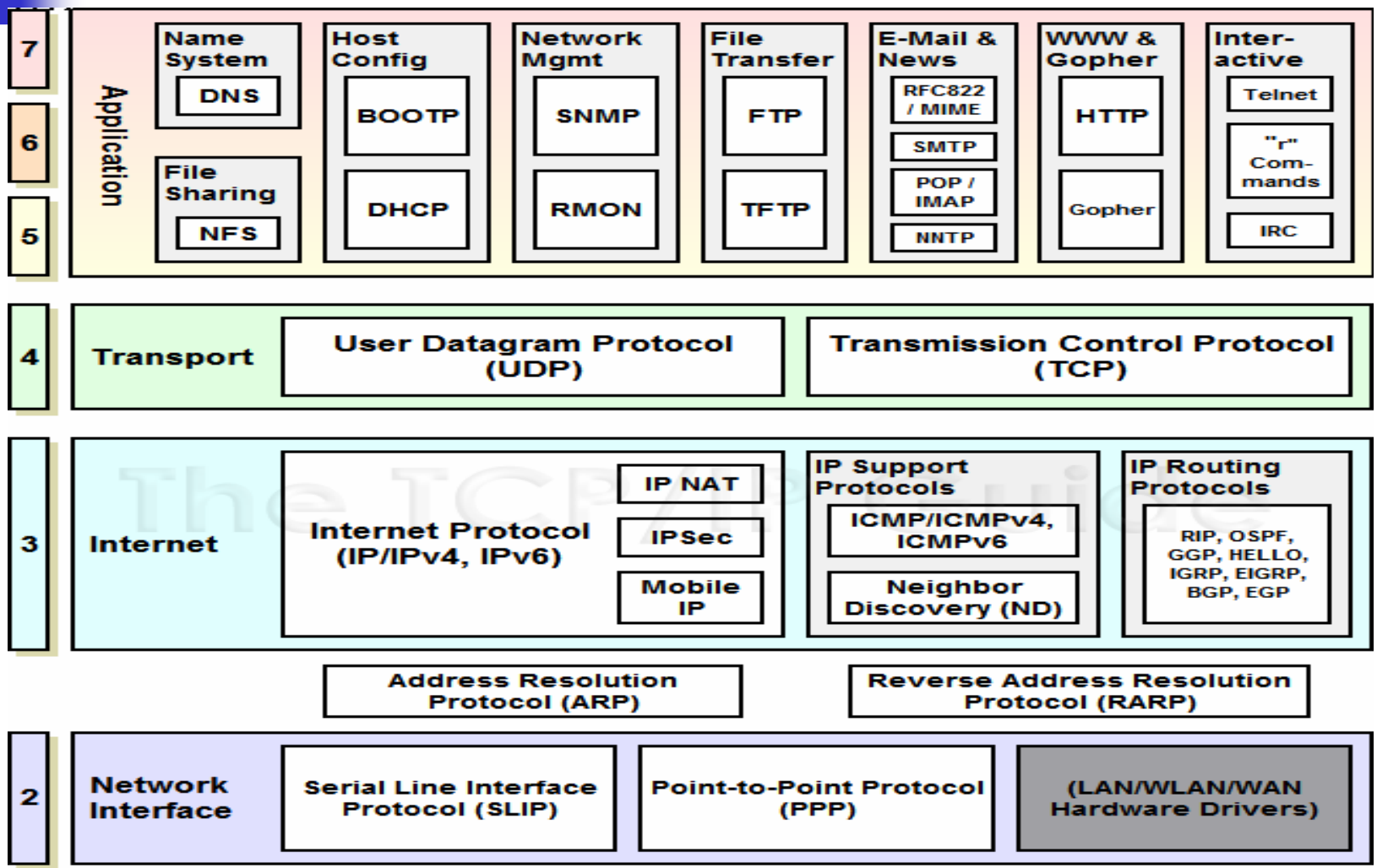
Định ra các thủ tục để giao tiếp với phần cứng mạng và truy nhập môi trường truyền. Có nhiều giao thức hoạt động tại lớp này

- Ethernet
- Fast Ethernet
- SLIP & PPP
- FDDI
- ATM, Frame Relay & SMDS
- ARP
- Proxy ARP
- RARP

Mô hình OSI và TCP/IP

Các giao thức trong mô hình TCP/IP





Các hệ thống số

- Hệ 2 (nhị phân): gồm 2 ký số 0, 1
- Hệ 8 (bát phân): gồm 8 ký số 0, 1, …, 7
- Hệ 10 (thập phân): gồm 10 ký số 0, 1, …, 9
- Hệ 16 (thập lục phân): gồm các ký số 0, 1, …, 9 và các chữ cái A, B, C, D, E, F

Các hệ thống số

Chuyển đổi giữa hệ nhị phân sang hệ thập phân

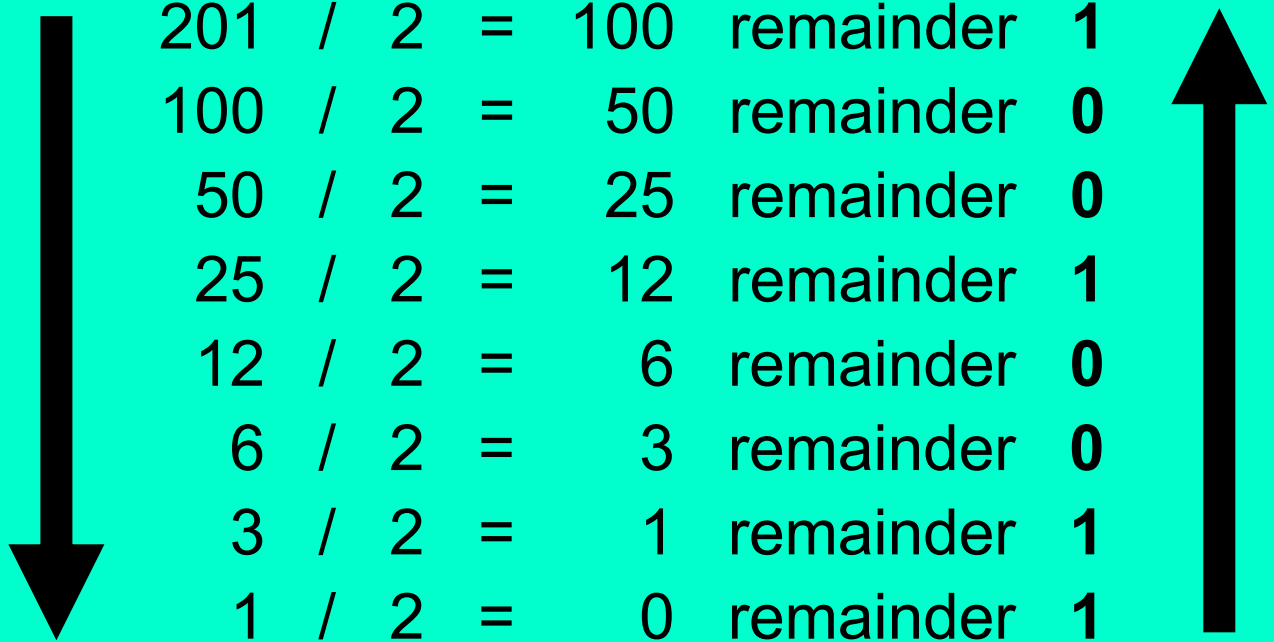
$10110_2 = (1 \times 2^4 = 16) + (0 \times 2^3 = 0) + (1 \times 2^2 = 4) + (1 \times 2^1 = 2) + (0 \times 2^0 = 0) = 22$

Place Value	128 64 32 16 8 4 2 1
Base^{Exponent}	$2^7 = 128$ $2^3 = 8$ $2^6 = 64$ $2^2 = 4$ $2^5 = 32$ $2^1 = 2$ $2^4 = 16$ $2^0 = 1$
Number of Symbols	2
Symbols	0, 1
Rationale	Two-state (discrete binary) voltage systems made from transistors can be diverse, powerful, inexpensive, tiny and relatively immune to noise.

Các hệ thống số

Chuyển đổi giữa hệ thập phân sang hệ nhị phân

Convert 201_{10} to binary:



201	/	2	=	100	remainder	**1**
100	/	2	=	50	remainder	**0**
50	/	2	=	25	remainder	**0**
25	/	2	=	12	remainder	**1**
12	/	2	=	6	remainder	**0**
6	/	2	=	3	remainder	**0**
3	/	2	=	1	remainder	**1**
1	/	2	=	0	remainder	**1**

When the quotient is 0, take all the remainders in reverse order for your answer: **$201_{10} = 11001001_2$**

Các hệ thống số

Chuyển đổi hệ nhị phân sang bát phân và thập lục phân

- Nhị phân sang bát phân:
  - Gom nhóm số nhị phân thành từng nhóm 3 chữ số tính từ phải sang trái. Mỗi nhóm tương ứng với một chữ số ở hệ bát phân.
  - Ví dụ: $1'101'100_{(2)} = 154_{(8)}$
- Nhị phân sang thập lục phân:
  - Tương tự như nhị phân sang bát phân nhưng mỗi nhóm có 4 chữ số.
  - Ví dụ: $110'1100_{(2)} = 6C_{(16)}$

Địa chỉ IP

Khái niệm về địa chỉ IP

- Địa chỉ IP là địa chỉ có cấu trúc với một con số có kích thước 32 bit, chia thành 4 phần mỗi phần 8 bit gọi là octet hoặc byte.
- Ví dụ:
  - 172.16.30.56
  - 10101100 00010000 00011110 00111000.
  - AC 10 1E 38

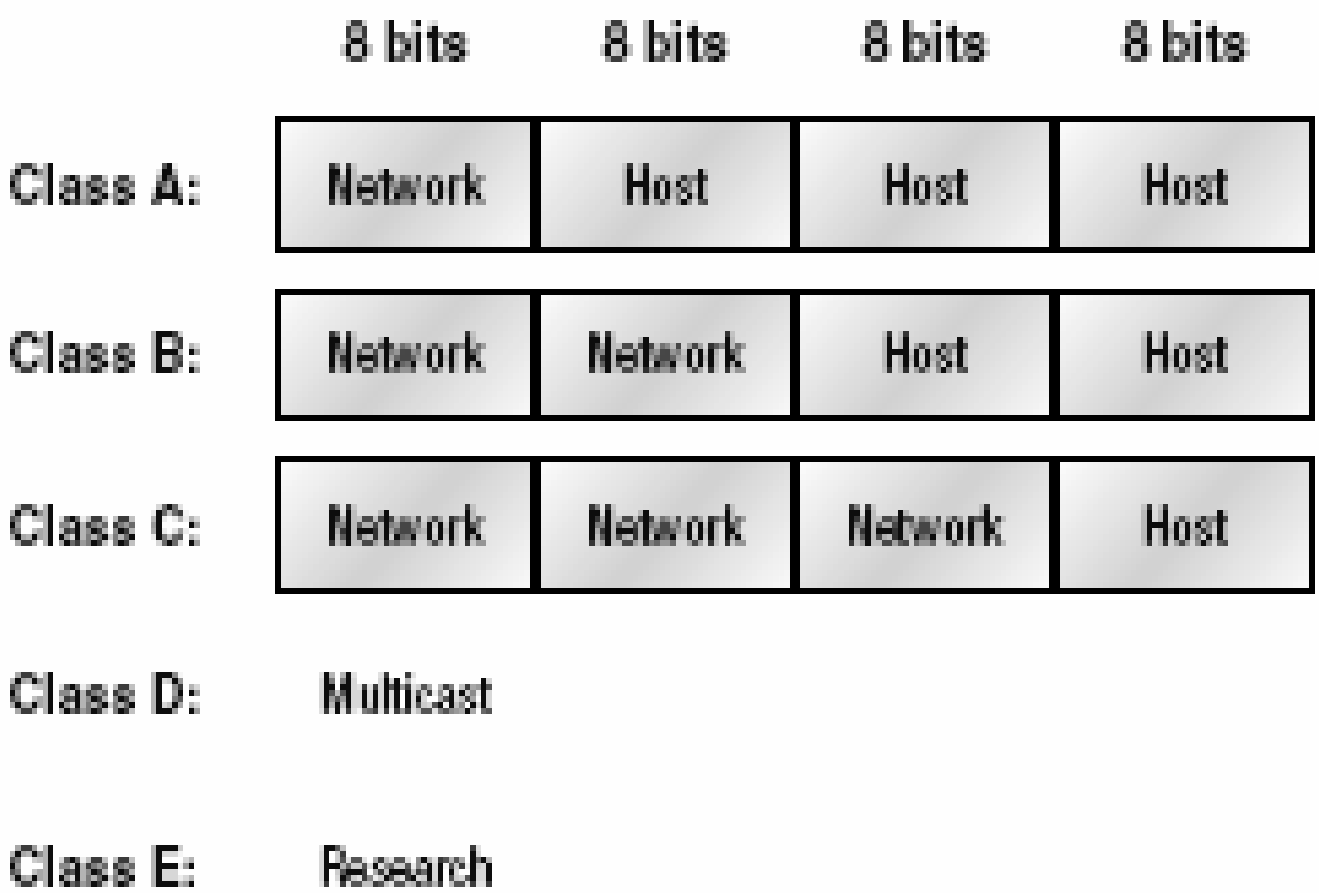
Địa chỉ IP

Khái niệm về địa chỉ IP

- Địa chỉ host là địa chỉ IP có thể dùng để đặt cho các interface của các host. Hai host nằm cùng một mạng sẽ có network_id giống nhau và host_id khác nhau.
- Địa chỉ mạng (network address): là địa chỉ IP dùng để đặt cho các mạng. Phần host_id của địa chỉ chỉ chứa các bit 0. Ví dụ 172.29.0.0
- Địa chỉ Broadcast: là địa chỉ IP được dùng để đại diện cho tất cả các host trong mạng. Phần host_id chỉ chứa các bit 1. Ví dụ 172.29.255.255.

Địa chỉ IP

Các lớp địa chỉ IP



Địa chỉ IP

Các lớp địa chỉ IP

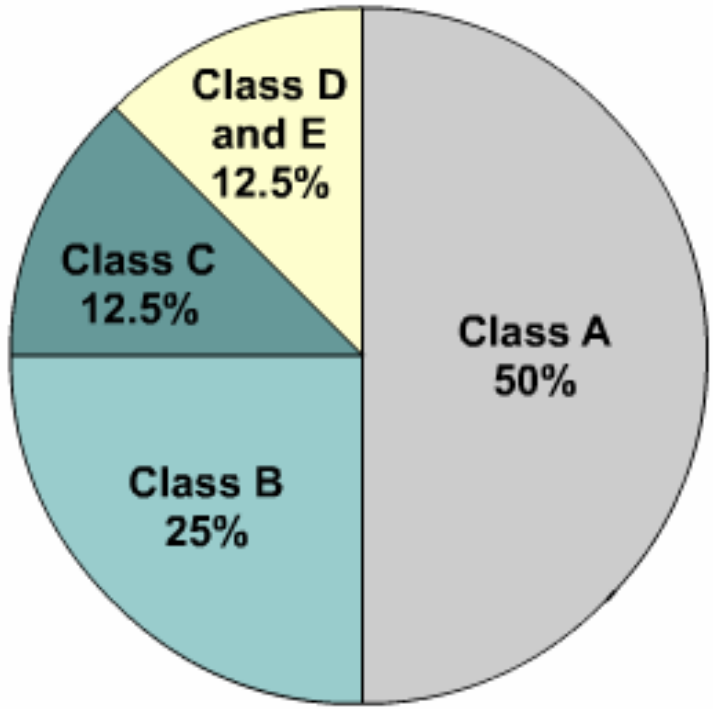
Address Class	Number of Networks	Number of Host per Network
A	126 *	16,777,216
B	16, 384	65,535
C	2,097,152	254
D (Multicast)	N/A	N/A

IP Address Class	High Order Bits	First Octet Address Range	Number of Bits in the Network Address
Class A	0	0 - 127 *	8
Class B	10	128 - 191	16
Class C	110	192 - 223	24
Class D	1110	224 - 239	28

Địa chỉ IP

Các lớp địa chỉ IP

IP address class	IP address range (First Octet Decimal Value)
Class A	1-126 (00000001-01111110) *
Class B	128-191 (10000000-10111111)
Class C	192-223 (11000000-11011111)
Class D	224-239 (11100000-11101111)
Class E	240-255 (11110000-11111111)



Địa chỉ IP

Địa chỉ IP dành riêng

Class	RFC 1918 internal address range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255.255

MÔI TRƯỜNG VÀ THIẾT BỊ TRUYỀN DẪN

- Môi trường truyền dẫn
- Băng thông (Bandwidth)
- Các đặc tả về cáp
- Cáp đồng trục (Coaxial cable)
- Cáp xoắn đôi (Twisted pair cable)
  - Cáp STP (Shield Twisted-Pair)
  - Cáp UTP (Unshield Twisted-Pair)
  - Các loại kết nối cáp
- Cáp quang (Fiber Optic Cable)
- Các thông số cơ bản của các loại cáp

Môi trường truyền dẫn

- Là phương tiện vật lý cho phép truyền tải tín hiệu giữa các thiết bị.
- Hai loại phương tiện truyền dẫn chính:
  - Hữu tuyến
  - Vô tuyến
- Hệ thống sử dụng hai loại tín hiệu:
  - Digital
  - Analog

Băng thông (bandwidth)

- Là lượng thông tin có thể chảy qua một kết nối mạng trong một khoảng thời gian cho trước.
  - Băng thông là hữu hạn
  - Băng thông không miễn phí
  - Nhu cầu băng thông tăng không ngừng
- Dạng tương tự băng thông:
  - Bề rộng một cái ống
  - Số làn xe trên đường cao tốc

Băng thông (bandwidth)

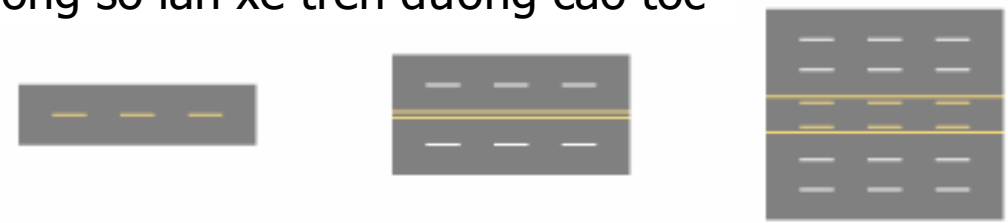
Băng thông giống độ lớn của ống

Các thiết bị mạng là máy bơm, van, lọc, đầu nối

Các gói là nước

Băng thông (bandwidth)

Băng thông giống số làn xe trên đường cao tốc



Các thiết bị mạng là các chỉ dẫn lưu thông, bản đồ

Các gói giống phương tiện giao thông

Băng thông
Đơn vị đo lường băng thông

Unit of Bandwidth	Abbreviation	Equivalence
Bits per second	bps	1 bps = fundamental unit of bandwidth
Kilobits per second	kbps	1 kbps = ~1,000 bps = 10^3 bps
Megabits per second	Mbps	1 Mbps = ~1,000,000 bps = 10^6 bps
Gigabits per second	Gbps	1 Gbps = ~1,000,000,000 bps = 10^9 bps
Terabits per second	Tbps	1 Tbps = ~1,000,000,000,000 bps = 10^{12} bps

Băng thông

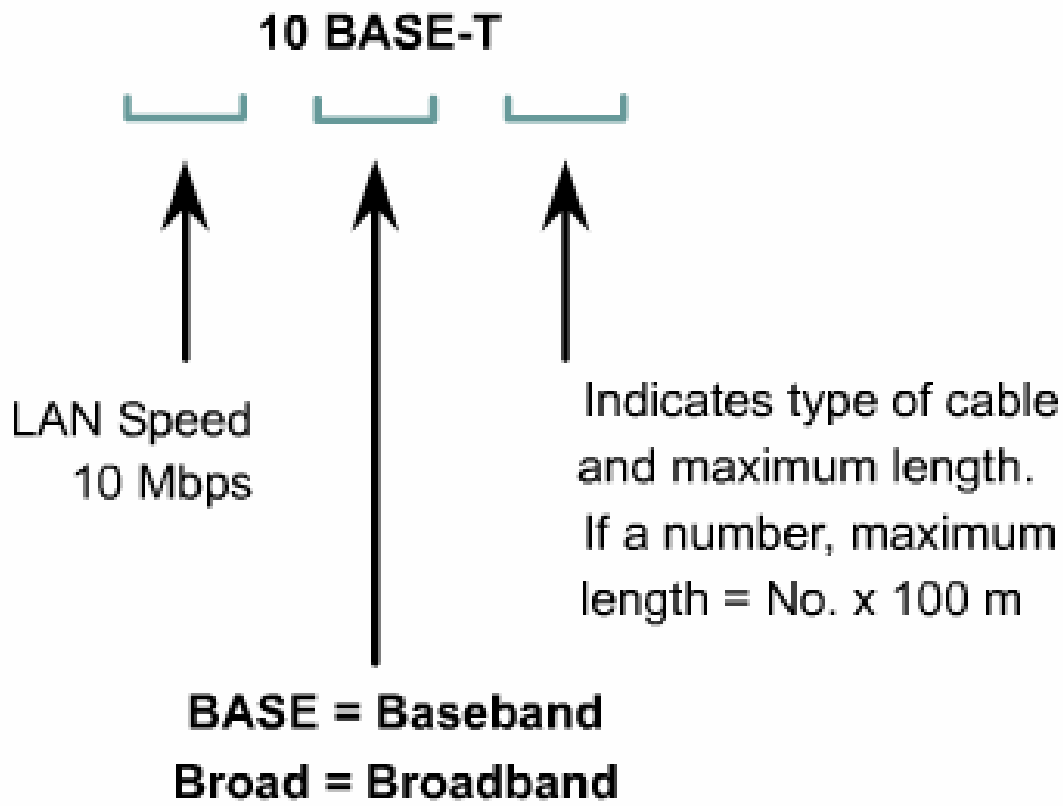
Các giới hạn của băng thông

Some Typical Media	Bandwidth	Max. Physical Distance
50-Ohm Coaxial Cable (Ethernet 10BASE2, ThinNet)	10-100 Mbps	185m
50-Ohm Coaxial Cable (Ethernet 10BASE5, ThickNet)	10-100 Mbps	500m
Category 5 Unshielded Twisted Pair (UTP) (Ethernet 10BASE-T)	10 Mbps	100m
Category 5 Unshielded Twisted Pair (UTP) (Ethernet 100BASE-TX)(Fast Ethernet)	100 Mbps	100m
Multimode (62.5/125μm) Optical Fiber 100BASE-FX	100 Mbps	2000m
Singlemode (9/125μm core) Optical Fiber 1000BASE-LX	1000 Mbps (1.000 Gbps)	3000m
Wireless	11 Mbps	a few 100meters

Các đặc tả về cáp

- Phẩm chất cáp
  - Tốc độ truyền số liệu
  - Truyền dẫn băng cơ bản (Baseband) và băng rộng (Broadband)
  - Truyền dẫn digital và analog
  - Khoảng cách truyền dẫn và sự suy giảm của tín hiệu
- Các đặc tả:
  - Ethernet: 10BASE-T, 10BASE5, 10BASE2
  - Fast Ethernet: 100BASE-T

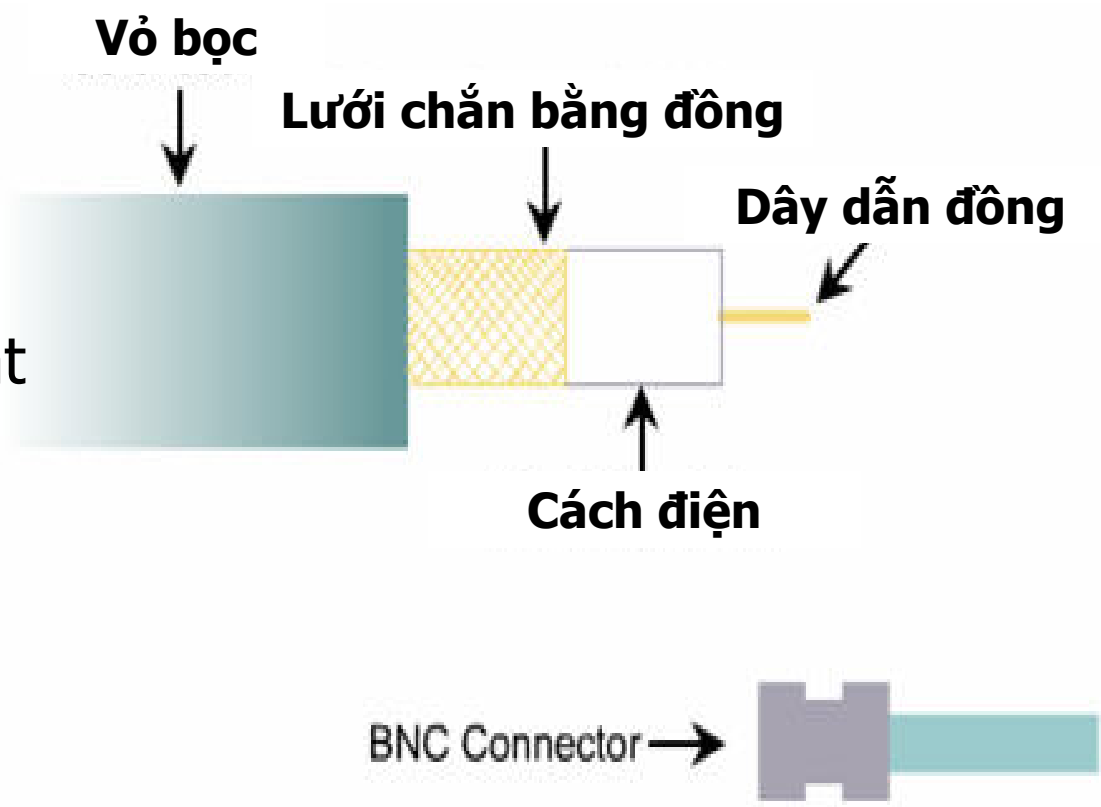
Các đặc tả về cáp



- T: twisted (cáp xoắn đôi)
- 5: 500 m
- 2: 200 m

Cáp đồng trục (Coaxial cable)

- Cấu tạo
- Phân loại
  - Thinnet/Thicknet
  - Baseband/ Broadband
- Thông số kỹ thuật
  - Chiều dài cáp
  - Tốc độ truyền
  - Nhiễu
  - Lắp đặt/bảo trì
  - Giá thành
  - Kết nối

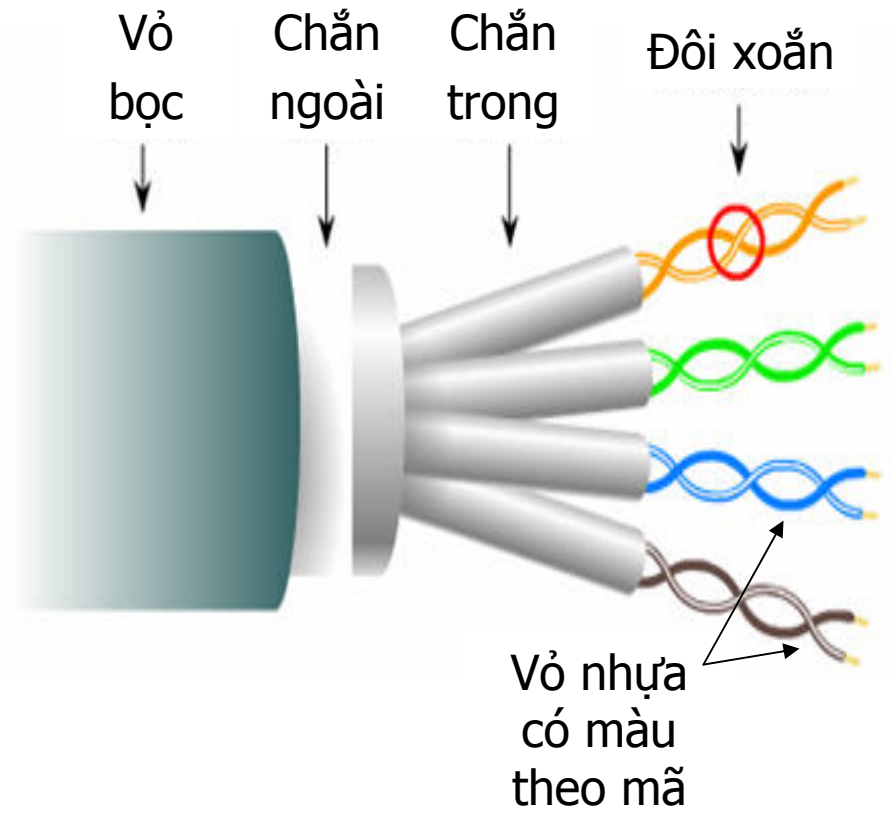


Cáp đồng trục (Coaxial cable)

- Thicknet: Cứng, khó lắp đặt, chi phí cao nên ít dùng.
- Thinnet: Chi phí thấp, dễ lắp đặt nhưng nhiễu cao.

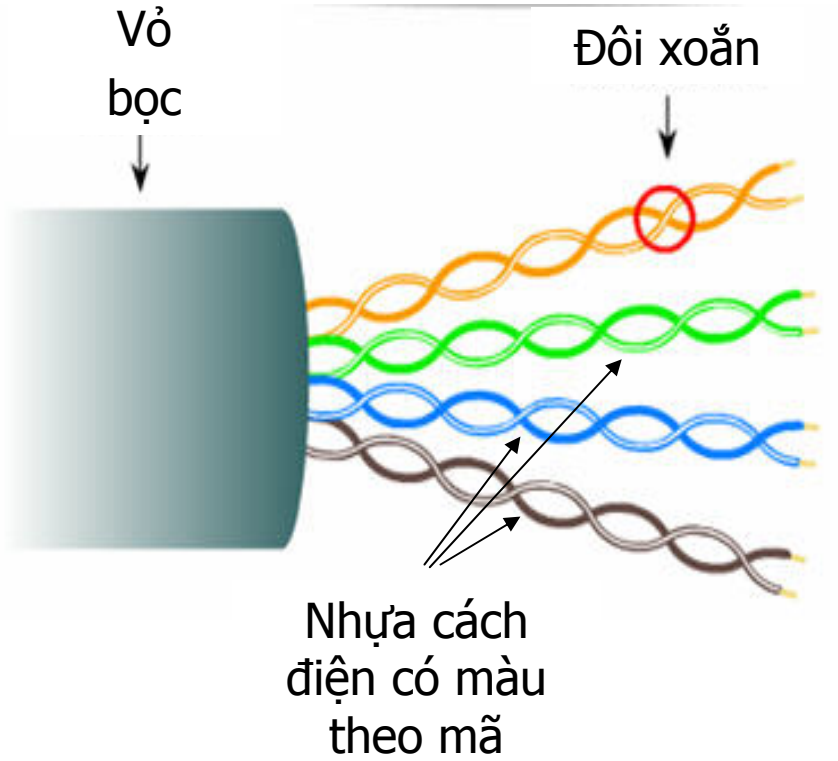
Cáp xoắn đôi

Cáp STP (Shield Twisted-Pair)



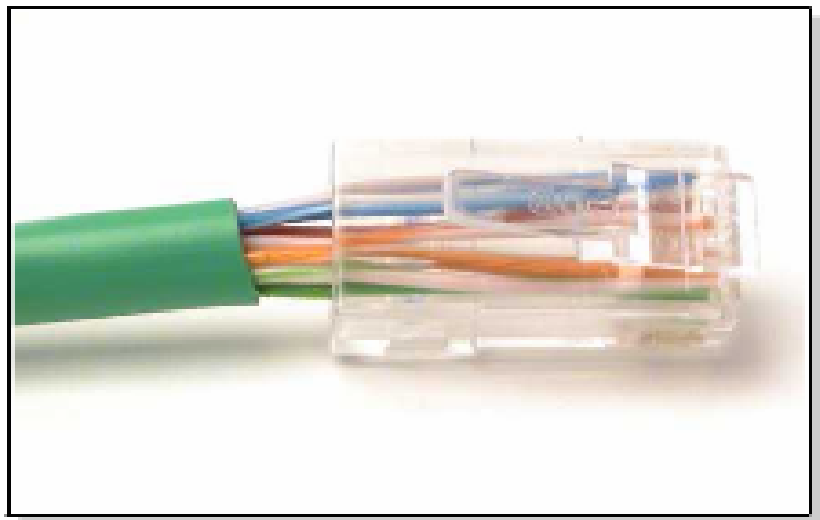
- Tốc độ: 10 – 100Mbps
- Giá: vừa phải
- Chiều dài cáp tối đa: 100 m
- Chống nhiễu tốt
- Dùng cho mạng có kích thước trung bình và lớn

Cáp xoắn đôi
Cáp UTP (Unshield Twisted-Pair)

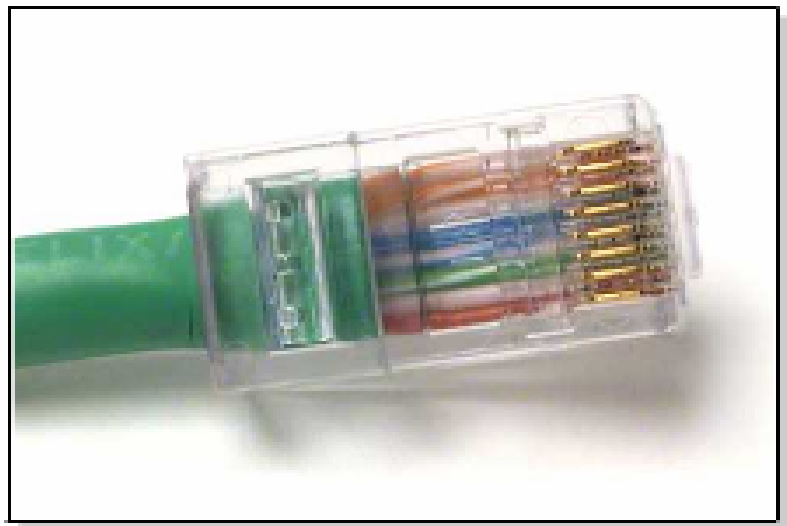


- Tốc độ: 10 – 100 – 1000 Mbps
- Giá: rẻ
- Chiều dài cáp tối đa: 100 m
- Chống nhiễu kém
- Dễ lắp đặt
- Dùng cho mạng có kích thước nhỏ

Các loại kết nối cáp



Kết nối kém



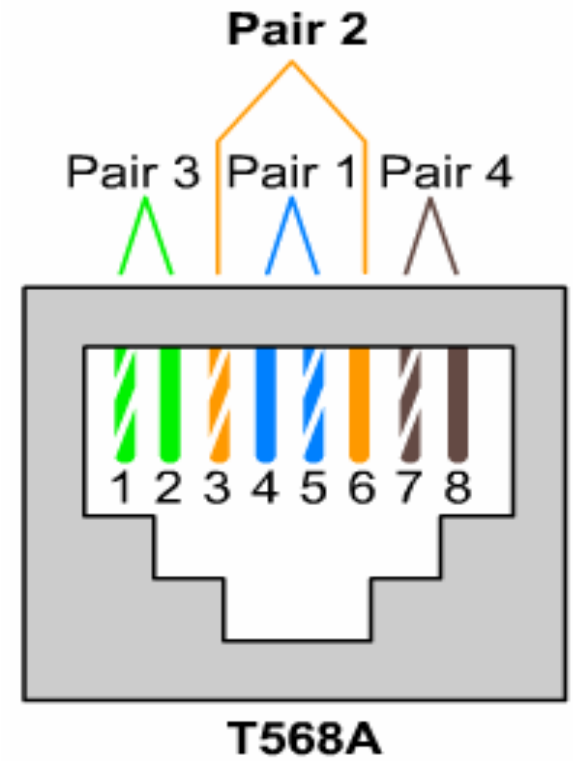
Kết nối tốt

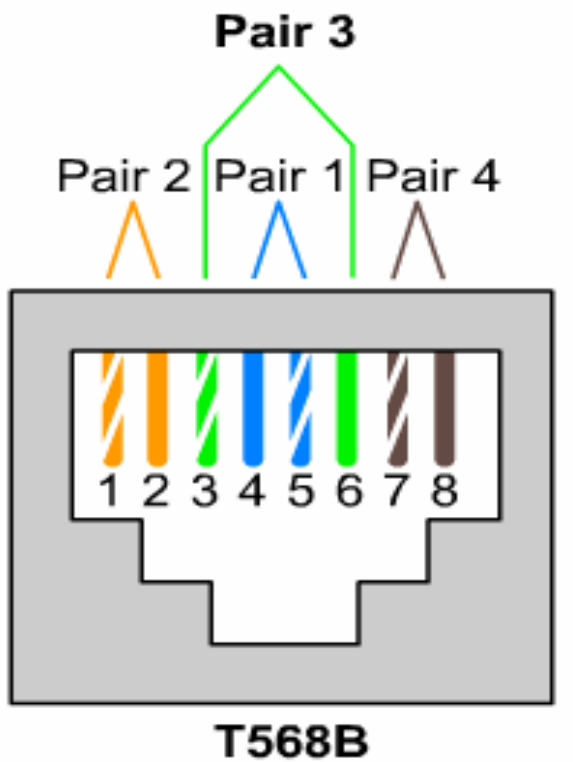
Các loại kết nối cáp

Straight-thru cable	Crossover cable	Rollover cable
Pin 1 --------- Pin 1	Pin 1 --------- Pin 3	Pin 1 --------- Pin 8
Pin 2 --------- Pin 2	Pin 2 --------- Pin 6	Pin 2 --------- Pin 7
Pin 3 --------- Pin 3	Pin 3 --------- Pin 1	Pin 3 --------- Pin 6
Pin 4 --------- Pin 4	Pin 4 --------- Pin 4	Pin 4 --------- Pin 5
Pin 5 --------- Pin 5	Pin 5 --------- Pin 5	Pin 5 --------- Pin 4
Pin 6 --------- Pin 6	Pin 6 --------- Pin 2	Pin 6 --------- Pin 3
Pin 7 --------- Pin 7	Pin 7 --------- Pin 7	Pin 7 --------- Pin 2
Pin 8 --------- Pin 8	Pin 8 --------- Pin 8	Pin 8 --------- Pin 1

Các loại kết nối cáp

- Cáp Straight-thru có T568B ở cả 2 đầu.
- Cáp Crossover có T568B ở một đầu và T568A ở đầu còn lại.
- Cáp Console có T568B ở một đầu và T568B đảo ở đầu còn lại (Rollover).





Các loại kết nối cáp

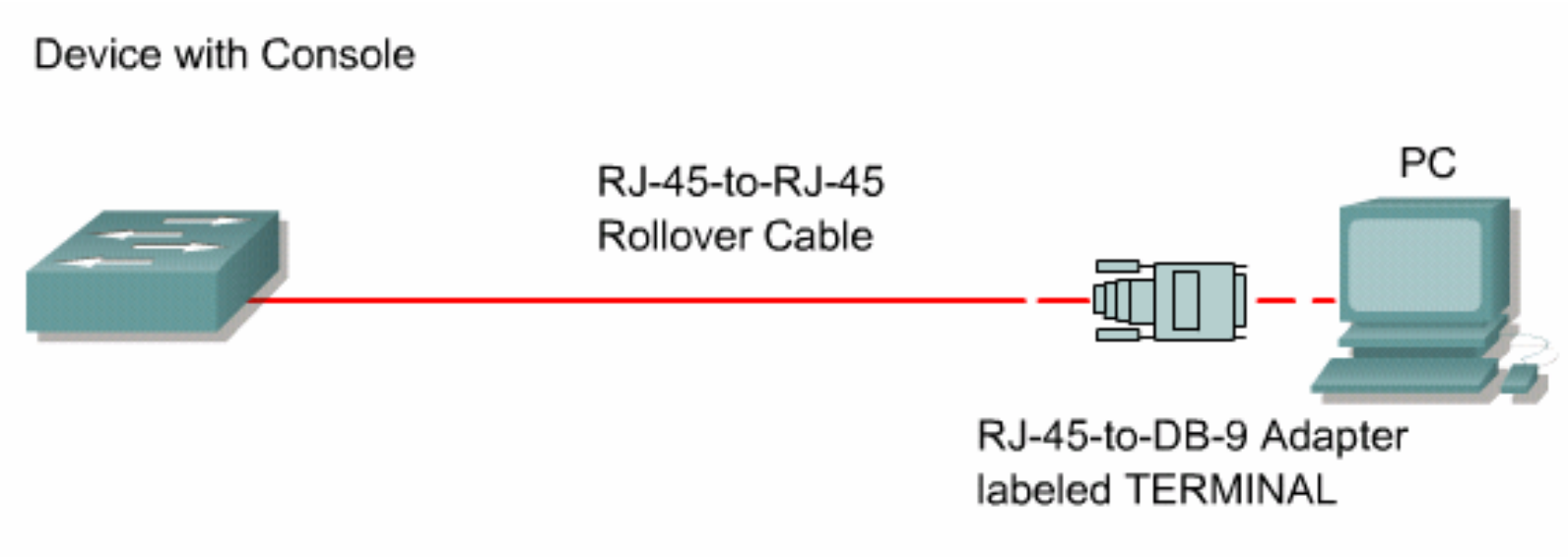
- Sử dụng cáp thẳng (Straight-through cable) đối với:
  - Switch – Router
  - Switch – PC hoặc Server
  - Hub – PC hoặc Server

Các loại kết nối cáp

- Sử dụng cáp Crossover đối với:
  - Switch – Switch
  - Switch – Hub
  - Hub – Hub
  - Router – Router
  - PC – PC

Các loại kết nối cáp

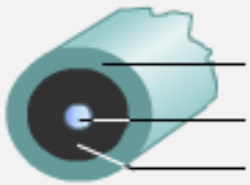
- Sử dụng cáp Rollover đối với:
  - PC – Router hoặc Switch (cổng COM nối cổng Console)



Cáp quang (Fiber Optic Cable)

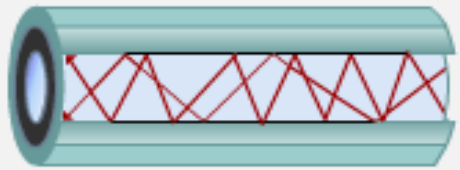
Single-mode

Requires very straight path

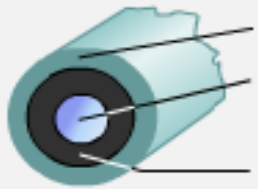


- Small core
- Less dispersion
- Suited for long distance applications (up to ~3km, 9,840 ft)
- Uses lasers as the light source often within campus backbones for distances of several thousand meters

Multimode

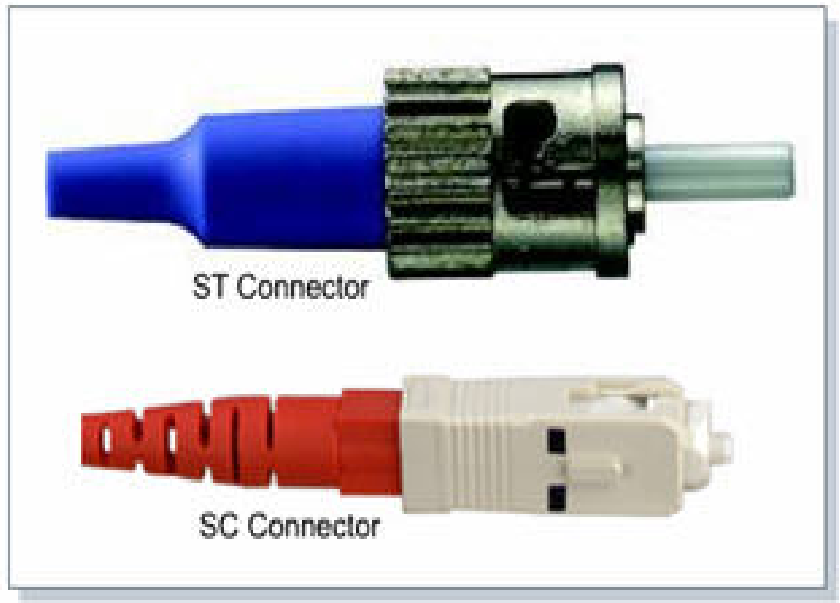


Multiple paths-sloppy



- Larger core than single-mode cable (50 or 62.5 microns or greater)
- Allows greater dipersion and therefore, loss of signal
- Used for long distance application, but shorter than single-mode (up to ~2km, 6,560 ft)
- Uses LEDs as the light source often within LANs or distances of a couple hundred meters within a campus network

Cáp quang (Fiber Optic Cable)



- ST Connector được dùng với cáp Single-mode.
- SC Connector được dùng với cáp Multimode

Thông số cơ bản của các loại cáp

Cáp	Chiều dài cáp tối đa	Tốc độ truyền	Lắp đặt	Nhiễu	Giá thành
UTP	100 m	10-100 Mbps	Dễ	Cao	Thấp nhất
STP	100 m	16-500 Mbps	Khá dễ	Thấp	Vừa phải
Thinnet	185 m	10 Mbps	Dễ	Thấp	Thấp
Thicknet	500 m	10 Mbps	Khó	Thấp	Cao
Fiber optics	2000 m	2 Gbps	Khó	Không	Đắt

Thông số cơ bản của các loại cáp

	10BASE2	10BASE5	10BASE-T	100BASE-TX	100BASE-FX
Media	50-ohm coaxial (Thinnet)	50-ohm coaxial (Thicknet)	EIA/TIA Category 3, 4, 5 UTP, two pair	EIA/TIA Category 5 UTP, two pair	62.5/125 multimode fiber
Maximum Segment Length	185 m (606.94 feet)	500 m (1640.4 feet)	100 m (328 feet)	100 m (328 feet)	400 m (1312.3 feet)
Topology	Bus	Bus	Star	Star	Star
Connector	BNC	Attachment unit interface (AUI)	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)	Duplex media interface connector (MIC) ST or SC connector

THIẾT BỊ LIÊN KẾT MẠNG

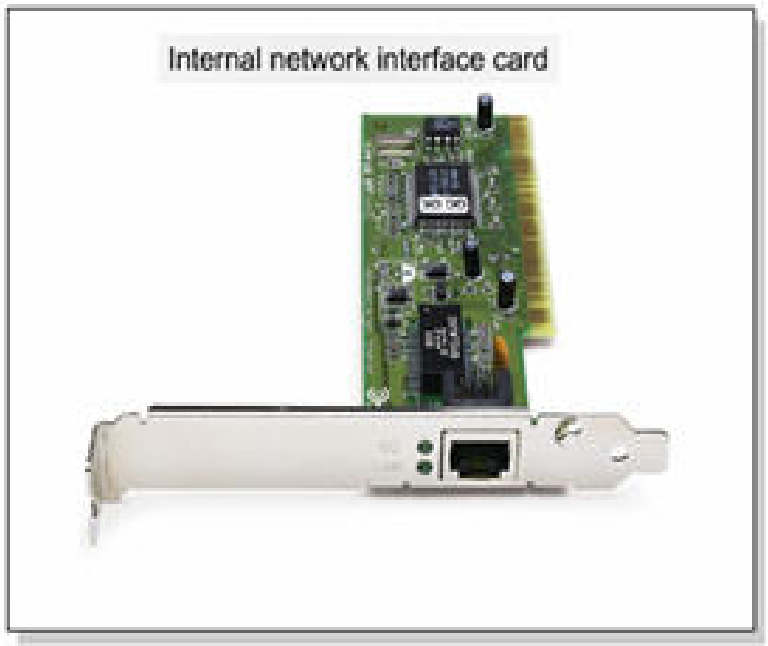
- Lab center
- NIC (Network Interface Card – Card mạng)
- Modem (Bộ điều hợp)
- Repeater (Bộ chuyển tiếp)
- Hub (Concentrator - Bộ tập trung)
- Bridge (Cầu nối)
- Switch (Bộ chuyển mạch)
- Router (Bộ định tuyến)
- Gateway (Cổng nối)
- Thiết bị mạng không dây
- Thiết bị hỗ trợ thi công mạng

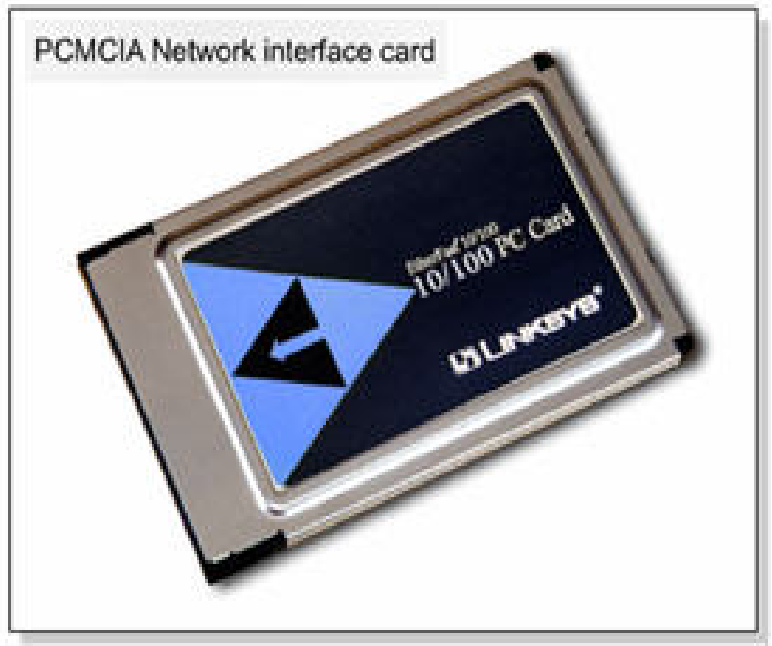
Lab center

Card mạng (NIC)

- Kết nối giữa máy tính và cáp mạng để phát hoặc nhận dữ liệu với các máy tính khác thông qua mạng.
- Kiểm soát luồng dữ liệu giữa máy tính và hệ thống cáp.

Card mạng (NIC)



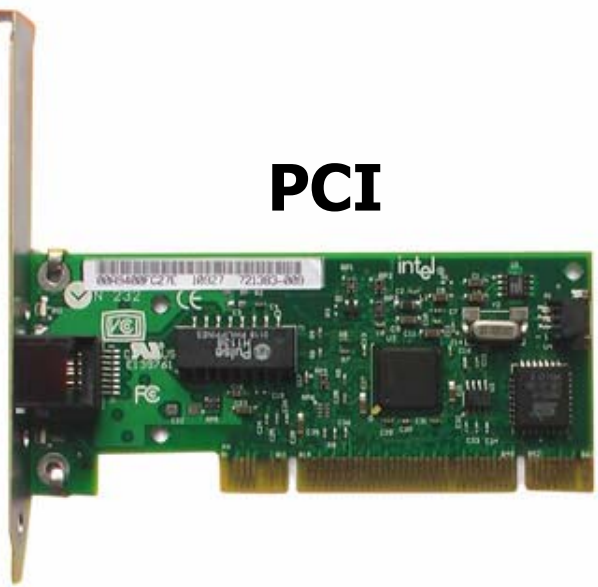


Khi chọn card mạng, cần chú ý các yếu tố:

- Các giao thức Ethernet, Token Ring hay FDDI.
- Môi trường cáp xoắn đôi, cáp đồng trục, không dây hay cáp quang.
- Loại bus PCI hay ISA.

Card mạng (NIC)

PCI

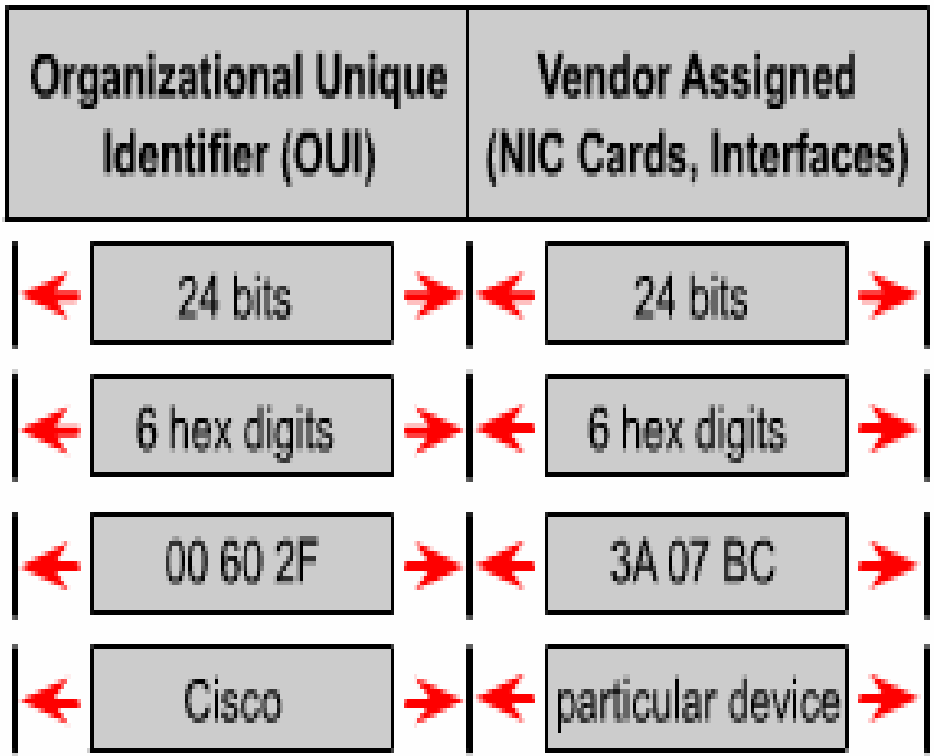


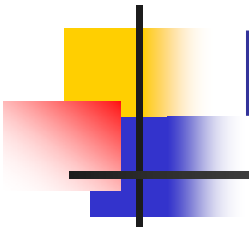
ISA

- Card ISA 8 bits hoặc 16 bits trong khi card PCI 32 bits.
- Tốc độ bus mặc định của slot ISA là 8,33MHz (băng thông 8,33MB/s) và slot PCI là 33,33MHz (băng thông 133,33MB/s).
- Card ISA phải cấu hình cứng bằng các jumper, card PCI có thể cấu hình bằng phần mềm. center

Card mạng (NIC)

- Mỗi NIC có một mã duy nhất gọi là địa chỉ MAC (Media Access Control).
- MAC address có 6 byte, 3 byte đầu là mã số nhà sản xuất, 3 byte sau là số serial của card.

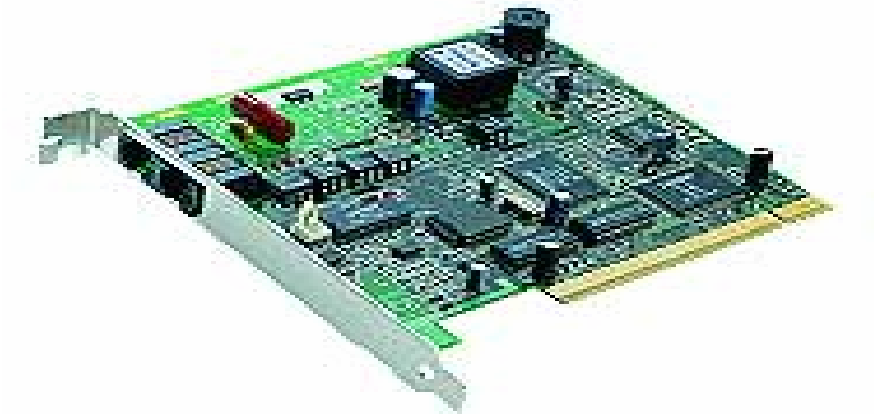




Modem

- Là tên viết tắt của hai từ điều chế (MOdulation) và giải điều chế (DEModulation).
- Điều chế tín hiệu số (Digital) sang tín hiệu tương tự (Analog) để gởi theo đường điện thoại và ngược lại.
- Có 2 loại là modem gắn trong (Internal) và modem gắn ngoài (External).

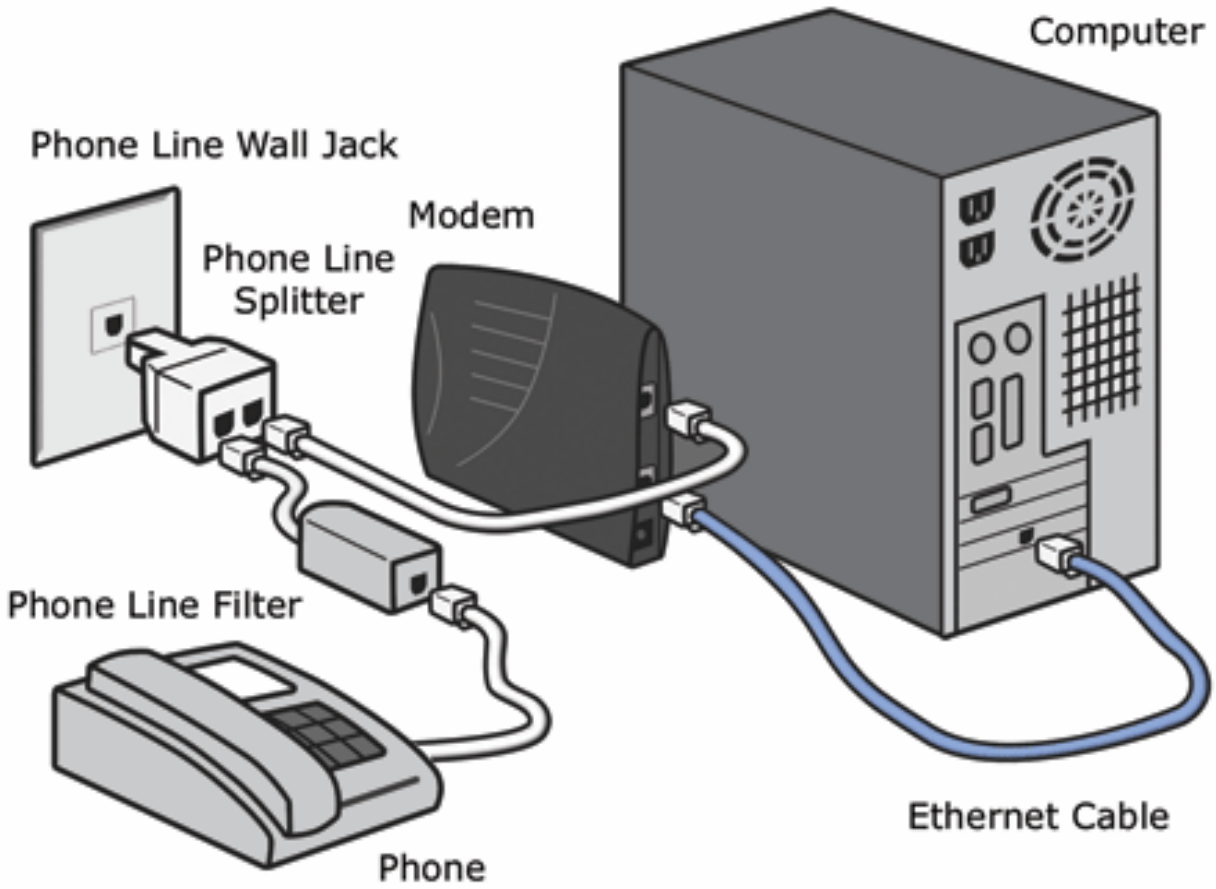
Modem



Modem trong

Modem ngoài

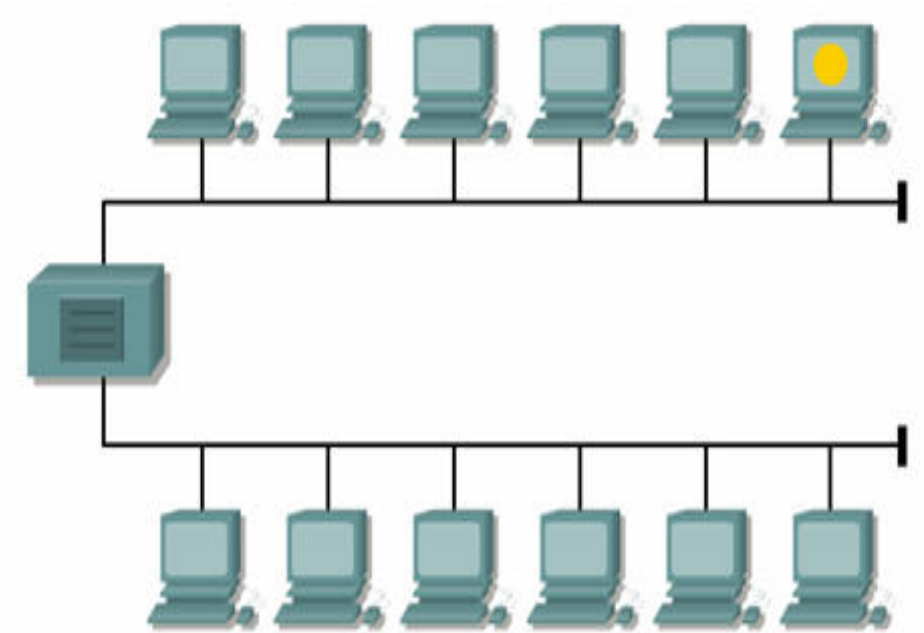
Modem


Computer
Phone Line Wall Jack
Modem
Phone Line
Splitter
Phone Line Filter
Phone
Ethernet Cable

Repeater (bộ chuyển tiếp)

- Khuếch đại, phục hồi các tín hiệu đã bị suy thoái do tổn thất năng lượng trong khi truyền.
- Cho phép mở rộng mạng vượt xa chiều dài giới hạn của một môi trường truyền.
- Chỉ được dùng nối hai mạng có cùng giao thức truyền thông.
- Hoạt động ở lớp Physical.

Repeater (bộ chuyển tiếp)

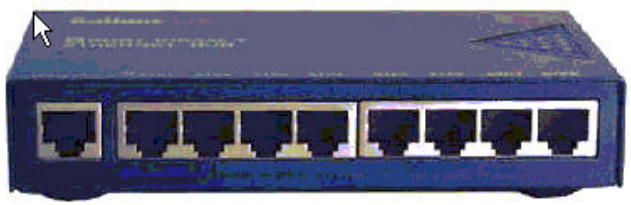


Hub (bộ tập trung)

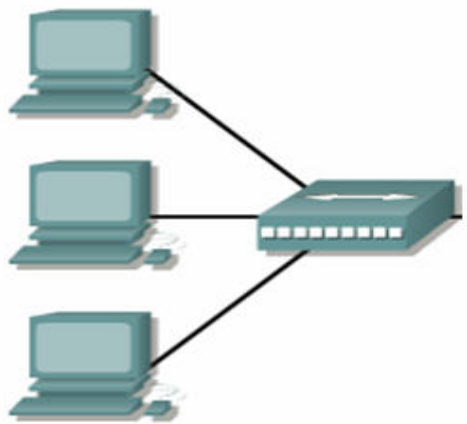
- Chức năng như Repeater nhưng mở rộng hơn với nhiều đầu cắm các đầu cáp mạng.
- Tạo ra điểm kết nối tập trung để nối mạng theo kiểu hình sao.
- Tín hiệu được phân phối đến tất cả các kết nối.
- Có 3 loại Hub: thụ động, chủ động, thông minh.

Hub (bộ tập trung)

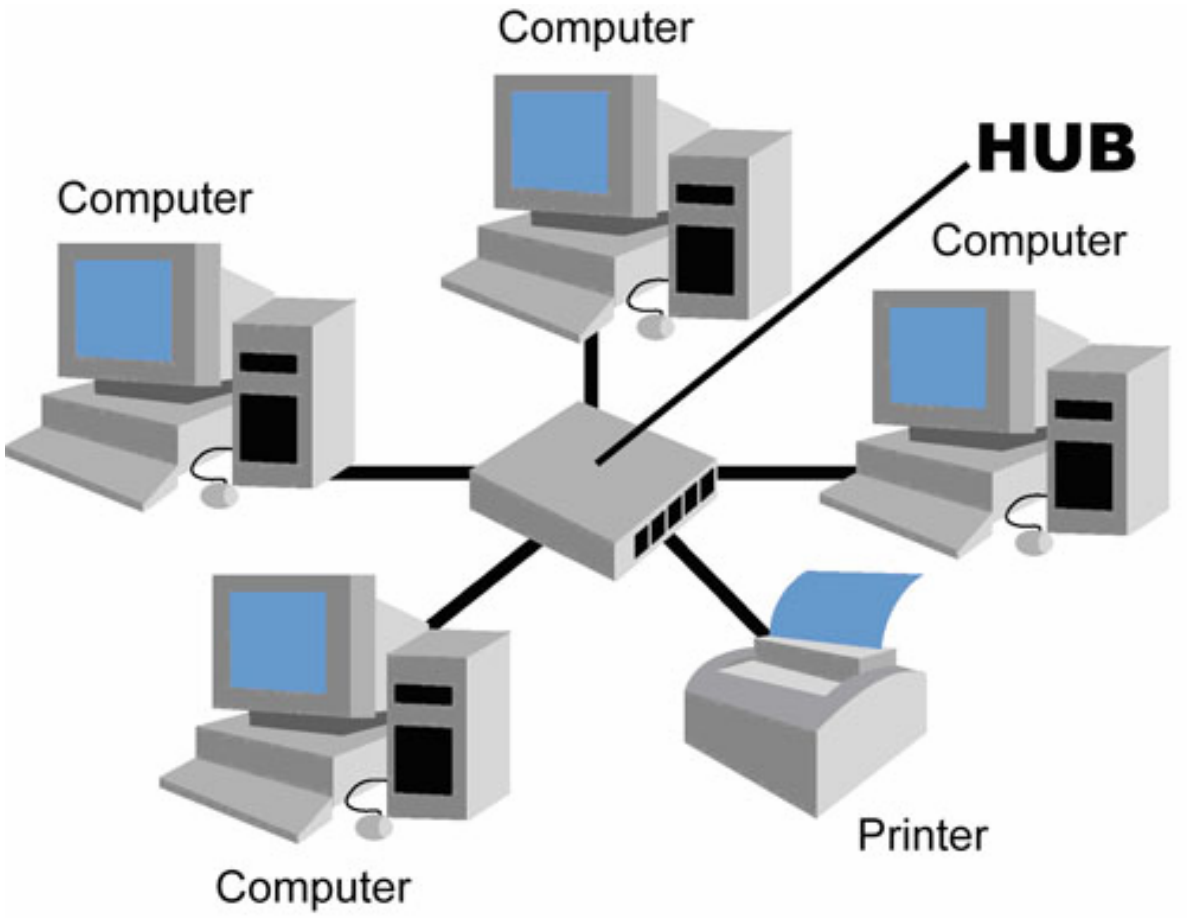
- Hub thụ động (Passive Hub): chỉ đảm bảo chức năng kết nối, không xử lý lại tín hiệu.
- Hub chủ động (Active Hub): có khả năng khuếch đại tín hiệu để chống suy hao.
- Hub thông minh (Intelligent Hub): là Hub chủ động nhưng có thêm khả năng tạo ra các gói tin thông báo hoạt động của mình giúp cho việc quản trị mạng dễ dàng hơn.



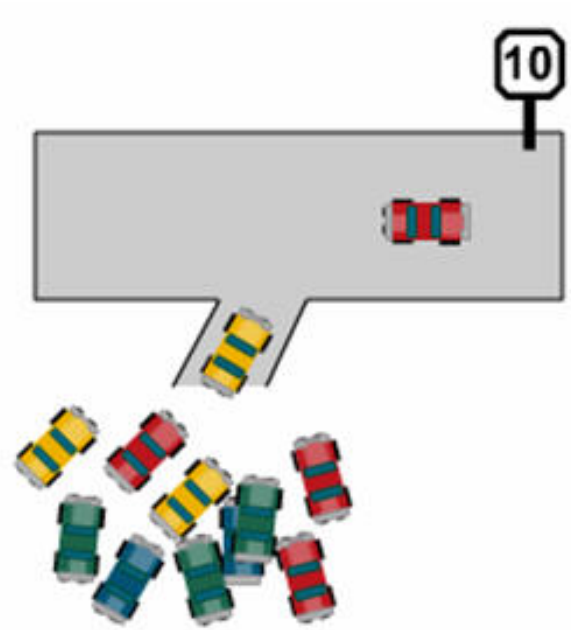
HUB



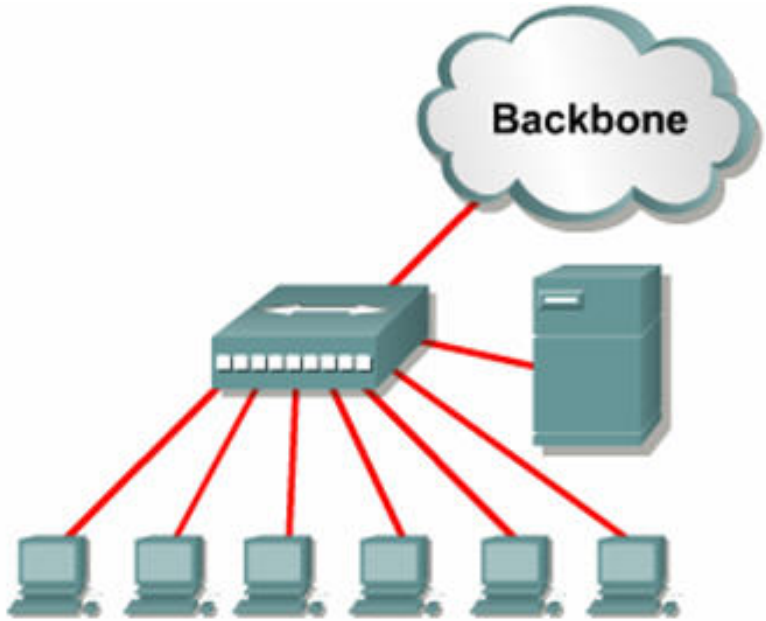
Hub (bộ tập trung)



Hub (bộ tập trung)



One device sending at a time

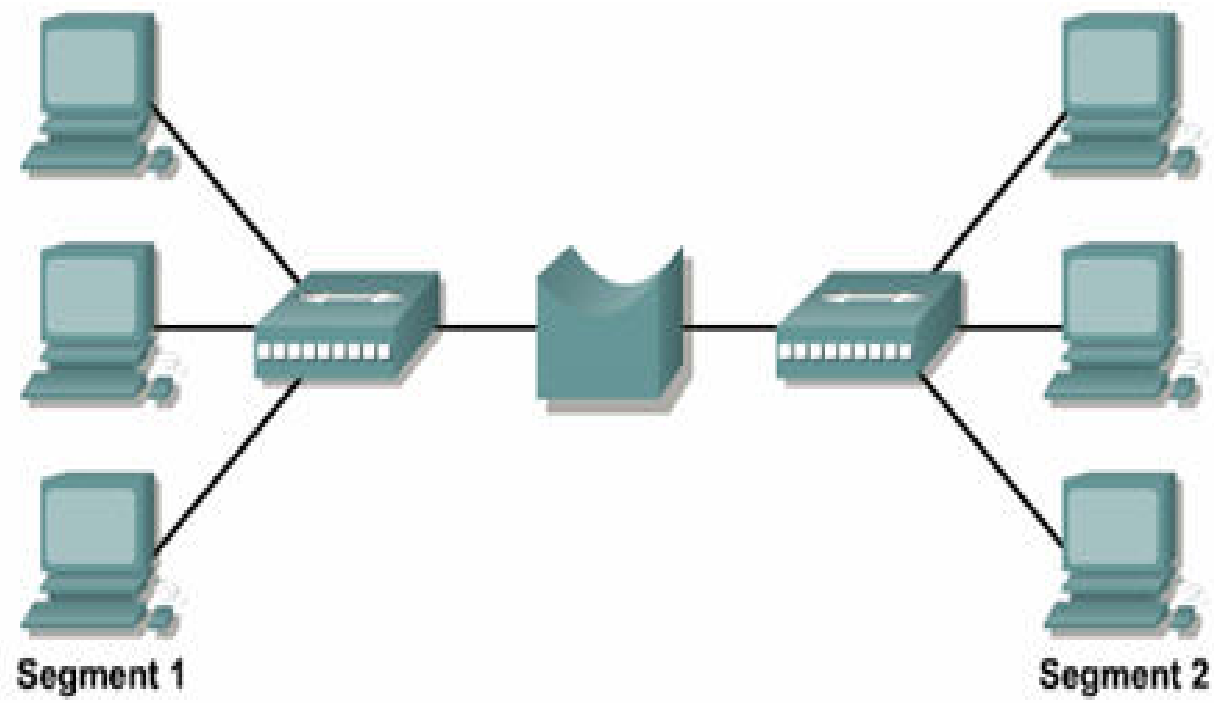


Each node shares 10 Mbps

Bridge (cầu nối)

- Dùng để nối 2 mạng có giao thức giống hoặc khác nhau.
- Chia mạng thành nhiều phân đoạn nhằm giảm lưu lượng trên mạng.
- Hoạt động ở lớp Data Link với 2 chức năng chính là lọc và chuyển vận.
- Dựa trên bảng địa chỉ MAC lưu trữ, Brigde kiểm tra các gói tin và xử lý chúng trước khi có quyết định chuyển đi hay không.

Bridge

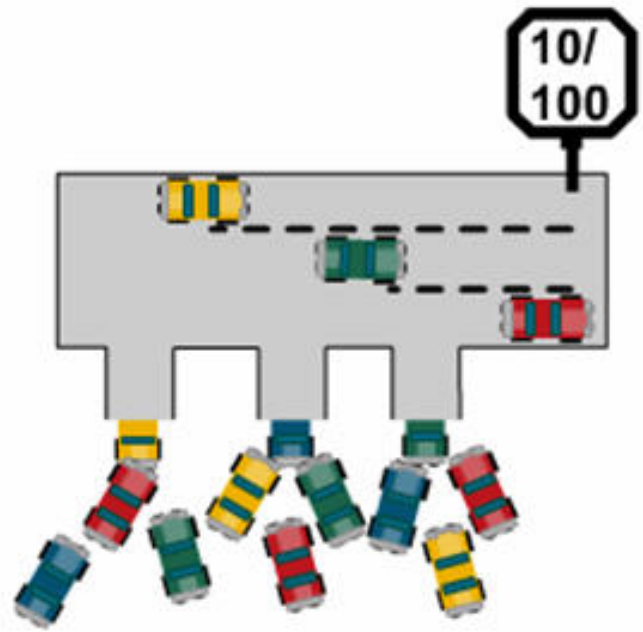


Switch (bộ chuyển mạch)

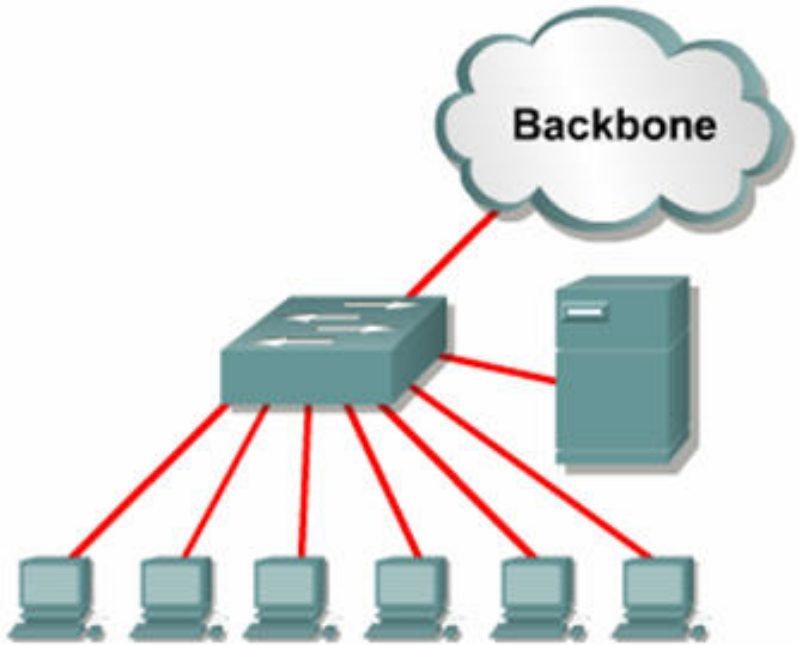
- Là thiết bị giống Bridge và Hub cộng lại nhưng thông minh hơn.
- Có khả năng chỉ chuyển dữ liệu đến đúng kết nối thực sự cần dữ liệu này làm giảm đụng độ trên mạng.
- Dùng để phân đoạn mạng trong các mạng cục bộ lớn (VLAN).
- Hoạt động ở lớp Data Link.

Switch (bộ chuyển mạch)

Switch (bộ chuyển mạch)



Multiple devices sending at the same time

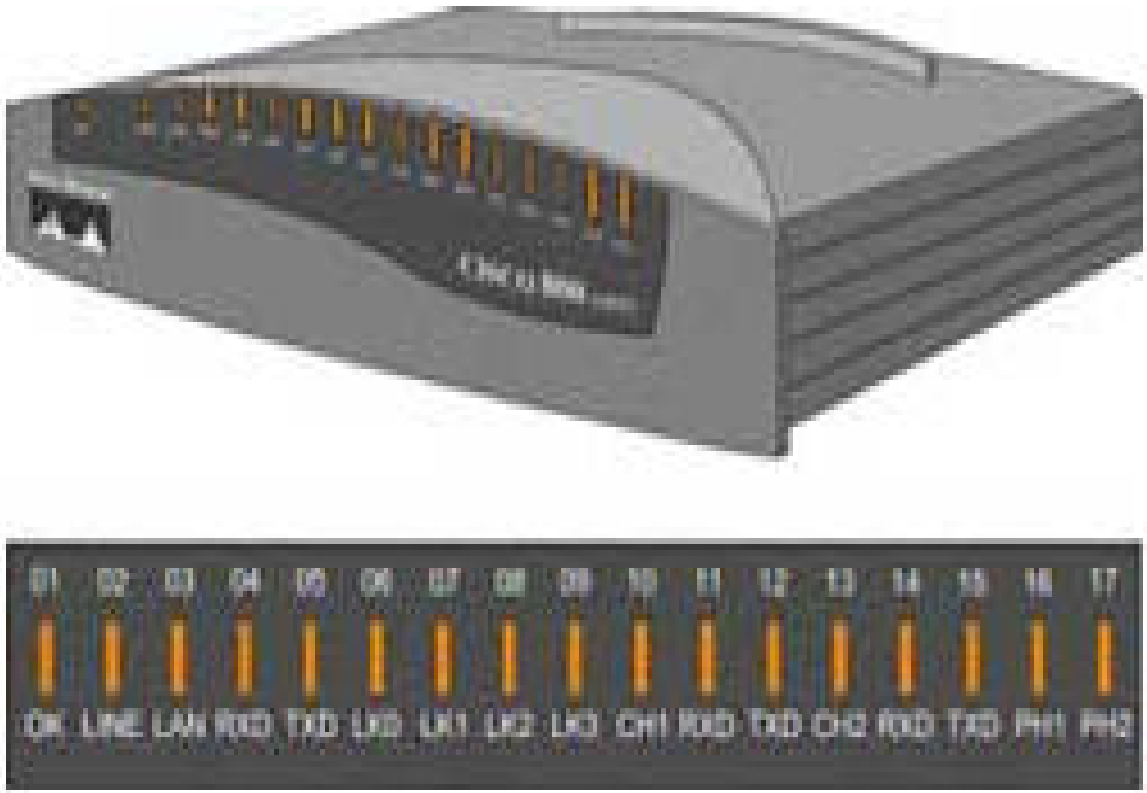


Each node has 10/100 Mbps

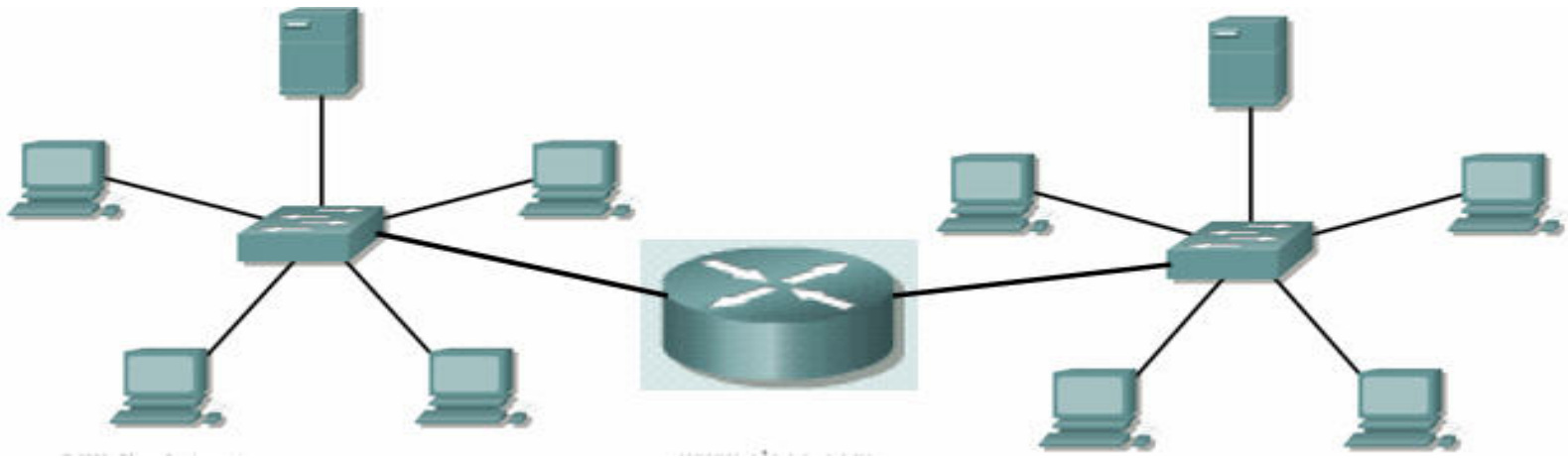
Router (Bộ định tuyến)

- Dùng để ghép nối các mạng cục bộ lại với nhau thành mạng rộng.
- Lựa chọn đường đi tốt nhất cho các gói tin hướng ra mạng bên ngoài.
- Hoạt động chủ yếu ở lớp Network.
- Có 2 phương thức định tuyến chính:
  - Định tuyến tĩnh: cấu hình các đường cố định và cài đặt các đường đi này vào bảng định tuyến.
  - Định tuyến động:
    - Vectơ khoảng cách: RIP, IGRP, EIGRP, BGP
    - Trạng thái đường liên kết: OSPF

Router (Bộ định tuyến)



Router (Bộ định tuyến)



Gateway (Proxy - cổng nối)

- Thường dùng để kết nối các mạng không thuần nhất, chủ yếu là mạng LAN với mạng lớn bên ngoài chứ không dùng kết nối LAN – LAN.
- Kiểm soát luồng dữ liệu ra vào mạng.
- Hoạt động phức tạp và chậm hơn Router.

Thiết bị mạng không dây

- Các chuẩn thông dụng là:
  - 802.11: tốc độ 1-2 Mbps
  - 802.11b: tốc độ 11 Mbps
  - 802.11a: tương tự 802.11b
- Mạng không dây gồm 2 thiết bị:
  - Các node (máy tính) có gắn wireless NIC.
  - Access point (AC) đóng vai trò như một central hub cho WLAN.

Thiết bị mạng không dây

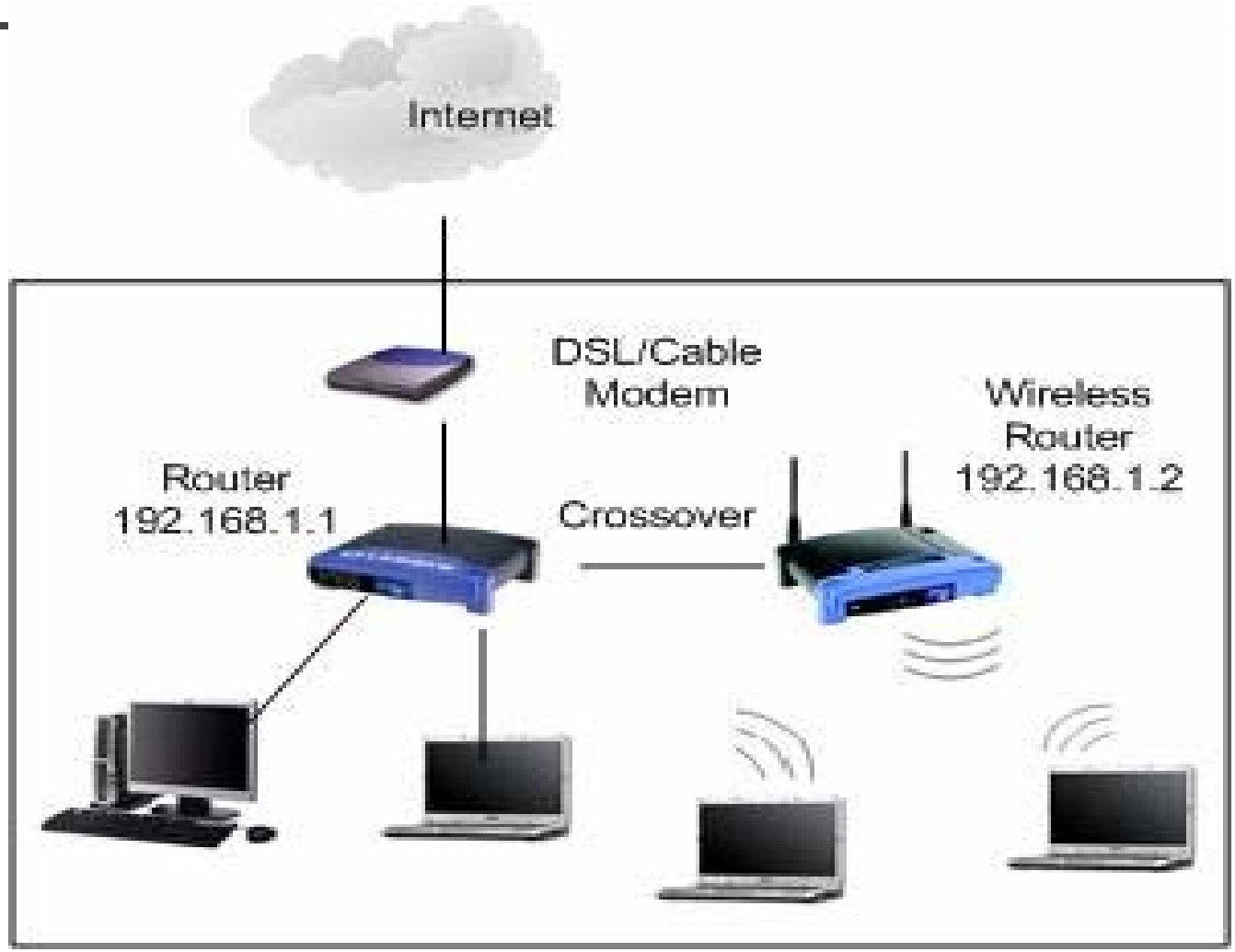
Linksys WRT54GS Wireless-G Broadband Router with SpeedBooster.

Thiết bị mạng không dây

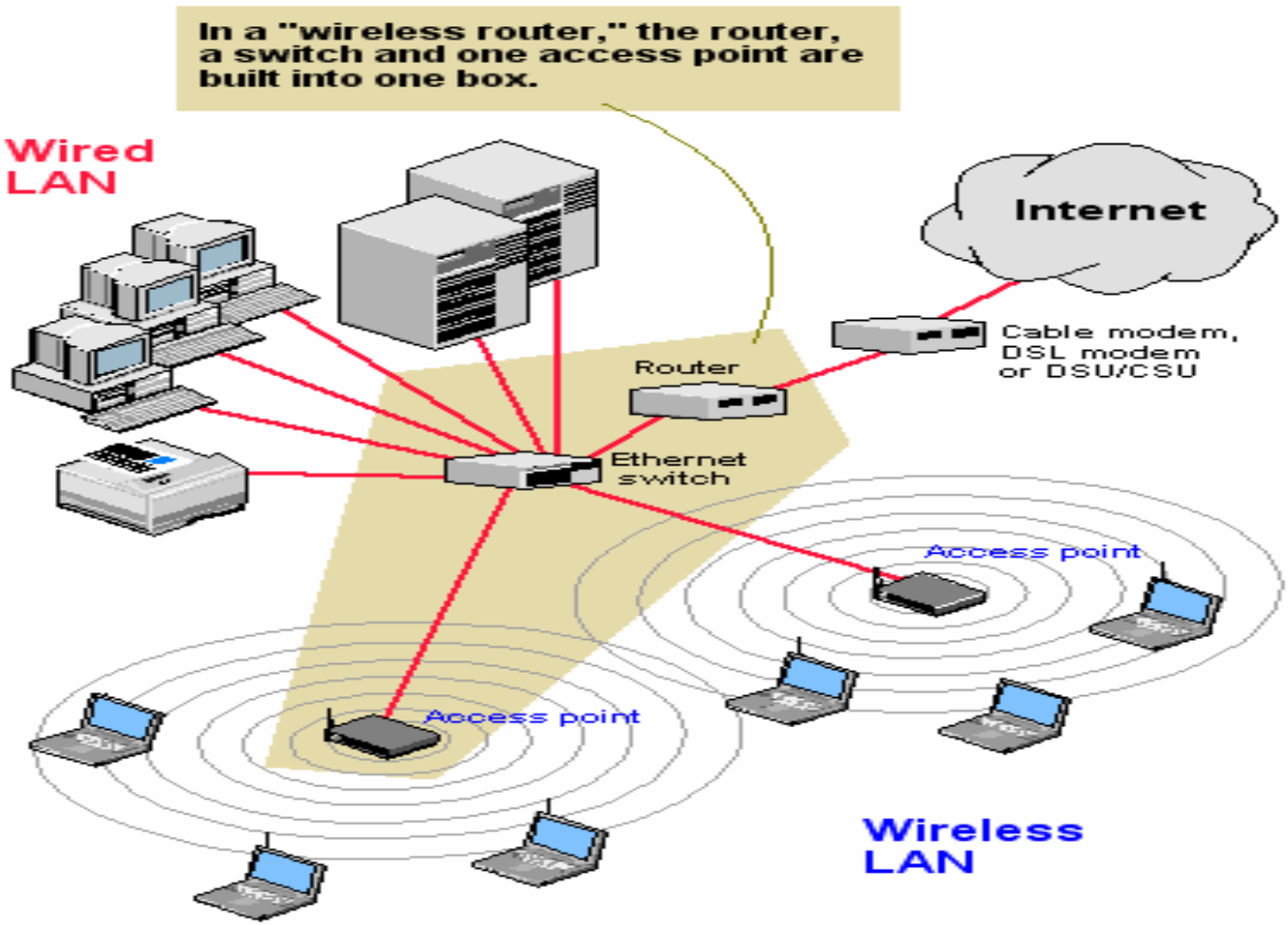
Linksys WMP54GS
Wireless-G PCI Adapter

Linksys WPC54GS
Wireless-G Notebook
Adapter

Thiết bị mạng không dây



Thiết bị mạng không dây



Thiết bị hỗ trợ thi công mạng

Thiết bị kiểm tra cable

Thiết bị hỗ trợ thi công mạng

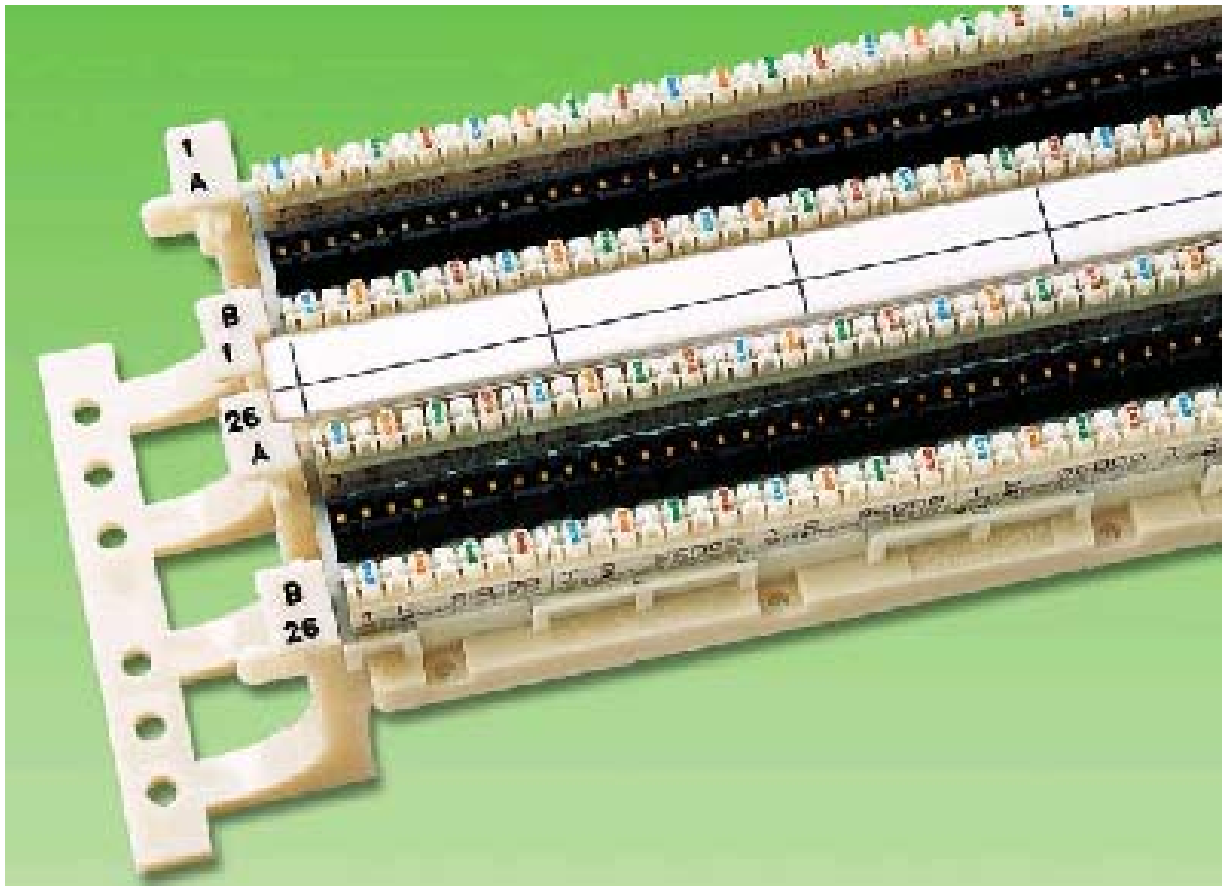
Crimp down the wires

Thiết bị hỗ trợ thi công mạng

Patch Panel

Thiết bị hỗ trợ thi công mạng

Wiring block



ROUTER (bộ định tuyến)

- Chức năng và phân loại Router
- Wan và Router
- Các thành phần của Router
- Khởi động Router
- Một số lệnh cơ bản
- Cấu hình cho Router

Chức năng và phân loại
Chức năng

- Hoạt động ở tầng Network.
- Phân cách các mạng thành các segment riêng biệt:
  - Giảm đụng độ
  - Giảm broadcast
  - Bảo mật
- Kết nối các mạng máy tính ở cách xa nhau qua các đường truyền thông như điện thoại, ISDN, T1, X25…

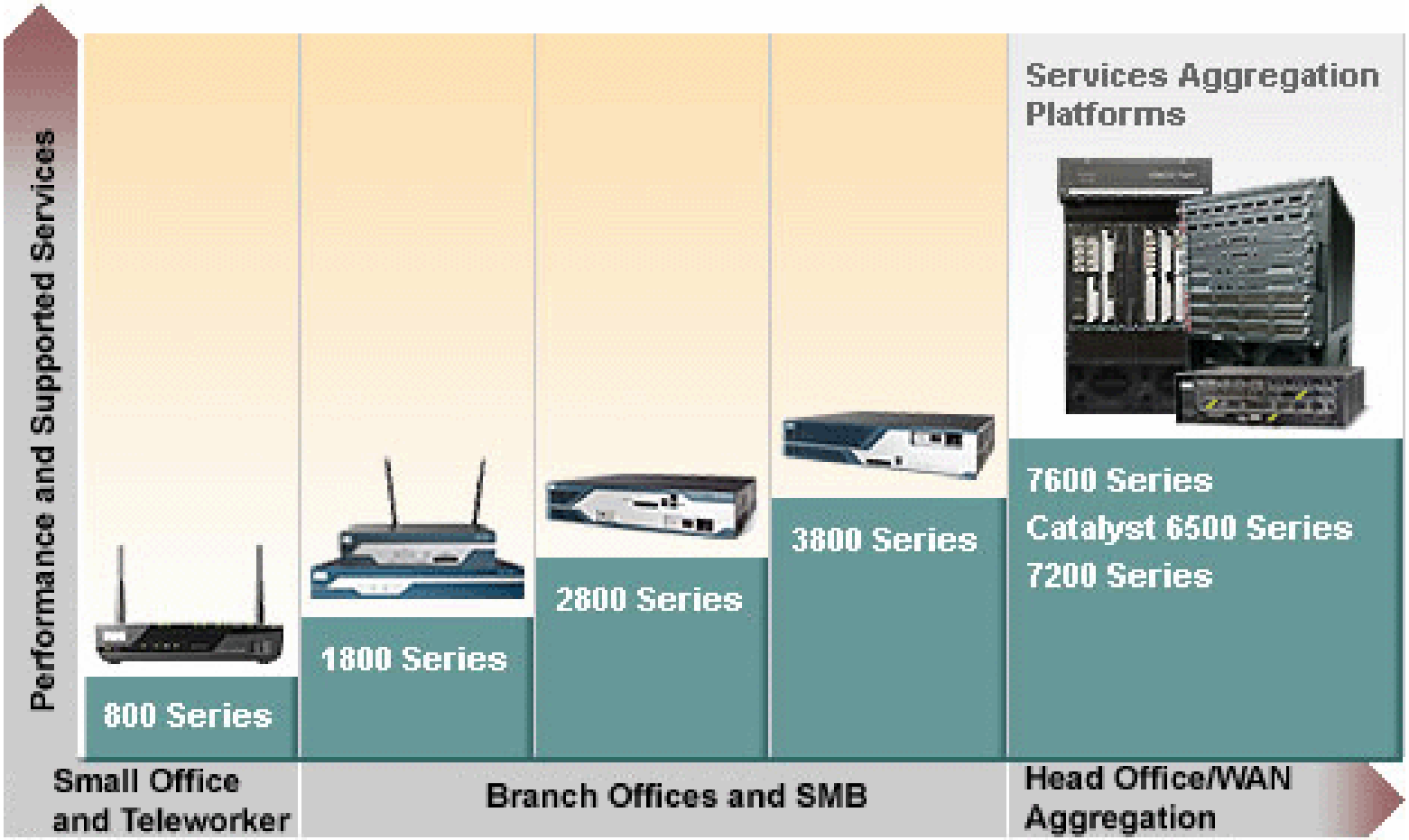
Chức năng và phân loại

Phân loại

Phân loại router của Cisco

Remote access	Low-end router	Fix configuration router			Modular router
		Multi protocol router	Multiport serial router	Router /hub	
Cisco 2509 Cisco 2510 Cisco 2511 Cisco 2512 AS5xxx Cisco 500-CS	Cisco 7xx Cisco 8xx Cisco 100x	Cisco 2501 Cisco 2502 Cisco 2503 Cisco 2504 Cisco 2513 Cisco 2514 Cisco 2515	Cisco 2520 Cisco 2521 Cisco 2522 Cisco 2523	Cisco 2505 Cisco 2506 Cisco 2507 Cisco 2508 Cisco 2516 Cisco 2518	Cisco 2524 Cisco 2525 Cisco 160x Cisco 17xx Cisco 26xx Cisco 36xx Cisco 4xxx Cisco 7xxx

Chức năng và phân loại
Series Cisco Router



Chức năng và phân loại

Series Cisco Router - **Cisco 800 Series Router**

Cisco 800 Series là giải pháp lý tưởng cho các kết nối Internet an toàn và các kết nối mạng cho các văn phòng nhỏ hoặc những người làm việc từ xa (teleworkers).

Chức năng và phân loại

Series Cisco Router - **Cisco 800 Series Router**

• Bên cạnh tính dễ triển khai và các tính năng quản lý tập trung, các thiết bị định tuyến truy nhập thuộc họ Cisco 800 với các dịch vụ tích hợp cung cấp những tính năng như:
• An ninh mạng tích hợp
• Một kết nối mạng WAN, với đa lựa chọn
• Bốn cổng chuyển mạch 10/100 Mbps được quản lý
• Có tới 10 đường hầm VPN
• Hỗ trợ các tiêu chuẩn mạng LAN vô tuyến 802.11b và 802.11g

Chức năng và phân loại

Series Cisco Router - **Cisco 800 Series Router**

Models Comparison: Integrated Services Routers					
Model	WAN Interface	VPN	3G Wireless WAN	802.11b/g wireless	802.11n wireless (b/g compatible)
815	Cable, DOCSIS 2.0	Yes	No	No	No
851	10/100 Mbps Fast Ethernet	Up to 5 tunnels	No	851W	No
857	ADSL (asymmetric DSL)	Up to 5 tunnels	No	857W	No
861	10/100 Mbps Fast Ethernet	Up to 5 tunnels	No	861W	861W
871	10/100 Mbps Fast Ethernet	Up to 10 tunnels	No	871W	No
876	ADSL (asymmetric DSL) over ISDN	Up to 10 tunnels	No	876W	No
877	ADSL (asymmetric DSL)	Up to 10 tunnels	No	877W	No
878	G.SHDSL (Symmetrical High-Data-Rate DSL)	Up to 10 tunnels	No	878W	No
881	10/100 Mbps Fast Ethernet	Up to 20 tunnels	Yes (excluding SRST model)		An option on all 881 SKUs
888	G.SHDSL (Symmetrical High-Data-Rate DSL)	Up to 20 tunnels	No		An option on all 888 SKUs

Chức năng và phân loại

Series Cisco Router - **Cisco 1800 Series Routers**

- An ninh mạng được tích hợp.
- Hệ thống quản lý thiết bị an ninh mạng và thiết bị định tuyến (SDM) để đơn giản hóa tác vụ quản lý.
- Có tới 2 cổng định tuyến tích hợp ở tốc độ 10/100 Mbps.
- Hỗ trợ các tiêu chuẩn mạng LAN không dây 802.11a/b/g

Chức năng và phân loại

Series Cisco Router - **Cisco 1800 Series Routers**

- Các dòng thiết bị cố định (1801, 1802, 1803, 1811, 1812):
  - Tốc độ truy nhập lên đến tốc độ băng rộng
  - 8 cổng chuyển mạch tích hợp tốc độ 10/100 Mbps với tùy chọn về cấp nguồn qua mạng Ethernet (PoE), để cung cấp nguồn DC đến các thiết bị mạng như các máy điện thoại IP
  - Lên tới 50 đường hầm VPN
- Thiết bị dòng 1841 có cấu trúc mô đun, cùng với:
  - Tốc độ có thể lên tới tốc độ T1/E1
  - 4 cổng chuyển mạch tích hợp tốc độ 10/100 Mbps
  - 800 đường hầm VPN

Chức năng và phân loại

Series Cisco Router - **Cisco 1800 Series Routers**

Models Comparison					
Model	DSL WAN Port	10/100 FE WAN Ports	8-Port Managed Switch	USB 2.0 Ports	802.11 a/b/g Wireless Model
1801 Product page Data sheet	ADSL over POTS	1	Yes	0	Yes
1802 Product page Data Sheet	ADSL over ISDN	1	Yes	0	Yes
1803 Product page Data sheet	G.SHDSL (4-wire)	1	Yes	0	Yes
1811 Product page Data sheet	-	2	Yes	2	Yes
1812 Product page Data sheet	-	2	Yes	2	Yes
1841 Product page Data sheet	ADSL, G.SHDSL VWICS	2	4-port single-wide 10/100 BASE-T with HWIC-4ESW	0 (1 USB 1.1 port)	Yes (with HWIC-AP)
1861 Product page Data sheet	HWICs: ADSL, G.SHDSL, 3G, T1/E1, Serial	2	Yes	none	-

Chức năng và phân loại

Series Cisco Router - **Cisco 2800 Series Routers**

- An ninh mạng tích hợp
- Một thiết bị có cấu trúc mô đun với một dải rất rộng các tùy chọn về giao diện
- Có tới 2 cổng định tuyến tích hợp tốc độ 10/100/1000 Mbps
- Có tới 64 cổng chuyển mạch tốc độ 10/100 Mbps với tùy chọn về cấp nguồn qua mạng Ethernet (PoE), để cấp nguồn DC đến các thiết bị mạng như là máy điện thoại IP
- Có tới 1500 đường hầm VPN

Chức năng và phân loại

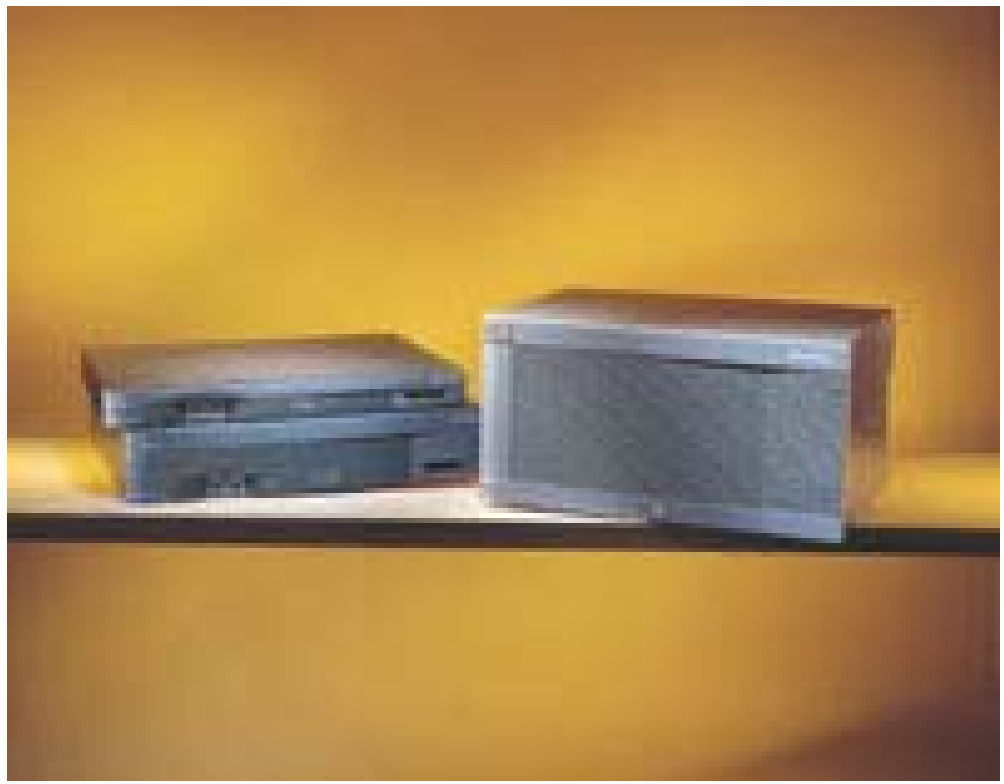
Series Cisco Router - **Cisco 2800 Series Routers**

Models Comparison						
Model	Onboard DSP Slots	Fixed LAN Ports	Optional Power over Ethernet	Slots for Interface Cards	Slots for Network Modules	Size
2801 Product page Data sheet	2	2 FE	120W	2 HWIC/WWIC/MIC/VIC 1 WWIC/MIC/VIC 1 VWIC/VIC (voice only)	0	1 RU
2811 Product page Data Sheet	2	2 FE	160W	4 HWIC	1 NME	1 RU
2821 Product page Data sheet	3	2 GE (10/100/1000)	240W	4 HWIC	1 NME or NME-X	2 RU
2851 Product page Data sheet	3	2 GE (10/100/1000)	360W	4 HWIC	1 NME, NMD, NME-X or NME-XD	2 RU

Chức năng và phân loại

Series Cisco Router - **Cisco 3600 Series Multiservice Platforms**

- Là dòng sản phẩm dạng modular, multiservice access platforms cho các văn phòng trung bình và lớn hoặc các ISP loại nhỏ.
- Có hơn 70 chọn lựa modular interfaces.
- Cisco 3600 cung cấp các giải pháp cho data, voice video, hybrid dial access, virtual private networks (VPNs), và multiprotocol data routing.



Chức năng và phân loại

Series Cisco Router - **Cisco 3700 Series Multiservice Access Routers**

- Cho phép các tính năng và module hoàn toàn mới và mạnh mẽ hơn, nhiều kết nối hơn.
- Khi sử dụng module 16- or 36-port EtherSwitch, Cisco 3700 Series trở thành một thiết bị tích hợp cả routing và low-density switching.
- Có thể hỗ trợ internal inline power cho các EtherSwitch ports, tạo nên một platform duy nhất cho giải pháp IP telephony.

Chức năng và phân loại

Series Cisco Router - **Cisco 3800 Series Routers**

- An ninh mạng tích hợp
- Có tới 2 cổng định tuyến tích hợp tốc độ 10/100/1000 Mbps
- Có tới 112 cổng chuyển mạch 10/100 Mbps với tùy chọn về cấp nguồn qua mạng Ethernet (PoE), để cấp nguồn DC đến các thiết bị mạng như máy điện thoại IP
- Có tới 2500 đường hầm VPN

Chức năng và phân loại

Series Cisco Router - **Cisco 7200 Series Routers**

Chức năng và phân loại

Series Cisco Router - **Cisco 7200 Series Routers**

- Gom lưu lượng băng rộng: lên tới 16,000 phiên PPP trên một khung máy
- Chuyển mạch nhãn đa giao thức (MPLS): Lựa chọn hàng đầu cho triển khai ở biên mạng của nhà cung cấp dịch vụ
- Mạng riêng ảo An ninh IP (IPsec): định cỡ tới 5000 đường hầm trêm một khung máy.
- Tích hợp thoại, dữ liệu và video.
- Thiết kế mô đun: diện tích đặt máy 3RU với một dải rộng các giao diện linh hoạt có tính mô đun (từ DS0 đến OC-3).
- Tính linh hoạt: hỗ trợ Fast Ethernet, Gigabit Ethernet, Packet trên nền SONET và nhiều tính năng khác.

Chức năng và phân loại

Series Cisco Router - **Cisco 7600 Series Routers**

Chức năng và phân loại

Series Cisco Router - **Cisco 7600 Series Routers**

Các tính năng quan trọng:

• Hiệu năng cao với tốc độ lên đến 720 Gbps trên một khung máy hoặc dung lượng 40 Gbps trên mỗi khe cắm

• Một lựa chọn về kích thước được xây dựng theo mục đích hoặc dành cho độ khả dụng cao

• Thiết kế I-Flex của Cisco: Một họ sản phẩm về bộ giao tiếp với cổng được chia sẻ (SPAs) và các bộ vi xử lý giao diện SPA (SIPs) với khả năng kiểm soát cảm nhận về các dịch vụ thoại, video và dữ liệu

• Kiểm soát tiếp nhận cuộc gọi Video tích hợp với cảm nhận về chất lượng hình ảnh sáng tạo dành cho cả phát thanh truyền hình quảng bá và video theo yêu cầu (VoD)

• Cổng dịch vụ thông minh, cung cấp số lượng thuê bao định cỡ và khả năng nhận biết ứng dụng với tính năng xác định đa chiều và các chính sách điều khiển

Chức năng và phân loại

Series Cisco Router - **Cisco 7600 Series Routers**

Các ứng dụng:

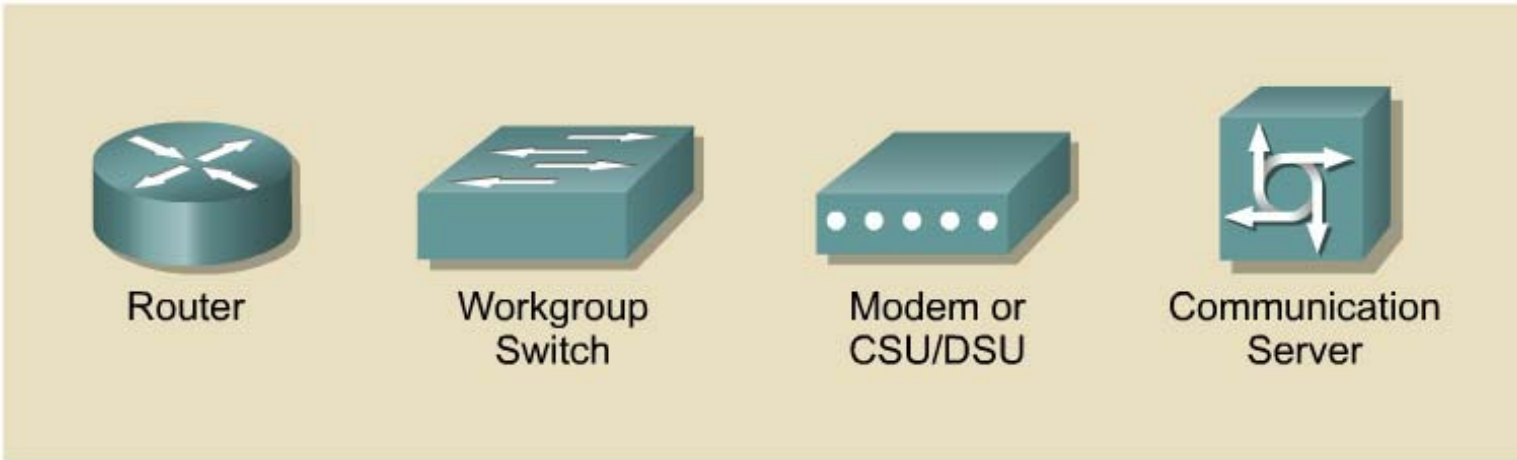
- Mạng Ethernet của nhà khai thác: gom lưu lượng từ các dịch vụ của doanh nghiệp và của người tiêu dùng
- Biên mạng dịch vụ Ethernet: các dịch vụ IP được cá nhân hóa
- Mạng vô tuyến hình lưới và hội tụ các dịch vụ di động
- Định tuyến biên mạng IP/MPLS của nhà cung cấp dịch vụ
- Gom lưu lượng mạng WAN doanh nghiệp
- Định tuyến mạng lõi trong trụ sở của doanh nghiệp

WAN và Router

Kết nối WAN

Distance Between Devices	Location of Hosts	Name
10m	Room	Local-area Network Classroom
100m	Building	Local-area Network School
1000m = 1km	Campus	Local-area Network University
10,000m = 10km	City	Metropolitan-area Network
100,000m = 100km	Country	Wide-area Network Cisco System, Inc.
1,000,000m = 1,000km	Continent	Wide-area Network Africa
10,000,000m = 10,000km	Planet	Wide-area Network Internet
100,000,000m = 100,000km	Earth-Moon Systems	Wide-area Network Earth and Artificial Satellites

WAN và Router
Kết nối WAN



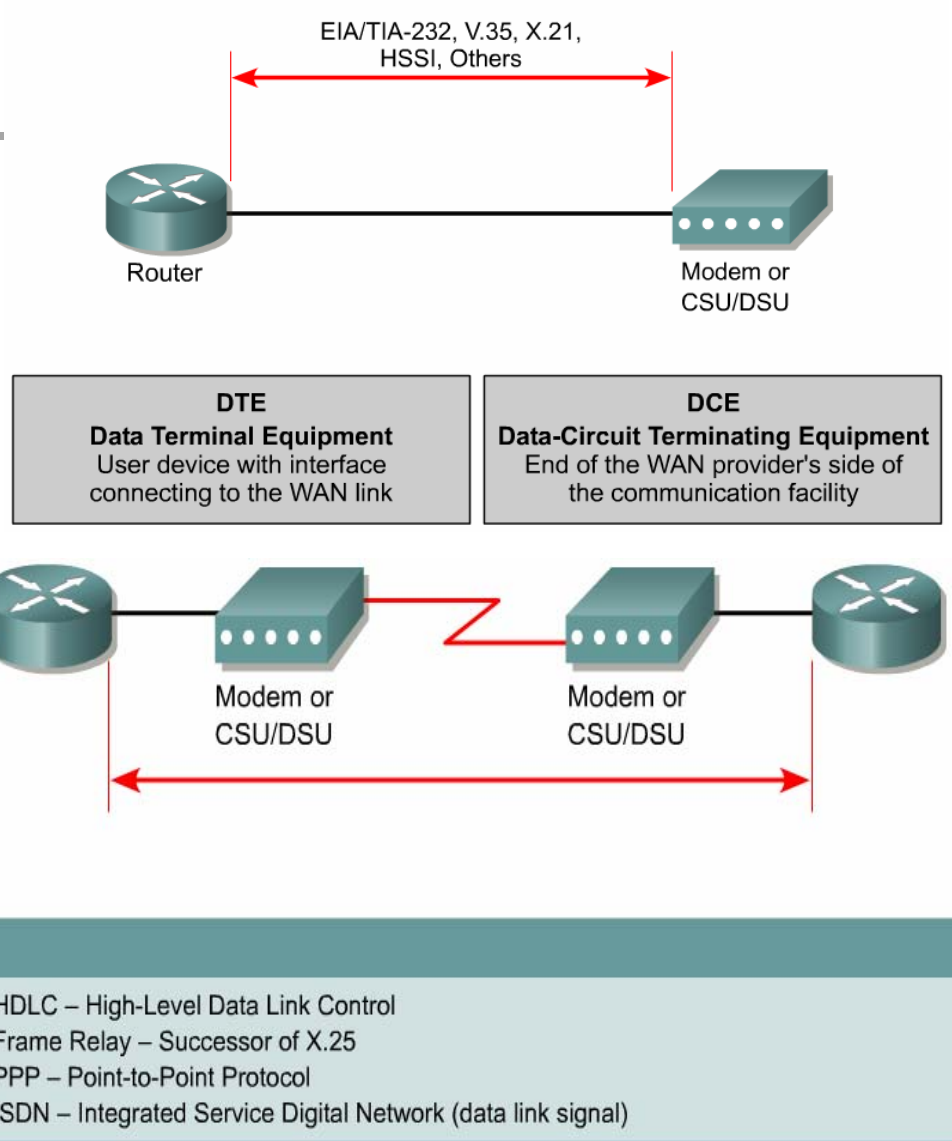
WANs are designed to:

- Operate over a large geographic area
- Allow access over serial interfaces operating at lower speeds
- Provide full-time and part-time connectivity

WAN và Router

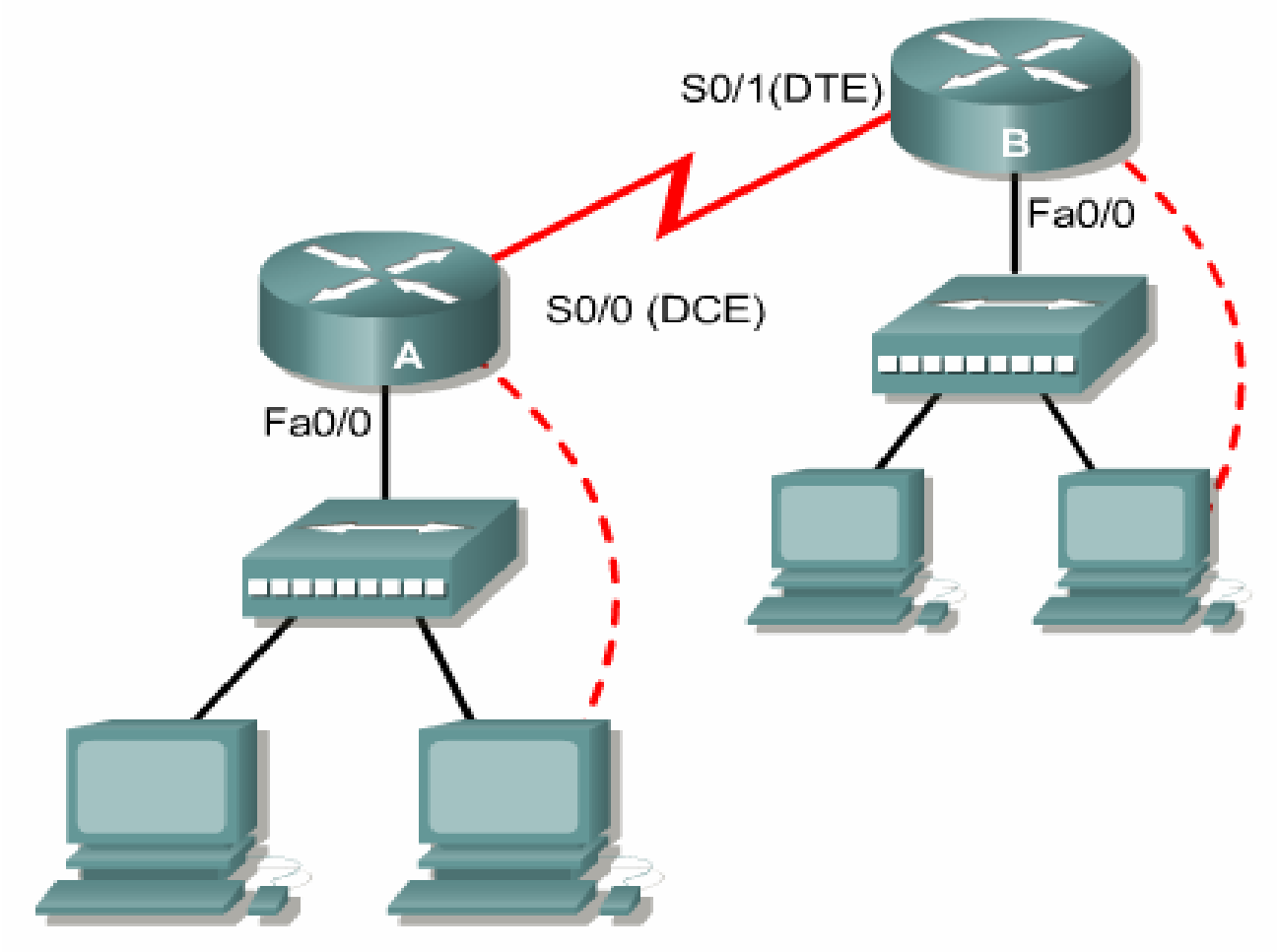
Kết nối WAN

- **DTE** (Data Terminal Equipment): thiết bị dữ liệu đầu cuối.
- **DCE** (Data Circuit-terminal Equipment): thiết bị đầu cuối mạch dữ liệu, thường ở phía nhà cung cấp dịch vụ, có thể là modem hoặc CSU/DSU.



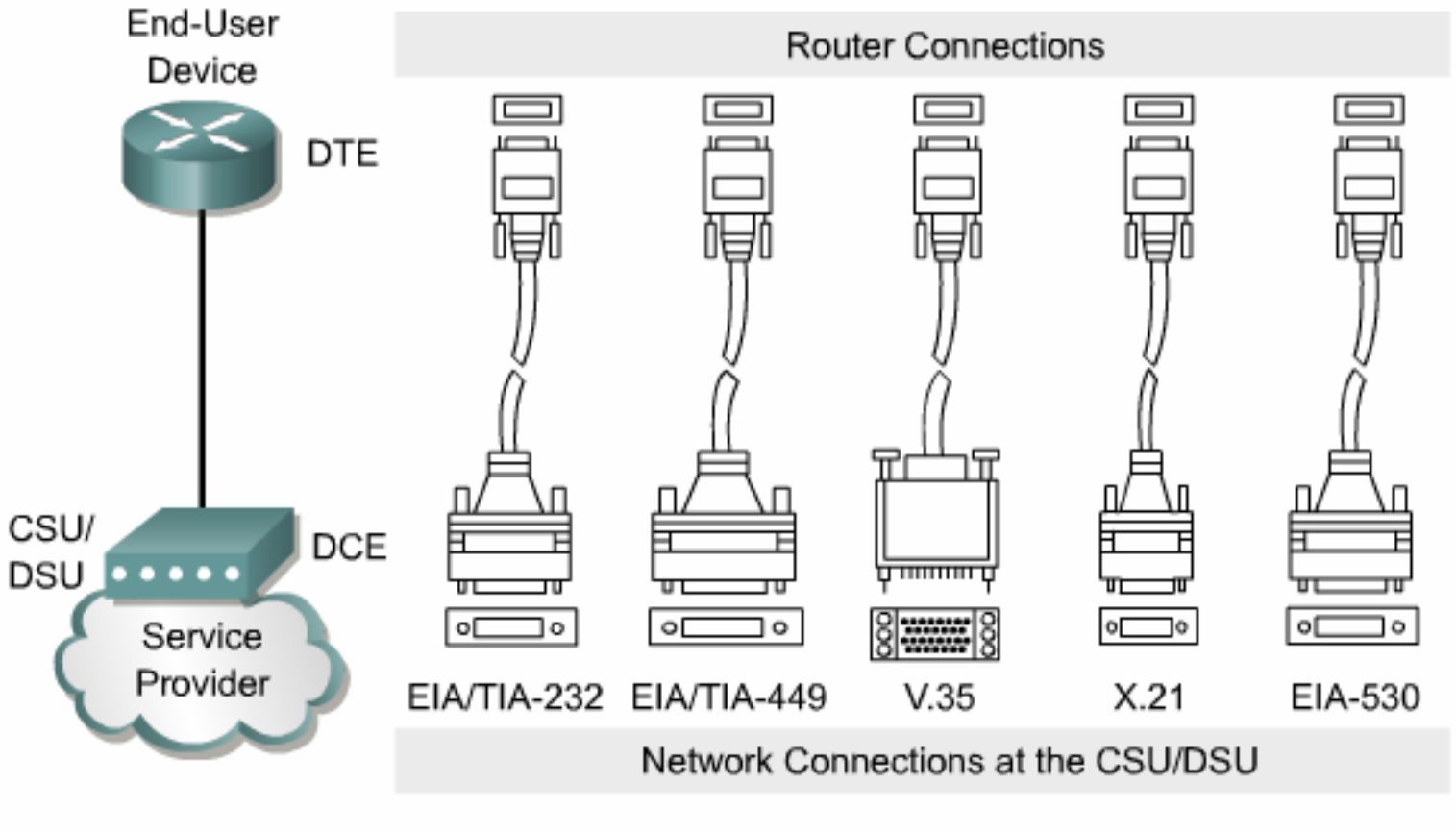
WAN và Router

Kết nối WAN



WAN và Router

Các loại đầu cáp kết nối trong mạng WAN

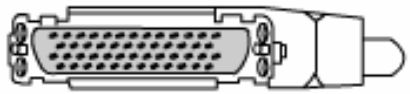


WAN và Router

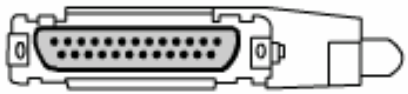
Các loại đầu cáp DCE

EIA/TIA-232 Male

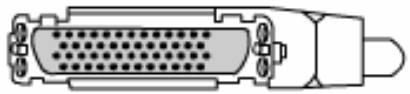
v.35 Male



EIA/TIA-232 Female

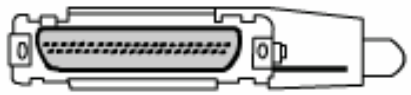


v.35 Female



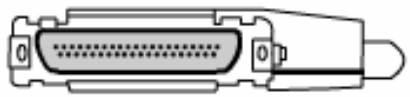
X.21 Male

EIA/TIA - 449 Male



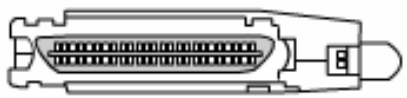
X.21 Female

EIA/TIA - 449 Female



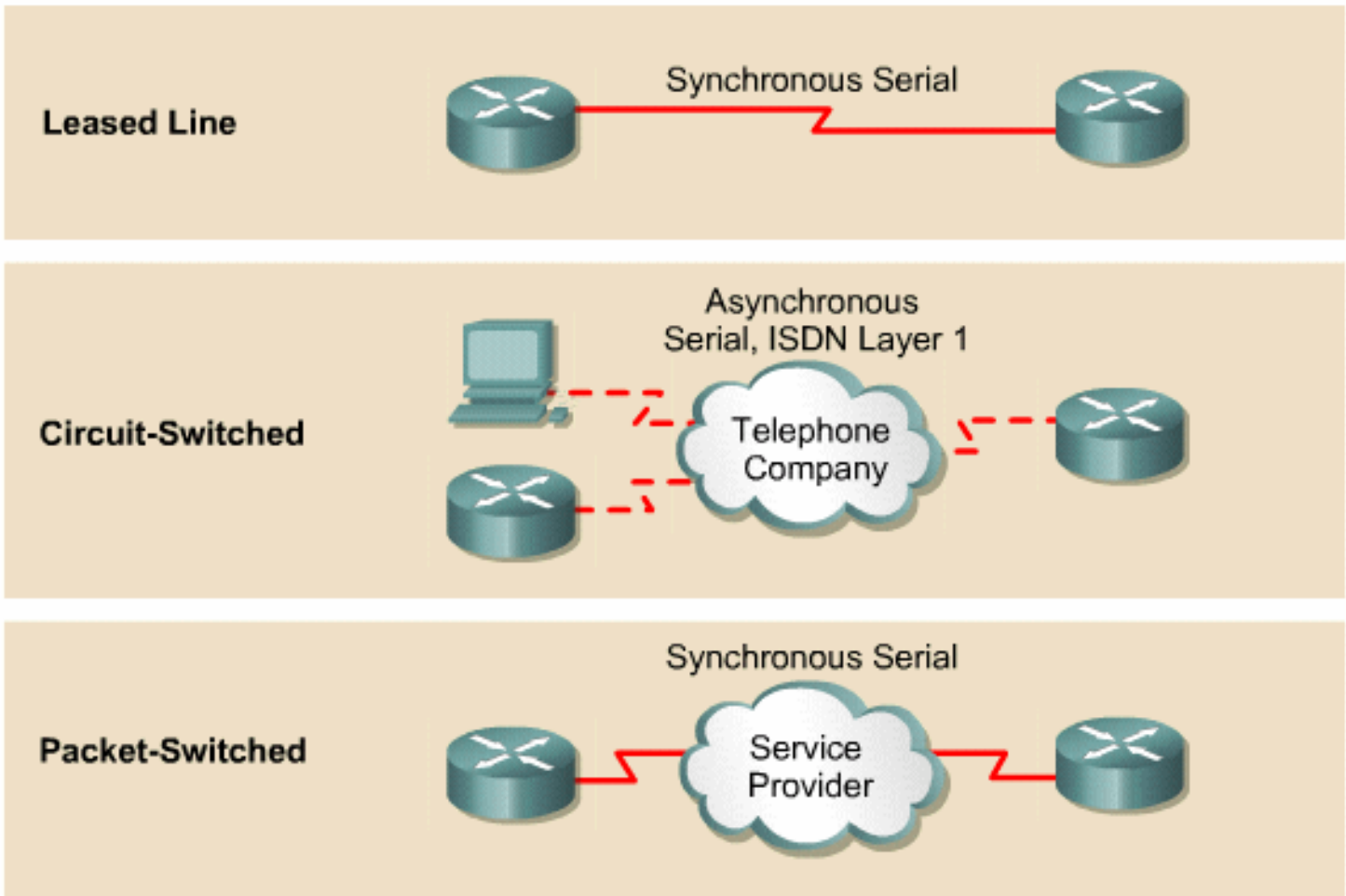
EIA-530 Male

EIA-613 HSSI Male



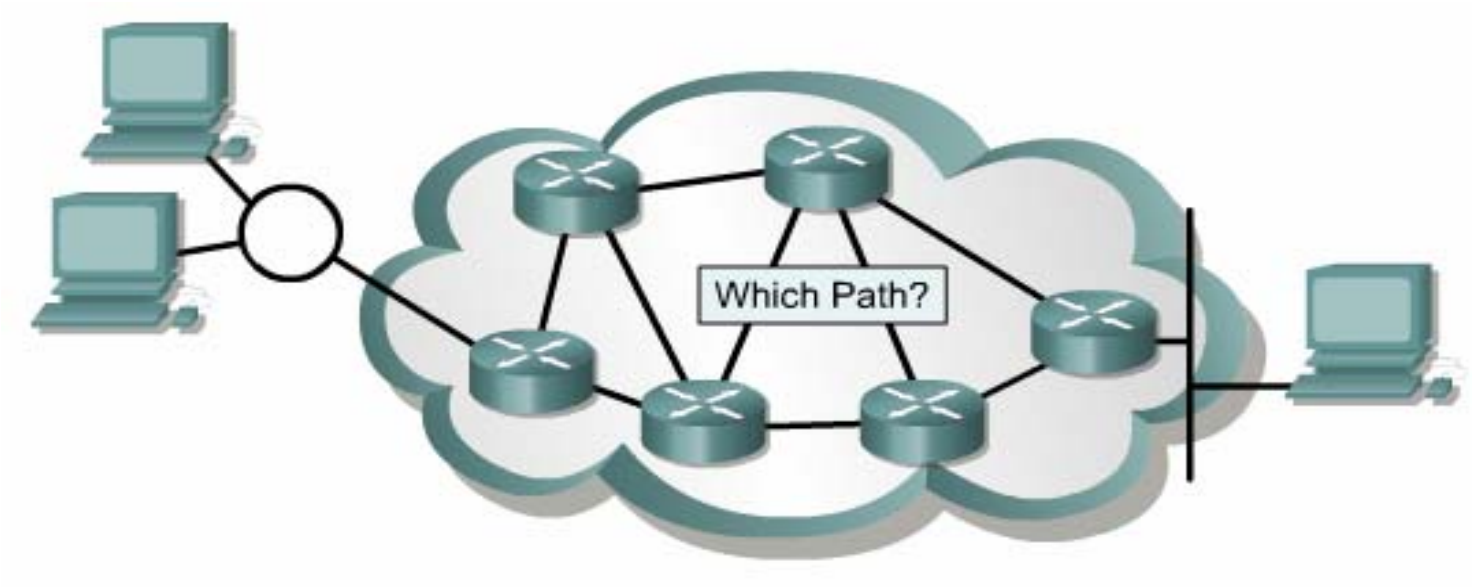
WAN và Router

Kiểu kết nối WAN



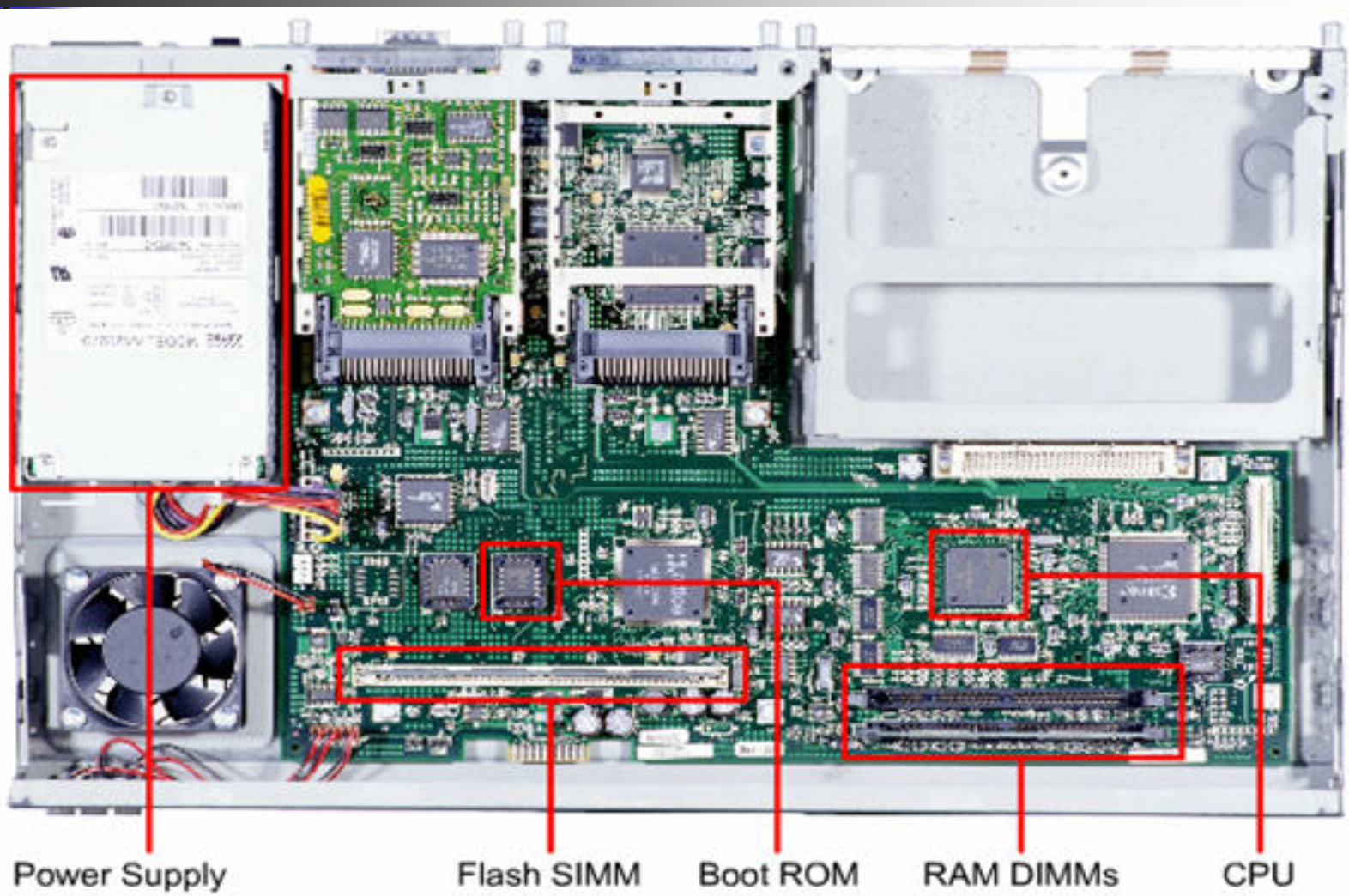
WAN và Router

Định tuyến trong mạng WAN

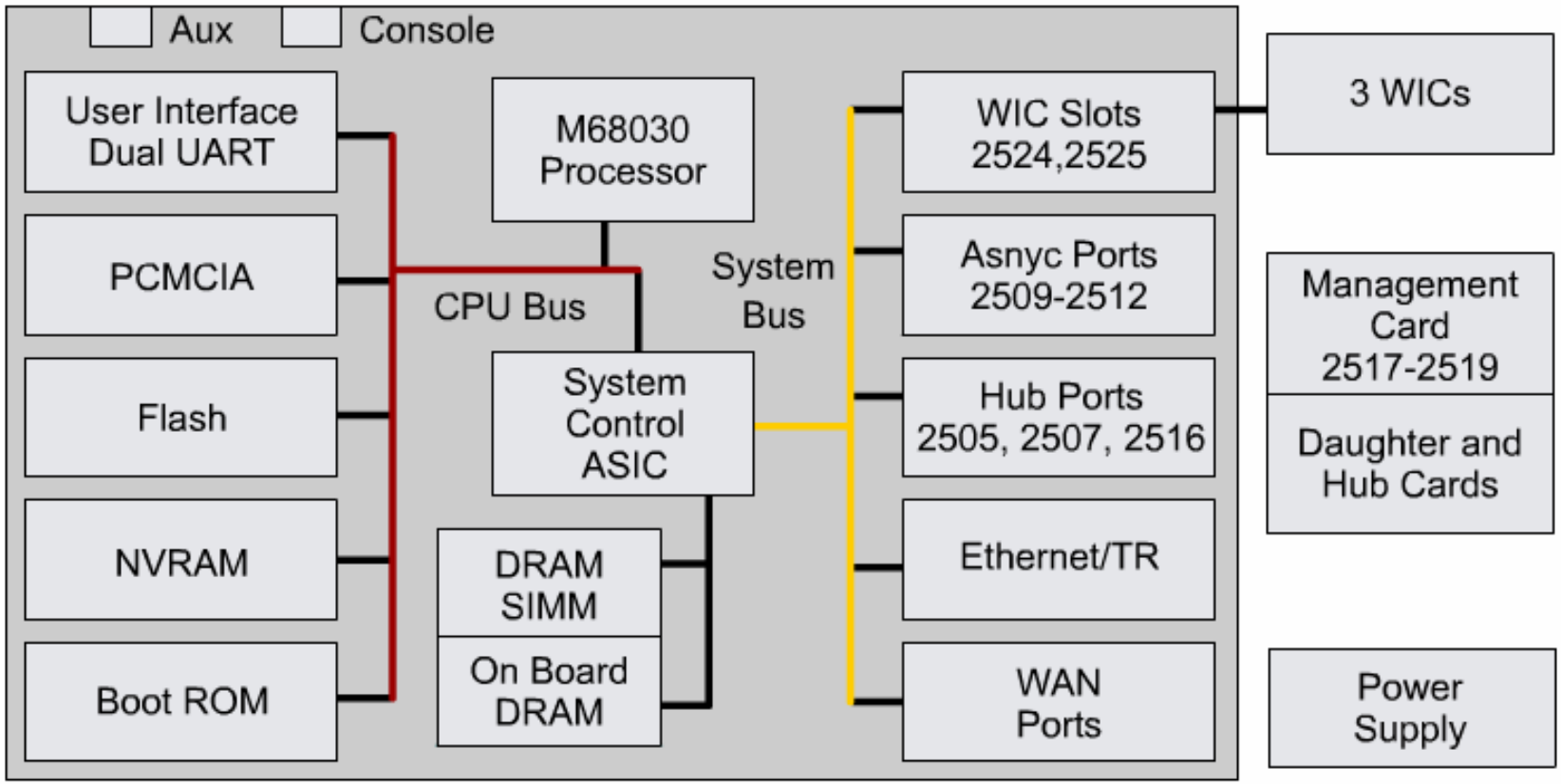


Các thành phần của Router

Series 2600 router

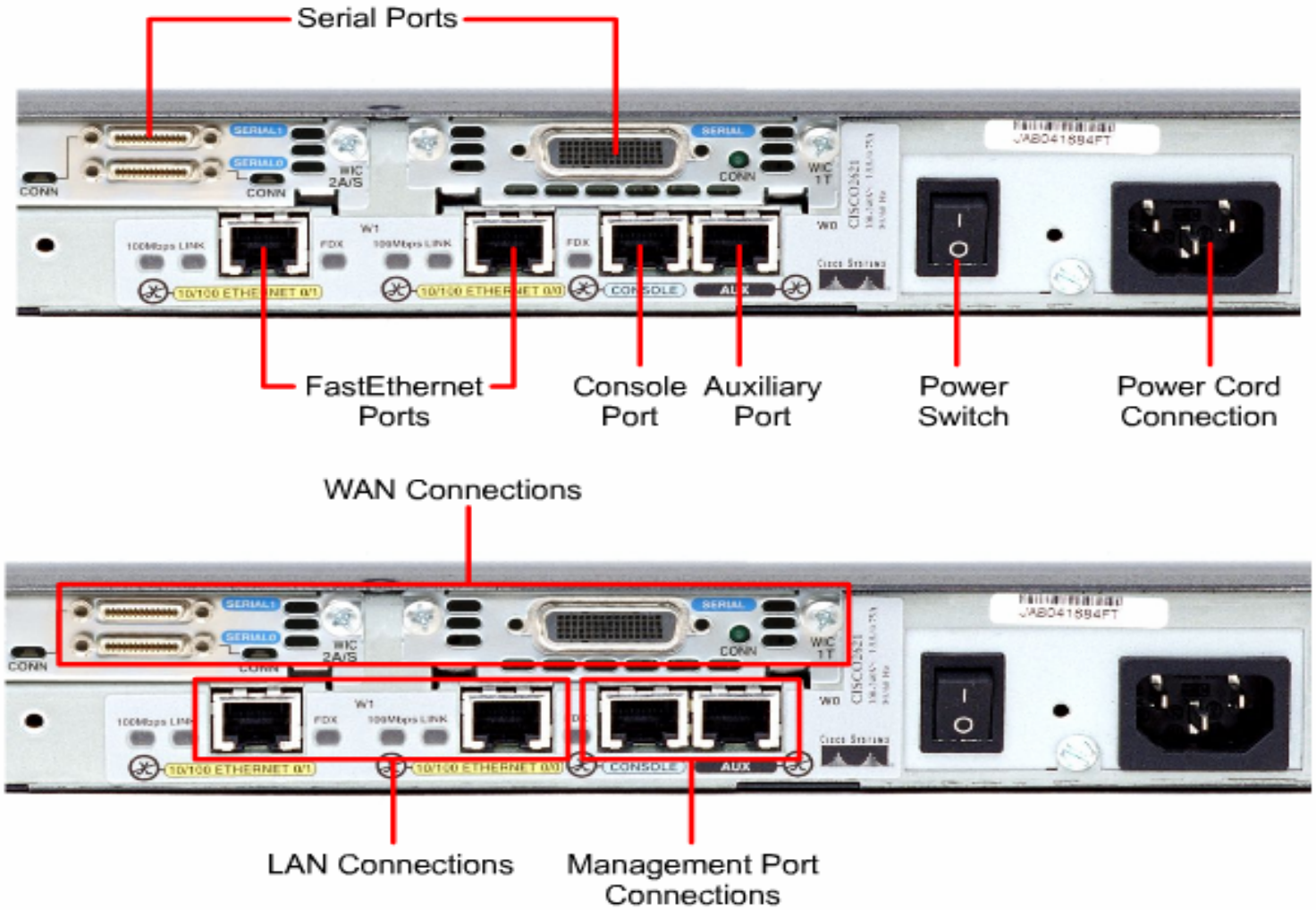


Các thành phần của Router

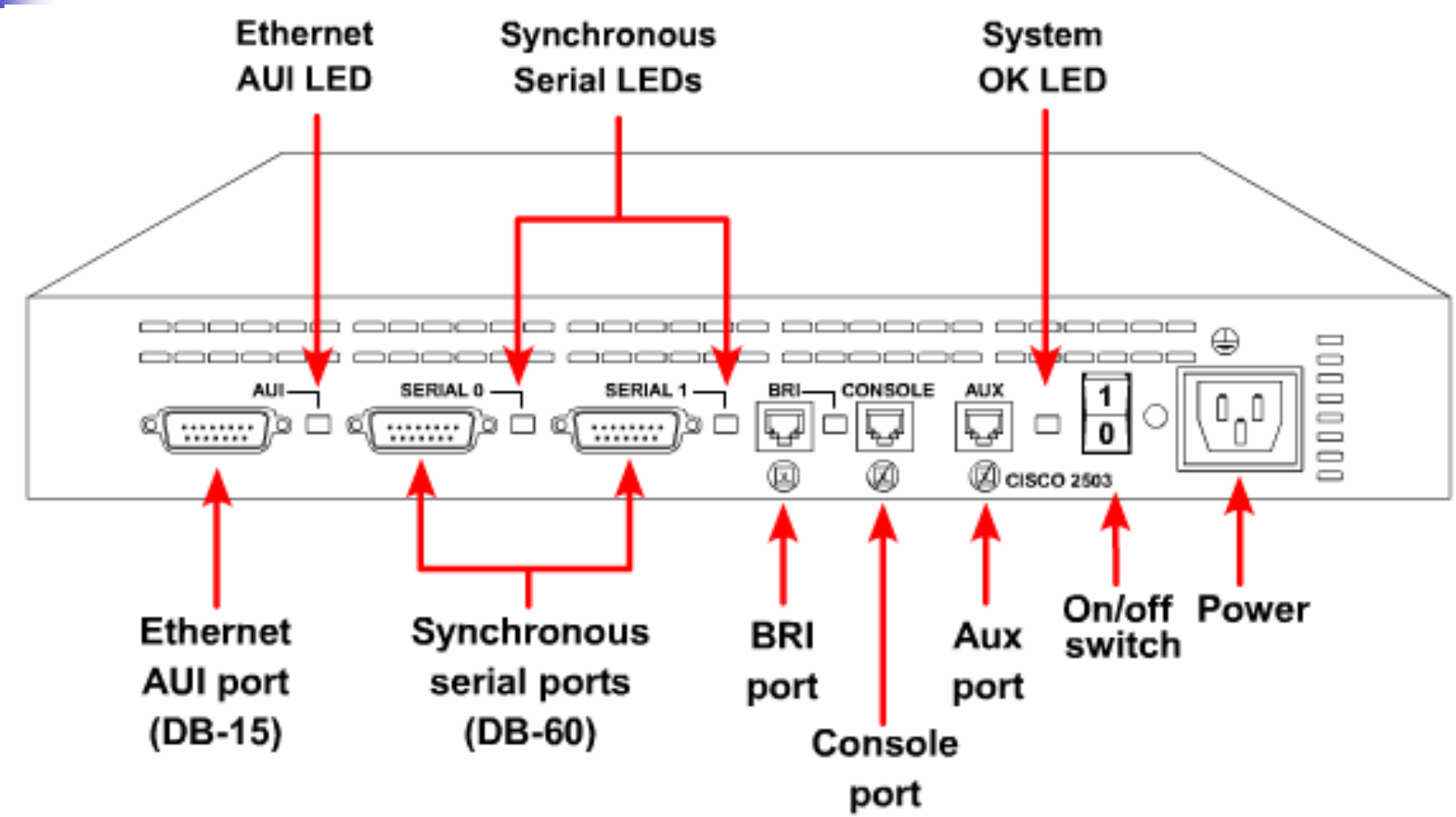


Các thành phần của Router

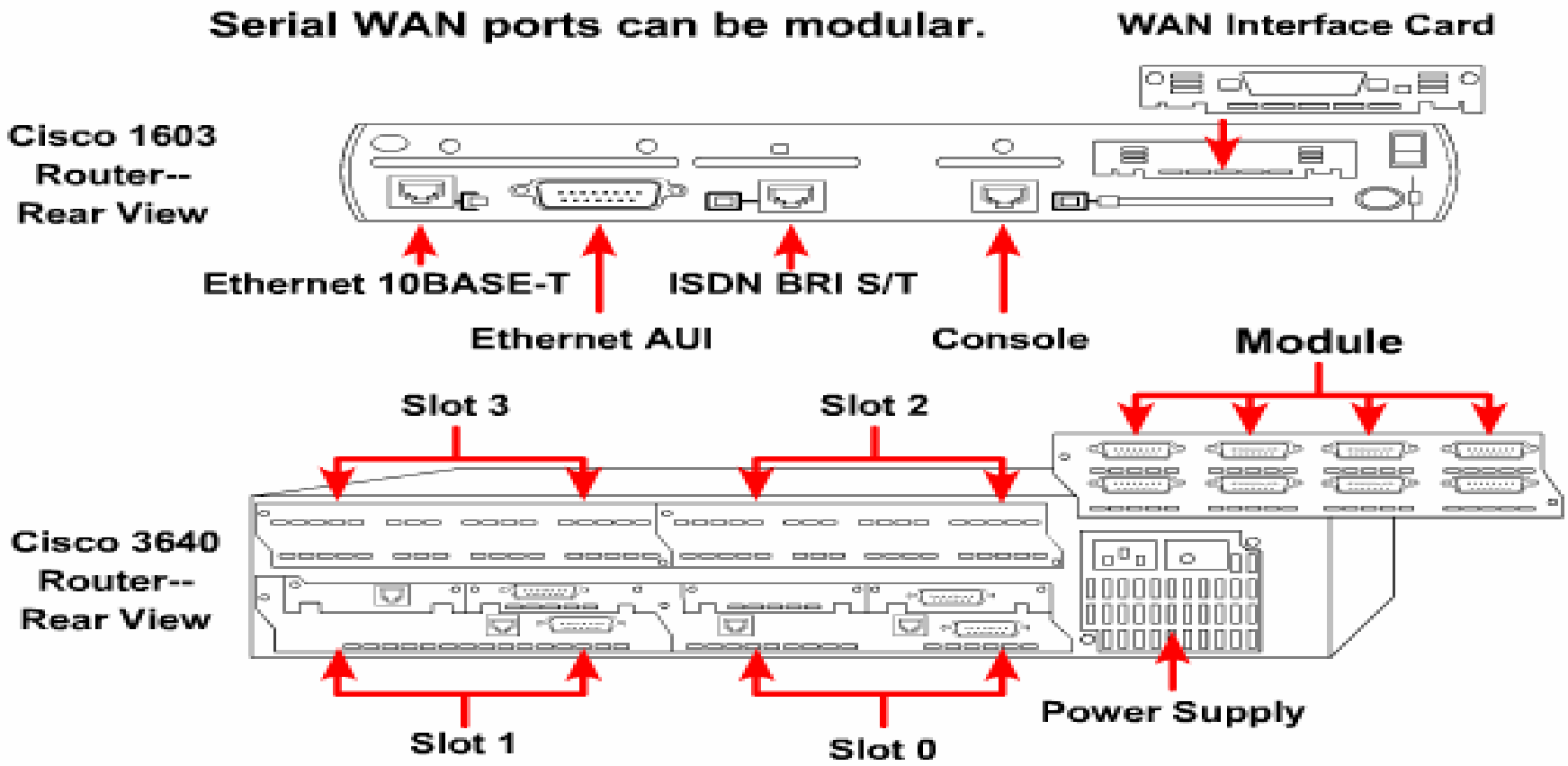
Series 2600 router



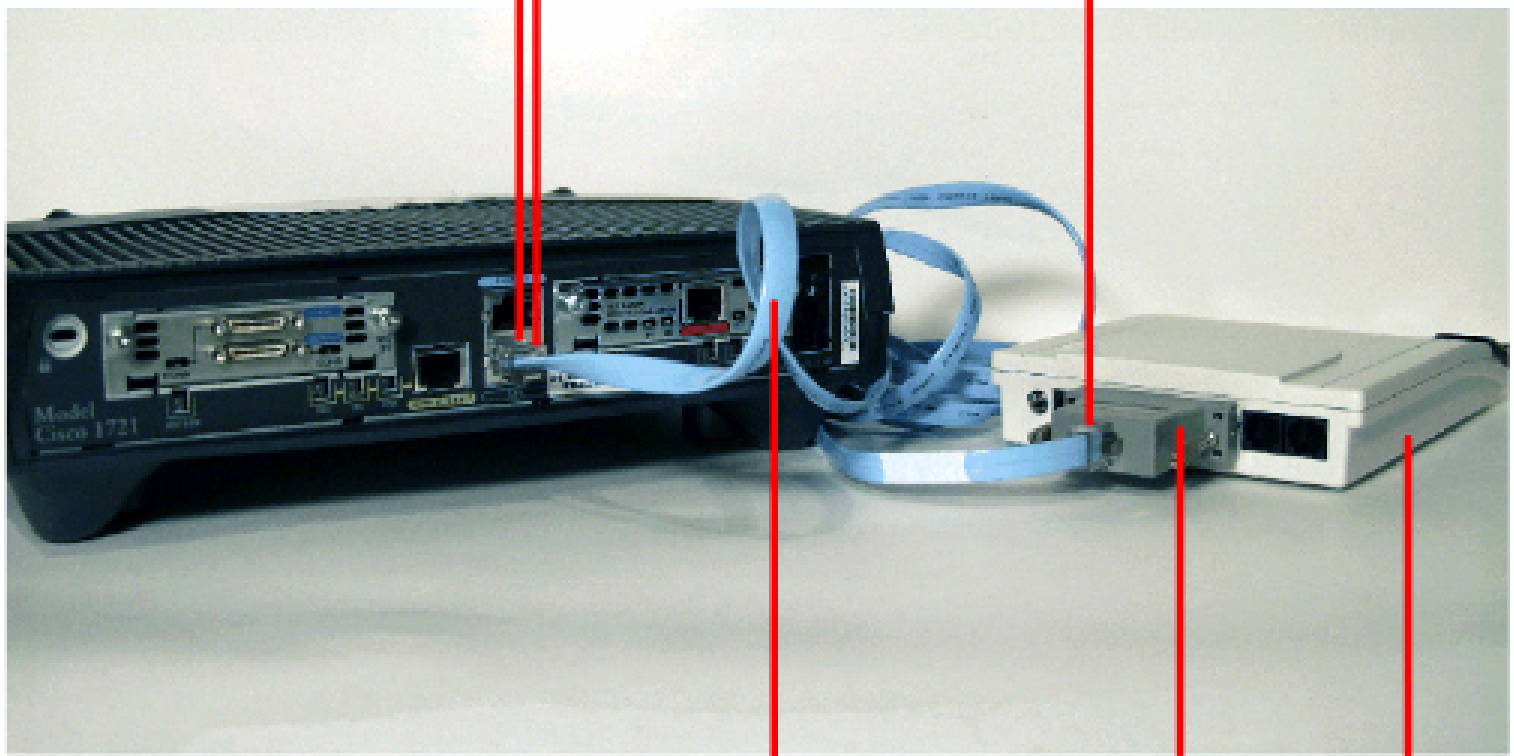
Các thành phần của Router



Các thành phần của Router

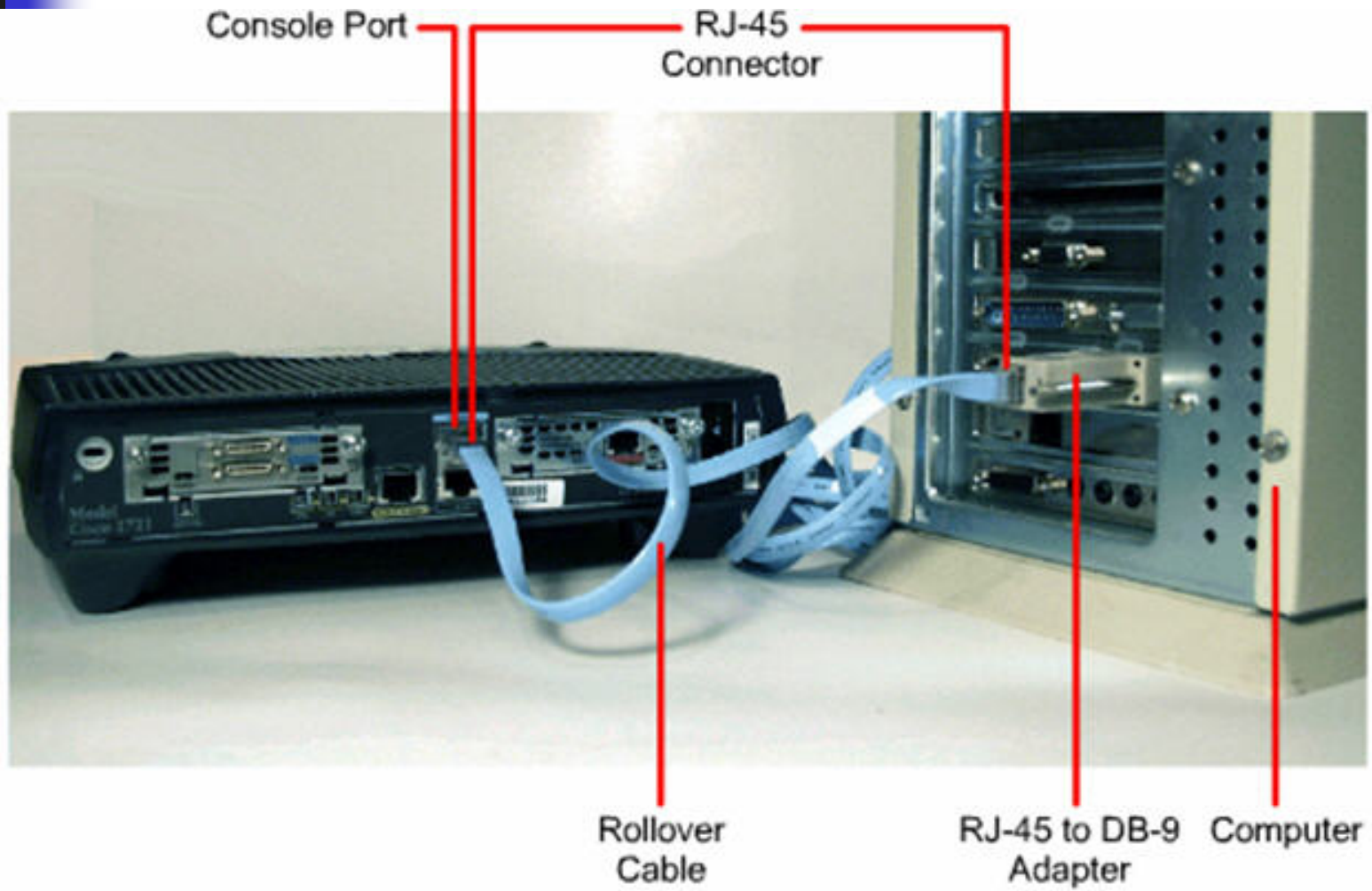


Các thành phần của Router
Kết nối cổng Auxiliary với Modem



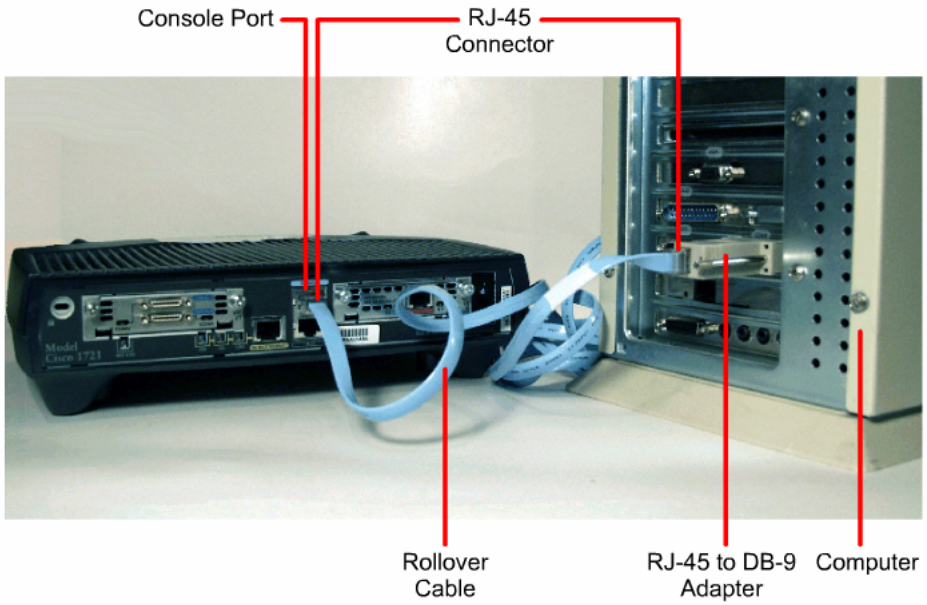
Các thành phần của Router

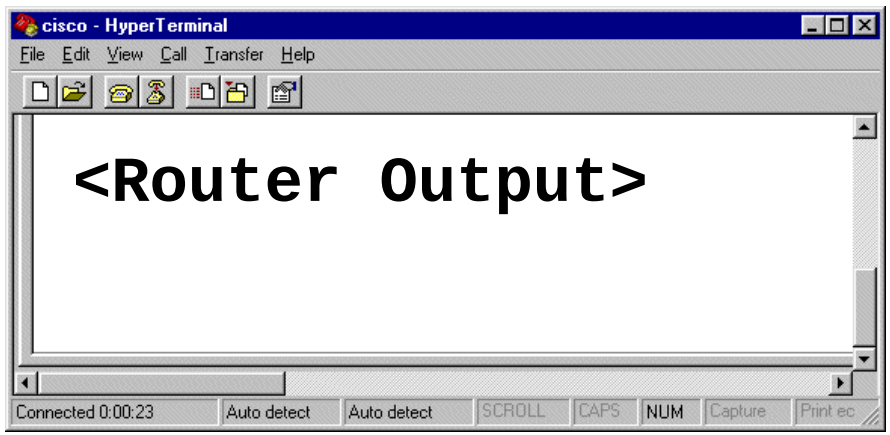
Kết nối Console với máy tính



Các thành phần của Router

Kết nối Console với máy tính

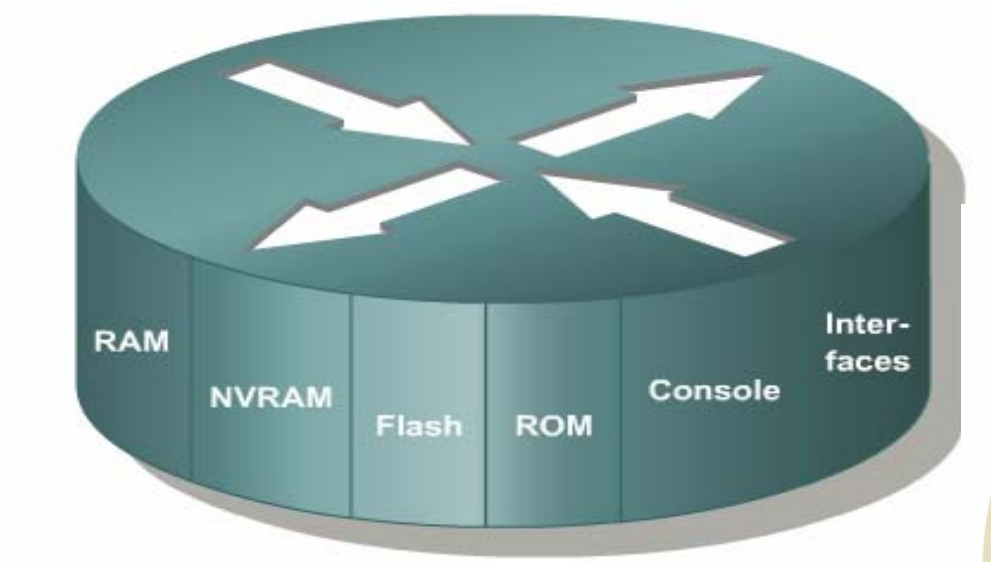


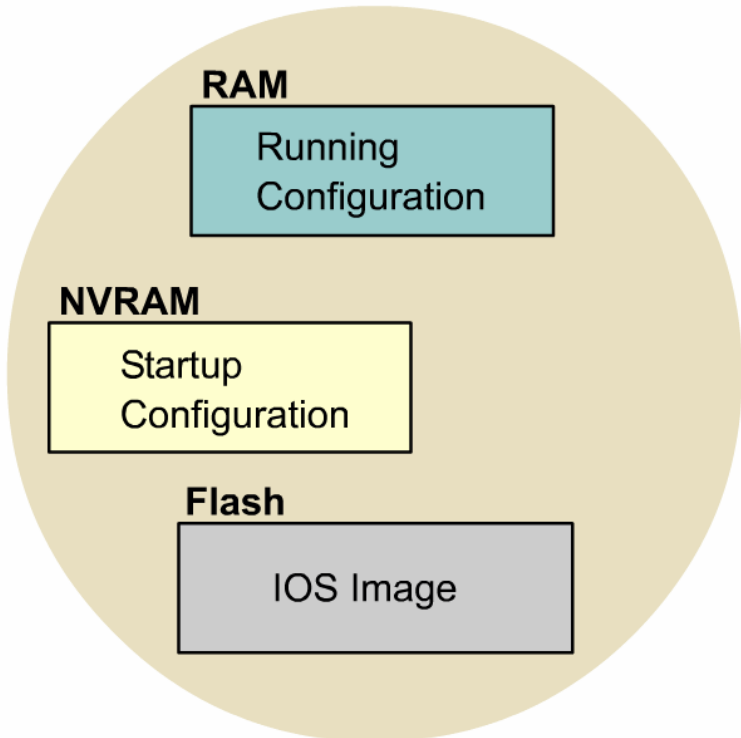


Các thành phần của Router

Kết nối Console với máy tính

Các thành phần của Router





Các thành phần của Router
CPU, RAM, ROM

- CPU: Đơn vị xử lý trung tâm.
- RAM (DRAM - Dynamic Random Access Memory)
  - Lưu bảng định tuyến và bảng ARP.
  - Duy trì hàng đợi và vùng nhớ đệm cho các gói dữ liệu.
  - Cung cấp bộ nhớ tạm thời cho tập tin cấu hình của router.
  - Thông tin trên DRAM sẽ mất đi khi bị ngắt điện.
- ROM (Read - Only Memory)
  - Lưu giữ chương trình tự kiểm tra khi khởi động (POST – Power-on Self Test).
  - Lưu chương trình bootstrap và hệ điều hành cơ bản.

Các thành phần của Router
NVRAM, FLASH MEMORY

- NVRAM (Non-volative Random-access Memory)
  - Lưu giữ tập tin cấu hình khởi động của router.
  - Nội dung NVRAM không mất đi khi bị tắt điện.
- Flash Memory
  - Lưu hệ điều hành IOS. Có thể cập nhật.
  - Nội dung vẫn được lưu giữ khi router bị ngắt điện.
  - Có thể lưu nhiều phiên bản IOS khác nhau trên flash.
  - Là loại ROM xoá và lập trình được (EPROM).

Các thành phần của Router
Các cổng giao tiếp

- Các cổng giao tiếp: 3 loại
  - LAN: Cổng Ethernet hoặc Token Ring. Có thể gắn cố định trên router hoặc dưới dạng card rời.
  - WAN: Cổng Serial hoặc ISDN. Có thể gắn cố định hoặc dưới dạng card rời.
  - Console/AUX: là cổng nối tiếp, thường dùng để kết nối với máy tính thông qua cổng COM hoặc modem khi cấu hình cho router.

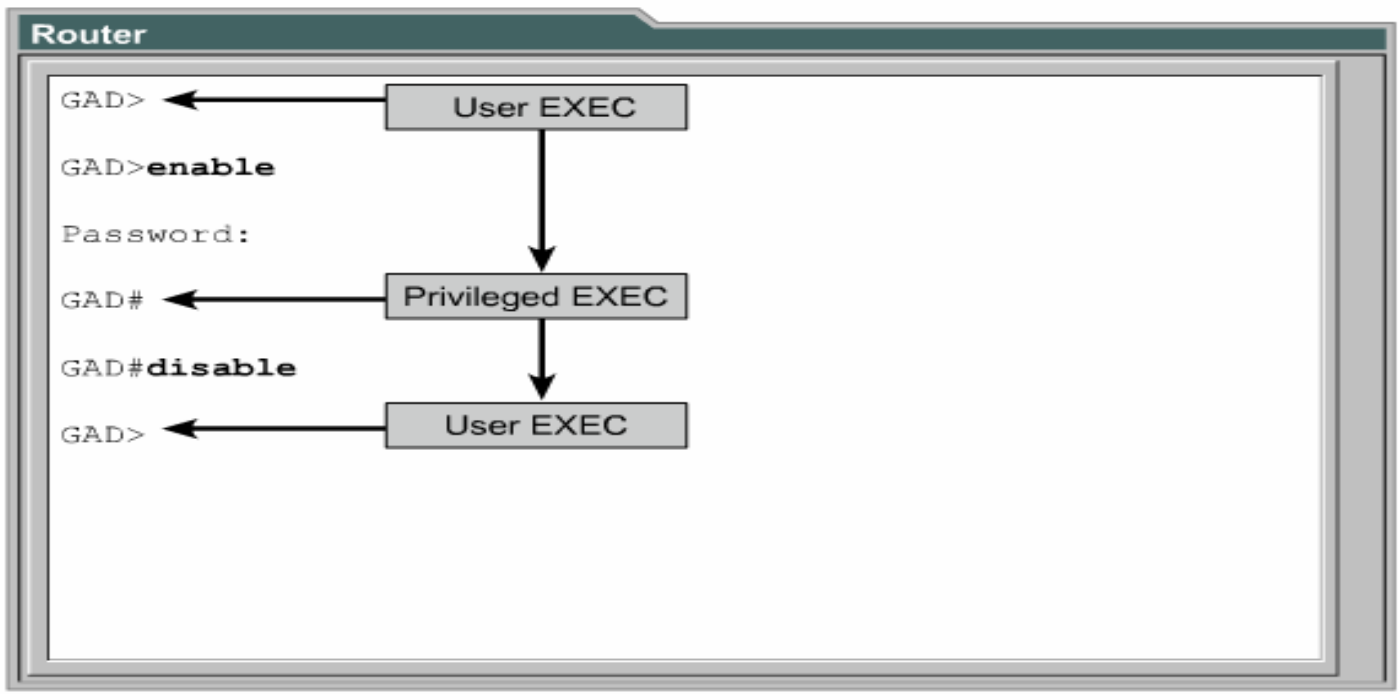
Khởi động Router
Các chế độ giao tiếp với người dùng

- Phần mềm IOS của Cisco sử dụng giao diện dòng lệnh command-line interface (CLI) làm giao tiếp truyền thống giữa người dùng và thiết bị.
- Có 3 phương pháp truy cập chính đến thiết bị:
  - Console
  - AUX port (modem)
  - Telnet

Khởi động Router

Các chế độ giao tiếp với người dùng

EXEC Mode	Prompt	Typical Use
User	**GAD>**	check the router status
Privileged	**GAD#**	accessing the router configuration modes



Khởi động Router

Tên tập tin hệ điều hành của Cisco Router

The name has three parts, separated by dashes: e.g. xxxx-yyyy-ww:

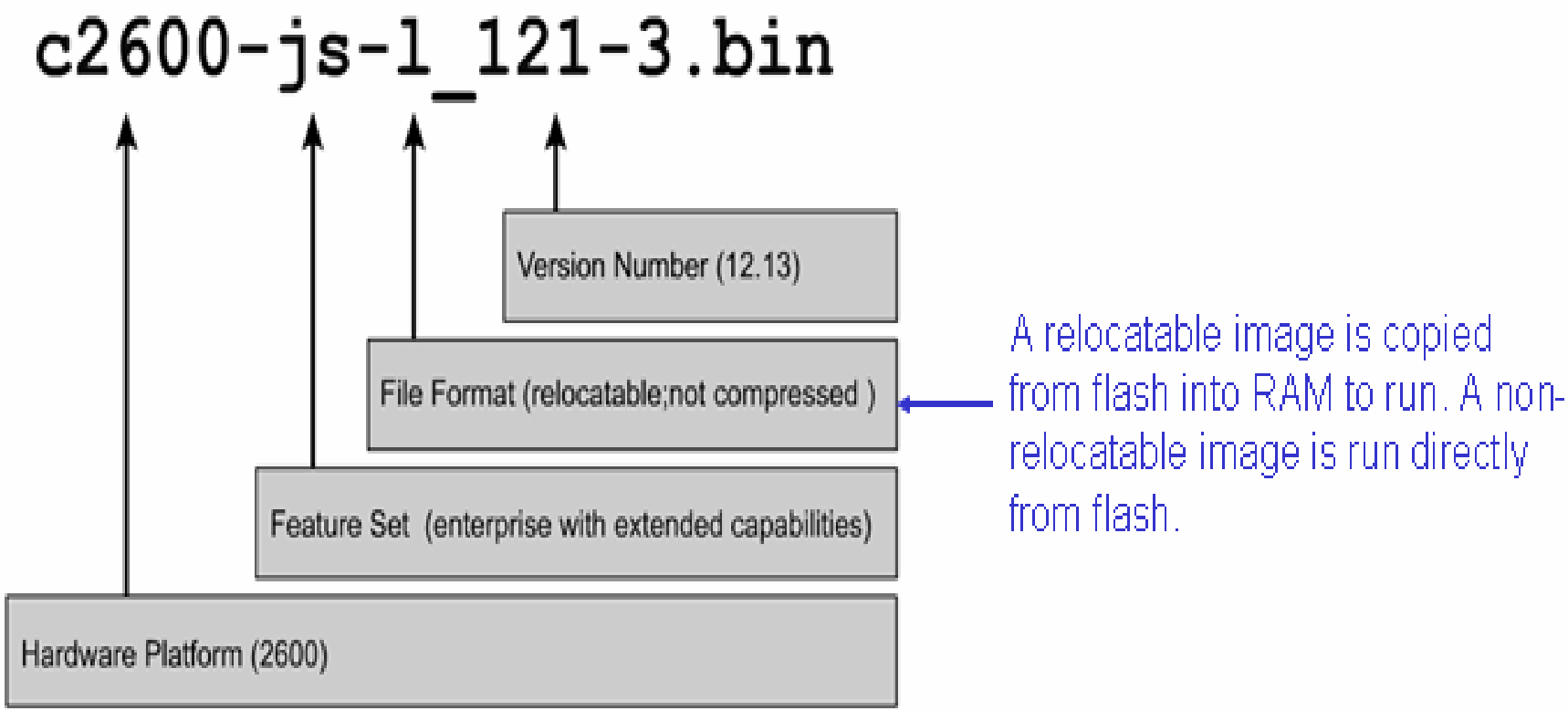
- xxxx = Platform
- yyyy = Features
- ww = Format - where it executes from if compressed

Name Codes

Platform (Hardware) (Partial list)	
c1005	1005
c1600	1600
c1700	1700, 1720, 1750
c2500	25xx, 3xxx, 5100, AO (11.2 and later only)
c2600	2600
c2800	Catalyst 2800
c2900	2910, 2950
c3620	3620
c3640	3640

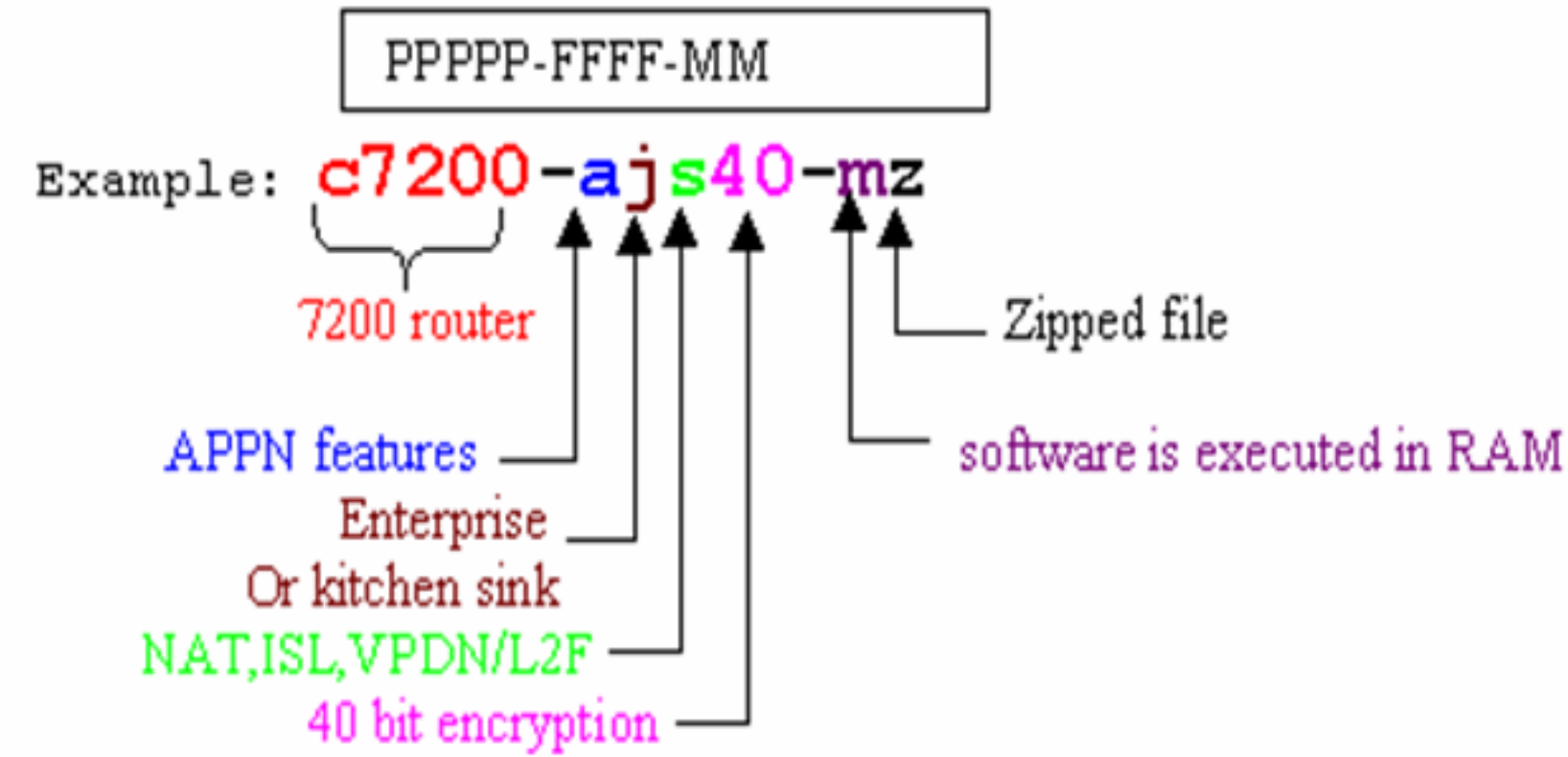
Khởi động Router

Tên tập tin hệ điều hành của Cisco Router



Khởi động Router

Tên tập tin hệ điều hành của Cisco Router



Khởi động Router
Xem phiên bản hệ điều hành

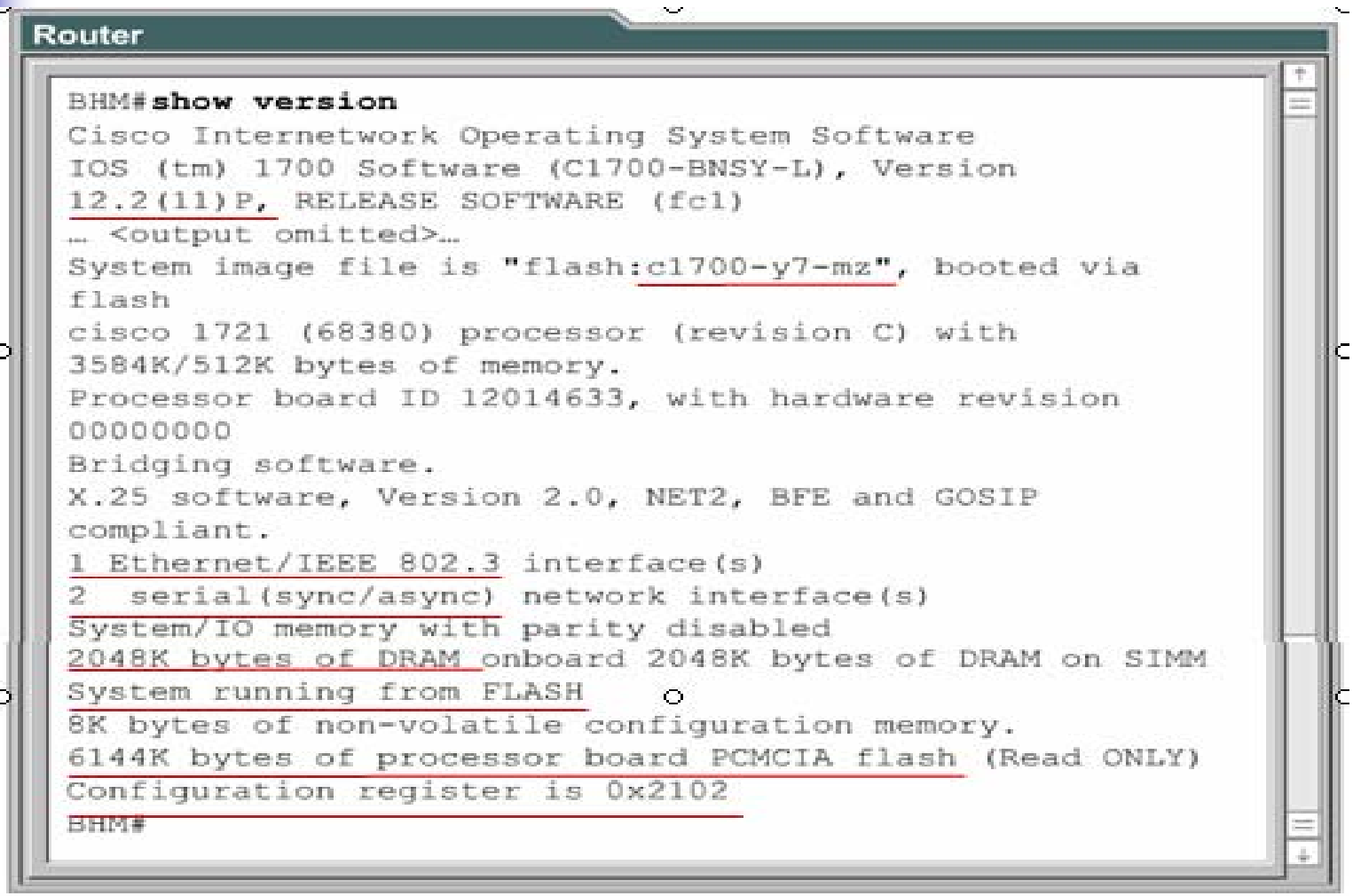
Operating Environment	Prompt	Usage
ROM monitor	> or ROMMON>	Failure or password recovery
Boot ROM	Router (boot) >	Flash image upgrade
Cisco IOS	Router>	Normal operation

Router

```
BHM#show flash
PCMCIA flash directory:
File  Length    Name/status
  1   6007232   c1700-bnsy-1.212-11.p
[6007296 bytes used, 284160 available, 6291456
total]
6144K bytes of processor board PCMCIA flash (Read
ONLY)
BHM#
```

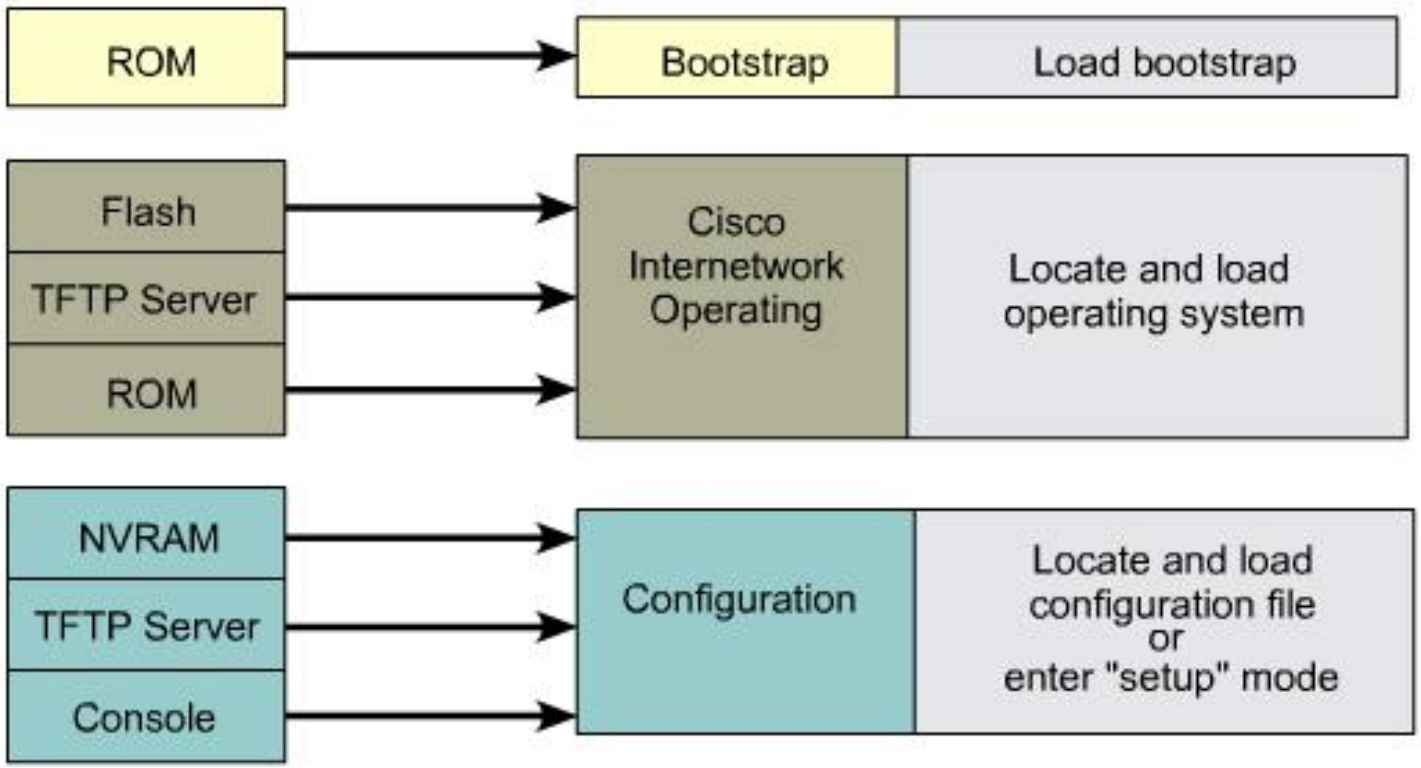
Khởi động Router

Xem phiên bản hệ điều hành



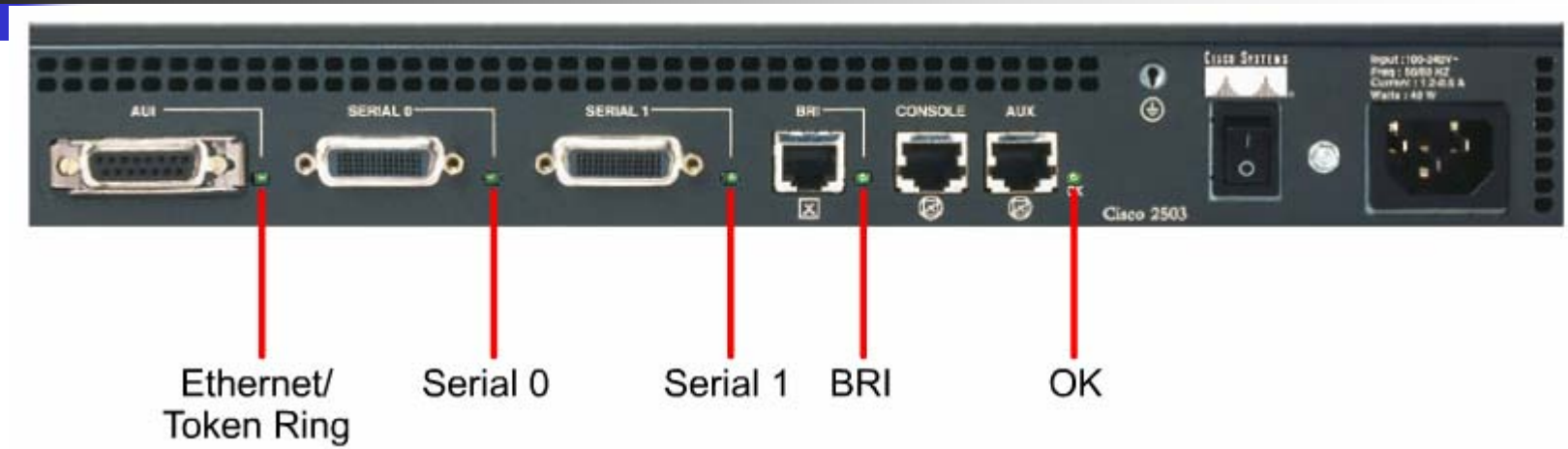
Khởi động Router

Các bước khởi động



Khởi động Router

Các chỉ thị đèn LET trên Router



- ON: An interface LED indicates the activity of the corresponding interface.
- OFF: If an LED is off when the interface is active and the interface is correctly connected, a problem may be indicated.
- ALWAYS ON: If an interface is extremely busy, its LED will always be on.
- The green OK LED to the right of the AUX port will be on after the system initializes correctly

Khởi động Router
Chế độ cài đặt

Router

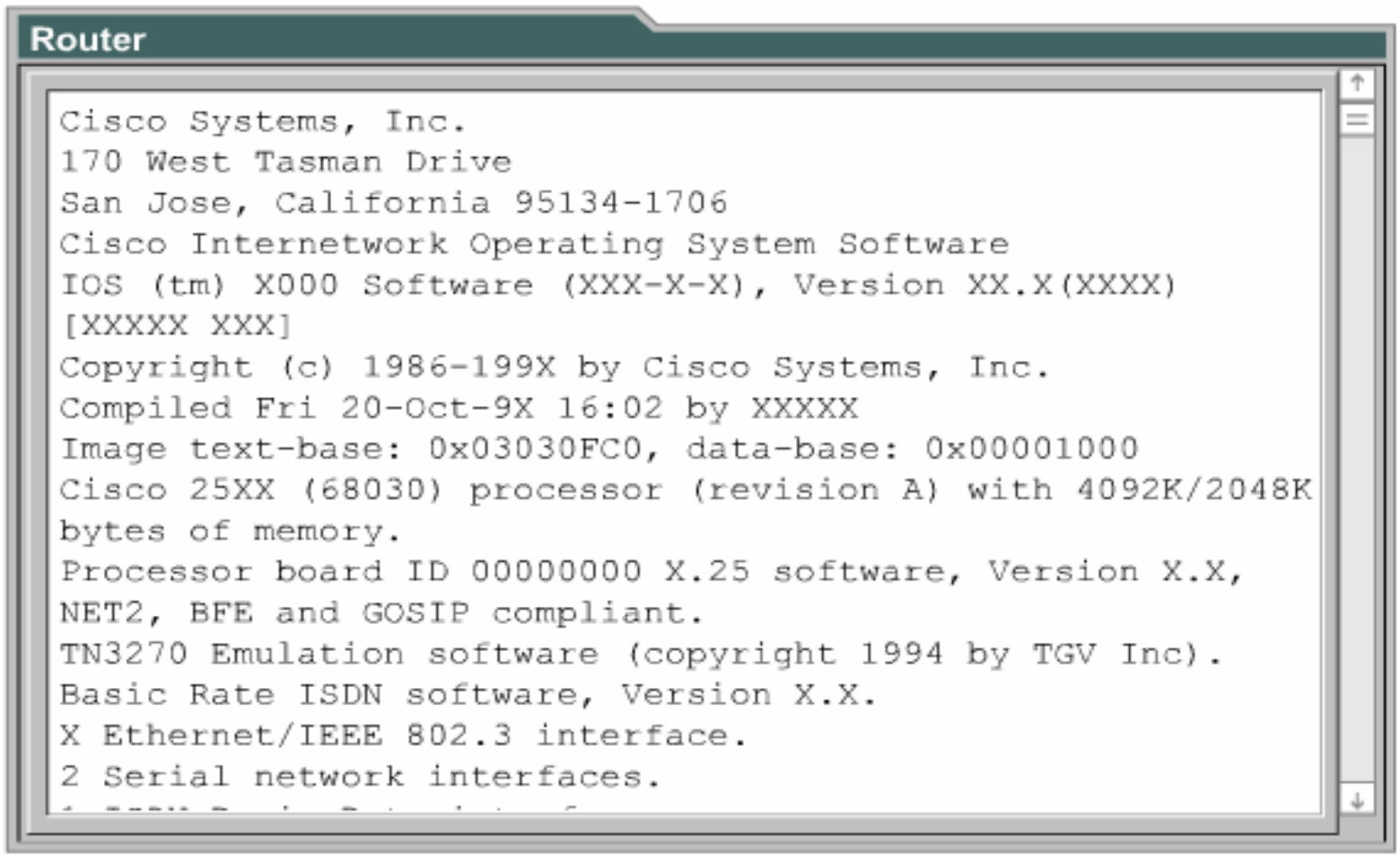
```
#setup

--System Configuration Dialog--
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Continue with configuration dialog? [yes].

First, would you like to see the current interface summary?
[yes]

Interface    IP-Address    OK?   Method    Status   Protocol
TokenRing0   unassigned    NO    not set    down     down
Ethernet0    unassigned    NO    not set    down     down
Serial0      unassigned    NO    not set    down     down
Fddi0        unassigned    NO    not set    down     down
```

Khởi động Router
Màn hình khởi động

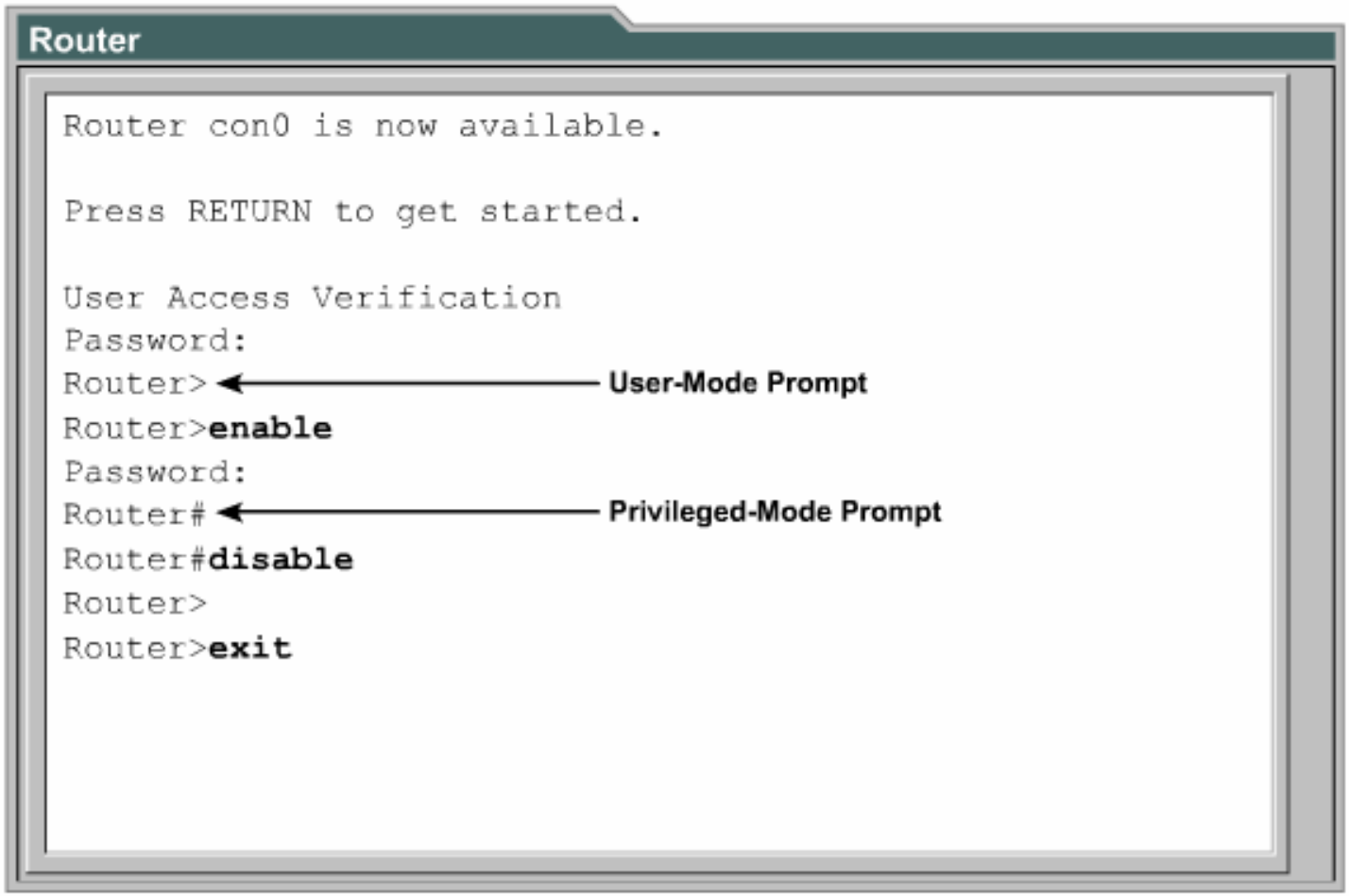
Router

```
System Bootstrap, Version X.X(XXXX) [XXXXX XX], RELEASE
SOFTWARE
Copyright (c) 1986-199X by Cisco Systems
2500 processor with 4096 Kbytes of main memory

Notice: NVRAM invalid, possibly due to write erase.

F3: 5797928+162396+258800 at 0x3000060

Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
```

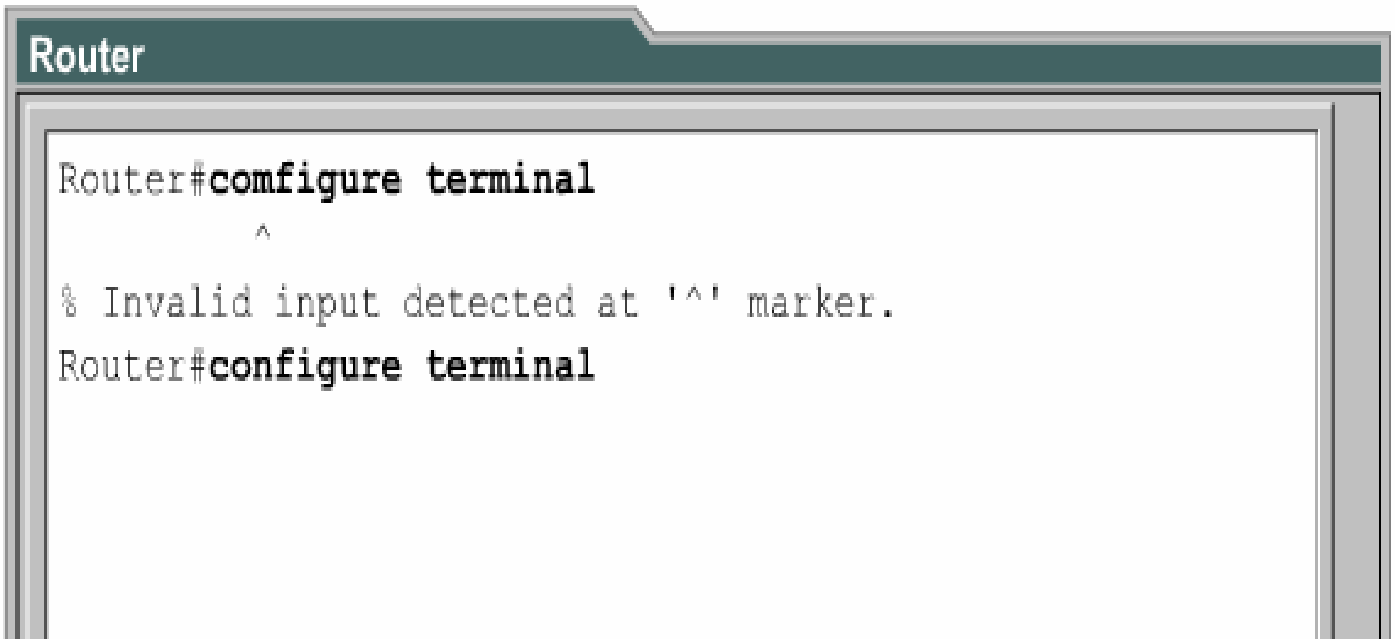
Khởi động Router
Màn hình khởi động



Khởi động Router
Màn hình khởi động



Một số lệnh cơ bản
Thông báo lỗi tại giao diện dòng lệnh



Một số lệnh cơ bản
Lệnh ?

Router

```
Cisco#?
Exec commands:
  access-enable     Create a temporary Access-List entry
  access-profile    Apply user-profile to interface
  access-template   Create a temporary Access-List entry
  archive           Manage archive files
  bfe               For manual emergency modes setting
  cd                Change current directory
  clear             Reset functions
  clock             Manage the system clock
  configure         Enter configuration mode
  connect           Open a terminal connection
  copy              Copy from one file to another
  debug             Debugging functions (see also
                    'undebug')
  delete            Delete a file
  dir               List files on a filesystem
```

Một số lệnh cơ bản
Lệnh ?

Router

```
Cisco#cl?
clear  clock
Cisco#clock
% Incomplete command.
Cisco#clock ?
  set  Set the time and date
Cisco#clock set
% Incomplete command.
Cisco#clock set ?
  hh:mm:ss  Current Time
```

Một số lệnh cơ bản
Di chuyển nhanh trong dòng lệnh

Command	Description
Ctrl-A	Moves to the beginning of the command line
Esc-B	Moves back one word
Ctrl-B (or right arow)	Moves back one character
Ctrl-E	Moves to the end of the command line
Ctrl-F(or left arrow)	Moves forward one character
Esc-F	Moves forward one word

Một số lệnh cơ bản
Xem history

Command	Description
Ctrl-P or up arrow key	Recalls last (previous) command
Ctrl-N or down arrow key	Recalls most recent command in the history buffer
Router>**show history**	Shows command buffer
Router>**terminal history size** *number-of-lines*	Sets the command history buffer size*
Router>**terminal no editing**	Disables advanced editing features
Router>**terminal editing**	Re-enables advanced editing
<Tab>	Completes the entry

Một số lệnh cơ bản
Lệnh show version

Router

```
GAD#show version
Cisco Internetwork Operating System Software
IOS (tm) 1700 Software (C1700-BNSY-L), Version
12.2(11)P, RELEASE SOFTWARE (fc1)
… <output omitted>…
ROM: System Bootstrap, Version 11.1(10)AA, EARLY
DEPLOYMENT RELEASE SOFTWARE (fc1)
ROM: 1700 Software (C1700-BOOT-R), Version
11.1(10)AA, EARLY DEPLOYMENT RELEASE SOFTWARE
(fc1)
GAD uptime is 3 weeks 6 days 2 hours, 11 minutes
System restarted by power-on
System image file is "flash:c1700-bnsy-l.122-
11.p", booted via flash
```

Một số lệnh cơ bản

Lệnh show version

```
Router>show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(5), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 15-Jun-99 20:08 by phanguye
Image text-base: 0x030380DC, data-base: 0x00001000

ROM: System Bootstrap, Version 11.0(10c)XB2, PLATFORM SPECIFIC RELEASE SOFTWARE
(fc1)
BOOTFLASH: 3000 Bootstrap Software (IGS-BOOT-R), Version 11.0(10c)XB2, PLATFORM
SPECIFIC RELEASE SOFTWARE (fc1)

Router uptime is 49 minutes
System restarted by reload
System image file is "flash:c2500-d-l_120-5.bin"

cisco 2516 (68030) processor (revision J) with 6144K/2048K bytes of memory.
Processor board ID 10375144, with hardware revision 00000001
Bridging software.
X.25 software, Version 3.0.0.
Basic Rate ISDN software, Version 1.1.
1 Ethernet/IEEE 802.3 interface(s)
14 Ethernet/IEEE 802.3 repeater port(s)
2 Serial network interface(s)
1 ISDN Basic Rate interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read ONLY)

Configuration register is 0x2102

Router>
```

IOS Version

ROM Version – not usually an issue

Router boot information

Booted this IOS file from flash

Amount of RAM memory

Model & CPU

Router interfaces

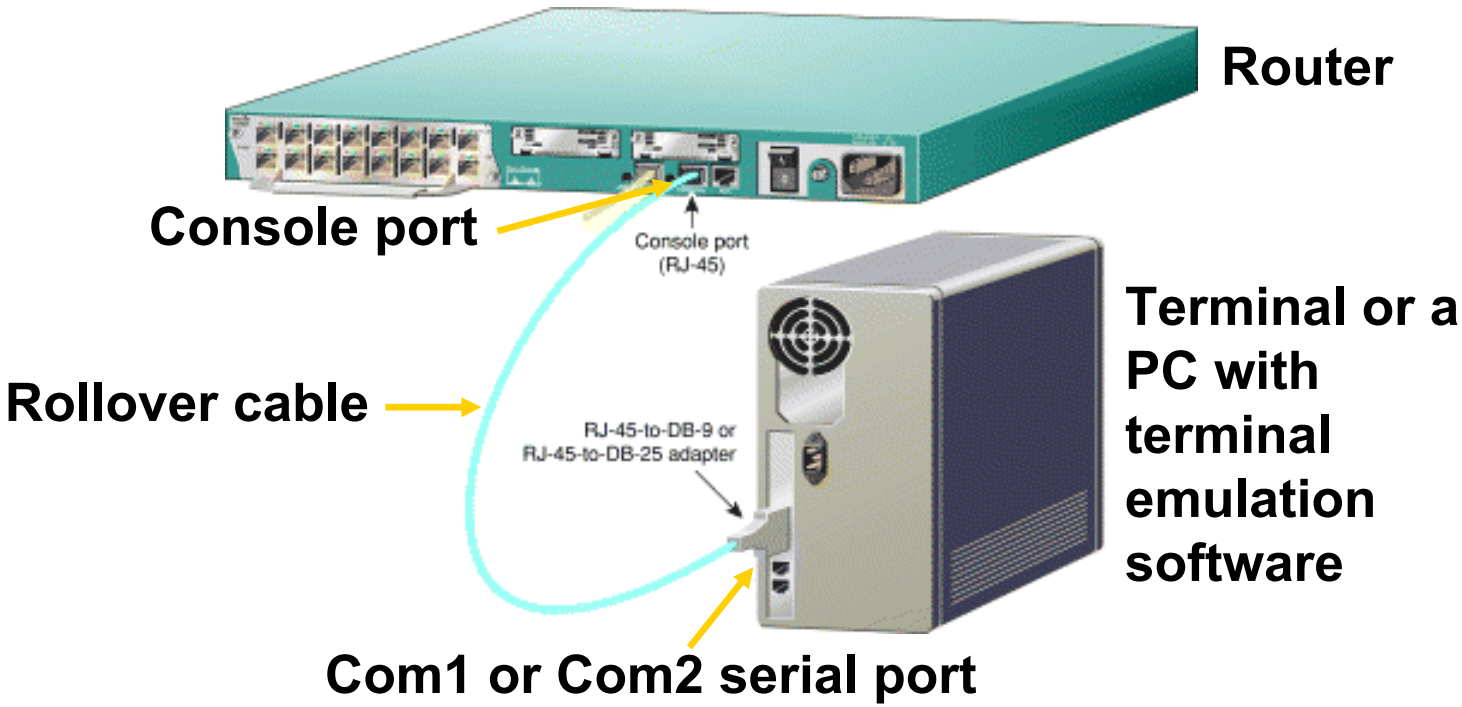
Amount of NVRAM

Amount of Flash

Configuration Register, important for password recovery. Must press space or return to get this last line!

Cấu hình cho Router

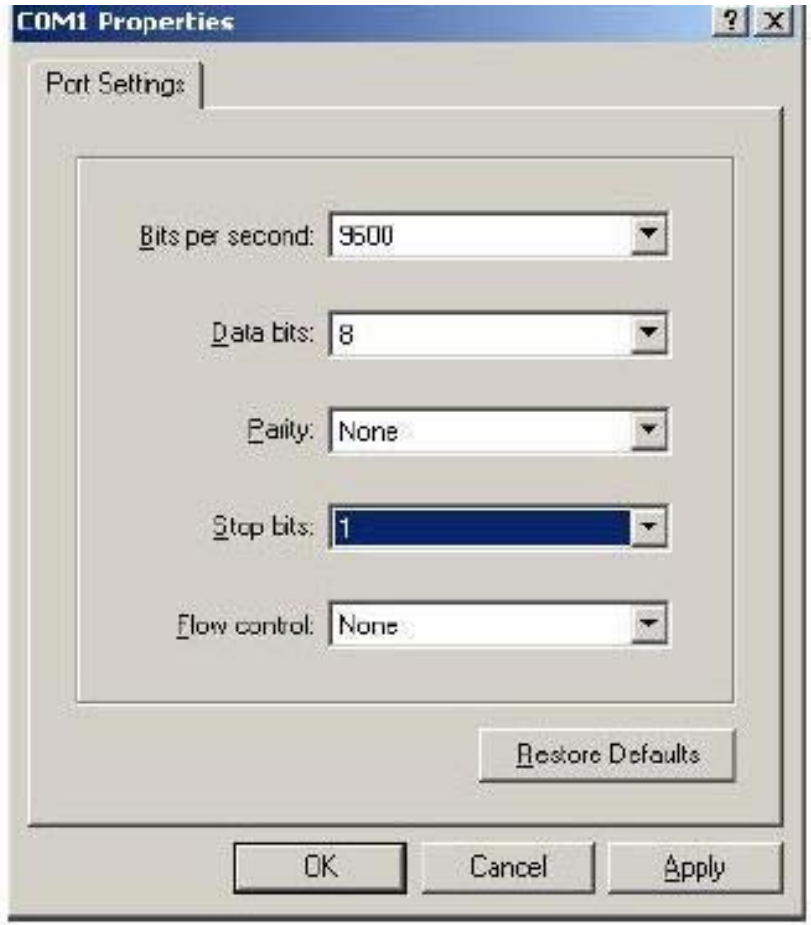
Thiết lập phiên kết nối bằng Hyper Terminal



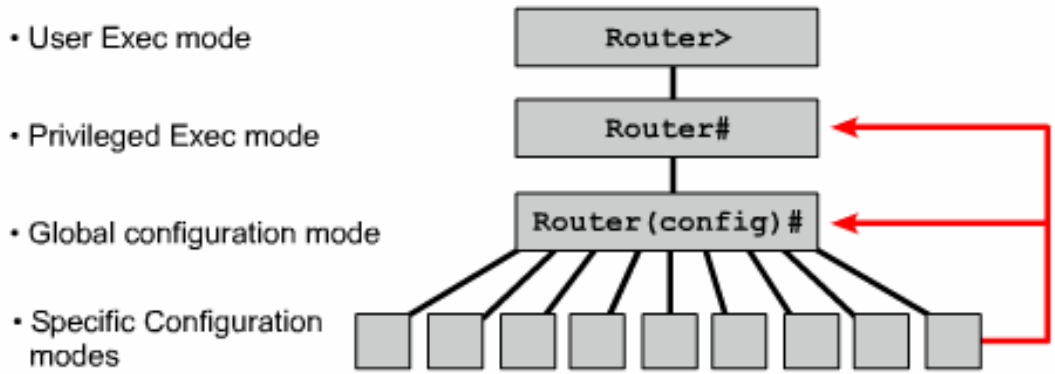
Cấu hình cho Router

Thiết lập phiên kết nối bằng Hyper Terminal

- Kết nối thiết bị đầu cuối (PC) vào cổng Console trên router bằng cáp rollover và bộ chuyển đổi RJ45-DB9 hoặc RJ45-DB25.
- Cấu hình thiết bị đầu cuối hoặc cấu hình phần mềm mô phỏng trên PC với các thông số: 9600 baud, 8 data bits, 1 stop bit, no flow control.



Cấu hình cho Router
Các chế độ giao tiếp dòng lệnh

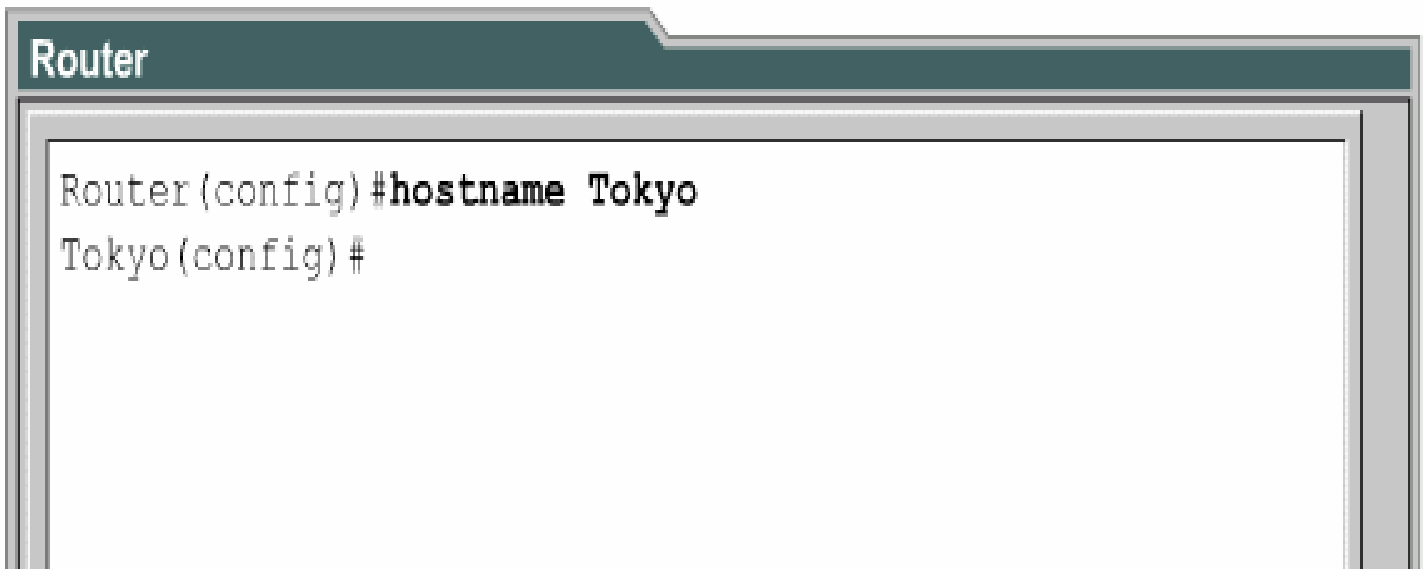


Configuration Mode	Prompt
Interface	`Router(config-if)#`
Subinterface	`Router(config-subif)#`
Controller	`Router(config-controller)#`
Map-list	`Router(config-map-list)#`
Map-class	`Router(config-map-class)#`
Line	`Router(config-line)#`
Router	`Router(config-router)#`
IPX-router	`Router(config-ipx-router)#`
Route-map	`Router(config-route-map)#`

Cấu hình cho Router

Đặt tên cho Router

```
Router#config t
Router(config)#hostname Router_A
Router_A(config)#exit
Router_A#
```



Cấu hình cho Router

Đặt mật khẩu cho Router

Console Password

```
Router(config)#line console 0
Router(config-line)#password cisco
Router(config-line)#login
```

Virtual Terminal Password

```
Router(config)#line vty 0 4
Router(config-line)#password cisco
Router(config-line)#login
```

Enable Password

```
Router(config)#enable password san-fran
```

Perform Password Encryption

```
Router(config)#service password-encryption
Router(config)#enable secret <password>
```

Cấu hình cho Router
Kiểm tra bằng các lệnh Show

- Show interface: hiển thị trạng thái các cổng giao tiếp
- Show host: hiển thị danh sách tên và địa chỉ tương ứng
- Show users: hiển thị các users đang kết nối vào router
- Show flash: hiển thị thông tin bộ nhớ flash và IOS
- Show ARP: hiển thị bảng ARP trên router
- Show protocol: hiển thị trạng thái toàn cục và trạng thái của các cổng giao tiếp đã được cấu hình giao thức lớp 3
- Show start: hiển thị tập tin cấu hình lưu trong NVRAM
- Show run: hiển thị tập tin cấu hình trên RAM

Cấu hình cho Router

Cấu hình cho cổng giao tiếp

In the following commands, the *type* argument includes serial, ethernet, fastethernet, token ring, and others:

```
Router(config)#interface type port
Router(config)#interface type slot/port
```

The following command is used to administratively turn off the interface:

```
Router(config-if)#shutdown
```

The following command is used to turn on an interface that has been shut down:

```
Router(config-if)#no shutdown
```

The following command is used to quit the current interface configuration mode:

```
Router(config-if)#exit
```

Router

```
Router(config)#interface e0
Router(config-if)#ip address 183.8.126.2 255.255.255.128
Router(config-if)#no shutdown
```

Cấu hình cho Router

Cấu hình cho cổng giao tiếp

```
Router#config t
Router(config)#interface serial 0/1
Router(config-if)#ip address 200.100.50.75 255.255.255.240
Router(config-if)#clock rate 56000     (required for serial DCE only)
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#int f0/0
Router(config-if)#ip address 150.100.50.25 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit
Router#
```

On older routers, Serial 0/1 would be just Serial 1 and f0/0 would be e0.
s = serial e = Ethernet f = fast Ethernet

Cấu hình cho Router
Cấu hình cho cổng Serial

```
Router#config t
Router(config)#interface serial 0/0
Router(config-if)#ip address 192.10.10.1 255.255.255.0
Router(config-if)#clock rate 56000 (if DCE is connected)
Router(config-if)#no shutdown
```

A router is by default administratively down, until it is brought up

Cấu hình cho Router

Cấu hình cho cổng Ethernet và FastEthernet

Ethernet

```
Router#config t
Router(config)#interface ethernet 0
Router(config-if)#ip address 192.10.10.1 255.255.255.0
Router(config-if)#no shutdown
```

FastEthernet

```
Router#config t
Router(config)#interface fastethernet 0
Router(config-if)#ip address 192.10.10.1 255.255.255.0
Router(config-if)#no shutdown
```

Cấu hình cho Router

Phân giải tên máy

```
Router(config)#ip host Auckland 172.16.32.1
Router(config)#ip host Beirut 192.168.53.1
Router(config)#ip host Capetown 192.168.89.1
Router(config)#ip host Denver 10.202.8.1
```

Cấu hình cho Router
TFTP

Command

```
Router#ping tftp - address
Type escape sequence to abort
Sending 5, 100-byte ICMP Echoes to 210.93.105.1
timeout is 2 seconds:
!!!.!
Success rate is 80 percent (4/5)
round trip min/avg/max = 68/68/168 ms
```

Be sure you can communicate with the TFTP server.

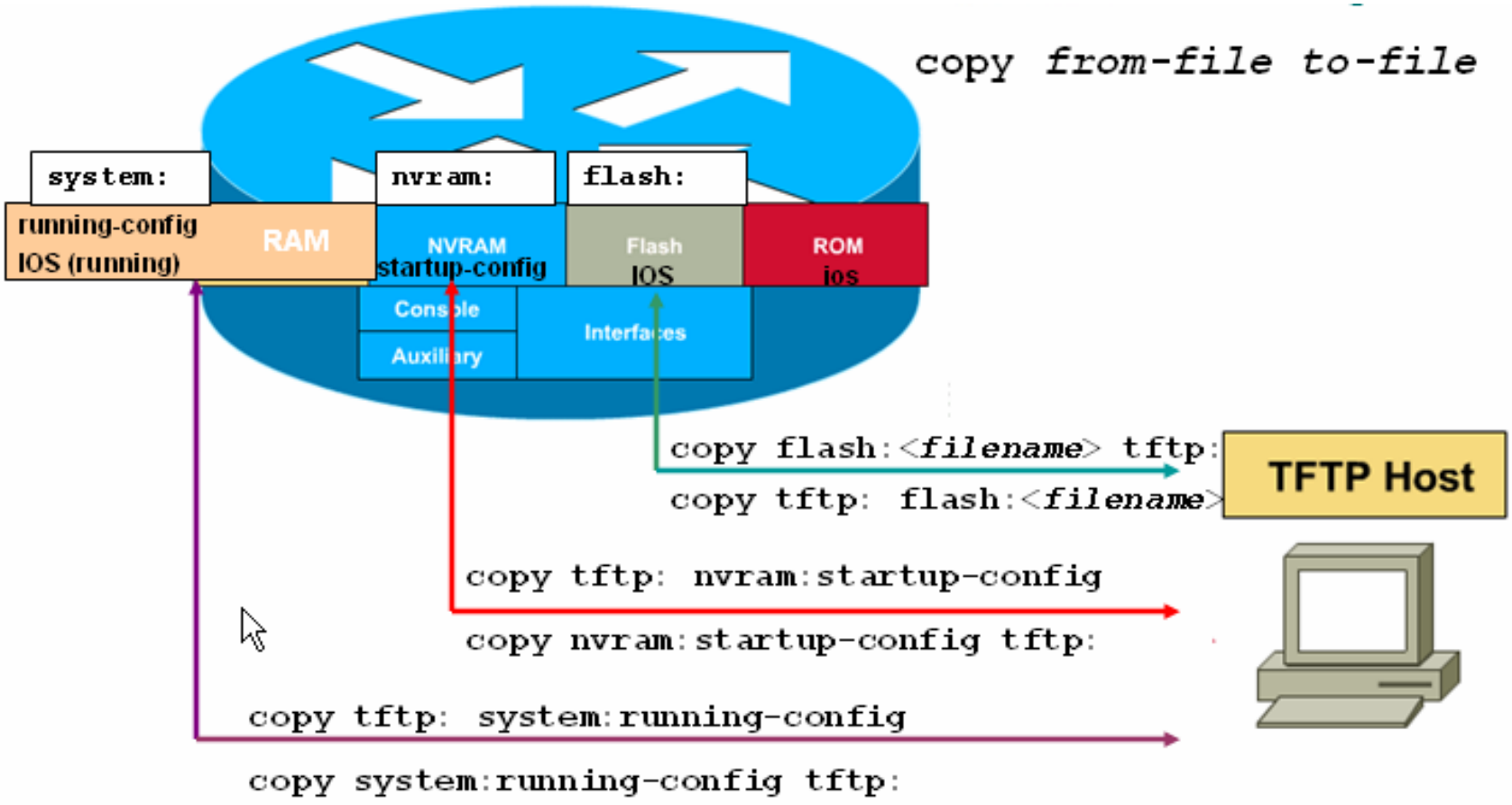
Command

```
Router# show flash
4096 bytes of flash memory on embedded flash (in XX).

file      offset      length          name
 0         0x40       1204637        xk09140z
  [903848/2097152 bytes free]
```

Know the name of the IOS file you are going to copy from on the router.

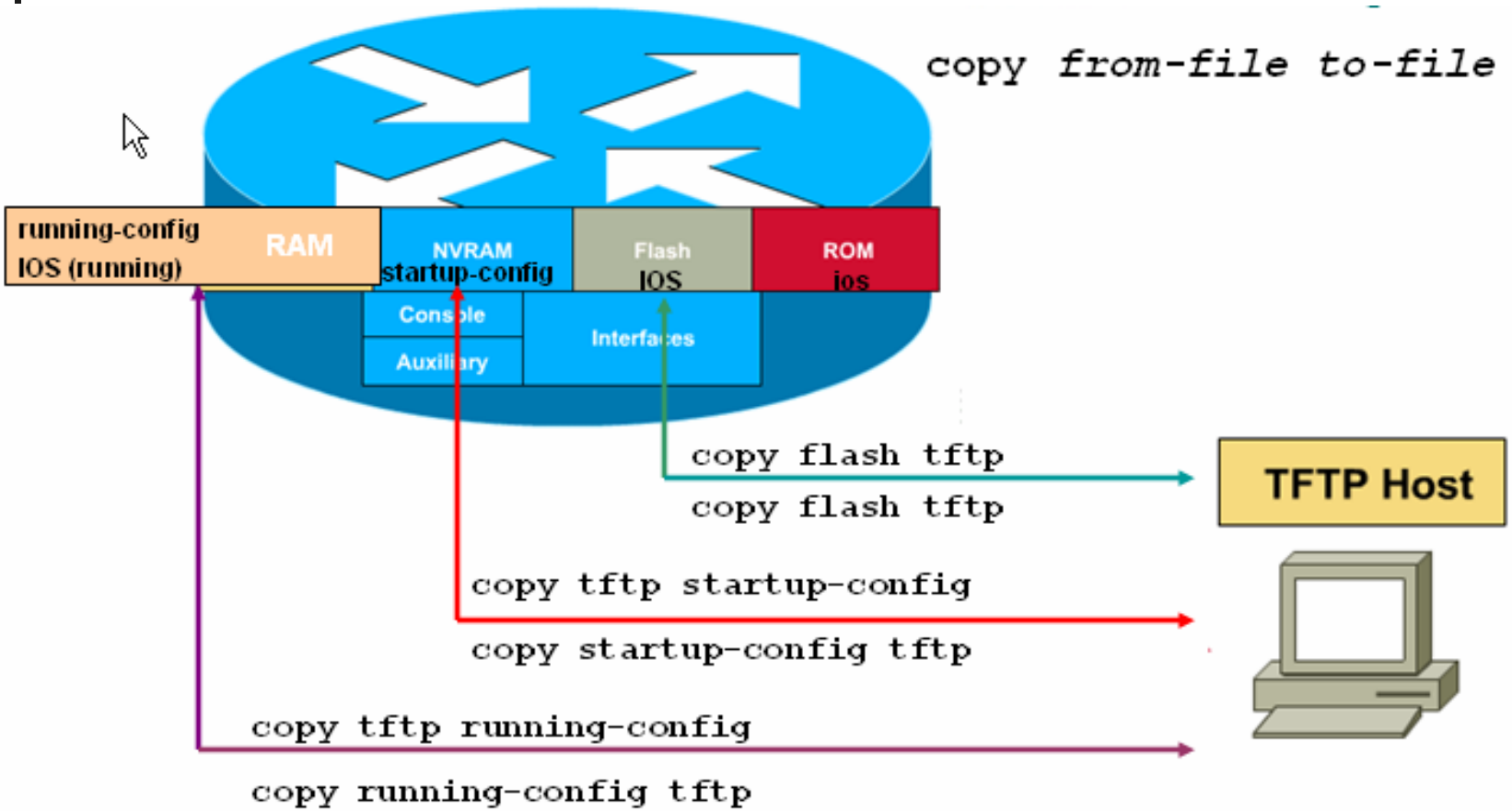
Cấu hình cho Router

Lưu hệ thống file IOS và tập tin cấu hình

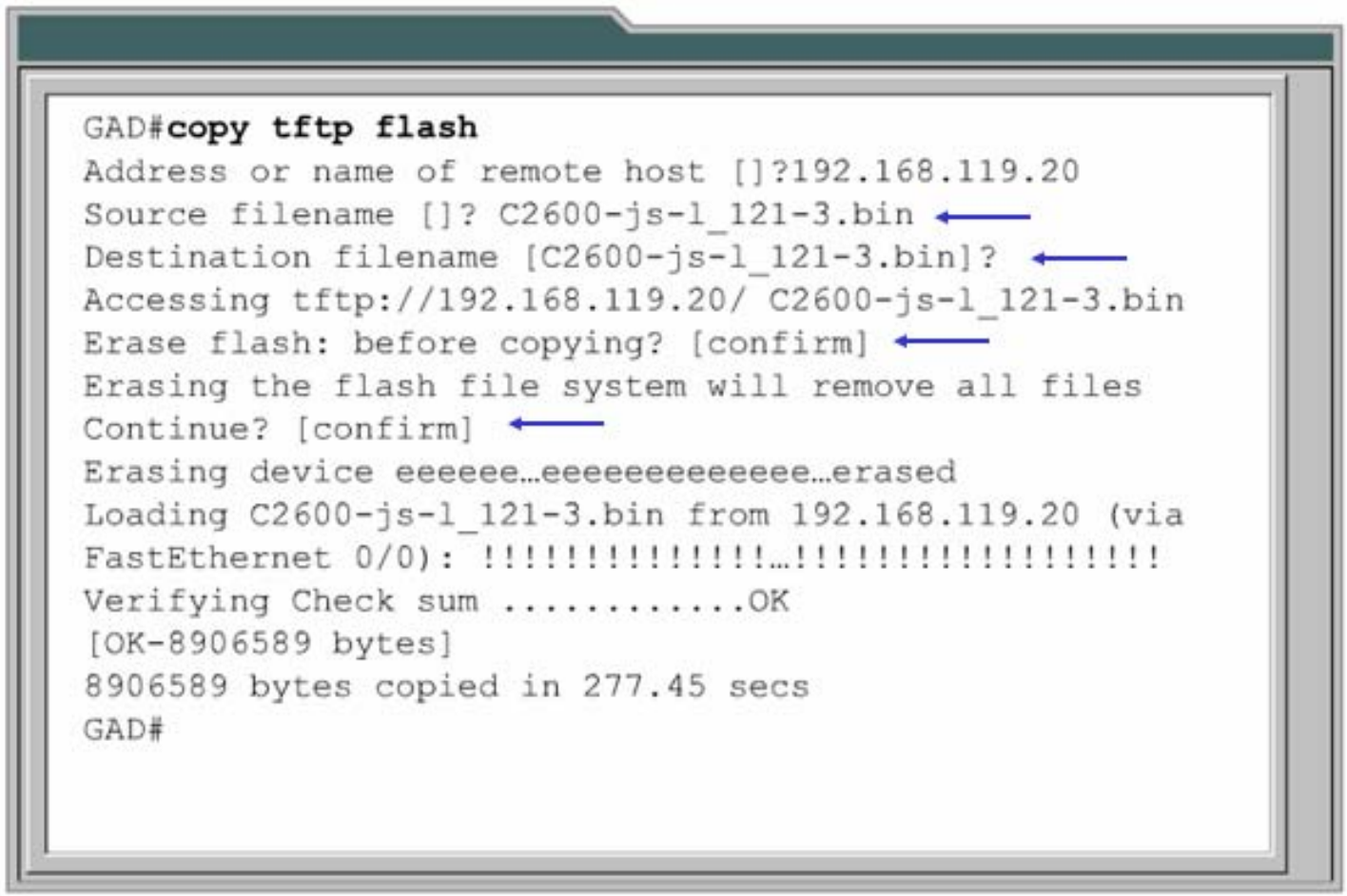


Cấu hình cho Router

Lưu hệ thống file IOS và tập tin cấu hình



Cấu hình cho Router
Lưu file IOS



Cấu hình cho Router

Lưu tập tin cấu hình

Router

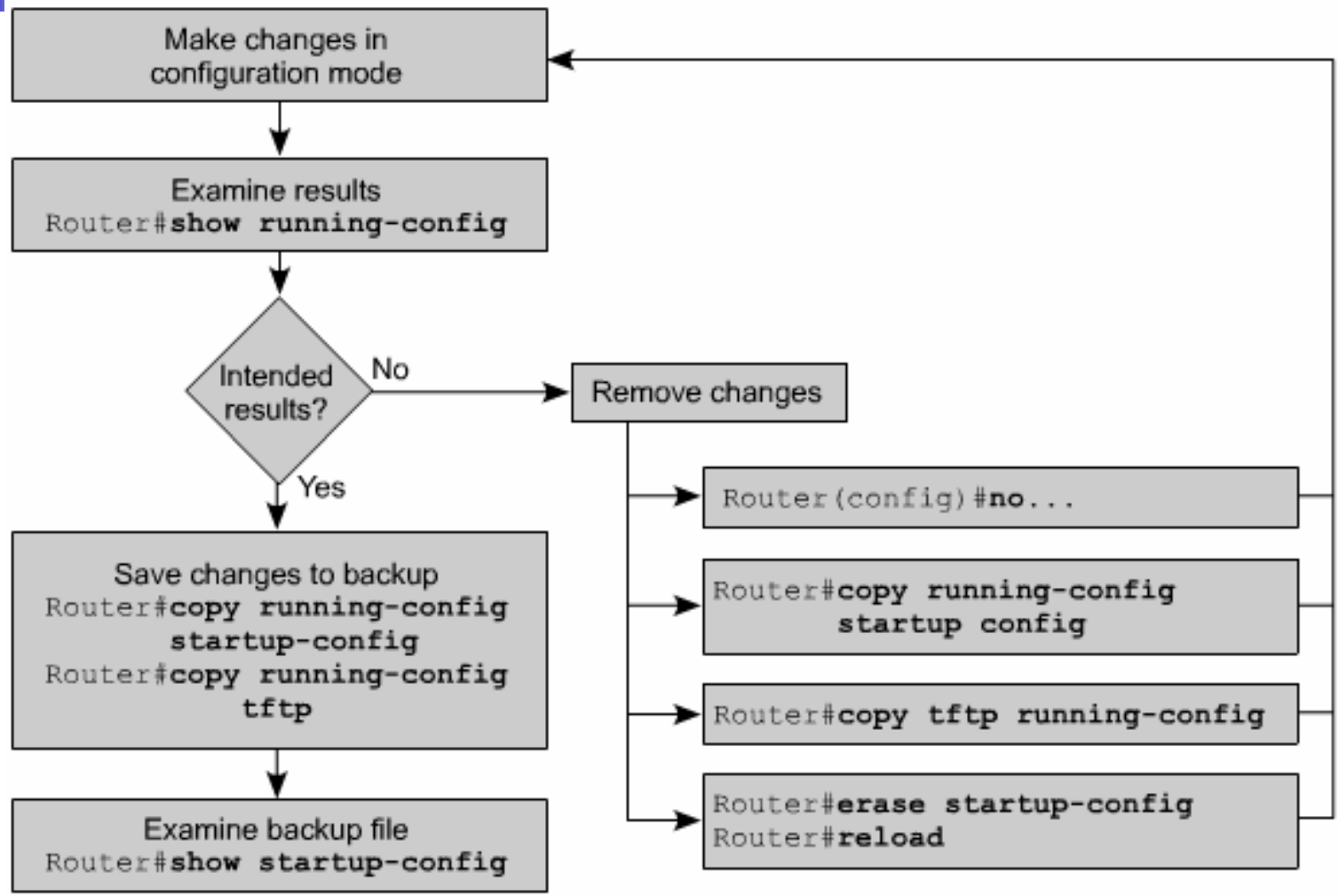
```
Router#copy running-config tftp
Remote host []? 131.108.2.155
Name of configuration file to write[tokyo-config]?tokyo.2
Write file tokyo.2 to 131.108.2.155? [confirm] y
Writing tokyo.2 !!!!!! [OK]
```

Router

```
Router#copy tftp running-config
Host or network configuration file [host]?
IP address of remote host [255.255.255.255]? 131.108.2.155
Name of configuration file [Router-config]? tokyo.2
Configure using tokyo.2 from 131.108.2.155? [confirm] y
Booting tokyo.2 from 131.108.2.155:!! [OK-874/16000 bytes]
tokyo#
```

Cấu hình cho Router

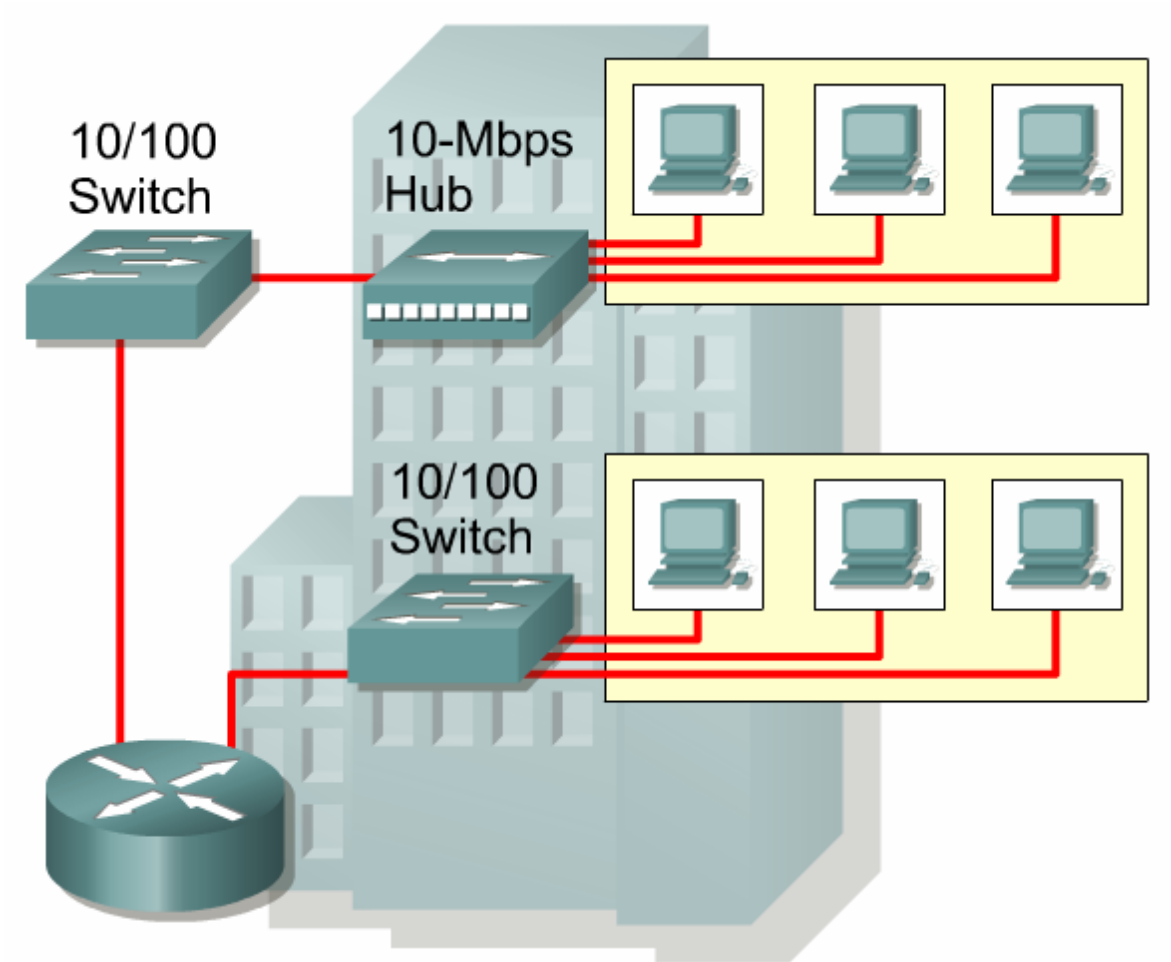
Sơ đồ tổng quát



SWITCH (bộ chuyển mạch)

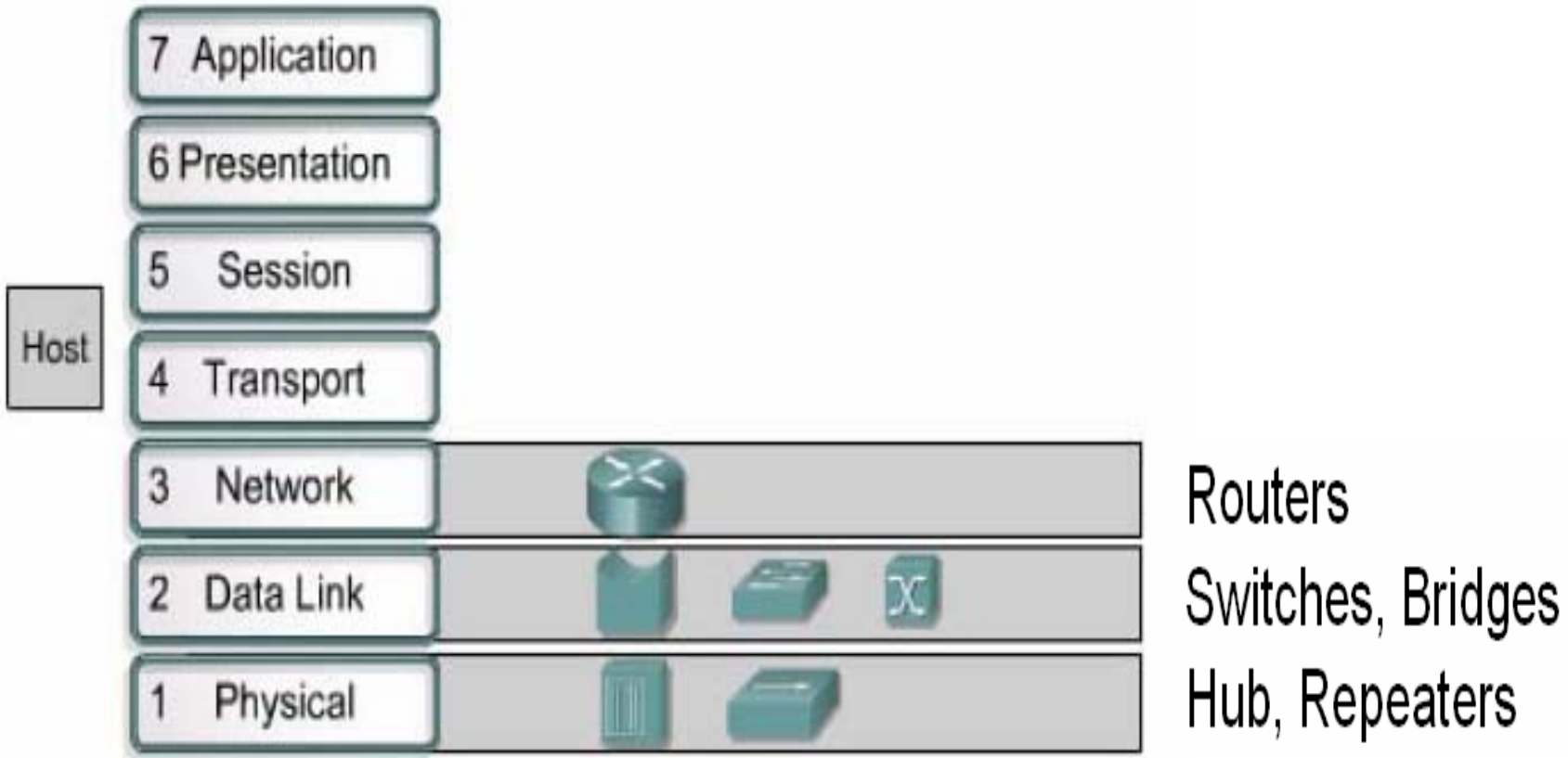
1. Các khái niệm về chuyển mạch
2. Thiết kế mạng LAN
3. Cấu hình Switch
4. Giao thức Spanning Tree
5. VLANs và VTP

Các khái niệm về chuyển mạch
Mạng LAN ngày nay



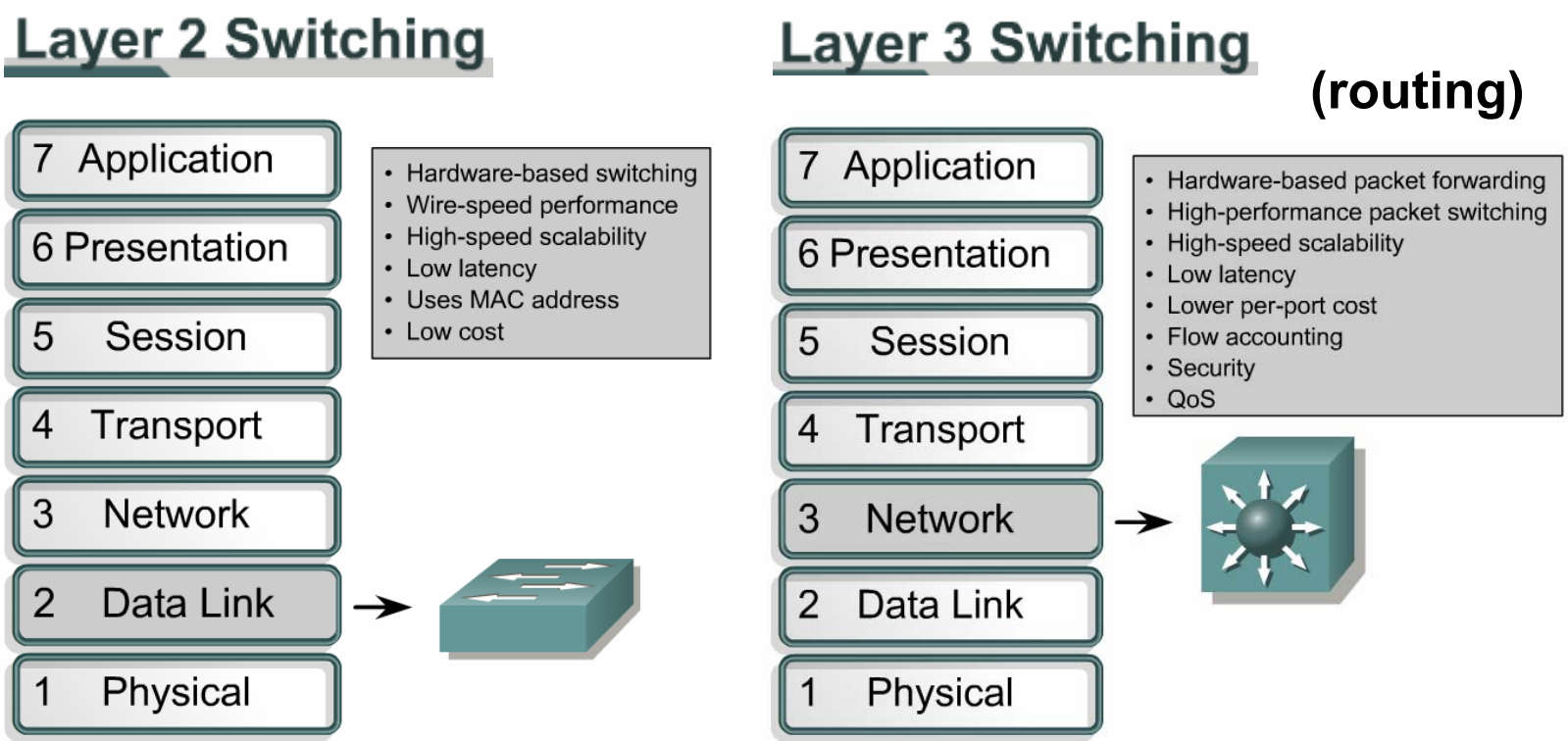
Các khái niệm về chuyển mạch

Chức năng hoạt động theo lớp của các thiết bị mạng

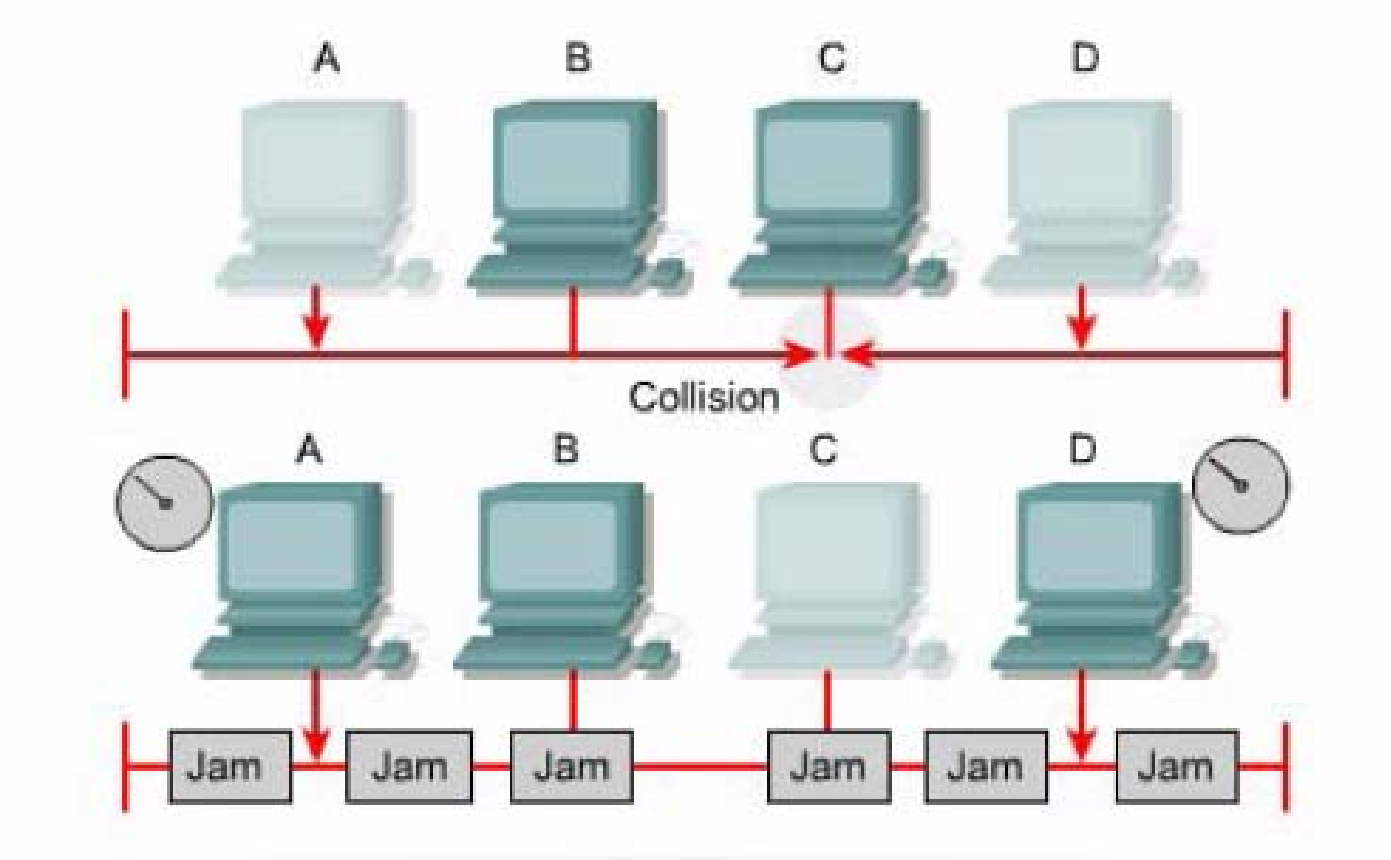


Các khái niệm về chuyển mạch

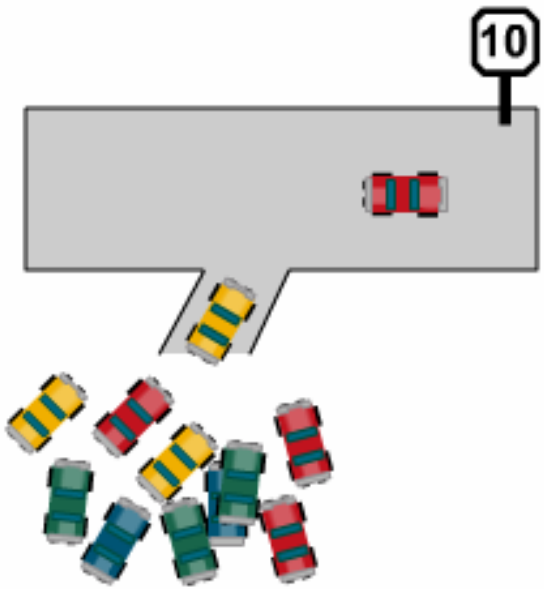
Chức năng hoạt động theo lớp của các thiết bị mạng



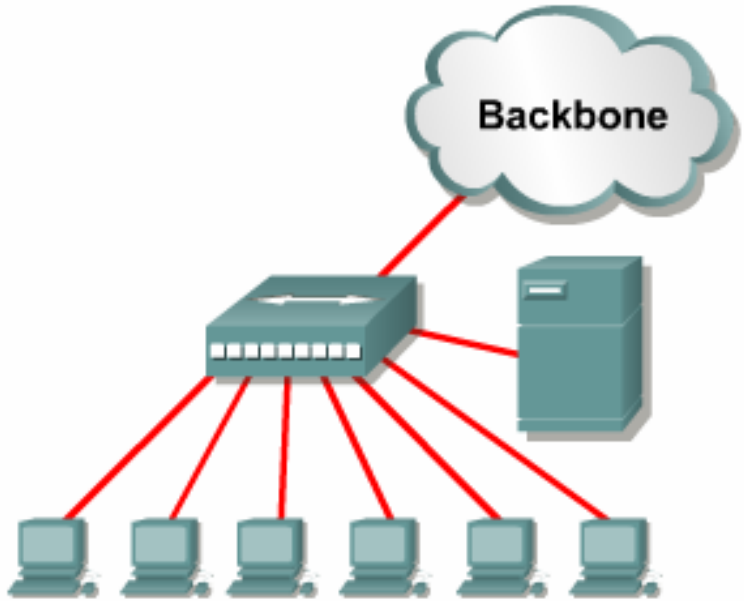
Các khái niệm về chuyển mạch
Đụng độ xảy ra trong mạng



Các khái niệm về chuyển mạch
Kết nối user bằng Hub

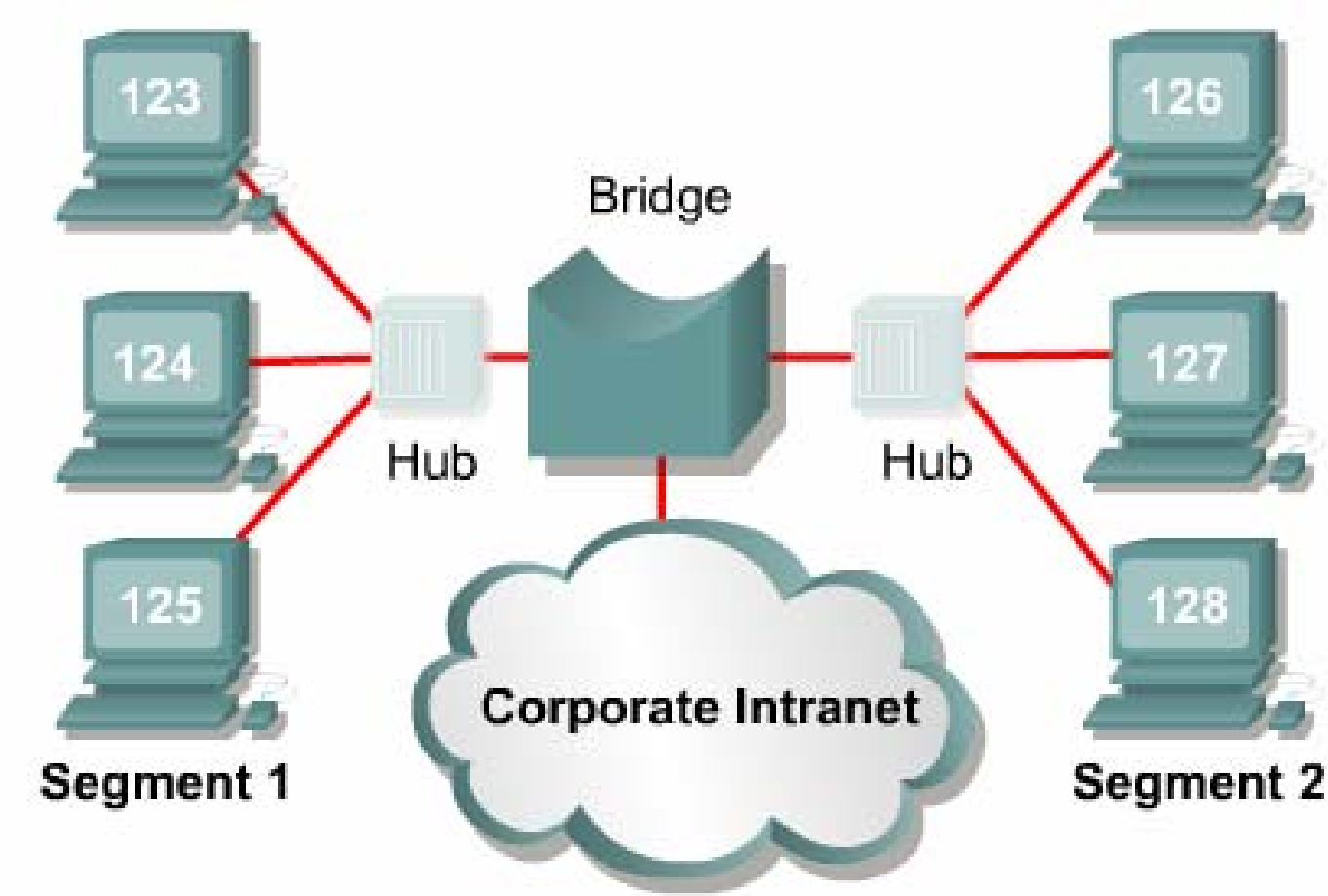


One device sending
at a time



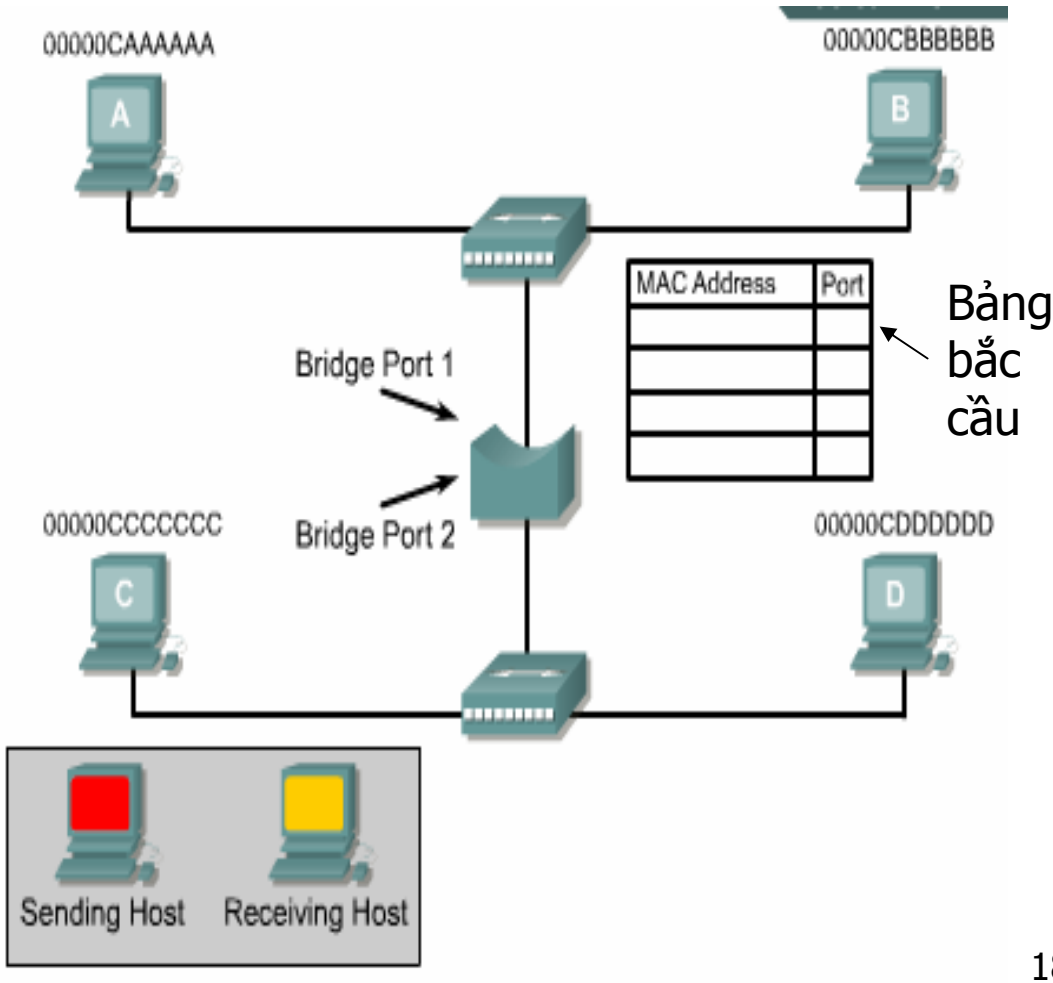
Each node shares 10 Mbps

Các khái niệm về chuyển mạch
Kết nối user bằng Bridge

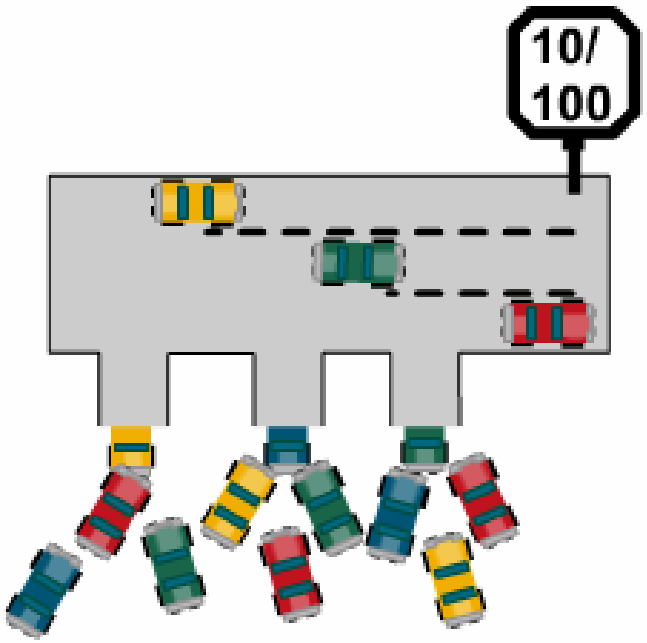


Các khái niệm về chuyển mạch
Layer 2 Bridging (Bắc cầu ở lớp 2)

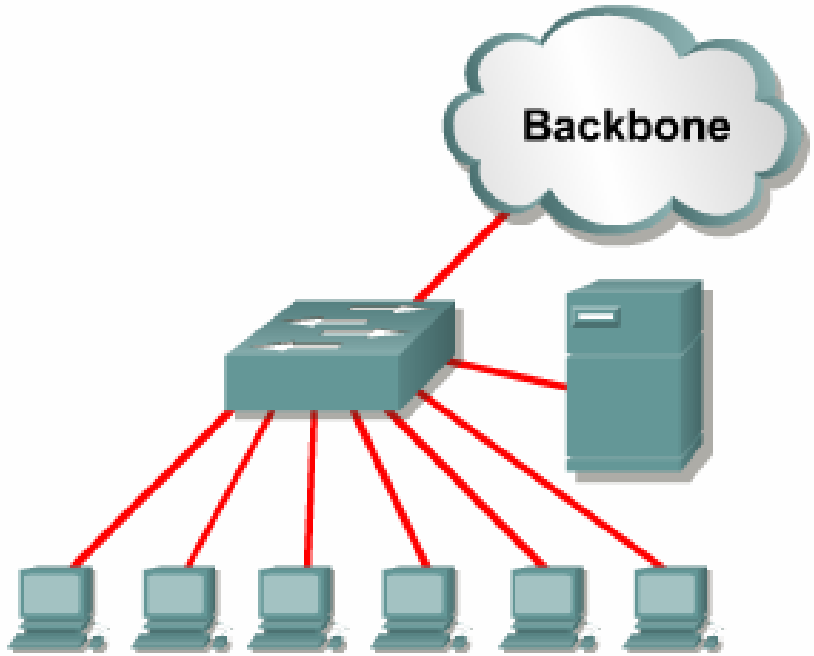
- Ethernet là một môi trường chia sẻ, chỉ một node có thể truyền số liệu vào một thời điểm
- Tăng số lượng host trên một segment, xác suất đụng độ tăng, đưa đến kết quả có nhiều hoạt động truyền lại hơn.
- Giải pháp: chia segment lớn thành nhiều segment nhỏ.



Các khái niệm về chuyển mạch
Kết nối user bằng Switch



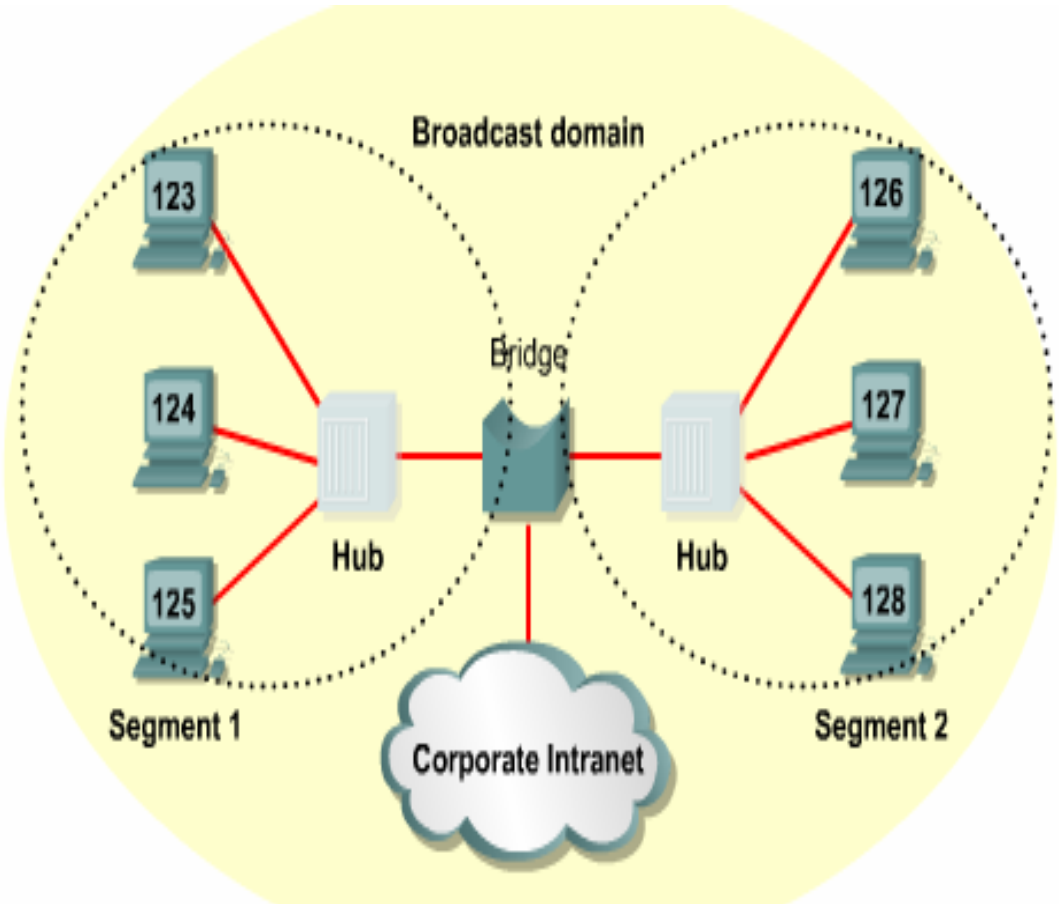
Multiple devices sending
at the same time



Each node has 10/100 Mbps

Các khái niệm về chuyển mạch
Layer 2 Switching (chuyển mạch ở lớp 2)

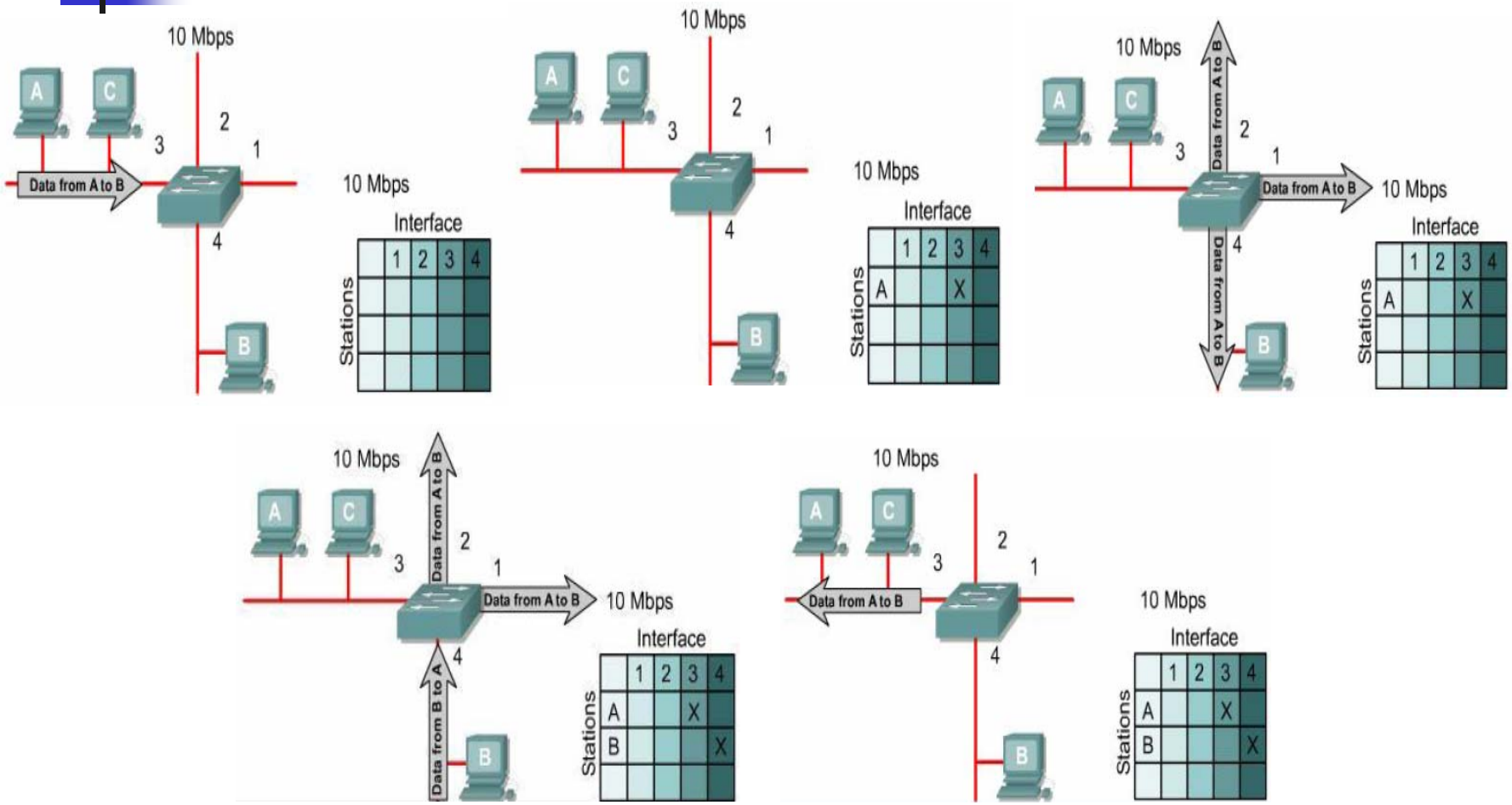
- Một bridge chỉ có hai port và chia một miền đụng độ thành hai phần.
- Bridge hoạt động dựa trên địa chỉ MAC và không ảnh hưởng đến địa chỉ lớp 3. Bridge chia miền đụng độ chứ không ảnh hưởng đến miền quảng bá.



Các khái niệm về chuyển mạch
Layer 2 Switching

- Một Switch về cơ bản là một bridge nhiều port, nó thiết lập động và duy trì một bảng CAM (Content Addressable Memory) lưu trữ tất cả thông tin MAC cho mỗi port.
- Khi nhận được gói tin, Switch sẽ kiểm tra địa chỉ nguồn của gói tin đã có trong bảng MAC chưa. Nếu chưa, nó sẽ thêm địa chỉ MAC này vào trong bảng MAC.
- Tiếp theo Switch sẽ kiểm tra địa chỉ đích của gói tin có trong bảng MAC chưa. Nếu chưa có thì nó sẽ gởi gói tin đi tất cả các cổng (ngoại trừ cổng gởi gói tin vào). Ngược lại Switch sẽ kiểm tra port đích và port nguồn, nếu trùng nhau thì nó sẽ loại bỏ gói tin, nếu khác nhau thì nó sẽ gởi gói tin đến port đích tương ứng.

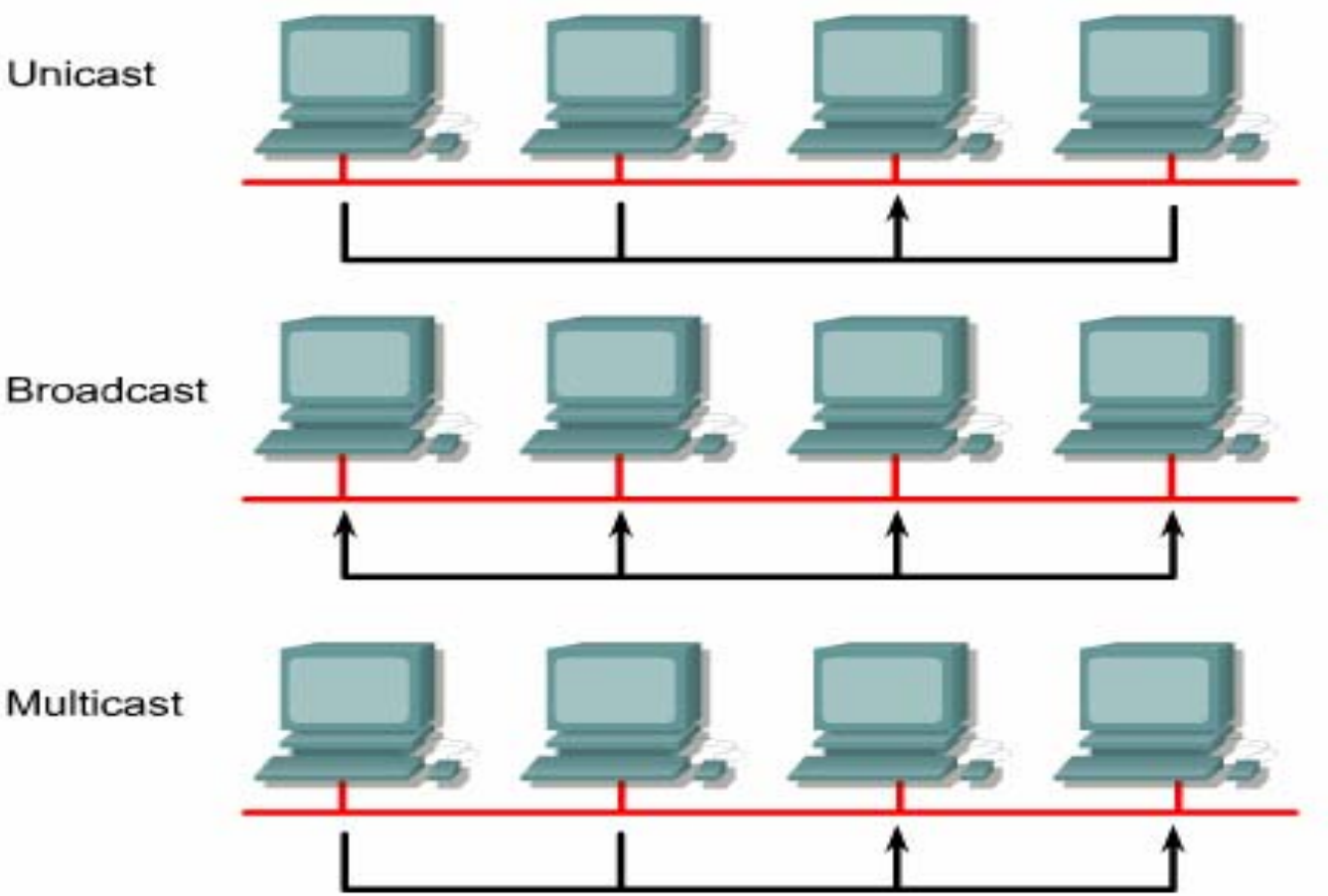
Các khái niệm về chuyển mạch
Hoạt động chuyển mạch của Switch



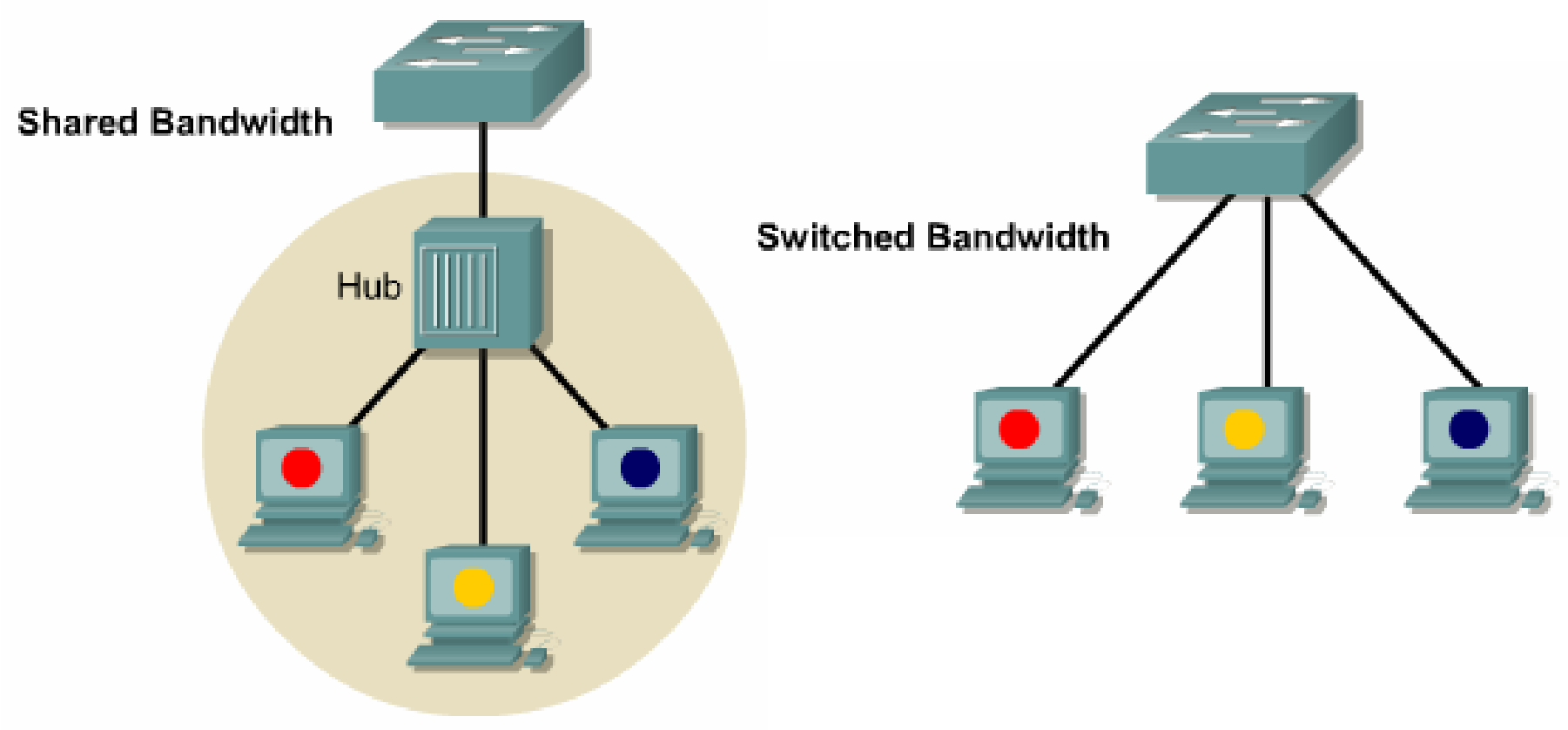
Các khái niệm về chuyển mạch
Các phương pháp chuyển mạch

- Store-and-Forward: Một switch nhận toàn bộ frame trước khi gởi nó ra ngoài port đích nhằm đảm bảo frame nhận được là tốt trước khi chuyển ra ngoài.
- Cut-Through: Một switch có thể bắt đầu truyền frame ngay khi nhận được MAC addr đích.
- Fragment-Free: Dung hòa giữa chế độ cut-through và store-and-forward, đọc 64 byte đầu tiên, bao gồm cả frame header và bắt đầu chuyển mạch trước khi toàn bộ data và checksum được đọc.

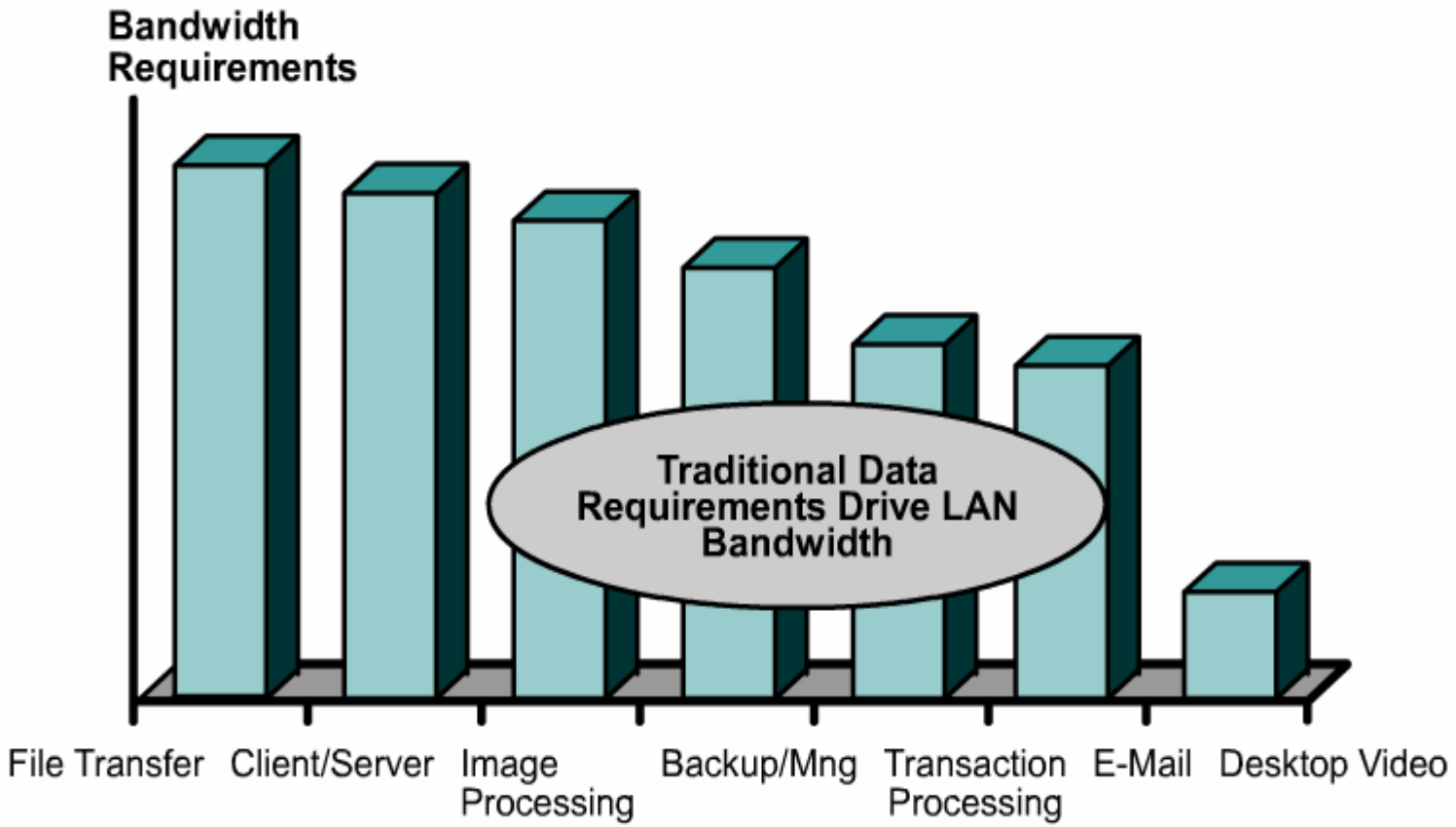
Các khái niệm về chuyển mạch
Các phương pháp chuyển mạch



Các khái niệm về chuyển mạch
Chia sẻ băng thông

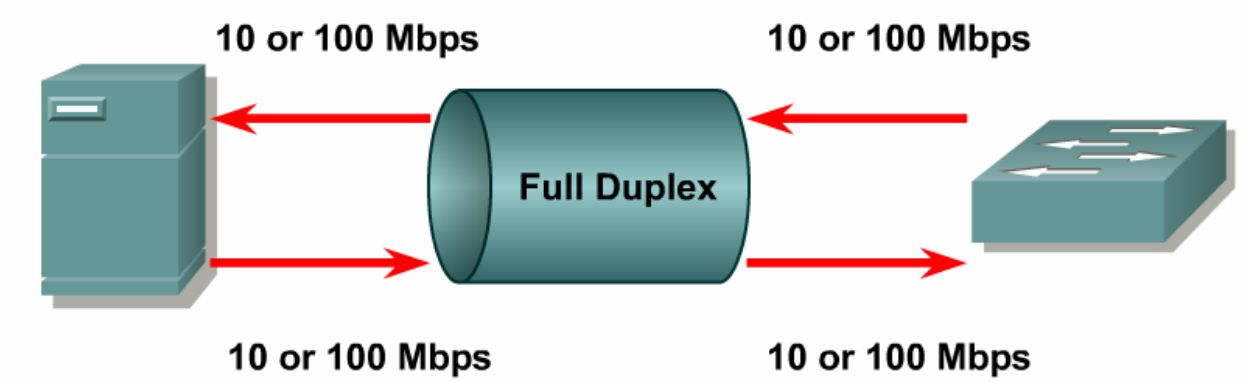


Các khái niệm về chuyển mạch
Các yếu tố tác động đến hiệu suất mạng



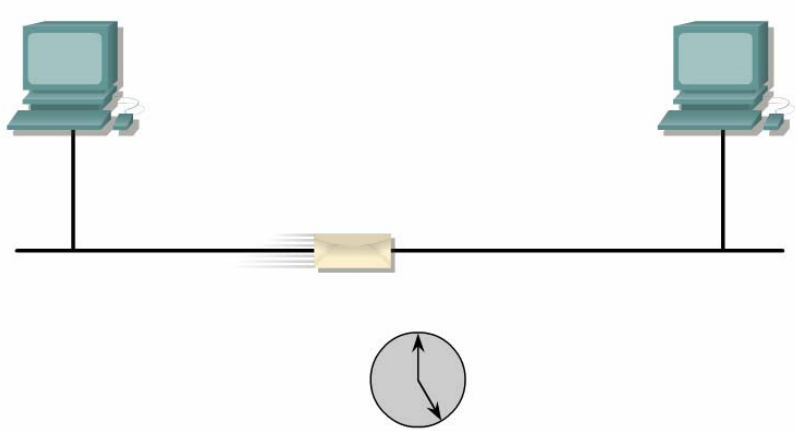
Các khái niệm về chuyển mạch
Chế độ song công và bán song công

- **Simplex Transmission**
- **Half-duplex Transmission**
- **Full-duplex Transmission**



Các khái niệm về chuyển mạch
Latency

- Latency là thời gian trễ tính từ thời điểm một frame bắt đầu rời khỏi nguồn cho đến thời điểm frame đi đến đích. Thời gian này bị ảnh hưởng bởi:
  - Trễ đường truyền.
  - Trễ mạch điện tử.
  - Trễ phần mềm.
  - Trễ bởi nội dung của frame.
  - ...



Các khái niệm về chuyển mạch
Miền đụng độ và miền quảng bá

- Miền đụng độ (Collision domain)
  - Là các segment mạng vật lý được kết nối ở đó có các đụng độ có thể xảy ra.
  - Mỗi khi một đụng độ xảy ra trên mạng, tất cả các hoạt động truyền dừng lại trong một khoảng thời gian.
  - Thiết bị thuộc lớp 1 không chia tách miền đụng độ mà chỉ mở rộng miền đụng độ.
  - Thiết bị thuộc lớp 2 và 3 chia tách miền đụng độ thành các miền đụng độ nhỏ hơn (sự phân đoạn mạng – segmentation).

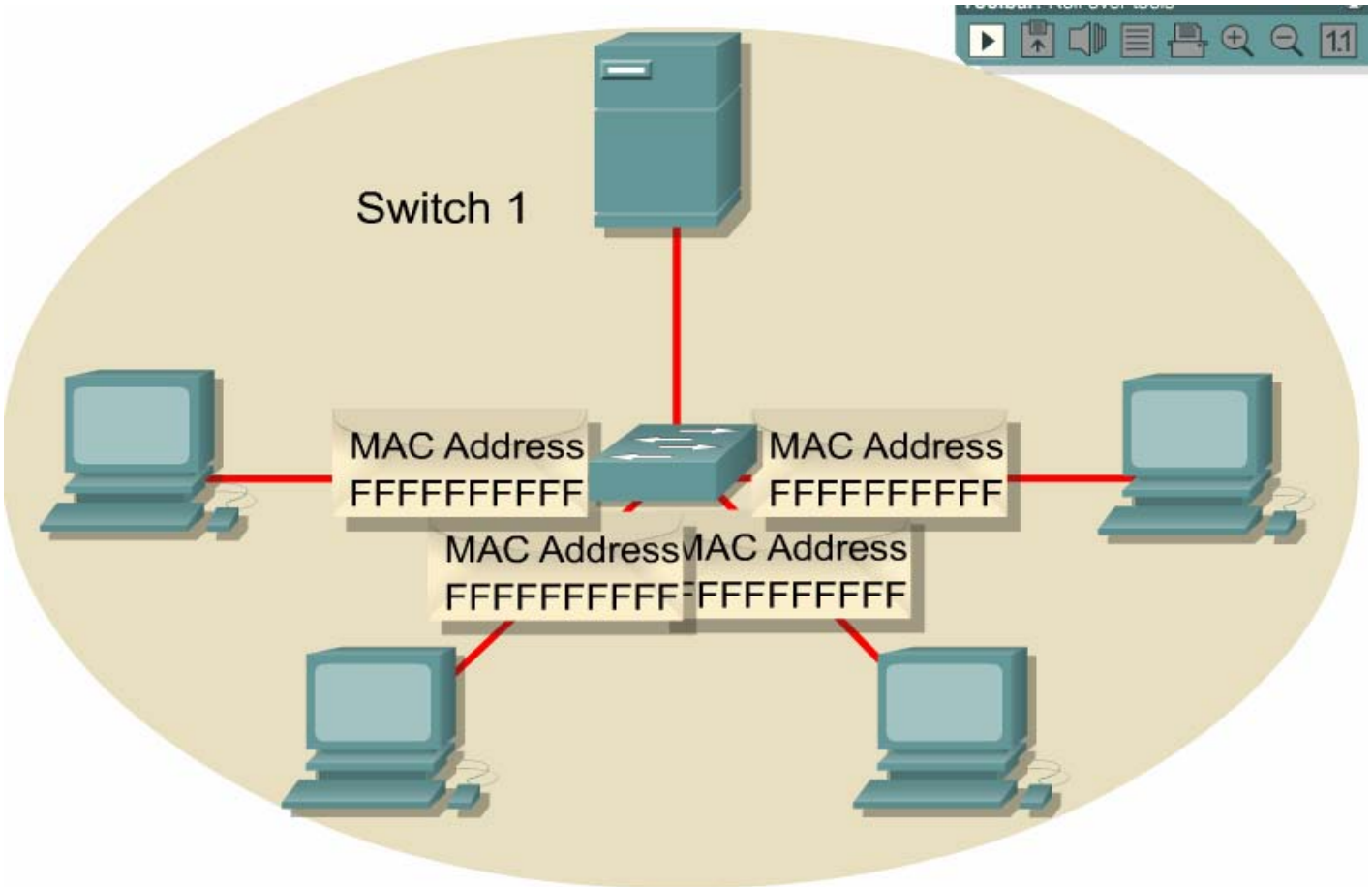
Các khái niệm về chuyển mạch
Miền đụng độ và miền quảng bá

- Miền quảng bá (Broadcast domain)
  - Một broadcast domain là một nhóm các miền đụng độ được kết nối bởi các thiết bị lớp 2.
  - Các broadcast nếu quá mức có thể làm giảm hiệu suất của mạng LAN.
  - Broadcast được kiểm soát bởi thiết bị lớp 3. Router có thể phân chia các broadcast domain.

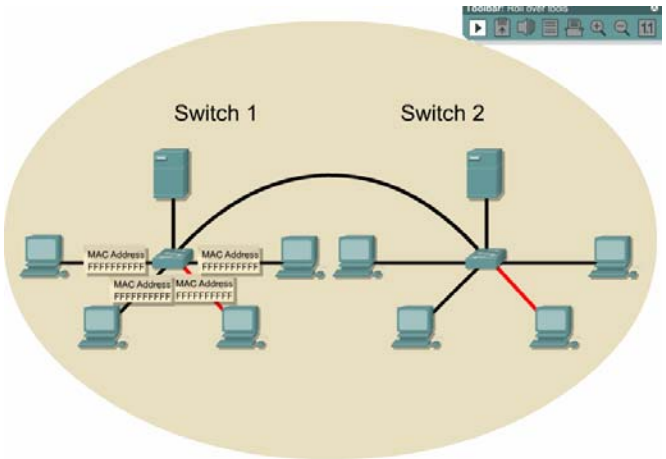
Các khái niệm về chuyển mạch
Miền đụng độ và miền quảng bá

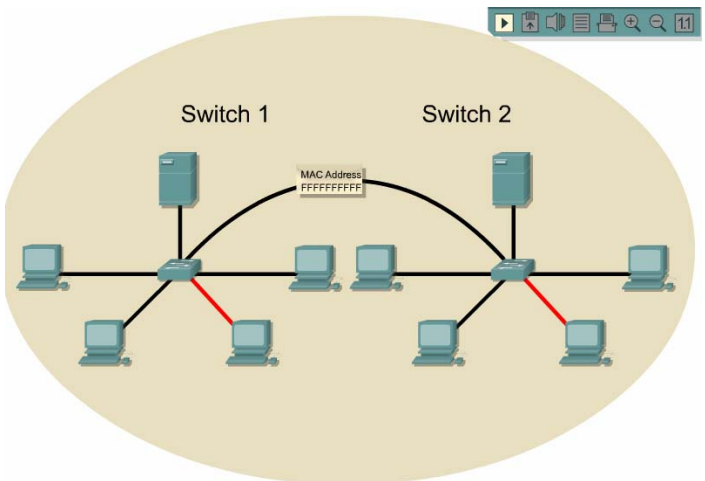
- Broadcast ở lớp 2
  - Khi một host cần truyền thông tới một host trên mạng, nó gởi một broadcast frame tới địa chỉ MAC đích là 0xFFFFFFFFFFFF.
  - Sự tích lũy lưu lượng broadcast có thể làm tràn ngập mạng và không còn băng thông cho ứng dụng truyền số liệu -> bão broadcast.
  - Các máy trạm broadcast để yêu cầu ARP khi cần định vị một địa chỉ MAC không có trong bảng ARP.
  - Các giao thức định tuyến cũng có thể gây ra broadcast. Mỗi 30 giây, RIPv1 dùng broadcast để truyền lại toàn bộ bảng định tuyến RIP đến các router khác.

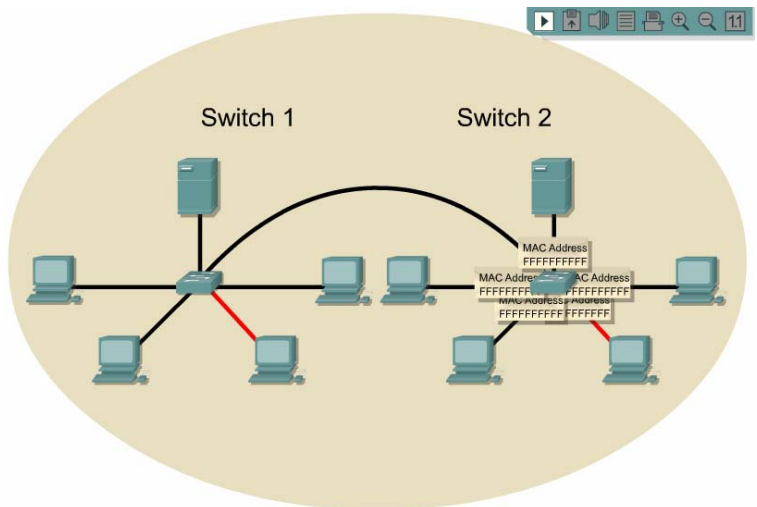
Các khái niệm về chuyển mạch
Miền đụng độ và miền quảng bá



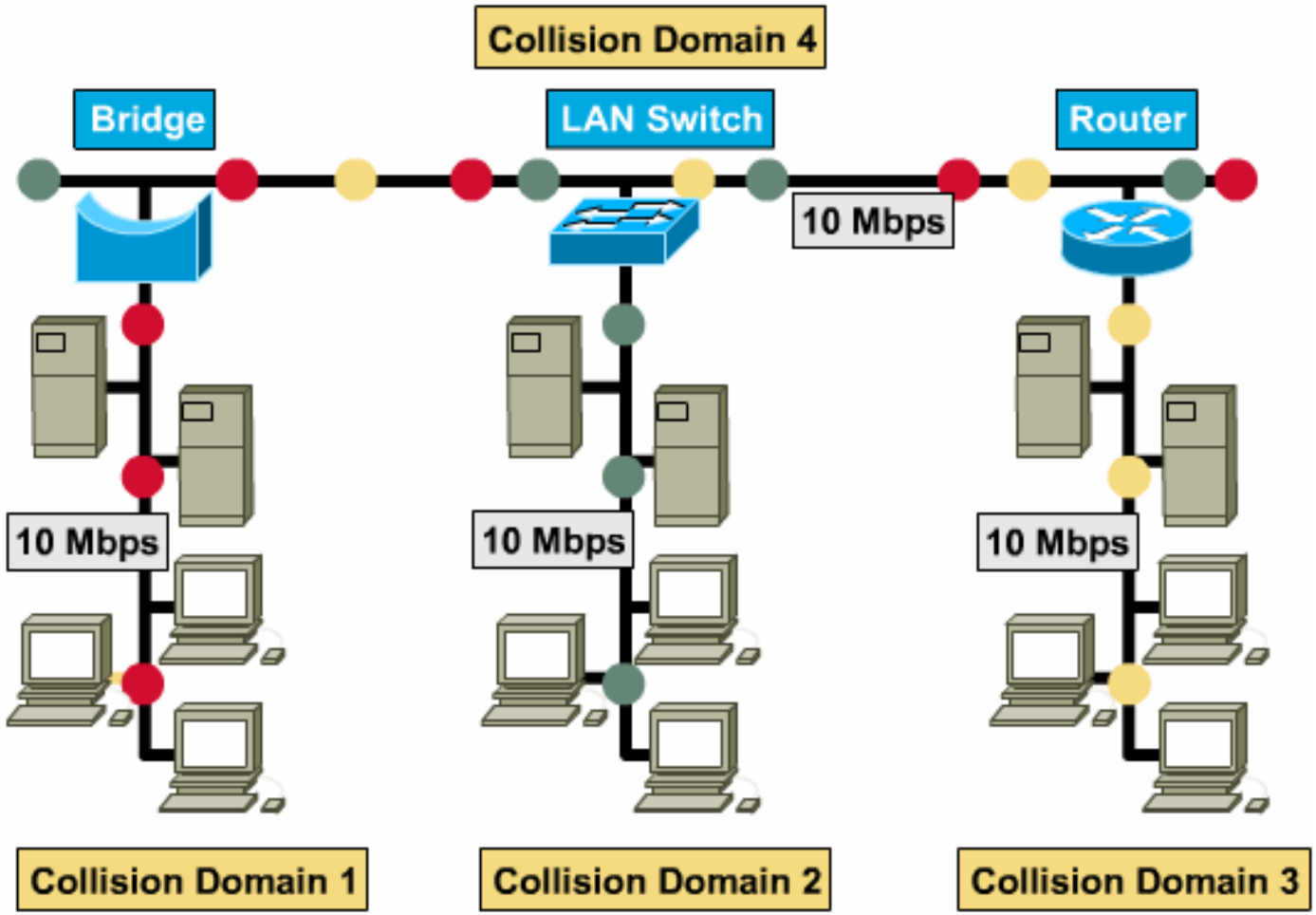
Các khái niệm về chuyển mạch
Miền đụng độ và miền quảng bá



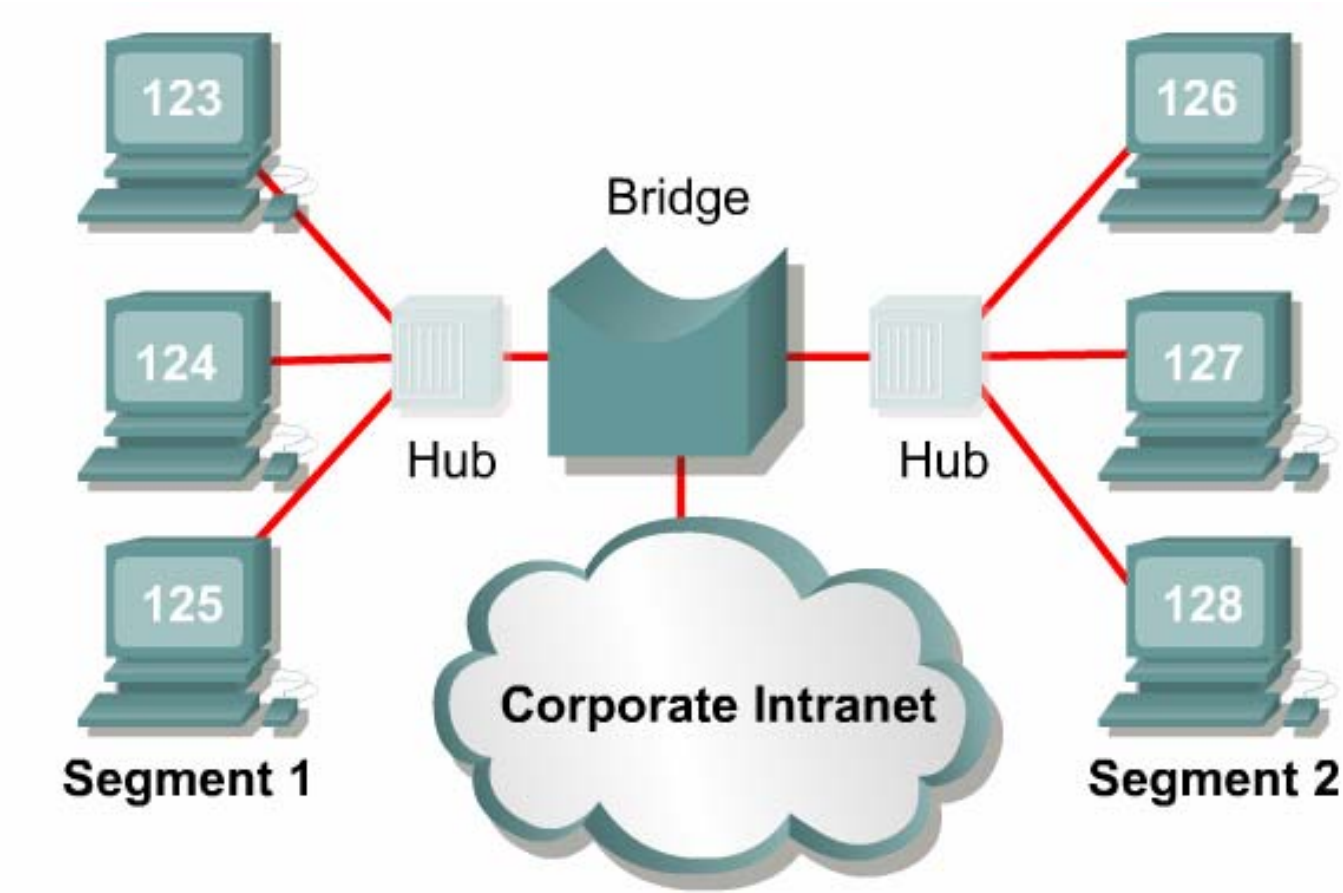




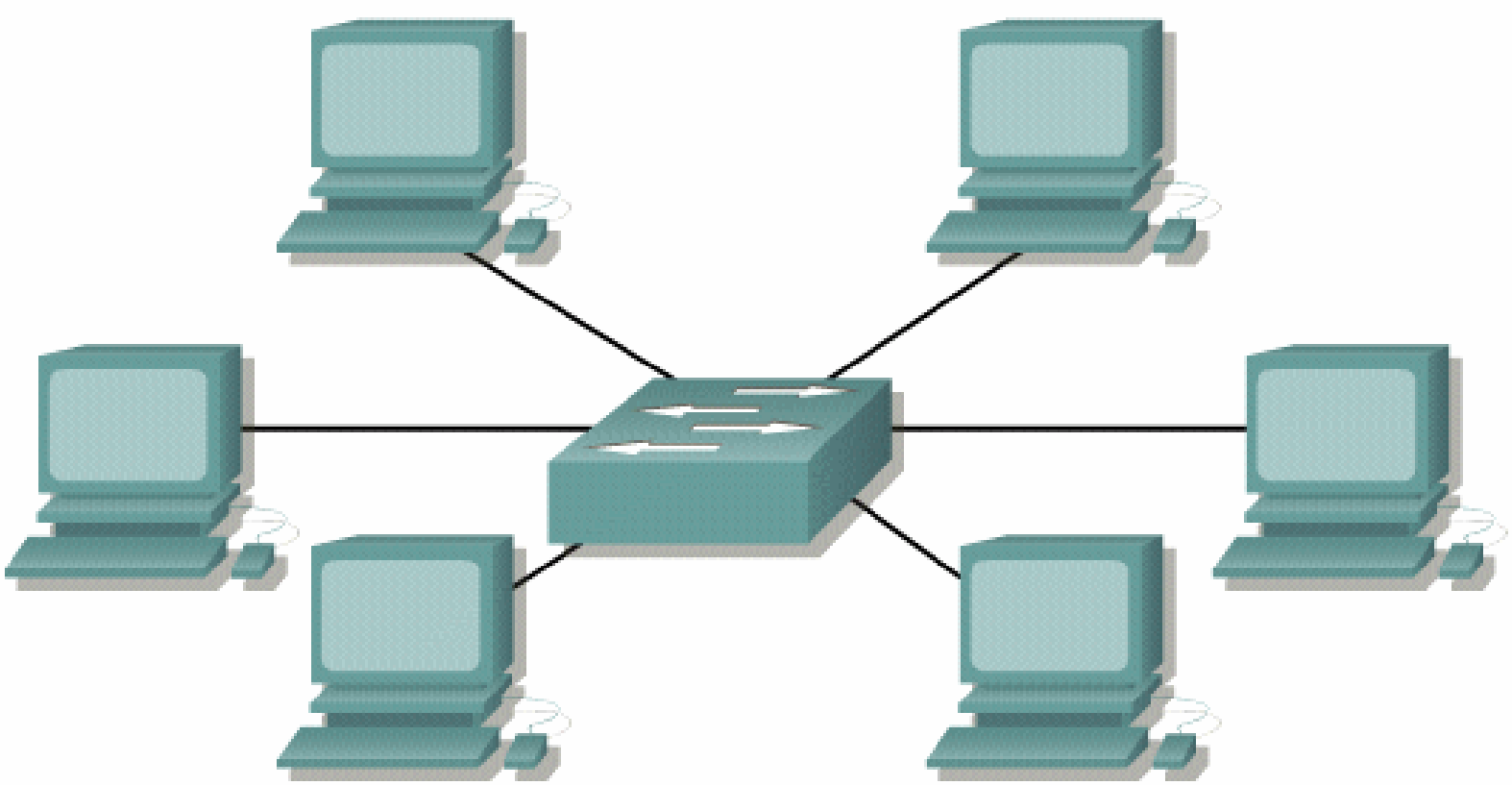
Các khái niệm về chuyển mạch
Phân đoạn mạng LAN



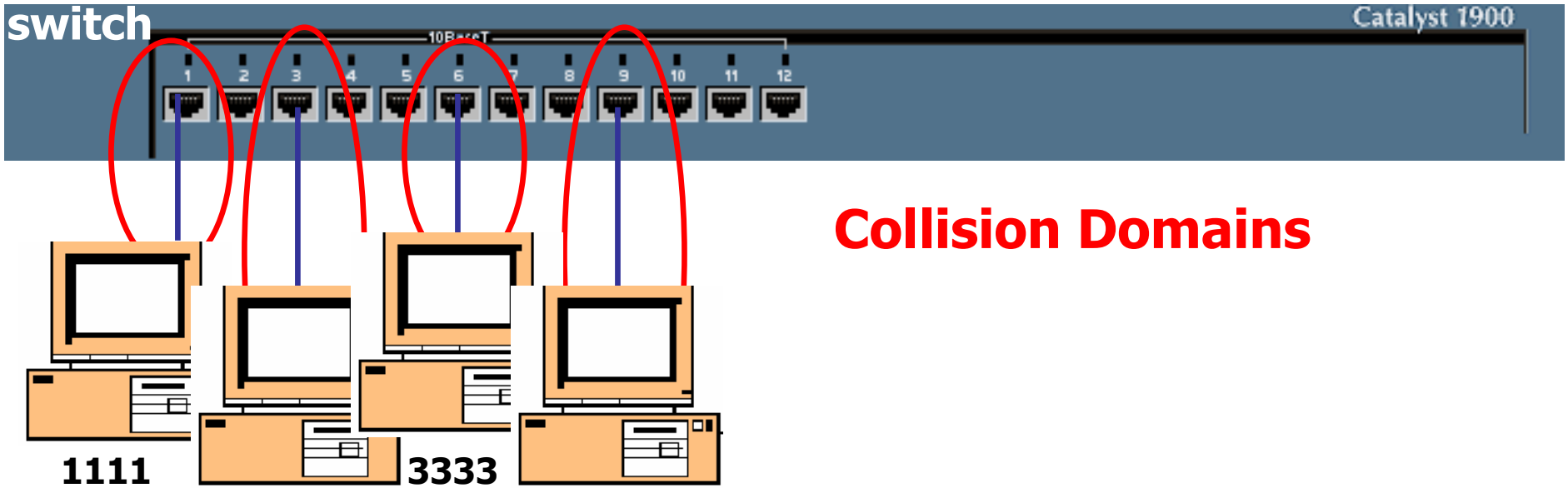
Các khái niệm về chuyển mạch
Phân đoạn mạng với Bridge



Các khái niệm về chuyển mạch
Phân đoạn mạng với Switch



Các khái niệm về chuyển mạch
Phân đoạn mạng với Switch

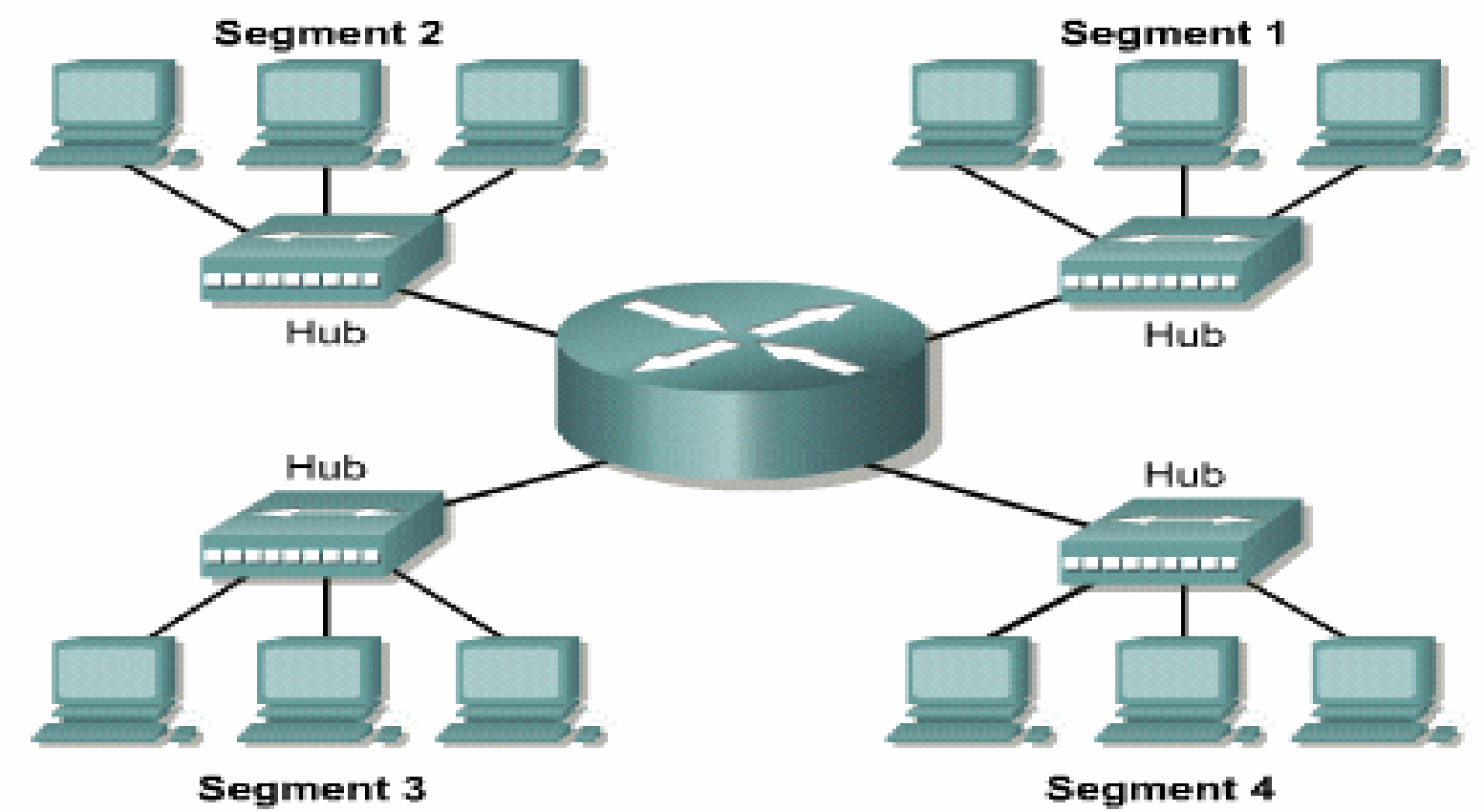


Collision Domains

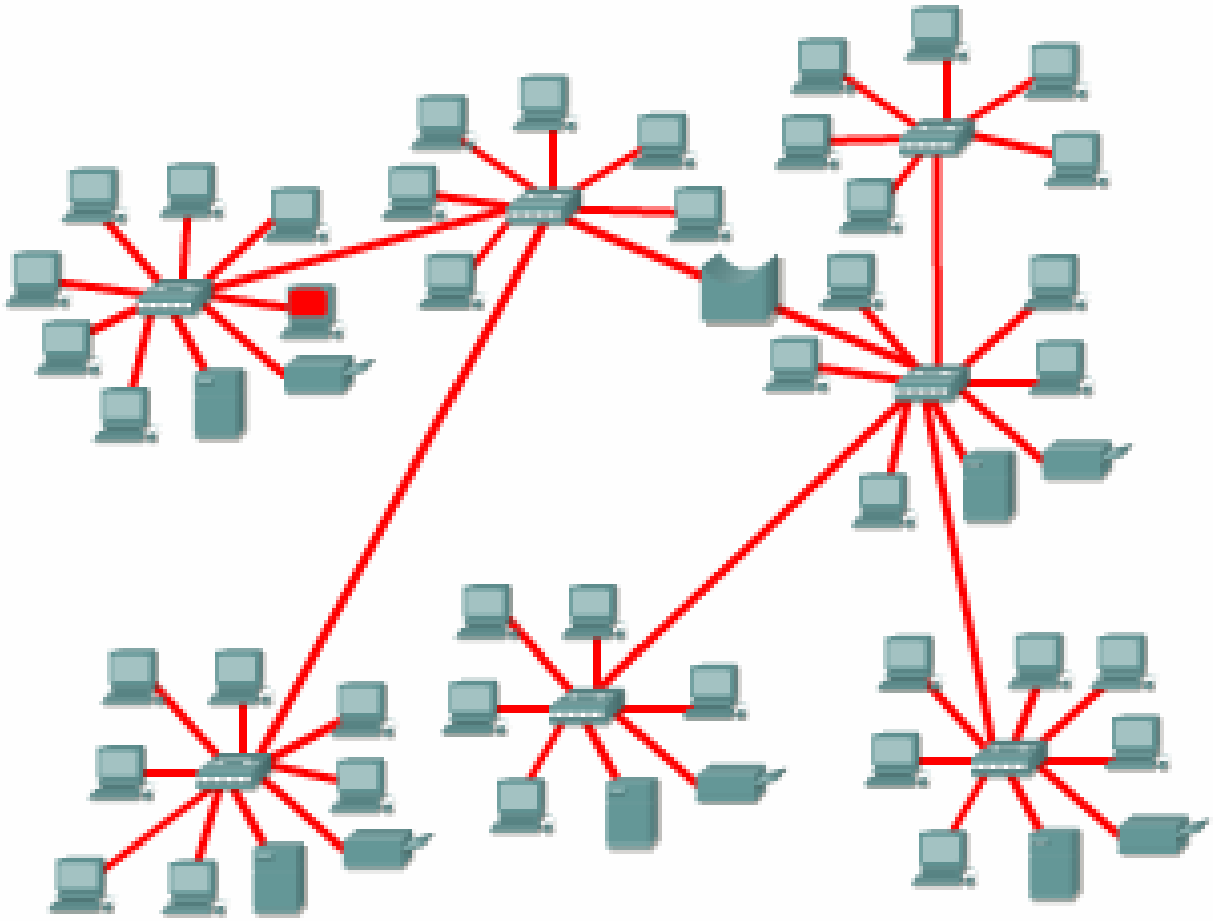
Abbreviated MAC addresses

2222 **4444**

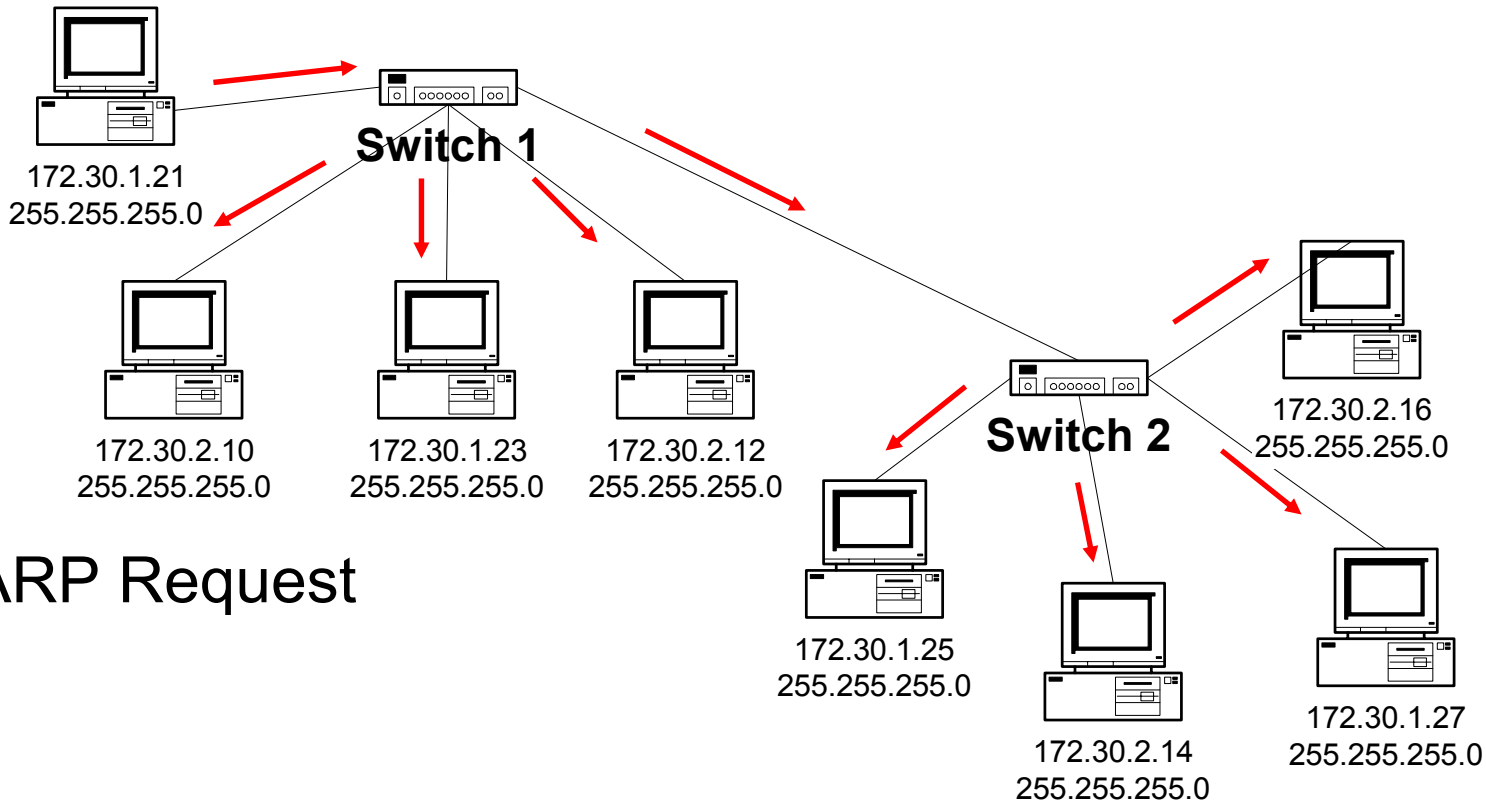
Các khái niệm về chuyển mạch
Phân đoạn mạng với Router



Các khái niệm về chuyển mạch
Layer 2 Broadcast

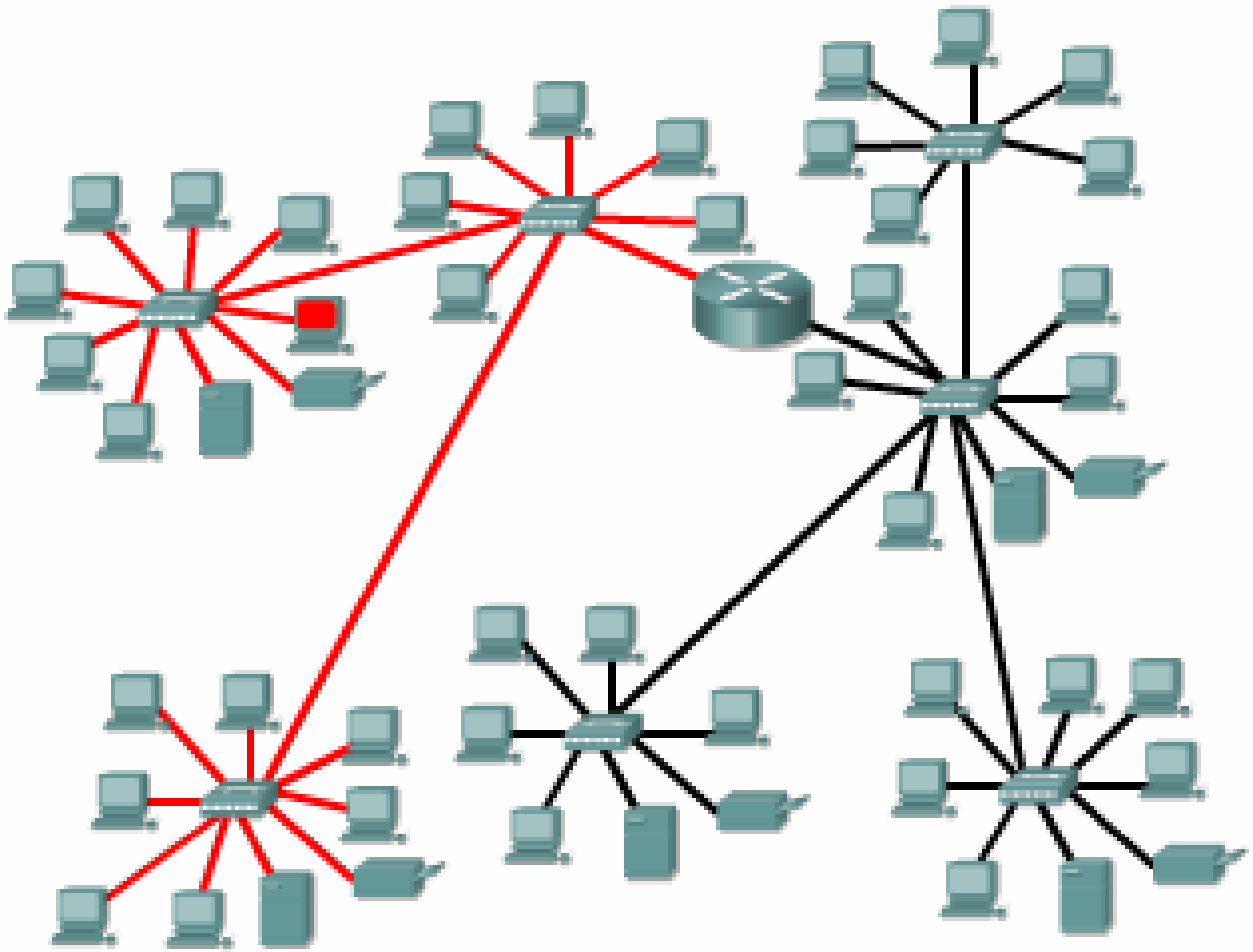


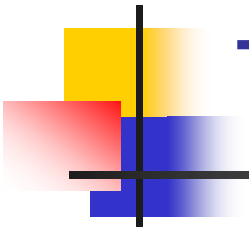
Các khái niệm về chuyển mạch
Broadcast Domain



- ARP Request

Các khái niệm về chuyển mạch
Broadcast Domain

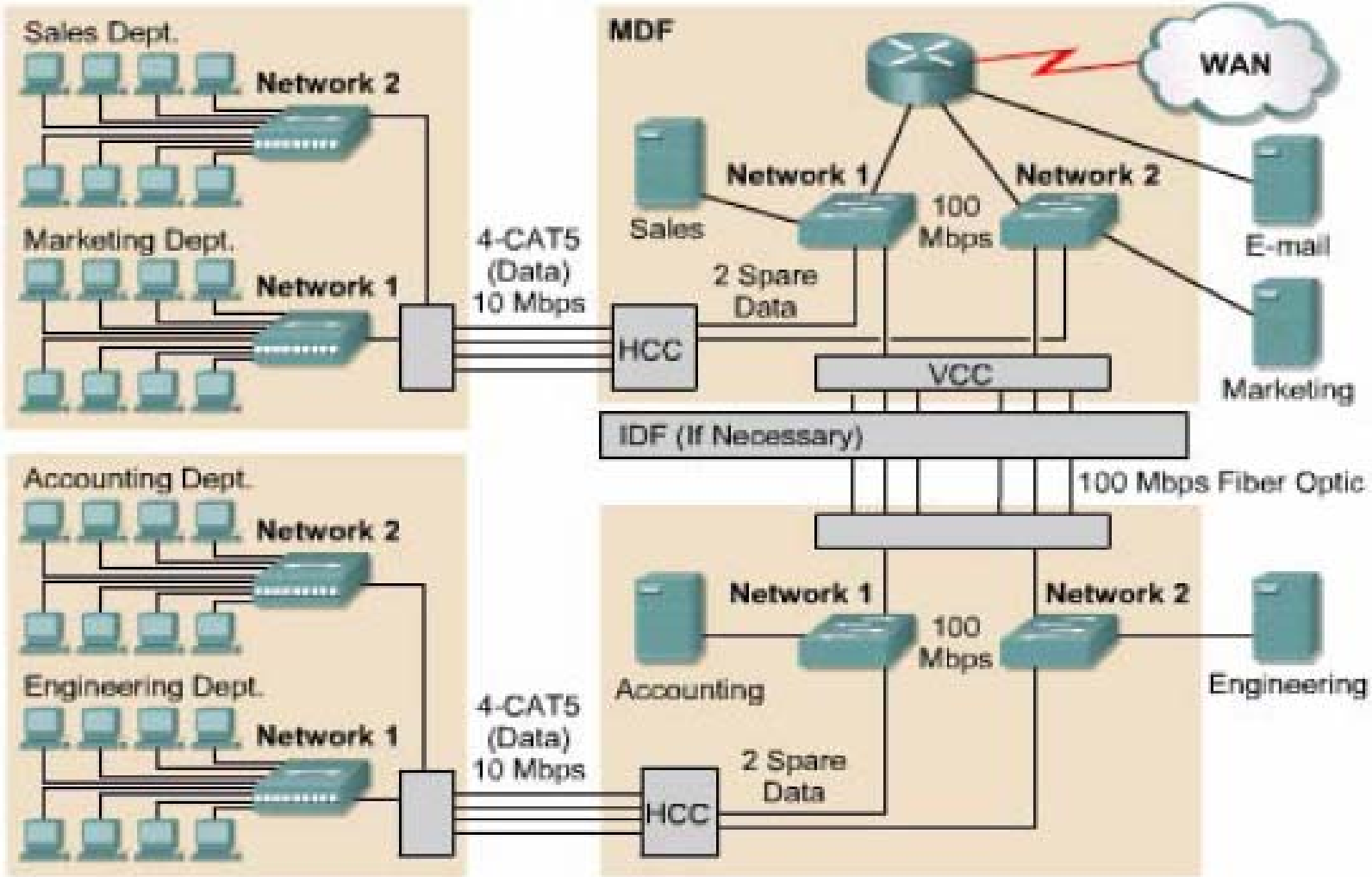




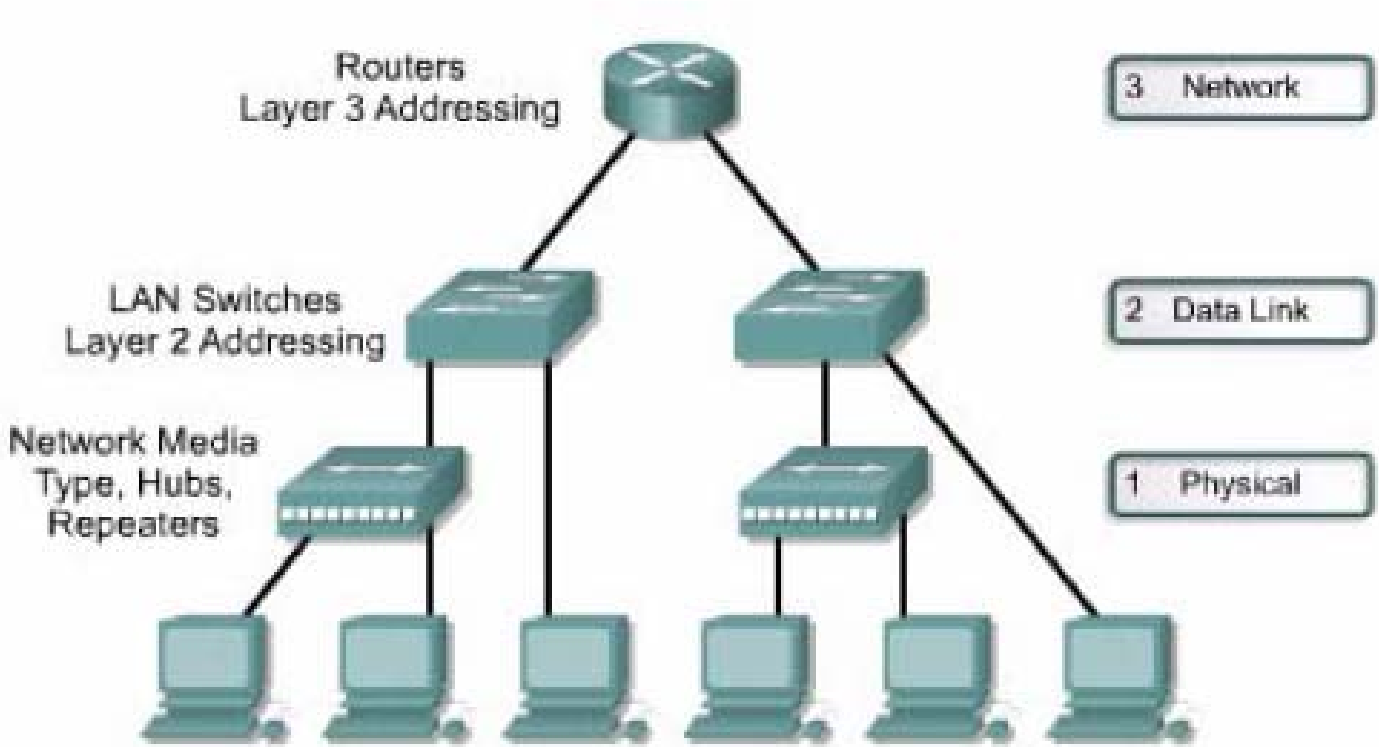
Thiết kế mạng LAN

- Các mục tiêu:
  - Khả năng hoạt động được
  - Khả năng mở rộng
  - Khả năng thích ứng
  - Khả năng quản lý
- Những điều cần quan tâm:
  - Chức năng và vị trí đặt server
  - Phát hiện đụng độ
  - Phân đoạn mạng
  - Miền quảng bá

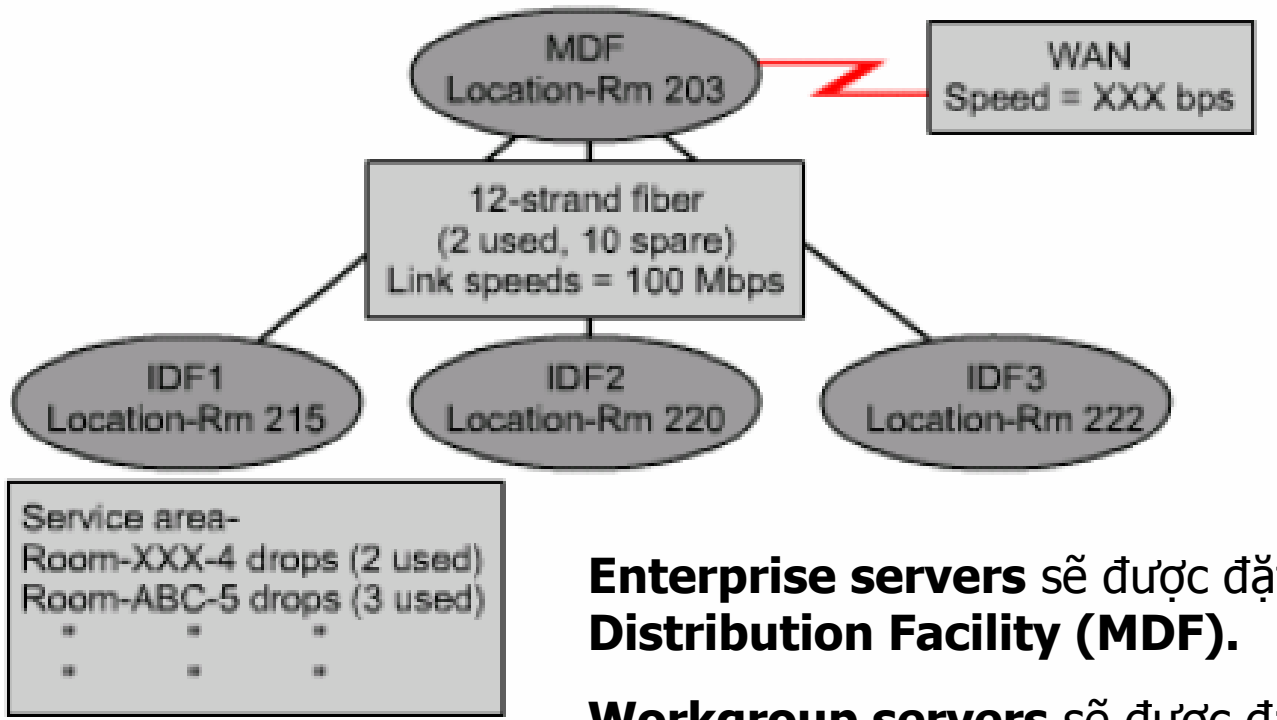
Thiết kế mạng LAN
Vị trí đặt server



Thiết kế mạng LAN
Sơ đồ mạng theo lớp OSI



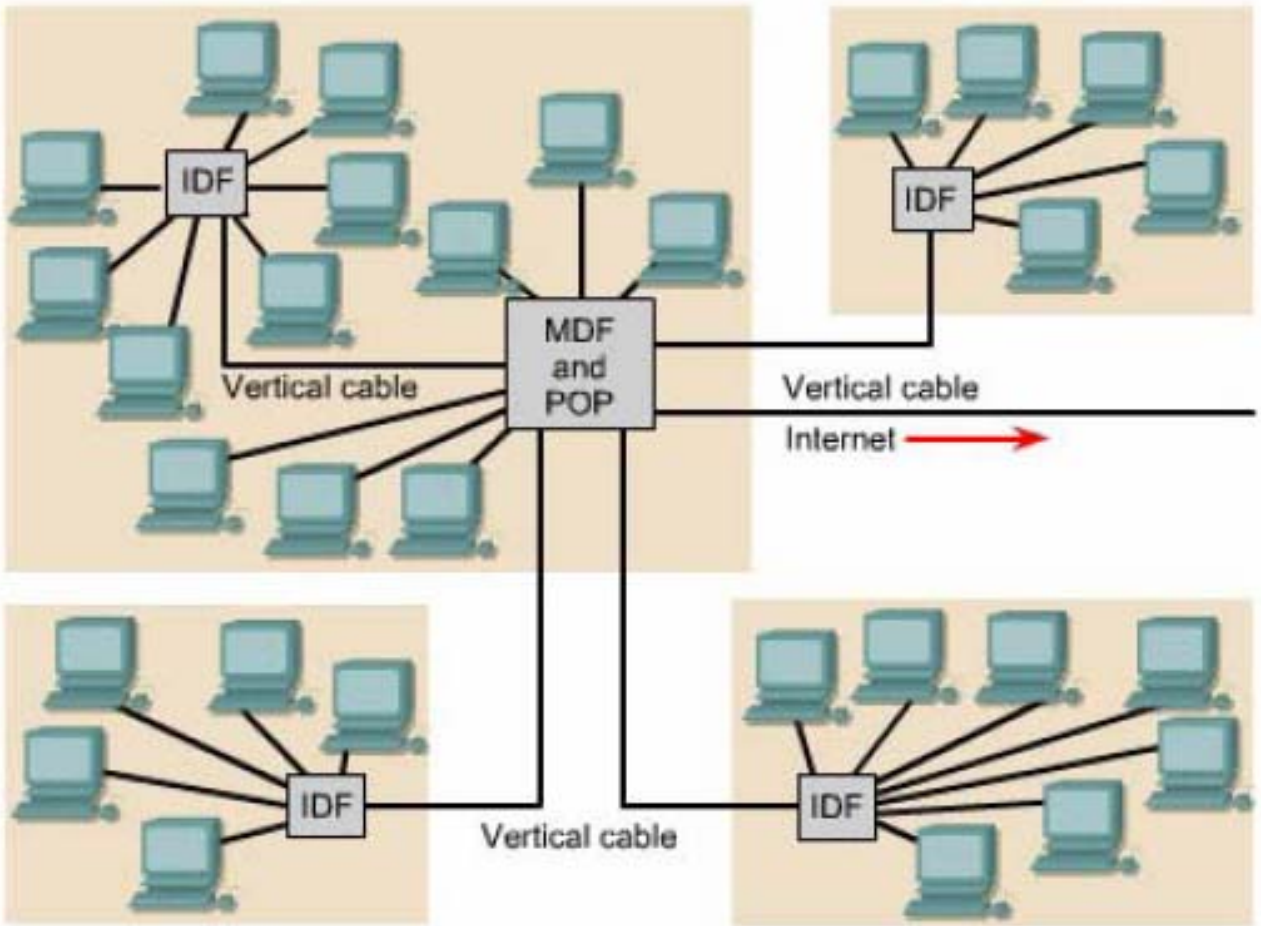
Thiết kế mạng LAN
Sơ đồ luận lý



Enterprise servers sẽ được đặt tại **Main Distribution Facility (MDF).**

Workgroup servers sẽ được đặt tại **Intermediate Distribution Facilities (IDFs)**

Thiết kế mạng LAN
Sơ đồ vật lý

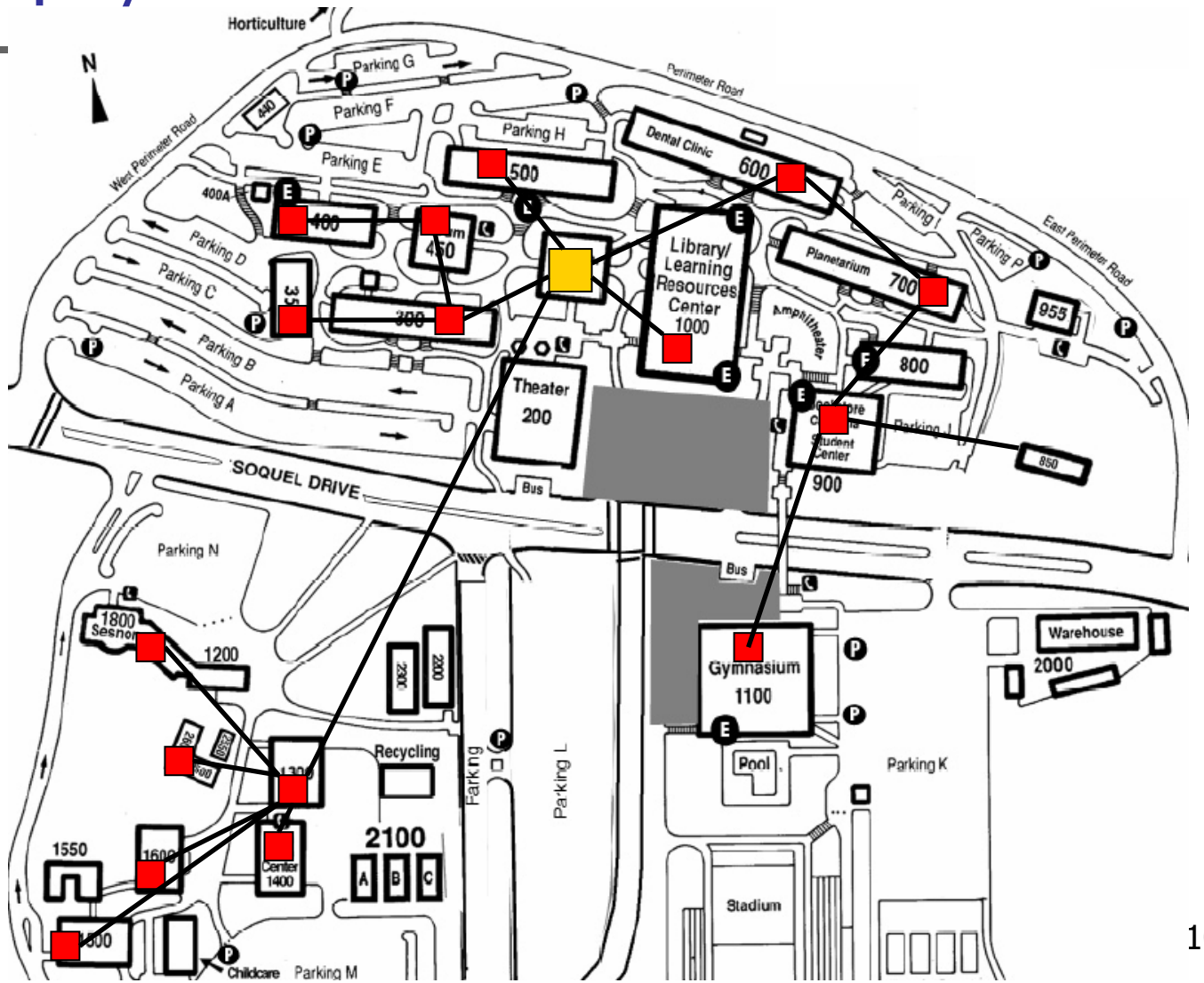


Thiết kế mạng LAN

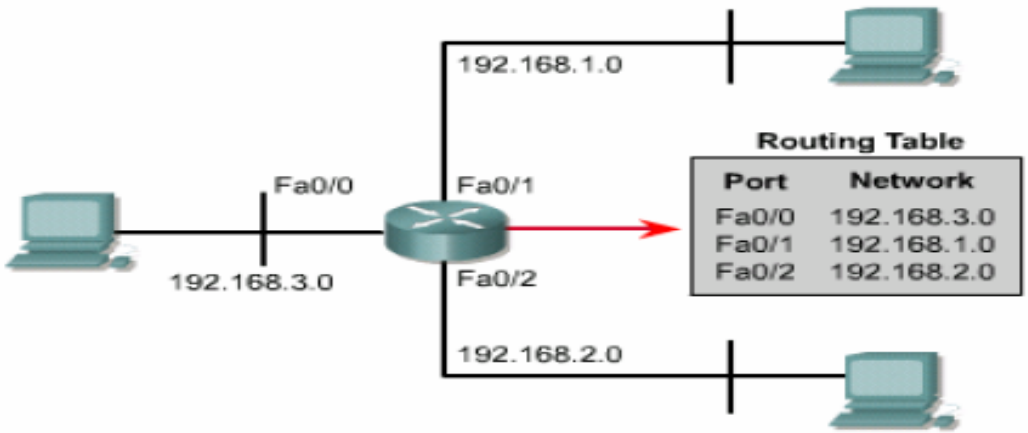
Sơ đồ vật lý

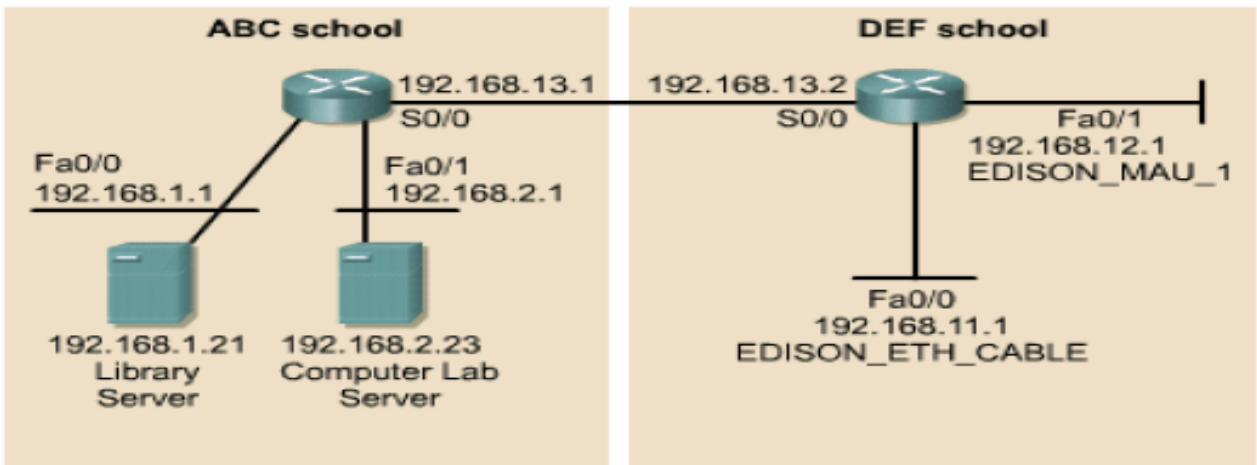
MDF

IDF



Thiết kế mạng LAN
Sơ đồ địa chỉ

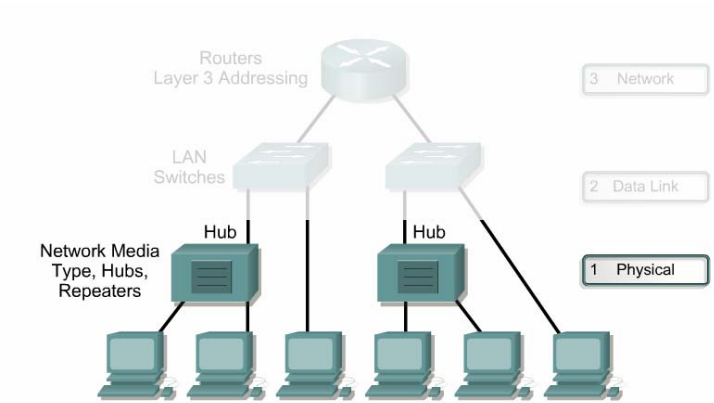


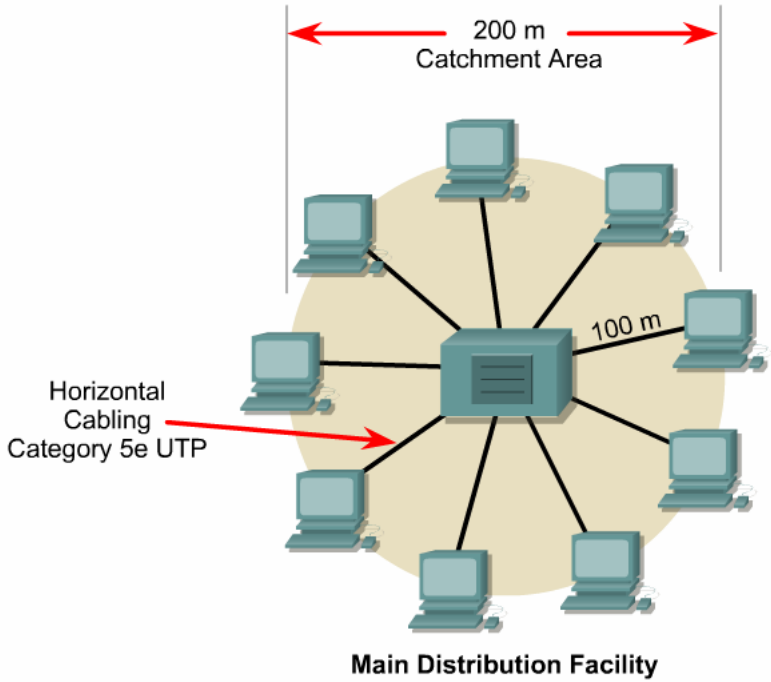


Thiết kế mạng LAN

Thiết kế Layer 1

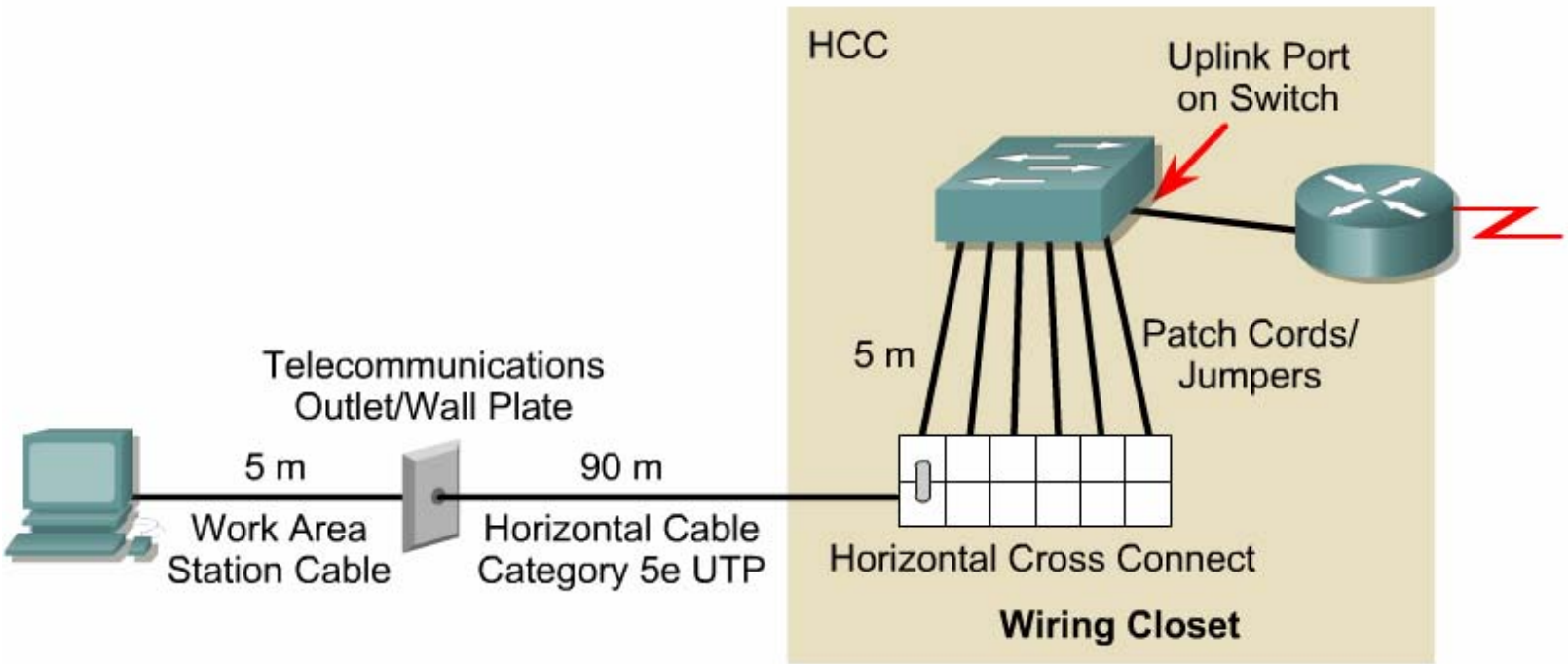
Characteristic	10BASE-T	10BASE-FL	100BASE-TX	100BASE-FX
Data rate	10 Mbps	10 Mbps	100Mbps	100 Mbps
Signaling method	Baseband	Baseband	Baseband	Baseband
Medium type	Category 5e UTP	Fiber-optic	Category 5e UTP	Multi-mode fiber (two strands)
Maximum length	100 meters	2000 meters	100 meters	2000 meters





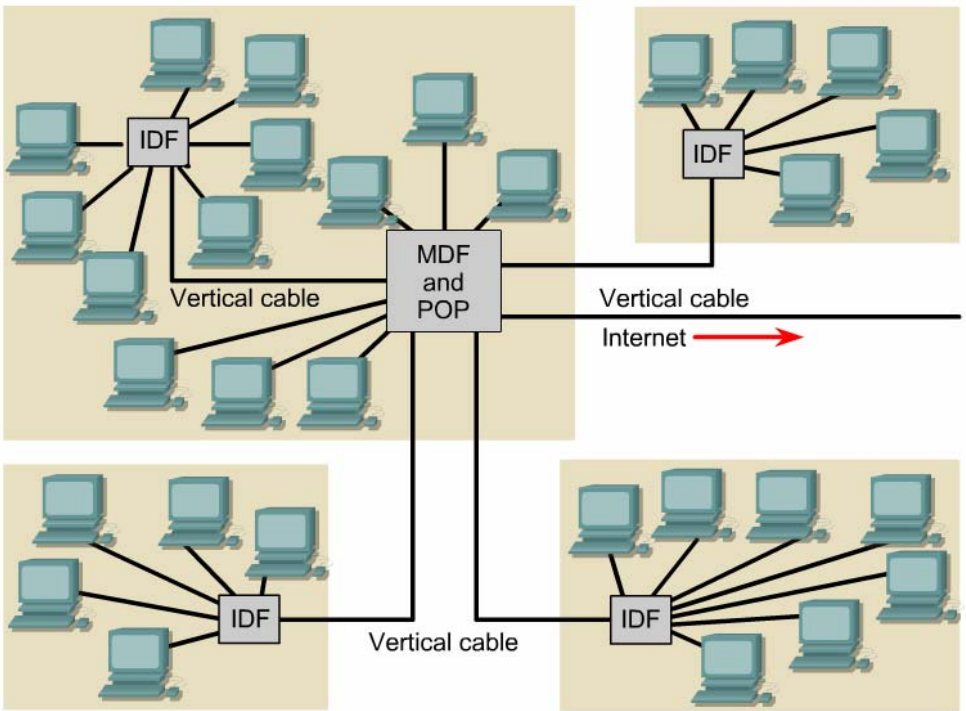
Thiết kế mạng LAN

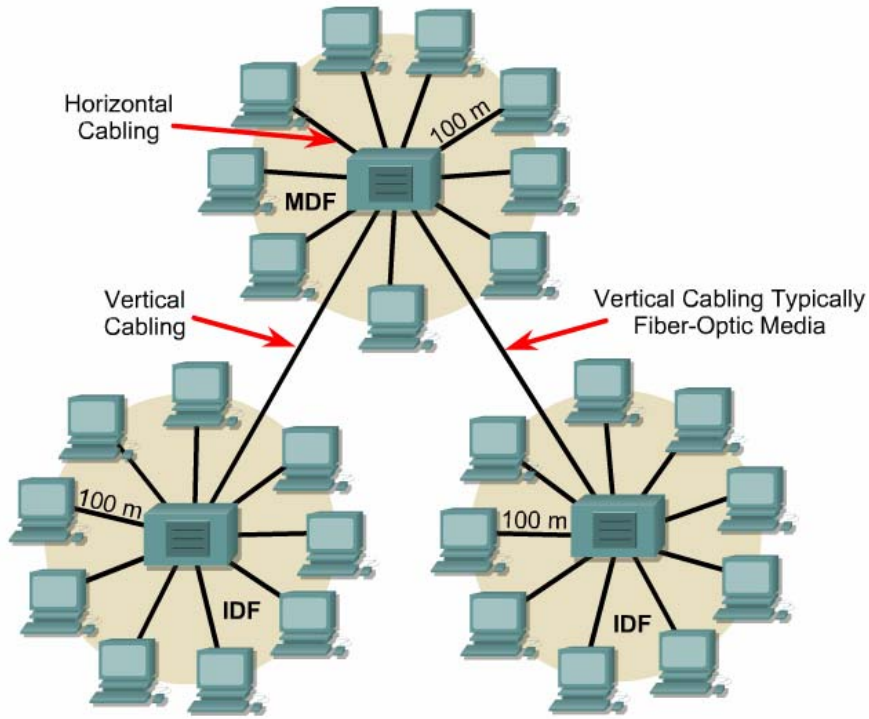
Thiết kế Layer 1



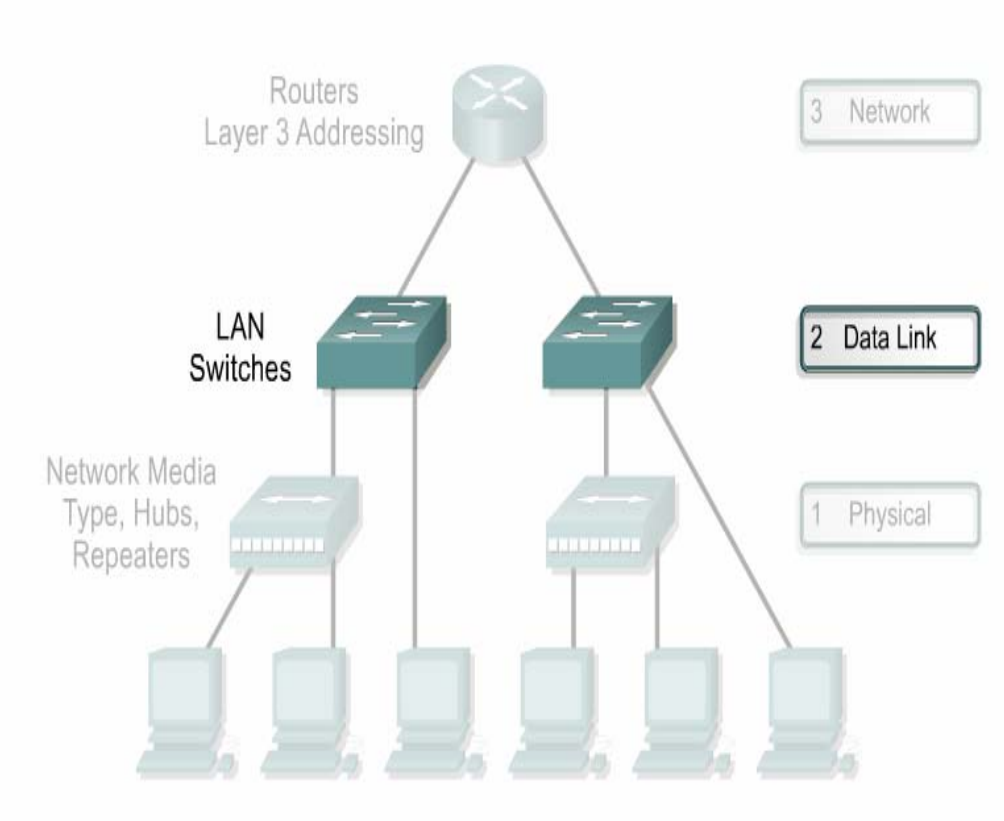
Thiết kế mạng LAN

Thiết kế Layer 1





Thiết kế mạng LAN
Thiết kế Layer 1



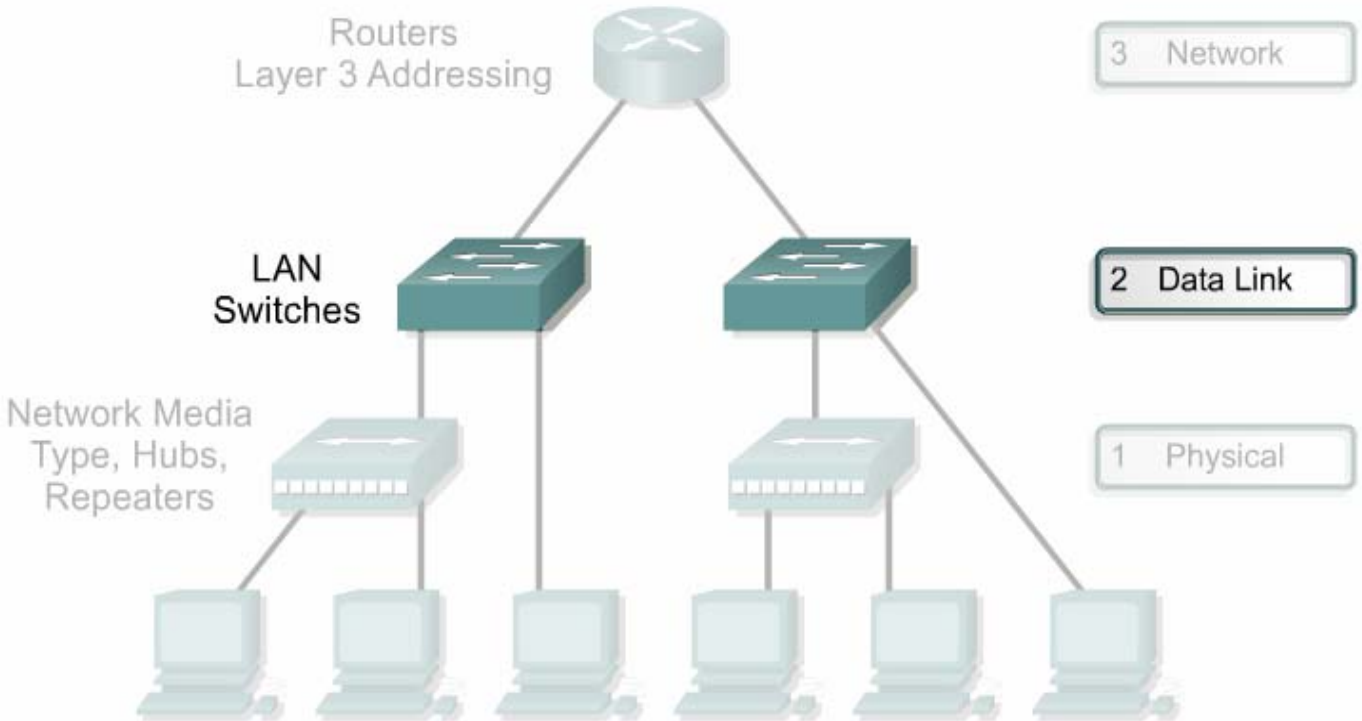
Hub A:
- Collision domain = 24 hosts
- Bandwidth average = 100 Mbps/24 hosts = 4.167 Mbps per host

Hub B:
- Collision domain = 24 hosts
- Bandwidth average = 10 Mbps/24 hosts = 0.4167 Mbps per host

Hub C:
- Collision domain = 8 hosts
- Bandwidth average = 100 Mbps/8 hosts = 12.5 Mbps per host

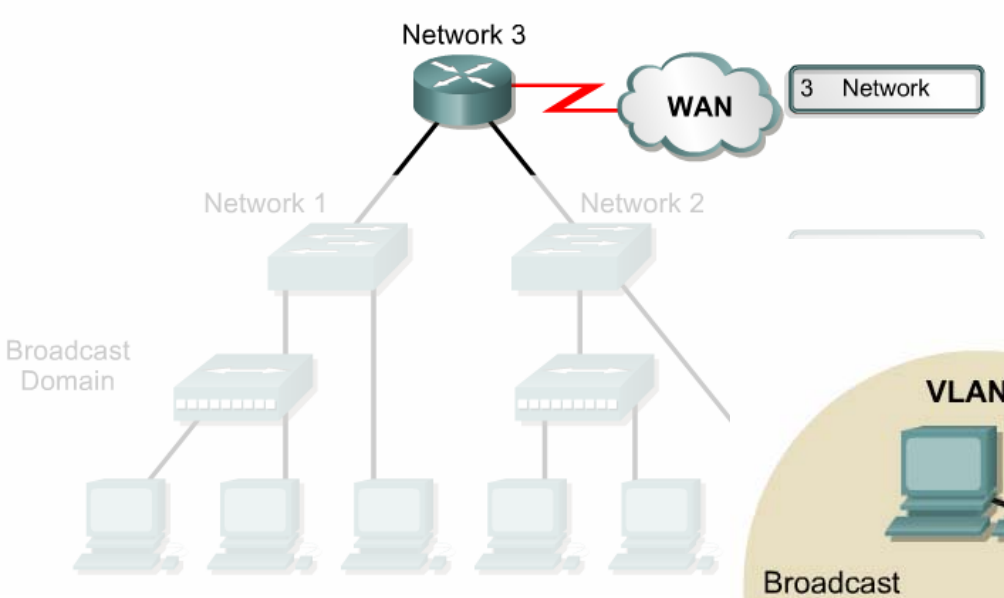
Hub D:
- Collision domain = 8 hosts
- Bandwidth average = 10 Mbps/8 hosts = 1.25 Mbps per host

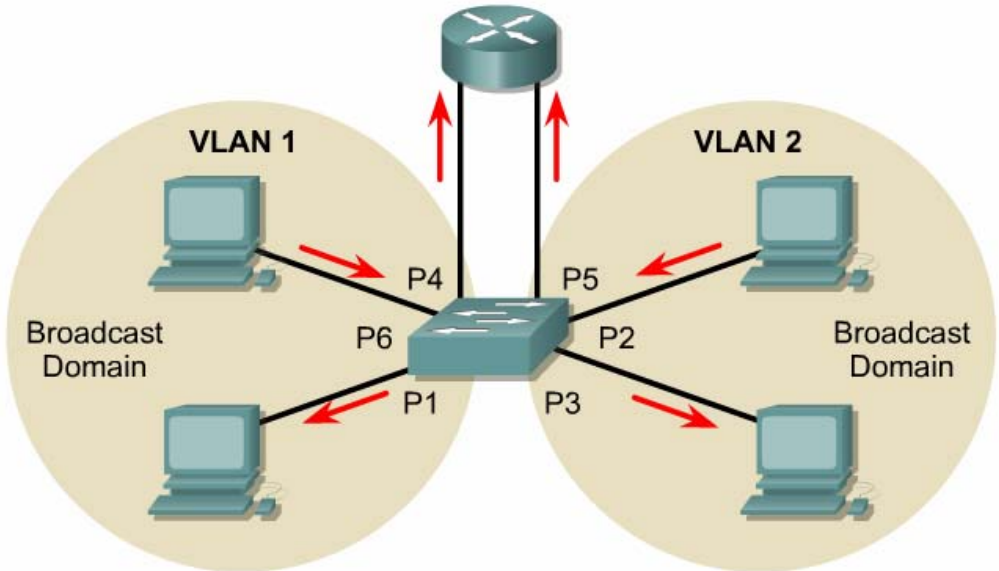
Thiết kế mạng LAN
Thiết kế Layer 2



Thiết kế mạng LAN

Thiết kế Layer 3





Thiết kế mạng LAN

Mô hình thiết kế phân cấp trong mạng LAN vừa và lớn

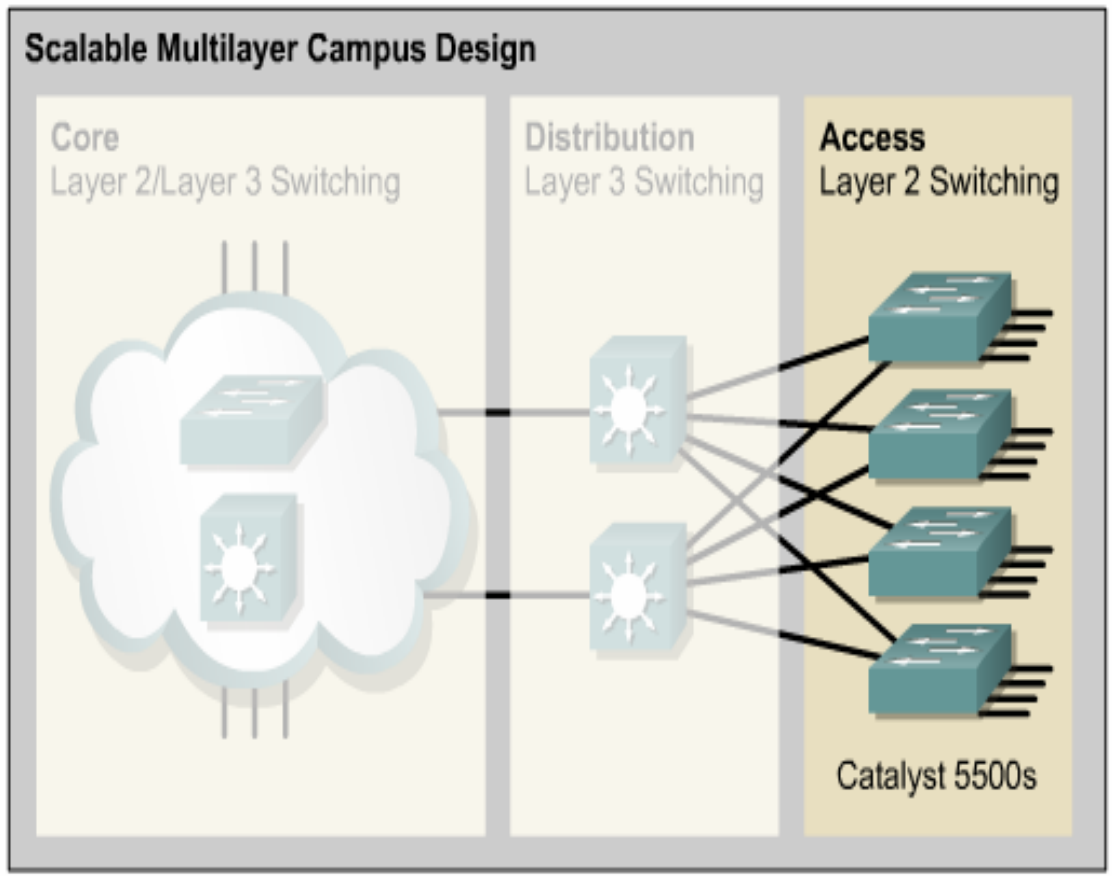
- Tầng truy cập: cung cấp kết nối vào hệ thống mạng cho user.
- Tầng phân phối: cung cấp các chính sách kết nối.
- Tầng trục chính: cung cấp sự vận chuyển tối ưu giữa các site.

Thiết kế mạng LAN

Mô hình thiết kế phân cấp trong mạng LAN vừa và lớn

Chức năng của tầng truy cập:

- Chia sẻ băng thông.
- Chuyển mạch băng thông.
- Lọc lớp MAC.
- Microsegment



Thiết kế mạng LAN

Mô hình thiết kế phân cấp trong mạng LAN vừa và lớn

Các dòng Switch của Cisco sử dụng ở tầng truy cập

Catalyst	Type	Supported OSI Layers	Ethernet Ports
1900 Series	Fixed configuration	Layer 2	12 or 24
2820 Series	Fixed configuration with modular expansion slots	Layer 2	24
2950 Series	Fixed configuration	Layer 2	0
4000 Series	Modular- multiple slots per chassis	Layer 2 and Layer 3	Configurable ports- up to 240
5000 Series	Modular- multiple slots per chassis	Layer 2 and Layer 3	Configurable ports- up to 528

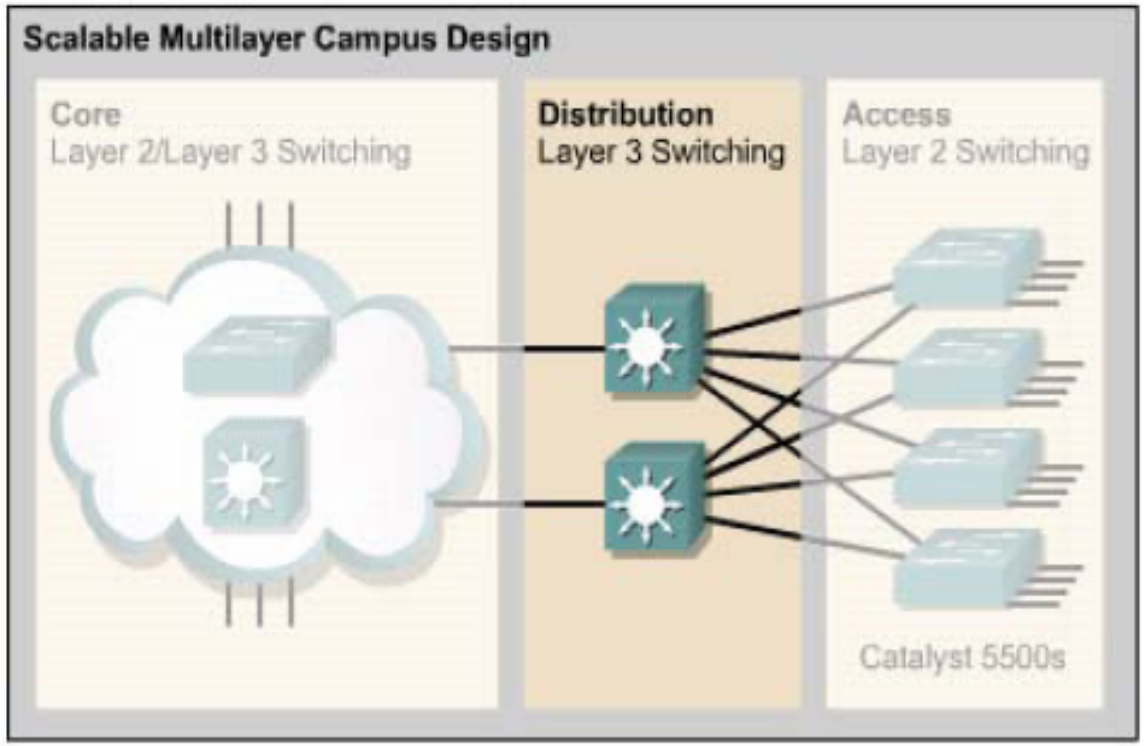
Catalyst 4000 Switch

Thiết kế mạng LAN

Mô hình thiết kế phân cấp trong mạng LAN vừa và lớn

Chức năng của tầng phân phối:

- Xác định miền quảng bá hay miền multicast.
- Định tuyến VLAN.
- Bảo mật



Thiết kế mạng LAN

Mô hình thiết kế phân cấp trong mạng LAN vừa và lớn

Các dòng Switch dùng ở tầng phân phối:

- Catalyst 2926G.
- Catalyst 5000.
- Catalyst 6000.

Catalyst 6500 Switch

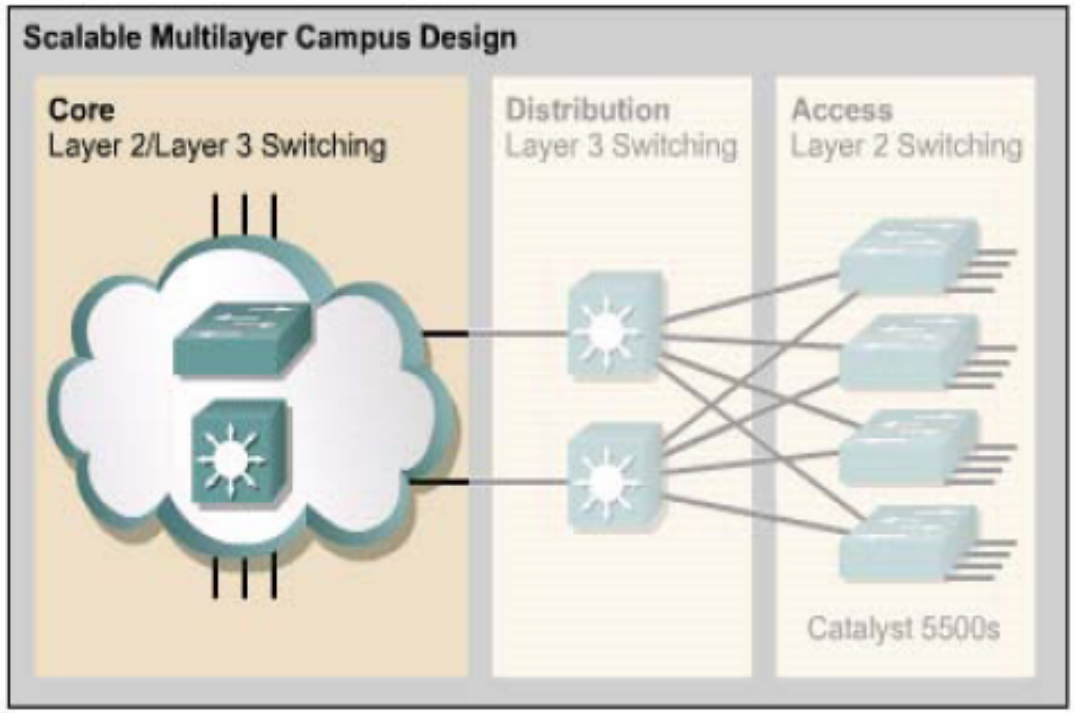
Catalyst 2926G Switch

Thiết kế mạng LAN

Mô hình thiết kế phân cấp trong mạng LAN vừa và lớn

Chức năng của tầng trục chính:

- Chuyển mạch tốc độ cao.
- Có thể sử dụng router riêng bên ngoài.
- Không cản trở gói để duy trì tốc độ.



Thiết kế mạng LAN

Mô hình thiết kế phân cấp trong mạng LAN vừa và lớn

Các dòng Switch dùng ở tầng trục chính:

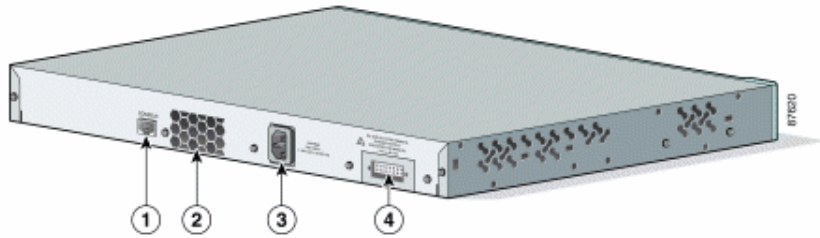
- Catalyst 6500.
- Catalyst 8500.
- IGX 8400.

Catalyst 8540 Switch

Switch đa dịch vụ IGX 8400

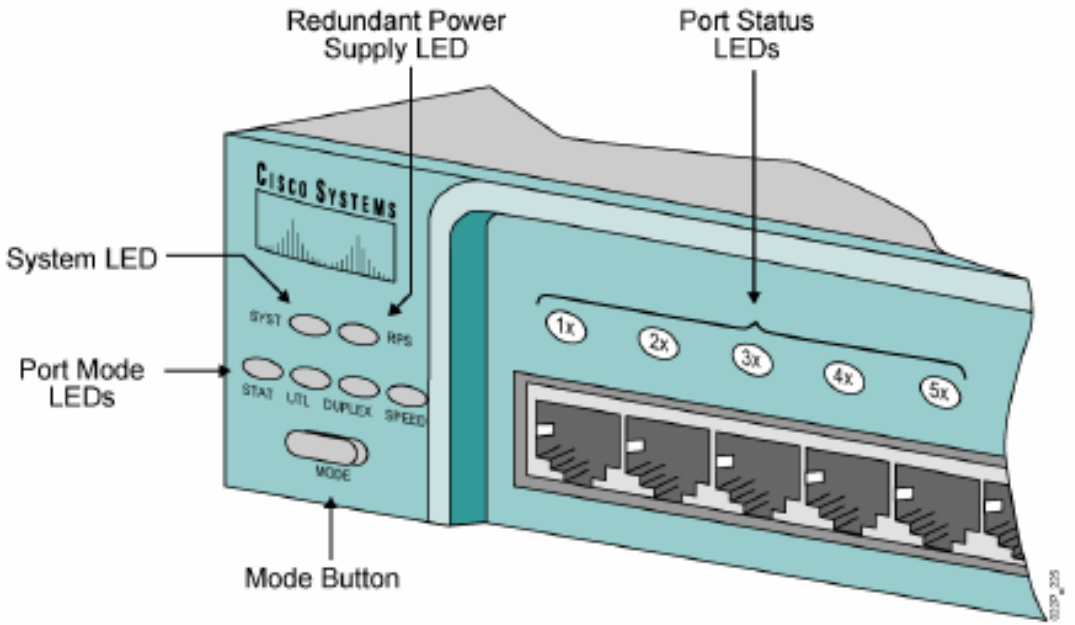
Cấu hình Switch
Cấu tạo vật lý

- Switch là một máy tính đặc biệt có:
  - CPU
  - RAM
  - Hệ điều hành
  - Ports



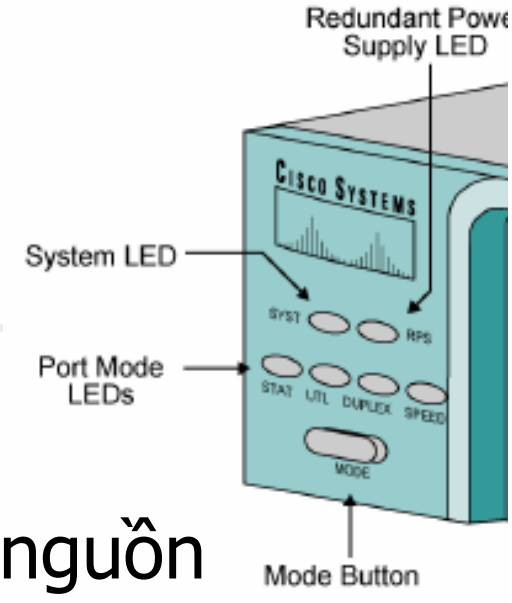
1	RJ-45 console port
2	Fan exhaust
3	AC power connector
4	RPS connector

Cấu hình Switch
Đèn LED báo hiệu trên switch



Cấu hình Switch

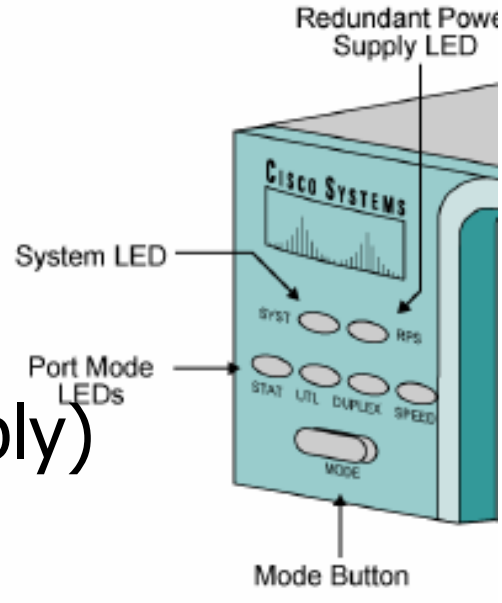
Đèn LED báo hiệu trên switch



- Đèn System:
  - Tắt: switch không được cấp nguồn
  - Xanh: switch được cấp nguồn và hoạt động
  - Vàng cam (Amber): hệ thống bị lỗi. Một hay nhiều lỗi xuất hiện trong quá trình power-on-selt-test (POST)

Cấu hình Switch

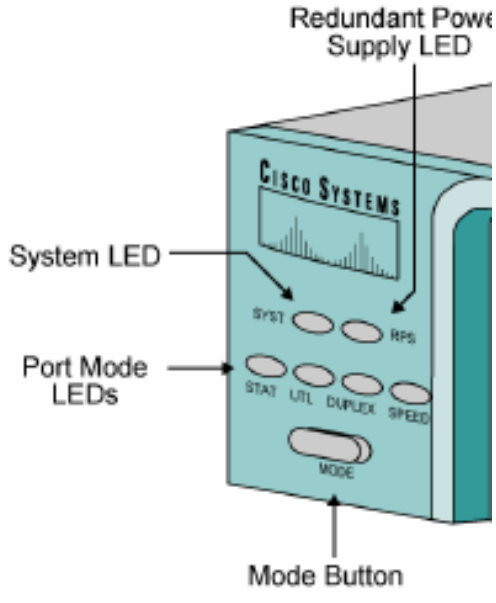
Đèn LED báo hiệu trên switch



- Đèn RPS (Redundant power supply)
  - Tắt: module RPS không cài đặt.
  - Xanh: module RPS đang hoạt động.
  - Chớp xanh (Flashing green): RPS đã kết nối nhưng không hoạt động vì đang cấp nguồn cho thiết bị khác.
  - Vàng cam (Amber): RPS đã cài đặt nhưng không hoạt động.
  - Chớp vàng cam (Flashing Amber): nguồn nội bị hỏng và RPS đang cung cấp nguồn cho switch.

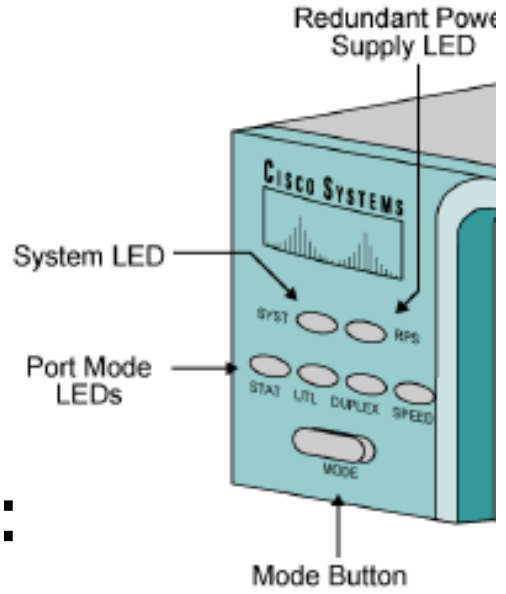
Cấu hình Switch

Đèn LED báo hiệu trên switch



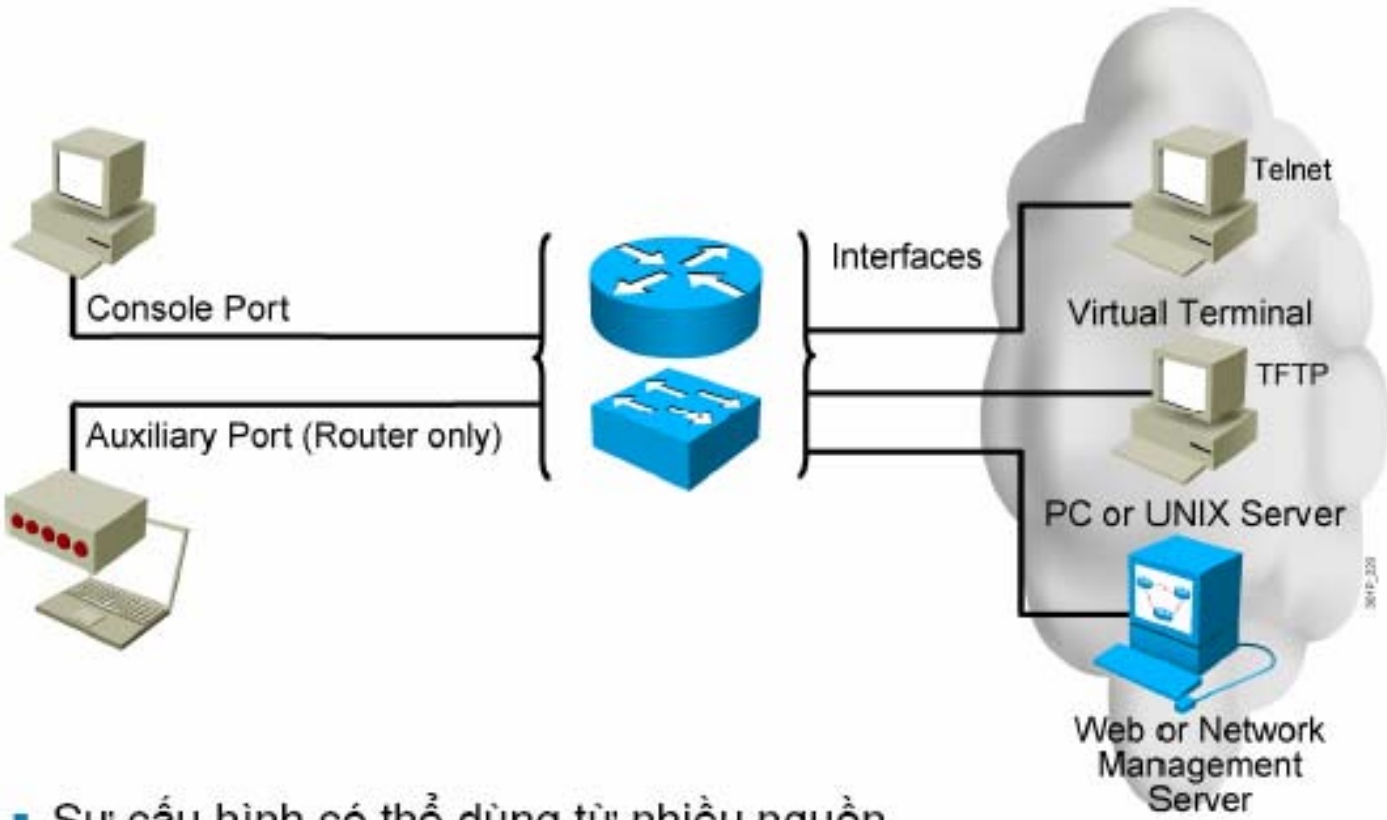
- Đèn STAT:
  - Tắt: không có link.
  - Xanh: link có, không kích hoạt.
  - Chớp xanh: có link, có dữ liệu truyền.
  - Xen kẻ Xanh và Vàng cam: link có lỗi.
  - Vàng cam (Amber): cổng không chuyển tiếp do không được kích hoạt vì lý do quản trị (vi phạm địa chỉ, bị khóa do Spanning Tree Protocol).

Cấu hình Switch
Đèn LED báo hiệu trên switch



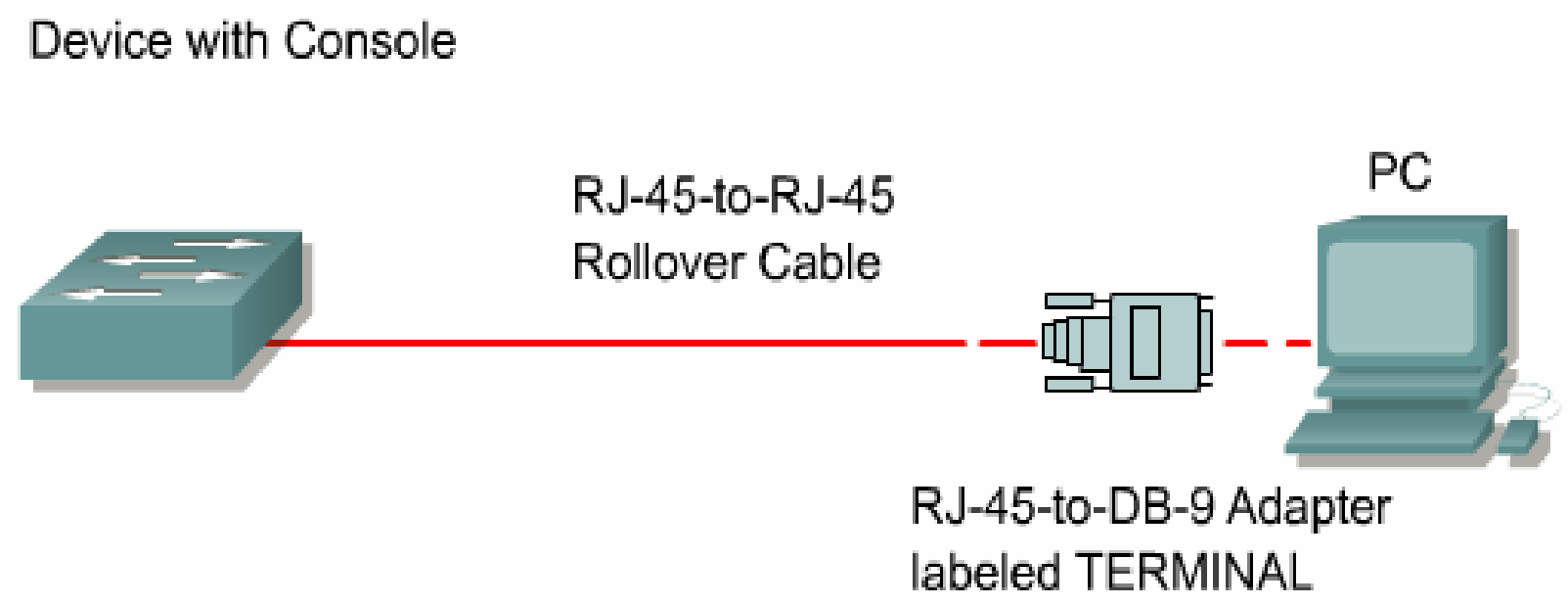
- Đèn theo dõi tải (Bandwidth utilization – UTL LED):
  - Xanh: hiện trang đang dùng tải.
  - Vàng cam: số tải cực đại đang dùng.
- Đèn Full –duplex (FDUP LED on):
  - Xanh: cổng được cấu hình full-duplex.
  - Tắt: cổng được cấu hình half-duplex.
- Đèn 100:
  - Tắt: đang hoạt động ở 10 Mbps.
  - Xanh: đang hoạt động ở 100 Mbps.

Cấu hình Switch
Kết nối switch đến máy tính

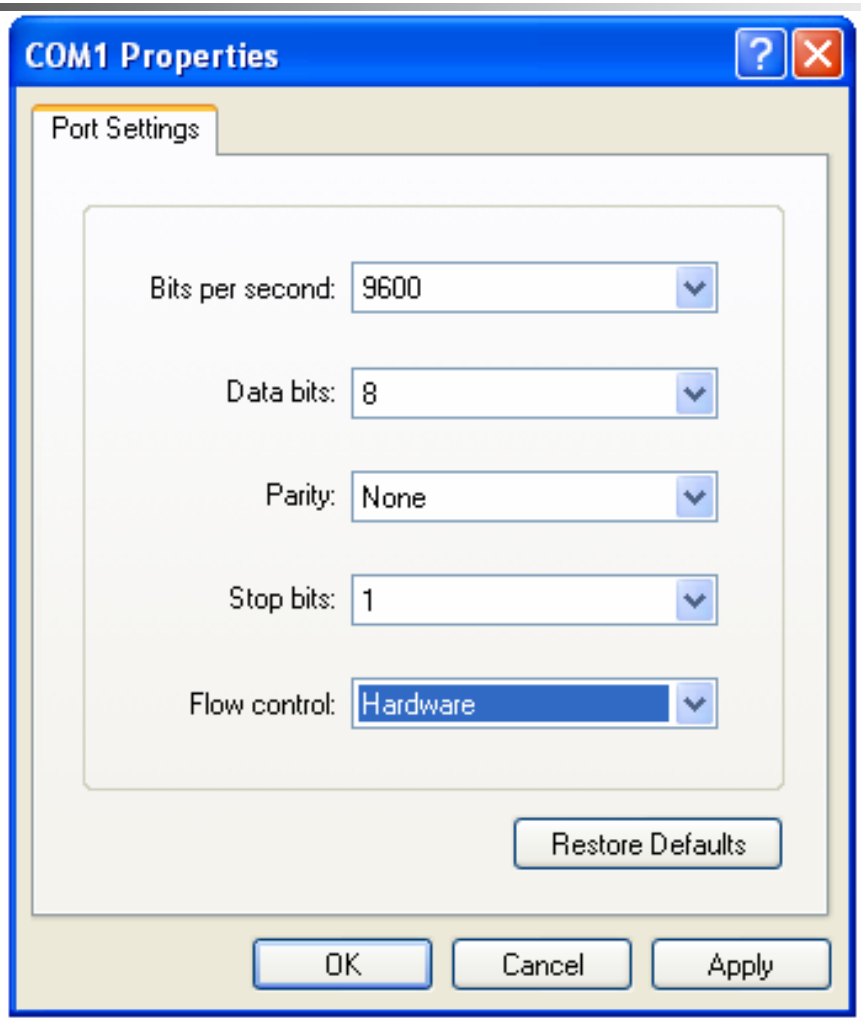


- Sự cấu hình có thể dùng từ nhiều nguồn.
- Sự cấu hình thực hiện trên bô nhớ của thiết bị.

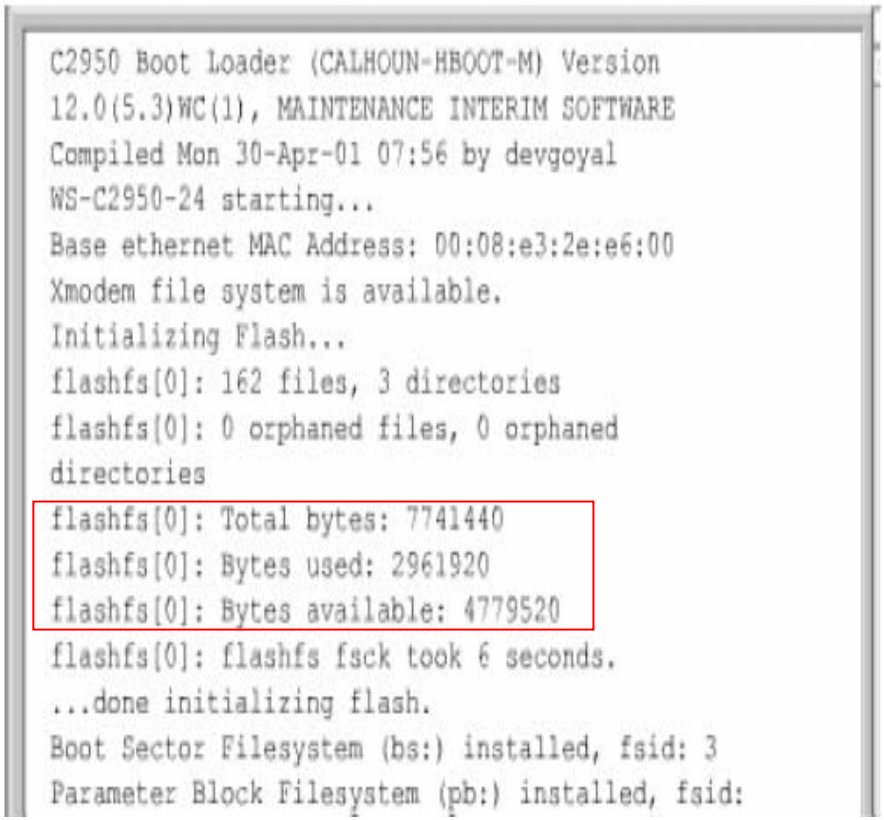
Cấu hình Switch
Kết nối switch đến máy tính



Cấu hình Switch
Cài đặt thông số cho Hyper Terminal



Cấu hình Switch
Quá trình khởi động của switch



Cấu hình Switch
Quá trình khởi động của switch

```
flashfs[1]: Bytes available: 4779520
flashfs[1]: flashfs fsck took 6 seconds.
flashfs[1]: Initialization complete.
Done initializing flashfs.
C2950 POST: System Board Test : Passed
C2950 POST: Ethernet Controller Test : Passed
C2950 POST: MII TEST : Passed

cisco WS-C2950-12 (RC32300) processor (revision
B0) with 22260K bytes of memory.
Processor board ID FOC0605W0BH
Last reset from system-reset

Processor is running Enterprise Edition Software
Cluster command switch capable
Cluster member switch capable
12 FastEthernet/IEEE 802.3 interface(s)

32K bytes of flash-simulated non-volatile
configuration memory.
Base ethernet MAC Address: 00:08:E3:2E:E6:00
Motherboard assembly number: 73-5782-08
Power supply part number: 34-0965-01
Motherboard serial number: FOC060502HP
Power supply serial number: PHI05500C5D
Model revision number: B0
Motherboard revision number: B0
Model number: WS-C2950-12
System serial number: FOC0605W0BH

Press RETURN to get started!
C2950 INIT: Complete

IOS (tm) C2950 Software (C2900XL-C3H2S-M), Version
12.0(5)XU,
RELEASE SOFTWARE
(fc1)
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Mon 03-Apr-00 16:37 by swati
--- System Configuration Dialog ---
At any point you may enter a question mark '?' for
help.
Use ctrl-c to abort configuration dialog at any
prompt.
Default settings are in square brackets '[]'.
Continue with configuration dialog? [yes/no]:
```

Cấu hình Switch
Kết nối switch đến máy tính

Cisco C2950

```
C2950 POST: System Board Test : Passed
C2950 POST: Ethernet Controller Test : Passed
C2950 POST: MII TEST : Passed

cisco WS-C2950-12 (RC32300) processor (revision
B0) with 22260K bytes of memory.
Processor board ID FOC0605W0BH
Last reset from system-reset

Processor is running Enterprise Edition Software
Cluster command switch capable
Cluster member switch capable
12 FastEthernet/IEEE 802.3 interface(s)

32K bytes of flash-simulated non-volatile
configuration memory.
Base ethernet MAC Address: 00:08:E3:2E:E6:00
```

Cấu hình Switch
Giao diện dòng lệnh (CLI) của switch

Cisco

```
Switch>?

Exec commands:

access-enable     Create a temporary Access-List entry

clear             Reset functions

connect           Open a terminal connection

disable           Turn off privileged commands

disconnect        Disconnect an existing network
                  connection

enable            Turn on privileged commands
```

Cấu hình Switch

Một số thao tác trên dòng lệnh của switch

	(Automatic scrolling of long lines)
Ctrl-A	Move to the beginning of the command line.
Ctrl-E	Move to the end of the command line.
Esc-B	Move back one word.
Esc-F	Move forward one word.
Ctrl-B	Move back one character.
Ctrl-F	Move forward one character.
Ctrl-D	Delete a single character.

