CCNA Exam Preparation

CCNA

TÀI LIỆU TIẾNG VIỆT

LỜI NÓI ĐẦU

Cuốn sách "Giáo trình hệ tính CCNA 2" được biện soạn dựa trên chương trình đào tạo chuyên viên mạng của Cisco. Lần xuất bản thứ nhất đã được bạn đọc nhiệt tình đón nhận. Đây là chương trình học có tính thực tế cao. Trong bối cảnh công nghệ phát triển liên tục nên giáo trình cần được cập nhật để bám sát thực tiễn. Đó chính là lý do chúng tôi giới thiệuđến bạn cuốn giáo trình mới trong lần xuất bản này.

Giáo trình này tương ứg với kỳ học thứ hai trong chương trình đào tạo CCNA của Cisco. Sách gồm có 11 chương, các chủ đề được trình bày có hệ thống và cô đọng. Nội dung chính của tập hai là khảo sát thành phần cấu trúc và hoạt động của router, đồng thời hướng dẫn người đọc cấu hình cơ bản cho router. So với phiên bản cũ, phiên bản mới có đề cập thêm hai phần mới là: Giao thức thông điệp điều khiển Internet (ICMP) và danh sách kiểm tra truy nhập (Access Control List). Bên cạnh đó, các phần về cấu trúc router, cấu hình router và xử lý sự cố cho router cũng được bổ sung thêm nhiều chi tiết mới so với phiên bản cũ.

Cuốn sách không chỉ là một giáo trình hữu ích cho các học viên mạng CCNA mà còn là tài liệu bổ ích cho các bạn đọc muốn trở thành những nhà networking chuyên nghiệp.

Mặc dù đã cố gắng sửa chữa, bổ sung cho cuốn sách được hoàn thiện hơn song chắc rằng không tránh khỏi những thiếu sót, hạn chế. Nhóm biên soạn mong nhận được cá ý kiến đóng góp quý báu của bạn đọc.

LỜI NGỎ

Kính thưa quý bạn đọc gần xa, Ban xuất bản MK.PUB trước hết xin bày tỏ lòng biết ơn và niềm vinh hạnh trước nhiệt tình của đông đảo Bạn đọc đối với tủ sách MK.PUB trong thời gian qua.

Khẩu hiệu chúng tôi là:

* Lao động khoa học nghiêm túc.

* Chất lượng và ngày càng chất lượng hơn.

* Tất cả vì Bạn đọc.

Rất nhiều Bạn đọc đã gửi *mail* cho chúng tôi đóng góp nhiều ý kiến quý báu cho tủ sách.

Ban xuất bản MK.PUB xin được kính mời quý Bạn đọc tham gia cùng nâng cao chất lượng tủ sách của chúng ta.

Trong quá trình đọc, xin các Bạn ghi chú lại các sai sót (dù nhỏ, lớn) của cuốn sách hoặc các nhận xét của riêng Bạn. Sau đó xin gửi về địa chỉ:

E-mail: mk.book@minhkhai.com.vn – mk.pub@minhkhai.com.vn

Hoặc gửi về: Nhà sách Minh Khai

249 Nguyễn Thị Minh Khai, Q.I, Tp. Hồ Chí Minh

Nếu Bạn ghi chú trực tiếp lên cuốn sách, rồi gửi cuốn sách đó cho chúng tôi thì chúng tôi sẽ xin hoàn lại cước phí bưu điện và gửi lại cho bạn cuốn sách khác.

Chúng tôi xin gửi tặng một cuốn sách của ủ sách MK.PUB ty chọn lựa của Bạn theo một danh mục thích hợp sẽ được gửi tới Bạn.

Với mục đích ngày càng nâng cao chất lượng của tủ sách MK.PUB, chúng tôi rất mong nhận được sự hợp tác của quý Bạn đọc gần xa.

"*MK.PUB và Bạn đọc cùng làm !*"

MK.PUB

MỤC LỤC

CHƯƠNG 1

WAN VÀ ROUTER

GIỚI THIỆU

Mạng diện rộng (WAN) là màng truyền dữ liệu qua những vùng địa lý rất lớn. WAN có nhiều đặc điểm quan trọng khác với LAN. Trong chương này, trước tiên các bạn sẽ có một cái nhìn tổng thể về các kỹ thuật và các giao thức của mạng WAN. Đồng thời trong chương này cũng sẽ giải thích những đặc điểm giống nhau và khác nhau giữa LAN và WAN.

Bên cạnh đó, kiến thức về các thành phần vật lý của router cũng rất quan trọng. Kiến thức này sẽ là nền tảng cho các kỹ năng và kiến thức khác khi bạn cấu hình router và quản trị mạng định tuyến. Trong chương này, các bạn sẽ được khảo sát thành phần vật lý bên trong và bên ngoài của router và các kỹ thiật kết nối với nhiều cổng khác nhau trên router.

Sau khi hoàn tất chương này, các bạn có thể thực hiện các việc sau:

- Xác định tổ chức quốc tế chịu trách nhiệm về các chuẩn của WAN.
- Giải thích sự khác nhau giữa LAN và WAN, giữa các loại địa chỉ mà mỗi mạng sử dụng.
- Mô tả vai trò của router trong WAN.
- Xác định các thành phần vật lý bên trong của router và các chức năng tương ứng.
- Mô tả các đặc điểm vật lý của router.
- Xác định các loại cổng trên router.
- Thực hiện các kết nối đến cổng Ethernet, cổng nối tiếp WAN và cổng console trên router.

1.1. WAN

1.1.1 Giới thiệu về WAN

WAN là mạngtruyền dữ liệu qua những vùng địa lý rất rộng lớn như các bang, tỉnh, quốc gia… Các phương tiện truyền dữ liệu trên WAN được cung cấp bởi các nhà cung cấp dịch vụ, ví dụ như các công ty điện thoại.

Mạng WAN có một số đặc điểm sau:

WAN dùng để kết nối các thiệt bị ở cách xa nhau bởi những địa lý lớn.

WAN sử dụng dịch vụ của các công ty cung cấp dịch vụ, ví dụ như: Regional Bell Operating Conpanies (RBOCs), Sprint, MCI, VPM internet servies, Inc., Altantes.net…

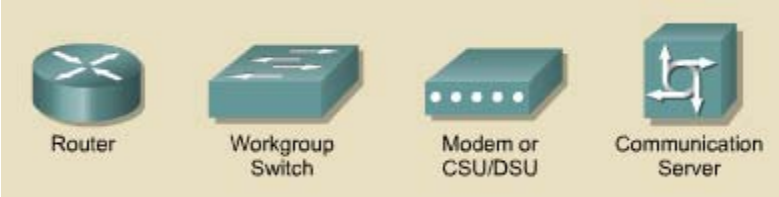
WAN sử dụng nhiều loại liên kết nối tiếp khác nhau.

WAN có một số điểm khác với LAN. Ví dụ như: LAN được sử dụng để kết nối các máy tính đơn lẻ, các thiết bị ngoại vi, các thiết bị đầu cuối và nhiều loại thiết bị khác trong cung một toà nhà hay một phạm vi địa lý nhỏ. Trong khi đó WAN được sử dụng để kết nối các chi nhánh của mình, nhờ đó mà thông tin được trao đổi dễ dàng giữa các trung tâm.

Mạng WAN hoạt động chủ yếu ở lớp Vật lý và lớp Liên kết dữ liệu mô hình OSI. WAN kết nối các mạng LAN lại với nhau. Do đó, WAN thực hiện chuyển đổi các gói dữ liệu giữa các router, switch và các mạng LAN mà nó kết nối.

Sau đây là các thiết bị được sử dụng trong WAN:

- Router: cung cấp nhiều dịch vụ khác nhau, bao gồm Internet và các giao tiếp WAN.
- Loại switch được sử dụng trong WAN cung cấp kết nối cho hoạt động thông tin liên lạc băng thoại video và dữ liệu.
- Modem: bao gồm: giao tiếp với dịch vụ truyền thoại; CSU/DSU (Chanel service units/ Digital service units) để giao tiếp với dịch vụ T1/E1; TA/NT1 (Terminal Adapters /Network Terminal 1) để giao tiếp với dịch vụ ISDN (Integrate Services Digital Network).
- Server thông tin liên lạc: tập trung xử lý cuộc gọi của người dùng.



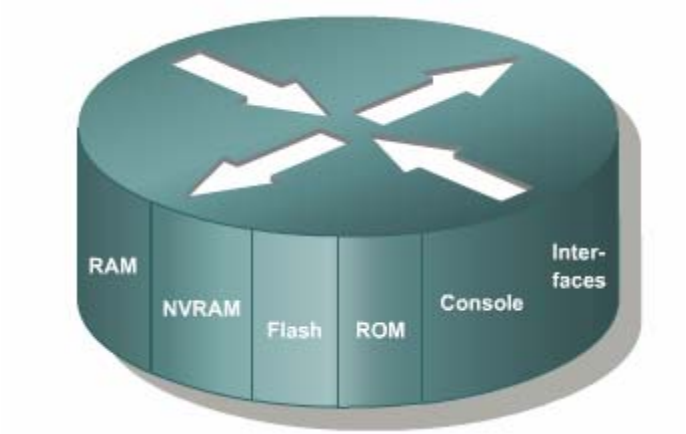
Hình 1.1.1: Các thiết bị WAN

Các giao thức ở lớp Liên kết dữ liệu của mạng WAN mô tả về cách thức mà gói dữ liệu được vận chuyển giữa các hệ thống trên một đường truyền dữ liệu. các giao thức này đươc thiết kế cho các dịch vụ chuyển mạch điểm-đến-điểm, đa điểm, đa truy nhập, ví dụ như: FrameRelay.

Các tiêu chuẩn của mạng WAN được định nghĩa và quản lý bởi các tổ chức quốc tế sau:

- Liên hiệp viễn thông quốc tế - lĩnh vực tiêu chuẩn viễn thông – ITUT (International Telecommunication Union-Telecommunication Standardization Sector), trước đây là Uỷ ban cố điện thoại và điện tín quốc tế - CCITT (Consultative Committee for International Telegraph and Telephone).
- Tổ chức quốc tế về tiêu chuẩn – ISO (International Organization for Standardization).
- Tổ chức đặc trách về kỹ thuật Internet – IETF (Internet Engineering Task Force).
- Liên hiệp công nghiệp điện tử - EIA (Eletronic Industries Association).

1.1.2 Giới thiệu về router trong mạng WAN



Hình 1.1.2

Router là một loại máy tính đặc biệt. Nó cũng có các thành phần cơ bản giống như máy tính: CPU, bộ nhớ, system bus và các cổng giao tiếp. Tuy nhiên router được kết là để thực hiện một số chức năng đặc biệt. Ví dụ: router được thiết kế là để thực hiện một số chức năng đặc biệt. Ví dụ: router kết nối hai hệ thống mạng với nhau và cho phép hai hệ thống này có thể liên lạc với nhau, ngoài ra router còn thực hiện việc chọn lựa đường đi tốt nhất cho dữ liệu.

Cũng giống như máy tính cần phải có hệ điều hành để chạy các trình ứng dụng thì router cũng cần phải có hệ điều hành để chạy các tập tin cấu hình. Tập tin cấu hình chứa các câu lệnh và các thông số để điều khiển luồng dữ liệu ra vào trên router. Đặc biệt là router còn sử dụng giao thức định tuyến để truyền để quyết định chọn đường đi tốt nhất cho các gói dữ liệu. Do đó, tập tin cấu hình cũng chứa các thông tin để cài đặt và chạy các giao thức định tuyến trên router.

Giáo trình này sẽ giải thích rõ cách xây dựng tập tin cấu hình từ các câu lệnh IOS để router có thể thực hiện được các chức năng cơ bản. Lúc ban đầu có thể bạn thấy tập tin cấu hình rất phức tạp nhưng đến cuối giáo trình này bạn sẽ thấy nó dễ hiểu hơn nhiều.

Các thành phần chính bên trong router bao gồm: bộ nhớ RAM, NVRAM, bộ nhớ flash, ROM và các cổng giao tiếp.

RAM, hay còn gọi là RAM động (DRAM- Dynamic RAM) có các đặc điểm và chức năng như sau

- Lưu bảng định tuyến.

- Lưu bảng ARP.
- Có vùng bộ nhớ chuyển mạch nhanh.
- Cung cấp vùng nhớ đệm cho các gói dữ liệu
- Duy trì hàng đợi cho các gói dữ liệu.
- Cung cấp bộ nhớ tạm thời cho tập tin cấu hình của router khi router đang hoạt động.
- Thông tin trên RAM sẽ bị xoá mất khi router khởi động lại hoặc bị tắt điện.

Đặc điểm và chức năng của NVRAM:

- Lưu giữ tập tin cấu hình khởi động của router.
- Nội dung của NVRAM vẫn được lưu giữ khi router khởi động lại hoặc bị tắt điện.

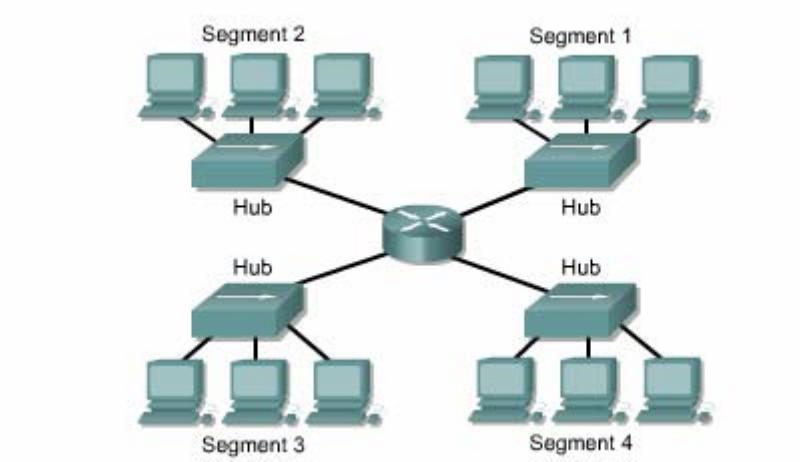
Đặc điểm và chức năng của bộ nhớ flash:

- Lưu hệ điều hành IOS.
- Có thể cập nhật phần mềm lưu trong Flash mà không cần thay đổi chip trên bộ xử lý.
- Nội dung của Flash vẫn được lưu giữ khi router khởi động lại hoặc bị tắt điện.
- Ta có thể lưu nhiều phiên bản khác nhau của phần mềm IOS trong Flash.
- Flash là loại ROM xoá và lập trình được (EPROM).

Đặc điểm và chức năng của các cổng giao tiếp:

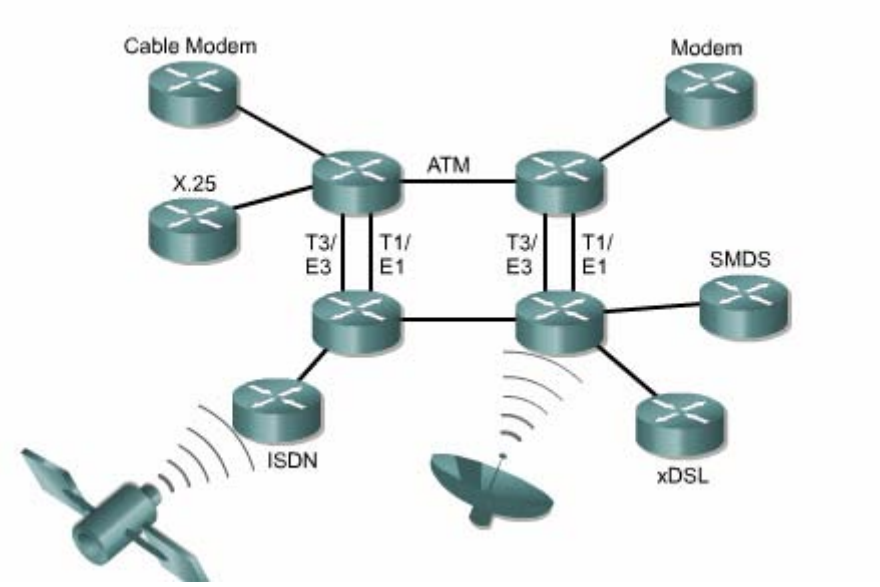
- Kết nối router vào hệ thống mạng để nhận và chuyển gói dữ liệu.
- Các cổng có thể gắn trực tiếp trên mainboard hoặc là dưới dạng card rời.

1.1.3 Router LAN và WAN



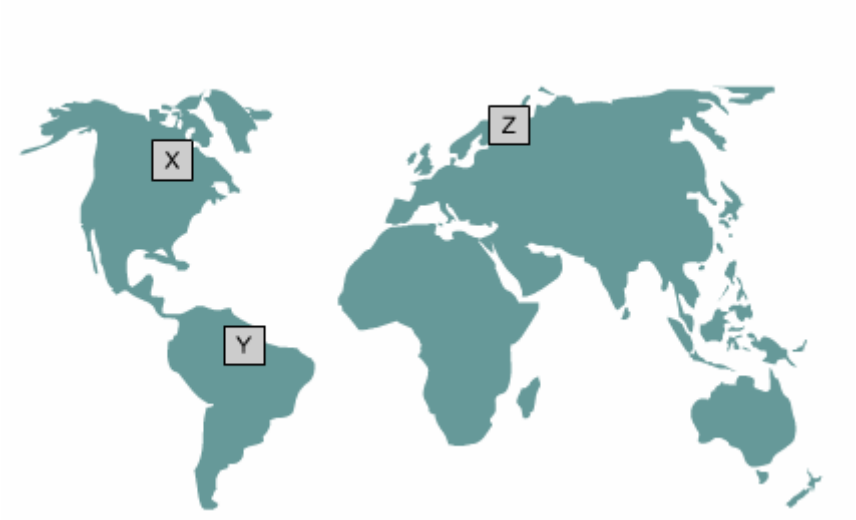
Hình 1.1.3a: Phân đoạn mạng LAN với router

Router vừa được sử dụng để phân đoạn mạng LAN vừa là thiết bị chính trong mạng WAN. Do đó, tên router có cả cổng giao tiếp LAN và WAN. Thực chất là các kỹ thuật WAN được sử dụng để kết nối các router, router này giao tiếp với router khác qua đường liên kết WAN. Router là thiết bị xương sống của mạng Intranet lớn và mạng Internet. Router hoạt động ở Lớp 3 và thực hiện chuyển gói dữ liệu dựa trên địa chỉ mạng. Router có hai chức năng chính là: chọn đường đi tốt nhất và chuyển mạch gói dữ liệu. Để thực hiện chức năng này, mỗi router phải xây dựng một bảng định tuyến và thực hiện trao đổi thông tin định tuyến với nhau.



Hình 1.1.3b: Kết nối router bằng các công nghệ WAN

Người quản trị mạng có thể duy trì bảng định tuyến bằng cách cấu hình định tuyến tĩnh, nhưng thông thường thi bảng định tuyến được lưu giữ động nhờ các giao thức định tuyến thực hiện trao đổi thông tin mạng giữa các router.



Hình 1.1.3c

Ví dụ: nếu máy tính X muốn thông tin liên lạc với máy tính Y ở một châu lục khác và với máy tính Z ở một vị trí khác nữa trên thế giới, khi đó cần phải có định tuyến để có thể truyền dữ liệu và đồng thời cũng cần phải có các đường dự phòng, thay thế để đảm bảo độ tin cậy. Rất nhiều thiết kế mạng và công nghệ được đưa ra để cho các máy tính như X Y, Z có thể liên lạc với nhau.

Một hệ thống mạng được cấu hình đúng phải có đầy đủ các đặc điểm sau:

- Có hệ thống địa chỉ nhất quán từ đầu cuối đến đầu cuối
- Cấu trúc địa chỉ phải thể hiện được cấu trúc mạng.
- Chọn được đường đi tốt nhất.
- Định tuyến động và tĩnh.
- Thực hiện chuyển mạch.

1.1.4Vai trò của router trong mạng WAN

Mạng WAN hoạt động chủ yếu ở lớp vật lý và lớp liên kết dữ liệu. Điều này không có nghĩa là năm lớp còn lại của mô hình OSI không có trong mạng WAN. Điều

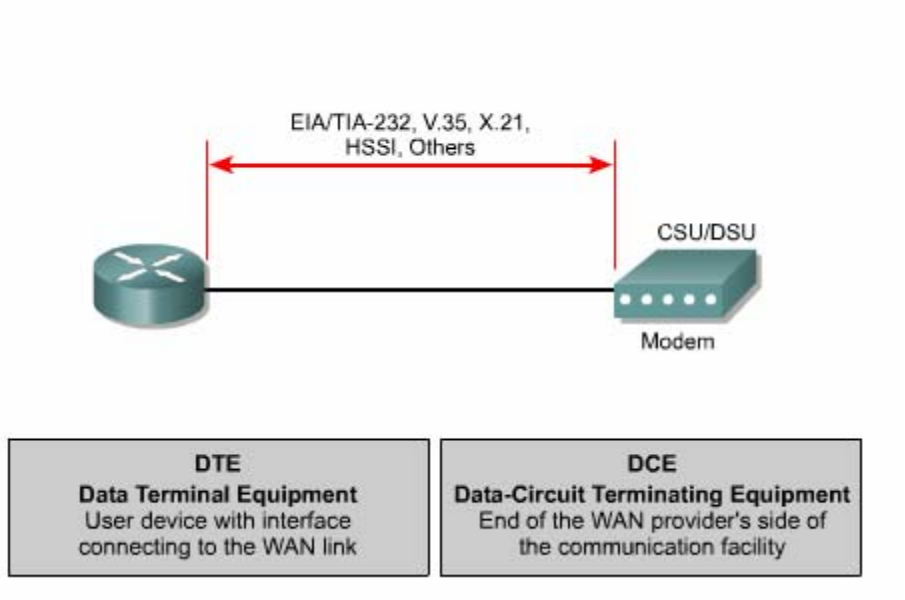
này đơn giản có nghĩa là mang WAN chỉ khác với mạng LAN ở lớp Vật lý và lớp Liên kết dữ liệu. Hay nói cách khác là các tiêu chuẩn và giao thức sử dụng trong mạng WAN ở lớp 1 và lớp 2 là khác với mạng LAN.

Lớp Vật lý trong mạng WAN mô tả các giao tiếp thiết bị dữ liệu đầu cuối DTE (Data Terminal Equipment) và thiết bị đầu cuối mạch dữ liệu DCE (Data Circuit-terminal Equipment). Thông thường, DCE là thiết bị ở phía nhà cung cấp dịch vụ và DTE là thiết bị kết nối vào DCE. Theo mô hình này thì DCE có thể là modem hoặc CSU/DSU.

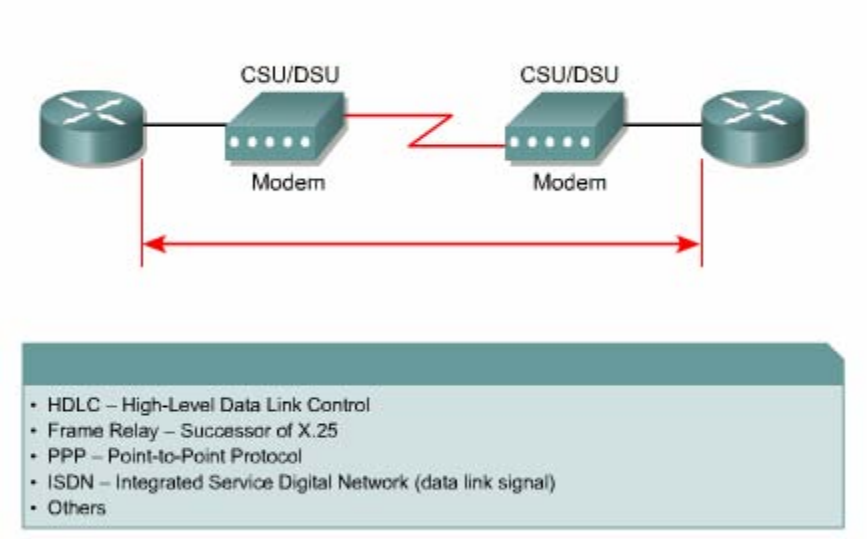
Chức năng chủ yếu của router là định tuyến. Hoạt động định tuyến diễn ra ở lớp 3 - lớp Mạng trong khi WAN hoạt động ở lớp 1 và 2. Vậy router là thiết bị LAN hay WAN? Câu trả lời là cả hai. Router có thể là thiết bị LAN, hoặc WAN, hoặc thiết bị trung gian giữa LAN và WAN hoặc có thể là LAN và WAN cùng một lúc.

Một trong những nhiệm vụ của router trong mạng WAN là định tuyến gói dữ liệu ở lớp 3, đây cúng là nhiệm vụ của router trong mạng LAN. Tuy nhiên, định tuyến không phải là nhiệm vụ chính yếu của router trong mạng WAN. Khi router sử dụng các chuẩn và giao thức của lớp Vật lý và lớp Liên kết dữ liệu để kết nối các mạng WAN thì lúc này nhiệm vụ chính yếu của router trong mạng WAN không phải là định tuyến nữa mà là cung cấp kết nối giữa các mạng WAN với các chuẩn vật lý và liên kết dữ liệu khác nhau. Ví dụ: một router có thể có một giao tiếp ISDN sử dụng kiểu đóng gói PPP và một giao tiếp nối tiếp T1 sử dụng kiểu đóng gói FrameRelay. Router phải có khả năng chuyển đổi luồng bit từ loại dịch vụ này sang dịch vụ khác. Ví dụ: chuyển đổi từ dịch vụ ISDN sang T1, đồng thời chuyển kiểu đóng gói lớp Liên kết dữ liệu từ PPP sang FrameRelay.

Chi tiết về các giao thức lớp 1 và 2 trong mạng WAN sẽ được đề cập ở tập sau của giáo trình này. Sau đây chỉ liệt kê một số chuẩn và giao thức WAN chủ yếu để các bạn tham khảo:



Hình 1.1.4a: Các chuẩn WAN ở lớp Vật lý



Hình 1.1.4b: Các kiểu đóng gói dữ liệu WAN ở Lớp liên kết dữ liệu

Các chuẩn và giao thức WAN lớp vật lý: EIA/TIA-232,449, V24, V35, X21, EIA-530, ISDN, T1, T3, E1, E3, Xdsl, sonet (oc-3, oc-12, oc-48, oc-192).

Các chuẩn và giao thức WAN lớp liên kết dữ liệu: HDLC, FrameRelay, PPP, SDLC, SLIP, X25, ATM, LAMB, LAPD, LAPF.

1.1.5Các bài thực hành mô phỏng

Trong các bài thực hành mô phỏng trong phòng lab, các mạng được kết nối bằng cáp serial trong thực tế không kết nối trực tiếp như vậy được. Ví dụ: trên thực tế, một router ở New York và một router ở Sydney, Australia. Người quản trị mạng ở Australia phải kết nối vào router ở New York thông qua đám mây WAN để xử lý sự cố trên router ở New York.

Trong các bài thực hành mô phỏng, các thiết bị trong dám mây WAN được giả lập bằng cáp DTE-DCE kết nối trực tiếp từ cổng S0/0 của router này đến cổng S0/1 của router kia (nối back-to-back).

1.2 Router

1.2.1 Các thành phần bên trong router

Cấu trúc chính xác của router rất khác nhau tuỳ theo từng phiên bản router. Trong phần này chỉ giới thiệu về các thành phần cơ bản của router.

CPU – Đơn vị xử lý trung tâm: thực thi các câu lệnh của hệ điều hành để thực hiện các nhiệm vụ sau: khởi động hệ thống, định tuyến, điều khiển các cổng giao tiếp mạng. CPU là một bộ giao tiếp mạng. CPU là một bộ vi xử lý. Trong các router lớn có thể có nhiều CPU.

RAM: Được sử dụng để lưu bảng định tuyến, cung cấp bộ nhớ cho chuyển mạch nhanh, chạy tập tin cấu hình và cung cấp hàng đợi cho các gói dữ liệu. Trong đa số router, hệ điều hành Cisco IOS chạy trên RAM. RAM thường được chia thành hai phần: phần bộ nhớ xử lý chính và phần bộ nhớ chia sẻ xuất/nhập. Phần bộ nhớ chia sẻ xuất/nhập được chia cho các cổng giao tiếp làm nơi lưu trữ tạm các gói dữ liệu.Toàn bộ nội dung trên RAM sẽ bị xoá khi tắt điện. Thông thường, RAM trên router là loại RAM động (DRAM – Dynamic RAM) và có thể nâng thêm RAM bằng cách gắn thêm DIMM (Dual In-Line Memory Module).

Flash: Bộ nhớ Flash được sử dụng để lưu toàn bộ phần mềm hệ điều hành Cisco IOS. Mặc định là router tìm IOS của nó trong flash. Bạn có thể nâng cấp hệ điều hành bằng cách chép phiên bản mới hơn vào flash. Phần mềm IOS có thể ở dưới dạng nén hoặc không nén. Đối với hầu hết các router, IOS được chép lên RAM trong quá trình khởi động router. Còn có một số router thì IOS có thể chạy trực tiếp

trên flash mà không cần chép lên RAM. Bạn có thể gắn thêm hoặc thay thế các thanh SIMM hay card PCMCIA để nâng dung lượng flash.

NVRAM (Non-volative Random-access Memory): Là bộ nhớ RAM không bị mất thông tin, được sử dụng để lưu tập tin cấu hình. Trong một số thiết bị có NVRAM và flash riêng, NVRAM được thực thi nhờ flash. Trong một số thiết bị, flash và NVRAM là cùng một bộ nhớ. Trong cả hai trường hợp, nội dung của NVRAM vẫn được lưu giữ khi tắt điện.

Bus: Phần lớn các router đều có bus hệ thống và CPU bus. Bus hệ thống được sử dụng để thông tin liên lạc giữa CPU với các cổng giao tiếp và các khe mở rộng. Loại bus này vận chuyển dữ liệu và các câu lệnh đi và đến các địa chỉ của ô nhớ tương ứng.

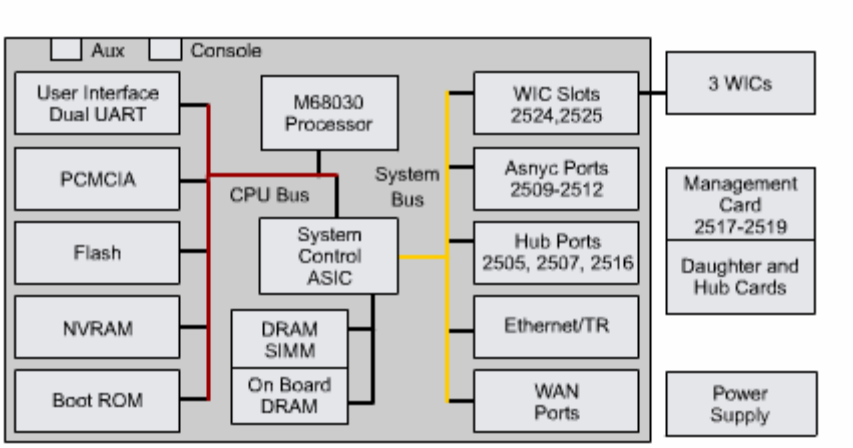
ROM (Read Only Memory): Là nơi lưu đoạn mã của chương trình kiểm tra khi khởi động. Nhiệm vụ chính của ROM là kiểm tra phần cứng của router khi khởi động, sau đó chép phần mềm Cisco IOS từ flash vào RAM. Một số router có thể có phiên bản IOS cũ dùng làm nguồn khởi động dự phòng. Nội dung trong ROM không thể xoá được. Ta chỉ có thể nâng cấp ROM bằng cách thay chip ROM mới.

Các cổng giao tiếp: Là nơi router kết nối với bên ngoài. Router có 3 loại cổng: LAN, WAN và console/AUX. Cổng giao tiếp LAN có thể gắn cố định trên router hoặc dưới dạng card rời.

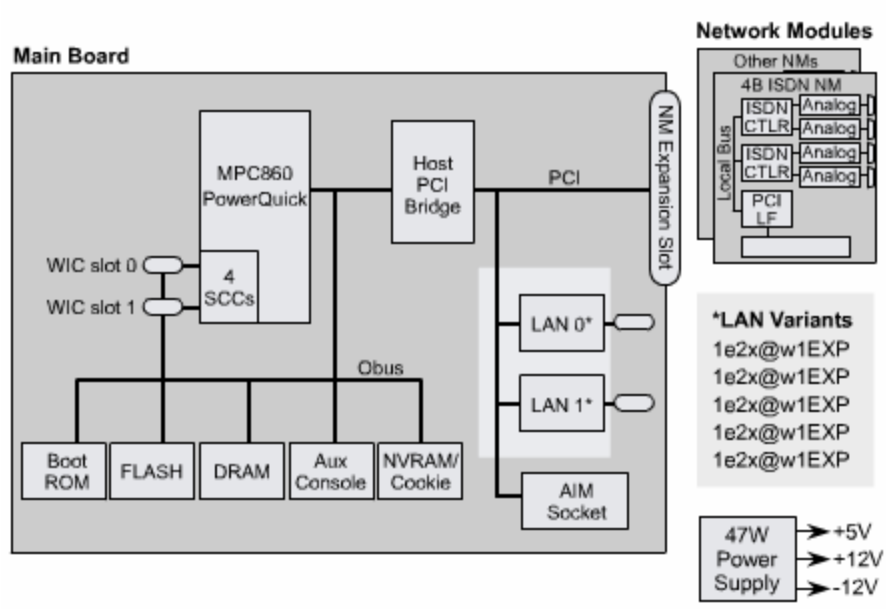
Cổng giao tiếp WAN có thể là cổng Serial, ISDN, cổng tích hợp đơn vị dịch vụ kênh CSU (Chanel Service Unit). Tương tự như cổng giao tiếp LAN, các cổng giao tiếp WAN cũng có chip điều khiển đặc biệt. Cổng giao tiếp WAN có thể định trên router hoặc ở dạng card rời.

Cổng console/AUX là cổng nối tiếp, chủ yếu được dử dụng để cấu hình router. Hai cổng này không phải là loại cổng để kết nối mạng mà là để kết nối vào máy tính thông qua modem hoặc thông qua cổng COM trên máy tính để từ máy tính thực hiện cấu hình router.

Nguồn điện: Cung cấp điện cho các thành phần của router, một số router lớn có thể sử dụng nhiều bộ nguồn hoặc nhiều card nguồn. Còn ở một số router nhỏ, nguồn điện có thể là bộ phận nằm ngoài router.



Hình 1.2.1a

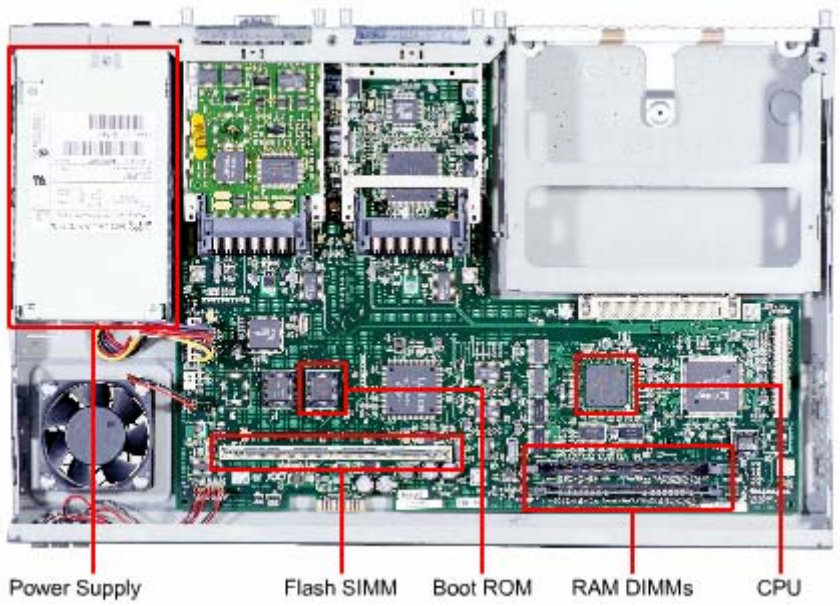


Hình 1.2.1b

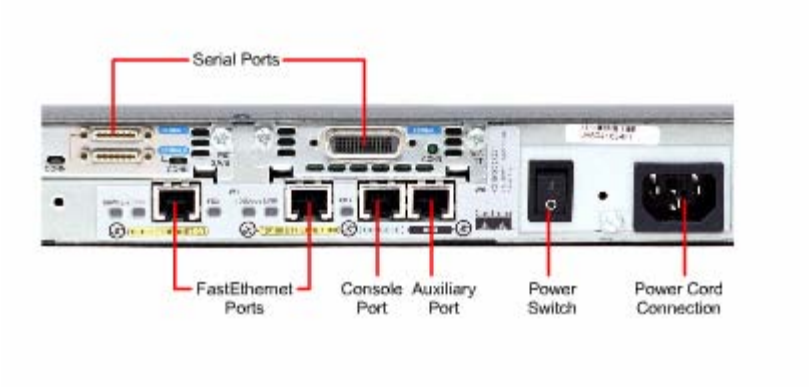
1.2.2 Đặc điểm vật lý của router

Không nhất thiết là bạn phải biết vị trí của các thành phần vật lý trong router mới có thể sử dụng được router. Tuy nhiên trong một số trường hợp, ví dụ như nâng cấp bộ nhớ chẳng hạn, những kiến thức này lại rất hữu dụng.

Các loại thành phần và vị trí của chúng trong router rất khác nhau tuỳ theo từng loại phiên bản thiết bị.



Hình 1.2.2a: Cấu trúc bên trong của router 2600



Hình 1.2.2b: Các loại kết nối bên ngoài của router 2600

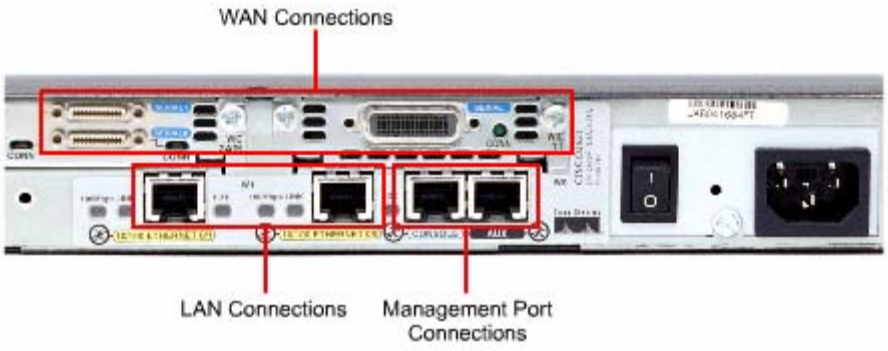
1.2.3 Các loại kết nối ngoài của router

Router có ba loại kết nối cơ bản là: cổng LAN, WAN và cổng quản lý router. Cổng giao tiếp LAN cho phép router kết nối vào môi trường mạng cục bộ LAN. Thông thường, cổng giao tiếp LAN là cổng Ethernet. Ngoài ra cũng có cổng Token Ring và ATM (Asynchronous Tranfer Mode).

Kết nối mạng WAN cung cấp kết nối thông qua các nhà cung cấp dịch vụ đến các chi nhánh ở xa hoặc kết nối vào Internet. Loại kết nối này có thể là nối tiếp hay bất kỳ loại giao tiếp WAN, bạn cần phải có thêm một thiết bị ngoại vi như CSU chẳng

hạn để nối router đến nhà cung câp dịch vụ. Đối với một số loại giao tiếp WAN khác thì bạn có thể kết nối trực tiếp router của mình đến nhà cung cấp dịch vụ.

Chức năng của port quản lý hoàn toàn khác với ai loại trên. kết nối LAN, WAN để kết nối router và mạng để router nhận và phát các gói dữ liệu. Trong khi đó, port quản lý cung cấp cho bạn một kết nối dạng văn bản để bạn có thể cấu hình hoặc xử lý trên router. Cổng quản lý thường là cổng console hoặc cổng AUX (Auxilliary). Đây là loại cổng nối tiếp bất đồng bộ EIA-232. Các cổng này kết nối vào cổng COM trên máy tính. Trên máy tính, chúng ta sử dụng chương trình mô phỏng thiết bị đầu cuối để thiết lập phiên kết nối dạng văn bản vào router. Thông qua kiểu kết nối này, người quản trị mạng có thể quản lý thiết bị của mình.



Hình 1.2.3

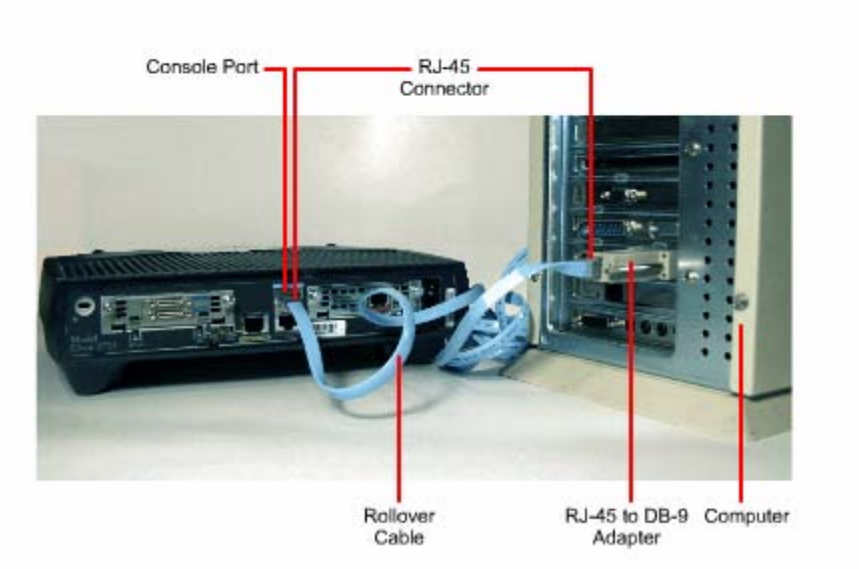
1.2.4 Kết nối vào cổng quản lý trên router

Cổng console và cổng AUX là cổng quản lý trên router. Loại cổng nối tiếp bất đồng bộ này được thiết kế không phải để kết nối mạng mà là để cấu hình router. Ta thường sử dụng cổng console để thiết lập cấu hình cho router vì không phải router nào cũng có cổng AUX.

Khi router hoạt động lần đầu tiên thì chưa có thông số mạng nào được cấu hình cả. Do đó router chưa thể giao tiếp với bất kỳ mạng nào. Để chuẩn bị khởi động và cấu hình router, ta dùng thiết bị đầu cuối ASCII kết nối vào cổng console trên router. Sau đó ta có thể dùng lệnh để cấu hình, cài đặt cho router.

Khi bạn nhập cấu hình cho router thông qua cổng console hay cổng AUX, router có thể kết nối mạng để xử lý sự cố hoặc theo dõi hoạt động mạng.

bạn có thể cấu hình router từ xa bằng cách quay số qua modem kết nối vào cổng console hay cổng AUX trên router.



Hình 1.2.4: Kết nối modem vào cổng console hay cổng AUX

Khi xử lý sự cố, bạn nên sử dụng cổng console thay vì cổng AUX. Vì mặc định là cổng console có thể hiển thị quá trình khởi động router, thông tinhoạt động và các thông điệp báo lỗi của router. Cổng console được sử dụng khi có một dịch vụ mạng không khởi động được hoặc bị lỗi, khi khôi phục lại mật mã hoặc khi router bị sự cố nghiêm trọng.

1.2.5 Thiết lập kết nối và cổng console

Cổng console là loại cổng quản lý, cung cấp đường kết nối riêng vào router. Cổng này được sử dụng để thiết lập cấu hình cho router, theo dõi hoạt động mạng và khôi phục router khi gặp sự cố nghiêm trọng.

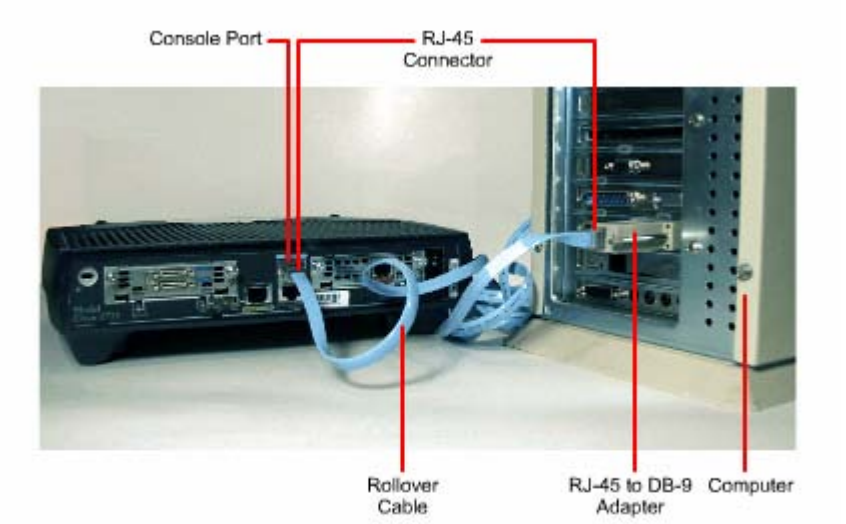
Để kết nối PC vào cổng console bạn cần có cáp rollover và bộ chuyển đổi RJ45-DB9. Cisco có cung cấp bộ chuyển đổi này để nối PC vào cổng console.

PC hay thiết bị đầu cuối phải có chương trình mô phỏng thiết bị đầu cuối VT100. Thông thường phần mềm này là HyperTerminal.

Sau đây là các bước thực hiện kết nối PC vào cổng console:

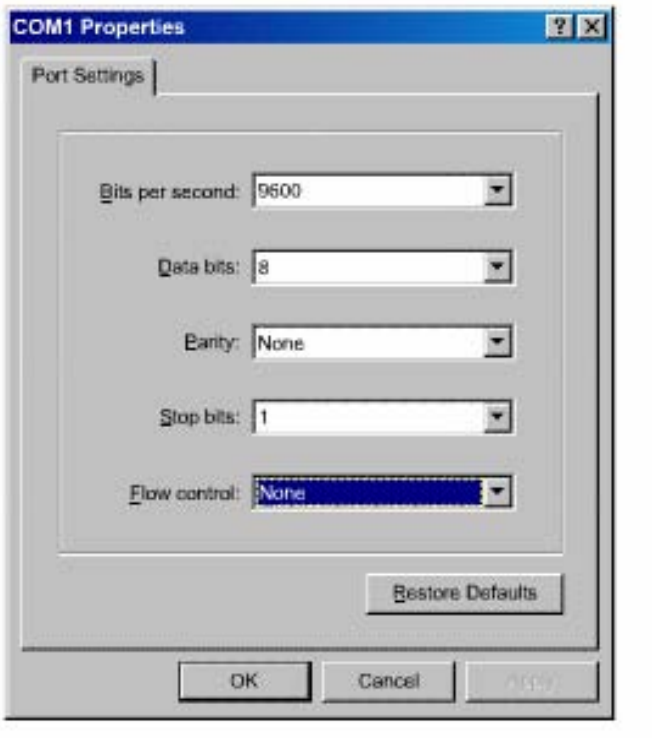
1. Cấu hình phần mềm giả lập thiết bị đầu cuối như sau:

- Chọn đúng cổng COM.
- Tốc độ band là 9600.
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None



Hình1.2.5a: Kết nối PC vào cổng console trên router

2. Cắm một đầu RJ45 của cáp rollover vào cổng console trên router.
3. Cắm đầu cáp còn lại vào bộ chuyển đổi RJ45-DB9.
4. Gắn đầu DB9 của bộ chuyển đổi vào cổng COM trên PC.



HÌnh 1.2.5b: Cấu hình hyper terminal để kết nối vào console

1.2.6 Thực hiện kết nối với cổng LAN

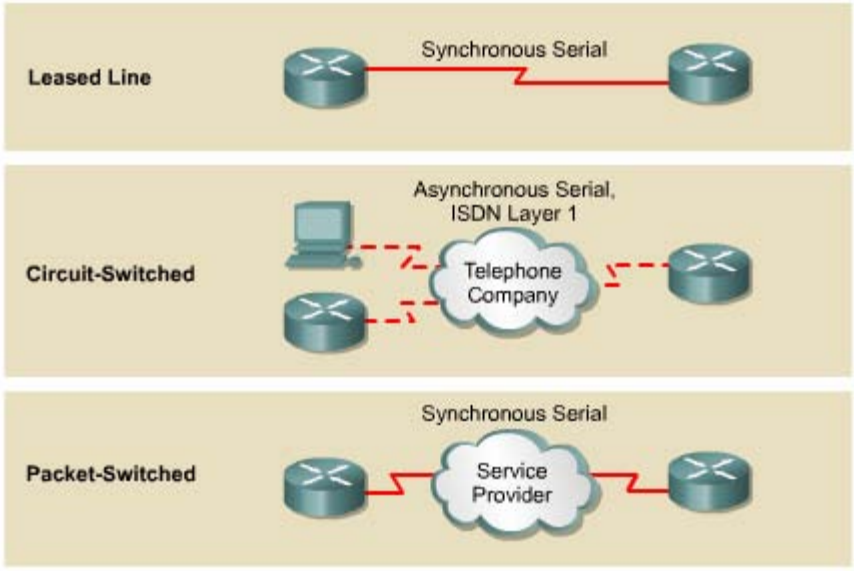
Trong hầu hết các môi trường mạng LAN hiện nay, router được kết nối vào LAN bằng cổng Ethernet hoặc Fast Ethernet. Router giao tiếp với mạng LAN thông qua hub hoặc switch. Chúng ta sử dụng cáp thẳng để nối router và hub/switch. Đối với tất cả các loại router có cổng 10/100BaseTx chúng ta đều phải sử dụng cáp UTP CAT5 hoặc cao hơn.

Trong một số trường hợp ta có thể kết nối trực tiếp cổng Ethernet trên router vào máy tính hoặc vào router khác bằng cáp chéo.

Khi thực hiện kết nối, chúng ta phải lưu ý cắp đúng cổng vì nếu cắm sai có thể gây hư hỏng cho router và thiết bị khác. Trên router có rất nhiều loại cổng khác nhau nhưng hình dạng cổng lai giống nhau. Ví dụ như: cổng Ethernet, ISDN BRI, console, AUX, cổng tích hợp CSU/DSU, cổng Token Ring đều sử dụng cổng 8 chân là RJ45, RJ48 hoặc RJ49.

1.2.7 Thực hiện kết nối với cổng WAN

Kết nối WAN có nhiều dạng khác nhau. Một kết nối WAN sử dụng nhiều ký thuật khác nhau để thực hiện truyền dữ liệu qua một vùng địa lý rộng lớn. Các dịch vụ WAN thường được thuê từ nhà cung cấp dịch vụ. Chúng ta có 3 loại kết nối WAN như sau: kết nối thuê kênh riêng, kết nối chuyển mạch - mạch, kết nối chuyển mạch gói.



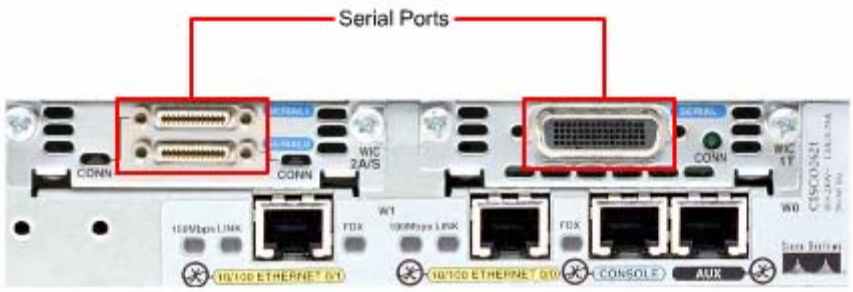
Hình 1.2.7a

Đối với từng loại dịch vụ WAN, thiết bị thuộc sở hữu của khách hàng (CPE – Customer Premises Equipment), thông thường là router, được gọi là thiết bị dữ liệu đầu cuối DTE (Data Terminal Equipment). Thiết bị DTE này được kết nối vào nhà cung cấp dịch vụ thông qua thiết bị kết cuối mạch dữ liệu DCE (Data Circuit-terminating Equipment), thông thường là modem hay CSU/DSU. Thiết bị DCE này được sử dụng để chuyển đổi dữ liệu từ DTE sang dạng phù hợp với dịch vụ của nhà cung cấp dịch vụ.

Hầu hết các cổng WAN trên router đều là cổng Serial. Công việc chọn lựa cho đúng loại cáp sẽ rất dễ dàng khi bạn trả lời được 4 câu hỏi sau:

- Loại kết nối trên thiết bị Cisco là loại nào? Cisco router sử dụng nhiều loài đầu nối khác nhau cho cổng Serial. Như trong hình 1.2.7b, cổng bên trái là cổng Smart Serial, cổng bên phải là cổng DB-60. Lựa chon

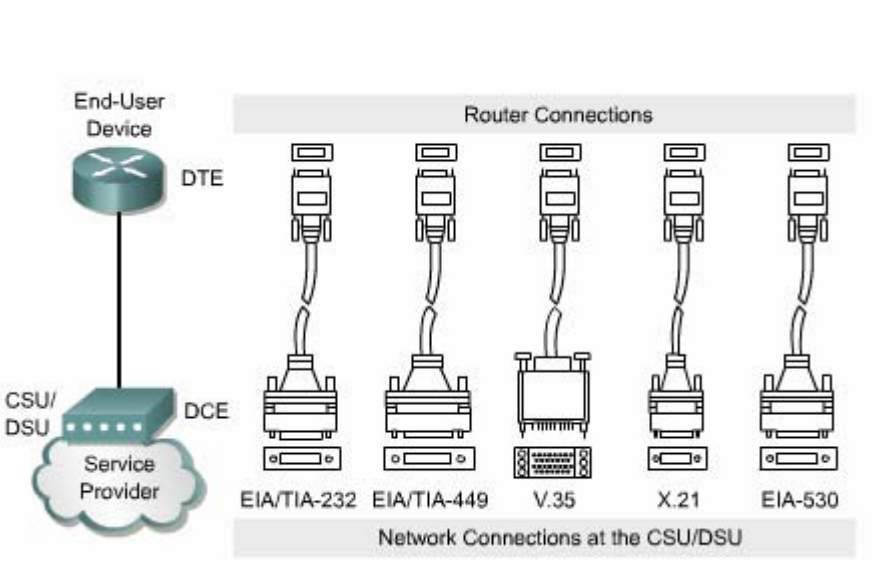
cáp Serial để kết nối hệ thống mạng là một phần then chốt trong qua trình thiết lập WAN.



Hình 1.2.7b

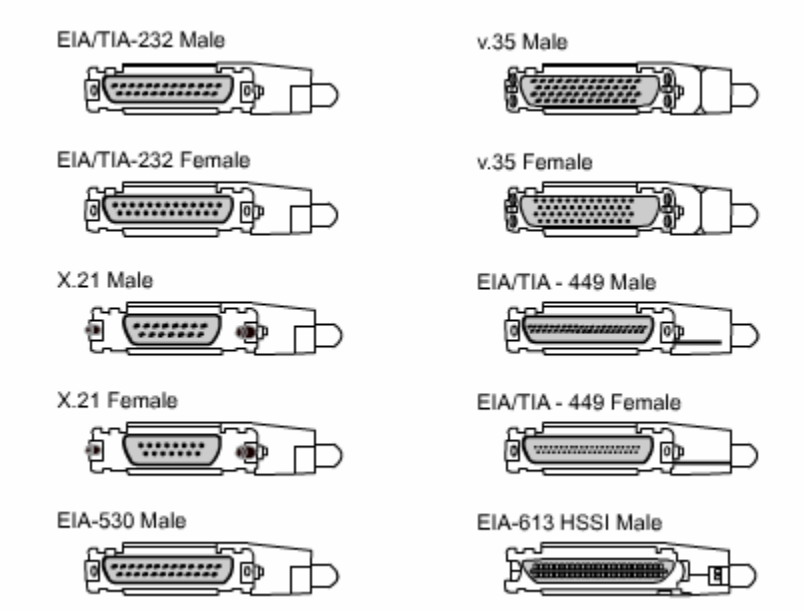
- Hệ thống mạng được kết nối và thiết bị DTE hay DCE? DTE và DCE là hai loại cổng serial khác nhau. Điểm khác nhau quan trọng giữa hai loại này là: thiết bị DCE cấp tín hiệu xung đồng hồ cho quá trình thông tin liên lạc trên bus. Bạn nên tham khảo tài liệu của thiết bị để xác định DTE và DCE.

- Thiết bị đòi hỏi chuẩn tín hiệu nào? mỗi loại thiết bị khác nhau sẽ sử dụng loại chuẩn Serial khác nhau. Mỗi chuẩn sẽ quy ước tín hiệu truyền trên cáp và loại đầu nối ở 2 đầu cáp. Bạn nên tham khảo tài liệu của thiết bị để xác định chuẩn tín hiệu của thiết bị.



Hình 1.2.7c

- Cáp có loại đầu nối đực hay cái? Nếu đầu nối có chân cắm ra ngoài thì đó là đầu đực. Nếu đầu nối chỉ có lỗ cắm cho các chân thì đó là đầu cái



Hình 1.2.7d

TỔNG KẾT

Sau đây là các điểm quan trọng bạn cần nắm được trong chương này:

- Khái niệm về WAN và LAN.
- Vai trò của router trong WANs và LANs.
- Các giao thức WAN.
- Cấu hình kiểu đóng gói cho cổng giao tiếp.
- Xác định và mô tả các thành phần bên trong router.
- Đặc điểm vật lý của router.
- Các loại cổng thường gặp trên router.
- Cách kết nối vào cổng console, cổng LAN và WAN.

CHƯƠNG 2

GIỚI THIỆU VỀ ROUTER

GIỚI THIỆU

Các kỹ thuật của Cisco đều được xây dựng dựa trên hệ điều hành mạng Cisco (ISO). Phần mềm IOS điều khiển quá trình định tuyến và chuyển mạch trên các thiết bị kết nối liên mạng. Do đó người quản trị mạng phải nắm vững về IOS. Trong chương này, chúng tôi sẽ giới thiệu cơ bản và khảo sát các đặc điểm của IOS. Tất cả các công việc cấu hình mạng từ đơn giản nhất đến phức tạp nhất đều dựa trên một nền tảng cơ bản là cấu hình router. Do đó trong chương này cũng giới thiệu về các kỹ thuật và công cụ cơ bản để cấu hình router mà chúng ta sẽ sử dụng trong suốt giáo trình này.

Sau khi hoàn tất chương này, các bạn có thể:

- Nắm được mục đích của IOS.
- Mô tả hoạt động cơ bản của IOS.
- Nắm được các đặc điểm của IOS.
- Nắm được phương thức thiết lập phiên giao tiếp bằng dòng lệnh với router.
- Chuyển đổi giữa các chế độ cấu hình router.
- Thiết lập kết nối bằng HyperTerminal vào router.
- Truy cập vào router.
- Sử dụng tính năng trợ giúp trong giao tiếp bằng dòng lệnh.
- Xử lý lỗi khi nhập câu lệnh.

2.1 Phần hệ điều hành Cisco IOS

2.1.1 Mục đích của phần mềm Cisco IOS

Tương tự như máy tính, router và switch không thể hoạt động được nếu không có hệ điều hành. Cisco gọi hệ điều hành của mình là hệ điều hành mạng Cisco hay gọi

tắt là Cisco IOS. Hệ điều hành được cài trên các Cisco router và Catalysst Switch. Cisco IOS cung cấp các dịch vụ mạng như sau:

- Định tuyến và chuyển mạch.
- Bảo đảm và bảo mật cho việc truy cập vàp tài nguyên mạng.
- Mở rộng hệ thống mạng.

2.1.2 Giao diện người dùng của router

Phần mềm Cisco sử dụng giao diện dòng lệnh (CLI – Command – line interface) cho môi trường console truyền thống. IOS là một kỹ thuật cơ bản, từ đó được phát triển cho nhiều dòng sản phẩm khác nhau của Cisco. Do đó hoạt động cụ thể của từng IOS sẽ rất khác nhau tuỳ theo từng loại thiết bị.

Chúng ta có nhiều cách khác nhau để truy cập vào giao diện CLI của router. Cách đầu tiên là kết nối trực tiếp từ máy tính hoặc thiết bị đầu cuối vào cổng console trên router. Cách thứ hai là sử dụng đường quay số qua modem hoặc kết nối null modem vào cổng AUX trên router. Cả hai cách trên đều không cần phải cấu hình trước cho router. Cách thứ ba là telnet vào router. Để thiết lập phiên telnet vào router thì trên router ít nhất phải có một cổng đã được cấu hình địa chỉ IP, các đường vty đã được cấu hình cho phép truy cập và đặt mật mã.

2.1.3 Các chế độ cấu hình router

Giao diện dòng lệnh của Cisco sử dụng cấu trúc phân cấp. Cấu trúc này đòi hỏi bạn muốn cấu hình cái gì thì phải vào chế độ tương ứng. Ví dụ: nếu bạn muốn cấu hình cổng giao tiếp nào của router thì bạn phải vào chế đọ cấu hình cổng giao tiếp đó. Từ chế độ này tất cả các cấu hình được nhập vào chỉ có hiệu lực đối với cổng giao tiếp tương ứng mà thôi. Tương ứng với mỗi chế độ cấu hình có một dấu nhắc đặc trưng riêng và một tập lệnh riêng.

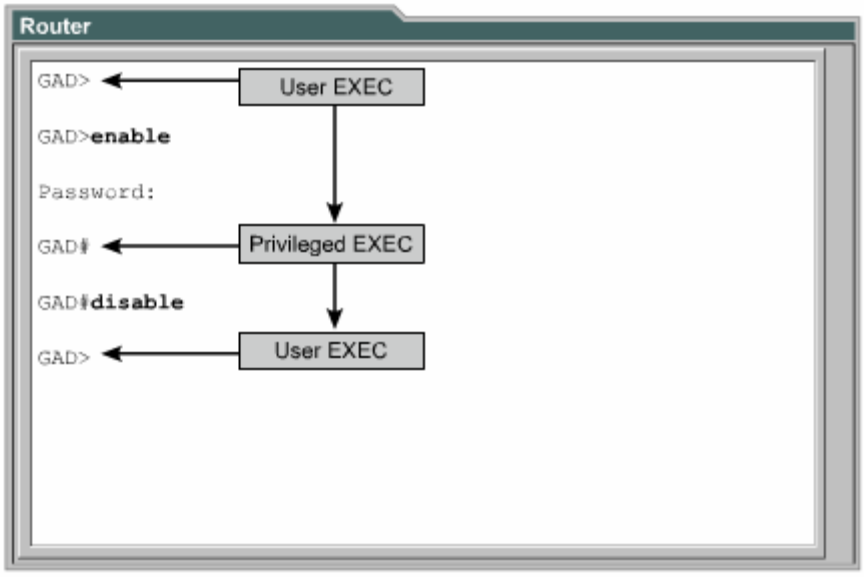
IOS có một trình thông dịch gọi là EXEC. Sau khi bạn nhập một câu lệnh thì EXEC sẽ thực thi ngay câu lệnh đó.