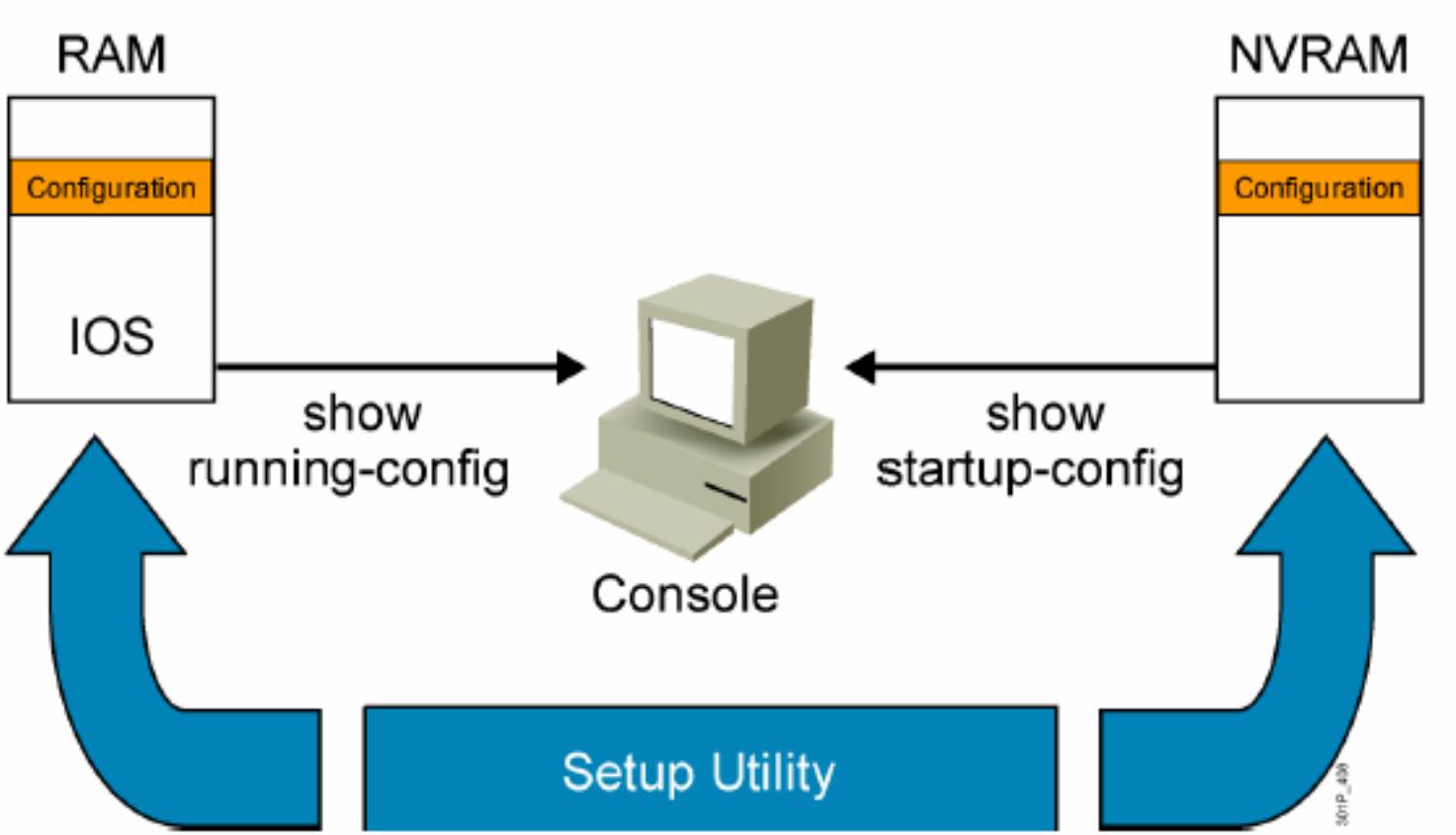
Ctrl-P or Up Arrow	**Recalls last (previous) commands.**
Ctrl-N or Down Arrow	**Recalls more recent commands.**
`show history`	**Shows command buffer contents.**
`terminal history size` *lines*	**Sets session command buffer size.**

Cấu hình Switch

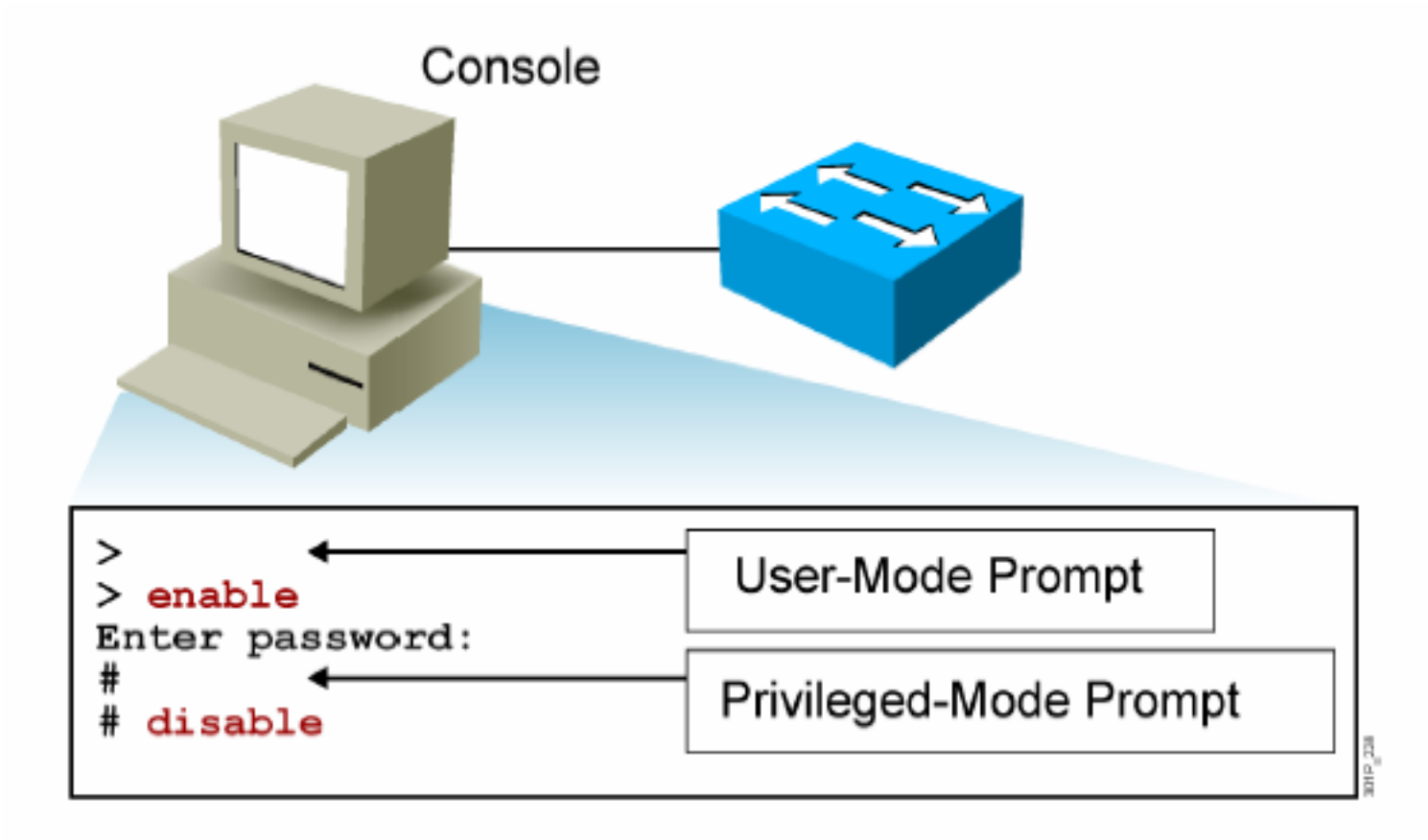
Một số lệnh Show trên switch

Lệnh	Giải thích
Show version	Xem các thông tin về phần cứng và phần mềm. Được sử dụng để xác định chính xác switch đang sử dụng module nào, phần mềm nào.
Show running-config	Hiển thị tập tin cấu hình đang chạy của switch
Show interfaces	Hiển thị trạng thái hoạt động của mỗi port, số lượng gói vào/ra và bị lỗi trên port đó.
Show interface status	Hiển thị chế độ hoạt động của port
Show controllers ethernet-controller	Xem số lượng frame bị hủy bỏ, bị trì hoãn, bị lỗi, bị đụng độ…
Show port	Xem thông tin về quá trình tự kiểm tra khi bật nguồn của switch (POST)

Cấu hình Switch
Một số lệnh Show trên switch



Cấu hình Switch
Chuyển đổi Mode



Cấu hình Switch
Xem phiên bản IOS

```
Switch#show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(25)SEE2, RELEASE

SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 28-Jul-06 11:57 by yenanh
Image text-base: 0x00003000, data-base: 0x00BB7944

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)SEE1, RELEASE SOFTWARE (fc1)

Switch uptime is 24 minutes

System returned to ROM by power-on
System image file is "flash:c2960-lanbasek9-mz.122-25.SEE2/c2960-lanbasek9-mz.122-
25.SEE2.bin"

cisco WS-C2960-24TT-L (PowerPC405) processor (revision B0) with 61440K/4088K bytes of
memory.

Processor board ID FOC1052W3XC
Last reset from power-on
1 Virtual Ethernet interface
24 FastEthernet interfaces
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

! Text omitted

Switch#
```

Cấu hình Switch
Kiểm tra cấu hình mặc định của switch

```
Switch#show running-config
Building configuration...

Current configuration:
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
!<OUTPUT OMITTED>
!
interface VLAN1
 no ip directed-broadcast
 no ip route-cache
!
!
!<OUTPUT OMITTED>
!
line con 0
 transport input none
 stopbits 1
line vty 5 15
!
end
```

Cấu hình Switch

Đặc điểm mặc định của các port trên switch

```
SwitchX#show interfaces FastEthernet0/2
FastEthernet0/2 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0008.a445.ce82 (bia 0008.a445.ce82)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 10Mb/s
  input flow-control is unsupported output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 4w6d, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     182979 packets input, 16802150 bytes, 0 no buffer
     Received 49954 broadcasts (0 multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 8 ignored
     0 watchdog, 20115 multicast, 0 pause input
     0 input packets with dribble condition detected
     3747473 packets output, 353656347 bytes, 0 underruns
 --More--
```

Cấu hình Switch
Quản lý bảng địa chỉ MAC

```
Switch#show mac-address-table
Dynamic Address Count:                    2
Secure Address Count:                     0
Static Address (User-defined) Count:      0
System Self Address Count:                13
Total MAC addresses:                      15
Maximum MAC addresses:                    8192
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination
Port
-------------------  ------------  ----  ---------------
0010.7a60.ad7e       Dynamic          1  FastEthernet0/2
00e0.2917.1884       Dynamic          1  FastEthernet0/5
```

Cấu hình Switch
Quản lý bảng địa chỉ MAC

```
Switch(config)#mac-address-table ?
  aging-time  Set MAC address table entry maximum
age
  secure      Configure a secure address
  static      Configure a static 802.1d static
address
Switch(config)#mac-address-table static
0010.7a60.1884 interface FastEthernet0/5 VLAN1
Switch(config)#no mac-address-table static
0010.7a60.1884 interface FastEthernet0/5 VLAN1
```

Cấu hình Switch
Cấu hình mặc định của VLAN

```
Switch#show vlan
VLAN  Name                    Status  Ports
----  ------------------      ------  -------------------------
1     default                 active  Fa0/1, Fa0/2, Fa0/3, Fa0/4,
                                      Fa0/5, Fa0/6, Fa0/7, Fa0/8,
                                      Fa0/9, Fa0/10,Fa0/11,Fa0/12
1002  fddi-default            active
1003  token-ring-default      active
1004  fddinet-default         active
1005  trnet-default           active

VLAN  Type   SAID     MTU    Parent  RingNo  BridgeNo
----  -----  ------   -----  ------  ------  --------
1     enet   100001   1500   -       -       -
1002  fddi   101002   1500   -       -       -
1003  tr     101003   1500   1005    0       -
1004  fdnet  101004   1500   -       -       1
1005  trnet  101005   1500   -       -       1

Stp  BrdgMode  Trans1  Trans2
---  --------  ------  ------
-    -         1002    1003
-    -         1       1003
-    srb       1       1002
ibm  -         0       0
ibm  -         0       0
```

Cấu hình Switch
Nội dung mặc định của flash

```
Switch#show flash or Switch#dir flash:
Directory of flash:/

  2   -rwx     1674921   Apr 30 2001 15:09:51  c2950-
c3h2s-mz.120-5.3.WC.1.bin
  3   -rwx         269   Jan 01 1970 00:00:57
env_vars
  4   drwx       10240   Apr 30 2001 15:09:52  html

7741440 bytes total (4780544 bytes free)
```

Cấu hình Switch

Xoá mọi cấu hình cũ trên switch

Catalyst 2950

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash:vlan.dat? [confirm]
Switch#erase startup-config
<output omitted>
Switch#reload
```

Catalyst 1900

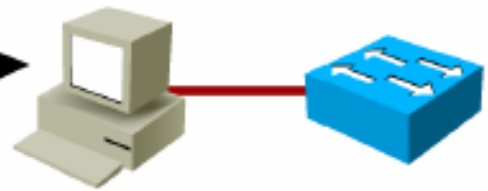
```
Switch#delete nvram
```

Cấu hình Switch

Đặt tên và mật khẩu cho đường console và vty

Console Password

```
SwitchX(config)#line console 0
SwitchX(config-line)#login
SwitchX(config-line)#password cisco
```



Virtual Terminal Password

```
SwitchX(config)#line vty 0 4
SwitchX(config-line)#login
SwitchX(config-line)#password sanjose
```

Enable Password

```
SwitchX(config)#enable password cisco
```

Secret Password

```
SwitchX(config)#enable secret sanfran
```

Service Password-Encryption Commands

```
SwitchX(config)#service password-encryption
SwitchX(config)#no service password-encryption
```

Cấu hình Switch

Cấu hình tốc độ và chế độ song công cho port

```
Enter configuration commands, one per line.  End with
CNTL/Z.
Switch(config)#interface FastEthernet0/2
Switch(config-if)#duplex full
Switch(config-if)#
00:34:01: %LINK-3-UPDOWN: Interface FastEthernet0/2,
changed state to down
00:34:02: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/2, changed state to down
00:34:03: %LINK-3-UPDOWN: Interface FastEthernet0/2,
changed state to up
00:34:04: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/2, changed state to up
Switch(config-if)#speed 100
Switch(config-if)#
00:34:24: %LINK-3-UPDOWN: Interface FastEthernet0/2,
changed state to down
00:34:25: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/2, changed state to down
00:34:27: %LINK-3-UPDOWN: Interface FastEthernet0/2,
changed state to up
00:34:28: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/2, changed state to up
```

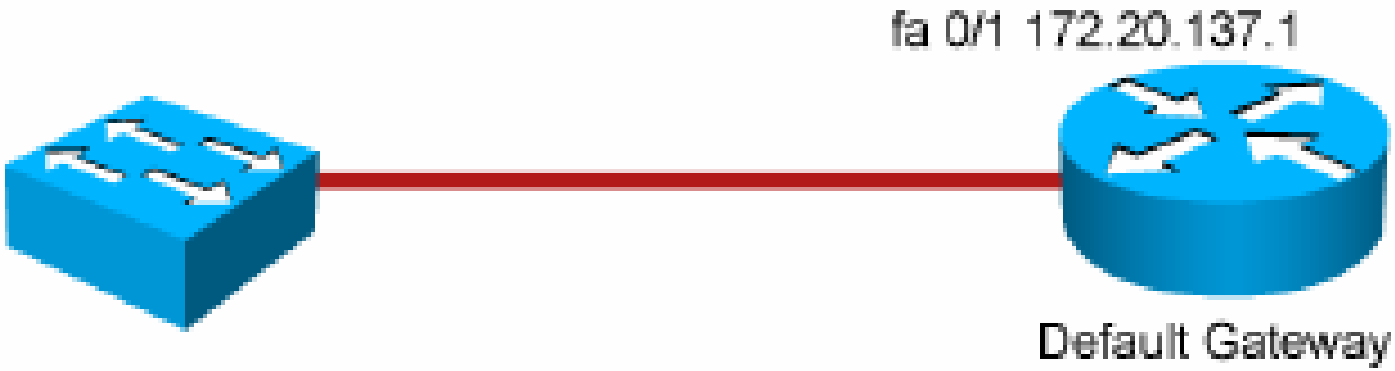
Cấu hình Switch
Cấu hình địa chỉ IP

```
SwitchX(config)#interface vlan 1
SwitchX(config-if)#ip address {ip address} {mask}
```

Example:

```
SwitchX(config)#interface vlan 1
SwitchX(config-if)#ip address 10.5.5.11 255.255.255.0
SwitchX(config-if)#no shutdown
```

Cấu hình Switch
Cấu hình Default Gateway




```
SwitchX(config)#ip default-gateway {ip address}
```

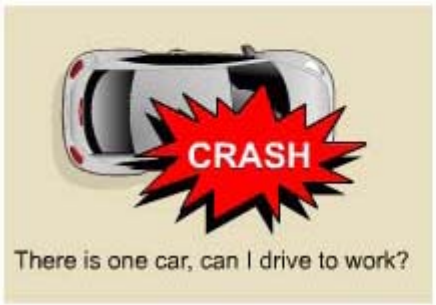
Example:

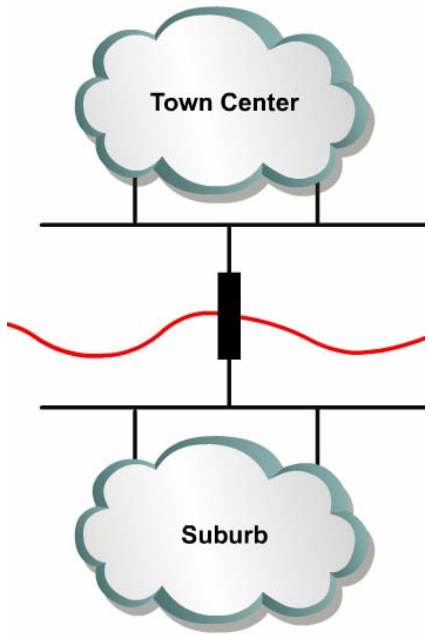
```
SwitchX(config)#ip default-gateway 172.20.137.1
```

Cấu hình Switch
Copy IOS từ TFTP Server

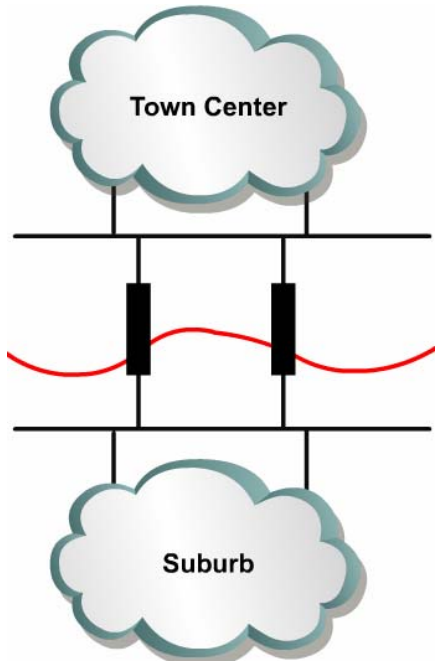
```
ALSwitch#copy tftp flash
Address or name of remote host []? 192.168.1.3
Source filename []? c2950-c3h2s-mz.120-5.3.WC.1.bin
Destination filename [c2950-c3h2s-mz.120-5.3.WC.1.bin]? [enter]
%Warning: There is a file already existing with this name

Do you want to over write? [confirm] [enter]
Accessing tftp://192.168.1.3/c2950-c3h2s-mz.120-5.3.WC.1.bin...
Loading c2950-c3h2s-mz.120-5.3.WC.1.bin from 192.168.1.3 (via VLAN1):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!
[OK - 1674921 bytes]
1674921 bytes copied in 51.732 secs (32841 bytes/sec)
ALSwitch#
```

Giao thức Spanning-Tree
Cấu trúc dự phòng (Redundancy)



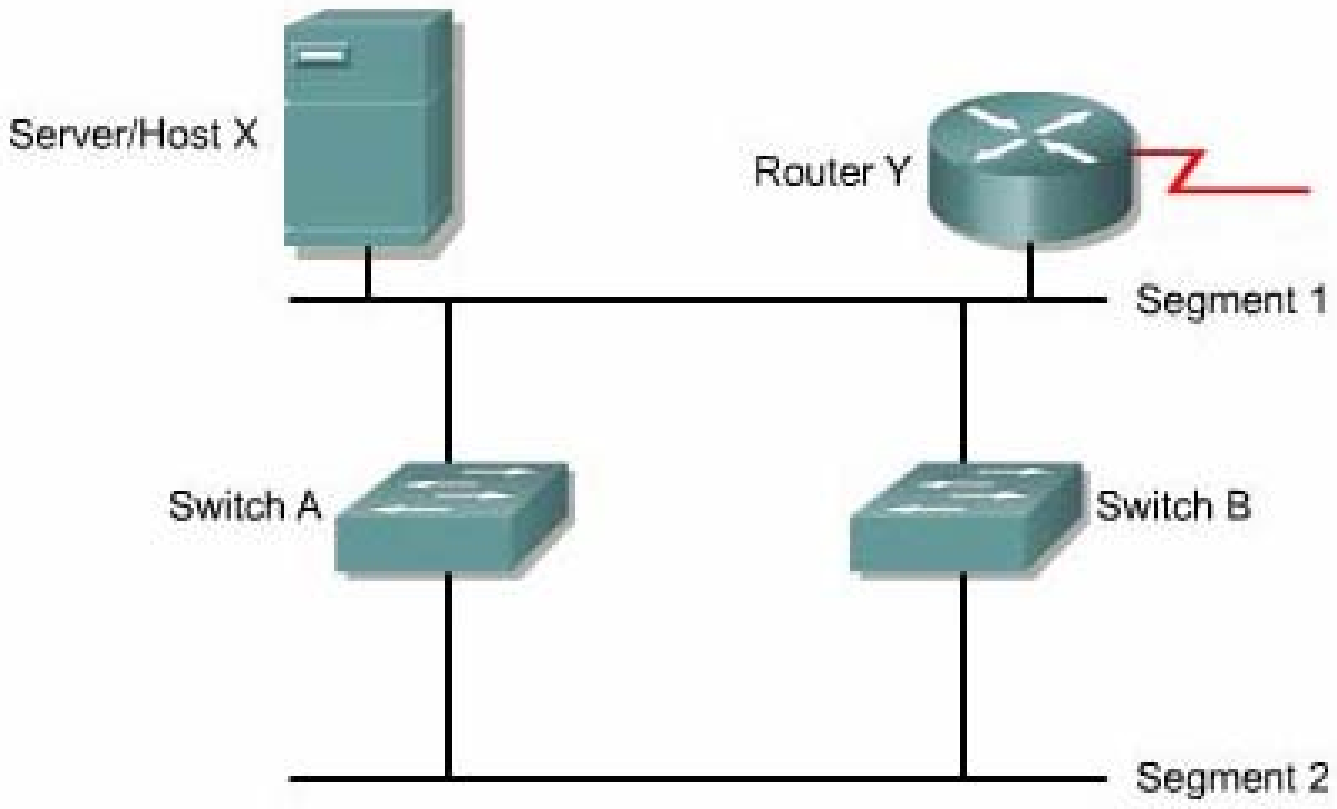


One Bridge

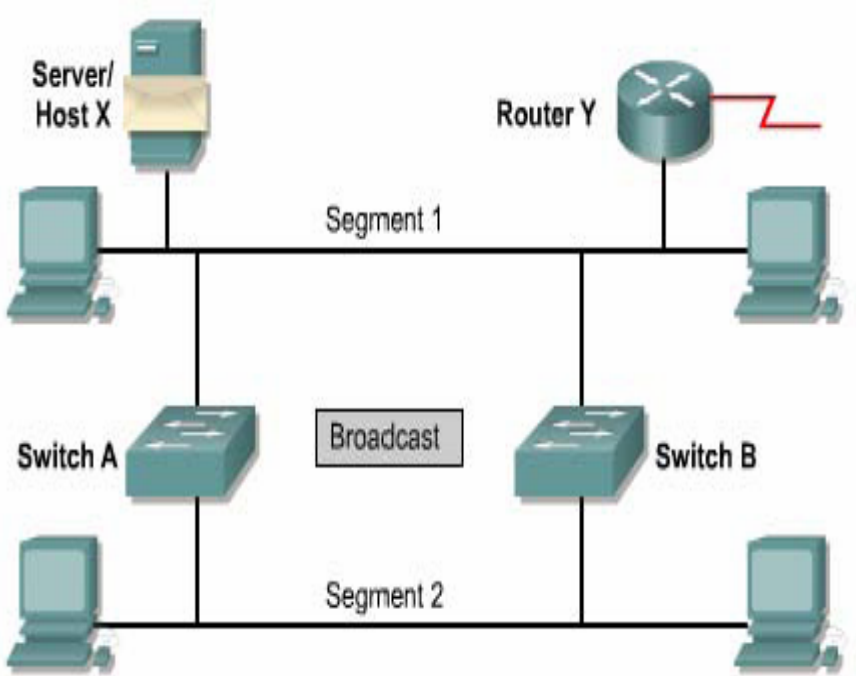


Redundant Bridges

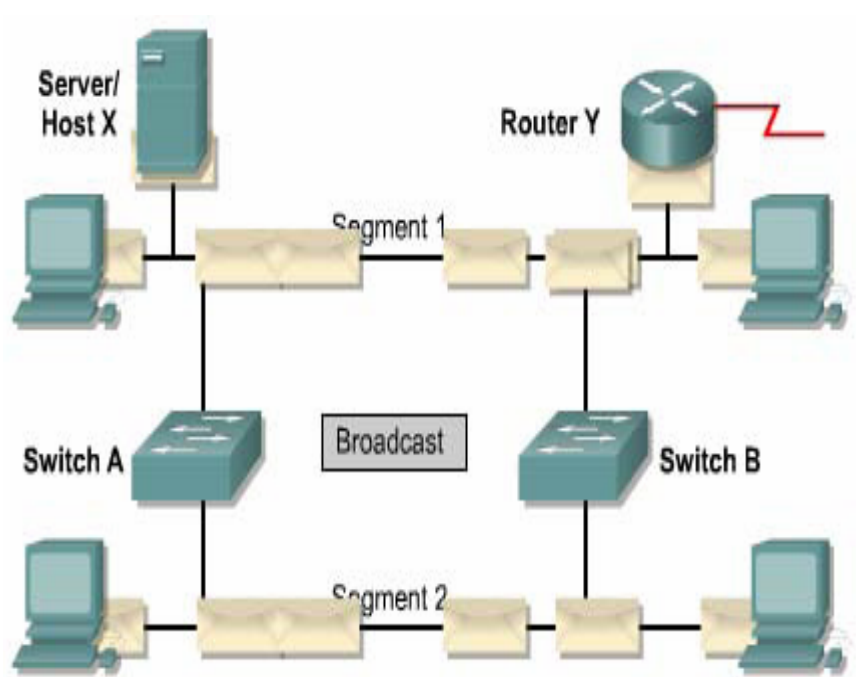
Giao thức Spanning-Tree
Cấu trúc chuyển mạch dự phòng



Giao thức Spanning-Tree
Trận bão quảng bá (Broadcast Storm)

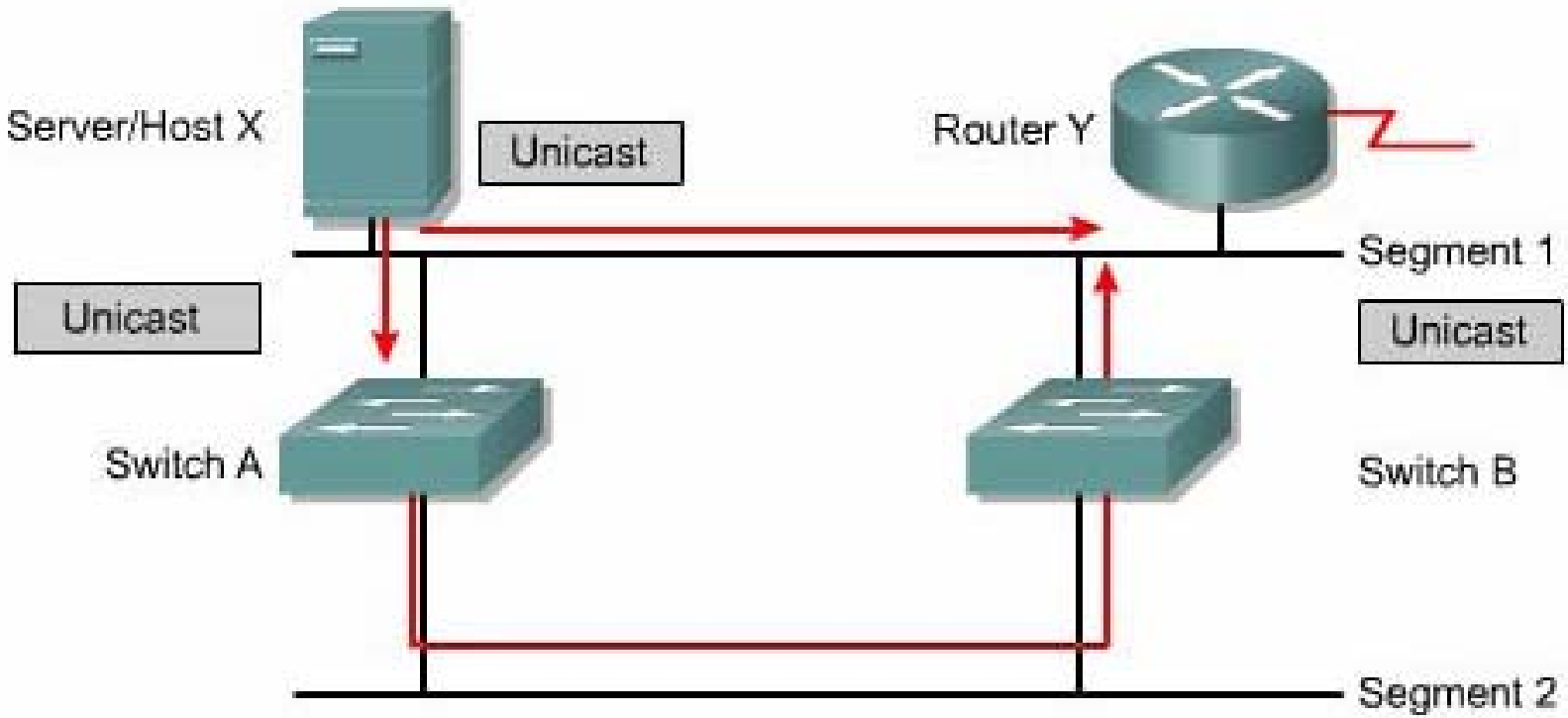


- Host X sends a broadcast.
- Switches continue to propagate broadcast traffic over and over.

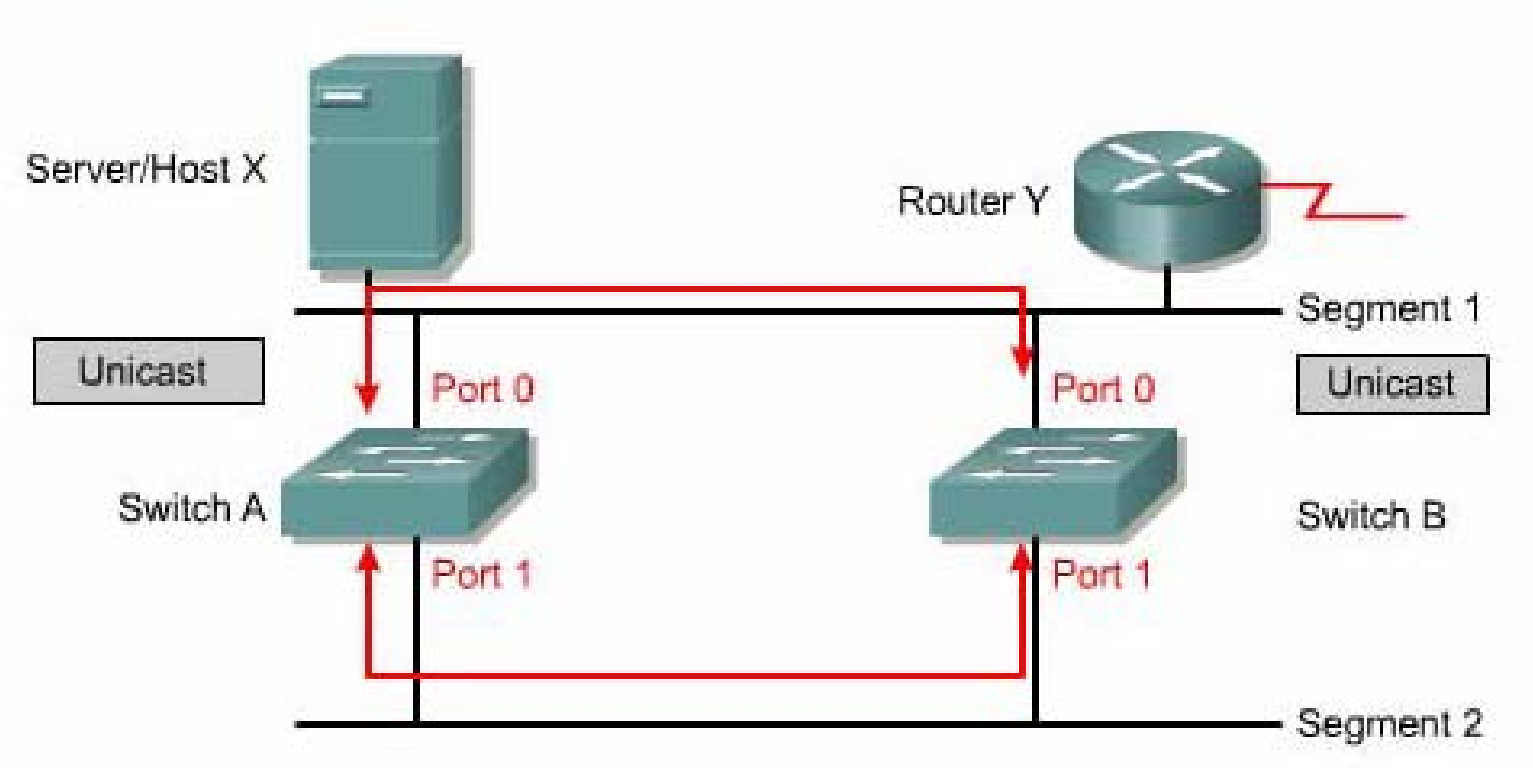


- Host X sends a broadcast.
- Switches continue to propagate broadcast traffic over and over.

Giao thức Spanning-Tree
Truyền nhiều lượt frame

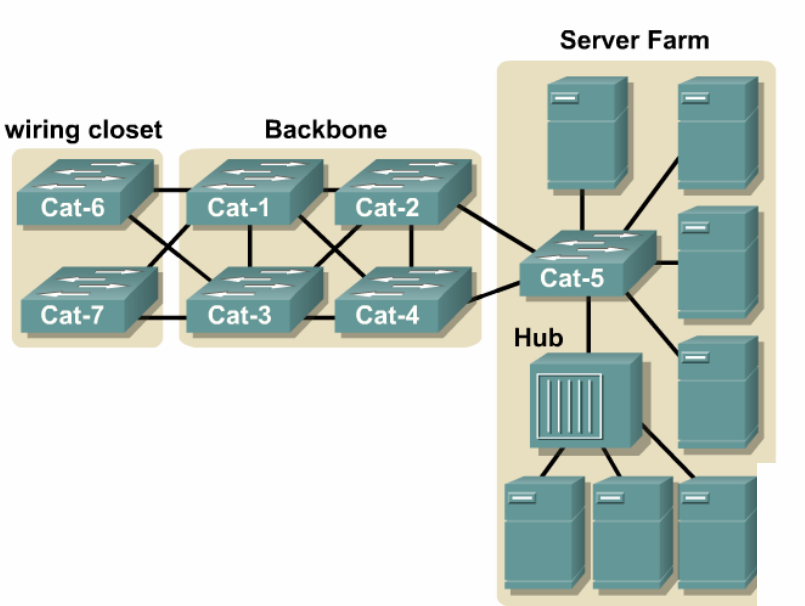


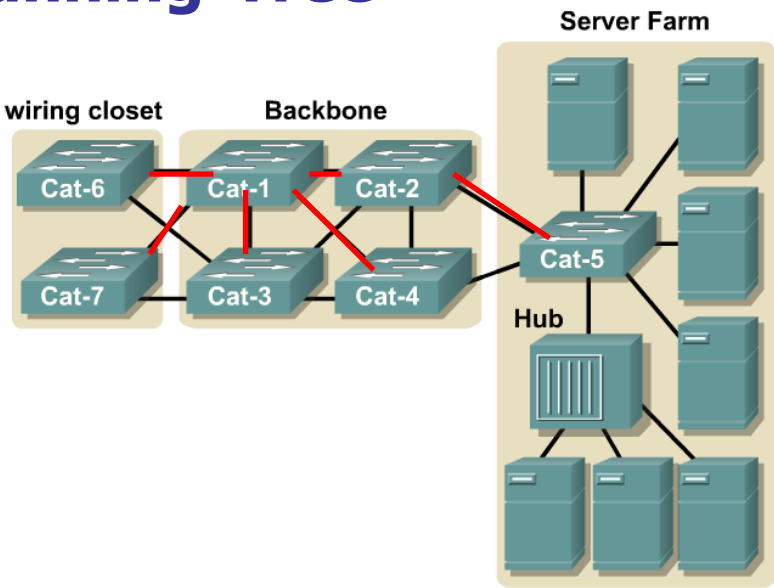
Giao thức Spanning-Tree
Cơ sở dữ liệu MAC không ổn định

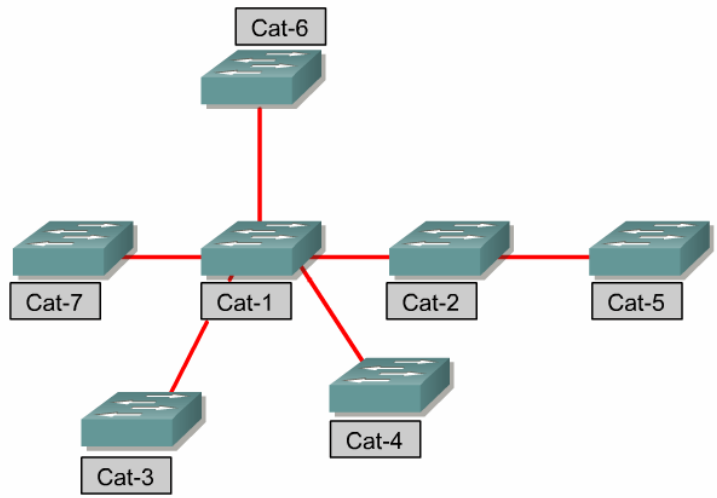


Giao thức Spanning-Tree

Cấu trúc dự phòng và Spanning-Tree

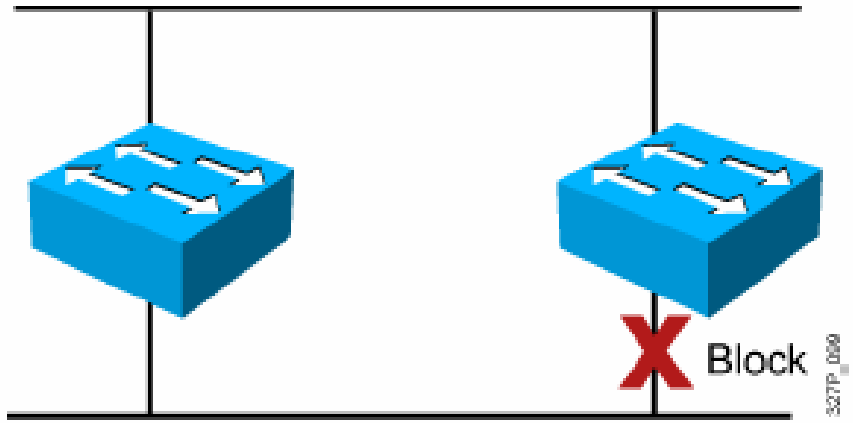






Giao thức Spanning-Tree

Cấu trúc dự phòng và Spanning-Tree

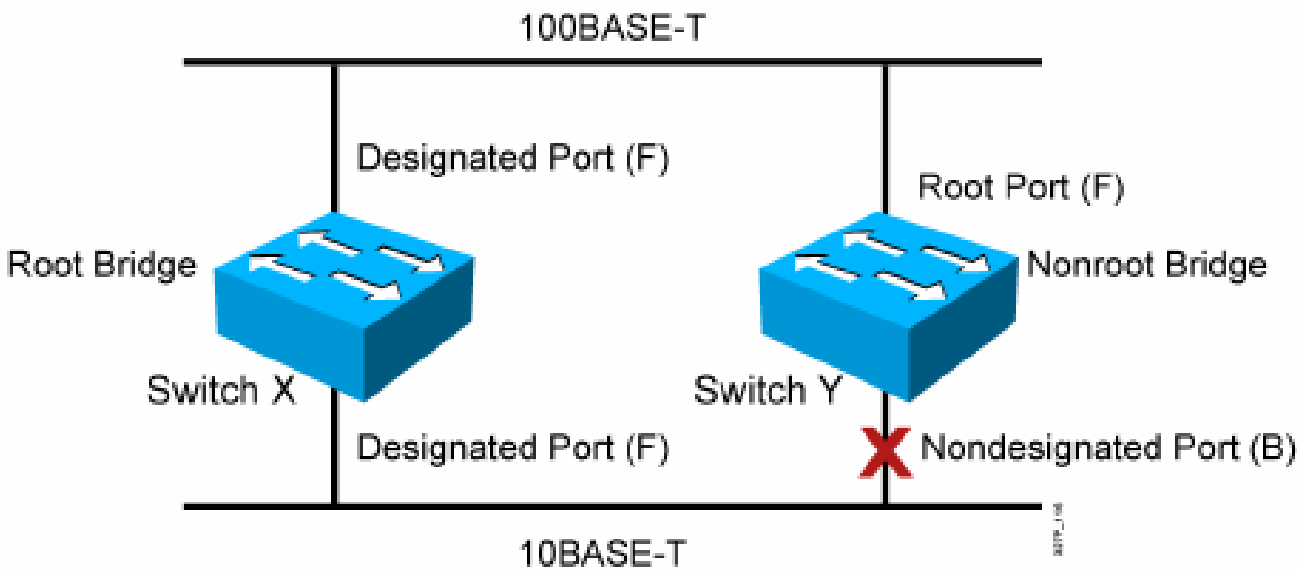


- Cung cấp một sơ đồ mạng dự phòng không có lặp bằng cách đặt những port nào đó vào trạng thái khóa
- Được đưa ra trong chuẩn IEEE 802.1D

Giao thức Spanning-Tree

Cấu trúc dự phòng và Spanning-Tree

- Một root bridge trên broadcast domain.
- Một root port trên nonroot bridge.
- Một designated port trên segment.
- Các Nondesignated port không được sử dụng.



Giao thức Spanning-Tree

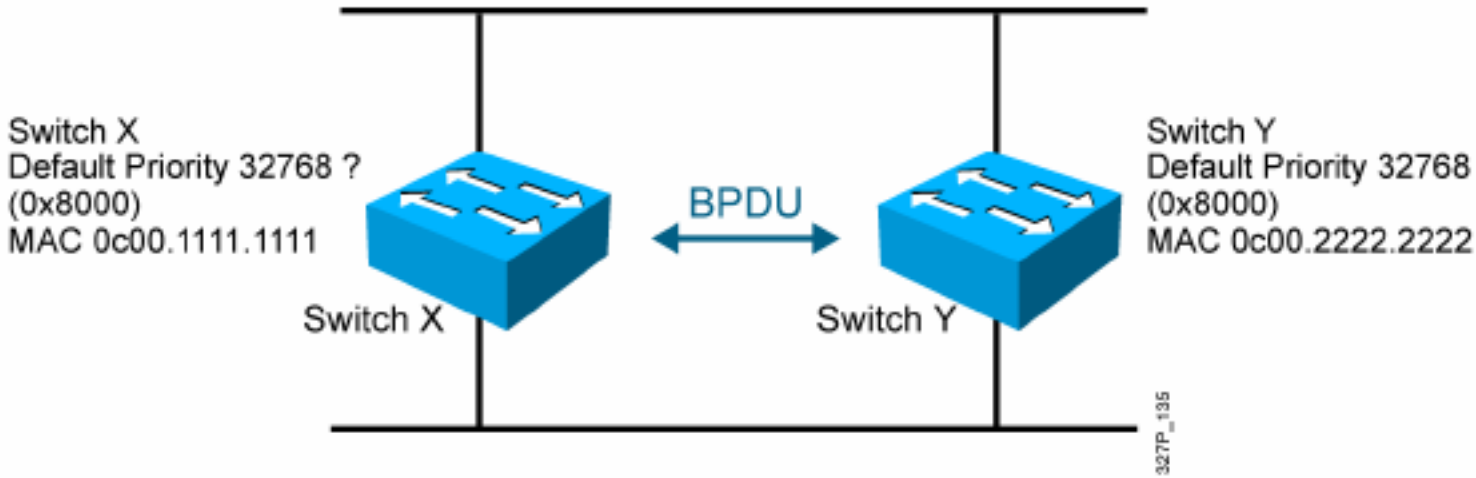
Giá trị chi phí mặc định tương ứng với tốc độ của đường kết nối

Tốc độ đường truyền	Giá thành (Revised IEEE Specification)	Giá thành (Previous IEEE Specification)
10 Gb/s	2	1
1 Gb/s	4	1
100 Mb/s	19	10
10 Mb/s	100	100

Giao thức Spanning-Tree

Kết quả tính toán của giao thức Spanning-Tree

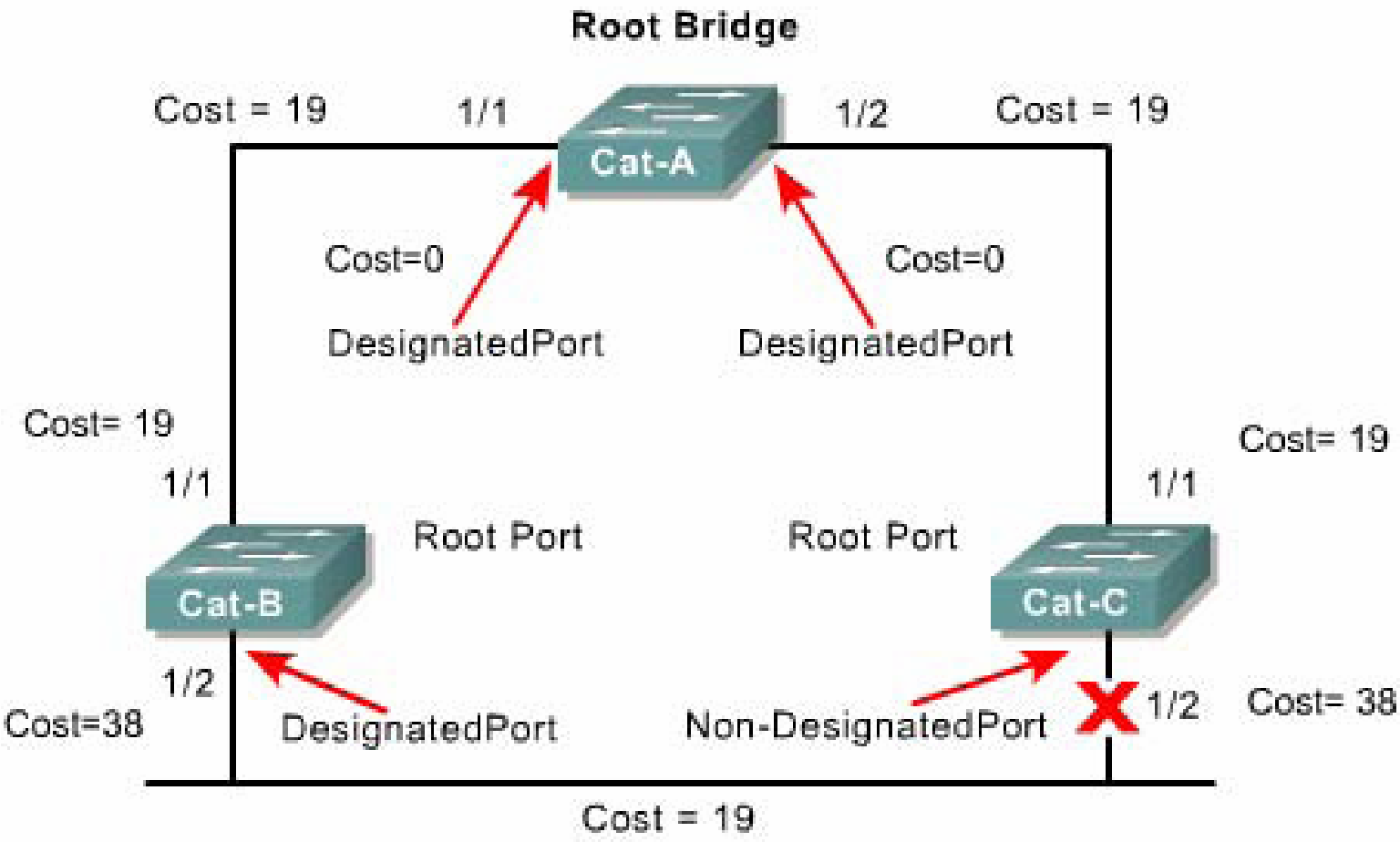
Chọn Root Bridge



- BPDU (mặc định gởi mỗi lần 2 giây)
- Root bridge = bridge với bridge ID nhỏ nhất
- Bridge ID = | Bridge Priority | MAC Address |

Giao thức Spanning-Tree

Kết quả tính toán của giao thức Spanning-Tree



Giao thức Spanning-Tree

Chọn Root Bridge

```
ALSwitch#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     0003.e334.6640
              Cost        19
              Port        23 (FastEthernet0/23)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000b.fc28.d400
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Port ID                      Designated                 Port ID
Name             Prio.Nbr      Cost Sts       Cost Bridge ID             Prio.Nbr
---------------- -------- --------- --- --------- -------------------- --------
Fa0/23           128.23          19 FWD         0 32768 0003.e334.6640 128.25

ALSwitch#
```

Giao thức Spanning-Tree

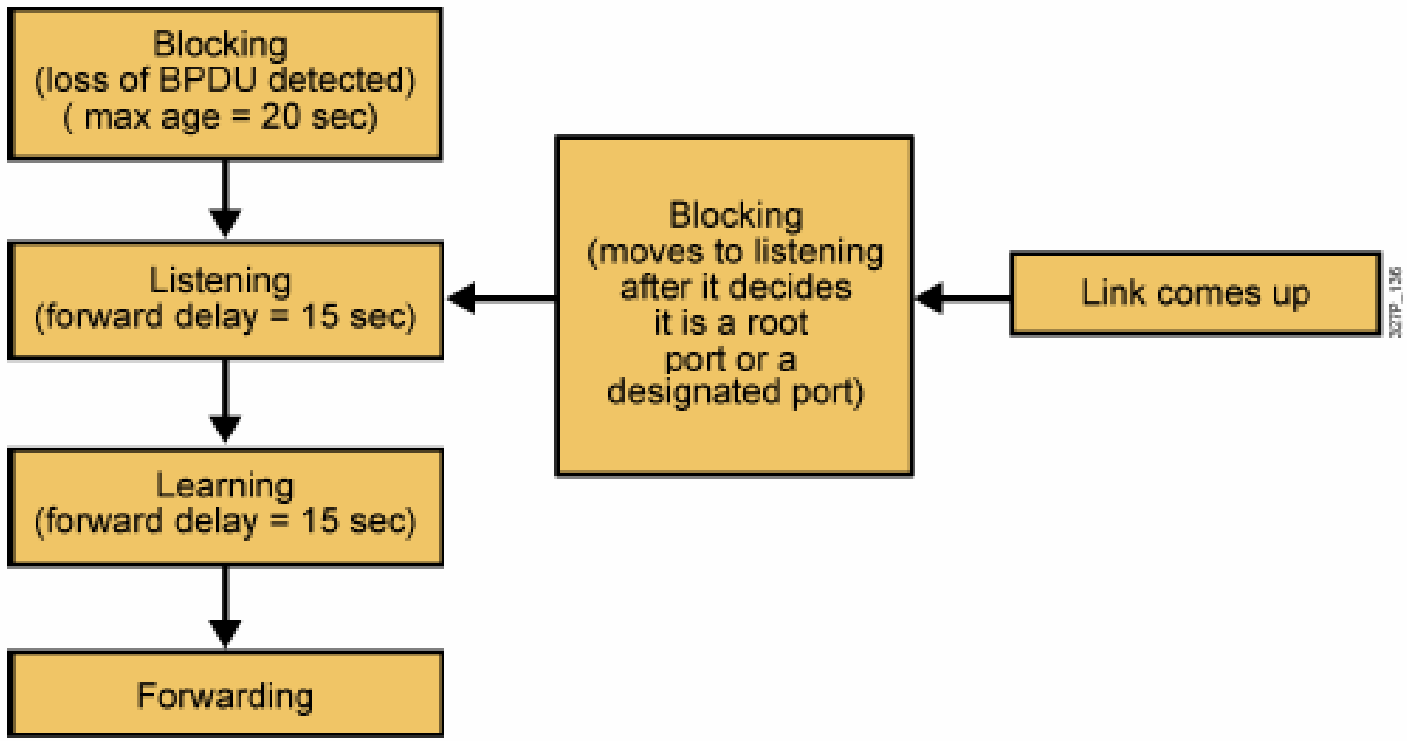
Chọn Root Porte

```
2950#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0003.e334.6640
             Cost        19
             Port        23 (FastEthernet0/23)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000b.fc28.d400
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Port ID                     Designated                 Port ID
Name             Prio.Nbr      Cost Sts      Cost Bridge ID             Prio.Nbr
---------------- -------- --------- --- --------- -------------------- --------
Fa0/23           128.23           19 FWD         0 32768 0003.e334.6640 128.2
```

Giao thức Spanning-Tree

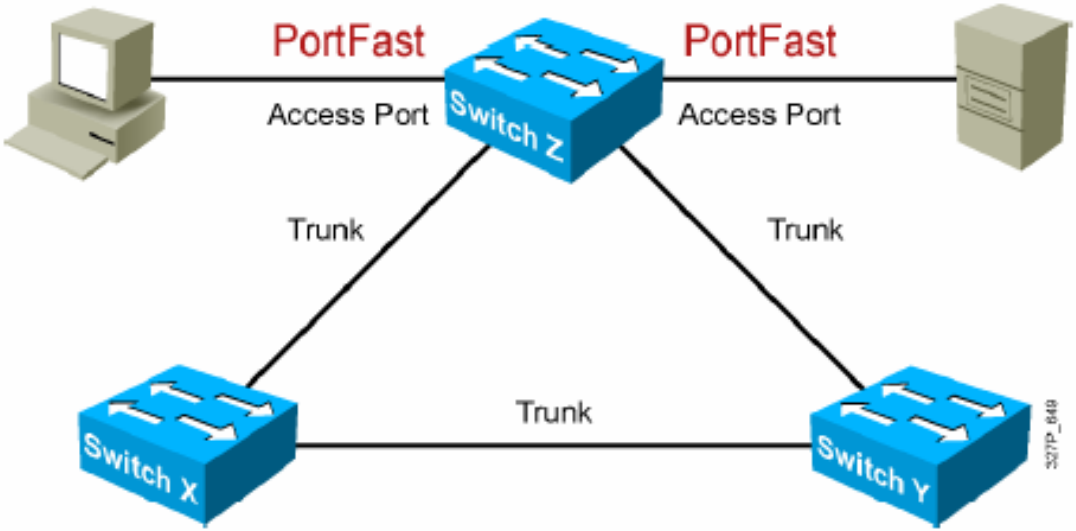
Trạng thái của các port trong Spanning-Tree

Spanning tree chuyển mỗi port ngang qua nhiều trạng thái khác nhau



Giao thức Spanning-Tree

PortFast



PortFast được cấu hình trên access ports, không phải trunk ports.

PortFast được cấu hình trên access port của switch để chuyển ngay từ trạng thái blocking sang trạng thái forwarding, bỏ qua trạng thái listening và learning.

Giao thức Spanning-Tree
cấu hình PortFast

```
SwitchX(config-if)#
spanning-tree portfast
```

- Cấu hình PortFast trên một interface

OR

```
SwitchX(config)#
spanning-tree portfast default
```

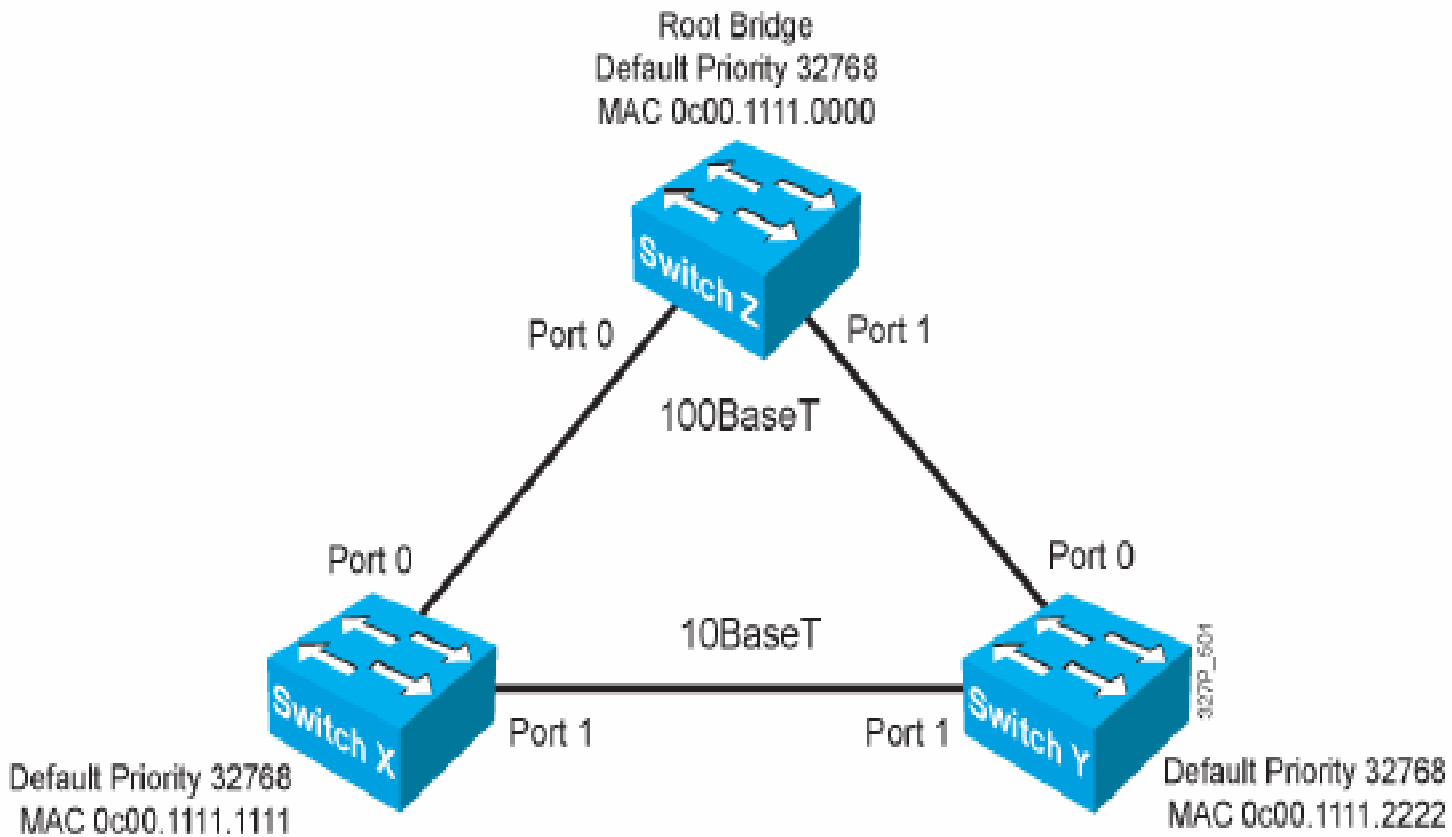
- Cấu hình PortFast trên tất cả interface không phải trunking

```
SwitchX#
show running-config interface interface
```

- Kiểm tra PortFast đã được cấu hình trên interface

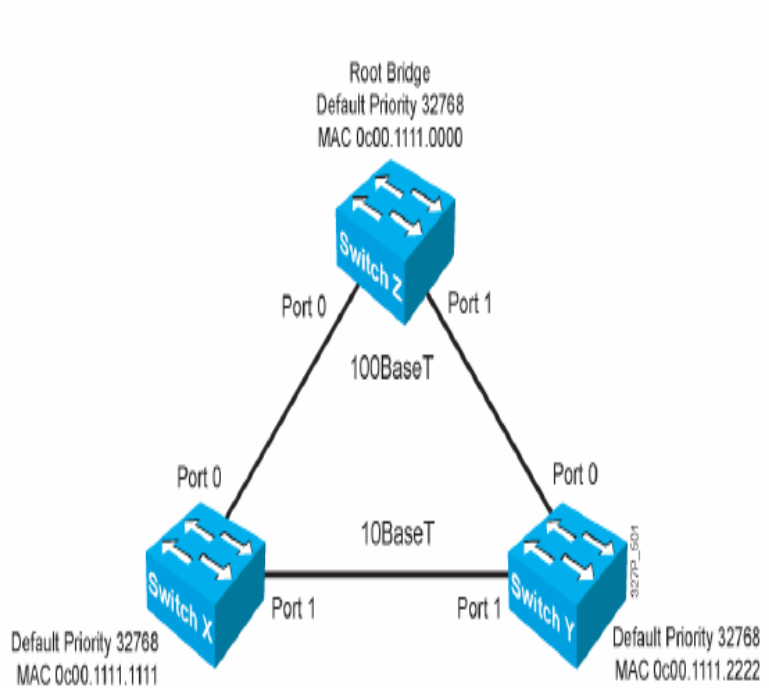
Giao thức Spanning-Tree

Hoạt động của giao thức Spanning-Tree



Giao thức Spanning-Tree

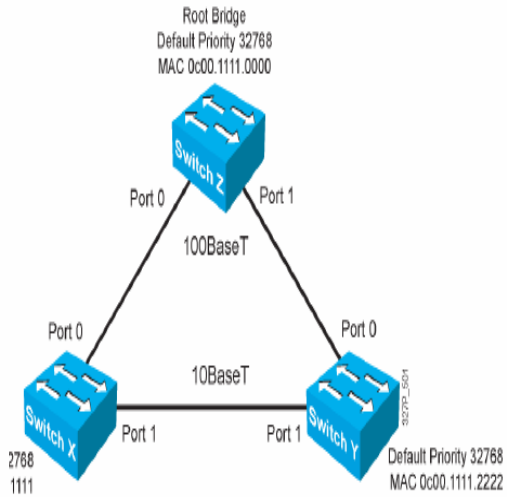
Hoạt động của giao thức Spanning-Tree



- Root bridge là switch Z, nó có BID nhỏ nhất.
- Root port là port 1 trên switch X và Y. Port 1 là đường có giá thành thấp nhất đến root trên cả 2 switch.

Giao thức Spanning-Tree

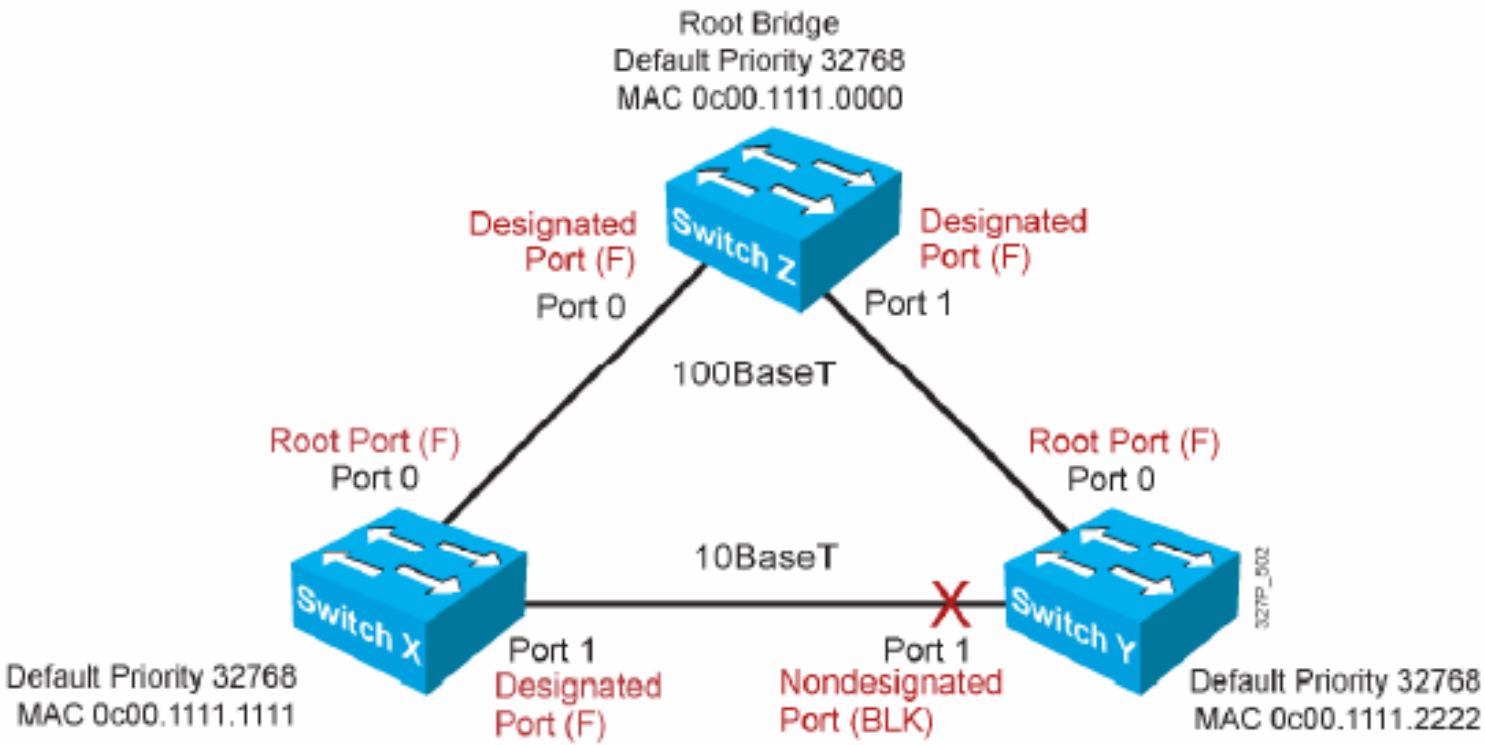
Hoạt động của giao thức Spanning-Tree



- Designated port trên switch Z là port 1 và 2. tất cả các port trên root là designated port. Port 2 của switch X là designated port cho segment giữa switch X và Y. Bởi vì switch X và Y có giá thành đường đi bằng nhau đến root bridge, designated port được chọn trên switch X bởi vì nó có BID thấp hơn Switch Y.
- Port 2 trên switch Y là nondesignated port trên segment và ở trạng thái blocking.
- Tất cả designated và root port đều ở trạng thái forwarding.

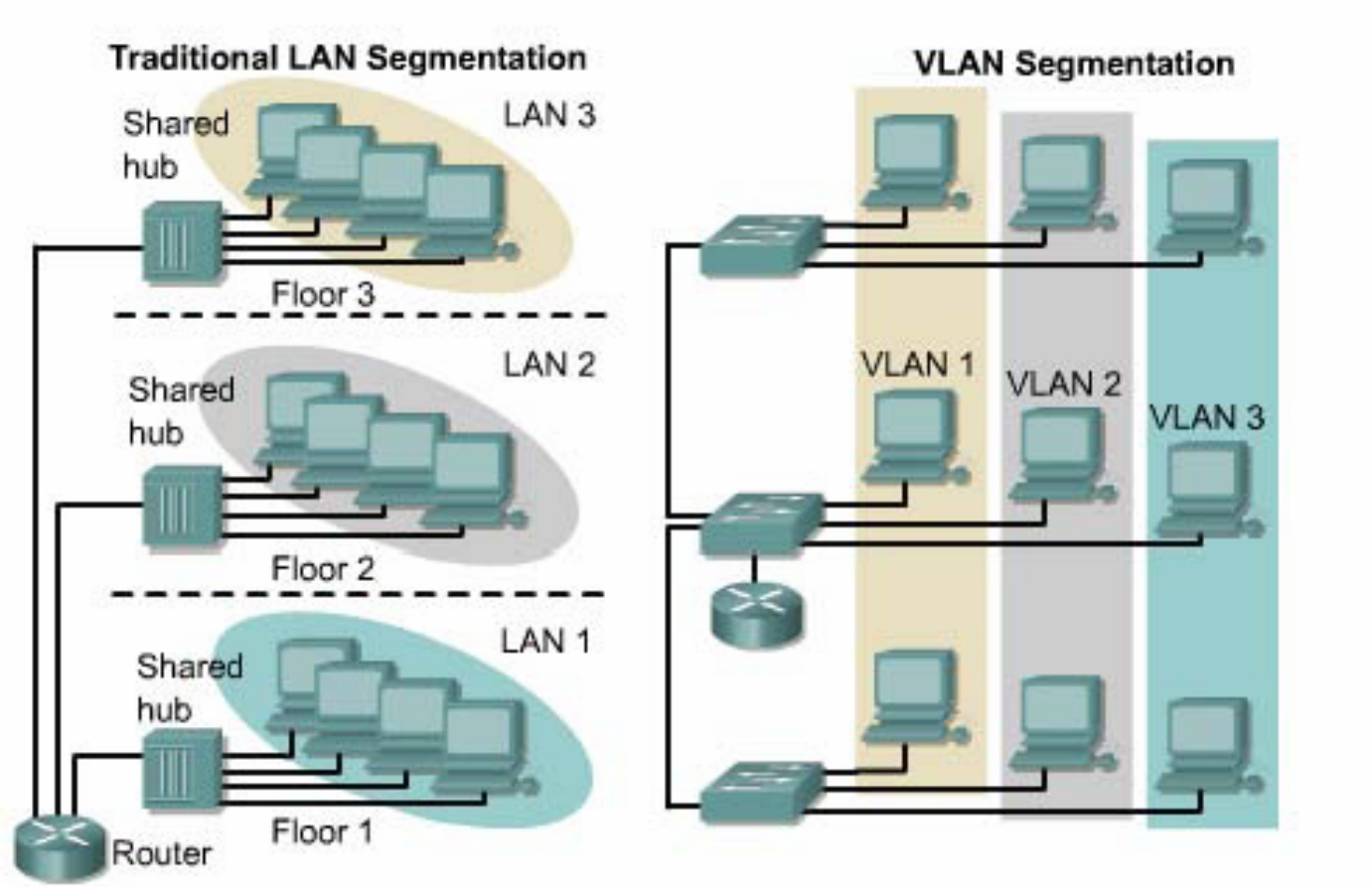
Giao thức Spanning-Tree

Tính toán lại Spanning-Tree

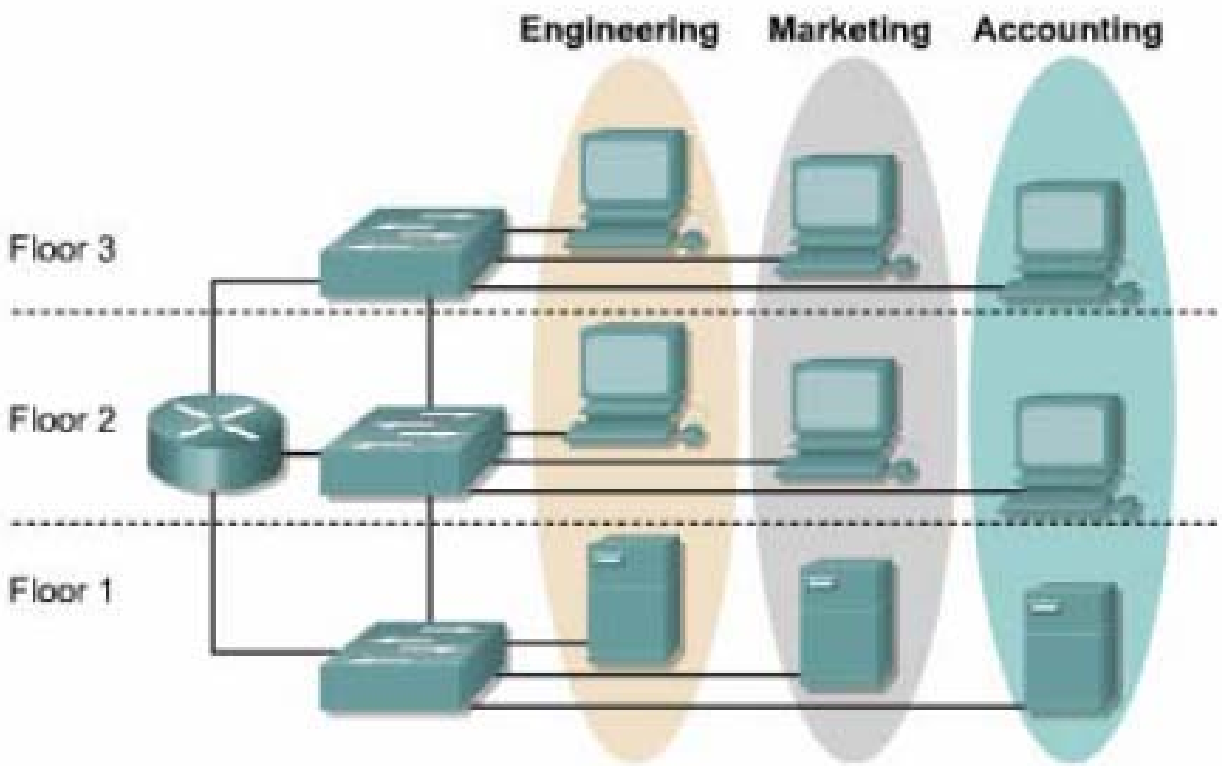


VLANs

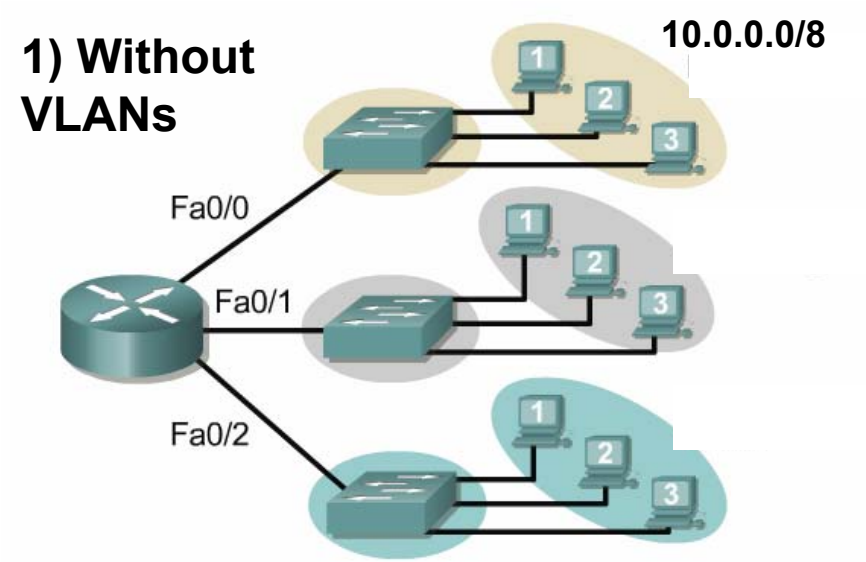
Phân đoạn mạng LAN truyền thống và theo VLAN

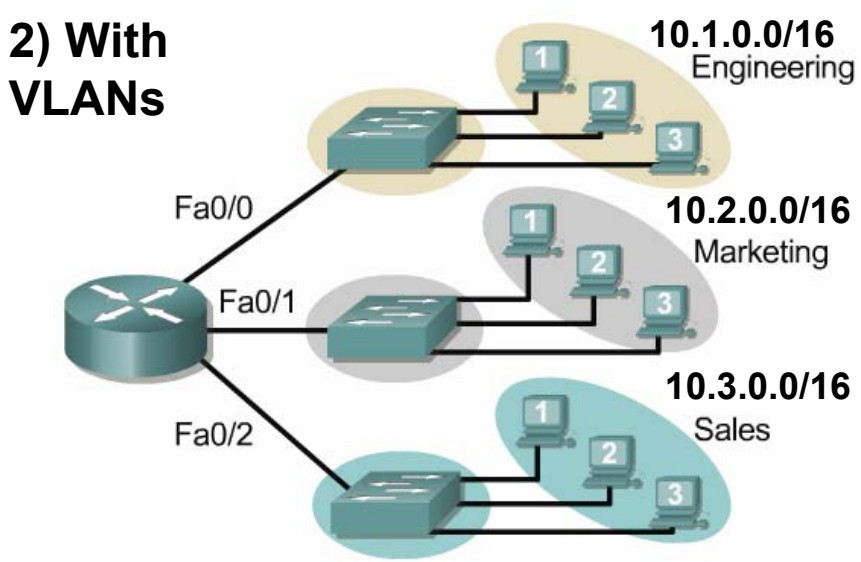


VLANs
Phân đoạn mạng LAN theo VLAN

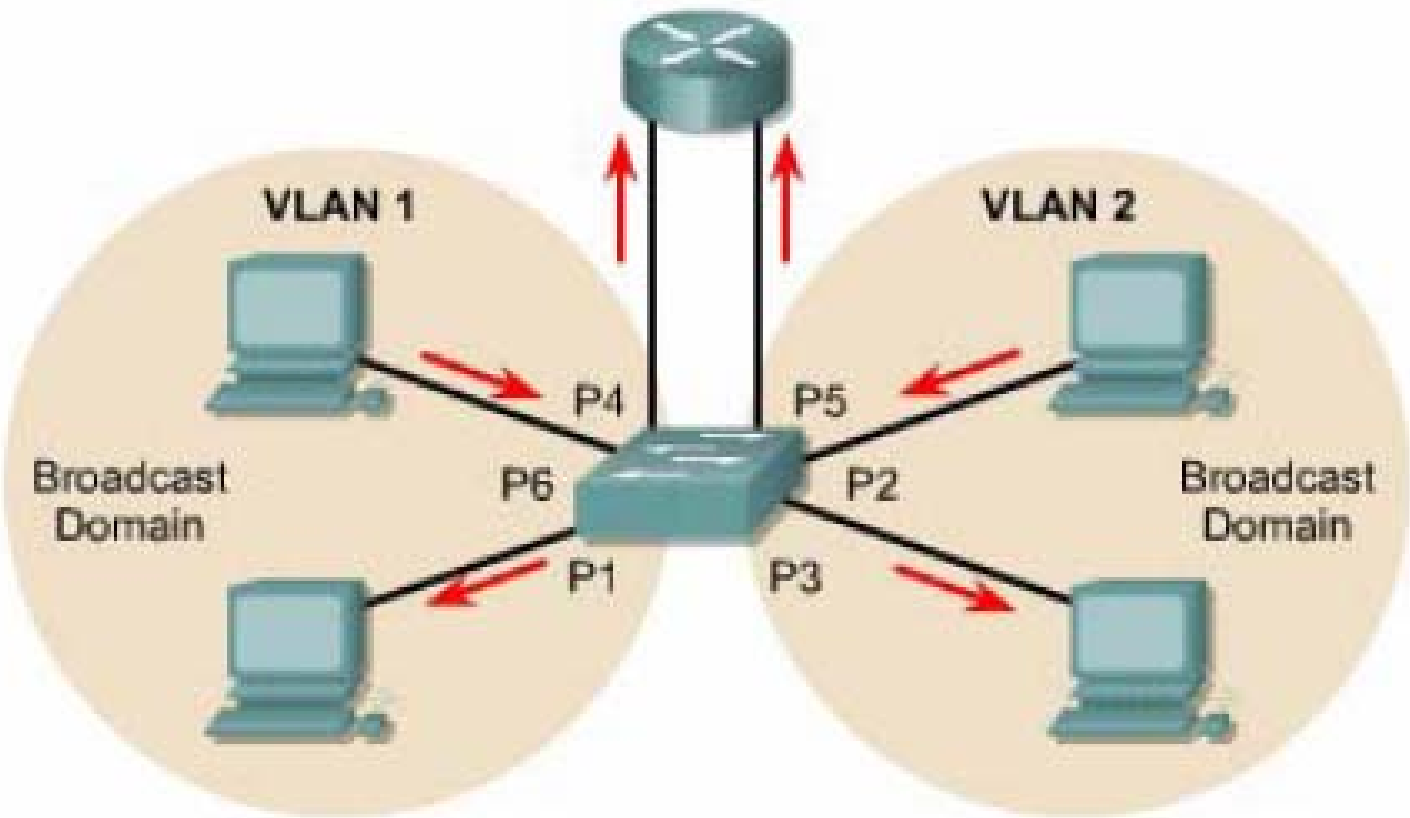


VLANs
Miền quảng bá với VLAN

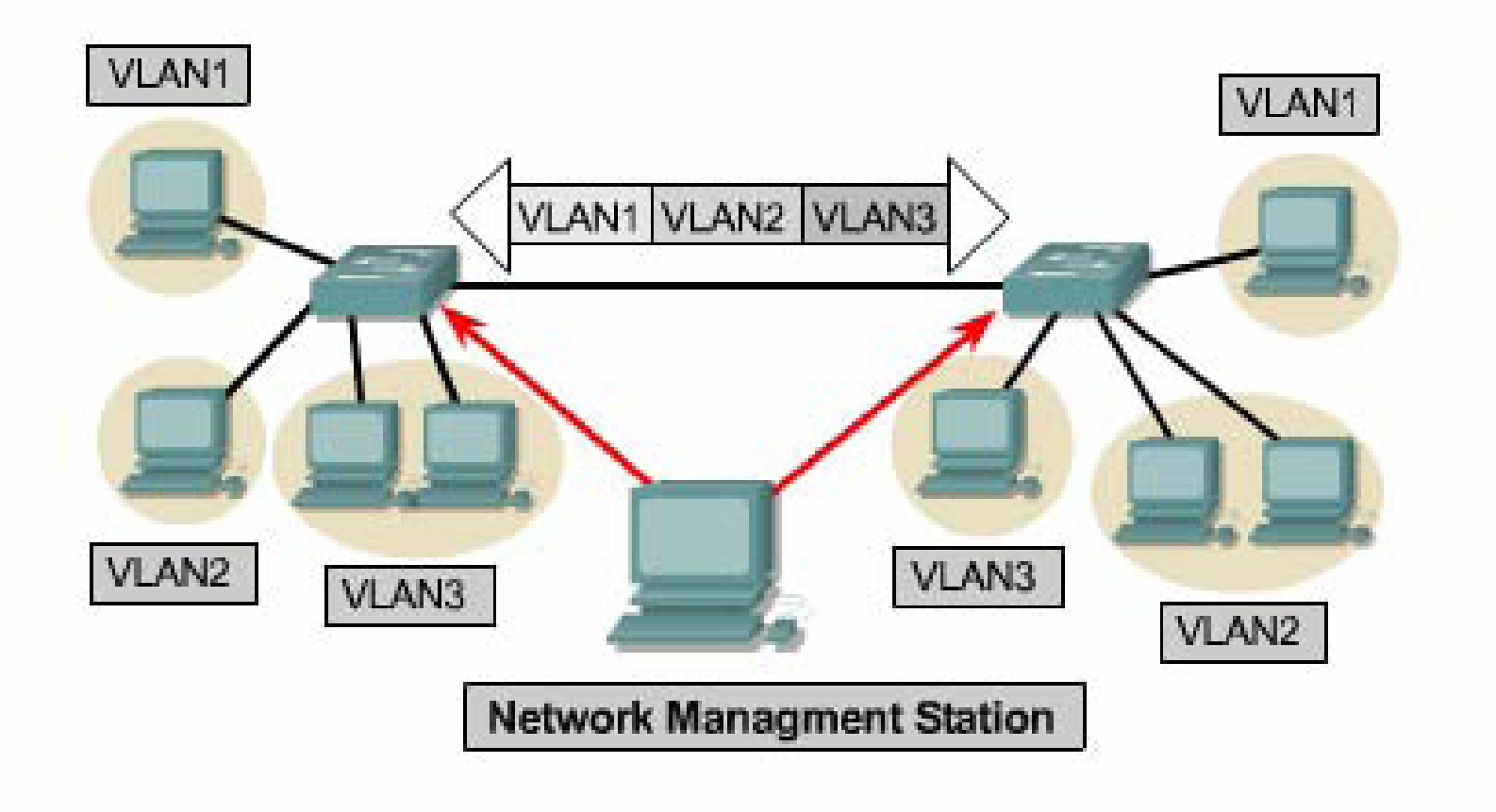




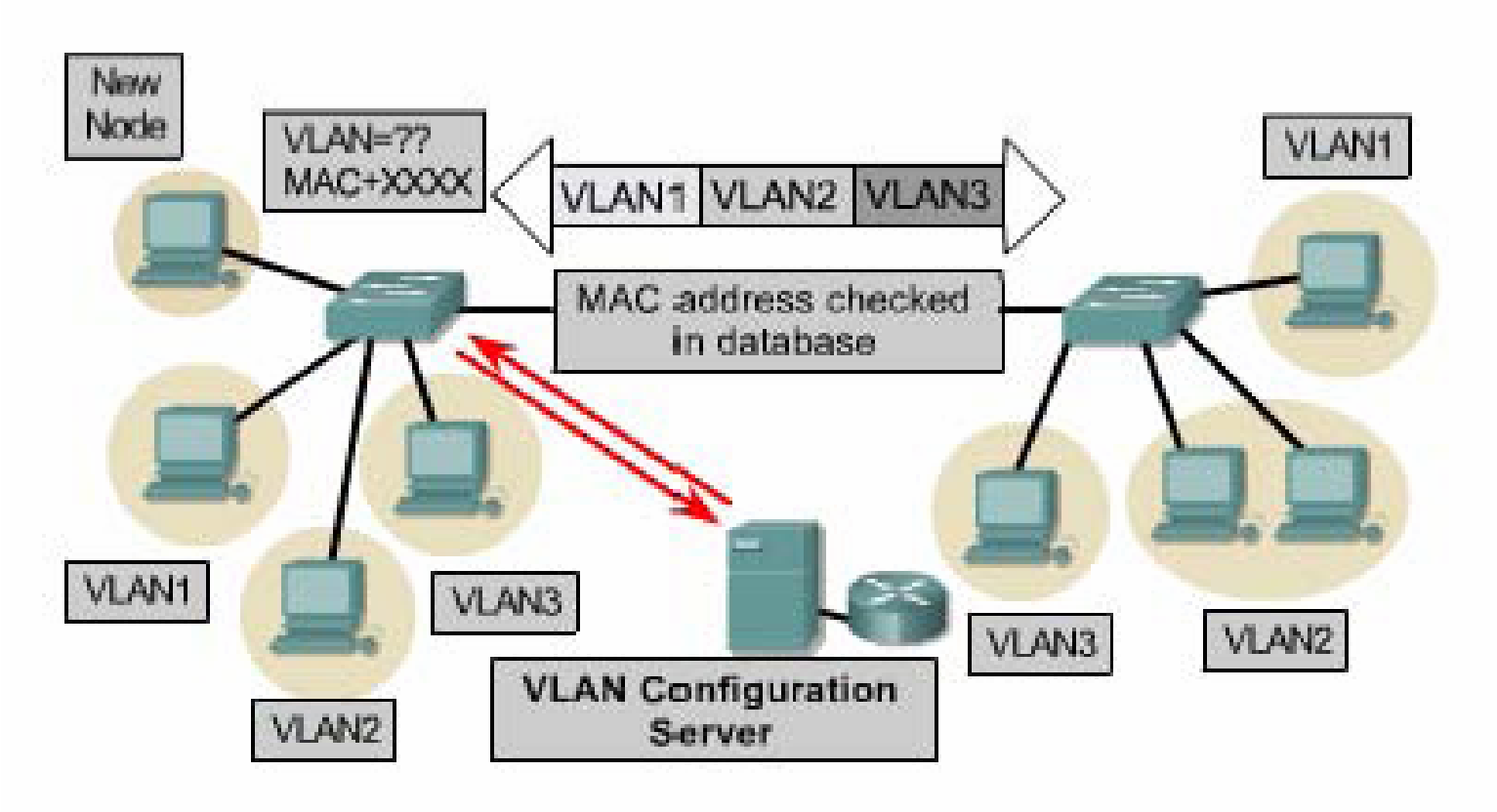
VLANs
Miền quảng bá với VLAN



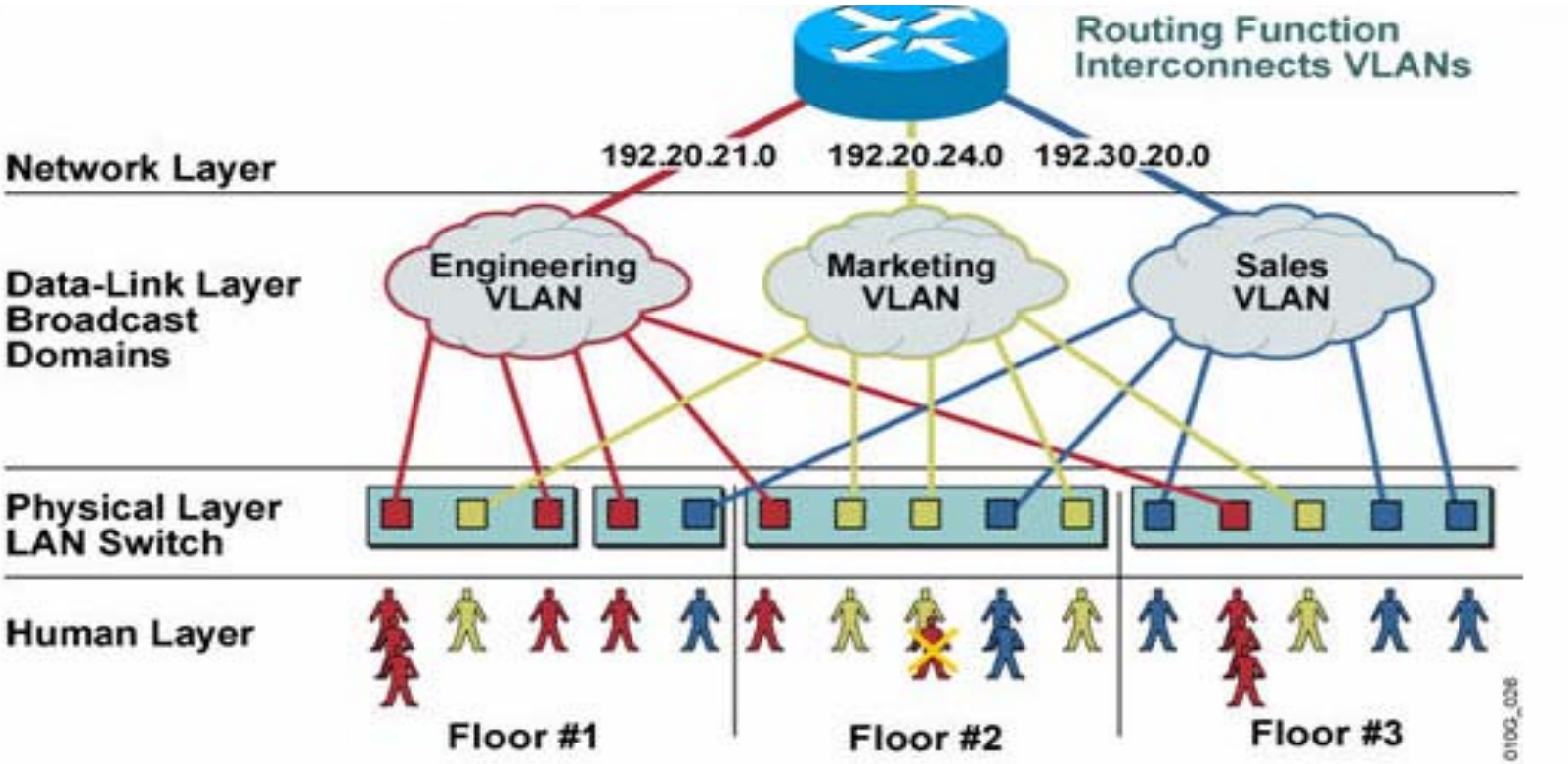
VLANs
VLAN cố định



VLANs
VLAN động



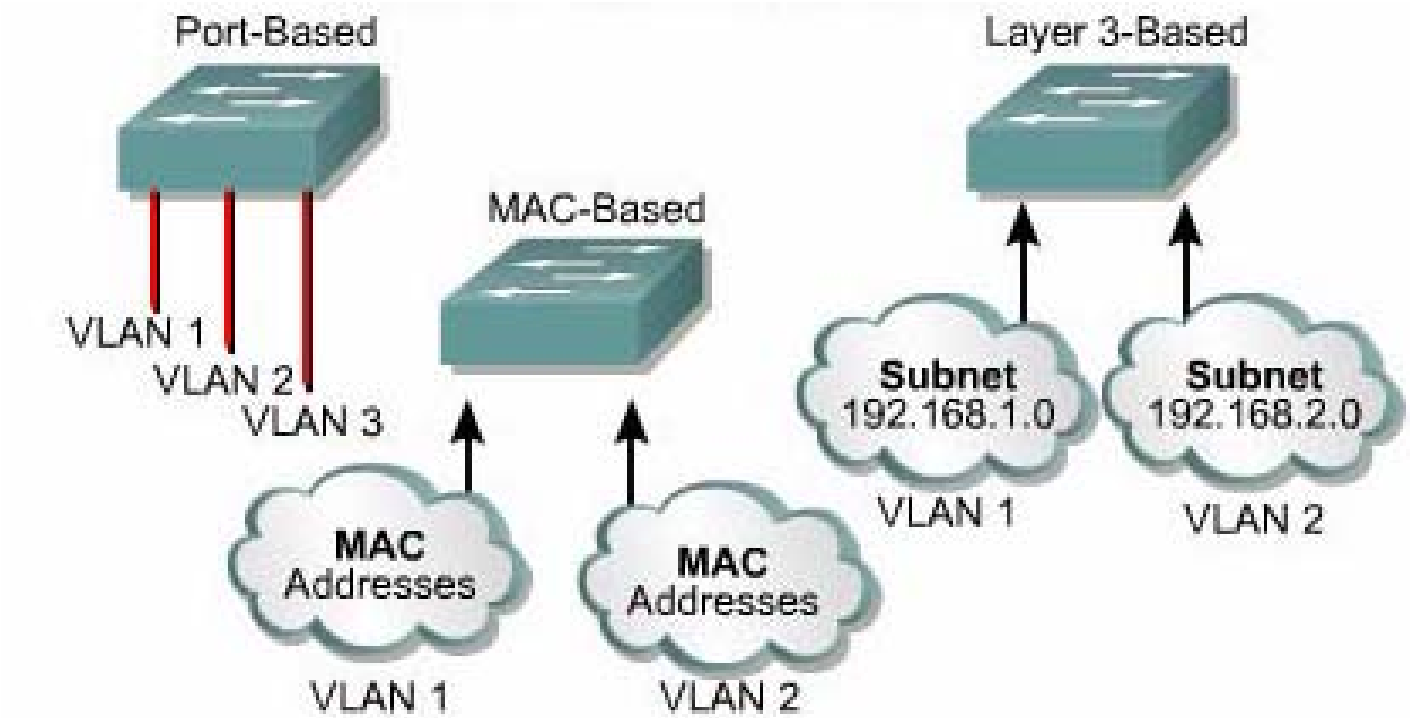
VLANs
Chia VLAN theo port



VLANs
Ích lợi của VLAN

- Di chuyển máy trạm trong LAN dễ dàng.
- Thêm máy trạm vào LAN dễ dàng.
- Thay đổi cấu hình LAN dễ dàng.
- Kiểm soát giao thông mạng dễ dàng.
- Gia tăng khả năng bảo mật.

VLANs
Các loại VLAN



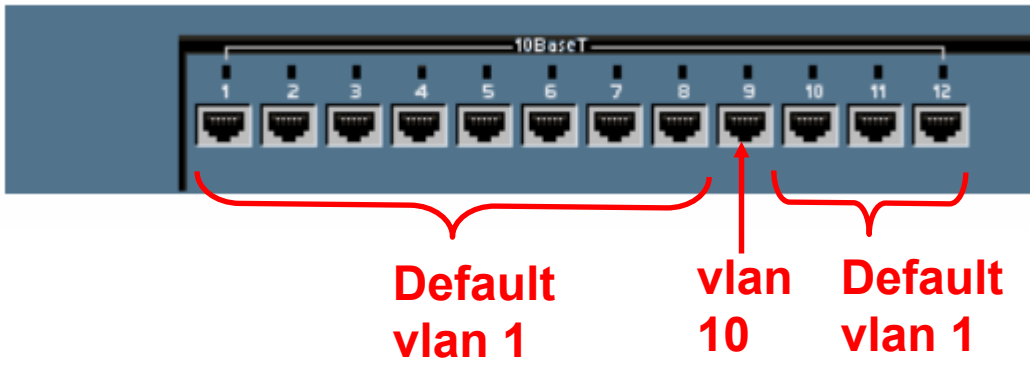
VLANs
Các loại VLAN

VLAN Types	Description
Port-based	• Most common configuration method. • Ports assigned individually, in groups, in rows, or across 2 or more switches. • Simple to use. • Often implemented where Dynamic Host Control Protocol (DHCP) is used to assign IP addresses to network hosts.
MAC address	• Rarely implemented today. • Each address must be entered into the switch and configured individually. • Users find it useful. • Difficult to administer, troubleshoot and manage.
Protocol Based	• Configured like MAC addresses, but instead uses a logical or IP address. • No longer common because of DHCP.

VLANs
Cấu hình VLAN cố định

- Số lượng VLAN tối đa phụ thuộc vào switch.
- VLAN 1 là VLAN mặc định.
- Switch phải ở chế độ VTP server để tạo, thêm hoặc xóa VLAN.
- Cấu hình VLAN:
  - Switch#vlan database
  - Switch(vlan)#vlan *vlan_number*
  - Switch(vlan)#exit
- Gán port vào VLAN:
  - Switch(config)#interface fastethernet 0/9
  - Switch(config-if)#switchport access vlan *vlan_number*

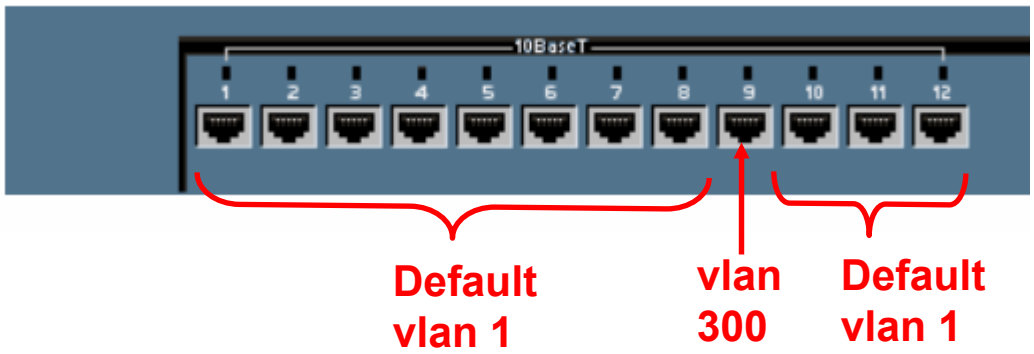
VLANs
Cấu hình VLAN cố định



- Assign ports to the VLAN
  - Switch(config)#**interface fastethernet 0/9**
  - Switch(config-if)#**switchport access vlan 10**

- **access** – Denotes this port as an access port and not a trunk link (later)

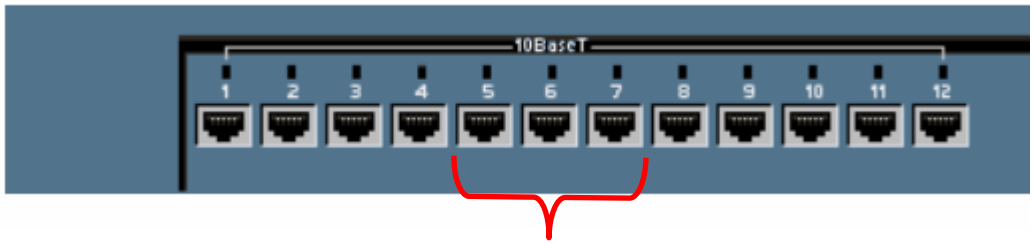
VLANs
Cấu hình VLAN cố định



Cisco

```
Enter configuration commands, one per line. End with CNTL/Z.

SydneySwitch#config terminal
SydneySwitch(config)#interface fastethernet 0/9
SydneySwitch(config-if)#switchport access vlan 300
SydneySwitch(config-if)#exit
SydneySwitch(config)#exit
```

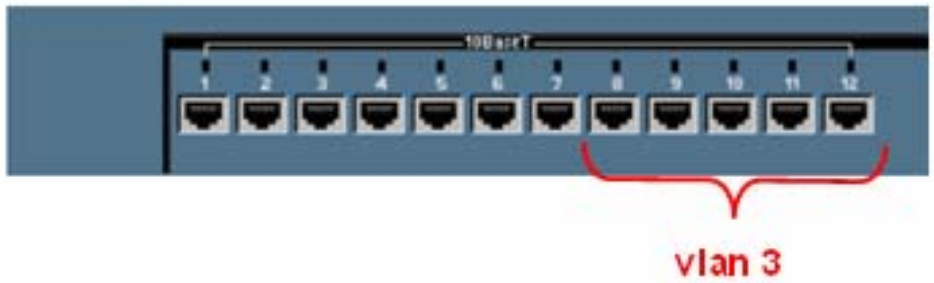
VLANs
Cấu hình VLAN cố định



vlan 2

- SydneySwitch(config)#**interface fastethernet 0/5**
- SydneySwitch(config-if)#**switchport access vlan 2**
- SydneySwitch(config-if)#**exit**
- SydneySwitch(config)#**interface fastethernet 0/6**
- SydneySwitch(config-if)#**switchport access vlan 2**
- SydneySwitch(config-if)#**exit**
- SydneySwitch(config)#**interface fastethernet 0/7**
- SydneySwitch(config-if)#**switchport access vlan 2**

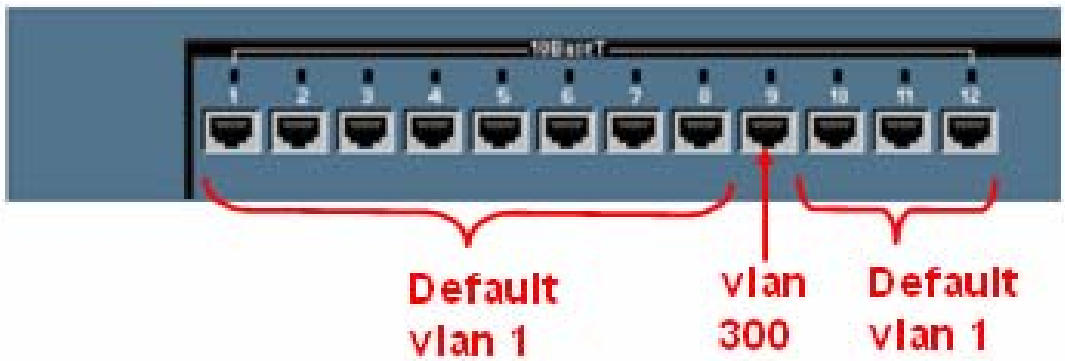
VLANs
Cấu hình VLAN cố định




```
SydneySwitch(config)#interface range fastethernet 0/8,
   fastethernet 0/12
SydneySwitch(config-if)#switchport access vlan 3
SydneySwitch(config-if)#exit
```

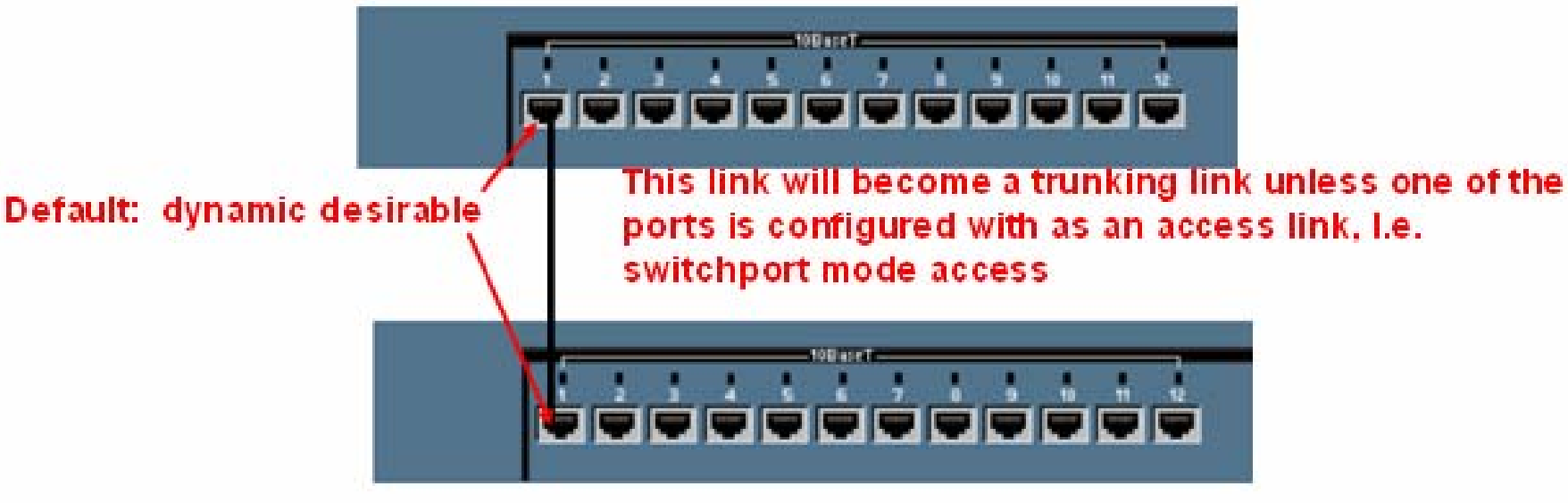
This command does not work on all 2900 switches, such as the 2900 Series XL. It does work on the 2950.

VLANs
Cấu hình VLAN cố định

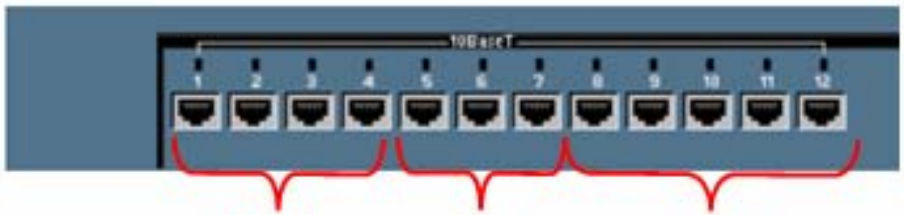



```
SydneySwitch(config)#interface fastethernet 0/1
SydneySwitch(config-if)#switchport mode access
SydneySwitch(config-if)#exit
```

VLANs
Cấu hình VLAN cố định

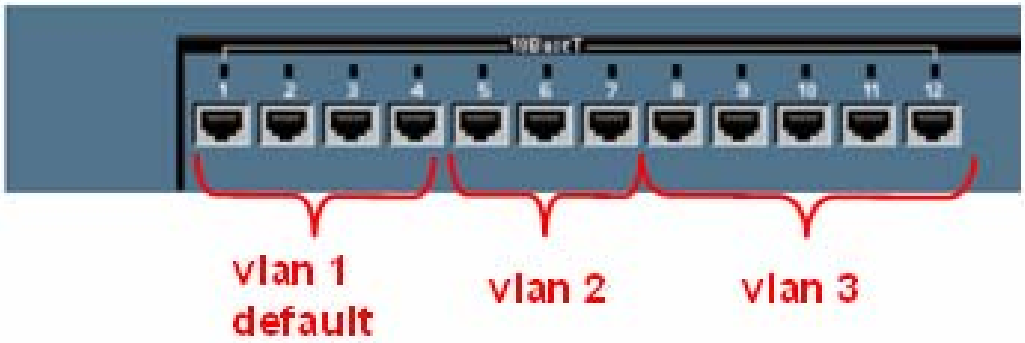


VLANs
Kiểm tra cấu hình VLAN



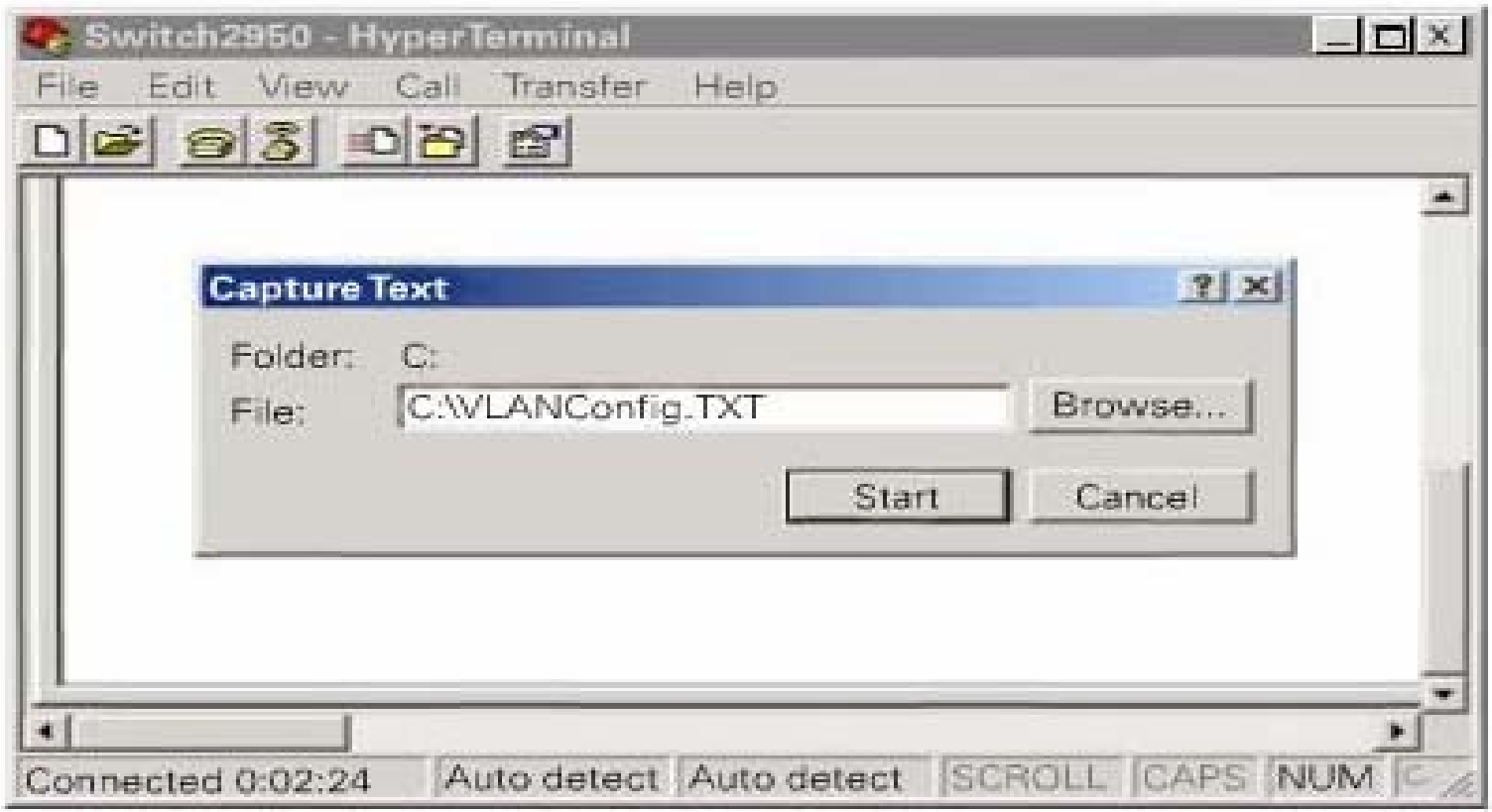

```
SydneySwitch#show vlan

VLAN Name                Status    Ports
---- ------------------- ------- -------------------------------

VLAN Name                Status    Ports
---- ------------------- ------- -------------------------------
1    default             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
2    VLAN2               active    Fa0/5, Fa0/6, Fa0/7
3    VLAN3               active    Fa0/8, Fa0/9, Fa0/10, Fa0/11,
                                   Fa0/12
1002 fddi-default        active
1003 token-ring-default  active
1004 fddinet-default     active
1005 trnet-default       active

VLAN Type SAID MTU  Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ---- ---- ---- ------ ------ -------- ---------- ------ -------
1    enet 100001 1500  -      -      -        -    -      1002   1003
2    enet 100002 1500  -      -      -        -    -      0      0
```

VLANs
Kiểm tra cấu hình VLAN




```
SydneySwitch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
2    VLAN2                            active    Fa0/5, Fa0/6, Fa0/7
3    VLAN3                            active    Fa0/8, Fa0/9, Fa0/10, Fa0/11,
                                                Fa0/12
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

VLANs
Lưu cấu hình VLAN

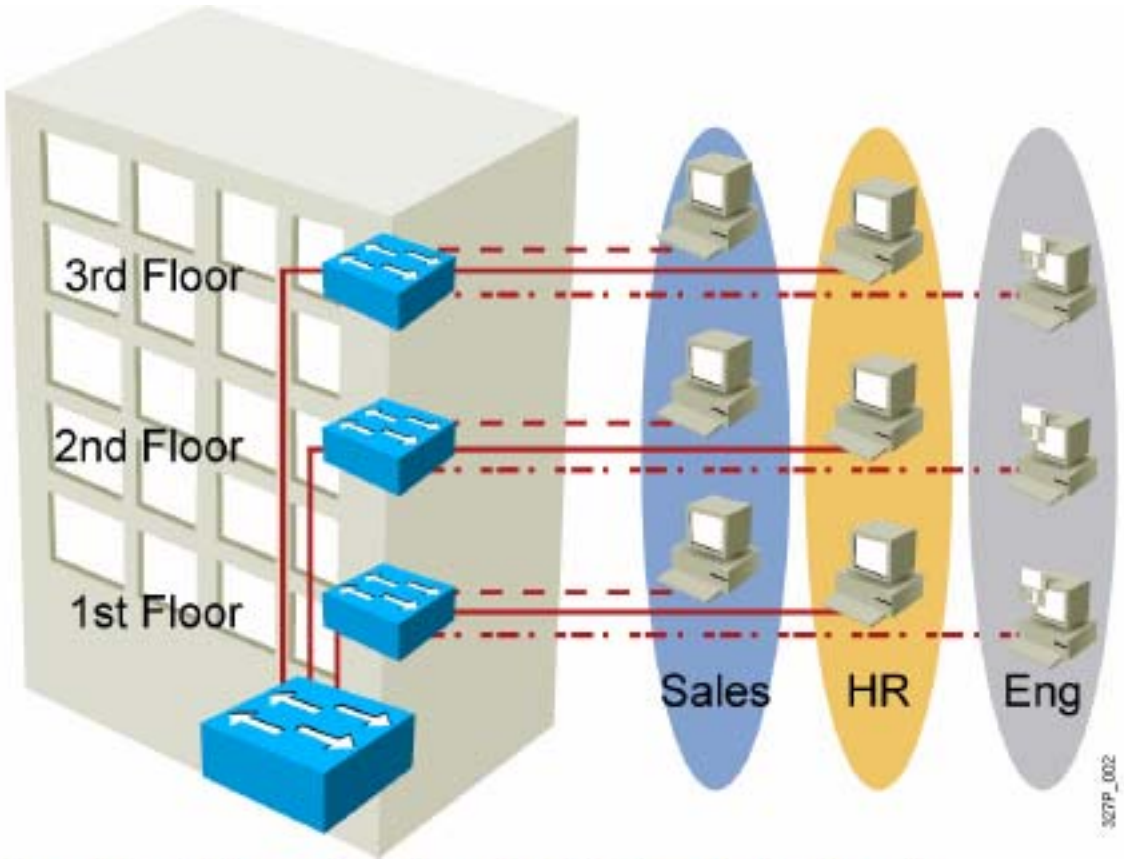


VLANs
Xoá VLAN

```
Switch(config)#interface fastethernet 0/9
Switch(config-if)#no switchport access vlan 300
```

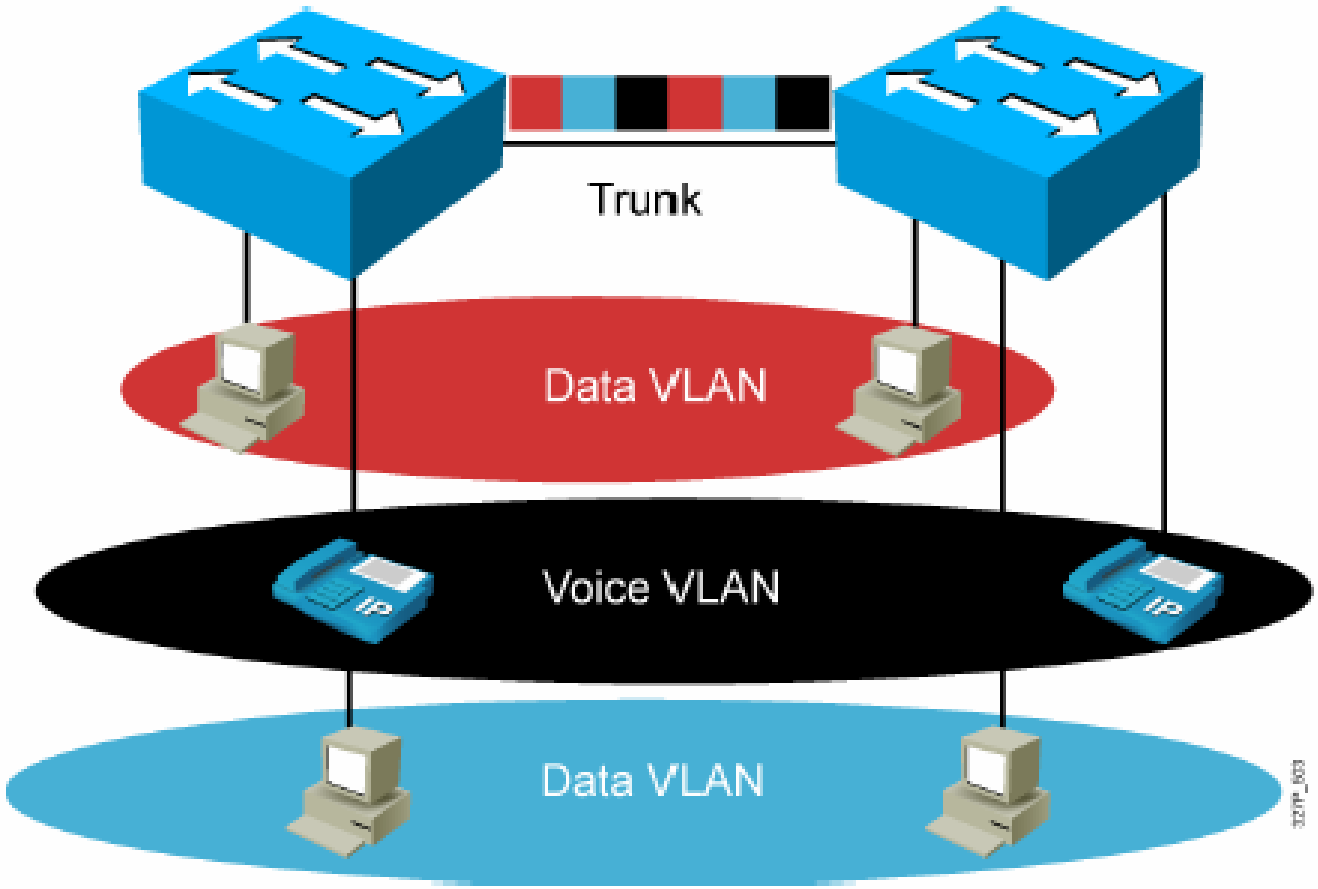
VTP (VLAN Trunking Protocol)
VLANs

- Phân đoạn
- Linh hoạt
- Bảo mật

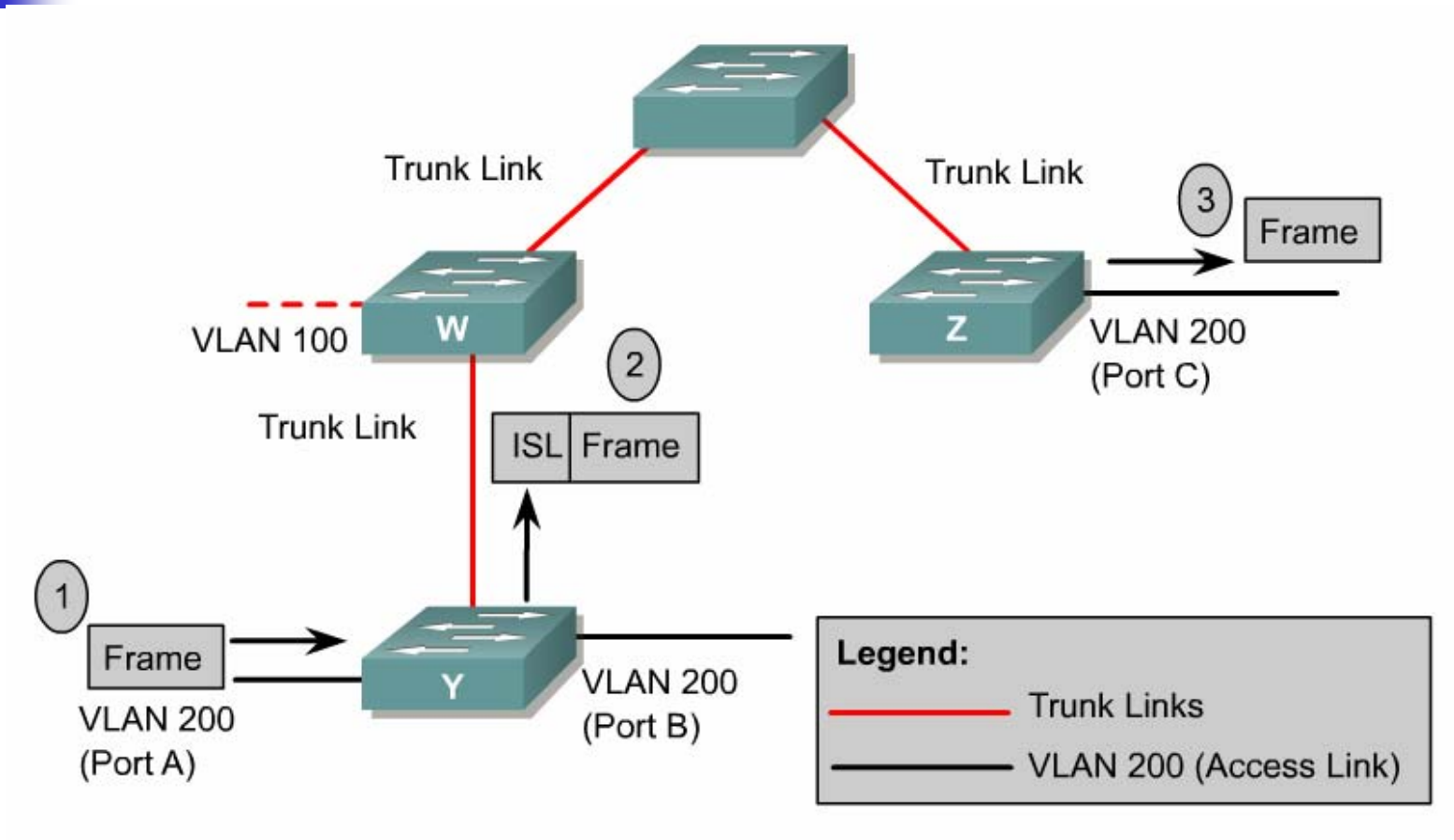


VLAN = Broadcast Domain = Logical Network (Subnet)

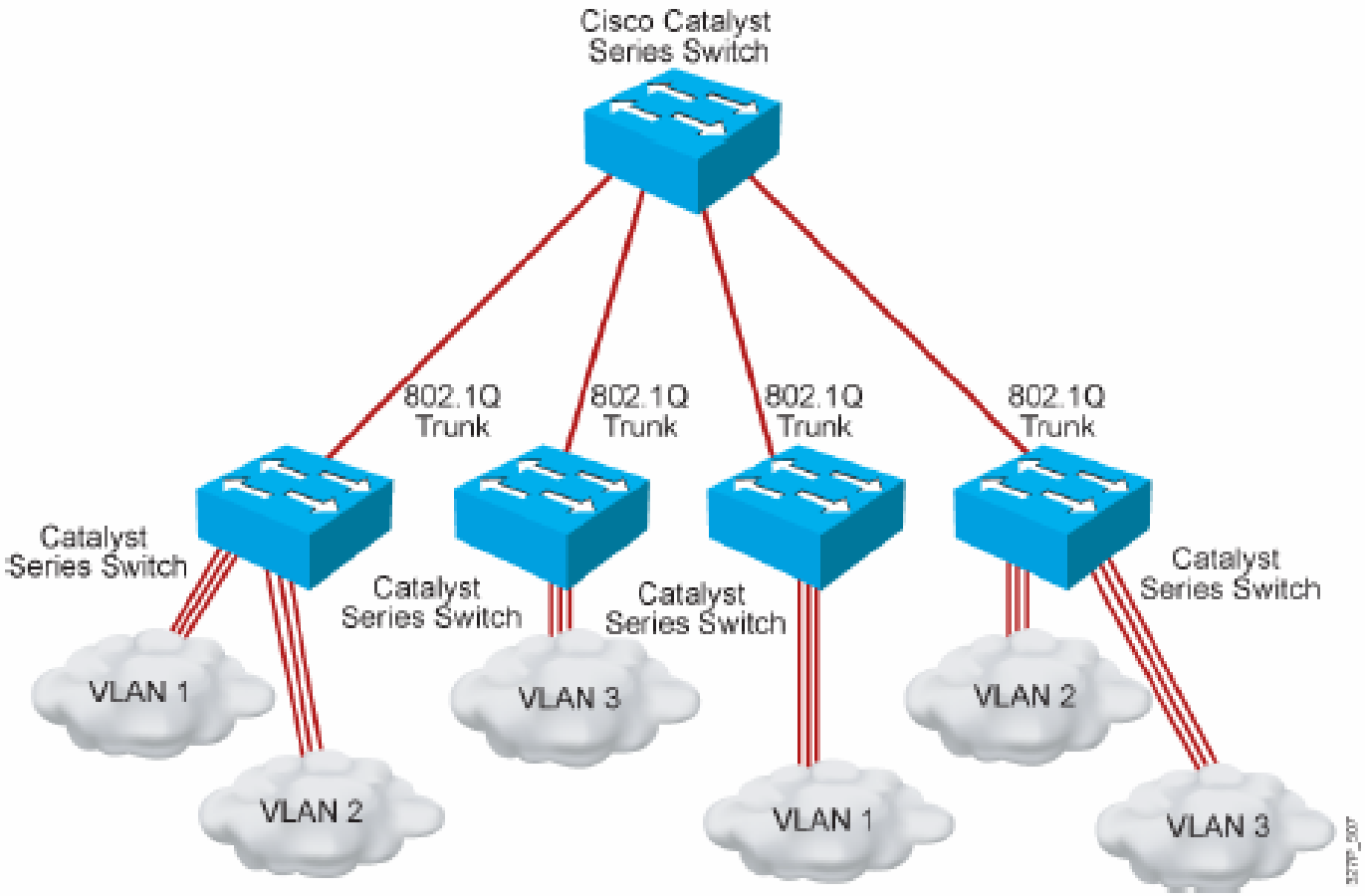
VTP (VLAN Trunking Protocol)
Trunking operation



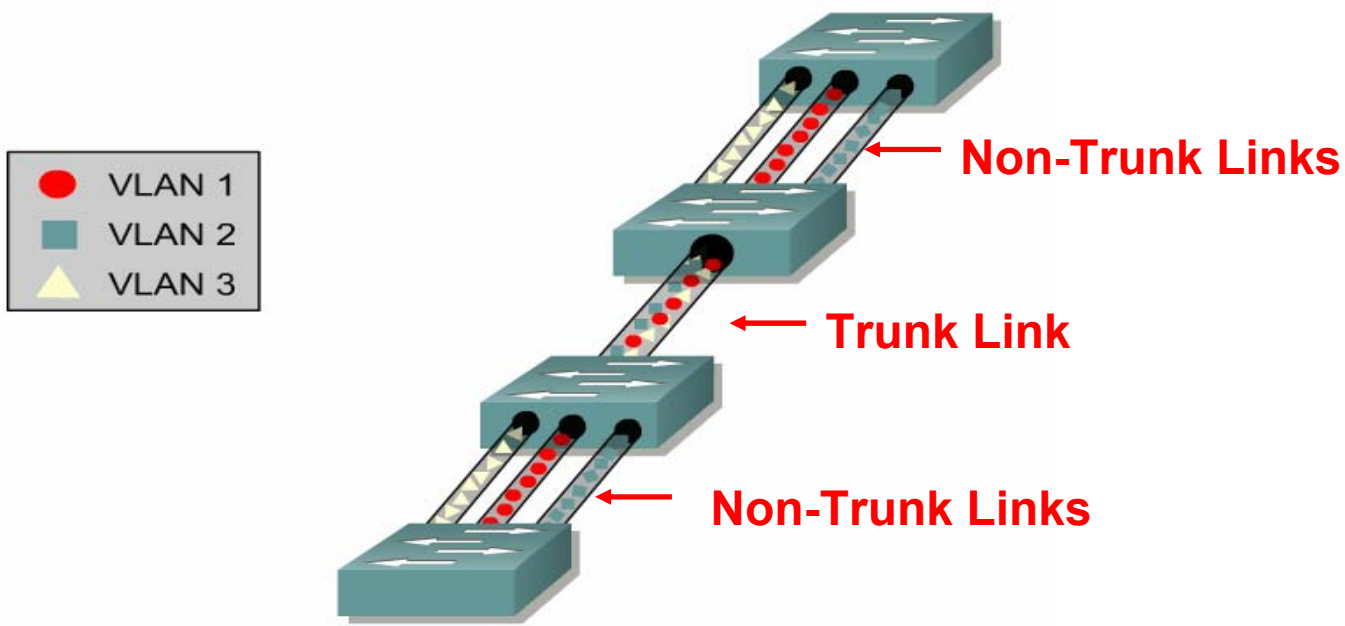
VTP (VLAN Trunking Protocol)
Trunking operation



VTP (VLAN Trunking Protocol)
Trunking operation



VTP
VLANs và Trunking



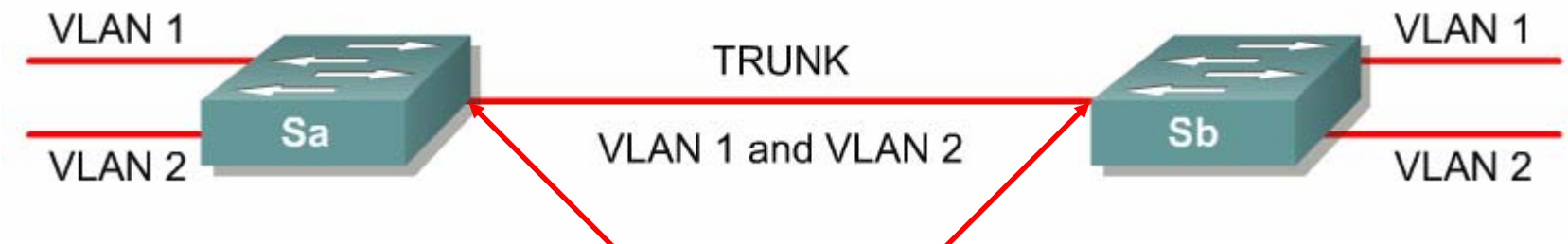
- Đường Trunk là một kết nối điểm nối điểm giữa một hay nhiều interface của switch và các thiết bị router hoặc switch khác.
- 802.1Q
- ISL

VTP
Cấu hình Trunking

```
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk ?
allowed         Set allowed VLAN characteristics when
                interface is in trunking mode
encapsulation   Set trunking encapsulation when interface
                is in trunking mode
native          Set trunking native characteristics when
                interface is in trunking mode
pruning         Set pruning VLAN characteristics when
                interface is in trunking mode

Switch(config-if)#switchport trunk encap ?
dot1q   Interface uses only 801.1q trunking encapsulation
        when trunking
isl     Interface uses only ISL trunking encapsulation
        when trunking
```

Lưu ý: Trên nhiều switches, lệnh **switchport trunk encapsulation** cần phải được thực hiện trước lệnh **switchport mode trunk.**

VTP
Cấu hình Trunking



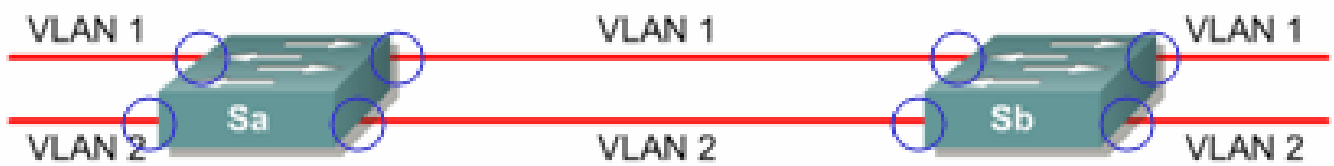

```
Switch(config-if)#switchport trunk encap ?
dot1q  Interface uses only 801.1q trunking encapsulation
       when trunking
isl    Interface uses only ISL trunking encapsulation
       when trunking
```

Switch(config-if)switchport trunk encapsulation [dot1q|isl]

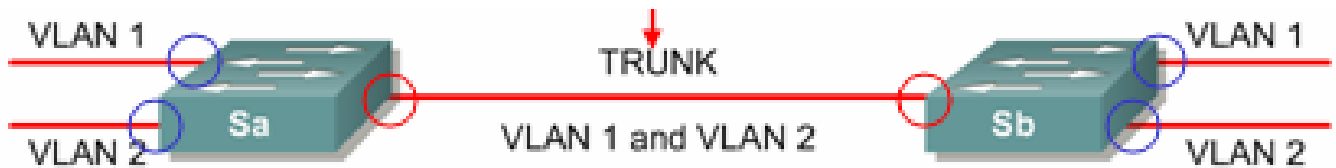
VTP
Cấu hình Trunking

```
Switch(config-if)#switchport mode trunk
```

```
Switch(config-if)switchport mode [access|trunk]
```

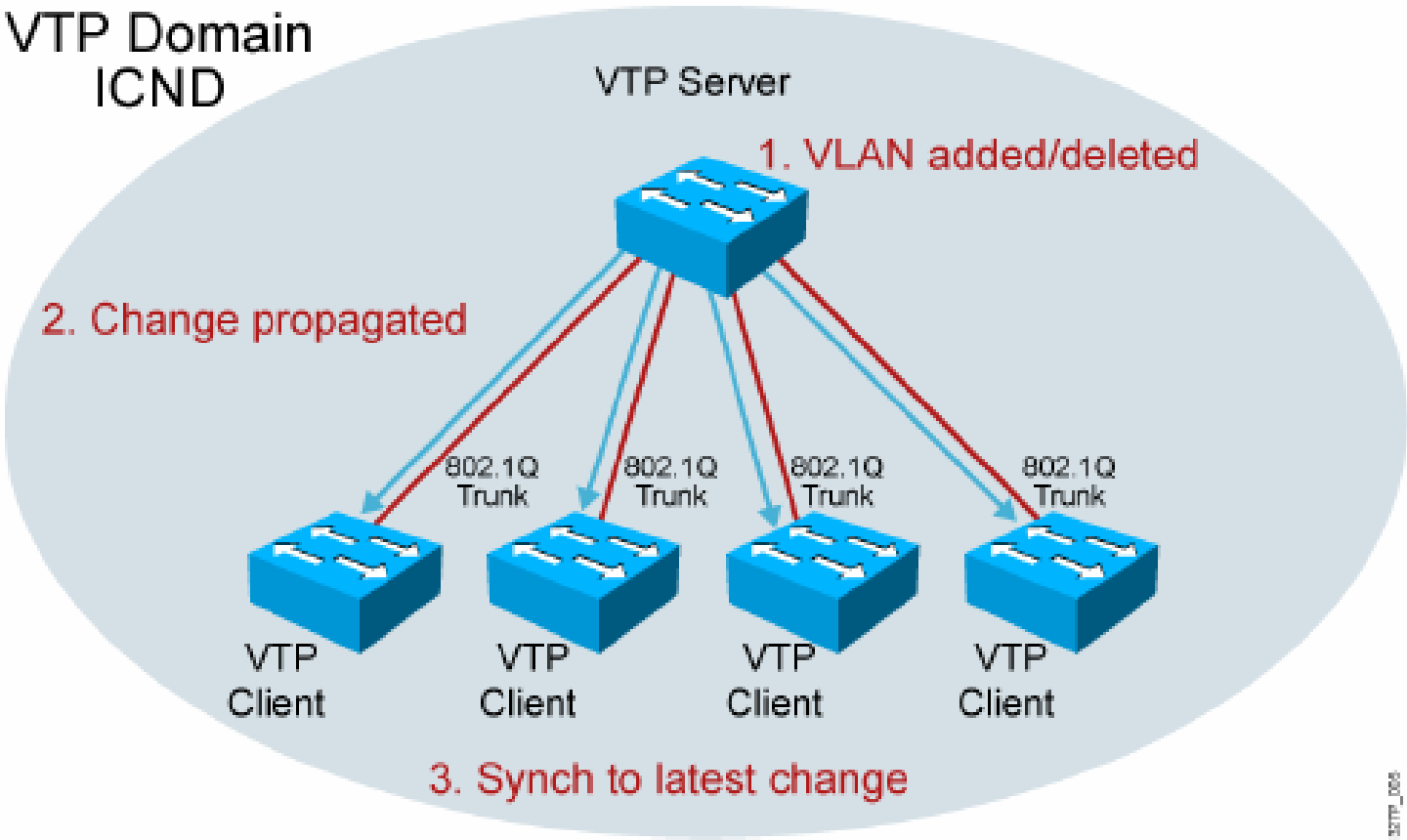



```
Switch(config-if)switchport mode access
```



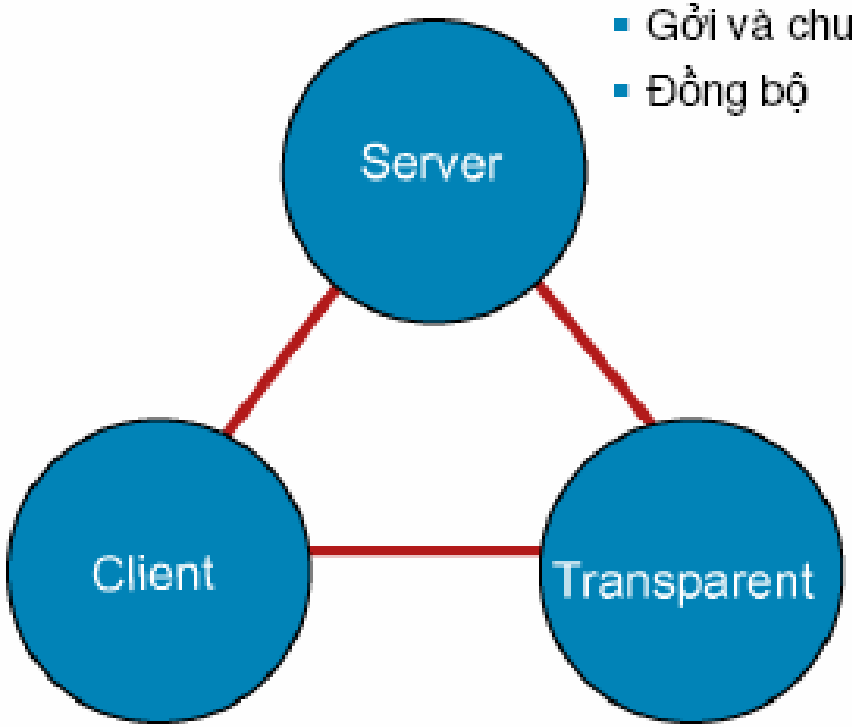

```
Switch(config-if)switchport mode trunk
```

VTP
Tính năng của VTP



VTP
Cơ chế của VTP

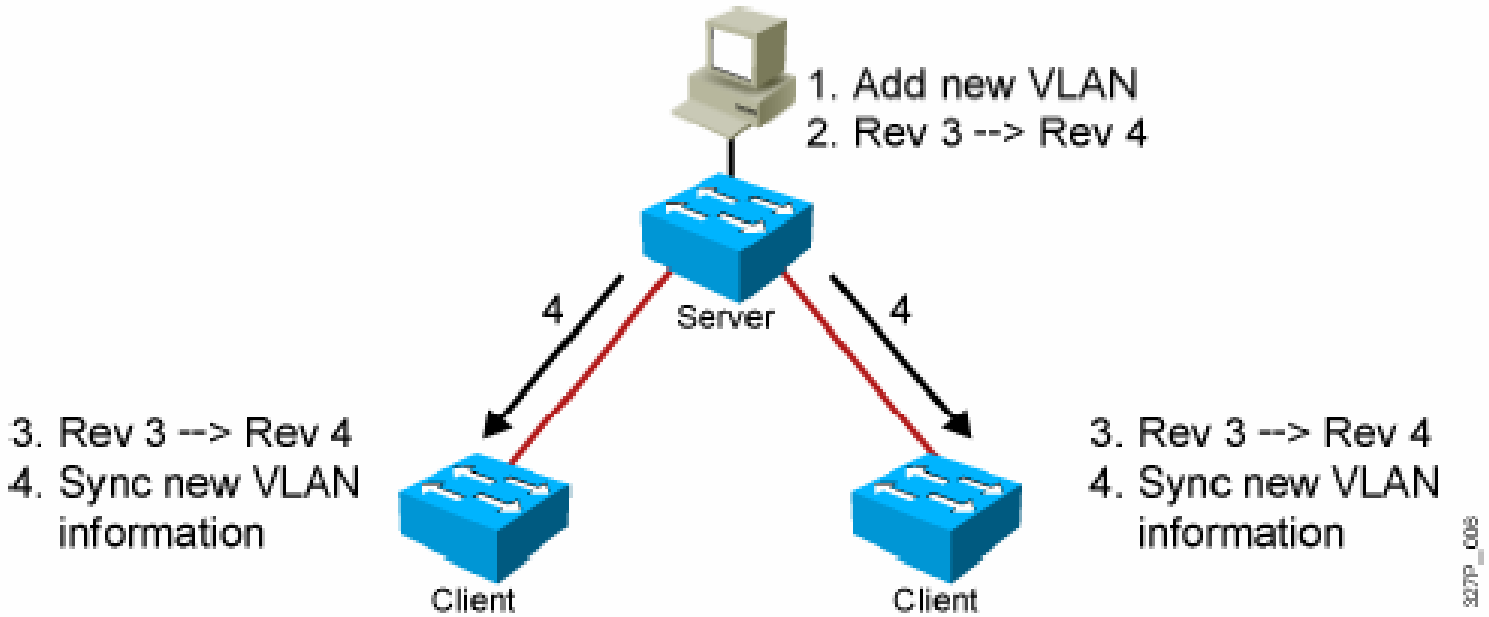
- Tạo VLANs
- Chỉnh sửa VLANs
- Xóa VLANs
- Gởi và chuyển quảng bá
- Đồng bộ



- Không thể tạo, thay đổi, hoặc xóa VLANS
- Gởi và chuyển những quảng bá
- Đồng bộ

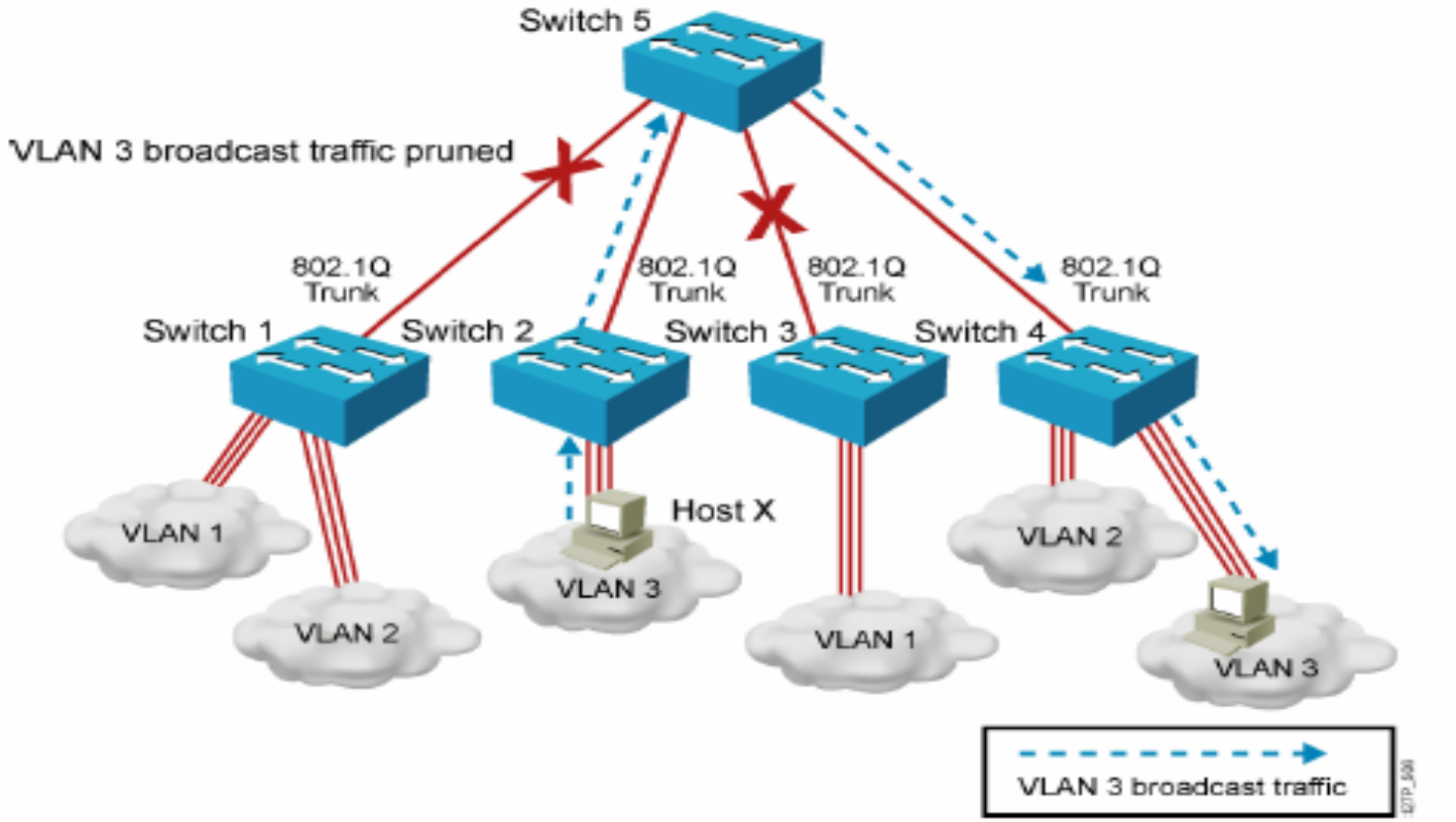
- Chỉ tạo VLANs cục bộ
- Chỉnh sửa VLANs cục bộ
- Xóa VLANs cục bộ
- Chuyển quảng bá
- Không đồng bộ

VTP
Hoạt động của VTP



- Thông điệp VTP được gởi như là multicast.
- VTP servers and clients được đồng bộ đến revision number sau cùng.
- Thông điệp VTP được gởi mỗi lần 5phút hoặc khi có thay đổi.

VTP
VTP Pruning



VTP Pruning dùng thông điệp VLAN để quyết định khi nào một đường trunk đang flood thông tin không cần thiết

VTP
Cấu hình VTP

- VTP mặc định trên Cisco Catalyst switch:
  - VTP domain name: None
  - VTP mode: Server mode
  - VTP pruning: Enabled or disabled (model specific)
  - VTP password: Null
  - VTP version: Version 1
- Một switch mới có thể tự động trở thành phần của domain khi nó nhận được một thông điệp từ server.
- Một VTP client có thể viết đè một database của VTP server database nếu client có revision number cao hơn.
- Một domain name không thể xóa sau khi nó đã được gán; nó chỉ có thể được gán lại.

VTP
Cấu hình VTP

- VTP mặc định trên Cisco Catalyst switch:
  - VTP domain name: None
  - VTP mode: Server mode
  - VTP pruning: Enabled or disabled (model specific)
  - VTP password: Null
  - VTP version: Version 1
- Một switch mới có thể tự động trở thành phần của domain khi nó nhận được một thông điệp từ server.
- Một VTP client có thể viết đè một database của VTP server database nếu client có revision number cao hơn.
- Một domain name không thể xóa sau khi nó đã được gán; nó chỉ có thể được gán lại.

VTP
Cấu hình VTP

```
SwitchX# configure terminal
SwitchX(config)# vtp mode [ server | client | transparent ]
SwitchX(config)# vtp domain domain-name
SwitchX(config)# vtp password password
SwitchX(config)# vtp pruning
SwitchX(config)# end
```

VTP
Cấu hình VTP

```
SwitchX(config)# vtp domain ICND
Changing VTP domain name to ICND
SwitchX(config)# vtp mode transparent
Setting device to VTP TRANSPARENT mode.
SwitchX(config)# end

SwitchX# show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 17
VTP Operating Mode              : Transparent
VTP Domain Name                 : ICND
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7D 0x6E 0x5E 0x3D 0xAF 0xA0 0x2F 0xAA
Configuration last modified by 10.1.1.4 at 3-3-93 20:08:05
SwitchX#
```

VTP
Cấu hình VTP

- VTP Configuration in global configuration mode:

```
Switch#config terminal
Switch(config)#vtp version 2
Switch(config)#vtp mode server
Switch(config)#vtp domain cisco
Switch(config)#vtp password mypassword
```

- VTP Configuration in VLAN configuration mode:

```
Switch#vlan database
Switch(vlan)#vtp v2-mode
Switch(vlan)#vtp server
Switch(vlan)#vtp domain cisco
Switch(vlan)#vtp password mypassword
```

VTP
Cấu hình 802.1Q Trungking

```
SwitchX(config-if)#
switchport mode {access |  dynamic {auto | desirable} | trunk}
```

- Cấu hình đặc điểm trunk của port

```
SwitchX(config-if)#
switchport mode trunk
```

- Cấu hình một port như là port trunk

VTP
Cấu hình VTP – Kiểm tra

```
Switch#show vtp staus
VTP Version                     :2
Configuration Revision          :2
Maximum VLANs supported locally :68
Number of existing VLANs        :6
VTP Operating Mode              :Client
VTP Domain Name                 :cisco
VTP Pruning Mode                :Disabled
VTP v2 Mode                     :Enabled
VTP Traps Generation            :Disabled
MD5 digest                      :0x35 0x84 0x7B 0x04 0x3D
                                 0x55 0x3B 0xDA
Configuration last modified by 0.0.0.0 at 10-5-00 20:33:41
Switch#
```

VTP
Cấu hình VTP – Kiểm tra

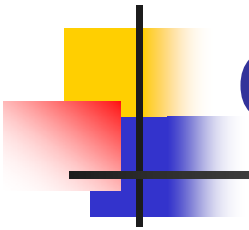
```
MDF_Switch#show vtp counters
VTP statistics:
Summary advertisments received             :4
Subset advertisments received              :1
Request advertisments received             :2
Summary advertisments transmitted          :7
Subset advertisments transmitted           :4
Request advertisments transmitted          :1
Number of config revision errors           :0
Number of config digest errors             :0
Number of V1 summary errors                :0
```

VTP
Cấu hình VTP – Kiểm tra

```
SwitchX# show interfaces interface [switchport | trunk]
```

```
SwitchX# show interfaces fa0/11 switchport
Name: Fa0/11
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
 . . .
```

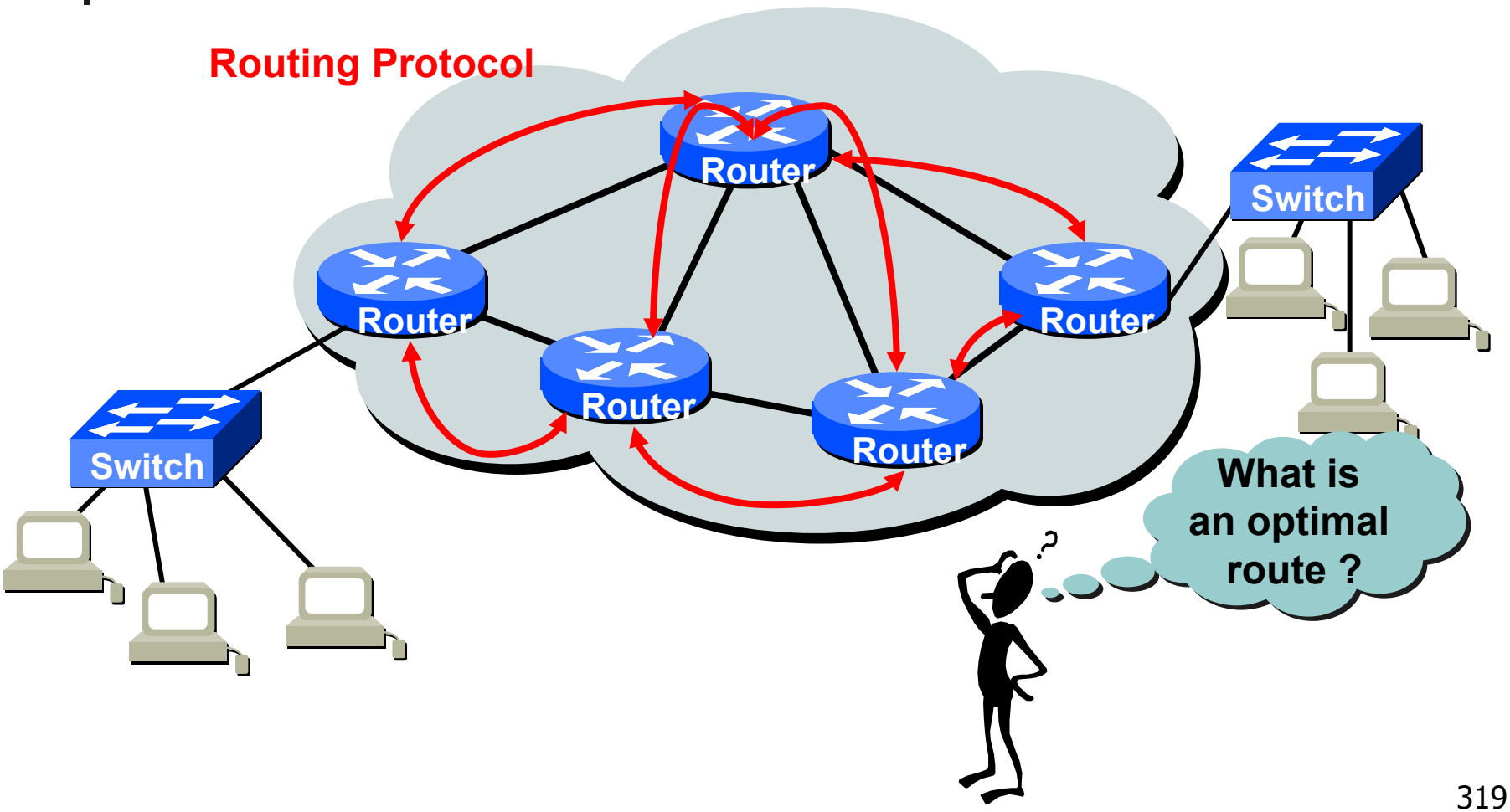
```
SwitchX# show interfaces fa0/11 trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/11      desirable    802.1q         trunking      1

Port      Vlans allowed on trunk
Fa0/11      1-4094

Port        Vlans allowed and active in management domain
Fa0/11      1-13
```



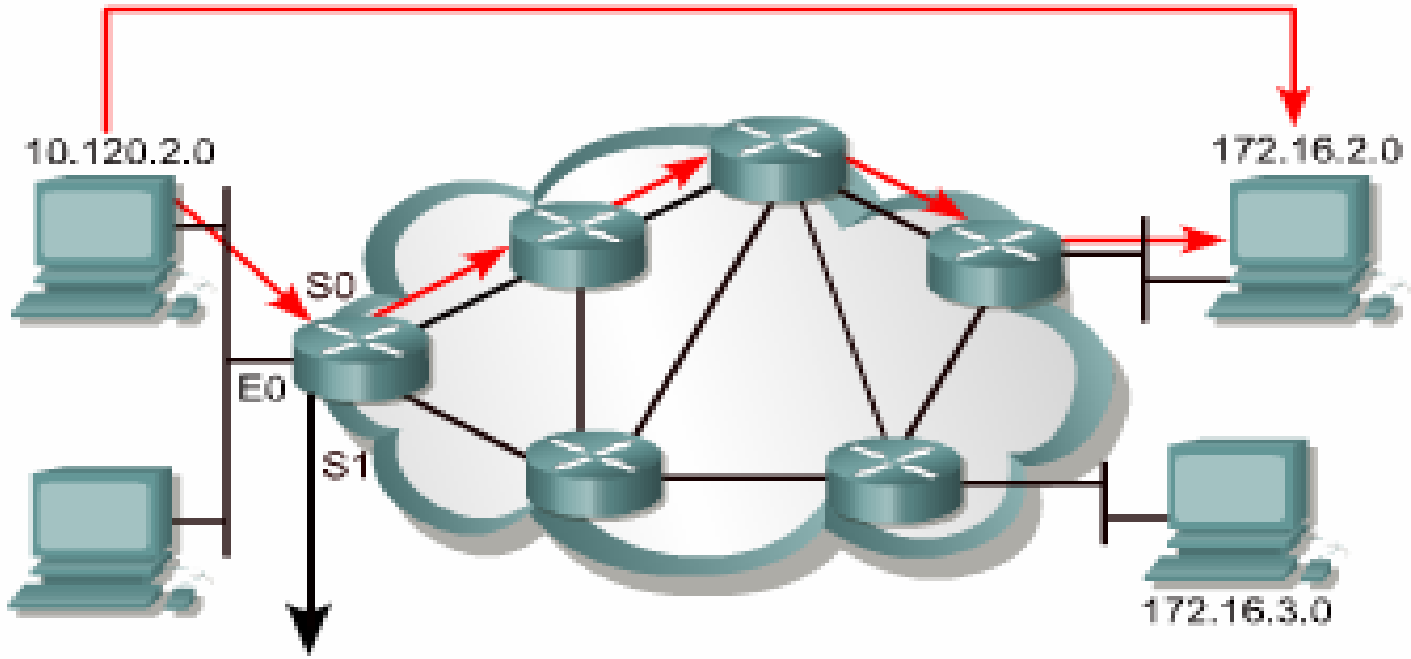
CÁC GIAO THỨC ĐỊNH TUYẾN

- Giới thiệu về định tuyến
- Định tuyến tĩnh
- Định tuyến động
  - Theo vectơ khoảng cách: RIP
  - Theo trạng thái đường liên kết: OSPF

Giới thiệu về định tuyến



Giới thiệu về định tuyến



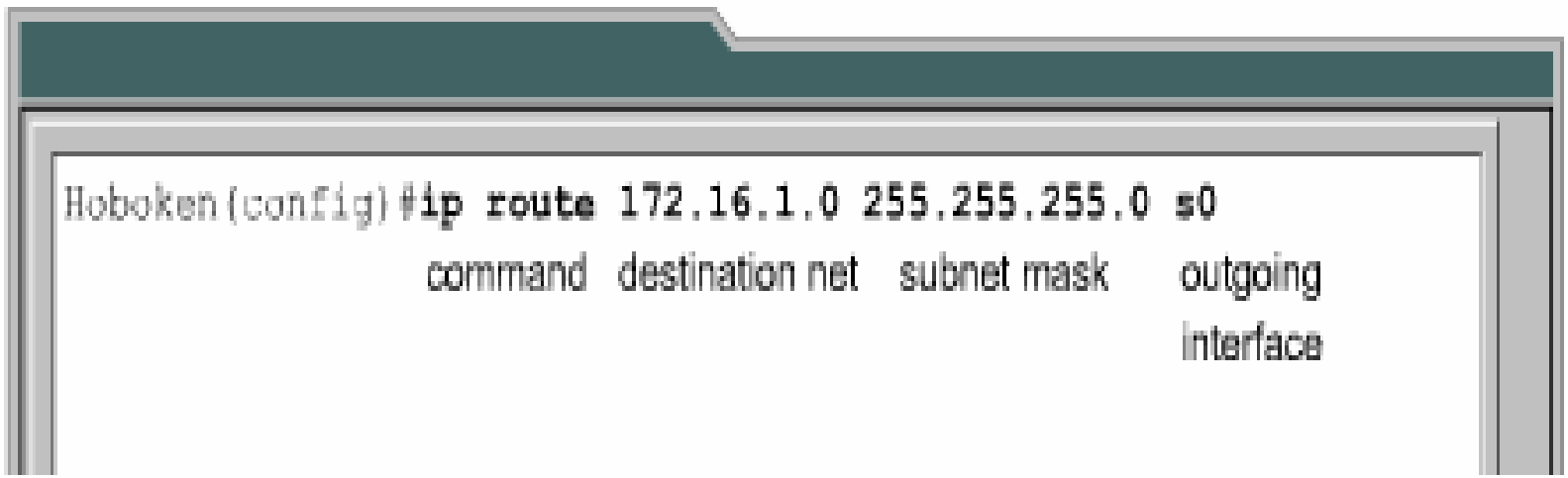
Network Protocol	Destination Network	Exit Interface
Connected	10.120.2.0	E0
RIP	172.16.2.0	S0
IGRP	172.16.3.0	S1

Routing protocols are used between routers to determine paths and maintaining routing tables

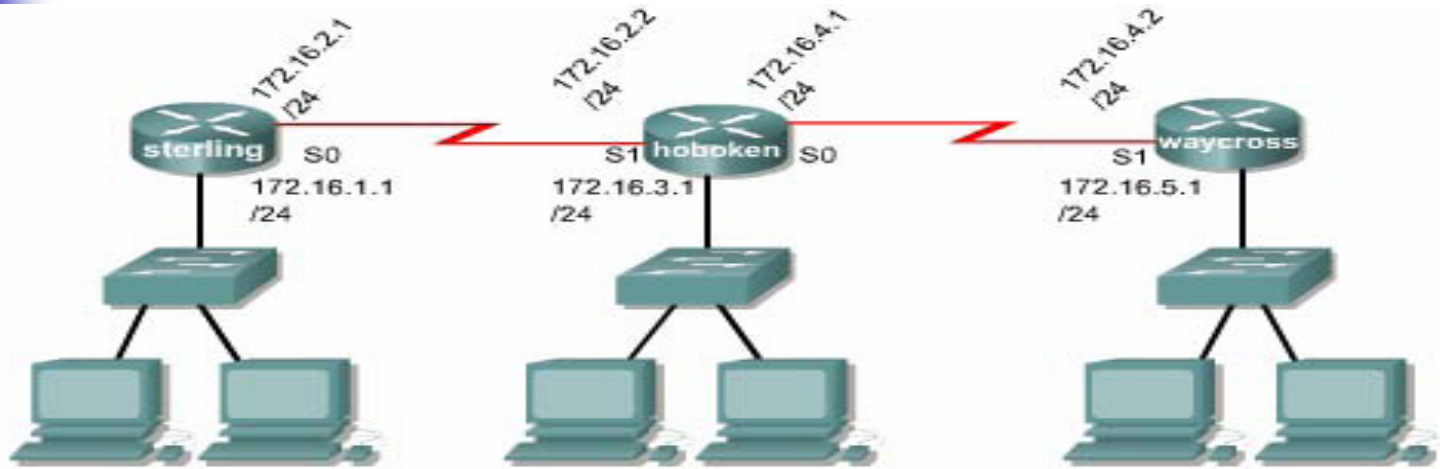
After the path is determined a router can route a routed protocol

Định tuyến tĩnh
Hoạt động của định tuyến tĩnh

- Người quản trị cấu hình các đường cố định cho router bằng lệnh *ip route*.
- Router cài đặt các đường đi này vào bảng định tuyến.
- Gói dữ liệu được định tuyến theo các đường cố định này.
- Lưu tập tin cấu hình đang hoạt động thành tập tin cấu hình khởi động bằng lệnh *copy running-config startup-config.*



Định tuyến tĩnh
Hoạt động của định tuyến tĩnh




```
Hoboken(config)#ip route 172.16.1.0 255.255.255.0 s1
                    command destination  sub mask    gateway
                            network
Hoboken(config)#ip route 172.16.5.0 255.255.255.0 s0
                    command destination  sub mask    gateway
                            network
```

0

```
Hoboken(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.1
                    command destination  sub mask    gateway
                            network
Hoboken(config)#ip route 172.16.5.0 255.255.255.0 172.16.4.2
                    command destination  sub mask    gateway
                            network
```

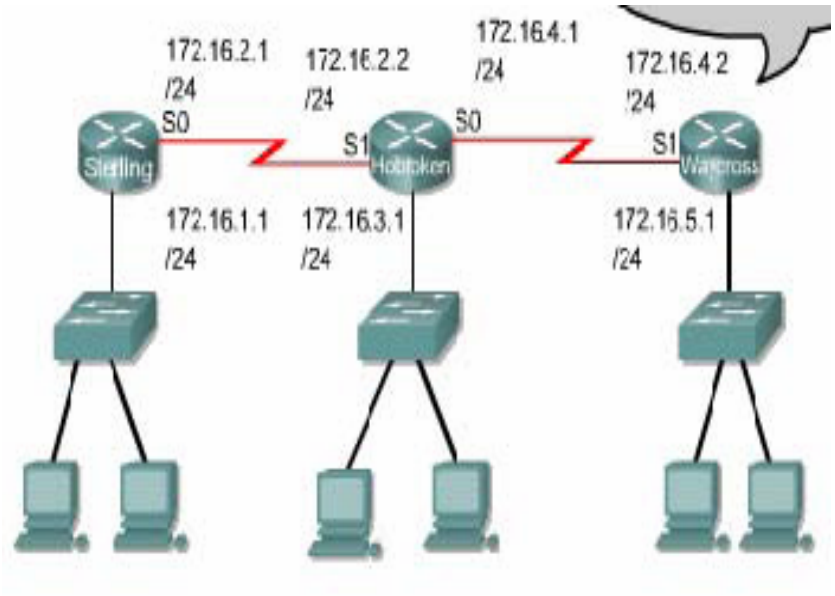
1

Chỉ số tin cậy

Định tuyến tĩnh

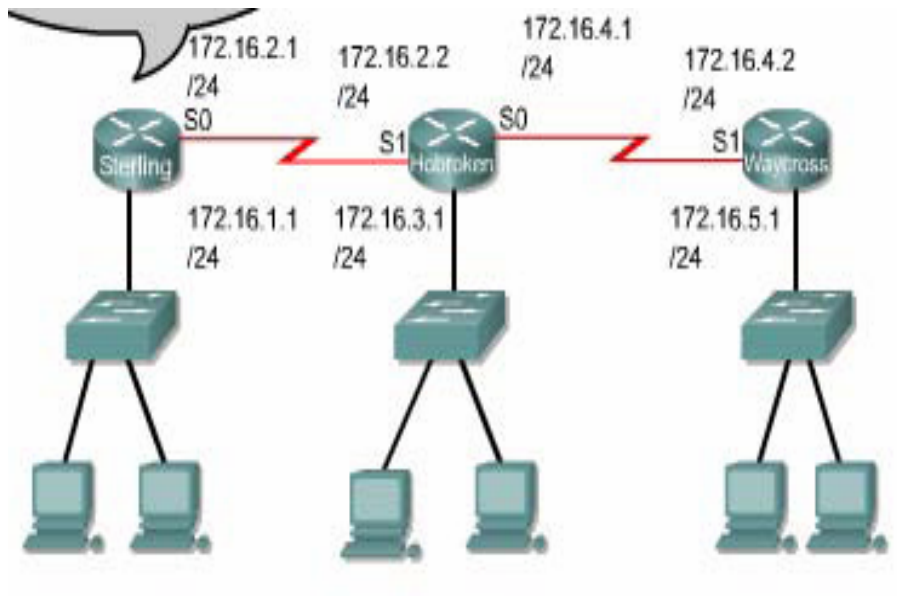
Cấu hình đường mặc định cho router chuyển gói đi

ip route 0.0.0.0 0.0.0.0 [*next-hop-address* | *outgoing interface*]



Waycross(config)#**ip route 0.0.0.0 0.0.0.0 S1**

This command points to all non-directly-connected networks



Sterling(config)#**ip route 0.0.0.0 0.0.0.0 S0**

This command points to all non-directly-connected networks

Định tuyến tĩnh

Kiểm tra cấu hình đường cố định với lệnh *show ip route*

```
Hoboken#show ip route
Codes:C-connected,S-static,I-IGRP,R-RIP,M-mobile,B-BGP
D-EIGRP,EX-EIGRP external,O- OSPF,IA-OSPF inter area
N1-OSPF NSSA external type 1,N2-OSPF NSSA external type2
E1-OSPF external type 1,E2-OSPF external type 2, E - EGP
i-IS-IS,L1-IS-IS level-1,L2-IS-IS level-2,ia-IS-IS inter
area
* -candidate default, U - per-user static route, o - ODR
P -periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 5 subnets
C       172.16.4.0 is directly connected, Serial0
S       172.16.5.0 is directly connected, Serial0
S       172.16.1.0 is directly connected, Serial1
C       172.16.2.0 is directly connected, Serial1
```

Định tuyến tĩnh
Xử lý sự cố với lệnh *ping* và *traceroute*

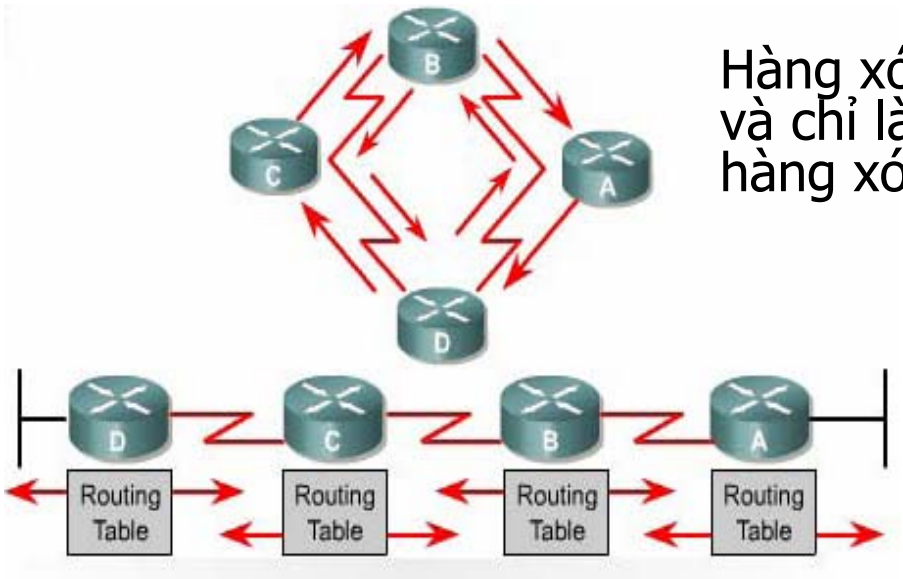
```
Sterling#ping 172.16.5.1
Type escape sequence to abort.
Sending 5,100-byte ICMP Echos to 172.16.5.1,timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)


Sterling#traceroute 172.16.5.1
Type escape sequence to abort.
Tracing the route to 172.16.5.1
  1 172.16.2.2 16 msec 16 msec 16 msec
  2 172.16.4.2 32 msec 28 msec *
  3  *  *  *
  4  *  *  *
  5  *  *  *
  6  *  *  *
```

Định tuyến tĩnh
Xử lý sự cố với lệnh *ping* và *traceroute*

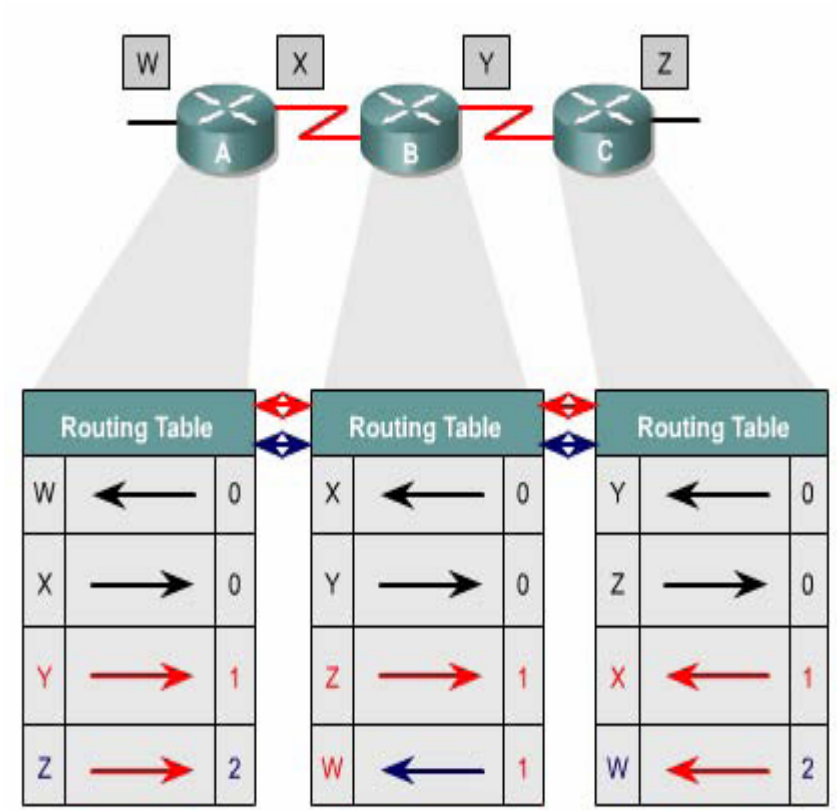
- Ping và Traceroute được sử dụng để kiểm tra kết nối.
- Nhưng trước khi sử dụng lệnh ping và traceroute, nên kiểm tra trạng thái của kết nối có đang "up" hay "down" bằng lệnh:
  - show interface
  - show interface s0
  - show ip interface brief

Định tuyến theo vectơ khoảng cách

Đặc điểm chung



Hàng xóm và chỉ là hàng xóm



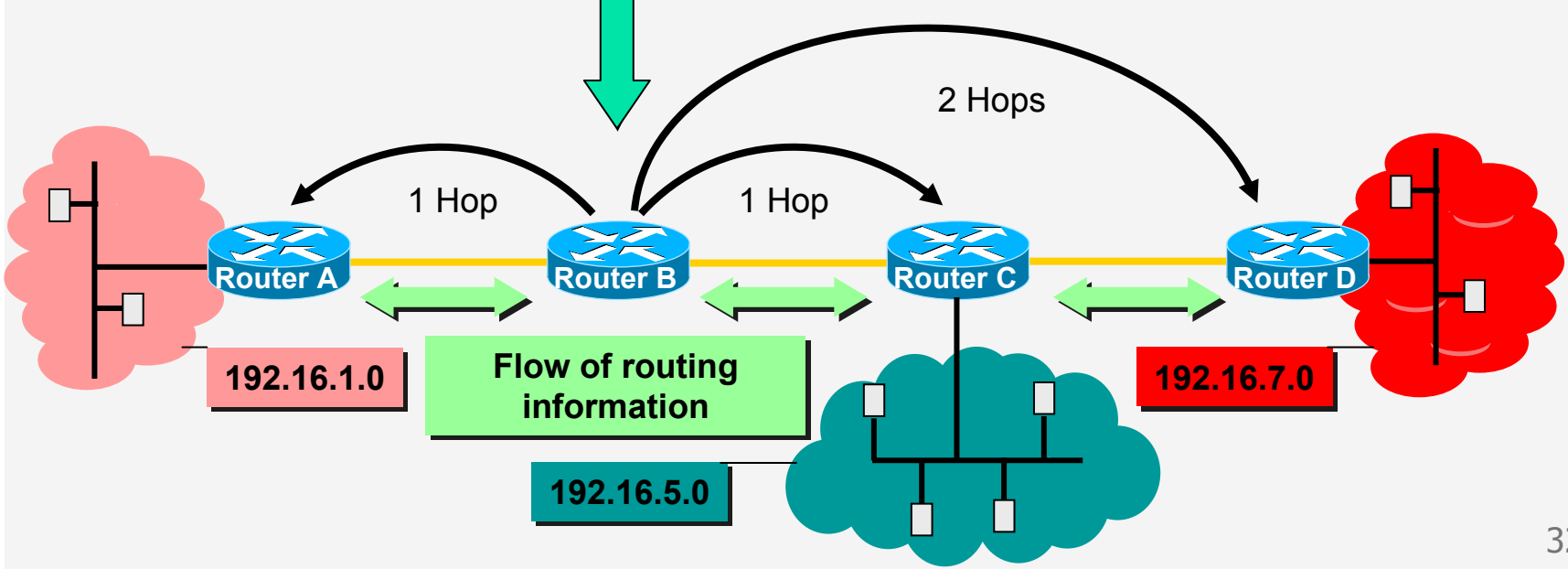
- Truyền bản sao của bảng định tuyến từ router này sang router khác theo định kỳ.
- Sử dụng thuật toán Bellman-Ford.

Định tuyến theo vectơ khoảng cách

Đặc điểm chung

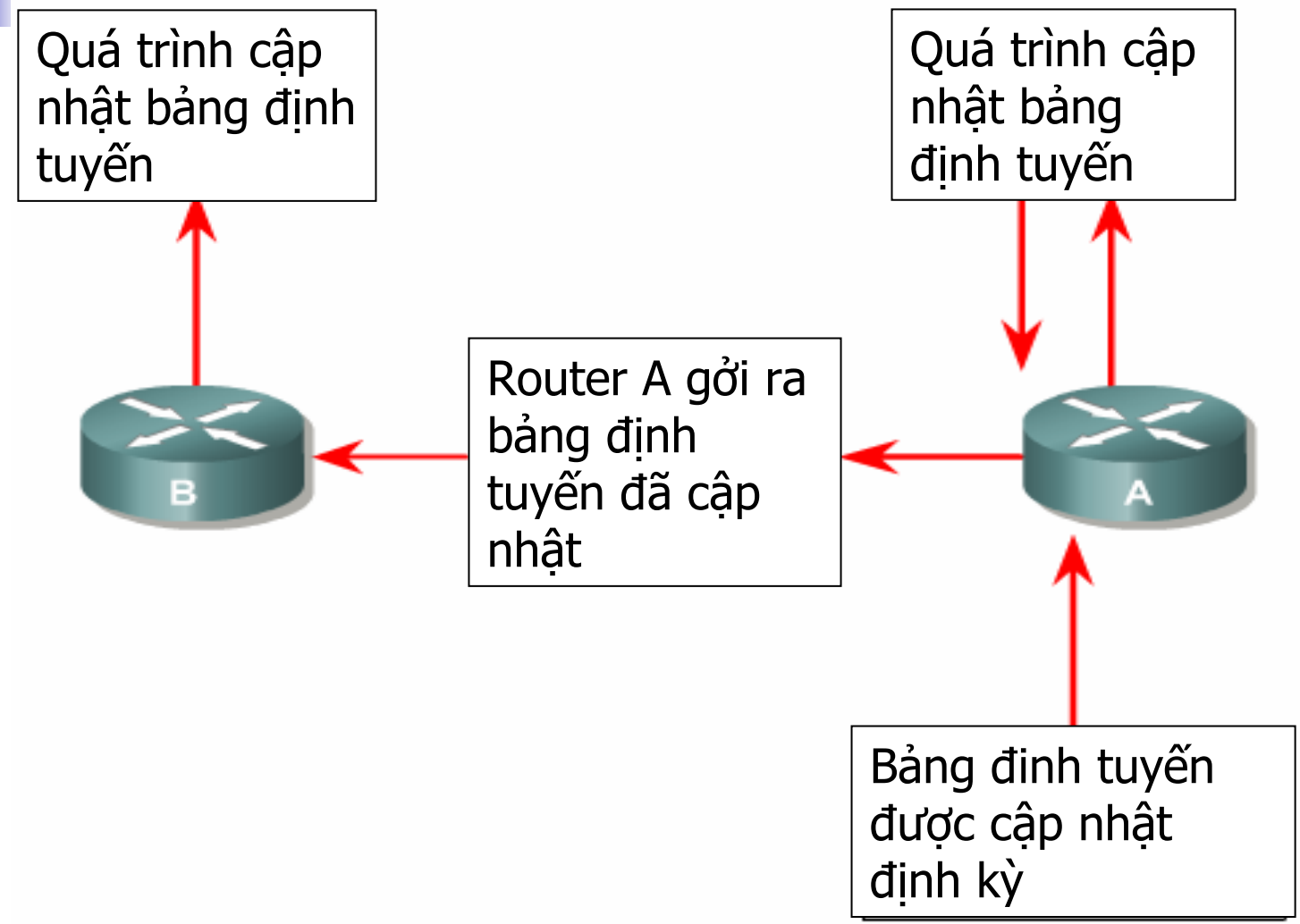
Destination	Distance
192.16.1.0	1
192.16.5.0	1
192.16.7.0	2

Routing table contains the addresses of destinations and the distance of the way to this destination.



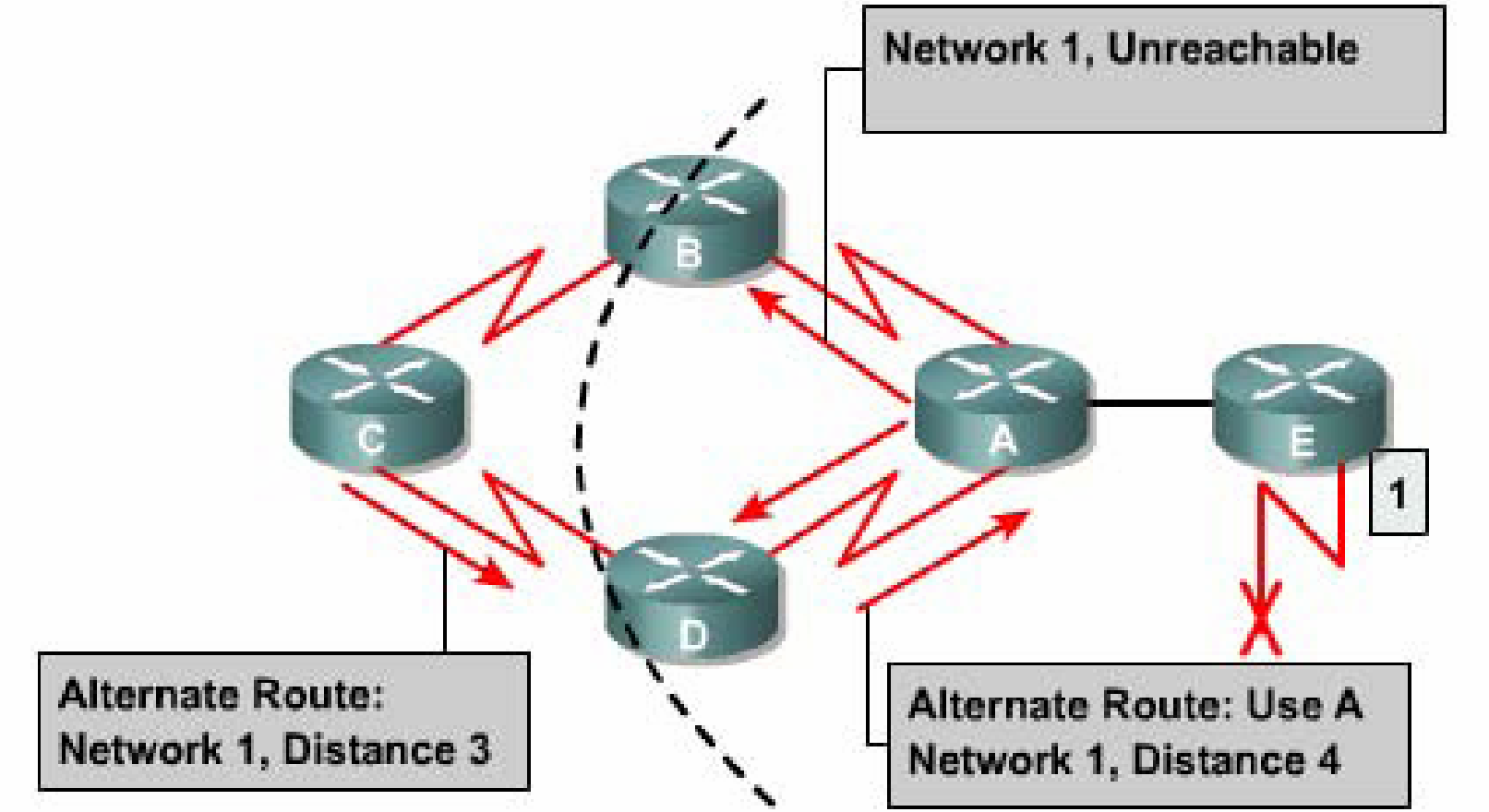
Định tuyến theo vectơ khoảng cách

Cập nhật thông tin định tuyến



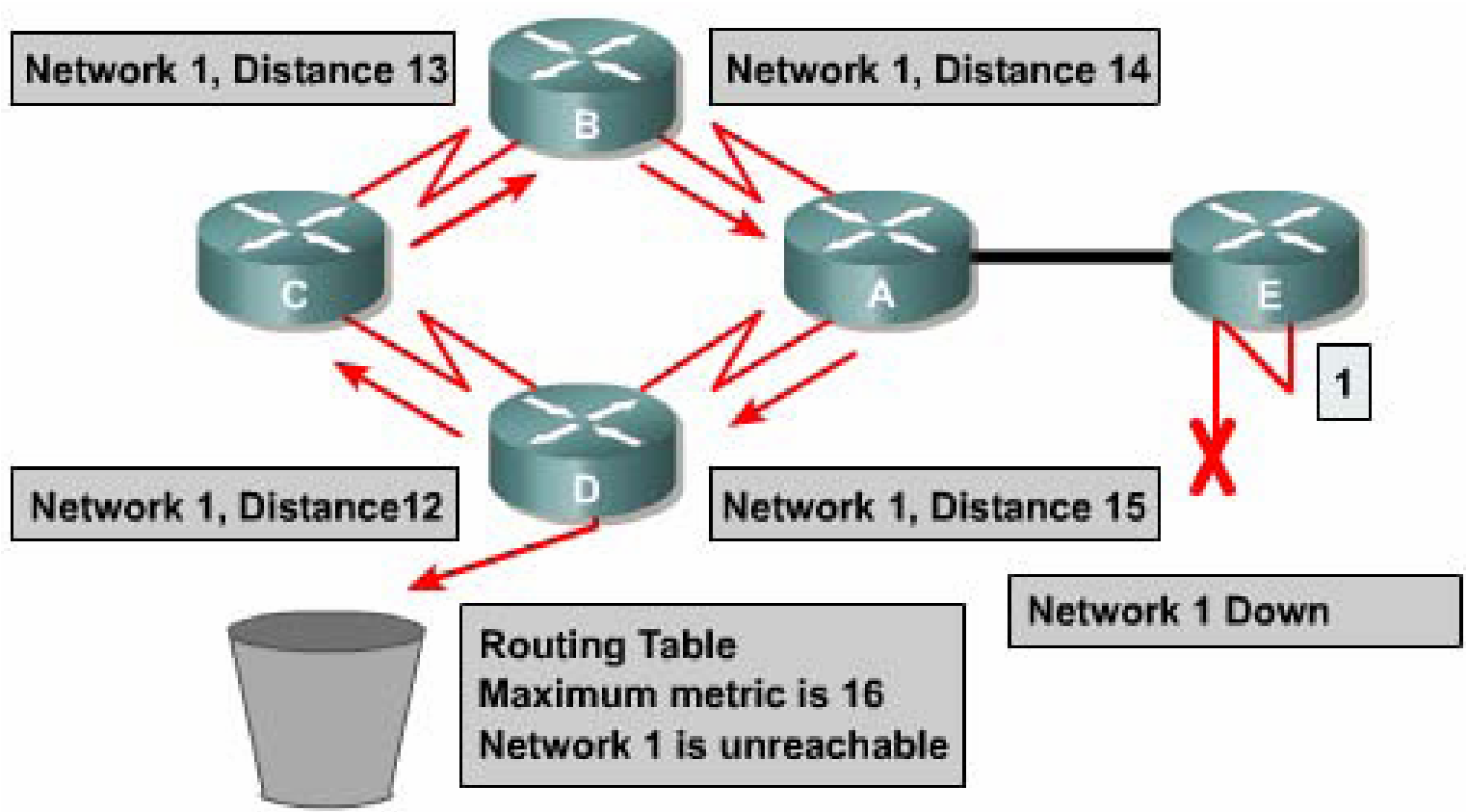
Định tuyến theo vectơ khoảng cách

Lỗi định tuyến lặp



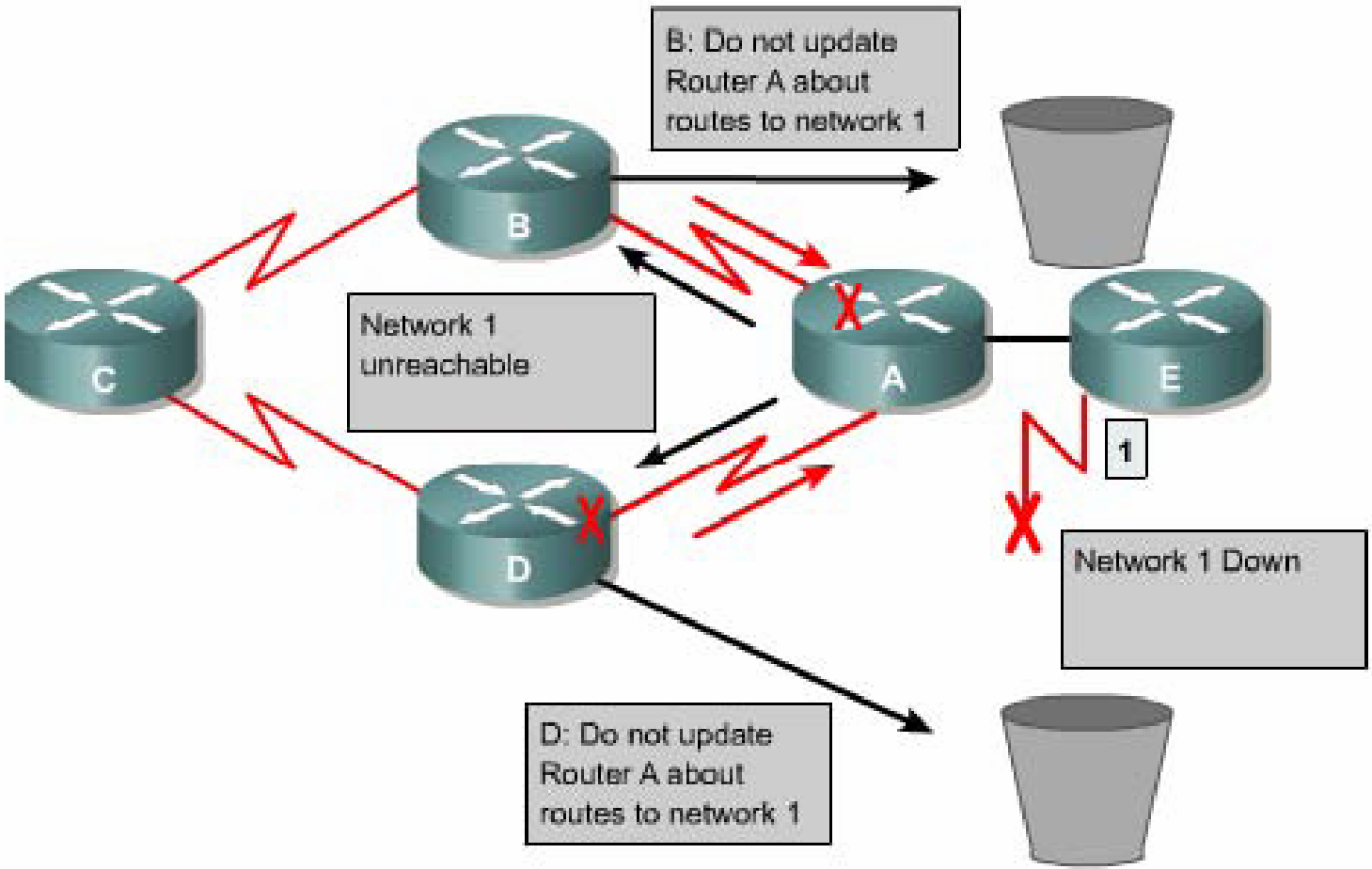
Định tuyến theo vectơ khoảng cách

Định nghĩa giá trị tối đa



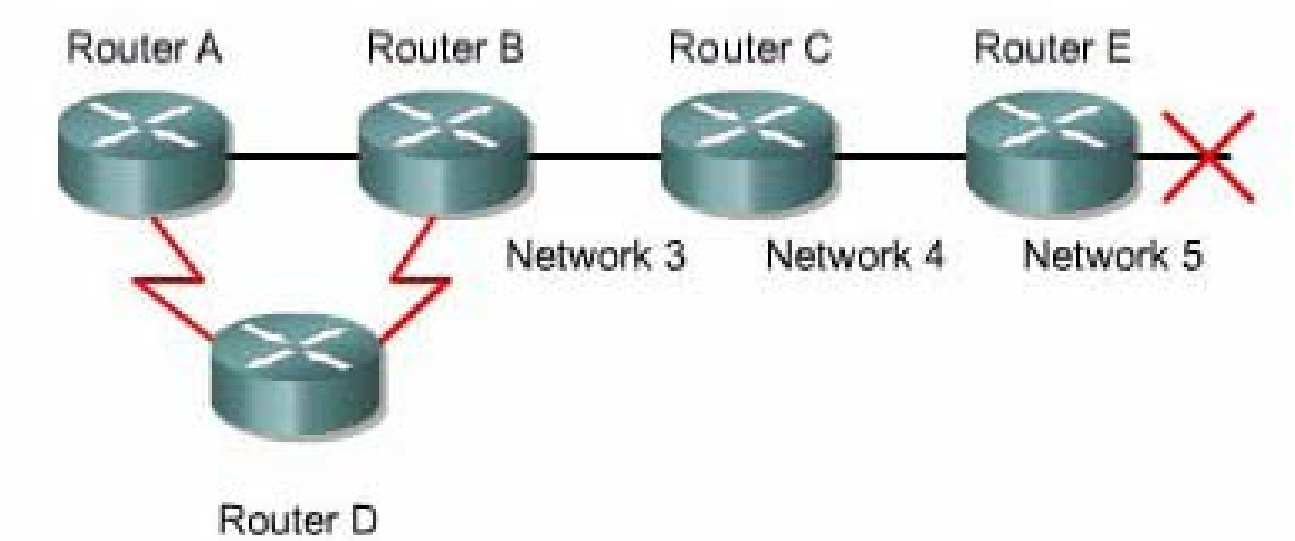
Định tuyến theo vectơ khoảng cách

Tránh định tuyến lặp vòng bằng split horizone



Định tuyến theo vectơ khoảng cách

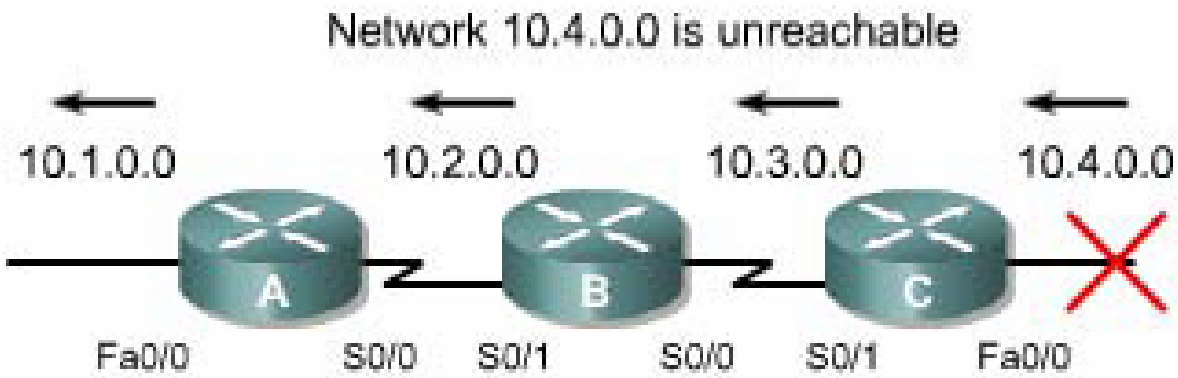
Tránh định tuyến lặp vòng bằng Route poisoning



When Network 5 goes down, Router E initiates route poisoning by entering a table entry metric of 16 (unreachable).

Định tuyến theo vectơ khoảng cách

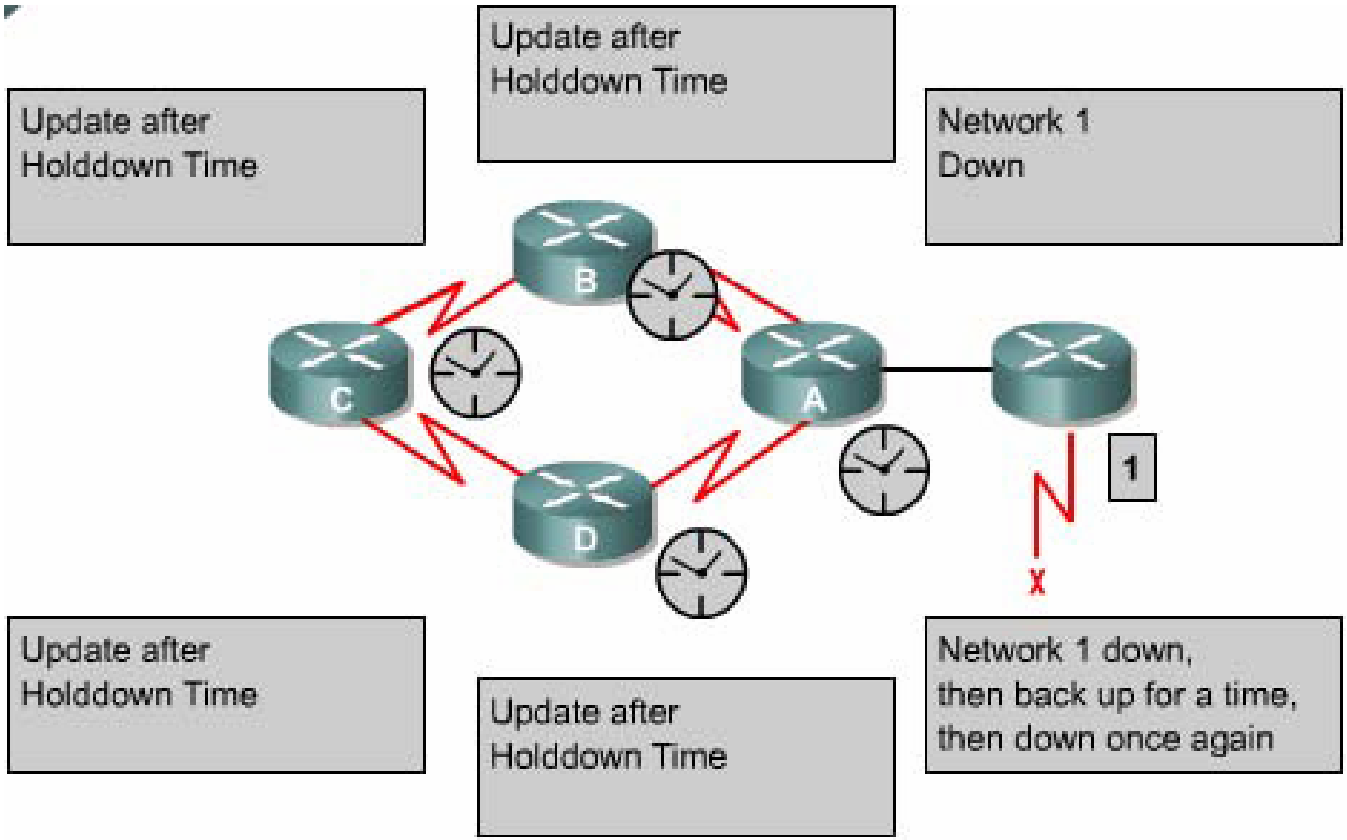
Tránh định tuyến lặp vòng bằng cơ chế cập nhật tức thời



With the triggered update approach, routers send messages as soon as they notice a change in their routing table.

Định tuyến theo vectơ khoảng cách

Tránh định tuyến lặp vòng bằng thời gian holddown



Định tuyến theo vectơ khoảng cách

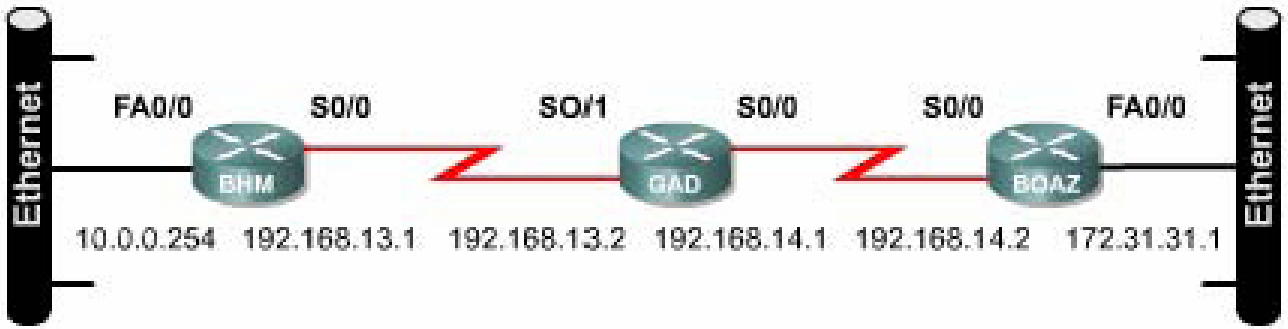
Đặc điểm chung

- Copy bảng định tuyến cho router láng giềng.
- Cập nhật định kỳ.
- RIPv1 và RIPv2 sử dụng số lượng hop làm thông số định tuyến.
- Mỗi router nhìn hệ thống mạng theo sự chi phối của các router láng giềng.
- Hội tụ chậm.
- Dễ bị lặp vòng.
- Dễ cấu hình và dễ quản trị.
- Tốn nhiều băng thông.

RIP (Routing Information Protocol)
Tiến trình của RIP

- Được mô tả trong RFC 1058 và Tiêu chuẩn Internet STD 56.
- Có 2 phiên bản là RIPv1 và RIPv2.
- RIPv2 có cơ chế xác minh giữa các router khi cập nhật để bảo mật cho bảng định tuyến và có hỗ trợ thêm VLSM (Variable Length Subnet Masking).
- Thông số định tuyến là số lượng hop. Số lượng hop tối đa cho mỗi đường là 15. Chu kỳ cập nhật mặc định là 30 giây.
- Có split horizon và thời gian holddown để tránh cập nhật thông tin định tuyến không chính xác.

RIP
Cấu hình RIP

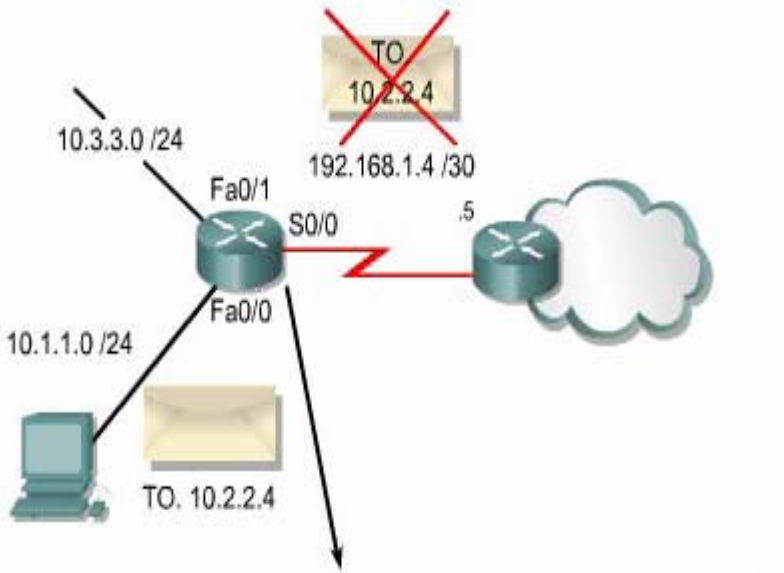



```
BHM(config)#router rip
BHM(config-router)#network 10.0.0.0
BHM(config-router)#network 192.168.13.0
```

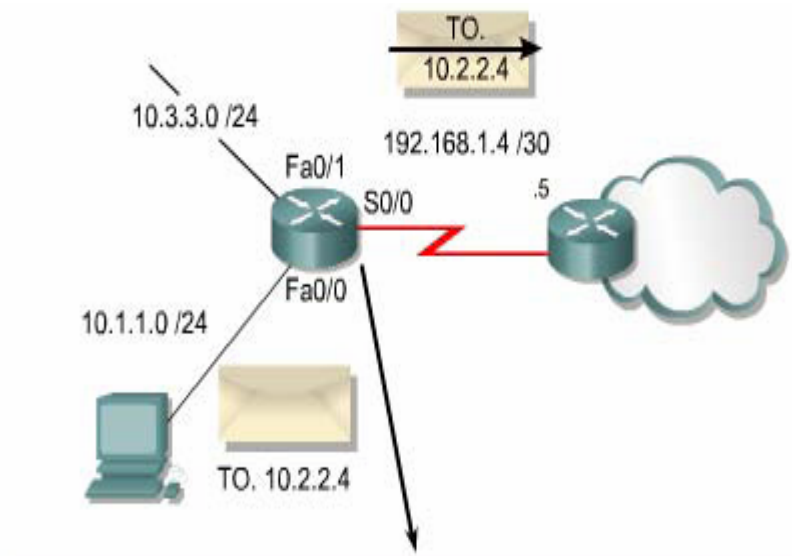
```
GAD(config)#router rip
GAD(config-router)#network 192.168.14.0
GAD(config-router)#network 192.168.13.0
```

```
BOAZ(config)#router rip
BOAZ(config-router)#network 192.168.14.0
BOAZ(config-router)#network 172.31.0.0
```

RIP
Sử dụng lệnh *ip classless*



Destination Network	Outbound Interface
10.1.1.0	Fa 0/0
10.3.3.0	Fa 0/1
0.0.0.0	S 0/0



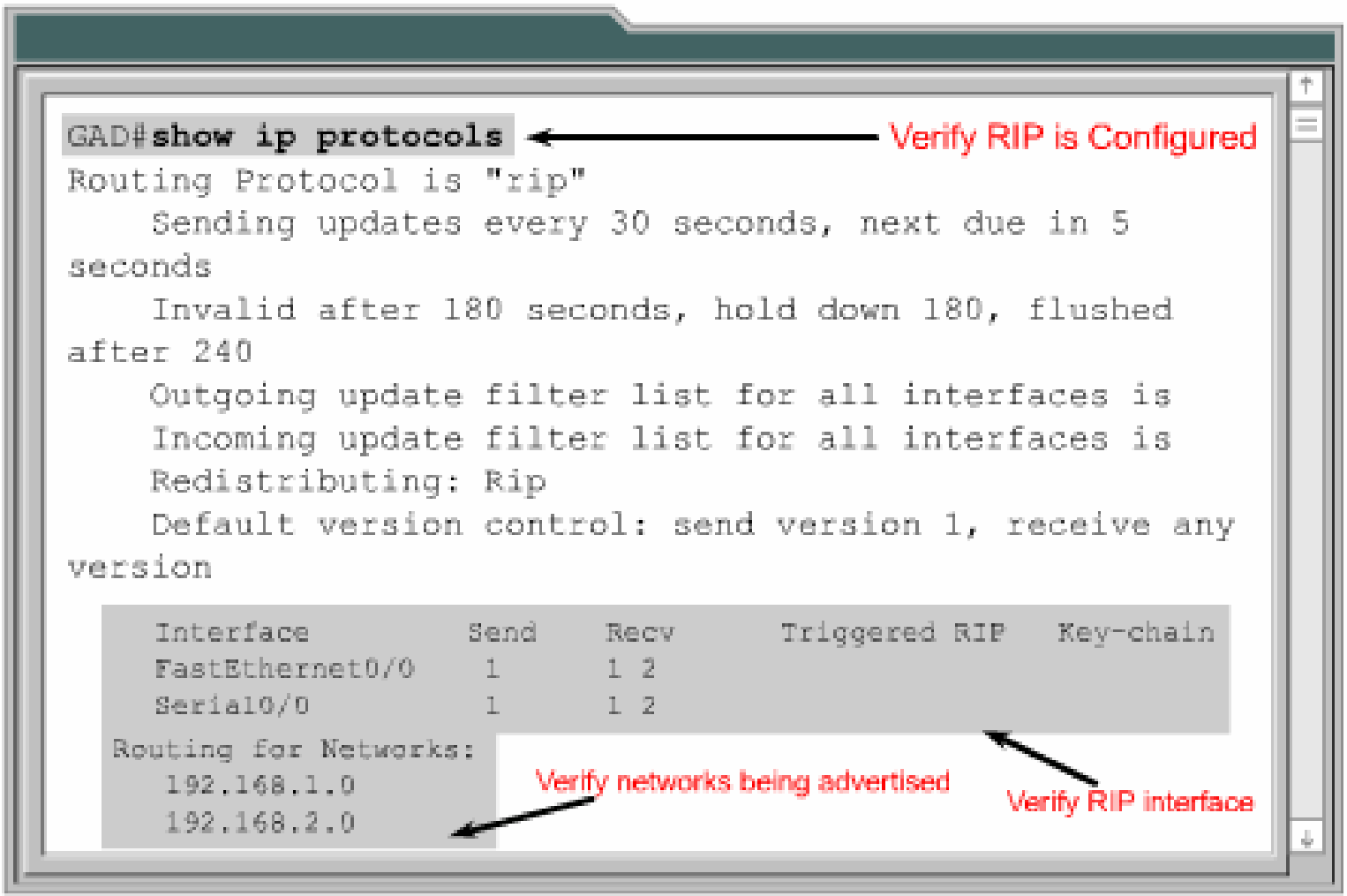
Destination Network	Outbound Interface
10.1.1.0	Fa 0/0
10.3.3.0	Fa 0/1
0.0.0.0	S 0/0

RIP

Một số lệnh tăng tốc độ hội tụ khi cấu hình RIP

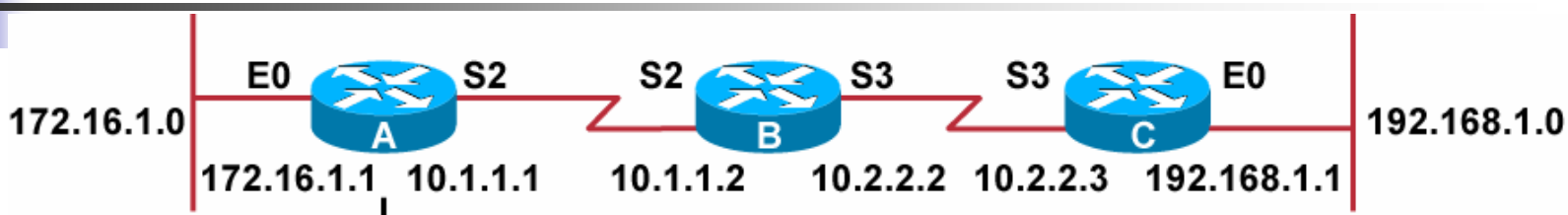
- Tắt cơ chế split horizon:
  - GAD(config-if)#**no ip split-horizon**
- Thay đổi thời gian holddown (ngầm định 180 giây):
  - Router(config-router)#**timer basic** *update invalid holddown flush [sleeptime]*
- Thay đổi chu kỳ cập nhật:
  - GAD(config-router)#**update-timer** *seconds*
- Không cho phép gởi thông tin cập nhật định tuyến ra một cổng nào đó:
  - GAD(config-router)#**passive-interface** Fa0/0

RIP
Kiểm tra cấu hình RIP



RIP

Kiểm tra cấu hình RIP




```
RouterA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate
default
       U - per-user static route, o - ODR
       T - traffic engineered route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, Ethernet0
     10.0.0.0/24 is subnetted, 2 subnets
R       10.2.2.0 [120/1] via 10.1.1.2, 00:00:07, Serial2
C       10.1.1.0 is directly connected, Serial2
R    192.168.1.0/24 [120/2] via 10.1.1.2, 00:00:07, Serial2
```

ICND20GR_231

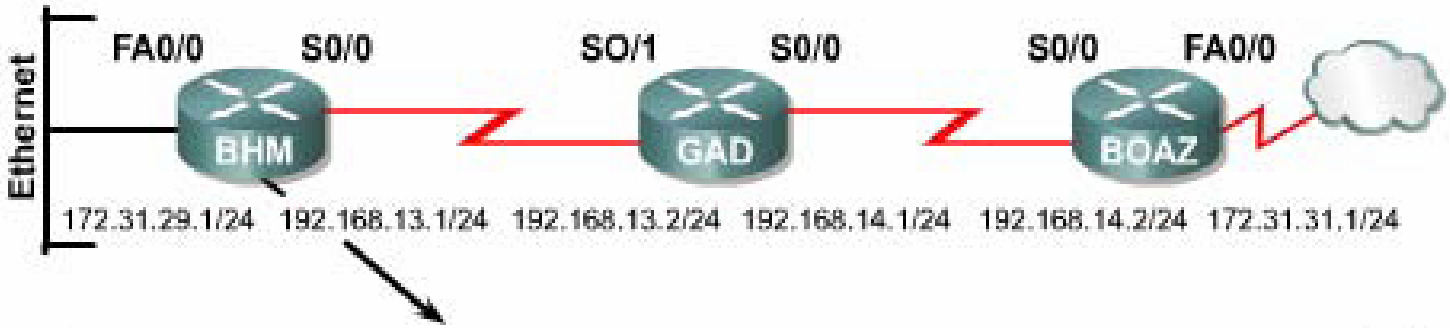
RIP

Xử lý sự cố về hoạt động cập nhật của RIP


```
BHM#debug ip rip
RIP event debugging is on
BHM#
00:45:33: RIP: received v1 update from 192.168.13.2
on Serial0/0
00:45:33:      192.168.14.0 in 1 hop
00:45:33:      172.31.0.0 in 2 hop
00:45:33:      172.29.0.0 15 hops
00:45:36: RIP: sending v1 update to 255.255.255.255
via Serial0/0 (192.168.13.1)
```

RIP

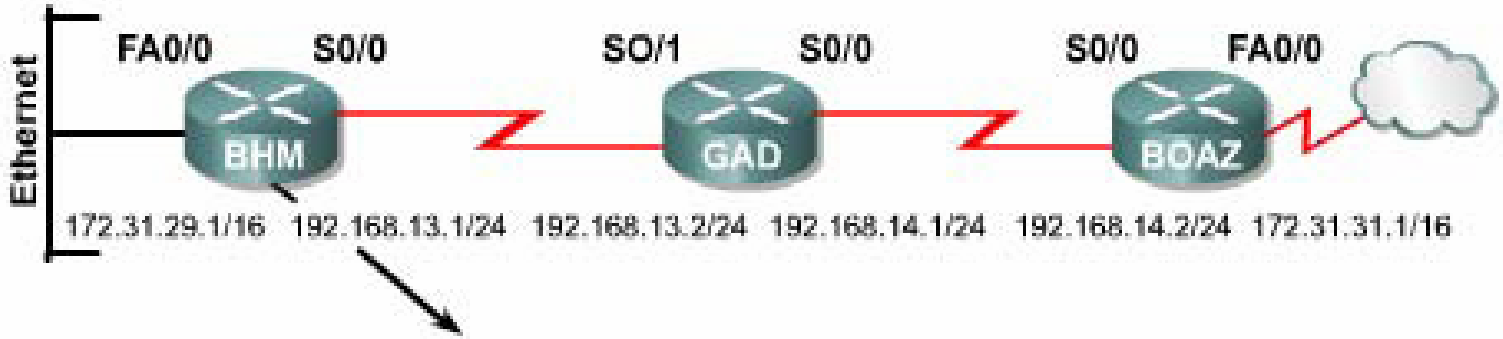
Xử lý sự cố về hoạt động cập nhật của RIP




```
BHM#debug ip rip
RIP event debugging is on
BHM#
7w2d: RIP:  received v1 update from 192.168.13.2 on
Serial 0/0
7w2d:          192.168.14.0 in 1 hop
7w2d:          172.31.0.0 in 2 hops
7w2d: RIP: sending v1 update to 255.255.255.255 via
Serial 0/0 (192.168.13.1)
7w2d:          network 172.31.0.0, metric 1
```

Subnet không liên tục

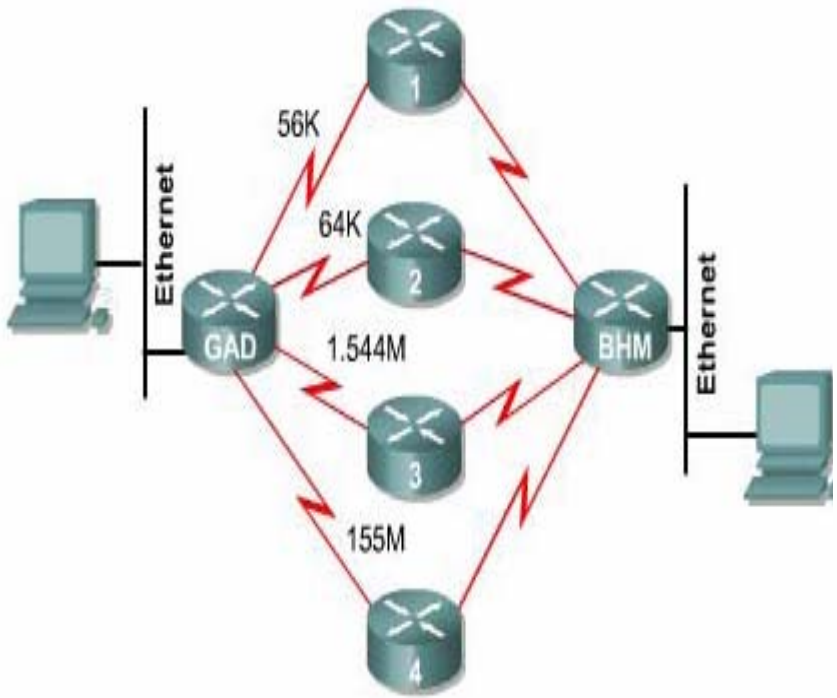
RIP
Xử lý sự cố về hoạt động cập nhật của RIP




```
BHM#debug ip rip
RIP event debugging is on
BHM#
7w2d: RIP:  received v1 update from 192.168.13.2 on
Serial 0/0
7w2d:          192.168.14.0 in 1 hop
7w2d:          172.31.0.0 in 2 hops
7w2d: RIP: sending v1 update to 255.255.255.255 via
Serial 0/0 (192.168.13.1)
7w2d:          network 172.31.0.0, metric 1
```

Trùng Subnet

RIP
Chia tải với RIP

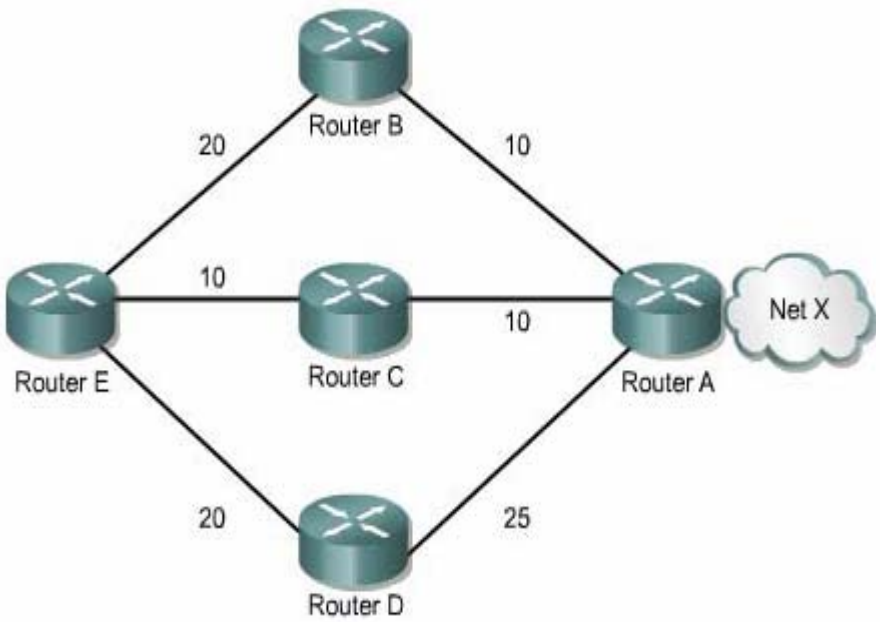



```
RouterC#show ip route 192.168.2.0
Routing entry for 192.168.2.0/24
 Known via "rip", distance 120, metric 1
 Redistributing via rip
 Last update from 192.168.4.2 on FastEthernet0/0,
00:00:18 ago
 Routing Descriptor Blocks:
 192.168.4.1, from 192.168.4.1, 00:02:45 ago, via
FastEthernet0/0
 Route metric is 1, traffic share count is 1
 * 192.168.4.2, from 192.168.4.2, 00:00:18 ago,
via FastEthernet0/0
 Route metric is 1, traffic share count is 1
```

- Ngầm định 4 đường, tối đa 6 đường.
- Chỉ quan tâm đến số hop.

Đường kế tiếp

RIP
Chia tải cho nhiều đường



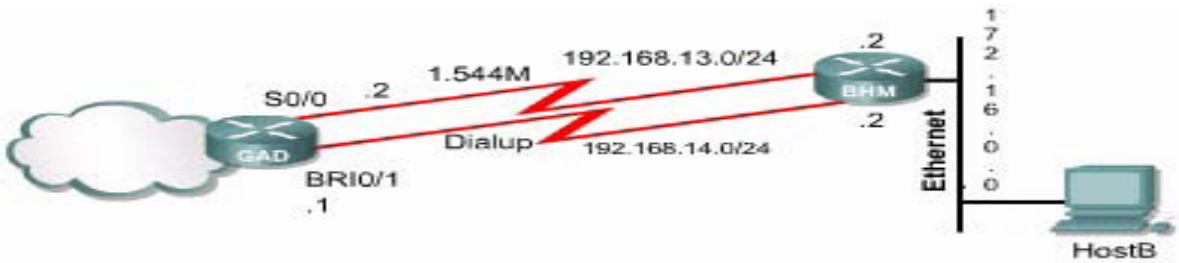
Administrative Distance Route Source	Default Distance
Connected interface	0
Static route	1
Enhanced IGRP summary route	5
External BGP	20
Internal Enhanced IGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP external route	170
Internal BGP	200
Unknown	255

- Chia tải theo gói dữ liệu
- Chia tải theo địa chỉ đích

Administrative distance: chỉ số tin cậy

RIP

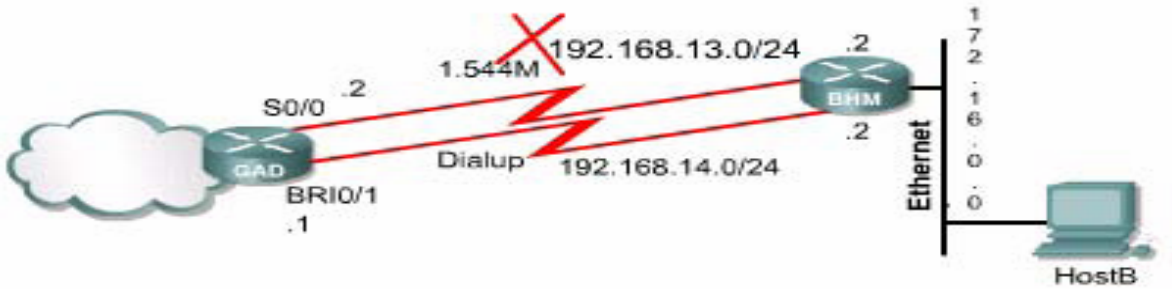
Tích hợp đường cố định với RIP




```
GAD#configure terminal
GAD(config)#ip route 172.16.0.0 255.255.0.0
192.168.14.2 130
GAD#show ip route
Codes: C - connected, s - static, I - IGRP, R - RIP,
M - mobile, B - BGP
               D - EIGRP, EX - EIGRP external, O -
OSPF, IA - OSPF inter area
              N1 - OSPF NSSA external type 1, N2 -
OSPF NSSA external type 2
              E 1 - OSPF external type 1, E2 - OSPF
external type 2, E - EGP
               i - IS-IS, L1 - IS-IS level - 1, L2 -
IS-IS level -2, ia - IS-IS inter area
               * - candidate default, U - per -user
static route, o - ODR
               p - periodic downloaded static route
    Gateway of last resort is not set

     C       192.168.13.0/24 is directly connected,
Serial 0/0
     C       192.169.14.0/24 is directly connected,
BRI0/1
     R       172.16.0.0/16 [120/1] via 192.16.13.2,
00:00:24, Serial0/0
```

RIP

Tích hợp đường cố định với RIP

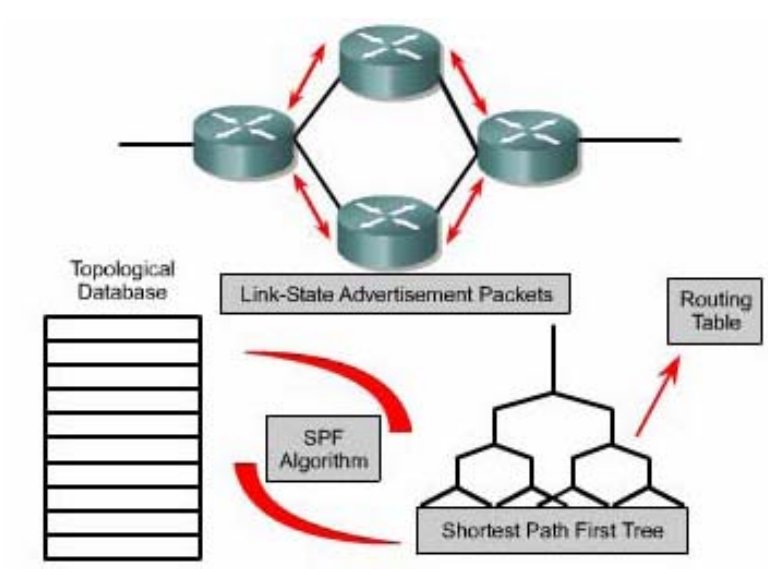


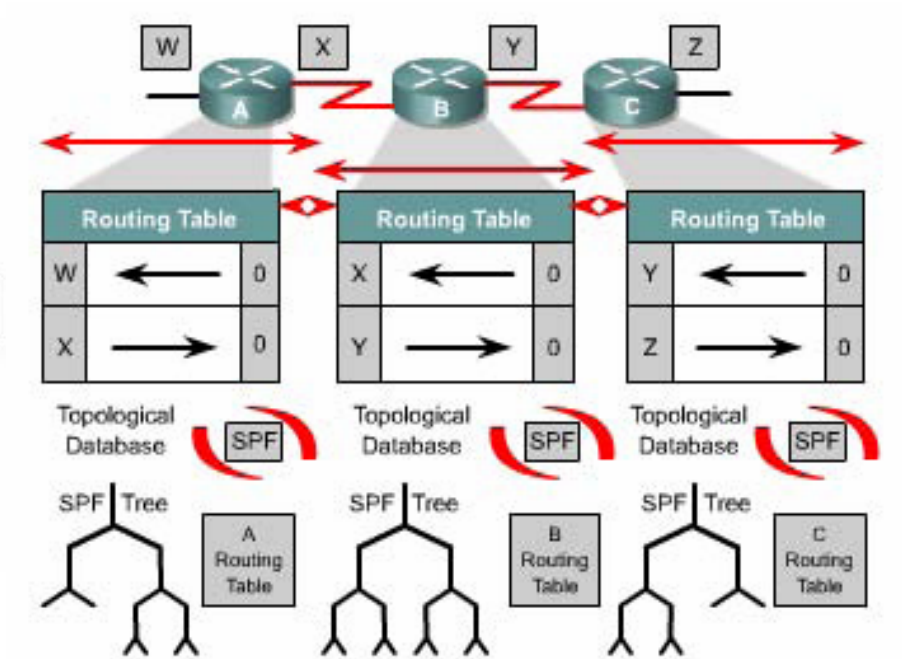

```
GAD#show ip route
Codes: C - connected, s - static, I - IGRP, R - RIP,
M - mobile, B - BGP
               D - EIGRP, EX - EIGRP external, O -
OSPF, IA - OSPF inter area
               N1 - OSPF NSSA external type 1, N2 -
OSPF NSSA external type 2
               E1 - OSPF external type 1, E2 - OSPF
external type 2, E - EGP
               i - IS-IS, L1 - IS-IS level - 1, L2 -
IS-IS level -2, ia - IS-IS inter area
               * - candidate default, U - per -user
static route, o - ODR
               p - periodic downloaded static route

Gateway of last resort is not set

     C       192.168.113.0/24 is directly connected,
Serial 0/0
     C       192.169.14.0/24 is directly connected,
BRI0/1
     R       172.16.0.0/16 [120/1] via 192.16.14.2
```

Định tuyến theo trạng thái đường liên kết
Đặc điểm chung

- Sử dụng đường ngắn nhất.
- Chỉ cập nhật khi có sự kiện xảy ra.
- Gởi gói thông tin về trạng thái các đường liên kết cho tất cả các router trong mạng.
- Mỗi router có cái nhìn đầy đủ về cấu trúc hệ thống mạng.
- Hội tụ nhanh.
- Không bị lặp vòng.
- Cấu hình phức tạp hơn.
- Đòi hỏi nhiều bộ nhớ.
- Tốn ít băng thông.

Định tuyến theo trạng thái đường liên kết
Đặc điểm chung



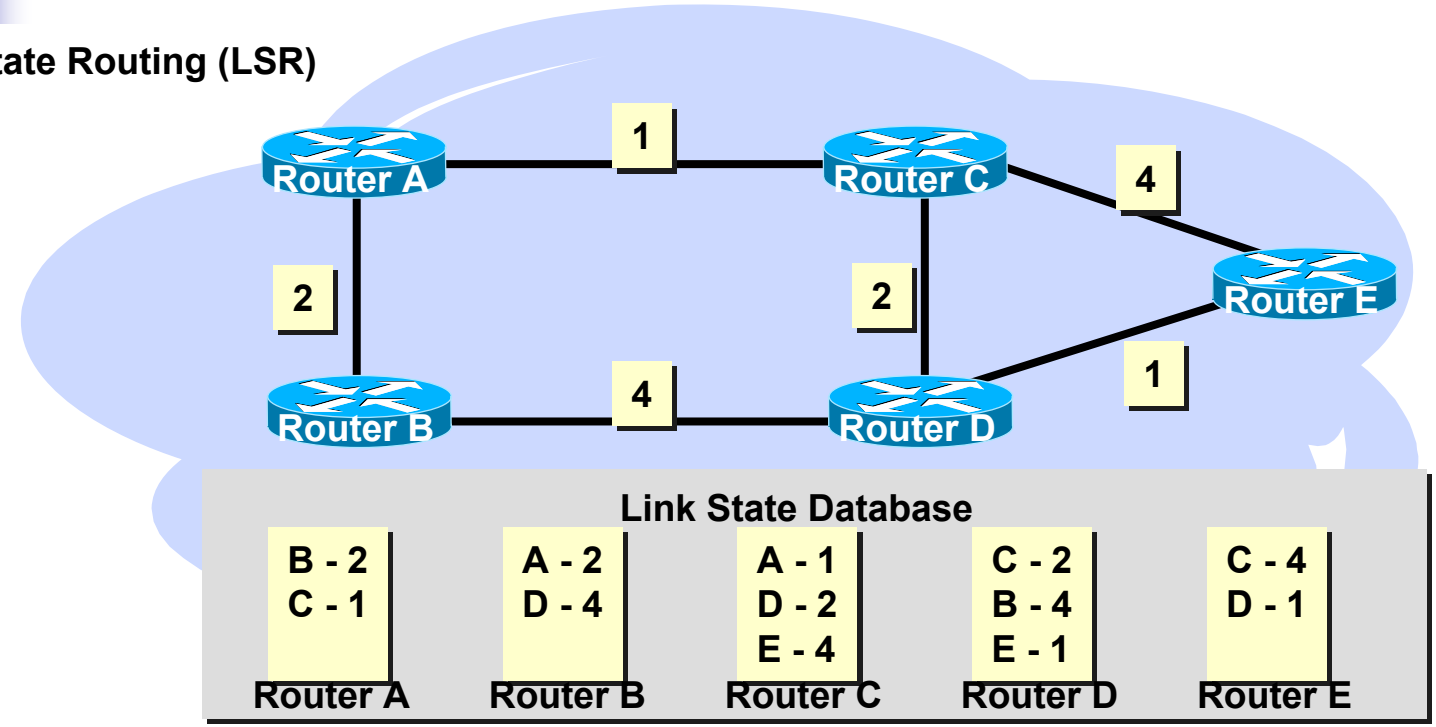


- Các router trao đổi thông tin định tuyến để xây dựng một bản đồ đầy đủ về cấu trúc hệ thống mạng. Router tự tính toán và chọn đường đi tốt nhất đến mạng đích để đưa lên bảng định tuyến.
- Khi các router đã được hội tụ thì mỗi thay đổi cấu trúc mạng sẽ được cập nhật bằng một gói thông tin nhỏ chứ không phải nguyên bảng định tuyến.

Định tuyến theo trạng thái đường liên kết

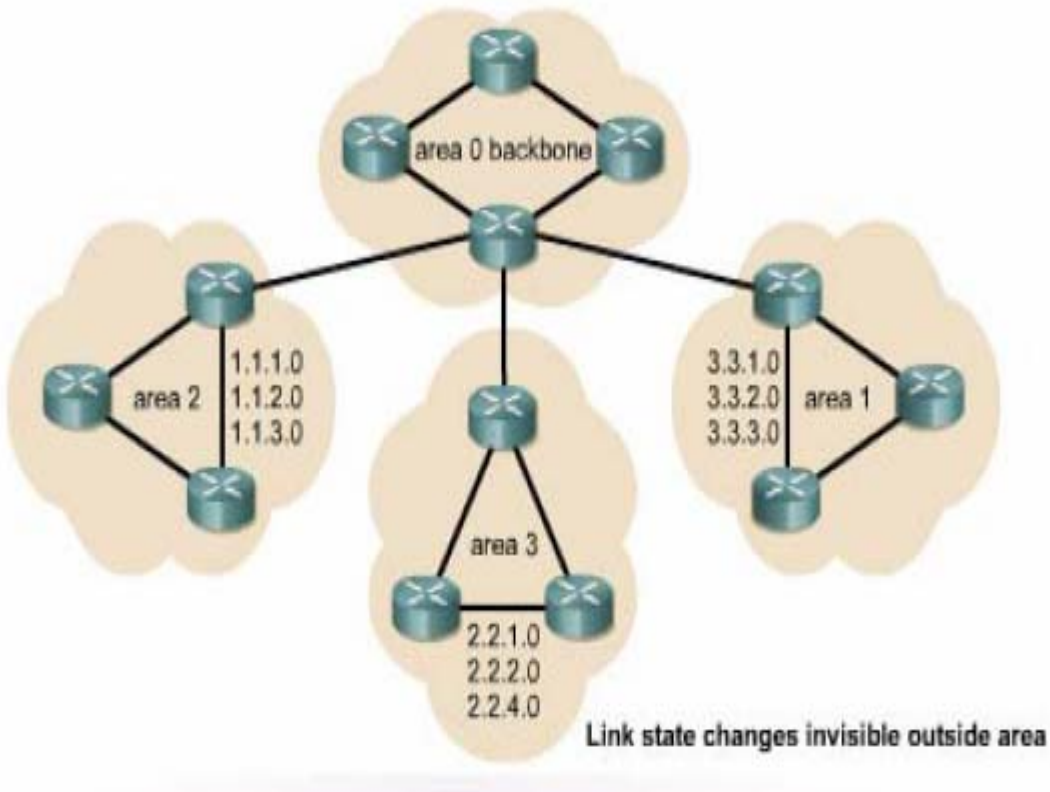
Đặc điểm chung

Link State Routing (LSR)



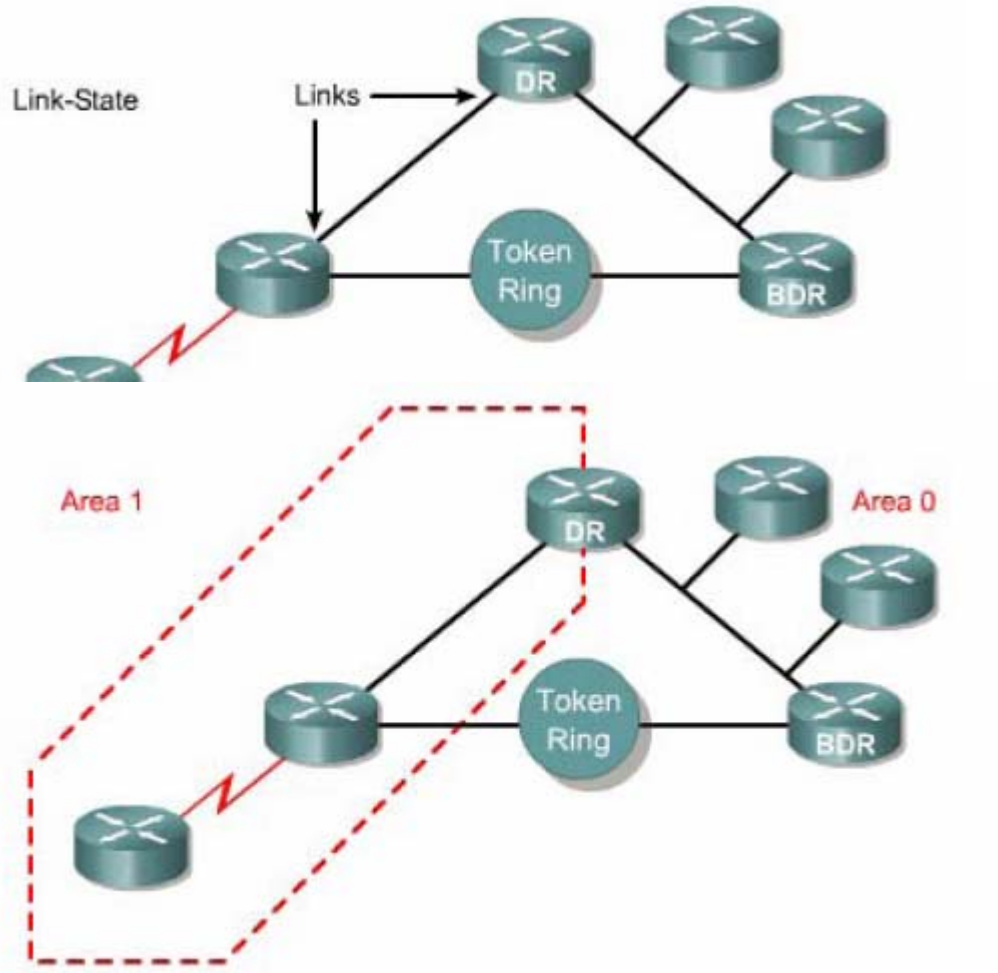
OSPF (OPEN SHORTEST PATH FIRST)
Tổng quát về OSPF

- OSPF được triển khai dựa theo các chuẩn mở.
- Tốt hơn RIP.
- Có khả năng mở rộng.
- Có thể cấu hình đơn vùng để sử dụng cho các mạng nhỏ.



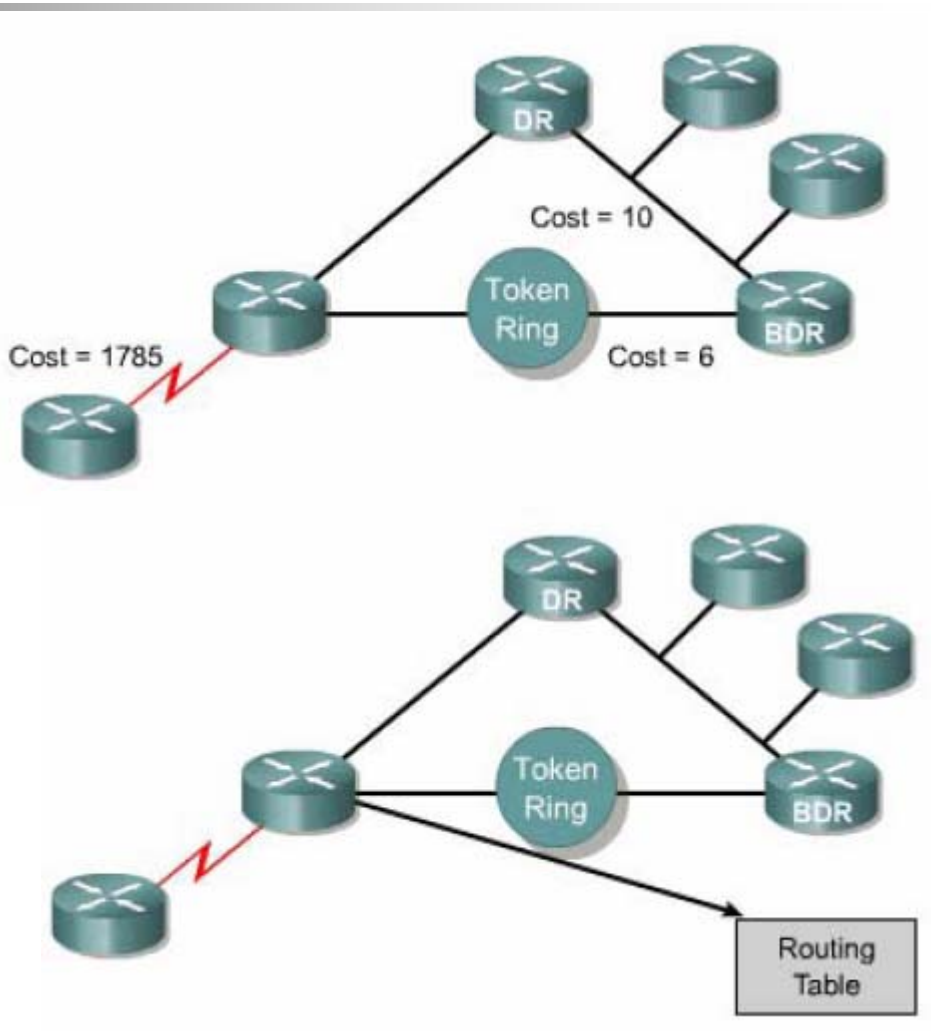
OSPF (OPEN SHORTEST PATH FIRST)
Một số thuật ngữ của OSPF

- Link: một cổng trên router.
- Link-state: trạng thái của một đường liên kết giữa 2 router.
- Topological database: danh sách các thông tin về mọi đường liên kết trong vùng.
- Area: tập hợp các mạng và các router có cùng chỉ số danh định vùng. Mỗi router trong 1 vùng chỉ xây dựng cơ sở dữ liệu về trạng thái đường liên kết trong vùng đó.



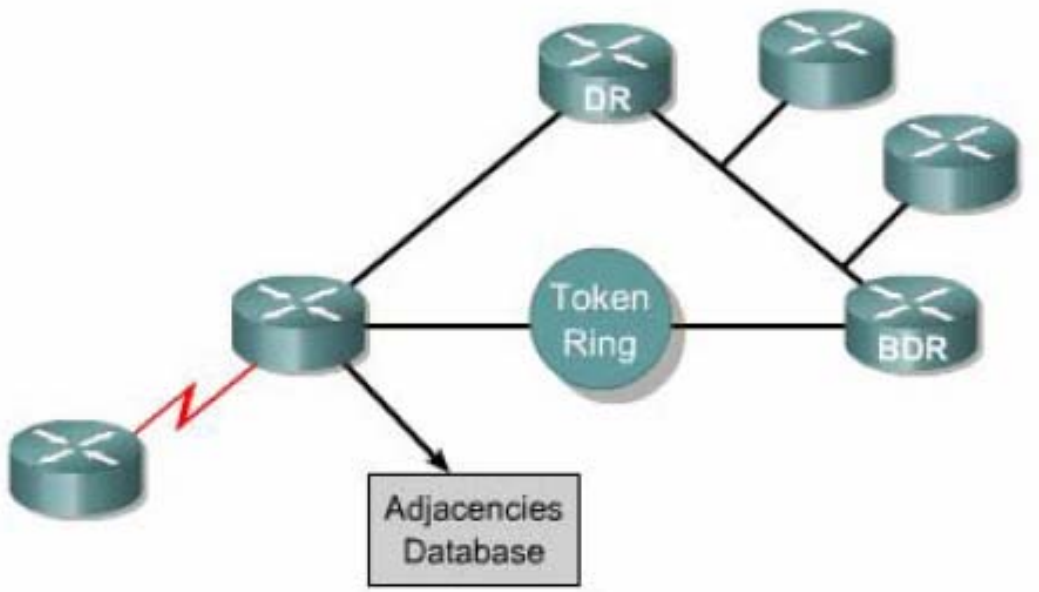
OSPF (OPEN SHORTEST PATH FIRST)
Một số thuật ngữ của OSPF

- Cost: giá trị chi phí đặt cho một đường liên kết (dựa trên băng thông hoặc tốc độ của đường liên kết đó).
- Routing table: bảng định tuyến là kết quả chọn đường của thuật toán chọn đường dựa trên cơ sở dữ liệu về trạng thái đường liên kết.

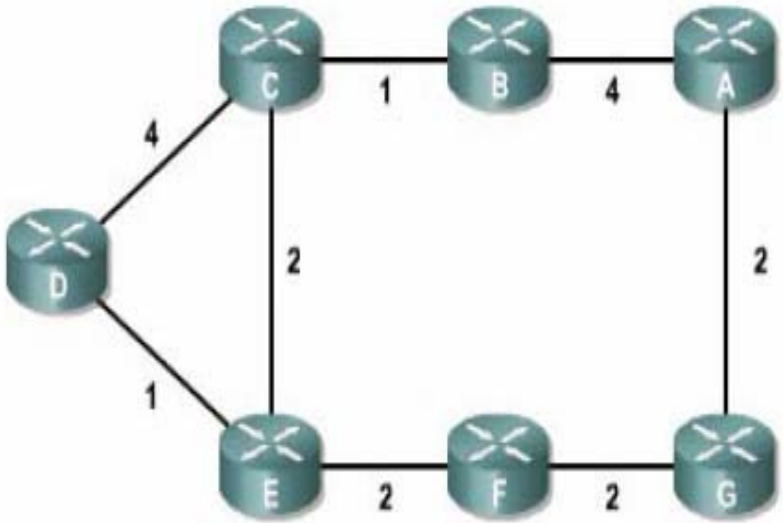


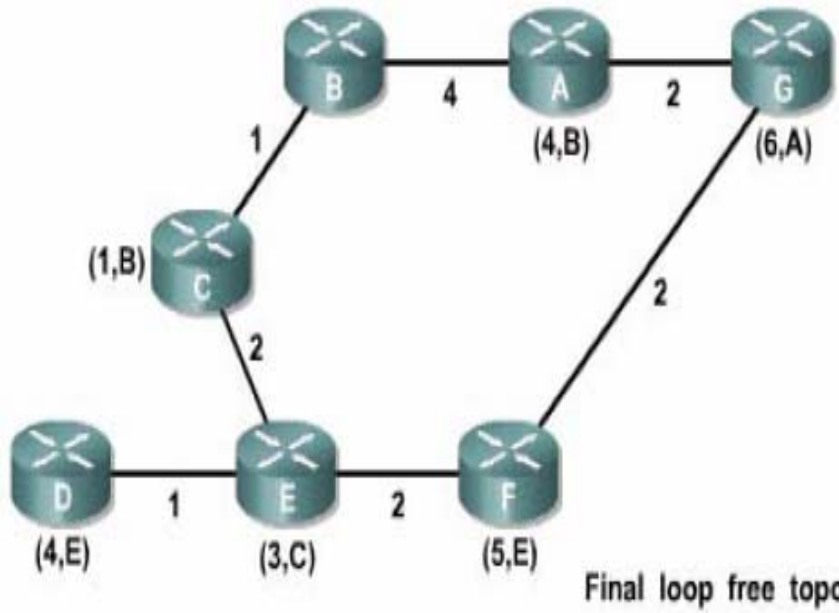
OSPF (OPEN SHORTEST PATH FIRST)
Một số thuật ngữ của OSPF

- Adjacency database: danh sách các router láng giềng có mối quan hệ hai chiều. Mỗi router có một danh sách khác nhau.
- DR (Designated Router) và BDR (Backup Designated Router) là router được tất cả các router khác trong cùng mạng bầu ra làm đại diện. Mỗi mạng sẽ có một DR và BDR riêng.



OSPF (OPEN SHORTEST PATH FIRST)
Thuật toán tìm đường ngắn nhất





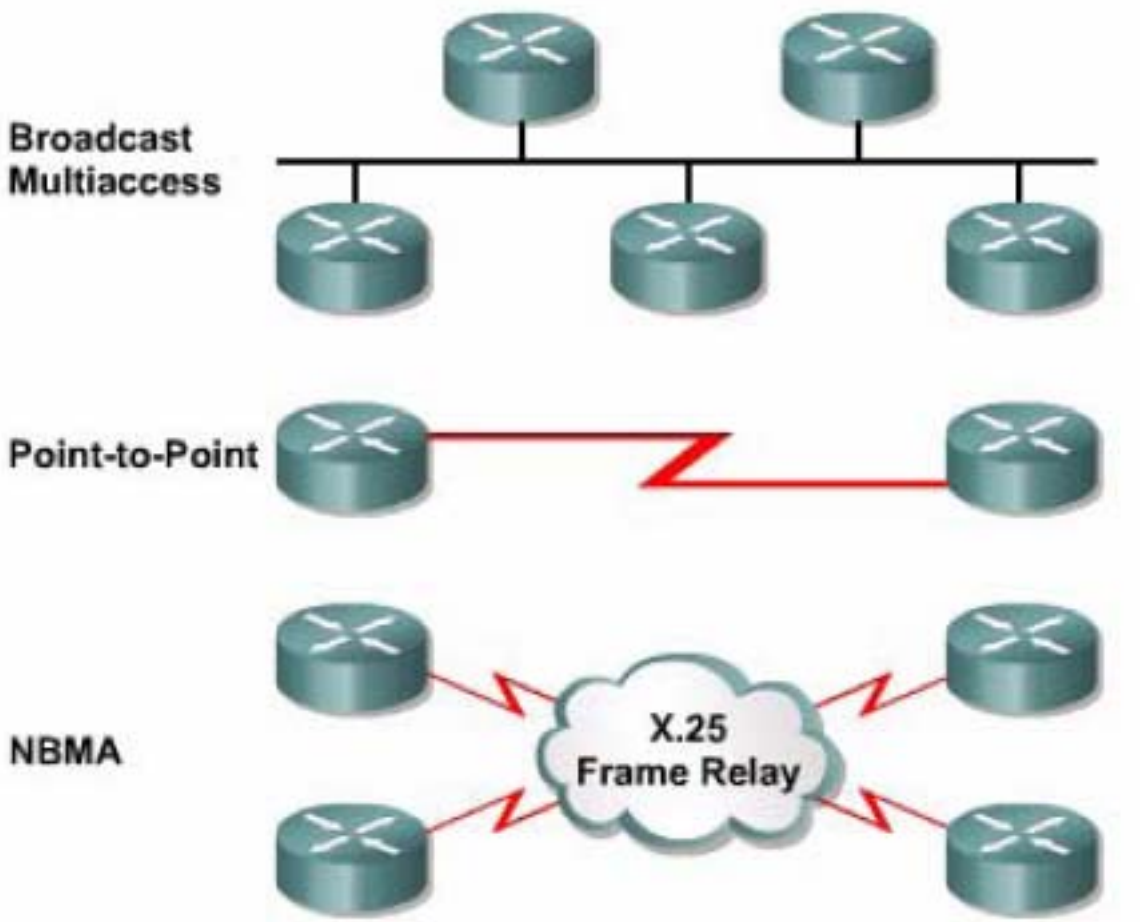
A	B	C	D	E	F	G
B/4	A/4	B/1	C/4	C/2	E/2	A/2
G/2	C/1	D/4	E/1	D/1	G/2	F/2
		E/2		F/2		

A	B	C	D	E	F	G
B/4	A/4	B/1	C/4	C/2	E/2	A/2
G/2	C/1	D/4	E/1	D/1	G/2	F/2
		E/2		F/2		

OSPF (OPEN SHORTEST PATH FIRST)
Các loại mạng OSPF

OSPF nhận biết 3 loại mạng:

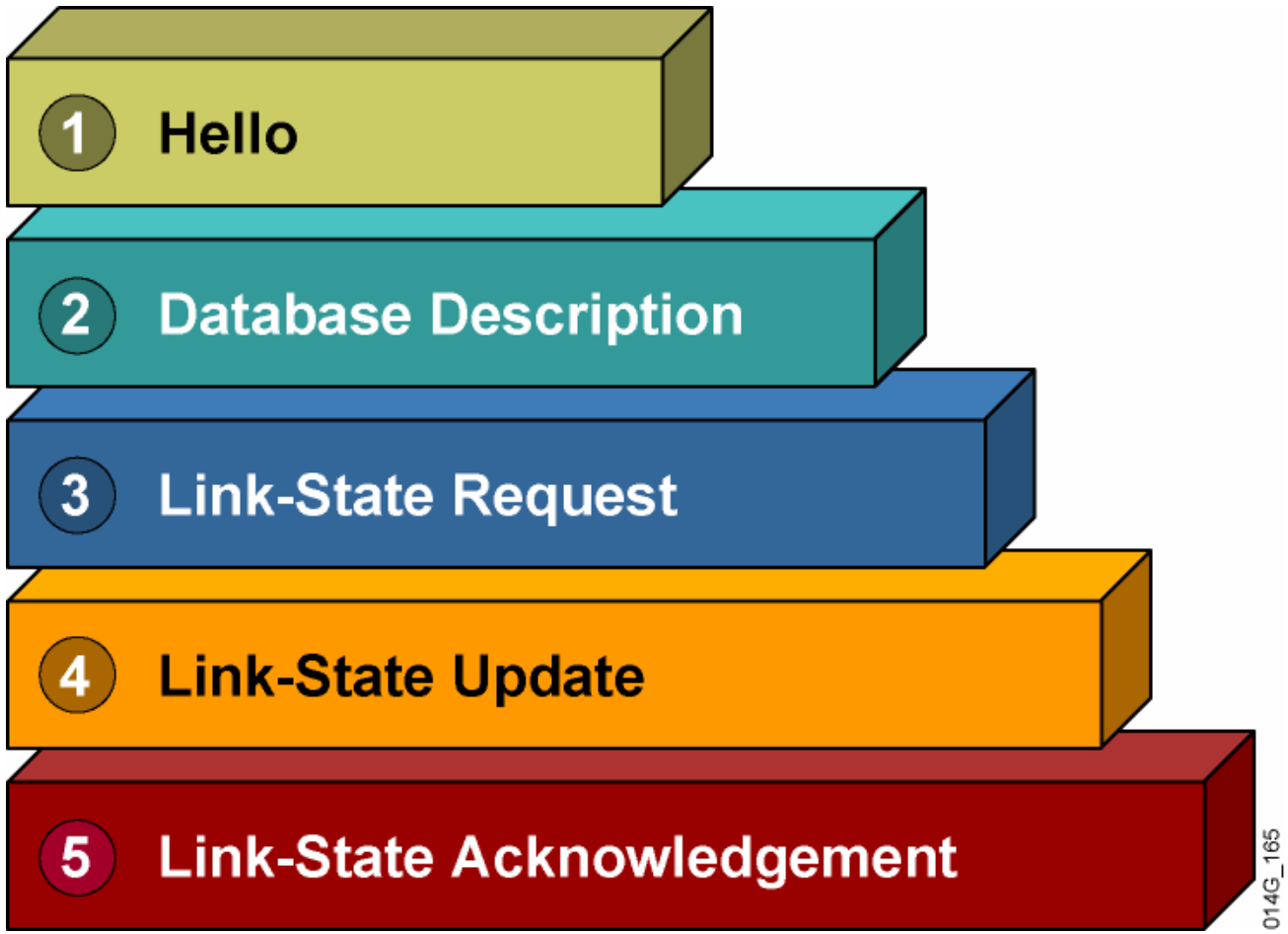
- Mạng quảng bá đa truy cập.
- Mạng điểm – nối – điểm.
- Mạng không quảng bá đa truy cập (NBMA – Nonbroadcast multiaccess).



OSPF (OPEN SHORTEST PATH FIRST)
Các loại mạng OSPF

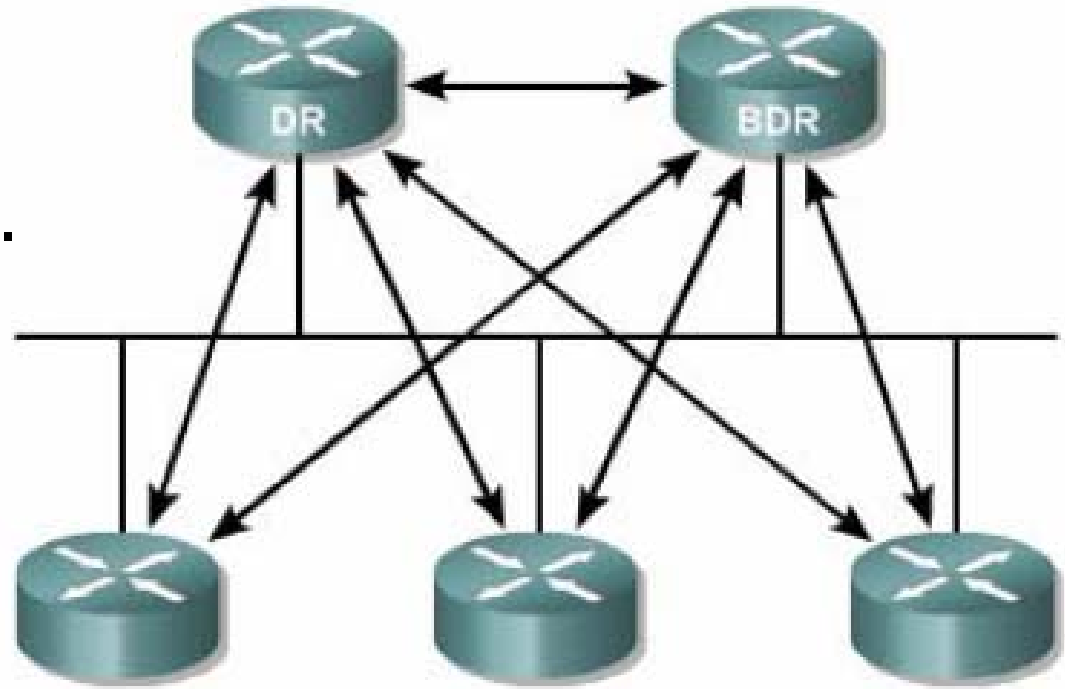
Network Type	Characteristics	DR Election?
Broadcast multiaccess	Ethernet, Token Ring, or FDDI	Yes
Nonbroadcast multiaccess	Frame Relay, X.25, SMDS	Yes
Point-to-point	PPP, HDLC	No
Point-to-multipoint	Configured by an administrator	No

OSPF (OPEN SHORTEST PATH FIRST)
Các kiểu gói tin OSPF

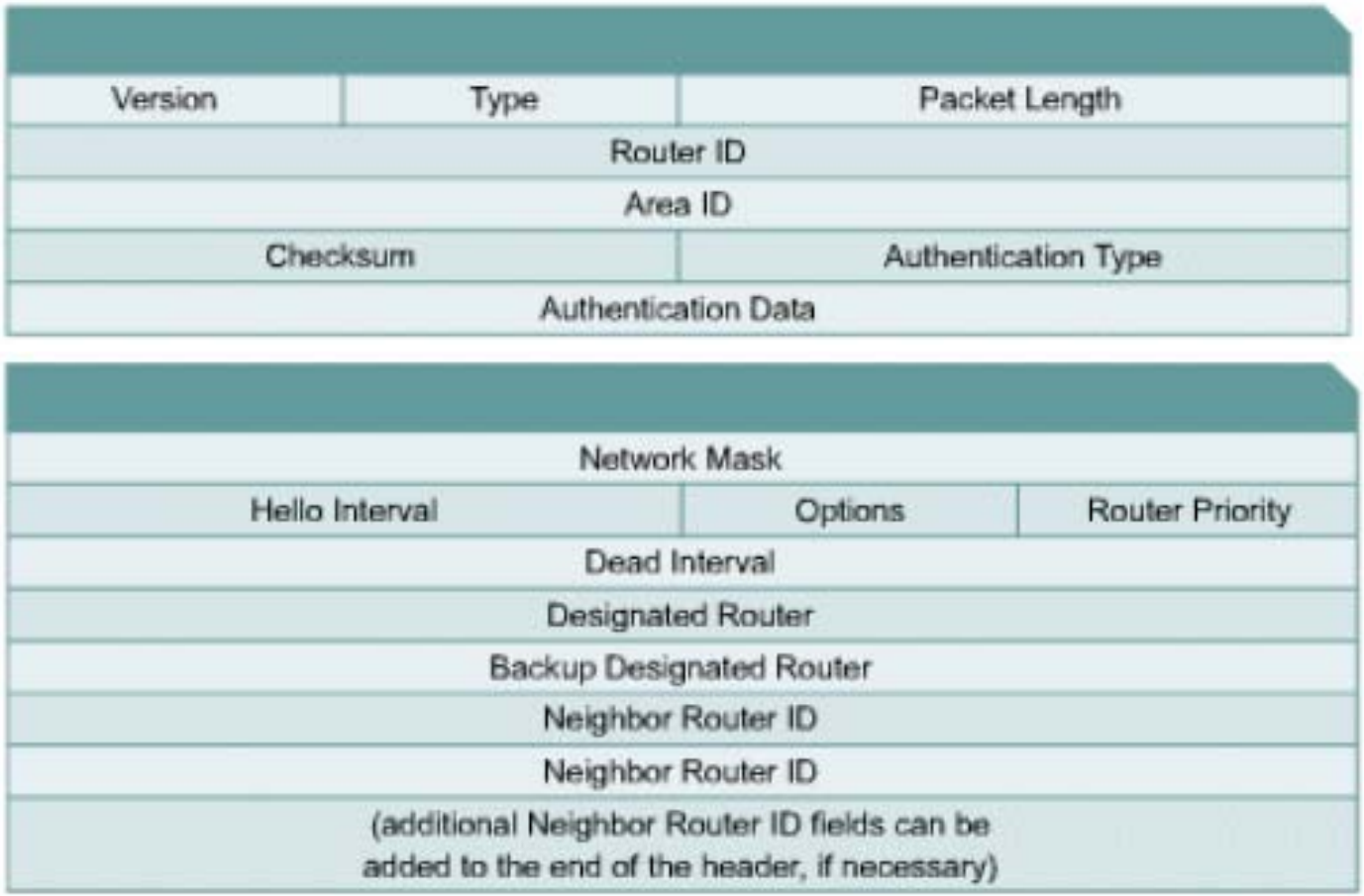


OSPF (OPEN SHORTEST PATH FIRST)
DR và BDR nhận các gói LSAs

- Router với Router ID cao nhất được chọn làm DR, kế tiếp là BDR.
- Các router chỉ gởi thông tin về trạng thái đường liên kết cho DR.
- DR sẽ gởi thông tin này cho các router trong mạng bằng địa chỉ multicast 224.0.0.5.



OSPF (OPEN SHORTEST PATH FIRST)
Phần header của gói OSPF và OSPF Hello



Version	Type	Packet Length
Router ID		
Area ID		
Checksum	Authentication Type	
Authentication Data		

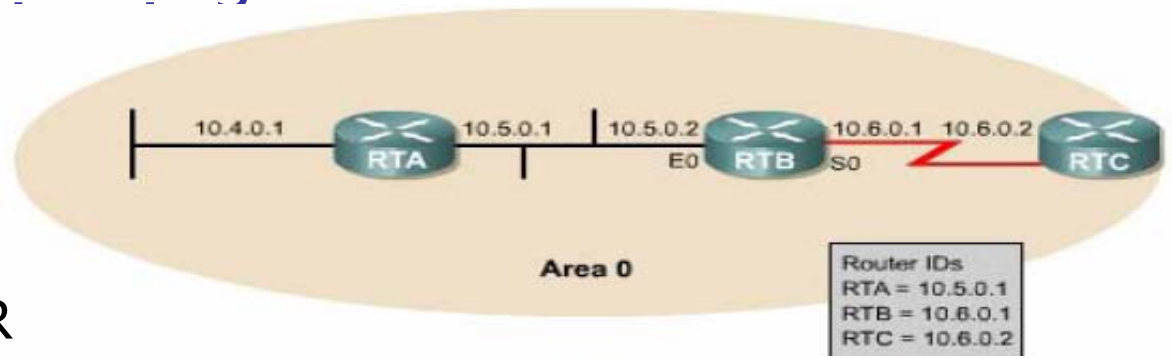
Network Mask		
Hello Interval	Options	Router Priority
Dead Interval		
Designated Router		
Backup Designated Router		
Neighbor Router ID		
Neighbor Router ID		
(additional Neighbor Router ID fields can be added to the end of the header, if necessary)		

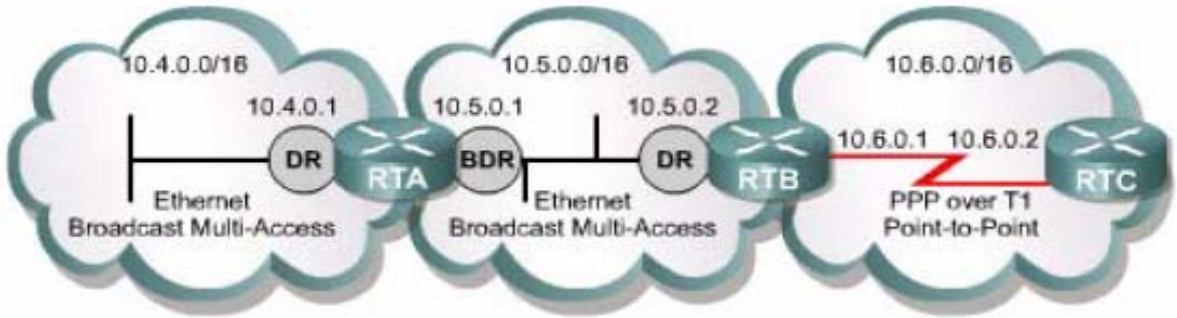
OSPF (OPEN SHORTEST PATH FIRST)
Router ID

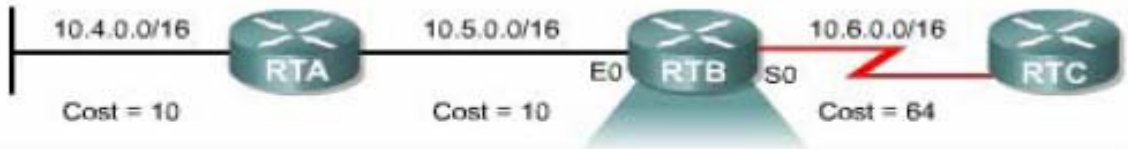
- Router ID là một số 32 bit, có giá trị duy nhất, dùng đển nhận dạng router.
- Mặc định Router ID được chọn từ địa chỉ IP cao nhất trong số các giao tiếp đang hoạt động trên router, ngoại trừ loopback interface hoặc Router Priority được cấu hình (mặc định là 1).

OSPF (OPEN SHORTEST PATH FIRST)
Các bước hoạt động của OSPF

- Bước 1: phát hiện router láng giềng bằng giao thức OSPF Hello.
- Bước 2: bầu DR và BDR (trong mạng đa truy cập).
- Bước 3: Mỗi router gởi thông tin về trạng thái đường liên kết trong gói LSAs (Link-State Advertisements). Sau khi cơ sở dữ liệu về trạng thái đường liên kết đã đầy đủ, áp dụng thuật toán SPF để chọn đường tốt nhất đưa vào bảng định tuyến.







Net	Cost	Out Interface
10.4.0.0	20	E0

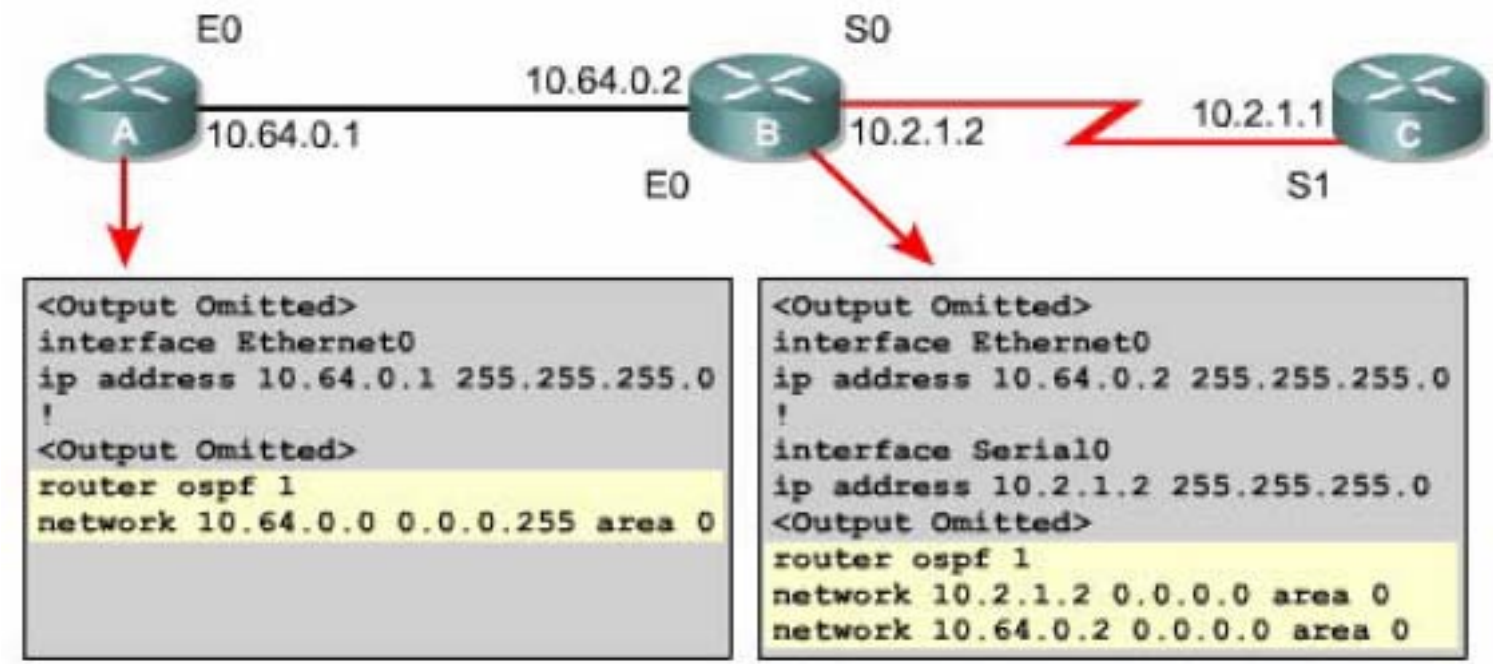
OSPF (OPEN SHORTEST PATH FIRST)
Cấu hình OSPF đơn vùng

Khởi động định tuyến OSPF:

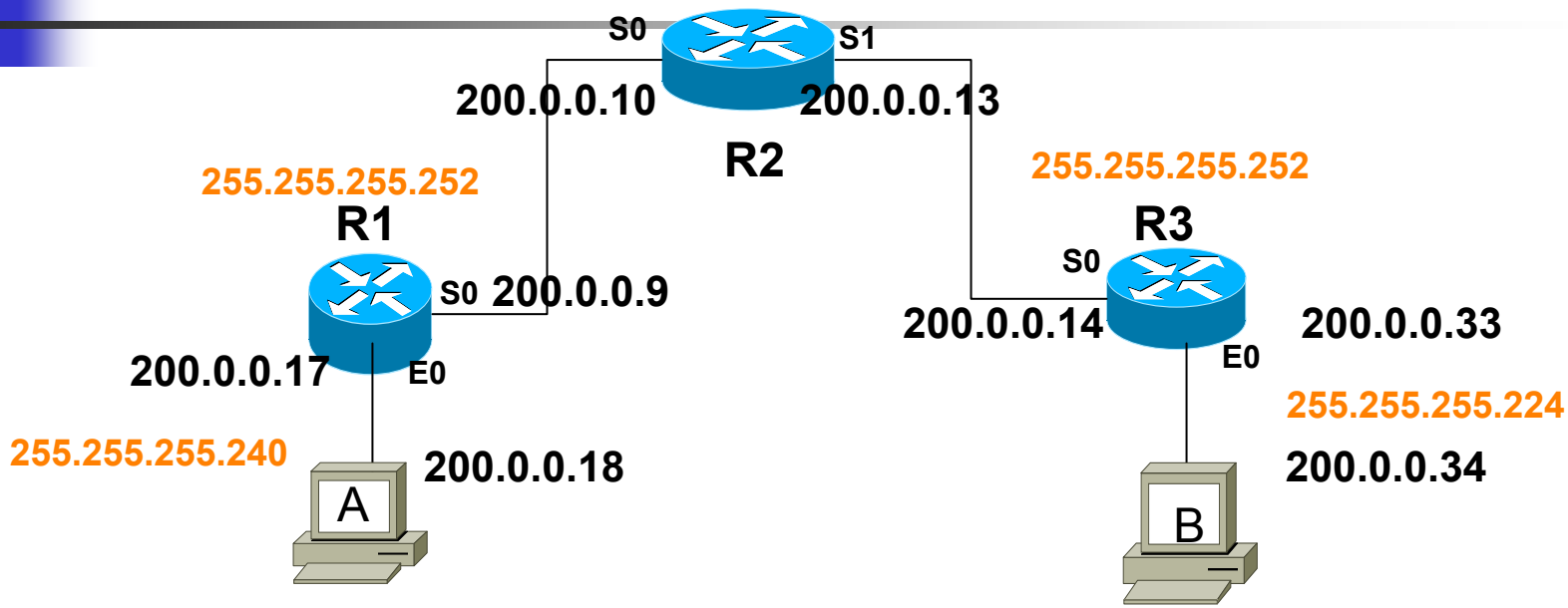
Router(config)#**router ospf** *process-id*

Khai báo địa chỉ mạng cho OSPF:

Router(config-router)#**network** *address willcard-mask* **area** *area-id*



OSPF (OPEN SHORTEST PATH FIRST)
Cấu hình OSPF đơn vùng



R1#**config t**
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#**router ospf 1**
R1(config-router)#**network 200.0.0.16 0.0.0.15 area 0**
R1(config-router)#**network 200.0.0. 8 0.0.0.3 area 0**
R1(config-router)#**^Z**

32 - 63

R3#**config t**
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#**router ospf 1**
R3(config-router)#**network 200.0.0. 32 0.0.0.31 area 0**
R3(config-router)#**network 200.0.0. 12 0.0.0.3 area 0**
R3(config-router)#**^Z**

12 - 15

OSPF (OPEN SHORTEST PATH FIRST)

Cấu hình địa chỉ loopback cho OSPF

Tạo cổng loopback và đặt địa chỉ IP:

Router(config)#**interface loopback** *number*

Router(config-if)#**ip address** *ip-address subnet-mask*

```
! Create the loopback 0 interface
Sydney3(config)#interface loopback 0
Sydney3(config-if)#ip address 192.168.31.33
255.255.255.255
Sydney3(config-if)#exit
! Remove loopback 0 interface
Sydney3(config)#no interface loopback 0
Sydney3(config)#
01:47:27: %LINK-5-CHANGED: Interface Loopback0, changed
state to administratively down
```

OSPF (OPEN SHORTEST PATH FIRST)

Cấu hình quyền ưu tiên cho router

Thay đổi giá trị ưu tiên cho OSPF:

Router(config-if)#**ip ospf priority** *number* ← (0 – 255)

Router#**show ip ospf interfacetype** *number*

```
Sydney1(config)#interface fastethernet 0/0
Sydney1(config-if)#ip ospf priority 50
Sydney1(config-if)#end
Sydney1#
00:21:57: %SYS-5-CONFIG_I: Configured from console
by console
```

OSPF (OPEN SHORTEST PATH FIRST)

Cấu hình quyền ưu tiên cho router

```
Sydney1>show ip ospf interface fastethernet 0/0
FastEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0
  Process ID 1, Router ID 192.168.31.11, Network
Type BROADCAST, Cost:1 Transmit Delay is 1 sec,
State DROTHER, Priority 50
  Designated Router (ID) 192.168.31.22, Interface
address 192.168.1.2
  Backup Designated router (ID) 192.168.31.33,
Interface address 192.168.1.3
  Timer intervals configured, Hello 10, Dead 40,
Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 2
  Last flood scan time is 0 msec, maximum is 0
msec
  Neighbor Count is 2, Adjacent neighbor count is
2
    Adjacent with neighbor 192.168.31.33  (Backup
Designated Router)
    Adjacent with neighbor 192.168.31.22
(Designated Router)
```

OSPF (OPEN SHORTEST PATH FIRST)

Thay đổi giá trị chi phí của OSPF

Thay đổi giá trị chi phí cho OSPF:

Router(config)#**interface serial** *0/0*

Router(config-if)#**bandwidth** *64*

Medium	Cost
56 kbps serial link	1785
T1 (1.544 Mbps serial link)	64
E1 (2.048 Mbps serial link)	48
4 Mbps Token Ring	25
Ethernet	10
16 Mbps Token Ring	6
100 Mbps Fast Ethernet, FDDI	1

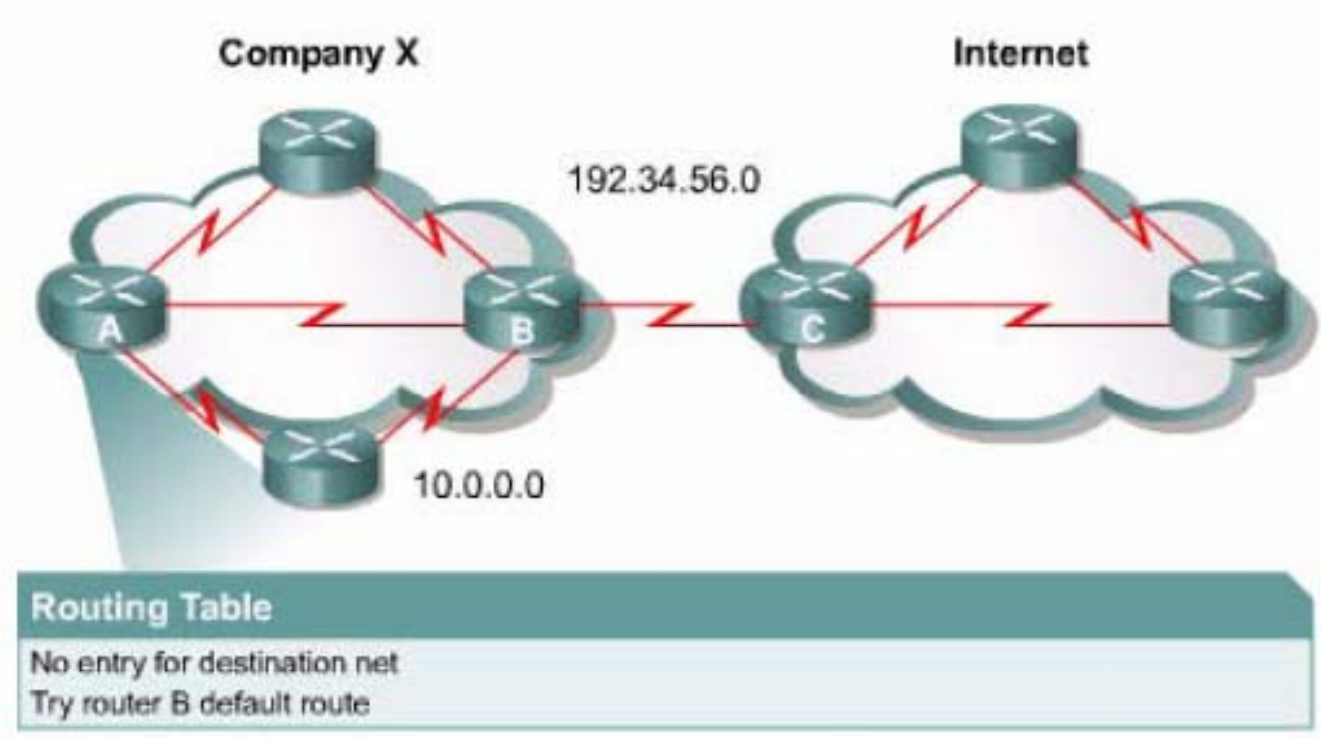
OSPF (OPEN SHORTEST PATH FIRST)

OSPF thực hiện quảng bá đường mặc định

Cấu hình đường mặc định cho router có cổng kết nối ra ngoài:

Router(config)#**ip route** *0.0.0.0 0.0.0.0 [interface | next-hop address]*

Router(config-router)#**default-information originate**



OSPF (OPEN SHORTEST PATH FIRST)

Các lệnh *show* dùng để kiểm tra cấu hình OSPF

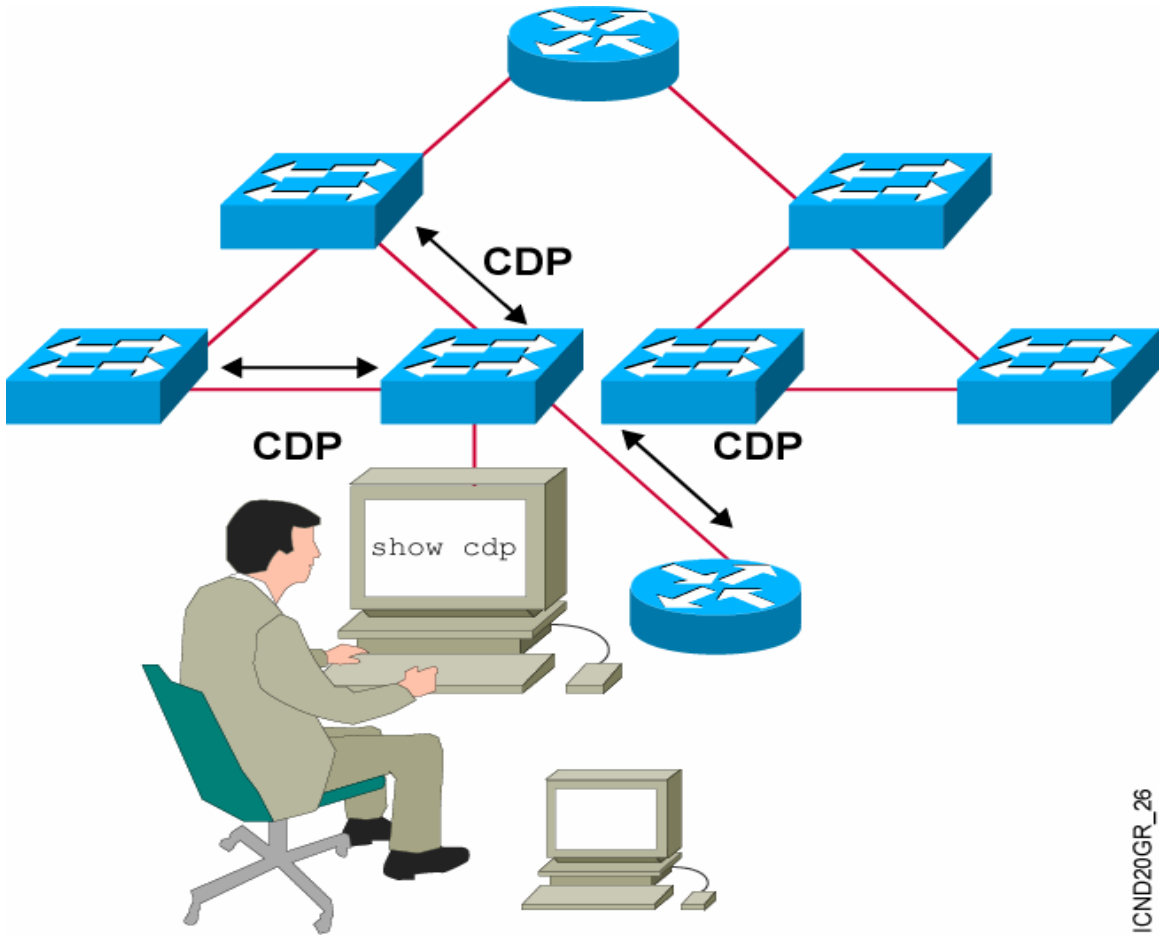
Lệnh	Giải thích
Show ip protocol	Hiển thị các thông tin về thông số thời gian, thông số định tuyến, mạng định tuyến và nhiều thông tin khác của tất cả các giao thức định tuyến đang hoạt động trên router.
Show ip route	Hiển thị bảng định tuyến của router, trong đó là danh sách các đường tốt nhất đến các mạng đích của bản thân router và cho biết router học được các đường đi này bằng cách nào.
Show ip ospf interface	Lệnh này cho biết cổng của router đã được cấu hình đúng với vùng mà nó thuộc về hay không. Nếu cổng loopback không được cấu hình thì ghi địa chỉ IP của cổng vật lý nào có giá trị lớn nhất sẽ được chọn làm router ID. Lệnh này cũng hiển thị các thông số của khoảng thời gian hello và khoảng thời gian bất động trên cổng đó, đồng thời cho biết các router láng giềng thân mật kết nối vào cổng.

OSPF (OPEN SHORTEST PATH FIRST)

Các lệnh *clear* và *debug* dùng để kiểm tra hoạt động OSPF

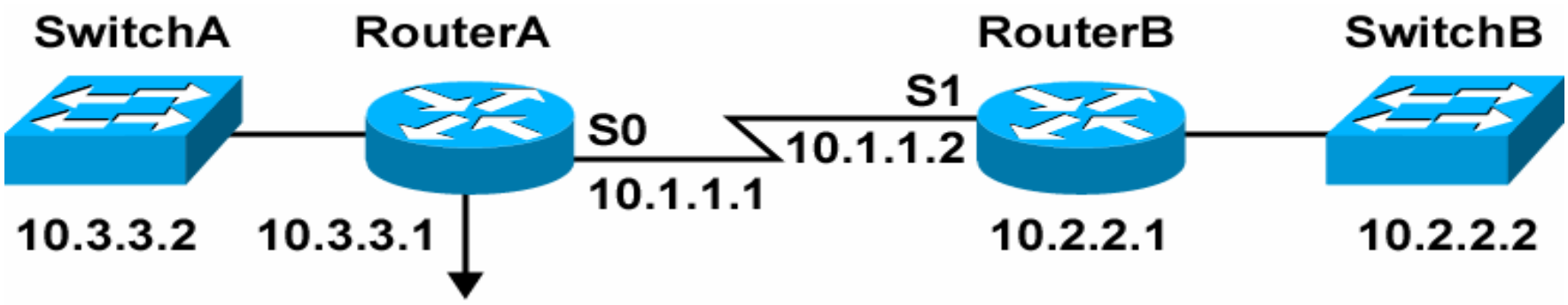
Lệnh	Giải thích
Clear ip route *	Xoá toàn bộ bảng định tuyến.
Clear ip route a.b.c.d	Xoá đường a.b.c.d trong bảng định tuyến.
Debug ip ospf events	Báo cáo mọi sự kiện của OSPF.
Debug ip ospf adj	Báo cáo mọi sự kiện về hoạt động quan hệ thân mật của OSPF.

CDP (Cisco Discovery Protocol)



CDP (Cisco Discovery Protocol)

Show cdp ?

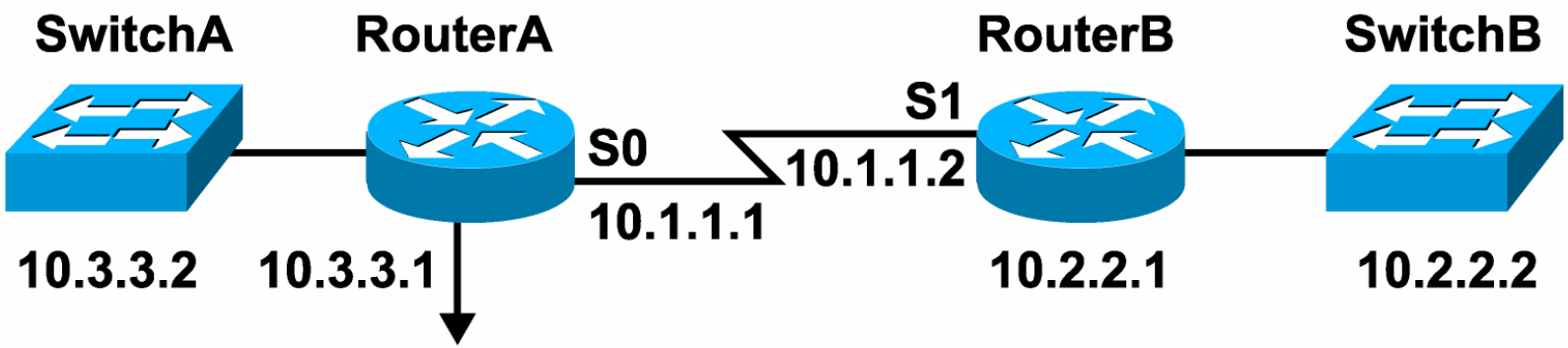



```
RouterA#show cdp ?
  entry      Information for specific neighbor entry
  interface  CDP interface status and configuration
  neighbors  CDP neighbors entries
  traffic    CDP statistics
  <cr>
RouterA(config-if)#exit
RouterA(config)#no cdp run
RouterA(config)#interface serial0
RouterA(config-if)#no cdp enable
```

ICND20GR_27

CDP (Cisco Discovery Protocol)

Show cdp neighbors



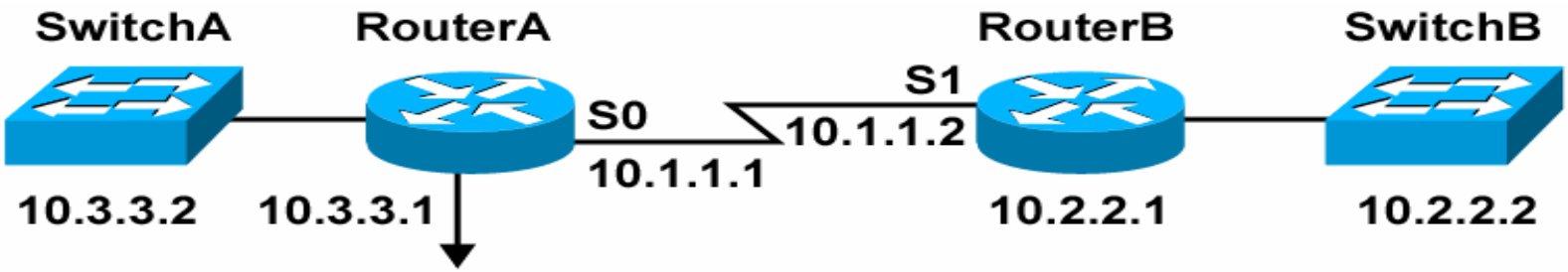

```
RouterA#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
RouterB              Ser 0         148          R        2522      Ser 1
SwitchA0050BD855780  Eth 0         167          T S      1900      2
```

ICND20GR_28

SwitchA also provides its MAC address (Catalyst 1900 only).

CDP (Cisco Discovery Protocol)

Show cdp entry

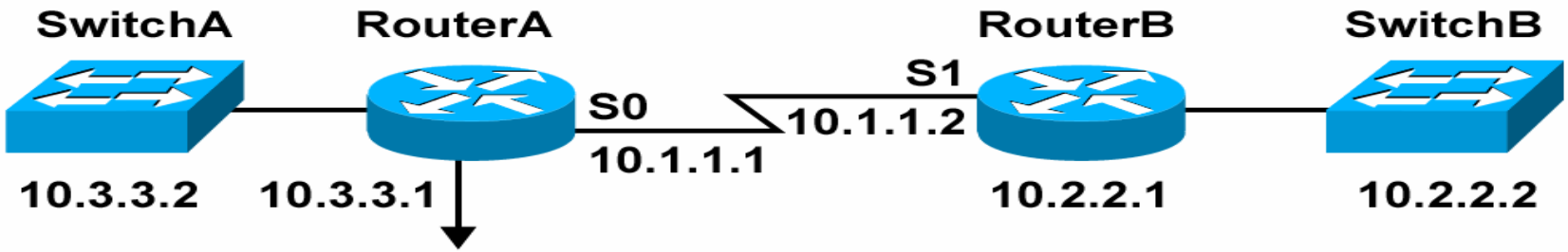



```
RouterA#show cdp entry *
-------------------------
Device ID: RouterB
Entry address(es):
  IP address: 10.1.1.2
Platform: cisco 2522,  Capabilities: Router
Interface: Serial0,  Port ID (outgoing port): Serial1
Holdtime : 168 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-JS-L), Version 12.0(3), RELEASE SOFTWARE (fci)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Mon 08-Feb-99 18:18 by phanguye
```

ICND20GR_29

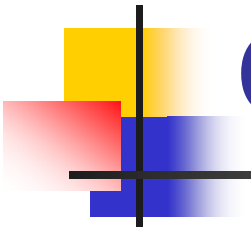
CDP (Cisco Discovery Protocol)

Show cdp traffic




```
RouterA#show cdp traffic
CDP counters :
 Packets output: 56, Input: 38
 Hdr syntax: 0, Chksum error: 0, Encaps failed: 3
 No memory: 0, Invalid packet: 0, Fragmented: 0


RouterA#show cdp interface
BRI0 is administratively down, line protocol is down
  Encapsulation HDLC
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
```

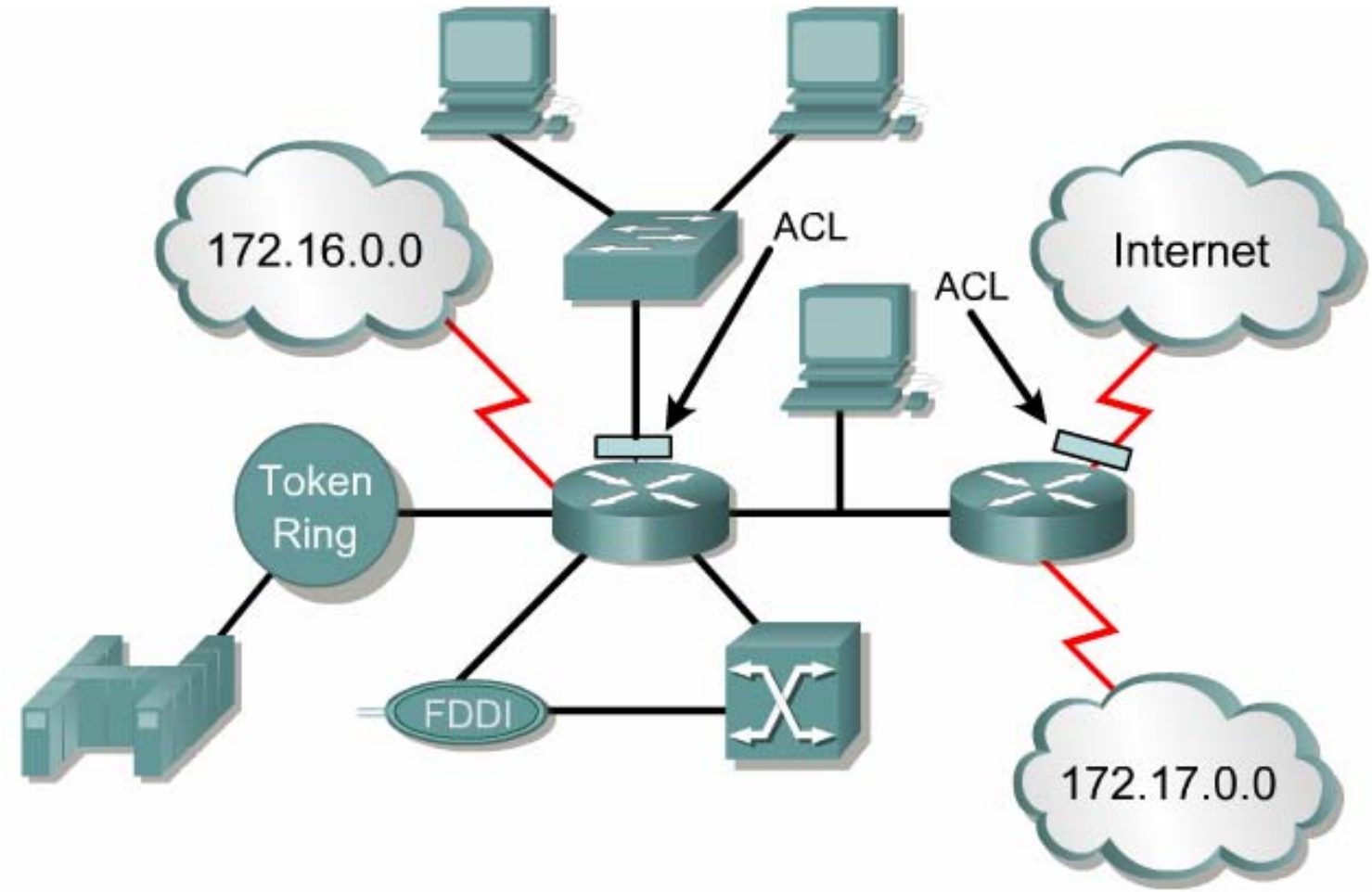
ICND20GR_30



CHƯƠNG 7

Access Control List

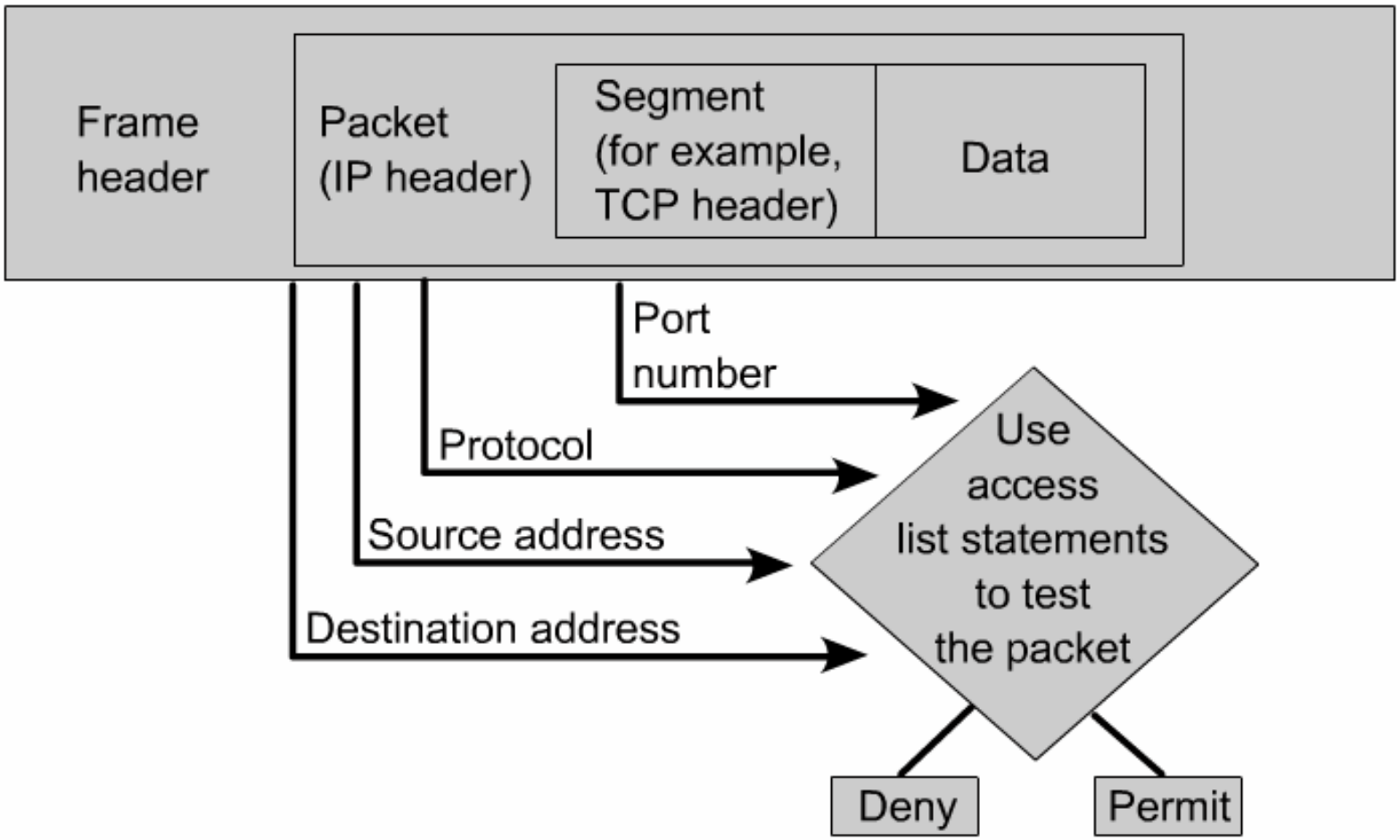
Danh sách kiểm tra truy cập (ACL)
Giới thiệu



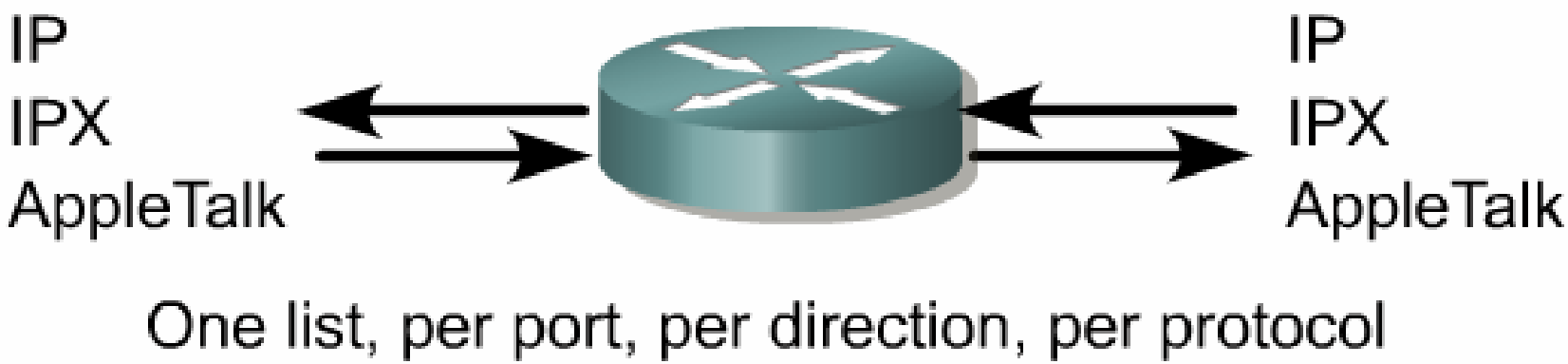
Danh sách kiểm tra truy cập (ACL)
Giới thiệu

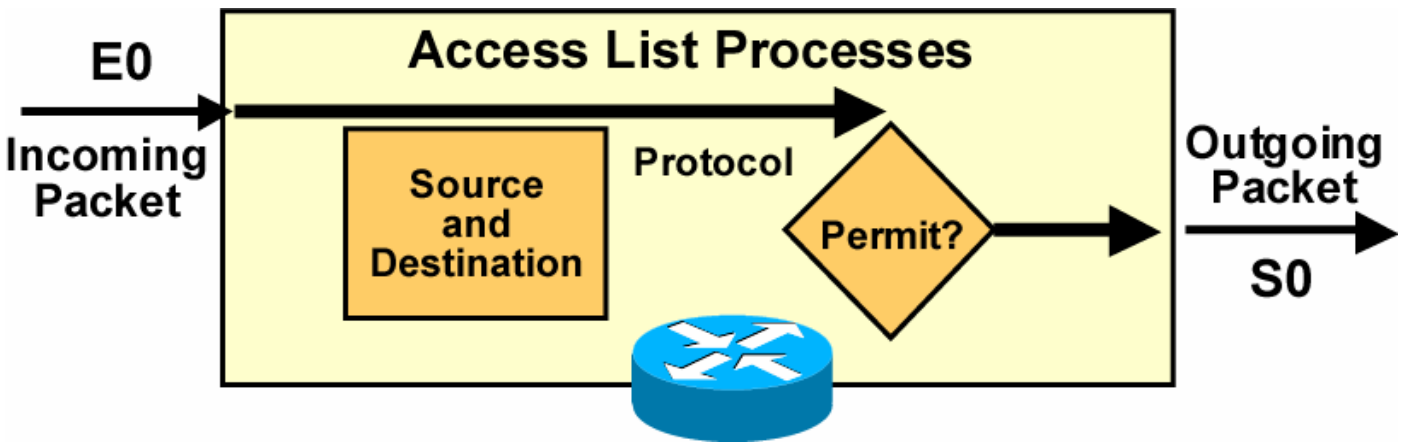
- ACL là một danh sách các điều kiện được áp dụng cho lưu lượng đi qua một cổng của router. Danh sách này cho biết loại gói nào được chấp nhận hay bị từ chối.
- ACL được sử dụng để quản lý lưu lượng mạng và bảo vệ truy cập ra hoặc vào hệ thống mạng.
- ACL kiểm tra các gói dựa vào địa chỉ nguồn và đích, giao thức, số port, hướng di chuyển của gói để quyết định chuyển gói đi hay hủy bỏ gói.

Danh sách kiểm tra truy cập (ACL)
Giới thiệu



Danh sách kiểm tra truy cập (ACL)
Giới thiệu



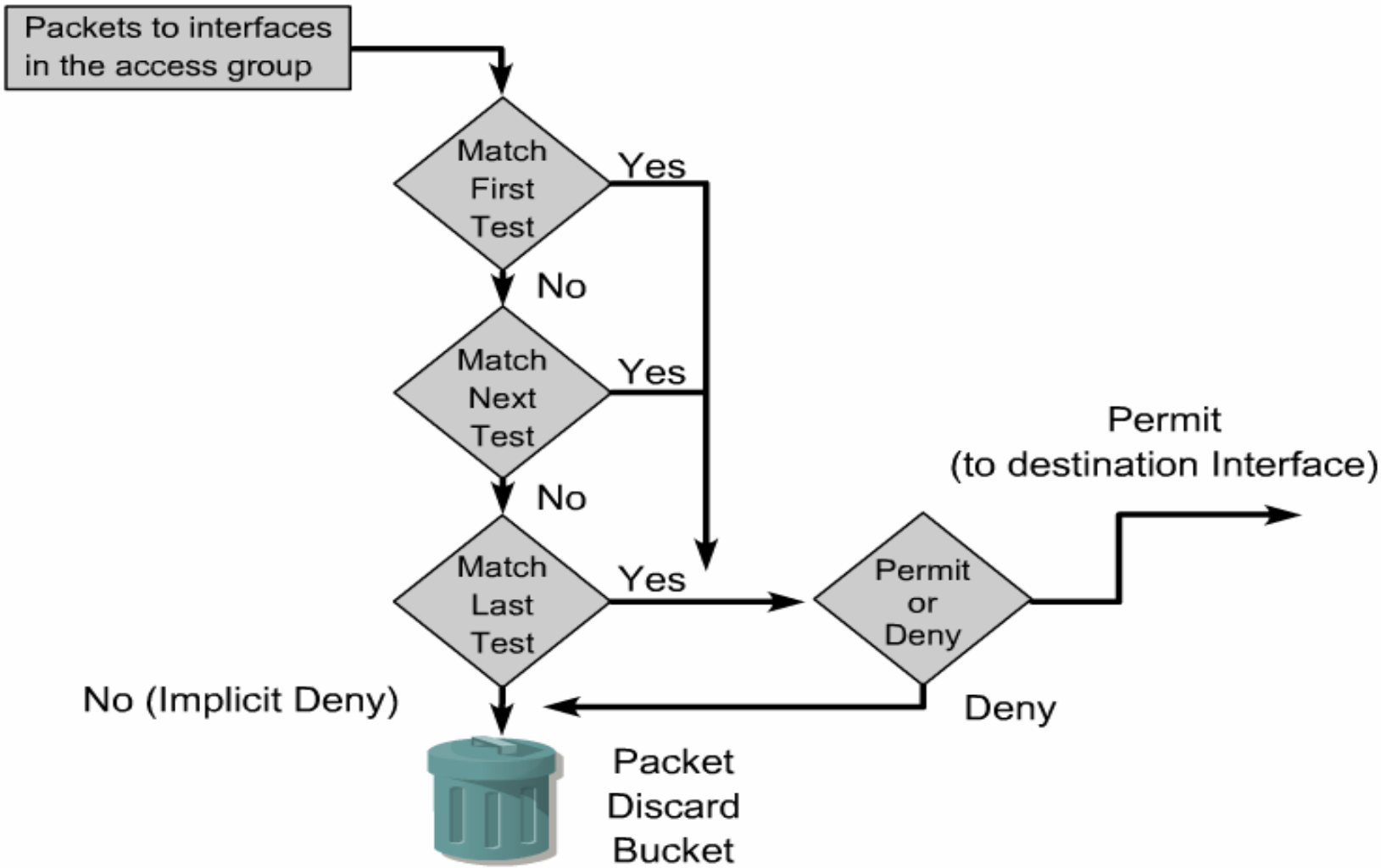


Danh sách kiểm tra truy cập (ACL)
Công dụng của ACL

- Giới hạn lưu lượng mạng để tăng hiệu suất hoạt động của mạng.
  - Ví dụ cấm lưu lượng truyền Video.
- Kiểm tra dòng lưu lượng, quyết định cho phép hoặc cấm loại lưu lượng nào được đi qua.
  - Ví dụ lưu lượng email, telnet.
- Bảo vệ truy cập.
  - Chỉ cho phép user truy cập vào một loại tập tin nào đó, vào vùng mạng nào đó trong hệ thống.

Danh sách kiểm tra truy cập (ACL)

Hoạt động của ACL



Danh sách kiểm tra truy cập (ACL)
Phân loại

Access List Type		Number Range/Identifier
IP	Standard	1-99, 1300-1999
	Extended	100-199, 2000-2699
	Named	Name

ICND20GR_57

- ACL cơ bản (1-99): thực hiện kiểm tra địa chỉ IP nguồn của gói dữ liệu.
- ACL mở rộng (100-199): kiểm tra địa chỉ nguồn và đích của gói dữ liệu, kiểm tra giao thức lẫn số port.
- ACL đặt tên (Name): từ phiên bản Cisco IOS 11.2 trở đi, cho phép tạo ACL cơ bản và mở rộng theo tên thay vì theo số.

Danh sách kiểm tra truy cập (ACL)
Tạo ACL cơ bản

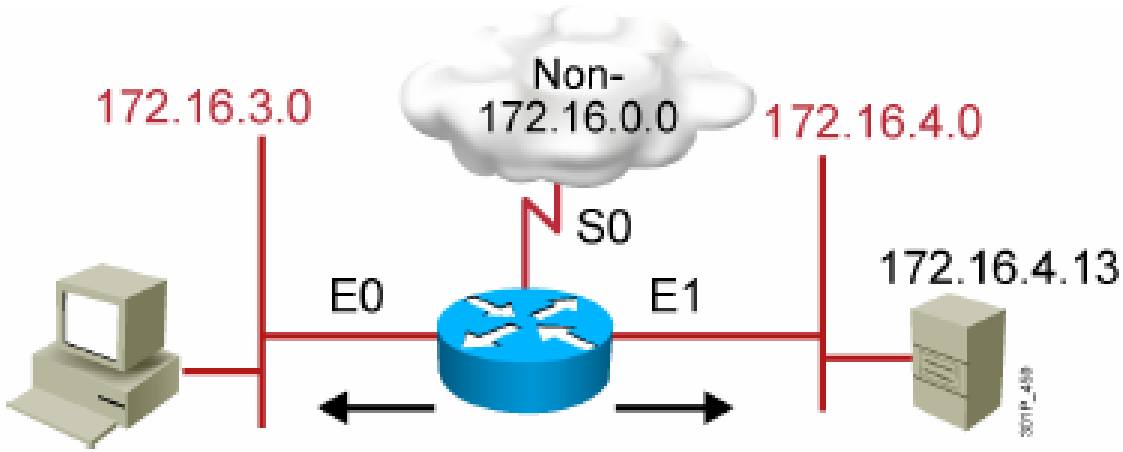
❑ Cú pháp lệnh:

Router(config)#**access-list** *access-list-number* {deny | permit} source [*source-wildcard*]
……..

Router(config-if)#{protocol} **access-group** *access-list-number* {in | out}

❑ Hủy một ACL:
Router(config)#**no access-list** *access-list-number*

Danh sách kiểm tra truy cập (ACL)
Tạo ACL cơ bản

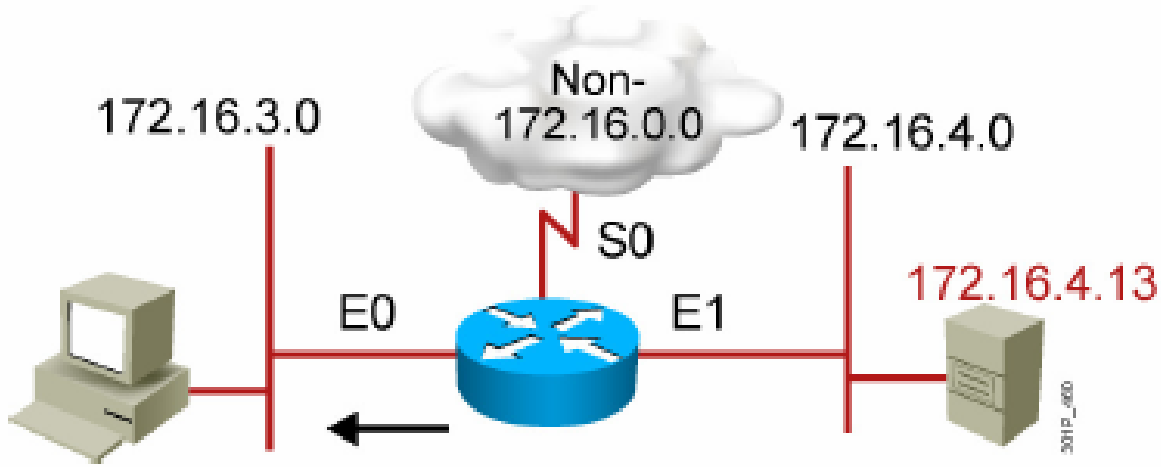



```
RouterX(config)# access-list 1 permit 172.16.0.0  0.0.255.255
(implicit deny all - not visible in the list)
(access-list 1 deny 0.0.0.0   255.255.255.255)

RouterX(config)# interface ethernet 0
RouterX(config-if)# ip access-group 1 out
RouterX(config)# interface ethernet 1
RouterX(config-if)# ip access-group 1 out
```

Chỉ cho phép các mạng nội bộ

Danh sách kiểm tra truy cập (ACL)

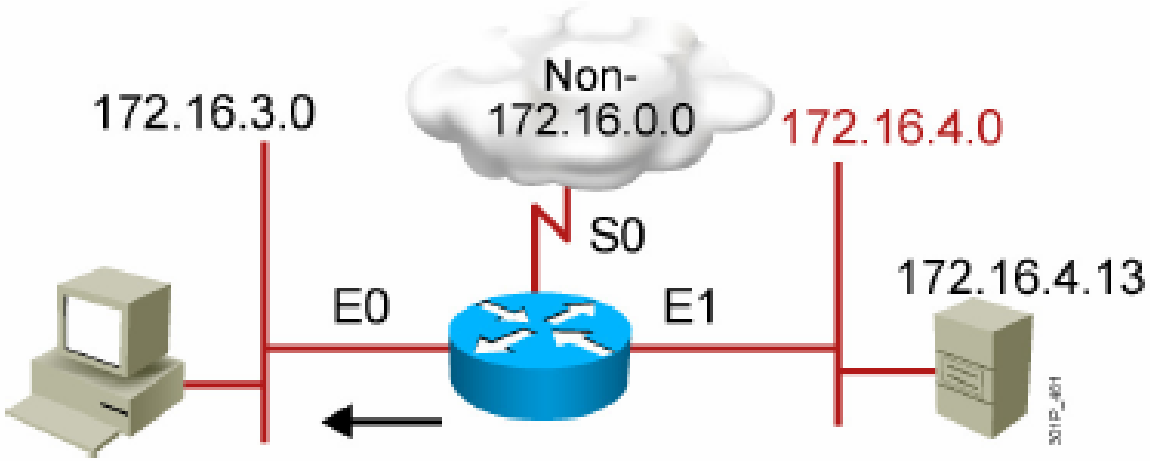
Tạo ACL cơ bản




```
RouterX(config)# access-list 1 deny 172.16.4.13 0.0.0.0
RouterX(config)# access-list 1 permit 0.0.0.0  255.255.255.255
(implicit deny all)
(access-list 1 deny 0.0.0.0   255.255.255.255)

RouterX(config)# interface ethernet 0
RouterX(config-if)# ip access-group 1 out
```

Cấm một host truy cập

Danh sách kiểm tra truy cập (ACL)
Tạo ACL cơ bản




```
RouterX(config)# access-list 1 deny 172.16.4.0  0.0.0.255
RouterX(config)# access-list 1 permit any
(implicit deny all)
(access-list 1 deny 0.0.0.0   255.255.255.255)

RouterX(config)# interface ethernet 0
RouterX(config-if)# ip access-group 1 out
```

Cấm một mạng con truy cập

Danh sách kiểm tra truy cập (ACL)
Tạo ACL cơ bản

```
RouterX(config-line)#
```

```
access-class access-list-number {in | out}
```

- Giới hạn kết nối vào và ra giữa cổng vty và địa chỉ trong ACL

Example:

```
access-list 12 permit 192.168.1.0 0.0.0.255
(implicit deny any)
!
line vty 0 4
 access-class 12 in
```

- Chỉ cho phép các host trong mạng 192.168.1.0 0.0.0.255 kết nối đến cổng vty của router

Danh sách kiểm tra truy cập (ACL)

Một số nguyên tắc cơ bản khi tạo ACL

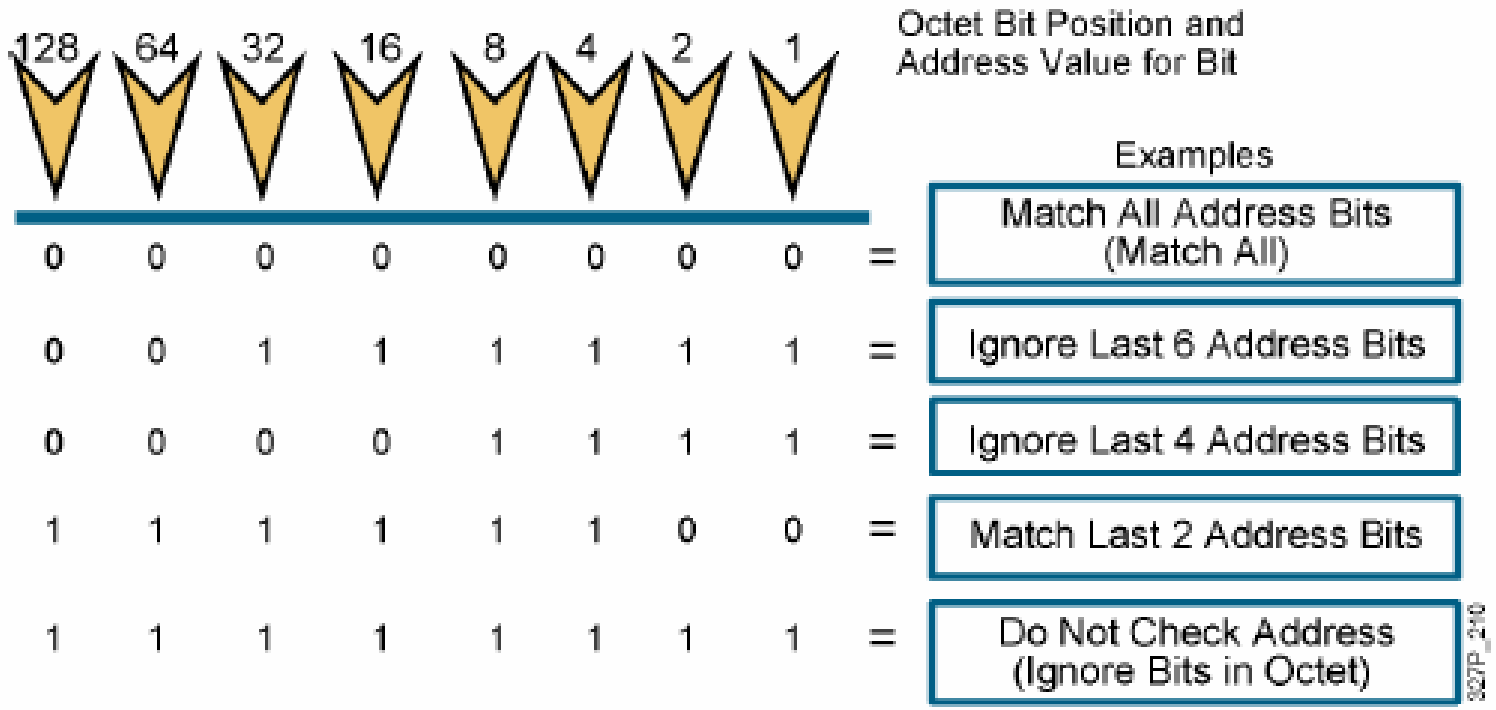
- Một ACL cho một giao thức trên một chiều của một cổng.
- ACL cơ bản nên đặt ở vị trí gần mạng đích nhất.
- ACL mở rộng nên đặt ở vị trí gần mạng nguồn nhất.
- Các câu lệnh trong một ACL sẽ được kiểm tra tuần tự từ trên xuống cho đến khi có một câu lệnh được thoả, nếu không thì gói dữ liệu đó cũng sẽ bị từ chối.

Danh sách kiểm tra truy cập (ACL)

Một số nguyên tắc cơ bản khi tạo ACL

- Có một câu lệnh từ chối tuyệt đối nằm ẩn ở cuối cùng trong ACL.
- Các câu lệnh trong ACL nên xếp từ chi tiết đến tổng quát.
- Trong một câu lệnh ACL, điều kiện được kiểm tra trước rồi mới kiểm tra tới việc cho phép hay từ chối.
- Nên sử dụng công cụ soạn thảo văn bản để soạn trước các câu lệnh ACL.
- Dòng lệnh mới luôn được thêm vào cuối danh sách ACL.
- Lệnh no access-list x sẽ xóa tòan bộ ACL x.

Danh sách kiểm tra truy cập (ACL)
Wildcard mask



- 0 nghĩa là kiểm tra sự phù hợp trong các bit địa chỉ tương ứng
- 1 nghĩa là lờ đi các bit địa chỉ tương ứng

Danh sách kiểm tra truy cập (ACL)
Wildcard mask

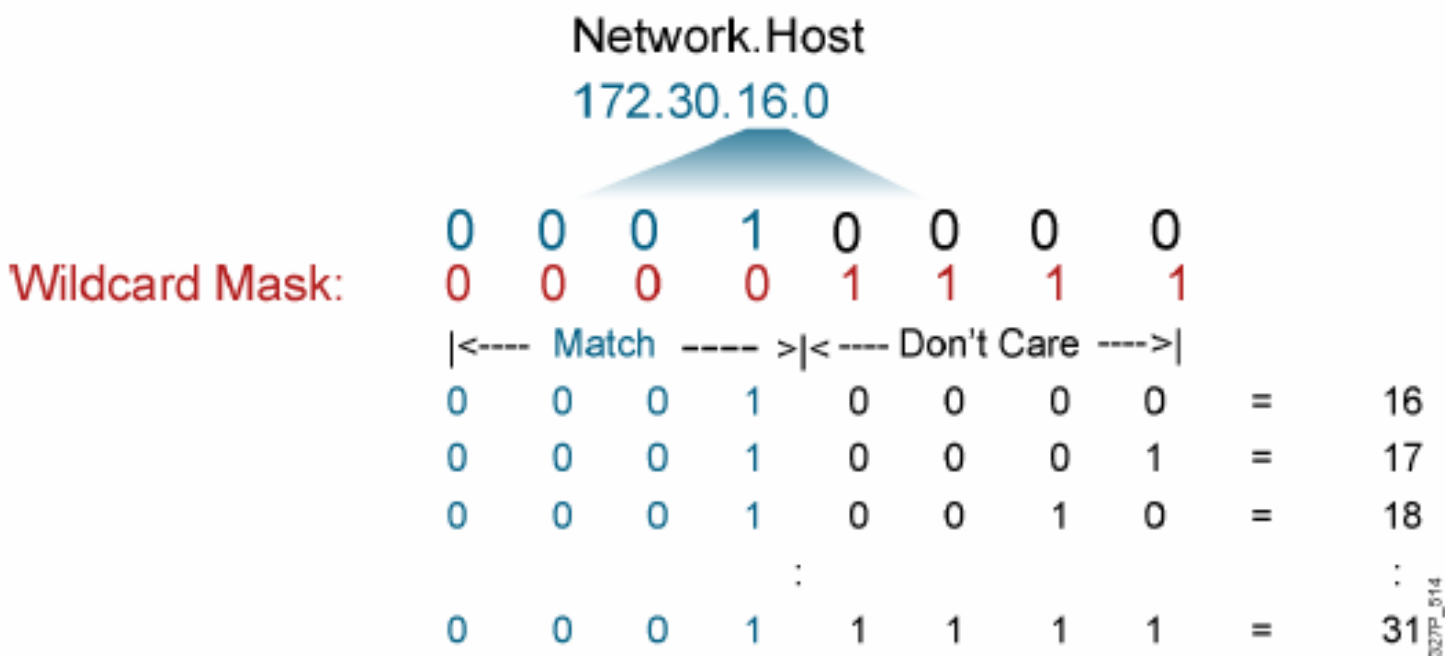
MASK (192.168.1.1)	Matching IP
0.0.0.0 (host)	192.168.1.1
0.0.0.255	192.168.1.0-255
0.0.255.255	192.168.0-255.0-255
0.255.255.255	192.0-255.0-255.0-255
255.255.255.255	0-255.0-255.0-255.0-255 (any)

Danh sách kiểm tra truy cập (ACL)
Wildcard mask

Kiểm tra sự phù hợp của các địa chỉ trong vùng từ 172.30.16.0/24 đến 172.30.31.0/24.

Địa chỉ và mặt nạ wildcard:

172.30.16.0 0.0.15.255



Danh sách kiểm tra truy cập (ACL)
Từ khóa Any và Host

Access-list 1 permit 0.0.0.0 255.255.255.255

hay

permit any

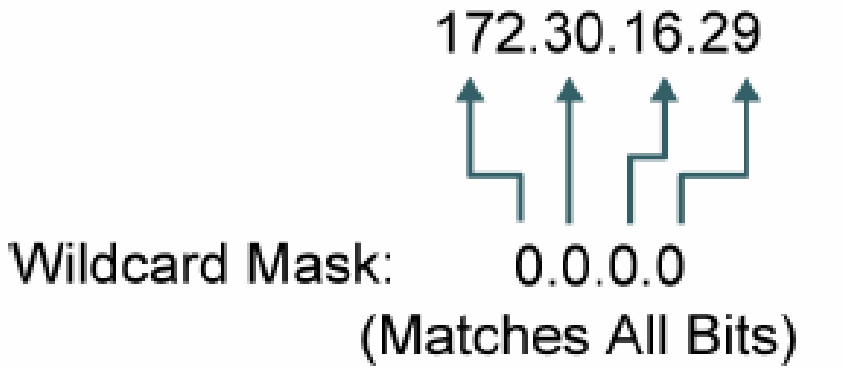
Access-list 1 permit 200.0.0.9 0.0.0.0

hay

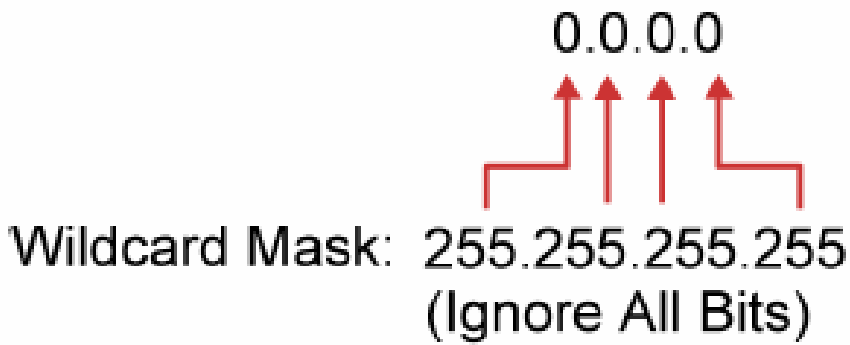
permit host 200.0.0.9

Danh sách kiểm tra truy cập (ACL)
Từ khóa Any và Host

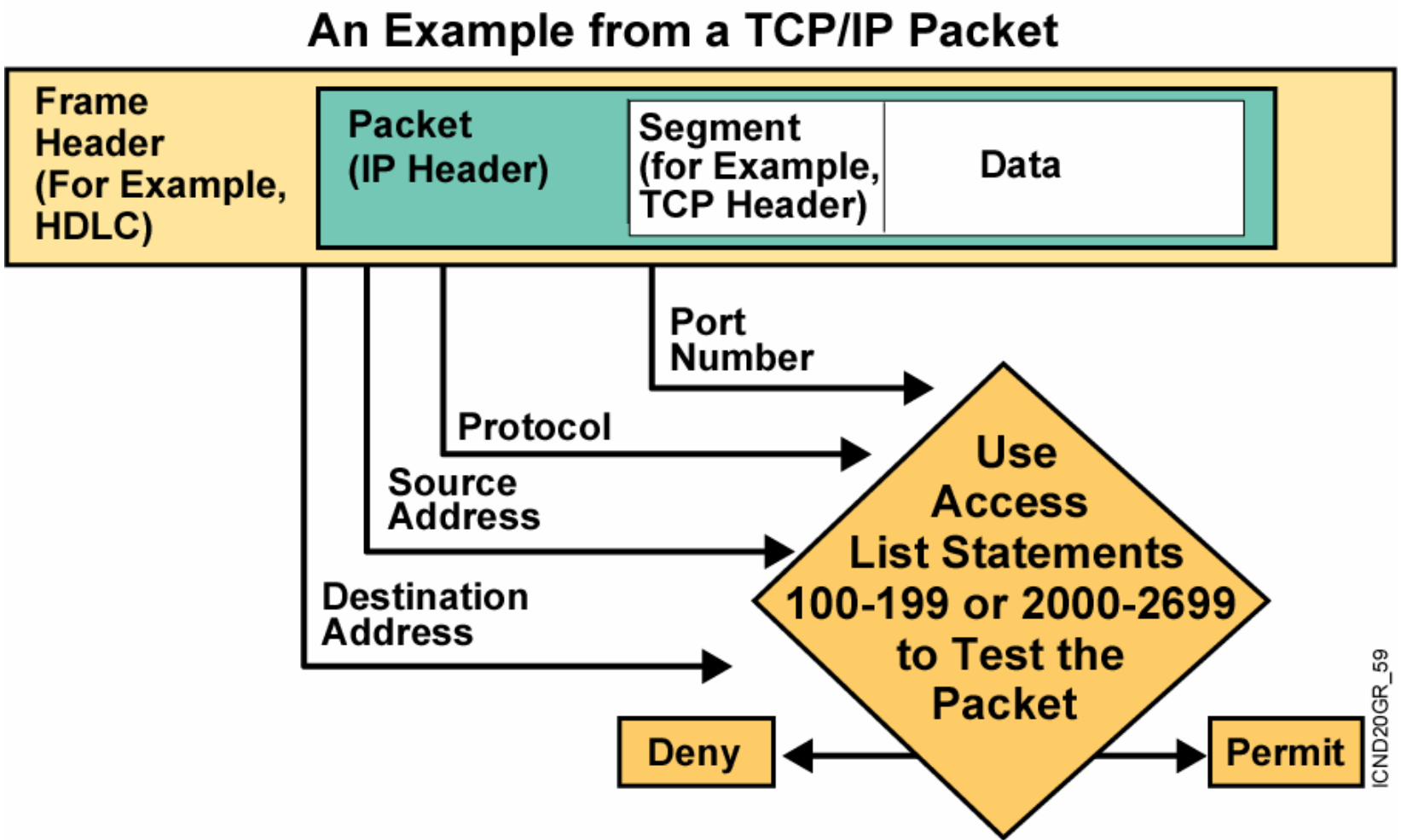
- 172.30.16.29 0.0.0.0 kiểm tra sự phù hợp của tất cả các bit địa chỉ
- Tóm tắt mặt nạ wildcard này bằng cách sử dụng từ khóa **host** (host 172.30.16.29)



- 0.0.0.0 255.255.255.255 lờ đi tất cả các bit địa chỉ
- Biểu diễn vắn tắt bằng từ khóa **any**



Danh sách kiểm tra truy cập (ACL)
Tạo ACL mở rộng



Danh sách kiểm tra truy cập (ACL)
Tạo ACL mở rộng

```
RouterX(config)#
access-list access-list-number {permit | deny}
protocol source source-wildcard [operator port]
destination destination-wildcard [operator port]
[established] [log]
```

- Thiết lập các thông số cho dòng khai báo này

```
RouterX(config-if)#
ip access-group access-list-number  {in | out}
```

- Kích hoạt ACL mở rộng trên cổng kết nối

Danh sách kiểm tra truy cập (ACL)
Tạo ACL mở rộng

```
RouterX(config)#
access-list access-list-number {permit | deny}
protocol source source-wildcard [operator port]
destination destination-wildcard [operator port]
[established] [log]
```

- Thiết lập các thông số cho dòng khai báo này

```
RouterX(config-if)#
ip access-group access-list-number  {in | out}
```

- Kích hoạt ACL mở rộng trên cổng kết nối

Danh sách kiểm tra truy cập (ACL)
Tạo ACL mở rộng

Access-list-number : Chỉ ra danh sách kiểm tra có số nằm trong khoảng từ 100 đến 199 hoặc từ 2000 đến 2699

Permit | deny : Chỉ ra dòng khai báo này cho phép hay từ chối gói tin

Protocol : IP,TCP,UDP,ICMP, GRE hoặc IGRP

Source and destination: Chỉ ra địa chỉ ip nguồn và đích

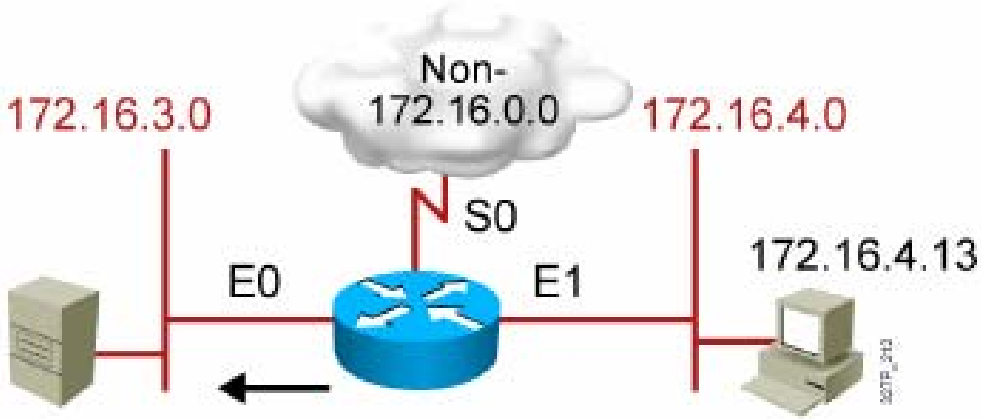
Source-wildcard and destination-wildcard : Mặt nạ wildcard ; 0 chỉ ra phần địa chỉ phải kiểm tra sự phù hợp , 1 chỉ ra phần không cần phải kiểm tra

Operator [port | app-name] : thông số này có thể là Lt (nhỏ hơn) , gt (lớn hơn) và eq (bằng) , neq (không bằng) . Số cổng ứng dụng có thể là nguồn hoặc đích , tùy thuộc vào vị trí cấu hình trong ACL . Để thay thế cho số port ứng dụng , có thể sử dụng tên cho các ứng dụng quen thuộc như là Telnet , FTP , SMTP , vv

Established : Chỉ sử dụng cho giao thức TCP theo chiều vào . Cho phép các gói tin TCP đi qua khi gói tin này là gói trả lời phiên làm việc khởi tạo từ bên ngoài . Loại gói tin này có bit ACK (xem phần ví dụ extended ACL với từ khóa Established)

Log : lưu lại nhật kí lên màn hình console

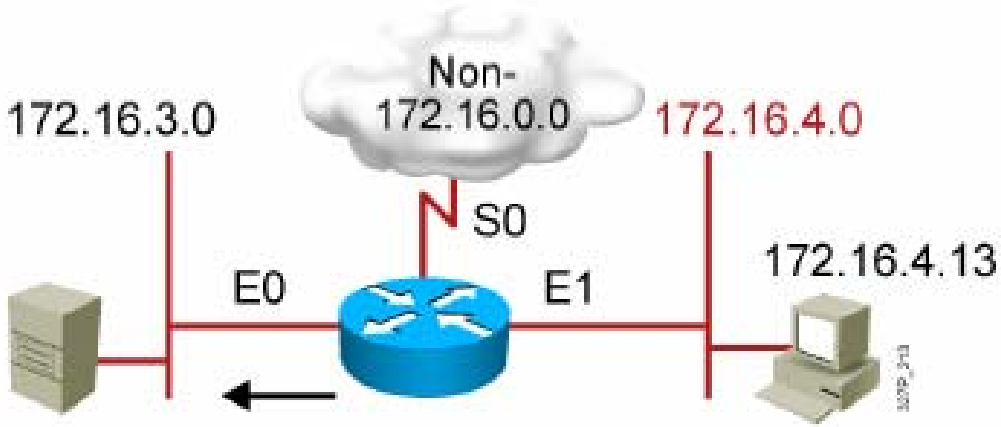
Danh sách kiểm tra truy cập (ACL)
Tạo ACL mở rộng




```
RouterX(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
RouterX(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20
RouterX(config)# access-list 101 permit ip any any
(implicit deny all)
(access-list 101 deny ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255)

RouterX(config)# interface ethernet 0
RouterX(config-if)# ip access-group 101 out
```

- Cấm dữ liệu FTP đi từ mạng 172.16.4.0 qua 172.16.3.0 ra khỏi E0
- Cho phép tất cả dữ liệu còn lại

Danh sách kiểm tra truy cập (ACL)
Tạo ACL mở rộng

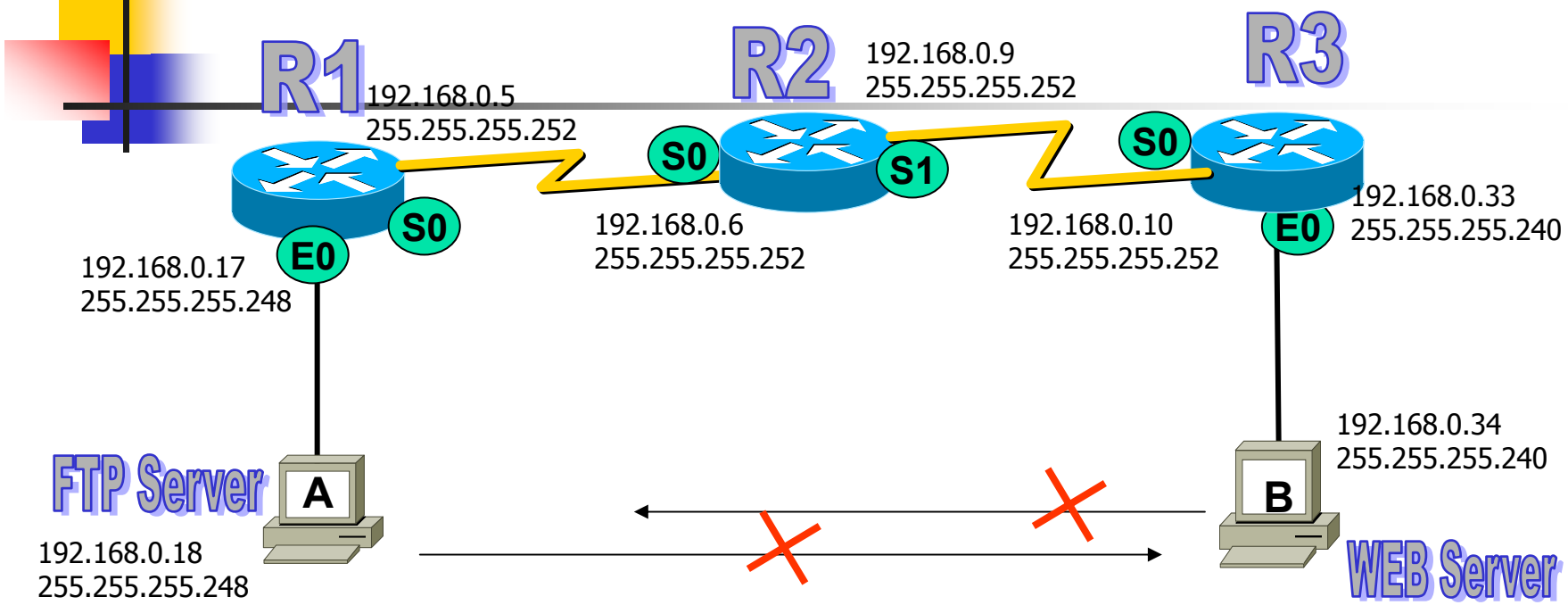



```
RouterX(config)# access-list 101 deny tcp 172.16.4.0  0.0.0.255  any eq 23
RouterX(config)# access-list 101 permit ip any any
(implicit deny all)

RouterX(config)# interface ethernet 0
RouterX(config-if)# ip access-group 101 out
```

- Cấm dữ liệu telnet từ mạng 172.16.4.0 ra E0
- Cho phép tất cả các dữ liệu còn lại

Danh sách kiểm tra truy cập (ACL)

Tạo ACL mở rộng



192.168.0.34 should be denied FTP of 192.168.0.18

On Router R1

Config# Access-list 100 deny tcp 192.168.0.34 0.0.0.0
192.168.0.18 0.0.0.0 eq 21

Config# access-list 100 permit IP any any

Config#int s0

Config-if# ip access-group 100 IN

192.168.0.18 should be denied website of 192.168.0.34

On Router R3

Config# Access-list 100 deny tcp 192.168. 0.18 0.0.0.0 192.168.0.34
0.0.0.0 eq 80

Config# access-list 100 permit IP any any

Config#int s0

Config-if# ip access-group 100 IN

Danh sách kiểm tra truy cập (ACL)
Tạo ACL đặt tên

```
RouterX(config)#
```

```
ip access-list {standard | extended} name
```

- Chuỗi kí tự tên gọi phải là duy nhất

```
RouterX(config {std- | ext-}nacl)#
```

```
[sequence-number] {permit | deny} {ip access list test conditions}
{permit | deny} {ip access list test conditions}
```

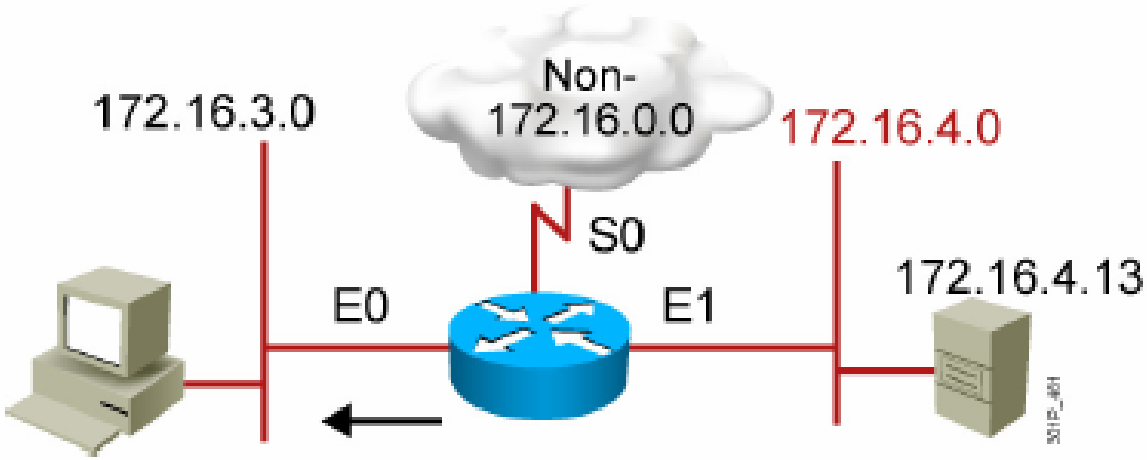
- Nếu như không cấu hình , số thứ tự được tạo ra tự động , bắt đầu từ 10 và tăng dần thêm 10
- **no** *sequence number* gỡ bỏ một khai báo trong ACL dạng tên

```
RouterX(config-if)#
```

```
ip access-group name {in | out}
```

- Kích hoạt ACL dạng tên trên cổng kết nối

Danh sách kiểm tra truy cập (ACL)
Tạo ACL đặt tên

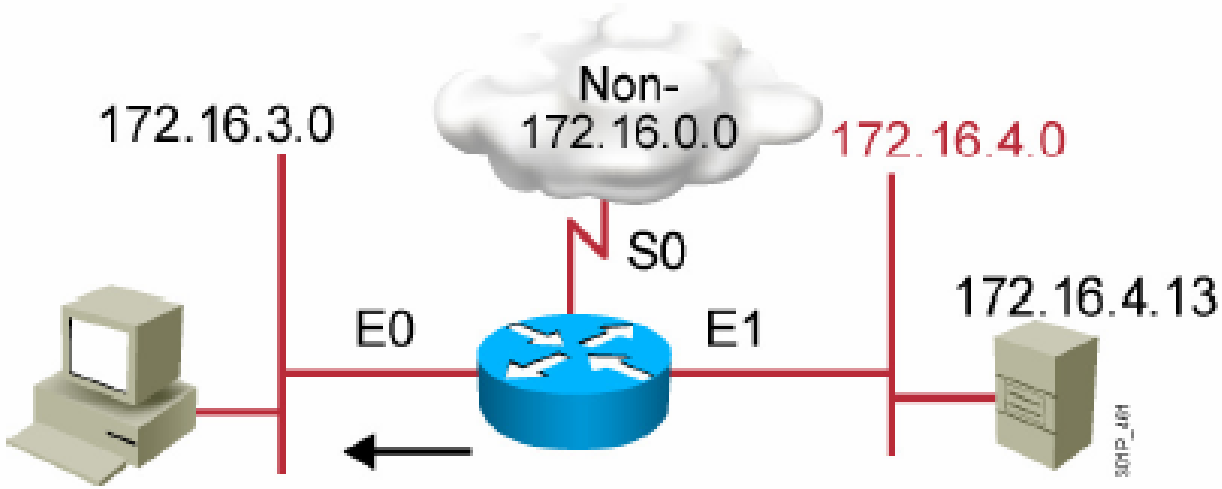



```
RouterX(config)#ip access-list standard troublemaker
RouterX(config-std-nacl)#deny host 172.16.4.13
RouterX(config-std-nacl)#permit 172.16.4.0 0.0.0.255
RouterX(config-std-nacl)#interface e0
RouterX(config-if)#ip access-group troublemaker out
```

Cấm một host truy cập

Danh sách kiểm tra truy cập (ACL)

Tạo ACL đặt tên




```
RouterX(config)#ip access-list extended badgroup
RouterX(config-ext-nacl)#deny tcp 172.16.4.0 0.0.0.255 any eq 23
RouterX(config-ext-nacl)#permit ip any any
RouterX(config-ext-nacl)#interface e0
RouterX(config-if)#ip access-group badgroup out
```

Cấm telnet từ một mạng con

Danh sách kiểm tra truy cập (ACL)
Kiểm tra ACL

```
RouterX# show access-lists {access-list number/name}
```

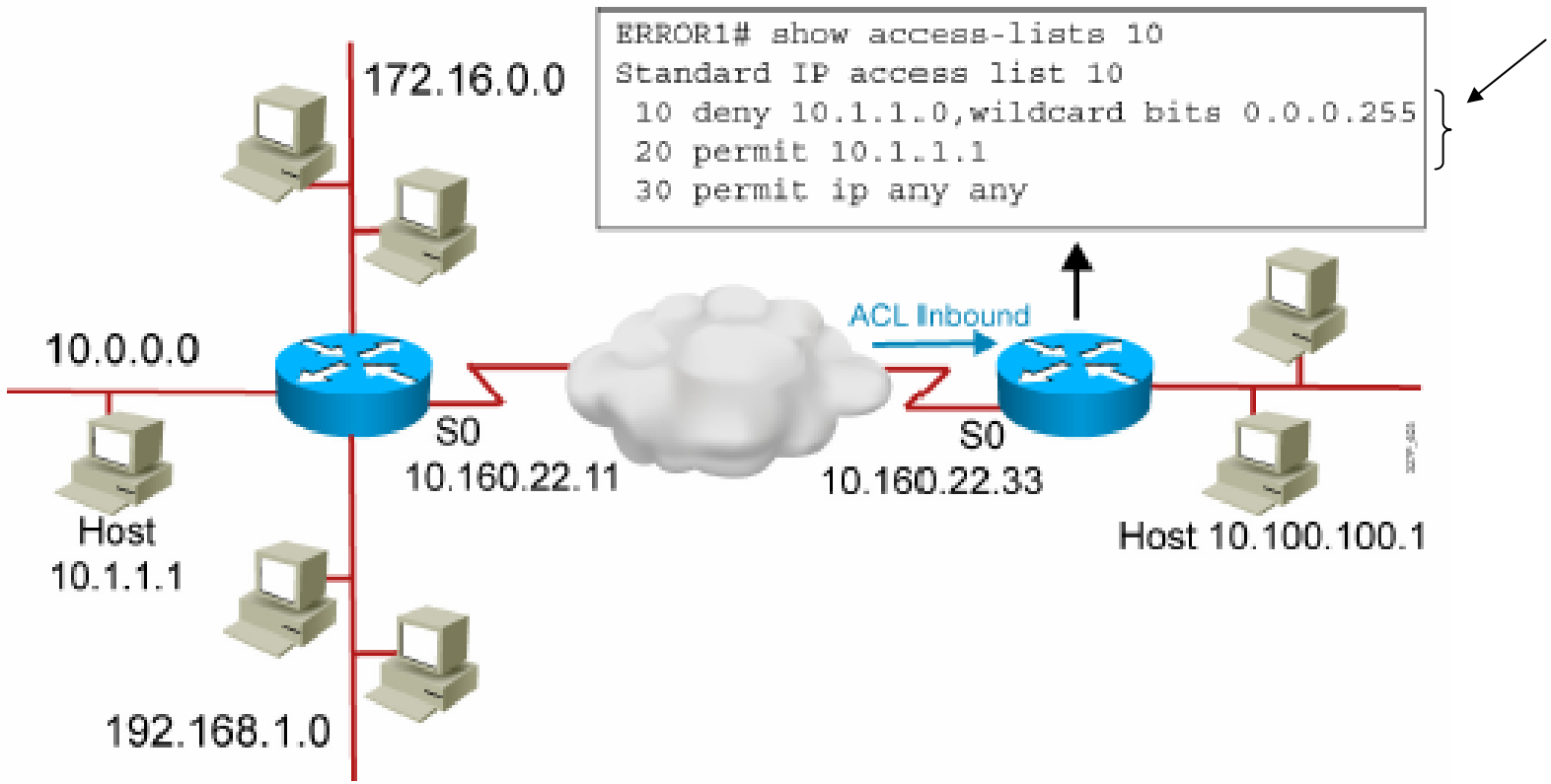
```
RouterX# show access-lists
Standard IP access list SALES
    10 deny   10.1.1.0, wildcard bits 0.0.0.255
    20 permit 10.3.3.1
    30 permit 10.4.4.1
    40 permit 10.5.5.1
Extended IP access list ENG
    10 permit tcp host 10.22.22.1 any eq telnet (25 matches)
    20 permit tcp host 10.33.33.1 any eq ftp
    30 permit tcp host 10.44.44.1 any eq ftp-data
```

Hiển thị tất cả ACL

Danh sách kiểm tra truy cập (ACL)
Kiểm tra ACL

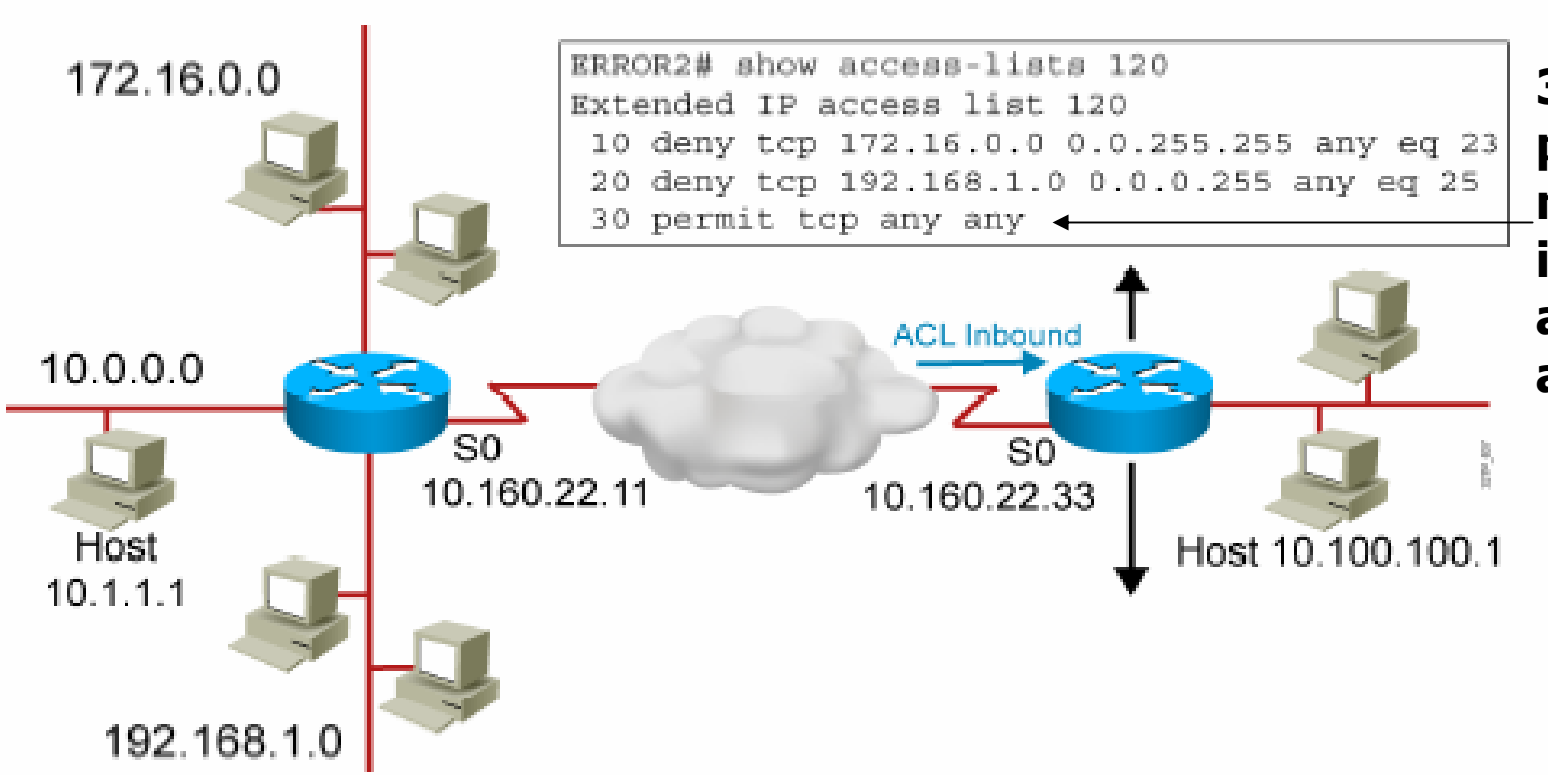
```
RouterX# show ip interfaces e0
Ethernet0 is up, line protocol is up
  Internet address is 10.1.1.11/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is 1
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Feature Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  <text ommitted>
```

Danh sách kiểm tra truy cập (ACL)
Xử lý sự cố ACL



Sự cố 1: Host 10.1.1.1 không kết nối được với 10.100.100.1.

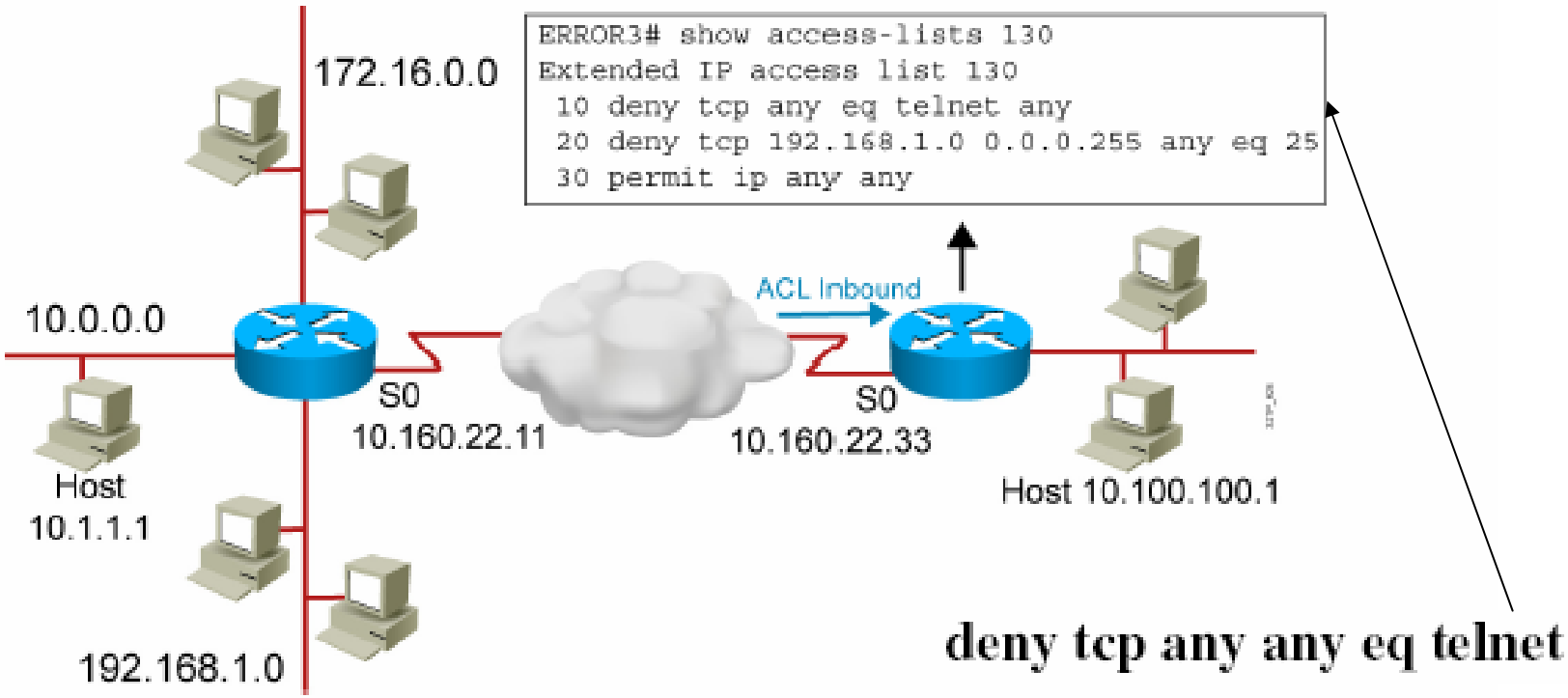
Danh sách kiểm tra truy cập (ACL)
Xử lý sự cố ACL



Sự cố 2: Mạng 192.168.1.0 không thể sử dụng TFTP để kết nối đến 10.100.100.1.

UDP

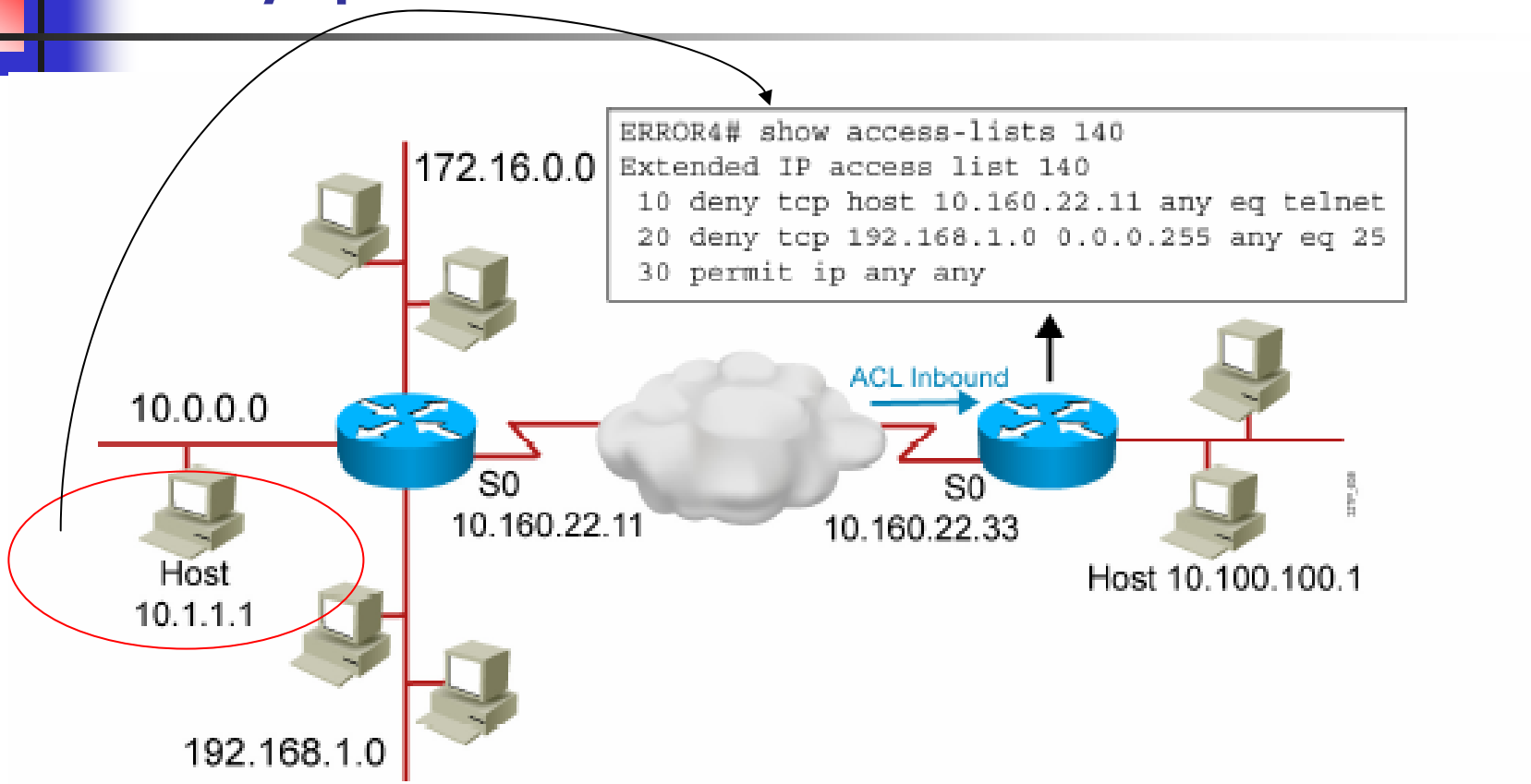
Danh sách kiểm tra truy cập (ACL)
Xử lý sự cố ACL



Sự cố 3: Mạng 172.16.0.0 vẫn telnet được đến 10.100.100.1, nhưng kết nối này không được phép

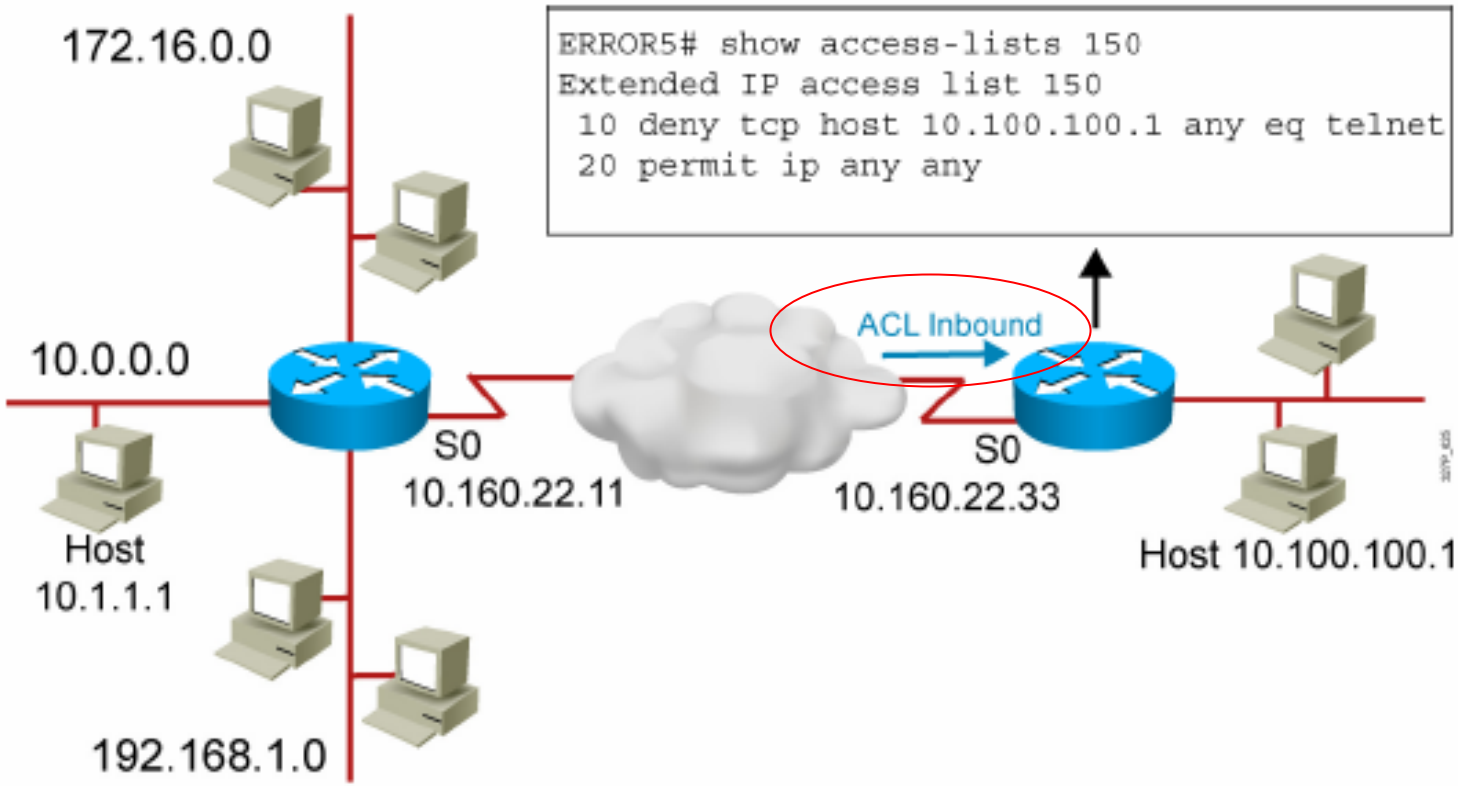
Danh sách kiểm tra truy cập (ACL)

Xử lý sự cố ACL



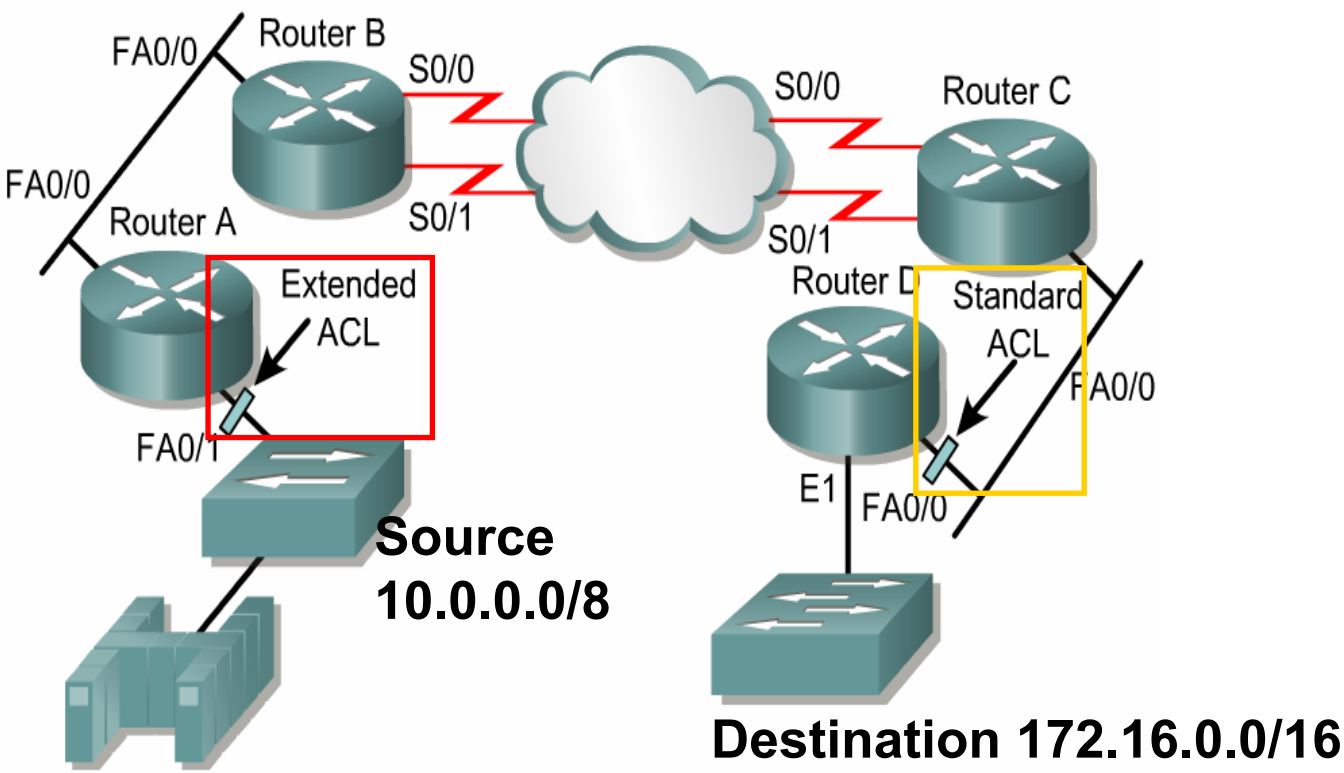
Sự cố 4: Host 10.1.1.1 vẫn telnet được đến 10.100.100.1, nhưng kết nối này không được phép

Danh sách kiểm tra truy cập (ACL)
Xử lý sự cố ACL

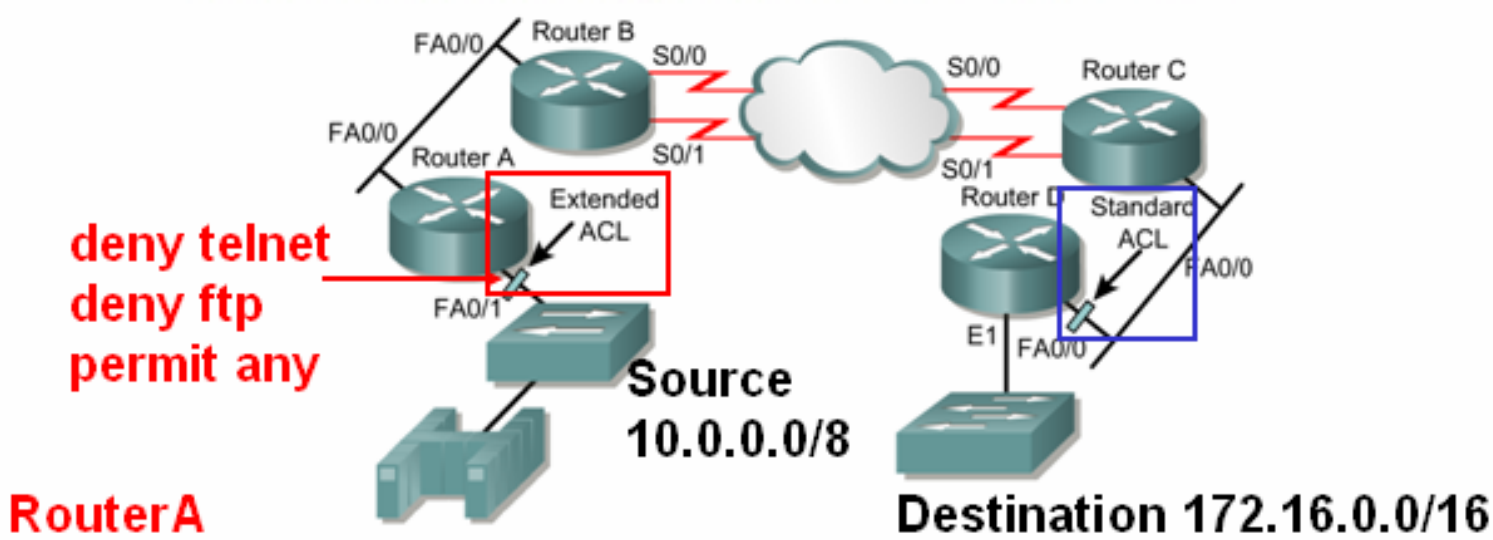


Sự cố 5: Host 10.100.100.1 vẫn telnet được đến 10.1.1.1, nhưng kết nối này không được phép

Danh sách kiểm tra truy cập (ACL)
Vị trí đặt ACL

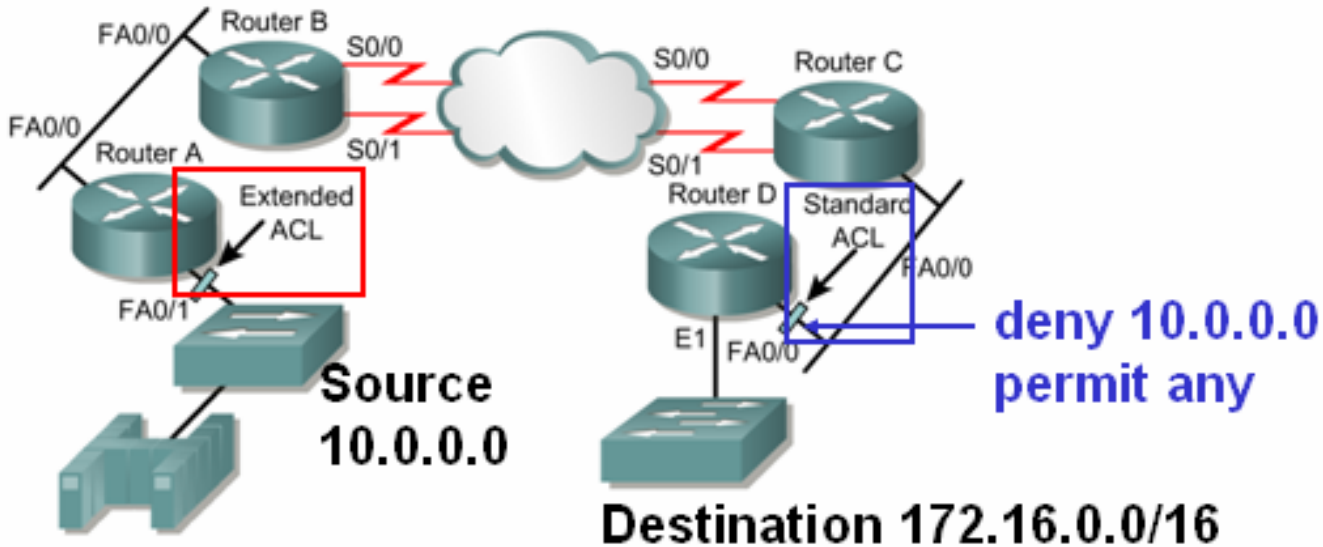


Danh sách kiểm tra truy cập (ACL)
Vị trí đặt ACL




```
interface fastethernet 0/1
    access-group 101 in
access-list 101 deny tcp any 172.16.0.0 0.0.255.255 eq telnet
access-list 101 deny tcp any 172.16.0.0 0.0.255.255 eq ftp
access-list 101 permit ip any any
```

Danh sách kiểm tra truy cập (ACL)
Vị trí đặt ACL



RouterD

```
interface fastethernet 0/0
    access-group 10 in
access-list 10 deny 10.0.0.0 0.255.255.255
access-list 10 permit any
```

NAT
Network Address Translation

- Khái niệm về NAT
- Static NAT
- Dynamic NAT
- PAT (Port Address Translation)

NAT
Khái niệm về NAT

- Được thiết kế để tiết kiệm địa chỉ IP.
- Cho phép mạng nội bộ sử dụng địa chỉ IP riêng.
- Địa chỉ IP riêng sẽ được chuyển đổi sang địa chỉ công cộng định tuyến được.
- Mạng riêng được tách biệt và giấu kín IP nội bộ.
- Thường sử dụng trên router biên của mạng một cửa.

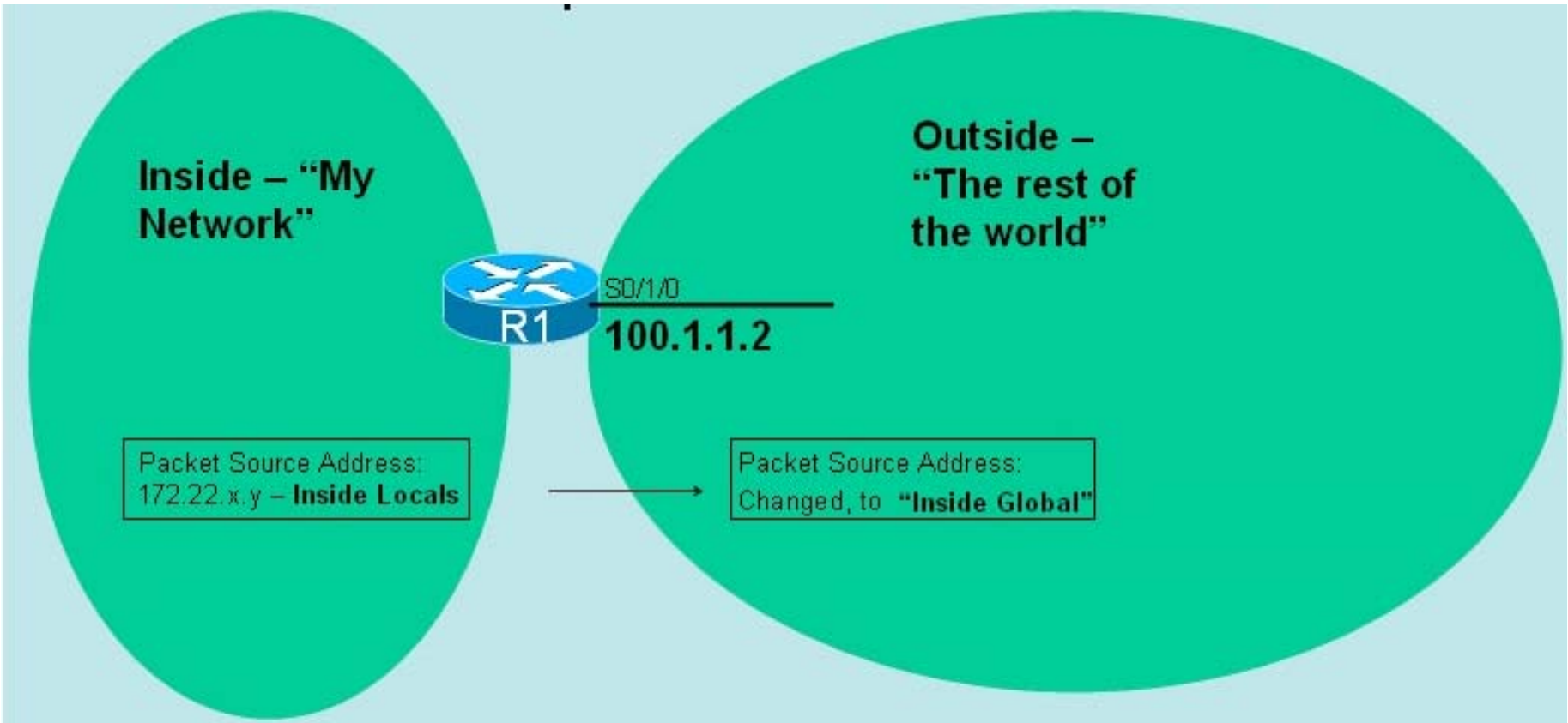
NAT
Khái niệm về NAT

- Địa chỉ cục bộ bên trong (Inside local address): Địa chỉ được phân phối cho các host bên trong mạng nội bộ.
- Địa chỉ toàn cục bên trong (Inside global address): Địa chỉ hợp pháp được cung cấp bởi InterNIC (Internet Network Information Center) hoặc nhà cung cấp dịch vụ Internet, đại diện cho một hoặc nhiều địa chỉ nội bộ bên trong đối với thế giới bên ngoài.

NAT
Khái niệm về NAT

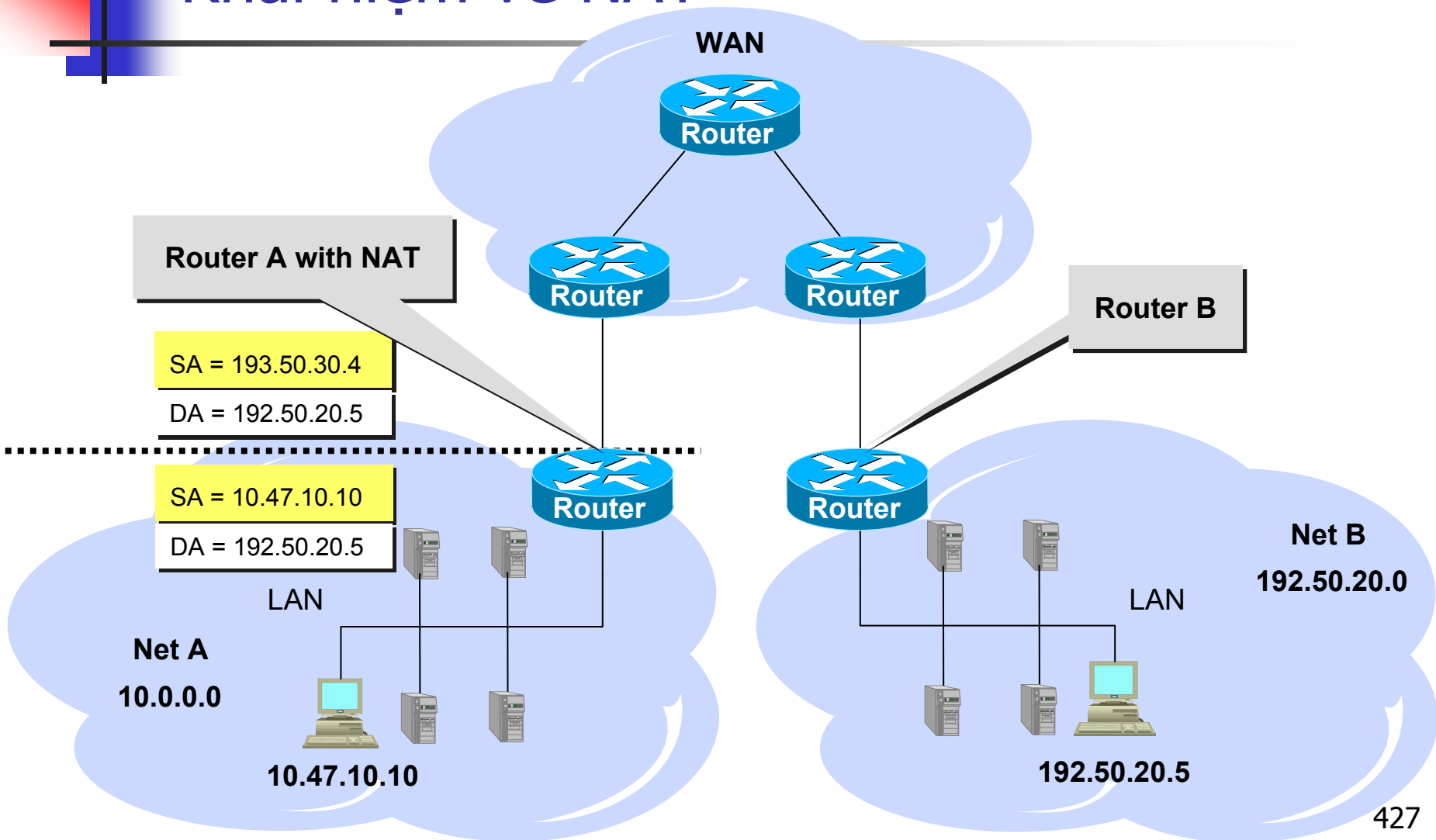
- Địa chỉ cục bộ bên ngoài (Outside local address): Địa chỉ riêng của host nằm bên ngoài mạng nội bộ.
- Địa chỉ toàn cục bên ngoài (Outside global address): Địa chỉ công cộng hợp pháp của host nằm bên ngoài mạng nội bộ.

NAT
Khái niệm về NAT



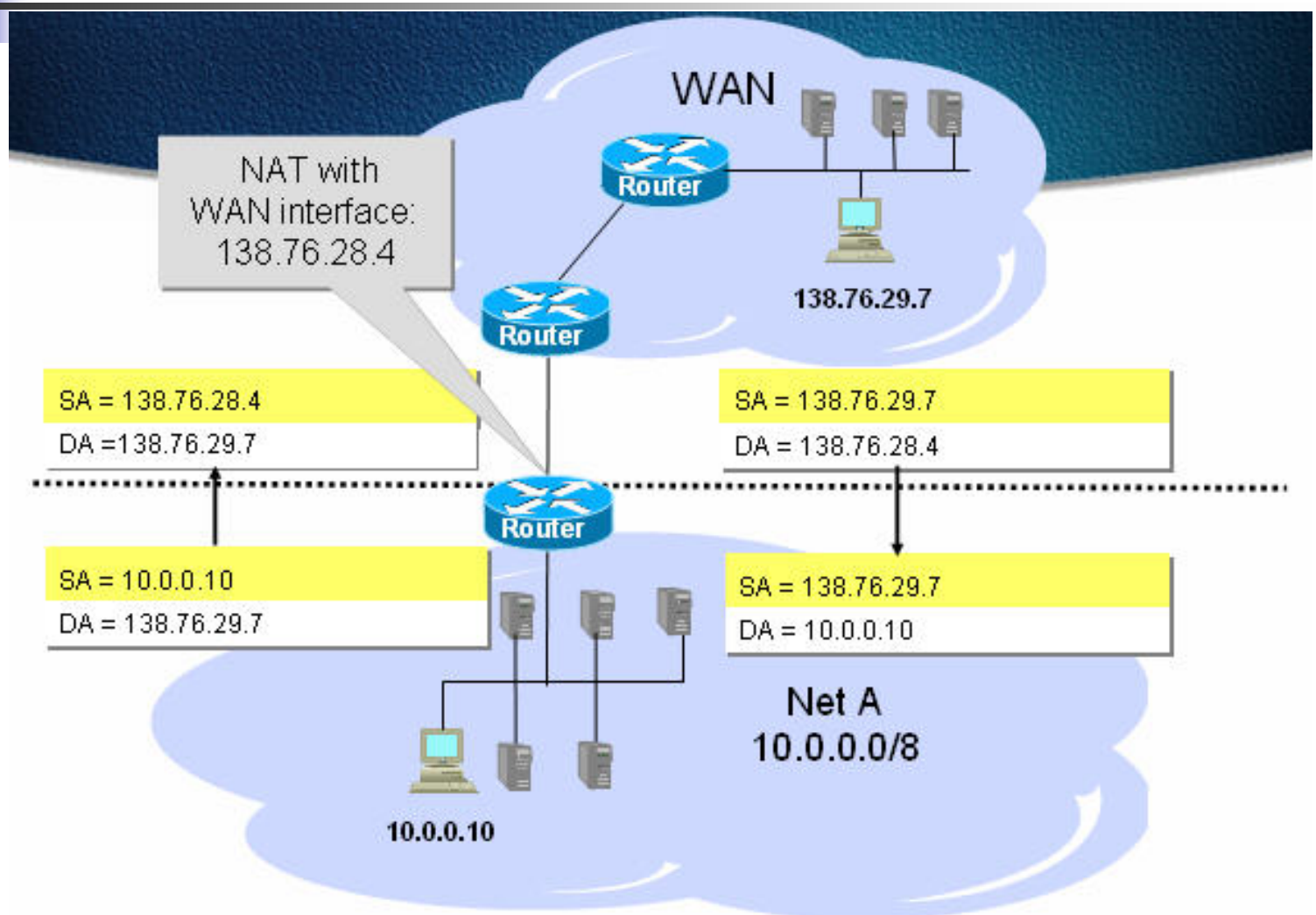
NAT

Khái niệm về NAT

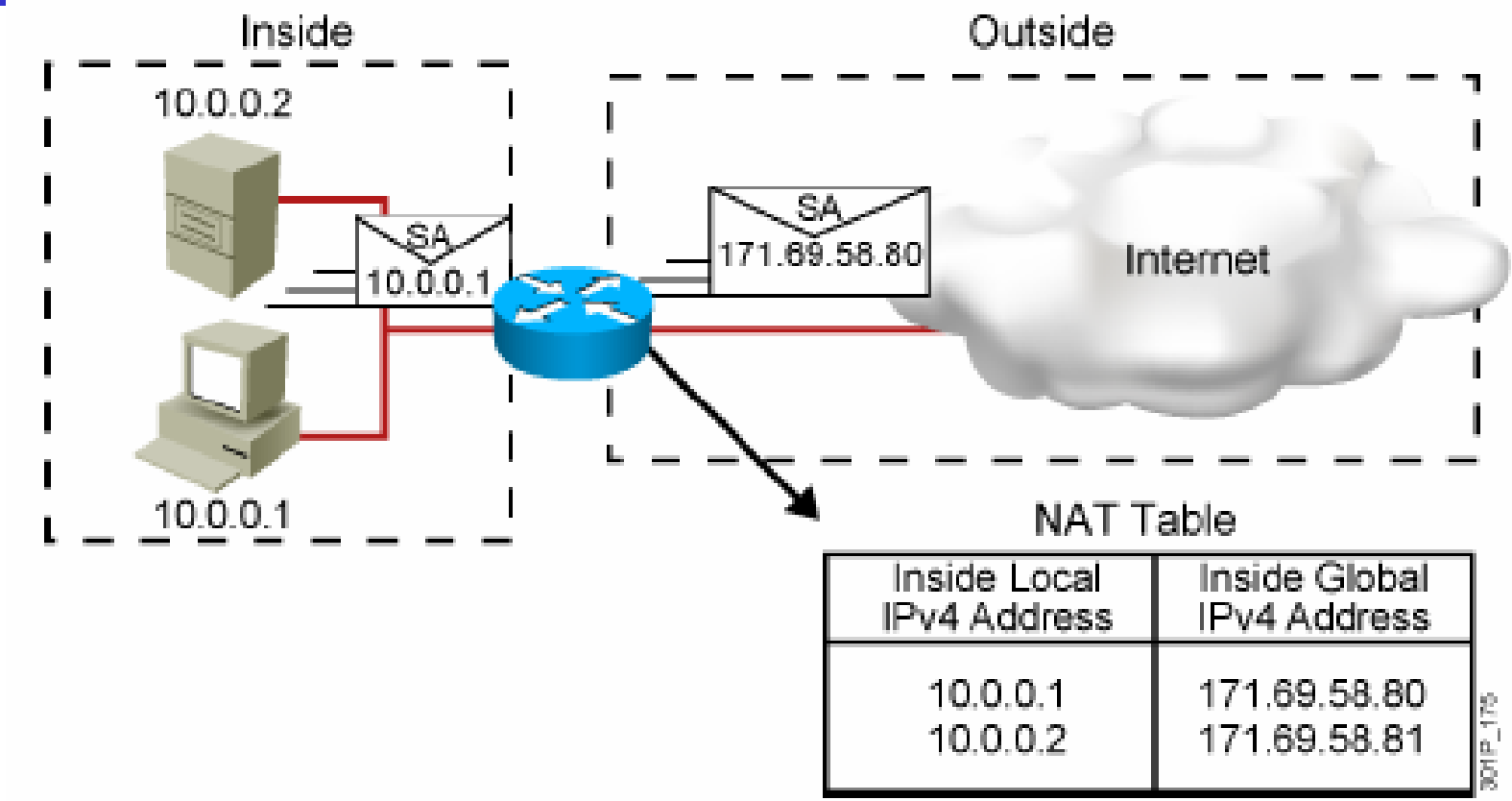


NAT

Khái niệm về NAT



NAT
Static NAT



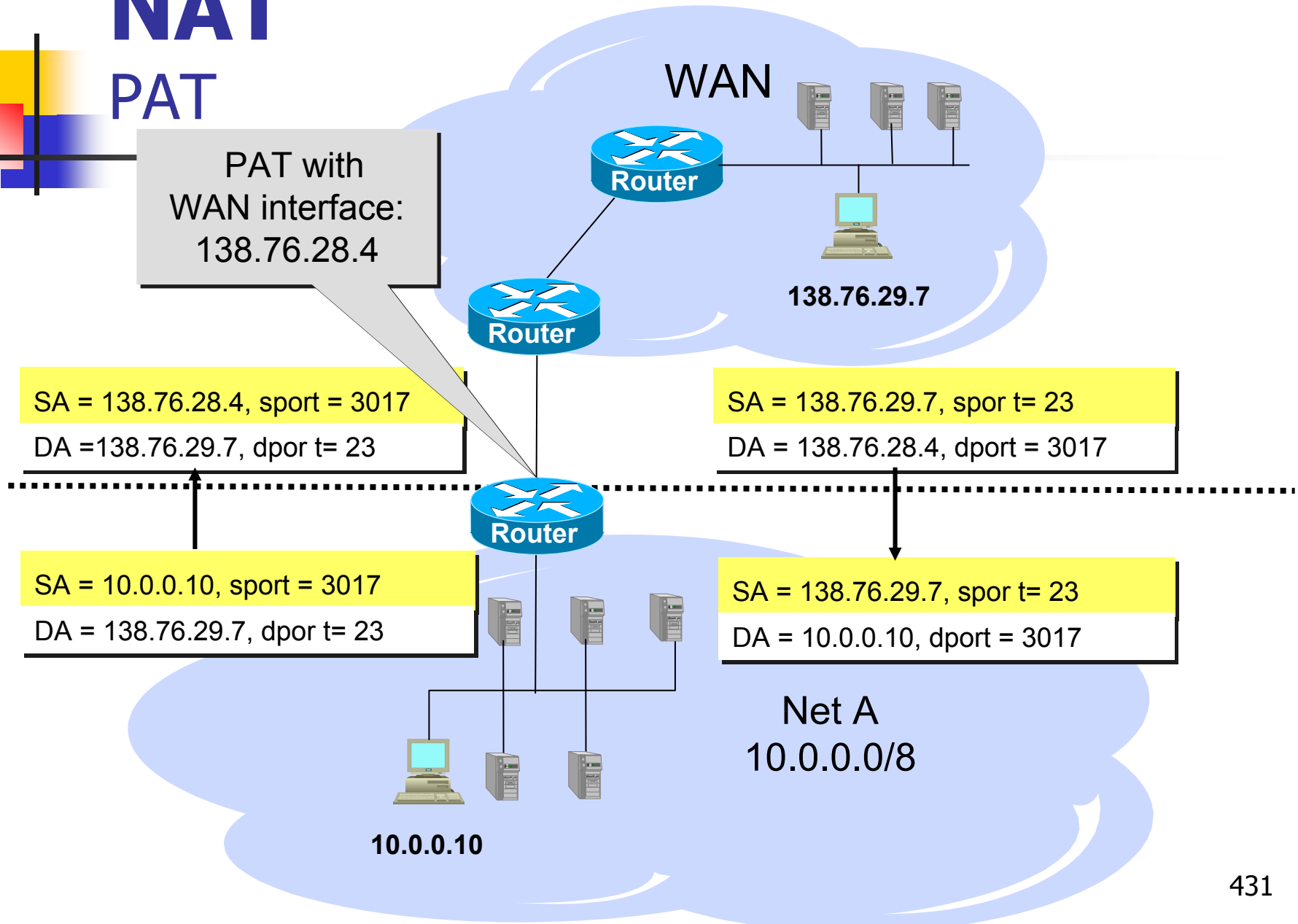
Ánh xạ một – một

NAT
Dynamic NAT và PAT

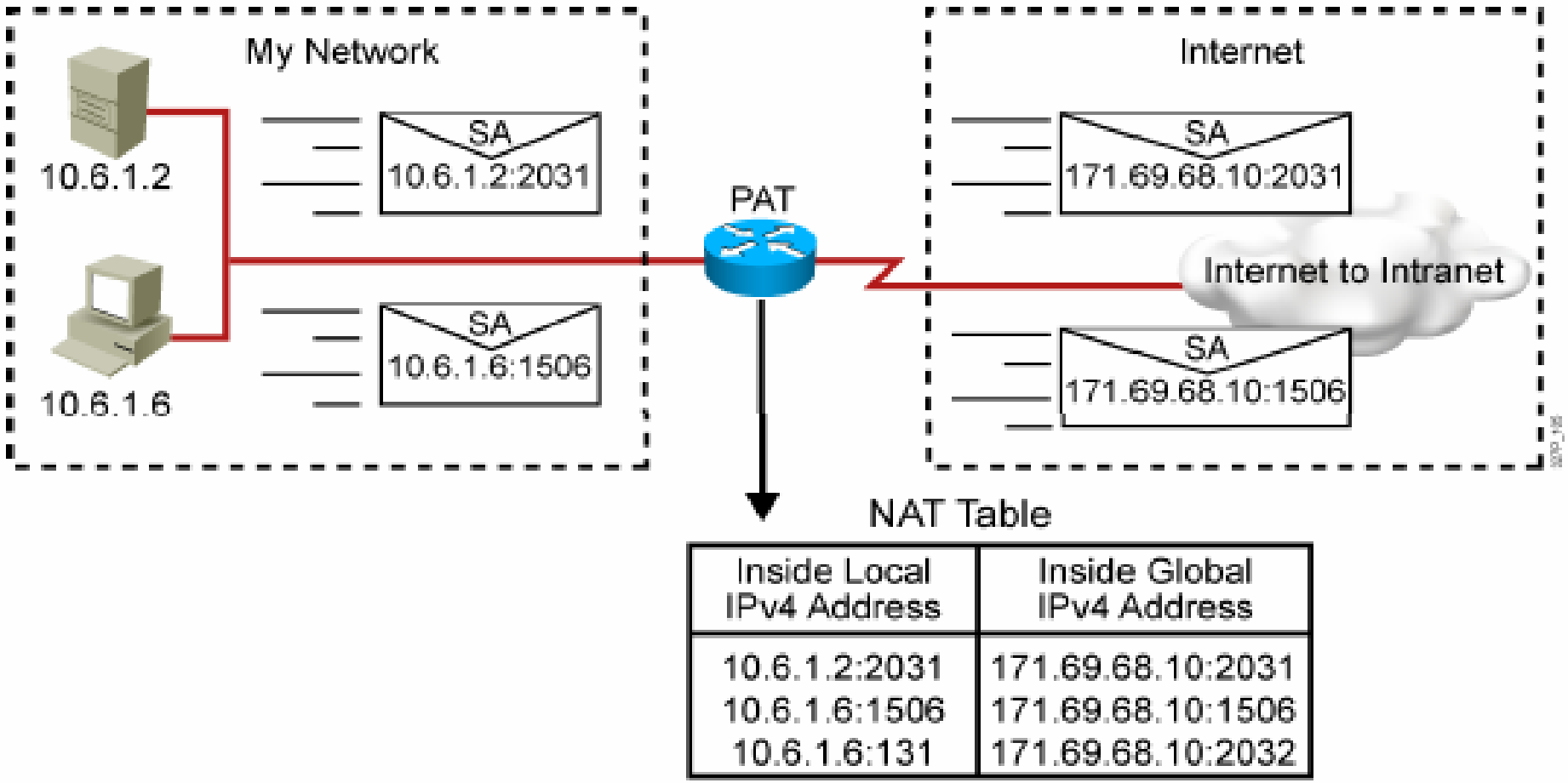
- NAT động được thiết kế để ánh xạ một địa chỉ IP riêng sang một địa chỉ công cộng một cách tự động. Bất kỳ địa chỉ IP nào nằm trong dải địa chỉ IP công cộng đã được định trước đều có thể được gán cho một host bên trong mạng.
- Overloading hoặc PAT (Port Address Translation) có thể ánh xạ nhiều địa chỉ IP sang một địa chỉ IP công cộng, mỗi địa chỉ riêng được phân biệt bằng số port.

NAT

PAT


PAT with
WAN interface:
138.76.28.4
WAN
Router
Router
138.76.29.7
SA = 138.76.28.4, sport = 3017
DA =138.76.29.7, dpor t= 23
SA = 138.76.29.7, spor t= 23
DA = 138.76.28.4, dport = 3017
Router
SA = 10.0.0.10, sport = 3017
DA = 138.76.29.7, dpor t= 23
SA = 138.76.29.7, spor t= 23
DA = 10.0.0.10, dport = 3017
Net A
10.0.0.0/8
10.0.0.10

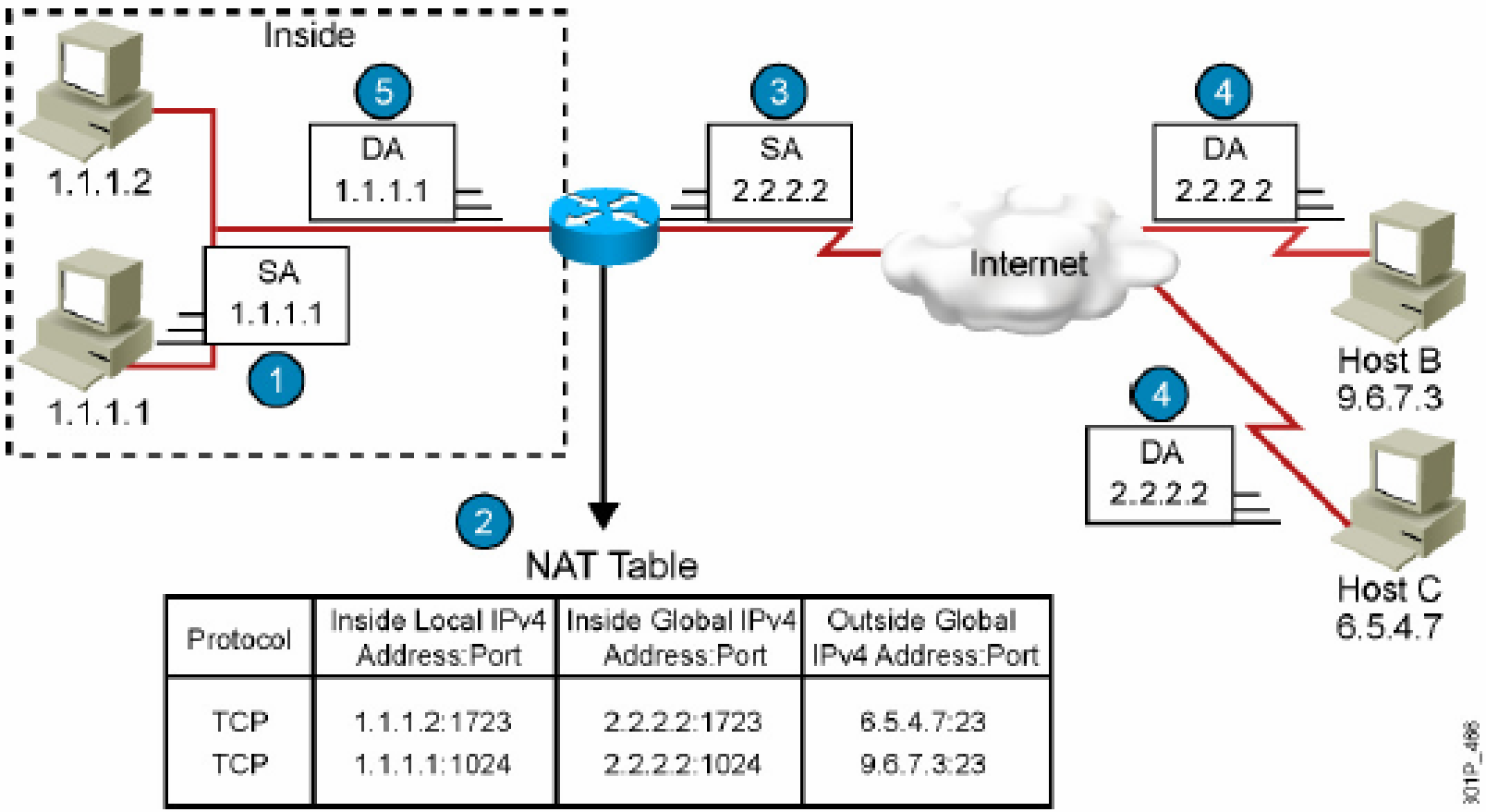
NAT
PAT



NAT Table

Inside Local IPv4 Address	Inside Global IPv4 Address
10.6.1.2:2031	171.69.68.10:2031
10.6.1.6:1506	171.69.68.10:1506
10.6.1.6:131	171.69.68.10:2032

NAT
PAT



Protocol	Inside Local IPv4 Address:Port	Inside Global IPv4 Address:Port	Outside Global IPv4 Address:Port
TCP	1.1.1.2:1723	2.2.2.2:1723	6.5.4.7:23
TCP	1.1.1.1:1024	2.2.2.2:1024	9.6.7.3:23

NAT
Cấu hình Static NAT

- **Tạo mối quan hệ chuyển đổi giữa địa chỉ local và global**

```
Router(config)#ip nat inside source static [local-ip]
[global-ip]
```

- **Xác định cổng kết nối vào mạng bên trong**

```
Router(config)#interface [type number]
```

- **Đánh dấu cổng này là cổng kết nối vào mạng bên trong**

```
Router(config-if)#ip nat inside
```

- **Xác định cổng kết nối ra mạng bên ngoài**

```
Router(config-if)#exit
Router(config)#interface [type number]
```

- **Đánh dấu cổng này là cổng kết nối ra mạng bên ngoài**

```
Router(config-if)#ip nat outside
```

NAT
Cấu hình Static NAT

- **Ví dụ:**

```
Hostname GW

Ip nat inside source static  10.1.1.2  179.9.8.80

Interface ethernet 0
Ip address  10.1.1.1  255.0.0.0
Ip nat inside

Interface serial 0
Ip address  179.9.8.80  255.255.0.0
Ip nat outside
```

NAT
Cấu hình Dynamic NAT

- **Xác định dải địa chỉ đại diện bên ngoài**

```
Router(config)#ip nat pool [name] [start-ip] [end-ip]
netmask [netmask]
```

- **Tạo ACL cơ bản để xác định dải địa chỉ bên trong**

```
Router(config)#access list [acl-number] permit source
[source-wildcard]
```

- **Xác định quan hệ giữa địa chỉ nguồn và dải địa chỉ ngoài**

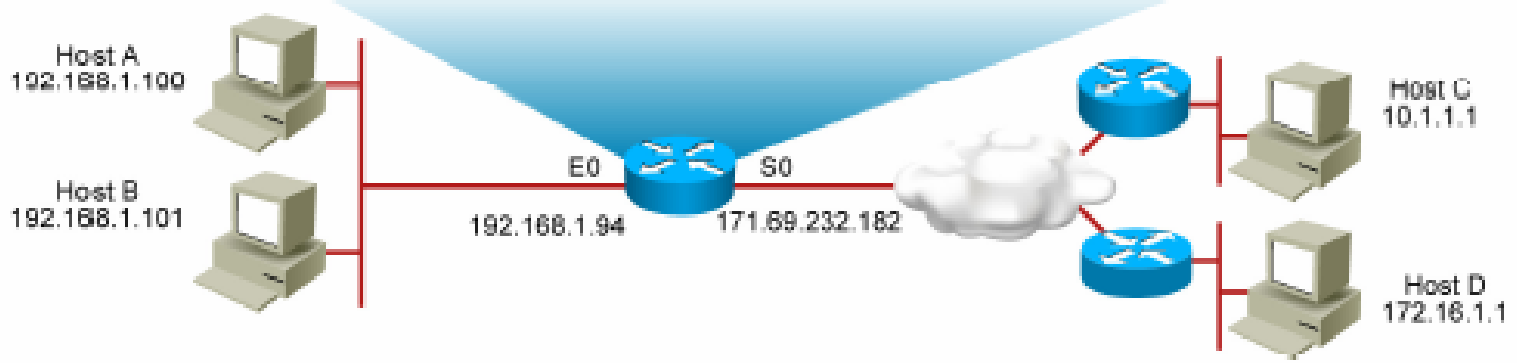
```
Router(config)#ip nat inside source list [acl-number] pool
[name]
```

- **Xác định cổng kết nối với mạng nội bộ và mạng ngoài**

```
Router(config)#interface [type number]
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface [type number]
Router(config-if)#ip nat outside
```

NAT
Cấu hình Dynamic NAT

```
ip nat pool net-208 171.69.233.209 171.69.233.222 netmask
255.255.255.240
ip nat inside source list 1 pool net-208
!
interface serial 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 0
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
```




```
RouterX# show ip nat translations
   Pro Inside global     Inside local      Outside local     Outside global
   --- 171.69.233.209    192.168.1.100          ---               ---
   --- 171.69.233.210    192.168.1.101          ---               ---
```

NAT
Cấu hình PAT

- **Tạo ACL để xác định dải địa chỉ bên trong**

```
Router(config)#access list [acl-number] permit
source [source-wildcard]
```

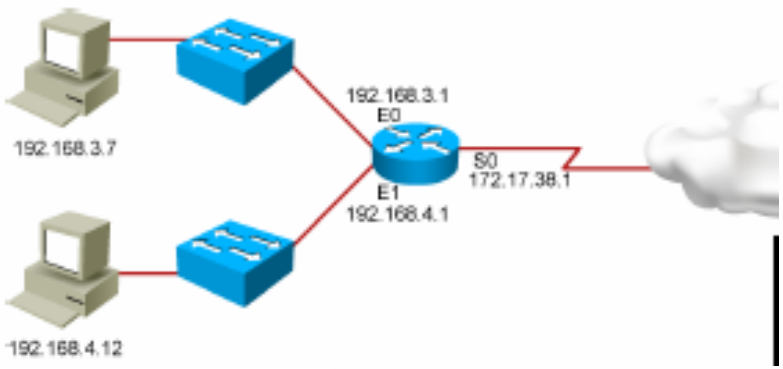
- **Xác định mối quan hệ giữa địa chỉ nguồn và cổng kết nối**

```
Router(config)#ip nat inside source list [acl-
number] interface [interface] overload
```

- **Xác định cổng kết nối với mạng nội bộ và mạng ngoài**

```
Router(config)#interface [type number]
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface [type number]
Router(config-if)#ip nat outside
```

NAT
Cấu hình PAT




```
hostname RouterI
!
interface Ethernet0
 ip address 192.168.3.1 255.255.255.0
 ip nat inside
!
interface Ethernet1
 ip address 192.168.4.1 255.255.255.0
 ip nat inside
!
interface Serial0
 description To ISP
 ip address 172.17.38.1 255.255.255.0
 ip nat outside
!
ip nat inside source list 1 interface Serial0 overload
!
ip route 0.0.0.0 0.0.0.0 Serial0
!
access-list 1 permit 192.168.3.0 0.0.0.255
access-list 1 permit 192.168.4.0 0.0.0.255
!
```

```
RouterX# show ip nat translations
      Pro Inside global      Inside local       Outside local      Outside global
      TCP 172.17.38.1:1050   192.168.3.7:1050    10.1.1.1:23        10.1.1.1:23
      TCP 172.17.38.1:1776   192.168.4.12:1776   10.2.2.2:25        10.2.2.2:25
```

NAT
Xoá cấu hình NAT

```
RouterX# clear ip nat translation *
```

- Clears all dynamic address translation entries

```
RouterX# clear ip nat translation inside global-ip
local-ip [outside local-ip global-ip]
```

- Clears a simple dynamic translation entry that contains an inside translation or both an inside and outside translation

```
RouterX# clear ip nat translation outside
local-ip global-ip
```

- Clears a simple dynamic translation entry that contains an outside translation

```
RouterX# clear ip nat translation protocol inside global-ip
global-port local-ip local-port [outside local-ip
local-port global-ip global-port]
```

- Clears an extended dynamic translation entry (PAT entry)

NAT
Kiểm tra cấu hình PAT

Hiển thị bảng NAT đang hoạt động:

Show ip nat translation

Hiển thị trạng thái hoạt động của NAT:

Show ip nat statistics

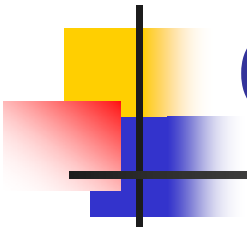
Kiểm tra hoạt động của NAT:

Debug ip nat

NAT
Kiểm tra cấu hình PAT

```
RouterX# debug ip nat

NAT: s=192.168.1.95->172.31.233.209, d=172.31.2.132 [6825]
NAT: s=172.31.2.132, d=172.31.233.209->192.168.1.95 [21852]
NAT: s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6826]
NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23311]
NAT*: s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6827]
NAT*: s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6828]
NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23312]
NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23313]
```

```
RouterX# show ip nat statistics
      Total active translations: 1 (1 static, 0 dynamic; 0 extended)
      Outside interfaces:
      Ethernet0, Serial2
      Inside interfaces:
      Ethernet1
      Hits: 5  Misses: 0
      --
```



CHƯƠNG 9

Các công nghệ WAN

Các công nghệ WAN

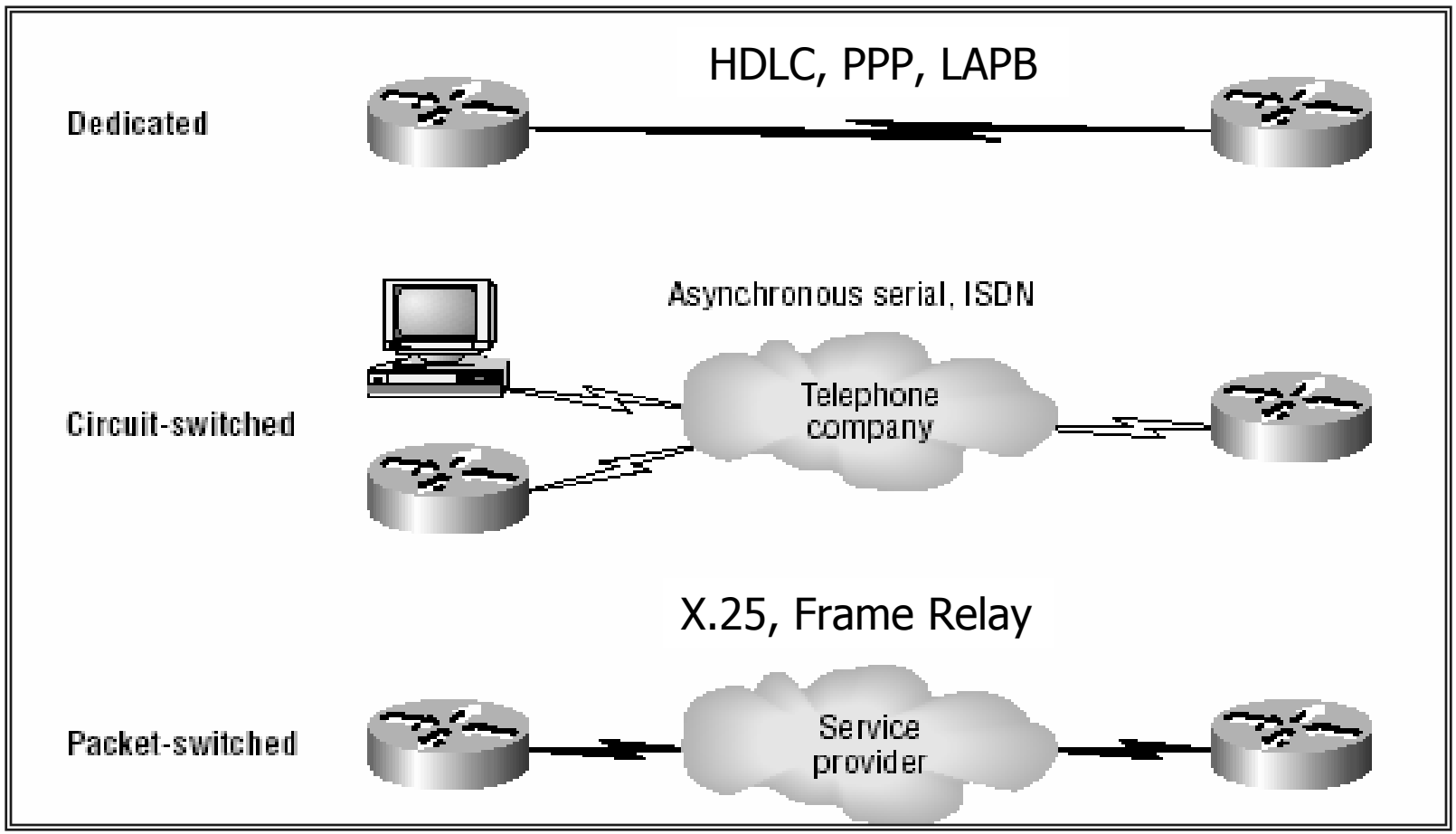
- Tổng quát về các công nghệ WAN
- Các công nghệ WAN
  - Dial-up
  - ISDN
  - Leased Line
  - X.25
  - Frame Relay
  - ATM
  - DSL
  - Cable modem

Các công nghệ WAN

Tổng quát

- Nhiều mạng LAN được kết nối thành mạng WAN.
- Một công ty bắt buộc phải thuê từ một nhà cung cấp dịch vụ WAN để sử dụng dịch vụ mạng WAN.
- WAN truyền các loại lưu lượng như thoại, dữ liệu, video…
- Có nhiều giải pháp khai triển một mạng WAN. Các giải pháp này khác nhau về kỹ thuật, tốc độ, chi phí.

Tổng quát về các công nghệ WAN
Kiểu kết nối WAN



Tổng quát về các công nghệ WAN
Giao thức đóng gói dữ liệu trong WAN

- Point-to-Point Protocol (PPP)
- Serial Line Internet Protocol (SLIP)
- High-Level Data Link Control Protocol (HDLC)
- X.25 / Link Access Procedure Balanced (LAPB)
- Frame Relay
- Asynchronous Transfer Mode (ATM)

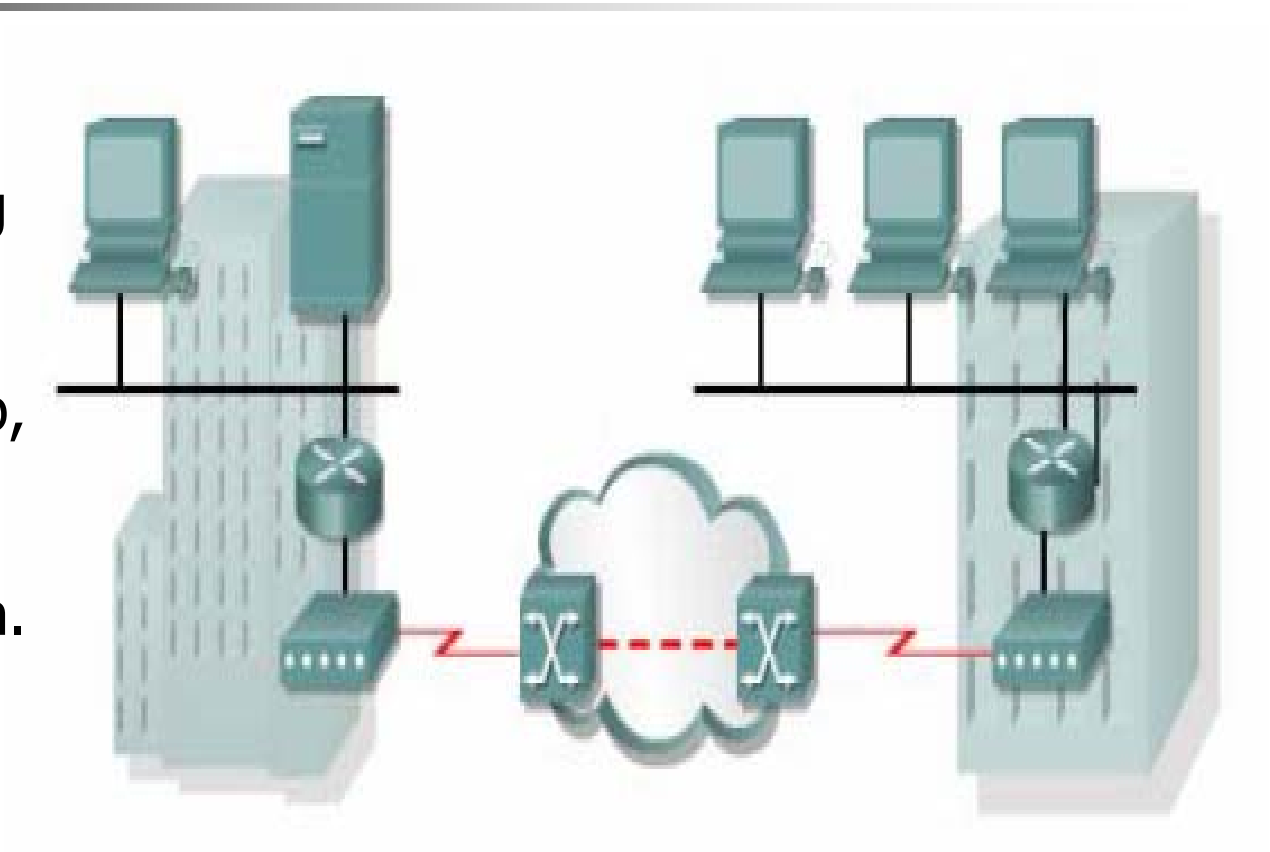
Tổng quát về các công nghệ WAN

Giao thức đóng gói dữ liệu trong WAN

WAN Type	Maximum Speed
Asynchronous Dial-Up	56-64 Kbps
X.25, ISDN – BRI	128 Kbps
ISDN – PRI	E1 / T1
Leased Line / Frame Relay	E3 / T3

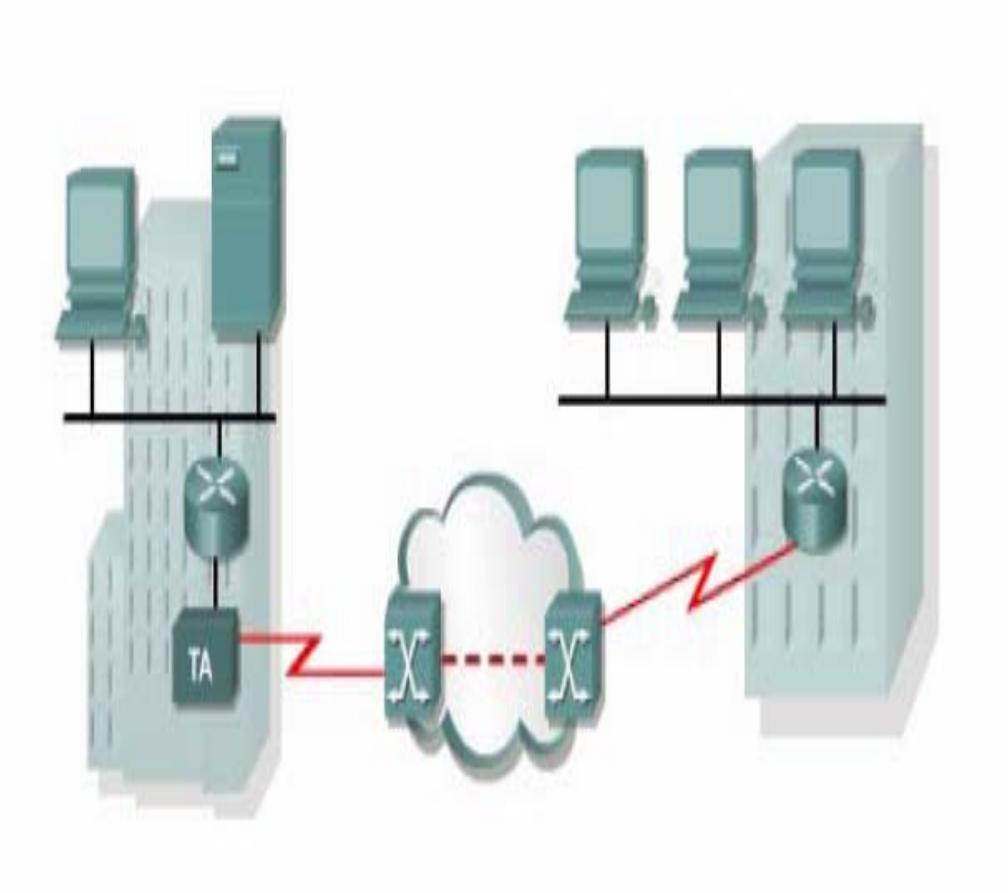
Các công nghệ WAN
Kênh quay số Dial-up

- Thông qua modem và mạng điện thoại công cộng.
- Dung lượng thấp, tốc độ thấp 33Kb/s-56Kb/s.
- Đơn giản, rẻ tiền. Dùng trong gia đình và doanh nghiệp nhỏ.

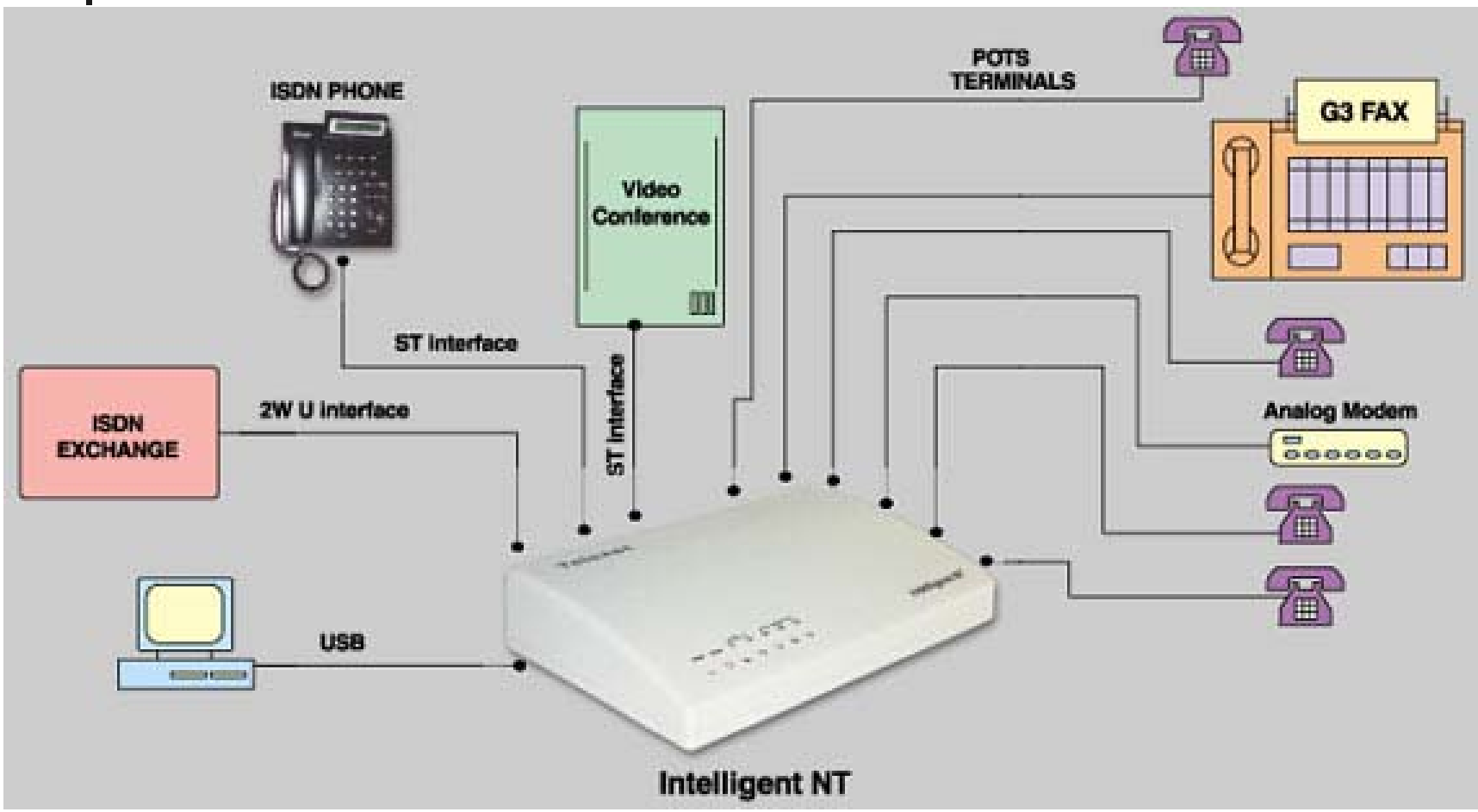


Các công nghệ WAN
ISDN

- Router cần có cổng ISDN hoặc kết nối qua bộ chuyển đổi giao tiếp.
- Giao tiếp tốc độ cơ bản BRI ISDN cung cấp 2 kênh B 64 kb/s và 1 kênh D 16 kb/s.
- Giao tiếp PRI ISDN có thể cung cấp tốc độ lên tới 2.048 Mb/s.
- Truyền tín hiệu số chứ không phải tín hiệu tương tự. Có thể truyền trên nhiều kênh cùng lúc.
- Thường thuê riêng hoặc làm đường truyền dự phòng.

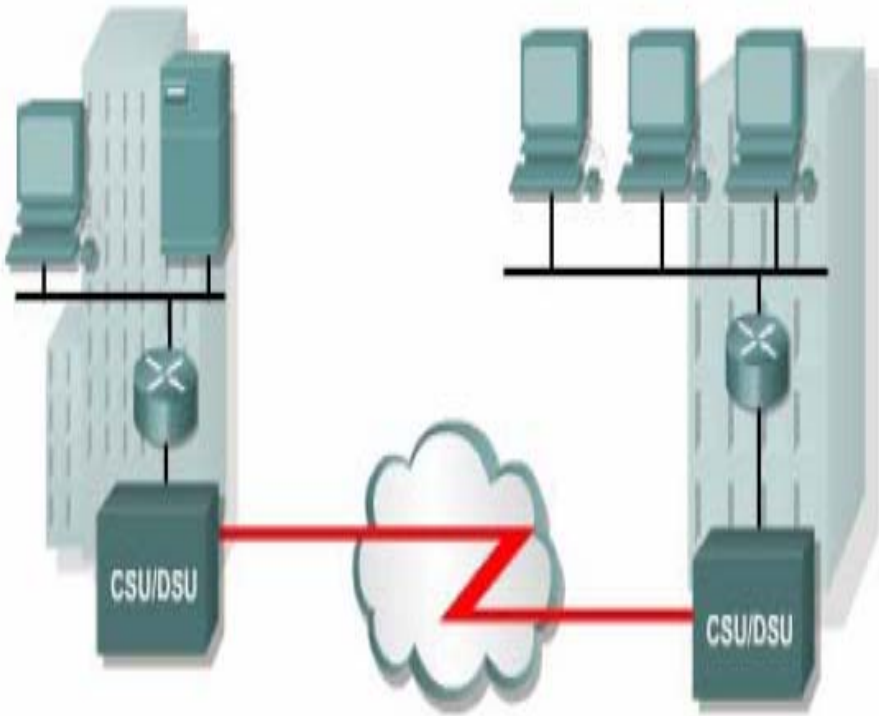


Các công nghệ WAN
ISDN



Các công nghệ WAN
Đường truyền thuê riêng (Leased Line)

- Kết nối điểm-đến-điểm từ vị trí của thuê bao thông qua mạng của nhà cung cấp dịch vụ đến điểm đích.
- Có nhiều mức dung lượng, có thể lên tới 2,5Gb/s.
- Giá cả phụ thuộc mức băng thông và khoảng cách giữa hai điểm kết nối.
- Không có thời gian trễ và nghẽn mạch.

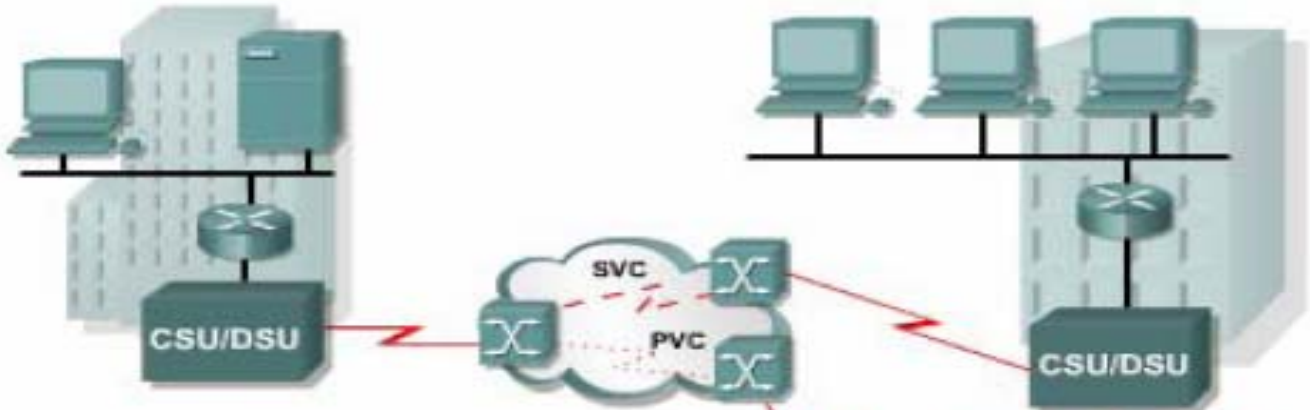


Các công nghệ WAN

Leased Line (Đường truyền thuê riêng)

Loại	Chuẩn	Dung lượng
56	DS0	56 Kbps
64	DS0	64 Kbps
T1	DS1	1.544 Mbps
E1	ZM	2.048 Mbps
E3	M3	34.064 Mbps
J1	Y1	2.048 Mbps
T3	DS3	44.736 Mbps
OC-1	SONET	51.84 Mbps
OC-3	SONET	155.54 Mbps
OC-9	SONET	466.56 Mbps
OC-12	SONET	622.08 Mbps
OC-18	SONET	933.12 Mbps
OC-24	SONET	1244.16 Mbps
OC-36	SONET	1866.24 Mbps
OC-48	SONET	2488.32 Mbps

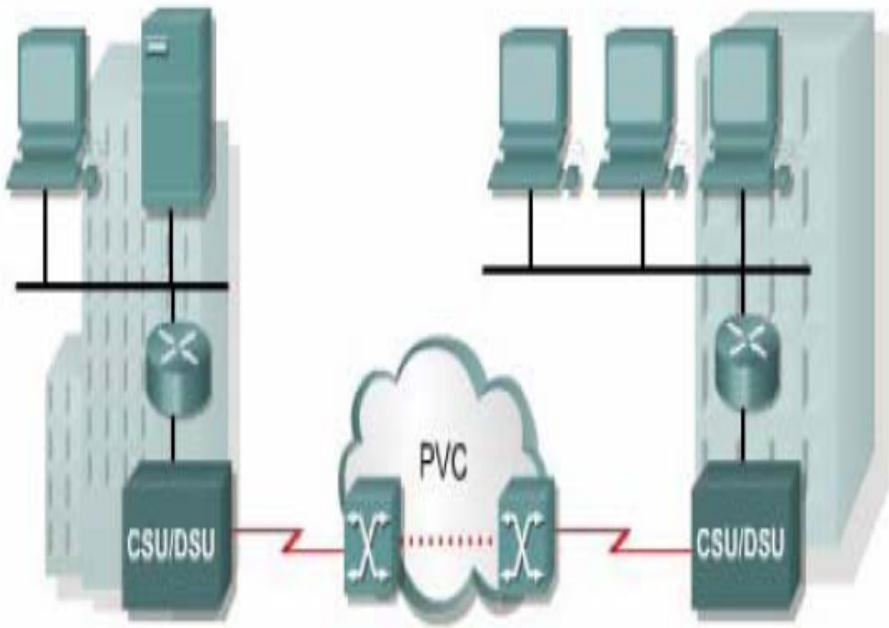
Các công nghệ WAN
X.25 (Đường truyền chia sẻ)



- Mạng chuyển mạch gói sử dụng đường truyền chia sẻ để giảm chi phí.
- Hoạt động ở lớp Mạng.
- Khi có yêu cầu, một mạch ảo SVC sẽ được thiết lập.
- Dung lượng thấp, tối đa là 48 kb/s.
- Chi phí cước được tính theo lưu lượng dữ liệu.

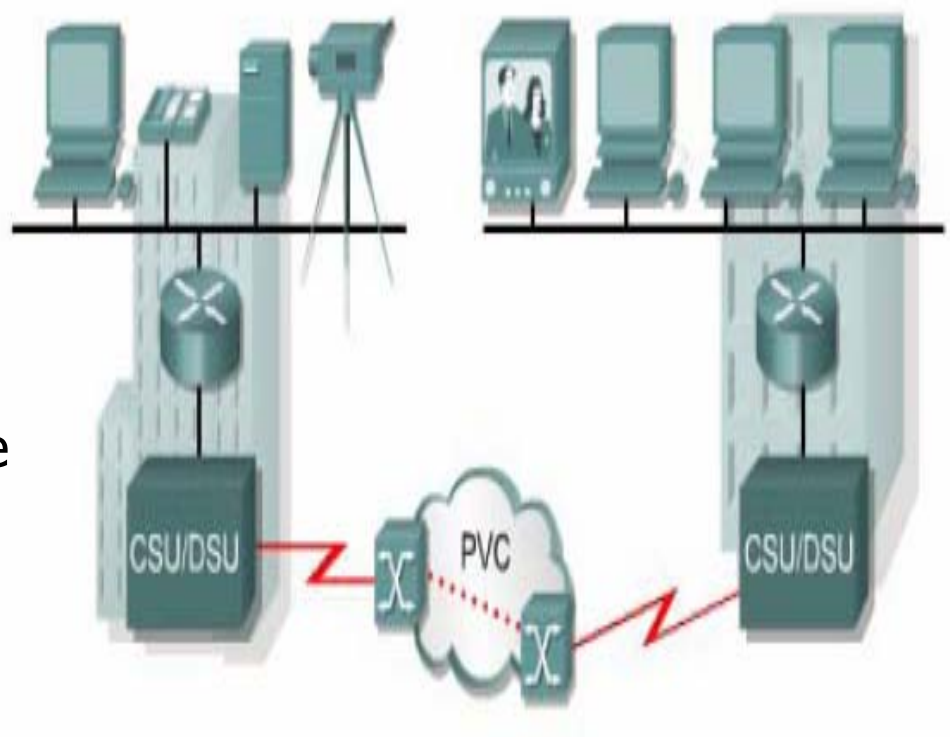
Các công nghệ WAN
Frame Relay (Đường truyền chia sẻ)

- Hoạt động như X.25 nhưng tốc độ cao hơn, lên đến 4Mb/s hoặc hơn nữa.
- Hoạt động ở lớp Liên kết dữ liệu và đơn giản hơn X.25.
- Kết nối kênh truyền cố định PVC.
- Chi phí cước được tính theo dung lượng kết nối.
- Được sử dụng phổ biến.



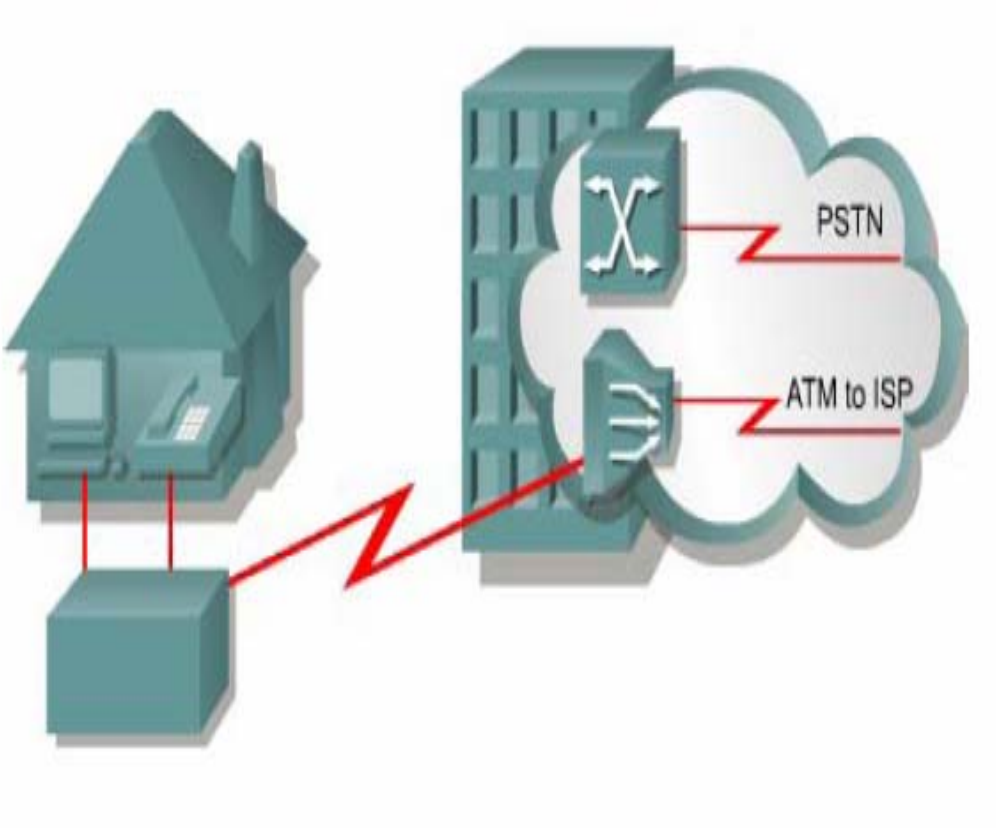
Các công nghệ WAN
ATM (Asynchronous Transfer Mode)

- Là đường truyền chia sẻ với thời gian trễ thấp, ít nghẽn mạch, băng thông cao.
- Tốc độ 155Mb/s.
- Có khả năng truyền thoại, video, dữ liệu.
- Gói dữ liệu không phải frame mà là tế bào (cell) với chiều dài cố định 53 byte.
- Cung cấp kết nối PVC và SVC.



Các công nghệ WAN
DSL (Digital Subscriber Line)

- Là công nghệ truyền băng thông rộng sử dụng đường truyền hai dây xoắn của hệ thống điện thoại.
- Bao gồm các công nghệ:
  - Asymmetric DSL (ADSL)
  - Symmetric DSL (SDSL)
  - High Bit Rate DSL (HDSL)
  - ISDN DSL (IDSL)
  - Consumer DSL (CDSL)

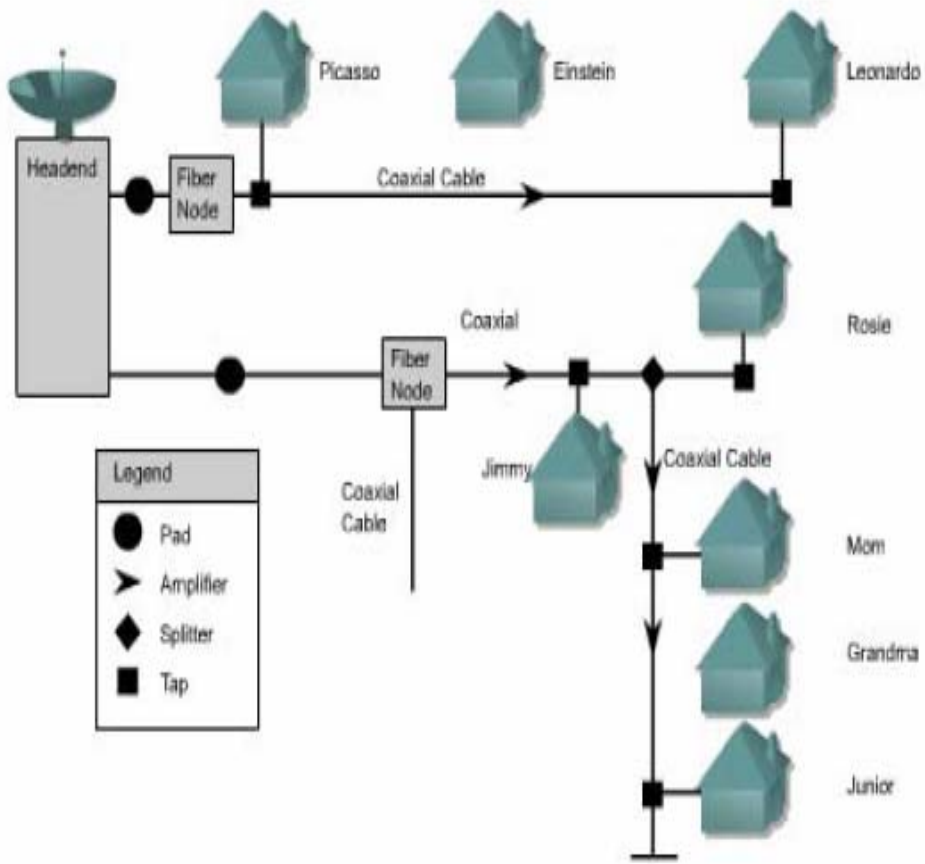


Các công nghệ WAN
DSL (Digital Subscriber Line)

Service	Download	Upload
ADSL	64 kbps - 8.192 Mbps	16 kbps - 640 kbps
SDSL	1.544 Mbps - 2.048 Mbps	1.544 Mbps - 2.048 Mbps
HDSL	1.544 Mbps - 2.048 Mbps	1.544 Mbps - 2.048 Mbps
IDSL	144 kbps	144 kbps
CDSL	1 Mbps	16 kbps - 160 kbps

Các công nghệ WAN
Cable modem

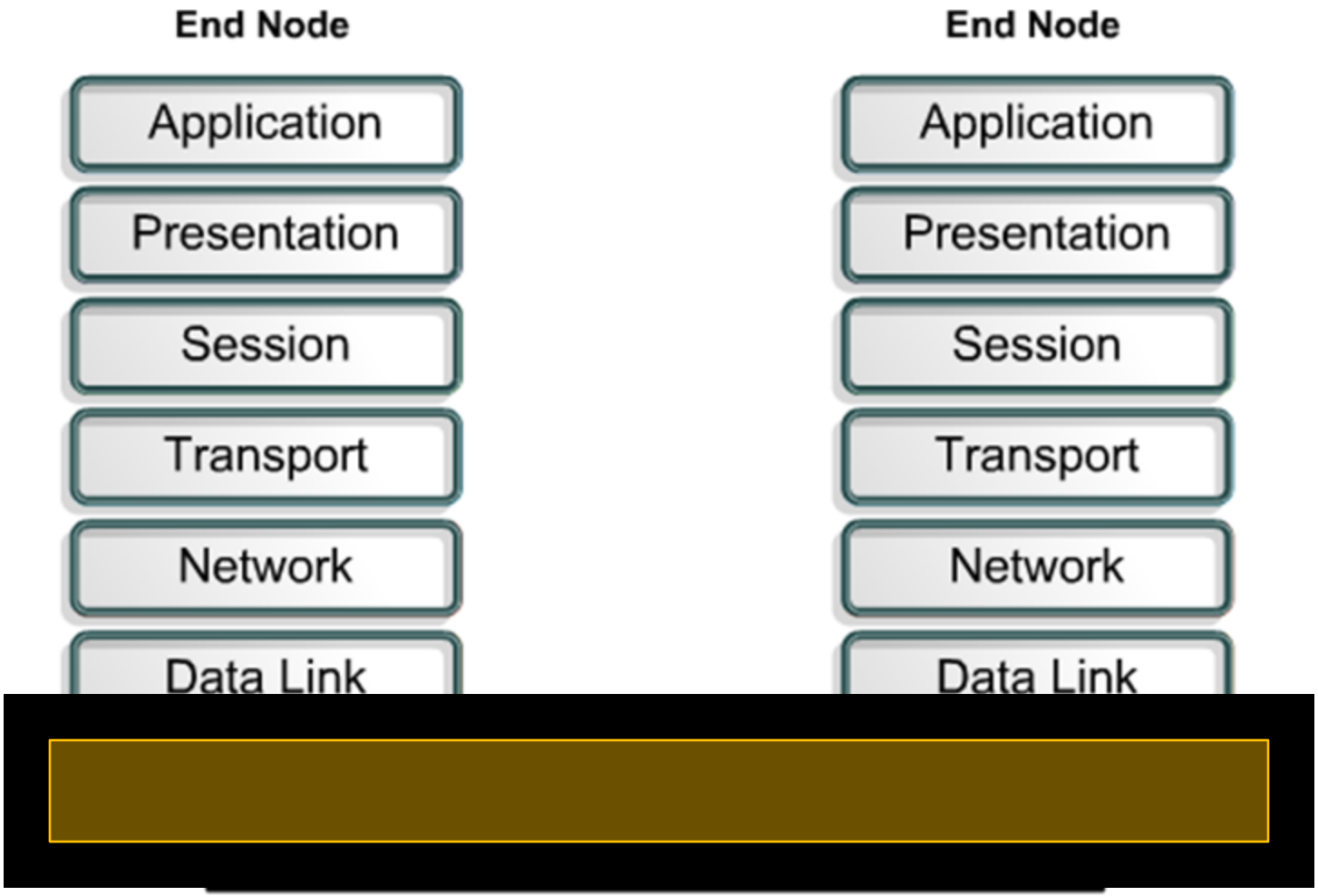
- Sử dụng cáp đồng trục trong hệ thống mạng cáp truyền hình.
- Dung lượng 30 – 40 Mb/s.
- Thuê bao nhận song song dịch vụ truyền hình cáp và dữ liệu thông qua một bộ phân giải 1-2 đơn giản.
- Tất cả các thuê bao nội bộ đều chia sẻ cùng một băng thông cáp nên càng nhiều người tham gia thì lượng băng thông sẽ càng giảm.



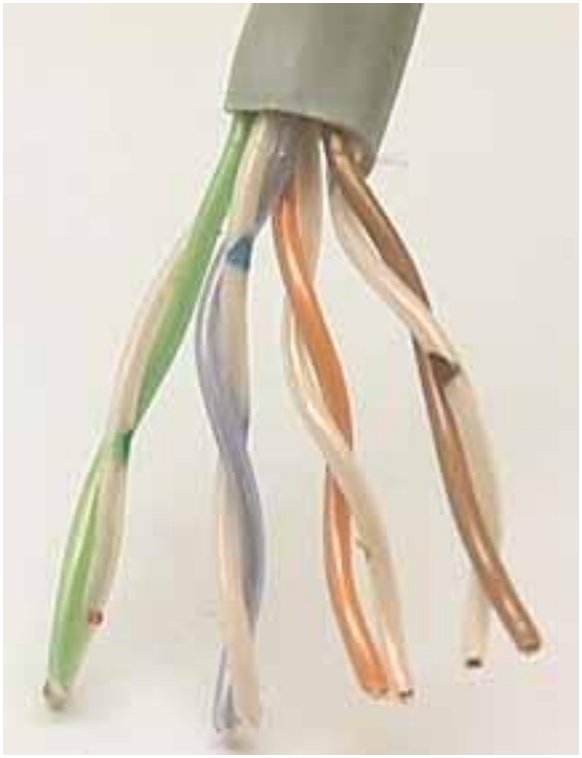

Hết

Thiết bị mạng thông dụng

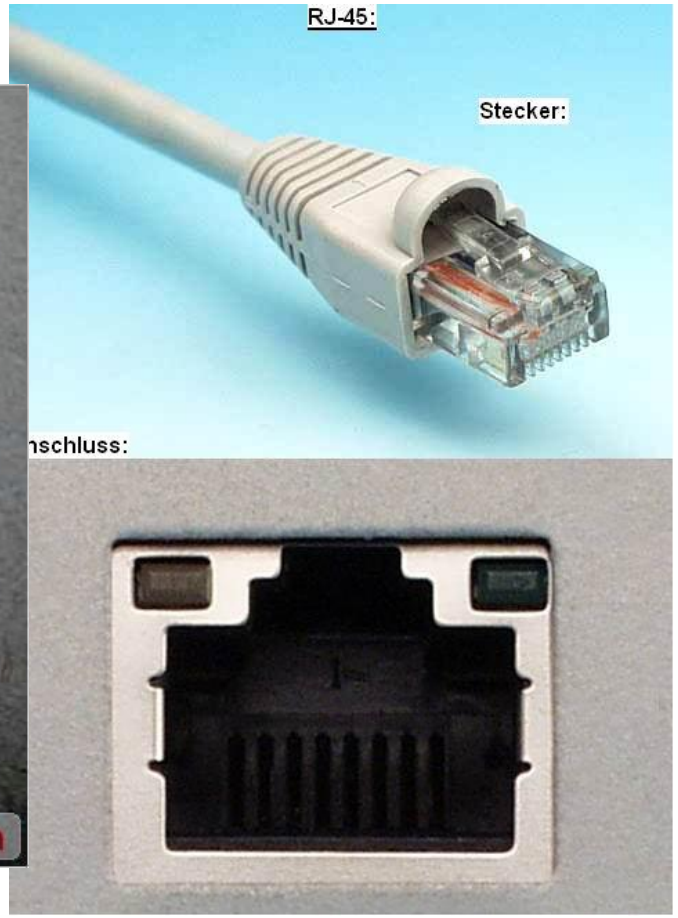
Tầng physical



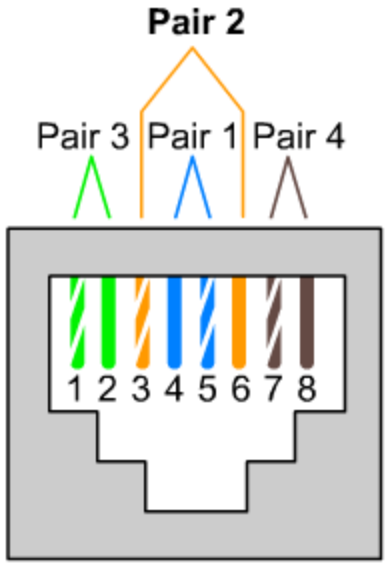
- UTP Cat 5

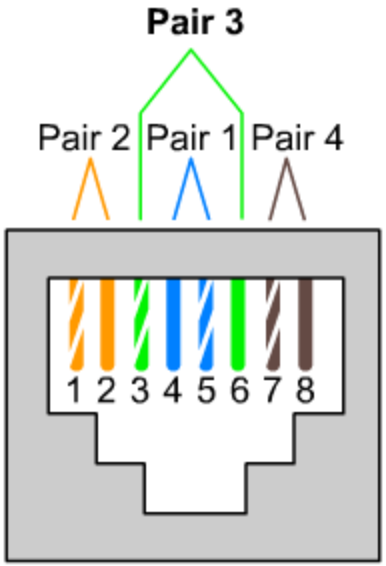


Đầu bấm cáp Rj 45



Cách bấm dây


Pair 2
Pair 3
Pair 1
Pair 4
1 2 3 4 5 6 7 8
T568A


Pair 3
Pair 2
Pair 1
Pair 4
1 2 3 4 5 6 7 8
T568B

converter

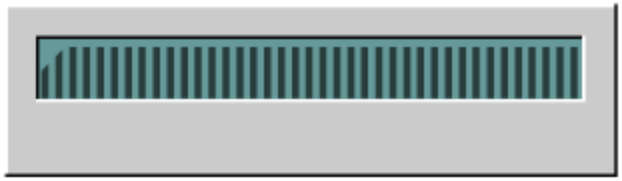

EO-200UC
Ethernet Converter
10Base-T to 10Base-2
ETHERNET
AUI-UTP
TRANSLATOR
EO-200UA
EO-200UF
Ethernet Converter
10Base-T to 10Base-FL

repeater

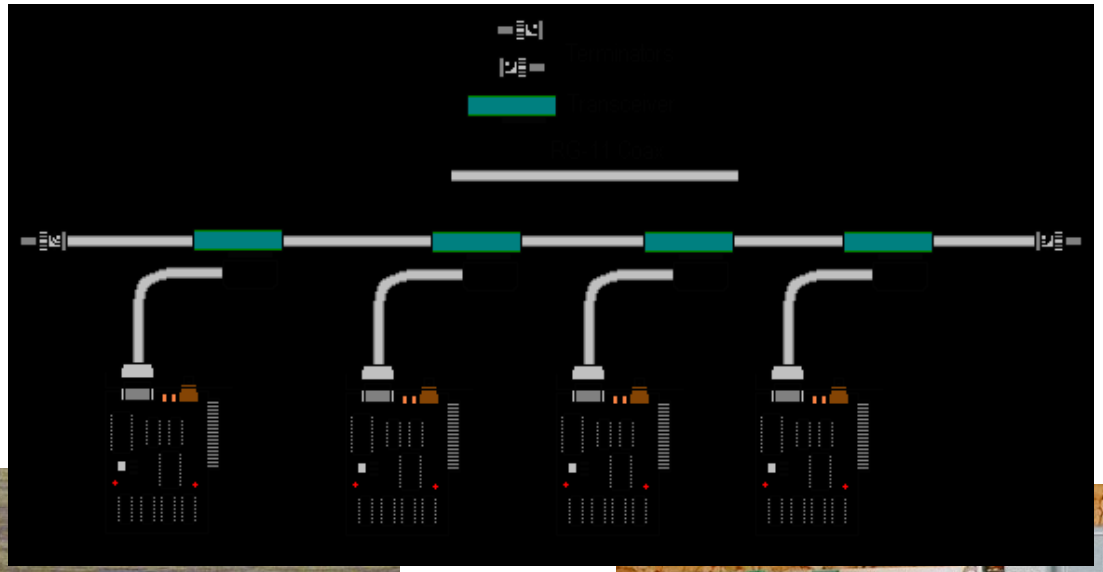
- Là thiết bị mạng nối 2 nhánh mạng có chức năng nhận tín hiệu ở một mạng, khuếch đại tính hiệu và truyền tiếpvào nhánh mạng còn lại
- Repeater chỉ khuếch đại tín hiệu không xử lý nội dung tín hiệu
- Số lượng repeater trong một mạng là có giới hạn (tối đa 4)
- Repeater là thiết bị ở tầng physical

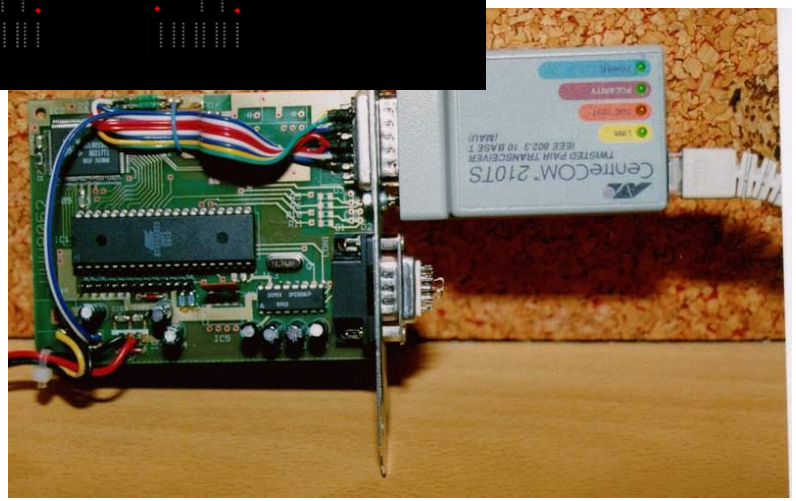
repeater

- Thuận lợi cho phép mở rộng mạng dể dàng
- Không có chi phí xử lý tín hiệu
- Cho phép nối kết các phần mạng của một mạng logic sử dụng kiểu cáp khác nhau
- Bất lợi
- Không cho phép kết nối các kiểu mạng logic khác nhau
- Không cho phép giảm tải mạng
- Số lượng repeater bị giới hạn



Các loại đầu kết nối AUI, AUI-RJ45

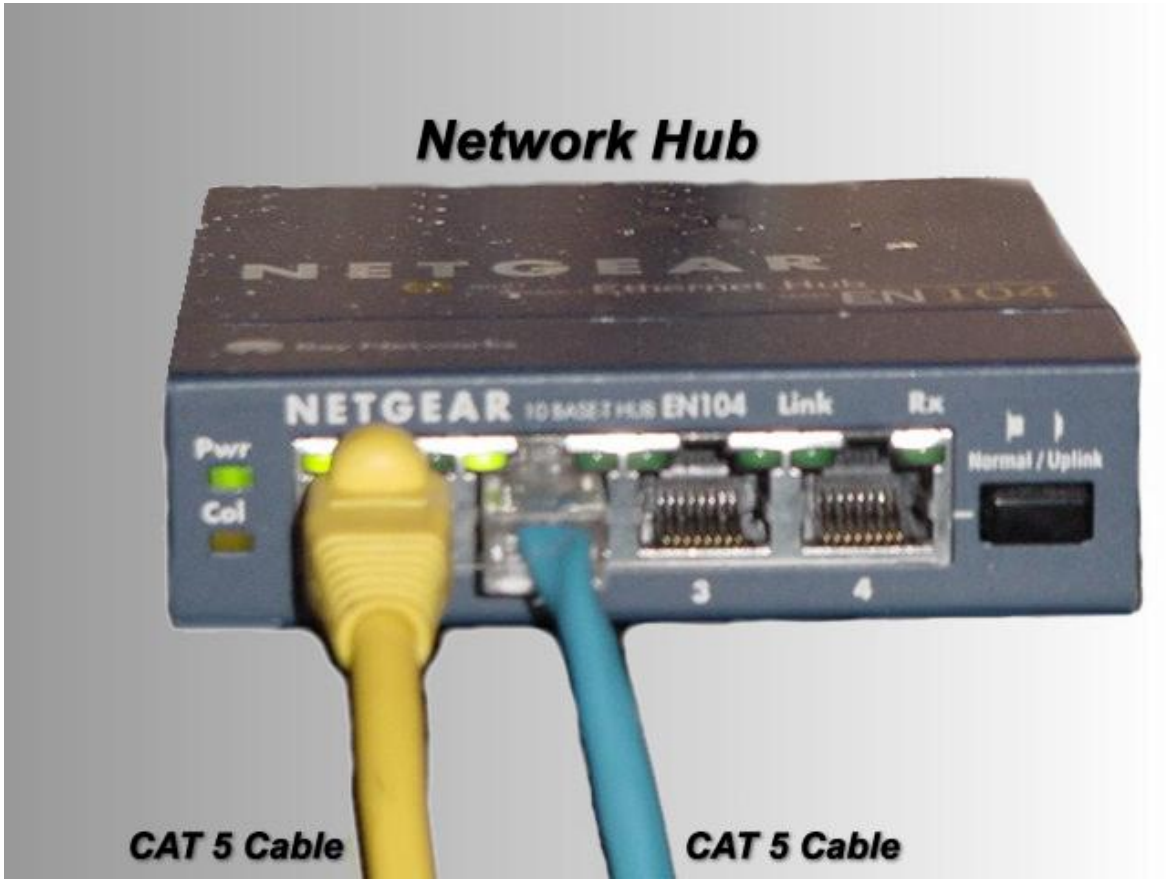




hubs

- Là thiết bị mạng cho phép tập kết dây dẫn mạng
- Trên hub có nhiều cổng (port) cho phép cấm vào đó các đầu cáp mạng
- Có 3 loại hub
  - Passive hub
  - Active huB
  - Intelligent hub

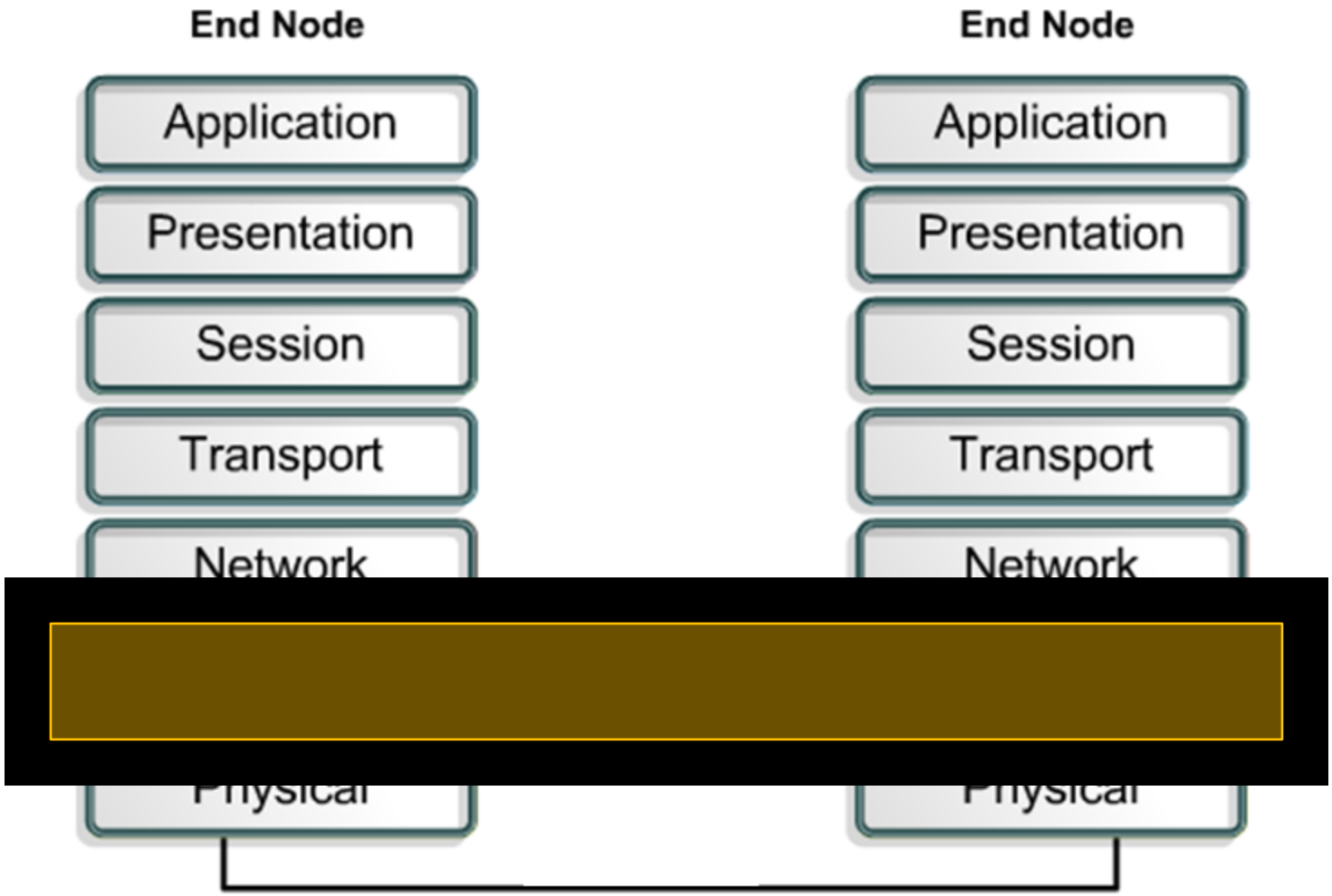
Hub

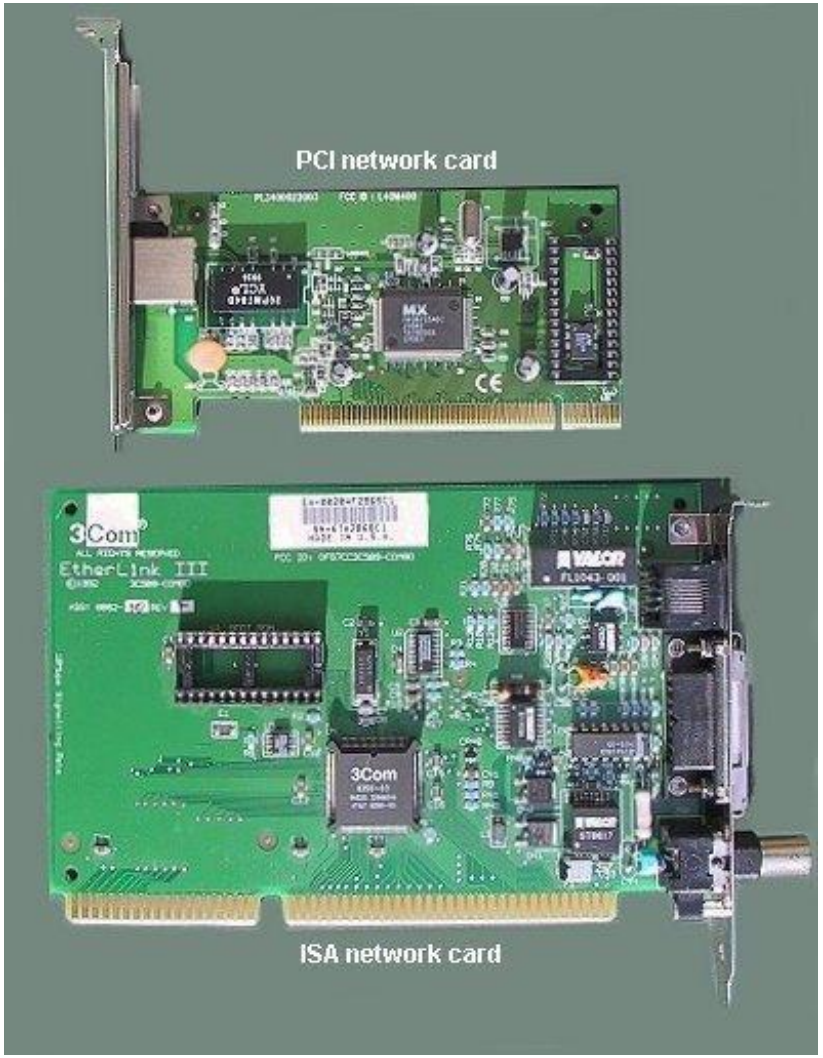

Network Hub
NETGEAR
NETGEAR 10 BASE-T HUB EN104
Link
Rx
Pwr
Col
Normal / Uplink
3
4
CAT 5 Cable
CAT 5 Cable

Các loại hub

- Passive hub
  - Là thiết bị đấu cáp, cho phép tín hiệu từ một đoạn cáp có thể truyền đến các đoạn cáp khác
  - Không có linh kiện điện tử
  - Không khuếch đại và xử lý tín hiệu
- Active hub
  - Là thiết bị đấu cáp cho phép tín hiệu từ một đoạn cáp có thể truyền đến các đoạn cáp khác nhau với chất lương cao hơn
  - Active hub có linh kiện điện tử
  - Hoạt động như một repeater có nhiều cổng
- Intelligent hubs: là một active hub với một số chức năng bổ sung
  - Cho phép quản lý các máy tính
  - Chuyển mạch chức năng này cho phép tín hiệu được chuyển đến các cổng vốn được nối với nhánh mang có chứa trạm nhận các tín hiệu không được chuyển đến các cổng không liên quan

Tầng Data Link

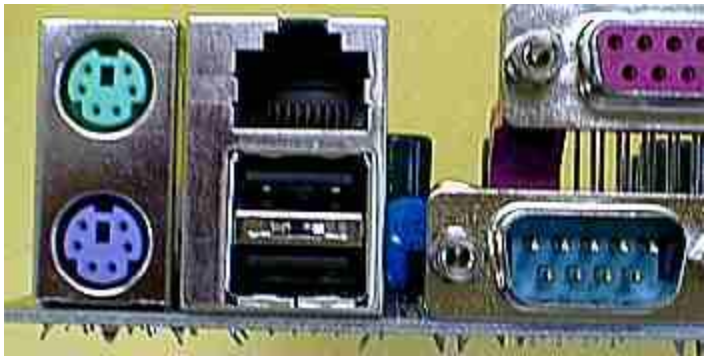



PCI network card
3Com
EtherLink III
3Com
ISA network card

Thiết bị

- Card mạng hỗ trợ cổng RJ45

Net card PCI

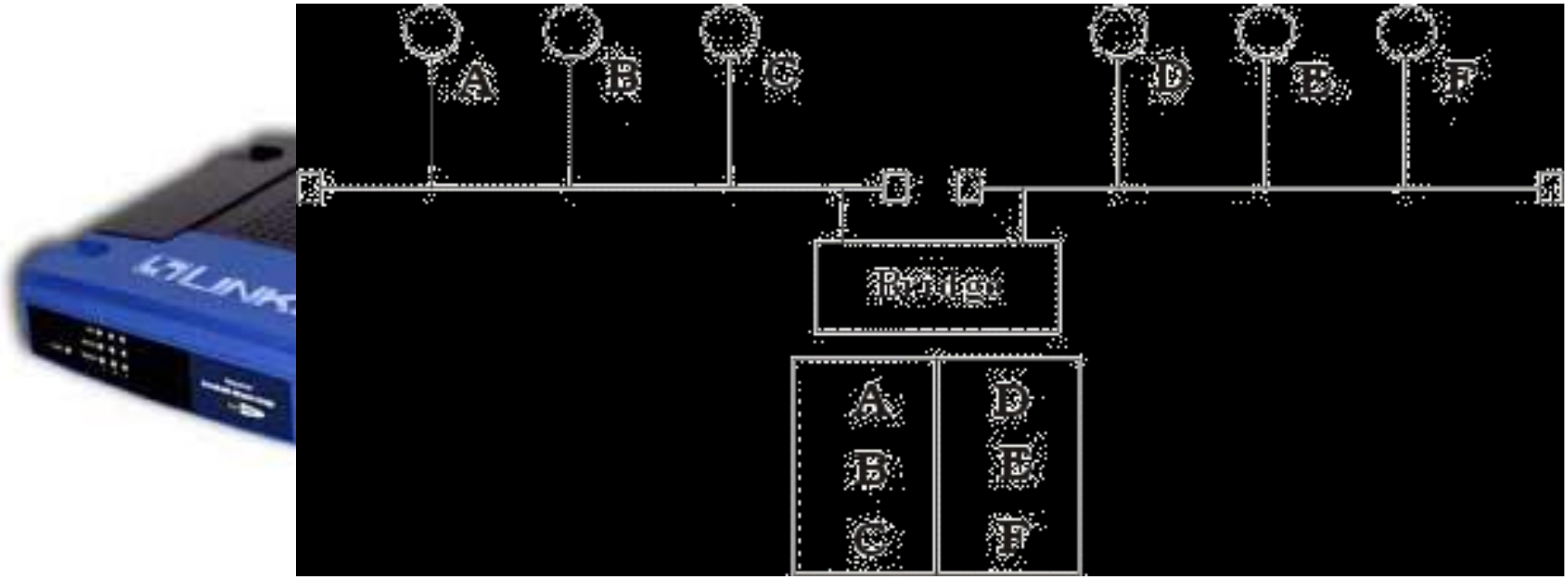


Net card onboard

Net card PCMCIA for laptop

bridge

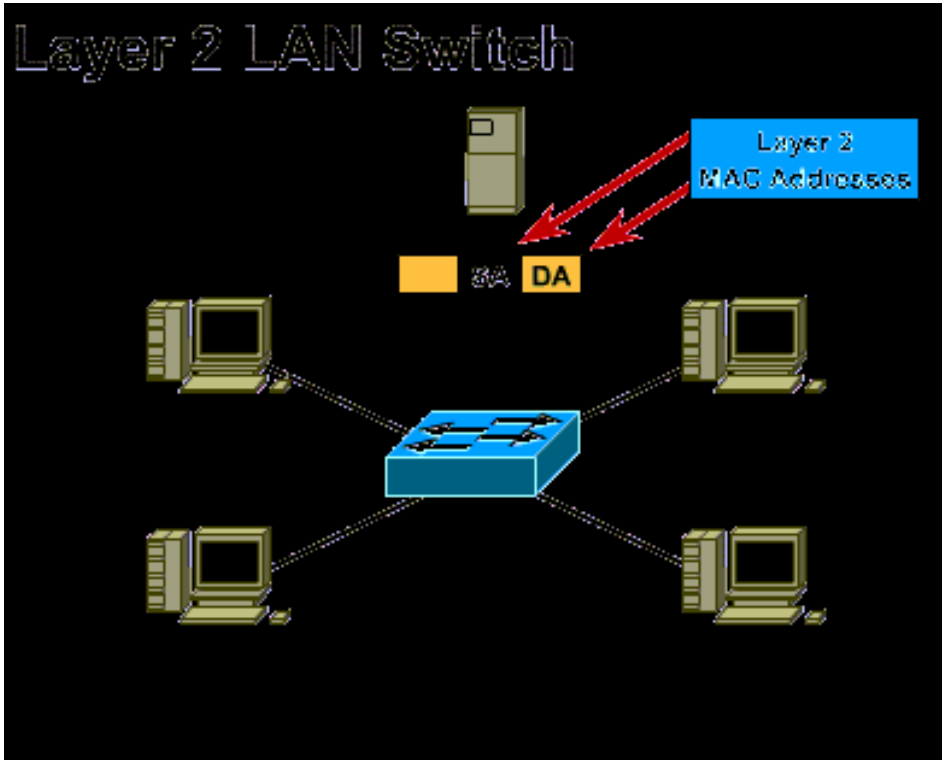
- Là thiết bị mạng cho phép nối kết 2 nhánh mạng, có chức năng chính chuyển có chọn lọc các gói tin đến nhánh mạng chứa trạm nhận gói tin



bridge

- Bridge duy trì một bảng địa chỉ, ứng với từng trạm bảng địa chỉ sẽ cho biết nhánh mạng mà trạm nó thuộc về. Bảng địa chỉ có thể được khởi tạo và duy trì tự động hoặc thủ công
- Có 2 loại bridge: transparent bridge (learning bridge) và source routing bridge
- Bridge là thiết bị ở tầng 2

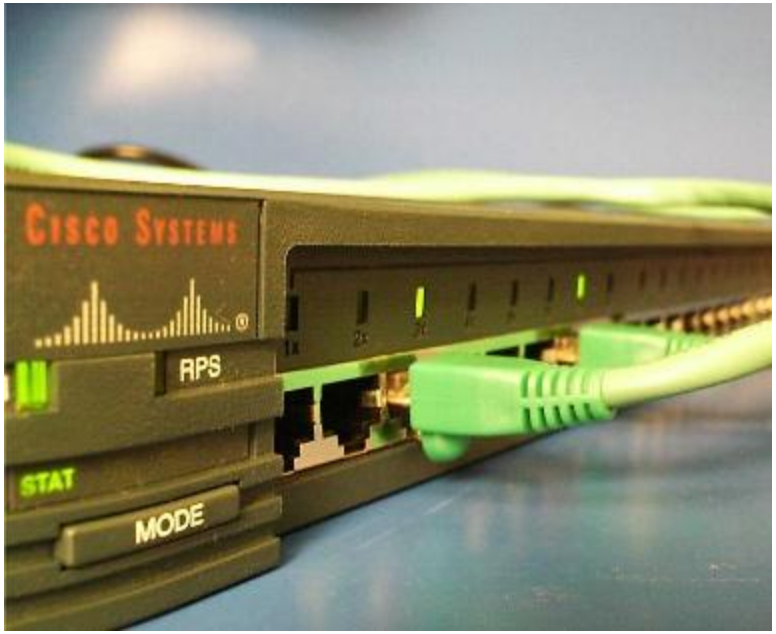

SMC


Layer 2 LAN Switch
Layer 2
MAC Addresses
SA
DA

Bridge thuận lợi và bất lợi

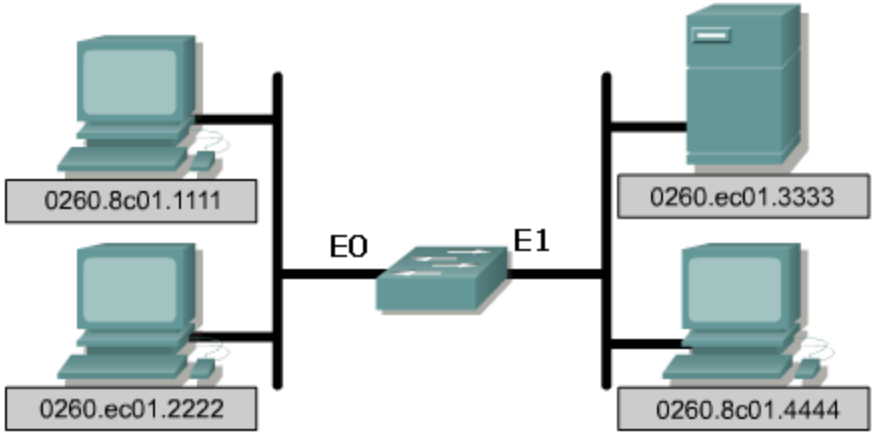
- Thuận lợi :
  - cho phép mở rộng cùng một mạng logic với nhiều kiểu chạy cáp khác nhau
  - Tách một mạng thành nhiều phần nhằm giảm lưu lượng mạng
- Bất lợi:
  - Chậm hơn repeater do phải xử lý gói tin
  - Không thể kết nối các mạng logic khác nhau
  - Không thể phân tích mạng để tìm đường đi tối ưu trong trường hợp có nhiều đường đi
  - Đắt tiền hơn repeater

Switch



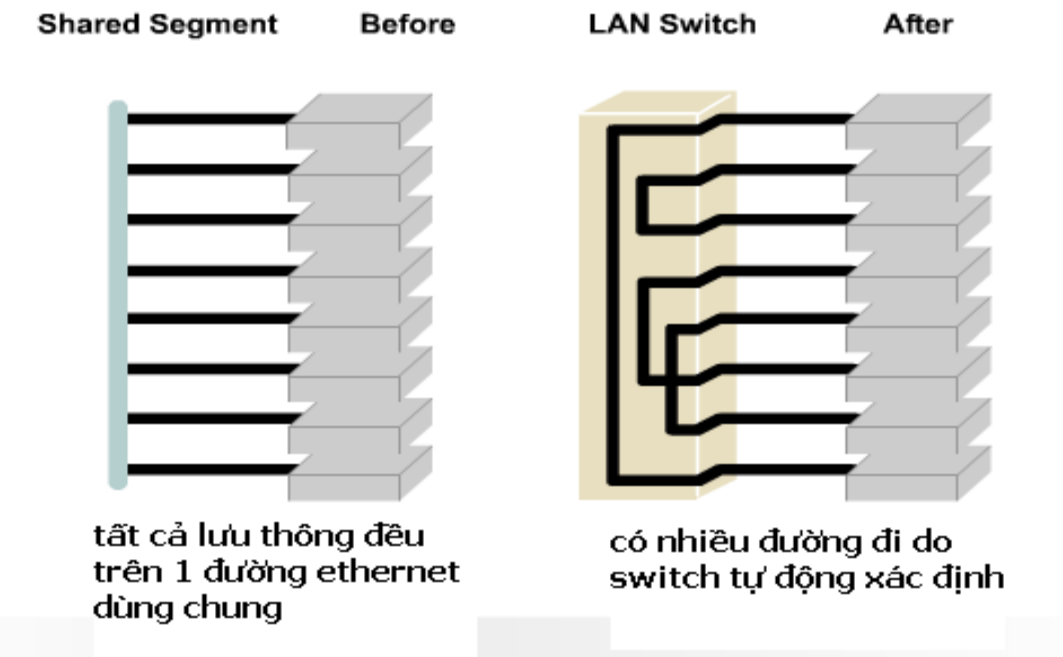
Cisco 2900 series

Interface	MAC Address
E0	0260.8c01.1111
E0	0260.ec01.2222
E1	0260.ec01.3333
E1	0260.8c01.4444



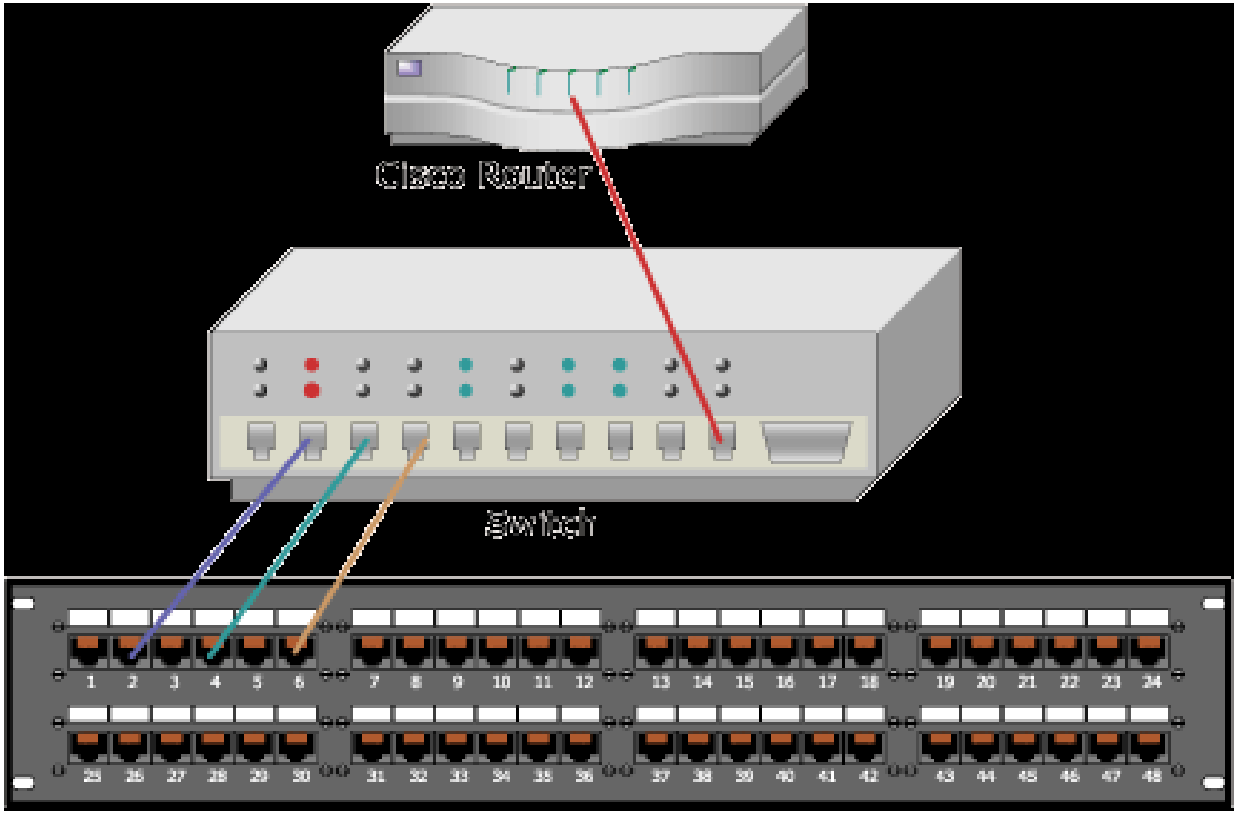
Bảng định tuyến theo địa chỉ MAC

Chia nhỏ mạng bằng switch

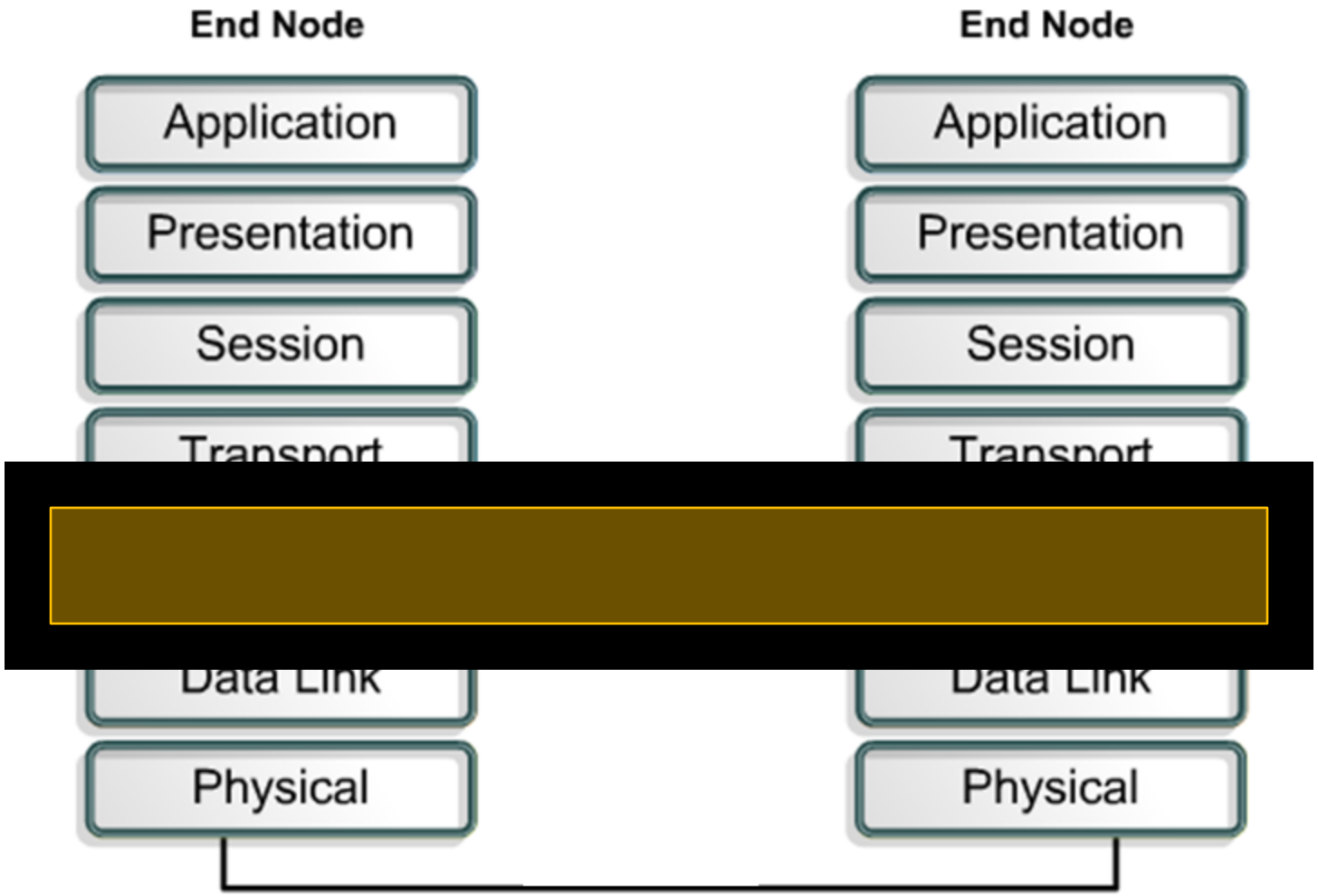


- Chỉ định đường đi giữa nơi nhận và nơi gửi
- Thay Hub bằng switch là tăng hiệu suất hiểu quả nhất (vì không cần thay đổi các thiết bị khác và cáp mạng)

Patch panel

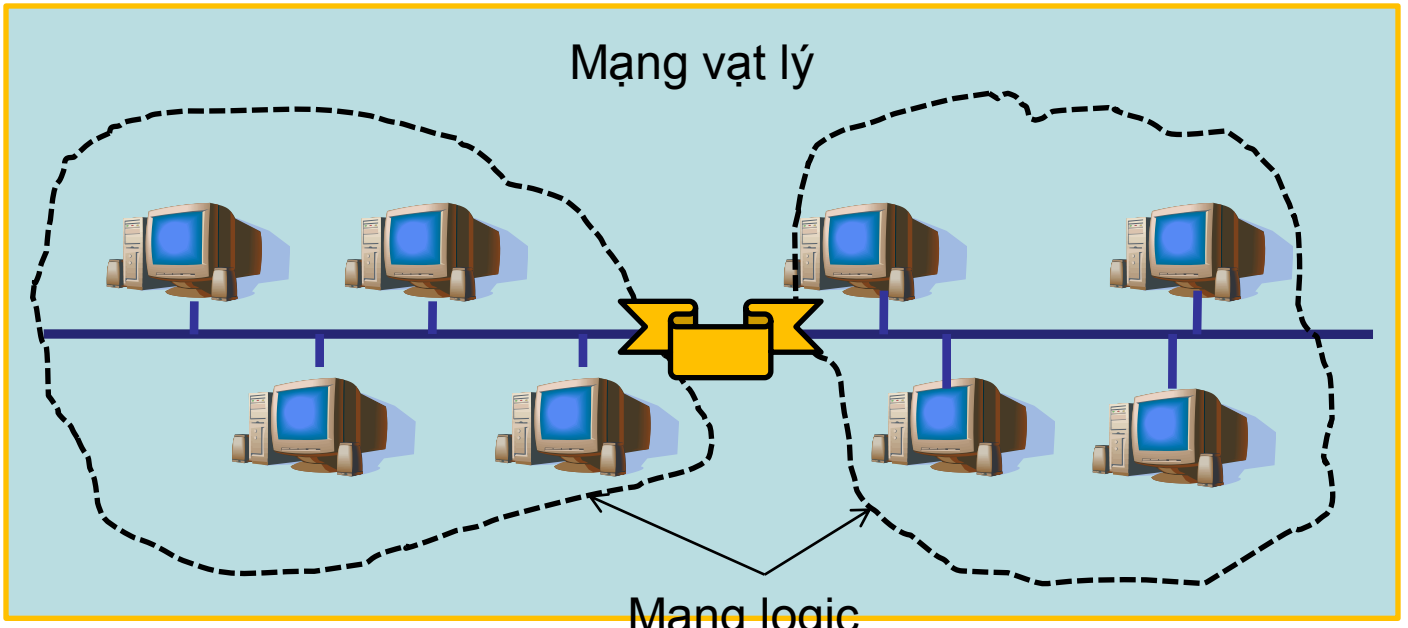

Cisco Router
Switch
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48

Tầng network



Định tuyến (routing)

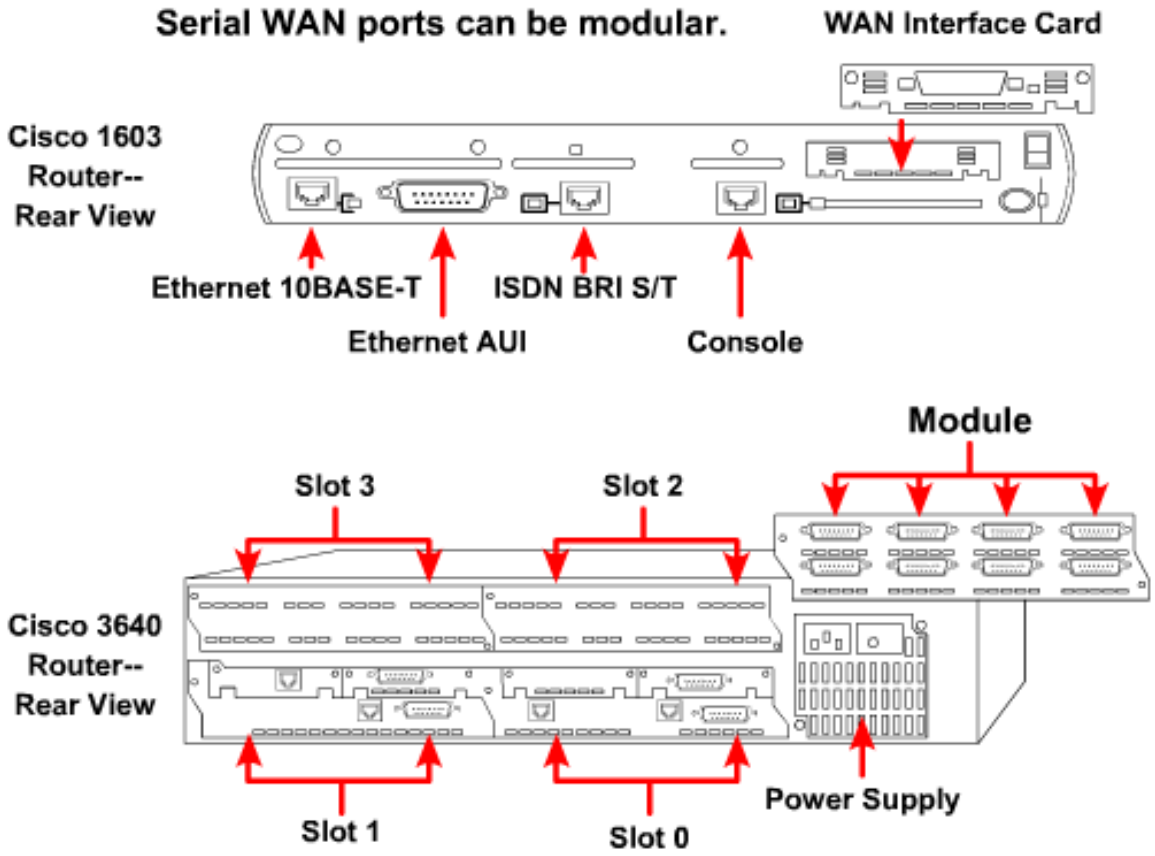
- Định tuyến xác định đường đi và chuyển gói tin đến đích
- Thiết bị định tuyến là router hoặc brouter

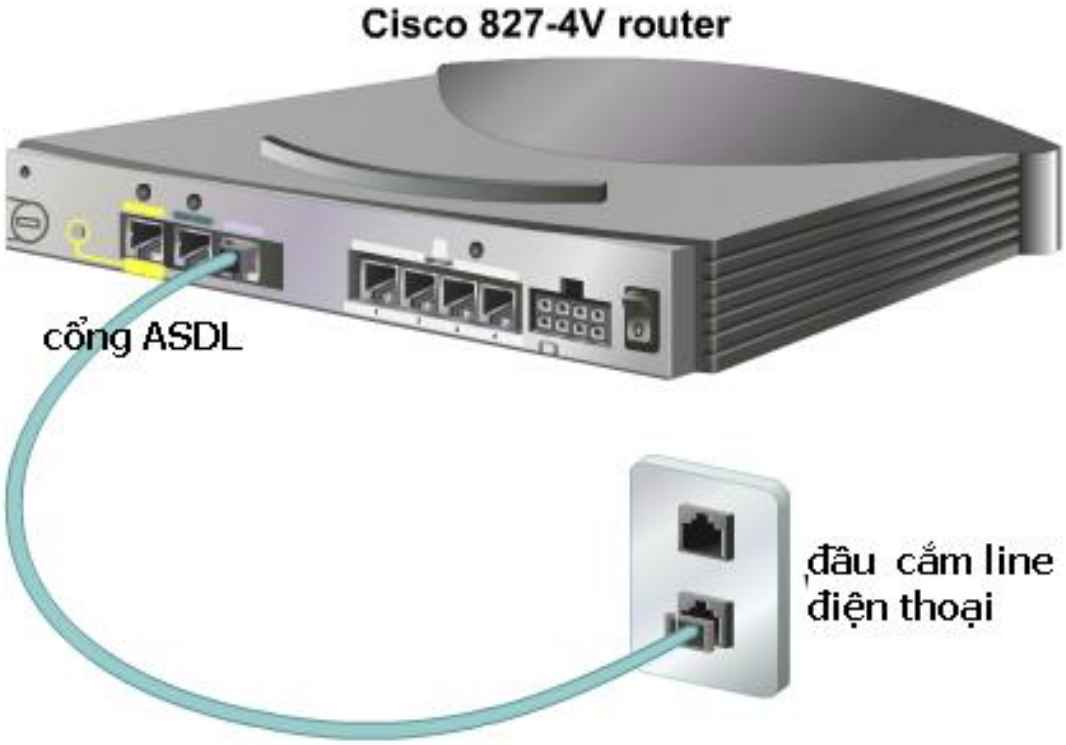


router

- Là thiết bị mạng cho phép
- Nối kết các mạng logic khác nhau
- Hạn chế lưu lương trên các mạng logic
- Xử lý thông tin mạng để tìm đường đi tối ưu cho các gói tin
- Router dùng bảng định tuyến để định tuyến mạng có thể dược cấu hình tĩnh hoặc động
- Router tĩnh
- Router động
- Router hoạt động ở tầng network
- Brouter (bridging router): router cho phép hoặt động như một bridge

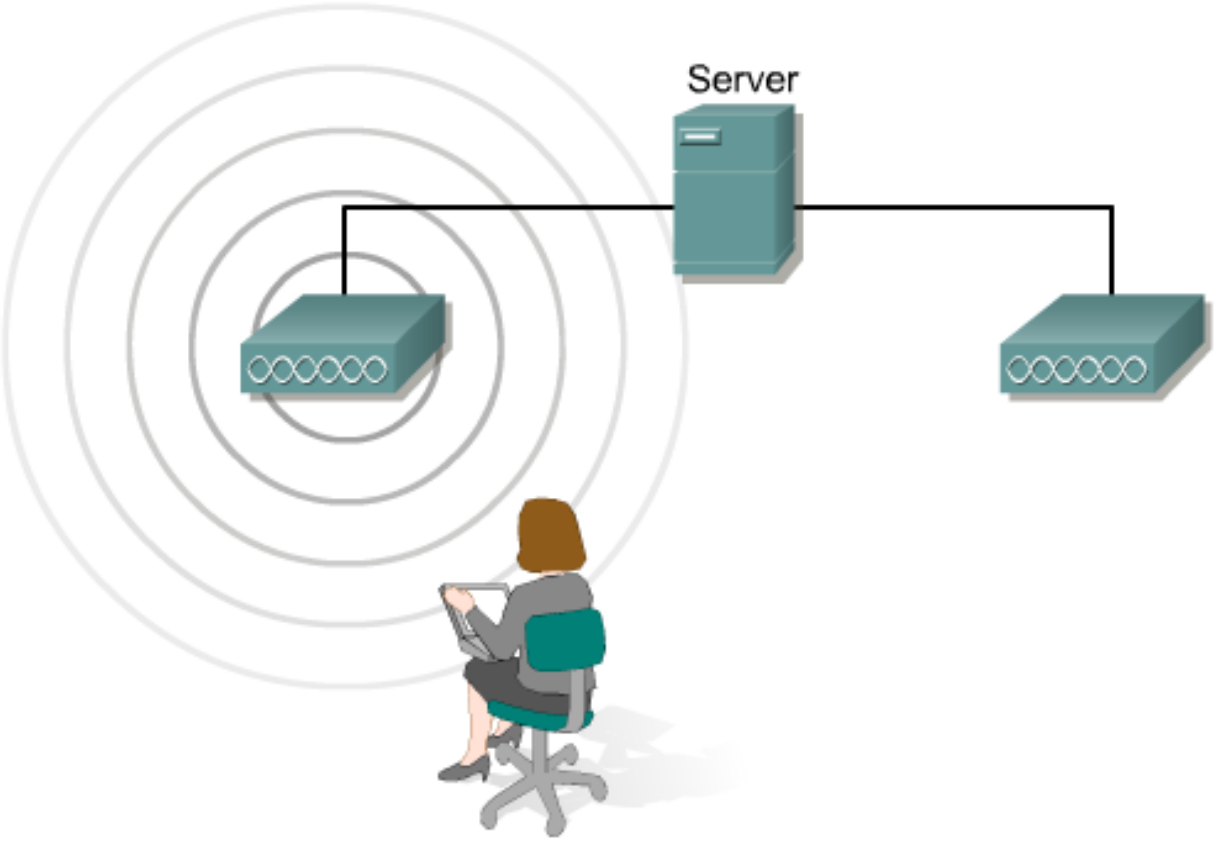
Các module mở rộng

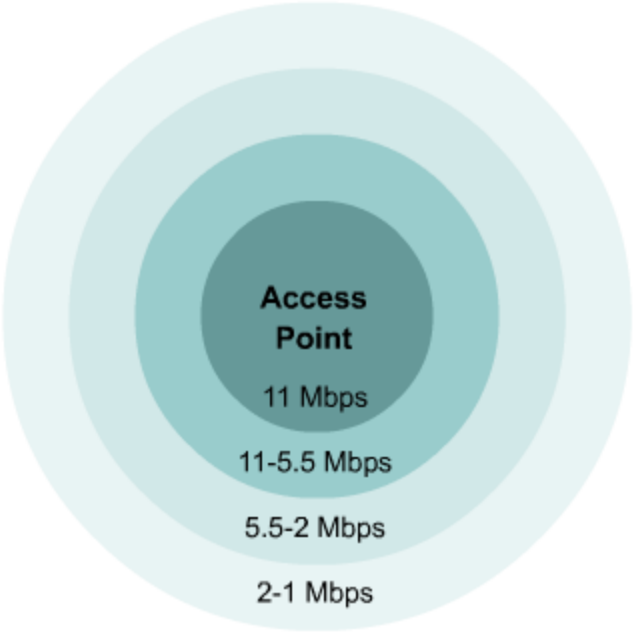



Cisco 827-4V router
cổng ASDL
đầu cắm line
điện thoại

gateway

Mạng không dây




Access Point
11 Mbps
11-5.5 Mbps
5.5-2 Mbps
2-1 Mbps

Không dây

CHƯƠNG 2
QUẢN TRỊ THIẾT BỊ MẠNG

Bộ môn Công nghệ thông tin
Trường Đại học Kinh tế Quốc dân

Nội dung chính

- Card giao tiếp mạng (NIC)
- Bộ chuyển tiếp (Repeater)
- Bộ tập trung (Hub)
- Bộ điều chế và giải điều chế (Modem)
- Cầu nối (Bridge)
- Bộ chuyển mạch (Switch)
- Bộ định tuyến (Router)
- Cổng nối (Gateway)

1. Card giao tiếp mạng (NIC)

- **Là thiết bị thông dụng nhất để nối máy tính với mạng.**
- **Mỗi card mạng có một địa chỉ vật lý duy nhất (địa chỉ MAC, 48 bits).**
- **Làm việc ở tầng 2 (mô hình OSI).**
- **Gồm một bộ thu/phát tín hiệu, bộ xử lý, các bộ đệm, khuếch đại...và đầu nối phù hợp với cáp đường truyền**
  - *Cáp đồng trục: đầu nối BNC*
  - *Cáp xoắn đôi: đầu nối RJ-45*

1. NIC...

- **Chức năng**
  - Truyền dữ liệu:
    - *Nhận dữ liệu từ máy tính*
    - *Tổ chức thành các frame*
    - *Chuyển thành tín hiệu đường truyền*
  - Nhận dữ liệu:
    - *Nhận tín hiệu đường truyền*
    - *Tổ chức thành các frame*
    - *Xử lý các frame (kiểm tra địa chỉ Mac, xử lý lỗi, xử lý luồng...)*
    - *Chuyển tiếp cho máy tính xử lý*

1. NIC...

- **Phân loại**
  - Theo chuẩn mạng
    - *Hữu tuyến : Ethernet (IEEE 802.3), Token bus (IEEE 802.4), Token ring (IEEE 802.5), FDDI/CDDI, 100VG-AnyLAN (IEEE 802.11)*
    - *Vô tuyến : Wi-Fi (IEEE 802.11), BlueTooth (IEEE 802.15), WiMAX (IEEE 802.16), WWAN (GRRS, UTMS, EV-DO)*
  - Theo tốc độ truyền (ví dụ Ethernet)
    - *Ethernet : 10 Mbps*
    - *Fast Ethernet : 100 Mbps*
    - *Gigabit Ethernet : 1.000 Mbps*
    - *10 Gigabit Ethernet : 10.000 Mbps*

1. NIC...

- **Phân loại...**
  - Theo loại môi trường truyền
    - *Hữu tuyến : Cáp xoắn đôi, đồng trục, cáp quang*
    - *Vô tuyến : Radio, viba, hồng ngoại*
  - Theo chuẩn khe cắm
    - *ISA, PCI, USB, PCMCIA (PC card, CardBus), Express Card, FireWire (IEEE 1394)*
    - *Onboard*

1. NIC...

Đầu nối BNC

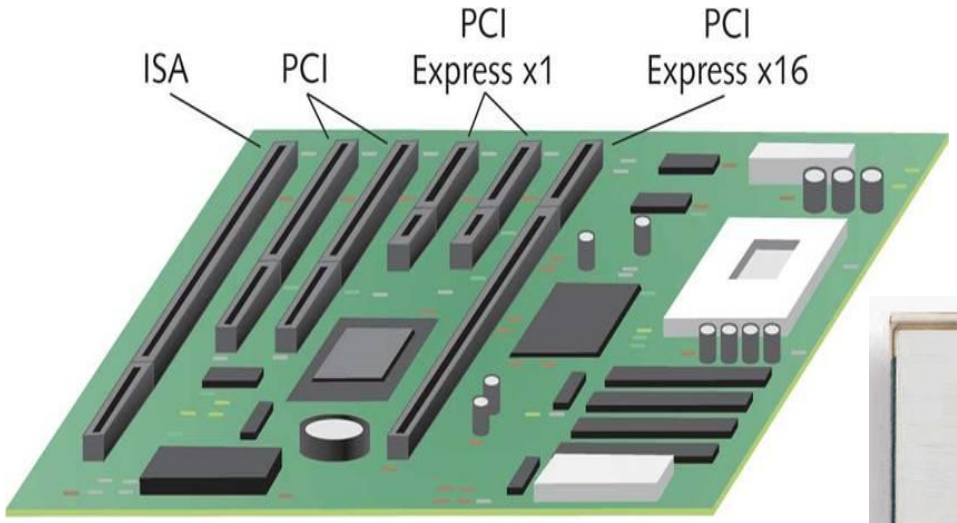
Đầu nối RJ-45

1. NIC...

NIC theo chuẩn ISA

NIC theo chuẩn PCI

1. NIC...


ISA
PCI
PCI
Express x1
PCI
Express x16


3Com Megahertz
LAN
10/100 LAN PC Card
with XJACK Connector
3Com
INSERT THIS END
Model 3CXFE574BT

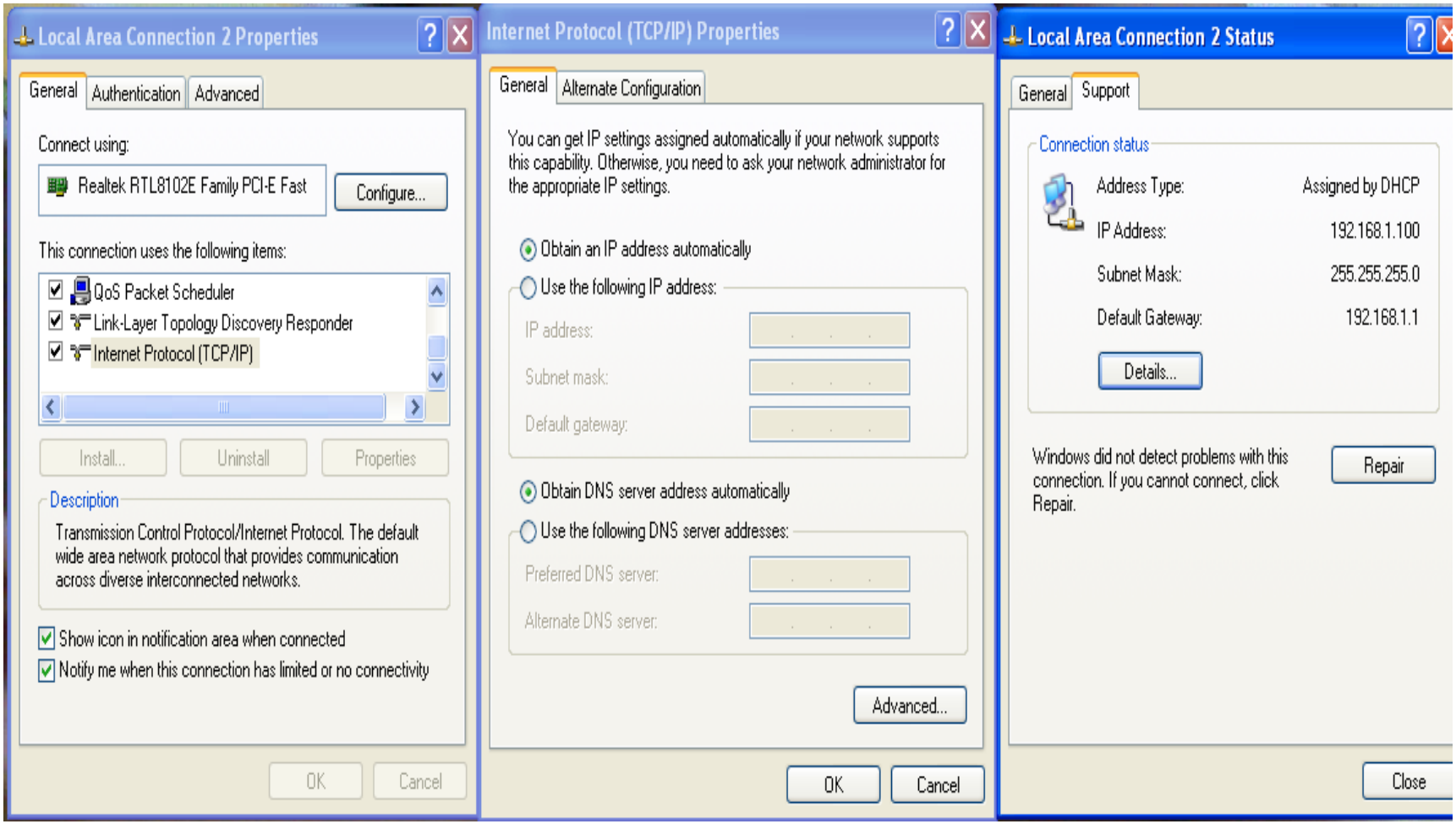
1. NIC...