Vì lý do bảo mật nên Cisco IOS chia phiên bản làm việc của EXEC thành hai chế độ là: chế độ EXEC người dùng và chế độ EXEC đặc quyền. Sau đây là các đặc điểm của chế độ EXEC người dùng và chế độ EXEC đặc quyền:

- Chế độ EXEC người dùng chỉ cho phép thực thi một số câu lệnh hiển thị các thông tin cơ bản của router mà thôi. Chế độ này chỉ để xem chứ không cho phép thực hiện các câu lệnh làm thay đổi cấu hình router. Chế độ EXEC người dùng có dấu nhắc là ">".

- Chế độ EXEC đặc quyền cho phép thực hiện tất cả các câu lệnh của router. Bạn có thể cấu hình để người dùng phải nhập mật mã trước khi truy nhập vào chế độ này. Ngoài ra, để tăng thêm tính bảo mật bạn có thể cấu hình thêm userID. Điều này cho phép chỉ những người nào được phép mới có thể truy cập vào router. Người quản trị mảng phải ở chế độ EXEC đặc quyền mới có thể sử dụng các câu lệnh để cấu hình hoặc quản lý router. Từ chế độ EXEC đặc quyền bạn có thể chuyển vào các chế độ đặc khác nhau như chế độ cấu hình toàn cục chẳng hạn. Chế độ EXEC đặc quyền được xác định bởi dấu nhắc "#".

Để chuyển từ chế độ EXEC người dùng sang chế độ EXEC đặc quyền hạn dùng lệnh **enable** tại dấu nhắc ">". Nếu mật mã đã được cài đặt thì router sẽ yêu cầu bạn nhập mật mã. Vì lý do bảo mật nên các thiết bị mạng Cisco không hiển thị mật mã trong lúc bạn nhập chúng. Sau khi mật mã được nhập vào chính xác thì dấu nhắc ">" chuyển thành "#" cho biết bạn đang ở chế độ EXEC đặc quyền. Bạn gõ dấu chầm hỏi (?) ở dấu nhắc này thì sẽ thấy router hiển thị ra nhiều câu lệnh hơn so với ở chế độ EXEC người dùng.



Hình 2.1.3

2.1.4 Các đặc điểm của phần mèm Cisco IOS

Cisco cung cấp rất nhiều loại IOS cho các loại sản phẩm mạng khác nhau.

Để tối ưu hoá phần mềm IOS cho nhiều loại thiết bị, Cisco đã phát triển nhiều loại phần mềm Cisco IOS. Mỗi loại phần mềm IOS phù hợp với từng loại thiết bị, với mức dung lượng bộ nhớ và với nhu cầu của khách hàng.

Mặc dù có nhiều phần mềm IOS khác nhau cho nhiều loại thiết bị với nhiều đặc tính khác nhau nhưng cấu trúc lệnh cấu hình cơ bản thì vẫn giống nhau. Do đó kỹ năng cấu hình và xử lý sự cố của bạn có thể ứng dụng cho nhiều loại sản phẩm khác nhau.

Tên của Cisco IOS được quy ước chia ra thành ba phần như sau:

- Phần thứ nhất thể hiện loại thiết bị mà phần mềm IOS này có thể sử dụng được.
- Phần thứ hai thể hiện các đặc tính của phần mềm IOS.
- Phần thứ ba thể hiện nơi chạy phần mêm IOS trên router và cho biết phần mềm này được cung cấp dưới dạng nén hay không nén.

Bạn có thể lựa chọn các đặc tính đặc biệt của IOS nhờ phần mềm Cisco Software Advisor. Cisco Software Advisor là một công cụ cung cấp các thông tin hiện tại và cho phép bạn chọn lựa các đặc tính cho phu hợp với yêu cầu của hệ thống mạng

The name has three parts, separated by dashes: e.g. xxx-yyy-ww: • xxxx = Platform • yyyy = Feature • ww = Format – where It execute 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
C4000	4000 (11.2 and later only)
C4500	4500, 4700
Feature (Partial list)	
B	Appletalk
Boot	Boot image
C	Commserver file (CiscoPro)
Drag	IOS based diagnostic images
G	ISDN subnet (SNMP, IP, Bridging, ISDN, PPP, IPX, Atalk)
I	IP subnet (SNMP, IP, Bridging, WAN, Remote Node, Terminal Services)
N	IPX
Q	Async
T	Telco return (12.0)
Y	Reduced IP (SNMP, IP RIP/IGRP/EIGRP, Bridging, ISDN, PPP) (C1003/4)
Z	Managed moderns
40	40 bit encryption
56	56 bit encryption
Format (Where the image runs in the route)	
F	Flash
M	Ram
R	Rom
L	Rebcatable
Compression Type	
Z	Zip compressed (note lower case)
X	M zip compressed
W	“STAC” compress

Hình 2.1.4a

Khi bạn chọn mua IOS mới thì một trong những điều quan trọng bạn cần phải chú ý là sự tương thích giữa IOS với bộ nhớ flash và RAM trong router. Thông thường

thì các phiên bản mới có thêm nhiều đặc tính mới thì lại đòi hỏi thêm nhiều bộ nhớ. Bạn có thể dùng lệnh **show version** để kiểm tra phần IOS hiện tại và dung lượng flash còn trống. Trên trang web hỗ trợ của Cisco có một số công cụ giúp bạn xác định dung lượng flash và RAM cần thiết cho từng loại IOS.

Trước khi cài đặt phần mềm Cisco IOS mới lên router, bạn phải kiểm tra xem router có đủ dung lượng bộ nhớ hay không. Để xem dung lượng RAM bạn dùng lệnh **show version**:

…<*output omited*>… cisco 1721 (68380) processor (revision c) with 3584k/512K bytes of memory.

Dòng trên cho biết dung lượng của bộ nhớ chính và bộ nhớ chia sẻ trên router. Có mốt số thiết bị sử dụng một phần DRAM làm bộ nhớ chia sẻ. Tổng hai dung lượng trên là dung lương thật sự của DRAM trên router.

Để xem dung lượng của bộ nhớ flash bạn dung lệnh **show flash**:

GAD#**show flash**

…<*output omitted*>…

1599897 bytes total (10889728 bytes free)

```
BHM#show version
Cisco Internetwork Operating System Software
IOS (tm) 1700 Software (C1700-BNSY-L), Version
12.2(11)P, RELEASE SOFTWARE (fc1)
… <output omitted>…
System image file is "flash:c1700-y7-mz", booted via
flash
cisco 1721 (68380) processor (revision C) with
3584K/512K bytes of memory.
Processor board ID 12014633, with hardware revision
00000000
Bridging software.
X.25 software, Version 2.0, NET2, BFE and GOSIP
compliant.
1 Ethernet/IEEE 802.3 interface(s)
2  serial(sync/async) network interface(s)
System/IO memory with parity disabled
2048K bytes of DRAM onboard 2048K bytes of DRAM on SIMM
System running from FLASH
8K bytes of non-volatile configuration memory.
6144K bytes of processor board PCMCIA flash (Read ONLY)
Configuration register is 0x2102
BHM#
```

Hình 2.1.4b

2.1.5 Hoạt động của phầm mềm Cisco IOS

Thiết bị Cisco IOS có 3 chế độ hoạt động sau:

- ROM monitor
- Boot ROM
- Cisco IOS.

Thông thường trong quá trình khởi động router, một trong các chế độ hoạt động trên được tải lên RAM để chạy. Người quản trị hệ thống có thể cài đặt giá trị cho thanh ghi để điều khiển chế độ khởi động mặc định router.

Chế độ ROM monitor thực hiện quá trình bootstrap và kiểm tra phần cứng. Chế độ này được sử dụng để khôi phục lại hệ thống khi bị lỗi ngiêm trọng hoặc khi người quản trị mạng bị mất mật mã. Chúng ta chỉ có thể truy cập vào chế độ ROM monitor bằng đường kết nối vật lý trực tiếp vào cổng console trên router. Ngoài ra chúng ta không thể truy cập vào chế độ này bằng bất ký cổng nào khác.

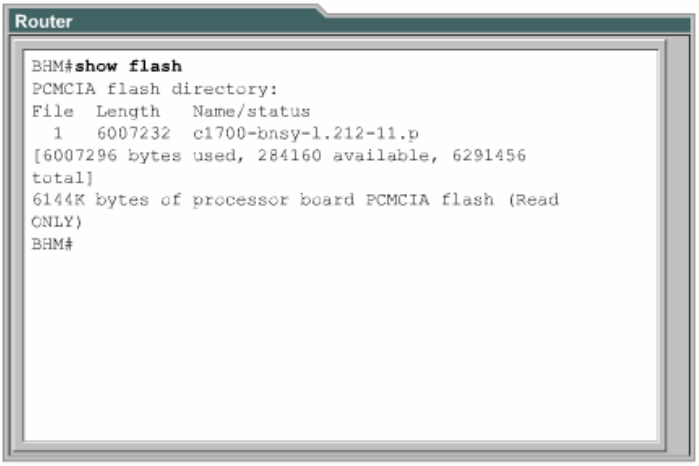
Khi router ở chế độ boot ROM, chỉ có một phần chức năng của Cisco IOS là hoạt động được. Chế độ boot ROM cho phép bạn chép được lên bộ nhớ flash, nên chế độ này thường được sử dụng để thay thế phần mềm Cisco IOS trong flash. Bạn dùng lệnh **copy tftp flash** để chép phần mềm IOS trên TFTP server vào bộ nhớ flash trên router.

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

Hình 2.1.5a

Router muốn hoạt động bình thường thì phải chạt được toàn bộ phần mềm IOS trong flash. Ở một số thiết bị, phần mềm IOS được chạy trực tiếp từ flash. Tuy nhiên, hầu hết các Cisco router đều chép phần mềm IOS lên RAM rồi chạy từ RAM. Một số phần mềm IOS lưu trong flash dưới dạng nén và được giải nén khi chép lên RAM.

Bạn dùng lệnh **show version** để xem các thông tin về phần mềm IOS, trong đó có hiển thị giá trị cấu hình của thanh ghi. Còn nếu bạn muốn xem hệ thống còn bao nhiêu dung lượng bộ nhớ để tải phần mềm Cisco IOS mới thì bạn dùng lệnh **show flash**.



Hình 2.1.5b

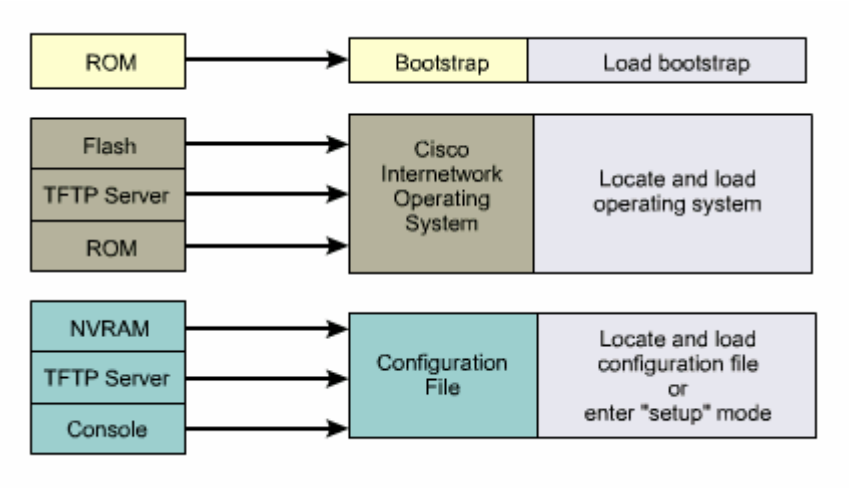
2.2 Bắt đầu với router

2.2.1 Khởi động router

Router khởi động bằng cách tải bootstrap, hệ điều hành và tập tin cấu hình. Nếu router không tìm thấy tập tin cấu hình thí sẽ tự động vào chế độ cài đặt. Khi bạn hoàn tất việc cấu hình trong chế độ cài đặt thì tập tin cấu hình đó sẽ được lưu trong NVRAM.

Để cho router bắt đầu hoạt động, quá trình khởi động phần mềm Cisco IOS thực hiện 3 công đoạn sau:

- Kiểm tra phần cứng của router và bảo đảm là chúng hoạt động tốt.
- Tìm và tải phần mềm Cisco IOS.
- Tìm và thực thi tập tin cấu hình khởi động hoặc vào chế độ cài đặt nếu không tìm thấy tập tin này.



Hình 2.2.1a: Các bước khởi động router

Khi router mới được bật điện lên thì nó thực hiện quá trình tự kiểm tra POST (Power on self test). Trong quá trình này, router chạy một trình từ ROM để kiểm tra tất cả các thành phần phần cứng trên router, ví dụ như kiểm tra hoạt động của CPU, bộ nhớ và các cổng giao tiếp mạng. Sau khi hoàn tất quá trình này, router bắt đầu thực hiện khởi động phần mềm.

Sau quá trình POST, router sẽ thực hiện các bước sau:

- Bước 1: Chạy chương trình nạp bootstrap từ ROM. Bootstrap chỉ đơn giản là một tập lệnh để thực hiện kiểm tra phần cứng và khởi động IOS.
- Bước 2: Tìm IOS. Giá trị khởi động trên thanh ghi cấu hình sẽ quyết định việc tim IOS ở đâu. Nếu giá trị này cho biết là tải IOS từ flash hay từ mạng thi các câu lệnh boot system trong tập tin cấu hình sẽ cho biết chính xác vị trí và tên của IOS.
- Bước 3: Tải hệ điều hành đã được tải xuống và bắt đầu hoạt động thì các bạn sẽ thấy hiện trên màn hình console danh sách các thành phần phần cứng và phần mềm có trên router.
- Bước 4: Tập tin cấu hình lưu trong VNRAM được chép lên bộ nhớ chính và được thực thi từng dòng lệnh một. Các câu lệnh cấu hình thực hiện khởi động quá trình định tuyến, đặt địa chỉ cho các cổng giao tiếp mạng và thiết lập nhiều đặc tính hoạt động khác cho router.
- Bước 5: Nếu không tìm thấy tập tin cấu hình trong VNRAM thì hệ điều hành sẽ đi tìm TFTP server. Nếu cũng không tìm thấy một TFTP server nào thì chế độ cài đặt sẽ được khởi động.

Trong chế độ cài đặt, các bạn không thể cấu hình cho các giao thức phức tạp của router. Mục đích của chế độ cài đặt chỉ là cho phép người quản trị mạng cài đặt một cấu hình tối thiểu cho router khi không thể tìm được tập tin cấu hình từ những nguồn khác.

Trong chế độ cài đặt, câu trả lời mặc định được đặt trong dấu ngoặc vuông [] ở sau mỗi câu hỏi. Bạn có thể nhấn phím Ctrl-C bất kỳ lúc nào để kết thúc quá trình cài đặt. Khi đó tất cả các cổng giao tiếp mạng trên router sẽ đóng lại.

Khi bạn hoàn tất cấu hình trong chế độ cài đặt, bạn sẽ gặp các dòng thông báo như sau:

[0] Go to the IOS command promt without saving this config.

[1] Return back to the setup without saving this config.

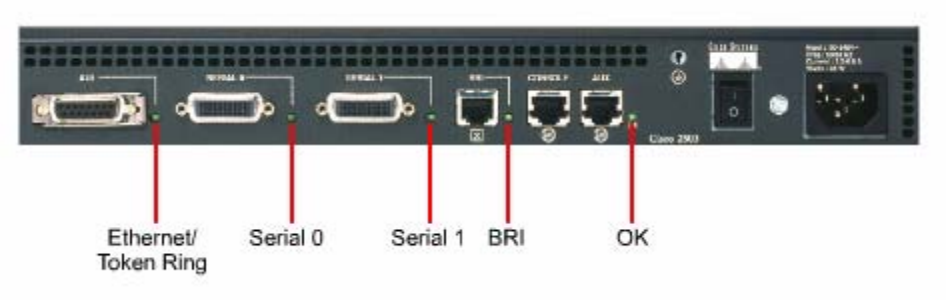
[2] Save this configuration to nvram and exit.

Enter your selection [2]:

Hình 2.2.1b: Chế độ cài đặt của 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
```

2.2.1. Đèn LED báo hiệu trên router

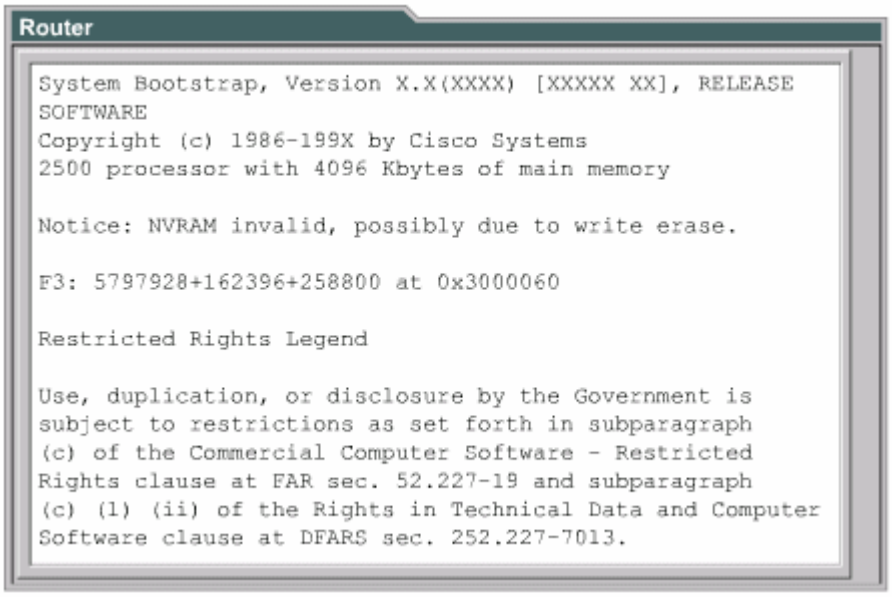


Hình 2.2.2

Cisco router sủ dụng đèn LED để báo hiệu các trạng thái hoạt động của router. Các loại đèn LED này sẽ khác nhau tuỳ theo các loại router khác nhau.

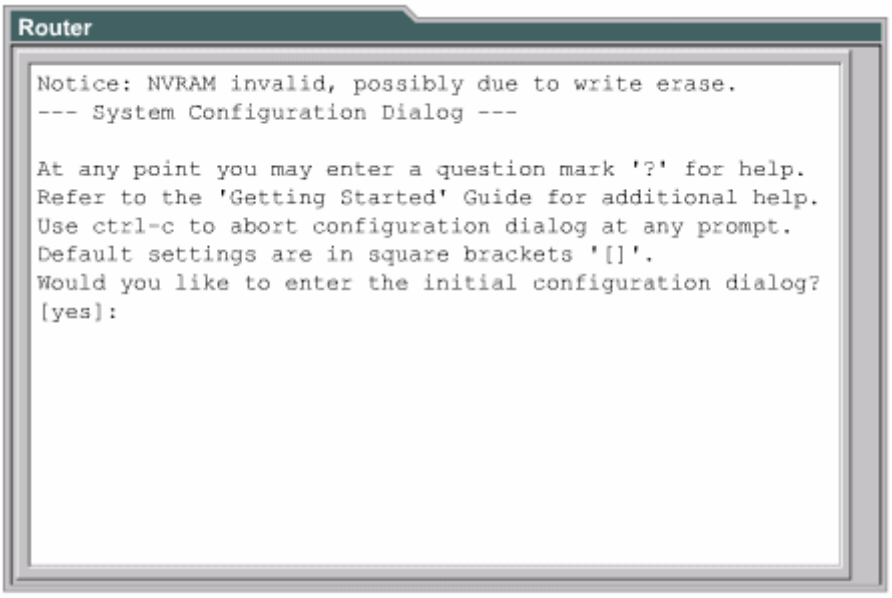
Các đèn LED của các cổng trên router sẽ cho biết trạng thái hoạt động của các cổng. Nếu đen LED của một cổng nào đó bị tắt trong khi cổng đó đang hoạt động và được kết nối đúng thì chứng tỏ là đã có sự cố đối với cổng đó. Nếu một cổng hoạt động liên tuc thì đèn LED của cổng đó sáng liên tục. Còn đèn LED OK ở bên phải cổng AUX sẽ bật sáng sau khi router hoạt động tốt.

2.23. Khảo sát quá trình khởi động của router

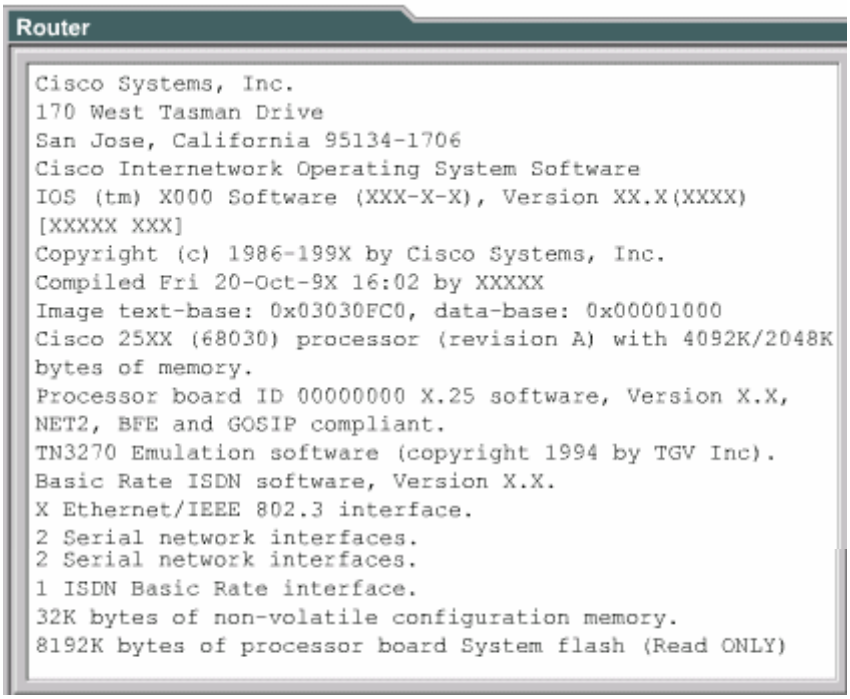


Hình 2.2.3a: Thông tin hiển thị trong quá trình khởi động router

Ví dụ ở hình 2.2.3a cho thấy nội dung các thông điệp được hiển thị trên màn hình console trong suốt quá trình khởi động của router. Các thông tin này sẽ khác nhau tuỳ theo các loại cổng có trên router và tuỳ theo từng phiên bản Cisco IOS. Do đó hình 2.2.3a chỉ là một ví dụ để tham khảo chứ không pản ánh chính xác toàn bộ những gì được hiện thị.



Trong hình 2.2.3b, câu "VNRAM invalid, possibly due to write erase" cho biết router này chưa được cấu hình hoặc là NVRAM đã bị xoá. Thông thường khi router đã được cấu hình thì tập tin cấu hình được lưu trong NVRAM, sau đó ta phải cấu hình thanh ghi để router sử dụng tập tin cấu hình này. Giá trị mặc định của thanh ghi cấu hình là 0x2102, khi đó router sẽ khởi động với Cisco IOS tải từ bộ nhớ flash và tập tin cấu hình tải từ NVRAM.



Hình 2.2.3c: Thông tin hiển thị trong quá trình khởi động router

Dựa vào thông tin như hình 2n2n3c, chúng ta có thể xác định được phiên bản của phần mềm boottrap và IOS đang được sử dụng trên router. Ngoài ra bạn cũng xác định được phiên bản của router, bộ xử lý là loại gì, cung lượng của bộ nhớ và một số các thông tin khác của router như:

- Số lượng các cổng giao tiếp.
- Các loại cổng giao tiếp.
- Dung lượng NVRAM.
- Dung lượng bộ nhớ flash.

2 Thiết lập phiên kết nối bằng HyperTerminal

Tất cả các Cisco router đều có cổng console nối tiếp bất đồng bộ TIA/EIA-232 (RJ45). Chúng ta cần phải có cáp và bộ chuyển đổi để kết nối từ thiết bị đầu cuối console vào cổng console trên router. Thiết bị đầu cuối console có thể là một thiết bị đầu cuối ASCII hoặc là một PC có chạy chương trình mô phỏng HyperTerminal. Để kết nối PC có cổng console chúng ta dùng cáp rollover và bộ chuyển đổi RJ45-DB9.

Thông số mặc định của cổng console là: 9000 baud, 8 data bits, 1 stop bit, no flow control. Cổng console không có hỗ trợ điều khiển luồng băng phần cứng. Sau đây là bước thực hiện để kết nối một thiết bị đầu cuối vào cổng console trên router:

- Kết nối thiết bị đầu cuối 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 sau: 96000 baud, 8 data bits, 1 stop bit, no flow control.

Truy cập vào router

Để cấu hình router bạn phải truy cập vào giao diện người dùng của router bằng thiết bị đầu cuối hoặc bằng đường truy cập từ xa. Sau khi truy cập được vào router thi bạn mới có thể nhập các câu lệnh cho router.

Vì lý do bảo mật nên router có 2 mức truy cập:

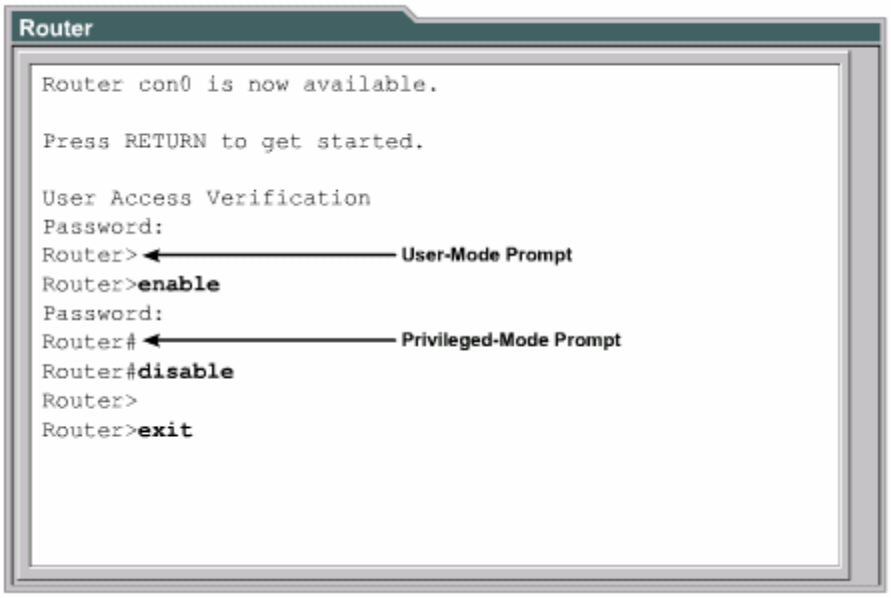
- Mức EXEC người dùng: chỉ có một số câu lệnh dùng để xem trạng thái của router. Ở mức này, bạn không thể thay đổi được cấu hình của router.
- Mức EXEC đặc quyền: bao gồm tất cả các câu lệnh để cấu hình router.

Ngay sau khi truy cập được vào router bạn sẽ gặp dâu nhắc của chế độ EXEC người dùng. Để sử dụng được toàn bộ tập lệnh bạn phải chuyển vào chế độ EXEC đặc quyền. Ở dấu nhắc “>” bạn gõ lệnh **enable**. Ở dấu nhắc **password**: bạn phải nhập mật mã đúng với mật mã đã được cấu hình cho router trước đó bằng lệnh **enable secret** hoặc **enable password**. Nếu mật mã của router đã được cấu hình bởi cả 2 lệnh trên thì mật mã của câu lệnh **enable secret** sẽ được áp dụng. Sau khi hoàn tất các bước trên bạn sẽ gặp dấu nhắc “#” cho biết là bạn đang ở chế độ EXEC đặc quyền. Từ chế độ này bạn mới có thể truy cập vào chế độ cấu hình toàn cục rồi sau đó là các chế độ cấu hình riêng biệt hơn như:

- Chế độ cấu hình cổng giao tiếp.
- Chế độ cấu hình cổng giao tiếp con.
- Chế độ cấu hình đường truy cập.
- Chế độ cấu hình router.

- Chế độ cấu hình route-map.

Từ chế độ EXEC đặc quyền, bạn gõ disable hoặc exit để trở về chế độ EXEC người dùng. Để trở về chế độ EXEC đặc quyền từ chế độ cấu hình toàn cục, bạn dùng lệnh exit hoặc Ctrl-Z. Lệnh Ctrl-Z có thể sử dùng để trở về ngay chế độ EXEC đặc quyền từ bất kỳ chế độ cấu hình riêng biệt nào.

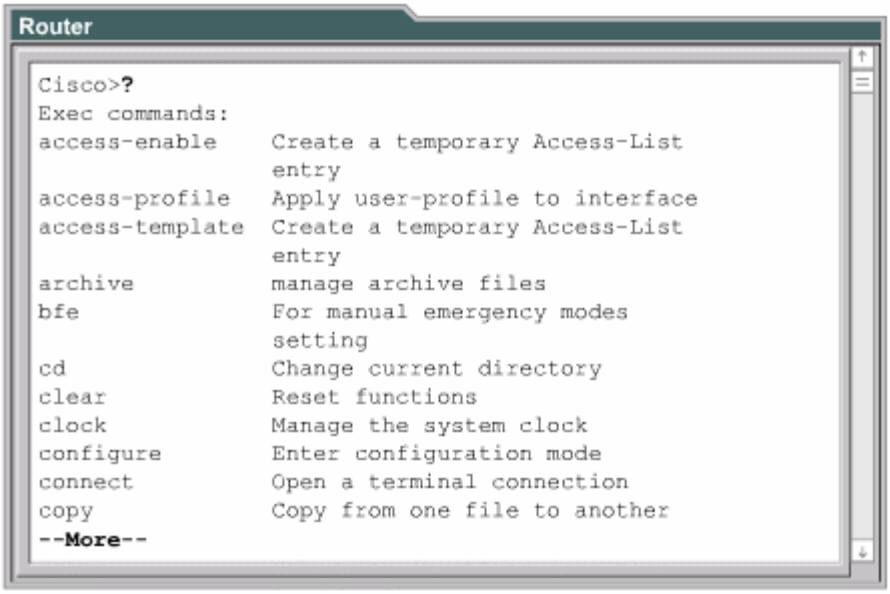


Hình 2.2.5a

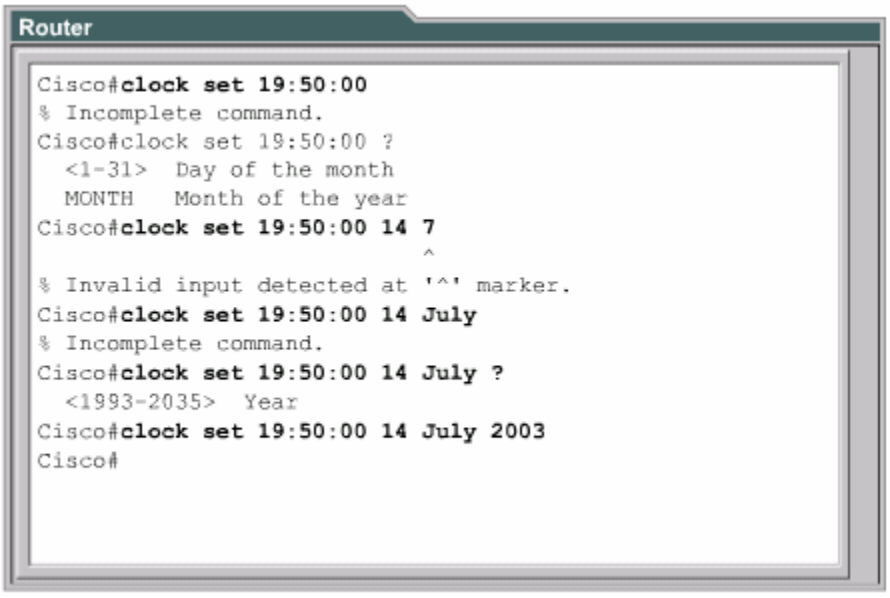
2.2.6. Phím trợ giúp trong router CLI

Khi bạn gõ dấu chấm hỏi (?) ở dấu nhắc thì router sẽ hiển thị danh sách các lệnh tương ứng với chế độ cấu hình mà bạn đang ở. Chữ "**--More--**" ở cuối màn hình cho biết là phần hiển thị vẫn còn tiếp. Để xem trang tiếp theo, bạn nhấn nhanh

Spacebar. Còn nếu bạn muốn hiển thị tiếp từng dòng một thì bạn nhấn phím Enter hoặc Return. Bạn có thể nhấn từng dòng một thì bạn nhấn phím bất kỳ nào khác để quay trở về dấu nhắc.



Hình 2.2.6a: Danh sách lệnh sử dụng ở chế độ EXEC người dung



Để chuyển vào chế độ EXEC đặc quyền bạn gõ **enable** hoặc gõ tắt là **ena** cũng được. Nếu mật mã đã được cài đặt vào cho router thì router sẽ yêu cầu bạn nhập mật mã. Sau khi bạn đã vào được chế độ này rồi thì bạn gõ dấu chấm hỏi (?), bạn

sẽ thấy là danh sách các câu lệnhdung chó chế độ EXEC đặc quyền nhiều hơn hẳn danh sách các câu lệnh mà bạn thấy trong chế độ EXEC người dùng. Tuy nhiên các tập lệnh này sẽ khác nhau tuỳ theo cấu hình của router và tuỳ theo từng phiên bản phần mềm Cisco IOS.

Bây giờ giả sử bạn muốn cài đặt đồng hồ cho router nhưng bạn lai không biết phải dùng lệnh nào thi khi đó chức năng trợ giúp của router sẽ giúp bạn tìm được câu lênh đúng. Bạn thực hiện theo các bước sau:

1. Dùng dấu chấm hỏi để tìm câu lệnh cài đặt đồng hồ. Trong danh sách các câu lệnh được hiển thị bạn sẽ tìm được lệnh **clock.**
2. Kiểm tra cú pháp câu lệnh để khai báo giờ.
3. Bạn nhập giờ, phút, giây theo đúng cú pháp câu lệnh. Bạn sẽ gặp câu thông báo là câu lệnh chưa hoàn tất như hình 2.2.6b.
4. Bạn nhấn **Ctrl-P** hoặc phím mũi tên (↑) để lại lệnh vừa mới nhập. Ở cuối câu lệnh đó bạn thêm một khoảng trắng và dấu chấm hỏi (?) để xem phần kế tiếp của câu lệnh. Sau đó bạn nhập lại đầy đủ câu lệnh.
5. Nếu bạn gặp dấu (^) thì có nghĩa là câu lệnh đã bị nhập sai. Vị trí của dấu (^) sữ cho biết vị trí mà câu lệnh từ đầu cho tới vị trí mà dấu (^) chỉ sai rồi bạn sẽ nhập thêm dấu chấm hỏi (?) để thêm cú pháp đúng tiếp theo của câu lệnh.
6. Bạn nhập lại đầy đủ câu lệnh theo đúng cú pháp rồi nhấn phím **Enter** hoặc **Return** để thực thi câu lệnh.

2.2.7. Mở rộng thêm về cách viết câu lệnh

Trong giao diện người dùng của router, router có thể có chế độ hỗ trợ soạn thảo câu lệnh. Bạn có thể sử dụng các tổ hợp phím như hình 2.2.7a để di chuyển con trỏ trên dòng lệnh mà bạn đang viết khi bạn cần phải chỉnh sửa câu lệnh đó. Trong các phiên bản phần mêm hiện nay, chế độ hỗ trợ soạn thảo câu lệnh là hoàn toàn tự động. Tuy nhiên nếu chế độ này lèn ảnh hưởng khi bạn biết các script thị bạn có thể tắt bằng lệnh **terminal no editing** trong chế độ EXEC đặc quyền.

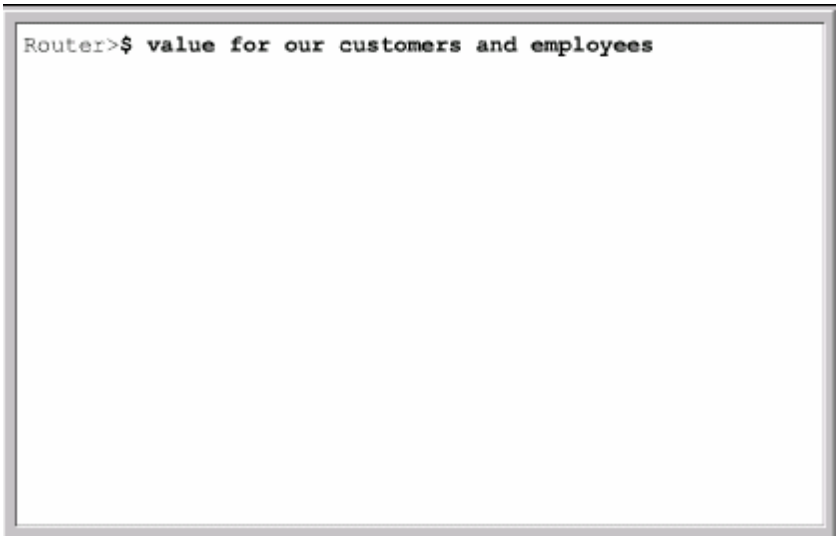
Command	Description
Ctrl-A	Moves to the beginning of the command line

Esc-B	Moves back one word
Ctrl-B (or right arrow)	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

Khi soạn thảo câu lệnh, màn hình sẽ cuộn ngang khi câu lệnh dài quá một hang. Khi con trỏ đến hết lề phải thì dòng lệnh sẽ dịch sang trái 10 khoảng trắng. Khi đó 10 ký tự đầu tiên của câu lệnh sẽ không nhìn thấy được trên màn hình nữa. Bạn có thể cuộn lại để xem bằng cách nhấn **Ctrl-B** hoặc nhấn phím mũi tên (←) cho tới khi màn hình cuộn tới đầu câu lệnh. Hoặc bạn có thể nhấn **Ctrl-A** để chuyển ngay về đầu dòng lệnh.

Trên hình 2.2.7b là ví dụ khi một câu lệnh dài quá một hành. Dấu ($) cho biết là câu lệnh đã được dịch sang trái.

Phím **Ctrl-Z** được sử dụng để quay trở về chế độ EXEC đặc quyền từ bất kỳ chế độ cấu hình riêng biệt nào.



Hình 2.2.7b

2.2.8. Gọi lại các lệnh đã sử dụng

Khi cấu hình router, router co lưu lại một số các lệnh bạn đã sử dụng. Điều này đặc biệt có ích khi bạn muốn lặp lại các câu lệnh dài và phức tạp. Với cơ chế này bạn có thể thực hiện các việc sau:

- Cài đặt kíchthước vùng bộ đệm để lưu các câu lệnh đã sử dụng.
- Gọi lại các câu lệnh đã sử dụng.
- Tắt chức năng này đi.

Mặc định là router sẽ lưu lại 10 câu lệnh trong bộ đệm. Bạn có thể thay đổi số lượng câu lệnh mà router lưu lại bằng lệnh **terminal history size** hoặc **history size**. Tối đa là 255 câu lệnh có thể lưu lại được.

Nếu bạn muốn gọi lại câu lệnh vừa mới sử dụng gần nhất thì bạn nhấn **Ctrl-P** hoặc phím mũi tên (↑). Nếu bạn tiếp tục nhấn thì mỗi lần nhấn như vậy bạn sẽ gọi lại tuần tự các câu lệnh trước đó nữa. Nếu bạn muốn gọi lui lạ một câu lệnh sau đó thì bạn nhấn **Ctrl-N** hoặc nhấn phím mũi tên (↓). Tương tự, nếu bạn tiếp tục nhấn như vậy thi mỗi lần nhấn bạn sẽ gọi lại một lệnh đó.

Khi gõ lệnh, bạn chỉ cần gõ các ký tự đủ để router phân biệt với mọi câu kệnh khác rồi nhấn phím **Tab** thì router sẽ tự động hoàn tất câu lệnh cho bạn. Khi bạn dùng phím **Tab** mà router hiển thị được đủ câu lệnh thì có nghĩa là router đã nhận biết được câu lệnh mà bạn muốn nhập.

Ngoài ra, hầu hết các router đều có them chức năng cho bạn đánh dấu khối và copy. Nhờ đó bạn có thể copy câu lệnh trước đó rồi dán hoặc chèn vào câu lệnh hiện tại.

Lệnh	Giải thích lệnh
Ctrl-P or up arrow key	Gọi lại lệnh ngay trước đó
Ctrl-N or down arrow key	Gọi lại lệnh ngay sau đó
Router>**show history**	Xem các lệnh đã sử dụng còn lưu trong bộ đệm
Router>**Terminal history size number-of-lines**	Cài đặt dung lượng bộ đệm đã lưu các lệnh đã sử dụng
Router>**terminal no editing**	Tắt chức năng soạn thảo lệnh nâng cao
Router>**terminal editing**	Mở chức năng soạn thảo lệnh nâng cao
<**Tab**>	Hoàn tất câu lệnh

Xử lý lỗi câu lệnh

Lỗi câu lệnh thường là do bạn gõ sai. Sau khi bạn gõ một câu lệnh bị sai thì bạn sẽ gặp dấu báo lỗi (^). Dấu báo lỗi (^) đặt ở vị trí mà câu lệnh bắt đầu bị sai. Dựa vào đó và vận dụng chức năng trợ giúp của hệ thống bạn sẽ tìm ra và chỉnh sửa lại lỗi cú pháp của câu lệnh.

Router#clock set 13:32:00 February 93
% Invalid input detected at "^" marker

Trong ví dụ trên, dấu báo lỗi cho biết câu lệnh bị sai ở số 93. Bạn gõ lại câu lệnh từ đầu tới vị trí bị lỗi rồi thêm dấu chấm hỏi (?) như sau:

Router # clock set 13:32:00 February ?
<1993-2035>Year

Sau đó bạn nhập lại câu lệnh với số năm đúng như cú pháp ở trên:

Router#**clock set 13:32:00 February 1993**

Sau khi bạn gõ xong câu lệnh rồi nhấn phím Enter mà câu lệnh đó bị sai thì bạn có thể dùng phím mũi tên (↑) để gọi câu lệnh vừa mới nhập. Sau đó bạn dùng các phím mũi tên sang phải, sang trái di chuyển con trỏ tới vị trí bị sai để sửa lại. Nếu cần xoá các ký tự thì bạn có thể dùng phím <backspace>.

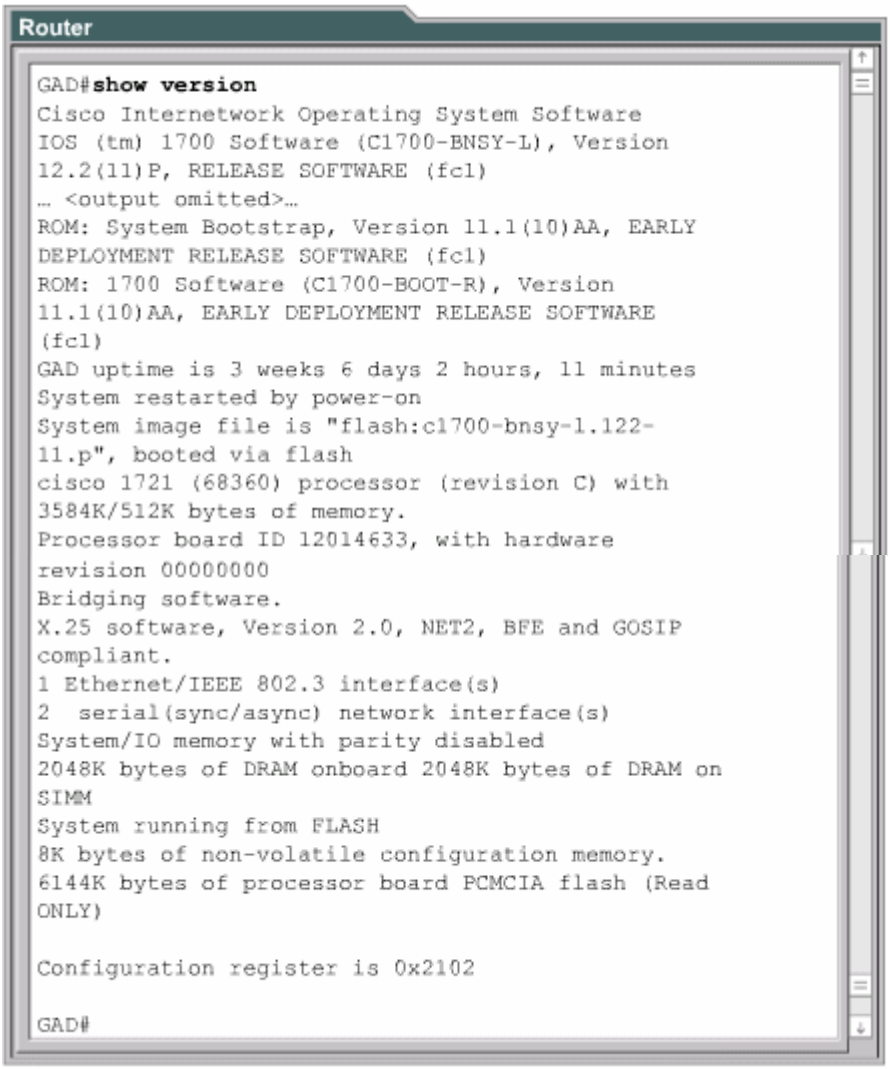
Lệnh show version

Lệnh show version dùng để hiển thị các thông tin về phiên bản phần mềm Cisco IOS đang chạy trên router, trong đó có cả thông tin về giá trị thanh ghi cấu hình.

Trong hình dưới các bạn sẽ thấy nhung thông tin được hiển thị do lệnh show version bao gồm:

- Phiên bản IOS và một ít thông tin đặc trưng.
- Phiên bản phần mềm Bootstrap ROM.
- Phiên bản phần mềm Boot ROM.
- Thời gian hoạt động của router.
- Phương thức khởi động router lần gần đây nhất.
- Tên và vị trí lưu phần mềm hệ điều hành.
- Phiên bản phần cứng của router.

- Giá trị cài đặt của thanh ghi cấu hình.



Chúng ta thường sử dụng lệnh show version để xác định phiên bản của phần mềm IOS và xem giá trị thanh ghi cài đặt cho qua trình khởi động của router.

TỔNG KẾT

Sau khi kết thúc chương này, chúng ta nắm được các ý như sau:

- Mục đích của IOS.
- Hoạt động cơ bản của IOS.
- Xác định các đặc tính khác nhau của các phiên bản IOS khác nhau.

- Các phương pháp thiết lập phiên kết nối CLI vào router.
- Sự khác nhau giữa 2 chế độ EXEC người dùng và EXEC đặc quyền
- Thiết lập phiên kết nối vào router bằng HyperTerminal.
- Truy cập vào router.
- Sử dụng chế độ trợ giúp của router trong giao diện dòng lệnh.
- Sử dụng cơ chế hỗ trợ soạn thảo câu lệnh.
- Gọi lại các câu lệnh đã sử dụng.
- Xử lý lỗi câu lệnh.
- Sử dụng lệnh show version.

CHƯƠNG 3

CẤU HÌNH ROUTER

GIỚI THIỆU

Cấu hình router để cho router thực hiện nhiều chức năng mạng phức tạp là một công việc đầy thử thách. Tuy nhiên bước bắt đầu cấu hình router thì không khó lắm. Nếu ngay từ bước này bạn cố gắng thực hành nhiều để làm quen và nắm vững được các bước di chuyển giữa các chế độ cấu hình của router thì công việc cấu hình phức tạp về sau sẽ trở nên đơn giản hơn rất nhiều. Trong chương này sẽ giới thiệu về các chế độ cấu hình cơ bản của router và một số lệnh cấu hình đơn giản.

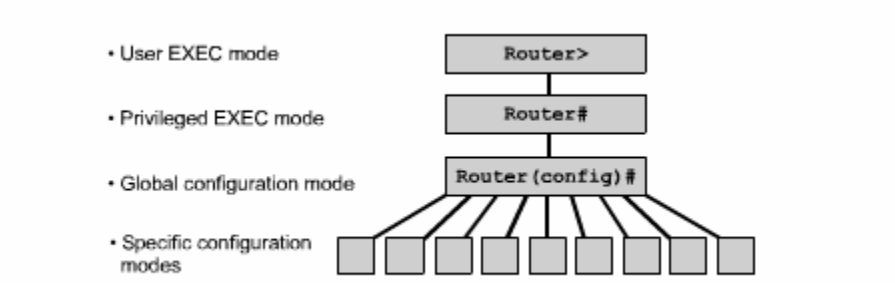
Kỹ năng đọc và hiểu một cách rõ ràng các tập tin cấu hình là một ký năng rất quan trọng của người quản trị mạng. Cisco IOS có cung cấp một số công cụ cho người quản trị mạng để thêm một số thông tin cần thiết vào tập tin cấu hình. Cũng giống như những người lập trình phải có tài liệu của từng bước lập trình thì người quản trị mạng cũng cần được cung cấp thông tin càng nhiều càng tốt khi mà hệ thống mạng do người khác quản trị.

Khi hoàn tất chương này các bạn có thể:

- Đặt tên cho router.
- Cài đặt mật mã cho router.
- Khảo sát các lệnh show.
- Cấu hình cổng Ethernet trên router.
- Thực hiện một số thay đổi trên router.
- Lưu các thay đổi đó lại.
- Cấu hình câu chú thích cho các cổng giao tiếp trên router.
- Cấu hình thông điệp hàng ngày cho router.
- Cấu hình bảng host cho router.
- Hiểu được tầm quan trọng của việc ghi nhận lại và lưu dự phòng cấu hình của router.

3.1.Cấu hình router

3.1.1.Chế độ giao tiếp dòng lệnh CLI



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)#

Hình 3.1.1

Tất cả các câu lệnh làm thay đổi cấu hình router đều xuất phát từ chế cầu hình toàn cục. Tuỳ theo ý bạn muốn thay đổi thay đổi phần cấu hình đặc biệt nào của router thì bạn chuyển vào chế độ chuyên biệt tương ứng. Các chế độ cấu hình chuyên biệt này đều là chế độ con của chế độ cấu hình toàn cục.

Các câu lệnh được sử dụng trong chế độ cấu hình toàn cục là những câu lệnh có tác động lên toàn bộ hệ thống. Bạn sử dụng câu lệnh sau để di chuyển vào chế độ cấu hình toàn cục:

Chú ý: *Sự thay đổi của dấu nhắc cho biết bạn đang ở chế độ cấu hình toàn cục*

Router # **configure terminal**

Router(config)#

Chế độ cấu hình toàn cục là chế độ cấu hình chính. Từ chế độ này bạn có thể chuyển vào các chế độ chuyên biệt như:

- Chế độ cấu hình cổng giao tiếp.
- Chế độ cấu hình đường truy cập.
- Chế độ cấu hình router.
- Chế độ cấu hình cổng con.
- Chế độ cấu hình bộ điều khiển.

Khi bạn chuyển vào chế độ cấu hình chuyên biệt nào thì dấu nhắc sẽ thay đổi tương ứng. Các câu lệnh trong đó chỉ có tác động đối với các cổng hay các tiến trình nào liên quan đến chế độ cấu hình đó thôi.

Bạn dùng lệnh exit để trở về chế độ cấu hình toàn cục hoặc bạn dùng phím Ctrl-Z để quay về thẳng chế độ EXEC đặc quyền.

3.1.2. Đặt tên cho router

Công việc đầu tiên khi cấu hình router là đặt tên cho router. Trong chế độ cấu hình toàn cục, bạn dùng lệnh sau:

Router(config)#**hostname Tokyo**

Tokyo (config)#

Ngay sau khi bạn nhấn phím Enter để thực thi câu lệnh bạn sẽ thấy dấu nhắc đổi từ tên mặc định (Router) sang tên mà bạn vừa mới đặt (Tokyo).

3.1.3. Đặt mật mã cho router

Mật mã được sử dụng để hạn chế việc truy cập vào router. Thông thường ta luôn đặt mật mã cho đường vty và console trên router. Ngoài ra mật mã còn được sử dụng để kiểm soát sự truy cập vào chế độ EXEC đặc quyền trên router. Khi đó, chỉ

những người nào được phép mới có thể thực hiện việc thay đổi tập tin cấu hình trên router.

Sau đây là các lệnh mà bạn cần sử dụng để thực hiện việc đặt mật mã cho đường console:

Router(config)#**line console** 0

Router(config-line)#**password** <password>

Router(config-line)#**login**

Chúng ta cũng cần đặt mật mã cho một hoặc nhiều đương vty để kiểm soát các user truy nhập từ xa vào router và Telnet. Thông thường Cisco router có 5 đường vty với thứ tự từ 0 đến 4. Chúng ta thường sử dụng một mật mã cho tất cả các đường vty, nhưng đôi khi chúng ta nên đặt thêm mật mã riêng cho một đường để dự phòng khi cả 4 đường kia đều đang được sủ dụng. Sau đây là các lệnh cần sử dụng để đặt mật mã cho đường vty:

Router(config)#**line vty** 0 4

Router(config-line)#**password** <password>

Router(config-line)#**login**

Mật mã **enable** và **enable secret** được sử dụng để hạn chế việc truy cập vào chế độ EXEC đặc quyền. Mật mã **enable** chỉ được sử dụng khi chúng ta cài đặt mật mã **enable secret** vì mật mã này được mã hoá còn mật mã **enable** thì không. Sau đây là các lệnh dùng để đặt mật mã **enable secret**:

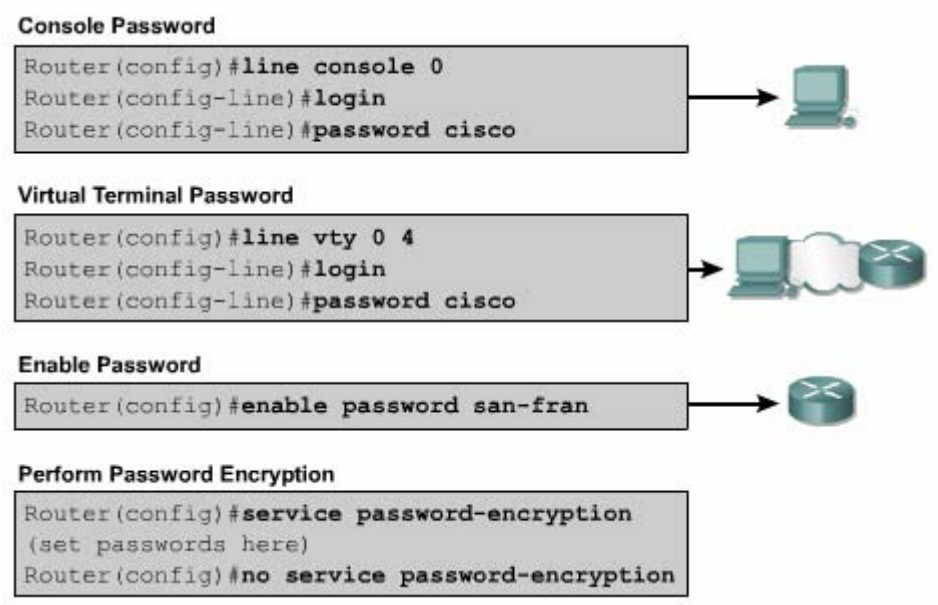
Router(config)#**enable password** <password>

Router(config)#**enable secret** <password>

Đôi khi bạn sẽ thấy là rất không an toàn khi mật mã được hiển thị rõ ràng khi sử dụng lệnh **show running-config** hoặc **show startup-config**. Để tránh điều này bạn nên dùng lệnh sau để mã hoá tất cả các mật mã hiển thị trên tập tin cấu hình của router:

Router(config)#**service password-encryption**

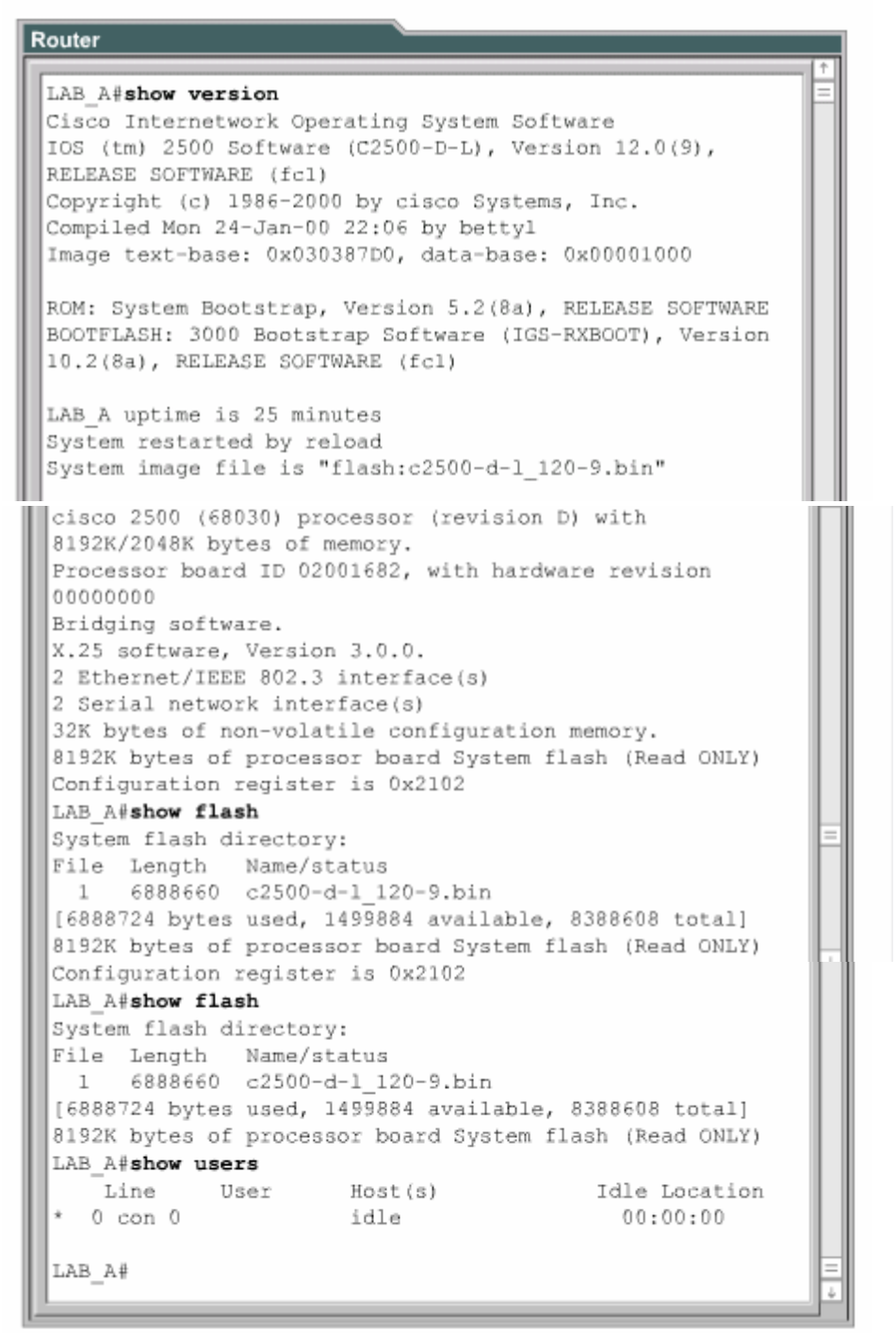
Lệnh **service password-encryption** sẽ áp dụng một cơ chế mã hoá đơn giản lên tất cả các mật mã chưa được mã hoá. Riêng mật má **enable secret** thì sử dụng một thuật toán mã hoá rất mạnh là MD5.



Hình 3.1.3

3.1.4. Kiểm tra băng các lệnh show

Chúng ta có rất nhiều lệnh **show** được dùng để kiểm tra nội dung các tập tin trên router và để tìm ra sự cố. Trong cả hai chế độ EXEC đặc quyền và EXEC người dùng, khi bạn gõ **show?** Thì bạn sẽ xem được danh sách các lệnh **show**. Đương nhiên là số lệnh **show** dùng được trong chế độ EXEC đặc quyền sẽ nhiều hơn trong chế độ EXEC người dùng.



Hình 3.1.4

- Show interface - hiển thị trạng thái của tất cả các cổng giao tiếp trên router. Để xem trạng thái của một cổng nào đó thì bạn thêm tên và số thứ tự của cổng đó sau lệnh show interface. Ví dụ như:
  Router#**show interface serial 0/1**

- Show controllers serial - hiển thị các thông tin chuyên biệt về phần cứng của các cổng serial.
- Show clock - hiển thị đồng hồ được cài đặt trên router.
- Show hosts - hiển thị danh sách tên và địa chỉ tương ứng.
- Show users - hiển thị tất cả các user đang kết nối vảo router.
- Show history - hiển thị danh sách các câu lệnh vừa mới được sử dụng.
- Show flash – hiển thị thông tin bộ nhớ flash và tập tin IOS chứa trong đó.
- Show version - hiển thị thông tin về router và IOS đang chạy trên RAM.
- 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 startup-configuration - hiển thị tập tin cấu hình đăng chạy trên RAM.

3.1.5. Cấu hình cổng serial

Chúng ta có thẻ cấuhình cổng serial bằng đường console hoặc vty. Sau đây là các bước cần thực hiện khi câu hình cổng serial:

1. Vào chế độ cấu hình toàn cục.
2. Vào chế độ cấu hình cổng serial.
3. Khai báo địa chỉ và subnet mask.
4. Đặt tốc độ clock nếu đầu cáp cắm vào cổng serial là DCE. Nếu đầu cáp là DTE thì chúng ta có thể bỏ qua này.
5. Khởi động serial.

Mỗi một cổng serial đều phải có một địa chỉ IP và subnet mask để chúng có thể định tuyến các gói IP. Để cấu hình địa chỉ IP chúng ta dùng lệnh sau:

Router(config)#**interface serial** 0/0
Router(config)#**ip address** <ip address> <netmask>

Cổng serial cần phải có tín hiệu clock để điều khiển thời gian thực hiện thông tin liên lạc. Trong hầu hết các trường hợp, thiết bị DCE, ví dụ như CSU, sẽ là thiết bị cung cấp tín hiệu clock. Mặc định thì Cisco router lad thiết bị DTE nhưng chúng ta có thể cấu hình chúng thành thiết bị DCE.

Trong môi trường làm lab thì các đường liên kết serial được kết nối trực tiếp với nhau. Do đó phải có một đầu là DCE để cấp tín hiệu clock. Bạn dùng lệnh **clockrate** để cài đặt tốc độ clock. Sau đây là các tốc độ clock mà bạn có thể đặt cho router (đơn vị của tốc độ clock là bit/s): 1200, 2400, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000, 4000000. Tuy nhiên sẽ có một số tốc độ bạn không sử dụng được tuỳ theo khả năng vật lý của từng cổng serial.

Mặc định thì các cổng giao tiếp trên router đều đóng. Nếu bạn muốn mở hay khởi động các cổng này thì bạn phải dùng lệnh **no shutdown**. Nếu bạn muốn đóng cổng lại để bảo trì hoặc xử lý sự cố thì bạn dùng lệnh **shutdown**.

Trong môi trường làm lab, tốc độ clock thường được sử dụng là 56000. Sau đây là các lệnh được sử dụng để cài đặt tốc độ clock và khởi động cổng serial:

Router(config)#**interface serial** 0/0

Router(config-if)#**clock rate** 56000

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

3.1.6. Thực hiện việc thêm bớt, dịch chuyển và thay đổi tập tin cấu hình

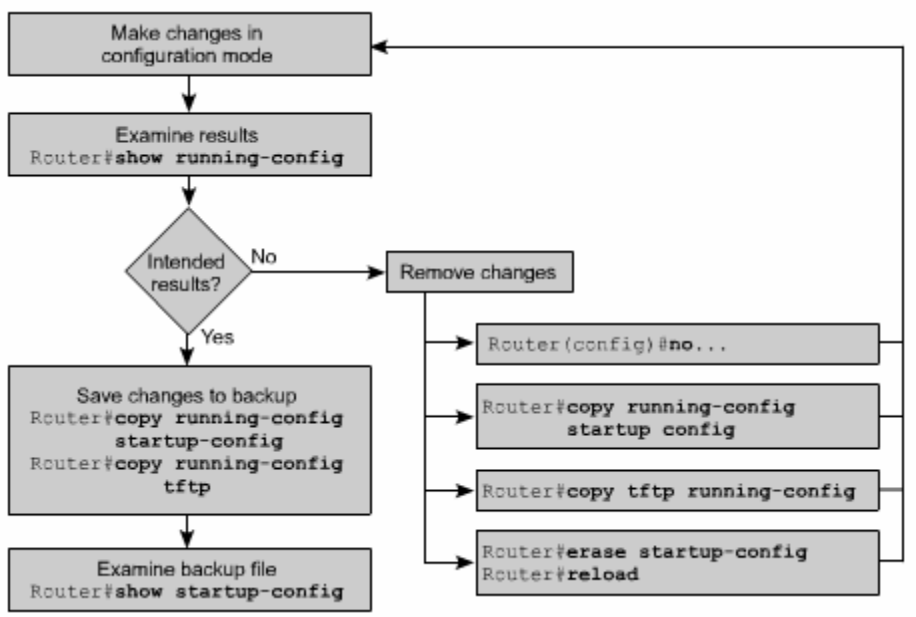
Nếu bạn cần chỉnh sửa tập tin cấu hình thì bạn phải di chuyển vào đùng chế độ cấu hình và thực hiện cần thiết. Ví dụ:nếu bạn cần mở một cổng nào đó trên router thì trước hết bạn phải vào chế độ cấu hình toàn cục, sau đó vào chế độ cấu của cổng đó rồi dùng lệnh **no shutdown**.

Để kiểm tra những gì mà bạn vừa mới thay đổi, bạn dùng lệnh **show running-config**. Lệnh này sẽ hiển thị nội dung của tập tin cấu hình hiện tại. Nếu kết quả hiển thị có những có những chi tiết không đúng thì bạn có thể chỉnh sửa lại bằng cách thực hiện một hoặc nhiều cách sau:

- Dùng dạng **no** của các lệnh cấu hình.
- Khởi động lại router với tập tin cấu hình nguyên thuỷ trong NVRAM.
- Chép tập tin cấu hình dự phòng từ TFTP server.
- Xoá tập tin cấu hình khởi động bằng lệnh **erase startup-config**,sau đó khởi động lại router và vào chế độ cài đặt.

Để lưu tập tin, cấu hình hiện tại thành tập tin cấu hình khởi động lưu trong NVRAM, bạn dùng lệnh như sau:

Router#**copy running-config startup-config**



Hình 3.1.6.

3.1.7. Cấu hình cổng Ethernet

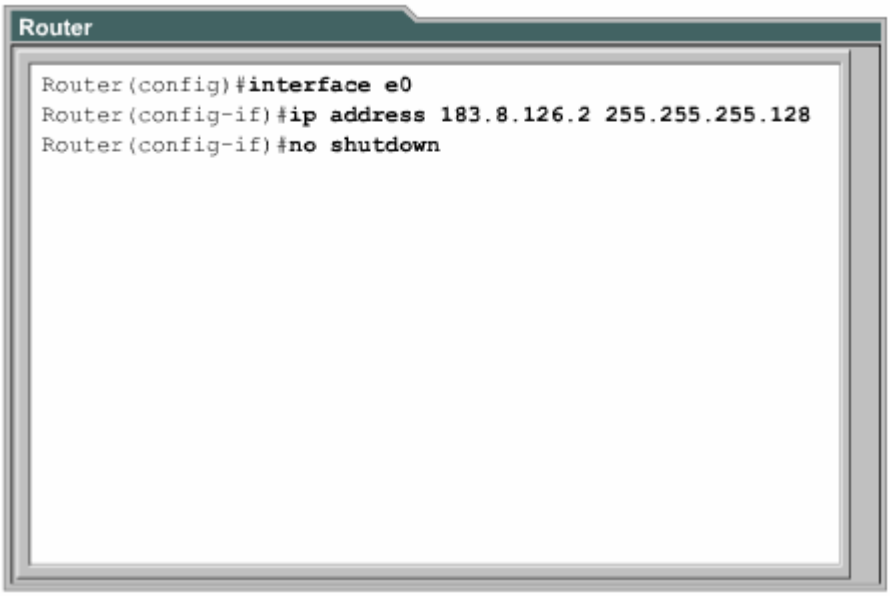
Tương tự như cổng serial, chúng ta có thể cấu hình cổng Ethernet bằng đường console hoặc vty.

Mỗi cổng Ethernet cũng cần phải có một địa chỉ IP và subnet mask để có thể thực hiện định tuyến các gói IP qua cổng đó.

Sau đây là các bước thực hiện cấu hình Ethernet:

- Vào chế độ cấu hình toàn cục.
- Vào chế độ cấu hình cổng Ethernet.
- Khai báo địa chỉ và subnet mask.
- Khởi động cổng Ethernet.

Măc định là các cổng trên router đều đóng. Do đó, bạn phải dùng lệnh **no shutdown** để mở hay khởi động cổng. Nếu bạn cần đóng cổng lại để bảo trì hay xử lý sự cố thì bạn dùng lệnh **shutdown.**



Hình 3.1.7

3.2. Hoàn chỉnh cấu hình router

3.2.1. Tầm quan trọng của việc chuẩn hoá tập tin cấu hình

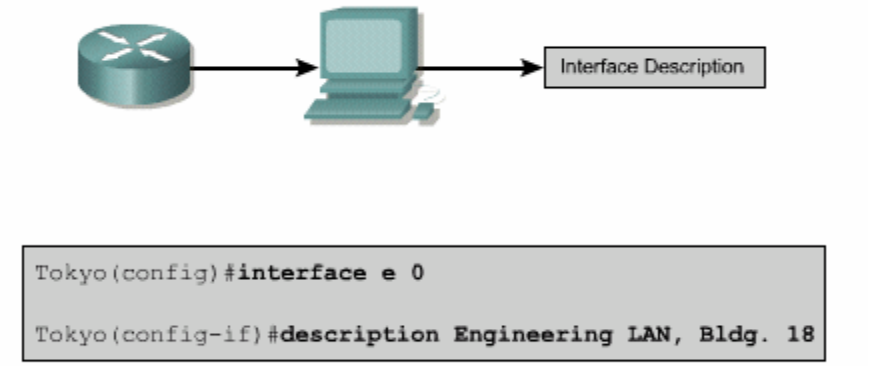
Trong một tổ chức việc phát các quy định dành cho các tập tin cấu hình là rất cần thiết. Từ đó ta có thể kiểm soát được các tập tin nào càn bảo trì, lưu các tập tin ở đâu và như thế nào.

Các quy định này có thể là những quy định được ứng dụng rộng rái hoặc cũng có thể chỉ có giá trị trong một phạm vi nào đó. Nếu không có một quy định chung cho tổ chức của mình thì hệ thống mạng của bạn sẽ trở nên lộn xộn và không đảm bảo được hoạt động thông suốt.

3.2.2. Câu chú thích cho các cổng giao tiếp

Trên các cổng giao tiếp bạn nên ghi chú lại một số thông tin quan trọng, ví dụ như chỉ số mạch mà cổng này kết nối vào, hay thông tin vào router khác, về phân đoạn mạng mà cổng này kết nối đến. Dựa vào các câu chú thích này, người quản trị mạng có thể biết được là cổng giao tiếp này kết nối vào đâu.

Câu chú thích chỉ đơn giản là ghi chú thêm cho các cổng giao tiếp, ngoài ra nó hoàn toàn không có tác động gì đối với hoạt động của router. Bẹn nên viết câu chú thích theo một định dạng chung và mỗi cổng giao tiếp có một câu chú thích riêng. Tuỳ theo cấu trúc mạng và quy ước chung, bạn có thể quyết định là ghi chú những thông tin nào liên quan đến cổng giao tiếp để giúp cho tập tin cấu hình được rõ ràng hơn, giúp cho việc xác định sự cố được nhanh hơn.



Hình 3.2.2

3.2.3. **Cấu hình chú thích cho các cổng giao tiếp**

Trước tiên bạn phải vào chế độ cấu hình toàn cục. Rồi từ chế độ cấu hình toàn cục bạn chuyển vào chế độ cấu hình cổng giao tiếp. Tại đây bạn gõ lệnh **description** và câu chú thích mà bạn muốn.

Sau đây là các bước để cấu hình câu chú thích cho cổng giao tiếp:

1. Vào chế độ cấu hình toàn cục bằng lệnh **configure terminal.**
2. Vào chế độ cấu hình cổng giao tiếp (ví dụ là cổng Ethernet 0): **interface Ethernet 0**.
3. Nhập lệnh **description** và theo sau là câu chú thích.
4. Thoát khỏi chế độ cấu hình giao tiếp để trở về chế độ EXEC đăc quyền bằng cách nhấn phím **Ctrl-Z**.
5. Lưu lại cấu hình vừa rồi vào NVRAM bằng lệnh **copy running-config startup-config**.

Sau đây là 2 ví dụ về cách viết câu chú thích:

Interface Ethernet 0
Description LAN Engineering, Bldg.2

Interface serial 0

Description ABC network 1, circuit 1

```
LAB_A# config terminal
Enter configuration commands, one per line. End with
CNTL_Z
LAB_A (config)# interface Ethernet 0
LAB_A (config-if)#description LAN Engineerinng, Bldg. 2
```

Hình 3.2.3

3.2.4. Thông điệp đăng nhập

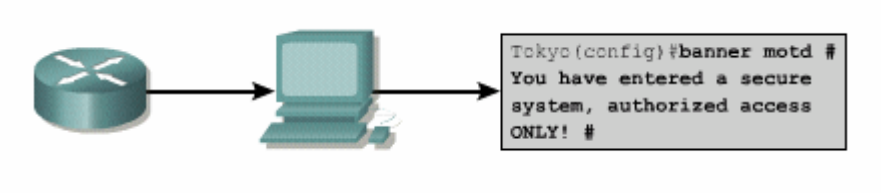
Thông điệp đăng nhập được hiển thị khi bạn đăng nhập vào hệ thống. Loại thông điệp này rất hữu dụng khi bạn cần cảnh báo trước khi đến giờ tắt hệ thống mạng.

Tất cả mọi người đều có thể nhìn thấy thông điệp đăng nhập. Cho nên bạn nên dùng các thông điệp mạng tính cảnh báo, thu hút sự chú ý. Còn những thông điệp để "chào đón" mọi người đăng nhập vào router là không thích hợp lắm.

Ví dụ một thông điệp như sau: "This is a secure system, authorized access only!" (Đây là hệ thống được bảo mật, chỉ dành cho những người có thẩm quyền!) được sử dụng để cảnh báo những vị khách viếng thăm bất hợp pháp.

Hình 3.2.4

3.2.5. **Cấu hình thông điệp đăng nhập (MOTD)**



Hình 3.2.5

Thông điệp MOTD có thể hiển thị trên tất vả các thiết bị đầu cuối kết nối vào router.

Để cấu hình thông điệp MOTD bạn vào chế độ cấu hình toàn cục. Tại đây bạn dùng lệnh **banner motd**, cách một khoảng trắng, nhập ký tự phân cách ví dụ như ký tự #, rồi viết câu thông báo, kết thúc bằng cách nhập ký tự phân cách một lần nữa.

Sau đây là các bước thực hiện để cấu hình thông điệp MOTD:

1. Vào chế độ cấu hình toàn cục bằng lệnh **configure terminal**
2. Nhập lệnh như sau: banner motd # The message of the day goes here #.
3. Lưu cấu hình vừa rồi bằng lệnh **copy running-config startup-config**.

3.2.6. Phân giải tên máy

Phân giải tên máy là quá trình máy tính phân giải từ tên mày thành địa chỉ IP tương ứng.

Để có thể liên hệ với các thiết bị IP khác bằng tên thì các thiết bị mạng như router cũng cần phải có khả năng phân giải tên máy thành địa chỉ IP. Danh sách giữa tên máy và địa chỉ IP tương ứng được gọi là bảng host.

Bảng host có thể bao gồm tất cả các thiết bị mạng trong tổ chức của mình. Mỗi một địa chỉ IP có một tên máy tương ứng. Phần mềm Cisco IOS có một vùng đệm để lưu tên máy và địa chỉ tương ứng. Vùng bộ đệm này giúp cho quá trình phân giải tên thành địa chỉ được nhanh hơn.

Tuy nhiên tên máy ở đây không giống như tên DNS, nó chỉ có ý nghĩa đối với router mà nó được cấu hình mà thôi. Người quản trị mạng có thể cấu hình bảng host trên router với bất kỳ tên nào với IP nào và các thông tin này chỉ có ý nghĩa đối với router đó mà thôi.

The following is an exemple of the configuration of a host table on a router:

```
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
```

Hình 3.2.6

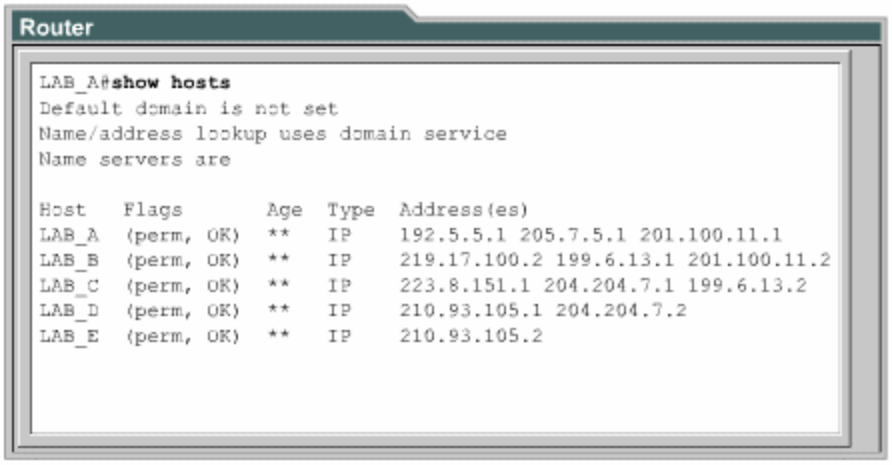
3.2.7. **Cấu hình bảng host**

Để khai báo tên cho các địa chỉ IP, đầu tiên bạn vào chế độ cấu hình toàn cục. Tại đây dùng lệnh **ip host**, theo sau là tên của thiết bị và tất cả các IP của nó. Như vậy tên máy này sẽ ánh xạ với từng địa chỉ IP của các cổng trên thiết bị đó. Khi đó bạn có thể dùng lệnh ping hay telnet tới thiết bị đó bằng tên của thiết bị hay địa chỉ IP tương ứng đều được.

Sau đay là các bước thực hiện cấu bảng host:

1. Vào chế độ cấu hình toàn cục của router.
2. Nhập lệnh **ip host** theo sau là tên của router và tất cả các địa chỉ IP của các cổng trên router đó.
3. Tiếp tục nhập tên và địa chỉ IP tương ứng của các router khác trong mạng

4. Lưu cấu hình vào NVRAM.



Hình 3.2.7

3.2.8. **Lập hồ sơ và lưu dự phòng tập tin cấu hình**

Tập tin cấu hình của các thiết bị mạng sẽ quyết định sự hoạt động của hệ thống. Công việc quản lý tập tin cấu hình của các thiết bị bao gồm các công việc sau:

- Lập danh sách và so sánh với tập tin cấu hình trên các thiết bị đang hoạt động.
- Lưu dự phòng các tập tin cấu hình lênh server mạng.
- Thực hiện cài đặt và nâng cấp các phần mềm.

Chúng ta cần lưu dự phòng các tập tin cấu hình để sử dụng trong trường hợp có sự cố. Tập tin cấu hình có thể được lưu trên server mạng, ví dụ như TFTP server, hoặc là lưu trên đĩa và cất ở nơi an toàn. Ngoài ra chúng ta cũng nên lập hồ sơ đi kèm với các tập tin này.

3.2.9. **Cắt, dán và chỉnh sửa tập tin cấu hình**

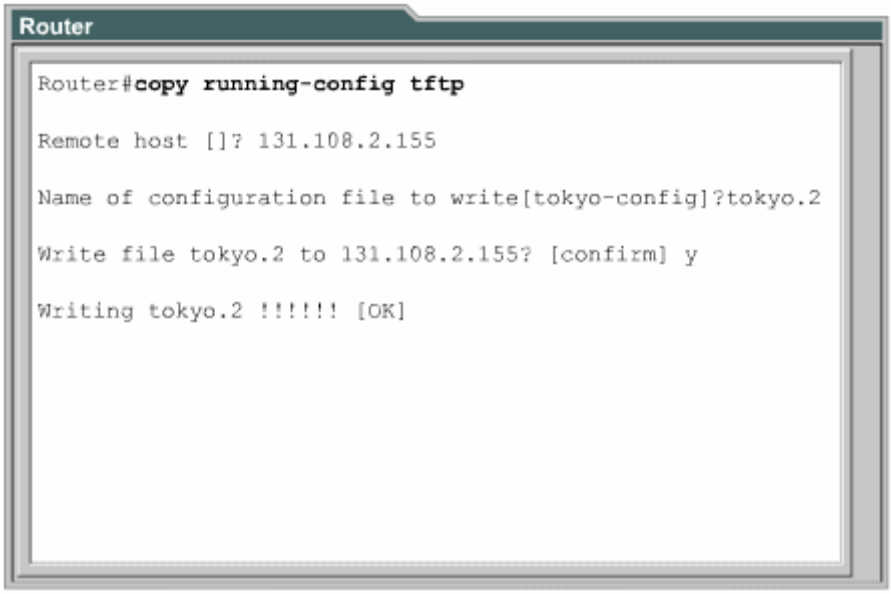
Chúng ta có thể dùng lệnh **copy running-config tftp** để sao chép tập tin cấu hình đang chạy trên router vào TFTP server. Sau đây là các bước thực hiện:

Bước 1: nhập lệnh **copy running-config tftp**.

Bước 2: nhập địa chỉ IP của máy mà chúng ta sẽ lưu tập tin cấu hình lên đó.

Bước 3: nhập tên tập tin.

Bước 4: xác nhận lại câu lệnh bằng cách trả lời “yes”



Hình 3.2.9a

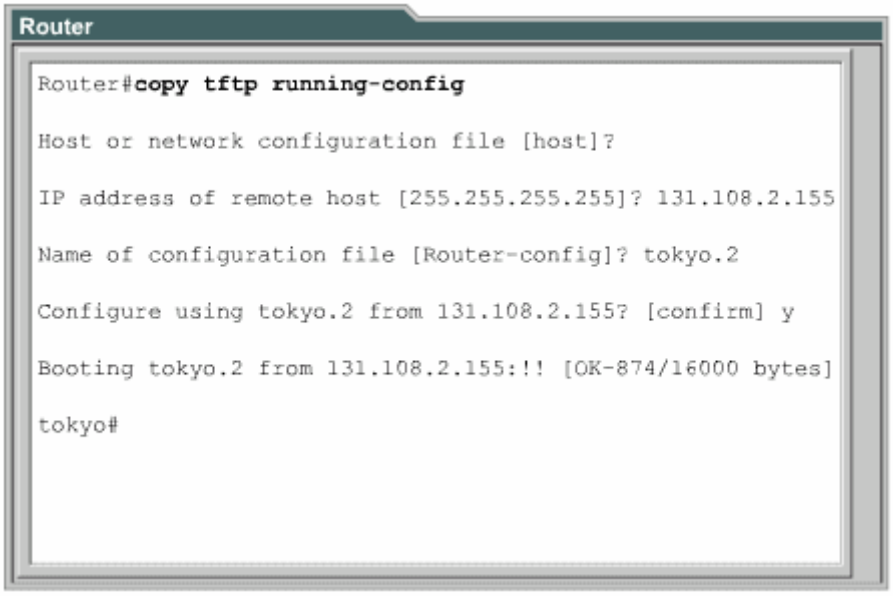
Chúng ta có thể sử dụng tập tin cấu hình lưu trên server mạng để cấu hình cho router.

Để thực hiện điều này bạn làm theo các bước sau:

1. Nhập lênh **copy tftp running-config**.
2. Ở dấu nhắc tiếp theo bạn chọn loại tập tin cấu hình máy hay tập tin cấu hình mạng. Tập tin cấu hình mạng có chứa các lệnh có thể thực thi cho tất cả các router và server trong mạng. Còn loại tập tin cấu hình máy thì cỉh s các lệnh thực thi cho một router mà thôi. Ở dấu nhắc kế tiếp, bạn nhập địa chỉ IP của máy nào mà bạn đang lưu tập tin cấu hình trên đó. Ví dụ như trên hình 3.2.9b: router được cấu hình từ TFTP server có địa chỉ IP là 131.108.2.155.
3. Sau đó nhập tên của tập tin hoặc là chấp nhận lấy tên mặc định. Tên của tập tin theo quy tắc của UNIX. Tên mặc định cho loại tập tin cấu hình máy là hostname-config, còn tên mặc định cho loại tập tin cấu hình mạng là netword-config. Trong môi trường DOS thì tên tập tin bị giới hạn với 8 ký tự và 3 ký tự mở rộng (ví dụ như: router.cfg). Cuối cùng bạn xác nhận lại tất cả các thông tin vừa rồi. Bạn lưu ý trên hình thì sẽ thấy là dấu nhắc chuyển

ngay sang tên Tokyo. Điều này chứng tỏ là router được cấu hình lại ngay sau khi tập tin cấu hình vừa được tải xuống.

Tập tin cấu hình trên router cũng có thể được lưu vào đĩa bằng cách sao chép dưới dạng văn bản rồi lưu vào đĩa mềm hoặc đĩa cứng. Khi nào cần chép trở lại rouer thì bạn dùng chức năng soạn thảo cơ bản của chương trình mô phỏng thiết bị đầu cuối để cắt dán các dòng lệnh vào router.



Hình 3.2.9b

TỔNG KẾT CHƯƠNG

Sau đây là phần tổng kết các ý chính mà bạn cần nắm khi cấu hình router.

Router có các chế độ sau:

- Chế độ EXEC người dùng.
- Chế độ EXEC đặc quyền.
- Chế độ cấu hình toàn cục.
- Các chế độ cấu hình khác.

Bạn có thể dùng giao diện dòng lệnh của router để thực hiện một số thay đổi cho cấu hình của router như:

- Đặt tên cho router.

- Đặt mật mã cho router.
- Cấu hình các cổng giao tiếp trên router.
- Chỉnh sửa tập tin cấu hình.
- Hiển thị tập tin cấu hình.

Ngoài ra, bạn cần nhớ một số điểm quan trọng sau:

- Xây dựng một cấu hình chuẩn là yếu tố quan trọng để thành công trong việc bảo trì bất kỳ hệ thống mạng của một tổ chức nào.
- Câu chú thích cho các cổng giao tiếp có thể mang một số thông tin quan trọng giúp cho người quản trị mạng nắm được cấu trúc hệ thống mạng và xử lý sự cố nhanh hơn.
- Thông điệp đăng nhập sẽ cung cấp các thông báo cho người dùng khi họ đăng nhập vào router.
- Phân giải tên máy thành địa chỉ IP cho phép router có thể chuyển đổi nhanh từ máy ra địa chỉ.
- Công việc lập hồ sơ và lưu dự phòng tập tin cấu hình là hết sức quan trọng để bảo đảm cho hệ thống mạng luôn hoạt động thông suốt.

CHƯƠNG 4
CẬP NHẬT THÔNG TIN TỪ CÁC THIẾT BỊ KHÁC

GIỚI THIỆU

Đôi khi người quản trị mạng sẽ phải xử lý những hệ thống mạng mà không có hồ sơ đầy đủ và chính xác. Trong những tình huống như vậy thì giao thức CDP-Cisco Discovery Protocol sẽ là một công cụ rất hữu ích giúp bạn xây dựng được cấu trúc cơ bản về hệ thống mạng. CDP là một giao thức hoạt động không phụ thuộc vào môi trường truyền của mạng, giao thức này là độc quyền của Cisco được sử dụng để phát hiện các thiết bị xung quanh. CDP sẽ hiển thị thông tin về các thiết bị kết nối trực tiếp mà bạn đang xử lý. Tuy nhiên đây không phải là một công cụ thực sự mạng.

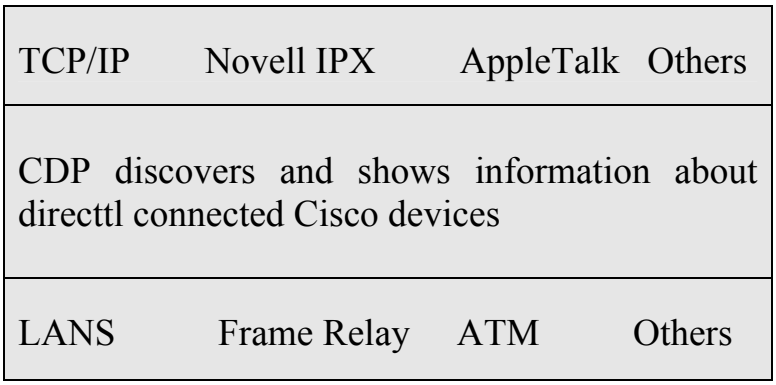
Trong nhiều trường hợp, sau khi router đã được cấu hình và đi vào hoạt đông thị nhà quản trị mạng sẽ khó có thể kết nối trực tiếp vào router để cấu hình hay làm gì khác. Khi đó, Telnet, là một ứng dụng của TCP/IP, sẽ giúp người quản trị mạng thiết lập kết nối từ xa vào chế độ giao tiếp dòng lệnh (CLI) của router để xem, cấu hình và xử lý sự cố. Đây là một công cụ chủ yếu của các chuyên gia mạng.

Sau khi hoàn tất chương này, các bạn sẽ nắm được các kiến thức sau:

- Bật và tắt CDP.
- Cách sử dụng lệnh **show cdp neighbors**.
- Cách xác định các thiết bị lân cận kết nối vào cổng giao tiếp.
- Ghi nhận thông tin về địa chỉ mạng của các thiết bị lân cận bằng cách sử dụng CDP.
- Thiết lập kết nối Telnet.
- Kiểm tra kết nối Telnet.
- Kết thúc phiên Telnet.
- Tạm ngưng một phiên Telnet.
- Thực hiện các kiểm tra kết nối khác.
- Xử lý sự cố với các kết nối từ xa.

4.1. Kết nối và khám phá các thiết bị lân cận

4.1.1. Giới thiệu về CDP



Hình 4.1.1

CDP là giao thức lớp 2 kết nối với lớp vật lý ở dưới và lớp mạng ở trên như hình vẽ. CDP được sử dụng để thu thập thông tin từ các thiết bị lân cận, ví dụ như thiết bị đó là loại thiết bị nào, trên thiết bị đó cổng nào là cổng kết nối và kết nối vào cổng nào trên thiết bị của chúng ta, phiên bản phần cứng của thiết bị đó là gì…CDP là giao thức hoạt động độc lập với môi trường truyền mạng và có thể chạy trên tất cả các thiết bị của Cisco trên nền giao thức truy cập mạng con SNAP (Subnet Access Protocol).

Phiên bản 2 của CDP (CDPv2) là phiên bản mới nhất của giao thức này. Cisco IOS từ phiên bản 12.0(3)T trở đi có hỗ trợ CDPv2. Mặc định thì Cisco IOS (từ phiên bản 10.3 đến 12.0(3) chạy CDP phiên bản 1).

Khi thiết bị Cisco được bật lên, CDP tự động hoạt động và cho phép thiết bị dò tìm các thiết bị lân cận khác cùng chạy CDP. CDP hoạt động ở lớp liên kết dữ liệu và cho phép 2 thiết bị thu thập thông tin lẫn nhau cho dù 2 thiết bị này có thể chạy giao thức lớp mạng khác nhau.

Mỗi thiết bị được cấu hình CDP sẽ gửi một thông điệp quảng cáo theo định kỳ cho các router khác. Mỗi thông điệp như vậy phải có ít nhất một địa chỉ mà thiết bị đó có thể nhận được thông điệp của giao thức quản lý mạng cơ bản SNMP (Simple Network Management Protocol) thông qua địa chỉ đó. Ngoài ra, mỗi thông điệp quảng cáo còn có "thời hạn sống" hoặc là thời hạn lưu giữ thông tin. Đây là khoảng thời gian cho các thiết bị lưu giữ thông tin nhận được trước khi xoá bỏ thông tin đó đi. Bên cạnh việc phát thông điệp, mỗi thiết bị cũng lắng nghe theo

định kỳ để nhận thông điệp từ các thiết bị lân cận khac để thu thập thông tin về chúng.

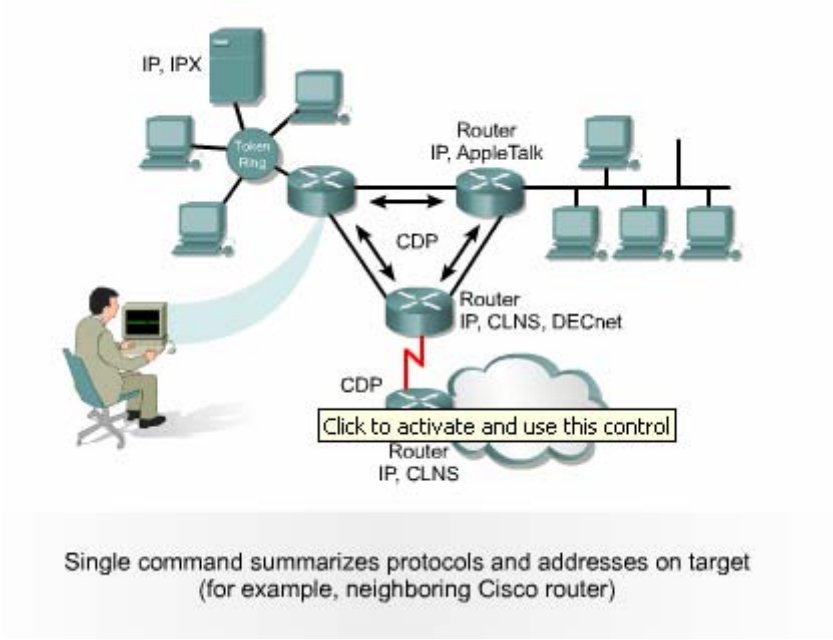
4.1.2. Thông tin thu nhận được từ CDP

CDP được sử dụng chủ yếu để phát hiện tất cả các thiết bị Cisco khác kết nối trực tiếp vào thiết bị của chúng ta. Bạn sử dụng lênh **show cdp neighbors** để hiển thị thông tin về các mạng kết nối trực tiếp vào router. CDP cung cấp thông tin về từng thiết bị CDP láng giềng bằng cách truyền thông báo CDP mang theo cac giá trị "type length" (TLVs).

TLVs được hiển thị bởi lệnh **show cdp neighbors** sẽ bao gồm các thông tin về:

- Device ID: Chỉ số danh định (ID) của thiết bị láng giềng.
- Local interface: Cổng trên thiết bị của chúng ta kết nối đến thiết bị láng giềng,
- Hold time: thời hạn lưu giữ thông tin cập nhật.
- Capability: loại thiết bị.
- Platform: phiên bản phần cứng của thiết bị.
- Port ID: chỉ số danh định (ID) của cổng trên thiết bị láng giềng kết nối vào thiết bị của chúng ta.
- VTP management domain name: tên miền quản lý của VTP (chỉ có ở CDPv2).
- Native VLAN: VLAN mặc định trên router (chỉ có ở CDPv2).
- Half/Full duplex: chế độ hoạt động song công hay bán song công.

Trong hình 4.1.2, router ở vị trí thấp nhất không kết nối trực tiếp vàp router mà người quản trị mạng đang thực hiện kết nối console. Do đó để xem được các thông tin CDP của router này, người quản trị mạng phải Telnet vào router kết nối trực tiếp với router đó.



Hình 4.1.2

4.1.3. Chạy CDP, kiểm tra và ghi nhận các thông tin CDP

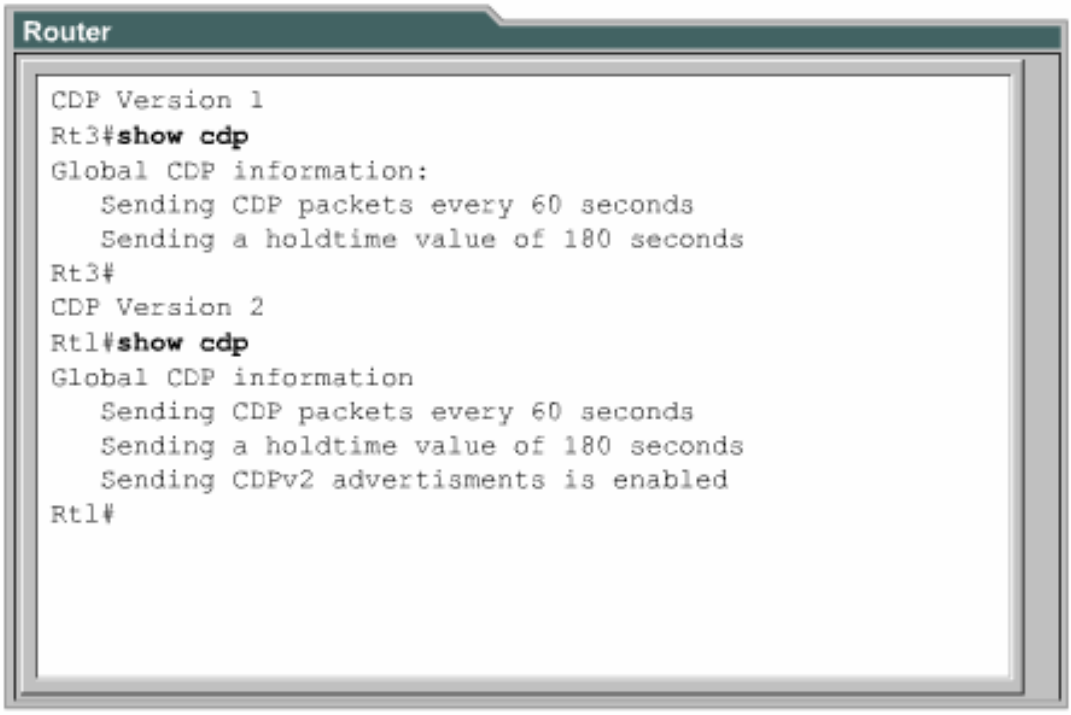
Lệnh	**Chế độ cấu hình của router để thực hiện câu lệnh**	**Chức năng của câu lệnh**
Cdp run	Chế độ cấu hình toàn cục	Khởi động cdp trên router.
Cdp enable	Chệ độ cấu hình cổng giao tiếp.	Khởi động CDP trên cổng giao tiếp tương ứng
Clear cdp counters	Chế độ EXEC người dùng	Xoá đòng hồ đếm lưu lượng trở về 0
Show cdp entry (&/device-name [*][protocol/version])	Chế độ EXEC đặc quyền	Hiển thị thông tin về một thiết bị láng giềng mà ta cân. Thông tin hiển thị có thể được giới hạn thoe giao thức hay theo phiên bản.
Show cdp	Chế độ EXEC đặc quyền	Hiển thị khoảng thời gian giữa các lần phát thông

		điệp quảng cáo CDP, số phiên bản và thời gian còn hiệu lực của các thông điệp này trên từng cổng của router.
Show cdp interface [type number]	Chế độ EXEC đặc quyền	Hiển thị thông tin về những cổng có chạy CDP
Show cdp neighbors [type number] [detial]	Chế độ EXEC đặc quyền	Hiển thị các thông tin về những thiết bị mà CDP phát hiện được: loại thiết bị, tên thiết bị, thiết bị đó kết nối vào cổng nào trên thiết bị của chúng ta. Nếu bạn có sử dụng từ khoá detail thị ban sẽ có thêm thông tin về VLAN ID, chế độ hoạt động song công, tên miền VTP.

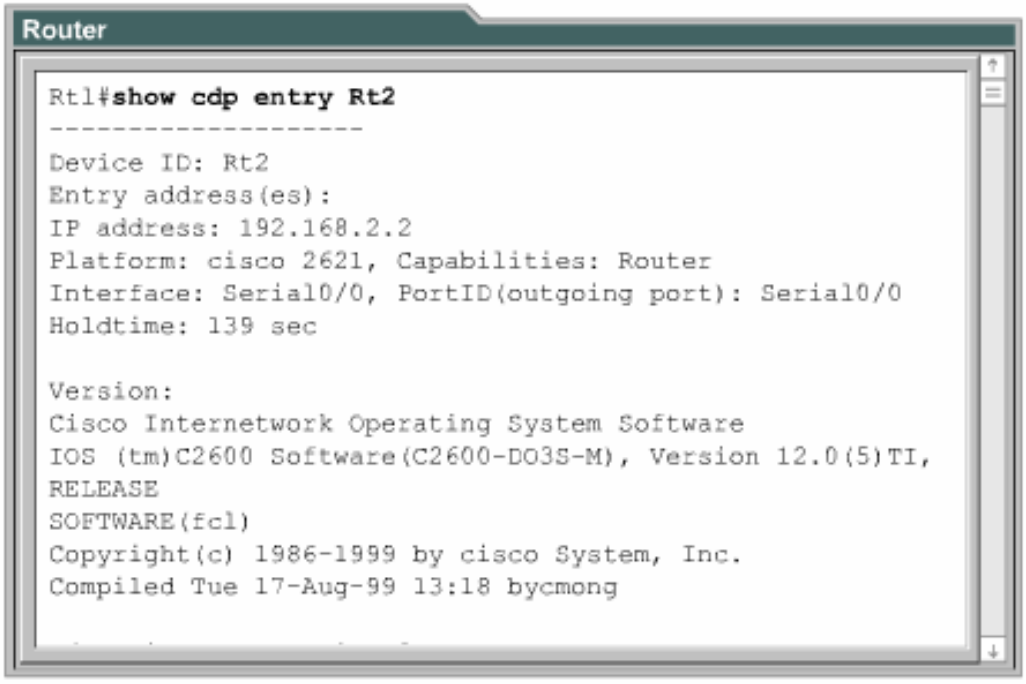
Router

```
Rtl#show cdp traffic
CDP counters:
     Total packets output: 6, Input:6
     Hdrsyntax: 0, Chksum error: 0, Encaps failed:0
     No memory: 0, Invalid packet: 0, Fragmented:0
     CDP version1 advertisements output: 0, Input:0
     CDP version2 advertisements output: 6, Input:6
Rtl#clear cdp counters
Rtl#show cdp traffic
CDP counters:
     Total packets output: 0, Input:0
     Hdrsyntax: 0, Chksum error: 0, Encaps failed:0
     No memory: 0, Invalid packet: 0, Fragmented:0
     CDP version1 advertisements output: 0, Input:0
     CDP version2 advertisements output: 0, Input:0
Rtl#
```

Hình 4.1.3a



Hình 4.1.3b



Hình 4.1.3c

Router

```
Rtl#show cdp interface serial0/0
Serial0/0 is up, line protocol is up
   Encapsulation HDLC
   Sending CDP packets every 60 seconds
   Holdtime is 180 seconds

Rtl#show cdp interface fastethernet0/0
FastEthernet0/0 is up, line protocol is up
   Encapsulation ARPA
   Sending CDP packets every 60 seconds
   Holdtime is 180 seconds
Rtl#
```

Hình 4.1.3d

Router

```
Rt2#show cdp neighbors
Capability Codes: R-Router, T-Trans Bridge, B-Source
Route Bridge, S-Switch, H-Host, I-IGMP, r-Repeater

DeviceID Local Intrfce Holdtme Capablty Platform  Port ID
Rt3      Ser0/1        152     R        2500      Ser1
Rtl      Ser0/0        121     R        2620      Ser0/0
Rt2#
```

Hình 4.1.3e

4.1.4. Xây dựng bản đồ mạng

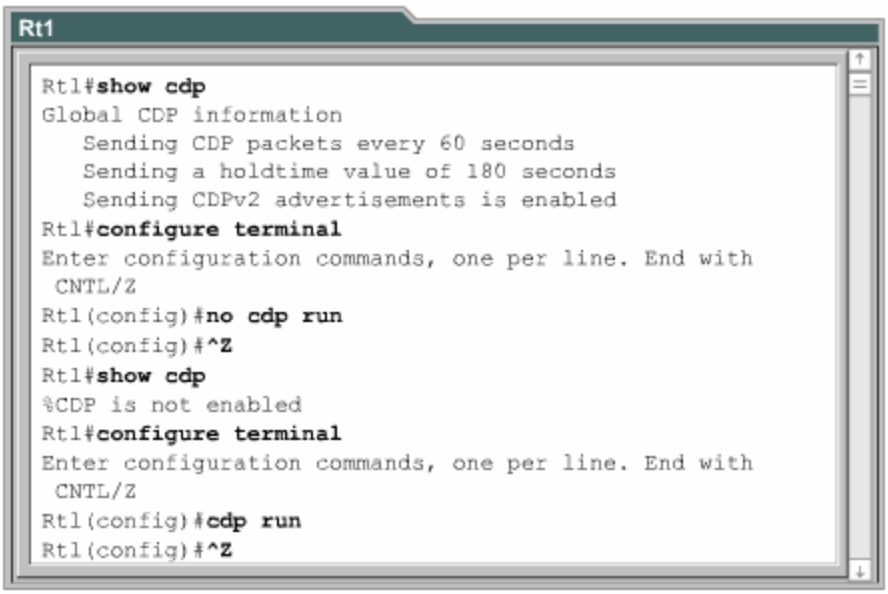
CDP là một giao thức được thiết kế và hoạt động khá nhẹ, đơn giản. Các gói CDP có kích thước nhỏ nhưng lại mang nhiều thông tin hữu ích về các thiết bị láng giềng Cisco.

Bạn có thể sử dụng các thông tin này để xây dựng sơ đồ mạng của các thiết bị. Bạn có thể Telnet vào các thiết bị láng giềng rồi dùng lệnh **show cdp neighbors** để tìm tiếp các thiết bị khác kết nối vào thiết bị này.

4.1.5. Tắt CDP

Để tắt toàn bộ CDP trên router, bạn dùng lệnh **no cdp run** chế độ cấu hình toàn cục. Khi bạn đã tắt toàn bộ CDP thì không có cổng nào trên router còn chạy được.

Đối với Cisco IOS phiên bản 10.3 trở đi, CDP chạy mặc định trên tất cả các cổng có thể gửi và nhận thông tin CDP. Tuy nhiên cũng có một số cổng như cổng Asynchronous chẳng hạn thì mặc định là CDP tắt trên các cổng này. Nếu CDP đang bị tắt trên một cổng nào đó thì bạn có thể khởi động lại CDP bằng lệnh **cdp enable** trong chế độ cấu hình cổng giao tiếp tương ứng. Còn nếu bạn muốn tắt CDP trên một cổng nào đó thì bạn dùng lệnh **no cdp enable** trong chế độ cấu hình cổng đó.



Hình 4.1.5

4.1.6. Xử lý sự cố của CDP

Lệnh	Mô tả
Clear cdp table	Xoá bảng thông tin của CDP về các thiết bị láng giềng
Clear cdp counters	Xoá bộ đếm lưu lượng trở về 0.
Show cdp traffic	Hiển thị bộ đếm của CDP, bao gồm số lượng gói CDP gửi và nhận, số lượng lỗi checksum
Show debugging	Hiển thị thông tin về các loại debug đang chạy trên router
Debug cdp adjacency	Kiểm tra thông tin CDP về các thiết bị láng giềng
Debug cdp events	Kiểm tra các hoạt động của CDP
Debug cdp ip	Kiểm tra thông tin CDP IP
Debug cdp packets	Kiểm tra thông tin về các gói CDP
Cdp timer	Cài đặt thời gian định kỳ gửi gói CDP cập nhật
Cdp holdtime	Cài đặt thời gian lưu giữ thông tin cho các gói CDP cập nhật được phát đi
Show cdp	Hiển thị thông tin toàn cục của CDP, bao gồm thời gian điịnh cập nhật và thời gian lưu giữ thông tin

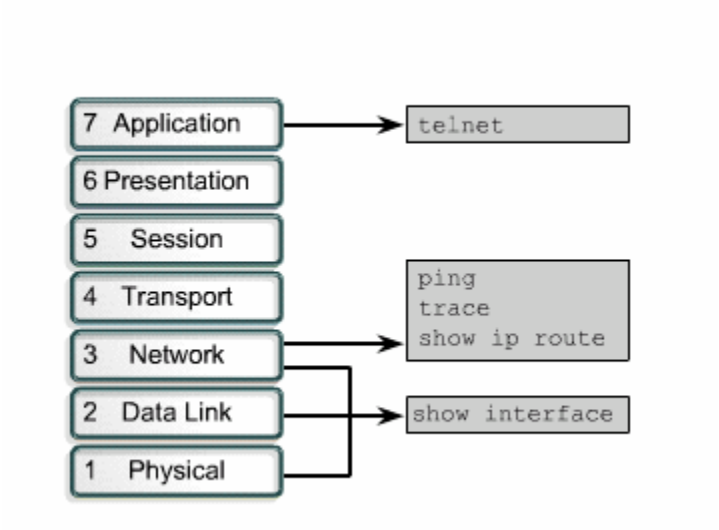
4.2.Thu thập thông tin về các thiết bị ở xa

4.2.1. Telnet

Telnet là giao thức giả lập đầu cuối ảo nằm trong bộ giao thức TCP/IP. Nó cho phép thiết lập kết nối từ xa vào thiết bị. Lệnh Telnet được sử dụng để kiểm tra hoạt động phần mềm ở lớp ứng dụng giữa 2 máy.

Telnet hoạt động ở lớp ứng dụng của mô hình OSI. Telnet hoạt động dựa trên cơ chế TCP để đảm bảo việc truyền dữ liệu giữa client và các server.

Một router có thể cho phép thực hiện đồng thời nhiều phiên kết nối Telnet. Đường vty 0-4 trên router là đường dành cho Telnet. 5 đường Telnet này có thể thực hiện cùng lúc. Chúng ta cần lưu ý rằng việc sử dụng Telnet để kiểm tra kết nối lớp ứng dụng chỉ là việc phụ. Telnet được sử dụng chủ yếu để thiết lập kết nối từ xa vào thiết bị. Telnet là một chương trình ứng dụng đơn giản và thông dụng nhất.



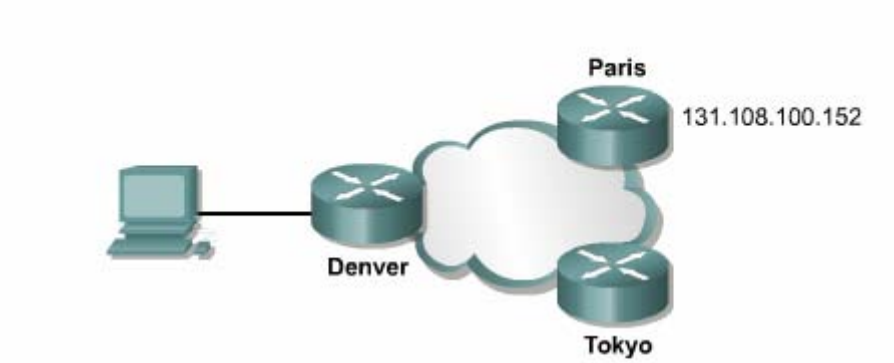
Hình 4.21.

4.2.2. Thiết lập và kiểm tra kết nối Telnet

Lệnh Telnet cho phép người dùng thực hiện Telnet từ một thiết bị Cisco này sang thiết bị khác. Chúng ta không cần phải nhập lệnh **connect** hay **telnet** để thiết lập kết nối Telnet mà chúng ta có thể nhập tên hoặc địa chỉ IP của router mà chúng ta muốn Telnet vào. Khi kết thúc phiên Telnet, bạn dùng lệnh **exit** hoặc **logout**.

Để thiết lập kết nối Telnet, bạn dùng một trong các lệnh sau:

Denver>**connect paris**
Denver>**paris**
Denver>**131.108.100.152**
Denver>**telnet paris**



Initiate a session:

```
Denver>telnet paris
```

Exit a session:

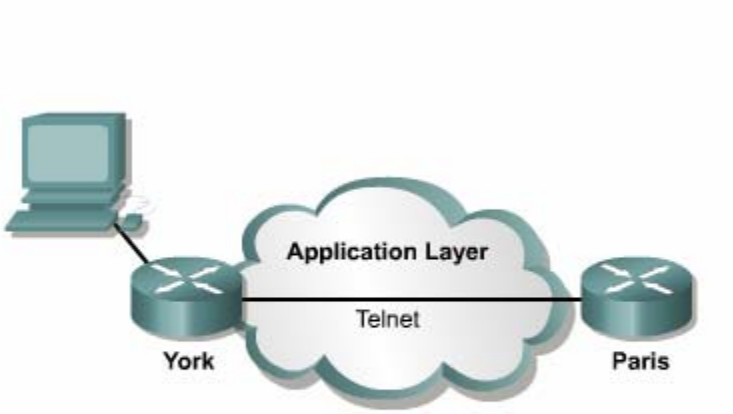
```
Paris>exit
```

Hình 4.2.2a

Router cần phải có bảng host hoặc là trong mạng phải có dịch vụ DNS phân giải tên máy mà chúng ta nhập vào. Nếu không thì bắt buộc bạn phải dùng địa chỉ IP.

Telnet được sử dụng để kiểm tra xem bạn có thể kết nối từ xa vào một router hay không. Ví dụ như hình 4.2.2b: nếu bạn Telnet ở chế độ EXEC người dùng và EXEC đặc quyền đều được.

Nếu bạn có thể truy cập từ xa vào router thi có nghĩa là đã có ít nhất một ứng dụng TCP/IP kết nối vào được router đó. Một kết nối Telnet thành công chứng tỏ rằng các ứng dụng lớp trên hoạt động tốt.



Hình 4.2.2b

Nếu bạn có thể Telnet vào một router này mà không Telnet vào được router khác thì có thể sự cố là do sai tên, địa chỉ hoặc do cấp quyền truy cập. Sai sót có thể nằm ở router mà bạn đang xủ lý hoặc nằm ở router mà bạn Telnet tới. Trong trường hợp này, bước tiếp theo bạn nên cố gắng **ping** thử. Lệnh **ping** cho phép chúng ta kiểm tra kết nối ở lớp Mạng từ đầu đến cuối.

Khi bạn đã Telnet xong, bạn có thể ngắt kết nối. Mặc định thì sau 10 phút mà không có bất kỳ hoạt động nào kết nối Telnet sẽ tự động ngắt. Hoặc là bạn có thể ngắt kết nối Telnet bằng lệnh **exit**.

4.2.3. Ngắt, tạm ngưng phiên Telnet

Telnet có một đặc tính quan trọng là bạn có thể tạm ngưng một phiên Telnet. Tuy nhiên có một rắc rối là khi bạn sử dụng phím **enter** sau khi tạm ngưng phiên Telnet thì phần mềm Cisco IOS sẽ tự động quay trở lại kết nối Telnet vừa mới tạm ngưng trước đó. Mà phím **enter** là phím rất hay được sử dụng. Do đó khi bạn tạm ngưng một phiên Telnet thì rất có thể sau đó bạn sẽ kết nối lại vào một router khác. Điều này rất nguy hiểm khi bạn thực hiện thay đổi cấu hình router. Do đó bạn cần chú ý cẩn thận cấu hình của router trước khi tạm ngưng phiên Telnet trên router đó.

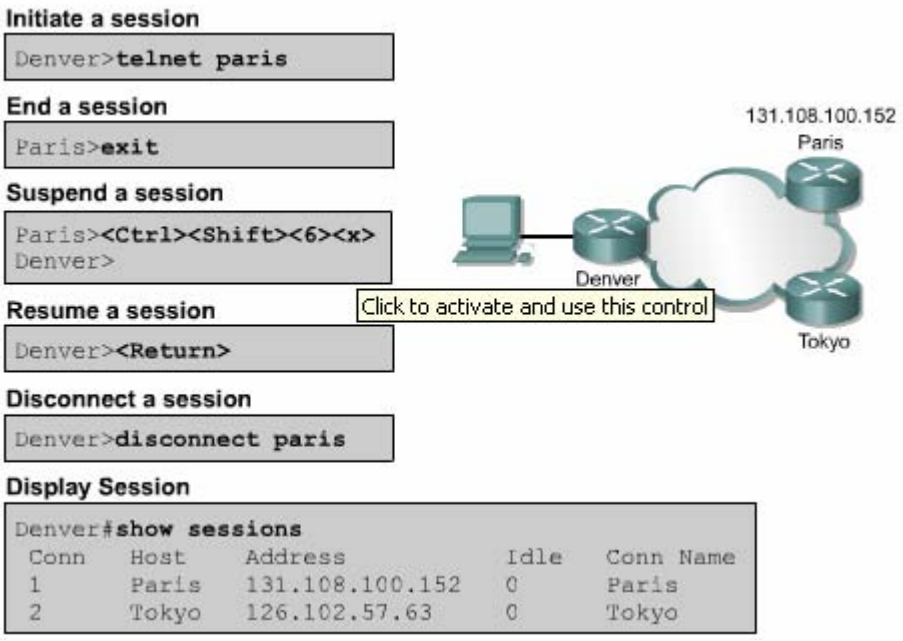
Mỗi một phiên Telnet chỉ được tạm ngưng trong một khoảng thời gian giới hạn. Để quay trở lại kết nối Telnet mà bạn đã tạm ngưng bạn chỉ cần nhấn phím Enter. Bạn dùng lệnh **show session** để xem các kết nối Telnet đang được mở.

Sau đây là trình tự các bước để bạn ngắt kết nối Telnet:

- Nhập lệnh **disconnect**.
- Tiếp theo sau lệnh này là tên hoặc địa chỉ IP của router. Ví dụ: Denver>**disconnect paris**

Sau đây là các bước thực hiện tạm ngưng phiên Telnet:

- Nhấn tổ hợp phím **Ctrl-Shift-6** cùng lúc, buông ra rồi nhấn tiếp chữ x.
- Nhập tên hoặc địa chỉ IP của router.



Hình 4.2.3

4.2.4. Mở rộng thêm về hoạt động Telnet

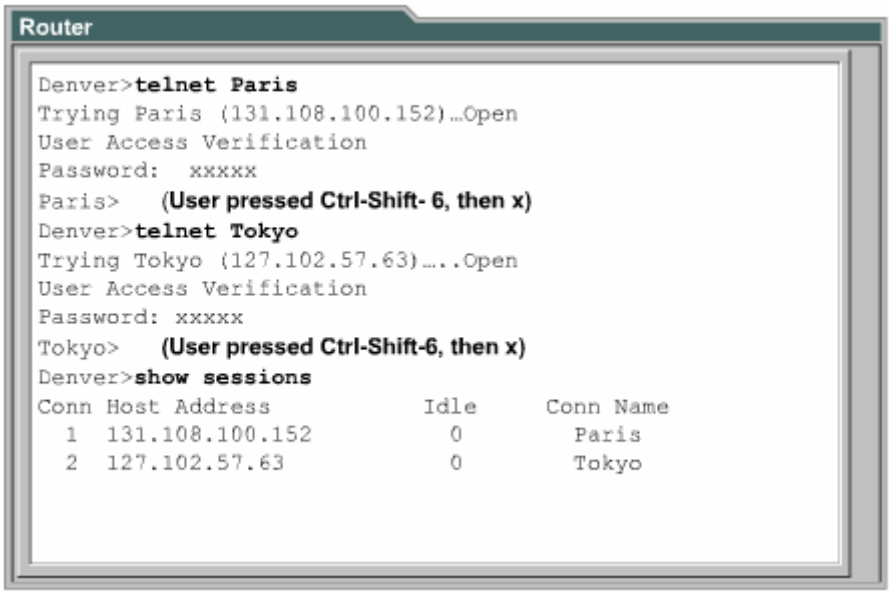
Trên router có thể mở nhiều phiên Telnet cùng lúc. Chúng ta có thể chuyển đổi qua lại giữa các phiên Telnet này. Bạn có thể ấn định số lượng phiên Telnet được phép mở đồng thời trên router bằng lệnh **session limit**.

Để chuyển đổi qua lại giữa các phiên Telnet, bạn tạm ngưng phiên Telnet hiện tại và quay trở lại phiên mới mở trước đó.

Nhấn tổ hợp phím **Ctrl-Shift-6** cùng lúc, buông ra rồi nhấn tiếp chữ x: tạm thoát khỏi kết nối hiện tại, quay lại dấu nhắc EXEC.

Tại dấu nhắc EXEC, bạn có thể thiết lập phiên kết nối mới. Router 2500 chỉ cho phép mở 5 phiên Telnet cùng lúc.

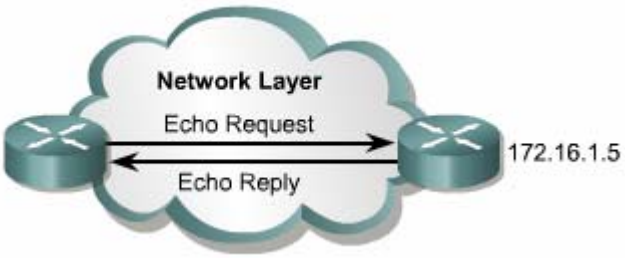
Bạn có thể mở nhiều phiên Telnet cùng lúc và tạm ngưng bằng tổ hợp phím **Ctrl-Shift-6**, **x**. Nếu bạn dùng phím Enter thì Cisco IOS sẽ tự động quay lại kết nối vừa mới tạm ngưng trước đó. Còn nếu bạn dùng lệnh **resume** thì bạn phải nhập thêm chỉ số ID bằng lệnh **show session**.



Hình 4.2.4

4.2.5. Các lệnh kiểm tra kết nối khác

Để hỗ trợ việc kiểm tra nối mạng cơ bản, nhiều giao thức mạng có hỗ trợ giao thức phản hồi (echo). Giao thức phản hồi được sử dụng để kiểm tra việc định tuyến các gói dữ liệu. Lệnh ping thực hiện gửi đi một gói dữ liệu tới máy đích và chờ nhận gói trả lời vè từ máy đích. Kết quả của giao thức phản hồi giúp bạn xác định độ tin cậy của đường truyền tới máy đích, thời gian trễ trên đường truyền, máy đích có đến được hay không, có hoạt động hay không. Lệnh ping là lệnh cơ bản để kiểm tra kết nối. Bạn có thể dùng lệnh này ở chế độ EXEC người dùng hày EXEC đặc quyền đều được.



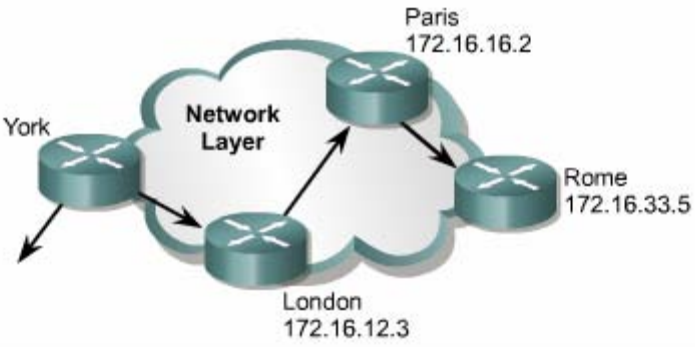

```
Router>ping 172.16.1.5
Type escape sequence to abort.
Sending 5, 100 byte ICMP Echos to 172.16.1.5,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent,
round-trip min/avg/max = 1/3/4 ms
Router>
```

Hình 4.2.5a

Hình 4.2.5a là ví dụ cho biết phản hồi hành công cho 5 gói gửi đi của lệnh ping 172.16.1.5. Dấu chấm than (!) cho biết là phản hồi thành công. Nếu bạn nhận được một hay nhiều dấu chấm thay vì dấu chấm than (!) thì điều đó có nghĩa là router đã hết thời gian chờ gói phản hồi từ máy đích. Lệnh ping sử dụng giao thức ICMP (Internet Control Message Protocol – giao thức thông điệp điều khiển internet).

Lệnh **traceroute** là một công cụ lý tưởng để bạn tìm đường đi của gói dữ liệu trên mạng. Lệnh **traceroute** cũng tương tự như lệnh **ping,** chỉ khác là lệnh ping thì chỉ kiểm tra kết nối từ đầu cuối đến đầu cuối, còn lệnh **traceroute** thì kiểm tra từng chặng một dọc theo đường truyền. Bạn có thể thực hiện lệnh **traceroute** ở chế độ EXEC người dùng hay EXEC đặc quyền đều được.

Trong ví dụ ở hình 4.2.5b, bạn thực hiện lệnh **traceroute** từ router York đến router Rome. Đường truyền này phải đi qua router London và Paris. Nếu có router nào không đến được thì kết quả phản hồi là dấu sao (*) thay vì tên của router đó. Trong trường hợp như vậy, lệnh **traceroute** vẫn sẽ tiếp tục cố gắng gửi đến trạm kế tiếp cho đến khi bạn nhấn tổ hợp phím Ctrl-shift-6.