Wireless NIC
NETGEAR
54 Mbps Wireless PCI Adapter
BELKIN
EZ Connect TURBO
22 Mbps Wireless
Cardbus Adapter
SMC
SMC

1. NIC...

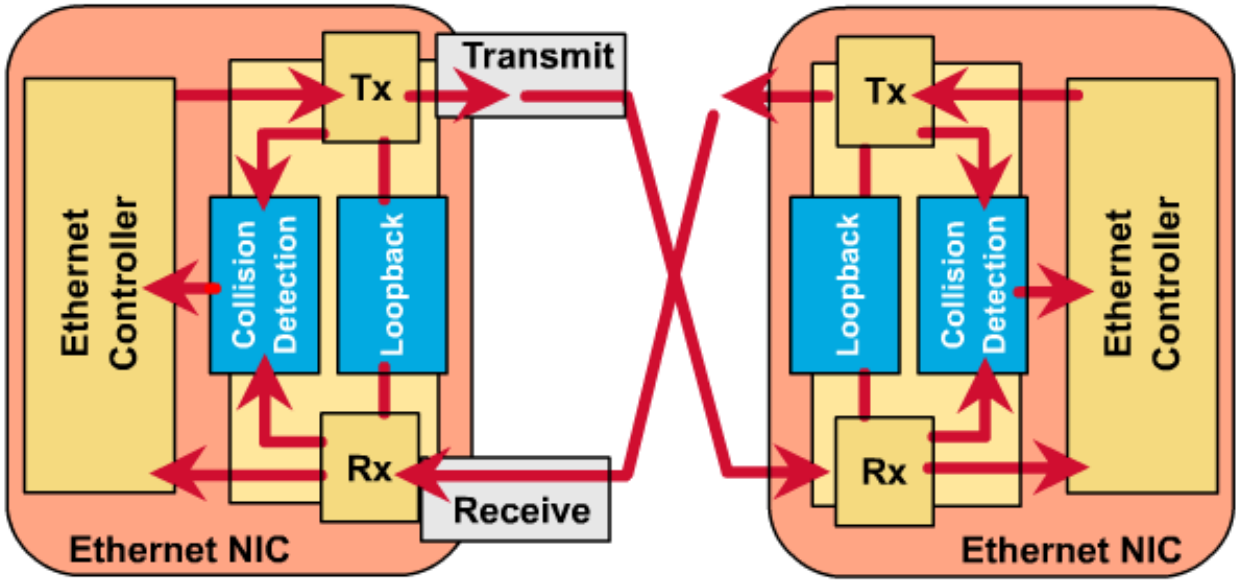
- **Lắp đặt card mạng**
  - Tham khảo tài liệu hướng dẫn kèm theo card mạng
  - Nếu lắp đặt nhiều card mạng phải cấu hình tham số khác nhau cho mỗi card mạng
- **Cài đặt driver và cấu hình cho card mạng**
  - Driver phụ thuộc vào loại hệ điều hành và loại card mạng
  - Được cung cấp kèm theo card mạng hoặc có sẵn trong hệ điều hành

1. NIC...


Local Area Connection 2 Properties
General
Authentication
Advanced
Connect using:
Realtek RTL8102E Family PCI-E Fast
Configure...
This connection uses the following items:
QoS Packet Scheduler
Link-Layer Topology Discovery Responder
Internet Protocol (TCP/IP)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
Notify me when this connection has limited or no connectivity
OK
Cancel
Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel
Local Area Connection 2 Status
General
Support
Connection status
Address Type:
Assigned by DHCP
IP Address:
192.168.1.100
Subnet Mask:
255.255.255.0
Default Gateway:
192.168.1.1
Details...
Windows did not detect problems with this connection. If you cannot connect, click Repair.
Repair
Close

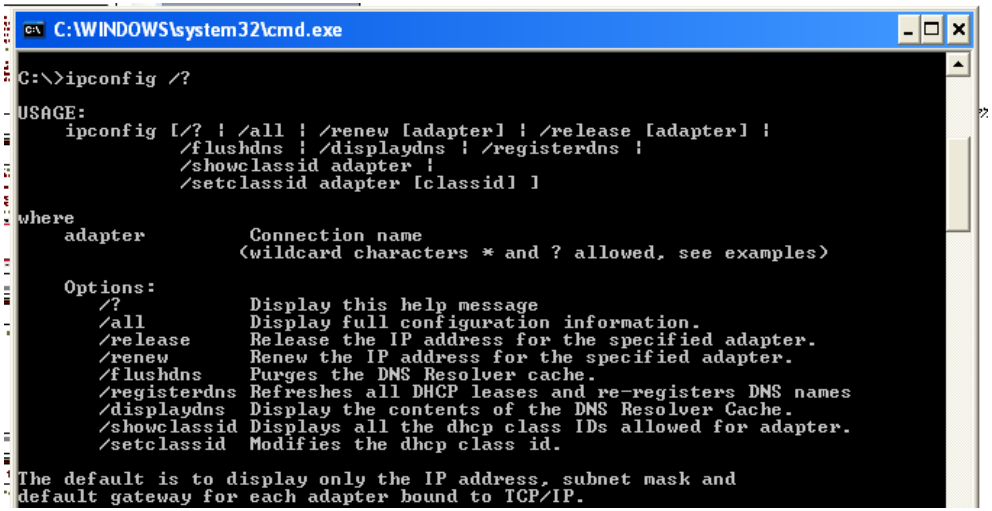
1. NIC...

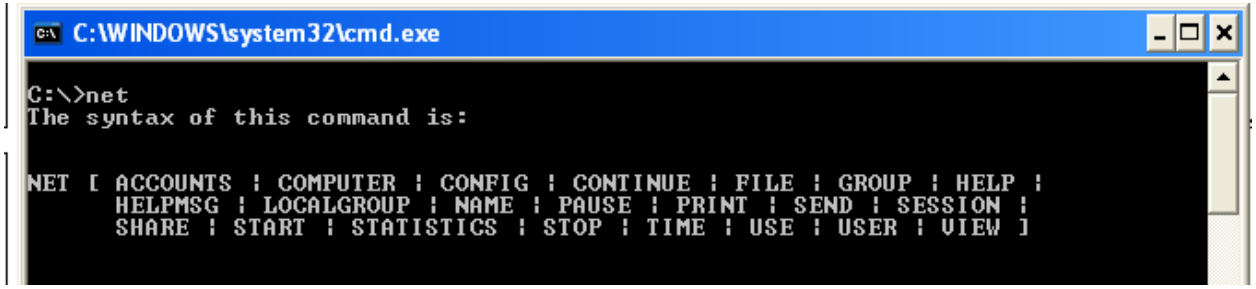
- **Trạng thái đèn LED trên card mạng**
  - **ACT**: Đèn chớp là đang truyền dữ liệu. Đèn sáng là đang truyền liên tục.
  - **LNK**: Đèn sáng là có kết nối với cáp và thiết bị mạng (hub, switch, …)
  - **TX**: Đèn sáng là đang gửi dữ liệu ra đường truyền
  - **RX**: Đèn sáng là đang nhận dữ liệu từ đường truyền
- **Card mạng có thể có từ 2 đến 4 đèn LED tuỳ loại.**



1. NIC...

- Các lệnh kiểm tra
  - ipconfig
  - ping
  - pathping
  - tracert
  - route
  - net
  - netstat





1. NIC...

```
C:\>ping www.yahoo.com

Pinging any-fp.wa1.b.yahoo.com [98.137.149.56] with 32 bytes of data:

Reply from 98.137.149.56: bytes=32 time=260ms TTL=50
Reply from 98.137.149.56: bytes=32 time=216ms TTL=50
Reply from 98.137.149.56: bytes=32 time=216ms TTL=50
Reply from 98.137.149.56: bytes=32 time=247ms TTL=50

Ping statistics for 98.137.149.56:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 216ms, Maximum = 260ms, Average = 234ms

C:\>tracert www.yahoo.com

Tracing route to any-fp.wa1.b.yahoo.com [98.137.149.56]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2    23 ms    23 ms    24 ms  localhost [123.16.144.1]
  3    23 ms    23 ms    22 ms  static.vnpt-hanoi.com.vn [222.252.96.105]
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *      503 ms   503 ms  localhost [123.31.2.81]
  8     *      503 ms   516 ms  xe-8-0-0.lax20.ip4.tinet.net [77.67.79.241]
  9   503 ms   503 ms   503 ms  xe-1-2-0.sjc10.ip4.tinet.net [89.149.184.150]
 10   215 ms   216 ms   215 ms  ge-0-3-9.pat1.sjc.yahoo.com [216.115.96.10]
 11   217 ms   498 ms   216 ms  ae-1-d160.msr1.sp1.yahoo.com [216.115.107.61]
 12   216 ms   218 ms   218 ms  te-9-1.bas2-1-prd.sp2.yahoo.com [67.195.128.245]

 13   217 ms   216 ms   219 ms  ir1.fp.vip.sp2.yahoo.com [98.137.149.56]

Trace complete.

C:\>
```

2. Bộ chuyển tiếp (Repeater)

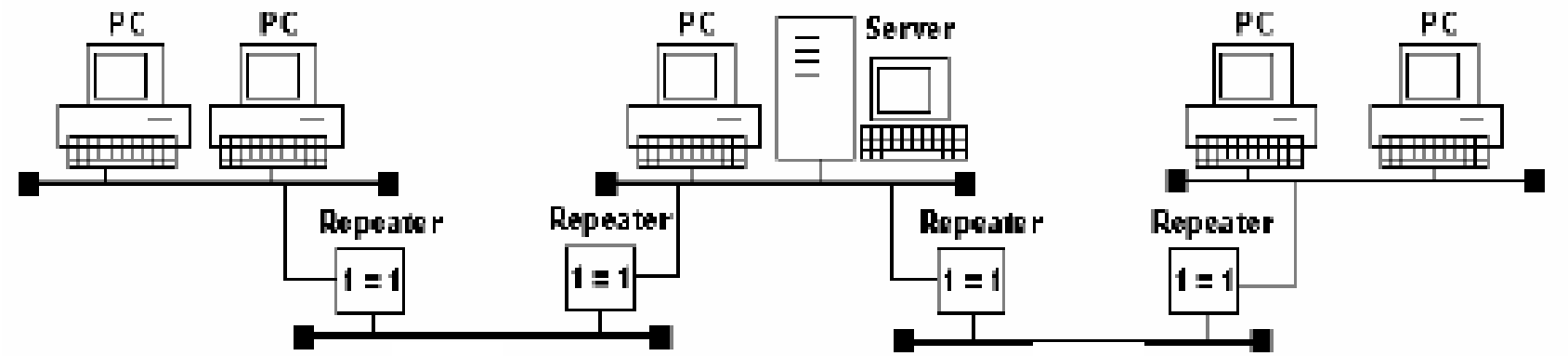
- Chức năng: Nhận, khuếch đại và chuyển tiếp tín hiệu
- Không lọc và xử lý dữ liệu
- Mở rộng phạm vi đường truyền mạng
- Thường dùng trong mạng dạng bus.

2. Repeater...

- **Làm việc ở tầng 1 (mô hình OSI).**
- **Phân loại:**
  - ***Repeater điện:*** liên kết với hai đầu đều là cáp điện
  - ***Repeater điện quang:*** liên kết với một đầu cáp quang và một đầu là cáp điện

2. Repeater...

Luật 5-4-3



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

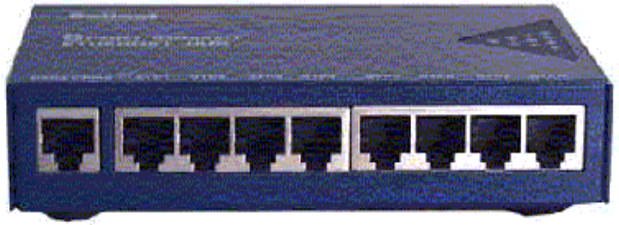
3. Bộ tập trung (Hub)

- Còn gọi là bộ chuyển tiếp nhiều cổng (multiport repeater)
- Làm việc ở tầng 1 (mô hình OSI).
- Không lọc và xử lý dữ liệu
- Thường dùng để nối các máy tính thành một mạng LAN theo topo hình sao
- Mỗi một cổng cho phép nối một máy tính vào mạng
- Chuyển tín hiệu nhận được từ một cổng đến tất cả các cổng còn lại (***Vấn đề bảo mật?***)
- Ưu điểm : Giá rẻ, dễ lắp đặt, dễ mở rộng mạng, không cần cấu hình.

3. Hub...

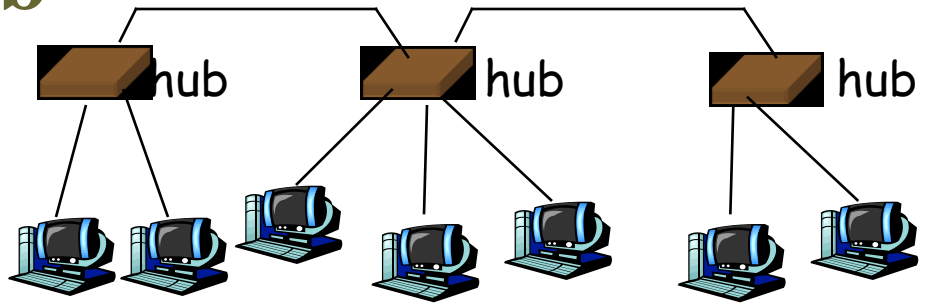
- **Phân loại**
  - Theo chức năng
    - *Hub thụ động (Passive hub)*
    - *Hub chủ động (Active hub)*
    - *Hub thông minh (Intelligent hub)*
    - *Hub đơn (Stand-alone hub)*
    - *Hub ghép tầng (Stackable hub)*
    - *Hub dạng module (modular hub)*
  - Theo tốc độ truyền
    - *10 Mbps, 100 Mbps, 1.000 Mbps*
    - *Auto sense 10/100, 10/100/1.000*

3. Hub...

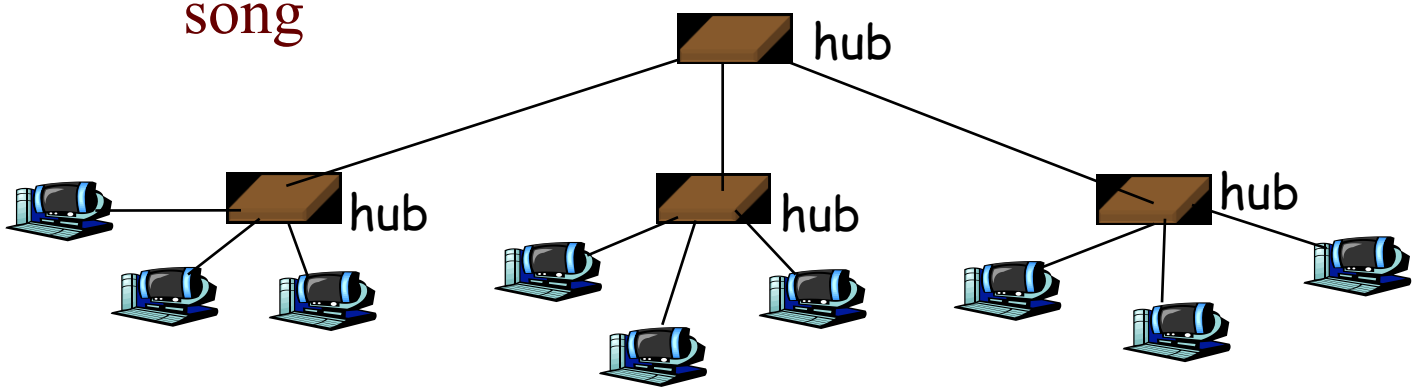


3. Hub...

Ví dụ: đấu nối hub



- Nối liên tiếp các hub lại với nhau: Cần tuân thủ luật 5-4-3, đảm bảo tín hiệu đi từ máy tính này đến máy tính khác trong mạng không đi qua nhiều hơn 4 hub.
- Khi sô lượng hub nhiều hơn 4: sử dụng một hub làm xương sống

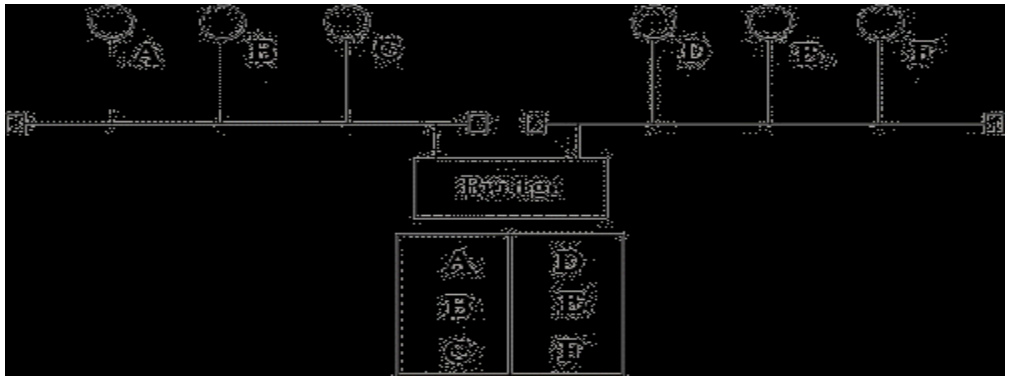


4. Bộ điều chế và giải điều chế (Modem)

- **Kết nối các máy tính thông qua đường điện thoại**
- **Phân loại:**
  - *Modem trong: gắn vào bo mạch chính của máy tính*
  - *Modem ngoài: là một thiết bị độc lập*
- **Modem quay số (dial-up):**
  - *Chuyển đổi tín hiệu số thành tín hiệu tương tự và ngược lại.*
  - *Tốc độ thấp: ~ 56Kbps*
- **Modem ADSL:**
  - *Gửi và nhận các tín hiệu số*
  - *Sử dụng kỹ thuật điều chế, tách một đường điện thoại thành 3 kênh: gửi dữ liệu, nhận dữ liệu và nói chuyện qua điện thoại.*
  - *Tốc độ upload: ~64 đến 640Kbps; download: ~1,5 đến 8Mbps*

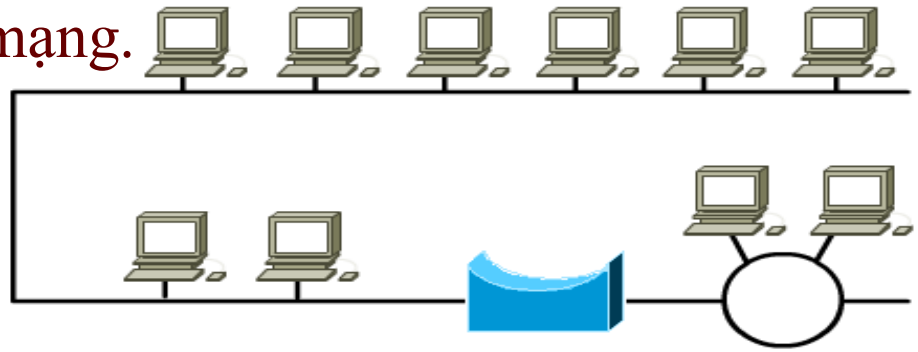
5. Cầu nối (Bridge)

- **Làm việc ở tầng 2 (mô hình OSI).**
- **Chức năng**
  - Kết nối các đoạn mạng (segment) trong một mạng
  - Cho phép nối hai mạng giống nhau hoặc khác nhau, khác chuẩn và khác tốc độ truyền.
  - Chọn lọc và chuyển tiếp gói tin từ mạng này sang mạng khác
  - Thông minh hơn trong việc quyết định có chuyển tín hiệu qua đoạn mạng kia hay không
  - Lọc lưu lượng dựa trên địa chỉ MAC. Tăng hiệu suất mạng bởi nó loại trừ lưu lượng mạng không cần thiết và giảm sự xung đột (collision)
  - Chuyển frame giữa các đoạn mạng có giao thức tầng 2 (OSI) khác nhau



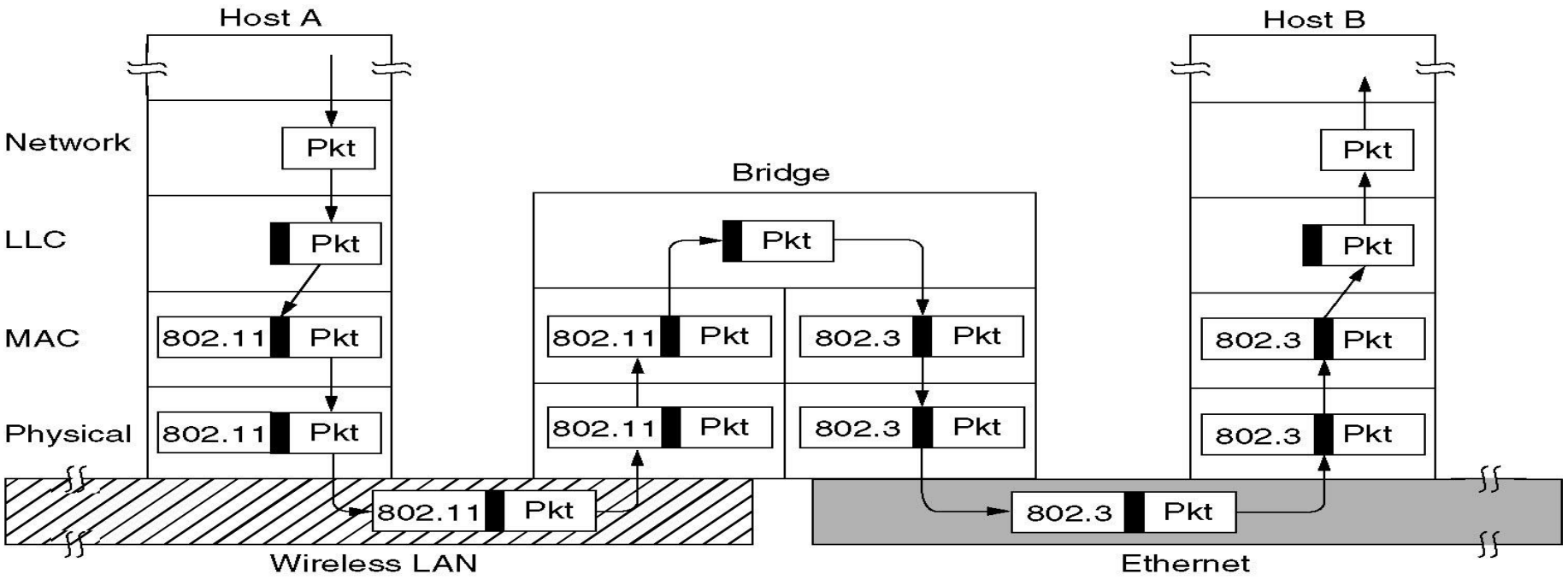
5. Bridge...

- **Lý do sử dụng:**
  - Mở rộng và ghép nối các mạng LAN nhỏ độc lập nhau.
  - Cho phép mở rộng mạng mà không phụ thuộc luật 5-4-3
  - Ghép nối các mạng trên 1 vùng địa lý lớn (vd : nhiều toà nhà cách biệt nhau).
  - Phân chia 1 mạng lớn thành nhiều mạng nhỏ hơn để giảm lưu lượng và xung đột trên mạng.
  - Kích thước mạng vượt quá qui định cho phép (chiều dài cáp, số lượng Node) cần chia ra nhiều phân đoạn mạng.
  - Tăng độ tin cậy trên mạng.
  - Tăng độ an toàn trên mạng.



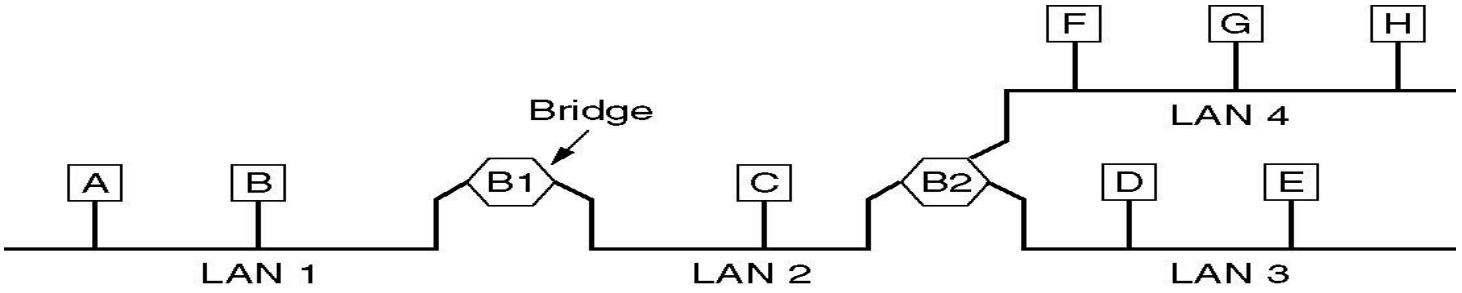
5. Bridge...

- Cơ chế kết nối các mạng có chuẩn khác nhau



5. Bridge...

- **Quyết định việc truyền tiếp 1 frame :**
  - Căn cứ vào **địa chỉ MAC** của máy đích trong frame để quyết định việc truyền tiếp 1 frame.
  - Nếu máy đích cùng mạng với máy nguồn: bỏ không truyền tiếp frame này.
  - Nếu máy đích khác mạng với máy nguồn: truyền frame đến mạng đích tương ứng.
  - Để xác định máy nào thuộc mạng nào cần khai báo trước trong bảng định tuyến (routing table) của cầu nối.
- **Nhược điểm :**
  - Người quản trị mạng phải cập nhật bảng định tuyến của tất cả các cầu nối khi có sự thay đổi cấu trúc mạng.

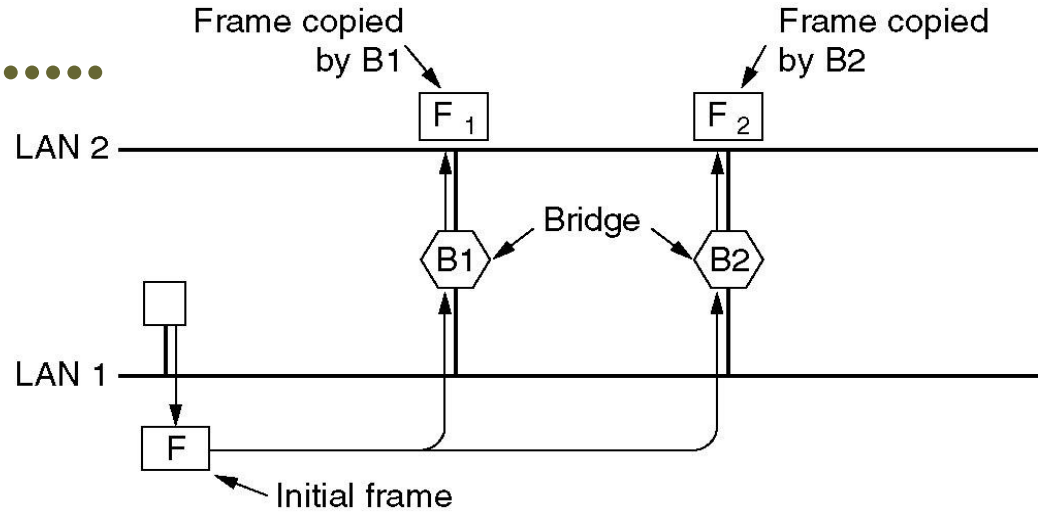


5. Bridge...

- **Cầu nối trong suốt (Transparent bridge)**
  - Người sử dụng không cần khai báo bảng định tuyến.
  - Khi nhận 1 frame, cầu nối căn cứ vào địa chỉ nguồn để biết máy nào thuộc mạng nào và cập nhật vào bảng định tuyến.
  - Thủ tục định tuyến : Vẫn căn cứ vào địa chỉ đích. Nếu biết máy đích thuộc mạng nào sẽ chỉ truyền frame đến lối ra tương ứng. Nếu chưa biết máy đích thuộc mạng nào sẽ truyền frame đến mọi lối ra còn lại.

5. Bridge...

- **Cầu nối trong suốt .....**
  - Ưu điểm
    - *Cầu nối hoạt động một cách tự động, không cần sự khai báo của con người.*



  - Nhược điểm
    - *Nếu di chuyển 1 máy từ mạng này sang mạng khác cầu nối sẽ định tuyến sai.*
      - Cách khắc phục: Qui định thời gian có giá trị của các địa chỉ trong bảng định tuyến. Nếu quá thời gian này địa chỉ sẽ mất giá trị, bắt buộc cầu nối phải cập nhật lại địa chỉ đó trong bảng định tuyến (Vd mỗi 300s cập nhật 1 lần).
    - *Khi kết nối các mạng LAN bằng nhiều cầu nối (ví dụ để tăng độ tin cậy) sẽ tạo ra vòng lặp (loop) dẫn đến khả năng truyền trùng lặp dữ liệu trên mạng*

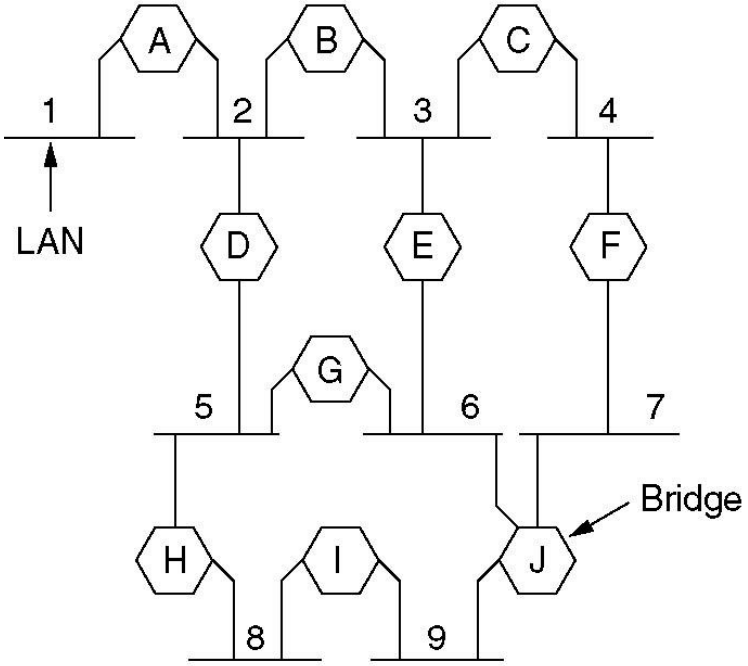
5. Bridge...

Cầu nối dạng cây bao trùm

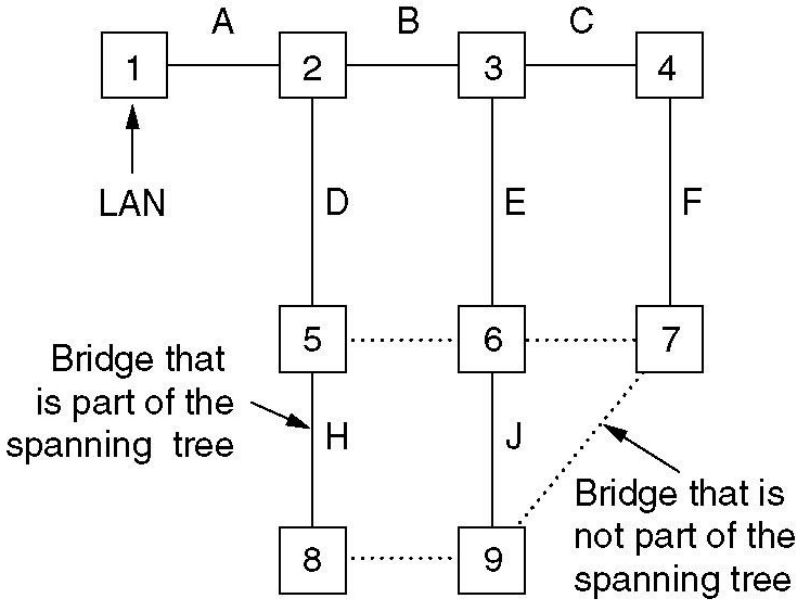
- Sử dụng giao thức cây bao trùm **STP** (Spanning Tree Protocol) theo chuẩn **IEEE 802.1D** để khắc phục tình trạng vòng lặp.
- Các cầu nối sẽ trao đổi thông tin **BPDU** (Bridge Protocol Data Units) lẫn nhau để xây dựng cây bao trùm:
  - *Chọn 1 cầu nối làm nút gốc.*
  - *Xây dựng đường đi ngắn nhất đến mọi cầu khác (theo tốc độ truyền).*
  - *Nếu 1 cầu nối hay LAN bị hỏng sẽ phải xây dựng lại cây bao trùm mới (kiểm tra sau mỗi 30-50s).*
  - *Các cầu không hoạt động sẽ ở trạng thái dự phòng.*
- Chuẩn **IEEE 802.1W** dùng giao thức **RSTP** (Rapid STP) cải tiến STP bằng cách chuyển sang 1 cây dự phòng chỉ sau 1s bị sự cố.

5. Bridge...

- Cầu nối dạng cây bao trùm...



(a)

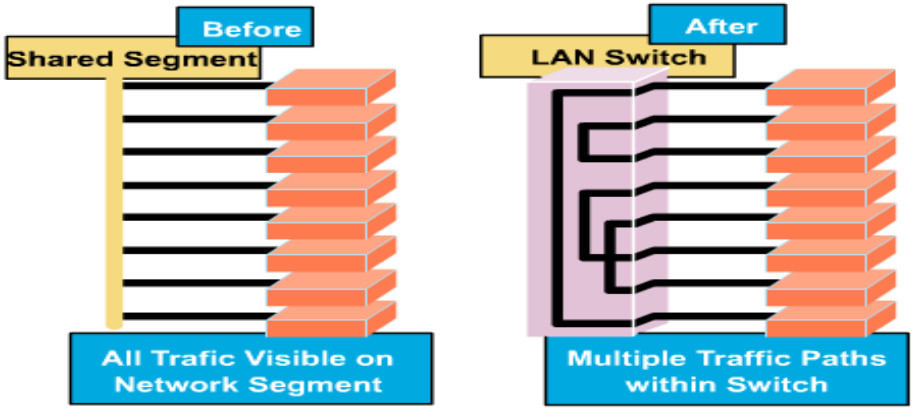


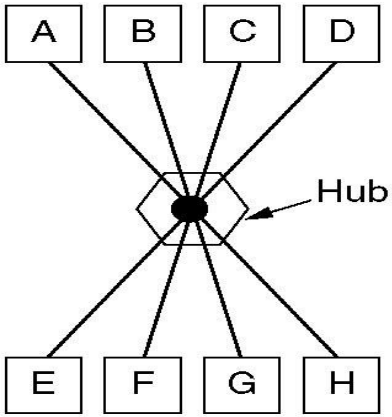
(b)

6. Bộ chuyển mạch (Switch)

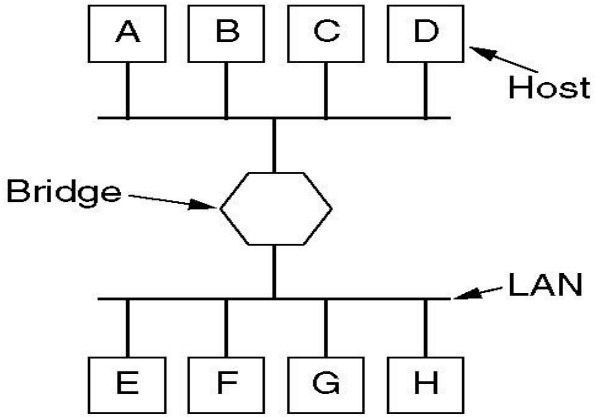
- Còn gọi là cầu nối nhiều cổng
- Làm việc ở tầng 2 (mô hình OSI).
- Cơ chế làm việc của switch hoàn toàn tương tự như bridge: Dùng địa chỉ MAC để quản lý lưu lượng truyền giữa các port trên switch.
- Ưu điểm : Giảm xung đột trên mạng so với kết nối bằng Hub. Hiện nay switch được sử dụng rộng rãi, thay thế cho các hub trước đây.

6. Switch...

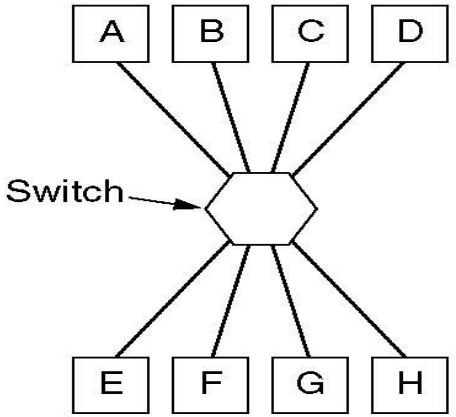

Before
Shared Segment
All Trafic Visible on Network Segment
After
LAN Switch
Multiple Traffic Paths within Switch


A
B
C
D
Hub
E
F
G
H

(a)


A
B
C
D
Host
Bridge
LAN
E
F
G
H

(b)


A
B
C
D
Switch
E
F
G
H

(c)

6. Switch...

Phân loại switch theo chế độ hoạt động

- Cut-through mode: Chỉ đọc địa chỉ MAC đích và chuyển frame dữ liệu ra port đích.
  - *Ưu điểm : Tốc độ xử lý nhanh, thời gian trễ nhỏ.*
  - *Nhược điểm : không kiểm soát lỗi và lưu lượng, chỉ sử dụng cho Ethernet cùng tốc độ các port.*
- Store and Forward Mode : Switch đọc toàn bộ nội dung 1 frame dữ liệu, kiểm tra lỗi rồi mới truyền ra port đích.
  - *Ưu điểm : Truyền dữ liệu tin cậy hơn, truyền được giữa các port khác tốc độ và khác chuẩn.*
  - *Nhược điểm : Tốc độ xử lý chậm, thời gian trễ lớn.*

6. Switch...

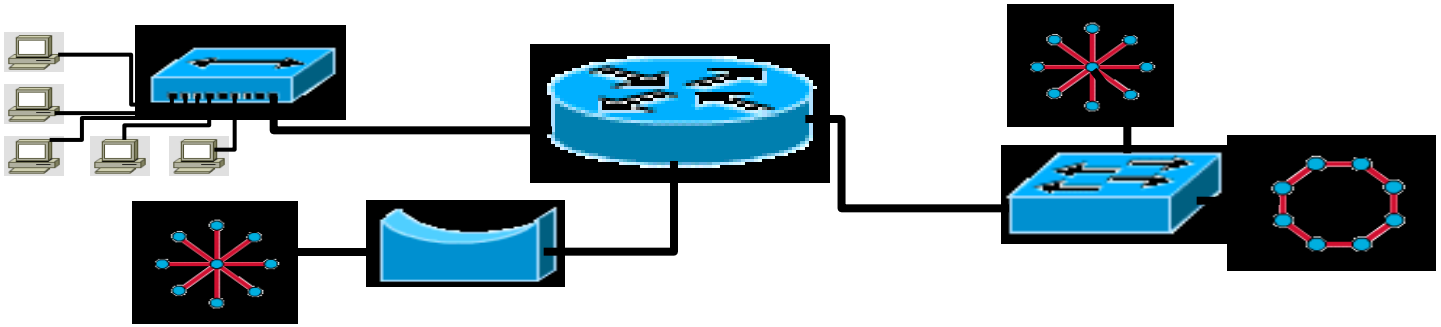
- **Mạng LAN ảo (Virtual LAN)**
  - Thông thường để tạo các LAN khác nhau chỉ cần kết nối máy tính vào các Hub/ switch khác nhau. Các thiết bị Switch cho phép cấu hình chỉ 1 nhóm port được phép truyền dữ liệu lẫn nhau. Mỗi nhóm coi như là 1 LAN riêng (VLAN) cùng chạy trên 1 Switch vật lý.
  - Để kết nối các VLAN cần sử dụng Router. Một số Switch được thiết kế có thêm tính năng routing giữa các VLAN được gọi là Switch L3 (Switch Layer 3).

6. Switch...

- **Switch mức cao**
  - Switch chuẩn làm việc trong tầng 2 (mô hình OSI) tương tự như cầu nối Bridge. Chuyển mạch dựa trên địa chỉ MAC.
  - Switch Layer 3: Cho phép phân chia VLAN và định tuyến giữa các VLAN, không cần 1 Router để kết nối các VLAN. Chuyển mạch dựa trên địa chỉ mạng.
  - Switch Layer 4: Thiết bị chuyển mạch dựa trên địa chỉ dịch vụ (port).
  - Switch Layer 7: Thiết bị chuyển mạch dựa trên loại ứng dụng. Ví dụ content switching, load balancing switch.

7. Bộ định tuyến (Router)

- Hoạt động ở tầng mạng (tầng 3 mô hình OSI)
- Kết nối nhiều mạng với nhau
  - nhiều loại mạng : LAN, MAN, WAN
  - các mạng có tốc độ tuyền khác nhau
  - các mạng có giao thức khác nhau
- Quản lý lưu lượng truyền giữa các mạng dựa vào địa chỉ IP



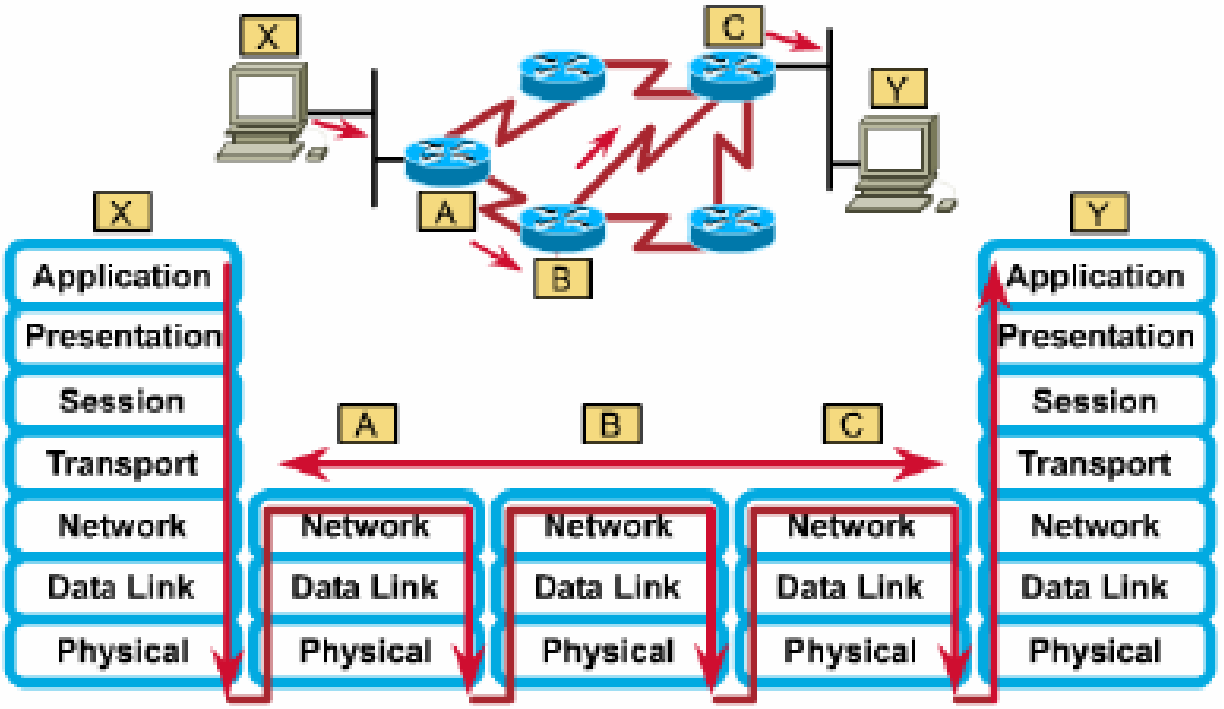
7. Router...

- **Chức năng**
  - Chức năng chính: Tìm đường đi cho các gói tin trên môi trường liên mạng (**định tuyến**) và chuyển tiếp các gói tin.
    - *Định tuyến tĩnh (**static routing**): Do người quản trị mạng khai báo sẵn trong router và không thay đổi trong quá trình sử dụng. Nếu trạng thái mạng thay đổi phải khai báo lại.*
    - *Định tuyến động (**dynamic routing**): Các router trên mạng tự trao đổi thông tin để xây dựng bảng định tuyến. Trong quá trình vận hành nếu trạng thái mạng thay đổi sẽ tự động cập nhật bảng định tuyến theo trạng thái mới.*
    - *Hai giải thuật định tuyến động thông dụng nhất hiện nay: **Distance vector** và **Link state***

7. Router...

- **Chức năng ...**
  - Các chức năng khác của Router:
    - *Kiểm soát tắc nghẽn trên mạng (congestion control)*
    - *Kiểm soát chất lượng dịch vụ trên mạng (QoS)*
    - *Gửi các thông báo lỗi trên mạng*
    - *Tách & ghép dữ liệu khi truyền qua các mạng có độ dài đơn vị dữ liệu khác nhau*
    - *Quản lý địa chỉ mạng (NAT, DHCP, ACL, cấm broadcast, tích hợp chức năng Firewall, ...)*
    - *Quản trị, giám sát, thống kê trạng thái hoạt động các mạng và đường truyền kết nối vào Router.*

7. Router...


X
C
Y
A
B
X
Y
Application
Presentation
Session
Transport
Network
Data Link
Physical
A
B
C
Network
Data Link
Physical
Network
Data Link
Physical
Network
Data Link
Physical
Application
Presentation
Session
Transport
Network
Data Link
Physical

7. Router...

- Định tuyến distance vector (vectơ khoảng cách)
  - Đầu tiên mỗi router sẽ cập nhật đường đi đến các mạng nối kết trực tiếp với mình vào bảng chọn đường.
  - Theo định kỳ (30-90 giây), một router phải gởi bảng chọn đường của mình cho các router láng giềng.
  - Khi nhận được bảng chọn đường của một láng giềng gởi sang, router sẽ tìm xem láng giềng của mình có đường đi đến một mạng nào mà mình chưa có hay một đường đi nào tốt hơn đường đi mình đã có hay không. Nếu có sẽ đưa đường đi mới này vào bảng chọn đường của mình với Next hop để đến đích chính là láng giềng này.
  - Nhược điểm :
    - *Thời gian xây dựng bảng định tuyến cho tất cả các router trên mạng chậm (còn gọi là thời gian hội tụ, convegent time)*
    - *Tốn băng thông để gửi toàn bộ bảng định tuyến đến mọi router*
    - *Xảy ra hiện tượng đếm đến vô cùng (Count-to-Infinity)*

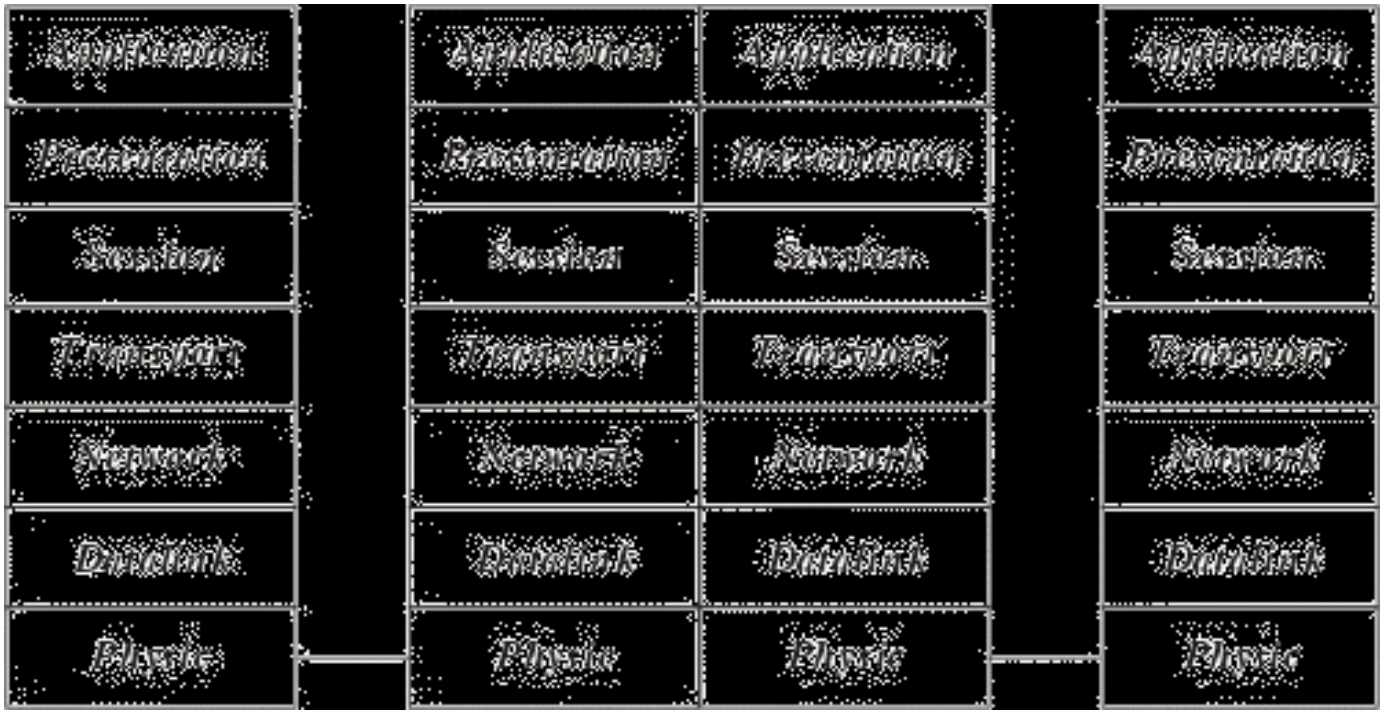
7. Router...

- Định tuyến link state (trạng thái liên kết)
  - Khắc phục các nhược điểm của distance vector
  - Nguyên tắc:
    - *Mỗi router sẽ gởi thông tin về trạng thái liên kết của mình (các mạng nối kết trực tiếp và các router láng giềng) cho tất cả các router trên toàn mạng. Các router sẽ thu thập thông tin về trạng thái liên kết của các router khác, từ đó xây dựng lại hình trạng mạng, chạy các giải thuật tìm đường đi ngắn nhất trên hình trạng mạng có được (giải thuật Dijkstra). Từ đó xây dựng bảng chọn đường cho mình.*
    - *Khi một router phát hiện trạng thái nối kết của mình bị thay đổi, nó sẽ gởi một thông điệp yêu cầu cập nhật trạng thái nối kết cho tất các các router trên toàn mạng. Nhận được thông điệp này, các router sẽ xây dựng lại hình trạng mạng, tính toán lại đường đi tối ưu và cập nhật lại bảng chọn đường của mình.*
    - *Tạo ra ít thông tin trên mạng. Tuy nhiên nó đòi hỏi router phải có bộ nhớ lớn, tốc độ tính toán của CPU phải cao.*

8. Cổng nối (Gateway)

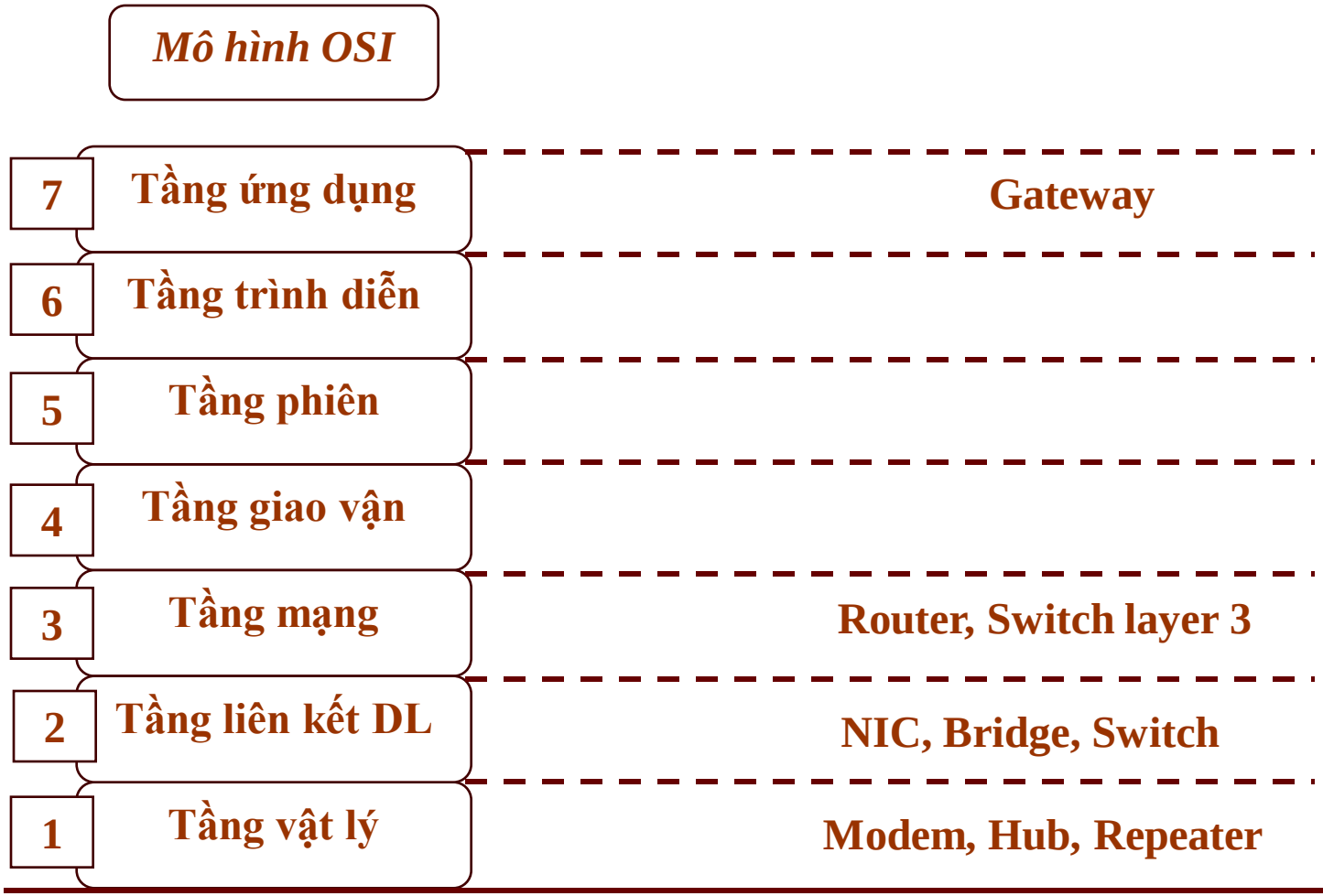
- Mục đích: Dùng để kết nối các ứng dụng với nhau
- Làm việc tầng 7 (mô hình OSI)
- Thường dùng để nối các mạng LAN với máy tính lớn
- Gateway có thể là thiết bị phần cứng hoặc phần mềm cài đặt trong máy tính.
- Hoạt động của gateway thường phức tạp hơn router nên thường chậm hơn và thường không dùng để nối LAN-LAN

8. Gateway...



Hoạt động của Gateway trong mô hình OSI

Tương đương chức năng thiết bị trong mô hình OSI



Phần mềm mô phỏng Boson Netsim

- Cài đặt
- Hướng dẫn sử dụng
- Thực hành

CÁC THIẾT BỊ MẠNG CƠ BẢN

NGUYỄN QUỐC KHÁNH
Khoa Công nghệ Thông tin

Nội dung

1. Thiết bị mạng
2. Định tuyến trong mạng
3. Phần mềm mô phỏng
4. Thực hành chương

Khái niệm Mạng máy tính

- Mạng máy tính hay hệ thống mạng (tiếng Anh: *computer network* hay *network system*), là một tập hợp các máy tính được kết nối nhau thông qua các phương tiện truyền dẫn để nhằm cho phép chia sẻ tài nguyên: máy in, máy fax, tệp tin, dữ liệu....

Tổng quan về Mạng máy tính

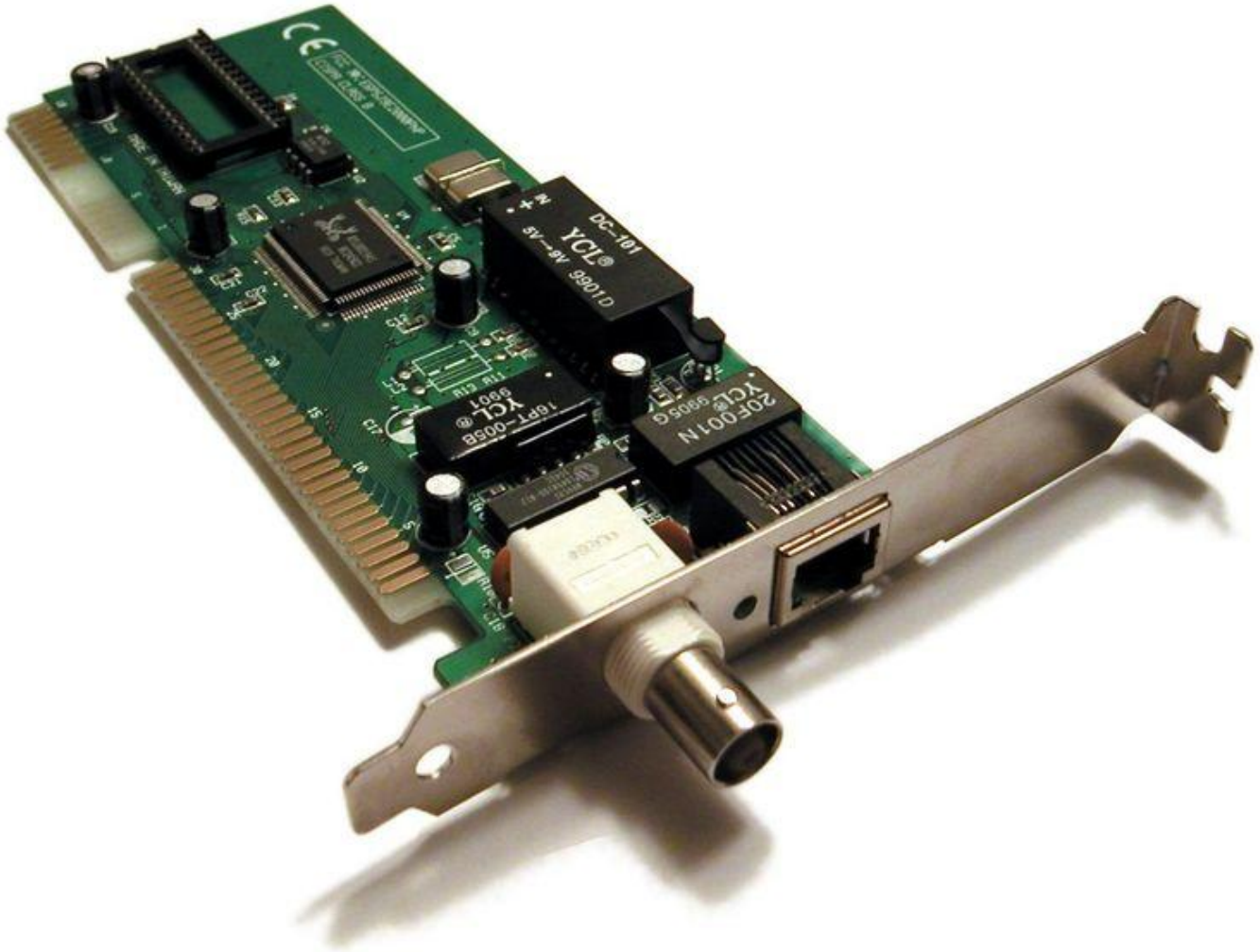
Các vấn đề xã hội

- Quan hệ giữa người với người trở nên nhanh chóng, dễ dàng và gần gũi hơn cũng mang lại nhiều vấn đề xã hội cần giải quyết như:
  - Lạm dụng hệ thống mạng để làm điều phi pháp hay thiếu đạo đức
  - Mạng càng lớn thì nguy cơ lan truyền các *phần mềm ác tính* càng dễ xảy ra.
  - Hệ thống buôn bán trở nên khó kiểm soát hơn nhưng cũng tạo điều kiện cho cạnh tranh gay gắt hơn.
  - Một vấn đề nảy sinh là xác định biên giới giữa việc kiểm soát nhân viên làm công và quyền tư hữu của họ
  - Vấn đề giáo dục thanh thiếu niên cũng trở nên khó khăn hơn vì các em có thể tham gia vào các việc trên mạng mà cha mẹ khó kiểm soát nổi.
  - Hơn bao giờ hết với phương tiện thông tin nhanh chóng thì sự tự do ngôn luận hay lạm dụng quyền ngôn luận cũng có thể ảnh hưởng sâu rộng hơn trước đây như là các trường hợp của các *phần mềm quảng cáo* (*adware*) và các *thư rác* (*spam mail)*

Thiết bị mạng cơ bản

- NIC – Network Interface Card
- Repeater/Hub
- Bridge
- Switch
- Router
- Modem

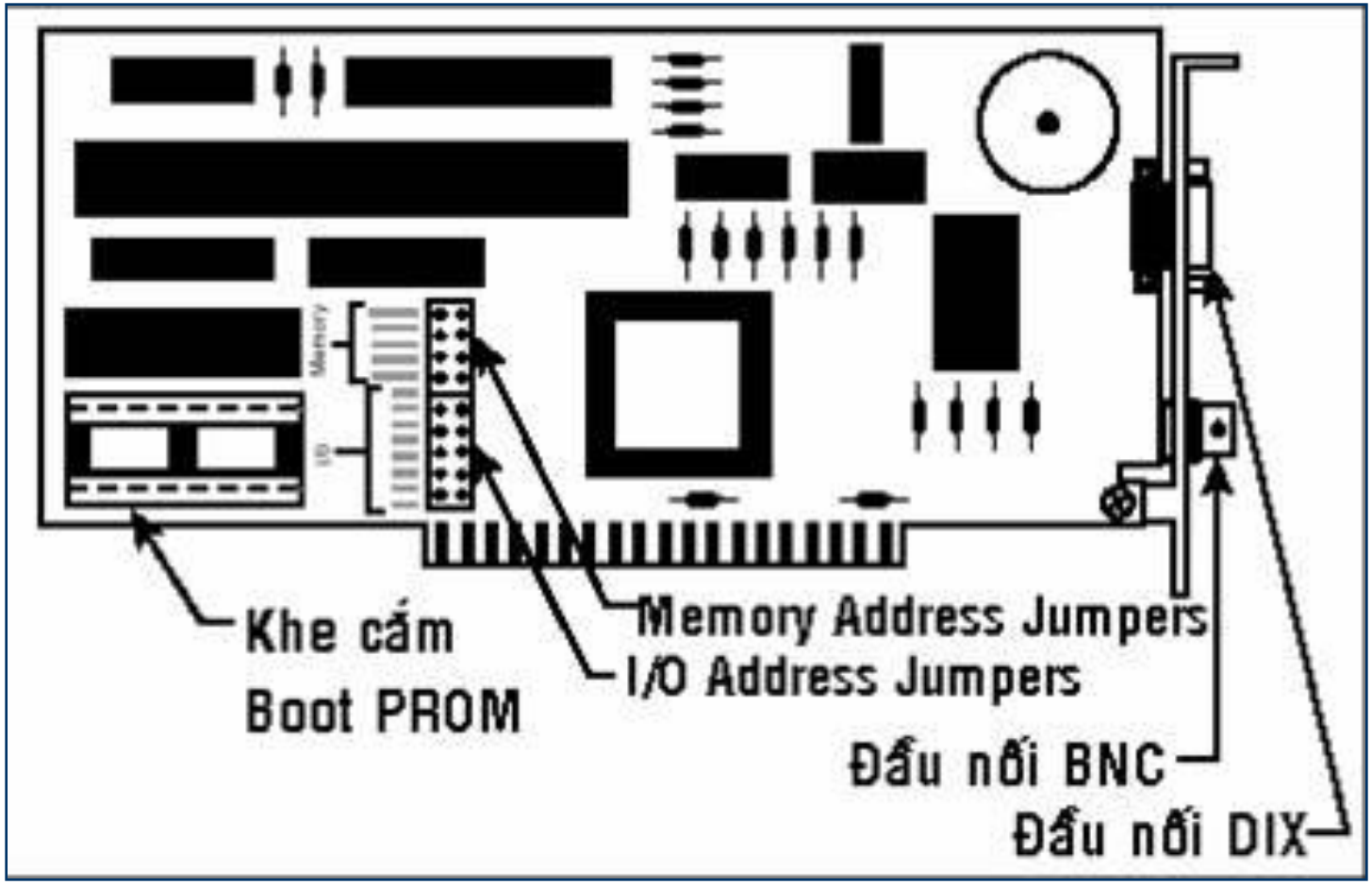
Card mạng



Khái niệm

- Cạc mạng (*network card*), hay cạc giao tiếp mạng (*Network Interface Card*), là một bản mạch cung cấp khả năng truyền thông mạng cho một máy tính.
  - Nó còn được gọi là bộ thích nghi LAN (*LAN adapter*).
  - Được cắm trong một khe (*slot*) của bản mạch chính và cung cấp một giao tiếp kết nối đến môi trường mạng.
  - Chủng loại cạc mạng phải phù hợp với môi trường truyền và giao thức được sử dụng trên mạng cục bộ.
- Nhiệm vụ:
  - Chuyển đổi các tín hiệu máy tính ra các tín hiệu trên phương tiện truyền dẫn và ngược lại
  - Gửi/nhận và kiểm soát luồng dữ liệu được truyền

Các thành phần trong card mạng

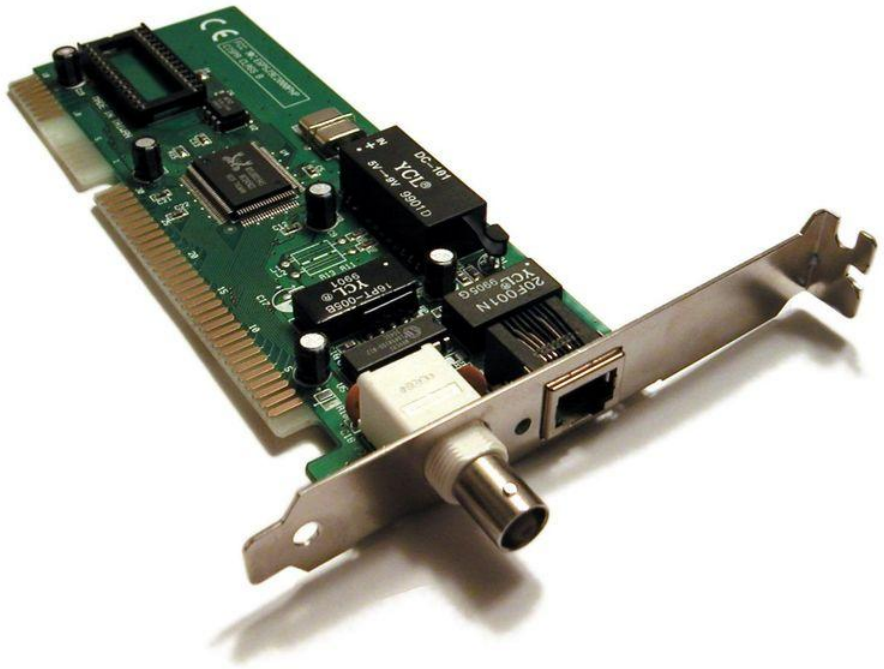


Các thành phần trong card mạng

- I/O Address: Địa chỉ bộ nhớ chính của máy tính, được dùng để trao đổi dữ liệu giữa máy tính với thiết bị (cạc mạng)
- Memory Address: Địa chỉ bộ nhớ chính của máy tính, là nơi bắt đầu vùng đệm dành cho các xử lí của cạc mạng
- DMA Channel: Cho phép thiết bị (cạc mạng) làm việc trực tiếp với bộ nhớ máy tính mà không cần thông qua CPU
- Boot PROM: Cho phép khởi động hệ thống và kết nối vào mạng
- MAC Address: Địa chỉ định danh duy nhất được IEEE cấp cho mỗi cạc mạng

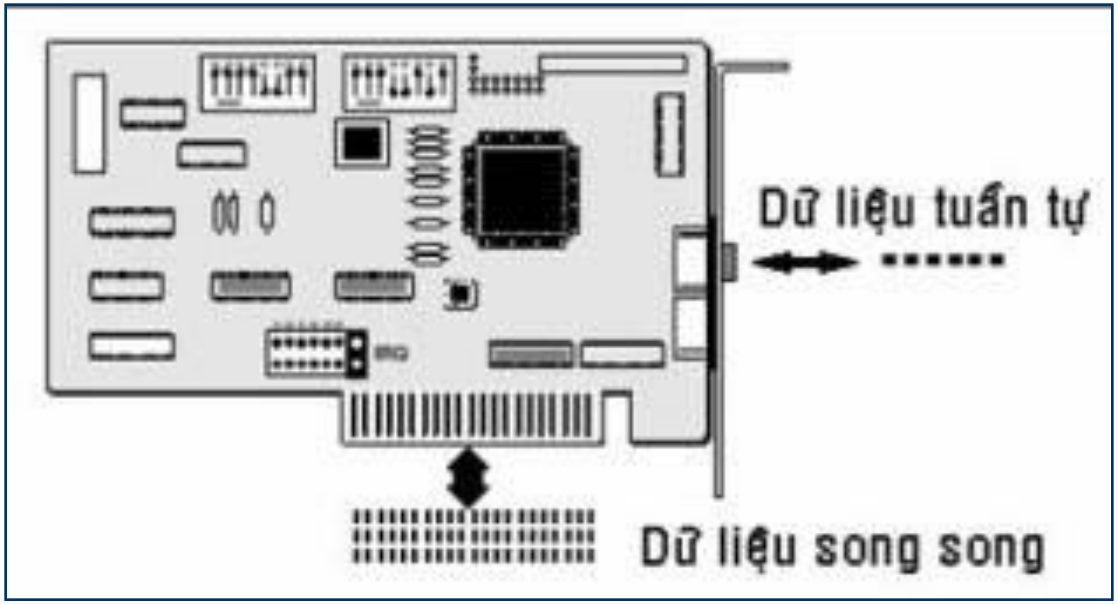
Các thành phần trong card mạng

- Đầu nối BNC: Nối cạc mạng với cáp qua đầu nối chữ T (10BASE2)
- Đầu nối RJ-45: Nối cạc mạng với cáp qua đầu nối RJ-45 (10BASE-T/100BASE-T)
- Đầu nối AUI: Nối cạc mạng với cáp (10BASE5)



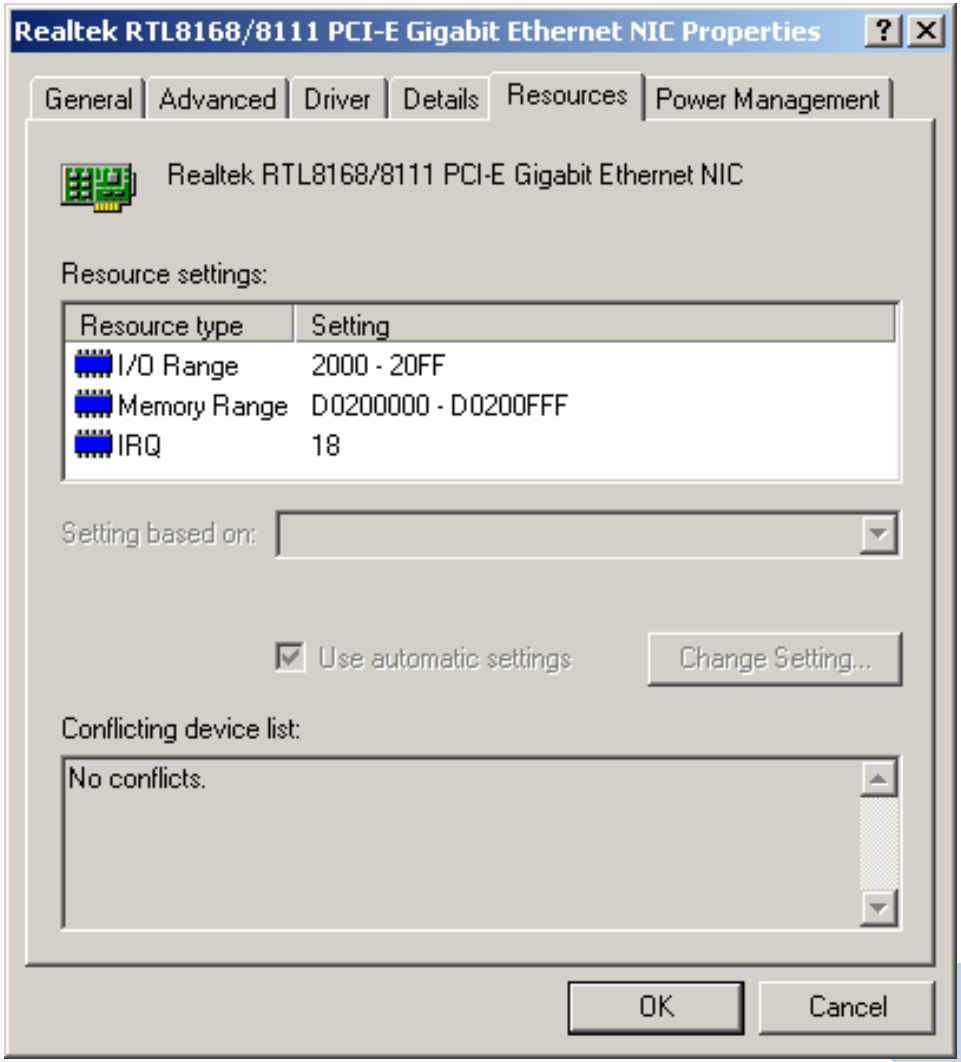
Giao tiếp qua cạc mạng

- Bộ thu phát (*transceiver*) chuyển đổi dữ liệu song song sang dữ liệu tuần tự và ngược lại.
- Dữ liệu tuần tự có thể ở dạng: tín hiệu tương tự (*analog signal*), tín hiệu số (*digital signal*) hoặc tín hiệu quang (*light signal*).



Giao tiếp qua cạc mạng

- Cạc mạng dùng một IRQ, một địa chỉ I/O và một không gian địa chỉ để làm việc với hệ điều hành

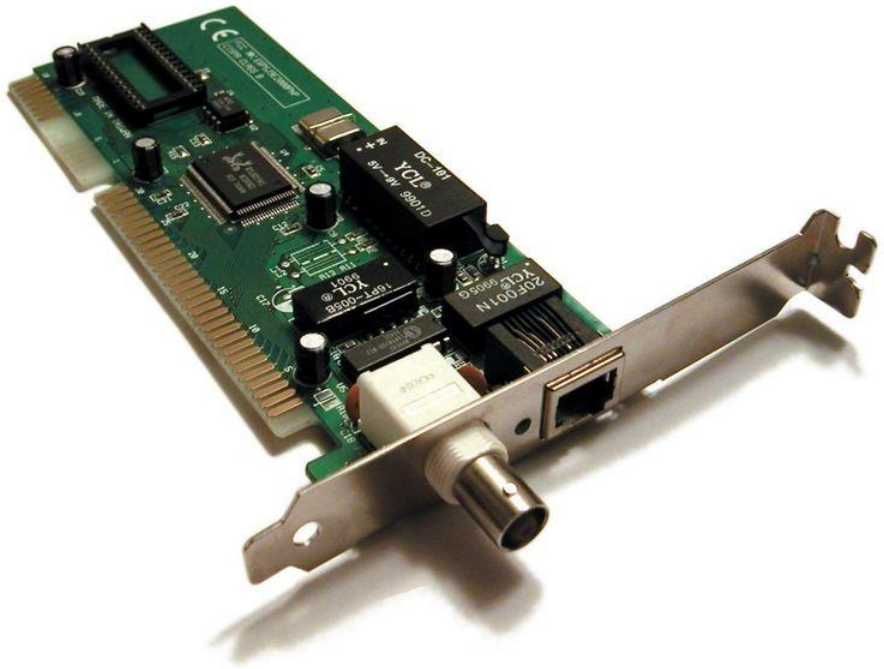


Trình điều khiển cạc mạng

- Trình điều khiển cạc mạng (*driver*) là bộ phận phần mềm trung gian có nhiệm vụ giao tiếp giữa cạc mạng và máy tính. Khi một trình điều khiển cạc mạng được nạp, nó cần phải kết hợp với một chồng giao thức.
- Phần mềm trình điều khiển cung cấp các chức năng ở tầng LLC.
- Hiện thực CSMA/CD để truy cập kênh truyền vật lý, phát hiện và xử lý đụng độ

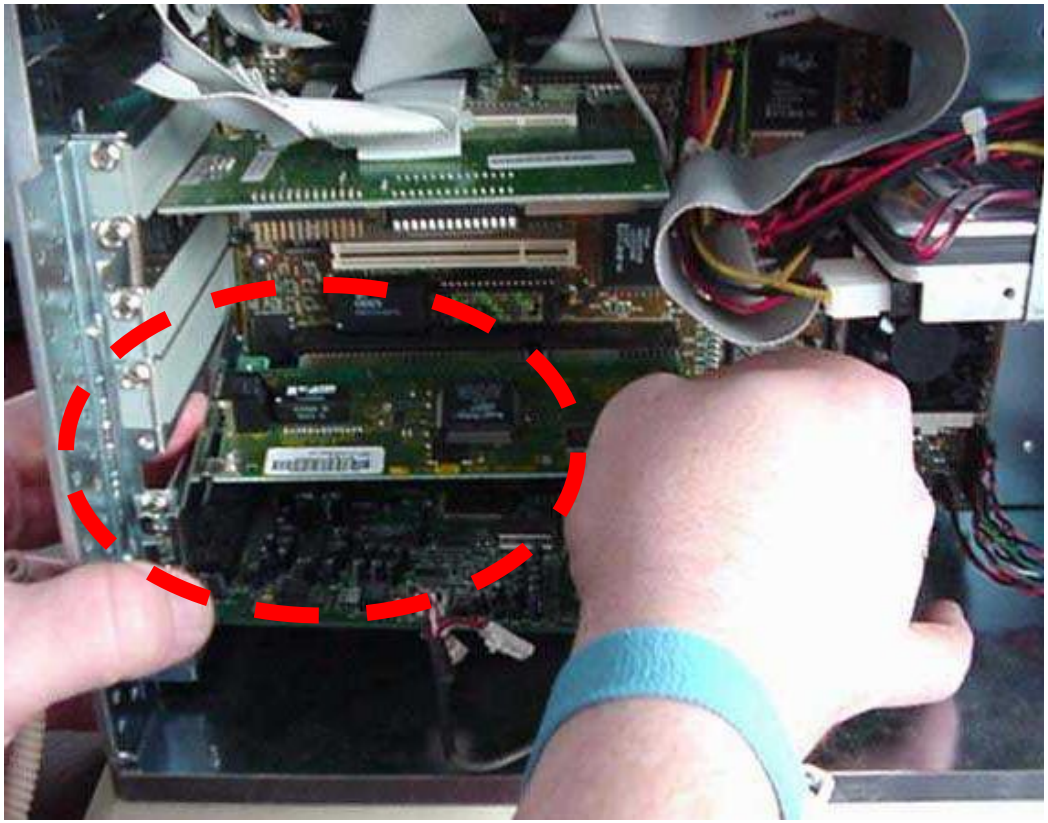
Các bước cơ bản cài đặt cạc mạng

- Khi chọn một cạc mạng, cần phải xem xét các yếu tố sau:
  - Các giao thức giao tiếp - Ethernet, Token Ring, hay FDDI...
  - Đầu nối: Cáp xoắn, cáp đồng trục, không dây hay cáp quang
  - Loại bus - PCI hay ISA



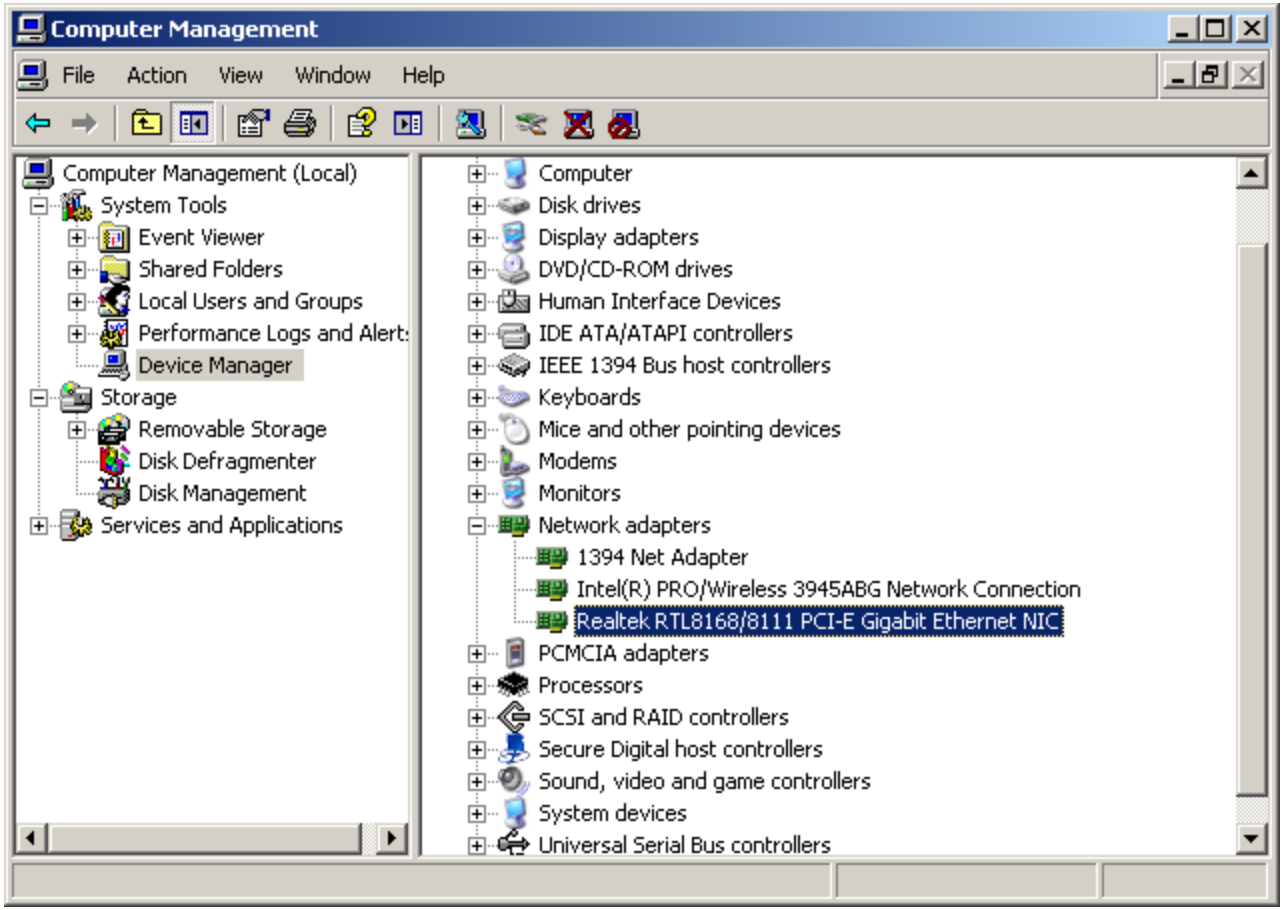
Các bước cơ bản cài đặt cạc mạng

- Các bước cơ bản cài đặt cạc mạng:
  - Gắn cạc mạng vào khe cắm mở rộng trên máy tính, thiết lập jumpers và các công tắc chuyển mạch.



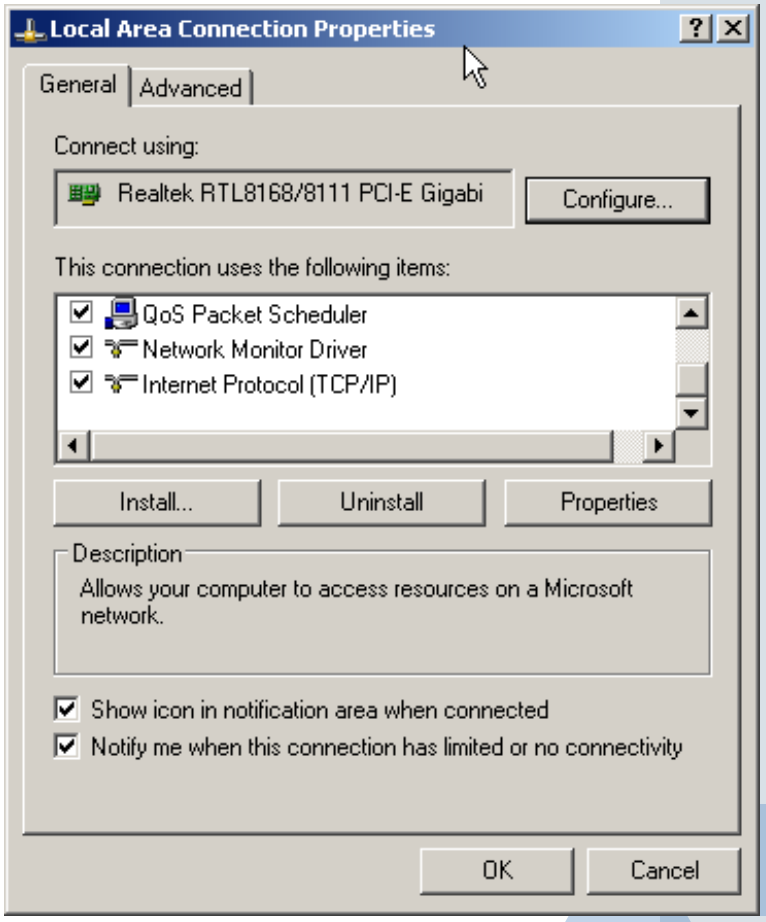
Các bước cơ bản cài đặt cạc mạng

- Cài đặt driver cạc mạng
- Định cấu hình cạc mạng để thiết bị này không tranh chấp với các thiết bị khác



Các bước cơ bản cài đặt cạc mạng

- Kết buộc cạc mạng với một giao thức truyền thông
- Gắn dây cáp vào cạc mạng
- Kiểm tra hoạt động



Các vấn đề khác

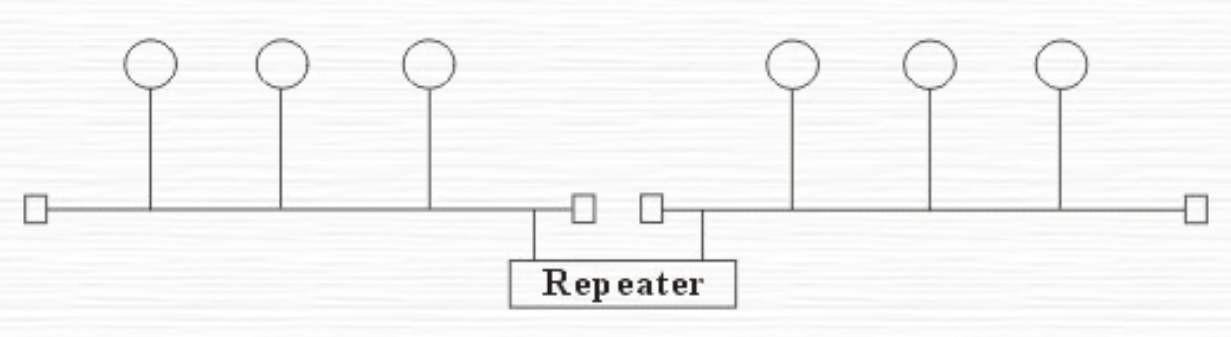
- Trình điều khiển cạc mạng (*driver*) là bộ phận phần mềm trung gian có nhiệm vụ giao tiếp giữa cạc mạng và máy tính. Khi một trình điều khiển cạc mạng được nạp, nó cần phải kết hợp với một chồng giao thức.
- Phần mềm trình điều khiển cung cấp các chức năng ở tầng LLC.
- Hiện thực CSMA/CD để truy cập kênh truyền vật lý, phát hiện và xử lý đụng độ

Repeater

- Các phương tiện truyền đều có giới hạn về tầm truyền đối với dữ liệu
- Mỗi thiết bị đều có phạm vi tối đa mà chúng có thể mang tín hiệu một cách tin cậy
- Trong một mạng LAN, giới hạn của cáp mạng là 100m (cho loại cáp mạng CAT 5 UTP – là cáp được dùng phổ biến nhất)
  - Tín hiệu bị suy hao trên đường truyền nên không thể đi xa hơn
  - → để có thể kết nối các thiết bị ở xa hơn, mạng cần các thiết bị để khuếch đại và định thời lại tín hiệu, giúp tín hiệu có thể truyền dẫn đi xa hơn giới hạn này

Repeater

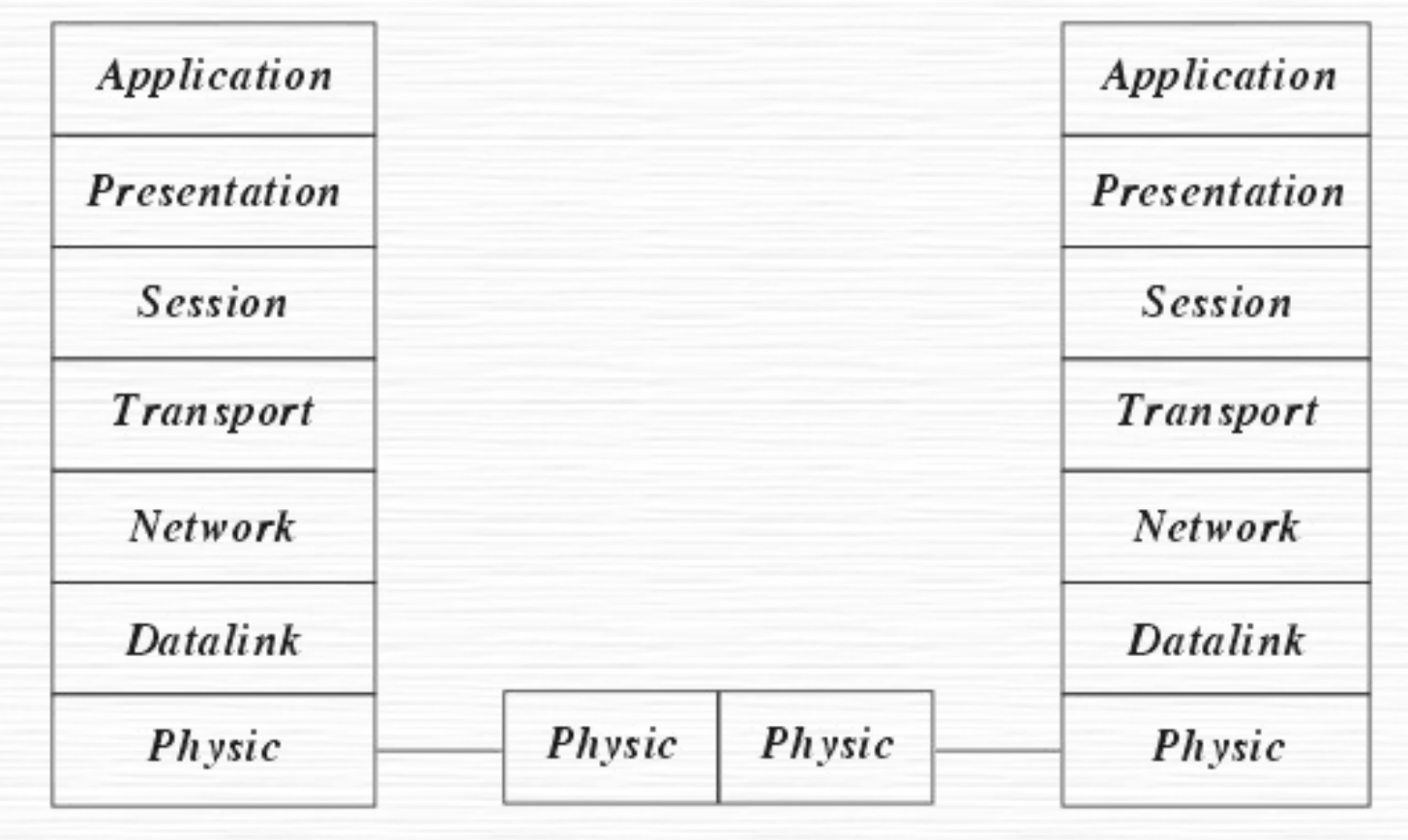
- Repeater là loại thiết bị phần cứng đơn giản nhất trong các thiết bị liên kết mạng
  - Lặp lại tín hiệu từ cổng này sang cổng khác mà nó nối
  - Hoạt động trong tầng vật lý của mô hình hệ thống mở OSI
- Repeater dùng để nối 2 mạng giống nhau hoặc các phần một mạng cùng có một giao thức và một cấu hình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



Repeater

- Đặc điểm:
  - 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)
  - Khôi phục lại tín hiệu ban đầu
  - Truyền thông mạng theo mọi hướng
  - Không đòi hỏi phải có thông tin địa chỉ của frame dữ liệu
  - Nếu dữ liệu bị sai lệch thì Repeater vẫn tái tạo tín hiệu đó
- Sử dụng Repeater làm tăng chiều dài của mạng
- Đơn giản và không đắt tiền

Repeater



Hoạt động của Repeater trong mô hình OSI

Repeater

- Phân loại:
  - **Repeater điện** nối với đường dây điện ở cả hai phía của 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
    - Khoảng cách đó luôn bị hạn chế bởi một khoảng cách tối đa do độ trễ của tín hiệu.
  - **Repeater điện quang** liên kết với một đầu cáp quang và một đầu là cáp điện
    - 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

Repeater

- Một số chú ý:
  - 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.
    - Ví dụ: như hai mạng Ethernet hay hai mạng Token ring
  - Nhưng không thể nối hai mạng có giao thức truyền thông khác nhau
    - Ví dụ như một mạng Ethernet và một mạng Token ring.
  - Repeater không làm thay đổi khối lượng chuyển vận trên mạng nên việc sử dụng không tính toán nó trên mạng lớn sẽ hạn chế hiệu năng của mạng
  - Khi lựa chọn sử dụng Repeater cần chú ý lựa chọn loại có tốc độ vận chuyển phù hợp với tốc độ của mạng

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
- Hub còn được gọi là bộ chuyển tiếp nhiều cổng
- Hoạt động ở tầng vật lý trong mô hình OSI

Hub

- Phân 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.
  - Khoảng cách giữa một máy tính và Hub không thể lớn hơn một nửa khoảng cách tối đa cho phép giữa 2 máy tính trên mạng
    - Ví dụ khoảng cách tối đa cho phép giữa 2 máy tính của mạng là 200m thì khoảng cách tối đa giữa một máy tính và hub là 100m
  - Các mạng ARCnet thường dùng Hub bị động.

Hub

- ***Hub chủ động (Active Hub)*** **:** Hub chủ động có các linh kiện điện tử có thể khuếch đại và xử lý các tín hiệu điện tử truyền giữa các thiết bị của mạng.
- Quá trình xử lý tín hiệu được gọi là tái sinh tín hiệu, nó làm cho tín hiệu trở nên tốt hơn, ít nhạy cảm với lỗi do vậy khoảng cách giữa các thiết bị có thể tăng lên.
- Tuy nhiên những ưu điểm đó cũng kéo theo giá thành của Hub chủ động cao hơn nhiều so với Hub bị động.
- Các mạng Token ring có xu hướng dùng Hub chủ động

Hub

- ***Hub thông minh (Intelligent Hub):*** cũng là Hub chủ động nhưng có thêm các chức năng mới so với loại trước, nó có thể có bộ vi xử lý của mình và bộ nhớ mà qua đó nó không chỉ cho phép điều khiển hoạt động thông qua các chương trình quản trị mạng mà nó có thể hoạt động như bộ tìm đường hay một cầu nối.
- Có thể cho phép tìm đường cho gói tin rất nhanh trên các cổng của nó thay vì phát lại gói tin trên mọi cổng thì nó có thể chuyển mạch để phát trên một cổng có thể nối tới trạm đích.

Hub

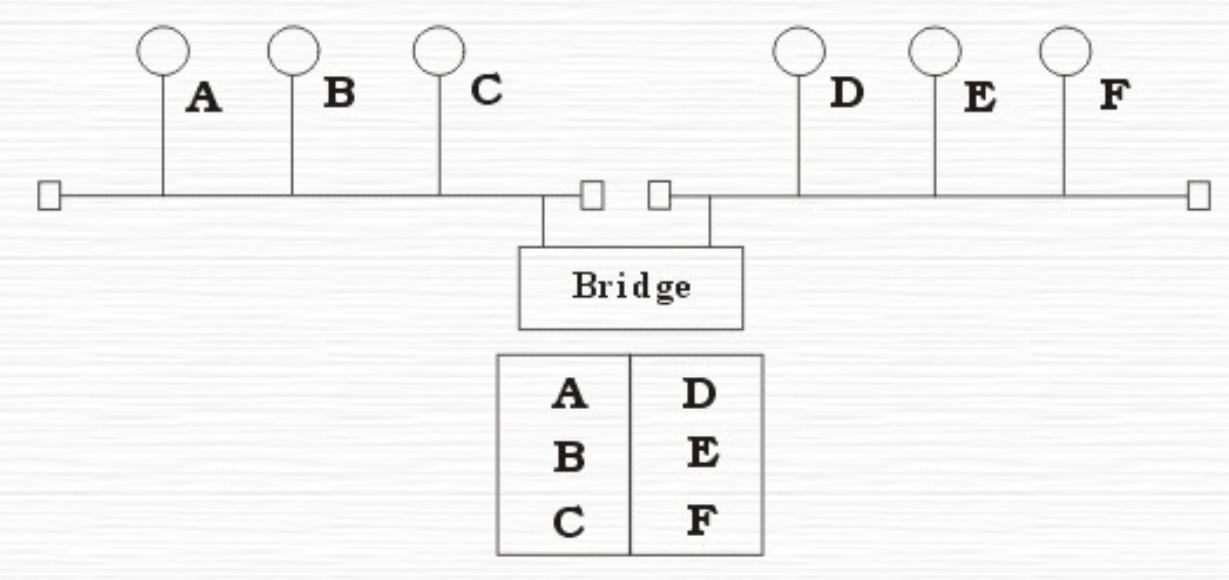
- Nhiệm vụ của Hub:
  - Cung cấp một điểm nối trung tâm cho tất cả máy tính trong mạng. Mọi máy tính đều được cắm vào Hub. Các Hub đa cổng có thể được được đặt xích lại nhau nếu cần thiết để cung cấp thêm cho nhiều máy tính.
  - Sắp xếp các cổng theo cách để nếu một máy tính thực hiện truyền tải dữ liệu, dữ liệu đó phải được gửi qua dây nhận của thiết bị khác
  - Khi một trạm gửi tín hiệu đi, Hub tiếp nhận và chuyển tời tất cả các cổng còn lại trên nó. Điều này sẽ làm giảm đi hiệu năng mạng khi có nhiều trạm cùng gửi tín hiệu.

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

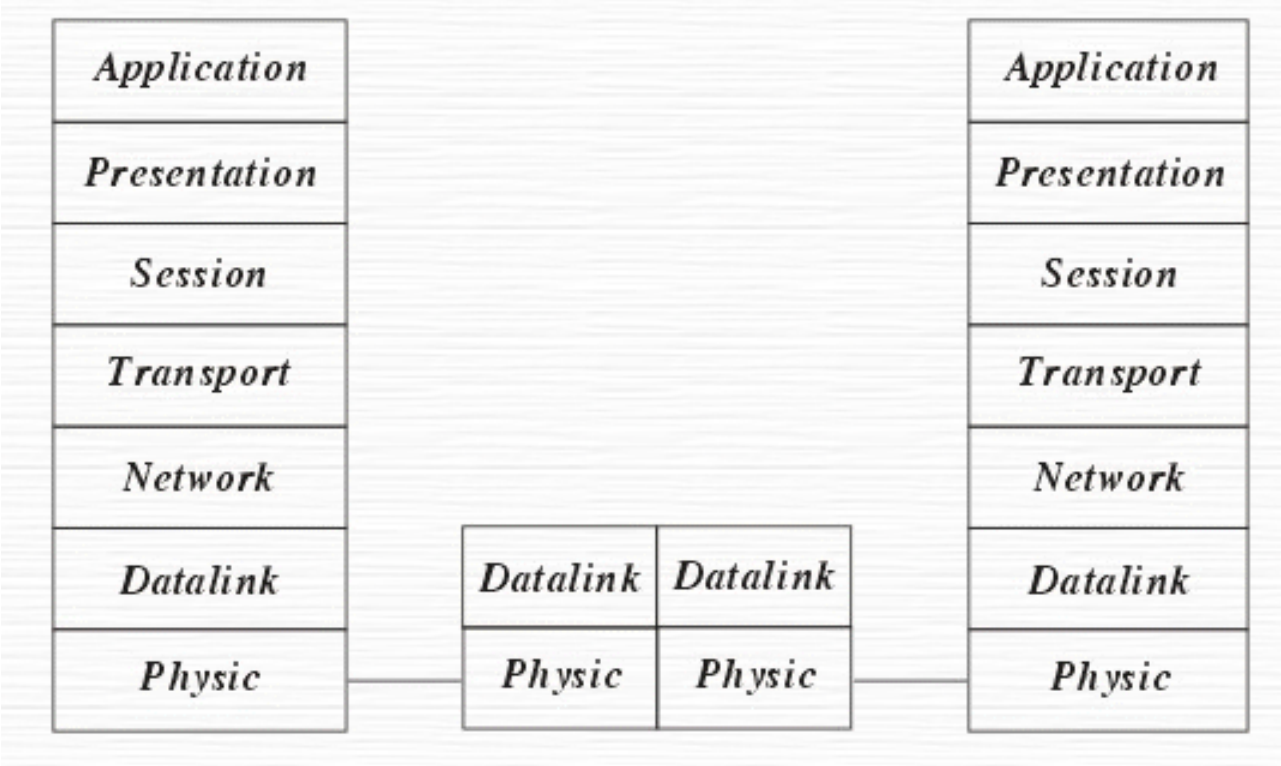
Bridge

- 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.



Bridge

- 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).



Bridge

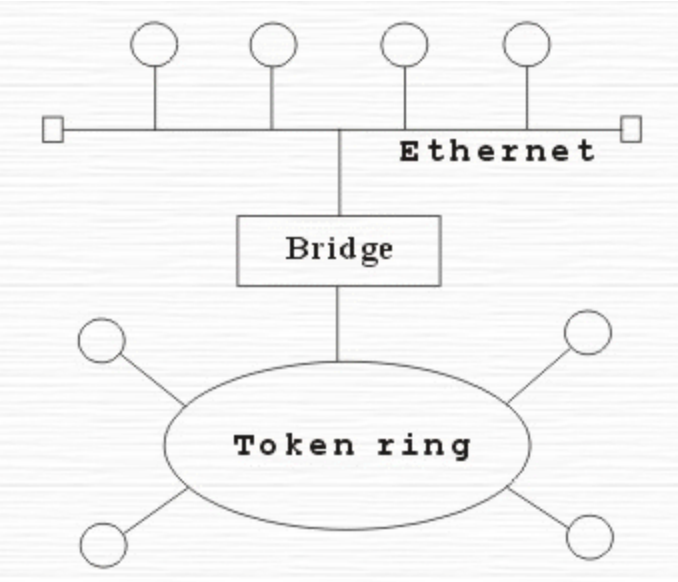
- Để đánh giá một Bridge người ta đưa ra hai khái niệm : Lọc và chuyển vận.
  - Quá trình xử lý mỗi gói tin được gọi là quá trình lọc trong đó tốc độ lọc thể hiện trực tiếp khả năng hoạt động của Bridge.
  - Tốc độ chuyển vận được thể hiện số gói tin/giây trong đó thể hiện khả năng của Bridge chuyển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

Bridge

- Phân loại: 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
  - 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 chuyển một gói tin theo chuẩn đang sử dụng trên mạng Enthernet sang chuẩn đang sử dụng trên mạng Token ring.

Bridge

- 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
  - 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.

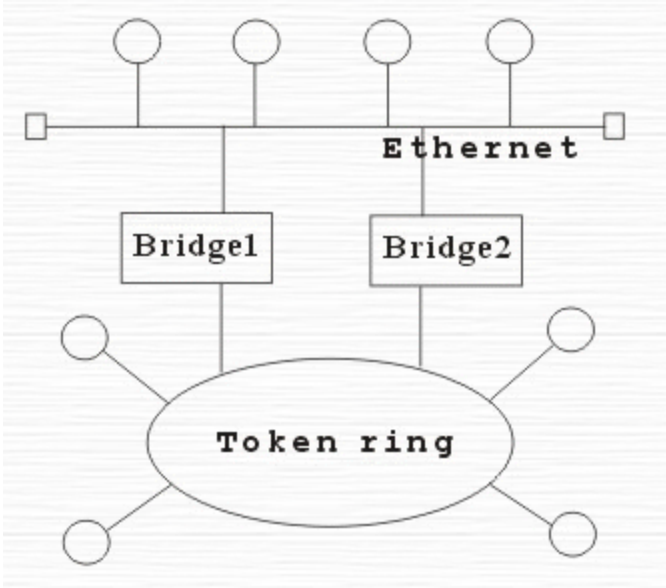


Bridge

- Ứng dụng:
  - 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 những 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.

Bridge

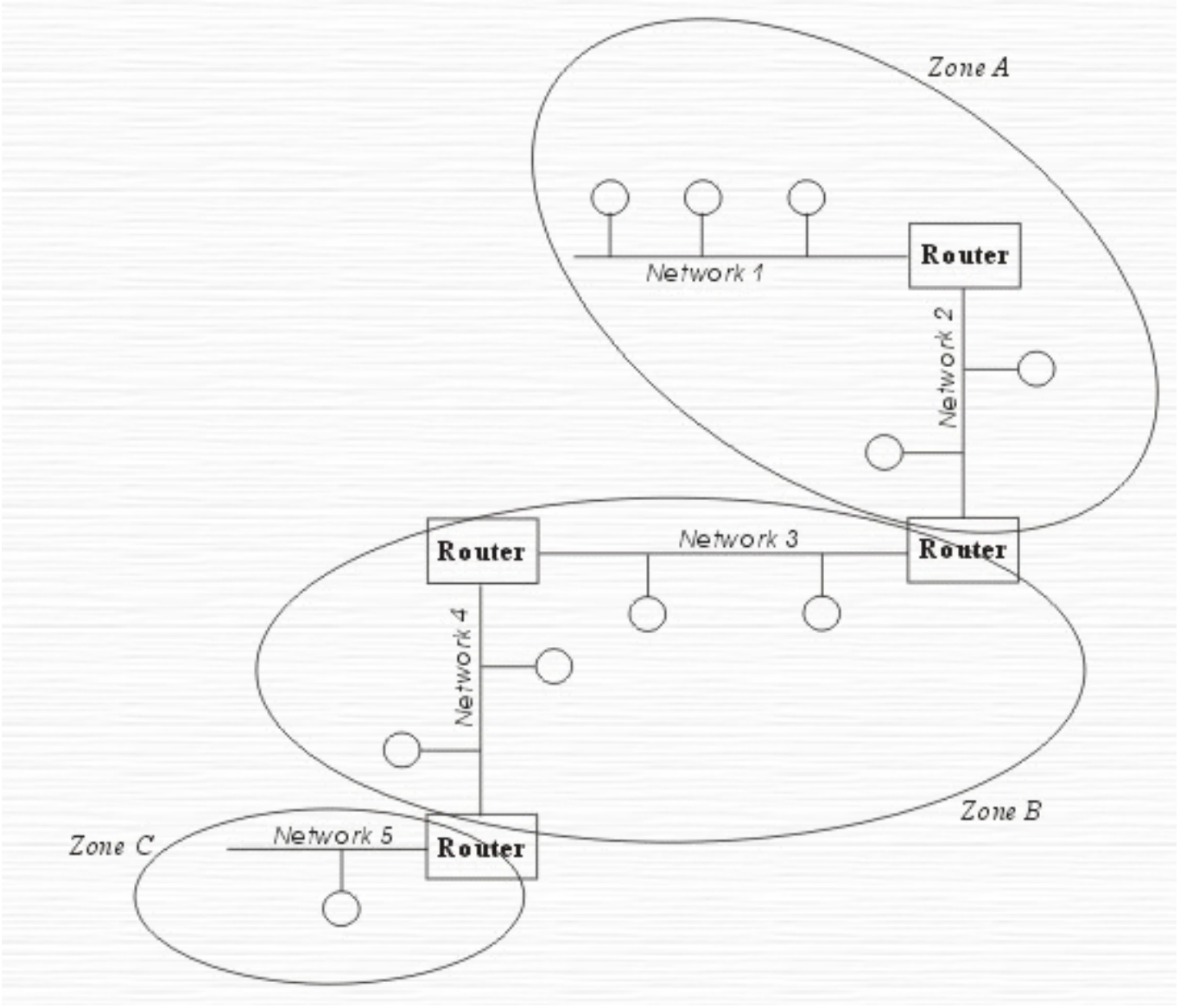
- Ứng dụng:
  - Một vài Bridge còn có khả năng lựa chọn đối tượng vận chuyển. Nó có thể chỉ chuyển vận những gói tin của những địa chỉ xác định. Ví dụ : cho phép gói tin của máy A, B qua Bridge 1, gói tin của máy C, D qua Bridge 2.
  - Một số Bridge được chế tạo thành một bộ riêng biệt, chỉ cần nối dây và bật. Các Bridge khác chế tạo như card chuyên dùng cắm vào máy tính, khi đó trên máy tính sẽ sử dụng phần mềm Bridge. Việc kết hợp phần mềm với phần cứng cho phép uyển chuyển hơn trong hoạt động của Bridge



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.
- 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.

Router


Zone A
Network 1
Router
Network 2
Router
Network 3
Router
Network 4
Zone B
Zone C
Network 5
Router

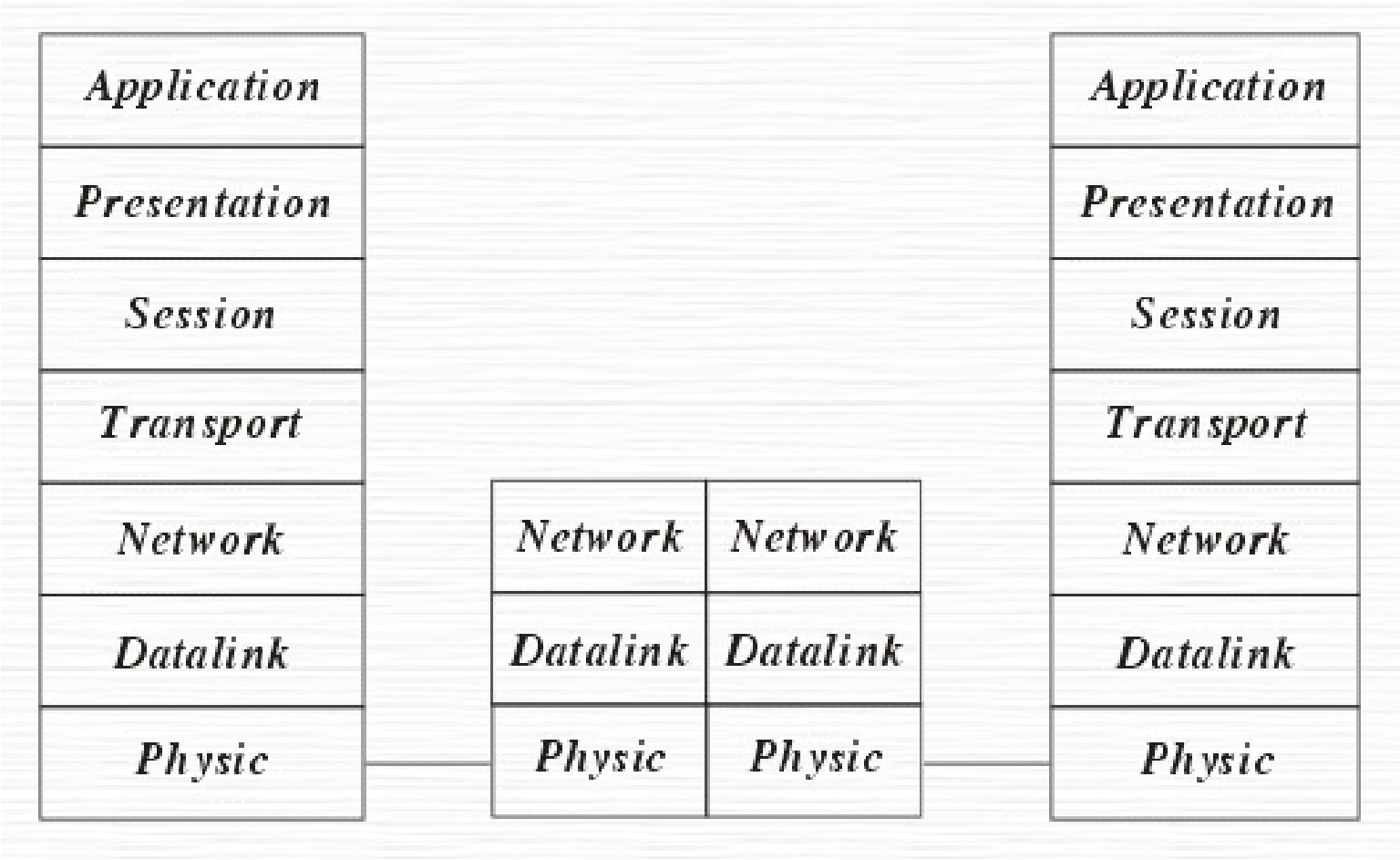
Router

- 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.

Router

- Người ta phân chia Router thành hai loại 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 ù chấp nhận kích thức các gói tin khác nhau (Router có thể chia nhỏ một gói tin lớn thành nhiều gói tin nhỏ trước truyền trên mạng).
- 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

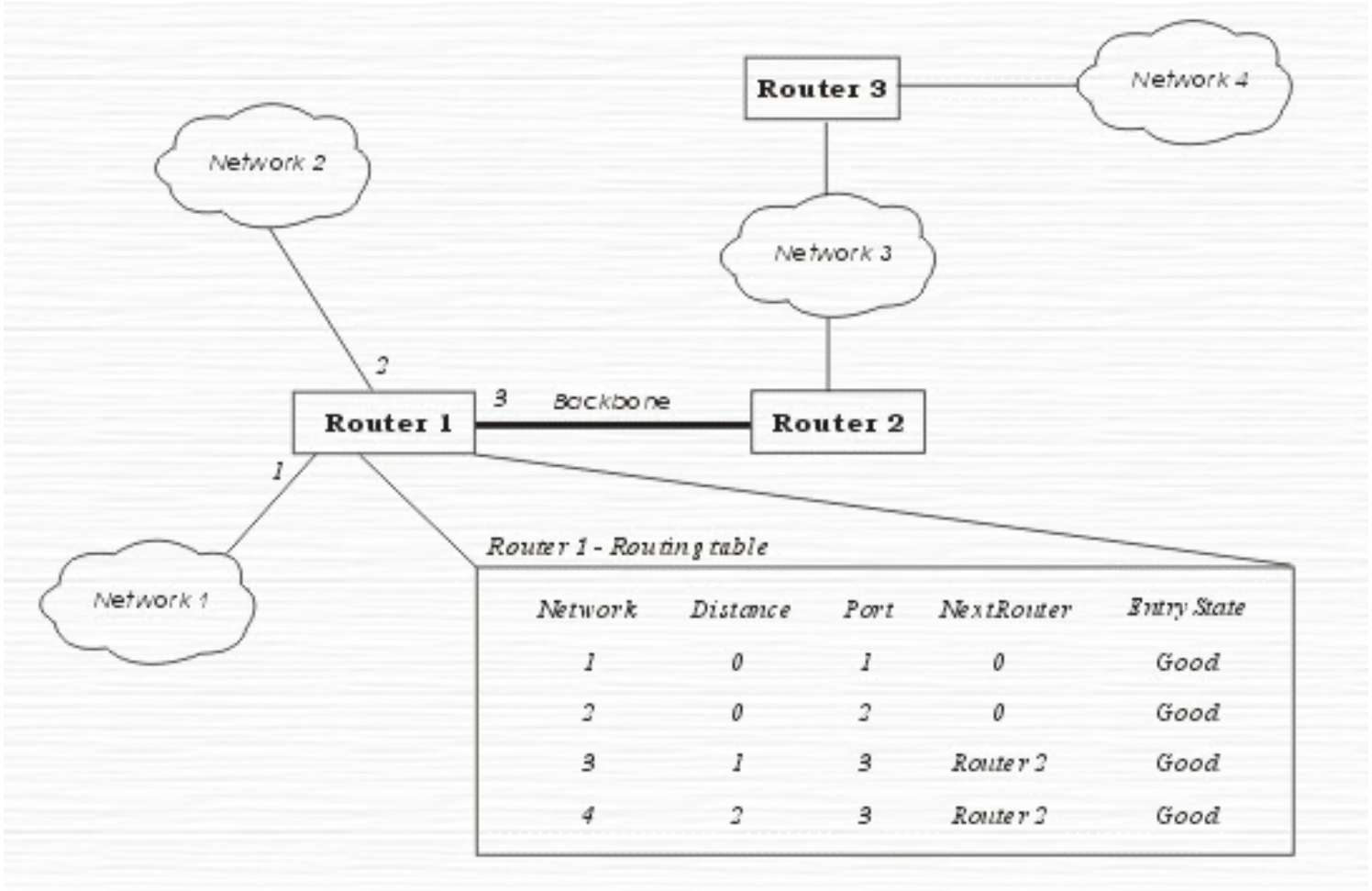
Router


Application
Presentation
Session
Transport
Network
Datalink
Physic
Network
Network
Datalink
Datalink
Physic
Physic
Application
Presentation
Session
Transport
Network
Datalink
Physic

Router

- 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.

Router



Router 1 - Routing table

Network	Distance	Port	NextRouter	Entry State
1	0	1	0	Good
2	0	2	0	Good
3	1	3	Router 2	Good
4	2	3	Router 2	Good

Router

- Phương thức hoạt động của Router: 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 và chỉ khi đó các Router khác cùng cập nhật lại bảng chỉ đường, thông tin truyền đi khi đó thường là thông tin về đường truyền.

Router

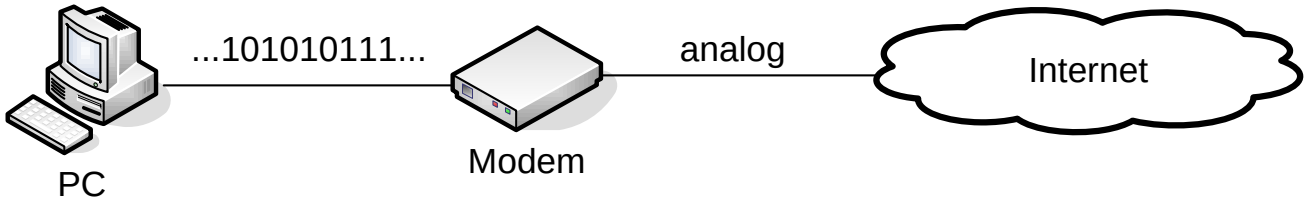
- Một số giao thức hoạt động chính của Router:
  - RIP (Routing Information Protocol) được phát triển bởi Xerox Network system và sử dụng SPX/IPX và TCP/IP. RIP hoạt động theo phương thức véc tơ khoảng cách.
  - NLSP (Netware Link Service Protocol) được phát triển bởi Novell dùng để thay thế RIP hoạt 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...
  - OSPF-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...

Modem

- Modem (**Mo**dulator-**Dem**odulator)
  - Là một thiết bị chuyển đổi các dữ liệu phát ra thông qua cổng nối tiếp thành 1 dạng tín hiệu để truyền đi trên các đường điện thoại khi gửi
  - Phục hồi các tín hiệu này thành dữ liệu mà máy tính hiểu được khi nhận
  - **Modem + Fax + Voice** (truyền dữ liệu, truyền Fax và truyền âm thanh).

Modem

- Sự cần thiết của modem:
  - Kỹ thuật điện thoại ra đời từ rất sớm, trước cả kỹ thuật máy tính
  - Khi kỹ thuật máy tính ra đời thì không thể dùng cáp điện thoại để truyền tín hiệu một cách trực tiếp
    - Giải pháp tạo ra thiết bị trung gian Modem
  - Thiết bị cần thiết cho việc liên lạc giữa các máy tính qua đường dây điện thoại thông thường
  - Modem hoạt động theo 2 hướng : điều chế dữ liệu khi phát, và giải điều chế dữ liệu khi nhận



Modem

- Phạm vi sử dụng:
  - Modem được dùng làm thiết bị truy xuất internet từ các máy tính cá nhân qua mạng điện thoại công cộng.
    - Để đáp ứng với lượng khách hàng lớn, các ISP (Internet Service Provider) sử dụng hàng loạt các modem tốc độ cao, loạt các modem này thường được gọi là ngân hàng modem.
    - Ngân hàng mođem được nối vào nhiều kênh điện thoại, nhưng chỉ có một hay vài số điện thoại tương ứng, nhớ đó mà nhiều khách hàng quay đồng thời cùng một số điện thoại nhưng đều được đáp ứng kết nối
  - Hiện nay, nhu cầu kết nối Internet ngày càng nhiều, một số giải pháp đề xuất là tận dụng mạng truyền hình cáp có sẵn để có thể truy xuất được cả các dịch vụ Internet
    - Sử dụng modem cáp

Modem

- Phân loại modem
  - External modem (modem ngoài): được nối với máy tính hoặc thiết bị đầu cuối qua sợi cáp dùng chuẩn RS232 hoặc RS449 của EIA.

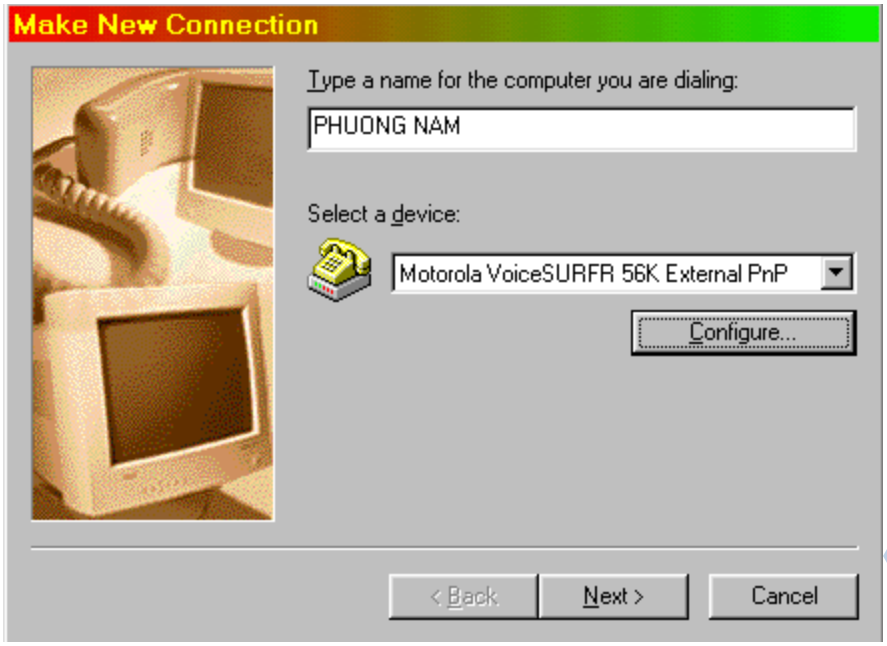
  - Internal Modem (modem trong): được tích hợp trên mainboard hay dưới dạng card cắm vào các slot.

Modem

RJ11

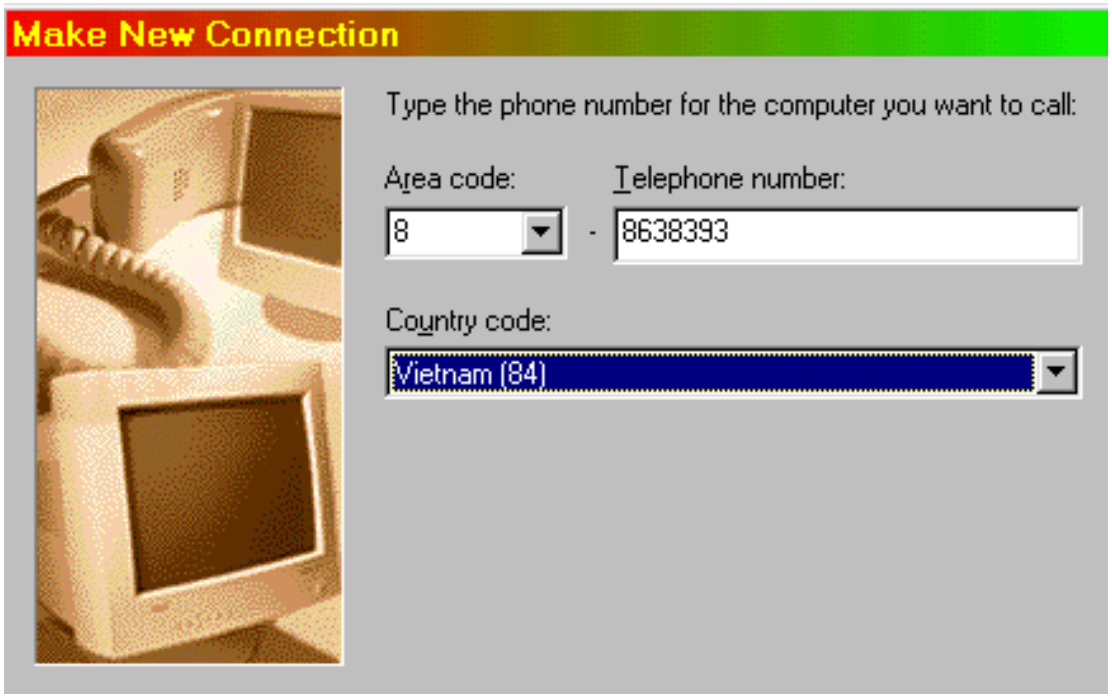
Modem

- Sử dụng Dial-Up để quay số vào mạng
  - Cài đặt các giao thức yêu cầu
  - Tạo địa chỉ Connection
    - Mở My Computer, click chuột vào icon Dial-Up Networking mở cửa sổ của Dial-Up Networking lên. Click chuột vào icon Make New Connection. Trong hộp thoại Make New Connection, bạn điền tên của Website mà mình muốn connect vào box trên cùng.
    - Click **Next**



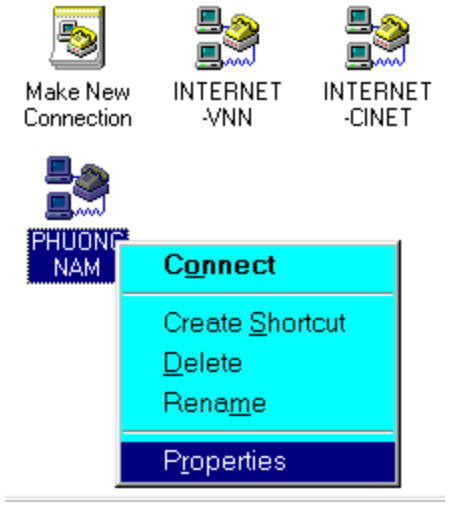
Modem

- Ở hộp thoại mới mở ra, điền số mã tỉnh thành (có thể bỏ trống cũng được) và số điện thoại của Website.
- Click nút **Next**.
- Trên hộp thoại mới, click vào nút **Finish** để hoàn công việc thiết lập địa chỉ connect mới này.



Modem

- Quay số Connect:
  - Mở cửa sổ Dial-Up Networking lên. Click double chuột vào icon của Website muốn connect
  - Hộp thoại **Connect To** xuất hiện



Modem

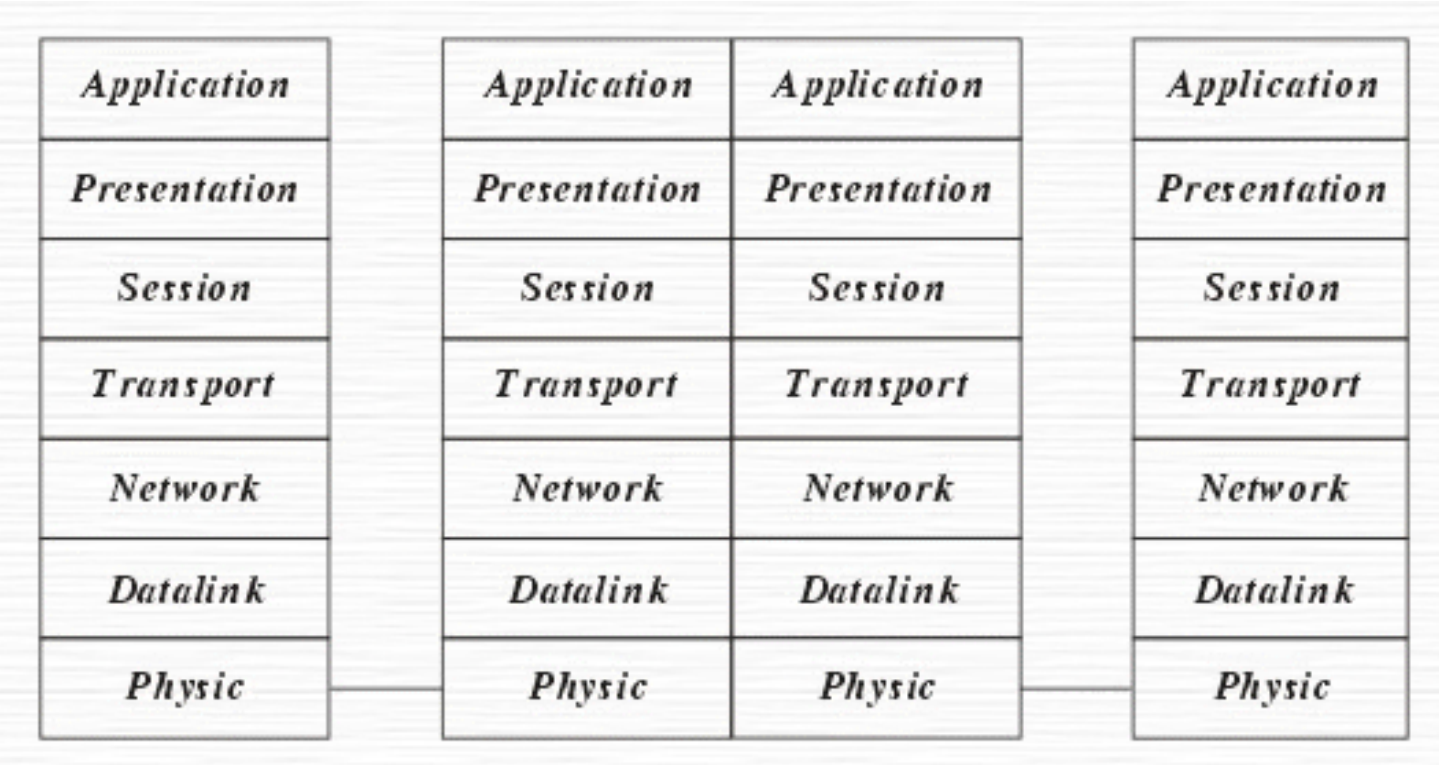
- Điền vào hộp **User name** và **Password** các thông số account của mình (do nhà quản trị Website cung cấp). Nếu máy chỉ có một mình sử dụng và không muốn mất công mỗi lần connect lại phải một phen điền các thông số password, đánh dấu kiểm vào box **Save password** cho nó lưu lại.
- Click chuột vào nút **Connect**.
- Sau khi connect thành công, hộp thoại connect sẽ biến mất và bên dưới màn hình, chỗ khay công cụ hệ thống (tức "khay đồng hồ") sẽ xuất hiện icon của Dial-Up Networking có hình hai máy vi tính đang kết mô-đen với nhau.

- Sử dụng các trình duyệt để vào mạng

Gateway

- Gateway dùng để kết nối các mạng không thuần nhất chẳng hạn như các mạng cục bộ và các mạng máy tính lớn (Mainframe)
  - Do các mạng hoàn toàn không thuần nhất nên việc chuyển đổi thực hiện trên cả 7 tầng của hệ thống mở OSI
  - Thường được sử dụng nối các mạng LAN vào máy tính lớn
  - Gateway đa giao thức thường được chế tạo như các Card có chứa các bộ xử lý riêng và cài đặt trên các máy tính hoặc thiết bị chuyên biệt
  - Hoạt động của Gateway thông thường phức tạp hơn là Router nên thông suất của nó thường chậm hơn và thường không dùng nối mạng LAN -LAN.

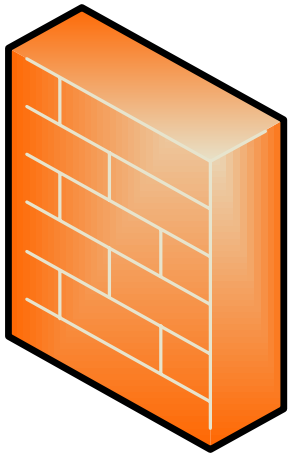
Gateway



Hoạt động của Gateway trong mô hình OSI

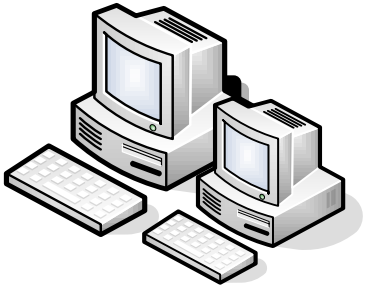
Firewall

- Định nghĩa:
  - Firewalls là hệ thống ngăn chặn việc truy nhập trái phép từ bên ngoài vào mạng
  - Phần cứng, phần mềm hoặc kết hợp cả hai
- Chức năng:
  - Bảo vệ tài nguyên
  - Kiểm soát truy cập
  - Nâng cao hiệu suất
  - Tự động hóa bảo vệ & cảnh báo

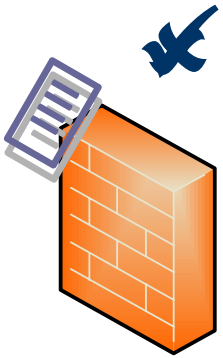


Firewall

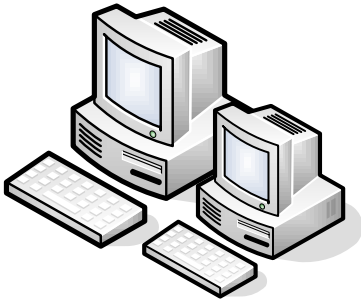
- Hoạt động:



Mạng ngoài



Firewall



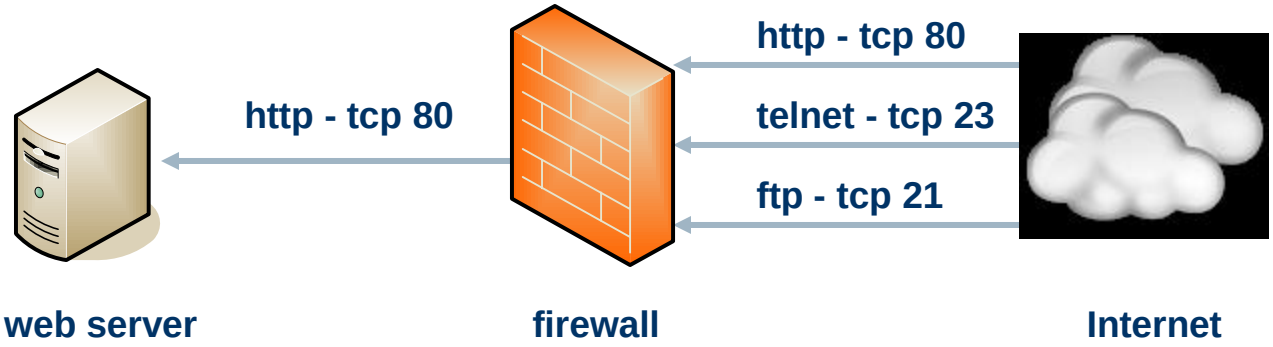
Mạng trong

Firewall

- Cấu trúc:
  - Một hoặc nhiều hệ thống máy chủ kết nối với các bộ định tuyến (router) hoặc có chức năng router.
  - Các phần mềm quản lí an ninh chạy trên hệ thống máy chủ
    - Hệ quản trị xác thực (Authentication)
    - Cấp quyền (Authorization)
    - Kế toán (Accounting).

Firewall

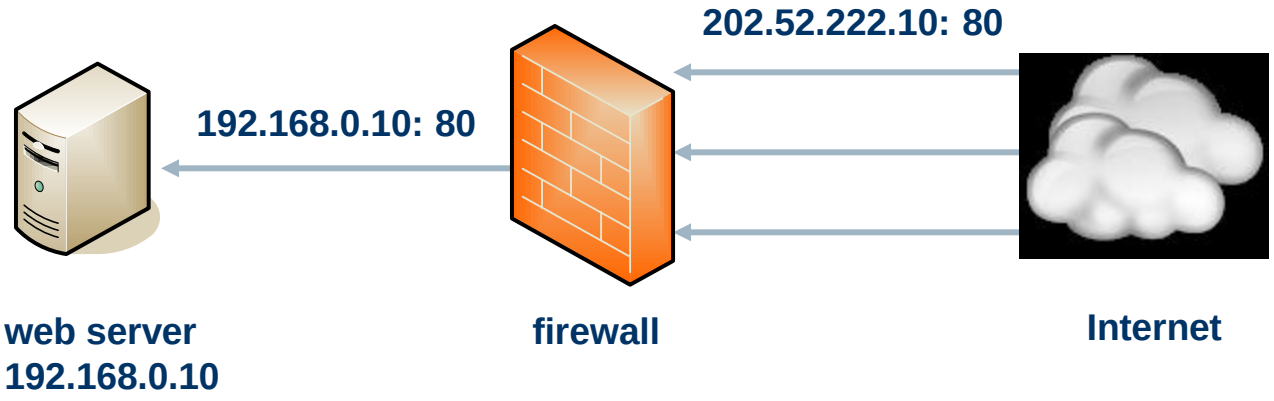
- Phân loại Firewall:
  - Packet filtering firewalls:
    - Kiểm tra địa chỉ IP, cổng đích & nguồn hay kiểu giao thức của một gói tin, dựa vào quy luật để cho hay ko cho phép gói đó tin đi qua mạng



- **Chỉ cho phép http - tcp 80**
- **Chặn tất cả**

Firewall

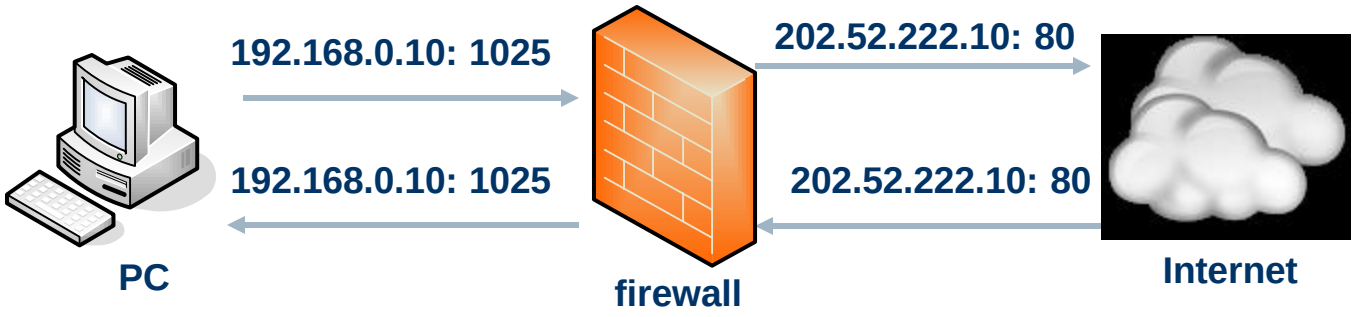
- Application layer firewalls:
  - Được xem như một firewall ủy quyền, cổng ứng dụng
  - Proxy như một đại diện cho những ai dùng proxy đó, che dấu thông tin thực khi giao tiếp bên ngoài
  - Các gói yêu cầu truy nhập được sẽ được biên dịch tại firewall trước khi vào mạng trong



Dịch địa chỉ 202.52.222.10 : 80
thành 192.168.0.10 : 80

Firewall

- Stateful inspection firewalls :
  - Kiểm tra trạng thái và nội dung của gói
  - Ghi nhớ những yêu cầu đi ra và chỉ cho phép những yêu cầu đó trở lại qua Firewall
  - Việc cố tình truy cập vào mạng trong sẽ bị từ chối nếu bên trong không yêu cầu



Chỉ cho phép những gói trả lại theo yêu cầu đặt ra

Khóa những đường truyền chưa đăng ký

Firewall

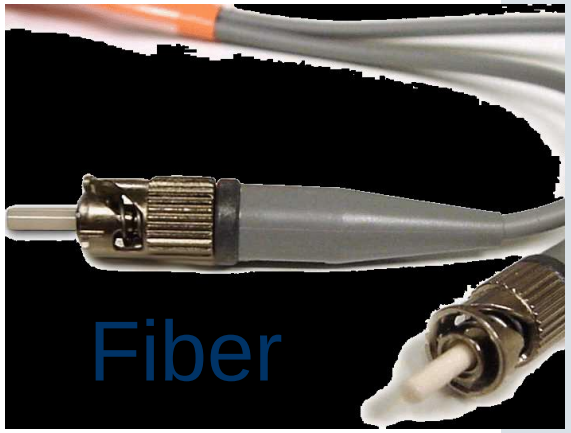
- Firewall bảo vệ chống lại cái gì?
  - Tấn công trực tiếp:
    - Cách thứ nhất là dùng phương pháp dò mật khẩu trực tiếp. Thông qua các chương trình dò tìm mật khẩu với một số thông tin về người sử dụng như ngày sinh, tuổi, địa chỉ v.v...và kết hợp với thư viện do người dùng tạo ra, kẻ tấn công có thể dò được mật khẩu của bạn. Trong một số trường hợp khả năng thành công có thể lên tới 30%.
    - Cách thứ hai là sử dụng lỗi của các chương trình ứng dụng và bản thân hệ điều hành đã được sử dụng từ những vụ tấn công đầu tiên và vẫn được để chiếm quyền truy cập (có được quyền của người quản trị hệ thống).
  - Nghe trộm: Có thể biết được tên, mật khẩu, các thông tin chuyền qua mạng thông qua các chương trình cho phép đưa vỉ giao tiếp mạng (NIC) vào chế độ nhận toàn bộ các thông tin lưu truyền qua mạng

Firewall

- Giả mạo địa chỉ IP
- Vô hiệu hoá các chức năng của hệ thống (deny service). Đây là kiểu tấn công nhằm làm tê liệt toàn bộ hệ thống không cho nó thực hiện các chức năng mà nó được thiết kế. Kiểu tấn công này không thể ngăn chặn được do những phương tiện tổ chức tấn công cũng chính là các phương tiện để làm việc và truy nhập thông tin trên mạng.
- Lỗi người quản trị hệ thống.
- Yếu tố con người với những tính cách chủ quan và không hiểu rõ tầm quan trọng của việc bảo mật hệ thống nên dễ dàng để lộ các thông tin quan trọng cho hacker.

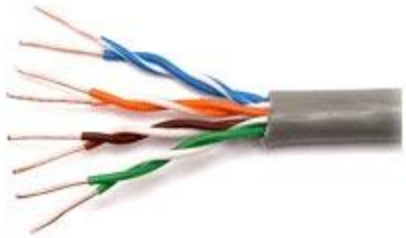
Đường truyền – Cáp mạng

- Cable:



Coaxial cable

UTP và RJ-45 jack



Chuẩn cáp Ethernet

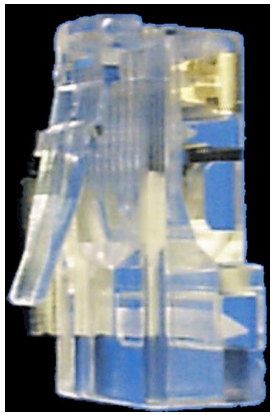
- Ethernet
  - 10Base-T (100m, Unshielded Twisted Pair = UTP)
  - 10Base-2 (~200m, Coax)
  - 10Base-5 (500m, Coax)
  - 10Base-FL (2000m=2km, Multimode Fiber)
- Fast Ethernet
  - 100Base-TX (100m over CAT5 UTP)
  - 100Base-FX (2000m=2km over MM Fiber)
- Gigabit Ethernet
  - 1000Base-SX (300m over MM Fiber)
  - 1000Base-LX (550m over MM Fiber, 3000m over SM Fiber)

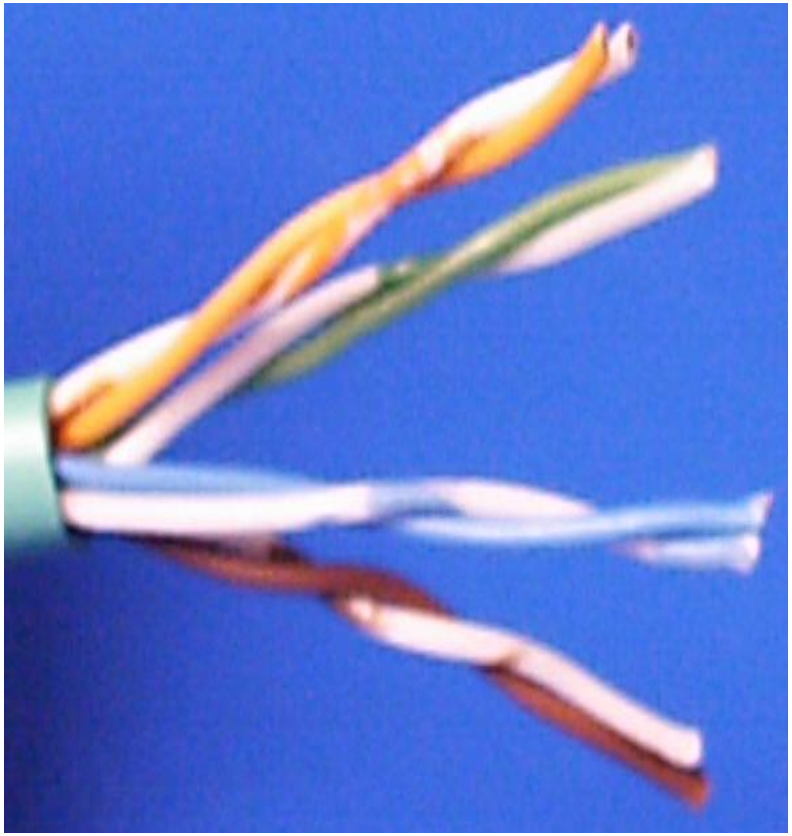
Chuẩn TIA/EIA 586

- TIA/EIA 568 (1991) là chuẩn đấu dây cho cáp Ethernet
- Để xây dựng mạng LAN theo chuẩn Ethernet, cần khảo sát chuẩn TIA/EIA 568A, B cho cáp UTP Cat 3, 5
  - Qui ước về mã màu trêp cáp
  - Qui ước đấu nối cáp
  - …

Quy ước mã màu cáp UTP

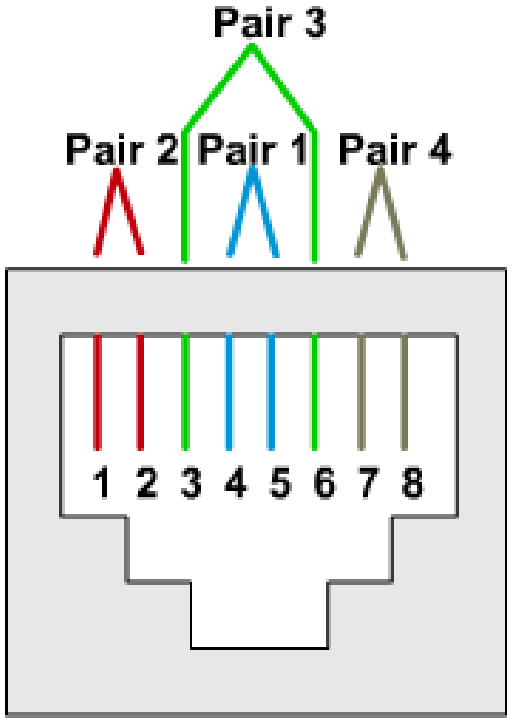
- Cáp UTP gồm 4 cặp sợi xoắn với nhau





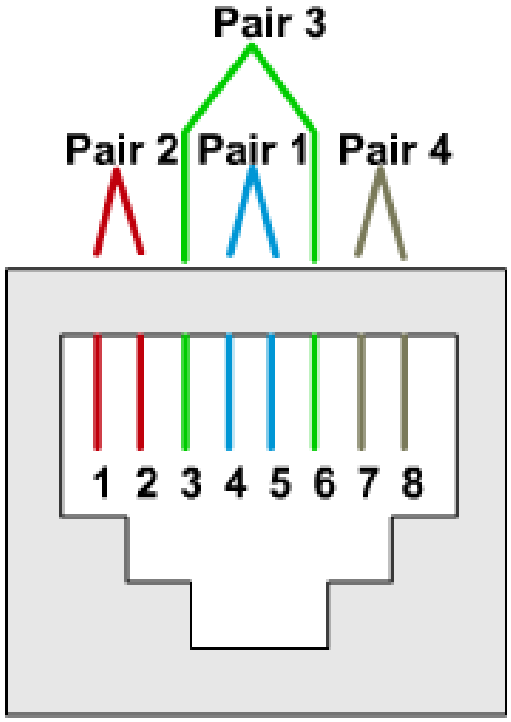
Qui ước NIC-port & TIA/EIA 568B

Pin	Use
1	Transmit
2	Transmit
3	Receive
4	NC
5	NC
6	Receive
7	NC
8	NC



Qui ước HUB-port & TIA/EIA 568B

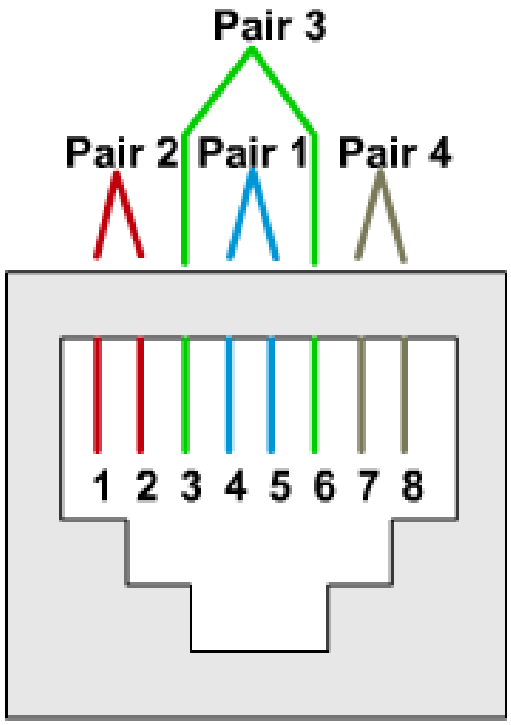
Pin	Use
1	Receive
2	Receeive
3	Transmit
4	NC
5	NC
6	Transmit
7	NC
8	NC



T568B

Qui ước mã màu cáp TIA/EIA 568B

Pin	Color
1	White Orange
2	Orange
3	White Green
4	Blue
5	White Blue
6	Green
7	White Brown
8	Brown



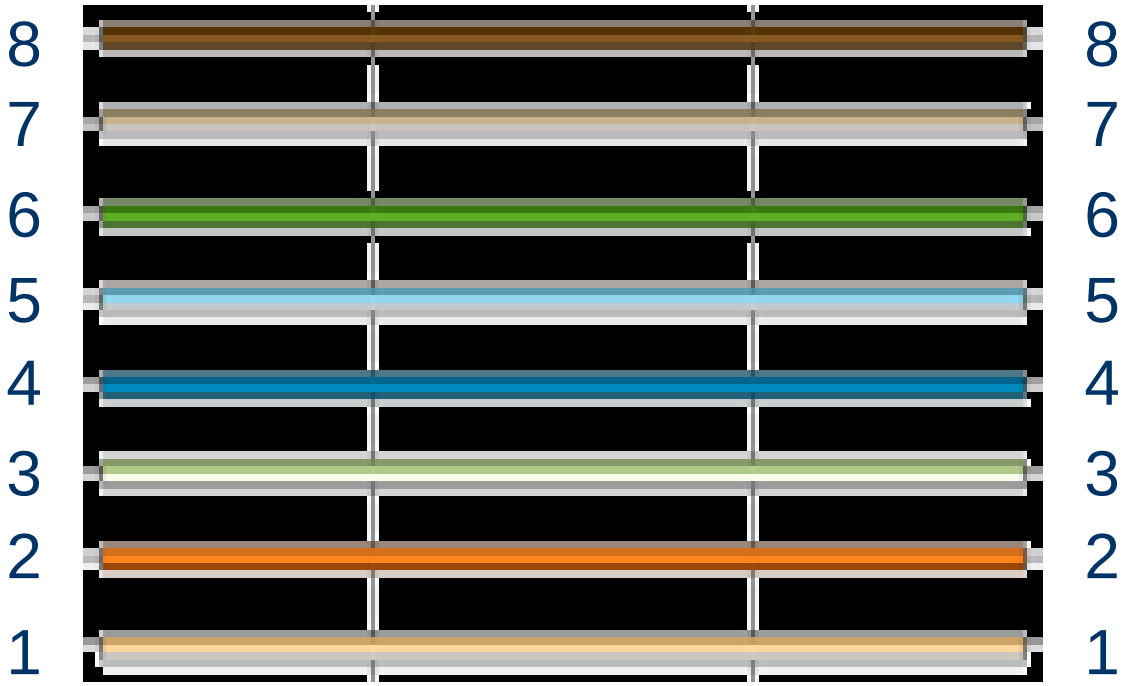
T568B

Quy ước đấu cáp

- Chiều dài tối đa đã được quy định trong kiến trúc mạng cho từng loại cáp và chiều dài không phụ thuộc vào kiểu dây hay cách bấm dây
  - Đối với cáp UTP thì chiều dài tối đa là 100m
  - Tối thiểu là 0.5m tính từ HUB to PC, còn PC to PC thì 2.5m.
- Cách bấm dây mạng có nhiều cách tùy vào mục đích sử dụng. Chọn cách bấm nào còn phụ thuộc loại dây cáp

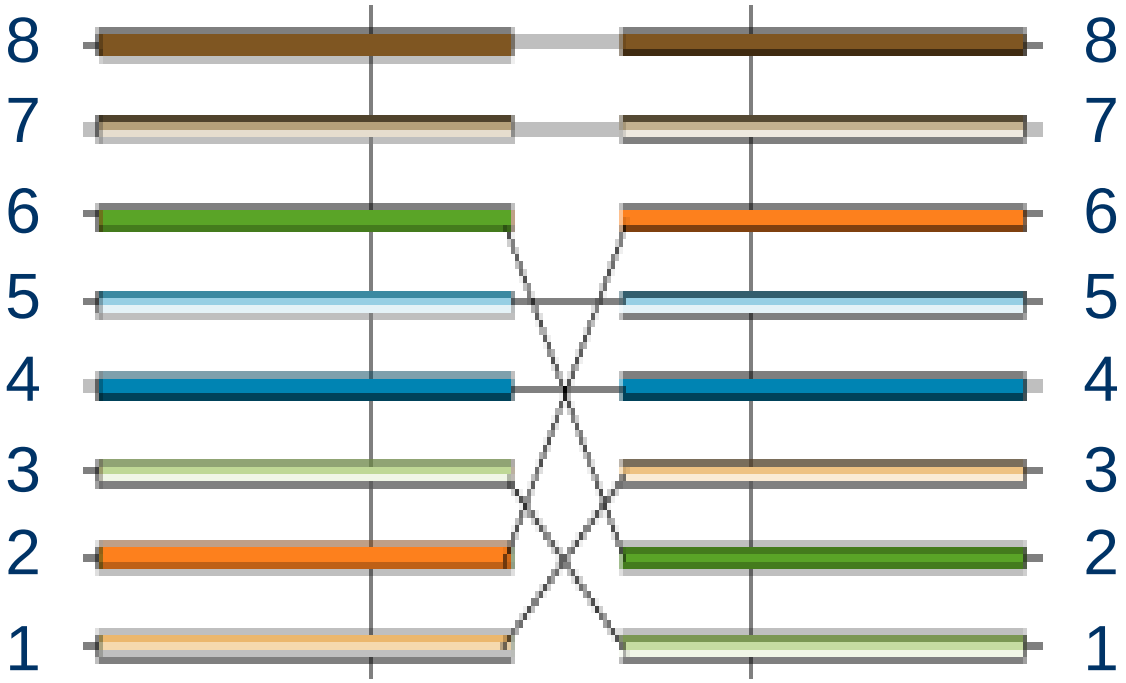
Quy ước đấu cáp

- Đấu thẳng (straight): PC-switch, switch-router, PC-hub



Quy ước đấu cáp

- Đấu chéo (crossover): nối các thiết bị hub-switch, hub-hub, switch-switch, router-router, router-PC, PC-PC.



Một số cách để bấm cáp đẹp

- Mua kềm tốt - Mua đầu Jack tốt - Mua cáp xịn (xách lên thấy nặng là được. vì nếu nặng thì tiết diện mỗi sợi dây sẽ lớn --> tốt hơn nhỏ)
- Bóc vỏ ngoài (không quá dài, không được làm hỏng vỏ những sợi cáp bên trong)
- Mở xoắn những đôi cáp --> làm thẳng những sợi cáp --> sắp cho đúng vị trí (theo chuẩn T568B hay T568A)
- Làm đầu những sợi cáp bằng nhau (lấy kềm cắt) --> nhét vào jack RJ45 (sao cho bạn phải nhìn thấy 8 đầu sợi cáp trên đầu Jack RJ45 - Bước này khá quan trọng)
- Kiểm tra --> 1-2-3 bấm --> Dùng máy test
- Chất lượng cáp CAT5 của LG chất lượng hơn cáp của AMP thông thường

Một số cách để bấm cáp đẹp

- Một cáp được bấm tốt thì đầu RJ45 phải ngậm một chút vỏ nhựa của sợi cáp, các pin bên trong phải khít tới đầu nhựa của RJ45, và bạn phải nhìn thấy đủ, đều các lõi đồng của các pin khi nhìn đứng RJ45.
- Cặp dây truyền tín hiệu (cặp TX hặc RX: ở trong trường hợp này thì 1-2 là một cặp, 3-6 là một cặp) phải xoắn đôi với nhau thì mới có tác dụng chống nhiễu.
- Trong môi trường bình thường thì nếu đấu cáp thẳng thì cứ hai đầu bấm giống nhau thì dùng OK, nhưng nếu trong môi trường nhiễu lớn (ví dụ như đặt gần các máy phát viba, anten thu phát ...) thì sẽ thấy ngay sự khác biệt giữa 2 cách bấm.
- Ngoài ra nếu bấm chuẩn thì sẽ tận dụng được chiều dài của cáp, nếu bấm lung tung không đúng cặp xoắn đôi thì chỉ truyền được với khoảng cách ngắn hơn khoảng cách chuẩn của dây do suy hao và nhiễu->lỗi gói tin

Giới thiệu về các giao thức định tuyến

- Thuật ngữ:
  - Routing Protocol:
    - Là ngôn ngữ để một router trao đổi với router khác để chia sẻ thông tin định tuyến về khả năng đến được cũng như trạng thái của mạng.
    - Được cài đặt tại các Router, chúng được sử dụng để: xây dựng nên bảng định tuyến để đảm bảo rằng tất cả các Router đều có bảng "Routing table " tương thích nhau cũng như đường đi đến các mạng phải được xác định trong "Routing Table".
  - Routed Protocol
    - Nó sử dụng các bảng "Routing Table" mà Routing Protocol xây dựng lên để đảm bảo việc truyền dữ liệu qua mạng một cách tin cậy. Ví dụ: IP và IPX

Giới thiệu về các giao thức định tuyến

- Vùng tự trị AS (Autonomous System)
  - Mạng Internet được chia thành các vùng nhỏ hơn gọi là các vùng tự trị (Autonomous System – AS).
  - AS bao gồm một tập hợp các mạng con được kết nối với nhau bởi Router. Một hệ thống AS thông thường thuộc quyền sử hữu của một công ty hay nhà cung cấp dịch vụ Internet (ISP)
  - Để các hệ thống AS này kết nối được với nhau, nhà quản lý phải đăng ký với cơ quan quản trị mạng trên Internet (Inter NIC) để lấy được một số nhận dạng AS cho riêng mình.
  - Bên trong mỗi AS, các nhà quản lý có quyền quyết định loại Router cũng như giao thức định tuyến cho hệ thống của mình.

Giới thiệu về các giao thức định tuyến

- Bảng định tuyến
  - Một host hay một Router phải xem xét bảng định tuyến của mình trước khi chuyển gói tin đến địa chỉ ở xa. Bảng này được gán tương ứng mỗi địa chỉ đích với một địa chỉ Router cần đến ở chặng tiếp theo
  - Bảng địa chỉ đích trong bảng có thể bao gồm các địa chỉ mạng, mạng con, các hệ thống độc lập. Trong bảng định tuyến có thể bao gồm một tuyến mặc định, được biểu diễn bằng địa chỉ 0.0.0.0
  - Bảng định tuyến của mỗi giao thức định tuyến là khác nhau, nhưng có thể bao gồm những thông tin sau :
    - Địa chỉ đích của mạng, mạng con hoặc hệ thống
    - Địa chỉ IP của Router chặng kế tiếp phải đến
    - Giao tiếp vật lý phải sử dụng để đi đến Router kế tiếp
    - Mặt nạ mạng của địa chỉ đích
    - Khoảng cách đến đích (thí dụ : số lượng chặng để đến đích).
    - Thời gian (tính theo giây) từ khi Router cập nhật lần cuối

Giới thiệu về các giao thức định tuyến

- Khoảng cách quản lý (Administrative Distance (AD))
  - Administrative Distance được sử dụng để đánh giá độ tin cậy của thông tin định tuyến mà Router nhận từ Router hàng xóm.
  - AD là một số nguyên biến đổi từ : 0 đến 255; 0 tương ứng với độ tin cậy cao nhất và 255 có nghĩa là không có lưu lượng đi qua tuyến này (tức là tuyến này không được sử dụng để vận chuyển thông tin của người sử dụng).
  - Tức là khi một Router nhận được một thông tin định tuyến, thông tin này được đánh giá và một tuyến hợp lệ được đưa vào bảng định tuyến của Router.
  - Thông tin định tuyến được đánh giá dựa vào AD, giả sử Router được cài đặt nhiều hơn một giao thức định tuyến thì giao thức định tuyến nào có AD nhỏ hơn sẽ được Router sử dụng.
  - Mỗi giao thức định tuyến có tương ứng một giá trị AD:
    - Directly 0
    - Static route 1
    - RIP 120
    - OSPF 110
    - IGRP 100

Nguyên tắc định tuyến

- Các giao thức định tuyến phải đạt được các yêu cầu đồng thời sau:
  - Khám phá động một topo mạng
  - Xây dựng các đường ngắn nhất
  - Kiểm soát tóm tắt thông tin về các mạng bên ngoài, có thể sử dụng các metric khác nhau trong mạng cục bộ.
  - Phản ứng nhanh với sự thay đổi topo mạng và cập nhật các cây đường ngắn nhất.
  - Làm tất cả các điều trên theo định kỳ thời gian.

Thực hành trên hệ mô phỏng

- Thiết bị mạng Cisco
  - Router
  - Switch
- Hệ mô phỏng Boson Netsim

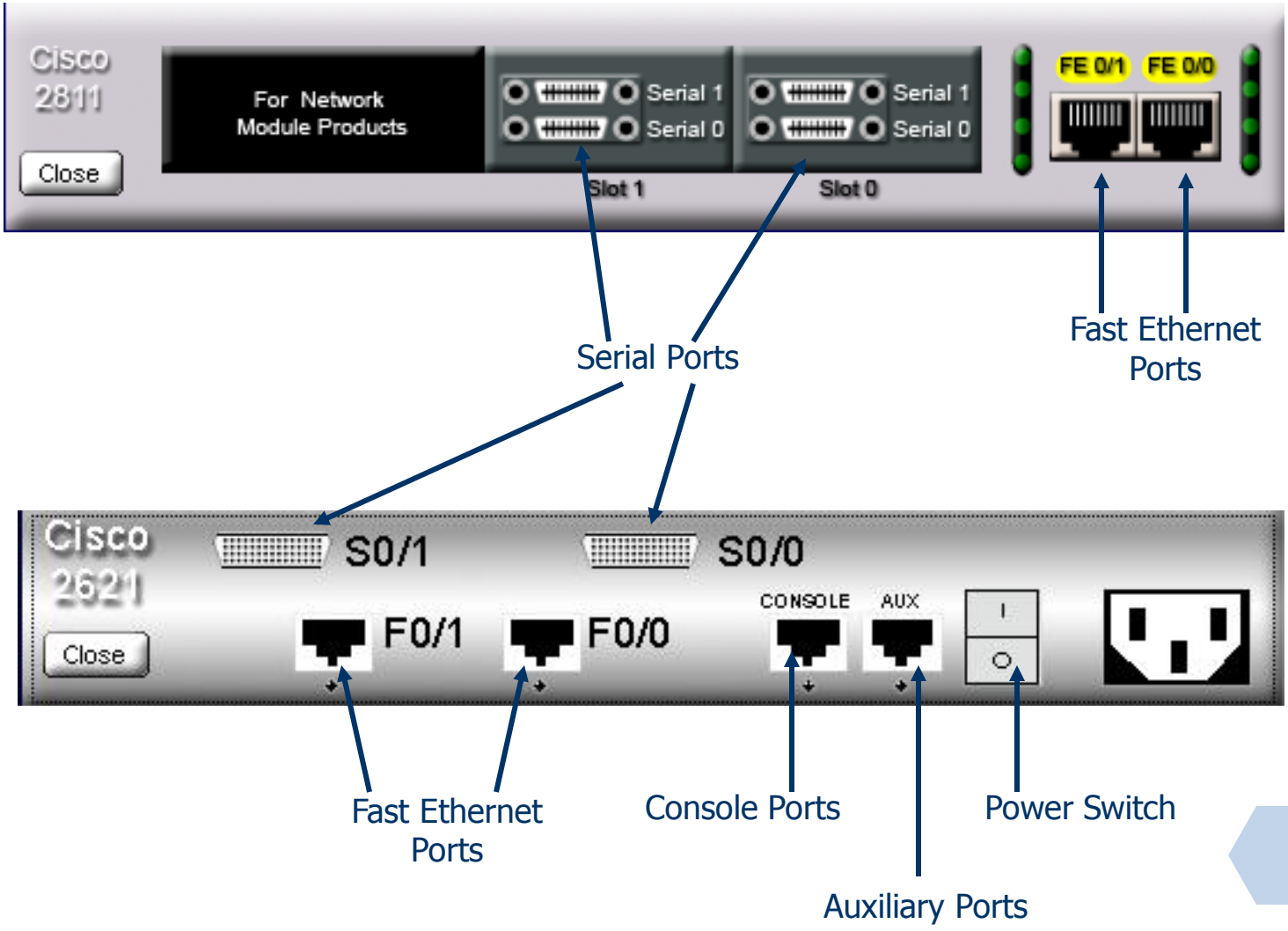
Router

- Có thể xem là một máy tính đặc biệt:
  - Có đủ các thành phần: CPU, bộ nhớ, bus hệ thống, các giao tiếp I/O…
  - Không có màn hình và bàn phím
- Router có đầy đủ chức năng của 3 lớp dưới cùng trong mô hình OSI

Router

- Hoạt động được nhờ một hệ điều hành, HĐH này được Cisco viết riêng cho router: gọi là hệ điều hành liên mạng IOS của Cisco
- Cấu hình Router thông qua IOS
- Trên Router có 3 loại giao tiếp:
  - Giao tiếp LAN
    - Thường nối với Ethernet LAN
  - Giao tiếp WAN
    - Kết nối đến nhà cung cấp dịch vụ ISP, Internet
    - Cổng nối tiếp (serial) đồng bộ, hay các cổng nối cho từng công nghệ WAN như PRI hay BRI
  - Cổng dành cho quản lý
    - Là cổng Console, Auxiliary: nối tiếp bất đồng bộ theo chuẩn EIA-232/V.24. Được nối đến cổng COM của máy tính

Router


Cisco 2811
For Network Module Products
Serial 1
Serial 0
Slot 1
Serial 1
Serial 0
Slot 0
FE 0/1
FE 0/0
Close
Serial Ports
Fast Ethernet Ports
Cisco 2621
S0/1
S0/0
F0/1
F0/0
CONSOLE
AUX
Close
Fast Ethernet Ports
Console Ports
Power Switch
Auxiliary Ports

Router

- Cần bổ sung cho Router một màn hình để quan sát và một bàn phím để nhập lệnh khi cấu hình
- Giải pháp:
  - Dùng một PC nối trực tiếp với Router thông qua cổng Console
    - Khoảng cách gần thì kết nối trực tiếp: sử dụng cáp nối với một đầu đổi từ RJ-45 sang DB-9 (cổng COM)
    - Khoảng cách xa: dùng Modem
  - Máy tính đóng vai trò là một DTE
  - Người quản trị có thể truy xuất Router qua mạng để cấu hình lại hoặc sửa chữa tham số cấu hình
    - Thực hiện qua dịch vụ Telnet
    - Router đóng vai trò là một Host: có Host name, IP Address

Switch

- Là thiết bị lớp 2 (Data Link layer), có thể xem là một cầu (Bridge) đa port.
  - Thiết bị thông minh, có thể đưa ra các quyết định chuyển dữ liệu căn cứ vào các địa chỉ MAC chứa trong Frame dữ liệu
  - Switch tự nhận biết các địa chỉ MAC của các thiết bị kết nối vào mỗi cổng của nó và xây dựng nên một bảng chuyển mạch cho mình (switching table)
  - Tạo ra một mạch ảo giữa 2 thiết bị truyền thông
    - Khi mạch ảo đã được thiết lập, một đường truyền thông cố định được thiết lập giữa 2 thiết bị

Switch

- Switch cũng là một máy tính đặc biệt
  - Có CPU, RAM
  - HĐH tương tự như Router
- Trên Switch có các cổng kết nối đến các host, và cổng console cho mục đích quản lý thiết bị
- Mỗi Switch được cấp một tên host, còn password được cài đặt qua các thao tác console
  - Để truy xuất đến Switch bằng Telnet
    - Cần cài một địa chỉ IP
    - Và một Default Gateway

Làm việc trên thiết bị ảo

- Khác với thực tế ở một số điểm:
  - Không thấy các dây cáp
  - Không thấy các cổng giao tiếp
  - Không quản trị thiết bị qua cổng console như thực tế
- Truy xuất vào các thiết bị (ảo) để quản trị theo cách tương tự như dùng Telnet truy xuất vào các thiết bị qua mạng
- Khi đã truy xuất vào một thiết bị ảo, có thể sử dụng các lệnh cấu hình để cài đặt cho thiết bị, giống hệt như đang làm việc trên IOS của Router hay Switch

Phần mềm Boson Netsim

- Là một phần mềm mô phỏng được thiết kế để giúp huấn luyện chuyên viên mạng CCNA, CCNP,…
- Cung cấp:
  - Thiết bị ảo: eRouter, eSwitch, eStation
  - Các liên kết: LAN hay WAN giả lập
  - Các eRouter, eSwitch có giao diện dòng lệnh (CLI) và động thái hoạt động giống hệt như thiết bị thực tế
- Cấu hình phần cứng:
  - Pentium, Celeron hay Athlon: [redacted]1Ghz
  - Windows 98/Me với 128 Mb RAM
  - Windows 2000/XP với 256 Mb RAM
  - Không hỗ trợ Wndows 95 hay Windows NT
  - 100 Mb dung lượng đĩa cứng còn trống

Phần mềm Boson Netsim

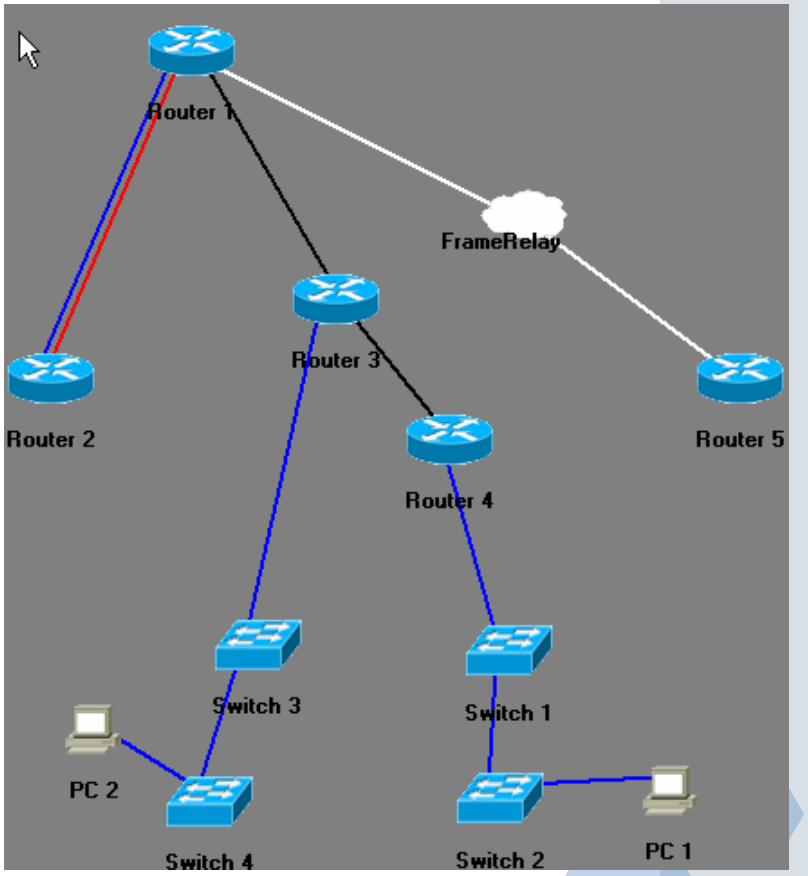
- Yêu cầu:
  - Máy tính phải được cài đặt các giao thức mạng:
  - Control Panel etwork Connections ocal Area Connections
  - Mở Properties xem đã có Client Microsoft Networks và Internet Protocol (TCP/IP) hay chưa
- Sau khi cài đặt xong Boson Netsim:

Quản trị, cấu hình

Thiết kế mạng

Phần mềm Boson Netsim

- Trong sơ đồ mạng mô phỏng, Netsim phân biệt các loại liên kết qua màu sắc:
  - Màu xanh: là Ethernet
  - Màu đỏ là ISDN/DialUp
  - Màu đen là Serial PPP
  - Màu trắng là Serial Frame Relay

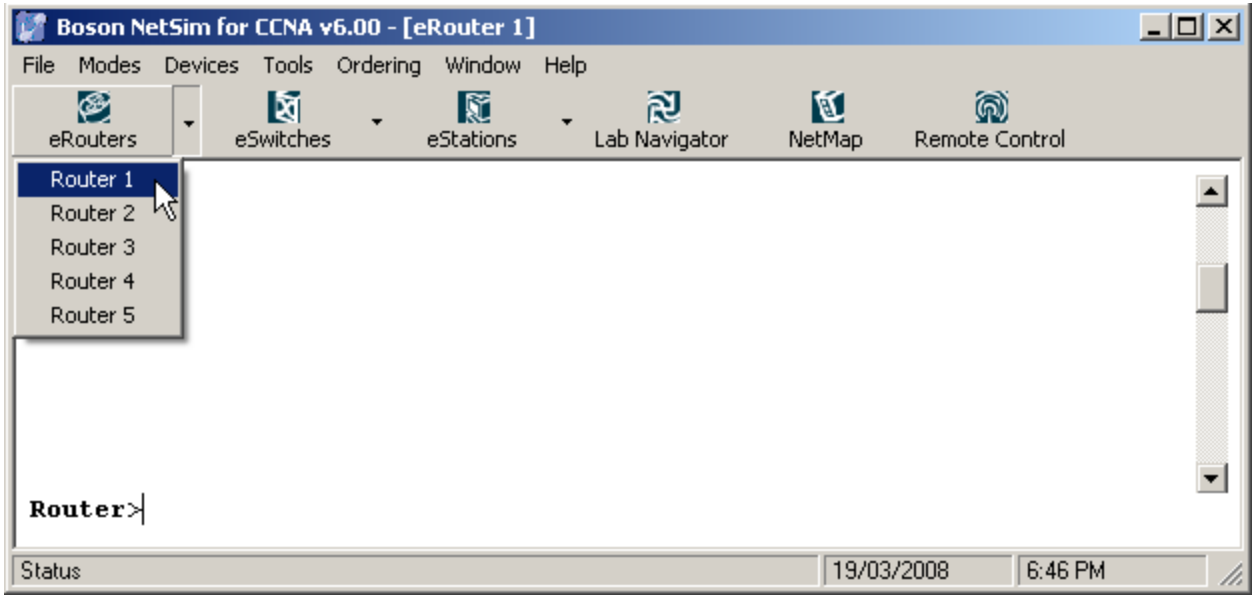


Phần mềm Boson Netsim

- Trong quá trình thực hành trên hệ mô phỏng với một topo mạng đã được nạp, ta phải truy xuất lần lượt vào các thiết bị ảo để tiến hành cấu hình và kiểm thử
- Để truy xuất, Netsim cung cấp một chương trình Telnet mặc định
- Có 4 cách để Telnet:

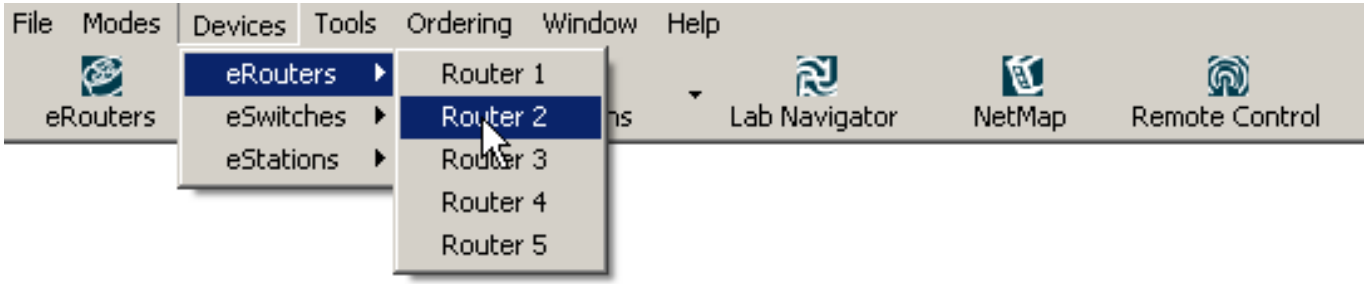
Phần mềm Boson Netsim

- Phương pháp 1:
  - Quan sát trên thanh công cụ sẽ thấy các biểu tượng thiết bị
  - Muốn Telnet vào thiết bị nào thì chọn thiết bị đó trong danh sách
  - Xuất hiện "Press Enter to Start"
  - Ấn Enter sẽ xuất hiện dấu nhắc hệ thống



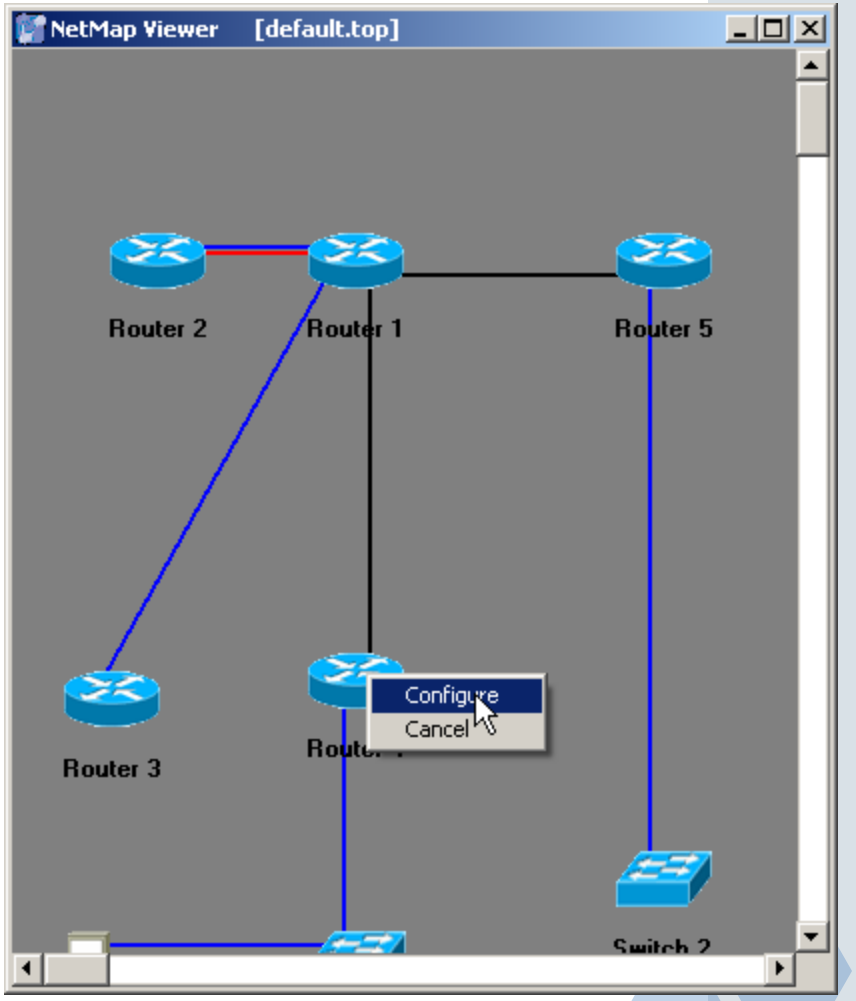
Phần mềm Boson Netsim

- Phương pháp 2:
  - Chọn thực đơn Devices
  - Xuất hiện các nhóm thiết bị
  - Thao tác giống như phương pháp 1



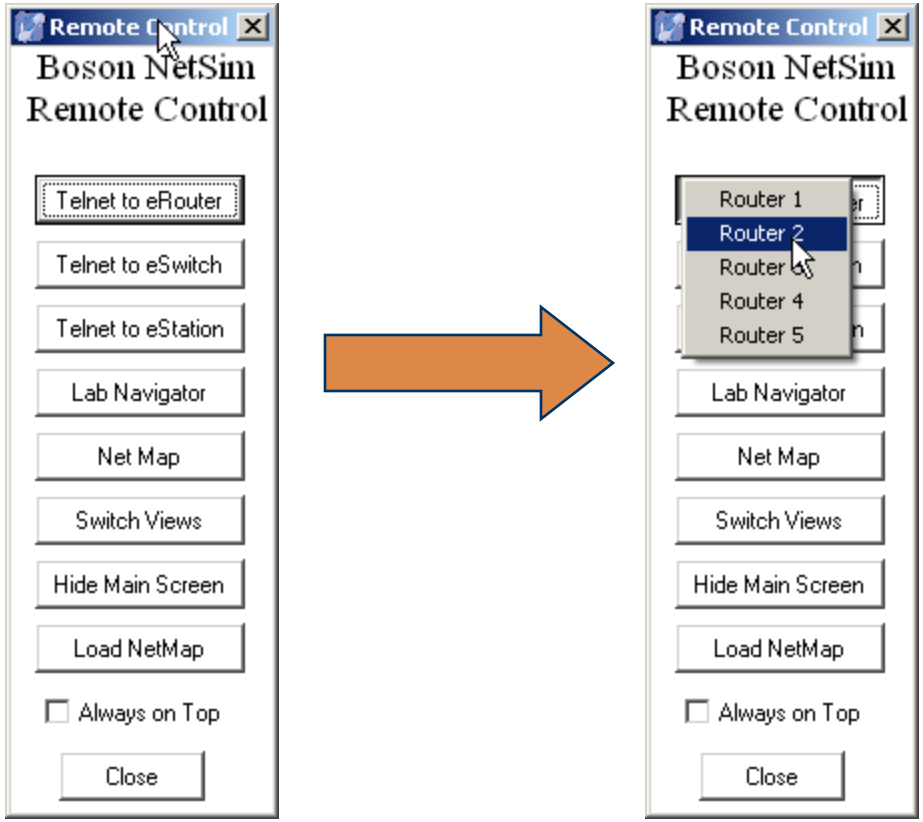
Phần mềm Boson Netsim

- Phương pháp 3:
  - Làm việc trực tiếp trên thiết bị mạng đang hiển thị
  - Chọn NetMap để hiển thị
  - Muốn Telnet vào thiết bị nào thì ấn phải chuột vào thiết bị đó, chọn Configure



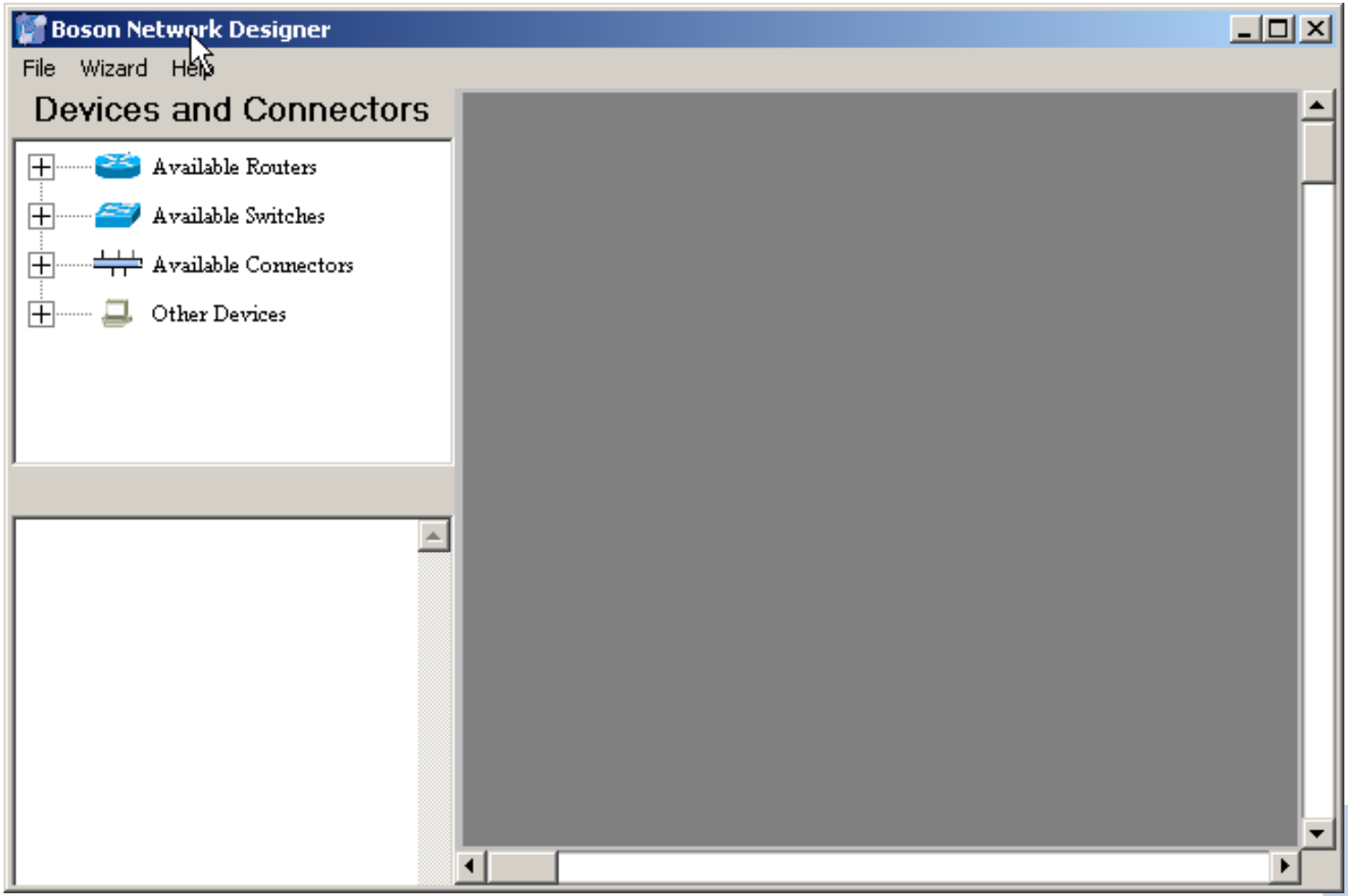
Phần mềm Boson Netsim

- Phương pháp 3:
  - Chương trình mô phỏng cung cấp một thanh công cụ chuyên hỗ trợ điều khiển gọi là Boson Netsim Remote Control
  - Bấm nút Remote Control để mở thanh công cụ ra



Sử dụng Network Designer

- Cho phép tạo ra một mạng mô phỏng tùy ý

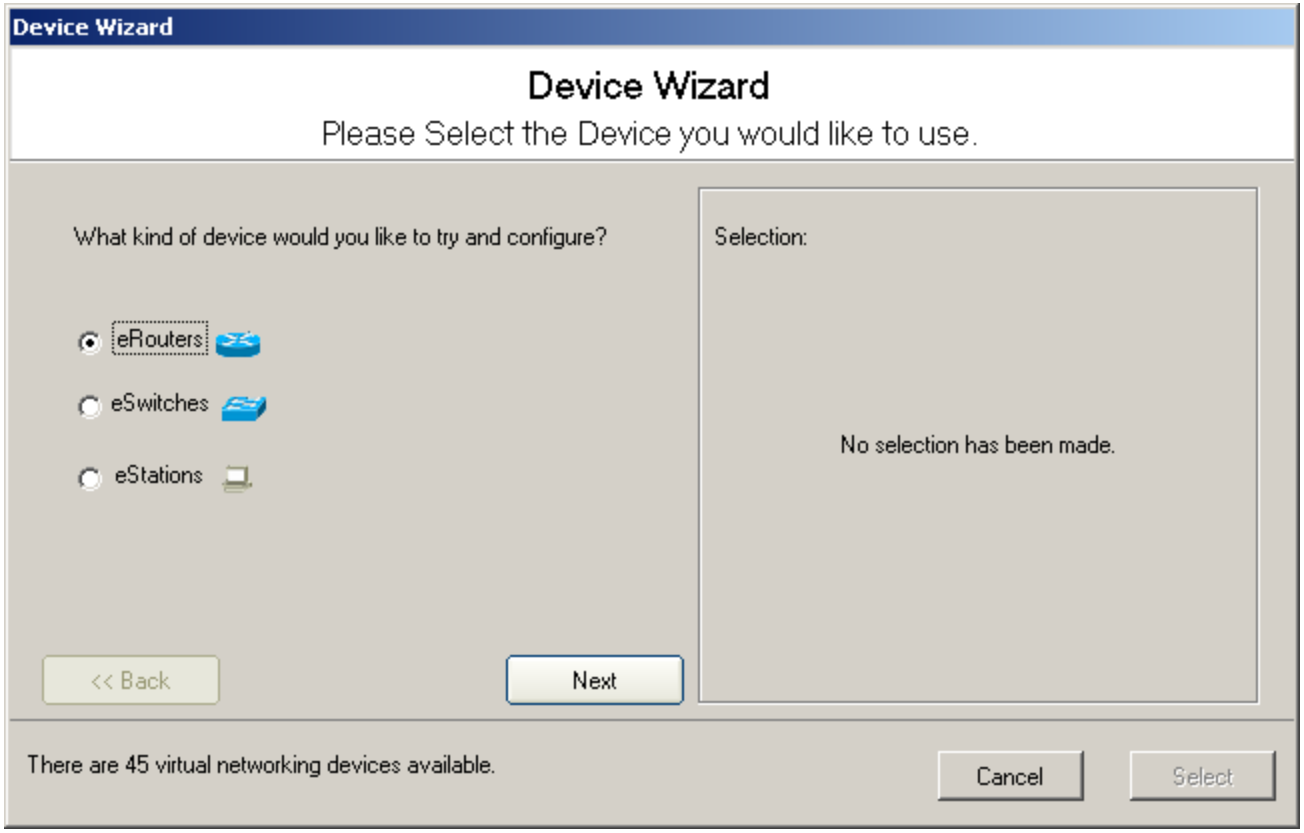


Sử dụng Network Designer

- Các bước thực hiện:
  1. Nạp Boson Network Designer từ File ew Netmap hoặc vào Start rograms oson Software . Network Designer
  2. Tạo topo mạng qua giao diện đồ họa
  3. Xác định các kết nối vật lý
  4. Lưu (Save) topo mạng bằng một tệp tin tự đặt (*.top)
  5. Thoát khỏi Network Designer và vào NetSim
  6. Từ File pad NetMap
  7. Chỉ ra tên tệp tin lưu giữ topo mạng vừa tạo
- Trong NetSim có thể xem cấu hình vật lý của mạng thông qua nút NetMap để hiện màn hình NetMap Viewer

Sử dụng Network Designer

- Nếu không muốn thêm thiết bị vào topo mạng qua thao tác trực tiếp trên giao diện đồ họa của Network Designer ta có thể dùng "Add Devices Wizard"



Sử dụng Network Designer

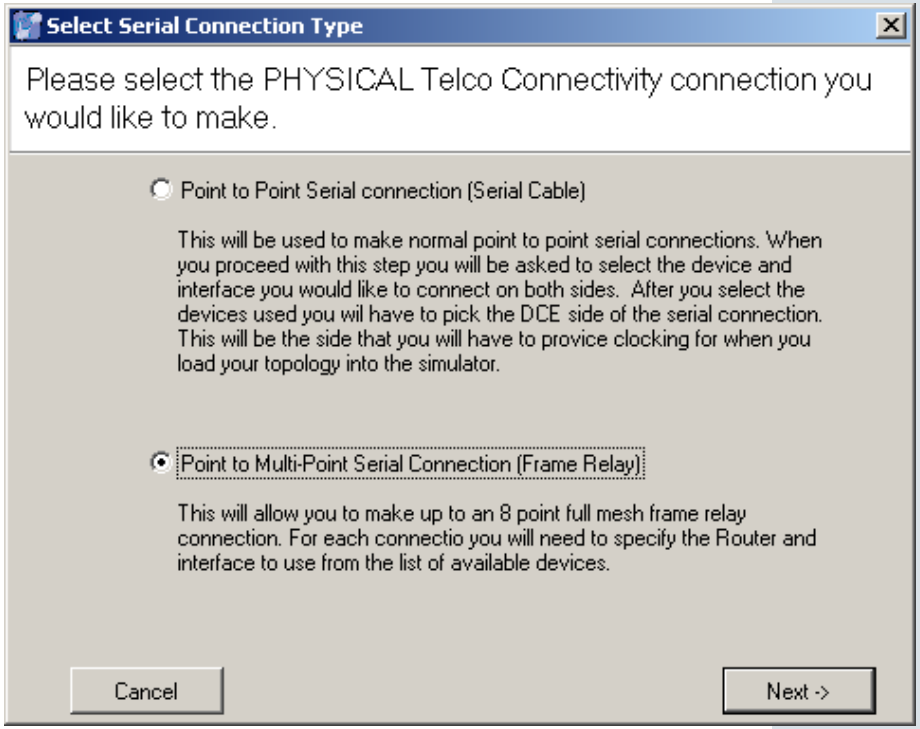
- Muốn xem thông tin về một thiết bị, nháy đúp chuột vào thiết bị đó
- Để bổ sung một kết nối vào topo mạng:
  - Thao tác trực tiếp bằng cách kéo thả kiểu kết nối vào vùng làm việc
  - Boson NetSim cung cấp 5 loại kết nối khác nhau:
    - Serial
    - Ethernet
    - Fast Ethernet (được chọn trong nhóm Ethernet)
    - ISDN
    - Frame Relay (được chọn từ Serial)
  - Hoặc có thể dùng Make Connection Wizard

Sử dụng Network Designer

- Tạo kết nối Ethernet giữa hai thiết bị:
  - Về nguyên tắc trước hết phải tạo ít nhất một thiết bị cho topo mạng của mình. Nếu chưa có thiết bị nào mà tạo kết nối thì chương trình sẽ báo lỗi.
  - Có 3 cách tạo kết nối Ethernet:
    - Cách thứ nhất: Dùng chuột kéo và thả kết nối Ethernet từ trái sang phải màn hình
    - Cách thứ hai: Dùng tùy chọn Make Connection Wizard trong menu Wizard. Chọn Ethernet [redacted]ext
    - Cách thứ ba: ấn phím phải chuột lên thiết bị muốn tạo kết nối Ethernet, rồi chọn Add Connection to:
  - Chương trình xuất hiện hộp thoại New Connection, trong đó liệt kê tất cả các cổng Ethernet liên quan đến loại kết nối Ethernet đang được chọn
  - Chọn mỗi thiết bị với cổng Ethernet tương ứng [redacted]nish

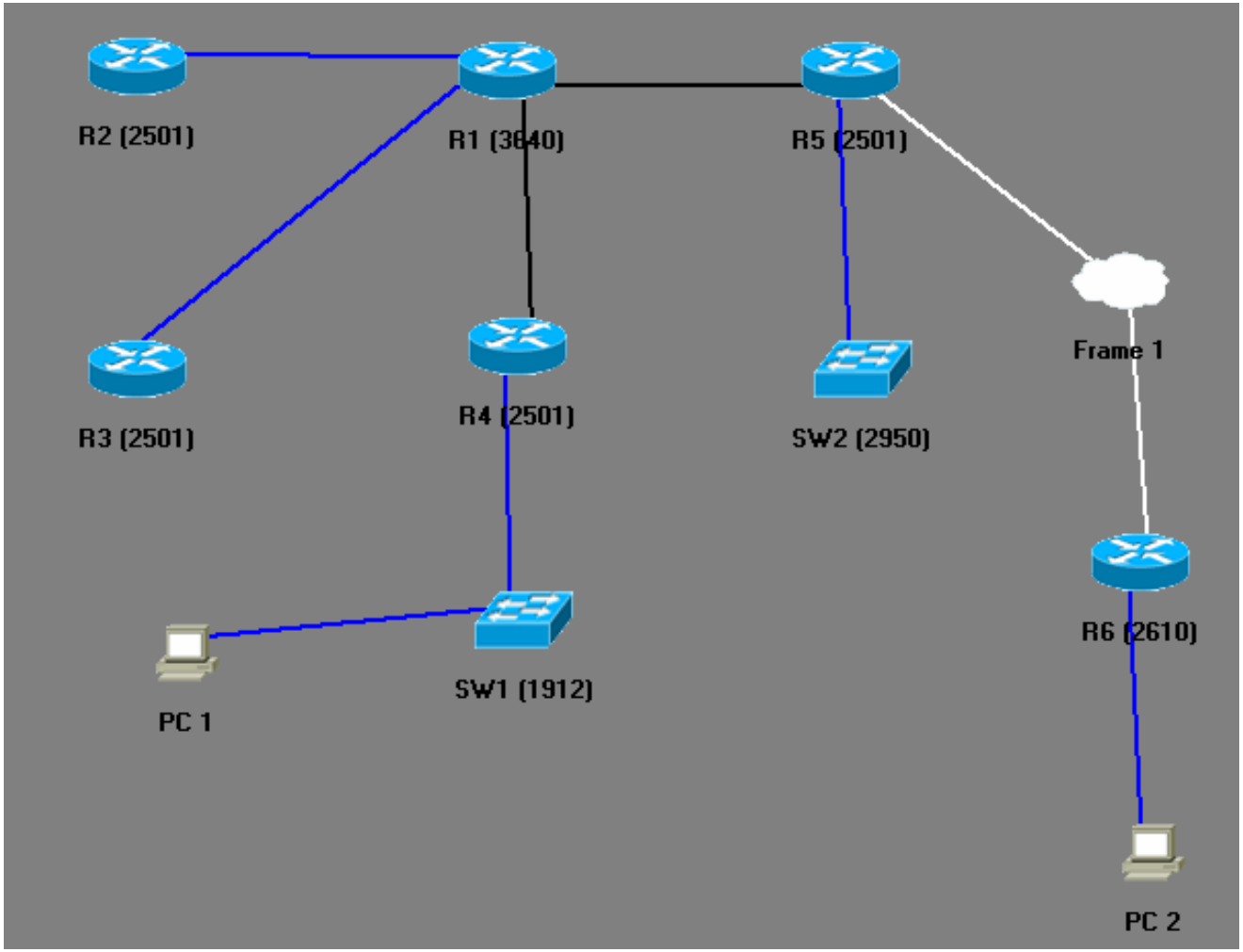
Sử dụng Network Designer

- Tạo kết nối Frame Relay:
  - Cơ bản cũng như tạo các kết nối khác
  - Chương trình cung cấp 2 dạng:
    - Point to Point Serial Connection
    - Point to Multi-Point Serial Connection
  - Nếu chọn Point to Multi-Point Serial Connection thì sẽ xuất hiện cửa sổ chọn thiết bị và cổng tương ứng để nối mạng Frame Relay
- Muốn xóa một kết nối nào, ấn phải chuột vào thiết bị có kết nối đó, chọn Remove Connection to:, chọn kết nối tương ứng muốn xóa.



Các bài thực hành cơ bản

- Sử dụng Network Designer xây dựng topo mạng:



Xây dựng topo mạng

- Chi tiết:
  - Router 1 (3640) là model 3640, chọn slot 0 có 4 cổng Ethernet, slot 1 có 4 cổng Serial và Slot 2 có 1 cổng BRI
  - Các Router từ Router 2 đến Router 5 đều là model 2501
  - Router 6 (2610) là model 2610, chọn slot 0 có 1 cổng Serial và slot 1 có 2 cổng Serial
- Thông tin tạo kết nối:

Thiết bị	Cổng trên thiết bị	Nối đến (thiết bị, cổng)
Router 1	E0/0	Router 2, E0
	E0/1	Router 3, E0
	S1/0	Router 4, S0
	S1/1	Router 5, S0
Router 2	E0	Router 1, E0/0

Xây dựng topo mạng

Thiết bị	Cổng trên thiết bị	Nối đến (thiết bị, cổng)
Router 3	E0	Router 1, E0/1
Router 4	E0	SW1, E0/1
	S0	Router 1, S1/0
Router 5	E0	SW2, Fast Ethernet 0/1
	S0	Router 1, S1/1
	S1 (Frame Relay)	Router 6, S0
Router 6	E0	PC2, E0
	S0 (Frame Relay)	Router 5, S1
SW1	E0/1	Router 4, E0
	E0/2	PC1, E0
SW2	Fast Ethernet 0/1	Router 5, E0
PC1	E0	SW1, E0/2
PC2	E0	Router 6, E0

Kết nối và đăng nhập vào một Router

- Mục đích:
  - Làm quen Router, biết được các chế độ làm việc trên Cisco IOS
  - Thực hiện thao tác đăng nhập Router trong chương trình mô phỏng
  - Tiếp xúc với giao diện giống như khi console vào một router thật
- Thực hành:
  - Bước 1: Trong NetSim chọn Router 1. Trên màn hình xuất hiện "Press Enter to Start" (Nếu để Beginner mode). Nhấn Enter để tiếp tục, lúc này màn hình xuất hiện dấu nhắc Router>. Lúc này ta đang ở chế độ **user mode**
  - Bước 2: Nhập lệnh enable để vào Privileged mode

    Router>enable

    Router#

Kết nối và đăng nhập vào một Router

- Bước 3: Để quay trở về user mode, gõ lệnh disable, rồi từ user mode gõ logout hay exit để thoát khỏi router

  Router#disable

  Router>

  Router>exit

  Router con0 is now available

  Press RETURN to get started

- Bước 4: Tiếp tục quay trở lại user mode và Privileged mode, vào chế độ cấu hình toàn cục (global config mode)

  <Enter>

  Router>enable

  Router#config terminal

  Router(config)#

- Bước 5: Thoát ra khỏi chế độ cấu hình toàn cục bằng lệnh **exit**

  Router(config)#exit

  Router#

Bài 2: Làm quen với giao tiếp USER cơ bản

- Mục đích:
  - Làm quen với giao diện dòng lệnh CLI (Command Line Interface) của hệ điều hành Cisco IOS
  - Làm việc với các chế độ giao tiếp: user mode, Privileged mode
  - Thực hành các lệnh trợ giúp cơ bản và các lệnh hiển thị (show) thông tin các loại
- Thực hành
  - Bước 1: Chọn lại Router R1 (3640) để vào user mode
  - Bước 2: Gõ lệnh ? Để hiển thị tất cả các lệnh khả dụng tại dấu nhắc này

    Router>?
  - Bước 3: Vào Privileged mode

    Router>enable

    Router#

Bài 2: Làm quen với giao tiếp USER cơ bản

- Bước 4: Hiển thị các lệnh khả dụng tại dấu nhắc này

  Router#?
- Bước 5: Hiển thị tất cả các lệnh show

  Router#show ?
- Bước 6: Hiển thị cấu hình hiện hành (đang được dùng trong router)

  Router#show running-config
- Bước 7: Nếu thấy xuất hiện dấu nhắc more, gõ phím cách (space bar) để xem thông tin kế tiếp
- Bước 8: Thoát khỏi router.

  Router#exit

Hay

  Router#disable

Bài 3: Thực hành các lệnh SHOW cơ bản

- Mục đích:
  - Biết được những gì đã xác lập bên trong Router
  - Có hướng xử lý cấu hình thích hợp
- Thực hành
  - Bước 1: Chọn Router 1, vào user mode

    Router>
  - Bước 2: Vào Privileged mode

    Router>enable

    Router#
  - Bước 3: Xem cấu hình hoạt động hiện hành trong bộ nhớ. Dùng lệnh "running-config". Trong user mode không thể dùng lện show này, lệnh chỉ khả dụng trong Privileged mode

    Router#show running-config

Bài 3: Thực hành các lệnh SHOW cơ bản

- Bước 4: Flash memory là bộ nhớ lưu giữ hệ điều hành của router (Operating system image file). Xem nội dung của Flash

  Router#show flash
- Bước 5: Giao diện dòng lệnh của router mặc định lưu giữ 10 lệnh mới dùng gần nhất. Xem lại các lệnh đã dùng:

  Router#show history
- Bước 6: Lấy lại lệnh ngay kế trước: ấn mũi tên hướng lên hoặc ^P (CTRL + P)
- Bước 7: Lấy lệnh kế tiếp trong bộ đệm quá khứ: ấn mũi tên hướng xuống hoặc ^N
- Bước 8: Xem trạng thái của giao thức định tuyến hiện hành tại lớp mạng (Network layer)

  Router#show protocols
- Bước 9: Xem phiên bản và một số thông tin hệ thống của router

  Router#show version

Bài 3: Thực hành các lệnh SHOW cơ bản

- Bước 10: Xem đồng hồ của router

  Router#show clock
- Bước 11: Hiển thị danh sách các host và các địa chỉ IP trên giao tiếp của chúng:

  Router#show hosts
- Bước 12: Xem danh sách tất cả các user được nối đến router

  Router#show users
- Bước 13: Xem thông tin chi tiết về mỗi giao tiếp

  Router#show interfaces
- Bước 14: Xem trạng thái toàn cục và trạng thái giao tiếp của bất kỳ giao thức lớp mạng nào

  Router#show protocols
- Nếu muốn đổi tên Host thì vào chế độ cấu hình toàn cục

  Router#conf t

  Router(config)#hostname R1

  R1(config)#

Bài 4: Thực hành lệnh cài đặt mật khẩu

- Mục đích:
  - Luyện tập lại các thao tác ban đầu
  - Cấu hình mật khẩu đăng nhập router
- Thực hành
  - Bước 1: Đăng nhập Router 1, lúc này đang có tên host là R1

    R1>
  - Bước 2: Vào Privileged mode

    R1>enable

    R1#
  - Bước 3: Xem tất cả các lệnh khả dụng trong Privileged mode

    R1#?
  - Bước 4: Vào chế độ cấu hình

    R1#config terminal

    R1(config)#

Bài 4: Thực hành lệnh cài đặt mật khẩu

- Bước 5: Tên host của router được dùng cho nhận dạng router. Thường chỉ ra vị trí (địa danh) hay chức năng của router. Ví dụ: có thể đặt lại tên host cho router 1 là Saigon như sau:

  R1(config)#hostname Saigon

  Saigon(config)#
- Bước 6: "Mật khẩu (password) cho phép" kiểm soát truy xuất vào Privileged mode là mật khẩu hết sức quan trọng, bởi trong chế độ này hoàn toàn có thể thay đổi các thông số cấu hình. Giả sử đặt mật khẩu này là milan007 bằng câu lệnh sau:

  Saigon(config)#enable password milan007
- Bước 7: Kiểm tra lại mật khẩu này. Thoát khỏi router và đăng nhập trở lại vào chế độ Privileged mode

```
R1>enable
Enter password:
R1#
```

Bài 4: Thực hành lệnh cài đặt mật khẩu

- Bước 8: Điều lo ngại đối với "mật khẩu cho phép" này là nó xuất hiện dưới dạng tường minh trong tệp tin cấu hình của router. Nếu ai đó xem tệp tin cấu hình (show running-config) thì tính an toàn của hệ thống bị phá vỡ bởi mật khẩu bị lộ.

```
hostname R1
enable password milan007
```

  Vì vậy cần mật mã mật khẩu này, đặt lại mật khẩu là "ciao" có mật mã bằng lệnh sau:

  Saigon(config)#enable secret ciao

- Bước 9: Kiểm tra lại hiệu lực của mật khẩu này bằng cách thoát ra rồi đăng nhập lại Privileged mode. "Mật khẩu mật mã" sẽ phủ quết "mật khẩu cho phép". Nếu có 2 mật khẩu cùng tồn tại thì "mật khẩu mật mã" sẽ là mật khẩu được dùng để đăng nhập vào Privileged mode.

```
hostname R1
enable secret 5 $sdf$6978yhg$jnb76sd
enable password milan007
```

Một số lệnh cần chú ý

- Cho phép giao tiếp hoạt động
  - Ví dụ:
    - Cho phép giao tiếp Serial 1/0 trên Router 1

    R1(config)#interface Serial 1/0

    R1(config-if)#no shutdown (cho phép một giao tiếp được cấu hình, đổi trạng thái từ **down** sang **up**)

    - Cho phép giao tiếp Ethernet 0/0 trên Router 1

    R1(config)#interface Ethernet 0/0

    R1(config-if)#no shutdown

    - Cho phép giao tiếp Serial 0 trên Router 4

    R4(config)#interface Serial 0

    R4(config-if)#no shutdown

Một số lệnh cần chú ý

- Một số lệnh xem thông tin CDP (Cisco Discovery Protocol)
  - Giao thức thăm dò, mặc định trên các thiết bị
  - Hoạt động ở tầng liên kết dữ liệu
  - Không định tuyến, chỉ có thể lan truyền trực tiếp giữa các thiết bị kết nối nhau

show cdp interface	Xem các cài đặt CDP trên giao tiếp
show cdp neighbor	Xem thông tin CDP của các thiết bị láng giềng
show cdp neighbor detail	Xem thông tin CDP chi tiết của các thiết bị láng giềng
show cdp	Xem thông tin CDP tổng quát

Bài 5: Cấu hình giao tiếp

- Mục đích:
  - Cho phép các giao tiếp trên Router
  - Làm cho giao tiếp thực sự mở (dùng Router 1 và Router 2)
- Thực hành:
  - Bước 1: Đăng nhập vào Router 1, và vào chế độ cấu hình để thay đổi host thành Saigon

    Router(config)#hostname Saigon
  - Bước 2: Cấu hình cho một giao tiếp Ethernet, chọn Ethernet 0/0. Trước hết, gõ lệnh để vào chế độ cấu hình:

    Saigon(config)#interface Ethernet 0/0
  - Bước 3: Gõ lệnh ? Để xem tất cả các lệnh khả dụng trong chế độ cấu hình giao tiếp này. Sử dụng lệnh mở Ethernet 0/0

    Saigon(config-if)#no shutdown

  Xem thông tin giao tiếp bằng lệnh Saigon#show interface

Bài 5: Cấu hình giao tiếp

- Bước 4: Bây giờ đăng nhập vào Router 2, thay đổi host thành Hanoi và giao tiếp Ethernet 0

  Router(config)#hostname Hanoi

  Hanoi(config)#interface Ethernet 0
- Bước 5: Cho phép giao tiếp Ethernet 0

  Hanoi(config-if)#no shutdown
- Bước 6: Lúc này giao tiếp Ethernet trên cả hai phía đều đã được cho phép, có thể xem bằng CDP

  Hanoi(config-if)#end

  Hanoi#show cdp neighbors
- Bước 7: Trở lại Router 1, vào chế độ cấu hình giao tiếp Serial 1/0. Cấu hình cho liên kết có băng thông 64kbps

  Saigon(config)#conf t

  Saigon(config-if)#interface serial 1/0

Bài 5: Cấu hình giao tiếp

```
Saigon(config-if)#bandwidth 64
Saigon(config-if)#clock rate 64000
Saigon(config-if)#no shut
Saigon(config-if)#exit
Saigon(config)#exit
Saigon#show interface serial 1/0
```

Bài 6: Cấu hình giao thức IP cho Router

- Mục đích:
  - Cấu hình cho Router 1, Router 2, Router 4 với các địa chỉ IP
  - Thực hiện lệnh **Ping** giữa chúng để thử kết nối
- Thực hành:
  - Bước 1: Đăng nhập vào Router 1 và thay đổi host thành R1

    Router(config)#hostname R1
  - Bước 2: Vào chế độ cấu hình cho giao tiếp Ethernet 0/0 để cài đặt địa chỉ IP cho giao tiếp

    R1(config)#interface Ethernet 0/0

    R1(config-if)#
  - Bước 3: Cài địa chỉ IP cho giao tiếp Ethernet 0/0 là 10.1.1.1 255.0.0.0

    R1(config-if)#ip address 10.1.1.1 255.0.0.0

Bài 6: Cấu hình giao thức IP cho Router

- Bước 4: Cho phép giao tiếp này

  R1(config-if)#no shutdown
- Bước 5: Cài địa chỉ IP trên giao tiếp Serial 1/0 là 192.16.10.1 255.255.255.0

  R1(config)#interface Serial 1/0

  R1(config-if)#ip address 192.16.10.1 255.255.255.0

  R1(config-if)#no shutdown
- Bước 6: Kết nối đến Router 2 và đổi tên host thành R2
- Bước 7: Cài địa chỉ IP cho giao tiếp Ethernet 0 là 10.1.1.2 255.0.0.0

  R2(config)#interface Ethernet 0

  R2(config-if)#ip address 10.1.1.2 255.0.0.0
- Bước 8: Cho phép giao tiếp này

  R2(config-if)#no shutdown

Bài 6: Cấu hình giao thức IP cho Router

- Bước 9: Kết nối với Router 4 và đổi tên host thành R4
- Bước 10: Cài địa chỉ IP cho giao tiếp Serial 0 là 192.16.10.2 255.255.255.0

  R4(config)#interface Serial 0

  R4(config-if)#ip address 192.16.10.2 255.255.255.0
- Bước 11: Cho phép giao tiếp này

  R4(config-if)#no shutdown
- Bước 12: Kết nối trở lại Router 1
- Bước 13: Thử Ping đến giao tiếp Ethernet trên Router 2

  R1#ping 10.1.1.2
- Bước 14: Thử Ping đến giao tiếp Serial trên Router 4

  R1#ping 192.16.10.2
- Bước 15: Kiểm tra xem đường dây và giao thức trên giao tiếp có ở trạng thái mở (up) hay không

  R1#show ip interface brief

Bài 6: Cấu hình giao thức IP cho Router

- Bước 16: Xem cấu hình hiện hành và xác nhận sự hiện diện của địa chỉ IP

  R1#show running-config
- Bước 17: Hiển thị thông tin chi tiết về IP trên giao tiếp

  R1#show ip interface
- Bước 18: Trên Router 1, liên kết tên 'router4' với địa chỉ IP ở xa 192.16.10.2. Điều này cho phép thực hiện lệnh ping bằng tên 'router4' thay vì phải nhớ địa chỉ của nó.

  R1#ip host Router4 192.16.10.2
- Bước 19: Kiểm tra lại tên trong bảng host của Router 1 bằng lệnh **show hosts**

  R1#show hosts
- Bước 20: Thử ping Router 4 bằng tên

  R1#router4

Bài 7: Đặt địa chỉ IP cho PC

- Yêu cầu:
  - Dùng Router 4 và PC 1
- Thực hành:
  - Bước 1: Kết nối đến Router 4 và vào chế độ cấu hình toàn cục

    Router(config)#
  - Bước 2: Đặt tên host là R4

    Router(config)#hostname R4

    R4(config)#
  - Bước 3: Vào chế độ cấu hình giao tiếp Ethernet 0

    R4(config)#interface Ethernet 0

    R4(config-if)#
  - Bước 4: Gán địa chỉ IP 20.24.1.1 255.255.255.0 cho giao tiếp

    R4(config-if)#ip address 20.24.1.1 255.255.255.0

Bài 7: Đặt địa chỉ IP cho PC

- Bước 5: Mở giao tiếp này

  R4(config-if)#no shutdown
- Bước 6: Chuyển đến PC1, nhập lệnh để cấu hình địa chỉ IP và default gateway cho PC1. Gán địa chỉ IP là 20.24.1.150 với mặt nạ 255.255.255.0. Gán default gateway là giao tiếp Ethernet 0 của Router 4 với đại chỉ IP 20.24.1.1

  C:>ipconfig /ip 20.24.1.150 255.255.255.0

  C:>ipconfig /dg 20.24.1.1
- Bước 7: Thực hiện lệnh Ping để kiểm tra kết nối

  C:>ping 20.24.1.1

Bài 8: Cấu hình SWITCH

- Mục đích:
  - Làm quen với một số chủ đề cơ bản của họ Switch 1900
  - Dùng SW 1 để thực hành
- Thực hành:
  - Bước 1: Kết nối đến SW1 bằng cách nháy chuột vào SW1(1912)

    >
  - Bước 2: Hiển thị phiên bản hệ điều hành của Switch

    >show version
  - Bước 3: Xem thông tin về các giao tiếp của Switch

    >show interfaces
  - Bước 4: Hiển thị bảng địa chỉ MAC

    >show mac-address-table
  - Bước 5: Vào chế độ Privileged mode, cho phép điều khiển tổng thể Swith

    >enable

Bài 8: Cấu hình SWITCH

- Bước 6: Hiển thị cấu hình hoạt động hiện hành của Switch

  #show running-config
- Bước 7: Để cấu hình Switch, cũng phải vào chế độ cấu hình toàn cục bằng lệnh config terminal

  #config terminal

  (config)#
- Bước 8: Thay đổi tên cho Switch

  (config)#hostname <tên>
- Bước 9: Mật khẩu cho phép (enable password) kiểm soát hoạt động truy xuất vào Privileged mode. Đây là mật khẩu rất quan trọng vì có thể làm thay đổi cấu hình của Switch. Trên họ Switch 1900 có nhiều mức cần phải đặt khi khai báo mật khẩu.

Ví dụ: đặt mật khẩu cho phép là 'milan'

(config)#enable password level 15 milan

Kiểm thử lại mật khẩu vừa đặt, bằng cách thoát khỏi Switch và đăng nhập vào lại Privileged mode.

Bài 8: Cấu hình SWITCH

- Bước 10: Đối với mật khẩu cho phép có một khuyết điểm đó là mật khẩu này xuất hiện dưới dạng bản rõ (plain text) trong tệp cấu hình của switch, điều này sẽ rất nguy hiểm nếu ai đó xem được tệp tin cấu hình.
- Cần tạo mật khẩu được bảo mật, ví dụ tạo mật khẩu là 'ciao'

  (config)#enable secret level 15 ciao

Mật khẩu bảo mật là một mật khẩu bổ sung, nó phủ quyết mật khẩu cho phép. Nếu trên hệ thống có cả hai mật khẩu thì mật khẩu bảo mật là mật khẩu vào Privileged mode. Mật khẩu cho phép vẫn còn nhưng đã bị vô hiệu

PHẦN I
KHÁI QUÁT VỀ CÔNG NGHỆ MẠNG

Chương 1: Tổng quan về công nghệ mạng máy tính và mạng cục bộ

Chương này cung cấp các khái niệm, các kiến thức cơ bản nhất về mạng máy tính và phân loại mạng máy tính. Các nội dung giới thiệu mang tính tổng quan về mạng cục bộ, kiến trúc mạng cục bộ, phương pháp truy cập trong mạng cục bộ và các chuẩn vật lý về các thiết bị mạng. Đây là những kiến thức cơ bản rất hữu ích do phạm vi sử dụng của mạng cục bộ là đang phổ biến hiện nay. Hầu hết các cơ quan, tổ chức, công ty có sử dụng công nghệ thông tin đều thiết lập mạng cục bộ riêng.

Các khái niệm, nội dung cơ bản trong chương 1 cần phải nắm vững đối với tất cả các học viên vì chúng sẽ được sử dụng nhiều trong các chương tiếp theo.

Mục 1: Mạng máy tính

I. Lịch sử mạng máy tính

Internet bắt nguồn từ đề án ARPANET (Advanced Research Project Agency Network) khởi sự trong năm 1969 bởi Bộ Quốc phòng Mỹ (American Department of Defense). Đề án ARPANET với sự tham gia của một số trung tâm nghiên cứu, đại học tại Mỹ (UCLA, Stanford, . . .) nhằm mục đích thiết kế một mạng WAN (Wide Area Network) có khả năng tự bảo tồn chống lại sự phá hoại một phân mạng bằng chiến tranh nguyên tử. Đề án này dẫn tới sự ra đời của nghi thức truyền IP (Internet Protocol). Theo nghi thức này, thông tin truyền sẽ được đóng thành các gói dữ liệu và truyền trên mạng theo nhiều đường khác nhau từ người gửi tới nơi người nhận. Một hệ thống máy tính nối trên mạng gọi là **Router** làm nhiệm vụ tìm đường đi tối ưu cho các gói dữ liệu,

tất cả các máy tính trên mạng đều tham dự vào việc truyền dữ liệu, nhờ vậy nếu một phân mạng bị phá huỷ các **Router** có thể tìm đường khác để truyền thông tin tới người nhận. Mạng ARPANET được phát triển và sử dụng trước hết trong các trường đại học, các cơ quan nhà nước Mỹ, tiếp theo đó, các trung tâm tính toán lớn, các trung tâm truyền vô tuyến điện và vệ tinh được nối vào mạng, . . . trên cơ sở này, ARPANET được nối với khắp các vùng trên thế giới.

Tới năm 1983, trước sự thành công của việc triển khai mạng ARPANET, Bộ quốc phòng Mỹ tách một phân mạng giành riêng cho quân đội Mỹ(MILNET). Phần còn lại, gọi là NSFnet, được quản lý bởi NSF (National Science Foundation) NSF dùng 5 siêu máy tính để làm **Router** cho mạng, và lập một tổ chức không chính phủ để quản lý mạng, chủ yếu dùng cho đại học và nghiên cứu cơ bản trên toàn thế giới. Tới năm 1987, NSFnet mở cửa cho cá nhân và cho các công ty tư nhân (BITnet), tới năm 1988 siêu mạng được mang tên INTERNET.

Tuy nhiên cho tới năm 1988, việc sử dụng INTERNET còn hạn chế trong các dịch vụ truyền mạng (FTP), thư điện tử(E-mail), truy nhập từ xa(TELNET) không thích ứng với nhu cầu kinh tế và đời sống hàng ngày. INTERNET chủ yếu được dùng trong môi trường nghiên cứu khoa học và giảng dạy đại học. Trong năm 1988, tại trung tâm nghiên cứu nguyên tử của Pháp CERN(Centre Européen de Recherche Nuclaire) ra đời đề án *Mạng nhện thế giới* WWW(World Wide Web). Đề án này, nhằm xây dựng một phương thức mới sử dụng INTERNET, gọi là phương thức *Siêu văn bản* (HyperText). Các tài liệu và hình ảnh được trình bày bằng ngôn ngữ HTML (HyperText Markup Language) và được phát hành trên INTERNET qua các hệ chủ làm việc với nghi thức HTTP (HyperText Transport Protocol). Từ năm 1992, phương thức làm việc này được đưa ra thử nghiêm trên INTERNET. Rất nhanh chóng, các công ty tư nhân tìm thấy qua phương thức này cách sử dụng INTERNET trong kinh tế và đời sống. Vốn đầu tư vào INTERNET được nhân lên hàng chục lần. Từ năm 1994 INTERNET trở thành siêu mạng kinh doanh. Số các công ty sử dụng INTERNET vào việc kinh doanh và quảng cáo lên gấp hàng nghìn lần kể từ năm 1995. Doanh số giao dịch thương mại qua mạng INTERNET lên hàng chục tỉ USD trong năm 1996 . . .

Với phương thức siêu văn bản, người sử dụng, qua một phần mềm truy đọc (Navigator), có thể tìm đọc tất cả các tài liệu siêu văn bản công bố tại mọi nơi trên thế giới (kể cả hình ảnh và tiếng nói). Với công nghệ WWW, chúng ta

bước vào giai đoạn mà mọi thông tin có thể có ngay trên bàn làm việc của mình. Mỗi công ty hoặc người sử dụng, được phân phối một *trang cội nguồn* (Home Page) trên hệ chủ HTTP. Trang cội nguồn, là siêu văn bản gốc, để tự do có thể tìm tới tất cả các siêu văn bản khác mà người sử dụng muốn phát hành. Địa chỉ của trang cội nguồn được tìm thấy từ khắp mọi nơi trên thế giới. Vì vậy, đối với một xí nghiệp, trang cội nguồn trở thành một văn phòng đại diện điện tử trên INTERNET. Từ khắp mọi nơi, khách hàng có thể xem các quảng cáo và liên hệ trực tiếp với xí nghiệp qua các dòng siêu liên (HyperLink) trong siêu văn bản.

Tới năm 1994, một điểm yếu của INTERNET là không có khả năng lập trình cục bộ, vì các máy nối vào mạng không đồng bộ và không tương thích. Thiếu khả năng này, INTERNET chỉ được dùng trong việc phát hành và truyền thông tin chứ không dùng để xử lý thông tin được. Trong năm 1994, hãng máy tính SUN Corporation công bố một ngôn ngữ mới, gọi là JAVA(cafe), cho phép lập trình cục bộ trên INTERNET, các chương trình JAVA được gọi thẳng từ các siêu văn bản qua các siêu liên (Applet). Vào mùa thu năm 1995, ngôn ngữ JAVA chính thức ra đời, đánh dấu một bước tiến quan trọng trong việc sử dụng INTERNET. Trước hết, ***một chương trình JAVA, sẽ được chạy trên máy khách (Workstation) chứ không phải trên máy chủ (server). Điều này cho phép sử dụng công suất của tất cả các máy khách vào việc xử lý số liệu. Hàng triệu máy tính (hoặc vi tính) có thể thực hiện cùng một lúc một chương trình ghi trên một siêu văn bản trong máy chủ***. Việc lập trình trên INTERNET cho phép truy nhập từ một trang siêu văn bản vào các chương trình xử lý thông tin, đặc biệt là các chương trình điều hành và quản lý thông tin của một xí nghiệp. phương thức làm việc này, được gọi là INTRANET. Chỉ trong năm 1995-1996, hàng trăm nghìn dịch vụ phần mềm INTRANET được phát triển. Nhiều hãng máy tính và phần mềm như Microsoft, SUN, IBM, Oracle, Netscape,... đã phát triển và kinh doanh hàng loạt phần mềm hệ thống và phần mềm cơ bản để phát triển các ứng dụng INTERNET / INTRANET.

II. Giới thiệu mạng máy tính

I.1. I.Định nghĩa mạng máy tính và mục đích của việc kết nối mạng

I.1.1. Nhu cầu của việc kết nối mạng máy tính

Việc nối máy tính thành mạng từ lâu đã trở thành một nhu cầu khách quan vì :

- Có rất nhiều công việc về bản chất là phân tán hoặc về thông tin, hoặc về xử lý hoặc cả hai đòi hỏi có sự kết hợp truyền thông với xử lý hoặc sử dụng phương tiện từ xa.

- Chia sẻ các tài nguyên trên mạng cho nhiều người sử dụng tại một thời điểm (ổ cứng, máy in, ổ CD ROM . . .)

- Nhu cầu liên lạc, trao đổi thông tin nhờ phương tiện máy tính.

- Các ứng dụng phần mềm đòi hòi tại một thời điểm cần có nhiều người sử dụng, truy cập vào cùng một cơ sở dữ liệu.

I.1.2. Định nghĩa mạng máy tính

Nói một cách ngắn gọn thì mạng máy tính là tập hợp các máy tính độc lập (autonomous) được kết nối với nhau thông qua các đường truyền vật lý và tuân theo các quy ước truyền thông nào đó.

Khái niệm máy tính độc lập được hiểu là các máy tính không có máy nào có khả năng khởi động hoặc đình chỉ một máy khác.

Các đường truyền vật lý được hiểu là các môi trường truyền tín hiệu vật lý (có thể là hữu tuyến hoặc vô tuyến).

Các quy ước truyền thông chính là cơ sở để các máy tính có thể "nói chuyện" được với nhau và là một yếu tố quan trọng hàng đầu khi nói về công nghệ mạng máy tính.

I.2. Đặc trưng kỹ thuật của mạng máy tính

Một mạng máy tính có các đặc trưng kỹ thuật cơ bản như sau:

I.2.1. Đường truyền

Là thành tố quan trọng của một mạng máy tính, là phương tiện dùng để truyền các tín hiệu điện tử giữa các máy tính. Các tín hiệu điệu tử đó chính là các thông tin, dữ liệu được biểu thị dưới dạng các xung nhị phân (ON_OFF), mọi tín hiệu truyền giữa các máy tính với nhau đều thuộc sóng điện từ, tuỳ theo tần số mà ta có thể dùng các đường truyền vật lý khác nhau

Đặc trưng cơ bản của đường truyền là giải thông nó biểu thị khả năng truyền tải tín hiệu của đường truyền.

Thông thường người ta hay phân loại đường truyền theo hai loại:

- Đường truyền hữu tuyến (các máy tính được nối với nhau bằng các dây cáp mạng).

- Đường truyền vô tuyến: các máy tính truyền tín hiệu với nhau thông qua các sóng vô tuyền với các thiết bị điều chế/giải điều chế ở các đầu mút.

I.2.2. Kỹ thuật chuyển mạch:

Là đặc trưng kỹ thuật chuyển tín hiệu giữa các nút trong mạng, các nút mạng có chức năng hướng thông tin tới đích nào đó trong mạng, hiện tại có các kỹ thuật chuyển mạch như sau:

- Kỹ thuật chuyển mạch kênh: Khi có hai thực thể cần truyền thông với nhau thì giữa chúng sẽ thiết lập một kênh cố định và duy trì kết nối đó cho tới khi hai bên ngắt liên lạc. Các dữ liệu chỉ truyền đi theo con đường cố định đó.

- Kỹ thuật chuyển mạch thông báo: thông báo là một đơn vị dữ liệu của người sử dụng có khuôn dạng được quy định trước. Mỗi thông báo có chứa các thông tin điều khiển trong đó chỉ rõ đích cần truyền tới của thông báo. Căn cứ vào thông tin điều khiển này mà mỗi nút trung gian có thể chuyển thông báo tới nút kế tiếp trên con đường dẫn tới đích của thông báo

- Kỹ thuật chuyển mạch gói: ở đây mỗi thông báo được chia ra thành nhiều gói nhỏ hơn được gọi là các gói tin (packet) có khuôn dạng qui định trước. Mỗi gói tin cũng chứa các thông tin điều khiển, trong đó có địa chỉ nguồn (người gửi) và địa chỉ đích (người nhận) của gói tin. Các gói tin của cùng một thông báo có thể được gởi đi qua mạng tới đích theo nhiều con đường khác nhau.

I.2.3. Kiến trúc mạng

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

Khi nói đến kiến trúc của mạng người ta muốn nói tới hai vấn đề là hình trạng mạng (Network topology) và giao thức mạng (Network protocol)

- Network Topology: Cách kết nối các máy tính với nhau về mặt hình học mà ta gọi là tô pô của mạng

Các hình trạng mạng cơ bản đó là: hình sao, hình bus, hình vòng

- Network Protocol: Tập hợp các quy ước truyền thông giữa các thực thể truyền thông mà ta gọi là giao thức (hay nghi thức) của mạng

Các giai thức thường gặp nhất là : TCP/IP, NETBIOS, IPX/SPX, . . .

I.2.4. Hệ điều hành mạng

Hệ điều hành mạng là một phần mềm hệ thống có các chức năng sau:

- Quản lý tài nguyên của hệ thống, các tài nguyên này gồm:

+ Tài nguyên thông tin (về phương diện lưu trữ) hay nói một cách đơn giản là quản lý tệp. Các công việc về lưu trữ tệp, tìm kiếm, xoá, copy, nhóm, đặt các thuộc tính đều thuộc nhóm công việc này

+ Tài nguyên thiết bị. Điều phối việc sử dụng CPU, các ngoại vi... để tối ưu hoá việc sử dụng

- Quản lý người dùng và các công việc trên hệ thống.

Hệ điều hành đảm bảo giao tiếp giữa người sử dụng, chương trình ứng dụng với thiết bị của hệ thống.

- Cung cấp các tiện ích cho việc khai thác hệ thống thuận lợi (ví dụ FORMAT đĩa, sao chép tệp và thư mục, in ấn chung ...)

Các hệ điều hành mạng thông dụng nhất hiện nay là: WindowsNT, Windows9X, Windows 2000, Unix, Novell.

I.3. Phân loại mạng máy tính

Có nhiều cách phân loại mạng khác nhau tuỳ thuộc vào yếu tố chính được chọn dùng để làm chỉ tiêu phân loại, thông thường người ta phân loại mạng theo các tiêu chí như sau

- Khoảng cách địa lý của mạng
- Kỹ thuật chuyển mạch mà mạng áp dụng
- Kiến trúc mạng
- Hệ điều hành mạng sử dụng ...

Tuy nhiên trong thực tế người ta thường chỉ phân loại theo hai tiêu chí đầu tiên

I.3.1. Phân loại mạng theo khoảng cách địa lý :

Nếu lấy khoảng cách địa lý làm yếu tố phân loại mạng thì ta có mạng cục bộ, mạng đô thị, mạng diện rộng, mạng toàn cầu.

Mạng cục bộ (LAN - Local Area Network) : là mạng được cài đặt trong phạm vi tương đối nhỏ hẹp như trong một toà nhà, một xí nghiệp...với khoảng cách lớn nhất giữa các máy tính trên mạng trong vòng vài km trở lại.

Mạng đô thị (MAN - Metropolitan Area Network) : là mạng được cài đặt trong phạm vi một đô thị, một trung tâm văn hoá xã hội, có bán kính tối đa khoảng 100 km trở lại.

Mạng diện rộng (WAN - Wide Area Network) : là mạng có diện tích bao phủ rộng lớn, phạm vi của mạng có thể vượt biên giới quốc gia thậm chí cả lục địa.

Mạng toàn cầu (GAN - Global Area Network) : là mạng có phạm vi trải rộng toàn cầu.

I.3.2. Phân loại theo kỹ thuật chuyển mạch:

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

Mạch chuyển mạch kênh (circuit switched network) : Khi có hai thực thể cần truyền thông với nhau thì giữa chúng sẽ thiết lập một kênh cố định và duy trì kết nối đó cho tới khi hai bên ngắt liên lạc. Các dữ liệu chỉ truyền đi theo con đường cố định đó. Nhược điểm của chuyển mạch kênh là tiêu tốn thời gian để thiết lập kênh truyền cố định và hiệu suất sử dụng mạng không cao.

Mạng chuyển mạch thông báo (message switched network) : Thông báo là một đơn vị dữ liệu của người sử dụng có khuôn dạng được quy định trước. Mỗi thông báo có chứa các thông tin điều khiển trong đó chỉ rõ đích cần truyền tới của thông báo. Căn cứ vào thông tin điều khiển này mà mỗi nút trung gian có thể chuyển thông báo tới nút kế tiếp trên con đường dẫn tới đích của thông báo. Như vậy mỗi nút cần phải lưu giữ tạm thời để đọc thông tin điều khiển trên thông báo, nếu thấy thông báo không gửi cho mình thì tiếp tục chuyển tiếp thông báo đi. Tuỳ vào điều kiện của mạng mà thông báo có thể được chuyển đi theo nhiều con đường khác nhau.

Ưu điểm của phương pháp này là :

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

- Mỗi nút mạng có thể lưu trữ thông tin tạm thời sau đó mới chuyển thông báo đi, do đó có thể điều chỉnh để làm giảm tình trạng tắc nghẽn trên mạng.

- Có thể điều khiển việc truyền tin bằng cách sắp xếp độ ưu tiên cho các thông báo.

- Có thể tăng hiệu suất sử dụng giải thông của mạng bằng cách gắn địa chỉ quảng bá (broadcast addressing) để gửi thông báo đồng thời tới nhiều đích.

Nhược điểm của phương pháp này là:

- Không hạn chế được kích thước của thông báo dẫn đến phí tổn lưu giữ tạm thời cao và ảnh hưởng đến thời gian trả lời yêu cầu của các trạm .

Mạng chuyển mạch gói (packet switched network) : ở đây mỗi thông báo được chia ra thành nhiều gói nhỏ hơn được gọi là các gói tin (packet) có khuôn dạng qui định trước. Mỗi gói tin cũng chứa các thông tin điều khiển,

trong đó có địa chỉ nguồn (người gửi) và địa chỉ đích (người nhận) của gói tin. Các gói tin của cùng một thông báo có thể được gởi đi qua mạng tới đích theo nhiều con đường khác nhau.

Phương pháp chuyển mạch thông báo và chuyển mạch gói là gần giống nhau. Điểm khác biệt là các gói tin được giới hạn kích thước tối đa sao cho các nút mạng (các nút chuyển mạch) có thể xử lý toàn bộ gói tin trong bộ nhớ mà không phải lưu giữ tạm thời trên đĩa. Bởi vậy nên mạng chuyển mạch gói truyền dữ liệu hiệu quả hơn so với mạng chuyển mạch thông báo.

Tích hợp hai kỹ thuật chuyển mạch kênh và chuyển mạch gói vào trong một mạng thống nhất được mạng tích hợp số ISDN (Integated Services Digital Network).

I.3.3. Phân loại theo kiến trúc mạng sử dụng

Kiến trúc của mạng bao gồm hai vấn đề: hình trạng mạng (Network topology) và giao thức mạng (Network protocol)

Hình trạng mạng: Cách kết nối các máy tính với nhau về mặt hình học mà ta gọi là tô pô của mạng

Giao thức mạng: Tập hợp các quy ước truyền thông giữa các thực thể truyền thông mà ta gọi là giao thức (hay nghi thức) của mạng

Khi phân loại theo topo mạng người ta thường có phân loại thành: mạng hình sao, tròn, tuyến tính

Phân loại theo giao thức mà mạng sử dụng người ta phân loại thành mạng : TCP/IP, mạng NETBIOS . ..

Tuy nhiên cách phân loại trên không phổ biến và chỉ áp dụng cho các mạng cục bộ.

I.3.4. Phân loại theo hệ điều hàng mạng

Nếu phân loại theo hệ điều hành mạng người ta chia ra theo mô hình mạng ngang hàng, mạng khách/chủ hoặc phân loại theo tên hệ điều hành mà mạng sử dụng: Windows NT, Unix, Novell . . .

I.4. Giới thiệu các mạng máy tính thông dụng nhất

I.4.1. Mạng cục bộ

Một mạng cục bộ là sự kết nối một nhóm máy tính và các thiết bị kết nối mạng được lắp đặt trên một phạm vị địa lý giới hạn, thường trong một toà nhà hoặc một khu công sở nào đó.

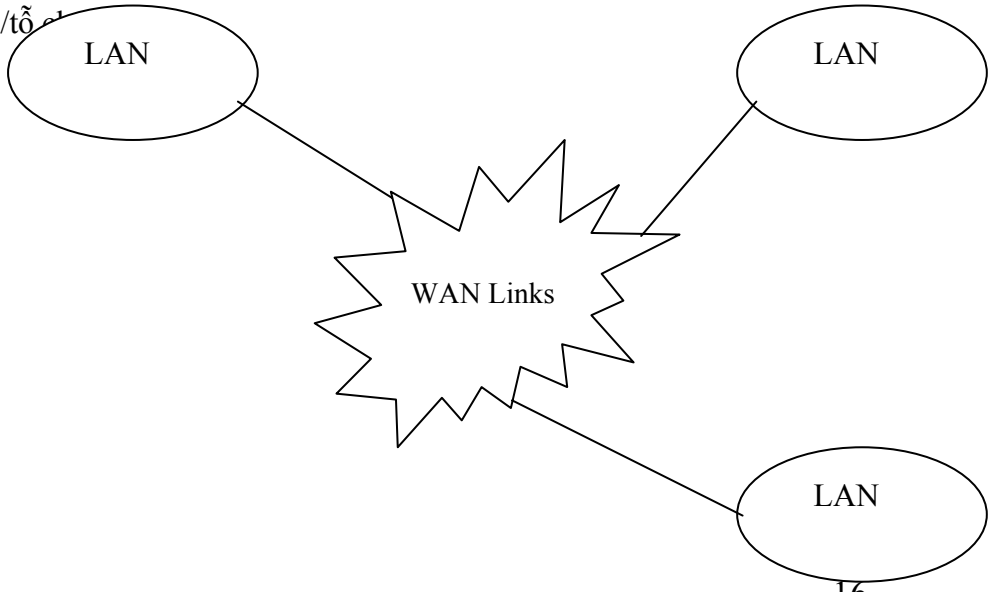
Mạng cục bộ có các đặc tính sau:

- Tốc độ truyền dữ liệu cao
- Phạm vi địa lý giới hạn
-Sở hữu của một cơ quan/tổ chức

I.4.2. Mạng diện rộng với kết nối LAN TO LAN

Mạng diện rộng bao giờ cũng là sự kết nối của các mạng LAN, mạng diện rộng có thể trải trên phạm vi một vùng, quốc gia hoặc cả một lục địa thậm chí trên phạm vi toàn cầu.

- Tốc độ truyền dữ liệu không cao
- Phạm vi địa lý không giới hạn
- Thường triển khai dựa vào các công ty truyền thông, bưu điện và dùng các hệ thống truyền thông này để tạo dựng đường truyền
- Một mạng WAN có thể là sở hữu của một tập đoàn/tổ chức hoặc là mạng kết nối của nhiều tập đoàn/tổ



I.4.3. Liên mạng INTERNET

Với sự phát triển nhanh chóng của công nghệ là sự ra đời của liên mạng INTERNET,

- Là một mạng toàn cầu

- Là sự kết hợp của vô số các hệ thống truyền thông, máy chủ cung cấp thông tin và dịch vụ, các máy trạm khai thác thông tin

- Dựa trên nhiều nền tảng truyền thông khác nhau, nhưng đều trên nền giao thức TCP/IP

- Là sở hữu chung của toàn nhân loại

- Càng ngày càng phát triển mãnh liệt

I.4.4. Mạng INTRANET

Thực sự là một mạng INTERNET thu nhỏ vào trong một cơ quan/công ty/tổ chức hay một bộ/nghành . . ., giới hạn phạm vi người sử dụng, có sử dụng các công nghệ kiểm soát truy cập và bảo mật thông tin .

Được phát triển từ các mạng LAN, WAN dùng công nghệ INTERNET

II. Mạng cục bộ, kiến trúc mạng cục bộ

II.1. Mạng cục bộ

Tên gọi "mạng cục bộ" được xem xét từ quy mô của mạng. Tuy nhiên, đó không phải là đặc tính duy nhất của mạng cục bộ nhưng trên thực tế, quy mô của mạng quyết định nhiều đặc tính và công nghệ của mạng. Sau đây là một số đặc điểm của mạng cục bộ:

Đặc điểm của mạng cục bộ

- Mạng cục bộ có quy mô nhỏ, thường là bán kính dưới vài km. Đặc điểm này cho phép không cần dùng các thiết bị dẫn đường với các mối liên hệ phức tạp

- Mạng cục bộ thường là sở hữu của một tổ chức. Điều này dường như có vẻ ít quan trọng nhưng trên thực tế đó là điều khá quan trọng để việc quản lý mạng có hiệu quả.

- Mạng cục bộ có tốc độ cao và ít lỗi. Trên mạng rộng tốc độ nói chung chỉ đạt vài Kbit/s. Còn tốc độ thông thường trên mạng cục bộ là 10, 100 Kb/s và tới nay với Gigabit Ethernet, tốc độ trên mạng cục bộ có thể đạt 1Gb/s. Xác suất lỗi rất thấp.

II.2. Kiến trúc mạng cục bộ

II.2.1. Đồ hình mạng (Network Topology)

*** Định nghĩa Topo mạng:**

Cách kết nối các máy tính với nhau về mặt hình học mà ta gọi là tô pô của mạng

Có hai kiểu nối mạng chủ yếu đó là :

- Nối kiểu điểm - điểm (point - to - point).

- Nối kiểu điểm - nhiều điểm (point - to - multipoint hay broadcast).

Theo kiểu điểm - điểm, các đường truyền nối từng cặp nút với nhau và mỗi nút đều có trách nhiệm lưu giữ tạm thời sau đó chuyển tiếp dữ liệu đi cho tới đích. Do cách làm việc như vậy nên mạng kiểu này còn được gọi là mạng "lưu và chuyển tiếp" (store and forward).

Theo kiểu điểm - nhiều điểm, tất cả các nút phân chia nhau một đường truyền vật lý chung. Dữ liệu gửi đi từ một nút nào đó sẽ được tiếp nhận bởi tất cả các nút còn lại trên mạng, bởi vậy cần chỉ ra địa chỉ đích của dữ liệu để căn cứ vào đó các nút kiểm tra xem dữ liệu đó có phải gửi cho mình không.

*** Phân biệt kiểu tô pô của mạng cục bộ và kiểu tô pô của mạng rộng.**

Tô pô của mạng rộng thông thường là nói đến sự liên kết giữa các mạng cục bộ thông qua các bộ dẫn đường (router). Đối với mạng rộng topo của mạng là hình trạng hình học của các bộ dẫn đường và các kênh viễn thông còn khi nói tới tô pô của mạng cục bộ người ta nói đến sự liên kết của chính các máy tính.

a) Mạng hình sao

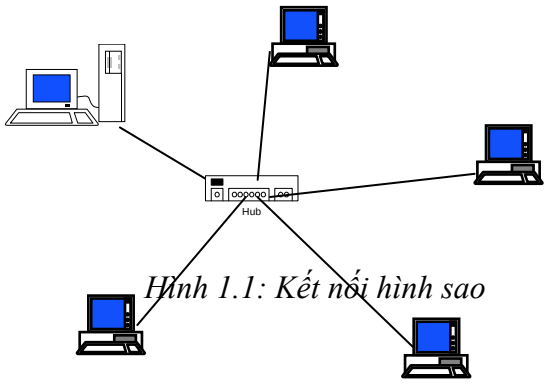
Mạng hình sao có tất cả các trạm được kết nối với một thiết bị trung tâm có nhiệm vụ nhận tín hiệu từ các trạm và chuyển đến trạm đích. Tuỳ theo yêu cầu truyền thông trên mạng mà thiết bị trung tâm có thể là bộ chuyển mạch (switch), bộ chọn đường (router) hoặc là bộ phân kênh (hub). Vai trò của thiết bị trung tâm này là thực hiện việc thiết lập các liên kết điểm-điểm (point-to-point) giữa các trạm.

Ưu điểm:

Thiết lập mạng đơn giản, dễ dàng cấu hình lại mạng (thêm, bớt các trạm), dễ dàng kiểm soát và khắc phục sự cố, tận dụng được tối đa tốc độ truyền của đường truyền vật lý.

Nhược điểm:

Độ dài đường truyền nối một trạm với thiết bị trung tâm bị hạn chế (trong vòng 100m, với công nghệ hiện nay).

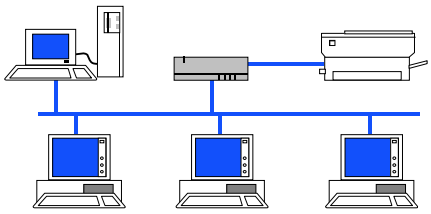


Hình 1.1: Kết nối hình sao

b) Mạng trục tuyến tính (Bus):

Trong mạng trục tất cả các trạm phân chia một đường truyền chung (bus). Đường truyền chính được giới hạn hai đầu bằng hai đầu nối đặc biệt gọi là terminator. Mỗi trạm được nối với trục chính qua một đầu nối chữ T (T-connector) hoặc một thiết bị thu phát (transceiver).

Khi một trạm truyền dữ liệu tín hiệu được quảng bá trên cả hai chiều của bus, tức là mọi trạm còn lại đều có thể thu được tín hiệu đó trực tiếp. Đối với các bus một chiều thì tín hiệu chỉ đi về một phía, lúc đó các terminator phải được thiết kế sao cho các tín hiệu đó phải được dội lại trên bus để cho các trạm trên mạng đều có thể thu nhận được tín hiệu đó. Như vậy với topo mạng trục dữ liệu được truyền theo các liên kết điểm-đa điểm (point-to-multipoint) hay quảng bá (broadcast).



Hình 1.2. Kết nối kiểu bus

Ưu điểm :

Dễ thiết kế, chi phí thấp

Nhược điểm:

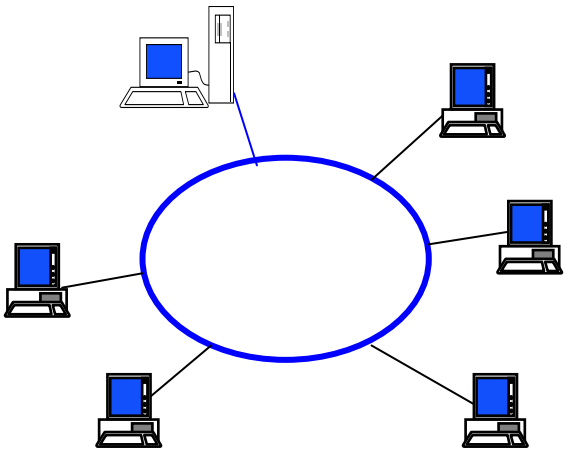
Tính ổn định kém, chỉ một nút mạng hỏng là toàn bộ mạng bị ngừng hoạt động

c) Mạng hình vòng

Trên mạng hình vòng tín hiệu được truyền đi trên vòng theo một chiều duy nhất. Mỗi trạm của mạng được nối với vòng qua một bộ chuyển tiếp (repeater) có nhiệm vụ nhận tín hiệu rồi chuyển tiếp đến trạm kế tiếp trên vòng. Như vậy tín hiệu được lưu chuyển trên vòng theo một chuỗi liên tiếp các liên kết điểm-điểm giữa các repeater do đó cần có giao thức điều khiển việc cấp phát quyền được truyền dữ liệu trên vòng mạng cho trạm có nhu cầu.

Để tăng độ tin cậy của mạng ta có thể lắp đặt thêm các vòng dự phòng, nếu vòng chính có sự cố thì vòng phụ sẽ được sử dụng.

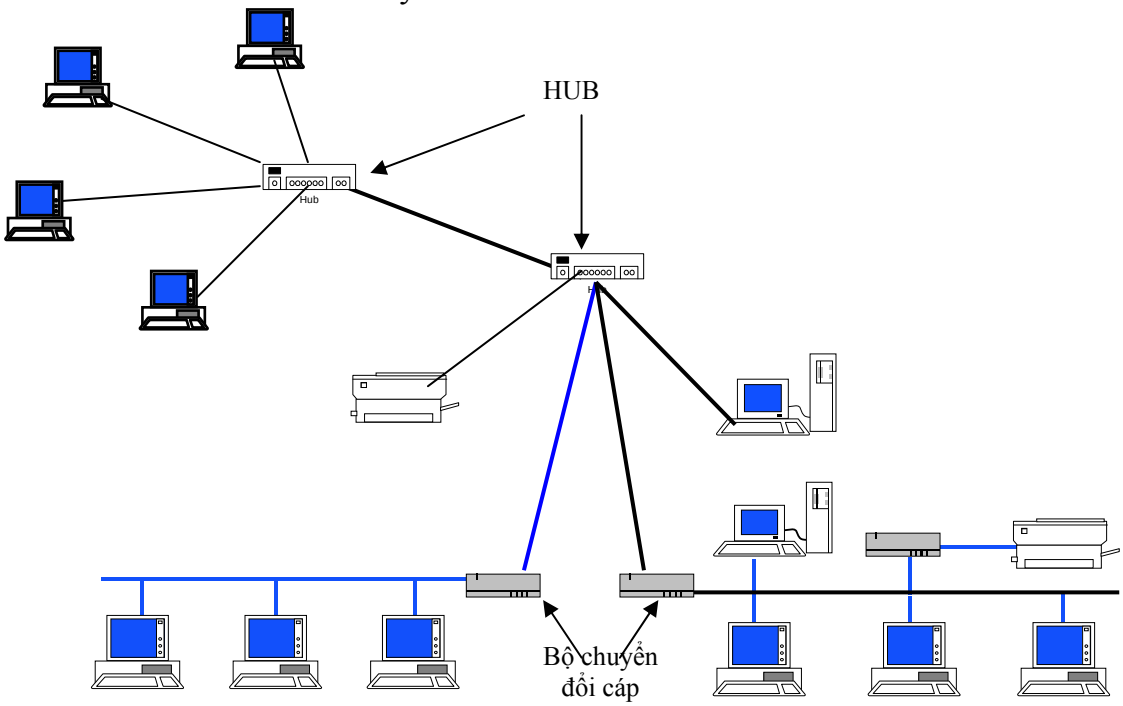
Mạng hình vòng có ưu nhược điểm tương tự mạng hình sao, tuy nhiên mạng hình vòng đòi hỏi giao thức truy nhập mạng phức tạp hơn mạng hình sao.



Hình 1.3. Kết nối kiểu vòng

d) Kết nối hỗn hợp

Là sự phối hợp các kiểu kết nối khác nhau, ví du hình cây là cấu trúc phân tầng của kiểu hình sao hay các HUB có thể được nối với nhau theo kiểu bus còn từ các HUB nối với các máy theo hình sao.



Hình 1.4. Một kết nối hỗn hợp

II.3. Các phương pháp truy cập đường truyền vật lý

Trong mạng cục bộ, tất cả các trạm kết nối trực tiếp vào đường truyền chung. Vì vậy tín hiệu từ một trạm đưa lên đường truyền sẽ được các trạm khác "nghe thấy". Một vấn đề khác là, nếu nhiều trạm cùng gửi tín hiệu lên đường truyền đồng thời thì tín hiệu sẽ chồng lên nhau và bị hỏng. Vì vậy cần phải có một phương pháp tổ chức chia sẻ đường truyền để việc truyền thông được đúng đắn.

Có hai phương pháp chia sẻ đường truyền chung thường được dùng trong các mạng cục bộ:

- Truy nhập đường truyền một cách ngẫu nhiên, theo yêu cầu. Đương nhiên phải có tính đến việc sử dụng luân phiên và nếu trong trường hợp do có nhiều trạm cùng truyền tin dẫn đến tín hiệu bị trùm lên nhau thì phải truyền lại.

- Có cơ chế trọng tài để cấp quyền truy nhập đường truyền sao cho không xảy ra xung đột

II.3.1 Phương pháp đa truy nhập sử dụng sóng mang có phát hiện xung đột CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

Giao thức CSMA (Carrier Sense Multiple Access) - đa truy nhập có cảm nhận sóng mang được sử dụng rất phổ biến trong các mạng cục bộ. Giao thức này sử dụng phương pháp thời gian chia ngăn theo đó thời gian được chia thành các khoảng thời gian đều đặn và các trạm chỉ phát lên đường truyền tại thời điểm đầu ngăn.

Mỗi trạm có thiết bị nghe tín hiệu trên đường truyền (tức là cảm nhận sóng mang). Trước khi truyền cần phải biết đường truyền có rỗi không. Nếu rỗi thì mới được truyền. Phương pháp này gọi là LBT (Listening before talking). Khi phát hiện xung đột, các trạm sẽ phải phát lại. Có một số chiến lược phát lại như sau:

- Giao thức CSMA 1-kiên trì. Khi trạm phát hiện kênh rỗi trạm truyền ngay. Nhưng nếu có xung đột, trạm đợi khoảng thời gian ngẫu nhiên rồi truyền lại. Do vậy xác suất truyền khi kênh rỗi là 1. Chính vì thế mà giao thức có tên là CSMA 1-kiên trì. (1)

- Giao thức CSMA không kiên trì khác một chút.Trạm nghe đường, nếu kênh rỗi thì truyền, nếu không thì ngừng nghe một khoảng thời gian ngẫu nhiên rồi mới thực hiện lại thủ tục. Cách này có hiệu suất dùng kênh cao hơn. (2)

- Giao thức CSMA p-kiên trì. Khi đã sẵn sàng truyền, trạm cảm nhận đường, nếu đường rỗi thì thực hiện việc truyền với xác suất là $p < 1$ (tức là ngay cả khi đường rỗi cũng không hẳn đã truyền mà đợi khoảng thời gian tiếp theo lại tiếp tục thực hiện việc truyền với xác suất còn lại $q=1-p$. (3)

- Ta thấy giải thuật (1) có hiệu quả trong việc tránh xung đột vì hai trạm cần truyền thấy đường truyền bận sẽ cùng rút lui chờ trong những khoảng thời gian ngẫu nhiên khác nhau sẽ quay lại tiếp tục nghe đường truyền. Nhược điểm của nó là có thể có thời gian không sử dụng đường truyền sau mỗi cuộc gọi.

- Giải thuật (2) cố gắng làm giảm thời gian "chết" bằng cách cho phép một trạm có thể được truyền dữ liệu ngay sau khi một cuộc truyền kết thúc. Tuy nhiên nếu lúc đó lại có nhiều trạm đang đợi để truyền dữ liệu thì khả năng xẩy ra xung đột sẽ rất lớn.

- Giải thuật (3) với giá trị p được họn hợp lý có thể tối thiểu hoá được cả khả năng xung đột lẫn thời gian "chết" của đường truyền.

- Xẩy ra xung đột thường là do độ trễ truyền dẫn, mấu chốt của vấn đề là : các trạm chỉ "nghe" trước khi truyền dữ liệu mà không "nghe" trong khi truyền, cho nên thực tế có xung đột thế nhưng các trạm không biết do đó vẫn truyền dữ liệu.

- Để có thể phát hiện xung đột, CSMA/CD đã bổ xung thêm các quy tắc sau đây :

- Khi một trạm truyền dữ liệu, nó vẫn tiếp tục "nghe" đường truyền . Nếu phát hiện xung đột thì nó ngừng ngay việc truyền, nhờ đó mà tiết kiệm được thời gian và giải thông, nhưng nó vẫn tiếp tục gửi tín hiệu thêm một thời gian nữa để đảm bảo rằng tất cả các trạm trên mạng đều "nghe" được sự kiện này.(như vậy phải tiếp tục nghe đường truyền trong khi truyền để phát hiện đụng độ (Listening While Talking))

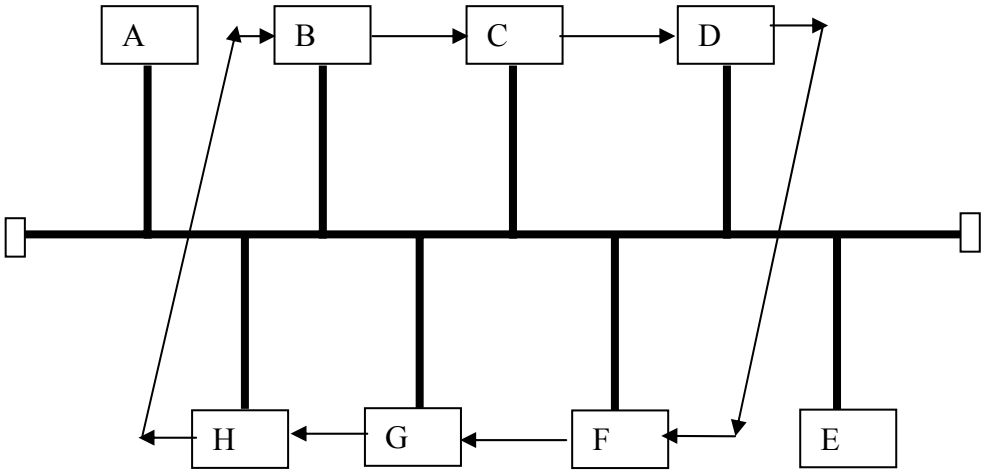
- Sau đó trạm sẽ chờ trong một khoảng thời gian ngẫu nhiên nào đó rồi thử truyền lại theo quy tắc CSMA.

Giao thức này gọi là **CSMA có phát hiện xung đột** (Carrier Sense Multiple Access with Collision Detection viết tắt là CSMA/CD), dùng rộng rãi trong LAN và MAN.

II.3.2. Phương pháp Token Bus

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

sau nó. Thứ tự của các trạm trên vòng logic có thể độc lập với thứ tự vật lý. Các trạm không hoặc chưa có nhu cầu truyền dữ liệu không được vào trong vòng logic.



Hình 1.5. Ví dụ về vòng logic

Trong ví dụ trên, các trạm A, E nằm ngoài vòng logic do đó chỉ có thể tiếp nhận được dữ liệu dành cho chúng.

Việc thiết lập vòng logic không khó nhưng việc duy trì nó theo trạng thái thực tế của mạng mới là khó. Cụ thể phải thực hiện các chức năng sau:

a) Bổ xung một trạm vào vòng logic : các trạm nằm ngoài vòng logic cần được xem xét một cách định kỳ để nếu có nhu cầu truyền dữ liệu thì được bổ xung vào vòng logic.

b) Loại bỏ một vòng khỏi vòng logic : khi một trạm không có nhu cầu truyền dữ liệu thì cần loại bỏ nó ra khỏi vòng logic để tối ưu hoá việc truyền dữ liệu bằng thẻ bài.

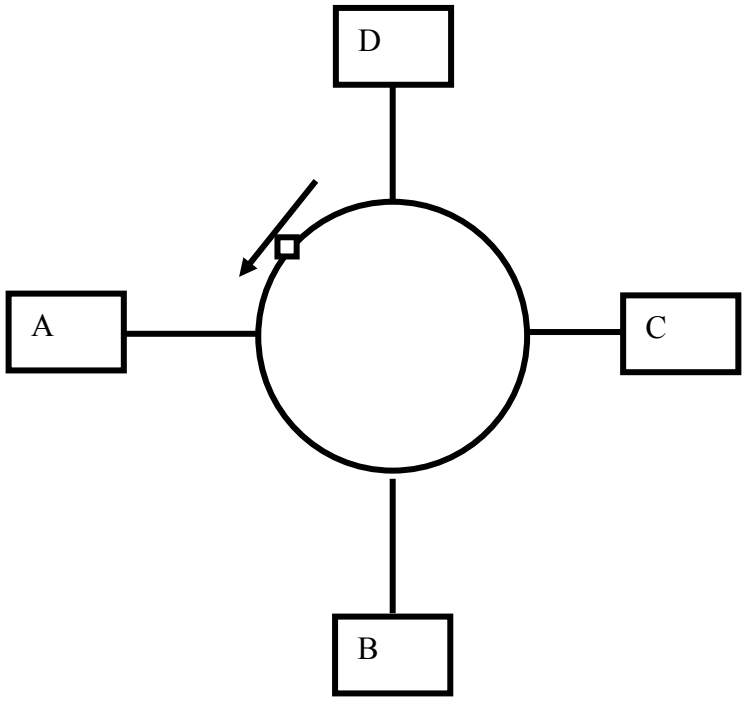
c) Quản lý lỗi : một số lỗi có thể xẩy ra như trùng hợp địa chỉ, hoặc đứt vòng logic.

d) Khởi taọ vòng logic : khi khởi tạo mạng hoặc khi đứt vòng logic cần phải khởi tạo lại vòng logic.

II.3.2. Phương pháp Token Ring

Phương pháp này cũng dựa trên nguyên tắc dùng thẻ bài để cấp phát quyền truy nhập đường truyền. Nhưng ở đây thẻ bài lưu chuyển theo theo vòng vật lý chứ không theo vòng logic như dối với phương pháp token bus.

Thẻ bài là một đơn vị truyền dữ liệu đặc biệt trong đó có một bit biểu diễn trạng thái của thẻ (bận hay rỗi). Một trạm muốn truyền dữ liệu phải chờ cho tới khi nhận được thẻ bài "rỗi". Khi đó trạm sẽ đổi bit trạng thái thành "bận" và truyền một đơn vị dữ liệu đi cùng với thẻ bài đi theo chiều của vòng. Lúc này không còn thẻ bài "rỗi " nữa do đó các trạm muốn truyền dữ liệu phải đợi. Dữ liệu tới trạm đích được sao chép lại, sau đó cùng với thẻ bài trở về trạm nguồn. Trạm nguồn sẽ xoá bỏ dữ liệu đổi bit trạng thái thành "rỗi" và cho lưu chuyển thẻ trên vòng để các trạm khác có nhu cầu truyền dữ liệu được phép truyền .



Hình 1.6. Thẻ bài trong mạng Ring

Sự quay trở lại trạm nguồn của dữ liệu và thẻ bài nhằm tạo khả năng báo nhận tự nhiên : trạm đích có thể gửi vào đơn vị dữ liệu (phần header) các thông tin về kết quả tiếp nhận dữ liệu của mình. Chẳng hạn các thông tin đó có thể là: trạm đích không tồn tại hoặc không hoạt động, trạm đích tồn tại nhưng dữ liệu không được sao chép, dữ liệu đã được tiếp nhận, có lỗi...

Trong phương pháp này cần giải quyết hai vấn đề có thể dẫn đến phá vỡ hệ thống đó là mất thẻ bài và thẻ bài "bận" lưu chuyển không dừng trên vòng .Có nhiều phương pháp giải quyết các vấn đề trên, dưới đây là một phương pháp được khuyến nghị:

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

Đối với vấn đề thẻ bài bận lưu chuyển không dừng, trạm điều khiển sử dụng một bit trên thẻ bài để đánh dấu khi gặp một thẻ bài "bận" đi qua nó. Nếu nó gặp lại thẻ bài bận với bit đã đánh dấu đó có nghĩa là trạm nguồn đã không nhận lại được đơn vị dữ liệu của mình do đó thẻ bài "bận" cứ quay vòng mãi. Lúc đó trạm điều khiển sẽ chủ động đổi bit trạng thái "bận" thành "rỗi" và cho thẻ bài chuyển tiếp trên vòng. Trong phương pháp này các trạm còn lại trên mạng sẽ đóng vai trò bị động, chúng theo dõi phát hiện tình trạng sự cố trên trạm chủ động và thay thế trạm chủ động nếu cần.

III. Chuẩn hoá mạng máy tính

III.1. Vấn đề chuẩn hoá mạng và các tổ chức chuẩn hoá mạng

Khi thiết kế, các nhà thiết kế tự do lựa chọn kiến trúc mạng cho riêng mình. Từ đó dẫn tới tình trạng không tương thích giữa các mạng máy tính với nhau. Nhu cầu trao đổi thông tin càng lớn thúc đẩy việc xây dựng khung chuẩnvề kiến trúc mạng để làm căn cứ cho các nhà thiết kế và chế tạo thiết bị mạng .

Chính vì lý do đó, tổ chức tiêu chuẩn hoá quốc tế ISO (Internatinal Organnization for Standarzation) đã xây dựng mô hình tham chiếu cho việc kết

nối các hệ thống mở OSI (reference model for Open Systems Interconnection). Mô hình này là cơ sở cho việc kết nối các hệ thống mở phục vụ cho các ứng dụng phân tán.

Có hai loại chuẩn cho mạng đó là :

- Các chuẩn chính thức (de jure) do các tổ chức chuẩn quốc gia và quốc tế ban hành.

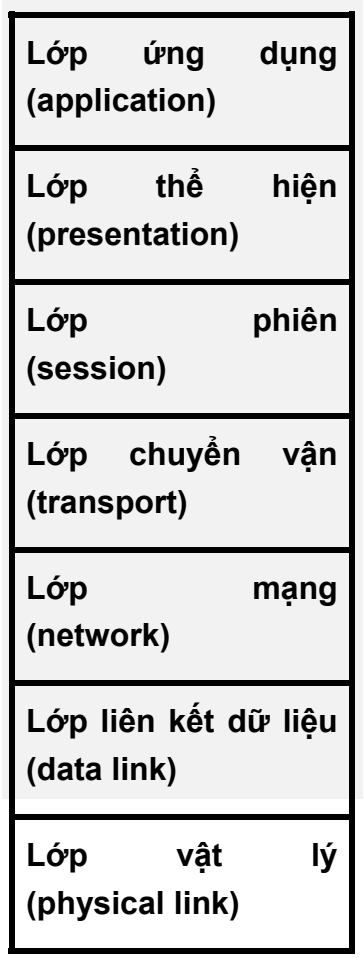
- Các chuẩn tực tiễn (de facto) do các hãng sản xuất, các tổ chức người sử dụng xây dựng và được dùng rộng rãi trong thực tế

III.2. Mô hình tham chiếu OSI 7 lớp

Khi thiết kế, các nhà thiết kế tự do lựa chọn kiến trúc mạng cho riêng mình. Từ đó dẫn tới tình trạng không tương thích giữa các mạng máy tính với nhau. Vấn đề không tương thích đó làm trở ngại cho sự tương tác giữa những người sử dụng mạng khác nhau. Nhu cầu trao đổi thông tin càng lớn thúc đẩy việc xây dựng khung chuẩn về kiến trúc mạng để làm căn cứ cho các nhà thiết kế và chế tạo thiết bị mạng .

Chính vì lý do đó, tổ chức tiêu chuẩn hoá quốc tế ISO (Internatinal Organnization for Standarzation) đã xây dựng mô hình tham chiếu cho việc kết nối các hệ thống mở OSI (reference model for Open Systems Interconnection). Mô hình này là cơ sở cho việc kết nối các hệ thống mở phục vụ cho các ứng dụng phân tán.

Mô hình OSI được biểu diễn theo hình dưới đây:



Hình 1.7. Mô hình OSI 7 lớp

a) Lớp vật lý

Lớp này bảo đảm các công việc sau:

- Lập, cắt cuộc nối.

- Truyền tin dạng bit qua kênh vật lý.

- Có thể có nhiều kênh.

b) Lớp liên kết dữ liệu

Lớp này đảm bảo việc biến đổi các tin dạng bit nhận được từ lớp dưới (vật lý) sang khung số liệu, thông báo cho hệ phát, kết quả thu được sao cho các thông tin truyền lên cho mức 3 không có lỗi. Các thông tin truyền ở mức 1 có thể làm hỏng các thông tin khung số liệu (frame error). Phần mềm mức hai

sẽ thông báo cho mức một truyền lại các thông tin bị mất / lỗi. Đồng bộ các hệ có tốc độ xử lý tính khác nhau, một trong những phương pháp hay sử dụng là dùng bộ đệm trung gian để lưu giữ số liệu nhận được. Độ lớn của bộ đệm này phụ thuộc vào tương quan xử lý của các hệ thu và phát. Trong trường hợp đường truyền song công toàn phần, lớp datalink phải đảm bảo việc quản lý các thông tin số liệu và các thông tin trạng thái.

c) Lớp mạng

Nhiệm vụ của lớp mạng là đảm bảo chuyển chính xác số liệu giữa các thiết bị cuối trong mạng. Để làm được việc đó, phải có chiến lược đánh địa chỉ thống nhất trong toàn mạng. Mỗi thiết bị cuối và thiết bị mạng có một địa chỉ mạng xác định. Số liệu cần trao đổi giữa các thiết bị cuối được tổ chức thành các gói *(packet)* có độ dài thay đổi và được gán đầy đủ địa chỉ nguồn *(source address)* và địa chỉ đích *(destination address)*.

Lớp mạng đảm bảo việc tìm đường tối ưu cho các gói dữ liệu bằng các giao thức chọn đường dựa trên các thiết bị chọn đường *(router)*. Ngoài ra, lớp mạng có chức năng điều khiển lưu lượng số liệu trong mạng để tránh xảy ra tắc ngẽn bằng cách chọn các chiến lược tìm đường khác nhau để quyết định việc chuyển tiếp các gói số liệu.

d) Lớp chuyển vận

Lớp này thực hiện các chức năng nhận thông tin từ lớp phiên (**session**) chia thành các gói nhỏ hơn và truyền xuống lớp dưới, hoặc nhận thông tin từ lớp dưới chuyển lên phục hồi theo cách chia của hệ phát (Fragmentation and Reassembly). Nhiệm vụ quan trọng nhất của lớp vận chuyển là đảm bảo chuyển số liệu chính xác giữa hai thực thể thuộc lớp phiên (end-to-end control). Để làm được việc đó, ngoài chức năng kiểm tra số tuần tự phát, thu, kiểm tra và phát hiện, xử lý lỗi.Lớp vận chuyển còn có chức năng điều khiển lưu lượng số liệu để đồng bộ giữa thể thu và phát , tránh tắc nghẽn số liệu khi chuyển qua lớp mạng. Ngoài ra, nhiều thực thể lớp phiên có thể trao đổi số liệu trên cùng một kết nối lớp mạng (multiplexing).

e) Lớp phiên

Liên kết giữa hai thực thể có nhu cầu trao đổi số liệu, ví dụ người dùng và một máy tính ở xa, được gọi là một phiên làm việc. Nhiệm vụ của lớp phiên là quản lý việc trao đổi số liệu, ví dụ: thiết lập giao diện giữa người dùng và

máy, xác định thông số điều khiển trao đổi số liệu (tốc độ truyền, số bit trong một byte, có kiểm tra lỗi parity hay không, v.v.), xác định loại giao thức mô phỏng thiết bị cuối (terminal emulation), v.v. Chức năng quan trọng nhất của lớp phiên là đảm bảo đồng bộ số liệu bằng cách thực hiện các điểm kiểm tra. Tại các điểm kiểm tra này, toàn bộ trạng thái và số liệu của phiên làm việc được lưu trữ trong bộ nhớ đệm. Khi có sự cố, có thể khởi tạo lại phiên làm việc từ điểm kiểm tra cuối cùng (không phải khởi tạo lại từ đầu).

f) Lớp thể hiện

Nhiệm vụ của lớp thể hiện là thích ứng các cấu trúc dữ liệu khác nhau của người dùng với cấu trúc dữ liệu thống nhất sử dụng trong mạng. Số liệu của người dùng có thể được nén và mã hoá ở lớp thể hiện, trước khi chuyển xuống lớp phiên. Ngoài ra, lớp thể hiện còn chứa các thư viện các yêu cầu của người dùng, thư viện tiện ích, ví dụ thay đổi dạng thể hiện của các *tệp*, nén *tệp*...

g) Lớp ứng dụng

Lớp ứng dụng cung cấp các phương tiện để người sử dụng có thể truy nhập được vào môi trường OSI, đồng thời cung cấp các dịch vụ thông tin phân tán. Lớp mạng cho phép người dùng khai thác các tài nguyên trong mạng tương tự như tài nguyên tại chỗ.

III.3. Các chuẩn kết nối thông dụng nhất IEEE 802.X và ISO 8802.X

Bên cạnh việc chuẩn hoá cho mạng nối chung dẫn đến kết quả cơ bản nhất là mô hình tham chiếu OSI như đã giới thiệu. Việc chuẩn hoá mạng cục bộ nói riêng đã được thực hiện từ nhiều năm nay để đáp ứng sự phát triển của mạng cục bộ.

Cũng như đối với mạng nói chung, có hai loại chuẩn cho mạng cục bộ, đó là :

- Các chuẩn chính thức (de jure) do các tổ chức chuẩn quốc gia và quốc tế ban hành.

- Các chuẩn tực tiễn (de facto) do các hãng soản xuất, các tổ chức người sử dụng xây dựng và được dùng rộng rãi trong thực tế

- Các chuẩn IEEE 802.x và ISO 8802.x

IEEE là tổ chức đi tiên phong trong lĩnh vực chuẩn hoá mạng cục bộ với đề án IEEE 802 với kết quả là một loạt các chuẩn thuộc họ IEEE 802.x ra đời . Cuối những năm 80, tổ chức ISO đã tiếp nhận họ chuẩn này và ban hành thành chuẩn quốc tế dưới mã hiệu tương ứng là ISO 8802.x.

IEEE 802.: là chuẩn đặc tả kiến trúc mạng, kết nối giữa các mạng và việc quản trị mạng đối với mạng cục bộ.

IEEE 802.2: là chuẩn đặc tả tầng dịch vụ giao thức của mạng cục bộ.

IEEE 802.3: là chuẩn đặc tả một mạng cục bộ dựa trên mạng Ethernet nổi tiếng của Digital, Intel và Xerox hợp tác xây dựng từ năm 1980.

Tầng vật lý của IEEE 802.3 có thể dùng các phương án sau để xây dựng:

- 10BASE5 : tốc độ 10Mb/s, dùng cáp xoắn đôi không bọc kim UTP (Unshield Twisted Pair), với phạm vi tín hiệu lên tới 500m, topo mạng hình sao.

- 10BASE2 : tốc độ 10Mb/s, dùng cáp đồng trục thin-cable với trở kháng 50 Ohm, phạm vi tín hiệu 200m,topo mạng dạng bus.

- 10BASE5 : tốc độ 10Mb/s, dùng cáp đồng trục thick-cable (đường kính 10mm) với trở kháng 50 Ohm, phạm vi tín hiệu 500m, topo mạng dạng bus.

- 10BASE-F: dùng cáp quang, tốc độ 10Mb/s phạm vi cáp 2000m.

IEEE 802.4: là chuẩn đặc tả mạng cục bộ với topo mạng dạng bus dùng thẻ bài để điều việc truy nhập đường truyền.

IEEE 802.5: là chuẩn đặc tả mạng cục bộ với topo mạng dạng vòng (ring) dùng thẻ bài để điều việc truy nhập đường truyền.

IEEE 802.6: là chuẩn đặc tả mạng tốc độ cao kết nối với nhiều mạng cục bộ thuộc các khu vực khác nhau của một đô thị (còn được gọi là mạng MAN - Metropolitan Area Network)

IEEE 802.9: là chuẩn đặc tả mạng tích hợp dữ liệu và tiếng nói bao gồm 1 kênh dị bộ 10 Mb/s cùng với 96 kênh 64Kb/s. Chuẩn này được thiết kế cho môi trường có lượng lưu thông lớn và cấp bách.

IEEE 802.10: là chuẩn đặc tả về an toàn thông tin trong các mạng cục bộ có khả năng liên tác .

IEEE 802.11: là chuẩn đặc tả mạng cục bộ không dây (Wireless LAN) hiện đang được tiếp tục phát triển.

IEEE 802.12: là chuẩn đặc tả mạng cục bộ dựa trên công nghệ được đề xuất bởi AT&T, IBM và HP gọi là 100 VG - AnyLAN. Mạng này có topo mạng hình sao và một phương pháp truy nhập đường truyền có điều khiển tranh chấp. Khi có nhu cầu truyền dữ liệu, một trạm sẽ gửi yêu cầu đến hub và trạm chỉ có truyền dữ liệu khi hub cho phép.

Mục 2: Các thiết bị mạng thông dụng và các chuẩn kết nối vật lý

I. Các thiết bị mạng thông dụng

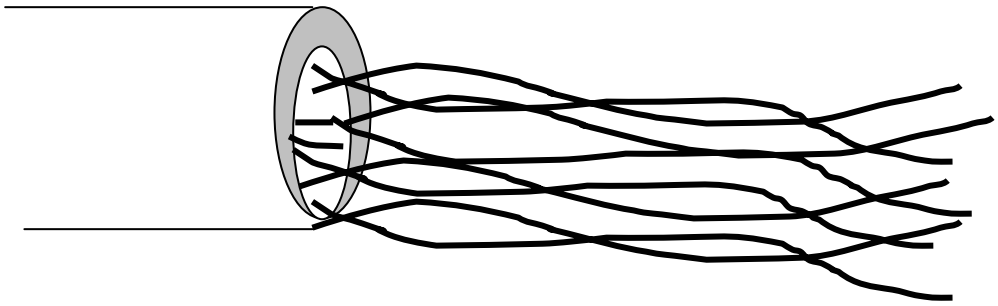
II.1. Các loại cáp truyền

II.1.1. Cáp đôi dây xoắn (Twisted pair cable)

Cáp đôi dây xoắn là cáp gồm hai dây đồng xoắn để tránh gây nhiễu cho các đôi dây khác, có thể kéo dài tới vài km mà không cần khuyếch đại. Giải tần trên cáp dây xoắn đạt khoảng 300–4000Hz, tốc độ truyền đạt vài kbps đến vài Mbps. Cáp xoắn có hai loại:

- Loại có bọc kim loại để tăng cường chống nhiễu gọi là cap STP (Shield Twisted Pair). Loại này trong vỏ bọc kim có thể có nhiều đôi dây. Về lý thuyết thì tốc độ truyền có thể đạt 500 Mb/s nhưng thực tế thấp hơn rất nhiều (chỉ đạt 155 Mbps với cáp dài 100 m)

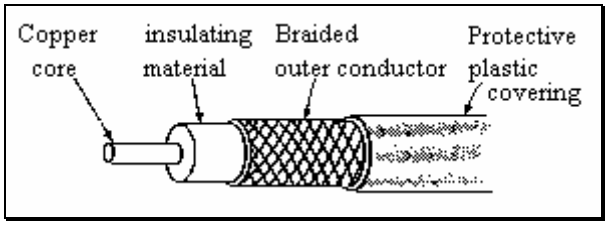
- Loại không bọc kim gọi là UTP (UnShield Twisted Pair), chất lượng kém hơn STP nhưng rất rẻ. Cap UTP được chia làm 5 hạng tuỳ theo tốc độ truyền. Cáp loại 3 dùng cho điện thoại. Cáp loại 5 có thể truyền với tốc độ 100Mb/s rất hay dùng trong các mạng cục bộ vì vừa rẻ vừa tiện sử dụng. Cáp này có 4 đôi dây xoắn nằm trong cùng một vỏ bọc



Hình 7. Cáp UTP Cat. 5

II.1.2. Cáp đồng trục (Coaxial cable) băng tần cơ sở

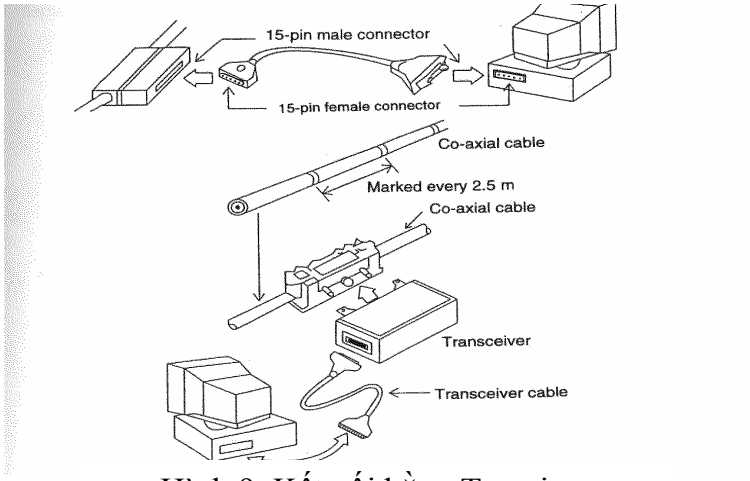
Là cáp mà hai dây của nó có lõi lồng nhau, lõi ngoài là lưới kim loại. , Khả năng chống nhiễu rất tốt nên có thể sử dụng với chiều dài từ vài trăm met đến vài km. Có hai loại được dùng nhiều là loại có trở kháng 50 ohm và loại có trở kháng 75 ohm



Hình 8. Cáp đồng trục

Dải thông của cáp này còn phụ thuộc vào chiều dài của cáp. Với khoảng cách1 km có thể đạt tốc độ truyền tư 1– 2 Gbps. Cáp đồng trục băng tần cơ sở thường dùng cho các mạng cục bộ. Có thể nối cáp bằng các đầu nối theo chuẩn BNC có hình chữ T. ở VN người ta hay gọi cáp này là cáp gầy do dịch từ tên trong tiếng Anh là 'Thin Ethernet".

Một loại cáp khác có tên là "Thick Ethernet" mà ta gọi là cáp béo. Loại này thường có màu vàng. Người ta không nối cáp bằng các đầu nối chữ T như



Hình 9. Kết nối bằng Traceiver

cáp gầy mà nối qua các kẹp bấm vào dây. Cứ 2m5 lại có đánh dấu để nối dây (nếu cần). Từ kẹp đó người ta gắn các tranceiver rồi nối vào máy tính. (Xem hình 9)

II.1.3. Cáp đồng trục băng rộng (Broadband Coaxial Cable)

Đây là loại cáp theo tiêu chuẩn truyền hình (thường dùng trong truyền hình cap) có giải thông từ 4 – 300 Khz trên chiều dài 100 km. Thuật ngữ "băng rộng" vốn là thuật ngữ của ngành truyền hình còn trong ngành truyền số liệu điều này chỉ có nghĩa là cáp loại này cho phép truyền thông tin tương tự (analog) mà thôi. Các hệ thống dựa trên cáp đồng trục băng rộng có thể truyền song song nhiều kênh. Việc khuyếch đại tín hiệu chống suy hao có thể làm theo kiểu khuyếch đại tín hiệu tương tự (analog). Để truyền thông cho máy tính cần chuyển tín hiệu số thành tín hiệu tương tự.

II.1.4. Cáp quang

Dùng để truyền các xung ánh sáng trong lòng một sợi thuỷ tinh phản xạ toàn phần. Môi trường cáp quang rất lý tưởng vì

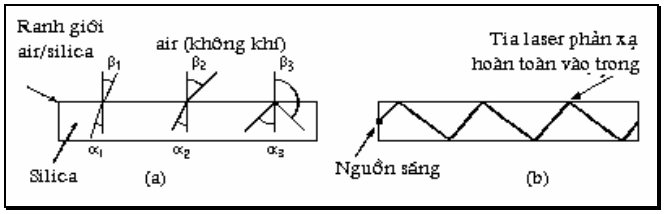
- Xung ánh sáng có thể đi hàng trăm km mà không giảm cường độ sáng.

- Giải thông rất cao vì tần số ánh sáng dùng đối với cáp quang cỡ khoảng 1014 –1016

- An toàn và bí mật

- Không bị nhiễu điện từ

Chỉ có hai nhược điểm là khó nối dây và giá thành cao.



Hình 10. Truyền tín hiệu bằng cáp quang

Để phát xung ánh sáng người ta dùng các đèn LED hoặc các diod laser. Để nhận người ta dùng các photo diode , chúng sẽ tạo ra xung điện khi bắt được xung ánh sáng

Cáp quang cũng có hai loại

- Loại đa mode (multimode fiber): khi góc tới thành dây dẫn lớn đến một mức nào đó thì có hiện tượng phản xạ toàn phần. Nhiều tia sáng có thể cùng truyền miễn là góc tới của chúng đủ lớn. Các cap đa mode có đường kính khoảng 50 μ

- Loại đơn mode (singlemode fiber): khi đường kính dây dẫn bằng bước sóng thì cáp quang giống như một ống dẫn sóng, không có hiện tượng phản xạ nhưng chỉ cho một tia đi. Loại nàycó cường kính khoản 8 μ và phải dùng diode laser. Cáp quang đa mode có thể cho phép truyền xa tới hàng trăm km mà không cần phải khuyếch đại.

II.2. Các thiết bị ghép nối

II.2.1. Card giao tiếp mạng (Network Interface Card viết tắt là NIC)

Đó là một card được cắm trực tiếp vào máy tính. Trên đó có các mạch điện giúp cho việc tiếp nhận (receiver) hoặc/và phát (transmitter) tín hiệu lên mạng. Người ta thường dùng từ tranceiver để chỉ thiết bị (mạch) có cả hai chức năng thu và phát. Transceiver có nhiều loại vì phải thích hợp đối với cả môi trường truyền và do đó cả đầu nối. Ví dụ với cáp gầy card mạng cần có đường giao tiếp theo kiểu BNC, với cáp UTP cần có đầu nối theo kiểu giắc điện thoại K5, cáp dày dùng đường nối kiểu AUI , với cáp quang phải có những transceiver cho phép chuyển tín hiệu điện thành các xung ánh sáng và ngược lại.

Để dễ ghép nối, nhiều card có thể có nhiều đầu nối ví dụ BNC cho cáp gầy, K45 cho UTP hay AUI cho cáp béo

Trong máy tính thường để sẵn các khe cắm để bổ sung các thiết bị ngoại vi hay cắm các thiết bị ghép nối.

II.2.2. Bộ chuyển tiếp (REPEATER)

Tín hiệu truyền trên các khoảng cách lớn có thể bị suy giảm. Nhiệm vụ của các repeater là hồi phục tín hiệu để có thể truyền tiếp cho các trạm khác. Một số repeater đơn giản chỉ là khuyếch đại tín hiệu. Trong trường hợp đó cả tín hiệu bị méo cũng sẽ bị khuyếch đại. Một số repeater có thể chỉnh cả tín hiệu.

II.2.3. Các bộ tập trung (Concentrator hay HUB)

HUB là một loại thiết bị có nhiều đầu để cắm các đầu cáp mạng. HUB có thể có nhiều loại ổ cắm khác nhau phù hợp với kiểu giắc mạng RJ45, AUI hay BCN. Như vậy người ta sử dụng HUB để nối dây theo kiểu hình sao. Ưu điểm của kiểu nối này là tăng độ độc lập của các máy . Nếu dây nối tới một máy nào đó tiếp xúc không tốt cũng không ảnh hưởng đến máy khác.

Đặc tính chủ yếu của HUB là hệ thống chuyển mạch trung tâm trong mạng có kiến trúc hình sao với việc chuyển mạch được thực hiện theo hai cách: store-and-forward hoặc on-the-fly. Tuy nhiên hệ thống chuyển mạch trung tâm làm nảy sinh vấn đề khi lỗi xảy ra ở chính trung tâm, vì vậy hướng phát triển trong suốt nhiều năm qua là khử lỗi để làm tăng độ tin cậy của HUB.

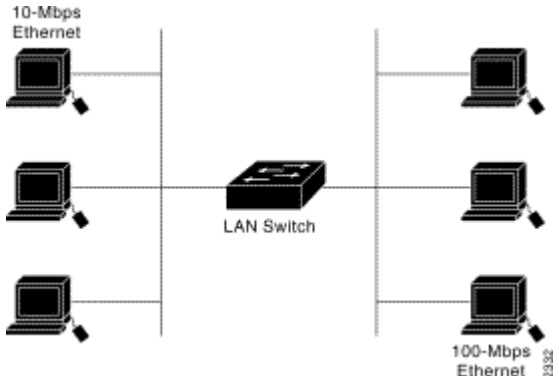
Có loại HUB thụ động (passive HUB) là HUB chỉ đảm bảo chức năng kết nối hoàn toàn không xử lý lại tín hiệu. Khi đó không thể dùng HUB để tăng khoảng cách giữa hai máy trên mạng.

HUB chủ động (active HUB) là HUB có chức năng khuyếch đại tín hiệu để chống suy hao. Với HUB này có thể tăng khoảng cách truyền giữa các máy.

HUB thông minh (intelligent HUB) là HUB chủ động nhưng có khả năng tạo ra các gói tin mang tin tức về hoạt động của mình và gửi lên mạng để người quản trị mạng có thể thực hiện quản trị tự động

II.2.4. Switching Hub (hay còn gọi tắt là switch)

Là các bộ chuyển mạch thực sự. Khác với HUB thông thường, thay vì chuyển một tín hiệu đến từ một cổng cho tất cả các cổng, nó chỉ chuyển tín hiệu đến cổng có trạm đích. Do vậy Switch là một thiết bị quan trọng trong các mạng cục bộ lớn dùng để phân đoạn mạng. Nhờ có switch mà đụng độ trên mạng giảm hẳn. Ngày nay switch là các thiết bị mạng quan trọng cho phép tuỳ biến trên mạng chẳng hạn lập mạng ảo.



Hình 11. LAN Switch nối hai Segment mạng

Switch thực chất là một loại bridge, về tính năng kỹ thuật, nó là loại bridge có độ trễ nhỏ nhất. Khác với bridge là phải đợi đến hết frame rồi mới truyền, switch sẽ chờ cho đến khi nhận được địa chỉ đích của frame gửi tới và lập tức được truyền đi ngay. Điều này có nghĩa là frame sẽ được gửi tới LAN cần gửi trước khi nó được switch nhận xong hoàn toàn.

II.2.5. Modem

Là tên viết tắt từ hai từ điều chế (MOdulation) và giải điều chế (DEModulation) là thiết bị cho phép điều chế để biến đổi tín hiệu số sang tín hiệu tương tự để có thể gửi theo đường thoại và khi nhận tín hiệu từ đường thoại có thể biến đổi ngược lại thành tín hiệu số. Tuy nhiên có thể sử dụng nó theo kiểu kết nối từ xa theo đường điện thoại

II.2.6. Multiplexor - Demultiplexor

Bộ dồn kênh có chức năng tổ hợp nhiều tín hiệu để cùng gửi trên một đường truyền. Đương nhiên tại nơi nhận cần phải tách kênh.

II.2.7. Router

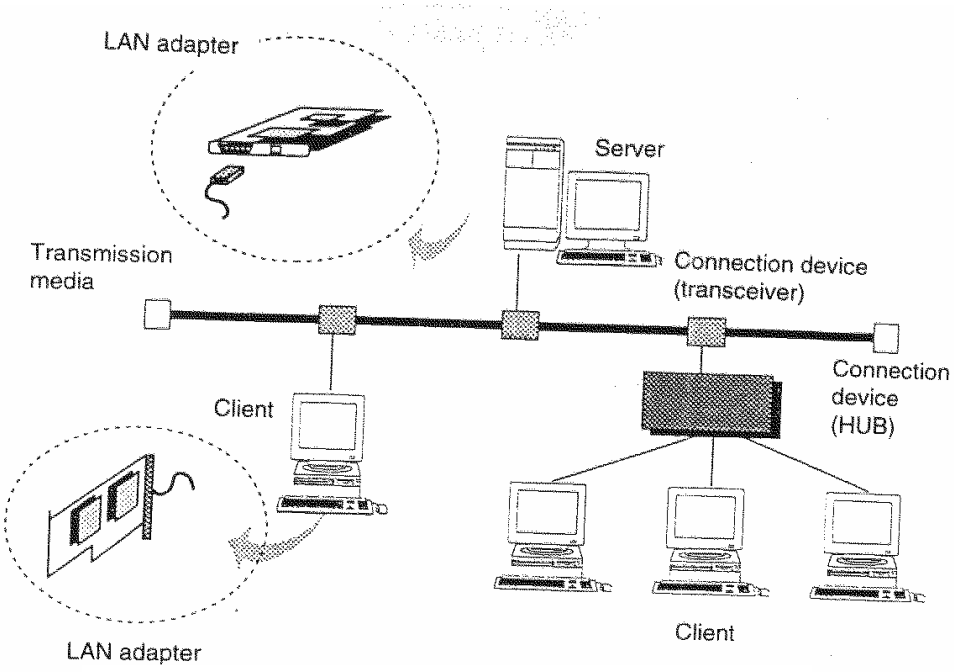
Router là một thiết bị không phải để ghép nối giữa các thiết bị trong một mạng cục bộ mà dùng để ghép nối các mạng cục bộ với nhau thành mạng rộng. Router thực sự là một máy tính làm nhiệm vụ chọn đường cho các gói tin hướng ra ngoài.

Khác với repeaters và bridges, router là thiết bị kết nối mạng độc lập phần cứng, nó được dùng để kết nối các mạng có cùng chung giao thức. Chức năng cơ bản nhất của router là cung cấp một môi trường chuyển mạch gói (packet switching) đáng tin cậy để lưu trữ và truyền số liệu. Để thực hiện điều đó, nó thiết lập các thông tin về các đường truyền hiện có trong mạng, và khi cần nó sẽ cung cấp hai hay nhiều đường truyền giữa hai mạng con bất kỳ tạo ra khả năng mềm dẻo trong việc tìm đường đi hợp lý nhất về một phương diện nào đó.

III.3. Một số kiểu nối mạng thông dụng và các chuẩn

III.3.1.Các thành phần thông thường trên một mạng cục bộ gồm có

- Các máy chủ cung cấp dịch vụ (server)
- Các máy trạm cho người làm việc (workstation)
- Đường truyền (cáp nối)
- Card giao tiếp giữa máy tính và đường truyền (network interface card)
- Các thiết bị nối (connection device)



Hình 9. Cấu hình của một mạng cục bộ

Hai yếu tố được quan tâm hàng đầu khi kết nối mạng cục bộ là tốc độ trong mạng và bán kính mạng. Tên các kiểu mạng dùng theo giao thức CSMA/CD cũng thể hiện điều này. Sau đây là một số kiểu kết nối đó với tốc độ 10 Mb/s khá thông dụng trong thời gian qua và một số thông số kỹ thuật:

Chuẩn	IEEE 802.3		
Kiểu	10BASE5	10BASE2	10BASE-T
Kiểu cáp	Cáp đồng trục	Cáp đồng trục	Cáp UTP
Tốc độ	10 Mb/s		
Độ dài cáp tối đa	500 m/segment	185 m/segment	100 m kể từ HUB
Số các thực thể truyền thông	100 host /segment	30 host / segment	Số cổng của HUB

III.3.2. Kiểu 10BASE5:

Là chuẩn CSMA/CD có tốc độ 10Mb và bán kính 500 m. Kiểu này dùng cáp đồng trục loại thick ethernet (cáp đồng trục béo) với tranceiver. Có thể kết nối vào mạng khoảng 100 máy

Đặc điểm của chuẩn 10BASE 5

Tốc độ tối đa	10 Mbps
Chiều dài tối đa của đoạn cáp của một phân đoạn (segment)	500 m
Số trạm tối đa trên mỗi đoạn	100
Khoảng cách giữa các trạm	>=2,5 m (bội số của 2,5 m (giảm thiểu hiện tượng giao thoa do sóng đứng trên các đoạn ?))
Khoảng cách tối đa giữa máy trạm và đường trục chung	50 m
Số đoạn kết nối tối đa	2 (=>tối đa có 3 phân đoạn)
Tổng chiều dài tối đa đoạn kết nối (có thể là một đoạn kết nối khi có hai phân đoạn, hoặc hai đoạn kết nối khi có ba phân đoạn)	1000 m
Tổng số trạm + các bộ lặp Repeater	Không quá 1024
Chiều dài tối đa	3*500+1000=2500 m

III.3.3. Kiểu 10BASE2:

Là chuẩn CSMA/CD có tốc độ 10Mb và bán kính 200 m. Kiểu này dùng cáp đồng trục loại thin ethernet với đầu nối BNC. Có thể kết nối vào mạng khoảng 30 máy

III.3.5. Kiểu 10BASE-F

Dùng cab quang (Fiber cab), chủ yếu dùng nối các thiết bị xa nhau, tạo dựng đường trục xương sống (backborn) để nối các mạng LAN xa nhau (2-10 km)

Chương 2 : Giới thiệu giao thức TCP/IP

Chương hai cung cấp các kiến thức liên quan đến TCP/IP và địa chỉ IP. Giao thức TCP/IP trở thành giao thức mạng phổ biến nhất nhờ sự phát triển không ngừng của mạng Internet. Các mạng máy tính của các cơ quan, tổ chức, công ty hầu hết đều sử dụng TCP/IP làm giao thức mạng nhờ tính dễ mở rộng và qui hoạch của nó. Đồng thời, do sự phát triển của mạng Internet nên nhu cầu kết nối ra Internet và sử dụng TCP/IP đã trở nên thiết yếu cho mọi đối tượng

Chương này đòi hỏi các học viên phải quen thuộc với các kiến thức cơ bản về hệ nhị phân, các khái niệm bit, byte, chuyển đổi nhị phân, thập phân. Các cách biểu diễn cấu trúc gói tin theo dạng trường bit, byte cũng yêu cầu học viên phải có được hiểu biết cơ sở về kỹ thuật thông tin truyền thông.

I.1. Giao thức IP

I.1.1. Họ giao thức TCP/IP

Sự ra đời của họ giao thức TCP/IP gắn liền với sự ra đời của Internet mà tiền thân là mạng **ARPA**net (**A**dvanced **R**esearch **P**rojects **A**gency) do Bộ Quốc phòng Mỹ tạo ra. Đây là bộ giao thức được dùng rộng rãi nhất vì tính mở của nó. Điều đó có nghĩa là bất cứ máy nào dùng bộ giao thức TCP/IP đều có thể nối được vào Internet. Hai giao thức được dùng chủ yếu ở đây là **TCP** (**T**ransmission **C**ontrol **P**rotocol) và **IP** (**I**nternet **P**rotocol). Chúng đã nhanh chóng được đón nhận và phát triển bởi nhiều nhà nghiên cứu và các hãng công nghiệp máy tính với mục đích xây dựng và phát triển một mạng truyền thông mở rộng khắp thế giới mà ngày nay chúng ta gọi là Internet. Phạm vi phục vụ của Internet không còn dành cho quân sự như **ARPA**net nữa mà nó đã mở rộng lĩnh vực cho mọi loại đối tượng sử dụng, trong đó tỷ lệ quan trọng nhất vẫn thuộc về giới nghiên cứu khoa học và giáo dục.

Khái niệm *giao thức (*protocol) là một khái niệm cơ bản của mạng thông tin máy tính. Có thể hiểu một cách khái quát rằng đó chính là tập hợp tất cả các qui tắc cần thiết (các thủ tục, các khuôn dạng dữ liệu, các cơ chế phụ trợ...) cho phép các thao tác trao đổi thông tin trên mạng được thực hiện một cách chính xác và an toàn. Có rất nhiều họ giao thức đang được thực hiện trên mạng thông

tin máy tính hiện nay như IEEE 802.X dùng trong mạng cục bộ, CCITT X25 dùng cho mạng diện rộng và đặc biệt là họ giao thức chuẩn của ISO (tổ chức tiêu chuẩn hóa quốc tế) dựa trên mô hình tham chiếu bảy tầng cho việc nối kết các hệ thống mở. Gần đây, do sự xâm nhập của Internet vào Việt nam, chúng ta được làm quen với họ giao thức mới là TCP/IP mặc dù chúng đã xuất hiện từ hơn 20 năm trước đây.

TCP/IP (Transmission Control Protocol/ Internet Protocol) TCP/IP là một họ giao thức cùng làm việc với nhau để cung cấp phương tiện truyền thông liên mạng được hình thành từ những năm 70.

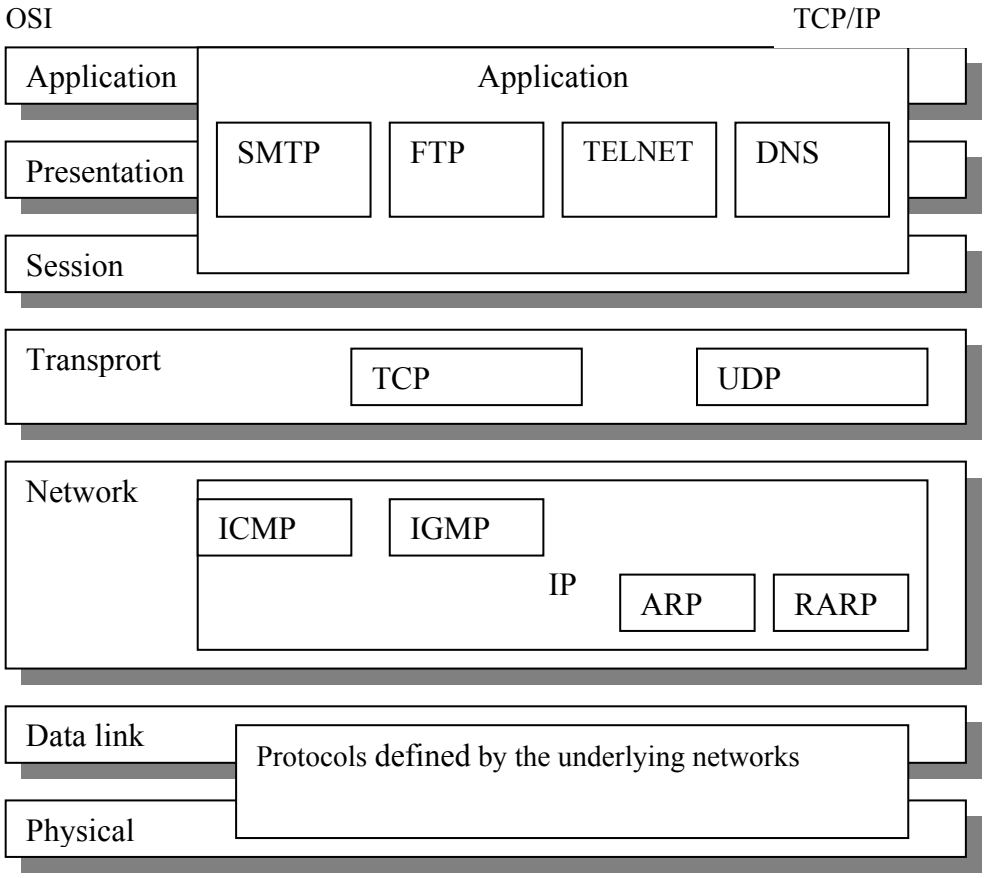
Đến năm 1981, TCP/IP phiên bản 4 mới hoàn tất và được phổ biến rộng rãi cho toàn bộ những máy tính sử dụng hệ điều hành UNIX. Sau này Microsoft cũng đã đưa TCP/IP trở thành một trong những giao thức căn bản của hệ điều hành Windows 9x mà hiện nay đang sử dụng.

Đến năm 1994, một bản thảo của phiên bản IPv6 được hình thành với sự cộng tác của nhiều nhà khoa học thuộc các tổ chức Internet trên thế giới để cải tiến những hạn chế của IPv4.

Khác với mô hình ISO/OSI tầng liên mạng sử dụng giao thức kết nối mạng "không liên kết" (connectionless) IP, tạo thành hạt nhân hoạt động của Internet. Cùng với các thuật toán định tuyến RIP, OSPF, BGP, tầng liên mạng IP cho phép kết nối một cách mềm dẻo và linh hoạt các loại mạng "vật lý" khác nhau như: Ethernet, Token Ring , X.25...

Giao thức trao đổi dữ liệu "có liên kết" (connection - oriented) TCP được sử dụng ở tầng vận chuyển để đảm bảo tính chính xác và tin cậy việc trao đổi dữ liệu dựa trên kiến trúc kết nối "không liên kết" ở tầng liên mạng IP.

Các giao thức hỗ trợ ứng dụng phổ biến như truy nhập từ xa (telnet), chuyển tệp (FTP), dịch vụ World Wide Web (HTTP), thư điện tử (SMTP), dịch vụ tên miền (DNS) ngày càng được cài đặt phổ biến như những bộ phận cấu thành của các hệ điều hành thông dụng như UNIX (và các hệ điều hành chuyên dụng cùng họ của các nhà cung cấp thiết bị tính toán như AIX của IBM, SINIX của Siemens, Digital UNIX của DEC), Windows9x/NT, Novell Netware,...



Hình 2.1 Mô hình OSI và mô hình kiến trúc của TCP/IP

Như vậy, TCP tương ứng với lớp 4 cộng thêm một số chức năng của lớp 5 trong họ giao thức chuẩn ISO/OSI. Còn IP tương ứng với lớp 3 của mô hình OSI.

Trong cấu trúc bốn lớp của TCP/IP, khi dữ liệu truyền từ lớp ứng dụng cho đến lớp vật lý, mỗi lớp đều cộng thêm vào phần điều khiển của mình để đảm bảo cho việc truyền dữ liệu được chính xác. Mỗi thông tin điều khiển này được gọi là một *header* và được đặt ở trước phần dữ liệu được truyền. Mỗi lớp xem tất cả các thông tin mà nó nhận được từ lớp trên là dữ liệu, và đặt phần thông tin điều khiển *header* của nó vào trước phần thông tin này. Việc cộng thêm vào các *header* ở mỗi lớp trong quá trình truyền tin được gọi là *encapsulation*. Quá trình nhận dữ liệu diễn ra theo chiều ngược lại: mỗi lớp sẽ tách ra phần *header* trước khi truyền dữ liệu lên lớp trên.

Mỗi lớp có một cấu trúc dữ liệu riêng, độc lập với cấu trúc dữ liệu được dùng ở lớp trên hay lớp dưới của nó. Sau đây là giải thích một số khái niệm thường gặp.

Stream là dòng số liệu được truyền trên cơ sở đơn vị số liệu là Byte.

Số liệu được trao đổi giữa các ứng dụng dùng TCP được gọi là *stream*, trong khi dùng UDP, chúng được gọi là *message*.

Mỗi gói số liệu TCP được gọi là *segment* còn UDP định nghĩa cấu trúc dữ liệu của nó là *packet*.

Lớp Internet xem tất cả các dữ liệu như là các khối và gọi là *datagram*. Bộ giao thức TCP/IP có thể dùng nhiều kiểu khác nhau của lớp mạng dưới cùng, mỗi loại có thể có một thuật ngữ khác nhau để truyền dữ liệu.

Phần lớn các mạng kết cấu phần dữ liệu truyền đi dưới dạng các *packets* hay là các *frames*.

Application	Stream
Transport	Segment/datagram
Internet	Datagram
Network Access	Frame

Cấu trúc dữ liệu tại các lớp của TCP/IP

Lớp truy nhập mạng

Network **A**ccess **L**ayer là lớp thấp nhất trong cấu trúc phân bậc của TCP/IP. Những giao thức ở lớp này cung cấp cho hệ thống phương thức để truyền dữ liệu trên các tầng vật lý khác nhau của mạng. Nó định nghĩa cách thức truyền các khối dữ liệu (datagram) IP. Các giao thức ở lớp này phải biết chi tiết các phần cấu trúc vật lý mạng ở dưới nó (bao gồm cấu trúc gói số liệu, cấu trúc địa chỉ...) để định dạng được chính xác các gói dữ liệu sẽ được truyền trong từng loại mạng cụ thể.

So sánh với cấu trúc OSI/OSI, lớp này của TCP/IP tương đương với hai lớp Datalink, và Physical.

Chức năng định dạng dữ liệu sẽ được truyền ở lớp này bao gồm việc nhúng các gói dữ liệu IP vào các *frame* sẽ được truyền trên mạng và việc ánh xạ các địa chỉ IP vào địa chỉ vật lý được dùng cho mạng.

Lớp liên mạng

Internet Layer là lớp ở ngay trên lớp Network Access trong cấu trúc phân lớp của TCP/IP. Internet Protocol là giao thức trung tâm của TCP/IP và là phần quan trọng nhất của lớp Internet. IP cung cấp các gói lưu chuyển cơ bản mà thông qua đó các mạng dùng TCP/IP được xây dựng.

I.1.2. Chức năng chính của - Giao thức liên mạng IP(v4)

Trong phần này trình bày về giao thức IPv4 (để cho thuận tiện ta viết IP có nghĩa là đề cập đến IPv4).

Mục đích chính của IP là cung cấp khả năng kết nối các mạng con thành liên mạng để truyền dữ liệu. IP cung cấp các chức năng chính sau:

- Định nghĩa cấu trúc các gói dữ liệu là đơn vị cơ sở cho việc truyền dữ liệu trên Internet.

- Định nghĩa phương thức đánh địa chỉ IP.

- Truyền dữ liệu giữa tầng vận chuyển và tầng mạng .

- Định tuyến để chuyển các gói dữ liệu trong mạng.

- Thực hiện việc phân mảnh và hợp nhất (fragmentation -reassembly) các gói dữ liệu và nhúng / tách chúng trong các gói dữ liệu ở tầng liên kết.

I.2. Địa chỉ IP

Sơ đồ địa chỉ hoá để định danh các trạm (host) trong liên mạng được gọi là địa chỉ IP. Mỗi địa chỉ IP có độ dài 32 bits (đối với IP4) được tách thành 4 vùng (mỗi vùng 1 byte), có thể được biểu thị dưới dạng thập phân, bát phân, thập lục phân hoặc nhị phân. Cách viết phổ biến nhất là dùng ký pháp thập phân có dấu chấm để tách giữa các vùng. Mục đích của địa chỉ IP là để định danh duy nhất cho một host bất kỳ trên liên mạng.

- Lớp B cho phép định danh tới 16384 mạng (10111111.11111111.host.host), với tối đa 65535 host trên mỗi mạng. Dạng của lớp B (network number. Network number.host.host). Nếu dùng ký pháp thập phân cho phép 128 đến 191 cho vùng đầu, 1 đến 255 cho các vùng còn lại

- Lớp C cho phép định danh tới 2.097.150 mạng và tối đa 254 host cho mỗi mạng. Lớp này được dùng cho các mạng có ít trạm. Lớp C sử dụng 3 bytes đầu định danh địa chỉ mạng (110xxxxx). Dạng của lớp C (network number. Network number.Network number.host). Nếu dùng dạng ký pháp thập phân cho phép 129 đến 233 cho vùng đầu và từ 1 đến 255 cho các vùng còn lại.

- Lớp D dùng để gửi IP datagram tới một nhóm các host trên một mạng. Tất cả các số lớn hơn 233 trong trường đầu là thuộc lớp D

- Lớp E dự phòng để dùng trong tương lai

Như vậy địa chỉ mạng cho lớp: A: từ 1 đến 126 cho vùng đầu tiên, 127 dùng cho địa chỉ loopback, B từ 128.1.0.0 đến 191.255.0.0, C từ 192.1.0.0 đến 233.255.255.0

Ví dụ:

192.1.1.1 địa chỉ lớp C có địa chỉ mạng 192.1.1.0, địa chỉ host là 1

200.6.5.4 địa chỉ lớp C có địa chỉ mạng 200.6.5, địa chỉ mạng là 4

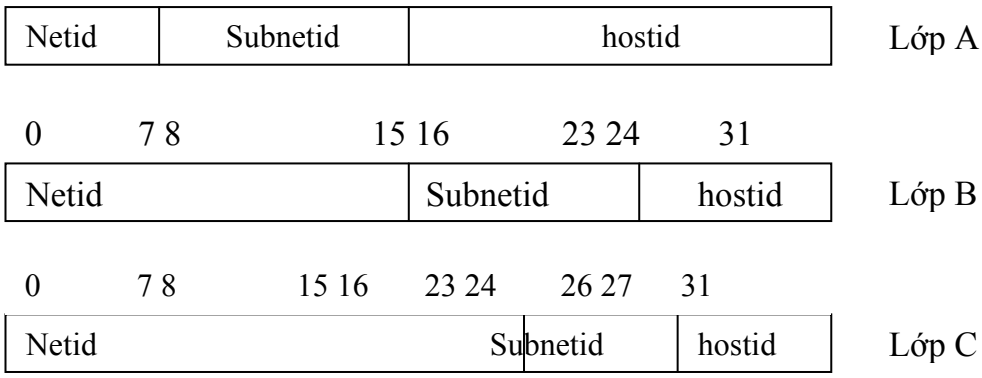
150.150.5.6 địa chỉ lớp B có địa chỉ mạng 150.150.0.0, địa chỉ host là 5.6

9.6.7.8 địa chỉ lớp A có địa chỉ mạng 9.0.0.0, địa chỉ host là 6.7.8

128.1.0.1 địa chỉ lớp B có địa chỉ mạng 128.1.0.0, địa chỉ host là 0.1

Subneting

Trong nhiều trường hợp, một mạng có thể được chia thành nhiều mạng con (subnet), lúc đó có thể đưa thêm các vùng subnetid để định danh các mạng con. Vùng subnetid được lấy từ vùng hostid, cụ thể đối với 3 lớp A, B, C như sau:



Hình 2.5 Bổ sung vùng subnetid

Ví dụ:

17.1.1.1 địa chỉ lớp A có địa chỉ mạng 17, địa chỉ subnet 1, địa chỉ host 1.1

129.1.1.1 địa chỉ lớp B có địa chỉ mạng 129.1, địa chỉ subnet 1, địa chỉ host 1.

I.3. Cấu trúc gói dữ liệu IP

IP là giao thức cung cấp dịch vụ truyền thông theo kiểu "không liên kết" (connectionless). Phương thức không liên kết cho phép cặp trạm truyền nhận không cần phải thiết lập liên kết trước khi truyền dữ liệu và do đó không cần phải giải phóng liên kết khi không còn nhu cầu truyền dữ liệu nữa. Phương thức kết nối "không liên kết" cho phép thiết kế và thực hiện giao thức trao đổi dữ liệu đơn giản (không có cơ chế phát hiện và khắc phục lỗi truyền). Cũng chính vì vậy độ tin cậy trao đổi dữ liệu của loại giao thức này không cao.

Các gói dữ liệu IP được định nghĩa là các datagram. Mỗi datagram có phần tiêu đề (header) chứa các thông tin cần thiết để chuyển dữ liệu (ví dụ địa chỉ IP của trạm đích). Nếu địa chỉ IP đích là địa chỉ của một trạm nằm trên cùng một mạng IP với trạm nguồn thì các gói dữ liệu sẽ được chuyển thẳng tới đích; nếu địa chỉ IP đích không nằm trên cùng một mạng IP với máy nguồn thì các gói dữ liệu sẽ được gửi đến một máy trung chuyển, IP gateway để chuyển tiếp. IP gateway là một thiết bị mạng IP đảm nhận việc lưu chuyển các gói dữ liệu IP giữa hai mạng IP khác nhau. Hình 2.3 mô tả cấu trúc gói số liệu IP.

- VER (4 bits) : chỉ Version hiện hành của IP được cài đặt.

- IHL (4 bits) : chỉ độ dài phần tiêu đề (Internet Header Length) của datagram, tính theo đơn vị word (32 bits). Nếu không có trường này thì độ dài mặc định của phần tiêu đề là 5 từ.

- Type of service (8 bits): cho biết các thông tin về loại dịch vụ và mức ưu tiên của gói IP, có dạng cụ thể như sau:

Precedence	D	T	R	Unused

Trong đó:

Precedence (3 bits): chỉ thị về quyền ưu tiên gửi datagram, cụ thể là:

111 Network Control (cao nhất) 011- flash

110 Internetwork Control 010 Immediate

101 CRITIC/ECP 001 Priority

100 Flas Override 000 Routine (thấp nhất)

D (delay) (1 bit) : chỉ độ trễ yêu cầu

D=0 độ trễ bình thường, D=1 độ trễ thấp

T (Throughput) (1 bit) : chỉ số thông lượng yêu cầu

T=1 thông lượng bình thường

T=1 thông lượng cao

R (Reliability) (1 bit): chỉ độ tin cậy yêu cầu

R=0 độ tin cậy bình thường

R=1 độ tin cậy cao

- Total Length (16 bits): chỉ độ dài toàn bộ datagram, kể cả phần header (tính theo đơn vị bytes), vùng dữ liệu của datagram có thể dài tới 65535 bytes.

- Identification (16 bits) : cùng với các tham số khác như (Source Address và Destination Address) tham số này dùng để định danh duy nhất cho một datagram trong khoảng thời gian nó vẫn còn trên liên mạng

- Header checksum (16 bits): mã kiểm soát lỗi sử dụng phương pháp CRC (Cyclic Redundancy Check) dùng để đảm bảo thông tin về gói dữ liệu được truyền đi một cách chính xác (mặc dù dữ liệu có thể bị lỗi). Nếu như việc kiểm tra này thất bại, gói dữ liệu sẽ bị huỷ bỏ tại nơi xác định được lỗi. Cần chú ý là IP không cung cấp một phương tiện truyền tin cậy bởi nó không cung cấp cho ta một cơ chế để xác nhận dữ liệu truyền tại điểm nhận hoặc tại những điểm trung gian. Giao thức IP không có cơ chế Error Control cho dữ liệu truyền đi, không có cơ chế kiểm soát luồng dữ liệu (flow control).

- Source Address (32 bits): địa chỉ của trạm nguồn.

- Destination Address (32 bits): địa chỉ của trạm đích.

- Option (có độ dài thay đổi) sử dụng trong một số trường hợp, nhưng thực tế chúng rất ít dùng. Option bao gồm bảo mật, chức năng định tuyến đặc biệt

- Padding (độ dài thay đổi): vùng đệm, được dùng để đảm bảo cho phần header luôn kết thúc ở một mốc 32 bits

- Data (độ dài thay đổi): vùng dữ liệu có độ dài là bội của 8 bits, tối đa là 65535 bytes.

I.4. Phân mảnh và hợp nhất các gói IP

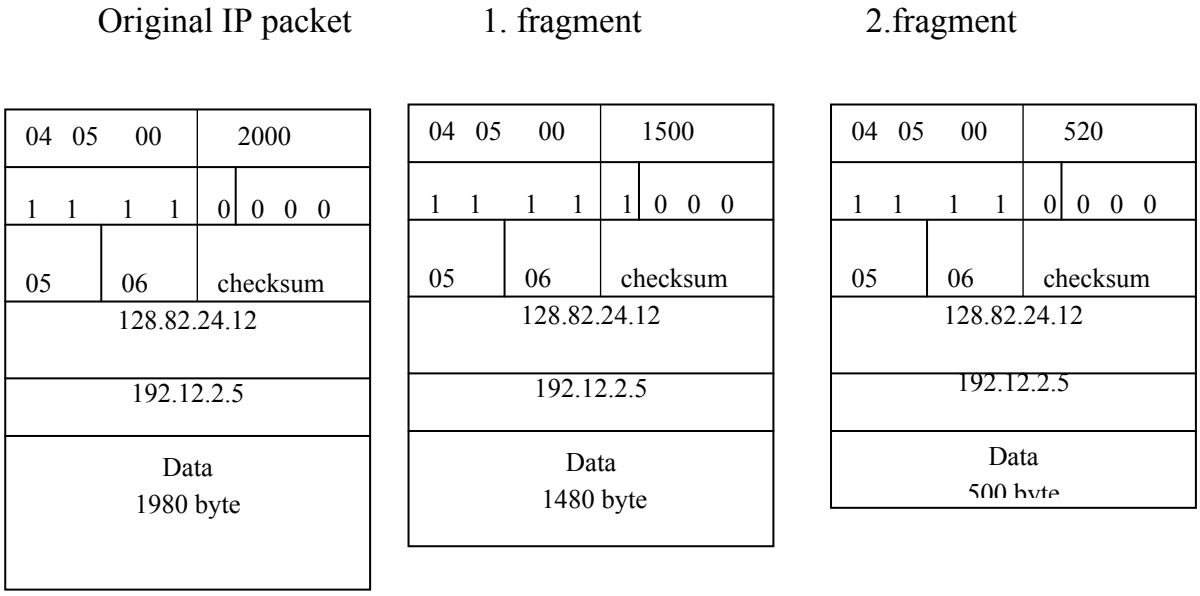
Các gói dữ liệu IP phải được nhúng trong khung dữ liệu ở tầng liên kết dữ liệu tương ứng, trước khi chuyển tiếp trong mạng. Quá trình nhận một gói dữ liệu IP diễn ra ngược lại. Ví dụ, với mạng Ethernet ở tầng liên kết dữ liệu quá trình chuyển một gói dữ liệu diễn ra như sau. Khi gửi một gói dữ liệu IP cho mức Ethernet, IP chuyển cho mức liên kết dữ liệu các thông số địa chỉ Ethernet đích, kiểu khung Ethernet (chỉ dữ liệu mà Ethernet đang mang là của IP) và cuối cùng là gói IP. Tầng liên kết số liệu đặt địa chỉ Ethernet nguồn là địa chỉ kết nối mạng của mình và tính toán giá trị checksum. Trường type chỉ ra kiểu khung là 0x0800 đối với dữ liệu IP. Mức liên kết dữ liệu sẽ chuyển khung dữ liệu theo thuật toán truy nhập Ethernet.

Một gói dữ liệu IP có độ dài tối đa 65536 byte, trong khi hầu hết các tầng liên kết dữ liệu chỉ hỗ trợ các khung dữ liệu nhỏ hơn độ lớn tối đa của gói dữ liệu IP nhiều lần (ví dụ độ dài lớn nhất của một khung dữ liệu Ethernet là

1500 byte). Vì vậy cần thiết phải có cơ chế phân mảnh khi phát và hợp nhất khi thu đối với các gói dữ liệu IP.

Độ dài tối đa của một gói dữ liệu liên kết là MTU (Maximum Transmit Unit). Khi cần chuyển một gói dữ liệu IP có độ dài lớn hơn MTU của một mạng cụ thể, cần phải chia gói số liệu IP đó thành những gói IP nhỏ hơn để độ dài của nó nhỏ hơn hoặc bằng MTU gọi chung là mảnh (fragment). Trong phần tiêu đề của gói dữ liệu IP có thông tin về phân mảnh và xác định các mảnh có quan hệ phụ thuộc để hợp thành sau này.

Ví dụ Ethernet chỉ hỗ trợ các khung có độ dài tối đa là 1500 byte. Nếu muốn gửi một gói dữ liệu IP gồm 2000 byte qua Ethernet, phải chia thành hai gói nhỏ hơn, mỗi gói không quá giới hạn MTU của Ethernet.



Hình 16. Nguyên tắc phân mảnh gói dữ liệu

P dùng cờ MF (3 bit thấp của trường Flags trong phần đầu của gói IP) và trường Flagment offset của gói IP (đã bị phân đoạn) để định danh gói IP đó là một phân đoạn và vị trí của phân đoạn này trong gói IP gốc. Các gói cùng trong chuỗi phân mảnh đều có trường này giống nhau. Cờ MF bằng 1 nếu là gói đầu của chuỗi phân mảnh và 0 nếu là gói cuối của gói đã được phân mảnh.

Quá trình hợp nhất diễn ra ngược lại với quá trình phân mảnh. Khi IP nhận được một gói phân mảnh, nó giữ phân mảnh đó trong vùng đệm, cho đến khi nhận được hết các gói IP trong chuỗi phân mảnh có cùng trường định danh. Khi phân mảnh đầu tiên được nhận, IP khởi động một bộ đếm thời gian (giá trị

ngầm định là 15s). IP phải nhận hết các phân mảnh kế tiếp trước khi đồng hồ tắt. Nếu không IP phải huỷ tất cả các phân mảnh trong hàng đợi hiện thời có cùng trường định danh.

Khi IP nhận được hết các phân mảnh, nó thực hiện hợp nhất các gói phân mảnh thành các gói IP gốc và sau đó xử lý nó như một gói IP bình thường. IP thường chỉ thực hiện hợp nhất các gói tại hệ thống đích của gói.

I.5. Định tuyến IP

Có hai loại định tuyến:

- Định tuyến trực tiếp: Định tuyến trực tiếp là việc xác định đường nối giữa hai trạm làm việc trong cùng một mạng vật lý.

- Định tuyến không trực tiếp. Định tuyến không trực tiếp là việc xác định đường nối giữa hai trạm làm việc không nằm trong cùng một mạng vật lý và vì vậy, việc truyền tin giữa chúng phải được thực hiện thông qua các trạm trung gian là các gateway.

Để kiểm tra xem trạm đích có nằm trên cùng mạng vật lý với trạm nguồn hay không, người gửi phải tách lấy phần địa chỉ mạng trong phần địa chỉ IP. Nếu hai địa chỉ này có địa chỉ mạng giống nhau thì datagram sẽ được truyền đi trực tiếp; ngược lại phải xác định một gateway, thông qua gateway này chuyển tiếp các datagram.

Khi một trạm muốn gửi các gói dữ liệu đến một trạm khác thì nó phải đóng gói datagram vào một khung (frame) và gửi các frame này đến gateway gần nhất. Khi một frame đến một gateway, phần datagram đã được đóng gói sẽ được tách ra và IP routing sẽ chọn gateway tiếp dọc theo đường dẫn đến đích. Datagram sau đó lại được đóng gói vào một frame khác và gửi đến mạng vật lý để gửi đến gateway tiếp theo trên đường truyền và tiếp tục như thế cho đến khi datagram được truyền đến trạm đích.

Chiến lược định tuyến: Trong thuật ngữ truyền thống của TCP/IP chỉ có hai kiểu thiết bị, đó là các cổng truyền (gateway) và các trạm (host). Các cổng truyền có vai trò gửi các gói dữ liệu, còn các trạm thì không. Tuy nhiên khi một trạm được nối với nhiều mạng thì nó cũng có thể định hướng cho việc lưu chuyển các gói dữ liệu giữa các mạng và lúc này nó đóng vai trò hoàn toàn như một gateway.

khác thì nó cần được phân mảnh ra thành các gói nhỏ hơn, gọi là *fragment.* Quá trình này gọi là quá trình phân mảnh. Dạng của một *fragment* cũng giống như dạng của một gói dữ liệu thông thường. Từ thứ hai trong phần *header* chứa các thông tin để xác định mỗi *fragment* và cung cấp các thông tin để hợp nhất các fragment này lại thành các gói như ban đầu. Trường *identification* dùng để xác định *fragment* này là thuộc về gói dữ liệu nào.

I.6. Một số giao thức điều khiển

I.6.1. Giao thức ICMP

ICMP ((Internet Control Message Protocol) là một giao thức điều khiển của mức 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 bộ giao thức TCP/IP. Ví dụ:

- Điều khiển lưu lượng dữ liệu (Flow control): khi các gói dữ liệu đến quá nhanh, thiết bị đích hoặc thiết bị định tuyến ở giữa sẽ gửi một thông điệp ICMP trở lại thiết bị gửi, yêu cầu thiết bị gửi tạm thời ngừng việc gửi dữ liệu.

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

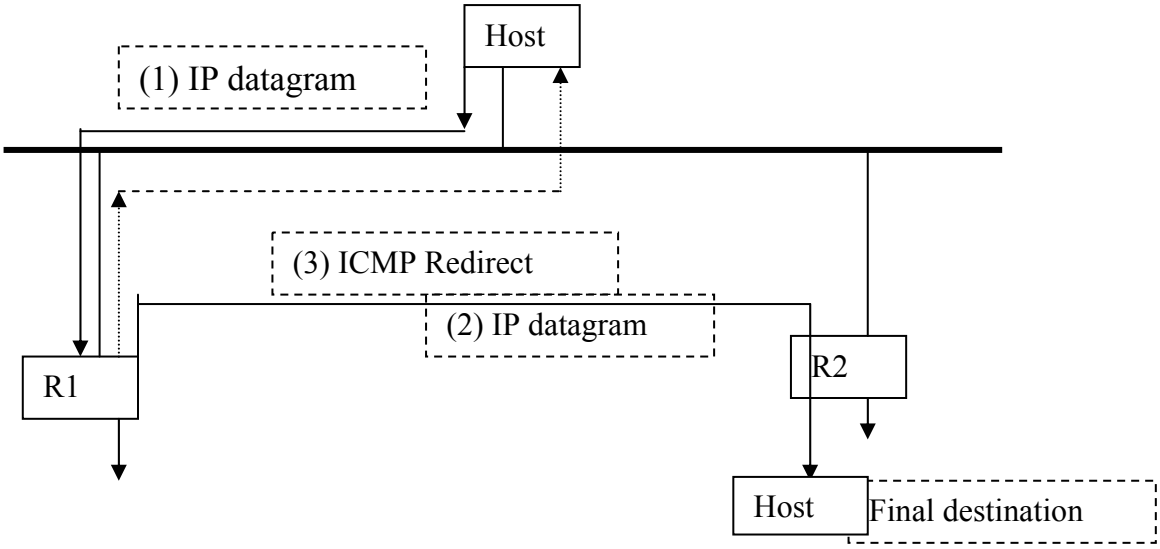
- Định hướng lại các tuyến đường: một thiết bị định tuyến sẽ gửi một thông điệp ICMP "định tuyến lại" (Redirect Router) để thông báo với một trạm là nên dùng thiết bị định tuyến khác để tới thiết bị đích. Thông điệp này có thể chỉ được dùng khi trạm nguồn ở trên cùng một mạng với cả hai thiết bị định tuyến.

- Kiểm tra các trạm ở xa: một trạm có thể gửi một thông điệp ICMP "Echo" để kiểm tra xem một trạm có hoạt động hay không.

Sau đây là mô tả một ứng dụng của giao thức ICMP thực hiện việc định tuyến lại (Redirect):

Ví dụ: giả sử host gửi một gói dữ liệu IP tới Router R1. Router R1 thực hiện việc quyết định tuyến vì R1 là router mặc định của host đó. R1 nhận gói dữ liệu và tìm trong bảng định tuyến và nó tìm thấy một tuyến tới R2. Khi R1 gửi gói dữ liệu tới R2 thì R1 phát hiện ra rằng nó đang gửi gói dữ liệu đó ra ngoài trên cùng một giao diện mà gói dữ liệu đó đã đến (là giao diện mạng

LAN mà cả host và hai Router nối đến). Lúc này R1 sẽ gửi một thông báo ICMP Redirect Error tới host, thông báo cho host nên gửi các gói dữ liệu tiếp theo đến R2 thì tốt hơn.



Tác dụng của ICMP Redirect là để cho mọt host với nhận biết tối thiểu về định tuyến xây dựng lên một bảng định tuyến tốt hơn theo thời gian. Host đó có thể bắt đầu với một tuyến mặc định (có thể R1 hoặc R2 như ví dụ trên) và bất kỳ lần nào tuyến mặc định này được dùng với host đó đến R2 thì nó sẽ được Router mặc định gửi thông báo Redirect để cho phép host đó cập nhật bảng định tuyến của nó một cách phù hợp hơn. Khuôn dạng của thông điệp ICMP redirect như sau:

0 7 8	15 16	31
type (5)	Code(0-3)	Checksum
Địa chỉ IP của Router mặc định		
IP header (gồm option) và 8 bytes đầu của gói dữ liệu IP nguồn		

Dạng thông điệp ICMP redirect

Có bốn loại thông báo ICMP redirect khác nhau với các giá trị mã (code) như bảng sau:

Code	Description
0	Redirect cho mạng
1	Redirect cho host
2	Redirect cho loại dịch vụ (TOS) và mạng
3	Redirect cho loại dịch vụ và host

Các loại định hướng lại của gói dữ liệu ICMP

Redirect chỉ xảy ra khi cả hai Router R1 và R2 cùng nằm trên một mạng với host nhận direct đó.

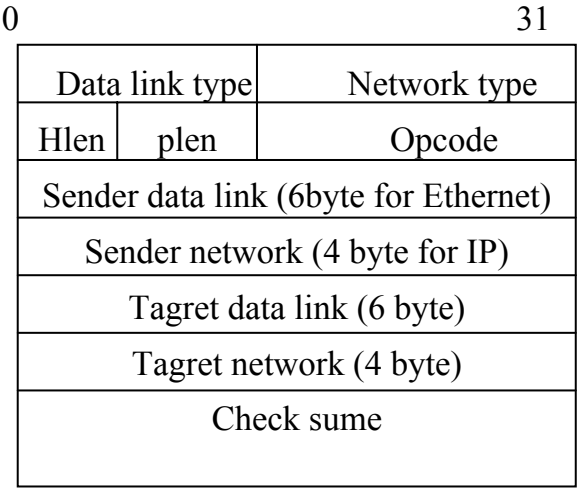
I.6.2. Giao thức ARP và giao thức RARP

Địa chỉ IP được dùng để định danh các host và mạng ở tầng mạng của mô hình OSI, chúng không phải là các địa chỉ vật lý (hay địa chỉ MAC) của các trạm đó trên một mạng cục bộ (Ethernet, Token Ring,...). Trên một mạng cục bộ hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau. Như vậy vấn đề đặt ra là phải thực hiện ánh xạ giữa địa chỉ IP (32 bits) và địa chỉ vật lý (48 bits) của một trạm. Giao thức ARP (Address Resolution Protocol) đã được xây dựng để chuyển đổi từ địa chỉ IP sang địa chỉ vật lý khi cần thiết. Ngược lại, giao thức RARP (Reverse Address Resolution Protocol) được dùng để chuyển đổi địa chỉ vật lý sang địa chỉ IP. Các giao thức ARP và RARP không phải là bộ phận của IP mà IP sẽ dùng đến chúng khi cần.

Giao thức ARP

Giao thức TCP/IP sử dụng ARP để tìm địa chỉ vật lý của trạm đích. Ví dụ khi cần gửi một gói dữ liệu IP cho một hệ thống khác trên cùng một mạng vật lý Ethernet, hệ thông gửi cần biết địa chỉ Ethernet của hệ thống đích để tầng liên kết dữ liệu xây dựng khung gói dữ liệu.

Thông thường, mỗi hệ thống lưu giữ và cập nhật bảng thích ứng địa chỉ IP-MAC tại chỗ (còn được gọi là bảng ARP cache). Bảng thích ứng địa chỉ được cập nhật bởi người quản trị hệ thống hoặc tự động bởi giao thức ARP sau mỗi lần ánh xạ được một địa chỉ thích ứng mới. Khuôn dạng của gói dữ liệu ARP được mô tả trong hình

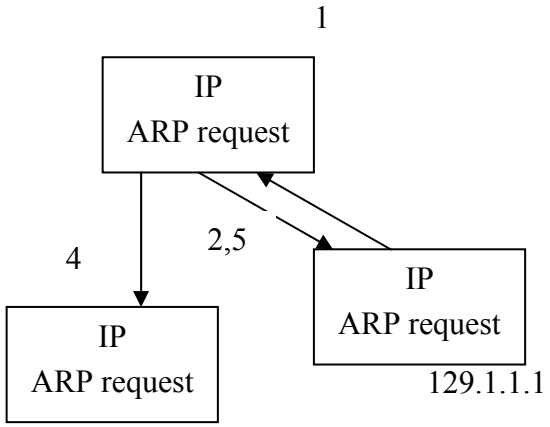


Mô tả khuôn dạng của gói ARP

- Data link type: cho biết loại công nghệ mạng mức liên kết (ví dụ đối với mạng Ethernet trường này có giá trị 01).
- Network type: cho biết loại mạng (ví dụ đối với mạng IPv4, trường này có giá trị 0800_{16}).
- Hlen (hardware length): độ dài địa chỉ mức liên kết (6 byte).
- Plen (Protocol length): cho biết độ dài địa chỉ mạng (4 byte)
- Opcode (operation code): mã lệnh yêu cầu: ; mã lệnh trả lời .
- Sender data link: địa chỉ mức liên kết của thiết bị phát gói dữ liệu này.
- Sender network : địa chỉ IP của thiết bị phát.
- Tagret data link: trong yêu cầu đây là địa chỉ mức liên kết cần tìm (thông thường được điền 0 bởi thiết bị gửi yêu cầu); trong trả lời đây là địa chỉ mức liên kết của thiết bị gửi yêu cầu.
- Tagret network : trong yêu cầu đây là địa chỉ IP mà địa chỉ mức liên kết tương ứng cần tìm; trong trả lời đây là địa chỉ IP của thiết bị gửi yêu cầu.

Mỗi khi cần tìm thích ứng địa chỉ IP - MAC, có thể tìm địa chỉ MAC tương ứng với địa IP đó trước tiên trong bảng địa chỉ IP - MAC ở mỗi hệ

thống. Nếu không tìm thấy, có thể sử dụng giao thức ARP để làm việc này. Trạm làm việc gửi yêu cầu ARP (ARP_Request) tìm thích ứng địa chỉ IP - MAC đến máy phục vụ ARP - server. Máy phục vụ ARP tìm trong bảng thích ứng 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. Tóm lại tiến trình của ARP được mô tả như sau



Tiến trình ARP

1. IP yêu cầu địa chỉ MAC.
2. Tìm kiếm trong bảng ARP.
3. Nếu tìm thấy sẽ trả lại địa chỉ MAC.
4. Nếu không tìm thấy, tạo gói ARP yêu cầu và gửi tới tất cả các trạm.
5. Tuỳ theo gói dữ liệu trả lời, ARP cập nhật vào bảng ARP và gửi địa chỉ MAC đó cho IP.

Giao thức RARP

Reverse ARP (Reverse Address Resolution Protocol) là giao thức giải thích ứng địa chỉ AMC - IP. Quá trình này ngược lại với quá trình giải thích ứng địa chỉ IP - MAC mô tả ở trên, nghĩa là cho trước địa chỉ mức liên kết, tìm địa chỉ IP tương ứng.

I.2. Giao thức lớp chuyển tải (Transport Layer)

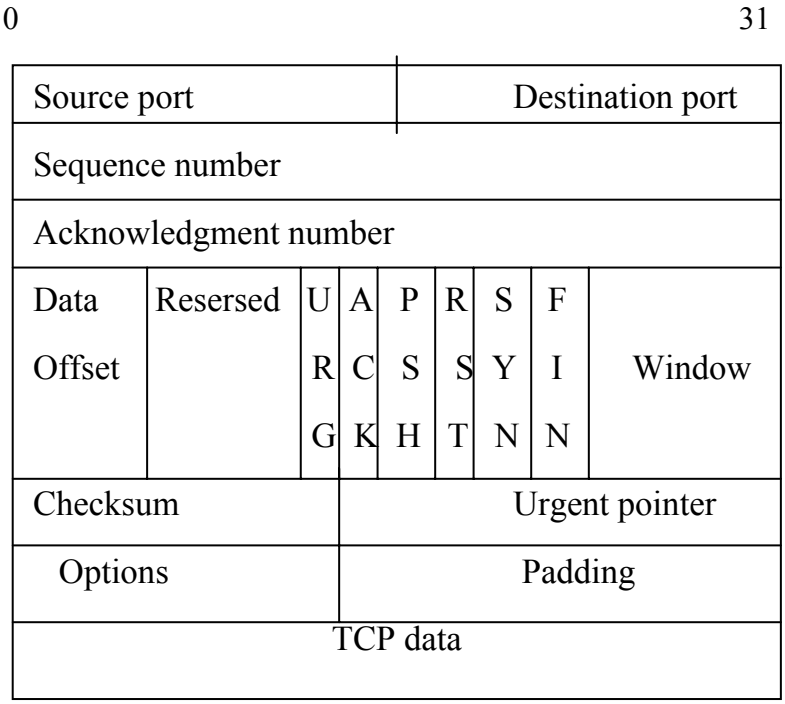
I.2.1. Giao thức TCP

TCP (Transmission Control Protocol) là một giao thức "có liên kết" (connection - oriented), nghĩa là cần thiết lập liên kết (logic), giữa một cặp thực thể TCP trước khi chúng trao đổi dữ liệu với nhau.

TCP cung cấp khả năng truyền dữ liệu một cách an toàn giữa các máy trạm trong hệ thống các mạng. Nó cung cấp thêm các chức năng nhằm kiểm tra tính chính xác của dữ liệu khi đến và bao gồm cả việc gửi lại dữ liệu khi có lỗi xảy ra. TCP cung cấp các chức năng chính sau:

1. Thiết lập, duy trì, kết thúc liên kết giữa hai quá trình.
2. Phân phát gói tin một cách tin cậy.
3. Đánh số thứ tự (sequencing) các gói dữ liệu nhằm truyền dữ liệu một cách tin cậy.
4. Cho phép điều khiển lỗi.
5. Cung cấp khả năng đa kết nối với các quá trình khác nhau giữa trạm nguồn và trạm đích nhất định thông qua việc sử dụng các cổng.
6. Truyền dữ liệu sử dụng cơ chế song công (full-duplex).

I.2.2 Cấu trúc gói dữ liệu TCP



Khuôn dạng của TCP segment

- Source port (16 bits) : số hiệu cổng của trạm nguồn

- Destination port (16 bits) : số hiệu cổng của trạm đích

- Sequence Number (32 bits): số hiệu của 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) và byte dữ liệu đầu tiên là ISN +1.

- Acknowlegment: vị trí tương đối của byte cuối cùng đã nhận đúng bởi thực thể gửi gói ACK cộng thêm 1. Giá trị của trường này còn được gọi là số tuần tự thu. Trường này được kiểm tra chỉ khi bit ACK=1.

- Data offset (4 bits) : số tượng từ 32 bit trong TCP header. Tham số này chỉ ra vị trí bắt đầu của vùng dữ liệu

- Reserved (6 bits) : dành để dùng trong tương lai. Phải được thiết lập là 0.

- Control bits : các bit điều khiển

  - URG : vùng con trỏ khẩn (Urgent Pointer) có hiệu lực.

  - ACK: vùng báo nhận (ACK number) có hiệu lực.

- PSH : chức năng Push. PSH=1 thực thể nhận phải chuyển dữ liệu này cho ứng dụng tức thời.

  - RST : thiết lập lại (reset) kết nối.

  - SYN : đồng bộ hoá các số hiệu tuần tự, dùng để thiết lập kết nối TCP.

  - FIN : thông báo thực thể gửi đã kết thúc gửi dữ liệu.

- Window (16 bits): cấp phát credit để kiểm soát luồng dữ liệu (cơ chế của sổ). Đây chính là số lượng các byte dữ liệu, bắt đầu từ byte được chỉ ra trong vùng ACK number, mà trạm nguồn đã sẵn sàng để nhận

- Checksum (16 bits) : mã kiểm soát lỗi (theo phương pháp CRC) cho toàn bộ segment (header + data)

- Urgent pointer (16 bits) : con trỏ này trỏ tới số hiệu tuần tự của byte đi theo sau 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

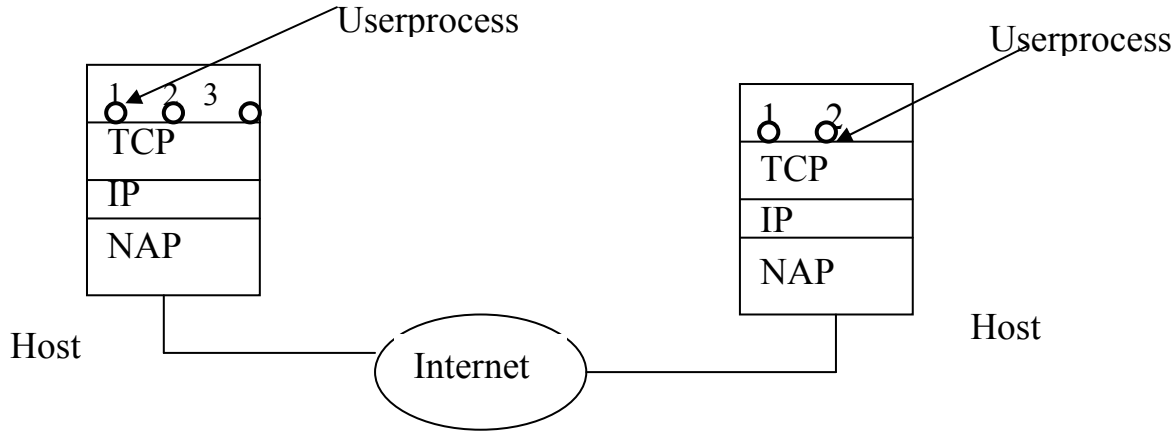
- Options (độ dài thay đổi): khai báo các option của TCP, trong đó có độ dài tối đa của vùng TCP data trong một segment

- Padding (độ dài thay đổi) : phần chèn thêm vào header để bảo đảm phần header luôn kết thúc ở một mốc 32 bits. Phần thêm này gồm toàn số 0.

- TCP data (độ dài thay đổi) : chứa dữ liệu của tầng trên, có độ dài tối đa ngầm định là 536 bytes. Giá trị này có thể điều chỉnh bằng cách khai báo trong vùng options.

Một tiến trình ứng dụng trong một host truy nhập vào các dịch vụ của TCP cung cấp thông qua một cổng (port) như sau:

Một cổng kết hợp với một địa chỉ IP tạo thành một socket duy nhất trong liên mạng. TCP được cung cấp nhờ một liên kết logic giữa một cặp socket. Một socket có thể tham gia nhiều liên kết với các socket ở xa khác nhau. Trước khi truyền dữ liệu giữa hai trạm cần phải thiết lập một liên kết TCP giữa chúng và khi kết thúc phiên truyền dữ liệu thì liên kết đó sẽ được giải phóng. Cũng giống như ở các giao thức khác, các thực thể ở tầng trên sử dụng TCP thông qua các hàm dịch vụ nguyên thuỷ (service primitives), hay còn gọi là các lời gọi hàm (function call).



NAP: Network Access Protocol

Cổng truy nhập dịch vụ TCP

I.2.3. Thiết lập và kết thúc kết nối TCP

Thiết lập kết nối

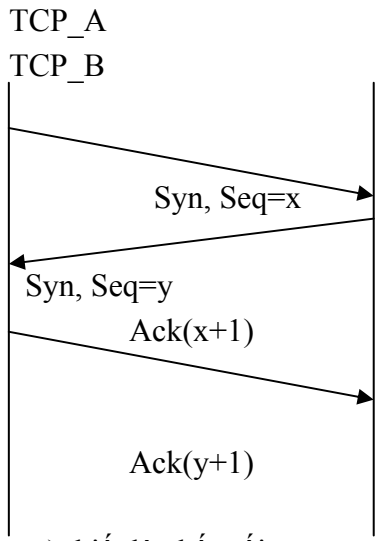
Thiết lập kết nối TCP được thực hiện trên cơ sở phương thức bắt tay ba bước (Tree - way Handsake) hình 2.11. Yêu cầu kết nối luôn được tiến trình trạm khởi tạo, bằng cách gửi một gói TCP với cờ SYN=1 và chứa giá trị khởi

tạo số tuần tự ISN của client. Giá trị ISN này là một số 4 byte không dấu và được tăng mỗi khi kết nối được yêu cầu (giá trị này quay về 0 khi nó tới giá trị 2^{32}). Trong thông điệp SYN này còn chứa số hiệu cổng TCP của phần mềm dịch vụ mà tiến trình trạm muốn kết nối (bước 1).

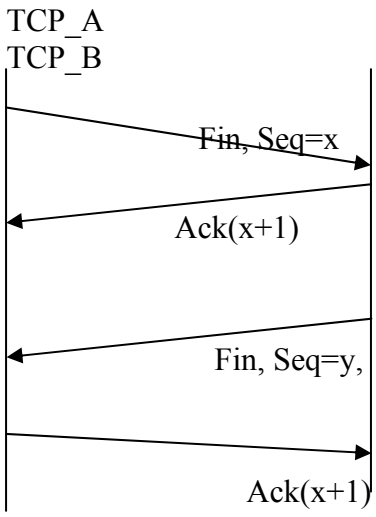
Mỗi thực thể kết nối TCP đều có một giá trị ISN mới số này được tăng theo thời gian. Vì một kết nối TCP có cùng số hiệu cổng và cùng địa chỉ IP được dùng lại nhiều lần, do đó việc thay đổi giá trị INS ngăn không cho các kết nối dùng lại các dữ liệu đã cũ (stale) vẫn còn được truyền từ một kết nối cũ và có cùng một địa chỉ kết nối.

Khi thực thể TCP của phần mềm dịch vụ nhận được thông điệp SYN, nó gửi lại gói SYN cùng giá trị ISN của nó và đặt cờ ACK=1 trong trường hợp sẵn sàng nhận kết nối. Thông điệp này còn chứa giá trị ISN của tiến trình trạm trong trường hợp số tuần tự thu để báo rằng thực thể dịch vụ đã nhận được giá trị ISN của tiến trình trạm (bước 2).

Tiến trình trạm trả lời lại gói SYN của thực thể dịch vụ bằng một thông báo trả lời ACK cuối cùng. Bằng cách này, các thực thể TCP trao đổi một cách tin cậy các giá trị ISN của nhau và có thể bắt đầu trao đổi dữ liệu. Không có thông điệp nào trong ba bước trên chứa bất kỳ dữ liệu gì; tất cả thông tin trao đổi đều nằm trong phần tiêu đề của thông điệp TCP (bước 3).



a) thiết lập kết nối



b) Kết thúc kết nối

Quá trình kết nối theo 3 bước

Kết thúc kết nối

Khi có nhu cầu kết thúc kết nối, thực thể TCP, ví dụ cụ thể A gửi yêu cầu kết thúc kết nối với FIN=1. Vì kết nối TCP là song công (full-duplex) nên mặc dù nhận được yêu cầu kết thúc kết nối của A (A thông báo hết số liệu gửi) thực thể B vẫn có thể tiếp tục truyền số liệu cho đến khi B không còn số liệu để gửi và thông báo cho A bằng yêu cầu kết thúc kết nối với FIN=1 của mình. Khi thực thể TCP đã nhận được thông điệp FIN và sau khi đã gửi thông điệp FIN của chính mình, kết nối TCP thực sụ kết thúc.

PHẦN II
QUẢN TRỊ MẠNG

Quản trị mạng lưới (network administration) được định nghĩa là các công việc quản lý mạng lưới bao gồm cung cấp các dịch vụ hỗ trợ, đảm bảo mạng lưới hoạt động hiệu quả, đảm bảo chất lượng mạng lưới cung cấp đúng như chỉ tiêu định ra.

Quản trị hệ thống (system administration) được định nghĩa là các công việc cung cấp các dịch vụ hỗ trợ, đảm bảo sự tin cậy, nâng cao hiệu quả hoạt động của hệ thống, và đảm bảo chất lượng dịch vụ cung cấp trên hệ thống đúng như chỉ tiêu định ra.

Một định nghĩa khái quát về công tác quản trị mạng là rất khó vì tính bao hàm rộng của nó. Quản trị mạng theo nghĩa mạng máy tính có thể được hiểu khái quát là tập bao gồm của các công tác quản trị mạng lưới và quản trị hệ thống.

Có thể khái quát công tác quản trị mạng bao gồm các công việc sau:

Quản trị cấu hình, tài nguyên mạng : Bao gồm các công tác quản lý kiểm soát cấu hình, quản lý các tài nguyên cấp phát cho các đối tượng sử dụng khác nhau. Có thể tham khảo các công việc quản trị cụ thể trong các tài liệu, giáo trình về quản trị hệ thống windows, linux, novell netware ...

Quản trị người dùng, dịch vụ mạng: Bao gồm các công tác quản lý người sử dụng trên hệ thống, trên mạng lưới và đảm bảo dịch vụ cung cấp có độ tin cậy cao, chất lượng đảm bảo theo đúng các chỉ tiêu đề ra. Có thể tham khảo các tài liệu, giáo trình quản trị hệ thống windows, novell netware, linux, unix, quản trị dịch vụ cơ bản thư tín điện tử, DNS...

Quản trị hiệu năng, hoạt động mạng : Bao gồm các công tác quản lý, giám sát hoạt động mạng lưới, đảm bảo các thiết bị, hệ thống, dịch vụ trên mạng hoạt động ổn định, hiệu quả. Các công tác quản lý, giám sát hoạt động của mạng lưới cho phép người quản trị tổng hợp, dự báo sự phát triển mạng lưới, dịch vụ, các điểm yếu, điểm mạnh của toàn mạng, các hệ thống và dịch vụ

đồng thời giúp khai thác toàn bộ hệ thống mạng với hiệu suất cao nhất. Có thể tham khảo các tài liệu, giáo trình về các hệ thống quản trị mạng NMS, HP Openview, Sunet Manager, hay các giáo trình nâng cao hiệu năng hoạt động của hệ thống (performance tuning).

Quản trị an ninh, an toàn mạng: Bao gồm các công tác quản lý, giám sát mạng lưới, các hệ thống để đảm bảo phòng tránh các truy nhập trái phép, có tính phá hoại các hệ thống, dịch vụ, hoặc mục tiêu đánh cắp thông tin quan trọng của các tổ chức, công ty hay thay đổi nội dung cung cấp lên mạng với dụng ý xấu. Việc phòng chống, ngăn chặn sự lây lan của các loại virus máy tính, các phương thức tấn công ví dụ như DoS làm tê liệt hoạt động mạng hay dịch vụ cũng là một phần cực kỳ quan trọng của công tác quản trị an ninh, an toàn mạng. Đặc biệt, hiện nay khi nhu cầu kết nối ra mạng Internet trở nên thiết yếu thì các công tác đảm bảo an ninh, an toàn được đặt lên hàng đầu, đặc biệt là với các cơ quan cần bảo mật nội dung thông tin cao độ (nhà băng, các cơ quan lưu trữ, các các báo điện tử, tập đoàn kinh tế mũi nhọn...).

Trong phần 2 của giáo trình này sẽ tập trung nghiên cứu sâu về một số kiến thức, kỹ năng cơ bản và thông dụng nhất về quản trị mạng. Tuy nhiên, các nội dung trình bày tại phần 2 sẽ không bao hàm hết được các nội dung đã khái quát ở trên do sự phức tạp phong phú của bản thân mỗi nội dung cũng như giới hạn về thời gian biên soạn. Với mục tiêu cung cấp các kỹ năng phổ biến nhất giúp cho các học viên tiếp cận nhanh chóng vào công tác quản trị mạng để đảm đương được nhiệm vụ cơ quan, công ty giao cho. Phần 2 của giáo trình sẽ bao gồm :

- Tổng quan về bộ định tuyến trên mạng
- Hệ thống tên miền DNS
- Dịch vụ truy cập từ xa và dịch vụ proxy
- Firewall và bảo mật hệ thống

Học viên cũng có thể tham khảo bổ sung thêm kiến thức về quản trị mạng với các giáo trình về mạng cục bộ, giáo trình về thư tín điện tử, giáo trình về các hệ điều hành Windows, Linux, Unix là các nội dung biên soạn trong bộ các giáo trình phục vụ đào tạo cho đề án 112.

Chương 3 : Tổng quan về bộ định tuyến

Chương ba cung cấp các kiến thức cơ bản về bộ định tuyến trên mạng và các bộ chuyển mạch lớp 3. Các thiết bị này là một phần thiết yếu của mạng máy tính hiện đại và là các thiết bị hạ tầng cốt lõi. Các minh họa tường tận về cấu trúc của các sản phẩm hãng Cisco sẽ giúp học viên nắm vững các lý thuyết hệ thống đặc biệt là lý thuyết định tuyến. Phần nội dung cũng bổ sung các kỹ năng cấu hình hoạt động của thiết bị trên các giao thức mạng WAN khác nhau như Frame Relay, X.25...

Chương ba đòi hỏi các học viên cần có các kiến thức sơ khởi về các giao thức trên mạng diện rộng như Frame Relay, x.25..., các kiến thức về địa chỉ lớp 2, lớp 3.

I. Lý thuyết về bộ định tuyến

I.1. Tổng quan về bộ định tuyến

Bộ định tuyến là thiết bị được sử dụng trên mạng để thực thi các hoạt động xử lý truyền tải thông tin trên mạng. Có thể xem bộ định tuyến là một thiết bị máy tính được thiết kế đặc biệt để đảm đương được vai trò xử lý truyền tải thông tin trên mạng của nó và do đó nó cũng bao gồm các CPU, trái tim của mọi hoạt động, bộ nhớ ROM, RAM, các giao tiếp, các bus dữ liệu, hệ điều hành v.v...

Chức năng của bộ định tuyến là định hướng cho các gói tin được truyền tải qua bộ định tuyến. Trên cơ sở các thuật toán định tuyến, thông tin cấu hình và chuyển giao, các bộ định tuyến sẽ quyết định hướng đi tốt nhất cho các gói tin được truyền tải qua nó. Bộ định tuyến còn có vai trò để xử lý các nhu cầu truyền tải và chuyển đổi giao thức khác.

Vai trò của bộ định tuyến trên mạng là đảm bảo các kết nối liên thông giữa các mạng với nhau, tính toán và trao đổi các thông tin liên mạng làm căn cứ cho các bộ định tuyến ra các quyết định truyền tải thông tin phù hợp với cấu hình thực tế của mạng. Bộ định tuyến làm việc với nhiều công nghệ đấu nối mạng diện rộng khác nhau như FRAME RELAY, X.25, ATM, SONET, ISDN, xDSL... đảm bảo các nhu cầu kết nối mạng theo nhiều các công nghệ và độ

chuẩn mực khác nhau mà nếu thiếu vai trò của bộ định tuyến thì không thể thực hiện được.

I.2. Các chức năng chính của bộ định tuyến, tham chiếu mô hình OSI

Mô hình OSI đã được học ở chương 1 gồm 7 lớp trong đó bao gồm

- 3 lớp thuộc về các lớp ứng dụng
  - lớp ứng dụng
  - lớp trình bày
  - lớp phiên
- 4 lớp thuộc về các lớp truyền thông
  - lớp vận chuyển
  - lớp mạng
  - lớp liên kết dữ liệu
  - lớp vật lý

Đối với các lớp truyền thông:

- Lớp vận chuyển: phân chia / tái thiết dữ liệu thành các dòng chảy dữ liệu. Các chức năng chính bao gồm điều khiển dòng dữ liệu, đa truy nhập, quản lý các mạch ảo, phát hiện và sửa lỗi. TCP, UDP là hai giao thức thuộc họ giao thức Internet (TCP/IP) thuộc về lớp vận chuyển này.

- Lớp mạng: cung cấp hoạt động định tuyến và các chức năng liên quan khác cho phép kết hợp các môi trường liên kết dữ liệu khác nhau lại với nhau cùng tạo nên mạng thống nhất. Các giao thức định tuyến hoạt đông trong lớp mạng này.

- Lớp liên kết dữ liệu: cung cấp khả năng truyền tải dữ liệu từ qua môi trường truyền dẫn vật lý. Mỗi đặc tả khác nhau của lớp liên kết dữ liệu sẽ có các định nghĩa khác nhau về giao thức và các chuẩn mực kết nối đảm bảo truyền tải dữ liệu.

- Lớp vật lý: định nghĩa các thuộc tính điện, các chức năng, thường trình dùng để kết nối các thiết bị mạng ở mức vật lý. Một số các thuộc tính được định nghĩa như mức điện áp, đồng bộ, tốc độ truyền tải vật lý, khoảng cách truyền tải cho phép...

Trong môi trường truyền thông, các thiết bị truyền thông giao tiếp với nhau thông qua các họ giao thức truyền thông khác nhau được xây dựng dựa trên các mô hình chuẩn OSI nhằm đảm bảo tính tương thích và mở rộng. Các giao thức truyền thông thường được chia vào một trong bốn nhóm: các giao thức mạng cục bộ, các giao thức mạng diện rộng, giao thức mạng và các giao thức định tuyến. *Giao thức mạng cục bộ* hoạt động trên lớp vật lý và lớp liên kết dữ liệu. *Giao thức mạng diện rộng* hoạt động trên 3 lớp dưới cùng trong mô hình OSI. *Giao thức định tuyến* là giao thức lớp mạng và đảm bảo cho các hoạt động định tuyến và truyền tải dữ liệu. *Giao thức mạng* là các họ các giao thức cho phép giao tiếp với lớp ứng dụng.

Vai trò của bộ định tuyến trong môi trường truyền thông là đảm bảo cho các kết nối giữa các mạng khác nhau với nhiều giao thức mạng, sử dụng các công nghệ truyền dẫn khác nhau.

Chức năng chính của bộ định tuyến là:

- Định tuyến (routing)
- Chuyển mạch các gói tin (packet switching)

Định tuyến là chức năng đảm bảo gói tin được chuyển chính xác tới địa chỉ cần đến. *Chuyển mạch các gói tin* là chức năng chuyển mạch số liệu, truyền tải các gói tin theo hướng đã định trên cơ sở các định tuyến được đặt ra. Như vậy, trên mỗi bộ định tuyến, ta phải xây dựng một bảng định tuyến, trên đó chỉ rõ địa chỉ cần đến và đường đi cho nó. Bộ định tuyến dựa vào địa chỉ của gói tin kết hợp với bảng định tuyến để chuyển gói tin đi đúng đến đích. Các gói tin không có đúng địa chỉ đích trên bảng định tuyến sẽ bị huỷ.

Chức năng đầu tiên của bộ định tuyến là chức năng định tuyến như tên gọi của nó cũng là chức năng chính của bộ định tuyến làm việc với các *giao thức định tuyến.* Bộ định tuyến được xếp vào các thiết bị mạng làm việc ở lớp 3, lớp mạng.

Bảng 3-1:Tương đương chức năng thiết bị trong mô hình OSI

Lớp 3	Lớp mạng	
Lớp 2	Lớp liên kết dữ liệu	
Lớp 1	Lớp vật lý	

Chức năng khác của bộ định tuyến là cho phép sử dụng các phương thức truyền thông khác nhau để đấu nối diện rộng. Chức năng kết nối diện rộng WAN của bộ định tuyến là không thể thiếu để đảm bảo vai trò kết nối truyền thông giữa các mạng với nhau. Chức năng kết nối mạng cục bộ, bất kỳ bộ định tuyến nào cũng cần có chức năng này để đảm bảo kết nối đến vùng dịch vụ của mạng. Bộ định tuyến còn có các chức năng đảm bảo hoạt động cho các giao thức mạng mà nó quản lý.

I.3. Cấu hình cơ bản và chức năng của các bộ phận của bộ định tuyến

Như đã nói ở phần trước, bộ định tuyến là một thiết bị máy tính được thiết kế đặc biệt để đảm đương được vai trò xử lý truyền tải thông tin trên mạng. Nó được thiết kế bao gồm các phần tử không thể thiếu như CPU, bộ nhớ ROM, RAM, các bus dữ liệu, hệ điều hành. Các phần tử khác tùy theo nhu cầu sử dụng có thể có hoặc không bao gồm các giao tiếp, các module và các tính năng đặc biệt của hệ điều hành.

CPU: điều khiển mọi hoạt động của bộ định tuyến trên cơ sở các hệ thống chương trình thực thi của hệ điều hành.

ROM: chứa các chương trình tự động kiểm tra và có thể có thành phần cơ bản nhất sao cho bộ định tuyến có thể thực thi được một số hoạt động tối thiểu ngay cả khi không có hệ điều hành hay hệ điều hành bị hỏng.

RAM: giữ các bảng định tuyến, các vùng đệm, tập tin cấu hình khi chạy, các thông số đảm bảo hoạt động của bộ định tuyến khác.

Flash: là thiết bị nhớ / lưu trữ có khả năng xoá và ghi được, không mất dữ liệu khi cắt nguồn. Hệ điều hành của bộ định tuyến được chứa ở đây. Tùy

thuộc các bộ định tuyến khác nhau, hệ điều hành sẽ được chạy trực tiếp từ Flash hay được giãn ra RAM trước khi chạy. Tập tin cấu hình cũng có thể được lưu trữ trong Flash.

Hệ điều hành: đảm đương hoạt động của bộ định tuyến. Hệ điều hành của các bộ định tuyến khác nhau có các chức năng khác nhau và thường được thiết kế khác nhau. Mỗi bộ định tuyến có thể chạy rất nhiều hệ điều hành khác nhau tùy thuộc vào nhu cầu sử dụng cụ thể, các chức năng cần thiết phải có của bộ định tuyến và các thành phần phần cứng có trong bộ định tuyến. Các thành phần phần cứng mới yêu cầu có sự nâng cấp về hệ điều hành. Các tính năng đặc biệt được cung cấp trong các bản nâng cấp riêng của hệ điều hành.

Các giao tiếp: bộ định tuyến có nhiều các giao tiếp trong đó chủ yếu bao gồm

- Giao tiếp WAN: đảm bảo cho các kết nối diện rộng thông qua các phương thức truyền thông khác nhau như leased-line, Frame Relay, X.25, ISDN, ATM, xDSL ... Các giao tiếp WAN cho phép bộ định tuyến kết nối theo nhiều các giao diện và tốc độ khác nhau: V.35, X.21, G.703, E1, E3, cáp quang v.v...
- Giao tiếp LAN: đảm bảo cho các kết nối mạng cục bộ, kết nối đến các vùng cung cấp dịch vụ trên mạng. Các giao tiếp LAN thông dụng: Ethernet, FastEthernet, GigaEthernet, cáp quang.

II. Giới thiệu về bộ định tuyến Cisco

II.1. Giới thiệu bộ định tuyến Cisco

Sơ lược về bộ định tuyến

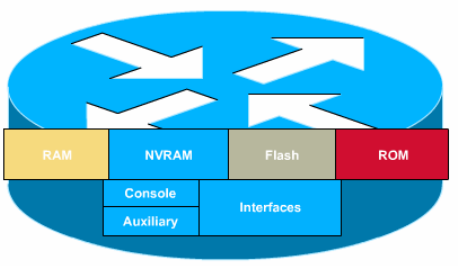
Bộ định tuyến Cisco bao gồm nhiều nền tảng phần cứng khác nhau được thiết kế xây dựng cho phù hợp với nhu cầu và mục đích sử dụng của các giải pháp khác nhau.

Các chức năng xử lý hoạt động của bộ định tuyến Cisco dựa trên nền tảng cốt lõi là hệ điều hành IOS.

Tuỳ theo các nhu cầu cụ thể mà một bộ định tuyến Cisco sẽ cần một IOS có các tính năng phù hợp. IOS có nhiều phiên bản khác nhau, một số loại phần

cứng mới được phát triển chỉ có thể được hỗ trợ bởi các IOS phiên bản mới nhất.

Các thành phần cấu thành bộ định tuyến



Hình 3-1:Các thành phần của bộ định tuyến Cisco

- RAM: Giữ bảng định tuyến, ARP Cache, fast-switching cache, packet buffer, và là nơi chạy các file cấu hình cho bộ định tuyến. Đây chính là nơi lưu giữ file Running-Config, chứa cấu hình đang hoạt động của Router. Khi ngừng cấp nguồn cho bộ định tuyến, bộ nhớ này sẽ tự động giải phóng. Tất cả các thông tin trong file Running-Config sẽ bị mất hoàn toàn.

- NVRAM: non-volatile RAM, là nơi giữ startup/backup configure, không bị mất thông tin khi mất nguồn vào. File Startup-Config được lưu trong này để đảm bảo khi khởi động lại, cấu hình của bộ định tuyến sẽ được tự động đưa về trạng thái đã lưu giữ trong file. Vì vậy, phải thường xuyên lưu file Running-Config thành file Startup-Config.

- Flash: Là ROM có khả năng xoá, và ghi đọc. Là nơi chứa hệ điều hành IOS của bộ định tuyến. Khi khởi động, bộ định tuyến sẽ tự đọc ROM để nạp IOS trước khi nạp file Startup-Config trong NVRAM.

- ROM: Chứa các chng trình tự động kiểm tra.

- Cổng Console: Được sử dụng để cấu hình trực tiếp bộ định tuyến. Tốc độ dữ liệu dùng cho cấu hình bằng máy tính qua cổng COM là 9600b/s. Giao diện ra của cổng này là RJ45 female.

- Cổng AUX: Được sử dụng để quản lý và cấu hình cho bộ định tuyến thông qua modem dự phòng cho cổng Console. Giao diện ra của cổng này cũng là RJ45 female.
- Các giao diện:
    - Cổng Ethernet / Fast Ethernet
    - Cổng Serial
    - Cổng ASYNC ...

II.2. Một số tính năng ưu việt của bộ định tuyến Cisco

- Có khả năng tích hợp nhiều chức năng xử lý trên cùng một sản phẩm với việc sử dụng các module chức năng thích hợp và IOS thích hợp.

- Dễ dàng trong việc nâng cấp bộ định tuyến Cisco cả về phần mềm lẫn phần cứng do đó dễ dàng đáp ứng các nhu cầu thay đổi, mở rộng mạng, đáp ứng các nhu cầu phát triển và ứng dụng công nghệ mới.

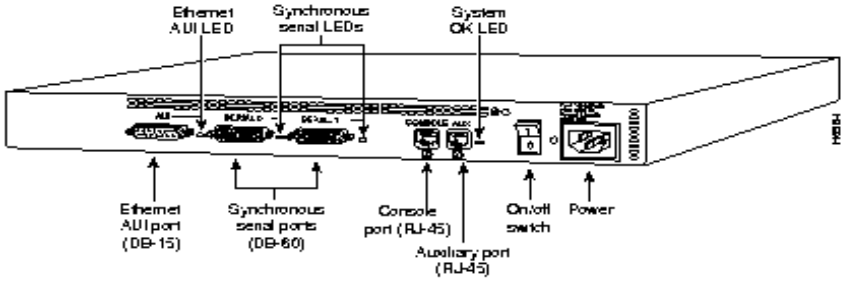
- Tương thích và dễ dàng mở rộng cho các nhu cầu về đa dịch vụ ngày càng gia tăng trên.

- Tính bền vững, an toàn và bảo mật.

II.3. Một số bộ định tuyến Cisco thông dụng

Bộ định tuyến Cisco 2500

- Bộ định tuyến Cisco 2509
- 01 cổng console, 01 AUX
- 02 cổng serial tốc độ tới 2Mbps: kết nối leased-line, X.25, Frame Relay...
- 01 Ethernet tốc độ 10Mbps giao diện AUI: cần thiết có đầu chuyển RJ45/AUI khi kết nối vào các mạng switch/hub thông thường.



Hình 3-2: Bộ định tuyến Cisco 2501

- 01 cổng Async cho phép kết nối đến 08 modem V34/V90. Sử dụng môt cáp kết nối Octal để kết nối các modem đến bộ định tuyến.

- Bộ định tuyến Cisco 2501

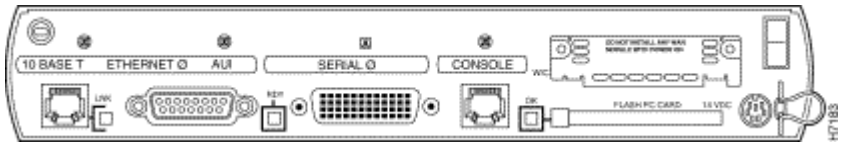
- 01 cổng console, 01 AUX

- 02 cổng serial tốc độ tới 2Mbps: kết nối leased-line, X.25, Frame Relay...

- 01 Ethernet tốc độ 10Mbps giao diện AUI: cần thiết có đầu chuyển RJ45/AUI khi kết nối vào các mạng switch/hub thông thường

Cisco đã ngừng sản xuất các bộ định tuyến Cisco dòng 2500.

Bộ định tuyến Cisco 1600



Hình 3-3: Bộ định tuyến Cisco 1601

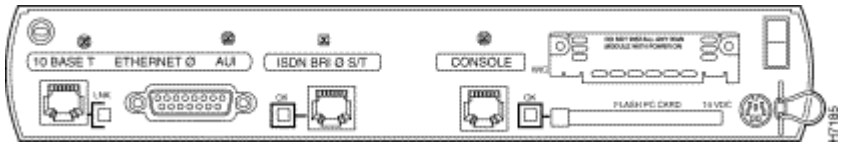
- Bộ định tuyến Cisco 1601

- 01 cổng console

- 01 cổng serial tốc độ tới 2Mbps: kết nối leased-line, X.25, Frame Relay...

- 01 Ethernet tốc độ 10Mbps giao diện AUI và RJ48 (Female Socket for RJ45 connector)

- 01 serial slot: có thể sử dụng cho cổng Serial thứ 2, card ISDN BRI



Hình 3-4: Bộ định tuyến Cisco 1603

- Bộ định tuyến Cisco 1603

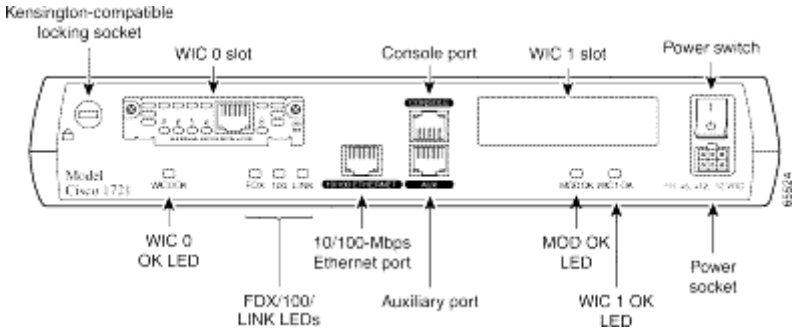
- 01 cổng console

- 01 cổng ISDN BRI giao diện S/T: kết nối ISDN tốc độ 2B+D, khi sử dụng ở Việt nam cần có thêm một bộ tiếp hợp NT1 để đấu nối vào mạng ISDN.

- 01 Ethernet tốc độ 10Mbps giao diện AUI và RJ48 (Female Socket for RJ45 connector)

- 01 serial slot: có thể sử dụng cho cổng Serial, card ISDN BRI

Bộ định tuyến Cisco 1700



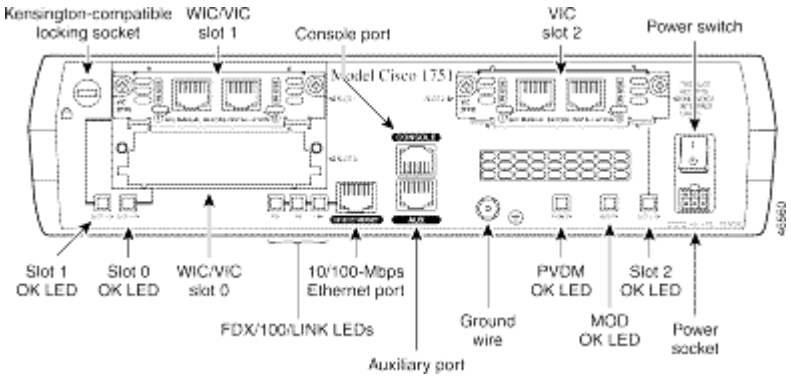
Hình 3-5: Bộ định tuyến Cisco 1721

- Bộ định tuyến Cisco 1721

- 01 cổng console, 01 AUX

- 01 FastEthernet tốc độ 10/100Mbps giao diện RJ48 (Female Socket for RJ45 connector)

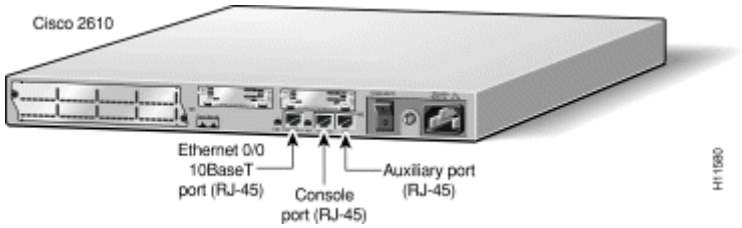
- 02 WAN slot: có thể sử dụng cho cổng Serial, card ISDN BRI...



Hình 3-6: Bộ định tuyến Cisco 1751

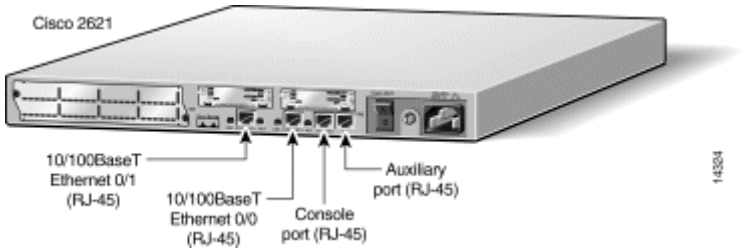
- Bộ định tuyến Cisco 1751
- 01 cổng console, 01 AUX
- 01 FastEthernet tốc độ 10/100Mbps giao diện RJ48 (Female Socket for RJ45 connector)
- 02 WAN slot: có thể sử dụng cho cổng Serial, card ISDN BRI...
- 01 Voice slot: chỉ cho phép cắm các card voice

Bộ định tuyến Cisco 2600



Hình 3-7: Bộ định tuyến Cisco 2610

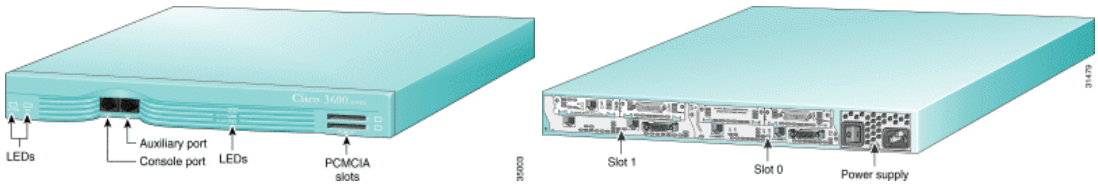
- Bộ định tuyến Cisco 2610
- 01 cổng console, 01AUX
- 01 Ethernet tốc độ 10Mbps giao diện RJ48 (Female Socket for RJ45 connector)
- 02 serial slot: có thể sử dụng cho cổng Serial, card ISDN BRI, card voice...
- 01 network module slot: có thể sử dụng module Async, Sync/Async, Channelized E1, PRI ...



Hình 3-8: Bộ định tuyến Cisco 2621

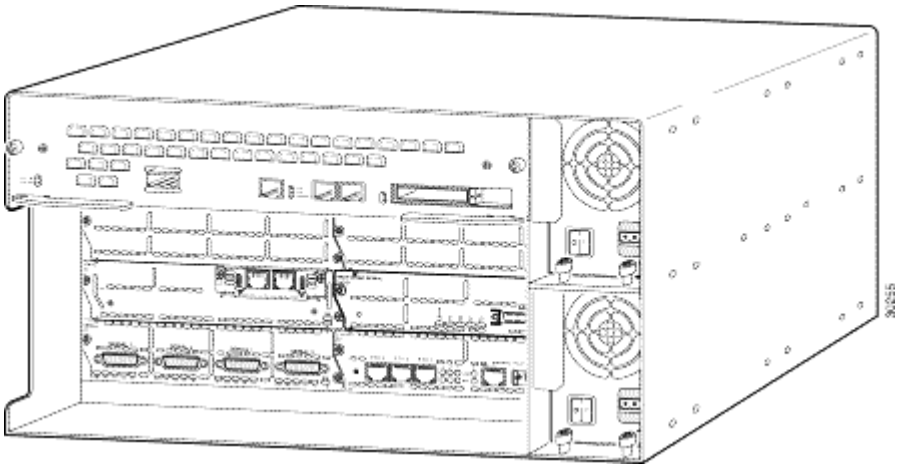
- Bộ định tuyến Cisco 2621
- 01 cổng console, 01AUX
- 02 FastEthernet tốc độ 10/100Mbps giao diện RJ48 (Female Socket for RJ45 connector)
- 02 serial slot: có thể sử dụng cho cổng Serial, card ISDN BRI, card voice...
- 01 network module slot: có thể sử dụng module Async, Sync/Async, Channelized E1, PRI ...

Bộ định tuyến Cisco 3600



Hình 3-9: Bộ định tuyến Cisco 3620

- Bộ định tuyến 3620
- 01 cổng console, 01AUX
- PCMCIA slot
- 02 network module slot: có thể sử dụng module Async, Sync/Async, Channelized E1, PRI, Ethernet/FastEthernet, Voice, VPN ...
- Khi kết nối với mạng LAN cần thiết có một Network module có cổng Ethernet/FastEthernet



Hình 3-10: Bộ định tuyến Cisco 3661

- Bộ định tuyến 3661
- 01 cổng console, 01AUX
- PCMCIA slot
- 01 FastEthernet tốc độ 100Mbps
- 06 network module slot: có thể sử dụng module Async, Sync/Async, Channelized E1, PRI, Ethernet/FastEthernet, Voice, VPN ...
- 02 module nguồn, hỗ trợ và dự phòng lẫn nhau, đảm bảo về mặt cung cấp nguồn điện cho bộ định tuyến. Có thể thay thế module nguồn mà không cần phải tắt điện toàn bộ bộ định tuyến.

II.4. Các giao tiếp của bộ định tuyến Cisco

- Cổng Console
  - Tốc độ có thể 11500Bps, làm việc ở tốc độ 9600Bps
  - Dùng cho cấu hình cho bộ định tuyến Cisco
  - Sử dụng cáp Console để kết nối
- Cổng AUX
  - Tốc độ 11500Bps
  - Sử dụng cho quản trị/cấu hình từ xa qua modem V34/V90
  - Có thể sử dụng để cấu hình trực tiếp sử dụng cáp Console

- Chỉ làm việc sau khi bộ định tuyến Cisco đã khởi động hoàn toàn
- Có thể cấu hình để AUX làm việc như một đường kết nối dự phòng

- Ethernet/FastEthernet
  - Tốc độ 10Mbps/100Mbps giao diện AUI hoặc RJ45
  - Dùng cho đấu nối trực tiếp vào mạng LAN
  - Tuân theo các chuẩn của IEEE802.3
- Serial
  - Tốc độ kết nối tới 2Mbps
  - Dùng cho kết nối mạng WAN
  - Có khả năng kết nối theo nhiều chuẩn giao diện khác nhau V35, V24, X21, EIA530... bằng việc sử dụng các cáp nối
- ISDN
  - Tốc độ 2B+D
  - Dùng cho kết nối mạng ISDN sử dụng cho Dialup Server hoặc kết nối dự phòng
  - Có các giao diện U hoặc S/T, giao diện S/T cần thiết có thiết bị NT1 để kết nối vào mạng
- Async
  - Giao diện truyền số liệu không đồng bộ
  - Dùng cho kết nối với các hệ thống modem V34/V90
  - Sử dụng cáp kết nối Async (Octal Cable) để nối tới 08 modem. Octal cable thường có giao diện RJ45 và cần có chuyển đổi RJ45-DB25 để phù hợp với giao diện của modem

II.5. Kiến trúc module của bộ định tuyến Cisco

Các bộ định tuyến có kiến trúc module

Các bộ định tuyến Cisco thông dụng được giới thiệu ở phần trước hầu hết là có kiến trúc module trừ bộ định tuyến 2500 đã không được tiếp tục sản xuất.

Ngoài các bộ định tuyến có kiến trúc module đã được biết, còn có các bộ định tuyến khác:

- **1600**: 1601, 1602, 1603, 1604, 1605
- **1700**: 1710, 1720, 1721, 1750, 1751, 1760
- **2600**: 2610, 2160XM, 2611, 2611XM, 2612, 2613, 2620, 2620XM, 2621, 2621XM, 2650, 2650XM, 2651, 2651XM, 2691
- **3600**: 3620, 3631, 3640, 3661, 3662
- **3700**: 3725, 3745

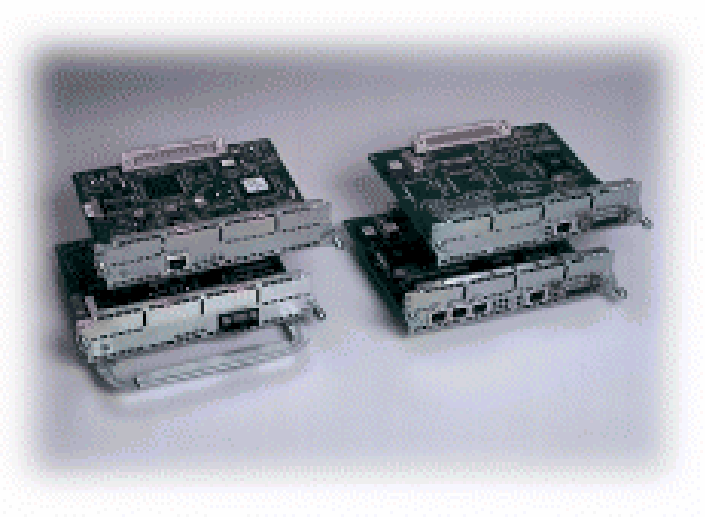
Tính tương thích dùng lẫn và thay thế

Các bộ định tuyến có kiến trúc module của Cisco được thiết kế để sử dụng chung một kho các card giao tiếp và module chức năng khác nhau.

Các card giao tiếp được sử dụng cho bất kỳ một bộ định tuyến nào có khe cắm tương thích. Tương thích phổ biến nhất là card giao tiếp Serial. Card giao tiếp serial có thể sử dụng trên bất kỳ bộ định tuyến nào. Một số card giao tiếp khác như card voice sẽ yêu cầu về cấu hình phần cứng và phần mềm tối thiểu. Các card giao tiếp được sử dụng cho các bộ định tuyến 1600, 1700 có thể sử dụng cho các bộ định tuyến 2600, 3600.

Bộ định tuyến 2600, 3600, 3700 cho phép sử dụng các module chức năng khác nhau. Một module chức năng có thể chỉ bao gồm một chức năng như module Async, module Serial, cũng có thể bao gồm nhiều chức năng hay bao gồm các khe cắm cho card giao tiếp khác như module NM-1E- có 01 cổng Ethernet và 02 khe cắm cho bất kỳ một loại card tương thích nào. Việc lựa chọn module tùy thuộc vào nhu cầu sử dụng cụ thể. Các module cùng được sử dụng giữa các bộ định tuyến. Một số module yêu cầu cấu hình tối thiểu về phần cứng và phần mềm. Bộ định tuyến 1600 và 1700 không cho phép sử dụng các module như các bộ định tuyến 2600, 3600.

Một số module thường gặp



Hình 3-11: Module Ethernet/FastEthernet

Bảng 3-2:Một số loại module Ethernet/FastEthernet

Loại module	Số cổng LAN	Số khe cắm WAN
Single-Port Ethernet	1	None
Four-Port Ethernet	4	None
Single-Port Ethernet Mixed Media	1	Two WAN interface card slots
Dual-Port Ethernet Mixed Media	2	Two WAN interface card slots
Single-Port Ethernet and Single-Port Token Ring	1/1	Two WAN interface card slots
Single Port Fast Ethernet	1	None

Hình 3-12: Module Ethernet có khe cắm WAN

Bảng 3-3: Một số loại module có khe cắm WAN

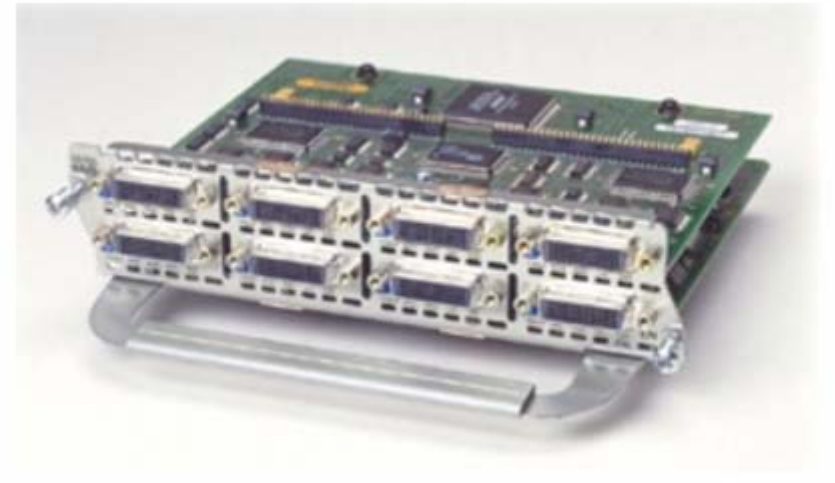
Tên module	Loại module
NM-1FE2W/NM-1FE2W-V2	1 10/100 Ethernet, 2 khe cắm WAN
NM-2FE2W/NM-2FE2W-V2	2 10/100 Ethernet, 2 khe cắm WAN
NM-1FE1R2W	1 10/100 Ethernet, 1 4/16 Token Ring, 2 khe cắm WAN
NM-2W	2 khe cắm WAN

Bảng 3-4: Giới hạn số lượng module trên các bộ định tuyến

	2600	2691	3620	3631	3640	3660	3725	3745
NM-1FE2W/NM-1FE2W-V2	N/A	1	2	N/A	4	6	2	4
NM-2FE2W/NM-2FE2W-V2	N/A	1	2	N/A	4	6	2	4
NM-1FE1R2W	N/A	1	2	N/A	4	6	2	4
NM-2W	1	1	1	N/A	3	6	2	4

Hình 3-13: Module 4 cổng serial

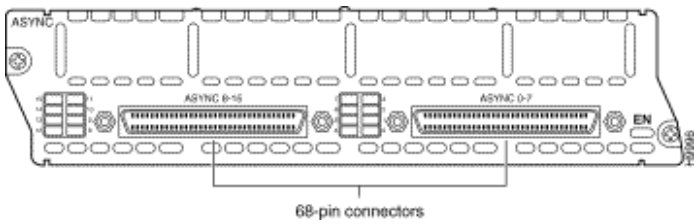
- Module 4 cổng serial
- Hỗ trợ tổng lưu lượng 8Mbps: có thể sử dụng tốc độ tối đa 8Mbps trên một cổng hoặc mỗi 2Mbps cho 4 cổng.
- Kết nối với modem theo các chuẩn V.35, X.21, EIA/TIA-232, EIA/TIA530... sử dụng các cáp phù hợp
- Sử dụng cho đấu nối leased-line, Frame Relay, X.25 ...



Hình 3-14: Module 8 cổng Sync/Async

- Module 8 cổng Sync/Async
- Tốc độ kết nối trên mỗi cổng thấp (tối đa 128Kbps)
- Có thể sử dụng ở hai chế độ đồng bộ và không đồng bộ. Có thể sử dụng cho modem quay số.

- Kết nối với modem theo các chuẩn V.35, X.21, EIA/TIA-232, EIA/TIA530... sử dụng các cáp phù hợp
- Sử dụng cho đấu nối leased-line, Frame Relay, X.25, modem quay số...



Hình 3-15: Module 16 cổng Async

- Module 16 cổng Async
- Kết nối không đồng bộ sử dụng cho modem quay số.
- Kết nối với modem theo các chuẩn EIA/TIA-232 sử dụng cáp Octal

Hình 3-16: Module và card ISDN BRI

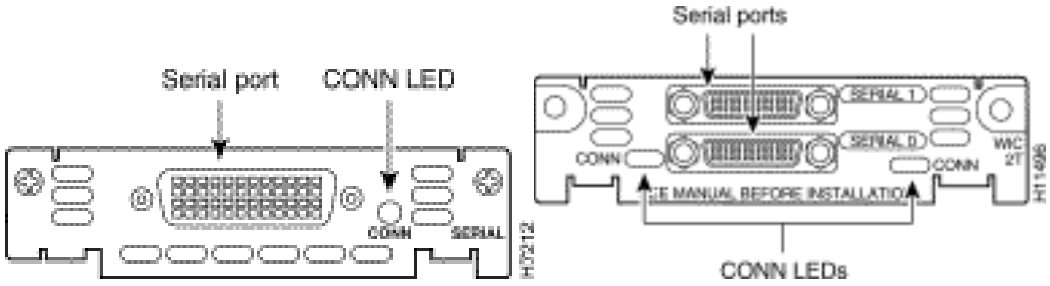
Bảng 3-5: Một số loại module ISDN BRI tốc độ 2B+D (128+16Kbps)

Loại module	Mô tả
NM-4B-S/T	4 cổng ISDN BRI giao diện S/T
NM-4B-U	4 cổng ISDN BRI giao diện U (tích hợp bộ tiếp hợp NT1)

NM-8B-S/T	8 cổng ISDN BRI giao diện S/T
NM-8B-U	8 cổng ISDN BRI giao diện U (tích hợp bộ tiếp hợp NT1)

Bảng 3-6: Một số loại card giao tiếp ISDN BRI tốc độ 2B+D (128+16Kbps)

Loại card	Mô tả
WIC-1B-S/T-V2	1 cổng ISDN BRI giao diện S/T
WIC 1B-U-V2	1 cổng ISDN BRI giao diện U (tích hợp bộ tiếp hợp NT1)



Hình 3-17: Card giao tiếp Serial

- Card một và hai cổng giao tiếp Serial
- Kết nối đồng bộ tốc độ đến 2Mbps
- Kết nối với modem theo các chuẩn V.35, X.21, EIA/TIA-232, EIA/TIA530... sử dụng các cáp phù hợp
- Sử dụng cho đấu nối leased-line, Frame Relay, X.25, modem quay số...

III. Cách sử dụng lệnh cấu hình bộ định tuyến

III.1. Giới thiệu giao tiếp dòng lệnh của bộ định tuyến Cisco

Giao tiếp dòng lệnh

Giao tiếp dòng lệnh CLI (Command Line Interface) khác với các giao tiếp đồ họa GUI (Graphic User Interface) là giao tiếp đặc biệt được Cisco thiết

kế cho phép người dùng, người quản trị làm việc với các thiết bị của Cisco thông qua các dòng lệnh trực tiếp.

Với giao tiếp dòng lệnh, người dùng, người quản trị có thể trực tiếp xem, cấu hình các thiết bị của Cisco thông qua các lệnh phù hợp. Để có thể sử dụng được giao tiếp dòng lệnh, người dùng phải nắm vững được các lệnh, các tham số lệnh và cách sử dụng các lệnh.

Mỗi thiết bị của Cisco đều có rất nhiều các lệnh, các bộ lệnh đi kèm tuy nhiên người sử dụng, người quản trị không nhất thiết phải hiểu hết toàn bộ các lệnh trong mỗi thiết bị mà chỉ cần hiểu, nắm vững một số lệnh cần thiết cho các mục đích sử dụng cụ thể.

Giao tiếp dòng lệnh của Cisco cung cấp cho người dùng khả năng sử dụng trợ giúp trực tuyến. Điều đó có nghĩa là trong quá trình làm việc với thiết bị thông qua giao tiếp dòng lệnh, người dùng có thể liệt kê các lệnh, xem lại ý nghĩa sử dụng của nó hay thậm chí xem các thông số lệnh.

Lưu ý: khi sử dụng giao tiếp dòng lệnh để cấu hình thiết bị, sau khi lệnh được thực thi (ấn phím Enter) các hoạt động của bộ định tuyến sẽ ảnh hưởng ngay lập tức bởi lệnh thực thi đó. Một cho những ví dụ là khi đang thực hiện cấu hình từ xa thông qua telnet, nếu thay đổi địa chỉ của bộ định tuyến, sẽ lập tức mất kết nối đến bộ định tuyến và chỉ có thể thực hiện cấu hình bộ định tuyến trực tiếp từ cổng console. Điều này có nghĩa cần thiết phải rất cẩn thận và chắc chắn cũng như thực hiện đúng trình tự mỗi khi thực hiện cấu hình bộ định tuyến.

```
Router#config terminal
Router(config)#interface s0/0
Router(config-if)#encapsolution ppp
Router(config-if)#ip address 192.168.100.5 255.255.255.0
Router(config-if)#
```

Hình 3-18: Ví dụ về giao tiếp dòng lệnh

Các khả năng thực hiện cấu hình bộ định tuyến Cisco

- Cấu hình bộ định tuyến trực tiếp từ cổng console: là phương pháp sử dụng một cáp console thông qua một phần mềm kết nối trực tiếp cổng COM như HyperTerminal của WINDOWS để truy nhập vào bộ định tuyến sau đó cấu hình bộ định tuyến theo giao thức dòng lệnh. Phương pháp cấu hình này được

sử dụng nhiều nhất và trong hầu hết các trường hợp. Các bộ định tuyến sử dụng lần đầu cũng phải được cấu hình bằng phương pháp này.

- Cấu hình bộ định tuyến thông qua truy nhập từ xa telnet: truy nhập từ xa tới bộ định tuyến với telnet chỉ có thể thực hiện được khi bộ định tuyến đã được cấu hình với ít nhất một địa chỉ mạng, có mật khẩu bảo vệ và máy tính sử dụng để cấu hình bộ định tuyến phải có khả năng kết nối được với bộ định tuyến thông qua môi trường mạng. Sau khi kết nối được tới bộ định tuyến, sử dụng giao diện dòng lệnh để cấu hình bộ định tuyến.

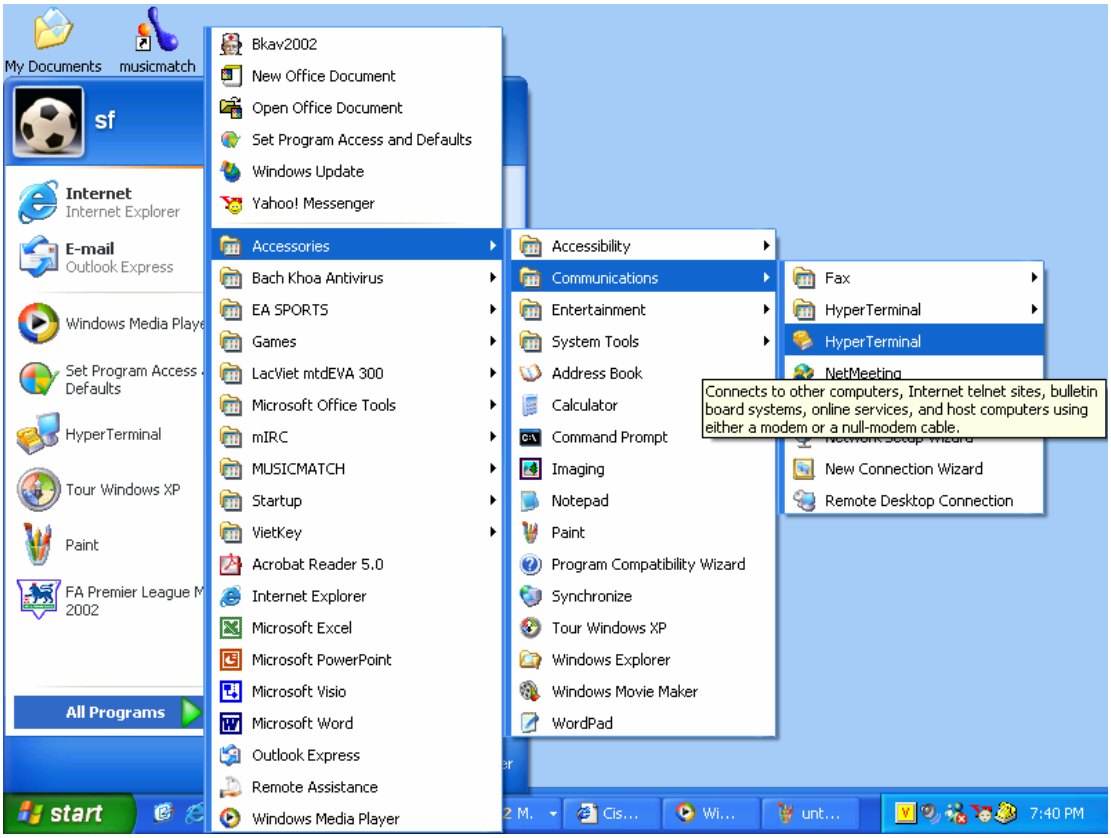
- Cấu hình bộ định tuyến sử dụng tập tin cấu hình lưu trữ trên máy chủ TFTP: trong một số trường hợp, tập tin cấu hình cho bộ định tuyến có thể được lưu trữ trên máy chủ TFTP, bộ định tuyến được cấu hình sao cho sau khi khởi động sẽ tìm kiếm tập tin cấu hình trên máy chủ TFTP thay vì sử dụng tập tin cấu hình lưu trữ trong NVRAM. Có thể sử dụng lệnh copy để tải tập tin cấu hình từ máy chủ TFTP về bộ định tuyến.

- Cấu hình bộ định tuyến thông qua giao diện WEB: chỉ thực hiện được sau khi bộ định tuyến đã được cấu hình với địa chỉ IP và cho phép cấu hình qua giao thức http.

Sử dụng giao tiếp dòng lệnh

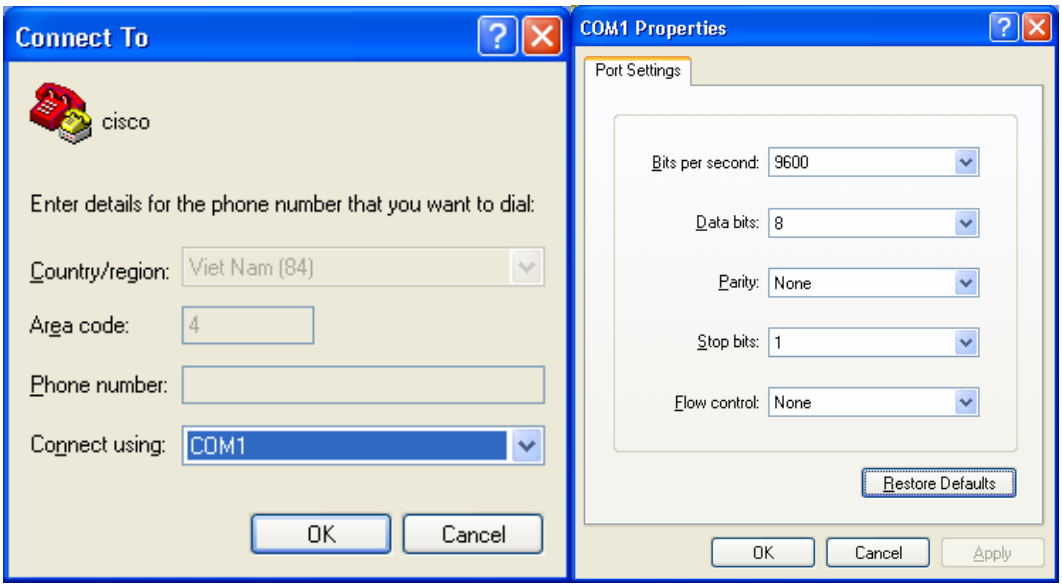
Để thực hiện việc kết nối máy tính với bộ định tuyến, người ta dùng cáp console của Cisco, một đầu cắm trực tiếp vào cổng CONSOLE của bộ định tuyến, đầu kia cắm vào cổng COM của máy tính, có thể sử dụng các đầu chuyển đổi DB9/RJ45 hoặc DB25/RJ45 khi cần thiết.

Phần mềm giao tiếp giữa máy tính và bộ định tuyến thông dụng nhất là HyperTerminal được cài đặt sẵn trong các phiên bản WINDOWS.

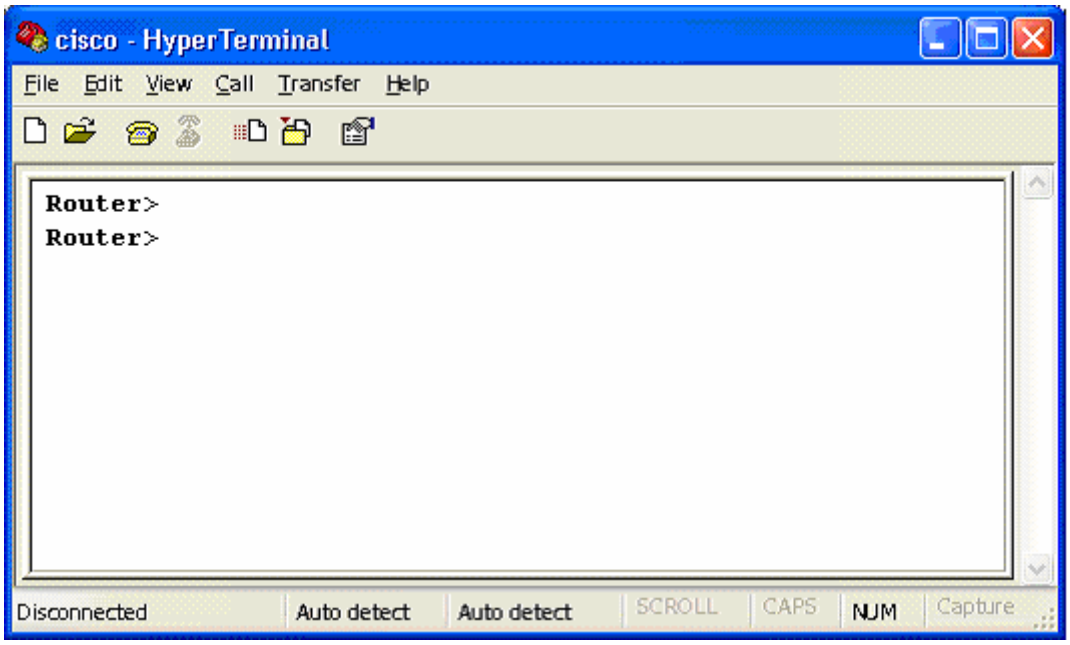


Hình 3-19:Sử dụng phần mềm HyperTerminal để kết nối đến bộ định tuyến

Chọn đúng cổng COM kết nối với cáp console để tiến hành cài đặt các thông số làm việc. Tốc độ kết nối thông qua cổng COM của máy tính và cổng CONSOLE của bộ định tuyến là 9600b/s (hình 3-20). Chọn OK, bấm phím Enter, cửa sổ làm việc xuất hiện dấu lớn hơn ">" sau tên của của bộ định tuyến, nghĩa là việc kết nối đã hoàn tất (hình 3-21).



Hình 3-20: Xác lập các tham số cho kết nối



Hình 3-21: Kết nối tới bộ định tuyến thành công

Sau khi đã kết nối thành công, sử dụng các lệnh của bộ định tuyến để xem, kiểm tra, cấu hình và bắt lỗi các hoạt động của bộ định tuyến.

Sử dụng dấu ? để truy cập thông tin trợ giúp

- Đánh dấu ? ngay sát sau câu lệnh chưa hoàn chỉnh sẽ hiện thị các lệnh có thể bắt đầu từ các từ chưa hoàn chỉnh đã gõ
- Đánh dấu ? sau câu lệnh một ký tự trắng sẽ hiển thị các tham số có thể của câu lệnh
- Khi câu lệnh không có sẽ hiển thị một báo lỗi

Sử dụng TAB ngay sát sau câu lệnh chưa hoàn chỉnh sẽ hiển thị câu lệnh hoàn chỉnh

III.2. Làm quen với các chế độ cấu hình

Chế độ người dùng

Bao gồm các tác vụ phổ biến chủ yếu gồm những lệnh kiểm tra trạng thái hoạt động của bộ định tuyến, trạng thái các giao tiếp, các bảng định tuyến v.v... và một số lệnh để kiểm tra kết nối mạng như ping, traceroute, telnet v.v.... Ở chế độ này không được phép thay đổi các cấu hình bộ định tuyến. Chế độ

người dùng không cho phép xem xét sâu đến các hoạt động của bộ định tuyến mà trong quá trình khai thác, vận hành, người quản trị phải cần thiết sử dụng chế độ quản trị để thực hiện. Biểu hiện của chế độ người dùng là dấu lớn hơn, >, sau tên bộ định tuyến.

```
Router>
Router>?
Exec commands:
  <1-99>           Session number to resume
  access-enable    Create a temporary Access-List entry
  access-profile   Apply user-profile to interface
  clear            Reset functions
  connect          Open a terminal connection
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network connection
  enable           Turn on privileged commands
  exit             Exit from the EXEC
      ----- các lệnh đã được bỏ bớt -----
  ping             Send echo messages
  ppp              Start IETF Point-to-Point Protocol (PPP)
  resume           Resume an active network connection
  rlogin           Open an rlogin connection
  show             Show running system information
  slip             Start Serial-line IP (SLIP)
  systat           Display information about terminal lines
  telnet           Open a telnet connection
  terminal         Set terminal line parameters
  traceroute       Trace route to destination
  tunnel           Open a tunnel connection
  udptn            Open an udptn connection
  where            List active connections
  x28              Become an X.28 PAD
  x3               Set X.3 parameters on PAD
```

Hình 3-22: Chế độ người dùng

Chế độ quản trị

Bao gồm hầu hết các lệnh của chế độ người dùng và các lệnh chỉ dành cho người quản trị. Chỉ có thể cấu hình bộ định tuyến ở chế độ này. Trong quá trình khai thác, vận hành, để hiểu rõ hoặc khi có sự cố xảy ra, người quản trị có thể sử dụng các lệnh debug để làm rõ thêm thông tin cần thiết. Đặc trưng cho chế độ quản trị là biểu hiện của dấu thăng, #.

```
Router>en
Password:
Router#
Router#?
Exec commands:
  <1-99>           Session number to resume
  access-enable    Create a temporary Access-List entry
  access-profile   Apply user-profile to interface
  access-template  Create a temporary Access-List entry
  archive          manage archive files
  bfe              For manual emergency modes setting
  cd               Change current directory
  clear            Reset functions
  clock            Manage the system clock
  configure        Enter configuration mode
  connect          Open a terminal connection
  copy             Copy from one file to another
  debug            Debugging functions (see also 'undebug')
      ----- các lệnh đã được bỏ bớt -----
  traceroute       Trace route to destination
  tunnel           Open a tunnel connection
  udptn            Open an udptn connection
  undebug          Disable debugging functions (see also 'debug')
```

```
upgrade          Upgrade firmware
verify           Verify a file
where            List active connections
write            Write running configuration to memory, network, or
                 terminal
x28              Become an X.28 PAD
x3               Set X.3 parameters on PAD
```

Hình 3-23: Chế độ quản trị

Chế độ cấu hình toàn cục

Là chế độ cấu hình các tham số toàn cục cho bộ định tuyến.

Có rất nhiều các cấu hình toàn cục như cấu hình tên bộ định tuyến, cấu hình tên và mật khẩu người dùng, cấu hình định tuyến toàn cục, cấu hình danh sách truy nhập v.v... Biểu hiện của chế độ cấu hình toàn cục xem hình 3-24.

```
Router#
Router#config terminal
Router(config)#hostname RouterA
RouterA(config)#
```

Hình 3-24: Chế độ cấu hình toàn cục

Chế độ cấu hình giao tiếp

Chế độ cấu hình giao tiếp là chế độ cấu hình cho các giao tiếp của bộ định tuyến như giao tiếp Serial, giao tiếp Ethernet, giao tiếp Async...

Chế độ cấu hình giao tiếp cho phép người quản trị mạng thiết lập các tham số hoạt động cho mỗi giao tiếp như các giao thức mạng được sử dụng trên giao tiếp, địa chỉ mạng của giao tiếp, gán các danh sách truy nhập cho giao tiếp v.v... Một ví dụ về chế độ cấu hình giao tiếp xem hình 3-25.

```
Router#
Router#config terminal
```

```
Router(config)#interface s0/0
Router(config-if)#encapsolution ppp
Router(config-if)#ip address 192.168.100.5 255.255.255.0
Router(config-if)#
```

Hình 3-25: Chế độ cấu hình giao tiếp

Chế độ cấu hình định tuyến

Là chế độ cấu hình các tham số cho các giao thức định tuyến. Các giao thức định tuyến được cấu hình độc lập với nhau và đều được thực hiện ở chế độ cấu hình định tuyến như ví dụ trên hình 3-26.

```
Router#
Router#config terminal
Router(config)#router rip
Router(config-router)#network 192.168.0.0
Router(config-if)#
```

Hình 3-26: Chế độ cấu hình định tuyến

Chế độ cấu hình đường kết nối

Chế độ cấu hình đường kết nối là một chế độ cấu hình đặc biệt sử dụng để thiết lập các tham số mức thấp cho giao tiếp logic trong đó điển hình là các tham số thiết lập cho các kết nối modem quay số.

```
Router#config terminal
Router(config)#line 33 48
Router(config-line)#modem inout
Router(config-line)#modem autoconfig discovery
Router(config-line)#
```

Hình 3-27: Chế độ cấu hình đường kết nối

Bảng 3-7:Một số chế độ cấu hình và thể hiện

Chế độ cấu hình	Thể hiện
Global	Router(config)#
Interface	Router(config-if)#
Subinterface	Router(config-subif)#
Controller	Router(config-controller)#
Map-list	Router(config-map-list)#
Map-class	Router(config-map-class)#
Line	Router(config-line)#
Router	Router(config-router)#
Route-map	Router(config-route-map)#

III.3. Làm quen với các lệnh cấu hình cơ bản

Enable: dùng để vào chế độ quản trị. Sau khi thực hiện lệnh enable, người dùng phải cung cấp mật khẩu quản trị đúng để thực sự được làm việc ở chế độ quản trị, mật khẩu không được phép nhập sai quá 3 lần.

```
Router>
Router>en
Password:
Password:
Password:
% Bad secrets

Router>en
Password:
Router#
```

```
Router#
Router#disa
Router>
```

Hình 3-28: Sử dụng lệnh enable và disable

Disable: thoát khỏi chế độ quản trị về chế độ người dùng.

Setup: thực hiện khởi tạo lại cấu hình của bộ định tuyến ở chế độ cấu hình hội thoại. Sau đây, hình 3-29, là một ví dụ về sử dụng lệnh setup. Chế độ hội thoại này cũng được thực hiện tự động đối với các bộ định tuyến chưa hề có tập tin cấu hình hay nói cách khác có NVRAM không chứa thông tin.

```
Router#setup

         --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: y

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: n

First, would you like to see the current interface summary? [yes]: n

Configuring global parameters:

  Enter host name [Router]:

  The enable secret is a password used to protect access to
```

```
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret [<Use current secret>]:

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password []:123456

  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: 654321
  Configure SNMP Network Management? [yes]:
    Community string [public]:
  Configure IP? [yes]:
    Configure IGRP routing? [yes]: n
    Configure RIP routing? [no]:
  Configure bridging? [no]:

Async lines accept incoming modems calls. If you will have
users dialing in via modems, configure these lines.

  Configure Async lines? [yes]: n

Configuring interface parameters:

Do you want to configure FastEthernet0/0  interface? [yes]: n

Do you want to configure Serial0/0  interface? [yes]: n

Do you want to configure Serial0/1  interface? [no]: y

  Some supported encapsulations are
        ppp/hdlc/frame-relay/lapb/x25/atm-dxi/smds
```

```
  Choose encapsulation type [hdlc]: ppp

  No serial cable seen.
  Choose mode from (dce/dte)  [dte]:
  Configure IP on this interface? [no]: y
    IP address for this interface: 192.168.100.5
    Subnet mask for this interface [255.255.255.0] :
    Class C network is 192.168.100.0, 24 subnet bits; mask is /24

The following configuration command script was created:

hostname Router
enable secret 5 $1$EuXV$Yhj/OYkz/U1R5VABqXsMC0
enable password 7 123456
line vty 0 4
password 7 654321
snmp-server community public
!
ip routing
no bridge 1
!
interface FastEthernet0/0
shutdown
no ip address
!
interface Serial0/0
shutdown
no ip address
!
interface Serial0/1
no shutdown
encapsulation ppp
ip address 192.168.100.5 255.255.255.0
dialer-list 1 protocol ip permit
```

```
dialer-list 1 protocol ipx permit
!
end

[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.
```

Hình 3-29: Lệnh setup

Config: cho phép thực hiện các lệnh cấu hình bộ định tuyến. Sau lênh config, quản trị mạng mới có thể thực hiện các lệnh cấu hình bộ định tuyến.

Trình tự thực hiện cấu hình cho một bộ định tuyến có thể được thể hiện như sau

- Đặt tên cho bộ định tuyến

```
Router#config terminal
Router(config)#
Router(config)#hostname RouterABC
RouterABC(config)#
```

- Đặt tên mật khẩu bí mật dành cho người quản trị

```
RouterABC(config)#enable secret matkhaubimat
RouterABC(config)#
```

- Đặt tên mật khẩu cho chế độ quản trị. Mật khẩu này chỉ sử dụng khi cấu hình bộ định tuyến không có mật khẩu bí mật dành cho quản trị.

```
RouterABC(config)#enable password matkhau
RouterABC(config)#
```

- Cấu hình cho phép người dùng truy cập từ xa đến bộ định tuyến

```
RouterABC(config)#line vty 0 4
RouterABC(config-line)#login
RouterABC(config-line)#password telnet
RouterABC(config-line)#
```

- Cấu hình các giao tiếp

```
RouterABC(config)#interface ethernet 0
RouterABC(config-if)#ip address 192.168.2.1 255.255.255.0
```

```
RouterABC(config-if)#no shutdown
RouterABC(config-if)#
```

- Cấu hình định tuyến

```
RouterABC(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.2
RouterABC(config)#
```

Copy: lệnh copy cho phép thực hiện các sao chép cấu hình của bộ định tuyến đi/đến máy chủ TFTP**,** sao chép, lưu trữ, nâng cấp các tập tin IOS của bộ định tuyến từ / tới máy chủ TFTP.

Để có thể lưu bản sao cấu hình hiện hành lên máy chủ TFTP, sử dụng lệnh *copy rumng-config tftp* như được trình bày trên hình 3-30. Hình 3-31 là tiến trình ngược lại với việc tải tập tin cấu hình từ máy chủ TFTP về bộ định tuyến.

- Nhập lệnh *copy runing-config tftp*
- Nhập địa chỉ IP của máy chủ TFTP nơi dùng để lưu tập tin cấu hình
- Nhập tên ấn định cho tập tin cấu hình
- Xác nhận chọn lựa với trả lời yes

```
Router#copy running-config tftp
Address or name of remote host []? 192.168.1.5
Name of configuration file to write [Router-config]?cisco.cfg
Write file cisco.cfg to 192.168.1.5? [confirm] y
Writing cisco.cfg !!!!! [OK]
Router#
```

Hình 3-30: Lệnh copy dùng để lưu tập tin cấu hình lên máy chủ

```
Router#copy tftp running-config
Address or name of remote host []? 192.168.1.5
Source filename []? cisco.cfg
Destination filename [running-config]?
```

Hình 3-31: Lệnh copy dùng để tải tập tin cấu hình từ máy chủ

Show: là lênh được dùng nhiều và phổ biến nhất.

Lệnh show dùng để xác định trạng thái hiện hành của bộ định tuyến. Các lệnh này giúp cho phép có được các thông tin quan trọng cần biết khi kiểm tra và điều chỉnh các hoạt động của bộ định tuyến.

- show version: hiển thị cấu hình phần cứng hệ thống, phiên bản phần mềm, tên và nguồn của các tập tin cấu hình, và ảnh chương trình khởi động.

- show processes: hiển thị thông tin các quá trình hoạt động của bộ định tuyến.

- show protocols: hiển thị các giao thức được cấu hình.

- show memory: thống kê về bộ nhớ của bộ định tuyến.

- show stacks: giám sát việc sử dụng stack của các quá trình, các thủ tục ngắt và hiển thị nguyên nhân khởi động lại hệ thống lần cuối cùng.

- show buffers: cung cấp thống kê về các vùng bộ đệm trên bộ định tuyến.

- show flash: thể hiện thông tin về bộ nhớ Flash.

- show running-config: hiển thị tập tin cấu hình đang hoạt động của bộ định tuyến.

- show startup-config: hiển thị tập tin cấu hình được lưu trữ trên NVRAM và được đưa vào bộ nhớ để hoạt động khi bật nguồn bộ định tuyến. Thông thường running-config và startup-config là giống nhau. Khi thực hiện các lệnh cấu hình, running-config và startup-config sẽ không còn giống nhau, cấu hình hoạt động (running-config) cần phải được ghi trở lại NVRAM sau khi kết thúc cấu hình bộ định tuyến.

- show interfaces: thống kê các giao tiếp của bộ định tuyến. Đây là một trong các lệnh được sử dụng nhiều nhất cho biết trạng thái hoạt động của các giao tiếp, số liệu thống kê lưu lượng, số lượng các gói tin lỗi v.v...

```
Router#sh run                          Router#sh startup-config
Building configuration...              Current configuration : 677 bytes
!                                      !
Version 12.1                           Version 12.1
service timestamps debug uptime        service timestamps debug uptime
service timestamps log uptime          service timestamps log uptime
no service password-encryption         no service password-encryption
!                                      !
hostname Router                        hostname Router
!                                      !
interface Ethernet0                    interface Ethernet0
 no ip address                          no ip address
 no ip directed-broadcast               no ip directed-broadcast
 shutdown
```

Hình 3-32: Lệnh show

```
Router#show interface s0/0
Serial0/0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Description: 2M link to the Internet
  Internet address is 192.168.100.5/24
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec,
     reliability 255/255, txload 248/255, rxload 84/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/12/0 (size/max/drops/flushes); Total output
drops: 2383688
  Queueing strategy: weighted fair
  Output queue: 24/1000/64/2383671 (size/max total/threshold/drops)
     Conversations  5/184/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 677000 bits/sec, 161 packets/sec
  5 minute output rate 1996000 bits/sec, 395 packets/sec
     106754998 packets input, 2930909441 bytes, 0 no buffer
     Received 68850 broadcasts, 0 runts, 0 giants, 0 throttles
     51143 input errors, 30726 CRC, 20248 frame, 0 overrun, 0
ignored, 169 abort
```

```
     319791176 packets output, 1669977392 bytes, 0 underruns
     0 output errors, 0 collisions, 125 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Hình 3-33: Lệnh show interface

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.1(2), RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Tue 09-May-00 23:34 by linda
Image text-base: 0x80008088, data-base: 0x807D2544

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)

Router uptime is 1 week, 1 day, 1 minute
System returned to ROM by power-on at 13:29:57 Hanoi Thu Jul 31 2003
System restarted at 20:24:22 Hanoi Tue Sep 2 2003
System image file is "flash:c2600-i-mz.121-2.bin"

cisco 2620 (MPC860) processor (revision 0x102) with 26624K/6144K
bytes of memory
.
Processor board ID JAD04340ID8 (2733840160)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
1 FastEthernet/IEEE 802.3 interface(s)
2 Serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)
```

```
Configuration register is 0x2102
```

Hình 3-34: Lệnh show version

Write: lệnh write sử dụng để ghi lại cấu hình hiện đang chạy của bộ định tuyến. Nhất thiết phải dùng lệnh *write memory* để ghi lại cấu hình của bộ định tuyến vào NVRAM mỗi khi có thay đổi về cấu hình.

```
Router#write ?
  erase     Erase NV memory
  memory    Write to NV memory
  network   Write to network TFTP server
  terminal  Write to terminal
  <cr>
```

Hình 3-35: Lệnh write

III.4. Cách khắc phục một số lỗi thường gặp

Lỗi kết nối đến cổng console sử dụng Hyper Terminal

- Kiểm tra lại xem đã sử dụng chính xác loại cáp dùng để cấu hình bộ định tuyến chưa. Cáp console dùng để cấu hình bộ định tuyến là cáp 8 sợi có hai đầu RJ45 có sơ đồ đấu nối như bảng 3-8 và sử dụng đầu chuyển đổi DB9/RJ45 được cung cấp kèm theo bộ định tuyến.
- Kiểm tra xem đã sử dụng đúng cổng kết nối COM của máy tính để nối tới bộ định tuyến.

Bảng 3-8: Sơ đồ đấu nối cáp console

Console	Cáp console		DB9/RJ45	COM
Tín hiệu	RJ45	RJ45	DB9	Tín hiệu
RTS	1	8	8	CTS

DTR	2	7	6	DSR
TxD	3	6	2	RxD
GND	4	5	5	GND
GND	5	4	5	GND
RxD	6	3	3	TxD
DSR	7	2	4	DTR
CTS	8	1	7	RTS

- Kiểm tra các tham số kết nối như hình 3-20. Tốc độ kết nối phải là 9600 cho kết nối qua cổng console.

Lỗi kết nối sử dụng telnet

Khi sử dụng telnet để cấu hình từ xa bộ định tuyến, người dùng có thể không kết nối được đến bộ định tuyến. Một trong các lỗi sau cần được kiểm tra:

- Máy tính dùng để cấu hình bộ định tuyến không có kết nối mạng với bộ định tuyến. Kiểm tra lại khả năng kết nối mạng từ máy tính đến bộ định tuyến. Có thể dùng lệnh *ping* để kiểm tra.

- Khi cấu hình bộ định tuyến lần đầu, người quản trị mạng đã quên không thiết lập mật khẩu cho truy nhập từ xa. Khi cố gắng truy nhập từ xa, người dùng sẽ nhận được thông báo về việc mật khẩu truy nhập chưa được thiết lập. Trường hợp này cần sử dụng cáp console để thiết lập mật khẩu theo trình tự như trình bày dưới đây

```
Router#config terminal
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password 123456
Router(config-line)#end
Router#write memory
```

- Kiểm tra về việc có hay không có các hạn chế telnet sử dụng các danh sách kiểm soát truy nhập (access-list).

IV. Cấu hình bộ định tuyến Cisco

IV.1. Cấu hình leased-line

Giới thiệu leased-line

Leased-line, hay còn được gọi là kênh thuê riêng, là một hình thức kết nối trực tiếp giữa các node mạng sử dụng kênh truyền dẫn số liệu thuê riêng.

Kênh truyền dẫn số liệu thuê riêng thông thường cung cấp cho người sử dụng sự lựa chọn trong suốt về giao thức đấu nối hay nói cách khác, có thể sử dụng các giao thức khác nhau trên kênh thuê riêng như PPP, HDLC, LAPB v.v...

Về mặt hình thức, kênh thuê riêng có thể là các đường cáp đồng trực tiếp kết nối giữa hai điểm hoặc có thể bao gồm các tuyến cáp đồng và các mạng truyền dẫn khác nhau. Khi kênh thuê riêng phải đi qua các mạng truyền dẫn khác nhau, các quy định về giao tiếp với mạng truyền dẫn sẽ được quy định bởi nhà cung cấp dịch vụ. Do đó, các thiết bị đầu cuối CSU/DSU cần thiết để kết nối kênh thuê riêng sẽ phụ thuộc và nhà cung cấp dịch vụ. Một số các chuẩn kết nối chính được sử dụng là HDSL, G703, 2B1Q v.v...

Khi sử dụng kênh thuê riêng, người sử dụng cần thiết phải có đủ các giao tiếp trên các bộ định tuyến sao cho có một giao tiếp kết nối WAN cho mỗi một kết nối kênh thuê riêng tại mỗi node. Điều đó có nghĩa là, tại điểm node có kết nối kênh thuê riêng đến 10 điểm khác nhất thiết phải có đủ 10 giao tiếp WAN để phục vụ cho các kết nối kênh thuê riêng. Đây là một vấn đề hạn chế về đầu tư thiết bị ban đầu, không linh hoạt trong mở rộng, phát triển, phức tạp trong quản lý, đặc biệt là chi phí thuê kênh lớn đối với các yêu cầu kết nối xa về khoảng cách địa lý.

Các giao thức sử dụng với đường lease-line

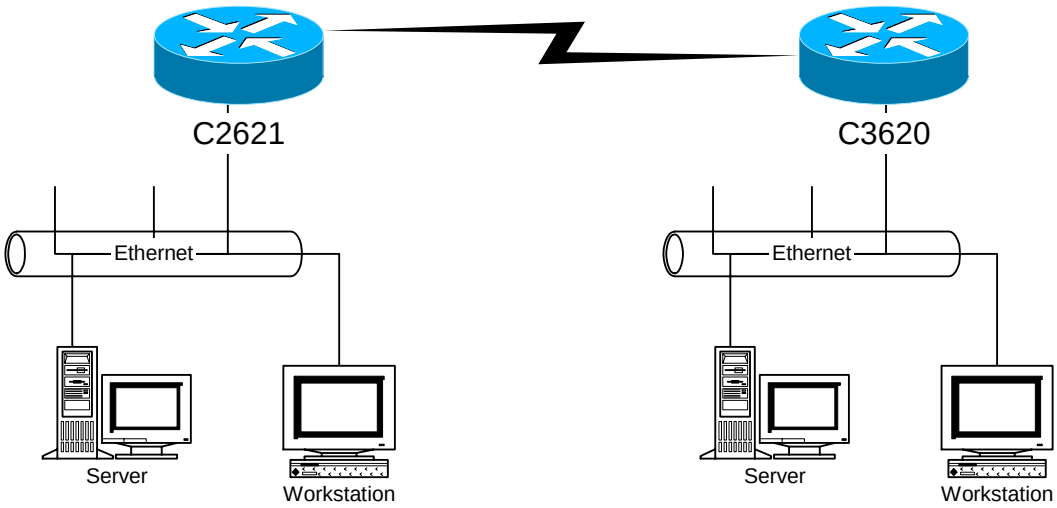
Hai giao thức sử dụng với leased-line là HDLC, PPP và LAPB. Trong đó:

- HDLC: là giao thức được sử dụng với họ các bộ định tuyến Cisco hay nói cách khác chỉ có thể sử dụng HDLC khi cả hai phía của kết nối leased-line đều là bộ định tuyến Cisco.

- PPP: là giao thức chuẩn quốc tế, tương thích với tất cả các bộ định tuyến của các hãng sản xuất khác nhau. Khi đấu nối kênh leased-line giữa một phía là thiết bị của Cisco và một phía là thiết bị của hãng thứ 3 thì nhất thiết phải dùng giao thức đấu nối này. PPP là giao thức lớp 2 cho phép nhiều giao thức mạng khác nhau có thể chạy trên nó do vậy nó được sử dụng phổ biến.

- LAPB: là giao thức truyền thông lớp hai tương tự như giao thức mạng X.25 với đầy đủ các thủ tục, quá trình kiểm soát truyền dẫn, phát hiện và sửa lỗi. LAPB ít được sử dụng.

Mô hình kết nối lease-line



Hình 3-36: Mô hình kết nối leased-line

Cấu hình kết nối lease-line cơ bản

- Phân định địa chỉ

o Việc phân định địa chỉ cho các mạng và cho các kết nối giữa các bộ định tuyến là rất quan trọng, đảm bảo cho việc liên lạc thông suốt giữa các mạng, đảm bảo cho vấn đề qui hoặch địa chỉ, nhóm gọn các định tuyến ...

o Khi thực hiện xây dựng một mạng dùng riêng, điều cần thiết phải ghi nhớ là chỉ được dùng các địa chỉ trong nhóm các địa chỉ dành cho mạng dùng riêng:10.x.x.x, 172.16.x.x – 172.31.x.x, 192.168.x.x

o Để đảm bảo không bị trùng lặp và giảm thiểu các vấn đề phát sinh, các kết nối mạng WAN theo kiểu leased-line cần được sắp xếp trên lớp mạng nhỏ nhất. Các kết nối mạng WAN trong trường hợp này được thực hiện trên các lớp mạng gồm 4 địa chỉ.

o Các lớp mạng khác tuỳ theo yêu cầu cụ thể và số lượng các địa chỉ có thể mà phân chia cho phù hợp.

- Để bắt đầu cấu hình mạng:

```
o Router> enable ↵
o Password: ****** ↵
o Router# config terminale ↵
o Router(config)#
```

- Thực hiện đặt tên, các mật khẩu, cấu hình cho phép telnet và các điều kiện cần thiết trước khi cấu hình các giao diện

- Cấu hình

```
o Router2621(config)# interface serial 0 ↵
```

- Lựa chọn giao thức sử dụng

```
o Router2621(config-if)# encapsolation HDLC ↵
```

- Đặt địa chỉ IP cho giao tiếp kết nối leased-line

```
o Router2621(config-if)# ip address 192.168.113.5
255.255.255.252 ↵
```

- Luôn phải đưa giao tiếp vào sử dụng bằng lệnh no shutdown

```
o Router2621(config-if)# no shutdown ↵
o Router2621(config-if)# interface serial 1 ↵
```

- Lựa chọn giao thức PPP sử dụng cho một giao tiếp khác

```
o Router2621(config-if)# encapsolation PPP ↵
o Router2621(config-if)# ip address 192.168.113.9
255.255.255.252 ↵
o Router2621(config-if)# no shutdown ↵
o Router2621(config-if)# exit ↵
```

- Sử dụng định tuyến tĩnh với cú pháp: ip route [địa chỉ mạng đích] [netmask] [địa chỉ next hop]

- **Router2621(config)# ip route 0.0.0.0 0.0.0.0 192.168.113.6 ↵**

- Luôn phải ghi lại cấu hình khi đã cấu hình xong

- **Router2621# write memory ↵**

- Thực hiện các phần việc còn lại tại các bộ định tuyến khác, chú ý về giao thức được sử dụng kiểm tra, giám sát các kết nối.