```
York#traceroute ROME
Type escape to abort.
Tracing the route to Rome (172.16.33.5)
  1 LONDON (172.16.12.3) 8 msec 8 msec 4 msec
  2 PARIS (172.16.16.2) 8 msec 8msec 8msec
  3 ROME (172.16.33.5) 8msec 8msec 4msec

York#
```

Hình 4.2.5b

Việc kiểm tra cơ bản cũng tập trung chủ yếu vào lớp Mạng. Bạn dùng lệnh **show ip route** để kiểm tra bảng định tuyến của router cho hệ thống mạng. Lệnh này sẽ được đề cập chi tiết hơn trong chương sau.

Sau đây là các bước thực hiện **ping**:

- Nhập lệnh ping, theo sau là địa chỉ IP hoặc tên của máy đích.
- Nhấn phím Enter.

Sau đây là các bước thực hiện lệnh **traceroute**:

- Nhập lệnh **traceroute**, theo sau là địa chỉ IP hoặc tên của máy đích.
- Nhấn phím Enter.

4.2.6. Xử lý sự cố về địa chỉ IP

Sự cố về địa chỉ là sự cố xảy ra phổ biến nhất trong mạng IP. Sau đây là 3 lệnh thường được sử dụng để xử lý các sự cố liên quan đến địa chỉ:

- **Ping:** sử dụng giao thức ICMP để kiểm tra kết nối vật lý và địa chỉ IP của lớp Mạng. Đây là lệnh kiểm tra cơ bản.

- **Telnet:** kiểm tra kết nối phần mềm lớp Ứng dụng giữa nguồn và máy đích. Đây là lệnh kiểm tra kết nối hoàn chỉnh.
- **Traceroute:** cho phép xác định vị trí lỗi trên đường truyền từ máy nguồn đến máy đích. Lệnh trace sử dụng giá trị Time to Live để tạo thông điệp từ mỗi router trên đường truyền.

TỔNG KẾT

Kết thúc chương này bạn cần nắm được những ý chính như sau:

- Mở và tắt CDP
- Sử dụng lệnh **show cdp neighbors**.
- Xác định được các thiết bị láng giềng kết nối vào các cổng trên thiết bị của mình.
- Thu nhập thông tin về các thiết bị láng giềng bằng cách sử dụng CDP.
- Thiết lập kết nối Telnet.
- Kết thúc kết nối Telnet.
- Tạm ngưng kết nối Telnet.
- Thực hiện kiểm tra kết nối.
- Xử lý sự cố của kết nối đầu cuối từ xa.

CHƯƠNG 5

QUẢN LÝ PHẦN MỀM CISCO IOS

GIỚI THIỆU

Cisco router không thể hoạt động được nếu không có hệ điều hành mạng Cisco (IOS). Mỗi router trong quá trình khởi động đều có bước tìm và tải IOS. Chương này sẽ mô tả chi tiết các bước khởi động của router và cho bạn thấy tầm quan trọng của quá trình này.

Các thiết bị mạng Cisco hoạt động với nhiều loại tập tin khác nhau, trong đó có hệ điều hành và tập tin cấu hình. Người quản trị mạng hay bất kỳ ai muốn quản trị cho hệ thống mạng hoạt động trôi chảy và tin cậy thì để phải bảo trì các tập tin này cẩn thận, bảo đảm rằng thiết bị đang chạy đúng phiên bản phần mềm và các tập tin hệ thống của Cisco và các công cụ hữu dụng để quản lý các tập tin này.

Khi hoàn tất chương này , các bạn có thể thực hiện được những việc sau:

- Xác định được router đang ở giai đoạn nào của quá trình khởi động.
- Xác định được các thiết bị Cisco tìm và tải Cisco IOS như thế nào.
- Sử dụng các lệnh **boot system**.
- Xác định giá trị của thanh ghi cấu hình.
- Mô tả khái quát các tập tin mà Cisco IOS sử dụng và chức năng tương ứng của chúng.
- Nắm được nơi mà router lưu các loại tập tin khác nhau.
- Mô tả khái quát cấu trúc tên của IOS.
- Lưu và khôi phục tập tin cấu hình bằng cách sử dụng TFTP và cắt – dán.
- Tải IOS bằng TFTP.
- Tải IOS bằng Xmodem.
- Kiểm tra tập tin hệ thống bằng các lệnh show.

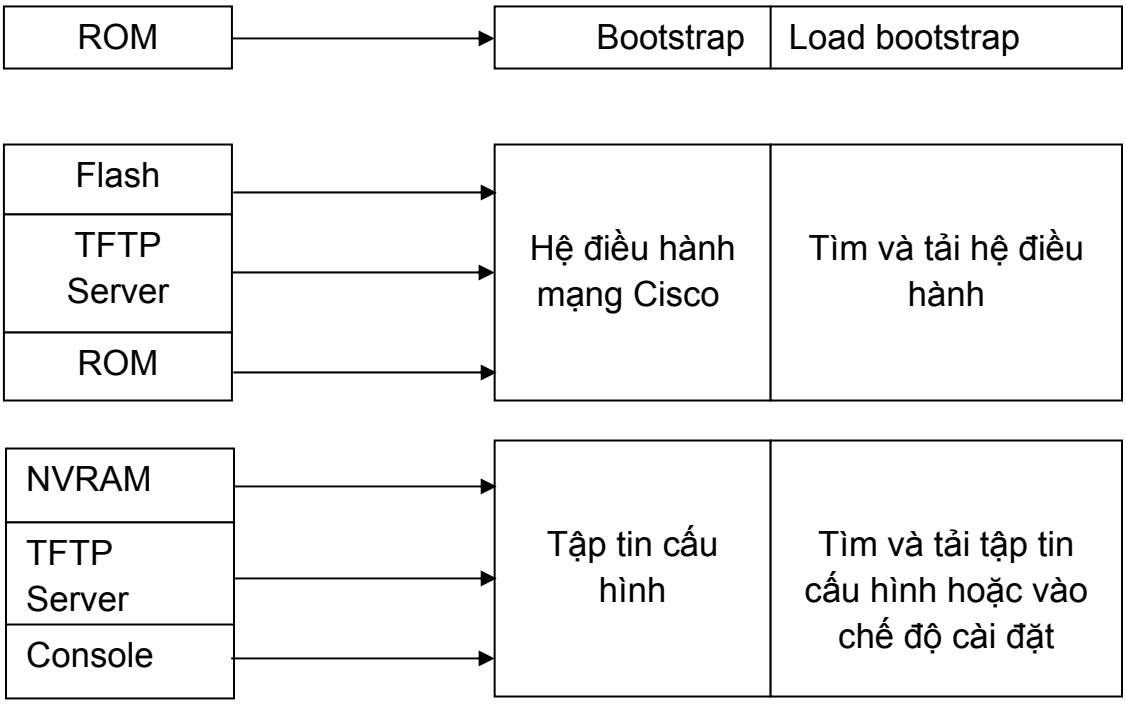
5.1. Khảo sát và kiểm tra quá trình khởi động router

5.1.1. Các giai đoạn khởi động router khi bắt đầu bật điện

Mục tiêu chính của quá trình khởi động router là khởi động các hoạt động của router. Router phải hoạt động với độ tin cậy cao để thực hiện kết nối cho bất kỳ

loại mạng nào. Do đó, quá trình khởi động router phải thực hiện các công việc như sau:

- Kiểm tra phần cứng của router
- Tìm và tải phần mềm Cisco IOS.
- Tìm và thực hiện các câu lệnh cấu hình, trong đó bao gồm các cấu hình giao thức và địa chỉ cho các cổng giao tiếp.



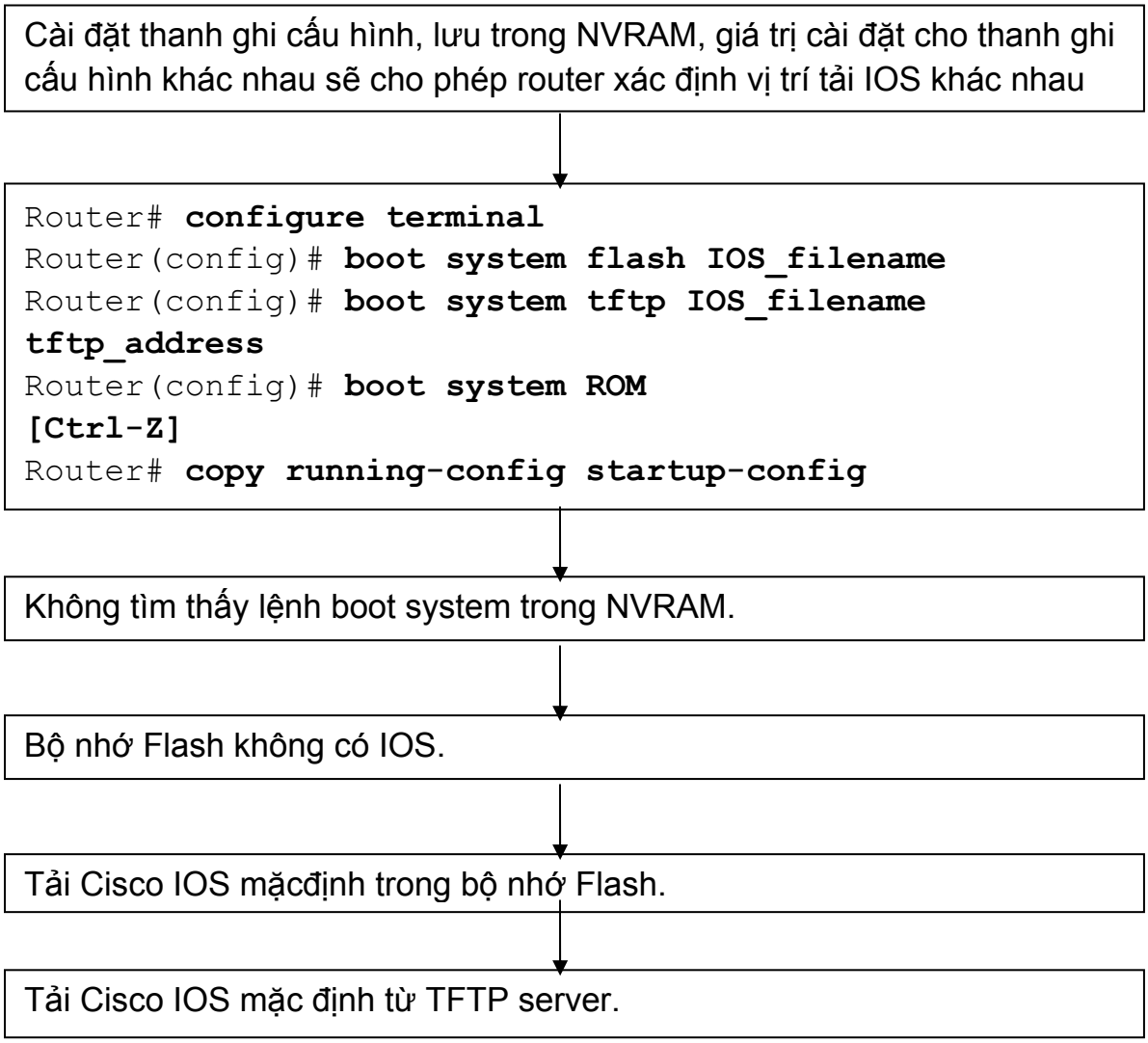
5.1.2. Thiết bị Cisco tìm và tải như thế nào

Nguồn mặc định tải phần mềm Cisco IOS thì khác nhau tuỳ theo phiên bản phần cứng của thiết bị, nhưng hầu hết các router đều tìm lệnh **boot system** lưu trong NVRAM. Phần mềm Cisco IOS có thế được tải từ nhiều nguồn khác nhau. Những nguồn này chúng ta có thể cấu hình hoặc router sẽ sử dụng quá trình tìm và tải phần mềm mặc định của nó.

Giá trị cài đặt cho thanh ghi cấu hình sẽ cho phép router tìm IOS như sau:

- Lệnh **boot system** cấu hình cho router nơi mà router tìm để tỉa IOS. Router sẽ sử dụng các câu lệnh này theo thứ tự khi khởi động.

- Nếu trong NVRAM không có các câu lệnh **boot system** thì hệ thống sẽ mặc định là sử dụng Cisco IOS trong bộ nhớ flash.
- Nếu trong bộ nhớ flash cũng không có IOS thì router sẽ cố gắng sử dụng TFTP để tải IOS về. Router sẽ sử dụng giá trị cài đặt cấu hình để biết tên tập tin lưu trên server mạng.



5.1.3 Sử dụng lệnh boot system

5.1.4 *Hình 5.1.3*Sử dụng lệnh boot system

Thứ tự các vị trí mà router tìm hệ điều hành được cài đặt trong phần khởi động của thanh ghi cấu hình. Giá trị mặc định của thanh ghi cấu hình có thể thay đổi bằng lệnh **config-register** trong chế độ cấu hình toàn cục. Thông số của lệnh này sủ đụng số hex.

Thanh ghi cấu hình là thanh ghi 16 bi lưu trong NVRAM. 4 bit thấp của thanh ghi cấu hình thể hiện cho phần khởi động router. Đầu tiên, ta dùng lệnh **show version** để xem giá trị hiện tại của thanh ghi cấu hình và cúng để đảm bảo là giá trị của 12 trên không có gì thay đổi. Sau đó ta dùng lệnh **cònig-register** để thay đổi giá trị cho thanh ghi, ta chỉ cần đổi giá trị của số hex cuối cùng mà thôi.

Ta thay đổi giá trị phần khởi động của thanh ghi cấu hình theo hướng dẫn sau:

- Để router khởi động vào chế độ ROM monitor, ta đặt giá trị cho thanh ghi cấu hình là 0xnnn0, trong đó nnn là giá trị của 12 bit trên, không thuộc phần khởi động. Còn 0 là gia trj của phần khởi động trên thanh ghi cấu hình, do đó 4 bit phần này có giá trị nhị phân là 0000. Từ chế độ ROM monitor, ta có thể khởi động hệ thống bằng lệnh **b.**
- Để cấu hình cho hệ thống tự động khởi động từ ROM, ta đặt giá trị cho thanh ghi cấu hình là 0xnnn1, trong đó nnn là giá trị của 12 bit trên, không thuộc phần khởi động. Còn 1 là giá trị của 4 bit phần khởi động trên thanh ghi cấu hình, như vậy 4 bit này có giá trị nhị phân là 0001.
- Để cấu hình cho hệ thống sử dụng cac câu lệnh **boot system** trong NVRAM, ta đặt giá trị cho thanh ghi cấu hìnn bất kỳ giá trị nào nằm trong khỏng 0xnnn2 – 0xnnnF. Khi đó, 4 bit trong phần khởi động của thanh ghi cấu hình sẽ có giá trị nhị phân là 0010-1111. Mặc định gia trị thanh ghi là 0x2102 và router sử dụng lệnh **boot system** trong NVRAM.

5.1.5 Sử dụng lệnh boot system

Khi router không khởi động được thì có thể là do một trong những nguyên nhân sau:

- Mất tập tin cấu hình hoặc câu lệnh **boot system** bị sai.
- Giá trị thanh ghi cấu hình bị sai.
- Bộ nhớ flash bị trục trặc.
- Hư hỏng phần cứng.

Khi router khởi động, router sẽ tìm câu lệnh **boot system** trong tập tin cấu hình. Lệnh **boot system** có thể cài đặt cho router khởi động từ IOS khác thay vì từ IOS trong flash. Để xác định xem router khởi động từ IOS nào, bạn dùng lệnh **show version** và tìm dòng nói về phần mềm khởi động hệ thống.

Sử dụng lệnh **show running-config** và tìm câu lệnh **boot system** nằm ở ngay phần đầu của tập tin cấu hình. Nếu câu lệnh **boot system** chỉ sai IOS thì chúng ta xoá lệnh đó đi bằng lệnh "no" của câu lệnh đó.

```
Router#show version
Cisco Interface Operating System Software
IOS (tm) C2600 Software (C2600-JK803S-M), Version 12.2 (17a), RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco  System, Inc
Complie Thu 19-Jun-03 16:35 by pwade
Image text-base: 0x8000808C, data-base: 0x815F7B34

ROM: System Bootstrap, Version 12.2 (7r) [cmong 7r], RELEASE SOFTWARE
fc1)

Danang uptime is 1 hour, 2 minutes
System returned to ROM by power-on
System image file is "flash:c2600-jk8o3s-mz.122-17a.bin"

This product contains cryptographic features and subject to United States and local
country laws goverining import, export, transfer and use. Delivery of Cisco
cryptographic product does not imply third-party authority to import, export,
distribute or use encryption. Importers, exporters, distributors and users are
responsible for compliance with US and local coutry laus. By using this product,
you compliance with US and local laws, return this product immediately.

A summary of US laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
```

If you require further assistance please contact us by sending email to export@cisco.com

Cisco 2620XM (MOC860P) professor (revision 0x100) with 59392K/6144K bytes of memory
Processor board ID JAE0718065A (41148118384)
M860 processor: part number 5, mask 2
Bridging software
X25 software, Version 3.0.0
Super LAT software (copyright 1990 by Meridian Technology Corp)
TN3270 Emulation software
Basic Rae ISDN software, Version 1.1.
1 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial (sync/async) network interface(s)
1 ISDN Basic Rate interface(s)
32K bytes of non-voltatile configuration memory.
16384K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102

Giá trị thanh ghi cấu hình không đúng cũng dẫn đến việc router không tải được IOS vì gia trị thanh ghi này sẽ cho router biết là tải IOS từ đâu. Chúng ta kiểm tra giá trị thanh ghi bằng lệnh **show version** và đọc dòng cuối cùng trong kết quả hiển thị của lệnh này. Giá trị thanh ghi cấu hình sẽ khác nhau đối với các biên bản phần cứng khác nhau. Bạn có thể tham khảo giá trị thanh ghi cấu hình trên đĩa CD tài liệu của Cisco hợc trên website của Cisco. Sau đó bạn chỉnh sửa lại giá trị thanh ghi cấu hình rồi lưu vào tập tin cấu hình khởi động.

Nếu sự cố vẫn tiếp tục xảy ra thì có thể là tập tin trong bộ nhớ flash bị lỗi. Thông thường, trong trường hợp như vậy bạn sẽ gặp các thông báo lỗi trong qua trình khởi động router. Ví dụ như một số câu thông báo như sau:

- Open: read error…requested 0x4 bytes, got 0x0
- Trouble reading device magic number
- Boot: cannot open “flash:”
- Boot: cannot determine first file name on device “flash:”

Nếu dùng là tập tin trong flash bị lỗi thì bạn cần chép lại IOS mới lên router.

Nếu tất cả các nguyên nhân trên vẫn không đúng thì có thể là router bị lỗi phần cứng. Trong trường hợp như vậy thì bạn nên liên hệ với trung tâm hỗ trợ kỹ thuật của Cisco (TAC – Terminal Assistance Centre). Mặc dù lỗi hư phần cứng rất hiếm gặp nhưng nó vẫn có khả năng xảy ra.

Lưu ý: Bạn không thể xem giá trị thanh ghi cấu hình bằng lệnh ***show running-config*** *hay* ***show start-up config*** *được,*

5.2. Quản lý tập tin hệ thống Cisco

5.2.1. Khái quát về tập tin hệ thống Cisco

Hoạt động của router và switch phụ thuộc vào phần mềm cài trên nó. Có 2 loại phần mềm cần phải có để thiết bị hoạt động là: hệ điều hành và tập tin cấu hình.

Hệ điều hành được sử dụng cho hầu hết các thiết bị Cisco là hệ điều hành liên mạng Cisco, gọi tắt là Cisco IOS (Internetwork Operating System). Phần mềm Cisco IOS cho phép thiết bị thực hiện các chức năng của router hay switch. Một tập tin IOS khoảng vài megabyte.

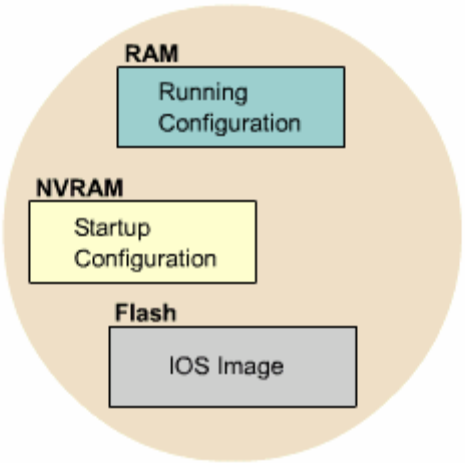
Phần mềm thứ 2 được sử dụng cho router và switch là tập tin cấu hình. Tập tin cấu hình chứa các hướng dẫn về hoạt động định tuyến hay chuyển mạch của thiết bị. Người quản trị mạng là người tạo tập tin cấu hình để các thiết bị Cisco thực hiện các chức năng theo đúng thiết kế của mình. Một số thông số mà bạn có thể cấu hình được là địa chỉ IP của các cổng trên router, giao thức định tuyến và các mạng mà giao thức định tuyến đó được thực hiện quảng bá… Thông thường, một tập tin cấu hình từ vài trăm đến vài ngàn byte.

Mỗi loại phần mềm được lưu thành từng tập tin riêng biệt trong từng bộ nhớ khác nhau.

IOS được lưu trong loại bộ nhớ được gọi là flash. Flash lưu giữ ổn định tập tin IOS và tập tin IOS này được sử dụng để khởi động router. Flash cho phép chúng ta nâng cấp IOS và lưu được nhiều IOS khác nhau. Trong cấu trúc của một số loại router, IOS được copy lên RAM và chạy trên RAM.

Tập tin cấu hình được lưu trong bộ nhớ NVRAM và tập tin này được sử dụng khi khởi động router. Do đó tập tin cấu hình được lưu trong NVRAM được gọi là tập tin cấu hình khởi động. Khi thiết bị khởi động, tập tin cấu hình khởi động được

chép lên RAM. Khi đó tập tin này được chạy trên RAM và luôn được cập nhật khi đang chạy. Do đó tập tin đang chạy trên RAM được gọi là tập tin cấu hình hoạt động.



Hình 5.2.1a

Bắt đầu từ phiên bản 12 của IOS, hệ thống tập tin Cisco IOS, gọi tắt là IFS (IOS File System), cung cấp một giao tiếp chung cho tất cả các hệ thống tập tin mà router đang sử dụng. IFS cung cấp một phương pháp chung để thực hiện quản lý toàn bộ hệ thống tập tin đang sử dụng cho router. Công việc này bao gồm tập tin trong bộ nhớ flash, hệ thống tập tin mạng (TFTP, rcp và FTP), đọc/viết dữ liệu (NVRAM, tập tin cấu hình hoạt động, ROM). IFS sử dụng các tiền tố như trong hình 5.2.1b để xác định hệ thống tập tin trên thiết bị.

Prefix	Descripton
Bootflash:	Bootflash memory
Flash:	Flash memory. This prefix is available on all platform. For platform that do not have a device named flash, the prefix flash: is allased to slot0:. Therefore, the prefix flash: can be used to refer to the main flash memory storage area on all platform
Flh:	Flash load helper log files
ftp:	File Transfer protocol (FTP) network sever
Nvram:	NVRAM
Rcp:	Remote copy protocol (rcp) network server
Slot0:	First Personal Computer Memory Card International Assiciontion

	(PCMCIA) flash memory card
Slot1:	Second PCMCIA flash memory card
System:	Contains the system memory, including the running configuration
Tftp:	TFTP nework server

Hình 5.2.1b

Pre IOS Version 12.0 Commands	IOS Version 12.x Commands
Configure network (pre-Cisco IOs Release 10.3) Copy rcp running –config Copy tftp running-config	Copy ftp: system: runnig-config Copy crp: system: runnig-config Copy tftp: system: runnig-config
Configure overwrite-network {pre-Cisco IOS Release 10.3} Copy rcp stratup-config Copy tftp satrup-config	Copy ftp: system: runnig-config Copy crp: system: runnig-config Copy tftp: system: runnig-config
Show configuration (pre-Cisco IOS release 10.3)	More nvram:startup-config
Write erase (pre-Cisco IOS release 10.3) Erase starup-config	Erase nvram:
Write erase (pre-Cisco IOS release 10.3) Copy running-config startup-config	Copy system: running-config Nvram: startup-config
Write network pre-Cisco IOS release 10.3) Copy running-config startup-config rcp Copy running-config startup-config tftp	Copy system: runnig-config ftp: Copy system: runnig-config crp: Copy system: runnig-config tftp:
Write terminal pre-Cisco IOS release 10.3) Show runnig -config	More system: running-config

Hình 5.2.1c

IFS sử dụng quy ước URL để xác định tập tin trên thiết bị và trên mạng. Quy ước URl xác định vị trí của tập tin đứng sau dâu hai chấm như sau [[[//vị trí]/thư mục]/tên tập tin]. IFS cũng hỗ truyền tải tập tin FTP.

5.2.2. Quy ước tên IOS

Cisco phát triển rất nhiều phiên bản IOS khác nhau. Các phiên bản này hỗ trợ cho các phiên bản phần cứng với nhiều đặc tính khác nhau. Hiện nay Cisco vẫn đang tiếp tục phát triển nhiều phiên bản IOS mới.

Để phân biệt giữa các phiên bản khác nhau, Cisco có một quy luật đặt tên cho IOS. Một tên của IOS bao gồm nhiều phần, mỗi phần thể hiện phiên bản phần cứng, các đặc tính hỗ trợ và sỗ phát hành.

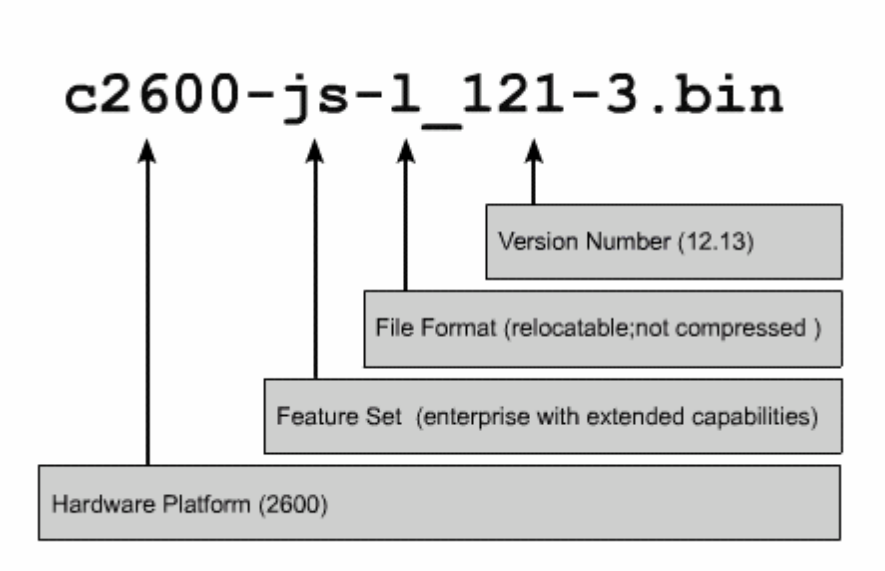
Phần đầu tiên của tập tin IOS cho biết IOS này được thiết kế cho phiên bản phần cứng nào.

Phần thứ hai của tên tập tin IOS cho biết tập tin này có hỗ trợ các đặc tính nào. Có rất nhiều đặc tính khác nhau để chọn lựa. Các đặc tính này được đóng gói trong Cisco IOS. Mỗi Cisco IOS chỉ có một số đặc tính chứ không có toàn bộ tất cả các đặc tính. Bên cạnh đó, các đặc tính này còn được phân loại như sau:

- Cơ bản: các đặc tính dành cho từng phiên bản phần cứng, ví dụ: IP, IP/FW.
- Mở rộng (Plus): là các đặc tính mở rộng hơn mức cơ bản, ví dụ IP Plus, IP/FW Plus, Enterprise Plus.
- Mã hoá: vẫn là các đặc tính cơ bản hay mở rộng như trên nhưng có thêm 56 bit để mã hoá. Ví dụ: IP/ATM PLUS IPSEC 56, Plus 56, Enterprise Plus 56. Từ Cisco IOS phiên bản 12.2 trở đi, đặc tính mã hoá được thiết kế thành 2 loại là k8/k9:
  - K8: 64 bit mã hoa trở xuống.
  - K9: hơn 64 bit mã hoá.

Phần thứ 3 của tên tập tin cho biết định dạng của tập tin đó. Phần này cho biết IOS được lưu trong flash dưới dạng nén hay không, rồi IOS sẽ được giải nén để chạy ở đâu. Nếu IOS lưu trong flash dưới dạng nén thì nó sẽ được giải nén, chép lên RAM trong quá trình khởi động router. Dạng tập tin như vậy gọi là tập tin không cố định. Còn loại tập tin có định thì chạy trực tiếp trên flash luôn mà không cần chép lên RAM.

Phần thứ 4 của tập tin cho biết phiên bản của IOS. Phiên bản càng mới thì số trong phần này càng lớn.



Hình 5.2.2

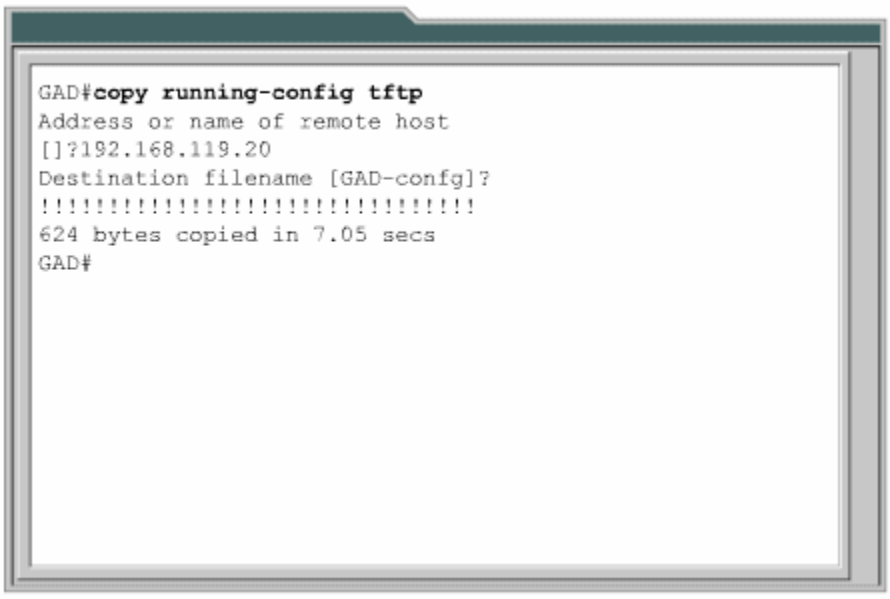
5.2.3. Quản lý tập tin cấu hình băng TFTP

Trên Cisco router và switch, tập tin cấu hình hoạt động được để trên RAM và nơi cấu hình khởi động là NVRAM. Khi bị mất tập tin cấu hình thì ta phải có tập tin cấu hình khởi động dự phòng. Một trong những nơi mà chúng ta có thể lưu dụ phòng tập tin cấu hình là TFTP server. Chúng ta dùng lệnh **copy running-config tftp** để chép tập tin cấu hình lên TFTP server. Sau đây là các bước thực hiện:

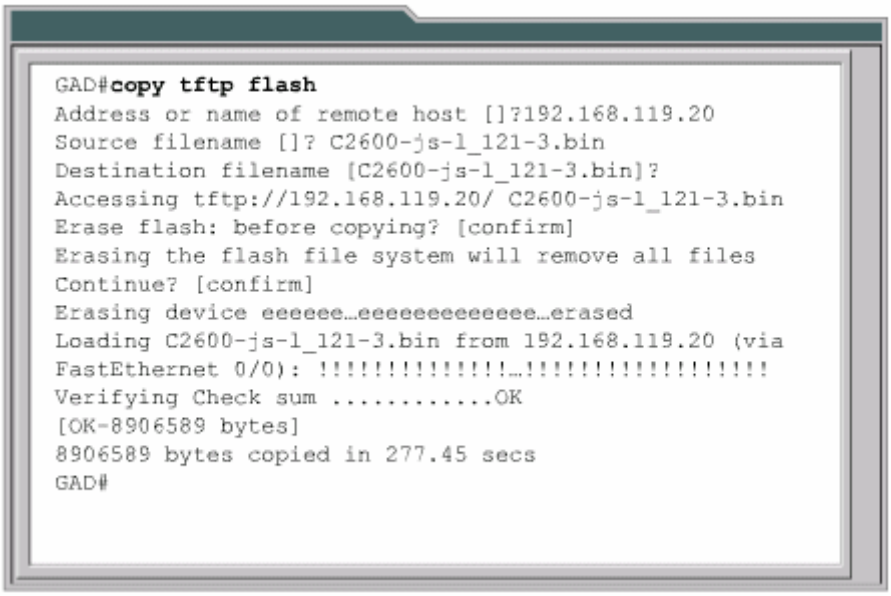
- Nhập lệnh **copy running-config tftp**.
- Ở dấu nhắc kế tiếp, nhập địa chỉ IP của TFTP server mà bạn định lưu tập tin cấu hình.
- Đặt tên cho tập tin hoặc là lấy tên mặc định.
- Xác nhận lại các chọn lựa vừa rồi bằng cách gõ **yes**.

Sau này bạn có thể khôi phục lại cấu hình router bằng cách chép tập tin cấu hình đã lưu dự phòng trên TFTP server về router. Sau đây là các bước thực hiện:

- Nhập lệnh **copy running-config**.
- Ở dấu nhắc kế tiếp, nhập địa chỉ IP của TFTP sever.
- Kế tiếp, nhập tên của tập tin cấu hình mà mình muốn chép.
- Xác nhận lại các chọn lựa rồi.



Hình 5.2.3a



Hình 5.2.3b

5.2.4. Quản lý tập tin cấu hình bằng cách cắt – dán

Một cách khác để tạo tập tin cấu hình dự phòng là chép lại kết quả hiển thị của lệnh **show running-config**. Từ thiết bị đầu cuối kết nối vào router, chúng ta chép lại kết quả hiển thị của lệnh **show running-config** rồi dán vào một tập tin văn bản,

sau đó lưu lại. Tuy nhiên tập tin văn bản này phải chỉnh sửa lại một chút trước khi chúng ta có thể sử dụng nó để khôi phục lại cấu hình router.

Sau đây là các bước thực hiện để bạn chép lại tập tin cấu hình khi bạn sử dụng Hyper Terminal:

1. Chọn **Transfer.**
2. Chọn **Capture Text**.
3. Đặt tên cho tập tin văn bản mà chúng ta sẽ chép tập tin cấu hình ra.
4. Chọn Start để bắt đầu quá trình chép.
5. Chọn hiển thị nội dung của tập tin cấu hình bằng lệnh **show running-config**.
6. Nhấn phím **space bar** mỗi khi có dấu nhắc "--More--" xuất hiện.
7. Sau khi tập tin cấu hình đã hiển thị đầy đủ, bạn kết thúc quá trình chép bằng cách:
8. Chọn **Transfer.**
9. Chọn **Capture**.
10. Chọn **Stop.**

Sau khi quá trình chép hoàn tất, bạn cần xoá bớt một số hang trong tập tin cấu hình để sau này chúng ta có thể sử dụng tập tin văn bản này "dán" lại vào router. Ngoài ra, bạn có thể them một số hang chú thích vào tập tin cấu hình. Các hàng chú thích này được bắt đầu bằng dấu chấm than (!) ở đầu hàng.

Bạn có thể sử dụng Notepad để chỉnh sửa tập tin cấu hình. Bạn ở Notepad, chọn **File>Open**. Chọn tên của tập tin cấu hình mà bạn vừa chép được. Nhấn phím **Open**.

Sau đây là những hàng trong tập tin cấu hình mà bạn cần xoá:

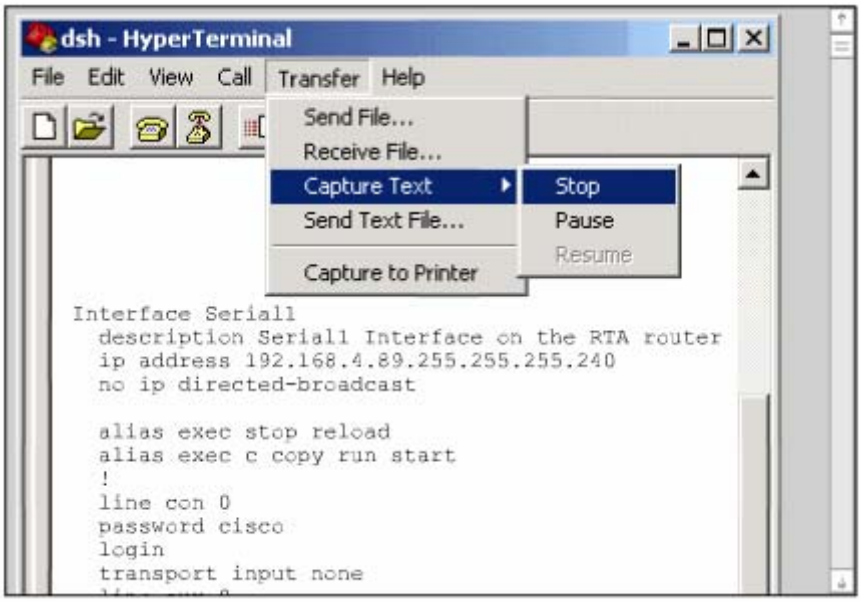
- Show running-config
- Building configuration…
- Current configuration:
- -More-
- Bất kỳ hàng nào ở sau dòng "End"

Bạn them lệnh **no shutdown** vào cuối mỗi phần cấu hình của các cổng giao tiếp. Sau đó chọn **File>Save** để lưu lại tập tin cấu hình.

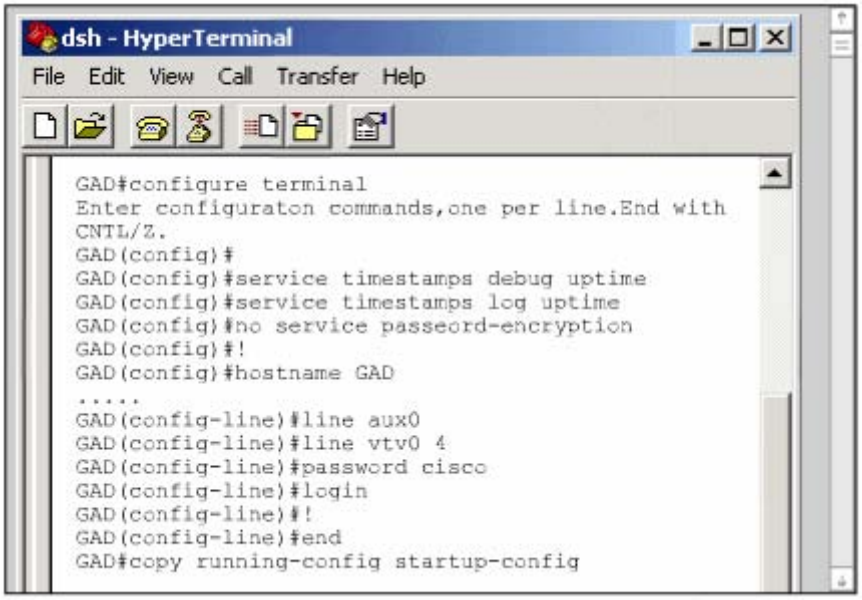
Sau này, từ kết nối bằng HyperTerminal bạn có thể khôi phục lại tập tin cấu hình cho router. Trước tiên, bạn phải xoá hết tập tin cấu hình đang có trong router bằng lệnh **erase startup-config** ở chế độ EXEC đặc quyền. Sau đó khởi động lại router bằng lệnh **reload**.

Sau đây là các bước thực hiện để chép lại tập tin cấu hình cho router từ kết nối HyperTerminal:

- Chuyển vào chế độ cấu hình toàn cục.
- Trên HyperTerminal chọn **Transfer>Send Text File**.
- Chọn tên của tập tin cấu hình mà bạn cần chép lên router.
- Từng dòng trong tập tin cấu hình sẽ được nhập vào y như lúc bạn gõ lệnh đó vậy.
- Theo dõi quá trình chép để xem có xảy ra lỗi gì hay không.
- Sau khi tập tin cấu hình đã được chép xong, bạn nhân Ctrl-Z để thoát khỏi chế độ cấu hình toàn cục.
- Lưu lại thành tập tin cấu hình khởi động bằng lệnh **copy running-config startup-config.**



Hình 5.2.4a: Quá Trình chép tập tin cấu hình từ router thành tập tin văn bản bằng kết nối HyperTerminal



Hình 5.2.4b: Quá trình chép tập tin cấu hình vào router bằng kết nối HyperTerminal

5.2.5. Quản lý Cisco IOS bằng TFTP

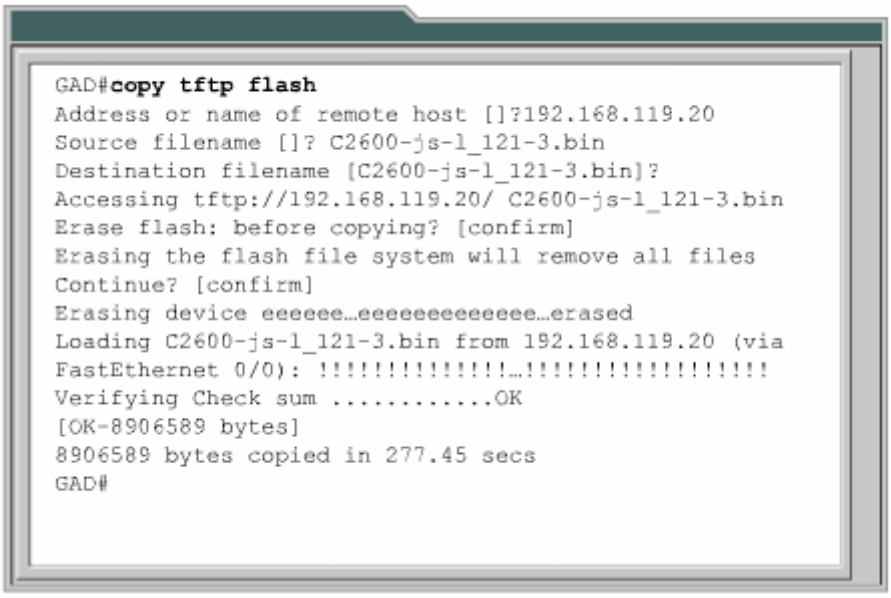
Thỉnh thoảng router cũng cần lưu dự phòng hoặc nâng cấp IOS. Đầu tiên sau khi mua router, chúng ta cần lưu lại IOS để dự phòng. Bạn có thể đặt IOS này trên một server trung tâm chung với các IOS khác. Các IOS này được sử dụng để thay thế hay nâng cấp cho các router, switch trong hệ thống mạng.

Server phải có chạy dịch vụ TFTP và chúng ta chép IOS từ server lên router bằng lệnh **copy tftp flash** ở chế độ EXEC đặc quyền.

Sau khi nhập lệnh trên, router sẽ hiển thị dấu nhắc yêu cầu bạn nhập địa chỉ IP của TFTP server. Sau đó router sẽ yêu cầu bạn xoá flash. Router thường yêu cầu bạn xoá flash khi bộ nhớ flash không còn đủ chỗ trống để lưu them IOS mới. Router sẽ hiển thị một chuỗi các chứ “e” trong suốt quá trình xoá flash.

Sau khi xoá xong flash, router bắt đầu tải IOS mới về. Router sẽ hiển thị một chuỗi các dấu chấm than (!) trong suốt quá trình chép. Một IOS có thể lớn khoảng vài Megabyte nên quá trình này cũng sẽ tốn một khoảng thời gian.

Sau khi chép xong, router sẽ kiểm tra lại IOS mới trong flash. Sau khi kiểm tra hoàn tất thì lúc này router đã sẵn sang cho bạn khởi động lại để sử dụng IOS mới.



Hình 5.2.5

5.2.6. Quản lý IOS băng Xmodem

Khi khởi động router mà IOS lưu trong flash bị xoá mất hoặc bị lỗi thì bạn phải khôi phục lại IOS từ chế độ ROM monitor (ROMmon). Ở nhiều thiết bị Cisco, chế độ ROMmon được hiển thị bởi dấu nhắc rommon 1>

Bước đầu tiên bạn cần phải xác định xem tại sao router không tải được IOS từ flash. Nguyên nhân là do mất IOS hay IOS bị lỗi. Bạn kiểm tra flash bằng lệnh **dir flash:**

Nếu trong flash vẫn có một IOS bình thường thì bạn thử khởi động router bằng IOS này bằng lệnh **boot flash:**. Ví dụ: nếu trong flash có rommon 1>**boot flash:c2600-is-mz.121-5**

Nếu router khởi động bình thường thì có 2 vấn đề bạn cần kiểm tra xem tại sao router lại khởi động vào chế độ ROMmon mà không khởi động từ IOS trong flash. Đầu tiên, bạn dung lệnh **show version** để kiểm tra giá trị của thanh ghi cấu hình xem có đúng giá trị mặc định hay không. Nếu giá trị thanh ghi cấu hình đúng thì

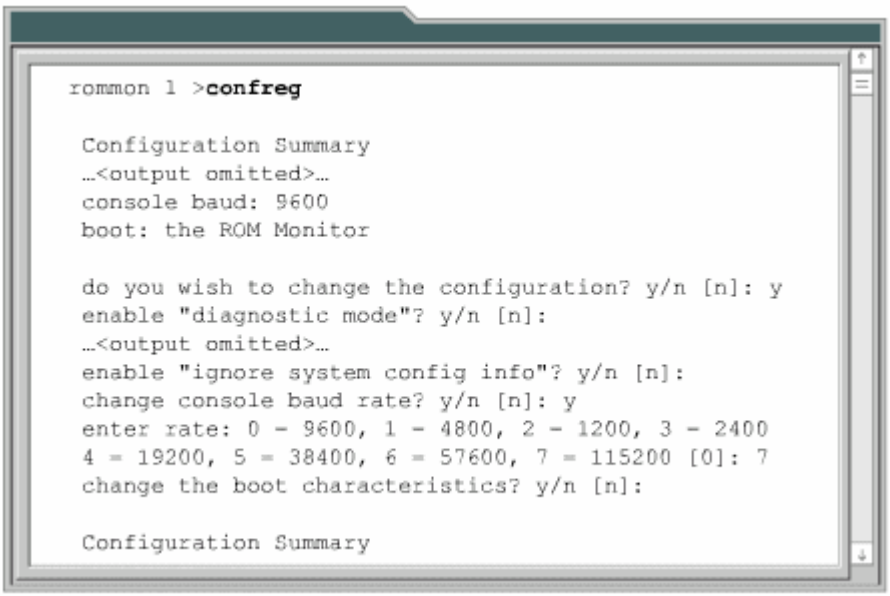
bạn dung lệnh **show startup-config** để xem có lệnh **boot system** nào cấu hình cho router khởi động vào chế độ ROM monitor hay không.

Nếu router vẫn không khởi động được hoặc là bạn không thấy có IOS nào trong flash thì bạn cần phải chép một IOS mới. Từ chế độ ROMmon, bạn có thể chép tập tin IOS bằng Xmodem qua đường console hoặc bằng TFTP.

Chép IOS bằng Xmodem từ chế độ ROMmon.

Trước tiên, bạn cần phải có tập tin IOS trên máy tính như HyperTerminal chẳng hạn. Bạn có thể chép IOS với tốc độ mặc định của đường console là 9600, hoặc là bạn có thể nâng tốc độ lên 115200. Trong chế độ ROMmon, bạn dùng lệnh **confreg**, router sẽ hiển thị các giá trị mà bạn có thể thay đổi được.

Sau đó bạn sẽ gặp câu hỏi "change console baud rate? y/n [n];", nhập chữ y để xác nhận tốc độ mới. Sau khi thay đổi tốc đường console và khởi động lại router vào chế độ ROMmon, bạn nên kết thúc phiên kết nối cũ (tốc độ 9600) và thiết lập lại phiên kết nối HyperTerminal mới với tốc độ mới là 115200 bit/s.



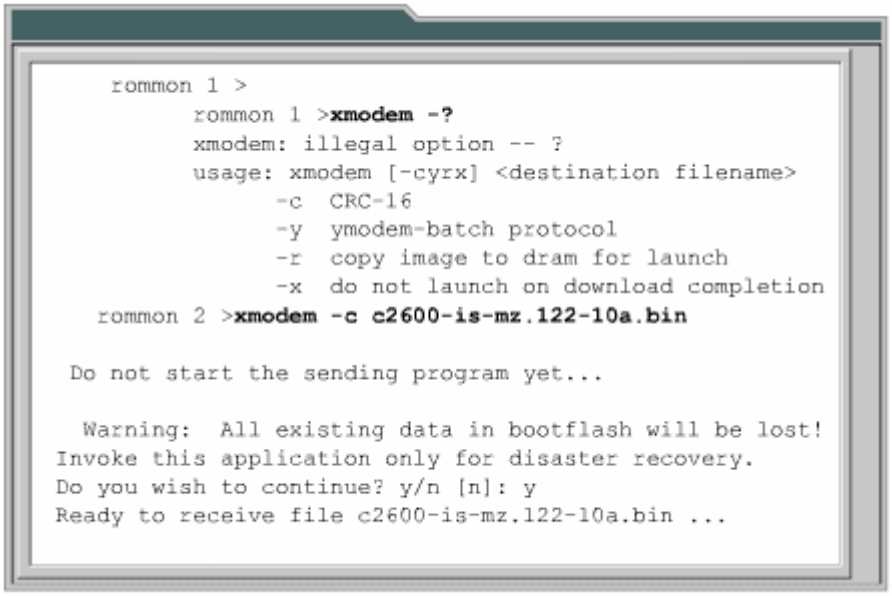
Hình 5.2.6a

Bây giờ bạn dùng lệnh **xmodem** để chép phần mềm IOS từ PC. Cấu trúc câu lệnh này như sau: **xmodem –c image_file_name**. Ví dụ: bạn chép IOS có tên là "c2600-is-mz.122-10a.bin" thì bạn gõ lệnh như sau:

Xmodem –c c2600-í-mz.122-10a.bin

Tham số -c là để cho quá trình Xmodem sử dụng CRC (Cyclic Rađunancy Check) kiểm tra lỗi trong suốt quá trình chép.

Sau đó router sẽ hiển thị một dòng thông báo chưa bắt đầu quá trình chép và một thông điệp cảnh báo. Thông điệp này cảnh báo là nội dung bộ nhớ flash sẽ bị mất nếu chúng ta tiếp tục quá trình này và yêu cầu chúng ta xác nhận có tiếp tục hay không. Nếu chúng ta xác nhận cho tiếp tục thì router sẽ bắt đầu thực hiện chép IOS.



Hình 5.2.6b: Lệnh Xmodem

Lúc này bạn cần cho bắt đầu quá trình Xmodem từ chương trình giả lập đầu cuối. Trong HyperTerminal bạn chọn **Transfer>Send File**. Trong cửa sổ của **Send File**: bạn chọn tên và vị trí lưu tập tin IOS, chọn giao thức là Xmodem, rồi bắt đầu quá trinh truyền. Trong suốt quá trình truyền, cửa sổ Send File sẽ hiển thị trạng thái truyền.

Khi quá trình truyền hoàn tất, bạn sẽ gặp một thông điệp cho biết là bộ nhớ flash đang bị xoá, sau đó IOS được chép vào flash. Cuối cùng bạn gặp thông điệp "Dowbload Complete!". Trước khi khởi động lại router, bạn cần phải cài đặt lại tốc

độ đường cốnle là 9600 và đặt lại giá trị thanh ghi cấu hình là 0x2102 bằng lệnh **config-register 0x2102**.

Trong lúc router đang khởi động lại thì bạn nên kết thúc phiên kết nối 115200 và thiết lập lại phiên kết nối mới với tộc độ 9600.

5.2.7. Biến môi trường

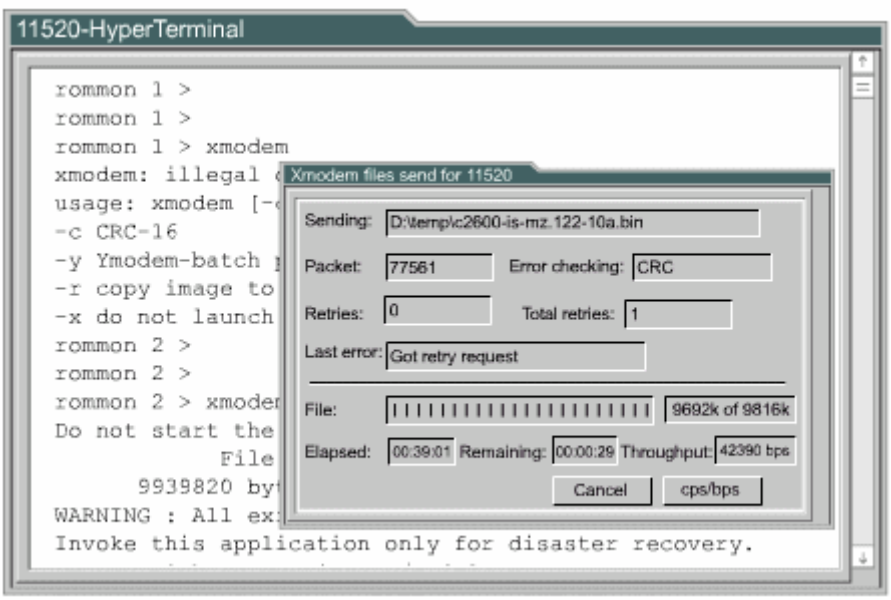
Bạn có thể khôi phục IOS bằng TFTP. Chép IOS bằng TFTP trong chế độ ROMmon là cách nhanh nhất để khôi phục IOS cho router. Để thực hiện cách này, bạn cài đặt biến môi trường rồi dùng lệnh **tftpdnld**.

Chế độ ROMmon có chức năng rất giới hạn vì chưa tải được tập tin cấu hình khi khởi động router. Do đó router không hề có IP hay cấu hình cho cổng giao tiếp nào. Các biến môi trường sẽ cung cấp cho router một cấu hình tối thiểu cho phép chạy TFTP để chép IOS. TFTP trong chế độ ROMmon chỉ hoạt động được với cổng LAN đầu tiên trên router, do đó bạn cần cài đặt các đặc tính IP cho cổng LAN này. Để cài đặt giá trị cho các biến môi trường, đầu tiên bạn nhập tên biến, tiếp theo là dấu bằng (=) rồi đến giá trị cài đặt cho biến đó (TÊN BIẾN = giá trị cài đặt). Vi dụ: bạn muốn đặt địa chỉ IP là 10.0.0.1 thì ở dấu nhắc của chế độ ROMmon bạn nhập câu lệnh là: IP_ADDRESS=10.0.0.1

Sau đây là các biến tối thiểu mà bạn cần phải đặt để sử dụng cho lệnh **tfpđnld**:

- IP_ADDRESS: địa chỉ IP cho cổng LAN.
- IP_SUBNET_MASK:subnet mask cho cổng LAN.
- DEFAULT_GATEWAY: đường mặc định cho cổng LAN.
- TFTP_SERVER: địa chỉ IP của TFTP server.
- TFTP_FILE: tên tập tin IOS lưu trên server.

Để kiểm tra lại giá trị của các biến môi trường, bạn dùng lệnh **set**.



Hình 5.2.6c: Cửa sổ Send File

Sau khi cài đặt xong các biến môi trường, bạn nhập lệnh **tftpdnld**, không có tham số nào tiếp theo hết. Router sẽ hiển thị lại giá trị các biến, theo sau là thông điệp cảnh báo quá trình này sẽ xoá flash và yêu cầu chúng ta xác nhận có cho tiếp tục quá trình này hay không.

Trong quá trình chép, router hiển thị dấu chấm than (!) cho biết đã nhận được các gói dữ liệu. Sau khi nhận xong tập tin IOS, router bắt đầu xoá flash rồi chép tập tin IOS mới vào flash. Bạn sẽ gặp một thông báo khi quá trình này hoàn tất.

Sau đó, từ dấu nhắc của chế độ ROMmon, bạn có thể khởi động lài router bằng cách nhập chữ **i**. Router sẽ khởi động lại với IOS mới trong flash.

5.2.8. Kiểm tra tập tin hệ thống

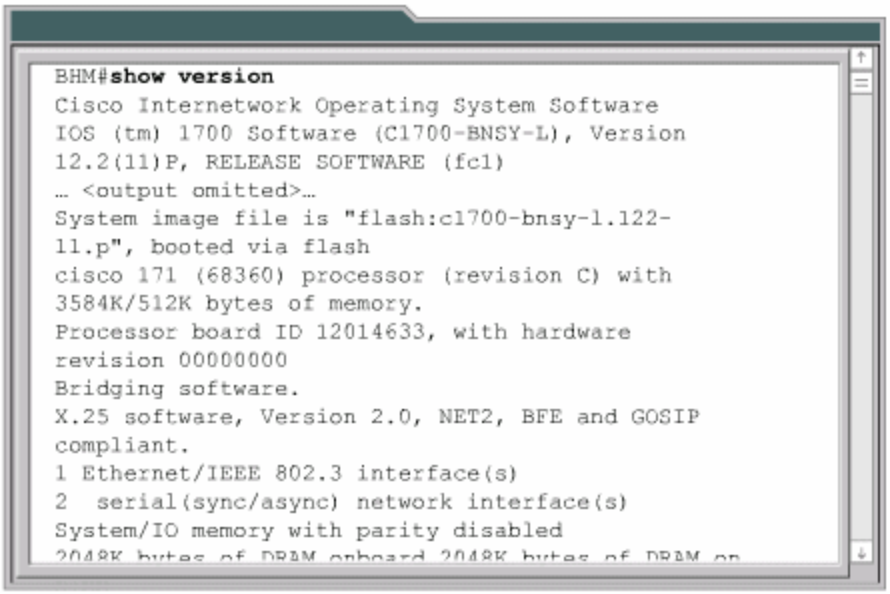
Có rất nhiều lệnh để kiểm tra tập tin hệ thống của router. Trong đó bạn có thể sử dụng lệnh **show version**. Lệnh **show version** có thể kiểm tra được tập tin hiện tại trong flash và tổng dung lượng của bộ nhớ flash. Ngoài ra lệnh này còn cung cấp thêm một số thông tin về lần tải IOS gần nhất như: trong lần khởi động gần nhất, router tải IOS nào, từ đâu; giá trị thanh ghi cấu hình hiện tại là bao nhiêu. Nếu vị trí mà router tải IOS trong flash đã bị mất hoặc bị lỗi, hoặc là có lệnh boot system trong tập tin cấu hình khởi động.

Bên cạnh đó, bạn có thể dùng lênh show flash để kiểm tra tập tin hệ thống. Lệnh này kiểm tra được trong flash hiện đang có tập tin IOS nào, tổng dung lượng flash còn trống là bao nhiêu. Chúng ta thường dùng lệnh này để xem bộ nhớ flash có đủ dung lượng cho IOS mới hay không.

Như các phần trên đã đề cập, tập tin cấu hình có thể có các lệnh boot system. Lệnh boot system xác định cho router vị trí tải IOS khi khởi động. Chúng ta có thể cấu hình nhiều lệnh boot system và router sẽ thực thi theo thứ tự các câu lệnh này trong tập tin cấu hình.

```
Router# show version
Router#show version
Cisco Interface Operating System Software
IOS (tm) C2600 Software (C2600-JK803S-M), Version 12.2 (17a), RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco  System, Inc
Complie Thu 19-Jun-03 16:35 by pwade
Image text-base: 0x8000808C, data-base: 0x815F7B34

ROM: System Bootstrap, Version 12.2 (7r) [cmong 7r], RELEASE SOFTWARE
fc1)
SGCTT-HCM uptime 1 week, 1 day, 1 hour, 9 minutes
System restarted by power-on
System image file is “flash:c2500-d-l.120-10”
Cisco 2500 (68030) processor (revision N) with 2048K/2048 K bytes of memory
Processor board ID 23101339, with hardware revise 00000000
Bridging software
X25 software, Version 3.0.0
Super LAT software (copyright 1990 by Meridian Technology Corp)
TN3270 Emulation software
Basic Rae ISDN software, Version 1.1.
1 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial (sync/async) network interface(s)
1 ISDN Basic Rate interface(s)
32K bytes of non-voltatile configuration memory.
16384K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102
```

Hình 5.2.8a



TỔNG KẾT

Sau đây là các ý chính các bạn cần nắm được trong chương này:

- Xác định quá trình khởi động router.
- Nắm được các thiết bị Cisco tìm và tải IOS như thế nào.
- Sử dụng lệnh boot system.
- Xác định giá trị thanh ghi cấu hình.
- Xử lý sự cố.
- Xác định tập tin Cisco IOS và chức năng của nó.
- Nắm được các vị trí mà router lưu các loại tập tin khác nhau.
- Nắm được cấu trúc tên của IOS.
- Quản lý tập tin cấu hình bằng TFTP.
- Quản lý tập tin cấu hình bằng cắt – dán.
- Quản lý IOS bằng TFTP.
- Quản lý IOS bằng Xmodem.
- Kiểm tra tập tin hệ thống bằng các lệnh show.

CHƯƠNG 6

ĐỊNH TUYẾN VÀ CÁC GIAO THỨC ĐỊNH TUYẾN

GIỚI THIỆU

Định tuyến đơn giản chỉ là tìm đường đi từ mạng này đến mạng khác. Thông tin về những con đường này có thể là được cập nhật tự động từ các router khác hoặc là do người quản trị mạng chỉ định cho router.

Chương này sẽ giới thiệu các khái niệm về định tuyến động, các loại giao thức định tuyến động và phân tích mỗi loại một giao thức tiêu biểu.

Người quản trị mạng khi chọn lựa một giao thức định tuyến động cần cân nhắc một số yếu tố như: độ lớn của hệ thống mạng, băng thông các đường truyền, khả năng của router. loại router và phiên bản router, các giao thức đang chạy trong hệ thống mạng. Chương này mô tả chi tiết về sự khác nhau giữa các giao thức định tuyến để giúp cho nhà quản trị mạng trong việc chọn lựa một giao thức định tuyến.

Khi hoàn tất chương này, các bạn sẽ thực hiện được những việc sau:

- Giải thích được ý nghĩa của định tuyến tĩnh.
- Cấu hình đường cố định và đường mặc định cho router.
- Kiểm tra và xử lý sự cố liên quan đến đường cố định và đường mặc định của router.
- Phân biệt các loại giao thức định tuyến.
- Nhận biết giao thức định tuyến theo vectơ khoảng cách.
- Nhận biết giao thức định tuyến theo trạng thái đường liên kết.
- Mô tả đặc điểm cơ bản của các giao thức định tuyến thông dụng.
- Phân biệt giao thức định tuyến nội bộ.
- Phân biệt giao thức định tuyến ngoại vi.
- Cấu hình RIP (Routing Information Protocol – Giao thức thông tin định tuyến) cho router.

6.1 Giới thiệu về định tuyến tĩnh

6.11 .Giới thiệu về định tuyến

Định tuyến là quá trình mà router thực hiện để chuyển gói dữ liệu tới mạng đích .Tất cả các router dọc theo đường đi đều dựa vào địa chỉ IP đích của gói dữ liệu để chuyển gói theo đúng hướng đến đích cuối cùng .Để thực hiện được điều này ,router phải học thông tin về đường đi tới các mạng khác .Nếu router chạy định tuyến động thì router tự động học những thông tin này từ các router khác .Còn nếu router chạy định tuyến tĩnh thì người quản trị mạng phải cấu hình các thông tin đến các mạng khác cho router .

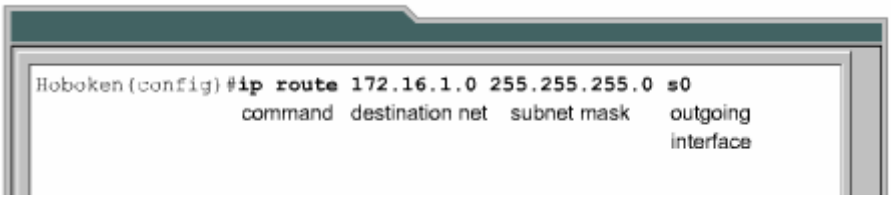
Đối với định tuyến tĩnh ,các thông tin về đường đi phải do người quản trị mạng nhập cho router .Khi cấu trúc mạng có bất kỳ thay đổi nào thì chính người quản trị mạng phải xoá hoặc thêm các thông tin về đường đi cho router .Những loại đường đi như vậy gọi là đường đi cố định .Đối với hệ thống mạng lớn thì công việc bảo trì mạng định tuyến cho router như trên tốn rất nhiều thời gian .Còn đối với hệ thống mạng nhỏ ,ít có thay đổi thì công việc này đỡ mất công hơn .Chính vì định tuyến tĩnh đòi hỏi người quản trị mạng phải cấu hình mọi thông tin về đường đi cho router nên nó không có được tính linh hoạt như định tuyến động .Trong những hệ thống mạng lớn ,định tuyến tĩnh thường được sử dụng kết hợp với giao thức định tuyến động cho một số mục đích đặc biệt.

6.1.2. Hoạt động của định tuyến tĩnh.

Hoạt động của định tuyến tĩnh có thể chia ra làm 3 bước như sau:

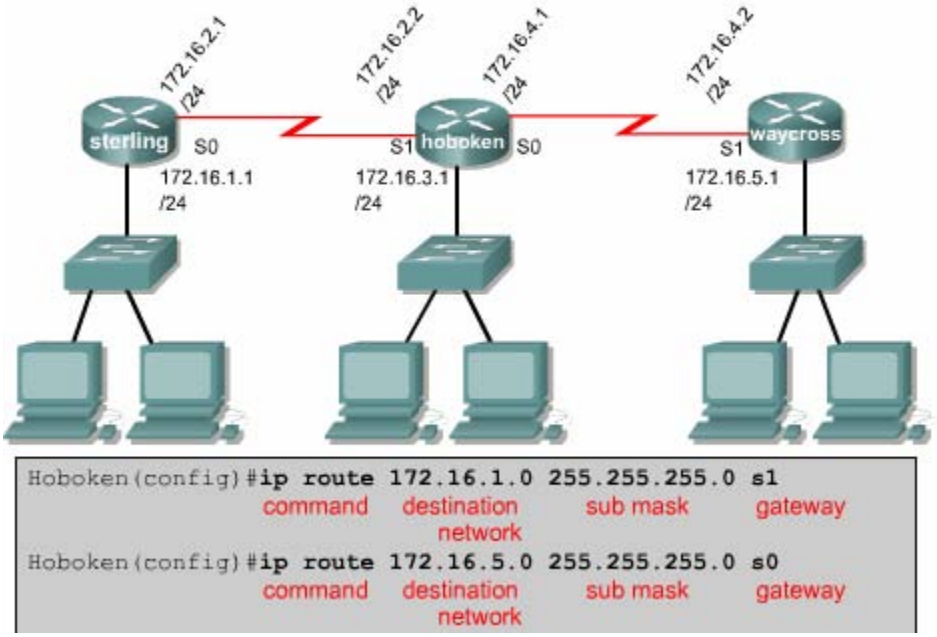
- Đầu tiên ,người quản trị mạng cấu hình các đường cố định cho router
- Router cài đặt các đường đi này vào bảng định tuyến .
- Gói dữ liệu được định tuyến theo các đường cố định này .

Người quản trị mạng cấu hình đường cố định cho router bằng lệnh iproute.Cú pháp của lệnh iproute như hình 6.1.2a:

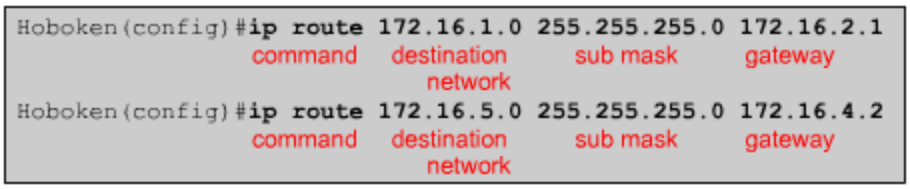


Hình 6.1.2a

Trong 2 hình 6.1.2.c và 6.1.2.c là 2 câu lệch mà người quản trị của router Hoboken cấu hình đường cố định cho router đến mạng 172.16.1.0/24 và 172.16.5.0/24 .Ở hình 6.1.2.b,câu lệnh này chỉ cho router biết đường đến mạng đích đi ra bằng cổng giao tiếp nào .Còn ở hình 6.1.2.c ,câu lệnh này chỉ cho router biết địa chỉ IP của router kế tiếp là gì để đến được mạng đích .Cả 2 câu lệnh đều cài đặt đường cố định vào bảng định tuyến của router Hoboken.Điểm khác nhau duy nhất giữa 2 câu lệnh này là chỉ số tin cậy của 2 đường cố định tương ứng trên bảng định tuyến của router sẽ khác nhau.



Hình 6.1.2.b



Hình 6.1.2.c

Chỉ số tin cậy là một thông số đo lường độ tin cậy của một đường đi .Chỉ số này càng thấp thì độ tin cậy càng cao .Do đó ,nếu đến cùng một đích thì con đường nào có chỉ số tin cậy thấp hơn thì đường đó được vào bảng định tuyến của router trước .Trong ví dụ trên,đường cố định sử dụng địa chỉ IP của trạm kế tiếp sẽ có chỉ số tin cậy mặc định là 1,còn đường cố định sử dụng cổng ra thì có chỉ số tin cậy

mặc định là 0 .Nếu bạn muốn chỉ định chỉ số tin cậy thay vì sử dụng giá trị mặc định thì bạn thêm thông số này vào sau thông số về cổng ra/địa chỉ IP trạm kế của câu lệnh .Giá trị của chỉ số này nằm trong khoảng từ 0 đến 255.

Waycross (config)# ip router 172.16.3.0 255.255.255.0 172.16.4.1.130

Nếu router không chuyển được gói ra cổng giao tiếp đã được cấu hình thì có nghĩa là cổng giao tiếp đang bị đóng,đường đi tương ứng cũng sẽ không được đặt vào bảng định tuyến .

Đôi khi chúng ta sử dụng đường cố định làm đường dự phòng cho đường định tuyến động .Router sẽ chỉ sử dụng đường cố định khi đường định tuyến động bị đứt .Để thực hiện điều này ,bạn chỉ cần đặt giá trị chỉ số tin cậy của đường cố định cao hơn chỉ số tin cậy của giao thức định tuyến động đang sử dụng là được .

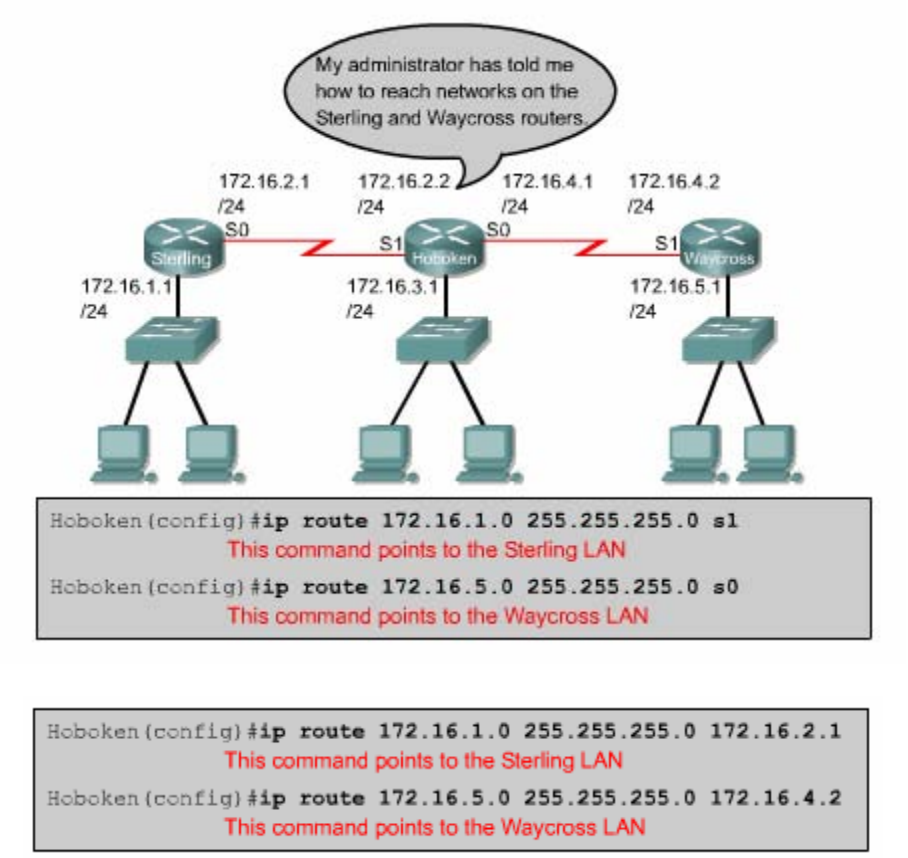
6.1.3. Cấu hình đường cố định

Sau đây là các bước để cấu hình đường cố định :

1. Xác định tất cả các mạng đích cần cấu hình ,subnet mask tương ứng và gateway tương ứng .Gateway có thể là cổng giao tiếp trên router hoặc là địa chỉ của trạm kế tiếp để đến được mạng đích .
2. Bạn vào chế độ cấu hình toàn cục của router .
3. Nhập lệnh ip route với địa chỉ mạng đích ,subnet mask tương ứng và gateway tương ứng mà bạn đã xác định ở bước 1.Nếu cần thì bạn thêm thông số về chỉ số tin cậy .
4. Lặp lại bước 3 cho những mạng đích khác
5. Thoát khỏi chế độ cấu hình toàn cục ,
6. Lưu tập tin cấu hình đang hoạt động thành tập tin cấu hình khởi động bằng lệnh copy running –config statup-config.

Hình 6.1.3 là ví dụ về cấu hình đường cố định với cấu trúc mạng chỉ có 3 router kết nối đơn giản .Trên router Hoboken chúng ta phải cấu hình đường đi tới mạng 172.16.1.0 và 172.16.5.0.Cả 2 mạng này đều có subnet mask là 255.255.255.0

Khi router Hoboken định tuyến cho các gói đến mạng đích là 172.16.1.0 thì nó sử dụng các đường đi cố định mà ta đã cấu hình cho router để định tuyến tới router Sterling ,còn gói nào đến mạng đích là 172.16.5.0 thì định tuyến tới router Waycross.



Hình 6.1.3

Ở khung phía trên của hình 6.1.3,cả 2 câu lệnh đều chỉ đường cố định cho router thông qua cổng ra trên router .Trong câu lệnh này lại không chỉ định giá trị cho chỉ số tin cậy nên trên bảng định tuyến 2 đường cố định nay có chỉ số tin cậy mặc định là 0.Đường có chí số tin cậy bằng 0 là tương đương với mạng kết nối trực tiếp vào router .

Ở khung bên dưới của hình 6.1.3, 2 câu lênh chỉ đường cố định cho router thông qua địa chỉ của router kế tiếp .Đường tới mạng 172.168.1.0 có địa chỉ của router kế tiếp là 172.16.2.1,đường tới mạng 172.16.5.0 có địa chỉ của router kế tiếp là 172.16.4.2 .Trong 2 câu này cũng không chỉ định giá trị cho chỉ số tin cậy nên 2 đường cố định tương ứng sẽ có chỉ số tin cậy mặc định là 1.

6.1.4 Cấu hình đường mặc định cho router chuyển gói đi

Đường mặc định là đường mà router sẽ sử dụng trong trường hợp router không tìm thấy đường đi nào phù hợp trong bảng định tuyến để tới đích của gói dữ liệu

.Chúng ta thường cấu hình đường mặc định cho đường ra Internet của router vì router không cần phải lưu thông tin định tuyến tới từng mạng trên Internet .Lệnh cấu hình đường mặc định thực chất cũng là lệnh cấu hình đường cố định ,cụ thể là câu lệnh như sau:

Ip route 0.0.0.0.0.0.0.0[next –hop-address/outgoing interface]

Subnet 0.0.0.0 khi được thực hiện phép toán AND logic với bất kỳ địa chỉ IP đích nào cũng có kết quả là mạng 0.0.0.0 .Do đó ,nếu gói dữ liệu có địa chỉ đích mà router không tìm được đường nào phù hợp thì gói dữ liệu đó sẽ được định tuyến tới mạng 0.0.0.0.

Sau đây là các bước cấu hình đường mặc định :

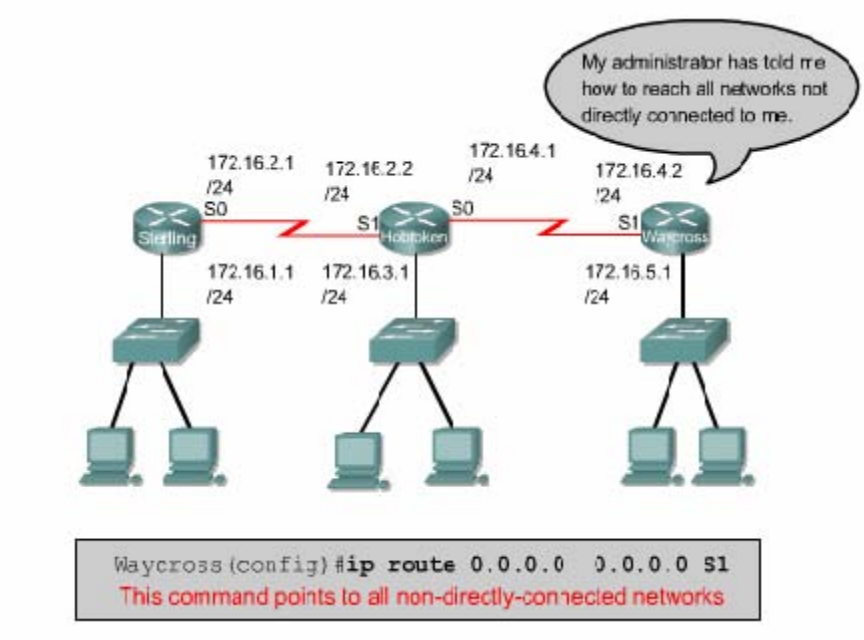
- Vào chế độ cấu hình toàn cục ,

Nhập lệnh ip route với mạng đích là 0.0.0.0 và subnet mask tương ứng là 0.0.0.0. Gateway của đường mặc định có thể là cổng giao tiếp trên router kế tiếp .Thông thường thì chúng ta nên sử dụng địa chỉ IP của router kế tiếp làm gateway .

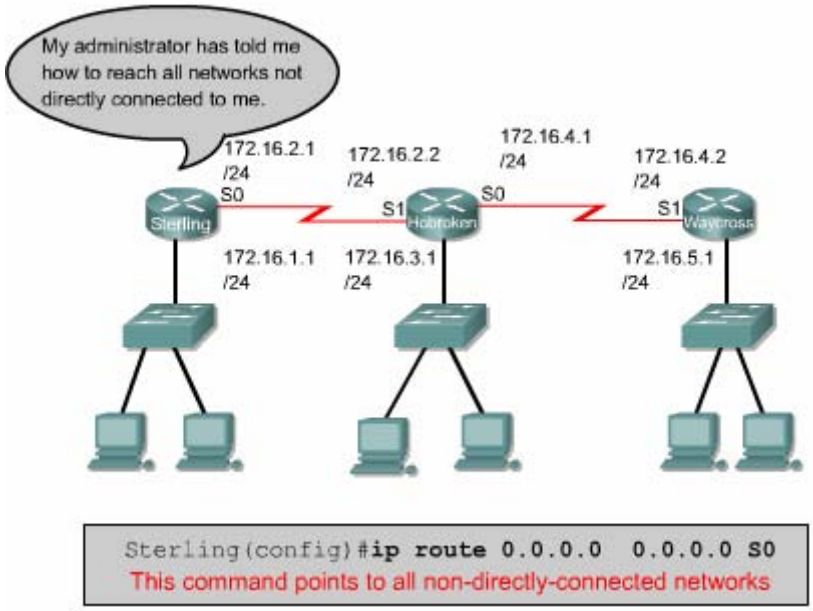
- Thoát khỏi chế độ cấu hình toàn cục ,
- Lưu lại thành tập tin cấu hình khởi động trong NVPAM bằng lệnh copy running –config.

Tiếp tục xét ví dụ trong phần 6.1.3 :router Hoboken đã được cấu hình để định tuyến dữ liệu tới mạng 172.16.1.0 trên router Sterling và tới mạng 1720160.5.0 trên router Waỷcoss để chỉ đường tới từng mạng một .Nhưng cách này thì không phải là một giải pháp hay cho những hệ thống mạng lớn.

Sterling kết nối đến tất cả các mạng khác thông qua một cổng Serial 0 mà thôi .Tương tự waycrooss cũng vậy .Waycross chỉ có một kết nối đến tất cả các mạng khác thông qua cổng Serial 1 mà thôi .Do đó chúng ta cấu hình đường mặc định cho Sterling và và Waycrooss thì 2 router này sẽ sử dụng đường mặc định để định tuyến cho gói dữ liệu đến tất cả các mạng nào không kết nối trực tiếp vào nó .



Hình 6.1.4a



Hình 6.1.4b

6.1.5.Kiểm tra cấu hình đường cố định

Sau khi cấu hình đường cố định ,chúng ta phải kiểm tra xem bảng định tuyến đã có đường ,cố định mà chúng ta đã cấu hình hay chưa ,hoạt động định tuyến có đúng hay không .Bạn dùng lệnh show running –config để kiểm tra nội dung tập tin

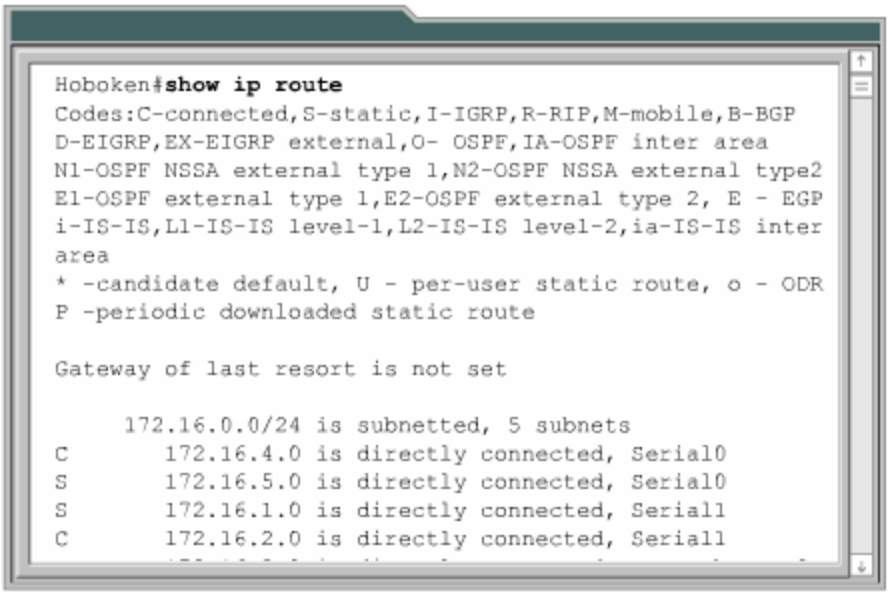
cấu hình đang chạy trên RAM xem câu lệnh cấu hình đường cố định đã được nhập vào đúng chưa .Sau đó bạn dùng lệnh show ip route để xem có đường cố định trong bảng định tuyến hay không .

Sau đây là các bước kiểm tra cấu hình đường cố định :

- Ở chế độ đặc quyền ,bạn nhập lệnh **show running-config** để xem tập tin cấu hình đang hoạt động .
- Kiểm tra xem câu lệnh –cấu hình đường cố định có đúng không .Nếu không đúng thì bạn phải vào lại chế độ cấu hình toàn cục ,xoá câu lệnh sai đi và nhập lại câu lệnh mới .
- Nhập lệnh **show ip roule**.
- Kiểm tra xem đường cố định mà bạn đã cấu hình có trong bảng định tuyến hay không

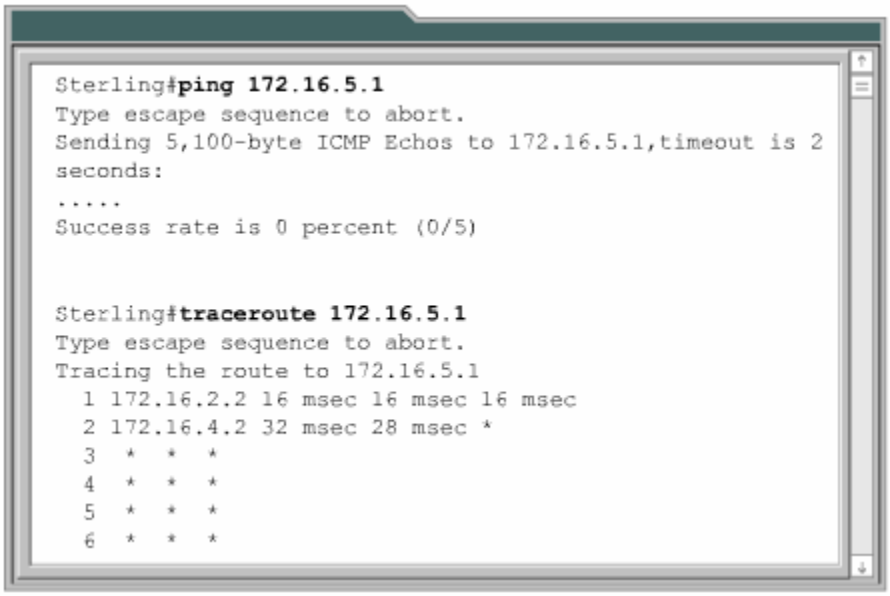
6.1.6. Xử lý sự cố

Xét ví dụ trong phần 6.1.3:router Hoboken đã được cấu hình đường cố định tới mạng 172.16.1.0 trên Sterling và tới mạng 172.16.5.0 trên waycross .Với cấu hình như vậy thì node trong mạng 172.16.1.0 ở Sterling không thể truyền dữ liệu cho node trong mạng 172.16.5.0 được .Bây giờ trên router Sterling ,bạn thực hiện lệnh **ping** tới một node trong mạng 172.16.5.0.Lệnh **ping** không thành công .Sau đó bạn dùng lệnh **traceroute** đến node mà bạn vừa mới ping để xem lệnh **traceroute** bị rớt ở đâu .Kết quả của câu lệnh **traceroute** cho thấy router Sterling nhận được gói ICMP trả lời từ router Hoboken mà không nhận được từ router waycross.Chúng ta telnet vào router Hoboken .Từ router Hoboken chúng ta thử ping đến node trong mạng 172.16.5.0 .Lệnh **ping** này sẽ thành công vì Hoboken kết nối trực tiếp với waycross.



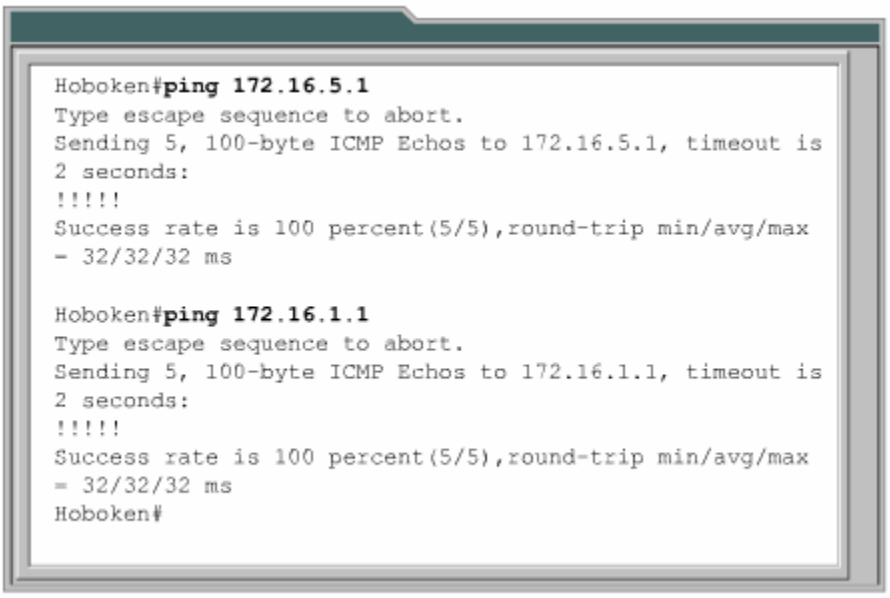
```
Hoboken#show ip route
Codes:C-connected,S-static,I-IGRP,R-RIP,M-mobile,B-BGP
D-EIGRP,EX-EIGRP external,O- OSPF,IA-OSPF inter area
N1-OSPF NSSA external type 1,N2-OSPF NSSA external type2
E1-OSPF external type 1,E2-OSPF external type 2, E - EGP
i-IS-IS,L1-IS-IS level-1,L2-IS-IS level-2,ia-IS-IS inter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

Hình 6.1.6a



```
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  *  *  *
```

Hình 6.1.6b



Hình 6.1.6c

6.2 Tổng quan về định tuyến động

6.2.1 Giới thiệu về giao thức định tuyến động

Giao thức định tuyến khác với giao thức được định tuyến cả về chức năng và nhiệm vụ .

Giao thức định tuyến được sử dụng để giao tiếp giữa các router với nhau.

Giao thức định tuyến cho phép router này chia sẻ các thông tin định tuyến mà nó biết cho các router khác .Từ đó ,các router có thể xây dựng và bảo trì bảng định tuyến của nó.

Sau đây là một số giao thức định tuyến :

- Routing information Protocol(RIP)
- Interior Gateway Routing Protocol(IGRP)
- Enhanced Inteior Gateway Routing Protocol(EIGRP)
- Open Shortest Path First(OSPF)

Còn giao thức được định tuyến thì được sử dụng để định hướng cho dữ liệu của người dùng .Một giao thức được định tuyến sẽ cung cấp đầy đủ thông tin về địa chỉ lớp mạng để gói dữ liệu có thể truyền đi từ host này đến host khác dựa trên cấu trúc địa chỉ đó .

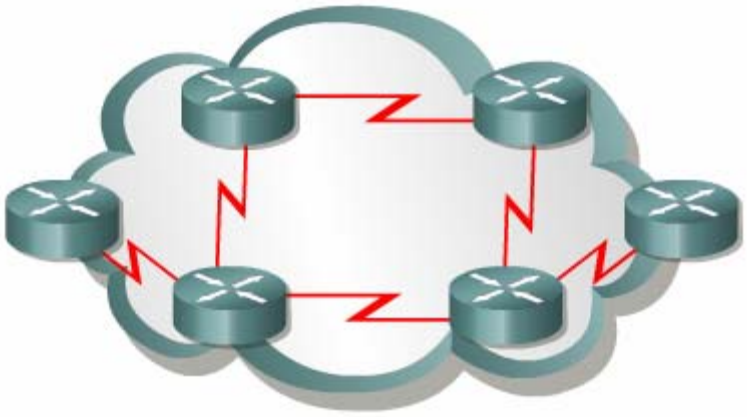
Sau đây là các giao thức được định tuyến:

- Internet Protocol (IP)
- Internetwork Packet Exchange(IPX)

6.2.2.Autonmous sytem(AS) (Hệ thống tự quản)

Hệ tự quản (AS) là một tập hợp các mạng hoạt động dưới cùng một cơ chế quản trị về định tuyến .Từ bên ngoài nhìn vào ,một AS được xem như một đơn vị .

Tổ chức Đăng ký số Internet của Mỹ (ARIN-American Regitry of Internet Numbers)là nơi quản lý việc cấp số cho mỗi AS .Chỉ số này dài 16 bit .Một số giao thức định tuyến ,ví dụ như giao thức IRGP của Cisco,đòi hỏi phải có số AS xác định khi hoạt động .



Hình 6.2.2:Một AS là bao gồm các router hoạt động dưới cùng một cơ chế quản trị

6.2.3. Muc đích của giao thức định tuyến và hệ thống tự quản

Múc đích của giao thức định tuyến là xây dựng và bảo trì bảng định tuyến .Bảng định tuyến này mang thông tin về các mạng khác và các cổng giao tiếp trên router đến các mạng này .Router sử dụng giao thức định tuyến để quản lý thông tin nhận được từ các router khác ,thông tin từ cấu hình của các cổng giao tiếp và thông tin cấu hình các đường cố định .

Giao thức định tuyến cấp nhật về tất cả các đường ,chọn đường tốt nhất đặt vào bảng định tuyến và xoá đi khi đường đó không sử dụng được nữa .Còn router thì sử dụng thông tin trêng bảng định tuyến để chuyển gói dữ liệu của các giao thức được định tuyến .

Định tuyến động hoạt động trên cơ sở các thuật toán định tuyến .Khi cấu trúc mạng có bất kỳ thay đổi nào như mở rộng thêm ,cấu hình lại ,hay bị trục trặc thì khi đó ta nói hệ thống mạng đã được hội tụ .Thời gian để các router đồng bộ với nhau càng ngắn càng tốt vì khi các router chưa đồng bộ với nhau về các thông tin trên mạng thì sẽ định tuyến sai.

Với hệ thống tự quản (AS) ,toàn bộ hệ thống mạng toàn cầu được chia ra thành nhiều mạng nhỏ, dể quản lý hơn.Mỗi AS có một số AS riêng ,không trùng lặp với bất kỳ AS khác ,và mỗi AS có cơ chế quản trị riêng của mình .

6.2.5 Phân loại các giao thức định tuyến

Đa số các thuật toán định tuyến được xếp vào 2 loại sau :

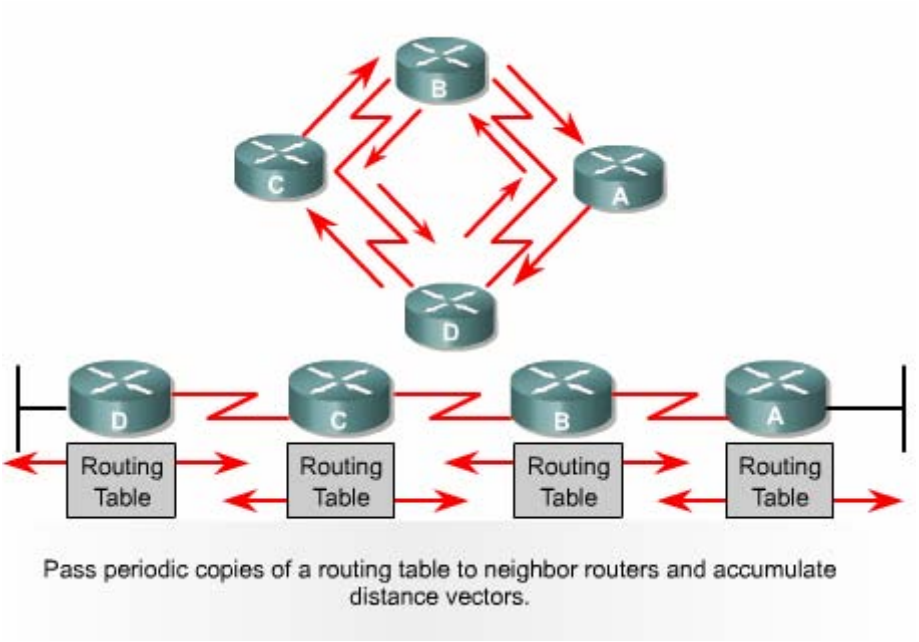
- Vectơ khoảng cách
- Trạng thái đường liên kết .

Định tuyến theo vectơ khoảng cách thực hiện truyền bản sao của bảng định tuyến từ router này sang router khác theo định kỳ .Việc cập nhật định kỳ giữa các router giúp trao đổi thông tin khi cấu trúc mạng thay đổi .Thuật toán định tuyến theo véctơ khoảng cách còn được gọi là thuật toán Bellman-Ford.

Mỗi router nhận được bảng định tuyến của những router láng giềng kết nối trực tiếp với nó .Ví dụ như hình 6.2.5a :router B nhận được thông tin từ router A .Sau đó router B sẽ cộng thêm khoảng cách từ router B đến router (ví dụ như tăng số hop lên)vào các thông tin định tuyến nhận được từ A.Khi đó router B sẽ có bảng định tuyến mới và truyền bảng định tuyến này cho router láng giềng khác là router C.Quá trình này xảy ra tương tự cho tất cả các router láng giềng khác.

Chuyển bảng định tyến cho router lán giềng theo định kỳ

và tính lại vectơ khoảng cách



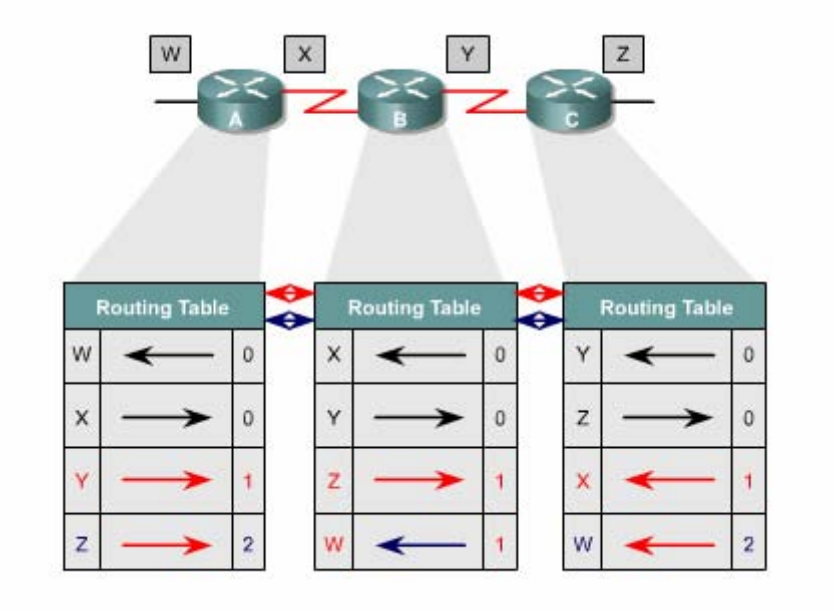
Hình 6.2.5.a

Router thu thập thông tin về khoảng cách đến các mạng khác ,từ đó nó xây dựng và bảo trì một cơ sở dữ liệu về thông tin định tuyến trong mạng. Tuy nhiên , hoạt động theo thuật toán vectơ khoảng cách như vậy thì router sẽ không biết được chính xác cấu trúc của toàn bộ hệ thống mạng mà chỉ biết được các router láng giềng kết nối trực tiếp với nó mà thôi .

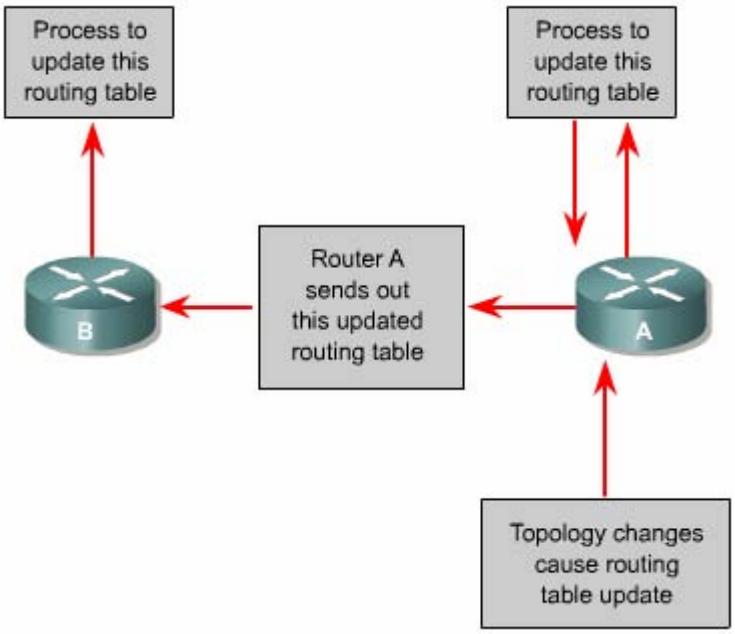
Khi sử dụng định tuyến theo vectơ khoảng cách ,bước đầu tiên là router phải xác định các router láng giềng với nó .Các mạng kết nối trực tiếp vào cổng giao tiếp của router sẽ có khoảng cách là 0.Còn đường đi tới các mạng không kết nối trực tiếp vào router thì router sẽ chọn đường tốt nhất dựa trên thông tin mà nó nhận đượctừ các router láng giềng .Ví dụ như hình vẽ 6.2.5b :router A nhận được thông tin về các mạng khác từ router B .Các thông tin này được đặt trong bảng định tuyến với vectơ khoảng cách đã được tính toán lại cho biết từ router A đến mạng đích thì đi theo hướng nào ,khoảng cách bao nhiêu.

Bảng định tuyến được cập nhật khi cấu trúc mạng có sự thay đổi .Quá trình cập nhật này cũng diễn ra từng bước một từ router này đến router khác.Khi cập nhật ,mỗi router gửi đi toàn bộ bảng định tuyến của nó cho các router láng giềng

.Trong bảng định tuyến có thông tin về đường đi tới từng mạng đích :tổng chi phí cho đường đi ,địa chỉ của router kế tiếp .



Hình 6.2.5b



Hình 6.2.5c

Một ví dụ tương tự vectơ khoảng cách mà bạn thường thấy là bảng thông tin chỉ đường ở các giao lộ đường cao tốc .Trên bảng này có các ký hiệu cho biết hướng đi tới đích và khoảng cánh tới đó là bao xa.

6.2.6. Đặc điểm của giao thức định tuyến theo trạng thái đường liên kết

Thuật toán định tuyến theo trạng thái đường liên kết là thuật toán Dijkstras hay còn gọi là thuật toán SPF (Shortest Path First tìm đường ngắn nhất).Thuật toán định tuyến theo trạng thái đường liên kết thực hiện việc xây dựng và bảo trì một cơ sở dữ liệu đầy đủ về cấu trúc của toàn bộ hệ thống mạng .

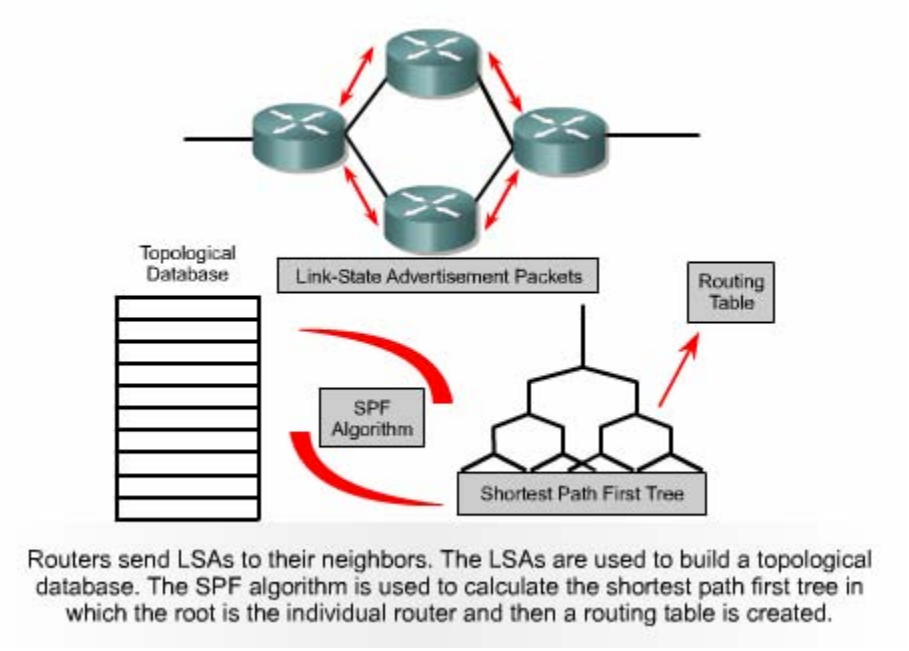
Định tuyến theo trạng thái đường liên kết sử dụng những công cụ sau:

- Thông điệp thông báo trạng thái đường liên kết (LSA-Link-state Advertisement): LSA là một gói dữ liệu nhỏ mang thông tin định tuyến được truyền đi giữa các router .
- Cơ sở dữ liệu về cấu trúc mạng :được xây dựng từ thông tin thu thập được từ các LSA .
- Thuật toán SPF :dựa trên cơ sở dữ liệu về cấu trúc mạng ,thuật toán SPF sẽ tính toán để tìm đường ngắn nhất .
- Bảng định tuyến :chứa danh sách các đường đi đã được chọn lựa .

Quá trình thu thập thông tin mạng để thực hiện định tuyến theo trạng thái đường liên kết:

Mỗi router bắt đầu trao đổi LSA với tất cả các router khác, trong đó LSA mang cơ sở dữ liệu dựa trên thông tin của các LSA.

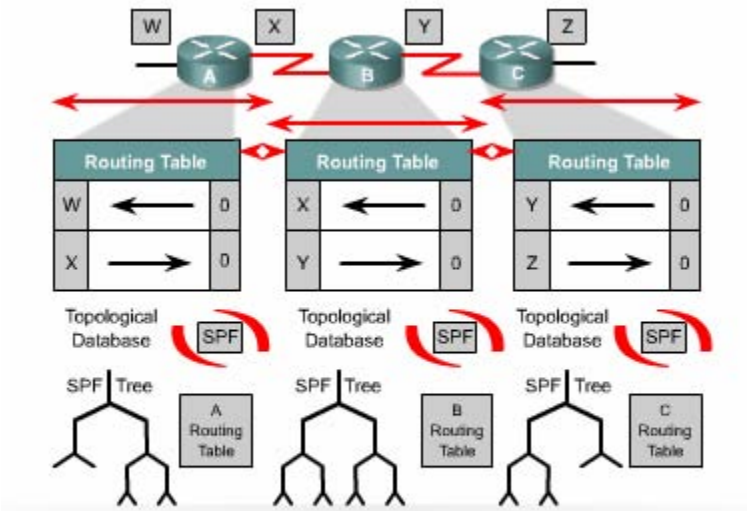
Mỗi router tiến hành xây dựng lại cấu trúc mạng theo dạng hình cây với bản than nó là gốc ,từ đó router vẽ ra tất cả các đường đi tới tất cả các mạng trong hệ thống .Sau đó thuật toán SPF chọn đường ngắn nhất để đưa vào bảng định tuyến. Trên bảng định tuyến sẽ chứa thông tin về các đường đi đã được chọn với cổng ra tương ứng.Bên cạnh đó, router vẫn tiếp tục duy trì cơ sở dữ liệu về cấu trúc hệ thống mạng và trạng thái của các đường liên kết. Router nào phát hiện cấu trúc mạng thay đổi đầu tiên sẽ phát thông tin cập nhật cho tất cả các router khác.Router phát gói LSA, trong đó có thông tin về router mới, các thay đổi về trạng thái đường liên kết. Gói LSA này được phát đi cho tất cả các router khác.



Routers send LSAs to their neighbors. The LSAs are used to build a topological database. The SPF algorithm is used to calculate the shortest path first tree in which the root is the individual router and then a routing table is created.

Hình 6.2.6a

Mỗi router có cơ sở dư liệu riêng về cấu trúc mạng và thuật toán SPF thực hiện tính toán dựa trên cơ sở dữ liệu này .



Each router has its own topological database on which the SPF algorithm is run.

Hình 6.2.6b

Khi router nhận được gói LSA thì nó sẽ cập nhật lại cơ sở dữ liệu của nó với thông tin mới vừa nhận được. Sau đó SPF sẽ tính lại để chọn đường lại và cập nhật lại cho bảng định tuyến .

Định tuyến theo trạng thái đường liên kết có một số nhược điểm sau:

- Bộ sử lý trung tâm của router phải tính toán nhiều
- Đòi hỏi dung lương bộ nhớ phải lớn
- Chiếm dụng băng thông đường truyền

Router sử dụng định tuyến theo trạng thái đường liên kết sẽ phải cần nhiều bộ nhớ hơn và hoạt động xử lý nhiều hơn là sử dụng định tuyến theo vectơ khoảng cách .Router phải có đủ bộ nhớ để lưu cơ sở dữ liệu về cấu trúc mạng ,bảng định tuyến .Khi khởi động việc định tuyến ,tất cả các router phải gửi gói LSA cho tất cả các router khác,khi đó băng thông đường truyền sẽ bị chiếm dụng làm cho băng thông dành cho đường truyền dữ liệu của người dùng bị giảm xuống. Nhưng sau khi các router đã thu thập đủ thông tin để xây dựng cơ sở dữ liệu về cấu trúc mạng thì băng thông đường truyền không bị chiếm dụng nữa .Chỉ khi nào cấu trúc mạng thay đổi thì router mới phát gói LSA để cập nhật và những gói LSA này chiếm một phần băng thông rộng rất nhỏ .

6.3 Tổng quát về giao thức định tuyến

6.3.1. Quyết định chọn đường đi

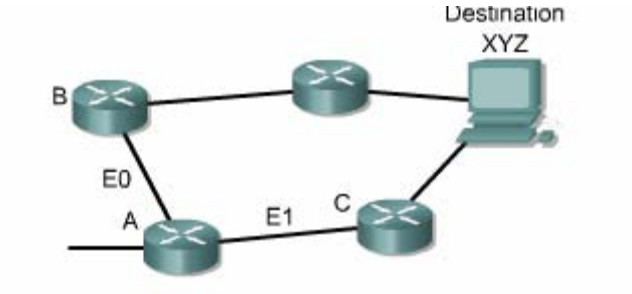
Router có 2 chức năng chính là :

- Quyết định chọn đường đi
- Chuyển mạch

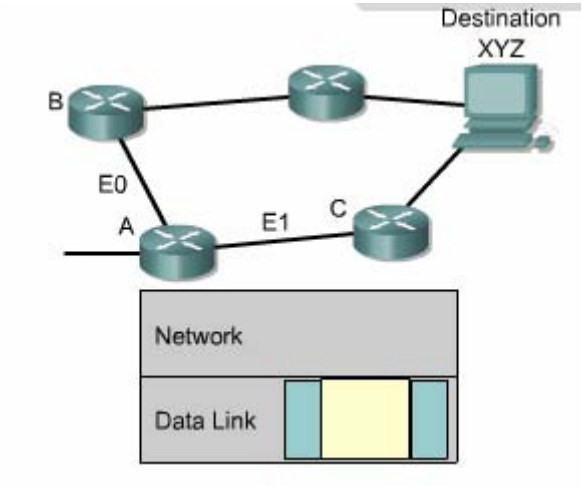
Quá trình chọn đường đi được thực hiện ở lớp Mạng.Router dựa vào bảng định tuyến để chọn đường cho gói dữ liệu ,sau khi quyết định đường ra thì router thực hiện việc chuyển mạch để phát gói dữ liệu .

Chuyển mạch là quá trình mà router thực hiện để chuyển gói từ cổng nhận vào ra cổng phát đi .Điểm quan trọng của quá trình này là router phải đóng gói dữ liệu cho phù hợp với đường truyền mà gói chuẩn bị đi ra

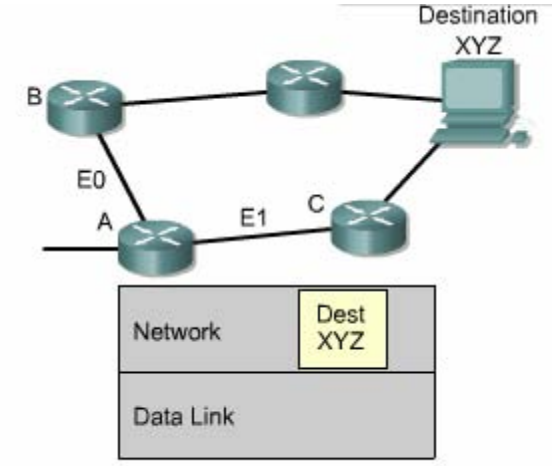
Trong các hình 6.3.1a-6.3.1e cho thấy cách mà router sử dụng địa chỉ mạng để quyết định chọn đường cho gói dữ liệu .



Hình 6.3.1a

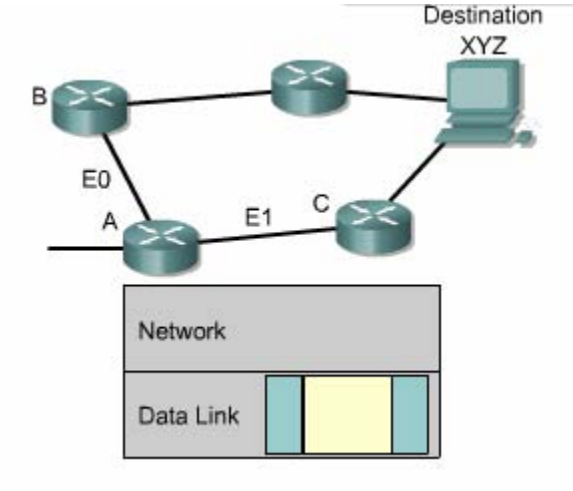


Hình 6.3.1b

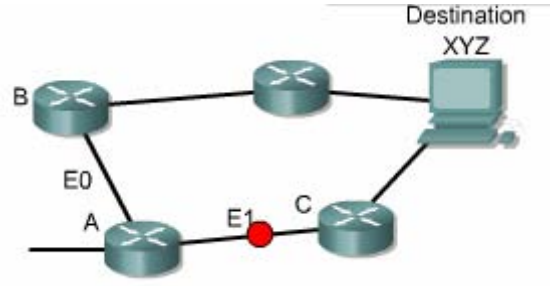


Interface	Desirability	Next Hop	Dest
E1	+	Router C	XYZ
E0	-	Router B	XYZ

Hình 6.3.1c



Hình 6.3.1d



Hình 6.3.1e

6.3.2 Cấu hình định tuyến

Để cấu hình giao thức định tuyến ,bạn cần cấu hình trong chế độ cấu hình toàn cục và cài đặt các đặc điểm định tuyến .Bước đầu tiên ,ở chế độ cấu hình toàn cục ,bạn cần khởi động giao thức định tuyến mà bạn muốn ,ví dụ như RIP ,IRGP,EIGRP hay OSPF. Sau đó ,trong chế độ cấu hình định tuyến ,công việc chính là bạn khái báo địa chỉ IP .Định tuyến động thường sử dụng broadcst và multicast để trao đổi thông tin giữa các router .Router sẽ dựa vào thông số định tuyến để chọn đường tốt nhất tới từng mạng đích.

Lệnh router dùng để khởi động giao thức định tuyến .

Lệnh network dùng để khai báo các cổng giao tiếp trên router mà ta muốn giao thức định tuyến gửi và nhận các thông tin cập nhật về định tuyến .

Sau đây là các ví dụ về cấu hình định tuyến:

GAD(config)#router rip

GAD(config-router)#network 172.16..0.0

Địa chỉ mạng khai báo trong câu lệnh **network** là địa chỉ mạng theo lớp A,B,hoặc C chứ không phải là địa chỉ mạng con (subnet)hay địa chỉ host riêng lẻ .

6.3.3 Các giao thức định tuyến

ở lớp Internet của bộ giao thức TCP/IP , router sử dụng một giao thức định tuyến IP để thực hiện việc định tuyến .Sau đây là một số giao thức định tuyến IP:

- **RIP –** giao thức định tuyến nội theo vectơ khoảng cách
- **IGRP-** giao thức định tuyến nội theo vectơ khoảng cách Cisco.
- **OSPF –** giao thức định tuyến nội theo trạng thái đường liên kết
- **EIGRP-** giao thức mở rộng của IGRP
- **BGP-** giao thức định tuyến ngoại theo vectơ khoảng cách

RIP (Routing information Protocol)được định nghĩa trong RPC 1058.

Sau đây là các đặc điểm chính của RIP :

- Là giao thức định tuyến theo vectơ khoảng cách
- Sử dụng số lượng hop để làm thông số chọn đường đi
- Nếu số lượng hop để tới đích lớn hơn 15 thì gói dữ liệu sẽ bị huỷ bỏ
- Cập nhật theo định kỳ mặc định là 30 giây

IGRP (Internet gateway routing Protocol)là giao thức được phát triển độc quyền bởi Cisco .Sau đây là một số đặc điểm mạnh của IGRP:

- Là giao thức định tuyến theo vectơ khoảng cách
- Sử dụng băng thông ,tải ,độ trễ và độ tin cậy của đường truyền làm thông số lựa chọn đường đi
- Cập nhật theo định kỳ mặc định là 90 giây

OSPF (Open Shortest Path First)là giao thức đình tuyến theo trạng thái đường liên kết .Sau đây là các đặc điểm chinhs của OSPF :

- Là giao thức định tuyến theo trạng thái đường liên kết
- Được định nghĩa trong RFC 2328 ,
- Sử dụng thuật toán SPF để tính toán chọn đường đi tốt nhất ,
- Chỉ cập nhật khi cấu trúc mạng có sự thay đổi ,

EIGRP Là giao thức định tuyến nâng cao theo vectơ khoảng cách ,và là giao thức độc quyền của Ciso.Sau đây là các đặc điểm chính của EIGRP:

- Là giao thức định tuyến nâng cao theo vectơ khoảng cách ,
- Có chia tải.
- Có các ưu điểm của định tuyến theo vectơ khoảng cách và định tuyến theo trạng thái đường liên kết.
- Sử dụng thuật toán DUAL (Diffused Update Algorithm)để tính toán chọn đường tốt nhất. Cập nhật theo định kỳ mặc định là 90 gây hoặc cập nhật khi có thay đổi về cấu trúc mạng.

BGP (Border Gateway Protocol) là giao thức định tuyến ngoại. Sau đây là các đặc điểm chính của BGP. Là giao thức định tuyến ngoại theo vectơ khoảng cách,

- Được sử dụng để định tuyến giữa các ISP hoặc giữa ISP và khách hàng ,
- Được sử dụng để định tuyến lưu lượng Internet giữa các hệ tự quản (AS).

6.3.4 Hệ tự quản, IGP và EGP

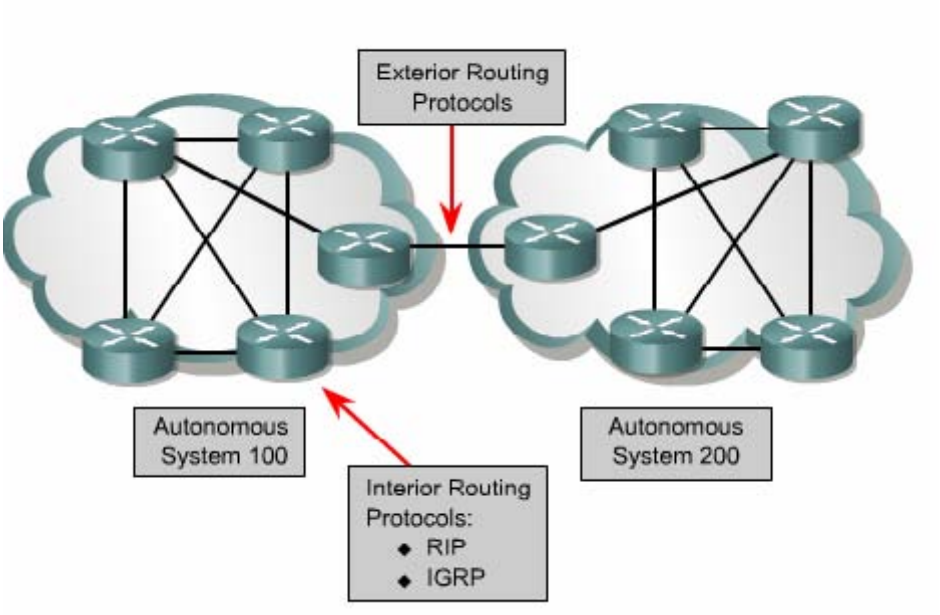
Giao thức định tuyến nội được thiết kế để sử dụng cho hệ thống mạng của một đơn vị tổ chức mà thôi .Điều quan trọng nhất đối với việc xây dựng một giao thức định tuyến nội là chọn thông số nào và sử dụng những thông số đó ra sao để chọn đường đi trong hệ thống mạng .

Giao thức định tuyến ngoại được thiết kế để sử dụng giữa 2 hệ thống mạng có 2 cơ chế quản lý khác nhau .Các giao thức loại này thường được sử dụng để định tuyến giữa các ISP .Giao thức định tuyến IP ngoại thường yêu cầu phải có 3 thông tin trước khi hoạt động ,đó là :

- Danh sách các router láng giềng để trao đổi thông tin định tuyến ,
- Danh sách các mạng kết nối trực tiếp mà giao thức cần quảng bá thông tin định tuyến .
- Chỉ số của hệ tự quản trên router .

Giao thức định tuyến ngoại vi cần phải phân biệt các hệ tự quản .Các bạn nên nhớ rằng mỗi hệ tự quản có một cơ chế quản tri riêng biệt .Giữa các hệ thống này phải có một giao thức để giao tiếp được với nhau .

Mỗi một hệ tự quản có một con số xác định được cấp bởi tổ chức đăng ký số Internet của Mỹ (ARIN – America Registry of Internet Number) hoặc được cấp bởi nhà cung cấp dịch vụ. Con số này là số 16 bit. Các giao thức định tuyến như IGRP và EIGRP của Cisco đòi hỏi phải khai báo số AS khi cấu hình



Hình 6.3.4

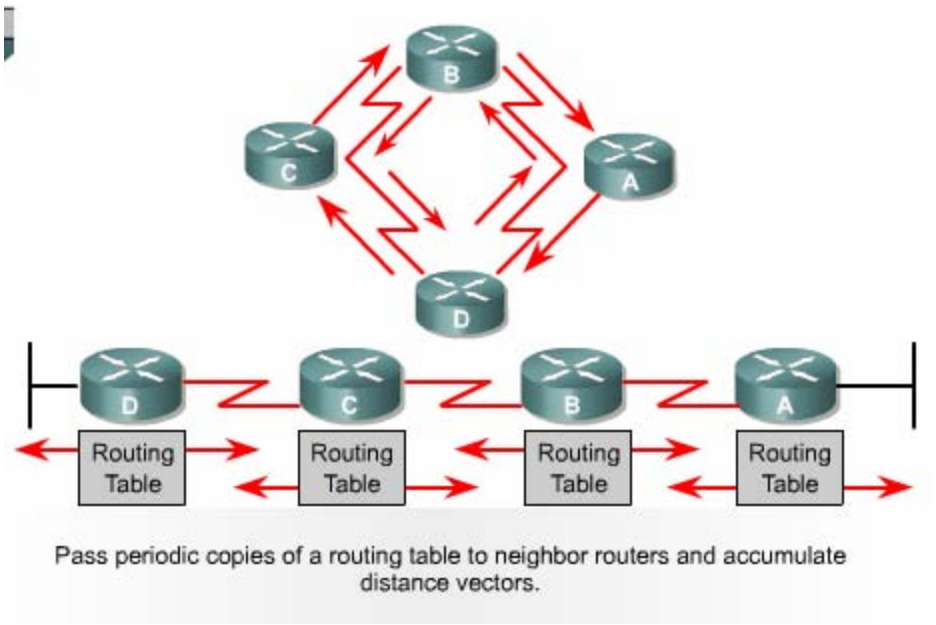
6.3.5. Vectơ khoảng cách

Thuật toán vectơ khoảng cách (hay còn gọi là thuật toán Bellman-Ford)yêu cầu mỗi router gửi một phần hoặc toàn bộ bảng định tuyến cho các router láng giềng kết nối trực tiếp với nó .Dựa vào thông tin cung cấp bởi các router láng giềng ,thuật toán vectơ khoảng cách sẽ lựa chọn đường đi tốt nhất .

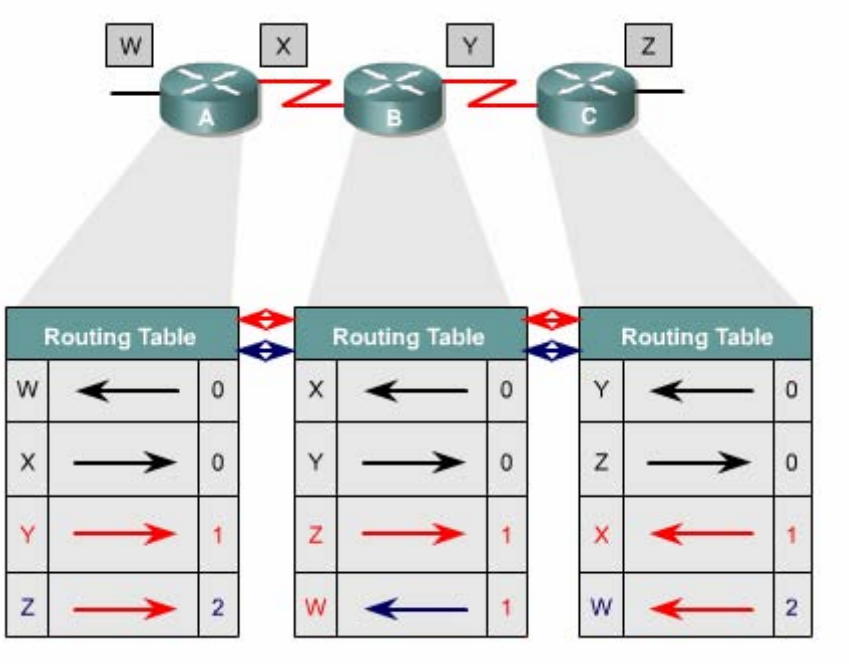
Sử dụng các giao thức định tuyến theo vectơ khoảng cách thường tốn ít tài nguyên của hệ thống nhưng tốc độ đồng bộ giữa các router lại chậm và thông số được sử dụng để chọn đường đi có thể không phù hợp với những hệ thống mạng lớn .Chủ yếu các giao thức định tyến theo vectơ khoảng cách chỉ xác định đường đi bằng khoảng cách (số lượng hop) và hướng đi (vectơ) đến mạng đích.Theo thuật toán này ,các router sẽ trao đổi bảng định tuyến với nhau theo định kỳ .Do vậy ,loại

định tuyến này chỉ đơn giản là mỗi router chỉ trao đổi bảng định tuyến với các router láng giềng của mình .Khi nhận được bảng định tuyến từ router láng giềng ,router sẽ lấy con đường nào đến mạng đích có chi phí thấp nhất rồi cộng thêm khoảng cách của mình vào đó thành một thông tin hoàn chỉnh về con đường đến mạng đích với hướng đi ,thông số đường đi từ chính nó đến đích rồi đưa vào bảng định tuyến đó gửi đi cập nhật tiếp cho các router kế cận khác .RIP và IGRP là 2 giao thức định tuyến theo vectơ khoảng cách .