- Dùng lệnh **show interface** để kiểm tra trạng thái của giao tiếp

- **show interface**: xem trạng thái tất cả các giao tiếp

- **show interface serial 0**: xem trạng thái cổng serial 0

- *Serial 0 is admininistrative down line protocole is down*: thể hiện trạng thái đang bị cấu hình là không làm việc, sử dụng lệnh no shutdown trong Interface mode để đưa giao tiếp serial 0 vào làm việc

- *Serial 0 is down line protocole is down*: kiểm tra lại đường truyền

- *Serial 0 is up line protocole is down*: kiểm tra lại các giao thức được sử dụng tại hai phía

- *Serial 0 is up line protocole is up*: là trạng thái làm việc

Cấu hình bộ định tuyến 2621

```
!
hostname 2621
!
!
interface FastEthernet0/0
 ip address 10.0.5.1 255.255.255.0
!
!
interface Serial0/0
 ip address 192.168.113.5 255.255.255.252
 encapsulation ppp
!
!
```

```
ip route 0.0.0.0 0.0.0.0 192.168.113.6
!
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Hình 3-37: Cấu hình của bộ định tuyến 2621

```
Cấu hình bộ định tuyến 3620

!
hostname 3620
!
!
interface FastEthernet0/0
 ip address 10.0.6.1 255.255.255.0
!
!
interface Serial1/0
 ip address 192.168.113.6 255.255.255.252
 encapsulation ppp
!
!
ip route 0.0.0.0 0.0.0.0 192.168.113.5
!
!
line con 0
 exec-timeout 0 0
 transport input none
```

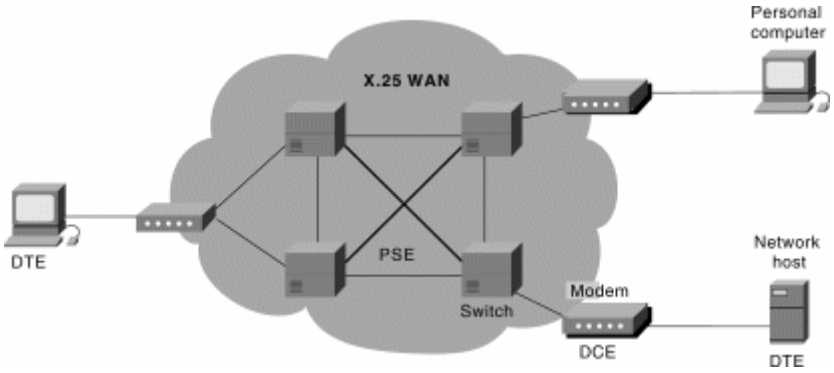
```
line aux 0
line vty 0 4
 login
!
end
```

Hình 3-38: Cấu hình của bộ định tuyến 3620

IV.2. Cấu hình X.25 & Frame Relay

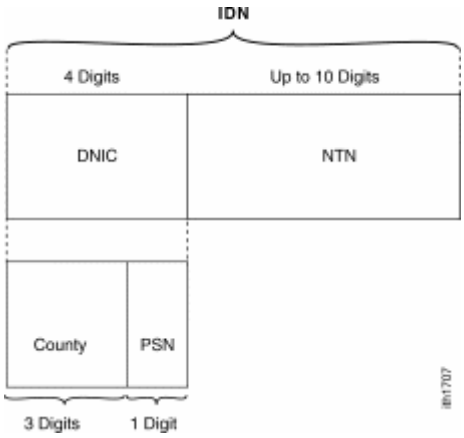
Giới thiệu X.25 và Frame Relay

X25: Năm 1978 ISO thay đổi thêm HDLC và CCITT thêm một số thông số để sinh ra LAPB "Link Access Procedure – Balanced Mode". LAPB định nghĩa một số quy luật cho mức Frame của X.25 như các loại khung đặc biệt như RR (Receive Ready), REJ (Reject) . . .



Hình 3-39: Chuyển mạch gói X.25

X.25 cung cấp các kết nối diện rộng thông qua môi trường chuyển mạch gói. Mỗi thuê bao X.25 có một địa chỉ xác định duy nhất được đánh số gồm các phần mã quốc gia, nhà cung cấp dịch vụ và địa chỉ của thuê bao trực thuộc nhà cung cấp dịch vụ.



Hình 3-40: Cấu trúc địa chỉ X.25

Khi có nhu cầu kết nối truyền dữ liệu, các thiết bị đầu cuối X.25 sẽ phát khởi tạo một VC (virtual circuit) tới địa chỉ đích. Sau khi VC được thiết lập, dữ liệu sẽ được truyền tải giữa hai điểm thông qua VC đó. Nếu nhu cầu dữ liệu lớn hơn, thiết bị đầu cuối sẽ khởi tạo thêm các VC mới. Khi hết giữ liệu, các VC sẽ được giải phóng cho các nhu cầu truyền tải khác.

X.25 qui định một số tham số xác định bao gồm:

- Độ lớn gói tin (ips/ops): là giá trị kích thước gói tin được quy định bởi nhà cung cấp dịch vụ.

- Độ lớn cửa sổ điều khiển luồng (win/wout): X.25 sử dụng cơ chế điều khiển luồng bằng cửa số để đảm bảo tốc độ gửi nhận tin phù hợp không làm mất mát thông tin. Với tham số cửa sổ bằng 7, X.25 cho phép gửi tối đa 7 gói tin khi chưa nhận được phúc đáp.

- Số lượng kênh VC tối đa cho chiều đến / hai chiều / chiều đi (hic/htc/hoc): Số lượng kênh VC được cung cấp cho mỗi thuê bao X.25 đã được xác định bởi nhà cung cấp. Thuê bao chỉ có thể truyền tải dữ liệu với số lượng các VC tối đa cho phép đã được xác định. Không thể thực hiện được yêu cầu truyền tải nếu có yêu cầu truyền tải tới các điểm mới khi số lượng VC đã hết. Khi các thiết bị đầu cuối X.25 thực hiện truyền tải dữ liệu nó phải tuân theo các quy tắc:

o Cuộc gọi ra được thực hiện từ VC lớn nhất còn trống. Điều đó có nghĩa là, nếu chưa hề có cuộc gọi nào và số VC được cung cấp cho một thuê bao là 16 thì cuộc gọi ra đầu tiên sẽ khởi tạo VC số 16 để thực hiện yêu cầu kết nối.Trong trường hợp đã dùng hết 3 VC gọi ra thì cuộc gọi ra thứ 4 sẽ sử dụng VC số 13 để thực hiện.

o Cuộc gọi tới được thực hiện từ VC nhỏ nhất còn trống. Tương tự như cuộc gọi ra, cuộc gọi vào đầu tiên sẽ nhận được trên VC số 1 và cuộc gọi vào thứ 10 sẽ nhận được trên VC số 10.

o Quá trình khởi tạo VC sẽ dừng lại khi không còn VC trống.

o Với các quy tắc này, yêu cầu cần thiết phải xác lập một cách chính xác các tham số cho thiết bị đầu cuối X.25 thì mới có thể thực hiện được các kết nối truyền tải dữ liệu.

Về đặc điểm của X.25

- Tốc độ truyền tải hạn chế, tại Việtnam tốc độ cung cấp tối đa là 128Kbps.
- Độ trễ lớn, không phù hợp cho các ứng dụng có yêu cầu cao về độ trễ.
- Khả năng mở rộng dễ dàng, chi phí không cao.
- An toàn và bảo mật, vẫn được sử dụng trong các giao dịch ngân hàng.

Frame Relay: Frame Relay ra đời trên nền tảng hạ tầng viễn thông ngày càng được cải thiện, không cần có quá nhiều các thủ tục phát hiện và sửa lỗi như X.25. Frame relay có thể chuyển nhận các khung lớn tới 4096 byte trong khi đó gói tiêu chuẩn của X.25 khuyến cáo dùng là 128 byte. Frame Relay rất thích hợp cho tryền 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.

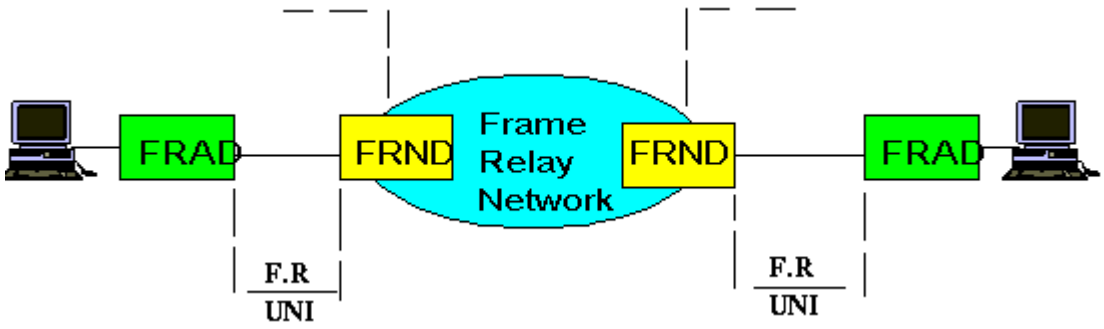
Bảng 3-9:So sánh giữa X.25 và Frame Relay

TT	Chức năng của mạng	X25	Frame relay
1	Phúc đáp khung thông tin nhận được	√	
2	Phúc đáp gói tin nhận được	√	
3	Dịch địa chỉ của gói tin	√	√
4	Cất giữ gói tin vào vùng đệm để chờ phúc đáp	√	
5	Phát hiện gói tin sai thứ tự	√	

6	Huỷ gói tin bị lỗi	√	√
7	Đảm bảo khung tin có giá trị N(s) là hợp lệ	√	
8	Thiết lập và huỷ bỏ kết nối logical	√	
9	Thiết lập và huỷ bỏ kênh ảo	√	
10	Điền các bit cờ vào giữa các khung	√	
11	Điều khiển luồng dữ liệu ở lớp liên kết logic	√	
12	Tạo và kiểm tra FCS	√	√
13	Tạo và nhận dạng bit cờ	√	√
14	Tạo ra khung báo chưa sẵn sàng	√	
15	Tạo ra khung báo đã sẵn sàng	√	
√16	Tạo ra khung báo khung bị từ chối	√	
17	Quản lý các bit D, M, Q trong gói tin	√	
18	Quản lý các khung ở mức liên kết dữ liệu	√	
19	Quản lý các bộ định thời ở mức 3	√	
20	Quản lý các bit Poll/Final trong khung	√	
21	Quản lý các bộ đếm số thứ tự của khung và gói tin	√	
22	Ghép các kênh logic	√	
23	Quản lý các thủ tục khởi động ở mức 2 và 3	√	
24	Nhận dạng các khung không hợp lệ	√	√
25	Trả lời các khung và gói tin báo chưa sẵn	√	

	sàng		
26	Trả lời các khung và gói tin báo đã sẵn sàng	√	
27	Trả lời các khung và gói tin báo từ chối khung	√	
28	Đánh dấu số lần phải truyền lại	√	
29	Chèn thêm và bỏ các bit 0 vào số liệu	√	√

Bảng chức năng trên cho thấy Frame relay đã giảm rất nhiều các công việc không cần thiết cho thiết bị chuyển mạch do đó giảm gánh nặng cũng như thời gian xử lý công việc cho các nút mạng, nhờ vậy mà làm giảm thời gian trễ cho các khung thông tin khi truyền trên mạng.



Hình 3-41: Mô hình mạng 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.

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.

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 cho từng cuộc gọi một mà phân phối băng thông một cách linh hoạt điều mà X.25 và thuê kênh riêng không có. Ví dụ người sử dụng hợp đồng sử dụng với tốc độ 64Kbps, khi họ chuyển đi một lượng thông tin quá lớn, Frame Relay cho phép truyền chúng ở tốc độ cao hơn 64Kbps. Hiện tượng này được gọi là bùng nổ Bursting.

Các đặc điểm của Frame Relay:

- Cung cấp các kết nối thông qua các kênh ảo cố định PVC. Khi có nhu cầu kết nối giữa 2 điểm, nhà cung cấp dịch vụ sẽ thiết lập các thông số trên các node Frame Relay tạo ra các kênh ảo cố định giữa 2 điểm. Không như X.25, hướng kết nối Frame Relay là cố định và không thể khởi tạo bởi người dùng. Khi có nhu cầu kết nối đến điểm đích khác, khách hàng phải thuê mới PVC đến điểm đích mới đó.

- CIR (Committed Information Rate): là tốc độ truyền dữ liệu mà nhà cung cấp dịch vụ cam kết sẽ đảm bảo cho khách hàng, điều đó có nghĩa là khách hàng sẽ được đảm bảo cung cấp đường truyền với đúng tốc độ yêu cầu. CIR được gắn liền với với các PVC và độc lập giữa các PVC khác nhau. Nếu tắc nghẽn xảy ra thì khách hàng vẫn truyền được với tốc độ yêu cầu khi ký kết hợp đồng.

- Frame Relay hỗ trợ truyền số liệu khi có bùng nổ số liệu hay còn gọi là "bursty", có nghĩa là lượng thông tin được gửi đi trong thời gian ngắn và với dung lượng lớn hơn dung lượng bình thường. Nói cách khác, khi có một nhu cầu truyền tải khối lượng dữ liệu lớn, mạng Frame Relay cho phép được thực hiện truyền tải dữ liệu với tốc độ lớn hơn tốc độ CIR đã mua của nhà cung cấp dịch vụ. Điều này đảm bảo cho khách hàng tiết kiệm được chi phí mà vẫn đảm bảo truyền dữ liệu với khối lượng lớn trong những điều kiện cần thiết đảm bảo lưu thông thông tin. Truyền dữ liệu bursty chỉ thực hiện được khi không có tắc nghẽn trên mạng.

- Frame Relay không sử dụng địa chỉ định danh như X.25. Để phân biệt các PVC, Frame Relay sử dụng DLCI, mỗi một PVC được gắn liền với một DLCI. DLCI chỉ có tính chất cục bộ có nghĩa là chỉ có ý nghĩa quản lý trên cùng một chuyển mạch. Nói cách khác số DLCI chỉ cần là duy nhất cho mỗi

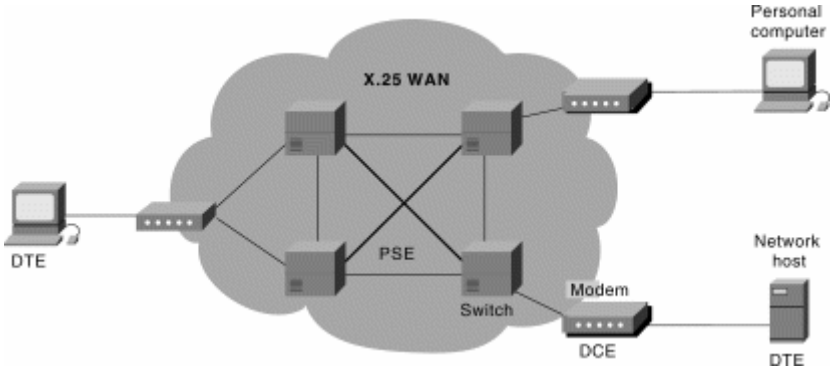
PVC trên một chuyển mạch còn có thể có cùng số DLCI đó trên một chuyển mạch khác.

- Frame Relay sử dụng giao thức LMI (Local Manegment Interface) là giao thức quản lý và trao đổi thông tin quản trị giữa các thiết bị mạng FRND và các thiết bị kết nối FRAD.

- Cũng như X.25, Frame Relay là môi trường mạng đa truy nhập không quảng bá (multiaccess nonbroadcast media). Vấn đề này cần được chú ý khi sử dụng với các giao thức định tuyến.

Các mô hình kết nối của X.25 và Frame Relay

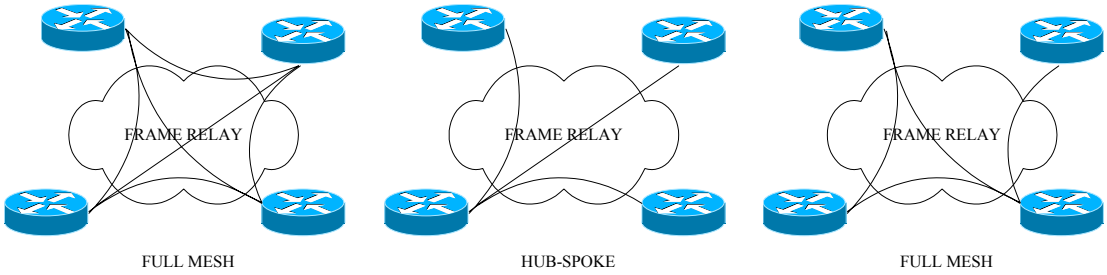
Khi sử dụng phương thức truyền thông X.25, mô hình kết nối cơ bản là điểm-đa điểm (point-to-multipoint) dựa trên tính chất cơ bản của X.25 là sử dụng các VC cho các nhu cầu truyền tải dữ liệu.



Hình 3-42: Mô hình kết nối X.25

Frame Relay đa dạng hơn về các mô hình kết nối. Frame Relay sử dụng các PVC định trước để thực hiện truyền tải dữ liệu giữa hai điểm, người ta chia Frame Relay thành các cấu hình kết nối mạng như mô tả trong hình 3-40. Trong đó:

- Full mesh: là mô hình kết nối mà trong đó bất cứ hai node mạng nào cũng có một PVC liên kết giữa chúng. Mô hình này đảm bảo tính sẵn sàng cho toàn bộ hệ thống mạng, nếu có một hoặc một vài PVC có sự cố, các PVC còn lại vẫn có thể đảm bảo cho kết nối mạng giữa các node mạng. Yếu điểm của mô hình mạng này là chi phí thuê các PVC quá lớn.



Hình 3-43: Mô hình kết nối Frame Relay

- Hub-Spoke: là mô hình có một điểm tập trung mọi kết nối Frame Relay tới các điểm khác, các trao đổi dữ liệu giữa 2 điểm bất kỳ đều phải đi qua điểm tập trung. Mô hình này có chi phí giảm thiểu nhất nhưng có yếu điểm về việc tập trung mọi gánh nặng lên điểm tập trung và nếu có bất kỳ sự cố trên một PVC nào thì sẽ mất khả năng truyền tải dữ liệu với điểm thuộc về PVC bị sự cố đó.

- Partial mesh: là mô hình được sử dụng nhiều nhất, nó là sự lai ghép giữa hai mô hình trên, đảm bảo chi phí và dự phòng cho các điểm thiết yếu.

Cấu hình X.25 cơ bản

Các lưu ý trong cấu hình X.25

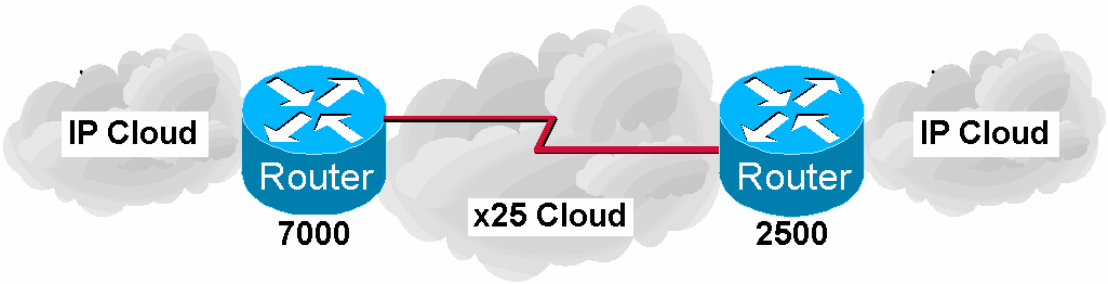
- X.25 là một môi trường đa truy nhập không broadcast (multi access non broadcast media) do đó phải lưu ý khi sử dụng với định tuyến động

- X.25 làm việc với sự khởi tạo các VC do đó khi thực hiện cấu hình phải thực hiện các thủ tục liên kết (map) và định tuyến theo địa chỉ

- Các tham số cần lưu ý

  - Độ lớn gói tin (ips/ops)
  - Độ lớn cửa sổ điều khiển luồng (win/wout)
  - Số lượng kênh VC tối đa cho chiều đến / hai chiều / chiều đi (hic/htc/hoc)
  - Số lượng VC dành cho một kết nối (nvc). Nên hạn chế số lượng VC cho phép kết nối đến một điểm trong giới hạn hợp lý để tổng số VC cần thiết không vượt quá số VC tối đa hiện có (HTC)
  - Khi thực hiện các liên kết (map) phải thực hiện map địa chỉ IP của phía đối phương tới địa chỉ X25 của họ

- Khi thực hiện định tuyến, phải thực hiện định tuyến với địa chỉ IP next hop
- Cấu hình mạng đấu nối X25 là cấu hình đa điểm, địa chỉ đấu nối phải nằm trong lớp mạng con đủ cho số lượng các điểm



Hình 3-44: Mô hình kết nối X.25 cơ bản

```
Cấu hình bộ định tuyến 7000
!
interface Serial1/1
 ip address 10.1.1.2 255.255.255.0
 encapsulation x25
 no ip mroute-cache
!--- Địa chỉ X.121 của gán cho bộ định tuyến 7000
 x25 address 4522973407000
!--- Các dòng lệnh dưới là các tham số X.25
 x25 ips 256
 x25 ops 256
 x25 htc 16
 x25 win 7
 x25 wout 7
!--- Dòng lệnh này dùng để gán địa chỉ IP của bộ định tuyến 2500 với
!địa chỉ X.121 của nó
 x25 map ip 10.1.1.1 4522973402500
!
!
```

Hình 3-45: Cấu hình của bộ định tuyến 7000

```
Cấu hình bộ định tuyến 2500
```

```
!
hostname 2500
!
interface Serial0
 ip address 10.1.1.1 255.255.255.0
 no ip mroute-cache
 encapsulation x25
 bandwidth 56
!--- Địa chỉ X.121 của gán cho bộ định tuyến 7000
 x25 address 4522973402500
!--- Các dòng lệnh dưới là các tham số X.25
 x25 ips 256
 x25 ops 256
 x25 htc 16
 x25 win 7
 x25 wout 7
!--- Dòng lệnh này dùng để gán địa chỉ IP của bộ định tuyến 7000 với
!địa chỉ X.121 của nó
 x25 map ip 10.1.1.1 4522973407000
!
```

Hình 3-46: Cấu hình của bộ định tuyến 2500

- Giám sát:
  - **Show interfaces serial 0:** dùng để kiểm tra trạng thái
  - **Show x25 vc:** hiển thị thông tin kết nối X.25
  - **Show x25 map:** hiển thị các liên kết hiện có của FR

Cấu hình Frame Relay cơ bản

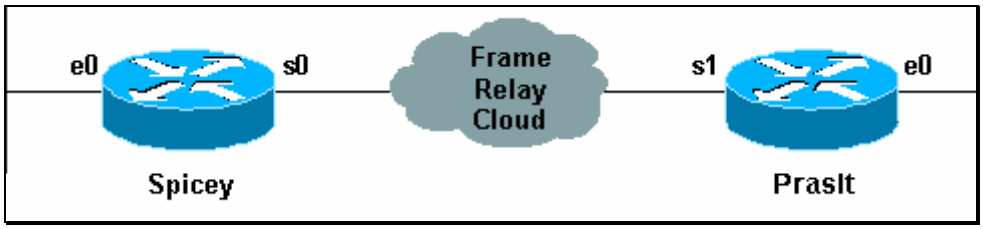
Các lưu ý trong cấu hình Frame Relay:

- Frame Relay là một môi trường đa truy nhập không broadcast (multi access non broadcast media) do đó phải lưu ý khi sử dụng với định tuyến động

- Khi sử dụng định tuyến động giao thức định tuyến vector như RIP, IGRP phải để ý đến luật Split Horizon. Luật Split Horizon là luật không cho

phép các thông tin định tuyến vừa đi vào một giao tiếp đi trở ra chính giao tiếp đó để tránh việc cập nhật sai các thông tin về định tuyến dẫn đến việc vòng đi vòng lại của các thông tin định tuyến. Vấn đề này được đặt ra do có nhiều PVC cùng chạy trên một giao tiếp vật lý.

- Giám sát:
  - **Show interfaces serial 0:** dùng để kiểm tra DLCI, LMI
  - **Show frame-relay lmi:** hiển thị thông tin tổng hợp về LMI
  - **Show frame-relay map:** hiển thị các liên kết hiện có của FR
  - **Show frame-relay pvc:** hiển thị các thông số của PVC
  - **Show frame-relay traffic:** hiển thị traffic



Hình 3-47: Mô hình kết nối Frame Relay cơ bản

- Để bắt đầu cấu hình mạng:
  - **Router> enable** ↵
  - **Password: ******** ↵
  - **Router# config terminale** ↵
  - **Router(config)#**

- Thực hiện đặt tên, các mật khẩu, cấu hình cho phép telnet và các điều kiện cần thiết trước khi cấu hình các giao diện

- Cấu hình
  - **Spicey(config)# interface serial 0** ↵

- Lựa chọn giao thức sử dụng
  - **Spicey(config-if)# encapsolation frame-relay** ↵

- Xác định giao thức quản trị LMI. Giao thức quản trị LMI nhất thiết phải có để đảm bảo việc trao đổi thông tin hai chiều giữa thiết bị đầu cuối và thiết bị mạng Frame Relay. LMI hoạt động như một thông báo keepalive.
  - **Spicey(config-if)# frame-relay lmi-type cisco** ↵

- Gán DLCI được cấp cho giao tiếp.
  - **Spicey(config-if)# frame-relay interface-dlci 140 ↵**
- Đặt địa chỉ IP cho giao tiếp kết nối leased-line
  - **Spicey(config-if)# ip address 3.1.3.1 255.255.255.0 ↵**
- Luôn phải đưa giao tiếp vào sử dụng bằng lệnh no shutdown
  - **Spicey(config-if)# no shutdown ↵**
  - **Spicey(config-if)# exit ↵**
- Sử dụng định tuyến động RIP
  - **Spicey(config)# router rip ↵**
  - **Spicey(config-router)# network 3.0.0.0 ↵**
  - **Spicey(config-router)# network 124.0.0.0 ↵**
  - **Spicey(config-router)# end ↵**
- Luôn phải ghi lại cấu hình khi đã cấu hình xong
  - **Spicey# write memory ↵**
- Thực hiện các phần việc còn lại tại các bộ định tuyến khác, chú ý về giao thức được sử dụng kiểm tra, giám sát các kết nối.

Cấu hình bộ định tuyến Spicey

```
Current configuration : 1705 bytes
!
version 12.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Spicey
!
interface Ethernet0
 ip address 124.124.124.1 255.255.255.0
!
interface Serial0
```

```
 ip address 3.1.3.1 255.255.255.0
 encapsulation frame-relay
 frame-relay interface-dlci 140
!
!
router rip
 network 3.0.0.0
 network 124.0.0.0
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

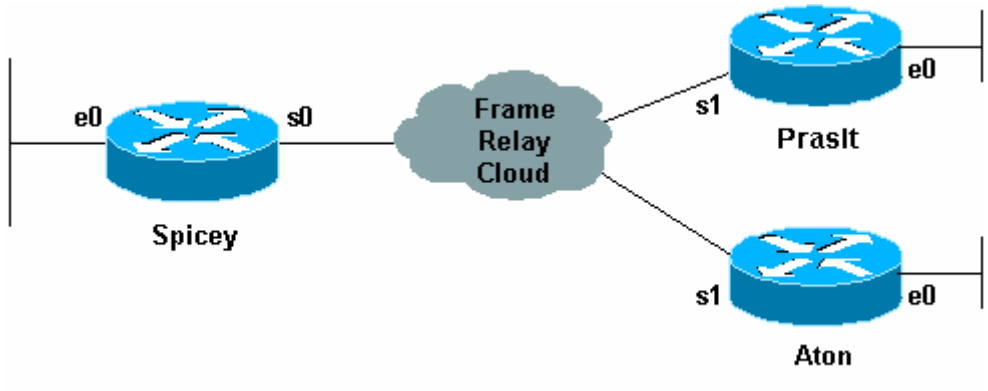
Hình 3-48: Cấu hình của bộ định tuyến Spicey

Cấu hình bộ định tuyến Prasit

```
Current configuration : 1499 bytes
!
version 12.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Prasit
!
!
!
interface Ethernet0
 ip address 123.123.123.1 255.255.255.0
```

```
!
!
interface Serial1
 ip address 3.1.3.2 255.255.255.0
 encapsulation frame-relay
 frame-relay interface-dlci 150
!
!
router rip
 network 3.0.0.0
 network 123.0.0.0
!
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Hình 3-49: Cấu hình của bộ định tuyến Prasit



Hình 3-50: Mô hình kết nối Frame Relay Hub-Spoke

- Cấu hình

o `Spicey(config)# interface serial 0 ↵`

- Lựa chọn giao thức sử dụng

```
Spicey(config-if)# encapsolation frame-relay ↵
```

- Xác định giao thức quản trị LMI. Lưu ý trong ví dụ này có sử dụng một chuẩn kết nối LMI khác. Chuẩn kết nối LMI không có giá trị toàn cục mà chỉ có giá trị tại giao tiếp của thiết bị đầu cuối với mạng Frame Relay. Trong cấu hình của các bộ định tuyến khác vẫn sử dụng LMI chuẩn cisco.

```
Spicey(config-if)# frame-relay lmi-type ansi ↵
```

- Luôn phải đưa giao tiếp vào sử dụng bằng lệnh no shutdown

```
Spicey(config-if)# no shutdown ↵
```

- Trong ví dụ này, sử dụng giao tiếp con, subinterface, nên không đặt địa chỉ cho giao tiếp thực, physical interface.

- Cấu hình giao tiếp con. Giao tiếp con phải sử dụng một trong hai lựa chọn là point-to-point hoặc multipoint, ở đây sử dụng point-to-point cho giao tiếp con s0.1 và multipoint cho giao tiếp con s0.2.

```
Spicey(config-if)# interface serial 0.1 point-to-point ↵
```

- Hoặc

```
Spicey(config-if)# exit ↵
Spicey(config)# interface serial 0.1 point-to-point ↵
```

- Gán DLCI được cấp cho giao tiếp. DLCI 140 là DLCI gắn với PVC nối giữa Spicey và Prasit, còn DLCI 130 gắn với PVC nối tới Aton.

```
Spicey(config-if)# frame-relay interface-dlci 140 ↵
```

- Xác lập địa chỉ IP cho giao tiếp con thứ nhất

```
Spicey(config-subif)# ip address 4.0.1.1 255.255.255.0 ↵
Spicey(config-subif)# exit ↵
```

- Cấu hình giao tiếp con thứ hai tới Aton

```
Spicey(config)# interface serial 0.2 multipoint ↵
```

- Gán DLCI được cấp cho giao tiếp là DLCI 130

```
Spicey(config-if)# frame-relay interface-dlci 130 ↵
```

- Xác lập địa chỉ IP cho giao tiếp con thứ 2

```
Spicey(config-subif)# ip address 3.1.3.1 255.255.255.0 ↵
Spicey(config-subif)# exit ↵
```

- Sử dụng định tuyến động RIP

```
Spicey(config)# router rip ↵
Spicey(config-router)# network 3.0.0.0 ↵
Spicey(config-router)# network 4.0.0.0 ↵
Spicey(config-router)# network 124.0.0.0 ↵
Spicey(config-router)# end ↵
```

- Luôn phải ghi lại cấu hình khi đã cấu hình xong

```
Spicey# write memory ↵
```

- Thực hiện các phần việc còn lại tại các bộ định tuyến khác, chú ý về giao thức được sử dụng kiểm tra, giám sát các kết nối.

Cấu hình bộ định tuyến Spicey

```
Spicey#show running-config
Building configuration...
!
version 12.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Spicey
!
!
interface Ethernet0
 ip address 124.124.124.1 255.255.255.0
!
interface Serial0
 no ip address
 encapsulation frame-relay
 frame-relay lmi-type ansi
!
```

```
interface Serial0.1 point-to-point
 ip address 4.0.1.1 255.255.255.0
 frame-relay interface-dlci 140
!
interface Serial0.2 multipoint
 ip address 3.1.3.1 255.255.255.0
 frame-relay interface-dlci 130
!
router igrp 2
 network 3.0.0.0
 network 4.0.0.0
 network 124.0.0.0
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Hình 3-51: Cấu hình của bộ định tuyến Spicey

```
Cấu hình bộ định tuyến Prasit

Prasit#show running-config
Building configuration...

version 12.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
```

```
hostname Prasit
!
interface Ethernet0
 ip address 123.123.123.1 255.255.255.0
!
interface Serial1
 no ip address
 encapsulation frame-relay
!
!--- LMI cisco là mặc định nên không thể hiện trong cấu hình
!--- Prasit và Spicey đã sử dụng 2 kiểu LMI khác nhau
!--- Bộ định tuyến tại Prasit sử dụng giao tiếp con point-to-point
interface Serial1.1 point-to-point
 ip address 4.0.1.2 255.255.255.0
 frame-relay interface-dlci 150
!
router igrp 2
 network 4.0.0.0
 network 123.0.0.0
!
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Hình 3-52: Cấu hình của bộ định tuyến Prasit

```
Cấu hình bộ định tuyến Aton

Aton#show running-config
```

```
Building configuration...


Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
!
hostname Aton
!
!
!
interface Ethernet0
 ip address 122.122.122.1 255.255.255.0
!
interface Serial1
 ip address 3.1.3.3 255.255.255.0
 encapsulation frame-relay
 frame-relay lmi-type q933a
!--- Aton có kiểu LMI khác hai bộ định tuyến kia
!--- Aton không sử dụng giao tiếp con. Giao tiếp con cần xác định
!là point-to-point hay multipoint ở bộ định tuyến trung tâm
!còn ở các bộ định tuyến còn lại có thể dùng giao tiếp con
!point-to-point hay giao tiếp thực, physical interface
 frame-relay interface-dlci 160
!
router igrp 2
 network 3.0.0.0
 network 122.0.0.0
!
line con 0
 exec-timeout 0 0
 transport input none
```

```
line aux 0
line vty 0 4
 login
!
end
```

Hình 3-53: Cấu hình của bộ định tuyến Aton

IV.3. Cấu hình Dial-up

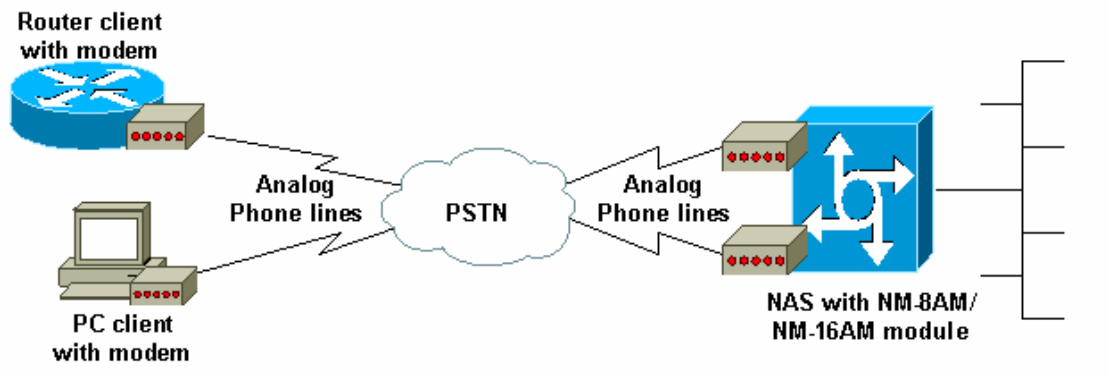
Giới thiệu quay số

Kết nối quay số cho phép sử dụng đường điện thoại để kết nối trao đổi dữ liệu. Tốc độ của kết nối quay số là không cao và chỉ có thể đáp ứng được cho các ứng dụng không yêu cầu về băng thông cũng như thời gian trễ.

Kết nối quay số sử dụng modem V34, V90 là phổ biến. Tốc độ truyền dữ liệu lên mạng và tải dữ liệu về tối đa là 33,6Kbps. Để có thể thực hiện tải về với tốc độ lớn hơn, tới 56Kbps, bộ định tuyến đóng vai trò điểm truy nhập phải có kết nối thuê bao dạng số và dùng modem số.

Đối với các doanh nghiệp nhỏ, việc xác thực người dùng có thể thực hiện bằng cách khai báo dữ liệu trực tiếp trên bộ định tuyến. Cách sử dụng này không thích hợp cho các doanh nghiệp vừa và lớn hay các doanh nghiệp cần có sự quản lý chặt chẽ người dùng một cách hệ thống. Lúc này cần thiết có các hệ thống quản lý người dùng. Các bộ định tuyến của Cisco cho phép sử dụng hai chuẩn xác thực TACACS+ và RADIUS.

Mô hình sử dụng quay số



Hình 3-54: Cấu hình của bộ định tuyến Aton

Cấu hình quay số cơ bản

Danh mục công việc:

- Cấu hình giao tiếp không đồng bộ Async
- Cấu hình giao tiếp điều khiển modem
- Cấu hình xác thực
- Giám sát
  - **Router#show interface Async 1**
  - **Router#show line 1**
  - **Router#debug ppp authentication**

Cấu hình quay số cơ bản

```
Current configuration : 1251 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
!
hostname cisco3640
!
boot system flash:c3640-i-mz.122-8.T
enable secret 5 <đã xóa>
!
! --- Tên truy nhập cho xác thực người dùng cục bộ
username abc password 0 abc
!
ip subnet-zero
!
no ip domain-lookup
ip domain-name cisco.com
```

```
!
! --- Xác định địa chỉ máy chủ DNS cho các máy trạm quay số
async-bootp dns-server 5.5.5.1 5.5.5.2
!
!
interface Loopback0
  ip address 1.1.1.1 255.255.255.0
!
interface Ethernet2/0
  ip address 20.20.20.1 255.255.255.0
  half-duplex
!
! <<--các giao tiếp không dùng được bỏ đi
!
!--- Giao tiếp Group-Async1 cấu hình cho tất cả các các modem
!--- không cần cấu hình riêng rẽ từng modem
interface Group-Async1
  ip unnumbered Loopback0
  encapsulation ppp
  dialer in-band
!--- Xác lập thời gian không sử dụng là 10 phút
!--- sau thời gian này, bộ định tuyến sẽ tự động cắt kết nối
  dialer idle-timeout 600
!--- Định nghĩa các loại hình dữ liệu được dùng
!--- thông qua cấu hình dialer-group và dialer-list
  dialer-group 1
!--- Chế độ interative cho phép người dùng sử dụng nhiều giao thức
!--- để không cho phép người dùng thiết lập các kết nối đến bộ định
tuyến sử dụng chế độ dedicated
  async mode interactive
!--- Các máy trạm khi quay số vào sẽ được cấp địa chỉ IP
!--- được qui định trong DIALIN
  peer default ip address pool DIALIN
  ppp authentication chap
```

```
!--- Xác lập các modem từ line 1 đến line 8 thuộc về nhóm này
  group-range 1 8
!
ip local pool DIALIN 10.1.1.1 10.1.1.10
ip classless
ip route 0.0.0.0 0.0.0.0 20.20.20.100
ip http server
ip pim bidir-enable
!
!--- Dòng lệnh sau cho phép giao thức IP là giao thức hoạt động
!--- nếu không có các dữ liệu IP đi qua sau khoảng thời gian 10 phút
!--- đường kết nối sẽ bị cắt
dialer-list 1 protocol ip permit
!
line con 0
  password abc
line 1 8
!--- Dòng lệnh dưới cho phép modem quay vào và quay ra
  modem InOut
  transport input all
  autoselect ppp
  flowcontrol hardware
line aux 0
line vty 0 4
  login
!
!
end
```

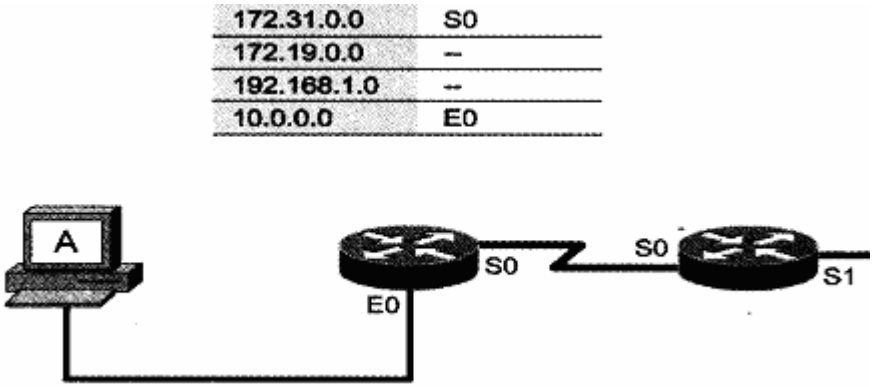
Hình 3-55: Cấu hình quay số cơ bản

IV.4. Định tuyến tĩnh và động

Sơ lược về định tuyến

Chức năng xác định đường dẫn cho phép bộ định tuyến ước lượng các đường dẫn khả thi để đến đích và thiết lập sự kiểm soát các gói tin. Bộ định tuyến sử dụng các cấu hình mạng để đánh giá các đường dẫn mạng. Thông tin này có thể được cấu hình bởi người quản trị mạng hay được thu thập thông qua quá trình xử lý động được thực thi trên mạng.

Lớp mạng dùng bảng định tuyến IP để gửi các gói tin từ mạng nguồn đến mạng đích. Bộ định tuyến dựa vào các thông tin được giữ trong bảng định tuyến để quyết định truyền tải các gói tin theo các giao tiếp thích hợp.



Hình 3-56: Sử dụng bảng định tuyến để truyền tải các gói tin

Một bảng định tuyến IP bao gồm các địa chỉ mạng đích, địa chỉ của điểm cần đi qua, giá trị định tuyến và giao tiếp để thực hiện việc truyền tải. Khi không có thông tin về mạng đích, bộ định tuyến sẽ gửi các gói tin theo một đường dẫn mặc định được cấu hình trên bộ định tuyến, nếu đường dẫn không tồn tại, bộ định tuyến tự động loại bỏ gói tin.

Có hai phương thức định tuyến là:

- Định tuyến tĩnh (static routing): là cách định tuyến không sử dụng các giao thức định tuyến. Các định tuyến đến một mạng đích sẽ được thực hiện một cách cố định không thay đổi trên mỗi bộ định tuyến. Mỗi khi thực hiện việc thêm hay bớt các mạng, phải thực hiện thay đổi cấu hình trên mỗi bộ định tuyến.

- Định tuyến động (dynamic routing): là việc sử dụng các giao thức định tuyến để thực hiện xây dựng nên các bảng định tuyến trên các bộ định tuyến. Các bộ định tuyến thông qua các giao thức định tuyến sẽ tự động trao đổi các

thông tin định tuyến, các bảng định tuyến với nhau. Mỗi khi có sự thay đổi về mạng, chỉ cần khai báo thông tin mạng mới trên bộ định tuyến quản lý trực tiếp mạng mới đó mà không cần phải khai báo lại trên mỗi bộ định tuyến. Một số giao thức định tuyến động được sử dụng là RIP, RIPv2, OSPF, EIGRP v.v...

Giá trị định tuyến được xây dựng tùy theo các giao thức định tuyến khác nhau. Giá trị định tuyến của các kết nối trực tiếp và định tuyến tĩnh có giá trị nhỏ nhất bằng 0, đối với định tuyến động thì giá trị định tuyến được tính toán tùy thuộc và từng giao thức cụ thể. Giá trị định tuyến được thể hiện trong bảng định tuyến là giá trị định tuyến tốt nhất đã được bộ định tuyến tính toán và xây dựng nên trên cơ sở các giao thức định tuyến được cấu hình và giá trị định tuyến của từng giao thức.

Các giao thức định tuyến động được chia thành 2 nhóm chính:

- **Các giao thức định tuyến khoảng cách véc tơ** (distance-vecto, *sau đây được gọi tắt là định tuyến vectơ)*: dựa vào các giải thuật định tuyến có cơ sở hoạt động là khoảng cách véc tơ.

Theo định kỳ các bộ định tuyến chuyển toàn bộ các thông tin có trong bảng định tuyến đến các bộ định tuyến láng giềng đấu nối trực tiếp với nó và cũng theo định kỳ nhận các bảng định tuyến từ các bộ định tuyến láng giềng. Sau khi nhận được các bảng định tuyến từ các bộ định tuyến láng giềng, bộ định tuyến sẽ so sánh với bảng định tuyến hiện có và quyết định về việc xây dựng lại bảng định tuyến theo thuật toán của từng giao thức hay không. Trong trường hợp phải xây dựng lại, bộ định tuyến sau đó sẽ gửi bảng định tuyến mới cho các láng giềng và các láng giềng lại thực hiện các công việc tương tự. Các bộ định tuyến tự xác định các láng giềng trên cơ sở thuật toán và các thông tin thu lượm từ mạng.

Từ việc cần thiết phải gửi các bảng định tuyến mới lại cho các láng giềng và các láng giềng sau khi xây dựng lại bảng định tuyến lại gửi trở lại bảng định tuyến mới, định tuyến thành vòng có thể xảy ra nếu sự hội về trạng thái bền vững của mạng diễn ra chậm trên một cấu hình mới. Các bộ định tuyến sử dụng các kỹ thuật bộ đếm định thời để đảm bảo không nảy sinh việc xây dựng một bảng định tuyến sai. Có thể diễn giải điều đó như sau:

- Khi một bộ định tuyến nhận một cập nhật từ một láng giềng chỉ rằng một mạng có thể truy xuất trước đây, nay không thể truy xuất được nữa, bộ

định tuyến đánh dấu tuyến là không thể truy xuất và khởi động một bộ định thời.

o Nếu tại bất cứ thời điểm nào mà trước khi bộ định thời hết hạn một cập nhật được tiếp nhận cũng từ láng giềng đó chỉ ra rằng mạng đã được truy xuất trở lại, bộ định tuyến đánh dấu là mạng có thể truy xuất và giải phóng bộ định thời.

o Nếu một cập nhật đến từ một bộ định tuyến láng giềng khác với giá trị định tuyến tốt hơn giá trị định tuyến được ghi cho mạng này, bộ định tuyến đánh dấu mạng có thể truy xuất và giải phóng bộ định thời. Nếu giá trị định tuyến tồi hơn, cập nhật được bỏ qua.

o Khi bộ định thời được đếm về 0, giá trị định tuyến mới được xác lập, bộ định tuyến có bảng định tuyến mới.

- **Các giao thức định tuyến trạng thái đường** (link-state, *gọi tắt là định tuyến trạng thái*): Giải thuật cơ bản thứ hai được dùng cho định tuyến là giải thuật 1ink-state. Các giải thuật định tuyến trạng thái, cũng được gọi là SPF (shortest path first, *chọn đường dẫn ngắn nhất*), duy trì một cơ sở dừ liệu phức tạp chứa thông tin về cấu hình mạng.

- Trong khi giải thuật vectơ không có thông tin đặc biệt gì về các mạng ở xa và cũng không biết các bộ định tuyến ở xa, giải thuật định tuyến trạng thái biết được đầy đủ về các bộ định tuyến ở xa và biết được chúng liên kết với nhau như thế nào.

Giao thức định tuyến trạng thái sử dụng:

o Các thông báo về trạng thái liên kết: LSA (Link State Advertisements).

o Một cơ sở dữ liệu về cấu hình mạng.

o Giải thuật SPF, và cây SPF sau cùng.

o Một bảng định tuyến liên hệ các đường dẫn và các cổng đến từng mạng.

Hoạt động tìm hiểu khám phá mạng trong định tuyến trạng thái được thực hiện như sau:

o Các bộ định tuyến trao đổi các LSA cho nhau. Mỗi bộ định tuyến bắt đầu với các mạng được kết nối trực tiếp để lấy thông tin.

- Mỗi bộ định tuyến đồng thời với các bộ định tuyến khác tiến hành xây dựng một cơ sở dữ liệu về cấu hình mạng bao gồm tất cả các LSA đến từ liên mạng.

- Giải thuật SPF tính toán mạng có thể đạt đến. Bộ định tuyến xây dựng cấu hình mạng luận lý này như một cây, tự nó là gốc, gồm tất cả các đường dẫn có thể đến mỗi mạng trong toàn bộ mạng đang chạy giao thức định tuyến trạng thái. Sau đó, nó sắp xếp các đường dẫn này theo chiến lược chọn đường dẫn ngắn nhất.

- Bộ định tuyến liệt kê các đường dẫn tốt nhất của nó, và các cổng dẫn đến các mạng đích, trong bảng định tuyến của nó. Nó cũng duy trì các cơ sở dữ liệu khác về các phần tử cấu hình mạng và các chi tiết về hiện trạng của mạng.

Khi có thay đổi về cấu hình mạng, bộ định tuyến đầu tiên nhận biết được sự thay đổi này gửi thông tin đến các bộ định tuyến khác hay đến một bộ định tuyến định trước được gán là tham chiếu cho tất cả các các bộ định tuyến trên mạng làm căn cứ cập nhật.

- Theo dõi các láng giềng của nó, xem xét có hoạt động hay không, và giá trị định tuyến đến láng giềng đó.

- Tạo một gói LSA trong đó liệt kê tên của tất cả các bộ định tuyến láng giềng và các giá trị định tuyến đối với các láng giềng mới, các thay đổi trong giá trị định tuyến, và các liên kết dẫn đến các láng giềng đã được ghi.

- Gửi gói LSA này đi sao cho tất cả các bộ định tuyến đều nhận được.

- Khi nhận một gói LSA, ghi gói LSA vào cơ sở dữ liệu để sao cho cập nhật gói LSA mới nhất được phát ra từ mỗi bộ định tuyến.

- Hoàn thành bản đồ của liên mạng bằng cách dùng dữ liệu từ các gói LSA tích lũy được và sau đó tính toán các tuyến dẫn đến tất cả các mạng khác sử dụng thuật toán SPF.

Có hai vấn đề lưu ý đối với giao thức định tuyến trạng thái:

- Hoạt động của các giao thức định tuyến trạng thái trong hầu hết các trường hợp đều yêu cầu các bộ định tuyến dùng nhiều bộ nhớ và thực thi nhiều hơn so với các giao thức định tuyến theo vectơ. Các yêu cầu này xuất phát từ việc cần thiết phải lưu trữ thông tin của tất cả các láng giềng, cơ sở dữ liệu mạng đến từ các nơi khác và việc thực thi các thuật toán định tuyến trạng thái.

Người quản lý mạng phải đảm bảo rằng các bộ định tuyến mà họ chọn có khả năng cung cấp các tài nguyên cần thiết này.

o Các nhu cầu về băng thông cần phải tiêu tốn để khởi động sự phát tán gói trạng thái. Trong khi khởi động quá trình khám phá, tất cả các bộ định tuyến dùng các giao thức định tuyến trạng thái để gửi các gói LSA đến tất cả các bộ định tuyến khác. Hành động này làm tràn ngập mạng khi mà các bộ định tuyến đồng loạt yêu cầu băng thông và tạm thời làm giảm lượng băng thông khả dụng dùng cho lưu lượng dữ liệu thực được định tuyến. Sau khởi động phát tán này, các giao thức định tuyến trạng thái thường chỉ yêu cầu một lượng băng thông tối thiểu để gửi các gói LSA kích hoạt sự kiện không thường xuyên nhằm phản ánh sự thay đổi của cấu hình mạng.

- **Và một nhóm giao thức thứ 3** là nhóm các giao thức định tuyến lai ghép giữa 2 nhóm trên hay nói cách khác có các tính chất của cả hai nhóm giao thức trên.

Các giao thức định tuyến

Bảng 3-10:Các giao thức định tuyến

Các đặc trưng	RIPv1	RIPv2	IRGP	EIGRP	OSPF
Khoảng cách vectơ	x	x	x	x	
Trạng thái đường					x
Tự động tóm tắt định tuyến	x	x	x	x	
Hỗ trợ VLSM[1]		x		x	x
Tương thích với sản phẩm thứ ba	x	x			x
Thích hợp	Nhỏ	Nhỏ	Vừa	Lớn	Lớn

[1] VLSM (Vary Length Subnet Mask): hỗ trợ định tuyến cho các mạng con subnetmask có độ dài thay đổi hay nói cách khác thông tin về subnetmask bao gồm trong bảng định tuyến

Thời gian hội tụ về trạng thái cân bằng	Chậm	Chậm	Chậm	Nhanh	Nhanh
Giá trị định tuyến	hop count[2]	hop count	~ BW[3]+D[4]	~ BW+D	~ 10E8/BW
Giới hạn hop count	15	15	100	100	
Cân bằng tải cùng giá trị định tuyến	x	x	x	x	x
Cân bằng tải không cùng giá trị định tuyến			x	x	
Thuật toán	Bellman-Ford	Bellman-Ford	Bellman-Ford	DUAL	Dijkstra

Cấu hình định tuyến động cơ bản với RIP

Một số lưu ý khi cấu hình định tuyến động với RIP

- RIP gửi các thông tin cập nhật theo các chu kỳ định trước, giá trị mặc định là 30 giây, và khi có sự thay đổi bảng định tuyến.

- RIP sử dụng số đếm các node (hop count) để làm giá trị đánh giá chất lượng của định tuyến (metric). RIP chỉ giữ duy nhất định tuyến có giá trị định tuyến thấp nhất.

- Giá trị hop count tối đa cho phép là 15.

- RIP sử dụng các bộ đếm thời gian cho việc thực hiện gửi các thông tin cập nhật, xoá bỏ một định tuyến trong bảng cũng như để điều khiển các quá trình tạo lập bảng định tuyến, tránh loop vòng.

- RIPv1: Classfull: không có thông tin về subnetmask

- RIPv2: Classless: có thông tin về subnetmask

[2] Hop count: được tính bằng số các điểm node mạng mà gói tin phải đi qua từ điểm này đến điểm kia hay chính bằng số các bộ định tuyến mà gói tin phải đi qua

[3] BW (bandwitch): băng thông

[4] D (delay): trễ

Cấu hình định tuyến với RIP:

- Cho phép giao thức định tuyến RIP hoạt động trên bộ định tuyến.

```
Router(config)#router rip
```

- Thiết lập các cấu hình mạng. Network là nhóm mạng tính theo lớp mạng cơ bản đang có các giao tiếp trực tiếp trên bộ định tuyến.

```
Router(config-router)#network 192.168.100.0
Router(config-router)#network 172.25.0.0
Router(config-router)#network 10.0.0.0
```

- Trong trường hợp sử dụng RIP với các mạng không phải là mạng broadcast như X.25, Frame Relay cần thiết cấu hình RIP với các địa chỉ Unicast là các địa chỉ mà RIP sẽ gửi tới các thông tin cập nhật

```
Router(config-router)#neighbor 192.168.113.1
Router(config-router)#neighbor 192.168.113.5
```

- Tuỳ theo điều kiện cụ thể về hạ tầng mạng có thể thay đổi chu kỳ cập nhật thông tin, các định nghĩa thời gian khác cho phù hợp.

```
Router(config-router)# timers basic update invalid holddown flush [sleeptime]
```

- Các thay đổi khác.

```
Router(config-router)# version {1 | 2}
Router(config-router)# ip rip authentication key-chain name-of-chain
Router(config-router)# ip rip authentication mode {text | md5}
```

- Giám sát.

```
show ip interfaces
show ip rip
```

Cấu hình bộ định tuyến với RIP

```
Current configuration : 1499 bytes
!
version 12.1
service timestamps debug datetime msec
service timestamps log datetime msec
```

```
no service password-encryption
!
hostname Prasit
!
!
interface Ethernet0
 ip address 123.123.123.1 255.255.255.0
!
!
interface Serial1
 ip address 3.1.3.2 255.255.255.0
 encapsulation frame-relay
 frame-relay interface-dlci 150
!
!
router rip
 network 3.0.0.0
 network 123.0.0.0
!
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Hình 3-57: Cấu hình của bộ định tuyến với RIP

V. Bài tập thực hành sử dụng bộ định tuyến Cisco

Bài 1: Thực hành nhận diện thiết bị, đấu nối thiết bị

Yêu cầu:

- Nhận diện đúng các chủng loại thiết bị
- Nhận diện các giao tiếp của bộ định tuyến, ý nghĩa và mục đích sử dụng
- Biết cách sử dụng các loại cáp với từng loại thiết bị, giao tiếp khác nhau
- Biết đấu nối bộ định tuyến với nhau và với các thiết bị modem khác
- Sử dụng phần mềm HyperTerminal kết nối với bộ định tuyến

Bài 2: Thực hành các lệnh cơ bản

- Các lệnh show
- Lệnh config

Yêu cầu:

- Nắm vững ý và sử dụng thành thạo các lệnh kiểm tra và các lệnh cấu hình cơ bản

Bài 3: Cấu hình bộ định tuyến với mô hình đấu nối leased-line

- Cấu hình Interface
- Cấu hình giao thức
- Cấu hình định tuyến

Yêu cầu:

- Sử dụng thiết bị phòng lab để cấu hình một kết nối leased-line cho phép kết nối 2 mạng với nhau.
- Vận dụng các kiến thức đã học kiểm soát và xử lý sự cố.

Bài 4: Cấu hình bộ định tuyến với Dial-up

- Cấu hình line vật lý
- Cấu hình async interface
- Cấu hình định tuyến
- Cấu hình xác thực

Yêu cầu:

- Sử dụng thiết bị phòng lab để cấu hình một điểm truy nhập gián tiếp quay số qua thoại.
- Vận dụng các kiến thức đã học kiểm soát và xử lý sự cố.

Thiết bị phòng lab

- 02 bộ định tuyến 2509 (leased-line và async) hoặc tương đương
- 02 modem leased-line CSU/DSU dùng cho kết nối leased-line
- 02 cáp V.35 DTE
- 04 modem dial-up 56kbps
- 02 cáp Async dùng cho kết nối modem 56kbps
- Phần mềm giả lập bộ định tuyến (router simulator)
- 02 máy tính dùng để cấu hình trực tiếp các bộ định tuyến
- các máy tính để thực hành trên phần mềm giả lập bộ định tuyến
- 04 đường điện thoại

Chương 4 : Hệ thống tên miền DNS

Chương 4 sẽ tập trung nghiên cứu về hệ thống tên miền là một hệ thống định danh phổ biến trên mạng TCP/IP nói chung và đặc biệt là mạng Internet.

Hệ thống tên miền tối quan trọng cho sự phát triển của các ứng dụng phổ biến như thư tín điện tử, web...Cấu trúc hệ thống tên miền, cấu trúc và ý nghĩa của các trường tên miền cũng như các kỹ năng cơ bản được cung cấp sẽ giúp cho người quản trị có thể hoạch định được các nhu cầu liên quan đến tên miền cho mạng lưới, tiến hành thủ tục đăng ký chính xác (nếu đăng ký tên miền Internet) và đảm nhận được các công tác tạo mới, sửa đổi ... hay nói chung là các công việc quản trị hệ thống máy chủ tên miền DNS

Chương 4 đòi hỏi các học viên phải quen thuộc với địa chỉ IP, việc soạn thảo quản trị các tiến trình trên các hệ thống linux, unix, windows.

I. Giới thiệu

I.1. Lịch sử hình thành của DNS

Vào những năm 1970 mạng ARPanet của bộ quốc phòng Mỹ rất nhỏ và dễ dàng quản lý các liên kết vài trăm máy tính với nhau. Do đó mạng chỉ cần một file HOSTS.TXT chứa tất cả thông tin cần thiết về máy tính trong mạng và giúp các máy tính chuyển đổi được thông tin địa chỉ và tên mạng cho tất cả máy tính trong mạng ARPanet một cách dễ dàng. Và đó chính là bước khởi đầu của hệ thống tên miền gọi tắt là DNS (Domain name system)

Như khi mạng máy tính ARPanet ngày càng phát triển thì việc quản lý thông tin chỉ dựa vào một file HOSTS.TXT là rất khó khăn và không khả thi. Vì thông tin bổ xung và sửa đổi vào file HOSTS.TXT ngày càng nhiều và nhất là khi ARPanet phát triển hệ thống máy tính dựa trên giao thức TCP/IP dẫn đến sự phát triển tăng vọt của mạng máy tính:

- Lưu lượng và trao đổi trên mạng tăng lên
- Tên miền trên mạng và địa chỉ ngày càng nhiều
- Mật độ máy tính ngày càng cao do đó đảm bảo phát triển ngày càng khó khăn

Đến năm 1984 Paul Mockpetris thuộc viện USC's Information Sciences Institute phát triển một hệ thống quản lý tên miền mới (miêu tả trong chuẩn RFC 882 - 883) gọi là DNS (Domain Name System) và ngày này nó ngày càng

được phát triển và hiệu chỉnh bổ xung tính năng để đảm bảo yêu cầu ngày càng cao của hệ thống (hiện nay dns được tiêu chuẩn theo chuẩn RFC 1034 - 1035)

1.2.Mục đích của hệ thống DNS

Máy tính khi kết nối vào mạng Internet thì được gán cho một địa chỉ IP xác định. Địa chỉ IP của mỗi máy là duy nhất và có thể giúp máy tính có thể xác định đường đi đến một máy tính khác một cách dễ dàng. Như đối với người dùng thì địa chỉ IP là rất khó nhớ. Do vậy cần phải sử dụng một hệ thống để giúp cho máy tính tính toán đường đi một cách dễ dàng và đồng thời cũng giúp người dùng dễ nhớ. Do vậy hệ thống DNS ra đời nhằm giúp cho người dùng có thể chuyển đổi từ địa chỉ IP khó nhớ mà máy tính sử dụng sang một tên dễ nhớ cho người sử dụng và đồng thời nó giúp cho hệ thống Internet dễ dàng sử dụng để liên lạc và ngày càng phát triển.

Hệ thống DNS sử dụng hệ thống cơ sở dữ liệu phân tán và phân cấp hình cây do đó việc quản lý sẽ dễ dàng và cũng rất thuận tiện cho việc chuyển đổi từ tên miền sang địa chỉ IP và ngược lại. Cũng giống như mô hình quản lý cá nhân của một đất nước mỗi cá nhân sẽ có một tên xác định đồng thời cũng có địa chỉ chứng minh thư để giúp quản lý con người một cách dễ dàng hơn (nhưng khác là tên miền không được trùng nhau còn tên người thì vẫn có thể trùng nhau)

Mỗi cá nhấn đều có một số căn cước để quản lý

Mỗi một địa chỉ IP tương ứng với một tên miền

Vậy tóm lại tên miền là (domain name) gì ? những tên gợi nhớ như home.vnn.vn hoặc www.cnn.com thì được gọi là tên miền (domain name hoặc dns name). Nó giúp cho người sử dụng dễ dàng nhớ vì nó ở dạng chữ mà người bình thường có thể hiểu và sử dụng hàng ngày.

Hệ thống DNS đã giúp cho mạng Internt thân thiện hơn với người sử dụng do đó mạng internet phát triển bùng nổ một vài năm lại đây. Theo thống trên thế giới vào thời điểm tháng 7/2000 số lượng tên miền được đăng ký là 93.000.000

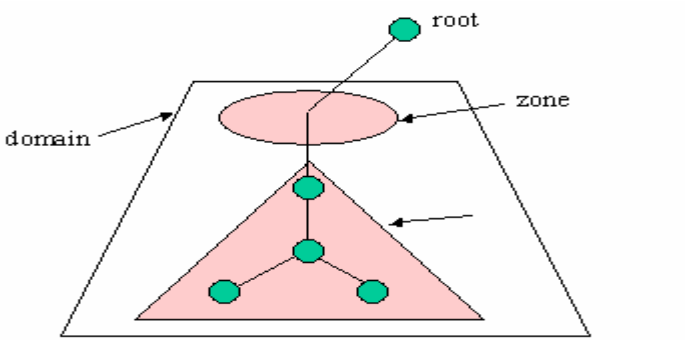
Tóm lại mục đích của hệ thống DNS là:

- Địa chỉ IP khó nhớ cho người sử dụng nhưng dễ dàng với máy tính
- Tên thì dễ nhớ với người sử dụng như không dùng được với máy tính
- Hệ thống DNS giúp chuyển đổi từ tên miền sang địa chỉ IP và ngược lại giúp người dùng dễ dàng sử dụng hệ thống máy tính

II. DNS server và cấu trúc cơ sở dữ liệu tên miền

II.1.Cấu trúc cơ sở dữ liệu

Cơ sở dữ liệu của hệ thống DNS là hệ thống cơ sở dữ liệu phân tán và phân cấp hình cây. Với .Root server là đỉnh của cây và sau đó các domain được phân nhánh dần xuống dưới và phần quyền quản lý. Khi một client truy vấn một tên miền nó sẽ lần lượt đi từ root phân cấp lần lượt xuống dưới để đến dns quản lý domain cần truy vấn.



Cấu trúc của dữ liệu được phân cấp hình cây root quản lý toàn bộ sơ đồ và phân quyền quản lý xuống dưới và tiếp đó các tên miền lại được tiếp tục chuyên xuống cấp thấp hơn (delegate) xuống dưới.

Zone

Hệ thống dns cho phép phân chia tên miền để quản lý và nó chia hệ thống tên miền ra thành zone và trong zone quản lý tên miền tên miền được phân chia đó và nó chứa thông tin về domain cấp thấp hơn và có khả năng chia thành các zone cấp thấp hơn và phân quyền cho các dns server khác quản lý.

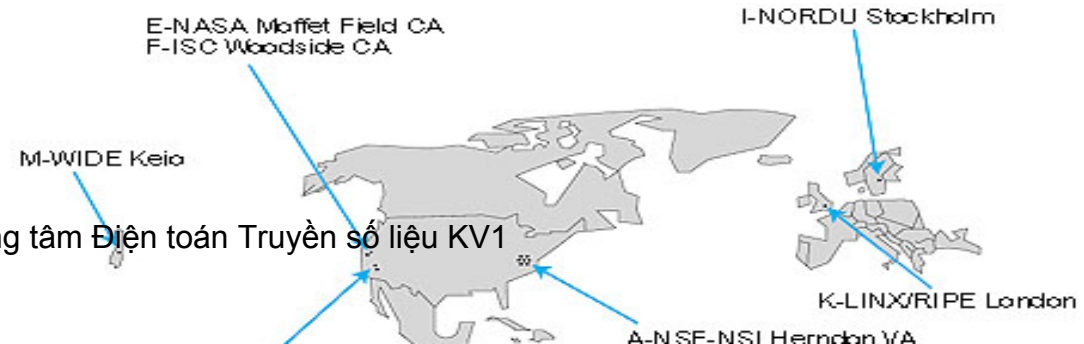
Ví dụ: zone *".com"* thì dns server quản lý zone *".com"* chưa thông tin về các bản ghi có đuôi là *".com"* và có khả năng chuyển quyền quản lý (delegate) các zone cấp thấp hơn cho các dns khác quản lý như *".microsoft.com"* là vùng (zone) do microsoft quản lý.

Root Server

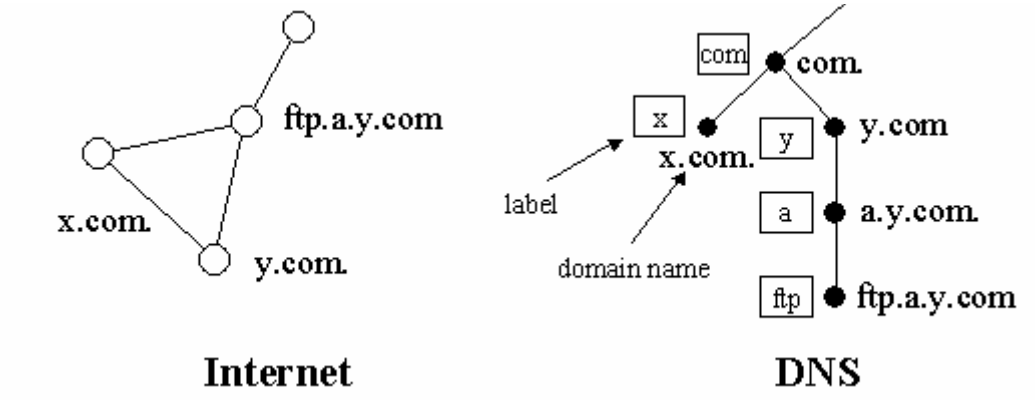
✓ Là server quản lý toàn bộ cấu trúc của hệ thống dns

✓ Root server không chứa dữ liệu thông tin về cấu trúc hệ thống DNS mà nó chỉ chuyển quyền (delegate) quản lý xuống cho các server cấp thấp hơn và do đó root server có khả năng xác định đường đến của một domain tại bất cứu đâu trên mạng

✓ Hiện nay trên thế giới có khoảng 13 root server quản lý toàn bộ hệ thống Internet (vị trí của root server như trên hình vẽ dưới)



Hệ thống cơ sở dữ liệu của dns là hệ thống dữ liệu phân tán hình cây như cấu trúc đó là cấu trúc logic trên mạng Internet



Về mặt vật lý hệ thống DNS nằm trên mạng Internet không có có cấu trúc hình cây nhưng nó được cấu hình phân cấp logic phân cấp hình cây phân quyền quản lý.

Một DNS server có thể nằm bất cứ vị trí nào trên mạng Internet nhưng được cấu hình logic để phân cấp chuyển tên miền cấp thấp hơn xuống cho các dns server khác nằm bất cứ vị trí nào trên mạng Internet (về nguyên tắc ta có thể đặt DNS tại bất cứ vị trí nào trên mạng Internet. Nhưng tốt nhất là đặt DNS tại vị trí nào gần với các client để dễ dàng truy vấn đến đồng thời cũng gần với vị trí của dns server cấp cao hơn trực tiếp của nó).

Mỗi một tên miền đều được quản lý bởi ít nhất một DNS server và trên đó ta khai các bản ghi của tên miền trên DNS server. Các bản ghi đó sẽ xác định địa chỉ IP của tên miền hoặc các dịch vụ xác định trên Internet như web, thư điệnt tử ...

Sau đây là các bản ghi trên dns

Tên trường	Tên đầy đủ	Mục đích
SOA	Start of Authority	Xác định máy chủ DNS có thẩm

		quyền cung cấp thông tin về tên miền xác định trên DNS
NS	Name Server	Chuyển quyền quản lý tên miền xuống một DNS cấp thấp hơn
A	Host	Ánh xạ xác định địa chỉ IP của một host
MX	Mail Exchanger	Xác định host có quyền quản lý thư điện tử cho một tên miền xác định
PTR	Pointer	Xác định chuyển từ địa chỉ IP sang tên miền
CNAME	Canonical NAME	Thường xử dụng xác định dịch vụ web hosting

Cấu trúc của một tên miền

- Domain sẽ có dạng : lable.lable.label...lable
- Độ dài tối đa của một tên miền là 255 ký tự
- Mỗi một Lable tối đa là 63 ký tự
- Lable phải bắt đầu bằng chữ hoặc số và chỉ được phép chứa chữ, số, dấu trừ(-), dấu chấm (.) mà không được chứa các ký tự khác.

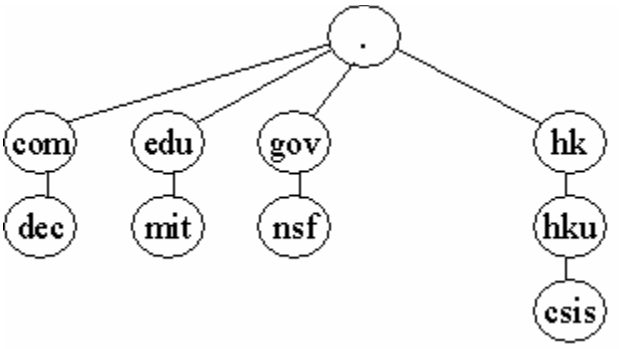
Phân loại tên miền

Hầu hết tên miền được chia thành các loại sau:

- *Arpa* : tên miền ngược (chuyển đổi từ địa chỉ IP sang tên miền reverse domain)
- *Com* : các tổ chức thương mại
- *Edu* : các cơ quan giáo dục
- *Gov* : các cơ quan chính phủ
- *Mil* : các tổ chức quân sự, quốc phòng

- *Net* : các trung tâm mạng lớn
- *Org* : các tổ chức khác
- *Int* : các tổ chức đa chính phủ (ít được sử dụng)

Ngoài ra hiện nay trên thế giới sử dụng loại tên miền có hai ký tự cuối để xác định tên miền thuộc quốc gia nào (được xác định trong chuẩn ISO3166)



Loại tên	Miêu tả	Ví dụ
Gốc (domain root)	Nó là đỉnh của nhánh cây của tên miền. Nó xác định kết thúc của domain (fully qualified domain names FQDNs).	Đơn giản nó chỉ là dấu chấm (.) sử dụng tại cuối của tên ví như "example.microsoft.com."
Tên miền cấp một (Top-level domain)	Là hai hoặc ba ký tự xác định nước/khu vực hoặc các tổ chức.	".com", xác định tên sử dụng trong xác định là tổ chức thương mại .
Tên miền cấp hai (Second-level domain)	Nó rất đa dạng trên internet, nó có thể là tên của một công ty, một tổ chức hay một cá nhân .v.v. đăng ký trên internet.	"microsoft.com.", là tên miền cấp hai đăng ký là công ty Microsoft.
Tên miền cấp nhỏ hơn	Chia nhỏ thêm ra của tên miên cấp hai xuống thường được sử dụng như chi	"example.microsoft.com." là phần quản lý tài liệu ví dụ của microsof

(Subdomain)	nhánh, phong ban của một cơ quan hay một chủ đề nào đó.

Một số chú ý khi đặt tên miền:

– Tên miền nên đặt giới hạn từ từ cấp 3 đến cấp 4 hoặc cấp 5 vì nếu nhiều hơn nữa việc quản trị là khó khăn.

– Sử dụng tên miền là phải duy nhất trong mạng internet

– Nên đặt tên đơn giản gợi nhớ và tránh đặt tên quá dài

II.2. Phân loại DNS server và đồng bộ dư liệu giữa các DNS server

Có ba loại DNS server sau:

- *Primary server*

Nguồn xác thực thông tin chính thức cho các domain mà nó được phép quản lý quản lý

Thông tin về tên miền do nó được phân cấp quản lý thì được lưu trữ tại đây và sau đó có thể được chuyển sang cho các secondary server.

Các tên miền do primary server quản lý thì được tạo và sửa đổi tại primary server và sau đó được cập nhập đến các secondary server.

- *Secondary server*

DNS được khuyến nghị nên sử dụng ít nhất là hai DNS server để lưu cho mỗi một zone. Primary DNS server quản lý các zone và secondary server được sử dụng để lưu trữ dự phòng cho zone cho primary server. Secondary DNS server được khuyến nghị dùng nhưng không nhất thiết phải có. Secondary server được phép quản lý domain nhưng dữ liệu về domain không phải tạo tại secondary server mà nó được lấy về từ primary server.

Secondary server có thể cung cấp hoạt động ở chế độ không có tải trên mạng. Khi lượng truy vấn zone tăng cao tại primary server nó sẽ chuyển bớt tải

sang secondary server hoặc khi primary server bị sự cố thì secondary sẽ hoạt động thay thế cho đến khi primary server hoạt động trở lại

Secondary server nên được sử dụng tại nới gần với client để có thể phục vụ cho việc truy vấn tên miền một cách dễ dàng. Nhưng không nên cài đặt secondary server trên cùng một subnet hoặc cùng một kết nối với primary server. Vì điều đó sẽ là một giải pháp tốt để sử dụng secondary server để dự phòng cho primary server vì có thể kết nối đến primary server bị hỏng thì cũng không ảnh hưởng gì đến secondary server.

Primary server luôn luôn duy trì một lượng lớn dữ liệu và thường xuyên thay đổi hoặc thêm vào các zone. Do đó DNS server sử dụng một cơ chế cho phép chuyển các thông tin từ primary server sang secondary server và lưu giữ nó trên đĩa. Các thông tin nhận dữ liệu về các zone có thể sử dụng giải pháp lấy toàn bộ (full) hoặc lấy phần thay đổi (incremental)

Nhiều secondary DNS server sẽ tăng độ ổn định hoạt động của mạng và việc lưu trữ thông tin của tên miền một cách đảm bảo như một điều cần quan tâm là dữ liệu của zone được chuyển trên mạng từ primary server đến các secondary server sẽ làm tăng lưu lượng đường truyền và yêu cầu thời gian để đồng bộ dữ liệu trên các secondary server.

- *Caching-only server*

Mặc dù tất cả các DNS server đều có khả năng lưu trữ dữ liệu trên bộ nhớ cache của máy để trả lời truy vấn một cách nhanh chóng. Caching-only server là loại DNS server chỉ sử dụng cho việc truy vấn, lưu giữ câu trả lời dữa trên thông tin trên cache của máy và cho kết quả truy vấn. Chúng không hề quản lý một domain nào và thông tin mà nó chỉ giới hạn những gì được lưu trên cache của server.

Khi nào thì sử dụng caching-only server ?. Khi mà server bắt đầu chạy thì nó không có thông tin lưu trong cache. Thông tin sẽ được cập nhập theo thời gian khi các client server truy vấn dịch vụ DNS. Nếu bạn sử dụng kết nối mạng WAN tốc độ thấp thì việc sử dụng caching-only DNS server là một giải pháp tốt nó cho phép giảm lưu lượng thông tin truy vấn trên đường truyền.

Chú ý

- Caching-only DNS server không chưa zone nào và cũng không quyền quản lý bất kỳ domain nào. Nó sử dụng bộ nhớ cache của mình để lưu các truy

vấn dns của client. Thông tin sẽ được lưu trong cache để trả lời cho các truy vấn đến của client

- Caching-only DNS có khả năng trả lời các truy vấn như không quản lý hoặc tạo bất cứ zone hoặc domain nào

- DNS server nói trung được khuyến nghị là được cấu hình sử dụng TCP/IP và dùng địa chỉ IP tĩnh.

Đồng bộ dữ liệu giữa các DNS server (zone transfer)

Truyền toàn bộ zone

Bởi vì tầm quan trọng của hệ thống DNS và việc quản lý các domain thuộc zone phải được đảm bảo. Do đó thường một zone thì thường được đặt trên hơn một DNS server để tránh lỗi khi truy vấn tên miền thuộc zone đó. Nói cách khác nếu chỉ có một server quản lý zone và khi server không trả lời truy vấn thì các tên miền trong zone đó sẽ không được trả lời và không còn tồn tại trên Internet. Do đó ta cần có nhiều DNS server cùng quản lý một zone và có cơ chế để chuyển dữ liệu của các zone và đồng bộ nó từ một DNS server này đến các DNS server khác

Khi một DNS server mới được thêm vào mạng thì nó được cấu hình như một secondary server mới cho một zone đã tồn tại. Nó sẽ tiến hành nhận toàn bộ (full) zone từ DNS server khác. Như DNS server thế hệ đầu tiên thường dùng giải pháp lấy toàn bộ cơ sở dữ liệu về zone khi có các thay đổi trong zone.

Truyền phần that đổi (Incremental zone)

Truyền chỉ những thay đổi (incremental zone transfer) của zone được miêu tả chi tiết trong tiêu chuẩn RFC 1995. Nó là phần bổ xung cho chuẩn sao chép dns zone. Incremental transfer thì đươc hỗ trợ bởi cả DNS server là nguồn lấy thông tin và DNS server nhận thông tin về zone, nó cung cấp giải pháp hiệu quả cho việc đồng bộ nhưng thay đổi hoặc thêm bớt zone.

Giải pháp ban đầu cho DNS yêu cầu cho việc thay đổi dữ liệu về zone là truyền toàn bộ dữ liệu của zone sử dụng truy vấn AXFR. Với việc chỉ truyền các thay đổi (incremental transfer) sẽ sử dụng truy vấn (IXFR) được sử dụng thay thế cho AXFR. Nó cho phép secondary server chỉ lấy về như zone thay đổi để đồng bộ dữ liệu.

Với trao đổi IXFR zone, thì sự khác nhau giữa versions của nguồn dữ liệu và bản sao của nó. Nếu cả hai bản đều có cùng version (xác định bởi số serial trong khai báo tại phần đầu của zone SOA "start of authority") thì việc truyền dữ liệu của zone sẽ không được thực hiện.

Nếu số serial cho dữ liệu nguồn lớn hơn số serial của secondary server thì nó sẽ thực hiện chuyển những thay đổi với các bản ghi nguồn (Resource record - RR) của zone. Để truy vấn IXFR thực hiện thành công và các thay đổi được gửi thì tại DNS server nguồn của zone phải lưu gữi các phần thay đổi để sử dụng truyền đến nơi yêu cầu của truy vấn IXFR. Incremental sẽ cho phép lưu lượng truyền dữ liệu là ít và thực hiện nhanh hơn.

```
@       IN      SOA     vdc-hn01.vnn.vn. postmaster.vnn.vn. (
        1999082802      ; serial number
        1800            ; refresh every 30 mins
        3600            ; retry every hour
        86400           ; expire after 24 hours
        6400            ; minimum TTL 2 hours
        )
        IN       NS       vdc-hn01.vnn.vn.
        IN       NS       hcm-server1.vnn.vn.
```

Zone transfer sẽ xẩy ra khi có nhưng hành động sau xẩy ra:

- Khi quá trình làm mới của zone kết thúc (refresh expire)
- Khi secondary server được thông báo zone đã thay đổi tại server nguồn quản lý zone
- Khi dịch vụ DNS bắt đầu chạy tại secondary server
- Tại secondary server yêu cầu chuyển zone

Sau đây là các bước yêu cầu từ secondary server đến DNS server chứa zone để yêu cầu lấy dữ liệu về zone mà nó quản lý.

1. Trong khi cấu hình mới DNS server. Thì nó sẽ gửi truy vấn yêu cầu gửi toàn bộ zone ("all zone" transfer (AXFR) request) đến DNS server quản lý chính dữ liệu của zone

2. DNS server chính quản lý dữ liệu của zone sẽ trả lời và truyền toàn bộ dữ liệu về zone đến secondary (destination) server mới cấu hình.

zone thì được chuyển đến DNS server yêu cầu căn cứ vào version được xác định bằng số Serial tại phần khai báo (start of authority SOA). Tại phần SOA cũng có chứa các thông số xác định thời gian làm mới lại zone ...

3. Khi thời gian làm mới (refresh interval) của zone hết, thì DNS server nhận dữ liệu sẽ truy vấn yêu cầu làm mới zone tới DNS server chính chưa dữ liệu zone.

4. DNS server chính quản lý dữ liệu sẽ trả lời truy vấn và gửi lại dữ liệu.

Trả lời sẽ bao gồm cả số serial của zone hiện tại tại dns server chính.

5. DNS server nhận dữ liệu về zone sẽ kiểm tra số serial trong trả lời và quyết định sẽ làm thế nào với zone

Nếu giá trị của số serial bằng với số hiện tại tại DNS server nhận trả lời thì nó sẽ kết luận rằng sẽ không cần chuyển dữ liệu về zone đến. Và nó sẽ thiết lập lại với các thông số cũ và thời gian để làm mới lại bắt đầu.

Nếu giá trị của số serial tại dns server chính lớn hơn giá trị hiện tại tại dữ liệu dns nới nhận thì nó kết luận rằng zone cần phải được cập nhập và việc chuyển zone là cần thiết.

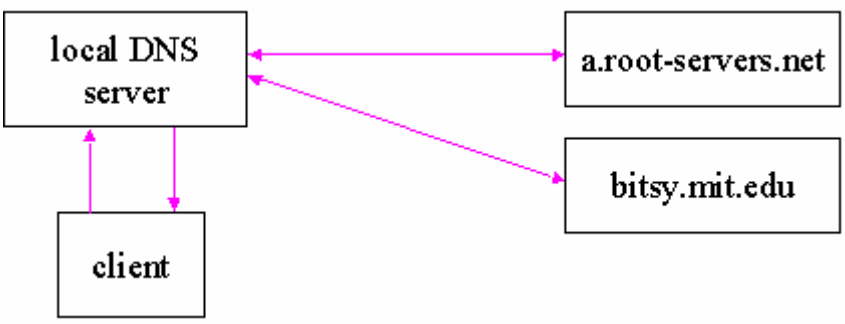
6. Nếu DNS server nơi nhận kết luận rằng zone cần phải thay đổi và nó sẽ gửi truy vấn IXFR tới DNS server chính để yêu cầu gửi zone

7. DNS server chính sẽ trả lời với việc gửi những thay đổi của zone hoặc toàn bộ zone

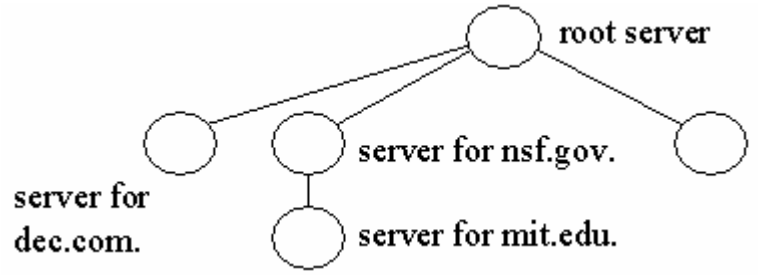
Nếu DNS server chính có hỗ trợ việc gửi những thay đổi của zone thì nó sẽ gửi những phần thay đổi (incremental zone transfer (IXFR) of the zone.). Nếu nó không hỗ trợ thì nó sẽ gửi toàn bộ zone (full AXFR transfer of the zone)

III. Hoạt động của hệ thống DNS

Hệ thống DNS hoạt động động tại lớp 4 của mô hình OSI nó sử dụng truy vấn bằng giao thức UDP và mặc định là sử dụng cổng 53 để trao đổi thông tin về tên miền.



Hoạt động của hệ thống DNS là chuyển đổi tên miền sang địa chủ IP và ngược lại. Hệ thống cơ sở dữ liệu của DNS là hệ thống cơ sở dữ liệu phân tán, các dns server được phân quyền quản lý các tên miền xác định và chúng liên kết với nhau để cho phép người dùng có thể truy vấn một tên miền bất kỳ (có tồn tại) tại bất cứ điểm nào trên mạng một các nhanh nhất



Như đã trình bầy các dns server phải biết ít nhất một cách để đến được root server và ngược lại. Như trên hình vẽ muốn xác định được tên miền mit.edu thì root server phải biết dns server nào được phân quyền quản lý tên miền mit.edu để chuyển truy vấn đến.

Nói tóm lại tất cả các dns server đều được kết nối một cách logic với nhau:

- Tất cả các dns server đều được cấu hình để biết ít nhất một cách đến root server
- Một máy tính kết nối vào mạng phải biết làm thế nào để liên lạc với ít nhất là một DNS server

Hoạt động của DNS

Khi DNS client cần xác định cho một tên miền nó sẽ truy vấn DNS.

Truy vấn dns và trả lời của hệ thống dns cho client sử dụng thủ tục UDP cổng 53, UPD hoạt động ở mức thứ 3 (network) của mô hình OSI, UDP là thủ tục phi kết nối (connectionless), tương tự như dịch vụ gửi thư bình thường bạn cho thư vào thùng thư và hy vọng có thể chuyển đến nơi bạn cần gửi tới.

Mỗi một message truy vấn được gửi đi từ client bao gồm ba phần thông tin :

- Tên của miền cần truy vấn (tên đầy đủ FQDN)
- Xác định loại bản ghi là mail, web ...
- Lớp tên miền (phần này thường được xác định là IN internet, ở đây không đi sâu vào phần này)

Ví dụ : tên miền truy vấn đầy đủ như "hostname.example.microsoft.com.", và loại truy vấn là địa chỉ A. Client truy vấn DNS hỏi "Có bản ghi địa chỉ A cho máy tính có tên là "hostname.example.microsoft.com" khi client nhận được câu trả lời của DNS server nó sẽ xác định địa chỉ IP của bản ghi A.

Có một số giải pháp để trả lời các truy vấn DNS. Client có thể tự trả lời bằng cách sử dụng các thông tin đã được lưu trữ trong bộ nhớ cache của nó từ những truy vấn trước đó. DNS server có thể sử dụng các thông tin được lưu trữ trong cache của nó để trả lời hoặc dns server có thể hỏi một dns server khác lấy thông tin đó để trả lời lại client.

Nói chung các bước của một truy vấn gồm có hai phần như sau:

- Truy vấn sẽ bắt đầu ngay tại client computer để xác định câu trả lời
- Khi ngay tại client không có câu trả lời, câu hỏi sẽ được chuyển đến DNS server để tìm câu trả lời.

Tự tìm câu trả lời truy vấn

Bước đầu tiên của quá trình sử lý một truy vấn. Tên miền sử dụng một chương trình trên ngay máy tính truy vấn để tìm câu trả lời cho truy vấn. Nếu truy vấn có câu trả lời thì quá trình truy vấn kết thúc

Ngay tại máy tính truy vấn thông tin được lấy từ hai nguồn sau:

- Trong file HOSTS được cấu hình ngay tại máy tính. Các thông tin ánh xạ từ tên miền sang địa chỉ được thiết lập ở file này được sử dụng đầu tiên. Nó được tải ngay lên bộ nhớ cache của máy khi bắt đầu chạy dns client.
- Thông tin được lấy từ các câu trả lời của truy vấn trước đó. Theo thời gian các câu trả lời truy vấn được lưu giữ trong bộ nhớ cache của máy tính và nó được sử dụng khi có một truy vấn lặp lại một tên miền trước đó.

Truy vấn DNS server

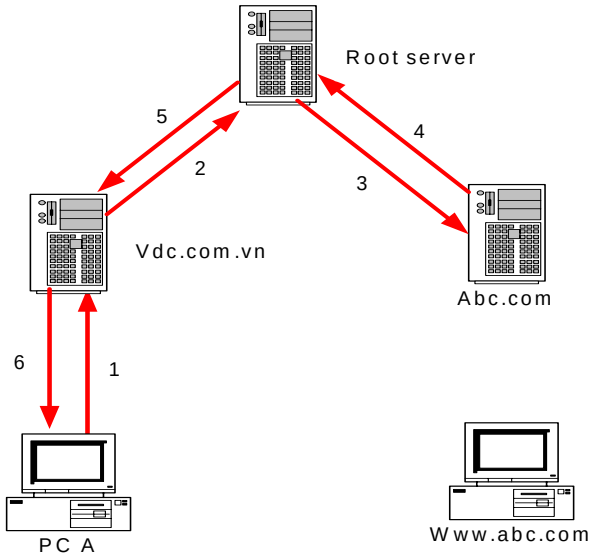
Khi DNS server nhận được một truy vấn. Đầu tiên nó sẽ kiểm tra câu trả lời liệu có phải là thông tin của bản ghi mà nó quản lý trong các zone của server. Nếu truy vấn phù hợp với bản ghi mà nó quản lý thì nó sẽ sử dụng thông tin đó để trả lời trả lời (authoritatively answer) và kết thúc truy vấn.

Nếu không có thông tin về zone của nó phù hợp với truy vấn. Nó sẽ kiểm tra các thông tin được lưu trong cache liệu có các truy vấn tương tư nào trước đó phù hợp không nếu có thông tin phù hợp nó sẽ sử dụng thông tin đó để trả lời và kết thúc truy vấn.

Nếu truy vấn không tìm thấy thông tin phù hợp để trả lời từ cả cache và zone mà dns server quản lý thì truy vấn sẽ tiếp tục. Nó sẽ nhờ DNS server khác để trả lời truy vấn đến khi tìm được câu trả lời.

Các cách để dns server liên lạc với nhau xác định câu trả lời

Trường hợp Root server kết nối trực tiếp với server tên miền cần truy vấn



Trong trường hợp root server biết được dns server quản lý tên miền cần truy vấn. Thì các bước của truy vấn sẽ như sau:

Bước 1 : PC A truy vấn DNS server tên miền vdc.com.vn. (là local name server) tên miền www.abc.com.

Bước 2 : DNS server tên miền vdc.com.vn không quản lý tên miền www.abc.com do vậy nó sẽ chuyển truy vấn lên root server.

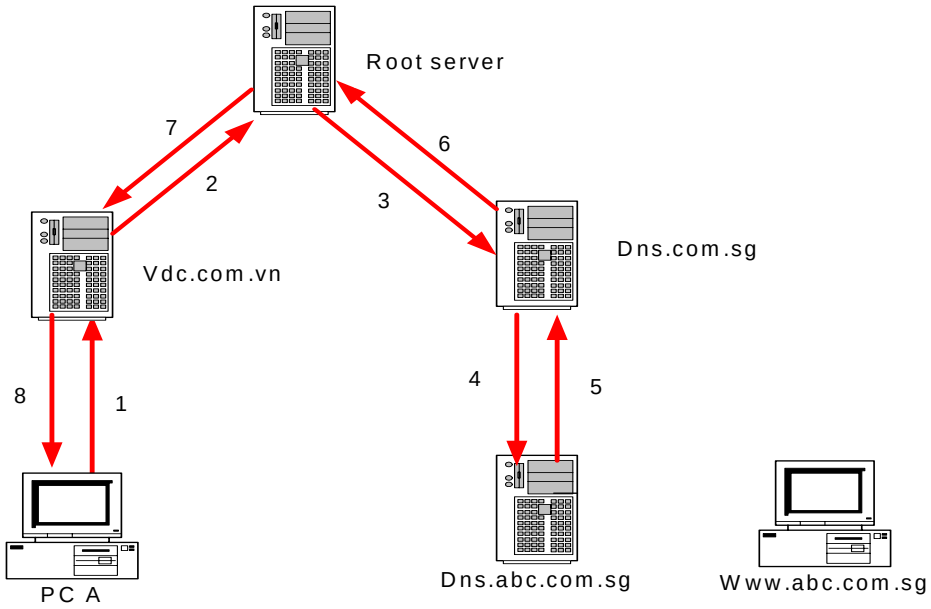
Bước 3 : Root server sẽ xác định được rằng dns server quản lý tên miền www.abc.com là server dns.abc.com và nó sẽ chuyển truy vấn đến dns server dns.abc.com để trả lời

Bước 4 : DNS server dns.abc.com sẽ xác định bản ghi www.abc.com và trả lời lại root server

Bước 5 : Root server sẽ chuyển câu trả lời lại cho server vdc.com.vn

Bước 6 : DNS server vdc.com.vn sẽ chuyển câu trả lời về cho PC A và từ đó PC A có thể kết nối đến PC B (quản lý www.abc.com)

Trường hợp root server không kết nối trực tiếp với server tên miền cần truy vấn



Trong trường hợp không kết nối trực tiếp thì root server sẽ hỏi server trung gian (phân lớp theo hình cây) để xác định được đến server tên miền quản lý tên miền cần truy vấn

Bước 1 - PC A truy vấn DNS server vdc.com.vn (local name server) tên miền www.acb.com.sg.

Bước 2 - DNS server vdc.com.vn không quản lý tên miền www.abc.com.sg vậy nó sẽ chuyển lên root server.

Bước 3 - Root server sẽ không xác định được dns server quản lý trực tiếp tên miền www.abc.com.sg nó sẽ căn cứ vào cấu trúc của hệ thống tên miền để chuyển đến dns quản lý cấp cao hơn của tên miền abc.com.sg đó là com.sg và nó xác định được rằng dns server dns.com.sg quản lý tên miền com.sg.

Bước 4 - dns.com.sg sau đó sẽ xác định được rằng dns server dns.abc.com.sg có quyền quản lý tên miền www.abc.com.sg.

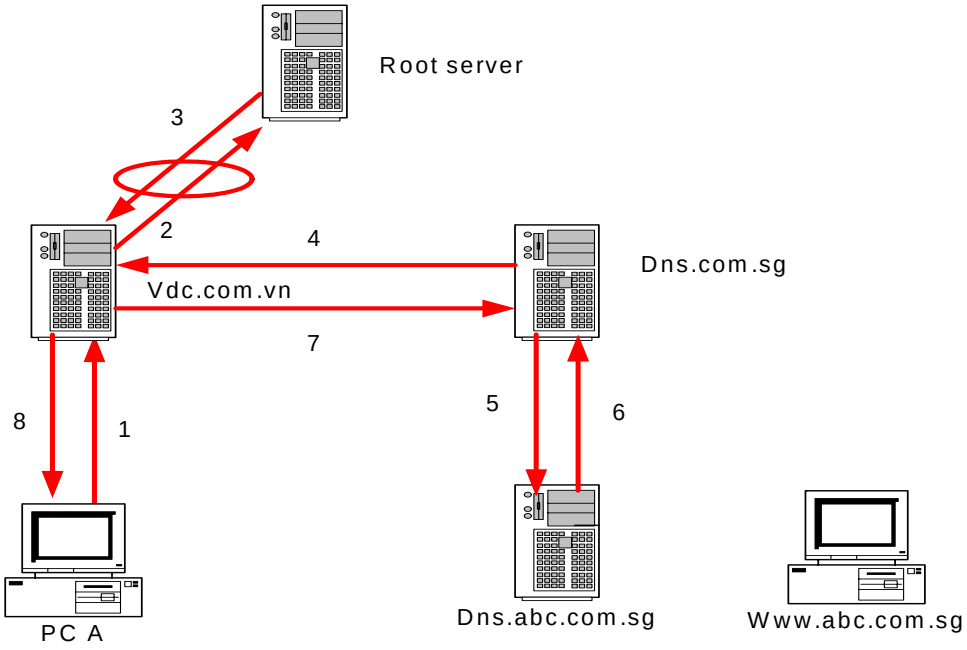
Bước 5 - dns.abc.com.sg sẽ lấy bản ghi xác định cho tên miền www.abc.com.sg để trả lời dns server dns.com.sg.

Bước 6 - dns.com.sg sẽ lại chuyển câu trả lời lên root server.

Bước 7 - Root server sẽ chuyển câu trả lời trở lại dns server vdc.com.vn.

Bước 8 - Và dns server vdc.com.vn sẽ trả lời về PC A câu trả lời và PC A đã kết nối được đến host quản lý tên miền www.abc.com.sg.

Khi các truy vấn lặp đi lặp lại thì hệ thống dns có khả năng thiết lập chuyển quyền trả lời đến dns trung gian mà không cần phải qua root server và nó cho phép thời gian truy vấn được giảm đi.



Hoạt động của DNS cache

Khi DNS server sử lý các truy vấn của client và sử dụng các truy vấn lặp lại. Nó sẽ xác định và lưu lại các thông tin quan trọng của tên miền mà client truy vấn. Thông tin đó sẽ được ghi lại trong bộ nhớ cache của dns server.

Cache lưu giữ thông tin là giải pháp hữu hiệu tăng tốc độ truy vấn thông tin cho các truy vấn thường xuyên của các tên miền hay được sử dụng và làm giảm lưu lượng thông tin truy vấn trên mạng.

DNS server khi thực hiện các truy vấn đệ quy cho client thì dns server sẽ tạm thời lưu trong cache bản ghi thông tin (resource record - RR) lấy được từ dns server lưu trữ thông tin về truy vấn đó. Sau đó một client khác truy vấn yêu cầu thông tin của đúng bản ghi đó thì nó sẽ lấy thông tin ban ghi (RR) lưu trong cache để trả lời.

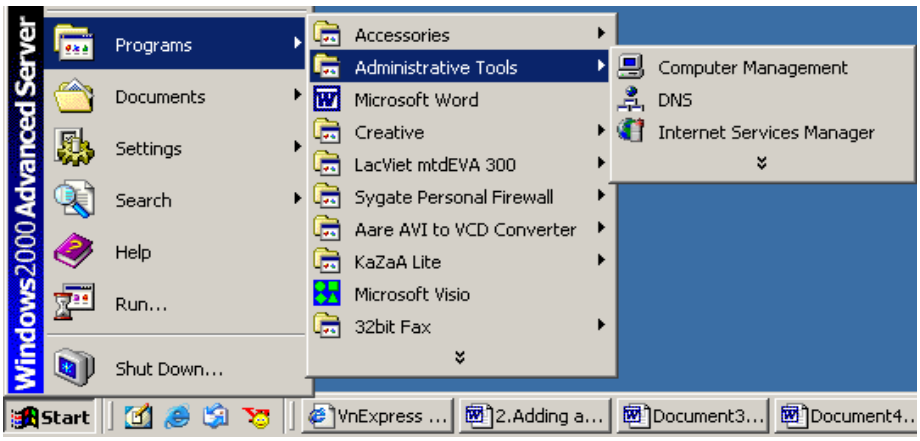
Khi thông tin được lưu trong cache. Thì các bản ghi RR được ghi trong cache sẽ được cung cấp thời gian sống (TTL - Time-To-Live). Thời gian sống của một bản ghi trong cache là thời gian mà nó tồn tại trong cache và được dùng để trả lời cho các truy vấn của client khi truy vấn tên miền trong bản ghi đó. Thời gian sống (TTL) được khai khi cấu hình cho các zone. Giá trị mặc định nhỏ nhất của thời gian sống (Minimum TTL) là 3600 giây (1 giờ) như giá

trị này ta có thể thay đổi khi cấu hình zone. Hết thời gian sống bản ghi sẽ được xóa khỏi bộ nhớ cache.

IV.Cài đặt DNS Server cho Window 2000

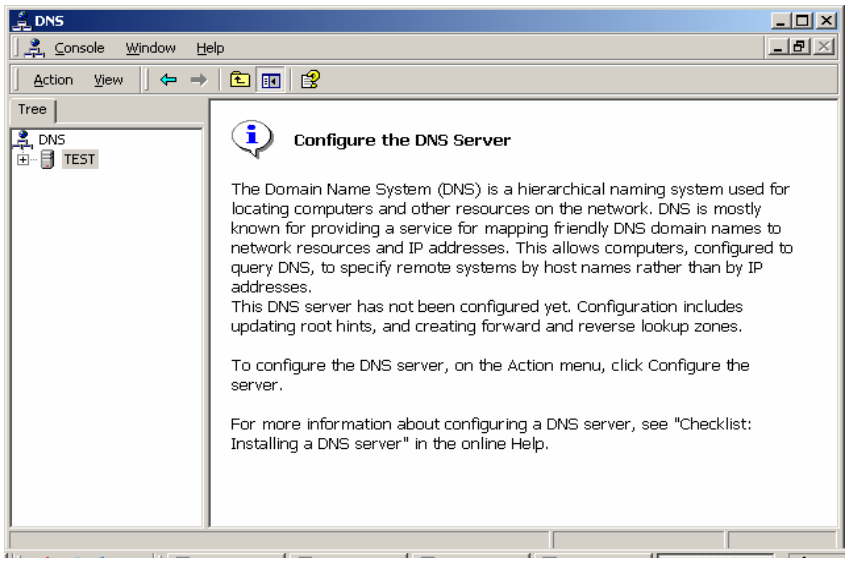
IV.1. Mở cửa sổ quản lý DNS

Bước 1: Mở của sổ quản lý DNS



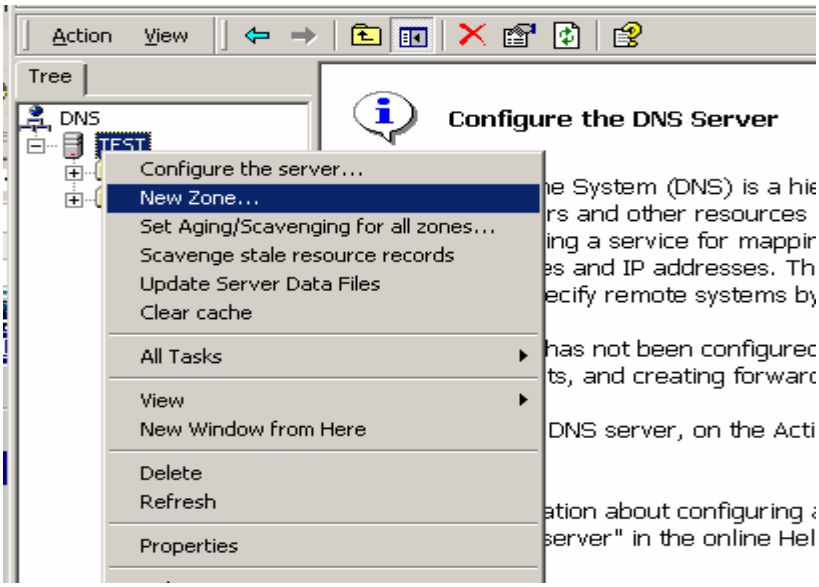
Bấm vào mune *Start* chọn *Programs* và sau đó là *"Administrative tools"* Chọn *"DNS Manager"*

Bước 2: Cửa sổ quản lý DNS server sẽ xuất hiện

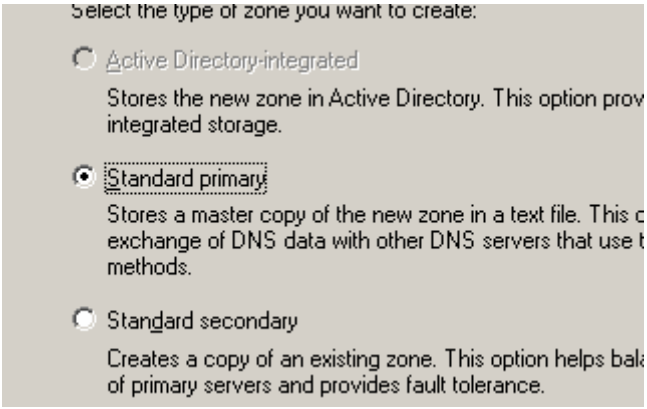


Tại cửa sổ quản lý DNS server bạn có thể khai báo các tính năng của DNS

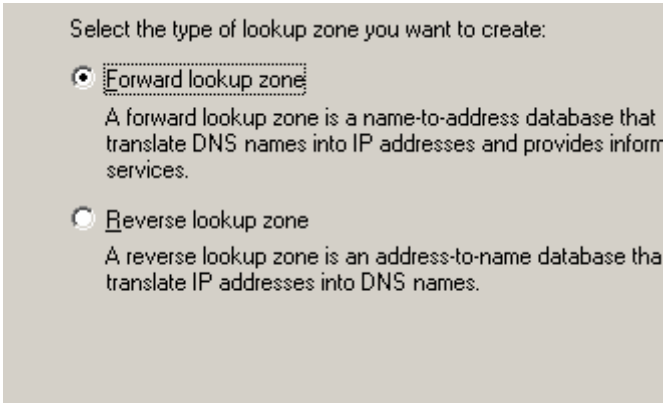
IV.2 Thêm trường (zone)



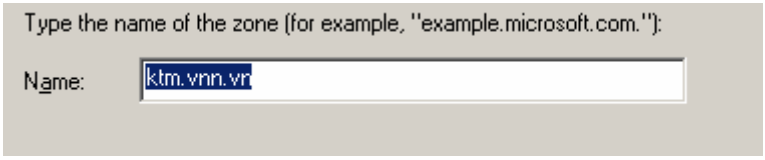
zone là tên miền (domain name) mà server quản lý. Tại cửa sổ quản lý DNS tại phần server quản lý bấm chuột phải để hiện menu và chọn *"new zone*" như hình trên



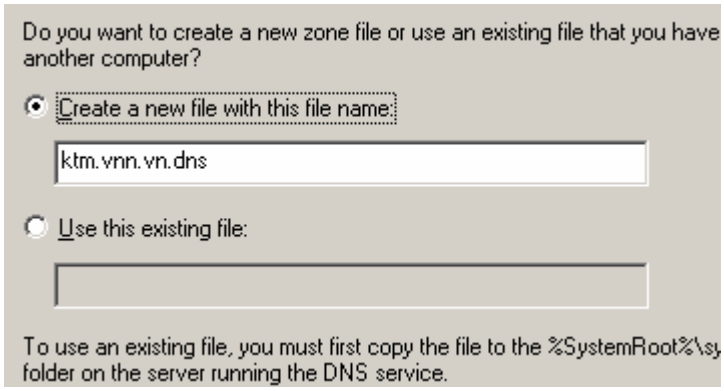
Bấm và *"new zone"* sẽ hiện cửa sổ cho phép chọn kiểu dữ liệu mà zone quản lý. *Standard Primary* là loại dữ liệu của zone được khai báo và quản lý ngay tại server. Còn *Stardard Secondary* là loại zone mà dữ liệu được lấy về từ *Standard Primary* và dữ liệu cũng nằm trên server . *Standard Primary* thường sử dụng để dự phòng cho các zone đã tồn tại. Bấm *Next* để tiếp tục



Sẽ xuất cửa sổ như trên. *Forward lookup zone* là loại zone quản lý việc chuyển đổi từ domain name sang địa chỉ IP. Còn phần *Reverse lookup zone* quản lý việc chuyển đổi từ IP sang Domain name. Bấm *Next* tiếp tục



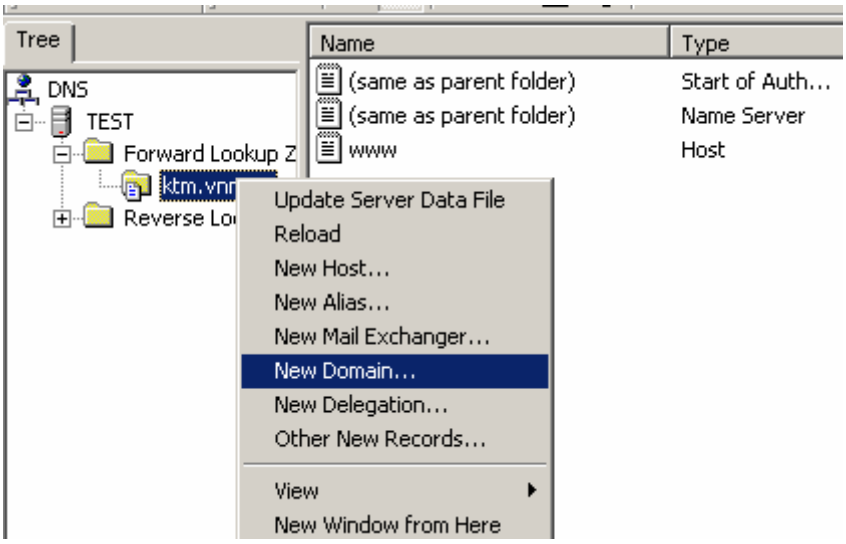
Tại cửa sổ này điền zone (domain name) mà sẽ quản lý. Bấm Next tiếp tục



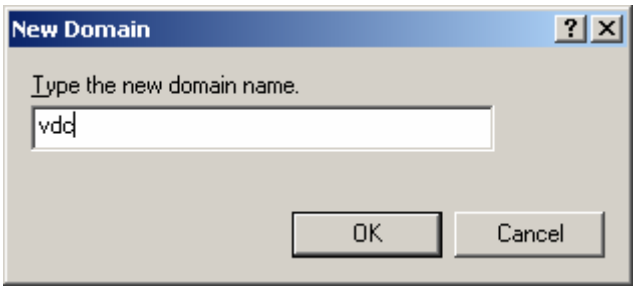
Điền tên của file để lưu trữ zone tại *"Create a new file with this file name"* hoặc sử dụng file có sẵn tại *"Use this existing file"* Và bấm *Next* cho đến khi xuất hiện nút *finish* để kết thúc tạo zone

IV.3.Thêm tên miên (domain name)

Tại của sổ quản lý domain chọn vào server và bấm chuột phải hiện lên menu và chọn *"New Domain..."* để điền một domain mới .

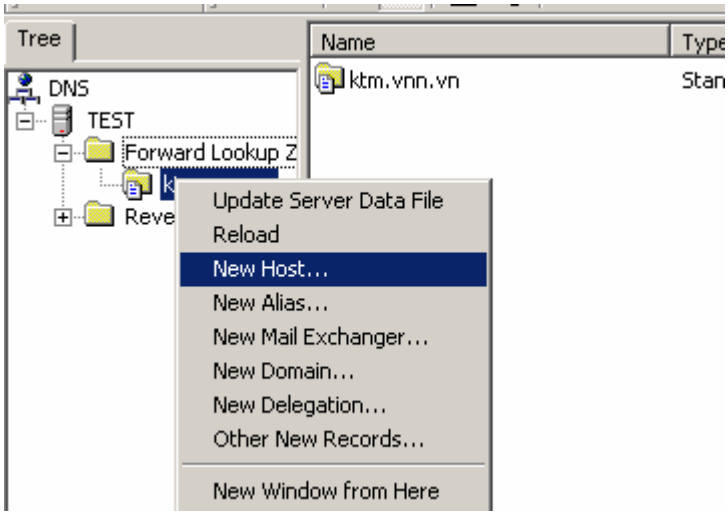


Sau khi bấm vào *"New Domain"* nó sẽ xuất hiện cửa sổ cho phép bạn điền tên miền mà server được phép quản lý. Sau khi điền bấm *"OK"* để kết thúc

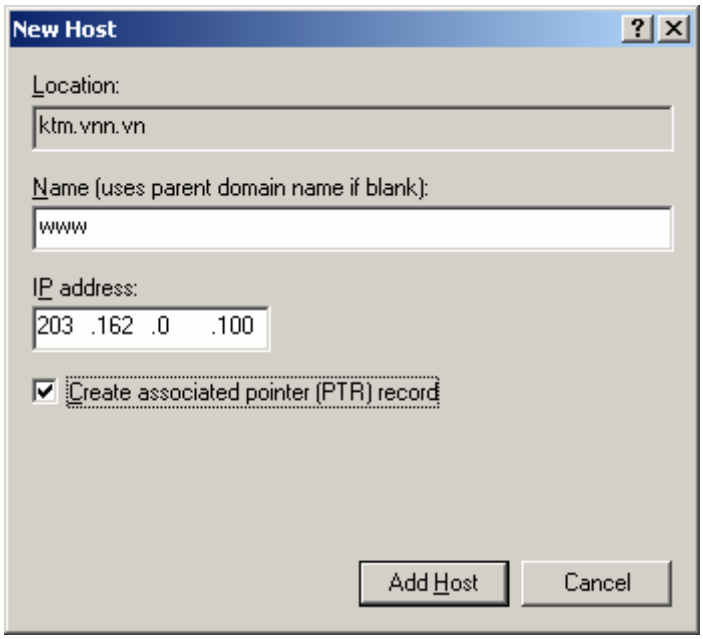


IV.4 Thêm một host mới

Tại cửa sổ quản lý DNS chọn zone đã tạo và bấm chuột phải chọn *"new host"*



Xuất hiện cửa sổ cho phép ta khai báo host mới



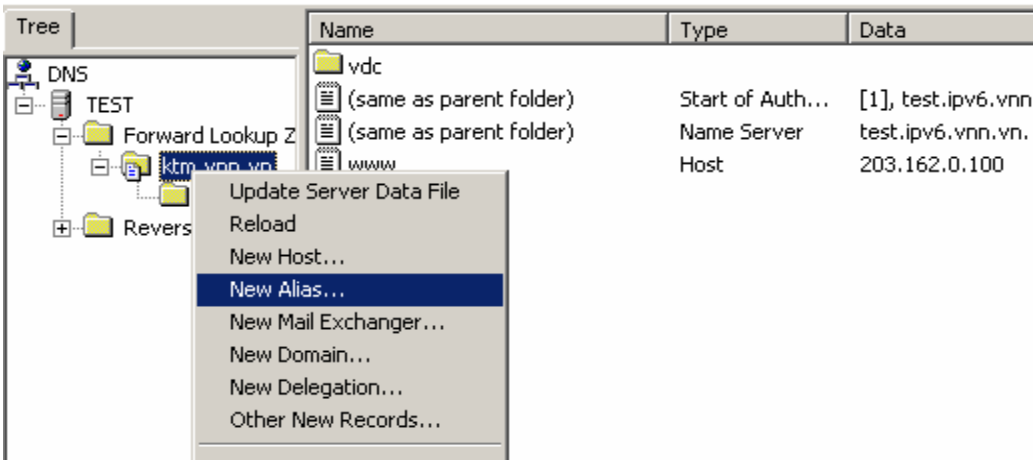
Bạn điền tên của host mà muốn tạo. Tên của host sẽ được tự động điền thêm phần domain để thành tên đầy đủ của host.

Ví dụ: như trên đây là vùng quản lý zone (*location*) là ktm.vnn.vn. Vậy khi bạn điền *Name* là www và *IP address* là 203.162.0.100 thì sẽ tương ứng với định nghĩa domain www.ktm.vnn.vn. trỏ đến địa chỉ IP 203.162.0.100

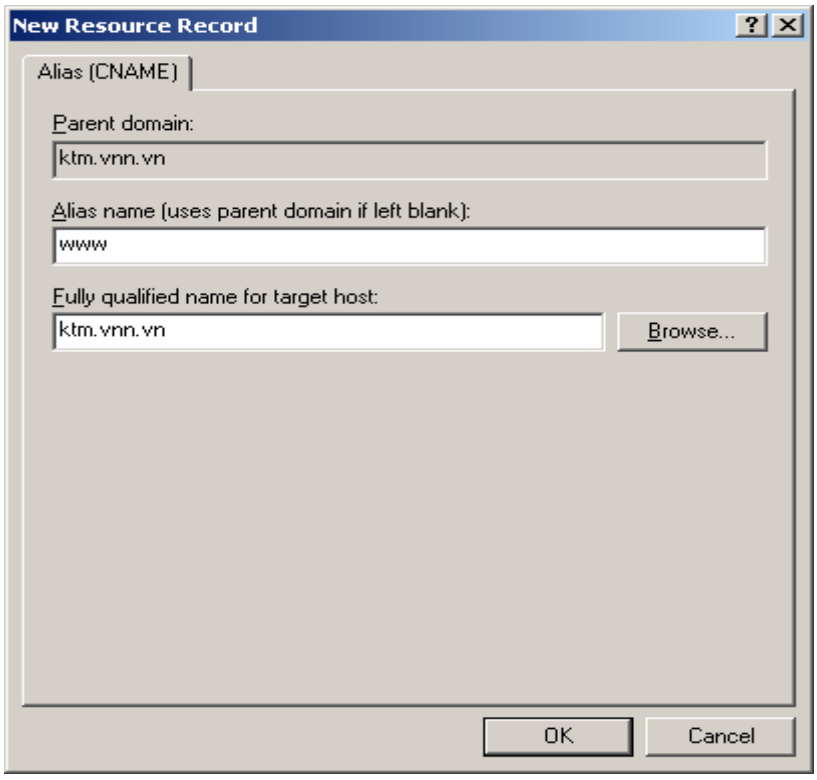
www.ktm.vnn.vn. IN A 203.162.0.100

IV.5 Tạo một bản ghi web (tạo bí danh)

Tại cửa sổ quản lý Domain và tên miền vừa tạo và bấm chuột phải và chọn *"New Alias"* để tạo một CNAME đến một host.



Bấm và *"New Alias..."* sẽ xuất hiện cửa sổ cho phép khai báo Alias



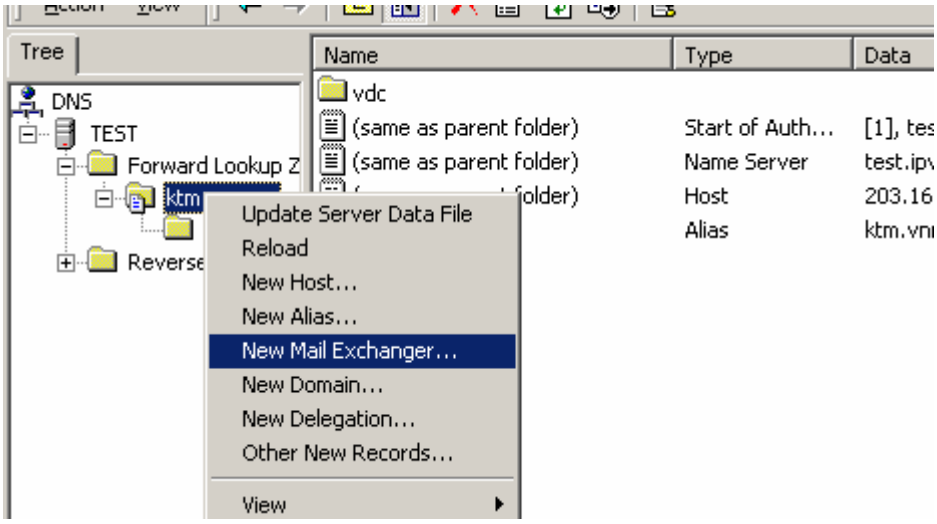
Tại phần *"Alias name"* điền tên tạo alias và tại phần *"Fully qualified name for target host"* điền tên đầy đủ của một host mà muốn tạo bí danh (thường được sử dụng cho webhosting)

Ví dụ : www.ktm.vnn.vn. IN CNAME ktm.vnn.vn.

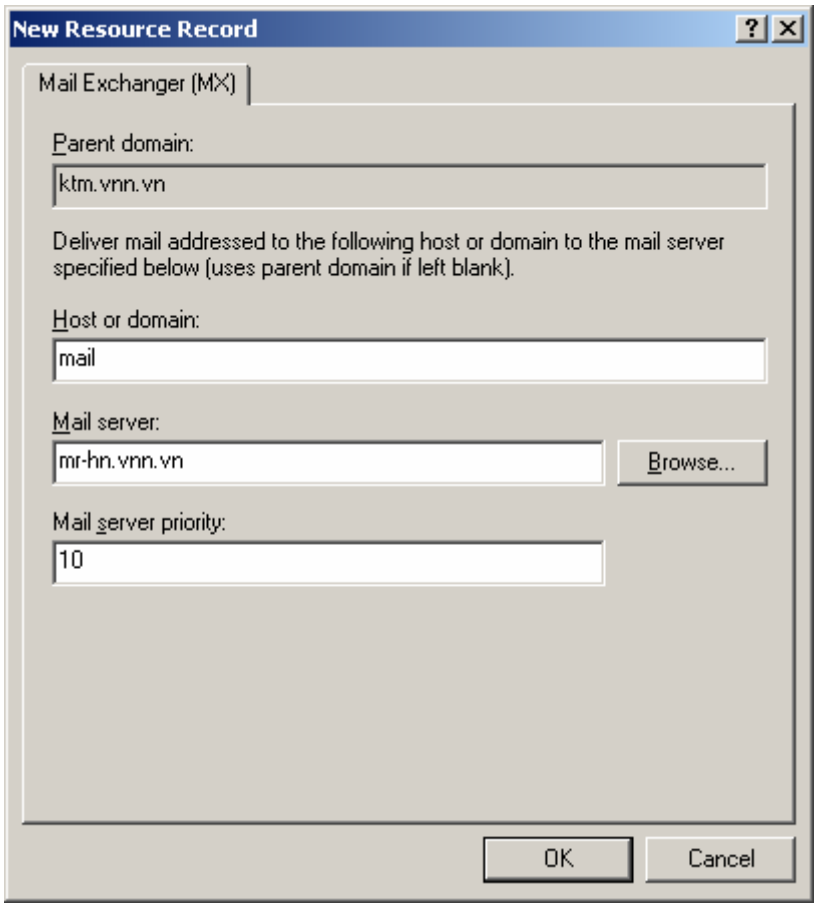
Ta sẽ có trang web www.ktm.vnn.vn đặt trên server web có tên là ktm.vnn.vn.

IV. 6 Tạo một bản ghi thư điện tử (MX)

Tại cửa sổ quản lý DNS tại tên miền muốn tạo bản ghi MX bấm chuột phải



Sau khi bấm vào *"New Mail Exchanger.."* sẽ xuất hiện cửa sổ cho phép tạo các thông số cho bản ghi mx



Điền tại *"Host or domain"* điền tên hoặc để trống tên này kết hợp với phần zone "*Parent domain"* để tạo thành domain đầy đủ của bản ghi thư điện tử. Tại *"Mail server"* điền tên của server thư điện tử và tại *"Mail server priority"* điền mức độ ưu tiên của server thư điện tử (độ lớn càng nhỏ mức ưu tiên càng cao)

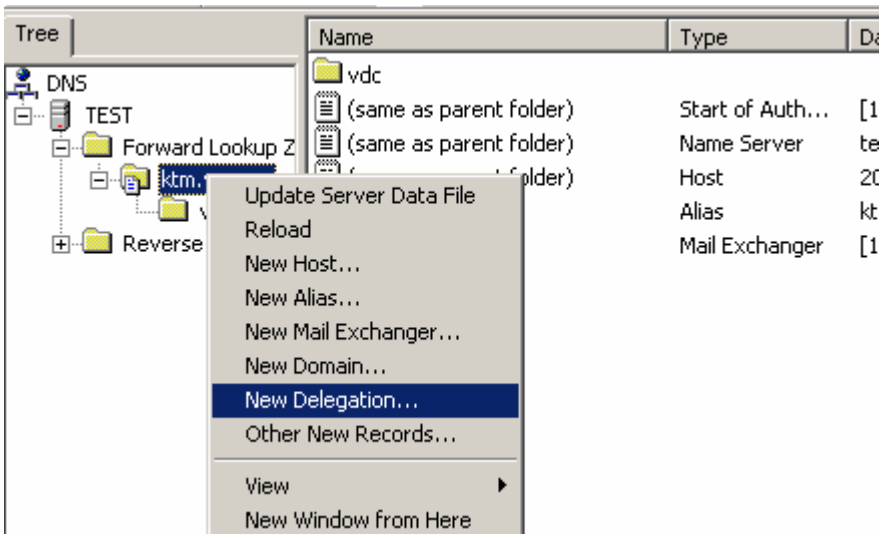
Ví dụ trên hình ta có:

mail.ktm.vnn.vn IN MX 10 mr-hn.vnn.vn.

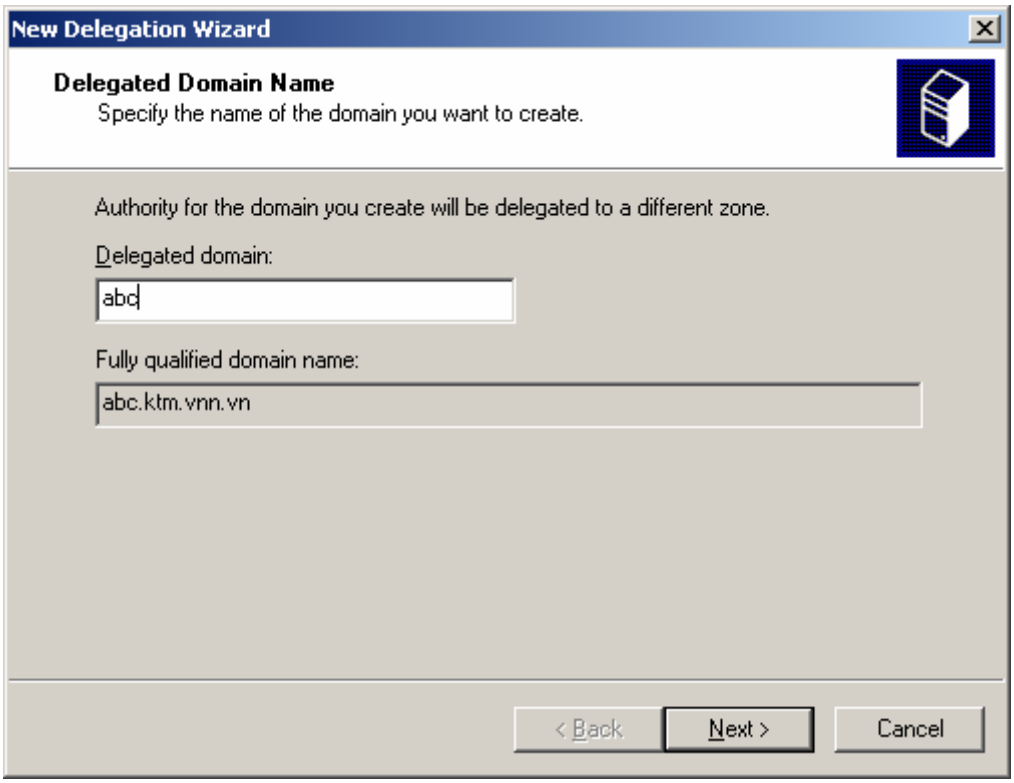
Ta có tên miền thư điện tử mail.ktm.vnn.vn. (ta có thể tạo được các hộp thư abc@mail.ktm.vnn.vn) được chứa tại server thư điện tử mr-hn.vnn.vn với mức ưu tiên là 10

IV. 7 Chuyển quyền quản lý têm miền (delegate)

Tại cửa sổ quản lý DNS tại domain muốn chuyển quyền quản lý bấm chuột phải.

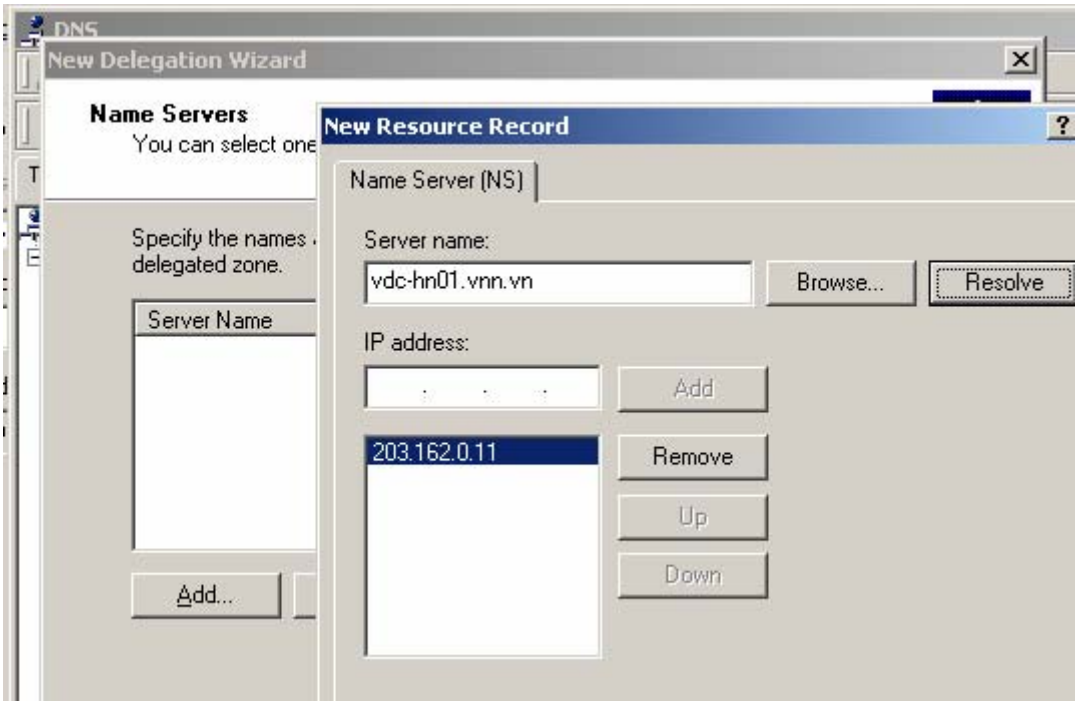


Bấm vào *"New Delegation..."* để hiện cửa sổ cho phép chuyển quyền quản lý tên miền



Điền phần domain mà bạn muốn chuyển quyền quản lý vào *"Delegated domain"*

Ví dụ ở đây điền là abc nghĩa là bạn muốn chuyển quyền quản lý domain abc.ktm.vnn.vn. Bấm *"Next"* để tiếp tục



Hiện cửa sổ điền vào *"Server name"* tên của dns server sẽ được phép quản lý tên miền abc.ktm.vnn.vn. Bấm *"Resolve"* để xác định địa chỉ IP của dns server. Sau đó bấm *"Ok"* để kết thúc.

Ví dụ abc.ktm.vnn.vn. IN NS vdc-hn01.vnn.vn.

Tương ứng tên miền abc.ktm.vnn.vn. sẽ được chuyển quyền về dns server vdc-hn01.vnn.vn để quản lý.

V. Cài đặt, cấu hình dns cho Linux

Hiện tại trên Internet rất nhiều nhà cung cấp phần mềm miễn phí cho DNS. Nhưng phần mền sử dụng dns cho unix được sử dụng phổ biến hiện này là gói phần mềm cho dns là Bind

Bind được phát triển bởi một tổ chức phi lợi nhuận là Internet Software Consortium (www.isc.org) và nó cung cấp phần mền bind miễn phí.

Hiện tại phần mềm bind có version là 9.2.2

Phần mền Bind còn cung cấp tiện ích nslookup là công cụ rất tiện lợi cho việc kiểm tra tên miền

Khai báo DNS cho client/server

Với client sử dụng linux hoặc unix ta vào file /etc/resolv.conf

- ✓ Client chỉ lấy thông tin về các domain
- ✓ Client chỉ gửi query tới server và nhận trả lời

Cấu hình dns server

- ✓ Cấu bình resolver như của (dns client)
- ✓ Cấu hình Bind cho name server (named)
- ✓ Xây dự cơ sở dữ liệu cho dns (cho các zone file)

Cấu hình cho dns client /etc/resolv.conf

Các từ khóa	Miêu tả
nameserver *địa chỉ*	Địa chỉ IP của dns server sẽ gửi truy vấn đến để lấy thông tin về domain

domain *name*	xác định domain mặc định của client

/etc/resolv.conf

```
# Domain name resolver configuration file
#
domain nuts.com
# try yourself first
nameserver 172.16.12.2
# try almond next
nameserver 172.16.12.1
# finally try filbert
nameserver 172.16.1.2
```

Với dns client chỉ cần cấu hình file resolv.conf

Cài đặt dns server.

Ta có thể lấy chương trình cài đặt bind cho dns tại www.isc.org lấy về server

cd /usr/src

mkdir bind-9.xx

cd bind-9.xx

Lấy chương trình cài đặt dns về đây bind-9.xx-src.tar.gz

gunzip bind-9.xx-src.tar.gz

tar xf bind-9.xx-src.tar

rm bind-9.xx-src.tar

cd src

make clean

make depend

make install

Vậy là ta đã cài xong phần mền named cho dns và các zone file sẽ được chứa trong /var/named còn file cấu hình nằm trong /usr/local/etc vậy ta phải tạo và đặt file cấu hình và zone file vào các thư mục trên và chạy

#/usr/local/sbin/named

Vậy là server đã sẵn sàng cho truy vấn dns

Cấu trúc file cơ sở dữ liệu (zone file)

Các file cơ sở dữ liệu zone được chỉ làm hai loại cho domain (có dạng db.domain hoặc domain.root) và các domain ngược (db.address) và nó nằm trong thư mục /var/named của dns server.

Các dữ liệu nằm trong file cơ dữ liệu được gọi là DNS resource record. Các loại resource record trong file dữ liệu bao gồm:

SOA record

Chỉ rõ domain ở cột quản lý bởi name server ghi sau trường SOA. Trong trường hợp file db.domain

```
@       IN      SOA     vdc-hn01.vnn.vn. postmaster.vnn.vn. (
        1999082802      ; serial number
        1800            ; refresh every 30 mins
        3600            ; retry every hour
        86400           ; expire after 24 hours
        6400            ; minimum TTL 2 hours
        )
        IN      NS      vdc-hn01.vnn.vn.
                IN      NS      hcm-server1.vnn.vn.
```

Khai báo zone ngược db.203.162.0

```
@       IN      SOA     vdc-hn01.vnn.vn. postmaster.vnn.vn. (
                1999082301   ; Serial
    10800       ; Refresh after 3 hours
    3600        ; Retry after 1 hour
    604800      ; Expire after 1 week
```

```
        86400 )     ; Minimum TTL of 1 day
;name servers
        IN      NS      vdc-hn01.vnn.vn.
        IN      NS      hcm-server1.vnn.vn.
6       IN      PTR             ldap.vnn.vn.
7       IN      PTR             hanoi-server1.vnn.vn.
8       IN      PTR             hanoi-server2.vnn.vn.
9       IN      PTR             mail.vnn.vn.
```

Trong mỗi zone chỉ khai một trường SOA. Như ví dụ trên trong trường hợp file db.com.vn, chữ @ biể thị các tất cả các domain trong file quản lý bởi name server vdc-hn01.vnn.vn và địa chỉ mail của admin mạng là postmaster.vnn.vn. Ngoài ra trong phần SOA có 5 thông số cần quản tâm sau:

Serial number : Thông số này có tác dụng với tất cả các dữ liệu trong file. Khi secondary server yêu cầu primary server các thông tin về domain mà nó quản lý thì đầu tiên nó sẽ so sánh serial number của secondary và primary server. Nếu serial number của secondary server nhỏ hơn của primary server thì dữ liệu của domain sẽ được cập nhập lại cho secondary server từ secondary server.

Mỗi khi ta thay đổi nội dung của file db.domain thì ta cần phải thay đổi serial number và thường ta đánh serial number theo nguyên tắc sau:

Serial number : yyyymmddtt

trong đó : yyyy là năm

mm là tháng

dd là ngày

tt là số lần sử đổi trong ngày

Refresh : là chu kỳ thời gian mà secondary server sẽ sánh và cập nhập lại dữ liệu của nó với primary server

Retry: nếu secondary server không kết nối được với primary server thì cứ sau một khoảng thời gian thì nó sẽ kết nối lại

Expire : là khoảng thời gian mà domain sẽ hết hiệu lực nếu secondary không kết nối được với primary server.

TTL (time to live) : khi một server bất kỳ yêu cầu thông tin về dữ liệu nào đó từ primary server, và dữ liệu đó sẽ được lưu giữ tại server đó và có hiệu lực trong khoảng thời gian của TTL. Hết khoảng thời gian đó nếu tiếp tục cần thì nó lại phải truy vấn lại primary server.

Các bản ghi thường dùng trong DNS server

NS (name server) : Còn bản ghi NS để xác định dns server nào sẽ quản lý tên miền. Như ví dụ ở trên là dns server vdc-hn01.vnn.vn. và hcm-server1.vnn.vn.

A (address) : Bản ghi dạng A cho tương ứng một domain name với một địa chỉ IP. Chỉ cho phép khai báo một bản ghi A cho một địa chỉ IP.

Ví dụ:

Tên miền	Internet	Loại bản ghi	Địa chỉ
mr.vnn.vn.	IN	A	203.162.4.148
mr-hn.vnn.vn.	IN	A	203.162.0.24
mail.vnn.vn.	IN	A	203.162.0.9
fmail.vnn.vn.	IN	A	203.162.4.147
hot.vnn.vn.	IN	A	203.162.0.23
home.vnn.vn.	IN	A	203.162.0.12
www.vnn.vn.	IN	A	203.162.0.16

CNAME (canonical name) : là tên phụ cho một host có sẵn tên miền dạng A. Nó thường được sử dụng cho các server web, ftp

Ví dụ : các domain có dạng CNAME được chỉ tới các máy chủ web

Tên miền	Internet	Loại bản ghi	Server
www.gpc.com.vn.	IN	CNAME	home.vnn.vn.
www.huonghai.com.vn.	IN	CNAME	home.vnn.vn.

www.songmayip.com.vn.	IN	CNAME	hot.vnn.vn.
www.covato2.com.vn.	IN	CNAME	hot.vnn.vn.

MX (mail exchange): là tên phụ cho các dịch vụ mail trên các máy chủ đã có tên miền dạng A. Bản ghi này cho phép máy chủ có thể cung cấp dịch vụ mail cho các domain khác nhau. Có thể khai báo nhiều domain khác nhau cùng chỉ tới một server hoặc một domain trỏ tới nhiều server khác nhau (sử dụng backup) trong trường hợp này giá trị ưu tiên phải đặt khác nhau. Với số ưu tiên càng nhỏ thì mức độ ưu tiên càng cao.

Ví dụ

Tên miền	*Internet*	**Loại bản ghi**	**mức ưu tiên**	**Server**
mrvn.vnn.vn.	IN	MX	10	mr.vnn.vn.
clipsalvn.vnn.vn.	IN	MX	10	mr-hn.vnn.vn.
dbqnam.vnn.vn.	IN	MX	10	mr-hn.vnn.vn.
thangloi.vnn.vn.	IN	MX	50	mail.netnam.vn.
	IN	MX	100	fallback.netnam.vn.

PTR (Pointer) : là bản ghi tương ứng địa chỉ IP với domain. Các file dạng db.address. Ví dụ db.203.162.0 cho tương ứng với các địa chỉ IP tương ứng với mạng 203.162.0.xxx

Chú ý :

Trước mỗi phần khai báo domain thường có dòng

$ORIGIN *domain.*

Để khai báo giá trị mặc định của domain. Cho phép trong phần khai báo giá trị không phải khai báo lặp lại phần domain mặc định.

Ví dụ :

vdc.com.vn. IN A 203.162.0.49

hoặc

```
$ORIGIN com.vn.
vdc             IN      A       203.162.0.49
```

Dấu "**;**" được sử dụng làm ký hiệu dòng chú thích, các phần sau dấu ";" đều không có tác dụng.

Định nghĩa cấu hình (name.conf)

Khi các file cơ sở dữ liệu (zone file) thì cần phải cấu hình để dns server đọc các zone file đó. Đối với hệ thống BIND cơ chế chỉ dẫn name server đọc các zone file được khai trong file named.conf nó được nằm trong thư mục /etc hoặc /usr/local/etc

Ví dụ : khai báo file db trong file named.conf:

```
        ; khai báo cho zone file domain.vn
zone "vn." in {
        type master;
        file "db.vn";
};
        ;khai báo cho zone file domain.gov.vn
zone "gov.vn." in {
        type master;
        file "db.gov.vn";
};
        ;khai báo cho zone ngược 203.162.0.xxx
zone "0.162.203.in-addr.arpa" in {
        type master;
        file "db.203.162.0";
};
        ;khai báo cho zone ngược 203.162.1.xxx
 zone "1.162.203.in-addr.arpa" in {
```

```
        type master;
        file "db.203.162.1";
};
```

Chú ý: sau mỗi lần thay đổi dữ liệu để sửa đổi có tác dụng thì cần phải làm động tác để dns server cập nhập thay đổi

```
%su
%password:
# ps -ef | grep named
   root 17413     1  5   Sep 07 ?       189:52 /usr/local/sbin/named
# kill -HUP 17413
```

Còn để chạy dns server

```
#/usr/local/sbin/named
```

Hướng dẫn sử dụng nslookup

nslookup - là công cụ trên internet cho phép truy vấn tên miền và địa chỉ IP một cách tương tác.

Cấu trúc câu lệnh

nslookup [-option ...] [host-to-find | - [server]]

Miêu tả các lệnh của nslookup

server domain & lserver domain Change the default server to domain. Lserver uses the initial server to look up information about domain while server uses the current default server. If an authoritative answer can't be found, the names of servers that might have the answer are returned.

root Thay đổi server mặc định sẽ làm root cho domain truy vấn.

ls [option] domain [>> filename]

Hiện danh sách thông tin của domain. Mặc định là hiện tên của host và địa chỉ IP. Ta có thể sử dụng các lựa chọn để hiện nhiều thông tin hơn:

-t querytype hiện danh sách tất cả bản ghi xác định bởi loại querytype

-a hiện danh sách các bí danh (aliaes) của domain host (tương tự như -t CNAME)

-d hiện danh sách các bản ghi của domain (tương tự như -t ANY)

-h hiện danh sách thông tin về CPU và thông tin về hệ điều hành của domain. (tương tự như -t HINFO)

? hiện danh sách các câu lệnh.

exit thoát khỏi chương trình.

set keyword[=value] câu lệnh dùng để thay đổi trạng thái thông tin mà có ảnh hưởng đến truy vấn. Các từ khoá:

all cho phép hiện tất cả các loại bản ghi

[no]debug bật chế độ tìm lỗi. Cho hiện rất nhiều loại thông tin cho phép xác định lỗi truy vấn đến domain. (mặc định=nodebug, viết tắt = [no]deb)

[no]d2 Bật chế độ tìm lỗi mức cao hơn. Tất cả các gói tin truy vấn đều được xuất hiện. (mặc định=nod2)

domain=name Thay đổi domain mặc định vào tên. Khi truy vấn một tên nó sẽ tự động điền thêm domain vào sau.

port=value Chuyển cổng mặc định sử dụng cho TCP/UDP name server thành cổng được thiết lập bởi giá trị này (mặc định= 53, viết tắt = po)

querytype=value

type=value Chọn loại truy vấn thông tin. Có các loại sau:

A truy vấn host (khai báo địa chỉ IP).

CNAME (canonical name) tạo tên bí danh (thường dùng cho web)

HINFO truy vấn loại CPU và hệ điều hành của server.

MINFO thông tin vê hộp thư hoặc mail list.

MX truy vấn về mail exchanger.

NS truy vấn về named zone.

PTR truy vấn chuyển từ địa chỉ IP sang domain.

SOA Thông tin về người quản lý về zone.

TXT Các thông tin khác.

UINFO Thông tin về người dùng.

WKS Hỗ trợ cho các dịch vụ khác.

Các loại khác (**ANY**, **AXFR**, **MB**, **MD**, **MF**, **NULL**) được miêu tả chi tiết trong tiêu chuẩn **RFC-1035** . (Mặc định = A, viết tắt = q, ty)

[no]recurse Yêu cầu name server truy vấn tới một server khác nếu nó không có thông tin về domain cần tìm. (mặc định = recurse, viết tắt = [no]rec)

retry=number Thiết lập số lần truy vấn. Khi truy vấn mà không nhận được trả lời trong khoảng thời gian nhất định (thiết lập bằng lệnh set timeout). Khi thời gian hết thì yêu cầu truy vấn sẽ được gửi lại. Và thiết lập ở đây để điều khiển số lần sẽ gửi lại trước khi từ bỏ truy vấn. (Mặc định = 4, viết tắt = ret)

root=host Đổi root server cho host

timeout=number Thiết lập thời gian timeout cho một quá trìn truy vấn tính bằng giây. (mặc định = 5 giây, viết tắt = ti)

[no]vc sử dụng một virtual circuit để gửi yêu cầu truy vấn đến server. (mặc định là = novc, viết tắt = [no]v)

Phân tích lỗi

Nếu truy vấn lookup không thành công thì một thông tin về lỗi sẽ được hiện ra. Và các lỗi có thể là :

Timed out

Server không trả lời truy vấn sau một khoảng thời gian (khoảng thời gian có thể thay đổi bằng câu lệnh *set timeout=value*) và and a certain number of retries (changed with set retry=value).

No response from server

Không có name server đang chạy tại server mà client chỉ đến.

No records

Server không có bản ghi tương ứng loại mà truy vấn cho host đa tồn tại. Loại truy vấn được thiết lập bằng câu lệnh "*set querytype"* .

Non-existent domain

Host hoặc domain name không tồn tại.

Connection refused

Network is unreachable

Kết nối tới name server hoặc finger server không thể được tại thời điển này. Lệnh này thường xuất hiện với các yêu cầu của câu lện ls và finger.

Server failure

Name server tìm thấy lỗi trong dữ liệu về domain và không thể đưa ra câu trả lời đúng.

Refused

Name server từ chối yêu cầu trả lời.

Format error

Name server thấy rằng các gói tin yêu cầu không đúng định dạng. Nó có thể là lỗi của chương trình nslookup.

Ví dụ :

Truy vấn dns sử dụng bản ghi a cho domain home.vnn.vn có địa chỉ IP là 203.162.0.12	Default Server: vdc-hn01.vnn.vn Address: 203.162.0.11 Aliases: 11.0.162.203.in-addr.arpa > set querytype=a > home.vnn.vn Server: vdc-hn01.vnn.vn Address: 203.162.0.11 Aliases: 11.0.162.203.in-addr.arpa Name: home.vnn.vn Address: 203.162.0.12 >
Truy vấn bản nghi mx (mail) cho domain hn.vnn.vn nó trỏ đến các host mu13.vnn.vn có địa chỉ 203.162.0.55 và	> set querytype=mx > hn.vnn.vn Server: vdc-hn01.vnn.vn Address: 203.162.0.11 Aliases: 11.0.162.203.in-addr.arpa

mu14.vnn.vn có địa chỉ 203.162.0.64	hn.vnn.vn MX preference = 20, mail exchanger = mu13.vnn.vn hn.vnn.vn MX preference = 10, mail exchanger = mu14.vnn.vn vnn.vn nameserver = vdc-hn01.vnn.vn vnn.vn nameserver = hcm-server1.vnn.vn mu13.vnn.vn internet address = 203.162.0.55 mu14.vnn.vn internet address = 203.162.0.64 vdc-hn01.vnn.vn internet address = 203.162.0.11 hcm-server1.vnn.vn internet address = 203.162.4.1 >
Truy vấn loại ns (name server) cho domain vn do các server nào quản lý sẽ cho ta một danh sách các nameserver quản ly các domain có đuôi vn	> set querytype=ns > vn Server: vdc-hn01.vnn.vn Address: 203.162.0.11 Aliases: 11.0.162.203.in-addr.arpa Non-authoritative answer: vn nameserver = dns-hcm01.vnnic.net.vn vn nameserver = ns.ripe.net vn nameserver = dns1.vn vn nameserver = ns1.gip.net vn nameserver = ns2.gip.net vn nameserver = ns3.rip.net vn nameserver = dns1.vnnic.net.vn vn nameserver = cheops.anu.edu.au dns-hcm01.vnnic.net.vn internet address = 203.162.87.66 ns.ripe.net AAAA IPv6 address = 2001:610:240:0:53:0:0:193 ns.ripe.net internet address = 193.0.0.193 dns1.vn internet address = 203.162.3.235

```
ns1.gip.net     internet address = 204.59.144.222
ns2.gip.net     internet address = 204.59.1.222
dns1.vnnic.net.vn       internet address = 203.162.57.105
cheops.anu.edu.au       internet address = 150.203.224.24
>
```

Chương 5 : Dịch vụ truy cập từ xa và Dịch vụ Proxy

Chương 5 cung cấp các kiến thức cơ bản của hai nội dung dịch vụ phổ biến trên mạng máy tính: dịch vụ truy cập từ xa và dịch vụ proxy.

Việc truy cập từ xa là nhu cầu thiết yếu mở rộng phạm vi hoạt động mạng của các tổ chức, công ty. Nội dung truy cập từ xa giới thiệu trong chương này là truy cập qua mạng thoại PSTN. Đây là hình thức truy cập từ xa cho tốc độ truy cập thấp vừa phải nhưng lại có tính phổ biến rộng rãi và dễ thiết lập nhất.

Dịch vụ proxy trên mạng được phát triển cho các mục đích tăng cường tốc độ truy nhập cho khách hàng trong mạng, tiết kiệm được tài nguyên mạng (địa chỉ IP) và đảm bảo được an toàn cho mạng lưới khi bắt buộc phải cung cấp truy nhập ra mạng ngoài hay ra mạng Internet. Thiết lập dịch vụ proxy là công tác mọi quản trị hệ thống mạng cần biết vì các nhu cầu kết nối liên mạng và kết nối Internet càng ngày càng trở nên không thể thiếu cho bất kỳ tổ chức, công ty nào.

Chương 5 yêu cầu các học viên nên trang bị các kiến thức cơ bản về mạng điện thoại PSTN, kiến thức về các giao thức mạng WAN PPP, SLIP... các giao thức xác thực như RADIUS...Trong phần proxy, học viên cần làm quen với khái niệm chuyển đổi địa chỉ NAT, hoạt động của các giao thức TCP/IP.

Mục 1 : Dịch vụ truy cập từ xa (Remote Access)

I. Các khái niệm và các giao thức.

I.1. Tổng quan về dịch vụ truy cập từ xa.

Dịch vụ truy nhập từ xa (Remote Access Service) cho phép người dùng từ xa có thể truy cập từ một máy tính qua một môi trường mạng truyền dẫn (ví dụ mạng điện thoại công cộng) đến một mạng dùng riêng như thể máy tính đó

được kết nối trực tiếp trong mạng đó. Người dùng từ xa kết nối tới mạng đó thông qua một máy chủ dịch vụ gọi là máy chủ truy cập (Access server). Khi đó người dùng từ xa có thể sử dụng tài nguyên trên trên mạng như là một máy tính kết nối trực tiếp trong mạng đó. Dịch vụ truy nhập từ xa cũng cung cấp khả năng tạo lập một kết nối WAN thông qua các mạng phương tiện truyền dẫn giá thành thấp như mạng thoại công cộng. Dịch vụ truy cập từ xa cũng là cầu nối để một máy tính hay một mạng máy tính thông qua nó được nối đến Internet theo cách được coi là hợp lý với chi phí không cao, phù hợp với các doanh nghiệp, tổ chức qui mô vừa và nhỏ. Khi lựa chọn và thiết kế giải pháp truy cập từ xa, chúng ta cần thiết phải quan tâm đến các yêu cầu sau:

– Số lượng kết nối tối đa có thể để phục vụ người dùng từ xa.

– Các nguồn tài nguyên mà người dùng từ xa muốn muốn truy cập.

– Công nghệ, phương thức và thông lượng kết nối. Ví dụ, các kết nối có thể sử dụng modem thông qua mạng điện thoại công cộng PSTN, mạng số hoá tích hợp các dịch vụ ISDN...

– Các phương thức an toàn cho truy cập từ xa, phương thức xác thực người dùng, phương thức mã hoá dữ liệu

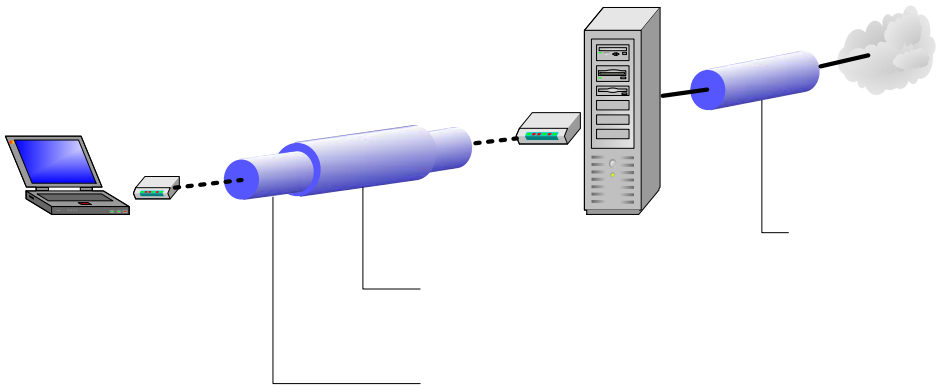
– Các giao thức mạng sử dụng để kết nối.

I.2. Kết nối truy cập từ xa và các giao thức sử dụng trong truy cập từ xa

1.Kết nối truy cập từ xa

Tiến trình truy cập từ xa được mô tả như sau: người dùng từ xa khởi tạo một kết nối tới máy chủ truy cập. Kết nối này được tạo lập bằng việc sử dụng một giao thức truy cập từ xa (ví dụ giao thức PPP- Point to Point Protocol). Máy chủ truy cập xác thực người dùng và chấp nhận kết nối cho tới khi kết thúc bởi người dùng hoặc người quản trị hệ thống. Máy chủ truy cập đóng vai trò như một gateway bằng việc trao đổi dữ liệu giữa người dùng từ xa và mạng nội bộ. Bằng việc sử dụng kết nối này, người dùng từ xa gửi và nhận dữ liệu từ máy chủ truy cập. Dữ liệu được truyền trong các khuôn dạng được định nghĩa bởi các giao thức mạng (ví dụ giao thức TCP/IP) và sau đó được đóng gói bởi

các giao thức truy cập từ xa. Tất cả các dịch vụ và các nguồn tài nguyên trong mạng người dùng từ xa đều có thể sử dụng thông qua kết nối truy cập từ xa này (hình 5.1)



Hình 5.1

2. Giao thức truy cập từ xa

SLIP (Serial Line Interface Protocol), PPP và Microsoft RAS là các giao thức truy cập để tạo lập kết nối được sử dụng trong truy cập từ xa. SLIP là giao thức truy cập kết nối điểm-điểm và chỉ hỗ trợ sử dụng với giao thức IP, hiện nay hầu như không còn được sử dụng. Microsoft RAS là giao thức riêng của Microsoft hỗ trợ sử dụng cùng với các giao thức NetBIOS, NetBEUI và được sử dụng trong các phiên bản cũ của Microsoft.

PPP giao thức truy cập kết nối điểm-điểm với khá nhiều tính năng ưu việt, là một giao thức chuẩn được hầu hết các nhà cung cấp hỗ trợ. RFC 1661 định nghĩa về PPP. Chức năng cơ bản của PPP là đóng gói thông tin giao thức lớp mạng thông qua các liên kết điểm – điểm.

Cơ chế làm việc và vận hành của PPP như sau: Để thiết lập truyền thông, mỗi đầu cuối của liên kết PPP phải gửi các gói LCP (Link Control Protocol) để thiết lập và kiểm tra liên kết dữ liệu. Sau khi liên kết được thiết lập với các tính năng tùy chọn được sắp đặt và thỏa thuận giữa hai đầu liên kết, PPP gửi các gói NCP (Network Control Protocol) để lựa chọn và cấu hình một hoặc nhiều giao thức lớp mạng. Mỗi lần một giao thức lớp mạng lựa chọn đã được cấu hình, lưu lượng từ mỗi giao thức lớp mạng có thể gửi qua liên kết

này. Liên kết tồn tại cho đến khi các gói LCP hoặc NCP đóng kết nối hoặc đến khi một sự kiện bên ngoài xẩy ra (chẳng hạn như một sự kiện hẹn giờ hay một sự can thiệp của người quản trị). Nói cách khác PPP là một con đường mở đồng thời cho nhiều giao thức.

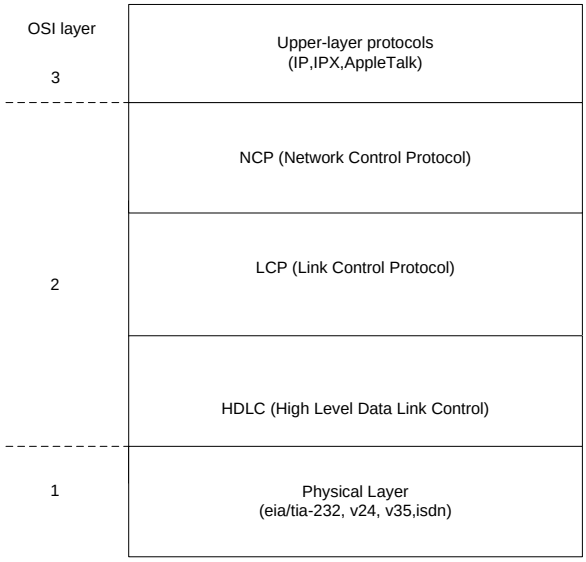
PPP khởi đầu được phát triển trong môi trường mạng IP, tuy nhiên nó thực hiện các chức năng độc lập với các giao thức lớp 3 và có thể được sử dụng cho các giao thức lớp mạng khác nhau. Như đã đề cập, PPP đóng gói các thủ tục lớp mạng đã được cấu hình để chuyển qua một liên kết PPP. PPP có nhiều các tính năng khiến nó rất mềm dẻo và linh hoạt, bao gồm:

- Ghép nối với các giao thức lớp mạng
- Lập cấu hình liên kết
- Kiểm tra chất lượng liên kết
- Nhận thực
- Nén các thông tin tiếp đầu
- Phát hiện lỗi
- Thỏa thuận các thông số liên kết

PPP hỗ trợ các tính năng này thông qua việc cung cấp LCP có khả năng mở rộng và NCP để thỏa thuận các thông số và các chức năng tùy chọn giữa các đầu cuối. Các giao thức, các tính năng tùy chọn, kiểu xác thực người dùng tất cả đều được truyền thông trong khi khởi tạo liên kết giữa hai điểm.

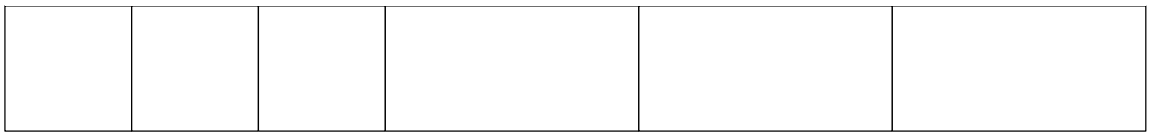
PPP có thể hoạt động trong bất kỳ giao diện DTE/DCE nào, PPP có thể hoạt động ở chế độ đồng bộ hoặc không đồng bộ. Ngoài những yêu cầu khác của các giao diện DTE/DCE, PPP không có hạn chế nào về tốc độ truyền dẫn.

Trong hầu hết các công nghệ mạng WAN, mô hình lớp được đưa ra để có những điểm liên hệ với mô hình OSI và để diễn tả vận hành của các công nghệ cụ thể. PPP không khác nhiều so với các công nghệ khác. PPP cũng có mô hình lớp để định nghĩa các cấu trúc và chức năng (hình 5.2)



Hình 5.2

Cũng như hầu hết các công nghệ, PPP có cấu trúc khung, cấu trúc này cho phép đóng gói bất cứ giao thức lớp 3 nào. Dưới đây là cấu trúc khung PPP (hình 5.3)



Hình 5.3

Các trường của khung PPP như sau:

Cờ: độ dài 1 byte sử dụng để chỉ ra rằng đây là điểm bắt đầu hay kết thúc một khung, trường này là một dãy bit 01111110

Địa chỉ: độ dài 1 byte bao gồm dãy bit 11111111, là địa chỉ quảng bá chuẩn. PPP không gán từng địa chỉ riêng.

Giao thức: độ dài 2 byte, nhận dạng giao thức đóng gói. Giá trị cập nhật của trường này được chỉ ra trong RFC 1700

Dữ liệu: có độ dài thay đổi, có thể 0 hoặc nhiều byte là các dữ liệu cho kiểu giao thức cụ thể đượoc chỉ ra trong trường giao thức. Phần cuối cùng của trường dữ liệu được nhận biết bằng cách đặt cờ và tiếp sau nó là 2 byte FCS. Giá trị ngầm định của trường này là 1500 byte. Tuy vậy giá trị lớn hơn có thể được sử dụng để tăng độ dài cho trường dữ lliệu.

FCS: thường là 2 byte, có thể sử dụng 4 byte FCS để tăng khả năng phát hiện lỗi.

LCP có thể thỏa thuận để chấp nhận sự thay đổi cấu trúc khung PPP chuẩn giữa hai đầu cuối của liên kết. Các khung đã thay đổi luôn luôn dễ nhận biết hơn so với các khung chuẩn. LCP cung cấp phương pháp để thiết lập, cấu hình, duy trì và kết thúc một kết nối điểm-điểm. LCP thực hiện các chức năng này thông qua bốn giai đoạn. Đầu tiên, LCP thực hiện thiết lập và thỏa thuận cấu hình giữa liên kết điểm điểm. Trước khi bất kỳ đơn vị dữ liệu lớp mạng nào được chuyển, LCP đầu tiên phải mở kết nối và thỏa thuận các thông số thiết lập. Quá trình này được hoàn thành khi một khung nhận biết cấu hình đã được gửi và nhận. Tiếp theo, LCP xác định chất lượng liên kết. Liên kết được kiểm tra để xác định xem liệu chất lượng có đủ để khởi tạo các giao thức lớp mạng không. Việc truyền dẫn của giao thức lớp mạng bị đình lại cho đến khi giai đoạn này hoàn tất. LCP cho phép đây là một tùy chọn sau giai đoạn thiết lập và thỏa thuận cấu hình của liên kết. Sau đó LCP thực hiện thỏa thuận cấu hình giao thức lớp mạng. Các giao thức lớp mạng có thể được cấu hình riêng rẽ bới NCP thích hợp và được khởi tạo hay dỡ bỏ vào bất kỳ thời điểm nào. Cuối cùng, LCP kết thúc liên kết khi xuất hiện yêu cầu từ người dùng hoặc theo các bộ định thời gian, do lỗi truyền dẫn hay do các yếu tố vật lý khác.

Ba kiểu khung LCP được sử dụng để hoàn thành các công việc đối với từng giai đoạn: khung thiết lập liên kết được sử dụng để thiết lập và cấu hình một liên kết, khung kết thúc liên kết được sử dụng để kết thúc một liên kết, khung duy trì liên kết được sử dụng để quản lý và gỡ rối liên kết.

3.Các giao thức mạng sử dụng trong truy cập từ xa.

Khi triển khai dịch vụ truy cập từ xa, các giao thức mạng thường được sử dụng là giao thức TCP/IP, IPX, NETBEUI.

TCP/IP là một bộ giao thức gồm có giao thức TCP và giao thức IP cùng làm việc với nhau để cung cấp phương tiện truyền thông trên mạng. TCP/IP là một bộ giao thức cơ bản, làm nền tảng cho truyền thông liên mạng là bộ giao thức mạng được sử dụng phổ biến nhất hiện nay. Với khả năng định tuyến và mở rộng, TCP/IP hỗ trợ một cách linh hoạt và phù hợp cho các tất cả các mạng.

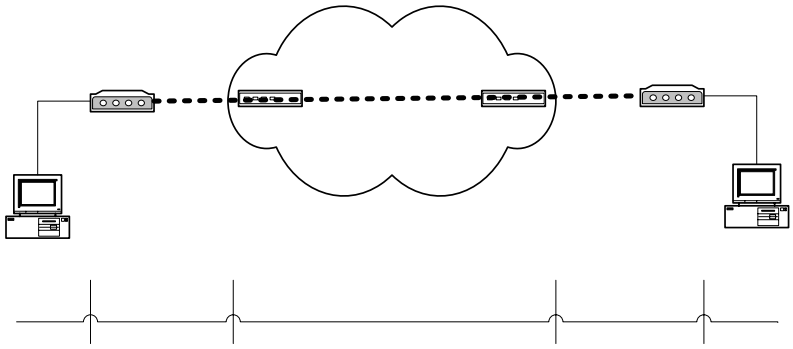
IPX (Internet Packet Exchange) là giao thức được sử dụng cho các mạng Novell NetWare. IPX là một giao thức có khả năng định tuyến và thường được sử dụng với các hệ thống mạng trước đây.

NetBEUI là giao thức dùng cho mạng cục bộ LAN của Microsoft. NetBEUI cho ta nhiều tiện ích và hầu như không phải làm gì nhiều với NetBEUI. Thông qua NetBEUI ta có thể truy cập tất cả các tài nguyên trên mạng. NETBEUI là một giao thức không có khả năng định tuyến và chỉ thích hợp với mô hình mạng nhỏ, đơn giản.

I.3. Modem và các phương thức kết nối vật lý.

1. Modem.

Máy tính làm việc với dữ liệu dạng số, khi truyền thông trên môi trường truyền dẫn với các dạng tín hiệu khác (ví dụ như với mạng điện thoại công cộng làm việc với các tín hiệu tương tự) ta cần một thiết bị để chuyển đổi tín hiệu số thành tín hiệu thích nghi với môi trường truyền dẫn, thiết bị đó là gọi là Modem (Modulator/demodulator). Như vậy Modem là một thiết bị chuyển đổi tín hiệu số sang dạng tín hiệu phù hợp với môi trường truyền dẫn và ngược lại. Hình dưới là một kết nối sử dụng modem qua mạng điện thoại điển hình (hình 5.4).



Hình 5.4

Các modem sử dụng các phương pháp nén dữ liệu nhằm mục đích tăng tốc độ truyền dữ liệu. Hiệu suất nén dữ liệu phụ thuộc vào dữ liệu, có hai giao thức nén thường được sử dụng là V.42bis và MNP 5. hiệu suất nén của V.42bis và MNP 5 có thể thay đổi từ 0 đến 400 % hay cao hơn phụ thuộc vào dữ liệu tự nhiên

Chuẩn modem V.90 cho phép các modem nhận dữ liệu với tốc độ 56 Kbps qua mạng điện thoại công cộng (PSTN). V.90 xem mạng PSTN như là một mạng số và chúng sẽ mã hóa dòng dữ liệu xuống theo kỹ thuật số thay vì điều chế để gửi đi như các chuẩn điều chế trước đây. Trong khi đó theo hướng ngược lại từ khách hàng đến nhà cung cấp dịch vụ dòng dữ liệu lên vẫn được điều chế theo các nguyên tắc thông thường và tốc độ tối ta đạt được là 33.6 Kbps, giao thức hướng lên này dựa trên chuẩn V.34

PC1

Digital A

Sự khác nhau giữa tín hiệu số ban đầu với tín hiệu số được phục hồi tại đầu nhận gọi là tạp âm lượng tử hóa (nhiễu lượng tử), chính tạp âm này đã hạn chế tốc độ truyền dữ liệu. Giữa các modem đầu cuối có một cấu trúc hạ tầng cho việc kết nối đó là mạng thoại công cộng. Các chuẩn modem trước đây đều giả sử cả hai đầu của kết nối giống nhau là có một kết nối tương tự vào mạng điện thoại công cộng, công nghệ V.90 đã lợi dụng ưu điểm của tổ chức mạng mà một đầu kết nối giữa hệ thống truy cập từ xa và mạng thoại công cộng là dạng số hoàn toàn còn đầu kia vẫn được kết nối vào mạng PSTN theo dạng tương tự nhờ đó tận dụng được các ưu điểm của liên kết số tốc độ cao, vì chỉ có quá trình biến đổi A/D mới gây ra tạp âm với các kết nối số thì không có lượng tử hóa do đó nhiễu lượng tử rất ít trong cấu trúc mạng này.

Định luật shanon nói rằng đường dây điện thoại tương tự hạn chế tốc độ truyền dữ liệu ở khoảng 35 kbps mà không xem xét đến một thực tế là một đầu của truyền thông đã được số hóa nên giảm nhỏ lượng tạp âm gây ra sự chậm trễ trong việc truyền dữ liệu. Nhiễu lượng tử đã giới hạn chuẩn truyền thông V.34 ở tốc độ 33.6 kbps, nhưng nhiễu lượng tử chỉ có ảnh hưởng khi chuyển đổi tương tự - số mà không có ảnh hưởng khi chuyển đổi số-tương tự và đây chính là chìa khóa cho công nghệ V.90 đồng thời cũng giải thích được vì sao tốc độ download có thể đạt được 56 kbps còn khi upload tốc độ chỉ đạt 33.6 kbps. Dữ liệu chuyển đi từ modem số V.90 qua mạng PSTN là một dòng số với tốc độ 64 Kbps nhưng tại sao V.90 chỉ hỗ trợ tốc độ đến 56 Kbps, vì các lí do sau: Thứ nhất mặc dù nhiễu lượng tử đã được bỏ qua nhưng nhiễu mức thấp do bộ chuyển đổi số - tương tự là không tuyến tính, do ảnh hưởng của vòng loop nội hạt. Lý do thứ hai là các tổ chức quốc tế có qui định chặt chẽ về mức năng lượng tín hiệu nhằm hạn chế nhiễu xuyên âm giữa các dây dẫn đặt gần kề nhau, và qui định này tương ứng với mức năng lượng tối đa trên đường dây điện thoại tương ứng là 56 kbps

Để xây dựng một hệ thống truy cập từ xa qua mạng thoại công cộng đạt được tốc độ 56 kbps giữa hai đầu kết nối cần hội đủ ba điều kiện sau: thứ nhất, một đầu của kết nối (thường là đầu trung tâm mạng) phải là kết nối số tới mạng PSTN. Thứ hai, chuẩn modem V.90 hỗ trợ tại hai đầu cuối của nối kết. Thứ ba, chỉ có một chuyển đổi duy nhất số-tương tự trên mạng thoại giữa hai đầu của kết nối

Khi vận hành modem V.90 thăm dò đường thoại để quyết định xem nó sẽ làm việc theo tiêu chuẩn nào, nếu phát hiện ra bất kỳ một chuyển đổi số-tương tự nào thì nó đơn giản chỉ làm việc ở chuẩn V.34 và cũng cố gắng kết nối ở chuẩn này nếu modem đầu xa không hỗ trợ chuẩn V.90.

2.Các phương thức kết nối vật lý cơ bản:

Một phương thức phổ biến và sẽ được dùng nhiều đó là kết nối qua mạng điện thoại công cộng (PSTN). Máy tính được nối qua một modem lắp đặt bên trong (Internal modem) hoặc qua cổng truyền số liệu nối tiếp COM port. Tốc độ truyền tối đa hiện nay có thể có được bằng phương thức này có thể lên đến 56 Kbps cho chiều lấy dữ liệu xuống và 33,6Kbps cho chiều truyền dữ liệu hướng lên với các chuẩn điều chế tín hiệu phổ biến V90, K56Flex, X2. Ta cũng

có thể sử dụng modem có yêu cầu về hạ tầng cơ sở thấp hơn với chuẩn điều chế V.24, V.32Bis, V.32...

Phương thức thứ hai là sử dụng mạng truyền số liệu số đa dịch vụ ISDN. Phương thức này đòi hỏi chi phí cao hơn và ngày càng được phổ biến rộng rãi. Ta có được khá nhiều các lợi ích từ việc sử dụng mạng ISDN mà một trong số đó là tốc độ. Ta có thể sử dụng các lựa chọn ISDN 2B+D BRI (2x64Kbps dữ liệu + 16Kbps dùng cho điều khiển) hoặc 23B+D PRI (23x64Kbps + 64Kbps) thông qua thiết bị TA (Terminal Adapter) hay các card ISDN.

Một phương thức khác nhưng ít được sử dụng là qua mạng truyền số liệu X.25, tốc độ không cao nhưng an toàn và bảo mật cao hơn. Yêu cầu cho người sử dụng trong trường hợp này là phải có sử dụng card truyền số liệu X.25 hoặc một thiết bị được gọi là PAD (Packet Asssembled Disassembled). Ta cũng có thể sử dụng các kết nối trực tiếp qua cáp modem, phương thức này cho ta các kết nối tốc độ cao nhưng phải thông qua các modem truyền số liệu có giá thành cao.

II. An toàn trong truy cập từ xa

II.1. Các phương thức xác thực kết nối

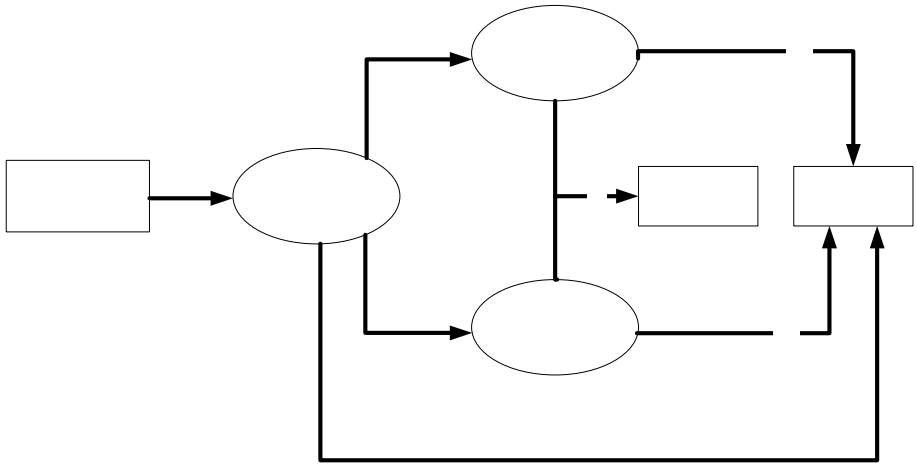
1.Qúa trình nhận thực.

Tiến trình nhận thực với các giao thức xác thực được thực hiện khi người dùng từ xa có các yêu cầu xác thực tới máy chủ truy cập, một thỏa thuận giữa người dùng từ xa và máy chủ truy cập để xác định phương thức xác thực sẽ sử dụng. Nếu không có phương thức nhận thực nào được sử dụng, tiến trình PPP sẽ khởi tạo kết nối giữa hai điểm ngay lập tức.

Phương thức xác thực có thể được sử dụng với các hình thức kiểm tra cơ sở dữ liệu địa phương (lưu trữ các thông tin về username và password ngay trên máy chủ truy cập) xem các thông tin về username và password được gửi đến có trùng với trong cơ sở dữ liệu hay không. Hoặc là gửi các yêu cầu xác thực tới một server khác để xác thực thường sử dụng là các RADIUS server (sẽ được trình bày ở phần sau)

Sau khi kiểm tra các thông tin gửi trả lại từ cơ sở dữ liệu địa phương hoặc từ RADIUS server. Nếu hợp lệ, tiến trình PPP sẽ khởi tạo một kết nối, nếu không yêu cầu kết nối của người dùng sẽ bị từ chối. (hình 5.5)

.

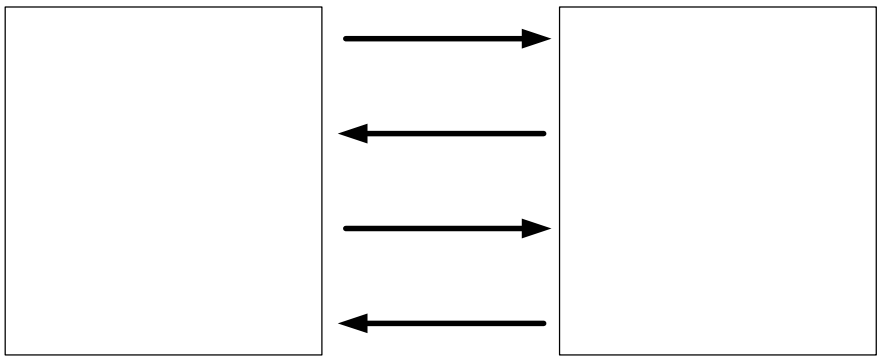


Hình 5.5

2.Giao thức xác thực PAP

PAP là một phương thức xác thực kết nối không an toàn, nếu sử dụng một chương trình phân tích gói tin trên đường kết nối ta có thể nhìn thấy các thông tin về username và password dưới dạng đọc được. Điều này có nghĩa là các thông tin gửi đi từ người dùng từ xa tới máy chủ truy cập không được mã hóa mà được gửi đi dưới dạng đọc được đó chính là lý do PAP không an toàn. Hình dưới mô tả quá trình xác thực PAP, sau khi thỏa thuận giao thức xác thực PAP trên liên kết PPP giữa các đầu cuối, người dùng từ xa gửi thông tin (username:nntrong, password:ras123) tới máy chủ truy cập từ xa, sau khi kiểm tra các thông tin này trong cơ sở dữ liệu của mình, máy chủ truy cập từ ra sẽ quyết định xem liệu yêu cầu kết nối có được thực hiện hay không (hình 5.6)

Incoming
PPP negotiation



Remote user

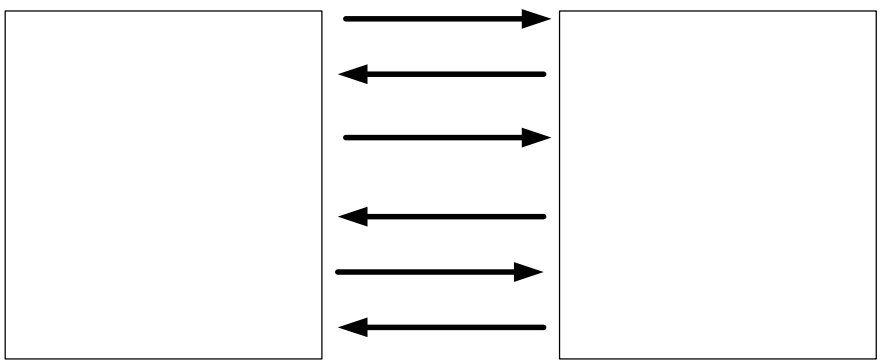
Hình 5.6

3.Giao thức xác thực CHAP

Sau khi thỏa thuận giao thức xác thực CHAP trên liên kết PPP giữa các đầu cuối, máy chủ truy cập gửi một "challenge" tới người dùng từ xa. Người dùng từ xa phúc đáp lại một giá trị được tính toán sử dụng tiến trình xử lý một chiều (hash). máy chủ truy cập kiểm tra và so sánh thông tin phúc đáp với giá trị hash mà tự nó tính được. Nếu các giá trị này bằng nhau việc xác thực là thành công, ngược lại kết nối sẽ bị hủy bỏ. Như vậy CHAP cung cấp cơ chế an toàn thông qua việc sử dụng giá trị challenge thay đổi, duy nhất và không thể đoán được. Các thông tin về username và password không được gửi đi dưới dạng đọc được trên mạng và do đó chống lại các truy cập trái phép bằng hình thức lấy trộm password trên đường kết nối (hình 5.7).

Inputs name ar

when pro



Hình 5.7

4.Giao thức xác thực mở rộng EAP

Ngoài các giao thức kiểm tra tính xác thực cơ bản PAP, CHAP, trong Microsoft Windows 2000 hỗ trợ thêm một số giao thức cho ta các khả năng nâng cao độ an toàn, bảo mật và đa truy nhập đó là giao thức xác thực mở rộng EAP (Extensible Authentication Protocol).

EAP cho phép có được một cơ cấu xác thực tuỳ ý để công nhận một kết nối gọi vào. Người sử dụng và máy chủ truy nhập từ xa sẽ trao đổi để tìm ra giao thức chính xác được sử dụng. EAP hỗ trợ các hình thức sau:

– Sử dụng các card vật lý dùng để cung cấp mật khẩu. Các card này dùng một số các phương thức xác thực khác nhau như sử dụng các đoạn mã thay đổi theo mỗi lượt sử dụng.

– Hỗ trợ MD5-CHAP, giao thức mã hoá tên người sử dụng, mật khẩu sử dụng thuật toán mã hoá MD5 (Message Digest 5).

– Hỗ trợ sử dụng cho các thẻ thông minh. Thẻ thông minh bao gồm thẻ và thiết bị đọc thẻ. Các thông tin xác thực về cá nhân người dùng được ghi lại trong các thẻ này.

– Các nhà phát triển phần mềm độc lập sử dụng giao diện chương trình ứng dụng EAP có thể phát triển các module chương trình cho các công nghệ áp dụng cho thẻ nhận dạng, thẻ thông minh, các phần cứng sinh học như nhận dạng võng mạc, các hệ thống sử dụng mật khẩu một lần.

II.2. Các phương thức mã hóa dữ liệu.

Dịch vụ truy cập từ xa cung cấp cơ chế an toàn bằng việc mã hóa và giải mã dữ liệu truyền giữa người dùng truy cập từ xa và máy chủ truy cập. Có hai phương thức mã hóa dữ liệu thường được sử dụng đó là mã hóa đối xứng và mã hóa phi đối xứng.

Phương thức mã hoá đối xứng, thông tin ở dạng đọc được, được mã hoá sử dụng khóa bí mật (khoá mà chỉ có người mã hoá mới biết được) tạo thành thông tin đã được mã hoá. ở phía nhận, thông tin mã hoá được giải mã cùng với khóa bí mật thành dạng gốc ban đầu. Điểm chú ý của phương pháp mã hoá này là việc sử dụng khoá bí mật cho cả quá trình mã hoá và quá trình giải mã. Do

đó, nhược điểm chính của phương thức này là cần có quá trình trao đổi khoá bí mật, dẫn đến tình trạng dễ bị lộ khoá bí mật.

Phương pháp mã hoá phi đối xứng, để khắc phục điểm hạn chế của phương pháp mã hoá đối xứng là quá trình trao đổi khoá bí mật, người ta đã sử dụng phương pháp mã hoá phi đối xứng sử dụng một cặp khoá tương ứng với nhau gọi là phương thức mã hoá phi đối xứng dùng khoá công khai. Phương thức mã hóa này sử dụng hai khóa là khóa công khai và khóa bí mật có các quan hệ toán học với nhau. Trong đó khóa bí mật được giữ bí mật và không có khả năng bị lộ do không cần phải trao đổi trên mạng. Khóa công khai không phải giữ bí mật và mọi người đều có thể nhận được khoá này. Do phương thức mã hóa này sử dụng 2 khóa khác nhau, nên người ta gọi nó là phương thức mã hóa phi đối xứng. Mặc dù khóa bí mật được giữ bí mật, nhưng không giống với "secret Key" được sử dụng trong phương thức mã hóa đối xứng sử dụng khoá bí mật do khóa bí mật không được trao đổi trên mạng. Khóa công khai và khóa bí mật tương ứng của nó có quan hệ toán học với nhau và được sinh ra sau khi thực hiện các hàm toàn học; nhưng các hàm toán học này luôn thoả mãn điều kiện là sao cho không thể tìm được khóa bí mật từ khóa công cộng và ngược lại. Do có mối quan hệ toán học với nhau, thông tin được mã hóa bằng khóa công khai chỉ có thể giải mã được bằng khóa bí mật tương ứng.

Giao thức thường được sử dụng để mã hóa dữ liệu hiện nay là giao thức IPsec. Hầu hết các máy chủ truy cập dựa trên phần cứng hay mềm hiện nay đều hỗ trợ IPSec. IPSec là một giao thức bao gồm các chuẩn mở bảo đảm các vấn đề bảo mật, an toàn và toàn vẹn dữ liệu cho các kết nối qua mạng sử dụng giao thức IP bằng các biện pháp mã hoá. IPSec bảo vệ chống lại các hành động phá hoại từ bên ngoài. Các client khởi tạo một mối liên quan bảo mật hoạt động tương tự như khoá công khai để mã hoá dữ liệu.

Ta có thể sử dụng các chính sách áp dụng cho IPSec để cấu hình nó. Các chính sách cung cấp nhiều mức độ và khả năng để bảo đảm an toàn cho từng loại dữ liệu. Các chính sách cho IPSec sẽ được thiết lập cho phù hợp với từng người dùng, từng nhóm người dùng, cho một ứng dụng, một nhóm miền hay toàn bộ hệ thống mạng.

III. Triển khai dịch vụ truy cập từ xa

III.1. Kết nối gọi vào và kết nối gọi ra

Cấu hình máy chủ truy cập để tạo lập các kết nối gọi vào cho phép người dùng từ xa truy cập vào mạng. Các thông số cơ bản thường được cấu hình khi tạo lập các kết nối gọi vào bao gồm xác định các phương thức xác thực người dùng, mã hóa hay không mã hóa dữ liệu, các phương thức mã hóa dữ liệu nếu yêu cầu, các giao thức mạng sẽ được sử dụng cho truy nhập từ xa, các thiết đặt về chính sách và các quyền truy nhập của người dùng từ xa, mức độ được phép truy nhập như thế nào, xác định phương thức cấp phát địa chỉ IP cho máy truy nhập từ xa, các yêu cầu cấu hình để tạo lập các kết nối VPN…

Kết nối gọi ra có thể được thiết lập để gọi ra tới một mạng dùng riêng hoặc tới một ISP. Trong windows 2000 hỗ trợ các hình thức kết nối sau:

Nối tới mạng dùng riêng, ta sẽ phải cung cấp số điện thoại nơi sẽ nối đến. Có thể là số điện thoại của ISP, của mạng dùng riêng hay của máy tính phía xa. Xác định quyền sử dụng kết nối này. .

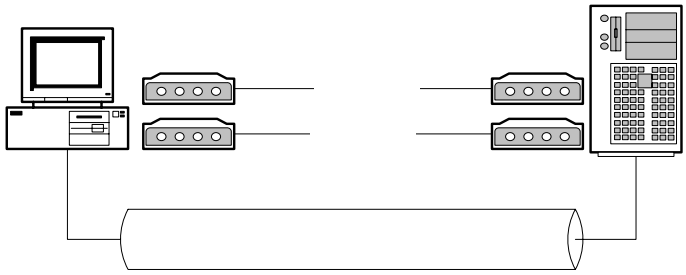
Nối tới Internet, hai lựa chọn có thể là sử dụng truy cập qua đường thoại và sử dụng truy cập qua mạng LAN. Sử dụng đường thoại, các vấn đề ta cần quan tâm là số điện thoại truy nhập, tên và mật khẩu được cung cấp bởi ISP. Sử dụng LAN, ta sẽ phải quan tâm đến proxy server và một số thiết đặt khác.

Tạo lập kết nối VPN, ***VPN là một mạng sử dụng các kết nối dùng giao thức tạo đường hầm (PPTP, L2TP, IPSEC,...) để tạo được các kết nối an toàn, bảo đảm thông tin không bị xâm phạm khi truyền tải qua các mạng công cộng. Tương tự như khi tạo lập một kết nối gọi ra, Nếu cần thiết phải thông qua một ISP trung gian trước khi nối tới mạng dùng riêng, lựa chọn một kết nối gọi ra. Cung cấp địa chỉ máy chủ, địa chỉ mạng nơi mà ta đang muốn nối tới. Các thiết lập khác là thiết đặt các quyền sử dụng kết nối.***

Tạo lập kết nối trực tiếp với máy tính khác, lựa chọn này được sử dụng để kết nối trực tiếp hai máy tính với nhau thông qua một cáp được thiết kế cho nối trực tiếp hai máy tính. Một trong hai máy tính được lựa chọn là chủ và máy tính kia được lựa chọn là tớ. Lựa chọn thiết bị cổng nơi hai máy tính nối với nhau.

III.2. Kết nối sử dụng đa luồng(Multilink)

Multilink là sự kết hợp nhiều liên kết vật lý trong một liên kết logic duy nhất nhằm gia tăng băng thông cho kết nối. Multilink cho phép sử dụng hai hoặc nhiều hơn các cổng truyền thông như là một cổng duy nhất có tốc độ cao. Điều này có nghĩa là ta có thể sử dụng hai modem để kết nối Internet với tốc độ cao gấp đôi so với việc sử dụng một modem. Multilink gia tăng băng thông và giảm độ trễ giữa các hệ thống bằng cơ chế chia các gói dữ liệu và gửi đi trên các mạch song song. Multilink sử dụng giao thức MPPP cho việc quản lý các kết nối của mình. Để sử dụng, MPPP cần phải được hỗ trợ ở cả hai phía của kết nối (hình 5.8).



Hình 5.8

Hình vẽ mô tả kết nối sử dụng Multilink, khi người dùng từ xa sử dụng hai modem và hai đường thoại kết nối với máy chủ truy cập, mỗi kết nối là việc theo chuẩn V.90 có tốc độ 56 kbps sử dụng kỹ thuật Multilink cho phép đạt tốc độ 112 Kbps giữa máy truy cập từ xa và máy chủ truy cập.

III.3. Các chính sách thiết lập cho dịch vụ truy nhập từ xa

Chính sách truy nhập từ xa là tập hợp các điều kiện và các thiết đặt cho phép người quản trị mạng gán cho mỗi người dùng từ xa các quyền truy cập và mức độ sử dụng các nguồn tài nguyên trên mạng. Ta có thể dùng các chính sách để có được nhiều các lựa chọn phù hợp với từng mức độ người dùng, tăng tính mềm dẻo, tính năng động khi cấp quyền truy nhập cho người dùng.

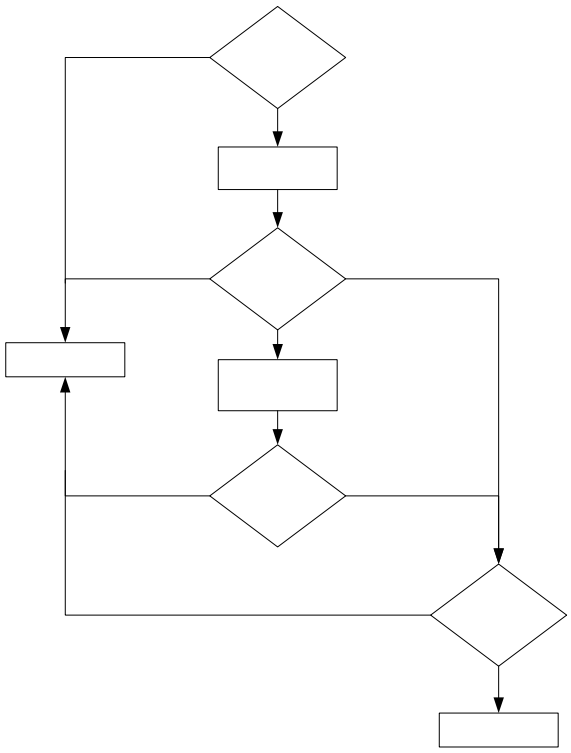
Một chính sách truy nhập từ xa thông thường bao gồm ba thành phần nhằm cung cấp các truy nhập an toàn có kiểm soát đến máy chủ truy cập.

Các điều kiện (Conditions): là một danh sách các tham số như ngày tháng, nhóm người dùng, mã người gọi, địa chỉ IP phù hợp với máy trạm đang nối đến máy chủ truy cập. Bộ chính sách điều kiện đầu tiên này tương ứng với các thông số của yêu cầu kết nối gọi đến được xử lý đối với sự cho phép truy cập và cấu hình.

Sự cho phép (Permission): Các kết nối truy nhập từ xa được cho phép và gán trực tiếp tới mỗi người dùng bởi các thiết đặt trong các chính sách truy nhập từ xa. Ví dụ một chính sách có thể gán tất cả người dùng trong một nhóm nào đấy quyền truy cập chỉ trong giờ làm việc hành chính từ 8:00 A.M đến 5:00 P.M, hay đồng thời gán cho một nhóm người dùng khác quyền truy cập liên tục 24/24.

Profile: Mỗi chính sách đều bao gồm một thiết đặt của profile áp dụng cho kết nối như là các thủ tục xác thực hay mã hóa. Các thiết đặt trong profile được thi hành ngay tới các kết nối. Ví dụ: nếu một profile thiết đặt cho một kết nối mà người dùng chỉ được phép sử dụng trong 30 phút mỗi lần thì người dùng sẽ bị ngắt kết nối tới máy chủ truy cập trong sau 30 phút.

Quá trình thực thi các chính sách truy cập từ xa được mô tả bằng hình dưới (hình 5.9)



Hình 5.9

Các điều kiện được gửi tới để tạo một kết nối, nếu các điều kiện gửi tới này không thích hợp truy cập bị từ chối, nếu thích hợp các điều kiện này được sử dụng để xác định sự truy cập. Tiếp theo máy chủ truy cập kiểm tra các cho phép quay số vào người dùng sẽ bị từ chối nếu thiết đặt này là Deny và được phép truy cập nếu là Allow, nếu thiết đặt là sử dụng các chính sách truy cập để xác định quyền truy cập thì sự cho phép của các chính sách sẽ quyết định quyền truy cập của người dùng. Nếu các chính sách này từ chối truy cập người dùng sẽ bị ngắt kết nối, nếu là cho phép sẽ chuyển tới để kiểm tra các chính sách trong profile là bước cuối cùng để xác định quyền truy cập của người dùng.

III.4. Sử dụng dịch vụ gán địa chỉ động DHCP cho truy cập từ xa

Khi thiết lập một máy chủ truy cập để cho phép người dùng từ xa truy cập vào mạng, ta có thể lựa chọn phương thức mà các máy từ xa có thể nhận được địa chỉ IP.

Với phương thức cấu hình địa chỉ IP tĩnh ngay trên các máy trạm, người dùng phải cấu hình bằng tay địa chỉ IP trên mỗi máy truy cập. Sử dụng phương thức này phải đảm bảo rằng các thông tin cấu hình địa chỉ IP là hợp lệ và chưa được sử dụng trên mạng. Đồng thời các thông tin về default gateway, DNS…cũng phải được cấu hình bằng tay một cách chính xác.Vì lí do này khuyến nghị không nên sử dụngphương pháp này cho việc gán IP cho các máy truy cập từ xa.

Máy chủ truy cập có thể gán động một địa chỉ IP cho các máy truy cập từ xa. Địa chỉ IP này thuộc trong khoảng địa chỉ mà ta đã cấu hình trên máy chủ truy cập. Sử dụng phương pháp này ta cần phải đảm bảo rằng khoảng địa chỉ IP này được dành riêng để cấp phát cho các máy truy cập từ xa.

Phương thức sử dụng DHCP server, máy chủ truy cập nhận địa chỉ IP từ DHCP server và gán cho các máy truy cập từ xa. Phương thức này rất linh hoạt, không cần phải dành riêng một khoảng địa chỉ IP dự trữ cho máy truy cập từ xa và thường được sử dụng trong một mạng có tổ chức và đa dạng trong các hình thức kết nối. Địa chỉ IP được cấp phát cho các máy truy cập từ xa một cách tự động, các thông tin cấu hình khác (Gateway, DNS server…) cũng được cung cấp tập trung, chính xác tới từng máy truy cập đồng thời các máy truy cập cũng không cần thiết phải cấu hình lại khi có các thay đổi về cấu trúc mạng.

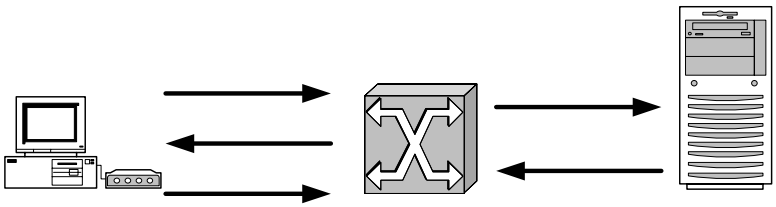
Hoạt động của DHCP được mô tả như sau: Mỗi khi DHCP client khởi động, nó yêu cầu một địa chỉ IP từ DHCP server. Khi DHCP server nhận yêu cầu, nó chọn một địa chỉ IP trong khoảng IP đã được định nghĩa trong cơ sở dữ liệu của nó. DHCP server cấp phát địa chỉ IP tới DHCP client Nếu DHCP client chấp nhận địa chỉ IP này, DHCP server cho thuê địa chỉ IP này trong một khoảng thời gian cụ thể (tùy theo thiết đặt). Các thông tin về địa chỉ IP được gửi từ DHCP server tới DHCP client thường bao gồm các thành phần sau: địa chỉ IP, subnet mask, các giá trị lựa chọn khác (default gateway, địa chỉ DNS server).

III.5. Sử dụng Radius server để xác thực kết nối cho truy cập từ xa.

1. Hoạt động của Radius server

RADIUS là một giao thức làm việc theo mô hình client/server. RADIUS cung cấp dịch vụ xác thực và tính cước cho mạng truy nhập gián tiếp. Radius

client là một máy chủ truy cập tiếp nhận các yêu cầu xác thực từ người dùng từ xa và chuyển các yêu cầu này tới Radius server. Radius server nhận các yêu cầu kết nối của người dùng xác thực và sau đó trả về các thông tin cấu hình cần thiết cho Radius client để chuyển dịch vụ tới người sử dụng (hình 5.10).



Hình 5.10

Quá trình hoạt động được mô tả như sau:

1. Người sử dụng từ xa khởi tạo quá trình xác thực PPP tới máy chủ truy cập

2. Máy chủ truy cập yêu cầu người dùng cung cấp thông tin về username và password bằng các giao thức PAP hoặc CHAP.

3. Người dùng từ xa phúc đáp và gửi thông tin username và password tới máy chủ truy cập.

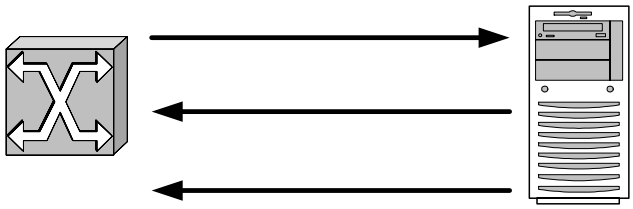
4. Máy chủ truy cập (Radius client) gửi chuyển tiếp các thông tin username và password đã được mã hóa tới Radius server

5. Radius server trả lời với các thông tin chấp nhận hay từ chối. Radius client thực hiện theo các dịch vụ và các thông số dịch vụ đi cùng với các phúc đáp chấp nhận hay từ chối từ Radius server

2. Nhận thực và cấp quyền

Khi Radius server nhận yêu cầu truy cập từ Radius client, Radius server tìm kiếm trong cơ sở dữ liệu các thông tin về yêu cầu này. Nếu username không có trong cơ sở dữ liệu này thì hoặc một profile mặc định được chuyển hoặc một thông báo từ chối truy cập được chuyển tới Radius client.

Trong RADIUS nhận thực và cấp quyền đi đôi với nhau, nếu username có trong cơ sở dữ liệu và password được xác nhận là đúng thì Radius server gửi trả về thông báo truy cập được chấp nhận, thông báo này bao gồm một danh sách các cặp đặc tính- giá trị mô tả các thông số được sử dụng cho phiên làm việc. Các thông số điển hình bao gồm: kiểu dịch vụ, kiểu giao thức, địa chỉ gán cho người dùng (động hoặc tĩnh), danh sách truy cập được áp dụng hay một định tuyến tĩnh được cài đặt trong bảng định tuyến của máy chủ truy cập. Thông tin cấu hình trong Radius server sẽ xác định những gì sẽ được cài đặt trên máy chủ truy cập. Hình vẽ dưới đây mô tả quá trình nhận thực và cấp quyền của Radius server (hình 5.11)



Hình 5.11

3.Tính cước

Các vấn đề về xử lý cước của RADIUS hoạt động độc lập với nhận thực và cấp quyền. Chức năng tính cước cho phép ghi lại dữ liệu được gửi tại thời điểm bắt đầu và kết thúc của một phiên làm việc và đưa ra các con số về mặt sử dụng tài nguyên như (thời gian, số gói, số byte...) được sử dụng trong phiên làm việc đó.

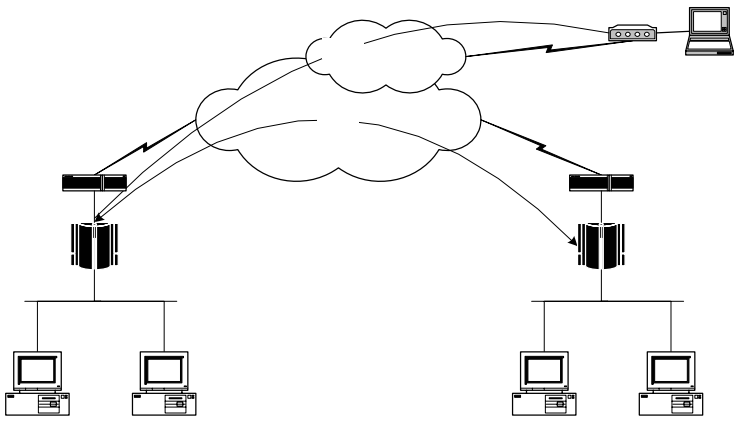
III.6. Mạng riêng ảo và kết nối sử dụng dịch vụ truy cập từ xa.

VPN (Virtual Private Network) là một mạng riêng được xây dựng trên nền tảng hạ tầng mạng công cộng (ví dụ mạng Internet), sử dụng mạng công cộng cho việc truyền thông riêng tư.

Giải pháp VPN cho phép người dùng làm việc tại nhà hoặc đang đi công tác ở xa có thể thực hiện một kết nối tới trụ sở chính bằng việc sử dụng hạ tầng

mạng là một mạng công cộng như là Internet, Như vậy thay vì phải thực hiện một kết nối đường dài tới trụ sở chính người sử dụng chỉ cần tạo lập một kết nối nội hạt tới một ISP khi đó bằng công nghệ VPN một kết nối VPN sẽ được thiết lập giữa người dùng với mạng trung tâm. Kết nối VPN cũng cho phép các tổ chức kết nối liên mạng giữa các địa điểm ở xa khác nhau thông qua các kết nối trực tiếp (leased line) từ các địa điểm đó tới một ISP. Như vậy kết nối VPN cho phép một tổ chức giảm chi phí gọi đường dài qua Dialup hay chi phí thuê đường leadline cho khoảng cách xa thay vì như vậy chỉ cần các kết nối nội hạt và điều này là tiết kiệm được chi phí. VPN gửi dữ liệu giữa các đầu cuối, dữ liệu được đóng gói, với các Header cung cấp thông tin định tuyến cho phép chuyển dữ liệu qua một liên kết hoặc một liên mạng công cộng tới đích. Dữ liệu chuyển đi được mã hoá để đảm bảo an toàn, các gói dữ liệu truyền thông trên mạng là không thể đọc mà không có khoá giải mã. Liên kết mà trong đó dữ liệu được đóng gói và mã hoá là một kết nối VPN.

Các hình thức kết nối: Có hai kiểu kết nối VPN, kết nối VPN truy cập từ xa và kết nối Site-to-site. Một kết nối VPN truy cập từ xa được thiết lập bởi một máy tính PC tới một mạng dùng riêng. VPN gateway cung cấp truy cập tới các tài nguyên của mạng dùng riêng. Các gói dữ liệu gửi qua kết nối VPN được khởi tạo từ các client. VPN client thực hiện việc xác thực tới VPN gateway. Kết nối site-to-site, được thiết lập bởi các VPN gateway và kết nối hai phần của một mạng dùng riêng. (hình 5.12).



Hình 5.12

Tunnel: là một phần quan trọng trong việc xây dựng một mạng VPN. Các chuẩn truyền thông sử dụng để quản lý các tulnnel và đóng gói dữ liệu của VPN bao gồm các giao thức làm việc ở lớp 2 như PPTP (Point-to-Point Tunlling Protocol) được phát triển bởi Microsoft hỗ trợ trong môi trường mạng Windows, L2TP (Layer 2 Tunnelling Protocol) được phát triển bởi Cisco. IPsec là một giao thức làm việc ở lớp 3, IPsec được phát triển bởi IETF và ngày càng được sử dụng rộng rãi.

L2TP và PPTP có mục đích là cung cấp các đường hầm dữ liệu thông qua mạng truyền dữ liệu công cộng. L2TP khác với PPTP ở chỗ nó tạo lập đường hầm nhưng không mã hoá dữ liệu. L2TP cung cấp các đường hầm bảo mật khi cùng hoạt động với các công nghệ mã hoá khác như IPSec. IPSec không yêu cầu phải có L2TP nhưng các chức năng mã hoá của nó đưa đến cho L2TP khả năng cung cấp các kênh thông tin bảo mật, cung cấp các giải pháp VPN. L2TP và PPTP cùng sử dụng PPP để đóng gói, thêm bớt thông tin tiếp đầu và truyền tải dữ liệu qua mạng.

Các kết nối VPN có các đặc trưng sau: đóng gói (Encapsulation), xác thực (Authentication) và mã hoá dữ liệu (Data encryption)

Đóng gói dữ liệu: Công nghệ VPN sử dụng một phương thức đóng gói dữ liệu trong đó cho phép dữ liệu truyền được qua mạng công cộng qua các giao thức tạo đường hầm.

Xác thực: Khi một kết nối VPN được thiết lập,VPN gateway sẽ xác thực VPN client đang yêu cầu kết nối và nếu được được phép kết nối được thực hiện. Nếu sự xác thực kết nối là qua lại được sử dụng, thì VPN client sẽ thực hiện việc xác thực lại VPN gateway, để đảm bảo rằng đấy chính là server mà mình cần gọi. Xác thực dữ liệu và tính toàn vẹn của dữ liệu: để xác nhận rằng dữ liệu đang được gửi từ một đầu của kết nối khác mà không bị thay đổi trong quá trình truyền, dữ liệu phải bao gồm một trường kiểm tra bằng mật mã dự trên một khoá mã hoá đã biết chỉ giữa người gửi và người nhận

Mã hóa dữ liệu: để đảm bảo dữ liệu truyền trên mạng, dữ liệu phải được mã hoá tại đầu gửi và giải mã tại đầu nhận. Việc mã hoá và giải mã dữ liệu phụ thuộc và người gửi và người nhận đang sử dụng phương thức mã hoá và giải mã nào.

III.7. Sử dụng Network and Dial-up Connection.

Network and Dial-up Connection (NDC) là một công cụ được Microsoft phát triển để hỗ trợ việc tạo lập các kết nối trong đó bao gồm các kết nối cho truy cập từ xa. Với việc sử dụng NDC ta có thể truy cập tới các tài nguyên dù đang ở trong mạng hay ở một địa điểm ở xa. Các kết nối được khởi tạo, thiết lập cấu hình, lưu giữ và quản lý bởi NDC. Mỗi một kết nối bao gồm một bộ các đặc tính được sử dụng để thiết lập liên kết giữa một máy tính tới máy tính hoặc mạng khác. Các kết nối gọi ra được liên lạc với một máy chủ truy cập ở xa bằng các hình thức truy cập gián tiếp thương là qua các mạng truyền dẫn mạng thoại công cộng, mạng ISDN. NDC cũng hỗ trợ việc thiết lập các kết nối gọi vào có nghĩa là đóng vai trò như một máy chủ truy cập.

Bởi vì tất cả các dịch vụ và các phương thức truyền thông đều được thiết lập trong kết nối nên không cần phải sử dụng các công cụ khác để cấu hình cho kết nối. Ví dụ để thiết lập cho một kết nối dial-up bao gồm các đặc tính được sử dụng trước, trong và sau khi kết nối. Các thông số này bao gồm: modem sẽ quay số, kiểu mã hóa password được sử dụng và các giao thức mạng sẽ sử dụng sau kết nối. Trạng thái kết nối bao gồm thời gian và tốc độ cũng được chính kết nối hiển thị mà không cần bất cứ một công cụ nào khác.

III.8. Một số vấn đề xử lý sự cố trong truy cập từ xa.

Các vấn đề liên quan đến sự cố trong truy cập từ xa, thường bao gồm:

Giám sát truy cập từ xa: giám sát máy chủ truy cập là phương pháp tốt nhất thường sử dụng để tìm ra nguồn gốc của các vấn đề xảy ra sự cố. Mỗi một chương trình phần mềm hay thiết bị phần cứng máy chủ truy cập bao giờ cũng có các công cụ sử dụng để giám sát và ghi lại các sự kiện xảy ra (trong các file log) đối với mỗi phiên truy cập từ xa.

Theo dõi các kết nối truy cập từ xa: khả năng theo dõi các kết nối truy cập từ xa của một Máy chủ truy cập cho ta xử lý các vấn đề phức tạp về sự cố mạng. Các thông tin theo dõi một kết nối từ xa thường rất phức tạp và khá chi tiết do đó để phân tích và xử lý cần thiết người quản trị mạng phải có kinh nghiệm và trình độ về hệ thống mạng.

Xử lý các sự cố về phần cứng: bao gồm các thiết bị truyền thông tại người dùng và tại máy chủ truy cập. Đối với các thiết bị tại người dùng (thường là các modem, cạc mạng...), hãy xem tài liệu về sản phẩm đó hay hỏi nhà cung cấp thiết bị về sản phẩm của họ về các cách kiểm tra và xác định lỗi của sản phẩm này. Nếu kết nối sử dụng modem, hãy kiểm tra rằng modem đã được cài đặt đúng chưa. Trong Windows 2000 các bước kiểm tra như sau:

- Trong Control Panel, kích Phone and Modem Options
- Trong trang modem, kích tên modem, sau đó kích Properties
- Kích Diagnostics, sau đó kích Query Modem.

Nếu modem đã được cài đặt đúng, bộ các thông số về modem sẽ được hiển thị, ngược lại hãy kiểm tra và cài đặt lại modem, trong trường hợp cuối cùng hãy hỏi nhà sản xuất thiết bị này. Để nhận thêm các thông tin về modem trong khi đang cố gắng tạo lập một kết nối, hãy xem thông tin trong log file để tìm ra nguyên nhân gạp sự cố. Để ghi các thông tin vào log file thực hiện theo các bước sau:

- Trong Control Panel, kích Phone and Modem Options
- Trong trang modem, kích tên modem, sau đó kích Properties
- Kích Diagnostics, sau đó kích lựa chọn Record a log, sau đó kích OK.

Đối với thiết bị truyền thông tại máy chủ truy cập: Kiểm tra các thiết bị phần cứng tương tự như trong trường hợp thiết bị tại người dùng, đồng thời kiểm tra log file về các sự kiện xẩy ra với hệ thống để tìm ra nguyên nhân sự cố. Một cách khác để kiểm tra modem tại máy chủ truy cập là sử dụng một đường điện thoại và gọi tới modem đó sau đó nghe xem modem đó có trả lời và cố gắng tạo một kết nối hay không. Nếu không có tín hiệu tạo kết nối từ modem đó thì có thể kết luận rằng đang có một vấn đề lỗi về modem tại máy chủ truy cập

Xử lý các sự cố về đường truyền thông: Thường là do cáp được đấu sai hay vì nguyên nhân từ nhà cung cấp dịch vụ điện thoại. Hãy kiểm tra đường điện thoại từ người dùng tới máy chủ truy cập bằng cách gọi điện thoại thông thường, thông qua chất lượng cuộc gọi ta cũng có thể phần nào dự đoán được chất lượng của đường truyền.

Xử lý các thiết đặt về cấu hình: Sau khi xác định rằng các vấn đề về phần cứng cũng như đường truyền thông đều tốt, bước tiếp theo ta kiểm tra các thiết đặt về cấu hình, bao gồm:

Các thiết đặt về mạng: lỗi cấu hình về mạng xảy ra khi đã tạo kết nối thành công nhưng vẫn không thể truy cập được các nguồn tài nguyên trên mạng, các lỗi thường xẩy ra như việc phân giải tên chưa hoạt động, các lỗi về định tuyến...khi lỗi về cấu hình mạng xảy ra, trước tiên ta kiểm tra rằng các máy kết nối trực tiếp (không thông qua dịch vụ truy cập từ xa) có thể truy cập được vào các nguồn tài nguyên trên mạng. Sau đó kiểm tra các cấu hình về TCP/IP bằng việc sử dụng lệnh ipconfig /all trên máy client. Kiểm tra rằng các thông số như DNS, địa chỉ IP, các thông số về định tuyến đã được thiết đặt đúng chưa. Sử dụng lệnh ping để kiểm tra kết nối mạng đã làm việc.

Các thiết đặt Máy chủ truy cập: Các thiết đặt trên máy chủ truy cập với các thông sô sai khi tạo lập kết nối có thể là nguyên nhân người dùng không thể truy cập vào các nguồn tài nguyên trên mạng. Để hỗ trợ cho việc xác định nguyên nhân gây lỗi, kiểm tra các sự kiện đã ghi log trên máy chủ truy cập và client, trong một số trường hợp cần thiết phải theo dõi (tracing) các kết nối trên máy chủ truy cập.

Các thiết đặt trên máy người dùng từ xa: kiểm tra các giao thức mạng làm việc trên client, các giao thức mạng làm việc trên client phải được hỗ trợ bởi máy chủ truy cập. Ví dụ, nếu người dùng từ xa thiết đặt trên client các giao thức NWLink, IPX/SPX và máy chủ truy cập chỉ hỗ trợ sử dụng TCP/IP, thì kết nối sẽ không thành công.

IV. Bài tập thực hành.

Yêu cầu về Phòng học lý thuyết: Số lượng máy tính theo số lượng học viên trong lớp học đảm bảo mỗi học viên có một máy tính, cấu hình máy tối thiểu như sau (PIII 800 MHZ, 256 MB RAM, HDD 1GB,FDD, CDROM 52 x). Máy tính đã cài đặt Windows 2000 advance server. Các máy tính đã được nối mạng chạy giao thức TCP/IP.

Thiết bị thực hành: Đĩa cài phần mềm Windows 2000 Advance Server. Mỗi máy tính có 01 Modem V.90 và 01 đường điện thoại. 01 account truy cập internet

Bài 1.

Thiết lập dialup networking để tạo ra kết nối Internet. truy cập Internet và giới thiệu các dịch vụ cơ bản

✓ Đăng nhập vào hệ thống với quyền Administrator.

✓ Kích Start, trỏ settings, sau đó kích Network and Dial-up Connections

✓ Trong Network and Dial-up Connections, kích đúp vào Make New Connection.

✓ Trong Network Connection Wizard, kích Next, có hai lựa chọn có thể sử dụng là Dial-up to private network hoặc Dial-up to the Internet.

✓ Nếu chọn Dial-up to private network, đưa vào số điện thoại truy cập của nhà cung cấp.

✓ Nếu chọn Dial-up to the Internet, lúc đó Internet Connection Wizard sẽ bắt đầu, làm theo các bước chỉ dẫn.

✓ Nếu muốn tất cả người dùng đều có thể sử dụng kết nối này thì lựa chọn, For all users, sau đó kích Next. Nếu muốn chỉ người dùng hiện tại sử dụng thì lựa chọn Only for myself, sau đó kích Next.

✓ Nếu đã lựa chọn Only for myself thì chuyển đến bước cuối cùng, Nếu lựa chọn For all users và muốn các máy tính khác trên mạng có thể chia sẻ kết nối này hãy lựa chọn Enable Internet Connection Sharing for this connection.

✓ Thiết đặt ngầm định là bất kỳ mày tính nào cũng có thể khởi tạo kết nối này một cách tự động, nếu muốn bỏ ngầm định này hãy xóa lựa chọn Enable on-demand dialing, sau đó kích next

✓ Đưa vào tên của kết nối và kích Finish.

Bài 2

Cài đặt và cấu hình dịch vụ truy cập từ xa cho phép người dùng từ xa truy cập vào mạng trên hệ điều hành Windows 2000 server.

Bước 1:

Cài đặt máy chủ dịch vụ truy cập từ xa

✓ Đăng nhập vào hệ thống với quyền Administrator

✓ Mở Routing and Remote Access từ menu Administrator Tools

✓ Kích chuột phải vào tên Server sau đó chọn Configure and Enable Routing and remote Access.

✓ Kịch bản Routing and Remote Access Server Setup xuất hiện, kích next

✓ Trong trang common Configuration, chọn Remote access server, sau đó kích next

✓ Trong trang Remote Client Protocol, xác định các giao thức sẽ hỗ trợ cho truy cập từ xa, sau đó kích next

✓ Trong trang Network Selection, lựa chọn kết nối mạng sẽ gán cho các máy truy cập từ xa, sau đó kích next

✓ Trong trang IP Address Asignment, lựa chọn Automaticlly hoặc From specified range of addresses cho việc gán các đị chỉ IP tới các máy truy cập từ xa

✓ Trong trang Managing Multiple Remote Acccess Servers cho phép lựa chọn cấu hình RADIUS, kích next

✓ Kích Finish để kết thúc.

Bước 2:

Thiết đặt tài khoản cho người dùng từ xa. Thiết lập một tài khoản có tên RemoteUser

✓ Đăng nhập với quyền Administrator

✓ Mở Active Directory Users and Computers từ menu Administrator Tools

✓ Kích chuột phải vào Users, chọn new và kích vào User

✓ Trong hộp thoại New Object-User, điền RemoteUser vào First name

✓ Trong hộp User logon name, gõ RemoteUser

✓ Thiết đặt Password cho tài khoản này, kích next sau đó kích Finish.

✓ Kích chuột phải vào RemoteUser sau đó kích Properties

✓ Trong trang Dial-In tab, kích Allow access, sau đó click OK

Thiết lập một Global group tên là RemoteGroup, sau đó thêm tài khoản người dùng vừa thiết lập vào nhóm này

✓ Kích chuột phải vào Users, chọn new sau đó kích Group

✓ Trong hộp thoại New Object-Group, mục Group name gõ vào RemoteGroup

✓ Trong mục Group scope kiểm tra Global đã được lựa chọn, trong mục Group type kiểm tra rằng Security đã được lựa chọn, sau đó kích OK

✓ Mở hộp thoại Properties của RemoteGroup

✓ Trong trang Member, kích Add

✓ Trong hộp thoại Select Users, Contacts, Computers, hoặc Group, Look in box, kiểm tra domain đã được hiển thị

✓ Trong danh sách các đối tượng, kích RemoteUser, kích Add sau đó kích OK

✓ Kích OK để đóng hộp thoại RemoteGroup Properties

Bước 3:

Kiểm tra cấu hình đã thiết lập ở bước trên bằng việc thực hiện một kết nối quay số tới máy chủ truy cập từ xa với tài khoản có tên là RemoteUser, kết nối được thiết lập sau đó đóng kết nối lại.

Bước 4:

Cấu hình cho phép tài khoản RemoteUser truy cập vào mạng được điều khiển truy cập bởi các chính sách truy cập từ xa (Remote access policy)

✓ Mở lại Active Directory Users and Computers từ menu Administrator Tools

✓ Mở hộp thoại Properties của tài khoản RemoteUser

✓ Trong trang Dial-in tab, kích Control access though Remote Policy sau đó kích OK, lư u ý rằng điều khiển vùng (Domain Controler) phải chạy ở chế độ Native.

✓ Thu nhỏ cửa sổ Active Directory Users and Computers

Bước 5:

Kiểm tra cấu hình đã thiết lập ở bước trên bằng việc thực hiện một kết nối quay số tới máy chủ truy cập từ xa với tài khoản có tên là RemoteUser. Thông báo lỗi xuất hiện, kết nối không được thiết lập.

Bước 6:

Sử dụng RRAS để thiết lập một chính sách mới đối với người dùng từ xa, tên chính sách này là Allow RemoteGroup Access cho phép người dùng trong nhóm RemoteGroup truy cập.

✓ Mở Routing and Remote Access từ menu Administrator Tools

✓ Mở rộng tên máy chủ đang cấu hình, kích chuột phải vào Remote Access Policy sau đó chọn New Remote Access Policy

✓ Trong trang Policy Name, gõ vào Allow RemoteGroup Access sau đó kích Next

✓ Trong trang Condition, kichs Add trong hộp thoại Select Attribute kích Windows-Groups sau đó kích Add

✓ Trong hộp thoại Groups kích Add

✓ Trong hộp thoại Select Groups, trong danh sách Look in, kích vào tên domain

✓ Trong hộp thoại Select Groups,dưới Name kích RemoteGroups kích Add sau đó kích OK

✓ Trong hộp thoại Groups kích OK

✓ Trong trang Condition kích Next

✓ Trong trang Permissions kích Grant remote access permission sau đó kích Next

✓ Trong trang User Profile kích Finish

✓ Trong trang Routing and Remote Access kích Remote Access Policies sau đó kích chuột phải Allow RemoteGroup access sau đó kích Move Up

Bước 7:

Kiểm tra cấu hình đã thiết lập ở bước trên bằng việc thực hiện một kết nối quay số tới máy chủ truy cập từ xa với tài khoản có tên là RemoteUser, kết nối được thiết lập sau đó đóng kết nối lại.

Bước 8:

Cấu hình để default policy được thi hành trước:

✓ Mở trang Routing and Remote Access, kích chuột phải RemoteGroup sau đó kích Move Down.

✓ Đóng cửa sổ Routing and Remote Access

Bước 9:

Kiểm tra cấu hình đã thiết lập ở bước trên bằng việc thực hiện một kết nối quay số tới máy chủ truy cập từ xa với tài khoản có tên là RemoteUser. Thông báo lỗi xuất hiện, kết nối không được thiết lập.

Bước 10:

Cấu hình cho phép truy cập sử dụng Properties của RemoteUser

✓ Mở lại Active Directory Users and Computers từ menu Administrator Tools

✓ Mở Properties của RemoteUser

✓ Trong trang Dial-in, kích Allow access sau đó kích OK

✓ Đóng Active Directory Users and Computers.

Bước 11:

Kiểm tra cấu hình đã thiết lập ở bước trên bằng việc thực hiện một kết nối quay số tới máy chủ truy cập từ xa với tài khoản có tên là RemoteUser, kết nối được thiết lập sau đó đóng kết nối lại

Bài 3

Cấu hình VPN server và thiết lập VPN Client, kiểm tra kết nối từ VPN Client tới VPN server

Bước 1:

Cấu hình cho kết nối VPN gọi vào

✓ Đăng nhập vào hệ thống với quyền Administrator

✓ Mở Routing and Remote Access từ menu Administrator Tools

✓ Kích chuột phải vào tên Server (Server là tên máy chủ đang cấu hình)

✓ Kịch bản thiết lập Routing and Remote Access xuất hiện, kích next

✓ Trong trang Network Selection, mục Name kiểm tra tên đã lựa chọn sau đó Click next

✓ Trong trang IP Address Assigment, kích From a specified range of addresses

✓ Trong trang Address Range Assignment, kích New

✓ Điền địa chỉ IP vào ô Start IP address và điền vào số địa chỉ vào ô Number of Address

✓ Kích OK, sau đó kích next

✓ Trong trang Managing Multiple Remote Access Servers, lựa chọn No, I don't want to set up this server to use RADIUS now, kích next sau đó kích Finish

✓ Kích OK để đóng hộp thoại Routing and Remote Access.

Cấu hình cho phép tài khoản Administrator truy cập vào mạng

✓ Mở Active Directory Users and Computers từ menu Administrator Tools.

✓ Mở rộng tên domain kích Users, kích đúp chuột vào Administrator

✓ Trong mục Dial-in, chọn Allow acces sau đó kích OK.

✓ Đóng của sổ Active Directory Users and Computers

Bước 2:

Cấu hình cho kết nối VPN gọi ra. Để kiểm tra dịch vụ truy cập từ xa đã làm việc phục vụ cho những người dùng từ xa, ta thiết lập một nối kết tới VPN server.

✓ Kích chuột phải vào My Network Places, sau đó kích Properties

✓ Trong của sổ Network Dialup Connections, kích đúp chuột vào Make new connection

✓ Trong trang Network Connection Type, kích Connect to a private network through the Internet, sau đó kích next

✓ Trong trang Destination Address page, gõ vào địa chỉ IP của máy cài đặt VPN server, sau đó kích next

✓ Trong trang Connection Availability, kích Only for my self, kích next sau đó kích Finish

✓ Khởi tạo kết nối tới VPN server

✓ Trong hộp thoại Connect Virtual Private Connection, kiểm tra tài khoản đăng nhập là Administrator và Password sau đó kích connect

✓ Kích OK để đóng thông báo Connnection Complete

✓ Đống của sổ Network Dialup Connections.

Sử dụng tiện ích Ipconfig để xác nhận rằng bạn đã thiết lập được một kết nối VPN và nhận được địa IP cho kết nối này lưu ý rằng đại chỉ IP cho kết nối VPN này là dãy địa chỉ tĩnh mà VPN server cấp phát

Đóng kết nối

✓ Kích đúp vào biểu tượng Connection trong khay hệ thống

✓ Trong hộp thoại Vitual Private Connection Status, kích disconnect

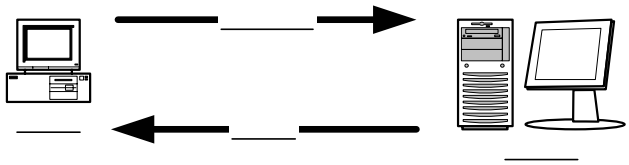
✓ Đóng tất cả các cửa sổ lại

Mục 2 : Dịch vụ Proxy - Giải pháp cho việc kết nối mạng dùng riêng ra Internet

I. Các khái niệm.

I.1. Mô hình client server và một số khả năng ứng dụng.

Mô hình chuẩn cho các ứng dụng trên mạng là mô hình client-server. Trong mô hình này máy tính đóng vai trò là một client là máy tính có nhu cầu cần phục vụ dịch vụ và máy tính đóng vai trò là một server là máy tính có thể đáp ứng được các yêu cầu về dịch vụ đó từ các client. Khái niệm client-server chỉ mang tính tương đối, điều này có nghĩa là một máy có thể lúc này đóng vai trò là client và lúc khác lại đóng vai trò là server. Nhìn chung, client là một máy tính cá nhân, còn các Server là các máy tính có cấu hình mạnh có chứa các cơ sở dữ liệu và các chương trình ứng dụng để phục vụ một dịch vụ nào đấy từ các yêu cầu của client (hình 6.1).



Hình 6.1

Cách thức hoạt động của mô hình client-server như sau: một tiến trình trên server khởi tạo luôn ở trạng thái chờ yêu cầu từ các tiến trình client tiến trình tại client được khởi tạo có thể trên cùng hệ thống hoặc trên các hệ thống khác được kết nối thông qua mạng, tiến trình client thường được khởi tạo bởi các lênh từ người dùng. Tiến trình client ra yêu cầu và gửi chúng qua mạng tới server để yêu cầu được phục vụ các dịch vụ. Tiến trình trên server thực hiện việc xác định yêu cầu hợp lệ từ client sau đó phục vụ và trả kết quả tới client và tiếp tục chờ đợi các yêu cầu khác. Một số kiểu dịch vụ mà server có thể cung

cấp như: dịch vụ về thời gian (trả yêu cầu thông tin về thời gian tới client), dịch vụ in ấn (phục vụ yêu cầu in tại client), dịch vụ file (gửi, nhận và các thao tác về file cho client), thi hành các lệnh từ client trên server...

Dịch vụ web là một dịch vụ cơ bản trên mạng Internet hoạt động theo mô hình client-server. Trình duyệt Web (Internet Explorer, Netscape...) trên các máy client sử dụng giao thức TCP/IP để đưa ra các yêu cầu HTTP tới máy server. Trình duyệt có thể đưa ra các yêu cầu một trang web cụ thể hay yêu cầu thông tin trong các cơ sở dữ liệu. Máy server sử dụng phần mềm của nó phân tích các yêu cầu từ các gói tin nhận được kiểm tra tính hợp lệ của client và thực hiện phục vụ các yêu cầu đó cụ thể là gửi trả lại client một trang web cụ thể hay các thông tin trên cơ sở dữ liệu dưới dạng một trang web. Server là nơi lưu trữ nội dung thông tin các website, phần mềm trên server cho phép server xác định được trang cần yêu cầu và gửi tới client. Cơ sở dữ liệu và các ứng dụng tương tự khác trên máy chủ được khai thác và kết nối qua các chương trình như CGI (Common Gateway Interface), khi các máy server nhận được yêu cầu về tra cứu trong cơ sở dữ liệu , nó chuyển yêu cầu tới server có chứa cơ sở dữ liệu hoặc ứng dụng để xử lý qua CGI.

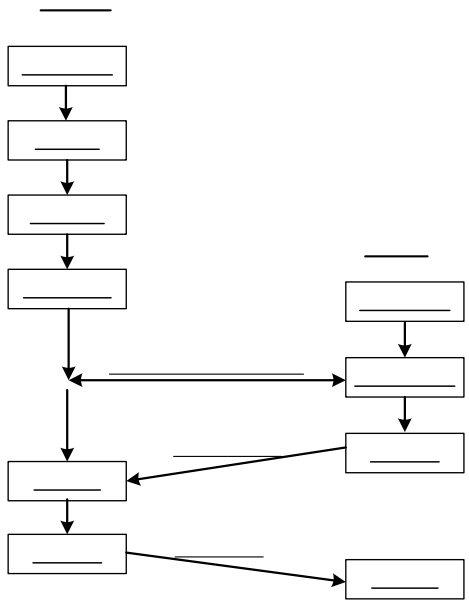
I.2. Socket.

Một kết nối được định nghĩa như là một liên kết truyền thông giữa các tiến trình, như vậy để xác định một kết nối cần phải xác định các thành phần sau: {Protocol, local-addr, local-process, remote-addr, remote-process}

Trong đó local-addr và remote-addr là địa chỉ của các máy địa phương và máy từ xa. local-process, remote-process để xác định vị trí tiến trình trên mỗi hệ thống. Chúng ta định nghĩa một nửa kết nối là {Protocol, local-addr, local-process} và {Protocol, remote-addr, remote-process} hay còn gọi là một socket.

Chúng ta đã biết để xác đinh một máy ta dựa vào địa chỉ IP của nó, nhưng trên một máy có vô số các tiến trình ứng dụng đang chạy, để xác định vị trí các tiến trình ứng dụng này người ta định danh cho mỗi tiến trình một số hiệu cổng, giao thức TCP sử dụng 16 bit cho việc định danh các cổng tiến trình và qui ước số hiệu cổng từ 1-1023 được sử dụng cho các tiến trình chuẩn (như FTP qui ước sử dụng cổng 21, dịch vụ WEB qui ước cổng 80, dịch vụ gửi thư

SMTP cổng 25...) số hiệu cổng từ 1024- 65535 dành cho các ứng dụng của người dùng. Như vậy một cổng kết hợp với một địa chỉ IP tạo thành một socket duy nhất trong liên mạng. Một kết nối TCP được cung cấp nhờ một liên kết logic giữa một cặp socket. Một socket có thể tham gia nhiều liên kết với các socket ở xa khác nhau. Trước khi truyền dữ liệu giữa hai trạm cần phải thiết lập một liên kết TCP giữa chúng và khi kết thúc phiên truyền dữ liệu thì liên kết đó sẽ được giải phóng.



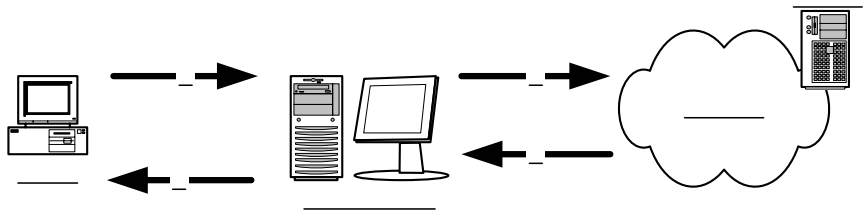
Hình 6.2

Quá trình thiết lập một socket với các lời gọi hệ thống được mô tả như sau: server thiết lập một socket với các thông số đặc tả các thủ tục truyền thông như (TCP, UDP, XNS...) và các kiểu truyền thông (SOCK_STREAM, SOCK_DGRAM...), sau đó liên kết tới socket này các thông số về địa chỉ như IP và các cổng TCP/UDP sau đó server ở chế độ chờ và chấp nhận kết nối đến từ client.

I.3. Phương thức hoạt động và đặc điểm của dịch vụ Proxy.

1. Phương thức hoạt động

Dịch vụ proxy được triển khai nhằm mục đích phục vụ các kết nối từ các máy tính trong mạng dùng riêng ra Internet. Khi đăng ký sử dụng dịch vụ internet tới nhà cung cấp dịch vụ, khách hàng sẽ được cấp hữu hạn số lượng địa chỉ IP từ nhà cung cấp, số lượng IP nhận được không đủ để cấp cho các máy tính trạm. Mặt khác với nhu cầu kết nối mạng dùng riêng ra Internet mà không muốn thay đổi lại cấu trúc mạng hiện tại đồng thời muốn gia tăng khả năng thi hành của mạng qua một kết nối Internet duy nhất và muốn kiểm soát tất cả các thông tin vào ra, muốn cấp quyền và ghi lại các thông tin truy cập của người sử dụng… Dịch vụ proxy đáp ứng được tất cả các yêu cầu trên. Hoạt động trên cơ sở mô hình client-server. Quá trình hoạt động của dịch vụ proxy theo các bước như sau:



Hình 6.3

1 Client yêu cầu một đối tượng trên mạng Internet

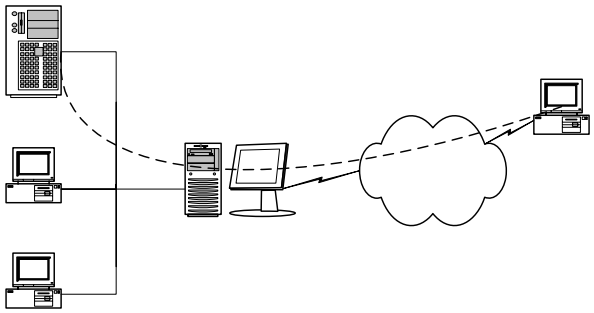
1 Proxy server tiếp nhận yêu cầu, kiểm tra tính hợp lệ cũng như thực hiện việc xác thực client nếu thỏa mãn proxy server gửi yêu cầu đối tượng này tới server trên Internet.

1 Server trên Internet gửi đối tượng yêu cầu về cho proxy server.

1 Proxy server gửi trả đối tượng về cho client

Ta có thể thiết lập proxy server để phục vụ cho nhiều dịch vụ như dịch vụ truyền file, dịch vụ web, dịch vụ thư điện tử…Mỗi một dịch vụ cần có một proxy server cụ thể để phục vụ các yêu cầu đặc thù của dịch vụ đó từ các client.

Proxy server còn có thể được cấu hình để cho phép quảng bá các server thuộc mạng trong ra ngoài Internet với mức độ an toàn cao. Ví dụ ta có thể thiết lập một web server thuộc mạng trong và thiết lập các qui tắc quảng bá web trên proxy server để cho phép quảng bá web server này ra ngoài Internet. Tất cả các yêu cầu truy cập web đến được chấp nhận bởi proxy server và proxy server sẽ thực hiện việc chuyển tiếp yêu cầu tới web server thuộc mạng trong (hình 6.4)



Hình 6.5

Các client được tổ chức trong một cấu trúc mạng gọi là mạng trong (Inside network) hay còn gọi là mạng dùng riêng. IANA (Internet Assigned Numbers Authority) đã dành riêng 3 khoảng địa chỉ IP tương ứng với 3 lớp mạng tiêu chuẩn cho các mạng dùng riêng đó là:

10.0.0.0 - 10.255.255.255 (lớp A)

172.16.0.0 - 172.31.255.255 (lớp B)

192.168.0.0 - 192.168.255.255 (lớp C)

Các địa chỉ này sử dụng cho các client trong mạng dùng riêng mà không được gán cho bất cứ máy chủ nào trên mạng Internet. Trong việc thiết kế và cấu hình mạng dùng riêng khuyến nghị nên sử dụng các khoảng địa chỉ IP này.

Khái niệm mạng ngoài (Outside network) là để chỉ vùng mà các server thuộc vào. Các địa chỉ sử dụng trên mạng này là các địa chỉ IP được đăng ký hợp lệ của nhà cung cấp dịch vụ Internet.

Proxy server sử dụng hai giao tiếp, giao tiếp mạng trong và giao tiếp ngoài. Giao tiếp trong điển hình là các cạc mạng sử dụng cho việc kết nối giữa proxy server với mạng dùng riêng và có địa chỉ được gán là địa chỉ thuộc mạng dùng riêng. Tất cả các thông tin giữa client thuộc mạng dùng riêng và proxy server được thực hiện thông qua giao tiếp này. Giao tiếp ngoài thường bằng các hình thức truy cập gián tiếp qua mạng điện thoại công cộng và qua cạc mạng bằng kết nối trực tiếp tới mạng ngoài. Giao tiếp ngoài được gán địa chỉ IP thuộc mạng ngoài được cung cấp hợp lệ bởi nhà cung cấp dịch vụ Internet.

2. Đặc điểm

Proxy Server kết nối mạng dùng riêng với mạng Internet toàn cầu và cũng cho phép các máy tính trên mạng internet có thể truy cập các tài nguyên trong mạng dùng riêng.

Proxy Server tăng cường khả năng kết nối ra Internet của các máy tính trong mạng dùng riêng bằng cách tập hợp các yêu cầu truy cập Internet từ các máy tính trong mạng và sau khi nhận được kết quả từ Internet sẽ trả lời lại cho máy có yêu cầu ban đầu.

Ngoài ra proxy server còn có khả năng bảo mật và kiểm soát truy cập Internet của các máy tính trong mạng dùng riêng. Cho phép thiết đặt các chính sách truy cập tới từng người dùng.

Proxy server lưu trữ tạm thời các kết quả đã được lấy từ Internet về nhằm trả lời cho các yêu cầu truy cập Internet với cùng địa chỉ. Việc lưu trữ này cho phép các yêu cầu truy cập Internet với cùng địa chỉ sẽ không cần phải lấy lại kết quả từ Internet, làm giảm thời gian truy cập Internet, tăng cường hoạt động của mạng và giảm tải trên đường kết nối Internet. Các công việc lưu trữ này gọi là quá trình cache.

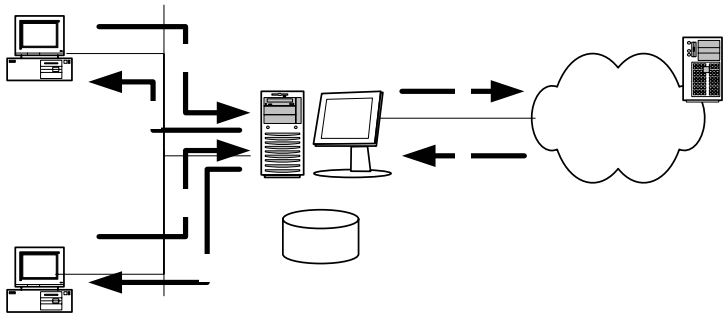
I.4. Cache và các phương thức cache.

Nhằm tăng cường khả năng truy cập Internet từ các máy tính trạm trong mạng sử dụng dịch vụ proxy ta sử dụng các phương thức cache. Dịch vụ proxy sử dụng cache để lưu trữ bản sao của các đối tượng đã được truy cập trước đó. Tất cả các đối tượng đều có thể được lưu trữ (như hình ảnh và các tệp tin), tuy nhiên một số đối tượng như yêu cầu xác thực (Authenticate) và sử dụng SSL (Secure Socket Layer) không được cache. Như vậy với các đối tượng đã được cache, khi một yêu cầu từ một máy tính trạm tới proxy server, proxy server thay vì kết nối tới địa chỉ mà máy tính trạm yêu cầu sẽ tìm kiếm trong cache các đối tượng thoã mãn và gửi trả kết quả về máy tính trạm. Như vậy cache cho phép cải thiện hiệu năng truy cập Internet của các máy trạm và làm giảm lưu lượng trên đường kết nối Internet. Vấn đề gặp phải khi sử dụng cache là khi các đối tượng được cache có sự thay đổi từ nguồn, các máy tính trạm yêu cầu một đối tượng tới proxy server, proxy server lấy đối tượng trong cache để phục vụ và như vậy thông tin chuyển tới các máy tính trạm là thông tin cũ so với nguồn, để giải quyết vấn đề này cần phải có các chính sách để cache các đối tượng đồng thời các đối tượng phải liên tục được cập nhật mới. Ví dụ: thông thường một địa chỉ WEB thì các đối tượng về hình ảnh ít có sự thay đổi còn nội dung text thường có sự thay đối do đó ta có thể thiết đặt chỉ cache những đối tượng hình ảnh, những đối tượng có nội dung text thì không cache, điều này không ảnh hưởng tới hiệu suất truy cập vì các tập tin về hình ảnh thường có kính thước rất lớn so với các đối tượng có nội dung text, việc cập nhật các đối tượng như thế nào phụ thuộc vào các phương thức cache mà ta sẽ trình bày dưới đây.

Proxy server thực thi cache cho các đối tượng được yêu cầu một cách có chu kỳ để tăng hiệu suất của mạng. Ta có thể thiết lập cache để đảm bảo rằng nó bao gồm những dữ liệu thường hay các client sử dụng nhất. Proxy server có thể sử dụng cho phép thông tin giữa mạng dùng riêng và Internet, việc thông tin có thể là client trong mạng truy cập Internet-trong trường hợp này proxy server thực hiện Forward caching, cũng có thể là client ngoài truy cập tói mạng trong (tới các server được quảng bá)-trong trường hợp này proxy server thực hiện reverse caching. Cả hai trường hợp đều có được từ khả năng của proxy server là lưu trữ thông tin (tạm thời) làm cho việc truyền thông thông tin được nhanh hơn, sau đây là các tính chất của cache proxy server:

- Phân cache: khi cài đặt một mảng các máy proxy server ta sẽ thiết lập được việc phân phối nội dung cache. Proxy server cho phép ghép nhiều hệ thống thành một cache logic duy nhất.
- Cache phân cấp: Khả năng phân phối cache còn có thể chuyên sâu hơn bằng cách cài đặt chế độ cache phân cấp liên kết một loạt các máy proxy server với nhau để client có thể truy cập tới gần chúng nhất.
- Cache định kỳ: sử dụng cache định kỳ nội dung download đối với các yêu cầu thường xuyên của các client
- Reverse cache: proxy server có thể cache các nội dung của các server quảng bá do đó tăng hiệu suất và khả năng truy cập, mọi đặc tính cache của proxy server đều có thể áp dụng cho nội dung trên các server quảng bá.

Proxy server có thể được triển khai như một Forward cache nhằm cung cấp tính năng cache cho các client mạng trong truy cập Internet. Proxy server duy trì bộ cache tập trung của các đối tượng Internet thường được yêu cầu có thể truy cập từ bất kỳ trình duyệt từ mày client. Các đối tượng phục vụ cho các yêu cầu từ các đĩa cache yêu cầu tác vụ xử lý nhỏ hơn đáng kế so với các đối tượng từ Internet, việc này tăng cường hiệu suất của trình duyệt trên client, giảm thời gian hồi đáp và giảm việc chiếm băng thông cho kết nối Internet. Hình vẽ sau mô tả proxy server xử lý các yêu cầu của người dùng ra sao (hình 6.6)



Hình 6.6

Hình trên mô tả quá trình các client trong mạng dùng riêng truy cập ra ngoài Internet nhưng tiến trình này cũng tương tự đối với các cache reverse (khi người dùng trên Internet truy cập vào các Server quảng bá) các bước bao gồm;

1 Client 1 yêu cầu một đối tượng trên mạng Internet

2 Proxy server kiểm tra xem đối tượng có trong cache hay không. Nếu đối tượng không có trong cache của proxy server thì proxy server gửi yêu cầu đối tượng tới server trên Internet.

3 Server trên Internet gửi đối tượng yêu cầu về cho proxy server .

4 proxy server gĩư bản copy của đối tượng trong cache của nó và trả đối tượng về cho client1

5 Client 2 gửi một yêu cầu về đối tượng tương tự

6 Proxy server gửicho client 2 đối tượng từ cache của nó chứ không phải từ Internet nữa.

Ta có thể triển khai dịch vụ proxy để quảng bá các server trong mạng dùng riêng ra ngoài Internet. Với các yêu cầu đến, proxy server có thể đòng vai trò như là một server bên ngoài, đáp ứng các yêu cầu của client từ các nội dung web trong cache của nó. Proxy server chuyển tiếp các yêu cầu cho server chỉ khi nào cache của nó không thể phục vụ yêu cầu đó (*Reverse cache).*

Lựa chọn các phương thức cache dựa trên các yếu tố: không gian ổ cứng sử dụng, đối tượng nào được cache và khi nào các đối tượng này sẽ được cập nhật. Về cơ bản ta có hai phương thức cache thụ động và chủ động.

Phương thức Cache thụ động (passive cache): Cache thụ động lưu trữ các đối tượng chỉ khi các máy tính trạm yêu cầu tới đối tượng. Khi một đối tượng được chuyển tới máy tính trạm, máy chủ Proxy xác định xem đối tượng này có thể cache hay không nếu có thể đối tượng sẽ được cache. Các đối tượng chỉ được cập nhật khi có nhu cầu. Đối tượng sẽ bị xoá khỏi cache dựa trên thời điểm gần nhất mà các máy tính trạm truy cập tới đối tượng. Phương thức này có lợi ích là sử dụng ít hơn bộ xử lý nhưng tốn nhiều không gian ổ đĩa hơn

Phương thức Cache chủ động (active cache): Cũng giống như phương thức cache thụ động, Cache chủ động lưu trữ các đối tượng khi các máy tính trạm ra yêu cầu tới một đối tượng máy chủ Proxy đáp ứng yêu cầu và lưu đối tượng này vào Cache. Phương thức này tự động cập nhật các đối tượng từ

Internet dựa vào: số lượng yêu cầu đối với các đối tượng, đối tượng thường xuyên thay đổi như thế nào. Phương thức này sẽ tự động cập nhật các đối tượng khi mà máy chủ Proxy đang phục vụ ở mức độ thấp và do đó không ảnh hưởng đến hiệu suất phục vụ các máy tính trạm. Đối tượng trong cache sẽ bị xoá dựa trên các thông tin header HTTP, URL.

II. Triển khai dịch vụ proxy

II.1. Các mô hình kết nối mạng

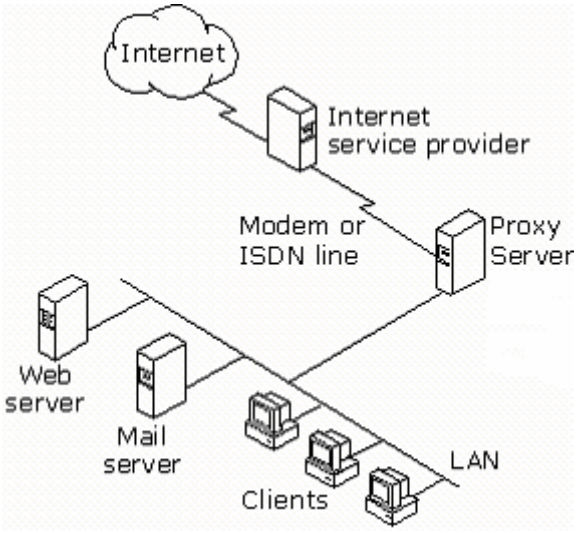
Đối tượng phục vụ của proxy server khá rộng, từ mạng văn phòng nhỏ, mạng văn phòng vừa tới mạng của các tập đoàn lớn. Với mỗi quy mô tổ chức sẽ có một cấu trúc mạng sử dụng proxy server cho phù hợp. Sau đây chúng ta sẽ xem xét một số mô hình cơ bản đối với mạng cỡ nhỏ, mạng cỡ trung bình và mạng tập đoàn lớn. Trong đó chúng ta sẽ đi sâu vào mô hình thứ nhất dành cho mạng văn phòng nhỏ bởi nó phù hợp quy mô tổ chức của các công ty vừa và nhỏ tại Việt nam.

Mô hình mạng văn phòng nhỏ

□□c tớnh c□a m□ng v□n phũng nh□ nh□ sau:

- Bao gồm một mạng LAN độc lập.
- Sử dụng giao thức IP.
- Kết nối Internet bằng đường thoại (qua mạng điện thoại công cộng bằng các hình thức quay dial-up hay sử dụng công nghệ ADSL) hoặc đường trực tiếp (Leased Line).
- ít hơn 250 máy tính trạm.

Mô hình kết nối mạng như hình vẽ (hình 6.7)



Hình 6.7

Theo mô hình này, với mỗi phương thức kết nối Internet Proxy server sử dụng 02 giao tiếp như sau:

- Kết nối Internet bằng đường thoại qua mạng PSTN:
- 01 giao tiếp với mạng nội bộ thông qua card mạng.
- 01 giao tiếp với Internet thông qua Modem.
- Kết nối Internet bằng đường trực tiếp (Leased Line)
- 01 giao tiếp với mạng nội bộ thông qua card mạng
- 01 giao tiếp với Internet thông qua card mạng khác. Lúc này bảng địa chỉ nội bộ (LAT-Local Address Table) được xây dựng dựa trên danh sách địa chỉ IP mạng nội bộ.

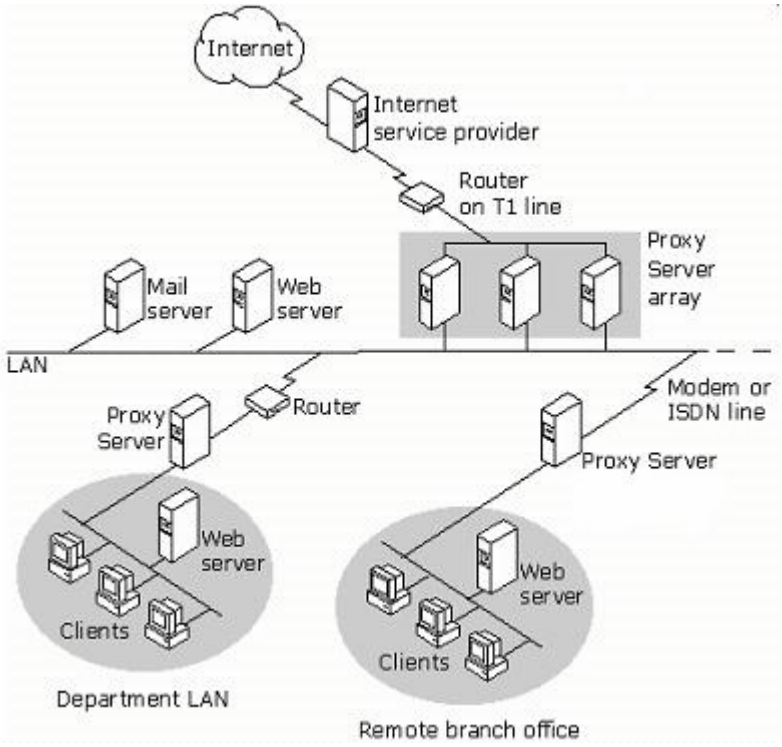
Mô hình kết nối mạng cỡ trung bình

Đặc trưng của mạng văn phòng cỡ trung bình như sau:

- Văn phòng trung tâm với một vài mạng LAN
- Mội văn phòng chi nhánh có một mạng LAN.
- Sử dụng giao thức IP.
- Kết nối bằng đường thoại từ văn phòng chi nhánh tới văn phòng trung tâm.
- Kết nối Internet từ văn phòng trung tâm tới ISP bằng đường thoại hoặc đường trực tiếp (Leased Line).

- ít hơn 2000 máy tính trạm

Mô hình mạng như hình 6.8. Theo mô hình này, văn phòng chi nhánh sử dụng một máy chủ Proxy cung cấp khả năng lưu trữ thông tin nội bộ (local caching), quản trị kết nối và kiểm soát truy cập tới văn phòng trung tâm. Tại văn phòng trung tâm, một số máy chủ Proxy hoạt động theo kiến trúc mảng (array) cung cấp khả năng bảo mật chung cho toàn mạng, cung cấp tính năng lưu trữ thông tin phân tán (distributed caching) và cung cấp kết nối ra Internet.



Hình 6.8

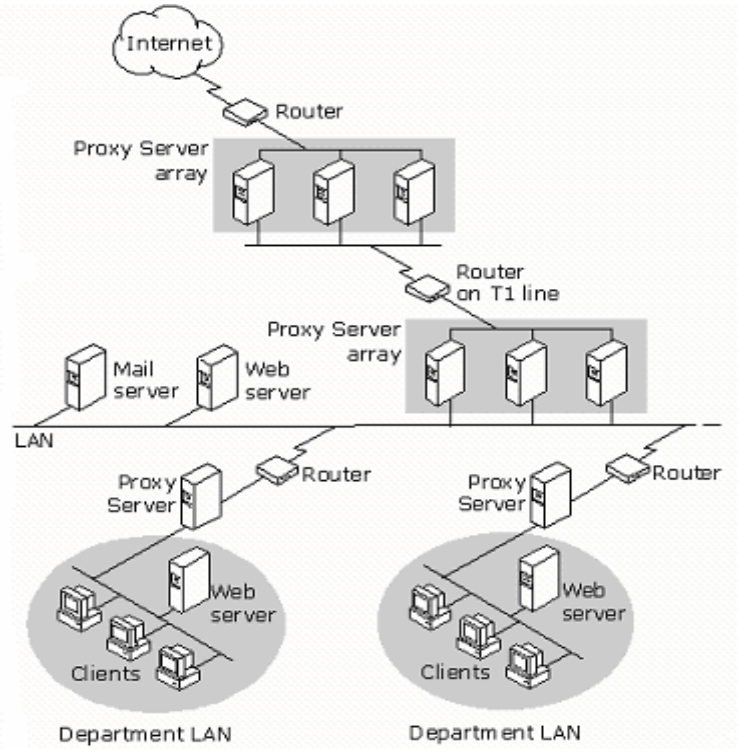
Mô hình kết nối mạng tập đoàn lớn

Mạng của các tập đoàn lớn có đặc trưng như sau:

- Văn phòng trung tâm có nhiều mạng LAN và có mạng trục LAN.
- Có vài văn phòng chi nhánh, mỗi văn phòng chi nhánh có một mạng LAN.
- Sử dụng giao thức mạng IP.
- Kết nối bằng đường thoại từ các văn phòng chi nhánh tới văn phòng trung tâm.

- Kết nối Internet từ văn phòng trung tâm tới ISP bằng đường đường trực tiếp (Leased Line).
- Có nhiều hơn 2000 máy tính trạm.

Mô hình mạng như hình 6.9. Theo mô hình này mạng tại các văn phòng chi nhánh cũng cấu hình tương tự như đối với mô hình các văn phòng cỡ trung bình. Các yêu cầu kết nối Internet không được đáp ứng bởi cache nội bộ tại máy chủ Proxy của văn phòng chi nhánh sẽ được chuyển tới một loạt máy chủ Proxy hoạt động theo kiến trúc mảng tại văn phòng trung tâm. Tại văn phòng trung tâm các máy chủ Proxy sử dụng 02 giao tiếp mạng (card mạng) trong đó 01 card mạng giao tiếp với mạng trục LAN và 01 card mạng giao tiếp với mạng LAN thành viên.



Hình 6.9

II.2. Thiết lập chính sách truy cập và các qui tắc

1..Các qui tắc.

Ta có thể thiết lập proxy server để đáp ứng các yêu cầu bảo mật và vận hành bằng cách thiết lập các qui tắc để xác định xem liệu người dùng, máy tính hoặc ứng dụng có được quyền truy cập và truy cập như thế nào tới máy tính

trong mạng hay trên Internet hay không. Thông thường một proxy server định nghĩa các loại qui tắc sau: Qui tắc về chính sách truy nhập, qui tắc về băng thông, qui tắc về chính sách quảng bá, các đặc tính lọc gói và qui tắc về định tuyến và chuỗi (chaining).

Khi một client trong mạng yêu cầu một đối tượng proxy server sẽ xử lý các qui tắc để xác định xem yêu cầu đó có được xác định chấp nhận hay không. Tương tự khi một client bên ngoài (Internet) yêu cầu một đối tượng từ một server trong mạng, proxy server cũng xử lý các bộ qui tắc xem yêu cầu có được cho phép không.

*Các qui tắc của chính sách truy nhập:*Ta có thể sử dụng proxy server để thiết lập chính sách bao gồm các qui tắc về giao thức, qui tắc về nội dung. Các qui tắc giao thức định nghĩa giao thức nào có thể sử dụng cho thông tin giữa mạng trong và Internet. Qui tắc giao thức sẽ được xử lý ở mức ứng dụng. Ví dụ một qui tắc giao thức có thể cho phép các Client sử dụng giao thức HTTP. Các qui tắc về nội dung qui định những nội dung nào trên các site nào mà client có thể truy nhập. Các qui tắc nội dung cùng được xử lý ở mức ứng dụng. Ví dụ một qui tắc về nội dung có thể cho phép các client truy nhập tới bất kỳ địa chỉ nào trên Internet.

Qui tắc băng thông: Qui tắc băng thông xác định kết nối nào nhận được quyền ưu tiên.Trong việc điều khiển băng thông thường thì proxy server không giới hạn độ rộng băng thông. Hơn nữa nó cho biết chất lượng dịch vụ (QoS) được cấp phát ưu tiên cho các kết nối mạng như thế nào. Thường thì bất kỳ kết nối nào không có qui tắc về băng thông kèm theo sẽ nhận được quyền ưu tiên ngầm định và bất kỳ kết nối nào có qui tắc băng thông đi kèm sẽ được sắp xếp với quyền ưu tiên hơn quyền ưu tiên ngầm định.

Các qui tắc về chính sách quảng bá: Ta có thể sử dụng proxy server để thiết lập chính sách quảng bá, bao gồm các qui tắc quảng bá server và qui tắc quảng bá web. Các qui tắc quảng bá server và web lọc tất cả các yêu cầu đến từ các yêu cầu của client ngoài mạng (internet) tới các server trong mạng. Các qui tắc quảng bá server và web sẽ đưa các yêu cầu đến cho các server thích hợp phía sau proxy server.

Đặc tính lọc gói: Đặc tính lọc gói của proxy server cho phép điều khiển luồng các gói IP đến và đi từ proxy server. Khi lọc gói hoạt động thì mọi gói trên giao diện bên ngoài đều bị rớt lại, trừ khi chúng được hoàn toàn cho phép

hoặc là một cách cố định bằng các bộ lọc gói IP, hoặc là một cách động bằng các chính sách truy cập hay quảng bá. Thậm chí nếu bạn không để lọc gói hoạt động thì truyền thông giữa mạng Internet và mạng cục bộ được cho phép khi nào bạn thiết lập rõ ràng các qui tắc cho phép truy cập. Trong hầu hết các trường hợp, việc mở các cổng động thường được sử dụng hơn. Do đó, người ta thường khuyến nghị rằng bạn nên thiết lập các qui tắc truy cập cho phép client trong mạng truy nhập vào Internet hoặc các qui tắc quảng bá cho phép client bên ngoài truy nhập vào các server bên trong. Đó là do các bộ lọc gói IP mở một cách cố định những chính sách truy nhập và qui tắc quảng bá lại mở các cổng kiểu động. Giả sử bạn muốn cấp quyền cho mọi người dùng trong mạng truy cập tới các site HTTP. Bạn không nên thiết lập một bộ lọc gói IP để mở cổng 80. Nên thiết lập qui tắc về site, nội dung và giao thức cần thiết để cho phép việc truy nhập này. Trong một vài trường hợp ta sẽ phải sử dụng các lọc gói IP, ví dụ nên thiết lập các lọc gói IP nếu ta muốn quảng bá các Server ra bên ngoài.

Qui tắc định tuyến và cấu hình chuỗi proxy (chaining): thường là qui tắc được áp dụng sau cùng để định tuyến các yêu cầu của client tới một server đã được chỉ định để phục vụ các yêu cầu đó.

2. Xử lý các yêu cầu đi

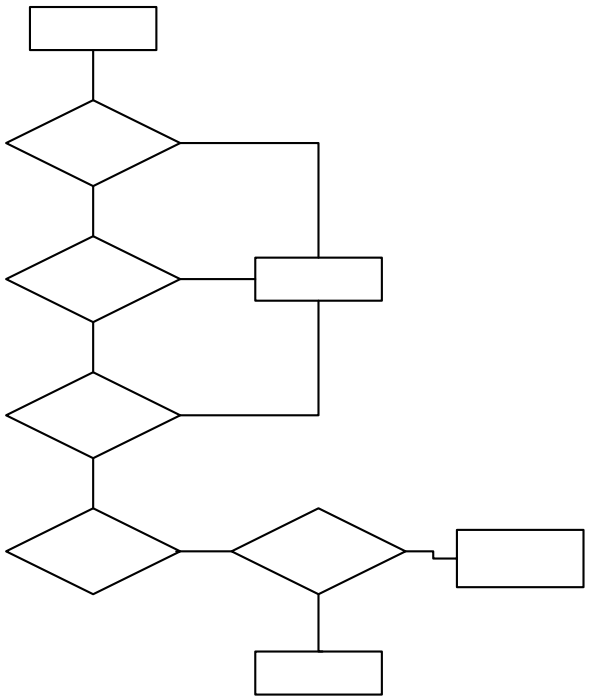
Một trong các chức năng chính của proxy server là khả năng kết nối mạng dùng riêng ra Internet trong khi bảo vệ mạng khỏi những nội dung có ác ý. Để thuận tiện cho việc kiểm soát kết nối này, ta dùng proxy server để tạo ra một chính sách truy cập cho phép các client truy cập tới các server trên Internet cụ thể, chính sách truy cập cùng với các qui tắc định tuyến quyết định các client truy cập Internet như thế nào.

Khi proxy server xử lý một yêu cầu đi, proxy server kiểm tra các qui tắc định tuyến các qui tắc về nội dung và các qui tắc giao thức để xem xét việc truy cập có được phép hay không. Yêu cầu chỉ được cho phép nếu cả quy tắc giao thức, qui tắc nội dung và site cho phép và nếu không một qui tắc nào từ chối yêu cầu.

Một vài qui tắc có thể được thiết lập để áp dụng cho các client cụ thể. Trong trường hợp này, các client có thể được chỉ định hoặc là bằng địa chỉ IP hoặc bằng user name. Proxy server xử lý các yêu cầu theo cách khác nhau phụ thuộc vào kiểu yêu cầu của client và việc thiết lập proxy server.Với một yêu

cầu, các qui tắc được xử lý theo thứ tự như sau: qui tắc giao thức, qui tắc nội dung, các lọc gói IP, qui tắc định tuyến hoặc cấu hình chuỗi proxy.

Hình dưới đưa ra quá trình xử lý đối với một yêu cầu đi (hình 6.10)



Hình 6.10

Trước tiên, proxy server kiểm tra các qui tắc giao thức, proxy server chấp nhận yêu cầu chỉ khi một qui tắc giao thức chấp nhận một cách cụ thể yêu cầu và không một qui tắc giao thức nào từ chối yêu cầu đó.

Sau đó, proxy server kiểm tra các qui tắc về nội dung. Proxy server chỉ chấp nhận yêu cầu nếu một qui tắc về nội dung chấp nhận yêu cầu và không có một qui tắc về nội dung nào từ chối nó.

Tiếp đến proxy server kiểm tra xem liệu có một bộ lọc gói IP nào được thiết lập để loại bỏ yêu cầu không để quyết định xem liệu yêu cầu có bị từ chối.

Cuối cùng, proxy server kiểm tra qui tắc định tuyến để quyết định xem yêu cầu được phục vụ như thế nào.

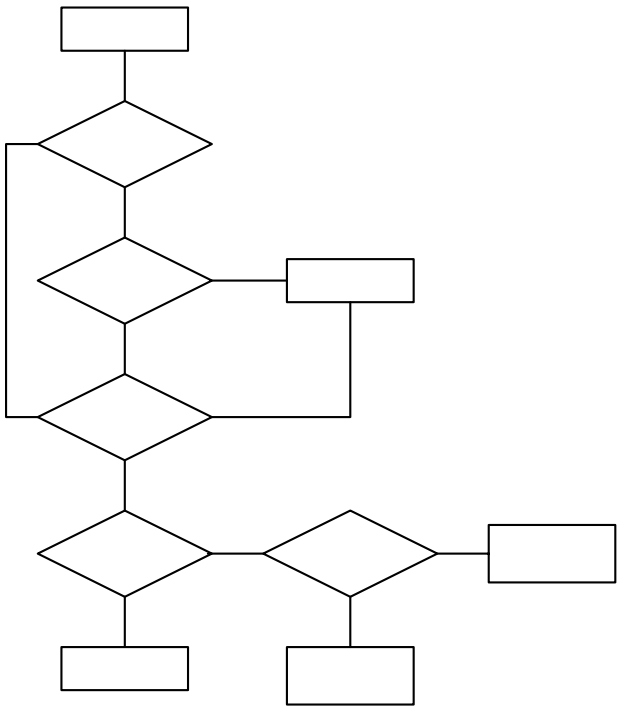
Giả sử cài đặt một proxy server trên một máy tính với hai giao tiếp kết nối, một kết nối với Internet và một kết nối vào mạng dùng riêng. Ta sẽ cho các

chỉ dẫn để cho phép tất cả client truy cập vào tất cả các site. Trong trường hợp này, chính sách truy nhập chỉ là các qui tắc như sau: một qui tắc về giao thức cho phép tất cả các client sử dụng mọi giao thức tại tất cả các thời điểm .Một qui tắc về nội dung cho phép tất cả mọi người truy cập tới mọi nội dung trên tất cả các site ở tất cả các thời điểm nào. Lưu ý rằng qui tắc này cho phép các client truy cập Internet nhưng không cho các client bên ngoài truy cập vào mạng của bạn.

3. Xử lý các yêu cầu đến

Proxy server có thể được thiết lập để các Server bên trong có thể truy cập an toàn đến từ các client ngoài. Ta có thể sử dụng proxy server để thiết lập một chính sách quảng bá an toàn cho các Server trong mạng. Chính sách quảng bá (bao gồm các bộ lọc gói IP, các qui tắc quảng bá Web, hoặc qui tắc quảng bá Server, cùng với các qui tắc định tuyến) sẽ quyết định các Server được quảng bá như thế nào.

Khi proxy server xử lý một yêu cầu xuất phát từ một client bên ngoài, nó sẽ kiểm tra các bộ lọc gói IP, các qui tắc quảng bá và các qui tắc định tuyến để quyết định xem liệu yêu cầu có được thực hiện hay không và Server trong nào sẽ thực hiện các yêu cầu đó.



Hình 6.11

Giả sử rằng đã cài đặt proxy server với hai giao tiếp kết nối, một kết nối tới Internet và một kết nối vào mạng dùng riêng. Nếu lọc gói hoạt động và sau đó, bộ lọc gói IP từ chối yêu cầu thì yêu cầu sẽ bị từ chối. Nếu các qui tắc quảng bá web từ chối yêu cầu thì yêu cầu cũng bị loại bỏ. Nếu một qui tắc định tuyến được thiết lập yêu cầu được định tuyến tới một Server upstream hoặc một site chủ kế phiên thì Server được xác định đó sẽ xử lý yêu cầu. Nếu một qui tắc định tuyến chỉ ra rằng các yêu cầu được định tuyến tới một Server cụ thể thì web Server trong sẽ trả về đối tượng.

II.3. Proxy client và các phương thức nhận thực

Chính sách truy nhập và các qui tắc quảng bá của Proxy server có thể được thiết lập để cho phép hoặc từ chối một nhóm máy tính hay một nhóm các người dùng truy nhập tới một server nào đó. Nếu qui tắc được áp dụng riêng với các người dùng, Proxy server sẽ kiểm tra các đặc tính yêu cầu để quyết định người dùng được nhận thực như thế nào.

Ta có thể thiết lập các thông số cho các yêu cầu thông tin đi và đến để người dùng phải được proxy server nhận thực trước khi xử lý các qui tắc. Việc này đảm bảo rằng các yêu cầu chỉ được phép nếu người dùng đưa ra các yêu cầu đã được xác thực. Bạn cũng có thể thiết lập các phương pháp nhận thực được sử dụng và có thể thiết lập các phương pháp nhận thực cho các yêu cầu đi và yêu cầu đến khác nhau. Về cơ bản một Proxy server thường hỗ trợ các phương pháp nhận thực sau đây: phương thức nhận thực cơ bản., nhận thực Digest, nhận thực tích hợp Microsoft windows, chứng thực client và chứng thực server.

Đảm bảo rằng các chương trình proxy client phải hỗ trợ một trong các phương pháp nhận thực mà proxy server đã đưa ra. Trình duyệt IE 5 trở lên hỗ trợ hầu hết các phương pháp nhận thực, một vài trình duyệt khác có thể chỉ hỗ trợ phương pháp nhận thực cơ bản. Đảm bảo rằng các trình duyệt client có thể hỗ trợ ít nhất một trong số các phương pháp nhận thực mà Proxy server hỗ trợ.

1. Phương pháp nhận thực cơ bản.

Phương pháp nhận thực này gửi và nhận các thông tin về người dùng là các ký tự text dễ dàng đọc được. Thông thường thì các thông tin về user name và password sẽ được mã hoá thì trong phương pháp này không có sự mã hoá nào được sử dụng. Tiến trình nhận thực được mô tả như sau, proxy client nhắc người dùng đưa vào username và password sau đó thông tin này được client gửi cho proxy server. Cuối cùng username và password được kiểm tra như là một tài khoản trên proxy server.

2. Phương pháp nhận thực Digest.

Phương pháp này có tính chất tương tự như phương pháp nhận thực cơ bản nhưng khác ở việc chuyển các thông tin nhận thực. Các thông tin nhận thực qua một tiến trình xử lý một chiều thường được biết với cái tên là "hashing". Kết quả của tiến trình này gọi là hash hay message digest và không thể giải mã chúng. Thông tin gốc không thể phục hồi từ hash. Các thông tin được bổ sung vào password trước khi hash nên không ai có thể bắt được password và sử dụng chúng để giả danh người dùng thực. Các giá trị được thêm vào để giúp nhận dạng người dùng. Một tem thời gian cũng được thêm vào để ngăn cản người dùng sử dụng một password sau khi nó đã bị huỷ. Đây là một ưu điểm rõ ràng so với phương pháp nhận thực cơ bản bởi vì người dùng bất hợp pháp không thể chặn bắt được password.

3. Phương pháp nhận thực tích hợp.

Phương pháp này được sử dụng tích hợp trong các sản phẩm của Microsoft. Đây cũng là phương pháp chuẩn của việc nhận thực bởi vì username và password không được gửi qua mạng. Phương pháp này sử dụng hoặc giao thức nhận thực V5 Kerberos hoặc giao thức nhận thực challenge/response của nó.

4. Chứng thực client và chứng thực server

Ta có thể sử dụng các đặc tính của SSL để nhận thực. Chứng thực được sử dụng theo hai cách khi một client yêu cầu một đối tượng từ server: server nhận thực chính nó bằng cách gửi đi một chứng thực server cho client. Server yêu cầu client nhận thực chính nó (Trong trường hợp này client phải đưa ra một chứng thực client phù hợp tới server).

SSL nhận thực bằng cách kiểm tra nội dung của một chứng thực số được mã hoá do proxy client đệ trình lên trong quá trình đăng nhập (Các người dùng

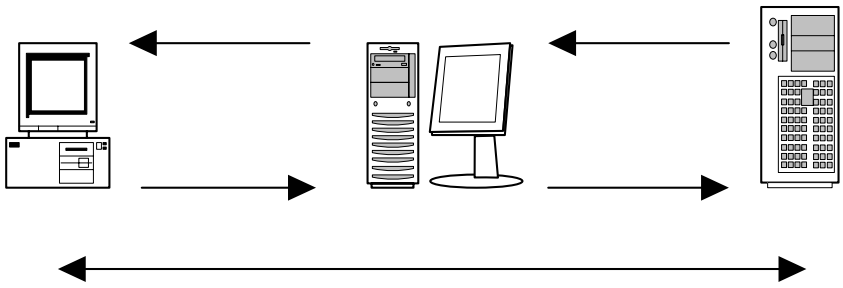
có thể có được các chứng thực số từ một tổ chức ngoài có độ tin tưởng cao). Các chứng thực về server bao gồm các thông tin nhận biết về server. Các chứng thực về client thường gồm các thông tin nhận biết về người dùng và tổ chức đưa ra chứng thực đó

Chứng thực client: Nếu chứng thực client được lựa chọn là phương thức xác thực thì proxy server yêu cầu client gửi chứng thực đến *trước* khi yêu cầu một đối tượng. Proxy server nhận yêu cầu và gửi một chứng thực cho client. Client nhận chứng thực này và kiểm tra xem có thực là thuộc về proxy server . Client gửi yêu cầu của nó cho proxy server, tuy nhiên proxy server yêu cầu một chứng thực từ client mà đã được đưa ra trước đó. Proxy server kiểm tra xem chứng thực có thực sự thuộcc về client được phép truy cập không.

Chứng thực server: Khi một client yêu cầu một đối tượng SSL từ một server, client yêu cầu server phải nhận thực chính nó. Nếu proxy server kết thúc một kết nối SSL thì sau đó proxy server sẽ phải nhận thực chính nó cho client. Ta phải thiết lập và chỉ định các chứng thực về phía server để sử dụng khi nhận thực server cho client

5. Nhận thực pass-though

Nhận thực pass-though chỉ đến khả năng của proxy server chuyển thông tin nhận thực của client cho server đích. Proxy server hỗ trợ nhận thực cho cả các yêu cầu đi và đến. Hình vẽ sau mô tả trường hợp nhận thực pass-though.



Hình 6.12

Client gửi yêu cầu lấy một đối tượng trên một web server cho proxy server. Proxy server chuyển yêu cầu này cho web server, bắt đầu từ đây việc nhận thực qua các bước sau:

1 Webserver nhận được yêu cầu lấy đối tượng và đáp lại rằng client cần phải nhận thực. Web server cũng chỉ ra các kiểu nhận thực được hỗ trợ.

2 Proxy server chuyển yêu cầu nhận thực cho client

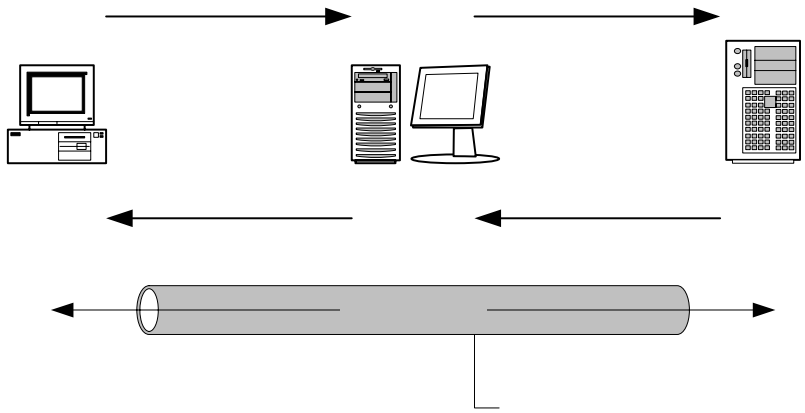
3 Client tiếp nhận yêu cầu và trả các thông tin nhận thực cho proxy server

4 Proxy server chuyển lại thông tin đó cho web server

5 Từ lúc này client liên lạc trực tiếp với web server

6. SSL Tunneling.

Với đường hầm SSL, một client có thể thiết lập một đường hầm qua proxy server trực tiếp tới server yeu cầu với các đối tượng yêu cầu là HTTPS. Bất cứ khi nào client yêu cầu một đối tượng HTTPS qua proxy server nó sử dụng đường hầm SSL. Đường hầm SSL làm việc bởi sự ngầm định các yêu cầu đi tới các cổng 443 và 563.



Hình 6.13

Tiến trình tạo đường hầm SSL được mô tả như sau:

1 Khi client yêu cầu một đối tượng HTTPS từ một web server trên Internet, proxy server gửi một yêu cầu kết nối https://*URL_name*

2 Yêu cầu tiếp theo được gửi tới cổng 8080 trên máy proxy server CONNECT *URL_name*:443 HTTP/1.1

3 Proxy server kết nối tới Web server trên cổng 443

4 Khi một kết nối TCP được thiết lập, proxy server trả lại kết nối đã được thiết lập HTTP/1.0 200

5 Từ đây, client thông tin trực tiếp với Web server bên ngoài

7. SSL bridging.

SSL bridging đề cập đến khả năng của proxy server trong việc mã hóa hoặc giải mã các yêu cầu của client và chuyển các yêu cầu này tới server đích. Ví dụ, trong trường hợp quảng bá (hoặc reverse proxy), proxy server có thể phục vụ một yêu cầu SSL của client bằng cách chấm dứt kết nối SSL với client và mở lại một kết nối mới với web server. SSL bridging được sử dụng khi proxy server kết thúc hoặc khởi tạo một kết nối SSL.

Khi một client yêu cầu một đối tượng HTTP. Proxy server mã hóa yêu cầu và chuyển tiếp nó cho web server. Web server trả về đối tượng đã mã hóa cho proxy server. Sau đó proxy server giải mã đối tượng và gửi lại cho client. Nói một cách khác các yêu cầu HTTP được chuyển tiếp như các yêu cầu SSL.

Khi client yêu cầu một đối tượng SSL. Proxy server giải mã yêu cầu, sau đó mã hóa lại một lần nữa và chuyển tiếp nó tới Web server. Web server trả về đối tượng mã hóa cho proxy server. Proxy server giải mã đối tượng và sau đó gửi nó cho client. Nói một cách khác các yêu cầu SSL được chuyển tiếp như là các yêu cầu SSL.

Khi client yêu cầu một đối tượng SSL. Proxy server giải mã yêu cầu và chuyển tiếp nó cho web server. Web server trả về đối tượng HTTP cho proxy server. Proxy server mã hóa đối tượng và chuyển nó cho client. Nói cách khác các yêu cầu SSL được chuyển tiếp như các yêu cầu HTTP.

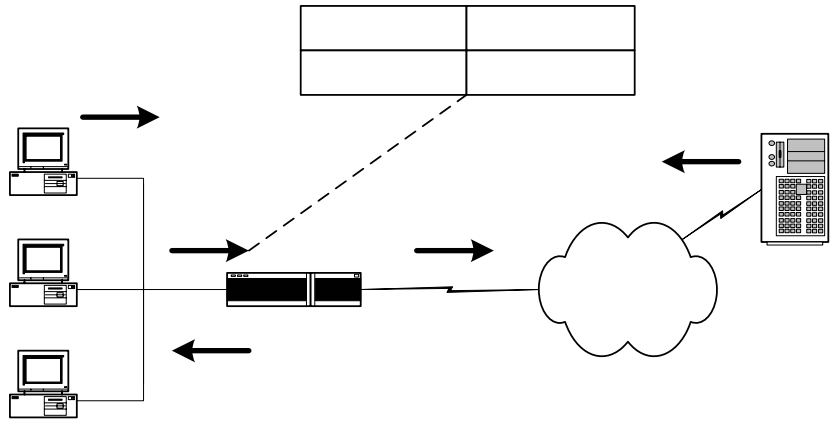
SSL bridging có thể được thiết lập cho các yêu cầu đi và đến. Tuy nhiên với các yêu cầu đi client phải hỗ trợ truyền thông bảo mật với proxy server.

II.4. NAT và proxy server

Khái niệm NAT (Network Addresss Tranlation).

NAT là một giao thức cho ta khả năng bản đồ hóa một một vùng địa chỉ IP sử dụng trong mạng dùng riêng ra mạng ngoài và ngược lại. NAT thường

được thiết lập trên các bộ định tuyến là ranh giới giữa mạng dùng riêng và mạng ngoài (ví dụ như mạng công cộng Internet). NAT chuyển đổi các địa chỉ IP trên mạng dùng riêng thành các địa chỉ IP được đăng ký hợp lệ trước khi chuyển các gói từ mạng dùng riêng tới Internet hoặc tới mạng ngoài khác. Trong phần này chúng ta sẽ chỉ tìm hiểu sự vận hành của NAT khi NAT được thiết lập để cung cấp các chức năng chuyển đổi các địa chỉ mạng dùng riêng trong việc phục vụ cho việc kết nối truy cập ra mạng ngoài như thế nào. Để làm việc này, NAT dùng tiến trình các bước theo hình vẽ dưới đây.



Hình 6.14

1. Người dùng tại máy 10.1.1.25 muốn mở một kết nối ra ngoài tới server 203.162.0.12

2. Khi gói dữ liệu đầu tiên tới NAT router, NAT router thực hiện việc kiểm tra trong bảng NAT. Nếu sự chuyển đổi địa chỉ đã có trong bảng, NAT router thực hiện bước thứ 3. Nếu không có sự chuyển đổi nào được tìm thấy, NAT router xác định rằng địa chỉ 10.1.1.25 phải được chuyển đổi. NAT router xác định một địa chỉ mới và cấu hình một chuyển đổi đối với địa chỉ 10.1.1.25 tới địa chỉ hợp lệ ngoài mạng (Internet) từ dãy địa chỉ động đã được định nghĩa từ trước ví dụ 203.162.94.163.

3. NAT router thay thế địa chỉ 10.1.1.25 bằng địa chỉ 203.162.94.163 sau đó gói được chuyển tiếp tới đích.

4. Server 203.162.0.12 trên Internet nhận gói và phúc đáp trở lại NAT router với địa chỉ 203.162.94.163.

5. Khi NAT router nhận được gói phúc đáp từ Server với địa chỉ đích đến là 203.162.94.163, nó thực hiện việc tìm kiếm trong bảng NAT. Bảng NAT chỉ ra rằng địa chỉ mạng trong 10.1.1.25 (tương ứng được ánh xạ tới địa chỉ 203.162.94.163 ở mạng ngoài) sẽ nhận được gói tin này. NAT router thực hiện việc chuyển đổi địa chỉ đích trong gói tin là 10.1.1.25 và chuyển gói tin này tới đích (10.1.1.25). Máy 10.1.1.25 nhận gói và tiếp tục thực hiện với các gói tiếp theo với các bước tuần tự như trên.

Trong trường hợp muốn sử dụng một địa chỉ mạng ngoài cho nhiều địa chỉ mạng trong. NAT router sẽ duy trì các thông tin thủ tục mức cao hơn trong bảng NAT đối với các số hiệu cổng TCP và UDP để chuyển đổi địa chỉ mạng ngoài trở lại chính xác tới các địa chỉ mạng trong.

Như vậy NAT cho phép các client trong mạng dùng riêng với việc sử dụng các địa chỉ IP dùng riêng truy cập vào một mạng bên ngoài như mạng Internet.Cung cấp kết nối ra ngoài Internet trong các mạng không được cung cấp đủ các địa chỉ Internet có đăng ký. Thích hợp cho việc chuyển đổi địa chỉ trong hai mạng Intranet ghép nối nhau. Chuyển đổi các địa chỉ IP nội tại được ISP cũ phân bố thành các địa chỉ được phân bố bởi ISP mới mà không cần thiết lập thủ công các giao diện mạng cục bộ.

NAT có thể được sử dụng một cách cố định hoặc động. Chuyển đổi cố định xảy ra khi ta thiết lập thủ công một bảng địa chỉ cùng các địa chỉ IP. Một địa chỉ cụ thể ở bên trong mạng sử dụng một địa chỉ IP (được thiết lập thủ công bởi người quản trị mạng) để truy cập ra mạng ngoài. Các thiết lập động cho phép người quản trị thiết lập một hoặc nhiều các nhóm địa chỉ IP dùng chung đã đăng ký. Những địa chỉ trong nhóm này có thể được sử dụng bởi các client trên mạng dùng riêng để truy cập ra mạng ngoài. Việc này cho phép nhiều client trong mạng sử dụng cùng một địa chỉ IP.

NAT cũng có một số nhược điểm như làm tăng độ trễ của các gói tin trên mạng. NAT phải xử lý mọi gói để quyết định xem liệu các header được thay đổi như thế nào. Không phải bất kỳ ứng dụng nào cũng có thể chạy được với NAT. NAT hỗ trợ nhiều giao thức truyền thông và cũng rất nhiều giao thức không được hỗ trợ. Các giao thức được NAT hỗ trợ như:TCP,UDP, HTTP,

TFTP, FTP…Các thông tin không được hỗ trợ như: IP multicast, BOOTP, DNS zone transfer, SNMP…

Proxy và NAT

Như đã phân tích cả dịch vụ NAT và dịch vụ Proxy đều có thể là một giải pháp để kết nối các mạng dùng riêng ra Internet, tuy nhiên mỗi dịch vụ lại có các ưu điểm và nhược điểm riêng.

Dịch vụ proxy cho khả năng thi hành và tốc độ cao hơn nhờ tính năng cache, tuy nhiên sử dụng cache có thể đưa ra các đối tượng đã quá hạn cần phải có các chính sách cache hợp lý đề đảm bảo tính thời sự của các đối tượng. Chính vì sử dụng cache nên giảm tải trên kết nối truy cập Internet. NAT không có tính năng cache.

Dịch vụ proxy phải được triển khai đối với từng ứng dụng, trong khi NAT là một tiến trình trong suốt hơn. Hầu hết các ứng dụng đều có thể làm việc được với NAT. NAT dễ cài đặt và vận hành, dường như không phải làm gì nhiều với NAT sau khi cài đặt.

Tại các client, đối với NAT không phải thiết đặt gì nhiều ngoài việc cấu hình tham số default gateway tới Server NAT. Trong khi sử dụng dịch vụ proxy, cần phải có các chương trình proxy client để làm việc với proxy server.

Dịch vụ proxy cho phép thiết đặt các chính sách tới người dùng, với NAT việc sử dụng các tính năng này có hạn chế rất nhiều, có thể nói sử dụng dịch vụ proxy là cách truy cập an toàn nhất để kết nối mạng dùng riêng ra ngoài Internet.

III. Các tính năng của phần mềm Microsoft ISA server 2000

III.1. Các phiên bản.

ISA server bao gồm hai phiên bản được thiết kế để phù hợp với từng nhu cầu của người sử dụng đó là ISA server Standard và ISA server Enterprise.

- ISA server Standard cung cấp khả năng an toàn firewall và khả năng web cache cho một môi trường kinh doanh, các nhóm làm việc hay văn phòng nhỏ. ISA server Standard cung cấp việc bảo mật chặt chẽ, truy cập web nhanh, quản lý trực quan, giá cả hợplý và khả năng thi hành cao.

- ISA server Enterprise được thiết kế đẻ đáp ứng các nhu cầu về hiệu suất, quản trị và cân bằng trong các môi trường Internet tốc độ cao với sự quản lý server tập trung, chính sách truy cập đa mức và các khả năng chống lỗi cao. ISA server Enterprisecung cấp sự bảo mật, truy cập Internet nhanh cho các môi trường có sự đòi hỏi khắt khe.

III.2. Lợi ích

ISA server là một trong các phần mềm máy chủ thuộc dòng .NET Enterprise Server. Các sản phẩm thuộc dòng .NET Enterprise Server là các server ứng dụng toàn diện của Microsoft trong việc xây dựng, triển khai, quản lý, tích hợp, các giải pháp dựa trên web và các dịch vụ. ISA server mang lại một số các lợi ích cho các tổ chức cần kết nối Internet nhanh, bảo mật, dễ quản lý.

1. Truy cập Web nhanh với cache hiệu suất cao.

- Người dùng có thể truy cập web nhanh hơn bằng các đối tượng tại chỗ trong cache so với việc phải kết nối vào Internet lúc nào cũng tiềm tàng nguy cơ tắc nghẽn.

- Giảm giá thành băng thông nhờ giảm lưu lượng từ Internet

- Phân tán nội dung của các Web server và các ứng dụng thương mại điện tử một cách hiệu quả, đáp ứng được nhu cầu khách hàng trên toàn cầu (khả năng phân phối nội dung web chỉ có trên phiên bản ISA server Enterprise)

2. Kết nối Internet an toàn nhờ Firewall nhiều lớp.

- Bảo vệ mạng trước các truy nhập bất hợp pháp bằng cách giám sát lưu lượng mạng tại nhiều lớp

- Bảo vệ các máy chủ web, email và các ứng dụng khác khỏi sự tấn công từ bên ngoài bằng việc sử dụng web và server quảng bá để xử lý một cách an toàn các yêu cầu đến

- Lọc lưu lượng mạng đi và đến để đảm bảo an toàn.

- Cung cấp truy cập an toan cho người dùng hợp lệ từ Internet tới mạng nội tại nhờ sử dụng mạng riêng ảo (VPN)

3. Quản lý thống nhất với sự quản trị tích hợp.

- Điều khiển truy cập tập trung để đảm bảo tính an toàn và phát huy hiệu lực của các chính sách vận hành.

- Tăng hiệu suất nhờ việc giới hạn truy cập sử dụng Internet đối với một số các ứng dụng và đích đến.

- Cấp phát băng thông để phù hợp với các ưu tiên.

- Cung cấp các công cụ giám sát và các báo cáo để chỉ ra kết nối Internet được sử dụng như thế nào.

- Tự động hóa các nhiệm vụ bằng việc sử dụng các script

4. Khả năng mở rộng.

- Chú trọng tới an toàn và thi hành nhờ sử dụng ISA server Softwware Development Kit (SDK) với sự phát triển các thành phần bổ sung.

- Chức năng quản lý và an toàn mở rộng cho các nhà sản xuất thứ ba

- Tự động các tác vụ quản trị với các đối tượng Script COM (Component Object Model)

III.3. Các chế độ cài đặt

ISA server có thể được cài đặt ở ba chế độ khác nhau: Cache, Firewall và Integrated

1. Chế độ cache: Trong chế độ này ta có thể nâng cao hiệu suất truy cập và tiết kiệm băng thông bằng cách lưu trữ các đối tượng web thường được truy xuất từ người dùng. Ta cũng có thể định tuyến các yêu cầu của người dùng tới cache server khác đang lưu giữ các đối tượng đó.

2. Chế độ firewall: Trong chế độ này cho phép ta đảm bảo an toàn lưu lượng mạng nhờ sự thiết lập các qui tắc điều khiển thông tin giữa mạng trong và Internet. Ta cũng có thể quảng bá các server trong để chia sẻ dữ liệu trên mạng với các đối tác và khách hàng.

3. Chế độ tích hợp: Trong chế độ này ta có thể tích hợp các dịch vụ cache và firewall trên một server.

III.4. Các tính năng của mỗi chế độ cài đặt

Các tính năng khác nhau tùy thuộc vào chế độ mà ta cài đặt, bảng sau liệt kê các tính năng có trong chế độ firewall và cache, chế độ tích hợp có tất cả các tính năng đó

Tính năng	Mô tả	Chế độ firewall	Chế độ cache
Chính sách truy cập	Định nghĩa các giao thức và nội dung Internet mà người dùng có thể sử dụng và truy cập	Có	Chỉ có HTTP và FTP
Cache	Lưu trữ định kỳ các đối tượng web vào RAM và đĩa cứng của ISA server	Không	Có
VPN	Mở rộng mạng riêng nhờ sử dụng các đường liên kết qua các mạng được chia sẻ hay mạng công cộng như Internet	Có	Không
Lọc gói	Điều khiển dòng gói IP đi và đến	Có	Không
Lọc ứng dụng	Thực thi các tác vụ của hệ thống hoặc của giao thức chỉ định, như là nhận thực để cung cấp một lớp bảo vệ bổ sung cho dịch vụ firewall	Có	Không
Quảng bá Web	Quảng bá web trong mạng để người dùng trong mạng có thể truy cập	Không	Có
Quảng bá Server	Cho phép các Server ứng dụng có	Có	Không

	thể phục vụ các client bên ngoài		
Giám sát thời gian thực	Cho phép giám sát tập trung các hoạt động của ISA server bao gồm các cảnh báo, giám sát các phiên làm việc và các dịch vụ	Có	Có
Cảnh báo	Báo cho ta biết các sự kiện đặc biệt xuất hiện và thực thi các hoạt động phù hợp	Có	Có
Báo cáo	Tổng hợp và phân tích hoạt động trên một hoặc nhiều máy ISA server	Có	Có

IV. Bài tập thực hành.

Yêu cầu về Phòng học lý thuyết: Số lượng máy tính theo số lượng học viên trong lớp học đảm bảo mỗi học viên có một máy tính, cấu hình máy tối thiểu như sau (PIII 800 MHZ, 256 MB RAM, HDD 1GB,FDD, CDROM 52 x). Máy tính đã cài đặt Windows 2000 advance server. Các máy tính đã được nối mạng chạy giao thức TCP/IP.

Thiết bị thực hành: Đĩa cài phần mềm Windows 2000 Advance Server, đĩa cài phần mềm ISA Server 2000. Mỗi máy tính có 01 Modem V.90 và 01 đường điện thoại. 01 account truy cập internet

Bài 1:

Các bước cài đặt cơ bản phần mềm ISA server 2000.

Bước 1:

Các bước cài đặt cơ bản.

- ✓ Đăng nhập vào hệ thống với quyền Administrator

✓ Đưa đĩa cài đặt Microsoft Internet Security and Acceleration Server 2000 Enterprise Edition vào ổ CD-ROM.

✓ Cửa sổ Microsoft ISA Server Setup mở ra. Nếu cửa sổ này không tự động xuất hiện, sử dụngWindows Explorer để chạy x:\ISAAutorun.exe (với x là tên ổ đĩa CD-ROM).

✓ Trong cửa sổ Microsoft ISA Server Setup, kích Install ISA Server.

✓ Trong hộp thoại Microsoft ISA Server (Enterprise Edition) Setup kích Continue.

✓ Vào CD Key sau đó kích OK hai lần.

✓ Trong hộp thoại Microsoft ISA Server Setup kích I Agree.

✓ Trong hộp thoại Microsoft ISA Server (Enterprise Edition) Setup kích Custom Installation.

✓ Trong hộp thoại Microsoft ISA Server (Enterprise Edition) – Custom Installation kích Add-in services sau đó kích Change Option.

✓ Trong hộp thoại Microsoft ISA Server (Enterprise Edition) – Add-in services kiểm tra lựa chọn Install H.323 Gatekeeper Service đã được chọn, chọn Message Screener sau đó kích OK.

✓ Trong hộp thoại Microsoft ISA Server (Enterprise Edition) – CustomInstallation kích Administration tools sau đó kích Change Option.

✓ Trong hộp thoại Microsoft ISA Server (Enterprise Edition) – Administration tools, kiểm tra lựa chọn ISA Management đã được chọn, chọn H.323 Gatekeeper Administration Tools sau đó kíchOK.

✓ Trong hộp thoại Microsoft ISA Server (Enterprise Edition) – Custom Installation kích Continue. Hộp thoại Microsoft Internet Security and Acceleration Server Setup xuất hiện, lưu ý bạn rằng máy tính không thể tham gia vào array. Bạn sẽ cấu hình máy tính này là một stand-alone server.

✓ Kích Yes để cấu hình máy tính này là một stand-alone server.

✓ Trong hộp thoại Microsoft ISA Server Setup đọc mô tả các mode cài đặt đảm bảo rằng mode Integrated đã được lựa chọn sau đó kích Continue.

✓ Trong hộp thoại Microsoft Internet Security and Acceleration Server Setup đọc thông báo về IIS publishing sau đó kích OK để biết rằng ISA Server Setup đang dừng dịch vụ IIS publishing.

✓ Kích OK và đặt ngầm định các giá trị thiết đặt cho cache.

Bước 2:

Cấu hình LAT để khai báo địa chỉ cho mạng riêng.

✓ Trong hộp thoại Microsoft Internet Security and Acceleration Server 2000 Setup kích Construct Table. Lưu ý rằng khi bạn thêm vào không đúng địa chỉ IP vào LAT, ISA server sẽ chuyển tiếp sai các gói tin do đó các máy client sẽ không thể truy cập Internet

✓ Trong hộp thoại Local Address Table, kích để xóa Add the following private ranges: 10.x.x.x, 192.168.x.x and 172.16.x.x-172.31.x.x

✓ Chọn adapter ip_address (với tên cạc mạng và địa chỉ IP là địa chỉ mạng riêng), sau đó kích OK.

✓ Trong thông báo Setup Message, kích OK.

✓ Trong Internal IP Ranges, kích 10.255.255.255-10.255.255.255, sau đó kích Remove.

✓ Kiểm tra rằng Internal IP Ranges chỉ chứa IP addresses trong mạng trong của bạn sau đó kích OK.

✓ Kết thúc việc cài đặt ISA Server và khởi tạo cấu hình ISA Server.

✓ Trong hộp thoại Launch ISA Management Tool, kích để xóa

✓ Start ISA Server Getting Started Wizard check box, sau đó kích OK.

✓ Trong hộp thông báo Microsoft ISA Server (Enterprise Edition) Setup kích OK.

✓ Đóng cửa sổ Microsoft ISA Server Setup.

✓ Lấy đĩa Microsoft Internet Security and Acceleration Server Enterprise Edition từ ổ đĩa CD-ROM.

Bước 3:

✓ Cấu hình Default Web Site trong Internet Information Services sử dụng cổng 8008, sau đó khởi động Default Web Site.

✓ Mở Internet Services Manager từ Administrative Tools.

✓ Trong Internet Information Services, mở rộng server(server là tên máy tính của bạn), sau đó kích DefaultWeb Site (Stopped).

✓ Kích chuột phải Default Web Site (Stopped), sau đó kích Properties. Vì ISA Server sử dụng các cổng 80 and 8080, bạn phải cấu hình IIS để phục vụ các kết nối từ các client tới trên cổng khác. Bạn sẽ cấu hình IIS để phục cụ các yêu cầu này trên cổng TCP 8008.

✓ Trong hộp thoại Default Web Site (Stopped) Properties, trong hộp TCP Port, gõ 8008 sau đó kích OK.

✓ Kích chuột phải Default Web Site (Stopped), sau đó kích Start.

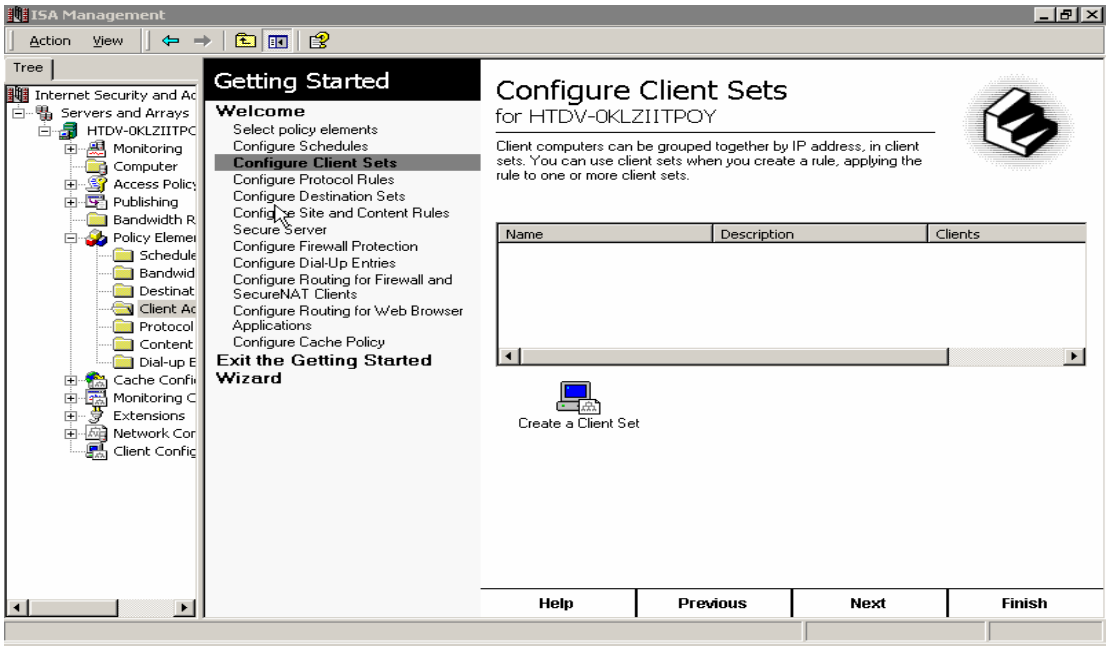
Bài 2:

Cấu hình ISA Server 2000 cho phép một mạng nội bộ có thể truy cập, sử dụng các dịch vụ cơ bản trên Internet qua 01 modem kết nối qua mạng PSTN.

Bước 1:

Cấu hình và quản trị cấu hình cho ISA server sử dụng Getting Started

Với Getting Started Wizard, có các lựa chọn cấu hình sau:



Hình 6.15

- ✓ Select Policy elements, cấu hình ngầm định chọn tất cả các thành phần để có thể sử dụng khi tạo các qui tắc.
- ✓ Configure Schedules, cấu hình ngầm định có hai lịch là Weekends và Work Hours, ta có thể sửa các lịch này hoặc tạo các lịch mới.
- ✓ Configure Client sets, các máy tính Client có thể tạo thành nhóm với nhau bằng các địa chỉ IP sử dụng cho mục đích tạo các qui tắc ứng với từng nhóm client
- ✓ Configure Protocol Rule, đưa ra các qui tắc giao thức để các client sử dụng truy nhập Internet
- ✓ Configure Destination Sets, cho phép thiết lập các máy tính trên mạng Internet thành nhóm bởi tên hay địa chỉ IP, Destination Sets được sử dụng để tạo ra các qui tắc, áp dụng các qui tắc cho một hay nhiều Destination Sets
- ✓ Configure Site and Content Rules, cấu hình các qui tắc về nội dung.
- ✓ Secure Server cho phép bạn có thể đặt các mức độ bảo vệ thích hợp cho mạng.
- ✓ Configure Filewall Protection, Packet Fitering bảo đảm cho ISA server sẽ lọc không có packet nào qua trừ khi được phép
- ✓ Cofigure Dial-Up Entries, cho phép chọn giao diện để kết nối với Internet
- ✓ Configure Routing for filewall and secureNat client.
- ✓ Configure Routing for Web browser Appilications cho phép tạo các qui tắc định tuyến, xác định rõ yêu cầu từ Web Proxy Client được gửi trực tiếp tới Internet hay tới Upstream server
- ✓ Configure Cache policy, cấu hình các chính sách về cache.

Bước 2:

Cấu hình ISA server cho phép các client sử dụng được các dịch vụ của Internet qua mạng thoại công cộng

- ✓ Tạo một Dial-Up Entries, để kết nối với InternetBước 2: Tạo một qui tắc giao thức.
- ✓ Mở ISA Management, kích Servers and arrays, sau đó kích tên máy chủ ISA.

- ✓ Kích Access Policy, kích chuột phải vào Protocol Rule, sau đó chọn New --> Rule.
- ✓ Đặt tên của Protocol Rule, sau đó kích Next.
- ✓ Kiểm tra rằng **Allow đã được chọn**, kích Next, sau đó chọn **All IP traffic**, kích Next Chọn **Always**, kích Next sau đó chọn **Any Request**, kích Next, sau đó kích Finish.

Bước 3:

Cấu hình Web Proxy Client: cấu hình Internet Explorer để sử dụng ISA server đối với các yêu cầu truy cập dịch vụ Web.

- ✓ Mở trình duyệt Internet Explorer.
- ✓ Trong Internet Connection Wizard, kích Cancel.
- ✓ Trong hộp thoại Internet Connection Wizard, chọn Do not show the Internet Connection wizard in the future, sau đó kích Yes.
- ✓ Trong Internet Explorer, trong ô Address , gõ http://vdc.com.vn sau đó chọn ENTER. Internet Explorer không thể kết nối tới trang web này.
- ✓ Trong menu Tools, kích Internet Options.
- ✓ Trong hộp thoại Internet Options, trong Connections kích LAN Settings.
- ✓ Trong hộp thoại Local Area Network (LAN) Settings , kích để bỏ lựa chọn Automatically detect settings. Chọn Use a proxy server, trong ô Address gõ vào địa chỉ IP của ISA Server .
- ✓ Trong hộp Port, gõ 8080
- ✓ Kiểm tra rằng lựa chọn Bypass proxy server for local addresses đã bỏ, sau đó kích OK hai lần.

Bài 3:

Thiết đặt các chính sách cho các yêu cầu truy cập và sử dụng các dịch vụ trên mạng internet.

I.Thiết lập các thành phần chính sách

Bước 1: Thiết lập lịch trình

- ✓ Đăng nhập vào hệ thống với quyền administrator
- ✓ Mở ISA Management từ thực đơn Microsoft ISA Server.
- ✓ Trong ISA Management, mở rộng Servers and Arrays, mở rộng server (server là tên của ISA Server), mở rộng Policy Elements, sau đó kích Schedules.
- ✓ Kích Create a Schedule để thiết lập một lịch trình.
- ✓ Trong hộp thoại New schedule trong mục Name đưa vào một tên lịch trình ví dụ schedule1.
- ✓ Trong mục Description gõ vào Daily period of most network utilization
- ✓ Kéo để lựa chọn toàn bộ lịch trình sau đó kích Inactive.
- ✓ Kéo để lựa chọn vùng từ thời điểm hiện tại tới 2 h tiếp theo đối với tất cả các ngày trong tuần sau đó kích active ví dụ, nếu thời điểm hiện tại là 3:15 P.M., thì lựa chọn vùng từ 3:00 P.M. tới 5:00 P.M. cho tất cả các ngày trong tuần.
- ✓ Kích OK.

Bước 2: Thiết lập destination set

- ✓ Trong ISA Management, kích Destination Sets.
- ✓ Kích Create a Destination Set.
- ✓ Trong hộp thoại New Destination Set trong mục Name cho vào một tên cho thiết lập mới này ví dụ set1.
- ✓ Trong mục Description box, gõ vào một nội dung mô tả cho thiết lập mới này
- ✓ Kích Add.
- ✓ Trong hộp thoại Add/Edit Destination trong mục Destination gõ home.vnn.vn

Bước 3: Thiết lập client address set

- ✓ Trong ISA Management kích Client Address Sets.
- ✓ Kích Create a Client Set.
- ✓ Trong hộp thoại Client Set trong mục Name gõ vào một tên cho thiết lập mới ví dụ Accounting Department.

- ✓ Trong mục Description gõ nội dung mô tả cho thiết lập mới này sau đó kích Add.
- ✓ Trong hộp thoại Add/Edit IP Addresses trong mục From gõ vào địa chỉ bắt đầu thuộc nhóm địa chỉ thuộc mạng dùng riêng .
- ✓ Trong mục To gõ vào địa chỉ kết thúc thuộc nhóm địa chỉ thuộc mạng dùng riêng kích OK hai lần.

Bước 4: Thiết lập protocol definition (sử dụng cổng UDP 39000 cho kết nối chính gọi ra và cổng TCP 39000 cho kết nối thứ hai)

- ✓ Trong ISA Management kích Protocol Definitions.
- ✓ Kích Create a Protocol Definition.
- ✓ Trong New Protocol Definition Wizard trong mục Protocol definition
- ✓ name gõ vào một tên cho thiết đặt mới sau đó kích Next.
- ✓ Trong trang Primary Connection Information trong mục Port number
- ✓ gõ vào 39000
- ✓ Trong danh sách Protocol type kích UDP.
- ✓ Trong danh sách Direction kích Send Receive sau đó kích Next.
- ✓ Trong trang Secondary Connections kích Yes sau đó kích New.
- ✓ Trong hộp thoại New/Edit Secondary Connection trong mục From và mục To gõ 39000
- ✓ Trong danh sách Protocol type kiểm tra rằng TCP đã được lựa chọn, trong mục Direction
- ✓ kích Outbound sau đó kích OK.
- ✓ Kích Next sau đó trong trang Completing the New Protocol Definition
- ✓ Wizard kích Finish.

II.Thiết lập các qui tắc giao thức

Bước 1:

Thiết lập một qui tắc giao thức cho phép HTTP, HTTP-S và FTP đối với mọi người dùng truy cập Internet tại mọi thời điểm bằng việc sử dụng các giao thức HTTP, HTTP-S và FTP .

- ✓ Mở trình duyệt Internet Explorer tại một máy trạm, trong ô Address gõ http://home.vnn.vn nhấn ENTER. Trình duyệt Internet Explorerkhông thể kết nối tới Web site vì ISA Server từ chối yêu cầu.
- ✓ Đóng Internet Explorer.
- ✓ Trong ISA Management mở rộng Access Policy sau đó kích Protocol Rules.
- ✓ Kích Create a Protocol Rule for Internet Access.
- ✓ Trong New Protocol Rule Wizard, trong mục Protocol rule name gõ Allow HTTP, HTTP-S, and FTP sau đó kích Next.
- ✓ Trong trang Protocols kiểm tra rằng Selected protocols đã được chọn, kích để xóa Gopher check box sau đó kích Next.
- ✓ Trong trang Schedule kiểm tra rằng Always đã được lựa chọn sau đó kích Next.
- ✓ Trong trang Client Type kiểm tra rằng Any request đã được chọn, sau đó kích Next.
- ✓ Trong trang Completing the New Protocol Rule Wizard kích Finish.
- ✓ Mở Internet Explorer tại một máy tính trạm, trong mục Address gõ http://home.vnn.vn sao đó ấn ENTER. Kiểm tra rằng trình duyệt kết nối thành công nội dung trang web được hiển thị
- ✓ Đóng Internet Explorer.

Bước 2:

Thiết lập một qui tắc giao thức cho phép người dùng trong nhóm Domain Admins truy cập Internet sử dụng tất cả các giao thức.

- ✓ Trong ISA Management kích Create a Protocol Rule.
- ✓ Trong New Protocol Rule Wizard, trong mục Protocol rule name gõ Allow All Access for Administrators sau đó kích Next.
- ✓ Trong trang Rule Action kiểm tra rằng Allow đã được chọn sau đó kích Next.
- ✓ Trong trang Protocols, trong danh sách Apply this rule to kiểm tra rằng All IP traffic đã được chọn sau đó kích Next.

- ✓ Trong trang Schedule, kiểm tra rằng Always đã được chọn sau đó kích Next.
- ✓ Trong trang Client Type, kích Specific users and groups, sau đó kích Next.
- ✓ Trong trang Users and Groups, kích Add.
- ✓ Trong hộp thoại Select Users or Groups, kích Domain Admins, kích Add, sau đó kích OK.
- ✓ Trong trang Users and Groups, kích Next.
- ✓ Trong trang Completing the New Protocol Rule Wizard kích Finish.

Bước 3:

Thiết lập một qui tắc giao thức từ chối người dùng trong nhóm Accounting Department đã định nghĩa trong client set truy cập Internet.

- ✓ Trong ISA Management, kích Create a Protocol Rule.
- ✓ Trong New Protocol Rule Wizard, trong mục Protocol rule name gõ vào Deny Access from Accounting Department , sau đó kích Next.
- ✓ Trong trang Rule Action, kích Deny, sau đó kích Next.
- ✓ Trong trang Protocols, trong danh sách Apply this rule to, kiểm tra rằng All IP traffic đã được lựa chọn, sau đó kích Next.
- ✓ Trong trang Schedule, kiểm tra rằng Always đã được lựa chọn, sau đó kích Next.
- ✓ Trong trang Client Type, kích Specific computers (client address
- ✓ sets), sau đó kích Next.
- ✓ Trong trang Client Sets, kích Add.
- ✓ Trong hộp thoại Add Client Sets, kích Accounting Department, kích Add, sau đó kíchOK.
- ✓ Trong trang Client Sets, kích Next.
- ✓ Trong trang Completing the New Protocol Rule Wizard, kích Finish.
- ✓ Kiểm tra để xác nhận việc truy cập không thành công từ nhóm nhóm Accounting Department

Bước 4:

Xóa qui tắc giao thức từ chối người dùng trong nhóm Accounting Department

- ✓ Trong In ISA Management, kích Deny Access from Accounting Department
- ✓ Kích Delete a Protocol Rule.
- ✓ Trong hộp thoại Confirm Delete, kích Yes.

III.Thiết lập các qui tắc nội dung

Bước 1:

Thiết lập một qui tắc nội dung để từ chối truy cập tới nội dung đã được định nghĩa trong destination set và với lịch trình đã thiết lập ở mục 1

- ✓ Trong ISA Management, kích Site and Content Rules.
- ✓ Kích Create a Site and Content Rule.
- ✓ Trong New Site and Content Rule Wizard, trong mục Site and content rule
- ✓ name, gõ vào một tên ví dụ Deny Access Rule sau đó kích Next.
- ✓ Trong trang Rule Action, kiểm tra rằng Deny đã được chọn, sau đó kích Next.
- ✓ Trong trang Destination Sets, trong danh sách Apply this rule to, kích Specified destination set.
- ✓ Trong danh sách Name, lựa chọn set1 (đã thiết lập ở phần trên), sau đó kích Next.
- ✓ Trong trang Schedule, chọn schedule1 (đã thiết lập ở phần trên), sau đó kích Next.
- ✓ Trong trang Client Type, kiểm tra rằng Any request đã được chọn, sau đó kích Next.
- ✓ Trong trang Completing the New Site and Content Rule Wizard, kích Finish.

Bước 2:

Kiểm tra qui tắc vừa thiết lập

- ✓ Mở trình duyệt Internet Explorer.

- ✓ Trong ô Address, gõ http://home.vnn.vn sau đó ấn ENTER. kiểm tra rằng trang web này không được hiển thị, vì qui tắc nội dung đã thiết lập ở trên đã có hiệu lực
- ✓ Đóng trình duyệt Internet Explorer.

Chương 6 : Bảo mật hệ thống và Firewall

Chương 6 tập trung vào các nội dung quan trọng về bảo mật hệ thống và mạng lưới. Nội dung của phần thứ nhất chương 6 cung cấp cho các học viên khái niệm về các hình thức tấn công mạng, các lỗ hổng, điểm yếu của mạng lưới. Các kỹ năng cơ bản trong phần một của chương 6 giúp người quản trị quản lý và xây dựng các chính sách bảo mật tương ứng cho các thành phần mạng, hệ thống hay dịch vụ ngay từ lúc bắt đầu hoạt động.

Phần 2 của chương 6 tập trung giới thiệu về thiết bị bảo mật mạnh và thông dụng trên mạng. Đó là thiết bị bức tường lửa (firewall). Học viên sẽ có được các kiến thức về cấu trúc firewall, các chức năng cơ bản và cách phân loại cũng như ưu nhược điểm của các loại firewall hoạt động theo các nguyên lý khác nhau. Những kỹ năng thiết lập cấu hình, luật, quản trị firewall với mô hình firewall checkpoint sẽ giúp cho các học viên hiểu cụ thể và các công việc quản trị và bảo mật hệ thống mạng

Chương 6 yêu cầu các học viên trang bị rất nhiều các kiến thức cơ bản như nắm vững các kiến thức quản trị hệ thống OS windows, linux, unix. Học viên cần hiểu sâu về giao thức TCP/IP, hoạt động của IP hay UDP, TCP. Học viên cần có hiểu biết về các port, socket của các giao thức dịch vụ như SMTP, POP3, WWW...Các kiến thức được trang bị trong các giáo trình quản trị hệ thống hoặc các tài liệu, sách giáo khoa về nội dung trên học viên nên tham khảo trước khi học chương 6 này.

I. Bảo mật hệ thống

I.1. Các vấn đề chung về bảo mật hệ thống và mạng

Do đặc điểm của một hệ thống mạng là có nhiều người sử dụng và phân tán về mặt địa lý nên việc bảo vệ các tài nguyên (mất mát, hoặc sử dụng không hợp lệ) trong môi trường mạng phức tạp hơn nhiều so với môi trường một máy tính đơn lẻ, hoặc một người sử dụng.

Hoạt động của người quản trị hệ thống mạng phải đảm bảo các thông tin trên mạng là tin cậy và sử dụng đúng mục đích, đối tượng đồng thời đảm bảo mạng hoạt động ổn định, không bị tấn công bởi những kẻ phá hoại.

Có một thực tế là không một hệ thống mạng nào đảm bảo là an toàn tuyệt đối, một hệ thống dù được bảo vệ chắc chắn đến mức nào thì cũng có lúc bị vô hiệu hoá bởi những kẻ có ý đồ xấu.

I.1.1. Một số khái niệm và lịch sử bảo mật hệ thống

Trước khi tìm hiểu các vấn đề liên quan đến phương thức phá hoại và các biện pháp bảo vệ cũng như thiết lập các chính sách về bảo mật, ta sẽ tìm hiểu một số khái niệm liên quan đến bảo mật thông tin trên mạng Internet.

I.1.1.1. Một số khái niệm:

a) Đối tượng tấn công mạng (Intruder):

Là những cá nhân hoặc các tổ chức sử dụng các kiến thức về mạng và các công cụ phá hoại (phần mềm hoặc phần cứng) để dò tìm các điểm yếu, lỗ hổng bảo mật trên hệ thống, thực hiện các hoạt động xâm nhập và chiếm đoạt tài nguyên mạng trái phép.

Một số đối tượng tấn công mạng là:

- Hacker: Là những kẻ xâm nhập vào mạng trái phép bằng cách sử dụng các công cụ phá mật khẩu hoặc khai thác các điểm yếu của các thành phần truy nhập trên hệ thống.

- Masquerader: Là những kẻ giả mạo thông tin trên mạng. Có một số hình thức như giả mạo địa chỉ IP, tên miền, định danh người dùng ...

- Eavesdropping: Là những đối tượng nghe trộm thông tin trên mạng, sử dụng các công cụ sniffer; sau đó dùng các công cụ phân tích và debug để lấy được các thông tin có giá trị.

Những đối tượng tấn công mạng có thể nhằm nhiều mục đích khác nhau như: ăn cắp những thông tin có giá trị về kinh tế, phá hoại hệ thống mạng có chủ định, hoặc cũng có thể chỉ là những hành động vô ý thức, thử nghiệm các chương trình không kiểm tra cẩn thận ...

b) Các lỗ hổng bảo mật:

Các lỗ hổng bảo mật là những điểm yếu trên hệ thống hoặc ẩn chứa trong một dịch vụ mà dựa vào đó kẻ tấn công có thể xâm nhập trái phép để thực hiện các hành động phá hoại hoặc chiếm đoạt tài nguyên bất hợp pháp.

Nguyên nhân gây ra những lỗ hổng bảo mật là khác nhau: có thể do lỗi của bản thân hệ thống, hoặc phần mềm cung cấp, hoặc do người quản trị yếu kém không hiểu sâu sắc các dịch vụ cung cấp ...

Mức độ ảnh hưởng của các lỗ hổng là khác nhau. Có những lỗ hổng chỉ ảnh hưởng tới chất lượng dịch vụ cung cấp, có những lỗ hổng ảnh hưởng nghiêm trọng tới toàn bộ hệ thống ...

c) Chính sách bảo mật:

Là tập hợp các qui tắc áp dụng cho mọi đối tượng có tham gia quản lý và sử dụng các tài nguyên và dịch vụ mạng.

Mục tiêu của chính sách bảo mật giúp người sử dụng biết được trách nhiệm của mình trong việc bảo vệ các tài nguyên thông tin trên mạng , đồng thời giúp các nhà quản trị thiết lập các biện pháp bảo đảm hữu hiệu trong quá trình trang bị, cấu hình, kiểm soát hoạt động của hệ thống và mạng

Một chính sách bảo mật được coi là hoàn hảo nếu nó xây dựng gồm các văn bản pháp qui, kèm theo các công cụ bảo mật hữu hiệu và nhanh chóng giúp người quản trị phát hiện, ngăn chặn các xâm nhập trái phép.

I.1.1.2. Lịch sử bảo mật hệ thống:

Có một số sự kiện đánh dấu các hoạt động phá hoại trên mạng, từ đó nảy sinh các yêu cầu về bảo mật hệ thống như sau:

- Năm 1988: Trên mạng Internet xuất hiện một chương trình tự nhân phiên bản của chính nó lên tất cả các máy trên mạng Internet. Các chương trình này gọi là "sâu". Tuy mức độ nguy hại của nó không lớn, nhưng nó đặt ra các vấn đề đối với nhà quản trị về quyền truy nhập hệ thống, cũng như các lỗi phần mềm.

- Năm 1990: Các hình thức truyền Virus qua địa chỉ Email xuất hiện phổ biến trên mạng Internet.

- Năm 1991: Phát hiện các chương trình trojans.

Cùng thời gian này sự phát triển của dịch vụ Web và các công nghệ liên quan như Java, Javascipts đã có rất nhiều các thông báo lỗi về bảo mật liên quan như: các lỗ hổng cho phép đọc nội dung các file dữ liệu của người dùng, một số lỗ hổng cho phép tấn công bằng hình thức DoS, spam mail làm ngưng trệ dịch vụ.

- Năm 1998: Virus Melisa lan truyền trên mạng Internet thông qua các chương trình gửi mail của Microsoft, gây những thiết hại kinh tế không nhỏ.

- Năm 2000: Một loạt các Web Site lớn như yahoo.com và ebay.com bị tê liệt, ngừng cung cấp dịch vụ trong nhiều giờ do bị tấn công bởi hình thức DoS.

I.1.2. Các lỗ hổng và phương thức tấn công mạng chủ yếu

I.1.2.1. Các lỗ hổng

Như phần trên đã trình bày, các lỗ hổng bảo mật trên một hệ thống là các điểm yếu có thể tạo ra sự ngưng trệ của dịch vụ, thêm quyền đối với người sử dụng hoặc cho phép các truy nhập không hợp pháp vào hệ thống. Các lỗ hổng cũng có thể nằm ngay các dịch vụ cung cấp như sendmail, web, ftp ... Ngoài ra các lỗ hổng còn tồn tại ngay chính tại hệ điều hành như trong Windows NT, Windows 95, UNIX hoặc trong các ứng dụng mà người sử dụng thường xuyên sử dụng như word processing, các hệ databases...

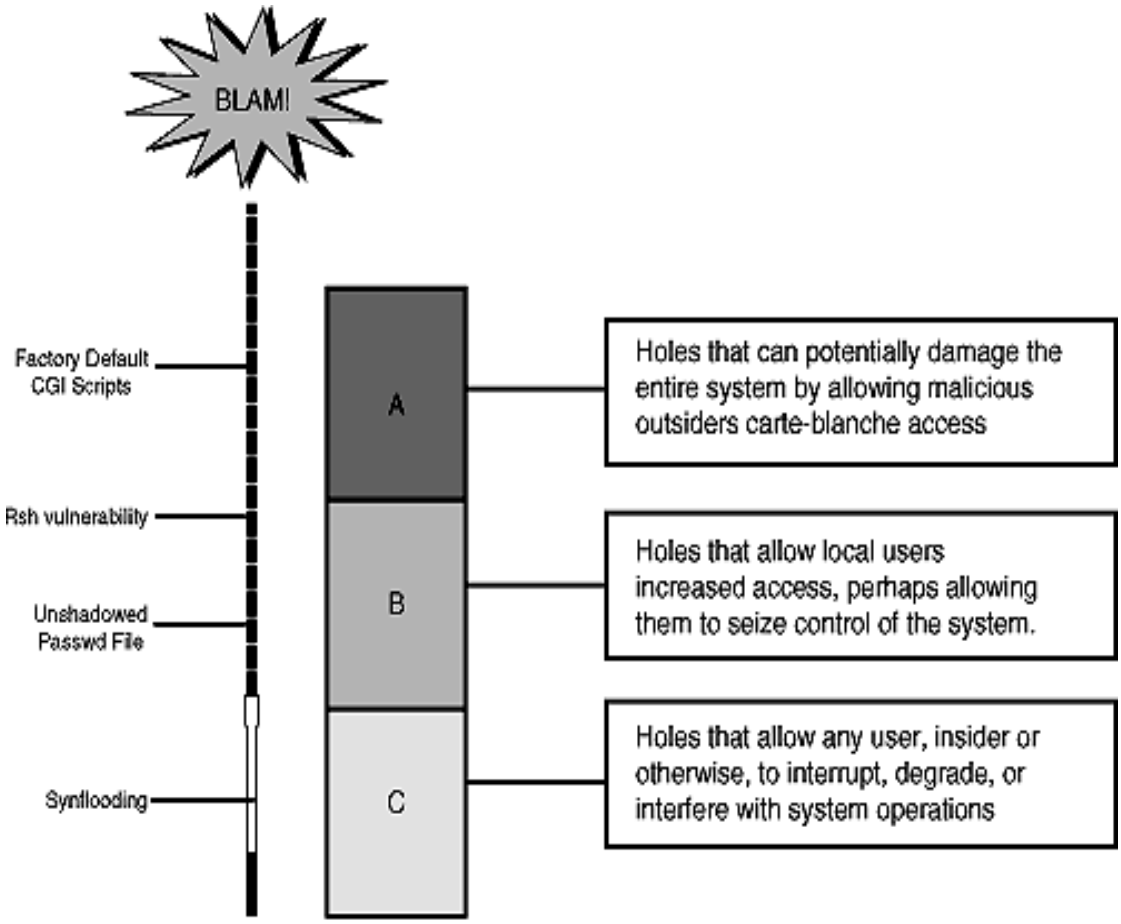
Có nhiều tổ chức khác nhau tiến hành phân loại các dạng lỗ hổng đặc biêt. Theo cách phân loại của Bộ quốc phòng Mỹ, các loại lỗ hổng bảo mật trên một hệ thống được chia như sau:

- Lỗ hổng loại C: các lỗ hổng loại này cho phép thực hiện các phương thức tấn công theo DoS (Denial of Services - Từ chối dịch vụ). Mức độ nguy hiểm thấp, chỉ ảnh hưởng tới chất lượng dịch vụ, có thể làm ngưng trệ, gián đoạn hệ thống; không làm phá hỏng dữ liệu hoặc đạt được quyền truy nhập bất hợp pháp.

- Lổ hổng loại B: Các lỗ hổng cho phép người sử dụng có thêm các quyền trên hệ thống mà không cần thực hiện kiểm tra tính hợp lệ nên có thể dẫn đến mất mát hoặc lộ thông tin yêu cầu bảo mật. Mức độ nguy hiểm trung bình. Những lỗ hổng này thường có trong các ứng dụng trên hệ thống.

- Lỗ hổng loại A: Các lỗ hổng này cho phép người sử dụng ở ngoài cho thể truy nhập vào hệ thống bất hợp pháp. Lỗ hổng này rất nguy hiểm, có thể làm phá hủy toàn bộ hệ thống.

Hình sau minh họa các mức độ nguy hiểm và loại lỗ hổng tương ứng:



Hình 1.1: Các loại lỗ hổng bảo mật và mức độ nguy hiểm

Sau đây ta sẽ phân tích một số lỗ hổng bảo mật thường xuất hiện trên mạng và hệ thống.

a) Các lỗ hổng loại C

Các lỗ hổng loại này cho phép thực hiện các cuộc tấn công DoS.

DoS là hình thức tấn công sử dụng các giao thức ở tầng Internet trong bộ giao thức TCP/IP để làm hệ thống ngưng trệ dẫn đến tình trạng từ chối người sử dụng hợp pháp truy nhập hay sử dụng hệ thống. Một số lượng lớn các gói tin được gửi tới server trong khoảng thời gian liên tục làm cho hệ thống trở nên

quá tải, kết quả là server đáp ứng chậm hoặc không thể đáp ứng các yêu cầu từ client gửi tới.

Các dịch vụ có lỗ hổng cho phép thực hiện các cuộc tấn công DoS có thể được nâng cấp hoặc sửa chữa bằng các phiên bản mới hơn của các nhà cung cấp dịch vụ. Hiện nay, chưa có một giải pháp toàn diện nào để khắc phục các lỗ hổng loại này vì bản thân việc thiết kế giao thức ở tầng Internet (IP) nói riêng và bộ giao thức TCP/IP đã chứa đựng những nguy cơ tiềm tàng của các lỗ hổng này.

Ví dụ điển hình của phương thức tấn công DoS là các cuộc tấn công vào một số Web Site lớn làm ngưng trệ hoạt động của web site này như: www.ebay.com và www.yahoo.com.

Tuy nhiên, mức độ nguy hiểm của các lỗ hổng loại này được xếp loại C, ít nguy hiểm vì chúng chỉ làm gián đoạn sự cung cấp dịch vụ của hệ thống trong một thời gian mà không làm nguy hại đến dữ liệu và những kẻ tấn công cũng không đạt được quyền truy nhập bất hợp pháp vào hệ thống.

Một lỗ hổng loại C khác cũng thường thấy đó là các điểm yếu của dịch vụ cho phép thực hiện tấn công làm ngưng trệ hệ thống của người sử dụng cuối. Chủ yếu hình thức tấn công này là sử dụng dịch vụ Web. Giả sử trên một Web Server có những trang Web trong đó có chứa các đoạn mã Java hoặc JavaScripts, làm "treo" hệ thống của người sử dụng trình duyệt Web của Netscape bằng các bước sau:

- Viết các đoạn mã để nhận biết được Web Browers sử dụng Netscape.

- Nếu sử dụng Netscape, sẽ tạo một vòng lặp vô thời hạn, sinh ra vô số các cửa sổ, trong mỗi cửa sổ đó nối đến các Web Server khác nhau.

Với một hình thức tấn công đơn giản này, có thể làm treo hệ thống trong khoảng thời gian 40 giây (đối với máy client có 64 MB RAM). Đây cùng là một hình thức tấn công kiểu DoS. Người sử dụng trong trường hợp này chỉ có thể khởi động lại hệ thống.

Một lỗ hổng loại C khác cũng thường gặp đối với các hệ thống mail là không xây dựng các cơ chế anti-relay (chống relay) cho phép thực hiện các hành động spam mail. Như chúng ta đã biết, cơ chế hoạt động của dịch vụ thư điện tử là lưu và chuyển tiếp. Một số hệ thống mail không có các xác thực khi người dùng gửi thư, dẫn đến tình trạng các đối tượng tấn công lợi dụng các

máy chủ mail này để thực hiện spam mail. Spam mail là hành động nhằm làm tê liệt dịch vụ mail của hệ thống bằng cách gửi một số lượng lớn các message tới một địa chỉ không xác định, vì máy chủ mail luôn phải tốn năng lực đi tìm những địa chỉ không có thực dẫn đến tình trạng ngưng trệ dịch vụ. Các message có thể sinh ra từ các chương trình làm bom thư rất phổ biến trên mạng Internet.

b) Các lỗ hổng loại B:

Lỗ hổng loại này có mức độ nguy hiểm hơn lỗ hổng loại C, cho phép người sử dụng nội bộ có thể chiếm được quyền cao hơn hoặc truy nhập không hợp pháp.

Ví dụ trên hình 12, lỗ hổng loại B có thể có đối với một hệ thống UNIX mà file /etc/passwd để ở dạng plaintext; không sử dụng cơ chế che mật khẩu trong UNIX (sử dụng file /etc/shadow)

Những lỗ hổng loại này thường xuất hiện trong các dịch vụ trên hệ thống. Người sử dụng local được hiểu là người đã có quyền truy nhập vào hệ thống với một số quyền hạn nhất định.

Một loại các vấn đề về quyền sử dụng chương trình trên UNIX cũng thương gây nên các lô hổng loại B. Vì trên hệ thống UNIX một chương trình có thể được thực thi với 2 khả năng:

- Người chủ sở hữu chương trình đó kích hoạt chạy.

- Người mang quyền của người sở hữu file đó kích hoạt chạy.

Một dạng khác của lỗ hổng loại B xảy ra đối với các chương trình có mã nguồn viết bằng C. Những chương trình viết bằng C thường sử dụng một vùng đệm - một vùng trong bộ nhớ sử dụng để lưu dữ liệu trước khi xử lý. Những người lập trình thường sử dụng vùng đệm trong bộ nhớ trước khi gán một khoảng không gian bộ nhớ cho từng khối dữ liệu. Ví dụ, người sử dụng viết chương trình nhập trường tên người sử dụng, qui định trường này dài 20 ký tự. Do đó họ sẽ khai báo:

char first_name [20];

Khai báo này sẽ cho phép người sử dụng nhập vào tối đa 20 ký tự. Khi nhập dữ liệu, trước tiên dữ liệu được lưu ở vùng đệm; nếu người sử dụng nhập vào 35 ký tự sẽ xảy ra hiện tượng tràn vùng đệm và kết quả 15 ký tự dư thừa sẽ nằm ở một vị trí không kiểm soát được trong bộ nhớ. Đối với những kẻ tấn công, có thể lợi dụng lỗ hổng này để nhập vào những ký tự đặc biệt, để thực thi

một số lệnh đặc biệt trên hệ thống. Thông thường, lỗ hổng này thường được lợi dụng bởi những người sử dụng trên hệ thống để đạt được quyền root không hợp lệ.

Việc kiểm soát chặt chẽ cấu hình hệ thống và các chương trình sẽ hạn chế được các lỗ hổng loại B.

c) Các lỗ hổng loại A:

Các lỗ hổng loại A có mức độ rất nguy hiểm, đe dọa tính toàn vẹn và bảo mật của hệ thống. Các lỗ hổng loại này thường xuất hiện ở những hệ thống quản trị yếu kém hoặc không kiểm soát được cấu hình mạng.

Một ví dụ thường thấy là trên nhiều hệ thống sử dụng Web Server là Apache, Đối với Web Server này thường cấu hình thư mục mặc định để chạy các script là cgi-bin; trong đó có một Scripts được viết sẵn để thử hoạt động của apache là test-cgi. Đối với các phiên bản cũ của Apache (trước version 1.1), có dòng sau trong file test-cgi:

echo QUERY_STRING = $QUERY_STRING

Biến môi trường QUERY_STRING do không được đặt trong có dấu " (quote) nên khi phía client thực hiện một yêu cầu trong đó chuỗi ký tự gửi đến gồm một số ký tự đặc biệt; ví dụ ký tự "*", web server sẽ trả về nội dung của toàn bộ thư mục hiện thời (là các thư mục chứa các script cgi). Người sử dụng có thể nhìn thấy toàn bộ nội dung các file trong thư mục hiện thời trên hệ thống server.

Một ví dụ khác cũng xảy ra tương tự đối với các Web server chạy trên hệ điều hành Novell: các web server này có một scripts là convert.bas, chạy scripts này cho phép đọc toàn bộ nội dung các files trên hệ thống.

Những lỗ hổng loại này hết sức nguy hiểm vì nó đã tồn tại sẵn có trên phần mềm sử dụng, người quản trị nếu không hiểu sâu về dịch vụ và phần mềm sử dụng sẽ có thể bỏ qua những điểm yếu này.

Đối với những hệ thống cũ, thường xuyên phải kiểm tra các thông báo của các nhóm tin về bảo mật trên mạng để phát hiện những lỗ hổng loại này. Một loạt các chương trình phiên bản cũ thường sử dụng có những lỗ hổng loại A như: FTP, Gopher, Telnet, Sendmail, ARP, finger...

I.1.2.2. Một số phương thức tấn công mạng phổ biến

a) Scanner

Scanner là một chương trình tự động rà soát và phát hiện những điểm yếu về bảo mật trên một trạm làm việc cục bộ hoặc trên một trạm ở xa. Với chức năng này, một kẻ phá hoại sử dụng chương trình Scanner có thể phát hiện ra những lỗ hổng về bảo mật trên một server ở xa.

Các chương trình scanner thường có một cơ chế chung là rà soát và phát hiện những port TCP/UDP được sử dụng trên một hệ thống cần tấn công từ đó phát hiện những dịch vụ sử dụng trên hệ thống đó. Sau đó các chương trình scanner ghi lại những đáp ứng trên hệ thống ở xa tương ứng với các dịch vụ mà nó phát hiện ra. Dựa vào những thông tin này, những kẻ tấn công có thể tim ra những điểm yếu trên hệ thống.

Những yếu tố để một chương trình Scanner có thể hoạt động như sau:

- Yêu cầu về thiết bị và hệ thống: Một chương trình Scanner có thể hoạt động được nếu môi trường đó có hỗ trợ TCP/IP (bất kể hệ thống là UNIX, máy tính tương thích với IBM, hoặc dòng máy Macintosh).

- Hệ thống đó phải kết nối vào mạng Internet.

Tuy nhiên không phải đơn giản để xây dựng một chương trình Scanner, những kẻ phá hoại cần có kiến thức sâu về TCP/IP, những kiến thức về lập trình C, PERL và một số ngôn ngữ lập trình shell. Ngoài ra người lập trình (hoặc người sử dụng) cần có kiễn thức là lập trình socket, phương thức hoạt động của các ứng dụng client/server.

Các chương trình Scanner có vai trò quan trọng trong một hệ thống bảo mật, vì chúng có khả năng phát hiện ra những điểm yếu kém trên một hệ thống mạng. Đối với người quản trị mạng những thông tin này là hết sức hữu ích và cần thiết; đối với những kẻ phá hoại những thông tin này sẽ hết sức nguy hiểm.

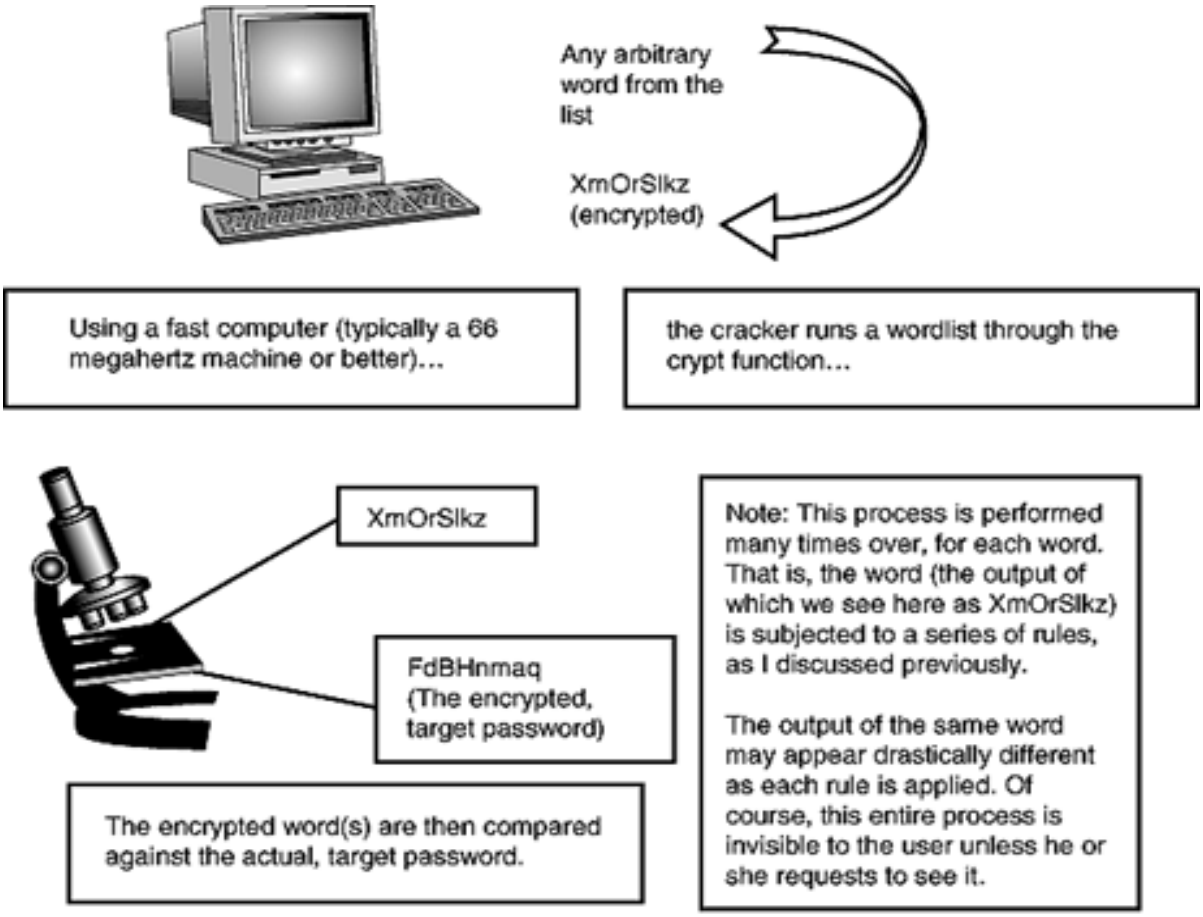
b) Password Cracker

Password cracker là một chương trình có khả năng giải mã một mật khẩu đã được mã hoá hoặc có thể vô hiệu hoá chức năng bảo vệ mật khẩu của một hệ thống.

Để hiểu cách thức hoạt động của các chương trình bẻ khoá, chúng ta cần hiểu cách thức mã hoá để tạo mật khẩu. Hầu hết việc mã hoá các mật khẩu

được tạo ra từ một phương thức mã hoá. Các chương trình mã hoá sử dụng các thuật toán mã hoá để mã hoá mật khẩu.

Quá trình hoạt động của các chương trình bẻ khoá được minh hoạ trong hình sau:



Hình 1.2: Hoạt động của các chương trình bẻ khóa

Theo sơ đồ trên, một danh sách các từ được tạo ra và được mã hoá đối với từng từ. Sau mỗi lần mã hoá, chương trình sẽ so sánh với mật khẩu đã mã hoá cần phá. Nếu không thấy trùng hợp, quá trình lại quay lại. Phương thức bẻ khoá này gọi là bruce-force.

Yếu tố về thiết bị phần cứng: Trong hình trên máy tính thực hiện các chương trình phá khoá là một máy PC 66MHz hoặc cấu hình cao hơn. Trong thực tế yêu cầu các thiết bị phần cứng rất mạnh đối với những kẻ phá khoá

chuyên nghiệp. Một phương thức khác có thể thay thế là thực hiện việc phá khoá trên một hệ thống phần tán; do vậy giảm bớt được các yêu cầu về thiết bị so với phương pháp làm tại một máy.

Nguyên tắc của một số chương trình phá khoá có thể khác nhau. Một vài chương trình tạo một một danh sách các từ giới hạn, áp dụng một số thuật toán mã hoá, từ kết quả so sánh với password đã mã hoá cần bẻ khoá để tạo ra một danh sách khác theo một lôgic của chương trình, cách này tuy không chuẩn tắc nhưng khá nhanh vì dựa vào nguyên tắc khi đặt mật khẩu người sử dụng thường tuân theo một số qui tắc để thuận tiện khi sử dụng.

Đến giai đoạn cuối cùng, nếu thấy phù hợp với mật khẩu đã được mã hoá, kẻ phá khoá sẽ có được mật khẩu dạng text thông thường. Trong hình trên, mật khẩu dạng text thông thường được ghi vào một file.

Để đánh giá khả năng thành công của các chương trình bẻ khoá ta có công thức sau:

$$P = L \times R / S$$

Trong đó:

P: Xác suất thành công

L: Thời gian sống của một mật khẩu

R: Tốc độ thử

S: Không gian mật khẩu = A^M (M là chiều dài mật khẩu)

Ví dụ, trên hệ thống UNIX người ta đã chứng minh được rằng nếu mật khẩu dài quá 8 ký tự thì xác suất phá khoá gần như = 0. Cụ thể như sau:

Nếu sử dụng khoảng 92 ký tự có thể đặt mật khẩu, không gian mật khẩu có thể có là $S = 92^8$

Với tốc độ thử là 1000 mật khẩu trong một giây có R = 1000/s

Thời gian sống của một mật khẩu là 1 năm

Ta có xác suất thành công là :

$P = 1x\ 365\ x\ 86400\ x\ 1000/92^8 = 1/1.000.000$

Như vậy việc dò mật khẩu là không thể vì sẽ mất khoảng 100 năm mới tìm ra mật khẩu chính xác.

Thông thường các chương trình phá khoá thường kết hợp một số thông tin khác trong quá trình dò mật khẩu như:

- Các thông tin trong tập tin /etc/passwd

- Một số từ điển

- Từ lặp và các từ liệt kê tuần tự, chuyển đổi cách phát âm của một từ ...

Biện pháp khắc phục đối với cách thức phá hoại này là cần xây dựng một chính sách bảo vệ mật khẩu đúng đắn.

c) Trojans

Dựa theo truyền thuyết cổ Hy lạp "Ngựa thành Trojan", trojans là một chương trình chạy không hợp lệ trên một hệ thống với vai trò như một chương trình hợp pháp. Những chương trình này thực hiện những chức năng mà người sử dụng hệ thống thường không mong muốn hoặc không hợp pháp. Thông thường, trojans có thể chạy được là do các chương trình hợp pháp đã bị thay đổi mã của nó bằng những mã bất hợp pháp.

Các chương trình virus là một loại điển hình của Trojans. Những chương trình virus che dấu các đoạn mã trong các chương trình sử dụng hợp pháp. Khi những chương trình này được kích hoạt thì những đoạn mã ẩn dấu sẽ được thực thi để thực hiện một số chức năng mà người sử dụng không biết.

Một định nghĩa chuẩn tắc về các chương trình Trojans như sau: chương trình trojans là một chương trình thực hiện một công việc mà người sử dụng không biết trước, giống như ăn cấp mật khẩu hay copy file mà người sử dụng không nhận thức được.

Những tác giả của các chương trình trojan xây dựng một kết hoạch. Xét về khía cạnh bảo mật trên Internet, một chương trình trojan sẽ thực hiện 1 trong những công việc sau:

- Thực hiện một vài chức năng hoặc giúp người lập trình phát hiện những thông tin quan trọng hoặc thông tin cá nhân trên một hệ thống hoặc một vài thành phần của hệ thống đó

- Che dấu một vài chức năng hoặc giúp người lập trình phát hiện những thông tin quan trọng hoặc thông tin cá nhân trên một hệ thống hoặc một vài thành phần của hệ thống đó

Một vài chương trình trojan có thể thực hiện cả 2 chức năng này. Ngoài ra, một số chương trình trojans còn có thể phá huỷ hệ thống bằng cách phá hoại các thông tin trên ổ cứng (ví dụ trường hợp của virus Melisa lây lan qua đường thư điện tử).

Hiện nay với nhiều kỹ thuật mới, các chương trình trojan kiểu này dễ dàng bị phát hiện và không có khả năng phát huy tác dụng. Tuy nhiên trong UNIX việc phát triển các chương trình trojan vẫn hết sức phổ biến.

Các chương trình trojan có thể lây lan qua nhiều phương thức, hoạt động trên nhiều môi trường hệ điều hành khác nhau (từ Unix tới Windows, DOS). Đặc biệt trojans thường lây lan qua một số dịch vụ phổ biến như Mail, FTP... hoặc qua các tiện ích, chương trình miễn phí trên mạng Internet.

Việc đánh giá mức độ ảnh hưởng của các chương trình trojans hết sức khó khăn. Trong một vài trường hợp, nó chỉ đơn giản là ảnh hưởng đến các truy nhập của khách hàng như các chương trình trojans lấy được nội dung của file passwd và gửi mail tới kẻ phá hoại. Cách thức sửa đơn giản nhất là thay thế toàn bộ nội dung của các chương trình đã bị ảnh hưởng bởi các đoạn mã trojans và thay thế các password của người sử dụng hệ thống.

Tuy nhiên với những trường hợp nghiêm trọng hơn, là những kẻ tán công tạo ra những lỗ hổng bảo mật thông qua các chương trình trojans. Ví dụ những kẻ tấn công lấy được quyền root trên hệ thống và lợi dụng nó để phá huỷ toàn bộ hoặc một phần của hệ thống. Chúng dùng quyền root để thay đổi logfile, cài đặt các chương trình trojans khác mà người quản trị không thể phát hiện. Trong trường hợp này, mức độ ảnh hưởng là nghiêm trọng và người quản trị hệ thống đó chỉ còn cách là cài đặt lại toàn bộ hệ thống

d) Sniffer

Đối với bảo mật hệ thống sniffer được hiểu là các công cụ (có thể là phần cứng hoặc phần mềm) "bắt" các thông tin lưu chuyển trên mạng và từ các thông tin "bắt" được đó để lấy được những thông tin có giá trị trao đổi trên mạng.

Hoạt động của sniffer cũng giống như các chương trình "bắt" các thông tin gõ từ bàn phím (key capture). Tuy nhiên các tiện ích key capture chỉ thực hiện trên một trạm làm việc cụ thể còn đối với sniffer có thể bắt được các thông tin trao đổi giữa nhiều trạm làm việc với nhau.

Các chương trình sniffer (sniffer mềm) hoặc các thiết bị sniffer (sniffer cứng) đều thực hiện bắt các gói tin ở tầng IP trở xuống (gồm IP datagram và Ethernet Packet). Do đó, có thể thực hiện sniffer đối với các giao thức khác nhau ở tầng mạng như TCP, UDP, IPX, ...

Mặt khác, giao thức ở tầng IP được định nghĩa công khai, và cấu trúc các trường header rõ ràng, nên việc giải mã các gói tin này không khó khăn.

Mục đích của các chương trình sniffer đó là thiết lập chế độ promiscuous (mode dùng chung) trên các card mạng ethernet - nơi các gói tin trao đổi trong mạng - từ đó "bắt" được thông tin.

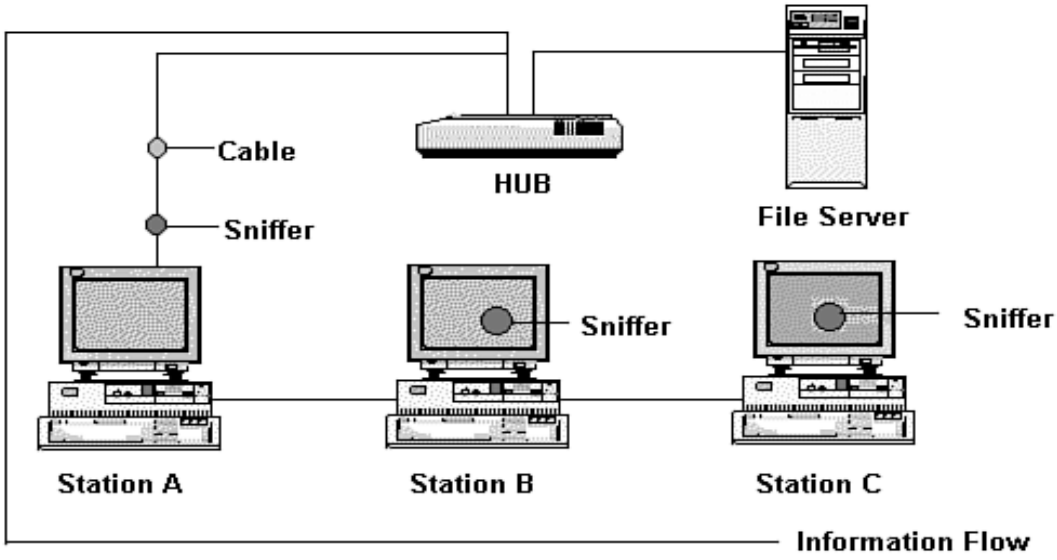
Các thiết bị sniffer có thể bắt được toàn bộ thông tin trao đổi trên mạng là dựa vào nguyên tắc broadcast (quảng bá) các gọi tin trong mạng Ethernet.

Trên hệ thống mạng không dùng hub, dữ liệu không chuyển đến một hướng mà được lưu chuyển theo mọi hướng. Ví dụ khi một trạm làm việc cần được gửi một thông báo đến một trạm làm việc khác trên cùng một segment mạng, một yêu cầu từ trạm đích được gửi tới tất cả các trạm làm việc trên mạng để xác định trạm nào là trạm cần nhận thông tin (trạm đích). Cho tới khi trạm nguồn nhận được thông báo chấp nhận từ trạm đích thì luồng dữ liệu sẽ được gửi đi. Theo đúng nguyên tắc, những trạm khác trên segment mạng sẽ bỏ qua các thông tin trao đổi giữa hai trạm nguồn và trạm đích xác định. Tuy nhiên, các trạm khác cũng không bị bắt buộc phải bỏ qua những thông tin này, do đó chúng vẫn có thể "nghe" được bằng cách thiết lập chế độ promiscous mode trên các card mạng của trạm đó. Sniffer sẽ thực hiện công việc này.

Một hệ thống sniffer có thể kết hợp cả các thiết bị phần cứng và phần mềm, trong đó hệ thống phần mềm với các chế độ debug thực hiện phân tích các gói tin "bắt" được trên mạng.

Hệ thống sniffer phải được đặt trong cùng một segment mạng (network block) cần nghe lén.

Hình sau minh hoạ vị trí đặt sniffer:



Hình 1.3: Các vị trí đặt sniffer trên 1 segment mạng

Phương thức tấn công mạng dựa vào các hệ thống sniffer là rất nguy hiểm vì nó được thực hiện ở các tầng rất thấp trong hệ thống mạng. Với việc thiết lập hệ thống sniffer cho phép lấy được toàn bộ các thông tin trao đổi trên mạng. Các thông tin đó có thể là:

- Các tài khoản và mật khẩu truy nhập

- Các thông tin nội bộ hoặc có giá trị cao...

Tuy nhiên việc thiết lập một hệ thống sniffer không phải đơn giản vì cần phải xâm nhập được vào hệ thống mạng đó và cài đặt các phần mềm sniffer. Đồng thời các chương trình sniffer cũng yêu cầu người sử dụng phải hiểu sâu về kiến trúc, các giao thức mạng.

Mặc khác, số lượng các thông tin trao đổi trên mạng rất lớn nên các dữ liệu do các chương trình sniffer sinh ra khá lớn. Thông thường, các chương trình sniffer có thể cấu hình để chỉ thu nhập từ 200 - 300 bytes trong một gói tin, vi thường những thông tin quan trọng như tên người dùng, mật khẩu nằm ở phần đầu gói tin.

Trong một số trường hợp quản trị mạng, để phân tích các thông tin lưu chuyển trên mạng, người quản trị cũng cần chủ động thiết lập các chương trình sniffer, với vai trò này sniffer có tác dụng tốt.

Việc phát hiện hệ thống bị sniffer không phải đơn giản, vì sniffer hoạt động ở tầng rất thấp, và không ảnh hưởng tới các ứng dụng cũng như các dịch

vụ hệ thống đó cung cấp. Một số biện pháp sau chỉ có tác dụng kiểm tra hệ thống như:

- Kiểm tra các tiến trình đang thực hiện trên hệ thống (bằng lệnh ps trên Unix hoặc trình quản lý tài nguyên trong Windows NT). Qua đó kiểm tra các tiến trình lạ trên hệ thống; tài nguyên sử dụng, thời gian khởi tạo tiến trình... để phát hiện các chương trình sniffer.

- Sử dụng một vài tiện ích để phát hiện card mạng có chuyển sang chế đố promiscous hay không. Những tiện ích này giúp phát hiện hệ thống của bạn có đang chạy sniffer hay không.

Tuy nhiên việc xây dựng các biện pháp hạn chế sniffer cũng không quá khó khăn nếu ta tuân thủ các nguyên tắc về bảo mật như:

- Không cho người lạ truy nhập vào các thiết bị trên hệ thống

- Quản lý cấu hình hệ thống chặt chẽ

- Thiết lập các kết nối có tính bảo mật cao thông qua các cơ chế mã hoá.

I.1.3. Một số điểm yếu của hệ thống

I.1.3.1. Deamon fingerd:

Một lỗ hổng của deamon fingerd là cơ hội để phương thức tấn công worm "sâu" trên Internet phát triển: đó là lỗi tràn vùng đệm trong các tiến trình fingerd (lỗi khi lập trình). Vùng đệm để lưu chuỗi ký tự nhập được giới hạn là 512 bytes. Tuy nhiên chương trình fingerd không thực hiện kiểm tra dữ liệu đầu vào khi lớn hơn 512 bytes. Kết quả là xảy ra hiện tượng tràn dữ liệu ở vùng đệm khi dữ liệu lớn hơn 512 bytes. Phần dữ liệu dư thừa chứa những đoạn mã để kích một script khác hoạt động; scripts này tiếp tục thực hiện finger tới một host khác. Kết quả là hình thành một mắt xích các "sâu" trên mạng Internet.

I.1.3.2. File hosts.equiv:

Nếu một người sử dụng được xác định trong file host.equiv cũng với địa chỉ máy của người đó, thì người sử dụng đó được phép truy nhập từ xa vào hệ thống đã khai báo. Tuy nhiên có một lỗ hổng khi thực hiện chức năng này đó là nó cho phép người truy nhập từ xa có được quyền của bất cứ người nào khác trên hệ thống. Ví dụ, nếu trên máy A có một file /etc/host.equiv có dòng định danh B julie, thì julie trên B có thể truy nhập vào hệ thống A và có bất được

quyền của bất cứ người nào khác trên A. Đây là do lỗi của thủ tục ruserok() trong thư viện libc khi lập trình.

I.1.3.3. Thư mục /var/mail

Nếu thư mục /var/mail được set là với quyền được viết (writeable) đối với tất cả mọi người trên hệ thống, thì bất cứ ai có thể tạo file trong thư mục này. Sau đó tạo một file với tên của một người đã có trên hệ thống rồi link tới một file trên hệ thống, thì các thư tới người sử dụng có tên trùng với tên file link sẽ được gán thêm vào trong file mà nó link tới.

Ví dụ, một người sử dụng tạo link từ /var/mail/root tới /etc/passwd, sau đó gửi mail bằng tên một người mới tới root thì tên người sử dụng mới này sẽ được gán thêm vào trong file /etc/passwd; Do vậy thư mục /var/mail không bao giờ được set với quyền writeable.

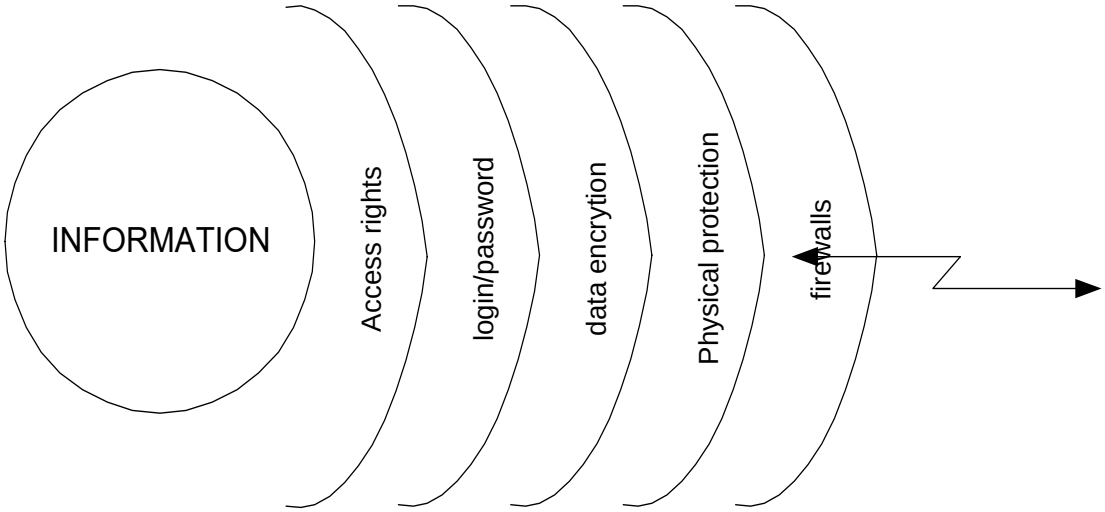
I.1.3.4. Chức năng proxy của FTPd:

Chức năng proxy server của FTPd cho phép một người sử dụng có thể truyền file từ một ftpd này tới một ftpd server khác. Sử dụng chức năng này sẽ có thể bỏ qua được các xác thực dựa trên địa chỉ IP.

Nguyên nhân là do người sử dụng có thể yêu cầu một file trên ftp server gửi một file tới bất kỳ địa chỉ IP nào. Nên người sử dụng có thể yêu cầu ftp server đó gửi một file gồm các lệnh là PORT và PASV tới các server đang nghe trên các port TCP trên bất kỳ một host nào; kết quả là một trong các host đó có ftp server chạy và tin cậy người sử dụng đó nên bỏ qua được xác thực địa chỉ IP.

I.1.4. Các mức bảo vệ an toàn mạng

Vì không có một giải pháp an toàn tuyệt đối nên người ta thường phải sử dụng đồng thời nhiều mức bảo vệ khác nhau tạo thành nhiều lớp "rào chắn" đối với các hoạt động xâm phạm. Việc bảo vệ thông tin trên mạng chủ yếu là bảo vệ thông tin cất giữ trong các máy tính, đặc biệt là trong các server của mạng. Hình sau mô tả các lớp rào chắn thông dụng hiện nay để bảo vệ thông tin tại các trạm của mạng:



Hình 1.4: Các mức độ bảo vệ mạng

Như minh hoạ trong hình trên, các lớp bảo vệ thông tin trên mạng gồm:

- Lớp bảo vệ trong cùng là quyền truy nhập nhằm kiểm soát các tài nguyên (ở đây là thông tin) của mạng và quyền hạn (có thể thực hiện những thao tác gì) trên tài nguyên đó. Hiện nay việc kiểm soát ở mức này được áp dụng sâu nhất đối với tệp.

- Lớp bảo vệ tiếp theo là hạn chế theo tài khoản truy nhập gồm đăng ký tên và mật khẩu tương ứng. Đây là phương pháp bảo vệ phổ biến nhất vì nó đơn giản, ít tốn kém và cũng rất có hiệu quả. Mỗi người sử dụng muốn truy nhập được vào mạng sử dụng các tài nguyên đều phải có đăng ký tên và mật khẩu. Người quản trị hệ thống có trách nhiệm quản lý, kiểm soát mọi hoạt động của mạng và xác định quyền truy nhập của những người sử dụng khác tuỳ theo thời gian và không gian.

- Lớp thứ ba là sử dụng các phương pháp mã hoá (encryption). Dữ liệu được biến đổi từ dạng clear text sang dạng mã hoá theo một thuật toán nào đó.

- Lớp thứ tư là bảo vệ vật lý (physical protection) nhằm ngăn cản các truy nhập vật lý bất hợp pháp vào hệ thống. Thường dùng các biện pháp truyền thống như ngăn cấm người không có nhiệm vụ vào phòng đặt máy, dùng hệ thống khoá trên máy tính, cài đặt các hệ thống báo động khi có truy nhập vào hệ thống ...

- Lớp thứ năm: Cài đặt các hệ thống bức tường lửa (firewall), nhằm ngăn chặn các thâm nhập trái phép và cho phép lọc các gói tin mà ta không muốn gửi đi hoặc nhận vào vì một lý do nào đó.

I.2. Các biện pháp bảo vệ mạng máy tính

I.2.1. Kiểm soát hệ thống qua logfile

Một trong những biện pháp dò tìm các dấu vết hoạt động trên một hệ thống là dựa vào các công cụ ghi logfile. Các công cụ này thực hiện ghi lại nhật ký các phiên làm việc trên hệ thống. Nội dung chi tiết thông tin ghi lại phụ thuộc vào cấu hình người quản trị hệ thống. Ngoài việc rà soát theo dõi hoạt động, đối với nhiều hệ thống các thông tin trong logfile giúp người quản trị đánh giá được chất lượng, hiệu năng của mạng lưới.

I.2.1.1. Hệ thống logfile trong Unix:

Trong Unix, các công cụ ghi log tạo ra logfile là các file dưới dạng text thông thường cho phép người sử dụng dùng những công cụ soạn thảo file text bất kỳ để có thể đọc được nội dung. Tuy nhiên, một số trường hợp logfile được ghi dưới dạng binary và chỉ có thể sử dụng một số tiện ích đặc biệt mới có thể đọc được thông tin.

a) Logfile lastlog:

Tiện ích này ghi lại những lần truy nhập gần đây đối với hệ thống. Các thông tin ghi lại gồm tên người truy nhập, thời điểm, địa chỉ truy nhập ... Các chương trình login sẽ đọc nội dung file lastlog, kiểm tra theo UID truy nhập vào hệ thống và sẽ thông báo lần truy nhập vào hệ thống gần đây nhất. Ví dụ như sau:

```
Last login: Fri Sep 15 2000 14:11:38
Sun Microsystems Inc.   SunOS 5.7       Generic October 1998
No mail.
Sun Microsystems Inc.   SunOS 5.7       Generic October 1998
```

```
/export/home/ptthanh
```

b) Logfile UTMP

Logfile này ghi lại thông tin về những người đang login vào hệ thống, thường nằm ở thư mục /etc/utmp. Để xem thông tin trong logfile có thể sử dụng các tiện ích như who, w, finger, rwho, users. Ví dụ nội dung của logfile dùng lệnh who như sau:

```
/export/home/vhai% who
root      console     Aug 10 08:45    (:0)
ptthanh     pts/4       Sep 15 15:27    (203.162.0.87)
ptthanh     pts/6       Sep 15 15:28    (203.162.0.87)
root      pts/12      Sep  7 16:35    (:0.0)
root      pts/13      Sep  7 11:35    (:0.0)
root      pts/14      Sep  7 11:39    (:0.0)
```

c) Logfile WTMP

Logfile này ghi lại các thông tin về các hoạt động login và logout vào hệ thống. Nó có chức năng tương tự với logfile UTMP. Ngoài ra còn ghi lại các thông tin về các lần shutdown, reboot hệ thống, các phiên truy nhập hoặc ftp và thường nằm ở thư mục /var/adm/wtmp. Logfile này thường được xem bằng lệnh "last". Ví dụ nội dung như sau:

```
/export/home/vhai% last | more
ptthanh     pts/10      203.162.0.85          Mon Sep 18 08:44   still logged in
ptthanh    pts/10                             Sat Sep 16 16:52 - 16:52  (00:00)
vtoan    pts/10      203.162.0.87            Fri Sep 15 15:30 - 16:52 (1+01:22)
vtoan    pts/6       203.162.0.87      Fri Sep 15 15:28   still logged in
vtoan    pts/4                              Fri Sep 15 15:12 - 15:12  (00:00)
```

d) Tiện ích Syslog

Đây là một công cụ ghi logfile rất hữu ích, được sử dụng rất thông dụng trên các hệ thống UNIX. Tiện ích syslog giúp người quản trị hệ thống dễ dàng trong việc thực hiện ghi logfile đối với các dịch vụ khác nhau. Thông thường tiện ích syslog thường được chạy dưới dạng một daemon và được kích hoạt khi hệ thống khởi động. Daemon syslogd lấy thông tin từ một số nguồn sau:

- /dev/log: Nhận các messages từ các tiến trình hoạt động trên hệ thống

- /dev/klog: nhận messages từ kernel

- port 514: nhận các messages từ các máy khác qua port 514 UDP.

Khi syslogd nhận các messages từ các nguồn thông tin này nó sẽ thực hiện kiểm tra file cấu hình của dịch vụ là syslog.conf để tạo log file tương ứng. Có thể cấu hình file syslog.conf để tạo một message với nhiều dịch vụ khác nhau.

Ví dụ nội dung một file syslog.conf như sau:

```
# This file is processed by m4 so be careful to quote (`') names
# that match m4 reserved words.  Also, within ifdef's, arguments
# containing commas must be quoted.
#
*.err;kern.notice;auth.notice                  /dev/console
*.err;kern.debug;daemon.notice;mail.crit       /var/adm/messages

*.alert;kern.err;daemon.err                    operator
*.alert                                        root

*.emerg                                        *

# if a non-loghost machine chooses to have authentication messages
```

Trong nội dung file syslog.conf chỉ ra, đối với các message có dạng *.emerg (message có tính khẩn cấp) sẽ được thông báo tới tất cả người sử dụng trên hệ thống; Đối với các messages có dạng *.err, hoặc kern.debug và những hoạt động truy cập không hợp pháp sẽ được ghi log trong file /var/adm/messages.

Mặc định, các messages được ghi vào logfile /var/adm/messages.

e) Tiện ích sulog

Bất cứ khi nào người sử dụng dùng lệnh "su" để chuyển sang hoạt động hệ thống dưới quyền một user khác đều được ghi log thông qua tiện ích sulog. Những thông tin logfile này được ghi vào logfile /var/adm/sulog. Tiện ích này cho phép phát hiện các trường hợp dùng quyền root để có được quyền của một user nào khác trên hệ thống.

Ví dụ nội dung của logfile sulog như sau:

```
# more /var/adm/sulog
SU 01/04 13:34 + pts/1 ptthanh-root
SU 01/04 13:53 + pts/6 ptthanh-root
SU 01/04 14:19 + pts/6 ptthanh-root
SU 01/04 14:39 + pts/1 ptthanh-root
```

f) Tiện ích cron

Tiện ích cron sẽ ghi lại logfile của các hoạt động thực hiện bởi lệnh crontabs. Thông thường, logfile của các hoạt động cron lưu trong file /var/log/cron/log. Ngoài ra, có thể cấu hình syslog để ghi lại các logfile của hoạt động cron.

Ví dụ nội dung của logfile cron như sau:

```
# more /var/log/cron/log
! *** cron started ***   pid = 2367 Fri Aug  4 16:32:38 2000
>  CMD: /export/home/mrtg/mrtg /export/home/mrtg/termcount.cfg
>  ptthanh 2386 c Fri Aug  4 16:34:01 2000
<  ptthanh 2386 c Fri Aug  4 16:34:02 2000
>  CMD: /export/home/mrtg/getcount.pl
>  ptthanh 2400 c Fri Aug  4 16:35:00 2000
<  ptthanh 2400 c Fri Aug  4 16:35:10 2000
>  CMD: /export/home/mrtg/mrtg /export/home/mrtg/termcount.cfg
```

g) Logfile của sendmail

Hoạt động ghi log của sendmail có thể được ghi qua tiện ích syslog. Ngoài ra chương trình sendmail còn có lựa chọn "-L + level security" với mức độ bảo mật từ "debug" tới "crit" cho phép ghi lại logfile. Vì sendmail là một chương trình có nhiều bug, với nhiều lỗ hổng bảo mật nền người quản trị hệ thống thường xuyên nên ghi lại logfile đối với dịch vụ này.

h) Logfile của dịch vụ FTP

Hầu hết các daemon FTP hiện nay đều cho phép cấu hình để ghi lại logfile sử dụng dịch vụ FTP trên hệ thống đó. Hoạt động ghi logfile của dịch vụ FTP thường được sử dụng với lựa chọn "-l", cấu hình cụ thể trong file /etc/inetd.conf như sau:

```
# more /etc/inetd.conf
ftp    stream  tcp    nowait  root   /etc/ftpd/in.ftpd      in.ftpd -l
```

Sau đó cấu hình syslog.conf tương ứng với dịch vụ FTP; cụ thể như sau:

```
#  Logfile FTP
daemon.info                          ftplogfile
```

Với lựa chọn này sẽ ghi lại nhiều thông tin quan trọng trong một phiên ftp như: thời điểm truy nhập, địa chỉ IP, dữ liệu get/put ... vào site FTP đó. Ví dụ nội dung logfile của một phiên ftp như sau:

```
Sun Jul 16 21:55:06 2000 12 nms 8304640 /export/home/ptthanh/PHSS_17926.depot b _ o r ptthanh ftp 0 * c
Sun Jul 16 21:56:45 2000 96 nms 64624640 /export/home/ptthanh/PHSS_19345.depot b _ o r ptthanh ftp 0 * c
Sun Jul 16 21:57:41 2000 4 nms 3379200 /export/home/ptthanh/PHSS_19423.depot b _ o r ptthanh ftp 0 * c
Sun Jul 16 22:00:38 2000 174 nms 130396160 /export/home/ptthanh/PHSS_19987.depot b _ o r ptthanh ftp 0 * c
```

i) Logfile của dịch vụ Web:

Tùy thuộc vào Web server sử dụng sẽ có các phương thức và cấu hình ghi logfile của dịch vụ Web khác nhau. Hầu hết các web server thông dụng hiện nay đều hỗ trợ cơ chế ghi log. Ví dụ nội dung logfile của dịch vụ Web sử dụng Web server Netscape như sau:

```
202.167.123.170 - - [03/Aug/2000:10:59:43 +0700] "GET /support/cgi-bin/search.pl HTTP/1.0" 401 223
203.162.46.67 - - [03/Sep/2000:22:50:52 +0700] "GET http://www.geocities.com/ HTTP/1.1" 401 223
203.162.0.85 - - [15/Sep/2000:07:43:17 +0700] "GET /support/cgi-bin/search.pl HTTP/1.0" 401 223
203.162.0.85 - ptthanh [15/Sep/2000:07:43:22 +0700] "GET /support/cgi-bin/search.pl HTTP/1.0" 404 207
203.162.0.85 - - [15/Sep/2000:07:43:17 +0700] "GET /support/cgi-bin/search.pl HTTP/1.0" 401 223
```

I.2.1.2. Một số công cụ hữu ích hỗ trợ phân tích logfile:

Đối với người quản trị, việc phân tích logfile của các dịch vụ là hết sức quan trọng. Một số công cụ trên mạng giúp người quản trị thực hiện công việc này dễ dàng hơn, đó là:

- Tiện ích chklastlog và chkwtmp giúp phân tích các logfile lastlog và WTMP theo yêu cầu người quản trị.

- Tiện ích netlog giúp phân tích các gói tin, gồm 3 thành phần:

+ TCPlogger: log lại tất cả các kết nối TCP trên một subnet

+ UDPlogger: log lại tất cả các kết nối UDP trên một subnet

+ Extract: Xử lý các logfile ghi lại bởi TCPlogger và UDBlogger.

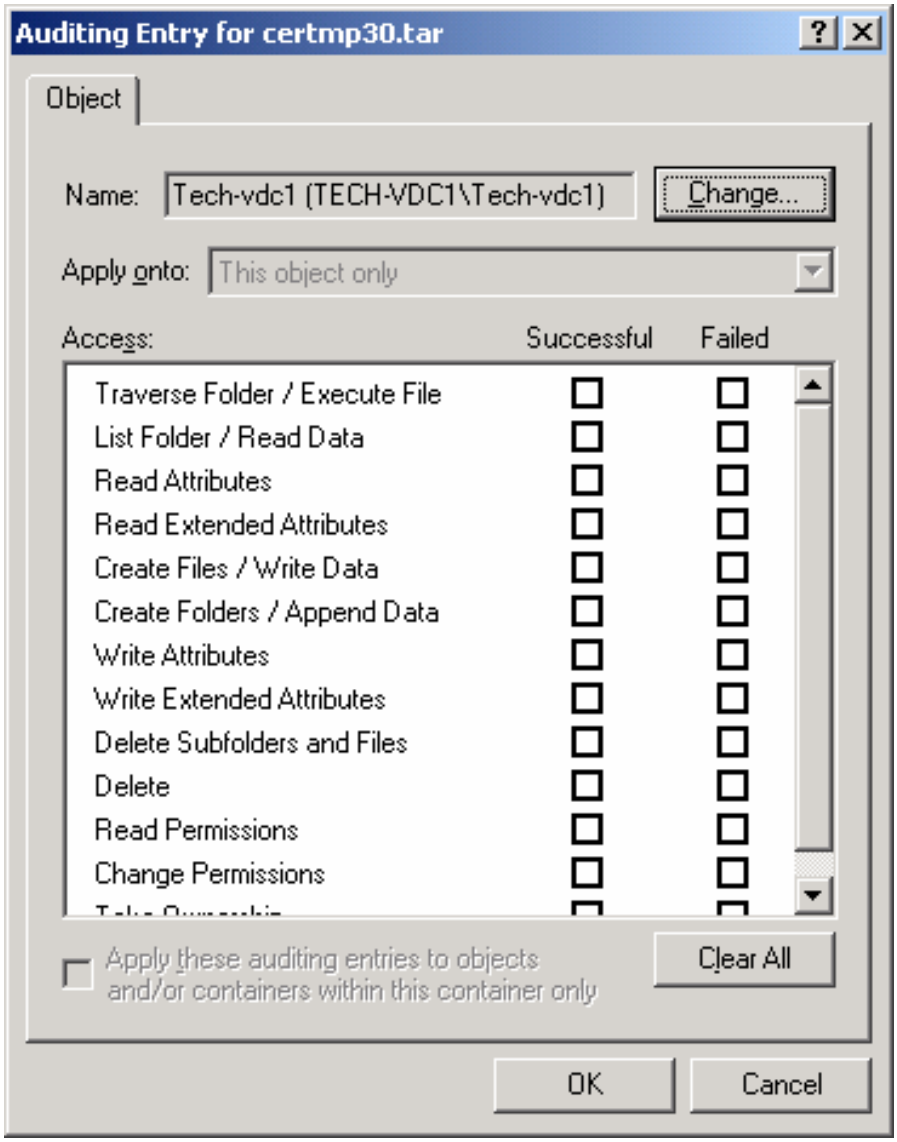
- Tiện ích TCP wrapper: Tiện ích này cho phép người quản trị hệ thống dễ dàng giám sát và lọc các gói tin TCP của các dịch vụ như systat, finger, telnet, rlogin, rsh, talk ...

I.2.1.3. Các công cụ ghi log thường sử dụng trong Windows NT và 2000:

Trong hệ thống Windows NT 4.0 và Windows 2000 hiện nay đều hỗ trợ đầy đủ các cơ chế ghi log với các mức độ khác nhau. Người quản trị hệ thống tùy thuộc vào mức độ an toàn của dịch vụ và các thông tin sử dụng có thể lựa chọn các mức độ ghi log khác nhau. Ngoài ra, trên hệ thống Windows NT còn hỗ trợ các cơ chế ghi logfile trực tiếp vào các database để tạo báo cáo giúp người quản trị phân tích và kiểm tra hệ thống nhanh chóng và thuận tiện. Sử dụng tiện ích event view để xem các thông tin logfile trên hệ thống với các mức độ như Application log; Security log; System log. Các hình dưới đây sẽ minh hoạ một số hoạt động ghi logfile trên hệ thống Windows:

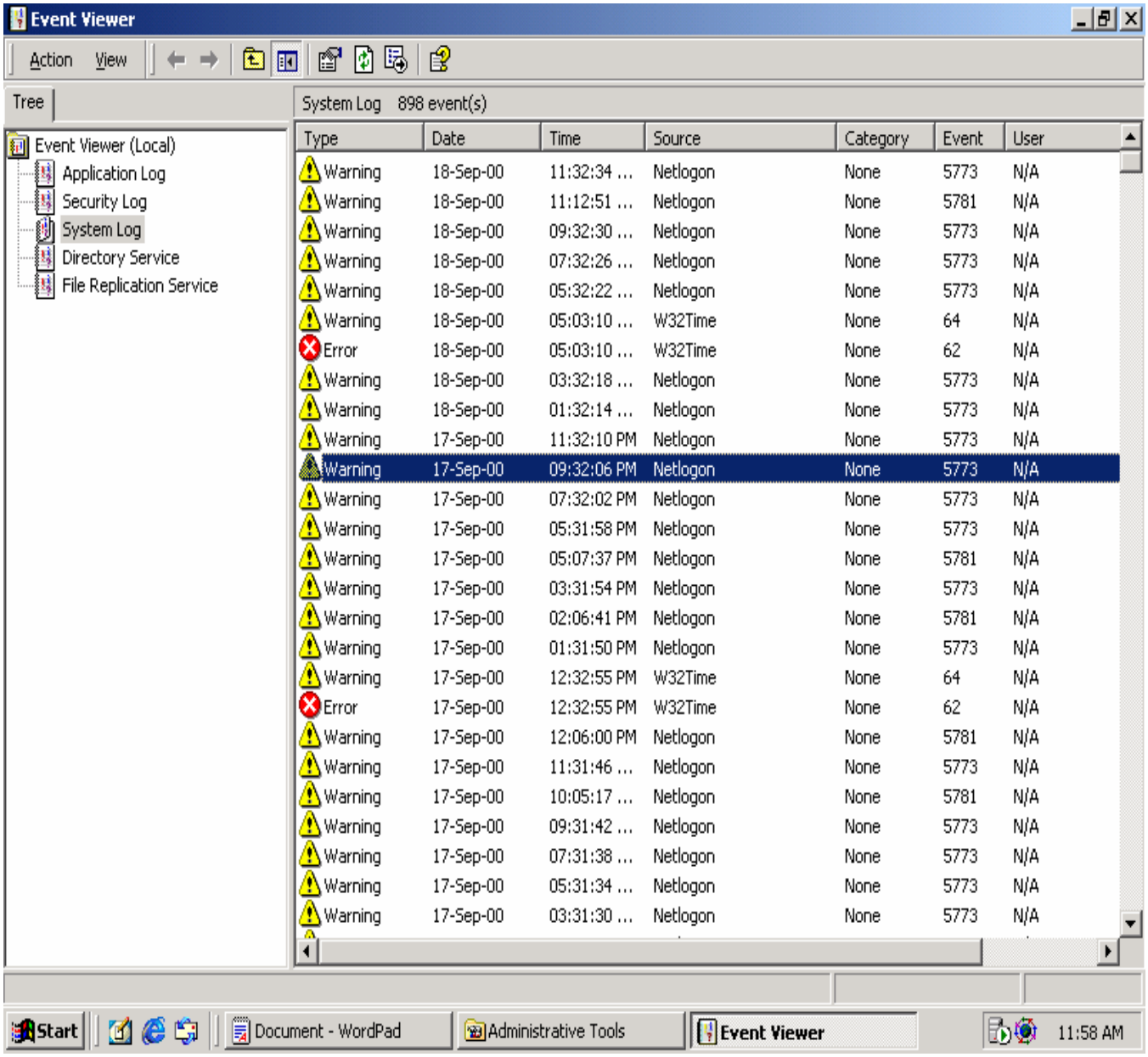
Ví dụ: Để ghi lại hoạt động đọc, viết, truy nhập.... đối với một file/thư mục là thành công hay không thành công người quản trị có thể cấu hình như sau:

Chọn File Manager - User Manager - Security - Auditing. Ví dụ hình sau minh họa các hoạt động có thể được ghi log trong Windows 2000:



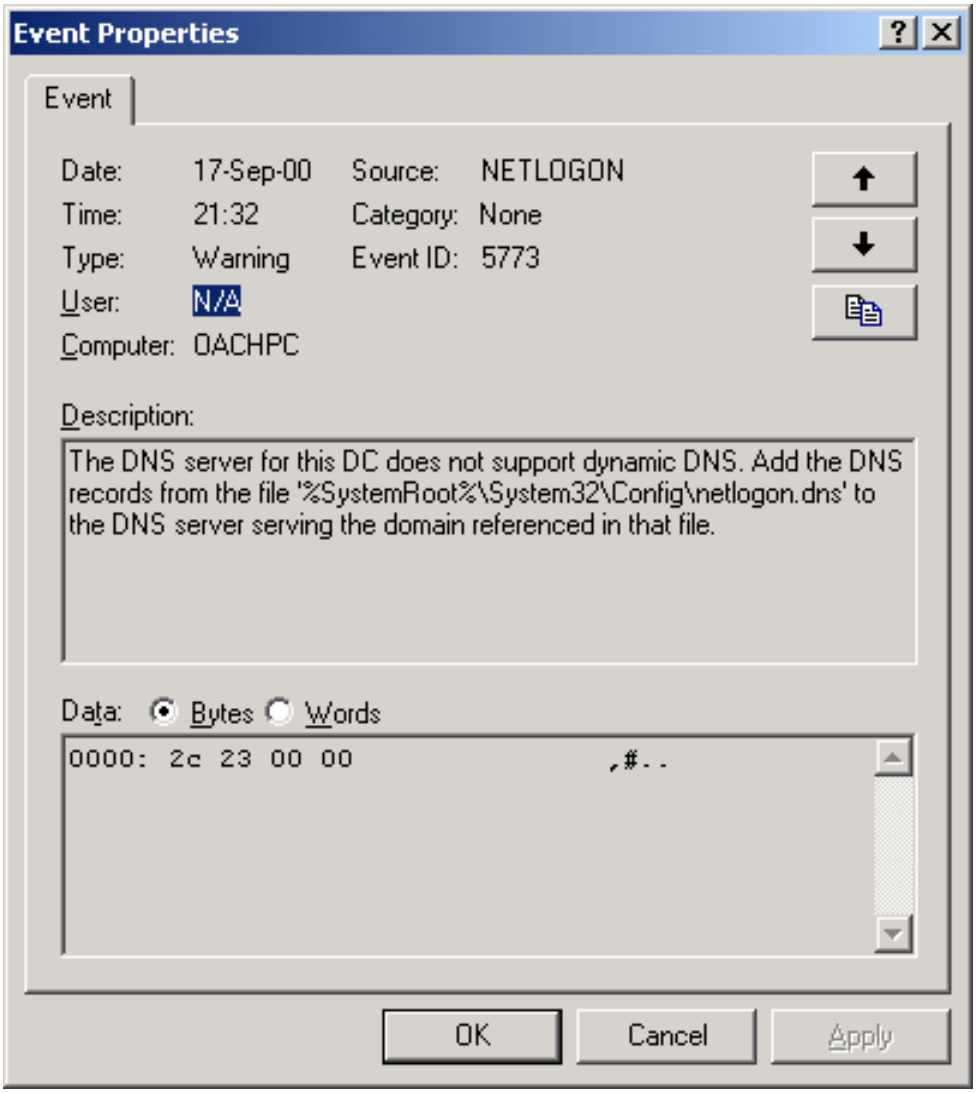
Hình 1.5: Ghi log trong Windows 2000

- Sử dụng tiện ích Event View cho phép xem những thông tin logfile như sau:



Hình 1.6: Công cụ Event View của Windows 2000

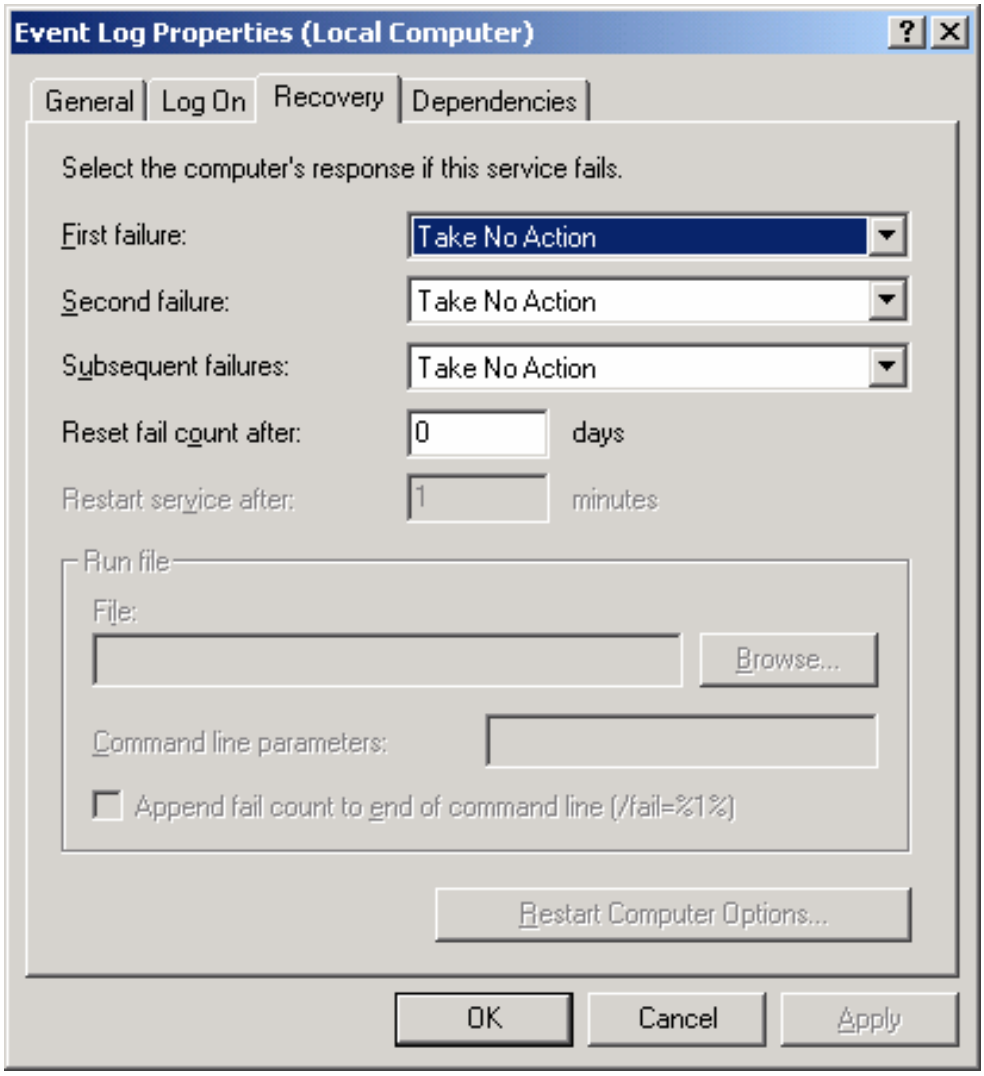
Xem chi tiết nội dung một message:



Hình 1.7: Chi tiết 1 thông báo lỗi trong Windows 2000

Thông báo này cho biết nguyên nhân, thời điểm xảy ra lỗi cũng như nhiều thông tin quan trọng khác.

Có thể cấu hình Event Service để thực hiện một action khi có một thông báo lỗi xảy ra như sau:



Hình 1.8: Cấu hình dịchvụ ghi log trong Windows 2000

Ngoài ra, cũng giống như trên UNIX, trong Windows NT cũng có các công cụ theo dõi logfile của một số dịch vụ thông dụng như FTP, Web. Tùy thuộc vào loại server sử dụng có các phương pháp cấu hình khác nhau.

I.2.2. Thiếp lập chính sách bảo mật hệ thống

Trong các bước xây dựng một chính sách bảo mật đối với một hệ thống, nhiệm vụ đầu tiên của người quản trị là xác định được đúng mục tiêu cần bảo mật. Việc xác định những mục tiêu của chính sách bảo mật giúp người sử dụng biết được trách nhiệm của mình trong việc bảo vệ các tài nguyên thông tin trên mạng, đồng thời giúp các nhà quản trị thiết lập các biện pháp đảm bảo hữu

hiệu trong quá trình trang bị, cấu hình và kiểm soát hoạt động của hệ thống. Những mục tiêu bảo mật bao gồm:

I.2.2.1. Xác định đối tượng cần bảo vệ:

Đây là mục tiêu đầu tiên và quan trọng nhất trong khi thiết lập một chính sách bảo mật. Người quản trị hệ thống cần xác định rõ những đối tượng nào là quan trọng nhất trong hệ thống cần bảo vệ và xác định rõ mức độ ưu tiên đối với những đối tượng đó. Ví dụ các đối tượng cần bảo vệ trên một hệ thống có thể là: các máy chủ dịch vụ, các router, các điểm truy nhập hệ thống, các chương trình ứng dụng, hệ quản trị CSDL, các dịch vụ cung cấp ...

Trong bước này cần xác định rõ phạm vi và ranh giới giữa các thành phần trong hệ thống để khi xảy ra sự cố trên hệ thống có thể cô lập các thành phần này với nhau, dễ dàng dò tìm nguyên nhân và cách khắc phục. Có thể chia các thành phần trên một hệ thống theo các cách sau:

- Phân tách các dịch vụ tùy theo mức độ truy cập và độ tin cậy.

- Phân tách hệ thống theo các thành phần vật lý như các máy chủ (server), router, các máy trạm (workstation)...

- Phân tách theo phạm vi cung cấp của các dịch vụ như: các dịch vụ bên trong mạng (NIS, NFS ...) và các dịch vụ bên ngoài như Web, FTP, Mail ...

I.2.2.2. Xác định nguy cơ đối với hệ thống

Các nguy cơ đối với hệ thống chính là các lỗ hổng bảo mật của các dịch vụ hệ thống đó cung cấp. Việc xác định đúng đắn các nguy cơ này giúp người quản trị có thể tránh được những cuộc tấn công mạng, hoặc có biện pháp bảo vệ đúng đắn. Thông thường, một số nguy cơ này nằm ở các thành phần sau trên hệ thống:

a) Các điểm truy nhập:

Các điểm truy nhập của hệ thống bất kỳ (Access Points) thường đóng vai trò quan trọng đối với mỗi hệ thống vì đây là điểm đầu tiên mà người sử dụng cũng như những kẻ tấn công mạng quan tâm tới. Thông thường các điểm truy nhập thường phục vụ hầu hết người dùng trên mạng, không phụ thuộc vào quyền hạn cũng như dịch vụ mà người sử dụng dùng. Do đó, các điểm truy nhập thường là thành phần có tính bảo mật lỏng lẻo. Mặt khác, đối với nhiều hệ

thống còn cho phép người sử dụng dùng các dịch vụ như Telnet, rlogin để truy nhập vào hệ thống, đây là những dịch vụ có nhiều lỗ hổng bảo mật.

b) Không kiểm soát được cấu hình hệ thống

Không kiểm soát hoặc mất cấu hình hệ thống chiếm một tỷ lệ lớn trong số các lỗ hổng bảo mật. Ngày nay, có một số lượng lớn các phần mềm sử dụng, yêu cầu cấu hình phức tạp và đa dạng hơn, điều này cũng dẫn đến những khó khăn để người quản trị nắm bắt được cấu hình hệ thống. Để khắc phục hiện tượng này, nhiều hãng sản xuất phần mềm đã đưa ra những cấu hình khởi tạo mặc định, trong khi đó những cấu hình này không được xem xét kỹ lưỡng trong một môi trường bảo mật. Do đó, nhiệm vụ của người quản trị là phải nắm được hoạt động của các phần mềm sử dụng, ý nghĩa của các file cấu hình quan trọng, áp dụng các biện pháp bảo vệ cấu hình như sử dụng phương thức mã hóa hashing code (MD5).

c) Những bug phần mềm sử dụng

Những bug phần mềm tạo nên những lỗ hổng của dịch vụ là cơ hội cho các hình thức tấn công khác nhau xâm nhập vào mạng. Do đó, người quản trị phải thường xuyên cập nhật tin tức trên các nhóm tin về bảo mật và từ nhà cung cấp phần mềm để phát hiện những lỗi của phần mềm sử dụng. Khi phát hiện có bug cần thay thế hoặc ngừng sử dụng phần mềm đó chờ nâng cấp lên phiên bản tiếp theo.

d) Những nguy cơ trong nội bộ mạng

Một hệ thống không những chịu tấn công từ ngoài mạng, mà có thể bị tấn công ngay từ bên trong. Có thể là vô tình hoặc cố ý, các hình thức phá hoại bên trong mạng vẫn thường xảy ra trên một số hệ thống lớn. Chủ yếu với hình thức tấn công ở bên trong mạng là kẻ tấn công có thể tiếp cận về mặt vật lý đối với các thiết bị trên hệ thống, đạt được quyền truy nhập bất hợp pháp tại ngay hệ thống đó. Ví dụ nhiều trạm làm việc có thể chiếm được quyền sử dụng nếu kẻ tấn công ngồi ngay tại các trạm làm việc đó.

I.2.2.3. Xác định phương án thực thi chính sách bảo mật

Sau khi thiết lập được một chính sách bảo mật, một hoạt động tiếp theo là lựa chọn các phương án thực thi một chính sách bảo mật. Một chính sách

bảo mật là hoàn hảo khi nó có tình thực thi cao. Để đánh giá tính thực thi này, có một số tiêu chí để lựa chọn đó là:

- Tính đúng đắn
- Tính thân thiện
- Tính hiệu quả

I.2.2.4. Thiết lập các qui tắc/thủ tục

a) Các thủ tục đối với hoạt động truy nhập bất hợp pháp

Sử dụng một vài công cụ có thể phát hiện ra các hành động truy nhập bất hợp pháp vào một hệ thống. Các công cụ này có thể đi kèm theo hệ điều hành, hoặc từ các hãng sản xuất phần mềm thứ ba. Đây là biện pháp phổ biến nhất để theo dõi các hoạt động hệ thống.

- Các công cụ logging: hầu hết các hệ điều hành đều hỗ trợ một số lượng lớn các công cụ ghi log với nhiều thông tin bổ ích. Để phát hiện những hoạt động truy nhập bất hợp pháp, một số qui tắc khi phân tích logfile như sau:

+ So sánh các hoạt động trong logfile với các log trong quá khứ. Đối với các hoạt động thông thường, các thông tin trong logfile thường có chu kỳ giống nhau như thời điểm người sử dụng login hoặc log out, thời gian sử dụng các dịch vụ trên hệ thống...

+ Nhiều hệ thống sử dụng các thông tin trong logfile để tạo hóa đơn cho khách hàng. Có thể dựa vào các thông tin trong hóa đơn thanh toán để xem xét các truy nhập bất hợp pháp nếu thấy trong hóa đơn đó có những điểm bất thường như thời điểm truy nhập, số điện thoại lạ ...

+ Dựa vào các tiện ích như syslog để xem xét, đặc biệt là các thông báo lỗi login không hợp lệ (bad login) trong nhiều lần.

+ Dựa vào các tiện ích kèm theo hệ điều hành để theo dõi các tiến trình đang hoạt động trên hệ thống; để phát hiện những tiến trình lạ, hoặc những chương trình khởi tạo không hợp lệ ...

- Sử dụng các công cụ giám sát khác: Ví dụ sử dụng các tiện ích về mạng để theo dõi các lưu lượng, tài nguyên trên mạng để phát hiện những điểm nghi ngờ.

b) Các thủ tục bảo vệ hệ thống

- Thủ tục quản lý tài khoản người sử dụng
- Thủ tục quản lý mật khẩu
- Thủ tục quản lý cấu hình hệ thống
- Thủ tục sao lưu và khôi phục dữ liệu
- Thủ tục báo cáo sự cố

I.2.2.5. Kiểm tra, đánh giá và hoàn thiện chính sách bảo mật

Một hệ thống luôn có những biến động về cấu hình, các dịch vụ sử dụng, và ngay cả nền tảng hệ điều hành sử dụng, các thiết bị phần cứng .... do vậy người thiết lập các chính sách bảo mật mà cụ thể là các nhà quản trị hệ thống luôn luôn phải rà sóat, kiểm tra lại chính sách bảo mật đảm bảo luôn phù hợp với thực tế. Mặt khác kiểm tra và đánh giá chính sách bảo mật còn giúp cho các nhà quản lý có kế hoạch xây dựng mạng lưới hiệu quả hơn.

a) Kiểm tra, đánh giá

Công việc này được thực hiện thường xuyên và liên tục. Kết quả của một chính sách bảo mật thể hiện rõ nét nhất trong chất lượng dịch vụ mà hệ thống đó cung cấp. Dựa vào đó có thể kiểm tra, đánh giá được chính sách bảo mật đó là hợp lý hay chưa. Ví dụ, một nhà cung cấp dịch vụ Internet có thể kiểm tra được chính sách bảo mật của mình dựa vào khả năng phản ứng của hệ thống khi bị tấn công từ bên ngoài như các hành động spam mail, DoS, truy nhập hệ thống trái phép ...

Hoạt động đánh giá một chính sách bảo mật có thể dựa vào một số tiêu chí sau:

- Tính thực thi.
- Khả năng phát hiện và ngăn ngừa các hoạt động phá hoại.
- Các công cụ hữu hiệu để hạn chế các hoạt động phá hoại hệ thống.

b) Hoàn thiện chính sách bảo mật:

Từ các hoạt động kiểm tra, đánh giá nêu trên, các nhà quản trị hệ thống có thể rút ra được những kinh nghiệm để có thể cải thiện chính sách bảo mật

hữu hiệu hơn. Cải thiện chính sách có thể là những hành động nhằm đơn giản công việc người sử dụng, giảm nhẹ độ phức tạp trên hệ thống ...

Những hoạt động cải thiện chính sách bảo mật có thể diễn ra trong suốt thời gian tồn tại của hệ thống đó. Nó gắn liền với các công việc quản trị và duy trì hệ thống. Đây cũng chính là một yêu cầu trong khi xây dựng một chính sách bảo mật, cần phải luôn luôn mềm dẻo, có những thay đổi phù hợp tùy theo điều kiện thực tế.

II. Tổng quan về hệ thống firewall

II.1. Giới thiệu về Firewall

II.1.1. Khái niệm Firewall

Firewall là thiết bị nhằm ngăn chặn sự truy nhập không hợp lệ từ mạng ngoài vào mạng trong. Hệ thống firewall thường bao gồm cả phần cứng và phần mềm. Firewall thường được dùng theo phương thức ngăn chặn hay tạo các luật đối với các địa chỉ khác nhau.

II.1.2. Các chức năng cơ bản của Firewall

Chức năng chính của Firewall là kiểm soát luồng thông tin giữa mạng cần bảo vệ (Trusted Network) và Internet thông qua các chính sách truy nhập đã đợc thiết lập.

- Cho phép hoặc cấm các dịch vụ truy nhập từ trong ra ngoài và từ ngoài vào trong.

- Kiểm soát địa chỉ truy nhập, và dịch vụ sử dụng.

- Kiểm soát khả năng truy cập người sử dụng giữa 2 mạng.

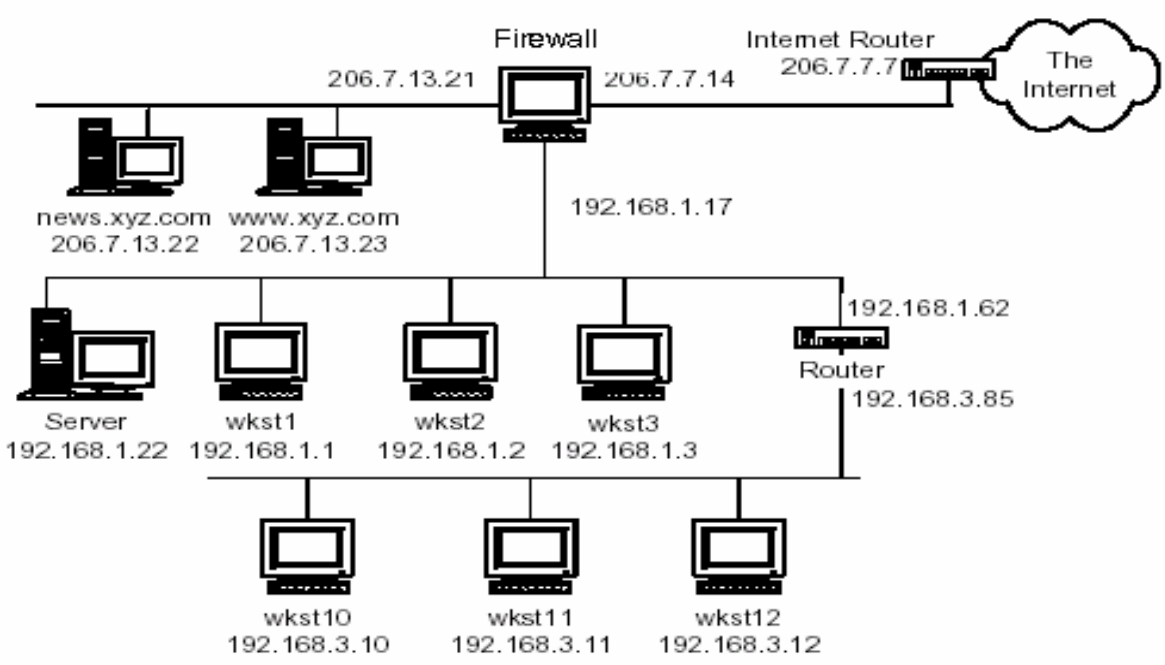
- Kiểm soát nội dung thông tin truyền tải giữa 2 mạng.

- Ngăn ngừa khả năng tấn công từ các mạng ngoài.

Xây dựng firewalls là một biện pháp khá hữu hiệu, nó cho phép bảo vệ và kiểm soát hầu hết các dịch vụ do đó được áp dụng phổ biến nhất trong các biện pháp bảo vệ mạng. Thông thường, một hệ thống firewall là một cổng (gateway) giữa mạng nội bộ giao tiếp với mạng bên ngoài và ngược lại

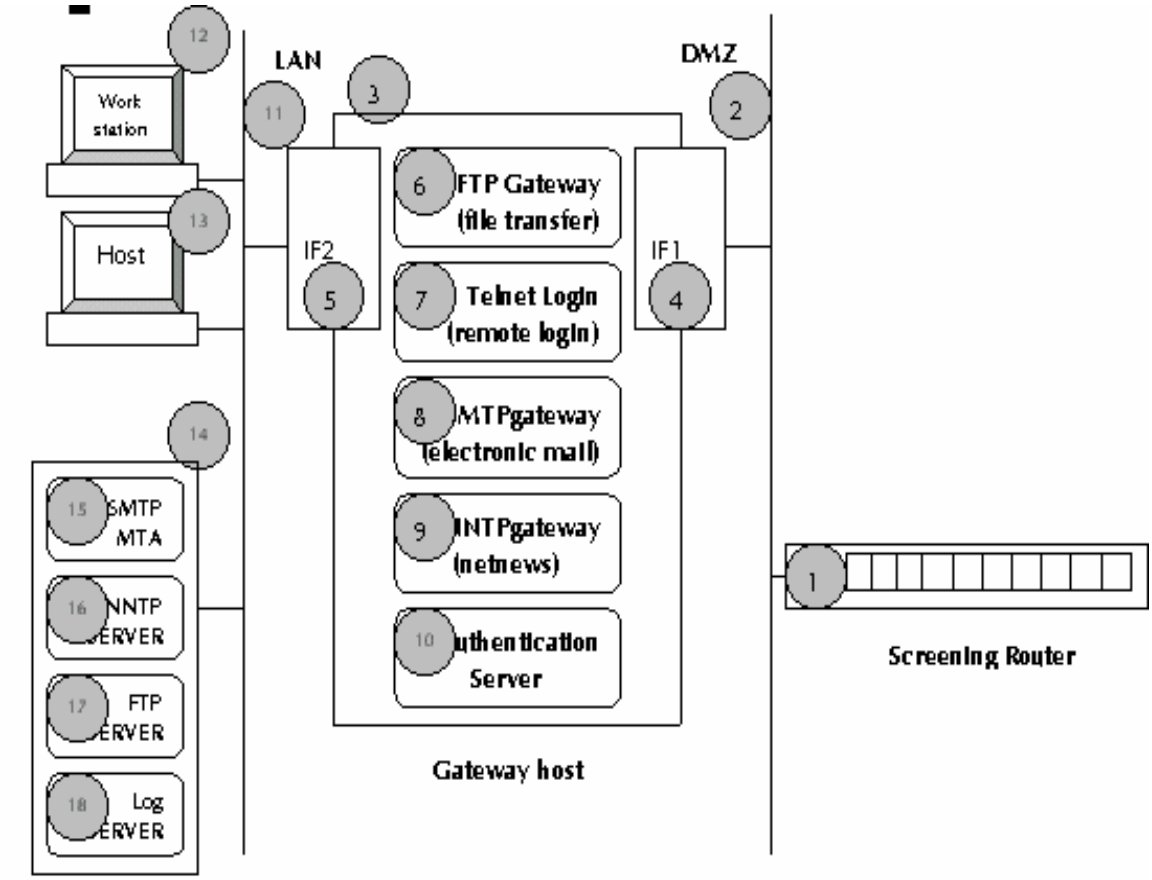
II.1.3. Mô hình mạng sử dụng Firewall

Kiến trúc của hệ thống có firewall như sau:



Hình 2.1: Kiến trúc hệ thống có firewall

Nhìn chung, mỗi hệ thống firewall đều có các thành phần chung như sau:



Hình 2.2: Các thành phần của hệ thống firewall

Firewall có thể bao gồm phần cứng hoặc phần mềm nhưng thường là cả hai. Về mặt phần cứng thì firewall có chức năng gần giống một router, nó cho phép hiển thị các địa chỉ IP đang kết nối qua nó. Điều này cho phép bạn xác định được các địa chỉ nào được phép và các địa chỉ IP nào không được phép kết nối.

Tất cả các firewall đều có chung một thuộc tính là cho phép phân biệt đối xử hay khả năng từ chối truy nhập dựa trên các địa chỉ nguồn.

Theo hình trên các thành phần của một hệ thống firewall bao gồm:

- Screening router: Là chặng kiểm soát đầu tiên cho LAN.

- DMZ: Khu "phi quân sự", là vùng có nguy cơ bị tấn công từ Internet.

- Gateway: là cổng ra vào giữa mạng LAN và DMZ, kiểm soát mọi liên lạc, thực thi các cơ chế bảo mật.

- IF1: Interface 1: Là card giao tiếp với vùng DMZ.

- IF2: Interface 2: Là card giao tiếp với vùng mạng LAN.

- FTP gateway: Kiểm soát truy cập FTP giữa LAN và vùng DMZ. Các truy cập ftp từ mạng LAN ra Internet là tự do. Các truy cập FTP vào LAN đòi hỏi xác thực thông qua Authentication Server.

- Telnet Gateway: Kiểm soát truy cập telnet giữa mạng LAN và Internet. Giống như FTP, người dùng có thể telnet ra ngoài tự do, các telnet từ ngoài vào yêu cầu phải xác thực qua Authentication Server

- Authentication Server: được sử dụng bởi các cổng giao tiếp, nhận diện các yêu cầu kết nối, dùng các kỹ thuật xác thực mạnh như one-time password/token (mật khẩu sử dụng một lần). Các máy chủ dịch vụ trong mạng LAN được bảo vệ an toàn, không có kết nối trực tiếp với Internet, tất cả các thông tin trao đổi đều được kiểm soát qua gateway.

II.1.4. Phân loại Firewall

Có khá nhiều loại firewall, mỗi loại có những ưu và nhược điểm riêng. Tuy nhiên để thuận tiện cho việc nghiên cứu người ta chia hệ thống làm 2 loại chính:

- Packet filtering: là hệ thống firewall cho phép chuyển thông tin giữa hệ thống trong và ngoài mạng có kiểm soát.

- Application-proxy firewall: là hệ thống firewall thực hiện các kết nối thay cho các kết nối trực tiếp từ máy khách yêu cầu.

II.1.4.1. Packet Filtering:

Kiểu firewall chung nhất là kiểu dựa trên mức mạng của mô hình OSI. Firewall mức mạng thường hoạt động theo nguyên tắc router hay còn được gọi là router, có nghĩa là tạo ra các luật cho phép quyền truy nhập mạng dựa trên mức mạng. Mô hình này hoạt động theo nguyên tắc lọc gói tin (packet filtering).

Ở kiểu hoạt động này các gói tin đều được kiểm tra địa chỉ nguồn nơi chúng xuất phát. Sau khi địa chỉ IP nguồn được xác định thì nó được kiểm tra với các luật đã được đặt ra trên router. Ví dụ người quản trị firewall quyết định rằng không cho phép bất kỳ một gói tin nào xuất phát từ mạng microsoft.com

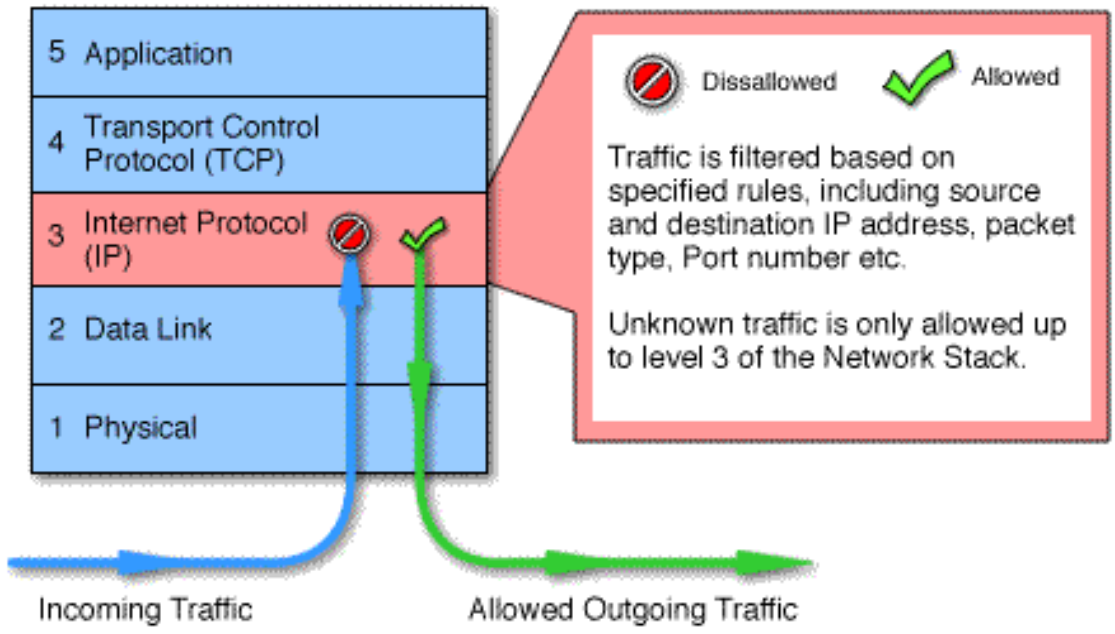
được kết nối với mạng trong thì các gói tin xuất phát từ mạng này sẽ không bao giờ đến được mạng trong.

Các firewall hoạt động ở lớp mạng (tương tự như một router) thường cho phép tốc độ xử lý nhanh bởi nó chỉ kiểm tra địa chỉ IP nguồn mà không có một lệnh thực sự nào trên router, nó không cần một khoảng thời gian nào để xác định xem là địa chỉ sai hay bị cấm. Nhưng điều này bị trả giá bởi tính tin cậy của nó. Kiểu firewall này sử dụng địa chỉ IP nguồn làm chỉ thị, điều này tạo ra một lỗ hổng là nếu một gói tin mang địa chỉ nguồn là địa chỉ giả thì như vậy nó sẽ có được một số mức truy nhập vào mạng trong của bạn.

Tuy nhiên có nhiều biện pháp kỹ thuật có thể được áp dụng cho việc lọc gói tin nhằm khắc phục yếu điểm này. Ví dụ như đối với các công nghệ packet filtering phức tạp thì không chỉ có trường địa chỉ IP được kiểm tra bởi router mà còn có các trường khác nữa được kiểm tra với các luật được tạo ra trên firewall, các thông tin khác này có thể là thời gian truy nhập, giao thức sử dụng, port ...

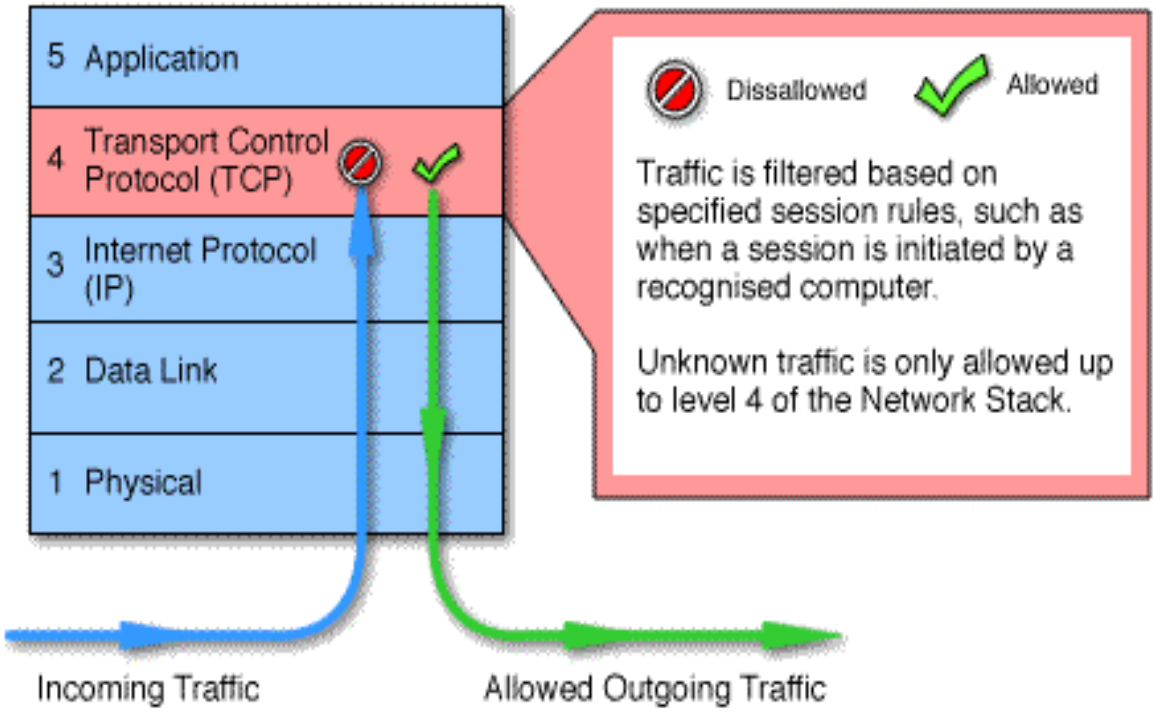
Firewall kiểu Packet Filtering có thể được phân thành 2 loại:

a) Packet filtering firewall: hoạt động tại lớp mạng của mô hình OSI hay lớp IP trong mô hình giao thức TCP/IP.



Hình 2.3: Packet filtering firewall

b) Circuit level gateway: hoạt động tại lớp phiên (session) của mô hình OSI hay lớp TCP trong mô hình giao thức TCP/IP.



Hình 2.4: Circuit level gateway

II.1.4.2. Application-proxy firewall

Kiểu firewall này hoạt động dựa trên phần mềm. Khi một kết nối từ một người dùng nào đó đến mạng sử dụng firewall kiểu này thì kết nối đó sẽ bị chặn lại, sau đó firewall sẽ kiểm tra các trường có liên quan của gói tin yêu cầu kết nối. Nếu việc kiểm tra thành công, có nghĩa là các trường thông tin đáp ứng được các luật đã đặt ra trên firewall thì firewall sẽ tạo một cái cầu kết nối giữa hai node với nhau.

Ưu điểm của kiểu firewall loại này là không có chức năng chuyển tiếp các gói tin IP, hơn nữa ta có thể điều khiển một cách chi tiết hơn các kết nối thông qua firewall. Đồng thời nó còn đưa ra nhiều công cụ cho phép ghi lại các quá trình kết nối. Tất nhiên điều này phải trả giá bởi tốc độ xử lý, bởi vì tất cả các kết nối cũng như các gói tin chuyển qua firewall đều được kiểm tra kỹ

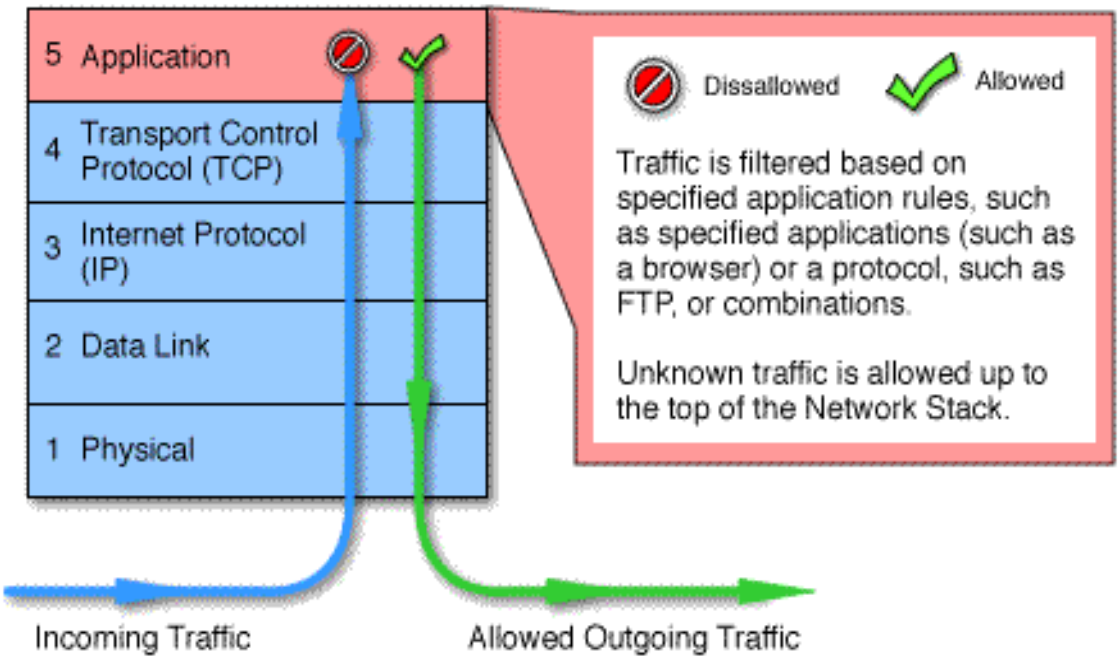
lưỡng với các luật trên firewall và rồi nếu được chấp nhận sẽ được chuyển tiếp tới node đích.

Sự chuyển tiếp các gói tin IP xảy ra khi một máy chủ nhận được một yêu cầu từ mạng ngoài rồi chuyển chúng vào mạng trong. Điều này tạo ra một lỗ hổng cho các kẻ phá hoại (hacker) xâm nhập từ mạng ngoài vào mạng trong.

Nhược điểm của kiểu firewall hoạt động dựa trên ứng dụng là phải tạo cho mỗi dịch vụ trên mạng một trình ứng dụng uỷ quyền (proxy) trên firewall ví dụ như phải tạo một trình ftp proxy dịch vụ ftp, tạo trình http proxy cho dịch vụ http... Như vậy ta có thể thấy rằng trong kiểu giao thức client-server như dịch vụ telnet làm ví dụ thì cần phải thực hiện hai bước để cho hai máy ngoài mạng và trong mạng có thể kết nối được với nhau. Khi sử dụng firewall kiểu này các máy client (máy yêu cầu dịch vụ) có thể bị thay đổi. Ví dụ như đối với dịch vụ telnet thì các máy client có thể thực hiện theo hai phương thức: một là bạn telnet vào firewall trước sau đó mới thực hiện việc telnet vào máy ở mạng khác; cách thứ hai là bạn có thể telnet thẳng tới đích tuỳ theo các luật trên firewall có cho phép hay không mà việc telnet của bạn sẽ được thực hiện. Lúc này firewall là hoàn toàn trong suốt, nó đóng vai trò như một cầu nối tới đích của bạn.

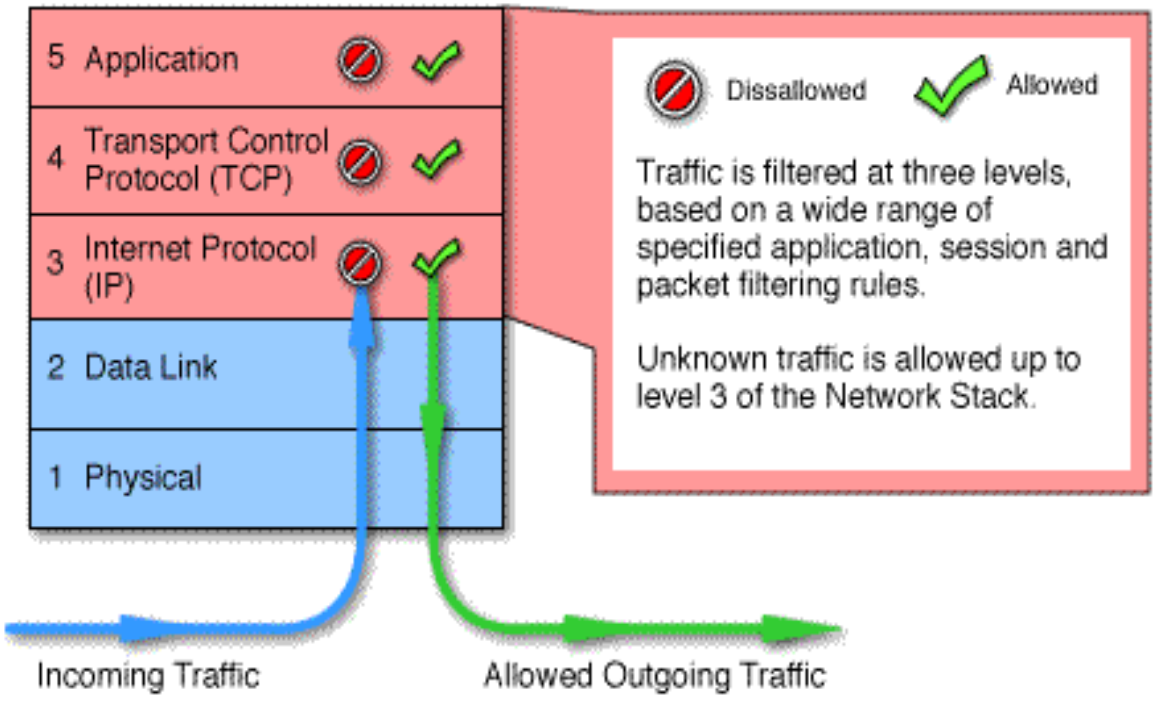
Firewall kiểu Application-proxy có thể được phân thành 2 loại:

a) Application level gateway: tính năng tương tự như loại circuit-level gateway nhưng lại hoạt động ở lớp ứng dụng trong mô hình giao thức TCP/IP.



Hình 2.5: Application level gateway

b) Stateful multilayer inspection firewall: đây là loại kết hợp được các tính năng của các loại firewall trên: lọc các gói tại lớp mạng và kiểm tra nội dung các gói tại lớp ứng dụng. Firewall loại này cho phép các kết nối trực tiếp giữa các client và các host nên giảm được các lỗi xảy ra do tính chất "không trong suốt" của firewall kiểu Application gateway. Stateful multilayer inspection firewall cung cấp các tính năng bảo mật cao và lại trong suốt đối với các end users.



Hình 2.6: Stateful multilayer inspection firewall

II.2. Một số phần mềm Firewall thông dụng

II.2.1. Packet filtering:

Kiểu lọc gói tin này có thể được thực hiện mà không cần tạo một firewall hoàn chỉnh, có rất nhiều các công cụ trợ giúp cho việc lọc gói tin trên Internet (kể cả phải mua hay được miễn phí). Sau đây ta có thể liệt kê một số tiện ích như vậy

II.2.1.1. TCP_Wrappers

TCP_Wrappers là một chương trình được viết bởi Wietse Venema. Chương trình hoạt động bằng cách thay thế các chương trình thường trú của hệ thống và ghi lại tất cả các yêu cầu kết nối, thời gian yêu cầu, và địa chỉ nguồn. Chương trình này cũng có khả năng ngăn chặn các địa chỉ IP hay các mạng không được phép kết nối.

II.2.1.2. NetGate

NetGate được đưa ra bởi Smallwork là một hệ thống dựa trên các luật về lọc gói tin. Nó được viết ra để sử dụng trên các hệ thống Sun Sparc OS 4.1.x. Tương tự như các kiểu packet filtering khác, NetGate kiểm tra tất cả các gói tin nó nhận được và so sánh với các luật đã được tạo ra.

II.2.1.3. Internet Packet Filter

Phần mềm này hoàn toàn miễn phí, được viết bởi Darren Reed. Đây là một chương trình khá tiện lợi, nó có khả năng ngăn chặn được việc tấn công bằng địa chỉ IP giả. Một số ưu điểm của chương trình là nó không chỉ có khả năng huỷ bỏ các gói tin TCP không đúng hoặc chưa hoàn thiện mà còn không gửi lại bản tin ICMP lỗi. Chương trình này cho phép bạn có thể kiểm tra thử các luật bạn ra trước khi sử dụng chúng.

II.2.2. Application-proxy firewall

II.2.2.1. TIS FWTK

TIS FWTK (Trusted information Systems Firewall Tool Kit) là một phần mềm đầu tiên đầy đủ tính năng của firewall và đặc trưng cho kiểu firewall hoạt động theo phương thức ứng dụng. Những phiên bản đầu tiên của phần mềm này là miễn phí và bao gồm nhiều thành phần riêng rẽ. Mỗi thành phần phục vụ cho một kiểu dịch vụ trên mạng. Các thành phần chủ yếu bao gồm: Telnet, FTP, rlogin, sendmail và http.

Phần mềm này là một hệ thống toàn diện, tuy nhiên nó không có khả năng bảo vệ mạng ngay sau khi cài đặt vì việc cài đặt và cấu hình không phải là dễ dàng. Khi cấu hình phần mềm này bạn phải thực sự hiểu mình đang làm gì bởi có thể với các luật bạn tạo ra thì mạng của bạn không thể được kết nối với bất kỳ mạng nào khác thậm chí ngay cả những mạng quen thuộc. Điểm đặc trưng nhất của phần mềm này là nó có sẵn nhiều tiện ích giúp bạn điều khiển được truy nhập đối với toàn mạng, một phần mạng hay thậm chí chỉ riêng một địa chỉ.

II.2.2.2. Raptor

Raptor là phần mềm firewall cung cấp đầy đủ các tính năng của một firewall chuyên nghiệp với hai giao diện quản lý, một trên hệ đều hành Unix (RCU) và một trên hệ điều hành Windows (RMC). Raptor có thể được cấu hình để bảo vệ mạng theo bốn phương thức: Standard Proxies, Generic Service

Passer, Virtual Private Network tunnels và Raptor Mobile. Tuy việc cấu hình cho Raptor khá phức tạp với việc tạo các route, định nghĩa các entity, user và group, thiết lập các authorization rule ... nhưng bù lại ta có thể sử dụng được rất nhiều tính năng ưu việt do Raptor cung cấp đề tuỳ biến các mức bảo vệ đối với mạng của mình.

II.3. Thực hành cài đặt và cấu hình firewall Check Point v4.0 for Windows

II.3.1. Yêu cầu phần cứng:

- Cấu hình tối thiểu đối với máy cài GUI Client

Hệ điều hành	Windows 95, Windows NT, X/Motif
Dung lượng đĩa trống	20 Mbytes
Bộ nhớ	16 Mbytes
Card mạng	Các loại card được hệ điều hành hỗ trợ
Thiết bị khác	CD-ROM

- Cấu hình tối thiểu đối với máy cài Management Server

Hệ điều hành	Windows NT (Intel x86 và Pentium)
Dung lượng đĩa trống	20 Mbytes
Bộ nhớ	tối thiểu 16MB, nên dùng 24MB
Card mạng	Các loại card được hệ điều hành hỗ trợ
Thiết bị khác	CD-ROM

- Cấu hình tối thiểu đối với máy cài Modul Firewall

Hệ điều hành	Windows NT (Intel x86 và Pentium)
Dung lượng đĩa trống	20 Mbytes
Bộ nhớ	16 Mbytes
Card mạng	Tối thiểu phải có 3 card mạng thuộc các loại card được hệ điều hành hỗ trợ.
Thiết bị khác	CD-ROM

II.3.2. Các bước chuẩn bị trước khi cài đặt:

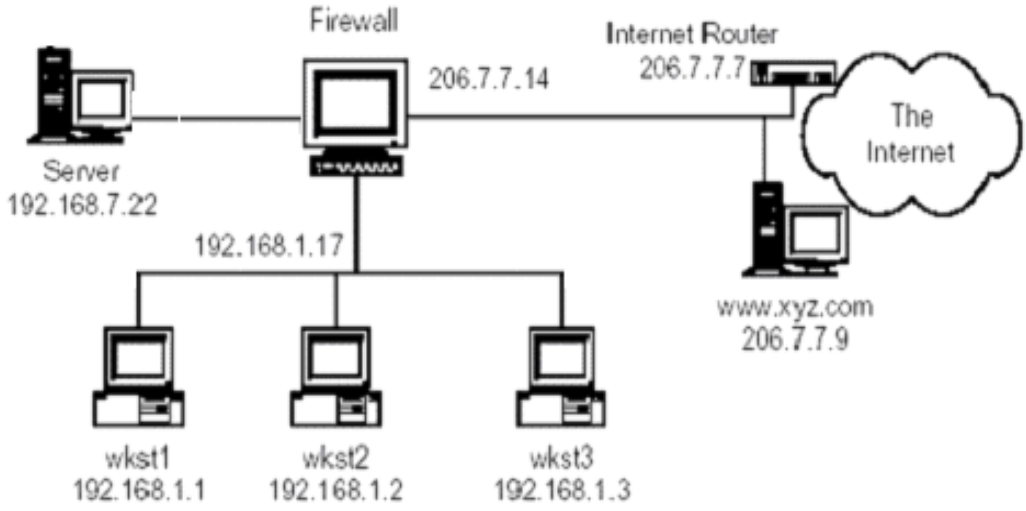
- Thắt chặt an ninh cho máy chủ cài firewall và các module của firewall như GUI Client và Management Server (tắt các dịch vụ không cần thiết, update các patch sửa lỗi của hệ điều hành ...).

- Kiểm tra các kết nối mạng trên các giao diện mạng, đảm bảo từ máy chủ cài Module Firewall có thể ping được các IP trên các giao diện mạng (sử dụng lệnh ifconfig , ping ...).

- Kiểm tra bảng Routing (sử dụng lệnh netstat -rn ...).

- Kiểm tra dịch vụ DNS (sử dụng lệnh nslookup).

- Lập sơ đồ mạng thử nghiệm, đối với máy chủ có 3 giao diện mạng có thể lập sơ đồ như sau:



Hình 2.7: Sơ đồ mạng thử nghiệm đối với máy chủ có 3 giao diện mạng

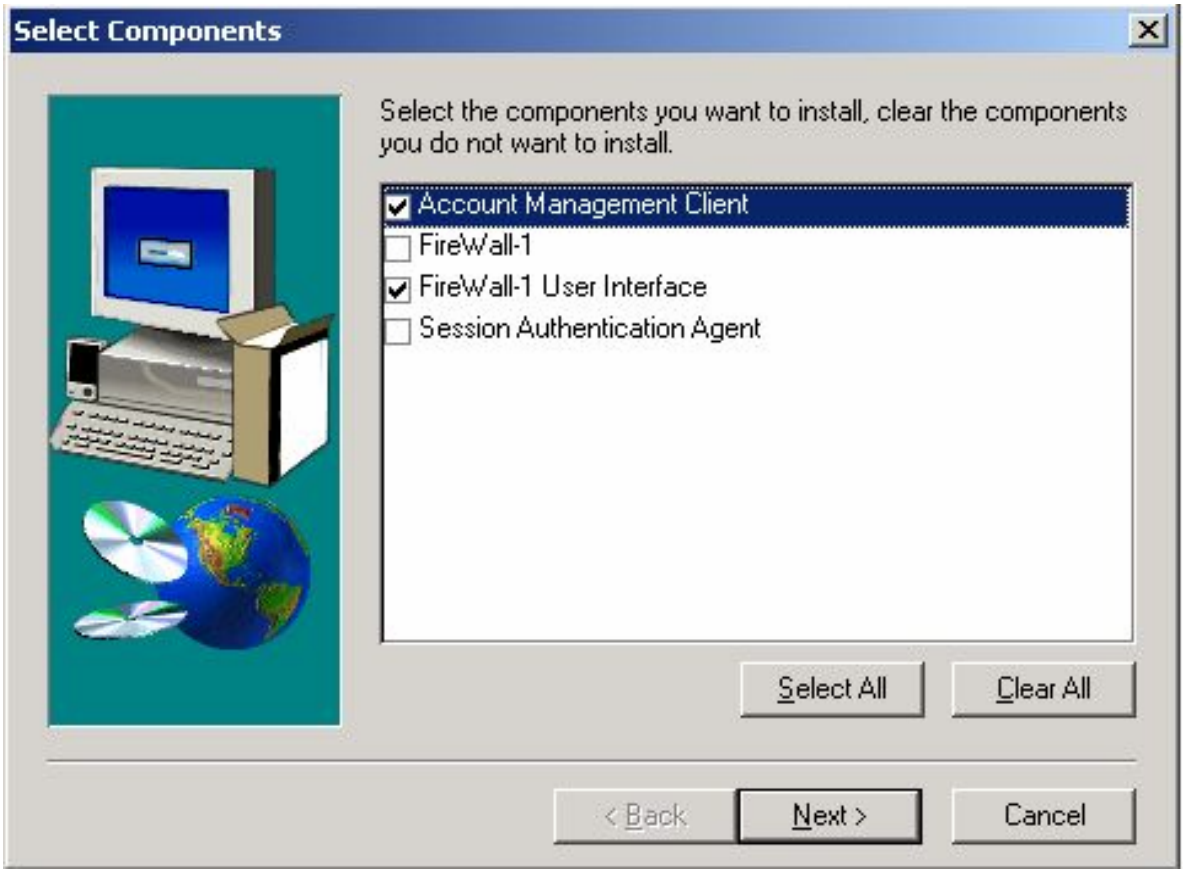
II.3.3. Tiến hành cài đặt:

Login dưới quyền Administrator và cài đặt hệ thống Firewall Checkpoint trên các máy theo trình tự sau:

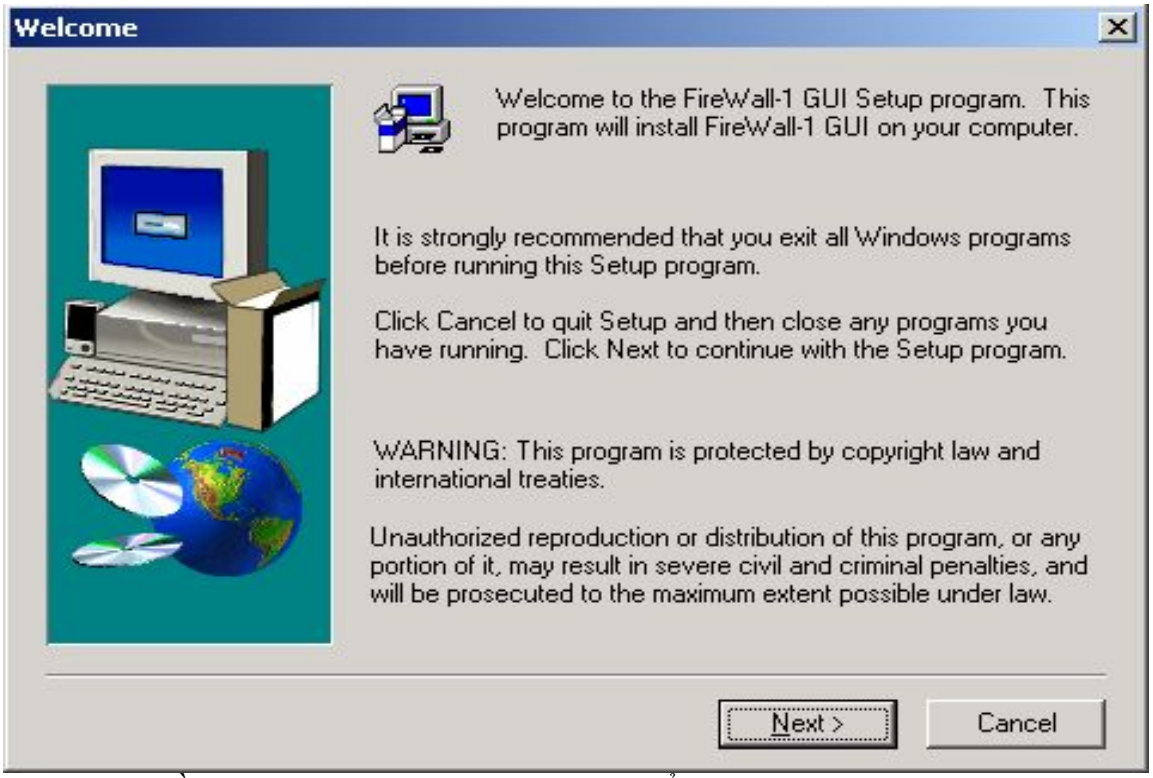
- Cài đặt GUI Client và Management Server.
- Cài đặt Module Firewall.

II.3.3.1. Cài đặt GUI Client và Management Server

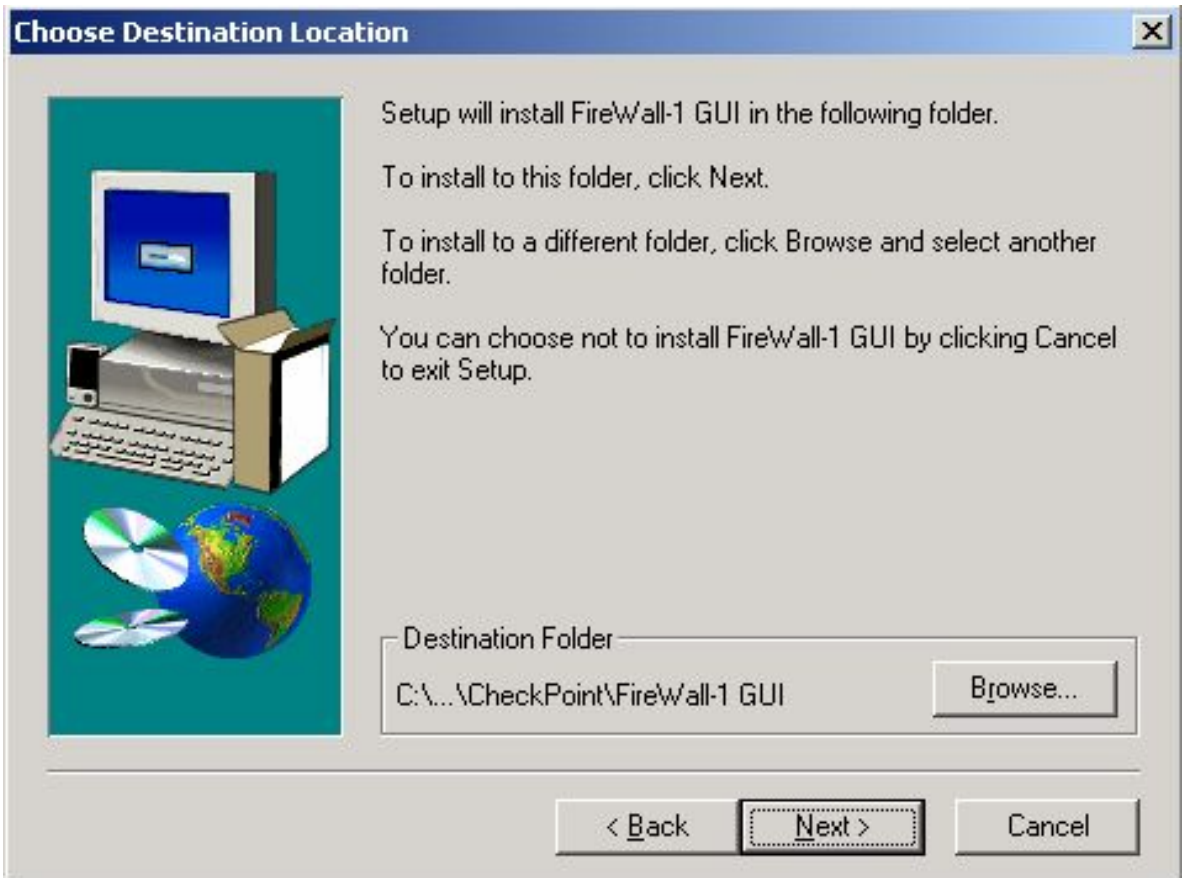
Đưa đĩa CD Checkpoint và chạy lệnh setup trong thư mục Windows, chọn Account Management Client và FireWall-1 User Interface trong cửa sổ Select Components:



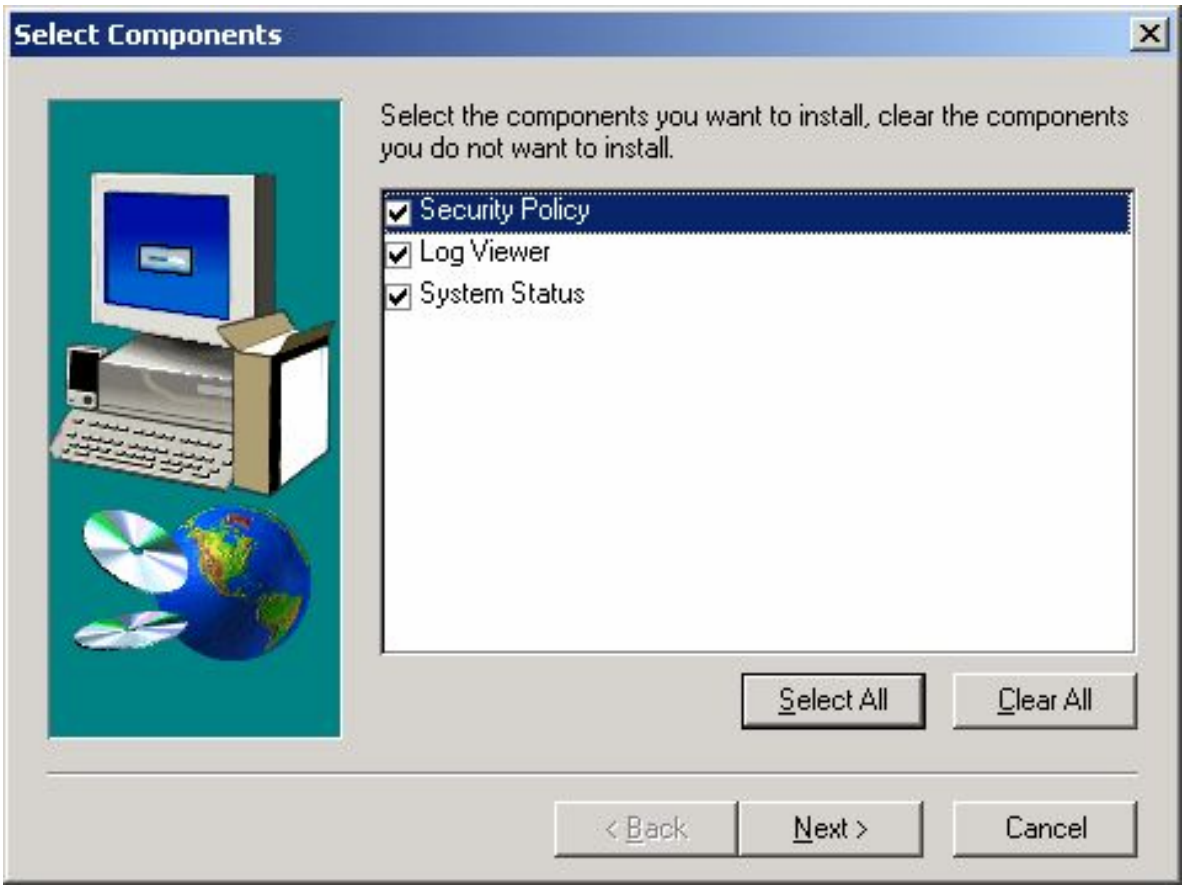
Chọn Next, màn hình sẽ hiện ra như sau:



Chọn Next rồi chọn thư mục cài đặt trong cửa sổ Choose Destination Location:



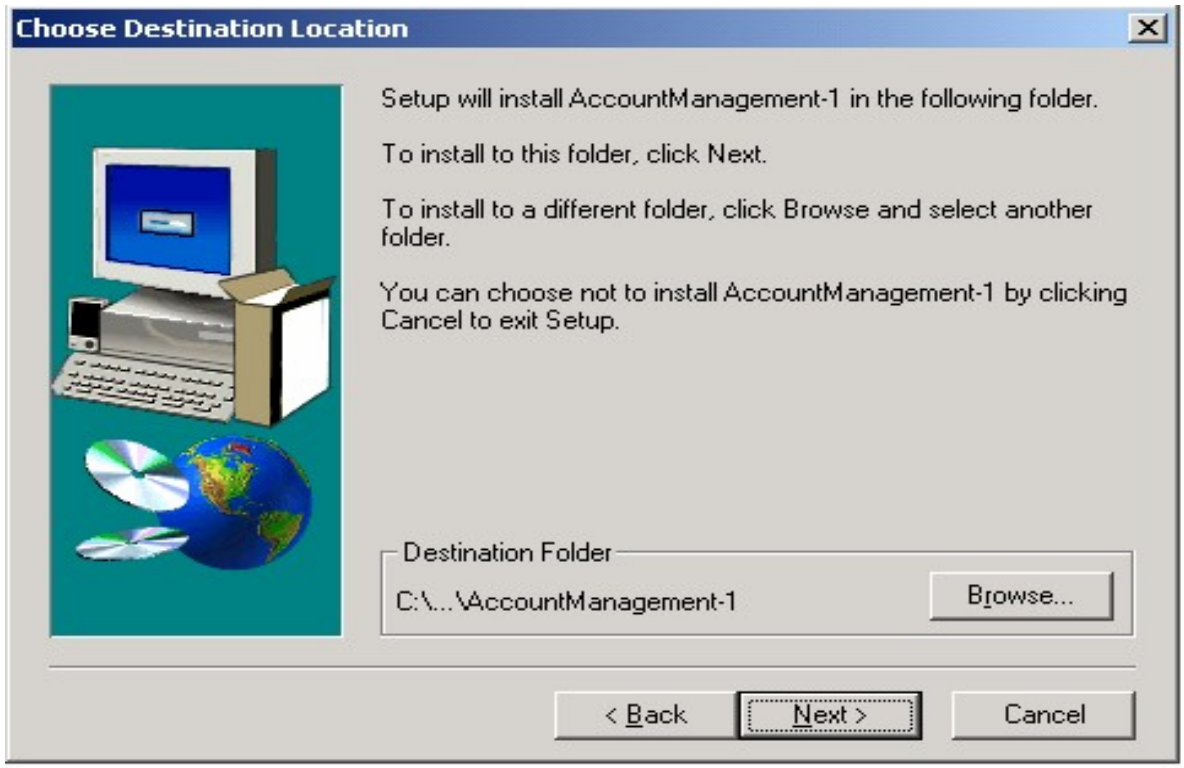
Chọn Next rồi chọn các thành phần trong cửa sổ Select Components:



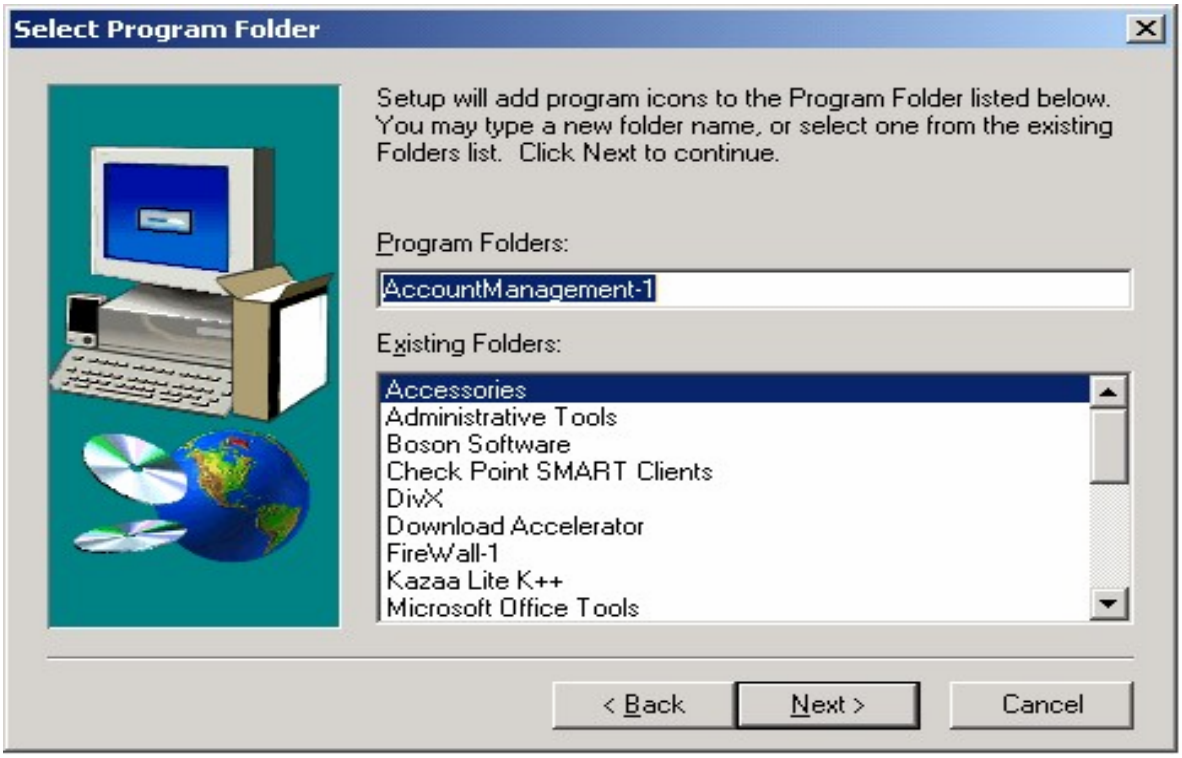
Chọn Next để bắt đầu quá trình cài đặt.

Sau khi cài xong GUI Client, màn hình sẽ tự động hiện ra phần cài đặt Account Management Client With Encryption Installation:

Chọn Next rồi chọn thư mục cài đặt trong cửa sổ Choose Destination Location:



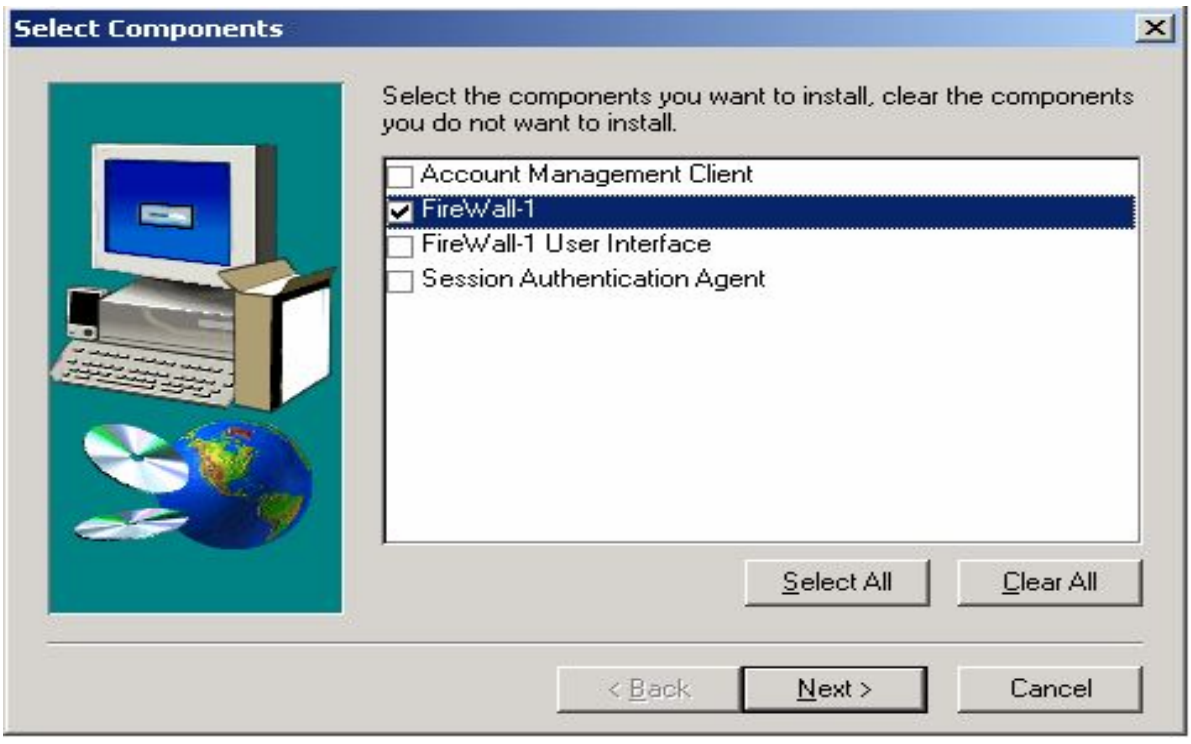
Chọn Next rồi chọn Folder trong cửa sổ Select Program Folder:



Chọn Next để bắt đầu quá trình cài đặt

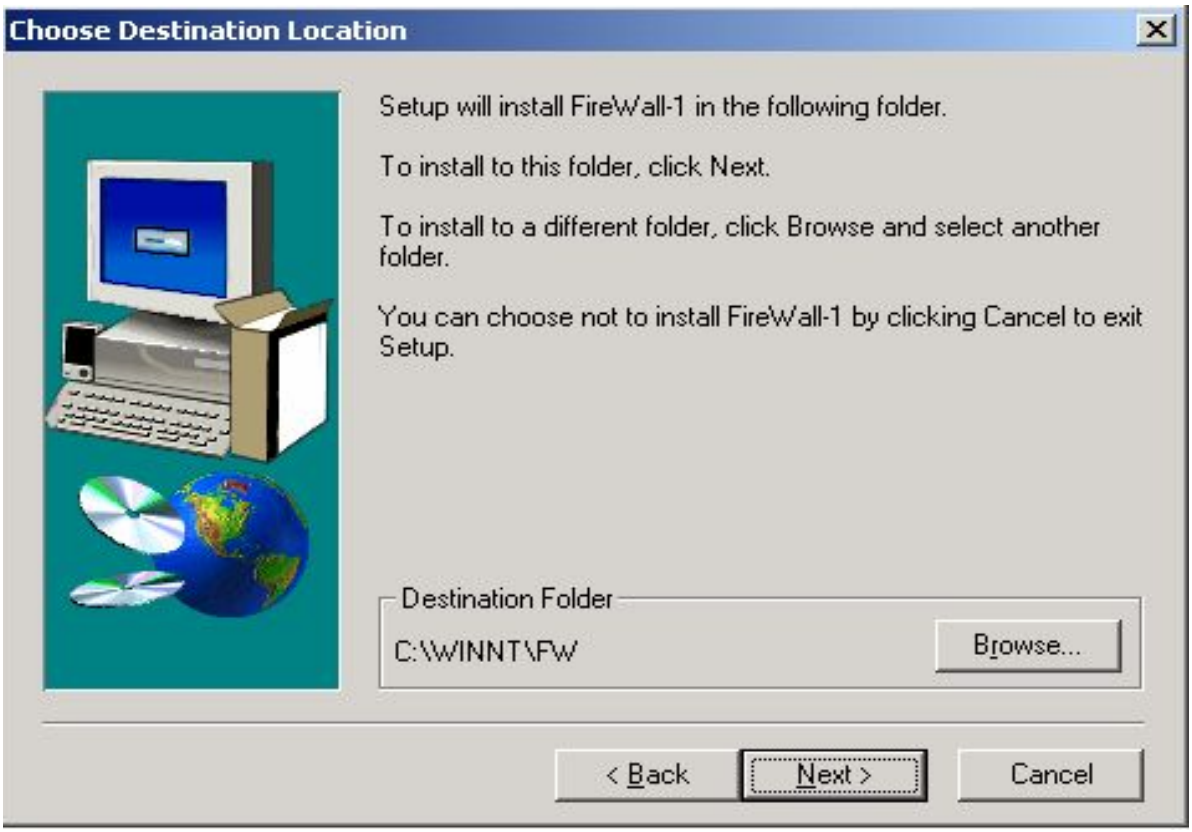
II.3.3.2. Cài đặt Module Firewall:

Chọn FireWall-1 trong cửa sổ Select Components ban đầu:



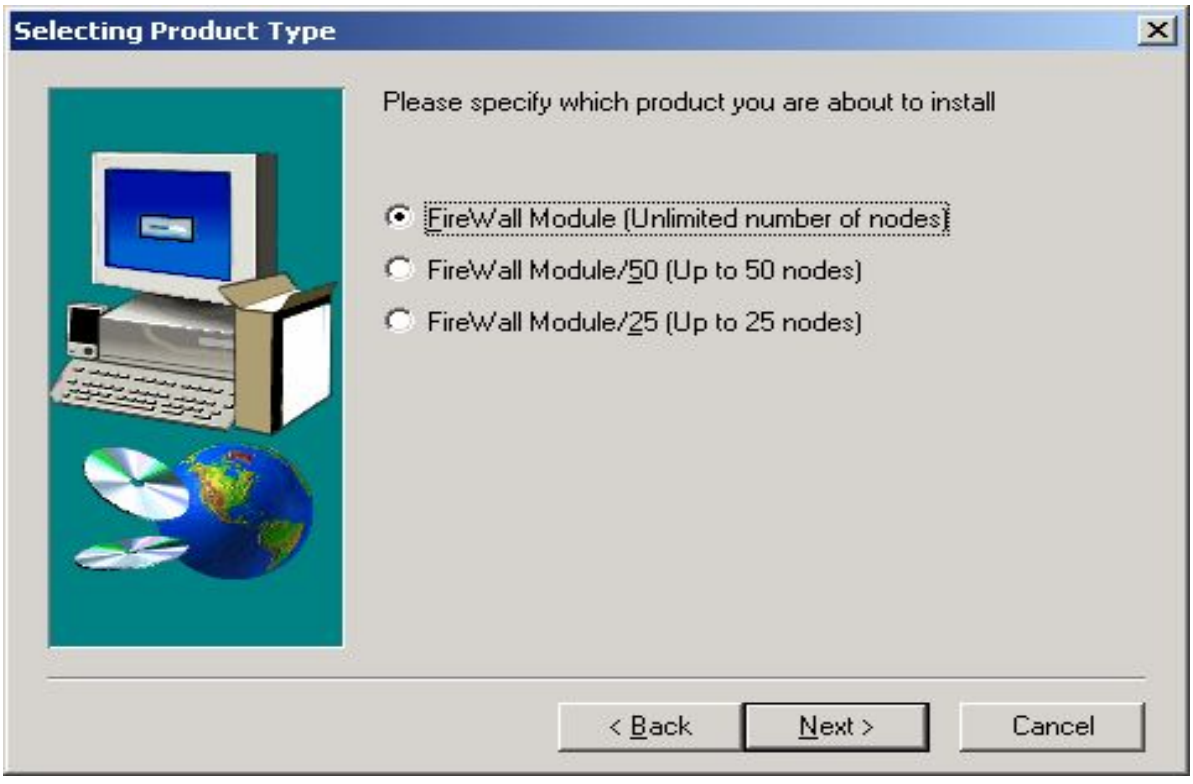
Chọn Next, màn hình sẽ hiện ra như sau:

Chọn Next rồi chọn thư mục cài đặt trong cửa sổ Choose Destination Location:



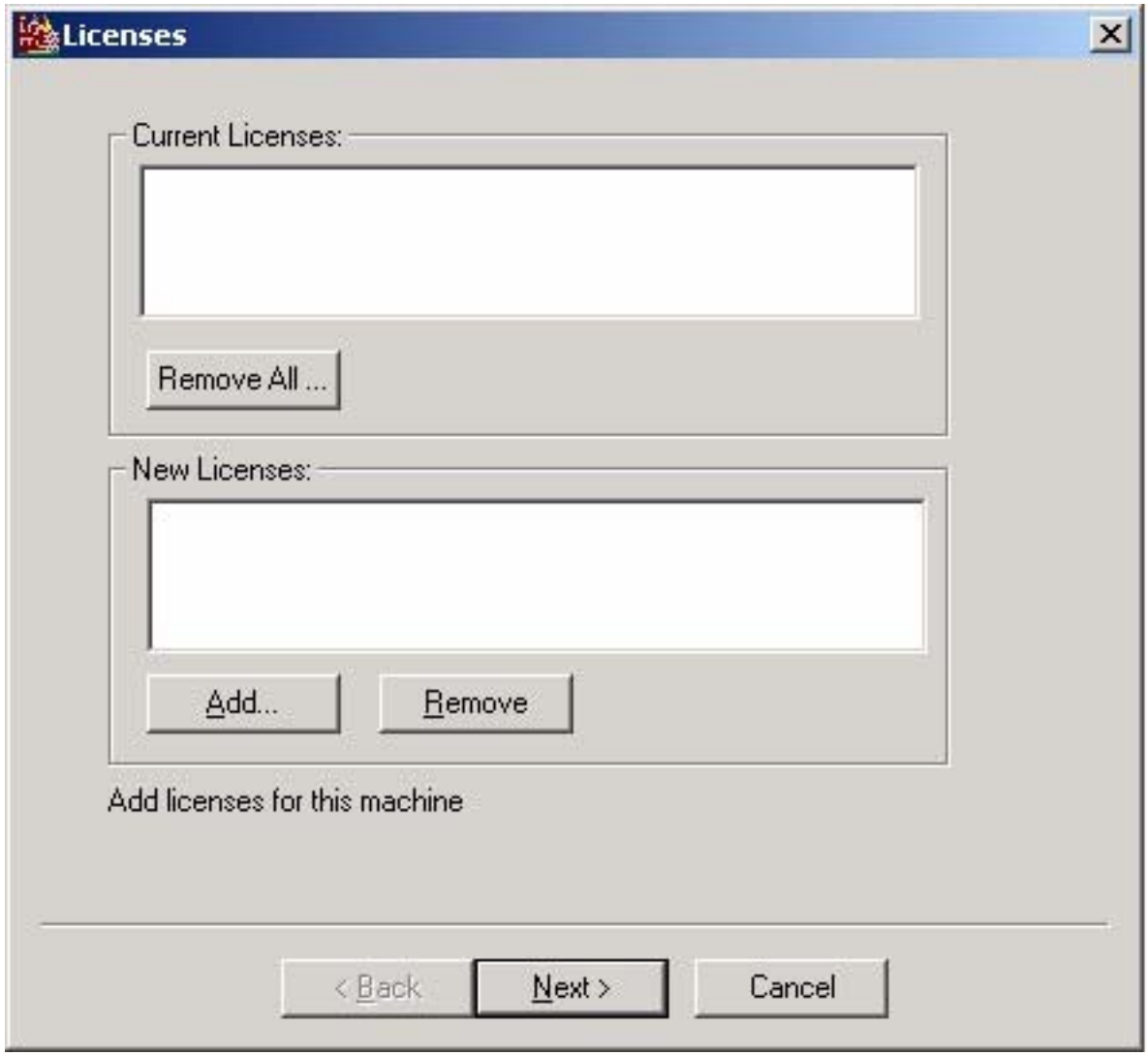
Chọn Next rồi chọn FireWall-1 FireWall Module trong cửa sổ Selecting Product Type:

Chọn Next rồi tùy theo phiên bản Checkpoint đăng ký để chọn số license phù hợp:

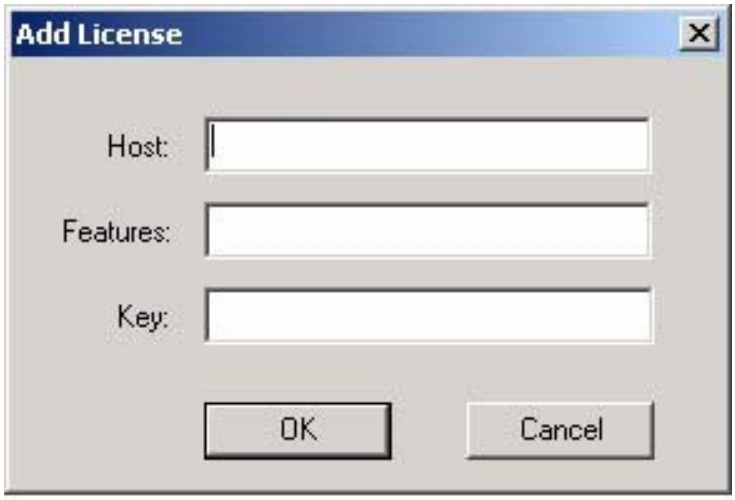


Chọn Next để bắt đầu quá trình cài đặt.

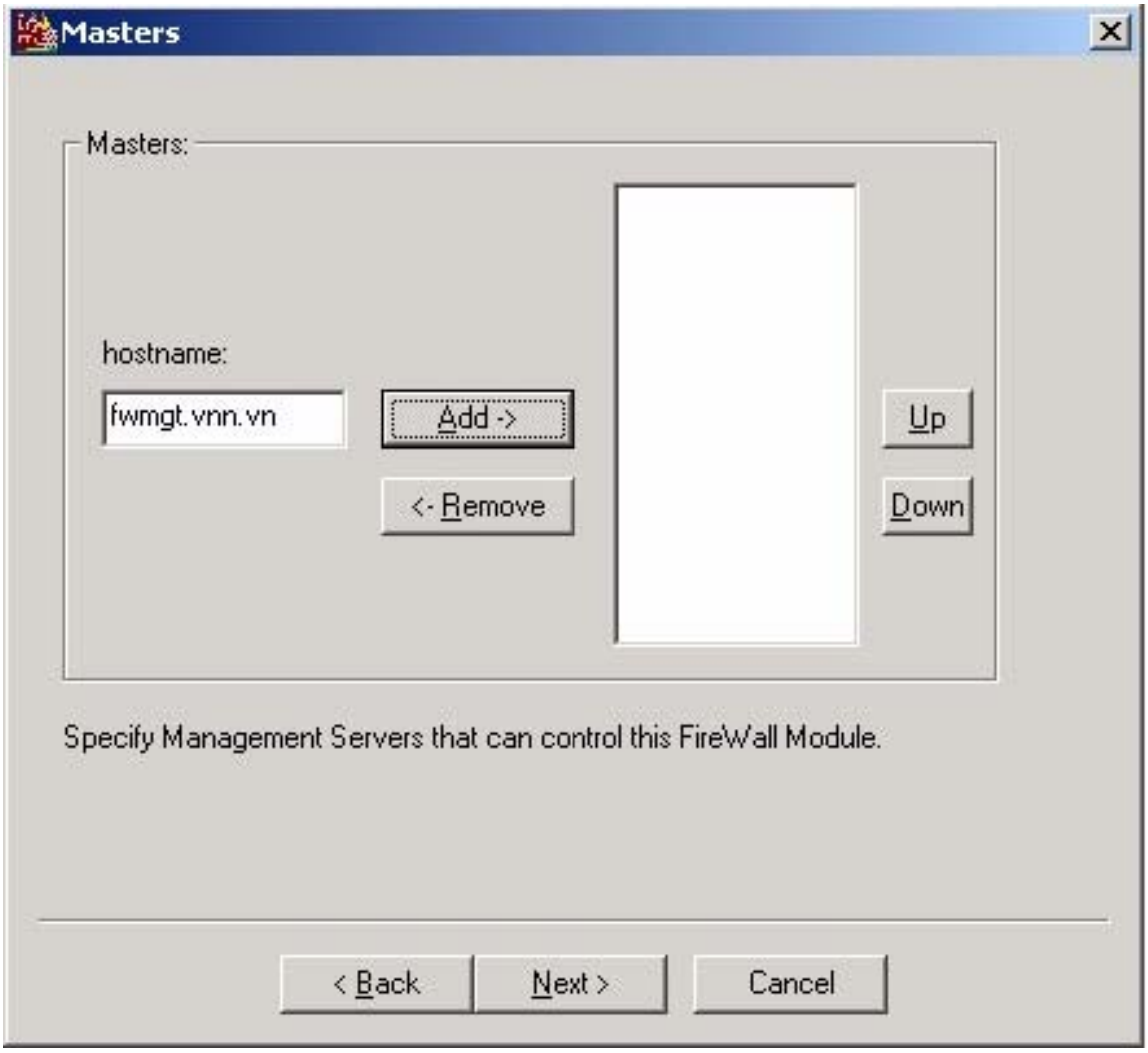
Sau khi cài xong, màn hình cài đặt license sẽ hiện lên như sau:



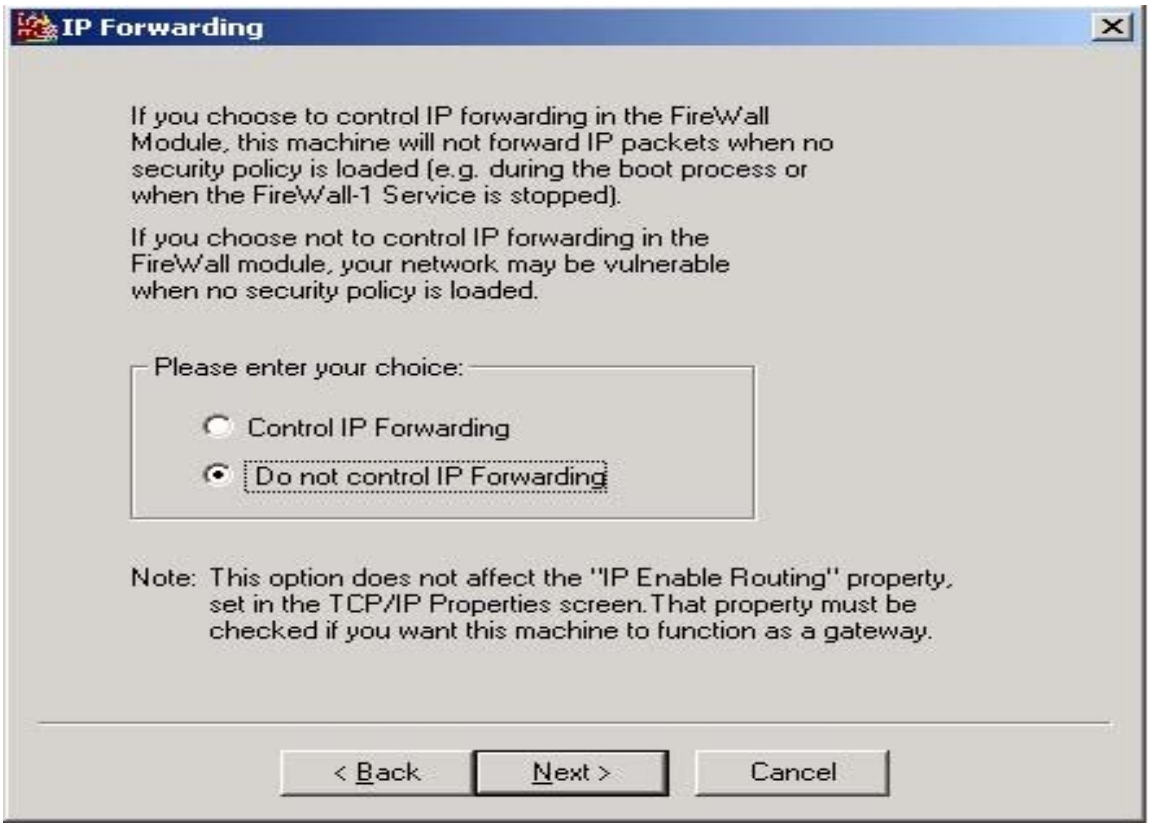
Chọn Add rồi nhập license vào cửa sổ sau :



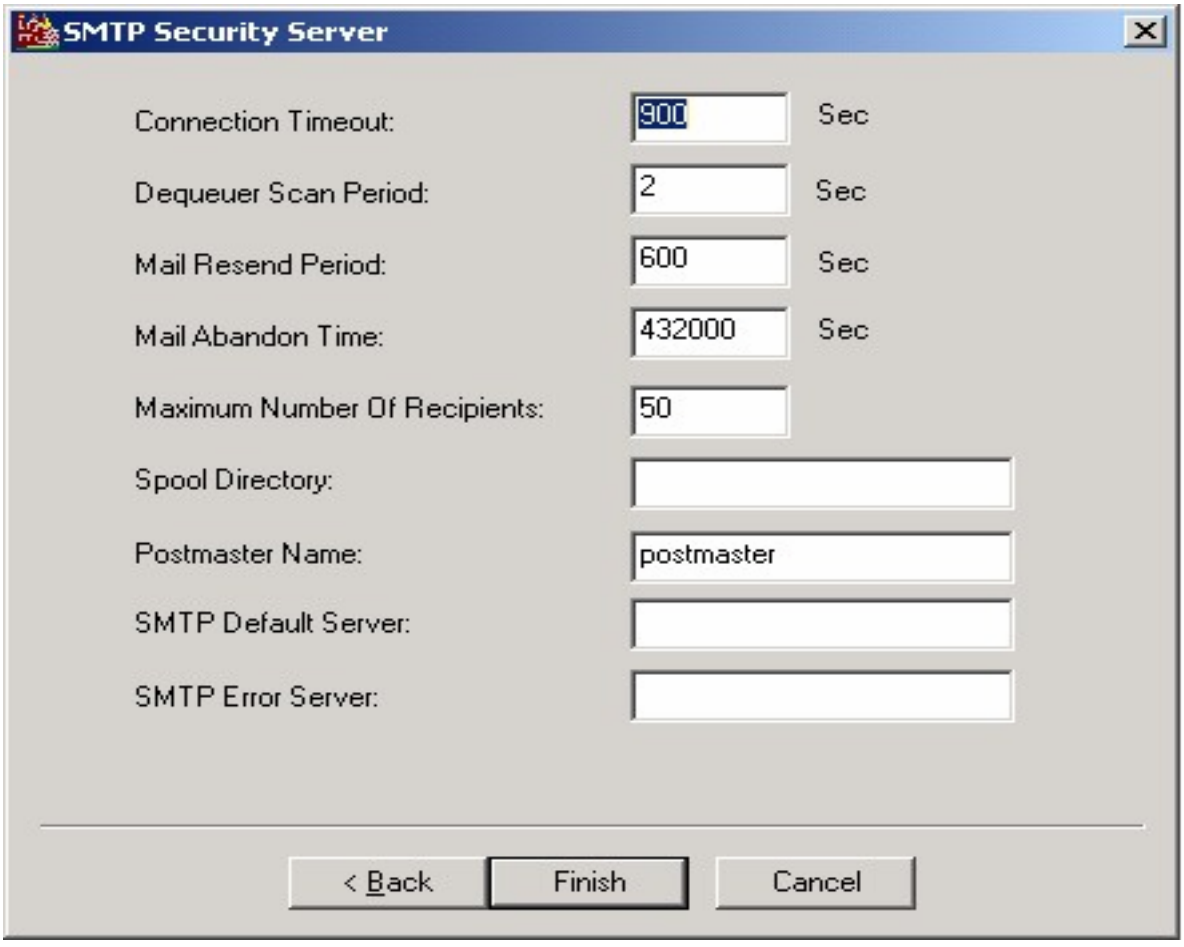
Chọn hostname của Management Server:



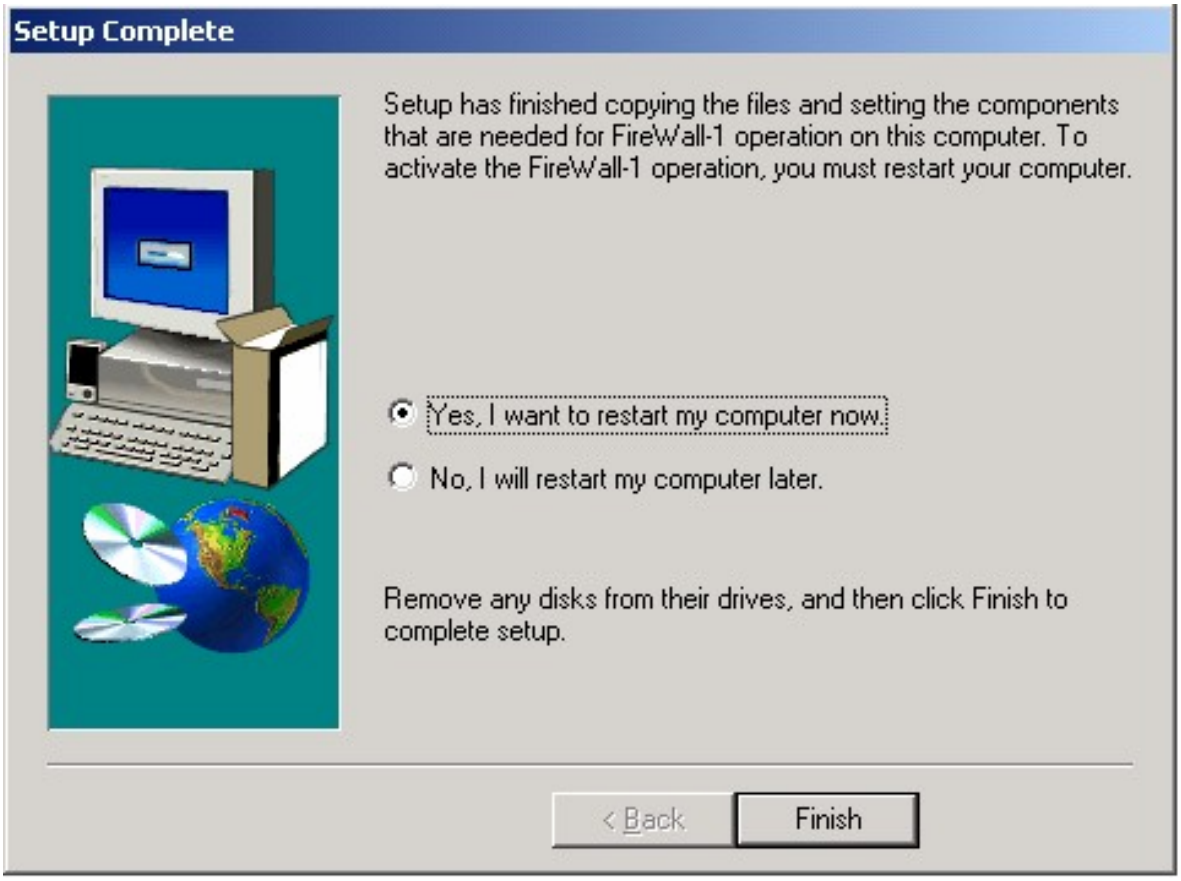
Chọn chế độ IP Forwarding:



Đặt các tham số cho SMTP Security Server:



Chọn Finish để kết thúc quá trình cài đặt rồi Restart lại máy.



Giáo trình

Quản trị mạng và Thiết bị mạng

Mục lục

Lời nói đầu

*Giáo trình "**Quản trị mạng và các thiết bị mạng**" được biên soạn với mục tiêu cung cấp các kiến thức lý thuyết và thực hành quản trị chủ yếu cho các hệ thống thiết bị quan trọng nền tảng của mạng máy tính hiện đại. Giáo trình gồm 2 phần :*

Phần 1. Khái quát về mạng máy tính :** Bao gồm những khái niệm định nghĩa cơ bản nhất về mạng máy tính, phân loại mạng máy tính, giới thiệu các giao thức mạng, đặc biệt là giao thức TCP/IP. Các cơ sở lý thuyết đưa ra trong chương này đòi hỏi học viên phải nắm vững để có thể tiếp thu được các nội dung trong phần 2. **Tuy vậy, nếu học viên đã tự trang bị các kiến thức cơ bản trên hoặc đã được đào tạo theo giáo trình "Thiết kế và xây dựng mạng LAN và WAN" của đề án 112 có thể bỏ qua nội dung của phần một và học vào nội dung của phần 2 giáo trình

***Phần 2. Quản trị mạng :** Đây là phần nội dung chính của giáo trình "Quản trị mạng và các thiết bị mạng" bao gồm 4 chương cung cấp các kiến thức lý thuyết và kỹ năng quản trị cơ bản với các thành phần trọng yếu của mạng bao gồm bộ định tuyến, bộ chuyển mạch, hệ thống tên miền, hệ thống truy cập từ xa, hệ thống proxy, hệ thống bức tường lửa (firewall). Các nội dung biên soạn về kỹ năng thực hành quản trị giúp học viên có đủ các kiến thức thực tế để có thể bắt tay vào công tác quản trị mạng cho đơn vị.*

Do phạm vi rộng của công tác quản trị mạng, giáo trình này không bao gồm hết được mọi nội dung của công tác quản trị mạng. Học viên có nhu cầu nên tham khảo thêm các giáo trình khác của đề án 112 như :

- Thiết kế và xây dựng mạng LAN và WAN
- Quản trị Windows 2000-NT
- Tổng quan về Lotus Notes Domino
- Thiết kế và quản trị website, portal
- Thiết lập và quản trị hệ thống thư điện tử

Giáo trình được biên soạn lần đầu tiên nên không tránh khỏi có những thiếu sót. Nhóm biên soạn rất mong nhận được các góp ý từ phía các học viên, bạn đọc để có thể hoàn thiện nội dung giáo trình tốt hơn.

PHẦN I: KHÁI QUÁT VỀ CÔNG NGHỆ MẠNG

Chương 1
Tổng quan về công nghệ mạng máy tính và mạng cục bộ

Mục 1: Mạng máy tính

1. Giới thiệu mạng máy tính

1.1. Định nghĩa mạng máy tính và mục đích của việc kết nối mạng

1.1.1. Nhu cầu của việc kết nối mạng máy tính

Việc nối máy tính thành mạng từ lâu đã trở thành một nhu cầu khách quan vì :

- Có rất nhiều công việc về bản chất là phân tán hoặc về thông tin, hoặc về xử lý hoặc cả hai đòi hỏi có sự kết hợp truyền thông với xử lý hoặc sử dụng phương tiện từ xa.
- Chia sẻ các tài nguyên trên mạng cho nhiều người sử dụng tại một thời điểm (ổ cứng, máy in, ổ CD ROM . . .)
- Nhu cầu liên lạc, trao đổi thông tin nhờ phương tiện máy tính.
- Các ứng dụng phần mềm đòi hòi tại một thời điểm cần có nhiều người sử dụng, truy cập vào cùng một cơ sở dữ liệu.

1.1.2. Định nghĩa mạng máy tính

Nói một cách ngắn gọn thì mạng máy tính là tập hợp các máy tính độc lập được kết nối với nhau thông qua các đường truyền vật lý và tuân theo các quy ước truyền thông nào đó.

Khái niệm máy tính độc lập được hiểu là các máy tính không có máy nào có khả năng khởi động hoặc đình chỉ một máy khác.

Các đường truyền vật lý được hiểu là các môi trường truyền tín hiệu vật lý (có thể là hữu tuyến hoặc vô tuyến).

Các quy ước truyền thông chính là cơ sở để các máy tính có thể "nói chuyện" được với nhau và là một yếu tố quan trọng hàng đầu khi nói về công nghệ mạng máy tính.

1.2. Đặc trưng kỹ thuật của mạng máy tính

Một mạng máy tính có các đặc trưng kỹ thuật cơ bản như sau:

1.2.1. Đường truyền

Là phương tiện dùng để truyền các tín hiệu điện tử giữa các máy tính.

Các tín hiệu điệu tử đó chính là các thông tin, dữ liệu được biểu thị dưới dạng các xung nhị phân (ON_OFF), mọi tín hiệu truyền giữa các máy tính với nhau đều thuộc sóng điện từ, tuỳ theo tần số mà ta có thể dùng các đường truyền vật lý khác nhau

Đặc trưng cơ bản của đường truyền là giải thông nó biểu thị khả năng truyền tải tín hiệu của đường truyền.

Thông thuờng người ta hay phân loại đường truyền theo hai loại:

- Đường truyền hữu tuyến (các máy tính được nối với nhau bằng các dây dẫn tín hiệu).
- Đường truyền vô tuyến: các máy tính truyền tín hiệu với nhau thông qua các sóng vô tuyến với các thiết bị điều chế/giải điều chế ở các đầu mút.

1.2.2. Kỹ thuật chuyển mạch

Là đặc trưng kỹ thuật chuyển tín hiệu giữa các nút trong mạng, các nút mạng có chức năng hướng thông tin tới đích nào đó trong mạng, hiện tại có các

kỹ thuật chuyển mạch như sau:
- Kỹ thuật chuyển mạch kênh: Khi có hai thực thể cần truyền thông với nhau thì giữa chúng sẽ thiết lập một kênh cố định và duy trì kết nối đó cho tới khi hai bên ngắt liên lạc. Các dữ liệu chỉ truyền đi theo con đường cố định đó.
- Kỹ thuật chuyển mạch thông báo: thông báo là một đơn vị dữ liệu của người sử dụng có khuôn dạng được quy định trước. Mỗi thông báo có chứa các thông tin điều khiển trong đó chỉ rõ đích cần truyền tới của thông báo. Căn cứ vào thông tin điều khiển này mà mỗi nút trung gian có thể chuyển thông báo tới nút kế tiếp trên con đường dẫn tới đích của thông báo
- Kỹ thuật chuyển mạch gói: ở đây mỗi thông báo được chia ra thành nhiều gói nhỏ hơn được gọi là các gói tin (packet) có khuôn dạng qui định trước. Mỗi gói tin cũng chứa các thông tin điều khiển, trong đó có địa chỉ nguồn (người gửi) và địa chỉ đích (người nhận) của gói tin. Các gói tin của cùng một thông báo có thể được gửi đi qua mạng tới đích theo nhiều con đường khác nhau.

1.2.3. Kiến trúc mạng

Kiến trúc mạng máy tính (network architecture) thể hiện cách nối các máy tính với nhau và tập hợp các quy tắc, quy ước mà tất cả các thực thể tham gia truyền thông trên mạng phải tuân theo để đảm bảo cho mạng hoạt động tốt. Khi nói đến kiến trúc của mạng người ta muốn nói tới hai vấn đề là hình trạng mạng (Network topology) và giao thức mạng (Network protocol)
- Network Topology: Cách kết nố_____i các máy tính với nhau về mặt hình học mà ta gọi là tô pô của mạng

Các hình trạng mạng cơ bản đó là: hình sao, hình bus, hình vòng

- Network Protocol: Tập hợp các quy ước truyền thông giữa các thực thể truyền thông mà ta gọi là giao thức (hay nghi thức) của mạng

Các giao thức thường gặp nhất là : TCP/IP, NETBIOS, IPX/SPX, . . .

1.2.4. Hệ điều hành mạng

Hệ điều hành mạng là một phần mềm hệ thống có các chức năng sau:
- Quản lý tài nguyên của hệ thống, các tài nguyên này gồm:
+ Tài nguyên thông tin (về phương diện lưu trữ) hay nói một cách đơn giản là quản lý tệp. Các công việc về lưu trữ tệp, tìm kiếm, xoá, copy, nhóm, đặt các thuộc tính đều thuộc nhóm công việc này
+ Tài nguyên thiết bị. Điều phối việc sử dụng CPU, các ngoại vi... để tối ưu hoá việc sử dụng
- Quản lý người dùng và các công việc trên hệ thống.

Hệ điều hành đảm bảo giao tiếp giữa người sử dụng, chương trình ứng dụng với thiết bị của hệ thống.
- Cung cấp các tiện ích cho việc khai thác hệ thống thuận lợi (ví dụ FORMAT đĩa, sao chép tệp và thư mục, in ấn chung ...)

Các hệ điều hành mạng thông dụng nhất hiện nay là: WindowsNT, Windows9X, Windows 2000, Unix, Novell.

1.3. Phân loại mạng máy tính

Có nhiều cách phân loại mạng khác nhau tuỳ thuộc vào yếu tố chính được chọn dùng để làm chỉ tiêu phân loại, thông thường người ta phân loại mạng theo các tiêu chí như sau
- Khoảng cách địa lý của mạng
- Kỹ thuật chuyển mạch mà mạng áp dụng
- Kiến trúc mạng
- Hệ điều hành mạng sử dụng ...

Tuy nhiên trong thực tế người ta thường chỉ phân loại theo hai tiêu chí

đầu tiên

1.3.1. Phân loại mạng theo khoảng cách địa lý

Nếu lấy khoảng cách địa lý làm yếu tố phân loại mạng thì ta có mạng cục bộ (LAN), mạng đô thị (MAN), mạng diện rộng (WAN), mạng toàn cầu.

1.3.2. Phân loại theo kỹ thuật chuyển mạch

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

Mạch chuyển mạch kênh (circuit switched network) : hai thực thể thiết lập một kênh cố định và duy trì kết nối đó cho tới khi hai bên ngắt liên lạc.

Mạng chuyển mạch thông báo (message switched network) : Thông báo là một đơn vị dữ liệu qui ước được gửi qua mạng đến điểm đích mà không thiết lập kênh truyền cố định. Căn cứ vào thông tin tiêu đề mà các nút mạng có thể xử lý được việc gửi thông báo đến đích

Mạng chuyển mạch gói (packet switched network) : ở đây mỗi thông báo được chia ra thành nhiều gói nhỏ hơn được gọi là các gói tin (packet) có khuôn dạng qui định trước. Mỗi gói tin cũng chứa các thông tin điều khiển, trong đó có địa chỉ nguồn (người gửi) và địa chỉ đích (người nhận) của gói tin. Các gói tin của cùng một thông báo có thể được gởi đi qua mạng tới đích theo nhiều con đường khác nhau.

1.3.3. Phân loại theo kiến trúc mạng sử dụng

Kiến trúc của mạng bao gồm hai vấn đề: hình trạng mạng (Network topology) và giao thức mạng (Network protocol)

Hình trạng mạng: Cách kết nối các máy tính với nhau về mặt hình học mà ta gọi là tô pô của mạng

Giao thức mạng: Tập hợp các quy ước truyền thông giữa các thực thể truyền thông mà ta gọi là giao thức (hay nghi thức) của mạng

Khi phân loại theo topo mạng người ta thường có phân loại thành: mạng hình sao, tròn, tuyến tính

Phân loại theo giao thức mà mạng sử dụng người ta phân loại thành mạng : TCP/IP, mạng NETBIOS . ..

Tuy nhiên các cách phân loại trên không phổ biến và chỉ áp dụng cho các mạng cục bộ.

1.3.4. Phân loại theo hệ điều hàng mạng

Nếu phân loại theo hệ điều hành mạng người ta chia ra theo mô hình mạng ngang hàng, mạng khách/chủ hoặc phân loại theo tên hệ điều hành mà mạng sử dụng: Windows NT, Unix, Novell . . .

1.4. Các mạng máy tính thông dụng nhất

1.4.1. Mạng cục bộ

Một mạng cục bộ là sự kết nối một nhóm máy tính và các thiết bị kết nối mạng được lắp đặt trên một phạm vị địa lý giới hạn, thường trong một toà nhà hoặc một khu công sở nào đó. Mạng có tốc độ cao

1.4.2. Mạng diệ_____n rộng với kết nối LAN to LAN

Mạng diện rộng bao giờ cũng là sự kết nối của các mạng LAN, mạng diện rộng có thể trải trên phạm vi một vùng, quốc gia hoặc cả một lục địa thậm chí trên phạm vi toàn cầu. Mạng có tốc độ truyền dữ liệu không cao, phạm vi địa lý không giới hạn

1.4.3. Liên mạng INTERNET

Với sự phát triển nhanh chóng của công nghệ là sự ra đời của liên mạng INTERNET. Mạng Internet là sở hữu của nhân loại, là sự kết hợp của rất nhiều mạng dữ liệu khác chạy trên nền tảng giao thức TCP/IP

1.4.4. Mạng INTRANET

Thực sự là một mạng INTERNET thu nhỏ vào trong một cơ quan/công ty/tổ chức hay một bộ/nghành . . ., giới hạn phạm vi người sử dụng, có sử dụng các công nghệ kiểm soát truy cập và bảo mật thông tin .

Được phát triển từ các mạng LAN, WAN dùng công nghệ INTERNET

2. Mạng cục bộ, kiến trúc mạng cục bộ

2.1. Mạng cục bộ

Tên gọi "mạng cục bộ" được xem xét từ quy mô của mạng. Tuy nhiên, đó không phải là đặc tính duy nhất của mạng cục bộ nhưng trên thực tế, quy mô của mạng quyết định nhiều đặc tính và công nghệ của mạng. Sau đây là một số đặc điểm của mạng cục bộ:

Đặc điểm của mạng cục bộ

- Mạng cục bộ có quy mô nhỏ, thường là bán kính dưới vài km.
- Mạng cục bộ thường là sở hữu của một tổ chức. Thực tế đó là điều khá quan trọng để việc quản lý mạng có hiệu quả.
- Mạng cục bộ có tốc độ cao và ít lỗi. Trên mạng rộng tốc độ nói chung chỉ đạt vài trăm Kbit/s đến Mb/s. Còn tốc độ thông thường trên mạng cục bộ là 10, 100 Mbit/s và tới nay với Gigabit Ethernet.

2.2. Kiến trúc mạng cục bộ

2.2.1. Đồ hình mạng (Network Topology)

*** Định nghĩa Topo mạng:**

Cách kết nối các máy tính với nhau về mặt hình học mà ta gọi là tô pô của mạng. Có hai kiểu nối mạng chủ yếu đó là :

- Nối kiểu điểm - điểm (point - to - point): các đường truyền nối từng cặp nút với nhau, mỗi nút "lưu và chuyển tiếp" dữ liệu
- Nối kiểu điểm - nhiều điểm (point - to - multipoint hay broadcast) : tất cả các nút phân chia nhau một đường truyền vật lý, gửi dữ liệu đến nhiều nút một lúc và kiểm tra gói tin theo địa chỉ

*** Phân biệt kiểu tô pô của mạng cục bộ và kiểu tô pô của mạng rộng.**

Tô pô của mạng diện rộng thông thường là nói đến sự liên kết giữa các mạng cục bộ thông qua các bộ dẫn đường (router) và kênh viễn thông. Khi nói tới tô pô của mạng cục bộ người ta nói đến sự liên kết của chính các máy tính.

- ***Mạng hình sao:*** Mạng hình sao có tất cả các trạm được kết nối với một thiết bị trung tâm có nhiệm vụ nhận tín hiệu từ các trạm và chuyển đến trạm đích Độ dài đường truyền nối một trạm với thiết bị trung tâm bị hạn chế (trong vòng 100m, với công nghệ hiện nay).

- Mạng trục tuyến tính (Bus):

Trong mạng trục tất cả các trạm phân chia một đường truyền chung (bus). Đường truyền chính được giới hạn hai đầu bằng hai đầu nối đặc biệt gọi là terminator. Mỗi trạm được nối với trục chính qua một đầu nối chữ T (Tconnector) hoặc một thiết bị thu phát (transceiver).

- Mạng hình vòng

Trên mạng hình vòng tín hiệu được truyền đi trên vòng theo một chiều duy nhất. Mỗi trạm của mạng được nối với vòng qua một bộ chuyển tiếp (repeater) do đó cần có giao thức điều khiển việc cấp phát quyền được truyền dữ liệu trên vòng mạng cho trạm có nhu cầu.

Mạng hình vòng có ưu nhược điểm tương tự mạng hình sao, tuy nhiên

mạng hình vòng đòi hỏi giao thức truy nhập mạng phức tạp hơn mạng hình sao.

Hub

Hình 1.1: Kết nối hình sao

Hình 1.2. Kết nối kiểu bus

d) Kết nối hỗn hợp

Là sự phối hợp các kiểu kết nối khác nhau,

2.3. Các phương pháp truy cập đường truyền vật lý

Trong mạng cục bộ, tất cả các trạm kết nối trực tiếp vào đường truyền chung. Nếu nhiều trạm cùng gửi tín hiệu lên đường truyền đồng thời thì tín hiệu sẽ chồng lên nhau và bị hỏng. Vì vậy cần phải có một phương pháp tổ chức chia sẻ đường truyền để việc truyền thông đực đúng đắn.

Có hai phương pháp chia sẻ đường truyền chung thường được dùng trong các mạng cục bộ:

- Truy nhập đường truyền một cách ngẫu nhiên, theo yêu cầu. Đương nhiên phải có tính đến việc sử dụng luân phiên và nếu trong trường hợp do có nhiều trạm cùng truyền tin dẫn đến tín hiệu bị trùm lên nhau thì phải truyền lại. Điển hình của phương pháp này là giao thức truy cập CSMA/CD

Hình 1.3. Kết nối kiểu vòng

Hình 1.4. Một kết nối hỗn hợp

Hub

Hub

HUB

Bộ chuyển đổi cáp

- Có cơ chế trọng tài để cấp quyền truy nhập đường truyền sao cho không xảy ra xung đột. Điển hình phương pháp này là giao thức truy cập Tokenring

3. Chuẩn hoá mạng máy tính

3.1. Vấn đề chuẩn hoá mạng và các tổ chức chuẩn hoá mạng

Khi thiết kế các giao thức mạng, các nhà thiết kế tự do lựa chọn kiến trúc cho riêng mình. Từ đó dẫn tới tình trạng không tương thích giữa các mạng máy tính với nhau. Vấn đề không tương thích đó làm trở ngại cho sự tương tác giữa những giao thức mạng khác nhau. Nhu cầu trao đổi thông tin càng lớn thúc đẩy việc xây dựng khung chuẩn về kiến trúc mạng để làm căn cứ cho các nhà thiết kế và chế tạo thiết bị mạng .

Chính vì lý do đó, tổ chức tiêu chuẩn hoá quốc tế ISO (Internatinal Organnization for Standarzation) đã xây dựng mô hình tham chiếu cho việc kết nối các hệ thống mở OSI (reference model for Open Systems Interconnection). Mô hình này là cơ sở cho việc kết nối các hệ thống mở phục vụ cho các ứng dụng phân tán.

3.2. Mô hình tham chiếu OSI 7 lớp

Mô hình OSI được biểu diễn theo hình dưới đây:

Mô hình OSI phân chia thành 7 lớp bao gồm các lớp ứng dụng, lớp thể hiện, lớp phiên, lớp vận chuyển, lớp mạng, lớp liên kết và lớp vật lý. Mô hình OSI cũng định nghĩa phần tiêu đề (header) của đơn vị dữ liệu và mối liên kết giữa các lớp, việc gắn thêm phần mào đầu (header) để chuyển dữ liệu từ các lớp trên xuống lớp dưới và mở gói là chức năng gỡ bỏ phần mào đầu để chuyển dữ liệu lên lớp trên.

Lớp ứng dụng
(application)

Lớp thể hiện
(presentation)
Lớp phiên
(session)
Lớp chuyển vận
(transport)
Lớp mạng
(network)
Lớp liên kết dữ liệu
(data link)
Lớp vật lý
Ebook 4 U *Hình 1.5. Mô hình OSI 7 lớp* ebook.vinagrid.com

(physical link)
Chức năng cụ thể của từng lớp theo mô hình OSI có thể tham khảo chi tiết thêm trong giáo trình "Thiết kế và xây dựng mạng LAN và WAN"

3.3. Các chuẩn kết nối thông dụng nhất IEEE 802.X và ISO 8802.X

Bên cạnh việc chuẩn hoá cho mạng nói chung dẫn đến kết quả cơ bản nhất là mô hình tham chiếu OSI như đã giới thiệu, người ta cũng chuẩn hóa các giao thức mạng cục bộ LAN.

- *Các chuẩn IEEE 802.x và ISO 8802.x*

IEEE là tổ chức đi tiên phong trong lĩnh vực chuẩn hoá mạng cục bộ với đề án IEEE 802 với kết quả là một loạt các chuẩn thuộc họ IEEE 802.x ra đời . Cuối những năm 80, tổ chức ISO đã tiếp nhận họ chuẩn này và ban hành thành chuẩn quốc tế dưới mã hiệu tương ứng là ISO 8802.x.

IEEE 802.: là chuẩn đặc tả kiến trúc mạng, kết nối giữa các mạng và việc quản trị mạng đối với mạng cục bộ.

IEEE 802.2: là chuẩn đặc tả tầng dịch vụ giao thức của mạng cục bộ.

IEEE 802.3: là chuẩn đặc tả một mạng cục bộ dựa trên mạng Ethernet nổi tiếng của Digital, Intel và Xerox hợp tác xây dựng từ năm 1980. Các chuẩn qui định vật lý như 10BASE5, 10BASE2, 10BASE-F,

IEEE 802.5: là chuẩn đặc tả mạng cục bộ với topo mạng dạng vòng (ring) dùng thẻ bài để điều việc truy nhập đường truyền.

IEEE 802.11: là chuẩn đặc tả mạng cục bộ không dây (Wireless LAN) hiện đang được tiếp tục phát triển.

Ngoài ra trong họ chuẩn 802.x còn có các chuẩn IEEE 802.4, 802.6, 802.9, 802.10 và 802.12

Mục 2: Các thiết bị mạng thông dụng và các chuẩn kết nối vật lý

1. Các thiết bị mạng thông dụng

1.1. Các loại cáp truyền

1.1.1. Cáp đôi dây xoắn (Twisted pair cable)

Cáp đôi dây xoắn là cáp gồm hai dây đồng xoắn để tránh gây nhiễu cho các đôi dây khác, có thể kéo dài tới vài km mà không cần khuyếch đại. Giải tần trên cáp dây xoắn đạt khoảng 300–4000Hz, tốc độ truyền đạt vài kbps đến vài Mbps. Cáp xoắn có hai loại:

- Loại có bọc kim loại để tăng cường chống nhiễu gọi là STP (Shield Twisted Pair). Loại này trong vỏ bọc kim có thể có nhiều đôi dây. Về lý thuyết thì tốc độ truyền có thể đạt 500 Mb/s nhưng thực tế thấp hơn rất nhiều (chỉ đạt

155 Mbps với cáp dài 100 m)
- Loại không bọc kim gọi là UTP (UnShield Twisted Pair), chất lượng kém hơn STP nhưng rất rẻ. Cap UTP được chia làm 5 hạng tuỳ theo tốc độ truyền. Cáp loại 3 dùng cho điện thoại. Cáp loại 5 có thể truyền với tốc độ 100Mb/s rất hay dùng trong các mạng cục bộ vì vừa rẻ vừa tiện sử dụng. Cáp này có 4 đôi dây xoắn nằm trong cùng một vỏ bọc

1.1.2. Cáp đồng trục (Coaxial cable) băng tần cơ sở

Là cáp mà hai dây của nó có lõi lồng nhau, lõi ngoài là lưới kim loại. , Khả năng chống nhiễu rất tốt nên có thể sử dụng với chiều dài từ vài trăm met đến vài km. Có hai loại được dùng nhiều là loại có trở kháng 50 ohm và loại có trở kháng 75 ohm.

Hình 1.6. Cáp UTP Cat. 5

Hình 1.7. Cáp đồng trục

Dải thông của cáp này còn phụ thuộc vào chiều dài của cáp. Với khoảng cách1 km có thể đạt tốc độ truyền từ 1– 2 Gbps. Cáp đồng trục băng tần cơ sở thường dùng cho các mạng cục bộ. Có thể nối cáp bằng các đầu nối theo chuẩn BNC có hình chữ T. ở VN người ta hay gọi cáp này là cáp gầy do dịch từ tên trong tiếng Anh là 'Thin Ethernet".

Một loại cáp khác có tên là "Thick Ethernet" mà ta gọi là cáp béo. Loại này thường có màu vàng. Người ta không nối cáp băng các đầu nối chữ T như cáp gầy mà nối qua các kẹp bấm vào dây. Cứ 2m5 lại có đánh dấu để nối dây (nếu cần). Từ kẹp đó người ta gắn các tranceiver rồi nối vào máy tính.

1.1.3. Cáp đồng trục băng rộng (Broadband Coaxial Cable)

Đây là loại cáp theo tiêu chuẩn truyền hình (thường dùng trong truyền hình cáp) có dải thông từ 4 – 300 Khz trên chiều dài 100 km. Thuật ngữ "băng rộng" vốn là thuật ngữ của ngành truyền hình còn trong ngành truyền số liệu điều này chỉ có nghĩa là cáp loại này cho phép truyền thông tin tương tự (analog) mà thôi. Các hệ thống dựa trên cáp đồng trục băng rộng có thể truyền song song nhiều kênh. Việc khuyếch đại tín hiệu chống suy hao có thể làm theo kiểu khuyếch đại tín hiệu tương tự (analog). Để truyền thông cho máy tính cần chuyển tín hiệu số thành tín hiệu tương tự.

1.1.4. Cáp quang

Dùng để truyền các xung ánh sáng trong lòng một sợi thuỷ tinh phản xạ toàn phần. Môi trường cáp quang rất lý tưởng vì
- Xung ánh sáng có thể đi hàng trăm km mà không giảm cường độ sáng.
- Dải thông rất cao vì tần số ánh sáng dùng đối với cáp quang cỡ khoảng 1014 –1016
- An toàn và bí mật, không bị nhiễu điện từ

Chỉ có hai nhược điểm là khó nối dây và giá thành cao.

Cáp quang cũng có hai loại
- Loại đa mode (multimode fiber): khi góc tới thành dây dẫn lớn đến một mức nào đó thì có hiện tượng phản xạ toàn phần. Các cáp đa mode có đường kính khoảng 50 µ
- Loại đơn mode (singlemode fiber): khi đường kính dây dẫn bằng bước sóng thì cáp quang giống như một ống dẫn sóng, không có hiện tượng phản xạ nhưng chỉ cho một tia đi. Loại này có đường kính khoản 8µm và phải dùng

Hình 1.8. Truyền tín hiệu bằng cáp quang

diode laser. Cáp quang đa mode có thể cho phép truyền xa tới hàng trăm km

mà không cần phải khuyếch đại.

1.2. Các thiết bị ghép nối

1.2.1. Card giao tiếp mạng (Network Interface Card - NIC)

Đó là một card được cắm trực tiếp vào máy tính trên khe cắm mở rộng ISA hoặc PCI hoặc tích hợp vào bo mạch chủ PC. Trên đó có các mạch điện giúp cho việc tiếp nhận (receiver) hoặc/và phát (transmitter) tín hiệu lên mạng. Người ta thường dùng từ tranceiver để chỉ thiết bị (mạch) có cả hai chức năng thu và phát.

1.2.2. Bộ chuyển tiếp (REPEATER)

Nhiệm vụ của các repeater là hồi phục tín hiệu để có thể truyền tiếp cho các trạm khác bao gồm cả công tác khuyếch đại tín hiệu, điều chỉnh tín hiệu.

1.2.3. Các bộ tập trung (Concentrator hay HUB)

HUB là một loại thiết bị có nhiều đầu cắm các đầu cáp mạng. Người ta sử dụng HUB để nối mạng theo kiểu hình sao. Ưu điểm của kiểu nối này là tăng độ độc lập của các máy khi một máy bị sự cố dây dẫn.

Có loại HUB thụ động (passive HUB) là HUB chỉ đảm bảo chức năng kết nối hoàn toàn không xử lý lại tín hiệu. HUB chủ động (active HUB) là HUB có chức năng khuyếch đại tín hiệu để chống suy hao.

HUB thông minh (intelligent HUB) là HUB chủ động nhưng có khả năng tạo ra các gói tin mang tin tức về hoạt động của mình và gửi lên mạng để người quản trị mạng có thể thực hiện quản trị tự động

1.2.4. Switching Hub (hay còn gọi tắt là switch)

Là các bộ chuyển mạch thực sự. Khác với HUB thông thường, thay vì chuyển một tín hiệu đến từ một cổng cho tất cả các cổng, nó chỉ chuyển tín hiệu đến cổng có trạm đích. Do vậy Switch là một thiết bị quan trọng trong các mạng cục bộ lớn dùng để phân đoạn mạng. Nhờ có switch mà đụng độ trên mạng giảm hẳn. Ngày nay switch là các thiết bị mạng quan trọng cho phép tuỳ biến trên mạng chẳng hạn lập mạng ảo VLAN.

Hình 1.9. LAN Switch nối hai Segment mạng

1.2.5. Modem

Là tên viết tắt từ hai từ điều chế (MOdulation) và giải điều chế (DEModulation) là thiết bị cho phép điều chế để biến đổi tín hiệu số sang tín hiệu tương tự để có thể gửi theo đường thoại và khi nhận tín hiệu từ đường thoại có thể biến đổi ngược lại thành tín hiệu số.

1.2.6. Multiplexor - Demultiplexor

Bộ dồn kênh có chức năng tổ hợp nhiều tín hiệu để cùng gửi trên một đường truyền. Bộ tách kênh có chức năng ngược lại ở nơi nhận tín hiệu

1.2.7. Router

Router là một thiết bị dùng để ghép nối các mạng cục bộ với nhau thành mạng rộng. Router thực sự là một máy tính làm nhiệm vụ chọn đường cho các gói tin hướng ra ngoài. Router độc lập về phần cứng và có thể dùng trên các mạng chạy giao thức khác nhau

2. Một số kiểu nối mạng thông dụng và các chuẩn

2.1.Các thành phần thông thường trên một mạng cục bộ

- Các máy chủ cung cấp dịch vụ (server)
- Các máy trạm cho người làm việc (workstation)
- Đường truyền (cáp nối)
- Card giao tiếp giữa máy tính và đường truyền (network interface card)
- Các thiết bị nối (connection device)

Hai yếu tố được quan tâm hàng đầu khi kết nối mạng cục bộ là tốc độ

trong mạng và bán kính mạng. Tên các kiểu mạng dùng theo giao thức CSMA/CD cũng thể hiện điều này. Sau đây là một số kiểu kết nối đó với tốc độ 10 Mb/s khá thông dụng trong thời gian qua và một số thông số kỹ thuật:

Chuẩn IEEE 802.3		
Kiểu	10BASE5	10BASE2 10BASE-T
Kiểu cáp	Cáp đồng trục	Cáp đồng trục Cáp UTP
Tốc độ	10 Mb/s	
Độ dài cáp tối đa từ HUB	500 m/segment	185 m/segment 100 m kể
Số các thực thể truyền thông	100 host /segment	30 host / segment Số cổng của HUB

2.2. Kiểu 10BASE5

Là chuẩn CSMA/CD có tốc độ 10Mb và bán kính 500 m. Kiểu này dùng cáp đồng trục loại thick ethernet (cáp đồng trục béo) với tranceiver. Có thể kết nối vào mạng khoảng 100 máy

Tranceiver: Thiết bị nối giữa card mạng và đường truyền, đóng vai trò là bộ thu-phát.

2.3. Kiểu 10BASE2

Là chuẩn CSMA/CD có tốc độ 10Mb và bán kính 200 m. Kiểu này dùng cáp đồng trục loại thin ethernet với đầu nối BNC. Có thể kết nối vào mạng khoảng 30 máy

Hình1.11: Nối theo chuẩn 10BASE2 với cáp đồng trục và đầu nối BNC

Hình 1.10. Kết nối theo chuẩn 10BASE5

2.4. Kiểu 10BASE-T

Là kiểu nối dùng HUB có các ổ nối kiểu RJ45 cho các cáp UTP. Ta có thể mở rộng mạng bằng cách tăng số HUB, nhưng cũng không được tăng quá nhiều tầng vì hoạt động của mạng sẽ kém hiệu quả nếu độ trễ quá lớn . Hiện nay mô hình phiên bản 100BASE-T, 1000BASE-T bắt đầu được sử dụng nhiều, tốc độ đạt tới 100 Mbps, 1000Mbps

2.5. Kiểu 10BASE-F

Dùng cab quang (Fiber cab), chủ yếu dùng nối các thiết bị xa nhau, tạo dựng đường trục xương sống (backborn) để nối các mạng LAN xa nhau (2-10 km). Hiện nay cũng đã có các phiên bản 100BASE-F và 1000BASE-F với tốc đọ truyền dữ liệu cao hơn 10 và 100 lần

Hình 1.12: Nối mạng theo kiểu 10BASE-T với cáp UTP và HUB

Chương 2
Giới thiệu giao thức TCP/IP

1. Giao thức IP

1.1. Họ giao thức TCP/IP

Sự ra đời của họ giao thức TCP/IP gắn liền với sự ra đời của Internet mà tiền thân là mạng **ARPA**net (**A**dvanced **R**esearch **P**rojects **A**gency) do Bộ Quốc phòng Mỹ tạo ra. Đây là bộ giao thức được dùng rộng rãi nhất vì tính mở

của nó. Hai giao thức được dùng chủ yếu ở đây là **TCP** (**T**ransmission **C**ontrol **P**rotocol) và **IP** (**I**nternet **P**rotocol). Chúng đã nhanh chóng được đón nhận và phát triển bởi nhiều nhà nghiên cứu và các hãng công nghiệp máy tính với mục đích xây dựng và phát triển một mạng truyền thông mở rộng khắp thế giới mà ngày nay chúng ta gọi là Internet.

Đến năm 1981, TCP/IP phiên bản 4 mới hoàn tất và được phổ biến rộng rãi cho toàn bộ những máy tính sử dụng hệ điều hành UNIX. Sau này Microsoft cũng đã đưa TCP/IP trở thành một trong những giao thức căn bản của hệ điều hành Windows 9x mà hiện nay đang sử dụng.

Đến năm 1994, một bản thảo của phiên bản IPv6 được hình thành với sự cộng tác của nhiều nhà khoa học thuộc các tổ chức Internet trên thế giới để cải tiến những hạn chế của IPv4.

Khác với mô hình ISO/OSI tầng liên mạng sử dụng giao thức kết nối mạng "không liên kết" (connectionless) IP, tạo thành hạt nhân hoạt động của Internet. Cùng với các thuật toán định tuyến RIP, OSPF, BGP, tầng liên mạng IP cho phép kết nối một cách mềm dẻo và linh hoạt các loại mạng "vật lý" khác nhau như: Ethernet, Token Ring , X.25...

Giao thức trao đổi dữ liệu "có liên kết" (connection - oriented) TCP được sử dụng ở tầng vận chuyển để đảm bảo tính chính xác và tin cậy việc trao đổi dữ liệu dựa trên kiến trúc kết nối "không liên kết" ở tầng liên mạng IP.

Các giao thức hỗ trợ ứng dụng phổ biến như truy nhập từ xa (telnet), chuyển tệp (FTP), dịch vụ World Wide Web (HTTP), thư điện tử (SMTP), dịch vụ tên miền (DNS) ngày càng được cài đặt phổ biến như những bộ phận cấu thành của các hệ điều hành thông dụng như UNIX (và các hệ điều hành chuyên dụng cùng họ của các nhà cung cấp thiết bị tính toán như AIX của IBM, SINIX của Siemens, Digital UNIX của DEC), Windows9x/NT, Novell Netware,...

1.2. Chức năng chính của giao thức liên mạng IP (v4)

Hình 2.1 Mô hình OSI và mô hình kiến trúc của TCP/IP

Trong cấu trúc bốn lớp của TCP/IP, khi dữ liệu truyền từ lớp ứng dụng cho đến lớp vật lý, mỗi lớp đều cộng thêm vào phần điều khiển của mình để đảm bảo cho việc truyền dữ liệu được chính xác. Mỗi thông tin điều khiển này được gọi là một *header* và được đặt ở trước phần dữ liệu được truyền. Mỗi lớp xem tất cả các thông tin mà nó nhận được từ lớp trên là dữ liệu, và đặt phần thông tin điều khiển *header* của nó vào trước phần thông tin này. Việc cộng thêm vào các *header* ở mỗi lớp trong quá trình truyền tin được gọi là *encapsulation*. Quá trình nhận dữ liệu diễn ra theo chiều ngược lại: mỗi lớp sẽ tách ra phần *header* trước khi truyền dữ liệu lên lớp trên.

Mỗi lớp có một cấu trúc dữ liệu riêng, độc lập với cấu trúc dữ liệu được dùng ở lớp trên hay lớp dưới của nó. Sau đây là giải thích một số khái niệm thường gặp.

Stream là dòng số liệu được truyền trên cơ sở đơn vị số liệu là Byte.

Số liệu được trao đổi giữa các ứng dụng dùng TCP được gọi là *stream*, trong khi dùng UDP, chúng được gọi là *message*.

Mỗi gói số liệu TCP được gọi là *segment* còn UDP định nghĩa cấu trúc dữ liệu của nó là *packet*.

OSI
Application
Presentation
Session
Transprort

Network
Data link
Physical
Application
SMTP FTP TELNET DNS
TCP UDP
IP
ICMP
ARP
IGMP
RARP
Protocols defined by the underlying networks
TCP/IP

Lớp Internet xem tất cả các dữ liệu như là các khối và gọi là *datagram*.
Bộ giao thức TCP/IP có thể dùng nhiều kiểu khác nhau của lớp mạng dưới cùng, mỗi loại có thể có một thuật ngữ khác nhau để truyền dữ liệu.
Phần lớn các mạng kết cấu phần dữ liệu truyền đi dưới dạng các *packets* hay là các *frames*.
Application Stream
Transport Segment/datagram
Internet Datagram
Network Access Frame
Hình 2.2: Cấu trúc dữ liệu tại các lớp của TCP/IP

1.2. Chức năng chính của - Giao thức liên mạng IP(v4)

Trong phần này trình bày về giao thức IPv4 (để cho thuận tiện ta viết IP có nghĩa là đề cập đến IPv4).
Mục đích chính của IP là cung cấp khả năng kết nối các mạng con thành liên mạng để truyền dữ liệu. IP cung cấp các chức năng chính sau:
- Định nghĩa cấu trúc các gói dữ liệu là đơn vị cơ sở cho việc truyền dữ liệu trên Internet.
- Định nghĩa phương thức đánh địa chỉ IP.
- Truyền dữ liệu giữa tầng vận chuyển và tầng mạng .
- Định tuyến để chuyển các gói dữ liệu trong mạng.
- Thực hiện việc phân mảnh và hợp nhất (fragmentation -reassembly) các gói dữ liệu và nhúng / tách chúng trong các gói dữ liệu ở tầng liên kết.

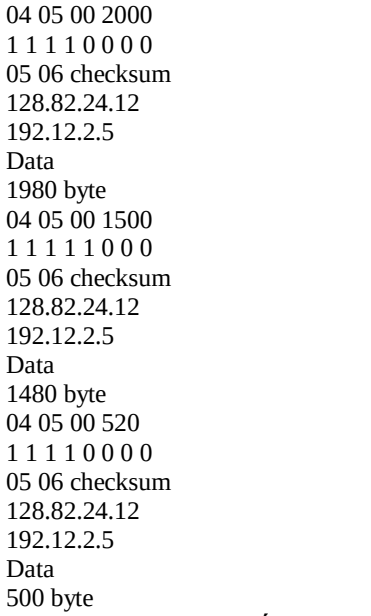
1.3. Địa chỉ IP

Mỗi địa chỉ IP có độ dài 32 bits (đối với IP4) được tách thành 4 vùng (mỗi vùng 1 byte), có thể được biểu thị dưới dạng thập phân, bát phân, thập lục phân hoặc nhị phân. Cách viết phổ biến nhất là dùng ký pháp thập phân có dấu chấm để tách giữa các vùng. Địa chỉ IP là để định danh duy nhất cho một host bất kỳ trên liên mạng.
Khuôn dạng địa chỉ IP: mỗi host trên mạng TCP/IP được định danh duy nhất bởi một địa chỉ có khuôn dạng
<Network Number, Host number>
Do tổ chức và độ lớn của các mạng con của liên mạng có thể khác nhau, người ta chia các địa chỉ IP thành 5 lớp ký hiệu A,B,C, D, E. Các bit đầu tiên của byte đầu tiên được dùng để định danh lớp địa chỉ (0-lớp A; 10 lớp B; 110 lớp C; 1110 lớp D; 11110 lớp E).
Hình 2.3: Cách đánh địa chỉ TCP/IP

Hình 2.5: Cấu trúc gói dữ liệu TCPIP
Subneting
Trong nhiều trường hợp, một mạng có thể được chia thành nhiều mạng con (subnet), lúc đó có thể đưa thêm các vùng subnetid để định danh các mạng con. Vùng subnetid được lấy từ vùng hostid, cụ thể đối với 3 lớp A, B, C như sau:
Hình 2.4: Bổ sung vùng subnetid
Tham khảo chi tiết thêm trong giáo trình "Thiết kế và xây dựng mạng LAN và WAN"
1.4. Cấu trúc gói dữ liệu IP
IP là giao thức cung cấp dịch vụ truyền thông theo kiểu "không liên kết" (connectionless). Các gói dữ liệu IP được định nghĩa là các datagram. Mỗi datagram có phần tiêu đề (header) chứa các thông tin cần thiết để chuyển dữ liệu (ví dụ địa chỉ IP của trạm đích). Nếu địa chỉ IP đích là địa chỉ của một trạm nằm trên cùng một mạng IP với trạm nguồn thì các gói dữ liệu sẽ được chuyển thẳng tới đích; nếu địa chỉ IP đích không nằm trên cùng một mạng IP với máy nguồn thì các gói dữ liệu sẽ được gửi đến một máy trung chuyển, IP gateway để chuyển tiếp. IP gateway là một thiết bị mạng IP đảm nhận việc lưu chuyển các gói dữ liệu IP giữa hai mạng IP khác nhau.
Netid Subnetid hostid Lớp A
Netid Subnetid hostid Lớp B
Netid Subnetid hostid Lớp C
0 7 8 15 16 23 24 31
0 7 8 15 16 23 24 26 27 31
VERS HLEN Service type Toltal length
Identification Flags Fragment offset
Time to live Protocol Header checksum
Source IP address
Destination IP address
IP options (maybe none) Padding
IP datagram data (up to 65535 bytes)
Bit 0 Bit 31
Header

1.5. Phân mảnh và hợp nhất các gói IP
Một gói dữ liệu IP có độ dài tối đa 65536 byte, trong khi hầu hết các tầng liên kết dữ liệu chỉ hỗ trợ các khung dữ liệu nhỏ hơn độ lớn tối đa của gói dữ liệu IP nhiều lần (ví dụ độ dài lớn nhất MTU của một khung dữ liệu Ethernet là 1500 byte). Vì vậy cần thiết phải có cơ chế phân mảnh khi phát và hợp nhất khi thu đối với các gói dữ liệu IP.
Original IP packet 1. fragment 2.fragment
P dùng cờ MF (3 bit thấp của trường Flags trong phần đầu của gói IP) và trường Flagment offset của gói IP (đã bị phân đoạn) để định danh gói IP đó là một phân đoạn và vị trí của phân đoạn này trong gói IP gốc. Các gói cùng trong chuỗi phân mảnh đều có trường này giống nhau. Cờ MF bằng 1 nếu là gói đầu của chuỗi phân mảnh và 0 nếu là gói cuối của gói đã được phân mảnh.
1.6. Định tuyến IP
Có hai loại định tuyến:
- Định tuyến trực tiếp: Định tuyến trực tiếp là việc xác định đường nối giữa hai trạm làm việc trong cùng một mạng vật lý.
- Định tuyến không trực tiếp. Định tuyến không trực tiếp là việc xác định

đường nối giữa hai trạm làm việc không nằm trong cùng một mạng vật lý và vì vậy, việc truyền tin giữa chúng phải được thực hiện thông qua các trạm trung gian là các gateway.
Để kiểm tra xem trạm đích có nằm trên cùng mạng vật lý với trạm nguồn hay không, người gửi phải tách lấy phần địa chỉ mạng trong phần địa chỉ IP. Nếu hai địa chỉ này có địa chỉ mạng giống nhau thì datagram sẽ được truyền đi trực tiếp; ngược lại phải xác định một gateway, thông qua gateway này chuyển tiếp các datagram.



Hình 2.6: Nguyên tắc phân mảnh gói dữ liệu

2. Một số giao thức điều khiển

2.1. Giao thức ICMP

ICMP ((Internet Control Message Protocol) là một giao thức điều khiển của mức 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 bộ giao thức TCP/IP. Ví dụ:
- Điều khiển lưu lượng dữ liệu (Flow control).
- Thông báo lỗi : ví dụ "Destination Unreachable".
- Định hướng lại các tuyến đường: gói tin redirect
- Kiểm tra các trạm ở xa: gói tin echo

Ví dụ khuôn dạng của thông điệp ICMP redirect như sau:

2.2. Giao thức ARP và giao thức RARP

Trên một mạng cục bộ hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau. Như vậy vấn đề đặt ra là phải thực hiện ánh xạ giữa địa chỉ IP (32 bits) và địa chỉ vật lý (48 bits) của một trạm. Giao thức ARP (Address Resolution Protocol) đã được xây dựng để chuyển đổi từ địa chỉ IP sang địa chỉ vật lý khi cần thiết. Ngược lại, giao thức RARP (Reverse Address

Network
Access Internet
Network
Gateway Gateway
Network A Network B Network C
Host A1 Host C1
Hình 2.7: Định tuyến giữa hai hệ thống
0 7 8 15 16 31
type (5) Code(0-3) Checksum
Địa chỉ IP của Router mặc định
IP header (gồm option) và 8 bytes đầu của gói dữ liệu IP nguồn

Resolution Protocol) được dùng để chuyển đổi địa chỉ vật lý sang địa chỉ IP. Các giao thức ARP và RARP không phải là bộ phận của IP mà IP sẽ dùng đến chúng khi cần.

3. Giao thức lớp chuyển tải (Transport Layer)

3.1. Giao thức TCP

TCP (Transmission Control Protocol) là một giao thức "có liên kết" (connection - oriented), nghĩa là cần thiết lập liên kết (logic), giữa một cặp thực thể TCP trước khi chúng trao đổi dữ liệu với nhau.

TCP cung cấp khả năng truyền dữ liệu một cách an toàn giữa các máy trạm trong hệ thống các mạng. Nó cung cấp thêm các chức năng nhằm kiểm tra tính chính xác của dữ liệu khi đến và bao gồm cả việc gửi lại dữ liệu khi có lỗi xảy ra. TCP cung cấp các chức năng chính sau:

1. Thiết lập, duy trì, kết thúc liên kết giữa hai quá trình.
2. Phân phát gói tin một cách tin cậy.
3. Đánh số thứ tự (sequencing) các gói dữ liệu nhằm truyền dữ liệu một cách tin cậy.
4. Cho phép điều khiển lỗi.
5. Cung cấp khả năng đa kết nối với các quá trình khác nhau giữa trạm nguồn và trạm đích nhất định thông qua việc sử dụng các cổng.
6. Truyền dữ liệu sử dụng cơ chế song công (full-duplex).

3.1.1 Cấu trúc gói dữ liệu TCP

0 31
Source port Destination port
Sequence number
Acknowledgment number
Data Resersed U A P R S F
Offset R C S S Y I Window
G K H T N N
Checksum Urgent pointer
Options Padding
TCP data

Có thể tham khảo nội dung chi tiết các trường trong giáo trình "Thiết kế và xây dựng mạng LAN và WAN"

Một tiến trình ứng dụng trong một host truy nhập vào các dịch vụ của TCP cung cấp thông qua một cổng (port) như sau:

Một cổng kết hợp với một địa chỉ IP tạo thành một socket duy nhất trong liên mạng. TCP được cung cấp nhờ một liên kết logic giữa một cặp

socket. Một socket có thể tham gia nhiều liên kết với các socket ở xa khác nhau. Trước khi truyền dữ liệu giữa hai trạm cần phải thiết lập một liên kết TCP giữa chúng và khi kết thúc phiên truyền dữ liệu thì liên kết đó sẽ được giải phóng. Cũng giống như ở các giao thức khác, các thực thể ở tầng trên sử dụng TCP thông qua các hàm dịch vụ nguyên thuỷ (service primitives), hay còn gọi là các lời gọi hàm (function call).

3.1.2 Thiết lập và kết thúc kết nối TCP

Thiết lập kết nối

Thiết lập kết nối TCP được thực hiện trên cơ sở phương thức bắt tay ba bước (Tree - way Handsake) hình sau. Yêu cầu kết nối luôn được tiến trình trạm khởi tạo, bằng cách gửi một gói TCP với cờ SYN=1 và chứa giá trị khởi tạo số tuần tự ISN của client. Giá trị ISN này là một số 4 byte không dấu và được tăng mỗi khi kết nối được yêu cầu (giá trị này quay về 0 khi nó tới giá trị 2_{32}). Trong thông điệp SYN này còn chứa số hiệu cổng TCP của phần mềm dịch vụ mà tiến trình trạm muốn kết nối (bước 1).

Mỗi thực thể kết nối TCP đều có một giá trị ISN mới số này được tăng theo thời gian. Vì một kết nối TCP có cùng số hiệu cổng và cùng địa chỉ IP được dùng lại nhiều lần, do đó việc thay đổi giá trị INS ngăn không cho các kết nối dùng lại các dữ liệu đã cũ (stale) vẫn còn được truyền từ một kết nối cũ và có cùng một địa chỉ kết nối.

Khi thực thể TCP của phần mềm dịch vụ nhận được thông điệp SYN, nó gửi lại gói SYN cùng giá trị ISN của nó và đặt cờ ACK=1 trong trường hợp sẵn sàng nhận kết nối. Thông điệp này còn chứa giá trị ISN của tiến trình trạm trong trường hợp số tuần tự thu để báo rằng thực thể dịch vụ đã nhận được giá trị ISN của tiến trình trạm (bước 2).

Tiến trình trạm trả lời lại gói SYN của thực thể dịch vụ bằng một thông báo trả lời ACK cuối cùng. Bằng cách này, các thực thể TCP trao đổi một cách tin cậy các giá trị ISN của nhau và có thể bắt đầu trao đổi dữ liệu. Không có thông điệp nào trong ba bước trên chứa bất kỳ dữ liệu gì; tất cả thông tin trao đổi đều nằm trong phần tiêu đề của thông điệp TCP (bước 3).

Hình 2.8: Quá trình kết nối theo 3 bước

Kết thúc kết nối

Khi có nhu cầu kết thúc kết nối, thực thể TCP, ví dụ cụ thể A gửi yêu cầu kết thúc kết nối với FIN=1. Vì kết nối TCP là song công (full-duplex) nên mặc dù nhận được yêu cầu kết thúc kết nối của A (A thông báo hết số liệu gửi) thực thể B vẫn có thể tiếp tục truyền số liệu cho đến khi B không còn số liệu để gửi và thông báo cho A bằng yêu cầu kết thúc kết nối với FIN=1 của mình. Khi thực thể TCP đã nhận được thông điệp FIN và sau khi đã gửi thông điệp FIN của chính mình, kết nối TCP thực sự kết thúc.

TCP_A
TCP_B
Syn, Seq=x
Syn, Seq=y
Ack(x+1)
Ack(y+1)
a) thiết lập kết nối
TCP_A
TCP_B
Fin, Seq=x
Ack(x+1)
Fin, Seq=y,

Ack(x+1)
Ack(y+1)
b) Kết thúc kết nối

PHẦN II : QUẢN TRỊ MẠNG

Quản trị mạng lưới (network administration) được định nghĩa là các công việc quản lý mạng lưới bao gồm cung cấp các dịch vụ hỗ trợ, đảm bảo mạng lưới hoạt động hiệu quả, đảm bảo chất lượng mạng lưới cung cấp đúng như chỉ tiêu định ra.

Quản trị hệ thống (system administration) được định nghĩa là các công việc cung cấp các dịch vụ hỗ trợ, đảm bảo sự tin cậy, nâng cao hiệu quả hoạt động của hệ thống, và đảm bảo chất lượng dịch vụ cung cấp trên hệ thống đúng như chỉ tiêu định ra.

Một định nghĩa khái quát về công tác quản trị mạng là rất khó vì tính bao hàm rộng của nó. Quản trị mạng theo nghĩa mạng máy tính có thể được hiểu khái quát là tập bao gồm của các công tác quản trị mạng lưới và quản trị hệ thống.

Có thể khái quát công tác quản trị mạng bao gồm các công việc sau:

Quản trị cấu hình, tài nguyên mạng : Bao gồm các công tác quản lý kiểm soát cấu hình, quản lý các tài nguyên cấp phát cho các đối tượng sử dụng khác nhau. Có thể tham khảo các công việc quản trị cụ thể trong các tài liệu, giáo trình về quản trị hệ thống windows, linux, novell netware ...

Quản trị người dùng, dịch vụ mạng: Bao gồm các công tác quản lý người sử dụng trên hệ thống, trên mạng lưới và đảm bảo dịch vụ cung cấp có độ tin cậy cao, chất lượng đảm bảo theo đúng các chỉ tiêu đề ra. Có thể tham khảo các tài liệu, giáo trình quản trị hệ thống windows, novell netware, linux, unix, quản trị dịch vụ cơ bản thư tín điện tử, DNS...

Quản trị hiệu năng, hoạt động mạng : Bao gồm các công tác quản lý, giám sát hoạt động mạng lưới, đảm bảo các thiết bị, hệ thống, dịch vụ trên mạng hoạt động ổn định, hiệu quả. Các công tác quản lý, giám sát hoạt động của mạng lưới cho phép người quản trị tổng hợp, dự báo sự phát triển mạng lưới, dịch vụ, các điểm yếu, điểm mạnh của toàn mạng, các hệ thống và dịch vụ đồng thời giúp khai thác toàn bộ hệ thống mạng với hiệu suất cao nhất. Có thể tham khảo các tài liệu, giáo trình về các hệ thống quản trị mạng NMS, HP Openview, Sunet Manager, hay các giáo trình nâng cao hiệu năng hoạt động của hệ thống (performance tuning).

Quản trị an ninh, an toàn mạng: Bao gồm các công tác quản lý, giám sát mạng lưới, các hệ thống để đảm bảo phòng tránh các truy nhập trái phép, có tính phá hoại các hệ thống, dịch vụ, hoặc mục tiêu đánh cắp thông tin quan trọng của các tổ chức, công ty hay thay đổi nội dung cung cấp lên mạng với dụng ý xấu. Việc phòng chống, ngăn chặn sự lây lan của các loại virus máy tính, các phương thức tấn công ví dụ như DoS làm tê liệt hoạt động mạng hay

dịch vụ cũng là một phần cực kỳ quan trọng của công tác quản trị an ninh, an toàn mạng. Đặc biệt, hiện nay khi nhu cầu kết nối ra mạng Internet trở nên thiết yếu thì các công tác đảm bảo an ninh, an toàn được đặt lên hàng đầu, đặc biệt là với các cơ quan cần bảo mật nội dung thông tin cao độ (nhà băng, các cơ quan lưu trữ, các các báo điện tử, tập đoàn kinh tế mũi nhọn...).

Trong phần 2 của giáo trình này sẽ tập trung nghiên cứu sâu về một số

kiến thức, kỹ năng cơ bản và thông dụng nhất về quản trị mạng. Tuy nhiên, các nội dung trình bày tại phần 2 sẽ không bao hàm hết được các nội dung đã khái quát ở trên do sự phức tạp phong phú của bản thân mỗi nội dung cũng như giới hạn về thời gian biên soạn. Với mục tiêu cung cấp các kỹ năng phổ biến nhất giúp cho các học viên tiếp cận nhanh chóng vào công tác quản trị mạng để đảm đương được nhiệm vụ cơ quan, công ty giao cho. Phần 2 của giáo trình sẽ bao gồm :

- Tổng quan về bộ định tuyến trên mạng
- Hệ thống tên miền DNS
- Dịch vụ truy cập từ xa và dịch vụ proxy
- Firewall và bảo mật hệ thống

Học viên cũng có thể tham khảo bổ sung thêm kiến thức về quản trị mạng với các giáo trình về mạng cục bộ, giáo trình về thư tín điện tử, giáo trình về các hệ điều hành Windows, Linux, Unix là các nội dung biên soạn trong bộ các giáo trình phục vụ đào tạo cho đề án 112.

Chương 3
Tổng quan về bộ định tuyến

Chương ba cung cấp các kiến thức cơ bản về bộ định tuyến trên mạng và các bộ chuyển mạch lớp 3. Các thiết bị này là một phần thiết yếu của mạng máy tính hiện đại và là các thiết bị hạ tầng cốt lõi. Các minh họa tường tận về cấu trúc của các sản phẩm hãng Cisco sẽ giúp học viên nắm vững các lý thuyết hệ thống đặc biệt là lý thuyết định tuyến. Phần nội dung cũng bổ sung các kỹ năng cấu hình hoạt động của thiết bị trên các giao thức mạng WAN khác nhau như Frame Relay, X.25...

Chương ba đòi hỏi các học viên cần có các kiến thức sơ khởi về các giao thức trên mạng diện rộng như Frame Relay, X.25..., các kiến thức về địa chỉ lớp 2, lớp 3.

1. Lý thuyết về bộ định tuyến

1.1. Tổng quan về bộ định tuyến

Bộ định tuyến là thiết bị được sử dụng trên mạng để thực thi các hoạt động xử lý truyền tải thông tin trên mạng. Có thể xem bộ định tuyến là một thiết bị máy tính được thiết kế đặc biệt để đảm đương được vai trò xử lý truyền tải thông tin trên mạng của nó và do đó nó cũng bao gồm các CPU, trái tim của mọi hoạt động, bộ nhớ ROM, RAM, các giao tiếp, các bus dữ liệu, hệ điều hành v.v...

Chức năng của bộ định tuyến là định hướng cho các gói tin được truyền tải qua bộ định tuyến. Trên cơ sở các thuật toán định tuyến, thông tin cấu hình và chuyển giao, các bộ định tuyến sẽ quyết định hướng đi tốt nhất cho các gói tin được truyền tải qua nó. Bộ định tuyến còn có vai trò để xử lý các nhu cầu truyền tải và chuyển đổi giao thức khác.

Vai trò của bộ định tuyến trên mạng là đảm bảo các kết nối liên thông giữa các mạng với nhau, tính toán và trao đổi các thông tin liên mạng làm căn cứ cho các bộ định tuyến ra các quyết định truyền tải thông tin phù hợp với cấu hình thực tế của mạng. Bộ định tuyến làm việc với nhiều công nghệ đấu nối mạng diện rộng khác nhau như FRAME RELAY, X.25, ATM, SONET, ISDN, xDSL... đảm bảo các nhu cầu kết nối mạng theo nhiều các công nghệ và độ chuẩn mực khác nhau mà nếu thiếu vai trò của bộ định tuyến thì không thể thực hiện được.

1.2. Các chức năng chính của bộ định tuyến, tham chiếu mô hình OSI

Mô hình OSI đã được học ở chương 1 gồm 7 lớp trong đó bao gồm:
- 3 lớp thuộc về các lớp ứng dụng
o lớp ứng dụng

o lớp trình bày
o lớp phiên
- 4 lớp thuộc về các lớp truyền thông
o lớp vận chuyển
o lớp mạng
o lớp liên kết dữ liệu
o lớp vật lý
Đối với các lớp truyền thông:
- Lớp vận chuyển: phân chia / tái thiết dữ liệu thành các dòng chảy dữ liệu. Các chức năng chính bao gồm điều khiển dòng dữ liệu, đa truy nhập, quản lý các mạch ảo, phát hiện và sửa lỗi. TCP, UDP là hai giao thức thuộc họ giao thức Internet (TCP/IP) thuộc về lớp vận chuyển này.
- Lớp mạng: cung cấp hoạt động định tuyến và các chức năng liên quan khác cho phép kết hợp các môi trường liên kết dữ liệu khác nhau lại với nhau cùng tạo nên mạng thống nhất. Các giao thức định tuyến hoạt động trong lớp mạng này.
- Lớp liên kết dữ liệu: cung cấp khả năng truyền tải dữ liệu từ qua môi trường truyền dẫn vật lý. Mỗi đặc tả khác nhau của lớp liên kết dữ liệu sẽ có các định nghĩa khác nhau về giao thức và các chuẩn mực kết nối đảm bảo truyền tải dữ liệu.
- Lớp vật lý: định nghĩa các thuộc tính điện, các chức năng, thường trình dùng để kết nối các thiết bị mạng ở mức vật lý. Một số các thuộc tính được định nghĩa như mức điện áp, đồng bộ, tốc độ truyền tải vật lý, khoảng cách truyền tải cho phép...
Trong môi trường truyền thông, các thiết bị truyền thông giao tiếp với nhau thông qua các họ giao thức truyền thông khác nhau được xây dựng dựa trên các mô hình chuẩn OSI nhằm đảm bảo tính tương thích và mở rộng. Các giao thức truyền thông thường được chia vào một trong bốn nhóm: các giao thức mạng cục bộ, các giao thức mạng diện rộng, giao thức mạng và các giao thức định tuyến. *Giao thức mạng cục bộ* hoạt động trên lớp vật lý và lớp liên kết dữ liệu. *Giao thức mạng diện rộng* hoạt động trên 3 lớp dưới cùng trong mô hình OSI. *Giao thức định tuyến* là giao thức lớp mạng và đảm bảo cho các hoạt động định tuyến và truyền tải dữ liệu. *Giao thức mạng* là các họ các giao thức cho phép giao tiếp với lớp ứng dụng.
Vai trò của bộ định tuyến trong môi trường truyền thông là đảm bảo cho các kết nối giữa các mạng khác nhau với nhiều giao thức mạng, sử dụng các công nghệ truyền dẫn khác nhau.
Chức năng chính của bộ định tuyến là:
- Định tuyến (routing)
- Chuyển mạch các gói tin (packet switching)

Định tuyến là chức năng đảm bảo gói tin được chuyển chính xác tới địa chỉ cần đến. *Chuyển mạch các gói tin* là chức năng chuyển mạch số liệu, truyền tải các gói tin theo hướng đã định trên cơ sở các định tuyến được đặt ra. Như vậy, trên mỗi bộ định tuyến, ta phải xây dựng một bảng định tuyến, trên đó chỉ rõ địa chỉ cần đến và đường đi cho nó. Bộ định tuyến dựa vào địa chỉ của gói

tin kết hợp với bảng định tuyến để chuyển gói tin đi đúng đến đích. Các gói tin không có đúng địa chỉ đích trên bảng định tuyến sẽ bị huỷ.
Chức năng đầu tiên của bộ định tuyến là chức năng định tuyến như tên gọi của nó cũng là chức năng chính của bộ định tuyến làm việc với các *giao thức định tuyến*. Bộ định tuyến được xếp vào các thiết bị mạng làm việc ở lớp 3, lớp mạng.
Bảng 3-1:Tương đương chức năng thiết bị trong mô hình OSI
Lớp 3 Lớp mạng
Lớp 2 Lớp liên kết dữ liệu
Lớp 1 Lớp vật lý
Chức năng khác của bộ định tuyến là cho phép sử dụng các phương thức truyền thông khác nhau để đấu nối diện rộng. Chức năng kết nối diện rộng WAN của bộ định tuyến là không thể thiếu để đảm bảo vai trò kết nối truyền thông giữa các mạng với nhau. Chức năng kết nối mạng cục bộ, bất kỳ bộ định tuyến nào cũng cần có chức năng này để đảm bảo kết nối đến vùng dịch vụ của mạng. Bộ định tuyến còn có các chức năng đảm bảo hoạt động cho các giao thức mạng mà nó quản lý.

1.3. Cấu hình cơ bản và chức năng của các bộ phận của bộ định tuyến

Như đã nói ở phần trước, bộ định tuyến là một thiết bị máy tính được thiết kế đặc biệt để đảm đương được vai trò xử lý truyền tải thông tin trên mạng. Nó được thiết kế bao gồm các phần tử không thể thiếu như CPU, bộ nhớ ROM, RAM, các bus dữ liệu, hệ điều hành. Các phần tử khác tùy theo nhu cầu sử dụng có thể có hoặc không bao gồm các giao tiếp, các module và các tính năng đặc biệt của hệ điều hành.
CPU: điều khiển mọi hoạt động của bộ định tuyến trên cơ sở các hệ thống chương trình thực thi của hệ điều hành.
ROM: chứa các chương trình tự động kiểm tra và có thể có thành phần cơ bản nhất sao cho bộ định tuyến có thể thực thi được một số hoạt động tối thiểu ngay cả khi không có hệ điều hành hay hệ điều hành bị hỏng.
RAM: giữ các bảng định tuyến, các vùng đệm, tập tin cấu hình khi chạy, các thông số đảm bảo hoạt động của bộ định tuyến khác.
Flash: là thiết bị nhớ / lưu trữ có khả năng xoá và ghi được, không mất dữ liệu khi cắt nguồn. Hệ điều hành của bộ định tuyến được chứa ở đây. Tùy thuộc các bộ định tuyến khác nhau, hệ điều hành sẽ được chạy trực tiếp từ

Flash hay được giãn ra RAM trước khi chạy. Tập tin cấu hình cũng có thể được lưu trữ trong Flash.
Hệ điều hành: đảm đương hoạt động của bộ định tuyến. Hệ điều hành của các bộ định tuyến khác nhau có các chức năng khác nhau và thường được thiết kế khác nhau. Mỗi bộ định tuyến có thể chạy rất nhiều hệ điều hành khác nhau tùy thuộc vào nhu cầu sử dụng cụ thể, các chức năng cần thiết phải có của bộ định tuyến và các thành phần phần cứng có trong bộ định tuyến. Các thành phần phần cứng mới yêu cầu có sự nâng cấp về hệ điều hành. Các tính năng đặc biệt được cung cấp trong các bản nâng cấp riêng của hệ điều hành.
Các giao tiếp: bộ định tuyến có nhiều các giao tiếp trong đó chủ yếu bao gồm:
- Giao tiếp WAN: đảm bảo cho các kết nối diện rộng thông qua các phương thức truyền thông khác nhau như leased-line, Frame Relay, X.25, ISDN, ATM, xDSL ... Các giao tiếp WAN cho phép bộ định tuyến kết nối theo nhiều các giao diện và tốc độ khác nhau: V.35, X.21, G.703, E1, E3, cáp quang v.v...

- Giao tiếp LAN: đảm bảo cho các kết nối mạng cục bộ, kết nối đến các vùng cung cấp dịch vụ trên mạng. Các giao tiếp LAN thông dụng: Ethernet, FastEthernet, GigaEthernet, cáp quang.

2. Giới thiệu về bộ định tuyến Cisco

2.1. Giới thiệu bộ định tuyến Cisco

Sơ lược về bộ định tuyến

Bộ định tuyến Cisco bao gồm nhiều nền tảng phần cứng khác nhau được thiết kế xây dựng cho phù hợp với nhu cầu và mục đích sử dụng của các giải pháp khác nhau.

Các chức năng xử lý hoạt động của bộ định tuyến Cisco dựa trên nền tảng cốt lõi là hệ điều hành IOS.

Tuỳ theo các nhu cầu cụ thể mà một bộ định tuyến Cisco sẽ cần một IOS có các tính năng phù hợp. IOS có nhiều phiên bản khác nhau, một số loại phần cứng mới được phát triển chỉ có thể được hỗ trợ bởi các IOS phiên bản mới nhất.

Các thành phần cấu thành bộ định tuyến

Hình 3.1:Các thành phần của bộ định tuyến Cisco

- RAM: Giữ bảng định tuyến, ARP Cache, fast-switching cache, packet buffer, và là nơi chạy các file cấu hình cho bộ định tuyến. Đây chính là nơi lưu giữ file Running-Config, chứa cấu hình đang hoạt động của Router. Khi ngừng cấp nguồn cho bộ định tuyến, bộ nhớ này sẽ tự động giải phóng. Tất cả các thông tin trong file Running-Config sẽ bị mất hoàn toàn.
- NVRAM: non-volatile RAM, là nơi giữ startup/backup configure, không bị mất thông tin khi mất nguồn vào. File Startup-Config được lưu trong này để đảm bảo khi khởi động lại, cấu hình của bộ định tuyến sẽ được tự động đưa về trạng thái đã lưu giữ trong file. Vì vậy, phải thường xuyên lưu file Running-Config thành file Startup-Config.
- Flash: Là ROM có khả năng xoá, và ghi đọc. Là nơi chứa hệ điều hành IOS của bộ định tuyến. Khi khởi động, bộ định tuyến sẽ tự đọc ROM để nạp IOS trước khi nạp file Startup-Config trong NVRAM.
- ROM: Chứa các chương trình tự động kiểm tra.
- Cổng Console: Được sử dụng để cấu hình trực tiếp bộ định tuyến. Tốc độ dữ liệu dùng cho cấu hình bằng máy tính qua cổng COM là 9600b/s. Giao diện ra của cổng này là RJ45 female.
- Cổng AUX: Được sử dụng để quản lý và cấu hình cho bộ định tuyến thông qua modem dự phòng cho cổng Console. Giao diện ra của cổng này cũng là RJ45 female.
- Các giao diện:
  - o Cổng Ethernet / Fast Ethernet
  - o Cổng Serial
  - o Cổng ASYNC ...

2.2. Một số tính năng ưu việt của bộ định tuyến Cisco

- Có khả năng tích hợp nhiều chức năng xử lý trên cùng một sản phẩm với việc sử dụng các module chức năng thích hợp và IOS thích hợp.
- Dễ dàng trong việc nâng cấp bộ định tuyến Cisco cả về phần mềm lẫn phần cứng do đó dễ dàng đáp ứng các nhu cầu thay đổi, mở rộng mạng, đáp ứng các nhu cầu phát triển và ứng dụng công nghệ mới.
- Tương thích và dễ dàng mở rộng cho các nhu cầu về đa dịch vụ ngày càng gia tăng trên.
- Tính bền vững, an toàn và bảo mật.

2.3. Một số bộ định tuyến Cisco thông dụng

Bộ định tuyến Cisco 2500

- Bộ định tuyến Cisco 2509
- 01 cổng console, 01 AUX
- 02 cổng serial tốc độ tới 2Mbps: kết nối leased-line, X.25, Frame Relay...

- 01 Ethernet tốc độ 10Mbps giao diện AUI: cần thiết có đầu chuyển RJ45/AUI khi kết nối vào các mạng switch/hub thông thường.

Hình 3.2: Bộ định tuyến Cisco 2501

- 01 cổng Async cho phép kết nối đến 08 modem V34/V90. Sử dụng môt cáp kết nối Octal để kết nối các modem đến bộ định tuyến.
- Bộ định tuyến Cisco 2501
- 01 cổng console, 01 AUX
- 02 cổng serial tốc độ tới 2Mbps: kết nối leased-line, X.25, Frame Relay...
- 01 Ethernet tốc độ 10Mbps giao diện AUI: cần thiết có đầu chuyển RJ45/AUI khi kết nối vào các mạng switch/hub thông thường

Cisco đã ngừng sản xuất các bộ định tuyến Cisco dòng 2500.

Bộ định tuyến Cisco 1600

Hình 3.3: Bộ định tuyến Cisco 1601

- Bộ định tuyến Cisco 1601
- 01 cổng console
- 01 cổng serial tốc độ tới 2Mbps: kết nối leased-line, X.25, Frame Relay...
- 01 Ethernet tốc độ 10Mbps giao diện AUI và RJ48 (Female Socket for RJ45 connector)
- 01 serial slot: có thể sử dụng cho cổng Serial thứ 2, card ISDN BRI

Hình 3.4: Bộ định tuyến Cisco 1603

- Bộ định tuyến Cisco 1603
- 01 cổng console
- 01 cổng ISDN BRI giao diện S/T: kết nối ISDN tốc độ 2B+D, khi sử dụng ở Việt nam cần có thêm một bộ tiếp hợp NT1 để đấu nối vào mạng ISDN.
- 01 Ethernet tốc độ 10Mbps giao diện AUI và RJ48 (Female Socket for RJ45 connector)
- 01 serial slot: có thể sử dụng cho cổng Serial, card ISDN BRI

Bộ định tuyến Cisco 1700

Hình 3.5: Bộ định tuyến Cisco 1721

- Bộ định tuyến Cisco 1721
- 01 cổng console, 01 AUX
- 01 FastEthernet tốc độ 10/100Mbps giao diện RJ48 (Female Socket for RJ45 connector)
- 02 WAN slot: có thể sử dụng cho cổng Serial, card ISDN BRI...

Hình 3.6: Bộ định tuyến Cisco 1751

- Bộ định tuyến Cisco 1751
- 01 cổng console, 01 AUX
- 01 FastEthernet tốc độ 10/100Mbps giao diện RJ48 (Female Socket for RJ45 connector)
- 02 WAN slot: có thể sử dụng cho cổng Serial, card ISDN BRI...

- 01 Voice slot: chỉ cho phép cắm các card voice

Bộ định tuyến Cisco 2600

Hình 3.7: Bộ định tuyến Cisco 2610

- Bộ định tuyến Cisco 2610
- 01 cổng console, 01AUX
- 01 Ethernet tốc độ 10Mbps giao diện RJ48 (Female Socket for RJ45 connector)
- 02 serial slot: có thể sử dụng cho cổng Serial, card ISDN BRI, card voice...
- 01 network module slot: có thể sử dụng module Async, Sync/Async, Channelized E1, PRI ...

Hình 3.8: Bộ định tuyến Cisco 2621

- Bộ định tuyến Cisco 2621
- 01 cổng console, 01AUX
- 02 FastEthernet tốc độ 10/100Mbps giao diện RJ48 (Female Socket for RJ45 connector)
- 02 serial slot: có thể sử dụng cho cổng Serial, card ISDN BRI, card voice...
- 01 network module slot: có thể sử dụng module Async, Sync/Async, Channelized E1, PRI ...

Bộ định tuyến Cisco 3600

Hình 3.9: Bộ định tuyến Cisco 3620

- Bộ định tuyến 3620
- 01 cổng console, 01AUX
- PCMCIA slot
- 02 network module slot: có thể sử dụng module Async, Sync/Async, Channelized E1, PRI, Ethernet/FastEthernet, Voice, VPN ...
- Khi kết nối với mạng LAN cần thiết có một Network module có cổng Ethernet/FastEthernet

Hình 3.10: Bộ định tuyến Cisco 3661

- Bộ định tuyến 3661
- 01 cổng console, 01AUX
- PCMCIA slot
- 01 FastEthernet tốc độ 100Mbps
- 06 network module slot: có thể sử dụng module Async, Sync/Async, Channelized E1, PRI, Ethernet/FastEthernet, Voice, VPN ...
- 02 module nguồn, hỗ trợ và dự phòng lẫn nhau, đảm bảo về mặt cung cấp nguồn điện cho bộ định tuyến. Có thể thay thế module nguồn mà không cần phải tắt điện toàn bộ bộ định tuyến.

2.4. Các giao tiếp của bộ định tuyến Cisco

- Cổng Console
  - o Tốc độ có thể 11500Bps, làm việc ở tốc độ 9600Bps
  - o Dùng cho cấu hình cho bộ định tuyến Cisco
  - o Sử dụng cáp Console để kết nối
- Cổng AUX
  - o Tốc độ 11500Bps
  - o Sử dụng cho quản trị/cấu hình từ xa qua modem V34/V90
  - o Có thể sử dụng để cấu hình trực tiếp sử dụng cáp Console

o Chỉ làm việc sau khi bộ định tuyến Cisco đã khởi động hoàn toàn

o Có thể cấu hình để AUX làm việc như một đường kết nối dự phòng
- Ethernet/FastEthernet
o Tốc độ 10Mbps/100Mbps giao diện AUI hoặc RJ45
o Dùng cho đấu nối trực tiếp vào mạng LAN
o Tuân theo các chuẩn của IEEE802.3
- Serial
o Tốc độ kết nối tới 2Mbps
o Dùng cho kết nối mạng WAN
o Có khả năng kết nối theo nhiều chuẩn giao diện khác nhau V35, V24, X21, EIA530... bằng việc sử dụng các cáp nối
- ISDN
o Tốc độ 2B+D
o Dùng cho kết nối mạng ISDN sử dụng cho Dialup Server hoặc kết nối dự phòng
o Có các giao diện U hoặc S/T, giao diện S/T cần thiết có thiết bị NT1 để kết nối vào mạng
- Async
o Giao diện truyền số liệu không đồng bộ
o Dùng cho kết nối với các hệ thống modem V34/V90
o Sử dụng cáp kết nối Async (Octal Cable) để nối tới 08 modem.
Octal cable thường có giao diện RJ45 và cần có chuyển đổi RJ45-DB25 để phù hợp với giao diện của modem

2.5. Kiến trúc module của bộ định tuyến Cisco

Các bộ định tuyến có kiến trúc module

Các bộ định tuyến Cisco thông dụng được giới thiệu ở phần trước hầu hết là có kiến trúc module trừ bộ định tuyến 2500 đã không được tiếp tục sản xuất.
Ngoài các bộ định tuyến có kiến trúc module đã được biết, còn có các bộ định tuyến khác:
- **1600**: 1601, 1602, 1603, 1604, 1605
- **1700**: 1710, 1720, 1721, 1750, 1751, 1760
- **2600**: 2610, 2160XM, 2611, 2611XM, 2612, 2613, 2620, 2620XM, 2621, 2621XM, 2650, 2650XM, 2651, 2651XM, 2691
- **3600**: 3620, 3631, 3640, 3661, 3662
- **3700**: 3725, 3745

Tính tương thích dùng lẫn và thay thế

Các bộ định tuyến có kiến trúc module của Cisco được thiết kế để sử dụng chung một kho các card giao tiếp và module chức năng khác nhau. Các card giao tiếp được sử dụng cho bất kỳ một bộ định tuyến nào có khe cắm tương thích. Tương thích phổ biến nhất là card giao tiếp Serial. Card giao tiếp serial có thể sử dụng trên bất kỳ bộ định tuyến nào. Một số card giao tiếp khác như card voice sẽ yêu cầu về cấu hình phần cứng và phần mềm tối thiểu. Các card giao tiếp được sử dụng cho các bộ định tuyến 1600, 1700 có thể sử dụng cho các bộ định tuyến 2600, 3600.
Bộ định tuyến 2600, 3600, 3700 cho phép sử dụng các module chức năng khác nhau. Một module chức năng có thể chỉ bao gồm một chức năng như

module Async, module Serial, cũng có thể bao gồm nhiều chức năng hay bao gồm các khe cắm cho card giao tiếp khác như module NM-1E- có 01 cổng Ethernet và 02 khe cắm cho bất kỳ một loại card tương thích nào. Việc lựa chọn module tùy thuộc vào nhu cầu sử dụng cụ thể. Các module cùng được sử dụng giữa các bộ định tuyến. Một số module yêu cầu cấu hình tối thiểu về phần cứng và phần mềm. Bộ định tuyến 1600 và 1700 không cho phép sử dụng các module như các bộ định tuyến 2600, 3600.

Một số module thường gặp

Hình 3.11: Module Ethernet/FastEthernet

Bảng 3-2:Một số loại module Ethernet/FastEthernet

Loại module	Số cổng LAN	Số khe cắm WAN
Single-Port Ethernet	1	None
Four-Port Ethernet	4	None
Single-Port Ethernet Mixed Media	1	Two WAN interface card slots
Dual-Port Ethernet Mixed Media	2	Two WAN interface card slots
Single-Port Ethernet and Single-Port Token Ring	1/1	Two WAN interface card slots
Single Port Fast Ethernet	1	None

Hình 3.12: Module Ethernet có khe cắm WAN

Bảng 3-3: Một số loại module có khe cắm WAN

Tên module	Loại module
NM-1FE2W/NM-1FE2W-V2	1 10/100 Ethernet, 2 khe cắm WAN
NM-2FE2W/NM-2FE2W-V2	2 10/100 Ethernet, 2 khe cắm WAN
NM-1FE1R2W	1 10/100 Ethernet, 1 4/16 Token Ring, 2 khe cắm WAN
NM-2W	2 khe cắm WAN

Bảng 3-4: Giới hạn số lượng module trên các bộ định tuyến

	2600	2691	3620	3631	3640	3660	3725	3745
NM-1FE2W/NM-1FE2W-V2	N/A	1	2	N/A	4	6	2	4
NM-2FE2W/NM-2FE2W-V2	N/A	1	2	N/A	4	6	2	4
NM-1FE1R2W	N/A	1	2	N/A	4	6	2	4
NM-2W	1	1	1	N/A	3	6	2	4

Hình 3.13: Module 4 cổng serial

- Module 4 cổng serial
- Hỗ trợ tổng lưu lượng 8Mbps: có thể sử dụng tốc độ tối đa 8Mbps trên một cổng hoặc mỗi 2Mbps cho 4 cổng.
- Kết nối với modem theo các chuẩn V.35, X.21, EIA/TIA-232, EIA/TIA530... sử dụng các cáp phù hợp

- Sử dụng cho đấu nối leased-line, Frame Relay, X.25 ...

Hình 3.14: Module 8 cổng Sync/Async
- Module 8 cổng Sync/Async
- Tốc độ kết nối trên mỗi cổng thấp (tối đa 128Kbps)
- Có thể sử dụng ở hai chế độ đồng bộ và không đồng bộ. Có thể sử dụng cho modem quay số.
- Kết nối với modem theo các chuẩn V.35, X.21, EIA/TIA-232, EIA/TIA530... sử dụng các cáp phù hợp
- Sử dụng cho đấu nối leased-line, Frame Relay, X.25, modem quay số...
Hình 3.15: Module 16 cổng Async
- Module 16 cổng Async
- Kết nối không đồng bộ sử dụng cho modem quay số.
- Kết nối với modem theo các chuẩn EIA/TIA-232 sử dụng cáp Octal

Hình 3.16: Module và card ISDN BRI
Bảng 3-5: Một số loại module ISDN BRI tốc độ 2B+D (128+16Kbps)

Loại module	Mô tả
NM-4B-S/T	4 cổng ISDN BRI giao diện S/T
NM-4B-U	4 cổng ISDN BRI giao diện U (tích hợp bộ tiếp hợp NT1)
NM-8B-S/T	8 cổng ISDN BRI giao diện S/T
NM-8B-U	8 cổng ISDN BRI giao diện U (tích hợp bộ tiếp hợp NT1)

Bảng 3-6: Một số loại card giao tiếp ISDN BRI tốc độ 2B+D (128+16Kbps)

Loại card	Mô tả
WIC-1B-S/T-V2	1 cổng ISDN BRI giao diện S/T
WIC 1B-U-V2	1 cổng ISDN BRI giao diện U (tích hợp bộ tiếp hợp NT1)

Hình 3.17: Card giao tiếp Serial

- Card một và hai cổng giao tiếp Serial
- Kết nối đồng bộ tốc độ đến 2Mbps
- Kết nối với modem theo các chuẩn V.35, X.21, EIA/TIA-232, EIA/TIA530... sử dụng các cáp phù hợp
- Sử dụng cho đấu nối leased-line, Frame Relay, X.25, modem quay số...

3. Cách sử dụng lệnh cấu hình bộ định tuyến

3.1. Giới thiệu giao tiếp dòng lệnh của bộ định tuyến Cisco

Giao tiếp dòng lệnh

Giao tiếp dòng lệnh CLI (Command Line Interface) khác với các giao tiếp đồ họa GUI (Graphic User Interface) là giao tiếp đặc biệt được Cisco thiết kế cho phép người dùng, người quản trị làm việc với các thiết bị của Cisco thông qua các dòng lệnh trực tiếp.

Với giao tiếp dòng lệnh, người dùng, người quản trị có thể trực tiếp xem, cấu hình các thiết bị của Cisco thông qua các lệnh phù hợp. Để có thể sử dụng được giao tiếp dòng lệnh, người dùng phải nắm vững được các lệnh, các tham số lệnh và cách sử dụng các lệnh.

Mỗi thiết bị của Cisco đều có rất nhiều các lệnh, các bộ lệnh đi kèm tuy nhiên người sử dụng, người quản trị không nhất thiết phải hiểu hết toàn bộ các lệnh trong mỗi thiết bị mà chỉ cần hiểu, nắm vững một số lệnh cần thiết cho các mục đích sử dụng cụ thể.

Giao tiếp dòng lệnh của Cisco cung cấp cho người dùng khả năng sử dụng trợ giúp trực tuyến. Điều đó có nghĩa là trong quá trình làm việc với thiết bị thông qua giao tiếp dòng lệnh, người dùng có thể liệt kê các lệnh, xem lại ý nghĩa sử dụng của nó hay thậm chí xem các thông số lệnh.
Lưu ý: khi sử dụng giao tiếp dòng lệnh để cấu hình thiết bị, sau khi lệnh được thực thi (ấn phím Enter) các hoạt động của bộ định tuyến sẽ ảnh hưởng ngay lập tức bởi lệnh thực thi đó. Một cho những ví dụ là khi đang thực hiện cấu hình từ xa thông qua telnet, nếu thay đổi địa chỉ của bộ định tuyến, sẽ lập tức mất kết nối đến bộ định tuyến và chỉ có thể thực hiện cấu hình bộ định tuyến trực tiếp từ cổng console. Điều này có nghĩa cần thiết phải rất cẩn thận và chắc chắn cũng như thực hiện đúng trình tự mỗi khi thực hiện cấu hình bộ định tuyến.
Ví dụ về giao tiếp dòng lệnh như sau:

```
Router#config terminal
Router(config)#interface s0/0
Router(config-if)#encapsolution ppp
Router(config-if)#ip address 192.168.100.5 255.255.255.0
```

Các khả năng thực hiện cấu hình bộ định tuyến Cisco

- Cấu hình bộ định tuyến trực tiếp từ cổng console: là phương pháp sử dụng một cáp console thông qua một phần mềm kết nối trực tiếp cổng COM như HyperTerminal của WINDOWS để truy nhập vào bộ định tuyến sau đó cấu hình bộ định tuyến theo giao thức dòng lệnh. Phương pháp cấu hình này được sử dụng nhiều nhất và trong hầu hết các trường hợp. Các bộ định tuyến sử dụng lần đầu cũng phải được cấu hình bằng phương pháp này.
- Cấu hình bộ định tuyến thông qua truy nhập từ xa telnet: truy nhập từ xa tới bộ định tuyến với telnet chỉ có thể thực hiện được khi bộ định tuyến đã được cấu hình với ít nhất một địa chỉ mạng, có mật khẩu bảo vệ và máy tính sử dụng để cấu hình bộ định tuyến phải có khả năng kết nối được với bộ định tuyến thông qua môi trường mạng. Sau khi kết nối được tới bộ định tuyến, sử dụng giao diện dòng lệnh để cấu hình bộ định tuyến.
- Cấu hình bộ định tuyến sử dụng tập tin cấu hình lưu trữ trên máy chủ TFTP: trong một số trường hợp, tập tin cấu hình cho bộ định tuyến có thể được lưu trữ trên máy chủ TFTP, bộ định tuyến được cấu hình sao cho sau khi khởi động sẽ tìm kiếm tập tin cấu hình trên máy chủ TFTP thay vì sử dụng tập tin cấu hình lưu trữ trong NVRAM. Có thể sử dụng lệnh copy để tải tập tin cấu hình từ máy chủ TFTP về bộ định tuyến.
- Cấu hình bộ định tuyến thông qua giao diện WEB: chỉ thực hiện được sau khi bộ định tuyến đã được cấu hình với địa chỉ IP và cho phép cấu hình qua giao thức http.

Sử dụng giao tiếp dòng lệnh

Để thực hiện việc kết nối máy tính với bộ định tuyến, người ta dùng cáp console của Cisco, một đầu cắm trực tiếp vào cổng CONSOLE của bộ định tuyến, đầu kia cắm vào cổng COM của máy tính, có thể sử dụng các đầu chuyển đổi DB9/RJ45 hoặc DB25/RJ45 khi cần thiết.
Phần mềm giao tiếp giữa máy tính và bộ định tuyến thông dụng nhất là HyperTerminal được cài đặt sẵn trong các phiên bản WINDOWS.

Hình 3.18: Sử dụng HyperTerminal để kết nối đến bộ định tuyến
Chọn đúng cổng COM kết nối với cáp console để tiến hành cài đặt các

thông số làm việc. Tốc độ kết nối thông qua cổng COM của máy tính và cổng CONSOLE của bộ định tuyến là 9600b/s (hình 3.19). Chọn OK, bấm phím Enter, cửa sổ làm việc xuất hiện dấu lớn hơn ">" sau tên của của bộ định tuyến, nghĩa là việc kết nối đã hoàn tất (hình 3-20).

Hình 3.19: Xác lập các tham số cho kết nối

Hình 3.20: Kết nối tới bộ định tuyến thành công

Sau khi đã kết nối thành công, sử dụng các lệnh của bộ định tuyến để xem, kiểm tra, cấu hình và bắt lỗi các hoạt động của bộ định tuyến.

Sử dụng dấu ? để truy cập thông tin trợ giúp

- Đánh dấu ? ngay sát sau câu lệnh chưa hoàn chỉnh sẽ hiện thị các lệnh có thể bắt đầu từ các từ chưa hoàn chỉnh đã gõ
- Đánh dấu ? sau câu lệnh một ký tự trắng sẽ hiển thị các tham số có thể của câu lệnh
- Khi câu lệnh không có sẽ hiển thị một báo lỗi

Sử dụng TAB ngay sát sau câu lệnh chưa hoàn chỉnh sẽ hiển thị câu lệnh hoàn chỉnh

3.2. Làm quen với các chế độ cấu hình

Chế độ người dùng

Bao gồm các tác vụ phổ biến chủ yếu gồm những lệnh kiểm tra trạng thái hoạt động của bộ định tuyến, trạng thái các giao tiếp, các bảng định tuyến v.v... và một số lệnh để kiểm tra kết nối mạng như ping, traceroute, telnet v.v.... Ở chế độ này không được phép thay đổi các cấu hình bộ định tuyến. Chế độ người dùng không cho phép xem xét sâu đến các hoạt động của bộ định tuyến mà trong quá trình khai thác, vận hành, người quản trị phải cần thiết sử dụng chế độ quản trị để thực hiện. Biểu hiện của chế độ người dùng là dấu lớn hơn, >, sau tên bộ định tuyến:

```
Router>
Router>?
Exec commands:
<1-99> Session number to resume
```



```
access-enable Create a temporary Access-List entry
access-profile Apply user-profile to interface
clear Reset functions
connect Open a terminal connection
disable Turn off privileged commands
disconnect Disconnect an existing network connection
enable Turn on privileged commands
exit Exit from the EXEC
----- các lệnh đã được bỏ bớt -----
ping Send echo messages
ppp Start IETF Point-to-Point Protocol (PPP)
resume Resume an active network connection
rlogin Open an rlogin connection
show Show running system information
slip Start Serial-line IP (SLIP)
systat Display information about terminal lines
telnet Open a telnet connection
terminal Set terminal line parameters
traceroute Trace route to destination
tunnel Open a tunnel connection
udptn Open an udptn connection
where List active connections
x28 Become an X.28 PAD
```

x3 Set X.3 parameters on PAD

Chế độ quản trị

Bao gồm hầu hết các lệnh của chế độ người dùng và các lệnh chỉ dành cho người quản trị. Chỉ có thể cấu hình bộ định tuyến ở chế độ này. Trong quá trình khai thác, vận hành, để hiểu rõ hoặc khi có sự cố xảy ra, người quản trị có thể sử dụng các lệnh debug để làm rõ thêm thông tin cần thiết. Đặc trưng cho chế độ quản trị là biểu hiện của dấu thăng, **#**.

Router>en
Password:
Router#
Router#?
Exec commands:
<1-99> Session number to resume
access-enable Create a temporary Access-List entry
access-profile Apply user-profile to interface
access-template Create a temporary Access-List entry
archive manage archive files
bfe For manual emergency modes setting
cd Change current directory

clear Reset functions
clock Manage the system clock
configure Enter configuration mode
connect Open a terminal connection
copy Copy from one file to another
debug Debugging functions (see also 'undebug')
----- các lệnh đã được bỏ bớt -----
traceroute Trace route to destination
tunnel Open a tunnel connection
udptn Open an udptn connection
undebug Disable debugging functions (see also 'debug')
upgrade Upgrade firmware
verify Verify a file
where List active connections
write Write running configuration to memory, network, or terminal
x28 Become an X.28 PAD
x3 Set X.3 parameters on PAD

Chế độ cấu hình toàn cục

Là chế độ cấu hình các tham số toàn cục cho bộ định tuyến.

Có rất nhiều các cấu hình toàn cục như cấu hình tên bộ định tuyến, cấu hình tên và mật khẩu người dùng, cấu hình định tuyến toàn cục, cấu hình danh sách truy nhập v.v... Biểu hiện của chế độ cấu hình toàn cục như sau:

Router#
Router#config terminal
Router(config)#hostname RouterA

Chế độ cấu hình giao tiếp

Chế độ cấu hình giao tiếp là chế độ cấu hình cho các giao tiếp của bộ định tuyến như giao tiếp Serial, giao tiếp Ethernet, giao tiếp Async...

Chế độ cấu hình giao tiếp cho phép người quản trị mạng thiết lập các tham số hoạt động cho mỗi giao tiếp như các giao thức mạng được sử dụng trên giao tiếp, địa chỉ mạng của giao tiếp, gán các danh sách truy nhập cho giao tiếp v.v... Một ví dụ về chế độ cấu hình giao tiếp như sau:

Router#
Router#config terminal
Router(config)#interface s0/0
Router(config-if)#encapsolution ppp
Router(config-if)#ip address 192.168.100.5 255.255.255.0
Router(config-if)#

Chế độ cấu hình định tuyến

Là chế độ cấu hình các tham số cho các giao thức định tuyến. Các giao thức định tuyến được cấu hình độc lập với nhau và đều được thực hiện ở chế độ cấu hình định tuyến như ví dụ sau:

```
Router#
Router#config terminal
Router(config)#router rip
Router(config-router)#network 192.168.0.0
Router(config-if)#
```

Chế độ cấu hình đường kết nối

Chế độ cấu hình đường kết nối là một chế độ cấu hình đặc biệt sử dụng để thiết lập các tham số mức thấp cho giao tiếp logic trong đó điển hình là các tham số thiết lập cho các kết nối modem quay số.

```
Router#config terminal
Router(config)#line 33 48
Router(config-line)#modem inout
Router(config-line)#modem autoconfig discovery
Router(config-line)#
```

Bảng 3-7:Một số chế độ cấu hình và thể hiện

Chế độ cấu hình	Thể hiện
Global	Router(config)#
Interface	Router(config-if)#
Subinterface	Router(config-subif)#
Controller	Router(config-controller)#
Map-list	Router(config-map-list)#
Map-class	Router(config-map-class)#
Line	Router(config-line)#
Router	Router(config-router)#
Route-map	Router(config-route-map)#

3.3. Làm quen với các lệnh cấu hình cơ bản

Enable: dùng để vào chế độ quản trị. Sau khi thực hiện lệnh enable, người dùng phải cung cấp mật khẩu quản trị đúng để thực sự được làm việc ở chế độ quản trị, mật khẩu không được phép nhập sai quá 3 lần.

```
Router>
Router>en
Password:
Password:
Password:
% Bad secrets
Router>en
Password:
Router#
Router#
Router#disa
Router>
```

Disable: thoát khỏi chế độ quản trị về chế độ người dùng.

Setup: thực hiện khởi tạo lại cấu hình của bộ định tuyến ở chế độ cấu hình hội thoại. Sau đây là một ví dụ về sử dụng lệnh setup. Chế độ hội thoại này cũng được thực hiện tự động đối với các bộ định tuyến chưa hề có tập tin cấu hình hay nói cách khác có NVRAM không chứa thông tin.

```
Router#setup
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: y
At any point you may enter a question mark '?' for help.
```

Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system
Would you like to enter basic management setup? [yes/no]: n
First, would you like to see the current interface summary? [yes]: n
Configuring global parameters:
Enter host name [Router]:
The enable secret is a password used to protect access to
privileged EXEC and configuration modes. This password, after
entered, becomes encrypted in the configuration.
Enter enable secret [<Use current secret>]:
The enable password is used when you do not specify an
enable secret password, with some older software versions, and
some boot images.
Enter enable password []:123456

The virtual terminal password is used to protect
access to the router over a network interface.
Enter virtual terminal password: 654321
Configure SNMP Network Management? [yes]:
Community string [public]:
Configure IP? [yes]:
Configure IGRP routing? [yes]: n
Configure RIP routing? [no]:
Configure bridging? [no]:
Async lines accept incoming modems calls. If you will have
users dialing in via modems, configure these lines.
Configure Async lines? [yes]: n
Configuring interface parameters:
Do you want to configure FastEthernet0/0 interface? [yes]: n
Do you want to configure Serial0/0 interface? [yes]: n
Do you want to configure Serial0/1 interface? [no]: y
Some supported encapsulations are
ppp/hdlc/frame-relay/lapb/x25/atm-dxi/smds
Choose encapsulation type [hdlc]: ppp
No serial cable seen.
Choose mode from (dce/dte) [dte]:
Configure IP on this interface? [no]: y
IP address for this interface: 192.168.100.5
Subnet mask for this interface [255.255.255.0] :
Class C network is 192.168.100.0, 24 subnet bits; mask is /24
The following configuration command script was created:
hostname Router
enable secret 5 1EuXV$Yhj/OYkz/U1R5VABqXsMC0
enable password 7 123456
line vty 0 4
password 7 654321
snmp-server community public
!
ip routing
no bridge 1
!
interface FastEthernet0/0
shutdown
no ip address
!
interface Serial0/0
shutdown
no ip address

```
!
interface Serial0/1
no shutdown
encapsulation ppp
ip address 192.168.100.5 255.255.255.0
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
end
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.
```

Config: cho phép thực hiện các lệnh cấu hình bộ định tuyến. Sau lênh config, quản trị mạng mới có thể thực hiện các lệnh cấu hình bộ định tuyến.

Trình tự thực hiện cấu hình cho một bộ định tuyến có thể được thể hiện như sau

- Đặt tên cho bộ định tuyến

```
Router#config terminal
Router(config)#
Router(config)#hostname RouterABC
RouterABC(config)#
```

- Đặt tên mật khẩu bí mật dành cho người quản trị

```
RouterABC(config)#enable secret matkhaubimat
RouterABC(config)#
```

- Đặt tên mật khẩu cho chế độ quản trị. Mật khẩu này chỉ sử dụng khi cấu hình bộ định tuyến không có mật khẩu bí mật dành cho quản trị.

```
RouterABC(config)#enable password matkhau
RouterABC(config)#
```

- Cấu hình cho phép người dùng truy cập từ xa đến bộ định tuyến

```
RouterABC(config)#line vty 0 4
RouterABC(config-line)#login
RouterABC(config-line)#password telnet
RouterABC(config-line)#
```

- Cấu hình các giao tiếp

```
RouterABC(config)#interface ethernet 0
RouterABC(config-if)#ip address 192.168.2.1 255.255.255.0
RouterABC(config-if)#no shutdown
RouterABC(config-if)#
```

- Cấu hình định tuyến

```
RouterABC(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.2
RouterABC(config)#
```


Copy: lệnh copy cho phép thực hiện các sao chép cấu hình của bộ định tuyến đi/đến máy chủ TFTP**,** sao chép, lưu trữ, nâng cấp các tập tin IOS của bộ định tuyến từ / tới máy chủ TFTP.

Để có thể lưu bản sao cấu hình hiện hành lên máy chủ TFTP, sử dụng lệnh *copy rumng-config tftp* như được trình bày ở dưới. Tiếp theo là tiến trình ngược lại với việc tải tập tin cấu hình từ máy chủ TFTP về bộ định tuyến.

- Nhập lệnh *copy runing-config tftp*
- Nhập địa chỉ IP của máy chủ TFTP nơi dùng để lưu tập tin cấu hình
- Nhập tên ấn định cho tập tin cấu hình
- Xác nhận chọn lựa với trả lời yes

Lệnh copy dùng để lưu tập tin cấu hình lên máy chủ:

```
Router#copy running-config tftp
Address or name of remote host []? 192.168.1.5
Name of configuration file to write [Router-config]?cisco.cfg
Write file cisco.cfg to 192.168.1.5? [confirm] y
Writing cisco.cfg !!!!! [OK]
Router#
```

Lệnh copy dùng để tải tập tin cấu hình từ máy chủ:

Router#copy tftp running-config
Address or name of remote host []? 192.168.1.5
Source filename []? cisco.cfg
Destination filename [running-config]?

Show: là lệnh được dùng nhiều và phổ biến nhất.

Lệnh show dùng để xác định trạng thái hiện hành của bộ định tuyến. Các lệnh này giúp cho phép có được các thông tin quan trọng cần biết khi kiểm tra và điều chỉnh các hoạt động của bộ định tuyến.

- show version: hiển thị cấu hình phần cứng hệ thống, phiên bản phần mềm, tên và nguồn của các tập tin cấu hình, và ảnh chương trình khởi động.
- show processes: hiển thị thông tin các quá trình hoạt động của bộ định tuyến.
- show protocols: hiển thị các giao thức được cấu hình.
- show memory: thống kê về bộ nhớ của bộ định tuyến.
- show stacks: giám sát việc sử dụng stack của các quá trình, các thủ tục ngắt và hiển thị nguyên nhân khởi động lại hệ thống lần cuối cùng.
- show buffers: cung cấp thống kê về các vùng bộ đệm trên bộ định tuyến.

- show flash: thể hiện thông tin về bộ nhớ Flash.
- show running-config: hiển thị tập tin cấu hình đang hoạt động của bộ định tuyến.
- show startup-config: hiển thị tập tin cấu hình được lưu trữ trên NVRAM và được đưa vào bộ nhớ để hoạt động khi bật nguồn bộ định tuyến. Thông thường running-config và startup-config là giống nhau. Khi thực hiện các lệnh cấu hình, running-config và startup-config sẽ không còn giống nhau, cấu hình hoạt động (running-config) cần phải được ghi trở lại NVRAM sau khi kết thúc cấu hình bộ định tuyến.
- show interfaces: thống kê các giao tiếp của bộ định tuyến. Đây là một trong các lệnh được sử dụng nhiều nhất cho biết trạng thái hoạt động của các giao tiếp, số liệu thống kê lưu lượng, số lượng các gói tin lỗi v.v...

Hình 3.21: Lệnh show

Router#show interface s0/0
Serial0/0 is up, line protocol is up
Hardware is PowerQUICC Serial
Description: 2M link to the Internet
Internet address is 192.168.100.5/24
MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec,
reliability 255/255, txload 248/255, rxload 84/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/12/0 (size/max/drops/flushes); Total output
drops: 2383688
Queueing strategy: weighted fair
Output queue: 24/1000/64/2383671 (size/max total/threshold/drops)
Conversations 5/184/256 (active/max active/max total)

Reserved Conversations 0/0 (allocated/max allocated)
5 minute input rate 677000 bits/sec, 161 packets/sec
5 minute output rate 1996000 bits/sec, 395 packets/sec
106754998 packets input, 2930909441 bytes, 0 no buffer
Received 68850 broadcasts, 0 runts, 0 giants, 0 throttles
51143 input errors, 30726 CRC, 20248 frame, 0 overrun, 0
ignored, 169 abort

319791176 packets output, 1669977392 bytes, 0 underruns
0 output errors, 0 collisions, 125 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up

Hình 3.22: Lệnh show interface

Router# show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.1(2), RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Tue 09-May-00 23:34 by linda
Image text-base: 0x80008088, data-base: 0x807D2544
ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)
Router uptime is 1 week, 1 day, 1 minute
System returned to ROM by power-on at 13:29:57 Hanoi Thu Jul 31 2003
System restarted at 20:24:22 Hanoi Tue Sep 2 2003
System image file is "flash:c2600-i-mz.121-2.bin"
cisco 2620 (MPC860) processor (revision 0x102) with 26624K/6144K
bytes of memory
.
Processor board ID JAD04340ID8 (2733840160)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
1 FastEthernet/IEEE 802.3 interface(s)
2 Serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)
Configuration register is 0x2102

Hình 3.23: Lệnh show version

Write: lệnh write sử dụng để ghi lại cấu hình hiện đang chạy của bộ định tuyến. Nhất thiết phải dùng lệnh *write memory* để ghi lại cấu hình của bộ định tuyến vào NVRAM mỗi khi có thay đổi về cấu hình.

Router#write ?
erase Erase NV memory
memory Write to NV memory
network Write to network TFTP server
terminal Write to terminal
<cr>

3.4. Cách khắc phục một số lỗi thường gặp

Lỗi kết nối đến cổng console sử dụng Hyper Terminal

- Kiểm tra lại xem đã sử dụng chính xác loại cáp dùng để cấu hình bộ định tuyến chưa. Cáp console dùng để cấu hình bộ định tuyến là cáp 8 sợi có hai đầu RJ45 có sơ đồ đấu nối như bảng 3-8 và sử dụng đầu chuyển đổi DB9/RJ45 được cung cấp kèm theo bộ định tuyến.
- Kiểm tra xem đã sử dụng đúng cổng kết nối COM của máy tính để nối tới bộ định tuyến.

Bảng 3-8: Sơ đồ đấu nối cáp console

Console Cáp console DB9/RJ45 COM
Tín hiệu RJ45 RJ45 DB9 Tín hiệu
RTS 1 8 8 CTS
DTR 2 7 6 DSR
TxD 3 6 2 RxD
GND 4 5 5 GND
GND 5 4 5 GND
RxD 6 3 3 TxD

DSR 7 2 4 DTR
CTS 8 1 7 RTS
- Kiểm tra các tham số kết nối. Tốc độ kết nối phải là 9600 cho kết nối qua cổng console.

Lỗi kết nối sử dụng telnet

Khi sử dụng telnet để cấu hình từ xa bộ định tuyến, người dùng có thể không kết nối được đến bộ định tuyến. Một trong các lỗi sau cần được kiểm tra:
- Máy tính dùng để cấu hình bộ định tuyến không có kết nối mạng với bộ định tuyến. Kiểm tra lại khả năng kết nối mạng từ máy tính đến bộ định tuyến. Có thể dùng lệnh *ping* để kiểm tra.
- Khi cấu hình bộ định tuyến lần đầu, người quản trị mạng đã quên không thiết lập mật khẩu cho truy nhập từ xa. Khi cố gắng truy nhập từ xa, người dùng sẽ nhận được thông báo về việc mật khẩu truy nhập chưa được thiết lập. Trường hợp này cần sử dụng cáp console để thiết lập mật khẩu theo trình tự như trình bày dưới đây:

```
Router#config terminal
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password 123456
Router(config-line)#end
Router#write memory
```

- Kiểm tra về việc có hay không có các hạn chế telnet sử dụng các danh sách kiểm soát truy nhập (access-list).

4. Cấu hình bộ định tuyến Cisco

4.1. Cấu hình leased-line

Giới thiệu leased-line

Leased-line, hay còn được gọi là kênh thuê riêng, là một hình thức kết nối trực tiếp giữa các node mạng sử dụng kênh truyền dẫn số liệu thuê riêng. Kênh truyền dẫn số liệu thuê riêng thông thường cung cấp cho người sử dụng sự lựa chọn trong suốt về giao thức đấu nối hay nói cách khác, có thể sử dụng các giao thức khác nhau trên kênh thuê riêng như PPP, HDLC, LAPB v.v...

Về mặt hình thức, kênh thuê riêng có thể là các đường cáp đồng trực tiếp kết nối giữa hai điểm hoặc có thể bao gồm các tuyến cáp đồng và các mạng truyền dẫn khác nhau. Khi kênh thuê riêng phải đi qua các mạng truyền dẫn khác nhau, các quy định về giao tiếp với mạng truyền dẫn sẽ được quy định bởi nhà cung cấp dịch vụ. Do đó, các thiết bị đầu cuối CSU/DSU cần thiết để kết nối kênh thuê riêng sẽ phụ thuộc và nhà cung cấp dịch vụ. Một số các chuẩn kết nối chính được sử dụng là HDSL, G703, 2B1Q v.v...

Khi sử dụng kênh thuê riêng, người sử dụng cần thiết phải có đủ các giao tiếp trên các bộ định tuyến sao cho có một giao tiếp kết nối WAN cho mỗi một kết nối kênh thuê riêng tại mỗi node. Điều đó có nghĩa là, tại điểm node có kết nối kênh thuê riêng đến 10 điểm khác nhất thiết phải có đủ 10 giao tiếp WAN để phục vụ cho các kết nối kênh thuê riêng. Đây là một vấn đề hạn chế về đầu tư thiết bị ban đầu, không linh hoạt trong mở rộng, phát triển, phức tạp

trong quản lý, đặc biệt là chi phí thuê kênh lớn đối với các yêu cầu kết nối xa về khoảng cách địa lý.

Các giao thức sử dụng với đường lease-line

Hai giao thức sử dụng với leased-line là HDLC, PPP và LAPB. Trong đó:

- HDLC: là giao thức được sử dụng với họ các bộ định tuyến Cisco hay nói cách khác chỉ có thể sử dụng HDLC khi cả hai phía của kết nối leased-line đều là bộ định tuyến Cisco.
- PPP: là giao thức chuẩn quốc tế, tương thích với tất cả các bộ định tuyến của các hãng sản xuất khác nhau. Khi đấu nối kênh leased-line giữa một phía là thiết bị của Cisco và một phía là thiết bị của hãng thứ 3 thì nhất thiết phải dùng giao thức đấu nối này. PPP là giao thức lớp 2 cho phép nhiều giao thức mạng khác nhau có thể chạy trên nó do vậy nó được sử dụng phổ biến.
- LAPB: là giao thức truyền thông lớp hai tương tự như giao thức mạng X.25 với đầy đủ các thủ tục, quá trình kiểm soát truyền dẫn, phát hiện và sửa lỗi. LAPB ít được sử dụng.

Mô hình kết nối lease-line

Ethernet
Server
Workstation
Ethernet
C2621 C3620
Server
Workstation

Cấu hình kết nối lease-line cơ bản

- Phân định địa chỉ
o Việc phân định địa chỉ cho các mạng và cho các kết nối giữa các bộ định tuyến là rất quan trọng, đảm bảo cho việc liên lạc thông suốt giữa các mạng, đảm bảo cho vấn đề qui hoạch địa chỉ, nhóm gọn các định tuyến ...
o Khi thực hiện xây dựng một mạng dùng riêng, điều cần thiết phải ghi nhớ là chỉ được dùng các địa chỉ trong nhóm các địa chỉ dành cho mạng dùng riêng:10.x.x.x, 172.16.x.x – 172.31.x.x, 192.168.x.x
o Để đảm bảo không bị trùng lặp và giảm thiểu các vấn đề phát sinh, các kết nối mạng WAN theo kiểu leased-line cần được sắp xếp trên lớp mạng nhỏ nhất. Các kết nối mạng WAN trong trường hợp này được thực hiện trên các lớp mạng gồm 4 địa chỉ.

o Các lớp mạng khác tuỳ theo yêu cầu cụ thể và số lượng các địa chỉ có thể mà phân chia cho phù hợp.
- Để bắt đầu cấu hình mạng:
o **Router> enable** □
o **Password: ******** □
o **Router# config terminale** □
o **Router(config)#**
- Thực hiện đặt tên, các mật khẩu, cấu hình cho phép telnet và các điều kiện cần thiết trước khi cấu hình các giao diện
- Cấu hình
o **Router2621(config)# interface serial 0** □
- Lựa chọn giao thức sử dụng
o **Router2621(config-if)# encapsolation HDLC** □
- Đặt địa chỉ IP cho giao tiếp kết nối leased-line
o **Router2621(config-if)# ip address 192.168.113.5 255.255.255.252** □
- Luôn phải đưa giao tiếp vào sử dụng bằng lệnh no shutdown
o **Router2621(config-if)# no shutdown** □
o **Router2621(config-if)# interface serial 1** □
- Lựa chọn giao thức PPP sử dụng cho một giao tiếp khác
o **Router2621(config-if)# encapsolation PPP** □
o **Router2621(config-if)# ip address 192.168.113.9 255.255.255.252** □
o **Router2621(config-if)# no shutdown** □
o **Router2621(config-if)# exit** □

- Sử dụng định tuyến tĩnh với cú pháp: ip route [địa chỉ mạng đích] [netmask] [địa chỉ next hop]
o **Router2621(config)# ip route 0.0.0.0 0.0.0.0 192.168.113.6**
- Luôn phải ghi lại cấu hình khi đã cấu hình xong
o **Router2621# write memory**
- Thực hiện các phần việc còn lại tại các bộ định tuyến khác, chú ý về giao thức được sử dụng kiểm tra, giám sát các kết nối.
o Dùng lệnh **show interface** để kiểm tra trạng thái của giao tiếp
o **show interface:** xem trạng thái tất cả các giao tiếp
o **show interface serial 0**: xem trạng thái cổng serial 0
o *Serial 0 is admininistrative down line protocole is down*: thể hiện trạng thái đang bị cấu hình là không làm việc, sử dụng lệnh no shutdown trong Interface mode để đưa giao tiếp serial 0 vào làm việc
o *Serial 0 is down line protocole is down*: kiểm tra lại đường truyền

o *Serial 0 is up line protocole is down*: kiểm tra lại các giao thức được sử dụng tại hai phía
o *Serial 0 is up line protocole is up*: là trạng thái làm việc

Cấu hình bộ định tuyến 2621

```
!
hostname 2621
!
!
interface FastEthernet0/0
ip address 10.0.5.1 255.255.255.0
!
!
interface Serial0/0
ip address 192.168.113.5 255.255.255.252
encapsulation ppp
!
!
ip route 0.0.0.0 0.0.0.0 192.168.113.6
!
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

Hình 3.24: Cấu hình của bộ định tuyến 2621

Cấu hình bộ định tuyến 3620

```
!
hostname 3620
!
!
interface FastEthernet0/0
ip address 10.0.6.1 255.255.255.0
!
!
interface Serial1/0
```



```
ip address 192.168.113.6 255.255.255.252
encapsulation ppp
```

```
!
!
ip route 0.0.0.0 0.0.0.0 192.168.113.5
!
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

Hình 3.25: Cấu hình của bộ định tuyến 3620

4.2. Cấu hình X.25 & Frame Relay

Giới thiệu X.25 và Frame Relay

X25: Năm 1978 ISO thay đổi thêm HDLC và CCITT thêm một số thông số để sinh ra LAPB "Link Access Procedure – Balanced Mode". LAPB định nghĩa một số quy luật cho mức Frame của X.25 như các loại khung đặc biệt như RR (Receive Ready), REJ (Reject) . . .

Hình 3.26: Chuyển mạch gói X.25

X.25 cung cấp các kết nối diện rộng thông qua môi trường chuyển mạch gói. Mỗi thuê bao X.25 có một địa chỉ xác định duy nhất được đánh số gồm các phần mã quốc gia, nhà cung cấp dịch vụ và địa chỉ của thuê bao trực thuộc nhà cung cấp dịch vụ.

Hình 3.27: Cấu trúc địa chỉ X.25

Khi có nhu cầu kết nối truyền dữ liệu, các thiết bị đầu cuối X.25 sẽ phát khởi tạo một VC (virtual circuit) tới địa chỉ đích. Sau khi VC được thiết lập, dữ liệu sẽ được truyền tải giữa hai điểm thông qua VC đó. Nếu nhu cầu dữ liệu lớn hơn, thiết bị đầu cuối sẽ khởi tạo thêm các VC mới. Khi hết giữ liệu, các VC sẽ được giải phóng cho các nhu cầu truyền tải khác.

X.25 qui định một số tham số xác định bao gồm:

- Độ lớn gói tin (ips/ops): là giá trị kích thước gói tin được quy định bởi nhà cung cấp dịch vụ.
- Độ lớn cửa sổ điều khiển luồng (win/wout): X.25 sử dụng cơ chế điều khiển luồng bằng cửa số để đảm bảo tốc độ gửi nhận tin phù hợp không làm mất mát thông tin. Với tham số cửa sổ bằng 7, X.25 cho phép gửi tối đa 7 gói tin khi chưa nhận được phúc đáp.
- Số lượng kênh VC tối đa cho chiều đến/hai chiều/chiều đi (hic/htc/hoc): Số lượng kênh VC được cung cấp cho mỗi thuê bao X.25 đã được xác định bởi nhà cung cấp. Thuê bao chỉ có thể truyền tải dữ liệu với số lượng các VC tối đa cho phép đã được xác định. Không thể thực hiện được yêu cầu truyền tải nếu có yêu cầu truyền tải tới các điểm mới khi số lượng VC đã hết. Khi các thiết bị đầu cuối X.25 thực hiện truyền tải dữ liệu nó phải tuân theo các quy tắc:
  - o Cuộc gọi ra được thực hiện từ VC lớn nhất còn trống. Điều đó có nghĩa là, nếu chưa hề có cuộc gọi nào và số VC được cung cấp cho một thuê bao là 16 thì cuộc gọi ra đầu tiên sẽ khởi tạo VC số 16 để thực hiện yêu cầu kết nối.Trong trường hợp đã dùng hết 3 VC gọi ra thì cuộc gọi ra thứ 4 sẽ sử dụng VC số 13 để thực hiện.
  - o Cuộc gọi tới được thực hiện từ VC nhỏ nhất còn trống. Tương tự như cuộc gọi ra, cuộc gọi vào đầu tiên sẽ nhận được trên VC số 1 và cuộc gọi vào thứ 10 sẽ nhận được trên VC số 10.
  - o Quá trình khởi tạo VC sẽ dừng lại khi không còn VC trống.

o Với các quy tắc này, yêu cầu cần thiết phải xác lập một cách chính xác các tham số cho thiết bị đầu cuối X.25 thì mới có thể thực hiện được các kết nối truyền tải dữ liệu.

Về đặc điểm của X.25

- Tốc độ truyền tải hạn chế, tại Việt Nam tốc độ cung cấp tối đa là 128Kbps.
- Độ trễ lớn, không phù hợp cho các ứng dụng có yêu cầu cao về độ trễ.
- Khả năng mở rộng dễ dàng, chi phí không cao.
- An toàn và bảo mật, vẫn được sử dụng trong các giao dịch ngân hàng.

Frame Relay: Frame Relay ra đời trên nền tảng hạ tầng viễn thông ngày càng được cải thiện, không cần có quá nhiều các thủ tục phát hiện và sửa lỗi như X.25. Frame relay có thể chuyển nhận các khung lớn tới 4096 byte trong khi đó gói tiêu chuẩn của X.25 khuyến cáo dùng là 128 byte. Frame Relay rất thích hợp cho tryền 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.

Bảng 3-9:So sánh giữa X.25 và Frame Relay

TT	Chức năng của mạng X25	Frame relay
1	Phúc đáp khung thông tin nhận được	√
2	Phúc đáp gói tin nhận được	√
3	Dịch địa chỉ của gói tin	√	√
4	Cất giữ gói tin vào vùng đệm để chờ phúc đáp	√
5	Phát hiện gói tin sai thứ tự	√
6	Huỷ gói tin bị lỗi	√	√
7	Đảm bảo khung tin có giá trị N(s) là hợp lệ	√
8	Thiết lập và huỷ bỏ kết nối logical	√
9	Thiết lập và huỷ bỏ kênh ảo	√
10	Điền các bit cờ vào giữa các khung	√
11	Điều khiển luồng dữ liệu ở lớp liên kết logic	√
12	Tạo và kiểm tra FCS	√	√
13	Tạo và nhận dạng bit cờ	√	√
14	Tạo ra khung báo chưa sẵn sàng	√
15	Tạo ra khung báo đã sẵn sàng	√

√16	Tạo ra khung báo khung bị từ chối	√
17	Quản lý các bit D, M, Q trong gói tin	√
18	Quản lý các khung ở mức liên kết dữ liệu	√
19	Quản lý các bộ định thời ở mức 3	√
20	Quản lý các bit Poll/Final trong khung	√
21	Quản lý các bộ đếm số thứ tự của khung và gói tin	√
22	Ghép các kênh logic	√
23	Quản lý các thủ tục khởi động ở mức 2 và 3	√
24	Nhận dạng các khung không hợp lệ	√	√
25	Trả lời các khung và gói tin báo chưa sẵn		

sang
√
26 Trả lời các khung và gói tin báo đã sẵn sàng √
27 Trả lời các khung và gói tin báo từ chối
khung
√
28 Đánh dấu số lần phải truyền lại √
29 Chèn thêm và bỏ các bit 0 vào số liệu √ √
Bảng chức năng trên cho thấy Frame relay đã giảm rất nhiều các công việc không cần thiết cho thiết bị chuyển mạch do đó giảm gánh nặng cũng như thời gian xử lý công việc cho các nút mạng, nhờ vậy mà làm giảm thời gian trễ cho các khung thông tin khi truyền trên mạng.
Hình 3.28: Mô hình mạng 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. 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.
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 cho từng cuộc gọi một mà phân phối băng thông một cách linh hoạt điều mà X.25 và thuê kênh riêng không có. Ví dụ người sử dụng hợp đồng sử dụng với tốc độ 64Kbps, khi họ chuyển đi một lượng thông tin quá lớn, Frame Relay cho phép truyền chúng ở tốc độ cao hơn 64Kbps. Hiện tượng này được gọi là bùng nổ Bursting.
Các đặc điểm của Frame Relay:
- Cung cấp các kết nối thông qua các kênh ảo cố định PVC. Khi có nhu cầu kết nối giữa 2 điểm, nhà cung cấp dịch vụ sẽ thiết lập các thông số trên các node Frame Relay tạo ra các kênh ảo cố định giữa 2 điểm. Không như X.25, hướng kết nối Frame Relay là cố định và không thể khởi tạo bởi người dùng. Khi có nhu cầu kết nối đến điểm đích khác, khách hàng phải thuê mới PVC đến điểm đích mới đó.
- CIR (Committed Information Rate): là tốc độ truyền dữ liệu mà nhà cung cấp dịch vụ cam kết sẽ đảm bảo cho khách hàng, điều đó có nghĩa là khách hàng sẽ được đảm bảo cung cấp đường truyền với đúng tốc độ yêu cầu. CIR được gắn liền với với các PVC và độc lập giữa các PVC khác nhau. Nếu tắc nghẽn xảy ra thì khách hàng vẫn truyền được với tốc độ yêu cầu khi ký kết hợp đồng.
- Frame Relay hỗ trợ truyền số liệu khi có bùng nổ số liệu hay còn gọi là "bursty", có nghĩa là lượng thông tin được gửi đi trong thời gian ngắn và với dung lượng lớn hơn dung lượng bình thường. Nói cách khác, khi có một nhu cầu truyền tải khối lượng dữ liệu lớn, mạng Frame Relay cho phép được thực

hiện truyền tải dữ liệu với tốc độ lớn hơn tốc độ CIR đã mua của nhà cung cấp dịch vụ. Điều này đảm bảo cho khách hàng tiết kiệm được chi phí mà vẫn đảm bảo truyền dữ liệu với khối lượng lớn trong những điều kiện cần thiết đảm bảo lưu thông thông tin. Truyền dữ liệu bursty chỉ thực hiện được khi không có tắc nghẽn trên mạng.
- Frame Relay không sử dụng địa chỉ định danh như X.25. Để phân biệt các PVC, Frame Relay sử dụng DLCI, mỗi một PVC được gắn liền với một DLCI. DLCI chỉ có tính chất cục bộ có nghĩa là chỉ có ý nghĩa quản lý trên cùng một chuyển mạch. Nói cách khác số DLCI chỉ cần là duy nhất cho mỗi PVC trên một chuyển mạch còn có thể có cùng số DLCI đó trên một chuyển mạch khác.

- Frame Relay sử dụng giao thức LMI (Local Manegment Interface) là giao thức quản lý và trao đổi thông tin quản trị giữa các thiết bị mạng FRND và các thiết bị kết nối FRAD.
- Cũng như X.25, Frame Relay là môi trường mạng đa truy nhập không quảng bá (multiaccess nonbroadcast media). Vấn đề này cần được chú ý khi sử dụng với các giao thức định tuyến.

Các mô hình kết nối của X.25 và Frame Relay

Khi sử dụng phương thức truyền thông X.25, mô hình kết nối cơ bản là điểm-đa điểm (point-to-multipoint) dựa trên tính chất cơ bản của X.25 là sử dụng các VC cho các nhu cầu truyền tải dữ liệu.

Hình 3.29: Mô hình kết nối X.25

Frame Relay đa dạng hơn về các mô hình kết nối. Frame Relay sử dụng các PVC định trước để thực hiện truyền tải dữ liệu giữa hai điểm, người ta chia Frame Relay thành các cấu hình kết nối mạng. Trong đó:
- Full mesh: là mô hình kết nối mà trong đó bất cứ hai node mạng nào cũng có một PVC liên kết giữa chúng. Mô hình này đảm bảo tính sẵn sàng cho toàn bộ hệ thống mạng, nếu có một hoặc một vài PVC có sự cố, các PVC còn lại vẫn có thể đảm bảo cho kết nối mạng giữa các node mạng. Yếu điểm của mô hình mạng này là chi phí thuê các PVC quá lớn.

FRAME RELAY FRAME RELAY
FULL MESH HUB-SPOKE
FRAME RELAY
FULL MESH

Hình 3.30: Mô hình kết nối Frame Relay

- Hub-Spoke: là mô hình có một điểm tập trung mọi kết nối Frame Relay tới các điểm khác, các trao đổi dữ liệu giữa 2 điểm bất kỳ đều phải đi qua điểm tập trung. Mô hình này có chi phí giảm thiểu nhất nhưng có yếu điểm về việc tập trung mọi gánh nặng lên điểm tập trung và nếu có bất kỳ sự cố trên một PVC nào thì sẽ mất khả năng truyền tải dữ liệu với điểm thuộc về PVC bị sự cố đó.

- Partial mesh: là mô hình được sử dụng nhiều nhất, nó là sự lai ghép giữa hai mô hình trên, đảm bảo chi phí và dự phòng cho các điểm thiết yếu.

Cấu hình X.25 cơ bản

Các lưu ý trong cấu hình X.25
- X.25 là một môi trường đa truy nhập không broadcast (multi access non broadcast media) do đó phải lưu ý khi sử dụng với định tuyến động
- X.25 làm việc với sự khởi tạo các VC do đó khi thực hiện cấu hình phải thực hiện các thủ tục liên kết (map) và định tuyến theo địa chỉ
- Các tham số cầ_____n lưu ý

o Độ lớn gói tin (ips/ops)
o Độ lớn cửa sổ điều khiển luồng (win/wout)
o Số lượng kênh VC tối đa cho chiều đến / hai chiều / chiều đi (hic/htc/hoc)
o Số lượng VC dành cho một kết nối (nvc). Nên hạn chế số lượng VC cho phép kết nối đến một điểm trong giới hạn hợp lý để tổng số VC cần thiết không vượt quá số VC tối đa hiện có (HTC)
o Khi thực hiện các liên kết (map) phải thực hiện map địa chỉ IP của phía đối phương tới địa chỉ X25 của họ
o Khi thực hiện định tuyến, phải thực hiện định tuyến với địa chỉ IP next hop
o Cấu hình mạng đấu nối X25 là cấu hình đa điểm, địa chỉ đấu nối phải nằm trong lớp mạng con đủ cho số lượng các điểm

Hình 3.31: Mô hình kết nối X.25 cơ bản

Cấu hình bộ định tuyến 7000
!
interface Serial1/1
ip address 10.1.1.2 255.255.255.0
encapsulation x25
no ip mroute-cache

!--- Địa chỉ X.121 của gán cho bộ định tuyến 7000
x25 address 4522973407000
!--- Các dòng lệnh dưới là các tham số X.25
x25 ips 256
x25 ops 256
x25 htc 16
x25 win 7
x25 wout 7
!--- Dòng lệnh này dùng để gán địa chỉ IP của bộ định tuyến 2500 với
!địa chỉ X.121 của nó
x25 map ip 10.1.1.1 4522973402500
!
!

Hình 3.32: Cấu hình của bộ định tuyến 7000

Cấu hình bộ định tuyến 2500
!
hostname 2500
!
interface Serial0
ip address 10.1.1.1 255.255.255.0
no ip mroute-cache
encapsulation x25
bandwidth 56
!--- Địa chỉ X.121 của gán cho bộ định tuyến 7000
x25 address 4522973402500
!--- Các dòng lệnh dưới là các tham số X.25
x25 ips 256
x25 ops 256
x25 htc 16
x25 win 7
x25 wout 7
!--- Dòng lệnh này dùng để gán địa chỉ IP của bộ định tuyến 7000 với
!địa chỉ X.121 của nó
x25 map ip 10.1.1.1 4522973407000!

Hình 3.33: Cấu hình của bộ định tuyến 2500

- Giám sát:
o **Show interfaces serial 0:** dùng để kiểm tra trạng thái
o **Show x25 vc:** hiển thị thông tin kết nối X.25

o **Show x25 map:** hiển thị các liên kết hiện có của FR

Cấu hình Frame Relay cơ bản

Các lưu ý trong cấu hình Frame Relay:

- Frame Relay là một môi trường đa truy nhập không broadcast (multi access non broadcast media) do đó phải lưu ý khi sử dụng với định tuyến động
- Khi sử dụng định tuyến động giao thức định tuyến vector như RIP, IGRP phải để ý đến luật Split Horizon. Luật Split Horizon là luật không cho phép các thông tin định tuyến vừa đi vào một giao tiếp đi trở ra chính giao tiếp đó để tránh việc cập nhật sai các thông tin về định tuyến dẫn đến việc vòng đi vòng lại của các thông tin định tuyến. Vấn đề này được đặt ra do có nhiều PVC cùng chạy trên một giao tiếp vật lý.
- Giám sát:

o **Show interfaces serial 0:** dùng để kiểm tra DLCI, LMI
o **Show frame-relay lmi:** hiển thị thông tin tổng hợp về LMI
o **Show frame-relay map:** hiển thị các liên kết hiện có của FR
o **Show frame-relay pvc:** hiển thị các thông số của PVC
o **Show frame-relay traffic:** hiển thị traffic

Hình 3.34: Mô hình kết nối Frame Relay cơ bản

- Để bắt đầu cấu hình mạng:

o **Router> enable** □
o **Password: ******** □
o **Router# config terminale** □
o **Router(config)#**

- Thực hiện đặt tên, các mật khẩu, cấu hình cho phép telnet và các điều kiện cần thiết trước khi cấu hình các giao diện
- Cấu hình

o **Spicey(config)# interface serial 0** □

- Lựa chọn giao thức sử dụng

o **Spicey(config-if)# encapsolation frame-relay** □

- Xác định giao thức quản trị LMI. Giao thức quản trị LMI nhất thiết phải có để đảm bảo việc trao đổi thông tin hai chiều giữa thiết bị đầu cuối và thiết bị mạng Frame Relay. LMI hoạt động như một thông báo keepalive.

o **Spicey(config-if)# frame-relay lmi-type cisco** □

- Gán DLCI được cấp cho giao tiếp.

o **Spicey(config-if)# frame-relay interface-dlci 140** □

- Đặt địa chỉ IP cho giao tiếp kết nối leased-line

o **Spicey(config-if)# ip address 3.1.3.1 255.255.255.0** □

- Luôn phải đưa giao tiếp vào sử dụng bằng lệnh no shutdown

o **Spicey(config-if)# no shutdown** □
o **Spicey(config-if)# exit** □

- Sử dụng định tuyến động RIP

o **Spicey(config)# router rip** □
o **Spicey(config-router)# network 3.0.0.0** □
o **Spicey(config-router)# network 124.0.0.0** □
o **Spicey(config-router)# end** □

- Luôn phải ghi lại cấu hình khi đã cấu hình xong

o **Spicey# write memory** □

- Thực hiện các phần việc còn lại tại các bộ định tuyến khác, chú ý về giao thức được sử dụng kiểm tra, giám sát các kết nối.

Cấu hình bộ định tuyến Spicey
Current configuration : 1705 bytes

```
!
version 12.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Spicey
!
interface Ethernet0
ip address 124.124.124.1 255.255.255.0
!
interface Serial0
ip address 3.1.3.1 255.255.255.0
encapsulation frame-relay
frame-relay interface-dlci 140
!
!
router rip
network 3.0.0.0
network 124.0.0.0
```


```
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
login
!
end
```
Hình 3.35: Cấu hình của bộ định tuyến Spicey

Cấu hình bộ định tuyến Prasit

```
Current configuration : 1499 bytes
!
version 12.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Prasit
!
!
!
interface Ethernet0
ip address 123.123.123.1 255.255.255.0
!
!
interface Serial1
ip address 3.1.3.2 255.255.255.0
encapsulation frame-relay
frame-relay interface-dlci 150
!
!
router rip
network 3.0.0.0
network 123.0.0.0
!
!
line con 0
exec-timeout 0 0
transport input none
```

line aux 0
line vty 0 4
login
!
end

Hình 3.36: Cấu hình của bộ định tuyến Prasit

Hình 3.37: Mô hình kết nối Frame Relay Hub-Spoke

- Cấu hình
  - **Spicey(config)# interface serial 0**
- Lựa chọn giao thức sử dụng
  - **Spicey(config-if)# encapsolation frame-relay**
- Xác định giao thức quản trị LMI. Lưu ý trong ví dụ này có sử dụng một chuẩn kết nối LMI khác. Chuẩn kết nối LMI không có giá trị toàn cục mà chỉ có giá trị tại giao tiếp của thiết bị đầu cuối với mạng Frame Relay. Trong cấu hình của các bộ định tuyến khác vẫn sử dụng LMI chuẩn cisco.
  - **Spicey(config-if)# frame-relay lmi-type ansi**
- Luôn phải đưa giao tiếp vào sử dụng bằng lệnh no shutdown
  - **Spicey(config-if)# no shutdown**
- Trong ví dụ này, sử dụng giao tiếp con, subinterface, nên không đặt địa chỉ cho giao tiếp thực, physical interface.
- Cấu hình giao tiếp con. Giao tiếp con phải sử dụng một trong hai lựa chọn là point-to-point hoặc multipoint, ở đây sử dụng point-to-point cho giao tiếp con s0.1 và multipoint cho giao tiếp con s0.2.
  - **Spicey(config-if)# interface serial 0.1 point-to-point**
- Hoặc
  - **Spicey(config-if)# exit**
  - **Spicey(config)# interface serial 0.1 point-to-point**

- Gán DLCI được cấp cho giao tiếp. DLCI 140 là DLCI gắn với PVC nối giữa Spicey và Prasit, còn DLCI 130 gắn với PVC nối tới Aton.
  - **Spicey(config-if)# frame-relay interface-dlci 140**
- Xác lập địa chỉ IP cho giao tiếp con thứ nhất
  - **Spicey(config-subif)# ip address 4.0.1.1 255.255.255.0**
  - **Spicey(config-subif)# exit**
- Cấu hình giao tiếp con thứ hai tới Aton
  - **Spicey(config)# interface serial 0.2 multipoint**
- Gán DLCI được cấp cho giao tiếp là DLCI 130
  - **Spicey(config-if)# frame-relay interface-dlci 130**
- Xác lập địa chỉ IP cho giao tiếp con thứ 2
  - **Spicey(config-subif)# ip address 3.1.3.1 255.255.255.0**
  - **Spicey(config-subif)# exit**
- Sử dụng định tuyến động RIP
  - **Spicey(config)# router rip**
  - **Spicey(config-router)# network 3.0.0.0**
  - **Spicey(config-router)# network 4.0.0.0**
  - **Spicey(config-router)# network 124.0.0.0**
  - **Spicey(config-router)# end**
- Luôn phải ghi lại cấu hình khi đã cấu hình xong
  - **Spicey# write memory**
- Thực hiện các phần việc còn lại tại các bộ định tuyến khác, chú ý về giao thức được sử dụng kiểm tra, giám sát các kết nối.

Cấu hình bộ định tuyến Spicey

Spicey#show running-config
Building configuration...
!
version 12.1
service timestamps debug datetime msec
service timestamps log datetime msec

no service password-encryption
!
hostname Spicey
!
!
interface Ethernet0
ip address 124.124.124.1 255.255.255.0
!

interface Serial0
no ip address
encapsulation frame-relay
frame-relay lmi-type ansi
!
interface Serial0.1 point-to-point
ip address 4.0.1.1 255.255.255.0
frame-relay interface-dlci 140
!
interface Serial0.2 multipoint
ip address 3.1.3.1 255.255.255.0
frame-relay interface-dlci 130
!
router igrp 2
network 3.0.0.0
network 4.0.0.0
network 124.0.0.0
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
login
!
end

Hình 3.38: Cấu hình của bộ định tuyến Spicey

Cấu hình bộ định tuyến Prasit
Prasit#show running-config
Building configuration...
version 12.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Prasit
!
interface Ethernet0
ip address 123.123.123.1 255.255.255.0

!
interface Serial1
no ip address
encapsulation frame-relay
!
!--- LMI cisco là mặc định nên không thể hiện trong cấu hình
!--- Prasit và Spicey đã sử dụng 2 kiểu LMI khác nhau
!--- Bộ định tuyến tại Prasit sử dụng giao tiếp con point-to-point
interface Serial1.1 point-to-point
ip address 4.0.1.2 255.255.255.0
frame-relay interface-dlci 150
!
router igrp 2

```
network 4.0.0.0
network 123.0.0.0
!
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

Hình 3.39: Cấu hình của bộ định tuyến Prasit

Cấu hình bộ định tuyến Aton

```
Aton#show running-config
Building configuration...
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
!
hostname Aton
!
!
!
```



```
interface Ethernet0
ip address 122.122.122.1 255.255.255.0
!
interface Serial1
ip address 3.1.3.3 255.255.255.0
encapsulation frame-relay
frame-relay lmi-type q933a
!--- Aton có kiểu LMI khác hai bộ định tuyến kia
!--- Aton không sử dụng giao tiếp con. Giao tiếp con cần xác định
!là point-to-point hay multipoint ở bộ định tuyến trung tâm
!còn ở các bộ định tuyến còn lại có thể dùng giao tiếp con
!point-to-point hay giao tiếp thực, physical interface
frame-relay interface-dlci 160
!
router igrp 2
network 3.0.0.0
network 122.0.0.0
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

Hình 3.40: Cấu hình của bộ định tuyến Aton

4.3. Cấu hình Dial-up

Giới thiệu quay số

Kết nối quay số cho phép sử dụng đường điện thoại để kết nối trao đổi dữ liệu. Tốc độ của kết nối quay số là không cao và chỉ có thể đáp ứng được cho các ứng dụng không yêu cầu về băng thông cũng như thời gian trễ.

Kết nối quay số sử dụng modem V34, V90 là phổ biến. Tốc độ truyền dữ liệu lên mạng và tải dữ liệu về tối đa là 33,6Kbps. Để có thể thực hiện tải về với tốc độ lớn hơn, tới 56Kbps, bộ định tuyến đóng vai trò điểm truy nhập phải

có kết nối thuê bao dạng số và dùng modem số.
Đối với các doanh nghiệp nhỏ, việc xác thực người dùng có thể thực hiện bằng cách khai báo dữ liệu trực tiếp trên bộ định tuyến. Cách sử dụng này không thích hợp cho các doanh nghiệp vừa và lớn hay các doanh nghiệp cần có sự quản lý chặt chẽ người dùng một cách hệ thống. Lúc này cần thiết có các hệ

thống quản lý người dùng. Các bộ định tuyến của Cisco cho phép sử dụng hai chuẩn xác thực TACACS+ và RADIUS.

Mô hình sử dụng quay số

Hình 3.41: Cấu hình của bộ định tuyến Aton

Cấu hình quay số cơ bản

Danh mục công việc:

- Cấu hình giao tiếp không đồng bộ Async
- Cấu hình giao tiếp điều khiển modem
- Cấu hình xác thực
- Giám sát
  - **Router#show interface Async 1**
  - **Router#show line 1**
  - **Router#debug ppp authentication**

Cấu hình quay số cơ bản

```
Current configuration : 1251 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
!
hostname cisco3640
!
boot system flash:c3640-i-mz.122-8.T
```



```
enable secret 5 <đã xóa>
!
! —- Tên truy nhập cho xác thực người dùng cục bộ
username abc password 0 abc
!
ip subnet-zero
!
no ip domain-lookup
ip domain-name cisco.com
!
! —- Xác định địa chỉ máy chủ DNS cho các máy trạm quay số
async-bootp DNS-server 5.5.5.1 5.5.5.2
!
!
interface Loopback0
ip address 1.1.1.1 255.255.255.0
!
interface Ethernet2/0
ip address 20.20.20.1 255.255.255.0
half-duplex
!
! <<--các giao tiếp không dùng được bỏ đi
!
!--- Giao tiếp Group-Async1 cấu hình cho tất cả các các modem
!--- không cần cấu hình riêng rẽ từng modem
interface Group-Async1
ip unnumbered Loopback0
```

```
encapsulation ppp
dialer in-band
!--- Xác lập thời gian không sử dụng là 10 phút
!--- sau thời gian này, bộ định tuyến sẽ tự động cắt kết nối
dialer idle-timeout 600
!--- Định nghĩa các loại hình dữ liệu được dùng
!--- thông qua cấu hình dialer-group và dialer-list
dialer-group 1
!--- Chế độ interative cho phép người dùng sử dụng nhiều giao thức
!--- để không cho phép người dùng thiết lập các kết nối đến bộ định
tuyến sử dụng chế độ dedicated
async mode interactive
!--- Các máy trạm khi quay số vào sẽ được cấp địa chỉ IP
!--- được qui định trong DIALIN
peer default ip address pool DIALIN
ppp authentication chap
```



```
!--- Xác lập các modem từ line 1 đến line 8 thuộc về nhóm này
group-range 1 8
!
ip local pool DIALIN 10.1.1.1 10.1.1.10
ip classless
ip route 0.0.0.0 0.0.0.0 20.20.20.100
ip http server
ip pim bidir-enable
!
!--- Dòng lệnh sau cho phép giao thức IP là giao thức hoạt động
!--- nếu không có các dữ liệu IP đi qua sau khoảng thời gian 10 phút
!--- đường kết nối sẽ bị cắt
dialer-list 1 protocol ip permit
!
line con 0
password abc
line 1 8
!--- Dòng lệnh dưới cho phép modem quay vào và quay ra
modem InOut
transport input all
autoselect ppp
flowcontrol hardware
line aux 0
line vty 0 4
login
!
!
end
```

Hình 3.42: Cấu hình quay số cơ bản

4.4. Định tuyến tĩnh và động

Sơ lược về định tuyến

Chức năng xác định đường dẫn cho phép bộ định tuyến ước lượng các đường dẫn khả thi để đến đích và thiết lập sự kiểm soát các gói tin. Bộ định tuyến sử dụng các cấu hình mạng để đánh giá các đường dẫn mạng. Thông tin này có thể được cấu hình bởi người quản trị mạng hay được thu thập thông qua quá trình xử lý động được thực thi trên mạng.

Lớp mạng dùng bảng định tuyến IP để gửi các gói tin từ mạng nguồn đến mạng đích. Bộ định tuyến dựa vào các thông tin được giữ trong bảng định tuyến để quyết định truyền tải các gói tin theo các giao tiếp thích hợp.

Hình 3.43: Sử dụng bảng định tuyến để truyền tải các gói tin

Một bảng định tuyến IP bao gồm các địa chỉ mạng đích, địa chỉ của

điểm cần đi qua, giá trị định tuyến và giao tiếp để thực hiện việc truyền tải. Khi không có thông tin về mạng đích, bộ định tuyến sẽ gửi các gói tin theo một đường dẫn mặc định được cấu hình trên bộ định tuyến, nếu đường dẫn không tồn tại, bộ định tuyến tự động loại bỏ gói tin.
Có hai phương thức định tuyến là:
- Định tuyến tĩnh (static routing): là cách định tuyến không sử dụng các giao thức định tuyến. Các định tuyến đến một mạng đích sẽ được thực hiện một cách cố định không thay đổi trên mỗi bộ định tuyến. Mỗi khi thực hiện việc thêm hay bớt các mạng, phải thực hiện thay đổi cấu hình trên mỗi bộ định tuyến.
- Đị_____nh tuyến động (dynamic routing): là việc sử dụng các giao thức định tuyến để thực hiện xây dựng nên các bảng định tuyến trên các bộ định tuyến. Các bộ định tuyến thông qua các giao thức định tuyến sẽ tự động trao đổi các thông tin định tuyến, các bảng định tuyến với nhau. Mỗi khi có sự thay đổi về mạng, chỉ cần khai báo thông tin mạng mới trên bộ định tuyến quản lý trực tiếp mạng mới đó mà không cần phải khai báo lại trên mỗi bộ định tuyến. Một số giao thức định tuyến động được sử dụng là RIP, RIPv2, OSPF, EIGRP v.v...
Giá trị định tuyến được xây dựng tùy theo các giao thức định tuyến khác nhau. Giá trị định tuyến của các kết nối trực tiếp và định tuyến tĩnh có giá trị nhỏ nhất bằng 0, đối với định tuyến động thì giá trị định tuyến được tính toán tùy thuộc và từng giao thức cụ thể. Giá trị định tuyến được thể hiện trong bảng định tuyến là giá trị định tuyến tốt nhất đã được bộ định tuyến tính toán và xây dựng nên trên cơ sở các giao thức định tuyến được cấu hình và giá trị định tuyến của từng giao thức.
Các giao thức định tuyến động được chia thành 2 nhóm chính:
- **Các giao thức định tuyến khoảng cách véc tơ** (distance-vecto, *sau đây được gọi tắt là định tuyến vectơ)*: dựa vào các giải thuật định tuyến có cơ sở hoạt động là khoảng cách véc tơ.
Theo định kỳ các bộ định tuyến chuyển toàn bộ các thông tin có trong bảng định tuyến đến các bộ định tuyến láng giềng đấu nối trực tiếp với nó và

cũng theo định kỳ nhận các bảng định tuyến từ các bộ định tuyến láng giềng. Sau khi nhận được các bảng định tuyến từ các bộ định tuyến láng giềng, bộ định tuyến sẽ so sánh với bảng định tuyến hiện có và quyết định về việc xây dựng lại bảng định tuyến theo thuật toán của từng giao thức hay không. Trong trường hợp phải xây dựng lại, bộ định tuyến sau đó sẽ gửi bảng định tuyến mới cho các láng giềng và các láng giềng lại thực hiện các công việc tương tự. Các bộ định tuyến tự xác định các láng giềng trên cơ sở thuật toán và các thông tin thu lượm từ mạng.
Từ việc cần thiết phải gửi các bảng định tuyến mới lại cho các láng giềng và các láng giềng sau khi xây dựng lại bảng định tuyến lại gửi trở lại bảng định tuyến mới, định tuyến thành vòng có thể xảy ra nếu sự hội về trạng thái bền vững của mạng diễn ra chậm trên một cấu hình mới. Các bộ định tuyến sử dụng các kỹ thuật bộ đếm định thời để đảm bảo không nảy sinh việc xây dựng một bảng định tuyến sai. Có thể diễn giải điều đó như sau:
o Khi một bộ định tuyến nhận một cập nhật từ một láng giềng chỉ rằng một mạng có thể truy xuất trước đây, nay không thể truy xuất được nữa, bộ định tuyến đánh dấu tuyến là không thể truy xuất và khởi động một bộ định thời.
o Nếu tại bất cứ thời điểm nào mà trước khi bộ định thời hết hạn một cập nhật được tiếp nhận cũng từ láng giềng đó chỉ ra rằng mạng đã được truy xuất

trở lại, bộ định tuyến đánh dấu là mạng có thể truy xuất và giải phóng bộ định thời.
o Nếu một cập nhật đến từ một bộ định tuyến láng giềng khác với giá trị định tuyến tốt hơn giá trị định tuyến được ghi cho mạng này, bộ định tuyến đánh dấu mạng có thể truy xuất và giải phóng bộ định thời. Nếu giá trị định tuyến tồi hơn, cập nhật được bỏ qua.
o Khi bộ định thời được đếm về 0, giá trị định tuyến mới được xác lập, bộ định tuyến có bảng định tuyến mới.
- **Các giao thức định tuyến trạng thái đường** (link-state, *gọi tắt là định tuyến trạng thái*): Giải thuật cơ bản thứ hai được dùng cho định tuyến là giải thuật 1ink-state. Các giải thuật định tuyến trạng thái, cũng được gọi là SPF (shortest path first, *chọn đường dẫn ngắn nhất*), duy trì một cơ sở dừ liệu phức tạp chứa thông tin về cấu hình mạng.
- Trong khi giải thuật vectơ không có thông tin đặc biệt gì về các mạng ở xa và cũng không biết các bộ định tuyến ở xa, giải thuật định tuyến trạng thái biết được đầy đủ về các bộ định tuyến ở xa và biết được chúng liên kết với nhau như thế nào.
Giao thức định tuyến trạng thái sử dụng:
o Các thông báo về trạng thái liên kết: LSA (Link State Advertisements).
o Một cơ sở dữ liệu về cấu hình mạng.
o Giải thuật SPF, và cây SPF sau cùng.
o Một bảng định tuyến liên hệ các đường dẫn và các cổng đến từng mạng.

Hoạt động tìm hiểu khám phá mạng trong định tuyến trạng thái được thực hiện như sau:
o Các bộ định tuyến trao đổi các LSA cho nhau. Mỗi bộ định tuyến bắt đầu với các mạng được kết nối trực tiếp để lấy thông tin.
o Mỗi bộ định tuyến đồng thời với các bộ định tuyến khác tiến hành xây dựng một cơ sở dữ liệu về cấu hình mạng bao gồm tất cả các LSA đến từ liên mạng.
o Giải thuật SPF tính toán mạng có thể đạt đến. Bộ định tuyến xây dựng cấu hình mạng luận lý này như một cây, tự nó là gốc, gồm tất cả các đường dẫn có thể đến mỗi mạng trong toàn bộ mạng đang chạy giao thức định tuyến trạng thái. Sau đó, nó sắp xếp các đường dẫn này theo chiến lược chọn đường dẫn ngắn nhất.
o Bộ định tuyến liệt kê các đường dẫn tốt nhất của nó, và các cổng dẫn đến các mạng đích, trong bảng định tuyến của nó. Nó cũng duy trì các cơ sở dữ liệu khác về các phần tử cấu hình mạng và các chi tiết về hiện trạng của mạng. Khi có thay đổi về cấu hình mạng, bộ định tuyến đầu tiên nhận biết được sự thay đổi này gửi thông tin đến các bộ định tuyến khác hay đến một bộ định tuyến định trước được gán là tham chiếu cho tất cả các các bộ định tuyến trên mạng làm căn cứ cập nhật.
o Theo dõi các láng giềng của nó, xem xét có hoạt động hay không, và giá trị định tuyến đến láng giềng đó.
o Tạo một gói LSA trong đó liệt kê tên của tất cả các bộ định tuyến láng giềng và các giá trị định tuyến đối với các láng giềng mới, các thay đổi trong giá trị định tuyến, và các liên kết dẫn đến các láng giềng đã được ghi.
o Gửi gói LSA này đi sao cho tất cả các bộ định tuyến đều nhận được.
o Khi nhận một gói LSA, ghi gói LSA vào cơ sở dữ liệu để sao cho cập nhật gói LSA mới nhất được phát ra từ mỗi bộ định tuyến.
o Hoàn thành bản đồ của liên mạng bằng cách dùng dữ liệu từ các gói

LSA tích lũy được và sau đó tính toán các tuyến dẫn đến tất cả các mạng khác sử dụng thuật toán SPF.
Có hai vấn đề lưu ý đối với giao thức định tuyến trạng thái:
o Hoạt động của các giao thức định tuyến trạng thái trong hầu hết các trường hợp đều yêu cầu các bộ định tuyến dùng nhiều bộ nhớ và thực thi nhiều hơn so với các giao thức định tuyến theo vectơ. Các yêu cầu này xuất phát từ việc cần thiết phải lưu trữ thông tin của tất cả các láng giềng, cơ sở dữ liệu mạng đến từ các nơi khác và việc thực thi các thuật toán định tuyến trạng thái. Người quản lý mạng phải đảm bảo rằng các bộ định tuyến mà họ chọn có khả năng cung cấp các tài nguyên cần thiết này.
o Các nhu cầu về băng thông cần phải tiêu tốn để khởi động sự phát tán gói trạng thái. Trong khi khởi động quá trình khám phá, tất cả các bộ định tuyến dùng các giao thức định tuyến trạng thái để gửi các gói LSA đến tất cả

các bộ định tuyến khác. Hành động này làm tràn ngập mạng khi mà các bộ định tuyến đồng loạt yêu cầu băng thông và tạm thời làm giảm lượng băng thông khả dụng dùng cho lưu lượng dữ liệu thực được định tuyến. Sau khởi động phát tán này, các giao thức định tuyến trạng thái thường chỉ yêu cầu một lượng băng thông tối thiểu để gửi các gói LSA kích hoạt sự kiện không thường xuyên nhằm phản ánh sự thay đổi của cấu hình mạng.
- **Và một nhóm giao thức thứ 3** là nhóm các giao thức định tuyến lai ghép giữa 2 nhóm trên hay nói cách khác có các tính chất của cả hai nhóm giao thức trên.

Các giao thức định tuyến

Bảng 3-10:Các giao thức định tuyến

Các đặc trưng	RIPv1	RIPv2	IRGP	EIGRP	OSPF
Khoảng cách vectơ	X	X	x	x	
Trạng thái đường					x
Tự động tóm tắt định tuyến	X	X	x	x	
Hỗ trợ VLSM[1]			X	x	x
Tương thích với sản phẩm thứ ba	X	X	X		
Thích hợp	Nhỏ	Nhỏ	Vừa	Lớn	Lớn
Thời gian hội tụ về trạng thái cân bằng	Chậm	Chậm	Chậm	Nhanh	Nhanh
Giá trị định tuyến	hop count[2]	hop count	~ BW[3]+D[4]	~ BW+D	~ 10E8/BW
Giới hạn hop count	15	15	100	100	
Cân bằng tải cùng giá					

trị định tuyến
X X x x X
1 VLSM (Vary Length Subnet Mask): hỗ trợ định tuyến cho các mạng con subnetmask có độ dài thay đổi hay nói cách khác thông tin về subnetmask bao gồm trong bảng định tuyến
2 Hop count: được tính bằng số các điểm node mạng mà gói tin phải đi qua từ điểm này đến điểm kia hay chính bằng số các bộ định tuyến mà gói tin phải đi qua
3 BW (bandwitch): băng thông
4 D (delay): trễ

Cân bằng tải không
cùng giá trị định tuyến
x x
Thuật toán Bellman-
Ford
Bellman-
Ford
Bellman-
Ford
DUAL Dijkstra

Cấu hình định tuyến động cơ bản với RIP

Một số lưu ý khi cấu hình định tuyến động với RIP

- RIP gửi các thông tin cập nhật theo các chu kỳ định trước, giá trị mặc định là 30 giây, và khi có sự thay đổi bảng định tuyến.
- RIP sử dụng số đếm các node (hop count) để làm giá trị đánh giá chất lượng của định tuyến (metric). RIP chỉ giữ duy nhất định tuyến có giá trị định tuyến thấp nhất.
- Giá trị hop count tối đa cho phép là 15.
- RIP sử dụng các bộ đếm thời gian cho việc thực hiện gửi các thông tin cập nhật, xoá bỏ một định tuyến trong bảng cũng như để điều khiển các quá trình tạo lập bảng định tuyến, tránh loop vòng.
- RIPv1: Classfull: không có thông tin về subnetmask
- RIPv2: Classless: có thông tin về subnetmask

Cấu hình định tuyến với RIP:

- Cho phép giao thức định tuyến RIP hoạt động trên bộ định tuyến.
  - **Router(config)#router rip**
- Thiết lập các cấu hình mạng. Network là nhóm mạng tính theo lớp mạng cơ bản đang có các giao tiếp trực tiếp trên bộ định tuyến.
  - **Router(config-router)#network 192.168.100.0**
  - **Router(config-router)#network 172.25.0.0**
  - **Router(config-router)#network 10.0.0.0**
- Trong trường hợp sử dụng RIP với các mạng không phải là mạng broadcast như X.25, Frame Relay cần thiết cấu hình RIP với các địa chỉ Unicast là các địa chỉ mà RIP sẽ gửi tới các thông tin cập nhật
  - **Router(config-router)#neighbor 192.168.113.1**
  - **Router(config-router)#neighbor 192.168.113.5**
- Tuỳ theo điều kiện cụ thể về hạ tầng mạng có thể thay đổi chu kỳ cập nhật thông tin, các định nghĩa thời gian khác cho phù hợp.
  - **Router(config-router)# timers basic update invalid holddown flush [sleeptime]**
- Các thay đổi khác.
  - **Router(config-router)# version {1 | 2}**
  - **Router(config-router)# ip rip authentication key-chain name-ofchain**
  - **Router(config-router)# ip rip authentication mode {text | md5}**

- Giám sát.
o **show ip interfaces**
o **show ip rip**

```
Cấu hình bộ định tuyến với RIP
version 12.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Prasit
!
interface Ethernet0
ip address 123.123.123.1 255.255.255.0
!
interface Serial1
ip address 3.1.3.2 255.255.255.0
encapsulation frame-relay
frame-relay interface-dlci 150
!
router rip
network 3.0.0.0
network 123.0.0.0
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
login
end
```

Hình 3.44: Cấu hình của bộ định tuyến với RIP

5. Bộ chuyển mạch lớp 3

5.1. Tổng quan và kiến trúc bộ chuyển mạch lớp 3

Tổng quan

Bộ chuyển mạch lớp 3 là một trong các thiết bị mạng được phát triển mới trên các công nghệ ngày càng tiên tiến. Bộ chuyển mạch lớp 3, như tên gọi của nó, bao gồm các chức năng xử lý gói tin hoạt động trên lớp 3, lớp mạng, trong mô hình 7 lớp OSI, thực hiện các chức năng định tuyến và xử lý gói tin tương tự bộ định tuyến đồng thời thực hiện chuyển mạch gói tin ở lớp 2 như các bộ chuyển

mạch lớp 2, khác hẳn với thế hệ trước đây của nó chỉ thực hiện các xử lý chuyển mạch gói tin ở lớp 2 căn cứ trên các địa chỉ MAC của gói tin.

Khi nhận được gói tin, bộ định tuyến sẽ thực hiện xem xét các thông tin lớp 3 của gói tin để lựa chọn đường đi cho gói tin còn bộ chuyển mạch thì chỉ căn cứ vào địa chỉ lớp 2, địa chỉ MAC, để thực hiện chuyển gói tin. Sự khác nhau cơ bản giữa bộ định tuyến và bộ chuyển mạch lớp 3 là bộ chuyển mạch lớp 3 được cấu thành từ các phần cứng chuyên dụng được thiết kế riêng cho bộ chuyển mạch cho phép thực hiện các chuyển mạch gói tin nhanh như các chuyển mạch lớp 2, điều không có ở các bộ định tuyến, trong khi vẫn có khả năng xử lý định tuyến các gói tin với chức năng tương tự như bộ định tuyến.

Trong môi trường LAN, bộ chuyển mạch lớp 3 được đánh giá là nhanh hơn so với bộ định tuyến và làm tăng năng lực hoạt động của mạng trên cơ sở năng lực chuyển mạch và định tuyến của nó. Tuy nhiên, bộ chuyển mạch lớp 3 không thể thay thế hoàn toàn cho bộ định tuyến do đặc trưng LAN của bộ chuyển mạch lớp 3 và không hoạt động trên môi trường đa giao thức như bộ định tuyến.

Chức năng và kiến trúc của bộ chuyển mạch lớp 3 cũng tương tự như bộ định tuyến và bao gồm:
- Chuyển mạch gói tin
- Các hoạt động định tuyến
- Tính năng mạng thông minh

Chuyển mạch gói tin

Chuyển mạch gói tin là chức năng cơ bản chính của bộ chuyển mạch lớp 3. Điều khác nhau cơ bản giữa bộ định tuyến và bộ chuyển mạch lớp 3 chính là bộ định tuyến dùng bộ xử lý trung tâm để thực hiện các xử lý chuyển mạch gói tin còn bộ chuyển mạch lớp 3 dùng các thành phần phần cứng được thiết kế chuyên dụng ASIC (Application Specific Integrated Circuit).

Thành phần chức năng chuyển mạch gói tin của bộ chuyển mạch thực hiện các công việc kiểm tra địa chỉ gói tin, so sánh với thông tin lưu trữ và thực hiện truyền tải chúng theo hướng xác định. Chúng đồng thời cũng thực hiện các xử lý lớp dưới tương tự bộ định tuyến với việc gán lại các địa chỉ MAC, giảm số đếm TTL... Chức năng chuyển mạch gói tin cũng thực hiện phép so sánh đúng nhất để lựa chọn đường đi đúng khi có nhiều hơn một khả năng để lựa chọn.

Các hoạt động định tuyến

Hoạt động định tuyến là một hoạt động độc lập khác so với hoạt động chuyển mạch gói tin. Bộ định tuyến cũng như bộ chuyển mạch lớp 3 quản lý và điều hành các thông tin định tuyến, xây dựng, cập nhật và trao đổi chúng thông qua các giao thức định tuyến mỗi khi có sự thay đổi về mạng như lỗi đường, thêm mới hay cập nhật thiết bị...

Cũng như các bộ định tuyến, bộ chuyển mạch lớp 3 hoạt động với hầu hết các giao thức định tuyến động hiện có.

Tính năng mạng thông minh

Các tính năng quản trị, cấp phát động, các tính năng định tuyến thông minh, các tính năng bảo mật, xác thực cũng được thiết kế và xây dựng trên bộ định tuyến lớp 3 qua đó dễ dàng cho người quản trị thực hiện việc xây dựng, quản trị và phát triển mạng.

5.2. Định tuyến trên bộ chuyển mạch lớp 3

VLAN

VLAN là khái niệm để chỉ một mạng LAN độc lập một cách logic với nhau. Về thực chất, tất cả các thiết bị mạng được đấu nối và hoạt động trên cùng một môi trường vật lý, hạ tầng mạng chung và hình thành một cách logic các mạng LAN trên môi trường đó dựa trên các thiết đặt nhận dạng độc lập với nhau đối với mỗi nhóm thành viên. Nói cách khác, mỗi cổng kết nối của các bộ chuyển mạch được định nghĩa thuộc về một nhóm làm việc (VLAN) nào đó và hình thành các khả năng độc lậ_____p tách rời của các nhóm làm việc đó với nhau. Các gói tin của một VLAN chỉ được lưu chuyển tới các cổng trong cùng VLAN mà không được lưu chuyển đến các cổng khác VLAN trừ cổng được định nghĩa là trung kế của các VLAN. Khác với LAN, VLAN không bị giới hạn về phạm vi địa lý cụ thể mà chỉ phụ thuộc vào nhu cầu và hình thức triển khai.

VLAN Trunking là khái niệm được dùng để chỉ việc kết nối giữa các bộ chuyển mạch với nhau mà qua đó cho phép các gói tin của tất cả các VLAN được truyền qua.

VLAN được cấu hình tại lớp 2 cho phép phân định các nhóm thiết bị máy tính độc lập logic với nhau, các nhu cầu trao đổi dữ liệu giữa các thiết bị khác VLAN phải được thực hiện bởi các thiết bị hoạt động ở lớp 3 như bộ chuyển mạch lớp 3 hay các bộ định tuyến.

Các giao thức và mô hình kết nối VLAN xin xem thêm trong các giáo trình về mạng nội bộ LAN.

Cấu trúc xử lý định tuyến

Như đã nói ở phần trước, bộ chuyển mạch lớp 3 đồng thời thực hiện các chức năng chuyển mạch và chức năng định tuyến. Bộ chuyển mạch lớp 3 cho phép các thiết bị thuộc về các nhóm mạng khác nhau, các VLAN khác nhau có thể kết nối được với nhau.

Ở đây cần phân biệt các nhu cầu kết nối trao đổi dữ liệu khác nhau trong đó bao gồm:

- Các nhu cầu kết nối trao đổi dữ liệu trên các mạng sử dụng nhóm giao thức mạng định tuyến được như IP, IPX.
- Các nhu cầu kết nối trao đổi dữ liệu trên các mạng sử dụng nhóm giao thức mạng không định tuyến được như NetBEUI, AppleTalk.

Đối với nhóm giao thức không định tuyến được, bộ chuyển mạch xử lý chúng bằng nhóm các giao thức cầu nối (bridge). Các giao thức định tuyến được sẽ được xử lý tương tự như một bộ định tuyến. Bộ chuyển mạch lớp 3 hỗ trợ định

tuyến - cầu nối kết hợp, định tuyến giữa các VLAN, các chuyển mạch nhiều lớp.

Chuyển mạch và định tuyến kết hợp

Cho phép bộ chuyển mạch chuyển các gói tin thuộc nhóm các giao thức không định tuyến được giữa các cổng được cấu hình ở chế độ cầu nối đồng thời cho phép chuyển các gói tin thuộc nhóm định tuyến được qua lại giữa các cổng thuộc về các VLAN sử dụng cho nhóm các giao thức định tuyến được. Giao thức chuyển mạch và định tuyến kết hợp chỉ thực hiện xử lý định hướng các gói tin trên cùng một thiết bị chuyển mạch.

Định tuyến giữa các VLAN

Việc định tuyến giữa các VLAN được thực hiện trên các bộ chuyển mạch lớp 3, thông qua các module định tuyến lớp 3 hoặc thực hiện trên các bộ chuyển mạch. Bộ chuyển mạch lớp 3 hỗ trợ các giao thức định tuyến tĩnh, định tuyến động RIP, OSPF, IGRP, EIGRP.

5.3. Sơ lược về các bộ chuyển mạch lớp 3 thông dụng của Cisco

Bộ chuyển mạch lớp 3 Cisco 2948G-L3

Hình 3.45: Bộ chuyển mạch lớp 3 Cisco 2948G-L3

- 48 cổng 10/100 Ethernet, giao diện RJ45
- 02 cổng uplink Gigabit Ethernet hỗ trợ GBIC (Gigabit Interface Converter) cho phép lựa chọn các giao diện khác nhau phù hợp với nhu cầu sử dụng cổng kết nối Gigabit
- Tốc độ chuyển mạch lớp 3: 10.000 gói tin/giây
- Thông lượng: 22Gbit/giây
- Hỗ trợ IP, IPX, IP multicast
- Chức năng định tuyến lớp 3: RIP, OSPF, IGRP, EIGRP
- Chức năng chuyển đổi dự phòng, hỗ trợ trung chuyển giao thức cấp địa chỉ động
- Hỗ trợ QoS
- Chức năng an ninh mạng với danh sách truy nhập ACL

Bộ chuyển mạch lớp 3 Cisco 3550

Hình 3.46: Các bộ chuyển mạch lớp 3 Cisco 3550

Loại chuyển mạch Số cổng 10/100 Số cổng Gigabit

Catalyst 3550-24 Switch 24 2 (GBIC)
Catalyst 3550-24 PWR
Switch
24 (cho phép cấp
nguồn qua cáp
mạng đến các
thiết bị khác như
thiết bị điểm truy
cập không dây)
2 (GBIC)
Catalyst 3550-24-DC Switch 24 2 (GBIC)
Catalyst 3550-24-FX Switch 24 (cổng quang
tốc độ 100Mbps)
2 (GBIC)
Catalyst 3550-48 Switch 48 2 (GBIC)
Catalyst 3550-12G Switch 10 (GBIC)
2 (10/100/1000BASE-T)
Catalyst 3550-12T switch 10 (10/100/1000BASE-T)
2 (GBIC)
- Năng lực xử lý cao:
o CEF: Cisco Express Forwarding
o Các giao thức định tuyến: RIP, OSPF, IGRP, EIGRP, BGPv4
o Inter-VLAN IP routing
o Các giao thức định tuyến multicast
o Các giao thức chuyển đổi dự phòng
- Tối ưu băng thông:
o 1,6 Gigabit cho cổng 10/100 và 16 Gigabit cho cổng Gigabit
o Chức năng làm việc với máy chủ cache theo giao thức WCCP
o Khả năng hạn chế tốc độ theo từng ứng dụng, nhóm người dùng

- Dễ dàng sử dụng và khai thác
- An toàn và bảo mật
o Xác thực người dùng với các hệ thống quản trị tập trung
TACACS+, RADIUS
o Mã hóa SSH, Kerberos
o Các tính năng xác thực thiết bị
o VLAN
- Dễ dàng thực hiện QoS với các mức độ đa dạng và linh hoạt.
- Quản trị từ xa và tập trung. Tương thích với các hệ thống quản trị thông
dụng.
Ngoài ra còn có các bộ chuyển mạch lớp 3 của Cisco với các dòng 4000, 6000..

6. Bài tập thực hành sử dụng bộ định tuyến Cisco

Bài 1: Thực hành nhận diện thiết bị, đấu nối thiết bị

Yêu cầu:
- Nhận diện đúng các chủng loại thiết bị
- Nhận diện các giao tiếp của bộ định tuyến, ý nghĩa và mục đích sử dụng
- Biết cách sử dụng các loại cáp với từng loại thiết bị, giao tiếp khác nhau
- Biết đấu nối bộ định tuyến với nhau và với các thiết bị modem khác
- Sử dụng phần mềm HyperTerminal kết nối với bộ định tuyến

Bài 2: Thực hành các lệnh cơ bản

- Các lệnh show

- Lệnh config
Yêu cầu:
- Nắm vững ý và sử dụng thành thạo các lệnh kiểm tra và các lệnh cấu hình cơ bản

Bài 3: Cấu hình bộ định tuyến với mô hình đấu nối leased-line

- Cấu hình Interface
- Cấu hình giao thức
- Cấu hình định tuyến

Yêu cầu:
- Sử dụng thiết bị phòng lab để cấu hình một kết nối leased-line cho phép kết nối 2 mạng với nhau.
- Vận dụng các kiến thức đã học kiểm soát và xử lý sự cố.

Bài 4: Cấu hình bộ định tuyến với Dial-up

- Cấu hình line vật lý

- Cấu hình async interface
- Cấu hình định tuyến
- Cấu hình xác thực

Yêu cầu:
- Sử dụng thiết bị phòng lab để cấu hình một điểm truy nhập gián tiếp quay số qua thoại.
- Vận dụng các kiến thức đã học kiểm soát và xử lý sự cố.

Thiết bị phòng lab

- 02 bộ định tuyến 2509 (leased-line và async) hoặc tương đương
- 02 modem leased-line CSU/DSU dùng cho kết nối leased-line
- 02 cáp V.35 DTE
- 04 modem dial-up 56kbps
- 02 cáp Async dùng cho kết nối modem 56kbps
- Phần mềm giả lập bộ định tuyến (router simulator)
- 02 máy tính dùng để cấu hình trực tiếp các bộ định tuyến
- các máy tính để thực hành trên phần mềm giả lập bộ định tuyến
- 04 đường điện thoại

Chương 4
Hệ thống tên miền DNS

Chương 4 sẽ tập trung nghiên cứu về hệ thống tên miền là một hệ thống định danh phổ biến trên mạng TCP/IP nói chung và đặc biệt là mạng Internet. Hệ thống tên miền tối quan trọng cho sự phát triển của các ứng dụng phổ biến như thư tín điện tử, web...Cấu trúc hệ thống tên miền, cấu trúc và ý nghĩa của các trường tên miền cũng như các kỹ năng cơ bản được cung cấp sẽ giúp cho người quản trị có thể hoạch định được các nhu cầu liên quan đến tên miền cho mạng lưới, tiến hành thủ tục đăng ký chính xác (nếu đăng ký tên miền Internet) và đảm nhận được các công tác tạo mới, sửa đổi ... hay nói chung là các công việc quản trị hệ thống máy chủ tên miền DNS

Chương 4 đòi hỏi các học viên phải quen thuộc với địa chỉ IP, việc soạn thảo quản trị các tiến trình trên các hệ thống linux, unix, windows.

1. Giới thiệu

1.1. Lịch sử hình thành của DNS

Vào những năm 1970 mạng ARPanet của bộ quốc phòng Mỹ rất nhỏ và dễ

dàng quản lý các liên kết vài trăm máy tính với nhau. Do đó mạng chỉ cần một file HOSTS.TXT chứa tất cả thông tin cần thiết về máy tính trong mạng và giúp các máy tính chuyển đổi được thông tin địa chỉ và tên mạng cho tất cả máy tính trong mạng ARPanet một cách dễ dàng. Và đó chính là bước khởi đầu của hệ thống tên miền gọi tắt là DNS (Domain name system)

Như khi mạng máy tính ARPanet ngày càng phát triển thì việc quản lý thông tin chỉ dựa vào một file HOSTS.TXT là rất khó khăn và không khả thi. Vì thông tin bổ xung và sửa đổi vào file HOSTS.TXT ngày càng nhiều và nhất là khi ARPanet phát triển hệ thống máy tính dựa trên giao thức TCP/IP dẫn đến sự phát triển tăng vọt của mạng máy tính:

− Lưu lượng và trao đổi trên mạng tăng lên
− Tên miền trên mạng và địa chỉ ngày càng nhiều
− Mật độ máy tính ngày càng cao do đó đảm bảo phát triển ngày càng khó khăn

Đến năm 1984 Paul Mockpetris thuộc viện USC's Information Sciences Institute phảt triển một hệ thống quản lý tên miền mới (miêu tả trong chuẩn RFC 882 - 883) gọi là DNS (Domain Name System) và ngày này nó ngày càng được phát triển và hiệu chỉnh bổ xung tính năng để đảm bảo yêu cầu ngày càng cao của hệ thống (hiện nay DNS được tiêu chuẩn theo chuẩn RFC 1034 - 1035)

1.2. Mục đích của hệ thống DNS

Máy tính khi kết nối vào mạng Internet thì được gán cho một địa chỉ IP xác định. Địa chỉ IP của mỗi máy là duy nhất và có thể giúp máy tính có thể xác định đường đi đến một máy tính khác một cách dễ dàng. Như đối với người dùng thì địa chỉ IP là rất khó nhớ. Do vậy cần phải sử dụng một hệ thống để giúp cho máy tính tính toán đường đi một cách dễ dàng và đồng thời cũng giúp người dùng dễ nhớ. Do vậy hệ thống DNS ra đời nhằm giúp cho người dùng có thể chuyển đổi từ địa chỉ IP khó nhớ mà máy tính sử dụng sang một tên dễ nhớ cho người sử dụng và đồng thời nó giúp cho hệ thống Internet dễ dàng sử dụng để liên lạc và ngày càng phát triển.

Hệ thống DNS sử dụng hệ thống cơ sở dữ liệu phân tán và phân cấp hình cây do đó việc quản lý sẽ dễ dàng và cũng rất thuận tiện cho việc chuyển đổi từ tên miền sang địa chỉ IP và ngược lại. Cũng giống như mô hình quản lý cá nhân của một đất nước mỗi cá nhân sẽ có một tên xác định đồng thời cũng có địa chỉ chứng minh thư để giúp quản lý con người một cách dễ dàng hơn (nhưng khác là tên miền không được trùng nhau còn tên người thì vẫn có thể trùng nhau)

Mỗi cá nhân đều có một số căn cước để quản lý

Mỗi một địa chỉ IP tương ứng với một tên miền

Vậy tóm lại tên miền là (domain name) gì ? những tên gợi nhớ như home.vnn.vn hoặc www.cnn.com thì được gọi là tên miền (domain name hoặc DNS name). Nó giúp cho người sử dụng dễ dàng nhớ vì nó ở dạng chữ mà người bình thường có thể hiểu và sử dụng hàng ngày.

Hệ thống DNS đã giúp cho mạng Internet thân thiện hơn với người sử dụng do đó mạng internet phát triển bùng nổ một vài năm lại đây. Theo thống trên thế giới vào thời điểm tháng 7/2000 số lượng tên miền được đăng ký là 93.000.000

Tóm lại mục đích của hệ thống DNS là:

− Địa chỉ IP khó nhớ cho người sử dụng nhưng dễ dàng với máy tính
− Tên thì dễ nhớ với người sử dụng như không dùng được với máy tính
− Hệ thống DNS giúp chuyển đổi từ tên miền sang địa chỉ IP và ngược lại

giúp người dùng dễ dàng sử dụng hệ thống máy tính

2. DNS server và cấu trúc cơ sở dữ liệu tên miền

2.1.Cấu trúc cơ sở dữ liệu

Cơ sở dữ liệu của hệ thống DNS là hệ thống cơ sở dữ liệu phân tán và phân cấp hình cây. Với .Root server là đỉnh của cây và sau đó các domain được phân nhánh dần xuống dưới và phần quyền quản lý. Khi một client truy vấn một tên miền nó sẽ lần lượt đi từ root phân cấp lần lượt xuống dưới để đến DNS quản lý domain cần truy vấn.

Cấu trúc của dữ liệu được phân cấp hình cây root quản lý toàn bộ sơ đồ và phân quyền quản lý xuống dưới và tiếp đó các tên miền lại được tiếp tục chuyển xuống cấp thấp hơn (delegate) xuống dưới.

Zone

Hệ thống DNS cho phép phân chia tên miền để quản lý và nó chia hệ thống tên miền ra thành zone và trong zone quản lý tên miền được phân chia đó và nó chứa thông tin về domain cấp thấp hơn và có khả năng chia thành các zone cấp thấp hơn và phân quyền cho các DNS server khác quản lý.

Ví dụ: zone *".com"* thì DNS server quản lý zone *".com"* chưa thông tin về các bản ghi có đuôi là *".com"* và có khả năng chuyển quyền quản lý (delegate) các zone cấp thấp hơn cho các DNS khác quản lý như *".microsoft.com"* là vùng (zone) do microsoft quản lý.

Root Server

- Là server quản lý toàn bộ cấu trúc của hệ thống DNS
- Root server không chứa dữ liệu thông tin về cấu trúc hệ thống DNS mà nó chỉ chuyển quyền (delegate) quản lý xuống cho các server cấp thấp hơn và do đó root server có khả năng xác định đường đến của một domain tại bất cứ đâu trên mạng
- Hiện nay trên thế giới có khoảng 13 root server quản lý toàn bộ hệ thống Internet (vị trí của root server như trên hình vẽ dưới)

Hệ thống cơ sở dữ liệu của DNS là hệ thống dữ liệu phân tán hình cây như cấu trúc đó là cấu trúc logic trên mạng Internet

Về mặt vật lý hệ thống DNS nằm trên mạng Internet không có có cấu trúc hình cây nhưng nó được cấu hình phân cấp logic phân cấp hình cây phân quyền quản lý.

Một DNS server có thể nằm bất cứ vị trí nào trên mạng Internet nhưng được cấu hình logic để phân cấp chuyển tên miền cấp thấp hơn xuống cho các DNS server khác nằm bất cứ vị trí nào trên mạng Internet (về nguyên tắc ta có thể đặt DNS tại bất cứ vị trí nào trên mạng Internet. Nhưng tốt nhất là đặt DNS tại vị trí nào gần với các client để dễ dàng truy vấn đến đồng thời cũng gần với vị trí của DNS server cấp cao hơn trực tiếp của nó).

Mỗi một tên miền đều được quản lý bởi ít nhất một DNS server và trên đó ta khai các bản ghi của tên miền trên DNS server. Các bản ghi đó sẽ xác định địa chỉ IP của tên miền hoặc các dịch vụ xác định trên Internet như web, thư điện tử ...

Sau đây là các bản ghi trên DNS

Tên trường Tên đầy đủ Mục đích

SOA Start of Authority Xác định máy chủ DNS có thẩm quyền cung cấp thông tin về tên miền xác định trên DNS
NS Name Server Chuyển quyền quản lý tên miền xuống một DNS cấp thấp hơn
A Host Ánh xạ xác định địa chỉ IP của một host
MX Mail Exchanger Xác định host có quyền quản lý thư điện tử cho một tên miền xác định
PTR Pointer Xác định chuyển từ địa chỉ IP sang tên miền
CNAME Canonical NAME Thường sử dụng xác định dịch vụ web hosting

Cấu trúc của một tên miền

− Domain sẽ có dạng : lable.lable.label...lable
− Độ dài tối đa của một tên miền là 255 ký tự
− Mỗi một Lable tối đa là 63 ký tự
− Lable phải bắt đầu bằng chữ hoặc số và chỉ được phép chứa chữ, số, dấu trừ(-), dấu chấm (.) mà không được chứa các ký tự khác.

Phân loại tên miền

Hầu hết tên miền được chia thành các loại sau:
− *Arpa* : tên miền ngược (chuyển đổi từ địa chỉ IP sang tên miền reverse domain)
− *Com* : các tổ chức thương mại
− *Edu* : các cơ quan giáo dục
− *Gov* : các cơ quan chính phủ
− *Mil* : các tổ chức quân sự, quốc phòng
− *Net* : các trung tâm mạng lớn
− *Org* : các tổ chức khác
− *Int* : các tổ chức đa chính phủ (ít được sử dụng)

Ngoài ra hiện nay trên thế giới sử dụng loại tên miền có hai ký tự cuối để xác định tên miền thuộc quốc gia nào (được xác định trong chuẩn ISO3166)

Loại tên	**Miêu tả**	**Ví dụ**
Gốc (domain root)	Nó là đỉnh của nhánh cây của tên miền. Nó xác định kết thúc của domain (fully qualified domain names FQDNs).	Đơn giản nó chỉ là dấu chấm (**.**) sử dụng tại cuối của tên ví như "example.microsoft.com."
Tên miền cấp một (Top-level domain)	Là hai hoặc ba ký tự xác định nước/khu vực hoặc các tổ chức.	

".com", xác định tên sử dụng trong
xác định là tổ chức thương mại .
Tên miền cấp
hai
(Second-level
domain)
Nó rất đa dạng trên internet,
nó có thể là tên của một
công ty, một tổ chức hay
một cá nhân .v.v. đăng ký
trên internet.
"microsoft.com.", là tên miền cấp
hai đăng ký là công ty Microsoft.
Tên miền cấp
nhỏ hơn
(Subdomain)
Chia nhỏ thêm ra của tên
miên cấp hai xuống thường
được sử dụng như chi
nhánh, phong ban của một
cơ quan hay một chủ đề nào
đó.
"example.microsoft.com." là phần
quản lý tài liệu ví dụ của microsof
Một số chú ý khi đặt tên miền:
− Tên miền nên đặt giới hạn từ từ cấp 3 đến cấp 4 hoặc cấp 5 vì nếu nhiều hơn nữa việc quản trị là khó khăn.
− Sử dụng tên miền là phải duy nhất trong mạng internet
− Nên đặt tên đơn giản gợi nhớ và tránh đặt tên quá dài

2.2. Phân loại DNS server và đồng bộ dư liệu giữa các DNS server

Có ba loại DNS server sau:

 Primary server

Nguồn xác thực thông tin chính thức cho các domain mà nó được phép quản lý quản lý

Thông tin về tên miền do nó được phân cấp quản lý thì được lưu trữ tại đây và sau đó có thể được chuyển sang cho các secondary server.

Các tên miền do primary server quản lý thì được tạo và sửa đổi tại primary server và sau đó được cập nhập đến các secondary server.

 Secondary server

DNS được khuyến nghị nên sử dụng ít nhất là hai DNS server để lưu cho mỗi một zone. Primary DNS server quản lý các zone và secondary server được sử dụng để lưu trữ dự phòng cho zone cho primary server. Secondary DNS server được khuyến nghị dùng nhưng không nhất thiết phải có. Secondary server được phép quản lý domain nhưng dữ liệu về domain không phải tạo tại secondary server mà nó được lấy về từ primary server.

Secondary server có thể cung cấp hoạt động ở chế độ không có tải trên mạng. Khi lượng truy vấn zone tăng cao tại primary server nó sẽ chuyển bớt tải sang secondary server hoặc khi primary server bị sự cố thì secondary sẽ hoạt động thay thế cho đến khi primary server hoạt động trở lại

Secondary server nên được sử dụng tại nới gần với client để có thể phục vụ

cho việc truy vấn tên miền một cách dễ dàng. Nhưng không nên cài đặt secondary server trên cùng một subnet hoặc cùng một kết nối với primary server. Vì điều đó sẽ là một giải pháp tốt để sử dụng secondary server để dự phòng cho primary server vì có thể kết nối đến primary server bị hỏng thì cũng không ảnh hưởng gì đến secondary server.

Primary server luôn luôn duy trì một lượng lớn dữ liệu và thường xuyên thay đổi hoặc thêm vào các zone. Do đó DNS server sử dụng một cơ chế cho phép chuyển các thông tin từ primary server sang secondary server và lưu giữ nó trên đĩa. Các thông tin nhận dữ liệu về các zone có thể sử dụng giải pháp lấy toàn bộ (full) hoặc lấy phần thay đổi (incremental)

Nhiều secondary DNS server sẽ tăng độ ổn định hoạt động của mạng và việc lưu trữ thông tin của tên miền một cách đảm bảo như một điều cần quan tâm là dữ liệu của zone được chuyển trên mạng từ primary server đến các secondary server sẽ làm tăng lưu lượng đường truyền và yêu cầu thời gian để đồng bộ dữ liệu trên các secondary server.

 Caching-only server

Mặc dù tất cả các DNS server đều có khả năng lưu trữ dữ liệu trên bộ nhớ cache của máy để trả lời truy vấn một cách nhanh chóng. Caching-only server là loại DNS server chỉ sử dụng cho việc truy vấn, lưu giữ câu trả lời dựa trên thông tin trên cache của máy và cho kết quả truy vấn. Chúng không hề quản lý một domain nào và thông tin mà nó chỉ giới hạn những gì được lưu trên cache của server.

Khi nào thì sử dụng caching-only server ?. Khi mà server bắt đầu chạy thì nó không có thông tin lưu trong cache. Thông tin sẽ được cập nhập theo thời gian khi các client server truy vấn dịch vụ DNS. Nếu bạn sử dụng kết nối mạng WAN tốc độ thấp thì việc sử dụng caching-only DNS server là một giải pháp tốt nó cho phép giảm lưu lượng thông tin truy vấn trên đường truyền.

Chú ý

- Caching-only DNS server không chưa zone nào và cũng không quyền quản lý bất kỳ domain nào. Nó sử dụng bộ nhớ cache của mình để lưu các truy vấn DNS của client. Thông tin sẽ được lưu trong cache để trả lời cho các truy vấn đến của client
- Caching-only DNS có khả năng trả lời các truy vấn như không quản lý hoặc tạo bất cứ zone hoặc domain nào
- DNS server nói trung được khuyến nghị là được cấu hình sử dụng TCP/IP và dùng địa chỉ IP tĩnh.

Đồng bộ dữ liệu giữa các DNS server (zone transfer)

Truyền toàn bộ zone

Bởi vì tầm quan trọng của hệ thống DNS và việc quản lý các domain thuộc zone phải được đảm bảo. Do đó thường một zone thì thường được đặt trên hơn một DNS server để tránh lỗi khi truy vấn tên miền thuộc zone đó. Nói cách khác nếu chỉ có một server quản lý zone và khi server không trả lời truy vấn thì các tên miền trong zone đó sẽ không được trả lời và không còn tồn tại trên Internet. Do đó ta cần có nhiều DNS server cùng quản lý một zone và có cơ chế để chuyển dữ liệu của các zone và đồng bộ nó từ một DNS server này đến các DNS server khác

Khi một DNS server mới được thêm vào mạng thì nó được cấu hình như một secondary server mới cho một zone đã tồn tại. Nó sẽ tiến hành nhận toàn bộ (full) zone từ DNS server khác. Như DNS server thế hệ đầu tiên thường dùng giải pháp lấy toàn bộ cơ sở dữ liệu về zone khi có các thay đổi trong zone.

Truyền phần thay đổi (Incremental zone)

Truyền chỉ những thay đổi (incremental zone transfer) của zone được miêu tả chi tiết trong tiêu chuẩn RFC 1995. Nó là phần bổ xung cho chuẩn sao chép DNS zone. Incremental transfer thì đươc hỗ trợ bởi cả DNS server là nguồn lấy thông tin và DNS server nhận thông tin về zone, nó cung cấp giải pháp hiệu quả cho việc đồng bộ nhưng thay đổi hoặc thêm bớt zone.

Giải pháp ban đầu cho DNS yêu cầu cho việc thay đổi dữ liệu về zone là truyền toàn bộ dữ liệu của zone sử dụng truy vấn AXFR. Với việc chỉ truyền các thay đổi (incremental transfer) sẽ sử dụng truy vấn (IXFR) được sử dụng thay thế cho AXFR. Nó cho phép secondary server chỉ lấy về như zone thay đổi để đồng bộ dữ liệu.

Với trao đổi IXFR zone, thì sự khác nhau giữa versions của nguồn dữ liệu và bản sao của nó. Nếu cả hai bản đều có cùng version (xác định bởi số serial

trong khai báo tại phần đầu của zone SOA "start of authority") thì việc truyền dữ liệu của zone sẽ không được thực hiện.

Nếu số serial cho dữ liệu nguồn lớn hơn số serial của secondary server thì nó sẽ thực hiện chuyển những thay đổi với các bản ghi nguồn (Resource record - RR) của zone. Để truy vấn IXFR thực hiện thành công và các thay đổi được gửi thì tại DNS server nguồn của zone phải lưu gữi các phần thay đổi để sử dụng truyền đến nơi yêu cầu của truy vấn IXFR. Incremental sẽ cho phép lưu lượng truyền dữ liệu là ít và thực hiện nhanh hơn.

```
SOA vdc-hn01.vnn.vn. postmaster.vnn.vn. (
82802 ; serial number
; refresh every 30 mins
; retry every hour
; expire after 24 hours
; minimum TTL 2 hours
NS vdc-hn01.vnn.vn.
NS hcm-server1.vnn.vn.
```

Zone transfer sẽ xảy ra khi có nhưng hành động sau xảy ra:

- Khi quá trình làm mới của zone kết thúc (refresh expire)
- Khi secondary server được thông báo zone đã thay đổi tại server nguồn quản lý zone
- Khi dịch vụ DNS bắt đầu chạy tại secondary server
- Tại secondary server yêu cầu chuyển zone

Sau đây là các bước yêu cầu từ secondary server đến DNS server chứa zone để yêu cầu lấy dữ liệu về zone mà nó quản lý.

1. Trong khi cấu hình mới DNS server. Thì nó sẽ gửi truy vấn yêu cầu gửi toàn bộ zone ("all zone" transfer (AXFR) request) đến DNS server quản lý chính dữ liệu của zone
2. DNS server chính quản lý dữ liệu của zone sẽ trả lời và chuyển toàn bộ dữ liệu về zone đến secondary (destination) server mới cấu hình.

zone thì được chuyển đến DNS server yêu cầu căn cứ vào version được xác định bằng số Serial tại phần khai báo (start of authority SOA). Tại phần SOA cũng có chứa các thông số xác định thời gian làm mới lại zone ...

3. Khi thời gian làm mới (refresh interval) của zone hết, thì DNS server nhận dữ liệu sẽ truy vấn yêu cầu làm mới zone tới DNS server chính chứa dữ liệu zone.
4. DNS server chính quản lý dữ liệu sẽ trả lời truy vấn và gửi lại dữ liệu. Trả lời sẽ bao gồm cả số serial của zone hiện tại tại DNS server chính.
5. DNS server nhận dữ liệu về zone sẽ kiểm tra số serial trong trả lời và

quyết định sẽ làm thế nào với zone

Nếu giá trị của số serial bằng với số hiện tại tại DNS server nhận trả lời thì nó sẽ kết luận rằng sẽ không cần chuyển dữ liệu về zone đến. Và nó sẽ thiết lập lại với các thông số cũ và thời gian để làm mới lại bắt đầu.
Nếu giá trị của số serial tại DNS server chính lớn hơn giá trị hiện tại tại dữ liệu DNS nới nhận thì nó kết luận rằng zone cần phải được cập nhập và việc chuyển zone là cần thiết.
6. Nếu DNS server nơi nhận kết luận rằng zone cần phải thay đổi và nó sẽ gửi truy vấn IXFR tới DNS server chính để yêu cầu gửi zone
7. DNS server chính sẽ trả lời với việc gửi những thay đổi của zone hoặc toàn bộ zone
Nếu DNS server chính có hỗ trợ việc gửi những thay đổi của zone thì nó sẽ gửi những phần thay đổi (incremental zone transfer (IXFR) of the zone.). Nếu nó không hỗ trợ _____thì nó sẽ gửi toàn bộ zone (full AXFR transfer of the zone)

3. Hoạt động của hệ thống DNS

Hệ thống DNS hoạt động động tại lớp 4 của mô hình OSI nó sử dụng truy vấn bằng giao thức UDP và mặc định là sử dụng cổng 53 để trao đổi thông tin về tên miền.
Hoạt động của hệ thống DNS là chuyển đổi tên miền sang địa chỉ IP và ngược lại. Hệ thống cơ sở dữ liệu của DNS là hệ thống cơ sở dữ liệu phân tán, các DNS server được phân quyền quản lý các tên miền xác định và chúng liên kết với nhau để cho phép người dùng có thể truy vấn một tên miền bất kỳ (có tồn tại) tại bất cứ điểm nào trên mạng một các nhanh nhất

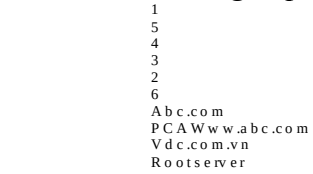
Như đã trình bầy các DNS server phải biết ít nhất một cách để đến được root server và ngược lại. Như trên hình vẽ muốn xác định được tên miền mit.edu thì root server phải biết DNS server nào được phân quyền quản lý tên miền mit.edu để chuyển truy vấn đến.

Nói tóm lại tất cả các DNS server đều được kết nối một cách logic với nhau:
 Tất cả các DNS server đều được cấu hình để biết ít nhất một cách đến root server
 Một máy tính kết nối vào mạng phải biết làm thế nào để liên lạc với ít nhất là một DNS server

Hoạt động của DNS

Khi DNS client cần xác định cho một tên miền nó sẽ truy vấn DNS.
Truy vấn DNS và trả lời của hệ thống DNS cho client sử dụng thủ tục UDP cổng 53, UPD hoạt động ở mức thứ 3 (network) của mô hình OSI, UDP là thủ tục phi kết nối (connectionless), tương tự như dịch vụ gửi thư bình thường bạn cho thư vào thùng thư và hy vọng có thể chuyển đến nơi bạn cần gửi tới.
Mỗi một message truy vấn được gửi đi từ client bao gồm ba phần thông tin :
 Tên của miền cần truy vấn (tên đầy đủ FQDN)
 Xác định loại bản ghi là mail, web ...
 Lớp tên miền (phần này thường được xác định là IN internet, ở đây không đi sâu vào phần này)
Ví dụ : tên miền truy vấn đầy đủ như "hostname.example.microsoft.com.", và loại truy vấn là địa chỉ A. Client truy vấn DNS hỏi "Có bản ghi địa chỉ A cho máy tính có tên là

"hostname.example.microsoft.com" khi client nhận được câu trả lời của DNS server nó sẽ xác định địa chỉ IP của bản ghi A.
Có một số giải pháp để trả lời các truy vấn DNS. Client có thể tự trả lời bằng cách sử dụng các thông tin đã được lưu trữ trong bộ nhớ cache của nó từ những truy vấn trước đó. DNS server có thể sử dụng các thông tin được lưu trữ trong cache của nó để trả lời hoặc DNS server có thể hỏi một DNS server khác lấy thông tin đó để trả lời lại client.
Nói chung các bước của một truy vấn gồm có hai phần như sau:
• Truy vấn sẽ bắt đầu ngay tại client computer để xác định câu trả lời
• Khi ngay tại client không có câu trả lời, câu hỏi sẽ được chuyển đến DNS server để tìm câu trả lời.
Tự tìm câu trả lời truy vấn
Bước đầu tiên của quá trình sử lý một truy vấn. Tên miền sử dụng một chương trình trên ngay máy tính truy vấn để tìm câu trả lời cho truy vấn. Nếu truy vấn có câu trả lời thì quá trình truy vấn kết thúc
Ngay tại máy tính truy vấn thông tin được lấy từ hai nguồn sau:
• Trong file HOSTS được cấu hình ngay tại máy tính. Các thông tin ánh xạ từ tên miền sang địa chỉ được thiết lập ở file này được sử dụng đầu tiên. Nó được tải ngay lên bộ nhớ cache của máy khi bắt đầu chạy DNS client.

• Thông tin được lấy từ các câu trả lời của truy vấn trước đó. Theo thời gian các câu trả lời truy vấn được lưu giữ trong bộ nhớ cache của máy tính và nó được sử dụng khi có một truy vấn lặp lại một tên miền trước đó.
Truy vấn DNS server
Khi DNS server nhận được một truy vấn. Đầu tiên nó sẽ kiểm tra câu trả lời liệu có phải là thông tin của bản ghi mà nó quản lý trong các zone của server. Nếu truy vấn phù hợp với bản ghi mà nó quản lý thì nó sẽ sử dụng thông tin đó để trả lời trả lời (authoritatively answer) và kết thúc truy vấn.
Nếu không có thông tin về zone của nó phù hợp với truy vấn. Nó sẽ kiểm tra các thông tin được lưu trong cache liệu có các truy vấn tương tư nào trước đó phù hợp không nếu có thông tin phù hợp nó sẽ sử dụng thông tin đó để trả lời và kết thúc truy vấn.
Nếu truy vấn không tìm thấy thông tin phù hợp để trả lời từ cả cache và zone mà DNS server quản lý thì truy vấn sẽ tiếp tục. Nó sẽ nhờ DNS server khác để trả lời truy vấn đến khi tìm được câu trả lời.
Các cách để DNS server liên lạc với nhau xác định câu trả lời
Trường hợp Root server kết nối trực tiếp với server tên miền cần truy vấn


Hình 4.1: Root server kết nối trực tiếp với server tên miền cần truy vấn
Trong trường hợp root server biết được DNS server quản lý tên miền cần truy vấn. Thì các bước của truy vấn sẽ như sau:
Bước 1 : PC A truy vấn DNS server tên miền vdc.com.vn. (là local name server) tên miền www.abc.com.
Bước 2 : DNS server tên miền vdc.com.vn không quản lý tên miền www.abc.com do vậy nó sẽ chuyển truy vấn lên root server.
Bước 3 : Root server sẽ xác định được rằng DNS server quản lý tên miền www.abc.com là server DNS.abc.com và nó sẽ chuyển truy vấn đến DNS server DNS.abc.com để trả lời

Bước 4 : DNS server DNS.abc.com sẽ xác định bản ghi www.abc.com và trả lời lại root server
Bước 5 : Root server sẽ chuyển câu trả lời lại cho server vdc.com.vn

Bước 6 : DNS server vdc.com.vn sẽ chuyển câu trả lời về cho PC A và từ đó PC A có thể kết nối đến PC B (quản lý www.abc.com)
Trường hợp root server không kết nối trực tiếp với server tên miền cần truy vấn
1
7
6
3
2
8
P C A W w w . a b c . c o m . s g
V d c . c o m . v n
R o o t s e r v e r
D n s . a b c . c o m . s g
D n s . c o m . s g
4 5
Hình 4.2: Root server không kết nối trực tiếp với server tên miền cần truy vấn
Trong trường hợp không kết nối trực tiếp thì root server sẽ hỏi server trung gian (phân lớp theo hình cây) để xác định được đến server tên miền quản lý tên miền cần truy vấn
Bước 1 - PC A truy vấn DNS server vdc.com.vn (local name server) tên miền www.acb.com.sg.
Bước 2 - DNS server vdc.com.vn không quản lý tên miền www.abc.com.sg vậy nó sẽ chuyển lên root server.
Bước 3 - Root server sẽ không xác định được DNS server quản lý trực tiếp tên miền www.abc.com.sg nó sẽ căn cứ vào cấu trúc của hệ thống tên miền để chuyển đến DNS quản lý cấp cao hơn của tên miền abc.com.sg đó là com.sg và nó xác định được rằng DNS server DNS.com.sg quản lý tên miền com.sg.
Bước 4 - DNS.com.sg sau đó sẽ xác định được rằng DNS server DNS.abc.com.sg có quyền quản lý tên miền www.abc.com.sg.
Bước 5 - DNS.abc.com.sg sẽ lấy bản ghi xác định cho tên miền www.abc.com.sg để trả lời DNS server DNS.com.sg.
Bước 6 - DNS.com.sg sẽ lại chuyển câu trả lời lên root server.
Bước 7 - Root server sẽ chuyển câu trả lời trở lại DNS server vdc.com.vn.
Bước 8 - Và DNS server vdc.com.vn sẽ trả lời về PC A câu trả lời và PC A đã kết nối được đến host quản lý tên miền www.abc.com.sg.
Khi các truy vấn lặp đi lặp lại thì hệ thống DNS có khả năng thiết lập chuyển quyền trả lời đến DNS trung gian mà không cần phải qua root server và nó cho phép thời gian truy vấn được giảm đi.

1
3
7
2 4
8
PC A Www.abc.com.sg
Vdc.com.vn
Root server
Dns.abc.com.sg
Dns.com.sg
5 6
Hoạt động của DNS cache
Khi DNS server sử lý các truy vấn của client và sử dụng các truy vấn lặp lại. Nó sẽ xác định và lưu lại các thông tin quan trọng của tên miền mà client truy vấn. Thông tin đó sẽ được ghi lại trong bộ nhớ cache của DNS server.

Cache lưu giữ thông tin là giải pháp hữu hiệu tăng tốc độ truy vấn thông tin cho các truy vấn thường xuyên của các tên miền hay được sử dụng và làm giảm lưu lượng thông tin truy vấn trên mạng.
DNS server khi thực hiện các truy vấn đệ quy cho client thì DNS server sẽ tạm thời lưu trong cache bản ghi thông tin (resource record - RR) lấy được từ DNS server lưu trữ thông tin về truy vấn đó. Sau đó một client khác truy vấn yêu cầu thông tin của đúng bản ghi đó thì nó sẽ lấy thông tin ban ghi (RR) lưu trong cache để trả lời.
Khi thông tin được lưu trong cache. Thì các bản ghi RR được ghi trong cache sẽ được cung cấp thời gian sống (TTL - Time-To-Live). Thời gian sống của một bản ghi trong cache là thời gian mà nó tồn tại trong cache và được dùng để trả lời cho các truy vấn của client khi truy vấn tên miền trong bản ghi đó. Thời gian sống (TTL) được khai khi cấu hình cho các zone. Giá trị mặc định nhỏ nhất của thời gian sống (Minimum TTL) là 3600 giây (1 giờ) như giá trị này ta có thể thay đổi khi cấu hình zone. Hết thời gian sống bản ghi sẽ được xóa khỏi bộ nhớ cache.

4. Bài tập thực hành

Bài 1: Cài đặt DNS Server cho Window 2000

Mở cửa sổ quản lý DNS

Bước 1: Mở của sổ quản lý DNS

Bấm vào mune *Start* chọn *Programs* và sau đó là *"Administrative tools"* Chọn *"DNS Manager"*

Bước 2: Cửa sổ quản lý DNS server sẽ xuất hiện

Tại cửa số quản lý DNS server bạn có thể khai báo các tính năng của DNS

Thêm trường (zone)

zone là tên miền (domain name) mà server quản lý. Tại cửa sổ quản lý DNS tại phần server quản lý bấm chuột phải để hiện menu và chọn *"new zone*" như hình trên

Bấm và *"new zone"* sẽ hiện cửa sổ cho phép chọn kiểu dữ liệu mà zone quản lý. *Standard Primary* là loại dữ liệu của zone được khai báo và quản lý ngay tại server. Còn *Stardard Secondary* là loại zone mà dữ liệu được lấy về từ *Standard Primary* và dữ liệu cũng nằm trên server . *Standard Primary* thường sử dụng để dự phòng cho các zone đã tồn tại. Bấm *Next* để tiếp tục

Sẽ xuất cửa sổ như trên. *Forward lookup zone* là loại zone quản lý việc chuyển đổi từ domain name sang địa chỉ IP. Còn phần *Reverse lookup zone* quản lý việc chuyển đổi từ IP sang Domain name. Bấm *Next* tiếp tục

Tại cửa sổ này điền zone (domain name) mà sẽ quản lý. Bấm Next tiếp tục

Điền tên của file để lưu trữ zone tại *"Create a new file with this file name"* hoặc sử dụng file có sẵn tại *"Use this existing file"* Và bấm *Next* cho đến khi xuất hiện nút *finish* để kết thúc tạo zone

Thêm tên miên (domain name)

Tại của sổ quản lý domain chọn vào server và bấm chuột phải hiện lên menu và chọn *"New Domain..."* để điền một domain mới.

Sau khi bấm vào *"New Domain"* nó sẽ xuất hiện cửa sổ cho phép bạn điền tên miền mà server được phép quản lý. Sau khi điền bấm *"OK"* để kết thúc

Thêm một host mới

Tại cửa sổ quản lý DNS chọn zone đã tạo và bấm chuột phải chọn *"new host"*

Xuất hiện cửa sổ cho phép ta khai báo host mới

Bạn điền tên của host mà muốn tạo. Tên của host sẽ được tự động điền thêm phần domain để thành tên đầy đủ của host.

Ví dụ: như trên đây là vùng quản lý zone (*location*) là ktm.vnn.vn. Vậy khi bạn điền *Name* là www và *IP address* là 203.162.0.100 thì sẽ tương ứng với định nghĩa domain www.ktm.vnn.vn. trỏ đến địa chỉ IP 203.162.0.100

www.ktm.vnn.vn. IN A 203.162.0.100

Tạo một bản ghi web (tạo bí danh)

Tại cửa sổ quản lý Domain và tên miền vừa tạo và bấm chuột phải và chọn *"New Alias"* để tạo một CNAME đến một host.

Bấm và *"New Alias..."* sẽ xuất hiện cửa sổ cho phép khai báo Alias

Tại phần *"Alias name"* điền tên tạo alias và tại phần *"Fully qualified name for target host"* điền tên đầy đủ của một host mà muốn tạo bí danh (thường được sử dụng cho webhosting)

Ví dụ : www.ktm.vnn.vn. IN CNAME ktm.vnn.vn.

Ta sẽ có trang web www.ktm.vnn.vn đặt trên server web có tên là ktm.vnn.vn.

Tạo một bản ghi thư điện tử (MX)

Tại cửa sổ quản lý DNS tại tên miền muốn tạo bản ghi MX bấm chuột phải

Sau khi bấm vào*"New Mail Exchanger.."* sẽ xuất hiện cửa sổ cho phép tạo các thông số cho bản ghi mx

Điền tại *"Host or domain"* điền tên hoặc để trống tên này kết hợp với phần zone "*Parent domain"* để tạo thành domain đầy đủ của bản ghi thư điện tử. Tại *"Mail server"* điền tên của server thư điện tử và tại *"Mail server priority"* điền mức độ ưu tiên của server thư điện tử (độ lớn càng nhỏ mức ưu tiên càng cao)

Ví dụ trên hình ta có:

mail.ktm.vnn.vn IN MX 10 mr-hn.vnn.vn.

Ta có tên miền thư điện tử mail.ktm.vnn.vn. (ta có thể tạo được các hộp thư abc@mail.ktm.vnn.vn) được chứa tại server thư điện tử mrhn.vnn.vn với mức ưu tiên là 10

Chuyển quyền quản lý têm miền (delegate)

Tại cửa sổ quản lý DNS tại domain muốn chuyển quyền quản lý bấm chuột phải.

Bấm vào *"New Delegation..."* để hiện cửa sổ cho phép chuyển quyền quản lý tên miền

Điền phần domain mà bạn muốn chuyển quyền quản lý vào *"Delegated domain"*
Ví dụ ở đây điền là abc nghĩa là bạn muốn chuyển quyền quản lý domain abc.ktm.vnn.vn. Bấm *"Next"* để tiếp tục

Hiện cửa sổ điền vào *"Server name"* tên của DNS server sẽ được phép quản lý tên miền abc.ktm.vnn.vn. Bấm *"Resolve"* để xác định địa chỉ IP của DNS server. Sau đó bấm *"Ok"* để kết thúc.
Ví dụ abc.ktm.vnn.vn. IN NS vdc-hn01.vnn.vn.
Tương ứng tên miền abc.ktm.vnn.vn. sẽ được chuyển quyền về DNS server vdc-hn01.vnn.vn để quản lý.

Bài 2: Cài đặt, cấu hình DNS cho Linux

Hiện tại trên Internet rất nhiều nhà cung cấp phần mềm miễn phí cho DNS. Nhưng phần mền sử dụng DNS cho unix được sử dụng phổ biến hiện này là gói phần mềm cho DNS là Bind
Bind được phát triển bởi một tổ chức phi lợi nhuận là Internet Software Consortium (www.isc.org) và nó cung cấp phần mền bind miễn phí.
Hiện tại phần mềm bind có version là 9.2.2
Phần mền Bind còn cung cấp tiện ích nslookup là công cụ rất tiện lợi cho việc kiểm tra tên miền
Khai báo DNS cho client/server
Với client sử dụng linux hoặc unix ta vào file /etc/resolv.conf
 Client chỉ lấy thông tin về các domain
 Client chỉ gửi query tới server và nhận trả lời
Cấu hình DNS server
 Cấu bình resolver như của (DNS client)
 Cấu hình Bind cho name server (named)

 Xây dự cơ sở dữ liệu cho DNS (cho các zone file)
Cấu hình cho DNS client /etc/resolv.conf
Các từ khóa Miêu tả
nameserver *địa chỉ* Địa chỉ IP của DNS server sẽ gửi truy vấn đến để lấy thông tin về domain
domain *name* xác định domain mặc định của client
Với DNS client chỉ cần cấu hình file resolv.conf
Cài đặt DNS server.
Ta có thể lấy chương trình cài đặt bind cho DNS tại www.isc.org lấy về server
cd /usr/src
mkdir bind-9.xx
cd bind-9.xx
Lấy chương trình cài đặt DNS về đây bind-9.xx-src.tar.gz
gunzip bind-9.xx-src.tar.gz
tar xf bind-9.xx-src.tar
rm bind-9.xx-src.tar
cd src
make clean
make depend
make install

Vậy là ta đã cài xong phần mền named cho DNS và các zone file sẽ được chứa trong /var/named còn file cấu hình nằm trong /usr/local/etc vậy ta phải tạo và đặt file cấu hình và zone file vào các thư mục trên và chạy
#/usr/local/sbin/named
Vậy là server đã sẵn sàng cho truy vấn DNS

Cấu trúc file cơ sở dữ liệu (zone file)
Các file cơ sở dữ liệu zone được chỉ làm hai loại cho domain (có dạng db.domain hoặc domain.root) và các domain ngược (db.address) và nó nằm trong thư mục /var/named của DNS server.
Các dữ liệu nằm trong file cơ dữ liệu được gọi là DNS resource record.
Các loại resource record trong file dữ liệu bao gồm:
SOA record
Chỉ rõ domain ở cột quản lý bởi name server ghi sau trường SOA. Trong trường hợp file db.domain
@ IN SOA vdc-hn01.vnn.vn. postmaster.vnn.vn. (
1999082802 ; serial number
1800 ; refresh every 30 mins
3600 ; retry every hour
86400 ; expire after 24 hours
6400 ; minimum TTL 2 hours
)
IN NS vdc-hn01.vnn.vn.
IN NS hcm-server1.vnn.vn.
Khai báo zone ngược db.203.162.0
@ IN SOA vdc-hn01.vnn.vn. postmaster.vnn.vn. (
1999082301 ; Serial
10800 ; Refresh after 3 hours
3600 ; Retry after 1 hour
604800 ; Expire after 1 week
86400) ; Minimum TTL of 1 day
; name servers
IN NS vdc-hn01.vnn.vn.
IN NS hcm-server1.vnn.vn.
6 IN PTR ldap.vnn.vn.
7 IN PTR hanoi-server1.vnn.vn.
8 IN PTR hanoi-server2.vnn.vn.
9 IN PTR mail.vnn.vn.
Trong mỗi zone chỉ khai một trường SOA. Như ví dụ trên trong trường hợp file db.com.vn, chữ @ biể thị các tất cả các domain trong file quản lý bởi name server vdc-hn01.vnn.vn và địa chỉ mail của admin mạng là postmaster.vnn.vn. Ngoài ra trong phần SOA có 5 thông số cần quản tâm sau:
Serial number : Thông số này có tác dụng với tất cả các dữ liệu trong file. Khi secondary server yêu cầu primary server các thông tin về domain mà nó quản lý thì đầu tiên nó sẽ so sánh serial number của secondary và primary server.

Nếu serial number của secondary server nhỏ hơn của primary server thì dữ liệu của domain sẽ được cập nhập lại cho secondary server từ secondary server.
Mỗi khi ta thay đổi nội dung của file db.domain thì ta cần phải thay đổi serial number và thường ta đánh serial number theo nguyên tắc sau:
Serial number : yyyymmddtt
trong đó : yyyy là năm
mm là tháng

dd là ngày
tt là số lần sửa đổi trong ngày
Refresh: là chu kỳ thời gian mà secondary server sẽ sánh và cập nhập lại dữ liệu của nó với primary server
Retry: nếu secondary server không kết nối được với primary server thì cứ sau một khoảng thời gian thì nó sẽ kết nối lại
Expire : là khoảng thời gian mà domain sẽ hết hiệu lực nếu secondary không kết nối được với primary server.
TTL (time to live) : khi một server bất kỳ yêu cầu thông tin về dữ liệu nào đó từ primary server, và dữ liệu đó sẽ được lưu giữ tại server đó và có hiệu lực trong khoảng thời gian của TTL. Hết khoảng thời gian đó nếu tiếp tục cần thì nó lại phải truy vấn lại primary server.

Các bản ghi thường dùng trong DNS server

NS (name server) : Bản ghi NS để xác định DNS server nào sẽ quản lý tên miền. Như ví dụ ở trên là DNS server vdc-hn01.vnn.vn. và hcmserver1. vnn.vn.
A (address) : Bản ghi dạng A cho tương ứng một domain name với một địa chỉ IP. Chỉ cho phép khai báo một bản ghi A cho một địa chỉ IP.
Ví dụ:

Tên miền Internet Loại bản ghi Địa chỉ
mr.vnn.vn. IN A 203.162.4.148
mr-hn.vnn.vn. IN A 203.162.0.24
mail.vnn.vn. IN A 203.162.0.9
fmail.vnn.vn. IN A 203.162.4.147
hot.vnn.vn. IN A 203.162.0.23
home.vnn.vn. IN A 203.162.0.12

www.vnn.vn. IN A 203.162.0.16
CNAME (canonical name) : là tên phụ cho một host có sẵn tên miền dạng A. Nó thường được sử dụng cho các server web, ftp
Ví dụ : các domain có dạng CNAME được chỉ tới các máy chủ web

Tên miền Internet Loại bản ghi Server
www.gpc.com.vn. IN CNAME home.vnn.vn.
www.huonghai.com.vn. IN CNAME home.vnn.vn.
www.songmayip.com.vn. IN CNAME hot.vnn.vn.
www.covato2.com.vn. IN CNAME hot.vnn.vn.
MX (mail exchange): là tên phụ cho các dịch vụ mail trên các máy chủ đã có tên miền dạng A. Bản ghi này cho phép máy chủ có thể cung cấp dịch vụ mail cho các domain khác nhau. Có thể khai báo nhiều domain khác nhau cùng chỉ tới một server hoặc một domain trỏ tới nhiều server khác nhau (sử dụng backup) trong trường hợp này giá trị ưu tiên phải đặt khác nhau. Với số ưu tiên càng nhỏ thì mức độ ưu tiên càng cao.
Ví dụ

Tên miền *Internet* **Loại bản ghi**
mức ưu tiên
Server
mrvn.vnn.vn. IN MX 10 mr.vnn.vn.
clipsalvn.vnn.vn. IN MX 10 mr-hn.vnn.vn.
dbqnam.vnn.vn. IN MX 10 mr-hn.vnn.vn.

thangloi.vnn.vn. IN MX 50 mail.netnam.vn.
IN MX 100 fallback.netnam.vn.
PTR (Pointer) : là bản ghi tương ứng địa chỉ IP với domain. Các file dạng db.address. Ví dụ db.203.162.0 cho tương ứng với các địa chỉ IP tương ứng với mạng 203.162.0.xxx
Chú ý :
Trước mỗi phần khai báo domain thường có dòng
$ORIGIN *domain.*
Để khai báo giá trị mặc định của domain. Cho phép trong phần khai báo giá trị không phải khai báo lặp lại phần domain mặc định.
Ví dụ :
vdc.com.vn. IN A 203.162.0.49
hoặc

$ORIGIN com.vn.
vdc IN A 203.162.0.49
Dấu "**;**" được sử dụng làm ký hiệu dòng chú thích, các phần sau dấu ";" đều không có tác dụng.
Định nghĩa cấu hình (name.conf)
Khi các file cơ sở dữ liệu (zone file) thì cần phải cấu hình để DNS server đọc các zone file đó. Đối với hệ thống BIND cơ chế chỉ dẫn name server đọc các zone file được khai trong file named.conf nó được nằm trong thư mục /etc hoặc /usr/local/etc
Ví dụ : khai báo file db trong file named.conf:
```
; khai báo cho zone file domain.vn
zone "vn." in {
type master;
file "db.vn";
};
;khai báo cho zone file domain.gov.vn
zone "gov.vn." in {
type master;
file "db.gov.vn";
};
;khai báo cho zone ngược 203.162.0.xxx
zone "0.162.203.in-addr.arpa" in {
type master;
file "db.203.162.0";
};
;khai báo cho zone ngược 203.162.1.xxx
zone "1.162.203.in-addr.arpa" in {
type master;
file "db.203.162.1";
};
```
Chú ý: sau mỗi lần thay đổi dữ liệu để sửa đổi có tác dụng thì cần phải làm động tác để DNS server cập nhập thay đổi
%su
%password:
ps -ef | grep named
root 17413 1 5 Sep 07 ? 189:52 /usr/local/sbin/named
kill -HUP 17413
Còn để chạy DNS server

#/usr/local/sbin/named
Hướng dẫn sử dụng nslookup
nslookup - là công cụ trên internet cho phép truy vấn tên miền và địa chỉ IP một cách tương tác.
Cấu trúc câu lệnh
nslookup [-option ...] [host-to-find | - [server]]
Miêu tả các lệnh của nslookup
server domain & lserver domain Change the default server to domain. Lserver uses the initial server to look up information about domain while server uses the current default server. If an authoritative answer can't be found, the names of servers that might have the answer are returned.
root Thay đổi server mặc định sẽ làm root cho domain truy vấn.
ls [option] domain [>> filename]
Hiện danh sách thông tin của domain. Mặc định là hiện tên của host và địa chỉ IP. Ta có thể sử dụng các lựa chọn để hiện nhiều thông tin hơn:
-t querytype hiện danh sách tất cả bản ghi xác định bởi loại querytype
-a hiện danh sách các bí danh (aliaes) của domain host (tương tự như -t CNAME)
-d hiện danh sách các bản ghi của domain (tương tự như -t ANY)
-h hiện danh sách thông tin về CPU và thông tin về hệ điều hành của domain. (tương tự như -t HINFO)
? hiện danh sách các câu lệnh.
exit thoát khỏi chương trình.
set keyword[=value] câu lệnh dùng để thay đổi trạng thái thông tin mà có ảnh hưởng đến truy vấn. Các từ khoá:
all cho phép hiện tất cả các loại bản ghi
[no]debug bật chế độ tìm lỗi. Cho hiện rất nhiều loại thông tin cho phép xác định lỗi truy vấn đến domain. (mặc định=nodebug, viết tắt = [no]deb)
[no]d2 Bật chế độ tìm lỗi mức cao hơn. Tất cả các gói tin truy vấn đều được xuất hiện. (mặc định=nod2)
domain=name Thay đổi domain mặc định vào tên. Khi truy vấn một tên nó sẽ tự động điền thêm domain vào sau.
port=value Chuyển cổng mặc định sử dụng cho TCP/UDP name server thành cổng được thiết lập bởi giá trị này (mặc định= 53, viết tắt = po)
querytype=value
type=value Chọn loại truy vấn thông tin. Có các loại sau:
A truy vấn host (khai báo địa chỉ IP).

CNAME (canonical name) tạo tên bí danh (thường dùng cho web)
HINFO truy vấn loại CPU và hệ điều hành của server.
MINFO thông tin vê hộp thư hoặc mail list.
MX truy vấn về mail exchanger.
NS truy vấn về named zone.
PTR truy vấn chuyển từ địa chỉ IP sang domain.
SOA Thông tin về người quản lý về zone.
TXT Các thông tin khác.
UINFO Thông tin về người dùng.
WKS Hỗ trợ cho các dịch vụ khác.
Các loại khác (**ANY**, **AXFR**, **MB**, **MD**, **MF**, **NULL**) được miêu tả chi tiết trong tiêu chuẩn **RFC-1035** . (Mặc định = A, viết tắt = q, ty)

[no]recurse Yêu cầu name server truy vấn tới một server khác nếu nó không có thông tin về domain cần tìm. (mặc định = recurse, viết tắt = [no]rec)
retry=number Thiết lập số lần truy vấn. Khi truy vấn mà không nhận được trả lời trong khoảng thời gian nhất định (thiết lập bằng lệnh set timeout). Khi thời gian hết thì yêu cầu truy vấn sẽ được gửi lại. Và thiết lập ở đây để điều khiển số lần sẽ gửi lại trước khi từ bỏ truy vấn. (Mặc định = 4, viết tắt = ret)
root=host Đổi root server cho host
timeout=number Thiết lập thời gian timeout cho một quá trìn truy vấn tính bằng giây. (mặc định = 5 giây, viết tắt = ti)
[no]vc sử dụng một virtual circuit để gửi yêu cầu truy vấn đến server. (mặc định là = novc, viết tắt = [no]v)

Phân tích lỗi

Nếu truy vấn lookup không thành công thì một thông tin về lỗi sẽ được hiện ra. Và các lỗi có thể là :

Timed out

Server không trả lời truy vấn sau một khoảng thời gian (khoảng thời gian có thể thay đổi bằng câu lệnh *set timeout=value*) và and a certain number of retries (changed with set retry=value).

No response from server

Không có name server đang chạy tại server mà client chỉ đến.

No records

Server không có bản ghi tương ứng loại mà truy vấn cho host đa tồn tại. Loại truy vấn được thiết lập bằng câu lệnh "*set querytype"* .

Non-existent domain

Host hoặc domain name không tồn tại.

Connection refused

Network is unreachable

Kết nối tới name server hoặc finger server không thể được tại thời điểm này. Lệnh này thường xuất hiện với các yêu cầu của câu lệnh ls và finger.

Server failure

Name server tìm thấy lỗi trong dữ liệu về domain và không thể đưa ra câu trả lời đúng.

Refused

Name server từ chối yêu cầu trả lời.

Format error

Name server thấy rằng các gói tin yêu cầu không đúng định dạng. Nó có thể là lỗi của chương trình nslookup.

Ví dụ :

Truy vấn DNS sử dụng bản ghi a cho domain home.vnn.vn có địa chỉ IP là 203.162.0.12

```
Default Server: vdc-hn01.vnn.vn
Address: 203.162.0.11
Aliases: 11.0.162.203.in-addr.arpa
> set querytype=a
> home.vnn.vn
Server: vdc-hn01.vnn.vn
Address: 203.162.0.11
Aliases: 11.0.162.203.in-addr.arpa
```

Name: home.vnn.vn
Address: 203.162.0.12
>
Truy vấn bản ghi
mx (mail) cho
domain hn.vnn.vn
nó trỏ đến các host
mu13.vnn.vn có địa
chỉ 203.162.0.55 và
mu14.vnn.vn có địa
chỉ 203.162.0.64
> set querytype=mx
> hn.vnn.vn
Server: vdc-hn01.vnn.vn
Address: 203.162.0.11
Aliases: 11.0.162.203.in-addr.arpa
hn.vnn.vn MX preference = 20, mail exchanger = mu13.vnn.vn
hn.vnn.vn MX preference = 10, mail exchanger = mu14.vnn.vn
vnn.vn nameserver = vdc-hn01.vnn.vn
vnn.vn nameserver = hcm-server1.vnn.vn
mu13.vnn.vn internet address = 203.162.0.55
mu14.vnn.vn internet address = 203.162.0.64
vdc-hn01.vnn.vn internet address = 203.162.0.11
hcm-server1.vnn.vn internet address = 203.162.4.1
>
Truy vấn loại ns > set querytype=ns

(name server) cho
domain vn do các
server nào quản lý
sẽ cho ta một danh
sách các nameserver
quản ly các domain
có đuôi vn
> vn
Server: vdc-hn01.vnn.vn
Address: 203.162.0.11
Aliases: 11.0.162.203.in-addr.arpa
Non-authoritative answer:
vn nameserver = DNS-hcm01.vnnic.net.vn
vn nameserver = ns.ripe.net
vn nameserver = DNS1.vn
vn nameserver = ns1.gip.net
vn nameserver = ns2.gip.net
vn nameserver = ns3.rip.net
vn nameserver = DNS1.vnnic.net.vn
vn nameserver = cheops.anu.edu.au
DNS-hcm01.vnnic.net.vn internet address = 203.162.87.66
ns.ripe.net AAAA IPv6 address = 2001:610:240:0:53:0:0:193
ns.ripe.net internet address = 193.0.0.193
DNS1.vn internet address = 203.162.3.235
ns1.gip.net internet address = 204.59.144.222
ns2.gip.net internet address = 204.59.1.222
DNS1.vnnic.net.vn internet address = 203.162.57.105
cheops.anu.edu.au internet address = 150.203.224.24
>

Chương 5
Dịch vụ truy cập từ xa và dịch vụ Proxy

Chương 5 cung cấp các kiến thức cơ bản của hai nội dung dịch vụ phổ biến trên mạng máy tính: dịch vụ truy cập từ xa và dịch vụ proxy.

Việc truy cập từ xa là nhu cầu thiết yếu mở rộng phạm vi hoạt động mạng của các tổ chức, công ty. Nội dung truy cập từ xa giới thiệu trong chương này là truy cập qua mạng thoại PSTN. Đây là hình thức truy cập từ xa cho tốc độ truy cập thấp vừa phải nhưng lại có tính phổ biến rộng rãi và dễ thiết lập nhất.

Dịch vụ proxy trên mạng được phát triển cho các mục đích tăng cườ_____ng tốc độ truy nhập cho khách hàng trong mạng, tiết kiệm được tài nguyên mạng (địa chỉ IP) và đảm bảo được an toàn cho mạng lưới khi bắt buộc phải cung cấp truy nhập ra mạng ngoài hay ra mạng Internet. Thiết lập dịch vụ proxy là công tác mọi quản trị hệ thống mạng cần biết vì các nhu cầu kết nối liên mạng và kết nối Internet càng ngày càng trở nên không thể thiếu cho bất kỳ tổ chức, công ty nào.

Chương 5 yêu cầu các học viên nên trang bị các kiến thức cơ bản về mạng điện thoại PSTN, kiến thức về các giao thức mạng WAN PPP, SLIP... các giao thức xác thực như RADIUS...Trong phần proxy, học viên cần làm quen với khái niệm chuyển đổi địa chỉ NAT, hoạt động của các giao thức TCP/IP.

Mục 1: Dịch vụ truy cập từ xa (Remote Access)

1. Các khái niệm và các giao thức

1.1. Tổng quan về dịch vụ truy cập từ xa.

Dịch vụ truy nhập từ xa (Remote Access Service) cho phép người dùng từ xa có thể truy cập từ một máy tính qua một môi trường mạng truyền dẫn (ví dụ mạng điện thoại công cộng) đến một mạng dùng riêng như thể máy tính đó được kết nối trực tiếp trong mạng đó. Người dùng từ xa kết nối tới mạng đó thông qua một máy chủ dịch vụ gọi là máy chủ truy cập (Access server). Khi đó người dùng từ xa có thể sử dụng tài nguyên trên trên mạng như là một máy tính kết nối trực tiếp trong mạng đó. Dịch vụ truy nhập từ xa cũng cung cấp khả năng tạo lập một kết nối WAN thông qua các mạng phương tiện truyền dẫn giá thành thấp như mạng thoại công cộng. Dịch vụ truy cập từ xa cũng là cầu nối để một máy tính hay một mạng máy tính thông qua nó được nối đến Internet theo cách được coi là hợp lý với chi phí không cao, phù hợp với các doanh nghiệp, tổ chức qui mô vừa và nhỏ. Khi lựa chọn và thiết kế giải pháp truy cập từ xa, chúng ta cần thiết phải quan tâm đến các yêu cầu sau:

− Số lượng kết nối tối đa có thể để phục vụ người dùng từ xa.

− Các nguồn tài nguyên mà người dùng từ xa muốn muốn truy cập.

− Công nghệ, phương thức và thông lượng kết nối. Ví dụ, các kết nối có thể sử dụng modem thông qua mạng điện thoại công cộng PSTN, mạng số hoá tích hợp các dịch vụ ISDN...

− Các phương thức an toàn cho truy cập từ xa, phương thức xác thực người dùng, phương thức mã hoá dữ liệu

− Các giao thức mạng sử dụng để kết nối.

1.2.Kết nối truy cập từ xa và các giao thức sử dụng trong truy cập từ xa

Kết nối truy cập từ xa

Tiến trình truy cập từ xa được mô tả như sau: người dùng từ xa khởi tạo

một kết nối tới máy chủ truy cập. Kết nối này được tạo lập bằng việc sử dụng một giao thức truy cập từ xa (ví dụ giao thức PPP- Point to Point Protocol). Máy chủ truy cập xác thực người dùng và chấp nhận kết nối cho tới khi kết thúc bởi người dùng hoặc người quản trị hệ thống. Máy chủ truy cập đóng vai trò như một gateway bằng việc trao đổi dữ liệu giữa người dùng từ xa và mạng nội bộ. Bằng việc sử dụng kết nối này, người dùng từ xa gửi và nhận dữ liệu từ máy chủ truy cập. Dữ liệu được truyền trong các khuôn dạng được định nghĩa bởi các giao thức mạng (ví dụ giao thức TCP/IP) và sau đó được đóng gói bởi các giao thức truy cập từ xa. Tất cả các dịch vụ và các nguồn tài nguyên trong mạng người dùng từ xa đều có thể sử dụng thông qua kết nối truy cập từ xa này (hình 5.1)

Hình 5.1: Kết nối truy cập từ xa

Giao thức truy cập từ xa

SLIP (Serial Line Interface Protocol), PPP và Microsoft RAS là các giao thức truy cập để tạo lập kết nối được sử dụng trong truy cập từ xa. SLIP là giao thức truy cập kết nối điểm-điểm và chỉ hỗ trợ sử dụng với giao thức IP, hiện nay hầu như không còn được sử dụng. Microsoft RAS là giao thức riêng của Microsoft hỗ trợ sử dụng cùng với các giao thức NetBIOS, NetBEUI và đượ_____c sử dụng trong các phiên bản cũ của Microsoft.

PPP giao thức truy cập kết nối điểm-điểm với khá nhiều tính năng ưu việt, là một giao thức chuẩn được hầu hết các nhà cung cấp hỗ trợ. RFC 1661 định nghĩa về PPP. Chức năng cơ bản của PPP là đóng gói thông tin giao thức lớp mạng thông qua các liên kết điểm – điểm.

Cơ chế làm việc và vận hành của PPP như sau: Để thiết lập truyền thông, mỗi đầu cuối của liên kết PPP phải gửi các gói LCP (Link Control Protocol) để thiết lập và kiểm tra liên kết dữ liệu. Sau khi liên kết được thiết lập với các tính năng tùy chọn được sắp đặt và thỏa thuận giữa hai đầu liên kết, PPP gửi các gói NCP (Network Control Protocol) để lựa chọn và cấu hình một hoặc nhiều giao thức lớp mạng. Mỗi lần một giao thức lớp mạng lựa chọn đã được cấu hình, lưu lượng từ mỗi giao thức lớp mạng có thể gửi qua liên kết này. Liên kết tồn tại cho đến khi các gói LCP hoặc NCP đóng kết nối hoặc đến khi một sự kiện bên ngoài xảy ra (chẳng hạn như một sự kiện hẹn giờ hay một sự can thiệp của người quản trị). Nói cách khác PPP là một con đường mở đồng thời cho nhiều giao thức.

PPP khởi đầu được phát triển trong môi trường mạng IP, tuy nhiên nó thực hiện các chức năng độc lập với các giao thức lớp 3 và có thể được sử dụng cho các giao thức lớp mạng khác nhau. Như đã đề cập, PPP đóng gói các thủ tục lớp mạng đã được cấu hình để chuyển qua một liên kết PPP. PPP có nhiều các tính năng khiến nó rất mềm dẻo và linh hoạt, bao gồm:

- Ghép nối với các giao thức lớp mạng
- Lập cấu hình liên kết
- Kiểm tra chất lượng liên kết
- Nhận thực
- Nén các thông tin tiếp đầu
- Phát hiện lỗi
- Thỏa thuận các thông số liên kết

PPP hỗ trợ các tính năng này thông qua việc cung cấp LCP có khả năng mở rộng và NCP để thỏa thuận các thông số và các chức năng tùy chọn giữa các đầu cuối. Các giao thức, các tính năng tùy chọn, kiểu xác thực người dùng tất cả đều được truyền thông trong khi khởi tạo liên kết giữa hai điểm.

PPP có thể hoạt động trong bất kỳ giao diện DTE/DCE nào, PPP có thể hoạt động ở chế độ đồng bộ hoặc không đồng bộ. Ngoài những yêu cầu khác của các giao diện DTE/DCE, PPP không có hạn chế nào về tốc độ truyền dẫn. Trong hầu hết các công nghệ mạng WAN, mô hình lớp được đưa ra để có những điểm liên hệ với mô hình OSI và để diễn tả vận hành của các công nghệ cụ thể. PPP không khác nhiều so với các công nghệ khác. PPP cũng có mô hình lớp để định nghĩa các cấu trúc và chức năng (hình 5.2)

Hình 5.2: Mô hình lớpPPP

Cũng như hầu hết các công nghệ, PPP có cấu trúc khung, cấu trúc này cho phép đóng gói bất cứ giao thức lớp 3 nào. Dưới đây là cấu trúc khung PPP (hình 5.3)

Hình 5.3: Cấu trúc khung PPP

Các trường của khung PPP như sau:

Cờ: độ dài 1 byte sử dụng để chỉ ra rằng đây là điểm bắt đầu hay kết thúc một khung, trường này là một dãy bit 01111110

Địa chỉ: độ dài 1 byte bao gồm dãy bit 11111111, là địa chỉ quảng bá chuẩn. PPP không gán từng địa chỉ riêng.

Giao thức: độ dài 2 byte, nhận dạng giao thức đóng gói. Giá trị cập nhật của trường này được chỉ ra trong RFC 1700

Dữ liệu: có độ dài thay đổi, có thể 0 hoặc nhiều byte là các dữ liệu cho kiểu giao thức cụ thể đượoc chỉ ra trong trường giao thức. Phần cuối cùng của trường dữ liệu được nhận biết bằng cách đặt cờ và tiếp sau nó là 2 byte FCS. Giá trị ngầm định của trường này là 1500 byte. Tuy vậy giá trị lớn hơn có thể được sử dụng để tăng độ dài cho trường dữ lliệu.

FCS: thường là 2 byte, có thể sử dụng 4 byte FCS để tăng khả năng phát hiện lỗi.

LCP có thể thỏa thuận để chấp nhận sự thay đổi cấu trúc khung PPP chuẩn giữa hai đầu cuối của liên kết. Các khung đã thay đổi luôn luôn dễ nhận biết hơn so với các khung chuẩn. LCP cung cấp phương pháp để thiết lập, cấu hình, duy trì và kết thúc một kết nối điểm-điểm. LCP thực hiện các chức năng này thông qua bốn giai đoạn. Đầu tiên, LCP thực hiện thiết lập và thỏa thuận cấu hình giữa liên kết điểm điểm. Trước khi bất kỳ đơn vị dữ liệu lớp mạng nào được chuyển, LCP đầu tiên phải mở kết nối và thỏa thuận các thông số thiết lập. Quá trình này được hoàn thành khi một khung nhận biết cấu hình đã được gửi và nhận. Tiếp theo, LCP xác định chất lượng liên kết. Liên kết được kiểm tra để xác định xem liệu chất lượng có đủ để khởi tạo các giao thức lớp mạng không. Việc truyền dẫn của giao thức lớp mạng bị đình lại cho đến khi giai đoạn này hoàn tất. LCP cho phép đây là một tùy chọn sau giai đoạn thiết lập và thỏa thuận cấu hình của liên kết. Sau đó LCP thực hiện thỏa thuận cấu hình giao thức lớp mạng. Các giao thức lớp mạng có thể được cấu hình riêng rẽ bởi NCP thích hợp và được khởi tạo hay dỡ bỏ vào bất kỳ thời điểm nào. Cuối cùng, LCP kết thúc liên kết khi xuất hiện yêu cầu từ người dùng hoặc theo các bộ định thời gian, do lỗi truyền dẫn hay do các yếu tố vật lý khác.

Ba kiểu khung LCP được sử dụng để hoàn thành các công việc đối với từng giai đoạn: khung thiết lập liên kết được sử dụng để thiết lập và cấu hình một liên kết, khung kết thúc liên kết được sử dụng để kết thúc một liên kết, khung duy trì liên kết được sử dụng để quản lý và gỡ rối liên kết.

Các giao thức mạng sử dụng trong truy cập từ xa.
Khi triển khai dịch vụ truy cập từ xa, các giao thức mạng thường được sử dụng là giao thức TCP/IP, IPX, NETBEUI.
TCP/IP là một bộ giao thức gồm có giao thức TCP và giao thức IP cùng làm việc với nhau để cung cấp phương tiện truyền thông trên mạng. TCP/IP là một bộ giao thức cơ bản, làm nền tảng cho truyền thông liên mạng là bộ giao thức mạng được sử dụng phổ biến nhất hiện nay. Với khả năng định tuyến và mở rộng, TCP/IP hỗ trợ một cách linh hoạt và phù hợp cho các tất cả các mạng.
IPX (Internet Packet Exchange) là giao thức được sử dụng cho các mạng Novell NetWare. IPX là một giao thức có khả năng định tuyến và thường được sử dụng với các hệ thống mạng trước đây.
NetBEUI là giao thức dùng cho mạng cục bộ LAN của Microsoft.
NetBEUI cho ta nhiều tiện ích và hầu như không phải làm gì nhiều với NetBEUI. Thông qua NetBEUI ta có thể truy cập tất cả các tài nguyên trên mạng. NETBEUI là một giao thức không có khả năng định tuyến và chỉ thích hợp với mô hình mạng nhỏ, đơn giản.

1.3. Modem và các phương thức kết nối vật lý.

1. Modem.
Máy tính làm việc với dữ liệu dạng số, khi truyền thông trên môi trường truyền dẫn với các dạng tín hiệu khác (ví dụ như với mạng điện thoại công cộng làm việc với các tín hiệu tương tự) ta cần một thiết bị để chuyển đổi tín hiệu số thành tín hiệu thích nghi với môi trường truyền dẫn, thiết bị đó gọi là Modem (Modulator/demodulator). Như vậy Modem là một thiết bị chuyển đổi tín hiệu số sang dạng tín hiệu phù hợp với môi trường truyền dẫn và ngược lại. Hình dưới là một kết nối sử dụng modem qua mạng điện thoại điển hình (hình 5.4).
Hình 5.4: Kết nối sử dụng modem qua mạng điện thoại điển hình
Các modem sử dụng các phương pháp nén dữ liệu nhằm mục đích tăng tốc độ truyền dữ liệu. Hiệu suất nén dữ liệu phụ thuộc vào dữ liệu, có hai giao thức nén thường được sử dụng là V.42bis và MNP 5. hiệu suất nén của V.42bis và MNP 5 có thể thay đổi từ 0 đến 400 % hay cao hơn phụ thuộc vào dữ liệu tự nhiên
Chuẩn modem V.90 cho phép các modem nhận dữ liệu với tốc độ 56 Kbps qua mạng điện thoại công cộng (PSTN). V.90 xem mạng PSTN như là một mạng số và chúng sẽ mã hóa dòng dữ liệu xuống theo kỹ thuật số thay vì điều chế để gửi đi như các chuẩn điều chế trước đây. Trong khi đó theo hướng ngược lại từ khách hàng đến nhà cung cấp dịch vụ dòng dữ liệu lên vẫn được điều chế theo các nguyên tắc thông thường và tốc độ tối ta đạt được là 33.6 Kbps, giao thức hướng lên này dựa trên chuẩn V.34
Sự khác nhau giữa tín hiệu số ban đầu với tín hiệu số được phục hồi tại đầu nhận gọi là tạp âm lượng tử hóa (nhiễu lượng tử), chính tạp âm này đã hạn chế tốc độ truyền dữ liệu. Giữa các modem đầu cuối có một cấu trúc hạ tầng cho việc kết nối đó là mạng thoại công cộng. Các chuẩn modem trước đây đều giả sử cả hai đầu của kết nối giống nhau là có một kết nối tương tự vào mạng điện thoại công cộng, công nghệ V.90 đã lợi dụng ưu điểm của tổ chức mạng mà một đầu kết nối giữa hệ thống truy cập từ xa và mạng thoại công cộng là dạng số hoàn toàn còn đầu kia vẫn được kết nối vào mạng PSTN theo dạng tương tự nhờ đó tận dụng được các ưu điểm của liên kết số tốc độ cao, vì chỉ có quá trình biến đổi A/D mới gây ra tạp âm với các kết nối số thì không có lượng tử hóa do đó nhiễu lượng tử rất ít trong cấu trúc mạng này.

Định luật shanon nói rằng đường dây điện thoại tương tự hạn chế tốc độ truyền dữ liệu ở khoảng 35 kbps mà không xem xét đến một thực tế là một đầu của truyền thông đã được số hóa nên giảm nhỏ lượng tạp âm gây ra sự chậm trễ trong việc truyền dữ liệu. Nhiễu lượng tử đã giới hạn chuẩn truyền thông V.34 ở tốc độ 33.6 kbps, nhưng nhiễu lượng tử chỉ có ảnh hưởng khi chuyển đổi tương tự - số mà không có ảnh hưởng khi chuyển đổi số-tương tự và đây chính là chìa khóa cho công nghệ V.90 đồng thời cũng giải thích được vì sao tốc độ download có thể đạt được 56 kbps còn khi upload tốc độ chỉ đạt 33.6 kbps. Dữ liệu chuyển đi từ modem số V.90 qua mạng PSTN là một dòng số với tốc độ 64 Kbps nhưng tại sao V.90 chỉ hỗ trợ tốc độ đến 56 Kbps, vì các lí do sau: Thứ nhất mặc dù nhiễu lượng tử đã được bỏ qua nhưng nhiễu mức thấp do bộ chuyển đổi số - tương tự là không tuyến tính, do ảnh hưởng của vòng loop nội hạt. Lý do thứ hai là các tổ chức quốc tế có qui định chặt chẽ về mức năng lượng tín hiệu nhằm hạn chế nhiễu xuyên âm giữa các dây dẫn đặt gần kề nhau, và qui định này tương ứng với mức năng lượng tối đa trên đường dây điện thoại tương ứng là 56 kbps

Để xây dựng một hệ thống truy cập từ xa qua mạng thoại công cộng đạt được tốc độ 56 kbps giữa hai đầu kết nối cần hội đủ ba điều kiện sau: thứ nhất, một đầu của kết nối (thường là đầu trung tâm mạng) phải là kết nối số tới mạng PSTN. Thứ hai, chuẩn modem V.90 hỗ trợ tại hai đầu cuối của nối kết. Thứ ba, chỉ có một chuyển đổi duy nhất số-tương tự trên mạng thoại giữa hai đầu của kết nối

Khi vận hành modem V.90 thăm dò đường thoại để quyết định xem nó sẽ làm việc theo tiêu chuẩn nào, nếu phát hiện ra bất kỳ một chuyển đổi số-tương tự nào thì nó đơn giản chỉ làm việc ở chuẩn V.34 và cũng cố gắng kết nối ở chuẩn này nếu modem đầu xa không hỗ trợ chuẩn V.90.

2.Các phương thức kết nối vật lý cơ bản:

Một phương thức phổ biến và sẽ được dùng nhiều đó là kết nối qua mạng điện thoại công cộng (PSTN). Máy tính được nối qua một modem lắp đặt bên trong (Internal modem) hoặc qua cổng truyền số liệu nối tiếp COM port. Tốc độ truyền tối đa hiện nay có thể có được bằng phương thức này có thể lên đến 56 Kbps cho chiều lấy dữ liệu xuống và 33,6Kbps cho chiều truyền dữ liệu hướng lên với các chuẩn điều chế tín hiệu phổ biến V90, K56Flex, X2. Ta cũng có thể sử dụng modem có yêu cầu về hạ tầng cơ sở thấp hơn với chuẩn điều chế V.24, V.32Bis, V.32...

Phương thức thứ hai là sử dụng mạng truyền số liệu số đa dịch vụ ISDN. Phương thức này đòi hỏi chi phí cao hơn và ngày càng được phổ biến rộng rãi. Ta có được khá nhiều các lợi ích từ việc sử dụng mạng ISDN mà một trong số đó là tốc độ. Ta có thể sử dụng các lựa chọn ISDN 2B+D BRI (2x64Kbps dữ liệu + 16Kbps dùng cho điều khiển) hoặc 23B+D PRI (23x64Kbps + 64Kbps) thông qua thiết bị TA (Terminal Adapter) hay các card ISDN.

Một phương thức khác nhưng ít được sử dụng là qua mạng truyền số liệu X.25, tốc độ không cao nhưng an toàn và bảo mật cao hơn. Yêu cầu cho

người sử dụng trong trường hợp này là phải có sử dụng card truyền số liệu X.25 hoặc một thiết bị được gọi là PAD (Packet Asssembled Disassembled). Ta cũng có thể sử dụng các kết nối trực tiếp qua cáp modem, phương thức này cho ta các kết nối tốc độ cao nhưng phải thông qua các modem truyền số liệu có giá thành cao.

2. An toàn trong truy cập từ xa

2.1. Các phương thức xác thực kết nối

1.Qúa trình nhận thực.

Tiến trình nhận thực với các giao thức xác thực được thực hiện khi người dùng từ xa có các yêu cầu xác thực tới máy chủ truy cập, một thỏa thuận giữa người dùng từ xa và máy chủ truy cập để xác định phương thức xác thực sẽ sử dụng. Nếu không có phương thức xác thực nào được sử dụng, tiến trình PPP sẽ khởi tạo kết nối giữa hai điểm ngay lập tức.

Phương thức xác thực có thể được sử dụng với các hình thức kiểm tra cơ sở dữ liệu địa phương (lưu trữ các thông tin về username và password ngay trên máy chủ truy cập) xem các thông tin về username và password được gửi đến có trùng với trong cơ sở dữ liệu hay không. Hoặc là gửi các yêu cầu xác thực tới một server khác để xác thực thường sử dụng là các RADIUS server (sẽ được trình bày ở phần sau)

Sau khi kiểm tra các thông tin gửi trả lại từ cơ sở dữ liệu địa phương hoặc từ RADIUS server. Nếu hợp lệ, tiến trình PPP sẽ khởi tạo một kết nối, nếu không yêu cầu kết nối của người dùng sẽ bị từ chối. (hình 5.5)

.

Hình 5.5: Xác thực kết nối

2.Giao thức xác thực PAP

PAP là một phương thức xác thực kết nối không an toàn, nếu sử dụng một chương trình phân tích gói tin trên đường kết nối ta có thể nhìn thấy các thông tin về username và password dưới dạng đọc được. Điều này có nghĩa là các thông tin gửi đi từ người dùng từ xa tới máy chủ truy cập không được mã hóa mà được gửi đi dưới dạng đọc được đó chính là lý do PAP không an toàn. Hình dưới mô tả quá trình xác thực PAP, sau khi thỏa thuận giao thức xác thực PAP trên liên kết PPP giữa các đầu cuối, người dùng từ xa gửi thông tin (username:nntrong, password:ras123) tới máy chủ truy cập từ xa, sau khi kiểm tra các thông tin này trong cơ sở dữ liệu của mình, máy chủ truy cập từ ra sẽ quyết định xem liệu yêu cầu kết nối có được thực hiện hay không (hình 5.6)

Hình 5.6: Giao thức xác thực PAP

3.Giao thức xác thực CHAP

Sau khi thỏa thuận giao thức xác thực CHAP trên liên kết PPP giữa các đầu cuối, máy chủ truy cập gửi một "challenge" tới người dùng từ xa. Người dùng từ xa phúc đáp lại một giá trị được tính toán sử dụng tiến trình xử lý một chiều (hash). máy chủ truy cập kiểm tra và so sánh thông tin phúc đáp với giá trị hash mà tự nó tính được. Nếu các giá trị này bằng nhau việc xác thực là thành công, ngược lại kết nối sẽ bị hủy bỏ. Như vậy CHAP cung cấp cơ chế an toàn thông qua việc sử dụng giá trị challenge thay đổi, duy nhất và không thể đoán được. Các thông tin về username và password không được gửi đi dưới dạng đọc được trên mạng và do đó chống lại các truy cập trái phép bằng hình thức lấy trộm password trên đường kết nối (hình 5.7).

Hình 5.7: Giao thức xác thực CHAP

4.Giao thức xác thực mở rộng EAP

Ngoài các giao thức kiểm tra tính xác thực cơ bản PAP, CHAP, trong Microsoft Windows 2000 hỗ trợ thêm một số giao thức cho ta các khả năng nâng cao độ an toàn, bảo mật và đa truy nhập đó là giao thức xác thực mở rộng

EAP (Extensible Authentication Protocol).
EAP cho phép có được một cơ cấu xác thực tuỳ ý để công nhận một kết nối gọi vào. Người sử dụng và máy chủ truy nhập từ xa sẽ trao đổi để tìm ra giao thức chính xác được sử dụng. EAP hỗ trợ các hình thức sau:
− Sử dụng các card vật lý dùng để cung cấp mật khẩu. Các card này dùng một số các phương thức xác thực khác nhau như sử dụng các đoạn mã thay đổi theo mỗi lượt sử dụng.
− Hỗ trợ MD5-CHAP, giao thức mã hoá tên người sử dụng, mật khẩu sử dụng thuật toán mã hoá MD5 (Message Digest 5).
− Hỗ trợ sử dụng cho các thẻ thông minh. Thẻ thông minh bao gồm thẻ và thiết bị đọc thẻ. Các thông tin xác thực về cá nhân người dùng được ghi lại trong các thẻ này.
− Các nhà phát triển phần mềm độc lập sử dụng giao diện chương trình ứng dụng EAP có thể phát triển các module chương trình cho các công nghệ áp dụng cho thẻ nhận dạng, thẻ thông minh, các phần cứng sinh học như nhận dạng võng mạc, các hệ thống sử dụng mật khẩu một lần.

2.2. Các phương thức mã hóa dữ liệu

Dịch vụ truy cập từ xa cung cấp cơ chế an toàn bằng việc mã hóa và giải mã dữ liệu truyền giữa người dùng truy cập từ xa và máy chủ truy cập.

Có hai phương thức mã hóa dữ liệu thường được sử dụng đó là mã hóa đối xứng và mã hóa phi đối xứng.

Phương thức mã hoá đối xứng, thông tin ở dạng đọc được, được mã hoá sử dụng khóa bí mật (khoá mà chỉ có người mã hoá mới biết được) tạo thành thông tin đã được mã hoá. ở phía nhận, thông tin mã hoá được giải mã cùng với khóa bí mật thành dạng gốc ban đầu. Điểm chú ý của phương pháp mã hoá này là việc sử dụng khoá bí mật cho cả quá trình mã hoá và quá trình giải mã. Do đó, nhược điểm chính của phương thức này là cần có quá trình trao đổi khoá bí mật, dẫn đến tình trạng dễ bị lộ khoá bí mật.

Phương pháp mã hoá phi đối xứng, để khắc phục điểm hạn chế của phương pháp mã hoá đối xứng là quá trình trao đổi khoá bí mật, người ta đã sử dụng phương pháp mã hoá phi đối xứng sử dụng một cặp khoá tương ứng với nhau gọi là phương thức mã hoá phi đối xứng dùng khoá công khai. Phương thức mã hóa này sử dụng hai khóa là khóa công khai và khóa bí mật có các quan hệ toán học với nhau. Trong đó khóa bí mật được giữ bí mật và không có khả năng bị lộ do không cần phải trao đổi trên mạng. Khóa công khai không phải giữ bí mật và mọi người đều có thể nhận được khoá này. Do phương thức mã hóa này sử dụng 2 khóa khác nhau, nên người ta gọi nó là phương thức mã hóa phi đối xứng. Mặc dù khóa bí mật được giữ bí mật, nhưng không giống với "secret Key" được sử dụng trong phương thức mã hóa đối xứng sử dụng khoá bí mật do khóa bí mật không được trao đổi trên mạng. Khóa công khai và khóa bí mật tương ứng của nó có quan hệ toán học với nhau và được sinh ra sau khi thực hiện các hàm toàn học; nhưng các hàm toán học này luôn thoả mãn điều kiện là sao cho không thể tìm được khóa bí mật từ khóa công cộng và ngược lại. Do có mối quan hệ toán học với nhau, thông tin được mã hóa bằng khóa công khai chỉ có thể giải mã được bằng khóa bí mật tương ứng.

Giao thức thường được sử dụng để mã hóa dữ liệu hiện nay là giao thức IPsec. Hầu hết các máy chủ truy cập dựa trên phần cứng hay mềm hiện nay đều hỗ _____trợ IPSec. IPSec là một giao thức bao gồm các chuẩn mở bảo đảm các vấn đề bảo mật, an toàn và toàn vẹn dữ liệu cho các kết nối qua mạng sử dụng giao thức IP bằng các biện pháp mã hoá. IPSec bảo vệ chống lại các hành động phá

hoại từ bên ngoài. Các client khởi tạo một mối liên quan bảo mật hoạt động tương tự như khoá công khai để mã hoá dữ liệu.
Ta có thể sử dụng các chính sách áp dụng cho IPSec để cấu hình nó. Các chính sách cung cấp nhiều mức độ và khả năng để bảo đảm an toàn cho từng loại dữ liệu. Các chính sách cho IPSec sẽ được thiết lập cho phù hợp với từng người dùng, từng nhóm người dùng, cho một ứng dụng, một nhóm miền hay toàn bộ hệ thống mạng.

3. Triển khai dịch vụ truy cập từ xa

3.1. Kết nối gọi vào và kết nối gọi ra

Cấu hình máy chủ truy cập để tạo lập các kết nối gọi vào cho phép người dùng từ xa truy cập vào mạng. Các thông số cơ bản thường được cấu

hình khi tạo lập các kết nối gọi vào bao gồm xác định các phương thức xác thực người dùng, mã hóa hay không mã hóa dữ liệu, các phương thức mã hóa dữ liệu nếu yêu cầu, các giao thức mạng sẽ được sử dụng cho truy nhập từ xa, các thiết đặt về chính sách và các quyền truy nhập của người dùng từ xa, mức độ được phép truy nhập như thế nào, xác định phương thức cấp phát địa chỉ IP cho máy truy nhập từ xa, các yêu cầu cấu hình để tạo lập các kết nối VPN…
Kết nối gọi ra có thể được thiết lập để gọi ra tới một mạng dùng riêng hoặc tới một ISP. Trong windows 2000 hỗ trợ các hình thức kết nối sau:
Nối tới mạng dùng riêng, ta sẽ phải cung cấp số điện thoại nơi sẽ nối đến. Có thể là số điện thoại của ISP, của mạng dùng riêng hay của máy tính phía xa. Xác định quyền sử dụng kết nối này. .
Nối tới Internet, hai lựa chọn có thể là sử dụng truy cập qua đường thoại và sử dụng truy cập qua mạng LAN. Sử dụng đường thoại, các vấn đề ta cần quan tâm là số điện thoại truy nhập, tên và mật khẩu được cung cấp bởi ISP. Sử dụng LAN, ta sẽ phải quan tâm đến proxy server và một số thiết đặt khác.
Tạo lập kết nối VPN, *VPN là một mạng sử dụng các kết nối dùng giao thức tạo đường hầm (PPTP, L2TP, IPSEC,...) để tạo được các kết nối an toàn, bảo đảm thông tin không bị xâm phạm khi truyền tải qua các mạng công cộng. Tương tự như khi tạo lập một kết nối gọi ra, Nếu cần thiết phải thông qua một ISP trung gian trước khi nối tới mạng dùng riêng, lựa chọn một kết nối gọi ra. Cung cấp địa chỉ máy chủ, địa chỉ mạng nơi mà ta đang muốn nối tới. Các thiết lập khác là thiết đặt các quyền sử dụng kết nối.*
Tạo lập kết nối trực tiếp với máy tính khác, lựa chọn này được sử dụng để kết nối trực tiếp hai máy tính với nhau thông qua một cáp được thiết kế cho nối trực tiếp hai máy tính. Một trong hai máy tính được lựa chọn là chủ và máy tính kia được lựa chọn là tớ. Lựa chọn thiết bị cổng nơi hai máy tính nối với nhau.

3.2. Kết nối sử dụng đa luồng (Multilink)

Multilink là sự kết hợp nhiều liên kết vật lý trong một liên kết logic duy nhất nhằm gia tăng băng thông cho kết nối. Multilink cho phép sử dụng hai hoặc nhiều hơn các cổng truyền thông như là một cổng duy nhất có tốc độ cao. Điều này có nghĩa là ta có thể sử dụng hai modem để kết nối Internet với tốc độ cao gấp đôi so với việc sử dụng một modem. Multilink gia tăng băng thông và giảm độ trễ giữa các hệ thống bằng cơ chế chia các gói dữ liệu và gửi đi trên các mạch song song. Multilink sử dụng giao thức MPPP cho việc quản lý các kết nối của mình. Để sử dụng, MPPP cần phải được hỗ trợ ở cả hai phía của kết nối (hình 5.8).

Hình 5.8: Kết nối sử dụng đa luồng
Hình vẽ mô tả kết nối sử dụng Multilink, khi người dùng từ xa sử dụng hai modem và hai đường thoại kết nối với máy chủ truy cập, mỗi kết nối là việc theo chuẩn V.90 có tốc độ 56 kbps sử dụng kỹ thuật Multilink cho phép đạt tốc độ 112 Kbps giữa máy truy cập từ xa và máy chủ truy cập.

3.3. Các chính sách thiết lập cho dịch vụ truy nhập từ xa

Chính sách truy nhập từ xa là tập hợp các điều kiện và các thiết đặt cho phép người quản trị mạng gán cho mỗi người dùng từ xa các quyền truy cập và mức độ sử dụng các nguồn tài nguyên trên mạng. Ta có thể dùng các chính sách để có được nhiều các lựa chọn phù hợp với từng mức độ người dùng, tăng tính mềm dẻo, tính năng động khi cấp quyền truy nhập cho người dùng.
Một chính sách truy nhập từ xa thông thường bao gồm ba thành phần nhằm cung cấp các truy nhập an toàn có kiểm soát đến máy chủ truy cập.
Các điều kiện (Conditions): là một danh sách các tham số như ngày tháng, nhóm người dùng, mã người gọi, địa chỉ IP phù hợp với máy trạm đang nối đến máy chủ truy cập. Bộ chính sách điều kiện đầu tiên này tương ứng với các thông số của yêu cầu kết nối gọi đến được xử lý đối với sự cho phép truy cập và cấu hình.
Sự cho phép (Permission): Các kết nối truy nhập từ xa được cho phép và gán trực tiếp tới mỗi người dùng bởi các thiết đặt trong các chính sách truy nhập từ xa. Ví dụ một chính sách có thể gán tất cả người dùng trong một nhóm nào đấy quyền truy cập chỉ trong giờ làm việc hành chính từ 8:00 A.M đến 5:00 P.M, hay đồng thời gán cho một nhóm người dùng khác quyền truy cập liên tục 24/24.
Profile: Mỗi chính sách đều bao gồm một thiết đặt của profile áp dụng cho kết nối như là các thủ tục xác thực hay mã hóa. Các thiết đặt trong profile được thi hành ngay tới các kết nối. Ví dụ: nếu một profile thiết đặt cho một kết nối mà người dùng chỉ được phép sử dụng trong 30 phút mỗi lần thì người dùng sẽ bị ngắt kết nối tới máy chủ truy cập trong sau 30 phút.
Quá trình thực thi các chính sách truy cập từ xa được mô tả bằng hình dưới (hình 5.9)

Dial-in
permission
No connection
Use Remote
Access Policy
Contidion/
permition
Profile
Make
Connection
Connection
Conditions
No
Yes
Yes
Deny Allow
No
Deny Allow
Hình 5.9: Quá trình thực thi các chính sách truy cập từ xa
Các điều kiện được gửi tới để tạo một kết nối, nếu các điều kiện gửi tới này không thích hợp truy cập bị từ chối, nếu thích hợp các điều kiện này được sử dụng để xác định sự truy cập. Tiếp theo máy chủ truy cập kiểm tra các cho phép quay số vào người dùng sẽ bị từ chối nếu thiết đặt này là Deny và được phép truy cập nếu là Allow, nếu thiết đặt là sử dụng các chính sách truy cập để xác định quyền truy cập thì sự cho phép của các chính sách sẽ quyết định

quyền truy cập của người dùng. Nếu các chính sách này từ chối truy cập người dùng sẽ bị ngắt kết nối, nếu là cho phép sẽ chuyển tới để kiểm tra các chính sách trong profile là bước cuối cùng để xác định quyền truy cập của người dùng.

3.4. Sử dụng dịch vụ gán địa chỉ động DHCP cho truy cập từ xa

Khi thiết lập một máy chủ truy cập để cho phép người dùng từ xa truy cập vào mạng, ta có thể lựa chọn phương thức mà các máy từ xa có thể nhận được địa chỉ IP.

Với phương thức cấu hình địa chỉ IP tĩnh ngay trên các máy trạm, người dùng phải cấu hình bằng tay địa chỉ IP trên mỗi máy truy cập. Sử dụng phương thức này phải đảm bảo rằng các thông tin cấu hình địa chỉ IP là hợp lệ và chưa được sử dụng trên mạng. Đồng thời các thông tin về default gateway, DNS…cũng phải được cấu hình bằng tay một cách chính xác.Vì lí do này

khuyến nghị không nên sử dụng phương pháp này cho việc gán IP cho các máy truy cập từ xa.

Máy chủ truy cập có thể gán động một địa chỉ IP cho các máy truy cập từ xa. Địa chỉ IP này thuộc trong khoảng địa chỉ mà ta đã cấu hình trên máy chủ truy cập. Sử dụng phương pháp này ta cần phải đảm bảo rằng khoảng địa chỉ IP này được dành riêng để cấp phát cho các máy truy cập từ xa.

Phương thức sử dụng DHCP server, máy chủ truy cập nhận địa chỉ IP từ DHCP server và gán cho các máy truy cập từ xa. Phương thức này rất linh hoạt, không cần phải dành riêng một khoảng địa chỉ IP dự trữ cho máy truy cập từ xa và thường được sử dụng trong một mạng có tổ chức và đa dạng trong các hình thức kết nối. Địa chỉ IP được cấp phát cho các máy truy cập từ xa một cách tự động, các thông tin cấu hình khác (Gateway, DNS server…) cũng được cung cấp tập trung, chính xác tới từng máy truy cập đồng thời các máy truy cập cũng không cần thiết phải cấu hình lại khi có các thay đổi về cấu trúc mạng.

Hoạt động của DHCP được mô tả như sau: Mỗi khi DHCP client khởi động, nó yêu cầu một địa chỉ IP từ DHCP server. Khi DHCP server nhận yêu cầu, nó chọn một địa chỉ IP trong khoảng IP đã được định nghĩa trong cơ sở dữ liệu của nó. DHCP server cấp phát địa chỉ IP tới DHCP client Nếu DHCP client chấp nhận địa chỉ IP này, DHCP server cho thuê địa chỉ IP này trong một khoảng thời gian cụ thể (tùy theo thiết đặt). Các thông tin về địa chỉ IP được gửi từ DHCP server tới DHCP client thường bao gồm các thành phần sau: địa chỉ IP, subnet mask, các giá trị lựa chọn khác (default gateway, địa chỉ DNS server).

3.5. Sử dụng RadiusServer để xác thực kết nối cho truy cập từ xa.

1. Hoạt động của Radius server

RADIUS là một giao thức làm việc theo mô hình client/server. RADIUS cung cấp dịch vụ xác thực và tính cước cho mạng truy nhập gián tiếp. Radius client là một máy chủ truy cập tiếp nhận các yêu cầu xác thực từ người dùng từ xa và chuyển các yêu cầu này tới Radius server. Radius server nhận các yêu cầu kết nối của người dùng xác thực và sau đó trả về các thông tin cấu hình cần thiết cho Radius client để chuyển dịch vụ tới người sử dụng (hình 5.10).

Hình 5.10: Hoạt động của Radius server

Quá trình hoạt động được mô tả như sau:

1. Người sử dụng từ xa khởi tạo quá trình xác thực PPP tới máy chủ truy cập

2. Máy chủ truy cập yêu cầu người dùng cung cấp thông tin về username và password bằng các giao thức PAP hoặc CHAP.
3. Người dùng từ xa phúc đáp và gửi thông tin username và password tới máy chủ truy cập.
4. Máy chủ truy cập (Radius client) gửi chuyển tiếp các thông tin username và password đã được mã hóa tới Radius server
5. Radius server trả lời với các thông tin chấp nhận hay từ chối. Radius client thực hiện theo các dịch vụ và các thông số dịch vụ đi cùng với các phúc đáp chấp nhận hay từ chối từ Radius server

2. Nhận thực và cấp quyền

Khi Radius server nhận yêu cầu truy cập từ Radius client, Radius server tìm kiếm trong cơ sở dữ liệu các thông tin về yêu cầu này. Nếu username không có trong cơ sở dữ liệu này thì hoặc một profile mặc định được chuyển hoặc một thông báo từ chối truy cập được chuyển tới Radius client.

Trong RADIUS nhận thực và cấp quyền đi đôi với nhau, nếu username có trong cơ sở dữ liệu và password được xác nhận là đúng thì Radius server gửi trả về thông báo truy cập được chấp nhận, thông báo này bao gồm một danh sách các cặp đặc tính- giá trị mô tả các thông số được sử dụng cho phiên làm việc. Các thông số điển hình bao gồm: kiểu dịch vụ, kiểu giao thức, địa chỉ gán cho người dùng (động hoặc tĩnh), danh sách truy cập được áp dụng hay một định tuyến tĩnh được cài đặt trong bảng định tuyến của máy chủ truy cập.

Thông tin cấu hình trong Radius server sẽ xác định những gì sẽ được cài đặt trên máy chủ truy cập. Hình vẽ dưới đây mô tả quá trình nhận thực và cấp quyền của Radius server (hình 5.11)

Hình 5.11: Nhận thực và cấp quyền

3.Tính cước

Các vấn đề về xử lý cước của RADIUS hoạt động độc lập với nhận thực và cấp quyền. Chức năng tính cước cho phép ghi lại dữ liệu được gửi tại thời điểm bắt đầu và kết thúc của một phiên làm việc và đưa ra các con số về mặt sử dụng tài nguyên như (thời gian, số gói, số byte...) được sử dụng trong phiên làm việc đó.

3.6. Mạng riêng ảo và kết nối dùng dịch vụ truy cập từ xa

VPN (Virtual Private Network) là một mạng riêng được xây dựng trên nền tảng hạ tầng mạng công cộng (ví dụ mạng Internet), sử dụng mạng công cộng cho việc truyền thông riêng tư.

Giải pháp VPN cho phép người dùng làm việc tại nhà hoặc đang đi công tác ở xa có thể thực hiện một kết nối tới trụ sở chính bằng việc sử dụng hạ tầng mạng là một mạng công cộng như là Internet, Như vậy thay vì phải thực hiện một kết nối đường dài tới trụ sở chính người sử dụng chỉ cần tạo lập một kết nối nội hạt tới một ISP khi đó bằng công nghệ VPN một kết nối VPN sẽ được thiết lập giữa người dùng với mạng trung tâm. Kết nối VPN cũng cho phép các tổ chức kết nối liên mạng giữa các địa điểm ở xa khác nhau thông qua các kết nối trực tiếp (leased line) từ các địa điểm đó tới một ISP. Như vậy kết nối VPN cho phép một tổ chức giảm chi phí gọi đường dài qua Dialup hay chi phí thuê đường leadline cho khoảng cách xa thay vì như vậy chỉ cần các kết nối nội hạt và điều này là tiết kiệm được chi phí. VPN gửi dữ liệu giữa các đầu cuối, dữ liệu được đóng gói, với các Header cung cấp thông tin định tuyến cho phép chuyển dữ liệu qua một liên kết hoặc một liên mạng công cộng tới đích. Dữ liệu chuyển đi được mã hoá để đảm bảo an toàn, các gói dữ liệu truyền thông trên mạng là không thể đọc mà không có khoá giải mã. Liên kết mà trong đó dữ

liệu được đóng gói và mã hoá là một kết nối VPN.
Các hình thức kết nối: Có hai kiểu kết nối VPN, kết nối VPN truy cập từ xa và kết nối Site-to-site. Một kết nối VPN truy cập từ xa được thiết lập bởi một máy tính PC tới một mạng dùng riêng. VPN gateway cung cấp truy cập tới các tài nguyên của mạng dùng riêng. Các gói dữ liệu gửi qua kết nối VPN được khởi tạo từ các client. VPN client thực hiện việc xác thực tới VPN gateway. Kết nối site-to-site, được thiết lập bởi các VPN gateway và kết nối hai phần của một mạng dùng riêng. (hình 5.12).
Hình 5.12: Kết nối site-to-site
Tunnel: là một phần quan trọng trong việc xây dựng một mạng VPN.
Các chuẩn truyền thông sử dụng để quản lý các tulnnel và đóng gói dữ liệu của VPN bao gồm các giao thức làm việc ở lớp 2 như PPTP (Point-to-Point Tunlling Protocol) được phát triển bởi Microsoft hỗ trợ trong môi trường mạng

Windows, L2TP (Layer 2 Tunnelling Protocol) được phát triển bởi Cisco. IPsec là một giao thức làm việc ở lớp 3, IPsec được phát triển bởi IETF và ngày càng được sử dụng rộng rãi.
L2TP và PPTP có mục đích là cung cấp các đường hầm dữ liệu thông qua mạng truyền dữ liệu công cộng. L2TP khác với PPTP ở chỗ nó tạo lập đường hầm nhưng không mã hoá dữ liệu. L2TP cung cấp các đường hầm bảo mật khi cùng hoạt động với các công nghệ mã hoá khác như IPSec. IPSec không yêu cầu phải có L2TP nhưng các chức năng mã hoá của nó đưa đến cho L2TP khả năng cung cấp các kênh thông tin bảo mật, cung cấp các giải pháp VPN. L2TP và PPTP cùng sử dụng PPP để đóng gói, thêm bớt thông tin tiếp đầu và truyền tải dữ liệu qua mạng.
Các kết nối VPN có các đặc trưng sau: đóng gói (Encapsulation), xác thực (Authentication) và mã hoá dữ liệu (Data encryption)
Đóng gói dữ liệu: Công nghệ VPN sử dụng một phương thức đóng gói dữ liệu trong đó cho phép dữ liệu truyền được qua mạng công cộng qua các giao thức tạo đường hầm.
Xác thực: Khi một kết nối VPN được thiết lập,VPN gateway sẽ xác thực VPN client đang yêu cầu kết nối và nếu được được phép kết nối được thực hiện. Nếu sự xác thực kết nối là qua lại được sử dụng, thì VPN client sẽ thực hiện việc xác thực lại VPN gateway, để đảm bảo rằng đấy chính là server mà mình cần gọi. Xác thực dữ liệu và tính toàn vẹn của dữ liệu: để xác nhận rằng dữ liệu đang được gửi từ một đầu của kết nối khác mà không bị thay đổi trong quá trình truyền, dữ liệu phải bao gồm một trường kiểm tra bằng mật mã dự trên một khoá mã hoá đã biết chỉ giữa người gửi và người nhận
Mã hóa dữ liệu: để đảm bảo dữ liệu truyền trên mạng, dữ liệu phải được mã hoá tại đầu gửi và giải mã tại đầu nhận. Việc mã hoá và giải mã dữ liệu phụ thuộc và người gửi và người nhận đang sử dụng phương thức mã hoá và giải mã nào.

3.7. Sử dụng Network and Dial-up Connection

Network and Dial-up Connection **(**NDC) là một công cụ được Microsoft phát triển để hỗ trợ việc tạo lập các kết nối trong đó bao gồm các kết nối cho truy cập từ xa. Với việc sử dụng NDC ta có thể truy cập tới các tài nguyên dù đang ở trong mạng hay ở một địa điểm ở xa. Các kết nối được khởi tạo, thiết lập cấu hình, lưu giữ và quản lý bởi NDC. Mỗi một kết nối bao gồm một bộ các đặc tính được sử dụng để thiết lập liên kết giữa một máy tính tới máy tính hoặc mạng khác. Các kết nối gọi ra được liên lạc với một máy chủ truy cập ở xa bằng các hình thức truy cập gián tiếp thương là qua các mạng truyền dẫn mạng

thoại công cộng, mạng ISDN. NDC cũng hỗ trợ việc thiết lập các kết nối gọi vào có nghĩa là đóng vai trò như một máy chủ truy cập.
Bởi vì tất cả các dịch vụ và các phương thức truyền thông đều được thiết lập trong kết nối nên không cần phải sử dụng các công cụ khác để cấu hình cho kết nối. Ví dụ để thiết lập cho một kết nối dial-up bao gồm các đặc tính được

sử dụng trước, trong và sau khi kết nối. Các thông số này bao gồm: modem sẽ quay số, kiểu mã hóa password được sử dụng và các giao thức mạng sẽ sử dụng sau kết nối. Trạng thái kết nối bao gồm thời gian và tốc độ cũng được chính kết nối hiển thị mà không cần bất cứ một công cụ nào khác.

3.8. Một số vấn đề xử lý sự cố trong truy cập từ xa

Các vấn đề liên quan đến sự cố trong truy cập từ xa, thường bao gồm:
Giám sát truy cập từ xa: giám sát máy chủ truy cập là phương pháp tốt nhất thường sử dụng để tìm ra nguồn gốc của các vấn đề xảy ra sự cố. Mỗi một chương trình phần mềm hay thiết bị phần cứng máy chủ truy cập bao giờ cũng có các công cụ sử dụng để giám sát và ghi lại các sự kiện xảy ra (trong các file log) đối với mỗi phiên truy cập từ xa.
Theo dõi các kết nối truy cập từ xa: khả năng theo dõi các kết nối truy cập từ xa của một Máy chủ truy cập cho ta xử lý các vấn đề phức tạp về sự cố mạng. Các thông tin theo dõi một kết nối từ xa thường rất phức tạp và khá chi tiết do đó để phân tích và xử lý cần thiết người quản trị mạng phải có kinh nghiệm và trình độ về hệ thống mạng.
Xử lý các sự cố về phần cứng: bao gồm các thiết bị truyền thông tại người dùng và tại máy chủ truy cập. Đối với các thiết bị tại người dùng (thường là các modem, cạc mạng...), hãy xem tài liệu về sản phẩm đó hay hỏi nhà cung cấp thiết bị về sản phẩm của họ về các cách kiểm tra và xác định lỗi của sản phẩm này. Nếu kết nối sử dụng modem, hãy kiểm tra rằng modem đã được cài đặt đúng chưa. Trong Windows 2000 các bước kiểm tra như sau:
o Trong Control Panel, kích Phone and Modem Options
o Trong trang modem, kích tên modem, sau đó kích Properties
o Kích Diagnostics, sau đó kích Query Modem.
Nếu modem đã được cài đặt đúng, bộ các thông số về modem sẽ được hiển thị, ngược lại hãy kiểm tra và cài đặt lại modem, trong trường hợp cuối cùng hãy hỏi nhà sản xuất thiết bị này. Để nhận thêm các thông tin về modem trong khi đang cố gắng tạo lập một kết nối, hãy xem thông tin trong log file để tìm ra nguyên nhân gặp sự cố. Để ghi các thông tin vào log file thực hiện theo các bước sau:
o Trong Control Panel, kích Phone and Modem Options
o Trong trang modem, kích tên modem, sau đó kích Properties
o Kích Diagnostics, sau đó kích lựa chọn Record a log, sau đó kích OK.
Đối với thiết bị truyền thông tại máy chủ truy cập: Kiểm tra các thiết bị phần cứng tương tự như trong trường hợp thiết bị tại người dùng, đồng thời kiểm tra log file về các sự kiện xảy ra với hệ thống để tìm ra nguyên nhân sự cố. Một cách khác để kiểm tra modem tại máy chủ truy cập là sử dụng một đường điện thoại và gọi tới modem đó sau đó nghe xem modem đó có trả lời và cố gắng tạo một kết nối hay không. Nếu không có tín hiệu tạo kết nối từ

modem đó thì có thể kết luận rằng đang có một vấn đề lỗi về modem tại máy chủ truy cập

Xử lý các sự cố về đường truyền thông: Thường là do cáp được đấu sai hay vì nguyên nhân từ nhà cung cấp dịch vụ điện thoại. Hãy kiểm tra đường điện thoại từ người dùng tới máy chủ truy cập bằng cách gọi điện thoại thông thường, thông qua chất lượng cuộc gọi ta cũng có thể phần nào dự đoán được chất lượng của đường truyền.
Xử lý các thiết đặt về cấu hình: Sau khi xác định rằng các vấn đề về phần cứng cũng như đường truyền thông đều tốt, bước tiếp theo ta kiểm tra các thiết đặt về cấu hình, bao gồm:
Các thiết đặt về mạng: lỗi cấu hình về mạng xảy ra khi đã tạo kết nối thành công nhưng vẫn không thể truy cập được các nguồn tài nguyên trên mạng, các lỗi thường xảy ra như việc phân giải tên chưa hoạt động, các lỗi về định tuyến...khi lỗi về cấu hình mạng xảy ra, trước tiên ta kiểm tra rằng các máy kết nối trực tiếp (không thông qua dịch vụ truy cập từ xa) có thể truy cập được vào các nguồn tài nguyên trên mạng. Sau đó kiểm tra các cấu hình về TCP/IP bằng việc sử dụng lệnh ipconfig /all trên máy client. Kiểm tra rằng các thông số như DNS, địa chỉ IP, các thông số về định tuyến đã được thiết đặt đúng chưa. Sử dụng lệnh ping để kiểm tra kết nối mạng đã làm việc.
Các thiết đặt Máy chủ truy cập: Các thiết đặt trên máy chủ truy cập với các thông số sai khi tạo lập kết nối có thể là nguyên nhân người dùng không thể truy cập vào các nguồn tài nguyên trên mạng. Để hỗ trợ cho việc xác định nguyên nhân gây lỗi, kiểm tra các sự kiện đã ghi log trên máy chủ truy cập và client, trong một số trường hợp cần thiết phải theo dõi (tracing) các kết nối trên máy chủ truy cập.
Các thiết đặt trên máy người dùng từ xa: kiểm tra các giao thức mạng làm việc trên client, các giao thức mạng làm việc trên client phải được hỗ trợ bởi máy chủ truy cập. Ví dụ, nếu người dùng từ xa thiết đặt trên client các giao thức NWLink, IPX/SPX và máy chủ truy cập chỉ hỗ trợ sử dụng TCP/IP, thì kết nối sẽ không thành công.

4. Bài tập thực hành

Yêu cầu về Phòng học lý thuyết: Số lượng máy tính theo số lượng học viên trong lớp học đảm bảo mỗi học viên có một máy tính, cấu hình máy tối thiểu như sau (PIII 800 MHZ, 256 MB RAM, HDD 1GB,FDD, CDROM 52 x). Máy tính đã cài đặt Windows 2000 advance server. Các máy tính đã được nối mạng chạy giao thức TCP/IP.
Thiết bị thực hành: Đĩa cài phần mềm Windows 2000 Advance Server. Mỗi máy tính có 01 Modem V.90 và 01 đường điện thoại. 01 account truy cập internet

Bài 1: Thiết lập dialup networking để tạo ra kết nối Internet. truy cập Internet và giới thiệu các dịch vụ cơ bản

 Đăng nhập vào hệ thống với quyền Administrator.

 Kích Start, trỏ settings, sau đó kích Network and Dial-up Connections
 Trong Network and Dial-up Connections, kích đúp vào Make New Connection.
 Trong Network Connection Wizard, kích Next, có hai lựa chọn có thể sử dụng là Dial-up to private network hoặc Dial-up to the Internet.
 Nếu chọn Dial-up to private network, đưa vào số điện thoại truy cập của nhà cung cấp.
 Nếu chọn Dial-up to the Internet, lúc đó Internet Connection Wizard sẽ bắt đầu, làm theo các bước chỉ dẫn.
 Nếu muốn tất cả người dùng đều có thể sử dụng kết nối này thì lựa chọn,

For all users, sau đó kích Next. Nếu muốn chỉ người dùng hiện tại sử dụng thì lựa chọn Only for myself, sau đó kích Next.
 Nếu đã lựa chọn Only for myself thì chuyển đến bước cuối cùng, Nếu lựa chọn For all users và muốn các máy tính khác trên mạng có thể chia sẻ kết nối này hãy lựa chọn Enable Internet Connection Sharing for this connection.
 Thiết đặt ngầm định là bất kỳ mày tính nào cũng có thể khởi tạo kết nối này một cách tự động, nếu muốn bỏ ngầm định này hãy xóa lựa chọn Enable on-demand dialing, sau đó kích next
 Đưa vào tên của kết nối và kích Finish.

Bài 2: Cài đặt và cấu hình dịch vụ truy cập từ xa cho phép người dùng từ xa truy cập vào mạng trên hệ điều hành Windows 2000 server.

Bước 1:

Cài đặt máy chủ dịch vụ truy cập từ xa
 Đăng nhập vào hệ thống với quyền Administrator
 Mở Routing and Remote Access từ menu Administrator Tools
 Kích chuột phải vào tên Server sau đó chọn Configure and Enable Routing and remote Access.
 Kịch bản Routing and Remote Access Server Setup xuất hiện, kích next
 Trong trang common Configuration, chọn Remote access server, sau đó kích next
 Trong trang Remote Client Protocol, xác định các giao thức sẽ hỗ trợ cho truy cập từ xa, sau đó kích next
 Trong trang Network Selection, lựa chọn kết nối mạng sẽ gán cho các máy truy cập từ xa, sau đó kích next
 Trong trang IP Address Asignment, lựa chọn Automaticlly hoặc From specified range of addresses cho việc gán các địa chỉ IP tới các máy truy cập từ xa

 Trong trang Managing Multiple Remote Acccess Servers cho phép lựa chọn cấu hình RADIUS, kích next
 Kích Finish để kết thúc.

Bước 2:

Thiết đặt tài khoản cho người dùng từ xa. Thiết lập một tài khoản có tên RemoteUser
 Đăng nhập với quyền Administrator
 Mở Active Directory Users and Computers từ menu Administrator Tools
 Kích chuột phải vào Users, chọn new và kích vào User
 Trong hộp thoại New Object-User, điền RemoteUser vào First name
 Trong hộp User logon name, gõ RemoteUser
 Thiết đặt Password cho tài khoản này, kích next sau đó kích Finish.
 Kích chuột phải vào RemoteUser sau đó kích Properties
 Trong trang Dial-In tab, kích Allow access, sau đó click OK

Thiết lập một Global group tên là RemoteGroup, sau đó thêm tài khoản người dùng vừa thiết lập vào nhóm này
 Kích chuột phải vào Users, chọn new sau đó kích Group
 Trong hộp thoại New Object-Group, mục Group name gõ vào RemoteGroup
 Trong mục Group scope kiểm tra Global đã được lựa chọn, trong mục Group type kiểm tra rằng Security đã được lựa chọn, sau đó kích OK
 Mở hộp thoại Properties của RemoteGroup

 Trong trang Member, kích Add
 Trong hộp thoại Select Users, Contacts, Computers, hoặc Group, Look in box, kiểm tra domain đã được hiển thị
 Trong danh sách các đối tượng, kích RemoteUser, kích Add sau đó kích OK
 Kích OK để đóng hộp thoại RemoteGroup Properties

Bước 3:

Kiểm tra cấu hình đã thiết lập ở bước trên bằng việc thực hiện một kết nối quay số tới máy chủ truy cập từ xa với tài khoản có tên là RemoteUser, kết nối được thiết lập sau đó đóng kết nối lại.

Bước 4:

Cấu hình cho phép tài khoản RemoteUser truy cập vào mạng được điều khiển truy cập bởi các chính sách truy cập từ xa (Remote access policy)

 Mở lại Active Directory Users and Computers từ menu Administrator Tools

 Mở hộp thoại Properties của tài khoản RemoteUser
 Trong trang Dial-in tab, kích Control access though Remote Policy sau đó kích OK, lư u ý rằng điều khiển vùng (Domain Controler) phải chạy ở chế độ Native.
 Thu nhỏ cửa sổ Active Directory Users and Computers

Bước 5:

Kiểm tra cấu hình đã thiết lập ở bước trên bằng việc thực hiện một kết nối quay số tới máy chủ truy cập từ xa với tài khoản có tên là RemoteUser. Thông báo lỗi xuất hiện, kết nối không được thiết lập.

Bước 6:

Sử dụng RRAS để thiết lập một chính sách mới đối với người dùng từ xa, tên chính sách này là Allow RemoteGroup Access cho phép người dùng trong nhóm RemoteGroup truy cập.

 Mở Routing and Remote Access từ menu Administrator Tools
 Mở rộng tên máy chủ đang cấu hình, kích chuột phải vào Remote Access Policy sau đó chọn New Remote Access Policy
 Trong trang Policy Name, gõ vào Allow RemoteGroup Access sau đó kích Next
 Trong trang Condition, kích Add trong hộp thoại Select Attribute kích Windows-Groups sau đó kích Add
 Trong hộp thoại Groups kích Add
 Trong hộp thoại Select Groups, trong danh sách Look in, kích vào tên domain
 Trong hộp thoại Select Groups,dưới Name kích RemoteGroups kích Add sau đó kích OK
 Trong hộp thoại Groups kích OK
 Trong trang Condition kích Next
 Trong trang Permissions kích Grant remote access permission sau đó kích Next
 Trong trang User Profile kích Finish
 Trong trang Routing and Remote Access kích Remote Access Policies sau đó kích chuột phải Allow RemoteGroup access sau đó kích Move Up

Bước 7:

Kiểm tra cấu hình đã thiết lập ở bước trên bằng việc thực hiện một kết nối quay số tới máy chủ truy cập từ xa với tài khoản có tên là RemoteUser, kết nối được

thiết lập sau đó đóng kết nối lại.

Bước 8:

Cấu hình để default policy được thi hành trước:

 Mở trang Routing and Remote Access, kích chuột phải RemoteGroup sau đó kích Move Down.

 Đóng cửa sổ Routing and Remote Access

Bước 9:

Kiểm tra cấu hình đã thiết lập ở bước trên bằng việc thực hiện một kết nối quay số tới máy chủ truy cập từ xa với tài khoản có tên là RemoteUser. Thông báo lỗi xuất hiện, kết nối không được thiết lập.

Bước 10:

Cấu hình cho phép truy cập sử dụng Properties của RemoteUser

 Mở lại Active Directory Users and Computers từ menu Administrator Tools

 Mở Properties của RemoteUser

 Trong trang Dial-in, kích Allow access sau đó kích OK

 Đóng Active Directory Users and Computers.

Bước 11:

Kiểm tra cấu hình đã thiết lập ở bước trên bằng việc thực hiện một kết nối quay số tới máy chủ truy cập từ xa với tài khoản có tên là RemoteUser, kết nối được thiết lập sau đó đóng kết nối lại

Bài 3: Cấu hình VPN server và thiết lập VPN Client, kiểm tra kết nối từ VPN Client tới VPN server

Bước 1:

Cấu hình cho kết nối VPN gọi vào

 Đăng nhập vào hệ thống với quyền Administrator

 Mở Routing and Remote Access từ menu Administrator Tools

 Kích chuột phải vào tên Server (Server là tên máy chủ đang cấu hình)

 Kịch bản thiết lập Routing and Remote Access xuất hiện, kích next

 Trong trang Network Selection, mục Name kiểm tra tên đã lựa chọn sau đó Click next

 Trong trang IP Address Assigment, kích From a specified range of addresses

 Trong trang Address Range Assignment, kích New

 Điền địa chỉ IP vào ô Start IP address và điền vào số địa chỉ vào ô Number of Address

 Kích OK, sau đó kích next

 Trong trang Managing Multiple Remote Access Servers, lựa chọn No, I don’t want to set up this server to use RADIUS now, kích next sau đó kích Finish

 Kích OK để đóng hộp thoại Routing and Remote Access.

Cấu hình cho phép tài khoản Administrator truy cập vào mạng

 Mở Active Directory Users and Computers từ menu Administrator Tools.

 Mở rộng tên domain kích Users, kích đúp chuột vào Administrator

 Trong mục Dial-in, chọn Allow acces sau đó kích OK.

 Đóng của sổ Active Directory Users and Computers

Bước 2:

Cấu hình cho kết nối VPN gọi ra. Để kiểm tra dịch vụ truy cập từ xa đã làm việc phục vụ cho những người dùng từ xa, ta thiết lập một nối kết tới VPN server.

 Kích chuột phải vào My Network Places, sau đó kích Properties
 Trong của sổ Network Dialup Connections, kích đúp chuột vào Make new connection
 Trong trang Network Connection Type, kích Connect to a private network through the Internet, sau đó kích next
 Trong trang Destination Address page, gõ vào địa chỉ IP của máy cài đặt VPN server, sau đó kích next
 Trong trang Connection Availability, kích Only for my self, kích next sau đó kích Finish
 Khởi tạo kết nối tới VPN server
 Trong hộp thoại Connect Virtual Private Connection, kiểm tra tài khoản đăng nhập là Administrator và Password sau đó kích connect
 Kích OK để đóng thông báo Connnection Complete
 Đóng của sổ Network Dialup Connections.

Sử dụng tiện ích Ipconfig để xác nhận rằng bạn đã thiết lập được một kết nối VPN và nhận được địa IP cho kết nối này lưu ý rằng đại chỉ IP cho kết nối VPN này là dãy địa chỉ tĩnh mà VPN server cấp phát

Đóng kết nối

 Kích đúp vào biểu tượng Connection trong khay hệ thống
 Trong hộp thoại Vitual Private Connection Status, kích disconnect
 Đóng tất cả các cửa sổ lại

Mục 2 : Dịch vụ Proxy - Giải pháp cho việc kết nối mạng dùng riêng ra Internet

1. Các khái niệm

1.1. Mô hình client server và một số khả năng ứng dụng

Mô hình chuẩn cho các ứng dụng trên mạng là mô hình client-server.

Trong mô hình này máy tính đóng vai trò là một client là máy tính có nhu cầu cần phục vụ dịch vụ và máy tính đóng vai trò là một server là máy tính có thể đáp ứng được các yêu cầu về dịch vụ đó từ các client. Khái niệm client-server chỉ mang tính tương đối, điều này có nghĩa là một máy có thể lúc này đóng vai trò là client và lúc khác lại đóng vai trò là server. Nhìn chung, client là một máy tính cá nhân, còn các Server là các máy tính có cấu hình mạnh có chứa các cơ sở dữ liệu và các chương trình ứng dụng để phục vụ một dịch vụ nào đấy từ các yêu cầu của client (hình 5.13).

Hình 5.13: Mô hình client server

Cách thức hoạt động của mô hình client-server như sau: một tiến trình trên server khởi tạo luôn ở trạng thái chờ yêu cầu từ các tiến trình client, tiến trình tại client được khởi tạo có thể trên cùng hệ thống hoặc trên các hệ thống khác được kết nối thông qua mạng, tiến trình client thường được khởi tạo bởi các lệnh từ người dùng. Tiến trình client ra yêu cầu và gửi chúng qua mạng tới server để yêu cầu được phục vụ các dịch vụ. Tiến trình trên server thực hiện việc xác định yêu cầu hợp lệ từ client sau đó phục vụ và trả kết quả tới client và tiếp tục chờ đợi các yêu cầu khác. Một số kiểu dịch vụ mà server có thể cung cấp như: dịch vụ về thời gian (trả yêu cầu thông tin về thời gian tới client), dịch vụ in ấn (phục vụ yêu cầu in tại client), dịch vụ file (gửi, nhận và các thao tác về file cho client), thi hành các lệnh từ client trên server...

Dịch vụ web là một dịch vụ cơ bản trên mạng Internet hoạt động theo

mô hình client-server. Trình duyệt Web (Internet Explorer, Netscape...) trên các máy client sử dụng giao thức TCP/IP để đưa ra các yêu cầu HTTP tới máy server. Trình duyệt có thể đưa ra các yêu cầu một trang web cụ thể hay yêu cầu thông tin trong các cơ sở dữ liệu. Máy server sử dụng phần mềm của nó phân tích các yêu cầu từ các gói tin nhận được kiểm tra tính hợp lệ của client và thực hiện phục vụ các yêu cầu đó cụ thể là gửi trả lại client một trang web cụ thể hay các thông tin trên cơ sở dữ liệu dưới dạng một trang web. Server là nơi lưu trữ nội dung thông tin các website, phần mềm trên server cho phép server xác định được trang cần yêu cầu và gửi tới client. Cơ sở dữ liệu và các ứng dụng tương tự khác trên máy chủ được khai thác và kết nối qua các chương trình như CGI (Common Gateway Interface), khi các máy server nhận được yêu cầu về tra cứu trong cơ sở dữ liệu , nó chuyển yêu cầu tới server có chứa cơ sở dữ liệu hoặc ứng dụng để xử lý qua CGI.

1.2. Socket

Một kết nối được định nghĩa như là một liên kết truyền thông giữa các tiến trình, như vậy để xác định một kết nối cần phải xác định các thành phần sau: {Protocol, local-addr, local-process, remote-addr, remote-process}

Trong đó local-addr và remote-addr là địa chỉ của các máy địa phương và máy từ xa. local-process, remote-process để xác định vị trí tiến trình trên mỗi hệ thống. Chúng ta định nghĩa một nửa kết nối là {Protocol, local-addr, localprocess} và {Protocol, remote-addr, remote-process} hay còn gọi là một socket.

Chúng ta đã biết để xác đinh một máy ta dựa vào địa chỉ IP của nó, nhưng trên một máy có vô số các tiến trình ứng dụng đang chạy, để xác định vị trí các tiến trình ứng dụng này người ta định danh cho mỗi tiến trình một số hiệu cổng, giao thức TCP sử dụng 16 bit cho việc định danh các cổng tiến trình và qui ước số hiệu cổng từ 1-1023 được sử dụng cho các tiến trình chuẩn (như FTP qui ước sử dụng cổng 21, dịch vụ WEB qui ước cổng 80, dịch vụ gửi thư SMTP cổng 25...) số hiệu cổng từ 1024- 65535 dành cho các ứng dụng của người dùng. Như vậy một cổng kết hợp với một địa chỉ IP tạo thành một socket duy nhất trong liên mạng. Một kết nối TCP được cung cấp nhờ một liên kết logic giữa một cặp socket. Một socket có thể tham gia nhiều liên kết với các socket ở xa khác nhau. Trước khi truyền dữ liệu giữa hai trạm cần phải thiết lập một liên kết TCP giữa chúng và khi kết thúc phiên truyền dữ liệu thì liên kết đó sẽ được giải phóng.

Hình 5.14: Socket

Quá trình thiết lập một socket với các lời gọi hệ thống được mô tả như sau: server thiết lập một socket với các thông số đặc tả các thủ tục truyền thông như (TCP, UDP, XNS...) và các kiểu truyền thông (SOCK_STREAM,

SOCK_DGRAM...), sau đó liên kết tới socket này các thông số về địa chỉ như IP và các cổng TCP/UDP sau đó server ở chế độ chờ và chấp nhận kết nối đến từ client.

1.3. Phương thức hoạt động và đặc điểm của dịch vụ Proxy

1. Phương thức hoạt động

Dịch vụ proxy được triển khai nhằm mục đích phục vụ các kết nối từ các máy tính trong mạng dùng riêng ra Internet. Khi đăng ký sử dụng dịch vụ internet tới nhà cung cấp dịch vụ, khách hàng sẽ được cấp hữu hạn số lượng địa chỉ IP từ nhà cung cấp, số lượng IP nhận được không đủ để cấp cho các máy

tính trạm. Mặt khác với nhu cầu kết nối mạng dùng riêng ra Internet mà không muốn thay đổi lại cấu trúc mạng hiện tại đồng thời muốn gia tăng khả năng thi hành của mạng qua một kết nối Internet duy nhất và muốn kiểm soát tất cả các thông tin vào ra, muốn cấp quyền và ghi lại các thông tin truy cập của người sử dụng… Dịch vụ proxy đáp ứng được tất cả các yêu cầu trên. Hoạt động trên cơ sở mô hình client-server. Quá trình hoạt động của dịch vụ proxy theo các bước như sau:

Hình 5.15: Hoạt động của dịch vụ Proxy

1 Client yêu cầu một đối tượng trên mạng Internet

1 Proxy server tiếp nhận yêu cầu, kiểm tra tính hợp lệ cũng như thực hiện việc xác thực client nếu thỏa mãn proxy server gửi yêu cầu đối tượng này tới server trên Internet.

1 Server trên Internet gửi đối tượng yêu cầu về cho proxy server.

1 Proxy server gửi trả đối tượng về cho client

Ta có thể thiết lập proxy server để phục vụ cho nhiều dịch vụ như dịch vụ truyền file, dịch vụ web, dịch vụ thư điện tử…Mỗi một dịch vụ cần có một proxy server cụ thể để phục vụ các yêu cầu đặc thù của dịch vụ đó từ các client. Proxy server còn có thể được cấu hình để cho phép quảng bá các server thuộc mạng trong ra ngoài Internet với mức độ an toàn cao. Ví dụ ta có thể thiết lập một web server thuộc mạng trong và thiết lập các qui tắc quảng bá web trên proxy server để cho phép quảng bá web server này ra ngoài Internet. Tất cả các yêu cầu truy cập web đến được chấp nhận bởi proxy server và proxy server sẽ thực hiện việc chuyển tiếp yêu cầu tới web server thuộc mạng trong (hình 5.16)

Hình 5.16: Hoạt động của dịch vụ Proxy

Các client được tổ chức trong một cấu trúc mạng gọi là mạng trong (Inside network) hay còn gọi là mạng dùng riêng. IANA (Internet Assigned Numbers Authority) đã dành riêng 3 khoảng địa chỉ IP tương ứng với 3 lớp mạng tiêu chuẩn cho các mạng dùng riêng đó là:

10.0.0.0 - 10.255.255.255 (lớp A)

172.16.0.0 - 172.31.255.255 (lớp B)

192.168.0.0 - 192.168.255.255 (lớp C)

Các địa chỉ này sử dụng cho các client trong mạng dùng riêng mà không được gán cho bất cứ máy chủ nào trên mạng Internet. Trong việc thiết kế và cấu hình mạng dùng riêng khuyến nghị nên sử dụng các khoảng địa chỉ IP này.

Khái niệm mạng ngoài (Outside network) là để chỉ vùng mà các server thuộc vào. Các địa chỉ sử dụng trên mạng này là các địa chỉ IP được đăng ký hợp lệ của nhà cung cấp dịch vụ Internet.

Proxy server sử dụng hai giao tiếp, giao tiếp mạng trong và giao tiếp ngoài. Giao tiếp trong điển hình là các cạc mạng sử dụng cho việc kết nối giữa proxy server với mạng dùng riêng và có địa chỉ được gán là địa chỉ thuộc mạng dùng riêng. Tất cả các thông tin giữa client thuộc mạng dùng riêng và proxy server được thực hiện thông qua giao tiếp này. Giao tiếp ngoài thường bằng các hình thức truy cập gián tiếp qua mạng điện thoại công cộng và qua cạc mạng bằng kết nối trực tiếp tới mạng ngoài. Giao tiếp ngoài được gán địa chỉ IP thuộc mạng ngoài được cung cấp hợp lệ bởi nhà cung cấp dịch vụ Internet.

2. Đặc điểm

Proxy Server kết nối mạng dùng riêng với mạng Internet toàn cầu và cũng cho phép các máy tính trên mạng internet có thể truy cập các tài nguyên trong mạng dùng riêng.

Proxy Server tăng cường khả năng kết nối ra Internet của các máy tính

trong mạng dùng riêng bằng cách tập hợp các yêu cầu truy cập Internet từ các máy tính trong mạng và sau khi nhận được kết quả từ Internet sẽ trả lời lại cho máy có yêu cầu ban đầu.
Ngoài ra proxy server còn có khả năng bảo mật và kiểm soát truy cập Internet của các máy tính trong mạng dùng riêng. Cho phép thiết đặt các chính sách truy cập tới từng người dùng.

Proxy server lưu trữ tạm thời các kết quả đã được lấy từ Internet về nhằm trả lời cho các yêu cầu truy cập Internet với cùng địa chỉ. Việc lưu trữ này cho phép các yêu cầu truy cập Internet với cùng địa chỉ sẽ không cần phải lấy lại kết quả từ Internet, làm giảm thời gian truy cập Internet, tăng cường hoạt động của mạng và giảm tải trên đường kết nối Internet. Các công việc lưu trữ này gọi là quá trình cache.

1.4. Cache và các phương thức cache

Nhằm tăng cường khả năng truy cập Internet từ các máy tính trạm trong mạng sử dụng dịch vụ proxy ta sử dụng các phương thức cache. Dịch vụ proxy sử dụng cache để lưu trữ bản sao của các đối tượng đã được truy cập trước đó. Tất cả các đối tượng đều có thể được lưu trữ (như hình ảnh và các tệp tin), tuy nhiên một số đối tượng như yêu cầu xác thực (Authenticate) và sử dụng SSL (Secure Socket Layer) không được cache. Như vậy với các đối tượng đã được cache, khi một yêu cầu từ một máy tính trạm tới proxy server, proxy server thay vì kết nối tới địa chỉ mà máy tính trạm yêu cầu sẽ tìm kiếm trong cache các đối tượng thoã mãn và gửi trả kết quả về máy tính trạm. Như vậy cache cho phép cải thiện hiệu năng truy cập Internet của các máy trạm và làm giảm lưu lượng trên đường kết nối Internet. Vấn đề gặp phải khi sử dụng cache là khi các đối tượng được cache có sự thay đổi từ nguồn, các máy tính trạm yêu cầu một đối tượng tới proxy server, proxy server lấy đối tượng trong cache để phục vụ và như vậy thông tin chuyển tới các máy tính trạm là thông tin cũ so với nguồn, để giải quyết vấn đề này cần phải có các chính sách để cache các đối tượng đồng thời các đối tượng phải liên tục được cập nhật mới. Ví dụ: thông thường một địa chỉ WEB thì các đối tượng về hình ảnh ít có sự thay đổi còn nội dung text thường có sự thay đổi do đó ta có thể thiết đặt chỉ cache những đối tượng hình ảnh, những đối tượng có nội dung text thì không cache, điều này không ảnh hưởng tới hiệu suất truy cập vì các tập tin về hình ảnh thường có kính thước rất lớn so với các đối tượng có nội dung text, việc cập nhật các đối tượng như thế nào phụ thuộc vào các phương thức cache mà ta sẽ trình bày dưới đây.
Proxy server thực thi cache cho các đối tượng được yêu cầu một cách có chu kỳ để tăng hiệu suất của mạng. Ta có thể thiết lập cache để đảm bảo rằng nó bao gồm những dữ liệu thường hay các client sử dụng nhất. Proxy server có thể sử dụng cho phép thông tin giữa mạng dùng riêng và Internet, việc thông tin có thể là client trong mạng truy cập Internet-trong trường hợp này proxy server thực hiện Forward caching, cũng có thể là client ngoài truy cập tới mạng trong (tới các server được quảng bá)-trong trường hợp này proxy server thực hiện reverse caching. Cả hai trường hợp đều có được từ khả năng của proxy server là lưu trữ thông tin (tạm thời) làm cho việc truyền thông thông tin được nhanh hơn, sau đây là các tính chất của cache proxy server:
- Phân cache: khi cài đặt một mảng các máy proxy server ta sẽ thiết lập được việc phân phối nội dung cache. Proxy server cho phép ghép nhiều hệ thống thành một cache logic duy nhất.
- Cache phân cấp: Khả năng phân phối cache còn có thể chuyên sâu hơn bằng cách cài đặt chế độ cache phân cấp liên kết một loạt các máy proxy server với

nhau để client có thể truy cập tới gần chúng nhất.

- Cache định kỳ: sử dụng cache định kỳ nội dung download đối với các yêu cầu thường xuyên của các client
- Reverse cache: proxy server có thể cache các nội dung của các server quảng bá do đó tăng hiệu suất và khả năng truy cập, mọi đặc tính cache của proxy server đều có thể áp dụng cho nội dung trên các server quảng bá.

Proxy server có thể được triển khai như một Forward cache nhằm cung cấp tính năng cache cho các client mạng trong truy cập Internet. Proxy server duy trì bộ cache tập trung của các đối tượng Internet thường được yêu cầu có thể truy cập từ bất kỳ trình duyệt từ mày client. Các đối tượng phục vụ cho các yêu cầu từ các đĩa cache yêu cầu tác vụ xử lý nhỏ hơn đáng kể so với các đối tượng từ Internet, việc này tăng cường hiệu suất của trình duyệt trên client, giảm thời gian hồi đáp và giảm việc chiếm băng thông cho kết nối Internet. Hình vẽ sau mô tả proxy server xử lý các yêu cầu của người dùng ra sao (hình 6.17)

Hình 5.17: Hoạt động của dịch vụ Proxy

Hình trên mô tả quá trình các client trong mạng dùng riêng truy cập ra ngoài Internet nhưng tiến trình này cũng tương tự đối với các cache reverse (khi người dùng trên Internet truy cập vào các Server quảng bá) các bước bao gồm;

1 Client 1 yêu cầu một đối tượng trên mạng Internet

2 Proxy server kiểm tra xem đối tượng có trong cache hay không. Nếu đối tượng không có trong cache của proxy server thì proxy server gửi yêu cầu đối tượng tới server trên Internet.

3 Server trên Internet gửi đối tượng yêu cầu về cho proxy server .

4 proxy server giữ bản copy của đối tượng trong cache của nó và trả đối tượng về cho client1

5 Client 2 gửi một yêu cầu về đối tượng tương tự

6 Proxy server gửicho client 2 đối tượng từ cache của nó chứ không phải từ Internet nữa.

Ta có thể triển khai dịch vụ proxy để quảng bá các server trong mạng dùng riêng ra ngoài Internet. Với các yêu cầu đến, proxy server có thể đóng vai trò như là một server bên ngoài, đáp ứng các yêu cầu của client từ các nội dung web trong cache của nó. Proxy server chuyển tiếp các yêu cầu cho server chỉ khi nào cache của nó không thể phục vụ yêu cầu đó (*Reverse cache).*

Lựa chọn các phương thức cache dựa trên các yếu tố: không gian ổ cứng sử dụng, đối tượng nào được cache và khi nào các đối tượng này sẽ được cập nhật. Về cơ bản ta có hai phương thức cache thụ động và chủ động.

Phương thức Cache thụ động (passive cache): Cache thụ động lưu trữ các đối tượng chỉ khi các máy tính trạm yêu cầu tới đối tượng. Khi một đối tượng được chuyển tới máy tính trạm, máy chủ Proxy xác định xem đối tượng này có thể cache hay không nếu có thể đối tượng sẽ được cache. Các đối tượng chỉ được cập nhật khi có nhu cầu. Đối tượng sẽ bị xoá khỏi cache dựa trên thời điểm gần nhất mà các máy tính trạm truy cập tới đối tượng. Phương thức này có lợi ích là sử dụng ít hơn bộ xử lý nhưng tốn nhiều không gian ổ đĩa hơn

Phương thức Cache chủ động (active cache): Cũng giống như phương thức cache thụ động, Cache chủ động lưu trữ các đối tượng khi các máy tính trạm ra yêu cầu tới một đối tượng máy chủ Proxy đáp ứng yêu cầu và lưu đối

tượng này vào Cache. Phương thức này tự động cập nhật các đối tượng từ Internet dựa vào: số lượng yêu cầu đối với các đối tượng, đối tượng thường xuyên thay đổi như thế nào. Phương thức này sẽ tự động cập nhật các đối tượng khi mà máy chủ Proxy đang phục vụ ở mức độ thấp và do đó không ảnh hưởng đến hiệu suất phục vụ các máy tính trạm. Đối tượng trong cache sẽ bị xoá dựa trên các thông tin header HTTP, URL.

2. Triển khai dịch vụ proxy

2.1. Các mô hình kết nối mạng

Đối tượng phục vụ của proxy server khá rộng, từ mạng văn phòng nhỏ, mạng văn phòng vừa tới mạng của các tập đoàn lớn. Với mỗi quy mô tổ chức sẽ có một cấu trúc mạng sử dụng proxy server cho phù hợp. Sau đây chúng ta sẽ xem xét một số mô hình cơ bản đối với mạng cỡ nhỏ, mạng cỡ trung bình và mạng tập đoàn lớn. Trong đó chúng ta sẽ đi sâu vào mô hình thứ nhất dành cho mạng văn phòng nhỏ bởi nó phù hợp quy mô tổ chức của các công ty vừa và nhỏ tại Việt nam.

Mô hình mạng văn phòng nhỏ:

- Bao gồm một mạng LAN độc lập.
- Sử dụng giao thức IP.
- Kết nối Internet bằng đường thoại (qua mạng điện thoại công cộng bằng các hình thức quay dial-up hay sử dụng công nghệ ADSL) hoặc đường trực tiếp (Leased Line).
- Ít hơn 250 máy tính trạm.

Mô hình kết nối mạng như hình vẽ (hình 5.18)

Hình 5.18: Mô hình kết nối mạng

Theo mô hình này, với mỗi phương thức kết nối Internet Proxy server sử dụng 02 giao tiếp như sau:

- Kết nối Internet bằng đường thoại qua mạng PSTN:
  - 01 giao tiếp với mạng nội bộ thông qua card mạng.
  - 01 giao tiếp với Internet thông qua Modem.
- Kết nối Internet bằng đường trực tiếp (Leased Line)
  - 01 giao tiếp với mạng nội bộ thông qua card mạng
  - 01 giao tiếp với Internet thông qua card mạng khác. Lúc này bảng địa chỉ nội bộ (LAT-Local Address Table) được xây dựng dựa trên danh sách địa chỉ IP mạng nội bộ.

Mô hình kết nối mạng cỡ trung bình

Đặc trưng của mạng văn phòng cỡ trung bình như sau:

- Văn phòng trung tâm với một vài mạng LAN
- Mỗi văn phòng chi nhánh có một mạng LAN.
- Sử dụng giao thức IP.
- Kết nối bằng đường thoại từ văn phòng chi nhánh tới văn phòng trung tâm.
- Kết nối Internet từ văn phòng trung tâm tới ISP bằng đường thoại hoặc đường trực tiếp (Leased Line).
- Ít hơn 2000 máy tính trạm

Mô hình mạng như hình 5.19. Theo mô hình này, văn phòng chi nhánh sử dụng một máy chủ Proxy cung cấp khả năng lưu trữ thông tin nội bộ (local caching), quản trị kết nối và kiểm soát truy cập tới văn phòng trung tâm. Tại văn phòng trung tâm, một số máy chủ Proxy hoạt động theo kiến trúc mảng (array) cung cấp khả năng bảo mật chung cho toàn mạng, cung cấp tính năng lưu trữ thông tin phân tán (distributed caching) và cung cấp kết nối ra Internet.

Hình 5.19: Mô hình kết nối mạng
Mô hình kết nối mạng tập đoàn lớn
Mạng của các tập đoàn lớn có đặc trưng như sau:
- Văn phòng trung tâm có nhiều mạng LAN và có mạng trục LAN.
- Có vài văn phòng chi nhánh, mỗi văn phòng chi nhánh có một mạng LAN.
- Sử dụng giao thức mạng IP.
- Kết nối bằng đường thoại từ các văn phòng chi nhánh tới văn phòng trung tâm.
- Kết nối Internet từ văn phòng trung tâm tới ISP bằng đường đường trực tiếp (Leased Line).
- Có nhiều hơn 2000 máy tính trạm.

Mô hình mạng như hình 5.20. Theo mô hình này mạng tại các văn phòng chi nhánh cũng cấu hình tương tự như đối với mô hình các văn phòng cỡ trung bình. Các yêu cầu kết nối Internet không được đáp ứng bởi cache nội bộ tại máy chủ Proxy của văn phòng chi nhánh sẽ được chuyển tới một loạt máy chủ Proxy hoạt động theo kiến trúc mảng tại văn phòng trung tâm. Tại văn phòng trung tâm các máy chủ Proxy sử dụng 02 giao tiếp mạng (card mạng) trong đó 01 card mạng giao tiếp với mạng trục LAN và 01 card mạng giao tiếp với mạng LAN thành viên.

Hình 5.20: Mô hình kết nối mạng

2.2. Thiết lập chính sách truy cập và các qui tắc

1..Các qui tắc.

Ta có thể thiết lập proxy server để đáp ứng các yêu cầu bảo mật và vận hành bằng cách thiết lập các qui tắc để xác định xem liệu người dùng, máy tính hoặc ứng dụng có được quyền truy cập và truy cập như thế nào tới máy tính trong mạng hay trên Internet hay không. Thông thường một proxy server định nghĩa các loại qui tắc sau: Qui tắc về chính sách truy nhập, qui tắc về băng thông, qui tắc về chính sách quảng bá, các đặc tính lọc gói và qui tắc về định tuyến và chuỗi (chaining).

Khi một client trong mạng yêu cầu một đối tượng proxy server sẽ xử lý các qui tắc để xác định xem yêu cầu đó có được xác định chấp nhận hay không. Tương tự khi một client bên ngoài (Internet) yêu cầu một đối tượng từ một server trong mạng, proxy server cũng xử lý các bộ qui tắc xem yêu cầu có được cho phép không.

*Các qui tắc của chính sách truy nhập:*Ta có thể sử dụng proxy server để thiết lập chính sách bao gồm các qui tắc về giao thức, qui tắc về nội dung. Các qui tắc giao thức định nghĩa giao thức nào có thể sử dụng cho thông tin giữa mạng trong và Internet. Qui tắc giao thức sẽ được xử lý ở mức ứng dụng. Ví dụ một qui tắc giao thức có thể cho phép các Client sử dụng giao thức HTTP. Các qui tắc về nội dung qui định những nội dung nào trên các site nào mà client có thể truy nhập. Các qui tắc nội dung cùng được xử lý ở mức ứng dụng. Ví dụ một qui tắc về nội dung có thể cho phép các client truy nhập tới bất kỳ địa chỉ nào trên Internet.

Qui tắc băng thông: Qui tắc băng thông xác định kết nối nào nhận được quyền ưu tiên.Trong việc điều khiển băng thông thường thì proxy server không giới hạn độ rộng băng thông. Hơn nữa nó cho biết chất lượng dịch vụ (QoS) được cấp phát ưu tiên cho các kết nối mạng như thế nào. Thường thì bất kỳ kết

nối nào không có qui tắc về băng thông kèm theo sẽ nhận được quyền ưu tiên ngầm định và bất kỳ kết nối nào có qui tắc băng thông đi kèm sẽ được sắ_____p xếp với quyền ưu tiên hơn quyền ưu tiên ngầm định.

Các qui tắc về chính sách quảng bá: Ta có thể sử dụng proxy server để thiết lập chính sách quảng bá, bao gồm các qui tắc quảng bá server và qui tắc quảng bá web. Các qui tắc quảng bá server và web lọc tất cả các yêu cầu đến từ các yêu cầu của client ngoài mạng (internet) tới các server trong mạng. Các qui tắc quảng bá server và web sẽ đưa các yêu cầu đến cho các server thích hợp phía sau proxy server.

Đặc tính lọc gói: Đặc tính lọc gói của proxy server cho phép điều khiển luồng các gói IP đến và đi từ proxy server. Khi lọc gói hoạt động thì mọi gói trên giao diện bên ngoài đều bị rớt lại, trừ khi chúng được hoàn toàn cho phép hoặc là một cách cố định bằng các bộ lọc gói IP, hoặc là một cách động bằng các chính sách truy cập hay quảng bá. Thậm chí nếu bạn không để lọc gói hoạt động thì truyền thông giữa mạng Internet và mạng cục bộ được cho phép khi nào bạn thiết lập rõ ràng các qui tắc cho phép truy cập. Trong hầu hết các trường hợp, việc mở các cổng động thường được sử dụng hơn. Do đó, người ta thường khuyến nghị rằng bạn nên thiết lập các qui tắc truy cập cho phép client trong mạng truy nhập vào Internet hoặc các qui tắc quảng bá cho phép client bên ngoài truy nhập vào các server bên trong. Đó là do các bộ lọc gói IP mở một cách cố định những chính sách truy nhập và qui tắc quảng bá lại mở các cổng kiểu động. Giả sử bạn muốn cấp quyền cho mọi người dùng trong mạng truy cập tới các site HTTP. Bạn không nên thiết lập một bộ lọc gói IP để mở cổng 80. Nên thiết lập qui tắc về site, nội dung và giao thức cần thiết để cho phép việc truy nhập này. Trong một vài trường hợp ta sẽ phải sử dụng các lọc gói IP, ví dụ nên thiết lập các lọc gói IP nếu ta muốn quảng bá các Server ra bên ngoài.

Qui tắc định tuyến và cấu hình chuỗi proxy (chaining): thường là qui tắc được áp dụng sau cùng để định tuyến các yêu cầu của client tới một server đã được chỉ định để phục vụ các yêu cầu đó.

2. Xử lý các yêu cầu đi

Một trong các chức năng chính của proxy server là khả năng kết nối mạng dùng riêng ra Internet trong khi bảo vệ mạng khỏi những nội dung có ác ý. Để thuận tiện cho việc kiểm soát kết nối này, ta dùng proxy server để tạo ra một chính sách truy cập cho phép các client truy cập tới các server trên Internet cụ thể, chính sách truy cập cùng với các qui tắc định tuyến quyết định các client truy cập Internet như thế nào.

Khi proxy server xử lý một yêu cầu đi, proxy server kiểm tra các qui tắc định tuyến các qui tắc về nội dung và các qui tắc giao thức để xem xét việc truy cập có được phép hay không. Yêu cầu chỉ được cho phép nếu cả quy tắc giao

thức, qui tắc nội dung và site cho phép và nếu không một qui tắc nào từ chối yêu cầu.

Một vài qui tắc có thể được thiết lập để áp dụng cho các client cụ thể. Trong trường hợp này, các client có thể được chỉ định hoặc là bằng địa chỉ IP hoặc bằng user name. Proxy server xử lý các yêu cầu theo cách khác nhau phụ thuộc vào kiểu yêu cầu của client và việc thiết lập proxy server.Với một yêu cầu, các qui tắc được xử lý theo thứ tự như sau: qui tắc giao thức, qui tắc nội dung, các lọc gói IP, qui tắc định tuyến hoặc cấu hình chuỗi proxy.

Hình dưới đưa ra quá trình xử lý đối với một yêu cầu đi (hình 5.21)

Hình 5.21: Quá trình xử lý đối với một yêu cầu đi

Trước tiên, proxy server kiểm tra các qui tắc giao thức, proxy server chấp nhận yêu cầu chỉ khi một qui tắc giao thức chấp nhận một cách cụ thể yêu cầu và không một qui tắc giao thức nào từ chối yêu cầu đó.
Sau đó, proxy server kiểm tra các qui tắc về nội dung. Proxy server chỉ chấp nhận yêu cầu nếu một qui tắc về nội dung chấp nhận yêu cầu và không có một qui tắc về nội dung nào từ chối nó.
Tiếp đến proxy server kiểm tra xem liệu có một bộ lọc gói IP nào được thiết lập để loại bỏ yêu cầu không để quyết định xem liệu yêu cầu có bị từ chối.
Cuối cùng, proxy server kiểm tra qui tắc định tuyến để quyết định xem yêu cầu được phục vụ như thế nào.
Giả sử cài đặt một proxy server trên một máy tính với hai giao tiếp kết nối, một kết nố_____i với Internet và một kết nối vào mạng dùng riêng. Ta sẽ cho các chỉ dẫn để cho phép tất cả client truy cập vào tất cả các site. Trong trường hợp này, chính sách truy nhập chỉ là các qui tắc như sau: một qui tắc về giao thức

cho phép tất cả các client sử dụng mọi giao thức tại tất cả các thời điểm .Một qui tắc về nội dung cho phép tất cả mọi người truy cập tới mọi nội dung trên tất cả các site ở tất cả các thời điểm nào. Lưu ý rằng qui tắc này cho phép các client truy cập Internet nhưng không cho các client bên ngoài truy cập vào mạng của bạn.

3. Xử lý các yêu cầu đến

Proxy server có thể được thiết lập để các Server bên trong có thể truy cập an toàn đến từ các client ngoài. Ta có thể sử dụng proxy server để thiết lập một chính sách quảng bá an toàn cho các Server trong mạng. Chính sách quảng bá (bao gồm các bộ lọc gói IP, các qui tắc quảng bá Web, hoặc qui tắc quảng bá Server, cùng với các qui tắc định tuyến) sẽ quyết định các Server được quảng bá như thế nào.
Khi proxy server xử lý một yêu cầu xuất phát từ một client bên ngoài, nó sẽ kiểm tra các bộ lọc gói IP, các qui tắc quảng bá và các qui tắc định tuyến để quyết định xem liệu yêu cầu có được thực hiện hay không và Server trong nào sẽ thực hiện các yêu cầu đó.

Hình 5.22: Xử lý các yêu cầu đến

Giả sử rằng đã cài đặt proxy server với hai giao tiếp kết nối, một kết nối tới Internet và một kết nối vào mạng dùng riêng. Nếu lọc gói hoạt động và sau đó, bộ lọc gói IP từ chối yêu cầu thì yêu cầu sẽ bị từ chối. Nếu các qui tắc quảng bá web từ chối yêu cầu thì yêu cầu cũng bị loại bỏ. Nếu một qui tắc định tuyến được thiết lập yêu cầu được định tuyến tới một Server upstream hoặc một site chủ kế phiên thì Server được xác định đó sẽ xử lý yêu cầu. Nếu một qui tắc định tuyến chỉ ra rằng các yêu cầu được định tuyến tới một Server cụ thể thì web Server trong sẽ trả về đối tượng.

2.3. Proxy client và các phương thức nhận thực

Chính sách truy nhập và các qui tắc quảng bá của Proxy server có thể được thiết lập để cho phép hoặc từ chối một nhóm máy tính hay một nhóm các người dùng truy nhập tới một server nào đó. Nếu qui tắc được áp dụng riêng với các người dùng, Proxy server sẽ kiểm tra các đặc tính yêu cầu để quyết định người dùng được nhận thực như thế nào.
Ta có thể thiết lập các thông số cho các yêu cầu thông tin đi và đến để người dùng phải được proxy server nhận thực trước khi xử lý các qui tắc. Việc này đảm bảo rằng các yêu cầu chỉ được phép nếu người dùng đưa ra các yêu

cầu đã được xác thực. Bạn cũng có thể thiết lập các phương pháp nhận thực được sử dụng và có thể thiết lập các phương pháp nhận thực cho các yêu cầu đi và yêu cầu đến khác nhau. Về cơ bản một Proxy server thường hỗ trợ các phương pháp nhận thực sau đây: phương thức nhận thực cơ bản., nhận thực Digest, nhận thực tích hợp Microsoft windows, chứng thực client và chứng thực server.

Đảm bảo rằng các chương trình proxy client phải hỗ trợ một trong các phương pháp nhận thực mà proxy server đã đưa ra. Trình duyệt IE 5 trở lên hỗ trợ hầu hết các phương pháp nhận thực, một vài trình duyệt khác có thể chỉ hỗ trợ phương pháp nhận thực cơ bản. Đảm bảo rằng các trình duyệt client có thể hỗ trợ ít nhất một trong số các phương pháp nhận thực mà Proxy server hỗ trợ.

1. Phương pháp nhận thực cơ bản.

Phương pháp nhận thực này gửi và nhận các thông tin về người dùng là các ký tự text dễ dàng đọc được. Thông thường thì các thông tin về user name và password sẽ được mã hoá thì trong phương pháp này không có sự mã hoá nào được sử dụng. Tiến trình nhận thực được mô tả như sau, proxy client nhắc người dùng đưa vào username và password sau đó thông tin này được client gửi cho proxy server. Cuối cùng username và password được kiểm tra như là một tài khoản trên proxy server.

2. Phương pháp nhận thực Digest.

Phương pháp này có tính chất tương tự như phương pháp nhận thực cơ bản nhưng khác ở việc chuyển các thông tin nhận thực. Các thông tin nhận thực qua một tiến trình xử lý một chiều thường được biết với cái tên là "hashing". Kết quả của tiến trình này gọi là hash hay message digest và không thể giải mã chúng. Thông tin gốc không thể phục hồi từ hash. Các thông tin được bổ sung vào password trước khi hash nên không ai có thể bắt được password và sử dụng chúng để giả danh người dùng thực. Các giá trị được thêm vào để giúp nhận dạng người dùng. Một tem thời gian cũng được thêm vào để ngăn cản người dùng sử dụng một password sau khi nó đã bị huỷ. Đây là một ưu điểm rõ ràng so với phương pháp nhận thực cơ bản bởi vì người dùng bất hợp pháp không thể chặn bắt được password.

3. Phương pháp nhận thực tích hợp.

Phương pháp này được sử dụng tích hợp trong các sản phẩm của Microsoft. Đây cũng là phương pháp chuẩn của việc nhận thực bởi vì username và password không được gửi qua mạng. Phương pháp này sử dụng hoặc giao

thức nhận thực V5 Kerberos hoặc giao thức nhận thực challenge/response của nó.

4. Chứng thực client và chứng thực server

Ta có thể sử dụng các đặc tính của SSL để nhận thực. Chứng thực được sử dụng theo hai cách khi một client yêu cầu một đối tượng từ server: server nhận thực chính nó bằng cách gửi đi một chứng thực server cho client. Server yêu cầu client nhận thực chính nó (Trong trường hợp này client phải đưa ra một chứng thực client phù hợp tới server).

SSL nhận thực bằng cách kiểm tra nội dung của một chứng thực số được mã hoá do proxy client đệ trình lên trong quá trình đăng nhập (Các người dùng có thể có được các chứng thực số từ một tổ chức ngoài có độ tin tưởng cao). Các chứng thực về server bao gồm các thông tin nhận biết về server. Các chứng thực về client thường gồm các thông tin nhận biết về người dùng và tổ chức đưa ra chứng thực đó

Chứng thực client: Nếu chứng thực client được lựa chọn là phương thức

xác thực thì proxy server yêu cầu client gửi chứng thực đến *trước* khi yêu cầu một đối tượng. Proxy server nhận yêu cầu và gửi một chứng thực cho client. Client nhận chứng thực này và kiểm tra xem có thực là thuộc về proxy server . Client gửi yêu cầu của nó cho proxy server, tuy nhiên proxy server yêu cầu một chứng thực từ client mà đã được đưa ra trước đó. Proxy server kiểm tra xem chứng thực có thực sự thuộcc về client được phép truy cập không.

Chứng thực server: Khi một client yêu cầu một đối tượng SSL từ một server, client yêu cầu server phải nhận thực chính nó. Nếu proxy server kết thúc một kết nối SSL thì sau đó proxy server sẽ phải nhận thực chính nó cho client. Ta phải thiết lập và chỉ định các chứng thực về phía server để sử dụng khi nhận thực server cho client

5. Nhận thực pass-though

Nhận thực pass-though chỉ đến khả năng của proxy server chuyển thông tin nhận thực của client cho server đích. Proxy server hỗ trợ nhận thực cho cả các yêu cầu đi và đến. Hình vẽ sau mô tả trường hợp nhận thực pass-though.

Hình 5.23: Nhận thực pass-though

Client gửi yêu cầu lấy một đối tượng trên một web server cho proxy server. Proxy server chuyển yêu cầu này cho web server, bắt đầu từ đây việc nhận thực qua các bước sau:

1 Webserver nhận được yêu cầu lấy đối tượng và đáp lại rằng client cần phải nhận thực. Web server cũng chỉ ra các kiểu nhận thực được hỗ trợ.

2 Proxy server chuyển yêu cầu nhận thực cho client

3 Client tiếp nhận yêu cầu và trả các thông tin nhận thực cho proxy server

4 Proxy server chuyển lại thông tin đó cho web server

5 Từ lúc này client liên lạc trực tiếp với web server

6. SSL Tunneling.

Với đường hầm SSL, một client có thể thiết lập một đường hầm qua proxy server trực tiếp tới server yeu cầu với các đối tượng yêu cầu là HTTPS. Bất cứ khi nào client yêu cầu một đối tượng HTTPS qua proxy server nó sử dụng đường hầm SSL. Đường hầm SSL làm việc bởi sự ngầm định các yêu cầu đi tới các cổng 443 và 563.

Hình 5.24: SSL Tunneling.

Tiến trình tạo đường hầm SSL được mô tả như sau:

1 Khi client yêu cầu một đối tượng HTTPS từ một web server trên Internet, proxy server gửi một yêu cầu kết nối https://*URL_name*

2 Yêu cầu tiếp theo được gửi tới cổng 8080 trên máy proxy server
CONNECT *URL_name*:443 HTTP/1.1

3 Proxy server kết nối tới Web server trên cổng 443

4 Khi một kết nối TCP được thiết lập, proxy server trả lại kết nối đã được thiết lập HTTP/1.0 200

5 Từ đây, client thông tin trực tiếp với Web server bên ngoài

7. SSL bridging.

SSL bridging đề cập đến khả năng của proxy server trong việc mã hóa hoặc giải mã các yêu cầu của client và chuyển các yêu cầu này tới server đích. Ví dụ, trong trường hợp quảng bá (hoặc reverse proxy), proxy server có thể phục vụ một yêu cầu SSL của client bằng cách chấm dứt kết nối SSL với client và mở lại một kết nối mới với web server. SSL bridging được sử dụng khi proxy server kết thúc hoặc khởi tạo một kết nối SSL.

Khi một client yêu cầu một đối tượng HTTP. Proxy server mã hóa yêu cầu và chuyển tiếp nó cho web server. Web server trả về đối tượng đã mã hóa cho proxy server. Sau đó proxy server giải mã đối tượng và gửi lại cho client. Nói một cách khác các yêu cầu HTTP được chuyển tiếp như các yêu cầu SSL.
Khi client yêu cầu một đối tượng SSL. Proxy server giải mã yêu cầu, sau đó mã hóa lại một lần nữa và chuyển tiếp nó tới Web server. Web server trả về đối tượng mã hóa cho proxy server. Proxy server giải mã đối tượng và sau đó gửi nó cho client. Nói một cách khác các yêu cầu SSL được chuyển tiếp như là các yêu cầu SSL.
Khi client yêu cầu một đối tượng SSL. Proxy server giải mã yêu cầu và chuyển tiếp nó cho web server. Web server trả về đối tượng HTTP cho proxy server. Proxy server mã hóa đối tượng và chuyển nó cho client. Nói cách khác các yêu cầu SSL được chuyển tiếp như các yêu cầu HTTP.
SSL bridging có thể được thiết lập cho các yêu cầu đi và đến. Tuy nhiên với các yêu cầu đi client phải hỗ trợ truyền thông bảo mật với proxy server.

2.4. NAT và proxy server

Khái niệm NAT (Network Addresss Tranlation)

NAT là một giao thức cho ta khả năng bản đồ hóa một một vùng địa chỉ IP sử dụng trong mạng dùng riêng ra mạng ngoài và ngược lại. NAT thường được thiết lập trên các bộ định tuyến là ranh giới giữa mạng dùng riêng và mạng ngoài (ví dụ như mạng công cộng Internet). NAT chuyển đổi các địa chỉ IP trên mạng dùng riêng thành các địa chỉ IP được đăng ký hợp lệ trước khi chuyển các gói từ mạng dùng riêng tới Internet hoặc tới mạng ngoài khác. Trong phần này chúng ta sẽ chỉ tìm hiểu sự vận hành của NAT khi NAT được thiết lập để cung cấp các chức năng chuyển đổi các địa chỉ mạng dùng riêng trong việc phục vụ cho việc kết nối truy cập ra mạng ngoài như thế nào. Để làm việc này, NAT dùng tiến trình các bước theo hình vẽ dưới đây.

Hình 5.25: NAT

1. Người dùng tại máy 10.1.1.25 muốn mở một kết nối ra ngoài tới server 203.162.0.12

2. Khi gói dữ liệu đầu tiên tới NAT router, NAT router thực hiện việc kiểm tra trong bảng NAT. Nếu sự chuyển đổi địa chỉ đã có trong bảng, NAT router thực hiện bước thứ 3. Nếu không có sự chuyển đổi nào được tìm thấy, NAT router xác định rằng địa chỉ 10.1.1.25 phải được chuyển đổi. NAT router xác định một địa chỉ mới và cấu hình một chuyển đổi đối với địa chỉ 10.1.1.25 tới địa chỉ hợp lệ ngoài mạng (Internet) từ dãy địa chỉ động đã được định nghĩa từ trước ví dụ 203.162.94.163.
3. NAT router thay thế địa chỉ 10.1.1.25 bằng địa chỉ 203.162.94.163 sau đó gói được chuyển tiếp tới đích.
4. Server 203.162.0.12 trên Internet nhận gói và phúc đáp trở lại NAT router với địa chỉ 203.162.94.163.
5. Khi NAT router nhận được gói phúc đáp từ Server với địa chỉ đích đến là 203.162.94.163, nó thực hiện việc tìm kiếm trong bảng NAT. Bảng NAT chỉ ra rằng địa chỉ mạng trong 10.1.1.25 (tương ứng được ánh xạ tới địa chỉ 203.162.94.163 ở mạng ngoài) sẽ nhận được gói tin này. NAT router thực hiện việc chuyển đổi địa chỉ đích trong gói tin là 10.1.1.25 và chuyển gói tin này tới đích (10.1.1.25). Máy 10.1.1.25 nhận gói và tiếp tục thực hiện với các gói tiếp theo với các bước tuần tự như trên.

Trong trường hợp muốn sử dụng một địa chỉ mạng ngoài cho nhiều địa chỉ mạng trong. NAT router sẽ duy trì các thông tin thủ tục mức cao hơn trong

bảng NAT đối với các số hiệu cổng TCP và UDP để chuyển đổi địa chỉ mạng ngoài trở lại chính xác tới các địa chỉ mạng trong.
Như vậy NAT cho phép các client trong mạng dùng riêng với việc sử dụng các địa chỉ IP dùng riêng truy cập vào một mạng bên ngoài như mạng Internet.Cung cấp kết nối ra ngoài Internet trong các mạng không được cung cấp đủ các địa chỉ Internet có đăng ký. Thích hợp cho việc chuyển đổi địa chỉ trong hai mạng Intranet ghép nối nhau. Chuyển đổi các địa chỉ IP nội tại được ISP cũ phân bố thành các địa chỉ được phân bố bởi ISP mới mà không cần thiết lập thủ công các giao diện mạng cục bộ.
NAT có thể được sử dụng một cách cố định hoặc động. Chuyển đổi cố định xảy ra khi ta thiết lập thủ công một bảng địa chỉ cùng các địa chỉ IP. Một địa chỉ cụ thể ở bên trong mạng sử dụng một địa chỉ IP (được thiết lập thủ công bởi người quản trị mạng) để truy cập ra mạng ngoài. Các thiết lập động cho phép người quản trị thiết lập một hoặc nhiều các nhóm địa chỉ IP dùng chung đã đăng ký. Những địa chỉ trong nhóm này có thể được sử dụng bởi các client trên mạng dùng riêng để truy cập ra mạng ngoài. Việc này cho phép nhiều client trong mạng sử dụng cùng một địa chỉ IP.
NAT cũng có một số nhược điểm như làm tăng độ trễ của các gói tin trên mạng. NAT phải xử lý mọi gói để quyết định xem liệu các header được thay đổi như thế nào. Không phải bất kỳ ứng dụng nào cũng có thể chạy được với NAT. NAT hỗ trợ nhiều giao thức truyền thông và cũng rất nhiều giao thức không được hỗ trợ. Các giao thức được NAT hỗ trợ như:TCP,UDP, HTTP, TFTP, FTP…Các thông tin không được hỗ trợ như: IP multicast, BOOTP, DNS zone transfer, SNMP…

Proxy và NAT

Như đã phân tích cả dịch vụ NAT và dịch vụ Proxy đều có thể là một giải pháp để kết nối các mạng dùng riêng ra Internet, tuy nhiên mỗi dịch vụ lại có các ưu điểm và nhược điểm riêng.
Dịch vụ proxy cho khả năng thi hành và tốc độ cao hơn nhờ tính năng cache, tuy nhiên sử dụng cache có thể đưa ra các đối tượng đã quá hạn cần phải có các chính sách cache hợp lý đề đảm bảo tính thời sự của các đối tượng. Chính vì sử dụng cache nên giảm tải trên kết nối truy cập Internet. NAT không có tính năng cache.
Dịch vụ proxy phải được triển khai đối với từng ứng dụng, trong khi NAT là một tiến trình trong suốt hơn. Hầu hết các ứng dụng đều có thể làm việc được với NAT. NAT dễ cài đặt và vận hành, dường như không phải làm gì nhiều với NAT sau khi cài đặt.
Tại các client, đối với NAT không phải thiết đặt gì nhiều ngoài việc cấu hình tham số default gateway tới Server NAT. Trong khi sử dụng dịch vụ proxy, cần phải có các chương trình proxy client để làm việc với proxy server.
Dịch vụ proxy cho phép thiết đặt các chính sách tới người dùng, với NAT việc sử dụng các tính năng này có hạn chế rất nhiều, có thể nói sử dụng dịch vụ proxy là cách truy cập an toàn nhất để kết nối mạng dùng riêng ra ngoài Internet.

3. Các tính năng của phần mềm Microsoft ISA server 2000

3.1. Các phiên bản

ISA server bao gồm hai phiên bản được thiết kế để phù hợp với từng nhu cầu của người sử dụng đó là ISA server Standard và ISA server Enterprise.
- ISA server Standard cung cấp khả năng an toàn firewall và khả năng web cache cho một môi trường kinh doanh, các nhóm làm việc hay văn phòng

nhỏ. ISA server Standard cung cấp việc bảo mật chặt chẽ, truy cập web nhanh, quản lý trực quan, giá cả hợplý và khả năng thi hành cao.
- ISA server Enterprise được thiết kế đẻ đáp ứng các nhu cầu về hiệu suất, quản trị và cân bằng trong các môi trường Internet tốc độ cao với sự quản lý server tập trung, chính sách truy cập đa mức và các khả năng chống lỗi cao. ISA server Enterprisecung cấp sự bảo mật, truy cập Internet nhanh cho các môi trường có sự đòi hỏi khắt khe.

3.2. Lợi ích

ISA server là một trong các phần mềm máy chủ thuộc dòng .NET Enterprise Server. Các sản phẩm thuộc dòng .NET Enterprise Server là các server ứng dụng toàn diện của Microsoft trong việc xây dựng, triển khai, quản lý, tích hợp, các giải pháp dựa trên web và các dịch vụ. ISA server mang lại một số các lợi ích cho các tổ chức cần kết nối Internet nhanh, bảo mật, dễ quản lý.

1. Truy cập Web nhanh với cache hiệu suất cao.
- Người dùng có thể truy cập web nhanh hơn bằng các đối tượng tại chỗ trong cache so với việc phải kết nối vào Internet lúc nào cũng tiềm tàng nguy cơ tắc nghẽn.
- Giảm giá thành băng thông nhờ giảm lưu lượng từ Internet
- Phân tán nội dung của các Web server và các ứng dụng thương mại điện tử một cách hiệu quả, đáp ứng được nhu cầu khách hàng trên toàn cầu (khả năng phân phối nội dung web chỉ có trên phiên bản ISA server Enterprise)
2. Kết nối Internet an toàn nhờ Firewall nhiều lớp.
- Bảo vệ mạng trước các truy nhập bất hợp pháp bằng cách giám sát lưu lượng mạng tại nhiều lớp
- Bảo vệ các máy chủ web, email và các ứng dụng khác khỏi sự tấn công từ bên ngoài bằng việc sử dụng web và server quảng bá để xử lý một cách an toàn các yêu cầu đến
- Lọc lưu lượng mạng đi và đến để đảm bảo an toàn.
- Cung cấp truy cập an toan cho người dùng hợp lệ từ Internet tới mạng nội tại nhờ sử dụng mạng riêng ảo (VPN)
3. Quản lý thống nhất với sự quản trị tích hợp.
- Điều khiển truy cập tập trung để đảm bảo tính an toàn và phát huy hiệu lực của các chính sách vận hành.
- Tăng hiệu suất nhờ việc giới hạn truy cập sử dụng Internet đối với một số các ứng dụng và đích đến.
- Cấp phát băng thông để phù hợp với các ưu tiên.
- Cung cấp các công cụ giám sát và các báo cáo để chỉ ra kết nối Internet được sử dụng như thế nào.
- Tự động hóa các nhiệm vụ bằng việc sử dụng các script
4. Khả năng mở rộng.
- Chú trọng tới an toàn và thi hành nhờ sử dụng ISA server Softwware Development Kit (SDK) với sự phát triển các thành phần bổ sung.
- Chức năng quản lý và an toàn mở rộng cho các nhà sản xuất thứ ba
- Tự động các tác vụ quản trị với các đối tượng Script COM (Component Object Model)

3.3. Các chế độ cài đặt

ISA server có thể được cài đặt ở ba chế độ khác nhau: Cache, Firewall và Integrated

1. Chế độ cache: Trong chế độ này ta có thể nâng cao hiệu suất truy cập và

tiết kiệm băng thông bằng cách lưu trữ các đối tượng web thường được truy xuất từ người dùng. Ta cũng có thể định tuyến các yêu cầu của người dùng tới cache server khác đang lưu giữ các đối tượng đó.

2. Chế độ firewall: Trong chế độ này cho phép ta đảm bảo an toàn lưu lượng mạng nhờ sự thiết lập các qui tắc điều khiển thông tin giữa mạng trong và Internet. Ta cũng có thể quảng bá các server trong để chia sẻ dữ liệu trên mạng với các đối tác và khách hàng.
3. Chế độ tích hợp: Trong chế độ này ta có thể tích hợp các dịch vụ cache và firewall trên một server.

3.4. Các tính năng của mỗi chế độ cài đặt

Các tính năng khác nhau tùy thuộc vào chế độ mà ta cài đặt, bảng sau liệt kê các tính năng có trong chế độ firewall và cache, chế độ tích hợp có tất cả các tính năng đó

Tính năng	**Mô tả**	**Chế độ firewall**	**Chế độ cache**
Chính sách truy cập	Định nghĩa các giao thức và nội dung Internet mà người dùng có thể sử dụng và truy cập	Có	Chỉ có HTTP và FTP
Cache	Lưu trữ định kỳ các đối tượng web vào RAM và đĩa cứng của ISA server	Không	Có
VPN	Mở rộng mạng riêng nhờ sử dụng các đường liên kết qua các mạng được chia sẻ hay mạng công cộng như Internet	Có	Không
Lọc gói	Điều khiển dòng gói IP đi và đến	Có	Không
Lọc ứng dụng	Thực thi các tác vụ của hệ thống hoặc của giao thức chỉ định, như là nhận thực để cung cấp một lớp bảo vệ bổ sung cho dịch vụ firewall	Có	Không
Quảng bá Web	Quảng bá web trong mạng để người dùng trong mạng có thể truy cập	Không	Có
Quảng bá Server	Cho phép các Server ứng dụng có thể phục vụ các client bên ngoài	Có	Không
Giám sát thời gian thực	Cho phép giám sát tập trung các hoạt động của ISA server bao gồm các cảnh báo, giám sát các phiên làm việc và các dịch vụ		

Có Có
Cảnh báo Báo cho ta biết các sự kiện đặc biệt
xuất hiện và thực thi các hoạt độ_____ng
phù hợp
Có Có

Báo cáo Tổng hợp và phân tích hoạt động
trên một hoặc nhiều máy ISA server
Có Có

4. Bài tập thực hành.

Yêu cầu về Phòng học lý thuyết: Số lượng máy tính theo số lượng học viên trong lớp học đảm bảo mỗi học viên có một máy tính, cấu hình máy tối thiểu như sau (PIII 800 MHZ, 256 MB RAM, HDD 1GB,FDD, CDROM 52 x). Máy tính đã cài đặt Windows 2000 advance server. Các máy tính đã được nối mạng chạy giao thức TCP/IP.

Thiết bị thực hành: Đĩa cài phần mềm Windows 2000 Advance Server, đĩa cài phần mềm ISA Server 2000. Mỗi máy tính có 01 Modem V.90 và 01 đường điện thoại. 01 account truy cập internet

Bài 1: Các bước cài đặt cơ bản phần mềm ISA server 2000.

Bước 1: Các bước cài đặt cơ bản.

 Đăng nhập vào hệ thống với quyền Administrator
 Đưa đĩa cài đặt Microsoft Internet Security and Acceleration Server 2000 Enterprise Edition vào ổ CD-ROM.
 Cửa sổ Microsoft ISA Server Setup mở ra. Nếu cửa sổ này không tự động xuất hiện, sử dụngWindows Explorer để chạy x:\ISAAutorun.exe (với x là tên ổ đĩa CD-ROM).
 Trong cửa sổ Microsoft ISA Server Setup, kích Install ISA Server.
 Trong hộp thoại Microsoft ISA Server (Enterprise Edition) Setup kích Continue.
 Vào CD Key sau đó kích OK hai lần.
 Trong hộp thoại Microsoft ISA Server Setup kích I Agree.
 Trong hộp thoại Microsoft ISA Server (Enterprise Edition) Setup kích Custom Installation.
 Trong hộp thoại Microsoft ISA Server (Enterprise Edition) – Custom Installation kích Add-in services sau đó kích Change Option.
 Trong hộp thoại Microsoft ISA Server (Enterprise Edition) – Add-in services kiểm tra lựa chọn Install H.323 Gatekeeper Service đã được chọn, chọn Message Screener sau đó kích OK.
 Trong hộp thoại Microsoft ISA Server (Enterprise Edition) – CustomInstallation kích Administration tools sau đó kích Change Option.
 Trong hộp thoại Microsoft ISA Server (Enterprise Edition) – Administration tools, kiểm tra lựa chọn ISA Management đã được chọn, chọn H.323 Gatekeeper Administration Tools sau đó kíchOK.

 Trong hộp thoại Microsoft ISA Server (Enterprise Edition) – Custom Installation kích Continue. Hộp thoại Microsoft Internet Security and Acceleration Server Setup xuất hiện, lưu ý bạn rằng máy tính không thể tham gia vào array. Bạn sẽ cấu hình máy tính này là một stand-alone server.
 Kích Yes để cấu hình máy tính này là một stand-alone server.
 Trong hộp thoại Microsoft ISA Server Setup đọc mô tả các mode cài đặt

đảm bảo rằng mode Integrated đã được lựa chọn sau đó kích Continue.
 Trong hộp thoại Microsoft Internet Security and Acceleration Server Setup đọc thông báo về IIS publishing sau đó kích OK để biết rằng ISA Server Setup đang dừng dịch vụ IIS publishing.
 Kích OK và đặt ngầm định các giá trị thiết đặt cho cache.
Bước 2: Cấu hình LAT để khai báo địa chỉ cho mạng riêng.
 Trong hộp thoại Microsoft Internet Security and Acceleration Server 2000 Setup kích Construct Table. Lưu ý rằng khi bạn thêm vào không đúng địa chỉ IP vào LAT, ISA server sẽ chuyển tiếp sai các gói tin do đó các máy client sẽ không thể truy cập Internet
 Trong hộp thoại Local Address Table, kích để xóa Add the following private ranges: 10.x.x.x, 192.168.x.x and 172.16.x.x-172.31.x.x
 Chọn adapter ip_address (với tên cạc mạng và địa chỉ IP là địa chỉ mạng riêng), sau đó kích OK.
 Trong thông báo Setup Message, kích OK.
 Trong Internal IP Ranges, kích 10.255.255.255-10.255.255.255, sau đó kích Remove.
 Kiểm tra rằng Internal IP Ranges chỉ chứa IP addresses trong mạng trong của bạn sau đó kích OK.
 Kết thúc việc cài đặt ISA Server và khởi tạo cấu hình ISA Server.
 Trong hộp thoại Launch ISA Management Tool, kích để xóa
 Start ISA Server Getting Started Wizard check box, sau đó kích OK.
 Trong hộp thông báo Microsoft ISA Server (Enterprise Edition) Setup kích OK.
 Đóng cửa sổ Microsoft ISA Server Setup.
 Lấy đĩa Microsoft Internet Security and Acceleration Server Enterprise Edition từ ổ đĩa CD-ROM.
Bước 3: Cấu hình Default Web Site trong Internet Information Services sử dụng cổng 8008, sau đó khởi động Default Web Site.
 Mở Internet Services Manager từ Administrative Tools.
 Trong Internet Information Services, mở rộng server(server là tên máy tính của bạn), sau đó kích DefaultWeb Site (Stopped).

 Kích chuột phải Default Web Site (Stopped), sau đó kích Properties. Vì ISA Server sử dụng các cổng 80 and 8080, bạn phải cấu hình IIS để phục vụ các kết nối từ các client tới trên cổng khác. Bạn sẽ cấu hình IIS để phục cụ các yêu cầu này trên cổng TCP 8008.
 Trong hộp thoại Default Web Site (Stopped) Properties, trong hộp TCP Port, gõ 8008 sau đó kích OK.
 Kích chuột phải Default Web Site (Stopped), sau đó kích Start.
Bài 2: Cấu hình ISA Server 2000 cho phép một mạng nội bộ có thể truy cập, sử dụng các dịch vụ cơ bản trên Internet qua 01 modem kết nối qua mạng PSTN.
Bước 1: Cấu hình và quản trị cấu hình cho ISA server sử dụng Getting Started Với Getting Started Wizard, có các lựa chọn cấu hình sau:
 Select Policy elements, cấu hình ngầm định chọn tất cả các thành phần để có thể sử dụng khi tạo các qui tắc.
 Configure Schedules, cấu hình ngầm định có hai lịch là Weekends và Work Hours, ta có thể sửa các lịch này hoặc tạo các lịch mới.
 Configure Client sets, các máy tính Client có thể tạo thành nhóm với nhau bằng các địa chỉ IP sử dụng cho mục đích tạo các qui tắc ứng với từng nhóm

client
 Configure Protocol Rule, đưa ra các qui tắc giao thức để các client sử dụng truy nhập Internet

 Configure Destination Sets, cho phép thiết lập các máy tính trên mạng Internet thành nhóm bởi tên hay địa chỉ IP, Destination Sets được sử dụng để tạo ra các qui tắc, áp dụng các qui tắc cho một hay nhiều Destination Sets
 Configure Site and Content Rules, cấu hình các qui tắc về nội dung.
 Secure Server cho phép bạn có thể đặt các mức độ bảo vệ thích hợp cho mạng.
 Configure Filewall Protection, Packet Fitering bảo đảm cho ISA server sẽ lọc không có packet nào qua trừ khi được phép
 Cofigure Dial-Up Entries, cho phép chọn giao diện để kết nối với Internet
 Configure Routing for filewall and secureNat client.
 Configure Routing for Web browser Appilications cho phép tạo các qui tắc định tuyến, xác định rõ yêu cầu từ Web Proxy Client được gửi trực tiếp tới Internet hay tới Upstream server
 Configure Cache policy, cấu hình các chính sách về cache.

Bước 2: Cấu hình ISA server cho phép các client sử dụng được các dịch vụ của Internet qua mạng thoại công cộng
 Tạo một Dial-Up Entries, để kết nối với InternetBước 2: Tạo một qui tắc giao thức.
 Mở ISA Management, kích Servers and arrays, sau đó kích tên máy chủ ISA.
 Kích Access Policy, kích chuột phải vào Protocol Rule, sau đó chọn New --> Rule.
 Đặt tên của Protocol Rule, sau đó kích Next.
 Kiểm tra rằng **Allow đã được chọn**, kích Next, sau đó chọn **All IP traffic**, kích Next Chọn **Always**, kích Next sau đó chọn **Any Request**, kích Next, sau đó kích Finish.

Bước 3: Cấu hình Web Proxy Client: cấu hình Internet Explorer để sử dụng ISA server đối với các yêu cầu truy cập dịch vụ Web.
 Mở trình duyệt Internet Explorer.
 Trong Internet Connection Wizard, kích Cancel.
 Trong hộp thoại Internet Connection Wizard, chọn Do not show the Internet Connection wizard in the future, sau đó kích Yes.
 Trong Internet Explorer, trong ô Address , gõ http://vdc.com.vn sau đó chọn ENTER. Internet Explorer không thể kết nối tới trang web này.
 Trong menu Tools, kích Internet Options.
 Trong hộp thoại Internet Options, trong Connections kích LAN Settings.
 Trong hộp thoại Local Area Network (LAN) Settings , kích để bỏ lựa chọn Automatically detect settings. Chọn Use a proxy server, trong ô Address gõ vào địa chỉ IP của ISA Server .
 Trong hộp Port, gõ 8080

 Kiểm tra rằng lựa chọn Bypass proxy server for local addresses đã bỏ, sau đó kích OK hai lần.

Bài 3: Thiết đặt các chính sách cho các yêu cầu truy cập và sử dụng các dịch vụ trên mạng internet.

I.Thiết lập các thành phần chính sách

Bước 1: Thiết lập lịch trình

 Đăng nhập vào hệ thống với quyền administrator
 Mở ISA Management từ thực đơn Microsoft ISA Server.
 Trong ISA Management, mở rộng Servers and Arrays, mở rộng server (server là tên của ISA Server), mở rộng Policy Elements, sau đó kích Schedules.
 Kích Create a Schedule để thiết lập một lịch trình.
 Trong hộp thoại New schedule trong mục Name đưa vào một tên lịch trình ví dụ schedule1.
 Trong mục Description gõ vào Daily period of most network utilization
 Kéo để lựa chọn toàn bộ lịch trình sau đó kích Inactive.
 Kéo để lựa chọn vùng từ thời điểm hiện tại tới 2 h tiếp theo đối với tất cả các ngày trong tuần sau đó kích active ví dụ, nếu thời điểm hiện tại là 3:15 P.M., thì lựa chọn vùng từ 3:00 P.M. tới 5:00 P.M. cho tất cả các ngày trong tuần.
 Kích OK.

Bước 2: Thiết lập destination set

 Trong ISA Management, kích Destination Sets.
 Kích Create a Destination Set.
 Trong hộp thoại New Destination Set trong mục Name cho vào một tên cho thiết lập mới này ví dụ set1.
 Trong mục Description box, gõ vào một nội dung mô tả cho thiết lập mới này
 Kích Add.
 Trong hộp thoại Add/Edit Destination trong mục Destination gõ home.vnn.vn

Bước 3: Thiết lập client address set

 Trong ISA Management kích Client Address Sets.
 Kích Create a Client Set.
 Trong hộp thoại Client Set trong mục Name gõ vào một tên cho thiết lập mới, ví dụ Accounting Department.
 Trong mục Description gõ nội dung mô tả cho thiết lập mới này sau đó kích Add.

 Trong hộp thoại Add/Edit IP Addresses trong mục From gõ vào địa chỉ bắt đầu thuộc nhóm địa chỉ thuộc mạng dùng riêng .
 Trong mục To gõ vào địa chỉ kết thúc thuộc nhóm địa chỉ thuộc mạng dùng riêng kích OK hai lần.

Bước 4: Thiết lập protocol definition (sử dụng cổng UDP 39000 cho kết nối chính gọi ra và cổng TCP 39000 cho kết nối thứ hai)

 Trong ISA Management kích Protocol Definitions.
 Kích Create a Protocol Definition.
 Trong New Protocol Definition Wizard trong mục Protocol definition
 name gõ vào một tên cho thiết đặt mới sau đó kích Next.
 Trong trang Primary Connection Information trong mục Port number
 gõ vào 39000
 Trong danh sách Protocol type kích UDP.
 Trong danh sách Direction kích Send Receive sau đó kích Next.
 Trong trang Secondary Connections kích Yes sau đó kích New.
 Trong hộp thoại New/Edit Secondary Connection trong mục From và mục To gõ 39000
 Trong danh sách Protocol type kiểm tra rằng TCP đã được lựa chọn, trong

mục Direction
 kích Outbound sau đó kích OK.
 Kích Next sau đó trong trang Completing the New Protocol Definition
 Wizard kích Finish.

II.Thiết lập các qui tắc giao thức

Bước 1: Thiết lập một qui tắc giao thức cho phép HTTP, HTTP-S và FTP đối với mọi người dùng truy cập Internet tại mọi thời điểm bằng việc sử dụng các giao thức HTTP, HTTP-S và FTP .

 Mở trình duyệt Internet Explorer tại một máy trạm, trong ô Address gõ http://home.vnn.vn nhấn ENTER. Trình duyệt Internet Explorerkhông thể kết nối tới Web site vì ISA Server từ chối yêu cầu.
 Đóng Internet Explorer.
 Trong ISA Management mở rộng Access Policy sau đó kích Protocol Rules.
 Kích Create a Protocol Rule for Internet Access.
 Trong New Protocol Rule Wizard, trong mục Protocol rule name gõ Allow HTTP, HTTP-S, and FTP sau đó kích Next.
 Trong trang Protocols kiểm tra rằng Selected protocols đã được chọn, kích để xóa Gopher check box sau đó kích Next.
 Trong trang Schedule kiểm tra rằng Always đã được lựa chọn sau đó kích Next.

 Trong trang Client Type kiểm tra rằng Any request đã được chọn, sau đó kích Next.
 Trong trang Completing the New Protocol Rule Wizard kích Finish.
 Mở Internet Explorer tại một máy tính trạm, trong mục Address gõ http://home.vnn.vn sao đó ấn ENTER. Kiểm tra rằng trình duyệt kết nối thành công nội dung trang web được hiển thị
 Đóng Internet Explorer.

Bước 2: Thiết lập một qui tắc giao thức cho phép người dùng trong nhóm Domain Admins truy cập Internet sử dụng tất cả các giao thức.

 Trong ISA Management kích Create a Protocol Rule.
 Trong New Protocol Rule Wizard, trong mục Protocol rule name gõ Allow All Access for Administrators sau đó kích Next.
 Trong trang Rule Action kiểm tra rằng Allow đã được chọn sau đó kích Next.
 Trong trang Protocols, trong danh sách Apply this rule to kiểm tra rằng All IP traffic đã được chọn sau đó kích Next.
 Trong trang Schedule, kiểm tra rằng Always đã được chọn sau đó kích Next.
 Trong trang Client Type, kích Specific users and groups, sau đó kích Next.
 Trong trang Users and Groups, kích Add.
 Trong hộp thoại Select Users or Groups, kích Domain Admins, kích Add, sau đó kích OK.
 Trong trang Users and Groups, kích Next.
 Trong trang Completing the New Protocol Rule Wizard kích Finish.

Bước 3: Thiết lập một qui tắc giao thức từ chối người dùng trong nhóm Accounting Department đã định nghĩa trong client set truy cập Internet.

 Trong ISA Management, kích Create a Protocol Rule.
 Trong New Protocol Rule Wizard, trong mục Protocol rule name gõ vào Deny Access from Accounting Department , sau đó kích Next.
 Trong trang Rule Action, kích Deny, sau đó kích Next.

 Trong trang Protocols, trong danh sách Apply this rule to, kiểm tra rằng All IP traffic đã được lựa chọn, sau đó kích Next.
 Trong trang Schedule, kiểm tra rằng Always đã được lựa chọn, sau đó kích Next.
 Trong trang Client Type, kích Specific computers (client address
 sets), sau đó kích Next.
 Trong trang Client Sets, kích Add.

 Trong hộp thoại Add Client Sets, kích Accounting Department, kích Add, sau đó kíchOK.
 Trong trang Client Sets, kích Next.
 Trong trang Completing the New Protocol Rule Wizard, kích Finish.
 Kiểm tra để xác nhận việc truy cập không thành công từ nhóm nhóm Accounting Department

Bước 4: Xóa qui tắc giao thức từ chối người dùng trong nhóm Accounting Department

 Trong In ISA Management, kích Deny Access from Accounting Department
 Kích Delete a Protocol Rule.
 Trong hộp thoại Confirm Delete, kích Yes.

III.Thiết lập các qui tắc nội dung

Bước 1: Thiết lập một qui tắc nội dung để từ chối truy cập tới nội dung đã được định nghĩa trong destination set và với lịch trình đã thiết lập ở mục 1

 Trong ISA Management, kích Site and Content Rules.
 Kích Create a Site and Content Rule.
 Trong New Site and Content Rule Wizard, trong mục Site and content rule
 name, gõ vào một tên ví dụ Deny Access Rule sau đó kích Next.
 Trong trang Rule Action, kiểm tra rằng Deny đã được chọn, sau đó kích Next.
 Trong trang Destination Sets, trong danh sách Apply this rule to, kích Specified destination set.
 Trong danh sách Name, lựa chọn set1 (đã thiết lập ở phần trên), sau đó kích Next.
 Trong trang Schedule, chọn schedule1 (đã thiết lập ở phần trên), sau đó kích Next.
 Trong trang Client Type, kiểm tra rằng Any request đã được chọn, sau đó kích Next.
 Trong trang Completing the New Site and Content Rule Wizard, kích Finish.

Bước 2:

Kiểm tra qui tắc vừa thiết lập

 Mở trình duyệt Internet Explorer.
 Trong ô Address, gõ http://home.vnn.vn sau đó ấn ENTER. kiểm tra rằng trang web này không được hiển thị, vì qui tắc nội dung đã thiết lập ở trên đã có hiệu lực
 Đóng trình duyệt Internet Explorer.

Chương 6 - Bảo mật hệ thống và Firewall

Chương 6 tập trung vào các nội dung quan trọng về bảo mật hệ thống và

mạng lưới. Nội dung của phần thứ nhất chương 6 cung cấp cho các học viên khái niệm về các hình thức tấn công mạng, các lỗ hổng, điểm yếu của mạng lưới. Các kỹ năng cơ bản trong phần một của chương 6 giúp người quản trị quản lý và xây dựng các chính sách bảo mật tương ứng cho các thành phần mạng, hệ thống hay dịch vụ ngay từ lúc bắt đầu hoạt động.
Phần 2 của chương 6 tập trung giới thiệu về thiết bị bảo mật mạnh và thông dụng trên mạng. Đó là thiết bị bức tường lửa (firewall). Học viên sẽ có được các kiến thức về cấu trúc firewall, các chức năng cơ bản và cách phân loại cũng như ưu nhược điểm của các loại firewall hoạt động theo các nguyên lý khác nhau. Những kỹ năng thiết lập cấu hình, luật, quản trị firewall với mô hình firewall checkpoint sẽ giúp cho các học viên hiểu cụ thể và các công việc quản trị và bảo mật hệ thống mạng
Chương 6 yêu cầu các học viên trang bị rất nhiều các kiến thức cơ bản như nắm vững các kiến thức quản trị hệ thống OS windows, linux, unix. Học viên cần hiểu sâu về giao thức TCP/IP, hoạt động của IP hay UDP, TCP. Học viên cần có hiểu biết về các port, socket của các giao thức dịch vụ như SMTP, POP3, WWW...Các kiến thức được trang bị trong các giáo trình quản trị hệ thống hoặc các tài liệu, sách giáo khoa về nội dung trên học viên nên tham khảo trước khi học chương 6 này.

1. Bảo mật hệ thống

1.1. Các vấn đề chung về bảo mật hệ thống và mạng

Do đặc điểm của một hệ thống mạng là có nhiều người sử dụng và phân tán về mặt địa lý nên việc bảo vệ các tài nguyên (mất mát, hoặc sử dụng không hợp lệ) trong môi trường mạng phức tạp hơn nhiều so với môi trường một máy tính đơn lẻ, hoặc một người sử dụng.
Hoạt động của người quản trị hệ thống mạng phải đảm bảo các thông tin trên mạng là tin cậy và sử dụng đúng mục đích, đối tượng đồng thời đảm bảo mạng hoạt động ổn định, không bị tấn công bởi những kẻ phá hoại.
Có một thực tế là không một hệ thống mạng nào đảm bảo là an toàn tuyệt đối, một hệ thống dù được bảo vệ chắc chắn đến mức nào thì cũng có lúc bị vô hiệu hoá bởi những kẻ có ý đồ xấu.

1.1.1. Một số khái niệm và lịch sử bảo mật hệ thống

Trước khi tìm hiểu các vấn đề liên quan đến phương thức phá hoại và các biện pháp bảo vệ cũng như thiết lập các chính sách về bảo mật, ta sẽ tìm hiểu một số khái niệm liên quan đến bảo mật thông tin trên mạng Internet.

1.1.1.1. Một số khái niệm
a) Đối tượng tấn công mạng (Intruder):
Là những cá nhân hoặc các tổ chức sử dụng các kiến thức về mạng và các công cụ phá hoại (phần mềm hoặc phần cứng) để dò tìm các điểm yếu, lỗ hổng bảo mật trên hệ thống, thực hiện các hoạt động xâm nhập và chiếm đoạt tài nguyên mạng trái phép.
Một số đối tượng tấn công mạng là:
- Hacker: Là những kẻ xâm nhập vào mạng trái phép bằng cách sử dụng các công cụ phá mật khẩu hoặc khai thác các điểm yếu của các thành phần truy nhập trên hệ thống.
- Masquerader: Là những kẻ giả mạo thông tin trên mạng. Có một số hình thức như giả mạo địa chỉ IP, tên miền, định danh người dùng ...
- Eavesdropping: Là những đối tượng nghe trộm thông tin trên mạng, sử dụng các công cụ sniffer; sau đó dùng các công cụ phân tích và debug để lấy được các thông tin có giá trị.

Những đối tượng tấn công mạng có thể nhằm nhiều mục đích khác nhau như: ăn cắp những thông tin có giá trị về kinh tế, phá hoại hệ thống mạng có chủ định, hoặc cũng có thể chỉ là những hành động vô ý thức, thử nghiệm các chương trình không kiểm tra cẩn thận ...

b) Các lỗ hổng bảo mật:

Các lỗ hổng bảo mật là những điểm yếu trên hệ thống hoặc ẩn chứa trong một dịch vụ mà dựa vào đó kẻ tấn công có thể xâm nhập trái phép để thực hiện các hành động phá hoại hoặc chiếm đoạt tài nguyên bất hợp pháp. Nguyên nhân gây ra những lỗ hổng bảo mật là khác nhau: có thể do lỗi của bản thân hệ thống, hoặc phần mềm cung cấp, hoặc do người quản trị yếu kém không hiểu sâu sắc các dịch vụ cung cấp ...

Mức độ ảnh hưởng của các lỗ hổng là khác nhau. Có những lỗ hổng chỉ ảnh hưởng tới chất lượng dịch vụ cung cấp, có những lỗ hổng ảnh hưởng nghiêm trọng tới toàn bộ hệ thống ...

c) Chính sách bảo mật:

Là tập hợp các qui tắc áp dụng cho mọi đối tượng có tham gia quản lý và sử dụng các tài nguyên và dịch vụ mạng.

Mục tiêu của chính sách bảo mật giúp người sử dụng biết được trách nhiệm của mình trong việc bảo vệ các tài nguyên thông tin trên mạng , đồng thời giúp các nhà quản trị thiết lập các biện pháp bảo đảm hữu hiệu trong quá trình trang bị, cấu hình, kiểm soát hoạt động của hệ thống và mạng

Một chính sách bảo mật được coi là hoàn hảo nếu nó xây dựng gồm các văn bản pháp qui, kèm theo các công cụ bảo mật hữu hiệu và nhanh chóng giúp người quản trị phát hiện, ngăn chặn các xâm nhập trái phép.

1.1.1.2. Lịch sử bảo mật hệ thống

Có một số sự kiện đánh dấu các hoạt động phá hoại trên mạng, từ đó nảy sinh các yêu cầu về bảo mật hệ thống như sau:

- Năm 1988: Trên mạng Internet xuất hiện một chương trình tự nhân phiên bản của chính nó lên tất cả các máy trên mạng Internet. Các chương trình này gọi là "sâu". Tuy mức độ nguy hại của nó không lớn, nhưng nó đặt ra các vấn đề đối với nhà quản trị về quyền truy nhập hệ thống, cũng như các lỗi phần mềm.
- Năm 1990: Các hình thức truyền Virus qua địa chỉ Email xuất hiện phổ biến trên mạng Internet.
- Năm 1991: Phát hiện các chương trình trojans.

Cùng thời gian này sự phát triển của dịch vụ Web và các công nghệ liên quan như Java, Javascipts đã có rất nhiều các thông báo lỗi về bảo mật liên quan như: các lỗ hổng cho phép đọc nội dung các file dữ liệu của người dùng, một số lỗ hổng cho phép tấn công bằng hình thức DoS, spam mail làm ngưng trệ dịch vụ.

- Năm 1998: Virus Melisa lan truyền trên mạng Internet thông qua các chương trình gửi mail của Microsoft, gây những thiết hại kinh tế không nhỏ.
- Năm 2000: Một loạt các Web Site lớn như yahoo.com và ebay.com bị tê liệt, ngừng cung cấp dịch vụ trong nhiều giờ do bị tấn công bởi hình thức DoS.

1.1.2. Các lỗ hổng và phương thức tấn công mạng chủ yếu

1.1.2.1. Các lỗ hổng

Như phần trên đã trình bày, các lỗ hổng bảo mật trên một hệ thống là các điểm yếu có thể tạo ra sự ngưng trệ của dịch vụ, thêm quyền đối với người sử dụng hoặc cho phép các truy nhập không hợp pháp vào hệ thống. Các lỗ

hổng cũng có thể nằm ngay các dịch vụ cung cấp như sendmail, web, ftp ... Ngoài ra các lỗ hổng còn tồn tại ngay chính tại hệ điều hành như trong Windows NT, Windows 95, UNIX hoặc trong các ứng dụng mà người sử dụng thường xuyên sử dụng như word processing, các hệ databases...

Có nhiều tổ chức khác nhau tiến hành phân loại các dạng lỗ hổng đặc biêt. Theo cách phân loại của Bộ quốc phòng Mỹ, các loại lỗ hổng bảo mật trên một hệ thống được chia như sau:

- Lỗ hổng loại C: các lỗ hổng loại này cho phép thực hiện các phương thức tấn công theo DoS (Denial of Services - Từ chối dịch vụ). Mức độ nguy hiểm thấp, chỉ ảnh hưởng tới chất lượng dịch vụ, có thể làm ngưng trệ, gián đoạn hệ thống; không làm phá hỏng dữ liệu hoặc đạt được quyền truy nhập bất hợp pháp.
- Lỗ hổng loại B: Các lỗ hổng cho phép người sử dụng có thêm các quyền trên hệ thống mà không cần thực hiện kiểm tra tính hợp lệ nên có thể dẫn đến mất mát hoặc lộ thông tin yêu cầu bảo mật. Mức độ nguy hiểm trung bình. Những lỗ hổng này thường có trong các ứng dụng trên hệ thống.

- Lỗ hổng loại A: Các lỗ hổng này cho phép người sử dụng ở ngoài cho thể truy nhập vào hệ thống bất hợp pháp. Lỗ hổng này rất nguy hiểm, có thể làm phá hủy toàn bộ hệ thống.

Hình sau minh họa các mức độ nguy hiểm và loại lỗ hổng tương ứng:

Hình 6.1: Các loại lỗ hổng bảo mật và mức độ nguy hiểm

Sau đây ta sẽ phân tích một số lỗ hổng bảo mật thường xuất hiện trên mạng và hệ thống.

a) Các lỗ hổng loại C

Các lỗ hổng loại này cho phép thực hiện các cuộc tấn công DoS.

DoS là hình thức tấn công sử dụng các giao thức ở tầng Internet trong bộ giao thức TCP/IP để làm hệ thống ngưng trệ dẫn đến tình trạng từ chối người sử dụng hợp pháp truy nhập hay sử dụng hệ thống. Một số lượng lớn các gói tin được gửi tới server trong khoảng thời gian liên tục làm cho hệ thống trở nên quá tải, kết quả là server đáp ứng chậm hoặc không thể đáp ứng các yêu cầu từ client gửi tới.

Các dịch vụ có lỗ hổng cho phép thực hiện các cuộc tấn công DoS có thể được nâng cấp hoặc sửa chữa bằng các phiên bản mới hơn của các nhà cung cấp dịch vụ. Hiện nay, chưa có một giải pháp toàn diện nào để khắc phục các lỗ

hổng loại này vì bản thân việc thiết kế giao thức ở tầng Internet (IP) nói riêng và bộ giao thức TCP/IP đã chứa đựng những nguy cơ tiềm tàng của các lỗ hổng này.

Ví dụ điển hình của phương thức tấn công DoS là các cuộc tấn công vào một số Web Site lớn làm ngưng trệ hoạt động của web site này như: www.ebay.com và www.yahoo.com.

Tuy nhiên, mức độ nguy hiểm của các lỗ hổng loại này được xếp loại C, ít nguy hiểm vì chúng chỉ làm gián đoạn sự cung cấp dịch vụ của hệ thống trong một thời gian mà không làm nguy hại đến dữ liệu và những kẻ tấn công cũng không đạt được quyền truy nhập bất hợp pháp vào hệ thống.

Một lỗ hổng loại C khác cũng thường thấy đó là các điểm yếu của dịch vụ cho phép thực hiện tấn công làm ngưng trệ hệ thống của người sử dụng cuối. Chủ yếu hình thức tấn công này là sử dụng dịch vụ Web. Giả sử trên một Web Server có những trang Web trong đó có chứa các đoạn mã Java hoặc

JavaScripts, làm "treo" hệ thống của người sử dụng trình duyệt Web của Netscape bằng các bước sau:
- Viết các đoạn mã để nhận biết được Web Browers sử dụng Netscape.
- Nếu sử dụng Netscape, sẽ tạo một vòng lặp vô thời hạn, sinh ra vô số các cửa sổ, trong mỗi cửa sổ đó nối đến các Web Server khác nhau.

Với một hình thức tấn công đơn giản này, có thể làm treo hệ thống trong khoảng thời gian 40 giây (đối với máy client có 64 MB RAM). Đây cùng là một hình thức tấn công kiểu DoS. Người sử dụng trong trường hợp này chỉ có thể khởi động lại hệ thống.

Một lỗ hổng loại C khác cũng thường gặp đối với các hệ thống mail là không xây dựng các cơ chế anti-relay (chống relay) cho phép thực hiện các hành động spam mail. Như chúng ta đã biết, cơ chế hoạt động của dịch vụ thư điện tử là lưu và chuyển tiếp. Một số hệ thống mail không có các xác thực khi người dùng gửi thư, dẫn đến tình trạng các đối tượng tấn công lợi dụng các máy chủ mail này để thực hiện spam mail. Spam mail là hành động nhằm làm tê liệt dịch vụ mail của hệ thống bằng cách gửi một số lượng lớn các message tới một địa chỉ không xác định, vì máy chủ mail luôn phải tốn năng lực đi tìm những địa chỉ không có thực dẫn đến tình trạng ngưng trệ dịch vụ. Các message có thể sinh ra từ các chương trình làm bom thư rất phổ biến trên mạng Internet.

b) Các lỗ hổng loại B:

Lỗ hổng loại này có mức độ nguy hiểm hơn lỗ hổng loại C, cho phép người sử dụng nội bộ có thể chiếm được quyền cao hơn hoặc truy nhập không hợp pháp.

Ví dụ trên hình 12, lỗ hổng loại B có thể có đối với một hệ thống UNIX mà file /etc/passwd để ở dạng plaintext; không sử dụng cơ chế che mật khẩu trong UNIX (sử dụng file /etc/shadow)

Những lỗ hổng loại này thường xuất hiện trong các dịch vụ trên hệ thống. Người sử dụng local được hiểu là người đã có quyền truy nhập vào hệ thống với một số quyền hạn nhất định.

Một loại các vấn đề về quyền sử dụng chương trình trên UNIX cũng thương gây nên các lỗ hổng loại B. Vì trên hệ thống UNIX một chương trình có thể được thực thi với 2 khả năng:
- Người chủ sở hữu chương trình đó kích hoạt chạy.
- Người mang quyền của người sở hữu file đó kích hoạt chạy.

Một dạng khác của lỗ hổng loại B xảy ra đối với các chương trình có mã nguồn viết bằng C. Những chương trình viết bằng C thường sử dụng một vùng đệm - một vùng trong bộ nhớ sử dụng để lưu dữ liệu trước khi xử lý. Những người lập trình thường sử dụng vùng đệm trong bộ nhớ trước khi gán một khoảng không gian bộ nhớ cho từng khối dữ liệu. Ví dụ, người sử dụng viết chương trình nhập trường tên người sử dụng, qui định trường này dài 20 ký tự. Do đó họ sẽ khai báo:

```
char first_name [20];
```

Khai báo này sẽ cho phép người sử dụng nhập vào tối đa 20 ký tự. Khi nhập dữ liệu, trước tiên dữ liệu được lưu ở vùng đệm; nếu người sử dụng nhập vào 35 ký tự sẽ xảy ra hiện tượng tràn vùng đệm và kết quả 15 ký tự dư thừa sẽ nằm ở một vị trí không kiểm soát được trong bộ nhớ. Đối với những kẻ tấn công, có thể lợi dụng lỗ hổng này để nhập vào những ký tự đặc biệt, để thực thi một số lệnh đặc biệt trên hệ thống. Thông thường, lỗ hổng này thường được lợi dụng bởi những người sử dụng trên hệ thống để đạt được quyền root không hợp lệ.

Việc kiểm soát chặt chẽ cấu hình hệ thống và các chương trình sẽ hạn chế được các lỗ hổng loại B.

c) Các lỗ hổng loại A:

Các lỗ hổng loại A có mức độ rất nguy hiểm, đe dọa tính toàn vẹn và bảo mật của hệ thống. Các lỗ hổng loại này thường xuất hiện ở những hệ thống quản trị yếu kém hoặc không kiểm soát được cấu hình mạng.

Một ví dụ thường thấy là trên nhiều hệ thống sử dụng Web Server là Apache, Đối với Web Server này thường cấu hình thư mục mặc định để chạy các script là cgi-bin; trong đó có một Scripts được viết sẵn để thử hoạt động của apache là test-cgi. Đối với các phiên bản cũ của Apache (trước version 1.1), có dòng sau trong file test-cgi:

echo QUERY_STRING = $QUERY_STRING

Biến môi trường QUERY_STRING do không được đặt trong có dấu " (quote) nên khi phía client thực hiện một yêu cầu trong đó chuỗi ký tự gửi đến gồm một số ký tự đặc biệt; ví dụ ký tự "*", web server sẽ trả về nội dung của toàn bộ thư mục hiện thời (là các thư mục chứa các script cgi). Người sử dụng có thể nhìn thấy toàn bộ nội dung các file trong thư mục hiện thời trên hệ thống server.

Một ví dụ khác cũng xảy ra tương tự đối với các Web server chạy trên hệ điều hành Novell: các web server này có một scripts là convert.bas, chạy scripts này cho phép đọc toàn bộ nội dung các files trên hệ thống.

Những lỗ hổng loại này hết sức nguy hiểm vì nó đã tồn tại sẵn có trên phần mềm sử dụng, người quản trị nếu không hiểu sâu về dịch vụ và phần mềm sử dụng sẽ có thể bỏ qua những điểm yếu này.

Đối với những hệ thống cũ, thường xuyên phải kiểm tra các thông báo của các nhóm tin về bảo mật trên mạng để phát hiện những lỗ hổng loại này.

Một loạt các chương trình phiên bản cũ thường sử dụng có những lỗ hổng loại A như: FTP, Gopher, Telnet, Sendmail, ARP, finger...

1.1.2.2. Một số phương thức tấn công mạng phổ biến

a) Scanner

Scanner là một chương trình tự động rà soát và phát hiện những điểm yếu về bảo mật trên một trạm làm việc cục bộ hoặc trên một trạm ở xa. Với chức năng này, một kẻ phá hoại sử dụng chương trình Scanner có thể phát hiện ra những lỗ hổng về bảo mật trên một server ở xa.

Các chương trình scanner thường có một cơ chế chung là rà soát và phát hiện những port TCP/UDP được sử dụng trên một hệ thống cần tấn công từ đó phát hiện những dịch vụ sử dụng trên hệ thống đó. Sau đó các chương trình scanner ghi lại những đáp ứng trên hệ thống ở xa tương ứng với các dịch vụ mà nó phát hiện ra. Dựa vào những thông tin này, những kẻ tấn công có thể tìm ra những điểm yếu trên hệ thống.

Những yếu tố để một chương trình Scanner có thể hoạt động như sau:

- Yêu cầu về thiết bị và hệ thống: Một chương trình Scanner có thể hoạt động được nếu môi trường đó có hỗ trợ TCP/IP (bất kể hệ thống là UNIX, máy tính tương thích với IBM, hoặc dòng máy Macintosh).
- Hệ thống đó phải kết nối vào mạng Internet.

Tuy nhiên không phải đơn giản để xây dựng một chương trình Scanner, những kẻ phá hoại cần có kiến thức sâu về TCP/IP, những kiến thức về lập trình C, PERL và một số ngôn ngữ lập trình shell. Ngoài ra người lập trình (hoặc người sử dụng) cần có kiễn thức là lập trình socket, phương thức hoạt động của các ứng dụng client/server.

Các chương trình Scanner có vai trò quan trọng trong một hệ thống bảo mật, vì chúng có khả năng phát hiện ra những điểm yếu kém trên một hệ thống mạng. Đối với người quản trị mạng những thông tin này là hết sức hữu ích và cần thiết; đối với những kẻ phá hoại những thông tin này sẽ hết sức nguy hiểm.

b) Password Cracker

Password cracker là một chương trình có khả năng giải mã một mật khẩu đã được mã hoá hoặc có thể vô hiệu hoá chức năng bảo vệ mật khẩu của một hệ thống.

Để hiểu cách thức hoạt động của các chương trình bẻ khoá, chúng ta cần hiểu cách thức mã hoá để tạo mật khẩu. Hầu hết việc mã hoá các mật khẩu được tạo ra từ một phương thức mã hoá. Các chương trình mã hoá sử dụng các thuật toán mã hoá để mã hoá mật khẩu.

Quá trình hoạt động của các chương trình bẻ khoá được minh hoạ trong hình sau:

Hình 6.2: Hoạt động của các chương trình bẻ khóa

Theo sơ đồ trên, một danh sách các từ được tạo ra và được mã hoá đối với từng từ. Sau mỗi lần mã hoá, chương trình sẽ so sánh với mật khẩu đã mã hoá cần phá. Nếu không thấy trùng hợp, quá trình lại quay lại. Phương thức bẻ khoá này gọi là bruce-force.

Yếu tố về thiết bị phần cứng: Trong hình trên máy tính thực hiện các chương trình phá khoá là một máy PC 66MHz hoặc cấu hình cao hơn. Trong thực tế yêu cầu các thiết bị phần cứng rất mạnh đối với những kẻ phá khoá chuyên nghiệp. Một phương thức khác có thể thay thế là thực hiện việc phá khoá trên một hệ thống phân tán; do vậy giảm bớt được các yêu cầu về thiết bị so với phương pháp làm tại một máy.

Nguyên tắc của một số chương trình phá khoá có thể khác nhau. Một vài chương trình tạo một một danh sách các từ giới hạn, áp dụng một số thuật toán mã hoá, từ kết quả so sánh với password đã mã hoá cần bẻ khoá để tạo ra một danh sách khác theo một lôgic của chương trình, cách này tuy không chuẩn tắc nhưng khá nhanh vì dựa vào nguyên tắc khi đặt mật khẩu người sử dụng thường tuân theo một số qui tắc để thuận tiện khi sử dụng.

Đến giai đoạn cuối cùng, nếu thấy phù hợp với mật khẩu đã được mã hoá, kẻ phá khoá sẽ có được mật khẩu dạng text thông thường. Trong hình trên, mật khẩu dạng text thông thường được ghi vào một file.

Để đánh giá khả năng thành công của các chương trình bẻ khoá ta có công thức sau:

$P = L \times R / S$

Trong đó:

P: Xác suất thành công

L: Thời gian sống của một mật khẩu

R: Tốc độ thử

S: Không gian mật khẩu = A_M (M là chiều dài mật khẩu)

Ví dụ, trên hệ thống UNIX người ta đã chứng minh được rằng nếu mật khẩu dài quá 8 ký tự thì xác suất phá khoá gần như = 0. Cụ thể như sau:

Nếu sử dụng khoảng 92 ký tự có thể đặt mật khẩu, không gian mật khẩu có thể có là $S = 92_8$

Với tốc độ thử là 1000 mật khẩu trong một giây có R = 1000/s

Thời gian sống của một mật khẩu là 1 năm
Ta có xác suất thành công là :
$P = 1x\ 365\ x\ 86400\ x\ 1000/92_8 = 1/1.000.000$
Như vậy việc dò mật khẩu là không thể vì sẽ mất khoảng 100 năm mới tìm ra mật khẩu chính xác.
Thông thường các chương trình phá khoá thường kết hợp một số thông tin khác trong quá trình dò mật khẩu như:
- Các thông tin trong tập tin /etc/passwd
- Một số từ điển
- Từ lặp và các từ liệt kê tuần tự, chuyển đổi cách phát âm của một từ ...
Biện pháp khắc phục đối với cách thức phá hoại này là cần xây dựng một chính sách bảo vệ mật khẩu đúng đắn.

c) Trojans

Dựa theo truyền thuyết cổ Hy lạp "Ngựa thành Trojan", trojans là một chương trình chạy không hợp lệ trên một hệ thống với vai trò như một chương trình hợp pháp. Những chương trình này thực hiện những chức năng mà người sử dụng hệ thống thường không mong muốn hoặc không hợp pháp. Thông thường, trojans có thể chạy được là do các chương trình hợp pháp đã bị thay đổi mã của nó bằng những mã bất hợp pháp.
Các chương trình virus là một loại điển hình của Trojans. Những chương trình virus che dấu các đoạn mã trong các chương trình sử dụng hợp

pháp. Khi những chương trình này được kích hoạt thì những đoạn mã ẩn dấu sẽ được thực thi để thực hiện một số chức năng mà người sử dụng không biết.
Một định nghĩa chuẩn tắc về các chương trình Trojans như sau: chương trình trojans là một chương trình thực hiện một công việc mà người sử dụng không biết trước, giống như ăn cấp mật khẩu hay copy file mà người sử dụng không nhận thức được.
Những tác giả của các chương trình trojan xây dựng một kết hoạch. Xét về khía cạnh bảo mật trên Internet, một chương trình trojan sẽ thực hiện một trong những công việc sau:
- Thực hiện một vài chức năng hoặc giúp người lập trình phát hiện những thông tin quan trọng hoặc thông tin cá nhân trên một hệ thống hoặc một vài thành phần của hệ thống đó
- Che dấu một vài chức năng hoặc giúp người lập trình phát hiện những thông tin quan trọng hoặc thông tin cá nhân trên một hệ thống hoặc một vài thành phần của hệ thống đó

Một vài chương trình trojan có thể thực hiện cả 2 chức năng này. Ngoài ra, một số chương trình trojans còn có thể phá huỷ hệ thống bằng cách phá hoại các thông tin trên ổ cứng (ví dụ trường hợp của virus Melisa lây lan qua đường thư điện tử).
Hiện nay với nhiều kỹ thuật mới, các chương trình trojan kiểu này dễ dàng bị phát hiện và không có khả năng phát huy tác dụng. Tuy nhiên trong UNIX việc phát triển các chương trình trojan vẫn hết sức phổ biến.
Các chương trình trojan có thể lây lan qua nhiều phương thức, hoạt động trên nhiều môi trường hệ điều hành khác nhau (từ Unix tới Windows, DOS). Đặc biệt trojans thường lây lan qua một số dịch vụ phổ biến như Mail, FTP... hoặc qua các tiện ích, chương trình miễn phí trên mạng Internet.
Việc đánh giá mức độ ảnh hưởng của các chương trình trojans hết sức khó khăn. Trong một vài trường hợp, nó chỉ đơn giản là ảnh hưởng đến các truy nhập của khách hàng như các chương trình trojans lấy được nội dung của

file passwd và gửi mail tới kẻ phá hoại. Cách thức sửa đơn giản nhất là thay thế toàn bộ nội dung của các chương trình đã bị ảnh hưởng bởi các đoạn mã trojans và thay thế các password của người sử dụng hệ thống.

Tuy nhiên với những trường hợp nghiêm trọng hơn, là những kẻ tán công tạo ra những lỗ hổng bảo mật thông qua các chương trình trojans. Ví dụ những kẻ tấn công lấy được quyền root trên hệ thống và lợi dụng nó để phá huỷ toàn bộ hoặc một phần của hệ thống. Chúng dùng quyền root để thay đổi logfile, cài đặt các chươ_____ng trình trojans khác mà người quản trị không thể phát hiện. Trong trường hợp này, mức độ ảnh hưởng là nghiêm trọng và người quản trị hệ thống đó chỉ còn cách là cài đặt lại toàn bộ hệ thống

d) Sniffer

Đối với bảo mật hệ thống sniffer được hiểu là các công cụ (có thể là phần cứng hoặc phần mềm) "bắt" các thông tin lưu chuyển trên mạng và từ các

thông tin "bắt" được đó để lấy được những thông tin có giá trị trao đổi trên mạng.

Hoạt động của sniffer cũng giống như các chương trình "bắt" các thông tin gõ từ bàn phím (key capture). Tuy nhiên các tiện ích key capture chỉ thực hiện trên một trạm làm việc cụ thể còn đối với sniffer có thể bắt được các thông tin trao đổi giữa nhiều trạm làm việc với nhau.

Các chương trình sniffer (sniffer mềm) hoặc các thiết bị sniffer (sniffer cứng) đều thực hiện bắt các gói tin ở tầng IP trở xuống (gồm IP datagram và Ethernet Packet). Do đó, có thể thực hiện sniffer đối với các giao thức khác nhau ở tầng mạng như TCP, UDP, IPX, ...

Mặt khác, giao thức ở tầng IP được định nghĩa công khai, và cấu trúc các trường header rõ ràng, nên việc giải mã các gói tin này không khó khăn.

Mục đích của các chương trình sniffer đó là thiết lập chế độ promiscuous (mode dùng chung) trên các card mạng ethernet - nơi các gói tin trao đổi trong mạng - từ đó "bắt" được thông tin.

Các thiết bị sniffer có thể bắt được toàn bộ thông tin trao đổi trên mạng là dựa vào nguyên tắc broadcast (quảng bá) các gọi tin trong mạng Ethernet. Trên hệ thống mạng không dùng hub, dữ liệu không chuyển đến một hướng mà được lưu chuyển theo mọi hướng. Ví dụ khi một trạm làm việc cần được gửi một thông báo đến một trạm làm việc khác trên cùng một segment mạng, một yêu cầu từ trạm đích được gửi tới tất cả các trạm làm việc trên mạng để xác định trạm nào là trạm cần nhận thông tin (trạm đích). Cho tới khi trạm nguồn nhận được thông báo chấp nhận từ trạm đích thì luồng dữ liệu sẽ được gửi đi. Theo đúng nguyên tắc, những trạm khác trên segment mạng sẽ bỏ qua các thông tin trao đổi giữa hai trạm nguồn và trạm đích xác định. Tuy nhiên, các trạm khác cũng không bị bắt buộc phải bỏ qua những thông tin này, do đó chúng vẫn có thể "nghe" được bằng cách thiết lập chế độ promiscous mode trên các card mạng của trạm đó. Sniffer sẽ thực hiện công việc này.

Một hệ thống sniffer có thể kết hợp cả các thiết bị phần cứng và phần mềm, trong đó hệ thống phần mềm với các chế độ debug thực hiện phân tích các gói tin "bắt" được trên mạng.

Hệ thống sniffer phải được đặt trong cùng một segment mạng (network block) cần nghe lén.

Hình sau minh hoạ vị trí đặt sniffer:

Hình 6.3: Các vị trí đặt sniffer trên 1 segment mạng

Phương thức tấn công mạng dựa vào các hệ thống sniffer là rất nguy hiểm vì nó được thực hiện ở các tầng rất thấp trong hệ thống mạng. Với việc thiết lập hệ thống sniffer cho phép lấy được toàn bộ các thông tin trao đổi trên mạng. Các thông tin đó có thể là:
- Các tài khoản và mật khẩu truy nhập
- Các thông tin nội bộ hoặc có giá trị cao...

Tuy nhiên việc thiết lập một hệ thống sniffer không phải đơn giản vì cần phải xâm nhập được vào hệ thống mạng đó và cài đặt các phần mềm sniffer. Đồng thời các chương trình sniffer cũng yêu cầu người sử dụng phải hiểu sâu về kiến trúc, các giao thức mạng.

Mặc khác, số lượng các thông tin trao đổi trên mạng rất lớn nên các dữ liệu do các chương trình sniffer sinh ra khá lớn. Thông thường, các chương trình sniffer có thể cấu hình để chỉ thu nhập từ 200 - 300 bytes trong một gói tin, vi thường những thông tin quan trọng như tên người dùng, mật khẩu nằm ở phần đầu gói tin.

Trong một số trường hợp quản trị mạng, để phân tích các thông tin lưu chuyển trên mạng, người quản trị cũng cần chủ động thiết lập các chương trình sniffer, với vai trò này sniffer có tác dụng tốt.

Việc phát hiện hệ thống bị sniffer không phải đơn giản, vì sniffer hoạt động ở tầng rất thấp, và không ảnh hưởng tới các ứng dụng cũng như các dịch vụ hệ thống đó cung cấp. Một số biện pháp sau chỉ có tác dụng kiểm tra hệ thống như:
- Kiểm tra các tiến trình đang thực hiện trên hệ thống (bằng lệnh ps trên Unix hoặc trình quản lý tài nguyên trong Windows NT). Qua đó kiểm tra các tiến trình lạ trên hệ thống; tài nguyên sử dụng, thời gian khởi tạo tiến trình... để phát hiện các chương trình sniffer.

- Sử dụng một vài tiện ích để phát hiện card mạng có chuyển sang chế đố promiscous hay không. Những tiện ích này giúp phát hiện hệ thống của bạn có đang chạy sniffer hay không.

Tuy nhiên việc xây dựng các biện pháp hạn chế sniffer cũng không quá khó khăn nếu ta tuân thủ các nguyên tắc về bảo mật như:
- Không cho người lạ truy nhập vào các thiết bị trên hệ thống
- Quản lý cấu hình hệ thống chặt chẽ
- Thiết lập các kết nối có tính bảo mật cao thông qua các cơ chế mã hoá.

1.1.3. Một số điểm yếu của hệ thống

1.1.3.1. Deamon fingerd

Một lỗ hổng của deamon fingerd là cơ hội để phương thức tấn công worm "sâu" trên Internet phát triển: đó là lỗi tràn vùng đệm trong các tiến trình fingerd (lỗi khi lập trình). Vùng đệm để lưu chuỗi ký tự nhập được giới hạn là 512 bytes. Tuy nhiên chương trình fingerd không thực hiện kiểm tra dữ liệu đầu vào khi lớn hơn 512 bytes. Kết quả là xảy ra hiện tượng tràn dữ liệu ở vùng đệm khi dữ liệu lớn hơn 512 bytes. Phần dữ liệu dư thừa chứa những đoạn mã để kích một script khác hoạt động; scripts này tiếp tục thực hiện finger tới một host khác. Kết quả là hình thành một mắt xích các "sâu" trên mạng Internet.

1.1.3.2. File hosts.equiv

Nếu một người sử dụng được xác định trong file host.equiv cũng với địa chỉ máy của người đó, thì người sử dụng đó được phép truy nhập từ xa vào hệ thống đã khai báo. Tuy nhiên có một lỗ hổng khi thực hiện chức năng này đó là nó cho phép người truy nhập từ xa có được quyền của bất cứ người nào khác trên hệ thống. Ví dụ, nếu trên máy A có một file /etc/host.equiv có dòng định

danh B julie, thì julie trên B có thể truy nhập vào hệ thống A và có bất được quyền của bất cứ người nào khác trên A. Đây là do lỗi của thủ tục ruserok() trong thư viện libc khi lập trình.

1.1.3.3. Thư mục /var/mail

Nếu thư mục /var/mail được set là với quyền được viết (writeable) đối với tất cả mọi người trên hệ thống, thì bất cứ ai có thể tạo file trong thư mục này. Sau đó tạo một file với tên của một người đã có trên hệ thống rồi link tới một file trên hệ thống, thì các thư tới người sử dụng có tên trùng với tên file link sẽ được gán thêm vào trong file mà nó link tới.

Ví dụ, một người sử dụng tạo link từ /var/mail/root tới /etc/passwd, sau đó gửi mail bằng tên một người mới tới root thì tên người sử dụng mới này sẽ được gán thêm vào trong file /etc/passwd; Do vậy thư mục /var/mail không bao giờ được set với quyền writeable.

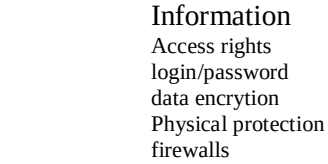
1.1.3.4. Chức năng proxy của FTPd

Chức năng proxy server của FTPd cho phép một người sử dụng có thể truyền file từ một ftpd này tới một ftpd server khác. Sử dụng chức năng này sẽ có thể bỏ qua được các xác thực dựa trên địa chỉ IP.

Nguyên nhân là do người sử dụng có thể yêu cầu một file trên ftp server gửi một file tới bất kỳ địa chỉ IP nào. Nên người sử dụng có thể yêu cầu ftp server đó gửi một file gồm các lệnh là PORT và PASV tới các server đang nghe trên các port TCP trên bất kỳ một host nào; kết quả là một trong các host đó có ftp server chạy và tin cậy người sử dụng đó nên bỏ qua được xác thực địa chỉ IP.

1.1.4. Các mức bảo vệ an toàn mạng

Vì không có một giải pháp an toàn tuyệt đối nên người ta thường phải sử dụng đồng thời nhiều mức bảo vệ khác nhau tạo thành nhiều lớp "rào chắn" đối với các hoạt động xâm phạm. Việc bảo vệ thông tin trên mạng chủ yếu là bảo vệ thông tin cất giữ trong các máy tính, đặc biệt là trong các server của mạng. Hình sau mô tả các lớp rào chắn thông dụng hiện nay để bảo vệ thông tin tại các trạm của mạng:



Hình 6.4: Các mức độ bảo vệ mạng

Như minh hoạ trong hình trên, các lớp bảo vệ thông tin trên mạng gồm:

- Lớp bảo vệ trong cùng là quyền truy nhập nhằm kiểm soát các tài nguyên (ở đây là thông tin) của mạng và quyền hạn (có thể thực hiện những thao tác gì) trên tài nguyên đó. Hiện nay việc kiểm soát ở mức này được áp dụng sâu nhất đối với tệp.
- Lớp bảo vệ tiếp theo là hạn chế theo tài khoản truy nhập gồm đăng ký tên và mật khẩu tương ứng. Đây là phương pháp bảo vệ phổ biến nhất vì nó đơn giản, ít tốn kém và cũng rất có hiệu quả. Mỗi người sử dụng muốn truy nhập được vào mạng sử dụng các tài nguyên đều phải có đăng ký tên và mật khẩu. Người quản trị hệ thống có trách nhiệm quản lý, kiểm soát mọi hoạt động

của mạng và xác định quyền truy nhập của những người sử dụng khác tuỳ theo thời gian và không gian.

- Lớp thứ ba là sử dụng các phương pháp mã hoá (encryption). Dữ liệu được biến đổi từ dạng clear text sang dạng mã hoá theo một thuật toán nào đó.
- Lớp thứ tư là bảo vệ vật lý (physical protection) nhằm ngăn cản các truy nhập vật lý bất hợp pháp vào hệ thống. Thường dùng các biện pháp truyền thống như ngăn cấm người không có nhiệm vụ vào phòng đặt máy, dùng hệ thống khoá trên máy tính, cài đặt các hệ thống báo động khi có truy nhập vào hệ thống ...
- Lớp thứ năm: Cài đặt các hệ thống bức tường lửa (firewall), nhằm ngăn chặn các thâm nhập trái phép và cho phép lọc các gói tin mà ta không muốn gửi đi hoặc nhận vào vì một lý do nào đó.

1.2. Các biện pháp bảo vệ mạng máy tính

1.2.1. Kiểm soát hệ thống qua logfile

Một trong những biện pháp dò tìm các dấu vết hoạt động trên một hệ thống là dựa vào các công cụ ghi logfile. Các công cụ này thực hiện ghi lại nhật ký các phiên làm việc trên hệ thống. Nội dung chi tiết thông tin ghi lại phụ thuộc vào cấu hình người quản trị hệ thống. Ngoài việc rà soát theo dõi hoạt động, đối với nhiều hệ thống các thông tin trong logfile giúp người quản trị đánh giá được chất lượng, hiệu năng của mạng lưới.

1.2.1.1. Hệ thống logfile trong Unix

Trong Unix, các công cụ ghi log tạo ra logfile là các file dưới dạng text thông thường cho phép người sử dụng dùng những công cụ soạn thảo file text bất kỳ để có thể đọc được nội dung. Tuy nhiên, một số trường hợp logfile được ghi dưới dạng binary và chỉ có thể sử dụng một số tiện ích đặc biệt mới có thể đọc được thông tin.

a) Logfile lastlog:

Tiện ích này ghi lại những lần truy nhập gần đây đối với hệ thống. Các thông tin ghi lại gồm tên người truy nhập, thời điểm, địa chỉ truy nhập ... Các chương trình login sẽ đọc nội dung file lastlog, kiểm tra theo UID truy nhập vào hệ thống và sẽ thông báo lần truy nhập vào hệ thống gần đây nhất. Ví dụ như sau:

Last login: Fri Sep 15 2000 14:11:38
Sun Microsystems Inc. SunOS 5.7 Generic October 1998
No mail.
Sun Microsystems Inc. SunOS 5.7 Generic October 1998
/export/home/ptthanh

b) Logfile UTMP

Logfile này ghi lại thông tin về những người đang login vào hệ thống, thường nằm ở thư mục /etc/utmp. Để xem thông tin trong logfile có thể sử dụng các tiện ích như who, w, finger, rwho, users. Ví dụ nội dung của logfile dùng lệnh who như sau:

/export/home/vhai% who
root console Aug 10 08:45 (:0)
ptthanh pts/4 Sep 15 15:27 (203.162.0.87)
ptthanh pts/6 Sep 15 15:28 (203.162.0.87)
root pts/12 Sep 7 16:35 (:0.0)
root pts/13 Sep 7 11:35 (:0.0)
root pts/14 Sep 7 11:39 (:0.0)

c) Logfile WTMP

Logfile này ghi lại các thông tin về các hoạt động login và logout vào hệ thống. Nó có chức năng tương tự với logfile UTMP. Ngoài ra còn ghi lại các thông tin về các lần shutdown, reboot hệ thống, các phiên truy nhập hoặc ftp và thường nằm ở thư mục /var/adm/wtmp. Logfile này thường được xem bằng

lệnh "last". Ví dụ nội dung như sau:
```
/export/home/vhai% last | more
ptthanh pts/10 203.162.0.85 Mon Sep 18 08:44 still logged in
ptthanh pts/10 Sat Sep 16 16:52 - 16:52 (00:00)
vtoan pts/10 203.162.0.87 Fri Sep 15 15:30 - 16:52 (1+01:22)
vtoan pts/6 203.162.0.87 Fri Sep 15 15:28 still logged in
vtoan pts/4 Fri Sep 15 15:12 - 15:12 (00:00)
```
d) Tiện ích Syslog

Đây là một công cụ ghi logfile rất hữu ích, được sử dụng rất thông dụng trên các hệ thống UNIX. Tiện ích syslog giúp người quản trị hệ thống dễ dàng trong việc thực hiện ghi logfile đối với các dịch vụ khác nhau. Thông thường tiện ích syslog thường được chạy dưới dạng một daemon và được kích hoạt khi hệ thống khởi động. Daemon syslogd lấy thông tin từ một số nguồn sau:

- /dev/log: Nhận các messages từ các tiến trình hoạt động trên hệ thống
- /dev/klog: nhận messages từ kernel
- port 514: nhận các messages từ các máy khác qua port 514 UDP.

Khi syslogd nhận các messages từ các nguồn thông tin này nó sẽ thực hiện kiểm tra file cấu hình của dịch vụ là syslog.conf để tạo log file tương ứng. Có thể cấu hình file syslog.conf để tạo một message với nhiều dịch vụ khác nhau.

Ví dụ nội dung một file syslog.conf như sau:
```
# This file is processed by m4 so be careful to quote (`') names
# that match m4 reserved words. Also, within ifdef's, arguments
# containing commas must be quoted.
#
*.err;kern.notice;auth.notice /dev/console
*.err;kern.debug;daemon.notice;mail.crit /var/adm/messages
*.alert;kern.err;daemon.err operator
*.alert root
*.emerg *
# if a non-loghost machine chooses to have authentication messages
```
Trong nội dung file syslog.conf chỉ ra, đối với các message có dạng *.emerg (message có tính khẩn cấp) sẽ được thông báo tới tất cả người sử dụng trên hệ thống; Đối với các messages có dạng *.err, hoặc kern.debug và những hoạt động truy cập không hợp pháp sẽ được ghi log trong file /var/adm/messages.

Mặc định, các messages được ghi vào logfile /var/adm/messages.

e) Tiện ích sulog

Bất cứ khi nào người sử dụng dùng lệnh "su" để chuyển sang hoạt động hệ thống dưới quyền một user khác đều được ghi log thông qua tiện ích sulog. Những thông tin logfile này được ghi vào logfile /var/adm/sulog. Tiện ích này cho phép phát hiện các trường hợp dùng quyền root để có được quyền của một user nào khác trên hệ thống.

Ví dụ nội dung của logfile sulog như sau:
```
# more /var/adm/sulog
SU 01/04 13:34 + pts/1 ptthanh-root
SU 01/04 13:53 + pts/6 ptthanh-root
SU 01/04 14:19 + pts/6 ptthanh-root
SU 01/04 14:39 + pts/1 ptthanh-root
```
f) Tiện ích cron

Tiện ích cron sẽ ghi lại logfile của các hoạt động thực hiện bởi lệnh crontabs. Thông thường, logfile của các hoạt động cron lưu trong file /var/log/cron/log. Ngoài ra, có thể cấu hình syslog để ghi lại các logfile của

hoạt động cron.
Ví dụ nội dung của logfile cron như sau:

```
# more /var/log/cron/log
! *** cron started *** pid = 2367 Fri Aug 4 16:32:38 2000
> CMD: /export/home/mrtg/mrtg /export/home/mrtg/termcount.cfg
> ptthanh 2386 c Fri Aug 4 16:34:01 2000
< ptthanh 2386 c Fri Aug 4 16:34:02 2000
> CMD: /export/home/mrtg/getcount.pl
> ptthanh 2400 c Fri Aug 4 16:35:00 2000
< ptthanh 2400 c Fri Aug 4 16:35:10 2000
> CMD: /export/home/mrtg/mrtg /export/home/mrtg/termcount.cfg
```
g) Logfile của sendmail
Hoạt động ghi log của sendmail có thể được ghi qua tiện ích syslog.
Ngoài ra chương trình sendmail còn có lựa chọn "-L + level security" với mức độ bảo mật từ "debug" tới "crit" cho phép ghi lại logfile. Vì sendmail là một chương trình có nhiều bug, với nhiều lỗ hổng bảo mật nền người quản trị hệ thống thường xuyên nên ghi lại logfile đối với dịch vụ này.
h) Logfile của dịch vụ FTP
Hầu hết các daemon FTP hiện nay đều cho phép cấu hình để ghi lại logfile sử dụng dịch vụ FTP trên hệ thống đó. Hoạt động ghi logfile của dịch vụ FTP thường được sử dụng với lựa chọn "-l", cấu hình cụ thể trong file /etc/inetd.conf như sau:
```
# more /etc/inetd.conf
ftp stream tcp nowait root /etc/ftpd/in.ftpd in.ftpd –l
```
Sau đó cấu hình syslog.conf tương ứng với dịch vụ FTP; cụ thể như sau:
```
# Logfile FTP
daemon.info ftplogfile
```
Với lựa chọn này sẽ ghi lại nhiều thông tin quan trọng trong một phiên ftp như: thời điểm truy nhập, địa chỉ IP, dữ liệu get/put ... vào site FTP đó. Ví dụ nội dung logfile của một phiên ftp như sau:
```
Sun Jul 16 21:55:06 2000 12 nms 8304640 /export/home/ptthanh/PHSS_17926.depot b _ o r
ptthanh ftp 0 * c
Sun Jul 16 21:56:45 2000 96 nms 64624640 /export/home/ptthanh/PHSS_19345.depot b _ o
r ptthanh ftp 0 * c
Sun Jul 16 21:57:41 2000 4 nms 3379200 /export/home/ptthanh/PHSS_19423.depot b _ o r
ptthanh ftp 0 * c
Sun Jul 16 22:00:38 2000 174 nms 130396160 /export/home/ptthanh/PHSS_19987.depot b _
o r ptthanh ftp 0 * c
```

i) Logfile của dịch vụ Web:
Tùy thuộc vào Web server sử dụng sẽ có các phương thức và cấu hình ghi logfile của dịch vụ Web khác nhau. Hầu hết các web server thông dụng hiện nay đều hỗ trợ cơ chế ghi log. Ví dụ nội dung logfile của dịch vụ Web sử dụng Web server Netscape như sau:
```
202.167.123.170 - - [03/Aug/2000:10:59:43 +0700] "GET /support/cgi-bin/search.pl
HTTP/1.0" 401 223
203.162.46.67 - - [03/Sep/2000:22:50:52 +0700] "GET http://www.geocities.com/ HTTP/1.1"
401 223
203.162.0.85 - - [15/Sep/2000:07:43:17 +0700] "GET /support/cgi-bin/search.pl HTTP/1.0"
401 223
203.162.0.85 - ptthanh [15/Sep/2000:07:43:22 +0700] "GET /support/cgi-bin/search.pl
HTTP/1.0" 404 207
```

203.162.0.85 - - [15/Sep/2000:07:43:17 +0700] "GET /support/cgi-bin/search.pl HTTP/1.0" 401 223

1.2.1.2. Một số công cụ hữu ích hỗ trợ phân tích logfile:

Đối với người quản trị, việc phân tích logfile của các dịch vụ là hết sức quan trọng. Một số công cụ trên mạng giúp người quản trị thực hiện công việc này dễ dàng hơn, đó là:

- Tiện ích chklastlog và chkwtmp giúp phân tích các logfile lastlog và WTMP theo yêu cầu người quản trị.
- Tiện ích netlog giúp phân tích các gói tin, gồm 3 thành phần:
+ TCPlogger: log lại tất cả các kết nối TCP trên một subnet
+ UDPlogger: log lại tất cả các kết nối UDP trên một subnet
+ Extract: Xử lý các logfile ghi lại bởi TCPlogger và UDBlogger.
- Tiện ích TCP wrapper: Tiện ích này cho phép người quản trị hệ thống dễ dàng giám sát và lọc các gói tin TCP của các dịch vụ như systat, finger, telnet, rlogin, rsh, talk ...

1.2.1.3. Các công cụ ghi log thường sử dụng trong Windows NT và 2000

Trong hệ thống Windows NT 4.0 và Windows 2000 hiện nay đều hỗ trợ đầy đủ các cơ chế ghi log với các mức độ khác nhau. Người quản trị hệ thống tùy thuộc vào mức độ an toàn của dịch vụ và các thông tin sử dụng có thể lựa chọn các mức độ ghi log khác nhau. Ngoài ra, trên hệ thống Windows NT còn hỗ trợ các cơ chế ghi logfile trực tiếp vào các database để tạo báo cáo giúp người quản trị phân tích và kiểm tra hệ thống nhanh chóng và thuận tiện. Sử dụng tiện ích event view để xem các thông tin logfile trên hệ thống với các mức độ như Application log; Security log; System log. Các hình dưới đây sẽ minh hoạ một số hoạt động ghi logfile trên hệ thống Windows:

Ví dụ: Để ghi lại hoạt động đọc, viết, truy nhập.... đối với một file/thư mục là thành công hay không thành công người quản trị có thể cấu hình như sau:

Chọn File Manager - User Manager - Security - Auditing. Ví dụ hình sau minh họa các hoạt động có thể được ghi log trong Windows 2000:

Hình 6.5: Ghi log trong Windows 2000

- Sử dụng tiện ích Event View cho phép xem những thông tin logfile như sau:

Hình 6.6: Công cụ Event View của Windows 2000

Xem chi tiết nội dung một message:

Hình 6.7: Chi tiết 1 thông báo lỗi trong Windows 2000

Thông báo này cho biết nguyên nhân, thời điểm xảy ra lỗi cũng như nhiều thông tin quan trọng khác.

Có thể cấu hình Event Service để thực hiện một action khi có một thông báo lỗi xảy ra như sau:

Hình 6.8: Cấu hình dịchvụ ghi log trong Windows 2000

Ngoài ra, cũng giống như trên UNIX, trong Windows NT cũng có các công cụ theo dõi logfile của một số dịch vụ thông dụng như FTP, Web. Tùy

thuộc vào loại server sử dụng có các phương pháp cấu hình khác nhau.

1.2.2. Thiết lập chính sách bảo mật hệ thống

Trong các bước xây dựng một chính sách bảo mật đối với một hệ thống, nhiệm vụ đầu tiên của người quản trị là xác định được đúng mục tiêu cần bảo mật. Việc xác định những mục tiêu của chính sách bảo mật giúp người sử dụng biết được trách nhiệm của mình trong việc bảo vệ các tài nguyên thông tin trên mạng, đồng thời giúp các nhà quản trị thiết lập các biện pháp đảm bảo hữu hiệu trong quá trình trang bị, cấu hình và kiểm soát hoạt động của hệ thống. Những mục tiêu bảo mật bao gồm:

1.2.2.1. Xác định đối tượng cần bảo vệ

Đây là mục tiêu đầu tiên và quan trọng nhất trong khi thiết lập một chính sách bảo mật. Người quản trị hệ thống cần xác định rõ những đối tượng nào là

quan trọng nhất trong hệ thống cần bảo vệ và xác định rõ mức độ ưu tiên đối với những đối tượng đó. Ví dụ các đối tượng cần bảo vệ trên một hệ thống có thể là: các máy chủ dịch vụ, các router, các điểm truy nhập hệ thống, các chương trình ứng dụng, hệ quản trị CSDL, các dịch vụ cung cấp ...

Trong bước này cần xác định rõ phạm vi và ranh giới giữa các thành phần trong hệ thống để khi xảy ra sự cố trên hệ thống có thể cô lập các thành phần này với nhau, dễ dàng dò tìm nguyên nhân và cách khắc phục. Có thể chia các thành phần trên một hệ thống theo các cách sau:

- Phân tách các dịch vụ tùy theo mức độ truy cập và độ tin cậy.
- Phân tách hệ thống theo các thành phần vật lý như các máy chủ (server), router, các máy trạm (workstation)...
- Phân tách theo phạm vi cung cấp của các dịch vụ như: các dịch vụ bên trong mạng (NIS, NFS ...) và các dịch vụ bên ngoài như Web, FTP, Mail ...

1.2.2.2. Xác định nguy cơ đối với hệ thống

Các nguy cơ đối với hệ thống chính là các lỗ hổng bảo mật của các dịch vụ hệ thống đó cung cấp. Việc xác định đúng đắn các nguy cơ này giúp người quản trị có thể tránh được những cuộc tấn công mạng, hoặc có biện pháp bảo vệ đúng đắn. Thông thường, một số nguy cơ này nằm ở các thành phần sau trên hệ thống:

a) Các điểm truy nhập:

Các điểm truy nhập của hệ thống bất kỳ (Access Points) thường đóng vai trò quan trọng đối với mỗi hệ thống vì đây là điểm đầu tiên mà người sử dụng cũng như những kẻ tấn công mạng quan tâm tới. Thông thường các điểm truy nhập thường phục vụ hầu hết người dùng trên mạng, không phụ thuộc vào quyền hạn cũng như dịch vụ mà người sử dụng dùng. Do đó, các điểm truy nhập thường là thành phần có tính bảo mật lỏng lẻo. Mặt khác, đối với nhiều hệ thống còn cho phép người sử dụng dùng các dịch vụ như Telnet, rlogin để truy nhập vào hệ thống, đây là những dịch vụ có nhiều lỗ hổng bảo mật.

b) Không kiểm soát được cấu hình hệ thống

Không kiểm soát hoặc mất cấu hình hệ thống chiếm một tỷ lệ lớn trong số các lỗ hổng bảo mật. Ngày nay, có một số lượng lớn các phần mềm sử dụng, yêu cầu cấu hình phức tạp và đa dạng hơn, điều này cũng dẫn đến những khó khăn để người quản trị nắm bắt được cấu hình hệ thống. Để khắc phục hiện tượng này, nhiều hãng sản xuất phần mềm đã đưa ra những cấu hình khởi tạo mặc định, trong khi đó những cấu hình này không được xem xét kỹ lưỡng trong một môi trường bảo mật. Do đó, nhiệm vụ của người quản trị là phải nắm được hoạt động của các phần mềm sử dụng, ý nghĩa của các file cấu hình quan trọng, áp dụng các biện pháp bảo vệ cấu hình như sử dụng phương thức mã hóa

hashing code (MD5).

c) Những bug phần mềm sử dụng

Những bug phần mềm tạo nên những lỗ hổng của dịch vụ là cơ hội cho các hình thức tấn công khác nhau xâm nhập vào mạng. Do đó, người quản trị

phải thường xuyên cập nhật tin tức trên các nhóm tin về bảo mật và từ nhà cung cấp phần mềm để phát hiện những lỗi của phần mềm sử dụng. Khi phát hiện có bug cần thay thế hoặc ngừng sử dụng phần mềm đó chờ nâng cấp lên phiên bản tiếp theo.

d) Những nguy cơ trong nội bộ mạng

Một hệ thống không những chịu tấn công từ ngoài mạng, mà có thể bị tấn công ngay từ bên trong. Có thể là vô tình hoặc cố ý, các hình thức phá hoại bên trong mạng vẫn thường xảy ra trên một số hệ thống lớn. Chủ yếu với hình thức tấn công ở bên trong mạng là kẻ tấn công có thể tiếp cận về mặt vật lý đối với các thiết bị trên hệ thống, đạt được quyền truy nhập bất hợp pháp tại ngay hệ thống đó. Ví dụ nhiều trạm làm việc có thể chiếm được quyền sử dụng nếu kẻ tấn công ngồi ngay tại các trạm làm việc đó.

1.2.2.3. Xác định phương án thực thi chính sách bảo mật

Sau khi thiết lập được một chính sách bảo mật, một hoạt động tiếp theo là lựa chọn các phương án thực thi một chính sách bảo mật. Một chính sách bảo mật là hoàn hảo khi nó có tình thực thi cao. Để đánh giá tính thực thi này, có một số tiêu chí để lựa chọn đó là:

- Tính đúng đắn
- Tính thân thiện
- Tính hiệu quả

1.2.2.4. Thiết lập các qui tắc/thủ tục

a) Các thủ tục đối với hoạt động truy nhập bất hợp pháp

Sử dụng một vài công cụ có thể phát hiện ra các hành động truy nhập bất hợp pháp vào một hệ thống. Các công cụ này có thể đi kèm theo hệ điều hành, hoặc từ các hãng sản xuất phần mềm thứ ba. Đây là biện pháp phổ biến nhất để theo dõi các hoạt động hệ thống.

- Các công cụ logging: hầu hết các hệ điều hành đều hỗ trợ một số lượng lớn các công cụ ghi log với nhiều thông tin bổ ích. Để phát hiện những hoạt động truy nhập bất hợp pháp, một số qui tắc khi phân tích logfile như sau:

+ So sánh các hoạt động trong logfile với các log trong quá khứ. Đối với các hoạt động thông thường, các thông tin trong logfile thường có chu kỳ giống nhau như thời điểm người sử dụng login hoặc log out, thời gian sử dụng các dịch vụ trên hệ thống...

+ Nhiều hệ thống sử dụng các thông tin trong logfile để tạo hóa đơn cho khách hàng. Có thể dựa vào các thông tin trong hóa đơn thanh toán để xem xét các truy nhập bất hợp pháp nếu thấy trong hóa đơn đó có những điểm bất thường như thời điểm truy nhập, số điện thoại lạ ...

+ Dựa vào các tiện ích như syslog để xem xét, đặc biệt là các thông báo lỗi login không hợp lệ (bad login) trong nhiều lần.

+ Dựa vào các tiện ích kèm theo hệ điều hành để theo dõi các tiến trình đang hoạt động trên hệ thống; để phát hiện những tiến trình lạ, hoặc những chương trình khởi tạo không hợp lệ ...

- Sử dụng các công cụ giám sát khác: Ví dụ sử dụng các tiện ích về mạng để theo dõi các lưu lượng, tài nguyên trên mạng để phát hiện những điểm

nghi ngờ.
b) Các thủ tục bảo vệ hệ thống
- Thủ tục quản lý tài khoản người sử dụng
- Thủ tục quản lý mật khẩu
- Thủ tục quản lý cấu hình hệ thống
- Thủ tục sao lưu và khôi phục dữ liệu
- Thủ tục báo cáo sự cố

1.2.2.5. Kiểm tra, đánh giá và hoàn thiện chính sách bảo mật

Một hệ thống luôn có những biến động về cấu hình, các dịch vụ sử dụng, và ngay cả nền tảng hệ điều hành sử dụng, các thiết bị phần cứng .... do vậy người thiết lập các chính sách bảo mật mà cụ thể là các nhà quản trị hệ thống luôn luôn phải rà sóat, kiểm tra lại chính sách bảo mật đảm bảo luôn phù hợp với thực tế. Mặt khác kiểm tra và đánh giá chính sách bảo mật còn giúp cho các nhà quản lý có kế hoạch xây dựng mạng lưới hiệu quả hơn.

a) Kiểm tra, đánh giá

Công việc này được thực hiện thường xuyên và liên tục. Kết quả của một chính sách bảo mật thể hiện rõ nét nhất trong chất lượng dịch vụ mà hệ thống đó cung cấp. Dựa vào đó có thể kiểm tra, đánh giá được chính sách bảo mật đó là hợp lý hay chưa. Ví dụ, một nhà cung cấp dịch vụ Internet có thể kiểm tra được chính sách bảo mật của mình dựa vào khả năng phản ứng của hệ thống khi bị tấn công từ bên ngoài như các hành động spam mail, DoS, truy nhập hệ thống trái phép ...

Hoạt động đánh giá một chính sách bảo mật có thể dựa vào một số tiêu chí sau:
- Tính thực thi.
- Khả năng phát hiện và ngăn ngừa các hoạt động phá hoại.
- Các công cụ hữu hiệu để hạn chế các hoạt động phá hoại hệ thống.

b) Hoàn thiện chính sách bảo mật:

Từ các hoạt động kiểm tra, đánh giá nêu trên, các nhà quản trị hệ thống có thể rút ra được những kinh nghiệm để có thể cải thiện chính sách bảo mật hữu hiệu hơn. Cải thiện chính sách có thể là những hành động nhằm đơn giản công việc người sử dụng, giảm nhẹ độ phức tạp trên hệ thống ...

Những hoạt động cải thiện chính sách bảo mật có thể diễn ra trong suốt thời gian tồn tại của hệ thống đó. Nó gắn liền với các công việc quản trị và duy

trì hệ thống. Đây cũng chính là một yêu cầu trong khi xây dựng một chính sách bảo mật, cần phải luôn luôn mềm dẻo, có những thay đổi phù hợp tùy theo điều kiện thực tế.

2. Tổng quan về hệ thống firewall

2.1. Giới thiệu về Firewall

2.1.1. Khái niệm Firewall

Firewall là thiết bị nhằm ngăn chặn sự truy nhập không hợp lệ từ mạng ngoài vào mạng trong. Hệ thống firewall thường bao gồm cả phần cứng và phần mềm. Firewall thường được dùng theo phương thức ngăn chặn hay tạo các luật đối với các địa chỉ khác nhau.

2.1.2. Các chức năng cơ bản của Firewall

Chức năng chính của Firewall là kiểm soát luồng thông tin giữa mạng cần bảo vệ (Trusted Network) và Internet thông qua các chính sách truy nhập đã được thiết lập.
- Cho phép hoặc cấm các dịch vụ truy nhập từ trong ra ngoài và từ ngoài vào trong.

- Kiểm soát địa chỉ truy nhập, và dịch vụ sử dụng.
- Kiểm soát khả năng truy cập người sử dụng giữa 2 mạng.
- Kiểm soát nội dung thông tin truyền tải giữa 2 mạng.
- Ngăn ngừa khả năng tấn công từ các mạng ngoài.

Xây dựng firewalls là một biện pháp khá hữu hiệu, nó cho phép bảo vệ và kiểm soát hầu hết các dịch vụ do đó được áp dụng phổ biến nhất trong các biện pháp bảo vệ mạng. Thông thường, một hệ thống firewall là một cổng (gateway) giữa mạng nội bộ giao tiếp với mạng bên ngoài và ngược lại

2.1.3. Mô hình mạng sử dụng Firewall

Kiến trúc của hệ thống có firewall như sau:

Hình 6.9: Kiến trúc hệ thống có firewall

Nhìn chung, mỗi hệ thống firewall đều có các thành phần như sau:

Hình 6.10: Các thành phần của hệ thống firewall

Firewall có thể bao gồm phần cứng hoặc phần mềm nhưng thường là cả hai. Về mặt phần cứng thì firewall có chức năng gần giống một router, nó cho phép hiển thị các địa chỉ IP đang kết nối qua nó. Điều này cho phép bạn xác định được các địa chỉ nào được phép và các địa chỉ IP nào không được phép kết nối.

Tất cả các firewall đều có chung một thuộc tính là cho phép phân biệt đối xử hay khả năng từ chối truy nhập dựa trên các địa chỉ nguồn.

Theo hình trên các thành phần của một hệ thống firewall bao gồm:

- Screening router: Là chặng kiểm soát đầu tiên cho LAN.
- DMZ: Khu "phi quân sự", là vùng có nguy cơ bị tấn công từ Internet.
- Gateway: là cổng ra vào giữa mạng LAN và DMZ, kiểm soát mọi liên lạc, thực thi các cơ chế bảo mật.
- IF1: Interface 1: Là card giao tiếp với vùng DMZ.
- IF2: Interface 2: Là card giao tiếp với vùng mạng LAN.

- FTP gateway: Kiểm soát truy cập FTP giữa LAN và vùng DMZ. Các truy cập ftp từ mạng LAN ra Internet là tự do. Các truy cập FTP vào LAN đòi hỏi xác thực thông qua Authentication Server.
- Telnet Gateway: Kiểm soát truy cập telnet giữa mạng LAN và Internet. Giống như FTP, người dùng có thể telnet ra ngoài tự do, các telnet từ ngoài vào yêu cầu phải xác thực qua Authentication Server
- Authentication Server: được sử dụng bởi các cổng giao tiếp, nhận diện các yêu cầu kết nối, dùng các kỹ thuật xác thực mạnh như one-time password/token (mật khẩu sử dụng một lần). Các máy chủ dịch vụ trong mạng LAN được bảo vệ an toàn, không có kết nối trực tiếp với Internet, tất cả các thông tin trao đổi đều được kiểm soát qua gateway.