Chuyển bảng định tuyến cho router láng giềng theo định kỳ và tính lại vectơ khoảng cách



Hình 6.3.5a



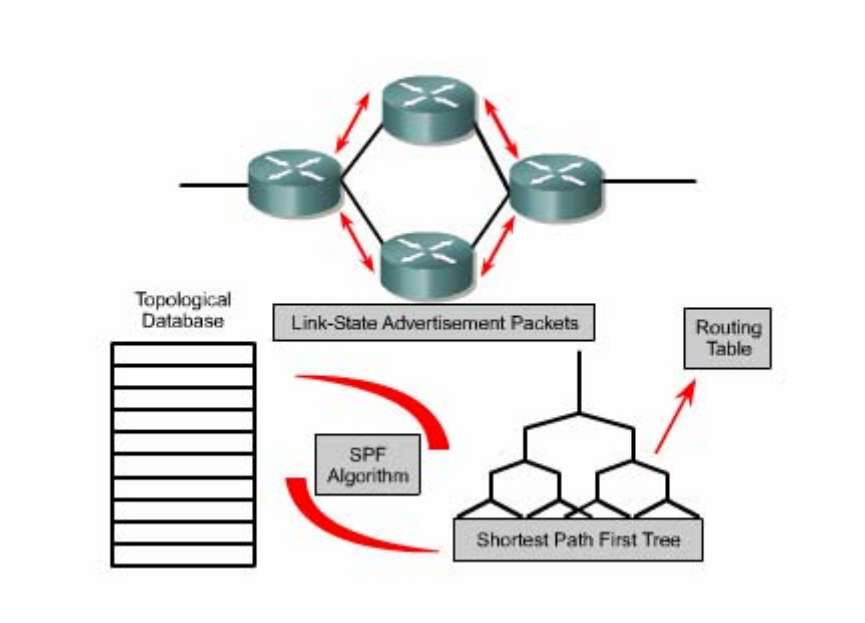
Hình 6.3.5b

6.3.6. Trạng thái đường liên kết

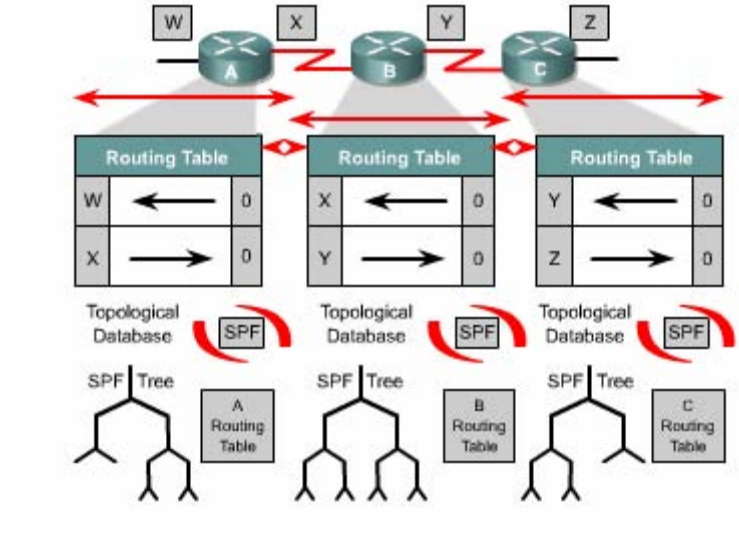
Thuật toán chọn đường theo trạng thái đường liên kết (hay còn gọi là thuật toán chọn đường ngắn nhất)thực hiện trao đổi thông tin định tuyến cho tất cả các router khi bắt đầu chạy để xây dựng một bản đồ đầy đủ về cấu trúc hệ thống mạng .Mỗi router sẽ gửi gói thông tin tới tất cả các router còn lại .Các gói này mang thông tin về các mạng kết nối vào router .Mỗi router thu thập các thông tin này từ tất cả các router khác để xây dựng một bản đồ cấu trúc đầy đủ của hệ thống mạng .Từ đó router tự tính toán và chọn đường đi tốt nhất đến mạng đích để đưa lên bảng định tuyến .Sau khi toàn bộ các router đã được hội tụ thì giao thức định tuyến theo trạng thái đường liên kết chỉ sử dụng gói thông tin nhỏ để cập nhật ,về sự thay đổi cấu trúc mạng chứ không gửi đi toàn bộ bảng định tuyến .Các gói thông tin cập nhật này được truyền đi cho tất cả router khi có sự thay đổi xảy ra ,do đó tốc độ hội tụ nhanh.

Do tốc độ hội tụ nhanh hơn so với giao thức định tuyến theo vectơ khoảng cách ,nên giao thức định tuyến theo trạng thái đường liên kết ít bị lặp vòng hơn .Mặc dù các giao thức loại này ít bị lỗi về định tuyến hơn nhưng lại tiêu tốn nhiều tài nguyên hệ thong hơn .Do đó chúng mắc tiền hơn nhưng bù lại chúng co khả năng mở rộng hơn so với giao thức định tuyến theo vectơ khoảng cách .

Khi trạng thái của một đường liên kết nào đó thay đổi thì gói quảng bá trạng thái đường liên kết LSA được truyền đi trên khắp hệ thống mạng .Tất cả các router đều nhận được gói thông tin này và dựa vào đó để điều chỉnh lại việc định tuyến của mình .Phương pháp cập nhật như vậy tin cậy hơn ,dễ kiểm tra hơn và tốn ít băng thông đường truyền hơn so với kiểu cập nhật của vectơ khoảng cách .OSPF và IS –IS là 2 giao thức định tuyến theo trạng thái đường liên kết.



Hình 6.3.6a



Hình 6.3.6b

Tổng kết

Sau đây là các điểm quan trọng mà các bạn cần nắm được trong chương này:

- Router sẽ không chuyển gói tin nếu không tìm được đường tới đích
- Đường cố định là do người quản trị mạng cấu hình cho router
- Đường mặc định là một loại đặc biệt của đường cố định .Đường mặc định là con đường cuối cùng cho router sử dụng khi không tìm được đường nào tới đích
- Ta có thể sử dụng các lệnh sau để kiểm tra cấu hình của đường cố định và đường mặc định :**show ip router ,ping ,traceroute.**
- Kiểm tra và xử lý sự cố liên quan đến đường cố định và đường mặc định .
- Các giao thức định tuyến
- Hệ tự quản
- Mục đích của giao thức định tuyến và hệ tự quản
- Các loại giao thức định tuyến
- Đặc điểm của giao thức định tuyến theo vectơ khoảng cách
- Đặc điểm của giao thức định tuyến theo trạng thái đường liên kết
- Quyết định chọn đường đi
- Cấu hình định tuyến
- Các giao thức định tuyến: RIP, IGRP, OSPF, EIGRP, BGP
- Hệ tự quản, IGP và EGP
- Định tuyến theo vectơ khoảng cách
- Định tuyến theo trạng thái đường liên kết

CHƯƠNG 7

GIAO THỨC ĐỊNH TUYẾN THEO VECTƠ KHOẢNG CÁCH

GIỚI THIỆU

Giao thức định tuyến động giúp cho "cuộc sống" của người quản trị mạng trở nên đơn giản hơn nhiều. Nhờ có định tuyến động mà người quản trị mạng không còn tốn thời gian để cấu hình đường cố định và chỉnh sửa lại chúng khi có sự cố. Với định tuyến động, router có thể tự động cập nhật và thay đổi việc định tuyến theo sự thay đổi của hệ thống mạng. Tuy nhiên định tuyến động cũng có những vấn đề của nó .Trong chương này sẽ đề cập đến các vấn đề của giao thức định tuyến theo vectơ khoảng cách và các phương pháp mà những nhà thiết kế sử dụng để giải quyết những vấn đề này.

RIP (Routing Information Protocol) là một giao thức định tuyến theo vectơ khoảng cách được sử dụng rộng rãi trên thế giới .Mặc dù RIP không có những khả năng và đặc điểm như những giao thức định tuyến khác nhưng RIP dựa trên những chuẩn mở và sử dụng đơn giản nên vẫn được các nhà quản trị mạng ưa dùng .Do đó RIP là một giao thức tốt để người học về mạng bước đầu làm quen .Trong chương này sẽ giới thiệu cấu hình RIP và xư lý sự cố đối với RIP .

Giống như RIP, IGRP (Interior Gateway Routing Protocol)cũng là một giao thức định tuyến theo vectơ khoảng cách. Nhưng khác với RIP, IGRP là giao thức độc quyền của Cisco chứ không phải là một giao thức dựa trên các chuẩn mở. IGRP phức tạp hơn so với RIP, sử dụng nhiều thông số để chọn đường đi tốt nhất đến đích nhưng IGRP vẫn là một giao thức sử dụng đơn giản .Trong chương này cũng sẽ giới thiệu cấu hình IGRP và xử lý sự cố đối với IGRP.

Sau khi hoàn tất chương trình ,các bạn sẽ thực hiện được những việc sau :

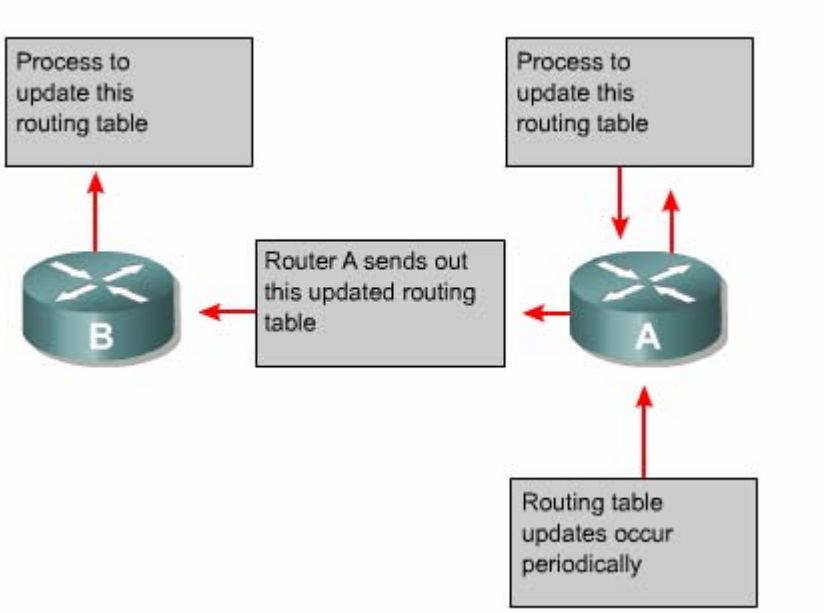
- Mô tả được tai sao định tuyến lặp vòng lại xảy ra đối với định tuyến theo vectơ khoảng cách .
- Mô tả được các phương pháp được sử dụng để đảm bảo cho các giao thức định tuyến theo vectơ khoảng cách định tuyến đúng.
- Cấu hình RIP
- Sử dụng lệnh ip classless

- Xử lý sự cố của RIP
- Cấu hình RIPđể chia tải
- Cấu hình đường cố định cho RIP
- Kiểm tra cấu hình RIP
- Cấu hình IGRP
- Kiểm tra hoạt động của IGRP
- Xử lý sự cố IGRP

7.1. Định tuyến theo vectơ khoảng cách

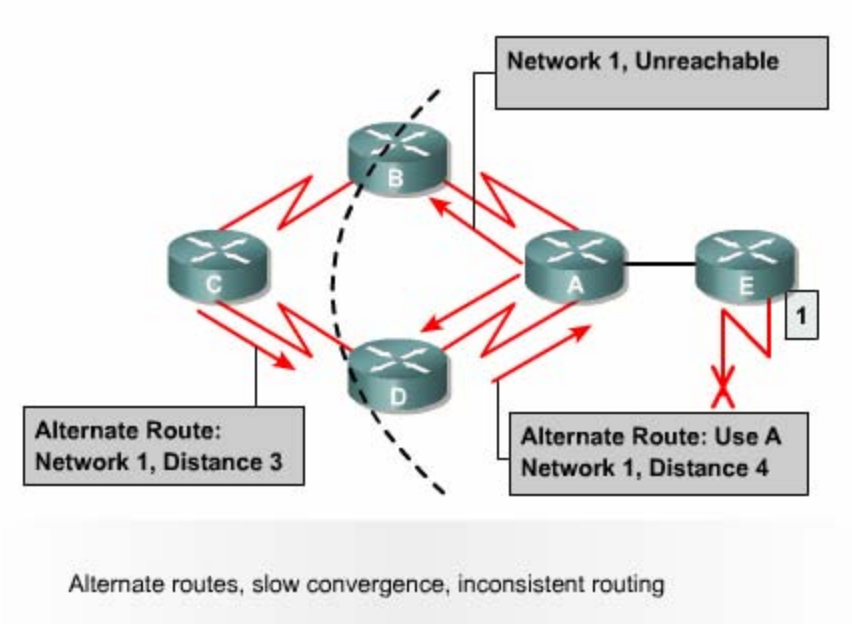
7.1.1. Cập nhật thông tin định tuyến

Bảng định tuyến được cập nhật theo chu kỳ hoặc khi cấu trúc mạng có sự thay đổi .Điểm quan trọng đối với một giao thức định tuyến là làm sao cập nhật bảng định tuyến một cách hiệu quả .Khi cấu trúc mạng thay đổi ,thông tin cập nhật phải được xử lý trong toàn bộ hệ thống .Đối với định tuyến theo vectơ khoảng cách thì mỗi router gửi toàn bộ bảng định tuyên của mình cho các router kết nối trực tiếp với nó.Bảng định tuyến bao gồm các thông tin về đường đi tới mạng đích như:tổng chi phí (ví dụ như khoảng cách chẳng hạn)tính từ bản thân router đến mạng đích ,địa chỉ của trạm kế tiếp trên đường đi.



Hình 7.1.1

7.1.1. Lỗi định tuyến lặp



Hình 7.1.2

Định tuyến lặp có thể xảy ra khi bảng định tuyến trên các router chưa được cập nhật hội tụ do quá trình hội tụ chậm.

1. Trước khi mạng 1 bị lỗi ,tất cả các router trong hệ thống mạng đều có thông tin đúng về cấu trúc mạng và bảng định tuyến là chính xác .Khi đó chúng ta nói các router đã hội tụ .Giả sử rằng :router C chọn đường đến Mạng 1 bằng con đường qua router Bvà khoảng cách của con đường này từ router C đến Mạng 1 và 3 (hops)(Nghĩa là nếu đi từ router C đến Mạng 1 theo con đường này thì còn cách 3 router nữa).
2. Ngay khi mạng 1 bị lỗi, router E liền gửi thông tin cập nhật cho router A. Router A lập tức ngưng việc định tuyến về Mạng 1. Nhưng router B, C và D vẫn tiếp tục việc này vì chúng vẫn chưa hay biết về việc Mạng 1 bị lỗi. Sau đó router A cập nhật thông tin về Mạng 1 cho router B và D. Router B,D lập tức ngưng định tuyến các gói dữ liệu về Mạng 1 nên nó vẫn định tuyến các gói dữ liệu đến Mạng 1 qua router B.
3. Đến thời điểm cập nhật định kỳ của router C, trong thông tin cập nhật của router C gửi cho router D vẫn có thông tin về đường đến Mạng 1 qua router B. Lúc này router D thấy rằng thông tin này tốt hơn thông tin báo Mạng 1 bị lỗi mà nó vừa nhận được từ router A lúc này. Do đó router D cập nhật lại thông tin này vào bảng định tuyến mà không biết rằng như vậy là sai .Lúc này, trên bảng định tuyến, router D có đường tới Mạng 1 là đi qua router C. Sau đó router D lấy bảng định tuyến vừa mới cập nhật xong gửi cho router A. Tương tự, router A cũng cập nhật lại đường đến Mạng 1 lúc này là qua

router D rồi gửi cho router Bvà E. Quá trình tương tự tiếp tục xảy ra ở router B,E. Khi đó, bất kỳ gói dữ liệu nào gửi tới Mạng 1 đều bị gửi lặp vòng từ router C tới router B tới router A tới router D rồi tới router C.

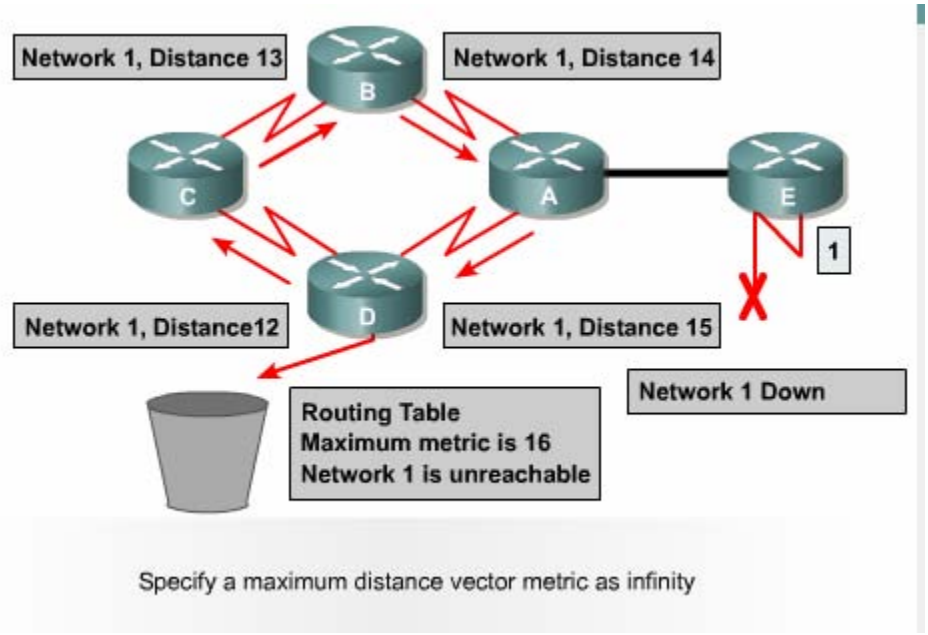
7.1.3. Định nghĩa giá trị tối đa

Việc cập nhật sai về Mạng 1 như trên sẽ bị lặp vòng như vậy hoài cho đến khi nào có một tiến trình khác cắt đứt được quá trình này. Tình trạng như vậy gọi là đếm vô hạn, gói dữ liệu sẽ bị lặp vòng trên mạng trong khi thực tế là Mạng 1 đã bị ngắt.

Với vectơ khoảng cách sử dụng thông số là số lượng hop thì mỗi khi router chuyển thông tin cập nhật cho router khác ,chỉ số hop sẽ tăng lên 1.Nếu không có biện pháp khắc phục tình trạng đếm vô hạn ,thì cứ như vậy chỉ số hop sẽ tăng lên đến vô hạn.

Bản thân thuật toán định tuyến theo vectơ khoảng cách có thể tự sữa lỗi được nhưng quá trình lặp vòng này có thể kéo dài đến khi nào đếm đến vô hạn. Do đó để tránh tình trạng lỗi này kéo dài, giao thức định tuyến theo vectơ khoảng cách đã định nghĩa giá trị tối đa.

Bằng cách này ,giao thức định tuyến cho phép vòng lặp kéo dài đến khi thông số định tuyến vượt qua giá trị tối đa. Ví dụ như hình vẽ dưới, khi thông số định tuyến là 16 hop lớn hơn giá trị tối đa là 15 thì thông tin cập nhật đó sẽ bị router huỷ bỏ. Trong bất kỳ trường hợp nào, khi giá trị của thông số định tuyến vượt qua giá trị tối đa thì xem như mạng đó là không đến được.

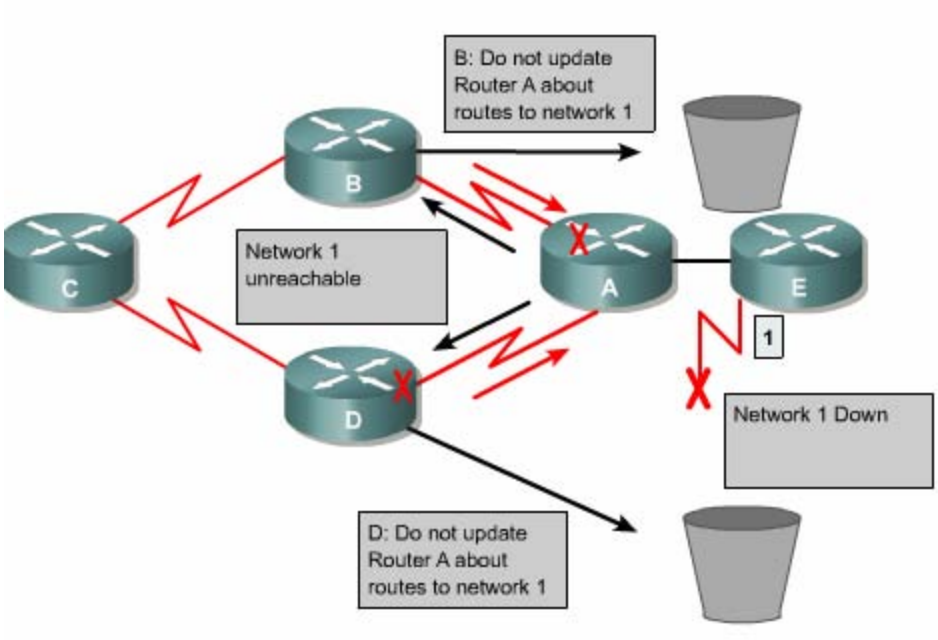


Hình 7.1.3

7.1.4. Tránh định tuyến lặp vòng bằng split horizone

Một nguyên nhân khác gây ra lặp vòng là router gửi lại những thông tin định tuyến mà nó vừa nhận được cho chính router đã gửi những thông tin đó. Phần sau đây sẽ phân tích cho các bạn thấy sự cố xảy ra như thế nào:

1. Router A gửi một thông tin cập nhật cho router B và D thông báo là Mạng 1 đã bị ngắt. Tuy nhiên router C vẫn gửi cập nhật cho router B là router C có đường đến Mạng 1 thông tin qua router D, khoảng cách của đường này là 4.
2. Khi đó router B tưởng lầm là router C vẫn có đường đến Mạng 1 mặc dù con đường này có thông số định tuyến không tốt bằng con đường cũ của router B lúc trước. Sau đó router B cũng cập nhật cho router A về đường mới đến Mạng 1 mà router B vừa mới nhận được.
3. Khi đó router A sẽ cập nhật lại là nó có thể gửi dữ liệu đến Mạng 1 thông qua router B. Router B thì định tuyến đến Mạng 1 thông qua router C. Router C lại định tuyến đến Mạng 1 thông qua router D. Kết quả là bất kỳ gói dữ liệu nào đến Mạng 1 sẽ rơi vào vòng lặp này.
4. Cơ chế split-horizon sẽ trách được tình huống này bằng cách: Nếu router B hoặc D nhận được thông tin cập nhật về Mạng 1 từ router A thì chúng sẽ không gửi lại thông tin cập nhật về Mạng 1 cho router A nữa. Nhờ đó, split-horizon làm giảm được việc cập nhật thông tin sai và giảm bớt việc xử lý thông tin cập nhật.



Hình 7.1.4

7.1.5. Route poisoning

Route poisoning được sử dụng để tránh xảy ra các vòng lặp lớn và giúp cho router thông báo thẳng là mạng đã không truy cập được nữa bằng cách đặt giá trị cho thông số định tuyến (số lượng hop chẳng hạn)lớn hơn giá trị tối đa.

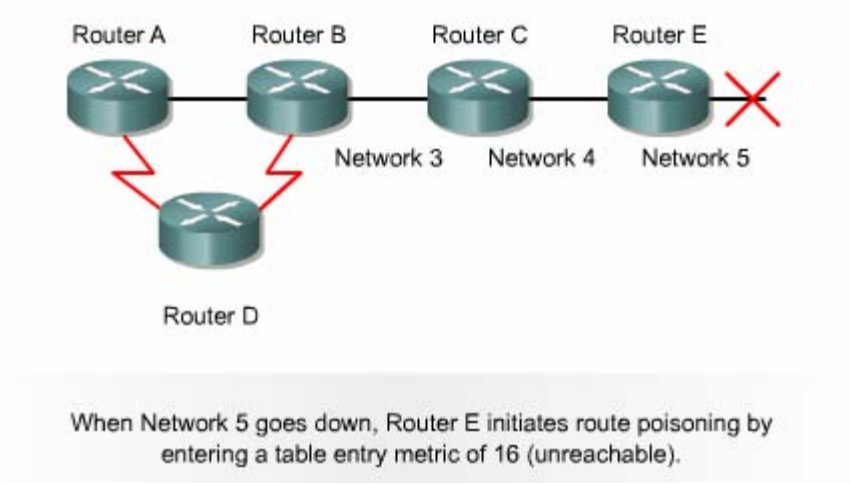
Ví dụ như hình 7.1.5 : khi Mạng 5 bị ngắt thì trên bảng định tuyến của router E giá trị hop cho đường đến Mạng 5 là 16,giá trị này có nghĩa là Mạng 5 không truy cập được nữa .Sau đó router E cập nhật cho router C bảng định tuyến này ,trong đó đường đến Mạng 5 có thông số hop là 16 được gọi là route poisoning .Sau khi router C nhận được cập nhật về route poisoning từ router E ,router C sẽ gửi ngược trở lại thông tin này cho router E .Lúc này ta gọi thông tin cập nhật về Mạng 5 từ router C gửi ngược lại cho router E là route poison reverse.Router C làm như vậy để đảm bảo là nó đã gửi thông tin route poisoning ra tất cả các đường mà nó có .

Khi route poisoning được sử dụng kết hợp với cập nhật tức thời sẽ giúp rút ngắn thời gian hội tụ giữa các router vì khi đó router không cần phải chờ hết 30 giây của chu kỳ cập nhật mới về route poisoning.

Tóm lại ,route poisoning có nghĩa là khi có một con đường nào đó bị ngắt thì router sẽ thông báo về con đường đó với thông số định tuyến lớn hơn giá trị tối đa

.Cơ chế route poisoning không hề gây mâu thuẫn với cơ chế split horizon .Split horizon có nghĩa là khi router gửi thông tin cập nhật ra một đường liên kết thì router không được gửi lại những thông tin nào mà nó vừa nhận vào từ đường liên kết đó.Bây giờ ,router vẫn gửi lại những thông tin đó nhưng với thông số định tuyến lớn hơn giá trị tối đa thì kết quả vẫn như vậy .Cơ chế này gọi là split horizon kết hợp với poison reverse.

Khi mạng 5 bị ngắt ,Router E sử dụng route poisoning bằng cách đặt giá trị 16 trên bảng định tuyến để cho biết mạng này không đến được nữa .



Hình 7.1.5

7.1.6 Trách định tuyến lặp vòng bằng cơ chế cập nhật tức thời

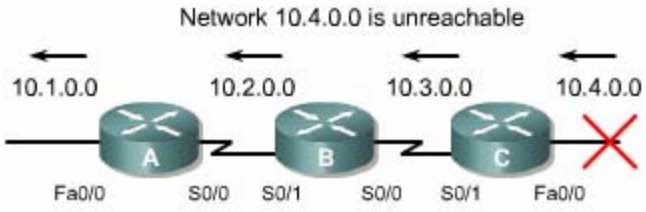
Hoạt động cập nhật bảng định tuyến giữa các router láng giềng được thực hiện theo chu kỳ .Ví dụ :cứ sau 30 giây RIP thực hiện cập nhật một lần .Ngoài ra còn có cơ chế cập nhật tức thời để thông báo về một thay đổi nào đó trong bảng định tuyến .Khi router phát hiện ra có một thay đổi nào đó trong cấu trúc thì nó lập tức gửi thông điệp cập nhật cho các router láng riềng để thông báo về sự thay đổi đó. Nhất là khi có một đường nào đó bị lỗi không truy cập được nữa thì router phải cập nhật tức thời thay vì đợi đến hết chu kỳ. Cơ chế cập nhật tức thời kết hợp với route poisoning sẽ đảm bảo cho tất cả các router nhận được thông tin khi có một đường nào đó bị ngắt trước khi thời gian holddown kết thúc.

Cơ chế cập nhật tức thời cho toàn bộ mạng khi có sự thay đổi trong cấu trúc mạng giúp cho các router được cập nhật kịp thời và khởi động thời gian holddown nhanh hơn.

Ví dụ như hình 7.1.6: router C cập nhật tức thời ngay khi mạng 10.4.0.0 không truy cập được nữa. Khi nhận được thông tin này, router B cũng phát thông báo về mạng 10.4.0.0 ra cổng S0/1. Đến lướt router A cũng sẽ phát thông báo ra cổng Fa0/0.

NetWordk 10.4.0.0 is unreachable

Với cập nhật tức thời, router sẽ gửi thông điệp ngay để thông báo sự thay đổi trong bảng định tuyến của mình



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

Hình 7.1.6

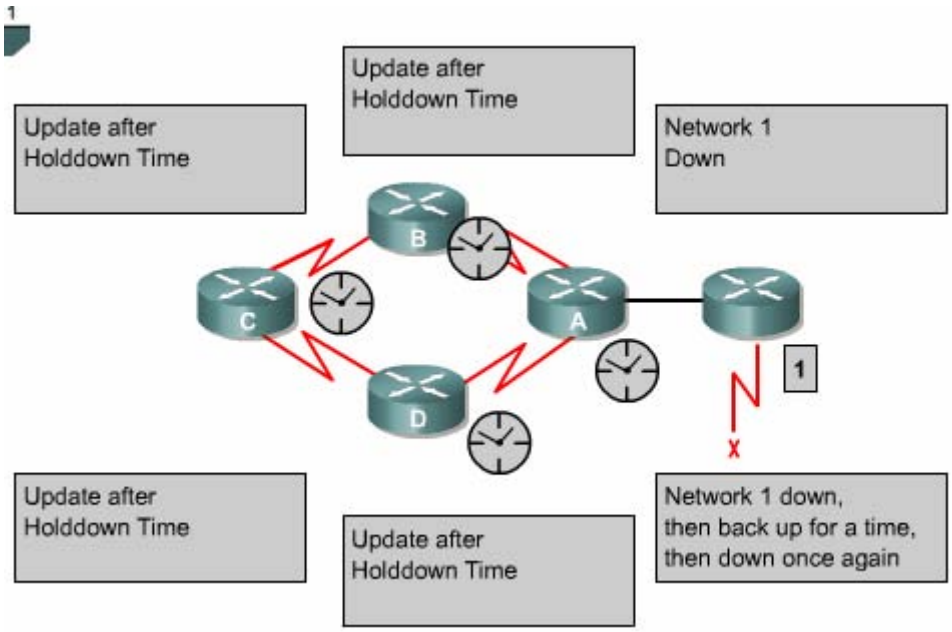
7.1.7. Tránh lặp vòng với thời gian holddown

Tình trạng lặp vòng đến vô hạn như đã đề cập ở phần 7.1.2 có thể tránh được bằng cách sử dụng thời gian holddown như sau:

Khi router nhận được từ router láng giềng một thông tin cho biết là một mạng X nào đó bây giờ không truy cập được nữa thì router sẽ đánh dấu vào con đường tới mạng X đó là không truy cập được nữa và khởi động thời gian holddown. Trong khoảng thời gian holddown này, nếu router nhận được thông tin cập nhật từ chính router láng riềng lúc nãy thông báo là mạng X đã truy cập lại được thì router mới cập nhật thông tin đó và kết thúc thời gian holddown.

Trong suốt thời gian holddown nết router nhận được thông tin cập nhật từ một router láng riêng khác (không phải là router láng giềng đã phát thông tin cập nhật về mạng X lúc nãy) nhưng thông tin này cho biết có đường đến mạng X với thông

số định tuyến tốt hơn con đường mà router trước đó thì nó sẽ bỏ qua, không cập nhật thông tin này. Cơ chế nay giúp cho router tránh được việc cập nhật nhầm những thông tin cũ do các router láng giềng chưa hay biết gì về việc mạng X đã không truy cập được nữa. Khỏng thời gian holddown bảo đảm cho tất cả các router trong hệ thống mạng đã được cập nhật xong về thông tin mới. Sau khi thời gian holddown hết thời hạn, tất cả các router trong hệ thống đều đã được cập nhật là mạng X không truy cập được nữa, khi đó các router đều có thể nhận biết chính xác về cấu trúc mạng. Do đó, sau khi thời gian holddown kết thúc thì các router lại cập nhật thông tin như bình thường.



Hình 7.1.7

7.2.RIP

7.2.1. Tiến trình của RIP

IP RIP được mô tả chi tiết trong 2 văn bản. Văn bản đầu tiên là RFC1058 và văn bản thứ 2 là Tiêu chuẩn Internet(STD)56.

RIP được phát triển trong nhiều năm bắt đầu từ phiên bản 1 (RIPv1)

RIP chỉ là giao thức định tuyến theo lớp địa chỉ cho đến phiên bản 2(RIPv2)

RIP trở thành giao thức định tuyến không theo lớp địa chỉ.

RIPv2 có những ưu điểm hơn như sau:

- Cung cấp thêm nhiều thông tin định tuyến hơn.
- Có cơ chế xác minh giữa các router khi cập nhật để bảo mật cho bảng định tuyến.
- Có hỗ trợ VLSM(variable Length Subnet Masking-Subnet mask có chiều dài khác nhau).

RIP tránh định tuyến lặp vòng đếm đến vô hạn bằng cách giới hạn số lượng hop tối đa cho phép từ máy gửi đến máy nhận, số lương hop tối đa cho mỗi con đường là 15. Đối với các con đường mà router nhân được từ thông tin cập nhật của router láng giềng, router sẽ tăng chỉ số hop lên 1 vì router xem bản thân nó cũng là 1 hop trên đường đi. Nếu sau khi tăng chỉ số hop lên 1 mà chỉ số này lớn hơn 15 thì router sẽ xem như mạng đích không tương ứng với con đương này không đến được. Ngoài ra, RIP cũng có những đặc tính tương tự như các giao thức định tuyến khác. Ví dụ như : RIP cũng có horizon và thời gian holddown để tránh cập nhật thông tin định tuyến không chính xác.

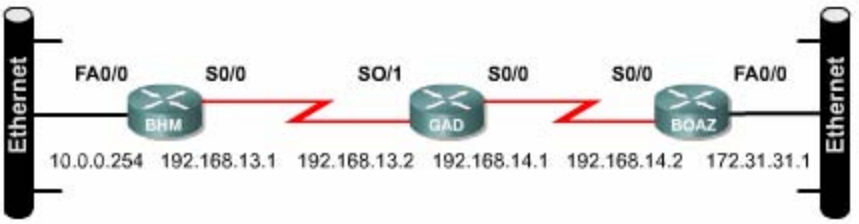
Các đặc điểm chính của RIP
• Là giao thức định tuyến theo vectơ khoảng cách. • Thông số định tuyến là số lương hop. • Nếu gói dữ liệu đến mạng đích có số lượng hop lớn hơn 15 thì gói dữ liệu đó sẽ bị huỷ bỏ. • Chu kỳ cập nhật mặc định là 30 giây.

7.2.2. Cấu hình RIP

Lênh router rip dùng để khởi động RIP. Lênh network dùng để khai báo những cổng giao tiếp nào của router được phép chạy RIP trên đó. Từ đó RIP sẽ bắt đầu gửi và nhận thông tin cập nhật trên các cổng tương ứng RIP cập nhật thông tin định tuyến theo chu kỳ. Khi router nhận được thông tin cập nhật có sự thay đổi nào đó thì nó sẽ cập nhật thông tin mới vào bảng định tuyến. Đối với những con đường tới mạng đích mà router học được từ router láng giềng thì nó sẽ tăng chỉ số hop lên 1 địa chi nguần của thông tin cập nhật này sẽ là địa chỉ trạm kế tiếp RIP

chỉ chon một con đường tốt nhất đến mạng đích, tuy nhiên nó cũng có thể sử dụng nhiều con đường có chỉ số bằng nhau đến cùng 1 đích.

Chúng ta có thể cấu hình cho RIP thực hiên cập nhật tức thời khi cấu trúc mạng thay đổi bằng lệnh ip rip triggered. Lệnh này chỉ áp dụng cho cổng serial của router. Khi cấu trúc mạng thay đổi, router nào nhận biết được sự thay đổi đầu tiên sẽ cập nhật vào bảng định tuyến của nó trước, sau đó nó lập tức gửi thông tin cập nhật cho các router khác để thông báo về sự thay đổi đó. Hoạt động này là cập nhật tức thời va nó xảy ra hoàn toàn độc lập với cập nhật đinh kỳ. hình 7.2.2 là một ví dụ về cấu hình của 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
```

Hình 7.2.2

- BHM(config)#router rip- chọn RIP làm giao thức định tuyến cho router.
- BHM(config- router)#network10.0.0.0- khai báo mạng kết nối trực tuyến vào router.
- BHM (config- router) #network 192.168.13.0-khai báo mạng kết nối trực tuyến vào router.

Các cổng trên router kết nối vào mạng 10.0.0.0 và 192.168.13.0 sẽ thực hiện gửi và nhận thông tin cập nhật về định tuyến.

Sau khi đã khởi động RIP trên các mạng rồi chúng ta có thể thực hiện thêm một số cấu hình khác. Những cấu hình này không bắt buộc phải làm, chúng ta chỉ cấu hình thêm nếu thấy cần thiết:

- Điều chỉnh các thông số định tuyến.
- Điều chỉnh các thông số về thời gian hoạt động của RIP.
- Khai báo phiên bản của RIP mà ta đang sử dụng(RIPv1 hay RIPv2).
- Cấu hình cho RIP chỉ gửi thông tin định tuyến rút gọn cho một cổng nào đó.
- Kiểm tra thông tin định tuyến IP rut gọn.
- Cấu hình cho IGRP và RIP chạy đồng thời .
- Không cho phép RIP nhận thông tin cập nhật từ một địa chỉ IP nào đó.
- Mở hoặc tắt chế độ split horizon.
- Kết nối RIP vào mạng WAN.

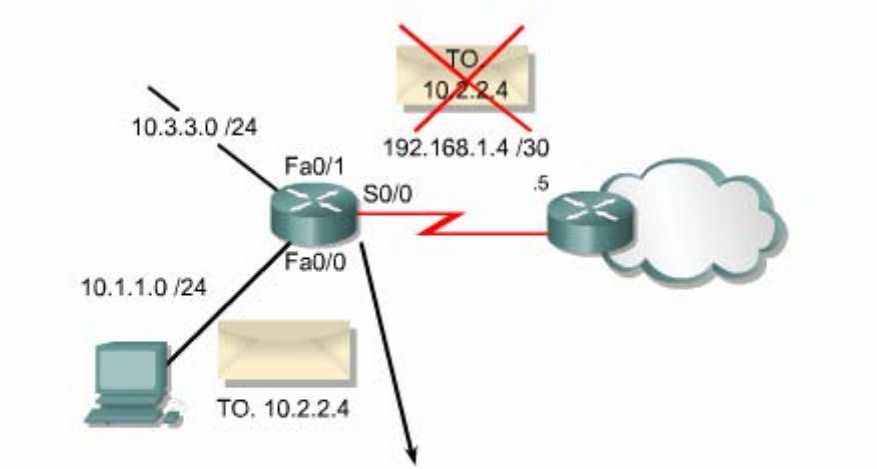
Tóm lại, để cấu hình RIP, chúng ta có thể bắt đầu từ chế độ cấu hình toàn cục như sau:

- Router(config)# router rip – khởi động giao thức định tuyến RIP.
- Router(config- router)#network network- number- khai báo các mạng mà RIP được phép chạy trên đó.

7.2.3. Sử dụng lệnh ip classless.

Khi router nhận được gói dữ liệu có địa chỉ đích là một subnet không có trên bảng định tuyến của router. Trên bảng định tuyến của router không có chính xác subnet với subnet đích của gói dữ liệu. Ví dụ: một tổ chức sử dụng địa chỉ mạng 10.10.0.0/16, khi đó subnet 10.10.10.0/24 có supernet là 10.10.0.0/16. Trong trường hợp như vậy, ta dung lệnh ip classless để router không hủy bỏ dữ liệu mà sẽ chuyển gói ra đường đến địa chỉ supernet, nếu có. Đối với phần mền Cisco IOS phiên bản 11.3 trở về sau, mặc định là lệnh ip classlet đã được chạy trong cấu hình của router. Nếu bạn tắt lệnh này đi thì dùng lệnh NO của câu lệnh này.

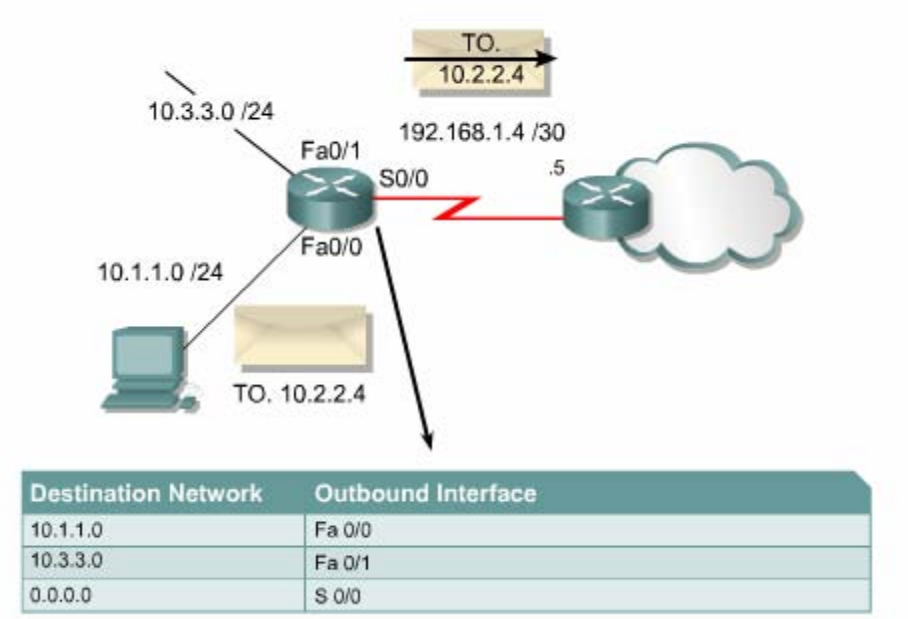
Tuy nhiên, nếu không có chức năng này thì tất cả các gói có địa chỉ đích là một subnet có cùng supernet với các địa chỉ mạng khác của router nhưng lại không có trong bảng định tuyến. Đây chính là đặc điểm quan trọng của giao thức định tuyến theo lớp. Nếu một địa chỉ mạng lớn được chia thành các subnet con chứ không có toàn bộ các subnet. Khi đó gói dữ liệu nào có địa chỉ đích là một subnet nằm trong địa chỉ mạng lớn nhưng lại không có trên bảng định tuyến của router thì router sẽ hủy bỏ.



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

Hình 72.2.3a.khi không có lệnh ip classless.

Cơ chế này bị nhầm lẫn nhất khi router có cấu hình đường mặc định. Từ một địa chỉ mạng lớn chia thành nhiêu subnet con. Kết nối trực tiếp vào router chỉ có một số subnet. Khi router xây dựng bảng định tuyến, trên bảng định tuyến đương nhiên có các subnet của mạng kết nối trực tiếp vào router. Còn những subnet nào không có thì router coi như subnet đó không tồn tại. Do đó, khi router nhận được gói dữ liệu có địa chỉ đích là một subnet không có trên bảng định tuyến nhưng lại có cùng supernet với các mạng kết nối trực tiếp vào router thì router xem như mạng đích đó không tồn tại và hủy bỏ gói dữ liệu cho dù trên bảng định tuyến của router có cấu hình đường mặc đinh. Lệnh ip classless sẽ giải quết vấn đề này băng cách cho phép router không cần quan tâm đến lớp của địa chỉ đích nữa. khi đó router không tìm thấy được cụ thể mạng đích trên bảng định tuyến thì nó sẽ sử dụng đương mặc định để chuyển gói đi.



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

Hình 7.2.3b: Khi có lệnh ip classless.

7.2.4. những vấn đề thường gặp khi cấu hình RIP.

Router định tuyến theo RIP phải dựa vào các router láng giềng để học thông tin đến các mạng mà không kết nối trực tiếp vào router. RIP sử dụng thuật toán đinh tuyến theo vectơ khoảng cách đề có nhược điểm chính tốc độ hội tụ chậm. Trạng thái hội tụ là khi tất cả các router trong hệ thống mạng đều có thông tin đinh tuyến về hệ thống mạng giống nhau và chính xác.

Các giao thức định tuyến theo vectơ khoảng cách thường gặp vấn đề về định tuyến lặp vòng và đếm đến vô hạn. Đây là hậu quả khi các router chưa được hội tụ nên truyền cho nhu những thông tin cũ chưa được cập nhật đúng.

Để giải những vấn đề này RIP sử dụng những kỹ thật sau

- Định nghĩa giá trị tối đa
- Split horizon.
- Poison reverse.
- Thời gian holddown.
- Cập nhật tức thời.

Có một số kỹ thuật đòi hỏi bạn phải cấu hình còn một số khác thì không cần cấu hình gì cả hoặc chỉ cần cấu hình một chút thôi.

RIP giới hạn số hop tối đa là 15. Bất kỳ mạng đích nào có số hop lớn hơn 15 thì xem như mạng đó không đếm được. Điều này làm cho RIP bị hạn chế không sử dụng được cho những hệ thống mạng lớn nhưng nó giúp cho RIP tránh được lỗi đếm đến vô hạn.

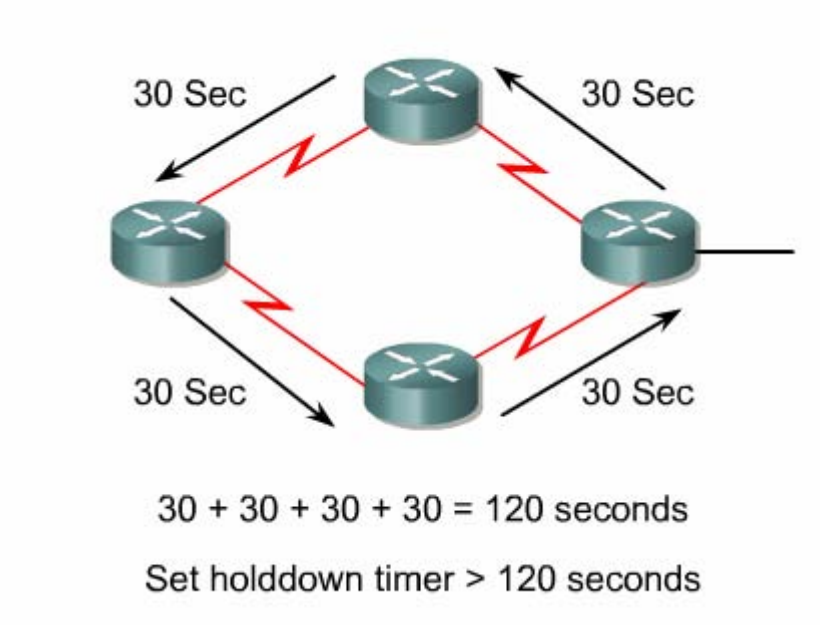
Luật split horizon la: khi gửi thông tin cập nhật ra một hướng nào đó thì không gửi lại những thông tin mà router đã nhận được từ hường đó. Trong một số cấu hình mạng thì bạn cần phải tắt cơ chế split horizon:

GAD (config-if)#no ip split- horizon

Thời gian holddown là một thông số mà bạn có thể thay đổi nếu cần. Khoảng thời gian holddown giúp cho router tránh bị lặp vòng đếm đến vô hạn nhưng đồng thời nó cũng làm tăng thời gian hội tụ giữa các router. Trong khoảng thời gian này, router không cập nhật những đường nào có thông số định tuyến không tốt bằng con đường mà router có trước đó, như vậy thì có khi có đường khác thay thế cho đường cũ thật nhưng router cũng không cập nhật. Thời gian holddown mặc định của RIP là 180 giây. Bạn có thể điều chỉnh thời gian holddown ngắn lại đêt tăng tốc độ hội tụ nhưng bạn nên cân nhắc kỹ. Thời gian holddown lý tưởng là phải dài hơn khoảng thời gian dài nhất có thể để cho toàn bộ hệ thống mạng được cập nhật song. Ví dụ như hình dưới, chúng ta có 4 router. Nếu mối router có thời gian cập nhật là 30 giây thì thời gian tối đa để cho cả 4 router cập nhật xong là 120 giây như vậy thời gian holddown phải dài hơn 120 giây.

Đêt thay đổi thời gian holddown bạn dùng lệnh sau

Router(config- router)#timers basic update invalid holddown flush[sleeptime]



Hình 7.2.4

Một lý do khác làm ảnh hưởng đến tốc độ hội tụ là chu kỳ cập nhật. chu kỳ cập nhật mặc định của RIP là 30 giây . Bạn có thể điều chỉnh cho chu kỳ cập nhật dài hơn để tiếp kiệm băng thông đường truyền hoặc rút ngắn chu kỳ cập nhật lại để tăng tốc độ hội tụ.

Để thay đổi chu kỳ cập nhật, bạn dụng lệnh sau GAD(config- router)#update-timer seconds.

Còn một vấn đề nữa mà ta thường gặp đối với giao thức định tuyến là ta không muốn cho các giao thức này gửi các thông tin cập nhật về định tuyến ra một cổng nào đó. Sau khi bạn nhập lệnh network để khai báo địa chỉ mạng là lập tức RIP bắt đầu gửi các thông tin định tuyến ra tất cả các cổng có địa chỉ mạng nằm trong mạng mà bạn vừa khai báo. Nhà quản trị mạng có thể không cho phép gửi thông tin cập nhật về định tuyến ra một cổng nào đó bằng lệnh **passive – interface**.

GAD(config- router)#passive- interface Fa0/0.

RIP là giao thức broadcast. Do đó, khi muốn chạy RIP trong mạng non-broadcast như Frame Relay thì ta cần phải khai báo các router RIP láng giềng bằng lệnh sau:

GAD(config- router) # neighbor ip address

Phần mền Cisco IOS mặc nhiên nhận gói thông tin của cả RIP phiên bản 1 và 2 nhưng chỉ gửi đi gói thông tin bằng RIP phiên bản 1. Nhà quản trị mạng có thể cấu hình cho router chỉ gửi và nhận gói phiên bản 1 hoặc là chỉ gửi gói phiên bản 2…bằng các lệnh sau:

GAD(config- router) # version {1/2}

GAD(config- if) # ip rip send version 1

GAD(config- if) # ip rip send version 2

GAD(config- if) # ip rip send version 1 2

GAD(config- if) # ip rip receive version 1

GAD(config- if) # ip rip receive version 2

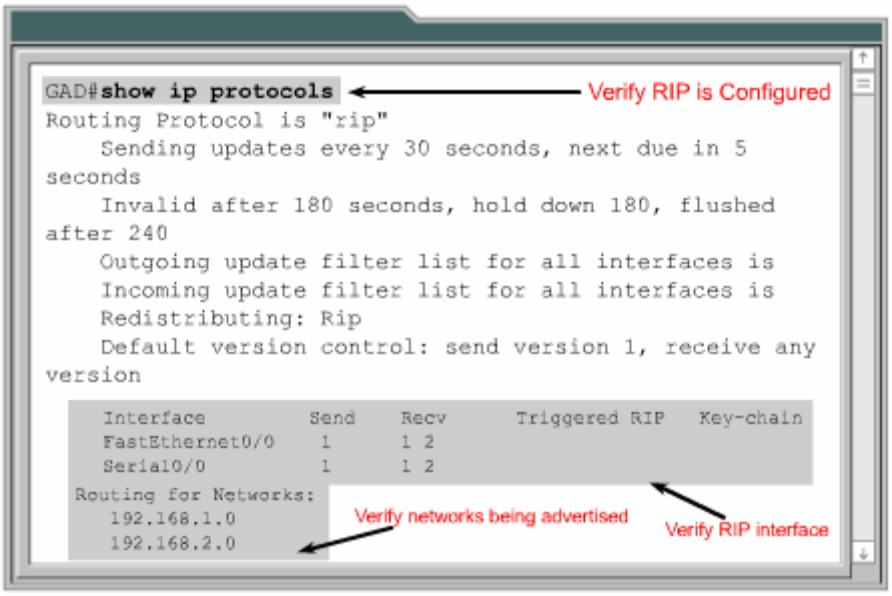
GAD(config- if) # ip rip receive version 1 2

7.2.5.kiểm tra cấu hình RIP

Có nhiều lệnh có thể sử dụng để kiểm tra cấu hình RIP có đúng hay không. Trong đó hai lệnh thường đước sử dụng nhiều nhất là **Show ip route và show ip protocols.**

Lệnh **show ip protocols** sẽ hiển thị các giao thức định tuyến IP đang được chạy trên router. Kết quả hiển thị của lệnh này có thể giúp bạn kiểm tra được phần lớn cấu hình của RIP nhưng chưa phải là đầy đủ, toàn bộ. sau đây là một số điểm bạn cần chú ý kiểm tra:

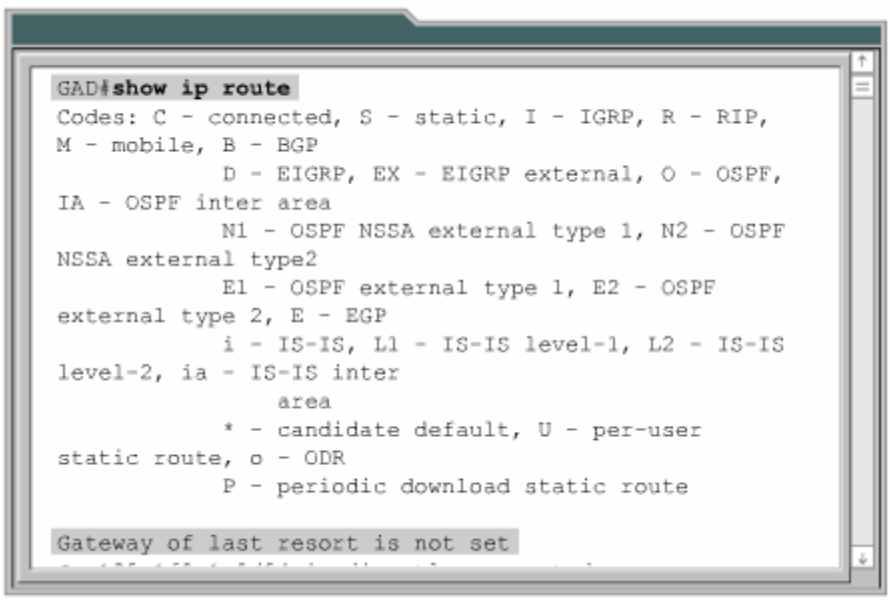
- Có đúng là giao thức định tuyến RIP đã được cấu hình hay không.
- RIP được cấu hình để gửi và nhận thông tin cập nhật trên các cổng vào, có chính xác hay không.
- Các địa chỉ mạng được khai báo trên router để chạy RIP có đúng hay không.



Hình 7.2.5a.

Lệnh **show ip router** được sử dụng để kiểm tra xem những đường đi mà router học được từ các router RIP láng giềng có được cài đặt vào bảng định tuyến không trên. Trên kết quả hiển thị bảng định tuyến, bạn kiểm tra các đường có đánh dấu bằng chữ "R" ở đầu dòng là những đường mà router học được từ các router RIP láng giềng. Bạn cũng nên nhớ rằng các router luôn có một khoảng thời gian để hội tụ với nhau, do đó các thông tin mới có thể chưa được hiển thị ngay trên bảng định tuyến được. Ngoài ra còn có một số lệnh khác mà bạn có thể sử dụng để kiểm tra cấu hình RIP :

- Show interface interface.
- Show ip interface interface.
- Show running –config

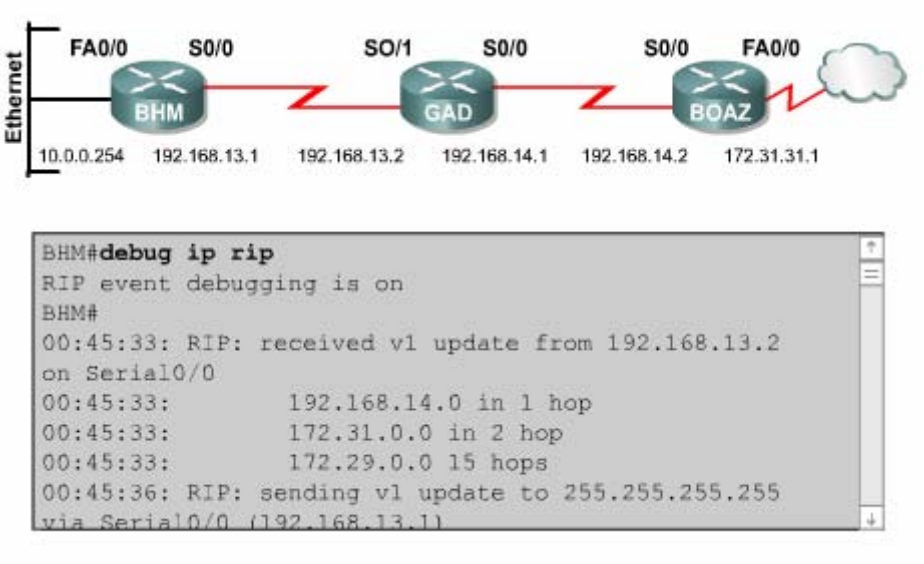


Hình 7.2.5b.

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

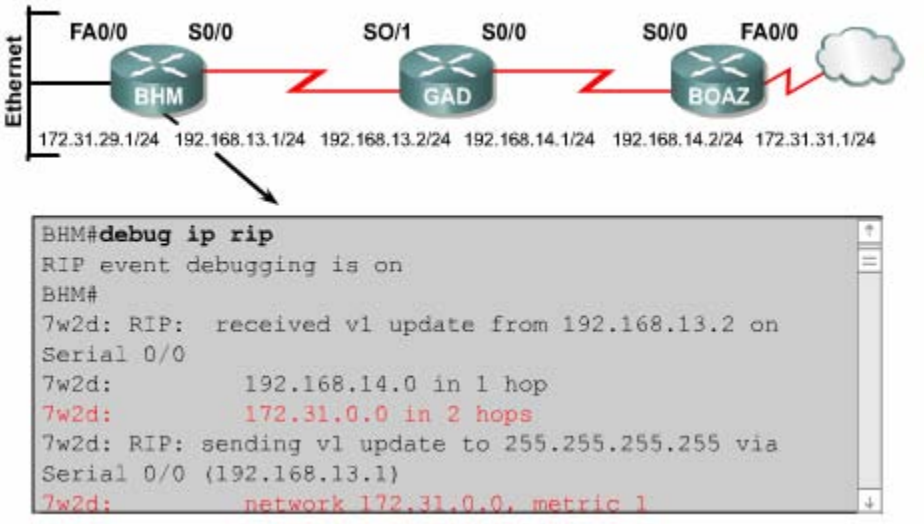
Hầu hết các lỗi cấu hình RIP đều do khai báo câu lệnh network sai, subnet không liên tục hoặc là do split horizon. Lệnh có tác dụng nhất trong việc tìm lỗi của RIP trong hoạt động cập nhật là lệnh debug ip rip

Lệnh debug ip rip sẽ hiển thị tất cả các thông tin định tuyến mà RIP gửi và nhận. Ví dụ trong hình 7.2.6a cho thấy kết quả hiển thị của lệnh debug ip rip. Sau khi nhận được thông tin cập nhật , router sẽ xử lý thông tin đó rồi sau đó gửi thông tin mới vừa cập nhật ra các cổng. Trong hình 7.2.6a cho thấy router chạy RIP phiên bản 1 và RTP gửi cập nhật theo kiểu broadcast(địa chỉ broadcast 255.255.255.255). Số trong ngoặc đơn là địa chỉ nguần của gói thông tin cập nhâth RIP.

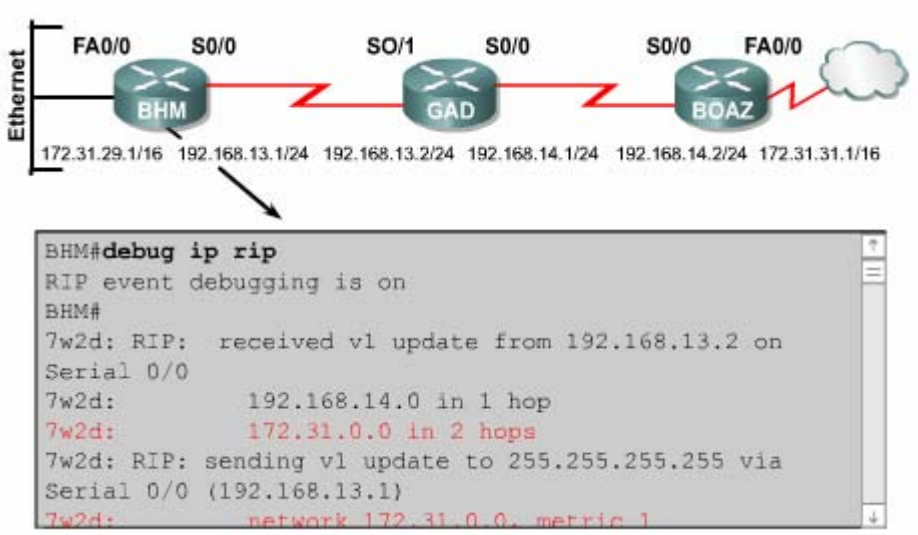


Hình 7.2.6a

Có rất nhiều điểm quan trọng mà bạn cần chú ý trong kết quả hiển thị của lênh debug ip rip. Một số vấn đề phải ví dụ như subnet không liên tục hay trùng subnet, có thể phát hiện được nhờ lệnh này. Trong những trường hợp như vậy bạn sẽ thấy là cùng một mạng đích nhưng router gửi thông tin đi thì mạng đích đó lại có thông số đinh tuyến thấp hơn so với khi router nhận vào trước đó.



Hình 7.2.6b. Subnet không liên tục



Hình 7.2.6c: Trùng Subnet

Ngoài ra còn một số lệnh có thể sử dụng để xử lý sự cố của RIP:

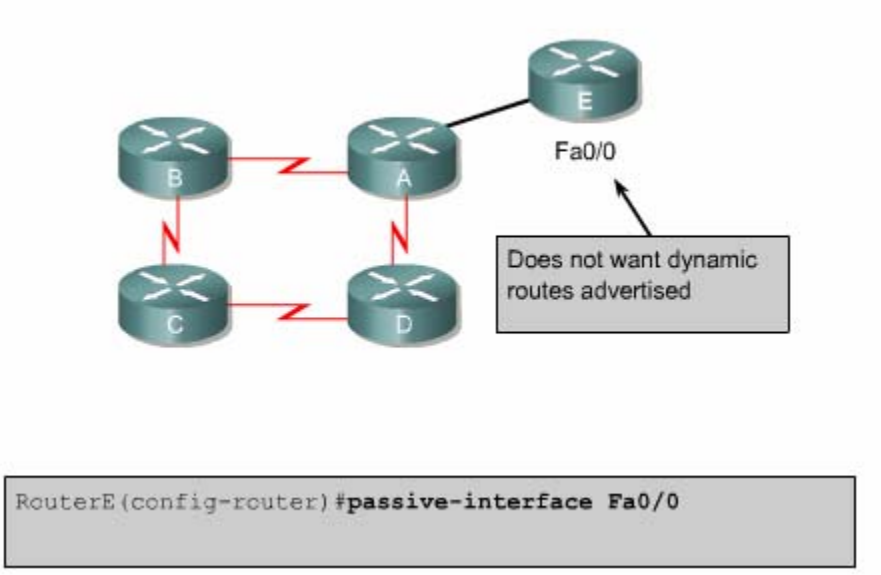
- Show ip database.
- Show ip protocols(summary).
- Show ip route.
- Debug ip rip{ events}.
- Show ip interface brief.

7.2.7. Ngăn không cho router gửi thông tin định tuyến ra một cổng giao tiếp

Router có thể thực hiện chọn lọc thông tin định tuyến khi cập nhật hoặc khi gửi thông tin cập nhật. Đối với router sử dụng giao thức định tuyến theo vectơ khoảng cách, cơ chế này có tác dụng vì router định tuyến dựa trên các thông tin định tuyến nhận được từ các router láng giềng. Tuy nhiên, đối với các router sử dụng giao thức định tuyến theo trạng thái đường liên kết thì cơ chế trên không hiệu quả vì các giao thức định tuyến này quyết định chọn đường đi dựa trên cơ sở dữ liệu về trạng thái các đường liên kết chứ không dựa vào thông tin định tuyến nhận được. Chính vì vậy mà cách thực hiện để ngăn không cho router gửi thông tin định tuyến ra một cổng giao tiếp được đề cập dưới đây chỉ sử dụng cho các giao thức định tuyến theo vectơ khoảng cách như RIP, IGRP thôi.

Bạn có thể sử dụng lệnh passive interface để ngăn không cho router gửi thông tin cập nhật về định tuyến ra một cổng nào đó. Làm như vậy thì bạn sẽ ngăn được hệ thống mạng khác học được các thông tin định tuyến trong hệ thống của mình.

Đối với RIP và IGRP, lênh passive interface sẽ làm cho router ngưng việc gửi thông tin cập nhật về định tuyến cho một router láng giềng nào đó, nhưng router vẫn tiếp tục lắng nghe và nhận thông tin cập nhật từ router láng giềng đó.



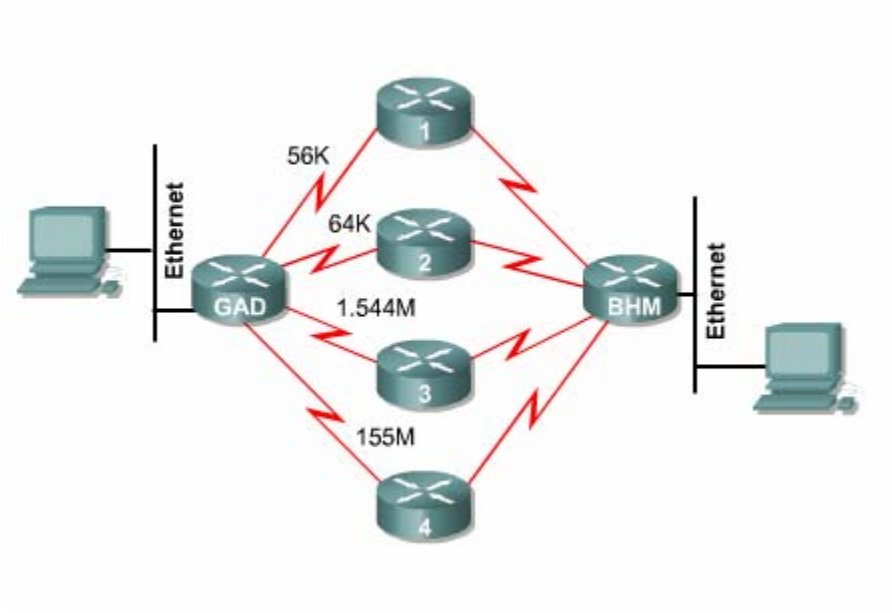
Hình 7.2.7

7.2.8. Chia tải với RIP

Router có thể chia tải ra nhiều đường khi có nhiều đường tốt đến cùng một đích. Bạn có thể cấu hình bằng tay cho router chia tai ra các đường hoặc là các giao thức định tuyến động có thể tự tính toán để chia tải.

RIP có khả năng chia tải ra tối đa là sáu đường có chi phí bằng nhau, còn mặc định thì RIP chỉ chia ra làm 4 đường. RIP thực hiện chia tải bằng cách sử dụng lần lượt và luân phiên từng đường.

Trong hình7.2.8a là ví dụ cho ta thấy RIP chia tải ra 4 đường có chi phí bằng nhau. Đầu tiên router bắt đầu với đường số 1 rồi sau đó lần lượt các đường 2-3-4 rồi1-2-3-4-1 và cứ tiếp tục luân phiên như vậy. vì thông số định tuyến của RIP là số lượng hop lên các đường này được xem là như nhau, RIP không cần quan tâm đến tốc độ của mỗi đường. Do đó đường 56kbps cũng giống như đường 155Mbps.



Hình 7.2.8a

Trong hình 7.2.8b là ví dụ về kết quả hiển thị của lệnh show ip route. Trong đó, bạn thấy có hai phần, mỗi phần mô tả về một đường. Trong phần mô tả về đường thứ hai có dấu(*) ở đầu dòng. Dấu (*) này cho biết con đường này là con đường kế tiếp sẽ được sử dụng.