2.1.4. Phân loại Firewall

Có khá nhiều loại firewall, mỗi loại có những ưu và nhược điểm riêng. Tuy nhiên để thuận tiện cho việc nghiên cứu người ta chia hệ thống làm 2 loại chính:

- Packet filtering: là hệ thống firewall cho phép chuyển thông tin giữa hệ thống trong và ngoài mạng có kiểm soát.
- Application-proxy firewall: là hệ thống firewall thực hiện các kết nối thay cho các kết nối trực tiếp từ máy khách yêu cầu.

2.1.4.1. Packet Filtering

Kiểu firewall chung nhất là kiểu dựa trên mức mạng của mô hình OSI.

Firewall mức mạng thường hoạt động theo nguyên tắc router hay còn được gọi là router, có nghĩa là tạo ra các luật cho phép quyền truy nhập mạng dựa trên mức mạng. Mô hình này hoạt động theo nguyên tắc lọc gói tin (packet filtering).
Ở kiểu hoạt động này các gói tin đều được kiểm tra địa chỉ nguồn nơi chúng xuất phát. Sau khi địa chỉ IP nguồn được xác định thì nó được kiểm tra với các luật đã được đặt ra trên router. Ví dụ người quản trị firewall quyết định rằng không cho phép bất kỳ một gói tin nào xuất phát từ mạng microsoft.com được kết nối với mạng trong thì các gói tin xuất phát từ mạng này sẽ không bao giờ đến được mạng trong.
Các firewall hoạt động ở lớp mạng (tương tự như một router) thường cho phép tốc độ xử lý nhanh bởi nó chỉ kiểm tra địa chỉ IP nguồn mà không có một lệnh thực sự nào trên router, nó không cần một khoảng thời gian nào để xác định xem là địa chỉ sai hay bị cấm. Nhưng điều này bị trả giá bởi tính tin cậy của nó. Kiểu firewall này sử dụng địa chỉ IP nguồn làm chỉ thị, điều này tạo ra một lỗ hổng là nếu một gói tin mang địa chỉ nguồn là địa chỉ giả thì như vậy nó sẽ có được một số mức truy nhập vào mạng trong của bạn.
Tuy nhiên có nhiều biện pháp kỹ thuật có thể được áp dụng cho việc lọc gói tin nhằm khắc phục yếu điểm này. Ví dụ như đối với các công nghệ packet filtering phức tạp thì không chỉ có trường địa chỉ IP được kiểm tra bởi router mà còn có các trường khác nữa được kiểm tra với các luật được tạo ra trên

firewall, các thông tin khác này có thể là thời gian truy nhập, giao thức sử dụng, port ...
Firewall kiểu Packet Filtering có thể được phân thành 2 loại:
a) Packet filtering firewall: hoạt động tại lớp mạng của mô hình OSI hay lớp IP trong mô hình giao thức TCP/IP.
Hình 6.11: Packet filtering firewall
b) Circuit level gateway: hoạt động tại lớp phiên (session) của mô hình OSI hay lớp TCP trong mô hình giao thức TCP/IP.
Hình 6.12: Circuit level gateway

2.1.4.2. Application-proxy firewall
Kiểu firewall này hoạt động dựa trên phần mềm. Khi một kết nối từ một người dùng nào đó đến mạng sử dụng firewall kiểu này thì kết nối đó sẽ bị chặn lại, sau đó firewall sẽ kiểm tra các trường có liên quan của gói tin yêu cầu kết nối. Nếu việc kiểm tra thành công, có nghĩa là các trường thông tin đáp ứng được các luật đã đặt ra trên firewall thì firewall sẽ tạo một cái cầu kết nối giữa hai node với nhau.
Ưu điểm của kiểu firewall loại này là không có chức năng chuyển tiếp các gói tin IP, hơn nữa ta có thể điều khiển một cách chi tiết hơn các kết nối thông qua firewall. Đồng thời nó còn đưa ra nhiều công cụ cho phép ghi lại các quá trình kết nối. Tất nhiên điều này phải trả giá bởi tốc độ xử lý, bởi vì tất cả các kết nối cũng như các gói tin chuyển qua firewall đều được kiểm tra kỹ lưỡng với các luật trên firewall và rồi nếu được chấp nhận sẽ được chuyển tiếp tới node đích.
Sự chuyển tiếp các gói tin IP xảy ra khi một máy chủ nhận được một yêu cầu từ mạng ngoài rồi chuyển chúng vào mạng trong. Điều này tạo ra một lỗ hổng cho các kẻ phá hoại (hacker) xâm nhập từ mạng ngoài vào mạng trong.
Nhược điểm của kiểu firewall hoạt động dựa trên ứng dụng là phải tạo

cho mỗi dịch vụ trên mạng một trình ứng dụng uỷ quyền (proxy) trên firewall ví dụ như phải tạo một trình ftp proxy dịch vụ ftp, tạo trình http proxy cho dịch vụ http... Như vậy ta có thể thấy rằng trong kiểu giao thức client-server như dịch vụ telnet làm ví dụ thì cần phải thực hiện hai bước để cho hai máy ngoài mạng và trong mạng có thể kết nối được với nhau. Khi sử dụng firewall kiểu này các máy client (máy yêu cầu dịch vụ) có thể bị thay đổi. Ví dụ như đối với dịch vụ telnet thì các máy client có thể thực hiện theo hai phương thức: một là bạn telnet vào firewall trước sau đó mới thực hiện việc telnet vào máy ở mạng khác; cách thứ hai là bạn có thể telnet thẳng tới đích tuỳ theo các luật trên firewall có cho phép hay không mà việc telnet của bạn sẽ được thực hiện. Lúc này firewall là hoàn toàn trong suốt, nó đóng vai trò như một cầu nối tới đích của bạn.

Firewall kiểu Application-proxy có thể được phân thành 2 loại:

a) Application level gateway: tính năng tương tự như loại circuit-level gateway nhưng lại hoạt động ở lớp ứng dụng trong mô hình giao thức TCP/IP.

Hình 6.13: Application level gateway

b) Stateful multilayer inspection firewall: đây là loại kết hợp được các tính năng của các loại firewall trên: lọc các gói tại lớp mạng và kiểm tra nội dung các gói tại lớp ứng dụng. Firewall loại này cho phép các kết nối trực tiếp giữa các client và các host nên giảm được các lỗi xảy ra do tính chất "không trong suốt" của firewall kiểu Application gateway. Stateful multilayer inspection firewall cung cấp các tính năng bảo mật cao và lại trong suốt đối với các end users.

Hình 6.14: Stateful multilayer inspection firewall

2.2. Một số phần mềm Firewall thông dụng

2.2.1. Packet filtering

Kiểu lọc gói tin này có thể được thực hiện mà không cần tạo một firewall hoàn chỉnh, có rất nhiều các công cụ trợ giúp cho việc lọc gói tin trên Internet (kể cả phải mua hay được miễn phí). Sau đây ta có thể liệt kê một số tiện ích như vậy

2.2.1.1. TCP_Wrappers

TCP_Wrappers là một chương trình được viết bởi Wietse Venema. Chương trình hoạt động bằng cách thay thế các chương trình thường trú của hệ thống và ghi lại tất cả các yêu cầu kết nối, thời gian yêu cầu, và địa chỉ nguồn. Chương trình này cũng có khả năng ngăn chặn các địa chỉ IP hay các mạng không được phép kết nối.

2.2.1.2. NetGate

NetGate được đưa ra bởi Smallwork là một hệ thống dựa trên các luật về lọc gói tin. Nó được viết ra để sử dụng trên các hệ thống Sun Sparc OS 4.1.x. Tương tự như các kiểu packet filtering khác, NetGate kiểm tra tất cả các gói tin nó nhận được và so sánh với các luật đã được tạo ra.

2.2.1.3. Internet Packet Filter

Phần mềm này hoàn toàn miễn phí, được viết bởi Darren Reed. Đây là một chương trình khá tiện lợi, nó có khả năng ngăn chặn được việc tấn công bằng địa chỉ IP giả. Một số ưu điểm của chương trình là nó không chỉ có khả

năng huỷ bỏ các gói tin TCP không đúng hoặc chưa hoàn thiện mà còn không gửi lại bản tin ICMP lỗi. Chương trình này cho phép bạn có thể kiểm tra thử các luật bạn ra trước khi sử dụng chúng.

2.2.2. Application-proxy firewall

2.2.2.1. TIS FWTK

TIS FWTK (Trusted information Systems Firewall Tool Kit) là một phần mềm đầu tiên đầy đủ tính năng của firewall và đặc trưng cho kiểu firewall hoạt động theo phương thức ứng dụng. Những phiên bản đầu tiên của phần mềm này là miễn phí và bao gồm nhiều thành phần riêng rẽ. Mỗi thành phần phục vụ cho một kiểu dịch vụ trên mạng. Các thành phần chủ yếu bao gồm: Telnet, FTP, rlogin, sendmail và http.

Phần mềm này là một hệ thống toàn diện, tuy nhiên nó không có khả năng bảo vệ mạng ngay sau khi cài đặt vì việc cài đặt và cấu hình không phải là dễ dàng. Khi cấu hình phần mềm này bạn phải thực sự hiểu mình đang làm gì bởi có thể với các luật bạn tạo ra thì mạng của bạn không thể được kết nối với bất kỳ mạng nào khác thậm chí ngay cả những mạng quen thuộc. Điểm đặc trưng nhất của phần mềm này là nó có sẵn nhiều tiện ích giúp bạn điều khiển được truy nhập đối với toàn mạng, một phần mạng hay thậm chí chỉ riêng một địa chỉ.

2.2.2.2. Raptor

Raptor là phần mềm firewall cung cấp đầy đủ các tính năng của một firewall chuyên nghiệp với hai giao diện quản lý, một trên hệ đều hành Unix (RCU) và một trên hệ điều hành Windows (RMC). Raptor có thể được cấu hình để bảo vệ mạng theo bốn phương thức: Standard Proxies, Generic Service Passer, Virtual Private Network tunnels và Raptor Mobile. Tuy việc cấu hình cho Raptor khá phức tạp với việc tạo các route, định nghĩa các entity, user và group, thiết lập các authorization rule ... nhưng bù lại ta có thể sử dụng được rất nhiều tính năng ưu việt do Raptor cung cấp để tuỳ biến các mức bảo vệ đối với mạng của mình.

2.3. Thực hành cài đặt và cấu hình firewall Check Point v4.0 for Windows

2.3.1. Yêu cầu phần cứng:

- Cấu hình tối thiểu đối với máy cài GUI Client

Hệ điều hành Windows 95, Windows NT, X/Motif
Dung lượng đĩa trống 20 Mbytes
Bộ nhớ 16 Mbytes
Card mạng Các loại card được hệ điều hành hỗ trợ
Thiết bị khác CD-ROM

- Cấu hình tối thiểu đối với máy cài Management Server

Hệ điều hành Windows NT (Intel x86 và Pentium)
Dung lượng đĩa trống 20 Mbytes
Bộ nhớ tối thiểu 16MB, nên dùng 24MB
Card mạng Các loại card được hệ điều hành hỗ trợ
Thiết bị khác CD-ROM

- Cấu hình tối thiểu đối với máy cài Modul Firewall

Hệ điều hành Windows NT (Intel x86 và Pentium)
Dung lượng đĩa trống 20 Mbytes
Bộ nhớ 16 Mbytes
Card mạng Tối thiểu phải có 3 card mạng thuộc các loại card được hệ điều hành hỗ trợ.
Thiết bị khác CD-ROM

2.3.2. Các bước chuẩn bị trước khi cài đặt

- Thắt chặt an ninh cho máy chủ cài firewall và các module của firewall như GUI Client và Management Server (tắt các dịch vụ không cần thiết, update các patch sửa lỗi của hệ điều hành ...).
- Kiểm tra các kết nối mạng trên các giao diện mạng, đảm bảo từ máy chủ cài Module Firewall có thể ping được các IP trên các giao diện mạng (sử dụng lệnh ifconfig , ping ...).
- Kiểm tra bảng Routing (sử dụng lệnh netstat -rn ...).
- Kiểm tra dịch vụ DNS (sử dụng lệnh nslookup).
- Lập sơ đồ mạng thử nghiệm, đối với máy chủ có 3 giao diện mạng có thể lập sơ đồ như sau:

Hình 6.15: Sơ đồ mạng thử nghiệm đối với máy chủ có 3 giao diện mạng

2.3.3. Tiến hành cài đặt

Login dưới quyền Administrator và cài đặt hệ thống Firewall Checkpoint trên các máy theo trình tự sau:
- Cài đặt GUI Client và Management Server.
- Cài đặt Module Firewall.

2.3.3.1. Cài đặt GUI Client và Management Server

Đưa đĩa CD Checkpoint và chạy lệnh setup trong thư mục Windows, chọn Account Management Client và FireWall-1 User Interface trong cửa sổ Select Components:

Chọn Next, màn hình sẽ hiện ra như sau:

Chọn Next rồi chọn thư mục cài đặt trong cửa sổ Choose Destination Location:

Chọn Next rồi chọn các thành phần trong cửa sổ Select Components:

Chọn Next để bắt đầu quá trình cài đặt.

Sau khi cài xong GUI Client, màn hình sẽ tự động hiện ra phần cài đặt Account Management Client With Encryption Installation:

Chọn Next rồi chọn thư mục cài đặt trong cửa sổ Choose Destination Location:

Chọn Next rồi chọn Folder trong cửa sổ Select Program Folder:

Chọn Next để bắt đầu quá trình cài đặt

2.3.3.2. Cài đặt Module Firewall:

Chọn FireWall-1 trong cửa sổ Select Components ban đầu:

Chọn Next, màn hình sẽ hiện ra như sau:

Chọn Next rồi chọn thư mục cài đặt trong cửa sổ Choose Destination Location:

Chọn Next rồi chọn FireWall-1 FireWall Module trong cửa sổ Selecting Product Type:

223
Chọn Next rồi tùy theo phiên bản Checkpoint đăng ký để chọn số license phù hợp:
Chọn Next để bắt đầu quá trình cài đặt.
Sau khi cài xong, màn hình cài đặt license sẽ hiện lên như sau:

224
Chọn Add rồi nhập license vào cửa sổ sau :
Chọn hostname của Management Server:

225
Chọn chế độ IP Forwarding:

226
Đặt các tham số cho SMTP Security Server:

227
Chọn Finish để kết thúc quá trình cài đặt rồi Restart lại máy.
Sau khi restart lại máy, login vào màn hình console của CheckPoint với user và password đã tạo để thiết lập cấu hình cho firewall:

228

2.3.4. Thiết lập cấu hình

Sau khi login vào màn hình điều khiển của CheckPoint, ta bắt đầu tiến hành quá trình thiết lập cấu hình cho firewall theo các bước sau:
- Định nghĩa cho các giao tiếp (Interface) thuộc mạng trong (Inside network) và mạng ngoài (Outside network) của máy chủ cài CheckPoint.
- Tạo các Network thuộc mạng trong: Theo mô hình thử nghiệm ở đây là mạng 192.168.7.0 và 192.168.1.0.
- Nhóm các Inside network thành một group để tiện quản lý.
- Thiết lập các luật để cho phép hoặc cấm các truy nhập từ trong ra ngoài và từ ngoài vào trong. Các luật này gồm các thành phần cơ bản sau:
+ Số thứ tự: biểu thị mức độ ưu tiên của luật. Luật nào có số thứ tự càng nhỏ thì mức độ ưu tiên càng lớn.
+ Nguồn (SOURCE)
+ Đích (DESTINATION)
+ Giao tiếp (IF VIA)
+ Dịch vụ (SERVICE): các dịch vụ được cho phép/cấm
+ Hành động (ACTION): cho phép/cấm
+ Ngoài ra còn có các tham số khác như TRACK, INSTALL ON, TIME …
Sau đây là một ví dụ về thiết lập luật cho firewall CheckPoint:

229

TÀI LIỆU THAM KHẢO

1. Interconnecting Cisco Network Devices - Steve McQuerry, 03/2000
2. Building Scalable Cisco Internetworks - Catherine Paquet, 01/2003
3. Routing TCP/IP Volume I - Jeff Doyle, 09/1998
4. Cisco Internetworking Basic - Cisco Press, 07/2001
5. Cisco WEB site http://www.cisco.com - Technologies

6. Microsoft Windows 2000 advanced server - Microsoft Press, 1985-1999
7. DNS and BIND, 3trd Edition - Paul Albitz and Cricket Liu, 09/1998
8. Internet System Consortium WEB site http://www.isc.org
9. Remote Access Study Guide - Robert Padjen, Todd Lammle, Wade Edwards, 9/2002
10. Building Cisco Remote Access Networks - Catherine Paquet, 08/1999.
11. Complete Book of Remote Access:Connectivity and Security , Victor Kasacavage (Editor), Weikai Yan, 12/2002
12. Designing & Implementing Microsoft Proxy Server- David Wolfe, Sams Net Publishing.
13. ISA Server 2000 Administration Study Guide- William Heldman (Sybex-MCSE).
14. Configuring ISA server for an Enterprise-Microsoft Training and Certification, 02/2001
15. Designing & Implementting Microsoft Windows2000 Network Infrastructure, Microsoft Training and Certification, 05/2000
16. Firewalls and Internet Security: Repelling the Wily Hacker, Steven M. Bellovin, 01/2003
17. Inside Network Perimeter Security, Karen Fredericks and Lenny Zeltser and Scott Winters, 01/2002
18. CCSP Cisco Secure PIX Firewall Advanced Exam Certification Guide, Greg Bastien and Christian Degu, 01/2003
19. Building Internet Firewalls, Elizabeth D. Zwicky & Simon Cooper, 01/2000
20. Firewalls: A Complete Guide, Marcus Goncalves, 01/1999
21. Configuring ISA server for an Enterprise-Microsoft Training and Certification, 02/2001

—

Giáo trình đào tạo
Quản trị mạng và các thiết bị mạng

PHẦN I
KHÁI QUÁT VỀ CÔNG NGHỆ MẠNG

Chương 1: Tổng quan về công nghệ mạng máy tính và mạng cục bộ

Chương này cung cấp các khái niệm, các kiến thức cơ bản nhất về mạng máy tính và phân loại mạng máy tính. Các nội dung giới thiệu mang tính tổng quan về mạng cục bộ, kiến trúc mạng cục bộ, phương pháp truy cập trong mạng cục bộ và các chuẩn vật lý về các thiết bị mạng. Đây là những kiến thức cơ bản rất hữu ích do phạm vi sử dụng của mạng cục bộ là đang phổ biến hiện nay. Hầu hết các cơ quan, tổ chức, công ty có sử dụng công nghệ thông tin đều thiết lập mạng cục bộ riêng.

Các khái niệm, nội dung cơ bản trong chương 1 cần phải nắm vững đối với tất cả các học viên vì chúng sẽ được sử dụng nhiều trong các chương tiếp theo.

Mục 1: Mạng máy tính

I. Lịch sử mạng máy tính

Internet bắt nguồn từ đề án ARPANET (Advanced Research Project Agency Network) khởi sự trong năm 1969 bởi Bộ Quốc phòng Mỹ (American Department of Defense). Đề án ARPANET với sự tham gia của một số trung tâm nghiên cứu, đại học tại Mỹ (UCLA, Stanford, . . .) nhằm mục đích thiết kế một mạng WAN (Wide Area Network) có khả năng tự bảo tồn chống lại sự phá hoại một phân mạng bằng chiến tranh nguyên tử. Đề án này dẫn tới sự ra đời của nghi thức truyền IP (Internet Protocol). Theo nghi thức này, thông tin truyền sẽ được đóng thành các gói dữ liệu và truyền trên mạng theo nhiều đường khác nhau từ người gửi tới nơi người nhận. Một hệ thống máy tính nối trên mạng gọi là **Router** làm nhiệm vụ tìm đường đi tối ưu cho các gói dữ liệu,

tất cả các máy tính trên mạng đều tham dự vào việc truyền dữ liệu, nhờ vậy nếu một phân mạng bị phá huỷ các **Router** có thể tìm đường khác để truyền thông tin tới người nhận. Mạng ARPANET được phát triển và sử dụng trước hết trong các trường đại học, các cơ quan nhà nước Mỹ, tiếp theo đó, các trung tâm tính toán lớn, các trung tâm truyền vô tuyến điện và vệ tinh được nối vào mạng, . . . trên cơ sở này, ARPANET được nối với khắp các vùng trên thế giới.

Tới năm 1983, trước sự thành công của việc triển khai mạng ARPANET, Bộ quốc phòng Mỹ tách một phân mạng giành riêng cho quân đội Mỹ(MILNET). Phần còn lại, gọi là NSFnet, được quản lý bởi NSF (National Science Foundation) NSF dùng 5 siêu máy tính để làm **Router** cho mạng, và lập một tổ chức không chính phủ để quản lý mạng, chủ yếu dùng cho đại học và nghiên cứu cơ bản trên toàn thế giới. Tới năm 1987, NSFnet mở cửa cho cá nhân và cho các công ty tư nhân (BITnet), tới năm 1988 siêu mạng được mang tên INTERNET.

Tuy nhiên cho tới năm 1988, việc sử dụng INTERNET còn hạn chế trong các dịch vụ truyền mạng (FTP), thư điện tử(E-mail), truy nhập từ xa(TELNET) không thích ứng với nhu cầu kinh tế và đời sống hàng ngày. INTERNET chủ yếu được dùng trong môi trường nghiên cứu khoa học và giảng dạy đại học. Trong năm 1988, tại trung tâm nghiên cứu nguyên tử của Pháp CERN(Centre Européen de Recherche Nuclaire) ra đời đề án *Mạng nhện thế giới* WWW(World Wide Web). Đề án này, nhằm xây dựng một phương thức mới sử dụng INTERNET, gọi là phương thức *Siêu văn bản* (HyperText). Các tài liệu và hình ảnh được trình bày bằng ngôn ngữ HTML (HyperText Markup Language) và được phát hành trên INTERNET qua các hệ chủ làm việc với nghi thức HTTP (HyperText Transport Protocol). Từ năm 1992, phương thức làm việc này được đưa ra thử nghiêm trên INTERNET. Rất nhanh chóng, các công ty tư nhân tìm thấy qua phương thức này cách sử dụng INTERNET trong kinh tế và đời sống. Vốn đầu tư vào INTERNET được nhân lên hàng chục lần. Từ năm 1994 INTERNET trở thành siêu mạng kinh doanh. Số các công ty sử dụng INTERNET vào việc kinh doanh và quảng cáo lên gấp hàng nghìn lần kể từ năm 1995. Doanh số giao dịch thương mại qua mạng INTERNET lên hàng chục tỉ USD trong năm 1996 . . .

Với phương thức siêu văn bản, người sử dụng, qua một phần mềm truy đọc (Navigator), có thể tìm đọc tất cả các tài liệu siêu văn bản công bố tại mọi nơi trên thế giới (kể cả hình ảnh và tiếng nói). Với công nghệ WWW, chúng ta

bước vào giai đoạn mà mọi thông tin có thể có ngay trên bàn làm việc của mình. Mỗi công ty hoặc người sử dụng, được phân phối một *trang cội nguồn* (Home Page) trên hệ chủ HTTP. Trang cội nguồn, là siêu văn bản gốc, để tự do có thể tìm tới tất cả các siêu văn bản khác mà người sử dụng muốn phát hành. Địa chỉ của trang cội nguồn được tìm thấy từ khắp mọi nơi trên thế giới. Vì vậy, đối với một xí nghiệp, trang cội nguồn trở thành một văn phòng đại diện điện tử trên INTERNET. Từ khắp mọi nơi, khách hàng có thể xem các quảng cáo và liên hệ trực tiếp với xí nghiệp qua các dòng siêu liên (HyperLink) trong siêu văn bản.

Tới năm 1994, một điểm yếu của INTERNET là không có khả năng lập trình cục bộ, vì các máy nối vào mạng không đồng bộ và không tương thích. Thiếu khả năng này, INTERNET chỉ được dùng trong việc phát hành và truyền thông tin chứ không dùng để xử lý thông tin được. Trong năm 1994, hãng máy tính SUN Corporation công bố một ngôn ngữ mới, gọi là JAVA(cafe), cho phép lập trình cục bộ trên INTERNET, các chương trình JAVA được gọi thẳng từ các siêu văn bản qua các siêu liên (Applet). Vào mùa thu năm 1995, ngôn ngữ JAVA chính thức ra đời, đánh dấu một bước tiến quan trọng trong việc sử dụng INTERNET. Trước hết, ***một chương trình JAVA, sẽ được chạy trên máy khách (Workstation) chứ không phải trên máy chủ (server). Điều này cho phép sử dụng công suất của tất cả các máy khách vào việc xử lý số liệu. Hàng triệu máy tính (hoặc vi tính) có thể thực hiện cùng một lúc một chương trình ghi trên một siêu văn bản trong máy chủ***. Việc lập trình trên INTERNET cho phép truy nhập từ một trang siêu văn bản vào các chương trình xử lý thông tin, đặc biệt là các chương trình điều hành và quản lý thông tin của một xí nghiệp. phương thức làm việc này, được gọi là INTRANET. Chỉ trong năm 1995-1996, hàng trăm nghìn dịch vụ phần mềm INTRANET được phát triển. Nhiều hãng máy tính và phần mềm như Microsoft, SUN, IBM, Oracle, Netscape,... đã phát triển và kinh doanh hàng loạt phần mềm hệ thống và phần mềm cơ bản để phát triển các ứng dụng INTERNET / INTRANET.

II. Giới thiệu mạng máy tính

I.1. I.Định nghĩa mạng máy tính và mục đích của việc kết nối mạng

I.1.1. Nhu cầu của việc kết nối mạng máy tính

Việc nối máy tính thành mạng từ lâu đã trở thành một nhu cầu khách quan vì :

- Có rất nhiều công việc về bản chất là phân tán hoặc về thông tin, hoặc về xử lý hoặc cả hai đòi hỏi có sự kết hợp truyền thông với xử lý hoặc sử dụng phương tiện từ xa.

- Chia sẻ các tài nguyên trên mạng cho nhiều người sử dụng tại một thời điểm (ổ cứng, máy in, ổ CD ROM . . .)

- Nhu cầu liên lạc, trao đổi thông tin nhờ phương tiện máy tính.

- Các ứng dụng phần mềm đòi hòi tại một thời điểm cần có nhiều người sử dụng, truy cập vào cùng một cơ sở dữ liệu.

I.1.2. Định nghĩa mạng máy tính

Nói một cách ngắn gọn thì mạng máy tính là tập hợp các máy tính độc lập (autonomous) được kết nối với nhau thông qua các đường truyền vật lý và tuân theo các quy ước truyền thông nào đó.

Khái niệm máy tính độc lập được hiểu là các máy tính không có máy nào có khả năng khởi động hoặc đình chỉ một máy khác.

Các đường truyền vật lý được hiểu là các môi trường truyền tín hiệu vật lý (có thể là hữu tuyến hoặc vô tuyến).

Các quy ước truyền thông chính là cơ sở để các máy tính có thể "nói chuyện" được với nhau và là một yếu tố quan trọng hàng đầu khi nói về công nghệ mạng máy tính.

I.2. Đặc trưng kỹ thuật của mạng máy tính

Một mạng máy tính có các đặc trưng kỹ thuật cơ bản như sau:

I.2.1. Đường truyền

Là thành tố quan trọng của một mạng máy tính, là phương tiện dùng để truyền các tín hiệu điện tử giữa các máy tính. Các tín hiệu điệu tử đó chính là các thông tin, dữ liệu được biểu thị dưới dạng các xung nhị phân (ON_OFF), mọi tín hiệu truyền giữa các máy tính với nhau đều thuộc sóng điện từ, tuỳ theo tần số mà ta có thể dùng các đường truyền vật lý khác nhau

Đặc trưng cơ bản của đường truyền là giải thông nó biểu thị khả năng truyền tải tín hiệu của đường truyền.

Thông thường người ta hay phân loại đường truyền theo hai loại:

- Đường truyền hữu tuyến (các máy tính được nối với nhau bằng các dây cáp mạng).

- Đường truyền vô tuyến: các máy tính truyền tín hiệu với nhau thông qua các sóng vô tuyền với các thiết bị điều chế/giải điều chế ở các đầu mút.

I.2.2. Kỹ thuật chuyển mạch:

Là đặc trưng kỹ thuật chuyển tín hiệu giữa các nút trong mạng, các nút mạng có chức năng hướng thông tin tới đích nào đó trong mạng, hiện tại có các kỹ thuật chuyển mạch như sau:

- Kỹ thuật chuyển mạch kênh: Khi có hai thực thể cần truyền thông với nhau thì giữa chúng sẽ thiết lập một kênh cố định và duy trì kết nối đó cho tới khi hai bên ngắt liên lạc. Các dữ liệu chỉ truyền đi theo con đường cố định đó.

- Kỹ thuật chuyển mạch thông báo: thông báo là một đơn vị dữ liệu của người sử dụng có khuôn dạng được quy định trước. Mỗi thông báo có chứa các thông tin điều khiển trong đó chỉ rõ đích cần truyền tới của thông báo. Căn cứ vào thông tin điều khiển này mà mỗi nút trung gian có thể chuyển thông báo tới nút kế tiếp trên con đường dẫn tới đích của thông báo

- Kỹ thuật chuyển mạch gói: ở đây mỗi thông báo được chia ra thành nhiều gói nhỏ hơn được gọi là các gói tin (packet) có khuôn dạng qui định trước. Mỗi gói tin cũng chứa các thông tin điều khiển, trong đó có địa chỉ nguồn (người gửi) và địa chỉ đích (người nhận) của gói tin. Các gói tin của cùng một thông báo có thể được gởi đi qua mạng tới đích theo nhiều con đường khác nhau.

I.2.3. Kiến trúc mạng

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

Khi nói đến kiến trúc của mạng người ta muốn nói tới hai vấn đề là hình trạng mạng (Network topology) và giao thức mạng (Network protocol)

- Network Topology: Cách kết nối các máy tính với nhau về mặt hình học mà ta gọi là tô pô của mạng

Các hình trạng mạng cơ bản đó là: hình sao, hình bus, hình vòng

- Network Protocol: Tập hợp các quy ước truyền thông giữa các thực thể truyền thông mà ta gọi là giao thức (hay nghi thức) của mạng

Các giai thức thường gặp nhất là : TCP/IP, NETBIOS, IPX/SPX, . . .

I.2.4. Hệ điều hành mạng

Hệ điều hành mạng là một phần mềm hệ thống có các chức năng sau:

- Quản lý tài nguyên của hệ thống, các tài nguyên này gồm:

+ Tài nguyên thông tin (về phương diện lưu trữ) hay nói một cách đơn giản là quản lý tệp. Các công việc về lưu trữ tệp, tìm kiếm, xoá, copy, nhóm, đặt các thuộc tính đều thuộc nhóm công việc này

+ Tài nguyên thiết bị. Điều phối việc sử dụng CPU, các ngoại vi... để tối ưu hoá việc sử dụng

- Quản lý người dùng và các công việc trên hệ thống.

Hệ điều hành đảm bảo giao tiếp giữa người sử dụng, chương trình ứng dụng với thiết bị của hệ thống.

- Cung cấp các tiện ích cho việc khai thác hệ thống thuận lợi (ví dụ FORMAT đĩa, sao chép tệp và thư mục, in ấn chung ...)

Các hệ điều hành mạng thông dụng nhất hiện nay là: WindowsNT, Windows9X, Windows 2000, Unix, Novell.

I.3. Phân loại mạng máy tính

Có nhiều cách phân loại mạng khác nhau tuỳ thuộc vào yếu tố chính được chọn dùng để làm chỉ tiêu phân loại, thông thường người ta phân loại mạng theo các tiêu chí như sau

- Khoảng cách địa lý của mạng
- Kỹ thuật chuyển mạch mà mạng áp dụng
- Kiến trúc mạng
- Hệ điều hành mạng sử dụng ...

Tuy nhiên trong thực tế người ta thường chỉ phân loại theo hai tiêu chí đầu tiên

I.3.1. Phân loại mạng theo khoảng cách địa lý :

Nếu lấy khoảng cách địa lý làm yếu tố phân loại mạng thì ta có mạng cục bộ, mạng đô thị, mạng diện rộng, mạng toàn cầu.

Mạng cục bộ (LAN - Local Area Network) : là mạng được cài đặt trong phạm vi tương đối nhỏ hẹp như trong một toà nhà, một xí nghiệp...với khoảng cách lớn nhất giữa các máy tính trên mạng trong vòng vài km trở lại.

Mạng đô thị (MAN - Metropolitan Area Network) : là mạng được cài đặt trong phạm vi một đô thị, một trung tâm văn hoá xã hội, có bán kính tối đa khoảng 100 km trở lại.

Mạng diện rộng (WAN - Wide Area Network) : là mạng có diện tích bao phủ rộng lớn, phạm vi của mạng có thể vượt biên giới quốc gia thậm chí cả lục địa.

Mạng toàn cầu (GAN - Global Area Network) : là mạng có phạm vi trải rộng toàn cầu.

I.3.2. Phân loại theo kỹ thuật chuyển mạch:

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

Mạch chuyển mạch kênh (circuit switched network) : Khi có hai thực thể cần truyền thông với nhau thì giữa chúng sẽ thiết lập một kênh cố định và duy trì kết nối đó cho tới khi hai bên ngắt liên lạc. Các dữ liệu chỉ truyền đi theo con đường cố định đó. Nhược điểm của chuyển mạch kênh là tiêu tốn thời gian để thiết lập kênh truyền cố định và hiệu suất sử dụng mạng không cao.

Mạng chuyển mạch thông báo (message switched network) : Thông báo là một đơn vị dữ liệu của người sử dụng có khuôn dạng được quy định trước. Mỗi thông báo có chứa các thông tin điều khiển trong đó chỉ rõ đích cần truyền tới của thông báo. Căn cứ vào thông tin điều khiển này mà mỗi nút trung gian có thể chuyển thông báo tới nút kế tiếp trên con đường dẫn tới đích của thông báo. Như vậy mỗi nút cần phải lưu giữ tạm thời để đọc thông tin điều khiển trên thông báo, nếu thấy thông báo không gửi cho mình thì tiếp tục chuyển tiếp thông báo đi. Tuỳ vào điều kiện của mạng mà thông báo có thể được chuyển đi theo nhiều con đường khác nhau.

Ưu điểm của phương pháp này là :

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

- Mỗi nút mạng có thể lưu trữ thông tin tạm thời sau đó mới chuyển thông báo đi, do đó có thể điều chỉnh để làm giảm tình trạng tắc nghẽn trên mạng.

- Có thể điều khiển việc truyền tin bằng cách sắp xếp độ ưu tiên cho các thông báo.

- Có thể tăng hiệu suất sử dụng giải thông của mạng bằng cách gắn địa chỉ quảng bá (broadcast addressing) để gửi thông báo đồng thời tới nhiều đích.

Nhược điểm của phương pháp này là:

- Không hạn chế được kích thước của thông báo dẫn đến phí tổn lưu giữ tạm thời cao và ảnh hưởng đến thời gian trả lời yêu cầu của các trạm .

Mạng chuyển mạch gói (packet switched network) : ở đây mỗi thông báo được chia ra thành nhiều gói nhỏ hơn được gọi là các gói tin (packet) có khuôn dạng qui định trước. Mỗi gói tin cũng chứa các thông tin điều khiển,

trong đó có địa chỉ nguồn (người gửi) và địa chỉ đích (người nhận) của gói tin. Các gói tin của cùng một thông báo có thể được gởi đi qua mạng tới đích theo nhiều con đường khác nhau.

Phương pháp chuyển mạch thông báo và chuyển mạch gói là gần giống nhau. Điểm khác biệt là các gói tin được giới hạn kích thước tối đa sao cho các nút mạng (các nút chuyển mạch) có thể xử lý toàn bộ gói tin trong bộ nhớ mà không phải lưu giữ tạm thời trên đĩa. Bởi vậy nên mạng chuyển mạch gói truyền dữ liệu hiệu quả hơn so với mạng chuyển mạch thông báo.

Tích hợp hai kỹ thuật chuyển mạch kênh và chuyển mạch gói vào trong một mạng thống nhất được mạng tích hợp số ISDN (Integated Services Digital Network).

I.3.3. Phân loại theo kiến trúc mạng sử dụng

Kiến trúc của mạng bao gồm hai vấn đề: hình trạng mạng (Network topology) và giao thức mạng (Network protocol)

Hình trạng mạng: Cách kết nối các máy tính với nhau về mặt hình học mà ta gọi là tô pô của mạng

Giao thức mạng: Tập hợp các quy ước truyền thông giữa các thực thể truyền thông mà ta gọi là giao thức (hay nghi thức) của mạng

Khi phân loại theo topo mạng người ta thường có phân loại thành: mạng hình sao, tròn, tuyến tính

Phân loại theo giao thức mà mạng sử dụng người ta phân loại thành mạng : TCP/IP, mạng NETBIOS . ..

Tuy nhiên cách phân loại trên không phổ biến và chỉ áp dụng cho các mạng cục bộ.

I.3.4. Phân loại theo hệ điều hàng mạng

Nếu phân loại theo hệ điều hành mạng người ta chia ra theo mô hình mạng ngang hàng, mạng khách/chủ hoặc phân loại theo tên hệ điều hành mà mạng sử dụng: Windows NT, Unix, Novell . . .

I.4. Giới thiệu các mạng máy tính thông dụng nhất

I.4.1. Mạng cục bộ

Một mạng cục bộ là sự kết nối một nhóm máy tính và các thiết bị kết nối mạng được lắp đặt trên một phạm vị địa lý giới hạn, thường trong một toà nhà hoặc một khu công sở nào đó.

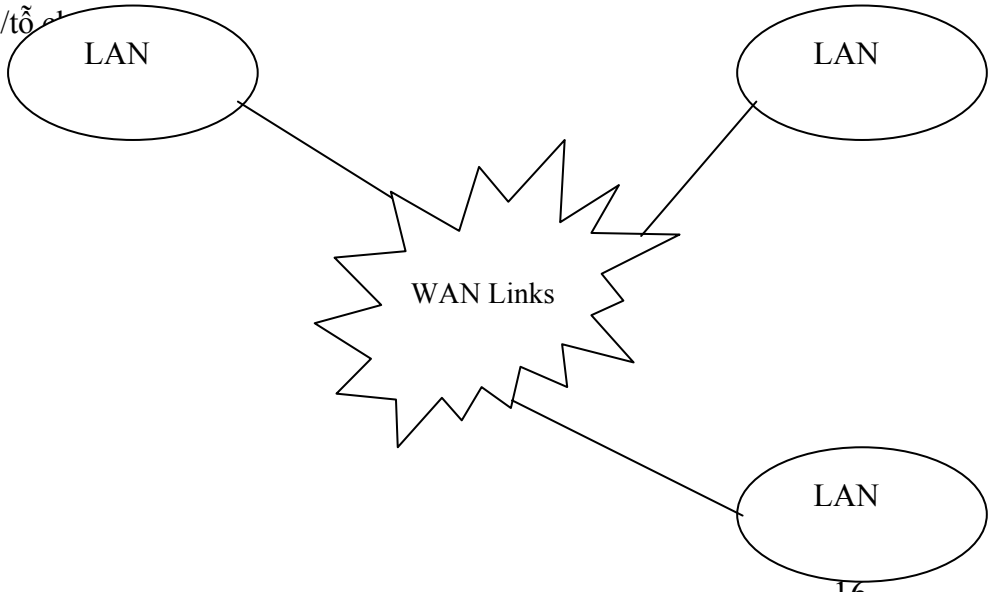
Mạng cục bộ có các đặc tính sau:

- Tốc độ truyền dữ liệu cao
- Phạm vi địa lý giới hạn
-Sở hữu của một cơ quan/tổ chức

I.4.2. Mạng diện rộng với kết nối LAN TO LAN

Mạng diện rộng bao giờ cũng là sự kết nối của các mạng LAN, mạng diện rộng có thể trải trên phạm vi một vùng, quốc gia hoặc cả một lục địa thậm chí trên phạm vi toàn cầu.

- Tốc độ truyền dữ liệu không cao
- Phạm vi địa lý không giới hạn
- Thường triển khai dựa vào các công ty truyền thông, bưu điện và dùng các hệ thống truyền thông này để tạo dựng đường truyền
- Một mạng WAN có thể là sở hữu của một tập đoàn/tổ chức hoặc là mạng kết nối của nhiều tập đoàn/tổ



I.4.3. Liên mạng INTERNET

Với sự phát triển nhanh chóng của công nghệ là sự ra đời của liên mạng INTERNET,

- Là một mạng toàn cầu

- Là sự kết hợp của vô số các hệ thống truyền thông, máy chủ cung cấp thông tin và dịch vụ, các máy trạm khai thác thông tin

- Dựa trên nhiều nền tảng truyền thông khác nhau, nhưng đều trên nền giao thức TCP/IP

- Là sở hữu chung của toàn nhân loại

- Càng ngày càng phát triển mãnh liệt

I.4.4. Mạng INTRANET

Thực sự là một mạng INTERNET thu nhỏ vào trong một cơ quan/công ty/tổ chức hay một bộ/nghành . . ., giới hạn phạm vi người sử dụng, có sử dụng các công nghệ kiểm soát truy cập và bảo mật thông tin .

Được phát triển từ các mạng LAN, WAN dùng công nghệ INTERNET

II. Mạng cục bộ, kiến trúc mạng cục bộ

II.1. Mạng cục bộ

Tên gọi "mạng cục bộ" được xem xét từ quy mô của mạng. Tuy nhiên, đó không phải là đặc tính duy nhất của mạng cục bộ nhưng trên thực tế, quy mô của mạng quyết định nhiều đặc tính và công nghệ của mạng. Sau đây là một số đặc điểm của mạng cục bộ:

Đặc điểm của mạng cục bộ

- Mạng cục bộ có quy mô nhỏ, thường là bán kính dưới vài km. Đặc điểm này cho phép không cần dùng các thiết bị dẫn đường với các mối liên hệ phức tạp

- Mạng cục bộ thường là sở hữu của một tổ chức. Điều này dường như có vẻ ít quan trọng nhưng trên thực tế đó là điều khá quan trọng để việc quản lý mạng có hiệu quả.

- Mạng cục bộ có tốc độ cao và ít lỗi. Trên mạng rộng tốc độ nói chung chỉ đạt vài Kbit/s. Còn tốc độ thông thường trên mạng cục bộ là 10, 100 Kb/s và tới nay với Gigabit Ethernet, tốc độ trên mạng cục bộ có thể đạt 1Gb/s. Xác suất lỗi rất thấp.

II.2. Kiến trúc mạng cục bộ

II.2.1. Đồ hình mạng (Network Topology)

*** Định nghĩa Topo mạng:**

Cách kết nối các máy tính với nhau về mặt hình học mà ta gọi là tô pô của mạng

Có hai kiểu nối mạng chủ yếu đó là :

- Nối kiểu điểm - điểm (point - to - point).

- Nối kiểu điểm - nhiều điểm (point - to - multipoint hay broadcast).

Theo kiểu điểm - điểm, các đường truyền nối từng cặp nút với nhau và mỗi nút đều có trách nhiệm lưu giữ tạm thời sau đó chuyển tiếp dữ liệu đi cho tới đích. Do cách làm việc như vậy nên mạng kiểu này còn được gọi là mạng "lưu và chuyển tiếp" (store and forward).

Theo kiểu điểm - nhiều điểm, tất cả các nút phân chia nhau một đường truyền vật lý chung. Dữ liệu gửi đi từ một nút nào đó sẽ được tiếp nhận bởi tất cả các nút còn lại trên mạng, bởi vậy cần chỉ ra địa chỉ đích của dữ liệu để căn cứ vào đó các nút kiểm tra xem dữ liệu đó có phải gửi cho mình không.

*** Phân biệt kiểu tô pô của mạng cục bộ và kiểu tô pô của mạng rộng.**

Tô pô của mạng rộng thông thường là nói đến sự liên kết giữa các mạng cục bộ thông qua các bộ dẫn đường (router). Đối với mạng rộng topo của mạng là hình trạng hình học của các bộ dẫn đường và các kênh viễn thông còn khi nói tới tô pô của mạng cục bộ người ta nói đến sự liên kết của chính các máy tính.

a) Mạng hình sao

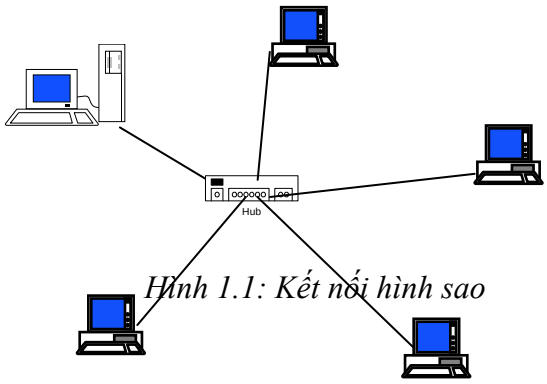
Mạng hình sao có tất cả các trạm được kết nối với một thiết bị trung tâm có nhiệm vụ nhận tín hiệu từ các trạm và chuyển đến trạm đích. Tuỳ theo yêu cầu truyền thông trên mạng mà thiết bị trung tâm có thể là bộ chuyển mạch (switch), bộ chọn đường (router) hoặc là bộ phân kênh (hub). Vai trò của thiết bị trung tâm này là thực hiện việc thiết lập các liên kết điểm-điểm (point-to-point) giữa các trạm.

Ưu điểm:

Thiết lập mạng đơn giản, dễ dàng cấu hình lại mạng (thêm, bớt các trạm), dễ dàng kiểm soát và khắc phục sự cố, tận dụng được tối đa tốc độ truyền của đường truyền vật lý.

Nhược điểm:

Độ dài đường truyền nối một trạm với thiết bị trung tâm bị hạn chế (trong vòng 100m, với công nghệ hiện nay).

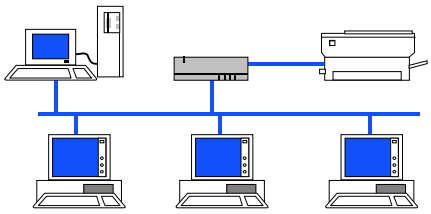


Hình 1.1: Kết nối hình sao

b) Mạng trục tuyến tính (Bus):

Trong mạng trục tất cả các trạm phân chia một đường truyền chung (bus). Đường truyền chính được giới hạn hai đầu bằng hai đầu nối đặc biệt gọi là terminator. Mỗi trạm được nối với trục chính qua một đầu nối chữ T (T-connector) hoặc một thiết bị thu phát (transceiver).

Khi một trạm truyền dữ liệu tín hiệu được quảng bá trên cả hai chiều của bus, tức là mọi trạm còn lại đều có thể thu được tín hiệu đó trực tiếp. Đối với các bus một chiều thì tín hiệu chỉ đi về một phía, lúc đó các terminator phải được thiết kế sao cho các tín hiệu đó phải được dội lại trên bus để cho các trạm trên mạng đều có thể thu nhận được tín hiệu đó. Như vậy với topo mạng trục dữ liệu được truyền theo các liên kết điểm-đa điểm (point-to-multipoint) hay quảng bá (broadcast).



Hình 1.2. Kết nối kiểu bus

Ưu điểm :

Dễ thiết kế, chi phí thấp

Nhược điểm:

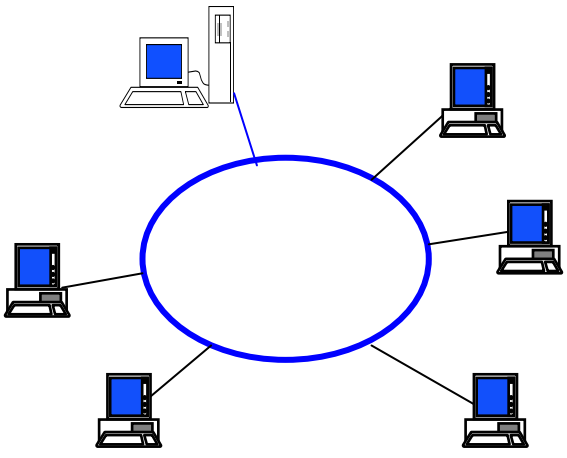
Tính ổn định kém, chỉ một nút mạng hỏng là toàn bộ mạng bị ngừng hoạt động

c) Mạng hình vòng

Trên mạng hình vòng tín hiệu được truyền đi trên vòng theo một chiều duy nhất. Mỗi trạm của mạng được nối với vòng qua một bộ chuyển tiếp (repeater) có nhiệm vụ nhận tín hiệu rồi chuyển tiếp đến trạm kế tiếp trên vòng. Như vậy tín hiệu được lưu chuyển trên vòng theo một chuỗi liên tiếp các liên kết điểm-điểm giữa các repeater do đó cần có giao thức điều khiển việc cấp phát quyền được truyền dữ liệu trên vòng mạng cho trạm có nhu cầu.

Để tăng độ tin cậy của mạng ta có thể lắp đặt thêm các vòng dự phòng, nếu vòng chính có sự cố thì vòng phụ sẽ được sử dụng.

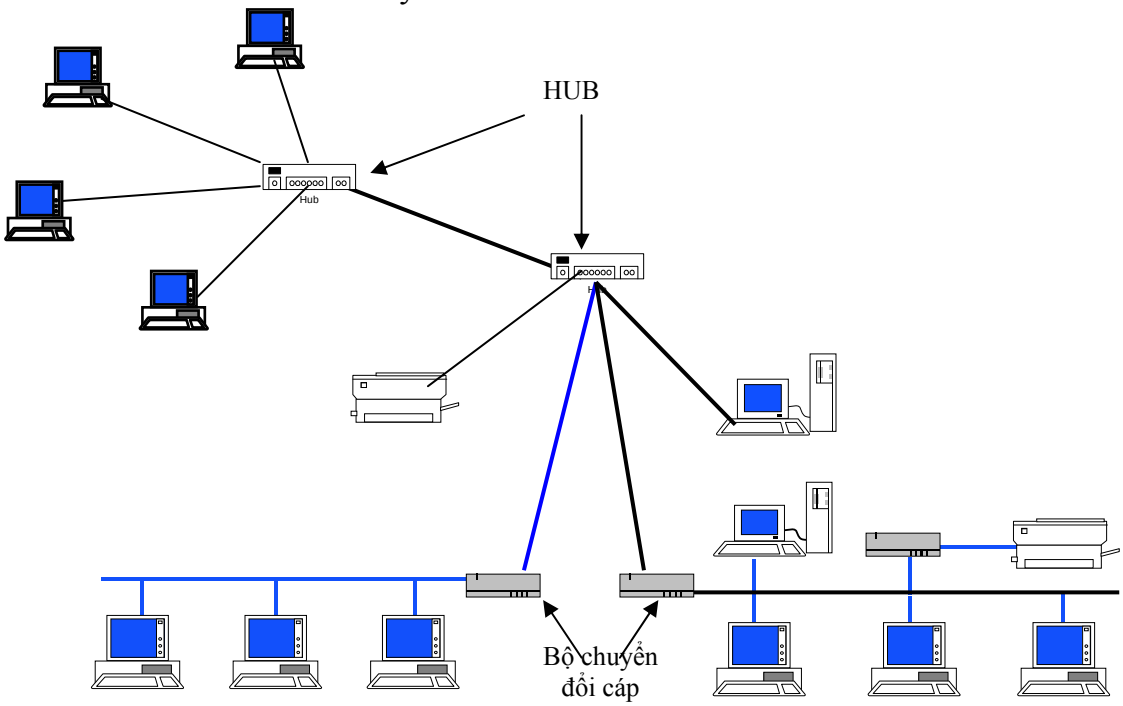
Mạng hình vòng có ưu nhược điểm tương tự mạng hình sao, tuy nhiên mạng hình vòng đòi hỏi giao thức truy nhập mạng phức tạp hơn mạng hình sao.



Hình 1.3. Kết nối kiểu vòng

d) Kết nối hỗn hợp

Là sự phối hợp các kiểu kết nối khác nhau, ví du hình cây là cấu trúc phân tầng của kiểu hình sao hay các HUB có thể được nối với nhau theo kiểu bus còn từ các HUB nối với các máy theo hình sao.



Hình 1.4. Một kết nối hỗn hợp

II.3. Các phương pháp truy cập đường truyền vật lý

Trong mạng cục bộ, tất cả các trạm kết nối trực tiếp vào đường truyền chung. Vì vậy tín hiệu từ một trạm đưa lên đường truyền sẽ được các trạm khác "nghe thấy". Một vấn đề khác là, nếu nhiều trạm cùng gửi tín hiệu lên đường truyền đồng thời thì tín hiệu sẽ chồng lên nhau và bị hỏng. Vì vậy cần phải có một phương pháp tổ chức chia sẻ đường truyền để việc truyền thông được đúng đắn.

Có hai phương pháp chia sẻ đường truyền chung thường được dùng trong các mạng cục bộ:

- Truy nhập đường truyền một cách ngẫu nhiên, theo yêu cầu. Đương nhiên phải có tính đến việc sử dụng luân phiên và nếu trong trường hợp do có nhiều trạm cùng truyền tin dẫn đến tín hiệu bị trùm lên nhau thì phải truyền lại.

- Có cơ chế trọng tài để cấp quyền truy nhập đường truyền sao cho không xảy ra xung đột

II.3.1 Phương pháp đa truy nhập sử dụng sóng mang có phát hiện xung đột CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

Giao thức CSMA (Carrier Sense Multiple Access) - đa truy nhập có cảm nhận sóng mang được sử dụng rất phổ biến trong các mạng cục bộ. Giao thức này sử dụng phương pháp thời gian chia ngăn theo đó thời gian được chia thành các khoảng thời gian đều đặn và các trạm chỉ phát lên đường truyền tại thời điểm đầu ngăn.

Mỗi trạm có thiết bị nghe tín hiệu trên đường truyền (tức là cảm nhận sóng mang). Trước khi truyền cần phải biết đường truyền có rỗi không. Nếu rỗi thì mới được truyền. Phương pháp này gọi là LBT (Listening before talking). Khi phát hiện xung đột, các trạm sẽ phải phát lại. Có một số chiến lược phát lại như sau:

- Giao thức CSMA 1-kiên trì. Khi trạm phát hiện kênh rỗi trạm truyền ngay. Nhưng nếu có xung đột, trạm đợi khoảng thời gian ngẫu nhiên rồi truyền lại. Do vậy xác suất truyền khi kênh rỗi là 1. Chính vì thế mà giao thức có tên là CSMA 1-kiên trì. (1)

- Giao thức CSMA không kiên trì khác một chút.Trạm nghe đường, nếu kênh rỗi thì truyền, nếu không thì ngừng nghe một khoảng thời gian ngẫu nhiên rồi mới thực hiện lại thủ tục. Cách này có hiệu suất dùng kênh cao hơn. (2)

- Giao thức CSMA p-kiên trì. Khi đã sẵn sàng truyền, trạm cảm nhận đường, nếu đường rỗi thì thực hiện việc truyền với xác suất là $p < 1$ (tức là ngay cả khi đường rỗi cũng không hẳn đã truyền mà đợi khoảng thời gian tiếp theo lại tiếp tục thực hiện việc truyền với xác suất còn lại $q=1-p$. (3)

- Ta thấy giải thuật (1) có hiệu quả trong việc tránh xung đột vì hai trạm cần truyền thấy đường truyền bận sẽ cùng rút lui chờ trong những khoảng thời gian ngẫu nhiên khác nhau sẽ quay lại tiếp tục nghe đường truyền. Nhược điểm của nó là có thể có thời gian không sử dụng đường truyền sau mỗi cuộc gọi.

- Giải thuật (2) cố gắng làm giảm thời gian "chết" bằng cách cho phép một trạm có thể được truyền dữ liệu ngay sau khi một cuộc truyền kết thúc. Tuy nhiên nếu lúc đó lại có nhiều trạm đang đợi để truyền dữ liệu thì khả năng xẩy ra xung đột sẽ rất lớn.

- Giải thuật (3) với giá trị p được họn hợp lý có thể tối thiểu hoá được cả khả năng xung đột lẫn thời gian "chết" của đường truyền.

- Xẩy ra xung đột thường là do độ trễ truyền dẫn, mấu chốt của vấn đề là : các trạm chỉ "nghe" trước khi truyền dữ liệu mà không "nghe" trong khi truyền, cho nên thực tế có xung đột thế nhưng các trạm không biết do đó vẫn truyền dữ liệu.

- Để có thể phát hiện xung đột, CSMA/CD đã bổ xung thêm các quy tắc sau đây :

- Khi một trạm truyền dữ liệu, nó vẫn tiếp tục "nghe" đường truyền . Nếu phát hiện xung đột thì nó ngừng ngay việc truyền, nhờ đó mà tiết kiệm được thời gian và giải thông, nhưng nó vẫn tiếp tục gửi tín hiệu thêm một thời gian nữa để đảm bảo rằng tất cả các trạm trên mạng đều "nghe" được sự kiện này.(như vậy phải tiếp tục nghe đường truyền trong khi truyền để phát hiện đụng độ (Listening While Talking))

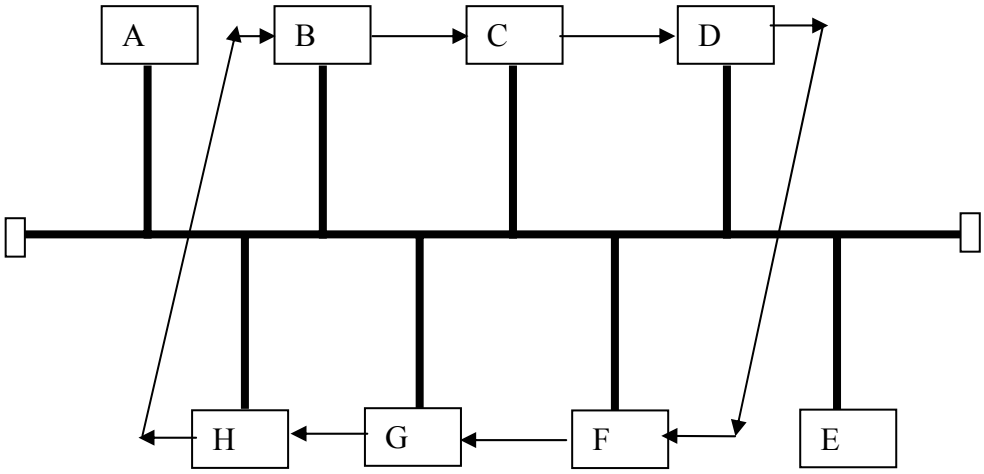
- Sau đó trạm sẽ chờ trong một khoảng thời gian ngẫu nhiên nào đó rồi thử truyền lại theo quy tắc CSMA.

Giao thức này gọi là **CSMA có phát hiện xung đột** (Carrier Sense Multiple Access with Collision Detection viết tắt là CSMA/CD), dùng rộng rãi trong LAN và MAN.

II.3.2. Phương pháp Token Bus

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

sau nó. Thứ tự của các trạm trên vòng logic có thể độc lập với thứ tự vật lý. Các trạm không hoặc chưa có nhu cầu truyền dữ liệu không được vào trong vòng logic.



Hình 1.5. Ví dụ về vòng logic

Trong ví dụ trên, các trạm A, E nằm ngoài vòng logic do đó chỉ có thể tiếp nhận được dữ liệu dành cho chúng.

Việc thiết lập vòng logic không khó nhưng việc duy trì nó theo trạng thái thực tế của mạng mới là khó. Cụ thể phải thực hiện các chức năng sau:

a) Bổ xung một trạm vào vòng logic : các trạm nằm ngoài vòng logic cần được xem xét một cách định kỳ để nếu có nhu cầu truyền dữ liệu thì được bổ xung vào vòng logic.

b) Loại bỏ một vòng khỏi vòng logic : khi một trạm không có nhu cầu truyền dữ liệu thì cần loại bỏ nó ra khỏi vòng logic để tối ưu hoá việc truyền dữ liệu bằng thẻ bài.

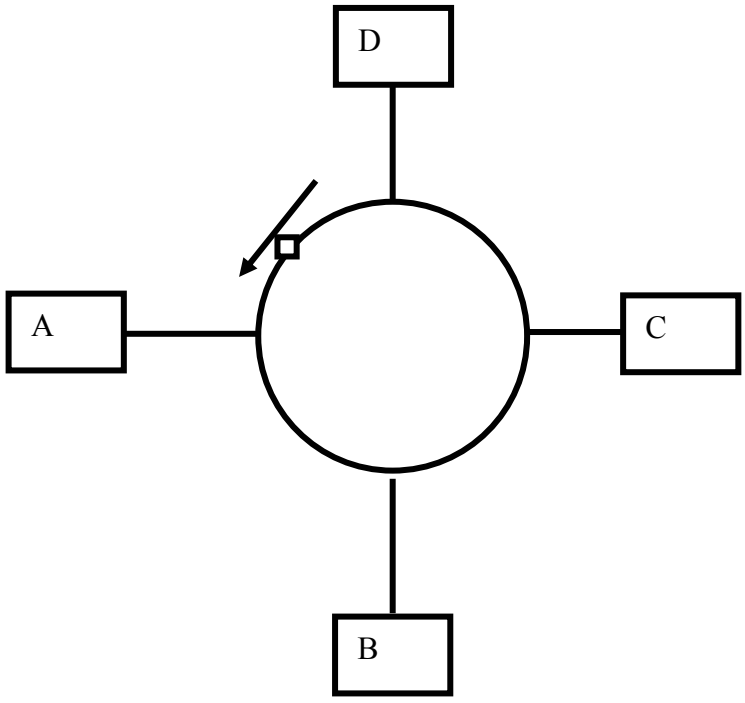
c) Quản lý lỗi : một số lỗi có thể xẩy ra như trùng hợp địa chỉ, hoặc đứt vòng logic.

d) Khởi taọ vòng logic : khi khởi tạo mạng hoặc khi đứt vòng logic cần phải khởi tạo lại vòng logic.

II.3.2. Phương pháp Token Ring

Phương pháp này cũng dựa trên nguyên tắc dùng thẻ bài để cấp phát quyền truy nhập đường truyền. Nhưng ở đây thẻ bài lưu chuyển theo theo vòng vật lý chứ không theo vòng logic như dối với phương pháp token bus.

Thẻ bài là một đơn vị truyền dữ liệu đặc biệt trong đó có một bit biểu diễn trạng thái của thẻ (bận hay rỗi). Một trạm muốn truyền dữ liệu phải chờ cho tới khi nhận được thẻ bài "rỗi". Khi đó trạm sẽ đổi bit trạng thái thành "bận" và truyền một đơn vị dữ liệu đi cùng với thẻ bài đi theo chiều của vòng. Lúc này không còn thẻ bài "rỗi " nữa do đó các trạm muốn truyền dữ liệu phải đợi. Dữ liệu tới trạm đích được sao chép lại, sau đó cùng với thẻ bài trở về trạm nguồn. Trạm nguồn sẽ xoá bỏ dữ liệu đổi bit trạng thái thành "rỗi" và cho lưu chuyển thẻ trên vòng để các trạm khác có nhu cầu truyền dữ liệu được phép truyền .



Hình 1.6. Thẻ bài trong mạng Ring

Sự quay trở lại trạm nguồn của dữ liệu và thẻ bài nhằm tạo khả năng báo nhận tự nhiên : trạm đích có thể gửi vào đơn vị dữ liệu (phần header) các thông tin về kết quả tiếp nhận dữ liệu của mình. Chẳng hạn các thông tin đó có thể là: trạm đích không tồn tại hoặc không hoạt động, trạm đích tồn tại nhưng dữ liệu không được sao chép, dữ liệu đã được tiếp nhận, có lỗi...

Trong phương pháp này cần giải quyết hai vấn đề có thể dẫn đến phá vỡ hệ thống đó là mất thẻ bài và thẻ bài "bận" lưu chuyển không dừng trên vòng .Có nhiều phương pháp giải quyết các vấn đề trên, dưới đây là một phương pháp được khuyến nghị:

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

Đối với vấn đề thẻ bài bận lưu chuyển không dừng, trạm điều khiển sử dụng một bit trên thẻ bài để đánh dấu khi gặp một thẻ bài "bận" đi qua nó. Nếu nó gặp lại thẻ bài bận với bit đã đánh dấu đó có nghĩa là trạm nguồn đã không nhận lại được đơn vị dữ liệu của mình do đó thẻ bài "bận" cứ quay vòng mãi. Lúc đó trạm điều khiển sẽ chủ động đổi bit trạng thái "bận" thành "rỗi" và cho thẻ bài chuyển tiếp trên vòng. Trong phương pháp này các trạm còn lại trên mạng sẽ đóng vai trò bị động, chúng theo dõi phát hiện tình trạng sự cố trên trạm chủ động và thay thế trạm chủ động nếu cần.

III. Chuẩn hoá mạng máy tính

III.1. Vấn đề chuẩn hoá mạng và các tổ chức chuẩn hoá mạng

Khi thiết kế, các nhà thiết kế tự do lựa chọn kiến trúc mạng cho riêng mình. Từ đó dẫn tới tình trạng không tương thích giữa các mạng máy tính với nhau. Nhu cầu trao đổi thông tin càng lớn thúc đẩy việc xây dựng khung chuẩnvề kiến trúc mạng để làm căn cứ cho các nhà thiết kế và chế tạo thiết bị mạng .

Chính vì lý do đó, tổ chức tiêu chuẩn hoá quốc tế ISO (Internatinal Organnization for Standarzation) đã xây dựng mô hình tham chiếu cho việc kết

nối các hệ thống mở OSI (reference model for Open Systems Interconnection). Mô hình này là cơ sở cho việc kết nối các hệ thống mở phục vụ cho các ứng dụng phân tán.

Có hai loại chuẩn cho mạng đó là :

- Các chuẩn chính thức (de jure) do các tổ chức chuẩn quốc gia và quốc tế ban hành.

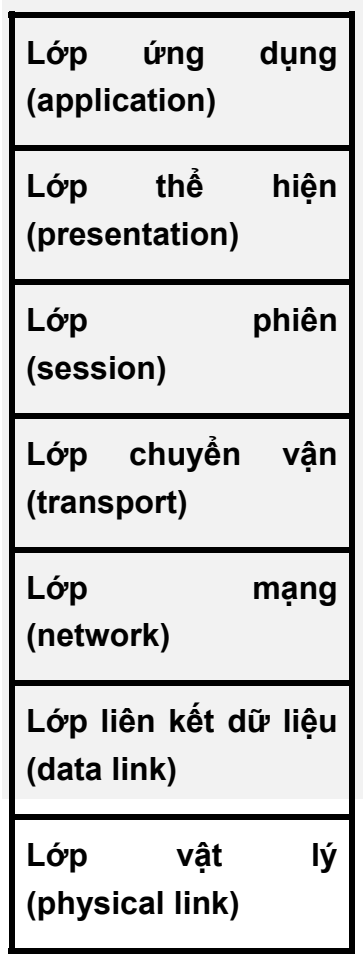
- Các chuẩn tực tiễn (de facto) do các hãng sản xuất, các tổ chức người sử dụng xây dựng và được dùng rộng rãi trong thực tế

III.2. Mô hình tham chiếu OSI 7 lớp

Khi thiết kế, các nhà thiết kế tự do lựa chọn kiến trúc mạng cho riêng mình. Từ đó dẫn tới tình trạng không tương thích giữa các mạng máy tính với nhau. Vấn đề không tương thích đó làm trở ngại cho sự tương tác giữa những người sử dụng mạng khác nhau. Nhu cầu trao đổi thông tin càng lớn thúc đẩy việc xây dựng khung chuẩn về kiến trúc mạng để làm căn cứ cho các nhà thiết kế và chế tạo thiết bị mạng .

Chính vì lý do đó, tổ chức tiêu chuẩn hoá quốc tế ISO (Internatinal Organnization for Standarzation) đã xây dựng mô hình tham chiếu cho việc kết nối các hệ thống mở OSI (reference model for Open Systems Interconnection). Mô hình này là cơ sở cho việc kết nối các hệ thống mở phục vụ cho các ứng dụng phân tán.

Mô hình OSI được biểu diễn theo hình dưới đây:



Hình 1.7. Mô hình OSI 7 lớp

a) Lớp vật lý

Lớp này bảo đảm các công việc sau:

- Lập, cắt cuộc nối.

- Truyền tin dạng bit qua kênh vật lý.

- Có thể có nhiều kênh.

b) Lớp liên kết dữ liệu

Lớp này đảm bảo việc biến đổi các tin dạng bit nhận được từ lớp dưới (vật lý) sang khung số liệu, thông báo cho hệ phát, kết quả thu được sao cho các thông tin truyền lên cho mức 3 không có lỗi. Các thông tin truyền ở mức 1 có thể làm hỏng các thông tin khung số liệu (frame error). Phần mềm mức hai

sẽ thông báo cho mức một truyền lại các thông tin bị mất / lỗi. Đồng bộ các hệ có tốc độ xử lý tính khác nhau, một trong những phương pháp hay sử dụng là dùng bộ đệm trung gian để lưu giữ số liệu nhận được. Độ lớn của bộ đệm này phụ thuộc vào tương quan xử lý của các hệ thu và phát. Trong trường hợp đường truyền song công toàn phần, lớp datalink phải đảm bảo việc quản lý các thông tin số liệu và các thông tin trạng thái.

c) Lớp mạng

Nhiệm vụ của lớp mạng là đảm bảo chuyển chính xác số liệu giữa các thiết bị cuối trong mạng. Để làm được việc đó, phải có chiến lược đánh địa chỉ thống nhất trong toàn mạng. Mỗi thiết bị cuối và thiết bị mạng có một địa chỉ mạng xác định. Số liệu cần trao đổi giữa các thiết bị cuối được tổ chức thành các gói *(packet)* có độ dài thay đổi và được gán đầy đủ địa chỉ nguồn *(source address)* và địa chỉ đích *(destination address)*.

Lớp mạng đảm bảo việc tìm đường tối ưu cho các gói dữ liệu bằng các giao thức chọn đường dựa trên các thiết bị chọn đường *(router)*. Ngoài ra, lớp mạng có chức năng điều khiển lưu lượng số liệu trong mạng để tránh xảy ra tắc ngẽn bằng cách chọn các chiến lược tìm đường khác nhau để quyết định việc chuyển tiếp các gói số liệu.

d) Lớp chuyển vận

Lớp này thực hiện các chức năng nhận thông tin từ lớp phiên (**session**) chia thành các gói nhỏ hơn và truyền xuống lớp dưới, hoặc nhận thông tin từ lớp dưới chuyển lên phục hồi theo cách chia của hệ phát (Fragmentation and Reassembly). Nhiệm vụ quan trọng nhất của lớp vận chuyển là đảm bảo chuyển số liệu chính xác giữa hai thực thể thuộc lớp phiên (end-to-end control). Để làm được việc đó, ngoài chức năng kiểm tra số tuần tự phát, thu, kiểm tra và phát hiện, xử lý lỗi.Lớp vận chuyển còn có chức năng điều khiển lưu lượng số liệu để đồng bộ giữa thể thu và phát , tránh tắc nghẽn số liệu khi chuyển qua lớp mạng. Ngoài ra, nhiều thực thể lớp phiên có thể trao đổi số liệu trên cùng một kết nối lớp mạng (multiplexing).

e) Lớp phiên

Liên kết giữa hai thực thể có nhu cầu trao đổi số liệu, ví dụ người dùng và một máy tính ở xa, được gọi là một phiên làm việc. Nhiệm vụ của lớp phiên là quản lý việc trao đổi số liệu, ví dụ: thiết lập giao diện giữa người dùng và

máy, xác định thông số điều khiển trao đổi số liệu (tốc độ truyền, số bit trong một byte, có kiểm tra lỗi parity hay không, v.v.), xác định loại giao thức mô phỏng thiết bị cuối (terminal emulation), v.v. Chức năng quan trọng nhất của lớp phiên là đảm bảo đồng bộ số liệu bằng cách thực hiện các điểm kiểm tra. Tại các điểm kiểm tra này, toàn bộ trạng thái và số liệu của phiên làm việc được lưu trữ trong bộ nhớ đệm. Khi có sự cố, có thể khởi tạo lại phiên làm việc từ điểm kiểm tra cuối cùng (không phải khởi tạo lại từ đầu).

f) Lớp thể hiện

Nhiệm vụ của lớp thể hiện là thích ứng các cấu trúc dữ liệu khác nhau của người dùng với cấu trúc dữ liệu thống nhất sử dụng trong mạng. Số liệu của người dùng có thể được nén và mã hoá ở lớp thể hiện, trước khi chuyển xuống lớp phiên. Ngoài ra, lớp thể hiện còn chứa các thư viện các yêu cầu của người dùng, thư viện tiện ích, ví dụ thay đổi dạng thể hiện của các *tệp*, nén *tệp*...

g) Lớp ứng dụng

Lớp ứng dụng cung cấp các phương tiện để người sử dụng có thể truy nhập được vào môi trường OSI, đồng thời cung cấp các dịch vụ thông tin phân tán. Lớp mạng cho phép người dùng khai thác các tài nguyên trong mạng tương tự như tài nguyên tại chỗ.

III.3. Các chuẩn kết nối thông dụng nhất IEEE 802.X và ISO 8802.X

Bên cạnh việc chuẩn hoá cho mạng nối chung dẫn đến kết quả cơ bản nhất là mô hình tham chiếu OSI như đã giới thiệu. Việc chuẩn hoá mạng cục bộ nói riêng đã được thực hiện từ nhiều năm nay để đáp ứng sự phát triển của mạng cục bộ.

Cũng như đối với mạng nói chung, có hai loại chuẩn cho mạng cục bộ, đó là :

- Các chuẩn chính thức (de jure) do các tổ chức chuẩn quốc gia và quốc tế ban hành.

- Các chuẩn tực tiễn (de facto) do các hãng soản xuất, các tổ chức người sử dụng xây dựng và được dùng rộng rãi trong thực tế

- Các chuẩn IEEE 802.x và ISO 8802.x

IEEE là tổ chức đi tiên phong trong lĩnh vực chuẩn hoá mạng cục bộ với đề án IEEE 802 với kết quả là một loạt các chuẩn thuộc họ IEEE 802.x ra đời . Cuối những năm 80, tổ chức ISO đã tiếp nhận họ chuẩn này và ban hành thành chuẩn quốc tế dưới mã hiệu tương ứng là ISO 8802.x.

IEEE 802.: là chuẩn đặc tả kiến trúc mạng, kết nối giữa các mạng và việc quản trị mạng đối với mạng cục bộ.

IEEE 802.2: là chuẩn đặc tả tầng dịch vụ giao thức của mạng cục bộ.

IEEE 802.3: là chuẩn đặc tả một mạng cục bộ dựa trên mạng Ethernet nổi tiếng của Digital, Intel và Xerox hợp tác xây dựng từ năm 1980.

Tầng vật lý của IEEE 802.3 có thể dùng các phương án sau để xây dựng:

- 10BASE5 : tốc độ 10Mb/s, dùng cáp xoắn đôi không bọc kim UTP (Unshield Twisted Pair), với phạm vi tín hiệu lên tới 500m, topo mạng hình sao.

- 10BASE2 : tốc độ 10Mb/s, dùng cáp đồng trục thin-cable với trở kháng 50 Ohm, phạm vi tín hiệu 200m,topo mạng dạng bus.

- 10BASE5 : tốc độ 10Mb/s, dùng cáp đồng trục thick-cable (đường kính 10mm) với trở kháng 50 Ohm, phạm vi tín hiệu 500m, topo mạng dạng bus.

- 10BASE-F: dùng cáp quang, tốc độ 10Mb/s phạm vi cáp 2000m.

IEEE 802.4: là chuẩn đặc tả mạng cục bộ với topo mạng dạng bus dùng thẻ bài để điều việc truy nhập đường truyền.

IEEE 802.5: là chuẩn đặc tả mạng cục bộ với topo mạng dạng vòng (ring) dùng thẻ bài để điều việc truy nhập đường truyền.

IEEE 802.6: là chuẩn đặc tả mạng tốc độ cao kết nối với nhiều mạng cục bộ thuộc các khu vực khác nhau của một đô thị (còn được gọi là mạng MAN - Metropolitan Area Network)

IEEE 802.9: là chuẩn đặc tả mạng tích hợp dữ liệu và tiếng nói bao gồm 1 kênh dị bộ 10 Mb/s cùng với 96 kênh 64Kb/s. Chuẩn này được thiết kế cho môi trường có lượng lưu thông lớn và cấp bách.

IEEE 802.10: là chuẩn đặc tả về an toàn thông tin trong các mạng cục bộ có khả năng liên tác .

IEEE 802.11: là chuẩn đặc tả mạng cục bộ không dây (Wireless LAN) hiện đang được tiếp tục phát triển.

IEEE 802.12: là chuẩn đặc tả mạng cục bộ dựa trên công nghệ được đề xuất bởi AT&T, IBM và HP gọi là 100 VG - AnyLAN. Mạng này có topo mạng hình sao và một phương pháp truy nhập đường truyền có điều khiển tranh chấp. Khi có nhu cầu truyền dữ liệu, một trạm sẽ gửi yêu cầu đến hub và trạm chỉ có truyền dữ liệu khi hub cho phép.

Mục 2: Các thiết bị mạng thông dụng và các chuẩn kết nối vật lý

I. Các thiết bị mạng thông dụng

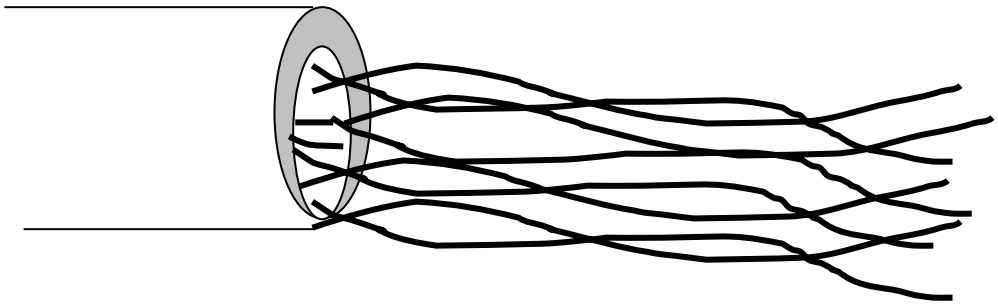
II.1. Các loại cáp truyền

II.1.1. Cáp đôi dây xoắn (Twisted pair cable)

Cáp đôi dây xoắn là cáp gồm hai dây đồng xoắn để tránh gây nhiễu cho các đôi dây khác, có thể kéo dài tới vài km mà không cần khuyếch đại. Giải tần trên cáp dây xoắn đạt khoảng 300–4000Hz, tốc độ truyền đạt vài kbps đến vài Mbps. Cáp xoắn có hai loại:

- Loại có bọc kim loại để tăng cường chống nhiễu gọi là cap STP (Shield Twisted Pair). Loại này trong vỏ bọc kim có thể có nhiều đôi dây. Về lý thuyết thì tốc độ truyền có thể đạt 500 Mb/s nhưng thực tế thấp hơn rất nhiều (chỉ đạt 155 Mbps với cáp dài 100 m)

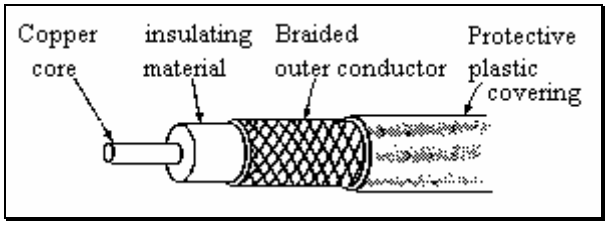
- Loại không bọc kim gọi là UTP (UnShield Twisted Pair), chất lượng kém hơn STP nhưng rất rẻ. Cap UTP được chia làm 5 hạng tuỳ theo tốc độ truyền. Cáp loại 3 dùng cho điện thoại. Cáp loại 5 có thể truyền với tốc độ 100Mb/s rất hay dùng trong các mạng cục bộ vì vừa rẻ vừa tiện sử dụng. Cáp này có 4 đôi dây xoắn nằm trong cùng một vỏ bọc



Hình 7. Cáp UTP Cat. 5

II.1.2. Cáp đồng trục (Coaxial cable) băng tần cơ sở

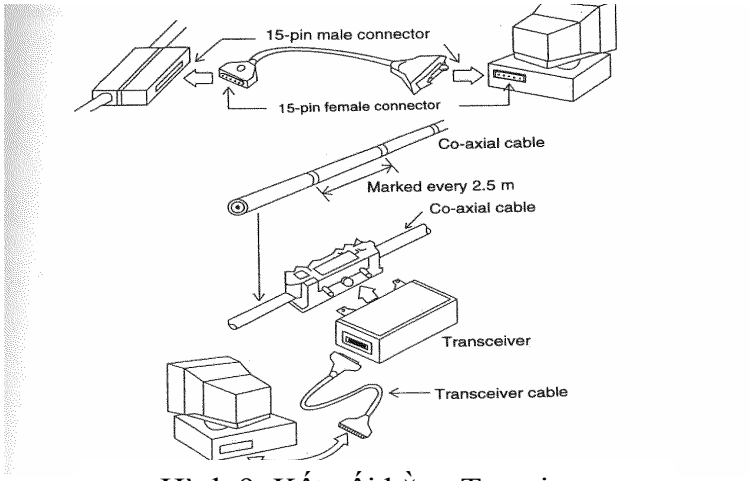
Là cáp mà hai dây của nó có lõi lồng nhau, lõi ngoài là lưới kim loại. , Khả năng chống nhiễu rất tốt nên có thể sử dụng với chiều dài từ vài trăm met đến vài km. Có hai loại được dùng nhiều là loại có trở kháng 50 ohm và loại có trở kháng 75 ohm



Hình 8. Cáp đồng trục

Dải thông của cáp này còn phụ thuộc vào chiều dài của cáp. Với khoảng cách1 km có thể đạt tốc độ truyền tư 1– 2 Gbps. Cáp đồng trục băng tần cơ sở thường dùng cho các mạng cục bộ. Có thể nối cáp bằng các đầu nối theo chuẩn BNC có hình chữ T. ở VN người ta hay gọi cáp này là cáp gầy do dịch từ tên trong tiếng Anh là 'Thin Ethernet".

Một loại cáp khác có tên là "Thick Ethernet" mà ta gọi là cáp béo. Loại này thường có màu vàng. Người ta không nối cáp bằng các đầu nối chữ T như



Hình 9. Kết nối bằng Traceiver

cáp gầy mà nối qua các kẹp bấm vào dây. Cứ 2m5 lại có đánh dấu để nối dây (nếu cần). Từ kẹp đó người ta gắn các tranceiver rồi nối vào máy tính. (Xem hình 9)

II.1.3. Cáp đồng trục băng rộng (Broadband Coaxial Cable)

Đây là loại cáp theo tiêu chuẩn truyền hình (thường dùng trong truyền hình cap) có giải thông từ 4 – 300 Khz trên chiều dài 100 km. Thuật ngữ "băng rộng" vốn là thuật ngữ của ngành truyền hình còn trong ngành truyền số liệu điều này chỉ có nghĩa là cáp loại này cho phép truyền thông tin tương tự (analog) mà thôi. Các hệ thống dựa trên cáp đồng trục băng rộng có thể truyền song song nhiều kênh. Việc khuyếch đại tín hiệu chống suy hao có thể làm theo kiểu khuyếch đại tín hiệu tương tự (analog). Để truyền thông cho máy tính cần chuyển tín hiệu số thành tín hiệu tương tự.

II.1.4. Cáp quang

Dùng để truyền các xung ánh sáng trong lòng một sợi thuỷ tinh phản xạ toàn phần. Môi trường cáp quang rất lý tưởng vì

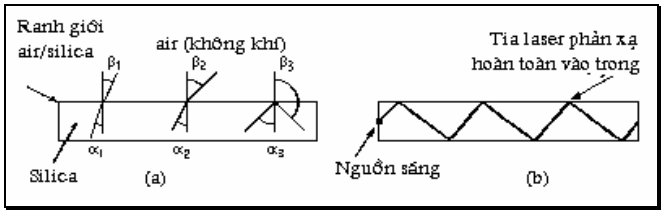
- Xung ánh sáng có thể đi hàng trăm km mà không giảm cường độ sáng.

- Giải thông rất cao vì tần số ánh sáng dùng đối với cáp quang cỡ khoảng 1014 –1016

- An toàn và bí mật

- Không bị nhiễu điện từ

Chỉ có hai nhược điểm là khó nối dây và giá thành cao.



Hình 10. Truyền tín hiệu bằng cáp quang

Để phát xung ánh sáng người ta dùng các đèn LED hoặc các diod laser. Để nhận người ta dùng các photo diode , chúng sẽ tạo ra xung điện khi bắt được xung ánh sáng

Cáp quang cũng có hai loại

- Loại đa mode (multimode fiber): khi góc tới thành dây dẫn lớn đến một mức nào đó thì có hiện tượng phản xạ toàn phần. Nhiều tia sáng có thể cùng truyền miễn là góc tới của chúng đủ lớn. Các cap đa mode có đường kính khoảng 50 μ

- Loại đơn mode (singlemode fiber): khi đường kính dây dẫn bằng bước sóng thì cáp quang giống như một ống dẫn sóng, không có hiện tượng phản xạ nhưng chỉ cho một tia đi. Loại nàycó cường kính khoản 8 μ và phải dùng diode laser. Cáp quang đa mode có thể cho phép truyền xa tới hàng trăm km mà không cần phải khuyếch đại.

II.2. Các thiết bị ghép nối

II.2.1. Card giao tiếp mạng (Network Interface Card viết tắt là NIC)

Đó là một card được cắm trực tiếp vào máy tính. Trên đó có các mạch điện giúp cho việc tiếp nhận (receiver) hoặc/và phát (transmitter) tín hiệu lên mạng. Người ta thường dùng từ tranceiver để chỉ thiết bị (mạch) có cả hai chức năng thu và phát. Transceiver có nhiều loại vì phải thích hợp đối với cả môi trường truyền và do đó cả đầu nối. Ví dụ với cáp gầy card mạng cần có đường giao tiếp theo kiểu BNC, với cáp UTP cần có đầu nối theo kiểu giắc điện thoại K5, cáp dày dùng đường nối kiểu AUI , với cáp quang phải có những transceiver cho phép chuyển tín hiệu điện thành các xung ánh sáng và ngược lại.

Để dễ ghép nối, nhiều card có thể có nhiều đầu nối ví dụ BNC cho cáp gầy, K45 cho UTP hay AUI cho cáp béo

Trong máy tính thường để sẵn các khe cắm để bổ sung các thiết bị ngoại vi hay cắm các thiết bị ghép nối.

II.2.2. Bộ chuyển tiếp (REPEATER)

Tín hiệu truyền trên các khoảng cách lớn có thể bị suy giảm. Nhiệm vụ của các repeater là hồi phục tín hiệu để có thể truyền tiếp cho các trạm khác. Một số repeater đơn giản chỉ là khuyếch đại tín hiệu. Trong trường hợp đó cả tín hiệu bị méo cũng sẽ bị khuyếch đại. Một số repeater có thể chỉnh cả tín hiệu.

II.2.3. Các bộ tập trung (Concentrator hay HUB)

HUB là một loại thiết bị có nhiều đầu để cắm các đầu cáp mạng. HUB có thể có nhiều loại ổ cắm khác nhau phù hợp với kiểu giắc mạng RJ45, AUI hay BCN. Như vậy người ta sử dụng HUB để nối dây theo kiểu hình sao. Ưu điểm của kiểu nối này là tăng độ độc lập của các máy . Nếu dây nối tới một máy nào đó tiếp xúc không tốt cũng không ảnh hưởng đến máy khác.

Đặc tính chủ yếu của HUB là hệ thống chuyển mạch trung tâm trong mạng có kiến trúc hình sao với việc chuyển mạch được thực hiện theo hai cách: store-and-forward hoặc on-the-fly. Tuy nhiên hệ thống chuyển mạch trung tâm làm nảy sinh vấn đề khi lỗi xảy ra ở chính trung tâm, vì vậy hướng phát triển trong suốt nhiều năm qua là khử lỗi để làm tăng độ tin cậy của HUB.

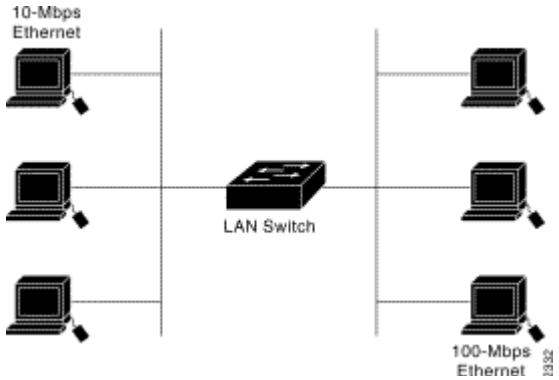
Có loại HUB thụ động (passive HUB) là HUB chỉ đảm bảo chức năng kết nối hoàn toàn không xử lý lại tín hiệu. Khi đó không thể dùng HUB để tăng khoảng cách giữa hai máy trên mạng.

HUB chủ động (active HUB) là HUB có chức năng khuyếch đại tín hiệu để chống suy hao. Với HUB này có thể tăng khoảng cách truyền giữa các máy.

HUB thông minh (intelligent HUB) là HUB chủ động nhưng có khả năng tạo ra các gói tin mang tin tức về hoạt động của mình và gửi lên mạng để người quản trị mạng có thể thực hiện quản trị tự động

II.2.4. Switching Hub (hay còn gọi tắt là switch)

Là các bộ chuyển mạch thực sự. Khác với HUB thông thường, thay vì chuyển một tín hiệu đến từ một cổng cho tất cả các cổng, nó chỉ chuyển tín hiệu đến cổng có trạm đích. Do vậy Switch là một thiết bị quan trọng trong các mạng cục bộ lớn dùng để phân đoạn mạng. Nhờ có switch mà đụng độ trên mạng giảm hẳn. Ngày nay switch là các thiết bị mạng quan trọng cho phép tuỳ biến trên mạng chẳng hạn lập mạng ảo.



Hình 11. LAN Switch nối hai Segment mạng

Switch thực chất là một loại bridge, về tính năng kỹ thuật, nó là loại bridge có độ trễ nhỏ nhất. Khác với bridge là phải đợi đến hết frame rồi mới truyền, switch sẽ chờ cho đến khi nhận được địa chỉ đích của frame gửi tới và lập tức được truyền đi ngay. Điều này có nghĩa là frame sẽ được gửi tới LAN cần gửi trước khi nó được switch nhận xong hoàn toàn.

II.2.5. Modem

Là tên viết tắt từ hai từ điều chế (MOdulation) và giải điều chế (DEModulation) là thiết bị cho phép điều chế để biến đổi tín hiệu số sang tín hiệu tương tự để có thể gửi theo đường thoại và khi nhận tín hiệu từ đường thoại có thể biến đổi ngược lại thành tín hiệu số. Tuy nhiên có thể sử dụng nó theo kiểu kết nối từ xa theo đường điện thoại

II.2.6. Multiplexor - Demultiplexor

Bộ dồn kênh có chức năng tổ hợp nhiều tín hiệu để cùng gửi trên một đường truyền. Đương nhiên tại nơi nhận cần phải tách kênh.

II.2.7. Router

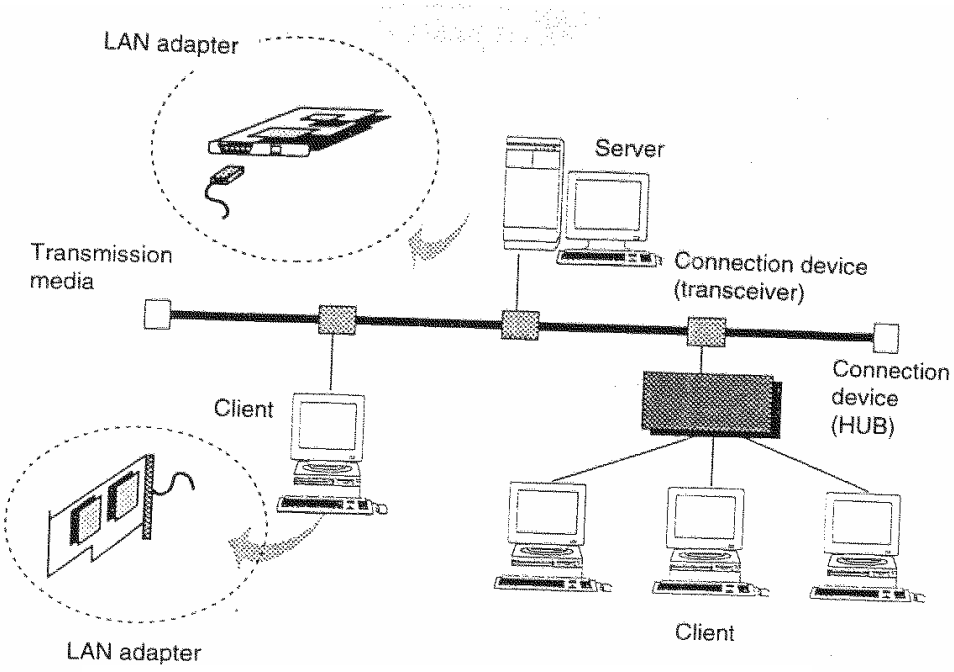
Router là một thiết bị không phải để ghép nối giữa các thiết bị trong một mạng cục bộ mà dùng để ghép nối các mạng cục bộ với nhau thành mạng rộng. Router thực sự là một máy tính làm nhiệm vụ chọn đường cho các gói tin hướng ra ngoài.

Khác với repeaters và bridges, router là thiết bị kết nối mạng độc lập phần cứng, nó được dùng để kết nối các mạng có cùng chung giao thức. Chức năng cơ bản nhất của router là cung cấp một môi trường chuyển mạch gói (packet switching) đáng tin cậy để lưu trữ và truyền số liệu. Để thực hiện điều đó, nó thiết lập các thông tin về các đường truyền hiện có trong mạng, và khi cần nó sẽ cung cấp hai hay nhiều đường truyền giữa hai mạng con bất kỳ tạo ra khả năng mềm dẻo trong việc tìm đường đi hợp lý nhất về một phương diện nào đó.

III.3. Một số kiểu nối mạng thông dụng và các chuẩn

III.3.1.Các thành phần thông thường trên một mạng cục bộ gồm có

- Các máy chủ cung cấp dịch vụ (server)
- Các máy trạm cho người làm việc (workstation)
- Đường truyền (cáp nối)
- Card giao tiếp giữa máy tính và đường truyền (network interface card)
- Các thiết bị nối (connection device)



Hình 9. Cấu hình của một mạng cục bộ

Hai yếu tố được quan tâm hàng đầu khi kết nối mạng cục bộ là tốc độ trong mạng và bán kính mạng. Tên các kiểu mạng dùng theo giao thức CSMA/CD cũng thể hiện điều này. Sau đây là một số kiểu kết nối đó với tốc độ 10 Mb/s khá thông dụng trong thời gian qua và một số thông số kỹ thuật:

Chuẩn	IEEE 802.3		
Kiểu	10BASE5	10BASE2	10BASE-T
Kiểu cáp	Cáp đồng trục	Cáp đồng trục	Cáp UTP
Tốc độ	10 Mb/s		
Độ dài cáp tối đa	500 m/segment	185 m/segment	100 m kể từ HUB
Số các thực thể truyền thông	100 host /segment	30 host / segment	Số cổng của HUB

III.3.2. Kiểu 10BASE5:

Là chuẩn CSMA/CD có tốc độ 10Mb và bán kính 500 m. Kiểu này dùng cáp đồng trục loại thick ethernet (cáp đồng trục béo) với tranceiver. Có thể kết nối vào mạng khoảng 100 máy

Đặc điểm của chuẩn 10BASE 5

Tốc độ tối đa	10 Mbps
Chiều dài tối đa của đoạn cáp của một phân đoạn (segment)	500 m
Số trạm tối đa trên mỗi đoạn	100
Khoảng cách giữa các trạm	>=2,5 m (bội số của 2,5 m (giảm thiểu hiện tượng giao thoa do sóng đứng trên các đoạn ?))
Khoảng cách tối đa giữa máy trạm và đường trục chung	50 m
Số đoạn kết nối tối đa	2 (=>tối đa có 3 phân đoạn)
Tổng chiều dài tối đa đoạn kết nối (có thể là một đoạn kết nối khi có hai phân đoạn, hoặc hai đoạn kết nối khi có ba phân đoạn)	1000 m
Tổng số trạm + các bộ lặp Repeater	Không quá 1024
Chiều dài tối đa	3*500+1000=2500 m

III.3.3. Kiểu 10BASE2:

Là chuẩn CSMA/CD có tốc độ 10Mb và bán kính 200 m. Kiểu này dùng cáp đồng trục loại thin ethernet với đầu nối BNC. Có thể kết nối vào mạng khoảng 30 máy

III.3.5. Kiểu 10BASE-F

Dùng cab quang (Fiber cab), chủ yếu dùng nối các thiết bị xa nhau, tạo dựng đường trục xương sống (backborn) để nối các mạng LAN xa nhau (2-10 km)

Chương 2 : Giới thiệu giao thức TCP/IP

Chương hai cung cấp các kiến thức liên quan đến TCP/IP và địa chỉ IP. Giao thức TCP/IP trở thành giao thức mạng phổ biến nhất nhờ sự phát triển không ngừng của mạng Internet. Các mạng máy tính của các cơ quan, tổ chức, công ty hầu hết đều sử dụng TCP/IP làm giao thức mạng nhờ tính dễ mở rộng và qui hoạch của nó. Đồng thời, do sự phát triển của mạng Internet nên nhu cầu kết nối ra Internet và sử dụng TCP/IP đã trở nên thiết yếu cho mọi đối tượng

Chương này đòi hỏi các học viên phải quen thuộc với các kiến thức cơ bản về hệ nhị phân, các khái niệm bit, byte, chuyển đổi nhị phân, thập phân. Các cách biểu diễn cấu trúc gói tin theo dạng trường bit, byte cũng yêu cầu học viên phải có được hiểu biết cơ sở về kỹ thuật thông tin truyền thông.

I.1. Giao thức IP

I.1.1. Họ giao thức TCP/IP

Sự ra đời của họ giao thức TCP/IP gắn liền với sự ra đời của Internet mà tiền thân là mạng **ARPA**net (**A**dvanced **R**esearch **P**rojects **A**gency) do Bộ Quốc phòng Mỹ tạo ra. Đây là bộ giao thức được dùng rộng rãi nhất vì tính mở của nó. Điều đó có nghĩa là bất cứ máy nào dùng bộ giao thức TCP/IP đều có thể nối được vào Internet. Hai giao thức được dùng chủ yếu ở đây là **TCP** (**T**ransmission **C**ontrol **P**rotocol) và **IP** (**I**nternet **P**rotocol). Chúng đã nhanh chóng được đón nhận và phát triển bởi nhiều nhà nghiên cứu và các hãng công nghiệp máy tính với mục đích xây dựng và phát triển một mạng truyền thông mở rộng khắp thế giới mà ngày nay chúng ta gọi là Internet. Phạm vi phục vụ của Internet không còn dành cho quân sự như **ARPA**net nữa mà nó đã mở rộng lĩnh vực cho mọi loại đối tượng sử dụng, trong đó tỷ lệ quan trọng nhất vẫn thuộc về giới nghiên cứu khoa học và giáo dục.

Khái niệm *giao thức (*protocol) là một khái niệm cơ bản của mạng thông tin máy tính. Có thể hiểu một cách khái quát rằng đó chính là tập hợp tất cả các qui tắc cần thiết (các thủ tục, các khuôn dạng dữ liệu, các cơ chế phụ trợ...) cho phép các thao tác trao đổi thông tin trên mạng được thực hiện một cách chính xác và an toàn. Có rất nhiều họ giao thức đang được thực hiện trên mạng thông

tin máy tính hiện nay như IEEE 802.X dùng trong mạng cục bộ, CCITT X25 dùng cho mạng diện rộng và đặc biệt là họ giao thức chuẩn của ISO (tổ chức tiêu chuẩn hóa quốc tế) dựa trên mô hình tham chiếu bảy tầng cho việc nối kết các hệ thống mở. Gần đây, do sự xâm nhập của Internet vào Việt nam, chúng ta được làm quen với họ giao thức mới là TCP/IP mặc dù chúng đã xuất hiện từ hơn 20 năm trước đây.

TCP/IP (Transmission Control Protocol/ Internet Protocol) TCP/IP là một họ giao thức cùng làm việc với nhau để cung cấp phương tiện truyền thông liên mạng được hình thành từ những năm 70.

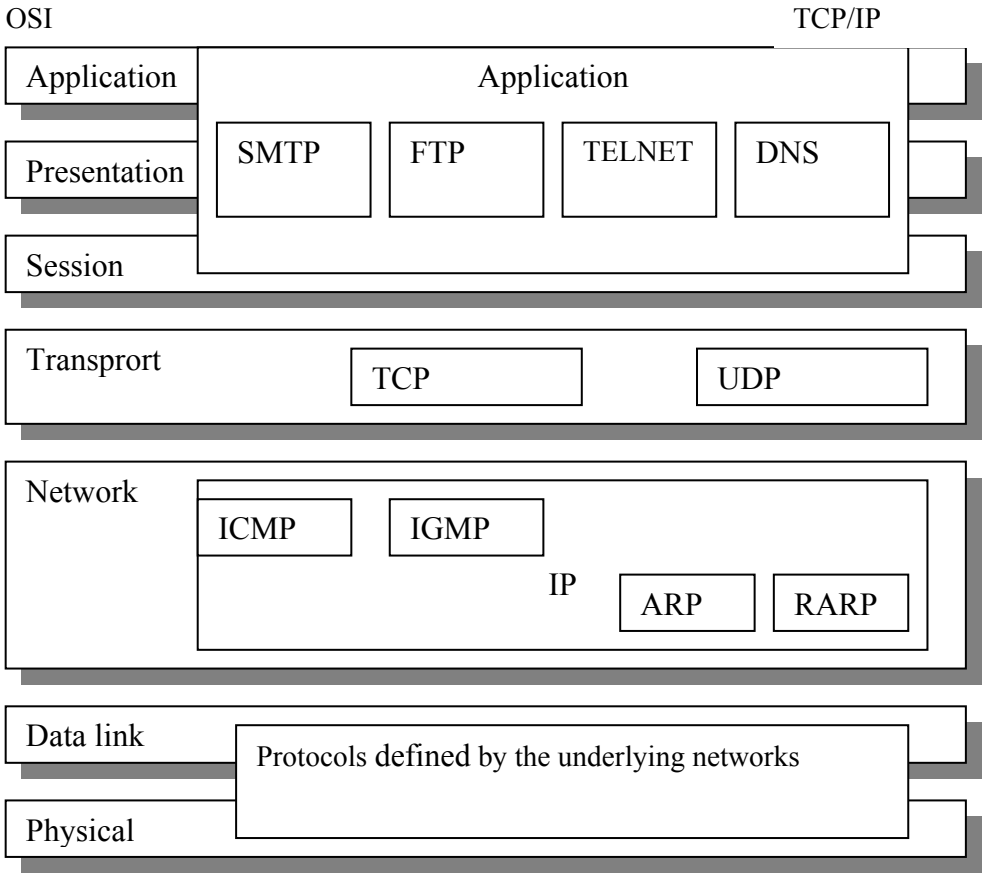
Đến năm 1981, TCP/IP phiên bản 4 mới hoàn tất và được phổ biến rộng rãi cho toàn bộ những máy tính sử dụng hệ điều hành UNIX. Sau này Microsoft cũng đã đưa TCP/IP trở thành một trong những giao thức căn bản của hệ điều hành Windows 9x mà hiện nay đang sử dụng.

Đến năm 1994, một bản thảo của phiên bản IPv6 được hình thành với sự cộng tác của nhiều nhà khoa học thuộc các tổ chức Internet trên thế giới để cải tiến những hạn chế của IPv4.

Khác với mô hình ISO/OSI tầng liên mạng sử dụng giao thức kết nối mạng "không liên kết" (connectionless) IP, tạo thành hạt nhân hoạt động của Internet. Cùng với các thuật toán định tuyến RIP, OSPF, BGP, tầng liên mạng IP cho phép kết nối một cách mềm dẻo và linh hoạt các loại mạng "vật lý" khác nhau như: Ethernet, Token Ring , X.25...

Giao thức trao đổi dữ liệu "có liên kết" (connection - oriented) TCP được sử dụng ở tầng vận chuyển để đảm bảo tính chính xác và tin cậy việc trao đổi dữ liệu dựa trên kiến trúc kết nối "không liên kết" ở tầng liên mạng IP.

Các giao thức hỗ trợ ứng dụng phổ biến như truy nhập từ xa (telnet), chuyển tệp (FTP), dịch vụ World Wide Web (HTTP), thư điện tử (SMTP), dịch vụ tên miền (DNS) ngày càng được cài đặt phổ biến như những bộ phận cấu thành của các hệ điều hành thông dụng như UNIX (và các hệ điều hành chuyên dụng cùng họ của các nhà cung cấp thiết bị tính toán như AIX của IBM, SINIX của Siemens, Digital UNIX của DEC), Windows9x/NT, Novell Netware,...



Hình 2.1 Mô hình OSI và mô hình kiến trúc của TCP/IP

Như vậy, TCP tương ứng với lớp 4 cộng thêm một số chức năng của lớp 5 trong họ giao thức chuẩn ISO/OSI. Còn IP tương ứng với lớp 3 của mô hình OSI.

Trong cấu trúc bốn lớp của TCP/IP, khi dữ liệu truyền từ lớp ứng dụng cho đến lớp vật lý, mỗi lớp đều cộng thêm vào phần điều khiển của mình để đảm bảo cho việc truyền dữ liệu được chính xác. Mỗi thông tin điều khiển này được gọi là một *header* và được đặt ở trước phần dữ liệu được truyền. Mỗi lớp xem tất cả các thông tin mà nó nhận được từ lớp trên là dữ liệu, và đặt phần thông tin điều khiển *header* của nó vào trước phần thông tin này. Việc cộng thêm vào các *header* ở mỗi lớp trong quá trình truyền tin được gọi là *encapsulation*. Quá trình nhận dữ liệu diễn ra theo chiều ngược lại: mỗi lớp sẽ tách ra phần *header* trước khi truyền dữ liệu lên lớp trên.

Mỗi lớp có một cấu trúc dữ liệu riêng, độc lập với cấu trúc dữ liệu được dùng ở lớp trên hay lớp dưới của nó. Sau đây là giải thích một số khái niệm thường gặp.

Stream là dòng số liệu được truyền trên cơ sở đơn vị số liệu là Byte.

Số liệu được trao đổi giữa các ứng dụng dùng TCP được gọi là *stream*, trong khi dùng UDP, chúng được gọi là *message*.

Mỗi gói số liệu TCP được gọi là *segment* còn UDP định nghĩa cấu trúc dữ liệu của nó là *packet*.

Lớp Internet xem tất cả các dữ liệu như là các khối và gọi là *datagram*. Bộ giao thức TCP/IP có thể dùng nhiều kiểu khác nhau của lớp mạng dưới cùng, mỗi loại có thể có một thuật ngữ khác nhau để truyền dữ liệu.

Phần lớn các mạng kết cấu phần dữ liệu truyền đi dưới dạng các *packets* hay là các *frames*.

Application	Stream
Transport	Segment/datagram
Internet	Datagram
Network Access	Frame

Cấu trúc dữ liệu tại các lớp của TCP/IP

Lớp truy nhập mạng

Network **A**ccess **L**ayer là lớp thấp nhất trong cấu trúc phân bậc của TCP/IP. Những giao thức ở lớp này cung cấp cho hệ thống phương thức để truyền dữ liệu trên các tầng vật lý khác nhau của mạng. Nó định nghĩa cách thức truyền các khối dữ liệu (datagram) IP. Các giao thức ở lớp này phải biết chi tiết các phần cấu trúc vật lý mạng ở dưới nó (bao gồm cấu trúc gói số liệu, cấu trúc địa chỉ...) để định dạng được chính xác các gói dữ liệu sẽ được truyền trong từng loại mạng cụ thể.

So sánh với cấu trúc OSI/OSI, lớp này của TCP/IP tương đương với hai lớp Datalink, và Physical.

Chức năng định dạng dữ liệu sẽ được truyền ở lớp này bao gồm việc nhúng các gói dữ liệu IP vào các *frame* sẽ được truyền trên mạng và việc ánh xạ các địa chỉ IP vào địa chỉ vật lý được dùng cho mạng.

Lớp liên mạng

Internet Layer là lớp ở ngay trên lớp Network Access trong cấu trúc phân lớp của TCP/IP. Internet Protocol là giao thức trung tâm của TCP/IP và là phần quan trọng nhất của lớp Internet. IP cung cấp các gói lưu chuyển cơ bản mà thông qua đó các mạng dùng TCP/IP được xây dựng.

I.1.2. Chức năng chính của - Giao thức liên mạng IP(v4)

Trong phần này trình bày về giao thức IPv4 (để cho thuận tiện ta viết IP có nghĩa là đề cập đến IPv4).

Mục đích chính của IP là cung cấp khả năng kết nối các mạng con thành liên mạng để truyền dữ liệu. IP cung cấp các chức năng chính sau:

- Định nghĩa cấu trúc các gói dữ liệu là đơn vị cơ sở cho việc truyền dữ liệu trên Internet.

- Định nghĩa phương thức đánh địa chỉ IP.

- Truyền dữ liệu giữa tầng vận chuyển và tầng mạng .

- Định tuyến để chuyển các gói dữ liệu trong mạng.

- Thực hiện việc phân mảnh và hợp nhất (fragmentation -reassembly) các gói dữ liệu và nhúng / tách chúng trong các gói dữ liệu ở tầng liên kết.

I.2. Địa chỉ IP

Sơ đồ địa chỉ hoá để định danh các trạm (host) trong liên mạng được gọi là địa chỉ IP. Mỗi địa chỉ IP có độ dài 32 bits (đối với IP4) được tách thành 4 vùng (mỗi vùng 1 byte), có thể được biểu thị dưới dạng thập phân, bát phân, thập lục phân hoặc nhị phân. Cách viết phổ biến nhất là dùng ký pháp thập phân có dấu chấm để tách giữa các vùng. Mục đích của địa chỉ IP là để định danh duy nhất cho một host bất kỳ trên liên mạng.

- Lớp B cho phép định danh tới 16384 mạng (10111111.11111111.host.host), với tối đa 65535 host trên mỗi mạng. Dạng của lớp B (network number. Network number.host.host). Nếu dùng ký pháp thập phân cho phép 128 đến 191 cho vùng đầu, 1 đến 255 cho các vùng còn lại

- Lớp C cho phép định danh tới 2.097.150 mạng và tối đa 254 host cho mỗi mạng. Lớp này được dùng cho các mạng có ít trạm. Lớp C sử dụng 3 bytes đầu định danh địa chỉ mạng (110xxxxx). Dạng của lớp C (network number. Network number.Network number.host). Nếu dùng dạng ký pháp thập phân cho phép 129 đến 233 cho vùng đầu và từ 1 đến 255 cho các vùng còn lại.

- Lớp D dùng để gửi IP datagram tới một nhóm các host trên một mạng. Tất cả các số lớn hơn 233 trong trường đầu là thuộc lớp D

- Lớp E dự phòng để dùng trong tương lai

Như vậy địa chỉ mạng cho lớp: A: từ 1 đến 126 cho vùng đầu tiên, 127 dùng cho địa chỉ loopback, B từ 128.1.0.0 đến 191.255.0.0, C từ 192.1.0.0 đến 233.255.255.0

Ví dụ:

192.1.1.1 địa chỉ lớp C có địa chỉ mạng 192.1.1.0, địa chỉ host là 1

200.6.5.4 địa chỉ lớp C có địa chỉ mạng 200.6.5, địa chỉ mạng là 4

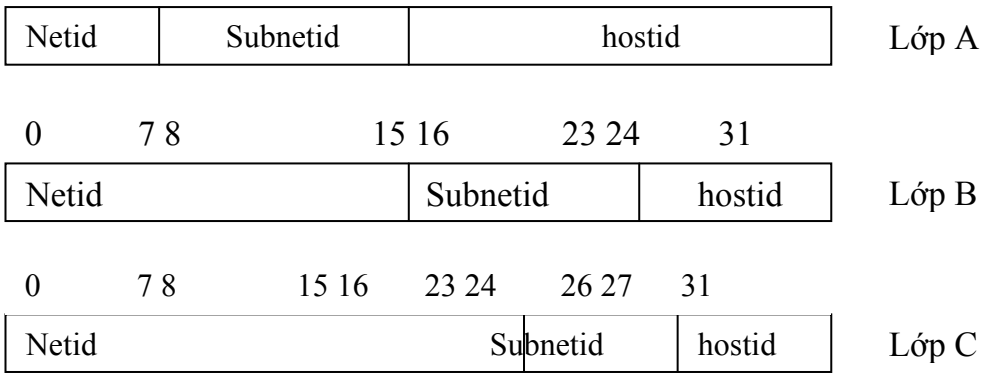
150.150.5.6 địa chỉ lớp B có địa chỉ mạng 150.150.0.0, địa chỉ host là 5.6

9.6.7.8 địa chỉ lớp A có địa chỉ mạng 9.0.0.0, địa chỉ host là 6.7.8

128.1.0.1 địa chỉ lớp B có địa chỉ mạng 128.1.0.0, địa chỉ host là 0.1

Subneting

Trong nhiều trường hợp, một mạng có thể được chia thành nhiều mạng con (subnet), lúc đó có thể đưa thêm các vùng subnetid để định danh các mạng con. Vùng subnetid được lấy từ vùng hostid, cụ thể đối với 3 lớp A, B, C như sau:



Hình 2.5 Bổ sung vùng subnetid

Ví dụ:

17.1.1.1 địa chỉ lớp A có địa chỉ mạng 17, địa chỉ subnet 1, địa chỉ host 1.1

129.1.1.1 địa chỉ lớp B có địa chỉ mạng 129.1, địa chỉ subnet 1, địa chỉ host 1.

I.3. Cấu trúc gói dữ liệu IP

IP là giao thức cung cấp dịch vụ truyền thông theo kiểu "không liên kết" (connectionless). Phương thức không liên kết cho phép cặp trạm truyền nhận không cần phải thiết lập liên kết trước khi truyền dữ liệu và do đó không cần phải giải phóng liên kết khi không còn nhu cầu truyền dữ liệu nữa. Phương thức kết nối "không liên kết" cho phép thiết kế và thực hiện giao thức trao đổi dữ liệu đơn giản (không có cơ chế phát hiện và khắc phục lỗi truyền). Cũng chính vì vậy độ tin cậy trao đổi dữ liệu của loại giao thức này không cao.

Các gói dữ liệu IP được định nghĩa là các datagram. Mỗi datagram có phần tiêu đề (header) chứa các thông tin cần thiết để chuyển dữ liệu (ví dụ địa chỉ IP của trạm đích). Nếu địa chỉ IP đích là địa chỉ của một trạm nằm trên cùng một mạng IP với trạm nguồn thì các gói dữ liệu sẽ được chuyển thẳng tới đích; nếu địa chỉ IP đích không nằm trên cùng một mạng IP với máy nguồn thì các gói dữ liệu sẽ được gửi đến một máy trung chuyển, IP gateway để chuyển tiếp. IP gateway là một thiết bị mạng IP đảm nhận việc lưu chuyển các gói dữ liệu IP giữa hai mạng IP khác nhau. Hình 2.3 mô tả cấu trúc gói số liệu IP.

- VER (4 bits) : chỉ Version hiện hành của IP được cài đặt.

- IHL (4 bits) : chỉ độ dài phần tiêu đề (Internet Header Length) của datagram, tính theo đơn vị word (32 bits). Nếu không có trường này thì độ dài mặc định của phần tiêu đề là 5 từ.

- Type of service (8 bits): cho biết các thông tin về loại dịch vụ và mức ưu tiên của gói IP, có dạng cụ thể như sau:

Precedence	D	T	R	Unused

Trong đó:

Precedence (3 bits): chỉ thị về quyền ưu tiên gửi datagram, cụ thể là:

111 Network Control (cao nhất) 011- flash

110 Internetwork Control 010 Immediate

101 CRITIC/ECP 001 Priority

100 Flas Override 000 Routine (thấp nhất)

D (delay) (1 bit) : chỉ độ trễ yêu cầu

D=0 độ trễ bình thường, D=1 độ trễ thấp

T (Throughput) (1 bit) : chỉ số thông lượng yêu cầu

T=1 thông lượng bình thường

T=1 thông lượng cao

R (Reliability) (1 bit): chỉ độ tin cậy yêu cầu

R=0 độ tin cậy bình thường

R=1 độ tin cậy cao

- Total Length (16 bits): chỉ độ dài toàn bộ datagram, kể cả phần header (tính theo đơn vị bytes), vùng dữ liệu của datagram có thể dài tới 65535 bytes.

- Identification (16 bits) : cùng với các tham số khác như (Source Address và Destination Address) tham số này dùng để định danh duy nhất cho một datagram trong khoảng thời gian nó vẫn còn trên liên mạng

- Header checksum (16 bits): mã kiểm soát lỗi sử dụng phương pháp CRC (Cyclic Redundancy Check) dùng để đảm bảo thông tin về gói dữ liệu được truyền đi một cách chính xác (mặc dù dữ liệu có thể bị lỗi). Nếu như việc kiểm tra này thất bại, gói dữ liệu sẽ bị huỷ bỏ tại nơi xác định được lỗi. Cần chú ý là IP không cung cấp một phương tiện truyền tin cậy bởi nó không cung cấp cho ta một cơ chế để xác nhận dữ liệu truyền tại điểm nhận hoặc tại những điểm trung gian. Giao thức IP không có cơ chế Error Control cho dữ liệu truyền đi, không có cơ chế kiểm soát luồng dữ liệu (flow control).

- Source Address (32 bits): địa chỉ của trạm nguồn.

- Destination Address (32 bits): địa chỉ của trạm đích.

- Option (có độ dài thay đổi) sử dụng trong một số trường hợp, nhưng thực tế chúng rất ít dùng. Option bao gồm bảo mật, chức năng định tuyến đặc biệt

- Padding (độ dài thay đổi): vùng đệm, được dùng để đảm bảo cho phần header luôn kết thúc ở một mốc 32 bits

- Data (độ dài thay đổi): vùng dữ liệu có độ dài là bội của 8 bits, tối đa là 65535 bytes.

I.4. Phân mảnh và hợp nhất các gói IP

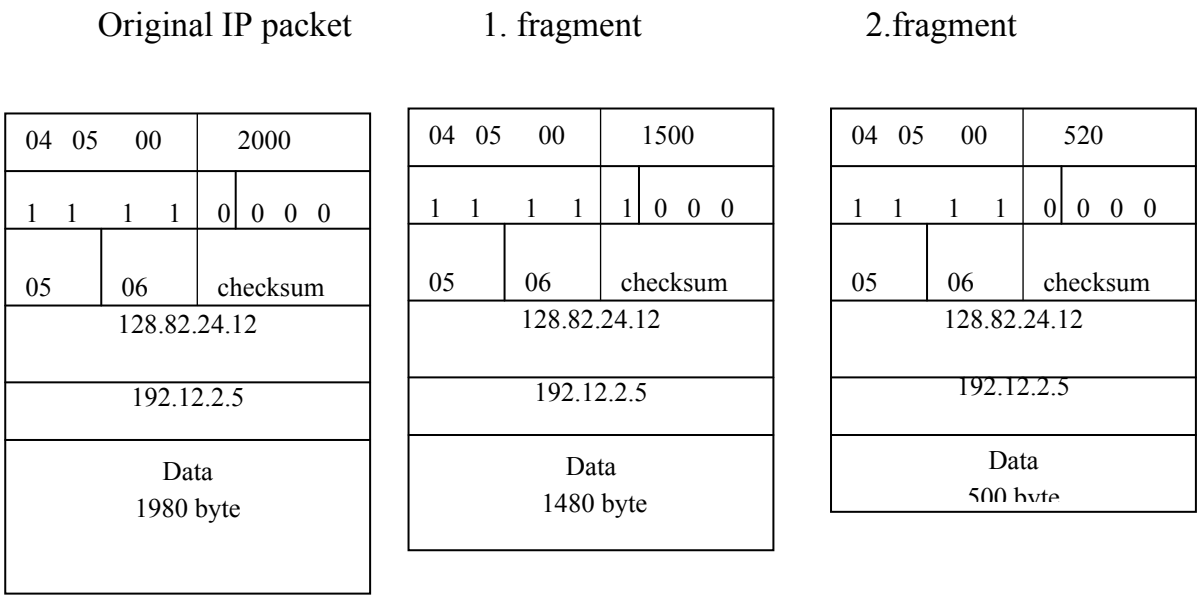
Các gói dữ liệu IP phải được nhúng trong khung dữ liệu ở tầng liên kết dữ liệu tương ứng, trước khi chuyển tiếp trong mạng. Quá trình nhận một gói dữ liệu IP diễn ra ngược lại. Ví dụ, với mạng Ethernet ở tầng liên kết dữ liệu quá trình chuyển một gói dữ liệu diễn ra như sau. Khi gửi một gói dữ liệu IP cho mức Ethernet, IP chuyển cho mức liên kết dữ liệu các thông số địa chỉ Ethernet đích, kiểu khung Ethernet (chỉ dữ liệu mà Ethernet đang mang là của IP) và cuối cùng là gói IP. Tầng liên kết số liệu đặt địa chỉ Ethernet nguồn là địa chỉ kết nối mạng của mình và tính toán giá trị checksum. Trường type chỉ ra kiểu khung là 0x0800 đối với dữ liệu IP. Mức liên kết dữ liệu sẽ chuyển khung dữ liệu theo thuật toán truy nhập Ethernet.

Một gói dữ liệu IP có độ dài tối đa 65536 byte, trong khi hầu hết các tầng liên kết dữ liệu chỉ hỗ trợ các khung dữ liệu nhỏ hơn độ lớn tối đa của gói dữ liệu IP nhiều lần (ví dụ độ dài lớn nhất của một khung dữ liệu Ethernet là

1500 byte). Vì vậy cần thiết phải có cơ chế phân mảnh khi phát và hợp nhất khi thu đối với các gói dữ liệu IP.

Độ dài tối đa của một gói dữ liệu liên kết là MTU (Maximum Transmit Unit). Khi cần chuyển một gói dữ liệu IP có độ dài lớn hơn MTU của một mạng cụ thể, cần phải chia gói số liệu IP đó thành những gói IP nhỏ hơn để độ dài của nó nhỏ hơn hoặc bằng MTU gọi chung là mảnh (fragment). Trong phần tiêu đề của gói dữ liệu IP có thông tin về phân mảnh và xác định các mảnh có quan hệ phụ thuộc để hợp thành sau này.

Ví dụ Ethernet chỉ hỗ trợ các khung có độ dài tối đa là 1500 byte. Nếu muốn gửi một gói dữ liệu IP gồm 2000 byte qua Ethernet, phải chia thành hai gói nhỏ hơn, mỗi gói không quá giới hạn MTU của Ethernet.



Hình 16. Nguyên tắc phân mảnh gói dữ liệu

P dùng cờ MF (3 bit thấp của trường Flags trong phần đầu của gói IP) và trường Flagment offset của gói IP (đã bị phân đoạn) để định danh gói IP đó là một phân đoạn và vị trí của phân đoạn này trong gói IP gốc. Các gói cùng trong chuỗi phân mảnh đều có trường này giống nhau. Cờ MF bằng 1 nếu là gói đầu của chuỗi phân mảnh và 0 nếu là gói cuối của gói đã được phân mảnh.

Quá trình hợp nhất diễn ra ngược lại với quá trình phân mảnh. Khi IP nhận được một gói phân mảnh, nó giữ phân mảnh đó trong vùng đệm, cho đến khi nhận được hết các gói IP trong chuỗi phân mảnh có cùng trường định danh. Khi phân mảnh đầu tiên được nhận, IP khởi động một bộ đếm thời gian (giá trị

ngầm định là 15s). IP phải nhận hết các phân mảnh kế tiếp trước khi đồng hồ tắt. Nếu không IP phải huỷ tất cả các phân mảnh trong hàng đợi hiện thời có cùng trường định danh.

Khi IP nhận được hết các phân mảnh, nó thực hiện hợp nhất các gói phân mảnh thành các gói IP gốc và sau đó xử lý nó như một gói IP bình thường. IP thường chỉ thực hiện hợp nhất các gói tại hệ thống đích của gói.

I.5. Định tuyến IP

Có hai loại định tuyến:

- Định tuyến trực tiếp: Định tuyến trực tiếp là việc xác định đường nối giữa hai trạm làm việc trong cùng một mạng vật lý.

- Định tuyến không trực tiếp. Định tuyến không trực tiếp là việc xác định đường nối giữa hai trạm làm việc không nằm trong cùng một mạng vật lý và vì vậy, việc truyền tin giữa chúng phải được thực hiện thông qua các trạm trung gian là các gateway.

Để kiểm tra xem trạm đích có nằm trên cùng mạng vật lý với trạm nguồn hay không, người gửi phải tách lấy phần địa chỉ mạng trong phần địa chỉ IP. Nếu hai địa chỉ này có địa chỉ mạng giống nhau thì datagram sẽ được truyền đi trực tiếp; ngược lại phải xác định một gateway, thông qua gateway này chuyển tiếp các datagram.

Khi một trạm muốn gửi các gói dữ liệu đến một trạm khác thì nó phải đóng gói datagram vào một khung (frame) và gửi các frame này đến gateway gần nhất. Khi một frame đến một gateway, phần datagram đã được đóng gói sẽ được tách ra và IP routing sẽ chọn gateway tiếp dọc theo đường dẫn đến đích. Datagram sau đó lại được đóng gói vào một frame khác và gửi đến mạng vật lý để gửi đến gateway tiếp theo trên đường truyền và tiếp tục như thế cho đến khi datagram được truyền đến trạm đích.

Chiến lược định tuyến: Trong thuật ngữ truyền thống của TCP/IP chỉ có hai kiểu thiết bị, đó là các cổng truyền (gateway) và các trạm (host). Các cổng truyền có vai trò gửi các gói dữ liệu, còn các trạm thì không. Tuy nhiên khi một trạm được nối với nhiều mạng thì nó cũng có thể định hướng cho việc lưu chuyển các gói dữ liệu giữa các mạng và lúc này nó đóng vai trò hoàn toàn như một gateway.

khác thì nó cần được phân mảnh ra thành các gói nhỏ hơn, gọi là *fragment.* Quá trình này gọi là quá trình phân mảnh. Dạng của một *fragment* cũng giống như dạng của một gói dữ liệu thông thường. Từ thứ hai trong phần *header* chứa các thông tin để xác định mỗi *fragment* và cung cấp các thông tin để hợp nhất các fragment này lại thành các gói như ban đầu. Trường *identification* dùng để xác định *fragment* này là thuộc về gói dữ liệu nào.

I.6. Một số giao thức điều khiển

I.6.1. Giao thức ICMP

ICMP ((Internet Control Message Protocol) là một giao thức điều khiển của mức 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 bộ giao thức TCP/IP. Ví dụ:

- Điều khiển lưu lượng dữ liệu (Flow control): khi các gói dữ liệu đến quá nhanh, thiết bị đích hoặc thiết bị định tuyến ở giữa sẽ gửi một thông điệp ICMP trở lại thiết bị gửi, yêu cầu thiết bị gửi tạm thời ngừng việc gửi dữ liệu.

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

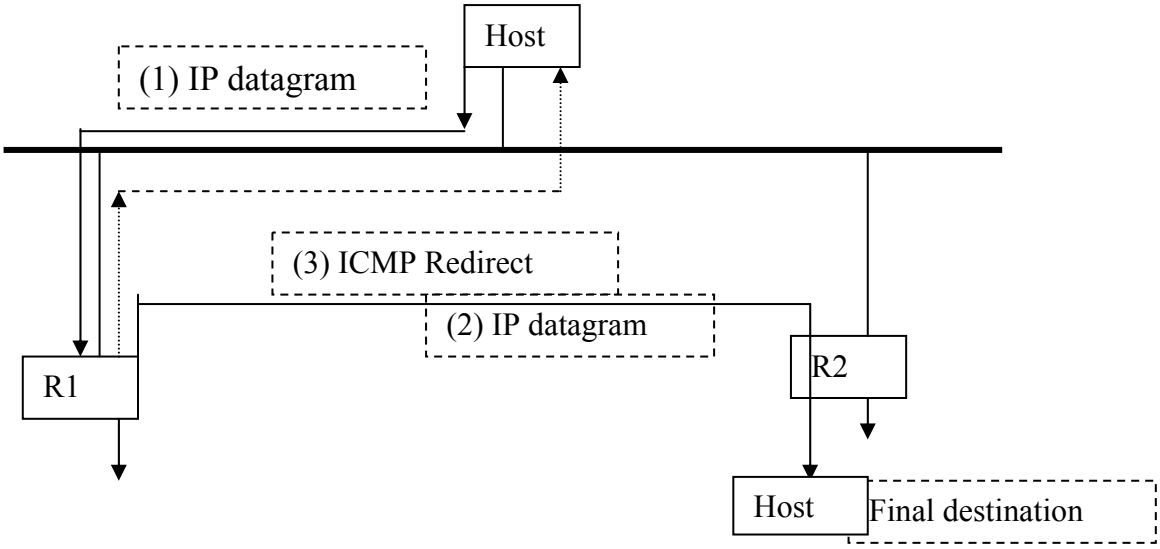
- Định hướng lại các tuyến đường: một thiết bị định tuyến sẽ gửi một thông điệp ICMP "định tuyến lại" (Redirect Router) để thông báo với một trạm là nên dùng thiết bị định tuyến khác để tới thiết bị đích. Thông điệp này có thể chỉ được dùng khi trạm nguồn ở trên cùng một mạng với cả hai thiết bị định tuyến.

- Kiểm tra các trạm ở xa: một trạm có thể gửi một thông điệp ICMP "Echo" để kiểm tra xem một trạm có hoạt động hay không.

Sau đây là mô tả một ứng dụng của giao thức ICMP thực hiện việc định tuyến lại (Redirect):

Ví dụ: giả sử host gửi một gói dữ liệu IP tới Router R1. Router R1 thực hiện việc quyết định tuyến vì R1 là router mặc định của host đó. R1 nhận gói dữ liệu và tìm trong bảng định tuyến và nó tìm thấy một tuyến tới R2. Khi R1 gửi gói dữ liệu tới R2 thì R1 phát hiện ra rằng nó đang gửi gói dữ liệu đó ra ngoài trên cùng một giao diện mà gói dữ liệu đó đã đến (là giao diện mạng

LAN mà cả host và hai Router nối đến). Lúc này R1 sẽ gửi một thông báo ICMP Redirect Error tới host, thông báo cho host nên gửi các gói dữ liệu tiếp theo đến R2 thì tốt hơn.



Tác dụng của ICMP Redirect là để cho mọt host với nhận biết tối thiểu về định tuyến xây dựng lên một bảng định tuyến tốt hơn theo thời gian. Host đó có thể bắt đầu với một tuyến mặc định (có thể R1 hoặc R2 như ví dụ trên) và bất kỳ lần nào tuyến mặc định này được dùng với host đó đến R2 thì nó sẽ được Router mặc định gửi thông báo Redirect để cho phép host đó cập nhật bảng định tuyến của nó một cách phù hợp hơn. Khuôn dạng của thông điệp ICMP redirect như sau:

0 7 8	15 16	31
type (5)	Code(0-3)	Checksum
Địa chỉ IP của Router mặc định		
IP header (gồm option) và 8 bytes đầu của gói dữ liệu IP nguồn		

Dạng thông điệp ICMP redirect

Có bốn loại thông báo ICMP redirect khác nhau với các giá trị mã (code) như bảng sau:

Code	Description
0	Redirect cho mạng
1	Redirect cho host
2	Redirect cho loại dịch vụ (TOS) và mạng
3	Redirect cho loại dịch vụ và host

Các loại định hướng lại của gói dữ liệu ICMP

Redirect chỉ xảy ra khi cả hai Router R1 và R2 cùng nằm trên một mạng với host nhận direct đó.

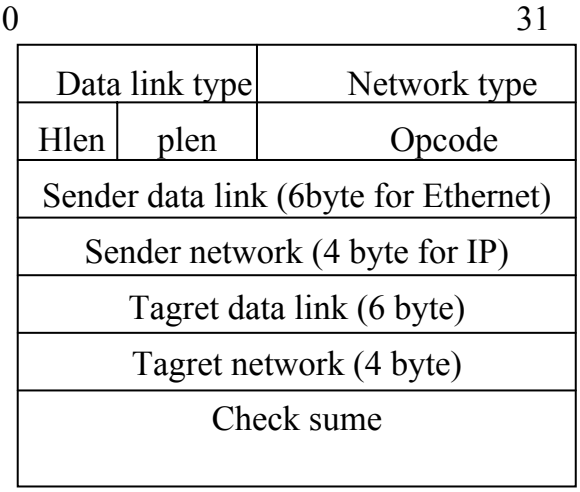
I.6.2. Giao thức ARP và giao thức RARP

Địa chỉ IP được dùng để định danh các host và mạng ở tầng mạng của mô hình OSI, chúng không phải là các địa chỉ vật lý (hay địa chỉ MAC) của các trạm đó trên một mạng cục bộ (Ethernet, Token Ring,...). Trên một mạng cục bộ hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau. Như vậy vấn đề đặt ra là phải thực hiện ánh xạ giữa địa chỉ IP (32 bits) và địa chỉ vật lý (48 bits) của một trạm. Giao thức ARP (Address Resolution Protocol) đã được xây dựng để chuyển đổi từ địa chỉ IP sang địa chỉ vật lý khi cần thiết. Ngược lại, giao thức RARP (Reverse Address Resolution Protocol) được dùng để chuyển đổi địa chỉ vật lý sang địa chỉ IP. Các giao thức ARP và RARP không phải là bộ phận của IP mà IP sẽ dùng đến chúng khi cần.

Giao thức ARP

Giao thức TCP/IP sử dụng ARP để tìm địa chỉ vật lý của trạm đích. Ví dụ khi cần gửi một gói dữ liệu IP cho một hệ thống khác trên cùng một mạng vật lý Ethernet, hệ thông gửi cần biết địa chỉ Ethernet của hệ thống đích để tầng liên kết dữ liệu xây dựng khung gói dữ liệu.

Thông thường, mỗi hệ thống lưu giữ và cập nhật bảng thích ứng địa chỉ IP-MAC tại chỗ (còn được gọi là bảng ARP cache). Bảng thích ứng địa chỉ được cập nhật bởi người quản trị hệ thống hoặc tự động bởi giao thức ARP sau mỗi lần ánh xạ được một địa chỉ thích ứng mới. Khuôn dạng của gói dữ liệu ARP được mô tả trong hình

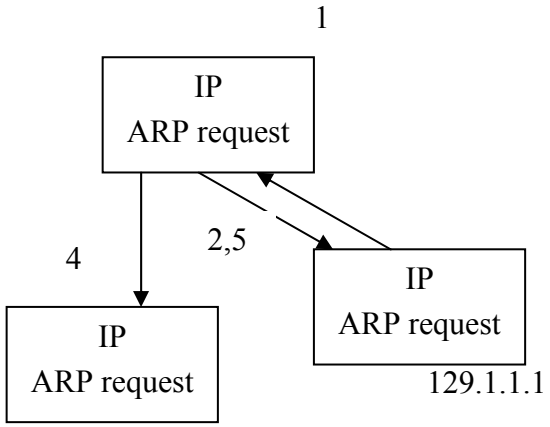


Mô tả khuôn dạng của gói ARP

- Data link type: cho biết loại công nghệ mạng mức liên kết (ví dụ đối với mạng Ethernet trường này có giá trị 01).
- Network type: cho biết loại mạng (ví dụ đối với mạng IPv4, trường này có giá trị 0800_{16}).
- Hlen (hardware length): độ dài địa chỉ mức liên kết (6 byte).
- Plen (Protocol length): cho biết độ dài địa chỉ mạng (4 byte)
- Opcode (operation code): mã lệnh yêu cầu: ; mã lệnh trả lời .
- Sender data link: địa chỉ mức liên kết của thiết bị phát gói dữ liệu này.
- Sender network : địa chỉ IP của thiết bị phát.
- Tagret data link: trong yêu cầu đây là địa chỉ mức liên kết cần tìm (thông thường được điền 0 bởi thiết bị gửi yêu cầu); trong trả lời đây là địa chỉ mức liên kết của thiết bị gửi yêu cầu.
- Tagret network : trong yêu cầu đây là địa chỉ IP mà địa chỉ mức liên kết tương ứng cần tìm; trong trả lời đây là địa chỉ IP của thiết bị gửi yêu cầu.

Mỗi khi cần tìm thích ứng địa chỉ IP - MAC, có thể tìm địa chỉ MAC tương ứng với địa IP đó trước tiên trong bảng địa chỉ IP - MAC ở mỗi hệ

thống. Nếu không tìm thấy, có thể sử dụng giao thức ARP để làm việc này. Trạm làm việc gửi yêu cầu ARP (ARP_Request) tìm thích ứng địa chỉ IP - MAC đến máy phục vụ ARP - server. Máy phục vụ ARP tìm trong bảng thích ứng 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. Tóm lại tiến trình của ARP được mô tả như sau



Tiến trình ARP

1. IP yêu cầu địa chỉ MAC.
2. Tìm kiếm trong bảng ARP.
3. Nếu tìm thấy sẽ trả lại địa chỉ MAC.
4. Nếu không tìm thấy, tạo gói ARP yêu cầu và gửi tới tất cả các trạm.
5. Tuỳ theo gói dữ liệu trả lời, ARP cập nhật vào bảng ARP và gửi địa chỉ MAC đó cho IP.

Giao thức RARP

Reverse ARP (Reverse Address Resolution Protocol) là giao thức giải thích ứng địa chỉ AMC - IP. Quá trình này ngược lại với quá trình giải thích ứng địa chỉ IP - MAC mô tả ở trên, nghĩa là cho trước địa chỉ mức liên kết, tìm địa chỉ IP tương ứng.

I.2. Giao thức lớp chuyển tải (Transport Layer)

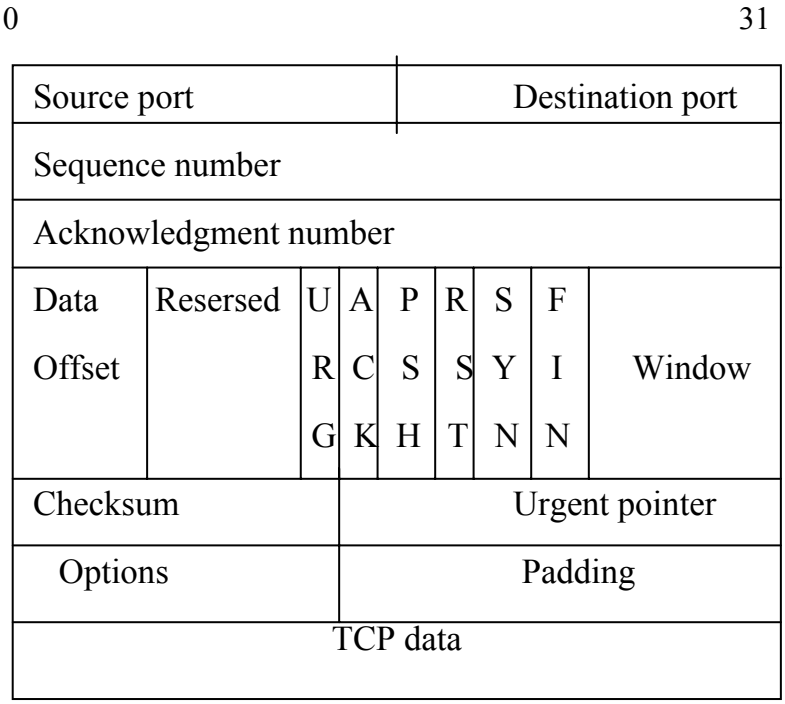
I.2.1. Giao thức TCP

TCP (Transmission Control Protocol) là một giao thức "có liên kết" (connection - oriented), nghĩa là cần thiết lập liên kết (logic), giữa một cặp thực thể TCP trước khi chúng trao đổi dữ liệu với nhau.

TCP cung cấp khả năng truyền dữ liệu một cách an toàn giữa các máy trạm trong hệ thống các mạng. Nó cung cấp thêm các chức năng nhằm kiểm tra tính chính xác của dữ liệu khi đến và bao gồm cả việc gửi lại dữ liệu khi có lỗi xảy ra. TCP cung cấp các chức năng chính sau:

1. Thiết lập, duy trì, kết thúc liên kết giữa hai quá trình.
2. Phân phát gói tin một cách tin cậy.
3. Đánh số thứ tự (sequencing) các gói dữ liệu nhằm truyền dữ liệu một cách tin cậy.
4. Cho phép điều khiển lỗi.
5. Cung cấp khả năng đa kết nối với các quá trình khác nhau giữa trạm nguồn và trạm đích nhất định thông qua việc sử dụng các cổng.
6. Truyền dữ liệu sử dụng cơ chế song công (full-duplex).

I.2.2 Cấu trúc gói dữ liệu TCP



Khuôn dạng của TCP segment

- Source port (16 bits) : số hiệu cổng của trạm nguồn

- Destination port (16 bits) : số hiệu cổng của trạm đích

- Sequence Number (32 bits): số hiệu của 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) và byte dữ liệu đầu tiên là ISN +1.

- Acknowlegment: vị trí tương đối của byte cuối cùng đã nhận đúng bởi thực thể gửi gói ACK cộng thêm 1. Giá trị của trường này còn được gọi là số tuần tự thu. Trường này được kiểm tra chỉ khi bit ACK=1.

- Data offset (4 bits) : số tượng từ 32 bit trong TCP header. Tham số này chỉ ra vị trí bắt đầu của vùng dữ liệu

- Reserved (6 bits) : dành để dùng trong tương lai. Phải được thiết lập là 0.

- Control bits : các bit điều khiển

  - URG : vùng con trỏ khẩn (Urgent Pointer) có hiệu lực.

  - ACK: vùng báo nhận (ACK number) có hiệu lực.

- PSH : chức năng Push. PSH=1 thực thể nhận phải chuyển dữ liệu này cho ứng dụng tức thời.

  - RST : thiết lập lại (reset) kết nối.

  - SYN : đồng bộ hoá các số hiệu tuần tự, dùng để thiết lập kết nối TCP.

  - FIN : thông báo thực thể gửi đã kết thúc gửi dữ liệu.

- Window (16 bits): cấp phát credit để kiểm soát luồng dữ liệu (cơ chế của sổ). Đây chính là số lượng các byte dữ liệu, bắt đầu từ byte được chỉ ra trong vùng ACK number, mà trạm nguồn đã sẵn sàng để nhận

- Checksum (16 bits) : mã kiểm soát lỗi (theo phương pháp CRC) cho toàn bộ segment (header + data)

- Urgent pointer (16 bits) : con trỏ này trỏ tới số hiệu tuần tự của byte đi theo sau 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

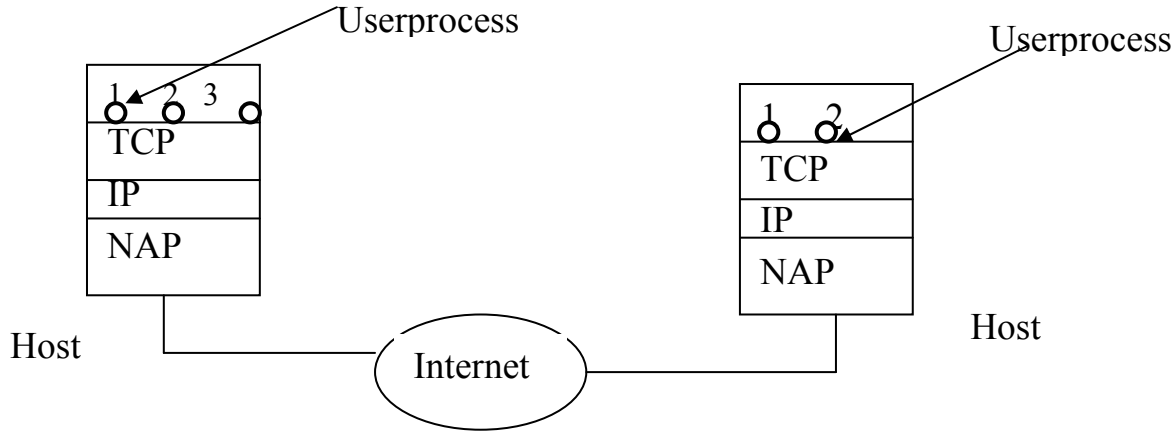
- Options (độ dài thay đổi): khai báo các option của TCP, trong đó có độ dài tối đa của vùng TCP data trong một segment

- Padding (độ dài thay đổi) : phần chèn thêm vào header để bảo đảm phần header luôn kết thúc ở một mốc 32 bits. Phần thêm này gồm toàn số 0.

- TCP data (độ dài thay đổi) : chứa dữ liệu của tầng trên, có độ dài tối đa ngầm định là 536 bytes. Giá trị này có thể điều chỉnh bằng cách khai báo trong vùng options.

Một tiến trình ứng dụng trong một host truy nhập vào các dịch vụ của TCP cung cấp thông qua một cổng (port) như sau:

Một cổng kết hợp với một địa chỉ IP tạo thành một socket duy nhất trong liên mạng. TCP được cung cấp nhờ một liên kết logic giữa một cặp socket. Một socket có thể tham gia nhiều liên kết với các socket ở xa khác nhau. Trước khi truyền dữ liệu giữa hai trạm cần phải thiết lập một liên kết TCP giữa chúng và khi kết thúc phiên truyền dữ liệu thì liên kết đó sẽ được giải phóng. Cũng giống như ở các giao thức khác, các thực thể ở tầng trên sử dụng TCP thông qua các hàm dịch vụ nguyên thuỷ (service primitives), hay còn gọi là các lời gọi hàm (function call).



NAP: Network Access Protocol

Cổng truy nhập dịch vụ TCP

I.2.3. Thiết lập và kết thúc kết nối TCP

Thiết lập kết nối

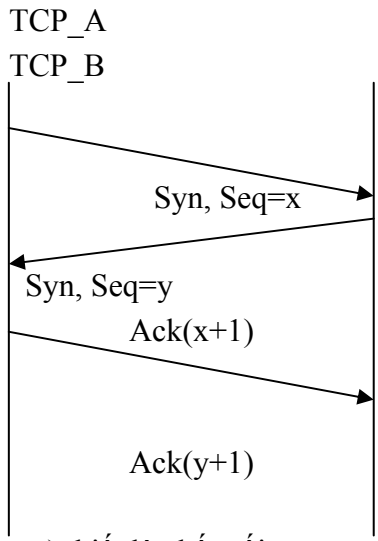
Thiết lập kết nối TCP được thực hiện trên cơ sở phương thức bắt tay ba bước (Tree - way Handsake) hình 2.11. Yêu cầu kết nối luôn được tiến trình trạm khởi tạo, bằng cách gửi một gói TCP với cờ SYN=1 và chứa giá trị khởi

tạo số tuần tự ISN của client. Giá trị ISN này là một số 4 byte không dấu và được tăng mỗi khi kết nối được yêu cầu (giá trị này quay về 0 khi nó tới giá trị 2^{32}). Trong thông điệp SYN này còn chứa số hiệu cổng TCP của phần mềm dịch vụ mà tiến trình trạm muốn kết nối (bước 1).

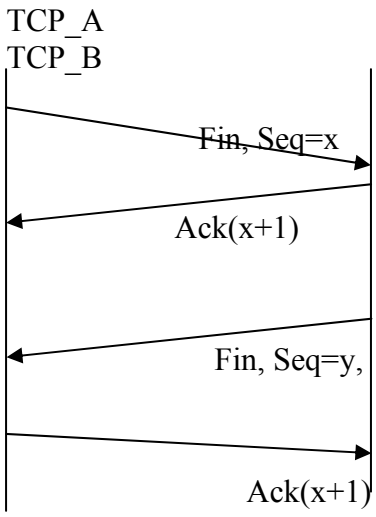
Mỗi thực thể kết nối TCP đều có một giá trị ISN mới số này được tăng theo thời gian. Vì một kết nối TCP có cùng số hiệu cổng và cùng địa chỉ IP được dùng lại nhiều lần, do đó việc thay đổi giá trị INS ngăn không cho các kết nối dùng lại các dữ liệu đã cũ (stale) vẫn còn được truyền từ một kết nối cũ và có cùng một địa chỉ kết nối.

Khi thực thể TCP của phần mềm dịch vụ nhận được thông điệp SYN, nó gửi lại gói SYN cùng giá trị ISN của nó và đặt cờ ACK=1 trong trường hợp sẵn sàng nhận kết nối. Thông điệp này còn chứa giá trị ISN của tiến trình trạm trong trường hợp số tuần tự thu để báo rằng thực thể dịch vụ đã nhận được giá trị ISN của tiến trình trạm (bước 2).

Tiến trình trạm trả lời lại gói SYN của thực thể dịch vụ bằng một thông báo trả lời ACK cuối cùng. Bằng cách này, các thực thể TCP trao đổi một cách tin cậy các giá trị ISN của nhau và có thể bắt đầu trao đổi dữ liệu. Không có thông điệp nào trong ba bước trên chứa bất kỳ dữ liệu gì; tất cả thông tin trao đổi đều nằm trong phần tiêu đề của thông điệp TCP (bước 3).



a) thiết lập kết nối



b) Kết thúc kết nối

Quá trình kết nối theo 3 bước

Kết thúc kết nối

Khi có nhu cầu kết thúc kết nối, thực thể TCP, ví dụ cụ thể A gửi yêu cầu kết thúc kết nối với FIN=1. Vì kết nối TCP là song công (full-duplex) nên mặc dù nhận được yêu cầu kết thúc kết nối của A (A thông báo hết số liệu gửi) thực thể B vẫn có thể tiếp tục truyền số liệu cho đến khi B không còn số liệu để gửi và thông báo cho A bằng yêu cầu kết thúc kết nối với FIN=1 của mình. Khi thực thể TCP đã nhận được thông điệp FIN và sau khi đã gửi thông điệp FIN của chính mình, kết nối TCP thực sụ kết thúc.

PHẦN II
QUẢN TRỊ MẠNG

Quản trị mạng lưới (network administration) được định nghĩa là các công việc quản lý mạng lưới bao gồm cung cấp các dịch vụ hỗ trợ, đảm bảo mạng lưới hoạt động hiệu quả, đảm bảo chất lượng mạng lưới cung cấp đúng như chỉ tiêu định ra.

Quản trị hệ thống (system administration) được định nghĩa là các công việc cung cấp các dịch vụ hỗ trợ, đảm bảo sự tin cậy, nâng cao hiệu quả hoạt động của hệ thống, và đảm bảo chất lượng dịch vụ cung cấp trên hệ thống đúng như chỉ tiêu định ra.

Một định nghĩa khái quát về công tác quản trị mạng là rất khó vì tính bao hàm rộng của nó. Quản trị mạng theo nghĩa mạng máy tính có thể được hiểu khái quát là tập bao gồm của các công tác quản trị mạng lưới và quản trị hệ thống.

Có thể khái quát công tác quản trị mạng bao gồm các công việc sau:

Quản trị cấu hình, tài nguyên mạng : Bao gồm các công tác quản lý kiểm soát cấu hình, quản lý các tài nguyên cấp phát cho các đối tượng sử dụng khác nhau. Có thể tham khảo các công việc quản trị cụ thể trong các tài liệu, giáo trình về quản trị hệ thống windows, linux, novell netware ...

Quản trị người dùng, dịch vụ mạng: Bao gồm các công tác quản lý người sử dụng trên hệ thống, trên mạng lưới và đảm bảo dịch vụ cung cấp có độ tin cậy cao, chất lượng đảm bảo theo đúng các chỉ tiêu đề ra. Có thể tham khảo các tài liệu, giáo trình quản trị hệ thống windows, novell netware, linux, unix, quản trị dịch vụ cơ bản thư tín điện tử, DNS...

Quản trị hiệu năng, hoạt động mạng : Bao gồm các công tác quản lý, giám sát hoạt động mạng lưới, đảm bảo các thiết bị, hệ thống, dịch vụ trên mạng hoạt động ổn định, hiệu quả. Các công tác quản lý, giám sát hoạt động của mạng lưới cho phép người quản trị tổng hợp, dự báo sự phát triển mạng lưới, dịch vụ, các điểm yếu, điểm mạnh của toàn mạng, các hệ thống và dịch vụ

đồng thời giúp khai thác toàn bộ hệ thống mạng với hiệu suất cao nhất. Có thể tham khảo các tài liệu, giáo trình về các hệ thống quản trị mạng NMS, HP Openview, Sunet Manager, hay các giáo trình nâng cao hiệu năng hoạt động của hệ thống (performance tuning).

Quản trị an ninh, an toàn mạng: Bao gồm các công tác quản lý, giám sát mạng lưới, các hệ thống để đảm bảo phòng tránh các truy nhập trái phép, có tính phá hoại các hệ thống, dịch vụ, hoặc mục tiêu đánh cắp thông tin quan trọng của các tổ chức, công ty hay thay đổi nội dung cung cấp lên mạng với dụng ý xấu. Việc phòng chống, ngăn chặn sự lây lan của các loại virus máy tính, các phương thức tấn công ví dụ như DoS làm tê liệt hoạt động mạng hay dịch vụ cũng là một phần cực kỳ quan trọng của công tác quản trị an ninh, an toàn mạng. Đặc biệt, hiện nay khi nhu cầu kết nối ra mạng Internet trở nên thiết yếu thì các công tác đảm bảo an ninh, an toàn được đặt lên hàng đầu, đặc biệt là với các cơ quan cần bảo mật nội dung thông tin cao độ (nhà băng, các cơ quan lưu trữ, các các báo điện tử, tập đoàn kinh tế mũi nhọn...).

Trong phần 2 của giáo trình này sẽ tập trung nghiên cứu sâu về một số kiến thức, kỹ năng cơ bản và thông dụng nhất về quản trị mạng. Tuy nhiên, các nội dung trình bày tại phần 2 sẽ không bao hàm hết được các nội dung đã khái quát ở trên do sự phức tạp phong phú của bản thân mỗi nội dung cũng như giới hạn về thời gian biên soạn. Với mục tiêu cung cấp các kỹ năng phổ biến nhất giúp cho các học viên tiếp cận nhanh chóng vào công tác quản trị mạng để đảm đương được nhiệm vụ cơ quan, công ty giao cho. Phần 2 của giáo trình sẽ bao gồm :

- Tổng quan về bộ định tuyến trên mạng
- Hệ thống tên miền DNS
- Dịch vụ truy cập từ xa và dịch vụ proxy
- Firewall và bảo mật hệ thống

Học viên cũng có thể tham khảo bổ sung thêm kiến thức về quản trị mạng với các giáo trình về mạng cục bộ, giáo trình về thư tín điện tử, giáo trình về các hệ điều hành Windows, Linux, Unix là các nội dung biên soạn trong bộ các giáo trình phục vụ đào tạo cho đề án 112.

Chương 3 : Tổng quan về bộ định tuyến

Chương ba cung cấp các kiến thức cơ bản về bộ định tuyến trên mạng và các bộ chuyển mạch lớp 3. Các thiết bị này là một phần thiết yếu của mạng máy tính hiện đại và là các thiết bị hạ tầng cốt lõi. Các minh họa tường tận về cấu trúc của các sản phẩm hãng Cisco sẽ giúp học viên nắm vững các lý thuyết hệ thống đặc biệt là lý thuyết định tuyến. Phần nội dung cũng bổ sung các kỹ năng cấu hình hoạt động của thiết bị trên các giao thức mạng WAN khác nhau như Frame Relay, X.25...

Chương ba đòi hỏi các học viên cần có các kiến thức sơ khởi về các giao thức trên mạng diện rộng như Frame Relay, x.25..., các kiến thức về địa chỉ lớp 2, lớp 3.

I. Lý thuyết về bộ định tuyến

I.1. Tổng quan về bộ định tuyến

Bộ định tuyến là thiết bị được sử dụng trên mạng để thực thi các hoạt động xử lý truyền tải thông tin trên mạng. Có thể xem bộ định tuyến là một thiết bị máy tính được thiết kế đặc biệt để đảm đương được vai trò xử lý truyền tải thông tin trên mạng của nó và do đó nó cũng bao gồm các CPU, trái tim của mọi hoạt động, bộ nhớ ROM, RAM, các giao tiếp, các bus dữ liệu, hệ điều hành v.v...

Chức năng của bộ định tuyến là định hướng cho các gói tin được truyền tải qua bộ định tuyến. Trên cơ sở các thuật toán định tuyến, thông tin cấu hình và chuyển giao, các bộ định tuyến sẽ quyết định hướng đi tốt nhất cho các gói tin được truyền tải qua nó. Bộ định tuyến còn có vai trò để xử lý các nhu cầu truyền tải và chuyển đổi giao thức khác.

Vai trò của bộ định tuyến trên mạng là đảm bảo các kết nối liên thông giữa các mạng với nhau, tính toán và trao đổi các thông tin liên mạng làm căn cứ cho các bộ định tuyến ra các quyết định truyền tải thông tin phù hợp với cấu hình thực tế của mạng. Bộ định tuyến làm việc với nhiều công nghệ đấu nối mạng diện rộng khác nhau như FRAME RELAY, X.25, ATM, SONET, ISDN, xDSL... đảm bảo các nhu cầu kết nối mạng theo nhiều các công nghệ và độ

chuẩn mực khác nhau mà nếu thiếu vai trò của bộ định tuyến thì không thể thực hiện được.

I.2. Các chức năng chính của bộ định tuyến, tham chiếu mô hình OSI

Mô hình OSI đã được học ở chương 1 gồm 7 lớp trong đó bao gồm

- 3 lớp thuộc về các lớp ứng dụng
  - lớp ứng dụng
  - lớp trình bày
  - lớp phiên
- 4 lớp thuộc về các lớp truyền thông
  - lớp vận chuyển
  - lớp mạng
  - lớp liên kết dữ liệu
  - lớp vật lý

Đối với các lớp truyền thông:

- Lớp vận chuyển: phân chia / tái thiết dữ liệu thành các dòng chảy dữ liệu. Các chức năng chính bao gồm điều khiển dòng dữ liệu, đa truy nhập, quản lý các mạch ảo, phát hiện và sửa lỗi. TCP, UDP là hai giao thức thuộc họ giao thức Internet (TCP/IP) thuộc về lớp vận chuyển này.

- Lớp mạng: cung cấp hoạt động định tuyến và các chức năng liên quan khác cho phép kết hợp các môi trường liên kết dữ liệu khác nhau lại với nhau cùng tạo nên mạng thống nhất. Các giao thức định tuyến hoạt đông trong lớp mạng này.

- Lớp liên kết dữ liệu: cung cấp khả năng truyền tải dữ liệu từ qua môi trường truyền dẫn vật lý. Mỗi đặc tả khác nhau của lớp liên kết dữ liệu sẽ có các định nghĩa khác nhau về giao thức và các chuẩn mực kết nối đảm bảo truyền tải dữ liệu.

- Lớp vật lý: định nghĩa các thuộc tính điện, các chức năng, thường trình dùng để kết nối các thiết bị mạng ở mức vật lý. Một số các thuộc tính được định nghĩa như mức điện áp, đồng bộ, tốc độ truyền tải vật lý, khoảng cách truyền tải cho phép...

Trong môi trường truyền thông, các thiết bị truyền thông giao tiếp với nhau thông qua các họ giao thức truyền thông khác nhau được xây dựng dựa trên các mô hình chuẩn OSI nhằm đảm bảo tính tương thích và mở rộng. Các giao thức truyền thông thường được chia vào một trong bốn nhóm: các giao thức mạng cục bộ, các giao thức mạng diện rộng, giao thức mạng và các giao thức định tuyến. *Giao thức mạng cục bộ* hoạt động trên lớp vật lý và lớp liên kết dữ liệu. *Giao thức mạng diện rộng* hoạt động trên 3 lớp dưới cùng trong mô hình OSI. *Giao thức định tuyến* là giao thức lớp mạng và đảm bảo cho các hoạt động định tuyến và truyền tải dữ liệu. *Giao thức mạng* là các họ các giao thức cho phép giao tiếp với lớp ứng dụng.

Vai trò của bộ định tuyến trong môi trường truyền thông là đảm bảo cho các kết nối giữa các mạng khác nhau với nhiều giao thức mạng, sử dụng các công nghệ truyền dẫn khác nhau.

Chức năng chính của bộ định tuyến là:

- Định tuyến (routing)
- Chuyển mạch các gói tin (packet switching)

Định tuyến là chức năng đảm bảo gói tin được chuyển chính xác tới địa chỉ cần đến. *Chuyển mạch các gói tin* là chức năng chuyển mạch số liệu, truyền tải các gói tin theo hướng đã định trên cơ sở các định tuyến được đặt ra. Như vậy, trên mỗi bộ định tuyến, ta phải xây dựng một bảng định tuyến, trên đó chỉ rõ địa chỉ cần đến và đường đi cho nó. Bộ định tuyến dựa vào địa chỉ của gói tin kết hợp với bảng định tuyến để chuyển gói tin đi đúng đến đích. Các gói tin không có đúng địa chỉ đích trên bảng định tuyến sẽ bị huỷ.

Chức năng đầu tiên của bộ định tuyến là chức năng định tuyến như tên gọi của nó cũng là chức năng chính của bộ định tuyến làm việc với các *giao thức định tuyến.* Bộ định tuyến được xếp vào các thiết bị mạng làm việc ở lớp 3, lớp mạng.

Bảng 3-1:Tương đương chức năng thiết bị trong mô hình OSI

Lớp 3	Lớp mạng	
Lớp 2	Lớp liên kết dữ liệu	
Lớp 1	Lớp vật lý	

Chức năng khác của bộ định tuyến là cho phép sử dụng các phương thức truyền thông khác nhau để đấu nối diện rộng. Chức năng kết nối diện rộng WAN của bộ định tuyến là không thể thiếu để đảm bảo vai trò kết nối truyền thông giữa các mạng với nhau. Chức năng kết nối mạng cục bộ, bất kỳ bộ định tuyến nào cũng cần có chức năng này để đảm bảo kết nối đến vùng dịch vụ của mạng. Bộ định tuyến còn có các chức năng đảm bảo hoạt động cho các giao thức mạng mà nó quản lý.

I.3. Cấu hình cơ bản và chức năng của các bộ phận của bộ định tuyến

Như đã nói ở phần trước, bộ định tuyến là một thiết bị máy tính được thiết kế đặc biệt để đảm đương được vai trò xử lý truyền tải thông tin trên mạng. Nó được thiết kế bao gồm các phần tử không thể thiếu như CPU, bộ nhớ ROM, RAM, các bus dữ liệu, hệ điều hành. Các phần tử khác tùy theo nhu cầu sử dụng có thể có hoặc không bao gồm các giao tiếp, các module và các tính năng đặc biệt của hệ điều hành.

CPU: điều khiển mọi hoạt động của bộ định tuyến trên cơ sở các hệ thống chương trình thực thi của hệ điều hành.

ROM: chứa các chương trình tự động kiểm tra và có thể có thành phần cơ bản nhất sao cho bộ định tuyến có thể thực thi được một số hoạt động tối thiểu ngay cả khi không có hệ điều hành hay hệ điều hành bị hỏng.

RAM: giữ các bảng định tuyến, các vùng đệm, tập tin cấu hình khi chạy, các thông số đảm bảo hoạt động của bộ định tuyến khác.

Flash: là thiết bị nhớ / lưu trữ có khả năng xoá và ghi được, không mất dữ liệu khi cắt nguồn. Hệ điều hành của bộ định tuyến được chứa ở đây. Tùy

thuộc các bộ định tuyến khác nhau, hệ điều hành sẽ được chạy trực tiếp từ Flash hay được giãn ra RAM trước khi chạy. Tập tin cấu hình cũng có thể được lưu trữ trong Flash.

Hệ điều hành: đảm đương hoạt động của bộ định tuyến. Hệ điều hành của các bộ định tuyến khác nhau có các chức năng khác nhau và thường được thiết kế khác nhau. Mỗi bộ định tuyến có thể chạy rất nhiều hệ điều hành khác nhau tùy thuộc vào nhu cầu sử dụng cụ thể, các chức năng cần thiết phải có của bộ định tuyến và các thành phần phần cứng có trong bộ định tuyến. Các thành phần phần cứng mới yêu cầu có sự nâng cấp về hệ điều hành. Các tính năng đặc biệt được cung cấp trong các bản nâng cấp riêng của hệ điều hành.

Các giao tiếp: bộ định tuyến có nhiều các giao tiếp trong đó chủ yếu bao gồm

- Giao tiếp WAN: đảm bảo cho các kết nối diện rộng thông qua các phương thức truyền thông khác nhau như leased-line, Frame Relay, X.25, ISDN, ATM, xDSL ... Các giao tiếp WAN cho phép bộ định tuyến kết nối theo nhiều các giao diện và tốc độ khác nhau: V.35, X.21, G.703, E1, E3, cáp quang v.v...
- Giao tiếp LAN: đảm bảo cho các kết nối mạng cục bộ, kết nối đến các vùng cung cấp dịch vụ trên mạng. Các giao tiếp LAN thông dụng: Ethernet, FastEthernet, GigaEthernet, cáp quang.

II. Giới thiệu về bộ định tuyến Cisco

II.1. Giới thiệu bộ định tuyến Cisco

Sơ lược về bộ định tuyến

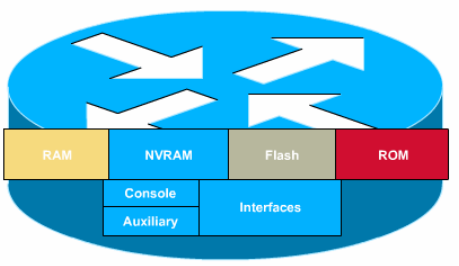
Bộ định tuyến Cisco bao gồm nhiều nền tảng phần cứng khác nhau được thiết kế xây dựng cho phù hợp với nhu cầu và mục đích sử dụng của các giải pháp khác nhau.

Các chức năng xử lý hoạt động của bộ định tuyến Cisco dựa trên nền tảng cốt lõi là hệ điều hành IOS.

Tuỳ theo các nhu cầu cụ thể mà một bộ định tuyến Cisco sẽ cần một IOS có các tính năng phù hợp. IOS có nhiều phiên bản khác nhau, một số loại phần

cứng mới được phát triển chỉ có thể được hỗ trợ bởi các IOS phiên bản mới nhất.

Các thành phần cấu thành bộ định tuyến



Hình 3-1:Các thành phần của bộ định tuyến Cisco

- RAM: Giữ bảng định tuyến, ARP Cache, fast-switching cache, packet buffer, và là nơi chạy các file cấu hình cho bộ định tuyến. Đây chính là nơi lưu giữ file Running-Config, chứa cấu hình đang hoạt động của Router. Khi ngừng cấp nguồn cho bộ định tuyến, bộ nhớ này sẽ tự động giải phóng. Tất cả các thông tin trong file Running-Config sẽ bị mất hoàn toàn.

- NVRAM: non-volatile RAM, là nơi giữ startup/backup configure, không bị mất thông tin khi mất nguồn vào. File Startup-Config được lưu trong này để đảm bảo khi khởi động lại, cấu hình của bộ định tuyến sẽ được tự động đưa về trạng thái đã lưu giữ trong file. Vì vậy, phải thường xuyên lưu file Running-Config thành file Startup-Config.

- Flash: Là ROM có khả năng xoá, và ghi đọc. Là nơi chứa hệ điều hành IOS của bộ định tuyến. Khi khởi động, bộ định tuyến sẽ tự đọc ROM để nạp IOS trước khi nạp file Startup-Config trong NVRAM.

- ROM: Chứa các chng trình tự động kiểm tra.

- Cổng Console: Được sử dụng để cấu hình trực tiếp bộ định tuyến. Tốc độ dữ liệu dùng cho cấu hình bằng máy tính qua cổng COM là 9600b/s. Giao diện ra của cổng này là RJ45 female.

- Cổng AUX: Được sử dụng để quản lý và cấu hình cho bộ định tuyến thông qua modem dự phòng cho cổng Console. Giao diện ra của cổng này cũng là RJ45 female.
- Các giao diện:
    - Cổng Ethernet / Fast Ethernet
    - Cổng Serial
    - Cổng ASYNC ...

II.2. Một số tính năng ưu việt của bộ định tuyến Cisco

- Có khả năng tích hợp nhiều chức năng xử lý trên cùng một sản phẩm với việc sử dụng các module chức năng thích hợp và IOS thích hợp.

- Dễ dàng trong việc nâng cấp bộ định tuyến Cisco cả về phần mềm lẫn phần cứng do đó dễ dàng đáp ứng các nhu cầu thay đổi, mở rộng mạng, đáp ứng các nhu cầu phát triển và ứng dụng công nghệ mới.

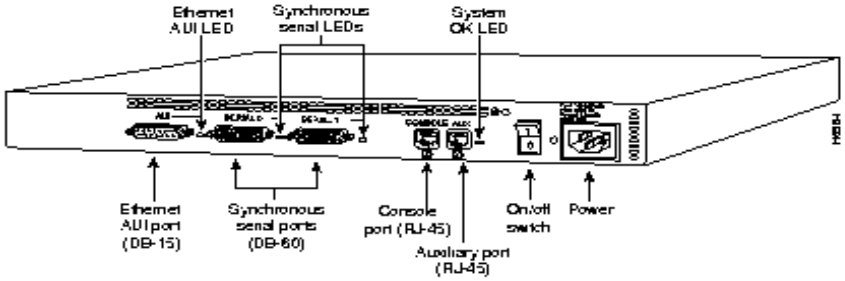
- Tương thích và dễ dàng mở rộng cho các nhu cầu về đa dịch vụ ngày càng gia tăng trên.

- Tính bền vững, an toàn và bảo mật.

II.3. Một số bộ định tuyến Cisco thông dụng

Bộ định tuyến Cisco 2500

- Bộ định tuyến Cisco 2509
- 01 cổng console, 01 AUX
- 02 cổng serial tốc độ tới 2Mbps: kết nối leased-line, X.25, Frame Relay...
- 01 Ethernet tốc độ 10Mbps giao diện AUI: cần thiết có đầu chuyển RJ45/AUI khi kết nối vào các mạng switch/hub thông thường.



Hình 3-2: Bộ định tuyến Cisco 2501

- 01 cổng Async cho phép kết nối đến 08 modem V34/V90. Sử dụng môt cáp kết nối Octal để kết nối các modem đến bộ định tuyến.

- Bộ định tuyến Cisco 2501

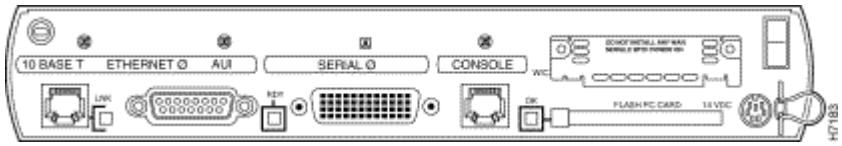
- 01 cổng console, 01 AUX

- 02 cổng serial tốc độ tới 2Mbps: kết nối leased-line, X.25, Frame Relay...

- 01 Ethernet tốc độ 10Mbps giao diện AUI: cần thiết có đầu chuyển RJ45/AUI khi kết nối vào các mạng switch/hub thông thường

Cisco đã ngừng sản xuất các bộ định tuyến Cisco dòng 2500.

Bộ định tuyến Cisco 1600



Hình 3-3: Bộ định tuyến Cisco 1601

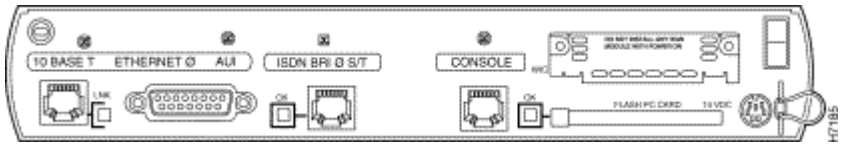
- Bộ định tuyến Cisco 1601

- 01 cổng console

- 01 cổng serial tốc độ tới 2Mbps: kết nối leased-line, X.25, Frame Relay...

- 01 Ethernet tốc độ 10Mbps giao diện AUI và RJ48 (Female Socket for RJ45 connector)

- 01 serial slot: có thể sử dụng cho cổng Serial thứ 2, card ISDN BRI



Hình 3-4: Bộ định tuyến Cisco 1603

- Bộ định tuyến Cisco 1603

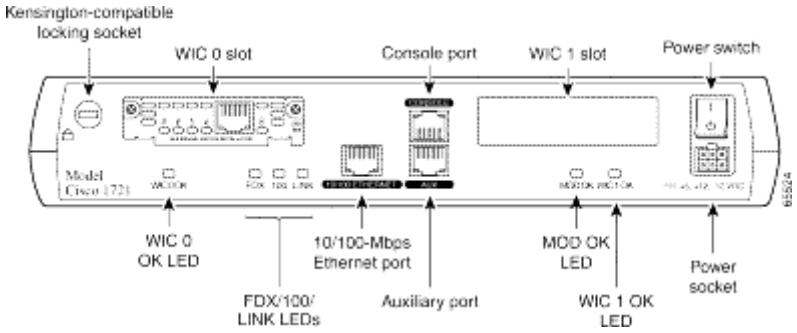
- 01 cổng console

- 01 cổng ISDN BRI giao diện S/T: kết nối ISDN tốc độ 2B+D, khi sử dụng ở Việt nam cần có thêm một bộ tiếp hợp NT1 để đấu nối vào mạng ISDN.

- 01 Ethernet tốc độ 10Mbps giao diện AUI và RJ48 (Female Socket for RJ45 connector)

- 01 serial slot: có thể sử dụng cho cổng Serial, card ISDN BRI

Bộ định tuyến Cisco 1700



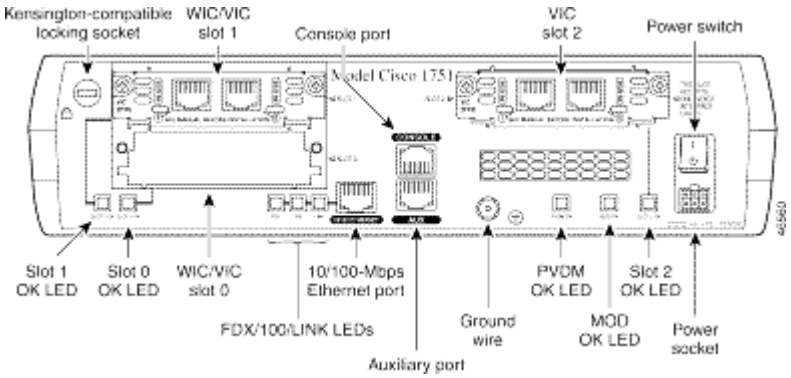
Hình 3-5: Bộ định tuyến Cisco 1721

- Bộ định tuyến Cisco 1721

- 01 cổng console, 01 AUX

- 01 FastEthernet tốc độ 10/100Mbps giao diện RJ48 (Female Socket for RJ45 connector)

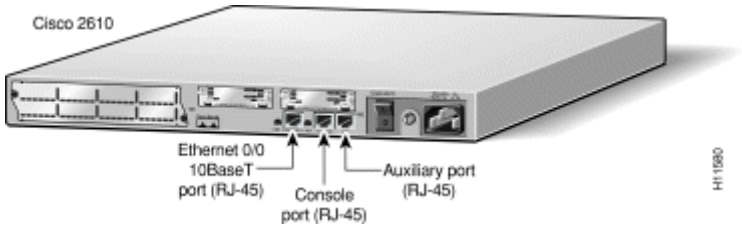
- 02 WAN slot: có thể sử dụng cho cổng Serial, card ISDN BRI...



Hình 3-6: Bộ định tuyến Cisco 1751

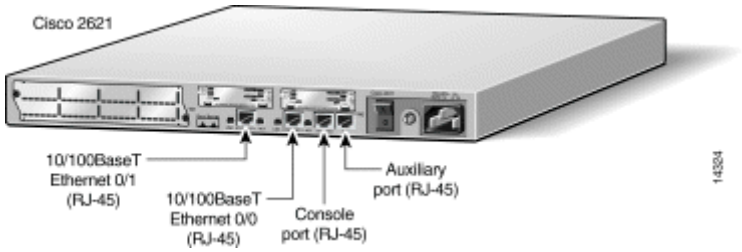
- Bộ định tuyến Cisco 1751
- 01 cổng console, 01 AUX
- 01 FastEthernet tốc độ 10/100Mbps giao diện RJ48 (Female Socket for RJ45 connector)
- 02 WAN slot: có thể sử dụng cho cổng Serial, card ISDN BRI...
- 01 Voice slot: chỉ cho phép cắm các card voice

Bộ định tuyến Cisco 2600



Hình 3-7: Bộ định tuyến Cisco 2610

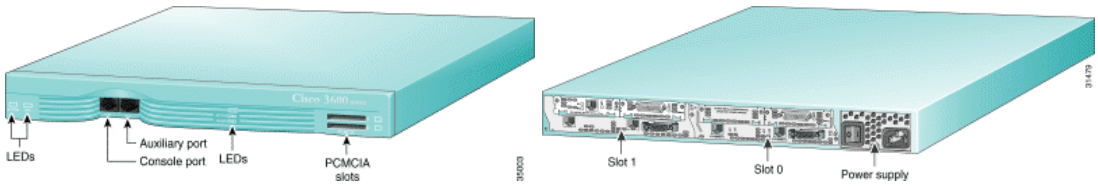
- Bộ định tuyến Cisco 2610
- 01 cổng console, 01AUX
- 01 Ethernet tốc độ 10Mbps giao diện RJ48 (Female Socket for RJ45 connector)
- 02 serial slot: có thể sử dụng cho cổng Serial, card ISDN BRI, card voice...
- 01 network module slot: có thể sử dụng module Async, Sync/Async, Channelized E1, PRI ...



Hình 3-8: Bộ định tuyến Cisco 2621

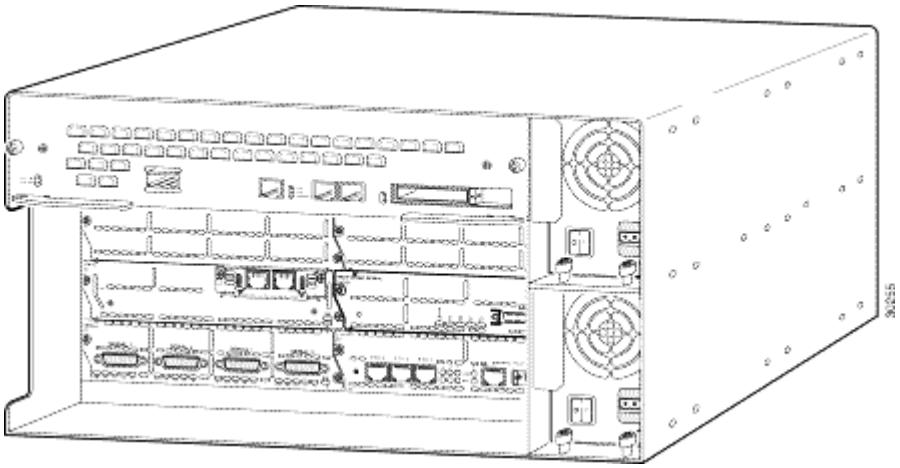
- Bộ định tuyến Cisco 2621
- 01 cổng console, 01AUX
- 02 FastEthernet tốc độ 10/100Mbps giao diện RJ48 (Female Socket for RJ45 connector)
- 02 serial slot: có thể sử dụng cho cổng Serial, card ISDN BRI, card voice...
- 01 network module slot: có thể sử dụng module Async, Sync/Async, Channelized E1, PRI ...

Bộ định tuyến Cisco 3600



Hình 3-9: Bộ định tuyến Cisco 3620

- Bộ định tuyến 3620
- 01 cổng console, 01AUX
- PCMCIA slot
- 02 network module slot: có thể sử dụng module Async, Sync/Async, Channelized E1, PRI, Ethernet/FastEthernet, Voice, VPN ...
- Khi kết nối với mạng LAN cần thiết có một Network module có cổng Ethernet/FastEthernet



Hình 3-10: Bộ định tuyến Cisco 3661

- Bộ định tuyến 3661
- 01 cổng console, 01AUX
- PCMCIA slot
- 01 FastEthernet tốc độ 100Mbps
- 06 network module slot: có thể sử dụng module Async, Sync/Async, Channelized E1, PRI, Ethernet/FastEthernet, Voice, VPN ...
- 02 module nguồn, hỗ trợ và dự phòng lẫn nhau, đảm bảo về mặt cung cấp nguồn điện cho bộ định tuyến. Có thể thay thế module nguồn mà không cần phải tắt điện toàn bộ bộ định tuyến.

II.4. Các giao tiếp của bộ định tuyến Cisco

- Cổng Console
  - Tốc độ có thể 11500Bps, làm việc ở tốc độ 9600Bps
  - Dùng cho cấu hình cho bộ định tuyến Cisco
  - Sử dụng cáp Console để kết nối
- Cổng AUX
  - Tốc độ 11500Bps
  - Sử dụng cho quản trị/cấu hình từ xa qua modem V34/V90
  - Có thể sử dụng để cấu hình trực tiếp sử dụng cáp Console

- Chỉ làm việc sau khi bộ định tuyến Cisco đã khởi động hoàn toàn
- Có thể cấu hình để AUX làm việc như một đường kết nối dự phòng

- Ethernet/FastEthernet
  - Tốc độ 10Mbps/100Mbps giao diện AUI hoặc RJ45
  - Dùng cho đấu nối trực tiếp vào mạng LAN
  - Tuân theo các chuẩn của IEEE802.3
- Serial
  - Tốc độ kết nối tới 2Mbps
  - Dùng cho kết nối mạng WAN
  - Có khả năng kết nối theo nhiều chuẩn giao diện khác nhau V35, V24, X21, EIA530... bằng việc sử dụng các cáp nối
- ISDN
  - Tốc độ 2B+D
  - Dùng cho kết nối mạng ISDN sử dụng cho Dialup Server hoặc kết nối dự phòng
  - Có các giao diện U hoặc S/T, giao diện S/T cần thiết có thiết bị NT1 để kết nối vào mạng
- Async
  - Giao diện truyền số liệu không đồng bộ
  - Dùng cho kết nối với các hệ thống modem V34/V90
  - Sử dụng cáp kết nối Async (Octal Cable) để nối tới 08 modem. Octal cable thường có giao diện RJ45 và cần có chuyển đổi RJ45-DB25 để phù hợp với giao diện của modem

II.5. Kiến trúc module của bộ định tuyến Cisco

Các bộ định tuyến có kiến trúc module

Các bộ định tuyến Cisco thông dụng được giới thiệu ở phần trước hầu hết là có kiến trúc module trừ bộ định tuyến 2500 đã không được tiếp tục sản xuất.

Ngoài các bộ định tuyến có kiến trúc module đã được biết, còn có các bộ định tuyến khác:

- **1600**: 1601, 1602, 1603, 1604, 1605
- **1700**: 1710, 1720, 1721, 1750, 1751, 1760
- **2600**: 2610, 2160XM, 2611, 2611XM, 2612, 2613, 2620, 2620XM, 2621, 2621XM, 2650, 2650XM, 2651, 2651XM, 2691
- **3600**: 3620, 3631, 3640, 3661, 3662
- **3700**: 3725, 3745

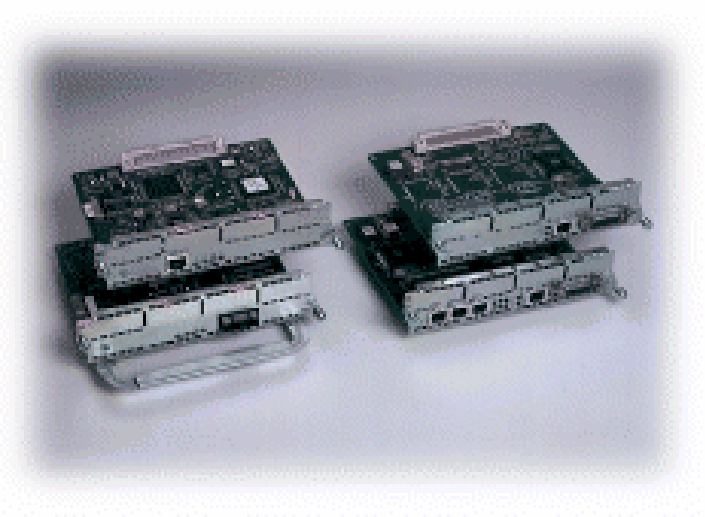
Tính tương thích dùng lẫn và thay thế

Các bộ định tuyến có kiến trúc module của Cisco được thiết kế để sử dụng chung một kho các card giao tiếp và module chức năng khác nhau.

Các card giao tiếp được sử dụng cho bất kỳ một bộ định tuyến nào có khe cắm tương thích. Tương thích phổ biến nhất là card giao tiếp Serial. Card giao tiếp serial có thể sử dụng trên bất kỳ bộ định tuyến nào. Một số card giao tiếp khác như card voice sẽ yêu cầu về cấu hình phần cứng và phần mềm tối thiểu. Các card giao tiếp được sử dụng cho các bộ định tuyến 1600, 1700 có thể sử dụng cho các bộ định tuyến 2600, 3600.

Bộ định tuyến 2600, 3600, 3700 cho phép sử dụng các module chức năng khác nhau. Một module chức năng có thể chỉ bao gồm một chức năng như module Async, module Serial, cũng có thể bao gồm nhiều chức năng hay bao gồm các khe cắm cho card giao tiếp khác như module NM-1E- có 01 cổng Ethernet và 02 khe cắm cho bất kỳ một loại card tương thích nào. Việc lựa chọn module tùy thuộc vào nhu cầu sử dụng cụ thể. Các module cùng được sử dụng giữa các bộ định tuyến. Một số module yêu cầu cấu hình tối thiểu về phần cứng và phần mềm. Bộ định tuyến 1600 và 1700 không cho phép sử dụng các module như các bộ định tuyến 2600, 3600.

Một số module thường gặp



Hình 3-11: Module Ethernet/FastEthernet

Bảng 3-2:Một số loại module Ethernet/FastEthernet

Loại module	Số cổng LAN	Số khe cắm WAN
Single-Port Ethernet	1	None
Four-Port Ethernet	4	None
Single-Port Ethernet Mixed Media	1	Two WAN interface card slots
Dual-Port Ethernet Mixed Media	2	Two WAN interface card slots
Single-Port Ethernet and Single-Port Token Ring	1/1	Two WAN interface card slots
Single Port Fast Ethernet	1	None

Hình 3-12: Module Ethernet có khe cắm WAN

Bảng 3-3: Một số loại module có khe cắm WAN

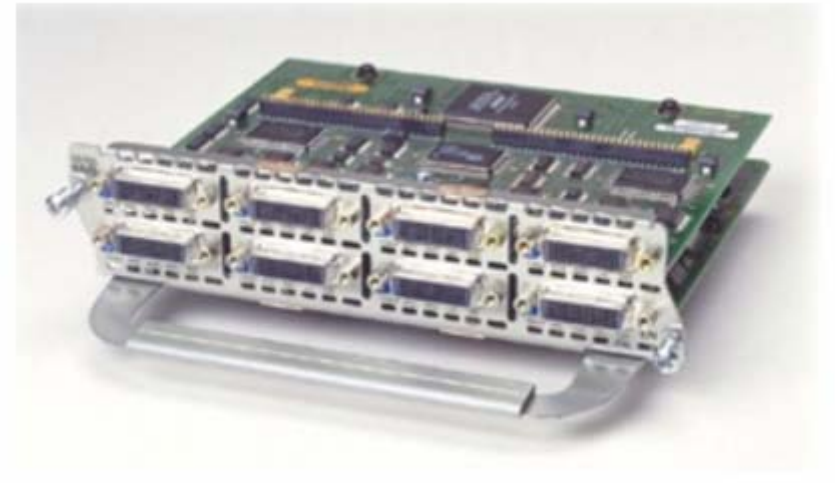
Tên module	Loại module
NM-1FE2W/NM-1FE2W-V2	1 10/100 Ethernet, 2 khe cắm WAN
NM-2FE2W/NM-2FE2W-V2	2 10/100 Ethernet, 2 khe cắm WAN
NM-1FE1R2W	1 10/100 Ethernet, 1 4/16 Token Ring, 2 khe cắm WAN
NM-2W	2 khe cắm WAN

Bảng 3-4: Giới hạn số lượng module trên các bộ định tuyến

	2600	2691	3620	3631	3640	3660	3725	3745
NM-1FE2W/NM-1FE2W-V2	N/A	1	2	N/A	4	6	2	4
NM-2FE2W/NM-2FE2W-V2	N/A	1	2	N/A	4	6	2	4
NM-1FE1R2W	N/A	1	2	N/A	4	6	2	4
NM-2W	1	1	1	N/A	3	6	2	4

Hình 3-13: Module 4 cổng serial

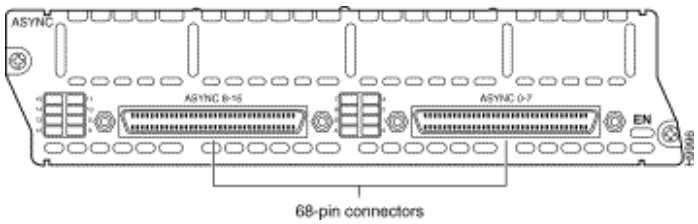
- Module 4 cổng serial
- Hỗ trợ tổng lưu lượng 8Mbps: có thể sử dụng tốc độ tối đa 8Mbps trên một cổng hoặc mỗi 2Mbps cho 4 cổng.
- Kết nối với modem theo các chuẩn V.35, X.21, EIA/TIA-232, EIA/TIA530... sử dụng các cáp phù hợp
- Sử dụng cho đấu nối leased-line, Frame Relay, X.25 ...



Hình 3-14: Module 8 cổng Sync/Async

- Module 8 cổng Sync/Async
- Tốc độ kết nối trên mỗi cổng thấp (tối đa 128Kbps)
- Có thể sử dụng ở hai chế độ đồng bộ và không đồng bộ. Có thể sử dụng cho modem quay số.

- Kết nối với modem theo các chuẩn V.35, X.21, EIA/TIA-232, EIA/TIA530... sử dụng các cáp phù hợp
- Sử dụng cho đấu nối leased-line, Frame Relay, X.25, modem quay số...



Hình 3-15: Module 16 cổng Async

- Module 16 cổng Async
- Kết nối không đồng bộ sử dụng cho modem quay số.
- Kết nối với modem theo các chuẩn EIA/TIA-232 sử dụng cáp Octal

Hình 3-16: Module và card ISDN BRI

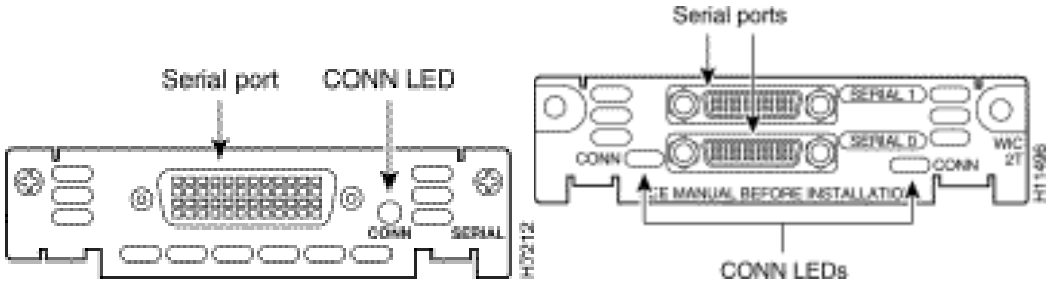
Bảng 3-5: Một số loại module ISDN BRI tốc độ 2B+D (128+16Kbps)

Loại module	Mô tả
NM-4B-S/T	4 cổng ISDN BRI giao diện S/T
NM-4B-U	4 cổng ISDN BRI giao diện U (tích hợp bộ tiếp hợp NT1)

NM-8B-S/T	8 cổng ISDN BRI giao diện S/T
NM-8B-U	8 cổng ISDN BRI giao diện U (tích hợp bộ tiếp hợp NT1)

Bảng 3-6: Một số loại card giao tiếp ISDN BRI tốc độ 2B+D (128+16Kbps)

Loại card	Mô tả
WIC-1B-S/T-V2	1 cổng ISDN BRI giao diện S/T
WIC 1B-U-V2	1 cổng ISDN BRI giao diện U (tích hợp bộ tiếp hợp NT1)



Hình 3-17: Card giao tiếp Serial

- Card một và hai cổng giao tiếp Serial
- Kết nối đồng bộ tốc độ đến 2Mbps
- Kết nối với modem theo các chuẩn V.35, X.21, EIA/TIA-232, EIA/TIA530... sử dụng các cáp phù hợp
- Sử dụng cho đấu nối leased-line, Frame Relay, X.25, modem quay số...

III. Cách sử dụng lệnh cấu hình bộ định tuyến

III.1. Giới thiệu giao tiếp dòng lệnh của bộ định tuyến Cisco

Giao tiếp dòng lệnh

Giao tiếp dòng lệnh CLI (Command Line Interface) khác với các giao tiếp đồ họa GUI (Graphic User Interface) là giao tiếp đặc biệt được Cisco thiết

kế cho phép người dùng, người quản trị làm việc với các thiết bị của Cisco thông qua các dòng lệnh trực tiếp.

Với giao tiếp dòng lệnh, người dùng, người quản trị có thể trực tiếp xem, cấu hình các thiết bị của Cisco thông qua các lệnh phù hợp. Để có thể sử dụng được giao tiếp dòng lệnh, người dùng phải nắm vững được các lệnh, các tham số lệnh và cách sử dụng các lệnh.

Mỗi thiết bị của Cisco đều có rất nhiều các lệnh, các bộ lệnh đi kèm tuy nhiên người sử dụng, người quản trị không nhất thiết phải hiểu hết toàn bộ các lệnh trong mỗi thiết bị mà chỉ cần hiểu, nắm vững một số lệnh cần thiết cho các mục đích sử dụng cụ thể.

Giao tiếp dòng lệnh của Cisco cung cấp cho người dùng khả năng sử dụng trợ giúp trực tuyến. Điều đó có nghĩa là trong quá trình làm việc với thiết bị thông qua giao tiếp dòng lệnh, người dùng có thể liệt kê các lệnh, xem lại ý nghĩa sử dụng của nó hay thậm chí xem các thông số lệnh.

Lưu ý: khi sử dụng giao tiếp dòng lệnh để cấu hình thiết bị, sau khi lệnh được thực thi (ấn phím Enter) các hoạt động của bộ định tuyến sẽ ảnh hưởng ngay lập tức bởi lệnh thực thi đó. Một cho những ví dụ là khi đang thực hiện cấu hình từ xa thông qua telnet, nếu thay đổi địa chỉ của bộ định tuyến, sẽ lập tức mất kết nối đến bộ định tuyến và chỉ có thể thực hiện cấu hình bộ định tuyến trực tiếp từ cổng console. Điều này có nghĩa cần thiết phải rất cẩn thận và chắc chắn cũng như thực hiện đúng trình tự mỗi khi thực hiện cấu hình bộ định tuyến.

```
Router#config terminal
Router(config)#interface s0/0
Router(config-if)#encapsolution ppp
Router(config-if)#ip address 192.168.100.5 255.255.255.0
Router(config-if)#
```

Hình 3-18: Ví dụ về giao tiếp dòng lệnh

Các khả năng thực hiện cấu hình bộ định tuyến Cisco

- Cấu hình bộ định tuyến trực tiếp từ cổng console: là phương pháp sử dụng một cáp console thông qua một phần mềm kết nối trực tiếp cổng COM như HyperTerminal của WINDOWS để truy nhập vào bộ định tuyến sau đó cấu hình bộ định tuyến theo giao thức dòng lệnh. Phương pháp cấu hình này được

sử dụng nhiều nhất và trong hầu hết các trường hợp. Các bộ định tuyến sử dụng lần đầu cũng phải được cấu hình bằng phương pháp này.

- Cấu hình bộ định tuyến thông qua truy nhập từ xa telnet: truy nhập từ xa tới bộ định tuyến với telnet chỉ có thể thực hiện được khi bộ định tuyến đã được cấu hình với ít nhất một địa chỉ mạng, có mật khẩu bảo vệ và máy tính sử dụng để cấu hình bộ định tuyến phải có khả năng kết nối được với bộ định tuyến thông qua môi trường mạng. Sau khi kết nối được tới bộ định tuyến, sử dụng giao diện dòng lệnh để cấu hình bộ định tuyến.

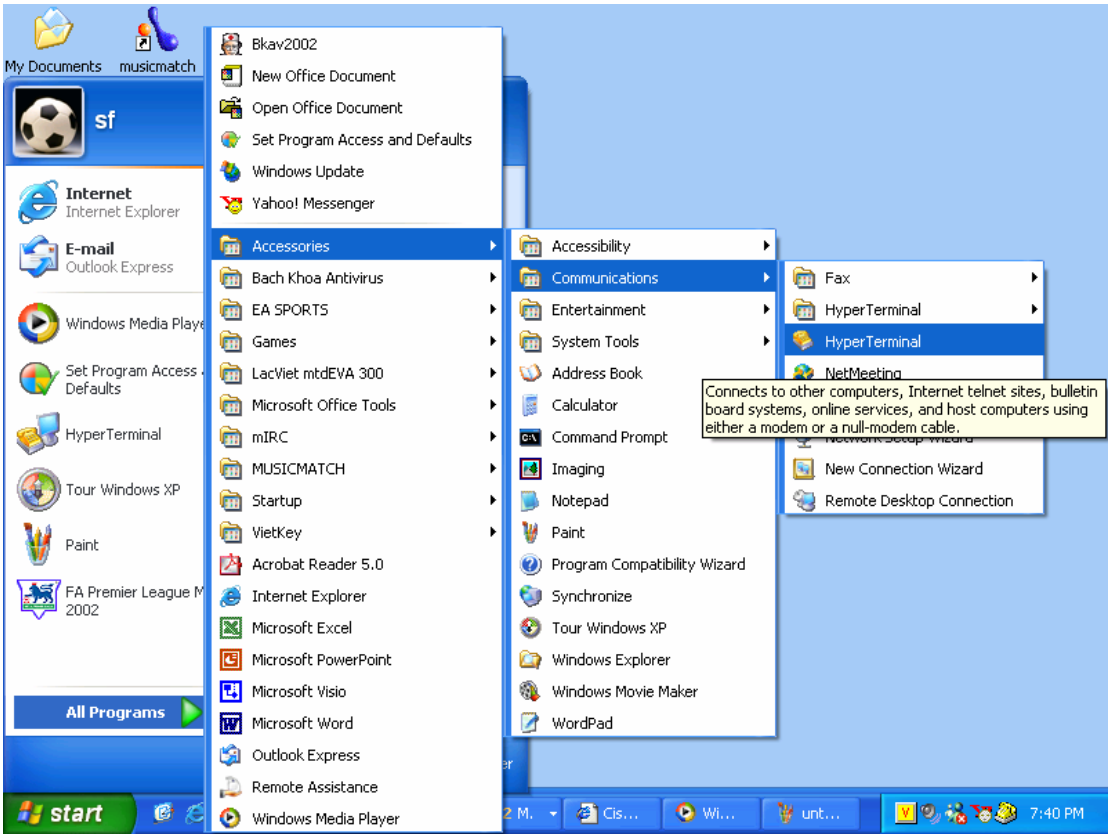
- Cấu hình bộ định tuyến sử dụng tập tin cấu hình lưu trữ trên máy chủ TFTP: trong một số trường hợp, tập tin cấu hình cho bộ định tuyến có thể được lưu trữ trên máy chủ TFTP, bộ định tuyến được cấu hình sao cho sau khi khởi động sẽ tìm kiếm tập tin cấu hình trên máy chủ TFTP thay vì sử dụng tập tin cấu hình lưu trữ trong NVRAM. Có thể sử dụng lệnh copy để tải tập tin cấu hình từ máy chủ TFTP về bộ định tuyến.

- Cấu hình bộ định tuyến thông qua giao diện WEB: chỉ thực hiện được sau khi bộ định tuyến đã được cấu hình với địa chỉ IP và cho phép cấu hình qua giao thức http.

Sử dụng giao tiếp dòng lệnh

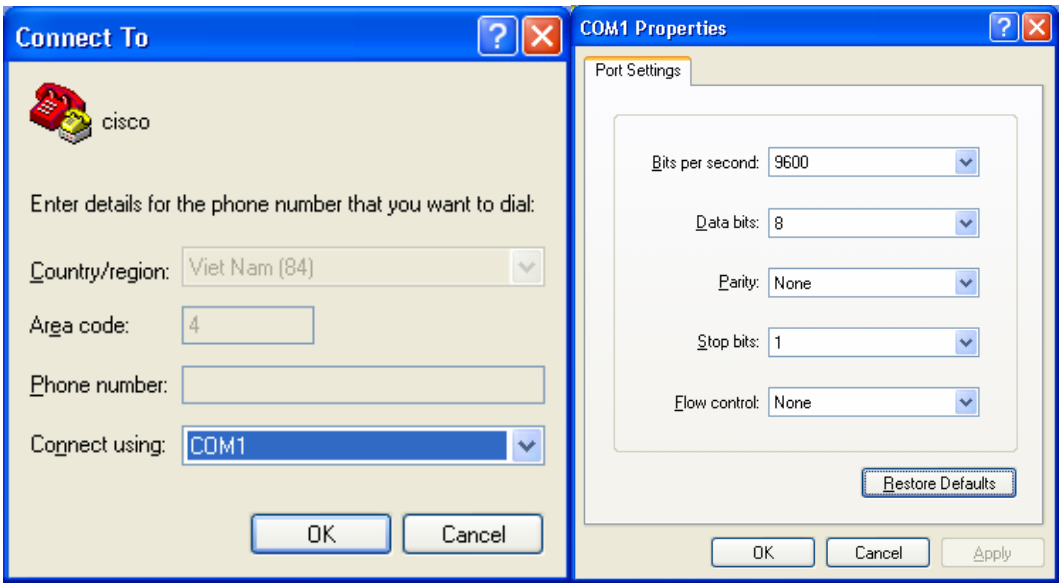
Để thực hiện việc kết nối máy tính với bộ định tuyến, người ta dùng cáp console của Cisco, một đầu cắm trực tiếp vào cổng CONSOLE của bộ định tuyến, đầu kia cắm vào cổng COM của máy tính, có thể sử dụng các đầu chuyển đổi DB9/RJ45 hoặc DB25/RJ45 khi cần thiết.

Phần mềm giao tiếp giữa máy tính và bộ định tuyến thông dụng nhất là HyperTerminal được cài đặt sẵn trong các phiên bản WINDOWS.

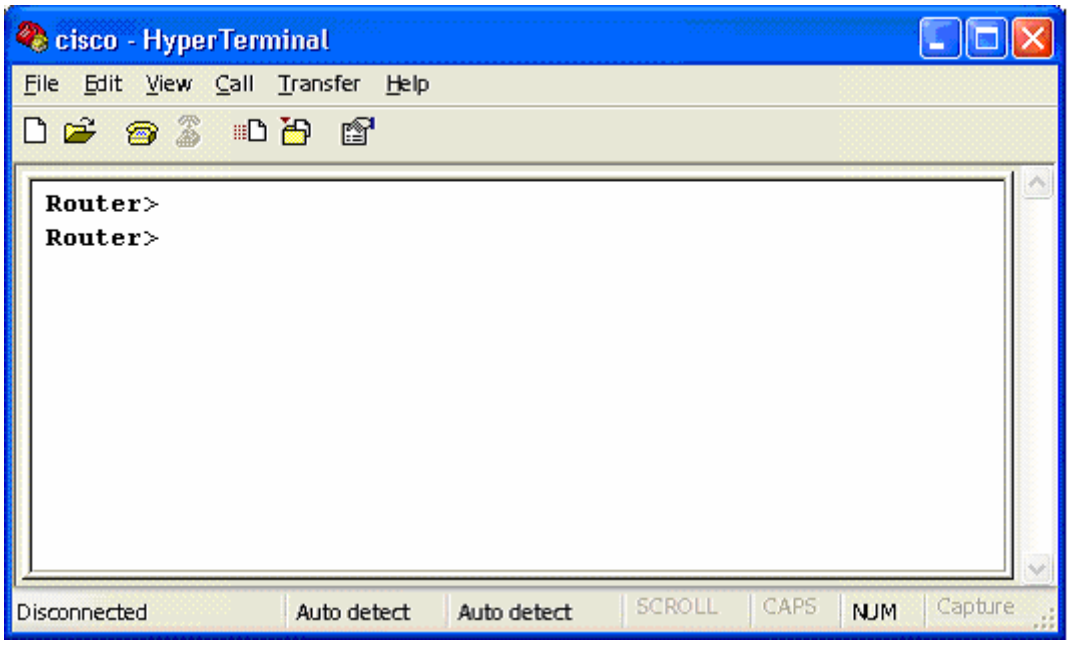


Hình 3-19:Sử dụng phần mềm HyperTerminal để kết nối đến bộ định tuyến

Chọn đúng cổng COM kết nối với cáp console để tiến hành cài đặt các thông số làm việc. Tốc độ kết nối thông qua cổng COM của máy tính và cổng CONSOLE của bộ định tuyến là 9600b/s (hình 3-20). Chọn OK, bấm phím Enter, cửa sổ làm việc xuất hiện dấu lớn hơn ">" sau tên của của bộ định tuyến, nghĩa là việc kết nối đã hoàn tất (hình 3-21).



Hình 3-20: Xác lập các tham số cho kết nối



Hình 3-21: Kết nối tới bộ định tuyến thành công

Sau khi đã kết nối thành công, sử dụng các lệnh của bộ định tuyến để xem, kiểm tra, cấu hình và bắt lỗi các hoạt động của bộ định tuyến.

Sử dụng dấu ? để truy cập thông tin trợ giúp

- Đánh dấu ? ngay sát sau câu lệnh chưa hoàn chỉnh sẽ hiện thị các lệnh có thể bắt đầu từ các từ chưa hoàn chỉnh đã gõ
- Đánh dấu ? sau câu lệnh một ký tự trắng sẽ hiển thị các tham số có thể của câu lệnh
- Khi câu lệnh không có sẽ hiển thị một báo lỗi

Sử dụng TAB ngay sát sau câu lệnh chưa hoàn chỉnh sẽ hiển thị câu lệnh hoàn chỉnh

III.2. Làm quen với các chế độ cấu hình

Chế độ người dùng

Bao gồm các tác vụ phổ biến chủ yếu gồm những lệnh kiểm tra trạng thái hoạt động của bộ định tuyến, trạng thái các giao tiếp, các bảng định tuyến v.v... và một số lệnh để kiểm tra kết nối mạng như ping, traceroute, telnet v.v.... Ở chế độ này không được phép thay đổi các cấu hình bộ định tuyến. Chế độ

người dùng không cho phép xem xét sâu đến các hoạt động của bộ định tuyến mà trong quá trình khai thác, vận hành, người quản trị phải cần thiết sử dụng chế độ quản trị để thực hiện. Biểu hiện của chế độ người dùng là dấu lớn hơn, >, sau tên bộ định tuyến.

```
Router>
Router>?
Exec commands:
  <1-99>           Session number to resume
  access-enable    Create a temporary Access-List entry
  access-profile   Apply user-profile to interface
  clear            Reset functions
  connect          Open a terminal connection
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network connection
  enable           Turn on privileged commands
  exit             Exit from the EXEC
      ----- các lệnh đã được bỏ bớt -----
  ping             Send echo messages
  ppp              Start IETF Point-to-Point Protocol (PPP)
  resume           Resume an active network connection
  rlogin           Open an rlogin connection
  show             Show running system information
  slip             Start Serial-line IP (SLIP)
  systat           Display information about terminal lines
  telnet           Open a telnet connection
  terminal         Set terminal line parameters
  traceroute       Trace route to destination
  tunnel           Open a tunnel connection
  udptn            Open an udptn connection
  where            List active connections
  x28              Become an X.28 PAD
  x3               Set X.3 parameters on PAD
```

Hình 3-22: Chế độ người dùng

Chế độ quản trị

Bao gồm hầu hết các lệnh của chế độ người dùng và các lệnh chỉ dành cho người quản trị. Chỉ có thể cấu hình bộ định tuyến ở chế độ này. Trong quá trình khai thác, vận hành, để hiểu rõ hoặc khi có sự cố xảy ra, người quản trị có thể sử dụng các lệnh debug để làm rõ thêm thông tin cần thiết. Đặc trưng cho chế độ quản trị là biểu hiện của dấu thăng, #.

```
Router>en
Password:
Router#
Router#?
Exec commands:
  <1-99>           Session number to resume
  access-enable    Create a temporary Access-List entry
  access-profile   Apply user-profile to interface
  access-template  Create a temporary Access-List entry
  archive          manage archive files
  bfe              For manual emergency modes setting
  cd               Change current directory
  clear            Reset functions
  clock            Manage the system clock
  configure        Enter configuration mode
  connect          Open a terminal connection
  copy             Copy from one file to another
  debug            Debugging functions (see also 'undebug')
      ----- các lệnh đã được bỏ bớt -----
  traceroute       Trace route to destination
  tunnel           Open a tunnel connection
  udptn            Open an udptn connection
  undebug          Disable debugging functions (see also 'debug')
```

```
upgrade          Upgrade firmware
verify           Verify a file
where            List active connections
write            Write running configuration to memory, network, or
                 terminal
x28              Become an X.28 PAD
x3               Set X.3 parameters on PAD
```

Hình 3-23: Chế độ quản trị

Chế độ cấu hình toàn cục

Là chế độ cấu hình các tham số toàn cục cho bộ định tuyến.

Có rất nhiều các cấu hình toàn cục như cấu hình tên bộ định tuyến, cấu hình tên và mật khẩu người dùng, cấu hình định tuyến toàn cục, cấu hình danh sách truy nhập v.v... Biểu hiện của chế độ cấu hình toàn cục xem hình 3-24.

```
Router#
Router#config terminal
Router(config)#hostname RouterA
RouterA(config)#
```

Hình 3-24: Chế độ cấu hình toàn cục

Chế độ cấu hình giao tiếp

Chế độ cấu hình giao tiếp là chế độ cấu hình cho các giao tiếp của bộ định tuyến như giao tiếp Serial, giao tiếp Ethernet, giao tiếp Async...

Chế độ cấu hình giao tiếp cho phép người quản trị mạng thiết lập các tham số hoạt động cho mỗi giao tiếp như các giao thức mạng được sử dụng trên giao tiếp, địa chỉ mạng của giao tiếp, gán các danh sách truy nhập cho giao tiếp v.v... Một ví dụ về chế độ cấu hình giao tiếp xem hình 3-25.

```
Router#
Router#config terminal
```

```
Router(config)#interface s0/0
Router(config-if)#encapsolution ppp
Router(config-if)#ip address 192.168.100.5 255.255.255.0
Router(config-if)#
```

Hình 3-25: Chế độ cấu hình giao tiếp

Chế độ cấu hình định tuyến

Là chế độ cấu hình các tham số cho các giao thức định tuyến. Các giao thức định tuyến được cấu hình độc lập với nhau và đều được thực hiện ở chế độ cấu hình định tuyến như ví dụ trên hình 3-26.

```
Router#
Router#config terminal
Router(config)#router rip
Router(config-router)#network 192.168.0.0
Router(config-if)#
```

Hình 3-26: Chế độ cấu hình định tuyến

Chế độ cấu hình đường kết nối

Chế độ cấu hình đường kết nối là một chế độ cấu hình đặc biệt sử dụng để thiết lập các tham số mức thấp cho giao tiếp logic trong đó điển hình là các tham số thiết lập cho các kết nối modem quay số.

```
Router#config terminal
Router(config)#line 33 48
Router(config-line)#modem inout
Router(config-line)#modem autoconfig discovery
Router(config-line)#
```

Hình 3-27: Chế độ cấu hình đường kết nối

Bảng 3-7:Một số chế độ cấu hình và thể hiện

Chế độ cấu hình	Thể hiện
Global	Router(config)#
Interface	Router(config-if)#
Subinterface	Router(config-subif)#
Controller	Router(config-controller)#
Map-list	Router(config-map-list)#
Map-class	Router(config-map-class)#
Line	Router(config-line)#
Router	Router(config-router)#
Route-map	Router(config-route-map)#

III.3. Làm quen với các lệnh cấu hình cơ bản

Enable: dùng để vào chế độ quản trị. Sau khi thực hiện lệnh enable, người dùng phải cung cấp mật khẩu quản trị đúng để thực sự được làm việc ở chế độ quản trị, mật khẩu không được phép nhập sai quá 3 lần.

```
Router>
Router>en
Password:
Password:
Password:
% Bad secrets

Router>en
Password:
Router#
```

```
Router#
Router#disa
Router>
```

Hình 3-28: Sử dụng lệnh enable và disable

Disable: thoát khỏi chế độ quản trị về chế độ người dùng.

Setup: thực hiện khởi tạo lại cấu hình của bộ định tuyến ở chế độ cấu hình hội thoại. Sau đây, hình 3-29, là một ví dụ về sử dụng lệnh setup. Chế độ hội thoại này cũng được thực hiện tự động đối với các bộ định tuyến chưa hề có tập tin cấu hình hay nói cách khác có NVRAM không chứa thông tin.

```
Router#setup

         --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: y

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: n

First, would you like to see the current interface summary? [yes]: n

Configuring global parameters:

  Enter host name [Router]:

  The enable secret is a password used to protect access to
```

```
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret [<Use current secret>]:

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password []:123456

  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: 654321
  Configure SNMP Network Management? [yes]:
    Community string [public]:
  Configure IP? [yes]:
    Configure IGRP routing? [yes]: n
    Configure RIP routing? [no]:
  Configure bridging? [no]:

Async lines accept incoming modems calls. If you will have
users dialing in via modems, configure these lines.

  Configure Async lines? [yes]: n

Configuring interface parameters:

Do you want to configure FastEthernet0/0  interface? [yes]: n

Do you want to configure Serial0/0  interface? [yes]: n

Do you want to configure Serial0/1  interface? [no]: y

  Some supported encapsulations are
        ppp/hdlc/frame-relay/lapb/x25/atm-dxi/smds
```

```
  Choose encapsulation type [hdlc]: ppp

  No serial cable seen.
  Choose mode from (dce/dte)  [dte]:
  Configure IP on this interface? [no]: y
    IP address for this interface: 192.168.100.5
    Subnet mask for this interface [255.255.255.0] :
    Class C network is 192.168.100.0, 24 subnet bits; mask is /24

The following configuration command script was created:

hostname Router
enable secret 5 $1$EuXV$Yhj/OYkz/U1R5VABqXsMC0
enable password 7 123456
line vty 0 4
password 7 654321
snmp-server community public
!
ip routing
no bridge 1
!
interface FastEthernet0/0
shutdown
no ip address
!
interface Serial0/0
shutdown
no ip address
!
interface Serial0/1
no shutdown
encapsulation ppp
ip address 192.168.100.5 255.255.255.0
dialer-list 1 protocol ip permit
```

```
dialer-list 1 protocol ipx permit
!
end

[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.
```

Hình 3-29: Lệnh setup

Config: cho phép thực hiện các lệnh cấu hình bộ định tuyến. Sau lênh config, quản trị mạng mới có thể thực hiện các lệnh cấu hình bộ định tuyến.

Trình tự thực hiện cấu hình cho một bộ định tuyến có thể được thể hiện như sau

- Đặt tên cho bộ định tuyến

```
Router#config terminal
Router(config)#
Router(config)#hostname RouterABC
RouterABC(config)#
```

- Đặt tên mật khẩu bí mật dành cho người quản trị

```
RouterABC(config)#enable secret matkhaubimat
RouterABC(config)#
```

- Đặt tên mật khẩu cho chế độ quản trị. Mật khẩu này chỉ sử dụng khi cấu hình bộ định tuyến không có mật khẩu bí mật dành cho quản trị.

```
RouterABC(config)#enable password matkhau
RouterABC(config)#
```

- Cấu hình cho phép người dùng truy cập từ xa đến bộ định tuyến

```
RouterABC(config)#line vty 0 4
RouterABC(config-line)#login
RouterABC(config-line)#password telnet
RouterABC(config-line)#
```

- Cấu hình các giao tiếp

```
RouterABC(config)#interface ethernet 0
RouterABC(config-if)#ip address 192.168.2.1 255.255.255.0
```

```
RouterABC(config-if)#no shutdown
RouterABC(config-if)#
```

- Cấu hình định tuyến

```
RouterABC(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.2
RouterABC(config)#
```

Copy: lệnh copy cho phép thực hiện các sao chép cấu hình của bộ định tuyến đi/đến máy chủ TFTP**,** sao chép, lưu trữ, nâng cấp các tập tin IOS của bộ định tuyến từ / tới máy chủ TFTP.

Để có thể lưu bản sao cấu hình hiện hành lên máy chủ TFTP, sử dụng lệnh *copy rumng-config tftp* như được trình bày trên hình 3-30. Hình 3-31 là tiến trình ngược lại với việc tải tập tin cấu hình từ máy chủ TFTP về bộ định tuyến.

- Nhập lệnh *copy runing-config tftp*
- Nhập địa chỉ IP của máy chủ TFTP nơi dùng để lưu tập tin cấu hình
- Nhập tên ấn định cho tập tin cấu hình
- Xác nhận chọn lựa với trả lời yes

```
Router#copy running-config tftp
Address or name of remote host []? 192.168.1.5
Name of configuration file to write [Router-config]?cisco.cfg
Write file cisco.cfg to 192.168.1.5? [confirm] y
Writing cisco.cfg !!!!! [OK]
Router#
```

Hình 3-30: Lệnh copy dùng để lưu tập tin cấu hình lên máy chủ

```
Router#copy tftp running-config
Address or name of remote host []? 192.168.1.5
Source filename []? cisco.cfg
Destination filename [running-config]?
```

Hình 3-31: Lệnh copy dùng để tải tập tin cấu hình từ máy chủ

Show: là lênh được dùng nhiều và phổ biến nhất.

Lệnh show dùng để xác định trạng thái hiện hành của bộ định tuyến. Các lệnh này giúp cho phép có được các thông tin quan trọng cần biết khi kiểm tra và điều chỉnh các hoạt động của bộ định tuyến.

- show version: hiển thị cấu hình phần cứng hệ thống, phiên bản phần mềm, tên và nguồn của các tập tin cấu hình, và ảnh chương trình khởi động.

- show processes: hiển thị thông tin các quá trình hoạt động của bộ định tuyến.

- show protocols: hiển thị các giao thức được cấu hình.

- show memory: thống kê về bộ nhớ của bộ định tuyến.

- show stacks: giám sát việc sử dụng stack của các quá trình, các thủ tục ngắt và hiển thị nguyên nhân khởi động lại hệ thống lần cuối cùng.

- show buffers: cung cấp thống kê về các vùng bộ đệm trên bộ định tuyến.

- show flash: thể hiện thông tin về bộ nhớ Flash.

- show running-config: hiển thị tập tin cấu hình đang hoạt động của bộ định tuyến.

- show startup-config: hiển thị tập tin cấu hình được lưu trữ trên NVRAM và được đưa vào bộ nhớ để hoạt động khi bật nguồn bộ định tuyến. Thông thường running-config và startup-config là giống nhau. Khi thực hiện các lệnh cấu hình, running-config và startup-config sẽ không còn giống nhau, cấu hình hoạt động (running-config) cần phải được ghi trở lại NVRAM sau khi kết thúc cấu hình bộ định tuyến.

- show interfaces: thống kê các giao tiếp của bộ định tuyến. Đây là một trong các lệnh được sử dụng nhiều nhất cho biết trạng thái hoạt động của các giao tiếp, số liệu thống kê lưu lượng, số lượng các gói tin lỗi v.v...

```
Router#sh run                          Router#sh startup-config
Building configuration...              Current configuration : 677 bytes
!                                      !
Version 12.1                           Version 12.1
service timestamps debug uptime        service timestamps debug uptime
service timestamps log uptime          service timestamps log uptime
no service password-encryption         no service password-encryption
!                                      !
hostname Router                        hostname Router
!                                      !
interface Ethernet0                    interface Ethernet0
 no ip address                          no ip address
 no ip directed-broadcast               no ip directed-broadcast
 shutdown
```

Hình 3-32: Lệnh show

```
Router#show interface s0/0
Serial0/0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Description: 2M link to the Internet
  Internet address is 192.168.100.5/24
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec,
     reliability 255/255, txload 248/255, rxload 84/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/12/0 (size/max/drops/flushes); Total output
drops: 2383688
  Queueing strategy: weighted fair
  Output queue: 24/1000/64/2383671 (size/max total/threshold/drops)
     Conversations  5/184/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 677000 bits/sec, 161 packets/sec
  5 minute output rate 1996000 bits/sec, 395 packets/sec
     106754998 packets input, 2930909441 bytes, 0 no buffer
     Received 68850 broadcasts, 0 runts, 0 giants, 0 throttles
     51143 input errors, 30726 CRC, 20248 frame, 0 overrun, 0
ignored, 169 abort
```

```
     319791176 packets output, 1669977392 bytes, 0 underruns
     0 output errors, 0 collisions, 125 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Hình 3-33: Lệnh show interface

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.1(2), RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Tue 09-May-00 23:34 by linda
Image text-base: 0x80008088, data-base: 0x807D2544

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)

Router uptime is 1 week, 1 day, 1 minute
System returned to ROM by power-on at 13:29:57 Hanoi Thu Jul 31 2003
System restarted at 20:24:22 Hanoi Tue Sep 2 2003
System image file is "flash:c2600-i-mz.121-2.bin"

cisco 2620 (MPC860) processor (revision 0x102) with 26624K/6144K
bytes of memory
.
Processor board ID JAD04340ID8 (2733840160)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
1 FastEthernet/IEEE 802.3 interface(s)
2 Serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)
```

```
Configuration register is 0x2102
```

Hình 3-34: Lệnh show version

Write: lệnh write sử dụng để ghi lại cấu hình hiện đang chạy của bộ định tuyến. Nhất thiết phải dùng lệnh *write memory* để ghi lại cấu hình của bộ định tuyến vào NVRAM mỗi khi có thay đổi về cấu hình.

```
Router#write ?
  erase     Erase NV memory
  memory    Write to NV memory
  network   Write to network TFTP server
  terminal  Write to terminal
  <cr>
```

Hình 3-35: Lệnh write

III.4. Cách khắc phục một số lỗi thường gặp

Lỗi kết nối đến cổng console sử dụng Hyper Terminal

- Kiểm tra lại xem đã sử dụng chính xác loại cáp dùng để cấu hình bộ định tuyến chưa. Cáp console dùng để cấu hình bộ định tuyến là cáp 8 sợi có hai đầu RJ45 có sơ đồ đấu nối như bảng 3-8 và sử dụng đầu chuyển đổi DB9/RJ45 được cung cấp kèm theo bộ định tuyến.
- Kiểm tra xem đã sử dụng đúng cổng kết nối COM của máy tính để nối tới bộ định tuyến.

Bảng 3-8: Sơ đồ đấu nối cáp console

Console	Cáp console		DB9/RJ45	COM
Tín hiệu	RJ45	RJ45	DB9	Tín hiệu
RTS	1	8	8	CTS

DTR	2	7	6	DSR
TxD	3	6	2	RxD
GND	4	5	5	GND
GND	5	4	5	GND
RxD	6	3	3	TxD
DSR	7	2	4	DTR
CTS	8	1	7	RTS

- Kiểm tra các tham số kết nối như hình 3-20. Tốc độ kết nối phải là 9600 cho kết nối qua cổng console.

Lỗi kết nối sử dụng telnet

Khi sử dụng telnet để cấu hình từ xa bộ định tuyến, người dùng có thể không kết nối được đến bộ định tuyến. Một trong các lỗi sau cần được kiểm tra:

- Máy tính dùng để cấu hình bộ định tuyến không có kết nối mạng với bộ định tuyến. Kiểm tra lại khả năng kết nối mạng từ máy tính đến bộ định tuyến. Có thể dùng lệnh *ping* để kiểm tra.

- Khi cấu hình bộ định tuyến lần đầu, người quản trị mạng đã quên không thiết lập mật khẩu cho truy nhập từ xa. Khi cố gắng truy nhập từ xa, người dùng sẽ nhận được thông báo về việc mật khẩu truy nhập chưa được thiết lập. Trường hợp này cần sử dụng cáp console để thiết lập mật khẩu theo trình tự như trình bày dưới đây

```
Router#config terminal
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password 123456
Router(config-line)#end
Router#write memory
```

- Kiểm tra về việc có hay không có các hạn chế telnet sử dụng các danh sách kiểm soát truy nhập (access-list).

IV. Cấu hình bộ định tuyến Cisco

IV.1. Cấu hình leased-line

Giới thiệu leased-line

Leased-line, hay còn được gọi là kênh thuê riêng, là một hình thức kết nối trực tiếp giữa các node mạng sử dụng kênh truyền dẫn số liệu thuê riêng.

Kênh truyền dẫn số liệu thuê riêng thông thường cung cấp cho người sử dụng sự lựa chọn trong suốt về giao thức đấu nối hay nói cách khác, có thể sử dụng các giao thức khác nhau trên kênh thuê riêng như PPP, HDLC, LAPB v.v...

Về mặt hình thức, kênh thuê riêng có thể là các đường cáp đồng trực tiếp kết nối giữa hai điểm hoặc có thể bao gồm các tuyến cáp đồng và các mạng truyền dẫn khác nhau. Khi kênh thuê riêng phải đi qua các mạng truyền dẫn khác nhau, các quy định về giao tiếp với mạng truyền dẫn sẽ được quy định bởi nhà cung cấp dịch vụ. Do đó, các thiết bị đầu cuối CSU/DSU cần thiết để kết nối kênh thuê riêng sẽ phụ thuộc và nhà cung cấp dịch vụ. Một số các chuẩn kết nối chính được sử dụng là HDSL, G703, 2B1Q v.v...

Khi sử dụng kênh thuê riêng, người sử dụng cần thiết phải có đủ các giao tiếp trên các bộ định tuyến sao cho có một giao tiếp kết nối WAN cho mỗi một kết nối kênh thuê riêng tại mỗi node. Điều đó có nghĩa là, tại điểm node có kết nối kênh thuê riêng đến 10 điểm khác nhất thiết phải có đủ 10 giao tiếp WAN để phục vụ cho các kết nối kênh thuê riêng. Đây là một vấn đề hạn chế về đầu tư thiết bị ban đầu, không linh hoạt trong mở rộng, phát triển, phức tạp trong quản lý, đặc biệt là chi phí thuê kênh lớn đối với các yêu cầu kết nối xa về khoảng cách địa lý.

Các giao thức sử dụng với đường lease-line

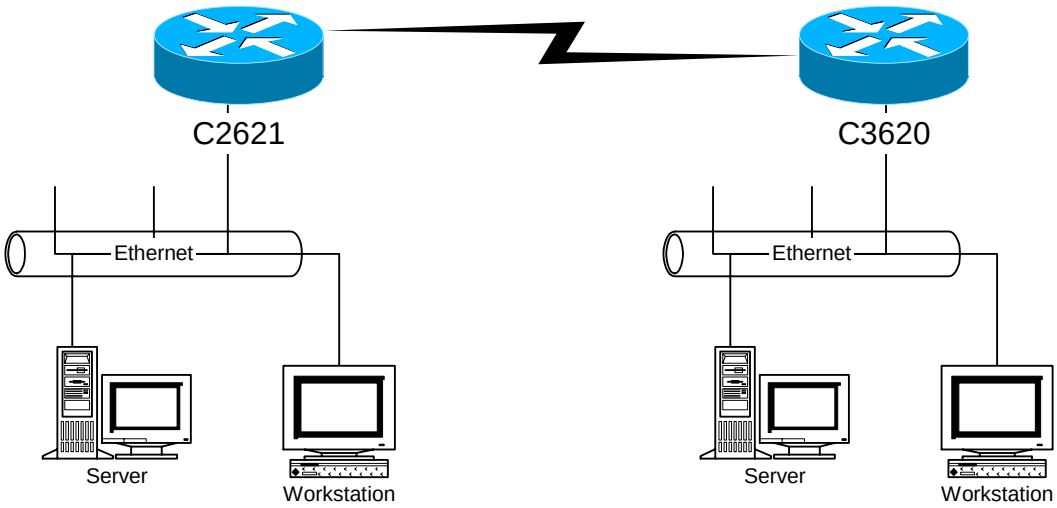
Hai giao thức sử dụng với leased-line là HDLC, PPP và LAPB. Trong đó:

- HDLC: là giao thức được sử dụng với họ các bộ định tuyến Cisco hay nói cách khác chỉ có thể sử dụng HDLC khi cả hai phía của kết nối leased-line đều là bộ định tuyến Cisco.

- PPP: là giao thức chuẩn quốc tế, tương thích với tất cả các bộ định tuyến của các hãng sản xuất khác nhau. Khi đấu nối kênh leased-line giữa một phía là thiết bị của Cisco và một phía là thiết bị của hãng thứ 3 thì nhất thiết phải dùng giao thức đấu nối này. PPP là giao thức lớp 2 cho phép nhiều giao thức mạng khác nhau có thể chạy trên nó do vậy nó được sử dụng phổ biến.

- LAPB: là giao thức truyền thông lớp hai tương tự như giao thức mạng X.25 với đầy đủ các thủ tục, quá trình kiểm soát truyền dẫn, phát hiện và sửa lỗi. LAPB ít được sử dụng.

Mô hình kết nối lease-line



Hình 3-36: Mô hình kết nối leased-line

Cấu hình kết nối lease-line cơ bản

- Phân định địa chỉ

o Việc phân định địa chỉ cho các mạng và cho các kết nối giữa các bộ định tuyến là rất quan trọng, đảm bảo cho việc liên lạc thông suốt giữa các mạng, đảm bảo cho vấn đề qui hoặch địa chỉ, nhóm gọn các định tuyến ...

o Khi thực hiện xây dựng một mạng dùng riêng, điều cần thiết phải ghi nhớ là chỉ được dùng các địa chỉ trong nhóm các địa chỉ dành cho mạng dùng riêng:10.x.x.x, 172.16.x.x – 172.31.x.x, 192.168.x.x

o Để đảm bảo không bị trùng lặp và giảm thiểu các vấn đề phát sinh, các kết nối mạng WAN theo kiểu leased-line cần được sắp xếp trên lớp mạng nhỏ nhất. Các kết nối mạng WAN trong trường hợp này được thực hiện trên các lớp mạng gồm 4 địa chỉ.

o Các lớp mạng khác tuỳ theo yêu cầu cụ thể và số lượng các địa chỉ có thể mà phân chia cho phù hợp.

- Để bắt đầu cấu hình mạng:

```
o Router> enable ↵
o Password: ****** ↵
o Router# config terminale ↵
o Router(config)#
```

- Thực hiện đặt tên, các mật khẩu, cấu hình cho phép telnet và các điều kiện cần thiết trước khi cấu hình các giao diện

- Cấu hình

```
o Router2621(config)# interface serial 0 ↵
```

- Lựa chọn giao thức sử dụng

```
o Router2621(config-if)# encapsolation HDLC ↵
```

- Đặt địa chỉ IP cho giao tiếp kết nối leased-line

```
o Router2621(config-if)# ip address 192.168.113.5
255.255.255.252 ↵
```

- Luôn phải đưa giao tiếp vào sử dụng bằng lệnh no shutdown

```
o Router2621(config-if)# no shutdown ↵
o Router2621(config-if)# interface serial 1 ↵
```

- Lựa chọn giao thức PPP sử dụng cho một giao tiếp khác

```
o Router2621(config-if)# encapsolation PPP ↵
o Router2621(config-if)# ip address 192.168.113.9
255.255.255.252 ↵
o Router2621(config-if)# no shutdown ↵
o Router2621(config-if)# exit ↵
```

- Sử dụng định tuyến tĩnh với cú pháp: ip route [địa chỉ mạng đích] [netmask] [địa chỉ next hop]

- **Router2621(config)# ip route 0.0.0.0 0.0.0.0 192.168.113.6 ↵**

- Luôn phải ghi lại cấu hình khi đã cấu hình xong

- **Router2621# write memory ↵**

- Thực hiện các phần việc còn lại tại các bộ định tuyến khác, chú ý về giao thức được sử dụng kiểm tra, giám sát các kết nối.

- Dùng lệnh **show interface** để kiểm tra trạng thái của giao tiếp

- **show interface**: xem trạng thái tất cả các giao tiếp

- **show interface serial 0**: xem trạng thái cổng serial 0

- *Serial 0 is admininistrative down line protocole is down*: thể hiện trạng thái đang bị cấu hình là không làm việc, sử dụng lệnh no shutdown trong Interface mode để đưa giao tiếp serial 0 vào làm việc

- *Serial 0 is down line protocole is down*: kiểm tra lại đường truyền

- *Serial 0 is up line protocole is down*: kiểm tra lại các giao thức được sử dụng tại hai phía

- *Serial 0 is up line protocole is up*: là trạng thái làm việc

Cấu hình bộ định tuyến 2621

```
!
hostname 2621
!
!
interface FastEthernet0/0
 ip address 10.0.5.1 255.255.255.0
!
!
interface Serial0/0
 ip address 192.168.113.5 255.255.255.252
 encapsulation ppp
!
!
```

```
ip route 0.0.0.0 0.0.0.0 192.168.113.6
!
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Hình 3-37: Cấu hình của bộ định tuyến 2621

```
Cấu hình bộ định tuyến 3620

!
hostname 3620
!
!
interface FastEthernet0/0
 ip address 10.0.6.1 255.255.255.0
!
!
interface Serial1/0
 ip address 192.168.113.6 255.255.255.252
 encapsulation ppp
!
!
ip route 0.0.0.0 0.0.0.0 192.168.113.5
!
!
line con 0
 exec-timeout 0 0
 transport input none
```

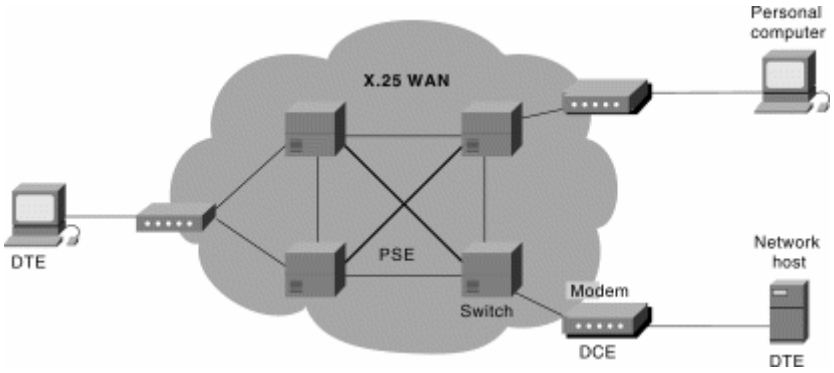
```
line aux 0
line vty 0 4
 login
!
end
```

Hình 3-38: Cấu hình của bộ định tuyến 3620

IV.2. Cấu hình X.25 & Frame Relay

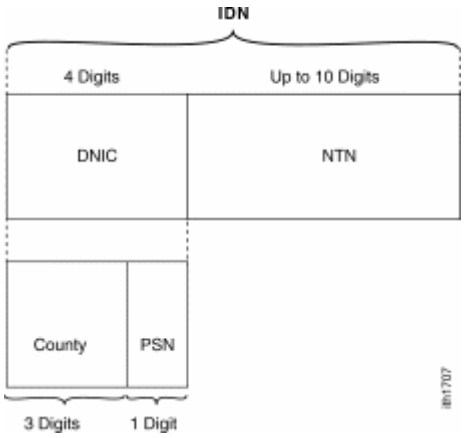
Giới thiệu X.25 và Frame Relay

X25: Năm 1978 ISO thay đổi thêm HDLC và CCITT thêm một số thông số để sinh ra LAPB "Link Access Procedure – Balanced Mode". LAPB định nghĩa một số quy luật cho mức Frame của X.25 như các loại khung đặc biệt như RR (Receive Ready), REJ (Reject) . . .



Hình 3-39: Chuyển mạch gói X.25

X.25 cung cấp các kết nối diện rộng thông qua môi trường chuyển mạch gói. Mỗi thuê bao X.25 có một địa chỉ xác định duy nhất được đánh số gồm các phần mã quốc gia, nhà cung cấp dịch vụ và địa chỉ của thuê bao trực thuộc nhà cung cấp dịch vụ.



Hình 3-40: Cấu trúc địa chỉ X.25

Khi có nhu cầu kết nối truyền dữ liệu, các thiết bị đầu cuối X.25 sẽ phát khởi tạo một VC (virtual circuit) tới địa chỉ đích. Sau khi VC được thiết lập, dữ liệu sẽ được truyền tải giữa hai điểm thông qua VC đó. Nếu nhu cầu dữ liệu lớn hơn, thiết bị đầu cuối sẽ khởi tạo thêm các VC mới. Khi hết giữ liệu, các VC sẽ được giải phóng cho các nhu cầu truyền tải khác.

X.25 qui định một số tham số xác định bao gồm:

- Độ lớn gói tin (ips/ops): là giá trị kích thước gói tin được quy định bởi nhà cung cấp dịch vụ.

- Độ lớn cửa sổ điều khiển luồng (win/wout): X.25 sử dụng cơ chế điều khiển luồng bằng cửa số để đảm bảo tốc độ gửi nhận tin phù hợp không làm mất mát thông tin. Với tham số cửa sổ bằng 7, X.25 cho phép gửi tối đa 7 gói tin khi chưa nhận được phúc đáp.

- Số lượng kênh VC tối đa cho chiều đến / hai chiều / chiều đi (hic/htc/hoc): Số lượng kênh VC được cung cấp cho mỗi thuê bao X.25 đã được xác định bởi nhà cung cấp. Thuê bao chỉ có thể truyền tải dữ liệu với số lượng các VC tối đa cho phép đã được xác định. Không thể thực hiện được yêu cầu truyền tải nếu có yêu cầu truyền tải tới các điểm mới khi số lượng VC đã hết. Khi các thiết bị đầu cuối X.25 thực hiện truyền tải dữ liệu nó phải tuân theo các quy tắc:

o Cuộc gọi ra được thực hiện từ VC lớn nhất còn trống. Điều đó có nghĩa là, nếu chưa hề có cuộc gọi nào và số VC được cung cấp cho một thuê bao là 16 thì cuộc gọi ra đầu tiên sẽ khởi tạo VC số 16 để thực hiện yêu cầu kết nối.Trong trường hợp đã dùng hết 3 VC gọi ra thì cuộc gọi ra thứ 4 sẽ sử dụng VC số 13 để thực hiện.

o Cuộc gọi tới được thực hiện từ VC nhỏ nhất còn trống. Tương tự như cuộc gọi ra, cuộc gọi vào đầu tiên sẽ nhận được trên VC số 1 và cuộc gọi vào thứ 10 sẽ nhận được trên VC số 10.

o Quá trình khởi tạo VC sẽ dừng lại khi không còn VC trống.

o Với các quy tắc này, yêu cầu cần thiết phải xác lập một cách chính xác các tham số cho thiết bị đầu cuối X.25 thì mới có thể thực hiện được các kết nối truyền tải dữ liệu.

Về đặc điểm của X.25

- Tốc độ truyền tải hạn chế, tại Việtnam tốc độ cung cấp tối đa là 128Kbps.
- Độ trễ lớn, không phù hợp cho các ứng dụng có yêu cầu cao về độ trễ.
- Khả năng mở rộng dễ dàng, chi phí không cao.
- An toàn và bảo mật, vẫn được sử dụng trong các giao dịch ngân hàng.

Frame Relay: Frame Relay ra đời trên nền tảng hạ tầng viễn thông ngày càng được cải thiện, không cần có quá nhiều các thủ tục phát hiện và sửa lỗi như X.25. Frame relay có thể chuyển nhận các khung lớn tới 4096 byte trong khi đó gói tiêu chuẩn của X.25 khuyến cáo dùng là 128 byte. Frame Relay rất thích hợp cho tryền 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.

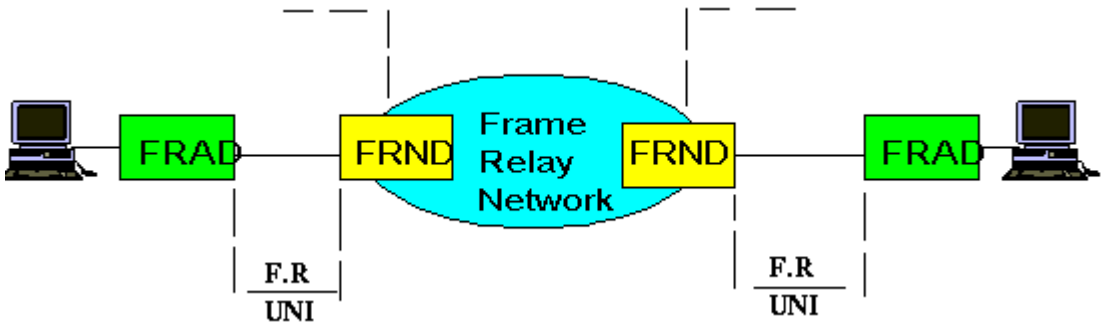
Bảng 3-9:So sánh giữa X.25 và Frame Relay

TT	Chức năng của mạng	X25	Frame relay
1	Phúc đáp khung thông tin nhận được	√	
2	Phúc đáp gói tin nhận được	√	
3	Dịch địa chỉ của gói tin	√	√
4	Cất giữ gói tin vào vùng đệm để chờ phúc đáp	√	
5	Phát hiện gói tin sai thứ tự	√	

6	Huỷ gói tin bị lỗi	√	√
7	Đảm bảo khung tin có giá trị N(s) là hợp lệ	√	
8	Thiết lập và huỷ bỏ kết nối logical	√	
9	Thiết lập và huỷ bỏ kênh ảo	√	
10	Điền các bit cờ vào giữa các khung	√	
11	Điều khiển luồng dữ liệu ở lớp liên kết logic	√	
12	Tạo và kiểm tra FCS	√	√
13	Tạo và nhận dạng bit cờ	√	√
14	Tạo ra khung báo chưa sẵn sàng	√	
15	Tạo ra khung báo đã sẵn sàng	√	
√16	Tạo ra khung báo khung bị từ chối	√	
17	Quản lý các bit D, M, Q trong gói tin	√	
18	Quản lý các khung ở mức liên kết dữ liệu	√	
19	Quản lý các bộ định thời ở mức 3	√	
20	Quản lý các bit Poll/Final trong khung	√	
21	Quản lý các bộ đếm số thứ tự của khung và gói tin	√	
22	Ghép các kênh logic	√	
23	Quản lý các thủ tục khởi động ở mức 2 và 3	√	
24	Nhận dạng các khung không hợp lệ	√	√
25	Trả lời các khung và gói tin báo chưa sẵn	√	

	sàng		
26	Trả lời các khung và gói tin báo đã sẵn sàng	√	
27	Trả lời các khung và gói tin báo từ chối khung	√	
28	Đánh dấu số lần phải truyền lại	√	
29	Chèn thêm và bỏ các bit 0 vào số liệu	√	√

Bảng chức năng trên cho thấy Frame relay đã giảm rất nhiều các công việc không cần thiết cho thiết bị chuyển mạch do đó giảm gánh nặng cũng như thời gian xử lý công việc cho các nút mạng, nhờ vậy mà làm giảm thời gian trễ cho các khung thông tin khi truyền trên mạng.



Hình 3-41: Mô hình mạng 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.

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.

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 cho từng cuộc gọi một mà phân phối băng thông một cách linh hoạt điều mà X.25 và thuê kênh riêng không có. Ví dụ người sử dụng hợp đồng sử dụng với tốc độ 64Kbps, khi họ chuyển đi một lượng thông tin quá lớn, Frame Relay cho phép truyền chúng ở tốc độ cao hơn 64Kbps. Hiện tượng này được gọi là bùng nổ Bursting.

Các đặc điểm của Frame Relay:

- Cung cấp các kết nối thông qua các kênh ảo cố định PVC. Khi có nhu cầu kết nối giữa 2 điểm, nhà cung cấp dịch vụ sẽ thiết lập các thông số trên các node Frame Relay tạo ra các kênh ảo cố định giữa 2 điểm. Không như X.25, hướng kết nối Frame Relay là cố định và không thể khởi tạo bởi người dùng. Khi có nhu cầu kết nối đến điểm đích khác, khách hàng phải thuê mới PVC đến điểm đích mới đó.

- CIR (Committed Information Rate): là tốc độ truyền dữ liệu mà nhà cung cấp dịch vụ cam kết sẽ đảm bảo cho khách hàng, điều đó có nghĩa là khách hàng sẽ được đảm bảo cung cấp đường truyền với đúng tốc độ yêu cầu. CIR được gắn liền với với các PVC và độc lập giữa các PVC khác nhau. Nếu tắc nghẽn xảy ra thì khách hàng vẫn truyền được với tốc độ yêu cầu khi ký kết hợp đồng.

- Frame Relay hỗ trợ truyền số liệu khi có bùng nổ số liệu hay còn gọi là "bursty", có nghĩa là lượng thông tin được gửi đi trong thời gian ngắn và với dung lượng lớn hơn dung lượng bình thường. Nói cách khác, khi có một nhu cầu truyền tải khối lượng dữ liệu lớn, mạng Frame Relay cho phép được thực hiện truyền tải dữ liệu với tốc độ lớn hơn tốc độ CIR đã mua của nhà cung cấp dịch vụ. Điều này đảm bảo cho khách hàng tiết kiệm được chi phí mà vẫn đảm bảo truyền dữ liệu với khối lượng lớn trong những điều kiện cần thiết đảm bảo lưu thông thông tin. Truyền dữ liệu bursty chỉ thực hiện được khi không có tắc nghẽn trên mạng.

- Frame Relay không sử dụng địa chỉ định danh như X.25. Để phân biệt các PVC, Frame Relay sử dụng DLCI, mỗi một PVC được gắn liền với một DLCI. DLCI chỉ có tính chất cục bộ có nghĩa là chỉ có ý nghĩa quản lý trên cùng một chuyển mạch. Nói cách khác số DLCI chỉ cần là duy nhất cho mỗi

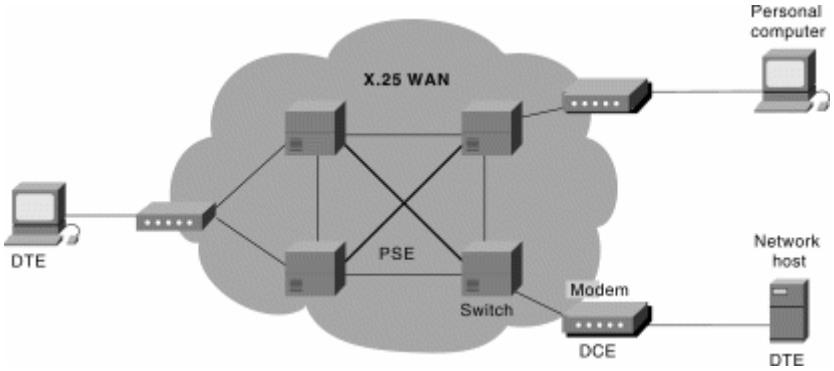
PVC trên một chuyển mạch còn có thể có cùng số DLCI đó trên một chuyển mạch khác.

- Frame Relay sử dụng giao thức LMI (Local Manegment Interface) là giao thức quản lý và trao đổi thông tin quản trị giữa các thiết bị mạng FRND và các thiết bị kết nối FRAD.

- Cũng như X.25, Frame Relay là môi trường mạng đa truy nhập không quảng bá (multiaccess nonbroadcast media). Vấn đề này cần được chú ý khi sử dụng với các giao thức định tuyến.

Các mô hình kết nối của X.25 và Frame Relay

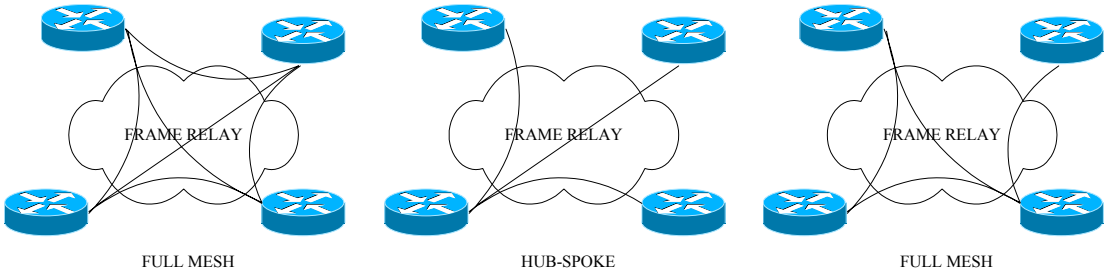
Khi sử dụng phương thức truyền thông X.25, mô hình kết nối cơ bản là điểm-đa điểm (point-to-multipoint) dựa trên tính chất cơ bản của X.25 là sử dụng các VC cho các nhu cầu truyền tải dữ liệu.



Hình 3-42: Mô hình kết nối X.25

Frame Relay đa dạng hơn về các mô hình kết nối. Frame Relay sử dụng các PVC định trước để thực hiện truyền tải dữ liệu giữa hai điểm, người ta chia Frame Relay thành các cấu hình kết nối mạng như mô tả trong hình 3-40. Trong đó:

- Full mesh: là mô hình kết nối mà trong đó bất cứ hai node mạng nào cũng có một PVC liên kết giữa chúng. Mô hình này đảm bảo tính sẵn sàng cho toàn bộ hệ thống mạng, nếu có một hoặc một vài PVC có sự cố, các PVC còn lại vẫn có thể đảm bảo cho kết nối mạng giữa các node mạng. Yếu điểm của mô hình mạng này là chi phí thuê các PVC quá lớn.



Hình 3-43: Mô hình kết nối Frame Relay

- Hub-Spoke: là mô hình có một điểm tập trung mọi kết nối Frame Relay tới các điểm khác, các trao đổi dữ liệu giữa 2 điểm bất kỳ đều phải đi qua điểm tập trung. Mô hình này có chi phí giảm thiểu nhất nhưng có yếu điểm về việc tập trung mọi gánh nặng lên điểm tập trung và nếu có bất kỳ sự cố trên một PVC nào thì sẽ mất khả năng truyền tải dữ liệu với điểm thuộc về PVC bị sự cố đó.

- Partial mesh: là mô hình được sử dụng nhiều nhất, nó là sự lai ghép giữa hai mô hình trên, đảm bảo chi phí và dự phòng cho các điểm thiết yếu.

Cấu hình X.25 cơ bản

Các lưu ý trong cấu hình X.25

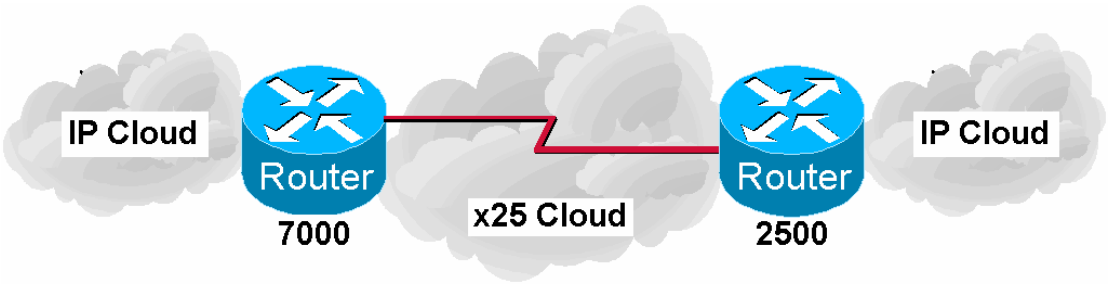
- X.25 là một môi trường đa truy nhập không broadcast (multi access non broadcast media) do đó phải lưu ý khi sử dụng với định tuyến động

- X.25 làm việc với sự khởi tạo các VC do đó khi thực hiện cấu hình phải thực hiện các thủ tục liên kết (map) và định tuyến theo địa chỉ

- Các tham số cần lưu ý

  - Độ lớn gói tin (ips/ops)
  - Độ lớn cửa sổ điều khiển luồng (win/wout)
  - Số lượng kênh VC tối đa cho chiều đến / hai chiều / chiều đi (hic/htc/hoc)
  - Số lượng VC dành cho một kết nối (nvc). Nên hạn chế số lượng VC cho phép kết nối đến một điểm trong giới hạn hợp lý để tổng số VC cần thiết không vượt quá số VC tối đa hiện có (HTC)
  - Khi thực hiện các liên kết (map) phải thực hiện map địa chỉ IP của phía đối phương tới địa chỉ X25 của họ

- Khi thực hiện định tuyến, phải thực hiện định tuyến với địa chỉ IP next hop
- Cấu hình mạng đấu nối X25 là cấu hình đa điểm, địa chỉ đấu nối phải nằm trong lớp mạng con đủ cho số lượng các điểm



Hình 3-44: Mô hình kết nối X.25 cơ bản

```
Cấu hình bộ định tuyến 7000
!
interface Serial1/1
 ip address 10.1.1.2 255.255.255.0
 encapsulation x25
 no ip mroute-cache
!--- Địa chỉ X.121 của gán cho bộ định tuyến 7000
 x25 address 4522973407000
!--- Các dòng lệnh dưới là các tham số X.25
 x25 ips 256
 x25 ops 256
 x25 htc 16
 x25 win 7
 x25 wout 7
!--- Dòng lệnh này dùng để gán địa chỉ IP của bộ định tuyến 2500 với
!địa chỉ X.121 của nó
 x25 map ip 10.1.1.1 4522973402500
!
!
```

Hình 3-45: Cấu hình của bộ định tuyến 7000

```
Cấu hình bộ định tuyến 2500
```

```
!
hostname 2500
!
interface Serial0
 ip address 10.1.1.1 255.255.255.0
 no ip mroute-cache
 encapsulation x25
 bandwidth 56
!--- Địa chỉ X.121 của gán cho bộ định tuyến 7000
 x25 address 4522973402500
!--- Các dòng lệnh dưới là các tham số X.25
 x25 ips 256
 x25 ops 256
 x25 htc 16
 x25 win 7
 x25 wout 7
!--- Dòng lệnh này dùng để gán địa chỉ IP của bộ định tuyến 7000 với
!địa chỉ X.121 của nó
 x25 map ip 10.1.1.1 4522973407000
!
```

Hình 3-46: Cấu hình của bộ định tuyến 2500

- Giám sát:
  - **Show interfaces serial 0:** dùng để kiểm tra trạng thái
  - **Show x25 vc:** hiển thị thông tin kết nối X.25
  - **Show x25 map:** hiển thị các liên kết hiện có của FR

Cấu hình Frame Relay cơ bản

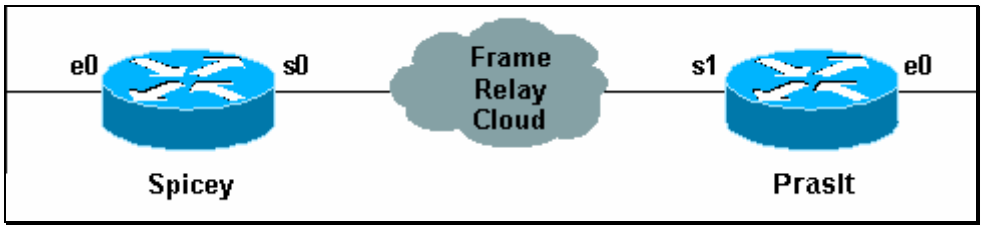
Các lưu ý trong cấu hình Frame Relay:

- Frame Relay là một môi trường đa truy nhập không broadcast (multi access non broadcast media) do đó phải lưu ý khi sử dụng với định tuyến động

- Khi sử dụng định tuyến động giao thức định tuyến vector như RIP, IGRP phải để ý đến luật Split Horizon. Luật Split Horizon là luật không cho

phép các thông tin định tuyến vừa đi vào một giao tiếp đi trở ra chính giao tiếp đó để tránh việc cập nhật sai các thông tin về định tuyến dẫn đến việc vòng đi vòng lại của các thông tin định tuyến. Vấn đề này được đặt ra do có nhiều PVC cùng chạy trên một giao tiếp vật lý.

- Giám sát:
  - **Show interfaces serial 0:** dùng để kiểm tra DLCI, LMI
  - **Show frame-relay lmi:** hiển thị thông tin tổng hợp về LMI
  - **Show frame-relay map:** hiển thị các liên kết hiện có của FR
  - **Show frame-relay pvc:** hiển thị các thông số của PVC
  - **Show frame-relay traffic:** hiển thị traffic



Hình 3-47: Mô hình kết nối Frame Relay cơ bản

- Để bắt đầu cấu hình mạng:
  - **Router> enable** ↵
  - **Password: ******** ↵
  - **Router# config terminale** ↵
  - **Router(config)#**

- Thực hiện đặt tên, các mật khẩu, cấu hình cho phép telnet và các điều kiện cần thiết trước khi cấu hình các giao diện

- Cấu hình
  - **Spicey(config)# interface serial 0** ↵

- Lựa chọn giao thức sử dụng
  - **Spicey(config-if)# encapsolation frame-relay** ↵

- Xác định giao thức quản trị LMI. Giao thức quản trị LMI nhất thiết phải có để đảm bảo việc trao đổi thông tin hai chiều giữa thiết bị đầu cuối và thiết bị mạng Frame Relay. LMI hoạt động như một thông báo keepalive.
  - **Spicey(config-if)# frame-relay lmi-type cisco** ↵

- Gán DLCI được cấp cho giao tiếp.
  - **Spicey(config-if)# frame-relay interface-dlci 140 ↵**
- Đặt địa chỉ IP cho giao tiếp kết nối leased-line
  - **Spicey(config-if)# ip address 3.1.3.1 255.255.255.0 ↵**
- Luôn phải đưa giao tiếp vào sử dụng bằng lệnh no shutdown
  - **Spicey(config-if)# no shutdown ↵**
  - **Spicey(config-if)# exit ↵**
- Sử dụng định tuyến động RIP
  - **Spicey(config)# router rip ↵**
  - **Spicey(config-router)# network 3.0.0.0 ↵**
  - **Spicey(config-router)# network 124.0.0.0 ↵**
  - **Spicey(config-router)# end ↵**
- Luôn phải ghi lại cấu hình khi đã cấu hình xong
  - **Spicey# write memory ↵**
- Thực hiện các phần việc còn lại tại các bộ định tuyến khác, chú ý về giao thức được sử dụng kiểm tra, giám sát các kết nối.

Cấu hình bộ định tuyến Spicey

```
Current configuration : 1705 bytes
!
version 12.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Spicey
!
interface Ethernet0
 ip address 124.124.124.1 255.255.255.0
!
interface Serial0
```

```
 ip address 3.1.3.1 255.255.255.0
 encapsulation frame-relay
 frame-relay interface-dlci 140
!
!
router rip
 network 3.0.0.0
 network 124.0.0.0
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

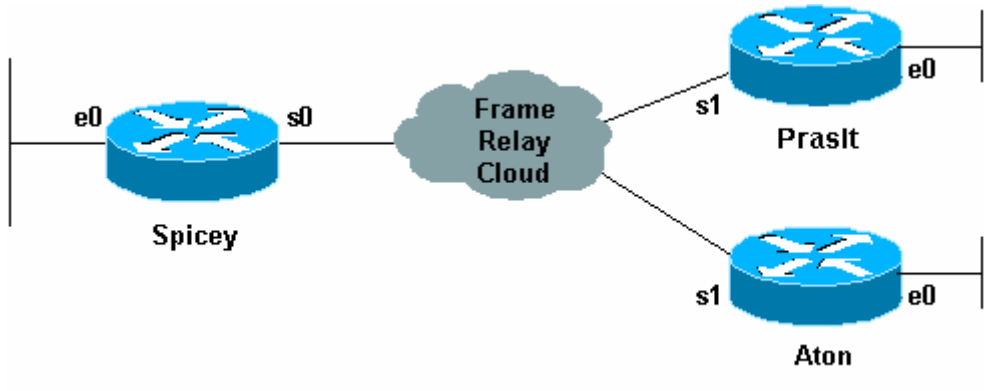
Hình 3-48: Cấu hình của bộ định tuyến Spicey

Cấu hình bộ định tuyến Prasit

```
Current configuration : 1499 bytes
!
version 12.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Prasit
!
!
!
interface Ethernet0
 ip address 123.123.123.1 255.255.255.0
```

```
!
!
interface Serial1
 ip address 3.1.3.2 255.255.255.0
 encapsulation frame-relay
 frame-relay interface-dlci 150
!
!
router rip
 network 3.0.0.0
 network 123.0.0.0
!
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Hình 3-49: Cấu hình của bộ định tuyến Prasit



Hình 3-50: Mô hình kết nối Frame Relay Hub-Spoke

- Cấu hình

o `Spicey(config)# interface serial 0 ↵`

- Lựa chọn giao thức sử dụng

```
Spicey(config-if)# encapsolation frame-relay ↵
```

- Xác định giao thức quản trị LMI. Lưu ý trong ví dụ này có sử dụng một chuẩn kết nối LMI khác. Chuẩn kết nối LMI không có giá trị toàn cục mà chỉ có giá trị tại giao tiếp của thiết bị đầu cuối với mạng Frame Relay. Trong cấu hình của các bộ định tuyến khác vẫn sử dụng LMI chuẩn cisco.

```
Spicey(config-if)# frame-relay lmi-type ansi ↵
```

- Luôn phải đưa giao tiếp vào sử dụng bằng lệnh no shutdown

```
Spicey(config-if)# no shutdown ↵
```

- Trong ví dụ này, sử dụng giao tiếp con, subinterface, nên không đặt địa chỉ cho giao tiếp thực, physical interface.

- Cấu hình giao tiếp con. Giao tiếp con phải sử dụng một trong hai lựa chọn là point-to-point hoặc multipoint, ở đây sử dụng point-to-point cho giao tiếp con s0.1 và multipoint cho giao tiếp con s0.2.

```
Spicey(config-if)# interface serial 0.1 point-to-point ↵
```

- Hoặc

```
Spicey(config-if)# exit ↵
Spicey(config)# interface serial 0.1 point-to-point ↵
```

- Gán DLCI được cấp cho giao tiếp. DLCI 140 là DLCI gắn với PVC nối giữa Spicey và Prasit, còn DLCI 130 gắn với PVC nối tới Aton.

```
Spicey(config-if)# frame-relay interface-dlci 140 ↵
```

- Xác lập địa chỉ IP cho giao tiếp con thứ nhất

```
Spicey(config-subif)# ip address 4.0.1.1 255.255.255.0 ↵
Spicey(config-subif)# exit ↵
```

- Cấu hình giao tiếp con thứ hai tới Aton

```
Spicey(config)# interface serial 0.2 multipoint ↵
```

- Gán DLCI được cấp cho giao tiếp là DLCI 130

```
Spicey(config-if)# frame-relay interface-dlci 130 ↵
```

- Xác lập địa chỉ IP cho giao tiếp con thứ 2

```
Spicey(config-subif)# ip address 3.1.3.1 255.255.255.0 ↵
Spicey(config-subif)# exit ↵
```

- Sử dụng định tuyến động RIP

```
Spicey(config)# router rip ↵
Spicey(config-router)# network 3.0.0.0 ↵
Spicey(config-router)# network 4.0.0.0 ↵
Spicey(config-router)# network 124.0.0.0 ↵
Spicey(config-router)# end ↵
```

- Luôn phải ghi lại cấu hình khi đã cấu hình xong

```
Spicey# write memory ↵
```

- Thực hiện các phần việc còn lại tại các bộ định tuyến khác, chú ý về giao thức được sử dụng kiểm tra, giám sát các kết nối.

Cấu hình bộ định tuyến Spicey

```
Spicey#show running-config
Building configuration...
!
version 12.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Spicey
!
!
interface Ethernet0
 ip address 124.124.124.1 255.255.255.0
!
interface Serial0
 no ip address
 encapsulation frame-relay
 frame-relay lmi-type ansi
!
```

```
interface Serial0.1 point-to-point
 ip address 4.0.1.1 255.255.255.0
 frame-relay interface-dlci 140
!
interface Serial0.2 multipoint
 ip address 3.1.3.1 255.255.255.0
 frame-relay interface-dlci 130
!
router igrp 2
 network 3.0.0.0
 network 4.0.0.0
 network 124.0.0.0
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Hình 3-51: Cấu hình của bộ định tuyến Spicey

```
Cấu hình bộ định tuyến Prasit

Prasit#show running-config
Building configuration...

version 12.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
```

```
hostname Prasit
!
interface Ethernet0
 ip address 123.123.123.1 255.255.255.0
!
interface Serial1
 no ip address
 encapsulation frame-relay
!
!--- LMI cisco là mặc định nên không thể hiện trong cấu hình
!--- Prasit và Spicey đã sử dụng 2 kiểu LMI khác nhau
!--- Bộ định tuyến tại Prasit sử dụng giao tiếp con point-to-point
interface Serial1.1 point-to-point
 ip address 4.0.1.2 255.255.255.0
 frame-relay interface-dlci 150
!
router igrp 2
 network 4.0.0.0
 network 123.0.0.0
!
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Hình 3-52: Cấu hình của bộ định tuyến Prasit

```
Cấu hình bộ định tuyến Aton

Aton#show running-config
```

```
Building configuration...


Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
!
hostname Aton
!
!
!
interface Ethernet0
 ip address 122.122.122.1 255.255.255.0
!
interface Serial1
 ip address 3.1.3.3 255.255.255.0
 encapsulation frame-relay
 frame-relay lmi-type q933a
!--- Aton có kiểu LMI khác hai bộ định tuyến kia
!--- Aton không sử dụng giao tiếp con. Giao tiếp con cần xác định
!là point-to-point hay multipoint ở bộ định tuyến trung tâm
!còn ở các bộ định tuyến còn lại có thể dùng giao tiếp con
!point-to-point hay giao tiếp thực, physical interface
 frame-relay interface-dlci 160
!
router igrp 2
 network 3.0.0.0
 network 122.0.0.0
!
line con 0
 exec-timeout 0 0
 transport input none
```

```
line aux 0
line vty 0 4
 login
!
end
```

Hình 3-53: Cấu hình của bộ định tuyến Aton

IV.3. Cấu hình Dial-up

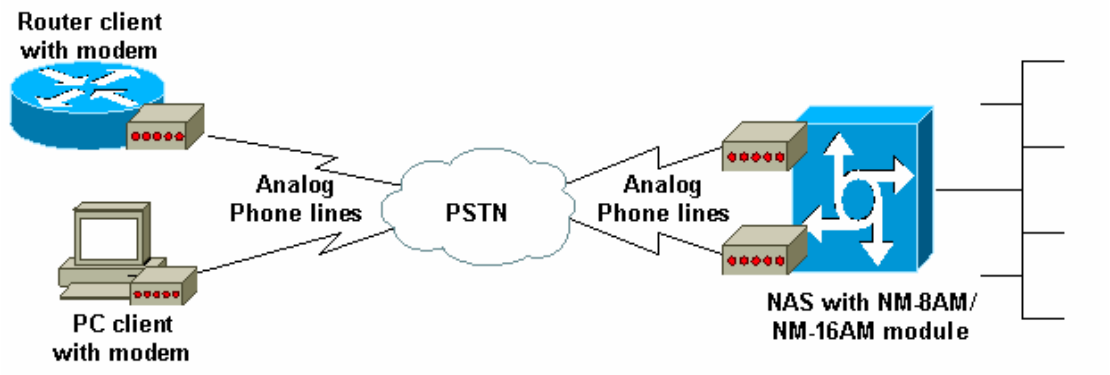
Giới thiệu quay số

Kết nối quay số cho phép sử dụng đường điện thoại để kết nối trao đổi dữ liệu. Tốc độ của kết nối quay số là không cao và chỉ có thể đáp ứng được cho các ứng dụng không yêu cầu về băng thông cũng như thời gian trễ.

Kết nối quay số sử dụng modem V34, V90 là phổ biến. Tốc độ truyền dữ liệu lên mạng và tải dữ liệu về tối đa là 33,6Kbps. Để có thể thực hiện tải về với tốc độ lớn hơn, tới 56Kbps, bộ định tuyến đóng vai trò điểm truy nhập phải có kết nối thuê bao dạng số và dùng modem số.

Đối với các doanh nghiệp nhỏ, việc xác thực người dùng có thể thực hiện bằng cách khai báo dữ liệu trực tiếp trên bộ định tuyến. Cách sử dụng này không thích hợp cho các doanh nghiệp vừa và lớn hay các doanh nghiệp cần có sự quản lý chặt chẽ người dùng một cách hệ thống. Lúc này cần thiết có các hệ thống quản lý người dùng. Các bộ định tuyến của Cisco cho phép sử dụng hai chuẩn xác thực TACACS+ và RADIUS.

Mô hình sử dụng quay số



Hình 3-54: Cấu hình của bộ định tuyến Aton

Cấu hình quay số cơ bản

Danh mục công việc:

- Cấu hình giao tiếp không đồng bộ Async
- Cấu hình giao tiếp điều khiển modem
- Cấu hình xác thực
- Giám sát
  - **Router#show interface Async 1**
  - **Router#show line 1**
  - **Router#debug ppp authentication**

Cấu hình quay số cơ bản

```
Current configuration : 1251 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
!
hostname cisco3640
!
boot system flash:c3640-i-mz.122-8.T
enable secret 5 <đã xóa>
!
! --- Tên truy nhập cho xác thực người dùng cục bộ
username abc password 0 abc
!
ip subnet-zero
!
no ip domain-lookup
ip domain-name cisco.com
```

```
!
! --- Xác định địa chỉ máy chủ DNS cho các máy trạm quay số
async-bootp dns-server 5.5.5.1 5.5.5.2
!
!
interface Loopback0
  ip address 1.1.1.1 255.255.255.0
!
interface Ethernet2/0
  ip address 20.20.20.1 255.255.255.0
  half-duplex
!
! <<--các giao tiếp không dùng được bỏ đi
!
!--- Giao tiếp Group-Async1 cấu hình cho tất cả các các modem
!--- không cần cấu hình riêng rẽ từng modem
interface Group-Async1
  ip unnumbered Loopback0
  encapsulation ppp
  dialer in-band
!--- Xác lập thời gian không sử dụng là 10 phút
!--- sau thời gian này, bộ định tuyến sẽ tự động cắt kết nối
  dialer idle-timeout 600
!--- Định nghĩa các loại hình dữ liệu được dùng
!--- thông qua cấu hình dialer-group và dialer-list
  dialer-group 1
!--- Chế độ interative cho phép người dùng sử dụng nhiều giao thức
!--- để không cho phép người dùng thiết lập các kết nối đến bộ định
tuyến sử dụng chế độ dedicated
  async mode interactive
!--- Các máy trạm khi quay số vào sẽ được cấp địa chỉ IP
!--- được qui định trong DIALIN
  peer default ip address pool DIALIN
  ppp authentication chap
```

```
!--- Xác lập các modem từ line 1 đến line 8 thuộc về nhóm này
  group-range 1 8
!
ip local pool DIALIN 10.1.1.1 10.1.1.10
ip classless
ip route 0.0.0.0 0.0.0.0 20.20.20.100
ip http server
ip pim bidir-enable
!
!--- Dòng lệnh sau cho phép giao thức IP là giao thức hoạt động
!--- nếu không có các dữ liệu IP đi qua sau khoảng thời gian 10 phút
!--- đường kết nối sẽ bị cắt
dialer-list 1 protocol ip permit
!
line con 0
  password abc
line 1 8
!--- Dòng lệnh dưới cho phép modem quay vào và quay ra
  modem InOut
  transport input all
  autoselect ppp
  flowcontrol hardware
line aux 0
line vty 0 4
  login
!
!
end
```

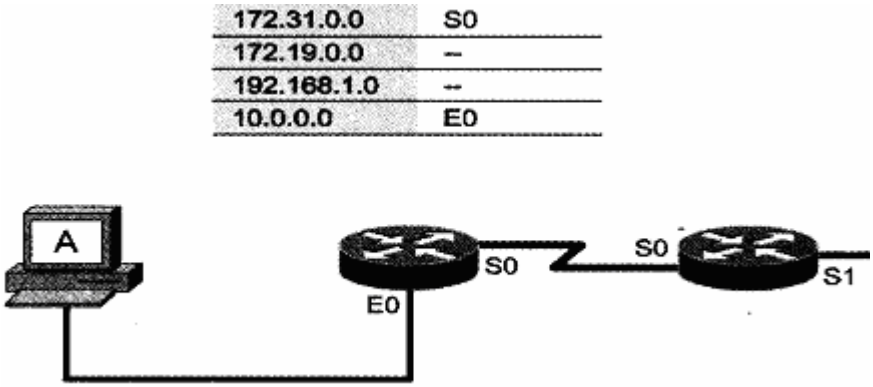
Hình 3-55: Cấu hình quay số cơ bản

IV.4. Định tuyến tĩnh và động

Sơ lược về định tuyến

Chức năng xác định đường dẫn cho phép bộ định tuyến ước lượng các đường dẫn khả thi để đến đích và thiết lập sự kiểm soát các gói tin. Bộ định tuyến sử dụng các cấu hình mạng để đánh giá các đường dẫn mạng. Thông tin này có thể được cấu hình bởi người quản trị mạng hay được thu thập thông qua quá trình xử lý động được thực thi trên mạng.

Lớp mạng dùng bảng định tuyến IP để gửi các gói tin từ mạng nguồn đến mạng đích. Bộ định tuyến dựa vào các thông tin được giữ trong bảng định tuyến để quyết định truyền tải các gói tin theo các giao tiếp thích hợp.



Hình 3-56: Sử dụng bảng định tuyến để truyền tải các gói tin

Một bảng định tuyến IP bao gồm các địa chỉ mạng đích, địa chỉ của điểm cần đi qua, giá trị định tuyến và giao tiếp để thực hiện việc truyền tải. Khi không có thông tin về mạng đích, bộ định tuyến sẽ gửi các gói tin theo một đường dẫn mặc định được cấu hình trên bộ định tuyến, nếu đường dẫn không tồn tại, bộ định tuyến tự động loại bỏ gói tin.

Có hai phương thức định tuyến là:

- Định tuyến tĩnh (static routing): là cách định tuyến không sử dụng các giao thức định tuyến. Các định tuyến đến một mạng đích sẽ được thực hiện một cách cố định không thay đổi trên mỗi bộ định tuyến. Mỗi khi thực hiện việc thêm hay bớt các mạng, phải thực hiện thay đổi cấu hình trên mỗi bộ định tuyến.

- Định tuyến động (dynamic routing): là việc sử dụng các giao thức định tuyến để thực hiện xây dựng nên các bảng định tuyến trên các bộ định tuyến. Các bộ định tuyến thông qua các giao thức định tuyến sẽ tự động trao đổi các

thông tin định tuyến, các bảng định tuyến với nhau. Mỗi khi có sự thay đổi về mạng, chỉ cần khai báo thông tin mạng mới trên bộ định tuyến quản lý trực tiếp mạng mới đó mà không cần phải khai báo lại trên mỗi bộ định tuyến. Một số giao thức định tuyến động được sử dụng là RIP, RIPv2, OSPF, EIGRP v.v...

Giá trị định tuyến được xây dựng tùy theo các giao thức định tuyến khác nhau. Giá trị định tuyến của các kết nối trực tiếp và định tuyến tĩnh có giá trị nhỏ nhất bằng 0, đối với định tuyến động thì giá trị định tuyến được tính toán tùy thuộc và từng giao thức cụ thể. Giá trị định tuyến được thể hiện trong bảng định tuyến là giá trị định tuyến tốt nhất đã được bộ định tuyến tính toán và xây dựng nên trên cơ sở các giao thức định tuyến được cấu hình và giá trị định tuyến của từng giao thức.

Các giao thức định tuyến động được chia thành 2 nhóm chính:

- **Các giao thức định tuyến khoảng cách véc tơ** (distance-vecto, *sau đây được gọi tắt là định tuyến vectơ)*: dựa vào các giải thuật định tuyến có cơ sở hoạt động là khoảng cách véc tơ.

Theo định kỳ các bộ định tuyến chuyển toàn bộ các thông tin có trong bảng định tuyến đến các bộ định tuyến láng giềng đấu nối trực tiếp với nó và cũng theo định kỳ nhận các bảng định tuyến từ các bộ định tuyến láng giềng. Sau khi nhận được các bảng định tuyến từ các bộ định tuyến láng giềng, bộ định tuyến sẽ so sánh với bảng định tuyến hiện có và quyết định về việc xây dựng lại bảng định tuyến theo thuật toán của từng giao thức hay không. Trong trường hợp phải xây dựng lại, bộ định tuyến sau đó sẽ gửi bảng định tuyến mới cho các láng giềng và các láng giềng lại thực hiện các công việc tương tự. Các bộ định tuyến tự xác định các láng giềng trên cơ sở thuật toán và các thông tin thu lượm từ mạng.

Từ việc cần thiết phải gửi các bảng định tuyến mới lại cho các láng giềng và các láng giềng sau khi xây dựng lại bảng định tuyến lại gửi trở lại bảng định tuyến mới, định tuyến thành vòng có thể xảy ra nếu sự hội về trạng thái bền vững của mạng diễn ra chậm trên một cấu hình mới. Các bộ định tuyến sử dụng các kỹ thuật bộ đếm định thời để đảm bảo không nảy sinh việc xây dựng một bảng định tuyến sai. Có thể diễn giải điều đó như sau:

- Khi một bộ định tuyến nhận một cập nhật từ một láng giềng chỉ rằng một mạng có thể truy xuất trước đây, nay không thể truy xuất được nữa, bộ

định tuyến đánh dấu tuyến là không thể truy xuất và khởi động một bộ định thời.

o Nếu tại bất cứ thời điểm nào mà trước khi bộ định thời hết hạn một cập nhật được tiếp nhận cũng từ láng giềng đó chỉ ra rằng mạng đã được truy xuất trở lại, bộ định tuyến đánh dấu là mạng có thể truy xuất và giải phóng bộ định thời.

o Nếu một cập nhật đến từ một bộ định tuyến láng giềng khác với giá trị định tuyến tốt hơn giá trị định tuyến được ghi cho mạng này, bộ định tuyến đánh dấu mạng có thể truy xuất và giải phóng bộ định thời. Nếu giá trị định tuyến tồi hơn, cập nhật được bỏ qua.

o Khi bộ định thời được đếm về 0, giá trị định tuyến mới được xác lập, bộ định tuyến có bảng định tuyến mới.

- **Các giao thức định tuyến trạng thái đường** (link-state, *gọi tắt là định tuyến trạng thái*): Giải thuật cơ bản thứ hai được dùng cho định tuyến là giải thuật 1ink-state. Các giải thuật định tuyến trạng thái, cũng được gọi là SPF (shortest path first, *chọn đường dẫn ngắn nhất*), duy trì một cơ sở dừ liệu phức tạp chứa thông tin về cấu hình mạng.

- Trong khi giải thuật vectơ không có thông tin đặc biệt gì về các mạng ở xa và cũng không biết các bộ định tuyến ở xa, giải thuật định tuyến trạng thái biết được đầy đủ về các bộ định tuyến ở xa và biết được chúng liên kết với nhau như thế nào.

Giao thức định tuyến trạng thái sử dụng:

o Các thông báo về trạng thái liên kết: LSA (Link State Advertisements).

o Một cơ sở dữ liệu về cấu hình mạng.

o Giải thuật SPF, và cây SPF sau cùng.

o Một bảng định tuyến liên hệ các đường dẫn và các cổng đến từng mạng.

Hoạt động tìm hiểu khám phá mạng trong định tuyến trạng thái được thực hiện như sau:

o Các bộ định tuyến trao đổi các LSA cho nhau. Mỗi bộ định tuyến bắt đầu với các mạng được kết nối trực tiếp để lấy thông tin.

- Mỗi bộ định tuyến đồng thời với các bộ định tuyến khác tiến hành xây dựng một cơ sở dữ liệu về cấu hình mạng bao gồm tất cả các LSA đến từ liên mạng.

- Giải thuật SPF tính toán mạng có thể đạt đến. Bộ định tuyến xây dựng cấu hình mạng luận lý này như một cây, tự nó là gốc, gồm tất cả các đường dẫn có thể đến mỗi mạng trong toàn bộ mạng đang chạy giao thức định tuyến trạng thái. Sau đó, nó sắp xếp các đường dẫn này theo chiến lược chọn đường dẫn ngắn nhất.

- Bộ định tuyến liệt kê các đường dẫn tốt nhất của nó, và các cổng dẫn đến các mạng đích, trong bảng định tuyến của nó. Nó cũng duy trì các cơ sở dữ liệu khác về các phần tử cấu hình mạng và các chi tiết về hiện trạng của mạng.

Khi có thay đổi về cấu hình mạng, bộ định tuyến đầu tiên nhận biết được sự thay đổi này gửi thông tin đến các bộ định tuyến khác hay đến một bộ định tuyến định trước được gán là tham chiếu cho tất cả các các bộ định tuyến trên mạng làm căn cứ cập nhật.

- Theo dõi các láng giềng của nó, xem xét có hoạt động hay không, và giá trị định tuyến đến láng giềng đó.

- Tạo một gói LSA trong đó liệt kê tên của tất cả các bộ định tuyến láng giềng và các giá trị định tuyến đối với các láng giềng mới, các thay đổi trong giá trị định tuyến, và các liên kết dẫn đến các láng giềng đã được ghi.

- Gửi gói LSA này đi sao cho tất cả các bộ định tuyến đều nhận được.

- Khi nhận một gói LSA, ghi gói LSA vào cơ sở dữ liệu để sao cho cập nhật gói LSA mới nhất được phát ra từ mỗi bộ định tuyến.

- Hoàn thành bản đồ của liên mạng bằng cách dùng dữ liệu từ các gói LSA tích lũy được và sau đó tính toán các tuyến dẫn đến tất cả các mạng khác sử dụng thuật toán SPF.

Có hai vấn đề lưu ý đối với giao thức định tuyến trạng thái:

- Hoạt động của các giao thức định tuyến trạng thái trong hầu hết các trường hợp đều yêu cầu các bộ định tuyến dùng nhiều bộ nhớ và thực thi nhiều hơn so với các giao thức định tuyến theo vectơ. Các yêu cầu này xuất phát từ việc cần thiết phải lưu trữ thông tin của tất cả các láng giềng, cơ sở dữ liệu mạng đến từ các nơi khác và việc thực thi các thuật toán định tuyến trạng thái.

Người quản lý mạng phải đảm bảo rằng các bộ định tuyến mà họ chọn có khả năng cung cấp các tài nguyên cần thiết này.

o Các nhu cầu về băng thông cần phải tiêu tốn để khởi động sự phát tán gói trạng thái. Trong khi khởi động quá trình khám phá, tất cả các bộ định tuyến dùng các giao thức định tuyến trạng thái để gửi các gói LSA đến tất cả các bộ định tuyến khác. Hành động này làm tràn ngập mạng khi mà các bộ định tuyến đồng loạt yêu cầu băng thông và tạm thời làm giảm lượng băng thông khả dụng dùng cho lưu lượng dữ liệu thực được định tuyến. Sau khởi động phát tán này, các giao thức định tuyến trạng thái thường chỉ yêu cầu một lượng băng thông tối thiểu để gửi các gói LSA kích hoạt sự kiện không thường xuyên nhằm phản ánh sự thay đổi của cấu hình mạng.

- **Và một nhóm giao thức thứ 3** là nhóm các giao thức định tuyến lai ghép giữa 2 nhóm trên hay nói cách khác có các tính chất của cả hai nhóm giao thức trên.

Các giao thức định tuyến

Bảng 3-10:Các giao thức định tuyến

Các đặc trưng	RIPv1	RIPv2	IRGP	EIGRP	OSPF
Khoảng cách vectơ	x	x	x	x	
Trạng thái đường					x
Tự động tóm tắt định tuyến	x	x	x	x	
Hỗ trợ VLSM[1]		x		x	x
Tương thích với sản phẩm thứ ba	x	x			x
Thích hợp	Nhỏ	Nhỏ	Vừa	Lớn	Lớn

[1] VLSM (Vary Length Subnet Mask): hỗ trợ định tuyến cho các mạng con subnetmask có độ dài thay đổi hay nói cách khác thông tin về subnetmask bao gồm trong bảng định tuyến

Thời gian hội tụ về trạng thái cân bằng	Chậm	Chậm	Chậm	Nhanh	Nhanh
Giá trị định tuyến	hop count[2]	hop count	~ BW[3]+D[4]	~ BW+D	~ 10E8/BW
Giới hạn hop count	15	15	100	100	
Cân bằng tải cùng giá trị định tuyến	x	x	x	x	x
Cân bằng tải không cùng giá trị định tuyến			x	x	
Thuật toán	Bellman-Ford	Bellman-Ford	Bellman-Ford	DUAL	Dijkstra

Cấu hình định tuyến động cơ bản với RIP

Một số lưu ý khi cấu hình định tuyến động với RIP

- RIP gửi các thông tin cập nhật theo các chu kỳ định trước, giá trị mặc định là 30 giây, và khi có sự thay đổi bảng định tuyến.

- RIP sử dụng số đếm các node (hop count) để làm giá trị đánh giá chất lượng của định tuyến (metric). RIP chỉ giữ duy nhất định tuyến có giá trị định tuyến thấp nhất.

- Giá trị hop count tối đa cho phép là 15.

- RIP sử dụng các bộ đếm thời gian cho việc thực hiện gửi các thông tin cập nhật, xoá bỏ một định tuyến trong bảng cũng như để điều khiển các quá trình tạo lập bảng định tuyến, tránh loop vòng.

- RIPv1: Classfull: không có thông tin về subnetmask

- RIPv2: Classless: có thông tin về subnetmask

[2] Hop count: được tính bằng số các điểm node mạng mà gói tin phải đi qua từ điểm này đến điểm kia hay chính bằng số các bộ định tuyến mà gói tin phải đi qua

[3] BW (bandwitch): băng thông

[4] D (delay): trễ

Cấu hình định tuyến với RIP:

- Cho phép giao thức định tuyến RIP hoạt động trên bộ định tuyến.

```
Router(config)#router rip
```

- Thiết lập các cấu hình mạng. Network là nhóm mạng tính theo lớp mạng cơ bản đang có các giao tiếp trực tiếp trên bộ định tuyến.

```
Router(config-router)#network 192.168.100.0
Router(config-router)#network 172.25.0.0
Router(config-router)#network 10.0.0.0
```

- Trong trường hợp sử dụng RIP với các mạng không phải là mạng broadcast như X.25, Frame Relay cần thiết cấu hình RIP với các địa chỉ Unicast là các địa chỉ mà RIP sẽ gửi tới các thông tin cập nhật

```
Router(config-router)#neighbor 192.168.113.1
Router(config-router)#neighbor 192.168.113.5
```

- Tuỳ theo điều kiện cụ thể về hạ tầng mạng có thể thay đổi chu kỳ cập nhật thông tin, các định nghĩa thời gian khác cho phù hợp.

```
Router(config-router)# timers basic update invalid holddown flush [sleeptime]
```

- Các thay đổi khác.

```
Router(config-router)# version {1 | 2}
Router(config-router)# ip rip authentication key-chain name-of-chain
Router(config-router)# ip rip authentication mode {text | md5}
```

- Giám sát.

```
show ip interfaces
show ip rip
```

Cấu hình bộ định tuyến với RIP

```
Current configuration : 1499 bytes
!
version 12.1
service timestamps debug datetime msec
service timestamps log datetime msec
```

```
no service password-encryption
!
hostname Prasit
!
!
interface Ethernet0
 ip address 123.123.123.1 255.255.255.0
!
!
interface Serial1
 ip address 3.1.3.2 255.255.255.0
 encapsulation frame-relay
 frame-relay interface-dlci 150
!
!
router rip
 network 3.0.0.0
 network 123.0.0.0
!
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Hình 3-57: Cấu hình của bộ định tuyến với RIP

V. Bài tập thực hành sử dụng bộ định tuyến Cisco

Bài 1: Thực hành nhận diện thiết bị, đấu nối thiết bị

Yêu cầu:

- Nhận diện đúng các chủng loại thiết bị
- Nhận diện các giao tiếp của bộ định tuyến, ý nghĩa và mục đích sử dụng
- Biết cách sử dụng các loại cáp với từng loại thiết bị, giao tiếp khác nhau
- Biết đấu nối bộ định tuyến với nhau và với các thiết bị modem khác
- Sử dụng phần mềm HyperTerminal kết nối với bộ định tuyến

Bài 2: Thực hành các lệnh cơ bản

- Các lệnh show
- Lệnh config

Yêu cầu:

- Nắm vững ý và sử dụng thành thạo các lệnh kiểm tra và các lệnh cấu hình cơ bản

Bài 3: Cấu hình bộ định tuyến với mô hình đấu nối leased-line

- Cấu hình Interface
- Cấu hình giao thức
- Cấu hình định tuyến

Yêu cầu:

- Sử dụng thiết bị phòng lab để cấu hình một kết nối leased-line cho phép kết nối 2 mạng với nhau.
- Vận dụng các kiến thức đã học kiểm soát và xử lý sự cố.

Bài 4: Cấu hình bộ định tuyến với Dial-up

- Cấu hình line vật lý
- Cấu hình async interface
- Cấu hình định tuyến
- Cấu hình xác thực

Yêu cầu:

- Sử dụng thiết bị phòng lab để cấu hình một điểm truy nhập gián tiếp quay số qua thoại.
- Vận dụng các kiến thức đã học kiểm soát và xử lý sự cố.

Thiết bị phòng lab

- 02 bộ định tuyến 2509 (leased-line và async) hoặc tương đương
- 02 modem leased-line CSU/DSU dùng cho kết nối leased-line
- 02 cáp V.35 DTE
- 04 modem dial-up 56kbps
- 02 cáp Async dùng cho kết nối modem 56kbps
- Phần mềm giả lập bộ định tuyến (router simulator)
- 02 máy tính dùng để cấu hình trực tiếp các bộ định tuyến
- các máy tính để thực hành trên phần mềm giả lập bộ định tuyến
- 04 đường điện thoại

Chương 4 : Hệ thống tên miền DNS

Chương 4 sẽ tập trung nghiên cứu về hệ thống tên miền là một hệ thống định danh phổ biến trên mạng TCP/IP nói chung và đặc biệt là mạng Internet.

Hệ thống tên miền tối quan trọng cho sự phát triển của các ứng dụng phổ biến như thư tín điện tử, web...Cấu trúc hệ thống tên miền, cấu trúc và ý nghĩa của các trường tên miền cũng như các kỹ năng cơ bản được cung cấp sẽ giúp cho người quản trị có thể hoạch định được các nhu cầu liên quan đến tên miền cho mạng lưới, tiến hành thủ tục đăng ký chính xác (nếu đăng ký tên miền Internet) và đảm nhận được các công tác tạo mới, sửa đổi ... hay nói chung là các công việc quản trị hệ thống máy chủ tên miền DNS

Chương 4 đòi hỏi các học viên phải quen thuộc với địa chỉ IP, việc soạn thảo quản trị các tiến trình trên các hệ thống linux, unix, windows.

I. Giới thiệu

I.1. Lịch sử hình thành của DNS

Vào những năm 1970 mạng ARPanet của bộ quốc phòng Mỹ rất nhỏ và dễ dàng quản lý các liên kết vài trăm máy tính với nhau. Do đó mạng chỉ cần một file HOSTS.TXT chứa tất cả thông tin cần thiết về máy tính trong mạng và giúp các máy tính chuyển đổi được thông tin địa chỉ và tên mạng cho tất cả máy tính trong mạng ARPanet một cách dễ dàng. Và đó chính là bước khởi đầu của hệ thống tên miền gọi tắt là DNS (Domain name system)

Như khi mạng máy tính ARPanet ngày càng phát triển thì việc quản lý thông tin chỉ dựa vào một file HOSTS.TXT là rất khó khăn và không khả thi. Vì thông tin bổ xung và sửa đổi vào file HOSTS.TXT ngày càng nhiều và nhất là khi ARPanet phát triển hệ thống máy tính dựa trên giao thức TCP/IP dẫn đến sự phát triển tăng vọt của mạng máy tính:

- Lưu lượng và trao đổi trên mạng tăng lên
- Tên miền trên mạng và địa chỉ ngày càng nhiều
- Mật độ máy tính ngày càng cao do đó đảm bảo phát triển ngày càng khó khăn

Đến năm 1984 Paul Mockpetris thuộc viện USC's Information Sciences Institute phát triển một hệ thống quản lý tên miền mới (miêu tả trong chuẩn RFC 882 - 883) gọi là DNS (Domain Name System) và ngày này nó ngày càng

được phát triển và hiệu chỉnh bổ xung tính năng để đảm bảo yêu cầu ngày càng cao của hệ thống (hiện nay dns được tiêu chuẩn theo chuẩn RFC 1034 - 1035)

1.2.Mục đích của hệ thống DNS

Máy tính khi kết nối vào mạng Internet thì được gán cho một địa chỉ IP xác định. Địa chỉ IP của mỗi máy là duy nhất và có thể giúp máy tính có thể xác định đường đi đến một máy tính khác một cách dễ dàng. Như đối với người dùng thì địa chỉ IP là rất khó nhớ. Do vậy cần phải sử dụng một hệ thống để giúp cho máy tính tính toán đường đi một cách dễ dàng và đồng thời cũng giúp người dùng dễ nhớ. Do vậy hệ thống DNS ra đời nhằm giúp cho người dùng có thể chuyển đổi từ địa chỉ IP khó nhớ mà máy tính sử dụng sang một tên dễ nhớ cho người sử dụng và đồng thời nó giúp cho hệ thống Internet dễ dàng sử dụng để liên lạc và ngày càng phát triển.

Hệ thống DNS sử dụng hệ thống cơ sở dữ liệu phân tán và phân cấp hình cây do đó việc quản lý sẽ dễ dàng và cũng rất thuận tiện cho việc chuyển đổi từ tên miền sang địa chỉ IP và ngược lại. Cũng giống như mô hình quản lý cá nhân của một đất nước mỗi cá nhân sẽ có một tên xác định đồng thời cũng có địa chỉ chứng minh thư để giúp quản lý con người một cách dễ dàng hơn (nhưng khác là tên miền không được trùng nhau còn tên người thì vẫn có thể trùng nhau)

Mỗi cá nhấn đều có một số căn cước để quản lý

Mỗi một địa chỉ IP tương ứng với một tên miền

Vậy tóm lại tên miền là (domain name) gì ? những tên gợi nhớ như home.vnn.vn hoặc www.cnn.com thì được gọi là tên miền (domain name hoặc dns name). Nó giúp cho người sử dụng dễ dàng nhớ vì nó ở dạng chữ mà người bình thường có thể hiểu và sử dụng hàng ngày.

Hệ thống DNS đã giúp cho mạng Internt thân thiện hơn với người sử dụng do đó mạng internet phát triển bùng nổ một vài năm lại đây. Theo thống trên thế giới vào thời điểm tháng 7/2000 số lượng tên miền được đăng ký là 93.000.000

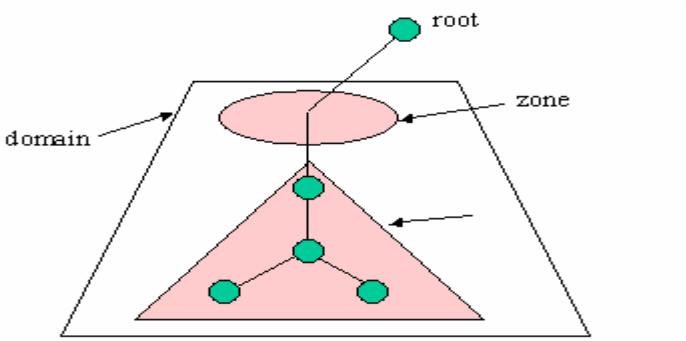
Tóm lại mục đích của hệ thống DNS là:

- Địa chỉ IP khó nhớ cho người sử dụng nhưng dễ dàng với máy tính
- Tên thì dễ nhớ với người sử dụng như không dùng được với máy tính
- Hệ thống DNS giúp chuyển đổi từ tên miền sang địa chỉ IP và ngược lại giúp người dùng dễ dàng sử dụng hệ thống máy tính

II. DNS server và cấu trúc cơ sở dữ liệu tên miền

II.1.Cấu trúc cơ sở dữ liệu

Cơ sở dữ liệu của hệ thống DNS là hệ thống cơ sở dữ liệu phân tán và phân cấp hình cây. Với .Root server là đỉnh của cây và sau đó các domain được phân nhánh dần xuống dưới và phần quyền quản lý. Khi một client truy vấn một tên miền nó sẽ lần lượt đi từ root phân cấp lần lượt xuống dưới để đến dns quản lý domain cần truy vấn.



Cấu trúc của dữ liệu được phân cấp hình cây root quản lý toàn bộ sơ đồ và phân quyền quản lý xuống dưới và tiếp đó các tên miền lại được tiếp tục chuyên xuống cấp thấp hơn (delegate) xuống dưới.

Zone

Hệ thống dns cho phép phân chia tên miền để quản lý và nó chia hệ thống tên miền ra thành zone và trong zone quản lý tên miền tên miền được phân chia đó và nó chứa thông tin về domain cấp thấp hơn và có khả năng chia thành các zone cấp thấp hơn và phân quyền cho các dns server khác quản lý.

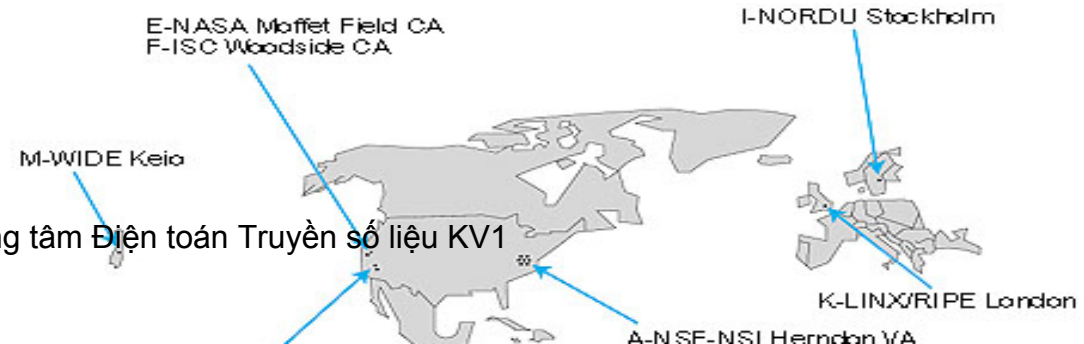
Ví dụ: zone *".com"* thì dns server quản lý zone *".com"* chưa thông tin về các bản ghi có đuôi là *".com"* và có khả năng chuyển quyền quản lý (delegate) các zone cấp thấp hơn cho các dns khác quản lý như *".microsoft.com"* là vùng (zone) do microsoft quản lý.

Root Server

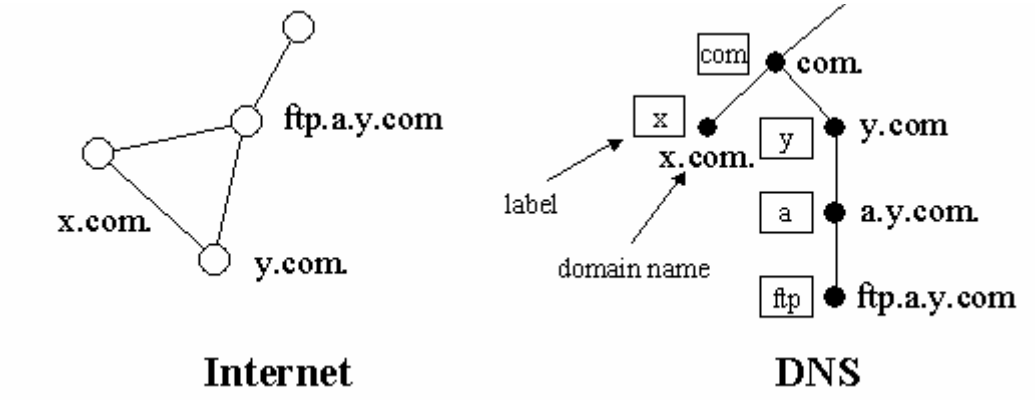
✓ Là server quản lý toàn bộ cấu trúc của hệ thống dns

✓ Root server không chứa dữ liệu thông tin về cấu trúc hệ thống DNS mà nó chỉ chuyển quyền (delegate) quản lý xuống cho các server cấp thấp hơn và do đó root server có khả năng xác định đường đến của một domain tại bất cứu đâu trên mạng

✓ Hiện nay trên thế giới có khoảng 13 root server quản lý toàn bộ hệ thống Internet (vị trí của root server như trên hình vẽ dưới)



Hệ thống cơ sở dữ liệu của dns là hệ thống dữ liệu phân tán hình cây như cấu trúc đó là cấu trúc logic trên mạng Internet



Về mặt vật lý hệ thống DNS nằm trên mạng Internet không có có cấu trúc hình cây nhưng nó được cấu hình phân cấp logic phân cấp hình cây phân quyền quản lý.

Một DNS server có thể nằm bất cứ vị trí nào trên mạng Internet nhưng được cấu hình logic để phân cấp chuyển tên miền cấp thấp hơn xuống cho các dns server khác nằm bất cứ vị trí nào trên mạng Internet (về nguyên tắc ta có thể đặt DNS tại bất cứ vị trí nào trên mạng Internet. Nhưng tốt nhất là đặt DNS tại vị trí nào gần với các client để dễ dàng truy vấn đến đồng thời cũng gần với vị trí của dns server cấp cao hơn trực tiếp của nó).

Mỗi một tên miền đều được quản lý bởi ít nhất một DNS server và trên đó ta khai các bản ghi của tên miền trên DNS server. Các bản ghi đó sẽ xác định địa chỉ IP của tên miền hoặc các dịch vụ xác định trên Internet như web, thư điệnt tử ...

Sau đây là các bản ghi trên dns

Tên trường	Tên đầy đủ	Mục đích
SOA	Start of Authority	Xác định máy chủ DNS có thẩm

		quyền cung cấp thông tin về tên miền xác định trên DNS
NS	Name Server	Chuyển quyền quản lý tên miền xuống một DNS cấp thấp hơn
A	Host	Ánh xạ xác định địa chỉ IP của một host
MX	Mail Exchanger	Xác định host có quyền quản lý thư điện tử cho một tên miền xác định
PTR	Pointer	Xác định chuyển từ địa chỉ IP sang tên miền
CNAME	Canonical NAME	Thường xử dụng xác định dịch vụ web hosting

Cấu trúc của một tên miền

- Domain sẽ có dạng : lable.lable.label...lable
- Độ dài tối đa của một tên miền là 255 ký tự
- Mỗi một Lable tối đa là 63 ký tự
- Lable phải bắt đầu bằng chữ hoặc số và chỉ được phép chứa chữ, số, dấu trừ(-), dấu chấm (.) mà không được chứa các ký tự khác.

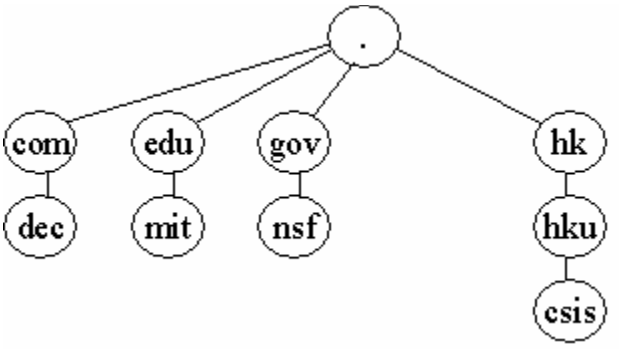
Phân loại tên miền

Hầu hết tên miền được chia thành các loại sau:

- *Arpa* : tên miền ngược (chuyển đổi từ địa chỉ IP sang tên miền reverse domain)
- *Com* : các tổ chức thương mại
- *Edu* : các cơ quan giáo dục
- *Gov* : các cơ quan chính phủ
- *Mil* : các tổ chức quân sự, quốc phòng

- *Net* : các trung tâm mạng lớn
- *Org* : các tổ chức khác
- *Int* : các tổ chức đa chính phủ (ít được sử dụng)

Ngoài ra hiện nay trên thế giới sử dụng loại tên miền có hai ký tự cuối để xác định tên miền thuộc quốc gia nào (được xác định trong chuẩn ISO3166)



Loại tên	Miêu tả	Ví dụ
Gốc (domain root)	Nó là đỉnh của nhánh cây của tên miền. Nó xác định kết thúc của domain (fully qualified domain names FQDNs).	Đơn giản nó chỉ là dấu chấm (.) sử dụng tại cuối của tên ví như "example.microsoft.com."
Tên miền cấp một (Top-level domain)	Là hai hoặc ba ký tự xác định nước/khu vực hoặc các tổ chức.	".com", xác định tên sử dụng trong xác định là tổ chức thương mại .
Tên miền cấp hai (Second-level domain)	Nó rất đa dạng trên internet, nó có thể là tên của một công ty, một tổ chức hay một cá nhân .v.v. đăng ký trên internet.	"microsoft.com.", là tên miền cấp hai đăng ký là công ty Microsoft.
Tên miền cấp nhỏ hơn	Chia nhỏ thêm ra của tên miên cấp hai xuống thường được sử dụng như chi	"example.microsoft.com." là phần quản lý tài liệu ví dụ của microsof

(Subdomain)	nhánh, phong ban của một cơ quan hay một chủ đề nào đó.

Một số chú ý khi đặt tên miền:

– Tên miền nên đặt giới hạn từ từ cấp 3 đến cấp 4 hoặc cấp 5 vì nếu nhiều hơn nữa việc quản trị là khó khăn.

– Sử dụng tên miền là phải duy nhất trong mạng internet

– Nên đặt tên đơn giản gợi nhớ và tránh đặt tên quá dài

II.2. Phân loại DNS server và đồng bộ dư liệu giữa các DNS server

Có ba loại DNS server sau:

- *Primary server*

Nguồn xác thực thông tin chính thức cho các domain mà nó được phép quản lý quản lý

Thông tin về tên miền do nó được phân cấp quản lý thì được lưu trữ tại đây và sau đó có thể được chuyển sang cho các secondary server.

Các tên miền do primary server quản lý thì được tạo và sửa đổi tại primary server và sau đó được cập nhập đến các secondary server.

- *Secondary server*

DNS được khuyến nghị nên sử dụng ít nhất là hai DNS server để lưu cho mỗi một zone. Primary DNS server quản lý các zone và secondary server được sử dụng để lưu trữ dự phòng cho zone cho primary server. Secondary DNS server được khuyến nghị dùng nhưng không nhất thiết phải có. Secondary server được phép quản lý domain nhưng dữ liệu về domain không phải tạo tại secondary server mà nó được lấy về từ primary server.

Secondary server có thể cung cấp hoạt động ở chế độ không có tải trên mạng. Khi lượng truy vấn zone tăng cao tại primary server nó sẽ chuyển bớt tải

sang secondary server hoặc khi primary server bị sự cố thì secondary sẽ hoạt động thay thế cho đến khi primary server hoạt động trở lại

Secondary server nên được sử dụng tại nới gần với client để có thể phục vụ cho việc truy vấn tên miền một cách dễ dàng. Nhưng không nên cài đặt secondary server trên cùng một subnet hoặc cùng một kết nối với primary server. Vì điều đó sẽ là một giải pháp tốt để sử dụng secondary server để dự phòng cho primary server vì có thể kết nối đến primary server bị hỏng thì cũng không ảnh hưởng gì đến secondary server.

Primary server luôn luôn duy trì một lượng lớn dữ liệu và thường xuyên thay đổi hoặc thêm vào các zone. Do đó DNS server sử dụng một cơ chế cho phép chuyển các thông tin từ primary server sang secondary server và lưu giữ nó trên đĩa. Các thông tin nhận dữ liệu về các zone có thể sử dụng giải pháp lấy toàn bộ (full) hoặc lấy phần thay đổi (incremental)

Nhiều secondary DNS server sẽ tăng độ ổn định hoạt động của mạng và việc lưu trữ thông tin của tên miền một cách đảm bảo như một điều cần quan tâm là dữ liệu của zone được chuyển trên mạng từ primary server đến các secondary server sẽ làm tăng lưu lượng đường truyền và yêu cầu thời gian để đồng bộ dữ liệu trên các secondary server.

- *Caching-only server*

Mặc dù tất cả các DNS server đều có khả năng lưu trữ dữ liệu trên bộ nhớ cache của máy để trả lời truy vấn một cách nhanh chóng. Caching-only server là loại DNS server chỉ sử dụng cho việc truy vấn, lưu giữ câu trả lời dữa trên thông tin trên cache của máy và cho kết quả truy vấn. Chúng không hề quản lý một domain nào và thông tin mà nó chỉ giới hạn những gì được lưu trên cache của server.

Khi nào thì sử dụng caching-only server ?. Khi mà server bắt đầu chạy thì nó không có thông tin lưu trong cache. Thông tin sẽ được cập nhập theo thời gian khi các client server truy vấn dịch vụ DNS. Nếu bạn sử dụng kết nối mạng WAN tốc độ thấp thì việc sử dụng caching-only DNS server là một giải pháp tốt nó cho phép giảm lưu lượng thông tin truy vấn trên đường truyền.

Chú ý

- Caching-only DNS server không chưa zone nào và cũng không quyền quản lý bất kỳ domain nào. Nó sử dụng bộ nhớ cache của mình để lưu các truy

vấn dns của client. Thông tin sẽ được lưu trong cache để trả lời cho các truy vấn đến của client

- Caching-only DNS có khả năng trả lời các truy vấn như không quản lý hoặc tạo bất cứ zone hoặc domain nào

- DNS server nói trung được khuyến nghị là được cấu hình sử dụng TCP/IP và dùng địa chỉ IP tĩnh.

Đồng bộ dữ liệu giữa các DNS server (zone transfer)

Truyền toàn bộ zone

Bởi vì tầm quan trọng của hệ thống DNS và việc quản lý các domain thuộc zone phải được đảm bảo. Do đó thường một zone thì thường được đặt trên hơn một DNS server để tránh lỗi khi truy vấn tên miền thuộc zone đó. Nói cách khác nếu chỉ có một server quản lý zone và khi server không trả lời truy vấn thì các tên miền trong zone đó sẽ không được trả lời và không còn tồn tại trên Internet. Do đó ta cần có nhiều DNS server cùng quản lý một zone và có cơ chế để chuyển dữ liệu của các zone và đồng bộ nó từ một DNS server này đến các DNS server khác

Khi một DNS server mới được thêm vào mạng thì nó được cấu hình như một secondary server mới cho một zone đã tồn tại. Nó sẽ tiến hành nhận toàn bộ (full) zone từ DNS server khác. Như DNS server thế hệ đầu tiên thường dùng giải pháp lấy toàn bộ cơ sở dữ liệu về zone khi có các thay đổi trong zone.

Truyền phần that đổi (Incremental zone)

Truyền chỉ những thay đổi (incremental zone transfer) của zone được miêu tả chi tiết trong tiêu chuẩn RFC 1995. Nó là phần bổ xung cho chuẩn sao chép dns zone. Incremental transfer thì đươc hỗ trợ bởi cả DNS server là nguồn lấy thông tin và DNS server nhận thông tin về zone, nó cung cấp giải pháp hiệu quả cho việc đồng bộ nhưng thay đổi hoặc thêm bớt zone.

Giải pháp ban đầu cho DNS yêu cầu cho việc thay đổi dữ liệu về zone là truyền toàn bộ dữ liệu của zone sử dụng truy vấn AXFR. Với việc chỉ truyền các thay đổi (incremental transfer) sẽ sử dụng truy vấn (IXFR) được sử dụng thay thế cho AXFR. Nó cho phép secondary server chỉ lấy về như zone thay đổi để đồng bộ dữ liệu.

Với trao đổi IXFR zone, thì sự khác nhau giữa versions của nguồn dữ liệu và bản sao của nó. Nếu cả hai bản đều có cùng version (xác định bởi số serial trong khai báo tại phần đầu của zone SOA "start of authority") thì việc truyền dữ liệu của zone sẽ không được thực hiện.

Nếu số serial cho dữ liệu nguồn lớn hơn số serial của secondary server thì nó sẽ thực hiện chuyển những thay đổi với các bản ghi nguồn (Resource record - RR) của zone. Để truy vấn IXFR thực hiện thành công và các thay đổi được gửi thì tại DNS server nguồn của zone phải lưu gữi các phần thay đổi để sử dụng truyền đến nơi yêu cầu của truy vấn IXFR. Incremental sẽ cho phép lưu lượng truyền dữ liệu là ít và thực hiện nhanh hơn.

```
@       IN      SOA     vdc-hn01.vnn.vn. postmaster.vnn.vn. (
        1999082802      ; serial number
        1800            ; refresh every 30 mins
        3600            ; retry every hour
        86400           ; expire after 24 hours
        6400            ; minimum TTL 2 hours
        )
        IN       NS       vdc-hn01.vnn.vn.
        IN       NS       hcm-server1.vnn.vn.
```

Zone transfer sẽ xẩy ra khi có nhưng hành động sau xẩy ra:

- Khi quá trình làm mới của zone kết thúc (refresh expire)
- Khi secondary server được thông báo zone đã thay đổi tại server nguồn quản lý zone
- Khi dịch vụ DNS bắt đầu chạy tại secondary server
- Tại secondary server yêu cầu chuyển zone

Sau đây là các bước yêu cầu từ secondary server đến DNS server chứa zone để yêu cầu lấy dữ liệu về zone mà nó quản lý.

1. Trong khi cấu hình mới DNS server. Thì nó sẽ gửi truy vấn yêu cầu gửi toàn bộ zone ("all zone" transfer (AXFR) request) đến DNS server quản lý chính dữ liệu của zone

2. DNS server chính quản lý dữ liệu của zone sẽ trả lời và truyền toàn bộ dữ liệu về zone đến secondary (destination) server mới cấu hình.

zone thì được chuyển đến DNS server yêu cầu căn cứ vào version được xác định bằng số Serial tại phần khai báo (start of authority SOA). Tại phần SOA cũng có chứa các thông số xác định thời gian làm mới lại zone ...

3. Khi thời gian làm mới (refresh interval) của zone hết, thì DNS server nhận dữ liệu sẽ truy vấn yêu cầu làm mới zone tới DNS server chính chưa dữ liệu zone.

4. DNS server chính quản lý dữ liệu sẽ trả lời truy vấn và gửi lại dữ liệu.

Trả lời sẽ bao gồm cả số serial của zone hiện tại tại dns server chính.

5. DNS server nhận dữ liệu về zone sẽ kiểm tra số serial trong trả lời và quyết định sẽ làm thế nào với zone

Nếu giá trị của số serial bằng với số hiện tại tại DNS server nhận trả lời thì nó sẽ kết luận rằng sẽ không cần chuyển dữ liệu về zone đến. Và nó sẽ thiết lập lại với các thông số cũ và thời gian để làm mới lại bắt đầu.

Nếu giá trị của số serial tại dns server chính lớn hơn giá trị hiện tại tại dữ liệu dns nới nhận thì nó kết luận rằng zone cần phải được cập nhập và việc chuyển zone là cần thiết.

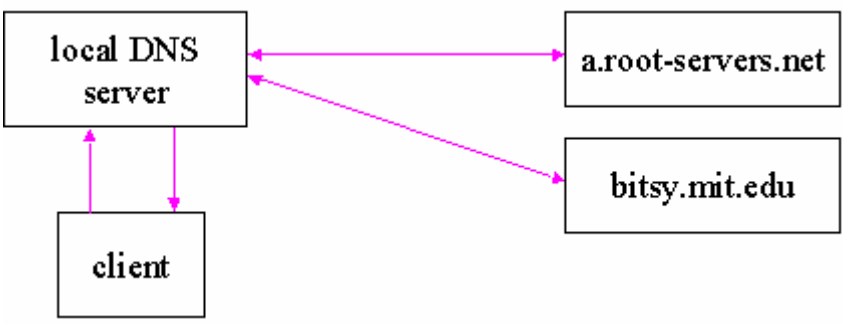
6. Nếu DNS server nơi nhận kết luận rằng zone cần phải thay đổi và nó sẽ gửi truy vấn IXFR tới DNS server chính để yêu cầu gửi zone

7. DNS server chính sẽ trả lời với việc gửi những thay đổi của zone hoặc toàn bộ zone

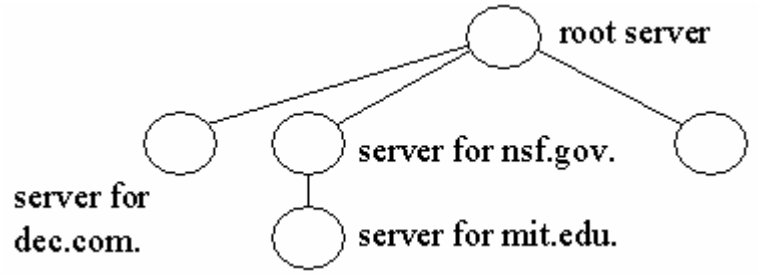
Nếu DNS server chính có hỗ trợ việc gửi những thay đổi của zone thì nó sẽ gửi những phần thay đổi (incremental zone transfer (IXFR) of the zone.). Nếu nó không hỗ trợ thì nó sẽ gửi toàn bộ zone (full AXFR transfer of the zone)

III. Hoạt động của hệ thống DNS

Hệ thống DNS hoạt động động tại lớp 4 của mô hình OSI nó sử dụng truy vấn bằng giao thức UDP và mặc định là sử dụng cổng 53 để trao đổi thông tin về tên miền.



Hoạt động của hệ thống DNS là chuyển đổi tên miền sang địa chủ IP và ngược lại. Hệ thống cơ sở dữ liệu của DNS là hệ thống cơ sở dữ liệu phân tán, các dns server được phân quyền quản lý các tên miền xác định và chúng liên kết với nhau để cho phép người dùng có thể truy vấn một tên miền bất kỳ (có tồn tại) tại bất cứ điểm nào trên mạng một các nhanh nhất



Như đã trình bầy các dns server phải biết ít nhất một cách để đến được root server và ngược lại. Như trên hình vẽ muốn xác định được tên miền mit.edu thì root server phải biết dns server nào được phân quyền quản lý tên miền mit.edu để chuyển truy vấn đến.

Nói tóm lại tất cả các dns server đều được kết nối một cách logic với nhau:

- Tất cả các dns server đều được cấu hình để biết ít nhất một cách đến root server
- Một máy tính kết nối vào mạng phải biết làm thế nào để liên lạc với ít nhất là một DNS server

Hoạt động của DNS

Khi DNS client cần xác định cho một tên miền nó sẽ truy vấn DNS.

Truy vấn dns và trả lời của hệ thống dns cho client sử dụng thủ tục UDP cổng 53, UPD hoạt động ở mức thứ 3 (network) của mô hình OSI, UDP là thủ tục phi kết nối (connectionless), tương tự như dịch vụ gửi thư bình thường bạn cho thư vào thùng thư và hy vọng có thể chuyển đến nơi bạn cần gửi tới.

Mỗi một message truy vấn được gửi đi từ client bao gồm ba phần thông tin :

- Tên của miền cần truy vấn (tên đầy đủ FQDN)
- Xác định loại bản ghi là mail, web ...
- Lớp tên miền (phần này thường được xác định là IN internet, ở đây không đi sâu vào phần này)

Ví dụ : tên miền truy vấn đầy đủ như "hostname.example.microsoft.com.", và loại truy vấn là địa chỉ A. Client truy vấn DNS hỏi "Có bản ghi địa chỉ A cho máy tính có tên là "hostname.example.microsoft.com" khi client nhận được câu trả lời của DNS server nó sẽ xác định địa chỉ IP của bản ghi A.

Có một số giải pháp để trả lời các truy vấn DNS. Client có thể tự trả lời bằng cách sử dụng các thông tin đã được lưu trữ trong bộ nhớ cache của nó từ những truy vấn trước đó. DNS server có thể sử dụng các thông tin được lưu trữ trong cache của nó để trả lời hoặc dns server có thể hỏi một dns server khác lấy thông tin đó để trả lời lại client.

Nói chung các bước của một truy vấn gồm có hai phần như sau:

- Truy vấn sẽ bắt đầu ngay tại client computer để xác định câu trả lời
- Khi ngay tại client không có câu trả lời, câu hỏi sẽ được chuyển đến DNS server để tìm câu trả lời.

Tự tìm câu trả lời truy vấn

Bước đầu tiên của quá trình sử lý một truy vấn. Tên miền sử dụng một chương trình trên ngay máy tính truy vấn để tìm câu trả lời cho truy vấn. Nếu truy vấn có câu trả lời thì quá trình truy vấn kết thúc

Ngay tại máy tính truy vấn thông tin được lấy từ hai nguồn sau:

- Trong file HOSTS được cấu hình ngay tại máy tính. Các thông tin ánh xạ từ tên miền sang địa chỉ được thiết lập ở file này được sử dụng đầu tiên. Nó được tải ngay lên bộ nhớ cache của máy khi bắt đầu chạy dns client.
- Thông tin được lấy từ các câu trả lời của truy vấn trước đó. Theo thời gian các câu trả lời truy vấn được lưu giữ trong bộ nhớ cache của máy tính và nó được sử dụng khi có một truy vấn lặp lại một tên miền trước đó.

Truy vấn DNS server

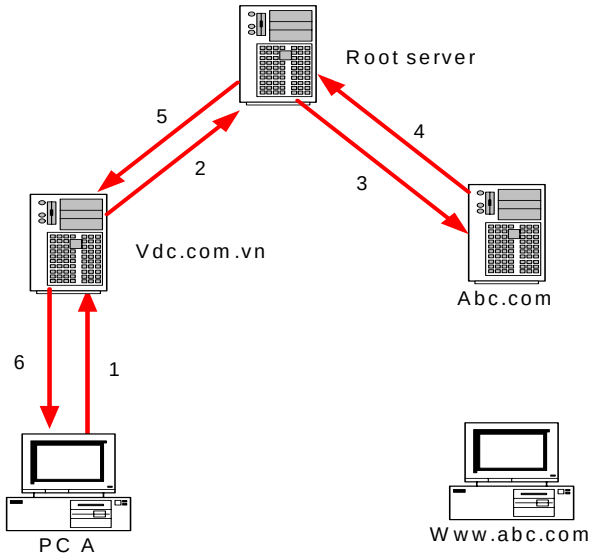
Khi DNS server nhận được một truy vấn. Đầu tiên nó sẽ kiểm tra câu trả lời liệu có phải là thông tin của bản ghi mà nó quản lý trong các zone của server. Nếu truy vấn phù hợp với bản ghi mà nó quản lý thì nó sẽ sử dụng thông tin đó để trả lời trả lời (authoritatively answer) và kết thúc truy vấn.

Nếu không có thông tin về zone của nó phù hợp với truy vấn. Nó sẽ kiểm tra các thông tin được lưu trong cache liệu có các truy vấn tương tư nào trước đó phù hợp không nếu có thông tin phù hợp nó sẽ sử dụng thông tin đó để trả lời và kết thúc truy vấn.

Nếu truy vấn không tìm thấy thông tin phù hợp để trả lời từ cả cache và zone mà dns server quản lý thì truy vấn sẽ tiếp tục. Nó sẽ nhờ DNS server khác để trả lời truy vấn đến khi tìm được câu trả lời.

Các cách để dns server liên lạc với nhau xác định câu trả lời

Trường hợp Root server kết nối trực tiếp với server tên miền cần truy vấn



Trong trường hợp root server biết được dns server quản lý tên miền cần truy vấn. Thì các bước của truy vấn sẽ như sau:

Bước 1 : PC A truy vấn DNS server tên miền vdc.com.vn. (là local name server) tên miền www.abc.com.

Bước 2 : DNS server tên miền vdc.com.vn không quản lý tên miền www.abc.com do vậy nó sẽ chuyển truy vấn lên root server.

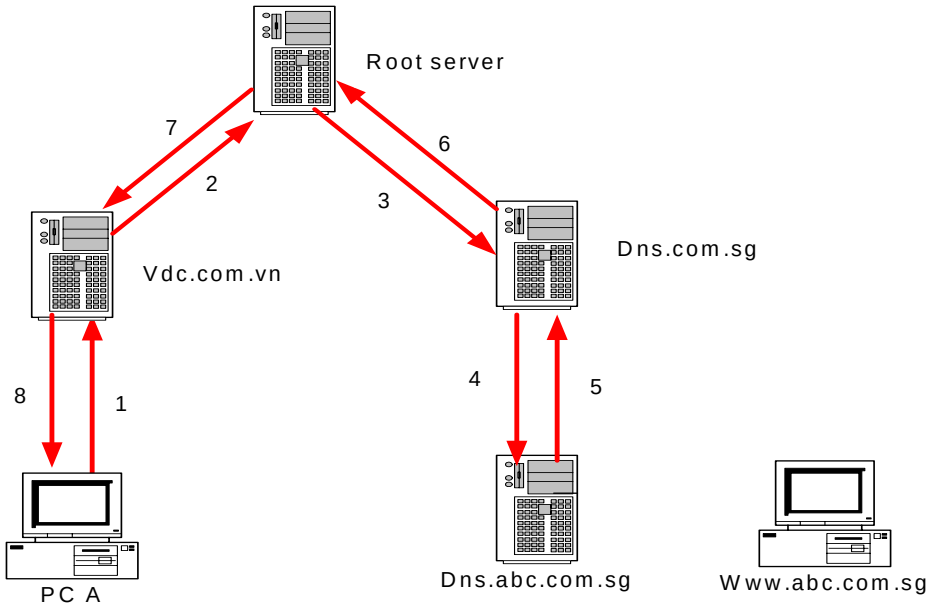
Bước 3 : Root server sẽ xác định được rằng dns server quản lý tên miền www.abc.com là server dns.abc.com và nó sẽ chuyển truy vấn đến dns server dns.abc.com để trả lời

Bước 4 : DNS server dns.abc.com sẽ xác định bản ghi www.abc.com và trả lời lại root server

Bước 5 : Root server sẽ chuyển câu trả lời lại cho server vdc.com.vn

Bước 6 : DNS server vdc.com.vn sẽ chuyển câu trả lời về cho PC A và từ đó PC A có thể kết nối đến PC B (quản lý www.abc.com)

Trường hợp root server không kết nối trực tiếp với server tên miền cần truy vấn



Trong trường hợp không kết nối trực tiếp thì root server sẽ hỏi server trung gian (phân lớp theo hình cây) để xác định được đến server tên miền quản lý tên miền cần truy vấn

Bước 1 - PC A truy vấn DNS server vdc.com.vn (local name server) tên miền www.acb.com.sg.

Bước 2 - DNS server vdc.com.vn không quản lý tên miền www.abc.com.sg vậy nó sẽ chuyển lên root server.

Bước 3 - Root server sẽ không xác định được dns server quản lý trực tiếp tên miền www.abc.com.sg nó sẽ căn cứ vào cấu trúc của hệ thống tên miền để chuyển đến dns quản lý cấp cao hơn của tên miền abc.com.sg đó là com.sg và nó xác định được rằng dns server dns.com.sg quản lý tên miền com.sg.

Bước 4 - dns.com.sg sau đó sẽ xác định được rằng dns server dns.abc.com.sg có quyền quản lý tên miền www.abc.com.sg.

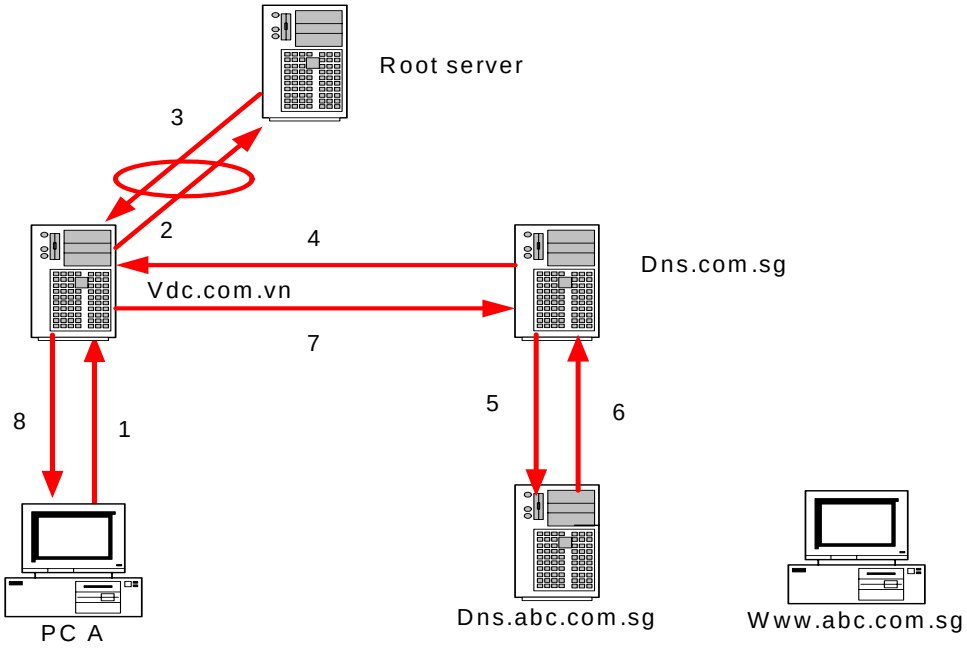
Bước 5 - dns.abc.com.sg sẽ lấy bản ghi xác định cho tên miền www.abc.com.sg để trả lời dns server dns.com.sg.

Bước 6 - dns.com.sg sẽ lại chuyển câu trả lời lên root server.

Bước 7 - Root server sẽ chuyển câu trả lời trở lại dns server vdc.com.vn.

Bước 8 - Và dns server vdc.com.vn sẽ trả lời về PC A câu trả lời và PC A đã kết nối được đến host quản lý tên miền www.abc.com.sg.

Khi các truy vấn lặp đi lặp lại thì hệ thống dns có khả năng thiết lập chuyển quyền trả lời đến dns trung gian mà không cần phải qua root server và nó cho phép thời gian truy vấn được giảm đi.



Hoạt động của DNS cache

Khi DNS server sử lý các truy vấn của client và sử dụng các truy vấn lặp lại. Nó sẽ xác định và lưu lại các thông tin quan trọng của tên miền mà client truy vấn. Thông tin đó sẽ được ghi lại trong bộ nhớ cache của dns server.

Cache lưu giữ thông tin là giải pháp hữu hiệu tăng tốc độ truy vấn thông tin cho các truy vấn thường xuyên của các tên miền hay được sử dụng và làm giảm lưu lượng thông tin truy vấn trên mạng.

DNS server khi thực hiện các truy vấn đệ quy cho client thì dns server sẽ tạm thời lưu trong cache bản ghi thông tin (resource record - RR) lấy được từ dns server lưu trữ thông tin về truy vấn đó. Sau đó một client khác truy vấn yêu cầu thông tin của đúng bản ghi đó thì nó sẽ lấy thông tin ban ghi (RR) lưu trong cache để trả lời.

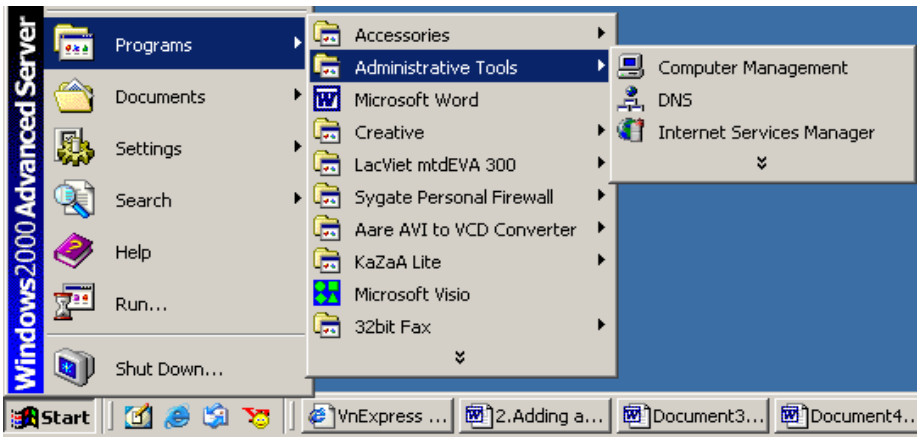
Khi thông tin được lưu trong cache. Thì các bản ghi RR được ghi trong cache sẽ được cung cấp thời gian sống (TTL - Time-To-Live). Thời gian sống của một bản ghi trong cache là thời gian mà nó tồn tại trong cache và được dùng để trả lời cho các truy vấn của client khi truy vấn tên miền trong bản ghi đó. Thời gian sống (TTL) được khai khi cấu hình cho các zone. Giá trị mặc định nhỏ nhất của thời gian sống (Minimum TTL) là 3600 giây (1 giờ) như giá

trị này ta có thể thay đổi khi cấu hình zone. Hết thời gian sống bản ghi sẽ được xóa khỏi bộ nhớ cache.

IV.Cài đặt DNS Server cho Window 2000

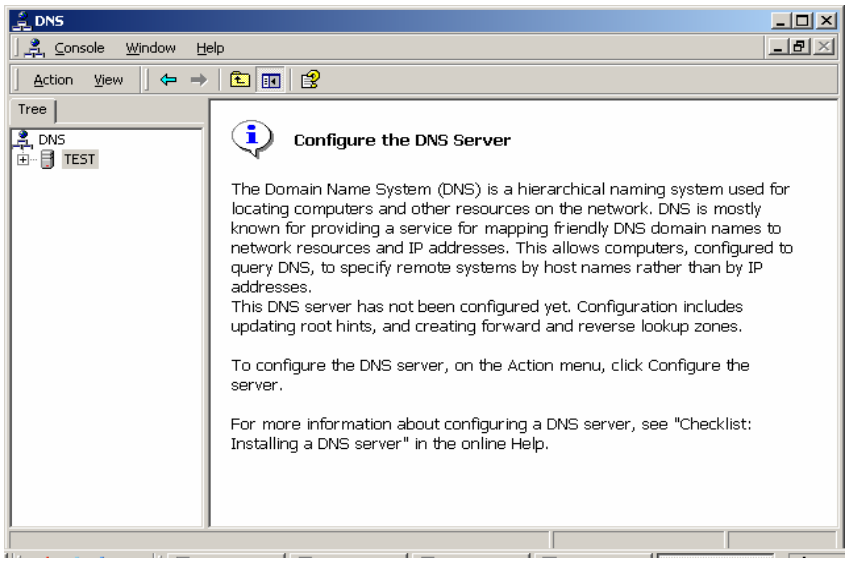
IV.1. Mở cửa sổ quản lý DNS

Bước 1: Mở của sổ quản lý DNS



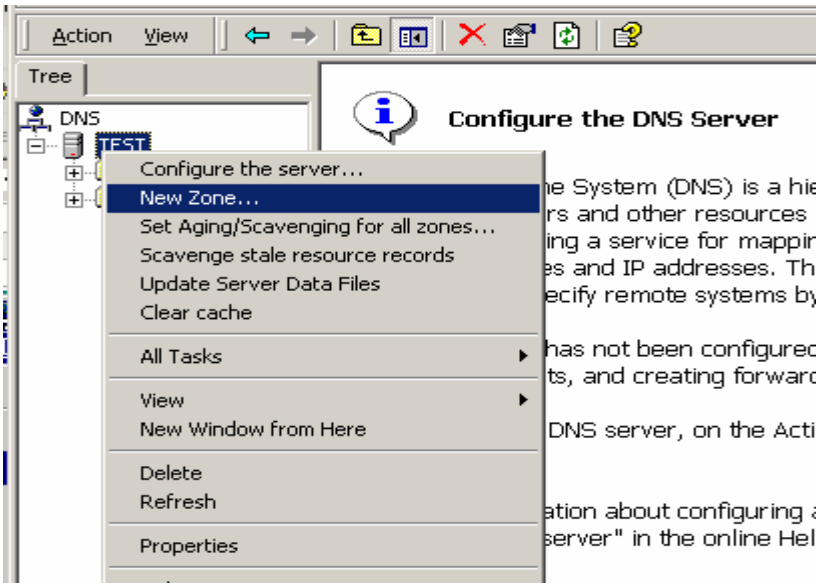
Bấm vào mune *Start* chọn *Programs* và sau đó là *"Administrative tools"* Chọn *"DNS Manager"*

Bước 2: Cửa sổ quản lý DNS server sẽ xuất hiện

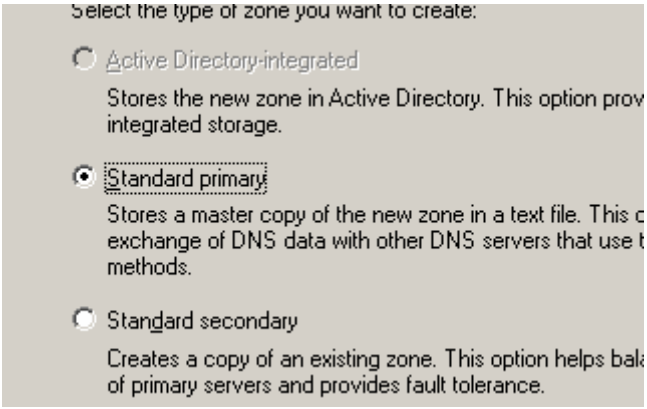


Tại cửa sổ quản lý DNS server bạn có thể khai báo các tính năng của DNS

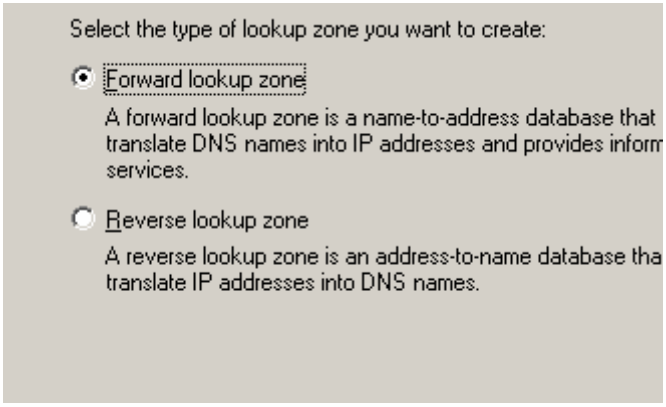
IV.2 Thêm trường (zone)



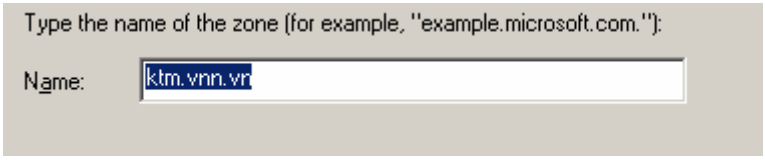
zone là tên miền (domain name) mà server quản lý. Tại cửa sổ quản lý DNS tại phần server quản lý bấm chuột phải để hiện menu và chọn *"new zone*" như hình trên



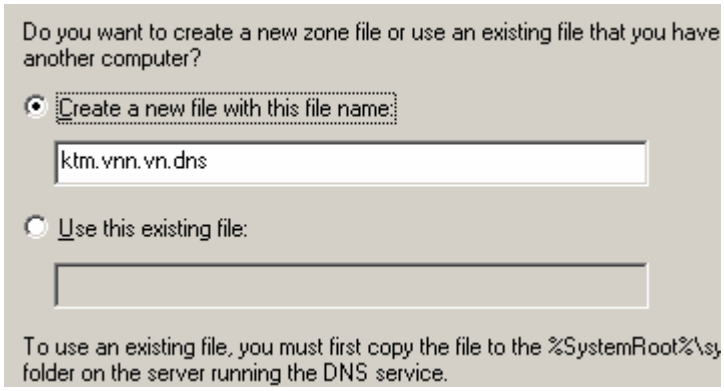
Bấm và *"new zone"* sẽ hiện cửa sổ cho phép chọn kiểu dữ liệu mà zone quản lý. *Standard Primary* là loại dữ liệu của zone được khai báo và quản lý ngay tại server. Còn *Stardard Secondary* là loại zone mà dữ liệu được lấy về từ *Standard Primary* và dữ liệu cũng nằm trên server . *Standard Primary* thường sử dụng để dự phòng cho các zone đã tồn tại. Bấm *Next* để tiếp tục



Sẽ xuất cửa sổ như trên. *Forward lookup zone* là loại zone quản lý việc chuyển đổi từ domain name sang địa chỉ IP. Còn phần *Reverse lookup zone* quản lý việc chuyển đổi từ IP sang Domain name. Bấm *Next* tiếp tục



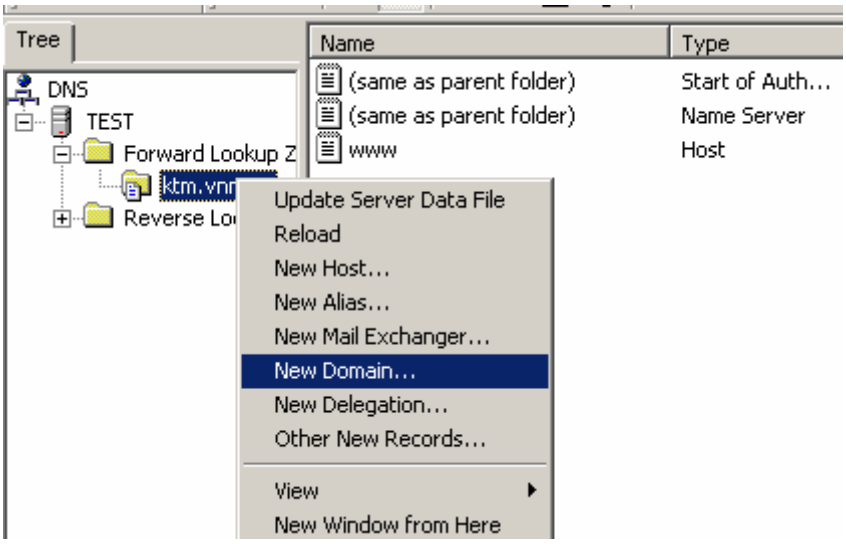
Tại cửa sổ này điền zone (domain name) mà sẽ quản lý. Bấm Next tiếp tục



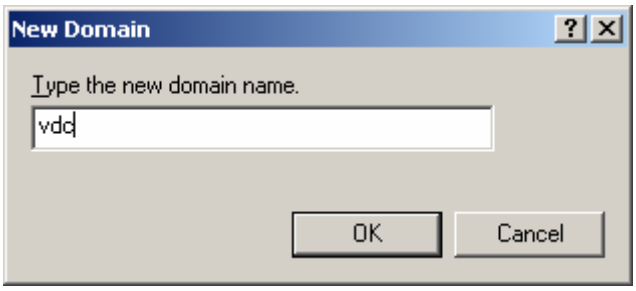
Điền tên của file để lưu trữ zone tại *"Create a new file with this file name"* hoặc sử dụng file có sẵn tại *"Use this existing file"* Và bấm *Next* cho đến khi xuất hiện nút *finish* để kết thúc tạo zone

IV.3.Thêm tên miên (domain name)

Tại của sổ quản lý domain chọn vào server và bấm chuột phải hiện lên menu và chọn *"New Domain..."* để điền một domain mới .

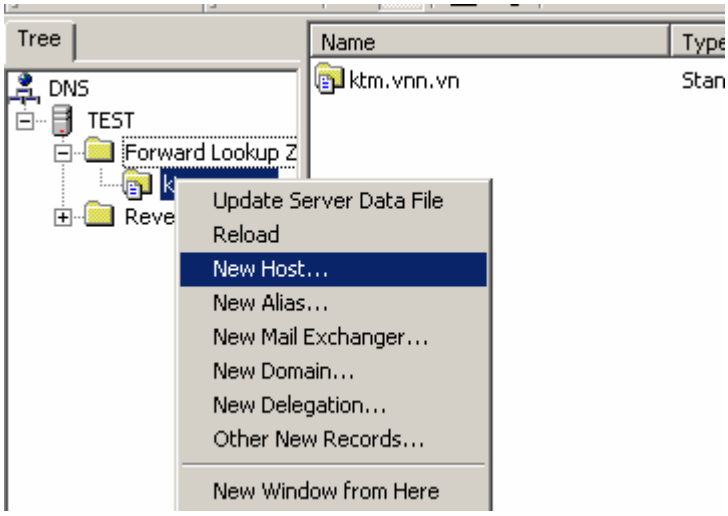


Sau khi bấm vào *"New Domain"* nó sẽ xuất hiện cửa sổ cho phép bạn điền tên miền mà server được phép quản lý. Sau khi điền bấm *"OK"* để kết thúc

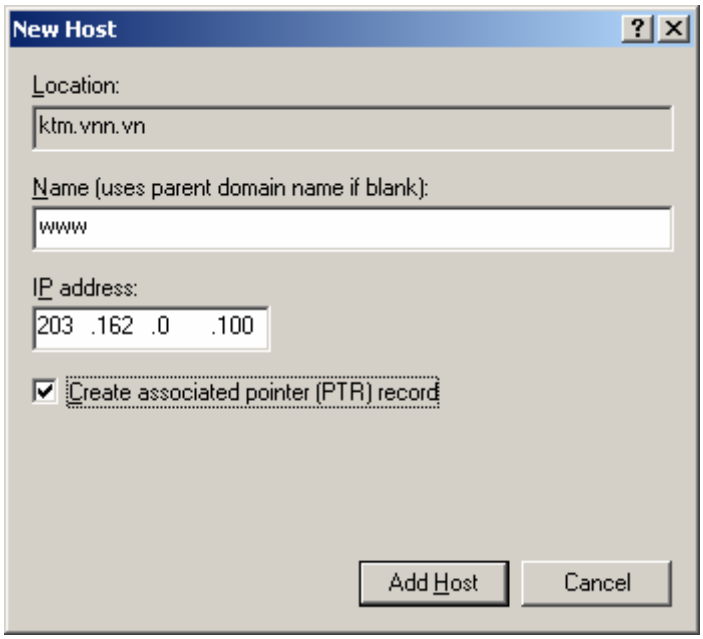


IV.4 Thêm một host mới

Tại cửa sổ quản lý DNS chọn zone đã tạo và bấm chuột phải chọn *"new host"*



Xuất hiện cửa sổ cho phép ta khai báo host mới



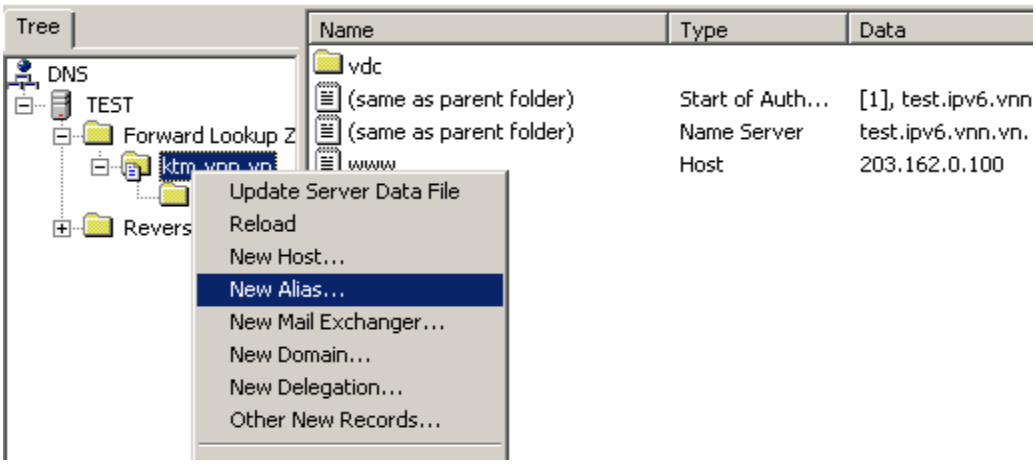
Bạn điền tên của host mà muốn tạo. Tên của host sẽ được tự động điền thêm phần domain để thành tên đầy đủ của host.

Ví dụ: như trên đây là vùng quản lý zone (*location*) là ktm.vnn.vn. Vậy khi bạn điền *Name* là www và *IP address* là 203.162.0.100 thì sẽ tương ứng với định nghĩa domain www.ktm.vnn.vn. trỏ đến địa chỉ IP 203.162.0.100

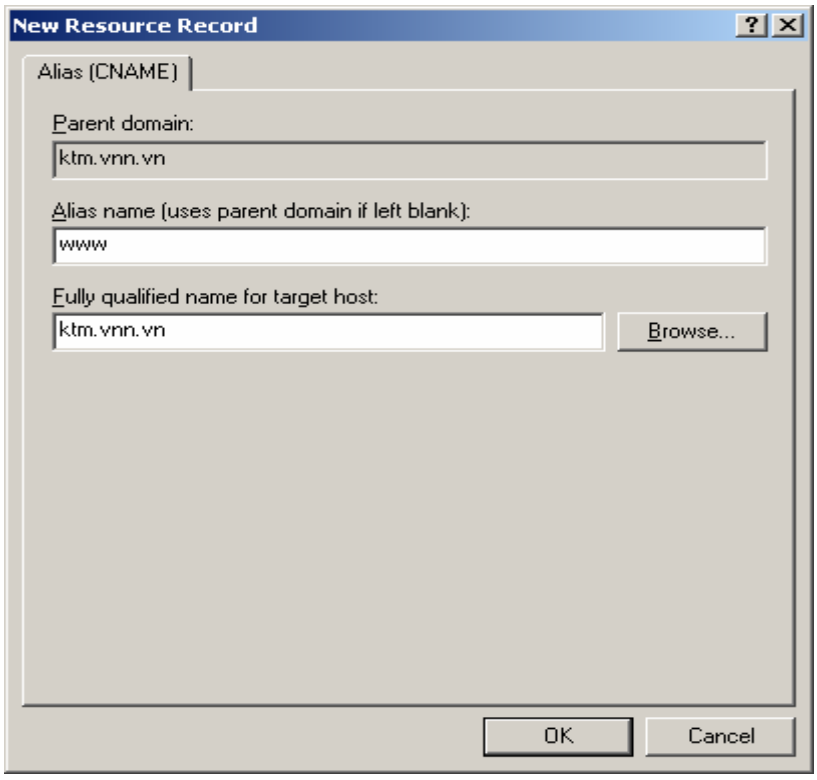
www.ktm.vnn.vn. IN A 203.162.0.100

IV.5 Tạo một bản ghi web (tạo bí danh)

Tại cửa sổ quản lý Domain và tên miền vừa tạo và bấm chuột phải và chọn *"New Alias"* để tạo một CNAME đến một host.



Bấm và *"New Alias..."* sẽ xuất hiện cửa sổ cho phép khai báo Alias



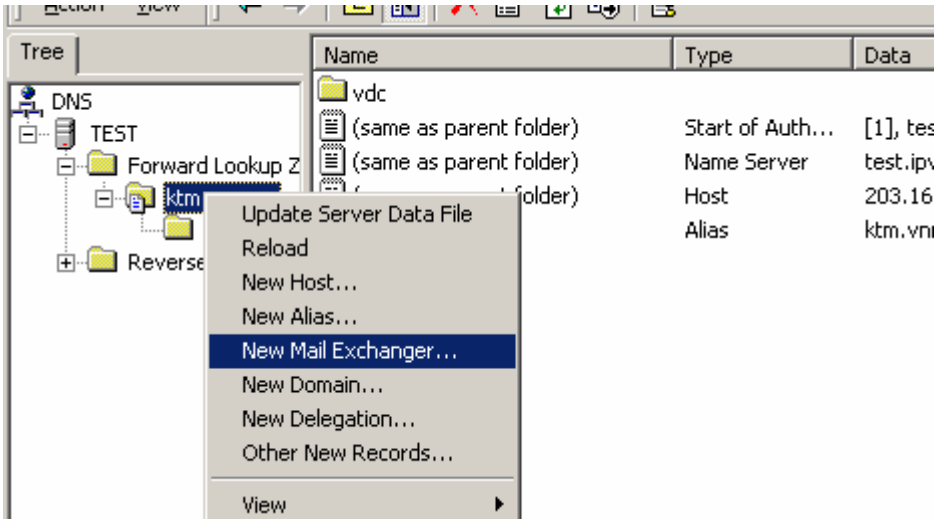
Tại phần *"Alias name"* điền tên tạo alias và tại phần *"Fully qualified name for target host"* điền tên đầy đủ của một host mà muốn tạo bí danh (thường được sử dụng cho webhosting)

Ví dụ : www.ktm.vnn.vn. IN CNAME ktm.vnn.vn.

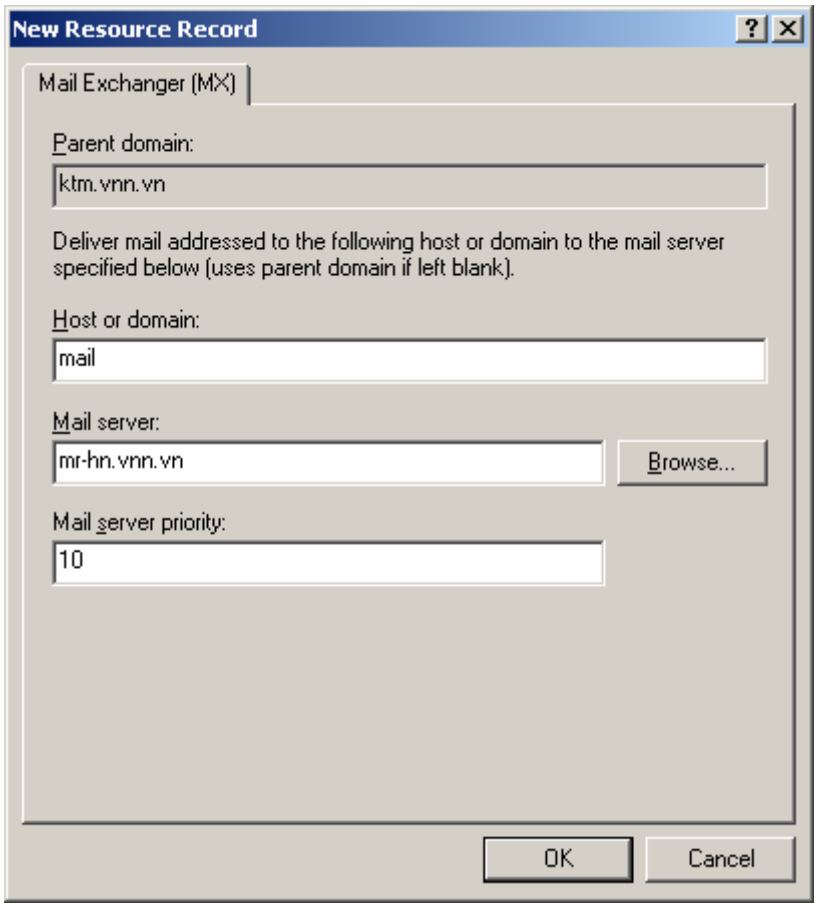
Ta sẽ có trang web www.ktm.vnn.vn đặt trên server web có tên là ktm.vnn.vn.

IV. 6 Tạo một bản ghi thư điện tử (MX)

Tại cửa sổ quản lý DNS tại tên miền muốn tạo bản ghi MX bấm chuột phải



Sau khi bấm vào *"New Mail Exchanger.."* sẽ xuất hiện cửa sổ cho phép tạo các thông số cho bản ghi mx



Điền tại *"Host or domain"* điền tên hoặc để trống tên này kết hợp với phần zone "*Parent domain"* để tạo thành domain đầy đủ của bản ghi thư điện tử. Tại *"Mail server"* điền tên của server thư điện tử và tại *"Mail server priority"* điền mức độ ưu tiên của server thư điện tử (độ lớn càng nhỏ mức ưu tiên càng cao)

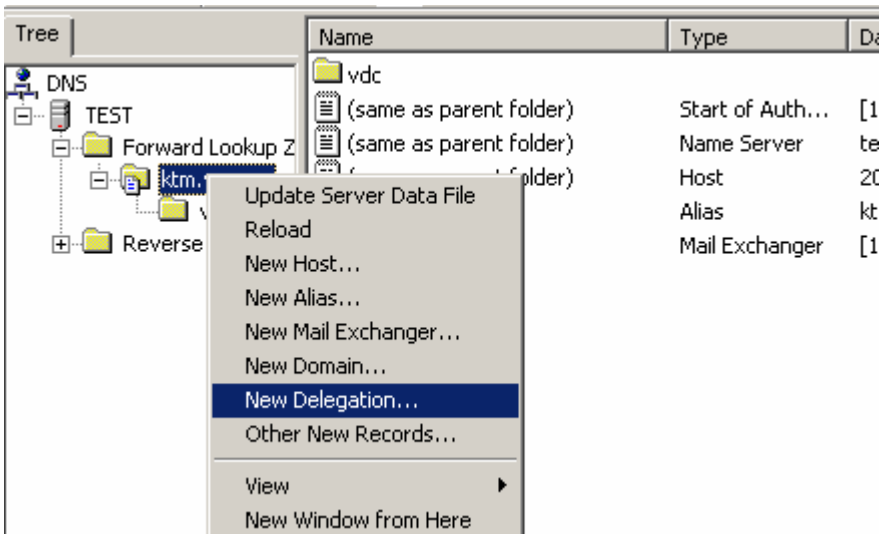
Ví dụ trên hình ta có:

mail.ktm.vnn.vn IN MX 10 mr-hn.vnn.vn.

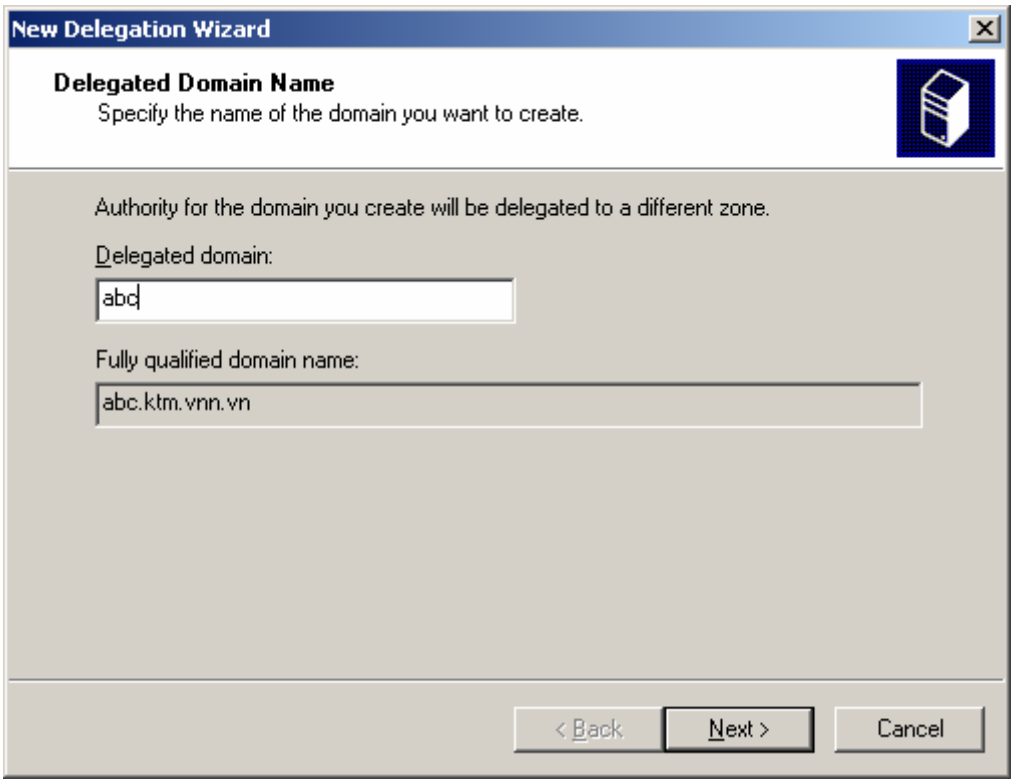
Ta có tên miền thư điện tử mail.ktm.vnn.vn. (ta có thể tạo được các hộp thư abc@mail.ktm.vnn.vn) được chứa tại server thư điện tử mr-hn.vnn.vn với mức ưu tiên là 10

IV. 7 Chuyển quyền quản lý têm miền (delegate)

Tại cửa sổ quản lý DNS tại domain muốn chuyển quyền quản lý bấm chuột phải.

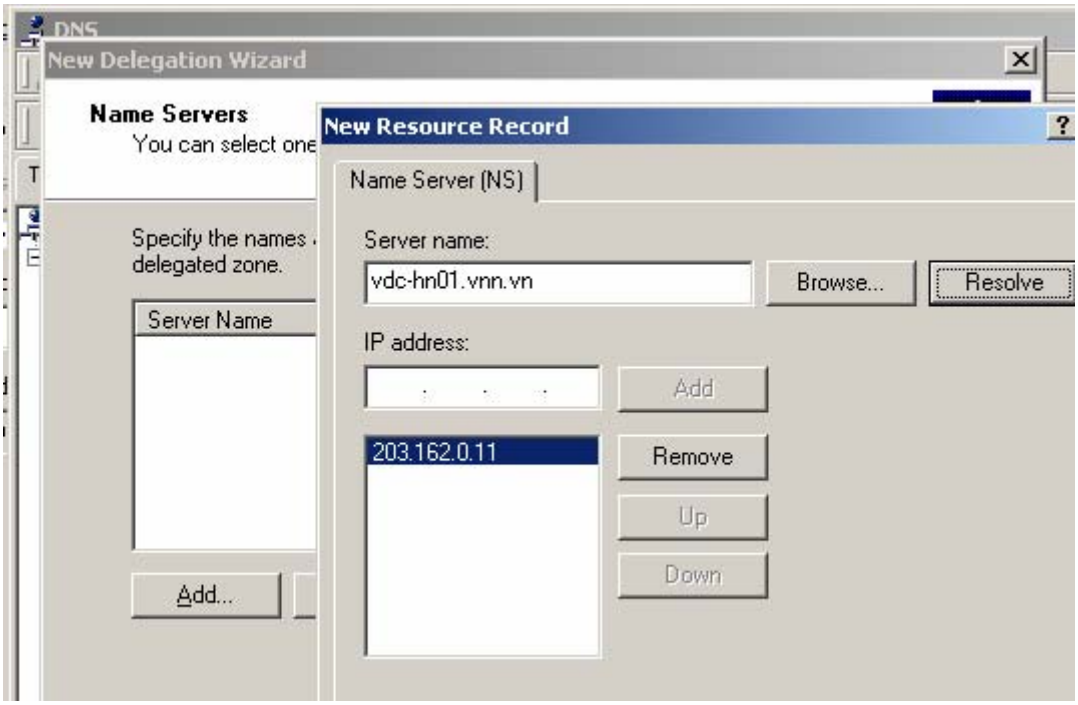


Bấm vào *"New Delegation..."* để hiện cửa sổ cho phép chuyển quyền quản lý tên miền



Điền phần domain mà bạn muốn chuyển quyền quản lý vào *"Delegated domain"*

Ví dụ ở đây điền là abc nghĩa là bạn muốn chuyển quyền quản lý domain abc.ktm.vnn.vn. Bấm *"Next"* để tiếp tục



Hiện cửa sổ điền vào *"Server name"* tên của dns server sẽ được phép quản lý tên miền abc.ktm.vnn.vn. Bấm *"Resolve"* để xác định địa chỉ IP của dns server. Sau đó bấm *"Ok"* để kết thúc.

Ví dụ abc.ktm.vnn.vn. IN NS vdc-hn01.vnn.vn.

Tương ứng tên miền abc.ktm.vnn.vn. sẽ được chuyển quyền về dns server vdc-hn01.vnn.vn để quản lý.

V. Cài đặt, cấu hình dns cho Linux

Hiện tại trên Internet rất nhiều nhà cung cấp phần mềm miễn phí cho DNS. Nhưng phần mền sử dụng dns cho unix được sử dụng phổ biến hiện này là gói phần mềm cho dns là Bind

Bind được phát triển bởi một tổ chức phi lợi nhuận là Internet Software Consortium (www.isc.org) và nó cung cấp phần mền bind miễn phí.

Hiện tại phần mềm bind có version là 9.2.2

Phần mền Bind còn cung cấp tiện ích nslookup là công cụ rất tiện lợi cho việc kiểm tra tên miền

Khai báo DNS cho client/server

Với client sử dụng linux hoặc unix ta vào file /etc/resolv.conf

- ✓ Client chỉ lấy thông tin về các domain
- ✓ Client chỉ gửi query tới server và nhận trả lời

Cấu hình dns server

- ✓ Cấu bình resolver như của (dns client)
- ✓ Cấu hình Bind cho name server (named)
- ✓ Xây dự cơ sở dữ liệu cho dns (cho các zone file)

Cấu hình cho dns client /etc/resolv.conf

Các từ khóa	Miêu tả
nameserver *địa chỉ*	Địa chỉ IP của dns server sẽ gửi truy vấn đến để lấy thông tin về domain

domain *name*	xác định domain mặc định của client

/etc/resolv.conf

```
# Domain name resolver configuration file
#
domain nuts.com
# try yourself first
nameserver 172.16.12.2
# try almond next
nameserver 172.16.12.1
# finally try filbert
nameserver 172.16.1.2
```

Với dns client chỉ cần cấu hình file resolv.conf

Cài đặt dns server.

Ta có thể lấy chương trình cài đặt bind cho dns tại www.isc.org lấy về server

cd /usr/src

mkdir bind-9.xx

cd bind-9.xx

Lấy chương trình cài đặt dns về đây bind-9.xx-src.tar.gz

gunzip bind-9.xx-src.tar.gz

tar xf bind-9.xx-src.tar

rm bind-9.xx-src.tar

cd src

make clean

make depend

make install

Vậy là ta đã cài xong phần mền named cho dns và các zone file sẽ được chứa trong /var/named còn file cấu hình nằm trong /usr/local/etc vậy ta phải tạo và đặt file cấu hình và zone file vào các thư mục trên và chạy

#/usr/local/sbin/named

Vậy là server đã sẵn sàng cho truy vấn dns

Cấu trúc file cơ sở dữ liệu (zone file)

Các file cơ sở dữ liệu zone được chỉ làm hai loại cho domain (có dạng db.domain hoặc domain.root) và các domain ngược (db.address) và nó nằm trong thư mục /var/named của dns server.

Các dữ liệu nằm trong file cơ dữ liệu được gọi là DNS resource record. Các loại resource record trong file dữ liệu bao gồm:

SOA record

Chỉ rõ domain ở cột quản lý bởi name server ghi sau trường SOA. Trong trường hợp file db.domain

```
@       IN      SOA     vdc-hn01.vnn.vn. postmaster.vnn.vn. (
        1999082802      ; serial number
        1800            ; refresh every 30 mins
        3600            ; retry every hour
        86400           ; expire after 24 hours
        6400            ; minimum TTL 2 hours
        )
        IN      NS      vdc-hn01.vnn.vn.
                IN      NS      hcm-server1.vnn.vn.
```

Khai báo zone ngược db.203.162.0

```
@       IN      SOA     vdc-hn01.vnn.vn. postmaster.vnn.vn. (
                1999082301   ; Serial
    10800       ; Refresh after 3 hours
    3600        ; Retry after 1 hour
    604800      ; Expire after 1 week
```

```
        86400 )     ; Minimum TTL of 1 day
;name servers
        IN      NS      vdc-hn01.vnn.vn.
        IN      NS      hcm-server1.vnn.vn.
6       IN      PTR             ldap.vnn.vn.
7       IN      PTR             hanoi-server1.vnn.vn.
8       IN      PTR             hanoi-server2.vnn.vn.
9       IN      PTR             mail.vnn.vn.
```

Trong mỗi zone chỉ khai một trường SOA. Như ví dụ trên trong trường hợp file db.com.vn, chữ @ biể thị các tất cả các domain trong file quản lý bởi name server vdc-hn01.vnn.vn và địa chỉ mail của admin mạng là postmaster.vnn.vn. Ngoài ra trong phần SOA có 5 thông số cần quản tâm sau:

Serial number : Thông số này có tác dụng với tất cả các dữ liệu trong file. Khi secondary server yêu cầu primary server các thông tin về domain mà nó quản lý thì đầu tiên nó sẽ so sánh serial number của secondary và primary server. Nếu serial number của secondary server nhỏ hơn của primary server thì dữ liệu của domain sẽ được cập nhập lại cho secondary server từ secondary server.

Mỗi khi ta thay đổi nội dung của file db.domain thì ta cần phải thay đổi serial number và thường ta đánh serial number theo nguyên tắc sau:

Serial number : yyyymmddtt

trong đó : yyyy là năm

mm là tháng

dd là ngày

tt là số lần sử đổi trong ngày

Refresh : là chu kỳ thời gian mà secondary server sẽ sánh và cập nhập lại dữ liệu của nó với primary server

Retry: nếu secondary server không kết nối được với primary server thì cứ sau một khoảng thời gian thì nó sẽ kết nối lại

Expire : là khoảng thời gian mà domain sẽ hết hiệu lực nếu secondary không kết nối được với primary server.

TTL (time to live) : khi một server bất kỳ yêu cầu thông tin về dữ liệu nào đó từ primary server, và dữ liệu đó sẽ được lưu giữ tại server đó và có hiệu lực trong khoảng thời gian của TTL. Hết khoảng thời gian đó nếu tiếp tục cần thì nó lại phải truy vấn lại primary server.

Các bản ghi thường dùng trong DNS server

NS (name server) : Còn bản ghi NS để xác định dns server nào sẽ quản lý tên miền. Như ví dụ ở trên là dns server vdc-hn01.vnn.vn. và hcm-server1.vnn.vn.

A (address) : Bản ghi dạng A cho tương ứng một domain name với một địa chỉ IP. Chỉ cho phép khai báo một bản ghi A cho một địa chỉ IP.

Ví dụ:

Tên miền	Internet	Loại bản ghi	Địa chỉ
mr.vnn.vn.	IN	A	203.162.4.148
mr-hn.vnn.vn.	IN	A	203.162.0.24
mail.vnn.vn.	IN	A	203.162.0.9
fmail.vnn.vn.	IN	A	203.162.4.147
hot.vnn.vn.	IN	A	203.162.0.23
home.vnn.vn.	IN	A	203.162.0.12
www.vnn.vn.	IN	A	203.162.0.16

CNAME (canonical name) : là tên phụ cho một host có sẵn tên miền dạng A. Nó thường được sử dụng cho các server web, ftp

Ví dụ : các domain có dạng CNAME được chỉ tới các máy chủ web

Tên miền	Internet	Loại bản ghi	Server
www.gpc.com.vn.	IN	CNAME	home.vnn.vn.
www.huonghai.com.vn.	IN	CNAME	home.vnn.vn.

www.songmayip.com.vn.	IN	CNAME	hot.vnn.vn.
www.covato2.com.vn.	IN	CNAME	hot.vnn.vn.

MX (mail exchange): là tên phụ cho các dịch vụ mail trên các máy chủ đã có tên miền dạng A. Bản ghi này cho phép máy chủ có thể cung cấp dịch vụ mail cho các domain khác nhau. Có thể khai báo nhiều domain khác nhau cùng chỉ tới một server hoặc một domain trỏ tới nhiều server khác nhau (sử dụng backup) trong trường hợp này giá trị ưu tiên phải đặt khác nhau. Với số ưu tiên càng nhỏ thì mức độ ưu tiên càng cao.

Ví dụ

Tên miền	*Internet*	**Loại bản ghi**	**mức ưu tiên**	**Server**
mrvn.vnn.vn.	IN	MX	10	mr.vnn.vn.
clipsalvn.vnn.vn.	IN	MX	10	mr-hn.vnn.vn.
dbqnam.vnn.vn.	IN	MX	10	mr-hn.vnn.vn.
thangloi.vnn.vn.	IN	MX	50	mail.netnam.vn.
	IN	MX	100	fallback.netnam.vn.

PTR (Pointer) : là bản ghi tương ứng địa chỉ IP với domain. Các file dạng db.address. Ví dụ db.203.162.0 cho tương ứng với các địa chỉ IP tương ứng với mạng 203.162.0.xxx

Chú ý :

Trước mỗi phần khai báo domain thường có dòng

$ORIGIN *domain.*

Để khai báo giá trị mặc định của domain. Cho phép trong phần khai báo giá trị không phải khai báo lặp lại phần domain mặc định.

Ví dụ :

vdc.com.vn. IN A 203.162.0.49

hoặc

```
$ORIGIN com.vn.
vdc             IN      A       203.162.0.49
```

Dấu "**;**" được sử dụng làm ký hiệu dòng chú thích, các phần sau dấu ";" đều không có tác dụng.

Định nghĩa cấu hình (name.conf)

Khi các file cơ sở dữ liệu (zone file) thì cần phải cấu hình để dns server đọc các zone file đó. Đối với hệ thống BIND cơ chế chỉ dẫn name server đọc các zone file được khai trong file named.conf nó được nằm trong thư mục /etc hoặc /usr/local/etc

Ví dụ : khai báo file db trong file named.conf:

```
        ; khai báo cho zone file domain.vn
zone "vn." in {
        type master;
        file "db.vn";
};
        ;khai báo cho zone file domain.gov.vn
zone "gov.vn." in {
        type master;
        file "db.gov.vn";
};
        ;khai báo cho zone ngược 203.162.0.xxx
zone "0.162.203.in-addr.arpa" in {
        type master;
        file "db.203.162.0";
};
        ;khai báo cho zone ngược 203.162.1.xxx
 zone "1.162.203.in-addr.arpa" in {
```

```
        type master;
        file "db.203.162.1";
};
```

Chú ý: sau mỗi lần thay đổi dữ liệu để sửa đổi có tác dụng thì cần phải làm động tác để dns server cập nhập thay đổi

```
%su
%password:
# ps -ef | grep named
   root 17413     1  5   Sep 07 ?       189:52 /usr/local/sbin/named
# kill -HUP 17413
```

Còn để chạy dns server

```
#/usr/local/sbin/named
```

Hướng dẫn sử dụng nslookup

nslookup - là công cụ trên internet cho phép truy vấn tên miền và địa chỉ IP một cách tương tác.

Cấu trúc câu lệnh

nslookup [-option ...] [host-to-find | - [server]]

Miêu tả các lệnh của nslookup

server domain & lserver domain Change the default server to domain. Lserver uses the initial server to look up information about domain while server uses the current default server. If an authoritative answer can't be found, the names of servers that might have the answer are returned.

root Thay đổi server mặc định sẽ làm root cho domain truy vấn.

ls [option] domain [>> filename]

Hiện danh sách thông tin của domain. Mặc định là hiện tên của host và địa chỉ IP. Ta có thể sử dụng các lựa chọn để hiện nhiều thông tin hơn:

-t querytype hiện danh sách tất cả bản ghi xác định bởi loại querytype

-a hiện danh sách các bí danh (aliaes) của domain host (tương tự như -t CNAME)

-d hiện danh sách các bản ghi của domain (tương tự như -t ANY)

-h hiện danh sách thông tin về CPU và thông tin về hệ điều hành của domain. (tương tự như -t HINFO)

? hiện danh sách các câu lệnh.

exit thoát khỏi chương trình.

set keyword[=value] câu lệnh dùng để thay đổi trạng thái thông tin mà có ảnh hưởng đến truy vấn. Các từ khoá:

all cho phép hiện tất cả các loại bản ghi

[no]debug bật chế độ tìm lỗi. Cho hiện rất nhiều loại thông tin cho phép xác định lỗi truy vấn đến domain. (mặc định=nodebug, viết tắt = [no]deb)

[no]d2 Bật chế độ tìm lỗi mức cao hơn. Tất cả các gói tin truy vấn đều được xuất hiện. (mặc định=nod2)

domain=name Thay đổi domain mặc định vào tên. Khi truy vấn một tên nó sẽ tự động điền thêm domain vào sau.

port=value Chuyển cổng mặc định sử dụng cho TCP/UDP name server thành cổng được thiết lập bởi giá trị này (mặc định= 53, viết tắt = po)

querytype=value

type=value Chọn loại truy vấn thông tin. Có các loại sau:

A truy vấn host (khai báo địa chỉ IP).

CNAME (canonical name) tạo tên bí danh (thường dùng cho web)

HINFO truy vấn loại CPU và hệ điều hành của server.

MINFO thông tin vê hộp thư hoặc mail list.

MX truy vấn về mail exchanger.

NS truy vấn về named zone.

PTR truy vấn chuyển từ địa chỉ IP sang domain.

SOA Thông tin về người quản lý về zone.

TXT Các thông tin khác.

UINFO Thông tin về người dùng.

WKS Hỗ trợ cho các dịch vụ khác.

Các loại khác (**ANY**, **AXFR**, **MB**, **MD**, **MF**, **NULL**) được miêu tả chi tiết trong tiêu chuẩn **RFC-1035** . (Mặc định = A, viết tắt = q, ty)

[no]recurse Yêu cầu name server truy vấn tới một server khác nếu nó không có thông tin về domain cần tìm. (mặc định = recurse, viết tắt = [no]rec)

retry=number Thiết lập số lần truy vấn. Khi truy vấn mà không nhận được trả lời trong khoảng thời gian nhất định (thiết lập bằng lệnh set timeout). Khi thời gian hết thì yêu cầu truy vấn sẽ được gửi lại. Và thiết lập ở đây để điều khiển số lần sẽ gửi lại trước khi từ bỏ truy vấn. (Mặc định = 4, viết tắt = ret)

root=host Đổi root server cho host

timeout=number Thiết lập thời gian timeout cho một quá trìn truy vấn tính bằng giây. (mặc định = 5 giây, viết tắt = ti)

[no]vc sử dụng một virtual circuit để gửi yêu cầu truy vấn đến server. (mặc định là = novc, viết tắt = [no]v)

Phân tích lỗi

Nếu truy vấn lookup không thành công thì một thông tin về lỗi sẽ được hiện ra. Và các lỗi có thể là :

Timed out

Server không trả lời truy vấn sau một khoảng thời gian (khoảng thời gian có thể thay đổi bằng câu lệnh *set timeout=value*) và and a certain number of retries (changed with set retry=value).

No response from server

Không có name server đang chạy tại server mà client chỉ đến.

No records

Server không có bản ghi tương ứng loại mà truy vấn cho host đa tồn tại. Loại truy vấn được thiết lập bằng câu lệnh "*set querytype"* .

Non-existent domain

Host hoặc domain name không tồn tại.

Connection refused

Network is unreachable

Kết nối tới name server hoặc finger server không thể được tại thời điển này. Lệnh này thường xuất hiện với các yêu cầu của câu lện ls và finger.

Server failure

Name server tìm thấy lỗi trong dữ liệu về domain và không thể đưa ra câu trả lời đúng.

Refused

Name server từ chối yêu cầu trả lời.

Format error

Name server thấy rằng các gói tin yêu cầu không đúng định dạng. Nó có thể là lỗi của chương trình nslookup.

Ví dụ :

Truy vấn dns sử dụng bản ghi a cho domain home.vnn.vn có địa chỉ IP là 203.162.0.12	Default Server: vdc-hn01.vnn.vn Address: 203.162.0.11 Aliases: 11.0.162.203.in-addr.arpa > set querytype=a > home.vnn.vn Server: vdc-hn01.vnn.vn Address: 203.162.0.11 Aliases: 11.0.162.203.in-addr.arpa Name: home.vnn.vn Address: 203.162.0.12 >
Truy vấn bản nghi mx (mail) cho domain hn.vnn.vn nó trỏ đến các host mu13.vnn.vn có địa chỉ 203.162.0.55 và	> set querytype=mx > hn.vnn.vn Server: vdc-hn01.vnn.vn Address: 203.162.0.11 Aliases: 11.0.162.203.in-addr.arpa

mu14.vnn.vn có địa chỉ 203.162.0.64	hn.vnn.vn MX preference = 20, mail exchanger = mu13.vnn.vn hn.vnn.vn MX preference = 10, mail exchanger = mu14.vnn.vn vnn.vn nameserver = vdc-hn01.vnn.vn vnn.vn nameserver = hcm-server1.vnn.vn mu13.vnn.vn internet address = 203.162.0.55 mu14.vnn.vn internet address = 203.162.0.64 vdc-hn01.vnn.vn internet address = 203.162.0.11 hcm-server1.vnn.vn internet address = 203.162.4.1 >
Truy vấn loại ns (name server) cho domain vn do các server nào quản lý sẽ cho ta một danh sách các nameserver quản ly các domain có đuôi vn	> set querytype=ns > vn Server: vdc-hn01.vnn.vn Address: 203.162.0.11 Aliases: 11.0.162.203.in-addr.arpa Non-authoritative answer: vn nameserver = dns-hcm01.vnnic.net.vn vn nameserver = ns.ripe.net vn nameserver = dns1.vn vn nameserver = ns1.gip.net vn nameserver = ns2.gip.net vn nameserver = ns3.rip.net vn nameserver = dns1.vnnic.net.vn vn nameserver = cheops.anu.edu.au dns-hcm01.vnnic.net.vn internet address = 203.162.87.66 ns.ripe.net AAAA IPv6 address = 2001:610:240:0:53:0:0:193 ns.ripe.net internet address = 193.0.0.193 dns1.vn internet address = 203.162.3.235

```
ns1.gip.net     internet address = 204.59.144.222
ns2.gip.net     internet address = 204.59.1.222
dns1.vnnic.net.vn       internet address = 203.162.57.105
cheops.anu.edu.au       internet address = 150.203.224.24
>
```

Chương 5 : Dịch vụ truy cập từ xa và Dịch vụ Proxy

Chương 5 cung cấp các kiến thức cơ bản của hai nội dung dịch vụ phổ biến trên mạng máy tính: dịch vụ truy cập từ xa và dịch vụ proxy.

Việc truy cập từ xa là nhu cầu thiết yếu mở rộng phạm vi hoạt động mạng của các tổ chức, công ty. Nội dung truy cập từ xa giới thiệu trong chương này là truy cập qua mạng thoại PSTN. Đây là hình thức truy cập từ xa cho tốc độ truy cập thấp vừa phải nhưng lại có tính phổ biến rộng rãi và dễ thiết lập nhất.

Dịch vụ proxy trên mạng được phát triển cho các mục đích tăng cường tốc độ truy nhập cho khách hàng trong mạng, tiết kiệm được tài nguyên mạng (địa chỉ IP) và đảm bảo được an toàn cho mạng lưới khi bắt buộc phải cung cấp truy nhập ra mạng ngoài hay ra mạng Internet. Thiết lập dịch vụ proxy là công tác mọi quản trị hệ thống mạng cần biết vì các nhu cầu kết nối liên mạng và kết nối Internet càng ngày càng trở nên không thể thiếu cho bất kỳ tổ chức, công ty nào.

Chương 5 yêu cầu các học viên nên trang bị các kiến thức cơ bản về mạng điện thoại PSTN, kiến thức về các giao thức mạng WAN PPP, SLIP... các giao thức xác thực như RADIUS...Trong phần proxy, học viên cần làm quen với khái niệm chuyển đổi địa chỉ NAT, hoạt động của các giao thức TCP/IP.

Mục 1 : Dịch vụ truy cập từ xa (Remote Access)

I. Các khái niệm và các giao thức.

I.1. Tổng quan về dịch vụ truy cập từ xa.

Dịch vụ truy nhập từ xa (Remote Access Service) cho phép người dùng từ xa có thể truy cập từ một máy tính qua một môi trường mạng truyền dẫn (ví dụ mạng điện thoại công cộng) đến một mạng dùng riêng như thể máy tính đó

được kết nối trực tiếp trong mạng đó. Người dùng từ xa kết nối tới mạng đó thông qua một máy chủ dịch vụ gọi là máy chủ truy cập (Access server). Khi đó người dùng từ xa có thể sử dụng tài nguyên trên trên mạng như là một máy tính kết nối trực tiếp trong mạng đó. Dịch vụ truy nhập từ xa cũng cung cấp khả năng tạo lập một kết nối WAN thông qua các mạng phương tiện truyền dẫn giá thành thấp như mạng thoại công cộng. Dịch vụ truy cập từ xa cũng là cầu nối để một máy tính hay một mạng máy tính thông qua nó được nối đến Internet theo cách được coi là hợp lý với chi phí không cao, phù hợp với các doanh nghiệp, tổ chức qui mô vừa và nhỏ. Khi lựa chọn và thiết kế giải pháp truy cập từ xa, chúng ta cần thiết phải quan tâm đến các yêu cầu sau:

– Số lượng kết nối tối đa có thể để phục vụ người dùng từ xa.

– Các nguồn tài nguyên mà người dùng từ xa muốn muốn truy cập.

– Công nghệ, phương thức và thông lượng kết nối. Ví dụ, các kết nối có thể sử dụng modem thông qua mạng điện thoại công cộng PSTN, mạng số hoá tích hợp các dịch vụ ISDN...

– Các phương thức an toàn cho truy cập từ xa, phương thức xác thực người dùng, phương thức mã hoá dữ liệu

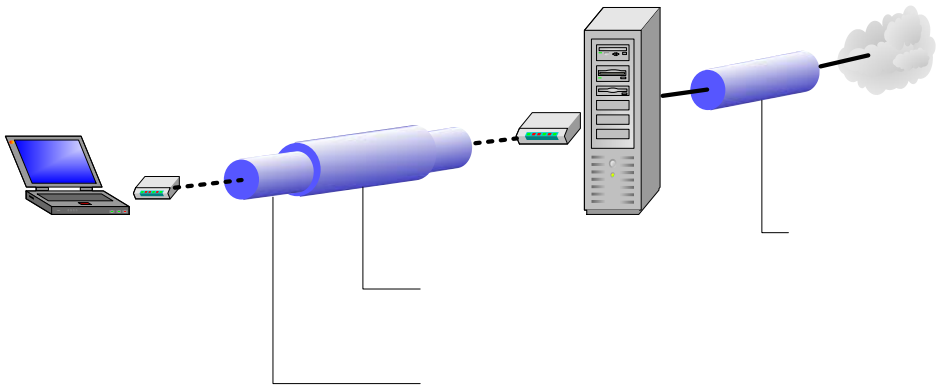
– Các giao thức mạng sử dụng để kết nối.

I.2. Kết nối truy cập từ xa và các giao thức sử dụng trong truy cập từ xa

1.Kết nối truy cập từ xa

Tiến trình truy cập từ xa được mô tả như sau: người dùng từ xa khởi tạo một kết nối tới máy chủ truy cập. Kết nối này được tạo lập bằng việc sử dụng một giao thức truy cập từ xa (ví dụ giao thức PPP- Point to Point Protocol). Máy chủ truy cập xác thực người dùng và chấp nhận kết nối cho tới khi kết thúc bởi người dùng hoặc người quản trị hệ thống. Máy chủ truy cập đóng vai trò như một gateway bằng việc trao đổi dữ liệu giữa người dùng từ xa và mạng nội bộ. Bằng việc sử dụng kết nối này, người dùng từ xa gửi và nhận dữ liệu từ máy chủ truy cập. Dữ liệu được truyền trong các khuôn dạng được định nghĩa bởi các giao thức mạng (ví dụ giao thức TCP/IP) và sau đó được đóng gói bởi

các giao thức truy cập từ xa. Tất cả các dịch vụ và các nguồn tài nguyên trong mạng người dùng từ xa đều có thể sử dụng thông qua kết nối truy cập từ xa này (hình 5.1)



Hình 5.1

2. Giao thức truy cập từ xa

SLIP (Serial Line Interface Protocol), PPP và Microsoft RAS là các giao thức truy cập để tạo lập kết nối được sử dụng trong truy cập từ xa. SLIP là giao thức truy cập kết nối điểm-điểm và chỉ hỗ trợ sử dụng với giao thức IP, hiện nay hầu như không còn được sử dụng. Microsoft RAS là giao thức riêng của Microsoft hỗ trợ sử dụng cùng với các giao thức NetBIOS, NetBEUI và được sử dụng trong các phiên bản cũ của Microsoft.

PPP giao thức truy cập kết nối điểm-điểm với khá nhiều tính năng ưu việt, là một giao thức chuẩn được hầu hết các nhà cung cấp hỗ trợ. RFC 1661 định nghĩa về PPP. Chức năng cơ bản của PPP là đóng gói thông tin giao thức lớp mạng thông qua các liên kết điểm – điểm.

Cơ chế làm việc và vận hành của PPP như sau: Để thiết lập truyền thông, mỗi đầu cuối của liên kết PPP phải gửi các gói LCP (Link Control Protocol) để thiết lập và kiểm tra liên kết dữ liệu. Sau khi liên kết được thiết lập với các tính năng tùy chọn được sắp đặt và thỏa thuận giữa hai đầu liên kết, PPP gửi các gói NCP (Network Control Protocol) để lựa chọn và cấu hình một hoặc nhiều giao thức lớp mạng. Mỗi lần một giao thức lớp mạng lựa chọn đã được cấu hình, lưu lượng từ mỗi giao thức lớp mạng có thể gửi qua liên kết

này. Liên kết tồn tại cho đến khi các gói LCP hoặc NCP đóng kết nối hoặc đến khi một sự kiện bên ngoài xẩy ra (chẳng hạn như một sự kiện hẹn giờ hay một sự can thiệp của người quản trị). Nói cách khác PPP là một con đường mở đồng thời cho nhiều giao thức.

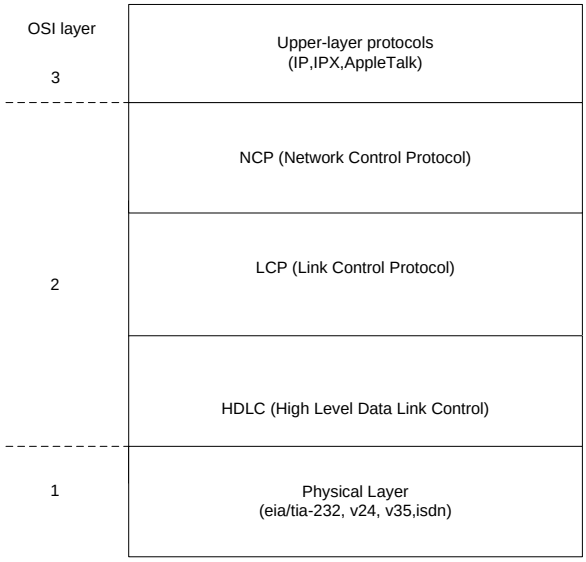
PPP khởi đầu được phát triển trong môi trường mạng IP, tuy nhiên nó thực hiện các chức năng độc lập với các giao thức lớp 3 và có thể được sử dụng cho các giao thức lớp mạng khác nhau. Như đã đề cập, PPP đóng gói các thủ tục lớp mạng đã được cấu hình để chuyển qua một liên kết PPP. PPP có nhiều các tính năng khiến nó rất mềm dẻo và linh hoạt, bao gồm:

- Ghép nối với các giao thức lớp mạng
- Lập cấu hình liên kết
- Kiểm tra chất lượng liên kết
- Nhận thực
- Nén các thông tin tiếp đầu
- Phát hiện lỗi
- Thỏa thuận các thông số liên kết

PPP hỗ trợ các tính năng này thông qua việc cung cấp LCP có khả năng mở rộng và NCP để thỏa thuận các thông số và các chức năng tùy chọn giữa các đầu cuối. Các giao thức, các tính năng tùy chọn, kiểu xác thực người dùng tất cả đều được truyền thông trong khi khởi tạo liên kết giữa hai điểm.

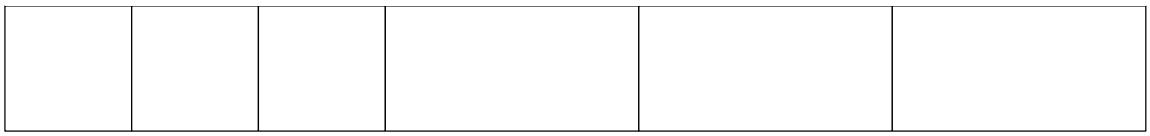
PPP có thể hoạt động trong bất kỳ giao diện DTE/DCE nào, PPP có thể hoạt động ở chế độ đồng bộ hoặc không đồng bộ. Ngoài những yêu cầu khác của các giao diện DTE/DCE, PPP không có hạn chế nào về tốc độ truyền dẫn.

Trong hầu hết các công nghệ mạng WAN, mô hình lớp được đưa ra để có những điểm liên hệ với mô hình OSI và để diễn tả vận hành của các công nghệ cụ thể. PPP không khác nhiều so với các công nghệ khác. PPP cũng có mô hình lớp để định nghĩa các cấu trúc và chức năng (hình 5.2)



Hình 5.2

Cũng như hầu hết các công nghệ, PPP có cấu trúc khung, cấu trúc này cho phép đóng gói bất cứ giao thức lớp 3 nào. Dưới đây là cấu trúc khung PPP (hình 5.3)



Hình 5.3

Các trường của khung PPP như sau:

Cờ: độ dài 1 byte sử dụng để chỉ ra rằng đây là điểm bắt đầu hay kết thúc một khung, trường này là một dãy bit 01111110

Địa chỉ: độ dài 1 byte bao gồm dãy bit 11111111, là địa chỉ quảng bá chuẩn. PPP không gán từng địa chỉ riêng.

Giao thức: độ dài 2 byte, nhận dạng giao thức đóng gói. Giá trị cập nhật của trường này được chỉ ra trong RFC 1700

Dữ liệu: có độ dài thay đổi, có thể 0 hoặc nhiều byte là các dữ liệu cho kiểu giao thức cụ thể đượoc chỉ ra trong trường giao thức. Phần cuối cùng của trường dữ liệu được nhận biết bằng cách đặt cờ và tiếp sau nó là 2 byte FCS. Giá trị ngầm định của trường này là 1500 byte. Tuy vậy giá trị lớn hơn có thể được sử dụng để tăng độ dài cho trường dữ lliệu.

FCS: thường là 2 byte, có thể sử dụng 4 byte FCS để tăng khả năng phát hiện lỗi.

LCP có thể thỏa thuận để chấp nhận sự thay đổi cấu trúc khung PPP chuẩn giữa hai đầu cuối của liên kết. Các khung đã thay đổi luôn luôn dễ nhận biết hơn so với các khung chuẩn. LCP cung cấp phương pháp để thiết lập, cấu hình, duy trì và kết thúc một kết nối điểm-điểm. LCP thực hiện các chức năng này thông qua bốn giai đoạn. Đầu tiên, LCP thực hiện thiết lập và thỏa thuận cấu hình giữa liên kết điểm điểm. Trước khi bất kỳ đơn vị dữ liệu lớp mạng nào được chuyển, LCP đầu tiên phải mở kết nối và thỏa thuận các thông số thiết lập. Quá trình này được hoàn thành khi một khung nhận biết cấu hình đã được gửi và nhận. Tiếp theo, LCP xác định chất lượng liên kết. Liên kết được kiểm tra để xác định xem liệu chất lượng có đủ để khởi tạo các giao thức lớp mạng không. Việc truyền dẫn của giao thức lớp mạng bị đình lại cho đến khi giai đoạn này hoàn tất. LCP cho phép đây là một tùy chọn sau giai đoạn thiết lập và thỏa thuận cấu hình của liên kết. Sau đó LCP thực hiện thỏa thuận cấu hình giao thức lớp mạng. Các giao thức lớp mạng có thể được cấu hình riêng rẽ bới NCP thích hợp và được khởi tạo hay dỡ bỏ vào bất kỳ thời điểm nào. Cuối cùng, LCP kết thúc liên kết khi xuất hiện yêu cầu từ người dùng hoặc theo các bộ định thời gian, do lỗi truyền dẫn hay do các yếu tố vật lý khác.

Ba kiểu khung LCP được sử dụng để hoàn thành các công việc đối với từng giai đoạn: khung thiết lập liên kết được sử dụng để thiết lập và cấu hình một liên kết, khung kết thúc liên kết được sử dụng để kết thúc một liên kết, khung duy trì liên kết được sử dụng để quản lý và gỡ rối liên kết.

3.Các giao thức mạng sử dụng trong truy cập từ xa.

Khi triển khai dịch vụ truy cập từ xa, các giao thức mạng thường được sử dụng là giao thức TCP/IP, IPX, NETBEUI.

TCP/IP là một bộ giao thức gồm có giao thức TCP và giao thức IP cùng làm việc với nhau để cung cấp phương tiện truyền thông trên mạng. TCP/IP là một bộ giao thức cơ bản, làm nền tảng cho truyền thông liên mạng là bộ giao thức mạng được sử dụng phổ biến nhất hiện nay. Với khả năng định tuyến và mở rộng, TCP/IP hỗ trợ một cách linh hoạt và phù hợp cho các tất cả các mạng.

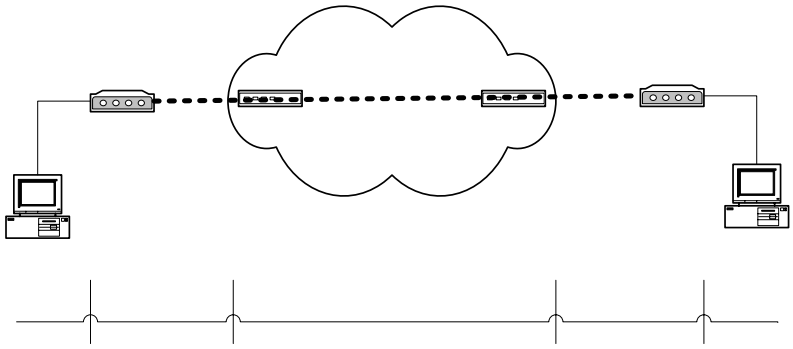
IPX (Internet Packet Exchange) là giao thức được sử dụng cho các mạng Novell NetWare. IPX là một giao thức có khả năng định tuyến và thường được sử dụng với các hệ thống mạng trước đây.

NetBEUI là giao thức dùng cho mạng cục bộ LAN của Microsoft. NetBEUI cho ta nhiều tiện ích và hầu như không phải làm gì nhiều với NetBEUI. Thông qua NetBEUI ta có thể truy cập tất cả các tài nguyên trên mạng. NETBEUI là một giao thức không có khả năng định tuyến và chỉ thích hợp với mô hình mạng nhỏ, đơn giản.

I.3. Modem và các phương thức kết nối vật lý.

1. Modem.

Máy tính làm việc với dữ liệu dạng số, khi truyền thông trên môi trường truyền dẫn với các dạng tín hiệu khác (ví dụ như với mạng điện thoại công cộng làm việc với các tín hiệu tương tự) ta cần một thiết bị để chuyển đổi tín hiệu số thành tín hiệu thích nghi với môi trường truyền dẫn, thiết bị đó là gọi là Modem (Modulator/demodulator). Như vậy Modem là một thiết bị chuyển đổi tín hiệu số sang dạng tín hiệu phù hợp với môi trường truyền dẫn và ngược lại. Hình dưới là một kết nối sử dụng modem qua mạng điện thoại điển hình (hình 5.4).



Hình 5.4

Các modem sử dụng các phương pháp nén dữ liệu nhằm mục đích tăng tốc độ truyền dữ liệu. Hiệu suất nén dữ liệu phụ thuộc vào dữ liệu, có hai giao thức nén thường được sử dụng là V.42bis và MNP 5. hiệu suất nén của V.42bis và MNP 5 có thể thay đổi từ 0 đến 400 % hay cao hơn phụ thuộc vào dữ liệu tự nhiên

Chuẩn modem V.90 cho phép các modem nhận dữ liệu với tốc độ 56 Kbps qua mạng điện thoại công cộng (PSTN). V.90 xem mạng PSTN như là một mạng số và chúng sẽ mã hóa dòng dữ liệu xuống theo kỹ thuật số thay vì điều chế để gửi đi như các chuẩn điều chế trước đây. Trong khi đó theo hướng ngược lại từ khách hàng đến nhà cung cấp dịch vụ dòng dữ liệu lên vẫn được điều chế theo các nguyên tắc thông thường và tốc độ tối ta đạt được là 33.6 Kbps, giao thức hướng lên này dựa trên chuẩn V.34

PC1

Digital A

Sự khác nhau giữa tín hiệu số ban đầu với tín hiệu số được phục hồi tại đầu nhận gọi là tạp âm lượng tử hóa (nhiễu lượng tử), chính tạp âm này đã hạn chế tốc độ truyền dữ liệu. Giữa các modem đầu cuối có một cấu trúc hạ tầng cho việc kết nối đó là mạng thoại công cộng. Các chuẩn modem trước đây đều giả sử cả hai đầu của kết nối giống nhau là có một kết nối tương tự vào mạng điện thoại công cộng, công nghệ V.90 đã lợi dụng ưu điểm của tổ chức mạng mà một đầu kết nối giữa hệ thống truy cập từ xa và mạng thoại công cộng là dạng số hoàn toàn còn đầu kia vẫn được kết nối vào mạng PSTN theo dạng tương tự nhờ đó tận dụng được các ưu điểm của liên kết số tốc độ cao, vì chỉ có quá trình biến đổi A/D mới gây ra tạp âm với các kết nối số thì không có lượng tử hóa do đó nhiễu lượng tử rất ít trong cấu trúc mạng này.

Định luật shanon nói rằng đường dây điện thoại tương tự hạn chế tốc độ truyền dữ liệu ở khoảng 35 kbps mà không xem xét đến một thực tế là một đầu của truyền thông đã được số hóa nên giảm nhỏ lượng tạp âm gây ra sự chậm trễ trong việc truyền dữ liệu. Nhiễu lượng tử đã giới hạn chuẩn truyền thông V.34 ở tốc độ 33.6 kbps, nhưng nhiễu lượng tử chỉ có ảnh hưởng khi chuyển đổi tương tự - số mà không có ảnh hưởng khi chuyển đổi số-tương tự và đây chính là chìa khóa cho công nghệ V.90 đồng thời cũng giải thích được vì sao tốc độ download có thể đạt được 56 kbps còn khi upload tốc độ chỉ đạt 33.6 kbps. Dữ liệu chuyển đi từ modem số V.90 qua mạng PSTN là một dòng số với tốc độ 64 Kbps nhưng tại sao V.90 chỉ hỗ trợ tốc độ đến 56 Kbps, vì các lí do sau: Thứ nhất mặc dù nhiễu lượng tử đã được bỏ qua nhưng nhiễu mức thấp do bộ chuyển đổi số - tương tự là không tuyến tính, do ảnh hưởng của vòng loop nội hạt. Lý do thứ hai là các tổ chức quốc tế có qui định chặt chẽ về mức năng lượng tín hiệu nhằm hạn chế nhiễu xuyên âm giữa các dây dẫn đặt gần kề nhau, và qui định này tương ứng với mức năng lượng tối đa trên đường dây điện thoại tương ứng là 56 kbps

Để xây dựng một hệ thống truy cập từ xa qua mạng thoại công cộng đạt được tốc độ 56 kbps giữa hai đầu kết nối cần hội đủ ba điều kiện sau: thứ nhất, một đầu của kết nối (thường là đầu trung tâm mạng) phải là kết nối số tới mạng PSTN. Thứ hai, chuẩn modem V.90 hỗ trợ tại hai đầu cuối của nối kết. Thứ ba, chỉ có một chuyển đổi duy nhất số-tương tự trên mạng thoại giữa hai đầu của kết nối

Khi vận hành modem V.90 thăm dò đường thoại để quyết định xem nó sẽ làm việc theo tiêu chuẩn nào, nếu phát hiện ra bất kỳ một chuyển đổi số-tương tự nào thì nó đơn giản chỉ làm việc ở chuẩn V.34 và cũng cố gắng kết nối ở chuẩn này nếu modem đầu xa không hỗ trợ chuẩn V.90.

2.Các phương thức kết nối vật lý cơ bản:

Một phương thức phổ biến và sẽ được dùng nhiều đó là kết nối qua mạng điện thoại công cộng (PSTN). Máy tính được nối qua một modem lắp đặt bên trong (Internal modem) hoặc qua cổng truyền số liệu nối tiếp COM port. Tốc độ truyền tối đa hiện nay có thể có được bằng phương thức này có thể lên đến 56 Kbps cho chiều lấy dữ liệu xuống và 33,6Kbps cho chiều truyền dữ liệu hướng lên với các chuẩn điều chế tín hiệu phổ biến V90, K56Flex, X2. Ta cũng

có thể sử dụng modem có yêu cầu về hạ tầng cơ sở thấp hơn với chuẩn điều chế V.24, V.32Bis, V.32...

Phương thức thứ hai là sử dụng mạng truyền số liệu số đa dịch vụ ISDN. Phương thức này đòi hỏi chi phí cao hơn và ngày càng được phổ biến rộng rãi. Ta có được khá nhiều các lợi ích từ việc sử dụng mạng ISDN mà một trong số đó là tốc độ. Ta có thể sử dụng các lựa chọn ISDN 2B+D BRI (2x64Kbps dữ liệu + 16Kbps dùng cho điều khiển) hoặc 23B+D PRI (23x64Kbps + 64Kbps) thông qua thiết bị TA (Terminal Adapter) hay các card ISDN.

Một phương thức khác nhưng ít được sử dụng là qua mạng truyền số liệu X.25, tốc độ không cao nhưng an toàn và bảo mật cao hơn. Yêu cầu cho người sử dụng trong trường hợp này là phải có sử dụng card truyền số liệu X.25 hoặc một thiết bị được gọi là PAD (Packet Asssembled Disassembled). Ta cũng có thể sử dụng các kết nối trực tiếp qua cáp modem, phương thức này cho ta các kết nối tốc độ cao nhưng phải thông qua các modem truyền số liệu có giá thành cao.

II. An toàn trong truy cập từ xa

II.1. Các phương thức xác thực kết nối

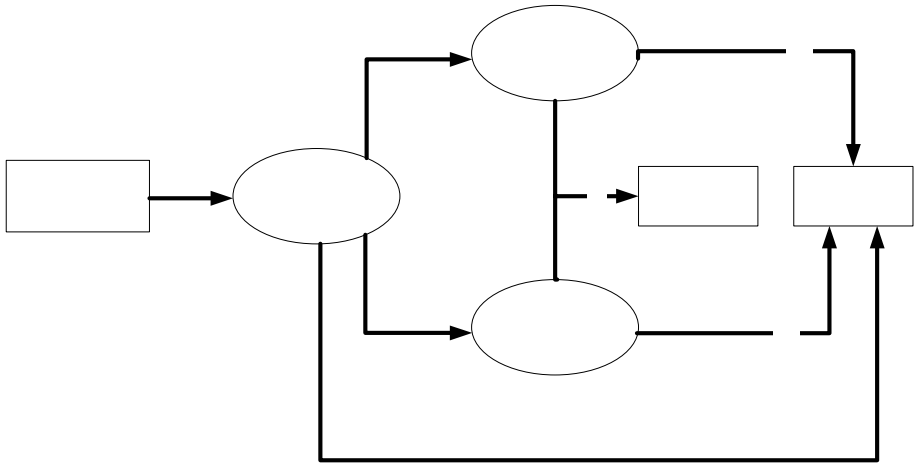
1.Qúa trình nhận thực.

Tiến trình nhận thực với các giao thức xác thực được thực hiện khi người dùng từ xa có các yêu cầu xác thực tới máy chủ truy cập, một thỏa thuận giữa người dùng từ xa và máy chủ truy cập để xác định phương thức xác thực sẽ sử dụng. Nếu không có phương thức nhận thực nào được sử dụng, tiến trình PPP sẽ khởi tạo kết nối giữa hai điểm ngay lập tức.

Phương thức xác thực có thể được sử dụng với các hình thức kiểm tra cơ sở dữ liệu địa phương (lưu trữ các thông tin về username và password ngay trên máy chủ truy cập) xem các thông tin về username và password được gửi đến có trùng với trong cơ sở dữ liệu hay không. Hoặc là gửi các yêu cầu xác thực tới một server khác để xác thực thường sử dụng là các RADIUS server (sẽ được trình bày ở phần sau)

Sau khi kiểm tra các thông tin gửi trả lại từ cơ sở dữ liệu địa phương hoặc từ RADIUS server. Nếu hợp lệ, tiến trình PPP sẽ khởi tạo một kết nối, nếu không yêu cầu kết nối của người dùng sẽ bị từ chối. (hình 5.5)

.

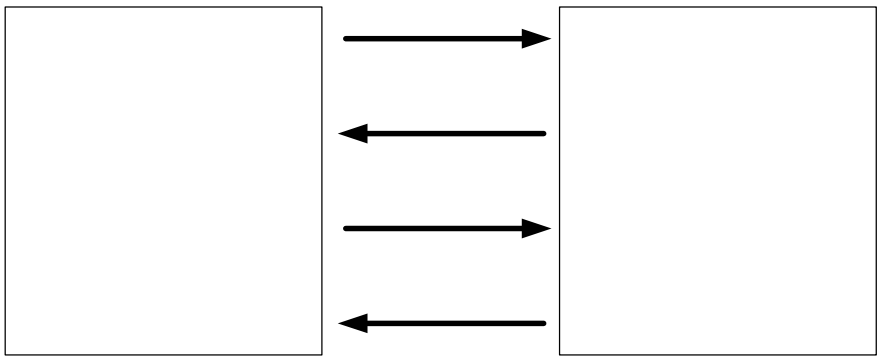


Hình 5.5

2.Giao thức xác thực PAP

PAP là một phương thức xác thực kết nối không an toàn, nếu sử dụng một chương trình phân tích gói tin trên đường kết nối ta có thể nhìn thấy các thông tin về username và password dưới dạng đọc được. Điều này có nghĩa là các thông tin gửi đi từ người dùng từ xa tới máy chủ truy cập không được mã hóa mà được gửi đi dưới dạng đọc được đó chính là lý do PAP không an toàn. Hình dưới mô tả quá trình xác thực PAP, sau khi thỏa thuận giao thức xác thực PAP trên liên kết PPP giữa các đầu cuối, người dùng từ xa gửi thông tin (username:nntrong, password:ras123) tới máy chủ truy cập từ xa, sau khi kiểm tra các thông tin này trong cơ sở dữ liệu của mình, máy chủ truy cập từ ra sẽ quyết định xem liệu yêu cầu kết nối có được thực hiện hay không (hình 5.6)

Incoming
PPP negotiation



Remote user

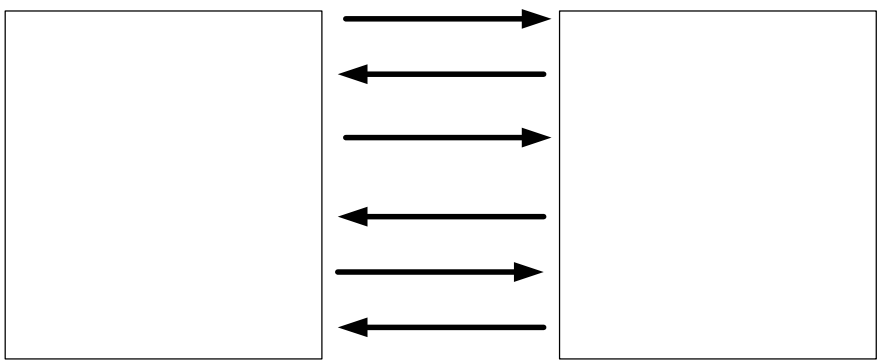
Hình 5.6

3.Giao thức xác thực CHAP

Sau khi thỏa thuận giao thức xác thực CHAP trên liên kết PPP giữa các đầu cuối, máy chủ truy cập gửi một "challenge" tới người dùng từ xa. Người dùng từ xa phúc đáp lại một giá trị được tính toán sử dụng tiến trình xử lý một chiều (hash). máy chủ truy cập kiểm tra và so sánh thông tin phúc đáp với giá trị hash mà tự nó tính được. Nếu các giá trị này bằng nhau việc xác thực là thành công, ngược lại kết nối sẽ bị hủy bỏ. Như vậy CHAP cung cấp cơ chế an toàn thông qua việc sử dụng giá trị challenge thay đổi, duy nhất và không thể đoán được. Các thông tin về username và password không được gửi đi dưới dạng đọc được trên mạng và do đó chống lại các truy cập trái phép bằng hình thức lấy trộm password trên đường kết nối (hình 5.7).

Inputs name ar

when pro



Hình 5.7

4.Giao thức xác thực mở rộng EAP

Ngoài các giao thức kiểm tra tính xác thực cơ bản PAP, CHAP, trong Microsoft Windows 2000 hỗ trợ thêm một số giao thức cho ta các khả năng nâng cao độ an toàn, bảo mật và đa truy nhập đó là giao thức xác thực mở rộng EAP (Extensible Authentication Protocol).

EAP cho phép có được một cơ cấu xác thực tuỳ ý để công nhận một kết nối gọi vào. Người sử dụng và máy chủ truy nhập từ xa sẽ trao đổi để tìm ra giao thức chính xác được sử dụng. EAP hỗ trợ các hình thức sau:

– Sử dụng các card vật lý dùng để cung cấp mật khẩu. Các card này dùng một số các phương thức xác thực khác nhau như sử dụng các đoạn mã thay đổi theo mỗi lượt sử dụng.

– Hỗ trợ MD5-CHAP, giao thức mã hoá tên người sử dụng, mật khẩu sử dụng thuật toán mã hoá MD5 (Message Digest 5).

– Hỗ trợ sử dụng cho các thẻ thông minh. Thẻ thông minh bao gồm thẻ và thiết bị đọc thẻ. Các thông tin xác thực về cá nhân người dùng được ghi lại trong các thẻ này.

– Các nhà phát triển phần mềm độc lập sử dụng giao diện chương trình ứng dụng EAP có thể phát triển các module chương trình cho các công nghệ áp dụng cho thẻ nhận dạng, thẻ thông minh, các phần cứng sinh học như nhận dạng võng mạc, các hệ thống sử dụng mật khẩu một lần.

II.2. Các phương thức mã hóa dữ liệu.

Dịch vụ truy cập từ xa cung cấp cơ chế an toàn bằng việc mã hóa và giải mã dữ liệu truyền giữa người dùng truy cập từ xa và máy chủ truy cập. Có hai phương thức mã hóa dữ liệu thường được sử dụng đó là mã hóa đối xứng và mã hóa phi đối xứng.

Phương thức mã hoá đối xứng, thông tin ở dạng đọc được, được mã hoá sử dụng khóa bí mật (khoá mà chỉ có người mã hoá mới biết được) tạo thành thông tin đã được mã hoá. ở phía nhận, thông tin mã hoá được giải mã cùng với khóa bí mật thành dạng gốc ban đầu. Điểm chú ý của phương pháp mã hoá này là việc sử dụng khoá bí mật cho cả quá trình mã hoá và quá trình giải mã. Do

đó, nhược điểm chính của phương thức này là cần có quá trình trao đổi khoá bí mật, dẫn đến tình trạng dễ bị lộ khoá bí mật.

Phương pháp mã hoá phi đối xứng, để khắc phục điểm hạn chế của phương pháp mã hoá đối xứng là quá trình trao đổi khoá bí mật, người ta đã sử dụng phương pháp mã hoá phi đối xứng sử dụng một cặp khoá tương ứng với nhau gọi là phương thức mã hoá phi đối xứng dùng khoá công khai. Phương thức mã hóa này sử dụng hai khóa là khóa công khai và khóa bí mật có các quan hệ toán học với nhau. Trong đó khóa bí mật được giữ bí mật và không có khả năng bị lộ do không cần phải trao đổi trên mạng. Khóa công khai không phải giữ bí mật và mọi người đều có thể nhận được khoá này. Do phương thức mã hóa này sử dụng 2 khóa khác nhau, nên người ta gọi nó là phương thức mã hóa phi đối xứng. Mặc dù khóa bí mật được giữ bí mật, nhưng không giống với "secret Key" được sử dụng trong phương thức mã hóa đối xứng sử dụng khoá bí mật do khóa bí mật không được trao đổi trên mạng. Khóa công khai và khóa bí mật tương ứng của nó có quan hệ toán học với nhau và được sinh ra sau khi thực hiện các hàm toàn học; nhưng các hàm toán học này luôn thoả mãn điều kiện là sao cho không thể tìm được khóa bí mật từ khóa công cộng và ngược lại. Do có mối quan hệ toán học với nhau, thông tin được mã hóa bằng khóa công khai chỉ có thể giải mã được bằng khóa bí mật tương ứng.

Giao thức thường được sử dụng để mã hóa dữ liệu hiện nay là giao thức IPsec. Hầu hết các máy chủ truy cập dựa trên phần cứng hay mềm hiện nay đều hỗ trợ IPSec. IPSec là một giao thức bao gồm các chuẩn mở bảo đảm các vấn đề bảo mật, an toàn và toàn vẹn dữ liệu cho các kết nối qua mạng sử dụng giao thức IP bằng các biện pháp mã hoá. IPSec bảo vệ chống lại các hành động phá hoại từ bên ngoài. Các client khởi tạo một mối liên quan bảo mật hoạt động tương tự như khoá công khai để mã hoá dữ liệu.

Ta có thể sử dụng các chính sách áp dụng cho IPSec để cấu hình nó. Các chính sách cung cấp nhiều mức độ và khả năng để bảo đảm an toàn cho từng loại dữ liệu. Các chính sách cho IPSec sẽ được thiết lập cho phù hợp với từng người dùng, từng nhóm người dùng, cho một ứng dụng, một nhóm miền hay toàn bộ hệ thống mạng.

III. Triển khai dịch vụ truy cập từ xa

III.1. Kết nối gọi vào và kết nối gọi ra

Cấu hình máy chủ truy cập để tạo lập các kết nối gọi vào cho phép người dùng từ xa truy cập vào mạng. Các thông số cơ bản thường được cấu hình khi tạo lập các kết nối gọi vào bao gồm xác định các phương thức xác thực người dùng, mã hóa hay không mã hóa dữ liệu, các phương thức mã hóa dữ liệu nếu yêu cầu, các giao thức mạng sẽ được sử dụng cho truy nhập từ xa, các thiết đặt về chính sách và các quyền truy nhập của người dùng từ xa, mức độ được phép truy nhập như thế nào, xác định phương thức cấp phát địa chỉ IP cho máy truy nhập từ xa, các yêu cầu cấu hình để tạo lập các kết nối VPN…

Kết nối gọi ra có thể được thiết lập để gọi ra tới một mạng dùng riêng hoặc tới một ISP. Trong windows 2000 hỗ trợ các hình thức kết nối sau:

Nối tới mạng dùng riêng, ta sẽ phải cung cấp số điện thoại nơi sẽ nối đến. Có thể là số điện thoại của ISP, của mạng dùng riêng hay của máy tính phía xa. Xác định quyền sử dụng kết nối này. .

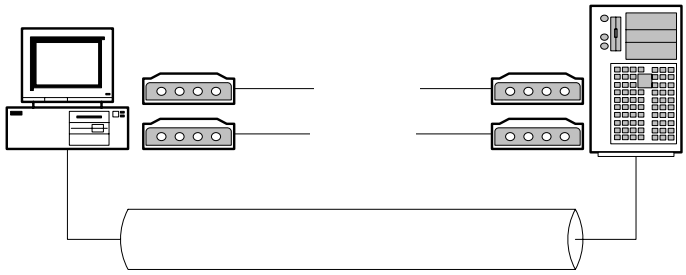
Nối tới Internet, hai lựa chọn có thể là sử dụng truy cập qua đường thoại và sử dụng truy cập qua mạng LAN. Sử dụng đường thoại, các vấn đề ta cần quan tâm là số điện thoại truy nhập, tên và mật khẩu được cung cấp bởi ISP. Sử dụng LAN, ta sẽ phải quan tâm đến proxy server và một số thiết đặt khác.

Tạo lập kết nối VPN, ***VPN là một mạng sử dụng các kết nối dùng giao thức tạo đường hầm (PPTP, L2TP, IPSEC,...) để tạo được các kết nối an toàn, bảo đảm thông tin không bị xâm phạm khi truyền tải qua các mạng công cộng. Tương tự như khi tạo lập một kết nối gọi ra, Nếu cần thiết phải thông qua một ISP trung gian trước khi nối tới mạng dùng riêng, lựa chọn một kết nối gọi ra. Cung cấp địa chỉ máy chủ, địa chỉ mạng nơi mà ta đang muốn nối tới. Các thiết lập khác là thiết đặt các quyền sử dụng kết nối.***

Tạo lập kết nối trực tiếp với máy tính khác, lựa chọn này được sử dụng để kết nối trực tiếp hai máy tính với nhau thông qua một cáp được thiết kế cho nối trực tiếp hai máy tính. Một trong hai máy tính được lựa chọn là chủ và máy tính kia được lựa chọn là tớ. Lựa chọn thiết bị cổng nơi hai máy tính nối với nhau.

III.2. Kết nối sử dụng đa luồng(Multilink)

Multilink là sự kết hợp nhiều liên kết vật lý trong một liên kết logic duy nhất nhằm gia tăng băng thông cho kết nối. Multilink cho phép sử dụng hai hoặc nhiều hơn các cổng truyền thông như là một cổng duy nhất có tốc độ cao. Điều này có nghĩa là ta có thể sử dụng hai modem để kết nối Internet với tốc độ cao gấp đôi so với việc sử dụng một modem. Multilink gia tăng băng thông và giảm độ trễ giữa các hệ thống bằng cơ chế chia các gói dữ liệu và gửi đi trên các mạch song song. Multilink sử dụng giao thức MPPP cho việc quản lý các kết nối của mình. Để sử dụng, MPPP cần phải được hỗ trợ ở cả hai phía của kết nối (hình 5.8).



Hình 5.8

Hình vẽ mô tả kết nối sử dụng Multilink, khi người dùng từ xa sử dụng hai modem và hai đường thoại kết nối với máy chủ truy cập, mỗi kết nối là việc theo chuẩn V.90 có tốc độ 56 kbps sử dụng kỹ thuật Multilink cho phép đạt tốc độ 112 Kbps giữa máy truy cập từ xa và máy chủ truy cập.

III.3. Các chính sách thiết lập cho dịch vụ truy nhập từ xa

Chính sách truy nhập từ xa là tập hợp các điều kiện và các thiết đặt cho phép người quản trị mạng gán cho mỗi người dùng từ xa các quyền truy cập và mức độ sử dụng các nguồn tài nguyên trên mạng. Ta có thể dùng các chính sách để có được nhiều các lựa chọn phù hợp với từng mức độ người dùng, tăng tính mềm dẻo, tính năng động khi cấp quyền truy nhập cho người dùng.

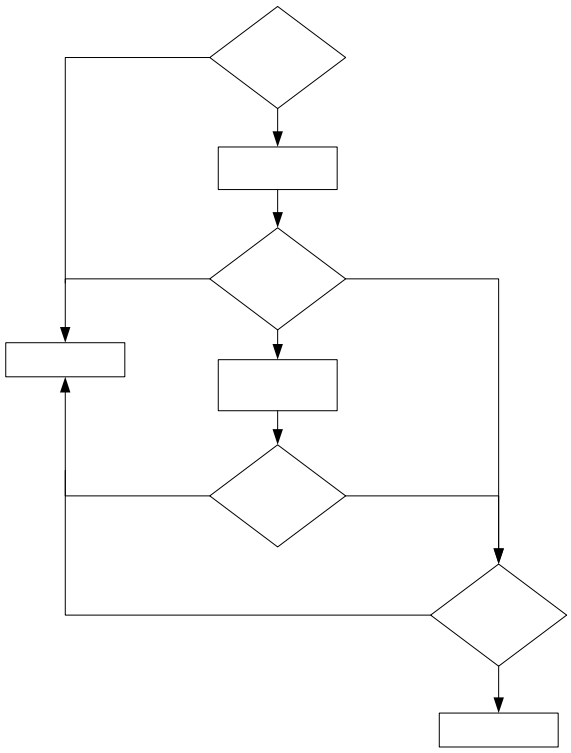
Một chính sách truy nhập từ xa thông thường bao gồm ba thành phần nhằm cung cấp các truy nhập an toàn có kiểm soát đến máy chủ truy cập.

Các điều kiện (Conditions): là một danh sách các tham số như ngày tháng, nhóm người dùng, mã người gọi, địa chỉ IP phù hợp với máy trạm đang nối đến máy chủ truy cập. Bộ chính sách điều kiện đầu tiên này tương ứng với các thông số của yêu cầu kết nối gọi đến được xử lý đối với sự cho phép truy cập và cấu hình.

Sự cho phép (Permission): Các kết nối truy nhập từ xa được cho phép và gán trực tiếp tới mỗi người dùng bởi các thiết đặt trong các chính sách truy nhập từ xa. Ví dụ một chính sách có thể gán tất cả người dùng trong một nhóm nào đấy quyền truy cập chỉ trong giờ làm việc hành chính từ 8:00 A.M đến 5:00 P.M, hay đồng thời gán cho một nhóm người dùng khác quyền truy cập liên tục 24/24.

Profile: Mỗi chính sách đều bao gồm một thiết đặt của profile áp dụng cho kết nối như là các thủ tục xác thực hay mã hóa. Các thiết đặt trong profile được thi hành ngay tới các kết nối. Ví dụ: nếu một profile thiết đặt cho một kết nối mà người dùng chỉ được phép sử dụng trong 30 phút mỗi lần thì người dùng sẽ bị ngắt kết nối tới máy chủ truy cập trong sau 30 phút.

Quá trình thực thi các chính sách truy cập từ xa được mô tả bằng hình dưới (hình 5.9)



Hình 5.9

Các điều kiện được gửi tới để tạo một kết nối, nếu các điều kiện gửi tới này không thích hợp truy cập bị từ chối, nếu thích hợp các điều kiện này được sử dụng để xác định sự truy cập. Tiếp theo máy chủ truy cập kiểm tra các cho phép quay số vào người dùng sẽ bị từ chối nếu thiết đặt này là Deny và được phép truy cập nếu là Allow, nếu thiết đặt là sử dụng các chính sách truy cập để xác định quyền truy cập thì sự cho phép của các chính sách sẽ quyết định quyền truy cập của người dùng. Nếu các chính sách này từ chối truy cập người dùng sẽ bị ngắt kết nối, nếu là cho phép sẽ chuyển tới để kiểm tra các chính sách trong profile là bước cuối cùng để xác định quyền truy cập của người dùng.

III.4. Sử dụng dịch vụ gán địa chỉ động DHCP cho truy cập từ xa

Khi thiết lập một máy chủ truy cập để cho phép người dùng từ xa truy cập vào mạng, ta có thể lựa chọn phương thức mà các máy từ xa có thể nhận được địa chỉ IP.

Với phương thức cấu hình địa chỉ IP tĩnh ngay trên các máy trạm, người dùng phải cấu hình bằng tay địa chỉ IP trên mỗi máy truy cập. Sử dụng phương thức này phải đảm bảo rằng các thông tin cấu hình địa chỉ IP là hợp lệ và chưa được sử dụng trên mạng. Đồng thời các thông tin về default gateway, DNS…cũng phải được cấu hình bằng tay một cách chính xác.Vì lí do này khuyến nghị không nên sử dụngphương pháp này cho việc gán IP cho các máy truy cập từ xa.

Máy chủ truy cập có thể gán động một địa chỉ IP cho các máy truy cập từ xa. Địa chỉ IP này thuộc trong khoảng địa chỉ mà ta đã cấu hình trên máy chủ truy cập. Sử dụng phương pháp này ta cần phải đảm bảo rằng khoảng địa chỉ IP này được dành riêng để cấp phát cho các máy truy cập từ xa.

Phương thức sử dụng DHCP server, máy chủ truy cập nhận địa chỉ IP từ DHCP server và gán cho các máy truy cập từ xa. Phương thức này rất linh hoạt, không cần phải dành riêng một khoảng địa chỉ IP dự trữ cho máy truy cập từ xa và thường được sử dụng trong một mạng có tổ chức và đa dạng trong các hình thức kết nối. Địa chỉ IP được cấp phát cho các máy truy cập từ xa một cách tự động, các thông tin cấu hình khác (Gateway, DNS server…) cũng được cung cấp tập trung, chính xác tới từng máy truy cập đồng thời các máy truy cập cũng không cần thiết phải cấu hình lại khi có các thay đổi về cấu trúc mạng.

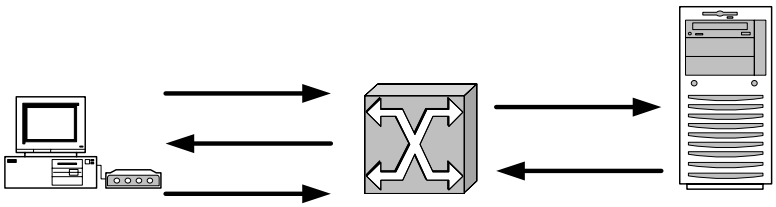
Hoạt động của DHCP được mô tả như sau: Mỗi khi DHCP client khởi động, nó yêu cầu một địa chỉ IP từ DHCP server. Khi DHCP server nhận yêu cầu, nó chọn một địa chỉ IP trong khoảng IP đã được định nghĩa trong cơ sở dữ liệu của nó. DHCP server cấp phát địa chỉ IP tới DHCP client Nếu DHCP client chấp nhận địa chỉ IP này, DHCP server cho thuê địa chỉ IP này trong một khoảng thời gian cụ thể (tùy theo thiết đặt). Các thông tin về địa chỉ IP được gửi từ DHCP server tới DHCP client thường bao gồm các thành phần sau: địa chỉ IP, subnet mask, các giá trị lựa chọn khác (default gateway, địa chỉ DNS server).

III.5. Sử dụng Radius server để xác thực kết nối cho truy cập từ xa.

1. Hoạt động của Radius server

RADIUS là một giao thức làm việc theo mô hình client/server. RADIUS cung cấp dịch vụ xác thực và tính cước cho mạng truy nhập gián tiếp. Radius

client là một máy chủ truy cập tiếp nhận các yêu cầu xác thực từ người dùng từ xa và chuyển các yêu cầu này tới Radius server. Radius server nhận các yêu cầu kết nối của người dùng xác thực và sau đó trả về các thông tin cấu hình cần thiết cho Radius client để chuyển dịch vụ tới người sử dụng (hình 5.10).



Hình 5.10

Quá trình hoạt động được mô tả như sau:

1. Người sử dụng từ xa khởi tạo quá trình xác thực PPP tới máy chủ truy cập

2. Máy chủ truy cập yêu cầu người dùng cung cấp thông tin về username và password bằng các giao thức PAP hoặc CHAP.

3. Người dùng từ xa phúc đáp và gửi thông tin username và password tới máy chủ truy cập.

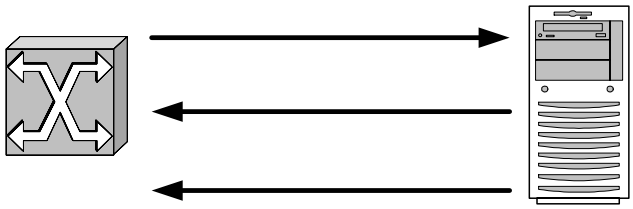
4. Máy chủ truy cập (Radius client) gửi chuyển tiếp các thông tin username và password đã được mã hóa tới Radius server

5. Radius server trả lời với các thông tin chấp nhận hay từ chối. Radius client thực hiện theo các dịch vụ và các thông số dịch vụ đi cùng với các phúc đáp chấp nhận hay từ chối từ Radius server

2. Nhận thực và cấp quyền

Khi Radius server nhận yêu cầu truy cập từ Radius client, Radius server tìm kiếm trong cơ sở dữ liệu các thông tin về yêu cầu này. Nếu username không có trong cơ sở dữ liệu này thì hoặc một profile mặc định được chuyển hoặc một thông báo từ chối truy cập được chuyển tới Radius client.

Trong RADIUS nhận thực và cấp quyền đi đôi với nhau, nếu username có trong cơ sở dữ liệu và password được xác nhận là đúng thì Radius server gửi trả về thông báo truy cập được chấp nhận, thông báo này bao gồm một danh sách các cặp đặc tính- giá trị mô tả các thông số được sử dụng cho phiên làm việc. Các thông số điển hình bao gồm: kiểu dịch vụ, kiểu giao thức, địa chỉ gán cho người dùng (động hoặc tĩnh), danh sách truy cập được áp dụng hay một định tuyến tĩnh được cài đặt trong bảng định tuyến của máy chủ truy cập. Thông tin cấu hình trong Radius server sẽ xác định những gì sẽ được cài đặt trên máy chủ truy cập. Hình vẽ dưới đây mô tả quá trình nhận thực và cấp quyền của Radius server (hình 5.11)



Hình 5.11

3.Tính cước

Các vấn đề về xử lý cước của RADIUS hoạt động độc lập với nhận thực và cấp quyền. Chức năng tính cước cho phép ghi lại dữ liệu được gửi tại thời điểm bắt đầu và kết thúc của một phiên làm việc và đưa ra các con số về mặt sử dụng tài nguyên như (thời gian, số gói, số byte...) được sử dụng trong phiên làm việc đó.

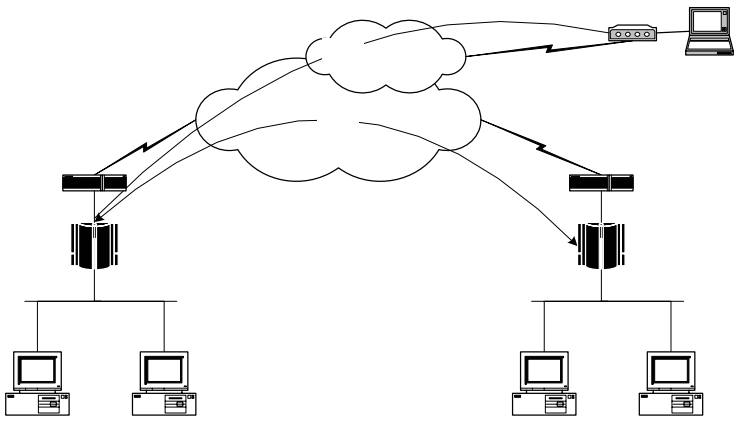
III.6. Mạng riêng ảo và kết nối sử dụng dịch vụ truy cập từ xa.

VPN (Virtual Private Network) là một mạng riêng được xây dựng trên nền tảng hạ tầng mạng công cộng (ví dụ mạng Internet), sử dụng mạng công cộng cho việc truyền thông riêng tư.

Giải pháp VPN cho phép người dùng làm việc tại nhà hoặc đang đi công tác ở xa có thể thực hiện một kết nối tới trụ sở chính bằng việc sử dụng hạ tầng

mạng là một mạng công cộng như là Internet, Như vậy thay vì phải thực hiện một kết nối đường dài tới trụ sở chính người sử dụng chỉ cần tạo lập một kết nối nội hạt tới một ISP khi đó bằng công nghệ VPN một kết nối VPN sẽ được thiết lập giữa người dùng với mạng trung tâm. Kết nối VPN cũng cho phép các tổ chức kết nối liên mạng giữa các địa điểm ở xa khác nhau thông qua các kết nối trực tiếp (leased line) từ các địa điểm đó tới một ISP. Như vậy kết nối VPN cho phép một tổ chức giảm chi phí gọi đường dài qua Dialup hay chi phí thuê đường leadline cho khoảng cách xa thay vì như vậy chỉ cần các kết nối nội hạt và điều này là tiết kiệm được chi phí. VPN gửi dữ liệu giữa các đầu cuối, dữ liệu được đóng gói, với các Header cung cấp thông tin định tuyến cho phép chuyển dữ liệu qua một liên kết hoặc một liên mạng công cộng tới đích. Dữ liệu chuyển đi được mã hoá để đảm bảo an toàn, các gói dữ liệu truyền thông trên mạng là không thể đọc mà không có khoá giải mã. Liên kết mà trong đó dữ liệu được đóng gói và mã hoá là một kết nối VPN.

Các hình thức kết nối: Có hai kiểu kết nối VPN, kết nối VPN truy cập từ xa và kết nối Site-to-site. Một kết nối VPN truy cập từ xa được thiết lập bởi một máy tính PC tới một mạng dùng riêng. VPN gateway cung cấp truy cập tới các tài nguyên của mạng dùng riêng. Các gói dữ liệu gửi qua kết nối VPN được khởi tạo từ các client. VPN client thực hiện việc xác thực tới VPN gateway. Kết nối site-to-site, được thiết lập bởi các VPN gateway và kết nối hai phần của một mạng dùng riêng. (hình 5.12).



Hình 5.12

Tunnel: là một phần quan trọng trong việc xây dựng một mạng VPN. Các chuẩn truyền thông sử dụng để quản lý các tulnnel và đóng gói dữ liệu của VPN bao gồm các giao thức làm việc ở lớp 2 như PPTP (Point-to-Point Tunlling Protocol) được phát triển bởi Microsoft hỗ trợ trong môi trường mạng Windows, L2TP (Layer 2 Tunnelling Protocol) được phát triển bởi Cisco. IPsec là một giao thức làm việc ở lớp 3, IPsec được phát triển bởi IETF và ngày càng được sử dụng rộng rãi.

L2TP và PPTP có mục đích là cung cấp các đường hầm dữ liệu thông qua mạng truyền dữ liệu công cộng. L2TP khác với PPTP ở chỗ nó tạo lập đường hầm nhưng không mã hoá dữ liệu. L2TP cung cấp các đường hầm bảo mật khi cùng hoạt động với các công nghệ mã hoá khác như IPSec. IPSec không yêu cầu phải có L2TP nhưng các chức năng mã hoá của nó đưa đến cho L2TP khả năng cung cấp các kênh thông tin bảo mật, cung cấp các giải pháp VPN. L2TP và PPTP cùng sử dụng PPP để đóng gói, thêm bớt thông tin tiếp đầu và truyền tải dữ liệu qua mạng.

Các kết nối VPN có các đặc trưng sau: đóng gói (Encapsulation), xác thực (Authentication) và mã hoá dữ liệu (Data encryption)

Đóng gói dữ liệu: Công nghệ VPN sử dụng một phương thức đóng gói dữ liệu trong đó cho phép dữ liệu truyền được qua mạng công cộng qua các giao thức tạo đường hầm.

Xác thực: Khi một kết nối VPN được thiết lập,VPN gateway sẽ xác thực VPN client đang yêu cầu kết nối và nếu được được phép kết nối được thực hiện. Nếu sự xác thực kết nối là qua lại được sử dụng, thì VPN client sẽ thực hiện việc xác thực lại VPN gateway, để đảm bảo rằng đấy chính là server mà mình cần gọi. Xác thực dữ liệu và tính toàn vẹn của dữ liệu: để xác nhận rằng dữ liệu đang được gửi từ một đầu của kết nối khác mà không bị thay đổi trong quá trình truyền, dữ liệu phải bao gồm một trường kiểm tra bằng mật mã dự trên một khoá mã hoá đã biết chỉ giữa người gửi và người nhận

Mã hóa dữ liệu: để đảm bảo dữ liệu truyền trên mạng, dữ liệu phải được mã hoá tại đầu gửi và giải mã tại đầu nhận. Việc mã hoá và giải mã dữ liệu phụ thuộc và người gửi và người nhận đang sử dụng phương thức mã hoá và giải mã nào.

III.7. Sử dụng Network and Dial-up Connection.

Network and Dial-up Connection (NDC) là một công cụ được Microsoft phát triển để hỗ trợ việc tạo lập các kết nối trong đó bao gồm các kết nối cho truy cập từ xa. Với việc sử dụng NDC ta có thể truy cập tới các tài nguyên dù đang ở trong mạng hay ở một địa điểm ở xa. Các kết nối được khởi tạo, thiết lập cấu hình, lưu giữ và quản lý bởi NDC. Mỗi một kết nối bao gồm một bộ các đặc tính được sử dụng để thiết lập liên kết giữa một máy tính tới máy tính hoặc mạng khác. Các kết nối gọi ra được liên lạc với một máy chủ truy cập ở xa bằng các hình thức truy cập gián tiếp thương là qua các mạng truyền dẫn mạng thoại công cộng, mạng ISDN. NDC cũng hỗ trợ việc thiết lập các kết nối gọi vào có nghĩa là đóng vai trò như một máy chủ truy cập.

Bởi vì tất cả các dịch vụ và các phương thức truyền thông đều được thiết lập trong kết nối nên không cần phải sử dụng các công cụ khác để cấu hình cho kết nối. Ví dụ để thiết lập cho một kết nối dial-up bao gồm các đặc tính được sử dụng trước, trong và sau khi kết nối. Các thông số này bao gồm: modem sẽ quay số, kiểu mã hóa password được sử dụng và các giao thức mạng sẽ sử dụng sau kết nối. Trạng thái kết nối bao gồm thời gian và tốc độ cũng được chính kết nối hiển thị mà không cần bất cứ một công cụ nào khác.

III.8. Một số vấn đề xử lý sự cố trong truy cập từ xa.

Các vấn đề liên quan đến sự cố trong truy cập từ xa, thường bao gồm:

Giám sát truy cập từ xa: giám sát máy chủ truy cập là phương pháp tốt nhất thường sử dụng để tìm ra nguồn gốc của các vấn đề xảy ra sự cố. Mỗi một chương trình phần mềm hay thiết bị phần cứng máy chủ truy cập bao giờ cũng có các công cụ sử dụng để giám sát và ghi lại các sự kiện xảy ra (trong các file log) đối với mỗi phiên truy cập từ xa.

Theo dõi các kết nối truy cập từ xa: khả năng theo dõi các kết nối truy cập từ xa của một Máy chủ truy cập cho ta xử lý các vấn đề phức tạp về sự cố mạng. Các thông tin theo dõi một kết nối từ xa thường rất phức tạp và khá chi tiết do đó để phân tích và xử lý cần thiết người quản trị mạng phải có kinh nghiệm và trình độ về hệ thống mạng.

Xử lý các sự cố về phần cứng: bao gồm các thiết bị truyền thông tại người dùng và tại máy chủ truy cập. Đối với các thiết bị tại người dùng (thường là các modem, cạc mạng...), hãy xem tài liệu về sản phẩm đó hay hỏi nhà cung cấp thiết bị về sản phẩm của họ về các cách kiểm tra và xác định lỗi của sản phẩm này. Nếu kết nối sử dụng modem, hãy kiểm tra rằng modem đã được cài đặt đúng chưa. Trong Windows 2000 các bước kiểm tra như sau:

- Trong Control Panel, kích Phone and Modem Options
- Trong trang modem, kích tên modem, sau đó kích Properties
- Kích Diagnostics, sau đó kích Query Modem.

Nếu modem đã được cài đặt đúng, bộ các thông số về modem sẽ được hiển thị, ngược lại hãy kiểm tra và cài đặt lại modem, trong trường hợp cuối cùng hãy hỏi nhà sản xuất thiết bị này. Để nhận thêm các thông tin về modem trong khi đang cố gắng tạo lập một kết nối, hãy xem thông tin trong log file để tìm ra nguyên nhân gạp sự cố. Để ghi các thông tin vào log file thực hiện theo các bước sau:

- Trong Control Panel, kích Phone and Modem Options
- Trong trang modem, kích tên modem, sau đó kích Properties
- Kích Diagnostics, sau đó kích lựa chọn Record a log, sau đó kích OK.

Đối với thiết bị truyền thông tại máy chủ truy cập: Kiểm tra các thiết bị phần cứng tương tự như trong trường hợp thiết bị tại người dùng, đồng thời kiểm tra log file về các sự kiện xẩy ra với hệ thống để tìm ra nguyên nhân sự cố. Một cách khác để kiểm tra modem tại máy chủ truy cập là sử dụng một đường điện thoại và gọi tới modem đó sau đó nghe xem modem đó có trả lời và cố gắng tạo một kết nối hay không. Nếu không có tín hiệu tạo kết nối từ modem đó thì có thể kết luận rằng đang có một vấn đề lỗi về modem tại máy chủ truy cập

Xử lý các sự cố về đường truyền thông: Thường là do cáp được đấu sai hay vì nguyên nhân từ nhà cung cấp dịch vụ điện thoại. Hãy kiểm tra đường điện thoại từ người dùng tới máy chủ truy cập bằng cách gọi điện thoại thông thường, thông qua chất lượng cuộc gọi ta cũng có thể phần nào dự đoán được chất lượng của đường truyền.

Xử lý các thiết đặt về cấu hình: Sau khi xác định rằng các vấn đề về phần cứng cũng như đường truyền thông đều tốt, bước tiếp theo ta kiểm tra các thiết đặt về cấu hình, bao gồm:

Các thiết đặt về mạng: lỗi cấu hình về mạng xảy ra khi đã tạo kết nối thành công nhưng vẫn không thể truy cập được các nguồn tài nguyên trên mạng, các lỗi thường xẩy ra như việc phân giải tên chưa hoạt động, các lỗi về định tuyến...khi lỗi về cấu hình mạng xảy ra, trước tiên ta kiểm tra rằng các máy kết nối trực tiếp (không thông qua dịch vụ truy cập từ xa) có thể truy cập được vào các nguồn tài nguyên trên mạng. Sau đó kiểm tra các cấu hình về TCP/IP bằng việc sử dụng lệnh ipconfig /all trên máy client. Kiểm tra rằng các thông số như DNS, địa chỉ IP, các thông số về định tuyến đã được thiết đặt đúng chưa. Sử dụng lệnh ping để kiểm tra kết nối mạng đã làm việc.

Các thiết đặt Máy chủ truy cập: Các thiết đặt trên máy chủ truy cập với các thông sô sai khi tạo lập kết nối có thể là nguyên nhân người dùng không thể truy cập vào các nguồn tài nguyên trên mạng. Để hỗ trợ cho việc xác định nguyên nhân gây lỗi, kiểm tra các sự kiện đã ghi log trên máy chủ truy cập và client, trong một số trường hợp cần thiết phải theo dõi (tracing) các kết nối trên máy chủ truy cập.

Các thiết đặt trên máy người dùng từ xa: kiểm tra các giao thức mạng làm việc trên client, các giao thức mạng làm việc trên client phải được hỗ trợ bởi máy chủ truy cập. Ví dụ, nếu người dùng từ xa thiết đặt trên client các giao thức NWLink, IPX/SPX và máy chủ truy cập chỉ hỗ trợ sử dụng TCP/IP, thì kết nối sẽ không thành công.

IV. Bài tập thực hành.

Yêu cầu về Phòng học lý thuyết: Số lượng máy tính theo số lượng học viên trong lớp học đảm bảo mỗi học viên có một máy tính, cấu hình máy tối thiểu như sau (PIII 800 MHZ, 256 MB RAM, HDD 1GB,FDD, CDROM 52 x). Máy tính đã cài đặt Windows 2000 advance server. Các máy tính đã được nối mạng chạy giao thức TCP/IP.

Thiết bị thực hành: Đĩa cài phần mềm Windows 2000 Advance Server. Mỗi máy tính có 01 Modem V.90 và 01 đường điện thoại. 01 account truy cập internet

Bài 1.

Thiết lập dialup networking để tạo ra kết nối Internet. truy cập Internet và giới thiệu các dịch vụ cơ bản

✓ Đăng nhập vào hệ thống với quyền Administrator.

✓ Kích Start, trỏ settings, sau đó kích Network and Dial-up Connections

✓ Trong Network and Dial-up Connections, kích đúp vào Make New Connection.

✓ Trong Network Connection Wizard, kích Next, có hai lựa chọn có thể sử dụng là Dial-up to private network hoặc Dial-up to the Internet.

✓ Nếu chọn Dial-up to private network, đưa vào số điện thoại truy cập của nhà cung cấp.

✓ Nếu chọn Dial-up to the Internet, lúc đó Internet Connection Wizard sẽ bắt đầu, làm theo các bước chỉ dẫn.

✓ Nếu muốn tất cả người dùng đều có thể sử dụng kết nối này thì lựa chọn, For all users, sau đó kích Next. Nếu muốn chỉ người dùng hiện tại sử dụng thì lựa chọn Only for myself, sau đó kích Next.

✓ Nếu đã lựa chọn Only for myself thì chuyển đến bước cuối cùng, Nếu lựa chọn For all users và muốn các máy tính khác trên mạng có thể chia sẻ kết nối này hãy lựa chọn Enable Internet Connection Sharing for this connection.

✓ Thiết đặt ngầm định là bất kỳ mày tính nào cũng có thể khởi tạo kết nối này một cách tự động, nếu muốn bỏ ngầm định này hãy xóa lựa chọn Enable on-demand dialing, sau đó kích next

✓ Đưa vào tên của kết nối và kích Finish.

Bài 2

Cài đặt và cấu hình dịch vụ truy cập từ xa cho phép người dùng từ xa truy cập vào mạng trên hệ điều hành Windows 2000 server.

Bước 1:

Cài đặt máy chủ dịch vụ truy cập từ xa

✓ Đăng nhập vào hệ thống với quyền Administrator

✓ Mở Routing and Remote Access từ menu Administrator Tools

✓ Kích chuột phải vào tên Server sau đó chọn Configure and Enable Routing and remote Access.

✓ Kịch bản Routing and Remote Access Server Setup xuất hiện, kích next

✓ Trong trang common Configuration, chọn Remote access server, sau đó kích next

✓ Trong trang Remote Client Protocol, xác định các giao thức sẽ hỗ trợ cho truy cập từ xa, sau đó kích next

✓ Trong trang Network Selection, lựa chọn kết nối mạng sẽ gán cho các máy truy cập từ xa, sau đó kích next

✓ Trong trang IP Address Asignment, lựa chọn Automaticlly hoặc From specified range of addresses cho việc gán các đị chỉ IP tới các máy truy cập từ xa

✓ Trong trang Managing Multiple Remote Acccess Servers cho phép lựa chọn cấu hình RADIUS, kích next

✓ Kích Finish để kết thúc.

Bước 2:

Thiết đặt tài khoản cho người dùng từ xa. Thiết lập một tài khoản có tên RemoteUser

✓ Đăng nhập với quyền Administrator

✓ Mở Active Directory Users and Computers từ menu Administrator Tools

✓ Kích chuột phải vào Users, chọn new và kích vào User

✓ Trong hộp thoại New Object-User, điền RemoteUser vào First name

✓ Trong hộp User logon name, gõ RemoteUser

✓ Thiết đặt Password cho tài khoản này, kích next sau đó kích Finish.

✓ Kích chuột phải vào RemoteUser sau đó kích Properties

✓ Trong trang Dial-In tab, kích Allow access, sau đó click OK

Thiết lập một Global group tên là RemoteGroup, sau đó thêm tài khoản người dùng vừa thiết lập vào nhóm này

✓ Kích chuột phải vào Users, chọn new sau đó kích Group

✓ Trong hộp thoại New Object-Group, mục Group name gõ vào RemoteGroup

✓ Trong mục Group scope kiểm tra Global đã được lựa chọn, trong mục Group type kiểm tra rằng Security đã được lựa chọn, sau đó kích OK

✓ Mở hộp thoại Properties của RemoteGroup

✓ Trong trang Member, kích Add

✓ Trong hộp thoại Select Users, Contacts, Computers, hoặc Group, Look in box, kiểm tra domain đã được hiển thị

✓ Trong danh sách các đối tượng, kích RemoteUser, kích Add sau đó kích OK

✓ Kích OK để đóng hộp thoại RemoteGroup Properties

Bước 3:

Kiểm tra cấu hình đã thiết lập ở bước trên bằng việc thực hiện một kết nối quay số tới máy chủ truy cập từ xa với tài khoản có tên là RemoteUser, kết nối được thiết lập sau đó đóng kết nối lại.

Bước 4:

Cấu hình cho phép tài khoản RemoteUser truy cập vào mạng được điều khiển truy cập bởi các chính sách truy cập từ xa (Remote access policy)

✓ Mở lại Active Directory Users and Computers từ menu Administrator Tools

✓ Mở hộp thoại Properties của tài khoản RemoteUser

✓ Trong trang Dial-in tab, kích Control access though Remote Policy sau đó kích OK, lư u ý rằng điều khiển vùng (Domain Controler) phải chạy ở chế độ Native.

✓ Thu nhỏ cửa sổ Active Directory Users and Computers

Bước 5:

Kiểm tra cấu hình đã thiết lập ở bước trên bằng việc thực hiện một kết nối quay số tới máy chủ truy cập từ xa với tài khoản có tên là RemoteUser. Thông báo lỗi xuất hiện, kết nối không được thiết lập.

Bước 6:

Sử dụng RRAS để thiết lập một chính sách mới đối với người dùng từ xa, tên chính sách này là Allow RemoteGroup Access cho phép người dùng trong nhóm RemoteGroup truy cập.

✓ Mở Routing and Remote Access từ menu Administrator Tools

✓ Mở rộng tên máy chủ đang cấu hình, kích chuột phải vào Remote Access Policy sau đó chọn New Remote Access Policy

✓ Trong trang Policy Name, gõ vào Allow RemoteGroup Access sau đó kích Next

✓ Trong trang Condition, kichs Add trong hộp thoại Select Attribute kích Windows-Groups sau đó kích Add

✓ Trong hộp thoại Groups kích Add

✓ Trong hộp thoại Select Groups, trong danh sách Look in, kích vào tên domain

✓ Trong hộp thoại Select Groups,dưới Name kích RemoteGroups kích Add sau đó kích OK

✓ Trong hộp thoại Groups kích OK

✓ Trong trang Condition kích Next

✓ Trong trang Permissions kích Grant remote access permission sau đó kích Next

✓ Trong trang User Profile kích Finish

✓ Trong trang Routing and Remote Access kích Remote Access Policies sau đó kích chuột phải Allow RemoteGroup access sau đó kích Move Up

Bước 7:

Kiểm tra cấu hình đã thiết lập ở bước trên bằng việc thực hiện một kết nối quay số tới máy chủ truy cập từ xa với tài khoản có tên là RemoteUser, kết nối được thiết lập sau đó đóng kết nối lại.

Bước 8:

Cấu hình để default policy được thi hành trước:

✓ Mở trang Routing and Remote Access, kích chuột phải RemoteGroup sau đó kích Move Down.

✓ Đóng cửa sổ Routing and Remote Access

Bước 9:

Kiểm tra cấu hình đã thiết lập ở bước trên bằng việc thực hiện một kết nối quay số tới máy chủ truy cập từ xa với tài khoản có tên là RemoteUser. Thông báo lỗi xuất hiện, kết nối không được thiết lập.

Bước 10:

Cấu hình cho phép truy cập sử dụng Properties của RemoteUser

✓ Mở lại Active Directory Users and Computers từ menu Administrator Tools

✓ Mở Properties của RemoteUser

✓ Trong trang Dial-in, kích Allow access sau đó kích OK

✓ Đóng Active Directory Users and Computers.

Bước 11:

Kiểm tra cấu hình đã thiết lập ở bước trên bằng việc thực hiện một kết nối quay số tới máy chủ truy cập từ xa với tài khoản có tên là RemoteUser, kết nối được thiết lập sau đó đóng kết nối lại

Bài 3

Cấu hình VPN server và thiết lập VPN Client, kiểm tra kết nối từ VPN Client tới VPN server

Bước 1:

Cấu hình cho kết nối VPN gọi vào

✓ Đăng nhập vào hệ thống với quyền Administrator

✓ Mở Routing and Remote Access từ menu Administrator Tools

✓ Kích chuột phải vào tên Server (Server là tên máy chủ đang cấu hình)

✓ Kịch bản thiết lập Routing and Remote Access xuất hiện, kích next

✓ Trong trang Network Selection, mục Name kiểm tra tên đã lựa chọn sau đó Click next

✓ Trong trang IP Address Assigment, kích From a specified range of addresses

✓ Trong trang Address Range Assignment, kích New

✓ Điền địa chỉ IP vào ô Start IP address và điền vào số địa chỉ vào ô Number of Address

✓ Kích OK, sau đó kích next

✓ Trong trang Managing Multiple Remote Access Servers, lựa chọn No, I don't want to set up this server to use RADIUS now, kích next sau đó kích Finish

✓ Kích OK để đóng hộp thoại Routing and Remote Access.

Cấu hình cho phép tài khoản Administrator truy cập vào mạng

✓ Mở Active Directory Users and Computers từ menu Administrator Tools.

✓ Mở rộng tên domain kích Users, kích đúp chuột vào Administrator

✓ Trong mục Dial-in, chọn Allow acces sau đó kích OK.

✓ Đóng của sổ Active Directory Users and Computers

Bước 2:

Cấu hình cho kết nối VPN gọi ra. Để kiểm tra dịch vụ truy cập từ xa đã làm việc phục vụ cho những người dùng từ xa, ta thiết lập một nối kết tới VPN server.

✓ Kích chuột phải vào My Network Places, sau đó kích Properties

✓ Trong của sổ Network Dialup Connections, kích đúp chuột vào Make new connection

✓ Trong trang Network Connection Type, kích Connect to a private network through the Internet, sau đó kích next

✓ Trong trang Destination Address page, gõ vào địa chỉ IP của máy cài đặt VPN server, sau đó kích next

✓ Trong trang Connection Availability, kích Only for my self, kích next sau đó kích Finish

✓ Khởi tạo kết nối tới VPN server

✓ Trong hộp thoại Connect Virtual Private Connection, kiểm tra tài khoản đăng nhập là Administrator và Password sau đó kích connect

✓ Kích OK để đóng thông báo Connnection Complete

✓ Đống của sổ Network Dialup Connections.

Sử dụng tiện ích Ipconfig để xác nhận rằng bạn đã thiết lập được một kết nối VPN và nhận được địa IP cho kết nối này lưu ý rằng đại chỉ IP cho kết nối VPN này là dãy địa chỉ tĩnh mà VPN server cấp phát

Đóng kết nối

✓ Kích đúp vào biểu tượng Connection trong khay hệ thống

✓ Trong hộp thoại Vitual Private Connection Status, kích disconnect

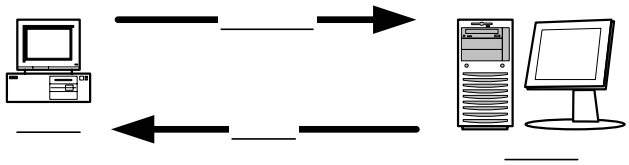
✓ Đóng tất cả các cửa sổ lại

Mục 2 : Dịch vụ Proxy - Giải pháp cho việc kết nối mạng dùng riêng ra Internet

I. Các khái niệm.

I.1. Mô hình client server và một số khả năng ứng dụng.

Mô hình chuẩn cho các ứng dụng trên mạng là mô hình client-server. Trong mô hình này máy tính đóng vai trò là một client là máy tính có nhu cầu cần phục vụ dịch vụ và máy tính đóng vai trò là một server là máy tính có thể đáp ứng được các yêu cầu về dịch vụ đó từ các client. Khái niệm client-server chỉ mang tính tương đối, điều này có nghĩa là một máy có thể lúc này đóng vai trò là client và lúc khác lại đóng vai trò là server. Nhìn chung, client là một máy tính cá nhân, còn các Server là các máy tính có cấu hình mạnh có chứa các cơ sở dữ liệu và các chương trình ứng dụng để phục vụ một dịch vụ nào đấy từ các yêu cầu của client (hình 6.1).



Hình 6.1

Cách thức hoạt động của mô hình client-server như sau: một tiến trình trên server khởi tạo luôn ở trạng thái chờ yêu cầu từ các tiến trình client tiến trình tại client được khởi tạo có thể trên cùng hệ thống hoặc trên các hệ thống khác được kết nối thông qua mạng, tiến trình client thường được khởi tạo bởi các lênh từ người dùng. Tiến trình client ra yêu cầu và gửi chúng qua mạng tới server để yêu cầu được phục vụ các dịch vụ. Tiến trình trên server thực hiện việc xác định yêu cầu hợp lệ từ client sau đó phục vụ và trả kết quả tới client và tiếp tục chờ đợi các yêu cầu khác. Một số kiểu dịch vụ mà server có thể cung

cấp như: dịch vụ về thời gian (trả yêu cầu thông tin về thời gian tới client), dịch vụ in ấn (phục vụ yêu cầu in tại client), dịch vụ file (gửi, nhận và các thao tác về file cho client), thi hành các lệnh từ client trên server...

Dịch vụ web là một dịch vụ cơ bản trên mạng Internet hoạt động theo mô hình client-server. Trình duyệt Web (Internet Explorer, Netscape...) trên các máy client sử dụng giao thức TCP/IP để đưa ra các yêu cầu HTTP tới máy server. Trình duyệt có thể đưa ra các yêu cầu một trang web cụ thể hay yêu cầu thông tin trong các cơ sở dữ liệu. Máy server sử dụng phần mềm của nó phân tích các yêu cầu từ các gói tin nhận được kiểm tra tính hợp lệ của client và thực hiện phục vụ các yêu cầu đó cụ thể là gửi trả lại client một trang web cụ thể hay các thông tin trên cơ sở dữ liệu dưới dạng một trang web. Server là nơi lưu trữ nội dung thông tin các website, phần mềm trên server cho phép server xác định được trang cần yêu cầu và gửi tới client. Cơ sở dữ liệu và các ứng dụng tương tự khác trên máy chủ được khai thác và kết nối qua các chương trình như CGI (Common Gateway Interface), khi các máy server nhận được yêu cầu về tra cứu trong cơ sở dữ liệu , nó chuyển yêu cầu tới server có chứa cơ sở dữ liệu hoặc ứng dụng để xử lý qua CGI.

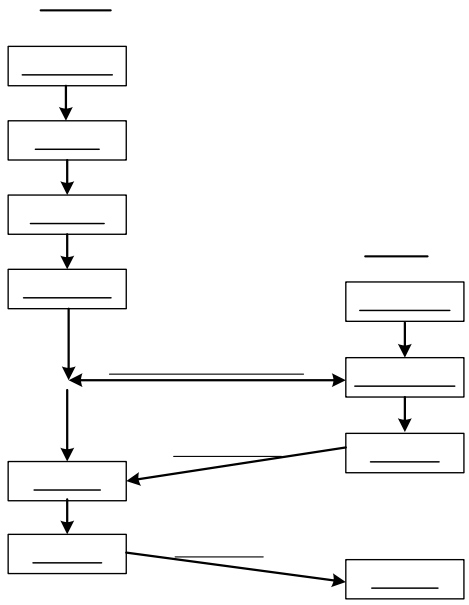
I.2. Socket.

Một kết nối được định nghĩa như là một liên kết truyền thông giữa các tiến trình, như vậy để xác định một kết nối cần phải xác định các thành phần sau: {Protocol, local-addr, local-process, remote-addr, remote-process}

Trong đó local-addr và remote-addr là địa chỉ của các máy địa phương và máy từ xa. local-process, remote-process để xác định vị trí tiến trình trên mỗi hệ thống. Chúng ta định nghĩa một nửa kết nối là {Protocol, local-addr, local-process} và {Protocol, remote-addr, remote-process} hay còn gọi là một socket.

Chúng ta đã biết để xác đinh một máy ta dựa vào địa chỉ IP của nó, nhưng trên một máy có vô số các tiến trình ứng dụng đang chạy, để xác định vị trí các tiến trình ứng dụng này người ta định danh cho mỗi tiến trình một số hiệu cổng, giao thức TCP sử dụng 16 bit cho việc định danh các cổng tiến trình và qui ước số hiệu cổng từ 1-1023 được sử dụng cho các tiến trình chuẩn (như FTP qui ước sử dụng cổng 21, dịch vụ WEB qui ước cổng 80, dịch vụ gửi thư

SMTP cổng 25...) số hiệu cổng từ 1024- 65535 dành cho các ứng dụng của người dùng. Như vậy một cổng kết hợp với một địa chỉ IP tạo thành một socket duy nhất trong liên mạng. Một kết nối TCP được cung cấp nhờ một liên kết logic giữa một cặp socket. Một socket có thể tham gia nhiều liên kết với các socket ở xa khác nhau. Trước khi truyền dữ liệu giữa hai trạm cần phải thiết lập một liên kết TCP giữa chúng và khi kết thúc phiên truyền dữ liệu thì liên kết đó sẽ được giải phóng.



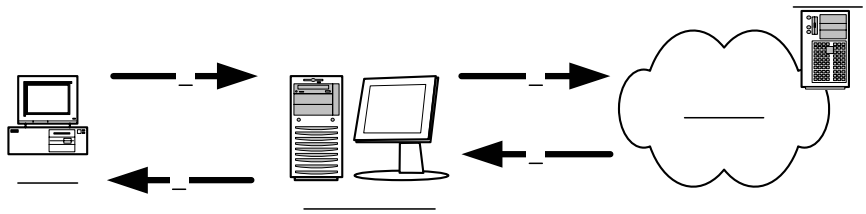
Hình 6.2

Quá trình thiết lập một socket với các lời gọi hệ thống được mô tả như sau: server thiết lập một socket với các thông số đặc tả các thủ tục truyền thông như (TCP, UDP, XNS...) và các kiểu truyền thông (SOCK_STREAM, SOCK_DGRAM...), sau đó liên kết tới socket này các thông số về địa chỉ như IP và các cổng TCP/UDP sau đó server ở chế độ chờ và chấp nhận kết nối đến từ client.

I.3. Phương thức hoạt động và đặc điểm của dịch vụ Proxy.

1. Phương thức hoạt động

Dịch vụ proxy được triển khai nhằm mục đích phục vụ các kết nối từ các máy tính trong mạng dùng riêng ra Internet. Khi đăng ký sử dụng dịch vụ internet tới nhà cung cấp dịch vụ, khách hàng sẽ được cấp hữu hạn số lượng địa chỉ IP từ nhà cung cấp, số lượng IP nhận được không đủ để cấp cho các máy tính trạm. Mặt khác với nhu cầu kết nối mạng dùng riêng ra Internet mà không muốn thay đổi lại cấu trúc mạng hiện tại đồng thời muốn gia tăng khả năng thi hành của mạng qua một kết nối Internet duy nhất và muốn kiểm soát tất cả các thông tin vào ra, muốn cấp quyền và ghi lại các thông tin truy cập của người sử dụng… Dịch vụ proxy đáp ứng được tất cả các yêu cầu trên. Hoạt động trên cơ sở mô hình client-server. Quá trình hoạt động của dịch vụ proxy theo các bước như sau:



Hình 6.3

1 Client yêu cầu một đối tượng trên mạng Internet

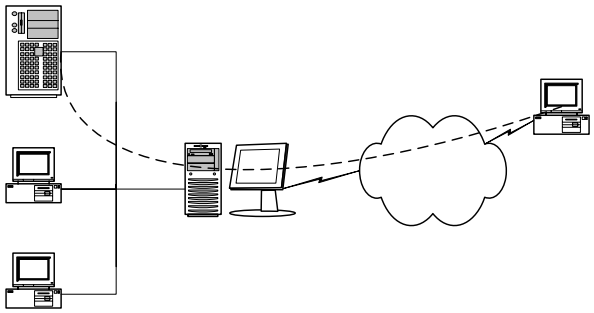
1 Proxy server tiếp nhận yêu cầu, kiểm tra tính hợp lệ cũng như thực hiện việc xác thực client nếu thỏa mãn proxy server gửi yêu cầu đối tượng này tới server trên Internet.

1 Server trên Internet gửi đối tượng yêu cầu về cho proxy server.

1 Proxy server gửi trả đối tượng về cho client

Ta có thể thiết lập proxy server để phục vụ cho nhiều dịch vụ như dịch vụ truyền file, dịch vụ web, dịch vụ thư điện tử…Mỗi một dịch vụ cần có một proxy server cụ thể để phục vụ các yêu cầu đặc thù của dịch vụ đó từ các client.

Proxy server còn có thể được cấu hình để cho phép quảng bá các server thuộc mạng trong ra ngoài Internet với mức độ an toàn cao. Ví dụ ta có thể thiết lập một web server thuộc mạng trong và thiết lập các qui tắc quảng bá web trên proxy server để cho phép quảng bá web server này ra ngoài Internet. Tất cả các yêu cầu truy cập web đến được chấp nhận bởi proxy server và proxy server sẽ thực hiện việc chuyển tiếp yêu cầu tới web server thuộc mạng trong (hình 6.4)



Hình 6.5

Các client được tổ chức trong một cấu trúc mạng gọi là mạng trong (Inside network) hay còn gọi là mạng dùng riêng. IANA (Internet Assigned Numbers Authority) đã dành riêng 3 khoảng địa chỉ IP tương ứng với 3 lớp mạng tiêu chuẩn cho các mạng dùng riêng đó là:

10.0.0.0 - 10.255.255.255 (lớp A)

172.16.0.0 - 172.31.255.255 (lớp B)

192.168.0.0 - 192.168.255.255 (lớp C)

Các địa chỉ này sử dụng cho các client trong mạng dùng riêng mà không được gán cho bất cứ máy chủ nào trên mạng Internet. Trong việc thiết kế và cấu hình mạng dùng riêng khuyến nghị nên sử dụng các khoảng địa chỉ IP này.

Khái niệm mạng ngoài (Outside network) là để chỉ vùng mà các server thuộc vào. Các địa chỉ sử dụng trên mạng này là các địa chỉ IP được đăng ký hợp lệ của nhà cung cấp dịch vụ Internet.

Proxy server sử dụng hai giao tiếp, giao tiếp mạng trong và giao tiếp ngoài. Giao tiếp trong điển hình là các cạc mạng sử dụng cho việc kết nối giữa proxy server với mạng dùng riêng và có địa chỉ được gán là địa chỉ thuộc mạng dùng riêng. Tất cả các thông tin giữa client thuộc mạng dùng riêng và proxy server được thực hiện thông qua giao tiếp này. Giao tiếp ngoài thường bằng các hình thức truy cập gián tiếp qua mạng điện thoại công cộng và qua cạc mạng bằng kết nối trực tiếp tới mạng ngoài. Giao tiếp ngoài được gán địa chỉ IP thuộc mạng ngoài được cung cấp hợp lệ bởi nhà cung cấp dịch vụ Internet.

2. Đặc điểm

Proxy Server kết nối mạng dùng riêng với mạng Internet toàn cầu và cũng cho phép các máy tính trên mạng internet có thể truy cập các tài nguyên trong mạng dùng riêng.

Proxy Server tăng cường khả năng kết nối ra Internet của các máy tính trong mạng dùng riêng bằng cách tập hợp các yêu cầu truy cập Internet từ các máy tính trong mạng và sau khi nhận được kết quả từ Internet sẽ trả lời lại cho máy có yêu cầu ban đầu.

Ngoài ra proxy server còn có khả năng bảo mật và kiểm soát truy cập Internet của các máy tính trong mạng dùng riêng. Cho phép thiết đặt các chính sách truy cập tới từng người dùng.

Proxy server lưu trữ tạm thời các kết quả đã được lấy từ Internet về nhằm trả lời cho các yêu cầu truy cập Internet với cùng địa chỉ. Việc lưu trữ này cho phép các yêu cầu truy cập Internet với cùng địa chỉ sẽ không cần phải lấy lại kết quả từ Internet, làm giảm thời gian truy cập Internet, tăng cường hoạt động của mạng và giảm tải trên đường kết nối Internet. Các công việc lưu trữ này gọi là quá trình cache.

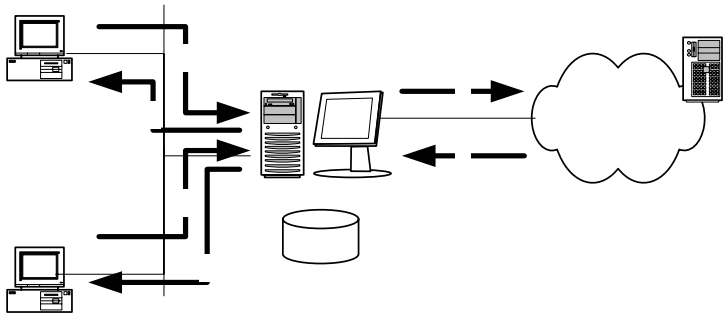
I.4. Cache và các phương thức cache.

Nhằm tăng cường khả năng truy cập Internet từ các máy tính trạm trong mạng sử dụng dịch vụ proxy ta sử dụng các phương thức cache. Dịch vụ proxy sử dụng cache để lưu trữ bản sao của các đối tượng đã được truy cập trước đó. Tất cả các đối tượng đều có thể được lưu trữ (như hình ảnh và các tệp tin), tuy nhiên một số đối tượng như yêu cầu xác thực (Authenticate) và sử dụng SSL (Secure Socket Layer) không được cache. Như vậy với các đối tượng đã được cache, khi một yêu cầu từ một máy tính trạm tới proxy server, proxy server thay vì kết nối tới địa chỉ mà máy tính trạm yêu cầu sẽ tìm kiếm trong cache các đối tượng thoã mãn và gửi trả kết quả về máy tính trạm. Như vậy cache cho phép cải thiện hiệu năng truy cập Internet của các máy trạm và làm giảm lưu lượng trên đường kết nối Internet. Vấn đề gặp phải khi sử dụng cache là khi các đối tượng được cache có sự thay đổi từ nguồn, các máy tính trạm yêu cầu một đối tượng tới proxy server, proxy server lấy đối tượng trong cache để phục vụ và như vậy thông tin chuyển tới các máy tính trạm là thông tin cũ so với nguồn, để giải quyết vấn đề này cần phải có các chính sách để cache các đối tượng đồng thời các đối tượng phải liên tục được cập nhật mới. Ví dụ: thông thường một địa chỉ WEB thì các đối tượng về hình ảnh ít có sự thay đổi còn nội dung text thường có sự thay đối do đó ta có thể thiết đặt chỉ cache những đối tượng hình ảnh, những đối tượng có nội dung text thì không cache, điều này không ảnh hưởng tới hiệu suất truy cập vì các tập tin về hình ảnh thường có kính thước rất lớn so với các đối tượng có nội dung text, việc cập nhật các đối tượng như thế nào phụ thuộc vào các phương thức cache mà ta sẽ trình bày dưới đây.

Proxy server thực thi cache cho các đối tượng được yêu cầu một cách có chu kỳ để tăng hiệu suất của mạng. Ta có thể thiết lập cache để đảm bảo rằng nó bao gồm những dữ liệu thường hay các client sử dụng nhất. Proxy server có thể sử dụng cho phép thông tin giữa mạng dùng riêng và Internet, việc thông tin có thể là client trong mạng truy cập Internet-trong trường hợp này proxy server thực hiện Forward caching, cũng có thể là client ngoài truy cập tói mạng trong (tới các server được quảng bá)-trong trường hợp này proxy server thực hiện reverse caching. Cả hai trường hợp đều có được từ khả năng của proxy server là lưu trữ thông tin (tạm thời) làm cho việc truyền thông thông tin được nhanh hơn, sau đây là các tính chất của cache proxy server:

- Phân cache: khi cài đặt một mảng các máy proxy server ta sẽ thiết lập được việc phân phối nội dung cache. Proxy server cho phép ghép nhiều hệ thống thành một cache logic duy nhất.
- Cache phân cấp: Khả năng phân phối cache còn có thể chuyên sâu hơn bằng cách cài đặt chế độ cache phân cấp liên kết một loạt các máy proxy server với nhau để client có thể truy cập tới gần chúng nhất.
- Cache định kỳ: sử dụng cache định kỳ nội dung download đối với các yêu cầu thường xuyên của các client
- Reverse cache: proxy server có thể cache các nội dung của các server quảng bá do đó tăng hiệu suất và khả năng truy cập, mọi đặc tính cache của proxy server đều có thể áp dụng cho nội dung trên các server quảng bá.

Proxy server có thể được triển khai như một Forward cache nhằm cung cấp tính năng cache cho các client mạng trong truy cập Internet. Proxy server duy trì bộ cache tập trung của các đối tượng Internet thường được yêu cầu có thể truy cập từ bất kỳ trình duyệt từ mày client. Các đối tượng phục vụ cho các yêu cầu từ các đĩa cache yêu cầu tác vụ xử lý nhỏ hơn đáng kế so với các đối tượng từ Internet, việc này tăng cường hiệu suất của trình duyệt trên client, giảm thời gian hồi đáp và giảm việc chiếm băng thông cho kết nối Internet. Hình vẽ sau mô tả proxy server xử lý các yêu cầu của người dùng ra sao (hình 6.6)



Hình 6.6

Hình trên mô tả quá trình các client trong mạng dùng riêng truy cập ra ngoài Internet nhưng tiến trình này cũng tương tự đối với các cache reverse (khi người dùng trên Internet truy cập vào các Server quảng bá) các bước bao gồm;

1 Client 1 yêu cầu một đối tượng trên mạng Internet

2 Proxy server kiểm tra xem đối tượng có trong cache hay không. Nếu đối tượng không có trong cache của proxy server thì proxy server gửi yêu cầu đối tượng tới server trên Internet.

3 Server trên Internet gửi đối tượng yêu cầu về cho proxy server .

4 proxy server gĩư bản copy của đối tượng trong cache của nó và trả đối tượng về cho client1

5 Client 2 gửi một yêu cầu về đối tượng tương tự

6 Proxy server gửicho client 2 đối tượng từ cache của nó chứ không phải từ Internet nữa.

Ta có thể triển khai dịch vụ proxy để quảng bá các server trong mạng dùng riêng ra ngoài Internet. Với các yêu cầu đến, proxy server có thể đòng vai trò như là một server bên ngoài, đáp ứng các yêu cầu của client từ các nội dung web trong cache của nó. Proxy server chuyển tiếp các yêu cầu cho server chỉ khi nào cache của nó không thể phục vụ yêu cầu đó (*Reverse cache).*

Lựa chọn các phương thức cache dựa trên các yếu tố: không gian ổ cứng sử dụng, đối tượng nào được cache và khi nào các đối tượng này sẽ được cập nhật. Về cơ bản ta có hai phương thức cache thụ động và chủ động.

Phương thức Cache thụ động (passive cache): Cache thụ động lưu trữ các đối tượng chỉ khi các máy tính trạm yêu cầu tới đối tượng. Khi một đối tượng được chuyển tới máy tính trạm, máy chủ Proxy xác định xem đối tượng này có thể cache hay không nếu có thể đối tượng sẽ được cache. Các đối tượng chỉ được cập nhật khi có nhu cầu. Đối tượng sẽ bị xoá khỏi cache dựa trên thời điểm gần nhất mà các máy tính trạm truy cập tới đối tượng. Phương thức này có lợi ích là sử dụng ít hơn bộ xử lý nhưng tốn nhiều không gian ổ đĩa hơn

Phương thức Cache chủ động (active cache): Cũng giống như phương thức cache thụ động, Cache chủ động lưu trữ các đối tượng khi các máy tính trạm ra yêu cầu tới một đối tượng máy chủ Proxy đáp ứng yêu cầu và lưu đối tượng này vào Cache. Phương thức này tự động cập nhật các đối tượng từ

Internet dựa vào: số lượng yêu cầu đối với các đối tượng, đối tượng thường xuyên thay đổi như thế nào. Phương thức này sẽ tự động cập nhật các đối tượng khi mà máy chủ Proxy đang phục vụ ở mức độ thấp và do đó không ảnh hưởng đến hiệu suất phục vụ các máy tính trạm. Đối tượng trong cache sẽ bị xoá dựa trên các thông tin header HTTP, URL.

II. Triển khai dịch vụ proxy

II.1. Các mô hình kết nối mạng

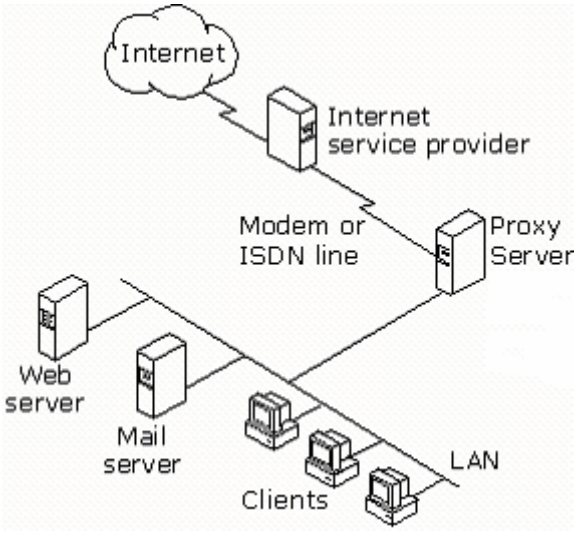
Đối tượng phục vụ của proxy server khá rộng, từ mạng văn phòng nhỏ, mạng văn phòng vừa tới mạng của các tập đoàn lớn. Với mỗi quy mô tổ chức sẽ có một cấu trúc mạng sử dụng proxy server cho phù hợp. Sau đây chúng ta sẽ xem xét một số mô hình cơ bản đối với mạng cỡ nhỏ, mạng cỡ trung bình và mạng tập đoàn lớn. Trong đó chúng ta sẽ đi sâu vào mô hình thứ nhất dành cho mạng văn phòng nhỏ bởi nó phù hợp quy mô tổ chức của các công ty vừa và nhỏ tại Việt nam.

Mô hình mạng văn phòng nhỏ

□□c tớnh c□a m□ng v□n phũng nh□ nh□ sau:

- Bao gồm một mạng LAN độc lập.
- Sử dụng giao thức IP.
- Kết nối Internet bằng đường thoại (qua mạng điện thoại công cộng bằng các hình thức quay dial-up hay sử dụng công nghệ ADSL) hoặc đường trực tiếp (Leased Line).
- ít hơn 250 máy tính trạm.

Mô hình kết nối mạng như hình vẽ (hình 6.7)



Hình 6.7

Theo mô hình này, với mỗi phương thức kết nối Internet Proxy server sử dụng 02 giao tiếp như sau:

- Kết nối Internet bằng đường thoại qua mạng PSTN:
- 01 giao tiếp với mạng nội bộ thông qua card mạng.
- 01 giao tiếp với Internet thông qua Modem.
- Kết nối Internet bằng đường trực tiếp (Leased Line)
- 01 giao tiếp với mạng nội bộ thông qua card mạng
- 01 giao tiếp với Internet thông qua card mạng khác. Lúc này bảng địa chỉ nội bộ (LAT-Local Address Table) được xây dựng dựa trên danh sách địa chỉ IP mạng nội bộ.

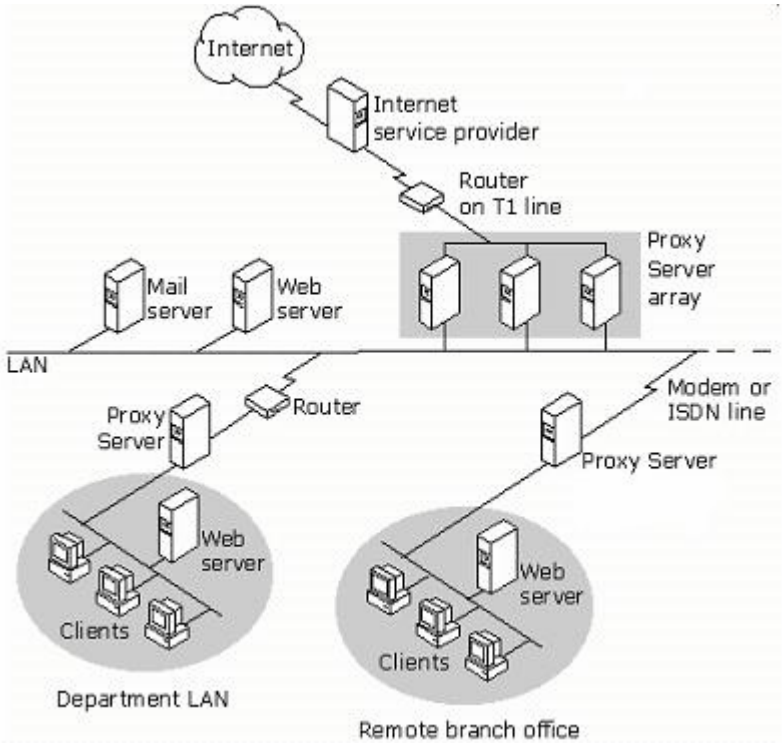
Mô hình kết nối mạng cỡ trung bình

Đặc trưng của mạng văn phòng cỡ trung bình như sau:

- Văn phòng trung tâm với một vài mạng LAN
- Mội văn phòng chi nhánh có một mạng LAN.
- Sử dụng giao thức IP.
- Kết nối bằng đường thoại từ văn phòng chi nhánh tới văn phòng trung tâm.
- Kết nối Internet từ văn phòng trung tâm tới ISP bằng đường thoại hoặc đường trực tiếp (Leased Line).

- ít hơn 2000 máy tính trạm

Mô hình mạng như hình 6.8. Theo mô hình này, văn phòng chi nhánh sử dụng một máy chủ Proxy cung cấp khả năng lưu trữ thông tin nội bộ (local caching), quản trị kết nối và kiểm soát truy cập tới văn phòng trung tâm. Tại văn phòng trung tâm, một số máy chủ Proxy hoạt động theo kiến trúc mảng (array) cung cấp khả năng bảo mật chung cho toàn mạng, cung cấp tính năng lưu trữ thông tin phân tán (distributed caching) và cung cấp kết nối ra Internet.



Hình 6.8

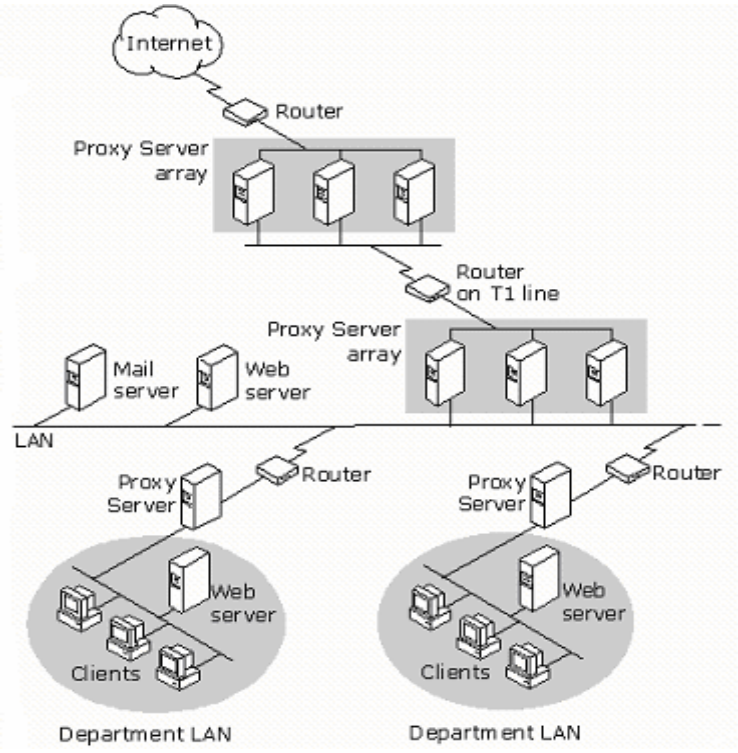
Mô hình kết nối mạng tập đoàn lớn

Mạng của các tập đoàn lớn có đặc trưng như sau:

- Văn phòng trung tâm có nhiều mạng LAN và có mạng trục LAN.
- Có vài văn phòng chi nhánh, mỗi văn phòng chi nhánh có một mạng LAN.
- Sử dụng giao thức mạng IP.
- Kết nối bằng đường thoại từ các văn phòng chi nhánh tới văn phòng trung tâm.

- Kết nối Internet từ văn phòng trung tâm tới ISP bằng đường đường trực tiếp (Leased Line).
- Có nhiều hơn 2000 máy tính trạm.

Mô hình mạng như hình 6.9. Theo mô hình này mạng tại các văn phòng chi nhánh cũng cấu hình tương tự như đối với mô hình các văn phòng cỡ trung bình. Các yêu cầu kết nối Internet không được đáp ứng bởi cache nội bộ tại máy chủ Proxy của văn phòng chi nhánh sẽ được chuyển tới một loạt máy chủ Proxy hoạt động theo kiến trúc mảng tại văn phòng trung tâm. Tại văn phòng trung tâm các máy chủ Proxy sử dụng 02 giao tiếp mạng (card mạng) trong đó 01 card mạng giao tiếp với mạng trục LAN và 01 card mạng giao tiếp với mạng LAN thành viên.



Hình 6.9

II.2. Thiết lập chính sách truy cập và các qui tắc

1..Các qui tắc.

Ta có thể thiết lập proxy server để đáp ứng các yêu cầu bảo mật và vận hành bằng cách thiết lập các qui tắc để xác định xem liệu người dùng, máy tính hoặc ứng dụng có được quyền truy cập và truy cập như thế nào tới máy tính

trong mạng hay trên Internet hay không. Thông thường một proxy server định nghĩa các loại qui tắc sau: Qui tắc về chính sách truy nhập, qui tắc về băng thông, qui tắc về chính sách quảng bá, các đặc tính lọc gói và qui tắc về định tuyến và chuỗi (chaining).

Khi một client trong mạng yêu cầu một đối tượng proxy server sẽ xử lý các qui tắc để xác định xem yêu cầu đó có được xác định chấp nhận hay không. Tương tự khi một client bên ngoài (Internet) yêu cầu một đối tượng từ một server trong mạng, proxy server cũng xử lý các bộ qui tắc xem yêu cầu có được cho phép không.

*Các qui tắc của chính sách truy nhập:*Ta có thể sử dụng proxy server để thiết lập chính sách bao gồm các qui tắc về giao thức, qui tắc về nội dung. Các qui tắc giao thức định nghĩa giao thức nào có thể sử dụng cho thông tin giữa mạng trong và Internet. Qui tắc giao thức sẽ được xử lý ở mức ứng dụng. Ví dụ một qui tắc giao thức có thể cho phép các Client sử dụng giao thức HTTP. Các qui tắc về nội dung qui định những nội dung nào trên các site nào mà client có thể truy nhập. Các qui tắc nội dung cùng được xử lý ở mức ứng dụng. Ví dụ một qui tắc về nội dung có thể cho phép các client truy nhập tới bất kỳ địa chỉ nào trên Internet.

Qui tắc băng thông: Qui tắc băng thông xác định kết nối nào nhận được quyền ưu tiên.Trong việc điều khiển băng thông thường thì proxy server không giới hạn độ rộng băng thông. Hơn nữa nó cho biết chất lượng dịch vụ (QoS) được cấp phát ưu tiên cho các kết nối mạng như thế nào. Thường thì bất kỳ kết nối nào không có qui tắc về băng thông kèm theo sẽ nhận được quyền ưu tiên ngầm định và bất kỳ kết nối nào có qui tắc băng thông đi kèm sẽ được sắp xếp với quyền ưu tiên hơn quyền ưu tiên ngầm định.

Các qui tắc về chính sách quảng bá: Ta có thể sử dụng proxy server để thiết lập chính sách quảng bá, bao gồm các qui tắc quảng bá server và qui tắc quảng bá web. Các qui tắc quảng bá server và web lọc tất cả các yêu cầu đến từ các yêu cầu của client ngoài mạng (internet) tới các server trong mạng. Các qui tắc quảng bá server và web sẽ đưa các yêu cầu đến cho các server thích hợp phía sau proxy server.

Đặc tính lọc gói: Đặc tính lọc gói của proxy server cho phép điều khiển luồng các gói IP đến và đi từ proxy server. Khi lọc gói hoạt động thì mọi gói trên giao diện bên ngoài đều bị rớt lại, trừ khi chúng được hoàn toàn cho phép

hoặc là một cách cố định bằng các bộ lọc gói IP, hoặc là một cách động bằng các chính sách truy cập hay quảng bá. Thậm chí nếu bạn không để lọc gói hoạt động thì truyền thông giữa mạng Internet và mạng cục bộ được cho phép khi nào bạn thiết lập rõ ràng các qui tắc cho phép truy cập. Trong hầu hết các trường hợp, việc mở các cổng động thường được sử dụng hơn. Do đó, người ta thường khuyến nghị rằng bạn nên thiết lập các qui tắc truy cập cho phép client trong mạng truy nhập vào Internet hoặc các qui tắc quảng bá cho phép client bên ngoài truy nhập vào các server bên trong. Đó là do các bộ lọc gói IP mở một cách cố định những chính sách truy nhập và qui tắc quảng bá lại mở các cổng kiểu động. Giả sử bạn muốn cấp quyền cho mọi người dùng trong mạng truy cập tới các site HTTP. Bạn không nên thiết lập một bộ lọc gói IP để mở cổng 80. Nên thiết lập qui tắc về site, nội dung và giao thức cần thiết để cho phép việc truy nhập này. Trong một vài trường hợp ta sẽ phải sử dụng các lọc gói IP, ví dụ nên thiết lập các lọc gói IP nếu ta muốn quảng bá các Server ra bên ngoài.

Qui tắc định tuyến và cấu hình chuỗi proxy (chaining): thường là qui tắc được áp dụng sau cùng để định tuyến các yêu cầu của client tới một server đã được chỉ định để phục vụ các yêu cầu đó.

2. Xử lý các yêu cầu đi

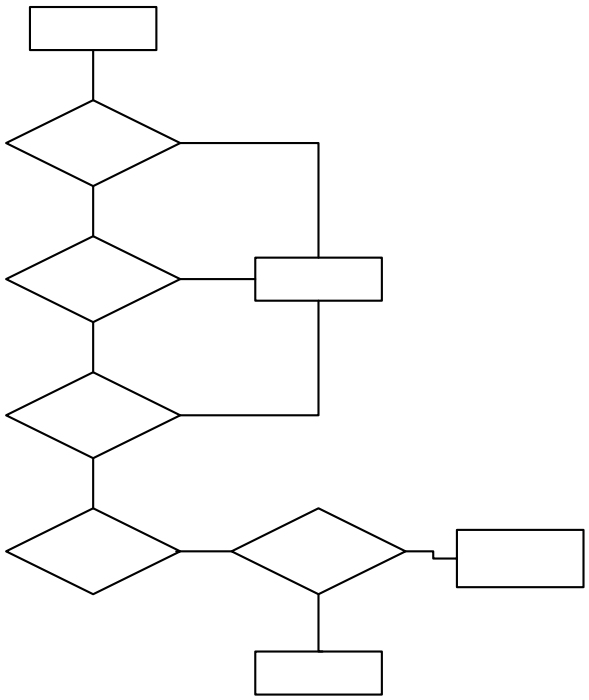
Một trong các chức năng chính của proxy server là khả năng kết nối mạng dùng riêng ra Internet trong khi bảo vệ mạng khỏi những nội dung có ác ý. Để thuận tiện cho việc kiểm soát kết nối này, ta dùng proxy server để tạo ra một chính sách truy cập cho phép các client truy cập tới các server trên Internet cụ thể, chính sách truy cập cùng với các qui tắc định tuyến quyết định các client truy cập Internet như thế nào.

Khi proxy server xử lý một yêu cầu đi, proxy server kiểm tra các qui tắc định tuyến các qui tắc về nội dung và các qui tắc giao thức để xem xét việc truy cập có được phép hay không. Yêu cầu chỉ được cho phép nếu cả quy tắc giao thức, qui tắc nội dung và site cho phép và nếu không một qui tắc nào từ chối yêu cầu.

Một vài qui tắc có thể được thiết lập để áp dụng cho các client cụ thể. Trong trường hợp này, các client có thể được chỉ định hoặc là bằng địa chỉ IP hoặc bằng user name. Proxy server xử lý các yêu cầu theo cách khác nhau phụ thuộc vào kiểu yêu cầu của client và việc thiết lập proxy server.Với một yêu

cầu, các qui tắc được xử lý theo thứ tự như sau: qui tắc giao thức, qui tắc nội dung, các lọc gói IP, qui tắc định tuyến hoặc cấu hình chuỗi proxy.

Hình dưới đưa ra quá trình xử lý đối với một yêu cầu đi (hình 6.10)



Hình 6.10

Trước tiên, proxy server kiểm tra các qui tắc giao thức, proxy server chấp nhận yêu cầu chỉ khi một qui tắc giao thức chấp nhận một cách cụ thể yêu cầu và không một qui tắc giao thức nào từ chối yêu cầu đó.

Sau đó, proxy server kiểm tra các qui tắc về nội dung. Proxy server chỉ chấp nhận yêu cầu nếu một qui tắc về nội dung chấp nhận yêu cầu và không có một qui tắc về nội dung nào từ chối nó.

Tiếp đến proxy server kiểm tra xem liệu có một bộ lọc gói IP nào được thiết lập để loại bỏ yêu cầu không để quyết định xem liệu yêu cầu có bị từ chối.

Cuối cùng, proxy server kiểm tra qui tắc định tuyến để quyết định xem yêu cầu được phục vụ như thế nào.

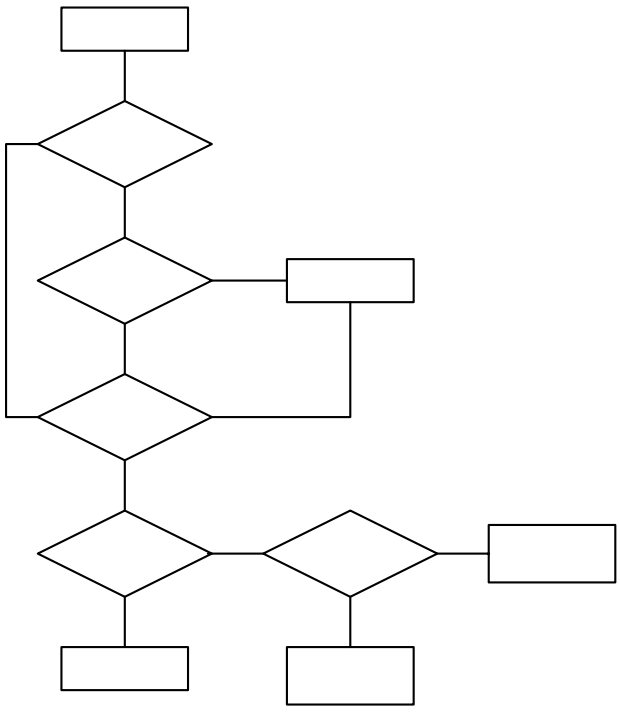
Giả sử cài đặt một proxy server trên một máy tính với hai giao tiếp kết nối, một kết nối với Internet và một kết nối vào mạng dùng riêng. Ta sẽ cho các

chỉ dẫn để cho phép tất cả client truy cập vào tất cả các site. Trong trường hợp này, chính sách truy nhập chỉ là các qui tắc như sau: một qui tắc về giao thức cho phép tất cả các client sử dụng mọi giao thức tại tất cả các thời điểm .Một qui tắc về nội dung cho phép tất cả mọi người truy cập tới mọi nội dung trên tất cả các site ở tất cả các thời điểm nào. Lưu ý rằng qui tắc này cho phép các client truy cập Internet nhưng không cho các client bên ngoài truy cập vào mạng của bạn.

3. Xử lý các yêu cầu đến

Proxy server có thể được thiết lập để các Server bên trong có thể truy cập an toàn đến từ các client ngoài. Ta có thể sử dụng proxy server để thiết lập một chính sách quảng bá an toàn cho các Server trong mạng. Chính sách quảng bá (bao gồm các bộ lọc gói IP, các qui tắc quảng bá Web, hoặc qui tắc quảng bá Server, cùng với các qui tắc định tuyến) sẽ quyết định các Server được quảng bá như thế nào.

Khi proxy server xử lý một yêu cầu xuất phát từ một client bên ngoài, nó sẽ kiểm tra các bộ lọc gói IP, các qui tắc quảng bá và các qui tắc định tuyến để quyết định xem liệu yêu cầu có được thực hiện hay không và Server trong nào sẽ thực hiện các yêu cầu đó.



Hình 6.11

Giả sử rằng đã cài đặt proxy server với hai giao tiếp kết nối, một kết nối tới Internet và một kết nối vào mạng dùng riêng. Nếu lọc gói hoạt động và sau đó, bộ lọc gói IP từ chối yêu cầu thì yêu cầu sẽ bị từ chối. Nếu các qui tắc quảng bá web từ chối yêu cầu thì yêu cầu cũng bị loại bỏ. Nếu một qui tắc định tuyến được thiết lập yêu cầu được định tuyến tới một Server upstream hoặc một site chủ kế phiên thì Server được xác định đó sẽ xử lý yêu cầu. Nếu một qui tắc định tuyến chỉ ra rằng các yêu cầu được định tuyến tới một Server cụ thể thì web Server trong sẽ trả về đối tượng.

II.3. Proxy client và các phương thức nhận thực

Chính sách truy nhập và các qui tắc quảng bá của Proxy server có thể được thiết lập để cho phép hoặc từ chối một nhóm máy tính hay một nhóm các người dùng truy nhập tới một server nào đó. Nếu qui tắc được áp dụng riêng với các người dùng, Proxy server sẽ kiểm tra các đặc tính yêu cầu để quyết định người dùng được nhận thực như thế nào.

Ta có thể thiết lập các thông số cho các yêu cầu thông tin đi và đến để người dùng phải được proxy server nhận thực trước khi xử lý các qui tắc. Việc này đảm bảo rằng các yêu cầu chỉ được phép nếu người dùng đưa ra các yêu cầu đã được xác thực. Bạn cũng có thể thiết lập các phương pháp nhận thực được sử dụng và có thể thiết lập các phương pháp nhận thực cho các yêu cầu đi và yêu cầu đến khác nhau. Về cơ bản một Proxy server thường hỗ trợ các phương pháp nhận thực sau đây: phương thức nhận thực cơ bản., nhận thực Digest, nhận thực tích hợp Microsoft windows, chứng thực client và chứng thực server.

Đảm bảo rằng các chương trình proxy client phải hỗ trợ một trong các phương pháp nhận thực mà proxy server đã đưa ra. Trình duyệt IE 5 trở lên hỗ trợ hầu hết các phương pháp nhận thực, một vài trình duyệt khác có thể chỉ hỗ trợ phương pháp nhận thực cơ bản. Đảm bảo rằng các trình duyệt client có thể hỗ trợ ít nhất một trong số các phương pháp nhận thực mà Proxy server hỗ trợ.

1. Phương pháp nhận thực cơ bản.

Phương pháp nhận thực này gửi và nhận các thông tin về người dùng là các ký tự text dễ dàng đọc được. Thông thường thì các thông tin về user name và password sẽ được mã hoá thì trong phương pháp này không có sự mã hoá nào được sử dụng. Tiến trình nhận thực được mô tả như sau, proxy client nhắc người dùng đưa vào username và password sau đó thông tin này được client gửi cho proxy server. Cuối cùng username và password được kiểm tra như là một tài khoản trên proxy server.

2. Phương pháp nhận thực Digest.

Phương pháp này có tính chất tương tự như phương pháp nhận thực cơ bản nhưng khác ở việc chuyển các thông tin nhận thực. Các thông tin nhận thực qua một tiến trình xử lý một chiều thường được biết với cái tên là "hashing". Kết quả của tiến trình này gọi là hash hay message digest và không thể giải mã chúng. Thông tin gốc không thể phục hồi từ hash. Các thông tin được bổ sung vào password trước khi hash nên không ai có thể bắt được password và sử dụng chúng để giả danh người dùng thực. Các giá trị được thêm vào để giúp nhận dạng người dùng. Một tem thời gian cũng được thêm vào để ngăn cản người dùng sử dụng một password sau khi nó đã bị huỷ. Đây là một ưu điểm rõ ràng so với phương pháp nhận thực cơ bản bởi vì người dùng bất hợp pháp không thể chặn bắt được password.

3. Phương pháp nhận thực tích hợp.

Phương pháp này được sử dụng tích hợp trong các sản phẩm của Microsoft. Đây cũng là phương pháp chuẩn của việc nhận thực bởi vì username và password không được gửi qua mạng. Phương pháp này sử dụng hoặc giao thức nhận thực V5 Kerberos hoặc giao thức nhận thực challenge/response của nó.

4. Chứng thực client và chứng thực server

Ta có thể sử dụng các đặc tính của SSL để nhận thực. Chứng thực được sử dụng theo hai cách khi một client yêu cầu một đối tượng từ server: server nhận thực chính nó bằng cách gửi đi một chứng thực server cho client. Server yêu cầu client nhận thực chính nó (Trong trường hợp này client phải đưa ra một chứng thực client phù hợp tới server).

SSL nhận thực bằng cách kiểm tra nội dung của một chứng thực số được mã hoá do proxy client đệ trình lên trong quá trình đăng nhập (Các người dùng

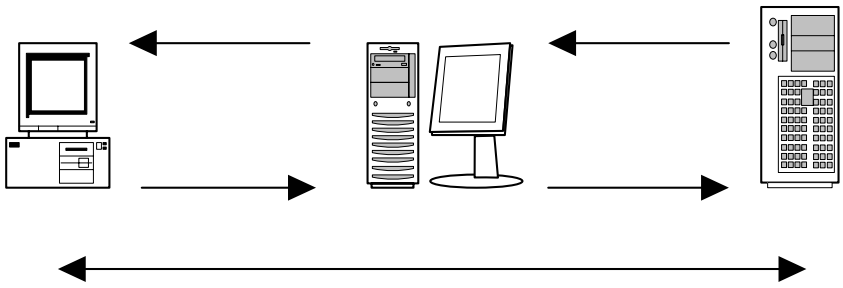
có thể có được các chứng thực số từ một tổ chức ngoài có độ tin tưởng cao). Các chứng thực về server bao gồm các thông tin nhận biết về server. Các chứng thực về client thường gồm các thông tin nhận biết về người dùng và tổ chức đưa ra chứng thực đó

Chứng thực client: Nếu chứng thực client được lựa chọn là phương thức xác thực thì proxy server yêu cầu client gửi chứng thực đến *trước* khi yêu cầu một đối tượng. Proxy server nhận yêu cầu và gửi một chứng thực cho client. Client nhận chứng thực này và kiểm tra xem có thực là thuộc về proxy server . Client gửi yêu cầu của nó cho proxy server, tuy nhiên proxy server yêu cầu một chứng thực từ client mà đã được đưa ra trước đó. Proxy server kiểm tra xem chứng thực có thực sự thuộcc về client được phép truy cập không.

Chứng thực server: Khi một client yêu cầu một đối tượng SSL từ một server, client yêu cầu server phải nhận thực chính nó. Nếu proxy server kết thúc một kết nối SSL thì sau đó proxy server sẽ phải nhận thực chính nó cho client. Ta phải thiết lập và chỉ định các chứng thực về phía server để sử dụng khi nhận thực server cho client

5. Nhận thực pass-though

Nhận thực pass-though chỉ đến khả năng của proxy server chuyển thông tin nhận thực của client cho server đích. Proxy server hỗ trợ nhận thực cho cả các yêu cầu đi và đến. Hình vẽ sau mô tả trường hợp nhận thực pass-though.



Hình 6.12

Client gửi yêu cầu lấy một đối tượng trên một web server cho proxy server. Proxy server chuyển yêu cầu này cho web server, bắt đầu từ đây việc nhận thực qua các bước sau:

1 Webserver nhận được yêu cầu lấy đối tượng và đáp lại rằng client cần phải nhận thực. Web server cũng chỉ ra các kiểu nhận thực được hỗ trợ.

2 Proxy server chuyển yêu cầu nhận thực cho client

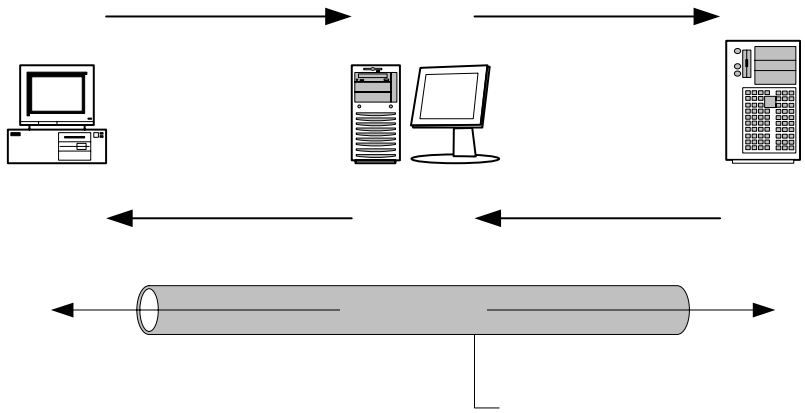
3 Client tiếp nhận yêu cầu và trả các thông tin nhận thực cho proxy server

4 Proxy server chuyển lại thông tin đó cho web server

5 Từ lúc này client liên lạc trực tiếp với web server

6. SSL Tunneling.

Với đường hầm SSL, một client có thể thiết lập một đường hầm qua proxy server trực tiếp tới server yeu cầu với các đối tượng yêu cầu là HTTPS. Bất cứ khi nào client yêu cầu một đối tượng HTTPS qua proxy server nó sử dụng đường hầm SSL. Đường hầm SSL làm việc bởi sự ngầm định các yêu cầu đi tới các cổng 443 và 563.



Hình 6.13

Tiến trình tạo đường hầm SSL được mô tả như sau:

1 Khi client yêu cầu một đối tượng HTTPS từ một web server trên Internet, proxy server gửi một yêu cầu kết nối https://*URL_name*

2 Yêu cầu tiếp theo được gửi tới cổng 8080 trên máy proxy server CONNECT *URL_name*:443 HTTP/1.1

3 Proxy server kết nối tới Web server trên cổng 443

4 Khi một kết nối TCP được thiết lập, proxy server trả lại kết nối đã được thiết lập HTTP/1.0 200

5 Từ đây, client thông tin trực tiếp với Web server bên ngoài

7. SSL bridging.

SSL bridging đề cập đến khả năng của proxy server trong việc mã hóa hoặc giải mã các yêu cầu của client và chuyển các yêu cầu này tới server đích. Ví dụ, trong trường hợp quảng bá (hoặc reverse proxy), proxy server có thể phục vụ một yêu cầu SSL của client bằng cách chấm dứt kết nối SSL với client và mở lại một kết nối mới với web server. SSL bridging được sử dụng khi proxy server kết thúc hoặc khởi tạo một kết nối SSL.

Khi một client yêu cầu một đối tượng HTTP. Proxy server mã hóa yêu cầu và chuyển tiếp nó cho web server. Web server trả về đối tượng đã mã hóa cho proxy server. Sau đó proxy server giải mã đối tượng và gửi lại cho client. Nói một cách khác các yêu cầu HTTP được chuyển tiếp như các yêu cầu SSL.

Khi client yêu cầu một đối tượng SSL. Proxy server giải mã yêu cầu, sau đó mã hóa lại một lần nữa và chuyển tiếp nó tới Web server. Web server trả về đối tượng mã hóa cho proxy server. Proxy server giải mã đối tượng và sau đó gửi nó cho client. Nói một cách khác các yêu cầu SSL được chuyển tiếp như là các yêu cầu SSL.

Khi client yêu cầu một đối tượng SSL. Proxy server giải mã yêu cầu và chuyển tiếp nó cho web server. Web server trả về đối tượng HTTP cho proxy server. Proxy server mã hóa đối tượng và chuyển nó cho client. Nói cách khác các yêu cầu SSL được chuyển tiếp như các yêu cầu HTTP.

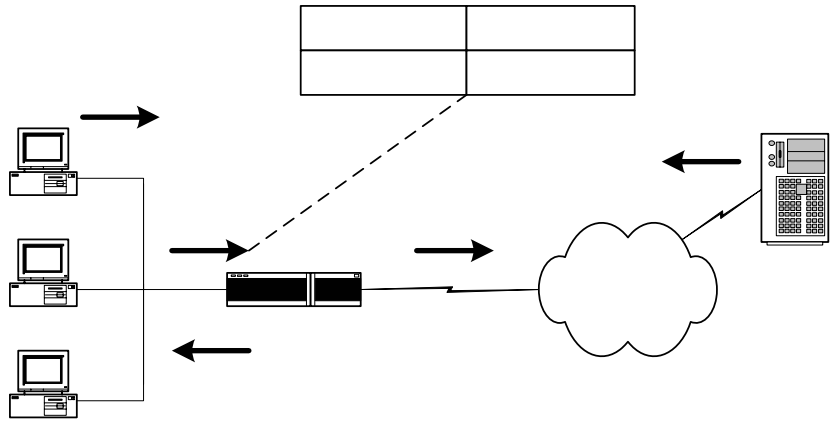
SSL bridging có thể được thiết lập cho các yêu cầu đi và đến. Tuy nhiên với các yêu cầu đi client phải hỗ trợ truyền thông bảo mật với proxy server.

II.4. NAT và proxy server

Khái niệm NAT (Network Addresss Tranlation).

NAT là một giao thức cho ta khả năng bản đồ hóa một một vùng địa chỉ IP sử dụng trong mạng dùng riêng ra mạng ngoài và ngược lại. NAT thường

được thiết lập trên các bộ định tuyến là ranh giới giữa mạng dùng riêng và mạng ngoài (ví dụ như mạng công cộng Internet). NAT chuyển đổi các địa chỉ IP trên mạng dùng riêng thành các địa chỉ IP được đăng ký hợp lệ trước khi chuyển các gói từ mạng dùng riêng tới Internet hoặc tới mạng ngoài khác. Trong phần này chúng ta sẽ chỉ tìm hiểu sự vận hành của NAT khi NAT được thiết lập để cung cấp các chức năng chuyển đổi các địa chỉ mạng dùng riêng trong việc phục vụ cho việc kết nối truy cập ra mạng ngoài như thế nào. Để làm việc này, NAT dùng tiến trình các bước theo hình vẽ dưới đây.



Hình 6.14

1. Người dùng tại máy 10.1.1.25 muốn mở một kết nối ra ngoài tới server 203.162.0.12

2. Khi gói dữ liệu đầu tiên tới NAT router, NAT router thực hiện việc kiểm tra trong bảng NAT. Nếu sự chuyển đổi địa chỉ đã có trong bảng, NAT router thực hiện bước thứ 3. Nếu không có sự chuyển đổi nào được tìm thấy, NAT router xác định rằng địa chỉ 10.1.1.25 phải được chuyển đổi. NAT router xác định một địa chỉ mới và cấu hình một chuyển đổi đối với địa chỉ 10.1.1.25 tới địa chỉ hợp lệ ngoài mạng (Internet) từ dãy địa chỉ động đã được định nghĩa từ trước ví dụ 203.162.94.163.

3. NAT router thay thế địa chỉ 10.1.1.25 bằng địa chỉ 203.162.94.163 sau đó gói được chuyển tiếp tới đích.

4. Server 203.162.0.12 trên Internet nhận gói và phúc đáp trở lại NAT router với địa chỉ 203.162.94.163.

5. Khi NAT router nhận được gói phúc đáp từ Server với địa chỉ đích đến là 203.162.94.163, nó thực hiện việc tìm kiếm trong bảng NAT. Bảng NAT chỉ ra rằng địa chỉ mạng trong 10.1.1.25 (tương ứng được ánh xạ tới địa chỉ 203.162.94.163 ở mạng ngoài) sẽ nhận được gói tin này. NAT router thực hiện việc chuyển đổi địa chỉ đích trong gói tin là 10.1.1.25 và chuyển gói tin này tới đích (10.1.1.25). Máy 10.1.1.25 nhận gói và tiếp tục thực hiện với các gói tiếp theo với các bước tuần tự như trên.

Trong trường hợp muốn sử dụng một địa chỉ mạng ngoài cho nhiều địa chỉ mạng trong. NAT router sẽ duy trì các thông tin thủ tục mức cao hơn trong bảng NAT đối với các số hiệu cổng TCP và UDP để chuyển đổi địa chỉ mạng ngoài trở lại chính xác tới các địa chỉ mạng trong.

Như vậy NAT cho phép các client trong mạng dùng riêng với việc sử dụng các địa chỉ IP dùng riêng truy cập vào một mạng bên ngoài như mạng Internet.Cung cấp kết nối ra ngoài Internet trong các mạng không được cung cấp đủ các địa chỉ Internet có đăng ký. Thích hợp cho việc chuyển đổi địa chỉ trong hai mạng Intranet ghép nối nhau. Chuyển đổi các địa chỉ IP nội tại được ISP cũ phân bố thành các địa chỉ được phân bố bởi ISP mới mà không cần thiết lập thủ công các giao diện mạng cục bộ.

NAT có thể được sử dụng một cách cố định hoặc động. Chuyển đổi cố định xảy ra khi ta thiết lập thủ công một bảng địa chỉ cùng các địa chỉ IP. Một địa chỉ cụ thể ở bên trong mạng sử dụng một địa chỉ IP (được thiết lập thủ công bởi người quản trị mạng) để truy cập ra mạng ngoài. Các thiết lập động cho phép người quản trị thiết lập một hoặc nhiều các nhóm địa chỉ IP dùng chung đã đăng ký. Những địa chỉ trong nhóm này có thể được sử dụng bởi các client trên mạng dùng riêng để truy cập ra mạng ngoài. Việc này cho phép nhiều client trong mạng sử dụng cùng một địa chỉ IP.

NAT cũng có một số nhược điểm như làm tăng độ trễ của các gói tin trên mạng. NAT phải xử lý mọi gói để quyết định xem liệu các header được thay đổi như thế nào. Không phải bất kỳ ứng dụng nào cũng có thể chạy được với NAT. NAT hỗ trợ nhiều giao thức truyền thông và cũng rất nhiều giao thức không được hỗ trợ. Các giao thức được NAT hỗ trợ như:TCP,UDP, HTTP,

TFTP, FTP…Các thông tin không được hỗ trợ như: IP multicast, BOOTP, DNS zone transfer, SNMP…

Proxy và NAT

Như đã phân tích cả dịch vụ NAT và dịch vụ Proxy đều có thể là một giải pháp để kết nối các mạng dùng riêng ra Internet, tuy nhiên mỗi dịch vụ lại có các ưu điểm và nhược điểm riêng.

Dịch vụ proxy cho khả năng thi hành và tốc độ cao hơn nhờ tính năng cache, tuy nhiên sử dụng cache có thể đưa ra các đối tượng đã quá hạn cần phải có các chính sách cache hợp lý đề đảm bảo tính thời sự của các đối tượng. Chính vì sử dụng cache nên giảm tải trên kết nối truy cập Internet. NAT không có tính năng cache.

Dịch vụ proxy phải được triển khai đối với từng ứng dụng, trong khi NAT là một tiến trình trong suốt hơn. Hầu hết các ứng dụng đều có thể làm việc được với NAT. NAT dễ cài đặt và vận hành, dường như không phải làm gì nhiều với NAT sau khi cài đặt.

Tại các client, đối với NAT không phải thiết đặt gì nhiều ngoài việc cấu hình tham số default gateway tới Server NAT. Trong khi sử dụng dịch vụ proxy, cần phải có các chương trình proxy client để làm việc với proxy server.

Dịch vụ proxy cho phép thiết đặt các chính sách tới người dùng, với NAT việc sử dụng các tính năng này có hạn chế rất nhiều, có thể nói sử dụng dịch vụ proxy là cách truy cập an toàn nhất để kết nối mạng dùng riêng ra ngoài Internet.

III. Các tính năng của phần mềm Microsoft ISA server 2000

III.1. Các phiên bản.

ISA server bao gồm hai phiên bản được thiết kế để phù hợp với từng nhu cầu của người sử dụng đó là ISA server Standard và ISA server Enterprise.

- ISA server Standard cung cấp khả năng an toàn firewall và khả năng web cache cho một môi trường kinh doanh, các nhóm làm việc hay văn phòng nhỏ. ISA server Standard cung cấp việc bảo mật chặt chẽ, truy cập web nhanh, quản lý trực quan, giá cả hợplý và khả năng thi hành cao.

- ISA server Enterprise được thiết kế đẻ đáp ứng các nhu cầu về hiệu suất, quản trị và cân bằng trong các môi trường Internet tốc độ cao với sự quản lý server tập trung, chính sách truy cập đa mức và các khả năng chống lỗi cao. ISA server Enterprisecung cấp sự bảo mật, truy cập Internet nhanh cho các môi trường có sự đòi hỏi khắt khe.

III.2. Lợi ích

ISA server là một trong các phần mềm máy chủ thuộc dòng .NET Enterprise Server. Các sản phẩm thuộc dòng .NET Enterprise Server là các server ứng dụng toàn diện của Microsoft trong việc xây dựng, triển khai, quản lý, tích hợp, các giải pháp dựa trên web và các dịch vụ. ISA server mang lại một số các lợi ích cho các tổ chức cần kết nối Internet nhanh, bảo mật, dễ quản lý.

1. Truy cập Web nhanh với cache hiệu suất cao.

- Người dùng có thể truy cập web nhanh hơn bằng các đối tượng tại chỗ trong cache so với việc phải kết nối vào Internet lúc nào cũng tiềm tàng nguy cơ tắc nghẽn.

- Giảm giá thành băng thông nhờ giảm lưu lượng từ Internet

- Phân tán nội dung của các Web server và các ứng dụng thương mại điện tử một cách hiệu quả, đáp ứng được nhu cầu khách hàng trên toàn cầu (khả năng phân phối nội dung web chỉ có trên phiên bản ISA server Enterprise)

2. Kết nối Internet an toàn nhờ Firewall nhiều lớp.

- Bảo vệ mạng trước các truy nhập bất hợp pháp bằng cách giám sát lưu lượng mạng tại nhiều lớp

- Bảo vệ các máy chủ web, email và các ứng dụng khác khỏi sự tấn công từ bên ngoài bằng việc sử dụng web và server quảng bá để xử lý một cách an toàn các yêu cầu đến

- Lọc lưu lượng mạng đi và đến để đảm bảo an toàn.

- Cung cấp truy cập an toan cho người dùng hợp lệ từ Internet tới mạng nội tại nhờ sử dụng mạng riêng ảo (VPN)

3. Quản lý thống nhất với sự quản trị tích hợp.

- Điều khiển truy cập tập trung để đảm bảo tính an toàn và phát huy hiệu lực của các chính sách vận hành.

- Tăng hiệu suất nhờ việc giới hạn truy cập sử dụng Internet đối với một số các ứng dụng và đích đến.

- Cấp phát băng thông để phù hợp với các ưu tiên.

- Cung cấp các công cụ giám sát và các báo cáo để chỉ ra kết nối Internet được sử dụng như thế nào.

- Tự động hóa các nhiệm vụ bằng việc sử dụng các script

4. Khả năng mở rộng.

- Chú trọng tới an toàn và thi hành nhờ sử dụng ISA server Softwware Development Kit (SDK) với sự phát triển các thành phần bổ sung.

- Chức năng quản lý và an toàn mở rộng cho các nhà sản xuất thứ ba

- Tự động các tác vụ quản trị với các đối tượng Script COM (Component Object Model)

III.3. Các chế độ cài đặt

ISA server có thể được cài đặt ở ba chế độ khác nhau: Cache, Firewall và Integrated

1. Chế độ cache: Trong chế độ này ta có thể nâng cao hiệu suất truy cập và tiết kiệm băng thông bằng cách lưu trữ các đối tượng web thường được truy xuất từ người dùng. Ta cũng có thể định tuyến các yêu cầu của người dùng tới cache server khác đang lưu giữ các đối tượng đó.

2. Chế độ firewall: Trong chế độ này cho phép ta đảm bảo an toàn lưu lượng mạng nhờ sự thiết lập các qui tắc điều khiển thông tin giữa mạng trong và Internet. Ta cũng có thể quảng bá các server trong để chia sẻ dữ liệu trên mạng với các đối tác và khách hàng.

3. Chế độ tích hợp: Trong chế độ này ta có thể tích hợp các dịch vụ cache và firewall trên một server.

III.4. Các tính năng của mỗi chế độ cài đặt

Các tính năng khác nhau tùy thuộc vào chế độ mà ta cài đặt, bảng sau liệt kê các tính năng có trong chế độ firewall và cache, chế độ tích hợp có tất cả các tính năng đó

Tính năng	Mô tả	Chế độ firewall	Chế độ cache
Chính sách truy cập	Định nghĩa các giao thức và nội dung Internet mà người dùng có thể sử dụng và truy cập	Có	Chỉ có HTTP và FTP
Cache	Lưu trữ định kỳ các đối tượng web vào RAM và đĩa cứng của ISA server	Không	Có
VPN	Mở rộng mạng riêng nhờ sử dụng các đường liên kết qua các mạng được chia sẻ hay mạng công cộng như Internet	Có	Không
Lọc gói	Điều khiển dòng gói IP đi và đến	Có	Không
Lọc ứng dụng	Thực thi các tác vụ của hệ thống hoặc của giao thức chỉ định, như là nhận thực để cung cấp một lớp bảo vệ bổ sung cho dịch vụ firewall	Có	Không
Quảng bá Web	Quảng bá web trong mạng để người dùng trong mạng có thể truy cập	Không	Có
Quảng bá Server	Cho phép các Server ứng dụng có	Có	Không

	thể phục vụ các client bên ngoài		
Giám sát thời gian thực	Cho phép giám sát tập trung các hoạt động của ISA server bao gồm các cảnh báo, giám sát các phiên làm việc và các dịch vụ	Có	Có
Cảnh báo	Báo cho ta biết các sự kiện đặc biệt xuất hiện và thực thi các hoạt động phù hợp	Có	Có
Báo cáo	Tổng hợp và phân tích hoạt động trên một hoặc nhiều máy ISA server	Có	Có

IV. Bài tập thực hành.

Yêu cầu về Phòng học lý thuyết: Số lượng máy tính theo số lượng học viên trong lớp học đảm bảo mỗi học viên có một máy tính, cấu hình máy tối thiểu như sau (PIII 800 MHZ, 256 MB RAM, HDD 1GB,FDD, CDROM 52 x). Máy tính đã cài đặt Windows 2000 advance server. Các máy tính đã được nối mạng chạy giao thức TCP/IP.

Thiết bị thực hành: Đĩa cài phần mềm Windows 2000 Advance Server, đĩa cài phần mềm ISA Server 2000. Mỗi máy tính có 01 Modem V.90 và 01 đường điện thoại. 01 account truy cập internet

Bài 1:

Các bước cài đặt cơ bản phần mềm ISA server 2000.

Bước 1:

Các bước cài đặt cơ bản.

- ✓ Đăng nhập vào hệ thống với quyền Administrator

✓ Đưa đĩa cài đặt Microsoft Internet Security and Acceleration Server 2000 Enterprise Edition vào ổ CD-ROM.

✓ Cửa sổ Microsoft ISA Server Setup mở ra. Nếu cửa sổ này không tự động xuất hiện, sử dụngWindows Explorer để chạy x:\ISAAutorun.exe (với x là tên ổ đĩa CD-ROM).

✓ Trong cửa sổ Microsoft ISA Server Setup, kích Install ISA Server.

✓ Trong hộp thoại Microsoft ISA Server (Enterprise Edition) Setup kích Continue.

✓ Vào CD Key sau đó kích OK hai lần.

✓ Trong hộp thoại Microsoft ISA Server Setup kích I Agree.

✓ Trong hộp thoại Microsoft ISA Server (Enterprise Edition) Setup kích Custom Installation.

✓ Trong hộp thoại Microsoft ISA Server (Enterprise Edition) – Custom Installation kích Add-in services sau đó kích Change Option.

✓ Trong hộp thoại Microsoft ISA Server (Enterprise Edition) – Add-in services kiểm tra lựa chọn Install H.323 Gatekeeper Service đã được chọn, chọn Message Screener sau đó kích OK.

✓ Trong hộp thoại Microsoft ISA Server (Enterprise Edition) – CustomInstallation kích Administration tools sau đó kích Change Option.

✓ Trong hộp thoại Microsoft ISA Server (Enterprise Edition) – Administration tools, kiểm tra lựa chọn ISA Management đã được chọn, chọn H.323 Gatekeeper Administration Tools sau đó kíchOK.

✓ Trong hộp thoại Microsoft ISA Server (Enterprise Edition) – Custom Installation kích Continue. Hộp thoại Microsoft Internet Security and Acceleration Server Setup xuất hiện, lưu ý bạn rằng máy tính không thể tham gia vào array. Bạn sẽ cấu hình máy tính này là một stand-alone server.

✓ Kích Yes để cấu hình máy tính này là một stand-alone server.

✓ Trong hộp thoại Microsoft ISA Server Setup đọc mô tả các mode cài đặt đảm bảo rằng mode Integrated đã được lựa chọn sau đó kích Continue.

✓ Trong hộp thoại Microsoft Internet Security and Acceleration Server Setup đọc thông báo về IIS publishing sau đó kích OK để biết rằng ISA Server Setup đang dừng dịch vụ IIS publishing.

✓ Kích OK và đặt ngầm định các giá trị thiết đặt cho cache.

Bước 2:

Cấu hình LAT để khai báo địa chỉ cho mạng riêng.

✓ Trong hộp thoại Microsoft Internet Security and Acceleration Server 2000 Setup kích Construct Table. Lưu ý rằng khi bạn thêm vào không đúng địa chỉ IP vào LAT, ISA server sẽ chuyển tiếp sai các gói tin do đó các máy client sẽ không thể truy cập Internet

✓ Trong hộp thoại Local Address Table, kích để xóa Add the following private ranges: 10.x.x.x, 192.168.x.x and 172.16.x.x-172.31.x.x

✓ Chọn adapter ip_address (với tên cạc mạng và địa chỉ IP là địa chỉ mạng riêng), sau đó kích OK.

✓ Trong thông báo Setup Message, kích OK.

✓ Trong Internal IP Ranges, kích 10.255.255.255-10.255.255.255, sau đó kích Remove.

✓ Kiểm tra rằng Internal IP Ranges chỉ chứa IP addresses trong mạng trong của bạn sau đó kích OK.

✓ Kết thúc việc cài đặt ISA Server và khởi tạo cấu hình ISA Server.

✓ Trong hộp thoại Launch ISA Management Tool, kích để xóa

✓ Start ISA Server Getting Started Wizard check box, sau đó kích OK.

✓ Trong hộp thông báo Microsoft ISA Server (Enterprise Edition) Setup kích OK.

✓ Đóng cửa sổ Microsoft ISA Server Setup.

✓ Lấy đĩa Microsoft Internet Security and Acceleration Server Enterprise Edition từ ổ đĩa CD-ROM.

Bước 3:

✓ Cấu hình Default Web Site trong Internet Information Services sử dụng cổng 8008, sau đó khởi động Default Web Site.

✓ Mở Internet Services Manager từ Administrative Tools.

✓ Trong Internet Information Services, mở rộng server(server là tên máy tính của bạn), sau đó kích DefaultWeb Site (Stopped).

✓ Kích chuột phải Default Web Site (Stopped), sau đó kích Properties. Vì ISA Server sử dụng các cổng 80 and 8080, bạn phải cấu hình IIS để phục vụ các kết nối từ các client tới trên cổng khác. Bạn sẽ cấu hình IIS để phục cụ các yêu cầu này trên cổng TCP 8008.

✓ Trong hộp thoại Default Web Site (Stopped) Properties, trong hộp TCP Port, gõ 8008 sau đó kích OK.

✓ Kích chuột phải Default Web Site (Stopped), sau đó kích Start.

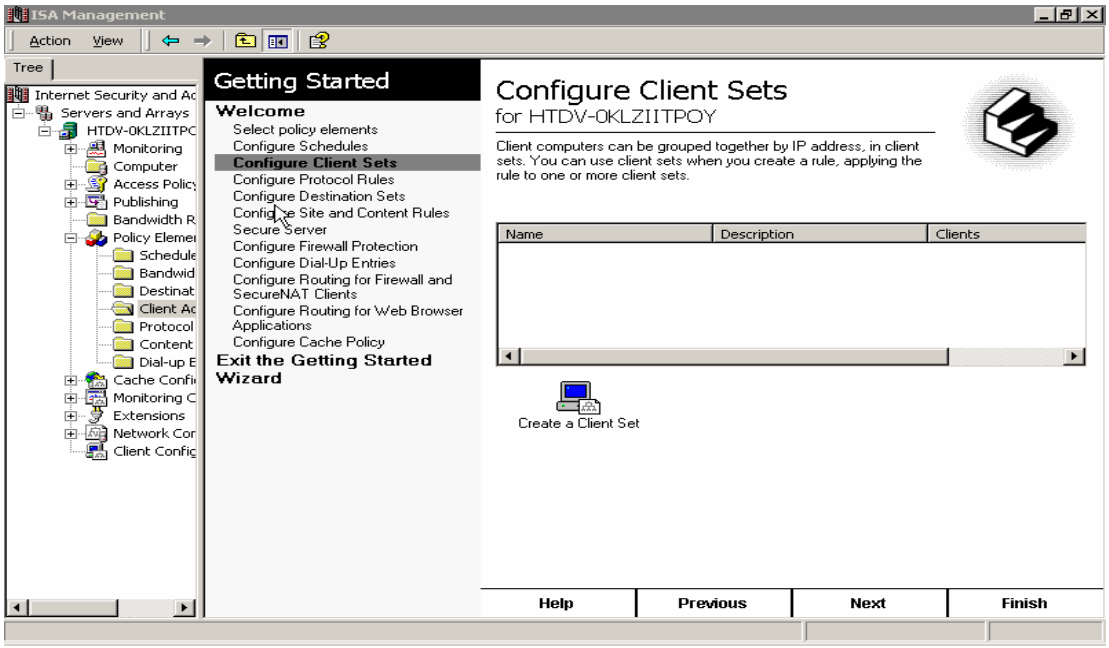
Bài 2:

Cấu hình ISA Server 2000 cho phép một mạng nội bộ có thể truy cập, sử dụng các dịch vụ cơ bản trên Internet qua 01 modem kết nối qua mạng PSTN.

Bước 1:

Cấu hình và quản trị cấu hình cho ISA server sử dụng Getting Started

Với Getting Started Wizard, có các lựa chọn cấu hình sau:



Hình 6.15

- ✓ Select Policy elements, cấu hình ngầm định chọn tất cả các thành phần để có thể sử dụng khi tạo các qui tắc.
- ✓ Configure Schedules, cấu hình ngầm định có hai lịch là Weekends và Work Hours, ta có thể sửa các lịch này hoặc tạo các lịch mới.
- ✓ Configure Client sets, các máy tính Client có thể tạo thành nhóm với nhau bằng các địa chỉ IP sử dụng cho mục đích tạo các qui tắc ứng với từng nhóm client
- ✓ Configure Protocol Rule, đưa ra các qui tắc giao thức để các client sử dụng truy nhập Internet
- ✓ Configure Destination Sets, cho phép thiết lập các máy tính trên mạng Internet thành nhóm bởi tên hay địa chỉ IP, Destination Sets được sử dụng để tạo ra các qui tắc, áp dụng các qui tắc cho một hay nhiều Destination Sets
- ✓ Configure Site and Content Rules, cấu hình các qui tắc về nội dung.
- ✓ Secure Server cho phép bạn có thể đặt các mức độ bảo vệ thích hợp cho mạng.
- ✓ Configure Filewall Protection, Packet Fitering bảo đảm cho ISA server sẽ lọc không có packet nào qua trừ khi được phép
- ✓ Cofigure Dial-Up Entries, cho phép chọn giao diện để kết nối với Internet
- ✓ Configure Routing for filewall and secureNat client.
- ✓ Configure Routing for Web browser Appilications cho phép tạo các qui tắc định tuyến, xác định rõ yêu cầu từ Web Proxy Client được gửi trực tiếp tới Internet hay tới Upstream server
- ✓ Configure Cache policy, cấu hình các chính sách về cache.

Bước 2:

Cấu hình ISA server cho phép các client sử dụng được các dịch vụ của Internet qua mạng thoại công cộng

- ✓ Tạo một Dial-Up Entries, để kết nối với InternetBước 2: Tạo một qui tắc giao thức.
- ✓ Mở ISA Management, kích Servers and arrays, sau đó kích tên máy chủ ISA.

- ✓ Kích Access Policy, kích chuột phải vào Protocol Rule, sau đó chọn New --> Rule.
- ✓ Đặt tên của Protocol Rule, sau đó kích Next.
- ✓ Kiểm tra rằng **Allow đã được chọn**, kích Next, sau đó chọn **All IP traffic**, kích Next Chọn **Always**, kích Next sau đó chọn **Any Request**, kích Next, sau đó kích Finish.

Bước 3:

Cấu hình Web Proxy Client: cấu hình Internet Explorer để sử dụng ISA server đối với các yêu cầu truy cập dịch vụ Web.

- ✓ Mở trình duyệt Internet Explorer.
- ✓ Trong Internet Connection Wizard, kích Cancel.
- ✓ Trong hộp thoại Internet Connection Wizard, chọn Do not show the Internet Connection wizard in the future, sau đó kích Yes.
- ✓ Trong Internet Explorer, trong ô Address , gõ http://vdc.com.vn sau đó chọn ENTER. Internet Explorer không thể kết nối tới trang web này.
- ✓ Trong menu Tools, kích Internet Options.
- ✓ Trong hộp thoại Internet Options, trong Connections kích LAN Settings.
- ✓ Trong hộp thoại Local Area Network (LAN) Settings , kích để bỏ lựa chọn Automatically detect settings. Chọn Use a proxy server, trong ô Address gõ vào địa chỉ IP của ISA Server .
- ✓ Trong hộp Port, gõ 8080
- ✓ Kiểm tra rằng lựa chọn Bypass proxy server for local addresses đã bỏ, sau đó kích OK hai lần.

Bài 3:

Thiết đặt các chính sách cho các yêu cầu truy cập và sử dụng các dịch vụ trên mạng internet.

I.Thiết lập các thành phần chính sách

Bước 1: Thiết lập lịch trình

- ✓ Đăng nhập vào hệ thống với quyền administrator
- ✓ Mở ISA Management từ thực đơn Microsoft ISA Server.
- ✓ Trong ISA Management, mở rộng Servers and Arrays, mở rộng server (server là tên của ISA Server), mở rộng Policy Elements, sau đó kích Schedules.
- ✓ Kích Create a Schedule để thiết lập một lịch trình.
- ✓ Trong hộp thoại New schedule trong mục Name đưa vào một tên lịch trình ví dụ schedule1.
- ✓ Trong mục Description gõ vào Daily period of most network utilization
- ✓ Kéo để lựa chọn toàn bộ lịch trình sau đó kích Inactive.
- ✓ Kéo để lựa chọn vùng từ thời điểm hiện tại tới 2 h tiếp theo đối với tất cả các ngày trong tuần sau đó kích active ví dụ, nếu thời điểm hiện tại là 3:15 P.M., thì lựa chọn vùng từ 3:00 P.M. tới 5:00 P.M. cho tất cả các ngày trong tuần.
- ✓ Kích OK.

Bước 2: Thiết lập destination set

- ✓ Trong ISA Management, kích Destination Sets.
- ✓ Kích Create a Destination Set.
- ✓ Trong hộp thoại New Destination Set trong mục Name cho vào một tên cho thiết lập mới này ví dụ set1.
- ✓ Trong mục Description box, gõ vào một nội dung mô tả cho thiết lập mới này
- ✓ Kích Add.
- ✓ Trong hộp thoại Add/Edit Destination trong mục Destination gõ home.vnn.vn

Bước 3: Thiết lập client address set

- ✓ Trong ISA Management kích Client Address Sets.
- ✓ Kích Create a Client Set.
- ✓ Trong hộp thoại Client Set trong mục Name gõ vào một tên cho thiết lập mới ví dụ Accounting Department.

- ✓ Trong mục Description gõ nội dung mô tả cho thiết lập mới này sau đó kích Add.
- ✓ Trong hộp thoại Add/Edit IP Addresses trong mục From gõ vào địa chỉ bắt đầu thuộc nhóm địa chỉ thuộc mạng dùng riêng .
- ✓ Trong mục To gõ vào địa chỉ kết thúc thuộc nhóm địa chỉ thuộc mạng dùng riêng kích OK hai lần.

Bước 4: Thiết lập protocol definition (sử dụng cổng UDP 39000 cho kết nối chính gọi ra và cổng TCP 39000 cho kết nối thứ hai)

- ✓ Trong ISA Management kích Protocol Definitions.
- ✓ Kích Create a Protocol Definition.
- ✓ Trong New Protocol Definition Wizard trong mục Protocol definition
- ✓ name gõ vào một tên cho thiết đặt mới sau đó kích Next.
- ✓ Trong trang Primary Connection Information trong mục Port number
- ✓ gõ vào 39000
- ✓ Trong danh sách Protocol type kích UDP.
- ✓ Trong danh sách Direction kích Send Receive sau đó kích Next.
- ✓ Trong trang Secondary Connections kích Yes sau đó kích New.
- ✓ Trong hộp thoại New/Edit Secondary Connection trong mục From và mục To gõ 39000
- ✓ Trong danh sách Protocol type kiểm tra rằng TCP đã được lựa chọn, trong mục Direction
- ✓ kích Outbound sau đó kích OK.
- ✓ Kích Next sau đó trong trang Completing the New Protocol Definition
- ✓ Wizard kích Finish.

II.Thiết lập các qui tắc giao thức

Bước 1:

Thiết lập một qui tắc giao thức cho phép HTTP, HTTP-S và FTP đối với mọi người dùng truy cập Internet tại mọi thời điểm bằng việc sử dụng các giao thức HTTP, HTTP-S và FTP .

- ✓ Mở trình duyệt Internet Explorer tại một máy trạm, trong ô Address gõ http://home.vnn.vn nhấn ENTER. Trình duyệt Internet Explorerkhông thể kết nối tới Web site vì ISA Server từ chối yêu cầu.
- ✓ Đóng Internet Explorer.
- ✓ Trong ISA Management mở rộng Access Policy sau đó kích Protocol Rules.
- ✓ Kích Create a Protocol Rule for Internet Access.
- ✓ Trong New Protocol Rule Wizard, trong mục Protocol rule name gõ Allow HTTP, HTTP-S, and FTP sau đó kích Next.
- ✓ Trong trang Protocols kiểm tra rằng Selected protocols đã được chọn, kích để xóa Gopher check box sau đó kích Next.
- ✓ Trong trang Schedule kiểm tra rằng Always đã được lựa chọn sau đó kích Next.
- ✓ Trong trang Client Type kiểm tra rằng Any request đã được chọn, sau đó kích Next.
- ✓ Trong trang Completing the New Protocol Rule Wizard kích Finish.
- ✓ Mở Internet Explorer tại một máy tính trạm, trong mục Address gõ http://home.vnn.vn sao đó ấn ENTER. Kiểm tra rằng trình duyệt kết nối thành công nội dung trang web được hiển thị
- ✓ Đóng Internet Explorer.

Bước 2:

Thiết lập một qui tắc giao thức cho phép người dùng trong nhóm Domain Admins truy cập Internet sử dụng tất cả các giao thức.

- ✓ Trong ISA Management kích Create a Protocol Rule.
- ✓ Trong New Protocol Rule Wizard, trong mục Protocol rule name gõ Allow All Access for Administrators sau đó kích Next.
- ✓ Trong trang Rule Action kiểm tra rằng Allow đã được chọn sau đó kích Next.
- ✓ Trong trang Protocols, trong danh sách Apply this rule to kiểm tra rằng All IP traffic đã được chọn sau đó kích Next.

- ✓ Trong trang Schedule, kiểm tra rằng Always đã được chọn sau đó kích Next.
- ✓ Trong trang Client Type, kích Specific users and groups, sau đó kích Next.
- ✓ Trong trang Users and Groups, kích Add.
- ✓ Trong hộp thoại Select Users or Groups, kích Domain Admins, kích Add, sau đó kích OK.
- ✓ Trong trang Users and Groups, kích Next.
- ✓ Trong trang Completing the New Protocol Rule Wizard kích Finish.

Bước 3:

Thiết lập một qui tắc giao thức từ chối người dùng trong nhóm Accounting Department đã định nghĩa trong client set truy cập Internet.

- ✓ Trong ISA Management, kích Create a Protocol Rule.
- ✓ Trong New Protocol Rule Wizard, trong mục Protocol rule name gõ vào Deny Access from Accounting Department , sau đó kích Next.
- ✓ Trong trang Rule Action, kích Deny, sau đó kích Next.
- ✓ Trong trang Protocols, trong danh sách Apply this rule to, kiểm tra rằng All IP traffic đã được lựa chọn, sau đó kích Next.
- ✓ Trong trang Schedule, kiểm tra rằng Always đã được lựa chọn, sau đó kích Next.
- ✓ Trong trang Client Type, kích Specific computers (client address
- ✓ sets), sau đó kích Next.
- ✓ Trong trang Client Sets, kích Add.
- ✓ Trong hộp thoại Add Client Sets, kích Accounting Department, kích Add, sau đó kíchOK.
- ✓ Trong trang Client Sets, kích Next.
- ✓ Trong trang Completing the New Protocol Rule Wizard, kích Finish.
- ✓ Kiểm tra để xác nhận việc truy cập không thành công từ nhóm nhóm Accounting Department

Bước 4:

Xóa qui tắc giao thức từ chối người dùng trong nhóm Accounting Department

- ✓ Trong In ISA Management, kích Deny Access from Accounting Department
- ✓ Kích Delete a Protocol Rule.
- ✓ Trong hộp thoại Confirm Delete, kích Yes.

III.Thiết lập các qui tắc nội dung

Bước 1:

Thiết lập một qui tắc nội dung để từ chối truy cập tới nội dung đã được định nghĩa trong destination set và với lịch trình đã thiết lập ở mục 1

- ✓ Trong ISA Management, kích Site and Content Rules.
- ✓ Kích Create a Site and Content Rule.
- ✓ Trong New Site and Content Rule Wizard, trong mục Site and content rule
- ✓ name, gõ vào một tên ví dụ Deny Access Rule sau đó kích Next.
- ✓ Trong trang Rule Action, kiểm tra rằng Deny đã được chọn, sau đó kích Next.
- ✓ Trong trang Destination Sets, trong danh sách Apply this rule to, kích Specified destination set.
- ✓ Trong danh sách Name, lựa chọn set1 (đã thiết lập ở phần trên), sau đó kích Next.
- ✓ Trong trang Schedule, chọn schedule1 (đã thiết lập ở phần trên), sau đó kích Next.
- ✓ Trong trang Client Type, kiểm tra rằng Any request đã được chọn, sau đó kích Next.
- ✓ Trong trang Completing the New Site and Content Rule Wizard, kích Finish.

Bước 2:

Kiểm tra qui tắc vừa thiết lập

- ✓ Mở trình duyệt Internet Explorer.

- ✓ Trong ô Address, gõ http://home.vnn.vn sau đó ấn ENTER. kiểm tra rằng trang web này không được hiển thị, vì qui tắc nội dung đã thiết lập ở trên đã có hiệu lực
- ✓ Đóng trình duyệt Internet Explorer.

Chương 6 : Bảo mật hệ thống và Firewall

Chương 6 tập trung vào các nội dung quan trọng về bảo mật hệ thống và mạng lưới. Nội dung của phần thứ nhất chương 6 cung cấp cho các học viên khái niệm về các hình thức tấn công mạng, các lỗ hổng, điểm yếu của mạng lưới. Các kỹ năng cơ bản trong phần một của chương 6 giúp người quản trị quản lý và xây dựng các chính sách bảo mật tương ứng cho các thành phần mạng, hệ thống hay dịch vụ ngay từ lúc bắt đầu hoạt động.

Phần 2 của chương 6 tập trung giới thiệu về thiết bị bảo mật mạnh và thông dụng trên mạng. Đó là thiết bị bức tường lửa (firewall). Học viên sẽ có được các kiến thức về cấu trúc firewall, các chức năng cơ bản và cách phân loại cũng như ưu nhược điểm của các loại firewall hoạt động theo các nguyên lý khác nhau. Những kỹ năng thiết lập cấu hình, luật, quản trị firewall với mô hình firewall checkpoint sẽ giúp cho các học viên hiểu cụ thể và các công việc quản trị và bảo mật hệ thống mạng

Chương 6 yêu cầu các học viên trang bị rất nhiều các kiến thức cơ bản như nắm vững các kiến thức quản trị hệ thống OS windows, linux, unix. Học viên cần hiểu sâu về giao thức TCP/IP, hoạt động của IP hay UDP, TCP. Học viên cần có hiểu biết về các port, socket của các giao thức dịch vụ như SMTP, POP3, WWW...Các kiến thức được trang bị trong các giáo trình quản trị hệ thống hoặc các tài liệu, sách giáo khoa về nội dung trên học viên nên tham khảo trước khi học chương 6 này.

I. Bảo mật hệ thống

I.1. Các vấn đề chung về bảo mật hệ thống và mạng

Do đặc điểm của một hệ thống mạng là có nhiều người sử dụng và phân tán về mặt địa lý nên việc bảo vệ các tài nguyên (mất mát, hoặc sử dụng không hợp lệ) trong môi trường mạng phức tạp hơn nhiều so với môi trường một máy tính đơn lẻ, hoặc một người sử dụng.

Hoạt động của người quản trị hệ thống mạng phải đảm bảo các thông tin trên mạng là tin cậy và sử dụng đúng mục đích, đối tượng đồng thời đảm bảo mạng hoạt động ổn định, không bị tấn công bởi những kẻ phá hoại.

Có một thực tế là không một hệ thống mạng nào đảm bảo là an toàn tuyệt đối, một hệ thống dù được bảo vệ chắc chắn đến mức nào thì cũng có lúc bị vô hiệu hoá bởi những kẻ có ý đồ xấu.

I.1.1. Một số khái niệm và lịch sử bảo mật hệ thống

Trước khi tìm hiểu các vấn đề liên quan đến phương thức phá hoại và các biện pháp bảo vệ cũng như thiết lập các chính sách về bảo mật, ta sẽ tìm hiểu một số khái niệm liên quan đến bảo mật thông tin trên mạng Internet.

I.1.1.1. Một số khái niệm:

a) Đối tượng tấn công mạng (Intruder):

Là những cá nhân hoặc các tổ chức sử dụng các kiến thức về mạng và các công cụ phá hoại (phần mềm hoặc phần cứng) để dò tìm các điểm yếu, lỗ hổng bảo mật trên hệ thống, thực hiện các hoạt động xâm nhập và chiếm đoạt tài nguyên mạng trái phép.

Một số đối tượng tấn công mạng là:

- Hacker: Là những kẻ xâm nhập vào mạng trái phép bằng cách sử dụng các công cụ phá mật khẩu hoặc khai thác các điểm yếu của các thành phần truy nhập trên hệ thống.

- Masquerader: Là những kẻ giả mạo thông tin trên mạng. Có một số hình thức như giả mạo địa chỉ IP, tên miền, định danh người dùng ...

- Eavesdropping: Là những đối tượng nghe trộm thông tin trên mạng, sử dụng các công cụ sniffer; sau đó dùng các công cụ phân tích và debug để lấy được các thông tin có giá trị.

Những đối tượng tấn công mạng có thể nhằm nhiều mục đích khác nhau như: ăn cắp những thông tin có giá trị về kinh tế, phá hoại hệ thống mạng có chủ định, hoặc cũng có thể chỉ là những hành động vô ý thức, thử nghiệm các chương trình không kiểm tra cẩn thận ...

b) Các lỗ hổng bảo mật:

Các lỗ hổng bảo mật là những điểm yếu trên hệ thống hoặc ẩn chứa trong một dịch vụ mà dựa vào đó kẻ tấn công có thể xâm nhập trái phép để thực hiện các hành động phá hoại hoặc chiếm đoạt tài nguyên bất hợp pháp.

Nguyên nhân gây ra những lỗ hổng bảo mật là khác nhau: có thể do lỗi của bản thân hệ thống, hoặc phần mềm cung cấp, hoặc do người quản trị yếu kém không hiểu sâu sắc các dịch vụ cung cấp ...

Mức độ ảnh hưởng của các lỗ hổng là khác nhau. Có những lỗ hổng chỉ ảnh hưởng tới chất lượng dịch vụ cung cấp, có những lỗ hổng ảnh hưởng nghiêm trọng tới toàn bộ hệ thống ...

c) Chính sách bảo mật:

Là tập hợp các qui tắc áp dụng cho mọi đối tượng có tham gia quản lý và sử dụng các tài nguyên và dịch vụ mạng.

Mục tiêu của chính sách bảo mật giúp người sử dụng biết được trách nhiệm của mình trong việc bảo vệ các tài nguyên thông tin trên mạng , đồng thời giúp các nhà quản trị thiết lập các biện pháp bảo đảm hữu hiệu trong quá trình trang bị, cấu hình, kiểm soát hoạt động của hệ thống và mạng

Một chính sách bảo mật được coi là hoàn hảo nếu nó xây dựng gồm các văn bản pháp qui, kèm theo các công cụ bảo mật hữu hiệu và nhanh chóng giúp người quản trị phát hiện, ngăn chặn các xâm nhập trái phép.

I.1.1.2. Lịch sử bảo mật hệ thống:

Có một số sự kiện đánh dấu các hoạt động phá hoại trên mạng, từ đó nảy sinh các yêu cầu về bảo mật hệ thống như sau:

- Năm 1988: Trên mạng Internet xuất hiện một chương trình tự nhân phiên bản của chính nó lên tất cả các máy trên mạng Internet. Các chương trình này gọi là "sâu". Tuy mức độ nguy hại của nó không lớn, nhưng nó đặt ra các vấn đề đối với nhà quản trị về quyền truy nhập hệ thống, cũng như các lỗi phần mềm.

- Năm 1990: Các hình thức truyền Virus qua địa chỉ Email xuất hiện phổ biến trên mạng Internet.

- Năm 1991: Phát hiện các chương trình trojans.

Cùng thời gian này sự phát triển của dịch vụ Web và các công nghệ liên quan như Java, Javascipts đã có rất nhiều các thông báo lỗi về bảo mật liên quan như: các lỗ hổng cho phép đọc nội dung các file dữ liệu của người dùng, một số lỗ hổng cho phép tấn công bằng hình thức DoS, spam mail làm ngưng trệ dịch vụ.

- Năm 1998: Virus Melisa lan truyền trên mạng Internet thông qua các chương trình gửi mail của Microsoft, gây những thiết hại kinh tế không nhỏ.

- Năm 2000: Một loạt các Web Site lớn như yahoo.com và ebay.com bị tê liệt, ngừng cung cấp dịch vụ trong nhiều giờ do bị tấn công bởi hình thức DoS.

I.1.2. Các lỗ hổng và phương thức tấn công mạng chủ yếu

I.1.2.1. Các lỗ hổng

Như phần trên đã trình bày, các lỗ hổng bảo mật trên một hệ thống là các điểm yếu có thể tạo ra sự ngưng trệ của dịch vụ, thêm quyền đối với người sử dụng hoặc cho phép các truy nhập không hợp pháp vào hệ thống. Các lỗ hổng cũng có thể nằm ngay các dịch vụ cung cấp như sendmail, web, ftp ... Ngoài ra các lỗ hổng còn tồn tại ngay chính tại hệ điều hành như trong Windows NT, Windows 95, UNIX hoặc trong các ứng dụng mà người sử dụng thường xuyên sử dụng như word processing, các hệ databases...

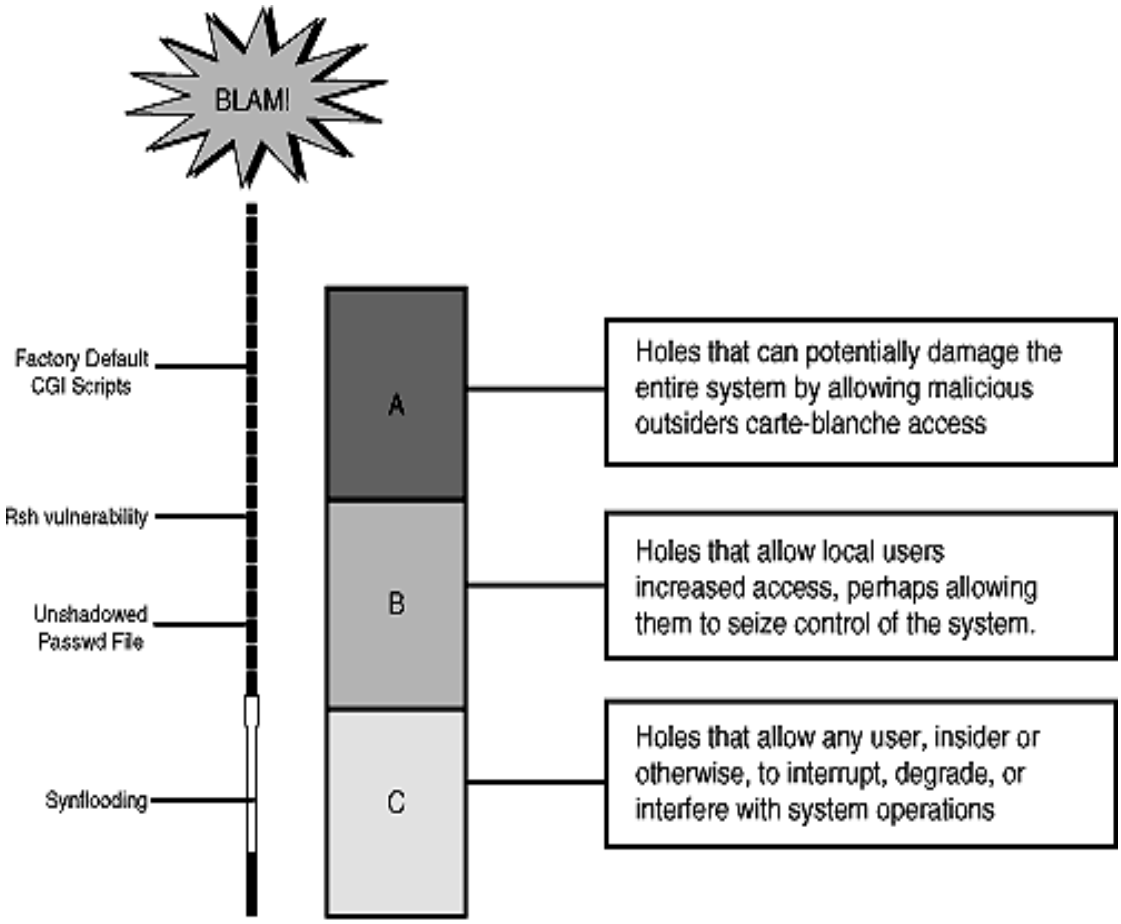
Có nhiều tổ chức khác nhau tiến hành phân loại các dạng lỗ hổng đặc biêt. Theo cách phân loại của Bộ quốc phòng Mỹ, các loại lỗ hổng bảo mật trên một hệ thống được chia như sau:

- Lỗ hổng loại C: các lỗ hổng loại này cho phép thực hiện các phương thức tấn công theo DoS (Denial of Services - Từ chối dịch vụ). Mức độ nguy hiểm thấp, chỉ ảnh hưởng tới chất lượng dịch vụ, có thể làm ngưng trệ, gián đoạn hệ thống; không làm phá hỏng dữ liệu hoặc đạt được quyền truy nhập bất hợp pháp.

- Lổ hổng loại B: Các lỗ hổng cho phép người sử dụng có thêm các quyền trên hệ thống mà không cần thực hiện kiểm tra tính hợp lệ nên có thể dẫn đến mất mát hoặc lộ thông tin yêu cầu bảo mật. Mức độ nguy hiểm trung bình. Những lỗ hổng này thường có trong các ứng dụng trên hệ thống.

- Lỗ hổng loại A: Các lỗ hổng này cho phép người sử dụng ở ngoài cho thể truy nhập vào hệ thống bất hợp pháp. Lỗ hổng này rất nguy hiểm, có thể làm phá hủy toàn bộ hệ thống.

Hình sau minh họa các mức độ nguy hiểm và loại lỗ hổng tương ứng:



Hình 1.1: Các loại lỗ hổng bảo mật và mức độ nguy hiểm

Sau đây ta sẽ phân tích một số lỗ hổng bảo mật thường xuất hiện trên mạng và hệ thống.

a) Các lỗ hổng loại C

Các lỗ hổng loại này cho phép thực hiện các cuộc tấn công DoS.

DoS là hình thức tấn công sử dụng các giao thức ở tầng Internet trong bộ giao thức TCP/IP để làm hệ thống ngưng trệ dẫn đến tình trạng từ chối người sử dụng hợp pháp truy nhập hay sử dụng hệ thống. Một số lượng lớn các gói tin được gửi tới server trong khoảng thời gian liên tục làm cho hệ thống trở nên

quá tải, kết quả là server đáp ứng chậm hoặc không thể đáp ứng các yêu cầu từ client gửi tới.

Các dịch vụ có lỗ hổng cho phép thực hiện các cuộc tấn công DoS có thể được nâng cấp hoặc sửa chữa bằng các phiên bản mới hơn của các nhà cung cấp dịch vụ. Hiện nay, chưa có một giải pháp toàn diện nào để khắc phục các lỗ hổng loại này vì bản thân việc thiết kế giao thức ở tầng Internet (IP) nói riêng và bộ giao thức TCP/IP đã chứa đựng những nguy cơ tiềm tàng của các lỗ hổng này.

Ví dụ điển hình của phương thức tấn công DoS là các cuộc tấn công vào một số Web Site lớn làm ngưng trệ hoạt động của web site này như: www.ebay.com và www.yahoo.com.

Tuy nhiên, mức độ nguy hiểm của các lỗ hổng loại này được xếp loại C, ít nguy hiểm vì chúng chỉ làm gián đoạn sự cung cấp dịch vụ của hệ thống trong một thời gian mà không làm nguy hại đến dữ liệu và những kẻ tấn công cũng không đạt được quyền truy nhập bất hợp pháp vào hệ thống.

Một lỗ hổng loại C khác cũng thường thấy đó là các điểm yếu của dịch vụ cho phép thực hiện tấn công làm ngưng trệ hệ thống của người sử dụng cuối. Chủ yếu hình thức tấn công này là sử dụng dịch vụ Web. Giả sử trên một Web Server có những trang Web trong đó có chứa các đoạn mã Java hoặc JavaScripts, làm "treo" hệ thống của người sử dụng trình duyệt Web của Netscape bằng các bước sau:

- Viết các đoạn mã để nhận biết được Web Browers sử dụng Netscape.

- Nếu sử dụng Netscape, sẽ tạo một vòng lặp vô thời hạn, sinh ra vô số các cửa sổ, trong mỗi cửa sổ đó nối đến các Web Server khác nhau.

Với một hình thức tấn công đơn giản này, có thể làm treo hệ thống trong khoảng thời gian 40 giây (đối với máy client có 64 MB RAM). Đây cùng là một hình thức tấn công kiểu DoS. Người sử dụng trong trường hợp này chỉ có thể khởi động lại hệ thống.

Một lỗ hổng loại C khác cũng thường gặp đối với các hệ thống mail là không xây dựng các cơ chế anti-relay (chống relay) cho phép thực hiện các hành động spam mail. Như chúng ta đã biết, cơ chế hoạt động của dịch vụ thư điện tử là lưu và chuyển tiếp. Một số hệ thống mail không có các xác thực khi người dùng gửi thư, dẫn đến tình trạng các đối tượng tấn công lợi dụng các

máy chủ mail này để thực hiện spam mail. Spam mail là hành động nhằm làm tê liệt dịch vụ mail của hệ thống bằng cách gửi một số lượng lớn các message tới một địa chỉ không xác định, vì máy chủ mail luôn phải tốn năng lực đi tìm những địa chỉ không có thực dẫn đến tình trạng ngưng trệ dịch vụ. Các message có thể sinh ra từ các chương trình làm bom thư rất phổ biến trên mạng Internet.

b) Các lỗ hổng loại B:

Lỗ hổng loại này có mức độ nguy hiểm hơn lỗ hổng loại C, cho phép người sử dụng nội bộ có thể chiếm được quyền cao hơn hoặc truy nhập không hợp pháp.

Ví dụ trên hình 12, lỗ hổng loại B có thể có đối với một hệ thống UNIX mà file /etc/passwd để ở dạng plaintext; không sử dụng cơ chế che mật khẩu trong UNIX (sử dụng file /etc/shadow)

Những lỗ hổng loại này thường xuất hiện trong các dịch vụ trên hệ thống. Người sử dụng local được hiểu là người đã có quyền truy nhập vào hệ thống với một số quyền hạn nhất định.

Một loại các vấn đề về quyền sử dụng chương trình trên UNIX cũng thương gây nên các lô hổng loại B. Vì trên hệ thống UNIX một chương trình có thể được thực thi với 2 khả năng:

- Người chủ sở hữu chương trình đó kích hoạt chạy.

- Người mang quyền của người sở hữu file đó kích hoạt chạy.

Một dạng khác của lỗ hổng loại B xảy ra đối với các chương trình có mã nguồn viết bằng C. Những chương trình viết bằng C thường sử dụng một vùng đệm - một vùng trong bộ nhớ sử dụng để lưu dữ liệu trước khi xử lý. Những người lập trình thường sử dụng vùng đệm trong bộ nhớ trước khi gán một khoảng không gian bộ nhớ cho từng khối dữ liệu. Ví dụ, người sử dụng viết chương trình nhập trường tên người sử dụng, qui định trường này dài 20 ký tự. Do đó họ sẽ khai báo:

char first_name [20];

Khai báo này sẽ cho phép người sử dụng nhập vào tối đa 20 ký tự. Khi nhập dữ liệu, trước tiên dữ liệu được lưu ở vùng đệm; nếu người sử dụng nhập vào 35 ký tự sẽ xảy ra hiện tượng tràn vùng đệm và kết quả 15 ký tự dư thừa sẽ nằm ở một vị trí không kiểm soát được trong bộ nhớ. Đối với những kẻ tấn công, có thể lợi dụng lỗ hổng này để nhập vào những ký tự đặc biệt, để thực thi

một số lệnh đặc biệt trên hệ thống. Thông thường, lỗ hổng này thường được lợi dụng bởi những người sử dụng trên hệ thống để đạt được quyền root không hợp lệ.

Việc kiểm soát chặt chẽ cấu hình hệ thống và các chương trình sẽ hạn chế được các lỗ hổng loại B.

c) Các lỗ hổng loại A:

Các lỗ hổng loại A có mức độ rất nguy hiểm, đe dọa tính toàn vẹn và bảo mật của hệ thống. Các lỗ hổng loại này thường xuất hiện ở những hệ thống quản trị yếu kém hoặc không kiểm soát được cấu hình mạng.

Một ví dụ thường thấy là trên nhiều hệ thống sử dụng Web Server là Apache, Đối với Web Server này thường cấu hình thư mục mặc định để chạy các script là cgi-bin; trong đó có một Scripts được viết sẵn để thử hoạt động của apache là test-cgi. Đối với các phiên bản cũ của Apache (trước version 1.1), có dòng sau trong file test-cgi:

echo QUERY_STRING = $QUERY_STRING

Biến môi trường QUERY_STRING do không được đặt trong có dấu " (quote) nên khi phía client thực hiện một yêu cầu trong đó chuỗi ký tự gửi đến gồm một số ký tự đặc biệt; ví dụ ký tự "*", web server sẽ trả về nội dung của toàn bộ thư mục hiện thời (là các thư mục chứa các script cgi). Người sử dụng có thể nhìn thấy toàn bộ nội dung các file trong thư mục hiện thời trên hệ thống server.

Một ví dụ khác cũng xảy ra tương tự đối với các Web server chạy trên hệ điều hành Novell: các web server này có một scripts là convert.bas, chạy scripts này cho phép đọc toàn bộ nội dung các files trên hệ thống.

Những lỗ hổng loại này hết sức nguy hiểm vì nó đã tồn tại sẵn có trên phần mềm sử dụng, người quản trị nếu không hiểu sâu về dịch vụ và phần mềm sử dụng sẽ có thể bỏ qua những điểm yếu này.

Đối với những hệ thống cũ, thường xuyên phải kiểm tra các thông báo của các nhóm tin về bảo mật trên mạng để phát hiện những lỗ hổng loại này. Một loạt các chương trình phiên bản cũ thường sử dụng có những lỗ hổng loại A như: FTP, Gopher, Telnet, Sendmail, ARP, finger...

I.1.2.2. Một số phương thức tấn công mạng phổ biến

a) Scanner

Scanner là một chương trình tự động rà soát và phát hiện những điểm yếu về bảo mật trên một trạm làm việc cục bộ hoặc trên một trạm ở xa. Với chức năng này, một kẻ phá hoại sử dụng chương trình Scanner có thể phát hiện ra những lỗ hổng về bảo mật trên một server ở xa.

Các chương trình scanner thường có một cơ chế chung là rà soát và phát hiện những port TCP/UDP được sử dụng trên một hệ thống cần tấn công từ đó phát hiện những dịch vụ sử dụng trên hệ thống đó. Sau đó các chương trình scanner ghi lại những đáp ứng trên hệ thống ở xa tương ứng với các dịch vụ mà nó phát hiện ra. Dựa vào những thông tin này, những kẻ tấn công có thể tim ra những điểm yếu trên hệ thống.

Những yếu tố để một chương trình Scanner có thể hoạt động như sau:

- Yêu cầu về thiết bị và hệ thống: Một chương trình Scanner có thể hoạt động được nếu môi trường đó có hỗ trợ TCP/IP (bất kể hệ thống là UNIX, máy tính tương thích với IBM, hoặc dòng máy Macintosh).

- Hệ thống đó phải kết nối vào mạng Internet.

Tuy nhiên không phải đơn giản để xây dựng một chương trình Scanner, những kẻ phá hoại cần có kiến thức sâu về TCP/IP, những kiến thức về lập trình C, PERL và một số ngôn ngữ lập trình shell. Ngoài ra người lập trình (hoặc người sử dụng) cần có kiễn thức là lập trình socket, phương thức hoạt động của các ứng dụng client/server.

Các chương trình Scanner có vai trò quan trọng trong một hệ thống bảo mật, vì chúng có khả năng phát hiện ra những điểm yếu kém trên một hệ thống mạng. Đối với người quản trị mạng những thông tin này là hết sức hữu ích và cần thiết; đối với những kẻ phá hoại những thông tin này sẽ hết sức nguy hiểm.

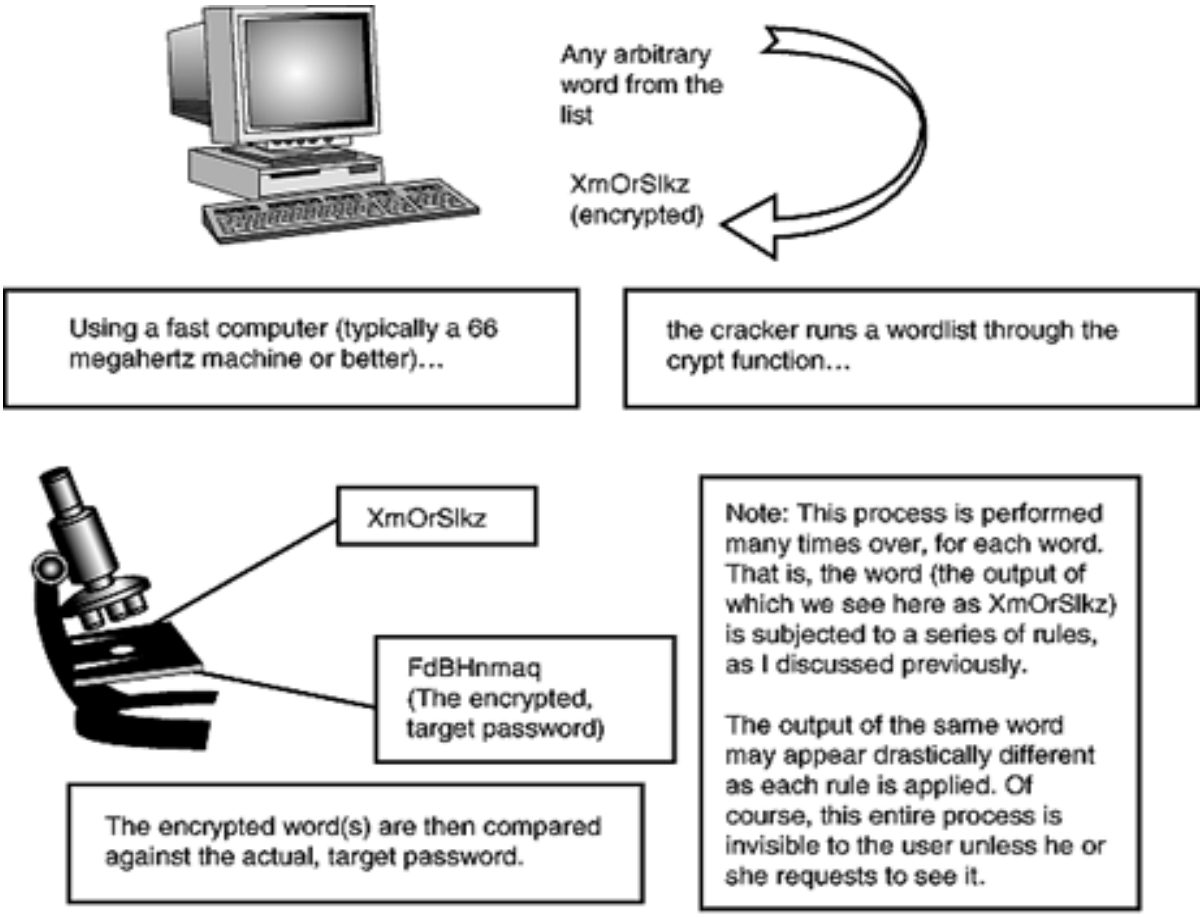
b) Password Cracker

Password cracker là một chương trình có khả năng giải mã một mật khẩu đã được mã hoá hoặc có thể vô hiệu hoá chức năng bảo vệ mật khẩu của một hệ thống.

Để hiểu cách thức hoạt động của các chương trình bẻ khoá, chúng ta cần hiểu cách thức mã hoá để tạo mật khẩu. Hầu hết việc mã hoá các mật khẩu

được tạo ra từ một phương thức mã hoá. Các chương trình mã hoá sử dụng các thuật toán mã hoá để mã hoá mật khẩu.

Quá trình hoạt động của các chương trình bẻ khoá được minh hoạ trong hình sau:



Hình 1.2: Hoạt động của các chương trình bẻ khóa

Theo sơ đồ trên, một danh sách các từ được tạo ra và được mã hoá đối với từng từ. Sau mỗi lần mã hoá, chương trình sẽ so sánh với mật khẩu đã mã hoá cần phá. Nếu không thấy trùng hợp, quá trình lại quay lại. Phương thức bẻ khoá này gọi là bruce-force.

Yếu tố về thiết bị phần cứng: Trong hình trên máy tính thực hiện các chương trình phá khoá là một máy PC 66MHz hoặc cấu hình cao hơn. Trong thực tế yêu cầu các thiết bị phần cứng rất mạnh đối với những kẻ phá khoá

chuyên nghiệp. Một phương thức khác có thể thay thế là thực hiện việc phá khoá trên một hệ thống phần tán; do vậy giảm bớt được các yêu cầu về thiết bị so với phương pháp làm tại một máy.

Nguyên tắc của một số chương trình phá khoá có thể khác nhau. Một vài chương trình tạo một một danh sách các từ giới hạn, áp dụng một số thuật toán mã hoá, từ kết quả so sánh với password đã mã hoá cần bẻ khoá để tạo ra một danh sách khác theo một lôgic của chương trình, cách này tuy không chuẩn tắc nhưng khá nhanh vì dựa vào nguyên tắc khi đặt mật khẩu người sử dụng thường tuân theo một số qui tắc để thuận tiện khi sử dụng.

Đến giai đoạn cuối cùng, nếu thấy phù hợp với mật khẩu đã được mã hoá, kẻ phá khoá sẽ có được mật khẩu dạng text thông thường. Trong hình trên, mật khẩu dạng text thông thường được ghi vào một file.

Để đánh giá khả năng thành công của các chương trình bẻ khoá ta có công thức sau:

$$P = L \times R / S$$

Trong đó:

P: Xác suất thành công

L: Thời gian sống của một mật khẩu

R: Tốc độ thử

S: Không gian mật khẩu = A^M (M là chiều dài mật khẩu)

Ví dụ, trên hệ thống UNIX người ta đã chứng minh được rằng nếu mật khẩu dài quá 8 ký tự thì xác suất phá khoá gần như = 0. Cụ thể như sau:

Nếu sử dụng khoảng 92 ký tự có thể đặt mật khẩu, không gian mật khẩu có thể có là $S = 92^8$

Với tốc độ thử là 1000 mật khẩu trong một giây có R = 1000/s

Thời gian sống của một mật khẩu là 1 năm

Ta có xác suất thành công là :

$P = 1x\ 365\ x\ 86400\ x\ 1000/92^8 = 1/1.000.000$

Như vậy việc dò mật khẩu là không thể vì sẽ mất khoảng 100 năm mới tìm ra mật khẩu chính xác.

Thông thường các chương trình phá khoá thường kết hợp một số thông tin khác trong quá trình dò mật khẩu như:

- Các thông tin trong tập tin /etc/passwd

- Một số từ điển

- Từ lặp và các từ liệt kê tuần tự, chuyển đổi cách phát âm của một từ ...

Biện pháp khắc phục đối với cách thức phá hoại này là cần xây dựng một chính sách bảo vệ mật khẩu đúng đắn.

c) Trojans

Dựa theo truyền thuyết cổ Hy lạp "Ngựa thành Trojan", trojans là một chương trình chạy không hợp lệ trên một hệ thống với vai trò như một chương trình hợp pháp. Những chương trình này thực hiện những chức năng mà người sử dụng hệ thống thường không mong muốn hoặc không hợp pháp. Thông thường, trojans có thể chạy được là do các chương trình hợp pháp đã bị thay đổi mã của nó bằng những mã bất hợp pháp.

Các chương trình virus là một loại điển hình của Trojans. Những chương trình virus che dấu các đoạn mã trong các chương trình sử dụng hợp pháp. Khi những chương trình này được kích hoạt thì những đoạn mã ẩn dấu sẽ được thực thi để thực hiện một số chức năng mà người sử dụng không biết.

Một định nghĩa chuẩn tắc về các chương trình Trojans như sau: chương trình trojans là một chương trình thực hiện một công việc mà người sử dụng không biết trước, giống như ăn cấp mật khẩu hay copy file mà người sử dụng không nhận thức được.

Những tác giả của các chương trình trojan xây dựng một kết hoạch. Xét về khía cạnh bảo mật trên Internet, một chương trình trojan sẽ thực hiện 1 trong những công việc sau:

- Thực hiện một vài chức năng hoặc giúp người lập trình phát hiện những thông tin quan trọng hoặc thông tin cá nhân trên một hệ thống hoặc một vài thành phần của hệ thống đó

- Che dấu một vài chức năng hoặc giúp người lập trình phát hiện những thông tin quan trọng hoặc thông tin cá nhân trên một hệ thống hoặc một vài thành phần của hệ thống đó

Một vài chương trình trojan có thể thực hiện cả 2 chức năng này. Ngoài ra, một số chương trình trojans còn có thể phá huỷ hệ thống bằng cách phá hoại các thông tin trên ổ cứng (ví dụ trường hợp của virus Melisa lây lan qua đường thư điện tử).

Hiện nay với nhiều kỹ thuật mới, các chương trình trojan kiểu này dễ dàng bị phát hiện và không có khả năng phát huy tác dụng. Tuy nhiên trong UNIX việc phát triển các chương trình trojan vẫn hết sức phổ biến.

Các chương trình trojan có thể lây lan qua nhiều phương thức, hoạt động trên nhiều môi trường hệ điều hành khác nhau (từ Unix tới Windows, DOS). Đặc biệt trojans thường lây lan qua một số dịch vụ phổ biến như Mail, FTP... hoặc qua các tiện ích, chương trình miễn phí trên mạng Internet.

Việc đánh giá mức độ ảnh hưởng của các chương trình trojans hết sức khó khăn. Trong một vài trường hợp, nó chỉ đơn giản là ảnh hưởng đến các truy nhập của khách hàng như các chương trình trojans lấy được nội dung của file passwd và gửi mail tới kẻ phá hoại. Cách thức sửa đơn giản nhất là thay thế toàn bộ nội dung của các chương trình đã bị ảnh hưởng bởi các đoạn mã trojans và thay thế các password của người sử dụng hệ thống.

Tuy nhiên với những trường hợp nghiêm trọng hơn, là những kẻ tán công tạo ra những lỗ hổng bảo mật thông qua các chương trình trojans. Ví dụ những kẻ tấn công lấy được quyền root trên hệ thống và lợi dụng nó để phá huỷ toàn bộ hoặc một phần của hệ thống. Chúng dùng quyền root để thay đổi logfile, cài đặt các chương trình trojans khác mà người quản trị không thể phát hiện. Trong trường hợp này, mức độ ảnh hưởng là nghiêm trọng và người quản trị hệ thống đó chỉ còn cách là cài đặt lại toàn bộ hệ thống

d) Sniffer

Đối với bảo mật hệ thống sniffer được hiểu là các công cụ (có thể là phần cứng hoặc phần mềm) "bắt" các thông tin lưu chuyển trên mạng và từ các thông tin "bắt" được đó để lấy được những thông tin có giá trị trao đổi trên mạng.

Hoạt động của sniffer cũng giống như các chương trình "bắt" các thông tin gõ từ bàn phím (key capture). Tuy nhiên các tiện ích key capture chỉ thực hiện trên một trạm làm việc cụ thể còn đối với sniffer có thể bắt được các thông tin trao đổi giữa nhiều trạm làm việc với nhau.

Các chương trình sniffer (sniffer mềm) hoặc các thiết bị sniffer (sniffer cứng) đều thực hiện bắt các gói tin ở tầng IP trở xuống (gồm IP datagram và Ethernet Packet). Do đó, có thể thực hiện sniffer đối với các giao thức khác nhau ở tầng mạng như TCP, UDP, IPX, ...

Mặt khác, giao thức ở tầng IP được định nghĩa công khai, và cấu trúc các trường header rõ ràng, nên việc giải mã các gói tin này không khó khăn.

Mục đích của các chương trình sniffer đó là thiết lập chế độ promiscuous (mode dùng chung) trên các card mạng ethernet - nơi các gói tin trao đổi trong mạng - từ đó "bắt" được thông tin.

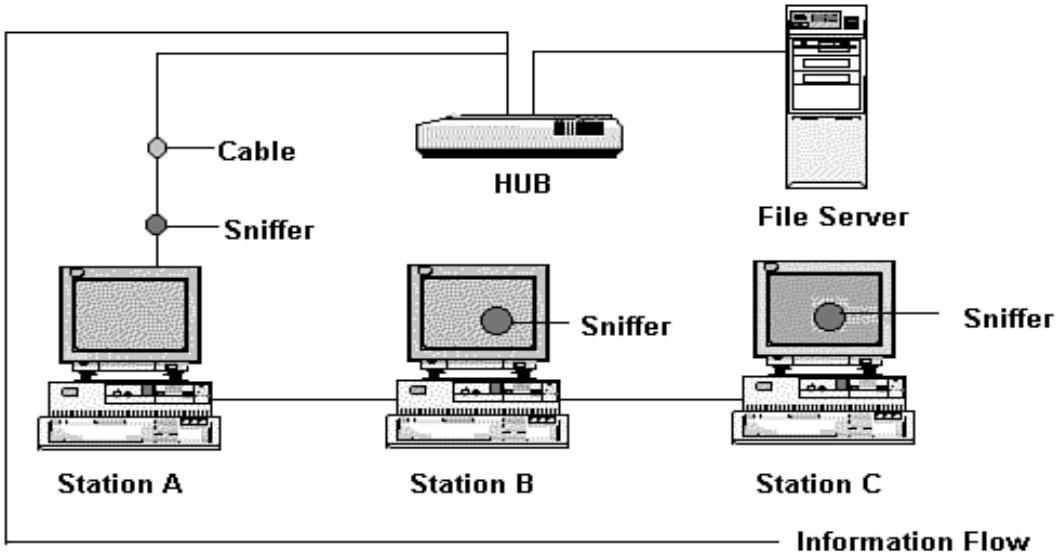
Các thiết bị sniffer có thể bắt được toàn bộ thông tin trao đổi trên mạng là dựa vào nguyên tắc broadcast (quảng bá) các gọi tin trong mạng Ethernet.

Trên hệ thống mạng không dùng hub, dữ liệu không chuyển đến một hướng mà được lưu chuyển theo mọi hướng. Ví dụ khi một trạm làm việc cần được gửi một thông báo đến một trạm làm việc khác trên cùng một segment mạng, một yêu cầu từ trạm đích được gửi tới tất cả các trạm làm việc trên mạng để xác định trạm nào là trạm cần nhận thông tin (trạm đích). Cho tới khi trạm nguồn nhận được thông báo chấp nhận từ trạm đích thì luồng dữ liệu sẽ được gửi đi. Theo đúng nguyên tắc, những trạm khác trên segment mạng sẽ bỏ qua các thông tin trao đổi giữa hai trạm nguồn và trạm đích xác định. Tuy nhiên, các trạm khác cũng không bị bắt buộc phải bỏ qua những thông tin này, do đó chúng vẫn có thể "nghe" được bằng cách thiết lập chế độ promiscous mode trên các card mạng của trạm đó. Sniffer sẽ thực hiện công việc này.

Một hệ thống sniffer có thể kết hợp cả các thiết bị phần cứng và phần mềm, trong đó hệ thống phần mềm với các chế độ debug thực hiện phân tích các gói tin "bắt" được trên mạng.

Hệ thống sniffer phải được đặt trong cùng một segment mạng (network block) cần nghe lén.

Hình sau minh hoạ vị trí đặt sniffer:



Hình 1.3: Các vị trí đặt sniffer trên 1 segment mạng

Phương thức tấn công mạng dựa vào các hệ thống sniffer là rất nguy hiểm vì nó được thực hiện ở các tầng rất thấp trong hệ thống mạng. Với việc thiết lập hệ thống sniffer cho phép lấy được toàn bộ các thông tin trao đổi trên mạng. Các thông tin đó có thể là:

- Các tài khoản và mật khẩu truy nhập

- Các thông tin nội bộ hoặc có giá trị cao...

Tuy nhiên việc thiết lập một hệ thống sniffer không phải đơn giản vì cần phải xâm nhập được vào hệ thống mạng đó và cài đặt các phần mềm sniffer. Đồng thời các chương trình sniffer cũng yêu cầu người sử dụng phải hiểu sâu về kiến trúc, các giao thức mạng.

Mặc khác, số lượng các thông tin trao đổi trên mạng rất lớn nên các dữ liệu do các chương trình sniffer sinh ra khá lớn. Thông thường, các chương trình sniffer có thể cấu hình để chỉ thu nhập từ 200 - 300 bytes trong một gói tin, vi thường những thông tin quan trọng như tên người dùng, mật khẩu nằm ở phần đầu gói tin.

Trong một số trường hợp quản trị mạng, để phân tích các thông tin lưu chuyển trên mạng, người quản trị cũng cần chủ động thiết lập các chương trình sniffer, với vai trò này sniffer có tác dụng tốt.

Việc phát hiện hệ thống bị sniffer không phải đơn giản, vì sniffer hoạt động ở tầng rất thấp, và không ảnh hưởng tới các ứng dụng cũng như các dịch

vụ hệ thống đó cung cấp. Một số biện pháp sau chỉ có tác dụng kiểm tra hệ thống như:

- Kiểm tra các tiến trình đang thực hiện trên hệ thống (bằng lệnh ps trên Unix hoặc trình quản lý tài nguyên trong Windows NT). Qua đó kiểm tra các tiến trình lạ trên hệ thống; tài nguyên sử dụng, thời gian khởi tạo tiến trình... để phát hiện các chương trình sniffer.

- Sử dụng một vài tiện ích để phát hiện card mạng có chuyển sang chế đố promiscous hay không. Những tiện ích này giúp phát hiện hệ thống của bạn có đang chạy sniffer hay không.

Tuy nhiên việc xây dựng các biện pháp hạn chế sniffer cũng không quá khó khăn nếu ta tuân thủ các nguyên tắc về bảo mật như:

- Không cho người lạ truy nhập vào các thiết bị trên hệ thống

- Quản lý cấu hình hệ thống chặt chẽ

- Thiết lập các kết nối có tính bảo mật cao thông qua các cơ chế mã hoá.

I.1.3. Một số điểm yếu của hệ thống

I.1.3.1. Deamon fingerd:

Một lỗ hổng của deamon fingerd là cơ hội để phương thức tấn công worm "sâu" trên Internet phát triển: đó là lỗi tràn vùng đệm trong các tiến trình fingerd (lỗi khi lập trình). Vùng đệm để lưu chuỗi ký tự nhập được giới hạn là 512 bytes. Tuy nhiên chương trình fingerd không thực hiện kiểm tra dữ liệu đầu vào khi lớn hơn 512 bytes. Kết quả là xảy ra hiện tượng tràn dữ liệu ở vùng đệm khi dữ liệu lớn hơn 512 bytes. Phần dữ liệu dư thừa chứa những đoạn mã để kích một script khác hoạt động; scripts này tiếp tục thực hiện finger tới một host khác. Kết quả là hình thành một mắt xích các "sâu" trên mạng Internet.

I.1.3.2. File hosts.equiv:

Nếu một người sử dụng được xác định trong file host.equiv cũng với địa chỉ máy của người đó, thì người sử dụng đó được phép truy nhập từ xa vào hệ thống đã khai báo. Tuy nhiên có một lỗ hổng khi thực hiện chức năng này đó là nó cho phép người truy nhập từ xa có được quyền của bất cứ người nào khác trên hệ thống. Ví dụ, nếu trên máy A có một file /etc/host.equiv có dòng định danh B julie, thì julie trên B có thể truy nhập vào hệ thống A và có bất được

quyền của bất cứ người nào khác trên A. Đây là do lỗi của thủ tục ruserok() trong thư viện libc khi lập trình.

I.1.3.3. Thư mục /var/mail

Nếu thư mục /var/mail được set là với quyền được viết (writeable) đối với tất cả mọi người trên hệ thống, thì bất cứ ai có thể tạo file trong thư mục này. Sau đó tạo một file với tên của một người đã có trên hệ thống rồi link tới một file trên hệ thống, thì các thư tới người sử dụng có tên trùng với tên file link sẽ được gán thêm vào trong file mà nó link tới.

Ví dụ, một người sử dụng tạo link từ /var/mail/root tới /etc/passwd, sau đó gửi mail bằng tên một người mới tới root thì tên người sử dụng mới này sẽ được gán thêm vào trong file /etc/passwd; Do vậy thư mục /var/mail không bao giờ được set với quyền writeable.

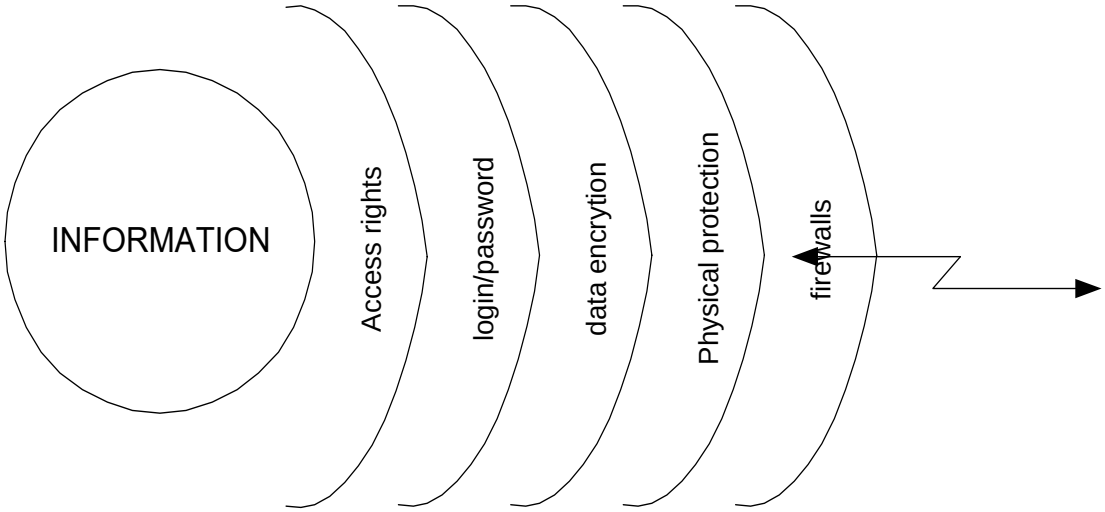
I.1.3.4. Chức năng proxy của FTPd:

Chức năng proxy server của FTPd cho phép một người sử dụng có thể truyền file từ một ftpd này tới một ftpd server khác. Sử dụng chức năng này sẽ có thể bỏ qua được các xác thực dựa trên địa chỉ IP.

Nguyên nhân là do người sử dụng có thể yêu cầu một file trên ftp server gửi một file tới bất kỳ địa chỉ IP nào. Nên người sử dụng có thể yêu cầu ftp server đó gửi một file gồm các lệnh là PORT và PASV tới các server đang nghe trên các port TCP trên bất kỳ một host nào; kết quả là một trong các host đó có ftp server chạy và tin cậy người sử dụng đó nên bỏ qua được xác thực địa chỉ IP.

I.1.4. Các mức bảo vệ an toàn mạng

Vì không có một giải pháp an toàn tuyệt đối nên người ta thường phải sử dụng đồng thời nhiều mức bảo vệ khác nhau tạo thành nhiều lớp "rào chắn" đối với các hoạt động xâm phạm. Việc bảo vệ thông tin trên mạng chủ yếu là bảo vệ thông tin cất giữ trong các máy tính, đặc biệt là trong các server của mạng. Hình sau mô tả các lớp rào chắn thông dụng hiện nay để bảo vệ thông tin tại các trạm của mạng:



Hình 1.4: Các mức độ bảo vệ mạng

Như minh hoạ trong hình trên, các lớp bảo vệ thông tin trên mạng gồm:

- Lớp bảo vệ trong cùng là quyền truy nhập nhằm kiểm soát các tài nguyên (ở đây là thông tin) của mạng và quyền hạn (có thể thực hiện những thao tác gì) trên tài nguyên đó. Hiện nay việc kiểm soát ở mức này được áp dụng sâu nhất đối với tệp.

- Lớp bảo vệ tiếp theo là hạn chế theo tài khoản truy nhập gồm đăng ký tên và mật khẩu tương ứng. Đây là phương pháp bảo vệ phổ biến nhất vì nó đơn giản, ít tốn kém và cũng rất có hiệu quả. Mỗi người sử dụng muốn truy nhập được vào mạng sử dụng các tài nguyên đều phải có đăng ký tên và mật khẩu. Người quản trị hệ thống có trách nhiệm quản lý, kiểm soát mọi hoạt động của mạng và xác định quyền truy nhập của những người sử dụng khác tuỳ theo thời gian và không gian.

- Lớp thứ ba là sử dụng các phương pháp mã hoá (encryption). Dữ liệu được biến đổi từ dạng clear text sang dạng mã hoá theo một thuật toán nào đó.

- Lớp thứ tư là bảo vệ vật lý (physical protection) nhằm ngăn cản các truy nhập vật lý bất hợp pháp vào hệ thống. Thường dùng các biện pháp truyền thống như ngăn cấm người không có nhiệm vụ vào phòng đặt máy, dùng hệ thống khoá trên máy tính, cài đặt các hệ thống báo động khi có truy nhập vào hệ thống ...

- Lớp thứ năm: Cài đặt các hệ thống bức tường lửa (firewall), nhằm ngăn chặn các thâm nhập trái phép và cho phép lọc các gói tin mà ta không muốn gửi đi hoặc nhận vào vì một lý do nào đó.

I.2. Các biện pháp bảo vệ mạng máy tính

I.2.1. Kiểm soát hệ thống qua logfile

Một trong những biện pháp dò tìm các dấu vết hoạt động trên một hệ thống là dựa vào các công cụ ghi logfile. Các công cụ này thực hiện ghi lại nhật ký các phiên làm việc trên hệ thống. Nội dung chi tiết thông tin ghi lại phụ thuộc vào cấu hình người quản trị hệ thống. Ngoài việc rà soát theo dõi hoạt động, đối với nhiều hệ thống các thông tin trong logfile giúp người quản trị đánh giá được chất lượng, hiệu năng của mạng lưới.

I.2.1.1. Hệ thống logfile trong Unix:

Trong Unix, các công cụ ghi log tạo ra logfile là các file dưới dạng text thông thường cho phép người sử dụng dùng những công cụ soạn thảo file text bất kỳ để có thể đọc được nội dung. Tuy nhiên, một số trường hợp logfile được ghi dưới dạng binary và chỉ có thể sử dụng một số tiện ích đặc biệt mới có thể đọc được thông tin.

a) Logfile lastlog:

Tiện ích này ghi lại những lần truy nhập gần đây đối với hệ thống. Các thông tin ghi lại gồm tên người truy nhập, thời điểm, địa chỉ truy nhập ... Các chương trình login sẽ đọc nội dung file lastlog, kiểm tra theo UID truy nhập vào hệ thống và sẽ thông báo lần truy nhập vào hệ thống gần đây nhất. Ví dụ như sau:

```
Last login: Fri Sep 15 2000 14:11:38
Sun Microsystems Inc.   SunOS 5.7       Generic October 1998
No mail.
Sun Microsystems Inc.   SunOS 5.7       Generic October 1998
```

```
/export/home/ptthanh
```

b) Logfile UTMP

Logfile này ghi lại thông tin về những người đang login vào hệ thống, thường nằm ở thư mục /etc/utmp. Để xem thông tin trong logfile có thể sử dụng các tiện ích như who, w, finger, rwho, users. Ví dụ nội dung của logfile dùng lệnh who như sau:

```
/export/home/vhai% who
root      console     Aug 10 08:45    (:0)
ptthanh     pts/4       Sep 15 15:27    (203.162.0.87)
ptthanh     pts/6       Sep 15 15:28    (203.162.0.87)
root      pts/12      Sep  7 16:35    (:0.0)
root      pts/13      Sep  7 11:35    (:0.0)
root      pts/14      Sep  7 11:39    (:0.0)
```

c) Logfile WTMP

Logfile này ghi lại các thông tin về các hoạt động login và logout vào hệ thống. Nó có chức năng tương tự với logfile UTMP. Ngoài ra còn ghi lại các thông tin về các lần shutdown, reboot hệ thống, các phiên truy nhập hoặc ftp và thường nằm ở thư mục /var/adm/wtmp. Logfile này thường được xem bằng lệnh "last". Ví dụ nội dung như sau:

```
/export/home/vhai% last | more
ptthanh     pts/10      203.162.0.85          Mon Sep 18 08:44   still logged in
ptthanh    pts/10                             Sat Sep 16 16:52 - 16:52  (00:00)
vtoan    pts/10      203.162.0.87            Fri Sep 15 15:30 - 16:52 (1+01:22)
vtoan    pts/6       203.162.0.87      Fri Sep 15 15:28   still logged in
vtoan    pts/4                              Fri Sep 15 15:12 - 15:12  (00:00)
```

d) Tiện ích Syslog

Đây là một công cụ ghi logfile rất hữu ích, được sử dụng rất thông dụng trên các hệ thống UNIX. Tiện ích syslog giúp người quản trị hệ thống dễ dàng trong việc thực hiện ghi logfile đối với các dịch vụ khác nhau. Thông thường tiện ích syslog thường được chạy dưới dạng một daemon và được kích hoạt khi hệ thống khởi động. Daemon syslogd lấy thông tin từ một số nguồn sau:

- /dev/log: Nhận các messages từ các tiến trình hoạt động trên hệ thống

- /dev/klog: nhận messages từ kernel

- port 514: nhận các messages từ các máy khác qua port 514 UDP.

Khi syslogd nhận các messages từ các nguồn thông tin này nó sẽ thực hiện kiểm tra file cấu hình của dịch vụ là syslog.conf để tạo log file tương ứng. Có thể cấu hình file syslog.conf để tạo một message với nhiều dịch vụ khác nhau.

Ví dụ nội dung một file syslog.conf như sau:

```
# This file is processed by m4 so be careful to quote (`') names
# that match m4 reserved words.  Also, within ifdef's, arguments
# containing commas must be quoted.
#
*.err;kern.notice;auth.notice                  /dev/console
*.err;kern.debug;daemon.notice;mail.crit       /var/adm/messages

*.alert;kern.err;daemon.err                    operator
*.alert                                        root

*.emerg                                        *

# if a non-loghost machine chooses to have authentication messages
```

Trong nội dung file syslog.conf chỉ ra, đối với các message có dạng *.emerg (message có tính khẩn cấp) sẽ được thông báo tới tất cả người sử dụng trên hệ thống; Đối với các messages có dạng *.err, hoặc kern.debug và những hoạt động truy cập không hợp pháp sẽ được ghi log trong file /var/adm/messages.

Mặc định, các messages được ghi vào logfile /var/adm/messages.

e) Tiện ích sulog

Bất cứ khi nào người sử dụng dùng lệnh "su" để chuyển sang hoạt động hệ thống dưới quyền một user khác đều được ghi log thông qua tiện ích sulog. Những thông tin logfile này được ghi vào logfile /var/adm/sulog. Tiện ích này cho phép phát hiện các trường hợp dùng quyền root để có được quyền của một user nào khác trên hệ thống.

Ví dụ nội dung của logfile sulog như sau:

```
# more /var/adm/sulog
SU 01/04 13:34 + pts/1 ptthanh-root
SU 01/04 13:53 + pts/6 ptthanh-root
SU 01/04 14:19 + pts/6 ptthanh-root
SU 01/04 14:39 + pts/1 ptthanh-root
```

f) Tiện ích cron

Tiện ích cron sẽ ghi lại logfile của các hoạt động thực hiện bởi lệnh crontabs. Thông thường, logfile của các hoạt động cron lưu trong file /var/log/cron/log. Ngoài ra, có thể cấu hình syslog để ghi lại các logfile của hoạt động cron.

Ví dụ nội dung của logfile cron như sau:

```
# more /var/log/cron/log
! *** cron started ***   pid = 2367 Fri Aug  4 16:32:38 2000
>  CMD: /export/home/mrtg/mrtg /export/home/mrtg/termcount.cfg
>  ptthanh 2386 c Fri Aug  4 16:34:01 2000
<  ptthanh 2386 c Fri Aug  4 16:34:02 2000
>  CMD: /export/home/mrtg/getcount.pl
>  ptthanh 2400 c Fri Aug  4 16:35:00 2000
<  ptthanh 2400 c Fri Aug  4 16:35:10 2000
>  CMD: /export/home/mrtg/mrtg /export/home/mrtg/termcount.cfg
```

g) Logfile của sendmail

Hoạt động ghi log của sendmail có thể được ghi qua tiện ích syslog. Ngoài ra chương trình sendmail còn có lựa chọn "-L + level security" với mức độ bảo mật từ "debug" tới "crit" cho phép ghi lại logfile. Vì sendmail là một chương trình có nhiều bug, với nhiều lỗ hổng bảo mật nền người quản trị hệ thống thường xuyên nên ghi lại logfile đối với dịch vụ này.

h) Logfile của dịch vụ FTP

Hầu hết các daemon FTP hiện nay đều cho phép cấu hình để ghi lại logfile sử dụng dịch vụ FTP trên hệ thống đó. Hoạt động ghi logfile của dịch vụ FTP thường được sử dụng với lựa chọn "-l", cấu hình cụ thể trong file /etc/inetd.conf như sau:

```
# more /etc/inetd.conf
ftp    stream  tcp    nowait  root   /etc/ftpd/in.ftpd      in.ftpd -l
```

Sau đó cấu hình syslog.conf tương ứng với dịch vụ FTP; cụ thể như sau:

```
#  Logfile FTP
daemon.info                          ftplogfile
```

Với lựa chọn này sẽ ghi lại nhiều thông tin quan trọng trong một phiên ftp như: thời điểm truy nhập, địa chỉ IP, dữ liệu get/put ... vào site FTP đó. Ví dụ nội dung logfile của một phiên ftp như sau:

```
Sun Jul 16 21:55:06 2000 12 nms 8304640 /export/home/ptthanh/PHSS_17926.depot b _ o r ptthanh ftp 0 * c
Sun Jul 16 21:56:45 2000 96 nms 64624640 /export/home/ptthanh/PHSS_19345.depot b _ o r ptthanh ftp 0 * c
Sun Jul 16 21:57:41 2000 4 nms 3379200 /export/home/ptthanh/PHSS_19423.depot b _ o r ptthanh ftp 0 * c
Sun Jul 16 22:00:38 2000 174 nms 130396160 /export/home/ptthanh/PHSS_19987.depot b _ o r ptthanh ftp 0 * c
```

i) Logfile của dịch vụ Web:

Tùy thuộc vào Web server sử dụng sẽ có các phương thức và cấu hình ghi logfile của dịch vụ Web khác nhau. Hầu hết các web server thông dụng hiện nay đều hỗ trợ cơ chế ghi log. Ví dụ nội dung logfile của dịch vụ Web sử dụng Web server Netscape như sau:

```
202.167.123.170 - - [03/Aug/2000:10:59:43 +0700] "GET /support/cgi-bin/search.pl HTTP/1.0" 401 223
203.162.46.67 - - [03/Sep/2000:22:50:52 +0700] "GET http://www.geocities.com/ HTTP/1.1" 401 223
203.162.0.85 - - [15/Sep/2000:07:43:17 +0700] "GET /support/cgi-bin/search.pl HTTP/1.0" 401 223
203.162.0.85 - ptthanh [15/Sep/2000:07:43:22 +0700] "GET /support/cgi-bin/search.pl HTTP/1.0" 404 207
203.162.0.85 - - [15/Sep/2000:07:43:17 +0700] "GET /support/cgi-bin/search.pl HTTP/1.0" 401 223
```

I.2.1.2. Một số công cụ hữu ích hỗ trợ phân tích logfile:

Đối với người quản trị, việc phân tích logfile của các dịch vụ là hết sức quan trọng. Một số công cụ trên mạng giúp người quản trị thực hiện công việc này dễ dàng hơn, đó là:

- Tiện ích chklastlog và chkwtmp giúp phân tích các logfile lastlog và WTMP theo yêu cầu người quản trị.

- Tiện ích netlog giúp phân tích các gói tin, gồm 3 thành phần:

+ TCPlogger: log lại tất cả các kết nối TCP trên một subnet

+ UDPlogger: log lại tất cả các kết nối UDP trên một subnet

+ Extract: Xử lý các logfile ghi lại bởi TCPlogger và UDBlogger.

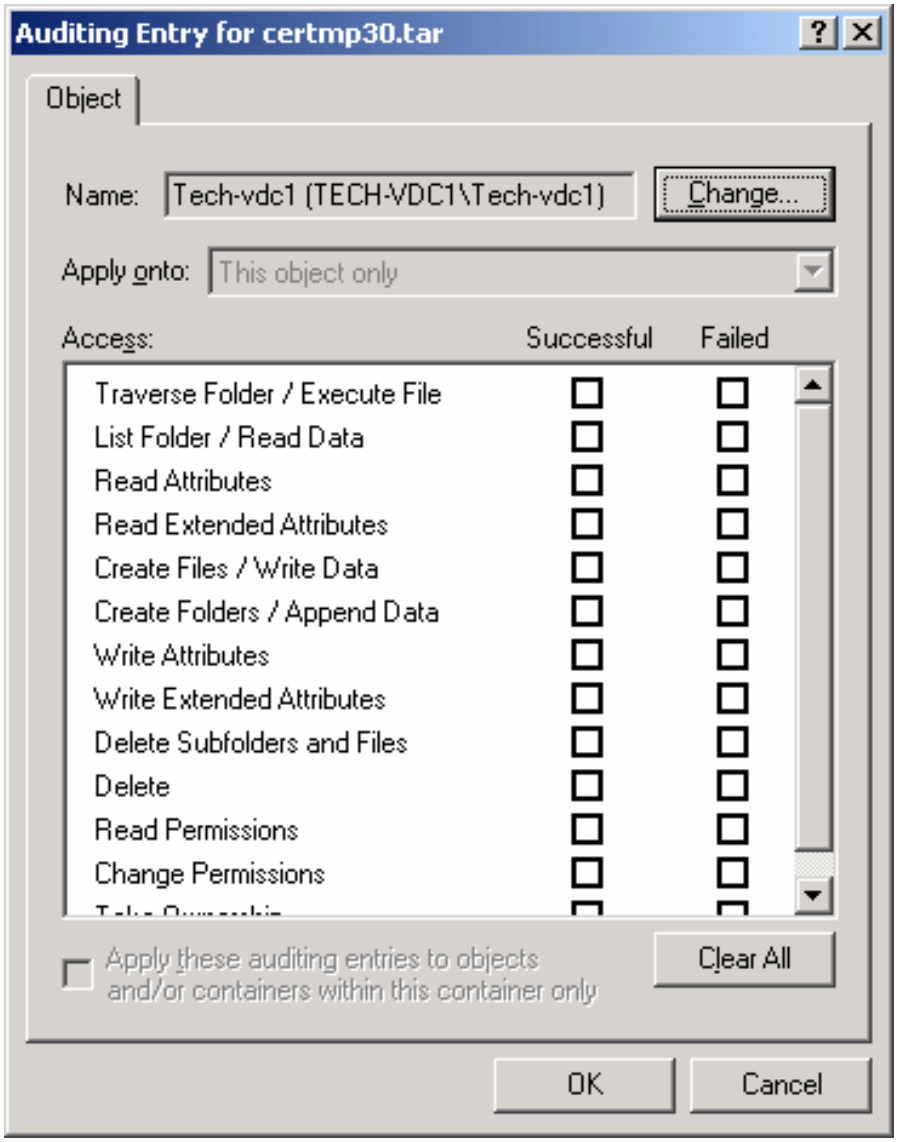
- Tiện ích TCP wrapper: Tiện ích này cho phép người quản trị hệ thống dễ dàng giám sát và lọc các gói tin TCP của các dịch vụ như systat, finger, telnet, rlogin, rsh, talk ...

I.2.1.3. Các công cụ ghi log thường sử dụng trong Windows NT và 2000:

Trong hệ thống Windows NT 4.0 và Windows 2000 hiện nay đều hỗ trợ đầy đủ các cơ chế ghi log với các mức độ khác nhau. Người quản trị hệ thống tùy thuộc vào mức độ an toàn của dịch vụ và các thông tin sử dụng có thể lựa chọn các mức độ ghi log khác nhau. Ngoài ra, trên hệ thống Windows NT còn hỗ trợ các cơ chế ghi logfile trực tiếp vào các database để tạo báo cáo giúp người quản trị phân tích và kiểm tra hệ thống nhanh chóng và thuận tiện. Sử dụng tiện ích event view để xem các thông tin logfile trên hệ thống với các mức độ như Application log; Security log; System log. Các hình dưới đây sẽ minh hoạ một số hoạt động ghi logfile trên hệ thống Windows:

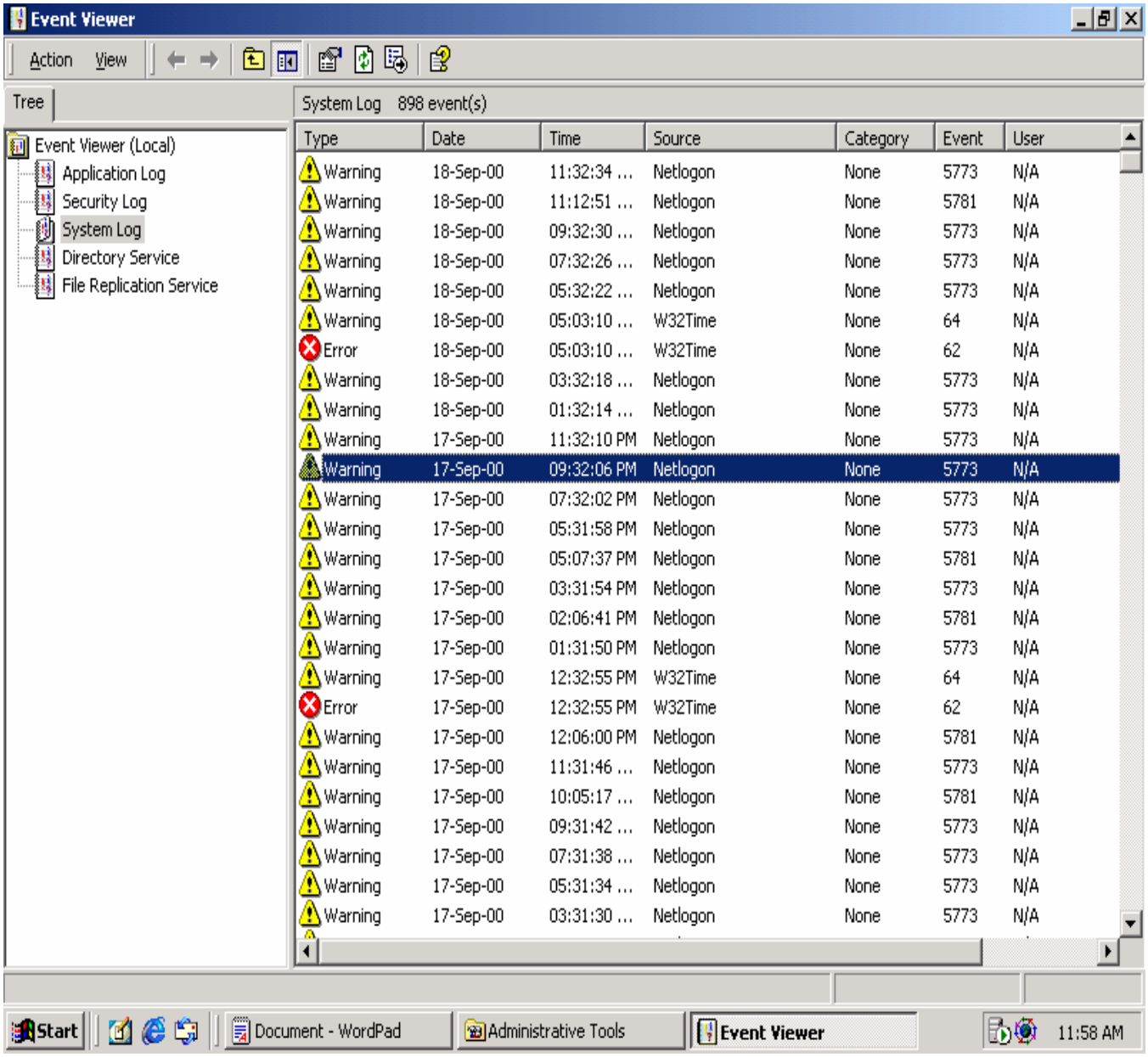
Ví dụ: Để ghi lại hoạt động đọc, viết, truy nhập.... đối với một file/thư mục là thành công hay không thành công người quản trị có thể cấu hình như sau:

Chọn File Manager - User Manager - Security - Auditing. Ví dụ hình sau minh họa các hoạt động có thể được ghi log trong Windows 2000:



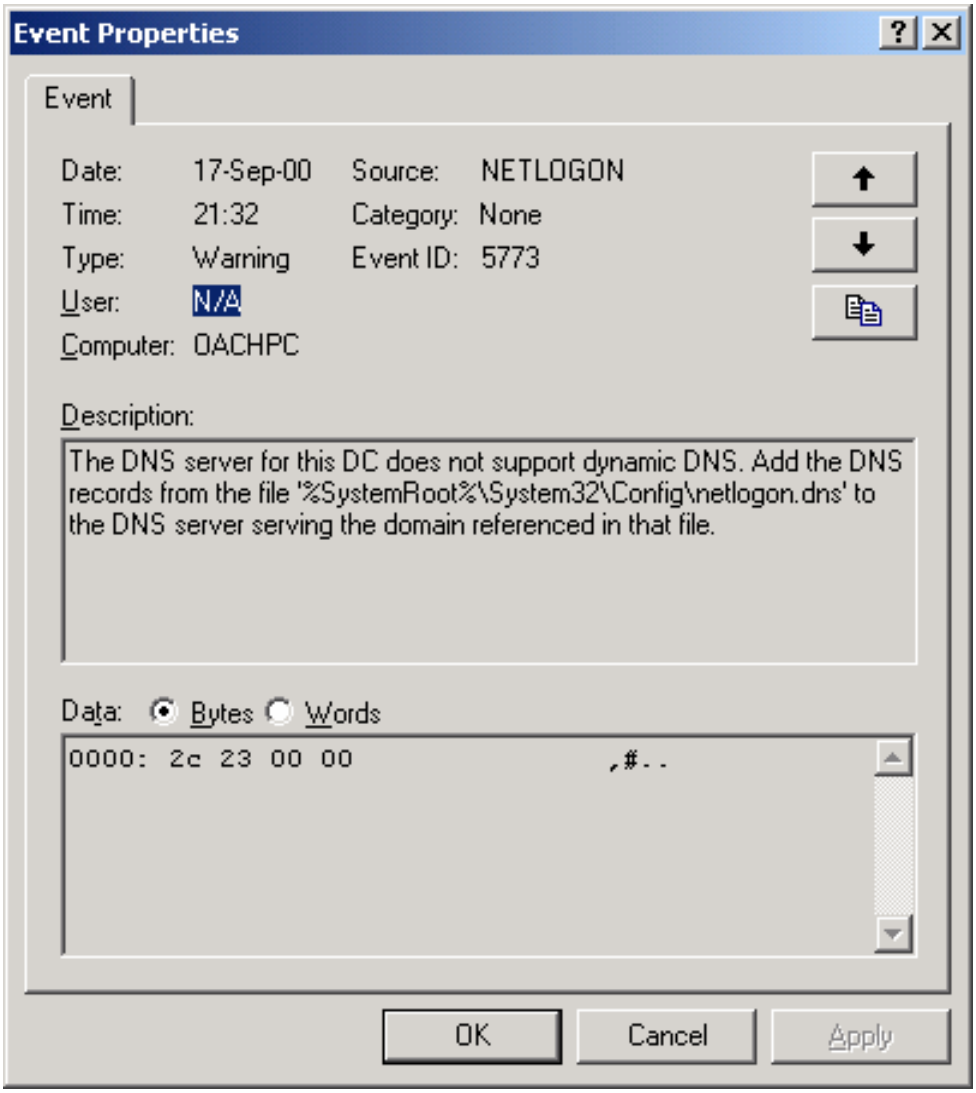
Hình 1.5: Ghi log trong Windows 2000

- Sử dụng tiện ích Event View cho phép xem những thông tin logfile như sau:



Hình 1.6: Công cụ Event View của Windows 2000

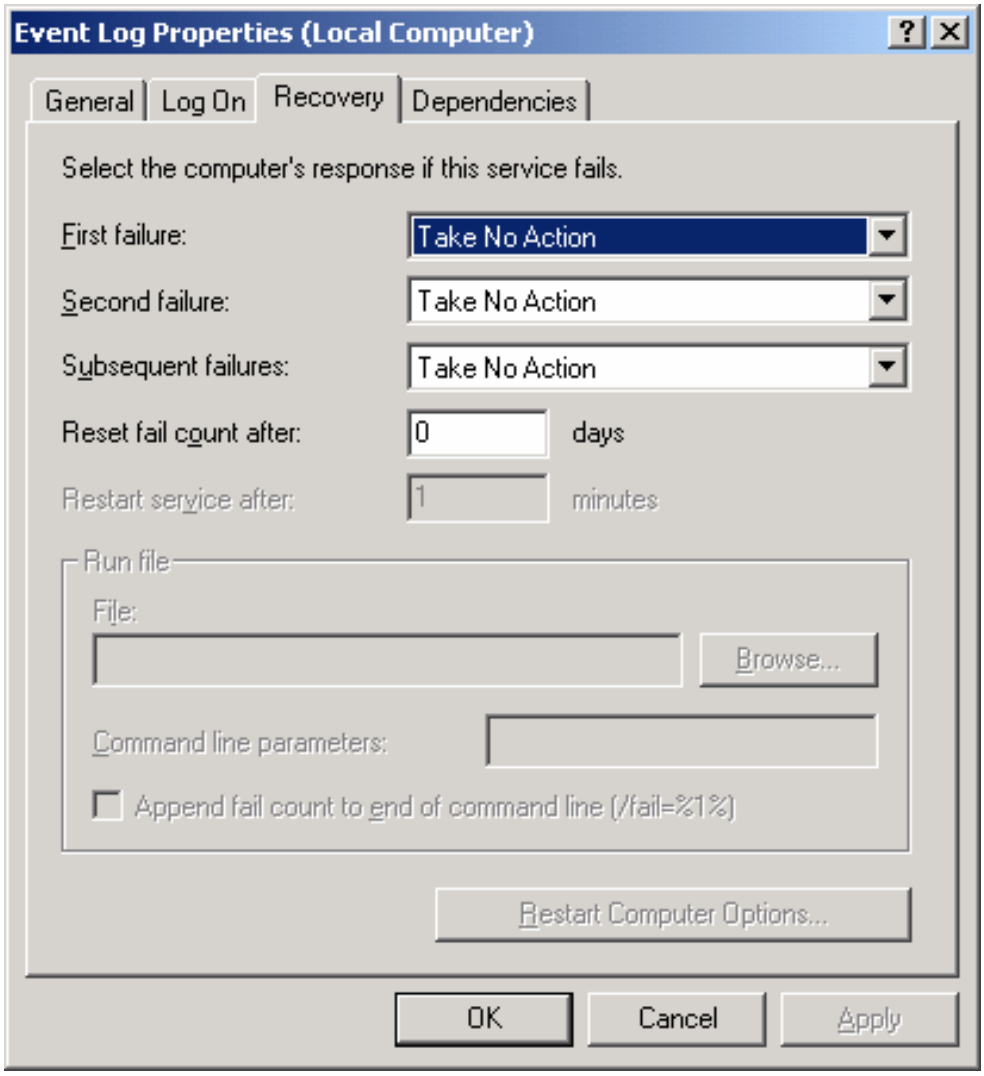
Xem chi tiết nội dung một message:



Hình 1.7: Chi tiết 1 thông báo lỗi trong Windows 2000

Thông báo này cho biết nguyên nhân, thời điểm xảy ra lỗi cũng như nhiều thông tin quan trọng khác.

Có thể cấu hình Event Service để thực hiện một action khi có một thông báo lỗi xảy ra như sau:



Hình 1.8: Cấu hình dịchvụ ghi log trong Windows 2000

Ngoài ra, cũng giống như trên UNIX, trong Windows NT cũng có các công cụ theo dõi logfile của một số dịch vụ thông dụng như FTP, Web. Tùy thuộc vào loại server sử dụng có các phương pháp cấu hình khác nhau.

I.2.2. Thiếp lập chính sách bảo mật hệ thống

Trong các bước xây dựng một chính sách bảo mật đối với một hệ thống, nhiệm vụ đầu tiên của người quản trị là xác định được đúng mục tiêu cần bảo mật. Việc xác định những mục tiêu của chính sách bảo mật giúp người sử dụng biết được trách nhiệm của mình trong việc bảo vệ các tài nguyên thông tin trên mạng, đồng thời giúp các nhà quản trị thiết lập các biện pháp đảm bảo hữu

hiệu trong quá trình trang bị, cấu hình và kiểm soát hoạt động của hệ thống. Những mục tiêu bảo mật bao gồm:

I.2.2.1. Xác định đối tượng cần bảo vệ:

Đây là mục tiêu đầu tiên và quan trọng nhất trong khi thiết lập một chính sách bảo mật. Người quản trị hệ thống cần xác định rõ những đối tượng nào là quan trọng nhất trong hệ thống cần bảo vệ và xác định rõ mức độ ưu tiên đối với những đối tượng đó. Ví dụ các đối tượng cần bảo vệ trên một hệ thống có thể là: các máy chủ dịch vụ, các router, các điểm truy nhập hệ thống, các chương trình ứng dụng, hệ quản trị CSDL, các dịch vụ cung cấp ...

Trong bước này cần xác định rõ phạm vi và ranh giới giữa các thành phần trong hệ thống để khi xảy ra sự cố trên hệ thống có thể cô lập các thành phần này với nhau, dễ dàng dò tìm nguyên nhân và cách khắc phục. Có thể chia các thành phần trên một hệ thống theo các cách sau:

- Phân tách các dịch vụ tùy theo mức độ truy cập và độ tin cậy.

- Phân tách hệ thống theo các thành phần vật lý như các máy chủ (server), router, các máy trạm (workstation)...

- Phân tách theo phạm vi cung cấp của các dịch vụ như: các dịch vụ bên trong mạng (NIS, NFS ...) và các dịch vụ bên ngoài như Web, FTP, Mail ...

I.2.2.2. Xác định nguy cơ đối với hệ thống

Các nguy cơ đối với hệ thống chính là các lỗ hổng bảo mật của các dịch vụ hệ thống đó cung cấp. Việc xác định đúng đắn các nguy cơ này giúp người quản trị có thể tránh được những cuộc tấn công mạng, hoặc có biện pháp bảo vệ đúng đắn. Thông thường, một số nguy cơ này nằm ở các thành phần sau trên hệ thống:

a) Các điểm truy nhập:

Các điểm truy nhập của hệ thống bất kỳ (Access Points) thường đóng vai trò quan trọng đối với mỗi hệ thống vì đây là điểm đầu tiên mà người sử dụng cũng như những kẻ tấn công mạng quan tâm tới. Thông thường các điểm truy nhập thường phục vụ hầu hết người dùng trên mạng, không phụ thuộc vào quyền hạn cũng như dịch vụ mà người sử dụng dùng. Do đó, các điểm truy nhập thường là thành phần có tính bảo mật lỏng lẻo. Mặt khác, đối với nhiều hệ

thống còn cho phép người sử dụng dùng các dịch vụ như Telnet, rlogin để truy nhập vào hệ thống, đây là những dịch vụ có nhiều lỗ hổng bảo mật.

b) Không kiểm soát được cấu hình hệ thống

Không kiểm soát hoặc mất cấu hình hệ thống chiếm một tỷ lệ lớn trong số các lỗ hổng bảo mật. Ngày nay, có một số lượng lớn các phần mềm sử dụng, yêu cầu cấu hình phức tạp và đa dạng hơn, điều này cũng dẫn đến những khó khăn để người quản trị nắm bắt được cấu hình hệ thống. Để khắc phục hiện tượng này, nhiều hãng sản xuất phần mềm đã đưa ra những cấu hình khởi tạo mặc định, trong khi đó những cấu hình này không được xem xét kỹ lưỡng trong một môi trường bảo mật. Do đó, nhiệm vụ của người quản trị là phải nắm được hoạt động của các phần mềm sử dụng, ý nghĩa của các file cấu hình quan trọng, áp dụng các biện pháp bảo vệ cấu hình như sử dụng phương thức mã hóa hashing code (MD5).

c) Những bug phần mềm sử dụng

Những bug phần mềm tạo nên những lỗ hổng của dịch vụ là cơ hội cho các hình thức tấn công khác nhau xâm nhập vào mạng. Do đó, người quản trị phải thường xuyên cập nhật tin tức trên các nhóm tin về bảo mật và từ nhà cung cấp phần mềm để phát hiện những lỗi của phần mềm sử dụng. Khi phát hiện có bug cần thay thế hoặc ngừng sử dụng phần mềm đó chờ nâng cấp lên phiên bản tiếp theo.

d) Những nguy cơ trong nội bộ mạng

Một hệ thống không những chịu tấn công từ ngoài mạng, mà có thể bị tấn công ngay từ bên trong. Có thể là vô tình hoặc cố ý, các hình thức phá hoại bên trong mạng vẫn thường xảy ra trên một số hệ thống lớn. Chủ yếu với hình thức tấn công ở bên trong mạng là kẻ tấn công có thể tiếp cận về mặt vật lý đối với các thiết bị trên hệ thống, đạt được quyền truy nhập bất hợp pháp tại ngay hệ thống đó. Ví dụ nhiều trạm làm việc có thể chiếm được quyền sử dụng nếu kẻ tấn công ngồi ngay tại các trạm làm việc đó.

I.2.2.3. Xác định phương án thực thi chính sách bảo mật

Sau khi thiết lập được một chính sách bảo mật, một hoạt động tiếp theo là lựa chọn các phương án thực thi một chính sách bảo mật. Một chính sách

bảo mật là hoàn hảo khi nó có tình thực thi cao. Để đánh giá tính thực thi này, có một số tiêu chí để lựa chọn đó là:

- Tính đúng đắn
- Tính thân thiện
- Tính hiệu quả

I.2.2.4. Thiết lập các qui tắc/thủ tục

a) Các thủ tục đối với hoạt động truy nhập bất hợp pháp

Sử dụng một vài công cụ có thể phát hiện ra các hành động truy nhập bất hợp pháp vào một hệ thống. Các công cụ này có thể đi kèm theo hệ điều hành, hoặc từ các hãng sản xuất phần mềm thứ ba. Đây là biện pháp phổ biến nhất để theo dõi các hoạt động hệ thống.

- Các công cụ logging: hầu hết các hệ điều hành đều hỗ trợ một số lượng lớn các công cụ ghi log với nhiều thông tin bổ ích. Để phát hiện những hoạt động truy nhập bất hợp pháp, một số qui tắc khi phân tích logfile như sau:

+ So sánh các hoạt động trong logfile với các log trong quá khứ. Đối với các hoạt động thông thường, các thông tin trong logfile thường có chu kỳ giống nhau như thời điểm người sử dụng login hoặc log out, thời gian sử dụng các dịch vụ trên hệ thống...

+ Nhiều hệ thống sử dụng các thông tin trong logfile để tạo hóa đơn cho khách hàng. Có thể dựa vào các thông tin trong hóa đơn thanh toán để xem xét các truy nhập bất hợp pháp nếu thấy trong hóa đơn đó có những điểm bất thường như thời điểm truy nhập, số điện thoại lạ ...

+ Dựa vào các tiện ích như syslog để xem xét, đặc biệt là các thông báo lỗi login không hợp lệ (bad login) trong nhiều lần.

+ Dựa vào các tiện ích kèm theo hệ điều hành để theo dõi các tiến trình đang hoạt động trên hệ thống; để phát hiện những tiến trình lạ, hoặc những chương trình khởi tạo không hợp lệ ...

- Sử dụng các công cụ giám sát khác: Ví dụ sử dụng các tiện ích về mạng để theo dõi các lưu lượng, tài nguyên trên mạng để phát hiện những điểm nghi ngờ.

b) Các thủ tục bảo vệ hệ thống

- Thủ tục quản lý tài khoản người sử dụng
- Thủ tục quản lý mật khẩu
- Thủ tục quản lý cấu hình hệ thống
- Thủ tục sao lưu và khôi phục dữ liệu
- Thủ tục báo cáo sự cố

I.2.2.5. Kiểm tra, đánh giá và hoàn thiện chính sách bảo mật

Một hệ thống luôn có những biến động về cấu hình, các dịch vụ sử dụng, và ngay cả nền tảng hệ điều hành sử dụng, các thiết bị phần cứng .... do vậy người thiết lập các chính sách bảo mật mà cụ thể là các nhà quản trị hệ thống luôn luôn phải rà sóat, kiểm tra lại chính sách bảo mật đảm bảo luôn phù hợp với thực tế. Mặt khác kiểm tra và đánh giá chính sách bảo mật còn giúp cho các nhà quản lý có kế hoạch xây dựng mạng lưới hiệu quả hơn.

a) Kiểm tra, đánh giá

Công việc này được thực hiện thường xuyên và liên tục. Kết quả của một chính sách bảo mật thể hiện rõ nét nhất trong chất lượng dịch vụ mà hệ thống đó cung cấp. Dựa vào đó có thể kiểm tra, đánh giá được chính sách bảo mật đó là hợp lý hay chưa. Ví dụ, một nhà cung cấp dịch vụ Internet có thể kiểm tra được chính sách bảo mật của mình dựa vào khả năng phản ứng của hệ thống khi bị tấn công từ bên ngoài như các hành động spam mail, DoS, truy nhập hệ thống trái phép ...

Hoạt động đánh giá một chính sách bảo mật có thể dựa vào một số tiêu chí sau:

- Tính thực thi.
- Khả năng phát hiện và ngăn ngừa các hoạt động phá hoại.
- Các công cụ hữu hiệu để hạn chế các hoạt động phá hoại hệ thống.

b) Hoàn thiện chính sách bảo mật:

Từ các hoạt động kiểm tra, đánh giá nêu trên, các nhà quản trị hệ thống có thể rút ra được những kinh nghiệm để có thể cải thiện chính sách bảo mật

hữu hiệu hơn. Cải thiện chính sách có thể là những hành động nhằm đơn giản công việc người sử dụng, giảm nhẹ độ phức tạp trên hệ thống ...

Những hoạt động cải thiện chính sách bảo mật có thể diễn ra trong suốt thời gian tồn tại của hệ thống đó. Nó gắn liền với các công việc quản trị và duy trì hệ thống. Đây cũng chính là một yêu cầu trong khi xây dựng một chính sách bảo mật, cần phải luôn luôn mềm dẻo, có những thay đổi phù hợp tùy theo điều kiện thực tế.

II. Tổng quan về hệ thống firewall

II.1. Giới thiệu về Firewall

II.1.1. Khái niệm Firewall

Firewall là thiết bị nhằm ngăn chặn sự truy nhập không hợp lệ từ mạng ngoài vào mạng trong. Hệ thống firewall thường bao gồm cả phần cứng và phần mềm. Firewall thường được dùng theo phương thức ngăn chặn hay tạo các luật đối với các địa chỉ khác nhau.

II.1.2. Các chức năng cơ bản của Firewall

Chức năng chính của Firewall là kiểm soát luồng thông tin giữa mạng cần bảo vệ (Trusted Network) và Internet thông qua các chính sách truy nhập đã đợc thiết lập.

- Cho phép hoặc cấm các dịch vụ truy nhập từ trong ra ngoài và từ ngoài vào trong.

- Kiểm soát địa chỉ truy nhập, và dịch vụ sử dụng.

- Kiểm soát khả năng truy cập người sử dụng giữa 2 mạng.

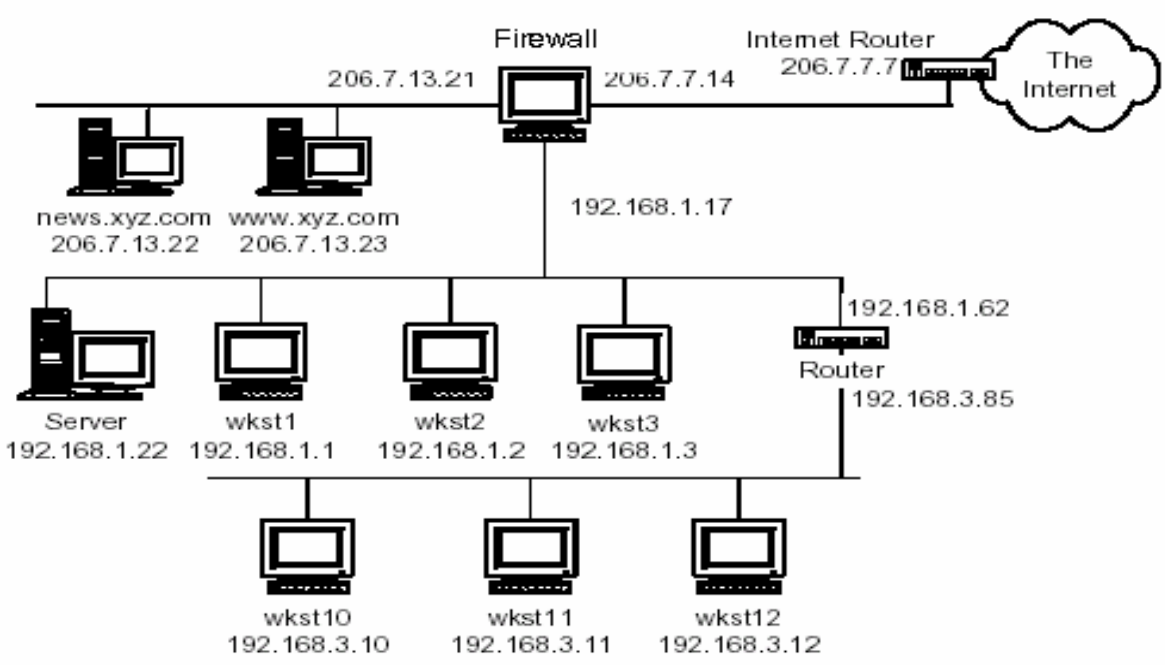
- Kiểm soát nội dung thông tin truyền tải giữa 2 mạng.

- Ngăn ngừa khả năng tấn công từ các mạng ngoài.

Xây dựng firewalls là một biện pháp khá hữu hiệu, nó cho phép bảo vệ và kiểm soát hầu hết các dịch vụ do đó được áp dụng phổ biến nhất trong các biện pháp bảo vệ mạng. Thông thường, một hệ thống firewall là một cổng (gateway) giữa mạng nội bộ giao tiếp với mạng bên ngoài và ngược lại

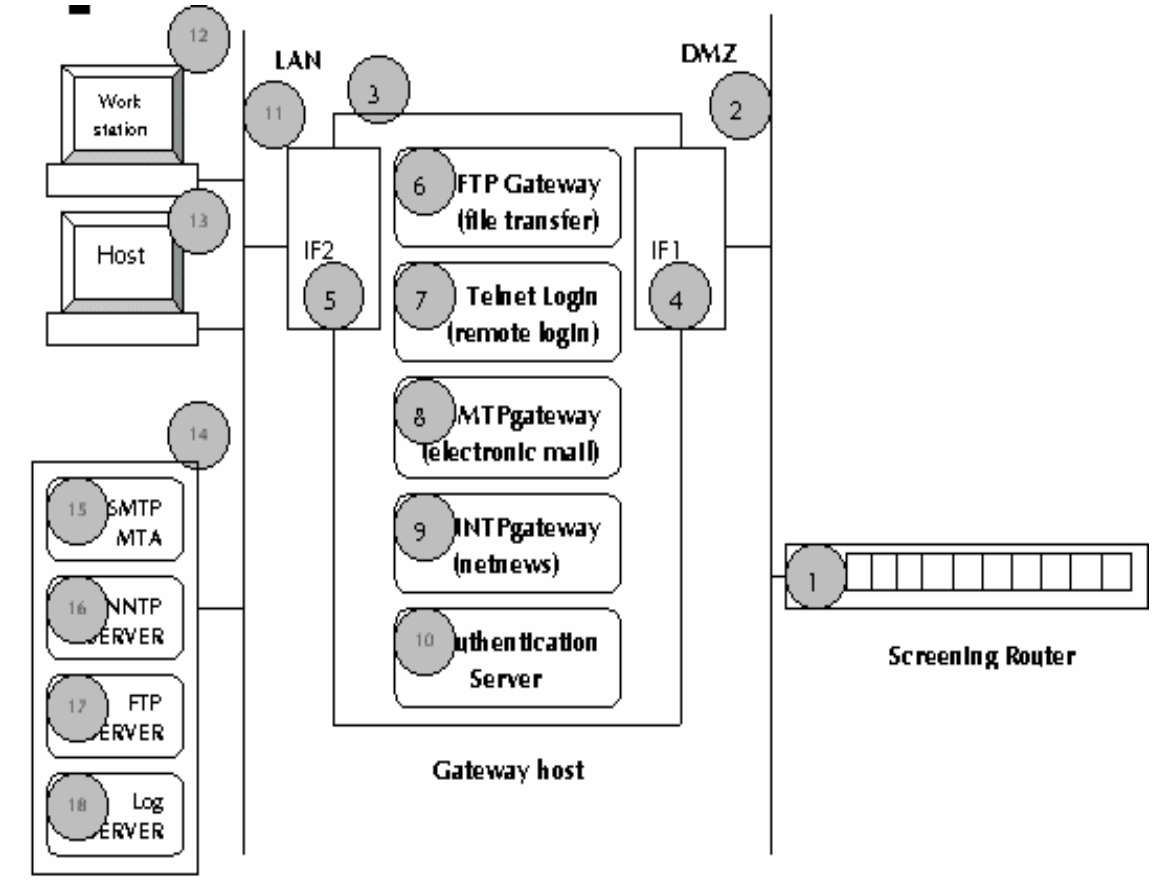
II.1.3. Mô hình mạng sử dụng Firewall

Kiến trúc của hệ thống có firewall như sau:



Hình 2.1: Kiến trúc hệ thống có firewall

Nhìn chung, mỗi hệ thống firewall đều có các thành phần chung như sau:



Hình 2.2: Các thành phần của hệ thống firewall

Firewall có thể bao gồm phần cứng hoặc phần mềm nhưng thường là cả hai. Về mặt phần cứng thì firewall có chức năng gần giống một router, nó cho phép hiển thị các địa chỉ IP đang kết nối qua nó. Điều này cho phép bạn xác định được các địa chỉ nào được phép và các địa chỉ IP nào không được phép kết nối.

Tất cả các firewall đều có chung một thuộc tính là cho phép phân biệt đối xử hay khả năng từ chối truy nhập dựa trên các địa chỉ nguồn.

Theo hình trên các thành phần của một hệ thống firewall bao gồm:

- Screening router: Là chặng kiểm soát đầu tiên cho LAN.

- DMZ: Khu "phi quân sự", là vùng có nguy cơ bị tấn công từ Internet.

- Gateway: là cổng ra vào giữa mạng LAN và DMZ, kiểm soát mọi liên lạc, thực thi các cơ chế bảo mật.

- IF1: Interface 1: Là card giao tiếp với vùng DMZ.

- IF2: Interface 2: Là card giao tiếp với vùng mạng LAN.

- FTP gateway: Kiểm soát truy cập FTP giữa LAN và vùng DMZ. Các truy cập ftp từ mạng LAN ra Internet là tự do. Các truy cập FTP vào LAN đòi hỏi xác thực thông qua Authentication Server.

- Telnet Gateway: Kiểm soát truy cập telnet giữa mạng LAN và Internet. Giống như FTP, người dùng có thể telnet ra ngoài tự do, các telnet từ ngoài vào yêu cầu phải xác thực qua Authentication Server

- Authentication Server: được sử dụng bởi các cổng giao tiếp, nhận diện các yêu cầu kết nối, dùng các kỹ thuật xác thực mạnh như one-time password/token (mật khẩu sử dụng một lần). Các máy chủ dịch vụ trong mạng LAN được bảo vệ an toàn, không có kết nối trực tiếp với Internet, tất cả các thông tin trao đổi đều được kiểm soát qua gateway.

II.1.4. Phân loại Firewall

Có khá nhiều loại firewall, mỗi loại có những ưu và nhược điểm riêng. Tuy nhiên để thuận tiện cho việc nghiên cứu người ta chia hệ thống làm 2 loại chính:

- Packet filtering: là hệ thống firewall cho phép chuyển thông tin giữa hệ thống trong và ngoài mạng có kiểm soát.

- Application-proxy firewall: là hệ thống firewall thực hiện các kết nối thay cho các kết nối trực tiếp từ máy khách yêu cầu.

II.1.4.1. Packet Filtering:

Kiểu firewall chung nhất là kiểu dựa trên mức mạng của mô hình OSI. Firewall mức mạng thường hoạt động theo nguyên tắc router hay còn được gọi là router, có nghĩa là tạo ra các luật cho phép quyền truy nhập mạng dựa trên mức mạng. Mô hình này hoạt động theo nguyên tắc lọc gói tin (packet filtering).

Ở kiểu hoạt động này các gói tin đều được kiểm tra địa chỉ nguồn nơi chúng xuất phát. Sau khi địa chỉ IP nguồn được xác định thì nó được kiểm tra với các luật đã được đặt ra trên router. Ví dụ người quản trị firewall quyết định rằng không cho phép bất kỳ một gói tin nào xuất phát từ mạng microsoft.com

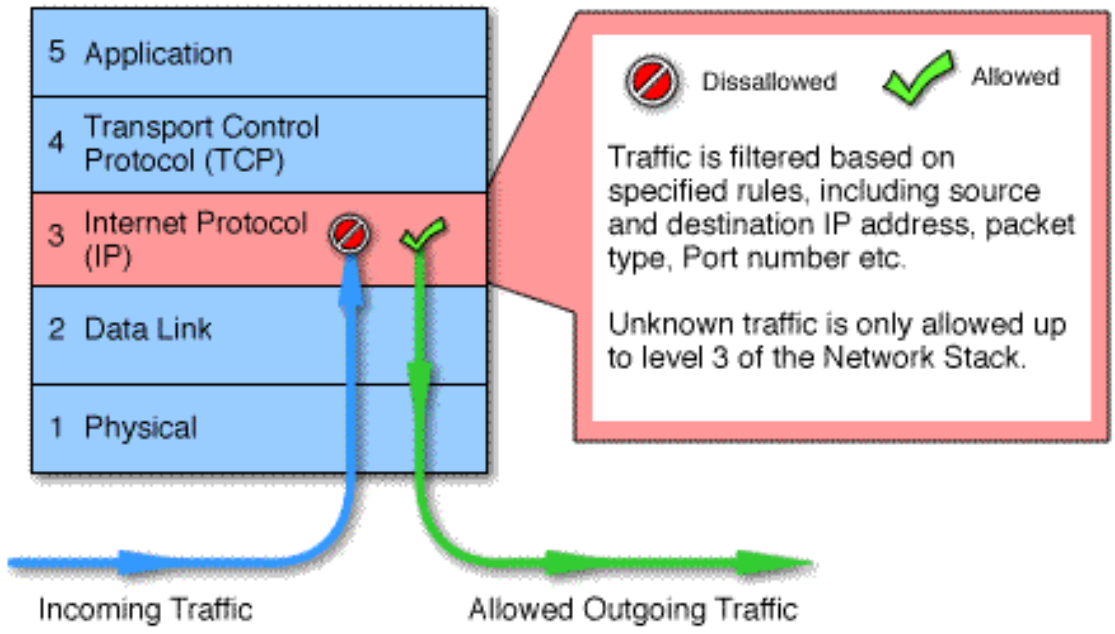
được kết nối với mạng trong thì các gói tin xuất phát từ mạng này sẽ không bao giờ đến được mạng trong.

Các firewall hoạt động ở lớp mạng (tương tự như một router) thường cho phép tốc độ xử lý nhanh bởi nó chỉ kiểm tra địa chỉ IP nguồn mà không có một lệnh thực sự nào trên router, nó không cần một khoảng thời gian nào để xác định xem là địa chỉ sai hay bị cấm. Nhưng điều này bị trả giá bởi tính tin cậy của nó. Kiểu firewall này sử dụng địa chỉ IP nguồn làm chỉ thị, điều này tạo ra một lỗ hổng là nếu một gói tin mang địa chỉ nguồn là địa chỉ giả thì như vậy nó sẽ có được một số mức truy nhập vào mạng trong của bạn.

Tuy nhiên có nhiều biện pháp kỹ thuật có thể được áp dụng cho việc lọc gói tin nhằm khắc phục yếu điểm này. Ví dụ như đối với các công nghệ packet filtering phức tạp thì không chỉ có trường địa chỉ IP được kiểm tra bởi router mà còn có các trường khác nữa được kiểm tra với các luật được tạo ra trên firewall, các thông tin khác này có thể là thời gian truy nhập, giao thức sử dụng, port ...

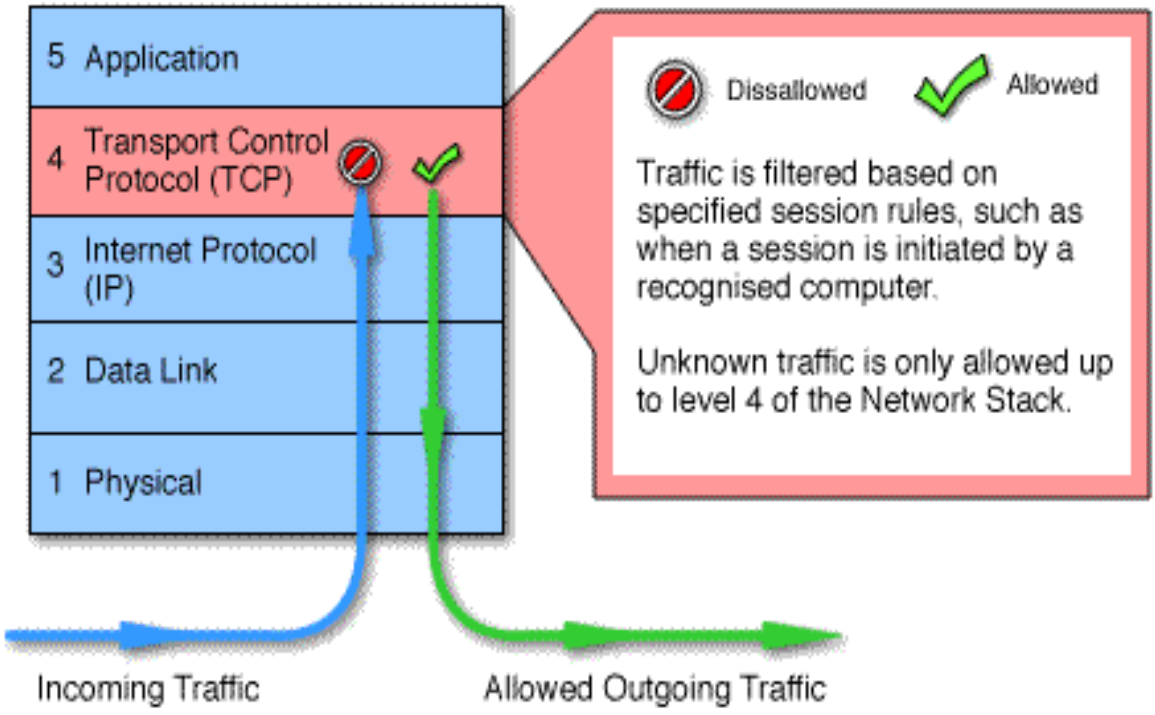
Firewall kiểu Packet Filtering có thể được phân thành 2 loại:

a) Packet filtering firewall: hoạt động tại lớp mạng của mô hình OSI hay lớp IP trong mô hình giao thức TCP/IP.



Hình 2.3: Packet filtering firewall

b) Circuit level gateway: hoạt động tại lớp phiên (session) của mô hình OSI hay lớp TCP trong mô hình giao thức TCP/IP.



Hình 2.4: Circuit level gateway

II.1.4.2. Application-proxy firewall

Kiểu firewall này hoạt động dựa trên phần mềm. Khi một kết nối từ một người dùng nào đó đến mạng sử dụng firewall kiểu này thì kết nối đó sẽ bị chặn lại, sau đó firewall sẽ kiểm tra các trường có liên quan của gói tin yêu cầu kết nối. Nếu việc kiểm tra thành công, có nghĩa là các trường thông tin đáp ứng được các luật đã đặt ra trên firewall thì firewall sẽ tạo một cái cầu kết nối giữa hai node với nhau.

Ưu điểm của kiểu firewall loại này là không có chức năng chuyển tiếp các gói tin IP, hơn nữa ta có thể điều khiển một cách chi tiết hơn các kết nối thông qua firewall. Đồng thời nó còn đưa ra nhiều công cụ cho phép ghi lại các quá trình kết nối. Tất nhiên điều này phải trả giá bởi tốc độ xử lý, bởi vì tất cả các kết nối cũng như các gói tin chuyển qua firewall đều được kiểm tra kỹ

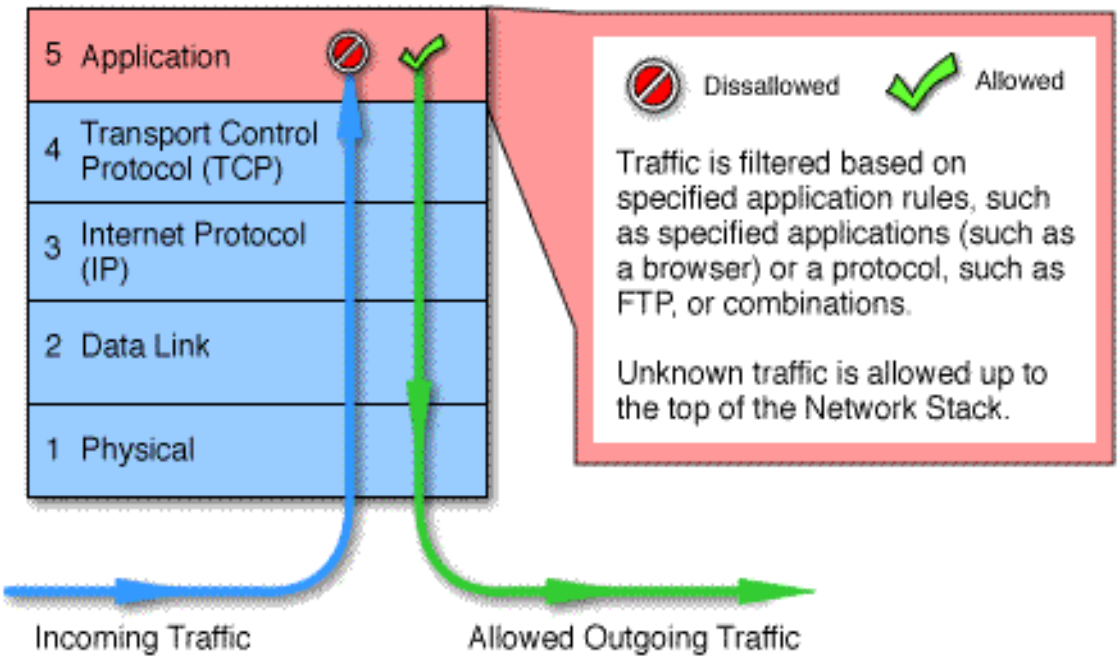
lưỡng với các luật trên firewall và rồi nếu được chấp nhận sẽ được chuyển tiếp tới node đích.

Sự chuyển tiếp các gói tin IP xảy ra khi một máy chủ nhận được một yêu cầu từ mạng ngoài rồi chuyển chúng vào mạng trong. Điều này tạo ra một lỗ hổng cho các kẻ phá hoại (hacker) xâm nhập từ mạng ngoài vào mạng trong.

Nhược điểm của kiểu firewall hoạt động dựa trên ứng dụng là phải tạo cho mỗi dịch vụ trên mạng một trình ứng dụng uỷ quyền (proxy) trên firewall ví dụ như phải tạo một trình ftp proxy dịch vụ ftp, tạo trình http proxy cho dịch vụ http... Như vậy ta có thể thấy rằng trong kiểu giao thức client-server như dịch vụ telnet làm ví dụ thì cần phải thực hiện hai bước để cho hai máy ngoài mạng và trong mạng có thể kết nối được với nhau. Khi sử dụng firewall kiểu này các máy client (máy yêu cầu dịch vụ) có thể bị thay đổi. Ví dụ như đối với dịch vụ telnet thì các máy client có thể thực hiện theo hai phương thức: một là bạn telnet vào firewall trước sau đó mới thực hiện việc telnet vào máy ở mạng khác; cách thứ hai là bạn có thể telnet thẳng tới đích tuỳ theo các luật trên firewall có cho phép hay không mà việc telnet của bạn sẽ được thực hiện. Lúc này firewall là hoàn toàn trong suốt, nó đóng vai trò như một cầu nối tới đích của bạn.

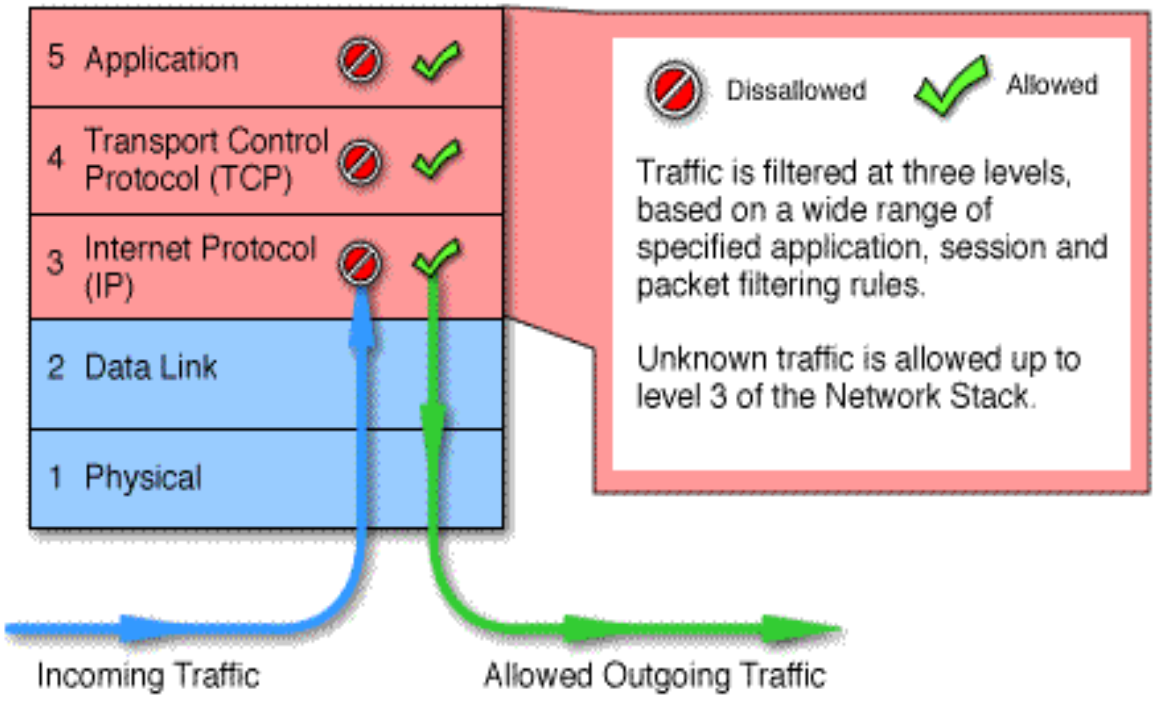
Firewall kiểu Application-proxy có thể được phân thành 2 loại:

a) Application level gateway: tính năng tương tự như loại circuit-level gateway nhưng lại hoạt động ở lớp ứng dụng trong mô hình giao thức TCP/IP.



Hình 2.5: Application level gateway

b) Stateful multilayer inspection firewall: đây là loại kết hợp được các tính năng của các loại firewall trên: lọc các gói tại lớp mạng và kiểm tra nội dung các gói tại lớp ứng dụng. Firewall loại này cho phép các kết nối trực tiếp giữa các client và các host nên giảm được các lỗi xảy ra do tính chất "không trong suốt" của firewall kiểu Application gateway. Stateful multilayer inspection firewall cung cấp các tính năng bảo mật cao và lại trong suốt đối với các end users.



Hình 2.6: Stateful multilayer inspection firewall

II.2. Một số phần mềm Firewall thông dụng

II.2.1. Packet filtering:

Kiểu lọc gói tin này có thể được thực hiện mà không cần tạo một firewall hoàn chỉnh, có rất nhiều các công cụ trợ giúp cho việc lọc gói tin trên Internet (kể cả phải mua hay được miễn phí). Sau đây ta có thể liệt kê một số tiện ích như vậy

II.2.1.1. TCP_Wrappers

TCP_Wrappers là một chương trình được viết bởi Wietse Venema. Chương trình hoạt động bằng cách thay thế các chương trình thường trú của hệ thống và ghi lại tất cả các yêu cầu kết nối, thời gian yêu cầu, và địa chỉ nguồn. Chương trình này cũng có khả năng ngăn chặn các địa chỉ IP hay các mạng không được phép kết nối.

II.2.1.2. NetGate

NetGate được đưa ra bởi Smallwork là một hệ thống dựa trên các luật về lọc gói tin. Nó được viết ra để sử dụng trên các hệ thống Sun Sparc OS 4.1.x. Tương tự như các kiểu packet filtering khác, NetGate kiểm tra tất cả các gói tin nó nhận được và so sánh với các luật đã được tạo ra.

II.2.1.3. Internet Packet Filter

Phần mềm này hoàn toàn miễn phí, được viết bởi Darren Reed. Đây là một chương trình khá tiện lợi, nó có khả năng ngăn chặn được việc tấn công bằng địa chỉ IP giả. Một số ưu điểm của chương trình là nó không chỉ có khả năng huỷ bỏ các gói tin TCP không đúng hoặc chưa hoàn thiện mà còn không gửi lại bản tin ICMP lỗi. Chương trình này cho phép bạn có thể kiểm tra thử các luật bạn ra trước khi sử dụng chúng.

II.2.2. Application-proxy firewall

II.2.2.1. TIS FWTK

TIS FWTK (Trusted information Systems Firewall Tool Kit) là một phần mềm đầu tiên đầy đủ tính năng của firewall và đặc trưng cho kiểu firewall hoạt động theo phương thức ứng dụng. Những phiên bản đầu tiên của phần mềm này là miễn phí và bao gồm nhiều thành phần riêng rẽ. Mỗi thành phần phục vụ cho một kiểu dịch vụ trên mạng. Các thành phần chủ yếu bao gồm: Telnet, FTP, rlogin, sendmail và http.

Phần mềm này là một hệ thống toàn diện, tuy nhiên nó không có khả năng bảo vệ mạng ngay sau khi cài đặt vì việc cài đặt và cấu hình không phải là dễ dàng. Khi cấu hình phần mềm này bạn phải thực sự hiểu mình đang làm gì bởi có thể với các luật bạn tạo ra thì mạng của bạn không thể được kết nối với bất kỳ mạng nào khác thậm chí ngay cả những mạng quen thuộc. Điểm đặc trưng nhất của phần mềm này là nó có sẵn nhiều tiện ích giúp bạn điều khiển được truy nhập đối với toàn mạng, một phần mạng hay thậm chí chỉ riêng một địa chỉ.

II.2.2.2. Raptor

Raptor là phần mềm firewall cung cấp đầy đủ các tính năng của một firewall chuyên nghiệp với hai giao diện quản lý, một trên hệ đều hành Unix (RCU) và một trên hệ điều hành Windows (RMC). Raptor có thể được cấu hình để bảo vệ mạng theo bốn phương thức: Standard Proxies, Generic Service

Passer, Virtual Private Network tunnels và Raptor Mobile. Tuy việc cấu hình cho Raptor khá phức tạp với việc tạo các route, định nghĩa các entity, user và group, thiết lập các authorization rule ... nhưng bù lại ta có thể sử dụng được rất nhiều tính năng ưu việt do Raptor cung cấp đề tuỳ biến các mức bảo vệ đối với mạng của mình.

II.3. Thực hành cài đặt và cấu hình firewall Check Point v4.0 for Windows

II.3.1. Yêu cầu phần cứng:

- Cấu hình tối thiểu đối với máy cài GUI Client

Hệ điều hành	Windows 95, Windows NT, X/Motif
Dung lượng đĩa trống	20 Mbytes
Bộ nhớ	16 Mbytes
Card mạng	Các loại card được hệ điều hành hỗ trợ
Thiết bị khác	CD-ROM

- Cấu hình tối thiểu đối với máy cài Management Server

Hệ điều hành	Windows NT (Intel x86 và Pentium)
Dung lượng đĩa trống	20 Mbytes
Bộ nhớ	tối thiểu 16MB, nên dùng 24MB
Card mạng	Các loại card được hệ điều hành hỗ trợ
Thiết bị khác	CD-ROM

- Cấu hình tối thiểu đối với máy cài Modul Firewall

Hệ điều hành	Windows NT (Intel x86 và Pentium)
Dung lượng đĩa trống	20 Mbytes
Bộ nhớ	16 Mbytes
Card mạng	Tối thiểu phải có 3 card mạng thuộc các loại card được hệ điều hành hỗ trợ.
Thiết bị khác	CD-ROM

II.3.2. Các bước chuẩn bị trước khi cài đặt:

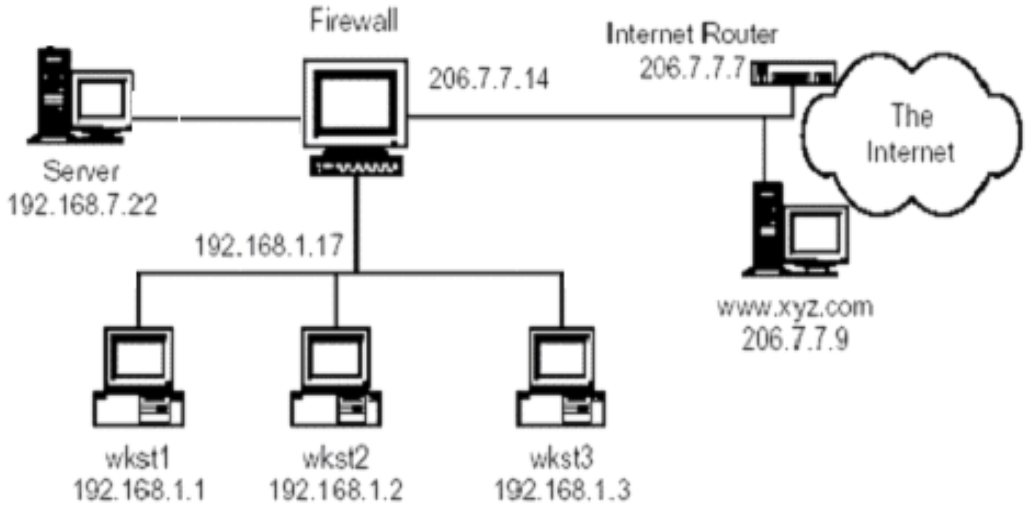
- Thắt chặt an ninh cho máy chủ cài firewall và các module của firewall như GUI Client và Management Server (tắt các dịch vụ không cần thiết, update các patch sửa lỗi của hệ điều hành ...).

- Kiểm tra các kết nối mạng trên các giao diện mạng, đảm bảo từ máy chủ cài Module Firewall có thể ping được các IP trên các giao diện mạng (sử dụng lệnh ifconfig , ping ...).

- Kiểm tra bảng Routing (sử dụng lệnh netstat -rn ...).

- Kiểm tra dịch vụ DNS (sử dụng lệnh nslookup).

- Lập sơ đồ mạng thử nghiệm, đối với máy chủ có 3 giao diện mạng có thể lập sơ đồ như sau:



Hình 2.7: Sơ đồ mạng thử nghiệm đối với máy chủ có 3 giao diện mạng

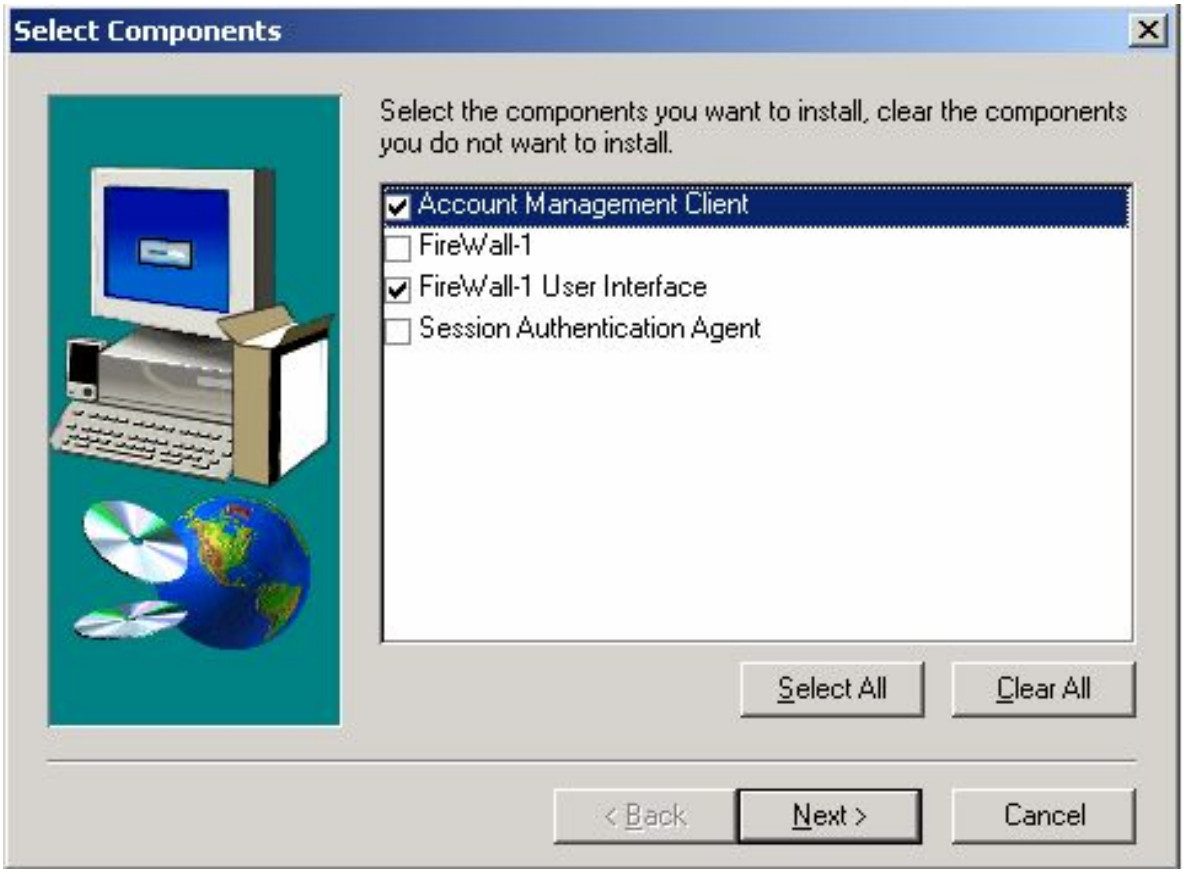
II.3.3. Tiến hành cài đặt:

Login dưới quyền Administrator và cài đặt hệ thống Firewall Checkpoint trên các máy theo trình tự sau:

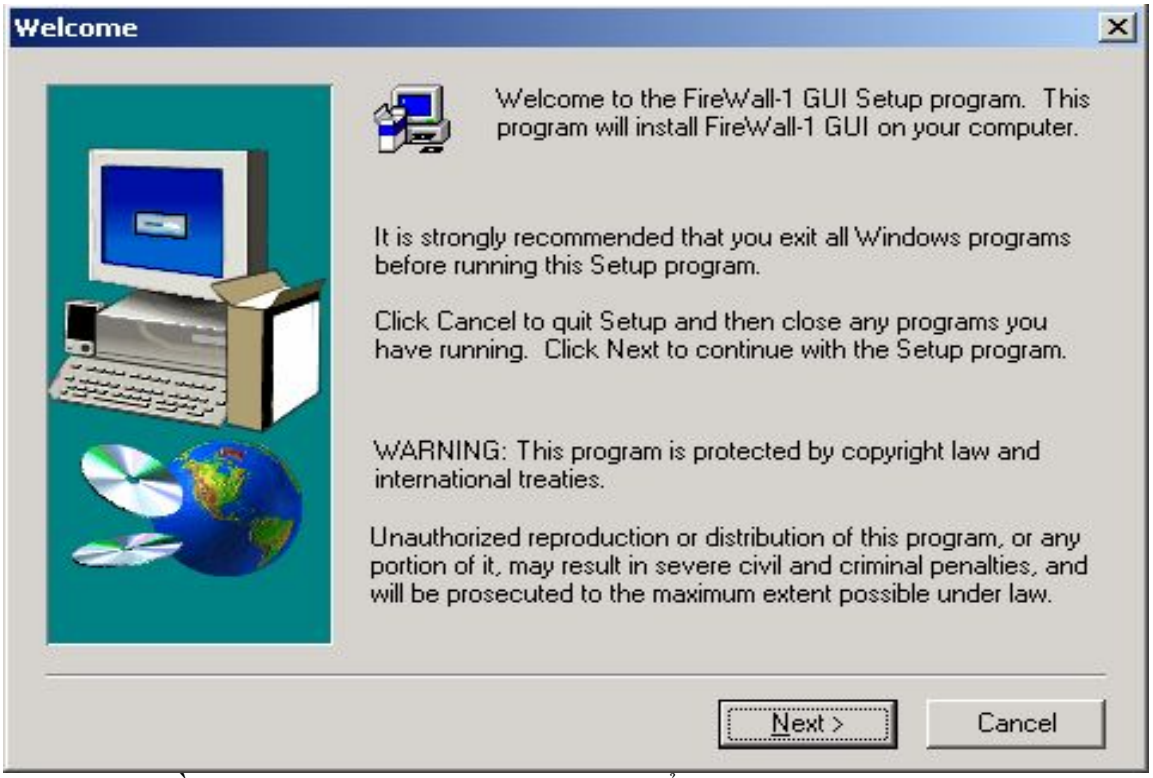
- Cài đặt GUI Client và Management Server.
- Cài đặt Module Firewall.

II.3.3.1. Cài đặt GUI Client và Management Server

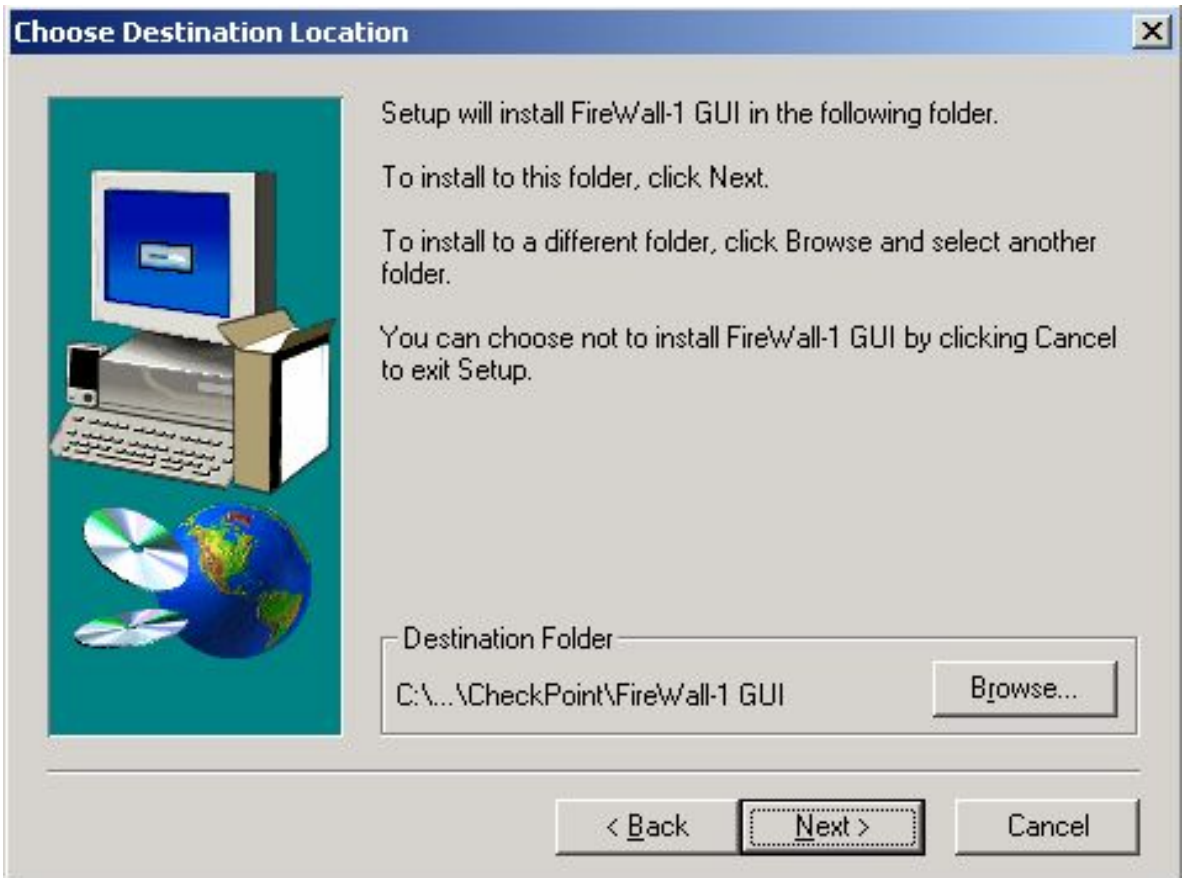
Đưa đĩa CD Checkpoint và chạy lệnh setup trong thư mục Windows, chọn Account Management Client và FireWall-1 User Interface trong cửa sổ Select Components:



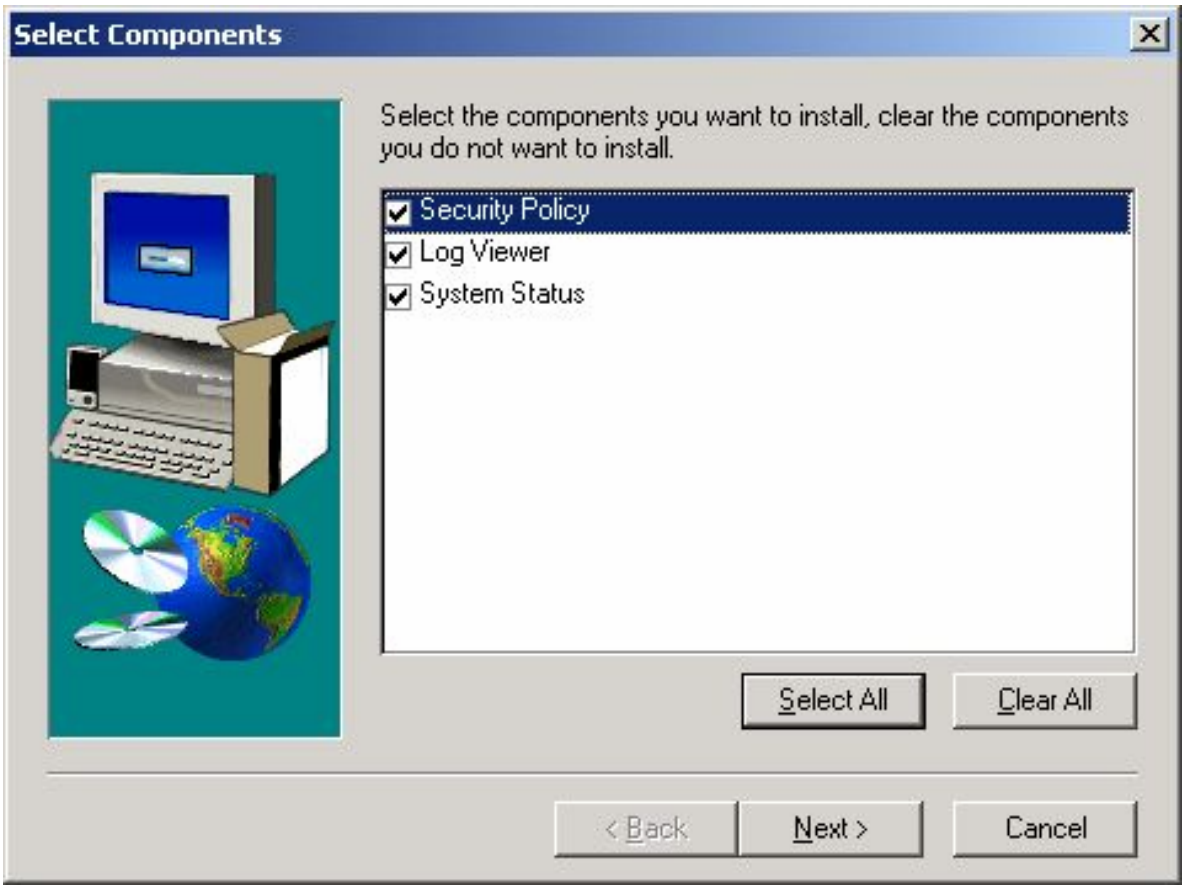
Chọn Next, màn hình sẽ hiện ra như sau:



Chọn Next rồi chọn thư mục cài đặt trong cửa sổ Choose Destination Location:



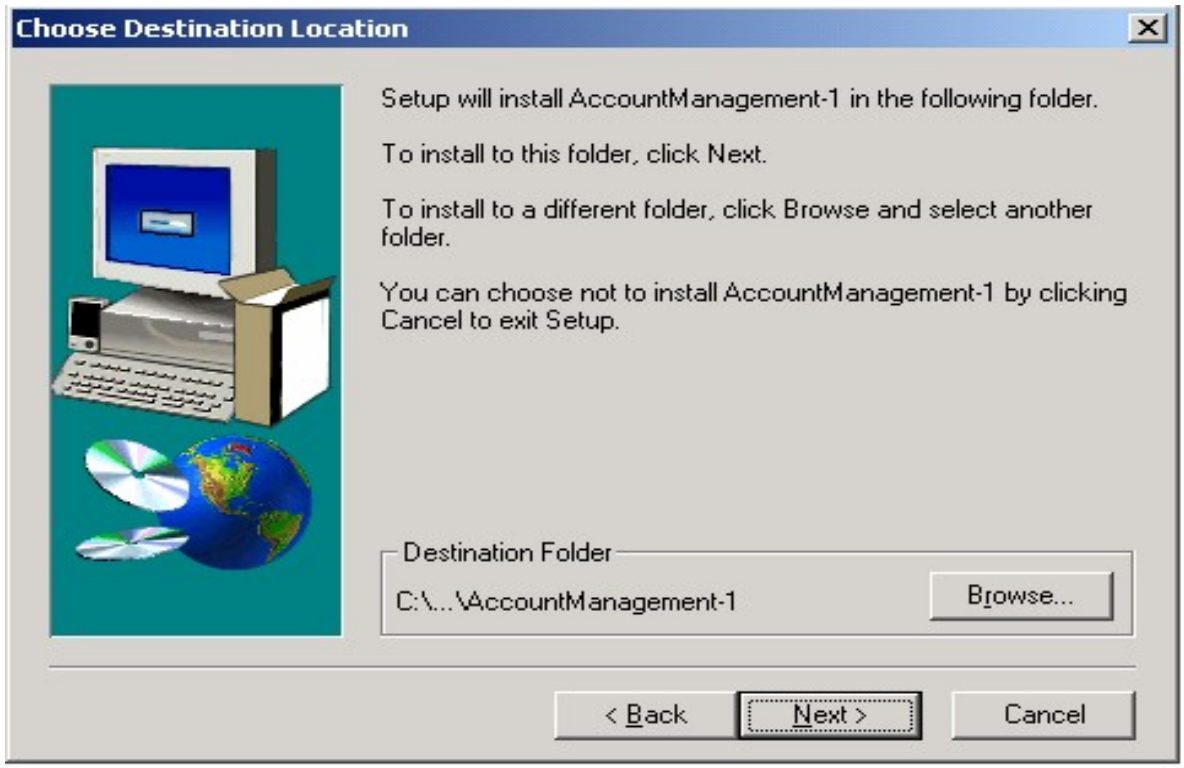
Chọn Next rồi chọn các thành phần trong cửa sổ Select Components:



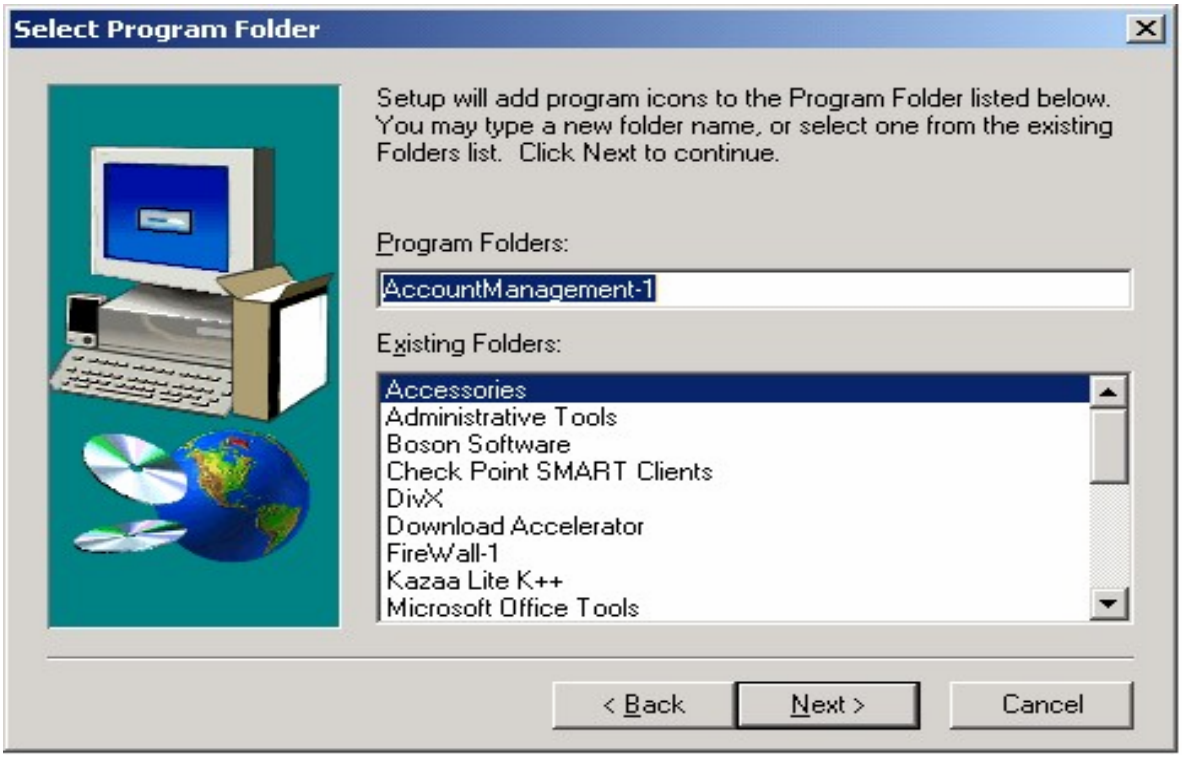
Chọn Next để bắt đầu quá trình cài đặt.

Sau khi cài xong GUI Client, màn hình sẽ tự động hiện ra phần cài đặt Account Management Client With Encryption Installation:

Chọn Next rồi chọn thư mục cài đặt trong cửa sổ Choose Destination Location:



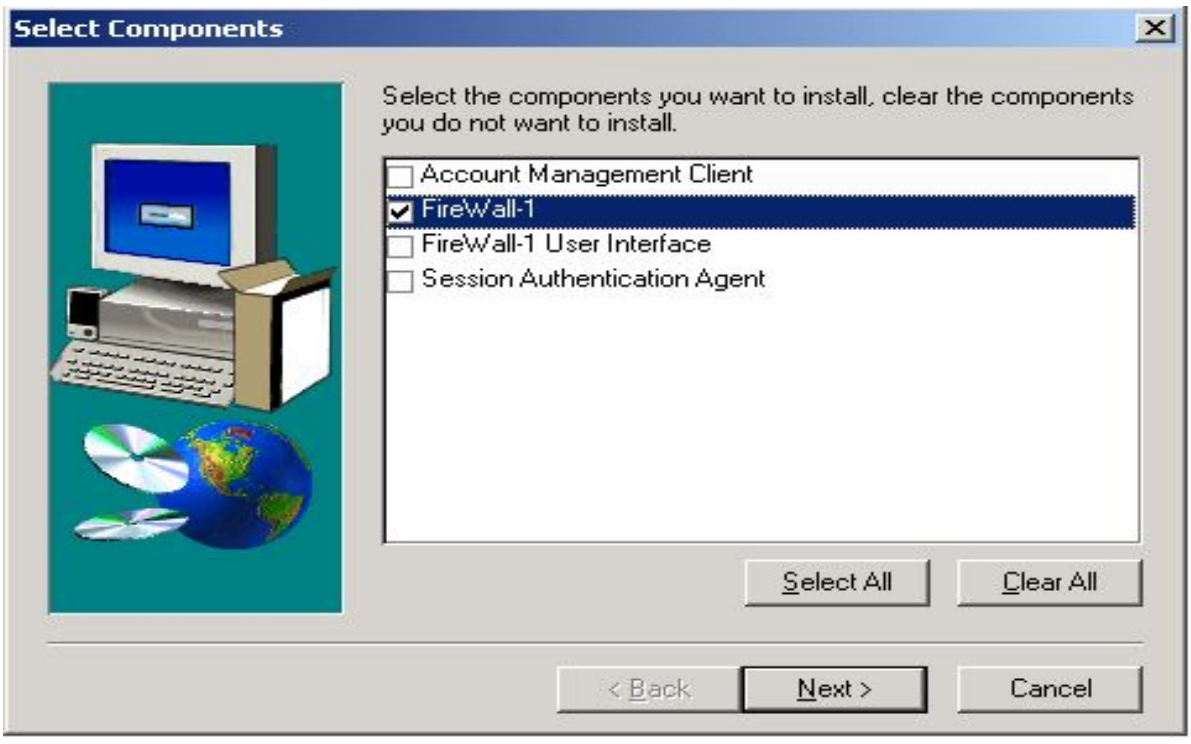
Chọn Next rồi chọn Folder trong cửa sổ Select Program Folder:



Chọn Next để bắt đầu quá trình cài đặt

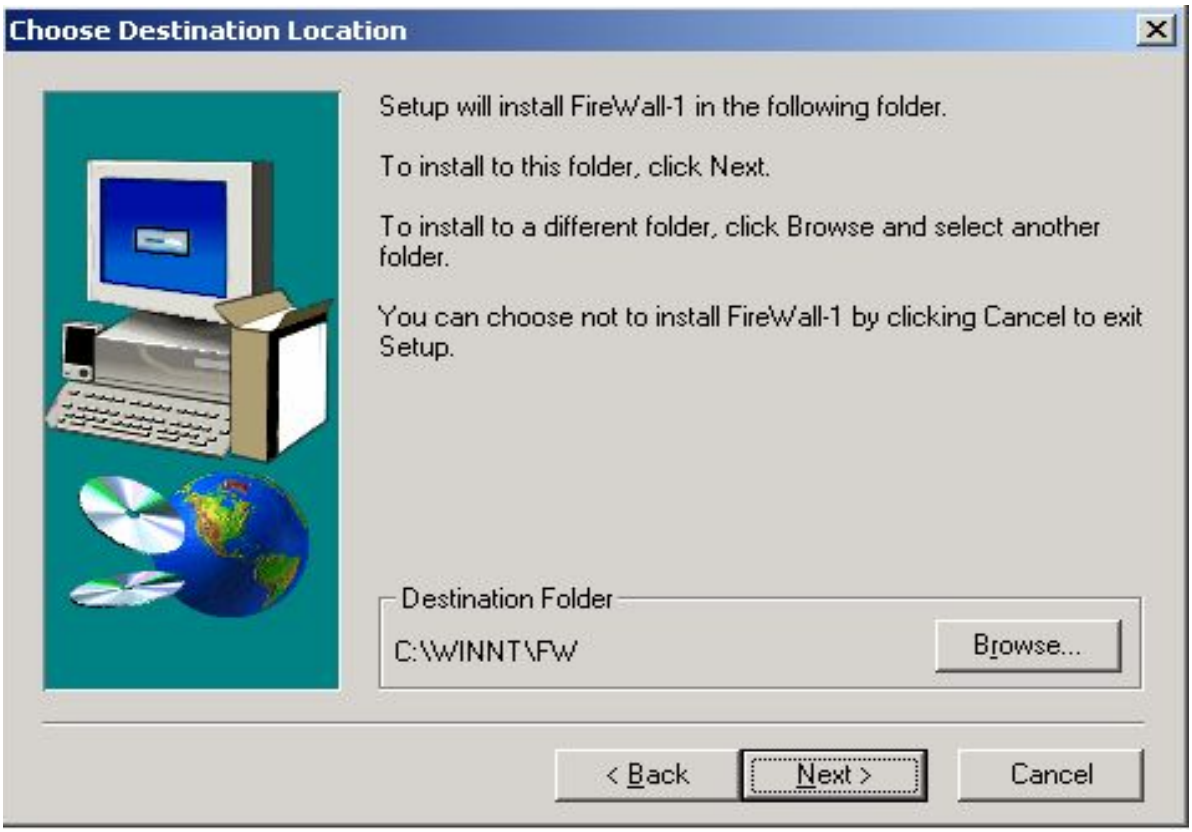
II.3.3.2. Cài đặt Module Firewall:

Chọn FireWall-1 trong cửa sổ Select Components ban đầu:



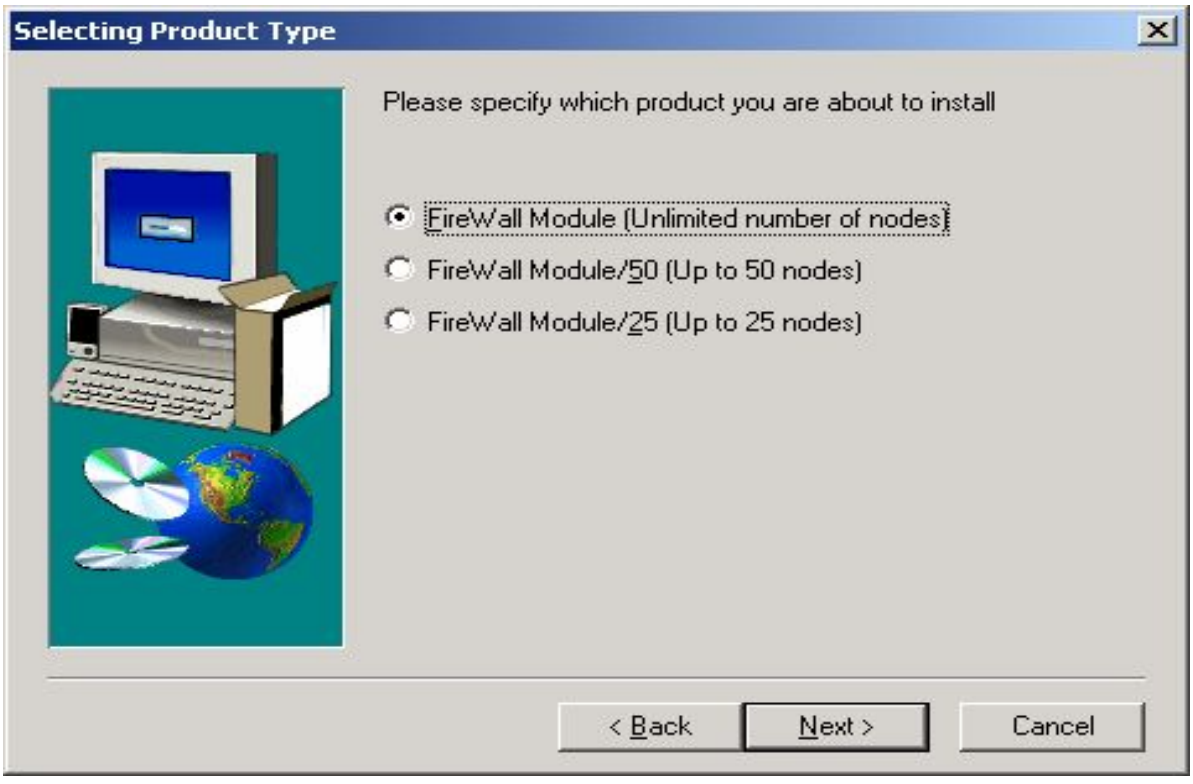
Chọn Next, màn hình sẽ hiện ra như sau:

Chọn Next rồi chọn thư mục cài đặt trong cửa sổ Choose Destination Location:



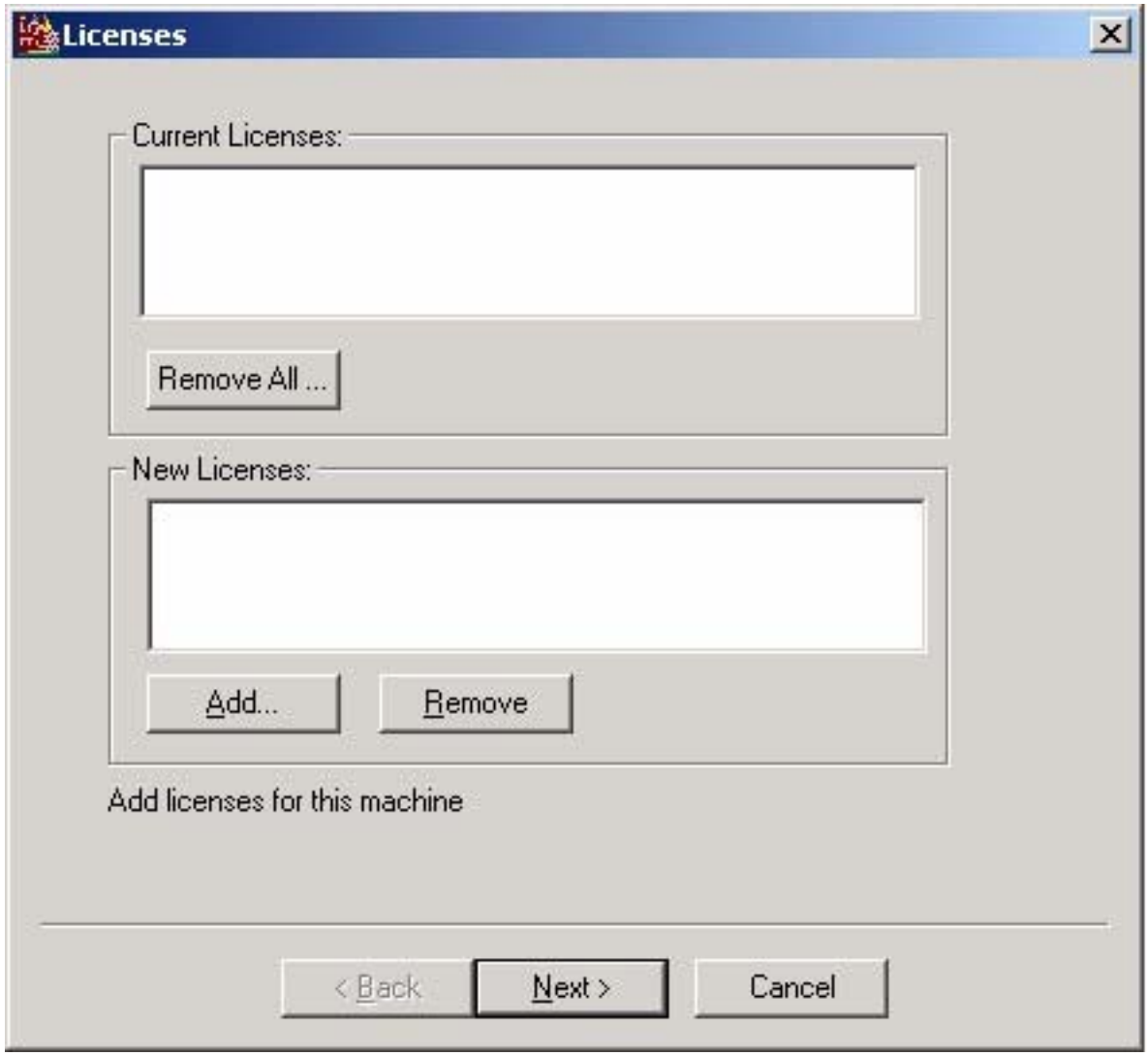
Chọn Next rồi chọn FireWall-1 FireWall Module trong cửa sổ Selecting Product Type:

Chọn Next rồi tùy theo phiên bản Checkpoint đăng ký để chọn số license phù hợp:

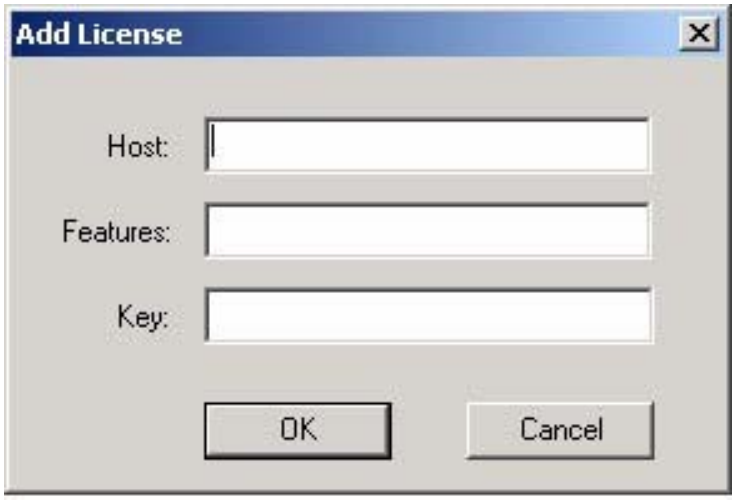


Chọn Next để bắt đầu quá trình cài đặt.

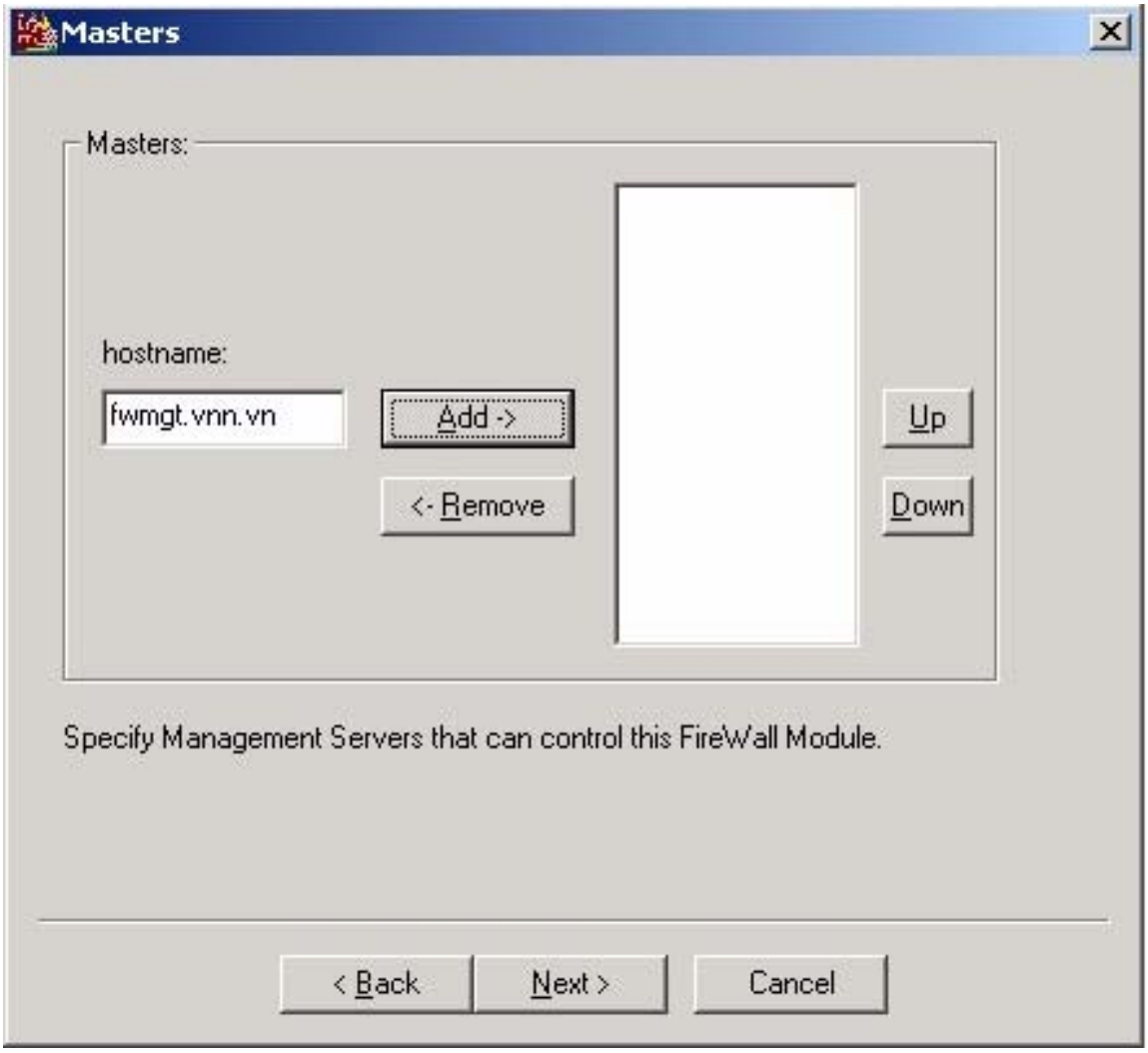
Sau khi cài xong, màn hình cài đặt license sẽ hiện lên như sau:



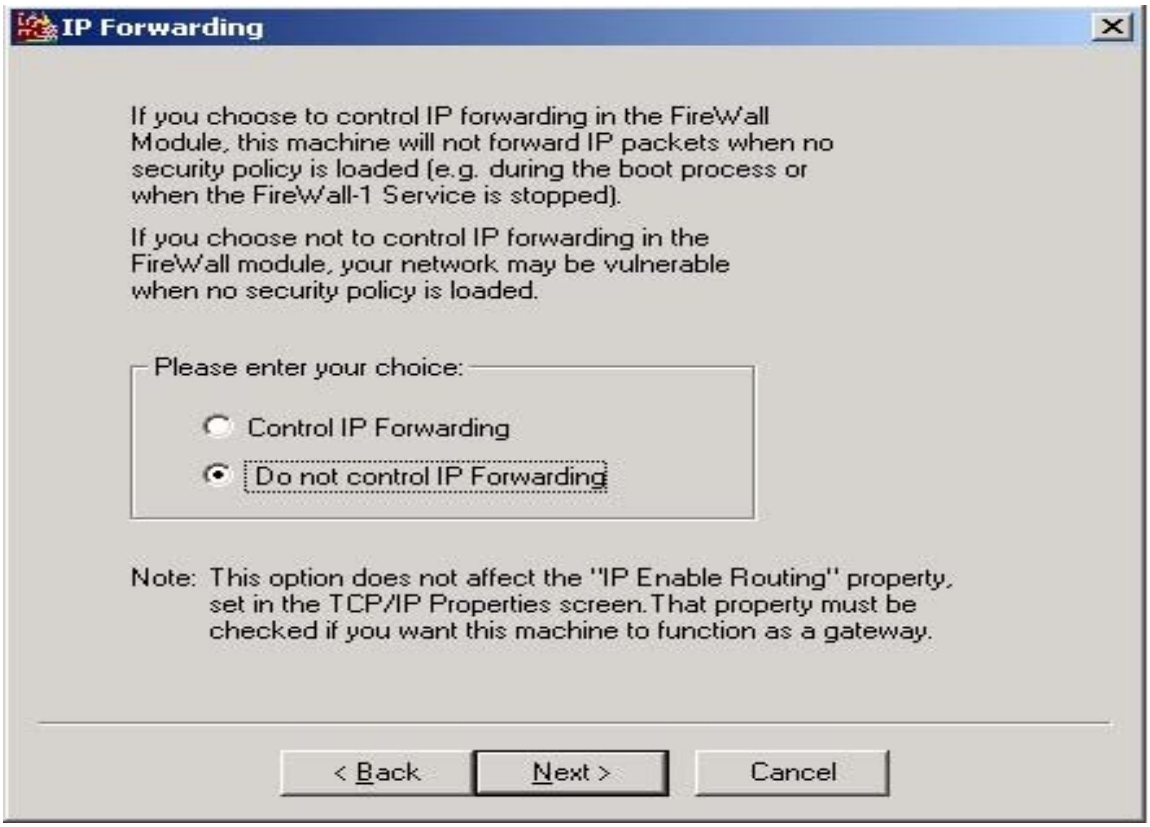
Chọn Add rồi nhập license vào cửa sổ sau :



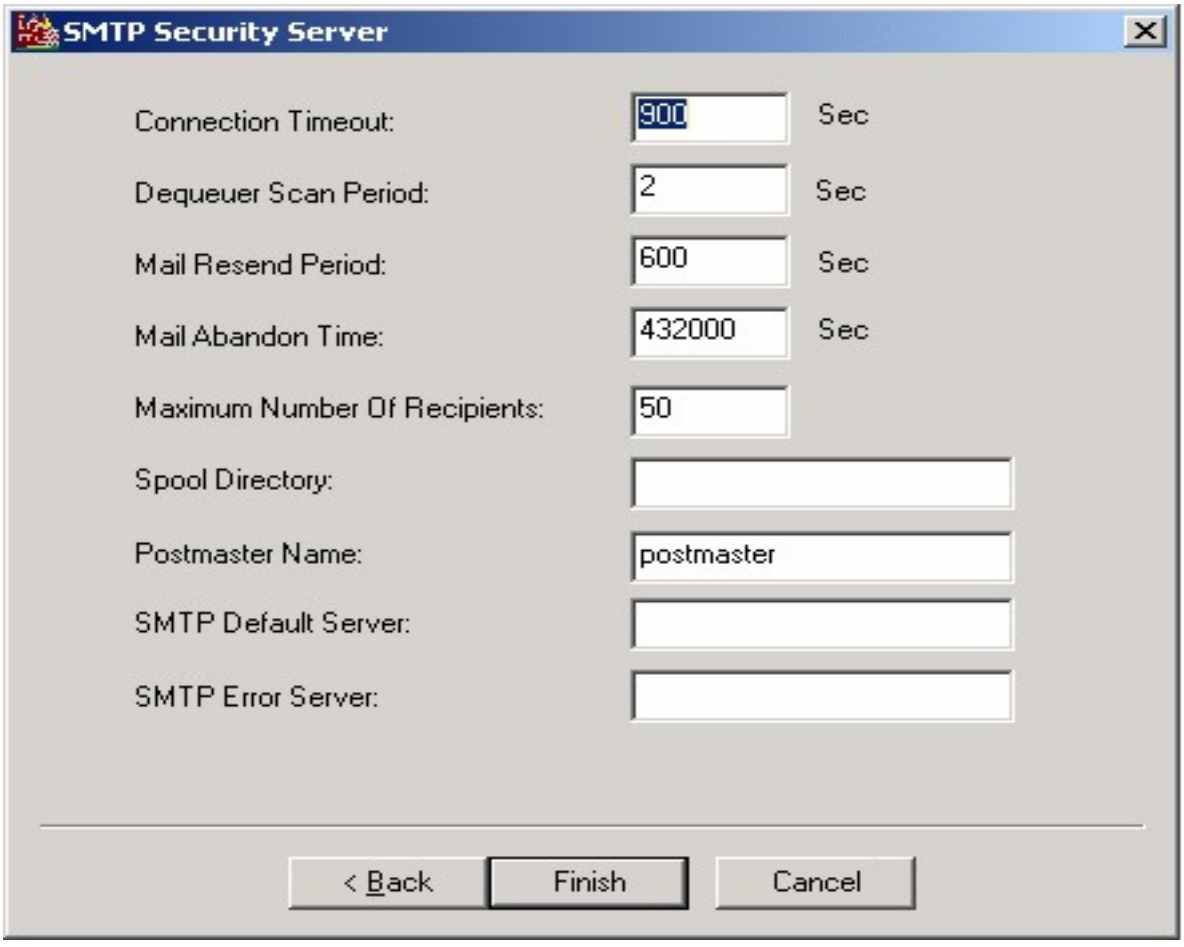
Chọn hostname của Management Server:



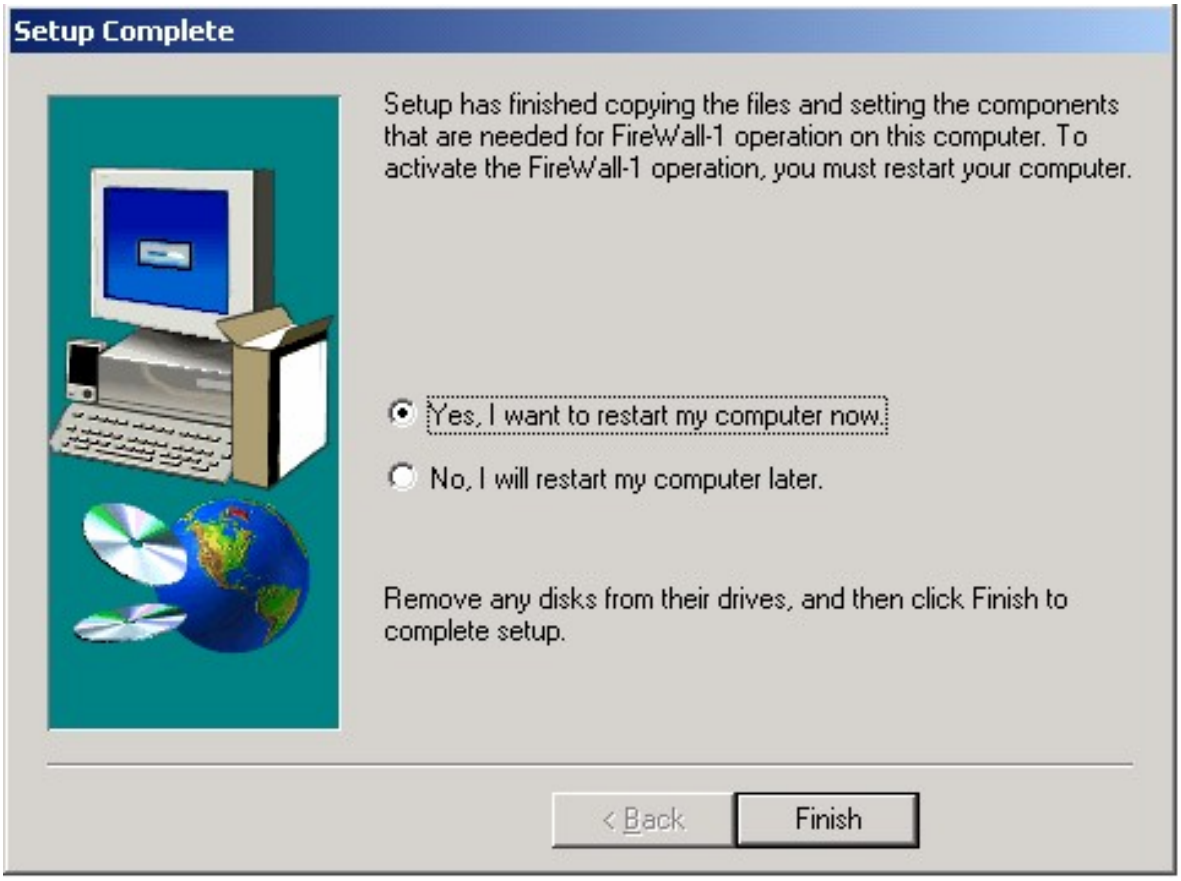
Chọn chế độ IP Forwarding:



Đặt các tham số cho SMTP Security Server:



Chọn Finish để kết thúc quá trình cài đặt rồi Restart lại máy.



GIÁO TRÌMH QUẢN TRỊ MẠNG VÀ THIẾT BỊ MẠNG

M c l c

L i nói d u

*Giáo trình " **Qu n tr m ng và các thi t b m ng** " du c biên so n v i m c tiêu cung c p các ki n th c lý thuy t và th c hành qu n tr ch y u cho các h th ng thi t b quan tr ng n n t ng c a m ng máy tính hi n d i. Giáo trình g m 2 ph n :*

- ***Ph n 1. Khái quát v m ng máy tính :*** *Bao g m nh ng khái ni m d nh nghia co b n nh t v m ng máy tính, phân lo i m ng máy tính, gi i thi u các giao th c m ng, d c bi t là giao th c TCP/IP. Các co s lý thuy t dua ra trong chuo ng này dòi h i h c viên ph i n m v ng d có th ti p thu du c các n i dung trong ph n 2.* ***Tuy v y, n u h c viên dã t trang b các ki n th c co b n trên ho c dã du c dào t o theo giáo trình "Thi t k và xây d ng m ng LAN và WAN" c a d án 112 có th b qua n i dung c a ph n m t và h c vào n i dung c a ph n 2 giáo trình***
- ***Ph n 2. Qu n tr m ng :*** *Đ ây là ph n n i dung chính c a giáo trình "Qu n tr m ng và các thi t b m ng" bao g m 4 chuong cung c p các ki n th c lý thuy t và k nang qu n tr co b n v i các thành ph n tr ng y u c a m ng bao g m b d nh tuy n, b chuy n m ch, h th ng tên mi n, h th ng truy c p t xa, h th ng proxy, h th ng b c tu ng l a (firewall). Các n i dung biên so n v k nang th c hành qu n tr giúp h c viên có d các ki n th c th c t d có th b t tay vào công tác qu n tr m ng cho don v .*

Do ph m vi r ng c a công tác qu n tr m ng, giáo trình này không bao g m h t du c m i n i dung c a công tác qu n tr m ng. H c viên có nhu c u nên tham kh o thêm các giáo trình khác c a d án 112 nhu :

- *Thi t k và xây d ng m ng LAN và WAN*
- *Qu n tr Windows 2000-NT*
- *T ng quan v Lotus Notes Domino*
- *Thi t k và qu n tr website, portal*
- *Thi t l p và qu n tr h th ng thu di n t*

Giáo trình du c biên so n l n d u tiên nên không tránh kh i có nh ng thi u sót. Nhóm biên so n r t mong nh n du c các góp ý t phía các h c viên, b n d c d có th hoàn thi n n i dung giáo trình t t hon.

PH N I: KHÁI QUÁT VỀ CÔNG NGHỆ M NG

Chuong 1

T ng quan v công ngh m ng máy tính và m ng c c b

M c 1: M ng máy tính

1. Gi i thi u m ng máy tính

1.1. Đ nh nghia m ng máy tính và m c dích c a vi c k t n i m ng

1.1.1. Nhu c u c a vi c k t n i m ng máy tính

Vi c n i máy tính thành m ng t lâu dã tr thành m t nhu c u khách quan vì :

- Có r t nhi u công vi c v b n ch t là phân tán ho c v thông tin, ho c v x lý ho c c hai dòi h i có s k t h p truy n thông v i x lý ho c s d ng phuong ti n t xa.
- Chia s các tài nguyên trên m ng cho nhi u ngu i s d ng t i m t th i di m (c ng, máy in, CD ROM . . .)
- Nhu c u liên l c, trao d i thông tin nh phuong ti n máy tính.
- Các ng d ng ph n m m dòi hòi t i m t th i di m c n có nhi u ngu i s d ng, truy c p vào cùng m t co s d li u.

1.1.2. Đ nh nghia m ng máy tính

Nói m t cách ng n g n thì m ng máy tính là t p h p các máy tính d c l p du c k t n i v i nhau thông qua các du ng truy n v t lý và tuân theo các quy u c truy n thông nào dó.

Khái ni m máy tính d c l p du c hi u là các máy tính không có máy nào có kh nang kh i d ng ho c dình ch m t máy khác.

Các du ng truy n v t lý du c hi u là các môi tru ng truy n tín hi u v t lý (có th là h u tuy n ho c vô tuy n).

Các quy u c truy n thông chính là co s d các máy tính có th "nói chuy n" du c v i nhau và là m t y u t quan tr ng hàng d u khi nói v công ngh m ng máy tính.

1.2. Đ c trung k thu t c a m ng máy tính

M t m ng máy tính có các d c trung k thu t co b n nhu sau:

1.2.1. Đu ng truy n

Là phuong ti n dùng d truy n các tín hi u di n t gi a các máy tính. Các tín hi u di u t dó chính là các thông tin, d li u du c bi u th du i d ng các xung nh phân (ON_OFF), m i tín hi u truy n gi a các máy tính v i nhau d u thu c sóng di n t , tu theo t n s mà ta có th dùng các du ng truy n v t lý khác nhau

Đ c tru ng co b n c a du ng truy n là gi i thông nó bi u th kh nang truy n t i tín hi u c a du ng truy n.

Thông thu ng ngu i ta hay phân lo i du ng truy n theo hai lo i:

- Đu ng truy n h u tuy n (các máy tính du c n i v i nhau b ng các dây d n tín hi u).
- Đu ng truy n vô tuy n: các máy tính truy n tín hi u v i nhau thông qua các sóng vô tuy n v i các thi t b di u ch /gi i di u ch các d u mút.

1.2.2. K thu t chuy n m ch

Là d c trung k thu t chuy n tín hi u gi a các nút trong m ng, các nút m ng có ch c nang hu ng thông tin t i dích nào dó trong m ng, hi n t i có các k thu t chuy n m ch nhu sau:

- K thu t chuy n m ch kênh: Khi có hai th c th c n truy n thông v i nhau thì gi a chúng s thi t l p m t kênh c d nh và duy trì k t n i dó cho t i khi hai bên ng t liên l c. Các d li u ch truy n di theo con du ng c d nh dó.
- K thu t chuy n m ch thông báo: thông báo là m t don v d li u c a ngu i s d ng có khuôn d ng du c quy d nh tru c. M i thông báo có ch a các thông tin di u khi n trong dó ch rõ dích c n truy n t i c a thông báo. Can c vào thông tin di u khi n này mà m i nút trung gian có th chuy n thông báo t i nút k ti p trên con du ng d n t i dích c a thông báo
- K thu t chuy n m ch gói: dây m i thông báo du c chia ra thành nhi u gói nh hon du c g i là các gói tin (packet) có khuôn d ng qui d nh tru c. M i gói tin cung ch a các thông tin di u khi n, trong dó có d a ch ngu n (ngu i g i) và d a ch dích (ngu i nh n) c a gói tin. Các gói tin c a cùng m t thông báo có th du c g i di qua m ng t i dích theo nhi u con du ng khác nhau.

1.2.3. Ki n trúc m ng

Ki n trúc m ng máy tính (network architecture) th hi n cách n i các máy tính v i nhau và t p h p các quy t c, quy u c mà t t c các th c th tham gia truy n thông trên m ng ph i tuân theo d d m b o cho m ng ho t d ng t t.

Khi nói d n ki n trúc c a m ng ngu i ta mu n nói t i hai v n d là hình tr ng m ng (Network topology) và giao th c m ng (Network protocol)

- Network Topology: Cách k t n i các máy tính v i nhau v m t hình h c mà ta g i là tô pô c a m ng

Các hình tr ng m ng co b n dó là: hình sao, hình bus, hình vòng

- Network Protocol: T p h p các quy u c truy n thông gi a các th c th truy n thông mà ta g i là giao th c (hay nghi th c) c a m ng

Các giao th c thu ng g p nh t là : TCP/IP, NETBIOS, IPX/SPX, . . .

1.2.4. H di u hành m ng

H di u hành m ng là m t ph n m m h th ng có các ch c nang sau:

- Qu n lý tài nguyên c a h th ng, các tài nguyên này g m:

+ Tài nguyên thông tin (v phuong di n luu tr) hay nói m t cách don gi n là qu n lý t p. Các công vi c v luu tr t p, tìm ki m, xoá, copy, nhóm, d t các thu c tính d u thu c nhóm công vi c này

+ Tài nguyên thi t b . Đi u ph i vi c s d ng CPU, các ngo i vi... d t i uu hoá vi c s d ng

- Qu n lý ngu i dùng và các công vi c trên h th ng.

H di u hành d m b o giao ti p gi a ngu i s d ng, chuong trình ng d ng v i thi t b c a h th ng.

- Cung c p các ti n ích cho vi c khai thác h th ng thu n l i (ví d FORMAT dia, sao chép t p và thu m c, in n chung ...)

Các h di u hành m ng thông d ng nh t hi n nay là: WindowsNT, Windows9X, Windows 2000, Unix, Novell.

1.3. Phân lo i m ng máy tính

Có nhi u cách phân lo i m ng khác nhau tu thu c vào y u t chính du c ch n dùng d làm ch tiêu phân lo i, thông thu ng ngu i ta phân lo i m ng theo các tiêu chí nhu sau

- Kho ng cách d a lý c a m ng
- K thu t chuy n m ch mà m ng áp d ng
- Ki n trúc m ng
- H di u hành m ng s d ng ...

Tuy nhiên trong th c t ngu i ta thu ng ch phân lo i theo hai tiêu chí d u tiên

1.3.1. Phân lo i m ng theo kho ng cách d a lý

N u l y kho ng cách d a lý làm y u t phân lo i m ng thì ta có m ng c c b (LAN), m ng dô th (MAN), m ng di n r ng (WAN), m ng toàn c u.

1.3.2. Phân lo i theo k thu t chuy n m ch

N u l y k thu t chuy n m ch làm y u t chính d phân lo i s có: m ng chuy n m ch kênh, m ng chuy n m ch thông báo và m ng chuy n m ch gói.

M ch chuy n m ch kênh (circuit switched network) : hai th c th thi t l p m t kênh c d nh và duy trì k t n i dó cho t i khi hai bên ng t liên l c.

M ng chuy n m ch thông báo (message switched network) : Thông báo là m t don v d li u qui u c du c g i qua m ng d n di m dích mà không thi t l p kênh truy n c d nh. Can c vào thông tin tiêu d mà các nút m ng có th x lý du c vi c g i thông báo d n dích

M ng chuy n m ch gói (packet switched network) : dây m i thông báo du c chia ra thành nhi u gói nh hon du c g i là các gói tin (packet) có khuôn d ng qui d nh tru c. M i gói tin cung ch a các thông tin di u khi n, trong dó có d a ch ngu n (ngu i g i) và d a ch dích (ngu i nh n) c a gói tin. Các gói tin c a cùng m t thông báo có th du c g i di qua m ng t i dích theo nhi u con du ng khác nhau.

1.3.3. Phân lo i theo ki n trúc m ng s d ng

Ki n trúc c a m ng bao g m hai v n d : hình tr ng m ng (Network topology) và giao th c m ng (Network protocol)

Hình tr ng m ng : Cách k t n i các máy tính v i nhau v m t hình h c mà ta g i là tô pô c a m ng

Giao th c m ng : T p h p các quy u c truy n thông gi a các th c th truy n thông mà ta g i là giao th c (hay nghi th c) c a m ng

Khi phân lo i theo topo m ng ngu i ta thu ng có phân lo i thành: m ng hình sao, tròn, tuy n tính

Phân lo i theo giao th c mà m ng s d ng ngu i ta phân lo i thành m ng : TCP/IP, m ng NETBIOS . ..

Tuy nhiên các cách phân lo i trên không ph bi n và ch áp d ng cho các m ng c c b .

1.3.4. Phân lo i theo h di u hàng m ng

N u phân lo i theo h di u hành m ng ngu i ta chia ra theo mô hình m ng ngang hàng, m ng khách/ch ho c phân lo i theo tên h di u hành mà m ng s d ng: Windows NT, Unix, Novell . . .

1.4. Các m ng máy tính thông d ng nh t

1.4.1. M ng c c b

M t m ng c c b là s k t n i m t nhóm máy tính và các thi t b k t n i m ng du c l p d t trên m t ph m v d a lý gi i h n, thu ng trong m t toà nhà ho c m t khu công s nào dó. M ng có t c d cao

1.4.2. M ng di n r ng v i k t n i LAN to LAN

M ng di n r ng bao gi cung là s k t n i c a các m ng LAN, m ng di n r ng có th tr i trên ph m vi m t vùng, qu c gia ho c c m t l c d a th m chí trên ph m vi toàn c u. M ng có t c d truy n d li u không cao, ph m vi d a lý không gi i h n

1.4.3. Liên m ng INTERNET

V i s phát tri n nhanh chóng c a công ngh là s ra d i c a liên m ng INTERNET. M ng Internet là s h u c a nhân lo i, là s k t h p c a r t nhi u m ng d li u khác ch y trên n n t ng giao th c TCP/IP

1.4.4. M ng INTRANET

Th c s là m t m ng INTERNET thu nh vào trong m t co quan/công ty/t ch c hay m t b /nghành . . ., gi i h n ph m vi ngu i s d ng, có s d ng các công ngh ki m soát truy c p và b o m t thông tin .

Đu c phát tri n t các m ng LAN, WAN dùng công ngh INTERNET

2. M ng c c b , ki n trúc m ng c c b

2.1. M ng c c b

Tên g i "m ng c c b " du c xem xét t quy mô c a m ng. Tuy nhiên, dó không ph i là d c tính duy nh t c a m ng c c b nhung trên th c t , quy mô c a m ng quy t d nh nhi u d c tính và công ngh c a m ng. Sau dây là m t s d c di m c a m ng c c b :

Đ c di m c a m ng c c b

- M ng c c b có quy mô nh , thu ng là bán kính du i vài km.
- M ng c c b thu ng là s h u c a m t t ch c. Th c t dó là di u khá quan tr ng d vi c qu n lý m ng có hi u qu .
- M ng c c b có t c d cao và ít l i. Trên m ng r ng t c d nói chung ch d t vài tram Kbit/s d n Mb/s. Còn t c d thông thu ng trên m ng c c b là 10, 100 Mbit/s và t i nay v i Gigabit Ethernet.

2.2. Ki n trúc m ng c c b

2.2.1. Đ hình m ng (Network Topology)

*** Đ nh nghia Topo m ng:**

Cách k t n i các máy tính v i nhau v m t hình h c mà ta g i là tô pô c a m ng. Có hai ki u n i m ng ch y u dó là :

- N i ki u di m - di m (point - to - point): các du ng truy n n i t ng c p nút v i nhau, m i nút "luu và chuy n ti p" d li u
- N i ki u di m - nhi u di m (point - to - multipoint hay broadcast) : t t c các nút phân chia nhau m t du ng truy n v t lý, g i d li u d n nhi u nút m t lúc và ki m tra gói tin theo d a ch

*** Phân bi t ki u tô pô c a m ng c c b và ki u tô pô c a m ng r ng.**

Tô pô c a m ng di n r ng thông thu ng là nói d n s liên k t gi a các m ng c c b thông qua các b d n du ng (router) và kênh vi n thông. Khi nói t i tô pô c a m ng c c b ngu i ta nói d n s liên k t c a chính các máy tính.

- ***M ng hình sao:*** M ng hình sao có t t c các tr m du c k t n i v i m t thi t b trung tâm có nhi m v nh n tín hi u t các tr m và chuy n d n tr m dích Đ dài du ng truy n n i m t tr m v i thi t b trung tâm b h n ch (trong vòng 100m, v i công ngh hi n nay).

Hình 1.1: K t n i hình sao

- ***M ng tr c tuy n tính (Bus):***
Trong m ng tr c t t c các tr m phân chia m t du ng truy n chung (bus). Đu ng truy n chính du c gi i h n hai d u b ng hai d u n i d c bi t g i là terminator. M i tr m du c n i v i tr c chính qua m t d u n i ch T (T-connector) ho c m t thi t b thu phát (transceiver).

Hình 1.2. K t n i ki u bus

- ***M ng hình vòng***
Trên m ng hình vòng tín hi u du c truy n di trên vòng theo m t chi u duy nh t. M i tr m c a m ng du c n i v i vòng qua m t b chuy n ti p (repeater) do dó c n có giao th c di u khi n vi c c p phát quy n du c truy n d li u trên vòng m ng cho tr m có nhu c u.
M ng hình vòng có uu nhu c di m tuong t m ng hình sao, tuy nhiên m ng hình vòng dòi h i giao th c truy nh p m ng ph c t p hon m ng hình sao.

Hình 1.3. K t n i ki u vòng

d) K t n i h n h p

Là s ph i h p các ki u k t n i khác nhau,

Hình 1.4. M t k t n i h n h p

2.3. Các phuo ng pháp truy c p du ng truy n v t lý

Trong m ng c c b , t t c các tr m k t n i tr c ti p vào du ng truy n chung. N u nhi u tr m cùng g i tín hi u lên du ng truy n d ng th i thì tín hi u s ch ng lên nhau và b h ng. Vì v y c n ph i có m t phuong pháp t ch c chia s du ng truy n d vi c truy n thông d oc dúng d n.

Có hai phuong pháp chia s du ng truy n chung thu ng du c dùng trong các m ng c c b :

- Truy nh p du ng truy n m t cách ng u nhiên, theo yêu c u. Đuong nhiên ph i có tính d n vi c s d ng luân phiên và n u trong tru ng h p do có nhi u tr m cùng truy n tin d n d n tín hi u b trùm lên nhau thì ph i truy n l i. Đ i n hình c a phuong pháp này là giao th c truy c p CSMA/CD

- Có co ch tr ng tài d c p quy n truy nh p du ng truy n sao cho không x y ra xung d t. Đi n hình phuong pháp này là giao th c truy c p Tokenring

3. Chu n hoá m ng máy tính

3.1. V n d chu n hoá m ng và các t ch c chu n hoá m ng

Khi thi t k các giao th c m ng, các nhà thi t k t do l a ch n ki n trúc cho riêng mình. T dó d n t i tình tr ng không tuong thích gi a các m ng máy tính v i nhau. V n d không tuong thích dó làm tr ng i cho s tuong tác gi a nh ng giao th c m ng khác nhau. Nhu c u trao d i thông tin càng l n thúc d y vi c xây d ng khung chu n v ki n trúc m ng d làm can c cho các nhà thi t k và ch t o thi t b m ng .

Chính vì lý do dó, t ch c tiêu chu n hoá qu c t ISO (Internatinal Organnization for Standarzation) dã xây d ng mô hình tham chi u cho vi c k t n i các h th ng m OSI (reference model for Open Systems Interconnection). Mô hình này là co s cho vi c k t n i các h th ng m ph c v cho các ng d ng phân tán.

3.2. Mô hình tham chi u OSI 7 l p

Mô hình OSI du c bi u di n theo hình du i dây:

Mô hình OSI phân chia thành 7 l p bao g m các l p ng d ng, l p th hi n, l p phiên, l p v n chuy n, l p m ng, l p liên k t và l p v t lý. Mô hình OSI cung d nh nghia ph n tiêu d (header) c a don v d li u và m i liên k t gi a các l p, vi c g n thêm ph n mào d u (header) d chuy n d li u t các l p trên xu ng l p du i và m gói là ch c nang g b ph n mào d u d chuy n d li u lên l p trên.

L p ng d ng
(application)

L p th hi n
(presentation)

L p phiên
(session)
L p chuy n v n
(transport)
L p m ng
(network)
L p liên k t d li u
(data link)
L p v t lý

Hình 1.5. Mô hình OSI 7 l p

(physical link)

Ch c nang c th c a t ng l p theo mô hình OSI có th tham kh o chi ti t thêm trong giáo trình "Thi t k và xây d ng m ng LAN và WAN"

3.3. Các chu n k t n i thông d ng nh t IEEE 802.X và ISO 8802.X

Bên c nh vi c chu n hoá cho m ng nói chung d n d n k t qu co b n nh t là mô hình tham chi u OSI nhu dã gi i thi u, ngu i ta cung chu n hóa các giao th c m ng c c b LAN.

- *Các chu n IEEE 802.x và ISO 8802.x*

IEEE là t ch c di tiên phong trong linh v c chu n hoá m ng c c b v i d án IEEE 802 v i k t qu là m t lo t các chu n thu c h IEEE 802.x ra d i . Cu i nh ng nam 80, t ch c ISO dã ti p nh n h chu n này và ban hành thành chu n qu c t du i mã hi u tuong ng là ISO 8802.x.

IEEE 802. : là chu n d c t ki n trúc m ng, k t n i gi a các m ng và vi c qu n tr m ng d i v i m ng c c b .

IEEE 802.2 : là chu n d c t t ng d ch v giao th c c a m ng c c b .

IEEE 802.3 : là chu n d c t m t m ng c c b d a trên m ng Ethernet n i ti ng c a Digital, Intel và Xerox h p tác xây d ng t nam 1980. Các chu n qui d nh v t lý nhu 10BASE5, 10BASE2, 10BASE-F,

IEEE 802.5 : là chu n d c t m ng c c b v i topo m ng d ng vòng (ring) dùng th bài d di u vi c truy nh p du ng truy n.

IEEE 802.11 : là chu n d c t m ng c c b không dây (Wireless LAN) hi n dang du c ti p t c phát tri n.

Ngoài ra trong h chu n 802.x còn có các chu n IEEE 802.4, 802.6, 802.9, 802.10 và 802.12

M c 2: Các thi t b m ng thông d ng và các chu n k t n i v t lý

1. Các thi t b m ng thông d ng

1.1. Các lo i cáp truy n

1.1.1. Cáp d ôi dây xo n (Twisted pair cable)

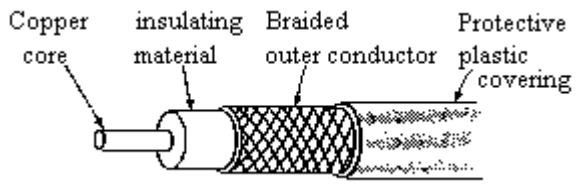
Cáp dôi dây xo n là cáp g m hai dây d ng xo n d tránh gây nhi u cho các dôi dây khác, có th kéo dài t i vài km mà không c n khuy ch d i. Gi i t n trên cáp dây xo n d t kho ng 300–4000Hz, t c d truy n d t vài kbps d n vài Mbps. Cáp xo n có hai lo i:

- Lo i có b c kim lo i d tang cu ng ch ng nhi u g i là STP (Shield Twisted Pair). Lo i này trong v b c kim có th có nhi u dôi dây. V lý thuy t thì t c d truy n có th d t 500 Mb/s nhung th c t th p hon r t nhi u (ch d t 155 Mbps v i cáp dài 100 m)
- Lo i không b c kim g i là UTP (UnShield Twisted Pair), ch t lu ng kém hon STP nhung r t r . Cap UTP du c chia làm 5 h ng tu theo t c d truy n. Cáp lo i 3 dùng cho di n tho i. Cáp lo i 5 có th truy n v i t c d 100Mb/s r t hay dùng trong các m ng c c b vì v a r v a ti n s d ng. Cáp này có 4 dôi dây xo n n m trong cùng m t v b c

Hình 1.6. Cáp UTP Cat. 5

1.1.2. Cáp d ng tr c (Coaxial cable) bang t n co s

Là cáp mà hai dây c a nó có lõi l ng nhau, lõi ngoài là lu i kim lo i. , Kh nang ch ng nhi u r t t t nên có th s d ng v i chi u dài t vài tram met d n vài km. Có hai lo i du c dùng nhi u là lo i có tr kháng 50 ohm và lo i có tr kháng 75 ohm.



Hình 1.7. Cáp d ng tr c

D i thông c a cáp này còn ph thu c vào chi u dài c a cáp. V i kho ng cách1 km có th d t t c d truy n t 1– 2 Gbps. Cáp d ng tr c bang t n co s thu ng dùng cho các m ng c c b . Có th n i cáp b ng các d u n i theo chu n BNC có hình ch T. VN ngu i ta hay g i cáp này là cáp g y do d ch t tên trong ti ng Anh là 'Thin Ethernet".

M t lo i cáp khác có tên là "Thick Ethernet" mà ta g i là cáp béo. Lo i này thu ng có màu vàng. Ngu i ta không n i cáp b ng các d u n i ch T nhu cáp g y mà n i qua các k p b m vào dây. C 2m5 l i có dánh d u d n i dây (n u c n). T k p dó ngu i ta g n các tranceiver r i n i vào máy tính.

1.1.3. Cáp d ng tr c bang r ng (Broadband Coaxial Cable)

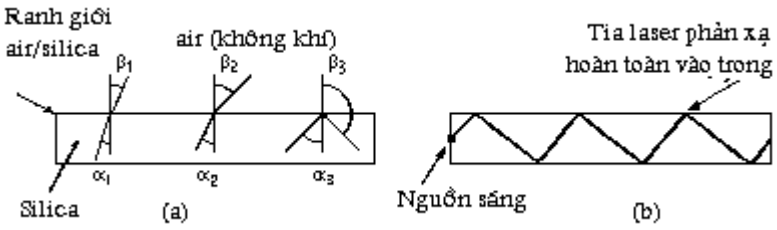
Đây là lo i cáp theo tiêu chu n truy n hình (thu ng dùng trong truy n hình cáp) có d i thông t 4 – 300 Khz trên chi u dài 100 km. Thu t ng "bang r ng" v n là thu t ng c a ngành truy n hình còn trong ngành truy n s li u di u này ch có nghia là cáp lo i này cho phép truy n thông tin tuong t (analog) mà thôi. Các h th ng d a trên cáp d ng tr c bang r ng có th truy n song song nhi u kênh. Vi c khuy ch d i tín hi u ch ng suy hao có th làm theo ki u khuy ch d i tín hi u tuong t (analog). Đ truy n thông cho máy tính c n chuy n tín hi u s thành tín hi u tuong t .

1.1.4. Cáp quang

Dùng d truy n các xung ánh sáng trong lòng m t s i thu tinh ph n x toàn ph n. Môi tru ng cáp quang r t lý tu ng vì

- Xung ánh sáng có th di hàng tram km mà không gi m cu ng d sáng.
- D i thông r t cao vì t n s ánh sáng dùng d i v i cáp quang c kho ng 1014 –1016
- An toàn và bí m t, không b nhi u di n t

Ch có hai nhu c di m là khó n i dây và giá thành cao.



Hình 1.8. Truy n tín hi u b ng cáp quang

Cáp quang cung có hai lo i
- Lo i da mode (multimode fiber): khi góc t i thành dây d n l n d n m t m c nào dó thì có hi n tu ng ph n x toàn ph n. Các cáp da mode có du ng kính kho ng 50 µ
- Lo i don mode (singlemode fiber): khi du ng kính dây d n b ng bu c sóng thì cáp quang gi ng nhu m t ng d n sóng, không có hi n tu ng ph n x nhung ch cho m t tia di. Lo i này có du ng kính kho n 8µm và ph i dùng

diode laser. Cáp quang da mode có th cho phép truy n xa t i hàng tram km mà không c n ph i khuy ch d i.

1.2. Các thi t b ghép n i

1.2.1. Card giao ti p m ng (Network Interface Card - NIC)

Đó là m t card du c c m tr c ti p vào máy tính trên khe c m m r ng ISA ho c PCI ho c tích h p vào bo m ch ch PC. Trên dó có các m ch di n giúp cho vi c ti p nh n (receiver) ho c/và phát (transmitter) tín hi u lên m ng. Ngu i ta thu ng dùng t tranceiver d ch thi t b (m ch) có c hai ch c nang thu và phát.

1.2.2. B chuy n ti p (REPEATER)

Nhi m v c a các repeater là h i ph c tín hi u d có th truy n ti p cho các tr m khác bao g m c công tác khuy ch d i tín hi u, di u ch nh tín hi u.

1.2.3. Các b t p trung (Concentrator hay HUB)

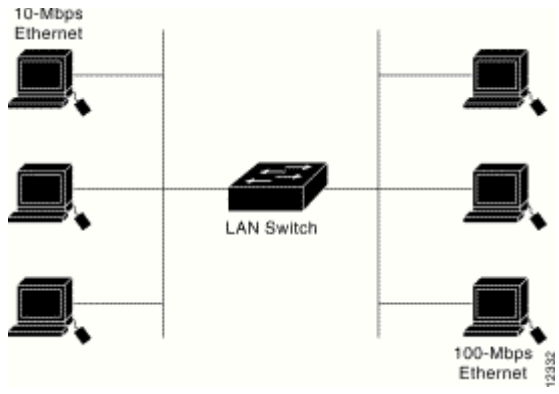
HUB là m t lo i thi t b có nhi u d u c m các d u cáp m ng. Ngu i ta s d ng HUB d n i m ng theo ki u hình sao. Uu di m c a ki u n i này là tang d d c l p c a các máy khi m t máy b s c dây d n.

Có lo i HUB th d ng (passive HUB) là HUB ch d m b o ch c nang k t n i hoàn toàn không x lý l i tín hi u. HUB ch d ng (active HUB) là HUB có ch c nang khuy ch d i tín hi u d ch ng suy hao.

HUB thông minh (intelligent HUB) là HUB ch d ng nhung có kh nang t o ra các gói tin mang tin t c v ho t d ng c a mình và g i lên m ng d ngu i qu n tr m ng có th th c hi n qu n tr t d ng

1.2.4. Switching Hub (hay còn g i t t là switch)

Là các b chuy n m ch th c s . Khác v i HUB thông thu ng, thay vì chuy n m t tín hi u d n t m t c ng cho t t c các c ng, nó ch chuy n tín hi u d n c ng có tr m dích. Do v y Switch là m t thi t b quan tr ng trong các m ng c c b l n dùng d phân do n m ng. Nh có switch mà d ng d trên m ng gi m h n. Ngày nay switch là các thi t b m ng quan tr ng cho phép tu bi n trên m ng ch ng h n l p m ng o VLAN.



Hình 1.9. LAN Switch n i hai Segment m ng

1.2.5. Modem

Là tên vi t t t hai t di u ch (MOdulation) và gi i di u ch (DEModulation) là thi t b cho phép di u ch d bi n d i tín hi u s sang tín hi u tuong t d có th g i theo du ng tho i và khi nh n tín hi u t du ng tho i có th bi n d i ngu c l i thành tín hi u s .

1.2.6. Multiplexor - Demultiplexor

B d n kênh có ch c nang t h p nhi u tín hi u d cùng g i trên m t du ng truy n. B tách kênh có ch c nang ngu c l i noi nh n tín hi u

1.2.7. Router

Router là m t thi t b dùng d ghép n i các m ng c c b v i nhau thành m ng r ng. Router th c s là m t máy tính làm nhi m v ch n du ng cho các gói tin hu ng ra ngoài. Router d c l p v ph n c ng và có th dùng trên các m ng ch y giao th c khác nhau

2. M t s ki u n i m ng thông d ng và các chu n

2.1.Các thành ph n thông thu ng trên m t m ng c c b

- Các máy ch cung c p d ch v (server)
- Các máy tr m cho ngu i làm vi c (workstation)
- Đu ng truy n (cáp n i)
- Card giao ti p gi a máy tính và du ng truy n (network interface card)
- Các thi t b n i (connection device)

Hai y u t du c quan tâm hàng d u khi k t n i m ng c c b là t c d trong m ng và bán kính m ng. Tên các ki u m ng dùng theo giao th c CSMA/CD cung th hi n di u này. Sau dây là m t s ki u k t n i dó v i t c d 10 Mb/s khá thông d ng trong th i gian qua và m t s thông s k thu t:

Chu n IEEE 802.3		
Ki u	10BASE5	10BASE2 10BASE-T
Ki u cáp	Cáp d ng tr c	Cáp d ng tr c Cáp UTP
T c d	10 Mb/s	
Đ dài cáp t i da	500 m/segment	185 m/segment 100 m k t HUB
S các th c th truy n thông	100 host /segment	30 host / segment S c ng c a HUB

2.2. Ki u 10BASE5

Là chu n CSMA/CD có t c d 10Mb và bán kính 500 m. Ki u này dùng cáp d ng tr c lo i thick ethernet (cáp d ng tr c béo) v i tranceiver. Có th k t n i vào m ng kho ng 100 máy

Tranceiver: Thi t b n i gi a card m ng và du ng truy n, dóng vai trò là b thu-phát.

2.3. Ki u 10BASE2

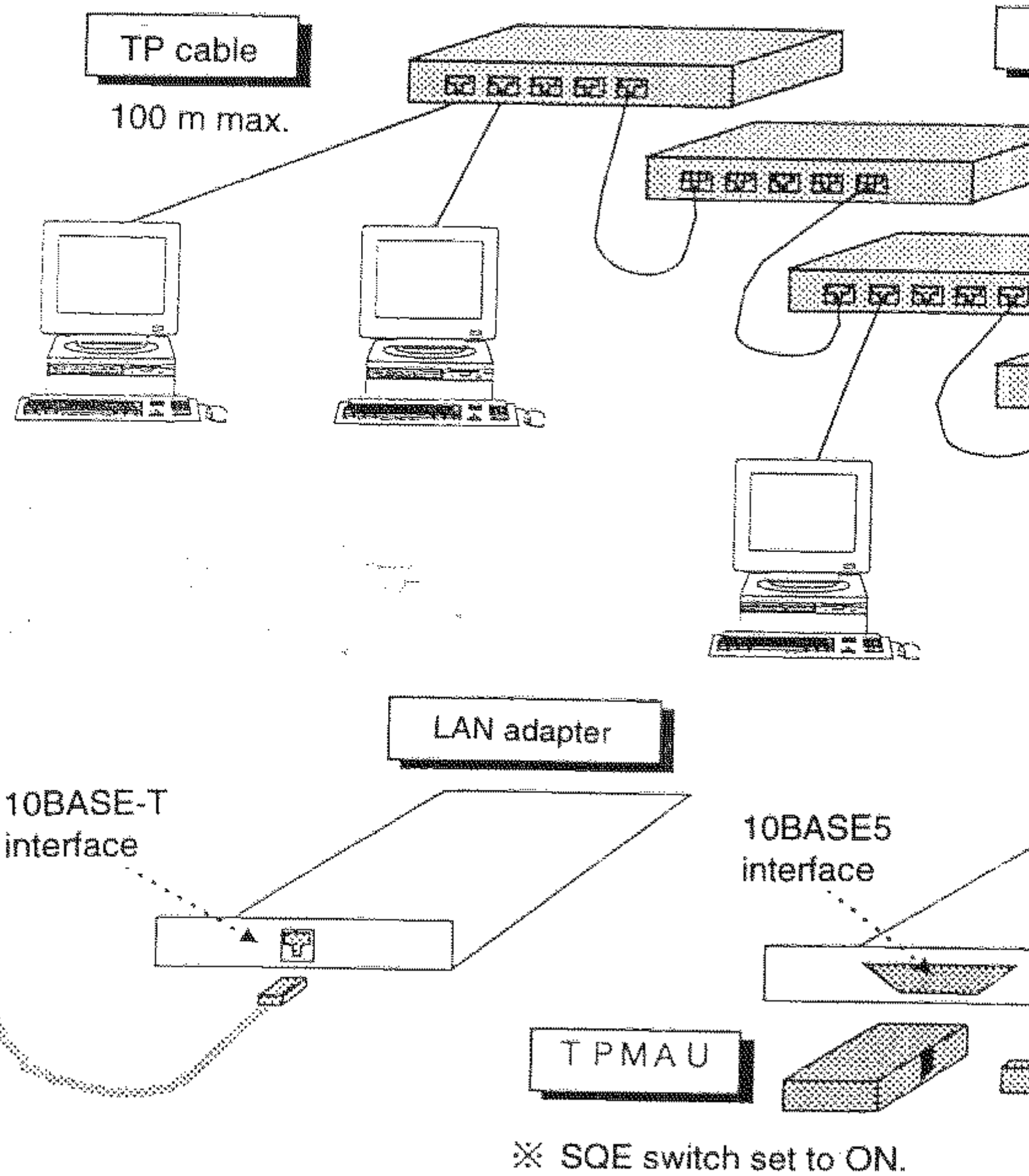
Là chu n CSMA/CD có t c d 10Mb và bán kính 200 m. Ki u này dùng cáp d ng tr c lo i thin ethernet v i d u n i BNC. Có th k t n i vào m ng kho ng 30 máy

Hình1.11: N i theo chu n 10BASE2 v i cáp d ng tr c và d u n i BNC

2.4. Ki u 10BASE-T

Là ki u n i dùng HUB có các n i ki u RJ45 cho các cáp UTP. Ta có th m r ng m ng b ng cách tang s HUB, nhung cung không du c tang quá nhi u t ng vì ho t d ng c a m ng s kém hi u qu n u d tr quá l n .

Hi n nay mô hình phiên b n 100BASE-T, 1000BASE-T b t d u du c s d ng nhi u, t c d d t t i 100 Mbps, 1000Mbps



Hình 1.12: N i m ng theo ki u 10BASE-T v i cáp UTP và HUB

er cab), ch y u dùng n i các thi t b xa nhau, t o d ng du ng tr c xuong s ng (backborn) d n i các m ng LAN xa nhau (2-10 km). Hi n nay cung dã có các phiên b n 100BASE-F và 1000BASE-F v i t c d truy n d li u cao hon 10 và 100 l n

Chuong 2
Gi i thi u giao th c TCP/IP

1. Giao th c IP

1.1. H giao th c TCP/IP

S ra d i c a h giao th c TCP/IP g n li n v i s ra d i c a Internet mà ti n thân là m ng **ARPA** net (**A** dvanced **R** esearch **P** rojects **A** gency) do B Qu c phòng M t o ra. Đây là b giao th c du c dùng r ng rãi nh t vì tính m c a nó. Hai giao th c du c dùng ch y u dây là **TCP** (**T** ransmission **C** ontrol **P** rotocol) và **IP** (**I** nternet **P** rotocol). Chúng dã nhanh chóng du c dón nh n và phát tri n b i nhi u nhà nghiên c u và các hãng công nghi p máy tính v i m c dích xây d ng và phát tri n m t m ng truy n thông m r ng kh p th gi i mà ngày nay chúng ta g i là Internet.

Đ n nam 1981, TCP/IP phiên b n 4 m i hoàn t t và du c ph bi n r ng rãi cho toàn b nh ng máy tính s d ng h di u hành UNIX. Sau này Microsoft cung dã dua TCP/IP tr thành m t trong nh ng giao th c can b n c a h di u hành Windows 9x mà hi n nay dang s d ng.

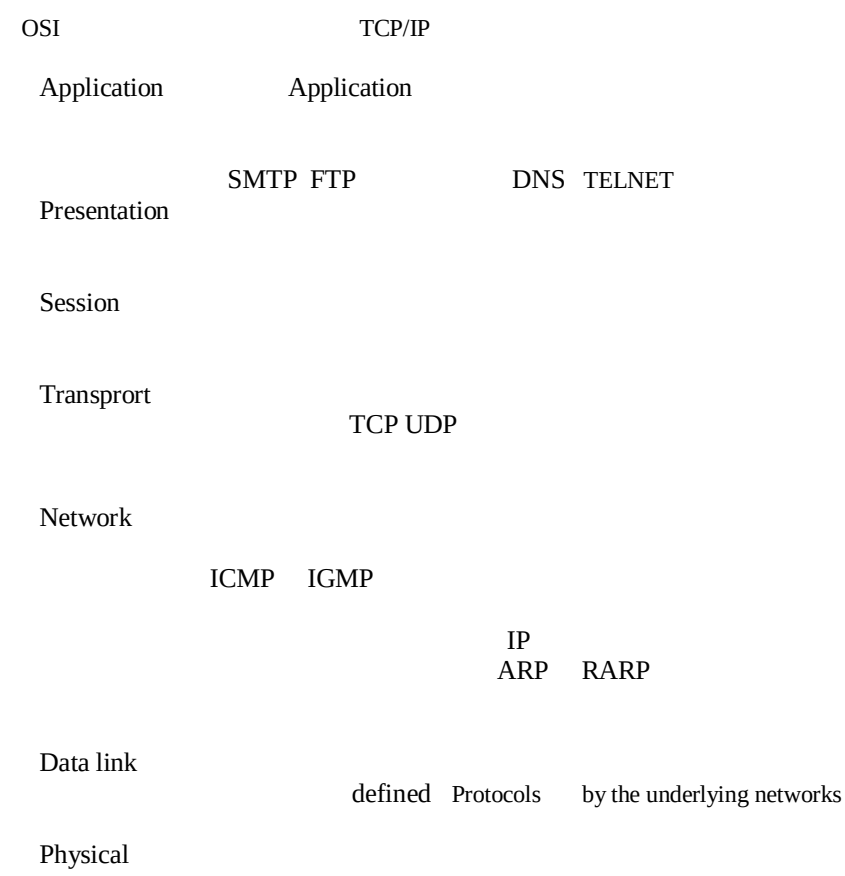
Đ n nam 1994, m t b n th o c a phiên b n IPv6 du c hình thành v i s c ng tác c a nhi u nhà khoa h c thu c các t ch c Internet trên th gi i d c i ti n nh ng h n ch c a IPv4.

Khác v i mô hình ISO/OSI t ng liên m ng s d ng giao th c k t n i m ng "không liên k t" (connectionless) IP, t o thành h t nhân ho t d ng c a Internet. Cùng v i các thu t toán d nh tuy n RIP, OSPF, BGP, t ng liên m ng IP cho phép k t n i m t cách m m d o và linh ho t các lo i m ng "v t lý" khác nhau nhu: Ethernet, Token Ring , X.25...

Giao th c trao d i d li u "có liên k t" (connection - oriented) TCP du c s d ng t ng v n chuy n d d m b o tính chính xác và tin c y vi c trao d i d li u d a trên ki n trúc k t n i "không liên k t" t ng liên m ng IP.

Các giao th c h tr ng d ng ph bi n nhu truy nh p t xa (telnet), chuy n t p (FTP), d ch v World Wide Web (HTTP), thu di n t (SMTP), d ch v tên mi n (DNS) ngày càng du c cài d t ph bi n nhu nh ng b ph n c u thành c a các h di u hành thông d ng nhu UNIX (và các h di u hành chuyên d ng cùng h c a các nhà cung c p thi t b tính toán nhu AIX c a IBM, SINIX c a Siemens, Digital UNIX c a DEC), Windows9x/NT, Novell Netware,...

1.2. Ch c nang chính c a giao th c liên m ng IP (v4)



Hình 2.1 Mô hình OSI và mô hình ki n trúc c a TCP/IP

Trong c u trúc b n l p c a TCP/IP, khi d li u truy n t l p ng d ng cho d n l p v t lý, m i l p d u c ng thêm vào ph n di u khi n c a mình d d m b o cho vi c truy n d li u du c chính xác. M i thông tin di u khi n này du c g i là m t *header* và du c d t tru c ph n d li u du c truy n. M i l p xem t t c các thông tin mà nó nh n du c t l p trên là d li u, và d t ph n thông tin di u khi n *header* c a nó vào tru c ph n thông tin này. Vi c c ng m i l p trong quá trình truy n tin du c g i là thêm vào các *header* *encapsulation* . Quá trình nh n d li u di n ra theo chi u ngu c l i: m i l p s tách ra ph n *header* tru c khi truy n d li u lên l p trên.

M i l p có m t c u trúc d li u riêng, d c l p v i c u trúc d li u du c dùng l p trên hay l p du i c a nó. Sau dây là gi i thích m t s khái ni m thu ng g p.

Stream là dòng s li u du c truy n trên co s don v s li u là Byte.

S li u du c trao d i gi a các ng d ng dùng TCP du c g i là *stream* , trong khi dùng UDP, chúng du c g i là *message* .

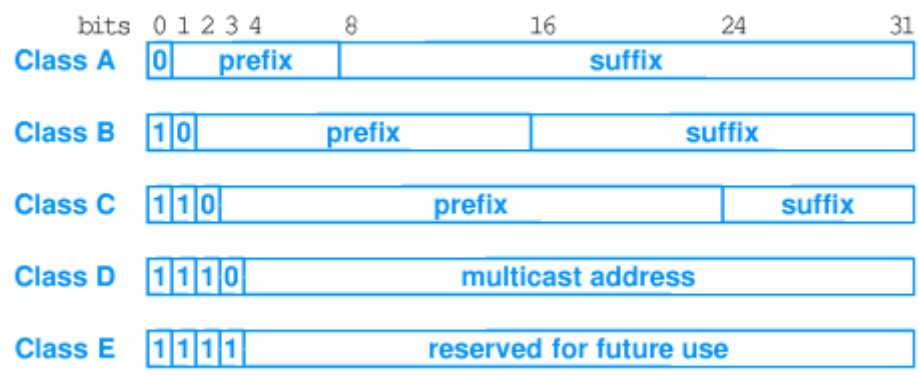
M i gói s li u TCP du c g i là *segment* còn UDP d nh nghia c u trúc d li u c a nó là *packet* .

L p Internet xem t t c các d li u nhu là các kh i và g i là *datagram* .
B giao th c TCP/IP có th dùng nhi u ki u khác nhau c a l p m ng du i cùng, m i lo i có th có m t thu t ng khác nhau d truy n d li u.
Ph n l n các m ng k t c u ph n d li u truy n di du i d ng các *packets* hay là các *frames* .

Application Stream

Transport Segment/datagram
Internet Datagram
Network Access Frame

Hình 2.2: C u trúc d li u t i các l p c a TCP/IP



(m i vùng 1 byte), có th du c bi u th du i d ng th p phân, bát phân, th p l c phân ho c nh phân. Cách vi t ph bi n nh t là dùng ký pháp th p phân có d u ch m d tách gi a các vùng. Đ a ch IP là d d nh danh duy nh t cho m t host b t k trên liên m ng.
Khuôn d ng d a ch IP: m i host trên m ng TCP/IP du c d nh danh duy nh t b i m t d a ch có khuôn d ng

<Network Number, Host number>

Do t ch c và d l n c a các m ng con c a liên m ng có th khác nhau, ngu i ta chia các d a ch IP thành 5 l p ký hi u A,B,C, D, E. Các bit d u tiên c a byte d u tiên du c dùng d d nh danh l p d a ch (0-l p A; 10 l p B; 110 l p C; 1110 l p D; 11110 l p E).

1.2. Ch c nang chính c a - Giao th c liên m ng IP(v4)

Trong ph n này trình bày v giao th c IPv4 (d cho thu n ti n ta vi t IP có nghia là d c p d n IPv4).
M c dích chính c a IP là cung c p kh nang k t n i các m ng con thành liên m ng d truy n d li u. IP cung c p các ch c nang chính sau:
- Đ nh nghia c u trúc các gói d li u là don v co s cho vi c truy n d li u
trên Internet.
- Đ nh nghia phuong th c dánh d a ch IP.
- Truy n d li u gi a t ng v n chuy n và t ng m ng .
Hình 2.3: Cách dánh d a ch TCP/IP
- Đ nh tuy n d chuy n các gói d li u trong m ng.

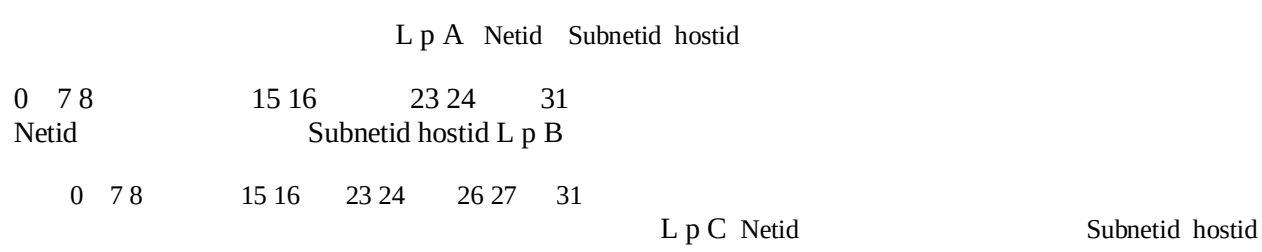
- Th c hi n vi c phân m nh và h p nh t (fragmentation -reassembly) các gói
d li u và nhúng / tách chúng trong các gói d li u t ng liên k t.

1.3. Đ a ch IP

M i d a ch IP có d dài 32 bits (d i v i IP4) du c tách thành 4 vùng

Subneting

Trong nhi u tru ng h p, m t m ng có th du c chia thành nhi u m ng con (subnet), lúc dó có th dua thêm các vùng subnetid d d nh danh các m ng con. Vùng subnetid du c l y t vùng hostid, c th d i v i 3 l p A, B, C nhu sau:

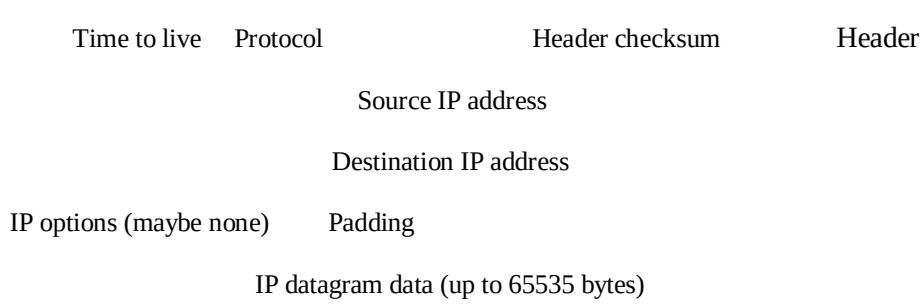


Hình 2.4: B sung vùng subnetid

Tham kh o chi ti t thêm trong giáo trình "Thi t k và xây d ng m ng LAN và WAN"

1.4. C u trúc gói d li u IP

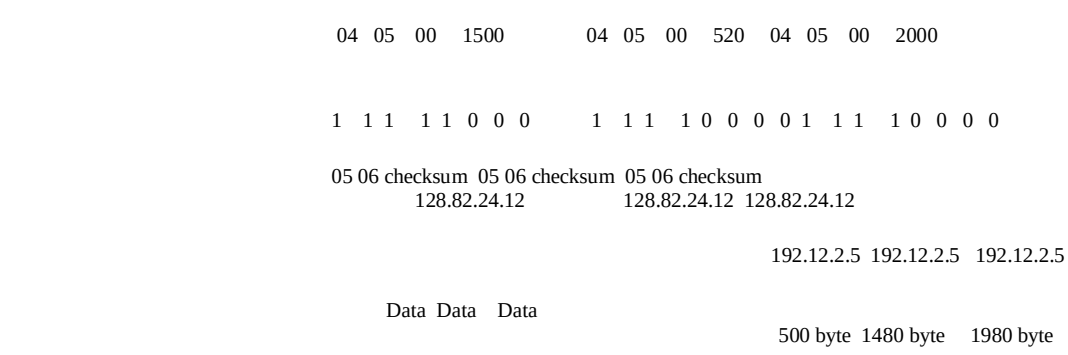
IP là giao th c cung c p d ch v truy n thông theo ki u "không liên k t" (connectionless). Các gói d li u IP du c d nh nghia là các datagram. M i datagram có ph n tiêu d (header) ch a các thông tin c n thi t d chuy n d li u (ví d d a ch IP c a tr m dích). N u d a ch IP dích là d a ch c a m t tr m n m trên cùng m t m ng IP v i tr m ngu n thì các gói d li u s du c chuy n th ng t i dích; n u d a ch IP dích không n m trên cùng m t m ng IP v i máy ngu n thì các gói d li u s du c g i d n m t máy trung chuy n, IP gateway d chuy n ti p. IP gateway là m t thi t b m ng IP d m nh n vi c luu chuy n các gói d li u IP gi a hai m ng IP khác nhau.



Hình 2.5: C u trúc gói d li u TCPIP

1.5. Phân m nh và h p nh t các gói IP

M t gói d li u IP có d dài t i da 65536 byte, trong khi h u h t các t ng liên k t d li u ch h tr các khung d li u nh hon d l n t i da c a gói d li u IP nhi u l n (ví d d dài l n nh t MTU c a m t khung d li u Ethernet là 1500 byte). Vì v y c n thi t ph i có co ch phân m nh khi phát và h p nh t khi thu d i v i các gói d li u IP.



Hình 2.6: Nguyên t c phân m nh gói d li u

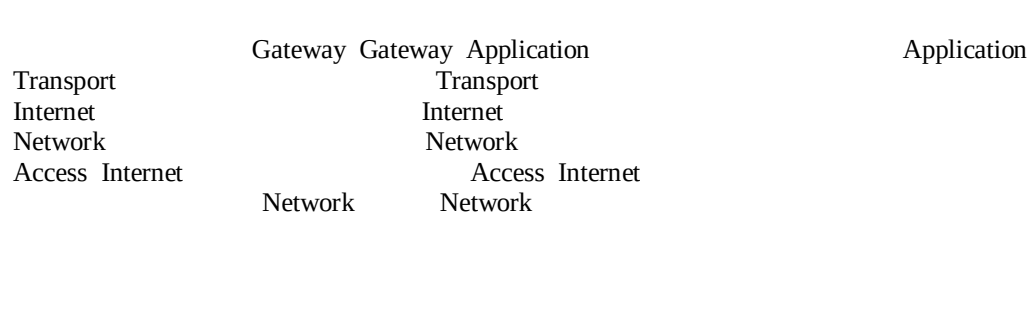
P dùng c MF (3 bit th p c a tru ng Flags trong ph n d u c a gói IP) và tru ng Flagment offset c a gói IP (dã b phân do n) d d nh danh gói IP dó là m t phân do n và v trí c a phân do n này trong gói IP g c. Các gói cùng trong chu i phân m nh d u có tru ng này gi ng nhau. C MF b ng 1 n u là gói d u c a chu i phân m nh và 0 n u là gói cu i c a gói dã du c phân m nh.

1.6. Đ nh tuy n IP

Có hai lo i d nh tuy n:

- Đ nh tuy n tr c ti p: Đ nh tuy n tr c ti p là vi c xác d nh du ng n i gi a hai tr m làm vi c trong cùng m t m ng v t lý.
- Đ nh tuy n không tr c ti p. Đ nh tuy n không tr c ti p là vi c xác d nh du ng n i gi a hai tr m làm vi c không n m trong cùng m t m ng v t lý và vì v y, vi c truy n tin gi a chúng ph i du c th c hi n thông qua các tr m trung gian là các gateway.

Đ ki m tra xem tr m dích có n m trên cùng m ng v t lý v i tr m ngu n hay không, ngu i g i ph i tách l y ph n d a ch m ng trong ph n d a ch IP. N u hai d a ch này có d a ch m ng gi ng nhau thì datagram s du c truy n di tr c ti p; ngu c l i ph i xác d nh m t gateway, thông qua gateway này chuy n ti p các datagram.



Hình 2.7: Đ nh tuy n gi a hai h th ng

2. M t s giao th c di u khi n

2.1. Giao th c ICMP

ICMP ((Internet Control Message Protocol) là m t giao th c di u khi n c a m c IP, du c dùng d trao d i các thông tin di u khi n dòng s li u, thông báo l i và các thông tin tr ng thái khác c a b giao th c TCP/IP. Ví d :

- Đi u khi n luu lu ng d li u (Flow control).
- Thông báo l i : ví d "Destination Unreachable".
- Đ nh hu ng l i các tuy n du ng: gói tin redirect
- Ki m tra các tr m xa: gói tin echo

Ví d khuôn d ng c a thông di p ICMP redirect nhu sau:

0 7 8 15 16 31

type (5) Code(0-3) Checksum

Đ a ch IP c a Router m c d nh

IP header (g m option) và 8 bytes d u c a gói d li u IP ngu n

2.2. Giao th c ARP và giao th c RARP

Trên m t m ng c c b hai tr m ch có th liên l c v i nhau n u chúng bi t d a ch v t lý c a nhau. Nhu v y v n d d t ra là ph i th c hi n ánh x gi a d a ch IP (32 bits) và d a ch v t lý (48 bits) c a m t tr m. Giao th c ARP (Address Resolution Protocol) dã du c xây d ng d chuy n d i t d a ch IP sang d a ch v t lý khi c n thi t. Ngu c l i, giao th c RARP (Reverse Address

Resolution Protocol) du c dùng d chuy n d i d a ch v t lý sang d a ch IP. Các giao th c ARP và RARP không ph i là b ph n c a IP mà IP s dùng d n chúng khi c n.

3. Giao th c l p chuy n t i (Transport Layer)

3.1. Giao th c TCP

TCP (Transmission Control Protocol) là m t giao th c "có liên k t" (connection - oriented), nghia là c n thi t l p liên k t (logic), gi a m t c p th c th TCP tru c khi chúng trao d i d li u v i nhau.

TCP cung c p kh nang truy n d li u m t cách an toàn gi a các máy tr m trong h th ng các m ng. Nó cung c p thêm các ch c nang nh m ki m tra tính chính xác c a d li u khi d n và bao g m c vi c g i l i d li u khi có l i x y ra. TCP cung c p các ch c nang chính sau:

1. Thi t l p, duy trì, k t thúc liên k t gi a hai quá trình.
2. Phân phát gói tin m t cách tin c y.
3. Đánh s th t (sequencing) các gói d li u nh m truy n d li u m t cách tin c y.
4. Cho phép di u khi n l i.
5. Cung c p kh nang da k t n i v i các quá trình khác nhau gi a tr m ngu n và tr m dích nh t d nh thông qua vi c s d ng các c ng.
6. Truy n d li u s d ng co ch song công (full-duplex).

3.1.1 C u trúc gói d li u TCP

0 31

Source port Destination port

Sequence number

Acknowledgment number

Data Resersed U A P R S F

Offset R C S S Y I Window

G K H T N N

Checksum Urgent pointer

Options Padding

TCP data

Có th tham kh o n i dung chi ti t các tru ng trong giáo trình "Thi t k và xây d ng m ng LAN và WAN"

M t ti n trình ng d ng trong m t host truy nh p vào các d ch v c a TCP cung c p thông qua m t c ng (port) nhu sau:

M t c ng k t h p v i m t d a ch IP t o thành m t socket duy nh t trong liên m ng. TCP du c cung c p nh m t liên k t logic gi a m t c p socket. M t socket có th tham gia nhi u liên k t v i các socket xa khác nhau. Tru c khi truy n d li u gi a hai tr m c n ph i thi t l p m t liên k t TCP gi a chúng và khi k t thúc phiên truy n d li u thì liên k t dó s du c gi i phóng. Cung gi ng nhu các giao th c khác, các th c th t ng trên s d ng TCP thông qua các hàm d ch v nguyên thu (service primitives), hay còn g i là các l i g i hàm (function call).

3.1.2 Thi t l p và k t thúc k t n i TCP

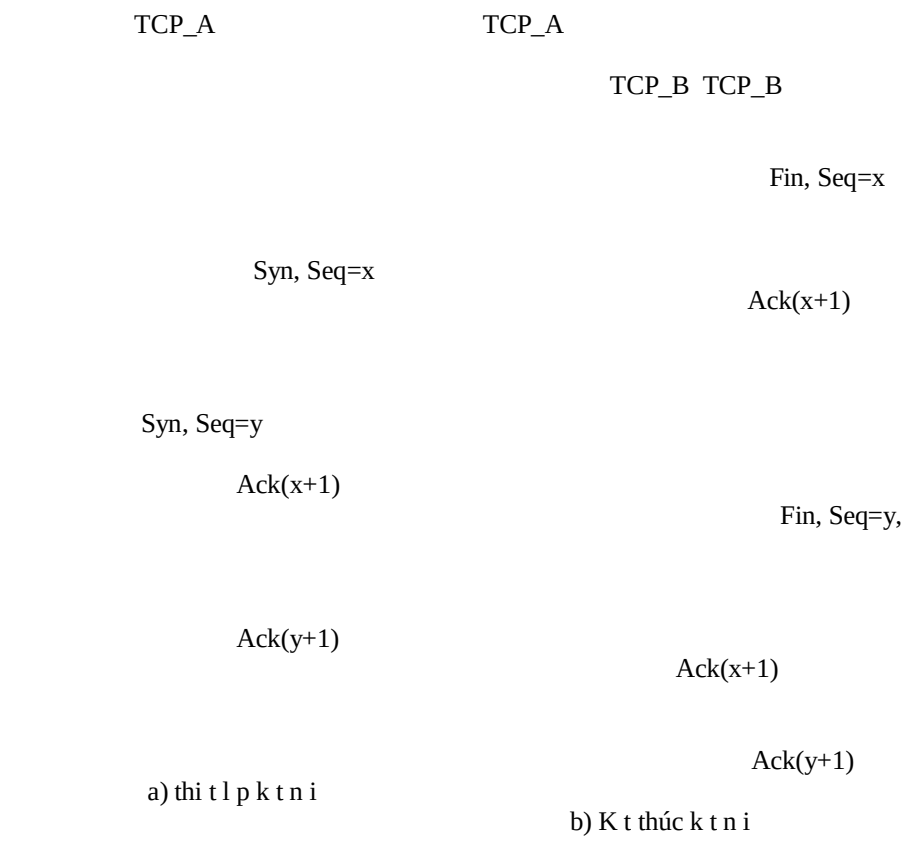
Thi t l p k t n i

Thi t l p k t n i TCP du c th c hi n trên co s phuong th c b t tay ba bu c (Tree - way Handsake) hình sau. Yêu c u k t n i luôn du c ti n trình tr m kh i t o, b ng cách g i m t gói TCP v i c SYN=1 và ch a giá tr kh i t o s tu n t ISN c a client. Giá tr ISN này là m t s 4 byte không d u và du c ta ng m i khi k t n i du c yêu c u (giá tr này quay v 0 khi nó t i giá tr 2). Trong thông di p SYN này còn ch a s hi u c ng TCP c a ph n m m d ch v mà ti n trình tr m mu n k t n i (bu c 1).

M i th c th k t n i TCP d u có m t giá tr ISN m i s này du c tang theo th i gian. Vì m t k t n i TCP có cùng s hi u c ng và cùng d a ch IP du c dùng l i nhi u l n, do dó vi c thay d i giá tr INS ngan không cho các k t n i dùng l i các d li u dã cu (stale) v n còn du c truy n t m t k t n i cu và có cùng m t d a ch k t n i.

Khi th c th TCP c a ph n m m d ch v nh n du c thông di p SYN, nó g i l i gói SYN cùng giá tr ISN c a nó và d t c ACK=1 trong tru ng h p s n sàng nh n k t n i. Thông di p này còn ch a giá tr ISN c a ti n trình tr m trong tru ng h p s tu n t thu d báo r ng th c th d ch v dã nh n du c giá tr ISN c a ti n trình tr m (bu c 2).

Ti n trình tr m tr l i l i gói SYN c a th c th d ch v b ng m t thông báo tr l i ACK cu i cùng. B ng cách này, các th c th TCP trao d i m t cách tin c y các giá tr ISN c a nhau và có th b t d u trao d i d li u. Không có thông di p nào trong ba bu c trên ch a b t k d li u gì; t t c thông tin trao d i d u n m trong ph n tiêu d c a thông di p TCP (bu c 3).



Hình 2.8: Quá trình k t n i theo 3 bu c

K t thúc k t n i

Khi có nhu c u k t thúc k t n i, th c th TCP, ví d c th A g i yêu c u k t thúc k t n i v i FIN=1. Vì k t n i TCP là song công (full-duplex) nên m c dù nh n du c yêu c u k t thúc k t n i c a A (A thông báo h t s li u g i) th c th B v n có th ti p t c truy n s li u cho d n khi B không còn s li u d g i và thông báo cho A b ng yêu c u k t thúc k t n i v i FIN=1 c a mình. Khi th c th TCP dã nh n du c thông di p FIN và sau khi dã g i thông di p FIN c a chính mình, k t n i TCP th c s k t thúc.

PH N II : QU N TR M NG

Qu n tr m ng lu i (network administration) du c d nh nghia là các công vi c qu n lý m ng lu i bao g m cung c p các d ch v h tr , d m b o m ng lu i ho t d ng hi u qu , d m b o ch t lu ng m ng lu i cung c p dúng nhu ch tiêu d nh ra.

Qu n tr h th ng (system administration) du c d nh nghia là các công vi c cung c p các d ch v h tr , d m b o s tin c y, nâng cao hi u qu ho t d ng c a h th ng, và d m b o ch t lu ng d ch v cung c p trên h th ng dúng nhu ch tiêu d nh ra.

M t d nh nghia khái quát v công tác qu n tr m ng là r t khó vì tính bao hàm r ng c a nó. Qu n tr m ng theo nghia m ng máy tính có th du c hi u khái quát là t p bao g m c a các công tác qu n tr m ng lu i và qu n tr h th ng.

Có th khái quát công tác qu n tr m ng bao g m các công vi c sau:

Qu n tr c u hình, tài nguyên m ng : Bao g m các công tác qu n lý ki m soát c u hình, qu n lý các tài nguyên c p phát cho các d i tu ng s d ng khác nhau. Có th tham kh o các công vi c qu n tr c th trong các tài li u, giáo trình v qu n tr h th ng windows, linux, novell netware ...

Qu n tr ngu i dùng, d ch v m ng: Bao g m các công tác qu n lý ngu i s d ng trên h th ng, trên m ng lu i và d m b o d ch v cung c p có d tin c y cao, ch t lu ng d m b o theo dúng các ch tiêu d ra. Có th tham kh o các tài li u, giáo trình qu n tr h th ng windows, novell netware, linux, unix, qu n tr d ch v co b n thu tín di n t , DNS...

Qu n tr hi u nang, ho t d ng m ng : Bao g m các công tác qu n lý, giám sát ho t d ng m ng lu i, d m b o các thi t b , h th ng, d ch v trên m ng ho t d ng n d nh, hi u qu . Các công tác qu n lý, giám sát ho t d ng c a m ng lu i cho phép ngu i qu n tr t ng h p, d báo s phát tri n m ng lu i, d ch v , các di m y u, di m m nh c a toàn m ng, các h th ng và d ch v d ng th i giúp khai thác toàn b h th ng m ng v i hi u su t cao nh t. Có th tham kh o các tài li u, giáo trình v các h th ng qu n tr m ng NMS, HP Openview, Sunet Manager, hay các giáo trình nâng cao hi u nang ho t d ng c a h th ng (performance tuning).

Qu n tr an ninh, an toàn m ng: Bao g m các công tác qu n lý, giám sát m ng lu i, các h th ng d d m b o phòng tránh các truy nh p trái phép, có tính phá ho i các h th ng, d ch v , ho c m c tiêu dánh c p thông tin quan tr ng c a các t ch c, công ty hay thay d i n i dung cung c p lên m ng v i d ng ý x u. Vi c phòng ch ng, ngan ch n s lây lan c a các lo i virus máy tính, các phuong th c t n công ví d nhu DoS làm tê li t ho t d ng m ng hay

d ch v cung là m t ph n c c k quan tr ng c a công tác qu n tr an ninh, an toàn m ng. Đ c bi t, hi n nay khi nhu c u k t n i ra m ng Internet tr nên thi t y u thì các công tác d m b o an ninh, an toàn du c d t lên hàng d u, d c bi t là v i các co quan c n b o m t n i dung thông tin cao d (nhà bang, các co quan lu u tr , các các báo di n t , t p doàn kinh t mui nh n...).

Trong ph n 2 c a giáo trình này s t p trung nghiên c u sâu v m t s ki n th c, k nang co b n và thông d ng nh t v qu n tr m ng. Tuy nhiên, các n i dung trình bày t i ph n 2 s không bao hàm h t du c các n i dung dã khái quát trên do s ph c t p phong phú c a b n thân m i n i dung cung nhu gi i h n v th i gian biên so n. V i m c tiêu cung c p các k nang ph bi n nh t giúp cho các h c viên ti p c n nhanh chóng vào công tác qu n tr m ng d d m duong du c nhi m v co quan, công ty giao cho. Ph n 2 c a giáo trình s bao g m :

- T ng quan v b d nh tuy n trên m ng
- H th ng tên mi n DNS
- D ch v truy c p t xa và d ch v proxy
- Firewall và b o m t h th ng

H c viên cung có th tham kh o b sung thêm ki n th c v qu n tr m ng v i các giáo trình v m ng c c b , giáo trình v thu tín di n t , giáo trình v các h di u hành Windows, Linux, Unix là các n i dung biên so n trong b các giáo trình ph c v dào t o cho d án 112.

Chuong 3
T ng quan v b d nh tuy n

Chuong ba cung c p các ki n th c co b n v b d nh tuy n trên m ng và các b chuy n m ch l p 3. Các thi t b này là m t ph n thi t y u c a m ng máy tính hi n d i và là các thi t b h t ng c t lõi. Các minh h a tu ng t n v c u trúc c a các s n ph m hãng Cisco s giúp h c viên n m v ng các lý thuy t h th ng d c bi t là lý thuy t d nh tuy n. Ph n n i dung cung b sung các k nang c u hình ho t d ng c a thi t b trên các giao th c m ng WAN khác nhau nhu Frame Relay, X.25...

Chuong ba dòi h i các h c viên c n có các ki n th c so kh i v các giao th c trên m ng di n r ng nhu Frame Relay, X.25..., các ki n th c v d a ch l p 2, l p 3.

1. Lý thuy t v b d nh tuy n

1.1. T ng quan v b d nh tuy n

B d nh tuy n là thi t b du c s d ng trên m ng d th c thi các ho t d ng x lý truy n t i thông tin trên m ng. Có th xem b d nh tuy n là m t thi t b máy tính du c thi t k d c bi t d d m duong du c vai trò x lý truy n t i thông tin trên m ng c a nó và do dó nó cung bao g m các CPU, trái tim c a m i ho t d ng, b nh ROM, RAM, các giao ti p, các bus d li u, h di u hành v.v...

Ch c nang c a b d nh tuy n là d nh hu ng cho các gói tin du c truy n t i qua b d nh tuy n. Trên co s các thu t toán d nh tuy n, thông tin c u hình và chuy n giao, các b d nh tuy n s quy t d nh hu ng di t t nh t cho các gói tin du c truy n t i qua nó. B d nh tuy n còn có vai trò d x lý các nhu c u truy n t i và chuy n d i giao th c khác.

Vai trò c a b d nh tuy n trên m ng là d m b o các k t n i liên thông gi a các m ng v i nhau, tính toán và trao d i các thông tin liên m ng làm can c cho các b d nh tuy n ra các quy t d nh truy n t i thông tin phù h p v i c u hình th c t c a m ng. B d nh tuy n làm vi c v i nhi u công ngh d u n i m ng di n r ng khác nhau nhu FRAME RELAY, X.25, ATM, SONET, ISDN, xDSL... d m b o các nhu c u k t n i m ng theo nhi u các công ngh và d chu n m c khác nhau mà n u thi u vai trò c a b d nh tuy n thì không th th c hi n du c.

1.2. Các ch c nang chính c a b d nh tuy n, tham chi u mô hình OSI

Mô hình OSI dã du c h c chuong 1 g m 7 l p trong dó bao g m:

- 3 l p thu c v các l p ng d ng
- o l p ng d ng

- o l p trình bày
- o l p phiên
- 4 l p thu c v các l p truy n thông
- o l p v n chuy n
- o l p m ng
- o l p liên k t d li u
- o l p v t lý

Đ i v i các l p truy n thông:

- L p v n chuy n: phân chia / tái thi t d li u thành các dòng ch y d li u. Các ch c nang chính bao g m di u khi n dòng d li u, da truy nh p, qu n lý các m ch o, phát hi n và s a l i. TCP, UDP là hai giao th c thu c h giao th c Internet (TCP/IP) thu c v l p v n chuy n này.
- L p m ng: cung c p ho t d ng d nh tuy n và các ch c nang liên quan khác cho phép k t h p các môi tru ng liên k t d li u khác nhau l i v i nhau cùng t o nên m ng th ng nh t. Các giao th c d nh tuy n ho t d ng trong l p m ng này.
- L p liên k t d li u: cung c p kh nang truy n t i d li u t qua môi tru ng truy n d n v t lý. M i d c t khác nhau c a l p liên k t d li u s có các d nh nghia khác nhau v giao th c và các chu n m c k t n i d m b o truy n t i d li u.
- L p v t lý: d nh nghia các thu c tính di n, các ch c nang, thu ng trình dùng d k t n i các thi t b m ng m c v t lý. M t s các thu c tính du c d nh nghia nhu m c di n áp, d ng b , t c d truy n t i v t lý, kho ng cách truy n t i cho phép...

Trong môi tru ng truy n thông, các thi t b truy n thông giao ti p v i nhau thông qua các h giao th c truy n thông khác nhau du c xây d ng d a trên các mô hình chu n OSI nh m d m b o tính tuong thích và m r ng. Các giao th c truy n thông thu ng du c chia vào m t trong b n nhóm: các giao th c m ng c c b , các giao th c m ng di n r ng, giao th c m ng và các giao th c d nh tuy n. *Giao th c m ng c c b* ho t d ng trên l p v t lý và l p liên k t d li u. *Giao th c m ng di n r ng* ho t d ng trên 3 l p du i cùng trong mô hình OSI. *Giao th c d nh tuy n* là giao th c l p m ng và d m b o cho các ho t d ng d nh tuy n và truy n t i d li u. *Giao th c m ng* là các h các giao th c cho phép giao ti p v i l p ng d ng.

Vai trò c a b d nh tuy n trong môi tru ng truy n thông là d m b o cho các k t n i gi a các m ng khác nhau v i nhi u giao th c m ng, s d ng các công ngh truy n d n khác nhau.

Ch c nang chính c a b d nh tuy n là:

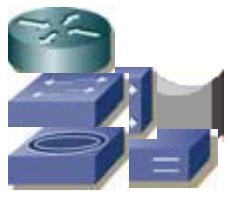
- Đ nh tuy n (routing)
- Chuy n m ch các gói tin (packet switching)

Đ nh tuy n là ch c nang d m b o gói tin du c chuy n chính xác t i đ a ch c n đ n. *Chuy n m ch các gói tin* là ch c nang chuy n m ch s li u, truy n t i các gói tin theo hu ng dã đ nh trên co s các đ nh tuy n du c đ t ra. Nhu v y, trên m i b đ nh tuy n, ta ph i xây d ng m t b ng đ nh tuy n, trên đó ch rõ đ a ch c n đ n và du ng di cho nó. B đ nh tuy n đ a vào đ a ch c a gói tin k t h p v i b ng đ nh tuy n đ chuy n gói tin di đúng đ n đích. Các gói tin không có đúng đ a ch đích trên b ng đ nh tuy n s b hu .

Ch c nang đ u tiên c a b đ nh tuy n là ch c nang đ nh tuy n nhu tên g i c a nó cung là ch c nang chính c a b đ nh tuy n làm vi c v i các *giao th c đ nh tuy n.* B đ nh tuy n du c x p vào các thi t b m ng làm vi c l p 3, l p m ng.

B ng 3-1:Tuong duong ch c nang thi t b trong mô hình OSI

L p 3 L p m ng



L p 2 L p liên k t d li u

L p 1 L p v t lý

Ch c na ng khác c a b đ nh tuy n là cho phép s đ ng các phuong th c truy n thông khác nhau đ đ u n i đi n r ng. Ch c nang k t n i đi n r ng WAN c a b đ nh tuy n là không th thi u đ đ m b o vai trò k t n i truy n thông gi a các m ng v i nhau. Ch c nang k t n i m ng c c b , b t k b đ nh tuy n nào cung c n có ch c nang này đ đ m b o k t n i đ n vùng đ ch v c a m ng. B đ nh tuy n còn có các ch c nang đ m b o ho t đ ng cho các giao th c m ng mà nó qu n lý.

1.3. C u hình co b n và ch c nang c a các b ph n c a b đ nh tuy n

Nhu dã nói ph n tru c, b đ nh tuy n là m t thi t b máy tính du c thi t k đ c bi t đ đ m duong du c vai trò x lý truy n t i thông tin trên m ng. Nó du c thi t k bao g m các ph n t không th thi u nhu CPU, b nh ROM, RAM, các bus đ li u, h đi u hành. Các ph n t khác tùy theo nhu c u s đ ng có th có ho c không bao g m các giao ti p, các module và các tính nang đ c bi t c a h đi u hành.

CPU : đi u khi n m i ho t đ ng c a b đ nh tuy n trên co s các h th ng chuong trình th c thi c a h đi u hành.

ROM : ch a các chuong trình t đ ng ki m tra và có th có thành ph n co b n nh t sao cho b đ nh tuy n có th th c thi du c m t s ho t đ ng t i thi u ngay c khi không có h đi u hành hay h đi u hành b h ng.

RAM : gi các b ng đ nh tuy n, các vùng đ m, t p tin c u hình khi ch y, các thông s đ m b o ho t đ ng c a b đ nh tuy n khác.

Flash : là thi t b nh / lu u tr có kh nang xoá và ghi du c, không m t d li u khi c t ngu n. H đi u hành c a b đ nh tuy n du c ch a dây. Tùy thu c các b đ nh tuy n khác nhau, h đi u hành s du c ch y tr c ti p t

Flash hay du c giãn ra RAM tru c khi ch y. T p tin c u hình cung có th du c lu u tr trong Flash.

H di u hành : d m duong ho t d ng c a b d nh tuy n. H di u hành c a các b d nh tuy n khác nhau có các ch c nang khác nhau và thu ng du c thi t k khác nhau. M i b d nh tuy n có th ch y r t nhi u h di u hành khác nhau tùy thu c vào nhu c u s d ng c th , các ch c nang c n thi t ph i có c a b d nh tuy n và các thành ph n ph n c ng có trong b d nh tuy n. Các thành ph n ph n c ng m i yêu c u có s nâng c p v h di u hành. Các tính nang d c bi t du c cung c p trong các b n nâng c p riêng c a h di u hành.

Các giao ti p : b d nh tuy n có nhi u các giao ti p trong dó ch y u bao g m:

- Giao ti p WAN: d m b o cho các k t n i di n r ng thông qua các phuong th c truy n thông khác nhau nhu leased-line, Frame Relay, X.25, ISDN, ATM, xDSL ... Các giao ti p WAN cho phép b d nh tuy n k t n i theo nhi u các giao di n và t c d khác nhau: V.35, X.21, G.703, E1, E3, cáp quang v.v...
- Giao ti p LAN: d m b o cho các k t n i m ng c c b , k t n i d n các vùng cung c p d ch v trên m ng. Các giao ti p LAN thông d ng: Ethernet, FastEthernet, GigaEthernet, cáp quang.

2. Gi i thi u v b d nh tuy n Cisco

2.1. Gi i thi u b d nh tuy n Cisco

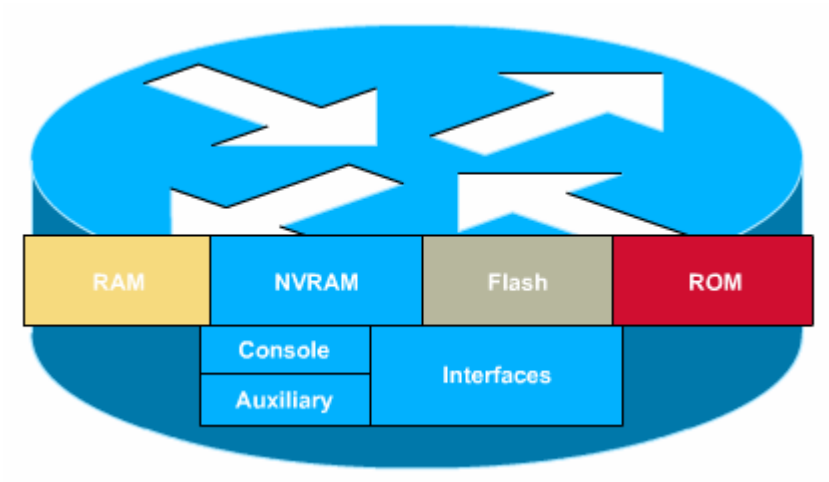
So lu c v b d nh tuy n

B d nh tuy n Cisco bao g m nhi u n n t ng ph n c ng khác nhau du c thi t k xây d ng cho phù h p v i nhu c u và m c dích s d ng c a các gi i pháp khác nhau.

Các ch c nang x lý ho t d ng c a b d nh tuy n Cisco d a trên n n t ng c t lõi là h di u hành IOS.

Tu theo các nhu c u c th mà m t b d nh tuy n Cisco s c n m t IOS có các tính nang phù h p. IOS có nhi u phiên b n khác nhau, m t s lo i ph n c ng m i du c phát tri n ch có th du c h tr b i các IOS phiên b n m i nh t.

Các thành ph n c u thành b d nh tuy n



Hình 3.1:Các thành ph n c a b d nh tuy n Cisco

- RAM: Gi b ng d nh tuy n, ARP Cache, fast-switching cache, packet buffer, và là noi ch y các file c u hình cho b d nh tuy n. Đây chính là noi luu gi file Running-Config, ch a c u hình dang ho t d ng c a Router. Khi ng ng c p ngu n cho b d nh tuy n, b nh này s t d ng gi i phóng. T t c các thông tin trong file Running-Config s b m t hoàn toàn.
- NVRAM: non-volatile RAM, là noi gi startup/backup configure, không b m t thông tin khi m t ngu n vào. File Startup-Config du c luu trong này d d m b o khi kh i d ng l i, c u hình c a b d nh tuy n s du c t d ng dua v tr ng thái dã luu gi trong file. Vì v y, ph i thu ng xuyên luu file Running-Config thành file Startup-Config.
- Flash: Là ROM có kh nang xoá, và ghi d c. Là noi ch a h di u hành IOS c a b d nh tuy n. Khi kh i d ng, b d nh tuy n s t d c ROM d n p IOS tru c khi n p file Startup-Config trong NVRAM.
- ROM: Ch a các chuong trình t d ng ki m tra.
- C ng Console: Đu c s d ng d c u hình tr c ti p b d nh tuy n. T c d d li u dùng cho c u hình b ng máy tính qua c ng COM là 9600b/s. Giao di n ra c a c ng này là RJ45 female.
- C ng AUX: Đu c s d ng d qu n lý và c u hình cho b d nh tuy n thông qua modem d phòng cho c ng Console. Giao di n ra c a c ng này cung là RJ45 female.
- Các giao di n:
    - C ng Ethernet / Fast Ethernet
    - C ng Serial
    - C ng ASYNC ...

2.2. M t s tính nang uu vi t c a b d nh tuy n Cisco

- Có kh nang tích h p nhi u ch c nang x lý trên cùng m t s n ph m v i vi c s d ng các module ch c nang thích h p và IOS thích h p.
- D dàng trong vi c nâng c p b d nh tuy n Cisco c v ph n m m l n ph n c ng do dó d dàng dáp ng các nhu c u thay d i, m r ng m ng, dáp ng các nhu c u phát tri n và ng d ng công ngh m i.
- Tuong thích và d dàng m r ng cho các nhu c u v da d ch v ngày càng gia tang trên.
- Tính b n v ng, an toàn và b o m t.

2.3. M t s b d nh tuy n Cisco thông d ng

B d nh tuy n Cisco 2500

- B d nh tuy n Cisco 2509
- 01 c ng console, 01 AUX
- 02 c ng serial t c d t i 2Mbps: k t n i leased-line, X.25, Frame Relay...

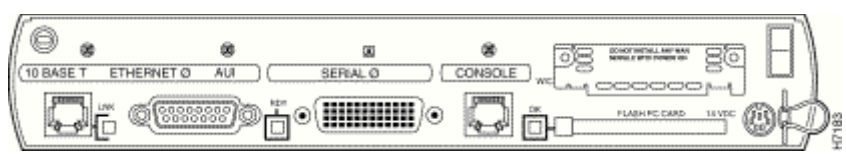
- 01 Ethernet t c d 10Mbps giao di n AUI: c n thi t có d u chuy n RJ45/AUI khi k t n i vào các m ng switch/hub thông thu ng.

Hình 3.2: B d nh tuy n Cisco 2501

- 01 c ng Async cho phép k t n i d n 08 modem V34/V90. S d ng môt cáp k t n i Octal d k t n i các modem d n b d nh tuy n.
- B d nh tuy n Cisco 2501
- 01 c ng console, 01 AUX
- 02 c ng serial t c d t i 2Mbps: k t n i leased-line, X.25, Frame Relay...
- 01 Ethernet t c d 10Mbps giao di n AUI: c n thi t có d u chuy n RJ45/AUI khi k t n i vào các m ng switch/hub thông thu ng

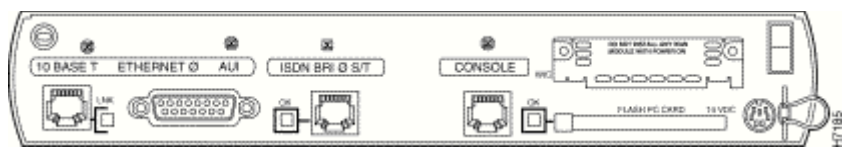
Cisco dã ng ng s n xu t các b d nh tuy n Cisco dòng 2500.

B d nh tuy n Cisco 1600



Hình 3.3: B d nh tuy n Cisco 1601

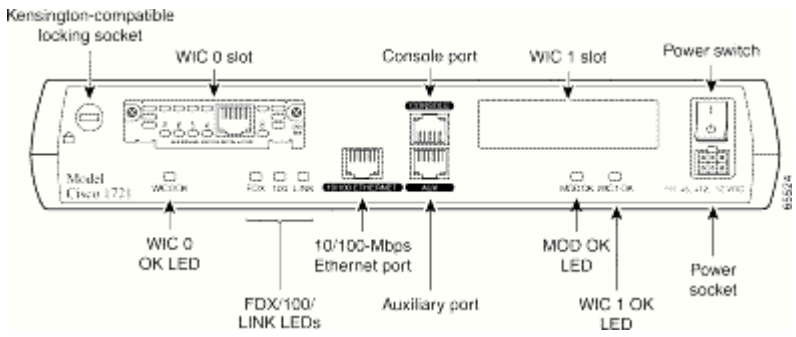
- B d nh tuy n Cisco 1601
- 01 c ng console
- 01 c ng serial t c d t i 2Mbps: k t n i leased-line, X.25, Frame Relay...
- 01 Ethernet t c d 10Mbps giao di n AUI và RJ48 (Female Socket for RJ45 connector)
- 01 serial slot: có th s d ng cho c ng Serial th 2, card ISDN BRI



Hình 3.4: B d nh tuy n Cisco 1603

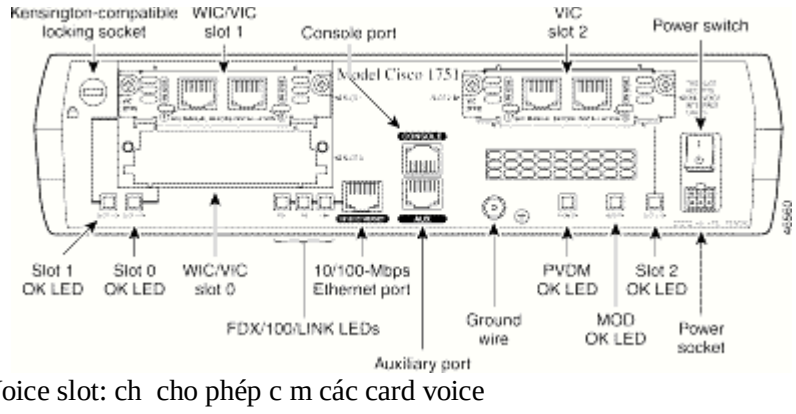
- B d nh tuy n Cisco 1603
- 01 c ng console
- 01 c ng ISDN BRI giao di n S/T: k t n i ISDN t c d 2B+D, khi s d ng Vi t nam c n có thêm m t b ti p h p NT1 d d u n i vào m ng ISDN.
- 01 Ethernet t c d 10Mbps giao di n AUI và RJ48 (Female Socket for RJ45 connector)
- 01 serial slot: có th s d ng cho c ng Serial, card ISDN BRI

B d nh tuy n Cisco 1700



Hình 3.5: B d nh tuy n Cisco 1721

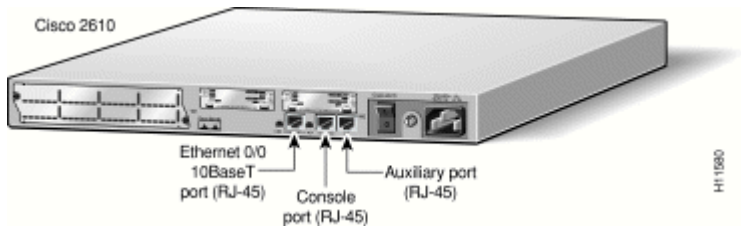
- B d nh tuy n Cisco 1721
- 01 c ng console, 01 AUX
- 01 FastEthernet t c d 10/100Mbps giao di n RJ48 (Female Socket for RJ45 connector)
- 02 WAN slot: có th s d ng cho c ng Serial, card ISDN BRI...



Hình 3.6: B d nh tuy n Cisco 1751

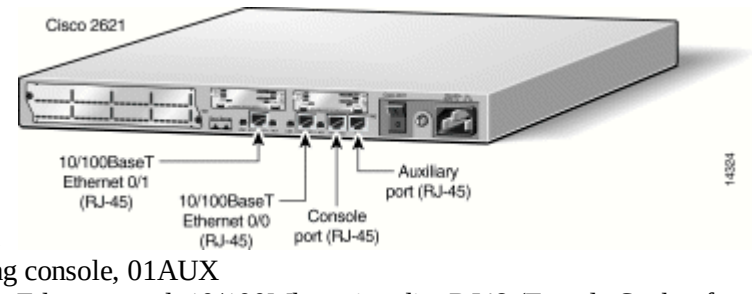
- B d nh tuy n Cisco 1751
- 01 c ng console, 01 AUX
- 01 FastEthernet t c d 10/100Mbps giao di n RJ48 (Female Socket for RJ45 connector)
- 02 WAN slot: có th s d ng cho c ng Serial, card ISDN BRI...
- 01 Voice slot: ch cho phép c m các card voice

B d nh tuy n Cisco 2600



Hình 3.7: B d nh tuy n Cisco 2610

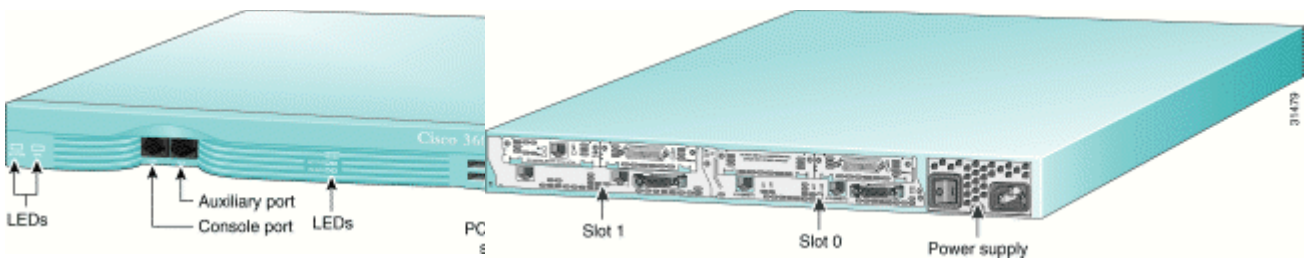
- B d nh tuy n Cisco 2610
- 01 c ng console, 01AUX
- 01 Ethernet t c d 10Mbps giao di n RJ48 (Female Socket for RJ45 connector)
- 02 serial slot: có th s d ng cho c ng Serial, card ISDN BRI, card voice...
- 01 network module slot: có th s d ng module Async, Sync/Async, Channelized E1, PRI ...



Hình 3.8: B d nh tuy n Cisco 2621

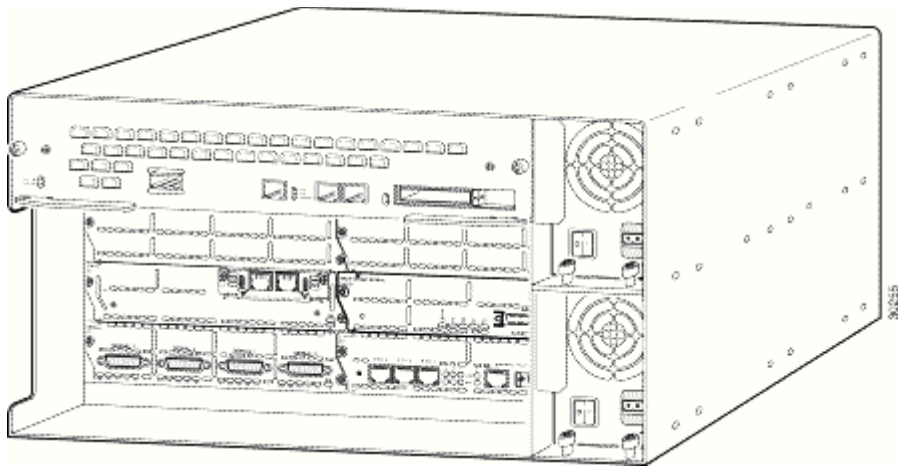
- B d nh tuy n Cisco 2621
- 01 c ng console, 01AUX
- 02 FastEthernet t c d 10/100Mbps giao di n RJ48 (Female Socket for RJ45 connector)
- 02 serial slot: có th s d ng cho c ng Serial, card ISDN BRI, card voice...
- 01 network module slot: có th s d ng module Async, Sync/Async, Channelized E1, PRI ...

B d nh tuy n Cisco 3600



Hình 3.9: B d nh tuy n Cisco 3620

- B d nh tuy n 3620
- 01 c ng console, 01AUX
- PCMCIA slot
- 02 network module slot: có th s d ng module Async, Sync/Async, Channelized E1, PRI, Ethernet/FastEthernet, Voice, VPN ...
- Khi k t n i v i m ng LAN c n thi t có m t Network module có c ng Ethernet/FastEthernet



Hình 3.10: B d nh tuy n Cisco 3661

- B d nh tuy n 3661
- 01 c ng console, 01AUX
- PCMCIA slot
- 01 FastEthernet t c d 100Mbps
- 06 network module slot: có th s d ng module Async, Sync/Async, Channelized E1, PRI, Ethernet/FastEthernet, Voice, VPN ...
- 02 module ngu n, h tr và d phòng l n nhau, d m b o v m t cung c p ngu n di n cho b d nh tuy n. Có th thay th module ngu n mà không c n ph i t t di n toàn b b d nh tuy n.

2.4. Các giao ti p c a b d nh tuy n Cisco

- C ng Console
  - T c d có th 11500Bps, làm vi c t c d 9600Bps
  - Dùng cho c u hình cho b d nh tuy n Cisco
  - S d ng cáp Console d k t n i
- C ng AUX
  - T c d 11500Bps
  - S d ng cho qu n tr /c u hình t xa qua modem V34/V90
  - Có th s d ng d c u hình tr c ti p s d ng cáp Console
  - Ch làm vi c sau khi b d nh tuy n Cisco dã kh i d ng hoàn toàn

- o Có th c u hình d AUX làm vi c nhu m t du ng k t n i d phòng
- Ethernet/FastEthernet
  - o T c d 10Mbps/100Mbps giao di n AUI ho c RJ45
  - o Dùng cho d u n i tr c ti p vào m ng LAN
  - o Tuân theo các chu n c a IEEE802.3
- Serial
  - o T c d k t n i t i 2Mbps
  - o Dùng cho k t n i m ng WAN
  - o Có kh na ng k t n i theo nhi u chu n giao di n khác nhau V35, V24, X21, EIA530... b ng vi c s d ng các cáp n i
- ISDN
  - o T c d 2B+D
  - o Dùng cho k t n i m ng ISDN s d ng cho Dialup Server ho c k t n i d phòng
  - o Có các giao di n U ho c S/T, giao di n S/T c n thi t có thi t b NT1 d k t n i vào m ng
- Async
  - o Giao di n truy n s li u không d ng b
  - o Dùng cho k t n i v i các h th ng modem V34/V90
  - o S d ng cáp k t n i Async (Octal Cable) d n i t i 08 modem. Octal cable thu ng có giao di n RJ45 và c n có chuy n d i RJ45-DB25 d phù h p v i giao di n c a modem

2.5. Ki n trúc module c a b d nh tuy n Cisco

Các b d nh tuy n có ki n trúc module

Các b d nh tuy n Cisco thông d ng du c gi i thi u ph n tru c h u h t là có ki n trúc module tr b d nh tuy n 2500 dã không du c ti p t c s n xu t.

Ngoài các b d nh tuy n có ki n trúc module dã du c bi t, còn có các b d nh tuy n khác:

- **1600** : 1601, 1602, 1603, 1604, 1605
- **1700** : 1710, 1720, 1721, 1750, 1751, 1760
- **2600** : 2610, 2160XM, 2611, 2611XM, 2612, 2613, 2620, 2620XM, 2621, 2621XM, 2650, 2650XM, 2651, 2651XM, 2691
- **3600** : 3620, 3631, 3640, 3661, 3662
- **3700** : 3725, 3745

Tính tuong thích dùng l n và thay th

Các b d nh tuy n có ki n trúc module c a Cisco du c thi t k d s d ng chung m t kho các card giao ti p và module ch c nang khác nhau.

Các card giao ti p du c s d ng cho b t k m t b d nh tuy n nào có khe c m tuong thích. Tuong thích ph bi n nh t là card giao ti p Serial. Card giao ti p serial có th s d ng trên b t k b d nh tuy n nào. M t s card giao ti p khác nhu card voice s yêu c u v c u hình ph n c ng và ph n m m t i thi u. Các card giao ti p du c s d ng cho các b d nh tuy n 1600, 1700 có th s d ng cho các b d nh tuy n 2600, 3600.

B d nh tuy n 2600, 3600, 3700 cho phép s d ng các module ch c nang khác nhau. M t module ch c nang có th ch bao g m m t ch c nang nhu module Async, module Serial, cung có th bao g m nhi u ch c nang hay bao g m các khe c m cho card giao ti p khác nhu module NM-1E- có 01 c ng Ethernet và 02 khe c m cho b t k m t lo i card tuong thích nào. Vi c l a ch n module tùy thu c vào nhu c u s d ng c th . Các module cùng du c s d ng gi a các b d nh tuy n. M t s module yêu c u c u hình t i thi u v ph n c ng và ph n m m. B d nh tuy n 1600 và 1700 không cho phép s d ng các module nhu các b d nh tuy n 2600, 3600.

M t s module thu ng g p

Hình 3.11: Module Ethernet/FastEthernet

B ng 3-2:M t s lo i module Ethernet/FastEthernet

Lo i module	c ng	S khe c m WAN
		S LAN
Single-Port Ethernet	1	None
Four-Port Ethernet	4	None
Single-Port Ethernet Mixed Media	1	Two WAN interface card slots
Dual-Port Ethernet Mixed Media	2	Two WAN interface card slots
Single-Port Ethernet and Single-Port Token Ring	1/1	Two WAN interface card slots
Single Port Fast Ethernet	1	None

Hình 3.12: Module Ethernet có khe c m WAN

B ng 3-3: M t s lo i module có khe c m WAN

Tên module	Lo i module
NM-1FE2W/NM-1FE2W-V2	1 10/100 Ethernet, 2 khe c m WAN
NM-2FE2W/NM-2FE2W-V2	2 10/100 Ethernet, 2 khe c m WAN
NM-1FE1R2W	1 10/100 Ethernet, 1 4/16 Token Ring,

2 khe c m WAN

NM-2W 2 khe c m WAN

B ng 3-4: Gi i h n s lu ng module trên các b d nh tuy n

2600	2691	3620	3631	3640	3660	3725	3745
NM-1FE2W/NM-1FE2W-V2	N/A	1	2	N/A	4	6	2 4
NM-2FE2W/NM-2FE2W-V2	N/A	1	2	N/A	4	6	2 4
NM-1FE1R2W	N/A	1	2	N/A	4	6	2 4
NM-2W	1	1	1	N/A	3	6	2 4

Hình 3.13: Module 4 c ng serial

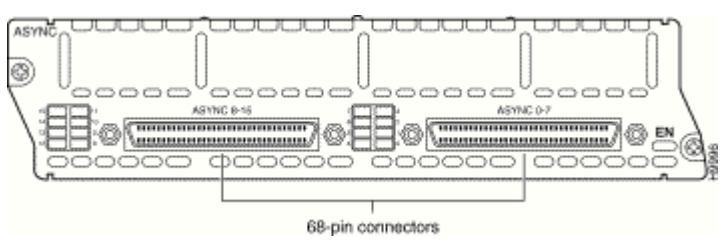
- Module 4 c ng serial
- H tr t ng lu u lu ng 8Mbps: có th s d ng t c d t i da 8Mbps trên m t c ng ho c m i 2Mbps cho 4 c ng.
- K t n i v i modem theo các chu n V.35, X.21, EIA/TIA-232, EIA/TIA530... s d ng các cáp phù h p
- S d ng cho d u n i leased-line, Frame Relay, X.25 ...

Hình 3.14: Module 8 c ng Sync/Async

-
- T
-

Module 8 c ng Sync/Async
c d k t n i trên m i c ng th p (t i da 128Kbps)
Có th s d ng hai ch d d ng b và không d ng b . Có th s d ng cho modem quay s .

- K t n i v i modem theo các chu n V.35, X.21, EIA/TIA-232, EIA/TIA530... s d ng các cáp phù h p
- S d ng cho d u n i leased-line, Frame Relay, X.25, modem quay s ...



Hình 3.15: Module 16 c ng Async

- Module 16 c ng Async
- K t n i không d ng b s d ng cho modem quay s .
- K t n i v i modem theo các chu n EIA/TIA-232 s d ng cáp Octal

Hình 3.16: Module và card ISDN BRI

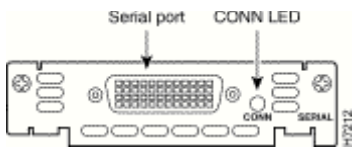
B ng *3-5: M t s lo i module ISDN BRI t c d 2B+D (128+16Kbps)*

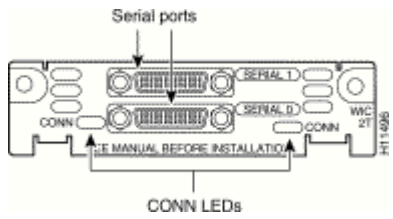
Lo i module	Mô t
NM-4B-S/T	4 c ng ISDN BRI giao di n S/T
NM-4B-U	4 c ng ISDN BRI giao di n U (tích h p b ti p h p NT1)
NM-8B-S/T	8 c ng ISDN BRI giao di n S/T
NM-8B-U	8 c ng ISDN BRI giao di n U (tích h p b ti p h p NT1)

B ng 3-6: M t s lo i card giao ti p ISDN BRI t c d 2B+D (128+16Kbps)

Lo i card	Mô t
WIC-1B-S/T-V2	1 c ng ISDN BRI giao di n S/T
WIC 1B-U-V2	1 c ng ISDN BRI giao di n U (tích h p b ti p h p NT1)

Hình 3.17: Card giao ti p Serial





46

- Card m t và hai c ng giao ti p Serial
- K t n i d ng b t c d d n 2Mbps
- K t n i v i modem theo các chu n V.35, X.21, EIA/TIA-232, EIA/TIA530... s d ng các cáp phù h p
- S d ng cho d u n i leased-line, Frame Relay, X.25, modem quay s ...

3. Cách s d ng l nh c u hình b d nh tuy n

3.1. Gi i thi u giao ti p dòng l nh c a b d nh tuy n Cisco

Giao ti p dòng l nh

Giao ti p dòng l nh CLI (Command Line Interface) khác v i các giao ti p d h a GUI (Graphic User Interface) là giao ti p d c bi t du c Cisco thi t k cho phép ngu i dùng, ngu i qu n tr làm vi c v i các thi t b c a Cisco thông qua các dòng l nh tr c ti p.

V i giao ti p dòng l nh, ngu i dùng, ngu i qu n tr có th tr c ti p xem, c u hình các thi t b c a Cisco thông qua các l nh phù h p. Đ có th s d ng du c giao ti p dòng l nh, ngu i dùng ph i n m v ng du c các l nh, các tham s l nh và cách s d ng các l nh.

M i thi t b c a Cisco d u có r t nhi u các l nh, các b l nh di kèm tuy nhiên ngu i s d ng, ngu i qu n tr không nh t thi t ph i hi u h t toàn b các l nh trong m i thi t b mà ch c n hi u, n m v ng m t s l nh c n thi t cho các m c dích s d ng c th .

Giao ti p dòng l nh c a Cisco cung c p cho ngu i dùng kh nang s d ng tr giúp tr c tuy n. Đi u dó có nghia là trong quá trình làm vi c v i thi t b thông qua giao ti p dòng l nh, ngu i dùng có th li t kê các l nh, xem l i ý nghia s d ng c a nó hay th m chí xem các thông s l nh.

Lu u ý: khi s d ng giao ti p dòng l nh d c u hình thi t b , sau khi l nh du c th c thi (n phím Enter) các ho t d ng c a b d nh tuy n s nh hu ng ngay l p t c b i l nh th c thi dó. M t cho nh ng ví d là khi dang th c hi n c u hình t xa thông qua telnet, n u thay d i d a ch c a b d nh tuy n, s l p t c m t k t n i d n b d nh tuy n và ch có th th c hi n c u hình b d nh tuy n tr c ti p t c ng console. Đi u này có nghia c n thi t ph i r t c n th n và ch c ch n cung nhu th c hi n dúng trình t m i khi th c hi n c u hình b d nh tuy n.

Ví d v giao ti p dòng l nh nhu sau:

```
Router#config terminal
Router(config)#interface s0/0
Router(config-if)#encapsolution ppp
Router(config-if)#ip address 192.168.100.5 255.255.255.0
```

Các kh nang th c hi n c u hình b d nh tuy n Cisco

- C u hình b d nh tuy n tr c ti p t c ng console: là phuong pháp s d ng m t cáp console thông qua m t ph n m m k t n i tr c ti p c ng COM nhu HyperTerminal c a WINDOWS d truy nh p vào b d nh tuy n sau dó c u hình b d nh tuy n theo giao th c dòng l nh. Phuong pháp c u hình này du c s d ng nhi u nh t và trong h u h t các tru ng h p. Các b d nh tuy n s d ng l n d u cung ph i du c c u hình b ng phuong pháp này.

- C u hình b d nh tuy n thông qua truy nh p t xa telnet: truy nh p t xa t i b d nh tuy n v i telnet ch có th th c hi n du c khi b d nh tuy n dã du c c u hình v i ít nh t m t d a ch m ng, có m t kh u b o v và máy tính s d ng d c u hình b d nh tuy n ph i có kh nang k t n i du c v i b d nh tuy n thông qua môi tru ng m ng. Sau khi k t n i du c t i b d nh tuy n, s d ng giao di n dòng l nh d c u hình b d nh tuy n.

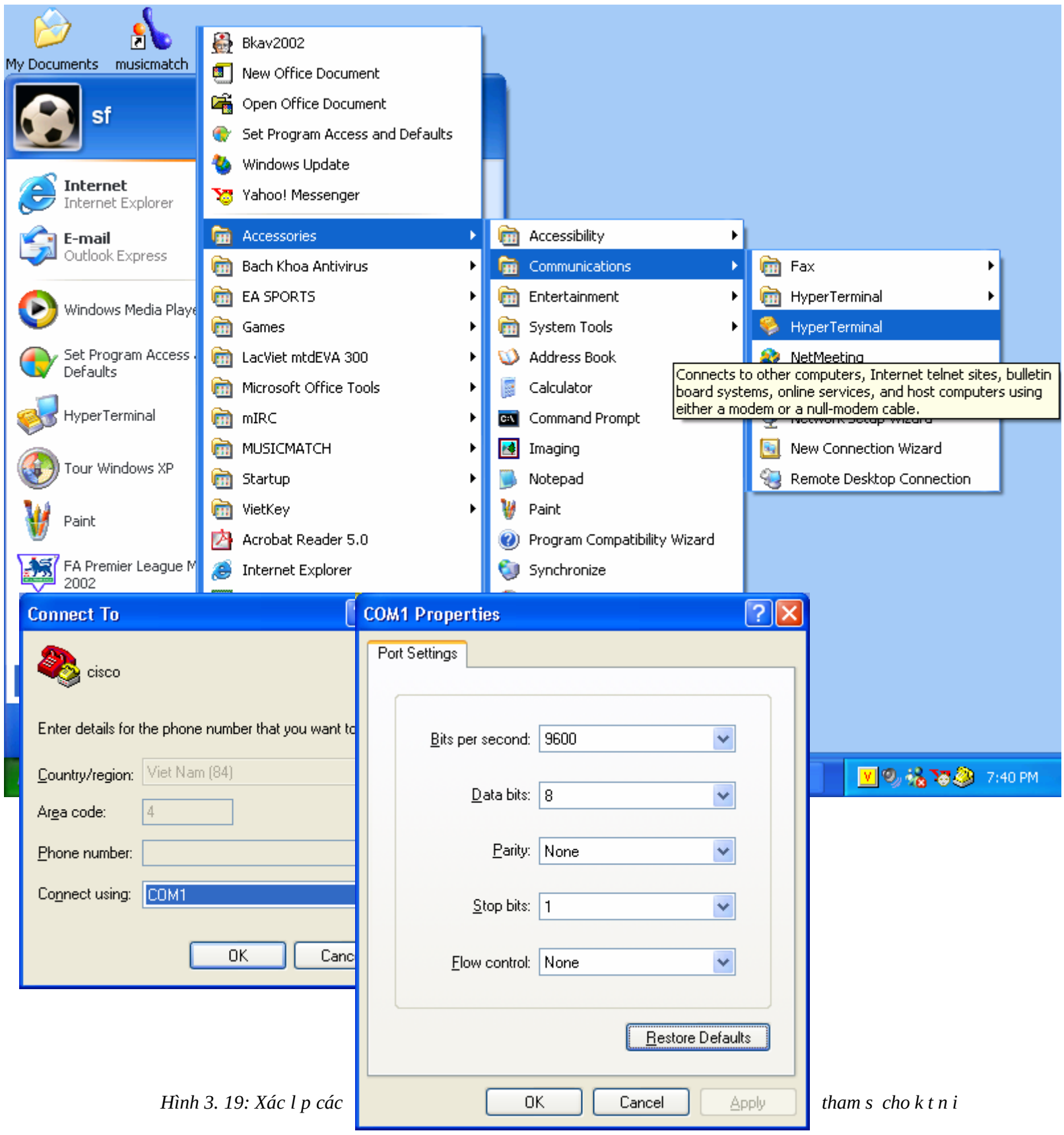
- C u hình b d nh tuy n s d ng t p tin c u hình luu tr trên máy ch TFTP: trong m t s tru ng h p, t p tin c u hình cho b d nh tuy n có th du c luu tr trên máy ch TFTP, b d nh tuy n du c c u hình sao cho sau khi kh i d ng s tìm ki m t p tin c u hình trên máy ch TFTP thay vì s d ng t p tin c u hình luu tr trong NVRAM. Có th s d ng l nh copy d t i t p tin c u hình t máy ch TFTP v b d nh tuy n.

- C u hình b d nh tuy n thông qua giao di n WEB: ch th c hi n du c sau khi b d nh tuy n dã du c c u hình v i d a ch IP và cho phép c u hình qua giao th c http.

S d ng giao ti p dòng l nh

Đ th c hi n vi c k t n i máy tính v i b d nh tuy n, ngu i ta dùng cáp console c a Cisco, m t d u c m tr c ti p vào c ng CONSOLE c a b d nh tuy n, d u kia c m vào c ng COM c a máy tính, có th s d ng các d u chuy n d i DB9/RJ45 ho c DB25/RJ45 khi c n thi t.

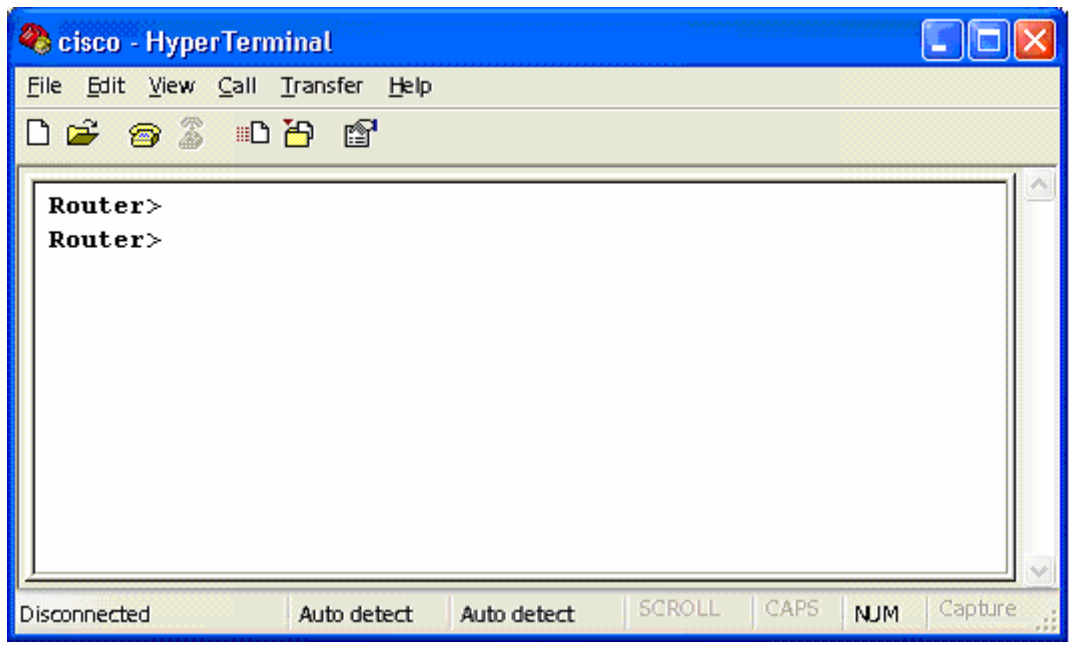
Ph n m m giao ti p gi a máy tính và b d nh tuy n thông d ng nh t là HyperTerminal du c cài d t s n trong các phiên b n WINDOWS.



Hình 3. 19: Xác l p các tham s cho k t n i

Hình 3.18: S d ng HyperTerminal d k t n i d n b d nh tuy n

Ch n dúng c ng COM k t n i v i cáp console d ti n hành cài d t các thông s làm vi c. T c d k t n i thông qua c ng COM c a máy tính và c ng CONSOLE c a b d nh tuy n là 9600b/s (hình 3.19). Ch n OK, b m phím Enter, c a s làm vi c xu t hi n d u l n hon " > " sau tên c a c a b d nh tuy n, nghia là vi c k t n i dã hoàn t t (hình 3-20).



Hình 3.20: K t n i t i b d nh tuy n thành công

Sau khi dã k t n i thành công, s d ng các l nh c a b d nh tuy n d xem, ki m tra, c u hình và b t l i các ho t d ng c a b d nh tuy n.

S d ng d u ? d truy c p thông tin tr giúp

- Đánh d u ? ngay sát sau câu l nh chua hoàn ch nh s hi n th các l nh có th b t d u t các t chua hoàn ch nh dã gõ
- Đánh d u ? sau câu l nh m t ký t tr ng s hi n th các tham s có th c a câu l nh
- Khi câu l nh không có s hi n th m t báo l i

S d ng TAB ngay sát sau câu l nh chua hoàn ch nh s hi n th câu l nh hoàn ch nh

3.2. Làm quen v i các ch d c u hình

Ch d ngu i dùng

Bao g m các tác v ph bi n ch y u g m nh ng l nh ki m tra tr ng thái ho t d ng c a b d nh tuy n, tr ng thái các giao ti p, các b ng d nh tuy n v.v... và m t s l nh d ki m tra k t n i m ng nhu ping, traceroute, telnet v.v.... ch d này không du c phép thay d i các c u hình b d nh tuy n. Ch d ngu i dùng không cho phép xem xét sâu d n các ho t d ng c a b d nh tuy n mà trong quá trình khai thác, v n hành, ngu i qu n tr ph i c n thi t s d ng ch d qu n tr d th c hi n. Bi u hi n c a ch d ngu i dùng là d u l n hon, > , sau tên b d nh tuy n:

```
Router>
Router>?
Exec commands:
  <1-99>          Session number to resume
```

```
access-enable    Create a temporary Access-List entry
access-profile   Apply user-profile to interface
clear            Reset functions
connect          Open a terminal connection
disable          Turn off privileged commands
disconnect       Disconnect an existing network connection
enable           Turn on privileged commands
exit             Exit from the EXEC
             ----- các l nh dã du c b   b t -----
ping             Send echo messages
ppp              Start IETF Point-to-Point Protocol (PPP)
resume           Resume an active network connection
rlogin           Open an rlogin connection
show             Show running system information
slip             Start Serial-line IP (SLIP)
systat           Display information about terminal lines
telnet           Open a telnet connection
terminal         Set terminal line parameters
traceroute       Trace route to destination
tunnel           Open a tunnel connection
udptn            Open an udptn connection
where            List active connections
x28              Become an X.28 PAD
x3               Set X.3 parameters on PAD
```

Ch d qu n tr

Bao g m h u h t các l nh c a ch d ngu i dùng và các l nh ch dành cho ngu i qu n tr . Ch có th c u hình b d nh tuy n ch d này. Trong quá trình khai thác, v n hành, d hi u rõ ho c khi có s c x y ra, ngu i qu n tr có th s d ng các l nh debug d làm rõ thêm thông tin c n thi t. Đ c trung cho ch d qu n tr là bi u hi n c a d u thang, # .

```
Router>en
Password:
Router#
Router#?
Exec commands:
  <1-99>         Session number to resume
  access-enable    Create a temporary Access-List entry
  access-profile   Apply user-profile to interface
  access-template  Create a temporary Access-List entry
  archive          manage archive files
  bfe              For manual emergency modes setting
  cd               Change current directory
```

```
clear          Reset functions
clock          Manage the system clock
configure      Enter configuration mode
connect        Open a terminal connection
copy           Copy from one file to another
debug          Debugging functions (see also 'undebug')
 ----- các l nh dã du c b   b t -----
traceroute     Trace route to destination
tunnel         Open a tunnel connection
udptn          Open an udptn connection
undebug        Disable debugging functions (see also 'debug')
upgrade        Upgrade firmware
verify         Verify a file
where          List active connections
write          Write running configuration to memory, network, or
  terminal
x28            Become an X.28 PAD
x3             Set X.3 parameters on PAD
```

Ch d c u hình toàn c c

Là ch d c u hình các tham s toàn c c cho b d nh tuy n.

Có r t nhi u các c u hình toàn c c nhu c u hình tên b d nh tuy n, c u hình tên và m t kh u ngu i dùng, c u hình d nh tuy n toàn c c, c u hình danh sách truy nh p v.v... Bi u hi n c a ch d c u hình toàn c c nhu sau:

```
Router#
Router#config terminal
Router(config)#hostname RouterA
```

Ch d c u hình giao ti p

Ch d c u hình giao ti p là ch d c u hình cho các giao ti p c a b d nh tuy n nhu giao ti p Serial, giao ti p Ethernet, giao ti p Async...

Ch d c u hình giao ti p cho phép ngu i qu n tr m ng thi t l p các tham s ho t d ng cho m i giao ti p nhu các giao th c m ng du c s d ng trên giao ti p, d a ch m ng c a giao ti p, gán các danh sách truy nh p cho giao ti p v.v... M t ví d v ch d c u hình giao ti p nhu sau:

```
Router#
Router#config terminal
Router(config)#interface s0/0
Router(config-if)#encapsolution ppp
Router(config-if)#ip address 192.168.100.5 255.255.255.0
Router(config-if)#
```

Ch d c u hình d nh tuy n

Là ch d c u hình các tham s cho các giao th c d nh tuy n. Các giao th c d nh tuy n du c c u hình d c l p v i nhau và d u du c th c hi n ch d c u hình d nh tuy n nhu ví d sau:

```
Router#
Router#config terminal
Router(config)#router rip
Router(config-router)#network 192.168.0.0
Router(config-if)#
```

Ch d c u hình du ng k t n i

Ch d c u hình du ng k t n i là m t ch d c u hình d c bi t s d ng d thi t l p các tham s m c th p cho giao ti p logic trong dó di n hình là các tham s thi t l p cho các k t n i modem quay s .

```
Router#config terminal
Router(config)#line 33 48
Router(config-line)#modem inout
Router(config-line)#modem autoconfig discovery
Router(config-line)#
```

B ng 3-7:M t s ch d c u hình và th hi n

Ch d c u hình	Th hi n
Global	Router(config)#
Interface	Router(config-if)#
Subinterface	Router(config-subif)#
Controller	Router(config-controller)#
Map-list	Router(config-map-list)#
Map-class	Router(config-map-class)#
Line	Router(config-line)#
Router	Router(config-router)#
Route-map	Router(config-route-map)#

3.3. Làm quen v i các l nh c u hình co b n

Enable : dùng d vào ch d qu n tr . Sau khi th c hi n l nh enable, ngu i dùng ph i cung c p m t kh u qu n tr dúng d th c s du c làm vi c ch d qu n tr , m t kh u không du c phép nh p sai quá 3 l n.

```
Router>
Router>en
Password:
Password:
Password:
% Bad secrets
Router>en
Password:
Router#
Router#
Router#disa
Router>
```

Disable : thoát kh i ch d qu n tr v ch d ngu i dùng.

Setup : th c hi n kh i t o l i c u hình c a b d nh tuy n ch d c u hình h i tho i. Sau dây là m t ví d v s d ng l nh setup. Ch d h i tho i này cung du c th c hi n t d ng d i v i các b d nh tuy n chua h có t p tin c u hình hay nói cách khác có NVRAM không ch a thông tin.

```
Router#setup
        --- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: y
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system
Would you like to enter basic management setup? [yes/no]: n
First, would you like to see the current interface summary? [yes]: n
Configuring global parameters:
  Enter host name [Router]:
  The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
Enter enable secret [<Use current secret>]:
The enable password is used when you do not specify an
enable secret password, with some older software versions, and
some boot images.
Enter enable password []:123456
```

```
  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: 654321
  Configure SNMP Network Management? [yes]:
    Community string [public]:
  Configure IP? [yes]:
    Configure IGRP routing? [yes]: n
    Configure RIP routing? [no]:
  Configure bridging? [no]:
Async lines accept incoming modems calls. If you will have
users dialing in via modems, configure these lines.
  Configure Async lines? [yes]: n
Configuring interface parameters:
Do you want to configure FastEthernet0/0  interface? [yes]: n
Do you want to configure Serial0/0  interface? [yes]: n
Do you want to configure Serial0/1  interface? [no]: y
  Some supported encapsulations are
       ppp/hdlc/frame-relay/lapb/x25/atm-dxi/smds
  Choose encapsulation type [hdlc]: ppp
  No serial cable seen.
  Choose mode from (dce/dte)  [dte]:
  Configure IP on this interface? [no]: y
    IP address for this interface: 192.168.100.5
    Subnet mask for this interface [255.255.255.0] :
    Class C network is 192.168.100.0, 24 subnet bits; mask is /24
The following configuration command script was created:
hostname Router
enable secret 5 $1$EuXV$Yhj/OYkz/U1R5VABqXsMC0
enable password 7 123456
line vty 0 4
password 7 654321
snmp-server community public
!
ip routing
no bridge 1
!
interface FastEthernet0/0
shutdown
no ip address
!
interface Serial0/0
shutdown
no ip address
```

```
!
interface Serial0/1
no shutdown
encapsulation ppp
ip address 192.168.100.5 255.255.255.0
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
end
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.
```

Config : cho phép th c hi n các l nh c u hình b d nh tuy n. Sau lênh config, qu n tr m ng m i có th th c hi n các l nh c u hình b d nh tuy n. Trình t th c hi n c u hình cho m t b d nh tuy n có th du c th hi n nhu sau

- Đ t tên cho b d nh tuy n

```
Router#config terminal
Router(config)#
Router(config)#hostname RouterABC
RouterABC(config)#
```

- Đ t tên m t kh u bí m t dành cho ngu i qu n tr

```
RouterABC(config)#enable secret matkhaubimat
RouterABC(config)#
```

- Đ t tên m t kh u cho ch d qu n tr . M t kh u này ch s d ng khi c u hình b d nh tuy n không có m t kh u bí m t dành cho qu n tr .

```
RouterABC(config)#enable password matkhau
RouterABC(config)#
```

- C u hình cho phép ngu i dùng truy c p t xa d n b d nh tuy n

```
RouterABC(config)#line vty 0 4
RouterABC(config-line)#login
RouterABC(config-line)#password telnet
RouterABC(config-line)#
```

- C u hình các giao ti p

```
RouterABC(config)#interface ethernet 0
RouterABC(config-if)#ip address 192.168.2.1 255.255.255.0
RouterABC(config-if)#no shutdown
RouterABC(config-if)#
```

- C u hình d nh tuy n

```
RouterABC(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.2
RouterABC(config)#
```

Copy : l nh copy cho phép th c hi n các sao chép c u hình c a b d nh tuy n di/d n máy ch TFTP **,** sao chép, lu u tr , nâng c p các t p tin IOS c a b d nh tuy n t / t i máy ch TFTP.

Đ có th lu u b n sao c u hình hi n hành lên máy ch TFTP, s d ng l nh *copy rumng-config tftp* nhu du c trình bày du i. Ti p theo là ti n trình ngu c l i v i vi c t i t p tin c u hình t máy ch TFTP v b d nh tuy n.

- Nh p l nh *copy runing-config tftp*
- Nh p d a ch IP c a máy ch TFTP noi dùng d lu u t p tin c u hình
- Nh p tên n d nh cho t p tin c u hình
- Xác nh n ch n l a v i tr l i yes

L nh copy dùng d luu t p tin c u hình lên máy ch :

```
Router#copy running-config tftp
Address or name of remote host []? 192.168.1.5
Name of configuration file to write [Router-config]?cisco.cfg
Write file cisco.cfg to 192.168.1.5? [confirm] y
Writing cisco.cfg !!!!! [OK]
Router#
```

L nh copy dùng d t i t p tin c u hình t máy ch :

```
Router#copy tftp running-config
Address or name of remote host []? 192.168.1.5
Source filename []? cisco.cfg
Destination filename [running-config]?
```

Show : là l nh du c dùng nhi u và ph bi n nh t.
L nh show dùng d xác d nh tr ng thái hi n hành c a b d nh tuy n. Các l nh này giúp cho phép có du c các thông tin quan tr ng c n bi t khi ki m tra và di u ch nh các ho t d ng c a b d nh tuy n.

- show version: hi n th c u hình ph n c ng h th ng, phiên b n ph n m m, tên và ngu n c a các t p tin c u hình, và nh chuong trình kh i d ng.
- show processes: hi n th thông tin các quá trình ho t d ng c a b d nh tuy n.
- show protocols: hi n th các giao th c du c c u hình.
- show memory: th ng kê v b nh c a b d nh tuy n.
- show stacks: giám sát vi c s d ng stack c a các quá trình, các th t c ng t và hi n th nguyên nhân kh i d ng l i h th ng l n cu i cùng.
- show buffers: cung c p th ng kê v các vùng b d m trên b d nh tuy n.

- show flash: th hi n thông tin v b nh Flash.
- show running-config: hi n th t p tin c u hình dang ho t d ng c a b d nh tuy n.
- show startup-config: hi n th t p tin c u hình du c luu tr trên NVRAM và du c dua vào b nh d ho t d ng khi b t ngu n b d nh tuy n. Thông thu ng running-config và startup-config là gi ng nhau. Khi th c hi n các l nh c u hình, running-config và startup-config s không còn gi ng nhau, c u hình ho t d ng (running-config) c n ph i du c ghi tr l i NVRAM sau khi k t thúc c u hình b d nh tuy n.
- show interfaces: th ng kê các giao ti p c a b d nh tuy n. Đây là m t trong các l nh du c s d ng nhi u nh t cho bi t tr ng thái ho t d ng c a các giao ti p, s li u th ng kê luu lu ng, s lu ng các gói tin l i v.v...

```
Router#sh run
Building configuration...
!
Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
interface Ethernet0
 no ip address
 no ip directed-broadcast
 shutdown
```

```
Router#sh startup-config
Current configuration : 677 bytes
!
Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
interface Ethernet0
 no ip address
 no ip directed-broadcast
```

Hình 3.21: L nh show

```
Router#show interface s0/0
Serial0/0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Description: 2M link to the Internet
  Internet address is 192.168.100.5/24
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec,
     reliability 255/255, txload 248/255, rxload 84/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/12/0 (size/max/drops/flushes); Total output
drops: 2383688
  Queueing strategy: weighted fair
  Output queue: 24/1000/64/2383671 (size/max total/threshold/drops)
     Conversations  5/184/256 (active/max active/max total)
```

```
    Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 677000 bits/sec, 161 packets/sec
  5 minute output rate 1996000 bits/sec, 395 packets/sec
    106754998 packets input, 2930909441 bytes, 0 no buffer
    Received 68850 broadcasts, 0 runts, 0 giants, 0 throttles
    51143 input errors, 30726 CRC, 20248 frame, 0 overrun, 0
ignored, 169 abort
    319791176 packets output, 1669977392 bytes, 0 underruns
    0 output errors, 0 collisions, 125 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
    DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Hình 3.22: L nh show interface

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.1(2), RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Tue 09-May-00 23:34 by linda
Image text-base: 0x80008088, data-base: 0x807D2544

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)

Router uptime is 1 week, 1 day, 1 minute
System returned to ROM by power-on at 13:29:57 Hanoi Thu Jul 31 2003
System restarted at 20:24:22 Hanoi Tue Sep 2 2003
System image file is "flash:c2600-i-mz.121-2.bin"

cisco 2620 (MPC860) processor (revision 0x102) with 26624K/6144K
bytes of memory
.
Processor board ID JAD04340ID8 (2733840160)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
1 FastEthernet/IEEE 802.3 interface(s)
2 Serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102
```

Hình 3.23: L nh show version

Write : l nh write s d ng d ghi l i c u hình hi n dang ch y c a b d nh tuy n. Nh t thi t ph i dùng l nh *write memory* d ghi l i c u hình c a b d nh tuy n vào NVRAM m i khi có thay d i v c u hình.

```
Router#write ?
 erase     Erase NV memory
 memory    Write to NV memory
 network   Write to network TFTP server
 terminal  Write to terminal
 <cr>
```

3.4. Cách kh c ph c m t s l i thu ng g p

L i k t n i d n c ng console s d ng Hyper Terminal

- Ki m tra l i xem dã s d ng chính xác lo i cáp dùng d c u hình b d nh tuy n chua. Cáp console dùng d c u hình b d nh tuy n là cáp 8 s i có hai d u RJ45 có so d d u n i nhu b ng 3-8 và s d ng d u chuy n d i DB9/RJ45 du c cung c p kèm theo b d nh tuy n.
- Ki m tra xem dã s d ng dúng c ng k t n i COM c a máy tính d n i t i b d nh tuy n.

B ng 3-8: So d d u n i cáp console

Console	**Cáp console DB9/RJ45**		**COM**
Tín hi u	**RJ45**	**DB9**	**Tín hi u**
RTS	1	8	CTS
DTR	2	7	DSR
TxD	3	6	RxD
GND	4	5	GND
GND	5	4	GND
RxD	6	3	TxD
DSR	7	2	DTR
CTS	8	1	RTS

- Ki m tra các tham s k t n i. T c d k t n i ph i là 9600 cho k t n i qua c ng console.

L i k t n i s d ng telnet

Khi s d ng telnet d c u hình t xa b d nh tuy n, ngu i dùng có th không k t n i du c d n b d nh tuy n. M t trong các l i sau c n du c ki m tra:

- Máy tính dùng d c u hình b d nh tuy n không có k t n i m ng v i b d nh tuy n. Ki m tr a l i kh nang k t n i m ng t máy tính d n b d nh tuy n. Có th dùng l nh *ping* d ki m tra.
- Khi c u hình b d nh tuy n l n d u, ngu i qu n tr m ng dã quên không thi t l p m t kh u cho truy nh p t xa. Khi c g ng truy nh p t xa, ngu i dùng s nh n du c thông báo v vi c m t kh u truy nh p chua du c thi t l p. Tru ng h p này c n s d ng cáp console d thi t l p m t kh u theo trình t nhu trình bày du i dây:

```
Router#config terminal
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password 123456
Router(config-line)#end
Router#write memory
```

- Ki m tra v vi c có hay không có các h n ch telnet s d ng các danh sách ki m soát truy nh p (access-list).

4. C u hình b d nh tuy n Cisco

4.1. C u hình leased-line

Gi i thi u leased-line

Leased-line, hay còn du c g i là kênh thuê riêng, là m t hình th c k t n i tr c ti p gi a các node m ng s d ng kênh truy n d n s li u thuê riêng.

Kênh truy n d n s li u thuê riêng thông thu ng cung c p cho ngu i s d ng s l a ch n trong su t v giao th c d u n i hay nói cách khác, có th s d ng các giao th c khác nhau trên kênh thuê riêng nhu PPP, HDLC, LAPB v.v...

V m t hình th c, kênh thuê riêng có th là các du ng cáp d ng tr c ti p k t n i gi a hai di m ho c có th bao g m các tuy n cáp d ng và các m ng truy n d n khác nhau. Khi kênh thuê riêng ph i di qua các m ng truy n d n khác nhau, các quy d nh v giao ti p v i m ng truy n d n s du c quy d nh b i nhà cung c p d ch v . Do dó, các thi t b d u cu i CSU/DSU c n thi t d k t n i kênh thuê riêng s ph thu c và nhà cung c p d ch v . M t s các chu n k t n i chính du c s d ng là HDSL, G703, 2B1Q v.v...

Khi s d ng kênh thuê riêng, ngu i s d ng c n thi t ph i có d các giao ti p trên các b d nh tuy n sao cho có m t giao ti p k t n i WAN cho m i m t k t n i kênh thuê riêng t i m i node. Đi u dó có nghia là, t i di m node có k t n i kênh thuê riêng d n 10 di m khác nh t thi t ph i có d 10 giao ti p WAN d ph c v cho các k t n i kênh thuê riêng. Đây là m t v n d h n ch v d u tu thi t b ban d u, không linh ho t trong m r ng, phát tri n, ph c t p

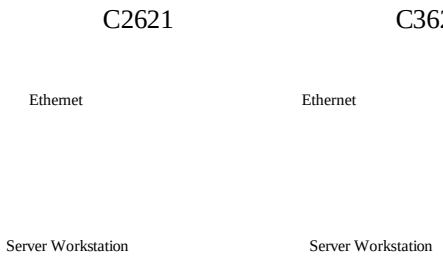
trong qu n lý, d c bi t là chi phí thuê kênh l n d i v i các yêu c u k t n i xa v kho ng cách d a lý.

Các giao th c s d ng v i du ng lease-line

Hai giao th c s d ng v i leased-line là HDLC, PPP và LAPB. Trong dó:

- HDLC: là giao th c du c s d ng v i h các b d nh tuy n Cisco hay nói cách khác ch có th s d ng HDLC khi c hai phía c a k t n i leased-line d u là b d nh tuy n Cisco.
- PPP: là giao th c chu n qu c t , tuong thích v i t t c các b d nh tuy n c a các hãng s n xu t khác nhau. Khi d u n i kênh leased-line gi a m t phía là thi t b c a Cisco và m t phía là thi t b c a hãng th 3 thì nh t thi t ph i dùng giao th c d u n i này. PPP là giao th c l p 2 cho phép nhi u giao th c m ng khác nhau có th ch y trên nó do v y nó du c s d ng ph bi n.
- LAPB: là giao th c truy n thông l p hai tuong t nhu giao th c m ng X.25 v i d y d các th t c, quá trình ki m soát truy n d n, phát hi n và s a l i. LAPB ít du c s d ng.

Mô hình k t n i lease-line



C u hình k t n i lease-line co b n

- Phân d nh d a ch
  - o Vi c phân d nh d a ch cho các m ng và cho các k t n i gi a các b d nh tuy n là r t quan tr ng, d m b o cho vi c liên l c thông su t gi a các m ng, d m b o cho v n d qui ho ch d a ch , nhóm g n các d nh tuy n ...
  - o Khi th c hi n xây d ng m t m ng dùng riêng, di u c n thi t ph i ghi nh là ch du c dùng các d a ch trong nhóm các d a ch dành cho m ng dùng riêng:10.x.x.x, 172.16.x.x – 172.31.x.x, 192.168.x.x
  - o Đ d m b o không b trùng l p và gi m thi u các v n d phát sinh, các k t n i m ng WAN theo ki u leased-line c n du c s p x p trên l p m ng nh nh t. Các k t n i m ng WAN trong tru ng h p này du c th c hi n trên các l p m ng g m 4 d a ch .

o Các l p m ng khác tu theo yêu c u c th và s lu ng các d a ch có th mà phân chia cho phù h p.

- Đ b t d u c u hình m ng:
  - o **Router> enable**
  - o **Password: ******
  - o **Router# config terminale**
  - o **Router(config)#**
- Th c hi n d t tên, các m t kh u, c u hình cho phép telnet và các di u ki n c n thi t tru c khi c u hình các giao di n
- C u hình
  - o **Router2621(config)# interface serial 0**
- L a ch n giao th c s d ng
  - o **Router2621(config-if)# encapsolation HDLC**
- Đ t d a ch IP cho giao ti p k t n i leased-line
  - o **Router2621(config-if)# ip address 192.168.113.5 255.255.255.252**
- Luôn ph i dua giao ti p vào s d ng b ng l nh no shutdown
  - o **Router2621(config-if)# no shutdown**
  - o **Router2621(config-if)# interface serial 1**
- L a ch n giao th c PPP s d ng cho m t giao ti p khác
  - o **Router2621(config-if)# encapsolation PPP**
  - o **Router2621(config-if)# ip address 192.168.113.9 255.255.255.252**
  - o **Router2621(config-if)# no shutdown**
  - o **Router2621(config-if)# exit**
- S d ng d nh tuy n tinh v i cú pháp: ip route [d a ch m ng dích] [netmask] [d a ch next hop]
  - o **Router2621(config)# ip route 0.0.0.0 0.0.0.0 192.168.113.6**
- Luôn ph i ghi l i c u hình khi dã c u hình xong
  - o **Router2621# write memory**
- Th c hi n các ph n vi c còn l i t i các b d nh tuy n khác, chú ý v giao th c du c s d ng ki m tra, giám sát các k t n i.
  - o Dùng l nh d ki m tra tr ng thái c a giao ti p **show interface**
  - o : xem tr ng thái t t c các giao ti p **show interface**
  - o : xem tr ng thái c ng serial 0 **show interface serial 0**
  - o *Serial 0 is admininistrative down line protocole is down* : th hi n tr ng thái dang b c u hình là không làm vi c, s d ng l nh no shutdown trong Interface mode d du a giao ti p serial 0 vào làm vi c
  - o *Serial 0 is down line protocole is down* : ki m tra l i du ng truy n

- *Serial 0 is up line protocole is down* : ki m tra l i các giao th c du c s d ng t i hai phía
- *Serial 0 is up line protocole is up* : là tr ng thái làm vi c

C u hình b d nh tuy n 2621

```
!
hostname 2621
!
!
interface FastEthernet0/0
 ip address 10.0.5.1 255.255.255.0
!
!
interface Serial0/0
 ip address 192.168.113.5 255.255.255.252
 encapsulation ppp
!
!
ip route 0.0.0.0 0.0.0.0 192.168.113.6
!
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Hình 3.24: C u hình c a b d nh tuy n 2621

C u hình b d nh tuy n 3620

```
!
hostname 3620
!
!
interface FastEthernet0/0
 ip address 10.0.6.1 255.255.255.0
!
!
interface Serial1/0
```

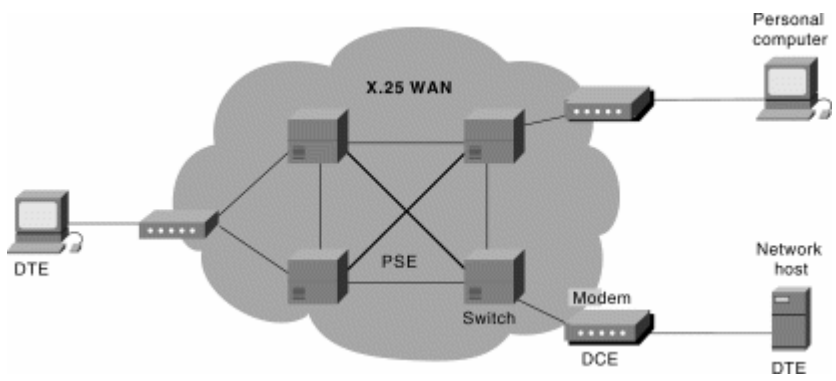
```
 ip address 192.168.113.6 255.255.255.252
 encapsulation ppp
!
!
ip route 0.0.0.0 0.0.0.0 192.168.113.5
!
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Hình 3.25: C u hình c a b d nh tuy n 3620

4.2. C u hình X.25 & Frame Relay

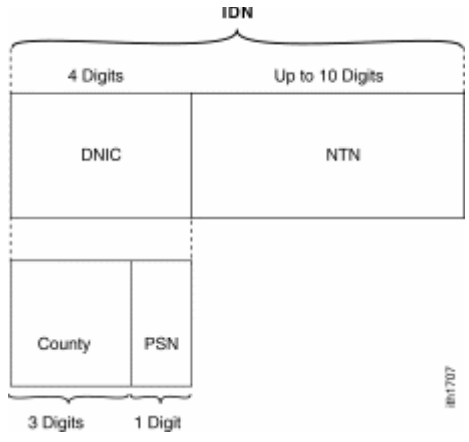
Gi i thi u X.25 và Frame Relay

X25 : Nam 1978 ISO thay d i thêm HDLC và CCITT thêm m t s thông s d sinh ra LAPB "Link Access Procedure – Balanced Mode". LAPB d nh nghia m t s quy lu t cho m c Frame c a X.25 nhu các lo i khung d c bi t nhu RR (Receive Ready), REJ (Reject) . . .



Hình 3.26: Chuy n m ch gói X.25

X.25 cung c p các k t n i di n r ng thông qua môi tru ng chuy n m ch gói. M i thuê bao X.25 có m t d a ch xác d nh duy nh t du c dánh s g m các ph n mã qu c gia, nhà cung c p d ch v và d a ch c a thuê bao tr c thu c nhà cung c p d ch v .



Hình 3.27: C u trúc d a ch X.25

Khi có nhu c u k t n i truy n d li u, các thi t b d u cu i X.25 s phát kh i t o m t VC (virtual circuit) t i d a ch dích. Sau khi VC du c thi t l p, d li u s du c truy n t i gi a hai di m thông qua VC dó. N u nhu c u d li u l n hon, thi t b d u cu i s kh i t o thêm các VC m i. Khi h t gi li u, các VC s du c gi i phóng cho các nhu c u truy n t i khác.

X.25 qui d nh m t s tham s xác d nh bao g m:

- Đ l n gói tin (ips/ops): là giá tr kích thu c gói tin du c quy d nh b i nhà cung c p d ch v .
- Đ l n c a s di u khi n lu ng (win/wout): X.25 s d ng co ch di u khi n lu ng b ng c a s d d m b o t c d g i nh n tin phù h p không làm m t mát thông tin. V i tham s c a s b ng 7, X.25 cho phép g i t i da 7 gói tin khi chua nh n du c phúc dáp.
- S lu ng kênh VC t i da cho chi u d n/hai chi u/chi u di (hic/htc/hoc): S lu ng kênh VC du c cung c p cho m i thuê bao X.25 dã du c xác d nh b i nhà cung c p. Thuê bao ch có th truy n t i d li u v i s lu ng các VC t i da cho phép dã du c xác d nh. Không th th c hi n du c yêu c u truy n t i n u có yêu c u truy n t i t i các di m m i khi s lu ng VC dã h t. Khi các thi t b d u cu i X.25 th c hi n truy n t i d li u nó ph i tuân theo các quy t c:
    - o Cu c g i ra du c th c hi n t VC l n nh t còn tr ng. Đi u dó có nghia là, n u chu a h có cu c g i nào và s VC du c cung c p cho m t thuê bao là 16 thì cu c g i ra d u tiên s kh i t o VC s 16 d th c hi n yêu c u k t n i.Trong tru ng h p dã dùng h t 3 VC g i ra thì cu c g i ra th 4 s s d ng VC s 13 d th c hi n.
    - o Cu c g i t i du c th c hi n t VC nh nh t còn tr ng. Tuong t nhu cu c g i ra, cu c g i vào d u tiên s nh n du c trên VC s 1 và cu c g i vào th 10 s nh n du c trên VC s 10.
    - o Quá trình kh i t o VC s d ng l i khi không còn VC tr ng.
    - o V i các quy t c này, yêu c u c n thi t ph i xác l p m t cách chính xác các tham s cho thi t b d u cu i X.25 thì m i có th th c hi n du c các k t n i truy n t i d li u.

V d c di m c a X.25

- T c d truy n t i h n ch , t i Vi t Nam t c d cung c p t i da là 128Kbps.
- Đ tr l n, không phù h p cho các ng d ng có yêu c u cao v d tr .
- Kh nang m r ng d dàng, chi phí không cao.
- An toàn và b o m t, v n du c s d ng trong các giao d ch ngân hàng.

Frame Relay : Frame Relay ra d i trên n n t ng h t ng vi n thông ngày càng du c c i thi n, không c n có quá nhi u các th t c phát hi n và s a l i nhu X.25. Frame relay có th chuy n nh n các khung l n t i 4096 byte trong khi dó gói tiêu chu n c a X.25 khuy n cáo dùng là 128 byte. Frame Relay r t thích h p cho try n s li u t c d cao và cho k t n i LAN to LAN và c cho âm thanh, nhung di u ki n tiên quy t d s d ng công ngh Frame relay là ch t lu ng m ng truy n d n ph i cao.

B ng 3-9:So sánh gi a X.25 và Frame Relay

TT	Ch c nang c a m ng X25	Frame relay
1	Phúc dáp khung thông tin nh n du c	v
2	Phúc dáp gói tin nh n du c	v
3	D ch d a ch c a gói tin	v v
4	C t gi gói tin vào vùng d m d ch phúc dáp	v
5	Phát hi n gói tin sai th t	v
6	Hu gói tin b l i	v v
7	Đ m b o khung tin có giá tr N(s) là h p l	v
8	Thi t l p và hu b k t n i logical	v
9	Thi t l p và hu b kênh o	v
10	Đ i n các bit c vào gi a các khung	v
11	Đ i u khi n lu ng d li u l p liên k t logic	v
12	T o và ki m tra FCS	v v
13	T o và nh n d ng bit c	v v
14	T o ra khung báo chua s n sàng	v
15	T o ra khung báo dã s n sàng	v

v16 T o ra khung báo khung b t ch i v
17 Qu n lý các bit D, M, Q trong gói tin v
18 Qu n lý các khung m c liên k t d li u v
19 Qu n lý các b d nh th i m c 3 v
20 Qu n lý các bit Poll/Final trong khung v
21 Qu n lý các b d m s th t c a khung và v
gói tin
22 Ghép các kênh logic v
23 Qu n lý các th t c kh i d ng m c 2 và 3 v
24 Nh n d ng các khung không h p l v v
25 Tr l i các khung và gói tin báo chua s n v
sang
26 Tr l i các khung và gói tin báo dã s n sàng v
27 Tr l i các khung và gói tin báo t ch i v
khung
28 Đ ánh d u s l n ph i truy n l i v
29 Chèn thêm và b các bit 0 vào s li u v v
B ng ch c nang trên cho th y Frame relay dã gi m r t nhi u các công vi c không c n thi t cho thi t b chuy n m ch do dó gi m gánh n ng cung nhu th i gian x lý công vi c cho các nút m ng, nh v y mà làm gi m th i gian tr cho các khung thông tin khi truy n trên m ng.

Hình 3.28: Mô hình m ng Frame Relay

Co s d t o du c m ng Frame relay là các thi t b truy nh p m ng FRAD (Frame Relay Access Device), các thi t b m ng FRND (Frame Relay
Network Device), du ng n i gi a các thi t b và m ng tr c Frame Relay. Thi t b FRAD có th là các LAN bridge, LAN Router v.v...

Thi t b FRND có th là các T ng dài chuy n m ch khung (Frame) hay t ng dài chuy n m ch t bào (Cell Relay - chuy n t i t ng h p các t bào c a các d ch v khác nhau nhu âm thanh, truy n s li u, video v.v..., m i t bào d dài 53 byte, dây là phuong th c c a công ngh ATM). Đu ng k t n i gi a các thi t b là giao di n chung cho FRAD và FRND, giao th c ngu i dùng và m ng hay g i F.R UNI (Frame Relay User Network Interface). M ng tr c Frame Relay cung tuong t nhu các m ng vi n thông khác có nhi u t ng dài k t n i v i nhau trên m ng truy n d n, theo th t c riêng c a mình.

Công ngh Frame Relay có m t uu di m d c trung r t l n là cho phép ngu i s d ng dùng t c d cao hon m c h dang ký trong m t kho ng th i gian nh t d nh, có nghia là Frame Relay không c d nh d r ng bang cho t ng cu c g i m t mà phân ph i bang thông m t cách linh ho t di u mà X.25 và thuê kênh riêng không có. Ví d ngu i s d ng h p d ng s d ng v i t c d 64Kbps, khi h chuy n di m t lu ng thông tin quá l n, Frame Relay cho phép truy n chúng t c d cao hon 64Kbps. Hi n tu ng này du c g i là bùng n Bursting.

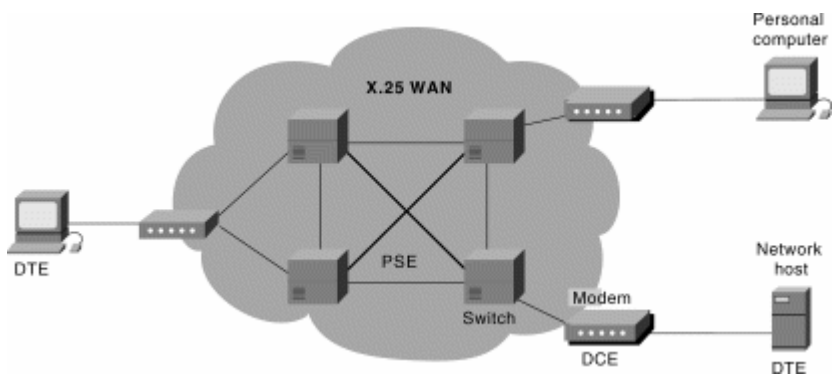
Các d c di m c a Frame Relay:

- Cung c p các k t n i thông qua các kênh o c d nh PVC. Khi có nhu c u k t n i gi a 2 di m, nhà cung c p d ch v s thi t l p các thông s trên các node Frame Relay t o ra các kênh o c d nh gi a 2 di m. Không nhu X.25, hu ng k t n i Frame Relay là c d nh và không th kh i t o b i ngu i dùng. Khi có nhu c u k t n i d n di m dích khác, khách hàng ph i thuê m i PVC d n di m dích m i dó.
- CIR (Committed Information Rate): là t c d truy n d li u mà nhà cung c p d ch v cam k t s d m b o cho khách hàng, di u dó có nghia là khách hàng s du c d m b o cung c p du ng truy n v i dúng t c d yêu c u. CIR du c g n li n v i v i các PVC và d c l p gi a các PVC khác nhau. N u t c ngh n x y ra thì khách hàng v n truy n du c v i t c d yêu c u khi ký k t h p d ng.
- Frame Relay h tr truy n s li u khi có bùng n s li u hay còn g i là "bursty", có nghia là lu ng thông tin du c g i di trong th i gian ng n và v i dung lu ng l n hon dung lu ng bình thu ng. Nói cách khác, khi có m t nhu c u truy n t i kh i lu ng d li u l n, m ng Frame Relay cho phép du c th c hi n truy n t i d li u v i t c d l n hon t c d CIR dã mua c a nhà cung c p d ch v . Đ i u này d m b o cho khách hàng ti t ki m du c chi phí mà v n d m b o truy n d li u v i kh i lu ng l n trong nh ng di u ki n c n thi t d m b o luu thông thông tin. Truy n d li u bursty ch th c hi n du c khi không có t c ngh n trên m ng.
- Frame Relay không s d ng d a ch d nh danh nhu X.25. Đ phân bi t các PVC, Frame Relay s d ng DLCI, m i m t PVC du c g n li n v i m t DLCI. DLCI ch có tính ch t c c b có nghia là ch có ý nghia qu n lý trên cùng m t chuy n m ch. Nói cách khác s DLCI ch c n là duy nh t cho m i PVC trên m t chuy n m ch còn có th có cùng s DLCI dó trên m t chuy n m ch khác.

- Frame Relay s d ng giao th c LMI (Local Manegment Interface) là giao th c qu n lý và trao d i thông tin qu n tr gi a các thi t b m ng FRND và các thi t b k t n i FRAD.
- Cung nhu X.25, Frame Relay là môi tru ng m ng da truy nh p không qu ng bá (multiaccess nonbroadcast media). V n d này c n du c chú ý khi s d ng v i các giao th c d nh tuy n.

Các mô hình k t n i c a X.25 và Frame Relay

Khi s d ng phuong th c truy n thông X.25, mô hình k t n i co b n là di m-da di m (point-to-multipoint) d a trên tính ch t co b n c a X.25 là s d ng các VC cho các nhu c u truy n t i d li u.



Hình 3.29: Mô hình k t n i X.25

Frame Relay da d ng hon v các mô hình k t n i. Frame Relay s d ng các PVC d nh tru c d th c hi n truy n t i d li u gi a hai di m, ngu i ta chia Frame Relay thành các c u hình k t n i m ng. Trong dó:

- Full mesh: là mô hình k t n i mà trong dó b t c hai node m ng nào cung có m t PVC liên k t gi a chúng. Mô hình này d m b o tính s n sàng cho toàn b h th ng m ng, n u có m t ho c m t vài PVC có s c , các PVC còn l i v n có th d m b o cho k t n i m ng gi a các node m ng. Y u di m c a mô hình m ng này là chi phí thuê các PVC quá l n.

FRAME RELAYFRAME RELAY FRAME RELAY

FULL MESH HUB-SPOKE FULL MESH

Hình 3.30: Mô hình k t n i Frame Relay

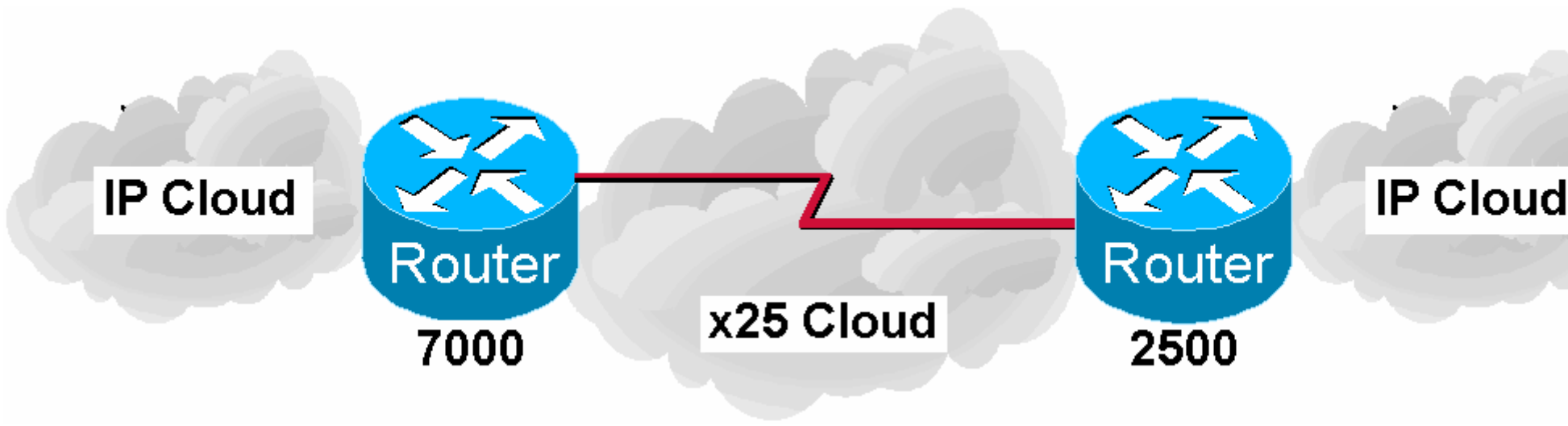
- Hub-Spoke: là mô hình có m t di m t p trung m i k t n i Frame Relay t i các di m khác, các trao d i d li u gi a 2 di m b t k d u ph i di qua di m t p trung. Mô hình này có chi phí gi m thi u nh t nhung có y u di m v vi c t p trung m i gánh n ng lên di m t p trung và n u có b t k s c trên m t PVC nào thì s m t kh nang truy n t i d li u v i di m thu c v PVC b s c dó.

- Partial mesh: là mô hình du c s d ng nhi u nh t, nó là s lai ghép gi a hai mô hình trên, d m b o chi phí và d phòng cho các di m thi t y u.

C u hình X.25 co b n

Các luu ý trong c u hình X.25

- X.25 là m t môi tru ng da truy nh p không broadcast (multi access non broadcast media) do dó ph i luu ý khi s d ng v i d nh tuy n d ng
- X.25 làm vi c v i s kh i t o các VC do dó khi th c hi n c u hình ph i th c hi n các th t c liên k t (map) và d nh tuy n theo d a ch
- Các tham s c n luu ý
  - o Đ l n gói tin (ips/ops)
  - o Đ l n c a s di u khi n lu ng (win/wout)
  - o S lu ng kênh VC t i da cho chi u d n / hai chi u / chi u di (hic/htc/hoc)
  - o S lu ng VC dành cho m t k t n i (nvc). Nên h n ch s lu ng VC cho phép k t n i d n m t di m trong gi i h n h p lý d t ng s VC c n thi t không vu t quá s VC t i da hi n có (HTC)
  - o Khi th c hi n các liên k t (map) ph i th c hi n map d a ch IP c a phía d i phuong t i d a ch X25 c a h
  - o Khi th c hi n d nh tuy n, ph i th c hi n d nh tuy n v i d a ch IP next hop
  - o C u hình m ng d u n i X25 là c u hình da di m, d a ch d u n i ph i n m trong l p m ng con d cho s lu ng các di m



:

Mô hình k t n i X.25 co b n

```
C u hình b   d  nh tuy n 7000
!
interface Serial1/1
 ip address 10.1.1.2 255.255.255.0
 encapsulation x25
 no ip mroute-cache
```

```
!--- Đ a ch  X.121 c a gán cho b  d nh tuy n 7000
 x25 address 4522973407000
!--- Các dòng l nh du i là các tham s  X.25
 x25 ips 256
 x25 ops 256
 x25 htc 16
 x25 win 7
 x25 wout 7
!--- Dòng l nh này dùng d  gán d a ch  IP c a b  d nh tuy n 2500 v i
!d a ch  X.121 c  a nó
 x25 map ip 10.1.1.1 4522973402500
!
!
```

Hình 3.32: C u hình c a b d nh tuy n 7000

```
C u hình b   d  nh tuy n 2500
!
hostname 2500
!
interface Serial0
 ip address 10.1.1.1 255.255.255.0
 no ip mroute-cache
 encapsulation x25
 bandwidth 56
!--- Đ a ch  X.121 c a gán cho b  d nh tuy n 7000
 x25 address 4522973402500
!--- Các dòng l nh du i là các tham s  X.25
 x25 ips 256
 x25 ops 256
 x25 htc 16
 x25 win 7
 x25 wout 7
!--- Dòng l nh này dùng d  gán d a ch  IP c a b  d nh tuy n 7000 v i
!d a ch  X.121 c  a nó
 x25 map ip 10.1.1.1 4522973407000!
```

Hình 3.33: C u hình c a b d nh tuy n 2500

- Giám sát:
  - o dùng d ki m tra tr ng thái
    Show interfaces serial 0:
    hi n th thông tin k t n i X.25
  - o **Show x25 vc:**
  - o hi n th các liên k t hi n có c a FR
    Show x25 map:

C u hình Frame Relay co b n

Các luu ý trong c u hình Frame Relay:

- Frame Relay là m t môi tru ng da truy nh p không broadcast (multi access non broadcast media) do dó ph i luu ý khi s d ng v i d nh tuy n d ng
- Khi s d ng d nh tuy n d ng giao th c d nh tuy n vector nhu RIP, IGRP ph i d ý d n lu t Split Horizon. Lu t Split Horizon là lu t không cho phép các thông tin d nh tuy n v a di vào m t giao ti p di tr ra chính giao ti p dó d tránh vi c c p nh t sai các thông tin v d nh tuy n d n d n vi c vòng di vòng l i c a các thông tin d nh tuy n. V n d này du c d t ra do có nhi u PVC cùng ch y trên m t giao ti p v t lý.
- Giám sát:
  - dùng d ki m tra DLCI, LMI

    Show interfaces serial 0:

    hi n th thông tin t ng h p v LMI
  - **Show frame-relay lmi:**
  - hi n th các liên k t hi n có c a FR

    Show frame-relay map:

    hi n th các thông s c a PVC
  - **Show frame-relay pvc:**

hi n th traffic o **Show frame-relay traffic:**

Hình 3.34: Mô hình k t n i Frame Relay co b n

- Đ b t d u c u hình m ng:
  - **Router> enable**
  - **Password: ******
  - **Router# config terminale**
  - **Router(config)#**
- Th c hi n d t tên, các m t kh u, c u hình cho phép telnet và các di u ki n c n thi t tru c khi c u hình các giao di n
- C u hình
  - **Spicey(config)# interface serial 0**
- L a ch n giao th c s d ng
  - **Spicey(config-if)# encapsolation frame-relay**
- Xác d nh giao th c qu n tr LMI. Giao th c qu n tr LMI nh t thi t ph i có d d m b o vi c trao d i thông tin hai chi u gi a thi t b d u cu i và thi t b m ng Frame Relay. LMI ho t d ng nhu m t thông báo keepalive.

- **Spicey(config-if)# frame-relay lmi-type cisco**

- Gán DLCI du c c p cho giao ti p.
  - **Spicey(config-if)# frame-relay interface-dlci 140**
- Đ t d a ch IP cho giao ti p k t n i leased-line
  - **Spicey(config-if)# ip address 3.1.3.1 255.255.255.0**
- Luôn ph i dua giao ti p vào s d ng b ng l nh no shutdown
  - **Spicey(config-if)# no shutdown**
  - **Spicey(config-if)# exit**
- S d ng d nh tuy n d ng RIP
  - **Spicey(config)# router rip**
  - **Spicey(config-router)# network 3.0.0.0**
  - **Spicey(config-router)# network 124.0.0.0**
  - **Spicey(config-router)# end**
- Luôn ph i ghi l i c u hình khi dã c u hình xong
  - **Spicey# write memory**
- Th c hi n các ph n vi c còn l i t i các b d nh tuy n khác, chú ý v giao th c du c s d ng ki m tra, giám sát các k t n i.

C u hình b d nh tuy n Spicey

```
Current configuration : 1705 bytes
!
version 12.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Spicey
!
interface Ethernet0
 ip address 124.124.124.1 255.255.255.0
!
interface Serial0
 ip address 3.1.3.1 255.255.255.0
 encapsulation frame-relay
 frame-relay interface-dlci 140
!
!
router rip
network 3.0.0.0
network 124.0.0.0
```

```
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

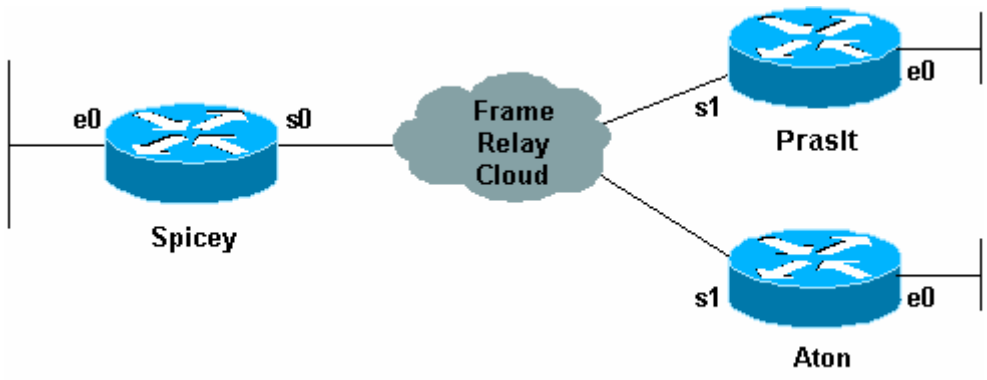
Hình 3.35: C u hình c a b d nh tuy n Spicey

C u hình b d nh tuy n Prasit

```
Current configuration : 1499 bytes
!
version 12.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Prasit
!
!
!
interface Ethernet0
 ip address 123.123.123.1 255.255.255.0
!
!
interface Serial1
 ip address 3.1.3.2 255.255.255.0
 encapsulation frame-relay
 frame-relay interface-dlci 150
!
!
router rip
 network 3.0.0.0
 network 123.0.0.0
!
!
line con 0
 exec-timeout 0 0
 transport input none
```

```
line aux 0
line vty 0 4
 login
!
end
```

Hình 3.36: C u hình c a b d nh tuy n Prasit



Hình 3.37: Mô hình k t n i Frame Relay Hub-Spoke

- C u hình
  - **Spicey(config)# interface serial 0**
- L a ch n giao th c s d ng
  - **Spicey(config-if)# encapsolation frame-relay**

- Xác d nh giao th c qu n tr LMI. Luu ý trong ví d này có s d ng m t chu n k t n i LMI khác. Chu n k t n i LMI không có giá tr toàn c c mà ch có giá tr t i giao ti p c a thi t b d u cu i v i m ng Frame Relay. Trong c u hình c a các b d nh tuy n khác v n s d ng LMI chu n cisco.
  - **Spicey(config-if)# frame-relay lmi-type ansi**
- Luôn ph i dua giao ti p vào s d ng b ng l nh no shutdown
  - **Spicey(config-if)# no shutdown**
- Trong ví d này, s d ng giao ti p con, subinterface, nên không d t d a ch cho giao ti p th c, physical interface.
- C u hình giao ti p con. Giao ti p con ph i s d ng m t trong hai l a ch n là point-to-point ho c multipoint, dây s d ng point-to-point cho giao ti p con s0.1 và multipoint cho giao ti p con s0.2.
  - **Spicey(config-if)# interface serial 0.1 point-to-point**
- Ho c
  - **Spicey(config-if)# exit**
  - **Spicey(config)# interface serial 0.1 point-to-point**

- Gán DLCI du c c p cho giao ti p. DLCI 140 là DLCI g n v i PVC n i gi a Spicey và Prasit, còn DLCI 130 g n v i PVC n i t i Aton.
  - **Spicey(config-if)# frame-relay interface-dlci 140**
- Xác l p d a ch IP cho giao ti p con th nh t
  - **Spicey(config-subif)# ip address 4.0.1.1 255.255.255.0**
  - **Spicey(config-subif)# exit**
- C u hình giao ti p con th hai t i Aton
  - **Spicey(config)# interface serial 0.2 multipoint**
- Gán DLCI du c c p cho giao ti p là DLCI 130
  - **Spicey(config-if)# frame-relay interface-dlci 130**
- Xác l p d a ch IP cho giao ti p con th 2
  - **Spicey(config-subif)# ip address 3.1.3.1 255.255.255.0**
  - **Spicey(config-subif)# exit**
- S d ng d nh tuy n d ng RIP
  - **Spicey(config)# router rip**
  - **Spicey(config-router)# network 3.0.0.0**
  - **Spicey(config-router)# network 4.0.0.0**
  - **Spicey(config-router)# network 124.0.0.0**
  - **Spicey(config-router)# end**
- Luôn ph i ghi l i c u hình khi dã c u hình xong
  - **Spicey# write memory**
- Th c hi n các ph n vi c còn l i t i các b d nh tuy n khác, chú ý v giao th c du c s d ng ki m tra, giám sát các k t n i.

C u hình b d nh tuy n Spicey

```
Spicey#show running-config
Building configuration...
!
version 12.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Spicey
!
!
interface Ethernet0
 ip address 124.124.124.1 255.255.255.0
!
```

```
interface Serial0
 no ip address
 encapsulation frame-relay
 frame-relay lmi-type ansi
!
interface Serial0.1 point-to-point
 ip address 4.0.1.1 255.255.255.0
 frame-relay interface-dlci 140
!
interface Serial0.2 multipoint
 ip address 3.1.3.1 255.255.255.0
 frame-relay interface-dlci 130
!
router igrp 2
 network 3.0.0.0
 network 4.0.0.0
 network 124.0.0.0
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Hình 3.38: C u hình c a b d nh tuy n Spicey

C u hình b d nh tuy n Prasit

```
Prasit#show running-config
Building configuration...

version 12.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Prasit
!
interface Ethernet0
ip address 123.123.123.1 255.255.255.0
```

```
!
interface Serial1
 no ip address
 encapsulation frame-relay
!
!--- LMI cisco là m c d nh nên không th  hi n trong c u hình
!--- Prasit và Spicey dã s  d ng 2 ki u LMI khác nhau
!--- B  d nh tuy  n t i Prasit s  d ng giao ti p con point-to-point
interface Serial1.1 point-to-point
 ip address 4.0.1.2 255.255.255.0
 frame-relay interface-dlci 150
!
router igrp 2
 network 4.0.0.0
 network 123.0.0.0
!
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Hình 3.39: C u hình c a b d nh tuy n Prasit

C u hình b d nh tuy n Aton

```
Aton#show running-config
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
!
hostname Aton
!
!
!
```

```
interface Ethernet0
 ip address 122.122.122.1 255.255.255.0
!
interface Serial1
 ip address 3.1.3.3 255.255.255.0
 encapsulation frame-relay
 frame-relay lmi-type q933a
!--- Aton có ki u LMI khác hai b  d nh tuy n kia
!--- Aton không s  d ng giao ti p con. Giao ti p con c n xác d nh
!là point-to-point hay multipoint   b  d nh tuy n trung tâm
!còn   các b  d nh tuy n còn l  i có th  dùng giao ti p con
!point-to-point hay giao ti  p th c, physical interface
 frame-relay interface-dlci 160
!
router igrp 2
 network 3.0.0.0
 network 122.0.0.0
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Hình 3.40: C u hình c a b d nh tuy n Aton

4.3. C u hình Dial-up

Gi i thi u quay s

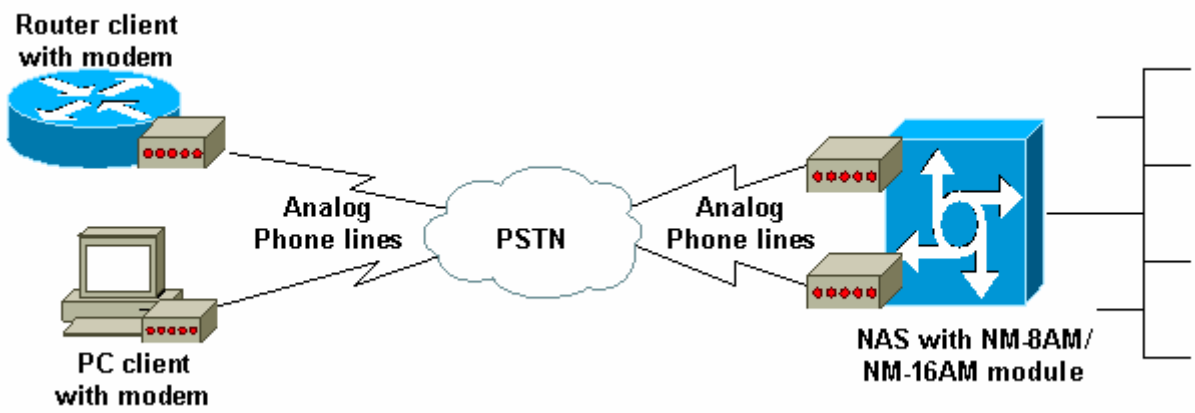
K t n i quay s cho phép s d ng du ng di n tho i d k t n i trao d i d li u. T c d c a k t n i quay s là không cao và ch có th đáp ng du c cho các ng d ng không yêu c u v bang thông cung nhu th i gian tr .

K t n i quay s s d ng modem V34, V90 là ph bi n. T c d truy n d li u lên m ng và t i d li u v t i da là 33,6Kbps. Đ có th th c hi n t i v v i t c d l n hon, t i 56Kbps, b d nh tuy n đóng vai trò đi m truy nh p ph i có k t n i thuê bao d ng s và dùng modem s .

Đ i v i các doanh nghi p nh , vi c xác th c ngu i dùng có th th c hi n b ng cách khai báo d li u tr c ti p trên b d nh tuy n. Cách s d ng này không thích h p cho các doanh nghi p v a và l n hay các doanh nghi p c n có s qu n lý ch t ch ngu i dùng m t cách h th ng. Lúc này c n thi t có các h

th ng qu n lý ngu i dùng. Các b d nh tuy n c a Cisco cho phép s d ng hai chu n xác th c TACACS+ và RADIUS.

Mô hình s d ng quay s



Hình 3.41: C u hình c a b d nh tuy n Aton

C u hình quay s co b n

Danh m c công vi c:

- C u hình giao ti p không d ng b Async
- C u hình giao ti p di u khi n modem
- C u hình xác th c
- Giám sát

- **Router#show interface Async 1**
- **Router#show line 1**
- **Router#debug ppp authentication**

C u hình quay s co b n

```
Current configuration : 1251 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
!
hostname cisco3640
!
boot system flash:c3640-i-mz.122-8.T
```

```
enable secret 5 <dã xóa>
!
! –-- Tên truy nh p cho xác th  c ngu i dùng c c b
username abc password 0 abc
!
ip subnet-zero
!
no ip domain-lookup
ip domain-name cisco.com
!
! –-- Xác d nh d  a ch  máy ch  DNS cho các máy tr m quay s
async-bootp DNS-server 5.5.5.1 5.5.5.2
!
!
interface Loopback0
  ip address 1.1.1.1 255.255.255.0
!
interface Ethernet2/0
  ip address 20.20.20.1 255.255.255.0
  half-duplex
!
! <<--các giao ti p không dùng du c b  di
!
!--- Giao ti p Group-Async1 c u hình cho t t c  các các modem
!--- không c n c  u hình riêng r  t ng modem
interface Group-Async1
  ip unnumbered Loopback0
  encapsulation ppp
  dialer in-band
!--- Xác l  p th i gian không s   d ng là 10 phút
!--- sau th i gian này, b  d nh tuy n s  t  d ng c t k t n  i
  dialer idle-timeout 600
!--- Đ nh nghi a các lo i hình d  li u du c dùng
!--- thông qua c  u hình dialer-group và dialer-list
  dialer-group 1
!--- Ch  d   interative cho phép ngu i dùng s   d ng nhi u giao th c
!--- d  không cho phép ngu i dùng thi t l  p các k t n i d n b   d nh
tuy n s  d  ng ch   d  dedicated
  async mode interactive
!--- Các máy tr m khi quay s  vào s  du c c p đ a ch  IP
!--- du c qui d nh trong DIALIN
  peer default ip address pool DIALIN
  ppp authentication chap
```

```
!--- Xác l  p các modem t   line 1 d n line 8 thu c v  nhóm này
  group-range 1 8
!
ip local pool DIALIN 10.1.1.1 10.1.1.10
ip classless
ip route 0.0.0.0 0.0.0.0 20.20.20.100
ip http server
ip pim bidir-enable
!
!--- Dòng l nh sau cho phép giao th c IP là giao th c ho t d ng
!--- n u không có các d  li  u IP di qua sau kho ng th i gian 10 phút
!--- du ng k t n  i s  b  c t
dialer-list 1 protocol ip permit
!
line con 0
  password abc
line 1 8
!--- Dòng l nh du i cho phép modem quay vào và quay ra
  modem InOut
  transport input all
  autoselect ppp
  flowcontrol hardware
line aux 0
line vty 0 4
  login
!
!
end
```

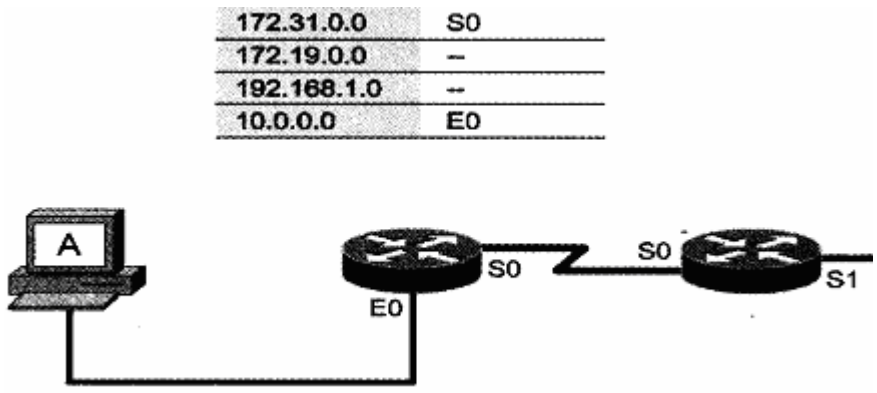
Hình 3.42: C u hình quay s co b n

4.4. Đ nh tuy n tinh và d ng

So lu c v d nh tuy n

Ch c nang xác d nh du ng d n cho phép b d nh tuy n u c lu ng các du ng d n kh thi d d n dích và thi t l p s ki m soát các gói tin. B d nh tuy n s d ng các c u hình m ng d dánh giá các du ng d n m ng. Thông tin này có th du c c u hình b i ngu i qu n tr m ng hay du c thu th p thông qua quá trình x lý d ng du c th c thi trên m ng.

L p m ng dùng b ng d nh tuy n IP d g i các gói tin t m ng ngu n d n m ng dích. B d nh tuy n d a vào các thông tin du c gi trong b ng d nh tuy n d quy t d nh truy n t i các gói tin theo các giao ti p thích h p.



Hình 3.43: S d ng b ng d nh tuy n d truy n t i các gói tin

M t b ng d nh tuy n IP bao g m các d a ch m ng dích, d a ch c a di m c n di qua, giá tr d nh tuy n và giao ti p d th c hi n vi c truy n t i. Khi không có thông tin v m ng dích, b d nh tuy n s g i các gói tin theo m t du ng d n m c d nh du c c u hình trên b d nh tuy n, n u du ng d n không t n t i, b d nh tuy n t d ng lo i b gói tin.

Có hai phuong th c d nh tuy n là:

- Đ nh tuy n tinh (static routing): là cách d nh tuy n không s d ng các giao th c d nh tuy n. Các d nh tuy n d n m t m ng dích s du c th c hi n m t cách c d nh không thay d i trên m i b d nh tuy n. M i khi th c hi n vi c thêm hay b t các m ng, ph i th c hi n thay d i c u hình trên m i b d nh tuy n.
- Đ nh tuy n d ng (dynamic routing): là vi c s d ng các giao th c d nh tuy n d th c hi n xây d ng nên các b ng d nh tuy n trên các b d nh tuy n. Các b d nh tuy n thông qua các giao th c d nh tuy n s t d ng trao d i các thông tin d nh tuy n, các b ng d nh tuy n v i nhau. M i khi có s thay d i v m ng, ch c n khai báo thông tin m ng m i trên b d nh tuy n qu n lý tr c ti p m ng m i dó mà không c n ph i khai báo l i trên m i b d nh tuy n. M t s giao th c d nh tuy n d ng du c s d ng là RIP, RIPv2, OSPF, EIGRP v.v...

Giá tr d nh tuy n du c xây d ng tùy theo các giao th c d nh tuy n khác nhau. Giá tr d nh tuy n c a các k t n i tr c ti p và d nh tuy n tinh có giá tr nh nh t b ng 0, d i v i d nh tuy n d ng thì giá tr d nh tuy n du c tính toán tùy thu c và t ng giao th c c th . Giá tr d nh tuy n du c th hi n trong b ng d nh tuy n là giá tr d nh tuy n t t nh t dã du c b d nh tuy n tính toán và xây d ng nên trên co s các giao th c d nh tuy n du c c u hình và giá tr d nh tuy n c a t ng giao th c.

Các giao th c d nh tuy n d ng du c chia thành 2 nhóm chính:

- **Các giao th c d nh tuy n kho ng cách véc to** (distance-vecto, *sau dây du c g i t t là d nh tuy n vecto)* : d a vào các gi i thu t d nh tuy n có co s ho t d ng là kho ng cách véc to.

Theo d nh k các b d nh tuy n chuy n toàn b các thông tin có trong b ng d nh tuy n d n các b d nh tuy n láng gi ng d u n i tr c ti p v i nó và

cung theo d nh k nh n các b ng d nh tuy n t các b d nh tuy n láng gi ng. Sau khi nh n du c các b ng d nh tuy n t các b d nh tuy n láng gi ng, b d nh tuy n s so sánh v i b ng d nh tuy n hi n có và quy t d nh v vi c xây d ng l i b ng d nh tuy n theo thu t toán c a t ng giao th c hay không. Trong tru ng h p ph i xây d ng l i, b d nh tuy n sau dó s g i b ng d nh tuy n m i cho các láng gi ng và các láng gi ng l i th c hi n các công vi c tuong t . Các b d nh tuy n t xác d nh các láng gi ng trên co s thu t toán và các thông tin thu lu m t m ng.

T vi c c n thi t ph i g i các b ng d nh tuy n m i l i cho các láng gi ng và các láng gi ng sau khi xây d ng l i b ng d nh tuy n l i g i tr l i b ng d nh tuy n m i, d nh tuy n thành vòng có th x y ra n u s h i v tr ng thái b n v ng c a m ng di n ra ch m trên m t c u hình m i. Các b d nh tuy n s d ng các k thu t b d m d nh th i d d m b o không n y sinh vi c xây d ng m t b ng d nh tuy n sai. Có th di n gi i di u dó nhu sau:

- o Khi m t b d nh tuy n nh n m t c p nh t t m t láng gi ng ch r ng m t m ng có th truy xu t tru c dây, nay không th truy xu t du c n a, b d nh tuy n dánh d u tuy n là không th truy xu t và kh i d ng m t b d nh th i.
- o N u t i b t c th i di m nào mà tru c khi b d nh th i h t h n m t c p nh t du c ti p nh n cung t láng gi ng dó ch ra r ng m ng dã du c truy xu t tr l i, b d nh tuy n dánh d u là m ng có th truy xu t và gi i phóng b d nh th i.
- o N u m t c p nh t d n t m t b d nh tuy n láng gi ng khác v i giá tr d nh tuy n t t hon giá tr d nh tuy n du c ghi cho m ng này, b d nh tuy n dánh d u m ng có th truy xu t và gi i phóng b d nh th i. N u giá tr d nh tuy n t i hon, c p nh t du c b qua.
- o Khi b d nh th i du c d m v 0, giá tr d nh tuy n m i du c xác l p, b d nh tuy n có b ng d nh tuy n m i.

- **Các giao th c d nh tuy n tr ng thái du ng** (link-state, *g i t t là d nh tuy n tr ng thái*): Gi i thu t co b n th hai du c dùng cho d nh tuy n là gi i thu t 1ink-state. Các gi i thu t d nh tuy n tr ng thái, cung du c g i là SPF (shortest path first, *ch n du ng d n ng n nh t*), duy trì m t co s d li u ph c t p ch a thông tin v c u hình m ng.
- Trong khi gi i thu t vecto không có thông tin d c bi t gì v các m ng xa và cung không bi t các b d nh tuy n xa, gi i thu t d nh tuy n tr ng thái bi t du c d y d v các b d nh tuy n xa và bi t du c chúng liên k t v i nhau nhu th nào.

Giao th c d nh tuy n tr ng thái s d ng:

- o Các thông báo v tr ng thái liên k t: LSA (Link State Advertisements).
- o M t co s d li u v c u hình m ng.
- o Gi i thu t SPF, và cây SPF sau cùng.
- o M t b ng d nh tuy n liên h các du ng d n và các c ng d n t ng m ng.

Ho t d ng tìm hi u khám phá m ng trong d nh tuy n tr ng thái du c th c hi n nhu sau:

o Các b d nh tuy n trao d i các LSA cho nhau. M i b d nh tuy n b t d u v i các m ng du c k t n i tr c ti p d l y thông tin.

o M i b d nh tuy n d ng th i v i các b d nh tuy n khác ti n hành xây d ng m t co s d li u v c u hình m ng bao g m t t c các LSA d n t liên m ng.

o Gi i thu t SPF tính toán m ng có th d t d n. B d nh tuy n xây d ng c u hình m ng lu n lý này nhu m t cây, t nó là g c, g m t t c các du ng d n có th d n m i m ng trong toàn b m ng dang ch y giao th c d nh tuy n tr ng thái. Sau dó, nó s p x p các du ng d n này theo chi n lu c ch n du ng d n ng n nh t.

o B d nh tuy n li t kê các du ng d n t t nh t c a nó, và các c ng d n d n các m ng dích, trong b ng d nh tuy n c a nó. Nó cung duy trì các co s d li u khác v các ph n t c u hình m ng và các chi ti t v hi n tr ng c a m ng.

Khi có thay d i v c u hình m ng, b d nh tuy n d u tiên nh n bi t du c s thay d i này g i thông tin d n các b d nh tuy n khác hay d n m t b d nh tuy n d nh tru c du c gán là tham chi u cho t t c các các b d nh tuy n trên m ng làm can c c p nh t.

o Theo dõi các láng gi ng c a nó, xem xét có ho t d ng hay không, và giá tr d nh tuy n d n láng gi ng dó.

o T o m t gói LSA trong dó li t kê tên c a t t c các b d nh tuy n láng gi ng và các giá tr d nh tuy n d i v i các láng gi ng m i, các thay d i trong giá tr d nh tuy n, và các liên k t d n d n các láng gi ng dã du c ghi.

o G i gói LSA này di sao cho t t c các b d nh tuy n d u nh n du c.

o Khi nh n m t gói LSA, ghi gói LSA vào co s d li u d sao cho c p nh t gói LSA m i nh t du c phát ra t m i b d nh tuy n.

o Hoàn thành b n d c a liên m ng b ng cách dùng d li u t các gói LSA tích luy du c và sau dó tính toán các tuy n d n d n t t c các m ng khác s d ng thu t toán SPF.

Có hai v n d luu ý d i v i giao th c d nh tuy n tr ng thái:

o Ho t d ng c a các giao th c d nh tuy n tr ng thái trong h u h t các tru ng h p d u yêu c u các b d nh tuy n dùng nhi u b nh và th c thi nhi u hon so v i các giao th c d nh tuy n theo vecto. Các yêu c u này xu t phát t vi c c n thi t ph i luu tr thông tin c a t t c các láng gi ng, co s d li u m ng d n t các noi khác và vi c th c thi các thu t toán d nh tuy n tr ng thái. Ngu i qu n lý m ng ph i d m b o r ng các b d nh tuy n mà h ch n có kh nang cung c p các tài nguyên c n thi t này.

o Các nhu c u v bang thông c n ph i tiêu t n d kh i d ng s phát tán gói tr ng thái. Trong khi kh i d ng quá trình khám phá, t t c các b d nh tuy n dùng các giao th c d nh tuy n tr ng thái d g i các gói LSA d n t t c

các b d nh tuy n khác. Hành d ng này làm tràn ng p m ng khi mà các b d nh tuy n d ng lo t yêu c u bang thông và t m th i làm gi m lu ng bang thông kh d ng dùng cho luu lu ng d li u th c du c d nh tuy n. Sau kh i d ng phát tán này, các giao th c d nh tuy n tr ng thái thu ng ch yêu c u m t lu ng bang thông t i thi u d g i các gói LSA kích ho t s ki n không thu ng xuyên nh m ph n ánh s thay d i c a c u hình m ng.

- **Và m t nhóm giao th c th 3** là nhóm các giao th c d nh tuy n lai ghép gi a 2 nhóm trên hay nói cách khác có các tính ch t c a c hai nhóm giao th c trên.

Các giao th c d nh tuy n

B ng 3-10:Các giao th c d nh tuy n

Các d c trung	RIPv1	RIPv2	IRGP	EIGRP	OSPF
Kho ng cách vecto	X	X	x	x	
Tr ng thái du ng			x		
T d ng tóm t t d nh tuy n			X	X	x x
H tr VLSM			X	x	x
Tuong thích v i s n ph m th ba			X	X	X
Thích h p	Nh	Nh	V a	L n	L n
Th i gian h i t v tr ng thái cân b ng	Ch m	Ch m	Ch m	Nhanh	Nhanh
Giá tr d nh tuy n hop	hop count	hop count	~ BW +D	~ BW+D	~ 10E8/BW
Gi i h n hop count	15	15	100	100	
Cân b ng t i cùng giá tr d nh tuy n			X	x	x X

VLSM (Vary Length Subnet Mask): h tr d nh tuy n cho các m ng con subnetmask có d dài [1] thay d i hay nói cách khác thông tin v subnetmask bao g m trong b ng d nh tuy n

Hop count: du c tính b ng s các di m node m ng mà gói tin ph i di qua t di m này d n di m [2] kia hay chính b ng s các b d nh tuy n mà gói tin ph i d i qua

BW (bandwitch): bang thông [3]

D (delay): tr [4]

Cân b ng t i không x x
cùng giá tr d nh tuy n
Thu t toán Bellman- Bellman- Bellman- DUAL Dijkstra
Ford Ford Ford

C u hình d nh tuy n d ng co b n v i RIP

M t s luu ý khi c u hình d nh tuy n d ng v i RIP

- RIP g i các thông tin c p nh t theo các chu k d nh tru c, giá tr m c d nh là 30 giây, và khi có s thay d i b ng d nh tuy n.
- RIP s d ng s d m các node (hop count) d làm giá tr dánh giá ch t lu ng c a d nh tuy n (metric). RIP ch gi duy nh t d nh tuy n có giá tr d nh tuy n th p nh t.
- Giá tr hop count t i da cho phép là 15.
- RIP s d ng các b d m th i gian cho vi c th c hi n g i các thông tin c p nh t, xoá b m t d nh tuy n trong b ng cung nhu d di u khi n các quá trình t o l p b ng d nh tuy n, tránh loop vòng.
- RIPv1: Classfull: không có thông tin v subnetmask
- RIPv2: Classless: có thông tin v subnetmask

C u hình d nh tuy n v i RIP:

Cho phép giao th c d nh tuy n RIP ho t d ng trên b d nh tuy n.

- **Router(config)#router rip**

Thi t l p các c u hình m ng. Network là nhóm m ng tính theo l p m ng co b n dang có các giao ti p tr c ti p trên b d nh tuy n.

- **Router(config-router)#network 192.168.100.0**
- **Router(config-router)#network 172.25.0.0**
- **Router(config-router)#network 10.0.0.0**

- Trong tru ng h p s d ng RIP v i các m ng không ph i là m ng broadcast nhu X.25, Frame Relay c n thi t c u hình RIP v i các d a ch Unicast là các d a ch mà RIP s g i t i các thông tin c p nh t

- **Router(config-router)#neighbor 192.168.113.1**
- **Router(config-router)#neighbor 192.168.113.5**

- Tu theo di u ki n c th v h t ng m ng có th thay d i chu k c p nh t thông tin, các d nh nghia th i gian khác cho phù h p.

- **Router(config-router)# timers basic update invalid holddown flush [sleeptime]**

- Các thay d i khác.