```
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
```

Hình 7.2.8b

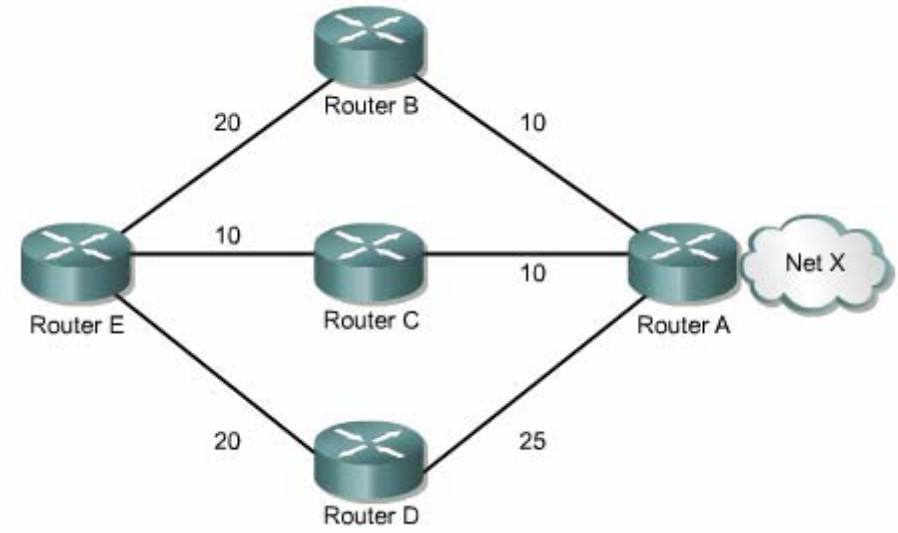
7.2.9. Chia tải cho nhiều đường

Router có khả năng chia tải ra nhiều đường để chuyển các gói dữ liệu đến cùng mục đích. Chúng ta có thể cấu hình bằng tay cho router thực hiện chia tải hoặc là các giao thức định tuyến động như RIP ,IGRP,EIGRP và OSPF sẽ tự động tính toán.

Khi router nhận được thông tin cập nhật về nhiều đường khác nhau đến cùng một đích thì router sẽ chọn đường nào có chỉ số tin cậy(Admintrative distance) nhỏ nhất để đặt vào bảng định tuyến. Trong trường hợp các đường này có cùng chỉ số tin cậy thì router sẽ chon đường nào có chi phí thấp nhất hoặc là đường nào có thông số định tuyến nhỏ nhất. Mỗi giao thức định tuyến sẽ có cách tính chi phí khác nhau và bạn cần phải cấu hình các chi phí này để router thực hiện chia tải.

Khi router có nhiều đường có cùng chỉ số tin cậy và cùng chi phí đến cùng một đích thì router sẽ thực hiện việc chia tải. Thông thường thì router có khả năng chia tải đến 6 đừong có cùng chi phí(giới hạn tối đa số đường chia tải là phụ thuộc vào bảng định tuyến của Cisco IOS), tuy nhiên một số giao thức định tuyến nội (IGP) có thể có giới hạn riêng. Ví dụ như EIGRP chỉ cho phép tối đa là 4 đường.

Mặc định thì hầu hết các giao thức định tuyến IP đều chia tải ra 4 đường. Đường cố định thì chia tải ra 6 đường. Chỉ riêng BGP là ngoại lệ, mặc định của BGP là chỉ cho phép định tuyến 1 đường đến 1 đích.



Hình 7.2.9a

Số đường tối đa mà router có thể chia tải là từ 1 đến 6 đường. Để thay đổi số đường tối đa cho phép bạn sử dụng lệnh sau:

Router(config- router) #maximum-paths[number].

IGRP có thể chia tải lên tối đa là 6 đường. RIP dựa vào số lượng hop để chọn đường chia tải, trong khi IGRP thì dựa vào băng thông để chọn đường chia tải.

Ví dụ như hình 7.2.9a, có ba đường đến mạng X :

- Từ E qua B qua A, thông số định tuyến là 30.
- Từ E qua C qua A , thông số định tuyến là 20.
- Từ E qua D qua A, thông số định tuyến là 45.

Router E sẽ chọn đường thứ 2 vì đường E –C-A có thông số định tuyến 20 là nhỏ nhất.

Khi định tuyến IP, Cisco IOS có hai cơ chế chia tải là: chia tải theo gói dữ liệu và chia tải theo địa chỉ đích. Nếu router chuyển mạch theo tiến trình thì router sẽ chia gói dữ liệu ra các đường. cách này gọi là chia tải theo gói dữ liệu. Còn nếu router chuyển mạch nhanh thì router sẽ chuyển tất cả gói dữ liệu đến cùng mục đích ra một đường. Các gói dữ liệu đến host khác nhưng trong cùng một mạng đich thì sẽ tải ra đường kế tiếp. Cách này gọi là chia tải theo địa chỉ đích.

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

Hình 7.2.9b

Đường cố định là đường do người quản trị cấu hình cho router chuyển gói tới mạng đích theo đường mà mình muốn. Mặt khác, lệnh để cấu hình đường cố định cũng được sử dụng để khai báo cho đường mặc định. Trong trường hợp router

không tìm thấy đường nào trên bảng định tuyến để chuyển gói đến mạng đích thì router sẽ sử dụng đường mặc định.

Router chạy RIP có thể nhận được thông tin về đường mặc định từ những thông tin cập nhật của các router RIP láng giềng khác. Hoặc là bản thân router được cấu hình đường mặc định sẽ cập nhật thông tin định tuyến này cho các router khác.

Bạn có thể xóa đường cố định bằng lệnh no ip route. Người quản trị mạng có thể cấu hình đường cố định bên cạnh định tuyến động. Mỗi một giao thức định tuyến động có 1 chỉ số tin cậy(AD).Người quản trị mạng có thể cấu hình một đường cố định tới cùng mạng đích với đường định tuyến động nhưng với chỉ số AD lớn hơn chỉ số AD của giao thức định tuyến động tương ứng. Khi đó đường định tuyến động có chỉ sốAD nhỏ hơn lên luôn luôn được router chọn lựa trước. Khi đường định tuyến động bị sự cố không sử dụng được nữa thì router sẽ sử dụng tới đường định tuyến cố định để chuyển gói đến mạng đích.

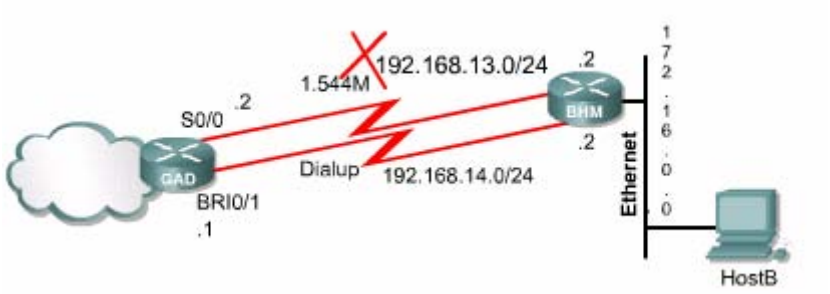
Nếu bạn cẩu hình đường cố định chỉ ra một cổng mà RIP cũng chạy trên cổng đó thì RIP sẽ gửi thông tin cập nhật về đường cố định này cho toàn bộ hệ thống mạng. Vì khi đó, đường cố định đó được xem như là kết nối trực tiếp vào router lên nó không còn bản chất là một đừong cố định nữa. Nếu bạn cấu hình đường cố định chỉ ra một cổng mà RIP không chạy trên cổng đó thì RIP sẽ không gửi thông tin cập nhật về đường cố định đó, trừ khi bạn phải cấu hình thêm lênh redistribute static cho RIP.

Khi một cổng giao tiếp bị ngắt thì tất cả các đường cố định chỉ ra cổng đó đều bị xóa bởi bảng định tuyến. Tương tự như vậy khi router không còn xác định được trạm kế tiếp trên đường cố định cho gói dữ liệu tới mạng đích thì đường cố định đó cũng sẽ bị xóa khỏi bảng định tuyến.

Trong hình 7.2.10a và 7.2.10b chúng ta thấy khi đường định tuyến động của RIP bị sự cố thì đường cố định mà ta đã cấu hình cho router GAD được sử dụng thay thê. Đường cố định như vậy được gọi là đừong cố định dự phòng. Như trong ví dụ này chúng ta thấy là đường cố định được cấu hình với chỉ số AD là 130 lớn hơn chỉ số AD của RIP (120). Bên cạch đó, bạn nên nhớ là trên router BHM cũng cần cấu hình đường mặc định tương ứng.


```
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
```

Hình 7.2.10a




```
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
```

Hình 7.2.10b

7.3.IGRP

7.3.1. Đặc điểm của IGRP

IGRP là một giao thức định tuyến nội và định tuyến theo vectơ khoảng cách. Giao thức định tuyến theo vectơ khoảng cách chọn lựa đường đi bằng cách so sách vectơ khoảng cách. Router chạy giao thức định tuyến theo vectơ khoảng cách thực hiện bảng đinh tuyến theo định kỳ cho các router láng giềng. Dựa vào thông tin cập nhật, router thực hiện 2 nhiệm vụ sau :

- Xác định mạng đích mới.
- Cập nhật sự cố về đường đi trên mạng

IGRP là giao thức định tuyến theo vectơ khoảng cách do Cisco phát triển nên. IGRP thực hiện cập nhật theo chu kỳ 90 giây / lần và chỉ gửi thông tin cập nhật trong phạm vi một hê tự quản. Sau đây là các đặc điểm chính của IGRP:

- Khả năng thích ứng với các cấu trúc mạng phức tạp và không xác định.
- Khả năng linh hoạt với các đặc tính băng thông và độ trễ khác nhau.
- Khả năng mở rộng cho hệ thống mạng lớn.

Mặc định thì IGRP sử dụng băng thông và độ trễ làm thông số định tuyến. Ngoài ra IGRP còn có thể cấu hình để sử dụng nhiều thông số khác để định tuyến. Sau đây là các thông số mà IGRP có thể sử dụng để định tuyến:

- Băng thông.
- Độ trễ.
- Độ tải.
- Độ tin cậy

7.3.2 Thông số định tuyến của IGRP

Bạn dùng lệnh show ip protocols để xem các thông số, các thông tin về mạng và các chính sách chọn lọc của các giao thức định tuyến đang hoạt động trên router. Trong đó bạn sẽ thấy được cách tính toán thông số định tuyến của IGRP như trong hình 7.3.2. Mỗi một thông số có hệ số từ K1 – K5. K1 là hệ số của băng thông, K3 là hệ số của độ trễ. Mặc định thì K1 và K3 có giá trị là 1, còn K2 , K4 và K5 có giá trị là 0.

Việc tính toàn thông số định tuyến từ nhiều thông số của đường đi như vậy sẽ cho kết quả chính xác hơn so với RIP chỉ dựa vào một thông số là số lượng hop. Nguyên tắc thì đường nào có thông số định tuyến nhỏ nhất là đường tốt nhất.:

Sau đây là các thông số của đường đi mà IGRP sử dụng để tính toán thông số định tuyến :

- Băng thông :Giá trị băng thông thấp nhất của đường truyền .
- Độ trễ :Tổng độ trễ dọc theo đường truyền .
- Độ tin cậy :Độ tin cậy trên một đường liên kết đến đích được xác định dựa trên hoạt động trao đổi các thông điệp keepalive.

```
Router>show ip protocols
Routing Protocol is igrp 300
  Sending updates every 90 seconds, next due in 55
seconds
  Invalid after 270 seconds, hold down 280, flushed
after 360
  Outgoing update filter list for all interfaces is
not set
  Incoming update filter list for all interfaces is
not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  IGRP maximum hopcount 100
  IGRP maximum metric variance 1
  Redistributing igrp 300
  Routing for Networks:
    183.8.0.0
    144.253.0.0
  Routing Information Sources
    Gateway                 Distance        Last
Update
    144.253.100.1           100              0:00:52
    183.8.128.12            100              0:00:43
    183.8.64.130            100              0:01:02
  Distance: (default is 100)
-- More --
```

- Độ tải :Độ tải của đường truyền tính bằng bit/ giây .
- MTU :Đơn vị truyền tối đa trên đường truyền .

Thông số định tuyến được tính dựa vào một công thức tính từ 5 thông số trên.Mặc định thì trong công thức này chỉ có băng thông và độ trễ .Còn những thông số khác thì chỉ được sử dụng khi được cấu hình .Bạn có thể cấu hình băng thông và độ trễ cho cổng giao tiếp của router.Bạn dùng lệnh **show ip route** sẽ xem được giá trị của thông số định tuyến của IGRP đặt trong ngoặc vuông .Đường nào có băng thông lớn hơn sẽ có thông số định tuyến nhỏ hơn , tượng tự đường nào có độ trễ ít hơn thì sẽ có thông số định tuyến nhỏ hơn.

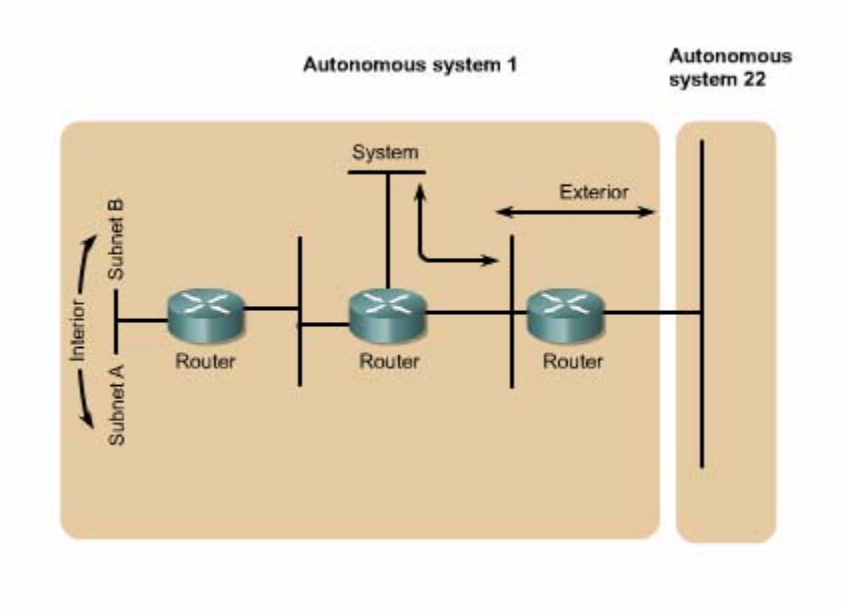
7.3.3. Các loại đường trong IGRP

IGRP thực hiện quảng bá những loại đường sau :

- Đường nội bộ.
- Đường hệ thống.
- Đường ngoại vi.

Đường nội bộ là những đường chỉ đi giữa các subnet kết nối vào cùng một cổng của router .Nếu một cổng giao tiếp của router kết nối vào một mạng không có chia thành nhiều subnet thì router không còn có đường nội bộ trong mạng đó .

Đường hệ thống là những đường đi giữa các mạng trong cùng một hệ tự quản.Router hoc về đường hệ thống bằng cách nhận biết các mạng kết nối trực tiếp vào nó và học từ các thông tin cập nhật từ các router IGRP khác .Trong IGRP ,các thông tin về đường hệ thống không có thông tin về subnet tương ứng.



Hình 7.3.3

Đường ngoại vi là những đường đi ra ngoài hệ tự quản (autonomous system).Thông thường thì đây là gateway của router để đi ra ngoài .Phần mềm Cisco IOS sẽ chọn một đường trong số những đường ngoại vi của IGRP để làm gateway .Router sẽ sử dụng đến đường gateway khi mạng đích là một mạng không kết nối trực tiếp vào router và router không tìm được một đường nào khác để đến mạng đích .Nếu trong một hệ tự quản có nhiều đường ngoại vi để kết nối ra ngoài thì mỗi router có thể chọn cho mình một gateway khác nhau.

7.3.4. Tính ổn định của IGRP

IGRP cũng có sử dụng một số kỹ thuật để tăng tính ổn định trong hoạt động định tuyến của nó như:

- Thời gian holddown
- Split horizon.
- Poison reverse

Holddowns :

Thời gian holddown được sử dụng để trách cho router cập nhật những thông tin được phát ra do chu kỳ cập nhật nhưng lại là những thông tin cũ , chưa được cập nhật mới.

Split horizons:

Split horizons là nguyên tắc giúp cho router tránh bị lặp vòng bằng cách ngăn không cho router gửi lại những thông tin cập nhật ra một hướng mà nó vừa nhận được tù chính hướng đó .

Poison resverse:

Split horizons chỉ tránh được lặp vòng giữa 2 router kết nối trực tiếp với nhau ,còn poison resverse có thể tránh được vòng lặp lớn hơn .Thông thường ,khi một đường nào đó có thông số định tuyến cứ tăng dần lên là đường đó đã bị lặp vòng .Khi đó router phải phát ra thông tin poison resverse để xóa con đường đó và đặt con đường đó vào trạng thái holddown .Đối với IGRP thì khi một con đường có thông số định tuyến tăng lên theo hệ số 1.1 hoặc lớn hơn nữa thì nó sẽ phát đi thông tin cập nhật poison resverse cho con đường đó .

Ngoài ra, IGRP còn có nhiều thông số về thời gian khác như: chu kỳ cập nhật ,thời gian invalid, thời gian holddown ,thời gian xóa.

Thông số của chu kỳ cập nhật cho biết thời gian bao lâu thì router thực hiện gửi thông tin cập nhật một lần .Đối với IGRP chu kỳ mặc định là 90 gây.

Giá trị của thời gian invalid cho biết trong khoảng thời gian bao lâu thì router vẫn thực hiện gửi thông tin cập nhật bình thường về một đường nào đó trước khi xác nhận chắc chắn là con đường đó không còn sử dụng được nữa .trong IGRP , thời gian invalid mặc định là bằng 3 lần chu kỳ cập nhật .

Nếu có một mạng đích bắt đầu được đặt vào trạng thái holddown thì thời gian holddown là khoảng thời gian mà router sẽ không cập nhật bất kỳ thông tin cập nhật nào về mạng đích đó nếu thông số định tuyến xấu hơn con đường router có trước đó . Trong IGRP ,thời gian holddown mặc định bằng 3 chu kỳ cập nhật cộng thêm 10giây. Cuối cùng ,thời gian xóa là khoảng thời gian mà router phải chờ trước khi thật sự xóa một con đường trong bảng định tuyến .Trong IGRP ,thời gian xóa bằng 7 lần chu kỳ cập nhật.

```
RouterB#show ip protocols
Routing Protocol is "igrp 101"
 Sending updates every 90 seconds, next due in 51
seconds
 Invalid after 270 seconds, hold down 280, flushed
after 630
 Outgoing update filter list for all interfaces is
 Incoming update filter list for all interfaces is
 Default networks flagged in outgoing updates
 Default networks accepted from incoming updates
 IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
 IGRP maximum hopcount 100
 IGRP maximum metric variance 1
 Redistributing: igrp 101
 Routing for Networks:
  192.168.2.0
  192.168.3.0
 Routing Information Sources:
  Gateway    Distance    Last Update
  192.168.2.1      100    00:00:54
 Distance: (default is 100)
```

Thieu vbản

```
RouterA(config)#router igrp 101
RouterA(config-router)#network 192.168.1.0
RouterA(config-router)#network 192.168.2.0

RouterB(config)#router igrp 101
RouterB(config-router)#network 192.168.2.0
RouterB(config-router)#network 192.168.3.0
```

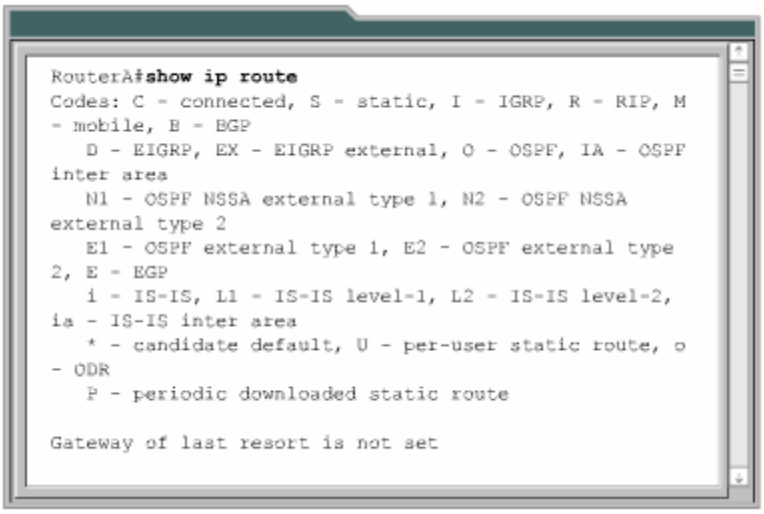
Hình 7.3.5

7.3.6 Sự chuyển đổi từ RIP sang IGRP

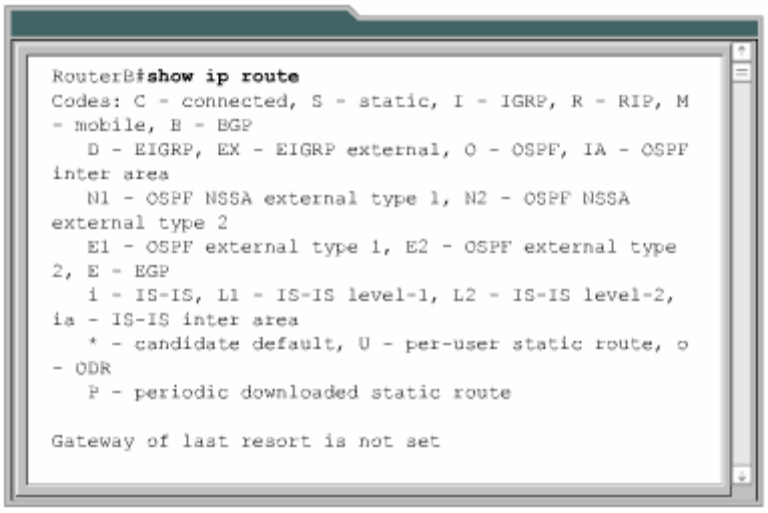
Với sự ra đời của IGRP vào đầu thập niên 80 ,Cisco Sytems đã trở thành công ty đầu tiên khắc phục được các nhược điểm của RIP khi định tuyến giữa các router nội bộ .IGRP quyết định chọn đường dựa vào bằng thông và độ trễ của các đường liên kết mạng .IGRP hội tụ nhanh hơn RIP nên cũng trách được lặp vòng tốt hơn .Hơn nữa ,IGRP không còn bị giới hạn bởi số lượng hop như RIP nữa .Nhờ những ưu điểm trên, IGRP có thể phát triển được cho các hệ thống mạng có cấu trúc lớn và phức tạp .

Sau đây là các bước để chuyển đổi từ RIP sang IGRP :

1. Kểm tra xem trên router có chạy RIP hay không .

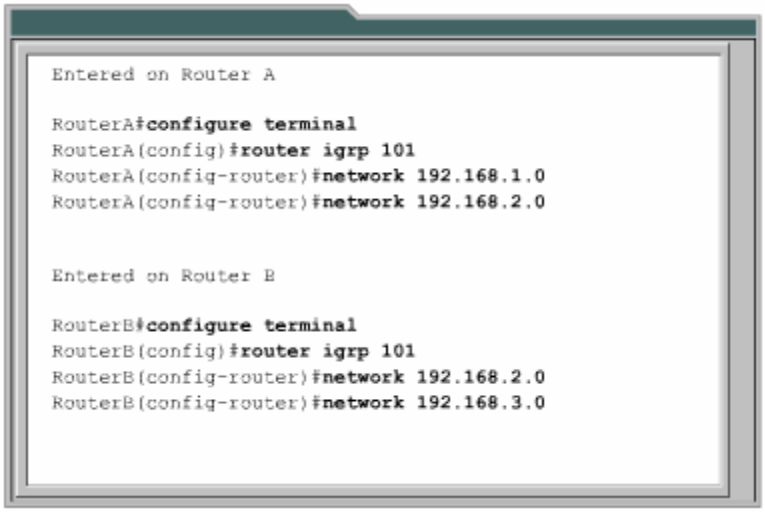


Hình 7.3.6a



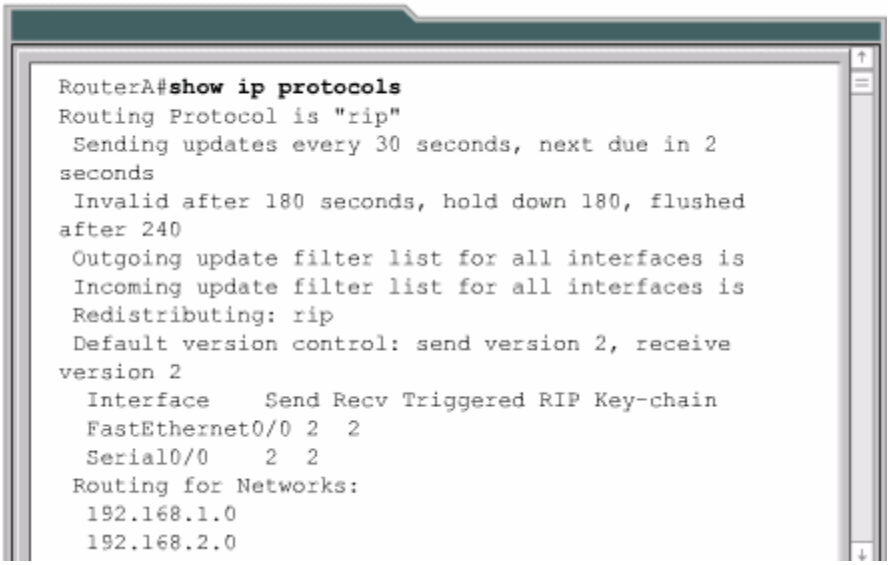
Hình 7.3.6b

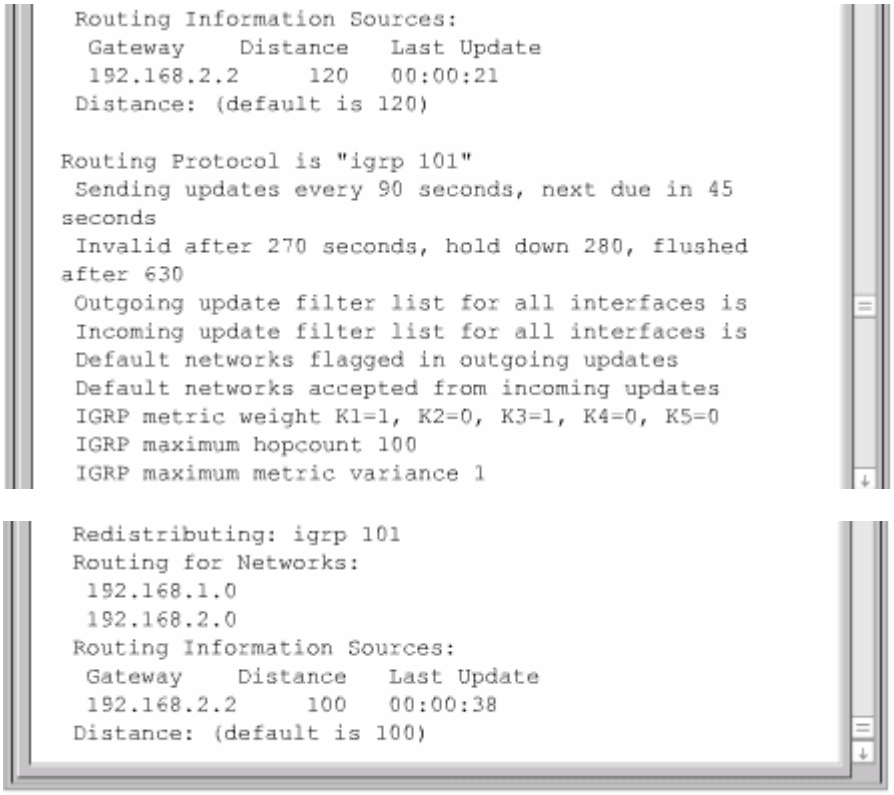
2. Cấu hình IGRP cho router A và B .



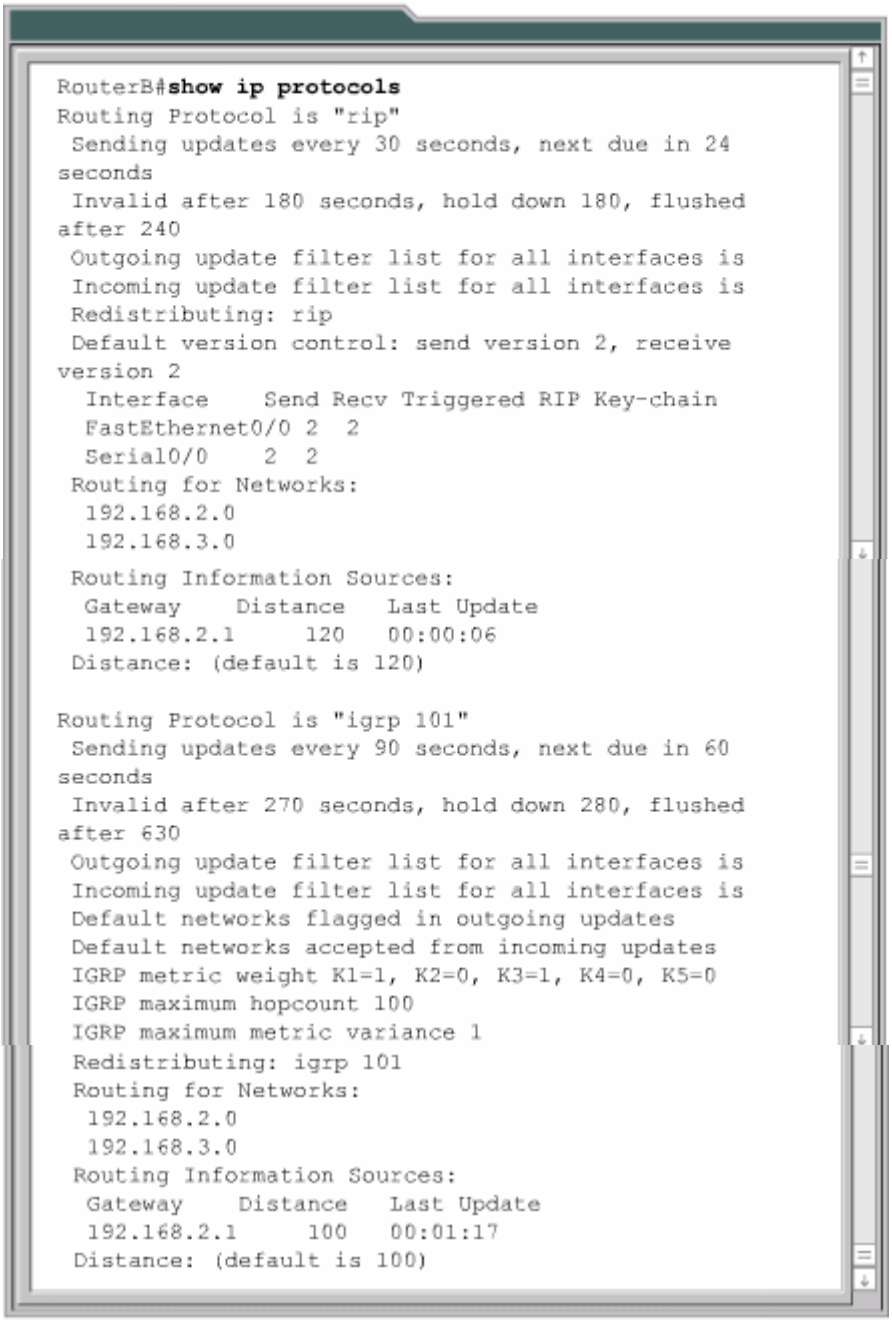
Hình 7.3.6c

3. Nhập lệnh show ip protocols trên router A và B .




Routing Information Sources:
Gateway Distance Last Update
192.168.2.2 120 00:00:21
Distance: (default is 120)
Routing Protocol is "igrp 101"
Sending updates every 90 seconds, next due in 45 seconds
Invalid after 270 seconds, hold down 280, flushed after 630
Outgoing update filter list for all interfaces is
Incoming update filter list for all interfaces is
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
IGRP maximum hopcount 100
IGRP maximum metric variance 1
Redistributing: igrp 101
Routing for Networks:
192.168.1.0
192.168.2.0
Routing Information Sources:
Gateway Distance Last Update
192.168.2.2 100 00:00:38
Distance: (default is 100)

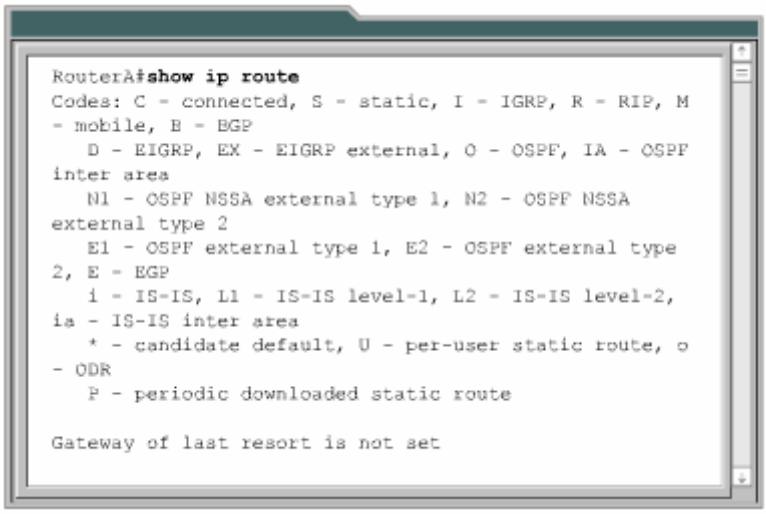
Hình 7.3.6d



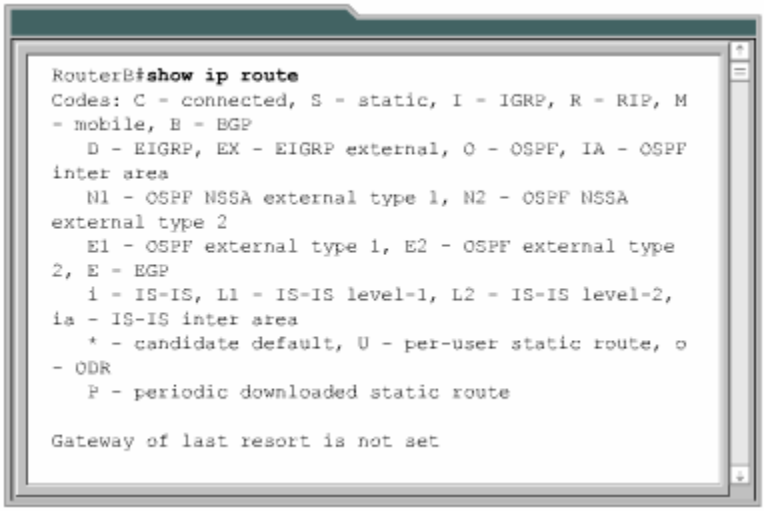
```
RouterB#show ip protocols
Routing Protocol is "rip"
 Sending updates every 30 seconds, next due in 24
seconds
 Invalid after 180 seconds, hold down 180, flushed
after 240
 Outgoing update filter list for all interfaces is
 Incoming update filter list for all interfaces is
 Redistributing: rip
 Default version control: send version 2, receive
version 2
   Interface    Send Recv Triggered RIP Key-chain
   FastEthernet0/0 2   2
   Serial0/0    2   2
 Routing for Networks:
   192.168.2.0
   192.168.3.0
 Routing Information Sources:
   Gateway    Distance    Last Update
   192.168.2.1      120    00:00:06
 Distance: (default is 120)

Routing Protocol is "igrp 101"
 Sending updates every 90 seconds, next due in 60
seconds
 Invalid after 270 seconds, hold down 280, flushed
after 630
 Outgoing update filter list for all interfaces is
 Incoming update filter list for all interfaces is
 Default networks flagged in outgoing updates
 Default networks accepted from incoming updates
 IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
 IGRP maximum hopcount 100
 IGRP maximum metric variance 1
 Redistributing: igrp 101
 Routing for Networks:
   192.168.2.0
   192.168.3.0
 Routing Information Sources:
   Gateway    Distance    Last Update
   192.168.2.1      100    00:01:17
 Distance: (default is 100)
```

Hình 7.3.6e

4. Nhập lệnh show ip route trên router A và B.



Hình 7.3.6f



Hình 7.3.6g

7.3.7 Kiểm tra cấu hình IGRP

Để kiểm tra xem IGRP đã được cấu hình đúng chưa bạn dùng lệnh show ip route và kiểm tra các đường của IGRP được đánh dấu bằng chữ "I" ở đầu dòng .

Ngoài ra còn các lệnh sau bạn có thể sử dụng để kiểm tra cấu hình IGRP :

- Show interface interface
- Show running-config

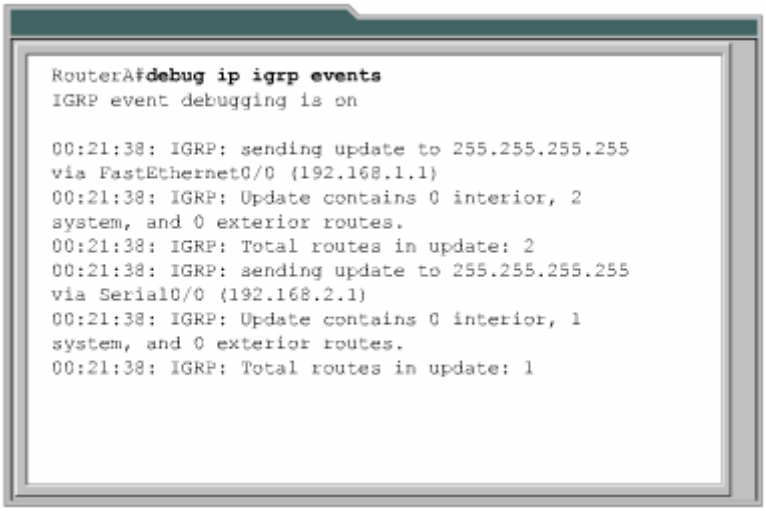
- Show running-config interface interface
- Show running-config | begin interface interface
- Show running-config | begin igrp
- Show ip protocols

Để kiểm tra xem cổng Ethernet đã được cấu hình đúng chưa thì bạn dùng lệnh show interface fa0/0.

Để kiểm tra IGRP đã được chạy trên router chưa thì bạn dùng lệnh show ip protocols.

7.3.8 Xử lý sự cố của IGRP

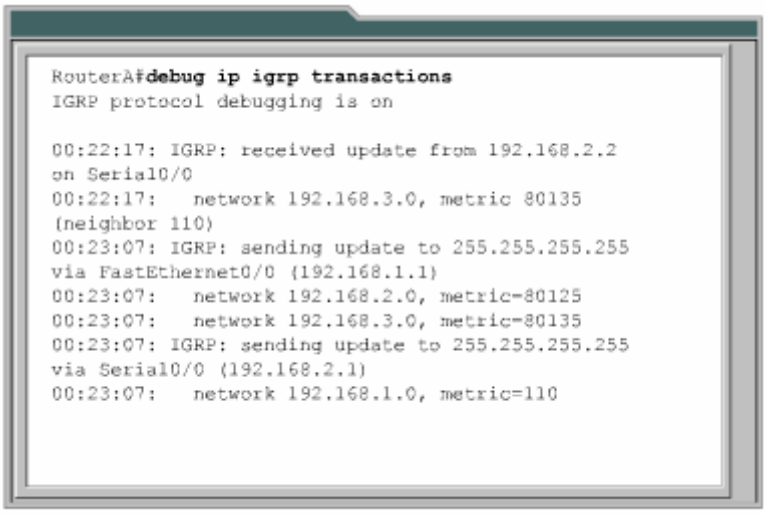
Phần lớn các sự cố của IGRP là do bạn khai báo sai lệnh network ,địa chỉ mạng IP không liên tục ,khai báo số AS sai .



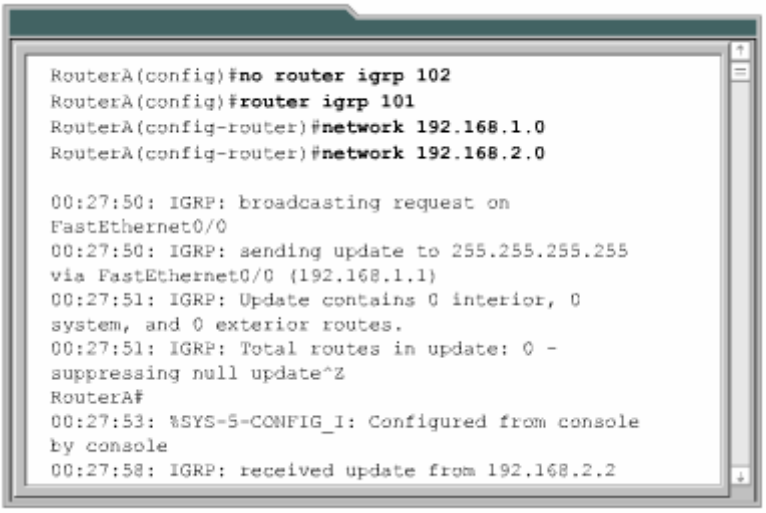
Hình 7.3.8a

Sau đây là các lệnh được sử dụng để tìm sự cố của IGRP :

- Show ip protocols
- Show ip route
- Debug ip igrp events
- Debug ip igrp transactions
- Ping
- Traceroute



Hình 7.3.8b



Hình 7.3.8c

Nếu chỉ số AS sai thì bạn có thể sửa lại chỉ số này như hình trên .

Tổng kết

Sau đây là các điểm quan trong bạn cần nắm được trong chương này:

- Giao thức định tuyến theo vectơ khoảng cách thực hiện bảo trì thông tin định tuyến như thế nào .
- Trong các giao thức định tuyến theo vectơ khoảng cách ,vòng lặp có thể xuất hiện như thê nào .

- Cơ chế định nghĩa giá trị tối đa để tránh đếm vô hạn .
- Tránh vòng lặp bằng split horizon .
- Route poisoning.
- Tránh lặp vòng bằng cơ chế cập nhật tức thời .
- Tránh lặp vòng bằng thời gian holddown .
- Ngăn không cho router gửi thông tin cập nhật về định tuyến ra một cổng .
- Chia tải ra nhiều đường .
- Tiến trình RIP
- Cấu hình RIP
- Sử dụng lệnh ip classless.
- Những vấn đề thường gặp khi cấu hình RIP
- Chia tải với RIP
- Tích hợp đường cố định vơi RIP
- Kiểm tra cấu hình RIP
- Đặc điểm của IGRP
- Thông số định tuyến của IGRP
- Các loại đường trong IGRP
- Tính ổn định của IGRP
- Cấu hình của IGRP
- Sự chuyển đổi từ RIP sang IGRP
- Kiểm tra cấu hình IGRP
- Xử lý sự cố của IGRP

CHƯƠNG 8

THÔNG ĐIỆP ĐIỀU KHIỂN VÀ BÁO LỖI CỦA TCP/IP

GIỚI THIỆU

IP là một giao thức tự nỗ lực tối đa (Best - effort)để chuyển gói tới đích. Nó không hề có cơ chế nào để xác nhận dữ liệu đã được chuyển tới đích .Dữ liệu có thể gặp sự cố trên đường đi tới đích vì rất nhiều lý do như phần cứng bị hư hỏng, cấu hình sai hoặc thông tin định tuyến không đúng. Để giúp xác định các sự cố xảy ra ,IP sử dụng giao thức thông điệp điều khiển Internet (ICMP - Internet Control Message Protocol) để thông báo cho máy nguồn biết là sự cố xảy ra trong quá trình truyền dữ liệu. Chương này sẽ mô tả các loại thông điệp báo lỗi khác nhau của ICMP và trường hợp nào thì chúng được sử dụng.

Bản thân IP không có cơ chế gửi thông điệp điều khiển và báo lỗi nên nó sử dụng ICMP để thực hiện việc gửi nhận các thông điệp điều khiển và báo lỗi cho host trên mạng. Chương này sẽ tập trung nhiều vào các thông điệp điều khiển .Đây là những thông điệp cung cấp thông tin về cấu hình ,định tính cho host .Am hiểu về thông điệp điều khiển của ICMP là một phần rất quan trọng giúp bạn xử lý sự cố mạng và hiểu được một cách đầy đủ về mạng IP.

Sau đây hoàn tất chương này ,bạn có thể thực hiện được những việc sau:

- Mô tả ICMP.
- Mô tả cấu trúc của thông điệp ICMP.
- Xác định loại thông điệp báo lỗi ICMP.
- Xác định nguyên nhân liên quan đến từng loại thông điệp báo lỗi ICMP.
- Mô tả thông điệp điều khiển ICMP.
- Xác định được cácloại thông điệp điều khiển ICMP được sử dụng trong mạng ngày nay.
- Xác định nguyên nhân liên quan đến thông điệp điều khiển ICMP.

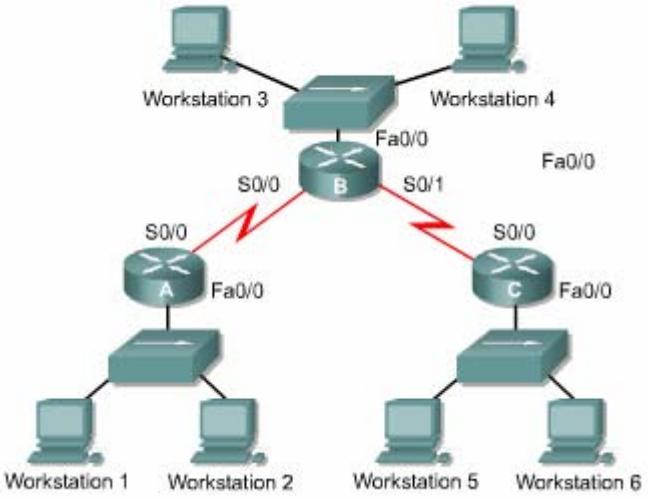
8.1.Tổng quát về thông điệp báo lỗi của TCP/IP

8.1.1. Giao thức thông điệp điều khiển Interne (ICMP)

IP là một phương thức truyền dữ liệu không tin cậy trên mạng. Nó là một giao thức tự nỗ lực tối đa để truyền dữ liệu tới đích. Trong đó, IP không hề có một cơ chế nào để xác nhận là dữ liệu đã đến đích. Nếu một thiết bị trung gian trên đường đi như router chẳng hạn bị sự cố, hay là thiết bị đích không kết nối vào mạng nên dữ liệu không truyền tới đích thì IP không hề có cơ chế nào để thông báo cho người gửi biết là quá trình truyền dữ liệu đã bị sự cố. Giao thức thông điệp điều khiển Internet (ICMP) là một giao thức của bộ TCP/IP đã bổ sung cho khiếm khuyết này của IP. ICMP không khắc phục được sự không tin cậy của IP. ICMP chỉ đơn giản là phát đi các thông điệp để thông báo về sự cố. Vấn đề về độ tin cậy thì sẽ được giải quyết ở các lớp trên nếu cần thiết.

8.1.2 . Thông báo lỗi và khắc phục lỗi.

ICMP là một giao thức thông báo lỗi của IP. Khi quá trình truyền dữ liệu xảy ra lỗi thì ICMP được sử dụng để thông báo lỗi cho nơi gửi dữ liệu. Ví dụ như hình 8.2.1. Máy 1 chuyển dữ liệu cho máy 6 nhưng cổng Fa0/0 trên Router C bị ngắt, khi đó Router C sử dụng ICMP để gửi thông báo lỗi cho Máy 1 biết là dữ liệu không truyền được tới đích. ICMP không khắc phục được sự cố mà nó chỉ đơn giản là thông báo về sự cố đã xảy ra.



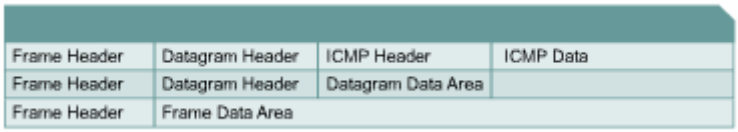
Hình 8.2.1

Router C nhận được gói dữ liệu từ Máy 1, nó chỉ biết được địa chỉ IP nguồn đích của gói dữ liệu thôi. Router C không thể biết chính xác con đường mà gói dữ liệu đã đi đến được Router C. Do đó khi gửi thông báo lỗi thì Router C chỉ có thể gửi cho Máy 1 chứ không gửi cho Router A và B. Như vậy là thông báo ICMP chỉ gửi cho thiết bị nguồn của gói dữ liệu chứ không gửi cho các router.

8.1.3.Truyền thông điệp ICMP

Thông điệp ICMP được đóng gói giống như các dữ liệu khác khi truyền đi bằng IP. Hình 8.1.3 cho thấy dữ liệu của ICMP được đóng gói trong gói IP như thế nào.

Thông điệp ICMP cũng được truyền đi như các gói dữ liệu khác cho nên nó cũng có thể gặp sự cố. Điều này dẫn tới một vấn đề là nếu một thông điệp báo lỗi gặp sự cố thì sẽ làm phát sinh thêm các thông điệp báo lỗi nữa và điều này làm cho mạng càng bị nghẽn hơn khi sự cố vốn đã xảy ra và còn đang tồn tại trên mạng. Chính vì vậy, các thông điệp báo lỗi của ICMP sẽ không tạo thêm các thông điệp báo lỗi cho chính nó .Như vậy thì các thông điệp báo lỗi cũng có khả năng là không bao giờ đến đến được máy nguồn của gói dữ liệu.



Hình 8.1.3

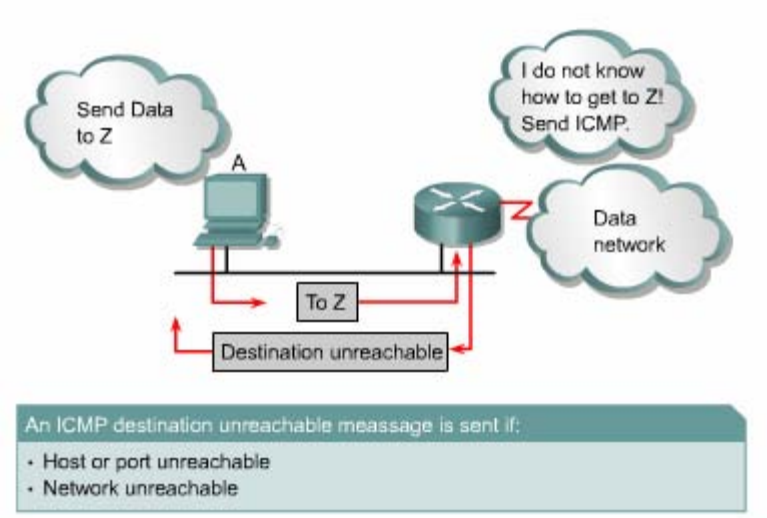
8.1.4. Mạng không đến được

Để thực hiện được việc thông tin liên lạc trên mạng thì các điều kiện cơ bản cần phải có đủ .Trước tiên là thiết bị gửi và nhận dữ liệu phải được cấu hình đúng bộ giao thức TCP/IP.Việc này bao gồm cài đặt bộ giao thức TPC/IP và cấu hình địa chỉ IP.,subnet mask cho thiết bị .Ngoài ra bạn cần phải khai báo Defoult gateway nếu thiết bị cần truyền dữ liệu ra ngoài phạm vi cục bộ .Thư hai là các thiết bị trung gian phải thực hiện việc định tuyến đúng để chuyển gói từ nguồn đến đích .Router là thiết bị thực hiện nhiệm vụ này .Do đó router phải

được cấu hình bộ TCP/IP cho các cổng giao tiếp và sử dụng giao thức định tuyến thích hợp .

Nếu 2 điều kiện trên không được đáp ứng thì hệ thống mạng không thể thực hiện thông tin liên lạc được .Ví dụ như khi một thiết bị gửi dữ liệu đến một địa chỉ IP không tồn tại hoặc là thiết bị đích đã bị ngắt kết nối ra khỏi mạng . Router cũng là nguyên nhân của sự cố nếu cổng giao tiếp trên router bị ngắt hoặc router không có thông tin cần thiết để tìm ra đường tới mạng đích .Những trường hợp như vậy đều được xem là mạng đích không đến được .

Hình 8.1.4 minh họa cho trường hợp router không thể gửi gói dữ liệu đến đích do router không biết đường đến mạng đích , router gửi thông điệp ICMP về cho máy nguồn để thông báo là mạng đích không đến được .

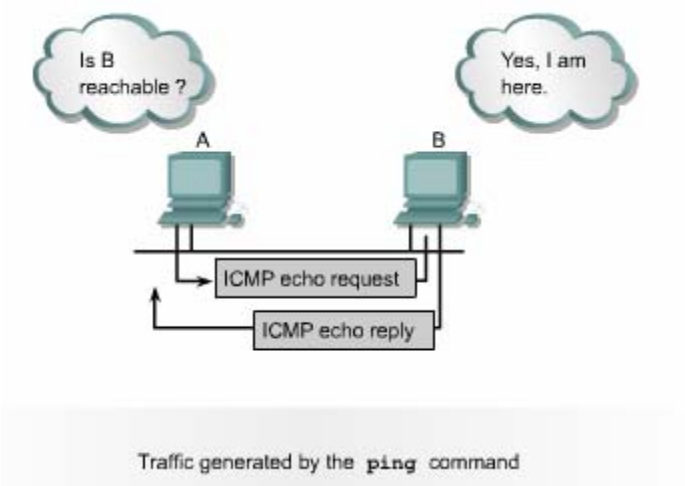


Hình 8.1.4

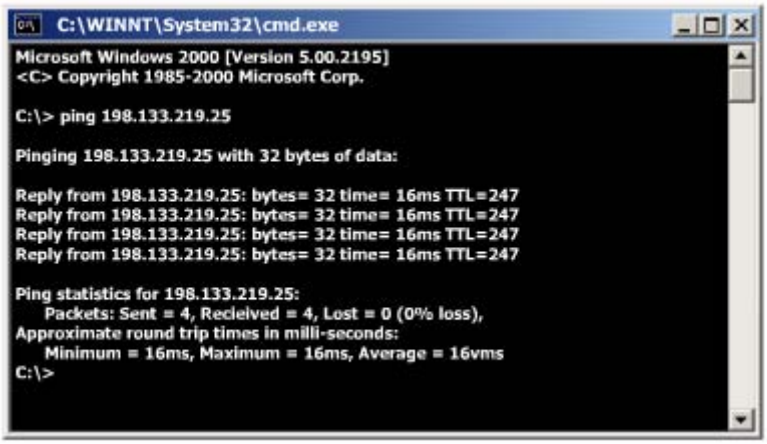
8.1.5 Sử dụng lệnh ping để kiểm tra xem địa chỉ đích có đến được không

Giao thức ICMP có thể được sử dụng để kiểm xem có đến được một địa chỉ nào đó hay không .ICMP sẽ gửi thông điệp echo request đến máy đích .Nếu máy đích nhận được echo request thì sẽ trả lời lại thông điệp echo reply cho máy nguồn .Nếu máy nguồn nhận được echo reply thì điều đó khặng định là máy đích có thể đến được bằng giao thức IP.

Lệnh ping khởi tạo các thông điệp echo request .Ví dụ như hình 8.1.5a và 8.1.5b ,chúng ta sử dụng lệnh ping với địa chỉ IP đích .Lệnh ping gửi đi 4 gói echo request và nhận về 4 gói echo reply xác nhận kết nối IP giữa 2 thiết bị hoạt động tốt.



Hình 8.1.5a



Hình 8.1.5b

8.1.6. Phát hiện đường dài quá giới hạn

Gói dữ liệu khi truyền đi trên mạng có thể bị truyền lòng vòng và không bao giờ đến được đích .Điều này có thể xảy ra khi thông tin định tuyến bị sai ,ví dụ như 2 router cú gửi một gói dữ liệu qua lại cho nhau vì router này nghĩ rằng router kia mới là trạm kế tiếp đến đích .

Giao thức định tuyến có quy trình có quy định giới hạn để xác định mạng đích không đến được .Ví dụ như RIP có số hop giới hạn là 15 .Điều này có nghĩa là gói dữ liệu chỉ được phép đi qua tối đa 15 router.

Khi con đường mà gói dữ liệu đi qua bị lặp vòng hoặc có quá nhiều hop thì khi gói dữ liệu vượt qua giá trị hop tối đa ,giá trị Time-to-live (TTl)của gói dữliệu cũng hết thời gian vì giá trị TTL được cài đặt khớp với số hop tối đa đã được định nghĩa của giao thức định tuyến.Mỗi một gói dữ liệu đều có một giá trị TTL .Mỗi router sau khi xử lý gói dữ liệu sẽ giảm giá trị TTL đi 1 .Khi giá trị TTL bằng 0 thì router sẽ hủy bỏ gói dữ liệu đó .Khi đó ICMP dùng thông điệp “Time exceeded” để thông báo cho máy nguồn biết là TTL của gói dữ liệu đã bị hết thời gian .

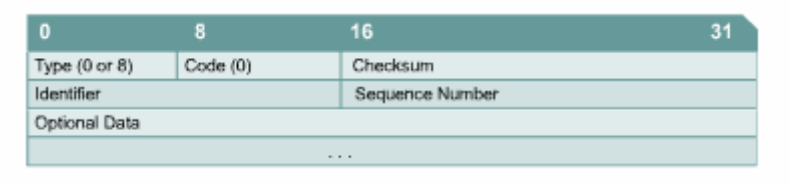
8.1.7.Thông điệp echo

Như bất kỳ các loại gói dữ liệu khác ,thông điệp ICMP cũng có định dạng riêng .Mỗi một loại thông điệp ICMP có một đặc điểm riêng nhưng tất cả các gói ICMP đều bắt đầu bằng 3 phần :

- Type
- Code
- Checksum

Phần type cho biết loại thông điệp nào của ICMP được gửi đi. Phần Code cho biết chi tiết hơn về loại thông điệp ICMP .Phần checksum cũng tương tự như trong các loại gói dữ liệu khác ,phần này được sử dụng để kiểm tra lỗi cho dư liệu.

Trong hình 8.1.7a là cấu trúc của thông điệp ICMP echo request và echo reply .Trong đó chỉ số Type và Code tương ứng với mỗi loại thông điệp .Phần Identifier và Sequence Number sẽ khác nhau đối với từng gói echo request và echo reply .Chỉ số trong 2 phần này được sử dụng để xác định echo reply tương ứng với echo request nào.Còn phần Data chứa các thông tin bổ sung của thông điệp echo request và echo reply.



0	8	16	31
Type (0 or 8)	Code (0)	Checksum	
Identifier		Sequence Number	
Optional Data			
. . .			

Hình 8.1.7a

ICMP Message Types	
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect/ Change Request
8	Echo Request
9	Router Advertisement
10	Router Selection
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply

Hình 8.1.7b

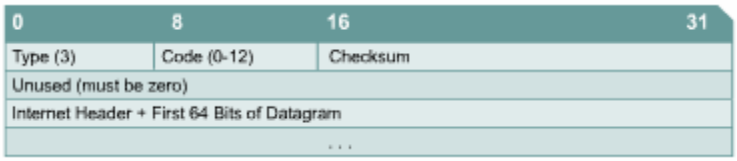
8.1.8.Thông điệp “Destination Unreachable”

Không phải lúc nào gói dữ liệu cũng chuyển được đến đích .Ví dụ như hư hỏng phần cứng ,cấu hình giao thức không đúng ,cổng giao tiếp bị ngắt ,thông tin định tuyên sai… là những nguyên nhân có thể gây ra làm cho gói dữ liệu không thể chuyển được tới đích .Trong những trường hợp như vậy thì ICMP gửi thông điệp “Destination Unreachable” cho máy gửi để thông báo là gói dữ liệu không chuyển được tới đích .

Trong hình 8.1.8a là cấu trúc của thông điệp “Destination Unreachable”.

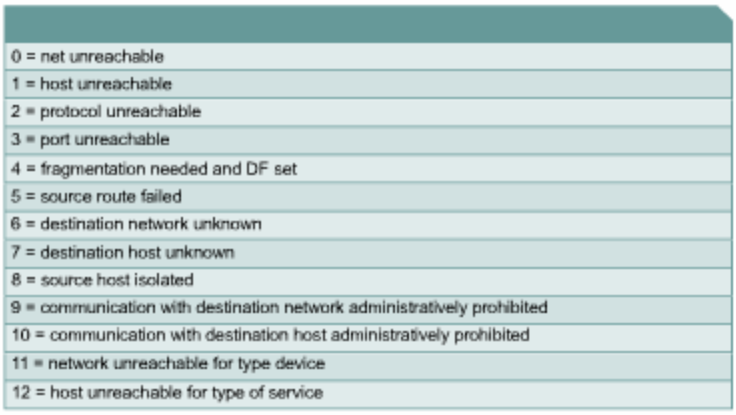
Giá trị 3 trong phần Type cho biết đây là thông điệp “Destination Unreachable”

.Giá trị trong phần Code sẽ cho biết nguyên nhân tại sao không chuyển được gói dữ liệu đến đích .Ví dụ như phần Code có giá trị 0 có nghĩa là mạng đích không đến được .



0	8	16	31
Type (3)	Code (0-12)	Checksum	
Unused (must be zero)			
Internet Header + First 64 Bits of Datagram			
...			

Hình 8.1.8a



0 = net unreachable
1 = host unreachable
2 = protocol unreachable
3 = port unreachable
4 = fragmentation needed and DF set
5 = source route failed
6 = destination network unknown
7 = destination host unknown
8 = source host isolated
9 = communication with destination network administratively prohibited
10 = communication with destination host administratively prohibited
11 = network unreachable for type device
12 = host unreachable for type of service

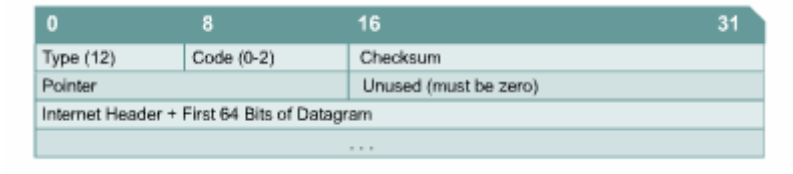
Hình 8.1.8b

Khi gói dữ liệu được chuyển từ mạng Token-ring ra mạng Ethernet thì thường phải phân mảnh ra thành các gói nhỏ hơn .Nếu gói dữ liệu không cho phép phân mảnh thì gói dữ liệu không thể chuyển ra được ,khi đó thông điệp “Destination Unreachable” sẽ được gửi đi.Thông điệp ICMP này cũng được gửi đi khi các dịch vụ liên quan đến IP như FTP ,Web không tim thấy .Điều quan trong khi xử lý sự cố mạng IP là bạn cần phải hiểu được các nguyên nhân khác nhau tạo nên thông điệp ICMP “Destination Unreachable”.

8.1.9.Thông báo các loại lỗi khác

Khi thiết bị xử lý gói dữ liệu không chuyển gói dữ liệu đi được do một số lỗi ở phần Header của gói dữ liệu .Loại dữ liệu này không liên quan gì đến host đích hay mạng đích nhưng nó vẫn làm cho gói dữ liệu không thể chuyền được đến đích .Trong trường hợp này ,thông điệp ICMP “Parameter Problem”,Type 12 sẽ được gửi về cho máy nguồn.

Trong hình 8.1.9 là cấu trúc của thông điệp “Parameter Problem”.Trong đó có phần Pointer .Khi giá trị Code là 0 ,phần Pointer cho biết octet nào trong gói dữ liệu bị lỗi .



0	8	16	31
Type (12)	Code (0-2)	Checksum	
Pointer		Unused (must be zero)	
Internet Header + First 64 Bits of Datagram			
...			

Hình 8.1.9

8.2.Thông điệp điều khiển của TCP/IP

8.2.1.Giới thiệu về thông điệp điều khiển

ICMP là một phần của bộ giao thức TCP/IP .Thực tế là tất cả các hệ thống IP đều phải bao gồm ICMP .Lý do của việc này hết sức đơn giản .Trước hết là IP không có cơ chế nào để đảm bảo là dữ liệu đã được chuyển tới đích ,hoàn toàn không thông báo gì cho host biết khi sự cố xảy ra .IP không có cơ chế cung cấp thông điệp thông báo hoặc điều khiển cho host .Và ICMP đã thực hiện việc này cho IP .

ICMP Message Types	
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect/ Change Request
8	Echo Request
9	Router Advertisement
10	Router Selection
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply

Hình 8.2.1

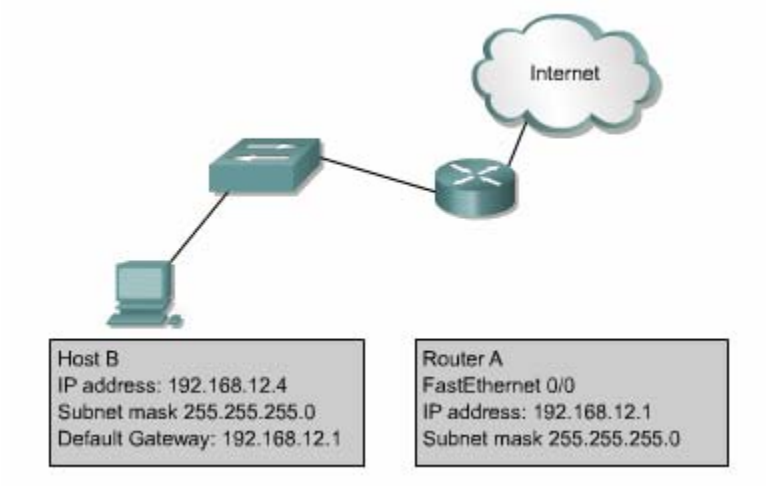
Không giống như thông điệp báo lỗi ,thông điệp điều khiển không phải được tạo ra là do mất gói dữ liệu hay do lỗi của quá trình truyền dữ liệu .Mà các thông điệp điều khiển được dùng để thông báo cho host biết về tình trạng nghẽn

mạch trên mạng hay thông báo cho host biết là có một gateway tốt hơn dẫn đến mạng đích …Cũng giống như tất cả các gói ICMP khác ,thông điệp điều khiển được đóng gói trong gói IP .ICMD sử dụng gói IP để truyền thông điệp trên mạng .

ICMP có rất nhiều loại thông điệp điều khiển khác nhau .Một số loại thường gặp nhất được thể hiện ở hình 8.2.1.

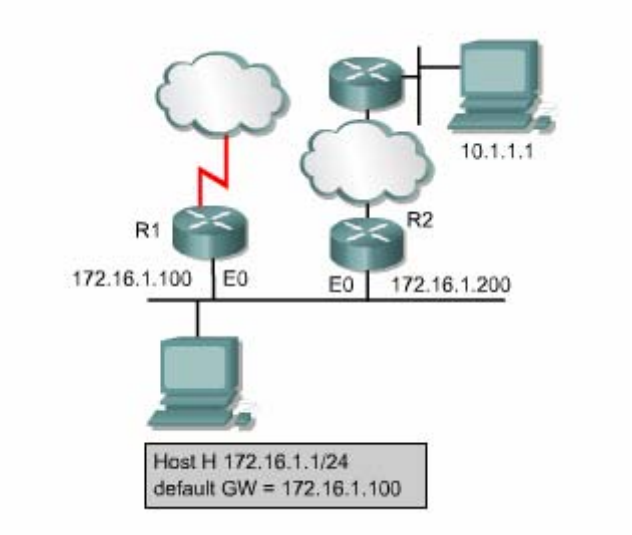
8.2.2.Thông điệp ICMP redirect/change request

Thông điệp điều khiển ICMP thường gặp nhất là redirect/change request.Loại thông điệp này được tạo ra bởi gateway mà thông thường đó chính là router .Tất cả các host khi muốn thông tin liên lạc với các mạng IP đều phải được cấu hình default gateway. Default gateway là địa chỉ của một cổng trên router kết nối vào cùng một mạng với host .Như trong hình 8.2.2a ,một host được nối vào router và router này có kết nối ra Internet.Host B được cấu hình default gateway là địa chỉ IP của cổng Fa0/0trên router.Host B sẽ sử dụng địa chỉ IP này để đến các mạng khác .Bình thường host B chỉ kết nối đến một gateway.Tuy nhiên cũng có trường hợp một host kết nối vào mạng 2 hay nhiều router.Trong trường hợp đó , default gateway của host sẽ cần dùng redirect/change request để thông báo cho host biết về một gateway khác tốt hơn để đến một mạng đích nào đó.



Hình 8.2.2a

Trong hình 8.2.2b là một ví dụ cho trường hợp cần sử dụng ICMP redirect.Host H gửi dữ liệu cho Host C trong mạng 10.0.0.0/8 .Vì mạng đích không kết nối trực tiếp vào Host H nên Host H gửi gói đến default gateway của nó là Router R1 .Router R1 tìm trên bảng định tuyến để tìm đường đến mạng 10.0.0.0/8 thì thấy rằng để chuyển gói tới đích router phải gửi gói này ngược trở ra cổng mà nó vừa mới nhận gói dữ liệu vào .Khi đó router R1 sẽ chuyển gói dữ liệu đi và đồng thời gửi thông điệp ICMP redirect/change request tới Host H để thông báo là Host H nên sử dụng Router R2 làm gateway cho tất cả các gói dữliệu đến mạng 10.0.0.0/8 .



Hình 8.2.2b

Default gateway chỉ gửi thông điệp ICMD redirect/change request khi gặp các điều kiện sau :

- Cổng mà router nhận gói dữ liệu vào cũng chính là cổng mà router sẽ chuyển gói dữ liệu đi.
- Địa chỉ IP của máy nguồn là cùng một mạng /subnet với địa chỉ IP của trạm kế tiếp .
- Gói dữ liệu nhận được không phải gửi ngược lại máy nguồn .
- Con đường mà router thực hiện thông báo cho host không phải là đường mặc định của router và cũng không phải là của một ICMP redirect nào khác.
- Router phải được cấu hình để thực hiện redirect.(Mặc định là Cisco router thực hiện gửi ICMP redirect.Bạn có thể dùng lệnh no ip redirect để tắt chức năng này trên một cổng nào đó của router).

Thông điệp ICMP redirect /change request có cấu trúc như hình 8.2.2c.Trong đó phần Type có giá trị là 5 ,phần Code có giá trị là 0,1,2 hoặc 3.

Phần Router Internet Address chứa địa chỉ IP của gateway mới .Ví dụ như trên : trong thông điệp redirect của Router R1 gửi cho Host H ,phần Router Internet Address sẽ có giá trị là 172.16.1.200,đây là địa chỉ IP của cổng E0 trên Router R2 .

0	8	16	31
Type (5)	Code (0-3)	Checksum	
Router Internet Address			
Internet Header+ First 64 Bits of Datagram			
. . .			

Hình 8.2.2c

Code Value	Required Action
0	Redirected datagrams for the network.
1	Redirected datagrams for the host.
2	Redirected datagrams for the type of services and networks.
3	Redirected datagrams for the type of services and host.

Hình 8.2.2d

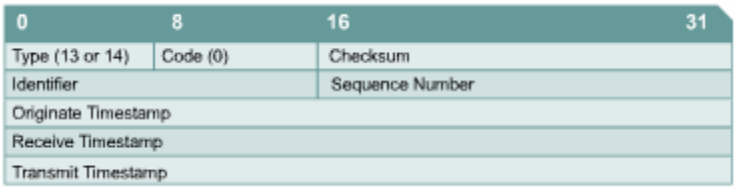
8.2.3.Đồng bộ đồng hồ và ước tính thời gian truyền dữ liệu

Bộ giao thức TCP/IP cho phép hệ thống mạng này kết nối với hệ thống mạng khác ở cách nhau rất xa thông qua nhiều hệ thống mạng trung gian .Mỗi một hệ thống mạng có một cơ chế đồng bộ đồng hồ riêng .Do đó khi một host ở mạng khác sử dụng phần mềm cần đồng bộ thời gian để thực hiện liên lạc thì có thể sẽ gặp rắc rối .Thông điệp ICMP Timestamp được thiết kế để giải quyết vấn đề này .

Thông điệp ICMP timestamp request cho phép một host hỏi giờ hiện tại trên một máy khác .Máy được hỏi sẽ dùng thông điệp ICMP timestamp reply để trả lời .

Phần Type trong thông điệp ICMP timestamp có giá trị là 13 (timestamp request)hoặc 14(timestamp reply) .Phần Code luôn có giá trị là 0 vì loại thông điệp này không có gì khác hơn. Phần Originate timestamp là thông tin về giờ hiện tại trên máy gửi ngay trước khi thông điệp ICMP timestamp request được gửi đi .Phần Recive timestamp là thời điểm mà máy đích nhận được yêu cầu request .Phần Transmit timestamp là thời điểm trên máy trả lời ngay trước khi máy này gửi thông điệp ICMP timestamp reply.

Tất cả 3 thống số về thời gian trên đều được tính bằng số mili giây tính từ thời điểm nửa đêm theo giờ Quốc tế (Univesal Time -UT).



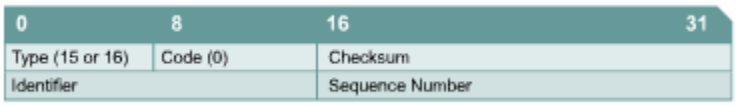
Hình 8.2.3

Tất cả các thông tin ICMP timestamp reply đều có đầy đủ 3 thông số :thời điểm gửi gói request ,thời điểm nhận được request và thời điểm gửi gói reply .Dựa vào 3 thông số này host có thể ước lượng được khoảng thời gian dữ liệu truyền trên mạng từ máy nguồn đến máy đích bằng cách lấy giá trị của phần Originate Timestamp trừ cho giá trị của phần Transmit timestamp.Kết quả này cũng chỉ mang tính chất ước lượng thôi vì thời gian truyền thật sự còn phụ thuộc vào lưu lượng truyền thực tế trên mạng lúc đó .Ngoài ra ,host còn có thể ước tính được giờ hiện tại trên máy đích .

Thông điệp ICMP timestamp là một cách đơn giản để ước đoán giờ trên máy đích và ước tính tổng thời gian truyền trên mạng nhưng đây chưa phải là cách tốt nhất .Giao thức Network Time Protocol (NTP) ở lớp trên của giao thức TCP/IP thực hiện đồng bộ đồng hồ theo cách tin cậy và chính xác hơn.

8.2.4.Thông điệp Information request và reply

Thông điệp ICMP information request và reply cho phép host xác định địa chỉ mạng của nó .Hình 8.2.4 là cấu trúc của loại thông điệp này.



Hình 8.2.4

Phần Type có 2 giá trị :giá trị 15 tương ứng với thông điệp Information reply .Loại thông điệp này của ICMP được xem là đã quá lỗi thời .Hiện nay ,các giao thức BOOTP và DHCP được sử dụng nhiều để cung cấp địa chỉ mạng cho host .

8.2.5 Thông điệp Address Mask

Khi người quản trị mạng dùng một địa chỉ IP lớn chia ra thành nhiều subnet ,các subnet sẽ có subnet mask tương ứng .Subnet mask được sử dụng để xác nhận các bit của phần Network .Subnet và các bit của thành phần Host trong địa chỉ IP .Nếu một host biết địa chỉ IP của router thì nó gửi yêu cầu tới trực tiếp của router ,còn nếu không thì nó sẽ quảng bá yêu cầu của nó .Khi router nhận được yêu cầu này ,router sẽ dùng thông điệp Address mask reply để trả lời .Trong thông điệp Address mask reply sẽ có subnet mask chính xác cho host.Ví dụ : môt host trong mạng lớp B có địa chỉ IP là 172.16.5.2 .Host này không biết subnet mask của mình nên nó broadcast thông điệp Address mask request như sau :

Source address:172.16.5.2

Destination address:255.255.255.255

Protocol :ICMP =1

Type :Address Mask Request =AM1

Code :0

Mask:255.255.255.0

Router 172.16.5.2 nhận được thông điệp trên và trả lời bằng thông điệp Address mask reply như sau :

Source address:172.16.5.1

Destination address:172.16.5.2

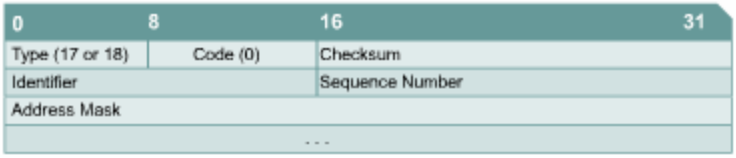
Protocol :ICMP =-1

Type :Address Mask Request =AM2

Code :0

Mask:255.255.255.0

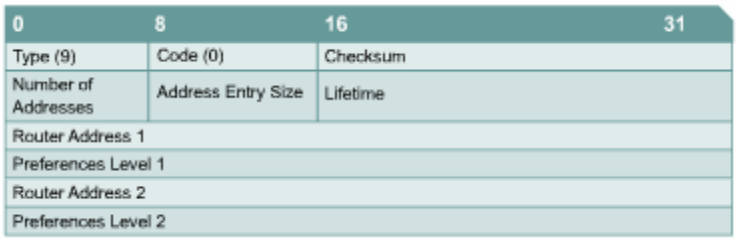
Cấu trúc của thông điệp Address Mask Request và reply được thể hiện ở hình 8.2.5.Thông điệp Address Mask Request và reply có cấu trúc hoàn toàn như nhau ,chỉ khác nhau giá trị phần Type .Phần Type có giá trị 17 là tương ứng với request ,còn giá trị 18 là tương ứng với reply .Phần Identifier và Sequênc Number giúp phân biệt reply nào tương ứng với request nào ,giá trị hai phần này thường là 0.Phần Checksum được dùng để kiểm tra lỗi cho thông điệp ICMP được tính bắt đầu từ phần Type trở đi.



Hình 8.2.5

8.2.6 . Thông điệp của router

Khi có host trong mạng bắt đầu khởi động và host chưa được cấu hình Default gateway thì nó có thể tìm gateway bằng thông điệp Router discovery.Trước tiên ,host gửi thông điệp Router solicitation cho tất cả các router bằng cách dùng địa chỉ multicast là 224.0.0.2 .Thông điệp này cũng có thể được gửi broadcast để gửi đến được những router không có cấu hình multicast .Khi nhận được thông điệp trên ,nếu router không có cấu hình hỗ trợ quá trình này thì router sẽ không trả lời gì hết .Còn nếu router có hỗ trợ quá trình này thì router sẽ trả lời lại bằng thông điệp Router advertisement .Cấu trúc của thông tin điệp Router advertisement được mô tả ở hình 8.2.6.



0	8	16	31
Type (9)	Code (0)	Checksum	
Number of Addresses	Address Entry Size	Lifetime	
Router Address 1			
Preferences Level 1			
Router Address 2			
Preferences Level 2			

Hình 8.2.6

8.2.7 . Thông điệp Router solicitation

Host gửi thông điệp Router solicitation trong trường hợp bị mất Default gateway.Thông điệp này được gửi multicast và đây chính là bước đầu tiên của quá trình tìm router đã đề cập ở phần 8.2.6 .Router sẽ trả lời lại bằng thông điệp Router Advertisement,trong đó có cung cấp Default gateway cho host .Hình 8.2.7 là cấu trúc của thông điệp Router solicitation:

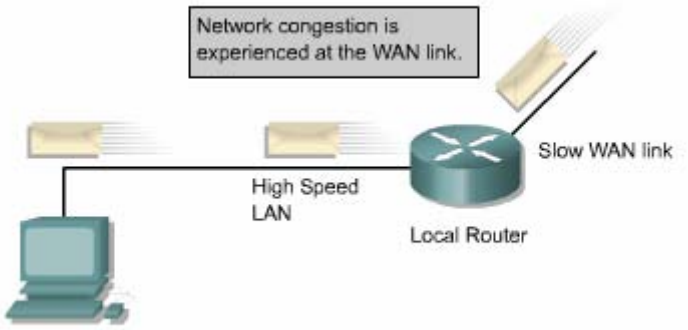
0	8	16	31
Type (10)	Code (0)	Checksum	
Reserved			

Hình 8.2.7

8.2.8.Thông điệp báo nghẽn và điều khiển luồng dữ liệu

Nếu có nhiều máy tính cùng lúc truy xuất vào cùng một máy đích thì máy đích có thể bị quá tải .Nghẽn mạch có thể xảy ra khi lưu lượng từ mạng LAN tốc độ cao được truyền ra kết nối WAN có tốc độ thấp hơn .Nếu mạng bị nghẽn quá mức thì các gói dữ liệu sẽ bị hủy bỏ .Thông điệp ICMP source-quence giúp làm giảm lượng dữ liệu bị hủy bỏ .Thông điệp này sẽ được gửi cho máy gửi để yêu cầu máy gửi giảm tốc độ phát gói dữ liệu .Sau khoảng thời gian ngăn ,nghẽn mạch được giải tỏa và máy gửi có thể tăng dần tốc độ truyền lên sau khi không còn nhận được thông điệp source-quence nào nữa .Mặc định là đa số các Cisco router không thực hiện gửi thông điệp source-quence vì có thể các thông điệp này còn làm cho tình trạng tắc nghẽn bị tăng thêm .

Mô hình văn phòng nhỏ -văn phòng tại nhà (SOHO –Small Office Home Office)là một trường hợp áp dụng tốt ICMP source-quence .Ví dụ một SOHO có một mạng gồm 4 máy tính được nối với nhau bằng cáp Cat5 và 4 máy này chia sẻ nhau một kết nối Internet 56K bằng moden .Chúng ta thấy rằng đường kết nối WAN với băng thông 56K sẽ nhanh chóng bị quá tải với mạng LAN băng thông 100Mbps của SOHO ,kết quả là dữ liệu sẽ bị mất và phải truyền lại nhiều lần .Máy tính có kết nối ra Internet và giữ vai trò gateway để chia sẻ đường truy cập Internet này cho các máy tính còn lại có thể dùng thông điệp ICMP yêu cầu các máy tính khác giảm tốc độ truyền để trách việc mất mát dữ liệu do nghẽn mạch.



Hình 8.2.8

TỔNG KẾT

Sau đây là các điểm quan trọng bạn cần nắm trong chương này :

- IP là cơ chế tự nỗ lực tối đa để truyền gói dữ liệu .IP sử dụng thông điệp ICMP để thông báo cho máy nguồn biết là dữ liệu đã không chuyển tới được đến đích .
- Thông điệp ICMP echo request và echo reply cho phép người quản trị mạng kiểm tra kết nối IP trong quá trình xử lý sự cố mạng .
- Thông điệp ICMP cũng được vận chuyển bằng giao thức IP nên quá trình truyền thông điệp ICMP không tin cậy .
- Gói ICMP có phần Header riêng đặc biệt bắt đầu bằng phần Type và Code.
- Xác định được nguyên nhân tạo ra các thông điệp báo lỗi của ICMP .

- Chức năng của các thông điệp điều khiển ICMP.
- Thông điệp ICMP redirect/change rquest .
- Thông điệp ICMP để đồng bộ đồng hồ và ước lượng thời gian truyền dữ liệu .
- Thông điệp ICMP information request và reply.
- Thông điệp ICMP để tìm router .
- Thông điệp ICMP router solicitation.
- Thông điệp ICMP để báo nghẽn và điều khiển luồng dữ liệu.

Lời nói đầu

Nhằn đảm bảo kiến thức cần thiết cho một CCNA giáo trình hệ thống mạng máy tính

CCNA 1 đã giới thiệu khái quát hệ thống mạng số liệu theo mô hình phân lớp. Trong giáo trình này toàn bộ kiến thức cơ bản về hệ thống mạng số liệu đã được giới thiệu. Kế tiếp giáo trình hệ thống mạng máy tính CCNA 2 giúp bạn tìm hiểu hoạt dộng của router và hướng dẫn cấu hình cơ bản cho router với các giao thức định tuyến đơn giản như RIP, IGRP. Như các bạn đã biết router là thiết bị quan trọng của mạng số liệu với nhiệm vụ then chốt là định tuyến . Nhiệm vụ định tuyến của router không dừng lại ở đó mà được phát triển tốt hơn. Từ đó . giáo trình hệ thống mạng máy tính CCNA 3 tiếp tục phân tích sâu sắc về các đặc điểm hoạt động của từng loại giao thức định tuyến phức tạp khác trong router. Đặc biệt hoạt động và cách thức cấu hình cho hai giao thức OSPF và EIGRP được trình bày rất chi tiết trong giáo trình này.

Ngoài ra giáo trình hệ thống mạng máy tính CCNA 3 còn giúp các bạn hiểu rõ hoạt động của switch và hướng dẫn cấu hình để đưa switch vào hoạt động. Giáo trình này cũng phân tích và so sánh chi tiêt hoạt động của các loại thiết bị mạng như reapeater, hub, switch và router. Đặc biệt một số chương giúp bạn tiếp cận VLAN về cơ chế hoạt động của switch trong VLAN và cách thức cấu hình switch, router để tạo các VLAN

Nói tóm lại mục tiêu của giáo trình hệ thống máy tính CCNA 3 là giúp các bạn nắm vững toàn bộ các khía cạnh nối mạng cơ bản cho một LAN. Chúc cácbạn đạt được mục tiêu này và thực sự làm chủ được một LAN. Khối kiến thức và kỹ năng quan trọng còn lại cho một CCNA. Là cáccông nghệ WAN dùng để kết nối giữa các mạng LAN. Chủ đề này sẽ được trình bày trong giáo tình hệ thống mạng máy tính CCNA 4

Mặc dù rất cố gắng trong quá trình biên soạn nhưng chắc không thể tránh khỏi những thiếu sót rất mong được bạn đọc ủng hộ và đóng góp ý kiến. Xin chân thành cảm ơn

Lời ngỏ

Kính thưa quý bạn đọc gần xa. Ban xuất bản MKPUB trước hết xin bày tỏ long biết ơn và niêm vinh hạnh trước nhiệt tình của đông đảo Bạn đọc đối với tủ sách MK MUB trong thời gian qua

Khẩu hiệu của chúng tôi là:
Lao động khoa học nghiêm túc

Chất lượng va ngày càng chất lượng hơn

Tất cả vì Bạn đọc

Rất nhiều bạn đọc đã gửi mail cho chúng tôi đóng góp nhiều ý kiến quý báo cho tủ sách

Ban xuất bản MK MUB xin được kính mời quý bạn đọc tham gia cùng nâng cao chất lượng tủ sách của chúng ta

Trong quá trình đọc, xin các bạn ghi chú lại các sai sót của cuốn sách hoặc các nhận xét của riêng bạn. Sau đó xin gửi về địa chỉ

Emal: mkbook@minhkhai.com.vn – mk.pub@minhkhai.com.vn

Hoặc gửi về : Nhà sách Minh khai

249 Nguyễn Thị Minh Khai, Q1, tp Hồ chí Minh

Nếu bạn ghi chú trực tiếp lên cuốn sách, rồi gửi cuốn sách đó cho chúng tôi thì chúng tôi sẽ xin hoàn lại cước phí bưu điện và gửi lại cho Bạn cuốn sách khác

Chúng tôi xin gửi tặng một cuốn sách của tủ sách MK PUB tùy chọn lựa của bạn theo một danh mục thích hợp sẽ được gửi tới bạn.

Với mục đích ngày càng nâng cao chất lượng của tủ sách MK. PUB chúng tôi rất mong nhận được sự hợp tác của quý bạn đọc gần xa

MK.PUB và bạn đọc cùng làm!

Mục lục

Chương 1:

GIỚI THIỆU VỀ ĐỊNH TUYẾN KHÔNG THEO LỚP ĐỊA CHỈ

GIỚI THIỆU

Người quản trị mạng phải có dự kiến và quản lý sự phát triển về mặt vật lý của hệ thống mạng, ví dụ như mua hoặc thuê thêm một tầng lầu trong toà nhà, trang bị thêm các thiết bị mới như switch, router, bộ tập trung cáp kệ để các thiết bị… Khi thiết kế hệ thống mạng người thiết kế thường phải chọn một sơ đồ phân phối địa chỉa cho phép mở rộng mạng về sau. Phân phối địa chỉ IP không cố định chiều dài subnet mask là một kỹ thuật phân phối địa chỉ IP hiệu quả, có khả năng mở rộng nhiều hơn

Với sụ phát triển phi thường của Internet và TCP/IP mỗi công ty tập đoàn đều phải triển khai sơ đồ địa chỉ IP của mình. Rất nhiều tổ chức chọn lựa TCP/IP là giao thức được định tuyến duy nhất trong hệ thống mạng của mìn. Nhưng thật không may, TCP/IP đã không thể lường trước được rằng giao thức của họ được ứng dụng trong mạng toàn cầu cho thông tin thương mại giải trí

Hai mươi năm trước đây,IP phiên bản 4 đưa ra một mô hình địa chỉ và cũng đáp ứng đủ. Trong khi đó , IP phiên bản 6 được xem là môt không gian địa chỉ trong giới hạn thì được triển khai thử nghiệm chậm chạm và có thể sẽ thay thế IPv4 một giao thức thống trị Internet hiện nay. Trong thời gian chờ đợi sự thay đổi đó hơn hai thập kỷ qua các kỹ sư mạng đã thành công trong việc vận dụng IPv4 một cách linh hoạt để hệ thống mạng của mình có thể tồn tại với sự phát triển rộng lớn của Internet. VLSM là một trong những kỹ thuật tận dụng không gian địa chỉ Ip hiệu quả

Cùng với sự phát triển của hệ thống mạng để đáp ứng nhu cầu của người sử dụng giao thức định tuyến cũng phải mở rộng theo. RIP vẫn được xem là một giao thức phù hợp cho hệ thống mạng nhỏ vì một số giới hạn khiến nó không có khả năng mở rộng. Để khắc phục những giới hạn này RIP phiên bản 2 đã được phát triển

Sauk hi hoàn tất chương này các bạn có thể thực hiện những việc sau:

- Định nghĩa VLSM và mô tả khái quát các lý do để sử dụng nó

- Chia một mạng lớn thành các mạng con có kích thước khác nhau bằng cách sử dụng VLSM
- Cấu hình router sử dụng VLSM
- Xác định các đặc tính chủ yếu của RIPv1 hoặc RIPv2
- Xác đin những điểm khác nhau quan trọng giữa RIPv1 và RIPv2
- Cấu hình RIPv2
- Kiểm tra và xử lý sự cố hoạt động RIPv2
- Cấu hình đường mặc định bằng lệnh ip route và ip default- network

1.1 VLSM

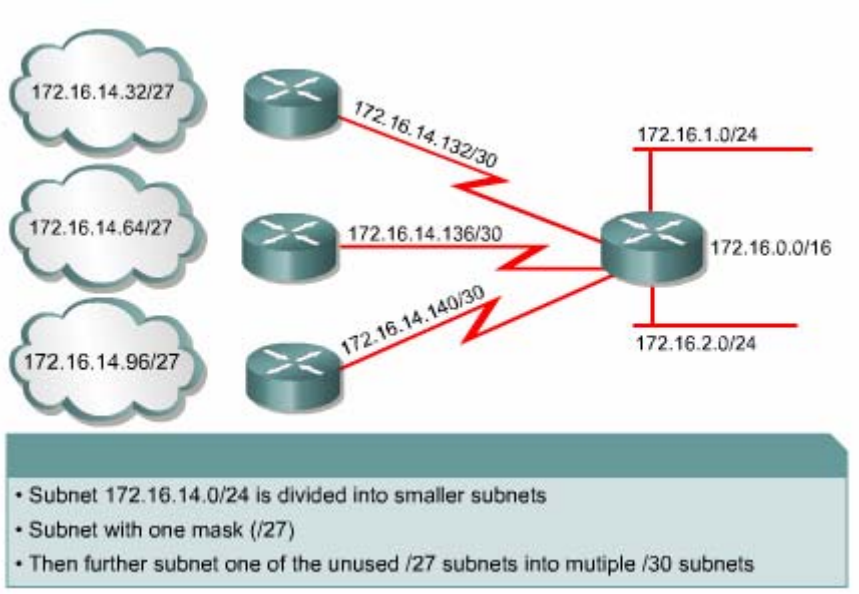
1.1.1 VLSM là gì và tại sao phải sử dụng nó

Khi mạng IP phát triển lớn hơn, người quản trị mạng phải có cách sử dụng không gian địa chỉ của mình một cách hiệu quả hơn. Một trong những kỹ thuật thường được sử dụn là VLSM. Với VLSM người quản trị mạng có thể chia địa chỉ mạng có subnet mask dài cho mạng có ít host và địa chỉ mạng có subnet mask ngắn cho mạng nhiều host

Khi sử dụng VLSM thì hệ thống mạng phải chạy giao thức định tuyến có hỗ trợ VLSM như OSPF, Intergrated IS – IS, EIGRP, RIPv2 và định tuyến cố định

VLSM cho phép một tổ chức sử dụng chiều dài subnet mask khác nhau trong một địa chỉ mạng lớn. VLSM còn được gọi là chia subnet trong một subnet lớn hơn giúp tận dụng tối đa không gian địa chỉ

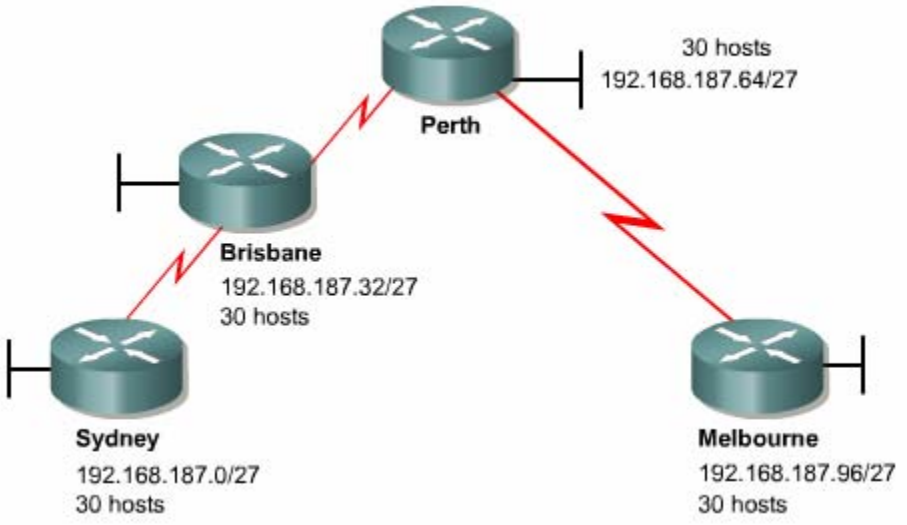
Giao thức định tuyến theo lớp địa chỉ mạng lớn hơn thành nhiều địa chỉ mạng con có kích thước khác nhau như địa chỉ mạng có 30 bit subnet mask , 255.255.255.532 để dành cho các kết nối mạng địa chỉ mạng có 24 bit subnet mask, 255.255.255.0 để dành cho các mạng có dưới 254 user, các địa chỉ mạng có 22 bit subnet mask, 255.255.22. để dành cho các mạng có tới 100 user.



Hình 1.1.1. Một ví dụ về địa chỉ IP theo VLSM

1.1.2 Sự phí phạm không gian địa chỉ

Trước đây khi chia subnet cho địa chỉ mạng IP subnet đầu tiên và subnet cuối cùng được khuyến cáo là không sử dụng . Hiện nay với VLSM chúng ta có thể tận dụng subnet đầu tiên và subnet cuối cùng



Subnet Number	Subnet Address	
Subnet 0	192.168.187.0	/27
Subnet 1	192.168.187.32	/27
Subnet 2	192.168.187.64	/27
Subnet 3	192.168.187.96	/27
Subnet 4	192.168.187.128	/27
Subnet 5	192.168.187.160	/27
Subnet 6	192.168.187.192	/27
Subnet 7	192.168.187.224	/27

Hình 1.1.2

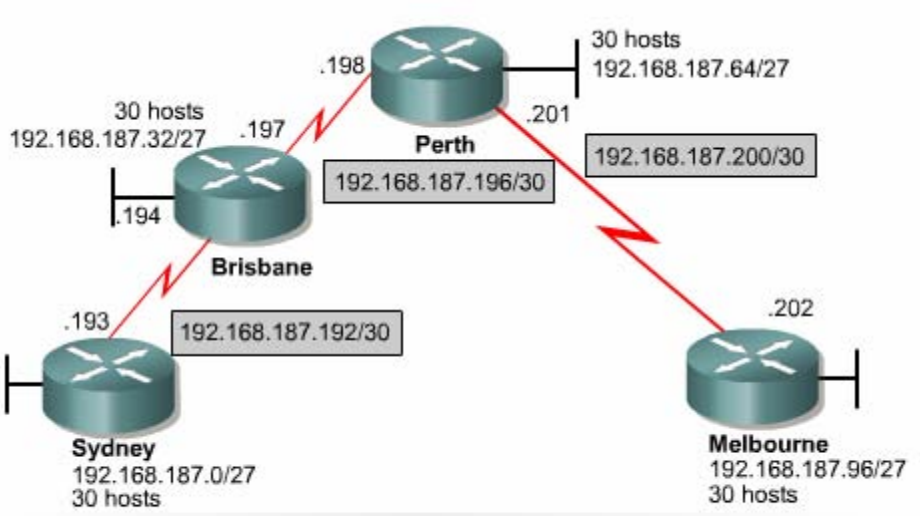
Ta xét ví dụ như hình 1..1.2. người quản trị mạng quyết định mượn 3 bit để chia subnet cho địa chỉ lớp C 192.168.187.0. Nếu sử dụng luôn subnet đầu tiên bằng cách thêm lệnh no ip subnet – zezo vào cấu hình router người quản trị mạng sẽ có 7 subnet sử dụng được mỗi subnet có 30 địa chỉ host Bắt đầu từ Cissco IOS phiên bản 12.0, Cissco router đã mặc định là sử dụng subnet zezo. Bây giờ mối subnet được phân phối cho một mạng LAN trên routerSydney, Brisbane, Perth và Melbourne như hình vẽ 1.1.2.3 subnet còn lại được phân phối cho 3 đường kết nối serial giữa các router. Như vậy là không còn subnet nào để dự phòng cho sự mở rộng mạng về sau. Trong khi đó kết nối serial giữa 2 router là kết nối điểm - đến - điểm nên chỉ có cần 2 địa chi host là đủ. Như vậy là phí mất 28 địa cỉ host trong mỗi subnet được phân phối cho kết nối WAN của router. Với cách chia đều , tất cả các subnet có chiều dài subnet bằng nhau như vạy 1/3 không gian địa chỉ đã bị phí phạm.

Cách phân phối địa chỉ như trên chỉ phù hợp với mạng nhỏ. Nhưng dù sao thì sơ đồ địa chỉ này cũng thực sự phí phạm địa chỉ cho các kết nối điểm - đến - điểm

1.1.3 Khi nào sử dụng VLSM

Thiết kế sơ đồ địa chỉ IP sao cho đáp ứng được sự mở rộng sau này và không phí phạm địa chỉ là một việc hết sức quan trọng. Trong phần này sẽ trình bày cách sử dụng VLSM để không láng phí địa chỉ trên các kết nối điểm - nối - điểm

Cùng với hệ thống mạng ví dụ ở phần trước. Lần này người quản trị mạng sử dụng VLSM để chia địa chỉ mạng lớp C 192.168.187.0 thành nhiều subnet có kích thước khác nhau



Notice the /27 bit masks for the LANs, and the /30 for the serial links

Subnet Number	Subnet Address	
subnet 0	192.168.187.0	/27
subnet 1	192.168.187.32	/27
subnet 2	192.168.187.64	/27
subnet 3	192.168.187.96	/27
subnet 4	192.168.187.128	/27
subnet 5	192.168.187.160	/27
subnet 6	192.168.187.192	/27
subnet 7	192.168.187.224	/27

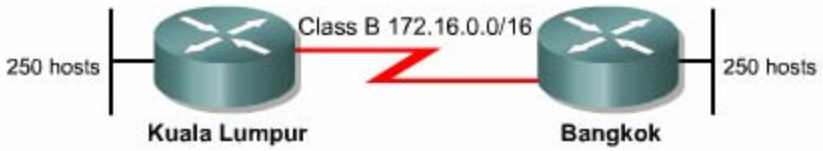
Subnet Number	Subnet Address	
sub-subnet 0	192.168.187.192	/30
sub-subnet 1	192.168.187.196	/30
sub-subnet 2	192.168.187.200	/30
sub-subnet 3	192.168.187.204	/30
sub-subnet 4	192.168.187.208	/30
sub-subnet 5	192.168.187.212	/30
sub-subnet 6	192.168.187.216	/30
sub-subnet 7	192.168.187.220	/30

Hình 1.1.3

Trước tiên ta xét mạng có nhiều user nhất trong hệ thống mạng. Mỗi mạng LAN ở Sydney, Brisbane, Pert và Melbourpe có khoảng 30 host. Do đó để đáp ứng cho các mạng LAN này người quản trị mạng mượn 3 bit để chia subnet cho địa chỉ mạng 192.168.187.0. Tương tự như ví dụ ở phần trước, người quản trị mạng có 7 subnet /27 sử dụng được. Lấy 4 subnet đầu tiên/ 27 để phân phối cho các mạng LAN trên router. Sau đó người quản trị mạng lấy subnet thứ 6 mượn tiếp 3 bit nữa

để chia thành 8 subnet/30 mỗi subnet /30 này chỉ có 2 địa chỉ host. Lấy 3 subnet/30 phân phối cho 3 kết nối serial giữa các router. Các subnet /27 và /30 còn lại được để dành sử dụng về sau

1.1.3 Tính toán chia subnet với VLSM



Each LAN must support over 250 hosts. The Class B network 172.16.0.0/16 can be subnetted with a 24-bit mask (255.255.255.0) to create large enough subnets for each LAN.

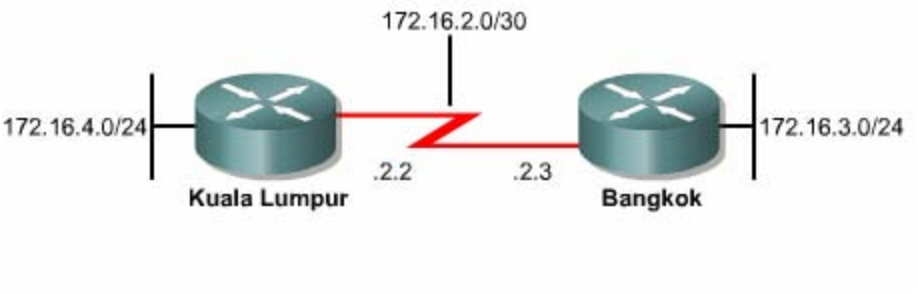
Subnetted Class B as 255.255.255.0

#	ID	Range	Broadcast
0	172.16.0.0	172.16.0.1 - 172.16.0.254	172.16.0.255
1	172.16.1.0	172.16.1.1 - 172.16.1.254	172.16.1.255
2	172.16.2.0	172.16.2.1 - 172.16.2.254	172.16.2.255
3	172.16.3.0	172.16.3.1 - 172.16.3.254	172.16.3.255
4	172.16.4.0	172.16.4.1 - 172.16.4.254	172.16.4.255
5	172.16.5.0	172.16.5.1 - 172.16.5.254	172.16.5.255
6	172.16.6.0	172.16.6.1 - 172.16.6.254	172.16.6.255
7	172.16.7.0	172.16.7.1 - 172.16.7.254	172.16.7.255
8	172.16.8.0	172.16.8.1 - 172.16.8.254	172.16.8.255
9	172.16.9.0	172.16.9.1 - 172.16.9.254	172.16.9.255
10	172.16.10.0	172.16.10.1 - 172.16.10.254	172.16.10.255
11	172.16.11.0	172.16.11.1 - 172.16.11.254	172.16.11.255
12	172.16.12.0	172.16.12.1 - 172.16.12.254	172.16.12.255
13	172.16.13.0	172.16.13.1 - 172.16.13.254	172.16.13.255
14	172.16.14.0	172.16.14.1 - 172.16.14.254	172.16.14.255
15	172.16.15.0	172.16.15.1 - 172.16.15.254	172.16.15.255

Hình 1.1.4.a

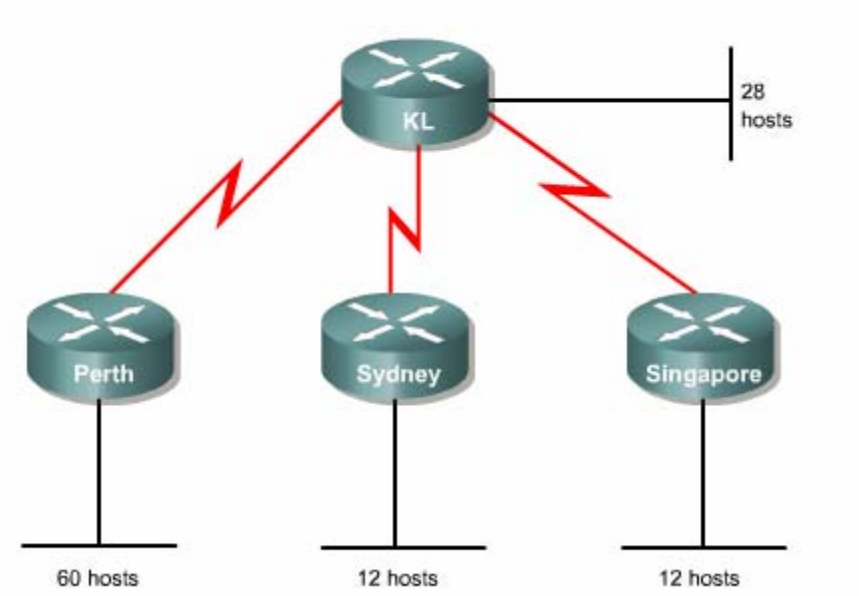
Xét ví dụ như hình 1.1.4.a. Hai mạng LAN ở Kuala Lumpur và Bankok yêu cầu tối thiểu 250 host trong mỗi tháng. Nếu hai router này sử dụng các giao thức tuyến theo lớp địa chỉ không hỗ trợ VLSM như RIPv1 IGRP và EGP thì phải chia subnet đều cho toàn bộ hệ thống mạng. Điều này có nghĩa là chúng ta mượn 8 bit để chia đại chỉ lớp B 172.160.0 thành các subnet /24 rồi phân phối cho tất cả các mạng trong hệ thống. Như vậy mỗi mạng trong hệ thống đều có địa chỉ mạng với 24 bit

mask giống nhau. Mặc dù hai subnet 172.16.3.0/24 và 172.16.4.0/24 đáp ứng được cho 2 mạng LAN 250 host nhưng subnet 172.16.2.0/24 phân phối cho kết nối WAN giữa hai router là quá phí. Một kết nối WAN chỉ cần 2 địa chỉ host còn lại 252 địa chỉ host bị bỏ phí.



Hình 1.1.4.b

Nếu chúng ta sử dụng kỹ thuật VLSM chúng ta có thể lấy subnet 172.16.2.0/24 chia tiếp thành các subnet/30. Sau đó lấy một subnet 172.16.2/20 để đặt cho kết nối WAN thì số lượng địa chỉ bị mất cho kết nối này giảm đi rất nhiều.



Hình 1.1.4.c

Bây giờ ta xét ví dụ như hình 1.1.4.c giả sử ta có địa chỉ mạng lớp C 12.168.10.0/24 để phân phối cho hệ thống mạng này.

Đầu tiên chúng ta xét mạng LAN có nhiều user nhất trong hệ thống. Hệ thống trên hình 1.1.4.c có mạng LAN lớn nhất là 60 host. Nếu chúng ta chia subnet như cách cũ chúng tá se chỉ mượn được 2 bit để chia subnet còn lại 6 bit dành cho host mới đủ đáp ứng cho mạng LAN 60 host. Nhưng như vậy chúng ta chỉ toa được 2^2= 4 subnet, trong đó sử dụng được tối đa 3 subnet không đủ đáp ứng cho toàn bộ hệ thống mạng. Rõ rang cách chia subnet đều không thể đáp ứng được

Chúng ta phải sử dụng VLSM như sau:

1. Bước đầu tiên chúng ta cũng xét mạng LAN lớn nhất trong hệ thống là mạng LAN 60 host ở Perth. Để đáp ứng cho mạng LAN này chúgn ta mượn 2 bit đầu tiên đẻ chia subnet cho địa chỉ 192.168.10/24. Chúng ta sẽ được 4 subnet /26 như sau:

#	ID	Dải địa chỉ host	Địa chỉ quảng bá
0	192.168.10.0	192.168.10.1 – 192.168.10.62	192.168.10.63
1	192.168.10.64	192.168.10.65 – 192.168.10.126	192.168.10.127
2	192.168.10.128	192.168.10.129 – 192.168.10.190	192.168.10.191
3	192.168.10.192	192.168.10.193– 192.168.10.254	192.168.10.255

Chúng ta lấy subnet đầu tiên 192.168.10.0/26 phân phối cho mạng LAN 60 host ở Perth.

2. Bước thứ 2 chúng ta xét tới mạng LAN lớn thứ 2 là mạng LAN 28 host ở KL. Để đáp ứng co mạng LAN này chúng ta lấy subnet tiếp theo là 192.168.10.64/26 mượn tiếp 1 bit nữa để tách thành 2 subnet nhỏ hơn như sau:

#	ID	Dải địa chỉ host	Địa chỉ quảng bá
0	192.168.10.64	192.168.10.65 – 192.168.10.94	192.168.10.95
1	192.168.10.96	192.168.10.97 – 192.168.10.126	192.168.10.127

Mỗi subnet /27 có 5 bit dành cho phần host nên đáp ứng được tối đa 2^{+}-2=30 host. Do đó ta lấy subnet 192.168.10.64/27 để phân phối cho mạng LAN 28 host ở Kuala Lumpur.

2 . Bước thứ 3 chúng ta xét tiếp đến các mạng LAN nhỏ hơn tiếp theo. Chúng ta còn lại hai mạng LAN ở Sydney và Singapore, mỗi mạng 12 host. Để đáp ứng cho hai mạng LAN này chúng ta lấy subnet 12.168.10.96/27 ở trên mượn tiếp 1 bit nữa để tách thành 2 subnet/28 như sau:

#	ID	Dải địa chỉ host	Địa chỉ quảng bá
0	192.168.10.0	192.168.10.1 – 192.168.10.62	192.168.10.63
1	192.168.10.64	192.168.10.65 – 192.168.10.126	192.168.10.127

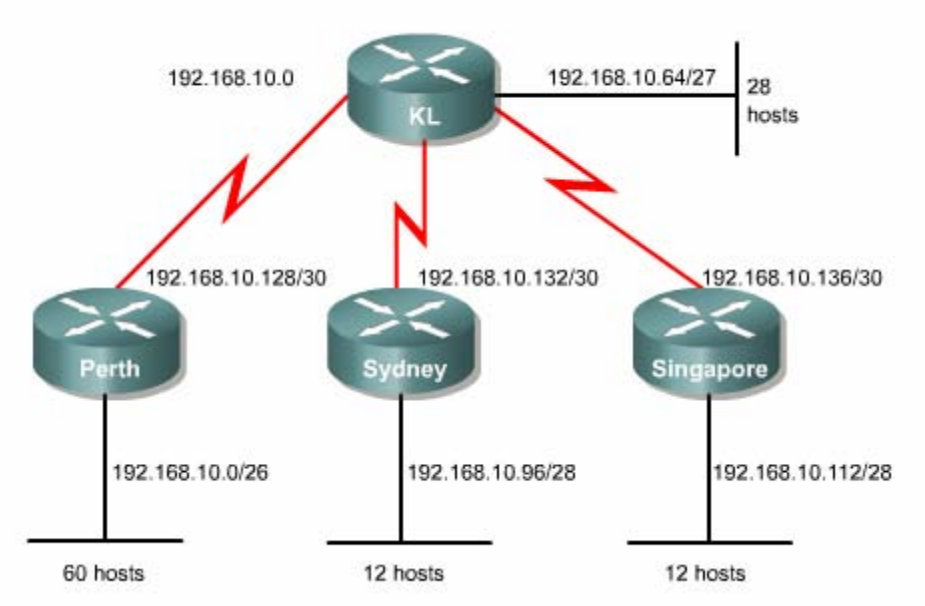
Mỗi subnet /28 còn 4 bit dành cho host nên đáp ứng được tối đa 2^{4+} - 2 =14 host. Chúng ta lấy hai subnet /28 trong bảng trên phân phối cho hai mạng LAN ở Sydney và Singapore

3. Bước cuối cùng bây giờ chúng ta chỉ còn lại ba đường liên kết WAN giữa các router, mỗi đường liên kết cần 2 địa chỉ host. Từ đầu đến giờ, chúng ta đã sử dụng hết dải địa chỉ từ 192.168.10.0 192.168.10.27. Bây giờ chúng ta lấy tiếp subnet 192.168.10.128/26 đã tạo ra ở bước 1, mượn tiếp 4 bit để tạo thành 16 subnet/30 như sau:

#	ID	Dải địa chỉ host	Địa chỉ quảng bá
0	192.168.10.28	192.168.10.129 – 192.168.10.130	192.168.10.131
1	192.168.10.132	192.168.10.133 – 192.168.10.134	192.168.10.135
2	192.168.10.136	192.168.10.137– 192.168.10.138	192.168.10.139
3	192.168.10.140	192.168.10.141 – 192.168.10.142	192.168.10.143
4	192.168.10.144	192.168.10.145 – 192.168.10.146	192.168.10.147
5	192.168.10.148	192.168.10.149 – 192.168.10.150	192.168.10.151
6	192.168.10.152	192.168.10.153– 192.168.10.154	192.168.10.155
7	192.168.10.156	192.168.10.157– 192.168.10.158	192.168.10.159
8	192.168.10.160	192.168.10.161 – 192.168.10.162	192.168.10.163
9	192.168.10.164	192.168.10.165 – 192.168.10.166	192.168.10.167
10	192.168.10.168	192.168.10.169 – 192.168.10.170	192.168.10.171
11	192.168.10.172	192.168.10.173 – 192.168.10.174	192.168.10.175
12	192.168.10.176	192.168.10.177– 192.168.10.178	192.168.10.179
13	192.168.10.180	192.168.10.181– 192.168.10.182	192.168.10.183
14	192.168.10.184	192.168.10.185– 192.168.10.186	192.168.10.187
15	192.168.10.188	192.168.10.189– 192.168.10.190	192.168.10.191

Chúng ta lấy 3 subnet /30 đầu tiên trong bảng trên để phân phối cho các đường WAN giữa các router:

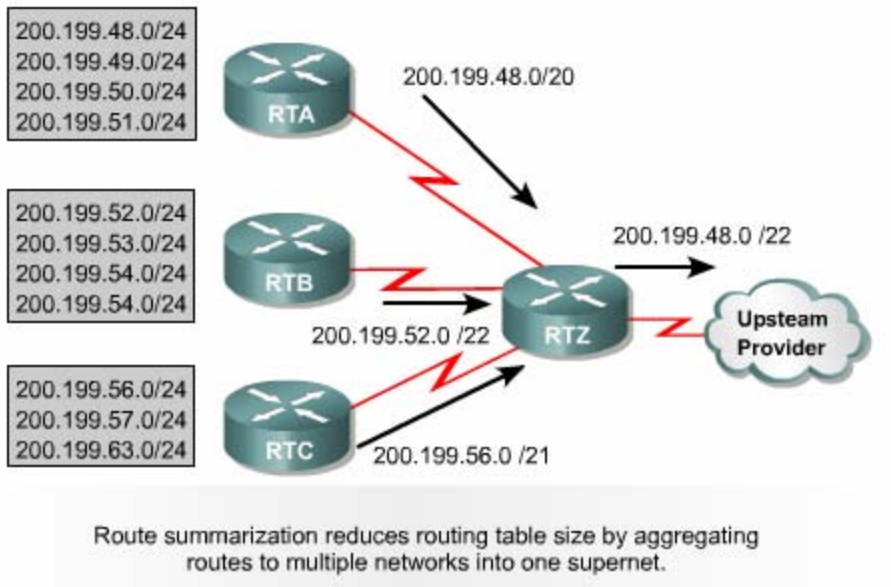
Kết quả sơ đồ phân phối địa chỉ theo VLSM được thể hiện ở hình 1.1.4.d



Hình 1.1.4.d

Quá trình địa chỉ IP theo VLSM ở trên được tóm tắt lại theo sơ đồ sau: 1.1.5 Tổng hợp địa chỉ với VLSM.

Khi sử dụng VLSM các bạn nên cố gắng phân bố các subnet liền nhau ở gần nhau để có thể tổng hợp địa chỉ. Trước 1997 không có tổng hợp địa chỉ hệ thống định tuyến xương sống của Internet gần như bị sụp đổ mấy lần.



Hình 1.1.5

Hình 1.1.5 là một ví dụ cho thấy sự tổng hợp địa chỉ lên các router tầng trên. Thực chất tổng hợp địa chỉ là bài toán đi ngược lại bài toán chia địa chỉ theo VLSM. Nếu như ví dụ ở phần 1.1.4 là một bài toán đi từ một địa chỉ mạng lớn 192.168.1.0/24 chi thành nhiều tầng subnet nhỏ hơn thì bây giờ bài toán ở hình 1.1.5 đi ngược lại, từ các subnet con tổng hợp lại thành subnet lớn hơn. Tổng hợp dẫn cho đến khi thành một địa chỉ mạng lớn 200.199.48.0/22 đại diện chung cho toàn bộ các subnet bên trong hệ thống.

Tương tự như VLSM các bạn muốn thực hiện được tổng hợp địa chỉ thì phải chạy giao thức định tuyến không theo lớp địa chỉ như OSPF EIGRP vì các giao thức này có truyền thông t in về subnet mask đi kèm với địa chỉ IP subnet trong các thông tin định tuyến. Mặt khác bạn muốn tổng hợp địa chỉ đúng thì khi chia địa chỉ theo VLSM để phân phối cho hệ thống mạng bạn phải chi a theo cấu trúc phân cấp như ví dụ ở phần 1.1.4 và phân phối các subnet liền nhau ở cạnh tranh nhau trong cấu trúc mạng.

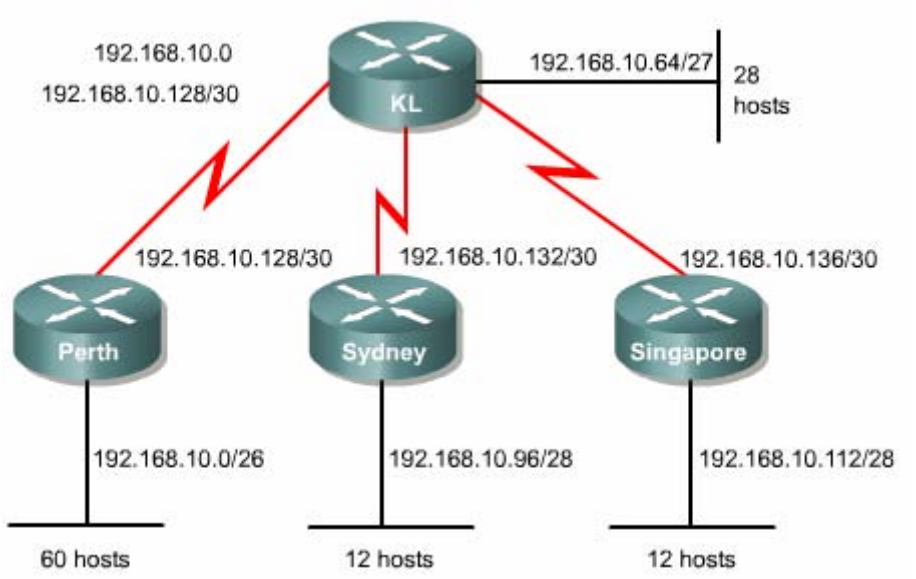
Sau đây là một số nguyên tắc bạn cần nhớ:

1. Mỗi router phải biết địa chỉ subnet cụ thể của tất cả các mạng kết nối trực tiếp vào nó
2. Mỗi router không cần phải gửi thông tin chi tiết về mỗi subne t của nó cho các router khác nếu như nó có thể tổng hợp các subnet thành một địa chỉ đại diện được
3. Khi tổng hợp địa chỉ như vậy bảng định tuyến của các router tầng trên sẽ được rút gọn lại

3.1.6 Cấu hình VLSM

Sauk hi chia địa chỉ IP theo VLSM xong thì bước tiếp theo là bạn cung cấp địa chỉ IP cho từng thiết bị trong hệ thống. Việc cấu hình địa chỉ IP choa các cổng giao tiếp của router vẫn như vậy. không có gì đặc biệt.

Ví dụ như hình 1.1.6 sau khi đã phân phối địa chỉ theo VLSM xong bạn cấu hình địa chỉ IP cho các cổng giao tiếp của router như sau:



Hình 1.1.6

3.2 Rip phiên bản 2

1.2.1 Lịch sử của RIP

Internet là một tập hợp các hệ tự quản. Mỗi Á có một cơ chế quản trị, một công nghệ định tuyến riêng, khác với các AS khác. Các giao théc định tuyến được sử dụng bên trong một AS được gọi là giao thức định tuyến nội vi IGP. Để thực hiện định tuyến giữa các AS với nhau chúng ta phải sử dụng mọt giao thức riêng gọi la giao thức định tuyến ngoại vi EGP. RIP được thiết kế như là một giao thức IGP dùng cho các AS có kích thước nhỏ không sử dụng cho các hệ thống mạng lớn và phức tạp.

RIPv1 là một giao thức định tuyến theo vectơ khoảng cách nên quảng bá toàn bộ bảng định tuyến của nó cho các router láng giềng theo định kỳ. Chu kỳ cập nhật của RIP là 30 giây. Thông số định tuyến của RIP là số lượng hop, giá trị tối đa là 15 hop.

RIPv1 là giao thức định tuyến theo lớp địa chỉ, Khi RIP router nhận thông tin về một mạng nào đó từ một cổng, trong thông tin định tuyến này không có thông tin về subnet mask đi kèm. Do đó router sẽ lấy subnet mask của cổng để áp dụng cho địa chỉ mạng mà nó nhận được từ cổng này. Nếu subnet mask này không phù hợp thì nó sẽ lấy subnet mask mặc định theo lớp địa chỉ để áp dụng cho địa chỉ mạng mà nó nhận được.

Địa chỉ lớp A có subnetmask mặc định là 255.0.0

Địa chỉ lớp B có subnet mask mặc định là 255.255.0.0