- **Router(config-router)# version {1 | 2}**
- **Router(config-router)# ip rip authentication key-chain name-of-chain**
- **Router(config-router)# ip rip authentication mode {text | md5}**

- Giám sát.
  - **show ip interfaces**
  - **show ip rip**

C u hình b d nh tuy n v i RIP

```
version 12.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Prasit
!
interface Ethernet0
 ip address 123.123.123.1 255.255.255.0
!
interface Serial1
 ip address 3.1.3.2 255.255.255.0
 encapsulation frame-relay
 frame-relay interface-dlci 150
!
router rip
 network 3.0.0.0
 network 123.0.0.0
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
end
```

Hình 3.44: C u hình c a b d nh tuy n v i RIP

5. B chuy n m ch l p 3

5.1. T ng quan và ki n trúc b chuy n m ch l p 3

T ng quan

B chuy n m ch l p 3 là m t trong các thi t b m ng du c phát tri n m i trên các công ngh ngày càng tiên ti n. B chuy n m ch l p 3, nhu tên g i c a nó, bao g m các ch c nang x lý gói tin ho t d ng trên l p 3, l p m ng, trong mô hình 7 l p OSI, th c hi n các ch c nang d nh tuy n và x lý gói tin tuong t b d nh tuy n d ng th i th c hi n chuy n m ch gói tin l p 2 nhu các b chuy n

m ch l p 2, khác h n v i th h tru c dây c a nó ch th c hi n các x lý chuy n m ch gói tin l p 2 can c trên các d a ch MAC c a gói tin.
Khi nh n du c gói tin, b d nh tuy n s th c hi n xem xét các thông tin l p 3 c a gói tin d l a ch n du ng di cho gói tin còn b chuy n m ch thì ch can c vào d a ch l p 2, d a ch MAC, d th c hi n chuy n gói tin. S khác nhau co b n gi a b d nh tuy n và b chuy n m ch l p 3 là b chuy n m ch l p 3 du c c u thành t các ph n c ng chuyên d ng du c thi t k riêng cho b chuy n m ch cho phép th c hi n các chuy n m ch gói tin nhanh nhu các chuy n m ch l p 2, di u không có các b d nh tuy n, trong khi v n có kh nang x lý d nh tuy n các gói tin v i ch c nang tuong t nhu b d nh tuy n.
Trong môi tru ng LAN, b chuy n m ch l p 3 du c dánh giá là nhanh hon so v i b d nh tuy n và làm tang nang l c ho t d ng c a m ng trên co s nang l c chuy n m ch và d nh tuy n c a nó. Tuy nhiên, b chuy n m ch l p 3 không th thay th hoàn toàn cho b d nh tuy n do d c trung LAN c a b chuy n m ch l p 3 và không ho t d ng trên môi tru ng da giao th c nhu b d nh tuy n.
Ch c nang và ki n trúc c a b chuy n m ch l p 3 cung tuong t nhu b d nh tuy n và bao g m:

- Chuy n m ch gói tin
- Các ho t d ng d nh tuy n
- Tính nang m ng thông minh

Chuy n m ch gói tin

Chuy n m ch gói tin là ch c nang co b n chính c a b chuy n m ch l p 3. Đi u khác nhau co b n gi a b d nh tuy n và b chuy n m ch l p 3 chính là b d nh tuy n dùng b x lý trung tâm d th c hi n các x lý chuy n m ch gói tin còn b chuy n m ch l p 3 dùng các thành ph n ph n c ng du c thi t k chuyên d ng ASIC (Application Specific Integrated Circuit).
Thành ph n ch c nang chuy n m ch gói tin c a b chuy n m ch th c hi n các công vi c ki m tra d a ch gói tin, so sánh v i thông tin luu tr và th c hi n truy n t i chúng theo hu ng xác d nh. Chúng d ng th i cung th c hi n các x lý l p du i tuong t b d nh tuy n v i vi c gán l i các d a ch MAC, gi m s d m TTL... Ch c nang chuy n m ch gói tin cung th c hi n phép so sánh dúng nh t d l a ch n du ng di dúng khi có nhi u hon m t kh nang d l a ch n.

Các ho t d ng d nh tuy n

Ho t d ng d nh tuy n là m t ho t d ng d c l p khác so v i ho t d ng chuy n m ch gói tin. B d nh tuy n cung nhu b chuy n m ch l p 3 qu n lý và di u hành các thông tin d nh tuy n, xây d ng, c p nh t và trao d i chúng thông qua các giao th c d nh tuy n m i khi có s thay d i v m ng nhu l i du ng, thêm m i hay c p nh t thi t b ...
Cung nhu các b d nh tuy n, b chuy n m ch l p 3 ho t d ng v i h u h t các giao th c d nh tuy n d ng hi n có.

Tính nang m ng thông minh

Các tính nang qu n tr , c p phát d ng, các tính nang d nh tuy n thông minh, các tính nang b o m t, xác th c cung du c thi t k và xây d ng trên b d nh tuy n l p 3 qua dó d dàng cho ngu i qu n tr th c hi n v i c xây d ng, qu n tr và phát tri n m ng.

5.2. Đ nh tuy n trên b chuy n m ch l p 3

VLAN

VLAN là khái ni m d ch m t m ng LAN d c l p m t cách logic v i nhau. V th c ch t, t t c các thi t b m ng du c d u n i và ho t d ng trên cùng m t môi tru ng v t lý, h t ng m ng chung và hình thành m t cách logic các m ng LAN trên môi tru ng dó d a trên các thi t d t nh n d ng d c l p v i nhau d i v i m i nhóm thành viên. Nói cách khác, m i c ng k t n i c a các b chuy n m ch du c d nh nghia thu c v m t nhóm làm vi c (VLAN) nào dó và hình thành các kh nang d c l p tách r i c a các nhóm làm vi c dó v i nhau. Các gói tin c a m t VLAN ch du c luu chuy n t i các c ng trong cùng VLAN mà không du c luu chuy n d n các c ng khác VLAN tr c ng du c d nh nghia là trung k c a các VLAN. Khác v i LAN, VLAN không b gi i h n v ph m vi d a lý c th mà ch ph thu c vào nhu c u và hình th c tri n khai.

VLAN Trunking là khái ni m du c dùng d ch vi c k t n i gi a các b chuy n m ch v i nhau mà qua dó cho phép các gói tin c a t t c các VLAN du c truy n qua.

VLAN du c c u hình t i l p 2 cho phép phân d nh các nhóm thi t b máy tính d c l p logic v i nhau, các nhu c u trao d i d li u gi a các thi t b khác VLAN ph i du c th c hi n b i các thi t b ho t d ng l p 3 nhu b chuy n m ch l p 3 hay các b d nh tuy n.

Các giao th c và mô hình k t n i VLAN xin xem thêm trong các giáo trình v m ng n i b LAN.

C u trúc x lý d nh tuy n

Nhu dã nói ph n tru c, b chuy n m ch l p 3 d ng th i th c hi n các ch c nang chuy n m ch và ch c nang d nh tuy n. B chuy n m ch l p 3 cho phép các thi t b thu c v các nhóm m ng khác nhau, các VLAN khác nhau có th k t n i du c v i nhau.

dây c n phân bi t các nhu c u k t n i trao d i d li u khác nhau trong dó bao g m:

- Các nhu c u k t n i trao d i d li u trên các m ng s d ng nhóm giao th c m ng d nh tuy n du c nhu IP, IPX.
- Các nhu c u k t n i trao d i d li u trên các m ng s d ng nhóm giao th c m ng không d nh tuy n du c nhu NetBEUI, AppleTalk.

Đ i v i nhóm giao th c không d nh tuy n du c, b chuy n m ch x lý chúng b ng nhóm các giao th c c u n i (bridge). Các giao th c d nh tuy n du c s du c x lý tuong t nhu m t b d nh tuy n. B chuy n m ch l p 3 h tr d nh

tuy n - c u n i k t h p, d nh tuy n gi a các VLAN, các chuy n m ch nhi u l p.

Chuy n m ch và d nh tuy n k t h p

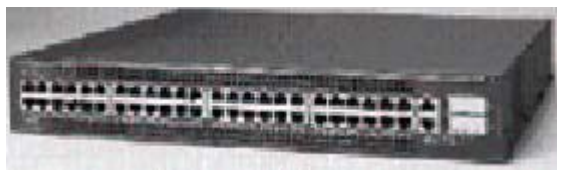
Cho phép b chuy n m ch chuy n các gói tin thu c nhóm các giao th c không d nh tuy n du c gi a các c ng du c c u hình ch d c u n i d ng th i cho phép chuy n các gói tin thu c nhóm d nh tuy n du c qua l i gi a các c ng thu c v các VLAN s d ng cho nhóm các giao th c d nh tuy n du c. Giao th c chuy n m ch và d nh tuy n k t h p ch th c hi n x lý d nh hu ng các gói tin trên cùng m t thi t b chuy n m ch.

Đ nh tuy n gi a các VLAN

Vi c d nh tuy n gi a các VLAN du c th c hi n trên các b chuy n m ch l p 3, thông qua các module d nh tuy n l p 3 ho c th c hi n trên các b chuy n m ch. B chuy n m ch l p 3 h tr các giao th c d nh tuy n tinh, d nh tuy n d ng RIP, OSPF, IGRP, EIGRP.

5.3. So lu c v các b chuy n m ch l p 3 thông d ng c a Cisco

B chuy n m ch l p 3 Cisco 2948G-L3



Hình 3.45: B chuy n m ch l p 3 Cisco 2948G-L3

- 48 c ng 10/100 Ethernet, giao di n RJ45
- 02 c ng uplink Gigabit Ethernet h tr GBIC (Gigabit Interface Converter) cho phép l a ch n các giao di n khác nhau phù h p v i nhu c u s d ng c ng k t n i Gigabit
- T c d chuy n m ch l p 3: 10.000 gói tin/giây
- Thông lu ng: 22Gbit/giây
- H tr IP, IPX, IP multicast
- Ch c nang d nh tuy n l p 3: RIP, OSPF, IGRP, EIGRP
- Ch c nang chuy n d i d phòng, h tr trung chuy n giao th c c p d a ch d ng
- H tr QoS
- Ch c nang an ninh m ng v i danh sách truy nh p ACL

B chuy n m ch l p 3 Cisco 3550

Hình 3.46: Các b chuy n m ch l p 3 Cisco 3550

Lo i chuy n m ch S c ng 10/100 S c ng Gigabit
Catalyst 3550-24 Switch 24 2 (GBIC)
Catalyst 3550-24 PWR 24 (cho phép c p 2 (GBIC)
Switch ngu n qua cáp
m ng d n các
thi t b khác nhu
thi t b di m truy
c p không dây)
Catalyst 3550-24-DC Switch 24 2 (GBIC)
Catalyst 3550-24-FX Switch 24 (c ng quang 2 (GBIC)
t c d 100Mbps)
Catalyst 3550-48 Switch 48 2 (GBIC)
Catalyst 3550-12G Switch 10 (GBIC)
2 (10/100/1000BASE-T)
Catalyst 3550-12T switch 10 (10/100/1000BASE-T)
2 (GBIC)

- N ang l c x lý cao:
  - CEF: Cisco Express Forwarding
  - Các giao th c d nh tuy n: RIP, OSPF, IGRP, EIGRP, BGPv4
  - Inter-VLAN IP routing
  - Các giao th c d nh tuy n multicast
  - Các giao th c chuy n d i d phòng
- T i uu bang thông:
  - 1,6 Gigabit cho c ng 10/100 và 16 Gigabit cho c ng Gigabit
  - Ch c nang làm vi c v i máy ch cache theo giao th c WCCP
  - Kh nang h n ch t c d theo t ng ng d ng, nhóm ngu i dùng

- D dàng s d ng và khai thác
- An toàn và b o m t
    - Xác th c ngu i dùng v i các h th ng qu n tr t p trung TACACS+, RADIUS
    - Mã hóa SSH, Kerberos
    - Các tính nang xác th c thi t b
    - VLAN
- D dàng th c hi n QoS v i các m c d da d ng và linh ho t.
- Qu n tr t xa và t p trung. Tuong thích v i các h th ng qu n tr thông d ng.

Ngoài ra còn có các b chuy n m ch l p 3 c a Cisco v i các dòng 4000, 6000..

6. Bài t p th c hành s d ng b d nh tuy n Cisco

Bài 1: Th c hành nh n di n thi t b , d u n i thi t b

Yêu c u:

- Nh n di n dúng các ch ng lo i thi t b
- Nh n di n các giao ti p c a b d nh tuy n, ý nghia và m c dích s d ng
- Bi t cách s d ng các lo i cáp v i t ng lo i thi t b , giao ti p khác nhau
- Bi t d u n i b d nh tuy n v i nhau và v i các thi t b modem khác
- S d ng ph n m m HyperTerminal k t n i v i b d nh tuy n

Bài 2: Th c hành các l nh co b n

- Các l nh show
- L nh config

Yêu c u:

- N m v ng ý và s d ng thành th o các l nh ki m tra và các l nh c u hình co b n

Bài 3: C u hình b d nh tuy n v i mô hình d u n i leased-line

- C u hình Interface
- C u hình giao th c
- C u hình d nh tuy n

Yêu c u:

- S d ng thi t b phòng lab d c u hình m t k t n i leased-line cho phép k t n i 2 m ng v i nhau.
- V n d ng các ki n th c dã h c ki m soát và x lý s c .

Bài 4: C u hình b d nh tuy n v i Dial-up

- C u hình line v t lý

- C u hình async interface
- C u hình d nh tuy n
- C u hình xác th c

Yêu c u:

- S d ng thi t b phòng lab d c u hình m t di m truy nh p gián ti p quay s qua tho i.
- V n d ng các ki n th c dã h c ki m soát và x lý s c .

Thi t b phòng lab

- 02 b d nh tuy n 2509 (leased-line và async) ho c tuong duong
- 02 modem leased-line CSU/DSU dùng cho k t n i leased-line
- 02 cáp V.35 DTE
- 04 modem dial-up 56kbps
- 02 cáp Async dùng cho k t n i modem 56kbps
- Ph n m m gi l p b d nh tuy n (router simulator)
- 02 máy tính dùng d c u hình tr c ti p các b d nh tuy n
- các máy tính d th c hành trên ph n m m gi l p b d nh tuy n
- 04 du ng di n tho i

Chuong 4
H th ng tên mi n DNS

Chuong 4 s t p trung nghiên c u v h th ng tên mi n là m t h th ng d nh danh ph bi n trên m ng TCP/IP nói chung và d c bi t là m ng Internet. H th ng tên mi n t i quan tr ng cho s phát tri n c a các ng d ng ph bi n nhu thu tín di n t , web...C u trúc h th ng tên mi n, c u trúc và ý nghia c a các tru ng tên mi n cung nhu các k nang co b n du c cung c p s giúp cho ngu i qu n tr có th ho ch d nh du c các nhu c u liên quan d n tên mi n cho m ng lu i, ti n hành th t c dang ký chính xác (n u dang ký tên mi n Internet) và d m nh n du c các công tác t o m i, s a d i ... hay nói chung là các công vi c qu n tr h th ng máy ch tên mi n DNS

Chuong 4 dòi h i các h c viên ph i quen thu c v i d a ch IP, vi c so n th o qu n tr các ti n trình trên các h th ng linux, unix, windows.

1. Gi i thi u

1.1. L ch s hình thành c a DNS

Vào nh ng nam 1970 m ng ARPanet c a b qu c phòng M r t nh và d dàng qu n lý các liên k t vài tram máy tính v i nhau. Do dó m ng ch c n m t file HOSTS.TXT ch a t t c thông tin c n thi t v máy tính trong m ng và giúp các máy tính chuy n d i du c thông tin d a ch và tên m ng cho t t c máy tính trong m ng ARPanet m t cách d dàng. Và dó chính là bu c kh i d u c a h th ng tên mi n g i t t là DNS (Domain name system)

Nhu khi m ng máy tính ARPanet ngày càng phát tri n thì vi c qu n lý thông tin ch d a vào m t file HOSTS.TXT là r t khó khan và không kh thi. Vì thông tin b xung và s a d i vào file HOSTS.TXT ngày càng nhi u và nh t là khi ARPanet phát tri n h th ng máy tính d a trên giao th c TCP/IP d n d n s phát tri n tang v t c a m ng máy tính:

- Lu u lu ng và trao d i trên m ng tang lên
- Tên mi n trên m ng và d a ch ngày càng nhi u
- M t d máy tính ngày càng cao do dó d m b o phát tri n ngày càng khó khan

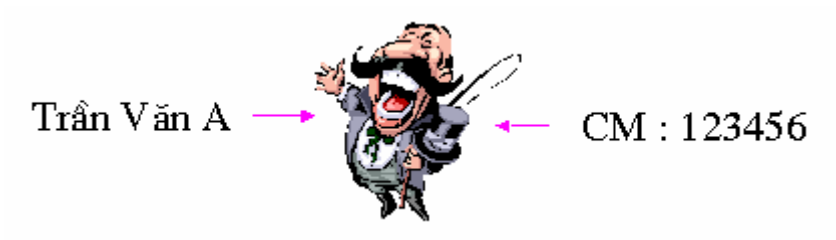
Đ n nam 1984 Paul Mockpetris thu c vi n USC's Information Sciences Institute ph t tri n m t h th ng qu n lý tên mi n m i (miêu t trong chu n RFC 882 - 883) g i là DNS (Domain Name System) và ngày này nó ngày càng du c phát tri n và hi u ch nh b xung tính nang d d m b o yêu c u ngày càng cao c a h th ng (hi n nay DNS du c tiêu chu n theo chu n RFC 1034 - 1035)

1.2. M c dích c a h th ng DNS

Máy tính khi k t n i vào m ng Internet thì du c gán cho m t d a ch IP xác d nh. Đ a ch IP c a m i máy là duy nh t và có th giúp máy tính có th xác d nh du ng di d n m t máy tính khác m t cách d dàng. Nhu d i v i ngu i dùng thì d a ch IP là r t khó nh . Do v y c n ph i s d ng m t h th ng d giúp cho máy tính tính toán du ng di m t cách d dàng và d ng th i cung giúp ngu i dùng d nh . Do v y h th ng DNS ra d i nh m giúp cho ngu i dùng có th chuy n d i t d a ch IP khó nh mà máy tính s d ng sang m t tên d nh cho ngu i s d ng và d ng th i nó giúp cho h th ng Internet d dàng s d ng d liên l c và ngày càng phát tri n.

H th ng DNS s d ng h th ng co s d li u phân tán và phân c p hình cây do dó vi c qu n lý s d dàng và cung r t thu n ti n cho vi c chuy n d i t tên mi n sang d a ch IP và ngu c l i. Cung gi ng nhu mô hình qu n lý cá nhân c a m t d t nu c m i cá nhân s có m t tên xác d nh d ng th i cung có d a ch ch ng minh thu d giúp qu n lý con ngu i m t cách d dàng hon (nhung khác là tên mi n không du c trùng nhau còn tên ngu i thì v n có th trùng nhau)

M i cá nh n d u có m t s can cu c d qu n lý



M i m t d a ch IP tuong ng v i m t tên mi n

V y tóm l i tên mi n là (domain name) gì ? nh ng tên g i nh nhu home.vnn.vn ho c www.cnn.com thì du c g i là tên mi n (domain name ho c DNS name). Nó giúp cho ngu i s d ng d dàng nh vì nó d ng ch mà ngu i bình thu ng có th hi u và s d ng hàng ngày.

H th ng DNS dã giúp cho m ng Internet thân thi n hon v i ngu i s d ng do dó m ng internet phát tri n bùng n m t vài nam l i dây. Theo th ng trên th gi i vào th i di m tháng 7/2000 s lu ng tên mi n du c dang ký là 93.000.000

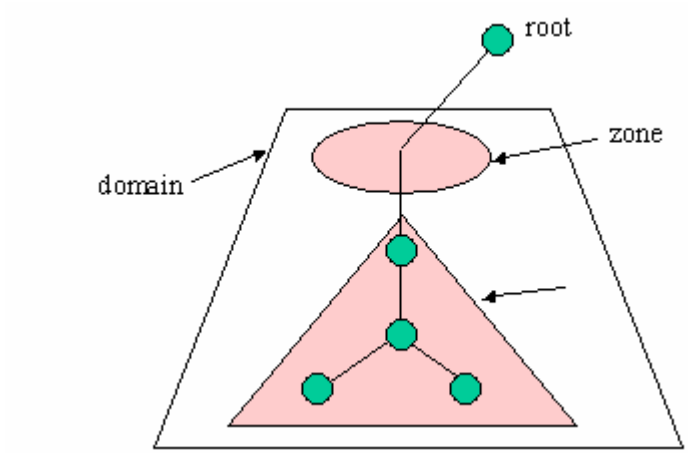
Tóm l i m c dích c a h th ng DNS là:

- Đ a ch IP khó nh cho ngu i s d ng nhu ng d dàng v i máy tính
- Tên thì d nh v i ngu i s d ng nhu không dùng du c v i máy tính
- H th ng DNS giúp chuy n d i t tên mi n sang d a ch IP và ngu c l i giúp ngu i dùng d dàng s d ng h th ng máy tính

2. DNS server và c u trúc co s d li u tên mi n

2.1.C u trúc co s d li u

Co s d li u c a h th ng DNS là h th ng co s d li u phân tán và phân c p hình cây. V i .Root server là d nh c a cây và sau dó các domain du c phân nhánh d n xu ng du i và ph n quy n qu n lý. Khi m t client truy v n m t tên mi n nó s l n lu t di t root phân c p l n lu t xu ng du i d d n DNS qu n lý domain c n truy v n.



C u trúc c a d li u du c phân c p hình cây root qu n lý toàn b so d và phân quy n qu n lý xu ng du i và ti p dó các tên mi n l i du c ti p t c chuy n xu ng c p th p hon (delegate) xu ng du i.

Zone

H th ng th ng tên và nó ch a DNS cho phép phân chia tên mi n d qu n lý và nó chia h mi n ra thành zone và trong zone qu n lý tên mi n du c phân chia dó thông tin v domain c p th p hon và có kh nang chia thành các zone c p th p hon và phân quy n cho các DNS server khác qu n lý.

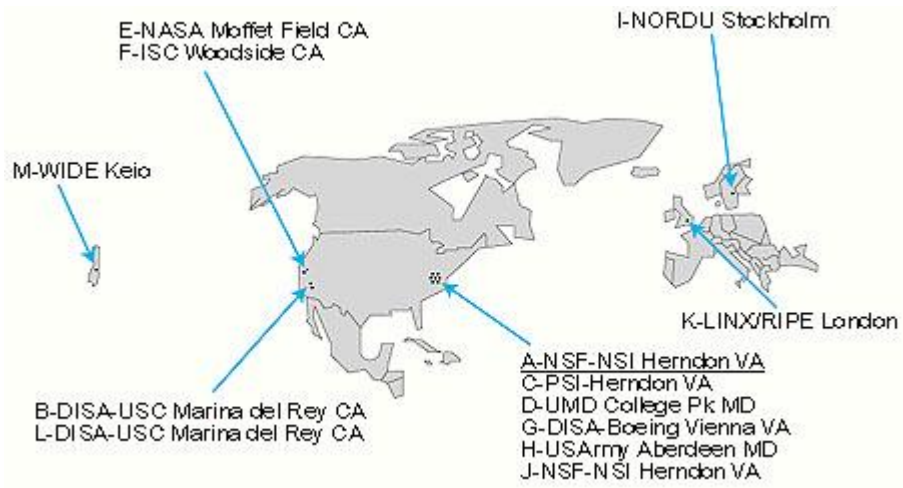
Ví d : zone *".com"* thì DNS server qu n lý zone *".com"* chua thông tin v các b n ghi có duôi là *".com"* và có kh nang chuy n quy n qu n lý (delegate) các zone c p th p hon cho các DNS khác qu n lý nhu *".microsoft.com"* là vùng (zone) do microsoft qu n lý.

Root Server

Là server qu n lý toàn b c u trúc c a h th ng DNS

Root server không ch a d li u thông tin v c u trúc h th ng DNS mà nó ch chuy n quy n (delegate) qu n lý xu ng cho các server c p th p hon và do dó root server có kh nang xác d nh du ng d n c a m t domain t i b t c dâu trên m ng

Hi n nay trên th gi i có kho ng 13 root server qu n lý toàn b h th ng Internet (v trí c a root server nhu trên hình v du i)



H th ng co s d li u c a DNS là h th ng d li u phân tán hình cây nhu c u trúc dó là c u trúc logic trên m ng Internet

V m t v t lý h th ng DNS n m trên m ng Internet không có có c u trúc hình cây nhung nó du c c u hình phân c p logic phân c p hình cây phân
quy n qu n lý.
M t DNS server có th n m b t c v trí nào trên m ng Internet nhu ng du c c u hình logic d phân c p chuy n tên mi n c p th p hon xu ng cho các DNS
server khác n m b t c v trí nào trên m ng Internet (v nguyên t c ta có th d t DNS t i b t c v trí nào trên m ng Internet. Nhung t t nh t là d t DNS t i v trí nào g n v i các client d d dàng truy v n d n d ng th i cung g n v i v trí c a DNS server c p cao hon tr c ti p c a nó).
M i m t tên mi n d u du c qu n lý b i ít nh t m t DNS server và trên dó ta khai các b n ghi c a tên mi n trên DNS server. Các b n ghi dó s xác d nh d a ch IP c a tên mi n ho c các d ch v xác d nh trên Internet nhu web, thu di n t ...

Sau dây là các b n ghi trên DNS

Tên tru ng Tên d y d M c d ích

SOA Start of Authority Xác d nh máy ch DNS có th m quy n cung c p thông tin v tên mi n xác d nh trên DNS

NS Name Server Chuy n quy n qu n lý tên mi n xu ng m t DNS c p th p hon

A Host Ánh x xác d nh d a ch IP c a m t host

MX Mail Exchanger Xác d nh host có quy n qu n lý thu di n t cho m t tên mi n xác d nh

PTR Pointer Xác d nh chuy n t d a ch IP sang tên mi n

CNAME Canonical NAME Thu ng s d ng xác d nh d ch v web hosting

C u trúc c a m t tên mi n

- Domain s có d ng : lable.lable.label...lable
- Đ dài t i da c a m t tên mi n là 255 ký t
- M i m t Lable t i da là 63 ký t
- Lable ph i b t d u b ng ch ho c s và ch du c phép ch a ch , s , d u tr (-), d u ch m (.) mà không du c ch a các ký t khác.

Phân lo i tên mi n

H u h t tên mi n du c chia thành các lo i sau:

- *Arpa* : tên mi n ngu c (chuy n d i t d a ch IP sang tên mi n reverse domain)
- *Com* : các t ch c thuong m i
- *Edu* : các co quan giáo d c
- *Gov* : các co quan chính ph
- *Mil* : các t ch c quân s , qu c phòng
- *Net* : các trung tâm m ng l n
- *Org* : các t ch c khác
- *Int* : các t ch c da chính ph (ít du c s d ng)

Ngoài ra hi n nay trên th gi i s d ng lo i tên mi n có hai ký t cu i d xác d nh tên mi n thu c qu c gia nào (du c xác d nh trong chu n ISO3166)

Lo i tên	**Miêu t Ví d**
G c (domain root)	Nó là d nh c a nhánh cây c a tên mi n. Nó xác d nh k t thúc c a domain (fully qualified domain names FQDNs).	d ng t i cu i c a tên ví nhu "example.microsoft.com."	Đon gi n nó ch là d u ch m (**.**) s
Tên mi n c p m t	Là hai ho c ba ký t xác d nh nu c/khu v c ho c các t ch c.	xác d nh tên s d ng trong ".com", xác d nh là t ch c thuong m i . (Top-level domain)
Tên mi n c p hai	Nó r t da d ng trên internet, Tên mi n c p nó có th là tên c a m t công ty, m t t ch c hay m t cá nhân .v.v. dang ký trên internet.	"microsoft.com.", là tên mi n c p hai dang ký là công ty Microsoft. (Second-level domain)
Tên mi n c p nh hon (Subdomain)	Chia nh thêm ra c a tên miên c p hai xu ng thu ng du c s d ng nhu chi nhánh, phong ban c a m t qu n lý tài li u ví d c a microsof co quan hay m t ch d nào dó.	"example.microsoft.com." là ph n

M t s chú ý khi d t tên mi n:

- Tên mi n nên d t gi i h n t t c p 3 d n c p 4 ho c c p 5 vì n u nhi u hon n a vi c qu n tr là khó khan.
- S d ng tên mi n là ph i duy nh t trong m ng internet
- Nên d t tên don gi n g i nh và tránh d t tên quá dài

2.2. Phân lo i DNS server và d ng b du li u gi a các DNS server

Có ba lo i DNS server sau:

Primary server

Ngu n xác th c thông tin chính th c cho các domain mà nó du c phép qu n lý qu n lý

Thông tin v tên mi n do nó du c phân c p qu n lý thì du c luu tr t i dây và sau dó có th du c chuy n sang cho các secondary server.

Các tên mi n do primary server qu n lý thì du c t o và s a d i t i primary server và sau dó du c c p nh p d n các secondary server.

Secondary server

DNS du c khuy n ngh nên s d ng ít nh t là hai DNS server d lu u cho m i m t zone. Primary DNS server qu n lý các zone và secondary server du c s d ng d luu tr d phòng cho zone cho primary server. Secondary DNS server du c khuy n ngh dùng nhung không nh t thi t ph i có. Secondary server du c phép qu n lý domain nhu ng d li u v domain không ph i t o t i secondary server mà nó du c l y v t primary server.

Secondary server có th cung c p ho t d ng ch d không có t i trên m ng. Khi lu ng truy v n zone tang cao t i primary server nó s chuy n b t t i sang secondary server ho c khi primary server b s c thì secondary s ho t d ng thay th cho d n khi primary server ho t d ng tr l i

Secondary server nên du c s d ng t i n i g n v i client d có th ph c v cho vi c truy v n tên mi n m t cách d dàng. Nhung không nên cài d t secondary server trên cùng m t subnet ho c cùng m t k t n i v i primary server. Vì di u dó s là m t gi i pháp t t d s d ng secondary server d d phòng cho primary server vì có th k t n i d n primary server b h ng thì cung không nh hu ng gì d n secondary server.

Primary server luôn luôn duy trì m t lu ng l n d li u và thu ng xuyên thay d i ho c thêm vào các zone. Do dó DNS server s d ng m t co ch cho phép chuy n các thông tin t primary server sang secondary server và luu gi nó trên dia. Các thông tin nh n d li u v các zone có th s d ng gi i pháp l y toàn b (full) ho c l y ph n thay d i (incremental)

Nhi u secondary DNS server s tang d n d nh ho t d ng c a m ng và vi c luu tr thông tin c a tên mi n m t cách d m b o nhu m t di u c n quan tâm là d li u c a zone du c chuy n trên m ng t primary server d n các secondary server s làm tang luu lu ng du ng truy n và yêu c u th i gian d d ng b d li u trên các secondary server.

Caching-only server

M c dù t t c các DNS server d u có kh nang luu tr d li u trên b nh cache c a máy d tr l i truy v n m t cách nhanh chóng. Caching-only server là lo i DNS server ch s d ng cho vi c truy v n, luu gi câu tr l i d a trên thông tin trên cache c a máy và cho k t qu truy v n. Chúng không h qu n lý m t domain nào và thông tin mà nó ch gi i h n nh ng gì du c luu trên cache c a server.

Khi nào thì s d ng caching-only server ?. Khi mà server b t d u ch y thì nó không có thông tin luu trong cache. Thông tin s du c c p nh p theo th i gian khi các client server truy v n d ch v DNS. N u b n s d ng k t n i m ng WAN t c d th p thì vi c s d ng caching-only DNS server là m t gi i pháp t t nó cho phép gi m luu lu ng thông tin truy v n trên du ng truy n.

Chú ý

Caching-only DNS server không chua zone nào và cung không quy n • qu n lý b t k domain nào. Nó s d ng b nh cache c a mình d luu các truy v n DNS c a client. Thông tin s du c luu trong cache d tr l i cho các truy v n d n c a client

Caching-only DNS có kh nang tr l i các truy v n nhu không qu n lý • ho c t o b t c zone ho c domain nào

DNS server nói trung du c khuy n ngh là du c c u hình s d ng • TCP/IP và dùng d a ch IP tinh .

Đ ng b d li u gi a các DNS server (zone transfer)

Truy n toàn b zone

B i vì t m quan tr ng c a h th ng DNS và vi c qu n lý các domain thu c zone ph i du c d m b o. Do dó thu ng m t zone thì thu ng du c d t trên hon m t DNS server d tránh l i khi truy v n tên mi n thu c zone dó. Nói cách khác n u ch có m t server qu n lý zone và khi server không tr l i truy v n thì các tên mi n trong zone dó s không du c tr l i và không còn t n t i trên Internet. Do dó ta c n có nhi u DNS server cùng qu n lý m t zone và có co ch d chuy n d li u c a các zone và d ng b nó t m t DNS server này d n các DNS server khác

Khi m t DNS server m i du c thêm vào m ng thì nó du c c u hình nhu m t secondary server m i cho m t zone dã t n t i. Nó s ti n hành nh n toàn b (full) zone t DNS server khác. Nhu DNS server th h d u tiên thu ng dùng gi i pháp l y toàn b co s d li u v zone khi có các thay d i trong zone.

Truy n ph n thay d i (Incremental zone)

Truy n ch nh ng thay d i (incremental zone transfer) c a zone du c miêu t chi ti t trong tiêu chu n RFC 1995. Nó là ph n b xung cho chu n sao chép DNS zone. Incremental transfer thì duoc h tr b i c DNS server là ngu n l y thông tin và DNS server nh n thông tin v zone, nó cung c p gi i pháp hi u qu cho vi c d ng b nhung thay d i ho c thêm b t zone.

Gi i pháp ban d u cho DNS yêu c u cho vi c thay d i d li u v zone là truy n toàn b d li u c a zone s d ng truy v n AXFR. V i vi c ch truy n các thay d i (incremental transfer) s s d ng truy v n (IXFR) du c s d ng thay th cho AXFR. Nó cho phép secondary server ch l y v nhu zone thay d i d d ng b d li u.

V i trao d i IXFR zone, thì s khác nhau gi a versions c a ngu n d li u và b n sao c a nó. N u c hai b n d u có cùng version (xác d nh b i s serial

trong khai báo t i ph n d u c a zone SOA "start of authority") thì vi c truy n d li u c a zone s không du c th c hi n.

N u s serial cho d li u ngu n l n hon s serial c a secondary server thì nó s th c hi n chuy n nh ng thay d i v i các b n ghi ngu n (Resource record - RR) c a zone. Đ truy v n IXFR th c hi n thành công và các thay d i du c g i thì t i DNS server ngu n c a zone ph i luu g i các ph n thay d i d s d ng truy n d n noi yêu c u c a truy v n IXFR. Incremental s cho phép luu lu ng truy n d li u là ít và th c hi n nhanh hon.

```
        SOA vdc-hn01.vnn.vn. postmaster.vnn.vn. (
      82802  ; serial number
         ; refresh every 30 mins
         ; retry every hour
         ; expire after 24 hours
         ; minimum TTL 2 hours

      NS     vdc-hn01.vnn.vn.
                                  NS     hcm-server1.vnn.vn.
```

Zone transfer s x y ra khi có nhung hành d ng sau x y ra:

- Khi quá trình làm m i c a zone k t thúc (refresh expire)
- Khi secondary server du c thông báo zone dã thay d i t i server ngu n qu n lý zone
- Khi d ch v DNS b t d u ch y t i secondary server
- T i secondary server yêu c u chuy n zone

Sau dây là các bu c yêu c u t secondary server d n DNS server ch a zone d yêu c u l y d li u v zone mà nó qu n lý .

1. Trong khi c u hình m i DNS server. Thì nó s g i truy v n yêu c u g i toàn b zone ("all zone" transfer (AXFR) request) d n DNS server qu n lý chính d li u c a zone
2. DNS server chính qu n lý d li u c a zone s tr l i và chuy n toàn b d li u v zone d n secondary (destination) server m i c u hình.

zone thì du c chuy n d n DNS server yêu c u can c vào version du c xác d nh b ng s Serial t i ph n khai báo (start of authority SOA). T i ph n SOA cung có ch a các thông s xác d nh th i gian làm m i l i zone ...

3. Khi th i gian làm m i (refresh interval) c a zone h t, thì DNS server nh n d li u s truy v n yêu c u làm m i zone t i DNS server chính ch a d li u zone.
4. DNS server chính qu n lý d li u s tr l i truy v n và g i l i d li u .

Tr l i s bao g m c s serial c a zone hi n t i t i DNS server chính.

5. DNS server nh n d li u v zone s ki m tra s serial trong tr l i và quy t d nh s làm th nào v i zone

N u giá tr c a s serial b ng v i s hi n t i t i DNS server nh n tr l i thì nó s k t lu n r ng s không c n chuy n d li u v zone d n. Và nó s thi t l p l i v i các thông s cu và th i gian d làm m i l i b t d u.

N u giá tr c a s serial t i DNS server chính l n hon giá tr hi n t i t i d li u DNS n i nh n thì nó k t lu n r ng zone c n ph i du c c p nh p và vi c chuy n zone là c n thi t.

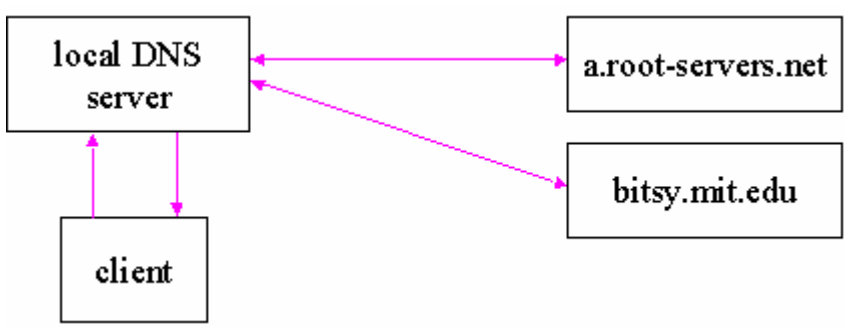
6. N u DNS server noi nh n k t lu n r ng zone c n ph i thay d i và nó s g i truy v n IXFR t i DNS server chính d yêu c u g i zone

7. DNS server chính s tr l i v i vi c g i nh ng thay d i c a zone ho c toàn b zone

N u DNS server chính có h tr vi c g i nh ng thay d i c a zone thì nó s g i nh ng ph n thay d i (incremental zone transfer (IXFR) of the zone.). N u nó không h tr thì nó s g i toàn b zone (full AXFR transfer of the zone)

3. Ho t d ng c a h th ng DNS

H th ng DNS ho t d ng d ng t i l p 4 c a mô hình OSI nó s d ng truy v n b ng giao th c UDP và m c d nh là s d ng c ng 53 d trao d i thông tin v tên mi n.



H at d ng c a h th ng DNS là chuy n d i tên mi n sang d a ch IP và ngu c l i. H th ng co s d li u c a DNS là h th ng co s d li u phân tán, các DNS server du c phân quy n qu n lý các tên mi n xác d nh và chúng liên k t v i nhau d cho phép ngu i dùng có th truy v n m t tên mi n b t k (có t n t i) t i b t c di m nào trên m ng m t các nhanh nh t

–

Nhu dã root mit.edu mi n

G ¹ T1 ¹ T2

trình b y các DNS server ph i bi t ít nh t m t cách d d n du c server và ngu c l i. Nhu trên hình v mu n xác d nh du c tên mi n thì root server ph i bi t DNS server nào du c phân quy n qu n lý tên mit.edu d chuy n truy v n d n.

Nói tóm l i t t c các DNS server d u du c k t n i m t cách logic v i nhau:

T t c các DNS server d u du c c u hình d bi t ít nh t m t cách d n root server

M t máy tính k t n i vào m ng ph i bi t làm th nào d liên l c v i ít nh t là m t DNS server

Ho t d ng c a DNS

Khi DNS client c n xác d nh cho m t tên mi n nó s truy v n DNS. Truy v n DNS và tr l i c a h th ng DNS cho client s d ng th t c UDP c ng 53, UPD ho t d ng m c th 3 (network) c a mô hình OSI, UDP là th t c phi k t n i (connectionless), tuong t nhu d ch v g i thu bình thu ng b n cho thu vào thùng thu và hy v ng có th chuy n d n noi b n c n g i t i.

M i m t message truy v n du c g i di t client bao g m ba ph n thông tin :

Tên c a mi n c n truy v n (tên d y d FQDN)

Xác d nh lo i b n ghi là mail, web ...

L p tên mi n (ph n này thu ng du c xác d nh là IN internet, dây không di sâu vào ph n này)

Ví d : tên mi n truy v n d y d nhu "hostname.example.microsoft.com.", và lo i truy v n là d a ch A. Client truy v n DNS h i "Có b n ghi d a ch A cho máy tính có tên là "hostname.example.microsoft.com" khi client nh n du c câu tr l i c a DNS server nó s xác d nh d a ch IP c a b n ghi A.

Có m t s gi i pháp d tr l i các truy v n DNS. Client có th t tr l i b ng cách s d ng các thông tin dã du c luu tr trong b nh cache c a nó t nh ng truy v n tru c dó. DNS server có th s d ng các thông tin du c luu tr trong cache c a nó d tr l i ho c DNS server có th h i m t DNS server khác l y thông tin dó d tr l i l i client.

Nói chung các bu c c a m t truy v n g m có hai ph n nhu sau:

- Truy v n s b t d u ngay t i client computer d xác d nh câu tr l i
- Khi ngay t i client không có câu tr l i, câu h i s du c chuy n d n DNS server d tìm câu tr l i.

T tìm câu tr l i truy v n

Bu c d u tiên c a quá trình s lý m t truy v n. Tên mi n s d ng m t chuong trình trên ngay máy tính truy v n d tìm câu tr l i cho truy v n. N u truy v n có câu tr l i thì quá trình truy v n k t thúc

Ngay t i máy tính truy v n thông tin du c l y t hai ngu n sau:

- Trong file HOSTS du c c u hình ngay t i máy tính. Các thông tin ánh x t tên mi n sang d a ch du c thi t l p file này du c s d ng d u tiên. Nó du c t i ngay lên b nh cache c a máy khi b t d u ch y DNS client.

Thông tin du c l y t các câu tr l i c a truy v n tru c dó. Theo th i gian các câu tr l i truy v n du c lu u gi trong b nh cache c a máy tính và nó du c s d ng khi có m t truy v n l p l i m t tên mi n tru c dó.

Truy v n DNS server

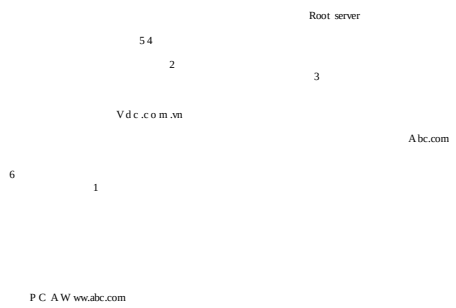
Khi DNS server nh n du c m t truy v n. Đ u tiên nó s ki m tra câu tr l i li u có ph i là thông tin c a b n ghi mà nó qu n lý trong các zone c a server. N u truy v n phù h p v i b n ghi mà nó qu n lý thì nó s s d ng thông tin dó d tr l i tr l i (authoritatively answer) và k t thúc truy v n.

N u không có thông tin v zone c a nó phù h p v i truy v n. Nó s ki m tra các thông tin du c lu u trong cache li u có các truy v n tuong tu nào tru c dó phù h p không n u có thông tin phù h p nó s s d ng thông tin dó d tr l i và k t thúc truy v n.

N u truy v n không tìm th y thông tin phù h p d tr l i t c cache và zone mà DNS server qu n lý thì truy v n s ti p t c. Nó s nh DNS server khác d tr l i truy v n d n khi tìm du c câu tr l i.

Các cách d DNS server liên l c v i nhau xác d nh câu tr l i

Tru ng h p Root server k t n i tr c ti p v i server tên mi n c n truy v n



Hình 4.1: Root server k t n i tr c ti p v i server tên mi n c n truy v n

Trong tru ng h p root server bi t du c DNS server qu n lý tên mi n c n truy v n. Thì các bu c c a truy v n s nhu sau:

Bu c 1 : PC A truy v n DNS server tên mi n vdc.com.vn. (là local name server) tên mi n www.abc.com.

Bu c 2 : DNS server tên mi n vdc.com.vn không qu n lý tên mi n www.abc.com do v y nó s chuy n truy v n lên root server.

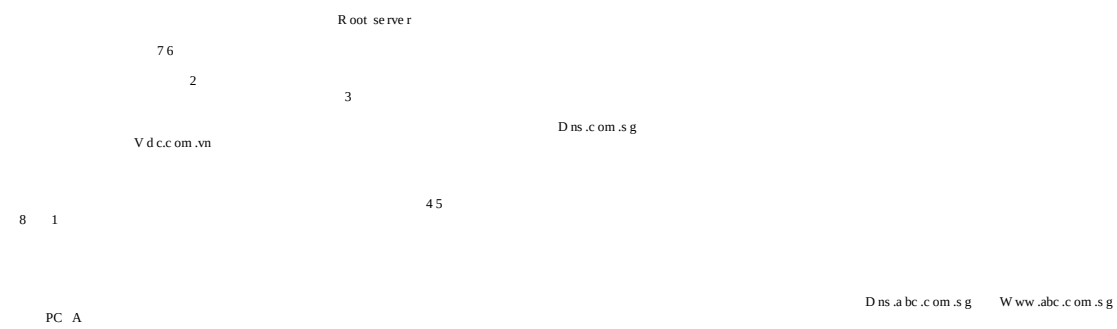
Bu c 3 : Root server s xác d nh du c r ng DNS server qu n lý tên mi n www.abc.com là server DNS.abc.com và nó s chuy n truy v n d n DNS server DNS.abc.com d tr l i

Bu c 4 : DNS server DNS.abc.com s xác d nh b n ghi www.abc.com và tr l i l i root server

Bu c 5 : Root server s chuy n câu tr l i l i cho server vdc.com.vn

Bu c 6 : DNS server vdc.com.vn s chuy n câu tr l i v cho PC A và t dó PC A có th k t n i d n PC B (qu n lý www.abc.com)

Tru ng h p root server không k t n i tr c ti p v i server tên mi n c n truy v n



Hình 4.2: Root server không k t n i tr c ti p v i server tên mi n c n truy v n

Trong tru ng h p không k t n i tr c ti p thì root server s h i server trung gian (phân l p theo hình cây) d xác d nh du c d n server tên mi n qu n lý tên mi n c n truy v n

Bu c 1 - PC A truy v n DNS server vdc.com.vn (local name server) tên mi n www.acb.com.sg.

Bu c 2 - DNS server vdc.com.vn không qu n lý tên mi n www.abc.com.sg v y nó s chuy n lên root server.

Bu c 3 - Root server s không xác d nh du c DNS server qu n lý tr c ti p tên mi n www.abc.com.sg nó s can c vào c u trúc c a h th ng tên mi n d chuy n d n DNS qu n lý c p cao hon c a tên mi n abc.com.sg dó là com.sg và nó xác d nh du c r ng DNS server DNS.com.sg qu n lý tên mi n com.sg.

Bu c 4 - DNS.com.sg sau dó s xác d nh du c r ng DNS server DNS.abc.com.sg có quy n qu n lý tên mi n www.abc.com.sg.

Bu c 5 - DNS.abc.com.sg s l y b n ghi xác d nh cho tên mi n www.abc.com.sg d tr l i DNS server DNS.com.sg.

Bu c 6 - DNS.com.sg s l i chuy n câu tr l i lên root server.

Bu c 7 - Root server s chuy n câu tr l i tr l i DNS server vdc.com.vn.

Bu c 8 - Và DNS server vdc.com.vn s tr l i v PC A câu tr l i và PC A dã k t n i du c d n host qu n lý tên mi n www.abc.com.sg.

Khi các truy v n l p di l p l i thì h th ng DNS có kh nang thi t l p chuy n quy n tr l i d n DNS trung gian mà không c n ph i qua root server và nó cho phép th i gian truy v n du c gi m di.

Ho t d ng c a DNS cache

Khi DNS server s lý các truy v n c a client và s d ng các truy v n l p l i. Nó s xác d nh và luu l i các thông tin quan tr ng c a tên mi n mà client truy v n. Thông tin dó s du c ghi l i trong b nh cache c a DNS server.

Cache luu gi thông tin là gi i pháp h u hi u tang t c d truy v n thông tin cho các truy v n thu ng xuyên c a các tên mi n hay du c s d ng và làm gi m luu lu ng thông tin truy v n trên m ng.

DNS server khi th c hi n các truy v n d quy cho client thì DNS server s t m th i luu trong cache b n ghi thông tin (resource record - RR) l y du c t DNS server lu u tr thông tin v truy v n dó. Sau dó m t client khác truy v n yêu c u thông tin c a dúng b n ghi dó thì nó s l y thông tin ban ghi (RR) luu trong cache d tr l i.

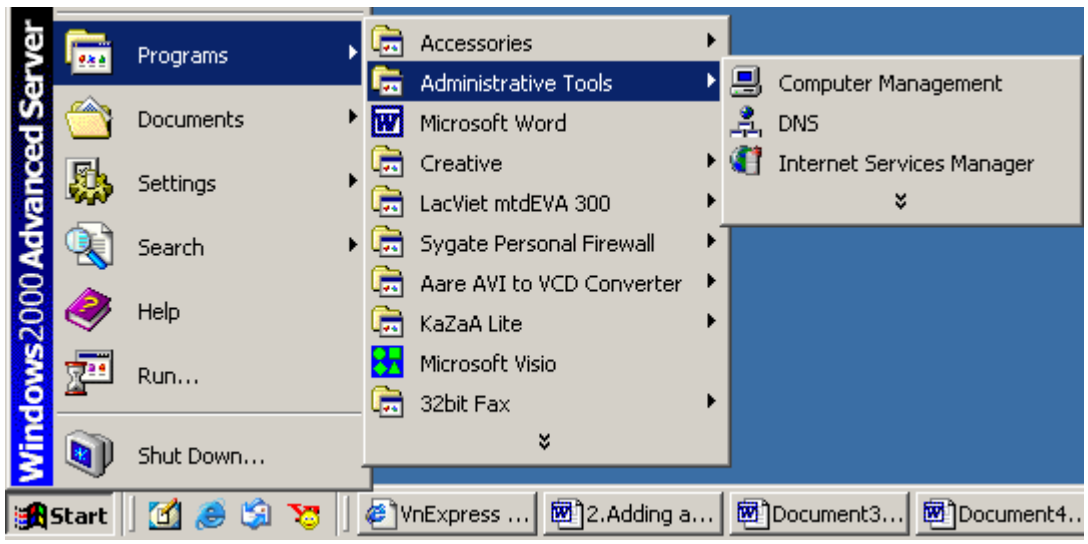
Khi thông tin du c luu trong cache. Thì các b n ghi RR du c ghi trong cache s du c cung c p th i gian s ng (TTL - Time-To-Live). Th i gian s ng c a m t b n ghi trong cache là th i gian mà nó t n t i trong cache và du c dùng d tr l i cho các truy v n c a client khi truy v n tên mi n trong b n ghi dó. Th i gian s ng (TTL) du c khai khi c u hình cho các zone. Giá tr m c d nh nh nh t c a th i gian s ng (Minimum TTL) là 3600 giây (1 gi) nhu giá tr này ta có th thay d i khi c u hình zone. H t th i gian s ng b n ghi s du c xóa kh i b nh cache.

4. Bài t p th c hành

Bài 1: Cài d t DNS Server cho Window 2000

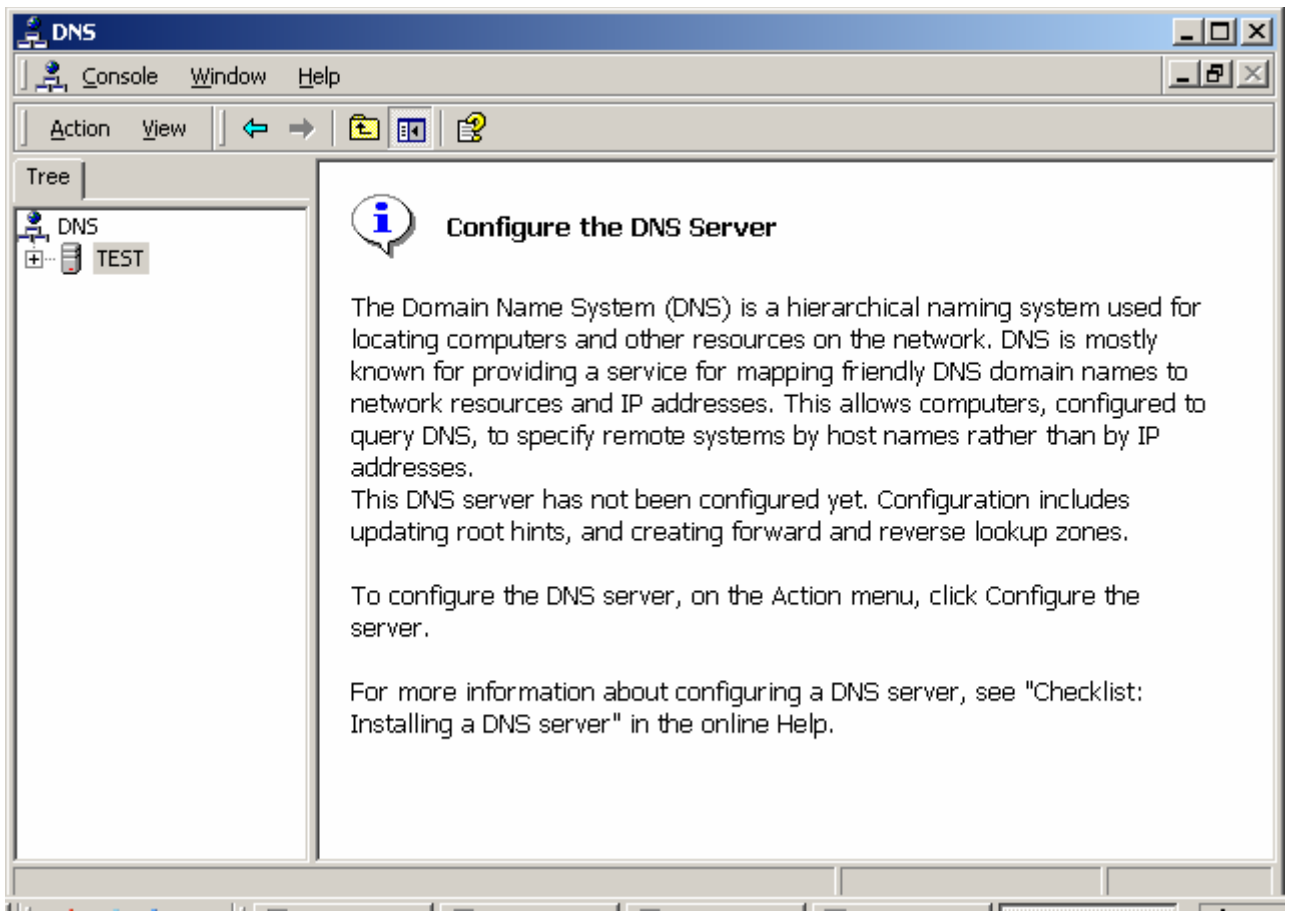
M c a s qu n lý DNS

Bu c 1 : M c a s qu n lý DNS



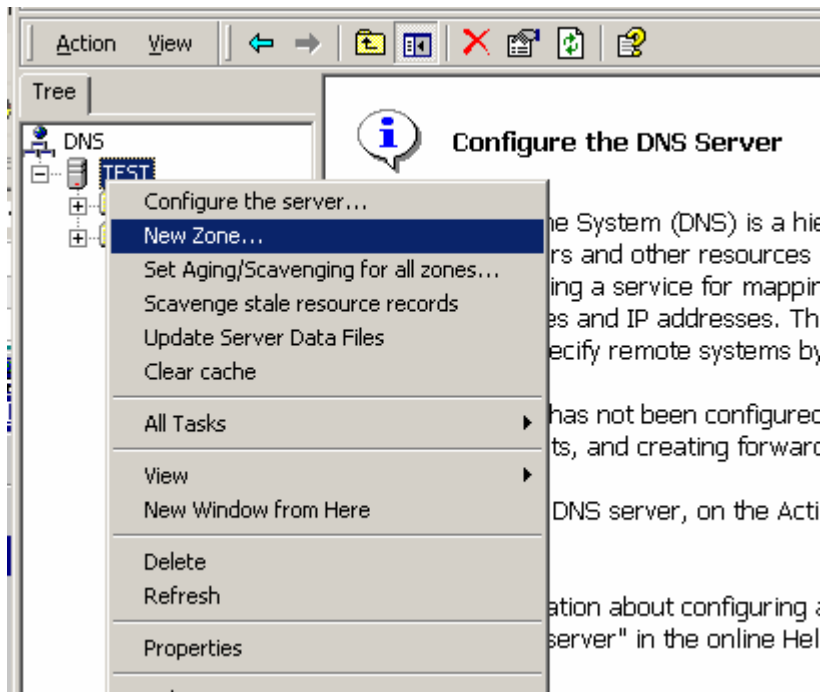
B m vào mune *Start* ch n *Programs* và sau dó là *"Administrative tools"* Ch n *"DNS Manager"*

Bu c 2: C a s qu n lý DNS server s xu t hi n

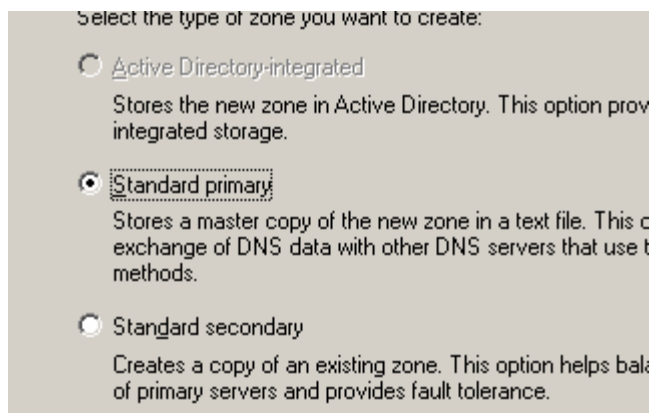


T i c a s qu n lý DNS server b n có th khai báo các tính nang c a DNS

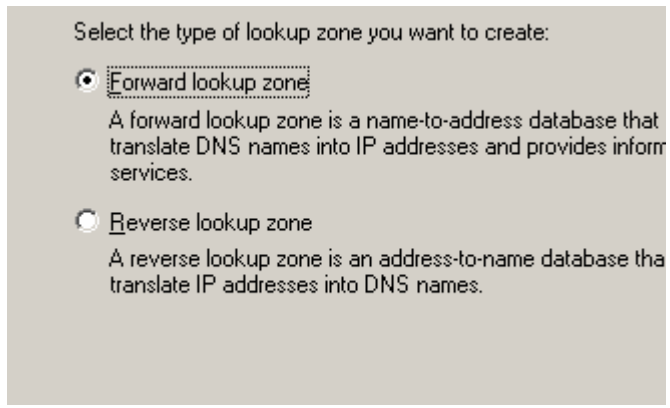
Thêm tru ng (zone)



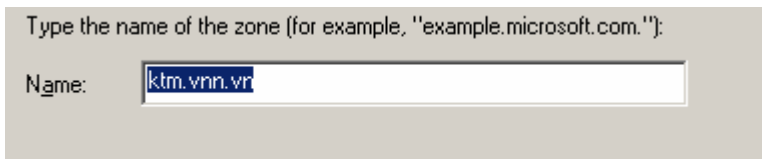
zone là tên mi n (domain name) mà server qu n lý. T i c a s qu n lý DNS t i ph n server qu n lý b m chu t ph i d hi n menu và ch n *"new zone* " nhu hình trên



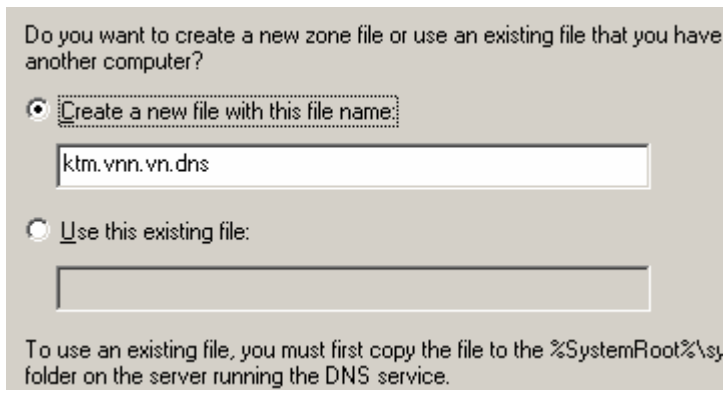
B m và *"new zone"* s hi n c a s cho phép ch n ki u d li u mà zone qu n lý. *Standard Primary* là lo i d li u c a zone du c khai báo và qu n lý ngay t i server. Còn *Stardard Secondary* là lo i zone mà d li u du c l y v t *Standard Primary* và d li u cung n m trên server . *Standard Primary* thu ng s d ng d d phòng cho các zone dã t n t i. B m *Next* d ti p t c



S xu t c a s nhu trên. *Forward lookup zone* là lo i zone qu n lý vi c chuy n d i t domain name sang d a ch IP. Còn ph n *Reverse lookup zone* qu n lý vi c chuy n d i t IP sang Domain name. B m *Next* ti p t c



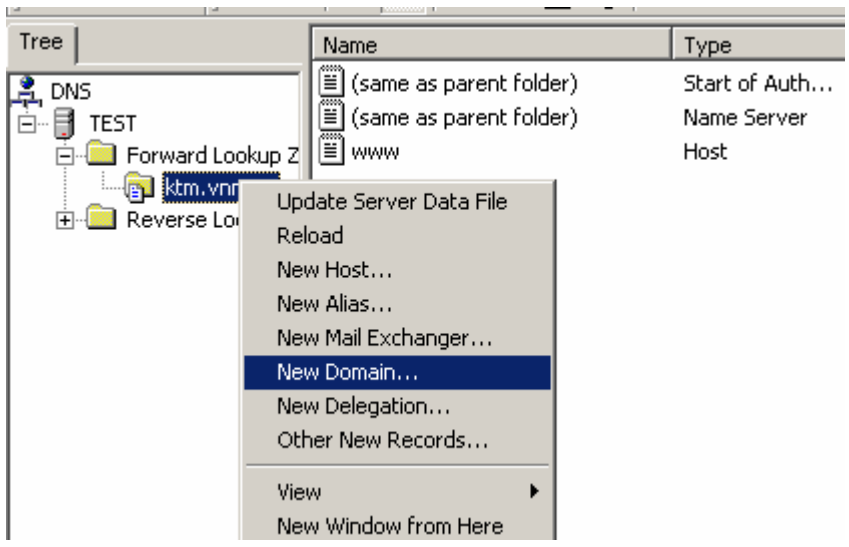
T i c a s này di n zone (domain name) mà s qu n lý. B m Next ti p t c



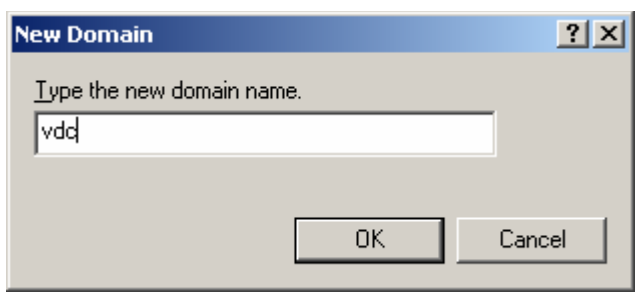
Đi n tên c a file d luu tr zone t i *"Create a new file with this file name"* ho c s d ng file có s n t i *"Use this existing file"* Và b m *Next* cho d n khi xu t hi n nút *finish* d k t thúc t o zone

Thêm tên miên (domain name)

T i c a s qu n lý domain ch n vào server và b m chu t ph i hi n lên menu và ch n *"New Domain..."* d di n m t domain m i.

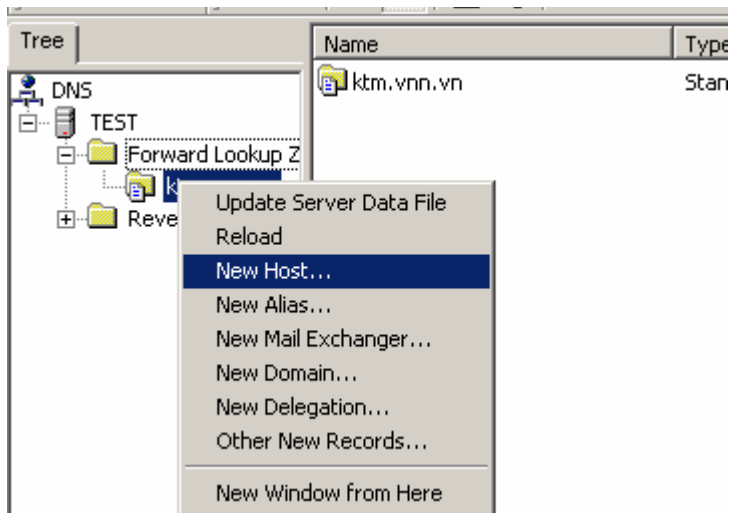


Sau khi b m vào *"New Domain"* nó s xu t hi n c a s cho phép b n di n tên mi n mà server du c phép qu n lý. Sau khi di n b m *"OK"* d k t thúc

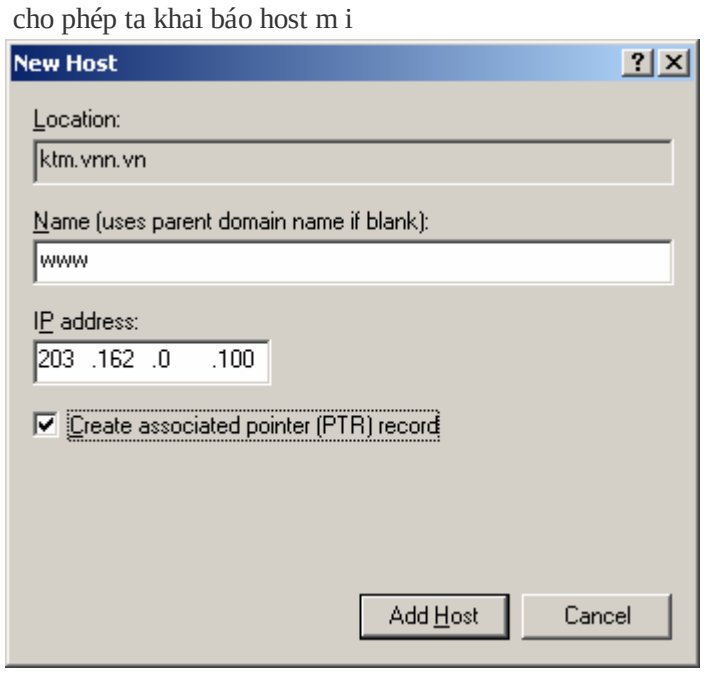


Thêm m t host m i

T i c a s qu n lý DNS ch n zone dã t o và b m chu t ph i ch n *"new host"*



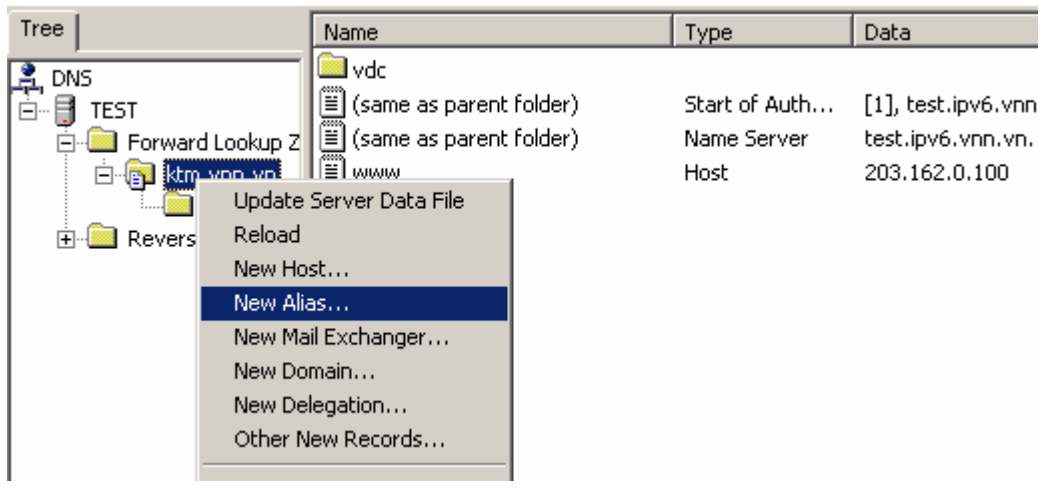
Xu t hi n c a s cho phép ta khai báo host m i



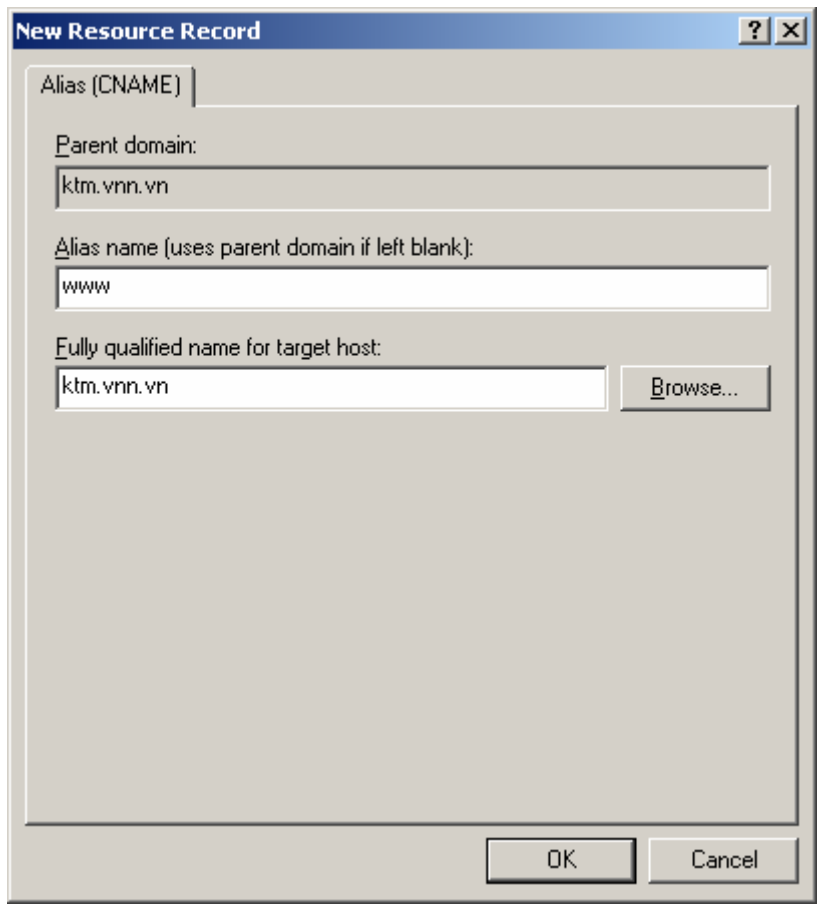
B n di n tên c a host mà mu n t o. Tên c a host s du c t d ng di n
thêm ph n domain d thành tên d y d c a host.
Ví d : nhu trên dây là vùng qu n lý zone (*location*) là ktm.vnn.vn. V y
khi b n di n *Name* là www và *IP address* là 203.162.0.100 thì s tuong ng
v i d nh nghia domain www.ktm.vnn.vn. tr d n d a ch IP 203.162.0.100
www.ktm.vnn.vn. IN A 203.162.0.100

T o m t b n ghi web (t o bí danh)

T i c a s qu n lý Domain và tên mi n v a t o và b m chu t ph i và
d t o m t CNAME d n m t host. ch n *"New Alias"*



B m và *"New Alias..."* s xu t hi n c a s cho phép khai báo Alias



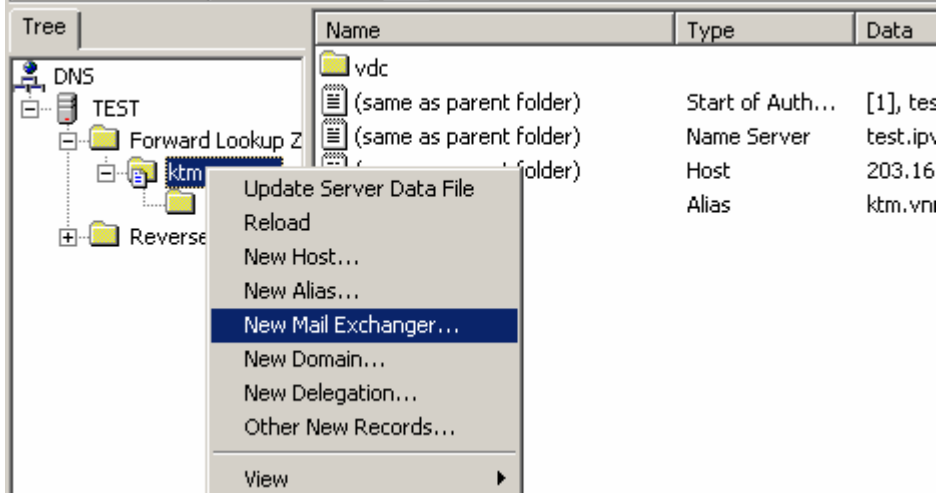
T i ph n *"Alias name"* di n tên t o alias và t i ph n *"Fully qualified for target host"* di n tên d y d c a m t host mà mu n t o bí danh (thu ng du c s d ng cho webhosting)

Ta s có Ví d : www.ktm.vnn.vn. IN CNAME ktm.vnn.vn.

T i c a s trang web www.ktm.vnn.vn d t trên server web có tên là ktm.vnn.vn.

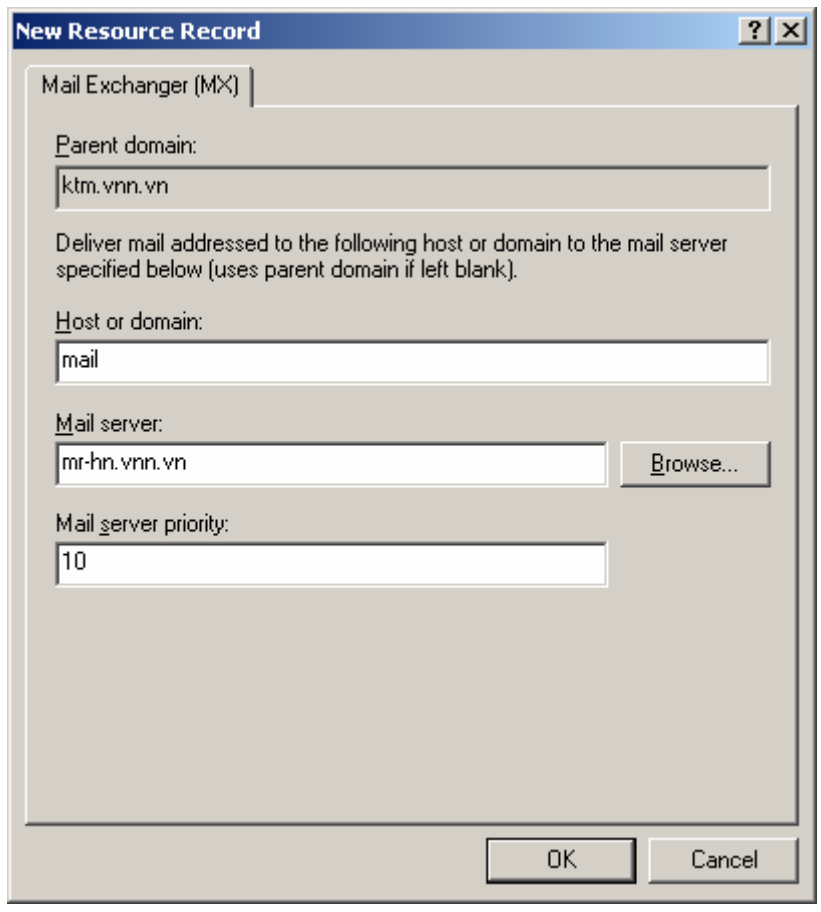
T o m t b n ghi thu di n t (MX)

ph i qu n lý DNS t i tên mi n mu n t o b n ghi MX b m chu t



t o

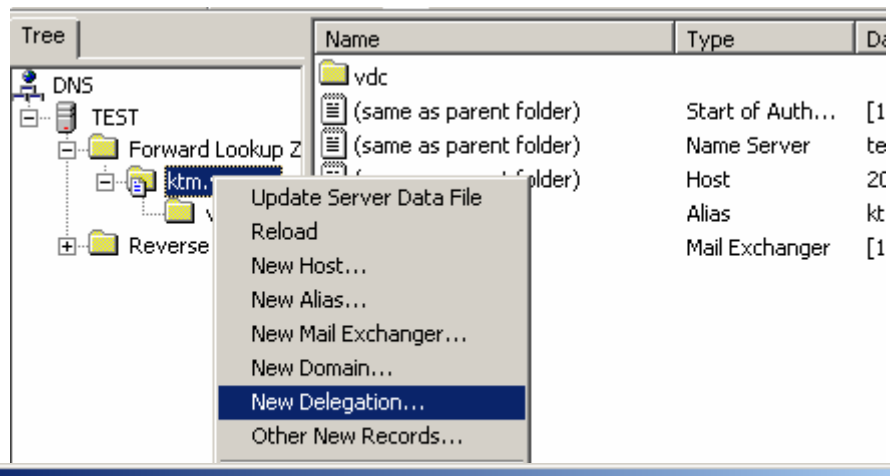
Sau khi b m vào *"New Mail Exchanger.."* s xu t hi n c a s cho phép các thông s cho b n ghi mx



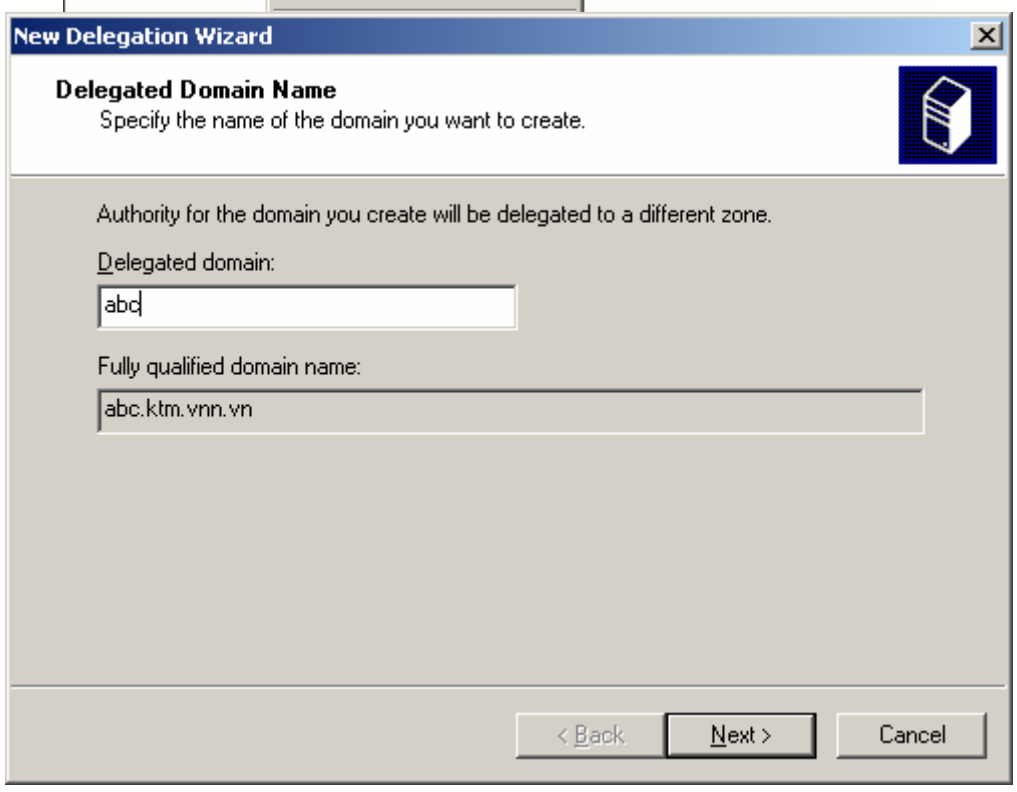
Đi n t i *"Host or domain"* di n tên ho c d tr ng tên này k t h p v i
ph n zone " *Parent domain"* d t o thành domain d y d c a b n ghi thu di n
t . T i *"Mail server"* di n tên c a server thu di n t và t i *"Mail server*
priority" di n m c d uu tiên c a server thu di n t (d l n càng nh m c uu
tiên càng cao)
Ví d trên hình ta có:
Ta có mail.ktm.vnn.vn IN MX 10 mr-hn.vnn.vn.
h p thu tên mi n thu di n t mail.ktm.vnn.vn. (ta có th t o du c các
hn.vnn.vn v i m c uu tiên là 10 abc@mail.ktm.vnn.vn) du c ch a t i server thu di n t mr-

Chuy n quy n qu n lý tên mi n (delegate)

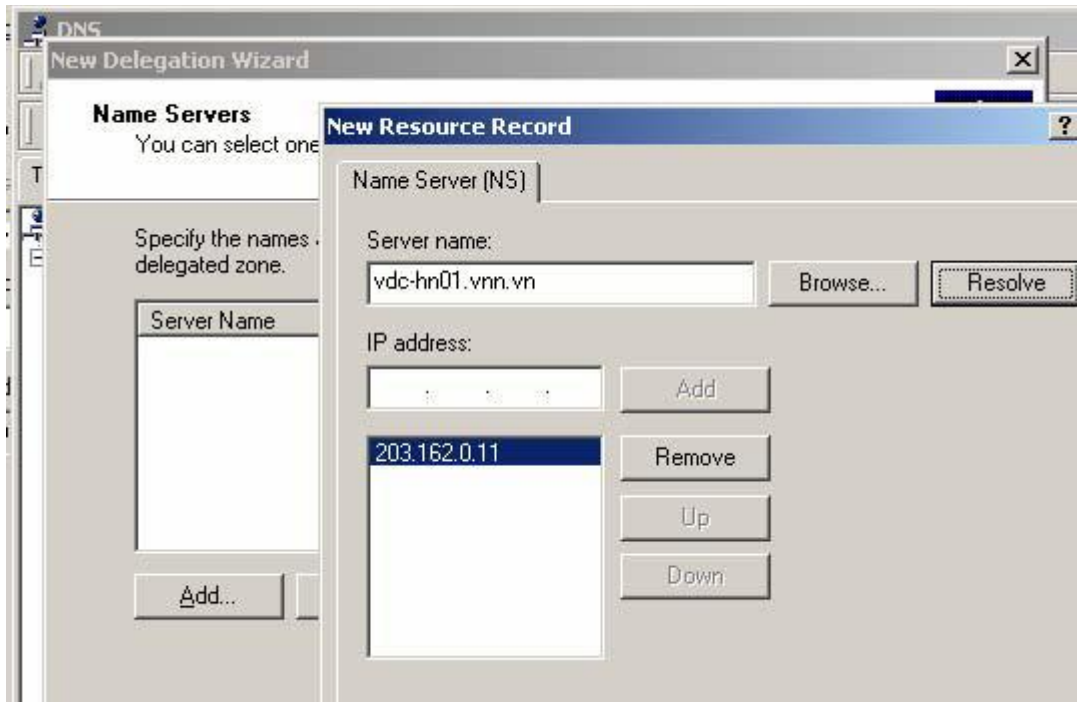
T i c a s qu n lý DNS t i domain mu n chuy n quy n qu n lý b m
chu t ph i.



qu n d hi n c a s cho phép chuy n quy n B m vào *"New Delegation..."* lý tên mi n



Đi n ph n domain mà b n mu n chuy n quy n qu n lý vào *"Delegated domain"*
Ví d dây di n là abc nghia là b n mu n chuy n quy n qu n lý domain abc.ktm.vnn.vn. B m *"Next"* d ti p t c



Hi n c a s di n vào *"Server name"* tên c a DNS server s du c phép qu n lý tên mi n abc.ktm.vnn.vn. B m *"Resolve"* d xác d nh d a ch IP c a
DNS server. Sau dó b m *"Ok"* d k t thúc.
Ví d abc.ktm.vnn.vn. IN NS vdc-hn01.vnn.vn.
Tuong ng tên mi n abc.ktm.vnn.vn. s du c chuy n quy n v DNS server vdc-hn01.vnn.vn d qu n lý.

Bài 2: Cài d t, c u hình DNS cho Linux

Hi n t i trên Internet r t nhi u nhà cung c p ph n m m mi n phí cho DNS. Nhung ph n m n s d ng DNS cho unix du c s d ng ph bi n hi n này là gói ph n m m cho DNS là Bind

Bind du c phát tri n b i m t t ch c phi l i nhu n là Internet Software Consortium ( ) và nó cung c p ph n m n bind mi n phí. www.isc.org

Hi n t i ph n m m bind có version là 9.2.2

Ph n m n Bind còn cung c p ti n ích nslookup là công c r t ti n l i cho vi c ki m tra tên mi n

Khai báo DNS cho client/server

V i client s d ng linux ho c unix ta vào file /etc/resolv.conf

Client ch l y thông tin v các domain

Client ch g i query t i server và nh n tr l i

C u hình DNS server

C u bình resolver nhu c a (DNS client)

C u hình Bind cho name server (named)

Xây d co s d li u cho DNS (cho các zone file)
C u hình cho DNS client /etc/resolv.conf

Các t khóa Miêu t

d a ch nameserver Đ a ch IP c a DNS server s g i truy v n d n d
l y thông tin v domain
domain *name* xác d nh domain m c d nh c a client

/etc/resolv.conf

```
# Do main na me resolver configuration file
#
do main nuts.co m
# try yourself first
na meserver 172.16.12.2
# try almond next
na meserver 172.16.12.1
# finally try filbert
na meserver 172.16.1.2
```

V i DNS client ch c n c u hình file resolv.conf

Cài d t DNS server.

Ta có th l y chuong trình cài d t bind cho DNS t i www.isc.org l y v
server

cd /usr/src
mkdir bind-9.xx
cd bind-9.xx

L y chuong trình cài d t DNS v dây bind-9.xx-src.tar.gz
gunzip bind-9.xx-src.tar.gz
tar xf bind-9.xx-src.tar
rm bind-9.xx-src.tar
cd src
make clean
make depend
make install
V y là ta dã cài xong ph n m n named cho DNS và các zone file s du c ch a trong /var/named còn file c u hình n m trong /usr/local/etc v y ta ph i t o và d t file c u hình và zone file vào các thu m c trên và ch y #/usr/local/sbin/named
V y là server dã s n sàng cho truy v n DNS

C u trúc file co s d li u (zone file)

Các file co s d li u zone du c ch làm hai lo i cho domain (có d ng db.domain ho c domain.root) và các domain ngu c (db.address) và nó n m trong thu m c /var/named c a DNS server.

Các d li u n m trong file co d li u du c g i là DNS resource record.

Các lo i resource record trong file d li u bao g m:

SOA record

Ch rõ domain c t qu n lý b i name server ghi sau tru ng SOA. Trong tru ng h p file db.domain

```
@  IN  SOA  vdc-hn01.vnn.vn. postmaster.vnn.vn. (
  1999082802  ; serial number
 1800  ; refresh every 30 mins
 3600  ; retry every hour
 86400  ; expire after 24 hours
  6400    ; minimum TTL 2 hours
 )
  IN      NS      vdc-hn01.vnn.vn.
                                                    IN      NS      hcm-server1.vnn.vn.
```

Khai báo zone ngu c db.203.162.0

```
@  IN  SOA  vdc-hn01.vnn.vn. postmaster.vnn.vn. (
    1999082301   ; Serial
       10800        ; Refresh after 3 hours
       3600         ; Retry after 1 hour
       604800       ; Expire after 1 week
       86400 )      ; Minimum TTL of 1 day
; name servers
       IN        NS       vdc-hn01.vnn.vn.
       IN        NS       hcm-server1.vnn.vn.
6  IN  PTR      ldap.vnn.vn.
7  IN  PTR      hanoi-server1.vnn.vn.
8  IN  PTR      hanoi-server2.vnn.vn.
                                          9  IN  PTR      mail.vnn.vn.
```

Trong m i zone ch khai m t tru ng SOA. Nhu ví d trên trong tru ng h p file db.com.vn, ch @ bi th các t t c các domain trong file qu n lý b i name server vdc-hn01.vnn.vn và d a ch mail c a admin m ng là postmaster.vnn.vn. Ngoài ra trong ph n SOA có 5 thông s c n qu n tâm sau:

Serial number : Thông s này có tác d ng v i t t c các d li u trong file. Khi secondary server yêu c u primary server các thông tin v domain mà nó qu n lý thì d u tiên nó s so sánh serial number c a secondary và primary server.

N u serial number c a secondary server nh hon c a primary server thì d li u c a domain s du c c p nh p l i cho secondary server t secondary server.
M i khi ta thay d i n i dung c a file db.domain thì ta c n ph i thay d i serial number và thu ng ta dánh serial number theo nguyên t c sau:
Serial number : yyyymmddtt
trong dó : yyyy là nam
mm là tháng
dd là ngày
tt là s l n s a d i trong ngày
Refresh : là chu k th i gian mà secondary server s sánh và c p nh p l i d li u c a nó v i primary server
Retry : n u secondary server không k t n i du c v i primary server thì c sau m t kho ng th i gian thì nó s k t n i l i
Expire : là kho ng th i gian mà domain s h t hi u l c n u secondary không k t n i du c v i primary server.
TTL (time to live) : khi m t server b t k yêu c u thông tin v d li u nào dó t primary server, và d li u dó s du c luu gi t i server dó và có hi u l c trong kho ng th i gian c a TTL. H t kho ng th i gian dó n u ti p t c c n thì nó l i ph i truy v n l i primary server.

Các b n ghi thu ng dùng trong DNS server
NS (name server) : B n ghi NS d xác d nh DNS server nào s qu n lý tên mi n. Nhu ví d trên là DNS server vdc-hn01.vnn.vn. và hcm-server1.vnn.vn.
A (address) : B n ghi d ng A cho tuong ng m t domain name v i m t d a ch IP. Ch cho phép khai báo m t b n ghi A cho m t d a ch IP.
Ví d :

Tên mi n Internet Lo i b n ghi Đ a ch
mr.vnn.vn. IN A 203.162.4.148
mr-hn.vnn.vn. IN A 203.162.0.24
mail.vnn.vn. IN A 203.162.0.9
fmail.vnn.vn. IN A 203.162.4.147
hot.vnn.vn. IN A 203.162.0.23
home.vnn.vn. IN A 203.162.0.12

www.vnn.vn. IN A 203.162.0.16

CNAME (canonical name) : là tên ph cho m t host có s n tên mi n d ng A. Nó thu ng du c s d ng cho các server web, ftp

Ví d : các domain có d ng CNAME du c ch t i các máy ch web

Tên mi n Internet	**Lo i b n ghi**	**Server**
www.gpc.com.vn.	IN CNAME	home.vnn.vn.
www.huonghai.com.vn.	IN CNAME	home.vnn.vn.
www.songmayip.com.vn.	IN CNAME	hot.vnn.vn.
www.covato2.com.vn .	IN CNAME	hot.vnn.vn.

MX (mail exchange): là tên ph cho các d ch v mail trên các máy ch dã có tên mi n d ng A. B n ghi này cho phép máy ch có th cung c p d ch v mail cho các domain khác nhau. Có th khai báo nhi u domain khác nhau cùng ch t i m t server ho c m t domain tr t i nhi u server khác nhau (s d ng backup) trong tru ng h p này giá tr u u tiên ph i d t khác nhau. V i s uu tiên càng nh thì m c d u u tiên càng cao.

Ví d

Tên mi n	**Lo i b n ghi**	**m c uu tiên**	**Server** *Internet*
mrvn.vnn.vn.	IN MX	10	mr.vnn.vn.
clipsalvn.vnn.vn.	IN MX	10	mr-hn.vnn.vn.
dbqnam.vnn.vn.	IN MX	10	mr-hn.vnn.vn.
thangloi.vnn.vn.	IN MX	50	mail.netnam.vn.
	IN MX	100	fallback.netnam.vn.

PTR (Pointer) : là b n ghi tuong ng d a ch IP v i domain. Các file d ng db.address. Ví d db.203.162.0 cho tuong ng v i các d a ch IP tuong ng v i m ng 203.162.0.xxx

Chú ý :

Tru c m i ph n khai báo domain thu ng có dòng

$ORIGIN *domain.*

Đ khai báo giá tr m c d nh c a domain. Cho phép trong ph n khai báo giá tr không ph i khai báo l p l i ph n domain m c d nh.

Ví d :

vdc.com.vn. IN A 203.162.0.49

ho c

```
 $ORIGIN com.vn.
 vdc  IN A 203.162.0.49
```

D u " **;** " du c s d ng làm ký hi u dòng chú thích, các ph n sau d u ";" d u không có tác d ng.

Đ nh nghi a c u hình (name.conf)

Khi các file co s d li u (zone file) thì c n ph i c u hình d DNS server d c các zone file dó. Đ i v i h th ng BIND co ch ch d n name server d c các zone file du c khai trong file named.conf nó du c n m trong thu m c /etc ho c /usr/local/etc

Ví d : khai báo file db trong file named.conf:

```
  ; khai báo cho zone file       domain .vn
zone "vn." in {
        type master;
        file "db.vn";
};
  ;khai báo cho zone file       domain .gov.vn
zone "gov.vn." in {
        type master;
        file "db.gov.vn";
};
  ;khai báo cho zone ngu c 203.162.0.xxx
zone "0.162.203.in-addr.arpa" in {
        type master;
        file "db.203.162.0";
};
  ;khai báo cho zone ngu c 203.162.1.xxx
 zone "1.162.203.in-addr.arpa" in {
        type master;
        file "db.203.162.1";
};
```

Chú ý: sau m i l n thay d i d li u d s a d i có tác d ng thì c n ph i làm d ng tác d DNS server c p nh p thay d i

```
%su
%password:
# ps -ef | grep named
    root 17413     1  5   Sep 07 ?       189:52 /usr/local/sbin/named
# kill -HUP 17413
```

Còn d ch y DNS server

#/usr/local/sbin/named

Hu ng d n s d ng nslookup
nslookup - là công c trên internet cho phép truy v n tên mi n và d a ch IP m t cách tuong tác.
C u trúc câu l nh
nslookup [-option ...] [host-to-find | - [server]]
Miêu t các l nh c a nslookup
server domain & lserver domain Change the default server to domain. Lserver uses the initial server to look up information about domain while server uses the current default server. If an authoritative answer can't be found, the names of servers that might have the answer are returned.
root Thay d i server m c d nh s làm root cho domain truy v n.
ls [option] domain [>> filename]
Hi n danh sách thông tin c a domain. M c d nh là hi n tên c a host và d a ch IP. Ta có th s d ng các l a ch n d hi n nhi u thông tin hon:
-t querytype hi n danh sách t t c b n ghi xác d nh b i lo i querytype
-a hi n danh sách các bí danh (aliaes) c a domain host (tuong t nhu -t CNAME)
-d hi n danh sách các b n ghi c a domain (tuong t nhu -t ANY)
-h hi n danh sách thông tin v CPU và thông tin v h di u hành c a domain. (tuong t nhu -t HINFO)
? hi n danh sách các câu l nh.
exit thoát kh i chuong trình.
set keyword[=value] câu l nh dùng d thay d i tr ng thái thông tin mà có nh hu ng d n truy v n. Các t khoá:
all cho phép hi n t t c các lo i b n ghi
[no]debug b t ch d tìm l i. Cho hi n r t nhi u lo i thông tin cho phép xác d nh l i truy v n d n domain. (m c d nh=nodebug, vi t t t = [no]deb)
[no]d2 B t ch d tìm l i m c cao hon. T t c các gói tin truy v n d u du c xu t hi n. (m c d nh=nod2)
domain=name Thay d i domain m c d nh vào tên. Khi truy v n m t tên nó s t d ng di n thêm domain vào sau.
port=value Chuy n c ng m c d nh s d ng cho TCP/UDP name server thành c ng du c thi t l p b i giá tr này (m c d nh= 53, vi t t t = po)
querytype=value
type=value Ch n lo i truy v n thông tin. Có các lo i sau:
A truy v n host (khai báo d a ch IP).

CNAME (canonical name) t o tên bí danh (thu ng dùng cho web)
HINFO truy v n lo i CPU và h di u hành c a server.
MINFO thông tin vê h p thu ho c mail list.
MX truy v n v mail exchanger.
NS truy v n v named zone.
PTR truy v n chuy n t d a ch IP sang domain.
SOA Thông tin v ngu i qu n lý v zone.
TXT Các thông tin khác.
UINFO Thông tin v ngu i dùng.
WKS H tr cho các d ch v khác.

Các lo i khác (**ANY** , **AXFR** , **MB** , **MD** , **MF** , **NULL**) du c miêu t chi ti t trong tiêu chu n **RFC-1035** . (M c d nh = A, vi t t t = q, ty)

[no]recurse Yêu c u name server truy v n t i m t server khác n u nó không có thông tin v domain c n tìm. (m c d nh = recurse, vi t t t = [no]rec)

retry=number Thi t l p s l n truy v n. Khi truy v n mà không nh n du c tr l i trong kho ng th i gian nh t d nh (thi t l p b ng l nh set timeout). Khi th i gian h t thì yêu c u truy v n s du c g i l i. Và thi t l p dây d di u khi n s l n s g i l i tru c khi t b truy v n. (M c d nh = 4, vi t t t = ret)

Đ i root server cho host **root=host**

timeout=number Thi t l p th i gian timeout cho m t quá trìn truy v n tính b ng giây. (m c d nh = 5 giây, vi t t t = ti)

[no]vc s d ng m t virtual circuit d g i yêu c u truy v n d n server. (m c d nh là = novc, vi t t t = [no]v)

Phân tích l i

N u truy v n lookup không thành công thì m t thông tin v l i s du c hi n ra. Và các l i có th là :

Timed out

Server không tr l i truy v n sau m t kho ng th i gian (kho ng th i gian có th thay d i b ng câu l nh *set timeout=value*) và and a certain number of retries (changed with set retry=value).

No response from server

Không có name server dang ch y t i server mà client ch d n.

No records

Server không có b n ghi tuong ng lo i mà truy v n cho host da t n t i. Lo i truy v n du c thi t l p b ng câu l nh " *set querytype"* .

Non-existent domain

Host ho c domain name không t n t i.

Connection refused

Network is unreachable
K t n i t i name server ho c finger server không th du c t i th i di m này.
L nh này thu ng xu t hi n v i các yêu c u c a câu l nh ls và finger.
Server failure
Name server tìm th y l i trong d li u v domain và không dtra ra câu tr
l i dúng.
Refused
Name server t ch i yêu c u tr l i.
Format error
Name server th y r ng các gói tin yêu c u không dúng d nh d ng. Nó có th là
l i c a chuong trình nslookup.
Ví d :
Truy v n DNS s Default Server: vdc01.vnn.vn
d ng b n ghi a cho

```
ch IP là > set querytype=a
203.162.0.12
> home.vnn.vn

Server: vdc-hn01.vnn.vn
Address: 203.162.0.11
Aliases: 11.0.162.203-in-addr.arpa
Name: home.vnn.vn
Address: 203.162.0.12
>
Truy v n b n ghi > set querytype=mx
mx (mail) cho
> hn.vnn.vn
domain hn.vnn.vn
Server: vdc-hn01.vnn.vn nó tr d n các host
mu13.vnn.vn có d a Address: 203.162.0.11
ch 203.162.0.55 và
Aliases: 11.0.162.203-in-addr.arpa
mu14.vnn.vn có d a
hn.vnn.vn MX preference = 20, mail exchanger = mu13.vnn.vn ch 203.162.0.64
hn.vnn.vn MX preference = 10, mail exchanger = mu14.vnn.vn
vnn.vn nameserver = vdc-hn01.vnn.vn
vnn.vn nameserver = hcm-server1.vnn.vn
mu13.vnn.vn internet address = 203.162.0.55
mu14.vnn.vn internet address = 203.162.0.64
vdc-hn01.vnn.vn internet address = 203.162.0.11
hcm-server1.vnn.vn internet address = 203.162.4.1
>
Truy v n lo i ns > set querytype=ns
```

Address: 203.162.0.11
domain
Aliases: 11.0.162.203-in-addr.arpa home.vnn.vn có d a

```
server nào qu n lý
Address:  203.162.0.11  s  cho ta m t danh
sách các nameserver  Aliases:  11.0.162.203.in-addr.arpa
qu n ly các domain
Non-authoritative answer:
có duôi vn
vn      nameserver = DNS-hcm01.vnnic.net.vn
vn      nameserver = ns.ripe.net
vn      nameserver = DNS1.vn
vn      nameserver = ns1.gip.net
vn      nameserver = ns2.gip.net
vn      nameserver = ns3.rip.net
vn      nameserver = DNS1.vnnic.net.vn
vn      nameserver = cheops.anu.edu.au
DNS-hcm01.vnnic.net.vn  internet address = 203.162.87.66
ns.ripe.net     AAAA IPv6 address = 2001:610:240:0:53:0:0:193
ns.ripe.net     internet address = 193.0.0.193
DNS1.vn internet address = 203.162.3.235
ns1.gip.net     internet address = 204.59.144.222
ns2.gip.net     internet address = 204.59.1.222
DNS1.vnnic.net.vn       internet address = 203.162.57.105
cheops.anu.edu.au       internet addres s = 150.203.224.24
>
```

(name server) cho > vn
domain vn do các
Server: vdc-hn01.vnn.vn

Chuong 5
D ch v truy c p t xa và d ch v Proxy

Chuong 5 cung c p các ki n th c co b n c a hai n i dung d ch v ph bi n trên m ng máy tính: d ch v truy c p t xa và d ch v proxy.

Vi c truy c p t xa là nhu c u thi t y u m r ng ph m vi ho t dong m ng c a các t ch c, công ty. N i dung truy c p t xa gi i thi u trong chuong này là truy c p qua m ng tho i PSTN. Đây là hình th c truy c p t xa cho t c d truy c p th p v a ph i nhung l i có tính ph bi n r ng rãi và d thi t l p nh t.

D ch v proxy trên m ng du c phát tri n cho các m c dích tang cu ng t c d truy nh p cho khách hàng trong m ng, ti t ki m du c tài nguyên m ng (d a ch IP) và d m b o du c an toàn cho m ng lu i khi b t bu c ph i cung c p truy nh p ra m ng ngoài hay ra ng Internet. Thi t l p d ch v proxy là công tác m i qu n tr h th ng m ng c n bi t vì các nhu c u k t n i liên m ng và k t n i Internet càng ngày càng tr nên không th thi u cho b t k t ch c, công ty nào.

Chuong 5 yêu c u các h c viên nên trang các ki n th c co b n v m ng di n tho i PSTN, ki n th c v các giao th c m ng WAN PPP, SLIP... các giao th c xác th c nhu RADIUS...Trong ph n proxy, h c viên c n làm quen v i khái ni m chuy n d i d a ch NAT, ho t d ng c a các giao th c TCP/IP.

M c 1: D ch v truy c p t xa (Remote Access)

1. Các khái ni m và các giao th c

1.1. T ng quan v d ch v truy c p t xa.

D ch v truy nh p t xa (Remote Access Service) cho phép ngu i dùng t xa có th truy c p t m t máy tính qua m t môi tru ng m truy n d n (ví d m ng di n tho i công c ng) d n m t m ng dùng riêng nhu th máy tính dó du c k t n i tr c ti p trong m ng dó. Ngu i dùng t xa k t n i t i m ng dó thông qua m t máy ch d ch v g i là máy ch truy c p (Access server). Khi dó ngui dùng t xa có th s d ng tài nguyên trên trên m ng nhu là m t máy tính k t n i tr c ti p trong m ng dó. D ch v truy nh p t xa cung cung c p kh nang t o l p m t k t n i WAN thông qua các m ng phuong ti n truy n d n giá thành th p nhu m ng tho i công c ng. D ch v truy c p t xa cung là c u n i d m t máy tính hay m t m ng máy tính thông qua nó du c n i d n Internet theo cách du c coi là h p lý v i chi phí không cao, phù h p v i các doanh ngh ep, t ch c qui mô v a và nh . Khi l a ch n và thi t k gi i pháp truy c p t xa, chúng ta c n thi t ph i quan tâm d n các yêu c u sau:

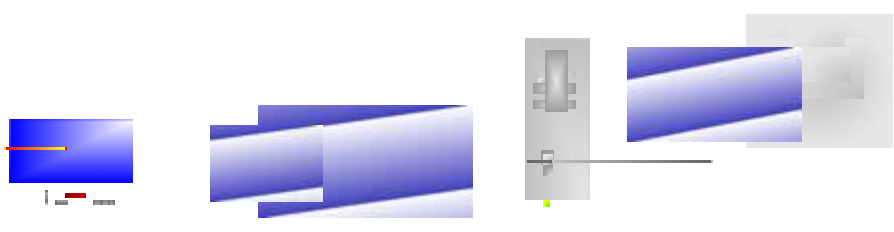
- S lu ng k t n i t i da có th d ph c v ngu i dùng t xa.
- Các ngu n tài nguyên mà ngu i dùng t xa mu n mu n truy c p.

- Công ngh , phuong th c và thông lu ng k t n i. Ví d , các k t n i có th s d ng modem thông qua m ng di n tho i công c ng PSTN, m ng s hoá tích h p các d ch v ISDN...
- Các phuong th c an toàn cho truy c p t xa, phuong th c xác th c ngu i dùng, phuong th c mã hoá d li u
- Các giao th c m ng s d ng d k t n i.

1.2.K t n i truy c p t xa và các giao th c s d ng trong truy c p t xa

K t n i truy c p t xa

Ti n trình truy c p t xa du c mô t nhu sau: ngu i dùng t xa t kh i m t k t n i t i máy ch truy c p. K t n i này du c t o l p b ng vi c s d ng m t giao th c truy c p t xa (ví d giao th c PPP-Point to Point Protocol). Máy ch truy c p xác th c ngu i dùng và ch p nh n k t n i cho t i khi k t thúc b i ngu i dùng ho c ngu i qu n tr h th ng. Máy ch truy c p dóng vai trò nhu m t gateway b ng vi c trao d i d li u gi a ngu i dùng t xa và m ng n i b . B ng vi c s d ng k t n i này, ngu i dùng t xa g i và nh n d li u t máy ch truy c p. D li u du c truy n trong các khuôn d ng du c d nh nghia b i các giao th c m ng (ví d giao th c TCP/IP) và sau dó du c dóng gói b i các giao th c truy c p t xa. T t c các d ch v và các ngu n tài nguyên trong m ng ngu i dùng t xa d u có th s d ng thông qua k t n i truy c p t xa này (hình 5.1)



Hình 5.1: K t n i truy c p t xa

Giao th c truy c p t xa

SLIP (Serial Line Interface Protocol), PPP và Microsoft RAS là các giao th c truy c p d t o l p k t n i du c s d ng trong truy c p t xa. SLIP là giao th c truy c p k t n i di m-di m và ch h tr s d ng v i giao th c IP, hi n nay h u nhu không còn du c s d ng. Microsoft RAS là giao th c riêng c a Microsoft h tr s d ng cùng v i các giao th c NetBIOS, NetBEUI và du c s d ng trong các phiên b cu c a Microsoft.

PPP giao th c truy c p k t n i di- di m v i khá nhi u tính nang uu vi t, là m t giao th c chu n du c h u h t các nhà cung c p h tr . RFC 1661 d nh nghia v PPP. Ch c nang co b n c a PPP là dóng gói thông tin giao th c l p m ng thông qua cácêh k t di m– di m.

Co ch làm vi c và v n hành c a PPP nhu sau: Đ thi t l p truy n thông, m i d u cu i c a liên k t PPP ph i g i các gói LCP (Link Control Protocol) d thi t l p và ki m tra liên k t d li u. Sau khi liên k t du c thi t l p v i các tính nang tùy ch n du c s p d t và th a thu n gi a hai d u liên k t, PPP g i các gói NCP (Network Control Protocol) d l a ch n và c u hình m t ho c nhi u giao th c l p m ng. M i l n m t giao th c l p m ng l a ch n dã du c c u hình, luu lu ng tm i giao th c l p m ng có th g i qua liên k t này. Liên k t t n t i cho d n khi các gói LCP ho c NCP dóng k t n i ho c d n khi m t s ki n bên ngoài x y ra (ch ng h n nhu m t s ki n h n gi hay m t s can thi p c a ngu i qu n tr). Nói cách khác là m t con du ng m d ng th i cho nhi u giao th c.

PPP kh i d u du c phát tri n trong môi tru ng m ng IP, tuy nhiên nó th c hi n các ch c nang d c l p v i các giao th c l p 3 và có th du c s d ng cho các giao th c l p m ng khác nhau. Nhu dã d PPP, dóng gói các th t c l p m ng dã du c c u hình d chuy n qua m t liên k t PPP. PPP có nhi u các tính nang khi n nó r t m m d o và linh ho t, bao g m:

- Ghép n i v i các giao th c l p m ng
- L p c u hình liên k t
- Ki m tra ch t lu ng liên k t
- Nh n th c
- Nén các thông tin ti p d u
- Phát hi n l i
- Th a thu n các thông s liên k t

PPP h tr các tính nang này thông qua vi c cung c p LCP có kh nang m r ng và NCP d th a thu n các thông s và các ch c nang tùy ch n gi a các d u cu i. Các giao th c, các tính nang tùy ch n, ki u xác th c ngu i dùng t t c d u du c truy n thông trong khi kh i t o liên k t gi a hai di m.

PPP có th ho t d ng trong b t k giao di n DTE/DCE nào, PPP có th ho t d ng ch d d ng b ho c không d ng b . Ngoài nh ng yêu c u khác c a các giao di n DTE/DCE, PPP không có h n ch nào v t c d truy n d n.

Trong h u h t các công ngh m ng WAN, mô hình l p du c dua ra d có nh ng di m liên h v i mô hình OSI và d di n t v n hành c a các công ngh c th PPP không khác nhi u so v i các công ngh khác. PPP cung có mô hình l p d d nh nghia các c u trúc và ch c nang (hình 5.2)

Hình 5.2: Mô hình l pPPP

Cung nhu h u h t các công ngh , PPP có c u trúc khung, c u trúc này cho phép dóng gói b t c giao th c l p 3 nào. Du i dây là c u trúc khung PPP (hình 5.3)

Hình 5.3: C u trúc khung PPP

Các tru ng c a khung PPP nhu sau:

C : d dài 1 byte s d ng d ch ra r ng dây là di m b t d u hay k t thúc m t khung, tru ng này là m t dãy bit 01111111

Đ a ch : d dài 1 byte bao g m dãy bit 11111111, là d a ch qu ng bá chu n. PPP không gán t ng d a ch riêng.

Giao th c: d dài 2 byte, nh n d ng giao th c dóng gói. Giá tr c p nh t c a tru ng này du c ch ra trong RFC 1700

D li u: có d dài thay d i, có th 0 ho c nhi u byte là các d li u cho ki u giao th c c th d oc ch ra trong tru ng giao th c. Ph n cu i cùng c a tru ng d li u du c nh n bi t b ng cách d t c và ti p sau nó là 2 byte FCS. Giá tr ng m d nh c a tru ng này là 1500 byte. Tuy v y giá tr l n hon có th du c s d ng d tang d dài cho tru ng d lli u.

FCS: thu ng là 2 byte, có th s d ng 4 byte FCS d tang kh nang phát hi n l i.

LCP có th th a thu n d ch p nh n s thay d i c u trúc khung PPP chu n gi a hai d u cu i c a liên k t. Các khung dã thay d i luôn luôn d nh n bi t hon so v i các khung chu n. LCP cung c p phuong pháp d thi t l p, c u hình, duy trì và k t thúc m t k t n i di-m-i m. LCP th c hi n các ch c nang này thông qua b n giai do n. Ð u tiên, LCP th c hi n thi t l p và th a thu n c u hình gi a liên k t di m di m. Tru c khi b t k don v d li u l p m ng nào du c chuy n, LCP d u tiên ph i m k t n i và th a thu n các thông s thi t l p. Quá trình này du c hoàn thành khi m t khung nh n bi t c u hình dã du g i và nh n. Ti p theo, LCP xác d nh ch t lu ng liên k t. Liên k t du c ki m tra d xác d nh xem li u ch t lu ng có d d kh i t o các giao th c l p m ng không. Vi c truy n d n c a giao th c l p m ng b dình l i cho d n khi giai do n này hoàn t t. LCP cho phép dây là m t tùy ch n sau giai do n thi t l p và th a thu n c u hình c a liên k t. Sau dó LCP th c hi n th a thu n c u hình giao th c l p m ng. Các giao th c l p m ng có th du c c u hình riêng r b i NCP thích h p và du c kh i t o hay d bovào t k th i di m nào. Cu i cùng, LCP k t thúc liên k t khi xu t hi n yêu c u t ngu i dùng ho c theo các b d nh th i gian, do l i truy n d n hay do các y u t v t lý khác.

Ba ki u khung LCP du c s d ng d hoàn thành các công vi c d i v i t ng giai do n: khung thi t l p liên k t du c s d ng d thi t l p và c u hình m t liên k t, khung k t thúc liên k t du c s d ng d k t thúc m t liên k t, khung duy trì liên k t du c s d ng d qu n lý và g r i liên k t.

Các giao th c m ng s d ng trong truy p t xa.

Khi tri n khai d ch v truy c p t xa, các giao th c m ng thu ng du c s d ng là giao th c TCP/IP, IPX, NETBEUI.

TCP/IP là m t b giao th c g m có giao th c TCP và giao th c IP cùng làm vi c v i nhau d cung c p phuong ti n truy n thông trên m ng. TCP/IP là m t b giao th c co b n, làm n n t ng cho truy n thông liên m ng là b giao th c m ng du c s d ng ph bi n nh t hi n nay. V i kh nang d nh tuy n và m r ng, TCP/IP h tr m t cách linh ho t và phù h p cho các t t c các m ng.

IPX (Internet Packet Exchange) là giao th c du c s d ng cho các m ng Novell NetWare. IPX là m t giao th c có kh nang d nh tuy n và thu ng du c s d ng v i các h th ng m ng tru c dây.

NetBEUI là giao th c dùng cho m ng c c b LAN c a Microsoft. NetBEUI cho ta nhi u ti n ích và h u nhu không ph i làm gì nhi u v i NetBEUI. Thông qua NetBEUI ta có th truy c p t t c các tài nguyên trên m ng. NETBEUI là m t giao th c không có kh nang d nh tuy n và ch thích h p v i mô hình m ng nh , don gi

1.3. Modem và các phuong th c k t n i v t lý.

1. Modem.

Máy tính làm vi c v i d li u d ng s , khi truy n thông trên môi tru ng truy n d n v i các d ng tín hi u khác (ví d nhu v i m ng di n tho i công c ng làm vi c v i các tín hi u tuong t) ta c n thi tt b d chuy n d i tín hi u s thành tín hi u thích nghi v i môi tru ng truy n d n, thi t b dó g i là Modem (Modulator/demodulator). Nhu v y Modem là m t thi t b chuy n d i tín hi u s sang d ng tín hi u phù h p v i môi tru ng truy n d n và ngu c lai. Hình du i là m t k t n i s d ng modem qua m ng di n tho i di n hình (hình 5.4).

Hình 5.4: K t n i s d ng modem qua m ng di n tho i di n hình

Các modem s d ng các phuong pháp nén d li u nh m m c dích tang t c d truy n d li uHi u su t nén d li u ph thu c vào d li u, có hai giao th c nén thu ng du c s d ng là V.42bis và MNP 5. hi u su t nén c a V.42bis và MNP 5 có th thay d i t 0 d n 400 % hay cao hon ph thu c vào d li u t nhiên

Chu n modem V.90 cho phép các modem nh n d li u v i t c d 56 Kbps qua m ng di n tho i công c ng (PSTN). V.90 xem m ng PSTN nhu là m t m ng s và chúng s mã hóa dòng d li u xu ng theo k thu t s thay vì di u ch d g i di nhu các chu n di u ch tru c dây. Trong khi dó theo hu ng lên t khách hàng d n nhà cung c p d ch v dòng d li u lên v n du c di u ch theo các nguyên t c thông thu ng và t c d t i ta d t du c là 33.6 Kbps, giao th c hu ng lên này d a trên chu n V.34

S khác nhau gi a tín hi u s ban d u v i tín hi u du c ph c h i t i d u nh n g i là t p âm lu ng t hóa (nhi u lu ng t), chính t p âm này dã h n ch t c d truy n d li u. Gi a các modem d u cu i có m t c u trúc h t ng cho vi c k t n i dó là m ng tho i công c ng. Các chu n modem tru c dây d u gi s c hai d u c a k t n i gi ng nhau là có m t k t n i tuong t vào m ng di n tho i công c ng, công ngh V.90 dã l i d ng uu di m c a t ch c m ng mà m t d u k t n i gi a h th ng truy c p t xa và m ng tho i công c ng là d ng s hoàn toàn còn d ia k v n du c k t n i vào m ng PSTN theo d ng tuong t nh dó t n d ng du c các uu di m c a liên k t s t c d cao, vì ch có quá trình bi n d i A/D m i gây ra t p âm v i các k t n i s thì không có lu ng t hóa do dó nhi u lu ng t r t ít trong c u trúc m ng này.

Đ nh lu t shanon nói r ng du ng dây di n tho i tuong t h n ch t c d truy n d li u kho ng 35 kbps mà không xem xét d n m t th c t là m t d u c a truy n thông dã du c s hóa nên gi m nh lu ng t p âm gây ra s ch m tr trong vi c truy n d li u. Nhu lu ng t dã gi i h n chu n truy n thông V.34 t c d 33.6 kbps, nhung nhi u lu ng t ch có nh hu ng khi chuy n d i tuong t - s mà không có nh hu ng khi chuy n d i tuong t - tuong t và dây chính là chìa khóa cho công ngh V.90 d ng th i cung gi i thích c vì sao t c d download có th d t du c 56 kbps còn khi upload t c d ch d t 33.6 kbps. D li u chuy n di t modem s V.90 qua m ng PSTN là m t dòng s v i t c d 64 Kbps nhung t i sao V.90 ch h tr t c d d n 56 Kbps, vì các lí do sau: Th nh t m c dù nhi u lu ng t dã du c b qua nhung nhi u m c th p do b chuy n d i s - tuong t là không tuy n tính, do nh hu ng c a vòng loop n i h t. Lý do th hai là các t ch c qu c t có qui d nh ch t ch v m c nang lu ng tín hi u nh m h n ch nhi u xuyên âm gi a các dây d n d t g n k nhau, và qui d nh này tuong ng v i m c nang lu ng t i da trên du ng dây di n tho i tuong ng là 56 kbps

Đ xây d ng m t h th ng truy c p t xa qua m ng tho i công c ng d t du c t c d 56 kbps gi a hai d u k i c n h i d ba di u ki n sau: th nh t, m t d u c a k t n i (thu ng là d u trung tâm m ng) ph i là k t n i s t i m ng PSTN. Th hai, chu n modem V.90 h tr t i hai d u cu i c a n i k t. Th ba, ch có m t chuy n d i duy nh t - tuong t trên mng tho i gi a hai d u c a k t n i

Khi v n hành modem V.90 tham dò du ng tho i d quy t d nh xem nó s làm vi c theo tiêu chu n nào, n u phát hi n ra b t k m t chuy n d i s tuong t nào thì nó don gi n ch làm vi c chu n V.34 và cung c g ng k t n i chu n này n u modem d u xa không h tr chu n V.90.

2.Các phuong th c k t n i v t lý co b n:

M t phuong th c ph bi n và s du c dùng nhi u dó là k t n i qua m ng di n tho i công c ng (PSTN). Máy tính du c n i qua m t modem l p d t bên trong (Internal modem) ho c qua c ng truy n s li u n i ti p COM port. T c d truy n t i da hi n nay có th có du c b ng phuong th c này có th lên d n 56 Kbps cho chi u l y d li u xu ng và 33,6Kbps cho chi u truy n d li u hu ng lên v i các chu n di u ch n hi u ph bi n V90, K56Flex, X2. Ta cung có th s d ng modem có yêu c u v h t ng co s th p hon v i chu n di u ch V.24, V.32Bis, V.32...

Phuo ng th c th hai là s d ng m ng truy n s li u s da d ch v ISDN. Phuong th c này dòi h i chi phí cao hon và ngày càng du c ph bi n r ng rãi. Ta có du c khá nhi u các l i ích t vi c s d ng m ng ISDN mà m t trong s dó là t c d . Ta có th s d ng các l a ch n ISDN 2B+D BRI (2x64Kbps d li u + 16Kbps dùng cho di u khi n) ho c 23B+D PRI (23x64Kbps+64Kbps) thông qua thi t b TA (Terminal Adapter) hay các card ISDN.

M t phuong th c khác nhung ít du c s d ng là qua m ng truy n s li u X.25, t c d không cao nhung an toàn và b o m t cao hon. Yêu c u cho

ngu i s d ng trong tru ng h p này là ph i có s d ng truy nh s li u X.25 ho c m t thi t b du c g i là PAD (Packet Asssembled Disassembled). Ta cung có th s d ng các k t n i tr c ti p qua cáp modem, phuong th c này cho ta các k t n i t c d cao nhung ph i thông qua các modem truy n s li u có giá thành cao.

2. An toàn trong truy c p t xa

2.1. Các phuong th c xác th c k t n i

1.Qúa trình nh n th c.

Ti n trình nh n th c v i các giao th c xác th c du c th c hi n khi ngu i dùng t xa có các yêu c u xác th c t i máy ch truy c p, m t thi t a thu gi a ngu i dùng t xa và máy ch truy c p d xác d nh phuong th c xác th c s s d ng. N u không có phuong th c xác th c nào du c s d ng, ti n trình PPP s kh i t o k t n i gi a hai di m ngay l p t c

Phuong th c xác th c có th du c s d ng các hình th c ki m tra co s d li u d a phuong (luu tr các thông tin v username và password ngay trên máy ch truy c p) xem các thông tin v username và password du c g i d n có trùng v i trong co s d li u hay không. Ho c là g i các yêu c u xác th c t i m t server khác d xác th c thu ng s d ng là các RADIUS server (s du c trình bày ph n sau)

Sau khi ki m tra các thông tin g i tr l i t co s d li u d a phuong ho c t RADIUS server. N u h p l , ti n trình PPP s kh i t o m t k t n i không yêu c u k t n i c a ngu i dùng s b t ch i. (hình 5.5)

.

Hình 5.5: Xác th c k t n i

2.Giao th c xác th c PAP

PAP là m t phuong th c xác th c k t n i không an toàn, n u s d ng m t chuong trình phân tích gói tin trên du ngrkitta có th nhìn th y các thông tin v username và password du i d ng d c du c. Đi u này có nghia là các thông tin g i di t ngu i dùng t xa t i máy ch truy c p không du c mã hóa mà du c g i di du i d ng d c du c dó chính là lý do PAP không an toàn. Hình du i mô t quá trình xác th c PAP, sau khi th a thu n giao th c xác th c PAP trên liên k t PPP gi a các d u cu i, ngu i dùng t xa g i thông tin (username:nntrong, password:ras123) t i máy ch truy c p t xa, sau khi ki m tra các thông tin này ung co s d li u c a mình, máy ch truy c p t ra s quy t d nh xem li u yêu c u k t n i có du c th c hi n hay không (hình 5.6)

Hình 5.6: Giao th c xác th c PAP

3.Giao th c xác th c CHAP

Sau khi th a thu n giao th c xác th c CHAP trên liên k t PPP gi a các d u cu i, máy ch truy c p g i m t "challenge" t i ngu i dùng t xa. Ngu i dùng t xa phúc dáp l i m t giá tr du c tính toán s d ng ti n trình x lý m t chi u (hash). máy ch truy c p ki m tra và so sánh thông tin phúc dáp v i giá tr hash mà t nó tính du c. N u các giá tr này b ng nhau vi c xác th c là thành công, ngu c l i k t n i s b h y b . Nhu v y CHAP cung c p co ch an toàn thông qua vi c s d ng giá tr challenge thay d i, duy nh t và không th doán du c. Các thông tin v username và password không du c g i di du i d ng d c du c trên m ng và do dó ch ng l i các truy c p trái phép b ng hình th c l y tr m password trên du ng k t n i (hình 5.7).

Remote

1 J X \ M Q 9 Q 7 [UQ Je Q J 7 &-1%V YBQP

Hình 5.7: Giao th c xác th c CHAP

4.Giao th c xác th c m r ng EAP

Ngoài các giao th c ki m tra tính xác th c co b n PAP, CHAP, trong Microsoft Windows 2000 h tr thêm m t s giao th c cho ta các kh nang nâng cao d an toàn, b o m t và da truy nh p dó là giao th c xác th c m r ng EAP (Extensible Authentication Protocol).

EAP cho phép có du c m t co c u xác th c tu ý d công nh n m t k t n i g i vào. Ngu i s d ng và máy ch truy nh p t xa s trao d i d tìm ra giao th c chính xác du c s d ng. EAP h tr các hình th c sau:

- S d ng các card v t lý dùng d cung c p m t kh u. Các card này dùng m t s các phuong th c xác th c khác nhau nhu s d ng các do n mã thay d i theo m i lu t s d ng.
- H tr MD5-CHAP, giao th c mã hoá tên ngu i s d ng, m t kh u s d ng thu ttoán mã hoá MD5 (Message Digest 5).
- H tr s d ng cho các th thông minh. Th thông minh bao g m th và thi t b d c th . Các thông tin xác th c v cá nhân ngu i dùng du c ghi l i trong các th này.
- Các nhà phát tri n ph n m m d c l p s gdgiao di n chuong trình ng d ng EAP có th phát tri n các module chuong trình cho các công ngh á d ng cho th nh n d ng, th thông minh, các ph n c ng sinh h c nhu nh n d ng võng m c, các h th ng s d ng m t kh u m t l n.

2.2. Các phuong th c mã hóa d li u

D ch v truy c p t xa cung c p co ch an toàn b ng vi c mã hóa và gi i mã d li u truy n gi a ngu i dùng truy c p t xa và máy ch truy c p.

Có hai phuo ng th c mã hóa d li u thu ng du c s d ng dó là mã hóa d i x ng và mã hóa phi d i x ng.

Phuong th c mã hoá d i x ng, thông tin d ng d c du c, du c mã hoá s d ng khóa bí m t (khoá mà ch có ngu i mã hoá m i bi t du c) t o thành thông tin dã du c mã hoá. phía nh n, thông tin mã hoá du c gi i mã cùng v i khóa bí m t thành d ng g c ban d u. Di m chú ý c a phuong pháp mã hoá này là vi c s d ng khoá bí m t cho c quá trình mã hoá và quá trình gi i mã. Do dó, nhu c di m chính c a phuong th c này là c n có quá trình trao d i khoá bí m t, d n d n tình tr ng d b l khoá bí m t.

Phuong pháp mã hoá phi d i x ng, d kh c ph c di m h n ch c a phuong pháp mã hoá d i x ng là quá trình trao d i khoá bí m t, ngu i ta dã s d ng phuong pháp mã hoá phi d i x ng s d ng m t c p khoá tuong ng v i nhau g i là phuong th c mã hoá phi d i x ng dùng khoá công khai. Phuong th c mã hóa này s d ng hai khóa là khóa công khai và khóa bí m t có các quan h toán h c v i nhau. Trong dó khóa bí m t du c gi bí m t và không có kh nang b l do không c n ph i trao d i trên m ng. Khóa công khai không ph i gi bí m t và m i ngu i d u có th nh n du c khoá này. Do phuong th c mã hóa này s d ng 2 khóa khác nhau, nên ngu i ta g i nó là phuong th c mã hóa phi d i x ng. M c dù khóa bí m t du c gi bí m t, nhung không gi ng v i "secret Key" du c s d ng trong phuong th c mã hóa d i x ng s d ng khoá bí m t do khóa bí m t không du c trao d i trên m ng. Khóa công khai và khóa bí m t tuong ng c a nó có quan h toán h c v i nhau và du c sinh ra sau khi th c hi n các hàm toàn h c; nhung các hàm toán h c dùng cho mã hóa này thoả mãn di u ki n là sao cho không th tìm du c khóa bí m t t khóa công c ng và ngu c l i. Do có m i quan h toán h c v i nhau, thông tin du c mã hóa b ng khóa công khai ch có th gi i mã du c b ng khóa bí m t tuong ng.

Giao th c thu ng du c s d ng d mã hóa d li u hi n nay là giao th c IPsec. H u h t các máy ch truy c p d a trên ph n c ng hay m m hi n nay d u h tr IPSec. IPSec là m t giao th c bao g m các chu n m b o d m các v n d b o m t, an toàn và toàn v n d li u cho các k t qua m ng s d ng giao th c IP b ng các bi n pháp mã hoá. IPSec b o v ch ng l i các hành d ng phá ho i t bên ngoài. Các client kh i t o m t m i liên quan b o m t ho t d ng tuong t nhu khoá công khai d mã hoá d li u.

Ta có th s d ng các chính sách áp d ng cho IPSec d c u hình nó. Các chính sách cung c p nhi u m c d và kh nang d b o d m an toàn cho t ng lo i d li u. Các chính sách cho IPSec s du c thi t l p cho phù h p v i t ng ngu i dùng, t ng nhóm ngu i dùng, cho m t ng d ng, nhóm mi n hay toàn b h th ng m ng.

3. Tri n khai d ch v truy c p t xa

3.1. K t n i g i vào và k t n i g i ra

C u hình máy ch truy c p d t o l p các k t n i g i vào cho phép ngu i dùng t xa truy c p vào m ng. Các thông s co b n thu ng du

hình khit o l p các k t n i g i vào bao g m xác d nh các phuong th c xác th c ngu i dùng, mã hóa hay không mã hóa d li u, các phuong th c mã hóa d li u n u yêu c u, các giao th c m ng s du c s d ng cho truy nh p t xa, các thi t d t v chính sách và các quy truy nh p c a ngu i dùng t xa, m c d du c phép truy nh p nhu th nào, xác d nh phuong th c c p phát d a ch IP cho máy truy nh p t xa, các yêu c u c u hình d t o l p các k t n i VPN…

K t n i g i ra có th du c thi t l p d g i ra t i m t máy dùng riêng ho c t i m t ISP. Trong windows 2000 h tr các hình th c k t n i sau:

N i t i m ng dùng riêng,ta s ph i cung c p s di n tho i noi s n i d n. Có th là s di n tho i c a ISP, c a m ng dùng riêng hay c a máy tính phía xa. Xác d nh quy s d ng k t n i này. .

N i t i Internet, hai l a ch n có th là s d ng truy c p qua du ng tho i và s d ng truy c p qua m ng LAN. S d ng du ng tho i, các v n d ta c n quan tâm là s di n tho i truy nh p, tên và m t kh u du c cung c p b i ISP. S d ng LAN, ta s ph i quan tâm d n proxy server và m t s thi t d t khác. T o l p k t n i VPN, VPN là m t m ng s d ng các k t n i dùng giao th c t o du ng h m (PPTP, L2TP, IPSEC,...) d t o du c các k t n i an toàn, b o d m thông tin không lâm vào tay ph m khi truy n t i qua các m ng công c ng. Tuong t nhu khi t o l p m t k t n i g i ra, N u c n thi t ph i thông qua m t ISP trung gian tru c khi n i t i m ng dùng riêng, l a ch n m t k t n i g i ra. Cung c p d a ch máy ch , d a ch m ng mà ta dang mu n n i t i. Các thi t l p khác là thi t d t các quy n s d ng k t n i.

T o l p k t n i tr c ti p v i máy tính khác,a ch n này du c s d ng d k t n i tr c ti p hai máy tính v i nhau thông qua m t cáp du c thi t k cho n i tr c ti p hai máy tính. M t trong hai máy tính du c l a ch n là ch và máy tính kia du c l a ch n là t . L a ch n thi t b c ng noi hai máy tính n i v i nhau.

3.2. K t n i s d ng da lu ng (Multilink)

Multilink là s k t h p nhi u liên k t v t lý trong m t liên k t logic duy nh t nh m gia tang bang thông cho k t n i. Multilink cho phép s d ng hai ho c nhi u hon các c ng truy n thông nhu là m t c ng duy nh t có t c d cao. Đi u này có nghia là ta có th s d ng hai modem d k t n i Internet v i t c d cao g p dôi so v i vi c s d ng m t modem. Multilink gia tang bang thông và gi m d tr gi a các h th ng b ng co ch chia các gói d li u và g i di trên các m ch song song. Multilink s d ng giao th c MPPP cho vi c qu n lý các k t n i c a mình. Đ s d ng, MPPP c n ph i du c h tr c hai phía c a k t n i (hình 5.8).

Hình 5.8: K t n i s d ng da lu ng

Hình v mô t k t n i s d ng Multilink, khi ngu i dùng t xa s d ng hai modem và hai du ng tho i k t n i v i máy ch truy c p, m i k t n i v i theo chu n V.90 có t c d 56 kbps s d ng k thu t Multilink cho phép d t t c d 112 Kbps gi a máy truy c p t xa và máy ch truy c p.

3.3. Các chính sách thi t l p cho d ch v truy nh p t xa

Chính sách truy nh p t xa là t p h p các di u ki n và các thi t d t cho phép ngu i qu n tr m ng gán cho m i ngu i dùng t xa các quy n truy c p và m c d s d ng các ngu n tài nguyên trên m ng. Ta có th dùng các chính sách d có du c nhi u các l a ch n phù h p v i t ng m c d ngu i dùng, tang tính m m d o, tính nang d ng khi c p quy n truy nh p cho ngu i dùng.

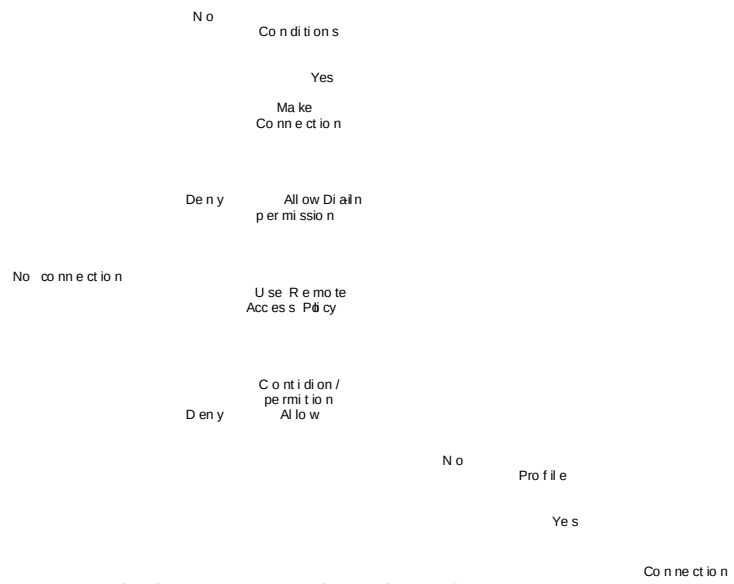
M t chính sách truy nh p t xa thông thu ng bao g m ba thành ph n nh m cung c p các truy nh p an toàn có ki m soát d n máy ch truy c p.

Các di u ki n (Conditions): là m t danh sách ki m tra các thám s nhu ngày tháng, nhóm ngu i dùng, mã ngu i g i, d a ch IP phù h p v i máy tr m dang n i d n máy ch truy c p. B chính sách di u ki n d u tiên này tuong ng v i các thông s c a yêu c u k t n i g i d n du c x lý d i v i s cho phép truy c p và c u hình.

S cho phép (Permission): Các k t n i truy nh p t xa du c cho phép và gán tr c ti p t i m i ngu i dùng b i các thi t d t trong các chính sách truy nh p t xa. Ví d m t chính sách có th gán t t c ngu i dùng trong m t nhóm nào d y quyn truy c p ch trong gi làm vi c hành chính t 8:00 A.M d n 5:00 P.M, hay d ng th i gán cho m t nhóm ngu i dùng khác quy n truy c p liên t c 24/24.

Profile: M i chính sách d u bao g m m t thi t d t c a profile áp d ng cho k t n i nhu là các th t các th c hay mã hóa. Các thi t d t trong profile du c thi hành ngay t i các k t n i. Ví d : n u m t profile thi t d t cho m t k t n i mà ngu i dùng ch du c phép s d ng trong 30 phút m i l n thì ngu i dùng s b ng t k t n i t i máy ch truy c p trong sau 30 phút.

Quá trình th c thi các chính sách truy c p t xa du c mô t b ng hình du i (hình 5.9)



Hình 5.9: Quá trình th c thi các chính sách truy c p t xa

Các di u ki n du c g i t i d t o m t k t n i, n u các di u ki n g i t i này không thích h p truy c p b t ch i, n u thích h p các di u ki n này du c s d ng d xác d nh s truy c p. Ti p theo máy ch truy c p ki m tra các cho phép quay s vào ngu i dùng s b t ch i n u thi t d t này là Deny và du c phép truy c p n u là Allow, n u thi t d t là s d ng các chính sách truy c p d xác d nh quy n truy c p thì s cho phép c a các chính sách s quy t d nh quy n truy c p c a ngu i dùng. N u các chính sách này t ch i truy c p ngu i dùng s b ng t k t n i, n u là cho phép thì s ti p tuy n t i d ki m tra các chính sách trong profile là bu c cu i cùng d xác d nh quy n truy c p c a ngu i dùng.

3.4. S d ng d ch v gán d a ch d ng DHCP cho truy c p t xa

Khi thi t l p m t máy ch truy c p d cho phép ngu i dùng t xa truy c pvào m ng, ta có th l a ch n phuong th c mà các máy t xa có th nh n du c d a ch IP.

V i phuong th c c u hình d a ch IP tinh ngay trên các máy tr m, ngu i dùng ph i c u hình b ng tay d a ch IP trên m i máy truy c p. S d ng phuong th c này ph i dm b o r ng các thông tin c u hình d a ch IP là h p l và chua du c s d ng trên m ng. Đ ng th i các thông tin v default gateway, DNS…cung ph i du c c u hình b ng tay m t cách chính xác.Vì lí do này

khuy n ngh không nên s d ng phuong pháp này cho vi c gán IP cho các máy truy c p t xa.

Máy ch truy c p có th gán d ng m t d a ch IP cho các máy truy c p t xa. Đ a ch IP này thu c trong kho ng d a ch mà ta dã c u hình trên máy ch truy c p. S d ng phuong pháp này ta c n ph i d m b o r ng kho ng d a ch IP này du c dành riêng d c p phát cho các máy truy c p t xa.

Phuo ng th c s d ng DHCP server, máy ch truy c p nh n d a ch IP t DHCP server và gán cho các máy truy c p t xa. Phuong th c này r t linh ho t, không c n ph i dành riêng m t kho ng d a ch IP dl tr cho máy truy c p t xa và thu ng du c s d ng trong m t m ng có t ch c và da d ng trong các hình th c k t n i. Đ a ch IP du c c p phát cho các máy truy c p t xa m t cách t d ng, các thông tin c u hình khác (Gateway, DNS server…) cung du c cung c p t p trung, chính xác t i t ng máy truy c p d ng th i các máy truy c p cung không c n thi t ph i c u hình l i khi có các thay d i v c u trúc m ng.

Ho t d ng c a DHCP du c mô t nhu sau: M i khi DHCP client kh i d ng, nó yêu c u m t d a ch IP t DHCP server. Khi DHCP server nh n yêu c u, nó ch n m t d a ch IP trong kho ng IP dã du c d nh nghia trong co s d li u c a nó. DHCP server c p phát d a ch IP t i DHCP client N u DHCP client ch p nh n d a ch IP này, DHCP server cho thuê d a ch IP này trong m t kho ng th i gian c th (tùy theo thi t d t). Các thông tin v d a ch IP du c g i t DHCP server t i DHCP client thu ng bao g m các thành ph n sau: d a ch IP, subnet mask, các giá tr l a ch n khác (default gateway, d a ch DNS server).

3.5. S d ng RadiusServer d xác th c k t n i cho truy c p t xa.

1. Ho t d ng c a Radius server

RADIUS là m t giao th c làm vi c theo mô hình client/server. RADIUS cung c p d ch v xác th c và tính cu c cho m ng truy nh p gián ti p. Radius client là m t máy ch truy c p ti p nh n các yêu c u xác th c t ngu i dùng t xa và chuy n các yêu c u này t i Radius server. Radius server nh n các yêu c u k t n i c a ngu i dùng xác th c và sau dó tr v các thông tin c u hình c n thi t cho Radius client d chuy n d ch v t i ngu i s d ng (hình 5.10).

Hình 5.10: Ho t d ng c a Radius server

Quá trình ho t d ng du c mô t nhu sau:

1. Ngu i s d ng t xa kh i t o quá trình xác th c PPP t i máy ch truy c p
2. Máy ch truy c p yêu c u ngu i dùng cung c p thông tin v username và password b ng các giao th c PAP ho c CHAP.
3. Ngu i dùng t xa phúc dáp và g i thông tin username và password t i máy ch truy c p.
4. Máy ch truy c p (Radius client) g i chuy n ti p các thông tin username và password ã du c mã hóa t i Radius server
5. Radius server tr l i v i các thông tin ch p nh n hay t ch i. Radius client th c hi n theo các d ch v và các thông s d ch v di cùng v i các phúc dáp ch p nh n hay t ch i t Radius server

2. Nh n th c và c p quy n

Khi Radius server nh n yêu c u truy c p t Radius client, Radius server tìm ki m trong co s d li u các thông tin v yêu c u này. N u username không có trong co s d li u này thì ho c m t profile m c d nh du c chuy n ho c m t thông báo t ch i truy c p du c chuy n t i Radius client.

Trong RADIUS nh n th c và c p quy n di dôi v i nhau, n u username có trong co s d li u và password du c xác nh n là dúng thì Radius server g i tr v thông báo truy c p du c ch p nh n, thông báo này bao g m danh sách các c p d c tính-giá tr mô t các thông s du c s d ng cho phiên làm vi c. Các thông s di n hình bao g m: ki u d ch v , ki u giao th c, d a ch gán cho ngu i dùng (d ng ho c tinh), danh sách truy c p du c áp d ng hay m t d nh tuy n tinh du c cài d t trong b ng d nh tuy n c a máy ch truy c p. Thông tin c u hình trong Radius server s xác d nh nh ng gì s du c cài d t trên máy ch truy c p. Hình v du i dây mô t quá trình nh n th c và c p quy n c a Radius server (hình 5.11)

Hình 5.11: Nh n th c và c p quy n

3.Tính cu c

Các v n d v x lý cu c c a RADIUS ho t d ng d c l p v i nh n th c và c p quy n. Ch c nang tính cu c cho phép ghi l i d li u du c g i t i th i di m b t d u và k t thúc c a m t phiên làm vi c và du các con s v m t s d ng tài nguyên nhu (th i gian, s gói, s byte...) du c s d ng trong phiên làm vi c dó.

3.6. M ng riêng o và k t n i dùng d ch v truy c p t xa

VPN (Virtual Private Network) là m t m ng riêng du c xây d ng trên n n t ng h t ng m ng công cng (ví d m ng Internet), s d ng m ng công c ng cho vi c truy n thông riêng tu.

Gi i pháp VPN cho phép ngu i dùng làm vi c t i nhà ho c dang di công tác xa có th th c hi n m t k t n i t i tr s chính b ng vi c s d ng h t ng m ng là m t m ng công c ng nhu là Internet, Nhu v y thay vì ph i th c hi n m t k t n i du ng dài t i tr s chính ngu i s d ng ch c n t o l p m t k t n i n i h t i m t ISP khi dó b ng công ngh VPN m t k t n i VPN s du c thi t l p gi a ngu i dùng v i m ng trung tâ K t n i VPN cung cho phép các t ch c k t n i liên m ng gi a các d a di m xa khác nhau thông qua các k t n i tr c ti p (leased line) t các d a di m dó t i m t ISP. Nhu v y k t n i VPN cho phép m t t ch c gi m chi phí g i du ng dài qua Dialup thi phí thuê du ng leadline cho kho ng cách xa thay vì nhu v y ch c n các k t n i n i h t và di u này là ti t ki m du c chi phí. VPN g i d li u gi a các d u cu i, d li u du c dóng gói, v i các Header cung c p thông tin d nh tuy n cho phép chuyn d li u qua m t liên k t ho c m t liên m ng công c ng t i dích. D li u chuy n di du c mã hoá d d m b o an toàn, các gói d li u truy n thông trên m ng là không th d c mà không có khoá gi i mã. Liên k t mà trong dó d li u du c dóng gói và mã hoá là t k t n i VPN.

Các hình th c k t n i: Có hai ki u k t n i VPN, k t n i VPN truy c p t xa và k t n i Site-to-site. M t k t n i VPN truy c p t xa du c thi t l p b i m t máy tính PC t i m t m ng dùng riêng. VPN gateway cung c p truy c p t i các tài nguyên c a m ng dùng riêng. Các gói d li u g i qua k t n i VPN du c kh i t o t các client. VPN client th c hi n vi c xác th c t i VPN gateway. K t n i site-to-site, du c thi t l p b i các VPN gateway và k t n i hai ph n c a m t m ng dùng riêng. (Hình 5.12).

Hình 5.12: K t n i site-to-site

Tunnel: là m t ph n quan tr ng trong vi c xây d ng m t m ng VPN. Các chu n truy n thông s d ng d qu n lý các tulnnel và dóng gói d li u c a VPN bao g m các giao th c làm vi c l p 2 nhu PPTP (Point-to-Point Tunlling Protocol) du c phát tri n b i Microsoft h tr trong môi tru ng m ng

Windows, L2TP (Layer 2 Tunnelling Protocol) du c phát tri n b i Cisco. IPsec là m t giao th c làm vi c l p 3, IPsec du c phát tri n b i IETF và ngày càng du c s d ng r ng rãi.

L2TP và PPTP có m c dích là cung c p các du ng h m d li u thông qua m ng truy n d li u công c ng. L2TP khác v i PPTP ch nó t o l p du ng h m nhung không mã hoá d li u. L2TP cung c p các du ng h m b o m t khi cùng ho t d ng v i các công ngh mã hoá khác nhu IPSec. IPSec không yêu c u ph i có L2TP nhung các ch c nang mã hoá c a nó dua d n cho L2TP kh nang cung c p các kênh thông tin b o m t, cung c p các gi i pháp VPN. L2TP và PPTP cùng s d ng PPP d dóng gói, thêm b t thông tin d u và truy n t i d li u qua m ng.

Các k t n i VPN có các d c trung sau: dóng gói (Encapsulation), xác th c (Authentication) và mã hoá d li u (Data encryption)

Đóng gói d li u: Công ngh VPN s d ng m t phuong th c dóng gói d li u trong dó cho phép d li u truy n du c qua m ng công c ng qua các giao th c t o du ng h m.

Xác th c: Khi m t k t n i VPN du c thi t l p, VPN gateway s xác th c VPN client dang yêu c u k t n i và n u du c du c phép k t n i du c th c hi n. N u s xác th c k t n i là qua l i du c s d ng, thì VPN client s th c hi n vi c xác th c l i VPN gateway, d d m b o r ng d y chính là server mà mình c n g i. Xác th c d li u và tính toàn v n c a d li u: d xác nh n r ng d li u dang du c g i t m t d u c a k t khác mà không b thay d i trong quá trình truy n, d li u ph i bao g m m t tru ng ki m tra b ng m t mã d trên m t khoá mã hoá dã bi t ch gi a ngu i g i và ngu i nh n

Mã hóa d li u: d d m b o d li u truy n trên m ng, d li u ph i du c mã hoá t i d u g i và gi i mã t i d u nh n. Vi c mã hoá và gi i mã d li u ph thu c và ngu i g i và ngu i nh n dang s d ng phuong th c mã hoá và gi i mã nào.

3.7. S d ng Network and Dial-up Connection

Network and Dial-up Connection (NDC) là m t công c du c Microsoft phát tri n d h tr vi c t o l p các k t n i trong dó bao g m các k t n i cho truy c p t xa. V i vi c s d ng NDC ta có th truy c p t i các tài nguyên dù dang trong m ng hay m t d a di m xa. Các k t n i du c kh i t o, thi l p c u hình, lu u gi và qu n lý b i NDC. M i m t k t n i bao g m m t b các d c tính du c s d ng d thi t l p liên k t gi a m t máy tính t i máy tính ho c m ng khác. Các k t n i g i ra du c liên l c v i m t máy ch truy c p xa b ng các hình th c truy c p gián ti p thuong là qua các m ng truy n d n m ng tho i công c ng, m ng ISDN. NDC cung h tr vi c thi t l p các k t n i g i vào có nghia là dóng vai trò nhu m t máy ch truy c p.

B i vì t t c các d ch v và các phuong th c truy n thông d u c thi t l p trong k t n i nên không c n ph i s d ng các công c khác d c u hình cho k t n i. Ví d d thi t l p cho m t k t n i dial-up bao g m các d c tính du c

s d ng tru c, trong và sau khi k t n i. Các thông s này bao g m: modem s quay s , ki u mã hóa password du c s d ng và các giao th c m ng s s d ng sau k t n i. Tr ng thái k t n i bao g m th i gian và t c d cung du c chính k t n i hi n th mà không c n b t c m t công c nào khác.

3.8. M t s v n d x lý s c trong truy c p t xa

Các v n d iên quan d n s c trong truy c p t xa, thu ng bao g m:

Giám sát truy c p t xagiám sát máy ch truy c p là phuong pháp t t nh t thu ng s d ng d tìm ra ngu n g c c a các v n d x y ra s c . M i m t chuong trình ph n m m hay thi t b ph n c ngy uá truy c p bao gi cung có các công c s d ng d giám sát và ghi l i các s ki n x y ra (trong các file log) d i v i m i phiên truy c p t xa.

Theo dõi các k t n i truy c p t xakh nang theo dõi các k t n i truy c p t xa c a m t Máy ch tyu c p cho ta x lý các v n d ph c t p v s c m ng. Các thông tin theo dõi m t k t n i t xa thu ng r t ph c t p và khá chi ti t do dó d phân tích và x lý c n thi t ngu i qu n tr m ng ph i có kinh nghi m và trình d v h th ng m ng.

X lý cács c v ph n c ngbao g m các thi t b truy n thông t i ngu i dùng và t i máy ch truy c p. Đ i v i các thi t b t i ngu i dùng (thu ng là các modem, c c m ng...), hãy xem tài li u v s n ph m dó hay h i nhà cung c p thi t b v s n ph m c a h vácc cách ki m tra và xác d nh l i c a s n ph m này. N u k t n i s d ng modem, hãy ki m tr a r ng modem dã du c cài d t dúng chua. Trong Windows 2000 các bu c ki m tra nhu sau:

- Trong Control Panel, kích Phone and Modem Options
- Trong trang modem, kích tên modem, sau dó kích Properties
- Kích Diagnostics, sau dó kích Query Modem.

N u modem dã du c cài d t dúng, b các thông s v modem s du c hi n th , ngu c l i hãy ki m tra và cài d t l i modem, trong tru ng h p cu i cùng hãy h i nhà s nxu t thi t b này. Đ nh n thêm các thông tin v modem trong khi dang c g ng t o l p m t k t n i, hãy xem thông tin trong log file d tìm ra nguyên nhân g p s c . Đ ghi các thông tin vào log file th c hi n theo các bu c sau:

- Trong Control Panel, kích Phone and Modem Options
- Trong trang modem, kích tên modem, sau dó kích Properties
- Kích Diagnostics, sau dó kích l a ch n Record a log, sau dó kích OK.

Đ i v i thi t b truy n thông t i máy ch truy c p: Ki m tra các thi t b ph n c ngtuong t nhu trong tru ng h p thi t b t i ngu i dùng, d ng th i ki m tra log file v các s ki n x y ra v i h th ng d tìm ra nguyên nhân s c . M t cách khác d ki m tra modem t i máy ch truy c p là s d ng m t du ng di n tho i và g i t i modem sáu dó nghe xem modem dó có tr l i và c g ng t o m t k t n i hay không. N u không có tín hi u t o k t n i t

modem dó thì có th k t lu n r ng dang có m t v n d l i v modem t i máy ch truy c p

X lý các s c v du ng truy n thông Thu ng là do cáp du c d ais hay vì nguyên nhân t nhà cung c p d ch v di n tho i. Hãy ki m tra du ng di n tho i t ngu i dùng t i máy ch truy c p b ng cách g i di n tho i thông thu ng, thông qua ch t lu ng cu c g i ta cung có th ph n nào d doán du c ch t lu ng c a du ngu truy n.

X lý các thi t d t v c u hình Sau khi xác d nh r ng các v n d v ph n c ng cung nhu du ng truy n thông d u t t, bu c ti p theo ta ki m tra các thi t d t v c u hình, bao g m:

Các thi t d t v m ng: l i c u hình v m ng x y ra khi dã ttonki thành công nhung v n không th truy c p du c các ngu n tài nguyên trên m ng, các l i thu ng x y ra nhu vi c phân gi i tên chua ho t d ng, các l i v d nh tuy n...khi l i v c u hình m ng x y ra, tru c tiên ta ki m tra r ng các máy k t n i tr ti p (không thông qua d ch v truy c p t xa) có th truy c p du c vào các ngu n tài nguyên trên m ng. Sau dó ki m tra các c u hình v TCP/IP b ng vi c s d ng l nh ipconfig /all trên máy client. Ki m tra r ng các thông s nhu DNS, d a ch IP, các thôngsố v d nh tuy n dã du c thi t d t dúng chua. S d ng l nh ping d ki m tra k t n i m ng dã làm vi c.

Các thi t d t Máy ch truy c p: Các thi t d t trên máy ch truy c p v i các thông s sai khi t o l p k t n i có th là nguyên nhân ngu i dùng **kh** không truy c p vào các ngu n tài nguyên trên m ng. Đ h tr cho vi c xác d nh nguyên nhân gây l i, ki m tra các s ki n dã ghi log trên máy ch truy c p và client, trong m t s tru ng h p c n thi t ph i theo dõi (tracing) các k t n i trên máy ch truyc p.

Các thi t d t trên máy ngu i dùng t xa: ki m tra các giao th c m ng làm vi c trên client, các giao th c m ng làm vi c trên client ph i du c h tr b i máy ch truy c p. Ví d , n u ngu i dùng t xa thi t d t trên client các giao th c NWLink, IPX/SPX và máy ch truy c p ch h tr s d ng TCP/IP, thì k t n i s không thành công.

4. Bài t p th c hành

Yêu c u v Phòng h c lý thuy tS lu ng máy tính theo s lu ng h c viên trong l p h c d m b o m i h c viên có m t máy tính, c u hình máy t thi u nhu sau (PIII 800 MHZ, 256 MB RAM, HDD 1GB,FDD, CDROM 52 x). Máy tính dã cài d t Windows 2000 advance server. Các máy tính dã du c n i m ng ch y giao th c TCP/IP.

Thi t b th c hành: Đia cài ph n m m Windows 2000 Advance Server i máy tính có 01 Modem V.90 và 01 du ng di n tho i. 01 account truyc p internet

Bài 1: Thi t l p dialup networking d t o ra k t n i Internet. truy c p Internet và gi i thi u các d ch v co b n

Đang nh p vào h th ng v i quy n Administrator.

Kích Start, tr setting, sau dó kích Network and Dialup Connections

Trong Network and Dialup Connections, kích dúp vào Make New Connection.

Trong Network Connection Wizard, kích Next, có hai l a ch n có th s d ng là Dialup to private network ho c Dialup to the Internet.

N u ch n Dialup to private network, dua vào s di n tho i truy c p c a nhà cung c p.

N u ch n Dialup to the Internet, lúc dó Internet Connection Wizard s b t d u, làm theo các bu c ch d n.

N u mu n t t c ngu i dùng d u có th s d ng k t n i này thì l a ch n, For all users, sau dó kích Next. N u mu n ch ngu i dùng hi n t i s d ng thì l a ch n Only for myself, sau dó kích Next.

N u dã l a ch n Only for myself thì chuy n d n bu c cu i cùng, N u l a ch n For all users và mu n các máy tính khác trên m ng có th chia s k t n i này hãy l a ch n Enable Internet Connection Sharing for this connection.

Thi t d t ng m d nh là b t k mày tính nào cung có th kh i t o k t n i này m t cách t d ng, n u mu n b ng m d nh này hãy xóa ch n Enable on-demand dialing, sau dó kích next

Ðua vào tên c a k t n i và kích Finish.

Bài 2: Cài d t và c u hình d ch v truy c p t xa cho phép ngu i dùng t xa truy c p vào m ng trên h di u hành Windows 2000 server.

Bu c 1:

Cài d t máy b d ch v truy c p t xa

Ðang nh p vào h th ng v i quy n Administrator

M Routing and Remote Access t menu Administrator Tools

Kích chu t ph i vào tên Server sau dó ch n Configure and Enable Routing and remote Access.

K ch b n Routing and Remote Access Server Setup xu t hi n, kích next

Trong trang common Configuration, ch n Remote access server, sau dó kích next

Trong trang Remote Client Protocol, xác d nh các giao th c s h tr cho truy c p t xa, sau dó kích next

Trong trang Network Selection, l a ch n k t n i m ng s gán cho các máy truy c p t xa, sau dó kích next

Trong trang IP Address Asignment, l a ch n Automaticlly ho c From specified range of addresses cho vi c gán các d a ch IP t i các máy truy c p t xa

Trong trang Managing Multiple Remote Acccess Servers cho phép l a ch n c u hình RADIUS, kích next

Kích Finish d k t thúc.

Bu c 2:

Thi t d t tài kho n cho ngu i dùng t xa. Thi t l p m t tài kho n có tên RemoteUser

Đang nh p v i quy n Administrator

M Active Directory Users and Computers t menu Administrator Tools

Kích chu t ph i vào Users, ch n new và kích vào User

Trong h p tho i New Object-User, di n RemoteUser vào First name

Trong h p User logon name, gõ RemoteUser

Thi t d t Password cho tài kho n này, kích next sau dó kích Finish.

Kích chu t ph i vào RemoteUser sau dó kích Properties

Trong trang Dial-In tab, kích Allow access, sau dó click OK

Thi t l p m t Global group tên là RemoteGroup, sau dó thêm tài kho n ngu i dùng v a thi t l p vào nhóm này

Kích chu t ph i vào Users, ch n new sau dó kích Group

Trong h p tho i New Object-Group, m c Group name gõ vào RemoteGroup

Trong m c Group scope ki m tra Global dã du c l a ch n, trong m c Group type ki m tra r ng Security dã du c l a ch n, sau dó kích OK

M h p tho i Properties c a RemoteGroup

Trong trang Member, kích Add

Trong h p tho i Select Users, Contacts, Computers, ho c Group, Look in box, ki m tra domain dã du c hi n th

Trong danh sách các d i tu ng, kích RemoteUser, kích Add sau dó kích OK

Kích OK d dóng h p tho i RemoteGroup Properties

Bu c 3:

Ki m tra c u hình dã thi t l p bu c trên b ng vi c th c hi n m t k t n i quay s t i máy ch truy c p t xa v i tài kho n có tên là RemoteUser, k t n i du thi t l p sau dó dóng k t n i l i.

Bu c 4:

C u hình cho phép tài kho n RemoteUser truy c p vào m ng du c di u khi n truy c p b i các chính sách truy c p t xa (Remote access policy)

M l i Active Directory Users and Computers t menu Administrat Tools

M h p tho i Properties c a tài kho n RemoteUser

Trong trang Dial-in tab, kích Control access though Remote Policy sau dó kích OK, lu u ý r ng di u khi n vùng (Domain Controler) ph i ch y ch d Native.

Thu nh c a s Active Directory Users and Computers

Bu c 5:

Ki m tra c u hình dã thi t l p bu c trên b ng vi c th c hi n m t k t n i quay s t i máy ch truy c p t xa v i tài kho n có tên là RemoteUser. Thông báo l i xu t hi n, k t n i không du c thi t l p.

Bu c 6:

S d ng RRAS d thi t l p m t chính sách m i d i v i ngu i dùng t xa, tên chính sách này là Allow RemoteGroup Access cho phép ngu i dùng trong nhóm RemoteGroup truy c p.

M Routing and Remote Access t menu Administrator Tools

M r ng tên máy ch dang c u hình, kích chu t ph i vào Remote Access Policy sau dó ch n New Remote Access Policy

Trong trang Policy Name, gõ vào Allow RemoteGroup Access sau dó kích Next

Trong trang Condition, kích Add trong h p tho i Select Attribute kích Windows-Groups sau dó kích Add

Trong h p tho i Groups kích Add

Trong h p tho i Select Groups, trong danh sách Look in, kích vào tên domain

Trong h p tho i Select Groups,du i Name kích RemoteGroups kích Add sau dó kích OK

Trong h p tho i Groups kích OK

Trong trang Condition kích Next

Trong trang Permissions kích Grant remote access permission sau dó kích Next

Trong trang User Profile kích Finish

Trong trang Routing and Remote Access kích Remote Access Policies sau dó kích chu t ph i Allow RemoteGroup access dó kích Move Up

Bu c 7:

Ki m tra c u hình dã thi t l p bu c trên b ng vi c th c hi n m t k t n i quay s t i máy ch truy c p t xa v i tài kho n có tên là RemoteUser, k t n i du c thi t l p sau dó dóng k t n i l i.

Bu c 8:

C u hình d default policy du c thi hành tru c:

M trang Routing and Remote Access, kích chu t ph i RemoteGroup sau dó kích Move Down.

Đóng c a s Routing and Remote Access

Bu c 9:

Ki m tra c u hình dã thi t l p bu c trên b ng vi c th c hi n m t k t n i quay s t i máy ch truy c p t xa v i tài kho n có tên là RemoteUser. Thông báo l i xu t hi n, k t n i không du c thi t l p.

Bu c 10:

C u hình cho phép truy c p s d ng Properties c a RemoteUser

M l i Active Directory Users and Computers t menu Administrator Tools

M Properties c a RemoteUser

Trong trang Dial-In, kích Allow access sau dó kích OK

Đóng Active Directory Users and Computers.

Bu c 11:

Ki m tra c u hình dã thi t l p bu c trên b ng vi c th c hi n m t k t n i quay s t i máy ch truy c p t xa v i tài kho n có tên là RemoteUser, k t n i du c thi t l p sau dó dóng k t n i l i

Bài 3: C u hình VPN server và thi t l p VPN Client, ki m tra k t n i t VPN Client t i VPN server

Bu c 1:

C u hình cho k t n i VPN g i vào

Đang nh p vào h th ng v i quy n Administrator

M Routing and Remote Access t menu Administrator Tools

Kích chu t ph i vào tên Server (Server là tên máy ch dang c u hình)

K ch b n thi t l p Routing and Remote Access xu t hi n, kích next

Trong trang Network Selection, m c Name ki m tra tên dã l a ch n sau dó Click next

Trong trang IP Address Assigment, kích From a specified range of addresses

Trong trang Address Range Assignment, kích New

Đi n d a ch IP vào ô Start IP address và di n vào s d a ch vào ô Number of Address

Kích OK, sau dó kích next

Trong trang Managing Multiple Remote Access Servers, l a ch n No, I don’t want to set up this server to use RADIUS now, kích next sau dó kích Finish

Kích OK d dóng h p tho i Routing and Remote Access.
C u hình cho phép tài kho n Administrator truy c p vào m ng
M Active Directory Users and Computers t menu Administrator Tools.
M r ng tên domain kích Users, kích dúp chu t vào Administrator
Trong m c Dialin, ch n Allow acces sau dó kích OK.
Đóng c a s Active Directory Users and Computers

Bu c 2:

C u hình cho k t n i VPN g i ra. Đ ki m tra d ch v truy c p t xa dã làm vi c ph c v cho nh ng ngu i dùng t xa, ta thi t l p m t n i k t t i VPN server.

Kích chu t ph i vào My Network Places, sau dó kích Properties
Trong c a s Network Dialup Connections, kích dúp chu t vào Make new connection
Trong trang Network Connection Type, kích Connect to a private network through the Internet, sau dó kích next
Trong trang Destination Address gõ vào d a ch IP c a máy cài d t VPN server, sau dó kích next
Trong trang Connection Availability, kích Only for my self, kích next sau dó kích Finish
Kh i t o k t n i t i VPN server
Trong h p tho i Connect Virtual Private Connection, kiểm tra tài kho n dang nh p là Administrator và Password sau dó kích connect
Kích OK d dóng thông báo Connnection Complete
Đóng c a s Network Dialup Connections.

S d ng ti n ích Ipconfig d xác nh n r ng b n dã thi t l p du c m t k t n i VPN và nhn du c d a IP cho k t n i này luu ý r ng d i ch IP cho k t n i VPN này là dãy d a ch tinh mà VPN server c p phát

Đóng k t n i

Kích dúp vào bi u tu ng Connection trong khay h th ng
Trong h p tho i Vitual Private Connection Status, kích disconnect
Đóng t t c các c a s l i

M c 2 : D ch v Proxy - Gi i pháp cho vi c k t n i m ng dùng riêng ra Internet

1. Các khái ni m

1.1. Mô hình client server và m t s kh nang ng d ng

Mô hình chu n cho các ng d ng trên m ng là mô hình client-server. Trong mô hình này máy tính dóng vai trò là m t client là máy tính có nhu c u c n ph c v d ch v và máy tính dóng vai trò là m t server là máy tính có th dáp ng du c các yêu c u v d ch v dó t các client. Khái ni m client-server ch mang tính tuong d i, dinày có nghia là m t máy có th lúc này dóng vai trò là client và lúc khác l i dóng vai trò là server. Nhìn chung, client là m t máy tính cá nhân, còn các Server là các máy tính có c u hình m nh có ch a các co s d li u và các chuong trình ng d ng cung c p d ch v m t d ch v nào d y t các yêu c u c a client (hình 5.13).

Hình 5.13: Mô hình client server

Cách th c ho t d ng c a mô hình client-server nhu sau: m t ti n trình trên server kh i t o luôn tr ng thái ch yêu c u t các ti n trình client. Ti n trình t i client du c kh i t o có th trên cùng h th ng ho c trên các h th ng khác du c k t n i thông qua m ng, ti n trình client thu ng du c kh i t o b i các l nh t ngu i dùng. Ti n trình client ra yêu c u và g i chúng qua m ng t i server d yêu c u du c ph c v các d ch v . Ti n trình trên server th c hi n vi c xác d nh yêu c u h p l t client sau dó ph c v và tr k t qu t i client và ti p t c ch d i các yêu c u khác. M t s ki u d ch v mà server có th cung c p nhu : d ch v th i gian (tr yêu c u thông tin v th i gian t i client), d ch v in n (ph c v yêu c u in t i client), d ch v file (g i, nh n và các thao tác v file cho client), thi hành các l nh t client trên server...

D ch v web là m t d ch v co b n trên ng Internet ho t d ng theo mô hình client-server. Trình duy t Web (Internet Explorer, Netscape...) trên các máy client s d ng giao th c TCP/IP d dua ra các yêu c u HTTP t i máy server. Trình duy t có th dua ra các yêu c u m t trang web c th hay các yêu thông tin trong các co s d li u. Máy server s d ng ph n m m c a nó phân tích các yêu c u t các gói tin nh n du c ki m tra tính h p l c a client và th c hi n ph c v các yêu c u dó c th là g i tr l i client m t trang web c th hay các thông tin trên co s d li u du i d ng m t trang web. Server là noi luu tr n i dung thông tin các website, ph n m m trên server cho phép server xác d nh du c trang c n yêu c u và g i t i client. Co s d li u và các ng d ng tuong t khác trên máy ch uoc khai thác và k t n i qua các chuong trình nhu CGI (Common Gateway Interface), khi các máy server nh n du c yêu c u v tra c u trong co s d li u , nó chuy n yêu c u t i server có ch a co s d li u ho c ng d ng d x lý qua CGI.

1.2. Socket

M t k t n i du c d nh nghia nhu là m t liên k t truy n thông gi a các ti n trình, nhu v y d xác d nh m t k t n i c n ph i xác d nh các thành ph n sau: {Protocol, local-addr, local-process, remote-addr, remote-process}

Trong dó local-addr và remote-addr là d a ch c a các máy d a phuong và máy t xa. local-process, remote-process d xác d nh v trí ti n trình trên m i h th ng. Chúng ta d nh nghia m t n a k t n i là {Protocol, local-addr, local-process} và {Protocol, remote-addr, remote-process} hay còn g i là m t socket.

Chúng ta dã bi t d xác dinh m t máy ta d a vào d a ch IP c a nó, nhung trên m t máy có vô s các ti n trình ng d ng dang ch y, d xác d nh v trí các ti n trình ng d ng này ngu i ta d nh danh cho m i ti n trình m t s hi u c ng, giao th c TCP s d ng 16 bit cho vi c d nh danh các c ng ti n trình và qui u c s hi u c ng t-1023 du c s d ng cho các ti n trình chu n (nhu FTP qui u c s d ng c ng 21, d ch v WEB qui u c c ng 80, d ch v g i thu SMTP c ng 25...) s hi u c ng t 1024-65535 dành cho các ng d ng c a ngu i dùng. Nhu v y m t c ng k t h p v i m t d a ch IP t o thành m t socket duy nh t trong liên m ng. M t k t n i TCP du c cung c p nh m t liên k t logic gi a m t c p socket. M t socket có th tham gia nhi u liên k t v i các socket xa khác nhau. Tru c khi truy n d li u gi a hai tr m c n ph i thi t l p m t liên k t TCP gi a chúng và khi k t thúc phiên truy n d li u thì liên k t dó s du c gi i phóng.

Hình 5.14: Socket

Quá trình thi t l p m t socket v i các l i g i h th ng du c mô t nhu sau: server thi t l p m t socket v i các thông s d c t các th t c truy n thông nhu (TCP, UDP, XNS...) và các ki u truy n thông (SOCK_STREAM,

SOCK_DGRAM...), sau dó liên k t t i socket này các thông s v d a ch nhu IP và các c ng TCP/UDP sau dó server ch d ch và ch p nh n k t n i d n t client.

1.3. Phuo ng th c ho t d ng và d c d i m c a d ch v Proxy

1. Phuo ng th c ho t d ng

D ch v proxy du c tri n khai nh m m c dích ph c v các k t n i t các máy tính trong m ng dùng riêng ra Internet. Khi dang ký s d ng d ch v internet t i nhà cung c p d ch v , khách hàng s du c c p h u h n s lu ng d a ch IP t nhà cung c p, s lu ng IP nh n du c không d d c p cho các máy tính tr m. M t khác v i nhu c u k t n i m ng dùng riêng ra Internet mà không mu n thay d i l i c u trúc m ng hi n t i d ng th i mu n gia tang kh nang thi hành c a m ng qua m t k t n i Internet duy nh t và mu n ki m soát t t c các thông tin vào ra, mu n c p quy n và ghi l i các thông tin truy c p c a ngu i s d ng… D ch v proxy dáp ng du c t t c các yêu c u trên. Ho t d ng trên co s mô hình client-server. Quá trình ho t d ng c a d ch v proxy theo các bu c nhu sau:

Hình 5.15: Ho t d ng c a d ch v Proxy

1 Client yêu c u m t d i tu ng trên m ng Internet

1 Proxy server ti p nh n yêu c u, ki m tra tính h p l cung nhu th c hi n vi c xác th c client n u th a mãn proxy server g i yêu c u d i tu ng này t i server trên Internet.

1 Server trên Internet g i d li u ng yêu c u v cho proxy server.

1 Proxy server g i tr d i tu ng v cho client

Ta có th thi t l p proxy server d ph c v cho nhi u d ch v nhu d ch v truy n file, d ch v web, d ch v thu di n t …M i m t d ch v c n có m t proxy server c th d ph c v các yêu c u d c thù c a d ch v dó t các client.

Proxy server còn có th du c c u hình d cho phép qu ng bá các server thu c m ng trong ra ngoài Internet v i m c d an toàn cao. Ví d ta có th thi t l p m t web server thu c m ng trong và t l p các qui t c qu ng bá web trên proxy server d cho phép qu ng bá web server này ra ngoài Internet. T t c các yêu c u truy c p web d n du c ch p nh n b i proxy server và proxy server s th c hi n vi c chuy n ti p yêu c u t i web server thu c m ng trong (hình 5.16)

Hình 5.16: Ho t d ng c a d ch v Proxy

Các client du c t ch c trong m t c u trúc m ng g i là m ng trong (Inside network) hay còn g i là m ng dùng riêng. IANA (Internet Assigned Numbers Authority) dã dành riêng 3 kho ng d a chtuIP ng ng v i 3 l p m ng tiêu chu n cho các m ng dùng riêng dó là:

10.0.0.0 - 10.255.255.255 (l p A)
172.16.0.0 - 172.31.255.255 (l p B)
192.168.0.0 - 192.168.255.255 (l p C)

Các d a ch này s d ng cho các client trong m ng dùng riêng mà không du c gán cho b t c máy ch nào trên m ng Internet. Trong vi c thi t k và c u hình m ng dùng riêng khuy n ngh nên s d ng các kho ng d a ch IP này.

Khái ni m m ng ngoài (Outside network) là d ch vùng mà các server thu cvào. Các d a ch s d ng trên m ng này là các d a ch IP du c dang ký h p l c a nhà cung c p d ch v Internet.

Proxy server s d ng hai giao ti p, giao ti p m ng trong và giao ti p ngoài. Giao ti p trong di n hình là các c c m ng s d ng cho vi c trao i gi a proxy server v i m ng dùng riêng và có d a ch du c gán là d a ch thu c m ng dùng riêng. T t c các thông tin gi a client thu c m ng dùng riêng và proxy server du c th c hi n thông qua giao ti p này. Giao ti p ngoài thu ng b ng các hình th c truy c p gián ti p qua m ng di n tho i công c ng và qua c c m ng b ng k t n i tr c ti p t i m ng ngoài. Giao ti p ngoài du c gán d a ch IP thu c m ng ngoài du c cung c p h p l b i nhà cung c p d ch v Internet.

2. Đ c di m

Proxy Server k t n i m ng dùng riêng v i m ng Internet toàn c u và cung cho phép các máy tính trên m ng internet có th truy c p các tài nguyên trong m ng dùng riêng.

Proxy Server tang cu ng kh nang k t n i ra Internet c a các máy tính trong m ng dùng riêng b ng cách t p h p các yêu c u truy c p Internet t các máy tính trong m ng và sau khi nh n du c k t qu t Internet s tr l i l i cho máy có yêu c u ban d u.

Ngoài ra proxy server còn có kh nang b o m t và ki m soát truy c p Internet c a các máy tính trong m ng dùng riêng. Cho phép thi t d t các chính sách truy c p t i t ng ngu i dùng.

Proxy server luu tr t m th i các k t qu dã du c l y t Internet v nh m tr l i cho các yêu c u truy c p Internet v i cùng d a ch . Vi c luu tr này cho phép các yêu c u truy c p Internet v i cùng d a ch s không c n ph i l y l i k t qu t Internet, làm gi m th i gian truy c p Internet, tang cu ng ho t d ng c a m ng và gi m t i trên du ng k t n i Internet. Các công vi c luu tr này g i là quá trình cache.

1.4. Cache và các phuo ng th c cache

Nh m tang cu ng kh nang truy c p Internet t các máy tính tr m trong m ng s d ng d ch v proxy ta s d ng các phuong th c cache. D ch v proxy s d ng cache d luu tr b n sao c a các d i tu ng dã du c truy c p tru c dó. T t c các d i tu ng d u có th du c luu tr (nhu hình nh và các t p tin), tuy nhiên m t s d i tu ng nhu yêu c u xác th c (Authenticate) và s d ng SSL (Secure Socket Layer) không du c cache. Nhu v y v i các d i tu ng dã du c cache, khi m t yêu c u t tm máy tính tr m t i proxy server, proxy server thay vì k t n i t i d a ch mà máy tính tr m yêu c u s tìm ki m trong cache các d i tu ng thoã mãn và g i tr k t qu v máy tính tr m. Nhu v y cache cho phép c i thi n hi u nang truy c p Internet c a mcác máy tr m và làm gi m luu lu ng trên du ng k t n i Internet. V n d g p ph i khi s d ng cache là khi các d i tu ng du c cache có s thay d i t ngu n, các máy tính tr m yêu c u m t d i tu ng t i proxy server, proxy server l y d i tu ng trong cache nh d v và nhu v y thông tin chuy n t i các máy tính tr m là thông tin cu so v i ngu n, d gi i quy t v n d này c n ph i có các chính sách d cache các d i tu ng d ng th i các d i tu ng ph i liên t c du c c p nh t m i. Ví d : thông thu ng m t d a chWEB thì các d i tu ng v hình nh ít có s thay d i còn n i dung text thu ng có s thay d i do dó ta có th thi t d t ch cache nh ng d i tu ng hình nh, nh ng d i tu ng có n i dung text thì không cache, di u này không nh hu ng t i hi u su t truy c vì các t p tin v hình nh thu ng có kính thu c r t l n so v i các d i tu ng có n i dung text, vi c c p nh t các d i tu ng nhu th nào ph thu c vào các phuong th c cache mà ta s trình bày du i dây.

Proxy server th c thi cache cho các d i tu ng yêu c u m t cách có chu k d tang hi u su t c a m ng. Ta có th thi t l p cache d d m b o r ng nó bao g m nh ng d li u thu ng hay các client s d ng nh t. Proxy server có th s d ng cho phép thông tin gi a m ng dùng riêng và Internet, vi c thông tin có th là client trong m ng truy c p Internet-trong tru ng h p này proxy server th c hi n Forward caching, cung có th là client ngoài truy c p t i m ng trong (t i các server du c qu ng bá)-trong tru ng h p này proxy server th c hi n reverse caching. C hai tru ng h p d u có du c t kh nang c a proxy server là lu u tr thông tin (t m th i) làm cho vi c truy n thông thông tin du c nhanh hon, sau dây là các tính ch t c a cache proxy server:

- Phân cache: khi cài d t m t m ng các máy proxy server ta s thi t l p du c vi c phân ph i n i dung cache. Proxy server cho phép ghép nhi u h th ng thành m t cache logic duy nh t.
- Cache phân c p: Kh nang phân ph i cache còn có th chuyên sâu hon b ng cách cài d t ch d cache phân c p liên k t-trong các máy proxy server v i nhau d client có th truy c p t i g n chúng nh t.

- Cache d nh k : s d ng cache d nh k n i dung download d i v i các yêu c u thu ng xuyên c a các client
- Reverse cache: proxy server có th cache các n i dung c a các server qu ng bá do dó tang hi u su t và kh nang truy c p, m i d c tính cache c a proxy server d u có th áp d ng cho n i dung trên các server qu ng bá.

Proxy server có th du c tri n khai nhu m t Forward cache nh m cung c p tính nang cache cho các client m ng trong truy c p Internet. Proxy server duy trì b cache t p trung c a các d i tu ng Internet thu ng du c yêu c u có th truy c p t b t k trình duy t t mày client. Các d i tu ng ph c v cho các yêu c u t các dia cache yêu c u tác v x lý nh hon dáng k so v i các d i tu ng t Internet, vi c này tang cu ng hi u su t c a trình duy t trên client, gi m th i gian h i dáp và gi m vi c chi m bang thông cho k t n i Internet. Hình v sau mô t proxy server x lý các yêu c u c a ngu i dùng ra sao (hình 6.17)

Hình 5.17: Ho t d ng c a d ch v Proxy

Hình trên mô t quá trình các client trong m ng dùng riêng truy c p ra ngoài Internet nhung ti n trình này cung tuong t d i v i các cache reverse (khi ngu i dùng trên Internet truy c p vào các Server qu ng bá) các bu c bao g m;

1 Client 1 yêu c u m t d i tu ng trên m ng Internet

2 Proxy server ki m tra xem d i tu ng có trong cache hay không. N u d i tu ng không có trong cache c a proxy server thì proxy server g i yêu c u d i tu ng t i server trên Internet.

3 Server trên Internet g i d i tu ng yêu c u v cho proxy server .

4 proxy server gi b n copy c a d i tu ng trong cache c a nó và tr d i tu ng v cho client1

5 Client 2 g i m t yêu c u v d i tu ng tuong t

6 Proxy server gcho client 2 d i tu ng t cache c a nó ch không ph i t Internet n a.

Ta có th tri n khai d ch v proxy d qu ng bá các server trong m ng dùng riêng ra ngoài Internet. V i các yêu c u d n, proxy server có th dóng vai trò nhu là m t server bên ngoài, dáp ng các yêu c a client t các n i dung web trong cache c a nó. Proxy server chuy n ti p các yêu c u cho server ch khi nào cache c a nó không th ph c v yêu c u nó (Reverse cache).

L a ch n các phuong th c cache d a trên các y u t : không gian c ng s d ng, d i tu ng nào du c cache và khi nào các d i tu ng này s du c c p nh t. V co b n ta có hai phuong th c cache th d ng và ch d ng.

Phuong th c Cache th d ng (passive cache): Cache th d ng lu u tr các d i tu ng ch khi các máy tính tr m yêu c u t i d i tu ng. Khi m t d i tu ng du c chuy n t i máy tính tr m, máy ch Proxy xác d nh xem d i tu ng này có th cache hay không n u có th d i tu ng s du c cache. Các d i tu ng ch du c c p nh t khi có nhu c u. Đ i tu ng s b xoá kh i cache d a trên di m g n nh t mà các máy tính tr m tr uy c p t i d i tu ng. Phuong th c này có l i ích là s d ng ít hon b x lý nhung t n nhi u không gian dia hon

Phuong th c Cache ch d ng (active cache): Cung gi ng nhu phuong th c cache th d ng, Cache ch ng luu tr các d i tu ng khi các máy tính tr m ra yêu c u t i m t d i tu ng máy ch Proxy dáp ng yêu c u và luu d i tu ng này vào Cache. Phuong th c này t d ng c p nh t các d i tu ng t Internet d a vào: s lu ng yêu c u d i v i các d i tu ng, d i tu ng thu ng xuyên thay d i nhu th nào. Phuong th c này s t d ng c p nh t các d i tu ng khi mà máy ch Proxy dang ph c v m c d th p và do dó không nh hu ng d n hi u su t ph c v các máy tính tr m. Đ i tu ng trong cache s b xoá d a trên các thông tin header HTTP, URL.

2. Tri n khai d ch v proxy

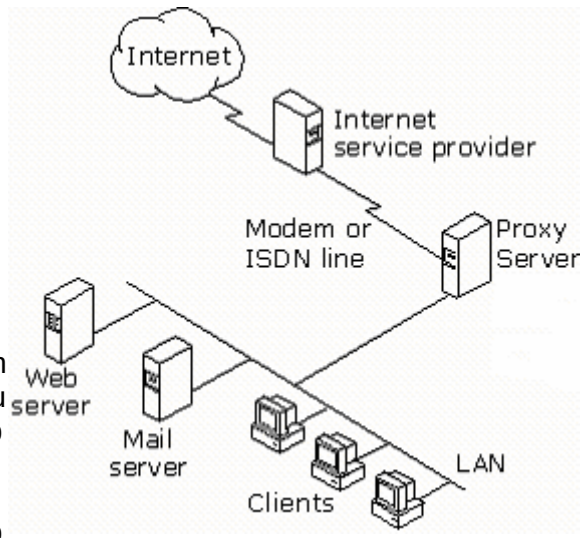
2.1. Các mô hình k t n i m ng

Đ i tu ng ph c v c a proxy server khá r ng, t m ng van phòng nh , m ng van phòng v a t i m ng c a các t p doàn l n. V i m i quy mô t ch c s có m t c u trúc m ng s d ng proxy server cho phù h p. Sau dây chúng ta s xem xét m t s mô hình co b n d i v i m ng c nh , m ng c trung bình và m ng t p doàn l n. Trong dó chúng ta s di sâu vào mô hình th nh t dành cho m ng van phòng nh b i nó phù h p quy mô h c c a các công ty v a và nh t i Vi t nam.

Mô hình m ng van phòng nh :

- Bao g m m t m ng LAN d c l p.
- S d ng giao th c IP.
- K t n i Internet b ng du ng tho i (qua m ng di n tho i công c ng b ng các hình th c quay dial up hay s d ng công ngh ADSL) ho c du ng tr c ti p (Leased Line).
- Ít hon 250 máy tính tr m.

Mô hình k t n i m ng nhu hình v (hình 5.18)



Hình 5.18: Mô hình k t n i m ng

Theo mô hình này, v i m i phuong th c k t n i Internet Proxy server s d ng 02 giao ti p nhu sau

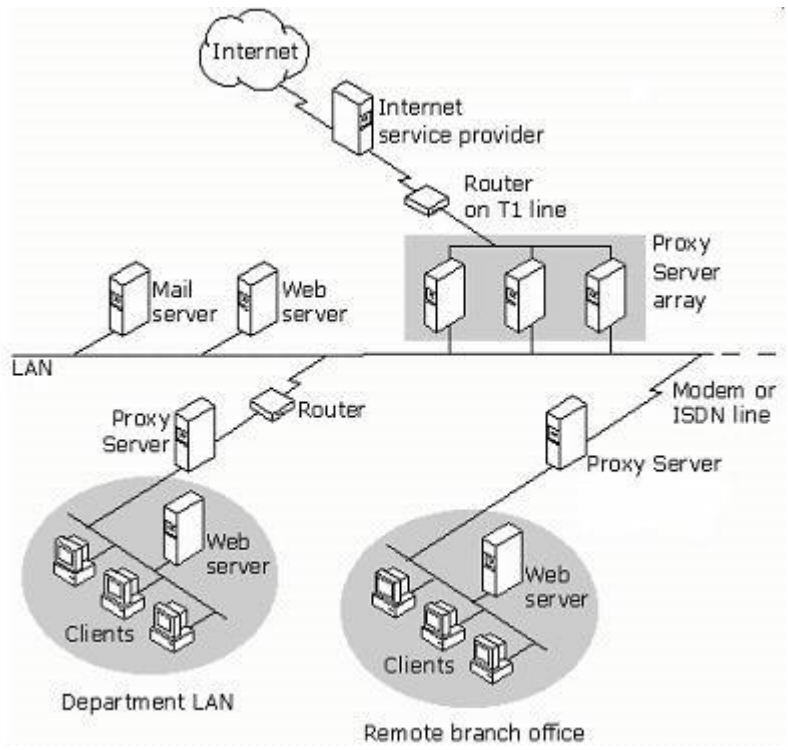
- K t n i Internet b ng du ng tho i qua m ng PSTN:
  - 01 giao ti p v i m ng n i b thông qua card m ng.
  - 01 giao ti p v i Internet thông qua Modem.
- K t n i Internet b ng du ng tr c ti p (Leased Line)
  - 01 giao ti p v i m ng n i b thông qua card m ng
  - 01 giao ti p v i Internet thông qua card m ng khác. Lúc này b ng d a ch n i b (LAT-Local Address Table) du c xây d ng d a trên danh sách d a ch IP m ng n i b .

Mô hình k t n i m ng c trung bình

Đ c tru ng c a m ng van phòngtrung bình nhu sau:

- Van phòng trung tâm v i m t vài m ng LAN
- M i van phòng chi nhánh có m t m ng LAN.
- S d ng giao th c IP.
- K t n i b ng du ng tho i t van phòng chi nhánh t i van phòng trung tâm.
- K t n i Internet t van phòng trungâm t i ISP b ng du ng tho i ho c du ng tr c ti p (Leased Line).
- Ít hon 2000 máy tính tr m

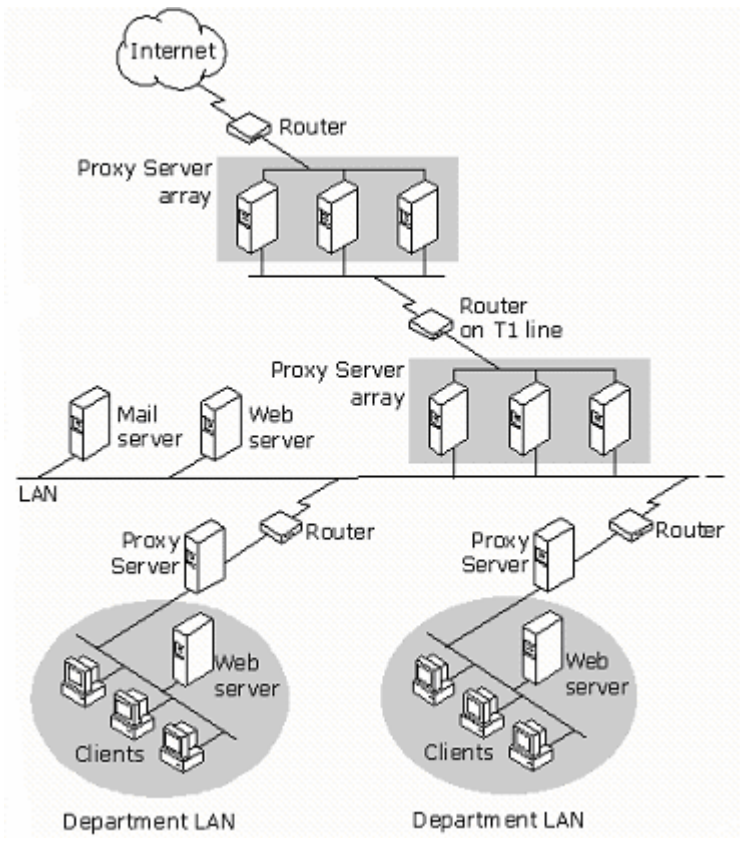
Mô hình m ng nhu hình 5.19. Theo mô hình này, van phòng chi nhánh s d ng m t máy ch Proxy cung c p kh nang lu u tr thông tin n i b (local caching), qu n tr k t n i và ki m soát truy c p t i van phòng trung tâm. T i van phòng trung tâm, m t s máy ch Proxy ho t d ng theo ki n trúc m ng (array) cung c p kh nang b o m t chung cho toàn m ng, cung c p tính nang luu tr thông tin phân tán (distributed caching) và cung c p k t n i ra Internet.



Hình 5.19: Mô hình k t n i m ng

Mô hình k t n i m ng t p doàn l n
M ng c a các t p doàn l n có d c trung nhu sau:
- Van phòng trung tâm có nhi u m ng LAN và có m ng tr c LAN.
- Có vài van phòng chinhánh, m i van phòng chi nhánh có m t m ng LAN.
- S d ng giao th c m ng IP.
- K t n i b ng du ng tho i t các van phòng chi nhánh t i van phòng trung tâm.
- K t n i Internet t van phòng trung tâm t i ISP b ng du ng du ng tr c ti p (Leased Line).
- Có nhi u hon 2000 máy tính tr m.

Mô hình m ng nhu hình 5.20. Theo mô hình này m ng t i các van phòng chi nhánh cung c u hình tuong t nhu d i v i mô hình các van phòng c trung bình. Các yêu c u k t n i Internet không du c dáp ng b i cache n i b t i máy ch Proxy c a van phòng chi nhánh s du c chuy n t i m t lo t máy ch Proxy ho t d ng theo ki n trúc m ng t i van phòng trung tâm. T i van phòng trung tâm các máy ch Proxy s d ng 02 giao ti p m ng (card m ng) trong dó 01 card m ng giao ti p i m ng tr c LAN và 01 card m ng giao ti p v i m ng LAN thành viên.



Hình 5.20: Mô hình k t n i m ng

2.2. Thi t l p chính sách truy c p và các qui t c

1..Các qui t c.

Ta có th thi t l p proxy server d áp ng các yêu c u b o m t và v n hành b ng cách thi t l p các qui t c d xác d nh xem li u ngu i dùng, máy tính ho c ng d ng có du c quy n truy c p và truy c p nhu th nào t i máy tính trong m ng hay trên Internet hay không. Thông thu ng m t proxy server d nh nghia các lo i qui t c sau: Qui t c v chính sách truy nh p, qui t c v bang thông, qui t c v chính sách qu ng bá, các d c tính l c gói và qui t c v d nh tuy n và chu i (chaining).

Khi m t client trong m ng yêu c u m t d i tu ng proxy server s x lý các qui t c d xác dhnxem yêu c u dó có du c xác d nh ch p nh n hay không. Tuong t khi m t client bên ngoài (Internet) yêu c u m t d i tu ng t m t server trong m ng, proxy server c ng x lý các b qui t c xem yêu c u có du c cho phép không.

Các qui t c c a chính sách truy nh p:Ta có th s d ng proxy server d thi t l p chính sách bao g m các qui t c v giao th c, qui t c v n i dung. Các qui t c giao th c d nh nghia giao th c nào có th s d ng cho thông tin gi a m ng trong và Internet. Qui t c giao th c s cdxu lý m c ng d ng. Ví d m t qui t c giao th c có th cho phép các Client s d ng giao th c HTTP. Các qui t c v n i dung qui d nh nh ng n i dung nào trên các site nào mà client có th truy nh p. Các qui t c n i dung cùng du c x lý m c ng dVíng. m t qui t c v n i dung có th cho phép các client truy nh p t i b t k d a ch nào trên Internet.

Qui t c bang thông:Qui t c bang thông xác d nh k t n i nào nh n du c quy n uu tiên.Trong vi c di u khi n bang thông thu ng thì proxy server không gi i h n d rng bang thông. Hon n a nó cho bi t ch t lu ng d ch v (QoS) du c c p phát uu tiên cho các k t n i m ng nhu th nào. Thu ng thì b t k k t n i nào không có qui t c v bang thông kèm theo s nh n du c quy n uu tiên ng m d nh và b t k k t n i nào cóiqu c bang thông di kèm s du c s p x p v i quy n uu tiên hon quy n uu tiên ng m d nh.

Các qui t c v chính sách qu ng bá:Ta có th s d ng proxy server d thi t l p chính sách qu ng bá, bao g m các qui t c qu ng bá server và qui t c qu ng bá web.Các qui t c qu ng bá server và web l c t t c các yêu c u d n t các yêu c u c a client ngoài m ng (internet) t i các server trong m ng. Các qui t c qu ng bá server và web s dua các yêu c u d n cho các server thích h p phía sau proxy server.

Đ c tính l c gói: Đ c tính l c gói c a proxy server cho phép di u khi n lu ng các gói IP d n và di t proxy server. Khi l c gói ho t d ng thì m i gói trên giao di n bên ngoài d u b r t l i, tr khi chúng du c hoàn toàn cho phép ho c là m t cách c d nh b ngéqcb l c gói IP, ho c là m t cách d ng b ng các chính sách truy c p hay qu ng bá. Th m chí n u b n không d l c gói ho t d ng thì truy n thông gi a m ng Internet và m ng c c b du c cho phép khi nào b n thi t l p rõ ràng các qui t c cho phép truy c p.Trong h u h t các tru ng h p, vi c m các c ng d ng thu ng du c s d ng hon. Do dó, ngu i ta thu ng khuy n ngh r ng b n nên thi t l p các qui t c truy c p cho phép client trong m ng truy nh p vào Internet ho c các qui t c qu ng bá cho phép client bênngoài truy nh p vào các server bên trong. Đó là do các b l c gói IP m m t cách c d nh nh ng chính sách truy nh p và qui t c qu ng bá l i m các c ng ki u d ng. Gi s b n mu n c p quy n cho m i ngu i dùng trong m ng truy c p t i các site HTTP. B kh ông nên thi t l p m t b l c gói IP d m c ng 80. Nên thi t l p qui t c v site, n i dung và giao th c c n thi t d cho phép vi c truy nh p này. Trong m t vài tru ng h p ta s ph i s d ng các l c gói IP, ví d nên thi t l p các l c gói IP n u ta mu qu ng bá các Server ra bên ngoài.

Qui t c d nh tuy n và c u hình chu i proxy (chaining):Đ u ng là qui t c du c áp d ng sau cùng d d nh tuy n các yêu c u c a client t i m t server dã du c ch d nh d ph c v các yêu c u dó.

2. X lý các yêu c udi

M t trong các ch c nang chính c a proxy server là kh nang k t n i m ng dùng riêng ra Internet trong khi b o v m ng kh i nh ng n i dung có ác ý. Đ thu n ti n cho vi c ki m soát k t n i này, ta dùng proxy server d t o ra m t chính sách truy c pcho phép các client truy c p t i các server trên Internet c th , chính sách truy c p cùng v i các qui t c d nh tuy n quy t d nh các client truy c p Internet nhu th nào.

Khi proxy server x lý m t yêu c u di, proxy server ki m tra các qui t c d nhtuy n các qui t c v n i dung và các qui t c giao th c d xem xét vi c truy c p có du c phép hay không. Yêu c u ch du c cho phép n u c quy t c giao

th c, qui t c n i dung và site cho phép và n u không m t qui t c nào t ch i yêu c u.

M t vài qui t c có th du c thi l p d áp d ng cho các client c th . Trong tru ng h p này, các client có th du c ch d nh ho c là b ng d a ch IP ho c b ng user name. Proxy server x lý các yêu c u theo cách khác nhau ph thu c vào ki u yêu c u c a client và vi c thi t l p proxy server.V i m t yêu c u, các qui t c du c x lý theo th t nhu sau: qui t c giao th c, qui t c n i dung, các l c gói IP, qui t c d nh tuy n ho c c u hình chu i proxy.
Hình du i dua ra quá trình x lý d i v i m t yêu c u di (hình 5.21)

Hình 5.21: Quá trình x lý d i v i m t yêu c u di

Tru c tiên, proxy server ki m tra các qui t c giao th c, proxy server ch p nh n yêu c u ch khi m t qui t c giao th c ch p nh n m t cách c th yêu c u và không m t qui t c giao th c nào t ch i yêu c u dó.

Sau dó, proxy server ki m tra các qui t c v n i dung. Proxy server ch p nh n yêu c u n u m t qui t c v n i dung ch p nh n yêu c u và không có m t qui t c v n i dung nào t ch i nó.

Ti p d n proxy server ki m tra xem li u có m t b l c gói IP nào du c thi t l p d lo i b yêu c u không d quy t d nh xem li u yêu c u có b t ch i. Cu i cùng, proxy server ki m tra qui t c d nh tuy n d quy t d nh xem yêu c u du c ph c v nhu th nào.

Gi s cài d t m t proxy server trên m t máy tính v i hai giao ti p k t n i, m t k t n i v i Internet và m t k t n i vào m ng dùng riêng. Ta s cho các ch d n d cho phép t t c client truy c p vào t t c các site. Trong tru ng h p này, chính sách truy nh p ch là các qui nhu sau: m t qui t c v giao th c

cho phép t t c các client s d ng m i giao th c t i t t c các th i di m .M t qui t c v n i dung cho phép t t c m i ngu i truy c p t i m i n i dung trên t t c các site t t c các th i di m nào. Luu ý r ng qui t c này ch p cho các client truy c p Internet nhung không cho các client bên ngoài truy c p vào m ng c a b n.

3. X lý các yêu c u d n

Proxy server có th du c thi t l p d các Server bên trong có th truy c p an toàn d n t các client ngoài. Ta có th s d ng proxy server d thi t l p m t chính sách qu ng bá an toàn cho các Server trong m ng. Chính sách qu ng bá (bao g m các b l c gói IP, các qui t c qu ng bá Web, ho c qui t c qu ng bá Server, cùng v i các qui t c d nh tuy n) s quy t d nh các Server du c qu ng bá nhu th nào.

Khi proxy server x lý m t yêu c u xu t phát t m t client bên ngoài, nó s ki m tra các b l c gói IP, các qui t c qu ng bá và các qui t c d nh tuy n d quy t d nh xem li u yêu c u có du c th c hi n hay không và Server trong nào s th c hi n các yêu c u dó.

Hình 5.22: X lý các yêu c u d n

Gi s r ng dã cài d t proxy server v i hai giao ti p k t n i, m t k t n i t i Internet và m t k t n i vào m ng dùng riêng. N u l c gói ho t d ng và sau dó, b l c gói IP tch i yêu c u thì yêu c u s b t ch i. N u các qui t c qu ng bá web t ch i yêu c u thì yêu c u cung b lo i b . N u m t qui t c d nh tuy n du c thi t l p yêu c u du c d nh tuy n t i m t Server upstream ho c m t site ch k phiên thì Server du c xác nh dó s x lý yêu c u. N u m t qui t c d nh tuy n ch ra r ng các yêu c u du c d nh tuy n t i m t Server c th thì web Server trong s tr v d i tu ng.

2.3. Proxy client và các phuong th c nh n th c

Chính sách truy nh p và các qui t c qu ng bá c a Proxy server có th
du c thi t l p d cho phép ho c t ch i m t nhóm máy tính hay m t nhóm các
ngu i dùng truy nh p t i m t server nào dó. N u qui t c du c áp d ng riêng
v i các ngu i dùng, Proxy server s ki m tra các d c tính yêu c u d quy t
d nh ngu i dùng du c nh n th c nhu th nào.

Ta có th thi t l p các thông s cho các yêu c u thông tin di và d n d
ngu i dùng ph i du c proxy server nh n th c tru c khi x lý các qui t c. Vi c
này d m b o r ng các yêu c u ch du c phép n u ngu i dùng dua ra các yêu
c u dã du c xác th c. B n cung có th thi t l p các phuong pháp nh n th c
du c s d ng và có th thi t l p các phuong pháp nh n th c cho các yêu c u di
và yêu c u d n khác nhau. V co b n m t Proxy server thu ng h tr các
phuong pháp nh n th c sau dây: Phuong th c nh n th c co b n., nh n th c
Digest, nh n th c tích h p Microsoft windows, ch ng th c client và ch ng
th c server.

Đ m b o r ng các chuong trình proxy client ph i h tr m t trong các
phuong pháp nh n th c mà proxy server dã du a ra. Ch ng h n Trình duy t IE 5 tr lên h
tr h u h t các phuong pháp nh n th c, m t vài trình duy t khác có th ch h
tr phuong pháp nh n th c co b n. Đ m b o r ng các trình duy t client có th
h tr ít nh t m t trong s các phuong pháp nh n th c mà Proxy server h tr.

1. Phuong pháp nh n th c co b n.

Phuo ng pháp nh n th c này g i và nh n các thông tin v ngu i dùng là
các ký t text d dàng d c du c. Thông thu ng thì các thông tin v user name
và password s du c mã hoá thì trong phuong pháp này không có mã hoá
nào du c s d ng. Ti n trình nh n th c du c mô t nhu sau, proxy client nh c
ngu i dùng du a vào username và password sau dó thông tin này du c client
g i cho proxy server. Cu i cùng username và password du c ki m tra nhu là
m t tài kho n trên proxy server.

2. Phuo ng pháp nh n th c Digest.

Phuong pháp này có tính ch t tuong t nhu phuong pháp nh n th c co
b n nhung khác vi c chuy n các thông tin nh n th c. Các thông tin nh n th c
qua m t ti n trình x lý m t chi u thu ng du c bi t dùng cái tên là "hashing".
K t qu c a ti n trình này g i là hash hay message digest và không th gi i mã
chúng. Thông tin g c không th ph c h i t hash. Các thông tin du c b sung
vào password tru c khi hash nên không ai có th b t du c password và s d n
chúng d gi danh ngu i dùng th c. Các giá tr du c thêm vào d giúp nh n
d ng ngu i dùng. M t tem th i gian cung du c thêm vào d ngan c n ngu i
dùng s d ng m t password sau khi nó dã b hu . Đây là m t uu di m rõ ràng
so v i phuong pháp nh n th c co b n b i vì ngu i dùng b t h p pháp không
th ch n b t du c password.

3. Phuo ng pháp nh n th c tích h p.

Phuong pháp này du c s d ng tích h p trong các s n ph m c a
Microsoft. Đây cung là phuong pháp chu n c a vi c nh n th c b i vì username
và password không du c g i qua m ng. Phuong pháp này s d ng ho c giao

thực nhận thực V5 Kerberos hoặc giao thức nhận thực challenge/response của nó.

4. Chứng thực client và chứng thực server

Ta có thể sử dụng các đặc tính của SSL để nhận thực. Chứng thực được sử dụng theo hai cách khi một client yêu cầu một đối tượng từ server: server nhận thực chính nó bằng cách gửi đi một chứng thực server cho client. Server yêu cầu client nhận thực chính nó (Trong trường hợp này client phải đưa ra một chứng thực client phù hợp tới server).

SSL nhận thực bằng cách kiểm tra nội dung của một chứng thực số được mã hoá do proxy client dự trình lên trong quá trình đang nhập (Các người dùng có thể có được các chứng thực số từ một tổ chức ngoài có độ tin tưởng cao). Các chứng thực về server bao gồm các thông tin nhận biết về server. Các chứng thực về client thường gồm các thông tin nhận biết về người dùng và tổ chức đưa ra chứng thực đó

Chứng thực client:Nếu chứng thực client được lựa chọn là phương thức xác thực thì proxy server sẽ yêu cầu client gửi chứng thực được trước khi yêu cầu một đối tượng. Proxy server nhận yêu cầu và gửi một chứng thực cho client. Client nhận chứng thực này và kiểm tra xem có thực là thuộc về proxy server . Client gửi yêu cầu của nó cho proxy server, tuy nhiên proxy server yêu cầu một chứng thực từ client mà dãy được đưa ra trước đó. Proxy server kiểm tra xem chứng thực có thực sự thuộc về client được phép truy cập không.

Chứng thực server:Khi một client yêu cầu một đối tượng SSL từ một server, client yêu cầu server phải nhận thực chính nó. Nếu proxy server kết thúc một kết nối SSL thì sau đó proxy server sẽ phải nhận thực chính nó cho client. Ta phải thiết lập và chỉ định các chứng thực về phía server để sử dụng khi nhận thực server cho client

5. Nhận thực passthough

Nhận thực passthough chỉ định khả nang của proxy server chuyển thông tin nhận thực của client cho server dích. Proxy server hỗ trợ nhận thực cho các yêu cầu đi và đến. Hình vẽ sau mô tả trường hợp nhận thực passthough

Hình 5.23: Nhận thực passthough

Client gửi yêu cầu lấy một đối tượng trên một web server cho proxy server. Proxy server chuyển yêu cầu này cho web server, bắt đầu tiến hành việc nhận thực qua các bước sau:

1 Webserver nh n du c yêu c u l y d i tu ng và d ng client c n ph i
nh n th c. Web server cung ch ra các ki u nh n th c du c h tr .
2 Proxy server chuy n yêu c u nh n th c cho client
3 Client ti p nh n yêu c u và tr các thông tin nh n th c cho proxy server
4 Proxy server chuy n l i thông tin dó cho web server
5 T lúc này client liên l c tr c ti p v i web server

6. SSL Tunneling.

V i du ng h m SSL, m t client có th thi t l p m t du ng h m qua proxy server tr c ti p t i server yeu c u v i các d i tu ng yêu c u là HTTPS. B t c khi nào client yêu c u m t d i tu ng HTTPS qua proxy server nó s d ng du ng h m SSL. Đu ng h m SSL làm vi c b i s ng m d nh các yêu c u di t i các c ng 443 và 563.

Hình 5.24: SSL Tunneling.

Ti n trình t o du ng h m SSL du c mô t nhu sau:

1 Khi client yêu c u m t d i tu ng HTTPS t m t web server trên Internet, proxy server g i m t yêu c u k t nh https://URL_name
2 Yêu c u ti p theo du c g i t i c ng 8080 trên máy proxy server CONNECT URL_name443 HTTP/1.1
3 Proxy server k t n iitWeb server trên c ng 443
4 Khi m t k t n i TCP du c thi t l p, proxy server tr l i k t n i dã du c thi t l p HTTP/1.0 200
5 T dây, client thông tin tr c ti p v i Web server bên ngoài

7. SSL bridging.

SSL bridging d c p d n kh nang c a proxy server trong vi c mã hóa ho c gi i mã các yêu c u c a client và chuy n các yêu c u này t i server dích. Ví d , trong tru ng h p qu ng bá (ho c reverse proxy), proxy server có th ph c v m t yêu c u SSL c a client b ng cách ch m d t k t n i SSL client và m l i m t k t n i m i v i web server. SSL bridging du c s d ng khi proxy server k t thúc ho c kh i t o m t k t n i SSL.

Khi m t client yêu c u m t d i tu ng HTTP. Proxy server mã hóa yêu c u và chuy n ti p nó cho web server. Web server tr v d i tu ng mã hóa cho proxy server. Sau dó proxy server gi i mã d i tu ng và g i l i cho client. Nói m t cách khác các yêu c u HTTP du c chuy n ti p nhu các yêu c u SSL.

Khi client yêu c u m t d i tu ng SSL. Proxy server gi i mã yêu c u, sau dó mã hóa l i m t l n n a và chuy n ti p nó t i Web server. Web server tr v d i tu ng mã hóa cho proxy server. Proxy server gi i mã d i tu ng và sau dó g i nó cho client. Nói m t cách khác các yêu c u SSL du c chuy n ti p nhu là các yêu c u SSL.

Khi client yêu c u m t d i tu ng SSL. Proxy server gi i mã yêu c u và chuy n ti p nó cho web server. Web server tr v d i tu ng HTTP cho proxy server. Proxy server mã hóa d i tu ng và chuy n nó cho client. Nói cách khác các yêu c u SSL du c chuy n ti p nhu các yêu c u HTTP.

SSL bridging có th du c thi t l p cho các yêu c u di và d n. Tuy nhiên v i các yêu c u di client ph i h tr truy n thông b o m t v i proxy server.

2.4. NAT và proxy server

Khái ni m NAT (Network Addresss Tranlation)

NAT là m t giao th c cho ta kh nang b n d hóa m t m t vùng d a ch IP s d ng trong m ng dùng riêng ra m ng ngoài và ngu c l i. NAT thu ng du c thi t l p trên các b d nh tuy n là ranh gi i gi a m ng dùng riêng và m ng ngoài (ví d nhu m ng công c ng Internet). NAT ch u d i các d a ch IP trên m ng dùng riêng thành các d a ch IP du c dang ký h p l tru c khi chuy n các gói t m ng dùng riêng t i Internet ho c t i m ng ngoài khác. Trong ph n này chúng ta s ch tìm hi u s v n hành c a NAT khi NAT du c thi t l p d cung c p các ch c nang chuy n d i các d a ch m ng dùng riêng trong vi c ph c v cho vi c k t n i truy c p ra m ng ngoài nhu th nào. Đ làm vi c này, NAT dùng ti n trình các bu c theo hình v du i dây.

Hình 5.25: NAT

1. Ngu i dùng t i máy 10.1.1.25 mu n m m t k t n i ra ngoài t i server 203.162.0.12

2. Khi gói d li u d u tiên t i NAT router, NAT router th c hi n vi c ki m tra trong b ng NAT. N u s chuy n d i d a ch dã có trong b ng, NAT router th c hi n bu c th 3. N u không có s chuy n đ i du c tìm th y, NAT router xác d nh r ng d a ch 10.1.1.25 ph i du c chuy n d i. NAT router xác d nh m t d a ch m i và c u hình m t chuy n d i d i v i d a ch 10.1.1.25 t i d a ch h p l ngoài m ng (Internet) t dãy d a ch d ng dã du c d nh nghia tru c ví d 203.162.94.163.

3. NAT router thay th d a ch 10.1.1.25 b ng d a ch 203.162.94.163 sau dó gói du c chuy n ti p t i dích.

4. Server 203.162.0.12 trên Internet nh n gói và phúc dáp tr l i NAT router v i d a ch 203.162.94.163.

5. Khi NAT router nh n du c gói phúc dáp t Server v i d a ch dích d n là 203.162.94.163, nó th c hi n vi c tìm ki m trong b ng NAT. B ng NAT ch ra r ng d a ch m ng trong 10.1.1.25 (tuong ng du c ánh x t i d a ch 203.162.94.163 m ng ngoài) s nh n du c gói tin này. NAT router th c hi n vi c chuy n d i d a ch dích trong gói tin là 10.1.1.25 và chuy n gói tin này t i dích (10.1.1.25). Máy 10.1.1.25 nh n gói và ti p t c th c hi n v i các gói ti p theo v i các bu c tu n t nhu trên.

Trong trung h p mu n s d ng m t d a ch m ng ngoài cho nhi u d a ch m ng trong. NAT router s duy trì các thông tin th t c m c cao hon trong b ng NAT d i v i các s hi u c ng TCP và UDP d chuy n d i d a ch m ng ngoài tr l i chính xác t i các d a ch m ng trong.

Nhu v y NAT cho phép các client trong m ng dùng riêng v i vi c s d ng các d a ch IP dùng riêng truy c p vào m t m ng bên ngoài nhu m ng Internet.Cung c p k t n i ra ngoài Internet trong các m ng không du c cung c p d các d a ch Internet c ng ký. Thích h p cho vi c chuy n d i d a ch trong hai m ng Intranet ghép n i nhau. Chuy n d i các d a ch IP n i t i du c ISP cu phân b thành các d a ch du c phân b b i ISP m i mà không c n thi t l p th công các giao di n m ng c c b .

NAT có th du c s d ng m t cách c d nh ho c d ng. Chuy n d i c d nh x y ra khi ta thi t l p th công m t b ng d a ch cùng các d a ch IP. M t d a ch c th bên trong m ng s d ng m t d a ch IP (du c thi t l p th công b i ngu i qu n tr m ng) d truy c p ra m ng ngoài. Các thi t l p d ng cho phép ngu i qu n tr thi t l p m t ho c nhi u các nhóm d a ch IP dùng chung dã dang ký. Nh ng d a ch trong nhóm này có th du c s d ng b i các client trên m ng dùng riêng d truy c p ra m ng ngoài. Vi c này cho phép nhi u client trong m ng s d ng cùng m t d a ch IP.

NAT cung có m t s nhu c di m nhu làm tang d tr c a các gói tin trên m ng. NAT ph i x lý m i gói d quy t d nh xem li u các header du c thay d i nhu th nào. Không ph i b t k ng d ng nào c ng có th ch y du c v i NAT. NAT h tr nhi u giao th c truy n thông và cung r t nhi u giao th c không du c h tr . Các giao th c du c NAT h tr nhu:TCP,UDP, HTTP, TFTP, FTP…Các thông tin không du c h tr nhu: IP multicast, BOOTP, DNS zone transfer, SNMP…

Proxy và NAT

Nhu dã phân tích c d ch v NAT và d ch v Proxy d u có th là m t gi i pháp d k t n i các m ng dùng riêng ra Internet, tuy nhiên m i d ch v l i có các uu di m và nhu c di m riêng.

D ch v proxy cho kh nang thi hành và t c d cao hon nh tính nang cache, tuy nhiên s d ng cache có th du a ra các d i tu ng dã quá h n c n ph i có các chính sách cache h p lý d d m b o tính th i s c a các d i tu ng. Chính vì s d ng cache nên gi m t i trên k t n i truy c p Internet. NAT không có tính nang cache.

D ch v proxy ph i du c tri n khai d i v i t ng ng d ng, trong khi NAT là m t ti n trình trong su t hon. H u h t các ng d ng d u có th làm vi c du c v i NAT. NAT d cài d t và v n hành, du ng nhu không ph i làm gì nhi u v i NAT sau khi cài d t.

T i các client, d i v i NAT không ph i thi t d t gì nhi u ngoài vi c c u hình tham s default gateway t i Server NAT. Trong khi s d ng d ch v proxy, c n ph i có các chuong trình proxy client d làm vi c v i proxy server.

D ch v proxy cho phép th c th i các chính sách t i ngu i dùng, v i NAT vi c s d ng các tính nang này có h n ch r t nhi u, có th nói s d ng d ch v proxy là cách truy c p an toàn nh t d k t n i m ng dùng riêng ra ngoài Internet.

3. Các tính nang c a ph n m m Microsoft ISA server 2000

3.1. Các phiên b n

ISA server bao g m hai phiên b n du c thi t k d phù h p v i t ng nhu c u c a ngu i s d ng dó là ISA server Standard và ISA server Enterprise.

- ISA server Standard cung c p kh nang an toàn firewall và kh ng na web cache cho m t môi tru ng kinh doanh, các nhóm làm vi c hay van phòng nh . ISA server Standard cung c p vi c b o m t ch t ch , truy c p web nhanh, qu n lý tr c quan, giá c h plý và kh nang thi hành cao.
- ISA server Enterprise du c thi t k dáp ng các nhu c u v hi u su t, qu n tr và cân b ng trong các môi tru ng Internet t c d cao v i s qu n lý server t p trung, chính sách truy c p da m c và các kh nang ch ng l i cao. ISA server Enterprisecung c p s b o m t, truy c p Internet nhanh cho các môi tru ng có s dòi h i kh t khe.

3.2. L i ích

ISA server là m t trong các ph n m m máy ch thu c dòng .NET Enterprise Server. Các s n ph m thu c dòng .NET Enterprise Server là các server ng d ng toàn di n c a Microsoft trong vây x d ng, tri n khai, qu n lý, tích h p, các gi i pháp d a trên web và các d ch v . ISA server mang l i m t s các l i ích cho các t ch c c n k t n i Internet nhanh, b o m t, d qu n lý.

1. Truy c p Web nhanh v i cache hi u su t cao.
- Ngu i dùng có th truy c p web nhanh hon b ng các d i tu ng t i ch trong cache so v i vi c ph i k t n i vào Internet lúc nào cung ti m tàng nguy co t c ngh n.
- Gi m giá thành bang thông nh gi m luu lu ng t Internet
- Phân tán n i dung c a các Web server và các ng d ng thu ong n t m t cách hi u qu , dáp ng du c nhu c u khách hàng trên toàn c u (kh nang phân ph i n i dung web ch có trên phiên b n ISA server Enterprise)

2. K t n i Internet an toàn nh Firewall nhi u l p.
- B o v m ng tru c các truy nh p b t h p pháp b ng cách giám sát luu lu ng m ng t i nhi u l p
- B o v các máy ch web, email và các ng d ng khác kh i s t n công t bên ngoài b ng vi c s d ng web và server qu ng bá d x lý m t cách an toàn các yêu c u d n
- L c luu lu ng m ng di vào n d m b o an toàn.
- Cung c p truy c p an toan cho ngu i dùng h p l t Internet t i m ng n i t i nh s d ng m ng riêng o (VPN)

3. Qu n lý th ng nh t v i s qu n tr tích h p.
- Đi u khi n truy c p t p trung d m b o tính an toàn và phát hi u l c a các chính sách v n hành.
- Tang hi u su t nh vi c gi i h n truy c p s d ng Internet d i v i m t s các ng d ng và dích d n.
- C p phát bang thông d phù h p v i các uu tiên.
- Cung c p các công c giám sát và các báo cáo d kh n ra Internet du c s d ng nhu th nào.
- T d ng hóa các nhi m v b ng vi c s d ng các script

4. Kh nang m r ng.
- Chú tr ng t i an toàn và thi hành nh s d ng ISA server Softwware Development Kit (SDK) v i s phát tri n các thành ph n ung.
- Ch c nang qu n lý và an toàn m r ng cho các nhà s n xu t th ba
- T d ng các tác v qu n tr v i các d i tu ng Script COM (Component Object Model)

3.3. Các ch d cài d t

ISA server có th du c cài d t ba ch d khác nhau: Cache, Firewall và Integrated

1. Ch d cache: Trong ch d này ta có th nâng cao hi u su t truy c p và ti t ki m bang thông b ng cách luu tr các d i tu ng web thu ng du c truy xu t t ngu i dùng. Ta cung có th d nh tuy n các yêu c u c a ngu i dùng t i cache server khác dang luu gi các d i tu ng dó.

2. Ch d firewall: Trong ch d này cho phép ta d m b o an toàn luu lu ng m ng nh s thi t l p các qui t c di u khi n thông tin gi a m ng trong và Internet. Ta cung có th qu ng bá các server trong d chia s tới i u m ng v i các d i tác và khách hàng.

3. Ch d tích h p: Trong ch d này ta có th tích h p các d ch v cache và firewall trên m t server.

3.4. Các tính nang c a m i ch d cài d t

Các tính nang khác nhau tùy thu c vào ch d mà ta cài d t, sau li t kê các tính nang có trong ch d firewall và cache, ch d tích h p có t t c các tính nang dó

Tính nang	Mô t	Ch d firewall	Ch d cache
Chính sách truy c p	Đ nh nghia các giao th c và n i dung Internet mà ngu i dùng có th s d ng và truy c p	Có	Ch có HTTP và FTP
Cache	Luu tr d nh k các d i tu ng web vào RAM và dia c ng c a ISA server	Không	Có
VPN M	r ng m ng riêng nh s d ng các du ng liên k t qua các m ng du c chia shay m ng công c ng nhu Internet	Có	Không
L c gói	Đi u khi n dòng gói IP di và d n	Có	Không
L c ng d ng	Th c thi các tác v c a h th ng ho c c a giao th c ch d nh, nhu là nh n th c d cung c p m t l p b o v b sung cho d ch v firewall	Có	Không
Qu ngbá Web	Qu ng bá web trong m ng d ngu i dùng trong m ng có th truy c p	Không	Có
Qu ng bá Server	Cho phép các Server ng d ng có th ph c v các client bên ngoài	Có	Không
Giám sát th i gian th c	Cho phép giám sát t p trung hoá các d ng c a ISA server bao g m các c nh báo, giám sát các phiên làm vi c và các d ch v	Có	Có
C nh báo	Báo cho ta bi t các s ki n d c bi t xu t hi n và th c thi các ho t d ng phù h p	Có	Có

Báo cáo T ng h p và phân tích hd ng trên m t ho c nhi u máy ISA server	Có	Có

4. Bài t p th c hành.

Yêu c u v Phòng h c lý thuy t S lu ng máy tính theo s lu ng h c viên trong l p h c d m b o m i h c viên có m t máy tính, c u hình máy t i thi u nhu sau (PIII 800 MHZ, 256 MB RAM, HDD 1GB,FDD, CDROM 52 x). Máy tính dã cài d t Windows 2000 advance server. Các máy tính dã du c n i m ng ch y giao th c TCP/IP.

Đia cài ph n m m Windows 2000 Advance Server, Thi t b th c hành: dia cài ph n m m i máy tính có 01 Modem V.90 và 01 ISA Server 2000. M du ng di n tho i. 01 account truy c p internet

Bài 1: Các bu c cài d t co b n ph n m m ISA server 2000.

Bu c 1: Các bu c cài d t co b n.

Đang nh p vào h th ng v i quy n Administrator

Đua dia cài d t Microsoft Internet Security and Acceleration Server 2000 Enterprise Edition vào CD ROM.

C a s Microsoft ISA Server Setup m ra. N u c a s này không t d ng xu t hi n, s d ng Windows Explorer d ch y file Autorun.exe (v i x là tên dia CD-ROM).

Trong c a s Microsoft ISA Server Setup, kích Install ISA Server.

Trong h p tho i Microsoft ISA Server (Enterprise Edition) Setup kích Continue.

Vào CD Key sau dó kích OK hai l n.

Trong h p tho i Microsoft ISA Server Setup kích I Agree.

Trong h p tho i Microsoft ISA Server (Enterprise Edition) Setup kích Custom Installation.

Trong h p tho i Microsoft ISA Server (Enterprise Edition) Custom Installation kích Add-In services sau dó kích Change Option.

Trong h p tho i Microsoft ISA Server (Enterprise Edition) Add-in services ki m tra l a ch n Install H.323 Gatekeeper Service dã du c ch n, ch n Message Screener sau dó kích OK.

Trong h p tho i Microsoft ISA Server (Enterprise Edition) CustomInstallation kích Administration tools sau dó kích Change Option.

Trong h p tho i Microsoft ISA Server (Enterprise Edition) Administration tools, ki m tra l a ch n ISA Management dã du c ch n, ch n H.323 Gatekeeper Administration Tools sau dó kích OK.

Trong h p tho i Microsoft ISA Server (Enterprise Edition) Setup, ch n Custom Installation kích Continue. H p tho i Microsoft Internet Security and Acceleration Server Setup xu t hi n, luu ý b n r ng máy tính không th tham gia vào array. B n s c u hình máy tính này là m t stand-alone server

Kích Yes d c u hình máy tính này là m t stand-alone server.

Trong h p tho i Microsoft ISA Server Setup d c mô t các mode cài d t d m b o r ng mode Integrated dã du c l a ch n sau dó kích Continue.

Trong h p tho i Microsoft Internet Security and Acceleration Server Setup d c thông báo v IIS publishing sau dó kích OK d bi t r ng ISA Server Setup dang d ng d ch v IIS publishing.

Kích OK và d t ng m d nh các giá tr thi t d t cho cache.

Bu c 2: C u hình LAT d khai báo d a ch cho m ng riêng.

Trong h p tho i Microsoft Internet Security and Acceleration Server 2000 Setup kích Construct Table. Luu ý r ng khi b n thêm vào không dúng d a ch IP vào LAT, ISA server s chuy n ti p sai các gói tin do dó các máy client s không th truy c p Internet

Trong h p tho i Local Address Table, kích d xóa Add the following private ranges: 10.x.x.x, 192.168.x.x and 172.16.x.x-172.31.x.x

Ch n adapter ip_address (v i tên c c m ng và d a ch IP là d a ch m ng riêng), sau dó kích OK.

Trong thông báo Setup Message, kích OK.

Trong Internal IP Ranges, kích 10.255.255.255-10.255.255.255, sau dó kích Remove.

Ki m tra r ng Internal IP Ranges ch ch a IP addresses trong m ng trong c a b n sau dó kích OK.

K t thúc vi c cài d t ISA Server và i t o c u hình ISA Server.

Trong h p tho i Launch ISA Management Tool, kích d xóa Start ISA Server Getting Started Wizard check box, sau dó kích OK.

Trong h p thông báo Microsoft ISA Server (Enterprise Edition) Setup kích OK.

Đóng c a sMicrosoft ISA Server Setup.

L y dia Microsoft Internet Security and Acceleration Server Enterprise Edition t dia CD-ROM.

Bu c 3: C u hình Default Web Site trong Internet Information Services s d ng c ng 8008, sau dó kh i d ng Default Web Site.

M Internet Services Manager t Administrative Tools.

Trong Internet Information Services, m r ng server(server là tên máy tính c a b n), sau dó kích DefaultWeb Site (Stopped).

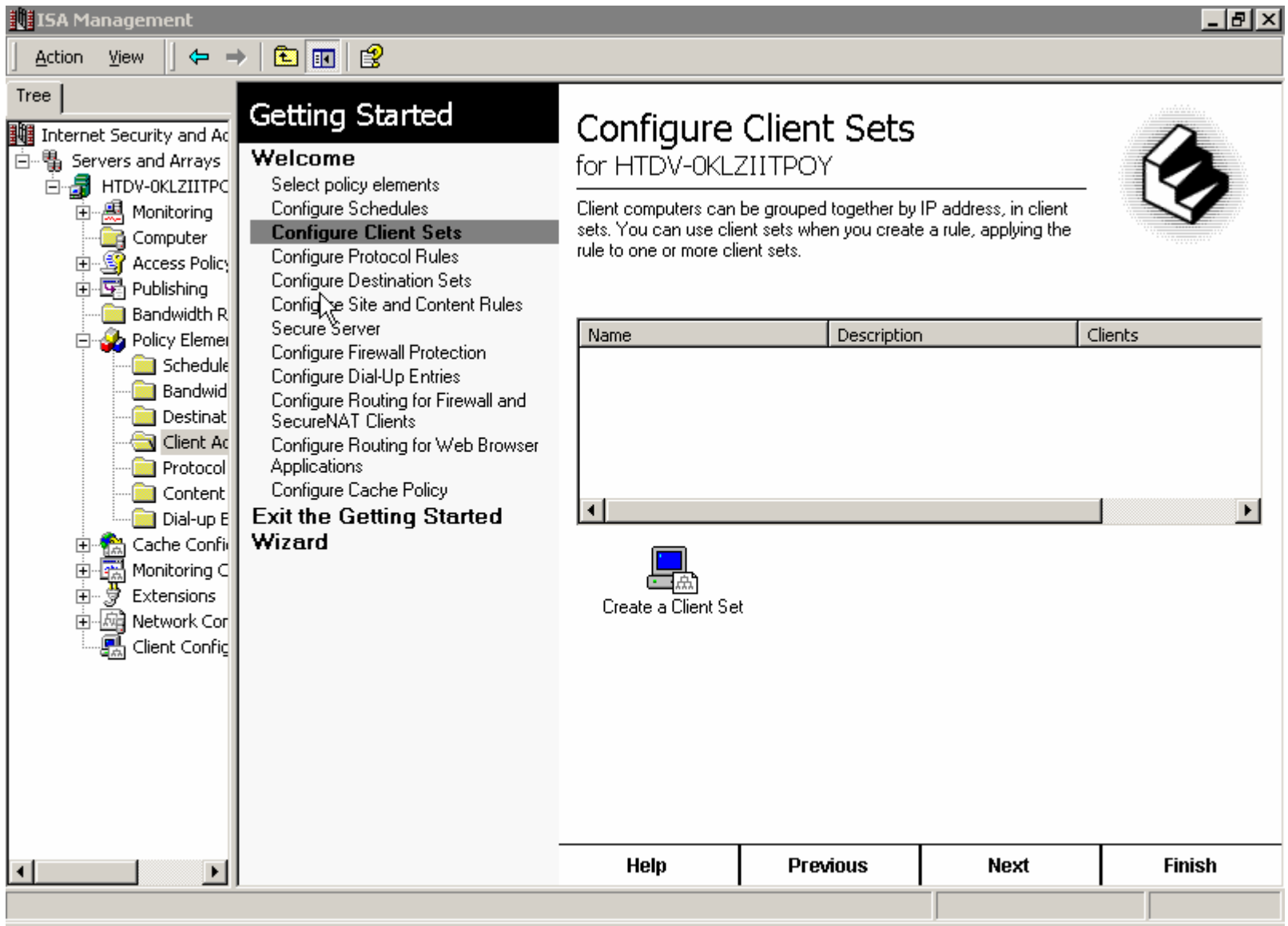
Kích chu t ph i Default Web Site (Stopped), sau dó kích Properties. Vì ISA Server s d ng các c ng 80 and 8080, b n ph i c u hình IIS d ph c v các k t n i t các client t i trên c ng khác. B n s c u hình IIS d ph c c các yêu c u này trên c ng TCP 8008.

Trong h p tho i Default Web Site (Stopped) Properties, trong h p TCP Port, gõ 8008 sau dó kích OK.

Kích chu t ph i Default Web Site (Stopped), sau dó kích Start.

Bài 2: C u hình ISA Server 2000 cho phép m t m ng n i b có th truy c p, s d ng các d ch v co b n trên Internet qua 01 modem k t n i qua m ng PSTN.

Bu c 1 : C u hình và qu n tr c u hình cho ISA server s d ng Getting Started V i Getting Started Wizard, có các l a ch n c u hình sau:



Select Policy elements, c
hình ng m d nh ch n t t
các thành ph n d có
th s d ng khi t ocác qui
c.
Configure Schedules, c
hình ng m d nh có hai l
là Weekends và Work
Hours, ta có th s a các l
này ho c t o các l ch m i.
Configure Client sets, c
máy tính Client có th t
thành nhóm v i nhau
b ng các d a ch IP s d
chom c dích t o các qui t
ng v i t ng nhóm
client
Configure Protocol Rul
dua ra các qui t c giao th

d các client s d ng
truy nh p Internet

Configure Destination Sets, cho phép thi t l p các máy tính trên m ng Internet thành nhóm b i tên hay d a ch IP. Destination Sets du c s d ng d t o ra các qui t c, áp d ng các qui t c cho m t hay nhi u Destination Sets
Configure Site and Content Rules, c u hình các qui t c v n i dung.
Secure Server cho phép b n có th d t các m c d b o v thích h p cho m ng.
Configure Filewall Protection, Packet Fitering b o d m cho ISA server s l c không có packet nào qua tr khi du c phép
Cofigure Dial-Up Entries, cho phép ch n giao di n d k t n i v i Internet
Configure Routing for filewall and secure Nat client.
Configure Routing for Web browser Appilications cho phép t o các qui t c d nh tuy n, xác d nh rõ yêu c u t Web Proxy Client du c g i tr c ti p t i Internet hay t i Upstream server
Configure Cache policy, c u hình các chính sách v cache.

Bu c 2: C u hình ISA server cho phép các client s d ng du c các d ch v c a Internet qua m ng tho i công c ng

T o m t Dial-Up Entries, d k t n i v i Internet Bu c 2: T o m t qui t c giao th c.

M ISA Management, kích Servers and arrays, sau dó kích tên máy ch ISA.
Kích Access Policy, kích chu t ph i vào Protocol Rule, sau dó ch n New -> Rule.
Đ t tên c a Protocol Rule, sau dó kích Next.
Ki m tra r ng **Allow** dã du c ch n , kích Next, sau dó ch n **All IP traffic** , kích Next Ch n **Always** , kích Next sau dó ch n **Any Request** , kích Next, sau dó kích Finish.

Bu c 3: C u hình Web Proxy Client: c u hình Internet Explorer d s d ng ISA server d i v i các yêu c u truy c p d ch v Web.

M trình duy t Internet Explorer.
Trong Internet Connection Wizard, kích Cancel.
Trong h p tho i Internet Connection Wizard, ch n Do not show the Internet Connection wizard in the future, sau dó kích Yes.
Trong Internet Explorer, trong ô Address , gõ http://vdc.com.vn sau dó ch n ENTER. Internet Explorer không th k t n i t i trang web này.
Trong menu Tools, kích Internet Options.
Trong h p tho i Internet Options, trong Connections kích LAN Settings.
Trong h p tho i Local Area Network (LAN) Settings , kích d b l a ch n Automatically detect settings. Ch n Use a proxy server, trong ô Address gõ vào d a ch IP c a ISA Server .
Trong h p Port, gõ 8080

Ki m tra r ng l a ch n Bypass proxy server for local addresses dã b , sau dó kích OK hai l n.

Bài 3: Thi t d t các chính sách cho các yêu c u truy c p và s d ng các d ch v trên m ng internet.

I.Thi t l p các thành ph n chính sách

Bu c 1: Thi t l p l ch trình

Đang nh p vào h th ng v i quy n administrator

M ISA Management t th c don Microsoft ISA Server.

Trong ISA Management, m r ng Servers and Arrays, m r ng server

(server là tên c a ISA Server), m r ng Policy Elements, sau dó kích Schedules

Kích Create a Schedule d thi t l p m t l ch trình.

Trong h ptho i New schedule trong m c Name dua vào m t tên l ch trình ví d schedule1.

Trong m c Description gõ vào Daily period of most network utilization

Kéo d l a ch n toàn b l ch trình sau dó kích Inactive.

Kéo d l a ch n vùng t th i di m hitri t i 2 h ti p theo d i v i t t c các ngày trong tu n sau dó kích active ví d , n u th i di m hi n t i là 3:15 P.M., thì l a ch n vùng t 3:00 P.M. t i 5:00 P.M. cho t t c các ngày trong tu n.

Kích OK.

Bu c 2: Thi t l p destination set

Trong ISA Management, kích Destination Sets.

Kích Create a Destination Set.

Trong h p tho i New Destination Set trong m c Name cho vào m t tên cho thi t l p m i này ví d set1.

Trong m c Description box, gõ vào m t n i dung mô t cho thi t lip m này

Kích Add.

Trong h p tho i Add/Edit Destination trong m c Destination gõ home.vnn.vn

Bu c 3: Thi t l p client address set

Trong ISA Management kích Client Address Sets.

Kích Create a Client Set.

Trong h p tho i Client Set trong m Name gõ vào m t tên cho thi t l p m i, ví d Accounting Department.

Trong m c Description gõ n i dung mô t cho thi t l p m i này sau dó kích Add.

Trong h p tho i Add/Edit IP Addresses trong m c From gõ vào d a ch b t d u thu c nhóm d a ch thu c m ng dùng riêng
Trong m c To gõ vào d a ch k t thúc thu c nhóm d a ch thu c m ng dùng riêng kích OK hai l n.

Bu c 4: Thi t l p protocol definition (s d ng c ng UDP 39000 cho k t n i chính g i ra và c ng TCP 39000 cho k t n i th hai)

Trong ISA Management kích Protocol Definitions.
Kích Create a Protocol Definition.
Trong New Protocol Definition Wizard trong m c Protocol definition name gõ vào m t tên cho thi t d t m i sau dó kích Next.
Trong trang Primary Connection Information trong m c Port number gõ vào 39000
Trong danh sách Protocol type kích UDP.
Trong danh sách Direction kích Send Receive sau dó kích Next.
Trong trang Secondary Connections kích Yes sau dó kích New.
Trong h p tho i New/Edit Secondary Connection trong m c Port và m c To gõ 39000
Trong danh sách Protocol type ki m tra r ng TCP dã du c l a ch n, trong m c Direction
kích Outbound sau dó kích OK.
Kích Next sau dó trong trang Completing the New Protocol Definition Wizard kích Finish

II.Thi t l p các qui t c giao th c

Bu c 1: Thi t l p m t qui t c giao th c cho phép HTTP, HTTPS và FTP d i v i m i ngu i dùng truy c p Internet t i m i th i di m b ng vi c s d ng các giao th c HTTP, HTTPS và FTP .

M trình duy t Internet Explorer t i m t máy tr m, trong ô Address gõ http://home.vnn.vn nh n ENTER. Trình duy t Internet Explorerkhông th k t n i t i Web site vì ISA Server t ch i yêu c u.
Đóng Internet Explorer.
Trong ISA Management m r ng Access Policy sau dó kích Protocol Rules.
Kích Create a Protocol Rule for Internet Access.
Trong New Protocol Rule Wizard, trong m c Protocol rule name gõ Allow HTTP, HTTPS, and FTP sau dó kích Next.
Trong trang Protocols ki m tra r ng Selected protocols dã du c kích h d xóa Gopher check box sau dó kích Next.
Trong trang Schedule ki m tra r ng Always dã du c l a ch n sau dó kích Next.

Trong trang Client Type ki m tra r ng Any request dã du c ch n, sau dó kích Next.
Trong trang Completing the New Protocol Rule Wizard kích Finish.
M Internet Explorer t i m t máy tính tr m, trong m c Address gõ http://home.vnn.vn sao dó n ENTER. Ki m tra r ng trình duy t k t n i thành công n i dung trang web du c hi n th
Đóng Internet Explorer.
Bu c 2: Thi t l p m t quit c giao th c cho phép ngu i dùng trong nhóm Domain Admins truy c p Internet s d ng t t c các giao th c.
Trong ISA Management kích Create a Protocol Rule.
Trong New Protocol Rule Wizard, trong m c Protocol rule name gõ Allow All Access for Administrators sau dó kích Next.
Trong trang Rule Action ki m tra r ng Allow dã du c ch n sau dó kích Next.
Trong trang Protocols, trong danh sách Apply this rule to ki m tra r ng All IP traffic dã du c ch n sau dó kích Next.
Trong trang Schedule, ki m tra r ng Always dã du c ch n sau dó kích Next.
Trong trang Client Type, kích Specific users and groups, sau dó kích Next.
Trong trang Users and Groups, kích Add.
Trong h p tho i Select Users or Groups, kích Domain Admins, kích Add, sau dó kích OK.
Trong trang Users and Groups, kích Next.
Trong trang Completing the New Protocol Rule Wizard kích Finish.
Bu c 3: Thi t l p m t qui t c giao th c t ch i ngu i dùng trong nhóm Accounting Department dã d nh nghia trong client set truy c p Internet.
Trong ISA Management, kích Create a Protocol Rule.
Trong New Protocol Rule Wizard, trong m c Protocol rule name gõ vào Deny Access from Accounting Department , sau dó kích Next.
Trong trang Rule Action, kích Deny, sau dó kích Next.
Trong trang Protocols, trong danh sách Apply this rule to, ki m tra r ng All IP traffic dã du c l a ch n, sau dó kích Next.
Trong trang Schedule, ki m tra r ng Always dã du c l a ch n, sau dó kích Next.
Trong trang Client Type, kích Specific computers (client address sets), sau dó kích Next.
Trong trang Client Sets, kích Add.

Trong h p tho i Add Client Sets, kích Accounting Department, kích Add, sau dó kíchOK.
Trong trang Client Sets, kích Next.
Trong trang Completing the New Protocol Rule Wizard, kích Finish.
Ki m tra d xác nh n vi c truy c p không thành công t nhóm nhóm Accounting Department
Bu c 4: Xóa qui t c giao th c t ch i ngu i dùng trong nhóm Accounting Department

Trong In ISA Management, kích Deny Access from Accounting Department
Kích Delete a Protocol Rule.
Trong h p tho i Confirm Delete, kích Yes.

III.Thi t l p các qui t c n i dung

Bu c 1: Thi t l p m t qui t c n i dung d t ch i truy c p t i n i dung dã du c d nh nghia trong destination set và v i l ch trình dã thi t l p m c 1
Trong ISA Management, kích Site and Content Rules.
Kích Create a Site and Content Rule.
Trong New Site and Content Rule Wizard, trong m c Site and content rule name, gõ vào m t tên ví d Deny Access Rule sau dó kích Next.
Trong trang Rule Action, ki m tra r ng Deny dã du c ch n, sau dó kích Next.
Trong trang Destination Sets, trong danh sách Apply this rule to, kích Specified destination set.
Trong danh sách Name, l a ch n set1 (dã thi t l p ph n trên), sau dó kích Next.
Trong trang Schedule, ch n schedule1 (dã thi t l p ph n trên), sau dó kích Next.
Trong trang Client Type, ki m tra r ng Any request dã du c ch n, sau dó kích Next.
Trong trang Completing the New Site and Content Rule Wizard, kích Finish.

Bu c 2:
Ki m tra qui t c v a thi t l p
M trình duy t Internet Explorer.
Trong ô Address, gõ http://home.vnn.vn sau dó n ENTER. ki m tra r ng trang web này không du c hi n th , vì qui t c n i dung dã thi t l p trên dã có hi u l c
Đóng trình duy t Internet Explorer

Chuong 6 - B o m t h th ng và Firewall

Chuong 6 t p trung vào các n i dung quan tr ng v b o m t h th ng và m ng lu i. N i dung c a ph n th nh t chuong 6 cung c p cho các h c viên khái ni m v các hình th c t n công m ng, các l h ng, di m y u c a m ng lu i. Các k nang co b n trong ph n m t c a chuong 6 giúp ngu i qu n tr qu n lý và xây d ng các chính sách b o m t tuong ng cho các thành ph n m ng, h th ng hay d ch v ngay t lúc b t dout hd ng.

Ph n 2 c a chuo ng 6 t p trung gi i thi u v thi t b b o m t m nh và thông d ng trên m ng. Đ ó là thi t b b c tu ng l a (firewall). H c viên s có du c các ki n th c v c u trúc firewall, các ch c nang co b n và cách phân lo i cung nhu **u** nhu c di m c a các lo i firewall ho t d ng theo các nguyên lý khác nhau. Nh ng k nang thi t l p c u hình, lu t, qu n tr firewall v i mô hình firewall checkpoint s giúp cho các h c viên hi u c th và các công vi c qu n tr và b o m t h th ng mgn

Chuong 6 yêu c u các h c viên trang b r t nhi u các ki n th c co b n nhu n m v ng các ki n th c qu n tr h th ng OS windows, linux, unix. H c viên c n hi u sâu v giao th c TCP/IP, ho t d ng c a IP hay UDP, TCP. H c viên c n có hi u bi t v các pto socket c a các giao th c d ch v nhu SMTP, POP3, WWW...Các ki n th c du c trang b trong các giáo trình qu n tr h th ng ho c các tài li u, sách giáo khoa v n i dung trên h c viên nên tham kh o tru c khi h c chuong 6 này.

1. B o m t h th ng

1.1. Các v n d chung v b o m t h th ng và m ng

Do d c di m c a m t h th ng m ng là có nhi u ngu i s d ng và phân tán v m t d a lý nên vi c b o v các tài nguyên (m t mát, ho c s d ng không h p l) trong môi tru ng m ng ph c t p hon nhi u so vôi tru ng m t máy tính don l , ho c m t ngu i s d ng.

Ho t d ng c a ngu i qu n tr h th ng m ng ph i d m b o các thông tin trên m ng là tin c y và s d ng dúng m c dích, d i tu ng d ng th i d m b o m ng ho t d ng n d nh, không b t n công b inh k phá ho i.

Có m t th c t là không m t h th ng m ng nào d m b o là an toàn tuy t d i, m t h th ng dù du c b o v ch c ch n d n m c nào thì cung có lúc b vô hi u hoá b i nh ng k có ý d x u.

1.1.1. M t s khái ni m và l ch s b o m t h th ng

Tru c khi tìm hi u các v n d liên quan d n phuong th c phá ho i và các bi n pháp b o v cung nhu thi t l p các chính sách v b o m t, ta s tìm hi u m t s khái ni m liên quan d n b o m t thông tin trên m ng Internet.

1.1.1.1. M t s khái ni m

a) Đ i tu ng t n công m ng (Intruder):

Là nh ng cá nhân ho c các t ch c s d ng các ki n th c v m ng và các công c phá ho i (ph n m m ho c ph n c ng) d dò tìm các di m y u, l h ng b o m t trên h th ng, th c hi n các ho t d ng xâm nh p và chi m do t tài nguyên m ng trái phép.

M t s d i tu ng t n công m ng là:

- Hacker: Là nh ng k xâm nh p vào m ng trái phép b ng cách s d ng các công c phá m t kh u ho c khai thác các di m y u c a các thành ph n truy nh p trên h th ng.

- Masquerader: Là nh ng k gi m o thông tin t m ng. Có m t s hình th c nhu gi m o d a ch IP, tên mi n, d nh danh ngu i dùng ...

- Eavesdropping: Là nh ng d i tu ng nghe tr m thông tin trên m ng, s d ng các công c sniffer; sau dó dùng các công c phân tích và debug d l y du c các thông tin có giá tr .

Nh ng d i tu ng t n công m ng có th nh m nhi u m c dích khác nhau nhu: an c p nh ng thông tin có giá tr v kinh t , phá ho i h th ng m ng có ch d nh, ho c cung có th ch là nh ng hành d ng vô ý th c, th nghi m các chuong trình không ki m tra c n th n ...

b) Các l h ng b o m t:

Các l h ng b o m t là nh ng di m y u trên h th ng ho c n ch a trong m t d ch v mà d a vào dó k t n công có th xâm nh p trái phép d th c hi n các hành d ng phá ho i ho c chi m do t tài nguyên m t cách bt pháp.

Nguyên nhân gây ra nh ng l h ng b o m t là khác nhau: Có th do l i c a b n thân h th ng, ho c ph n m m cung c p, ho c do ngu i qu n tr y u kém không hi u sâu s c các d ch v cung c p ...

M c d nh hu ng c a các l h ng là khác nhau nhung l h ng ch nh hu ng t i ch t lu ng d ch v cung c p, có nh ng l h ng nh hu ng nghiêm tr ng t i toàn b h th ng ...

c) Chính sách b o m t:

Là t p h p các qui t c áp d ng cho m i d i tu ng có tham gia qu n lý và s d ng các tài nguyên và d ch v m ng.

M c tiêu c a chính sách b o m t giúp ngu i s d ng bi t du c trách nhi m c a mình trong vi c b o v các tài nguyên thông tin trên m ng , d ng th i giúp các nhà qu n tr thi t l p các bi n pháp b o d m h u hi u trong quá trình trang b , c u hình, ki m soát ho t d ng c a h th ng và m ng

M t chính sách b o m t du c coi là hoàn h o n u nó xây d ng g m các van b n pháp qui, kèm theo các công c b o m t h u hi u và nhanh chóng giúp ngu i qu n tr phát hi n, ngan ch n các xâm nh p trái.phép

1.1.1.2. L ch s b o m t h th ng

Có m t s s ki n dánh d u các ho t d ng phá ho i trên m ng, t dó n y sinh các yêu c u v b o m t h th ng nhu sau:

- Nam 1988: Trên m ng Internet xu t hi n m t chuong trình t nhân phiên b n c a chính nó lên t t c các máy trên m ng Internet. Các chuong trình này g i là "sâu". Tuy m c d nguy h i c a nó không l n, nhung nó d t ra các v n d d i v i nhà qu n tr v quy n truy nh p h th ng, cung nhu các l i ph n m m.

- Nam 1990: Các hình th c truy n Virus qua d a ch Email xu t hi n và bi n trên m ng Internet.

- Nam 1991: Phát hi n các chuong trình trojans.

Cùng th i gian này s phát tri n c a d ch v Web và các công ngh liên quan nhu Java, Javascipts dã có r t nhi u các thông báo l i v b o m t liên quan nhu: các l h ng cho phép d c n i dung các file d li u c a ngu i dùng, m t s l h ng cho phép t n công b ng hình th c DoS, spam mail làm ngung tr d ch v .

- Nam 1998: Virus Melisa lan truy n trên m ng Internet thông qua các chuong trình g i mail c a Microsoft, gây nh ng thi t h i kinh t không nh .

- Nam 2000: M t lo t các Web Site l n nhu yahoo.com và ebay.com b tê li t, ng ng cung c p d ch v trong nhi u gi do b t n công b i hình th c DoS.

1.1.2. Các l h ng và phuong th c t n công m ng ch y u

1.1.2.1. Các l h ng

Nhu ph n trên dã trình bày, các l h ng b o m t trên m t h th ng là các di m y u có th t o ra s ngung tr c a d ch v , thêm quy n d i v i ngu i s d ng ho c cho phép các truy nh p không h p pháp vào h th ng. Các l h ng cung có th n m ngay các d ch v cung c p nhu sendmail, web, ftp ... Ngoài ra các l h ng còn t n t i ngay chính t i h di u hành nhu trong Windows NT, Windows 95, UNIX ho c trong các ng d ng mà ngu i s d ng thu ng xuyên s d ng nhu word processing, các h databases.

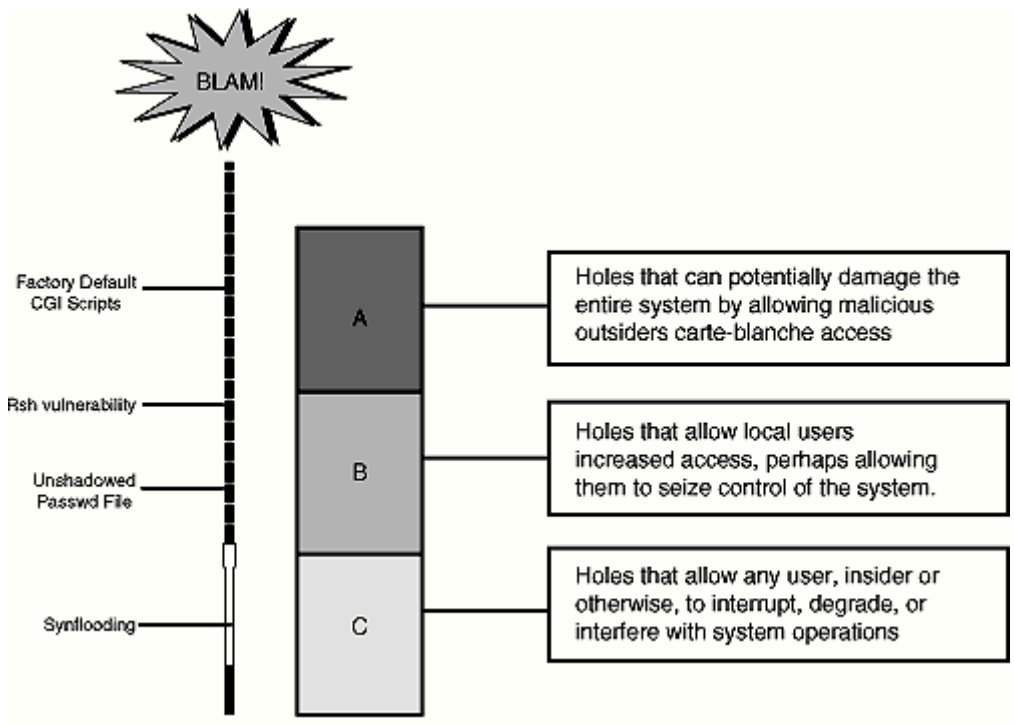
Có nhi u t ch c khác nhau ti n hành phân lo i các d ng l h ng d c biêt. Theo cách phân lo i c a B qu c phòng M , các lo i l h ng b o m t trên m t h th ng du c chia nhu sau:

- L h ng lo i C: các l h ng lo i này cho phép th c hi n các phuong th c t n công theo DoS (Denial of Service-Ts ch i d ch v). M c d nguy hi m th p, ch nh hu ng t i ch t lu ng d ch v , có th làm ngung tr , gián do n h th ng; không làm phá h ng d li u ho c d t du c quy n truy nh p b t h p pháp.

- L h ng loi B: Các l h ng cho phép ngu i s d ng có thêm các quy n trên h th ng mà không c n th c hi n ki m tra tính h p l nên có th d n d n m t mát ho c l thông tin yêu c u b o m t. M c d nguy hi m trung bình. Nh ng l h ng này thu ng có trong các ng d ng h th ng.

- L h ng lo i A: Các l h ng này cho phép ngu i s d ng ngoài cho th truy nh p vào h th ng b t h p pháp. L h ng này r t nguy hi m, có th làm phá h y toàn b h th ng.

Hình sau minh h a các m c d nguy hi m và lo i l h ng tuong ng:



Hình 6.1: Các lo i l h ng b o m t và m c d ngu y hi m

Sau dây ta s phân tích m t s l h ng b o m t thu ng xu t hi n trên m ng và h th ng.

a) Các l h ng lo i C

Các l h ng lo i này cho phép th c hi n các cu c t n công DoS.

DoS là hình th c t n công s d ng các giao th c t ng Internet trong b giao th c TCP/IP d làm h th ng ngu ng tr d n d n tình tr ng t ch i ngu i s d ng h p pháp truy nh p hay s d ng h th ng. M t s lu ng l n các gói tin du c g i t i server trong kho ng th i gian liên t c làm cho h th ng tr nên quá t i, k t qu là server dáp ng ch m ho c không th dáp ng các yêu c u t client g i t i.

Các d ch v có l h ng cho phép th c hi n các cu c t n công DoS có th du c nâng c p ho c s a ch a b ng cách cài các b n m i hon c a các nhà cung c p d ch v . Hi n nay, chua có m t gi i pháp toàn di n nào d kh c ph c các l

h ng lo i này vì b n thân vi c thi t k giao th c t ng Internet (IP) nói riêng và b giao th c TCP/IP dã ch a d ng nh ng nguy co ti m tàng c a các l h ng này.

Ví d di n hình c a phuong th c t n công DoS là các cu c t n công vào m t s Web Site l n làm ngung tr ho t d ng c a web site này nhu: www.ebay.com và www.yahoo.com.

Tuy nhiên, m c d nguy hi m c a các l h ng lo i này du c x p lo i C, ít nguy hi m vìchúng ch làm gián do n s cung c p d ch v c a h th ng trong m t th i gian mà không làm nguy h i d n d li u và nh ng k t n công cung không d t du c quy n truy nh p b t h p pháp vào h th ng.

M t l h ng lo i C khác cung thu ng th y dó là các di m cung c p d ch v cho phép th c hi n t n công làm ngu ng tr h th ng c a ngu i s d ng cu i. Ch y u hình th c t n công này là s d ng d ch v Web. Gi s trên m t Web Server có nh ng trang Web trong dó có ch a các do n mã Java ho c JavaScripts, làm 'treo" h th ng c a ngu i s d ng trình duy t Web c a Netscape b ng các bu c sau:

- Vi t các do n mã d nh n bi t du c Web Browers s d ng Netscape.

- N u s d ng Netscape, s t o m t vòng l p vô th i h n, sinh ra vô s các c a s , trong m i c a s dó l n các Web Server khác nhau.

V i m t hình th c t n công don gi n này, có th làm treo h th ng trong kho ng th i gian 40 giây (d i v i máy client có 64 MB RAM). Đây cùng là m t hình th c t n công ki u DoS. Ngu i s d ng trong tru ng h p này ch có th kh i d ng l i h th ng.

M t l h ng lo i C khác cung thu ng g p d i v i các h th ng mail là không xây d ng các co ch anti-relay (ch ng relay) cho phép th c hi n các hành d ng spam mail. Nhu chúng ta dã bi t, co ch ho t d ng c a d ch v thu di n t là luu và chuy n ti p. M t s h th ng mail không có các xác th c khi ngu i dùng g i thu, d n d n tình tr ng các d i tu ng t n công l i d ng các máy ch mail này d th c hi n spam mail. Spam mail là hành d ng nh m làm tê li t d ch v mail c a h th ng b ng cách g i m t s lu ng l n các message t i m t d a ch không xác d nh, vì máy ch mail luôn ph i t n nang l c di tìm nh ng d a ch không có th c d n d n tình tr ng ngung tr d ch v . Các message có th sinh ra t các chuong trình làm bom thu phi tbi n trên m ng Internet.

b) Các l h ng lo i B:

L h ng lo i này có m c d nguy hi m hon l h ng lo i C, cho phép ngu i s d ng n i b có th chi m du c quy n cao hon ho c truy nh p không h p pháp.

Ví d trên hình 12, l h ng lo i B có th có v i m t h th ng UNIX mà file /etc/passwd d d ng plaintext; không s d ng co ch che m t kh u trong UNIX (s d ng file /etc/shadow)

Nh ng l h ng lo i này thu ng xu t hi n trong các d ch v trên h th ng. Ngu i s d ng local du c hi u là ngu i dã quy n truy nh p vào h th ng v i m t s quy n h n nh t d nh.

Một lỗi các vấn đề về quyền sử dụng chương trình trên UNIX cũng thường gây nên các lỗ hổng lỗi B. Vì trên hệ thống UNIX một chương trình có thể được thực thi với 2 khả năng:

- Người chủ sở hữu chương trình đó kích hoạt chương trình.
- Người mang quyền của người sở hữu file đó kích hoạt chương trình.

Một dạng khác của lỗ hổng lỗi B xảy ra đối với các chương trình có mã nguồn viết bằng C. Những chương trình viết bằng C thường sử dụng một vùng đệm - một vùng trong bộ nhớ để lưu dữ liệu được truyền khi xử lý. Những người lập trình thường sử dụng vùng đệm trong bộ nhớ được truyền khi gán một không gian bộ nhớ cho từng khối dữ liệu. Ví dụ, người sử dụng viết chương trình nhập trường tên người sử dụng, quy định trường này là 20 ký tự. Do đó hệ thống khai báo:

char first_name [20];

Khai báo này sẽ cho phép người sử dụng nhập vào tối đa 20 ký tự. Khi nhập dữ liệu, trước tiên dữ liệu được lưu vùng đệm; nếu người sử dụng nhập vào 35 ký tự sẽ xảy ra hiện tượng tràn vùng đệm và kết quả 15 ký tự dư thừa sẽ nằm một vị trí không kiểm soát được trong bộ nhớ. Đối với những kẻ tấn công, có thể lợi dụng lỗ hổng này để nhập vào những ký tự được biết, để thực thi một số lệnh được biết trên hệ thống. Thông thường, lỗ hổng này được sử dụng để lại những người sử dụng bình thường người sử dụng trên hệ thống để đạt được quyền root không hợp lệ.

Việc kiểm soát chặt chẽ cấu hình hệ thống và các chương trình sẽ hạn chế được các lỗ hổng lỗi B.

c) Các lỗ hổng lỗi A:

Các lỗ hổng lỗi A có mức độ rất nguy hiểm, dễ dàng tính toán với và bảo mật của hệ thống. Các lỗ hổng lỗi này thường xuất hiện những hệ thống quản trị yếu kém hoặc không kiểm soát được cấu hình mạng.

Một ví dụ thường thấy là trên nhiều hệ thống sử dụng Web Server là Apache, Đối với Web Server này thường cấu hình thư mục mặc định chạy các script là cgi-bin; trong đó có một Scripts được viết sẵn để thử hoạt động của apache là test-cgi. Đối với các phiên bản cũ của Apache (trước version 1.1), có dòng sau trong file test-cgi:

echo QUERY_STRING = $QUERY_STRING

Biến môi trường QUERY_STRING do không được đặt trong có dấu " (quote) nên khi phía client thực hiện một yêu cầu trong đó chứa ký tự đặc biệt; ví dụ ký tự "*", web server sẽ trả về nội dung của toàn bộ thư mục hiện thời (là các thư mục chứa các script cgi). Người sử dụng có thể nhìn thấy toàn bộ nội dung các file trong thư mục hiện thời trên hệ thống server.

Một ví dụ khác cũng xảy ra tương tự đối với các Web server chạy trên hệ điều hành Novell: các web server này có một scripts là convert.bas, chạy scripts này cho phép đọc toàn bộ nội dung các files trên hệ thống.

Nh ng l h ng lo i này h t s c nguy hi m vì nó dã t n t i s n có trên ph n m m s d ng, ngu i qu n tr n u không hi u sâu v d ch v và ph n m m s d ng s có th b qua nh ng di m y u này.

Đ i v i nh ng h th ng cu, thu ng xuyên ph i ki m tra các thông báo c a các nhóm tin v b o m t trên m ng d phát hi n nh ng l h ng lo i này. M t lo t các chuong trình phiên b n cu thu ng s d ng có nh ng lo i A nhu: FTP, Gopher, Telnet, Sendmail, ARP, finger...

1.1.2.2. M t s phuong th c t n công m ng ph bi n

a) Scanner

Scanner là m t chuong trình t d ng rà soát và phát hi n nh ng di m y u v b o m t trên m t tr m làm vi c c c b hoc trên m t tr m xa. V i ch c nang này, m t k phá ho i s d ng chuong trình Scanner có th phát hi n ra nh ng l h ng v b o m t trên m t server xa.

Các chuong trình scanner thu ng có m t co ch chung là rà soát và phát hi n nh ng port TCP/UDP du c s ng trên m t h th ng c n t n công t dó phát hi n nh ng d ch v s d ng trên h th ng dó. Sau dó các chuong trình scanner ghi l i nh ng dáp ng trên h th ng xa tuong ng v i các d ch v mà nó phát hi n ra. D a vào nh ng thông tin này, nh ng k có th tìm ra nh ng di m y u trên h th ng.

Nh ng y u t d m t chuong trình Scanner có th ho t d ng nhu sau:

- Yêu c u v thi t b và h th ng: M t chuong trình Scanner có th ho t d ng du c n u môi tru ng dó có h tr TCP/IP (b t k h th ng nào là UNIX, máy tính tuong thích v i IBM, ho c dòng máy Macintosh).
- H th ng dó ph i k t n i vào m ng Internet.

Tuy nhiên không ph i don gi n d xây d ng m t chuong trình Scanner, nh ng k phá ho i c n có ki n th c sâu v TCP/IP, nh ng ki n th c v l trình C, PERL và m t s ngôn ng l p trình shell. Ngoài ra ngu i l p trình (ho c ngu i s d ng) c n có ki n th c là l p trình socket, phuong th c ho t d ng c a các ng d ng client/server.

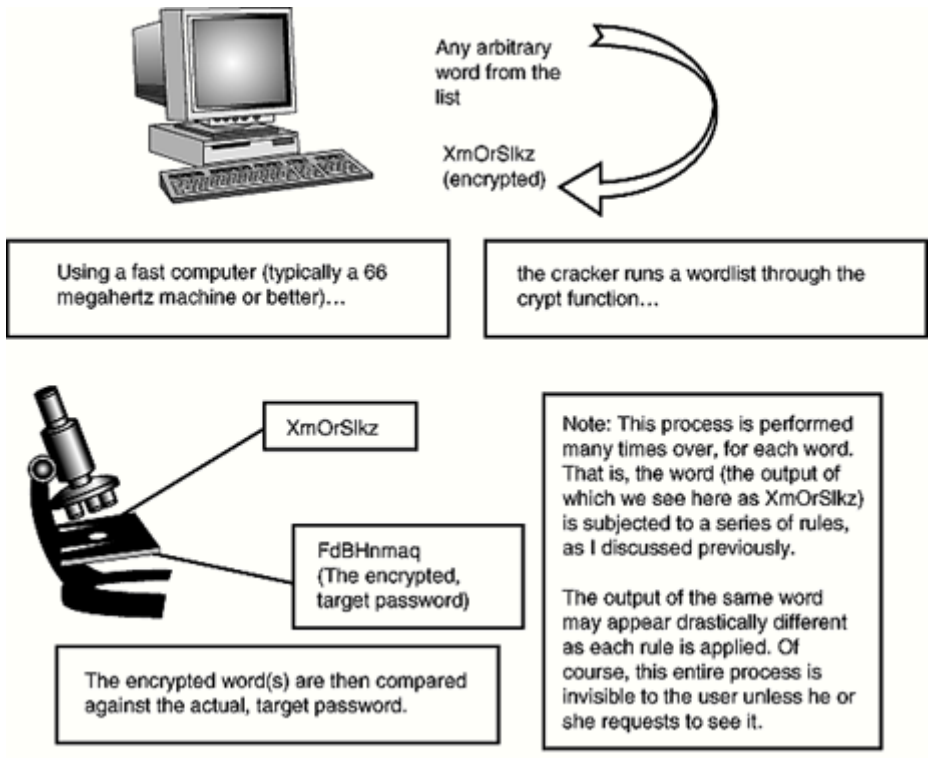
Các chuong trình Scanner có vai trò quan tr ng trong m t h th ng b o m t, vì chúng có kh nang phát hi n ra nh ng di m y u kém trên m t h th ng m ng. Đ i v i ngu i qu n tr m ng nh ng thông tin này là h t s c h u ích và c n thi t; d i v i nh ng k phá ho i nh ng thông tin này s h t s c nguy hi m.

b) Password Cracker

Password cracker là m t chuong trình có kh nang gi i mã m t m t kh u dã du c mã hoá ho c có th vô hi u hoá ch c nang b o v m t kh u c a m t h th ng.

Đ hi u cách th c ho t d ng c a các chuong trình b khoá, chúng ta c n hi u cách thc mã hoá d t o m t kh u. H u h t vi c mã hoá các m t kh u du c t o ra t m t phuong th c mã hoá. Các chuong trình mã hoá s d ng các thu t toán mã hoá d mã hoá m t kh u.

Quá trình ho t d ng c a các chuong trình b khoá du c minh ho trong hình sau:



Hình 6.2: Ho t d ng c a các chuong trình b khóa

Theo so d trên, m t danh sách các t du c t o ra và du c mã hoá d i v i t ng t . Sau m i l n mã hoá, chuong trình s so sánh v i m t kh u dã mã hoá c n phá. N u không th y trùng h p, quá trình quay l i. Phuong th c b khoá này g i là brute-force.

Y u t v thi t b ph n c ng: Trong hình trên máy tính th c hi n các chuong trình phá khoá là m t máy PC 66MHz ho c c u hình cao hon. Trong th c t yêu c u các thi t b ph n c ng r t m nh d nh ng k phá khoá chuyên nghi p. M t phuong th c khác có th thay th là th c hi n vi c phá khoá trên m t h th ng phân tán; do v y gi m b t du c các yêu c u v thi t b so v i phuong pháp làm t i m t máy.

Nguyên t c c a m t s chuong trình phá khóa có th khác nhau. M t vài chuong trình t o m t m t danh sách các t gi i h n, áp d ng m t s thu t toán mã hoá, t k t qu so sánh v i password dã mã hoá c n b khoá d t o ra m t danh sách khác theo m t lôgic c a chuong trình, cách này tuy không tuc nhung khá nhanh vì d a vào nguyên t c khi d t m t kh u ngu i s d ng thu ng tuân theo m t s qui t c d thu n ti n khi s d ng.

Đ n giai do n cu i cùng, n u th y phù h p v i m t kh u dã du c mã hoá, k phá khoá s có du c m t kh u d ng text thông thu ng. Trong hình trê m t kh u d ng text thông thu ng du c ghi vào m t file.

Đ dánh giá kh nang thành công c a các chuong trình b khoá ta có công th c sau:

P = L x R /S

Trong dó:

P: Xác su t thành công

L: Th i gian s ng c a m t m t kh u

R: T c d th

S: Khônggian m t kh u = A (M là chi u dài m t kh u)

Ví d , trên h th ng UNIX ngu i ta dã ch ng minh du c r ng n u m t kh u dài quá 8 ký t thì xác su t phá khoá g n nhu = 0. C th nhu sau:

N u s d ng kho ng 92 ký t có th d t m t kh u, không gian kh u có th có là S = 92

V i t c d th là 1000 m t kh u trong m t giây có R = 1000/s

Th i gian s ng c a m t m t kh u là 1 nam

Ta có xác su t thành công là :

P = 1x 365 x 86400 x 1000/92 = 1/1.000.000

Nhu v y vi c dò m t kh u là không th s m t kho ng 100 nam m i tìm ra m t kh u chính xác.

Thông thu ng các chuong trình phá khoá thu ng k t h p m t s thông tin khác trong quá trình dò m t kh u nhu:

- Các thông tin trong t p tin /etc/passwd
- M t s t di n
- T l p và các t li t k tu n t , chuy n d i cách phát âm c a m t t ...

Bi n pháp kh c ph c d i v i cách th c phá ho i này là c n xây d ng m t chính sách b o v m t kh u dúng d n.

c) Trojans

D a theo truy n thuy t c Hy l p "Ng a thành Troja", trojans là m t chuong trình ch y không h p l trên m t h th ng v i vai trò nhu m t chuong trình h p pháp. Nh ng chuong trình này th c hi n nh ng ch c nang mà ngu i s d ng h th ng thu ng không mong mu n ho c không h p pháp. Thông thu ng, trojans có th ch y du c là do chuong trình h p pháp dã b thay d i mã c a nó b ng nh ng mã b t h p pháp.

Các chuong trình virus là m t lo i di n hình c a Trojans. Nh ng chuong trình virus che d u các do n mã trong các chuong trình s d ng h p

pháp. Khi nh ng chuong trình này du c kích ho t thì nh ng dã m d u s du c th c thi d th c hi n m t s ch c nang mà ngu i s d ng không bi t.

M t d nh nghia chu n t c v các chuong trình Trojans nhu sau: chuong trình trojans là m t chuong trình th c hi n m t công vi c mà ngu i s d ng không bi t tru c, ng nhu an c p m t kh u hay copy file mà ngu i s d ng không nh n th c du c.

Nh ng tác gi c a các chuong trình trojan xây d ng m t k t ho ch. Xét v khía c nh b o m t trên Internet, m t chuong trình trojan s th c hi n m t trong nh ng công vi c sau:

- Th c hi n m t vài ch c nang ho c giúp ngu i l p trình phát hi n nh ng thông tin quan tr ng ho c thông tin cá nhân trên m t h th ng ho c m t vài thành ph n c a h th ng dó

- Che d u m t vài ch c nang ho c giúp ngu i l p trình phát hi n nh ng thôngtin quan tr ng ho c thông tin cá nhân trên m t h th ng ho c m t vài thành ph n c a h th ng dó

M t vài chuong trình trojan có th th c hi n c 2 ch c nang này. Ngoài ra, m t s chuong trình trojans còn có th phá hu h th ng b ng cách phá ho i các thông tin trên c ng (ví d truòng h p c a virus Melisa lây lan qua du ng thu di n t).

Hi n nay v i nhi u k thu t m i, các chuong trình trojan ki u này d dàng b phát hi n và không có kh nang phát huy tác d ng. Tuy nhiên trong UNIX vi c phát tri ncác chuong trình trojan v n h t s c ph bi n.

Các chuong trình trojan có th lây lan qua nhi u phuong th c, ho t d ng trên nhi u môi tru ng h di u hành khác nhau (t Unix t i Windows, DOS). Đ c bi t trojans thu ng lây lan qua m t s d ch v ph bi n nhu Mail, FTP... ho c qua các ti n ích, chuong trình mi n phí trên m ng Internet.

Vi c dánh giá m c d nh hu ng c a các chuong trình trojans h t s c khó khan. Trong m t vài tru ng h p, nó ch don gi n là nh hu ng d n các truy nh p c a khách hàng nhu các chuong trình trojans l y du c n i dung c a file passwd và g i mail t i k phá ho i. Cách th c s a don gi n nh t là thay th toàn b n i dung c a các chuong trình dã b nh hu ng b i các do n mã trojans và thay th các password c a ngu i s d ng thành ng.

Tuy nhiên v i nh ng tru ng h p nghiêm tr ng hon, là nh ng k tán công t o ra nh ng l h ng b o m t thông qua các chuong trình trojans. Ví d nh ng k t n công l y du c quy n root trên h th ng và l i d ng nó d phá hu toàn b ho c m t ph n c a h th ng. Chúng dùng quy n root d thay d i logfile, cài d t các chuong trình trojans khác mà ngu i qu n tr không th phát hi n. Trong tru ng h p này, m c d nh hu ng là nghiêm tr ng và ngu i qu n tr h th ng dó ch còn cách là cài d t l i toàn b h th ng

d) Sniffer

Đ i v i b o m t h th ng sniffer du c hi u là các công c (có th là ph n c ng ho c ph n m m) "b t" các thông tin luu chuy n trên m ng và t các

thông tin "b t" du c dó d l y du c nh ng thông tin có giá tr trao d i trên m ng.

Ho t d ng c a sniffer cung gi ng nhu các chuong trình "b t" các thông tin gõ t bàn phím (key capture). Tuy nhiên các ti n ích key capture ch th c hi n trên m t tr m làm vi c c th còn d i v i sniffer có th b t du c các thông tin trao d i gi a nhi u tr m làm vi c v i nhau.

Các chuong trình sniffer (sniffer m m) ho c các thi t b sniffer (sniffer c ng) d u th c hi n b t các gói tin t ng IP tr xu ng (g m IP datagram và Ethernet Packet). Do dó, có th th c hi n sniffer d i v i các giao th c khác nhau t ng m ng nhu TCP, UDP, IPX, ...

M t khác, giao th c t ng IP du c d nh nghia công khai, và c u trúc các tru ng header rõ ràng, nên vi c gi i mã các gói tin này không khó khan.

M c dích c a các chuong trình sniffer dó là thi t l p ch d promiscuous (mode dùng chung) trên các card m ng ethernet-nh i các gói tin trao d i trong m ng t dó "b t" du c thông tin.

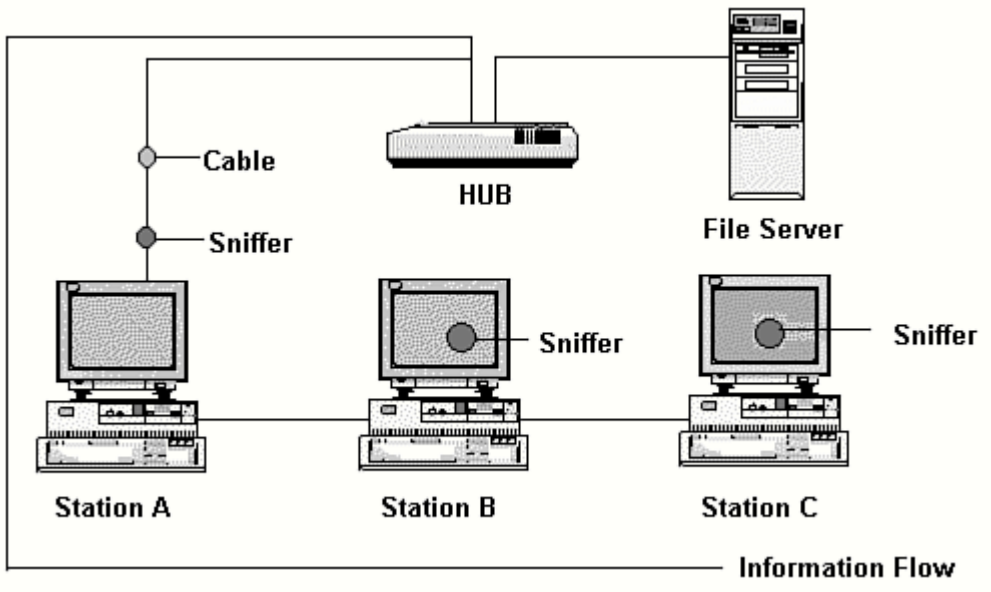
Các thi t b sniffer có th b t du c toàn b thông tin trao d i trên m ng là d a vào nguyên t c broadcast (qu ng bá) các g i tin trong m ng Ethernet.

Trên h th ng m ng không dùng hub, d li u không chuy n d n m t hu ng mà du c luu chuy n theo m i hu ng. Ví d khi m t tr m làm vi c c n du c g i m t thông báo d n m t tr m làm vi c khác trên cùng m t segment m ng, m t yêu c u t tr m dích du c gi i t t c các tr m làm vi c trên m ng d xác d nh tr m nào là tr m c n nh n thông tin (tr m dích). Cho t i khi tr m ngu n nh n du c thông báo ch p nh n t tr m dích thì lu ng d li u s du c g i di. Theo dúng nguyên t c, nh ng tr m khác trên segment s b qua các thông tin trao d i gi a hai tr m ngu n và tr m dích xác d nh. Tuy nhiên, các tr m khác cung không b b t bu c ph i b qua nh ng thông tin này, do dó chúng v n có th "nghe" du c b ng cách thi t l p ch d promiscous mode trên các card m ng c a tr m dó. Sniffer s th c hi n công vi c này.

M t h th ng sniffer có th k t h p c các thi t b ph n c ng và ph n m m, trong dó h th ng ph n m m v i các ch d debug th c hi n phân tích các gói tin "b t" du c trên m ng.

H th ng sniffer ph i du c d t trong cùng m t segment m ng (network block) c n nghe lén.

Hình sau minh ho v trí d t sniffer:



Hình 6.3: Các v trí d t sniffer trên 1 segment m ng

Phuong th c t n công m ng d a vào các h th ng sniffer là r t nguy hi m vì nó du c thc hi n các t ng r t th p trong h th ng m ng. V i vi c thi t l p h th ng sniffer cho phép l y du c toàn b các thông tin trao d i m ng. Các thông tin dó có th là:

- Các tài kho n và m t kh u truy nh p
- Các thông tin n i b ho c có giá tr ca

Tuy nhiên vi c thi t l p m t h th ng sniffer không ph i don gi n vì c n ph i xâm nh p du c vào h th ng m ng dó và cài d t các ph n m m sniffer. Đ ng th i các chuong trình sniffer cung yêu c u ngu i s d ng ph i hi u sâu v ki n trúc, các giaohtc m ng.

M c khác, s lu ng các thông tin trao d i trên m ng r t l n nên các d li u do các chuong trình sniffer sinh ra khá l n. Thông thu ng, các chuong trình sniffer có th c u hình d ch thu nh p t 2030 00 bytes trong m t gói tin, vi thu ng mn ng thông tin quan tr ng nhu tên ngu i dùng, m t kh u n m ph n d u gói tin.

Trong m t s tru ng h p qu n tr m ng, d phân tích các thông tin luu chuy n trên m ng, ngu i qu n tr cung c n ch d ng thi t l p các chuong trình sniffer, v i vai trò nà sniffer có tác d ng t t.

Vi c phát hi n h th ng b sniffer không ph i don gi n, vì sniffer ho t d ng t ng r t th p, và không nh hu ng t i các ng d ng cung nhu các d ch v h th ng dó cung c p. M t s bi n pháp sau ch có tác d ng ki m tra h th ng nhu:

- Ki m tra các ti n trình dang th c hi n trên h th ng (b ng l nh ps trên Unix ho c trình qu n lý tài nguyên trong Windows NT). Qua dó ki m tra các ti n trình l trên h th ng; tài nguyên s d ng, th i gian kh i t o ti n trình... d phát hi ncác chuong trình sniffer.

- S d ng m t vài ti n ích d phát hi n card m ng có chuy n sang ch d promiscous hay không. Nh ng ti n ích này giúp phát hi n h th ng c a b n có dang ch y sniffer hay không.

Tuy nhiên vi c xây d ng các bi n pháp h n ch sniffer cung không quá khó khan n u ta tuân th các nguyên t c v b o m t nhu :

- Không cho ngu i l truy nh p vào các thi t b trên h th ng
- Qu n lý c u hình h th ng ch t ch
- Thi t l p các k t n i có tính b o m t cao thông qua các co ch mã hoá.

1.1.3. M t s di m y u c a h th ng

1.1.3.1. Deamon fingerd

M t l h ng c a deamon fingerd là co h i d phuong th c t n công worm "sâu" trên Internet phát tri n: dó là l i tràn vùng d m trong các ti n trình fingerd (l i khi l p trình). Vùng d m d lu u chu i ký t nh p dung i h n là 512 bytes. Tuy nhiên chuong trình fingerd không th c hi n ki m tra d li u d u vào khi l n hon 512 bytes. K t qu là x y ra hi n tu ng tràn d li u vùng d m khi d li u l n hon 512 bytes. Ph n d li u du th a ch a nh ng do n mã d kích m t script khác ho t d ng; scripts này ti p t c th c hi n finger t i m t host khác. K t qu là hình thành m t m t xích các "sâu" trên m ng Internet.

1.1.3.2. File hosts.equiv

N u m t ngu i s d ng du c xác d nh trong file host.equiv cung v i d a ch máy c a ngu i dó, thì ngu i s d ng dó du c phép truy nh p t xa vào h th ng dã khai báo. Tuy nhiên có m t l h ng khi th c hi n ch c nang này dó là nó cho phép ngu i truy nh p t xa có du c quy n c a b t c ngu i nào khác trên h th ng. Ví d , n uên máy A có m t file /etc/host.equiv có dòng d nh danh B julie, thì julie trên B có th truy nh p vào h th ng A và có b t du c quy n c a b t c ngu i nào khác trên A. Đây là do l i c a th t c ruserok() trong thu vi n libc khi l p trình.

1.1.3.3. Thu m c /var/mail

N u thu m c /var/mail du c set là v i quy n du c vi t (writeable) d i v i t t c m i ngu i trên h th ng, thì b t c ai có th t o file trong thu m c này. Sau dó t o m t file v i tên c a m t ngu i dã có trên h th ng r i link t i m t file trên h th ng, thì các thu t i ngu i s d ng có tên trùng v i tên file link s du c gán thêm vào trong file mà nó link t i.

Ví d , m t ngu i s d ng t o link t /var/mail/root t i /etc/passwd, sau dó g i mail b ng tên m t ngu i m i t i root thì tên ngu i s d ng m i này s du c gán thêm vào trong file /etc/passwd; Do v y thu m c /var/mail không bao gi du c set v i quy n writeable.

1.1.3.4. Ch c nang proxy c a FTPd

Ch c nang proxy server c a FTPd cho phép m t ngu i s d ng có th truy n file t m t ftpd này t i m t ftpd server khác. S d ng ch c nang này s có th b qua du c các xác th c d a trên d a ch IP.

Nguyên nhân là do ngu i s d ng có th yêu c u m t file trên ftp server g i m t file t i b t k d a ch IP nào. Nên ngu i s d ng có th yêu c u ftp server dó g i m t file g m các l nh là PORT và PASV t i các server dang nghe trên các port TCP trên b t k m t host nào; k t qu là m t trong các host dó có ftp server ch y và tin c y ngu i s d ng dó nên b qua du c xác th c d a ch IP.

1.1.4. Các m c b o v an toàn m ng

Vì không có m t gi i pháp an toàn tuy t d i nên ngu i ta thu ng ph i s d ng d ng th i nhi u m c b o v khác nhau t o thành nhi u l p "rào ch n" d i v i các ho t d ng xâm ph m. Vi c b o v thông tin trên m ng ch y u là b o v thông tin c t gi trong các máy tính, d c bi t là trong các server c a m ng. Hình sau mô t các l p rào ch n thông d ng hi n nay d b o v thông tin t i các tr m c a m ng:

Information

Hình 6.4: Các m c d b o v m ng

Nhu minh ho trong hình trên, các l p b o v thông tin trên m ng g m:

- L p b o v trong cùng là quy n truy nh p nh m ki m soát các tài nguyên (dây là thông tin) c a m ng và quy n h n (có th th c hi n nh ng thao tác gì) trên tài nguyên dó. Hi n nay vi c ki m soát m c này áp d ng sâu nh t d i v i t p.
- L p b o v ti p theo là h n ch theo tài kho n truy nh p g m dang ký tên và m t kh u tuong ng. Đ ây là phuong pháp b o v ph bi n nh t vì nó don gi n, ít t n kém và cung r t có hi u qu . M i ngu i s d ng muy n tr nh p du c vào m ng s d ng các tài nguyên d u ph i có dang ký tên và m t kh u. Ngu i qu n tr h th ng có trách nhi m qu n lý, ki m soát m i ho t d ng

c a m ng và xác d nh quy n truy nh p c a nh ng ngu i s d ng khác tu theo th i gian và không gian.

- L p th ba là s d ng các phuong pháp mã hoá (encryption). D li u du c bi n d i t d ng clear text sang d ng mã hoá theo m t thu t toán nào dó.

- L p th tu là b o v v t lý (physical protection) nh m ngan c n các truy nh p v t lý b t h p pháp vào h th ng. Thu ng dùng các bi n pháp truy n th ng nhu ngan c m ngu i không có nhi m v vào phòng d t máy, dùng h th ng khoá trên máy tính, cài d t các h th ng báo d ng khi có truy nh p vào h th ng ...

- L p th na m: Cài d t các h th ng b c tu ng l a (firewall), nh m ngan ch n các thâm nh p trái phép và cho phép l c các gói tin mà ta không mu n g i di ho c nh n vào vì m t lý do nào dó.

1.2. Các bi n pháp b o v m ng máy tính

1.2.1. Ki m soát h th ng qua logfile

M t trong nh ng bi n pháp dò tìm các d u v t ho t d ng trên m t h th ng là d a vào các công c ghi logfile. Các công c này th c hi n ghi l i nh t ký các phiên làm vi c trên h th ng. N i dung chi ti t thông tin ghi l i ph thu c vào c u hình ngu i qu n tr h th ng. Ngoài vi c rà soát theo dõi ho t d ng, d i v i nhi u h th ng các thông tin trong logfile giúp ngu i qu n tr dánh giá du c ch t lu ng, hi u nang c a m ng lu i.

1.2.1.1. H th ng logfile trong Unix

Trong Unix, các công c ghi log t o ra logfile là các file du i d ng text thông thu ng cho phép ngu i s d ng dùng nh ng công c so n th o file text b t k d có th d c du c n i dung. Tuy nhiên, m t s tru ng h p logfile du c ghi du i d ng binary và ch có th s d ng m t s ti n ích d c bi t m i có th d c du c thông tin.

a) Logfile lastlog:

Ti n ích này ghi l i nh ng l n truy nh p g n dây d i v i h th ng. Các thông tin ghi l i g m tên ngu i truy nh p, th i di m, d a ch truy nh p ... Các chuong trình login s d c n i dung file lastlog, ki m tra theo UID truy nh p vào h th ng và thông báo l n truy nh p vào h th ng g n dây nh t. Ví d nhu sau:

```
Last login: Fri Sep 15 2000 14:11:38
Sun Microsystems Inc.   SunOS 5.7       Generic October 1998
No mail.
Sun Microsystems Inc.   SunOS 5.7       Generic October 1998
                        /export/home/ptthanh
```

b) Logfile UTMP

Logfile này ghi l i thông tin v nh ng ngu i dang login vào h th ng, thu ng n m thu m c /etc/utmp. Đ xem thông tin trong logfile có th s d ng các ti n ích nhu who, w, finger, rwho, users. Ví d n i dung c a logfile dùng l nh who nhu sau:

```
/export/home/vhai% who
root      console      Aug 10 08:45    (:0)
ptthanh   pts/4        Sep 15 15:27    (203.162.0.87)
ptthanh   pts/6        Sep 15 15:28    (203.162.0.87)
root      pts/12       Sep  7 16:35    (:0.0)
root      pts/13       Sep  7 11:35    (:0.0)
                                        root      pts/14       Sep  7 11:39    (:0.0)
```

c) Logfile WTMP

Logfile này ghi l i các thông tin v các ho t d ng login và logout vào h th ng. Nó có ch c nang tuong t v i logfile UTMP. Ngoài ra còn ghi l i các thông tinv các l n shutdown, reboot h th ng, các phiên truy nh p ho c ftp và thu ng n m thu m c /var/adm/wtmp. Logfile này thu ng du c xem b ng l nh "last". Ví d n i dung nhu sau:

```
/export/home/vhai% last | more
ptthanh   pts/10       203.162.0.85  Mon Sep 18 08:44   still logged in
ptthanh   pts/10                     Sat Sep 16 16:52   (00:00)
vtoan     pts/10       203.162.0.87      Fri Sep 15 15:36   (1+01:22)
vtoan     pts/6        203.162.0.87      Fri Sep 15 15:28   still logged in
vtoan     pts/4                          Fri Sep 15 15:12   (00:00)
```

d) Ti n ích Syslog

Đây là m t công c ghi logfile r t h u ích, du c s d ng r t thông d ng trên các h th ng UNIX. Ti n ích syslog giúp ngu i qu n tr h th ng d dàng trong vi c th c hi n ghi logfile d i v i các d ch v khác nhau. Thông thu ng ti n ích syslog thu ng du c ch y du i d ng m t daemon và du c kích ho t khi h th ng kh i d ng. Daemon syslogd l y thông tin t m t s ngu n sau:

- /dev/log: Nh n các messages t các ti n trình ho t d ng trên h th ng
- /dev/klog: nh n messages t kernel
- port 514: nh n các messages t các máy khác qua port 514 UDP.

Khi syslogd nh n các messages t các ngu n thông tin này nó s th c hi n ki m tra file c u hình c a d ch v là syslog.conf d t o log file tuong ng. Có th c u hình file syslog.conf d t o m t message v i nhi u d ch v khác nhau.

Ví d n i dung m t file syslog.conf nhu sau:

```
# This file is processed by m4 so be careful to quote (`') names
# that match m4 reserved words.  Also, within ifdef's, arguments
# containing commas must be quoted.
#
*.err;kern.notice;auth.notice                   /dev/console
*.err;kern.debug;daemon.notice;mail.crit        /var/adm/messages
*.alert;kern.err;daemon.err                     operator
*.alert                                         root
*.emerg                                         *
# if a non-loghost machine chooses to have authentication messages
```

Trong n i dung file syslog.conf ch ra, d i v i các message có d ng *.emerg (message có tính kh n c p) s du c thông báo t i t t c ngu i s d ng trên h th ng; Đ i v i các messages có d ng *.err, ho c kern.debug và nh ng ho t d ng truy c p không h p pháp s du c ghi log trong file /var/adm/messages.

M c d nh, các messages du c ghi vào logfile /var/adm/messages.

e) Ti n ích sulog

B t c khi nào ngu i s d ng dùng l nh "su" d chuy n sang ho t d ng h th ng du i quy n m t user khác d u du c ghi log thông qua ti n ích sulog. Nh ng thông tin logfile này du c ghi vào logfile /var/adm/sulog. Ti n ích này cho phép phát hi n các tru ng h p dùng quy n root d có du c quy n c a m t user nào khác trên h th ng.

Ví d n i dung c a logfile sulog nhu sau:

```
# more /var/adm/sulog
SU 01/04 13:34 + pts/1 ptthanh-root
SU 01/04 13:53 + pts/6 ptthanh-root
SU 01/04 14:19 + pts/6 ptthanh-root
SU 01/04 14:39 + pts/1 ptthanh-root
```

f) Ti n ích cron

Ti n ích cron s ghi l i logfile c a các ho t d ng th c hi n b i l nh crontabs. Thông thu ng, logfile c a các ho t d ng cron trong file /var/log/cron/log. Ngoài ra, có th c u hình syslog d ghi l i các logfile c a ho t d ng cron.

Ví d n i dung c a logfile cron nhu sau:

```
# more /var/log/cron/log
! *** cron started ***   pid = 2367 Fri Aug  4 16:32:38 2000
>  CMD: /export/home/mrtg/mrtg /export/home/mrtg/termcount.cfg
>  ptthanh 2386 c Fri Aug  4 16:34:01 2000
<  ptthanh 2386 c Fri Aug  4 16:34:02 2000
>  CMD: /export/home/mrtg/getcount.pl
>  ptthanh 2400 c Fri Aug  4 16:35:00 2000
<  ptthanh 2400 c Fri Aug  4 16:35:10 2000
>  CMD: /export/home/mrtg/mrtg /export/home/mrtg/termcount.cfg
```

g) Logfile c a sendmail

Ho t d ng ghi log c a sendmail có th du c ghi qua ti n ích syslog. Ngoài ra chuong trình sendmail còn có l a ch-Ln "+ level security" v i m c d b o m t t "debug" t"icrit" cho phép ghi l i logfile. Vì sendmail là m t chuong trình có nhi u bug, v i nhi u l h ng b o m t n n ngu i qu n tr h th ng thu ng xuyên nên ghi l i logfile d i v i d ch v này.

h) Logfile c a d ch v FTP

H u h t các daemon FTP hi n nay dhoqphép c u hình d ghi l i logfile s d ng d ch v FTP trên h th ng dó. Ho t d ng ghi logfile c a d ch v FTP thu ng du c s d ng v i l a ch-H","c u hình c th trong file /etc/inetd.conf nhu sau:

```
# more /etc/inetd.conf
ftp     stream  tcp  nowait  root    /etc/ftpd/in.ftpd       in.ftpd -l
```

Sau dó c u hình syslog.conf tuong ng v i d ch v FTP; c th nhu sau:

```
#  Logfile FTP
daemon.info     ftplogfile
```

V i l a ch n này s ghi l i nhi u thông tin quan tr ng trong m t phiên ftp nhu: th i dim truy nh p, d a ch IP, d li u get/put ... vào site FTP dó. Ví d n i dung logfile c a m t phiên ftp nhu sau:

```
Sun Jul 16 21:55:06 2000 12 nms 8304640 /export/home/ptthanh/PHSS_17926.depot b _ o r
ptthanh ftp 0 * c
Sun Jul 16 21:56:45 2000 96 nms 8464640 /export/home/ptthanh/PHSS_19345.depot b _ o
r ptthanh ftp 0 * c
Sun Jul 16 21:57:41 2000 4 nms 3379200 /export/home/ptthanh/PHSS_19423.depot b _ o r
ptthanh ftp 0 * c
Sun Jul 16 22:00:38 2000 174 nms 130396160 /export/home/ptthanh/PHSS_19987.depo
o r ptthanh ftp 0 * c
```

i) Logfile c a d ch v Web:

Tùy thu c vào Web server s d ng s có các phuong th c và c u hình ghi logfile c a d ch v Web khác nhau. H u h t các web server thông d ng hi n nay d u h tr co ch ghi log. Ví d n i dung logfile c a d ch v Web s d ng Web server Netscape nhu sau:

```
202.167.123.170 - - [03/Aug/2000:10:59:43 +0700] "GET /support/cgi-bin/search.pl
HTTP/1.0" 401 223
203.162.46.67 - - [03/Sep/2000:22:50:52 +0700] "GET http://www.geocities.com/ HTTP/1.1"
401 223
203.162.0.85 - - [15/Sep/2000:07:43:17 +0700] "GET /support/cgi-bin/search.pl HTTP/1.0"
401 223
203.162.0.85 - ptthanh [15/Sep/2000:07:43:22 +0700] "GET /support/cgi-bin/search.pl
HTTP/1.0" 404 207
203.162.0.85 - - [15/Sep/2000:07:43:17 +0700] "GET /support/cgi-bin/search.pl HTTP/1.0"
401 223
```

1.2.1.2. M t s công c h u ích h tr phân tích logfile:

Đ i v i ngu i qu n tr , vi c phân tích logfile c a các d ch v là h t s c quan tr ng. M t s công c trên m ng giúp ngu i qu n tr th c hi n công vi c này d dàng hon, đó là:

- Ti n ích chklastlog và chkwtmp giúp phân tích các logfile lastlog và WTMP theo yêu c u ngu i qu n tr .

- Ti n ích netlog giúp phân tích các gói tin, g m 3 thành ph n:

+ TCPlogger: log l i t t c các k t n i TCP trên m t subnet

+ UDPlogger: log i t t c các k t n i UDP trên m t subnet

+ Extract: X lý các logfile ghi l i b i TCPlogger và UDBlogger.

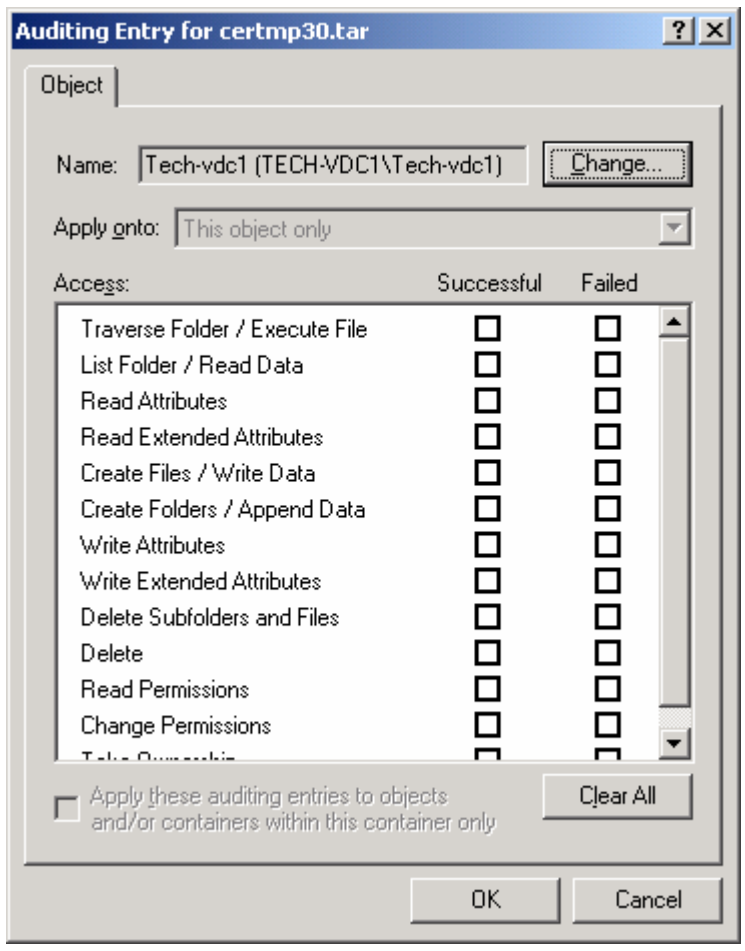
- Ti n ích TCP wrapper: Ti n ích này cho phép ngu i qu n tr h th ng d dàng giám sát và l c các gói tin TCP c a các d ch v nhu systat, finger telnet, rlogin, rsh, talk ...

1.2.1.3. Các công c ghi log thu ng s d ng trong Windows NT và 2000

Trong h th ng Windows NT 4.0 và Windows 2000 hi n nay d u h tr d y d các co ch ghi log v i các m c d khác nhau. Ngu i qu n tr h th ng tùy thuc vào m c d an toàn c a d ch v và các thông tin s d ng có th l a ch n các m c d ghi log khác nhau. Ngoài ra, trên h th ng Windows NT còn h tr các co ch ghi logfile tr c ti p vào các database d t o báo cáo giúp ngu i qu n tr phân tích và ki tra h th ng nhanh chóng và thu n ti n. S d ng ti n ích event view d xem các thông tin logfile trên h th ng v i các m c d nhu Application log; Security log; System log. Các hình du i dây s minh ho m t s ho t d ng ghi logfile trên h th ng Windows

Ví d : Đ ghi l i ho t d ng d c, vi t, truy nh p.... d i v i m t file/thu m c là thành công hay không thành công ngu i qu n tr có th c u hình nhu sau:

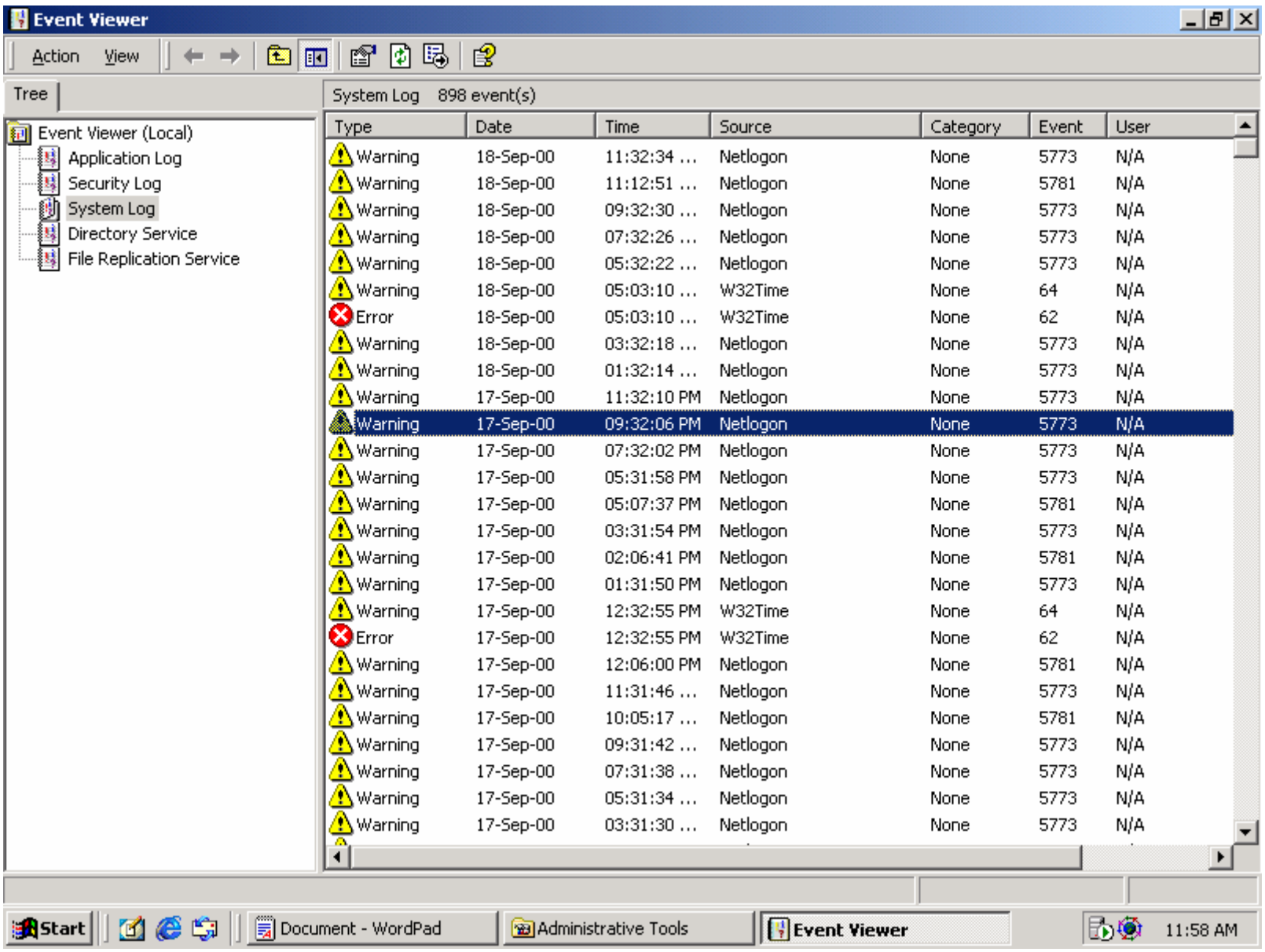
Ch n File Manager- User Manager- Security- Auditing. Ví d hình sau minh h a các ho t d ng có th du c ghi log trong Windows 2000:



Hình 6.5: Ghi log trong Windows 2000

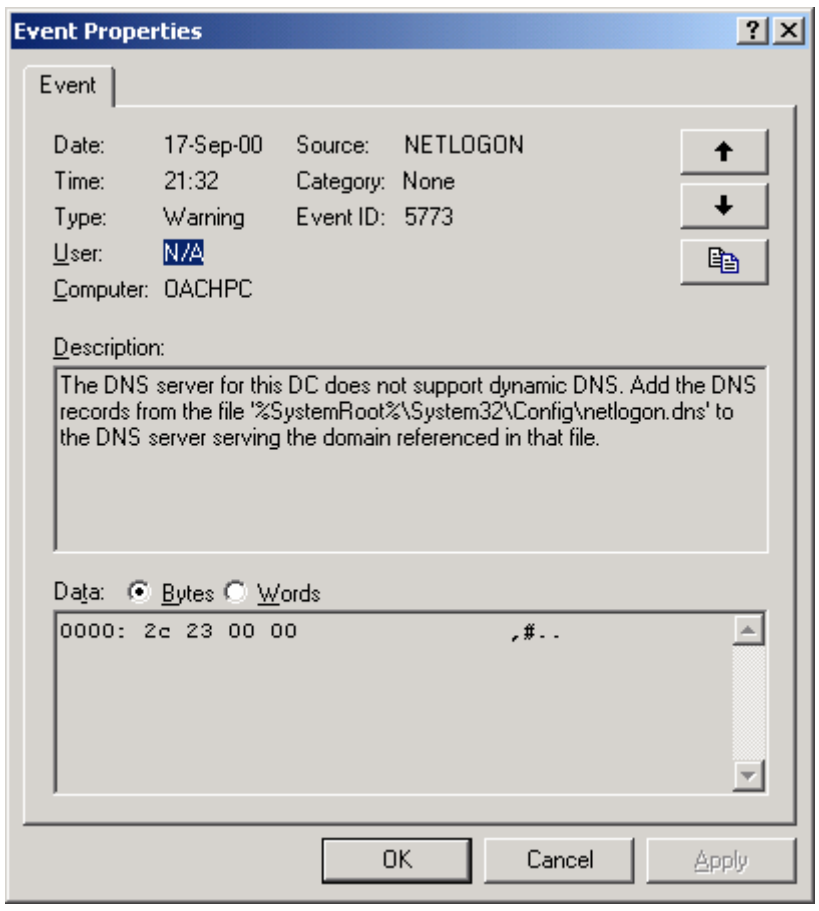
nhu

- S d ng ti n ích Event View cho phép xem nh ng thông tin logfile sau:



Hình 6.6: Công c Eve View c a Windows 2000

Xem chi ti t n i dung m message:



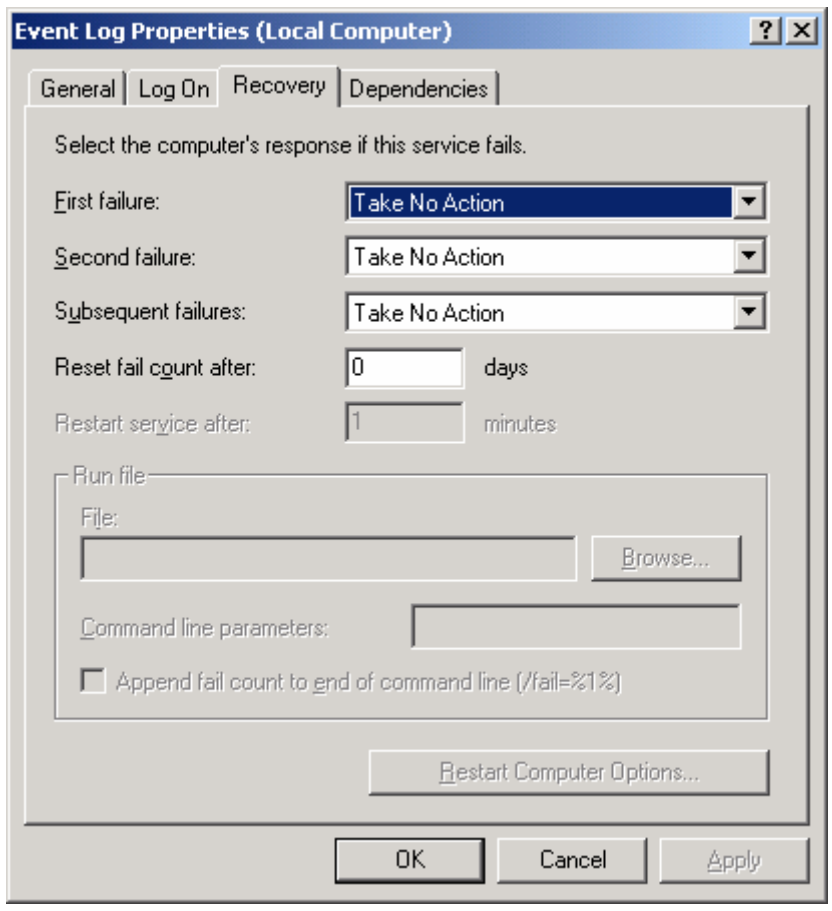
Hình 6.7: Chi ti t 1 thông báo l i trong Windows 2000

nhi u

Thông báo này cho bi t nguyên nhân, th i di m x y ra l i cung nhu thông tin quan tr ng khác.

báo l i

Có th c u hình Event Service d th c hi n mtoan khi có m t thông x y ra nhu sau:



Hình 6.8: C u hình d ch v ghi log trong Windows 2000

Ngoài ra, cung gi ng nhu trên UNIX, trong Windows NT cung có các công c theo dõi logfile c a m t s d ch v thông d ng nh FTP, Web. Tùy thu c vào lo i server s d ng có các phuong pháp c u hình khác nhau.

1.2.2. Thi t l p chính sách b o m t h th ng

Trong các bu c xây d ng m t chính sách b o m t d i v i m t h th ng, nhi m v d u tiên c a ngu i qu n tr là xác d nh dúng m c tiêu c n b o m t. Vi c xác d nh nh ng m c tiêu c a chính sách b o m t giúp ngu i s d ng bi t du c trách nhi m c a mình trong vi c b o v các tài nguyên thông tin trên m ng, d ng th i giúp các nhà qu n tr thi t l p các bi n pháp d mub o h hi u trong quá trình trang b , c u hình và ki m soát ho t d ng c a h th ng. Nh ng m c tiêu b o m t bao g m:

1.2.2.1. Xác d nh d i tu ng c n b o v

Đây là m c tiêu d u tiên và quan tr ng nh t trong khi thi t l p m t chính sách b o m t. Ngu i qu n tm th ng c n xác d nh rõ nh ng d i tu ng nào là

quan tr ng nh t trong h th ng c n b o v và xác d nh rõ m c d uu tiên d i v i nh ng d i tu ng dó. Ví d các d i tu ng c n b o v trên m t h th ng có th là: các máy ch d ch v , các router, các di m truy nh p h th ng, các chuong trình ng d ng, h qu n tr CSDL, các d ch v cung c p ...

Trong bu c này c n xác d nh rõ ph m vi và ranh gi i gi a các thành ph n trong h th ng d khi x y ra s c trên h th ng có th cô l p các thành ph n này v i nhau, d dàng dò tìm nguyên nhân và cách kh c ph c. Có th chia các thành ph n trên m t h th ng theo các cách sau:

- Phân tách các d ch v tùy theo m c d truy c p và d tin c y.
- Phân tách h th ng theo các thành ph n v t lý nhu các máy ch (server), router, các máy tr m (workstation)...
- Phân tách theo ph m vi cung c p c a các d ch v nhu: các d ch v bên trong m ng (NIS, NFS ...) và các d ch v bên ngoài nhu Web, FTP, Mail ...

1.2.2.2. Xác d nh nguy co d i v i h th ng

Các nguy co d i v i h th ng chính là các l h ng b o m t c a các d ch v h th ng dó cung c p. Vi c xác d nh dúng d n các nguy co này giúp ngu i qu n tr có th tránh du c nh ng cu c t n công m ng, ho c có bi n pháp b o v dúng d n. Thông thu ng, m t s nguy co này n m các thành ph n sau trên h th ng:

a) Các di m truy nh p:

Các di m truy nh p c a h th ng b t k (Access Points) thu ng dóng vai trò quan tr ng d i v i m i h th ng vì dây là di m d u tiên mà ngu i s d ng cung nhu nh ng k t n công m ng quan tâm t i. Thông thu ng các di m truy nh pthu ng ph c v h u h t ngu i dùng trên m ng, không ph thu c vào quy n h n cung nhu d ch v mà ngu i s d ng dùng. Do dó, các di m truy nh p thu ng là thành ph n có tính b o m t l ng l o. M t khác, d i v i nhi u h th ng còn cho phép ngu i s d ng dùng các d ch v nhu Telnet, rlogin d truy nh p vào h th ng, dây là nh ng d ch v có nhi u l h ng b o m t.

b) Không ki m soát du c c u hình h th ng

Không ki m soát ho c m t c u hình h th ng chi m m t t l l n trong s các l h ng b o m t. Ngày nay, ó m t s lu ng l n các ph n m m s d ng, yêu c u c u hình ph c t p và da d ng hon, di u này cung d n d n nh ng khó khan d ngu i qu n tr n m b t du c c u hình h th ng. Đ kh c ph c hi n tu ng này, nhi u hãng s n xu t ph n m m dã dua ra nh ng c u hình t o m c d nh, trong khi dó nh ng c u hình này không du c xem xét k lu ng trong m t môi tru ng b o m t. Do dó, nhi m v c a ngu i qu n tr là ph i n m du c ho t d ng c a các ph n m m s d ng, ý nghia c a các file c u hình quan tr ng, áp d ng cách i n pháp b o v c u hình nhu s d ng phuong th c mã hóa hashing code (MD5).

c) Nh ng bug ph n m m s d ng

Nh ng bug ph n m m t o nên nh ng l h ng c a d ch v là co h i cho các hình th c t n công khác nhau xâm nh p vào m ng. Do dó, ngu i qu n tr

ph i thu ng xuyên c p nh t thông tin t c trên các nhóm tin v b o m t và t nhà cung c p ph n m m d phát hi n nh ng l i c a ph n m m s d ng. Khi phát hi n có bug c n thay th ho c ng ng s d ng ph n m m dó ch nâng c p lên phiên b n ti p theo.

d) Nh ng nguy co trong n i b m ng

M t h th ng không nh ng ch u t n công t ngoài m ng, mà có th b t n công ngay t bên trong. Có th là vô tình ho c c ý, các hình th c phá ho i bên trong m ng v n thu ng x y ra trên m t s h th ng l n. Ch y u v i hình th c t n công bên trong m ng là k t n công có th ti p c n v m t v t lý d i v i các thi t b trên h th ng, d t du c quy n truy nh p b t h p pháp t i ngay h th ng dó. Ví d nhi u tr m làm vi c có th chi m du c quy n s d ng n u k t n công ng i ngay t i các tr m làm vi c dó.

1.2.2.3. Xác d nh phuong án th c thi chính sách b o m t

Sau khi thi t l p du c m t chính sách b o m t, m t ho t d ng ti p theo là l a ch n các phuong án th c thi m t chính sách b o m t. M t chính sách b o m t là hoàn h o khi nó có tình th c thi cao. Đ dánh giá tính th c thi này, có m t s tiêu chí d l a ch n dó là:

- Tính dúng d n
- Tính thân thi n
- Tính hi u qu

1.2.2.4. Thi t l p các qui t c/th t c

a) Các th t c d i v i ho t d ng truy nh p b t h p pháp

S d ng m t vài công c dó phát hi n ra các hành d ng truy nh p b t h p pháp vào m t h th ng. Các công c này có th di kèm theo h di u hành, ho c t các hãng s n xu t ph n m m th ba. Đây là bi n pháp ph bi n nh t d theo dõi các ho t d ng h th ng.

- Các công c logging: h u h t các h di u hành d u h tr m t s lu ng l n các công c ghi log v i nhi u thông tin b ích. Đ phát hi n nh ng ho t d ng truy nh p b t h p pháp, m t s qui t c khi phân tích logfile nhu sau:

+ So sánh các ho t d ng trong logfile v i các ho t dong quá kh . Đ i v i các ho t d ng thông thu ng, các thông tin trong logfile thu ng có chu k gi ng nhau nhu th i di m ngu i s d ng login ho c log out, th i gian s d ng các d ch v trên h th ng...

+ Nhi u h th ng s d ng các thông tin trong logfile d t o hóa don cho khách hàng. Có th d a vào các thông tin trong hóa don thanh toán d xem xét các truy nh p b t h p pháp n u th y trong hóa don dó có nh ng di m b t thu ng nhu th i di m truy nh p, s di n tho i l ...

+ D a vào các ti n ích nhu syslog d xem xét, d c bi t là các thông báo l i login không h p l (bad login) trong nhi u l n.

+ D a vào các ti n ích kèm theo h di u hành d theo dõi các ti n trình dang ho t d ng trên h th ng; d phát hi n nh ng ti n trình l , ho c nh ng chuong trình kh i t o không hlp...

- S d ng các công c giám sát khác: Ví d s d ng các ti n ích v m ng d theo dõi các luu lu ng, tài nguyên trên m ng d phát hi n nh ng di m nghi ng .

b) Các th t c b o v h th ng

- Th t c qu n lý tài kho n ngu i s d ng
- Th t c qun lý m t kh u
- Th t c qu n lý c u hình h th ng
- Th t c sao luu và khôi ph c d li u
- Th t c báo cáo s c

1.2.2.5. Ki m tra, dánh giá và hoàn thi n chính sách b o m t

M t h th ng luôn có nh ng bi n d ng v c u hình, các d ch v s d ng,và ngay c n n t ng h di u hành s d ng, các thi t b ph n c ng .... do v y ngu i thi t l p các chính sách b o m t mà c th là các nhà qu n tr h th ng luôn luôn ph i rà sóat, ki m tra l i chính sách b o m t d m b o luôn phù h p v i th c t . M t khác ki m tra và dánh giá chính sách b o m t còn giúp cho các nhà qu n lý có k ho ch xây d ng m ng lu i hi u qu hon.

a) Ki m tra, dánh giá

Công vi c này du c th c hi n thu ng xuyên và liên t c. K t qu c a m t chính sách b o m t th hi n rõ nét nhtng ch t lu ng d ch v mà h th ng dó cung c p. D a vào dó có th ki m tra, dánh giá du c chính sách b o m t dó là h p lý hay chua. Ví d , m t nhà cung c p d ch v Internet có th ki m tra du c chính sách b o m t c a mình d a vào kh nang ph n hmg c a th ng khi b t n công t bên ngoài nhu các hành d ng spam mail, DoS, truy nh p h th ng trái phép ...

Ho t d ng dánh giá m t chính sách b o m t có th d a vào m t s tiêu chí sau:

- Tính th c thi.
- Kh nang phát hi n và ngan ng a các ho t d ng phá ho i.
- Các công c h u hi u d h n ch các ho t d ng phá ho i h th ng.

b) Hoàn thi n chính sách b o m t:

T các ho t d ng ki m tra, dánh giá nêu trên, các nhà qu n tr h th ng có th rút ra du c nh ng kinh nghi m d có th c i thi n chính sách nh h u hi u hon. C i thi n chính sách có th là nh ng hành d ng nh m don gi n công vi c ngu i s d ng, gi m nh d ph c t p trên h th ng ...

Nh ng ho t d ng c i thi n chính sách b o m t có th di n ra trong su t th i gian t n t i c a h th ng dó. Nó g n li n v i các công vi c qu n tr và duy

trì h th ng. Đây cung chính là m t yêu c u trong khi xây d ng m t chính sách b o m t, c n ph i luôn luôn m m d o, có nh ng thay d i phù h p tùy theo di u ki n th c t .

2. T ng quan v h th ng firewall

2.1. Gi i thi u v Firewall

2.1.1. Khái ni m Firewall

Firewall là thi t b nh m ngan ch n s truy nh p không h p l t m ng ngoài vào m ng trong. H th ng firewall thu ng bao g m c ph n c ng và ph n m m. Firewall thu ng du c dùng theo phuong th c ngan ch n truy t o các lu t d i v i các d a ch khác nhau.

2.1.2. Các ch c nang co b n c a Firewall

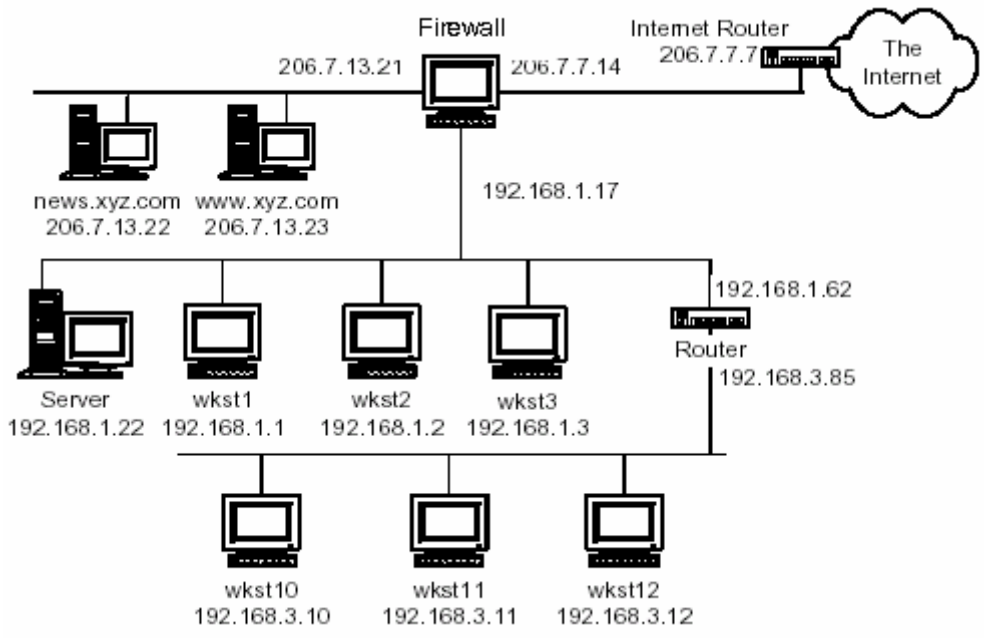
Ch c nang chính c a Firewall là ki m soát lu ng thông tin gi a m ng c n b o v (Trusted Network) và Internet thông qua các chính sách truy nh p dã du c thi t p.

- Cho phép ho c c m các d ch v truy nh p t trong ra ngoài và t ngoài vào trong.
- Ki m soát d a ch truy nh p, và d ch v s d ng.
- Ki m soát kh nang truy c p ngu i s d ng gi a 2 m ng.
- Ki m soát n i dung thông tin truy n t i gi a 2 m ng.
- Ngan ng a kh nang t n công t các m ng ngoài.

Xây d ng firewalls là m t bi n pháp khá h u hi u, nó cho phép b o v và ki m soát h u h t các d ch v do dó du c áp d ng ph bi n nh t trong các bi n pháp b o v m ng. Thông thu ng, m t h th ng firewall là m t c ng (gateway) gi a m ng n i b giao ti p v i m ng bên ngoài và ngu c l i

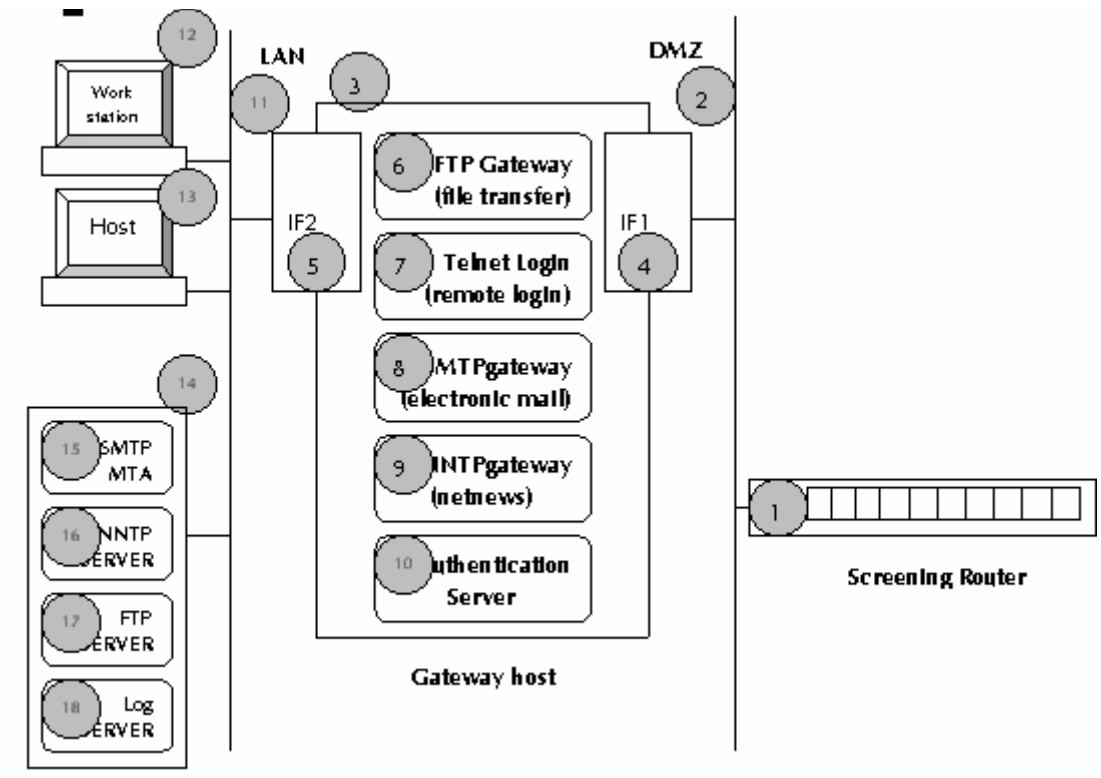
2.1.3. Mô hình m ng s d ng Firewall

Ki n trúc c a h th ng có firewall nhu sau:



Hình 6.9: Ki n trúc h th ng có firewall

Nhìn chung, m i h th ng firewall d u có cáu th ph n nhu sau:



Hình 6.10: Các thành ph n c a h th ng firewall

Firewall có th bao g m ph n c ng ho c ph n m m nhung thu ng là hai. V m t ph n c ng thì firewall có ch c nang g n gi ng m t router, nó cho phép hi n th các d ch IP dang k t n i qua nó. Đi u này cho phép b n xác d nh du c các d a ch nào du c phép và các d a ch IP nào không du c phép k t n i.

T t c các firewall d u có chung m t thu c tính là cho phép phân bi t d i x hay kh nang t ch i truy nh p d a trên các d a ch ngu n.

Theo hình trên các thành ph n c a m t h th ng firewall bao g m:

- Screening router: Là ch ng ki m soát d u tiên cho LAN.
- DMZ: Khu "phi quân s ", là vùng có nguy co b t n công t Internet.
- Gateway: là c ng ra vào gi a m ng LAN và DMZ, ki m soát m i liên l c, th c thi các co ch b o m t.
- IF1: Interface 1: Là card giao ti p v i vùng DMZ.
- IF2: Interface 2: Là card giao ti p v i vùng m ng LAN.

- FTP gateway: Ki m soát truy c p FTP gi a LAN và vùng DMZ. Các truy c p ftp t m ng LAN ra Internet là t do. Các truy c p FTP vào LAN dòi h i xác th c thông qua Authentication Server.

- Telnet Gateway: Ki m soát truy c p telnet gi a m ng LAN và Internet. Gi ng nhu FTP, ngu i dùng có th telnet ra ngoài t do, các telnet t ngoài vào yêu c u ph i xác th c qua Authentication Server

- Authentication Server: du c s d ng b i các c ng giao ti p, nh n di n các yêu c u k t n i, dùng các k thu t xác th c m nh nhu one-time password/token (m t kh u s d ng m t l n). Các máy ch d ch v trong m ng LAN du c b o v an toàn, không có k t n i tr c ti p v i Internet, t t c các thông tin trao d i d u du c ki m soát qua gateway.

2.1.4. Phân lo i Firewall

Có khá nhi u lo i firewall, m i lo i có nh ng uu và nhu c di m riêng. Tuy nhiên d thu n ti n cho vi nghiên c u ngu i ta chia h th ng làm 2 lo i chính:

- Packet filtering: là h th ng firewall cho phép chuy n thông tin gi a h th ng trong và ngoài m ng có ki m soát.

- Application-proxy firewall: là h th ng firewall th c hi n các k t n i thay cho các k t n i tr c ti p t máy khách yêu c u.

2.1.4.1. Packet Filtering

Ki u firewall chung nh t là ki u d a trên m c m ng c a mô hình OSI. Firewall m c m ng thu ng ho t d ng theo nguyên t c router hay còn du c g i là router, có nghia là t o ra các ctl cho phép quy n truy nh p m ng d a trên m c m ng. Mô hình này ho t d ng theo nguyên t c l c gói tin (packet filtering).

ki u ho t d ng này các gói tin d u du c ki m tra d a ch ngu n noi chúng xu t phát. Sau khi d a ch IP ngu n du c xác dinh thì du c ki m tra v i các lu t dã du c d t ra trên router. Ví d ngu i qu n tr firewall quy t d nh r ng không cho phép b t k m t gói tin nào xu t phát t m ng microsoft.com du c k t n i v i m ng trong thì các gói tin xu t phát t m ng này s không b gi d n du c m ng trong.

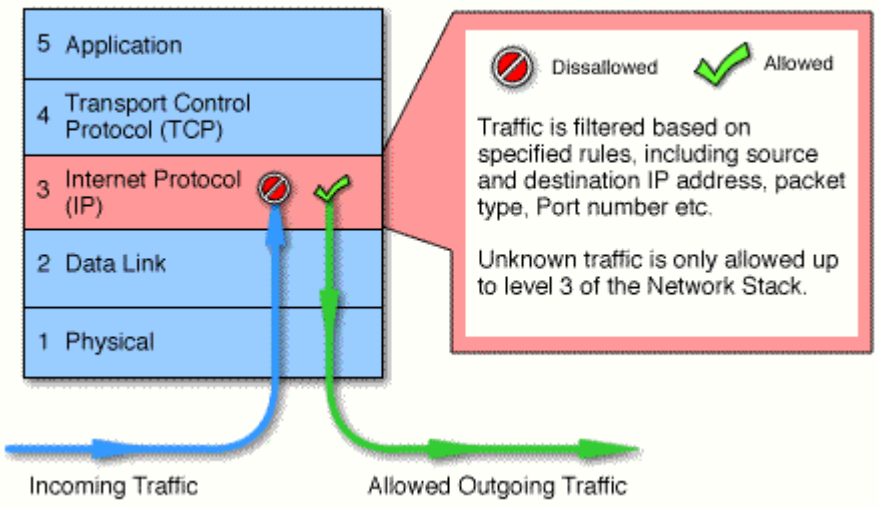
Các firewall ho t d ng l p m ng (tuong t nhu m t router) thu ng cho phép t c d x lý nhanh b i nó ch ki m tra d a ch IP ngu n mà không có m t l nh th c s nào trên router, nó không c n m t kho ng th i gian nào d xácd nh xem là d a ch sai hay b c m. Nhung di u này b tr giá b i tính tin c y c a nó. Ki u firewall này s d ng d a ch IP ngu n làm ch th , di u này t o ra m t l h ng là n u m t gói tin mang d a ch ngu n là d a ch gi thì nhu v y nó s có du c m truy nh p vào m ng trong c a b n.

Tuy nhiên có nhi u bi n pháp k thu t có th du c áp d ng cho vi c l c gói tin nh m kh c ph c y u di m này. Ví d nhu d i v i các công ngh packet filtering ph c t p thì không ch có tru ng d a ch IP du c kiam b i router mà còn có các tru ng khác n a du c ki m tra v i các lu t du c t o ra trên

firewall, các thông tin khác này có th là th i gian truy nh p, giao th c s d ng, port ...

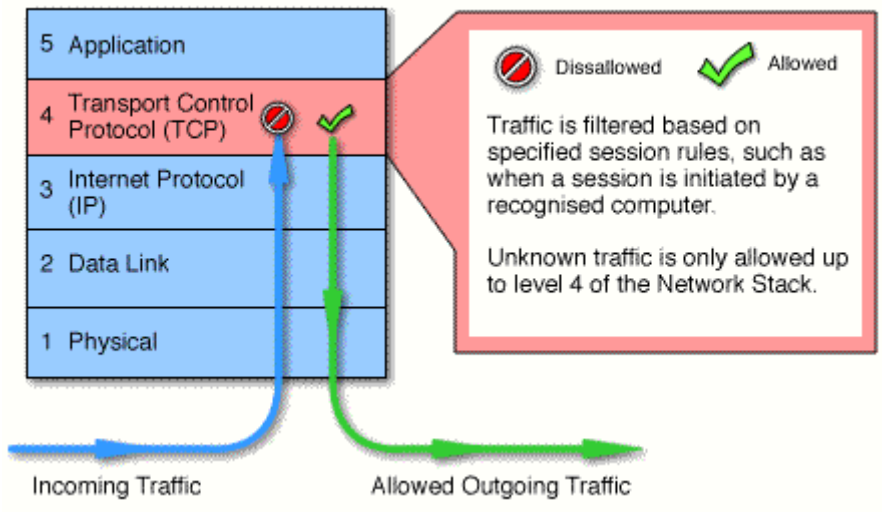
Firewall ki u Packet Filtering có th du c phân thành 2 lo i:

a) Packet filtering firewall: ho t d ng t i l p m ng c a mô hình OSI hay l p IP trong mô hình giao th c TCP/IP.



Hình 6.11: Packet filtering firewall

b) Circuit level gateway: ho t d ng t i l p phiên (session) c a mô hình OSI hay l p TCP trong mô hình giao th c TCP/IP.



Hình 6.12: Circuit level gateway

2.1.4.2. Application-proxy firewall

Ki u firewall này ho t d ng d a trên ph n m m. Khi m t k t n i t m t ngu i dùng nào dó d n m ng s d ng firewall ki u này thì k t n i dó s b ch n l i, sau dó firewall s ki m tra các tru ng có liên quan c a gói tin yêu c u k t n i. N u vi c ki m tra thành công, có nghia là các tru ng thông tin dáp ng du c các lu t dã d t ra trên firewall thì firewall s t o m t cái c u k t n i gi a hai node v i nhau.

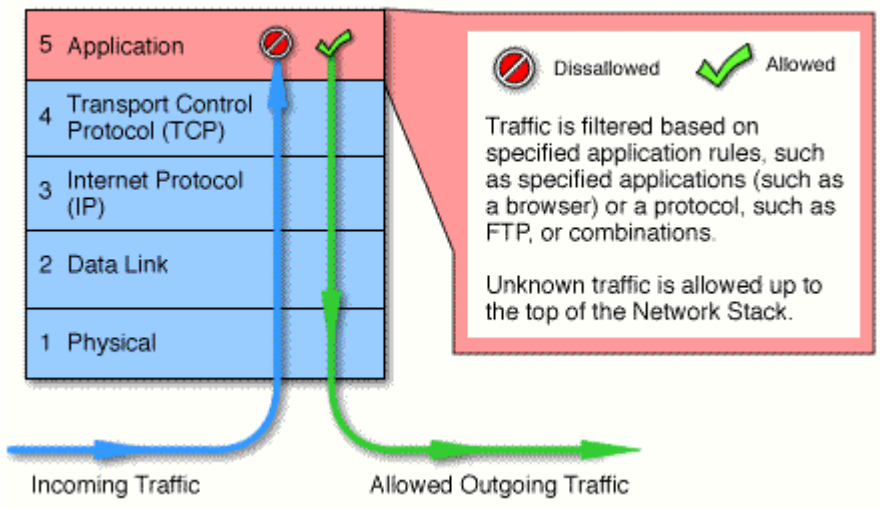
Uu di m c a ki u firewall lo i này là không có ch c nang chuy n ti p các gói tin IP, hon n a ta có th di u khi n m t cách chi ti t hon các k t n i thông qua firewall. Đ ng th i nó còn dua ra nhi u công c cho phép ghi l i các quá trình k t n i. T t nhiên di u này ph i giá b i t c d x lý, b i vì t t c các k t n i cung nhu các gói tin chuy n qua firewall d u du c ki m tra k lu ng v i các lu t trên firewall và r i n u du c ch p nh n s du c chuy n ti p t i node dích.

S chuy n ti p các gói tin IP x y ra khi m t máy ch nh n du c m t yêu c u t m ng ngoài r i chuy n chúng vào m ng trong. Đi u này t o ra m t l h ng cho các k phá ho i (hacker) xâm nh p t m ng ngoài vào m ng trong.

Nhu c di m c a ki u firewall ho t d ng d a trên ng d ng là ph i t o cho m i dch v trên m ng m t trình ng d ng u quy n (proxy) trên firewall ví d nhu ph i t o m t trình ftp proxy d ch v ftp, t o trình http proxy cho d ch v http... Nhu v y ta có th th y r ng trong ki u giao th c client-server nhu d ch v telnet làm ví d thì c n ph i th c hi n hai bu c d cho hai máy ngoài m ng và trong m ng có th k t n i du c v i nhau. Khi s d ng firewall ki u này các máy client (máy yêu c u d ch v) có th b thay d i. Ví d nhu d i v i d ch v telnet thì các máy client có th th hi n theo hai phuong th c: m t là b n telnet vào firewall tru c sau dó m i th c hi n vi c telnet vào máy m ng khác; cách th hai là b n có th telnet th ng t i dích tu theo các lu t trên firewall có cho phép hay không mà vi c telnet c a b n s tu du c chi n. Lúc này firewall là hoàn toàn trong su t, nó dóng vai trò nhu m t c u n i t i dích c a b n.

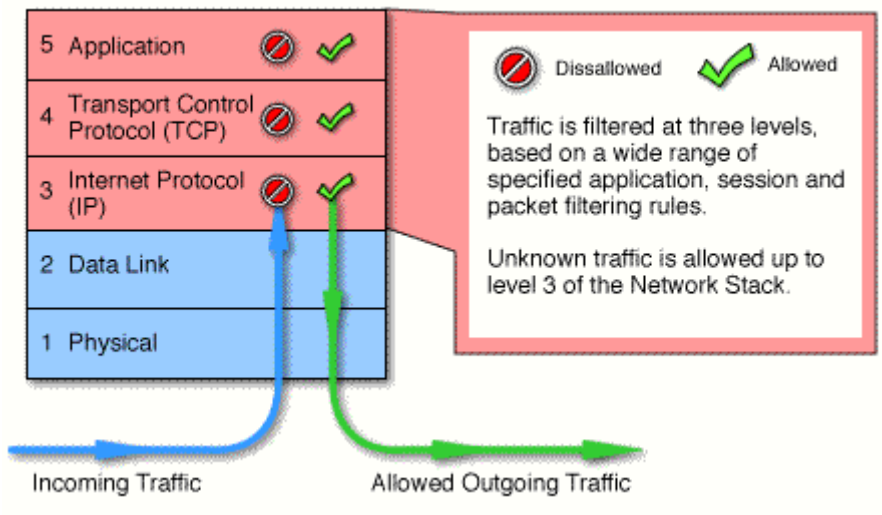
Firewall ki u Application-proxy có th du c phân thành 2 lo i:

a) Application level gateway tính nang tuong t nhu lo i circuit-level gateway nhung l i ho t d ng l p ng d ng trong mô hình giao th c TCP/IP.



Hình 6.13: Application level gateway

dây là lo i k t h p du c cáb) Stateful multilayer inspection firewall:
tính nang c a các lo i firewall trên: l c các gói t i l p m ng iva kra n i
dung các gói t i l p ng d ng. Firewall lo i này cho phép các k t n i tr c ti p
gi a các client và các host nên gi m du c các l i x y ra do tính ch t "không
trong su t" c a firewall ki u Application gateway. Stateful multilayer
inspectionfirewall cung c p các tính nang b o m t cao và l i trong su t d i v i
các end users.



Hình 6.14: Stateful multilayer inspection firewall

2.2. M t s ph n m m Firewall thông d ng

2.2.1. Packet filtering

Ki u l c gói tin này có th d oc th hi n mà không c n t o m t firewall hoàn ch nh, có r t nhi u các công c tr giúp cho vi c l c gói tin trên Internet (k c ph i mua hay du c mi n phí). Sau dây ta có th li t kê m t s ti n ích nhu v y

2.2.1.1. TCP_Wrappers

TCP_Wrappers là m t chương trình du c vi t b i Wietse Venema. Chuong trình ho t d ng b ng cách thay th các chuong trình thu ng trú c a h th ng và ghi l i t t c các yêu c u k t n i, th i gian yêu c u, và d a ch ngu n. Chuong trình này cung có kh nang ngan ch n các dIa chay các m ng không du c phép k t n i.

2.2.1.2. NetGate

NetGate du c dua ra b i Smallwork là m t h th ng d a trên các lu t v l c gói tin. Nó du c vi t ra d s d ng trên các h th ng Sun Sparc OS 4.1.x. Tuong t nhu các ki u packet filtering khác, NetGate ki m tra t t c các gói tin nó nh n du c và so sánh v i các lu t dã du c t o ra.

2.2.1.3. Internet Packet Filter

Ph n m m này hoàn toàn mi n phí, du c vi t b i Darren Reed. Đây là m t chuong trình khá ti n l i, nó có kh nang ngan ch n vduc t n công b ng d a ch IP gi . M t s u u di m c a chuong trình là nó không ch có kh

nang hu b các gói tin TCP không dúng ho c chua hoàn thi n mà còn không g i l i b n tin ICMP l i. Chuong trình này cho phép b n có th ki m tra th các lu t b n ra tru c khi s d ng chúng.

2.2.2. Application-proxy firewall

2.2.2.1. TIS FWTK

TIS FWTK (Trusted information Systems Firewall Tool Kit) là m t ph n m m m d u tiên d y d tính nang c a firewall và d c trung cho ki u firewall ho t d ng theo phuong th c ng d ng. Nh ng phiên b u tiên c a ph n m m này là mi n phí và bao g m nhi u thành ph n riêng r . M i thành ph n ph c v cho m t ki u d ch v trên m ng. Các thành ph n ch y u bao g m: Telnet, FTP, rlogin, sendmail và http.

Ph n m m này là m t h th ng toàn di n, tuy nhiên không có kh nang b o v m ng ngay sau khi cài d t vì vi c cài d t và c u hình không ph i là d dàng. Khi c u hình ph n m m này b n ph i th c s hi u mình dang làm gì b i có th v i các lu t b n t o ra thì m ng c a b n không th du c k t n i v i b t k m ng nào khác th m chí ngay c nh ng m ng quen thu c. Đi m d c trung nh t c a ph n m m này là nó có s n nhi u ti n ích giúp b n di u khi n du c truy nh p d i v i toàn m ng, m t ph n m ng hay th m chí ch riêng m t d a ch .

2.2.2.2. Raptor

Raptor là ph n m m firewall cung c p d y d các tính nang c a m t firewall chuyên nghi p v i hai giao di n qu n lý, m t trên h d u hành Unix (RCU) và m t trên h di u hành Windows (RMC). Raptor có th du c c u hình d b o v m ng theo b n phuong th c: Standard Proxies, Generic Service Passer, Virtual Private Network tunnels và Raptor Mobile. Tuy vi c c u hình cho Raptor khá ph c t p v i vi c t o các route, d nh nghia các entity, user và group, thi t l p các authorization rule ... nhung bù l i ta có th d ng du c r t nhi u tính nang uu vi t do Raptor cung c p d tu bi n các m c b o v d i v i m ng c a mình.

2.3. Th c hành cài d t và c u hình firewall Check Point v4.0 for Windows

2.3.1. Yêu c u ph n c ng:

- C u hình t i thi u d i v i máy cài GUI Client

  H di u hành Windows 95, Windows NT, X/Motif

  Dung lu ng dia tr ng 20 Mbytes

  B nh 16 Mbytes

  Card m ng Các lo i card du c h di u hành h tr

  Thi t b khác CD-ROM

- C u hình t i thi u d i v i máy cài Management Server

H di u hành Windows NT n(tel x86 và Pentium)

Dung lu ng dia tr ng 20 Mbytes

B nh t i thi u 16MB, nên dùng 24MB

Card m ng Các lo i card du c h di u hành h tr

Thi t b khác CD-ROM

- C u hình t i thi u d i v i máy cài Modul Firewall

H di u hành Windows NT n(tel x86 và Pentium)

Dung lu ng dia tr ng 20 Mbytes

B nh 16 Mbytes

Card m ng T i thi u ph i có 3 card m ng thu c các lo i card du c h di u hành h tr .

Thi t b khác CD-ROM

2.3.2. Các bu c chu n b tru c khi cài d t

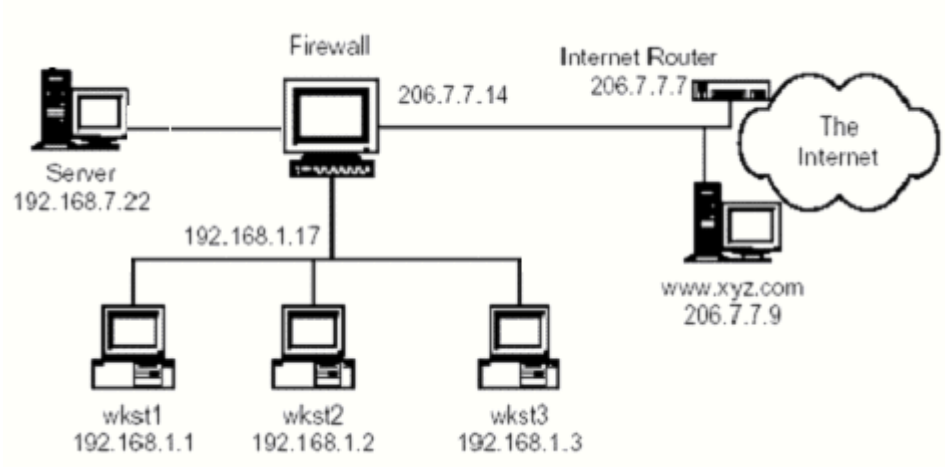
- Th t cht an ninh cho máy ch cài firewall và các module c a firewall nhu GUI Client và Management Server (t t các d ch v không c n thi t, update các patch s a l i c a h di u hành ...).

- Ki m tra các k t n i m ng trên các giao di n m ng, d m b o t máy ch cài Module Firewall có th ping du c các IP trên các giao di n m ng (s d ng l nh ifconfig , ping ...).

- Ki m tra b ng Routing (s d ng l nh netstat -rn ...).

- Ki m tra d ch v DNS (s d ng l nh nslookup).

- L p so d m ng th nghi m, d i v i máy có 3 giao di n m ng có th l p so d nhu sau:



Hình 6.15: So d m ng th nghi m d i v i máy ch có 3 giao di n m ng

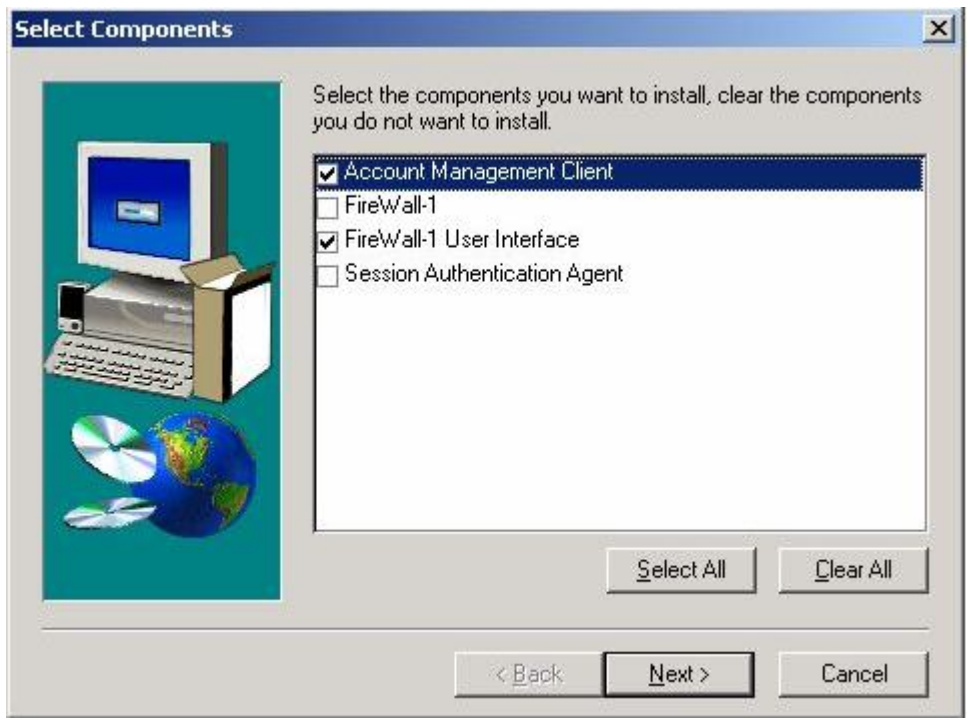
2.3.3. Ti n hành cài d t

Login du i quy n Administrator và cài d t h th ng Firewall Checkpoint trên các máy theo trình t sau:

- Cài d t GUI Client và Management Server.
- Cài d t Module Firewall.

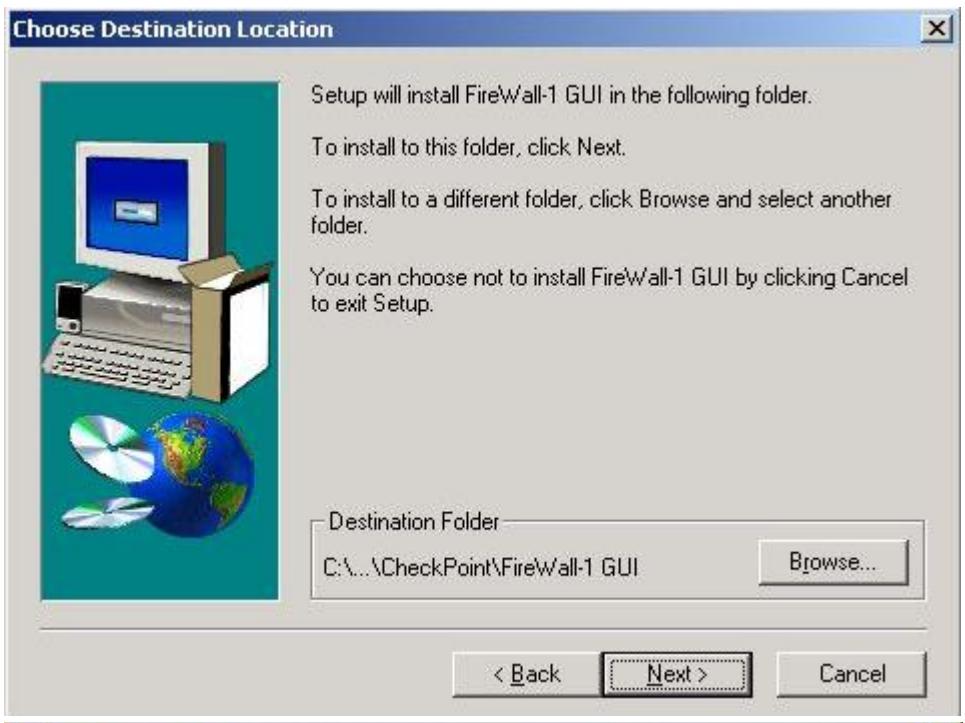
2.3.3.1. Cài d t GUI Client và Management Server

Đua dia CD Checkpoint và ch y l nh setup trong thu m c Windows, ch n Account Management Client và FireWall-1 User Interface trong c a s Select Components:

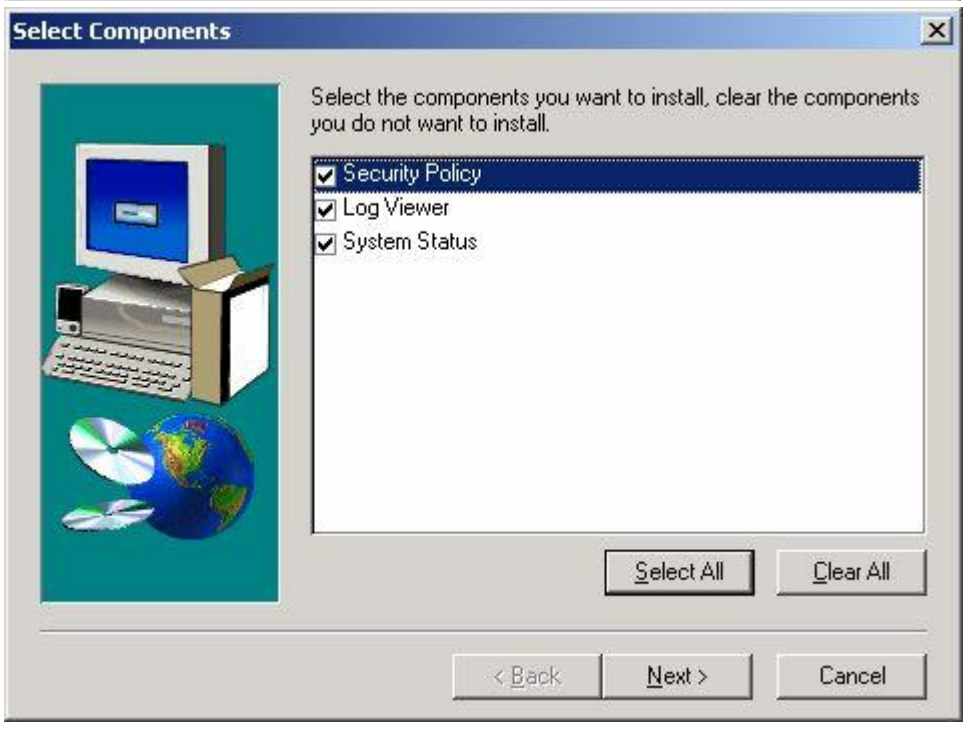


Ch n Next, màn hình s hi n ra nhu sau:

Ch n Next r i ch n thu m c cài d t trong c a s Choose Destination Locati

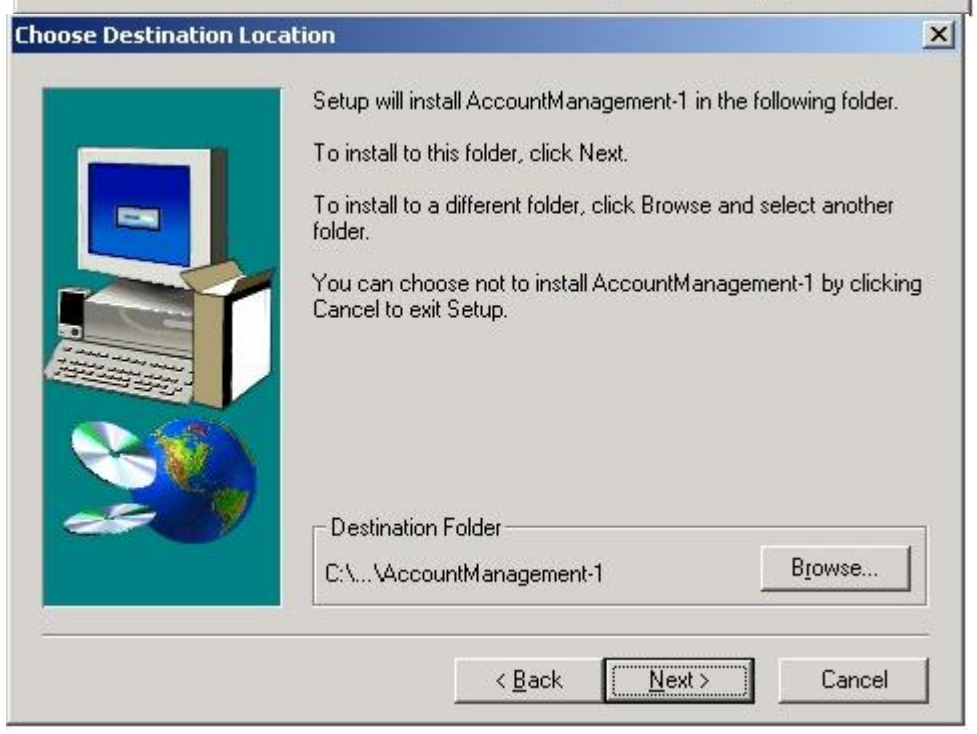


Ch n Next r i ch n các thành ph n trong c a s Select Components:

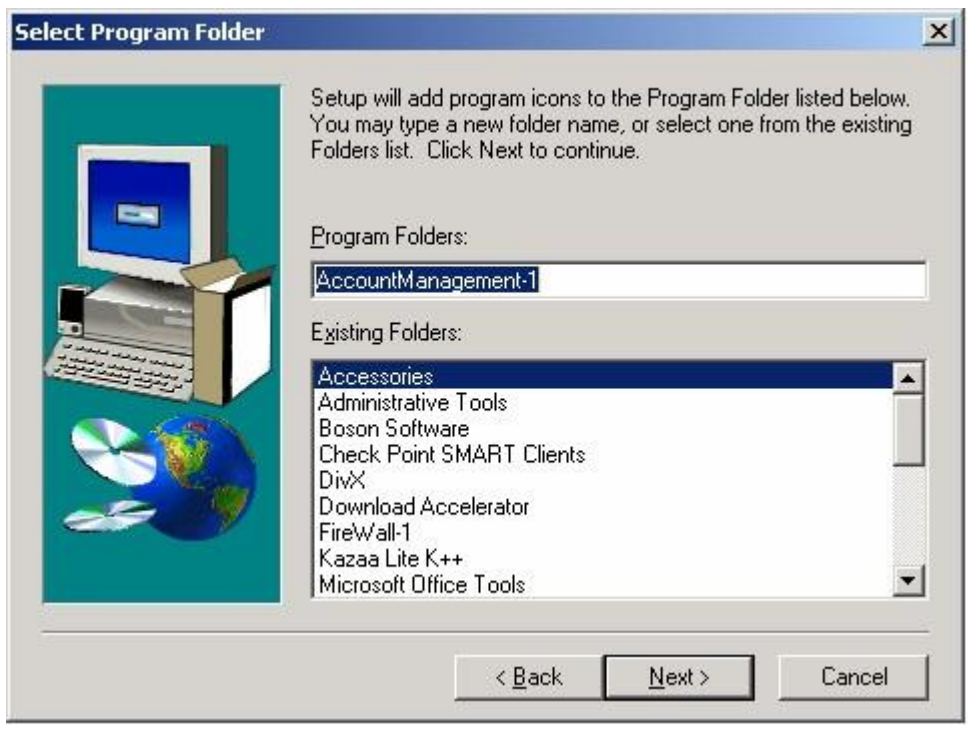


Ch n Next d b t d u quá trình cài d t.
Sau khi cài xong GUI Client, màn hình s t d ng hi n ra ph n cài d t Accour
Management Client With Encryption Installation:

Ch n Next r i ch n thu m c cài d t trong c a s Choose Destination Location:

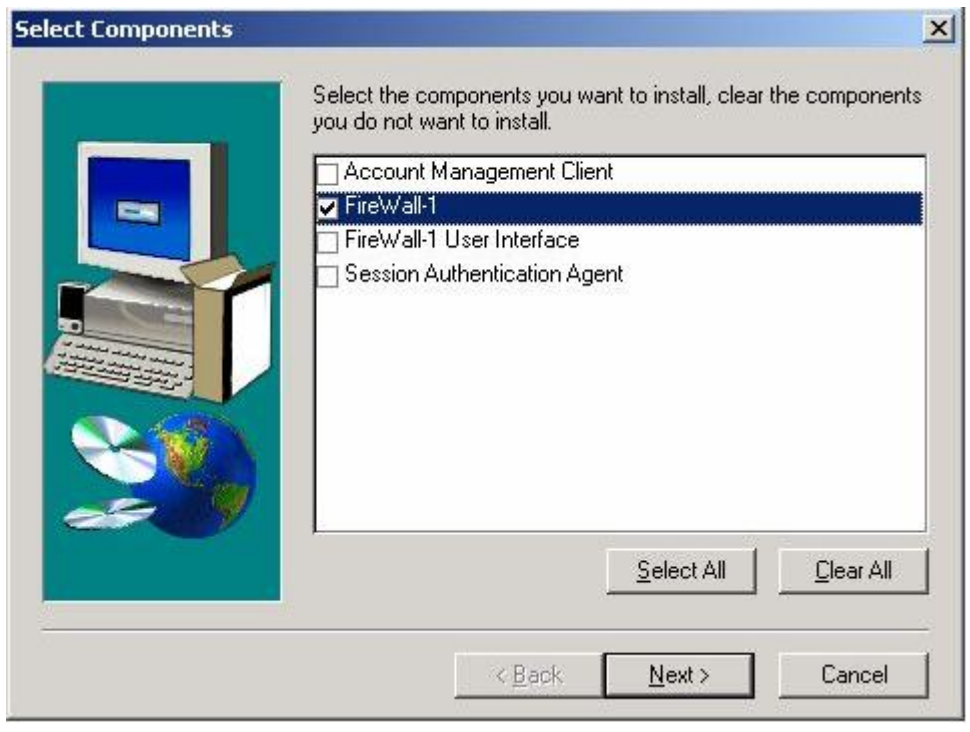


Ch n Next r i ch n Folder trong c a s Select Program Folder:



Ch n Next d b t d u quá trình cài d t

2.3.3.2. Cài d t Module Firewall:
Ch n FireWall-1 trong c a s Select Components ban d u:

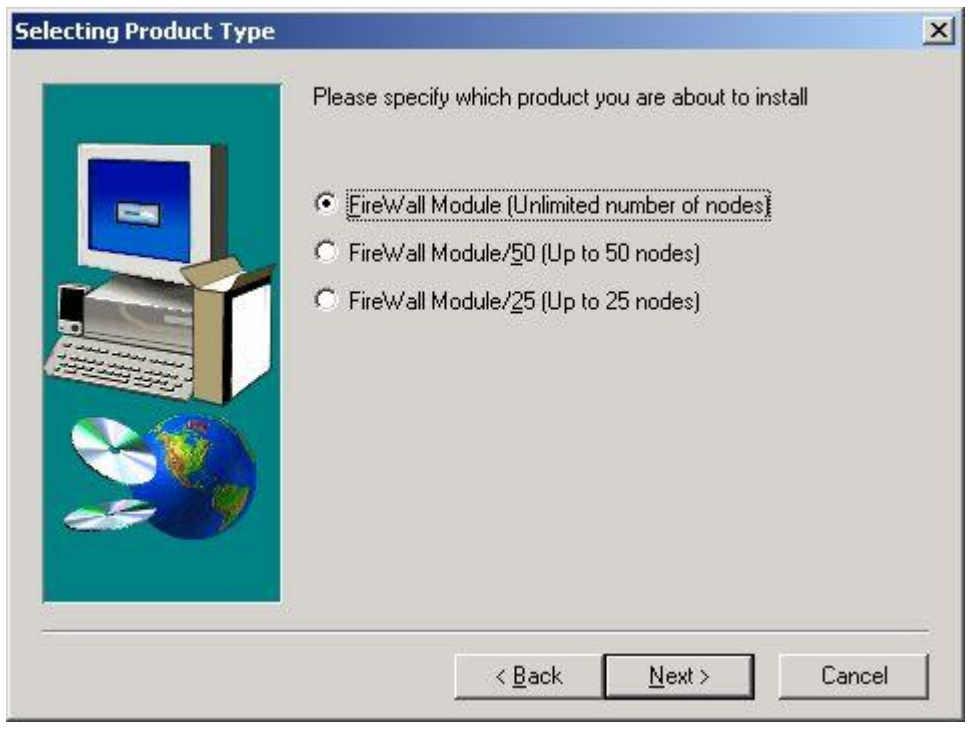


Ch n Next,màn hình s hi n ra nhu sau:

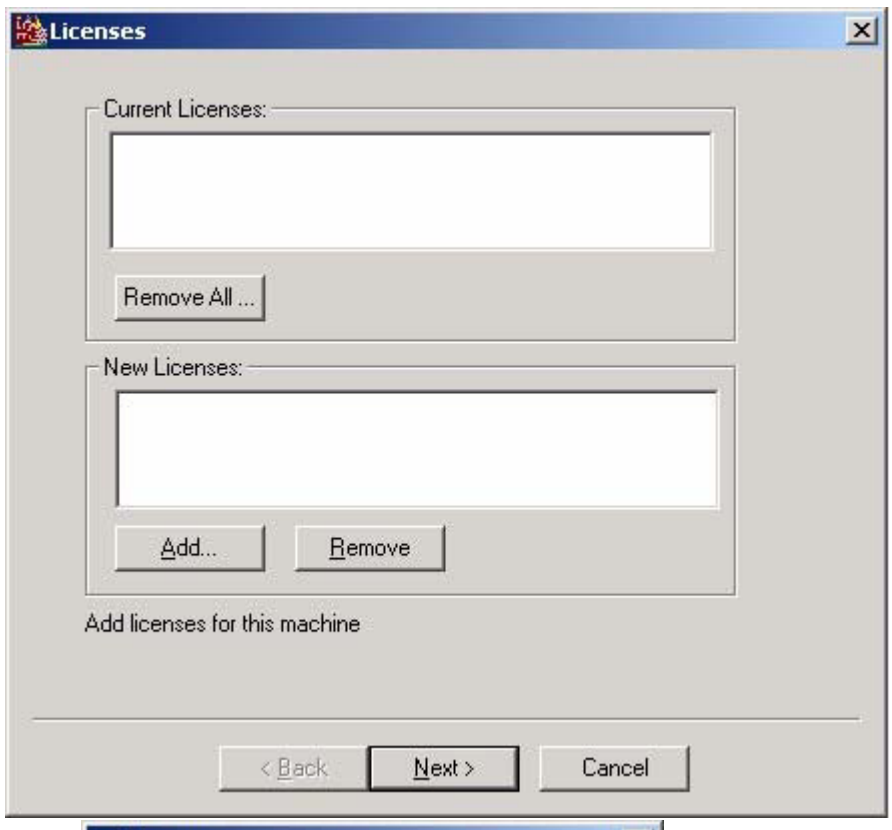
Ch n Next r i ch n thu m c cài d t trong c a s Choose Destination Location

Ch n Next r i ch n FireWall-1 FireWall Module trong c a s Selecting Product Type:

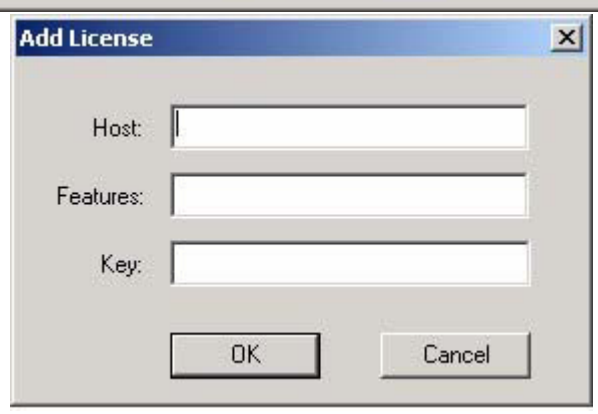
Ch n Next r i tùy theo phiên b n Checkpoint dang ký d ch license phù h p:



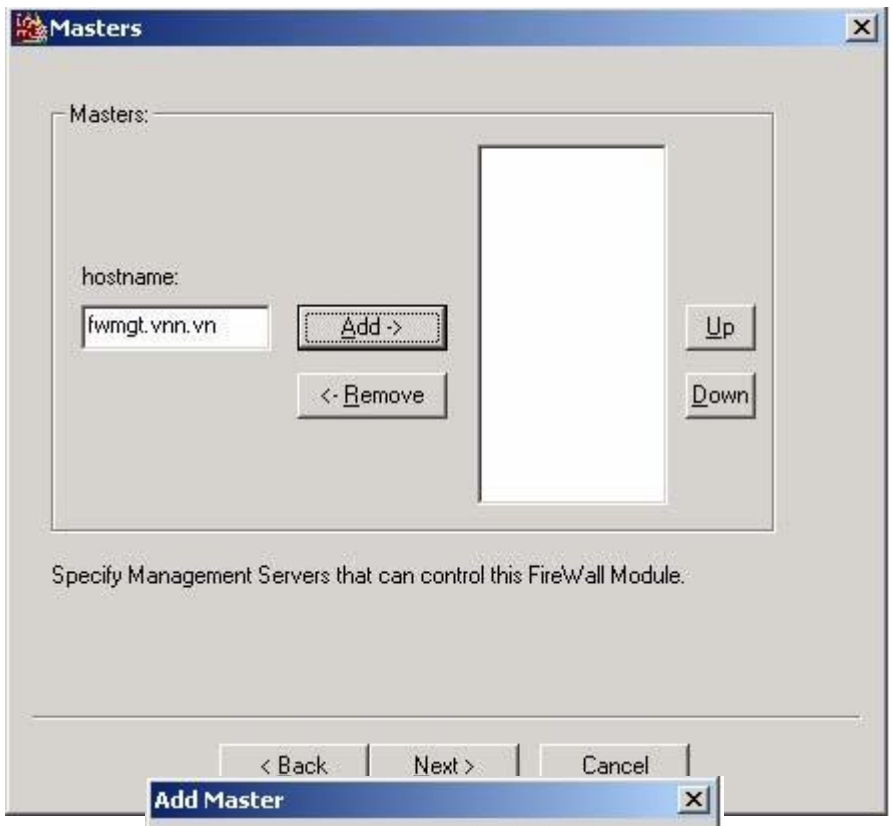
Ch n Next d b t d u quá trình cài d t.
Sau khi cài xong, màn hình cài d t license s hi n lên nhu sau:



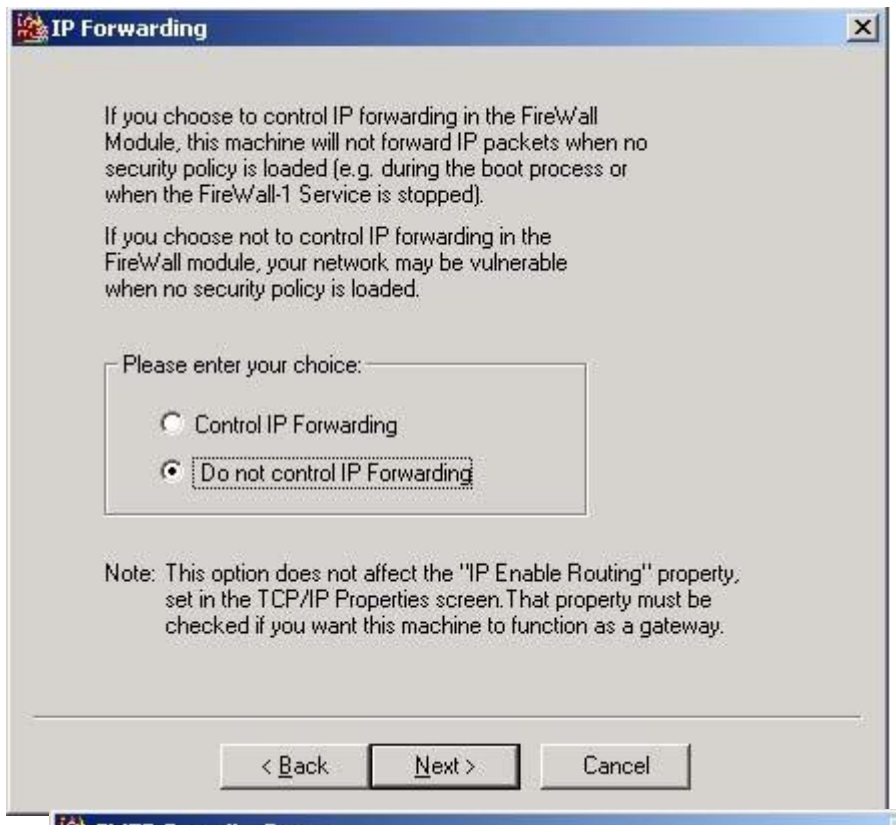
Ch n Add r i nh p license vào c a s sau :



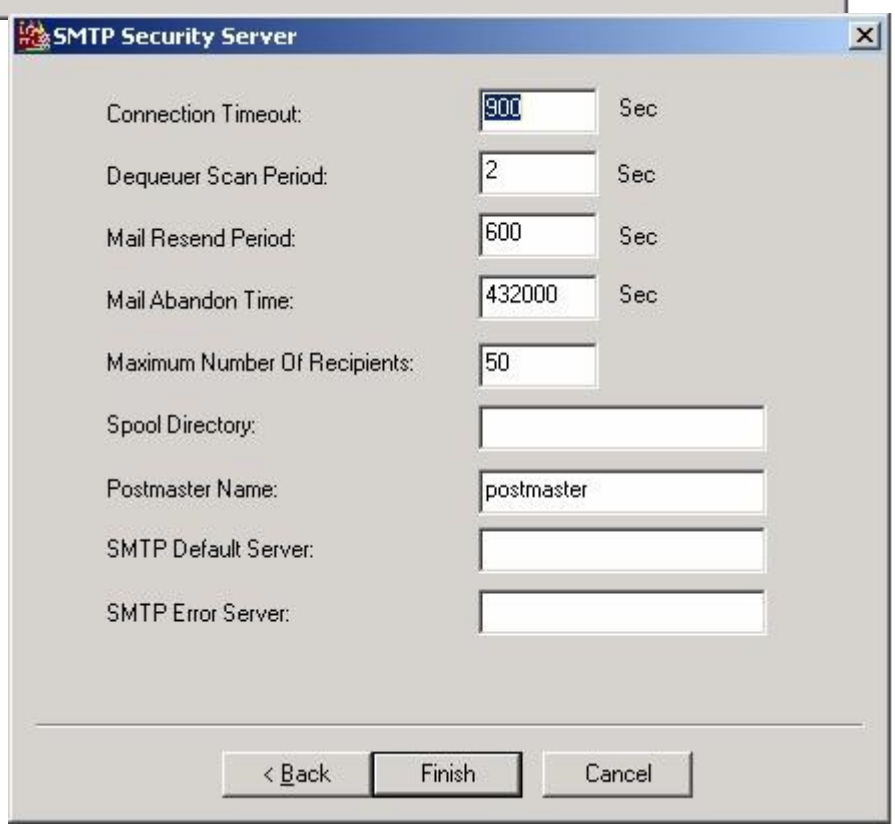
Ch n hostname c a Management Server:



Ch n ch d IP Forwarding:

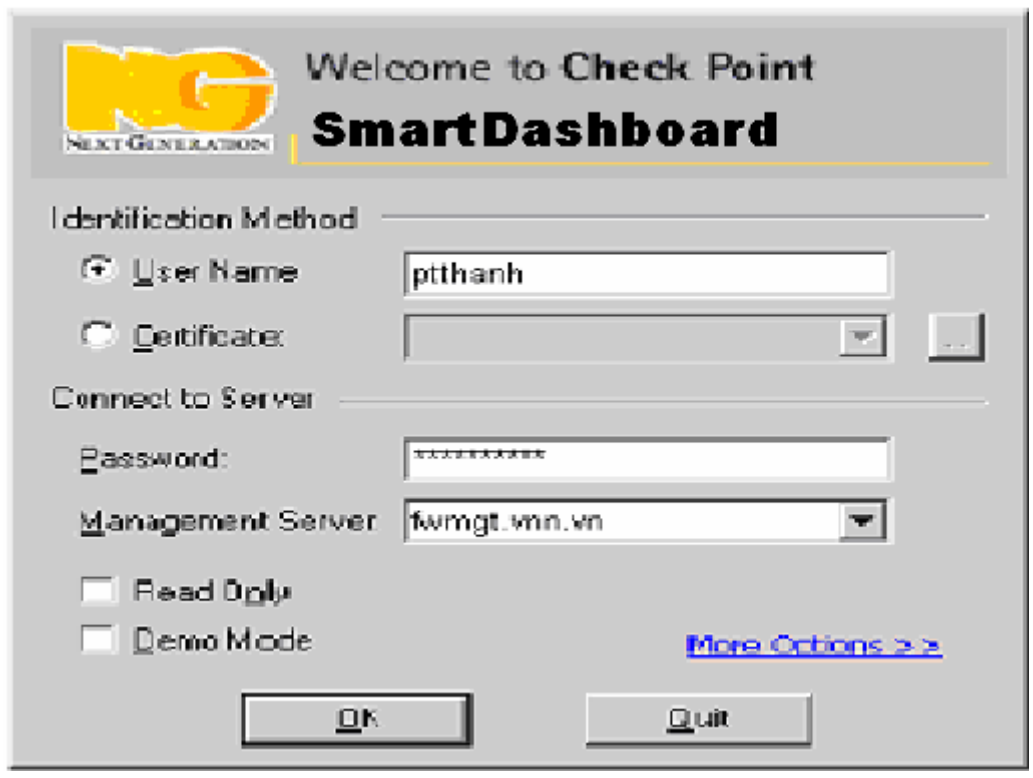


Đ t các tham s cho SMTP Security Server:



Ch n Finish d k t thúc quá trình cài d t r i Restart l i máy.

Sau khi restart l i máy, login vào màn hình console c a CheckPoint v i use password dã t o d thi t l p c u hình chovirel:



2.3.4. Thi t l p c u hình

Sau khi login vào màn hình di u khi n c a CheckPoint, ta b t d u ti n hành quá trình thi t l p c u hình cho firewall theo các bu c sau:

- Đ nh nghia cho các giao ti p (Interface) thu c m ng trong (Inside network) và m ngngoài (Outside network) c a máy ch cài CheckPoint.
- T o các Network thu c m ng trongTheo mô hình th nghi m dây là m ng 192.168.7.0 và 192.168.1.0.
- Nhóm các Inside network thành m t group d ti n qu n lý.
- Thi t l p các lu t d cho phép hoccm các truy nh p t trong ra ngoài và t ngoài vào trong. Các lu t này g m các thành ph n co b n sau:
  + S th t : bi u th m c d uu tiên c a lu t. Lu t nào có s th t càng nh thì m c d uu tiên càng l n.
  + Ngu n (SOURCE)
  + Đích (DESTINATION)
  + Giao ti p (IF VIA)
  + D ch v (SERVICE): các d ch v du c cho phép/c m
  + Hành d ng (ACTION): cho phép/c m
  + Ngoài ra còn có các tham s khác nhu TRACK, INSTALL ON, TIME …

Sau dây là m t ví d v thi t l p lu t cho firewall CheckPoint:

No.	Source	Destination	Service	Action	Track	Install On
1	Any	mailserver	smtp	accept		Gateways
2	Any	London	Any	drop		Gateways
3	localnet	DMZ	ftp	accept		Gateways
4	localnet	DMZ	http	accept		Gateways
5	localnet	DMZ	ftp	accept		Gateways
6	localnet	DMZ	http	accept		Gateways
7	Any	Any	Any	reject		Gateways

TÀI LI U THAM KH O

1. **Interconnecting Cisco Network Devices** - Steve McQuerry, 03/2000
2. **Building Scalable Cisco Internetworks** - Catherine Paquet, 01/2003
3. **Routing TCP/IP Volume I** - Jeff Doyle, 09/1998
4. **Cisco Internetworking Basic** - Cisco Press, 07/2001
5. **Cisco WEB site** http://www.cisco.com - Technologies
6. **Microsoft Windows 2000 advanced server** - Microsoft Press, 1985 1999
7. **DNS and BIND, 3trd Edition** - Paul Albitz and Cricket Liu, 09/1998
8. **Internet System Consortium WEB site** http://www.isc.org
9. **Remote Access Study Guide** - Robert Padjen, Todd Lammle, Wade Edwards, 9/2002
10. **Building Cisco Remote Access Networks** - Catherine Paquet, 08/1999.
11. **Complete Book of Remote Access:Connectivity and Security** , Victor Kasacavage (Editor), Weikai Yan, 12/2002
12. **Designing & Implementing Microsoft Proxy Server** - David Wolfe, Sams Net Publishing.
13. **ISA Server 2000 Administration Study Guide** - William Heldman (SybexMCSE).
14. **Configuring ISA server for an Enterprise** -Microsoft Training and Certification , 02/2001
15. **Designing & Implementting Microsoft Windows2000 Network Infrastructure,** Microsoft Training and Certification, 05/2000
16. **Firewalls and Internet Security** : Repelling the Wily Hacker, Steven M. Bellovin, 01/2003
17. **Inside Network Perimeter Security** , Karen Fredericks and Lenny Zeltser and Scott Winters, 01/2002
18. **CCSP Cisco Secure PIX Firewall Advanced Exam Certification Guide** , Greg Bastien and Christian Degu, 01/2003
19. **Building Internet Firewalls** , Elizabeth D. Zwicky & Simon Cooper, 01/2000
20. **Firewalls: A Complete Guide** , Marcus Goncalves, 01/1999
21. **Configuring ISA server for an Enterprise** -Microsoft Training and Certification, 02/2001

Khái niệm căn bản về thiết bị mạng

00:32' 12/01/2006 (GMT+7)

Để hệ thống mạng làm việc trơn tru, hiệu quả và khả năng kết nối tới những hệ thống mạng khác đòi hỏi phải sử dụng những thiết bị mạng chuyên dụng. Những thiết bị mạng này rất đa dạng và phong phú về chủng loại nhưng đều dựa trên những thiết bị cơ bản là Repeater, Hub, Switch, Router và Gateway.

Bài viết này sẽ giúp bạn đọc có được một những hiểu biết cơ bản về các thiết bị mạng kể trên:

Repeater

Trong một mạng LAN, giới hạn của cáp mạng là 100m (cho loại cáp mạng CAT 5 UTP – là cáp được dùng phổ biến nhất), bởi tín hiệu bị suy hao trên đường truyền nên không thể đi xa hơn. Vì vậy, để có thể kết nối các thiết bị ở xa hơn, mạng cần các thiết bị để khuếch đại và định thời lại tín hiệu, giúp tín hiệu có thể truyền dẫn đi xa hơn giới hạn này.

Repeater là một thiết bị ở lớp 1 (*Physical Layer*) trong mô hình OSI. Repeater có vai trò khuếch đại tín hiệu vật lý ở đầu vào và cung cấp năng lượng cho tín hiệu ở đầu ra để có thể đến được những chặng đường tiếp theo trong mạng. Điện tín, điện thoại, truyền thông tin qua sợi quang… và các nhu cầu truyền tín hiệu đi xa đều cần sử dụng Repeater.

Hub

Hub được coi là một Repeater có nhiều cổng. Một Hub có từ 4 đến 24 cổng và có thể còn nhiều hơn. Trong phần lớn các trường hợp, Hub được sử dụng trong các mạng 10BASE-T hay 100BASE-T. Khi cấu hình mạng là hình sao (*Star topology*), Hub đóng vai trò là trung tâm của mạng. Với một Hub, khi thông tin vào từ một cổng và sẽ được đưa đến tất cả các cổng khác.

Hub có 2 loại là Active Hub và Smart Hub. Active Hub là loại Hub được dùng phổ biến, cần được cấp nguồn khi hoạt động, được sử dụng để khuếch đại tín hiệu đến và cho tín hiệu ra những cổng còn lại, đảm bảo mức tín hiệu cần thiết. Smart Hub (*Intelligent Hub*) có chức năng tương tự như Active Hub, nhưng có tích hợp thêm chip có khả năng tự động dò lỗi - rất hữu ích trong trường hợp dò tìm và phát hiện lỗi trong mạng.

Bridge

Bridge là thiết bị mạng thuộc lớp 2 của mô hình OSI (*Data Link Layer*). Bridge được sử dụng để ghép nối 2 mạng để tạo thành một mạng lớn duy nhất. Bridge được sử dụng phổ biến để làm cầu nối giữa hai mạng Ethernet. Bridge quan sát các gói tin (*packet*) trên mọi mạng. Khi thấy một gói tin từ một máy tính thuộc mạng này chuyển tới một máy tính trên mạng khác, Bridge sẽ sao chép và gửi gói tin này tới mạng đích.

Ưu điểm của Bridge là hoạt động trong suốt, các máy tính thuộc các mạng khác nhau vẫn có thể gửi các thông tin với nhau đơn giản mà không cần biết có sự "can thiệp" của Bridge. Một Bridge có thể xử lý được nhiều lưu thông trên mạng như Novell, Banyan... cũng như là địa chỉ IP cùng một lúc. Nhược điểm của Bridge là chỉ kết nối những mạng cùng loại và sử dụng Bridge cho những mạng hoạt động nhanh sẽ khó khăn nếu chúng không nằm gần nhau về mặt vật lý.

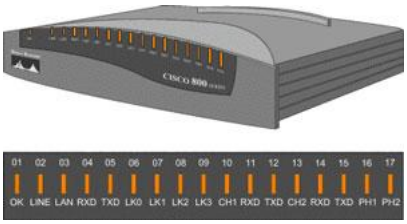
Switch

Switch đôi khi được mô tả như là một Bridge có nhiều cổng. Trong khi một Bridge chỉ có 2 cổng để liên kết được 2 segment mạng với nhau, thì Switch lại có khả năng kết nối được nhiều segment lại với nhau tuỳ thuộc vào số cổng (port) trên Switch. Cũng giống như Bridge, Switch cũng "học" thông tin của mạng thông qua các gói tin (*packet*) mà nó nhận được từ các máy trong mạng. Switch sử dụng các thông tin này để xây dựng lên bảng Switch, bảng này cung cấp thông tin giúp các gói thông tin đến đúng địa chỉ.

Ngày nay, trong các giao tiếp dữ liệu, Switch thường có 2 chức năng chính là chuyển các khung dữ liệu từ nguồn đến đích, và xây dựng các bảng Switch. Switch hoạt động ở tốc độ cao hơn nhiều so với Repeater và có thể cung cấp nhiều chức năng hơn như khả năng tạo mạng LAN ảo (VLAN).

Router

Router là thiết bị mạng lớp 3 của mô hình OSI (*Network Layer*). Router kết nối hai hay nhiều mạng IP với nhau. Các máy tính trên mạng phải "nhận thức" được sự tham gia của một router, nhưng đối với các mạng IP thì một trong những quy tắc của IP là mọi máy tính kết nối mạng đều có thể giao tiếp được với router.



Ưu điểm của Router: Về mặt vật lý, Router có thể kết nối với các loại mạng khác lại với nhau, từ những Ethernet cục bộ tốc độ cao cho đến đường dây điện thoại đường dài có tốc độ chậm.

Nhược điểm của Router: Router chậm hơn Bridge vì chúng đòi hỏi nhiều tính toán hơn để tìm ra cách dẫn đường cho các gói tin, đặc biệt khi các mạng kết nối với nhau không cùng tốc độ. Một mạng hoạt động nhanh có thể phát các gói tin nhanh hơn nhiều so với một mạng chậm và có thể gây ra sự nghẽn mạng. Do đó, Router có thể yêu cầu máy tính gửi các gói tin đến chậm hơn. Một vấn đề khác là các Router có đặc điểm chuyên biệt theo giao thức - tức là, cách một máy tính kết nối mạng giao tiếp với một router IP thì sẽ khác biệt với cách nó giao tiếp với một router Novell hay DECnet. Hiện nay vấn đề này được giải quyết bởi một mạng biết đường dẫn của mọi loại mạng được biết đến. Tất cả các router thương mại đều có thể xử lý nhiều loại giao thức, thường với chi phí phụ thêm cho mỗi giao thức.

Gateway

Gateway cho phép nối ghép hai loại giao thức với nhau. Ví dụ: mạng của bạn sử dụng giao thức IP và mạng của ai đó sử dụng giao thức IPX, Novell, DECnet, SNA... hoặc một giao thức nào đó thì Gateway sẽ chuyển đổi từ loại giao thức này sang loại khác.

Qua Gateway, các máy tính trong các mạng sử dụng các giao thức khác nhau có thể dễ dàng "nói chuyện" được với nhau. Gateway không chỉ phân biệt các giao thức mà còn còn có thể phân biệt ứng dụng như cách bạn chuyển thư điện tử từ mạng này sang mạng khác, chuyển đổi một phiên làm việc từ xa...

Phân biệt đèn chỉ thị trong Cisco Switch

13:57' 22/01/2006 (GMT+7)

Là nhân viên công ty có hệ thống mạng máy tính lớn, có sử dụng nhiều switch của Cisco, mỗi khi nhìn thấy các đèn nhấp nháy của Switch như dải đèn của máy nghe nhạc, trông chúng thật hấp dẫn và cuốn hút, nhưng liệu bạn có biết chúng truyền tải thông điệp gì?

Vậy, thực chất những giải đèn này nhằm mục đích gì, nguyên tắc hoạt động như thế nào, và chức năng ra sao? Bài viết này sẽ giải đáp những thắc mắc giùm bạn.

Giống như các loại thiết bị điện tử khác, Switch cũng có các loại đèn chỉ thị để cho người sử dụng có thể biết được trạng thái hoạt động của nó. Switch gồm có 4 loại đèn ở phía trước:

- **Đèn hệ thống - System Led**
- **Đèn nguồn nuôi bên ngoài - Remote Power Supply Led(RPS)**
- **Đèn chế độ báo hiệu - Port Mode Led**
- **Đèn trạng thái các cổng - Port status Led**

Đèn hệ thống - System Led

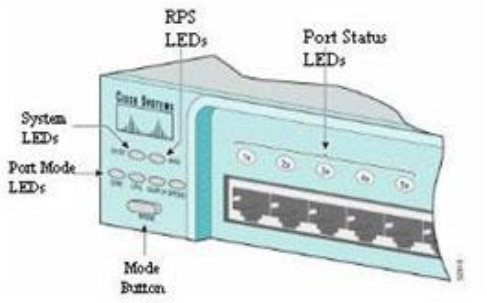
Đèn hệ thống thông báo hệ thống đang được cấp nguồn và đang hoạt động đúng chức năng hay chưa. Mỗi khi cắm dây nguồn, Switch sẽ bắt đầu quá trình kiểm tra phần cứng. Trong quá trình này, đèn hệ thống sẽ không sáng. Sau đó, nếu kiểm tra thành công, đèn sẽ báo màu xanh lá cây. Ngược lại, khi có lỗi đèn sẽ có màu da cam. Thật đáng rất tiếc, khi có đèn có màu cam điều này cũng có nghĩa là bạn phải đem thiết bị đi bảo hành.

Đèn nguồn nuôi bên ngoài- RPS

Đèn nguồn nuôi bên ngoài thông báo Switch đang được cấp nguồn nuôi từ bên ngoài hay không. Đèn này chỉ sáng khi switch được cấp nguồn từ ngoài.

Đèn chế độ báo hiệu và đèn trạng thái cổng

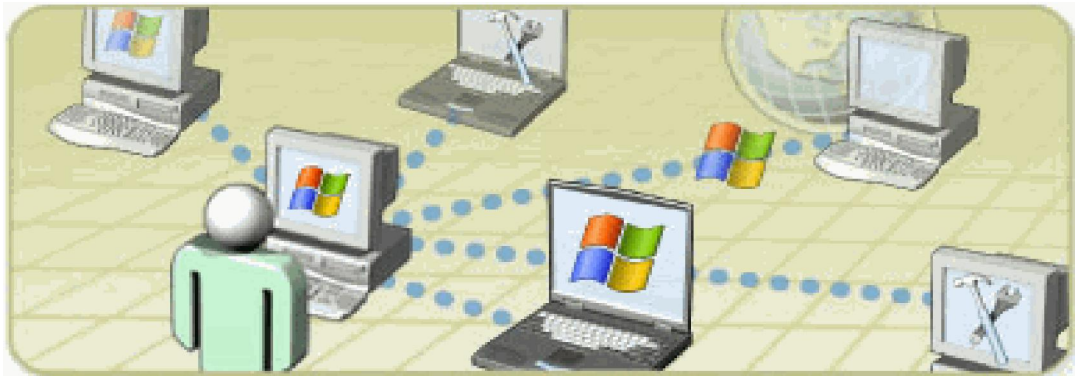
Đèn báo chế độ báo hiệu có 4 chế độ (STAT, UTL, FDUP, SPEED), bạn có thể chọn các chế độ bằng cách bấm vào phím "Mode", được mô tả trong hình vẽ sau:



Ứng với mỗi chế độ báo hiệu, vai trò hiển thị của các đèn trạng thái cổng sẽ tương ứng theo bảng sau:

Đèn chế độ báo hiệu	Đèn trạng thái cổng	Giải thích
STAT	Tắt	Cổng tương ứng không có kết nối
	Xanh liên lục	Đang khởi động kết nối
	Xanh nhấp nháy	Cổng đang trao đổi dữ liệu
	Nháy xanh/da cam	Kết nối bị lỗi
	Da cam liên tục	Cổng đang bị khoá
UTL	Tắt	Mỗi một đèn trạng thái cổng khi tắt sẽ chỉ thị Switch sử dụng băng thông giảm đi một nửa. Các đèn sẽ tắt theo thứ tự từ phải sang trái. Nếu đèn ở ngoài cùng bên phải tắt có nghĩa là Switch đang sử dụng ít hơn 50% tổng băng thông. Nếu đèn tiếp theo tắt thì Switch đang sử dụng ít hơn 25% tổng băng thông ....
	Xanh	Nếu tất cả các đèn đều xanh có nghĩa là Switch đang sử dụng trên 50% tổng băng thông
FDUP	Tắt	Cổng đang chạy ở chế độ bán song công (half-duplex)
	Xanh	Cổng đang chạy ở chế độ song công (full-duplex)
Speed	Tắt	Cổng chạy với tốc độ 10Mbps
	Xanh	Cổng chạy với tốc độ 100Mbps

Các thiết bị Mạng

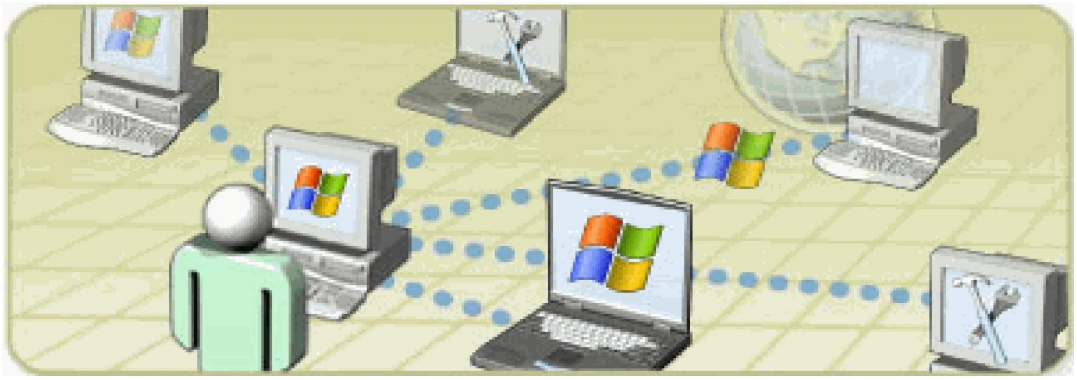


Nội Dung

- Network Interface Card
- Repeater
- HUB
- Bridge
- Switch
- Router
- Gateway
- Modem: ADSL, Dial-up

Network Interface Card

- Card mạng (NIC)
  - Là thiết bị kết nối giữa máy tính và cáp mạng
  - Chúng thường giao tiếp với nhau thông qua các khe cắm như: PCI, ISA, USB, PCMCIA
  - Phần giao tiếp với cáp mạng thông thường theo các chuẩn như: UTP, BNC, AUI



Network Interface Card

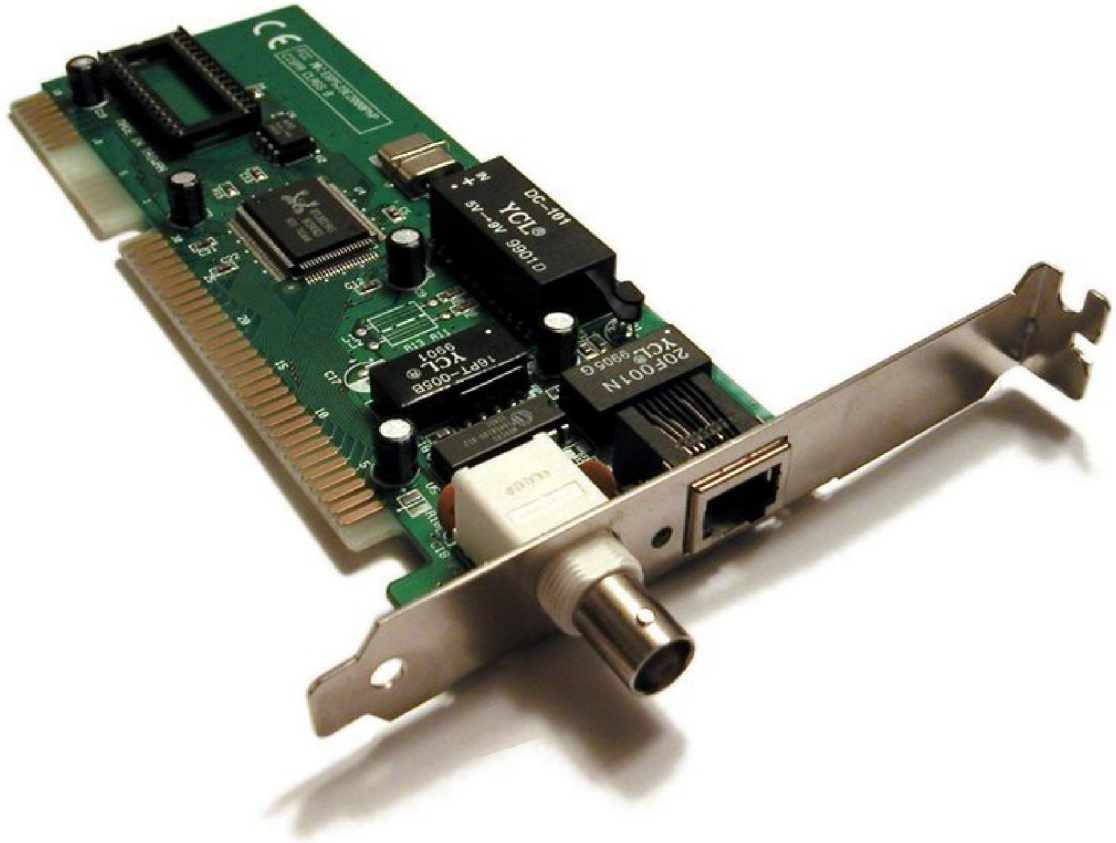
- Chức năng của NIC:
  - Chuẩn bị dữ liệu đưa lên mạng: trước khi đưa lên mạng, dữ liệu sẽ được chuyển từ dạng Byte, Bit sang tín hiệu điện để truyền trên cáp
  - Gởi dữ liệu đến máy tính khác
  - Kiểm soát luồng dữ liệu giữa máy tính và hệ thống cáp

Network Interface Card

- Địa chỉ MAC (Media Access Control)
  - Mỗi Card mạng đều có 1 địa chỉ riêng để phân biệt với các Card mạng khác
  - Do IEEE (Viện công nghệ điện-điện tử) cấp cho các nhà sản xuất Card mạng
  - Địa chỉ này gồm 6byte (48bit), có dạng: XXXXXX.XXXXXX
  - 3byte đầu là mã số của NSX, 3byte sau là số serial của Card mạng

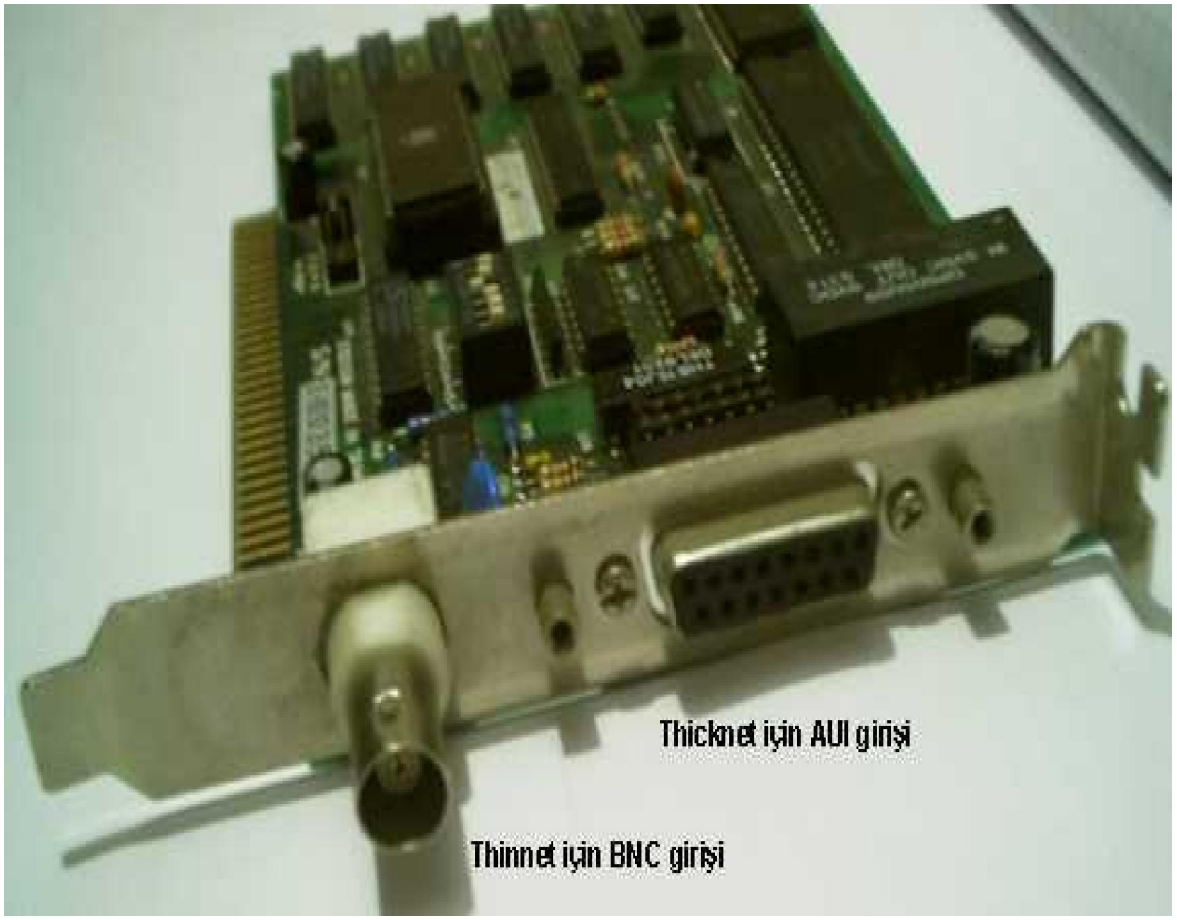
Network Interface Card

- Card mạng chuẩn BNC, UTP, STP



Network Interface Card

- Card mạng chuẩn BNC, AUI

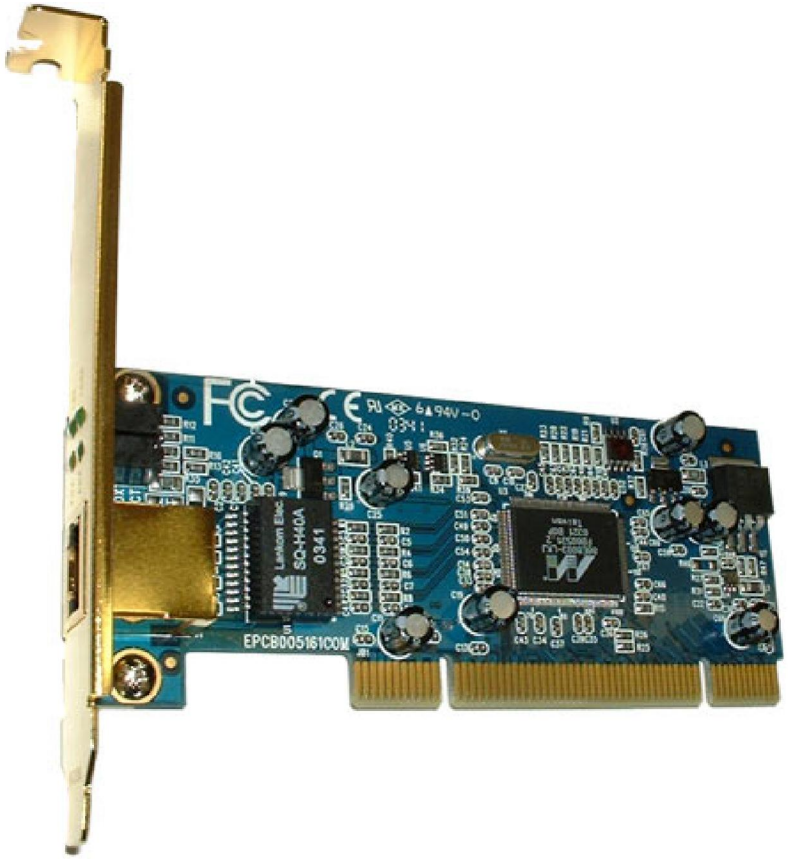


Network Interface Card

- Card mạng RE100TX (10/100BaseT)

Network Interface Card

- Card mạng FL1000T (10/100/1000BaseT)

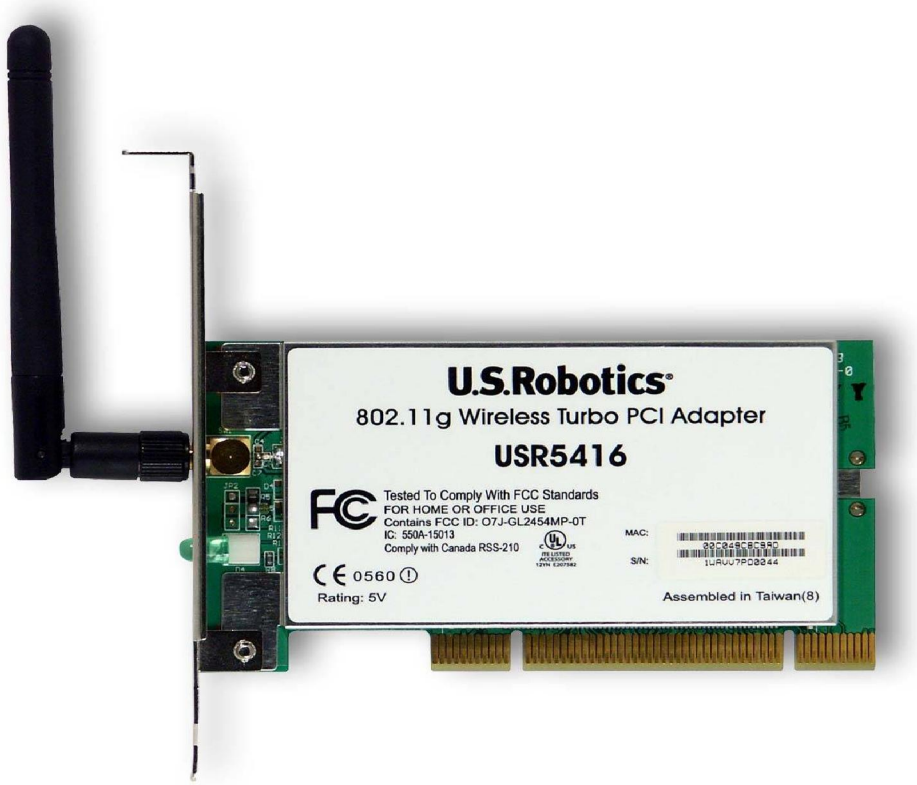


Network Interface Card

- Card mạng USB (10/100BaseT)

Network Interface Card

- Card mạng không dây (Desktop PC)

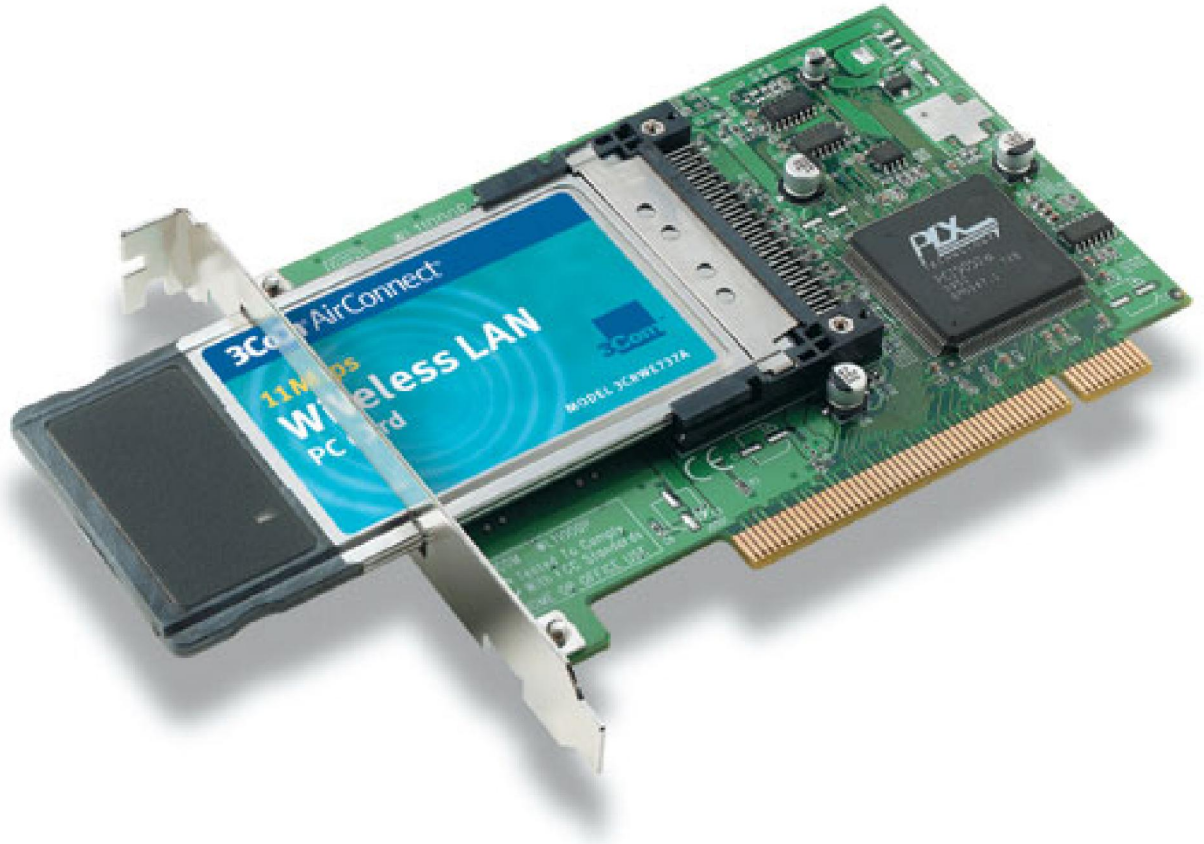


Network Interface Card

- Card mạng không dây PCMCIA (Laptop)

Network Interface Card

- Card mạng không dây PCMCIA (Desktop)



Network Interface Card

- Card mạng không dây USB (54Mbps)

Network Interface Card

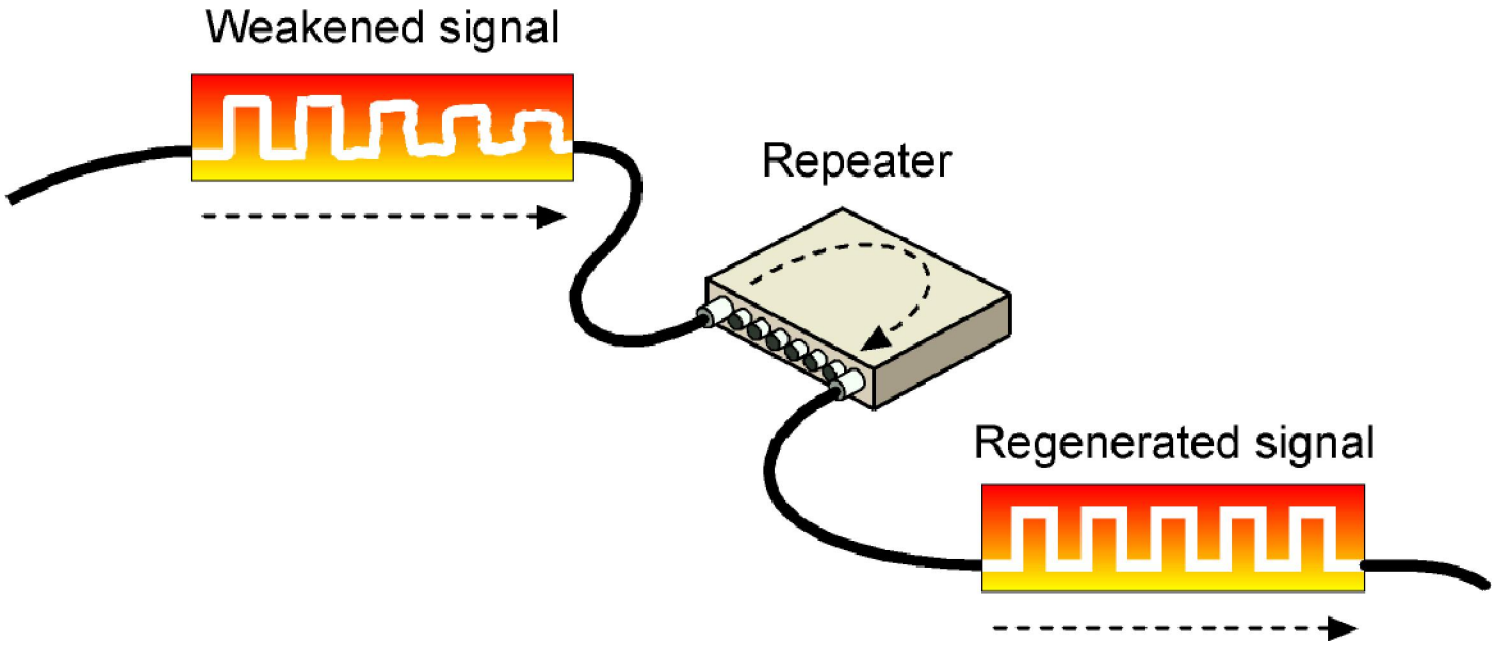
- Card mạng không dây USB (54Mbps)

Repeater

- Repeater:
  - Là thiết bị dùng để khuyếch đại tín hiệu trên các đoạn cáp dài
  - Hoạt động ở lớp vật lý nên chỉ hiểu tín hiệu điện không lọc được bất kỳ dạng nào
  - Chú ý nếu cứ tiếp tục dùng nhiều Repeater để khuyếch đại và mở rộng kích thước mạng thì tín hiệu sẽ sai lệch dần
  - Áp dụng nhiều trong mô hình mạng Bus

Repeater

- Repeater:



Repeater

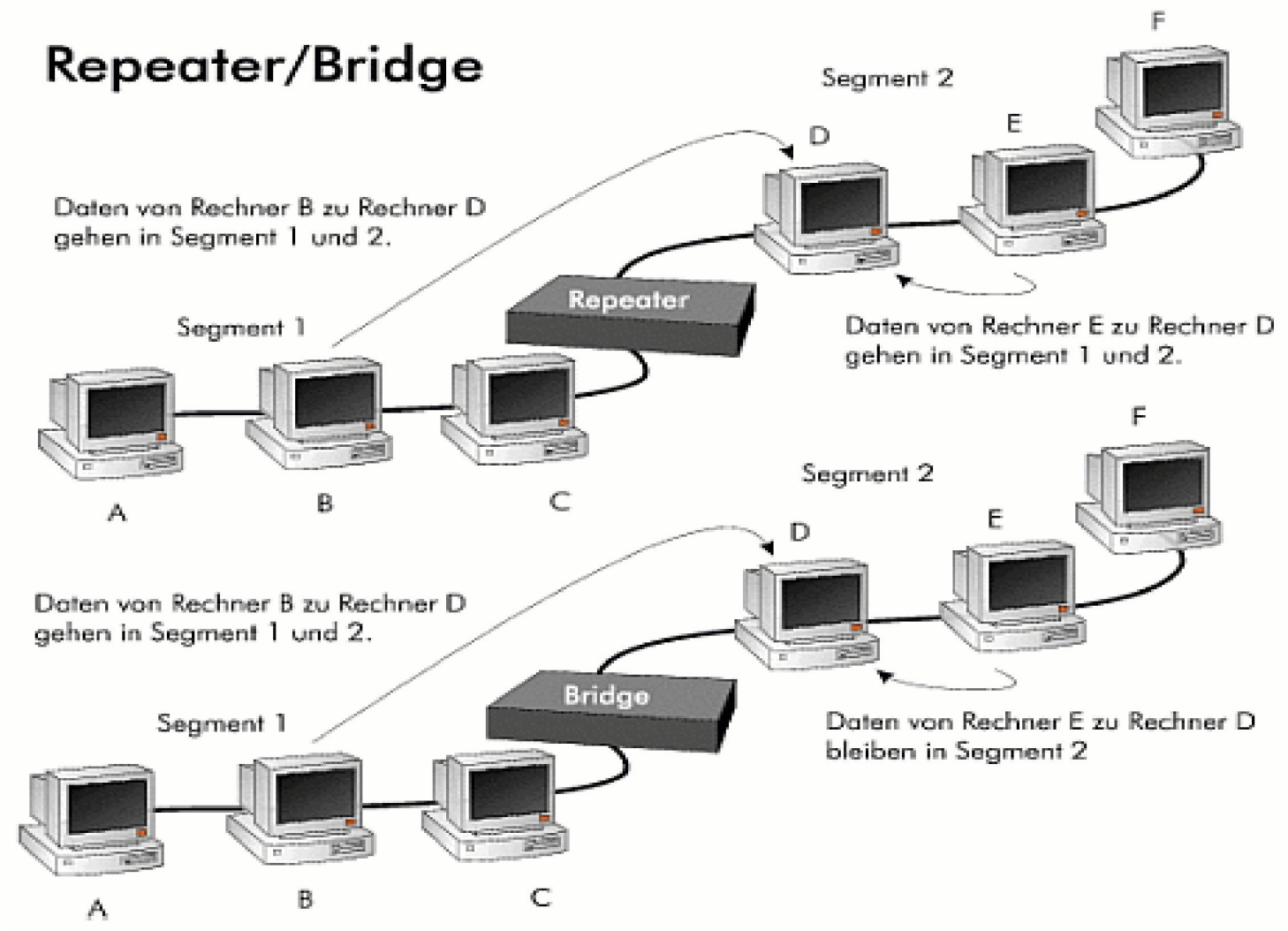
- Repeater:

Repeater

Repeater

- Repeater:

Repeater

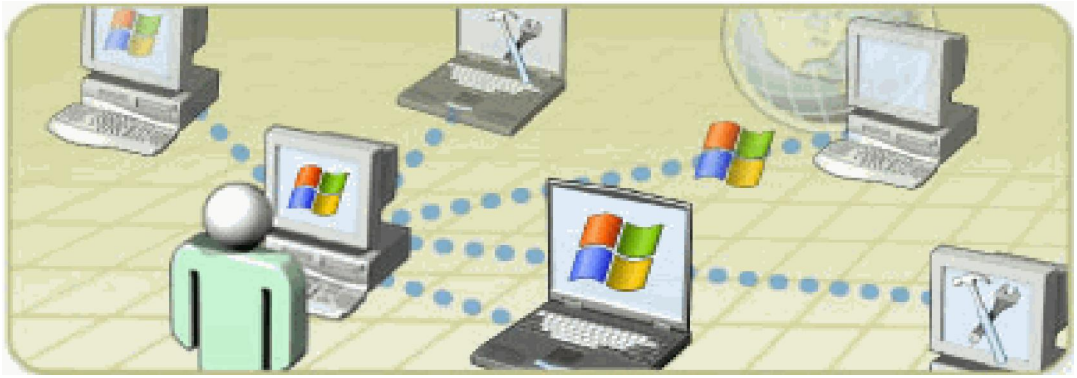


HUB

- HUB:
  - Là thiết bị giống như Repeater nhưng nhiều Port hơn, cho phép kết nối nhiều máy tính với nhau
  - Cũng khuyếch đại tín hiệu điện và truyền đến tất cả các port còn lại đồng thời không lọc được dữ liệu
  - Thông thường HUB hoạt động ở tầng vật lý trong mô hình OSI

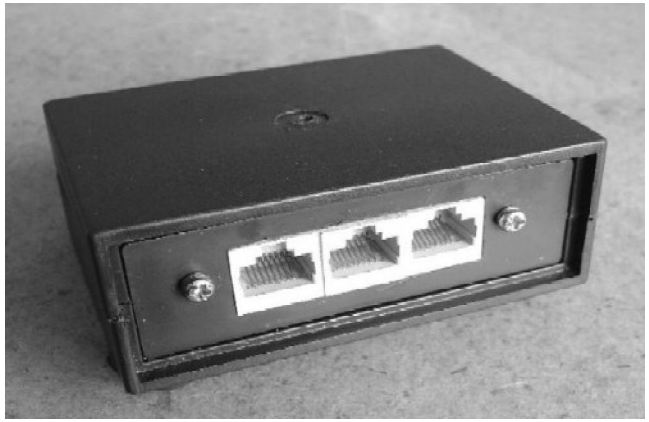
HUB

- Hub được chia thành 3 loại:
  - Passive Hub: (Hub thụ động)
  - Active Hub: (Hub chủ động)
  - Intelligent Hub: (Hub thông minh)



HUB

- Passive Hub:
  - Là thiết bị đấu nối cáp dùng để chuyển tiếp tín hiệu từ cổng giao tiếp này sang các cổng giao tiếp khác
  - Không có chức năng khuyếch đại tín hiệu, xử lý tín hiệu vì không có các linh kiện điện tử và nguồn điện riêng

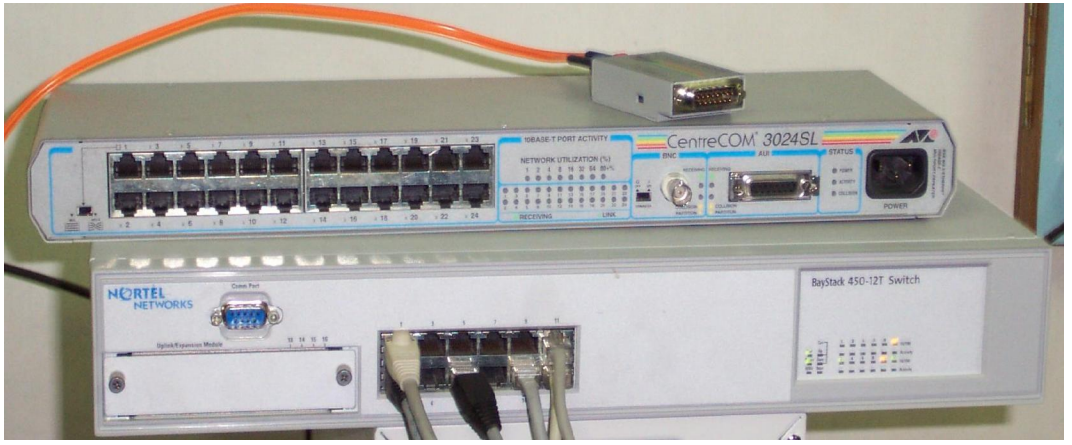


HUB

- Active Hub:
  - Là thiết bị đấu nối cáp dùng để chuyển tiếp tín hiệu từ cổng giao tiếp này sang các cổng giao tiếp khác với chất lượng cao hơn
  - Thiết bị này có sử dụng các linh kiện điện tử, và nguồn riêng để khuyếch đại, xử lý tín hiệu

HUB

- Intelligent Hub:
  - Là 1 Active Hub nhưng nó có thêm các tính năng vượt trội như:
    - Cho phép quản lý từ các máy tính
    - Sử dụng cơ chế chuyển mạch (switching)
    - Cho phép chuyển đến đúng port cần nhận



Bridge

- Bridge:
  - Dùng để kết nối các phân đoạn mạng nhỏ có cùng cách đánh địa chỉ và công nghệ mạng lại với nhau
  - Các dữ liệu chỉ trao đổi trong một phân đoạn mạng sẽ không được truyền qua phân đoạn khác
  - Để lọc được các gói tin và biết gói tin nào thuộc nhánh mạng nào thì Bridge chứa 1 bảng địa chỉ MAC

Bridge

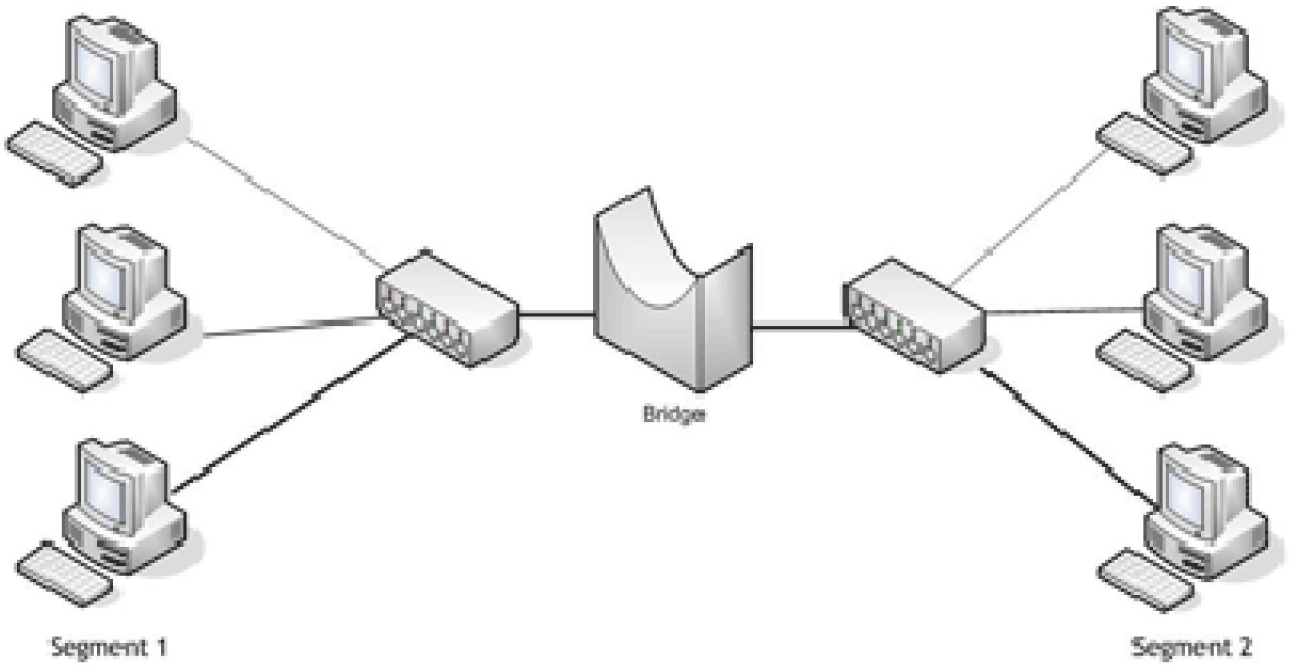
- Bridge:
  - Tất cả các địa chỉ MAC của các nhánh mạng đều phải được cập nhật vào bảng MAC này (tự động, bằng tay)
  - Khi thấy một gói tin từ một máy tính thuộc mạng này chuyển tới một máy tính trên mạng khác, Bridge sẽ sao chép và gửi gói tin này tới mạng đích
  - Bridge có thể nối nhiều hub/Switch lại với nhau tạo thành một hệ thống mạng chung

Bridge

- Bridge:

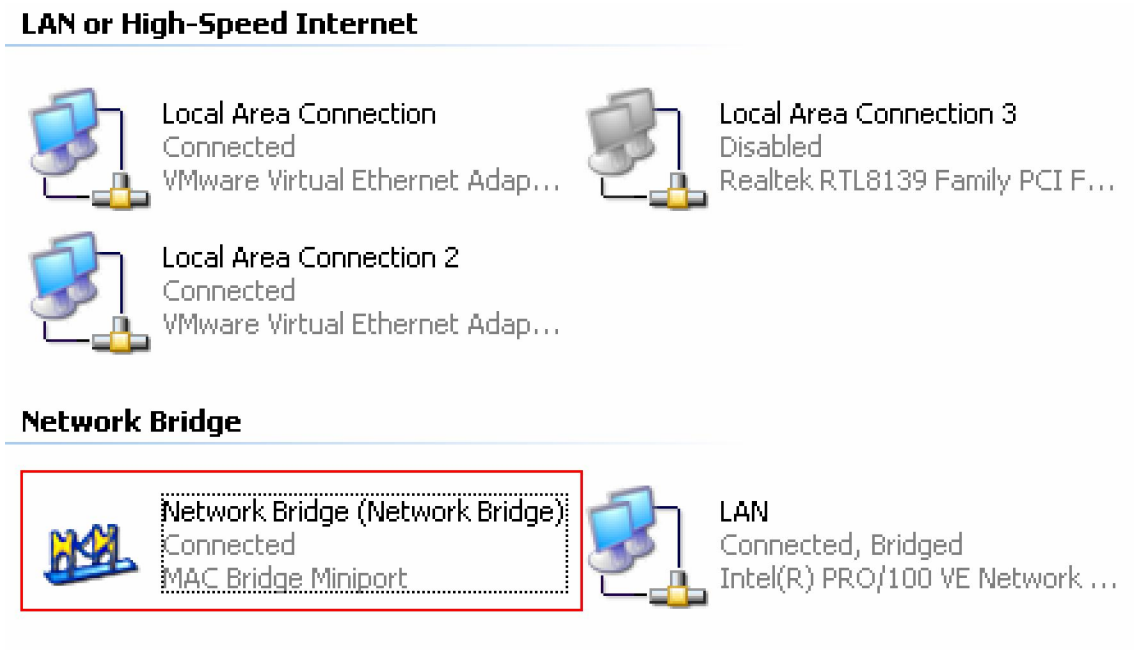
Bridge

- Bridge:



Bridge

- Bridge mềm trên windows:
  - Mục đích là share Net cho 1 máy thứ 2. Tức là máy thứ 1 có 2 card mạng, card thứ 1 kết nối ra Net, card thứ 2 kết nối với máy muốn share Net



Bridge

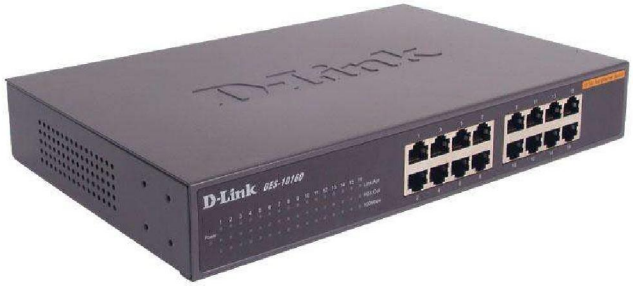
- Ưu điểm:
  - Cho phép mở rộng cùng một mạng logic với nhiều kiểu cáp khác nhau
  - Chia mạng thành nhiều phân đoạn khác nhau
- Khuyết điểm:
  - Chậm hơn Repeater vì phải xử lý các gói tin
  - Chưa tìm được đường đi tối ưu trong trường hợp có nhiều đường đi
  - Chỉ kết nối 2 mạng có cùng giao thức

Switch

- Switch:
  - Là thiết bị giống như Bridge nhưng nhiều port hơn, cho phép ghép nhiều đoạn mạng với nhau
  - Switch cũng dựa vào bảng địa chỉ MAC để định ra đường đi tốt nhất cho dữ liệu truyền qua nó
  - Switch hiểu được địa chỉ MAC nên hoạt động ở tầng Data-link

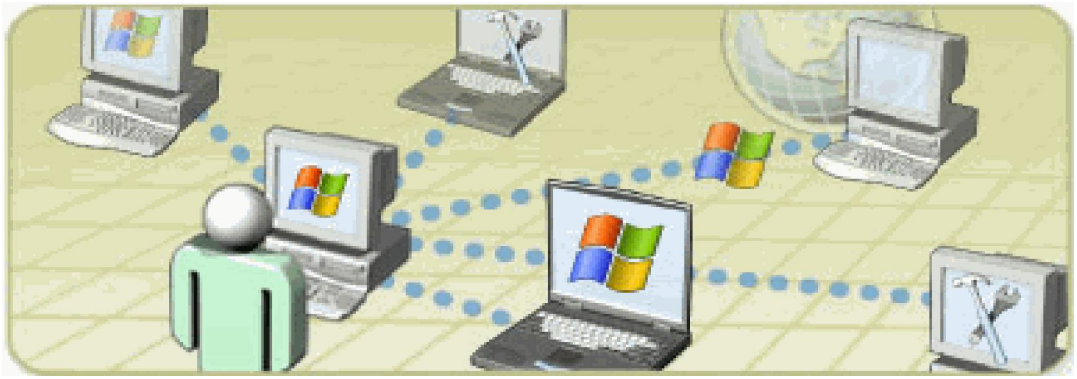
Switch

- Switch:



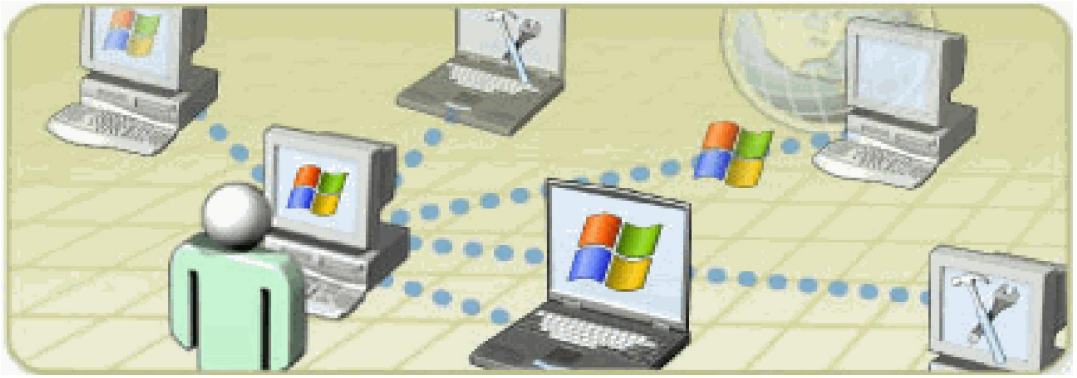
Switch

- Các tính năng mở rộng của Switch:
  - Store and Forward (bộ nhớ đệm)
  - Cut Through (chuyển tiếp)
  - Trunking (MAC base)
  - VLAN (mạng ảo)



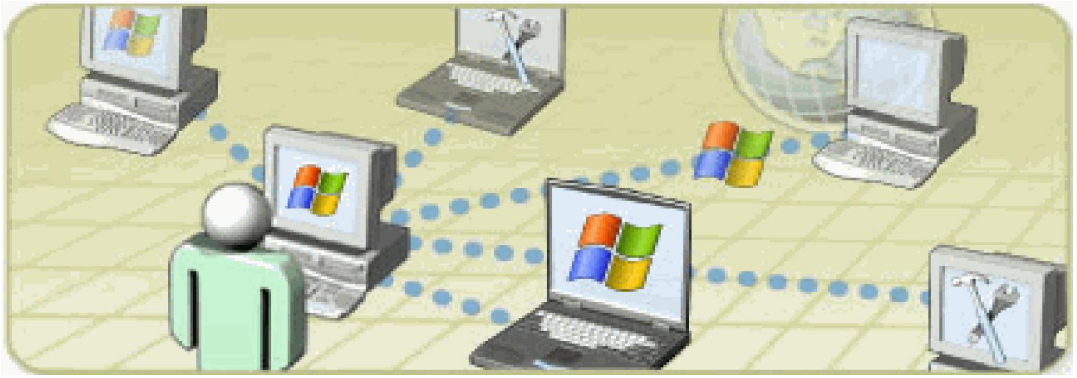
Switch

- Store and Forward:
  - Là tính năng lưu dữ liệu trong bộ đệm trước khi truyền sang các port khác để tránh đụng độ
  - Với kỹ thuật này tất cả gói tin phải được nhận đủ trước khi Switch chuyển Frame này đi do đó độ trễ phụ thuộc vào chiều dài của Frame



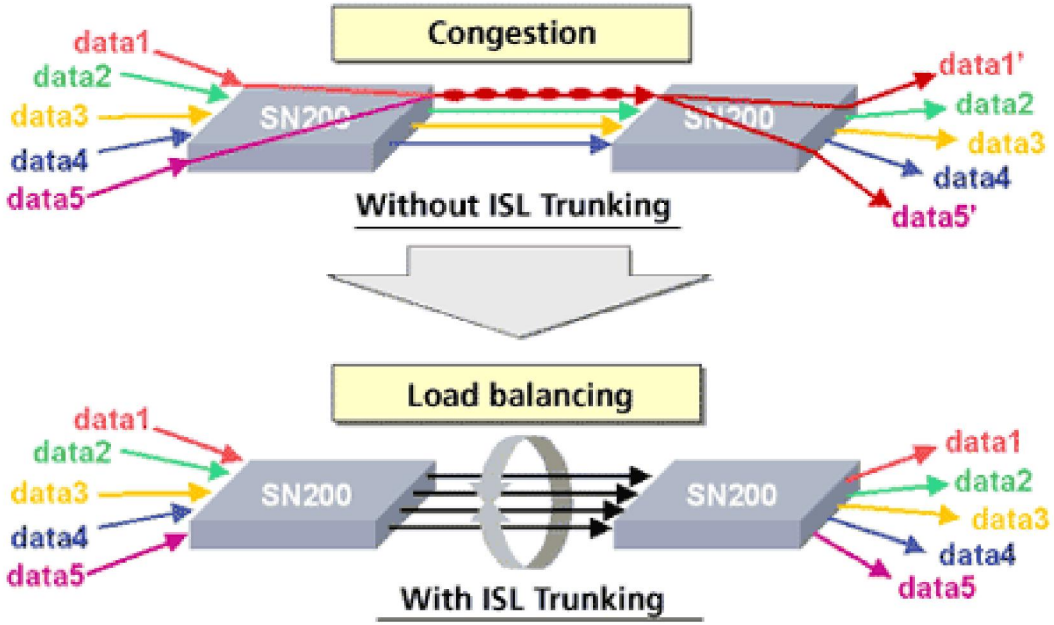
Switch

- Cut Through (chuyển tiếp):
  - Switch sẽ chuyển gói tin ngay lập tức một khi nó biết được địa chỉ đích của gói tin
  - Kỹ thuật này có độ trễ thấp hơn so với kỹ thuật Store and Forward



Switch

- Trunking (MAC Base):
  - Tính năng này giúp tăng tốc độ truyền giữa 2 Switch
  - Nhưng chú ý 2 Switch phải cùng loại, tốc độ

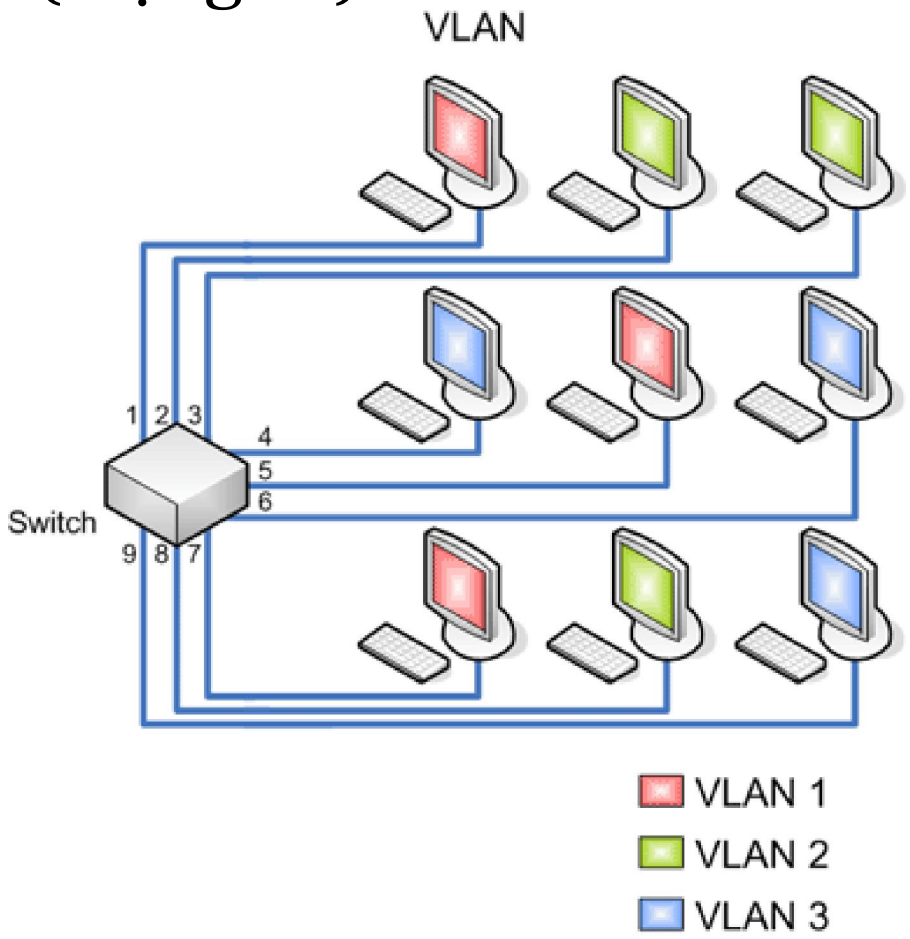


Switch

- VLAN (mạng ảo):
  - Tạo các mạng ảo nhằm đảm bảo tính bảo mật khi mở rộng mạng bằng cách nối các Switch với nhau
  - Mô hình:

Switch

- VLAN (mạng ảo):



Router

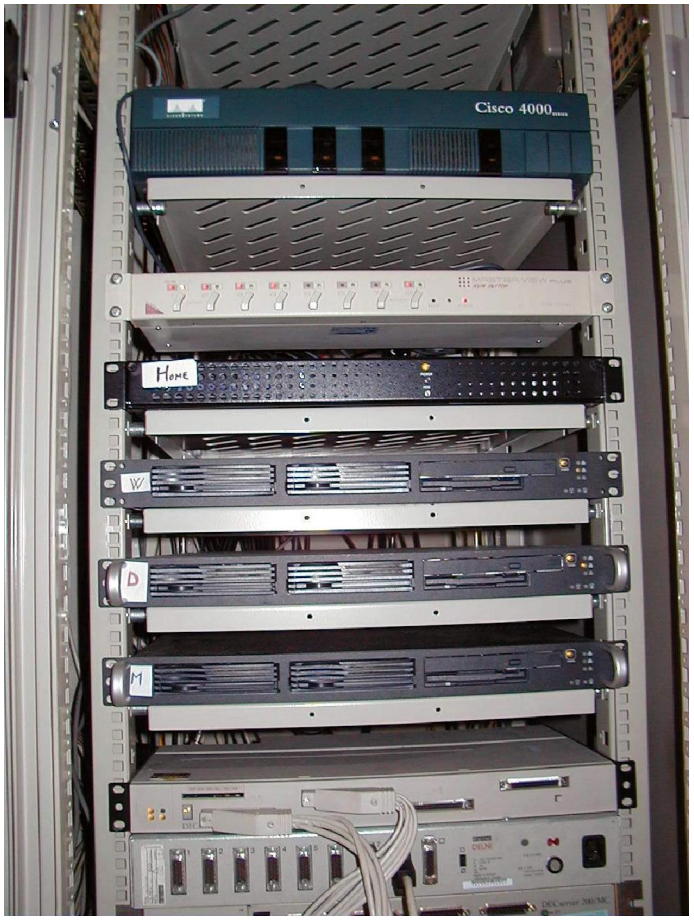
- Router:
  - Là bộ định tuyến dùng để kết nối nhiều phân đoạn mạng, hay nhiều kiểu mạng khác nhau
  - Thông thường router có 1 bộ xử lý, bộ nhớ, và các cổng giao tiếp
  - Khả năng vận chuyển dữ liệu với độ thông minh cao bằng cách xác định đường đi ngắn nhất

Router

- Router:
  - Các router dùng bảng định tuyến (routing table), bảng này chứa các thông tin về: đường đi, ước lượng thời gian, khoảng cách…
  - Router cũng có 2 loại:
    - **Router cứng**
    - **Router mềm**

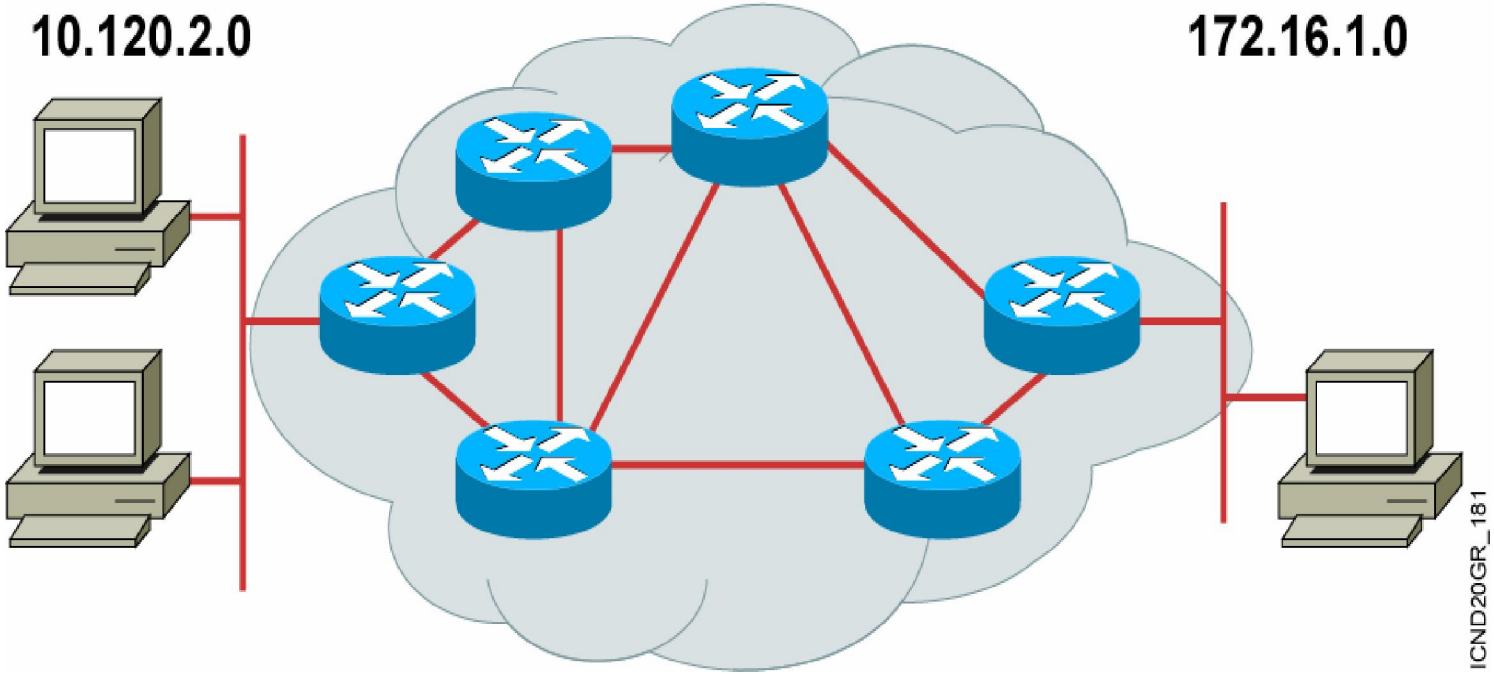
Router

- Router:



Router

- Mô hình:



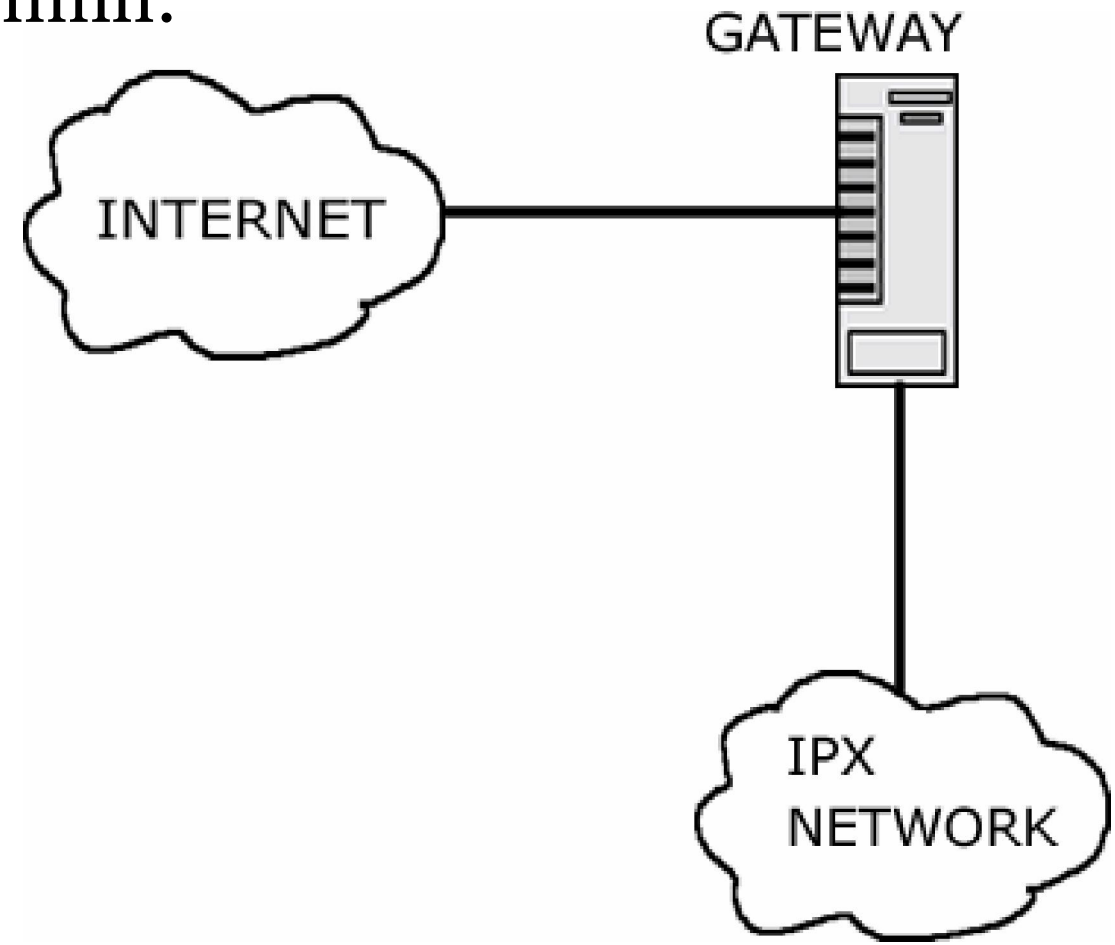
Gateway

- Gateway:
  - **Gateway cho phép nối ghép hai loại giao thức với nhau**
  - **Các máy tính trong các mạng sử dụng các giao thức khác nhau có thể dễ dàng "nói chuyện" được với nhau**
  - Ví dụ: mạng của bạn sử dụng giao thức TCP/IP và mạng của ai đó sử dụng giao thức IPX/SPX, hoặc một giao thức nào đó thì Gateway sẽ chuyển đổi từ loại giao thức này sang loại khác

Gateway

Gateway

- Mô hình:



Modem

- Modem:
  - Là thiết bị dùng để chuyển đổi từ tín hiệu số (Digital) sang tín hiệu tuần tự (Analog) và ngược lại
  - Modem chia thành 2 loại: Internal, External

Modem

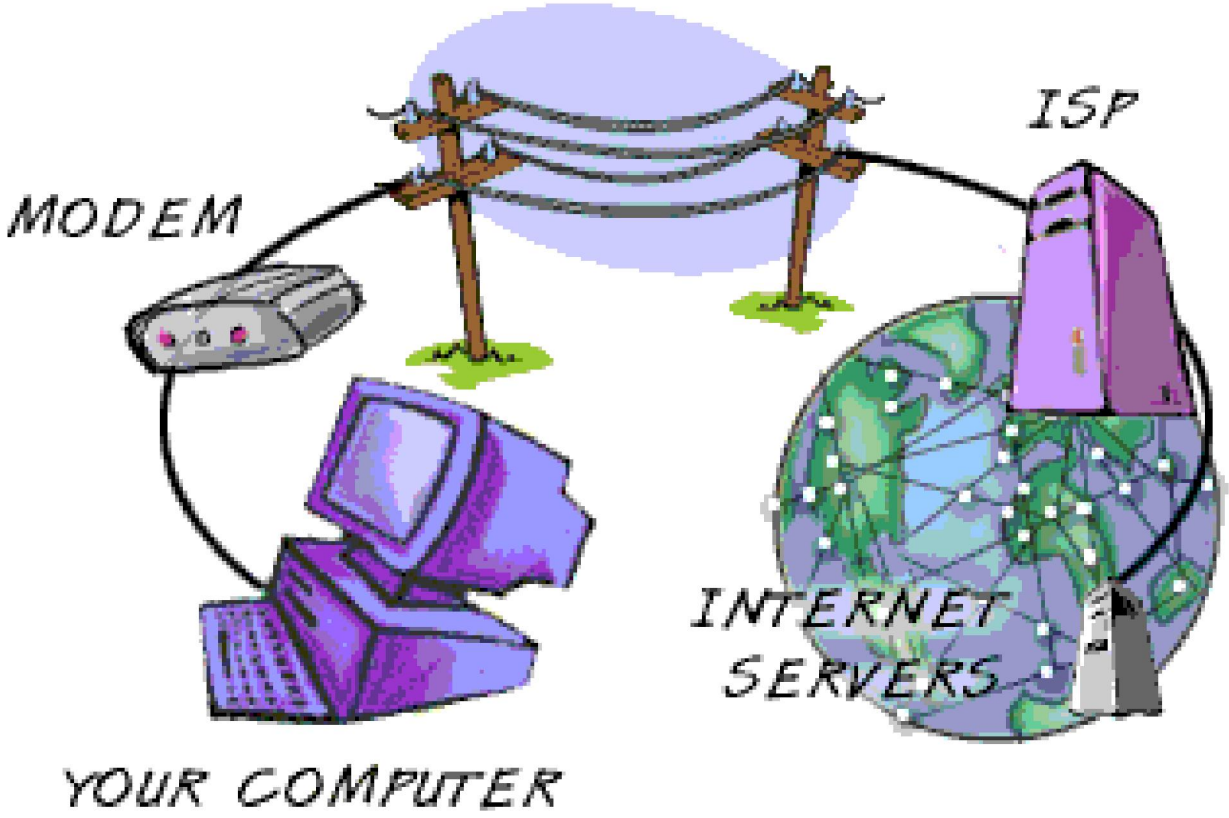
- Modem Internal:
  - Giao tiếp với máy tính bằng các khe cắm mở rộng như: PCI, ISA
  - Tốc độ truy cập trên lý thuyết 56Kbps
- Modem External:
  - Giao tiếp với máy tính bằng cổng COM, USB
  - Tốc độ truy cập trên lý thuyết 56Kbps

Modem

- Tính năng:
  - Phương tiện truyền dẫn của modem là cáp điện thoại, sử dụng đầu RJ11 để giao tiếp
  - Dùng kết nối Dial-up để kết nối ra NET
  - Có thể kết nối 2 mạng LAN với nhau tạo thành 1 mạng WAN
  - Có thể quản lý từ xa bằng công cụ RAS

Modem

- Mô hình:



Modem

- Mô hình LAN to LAN: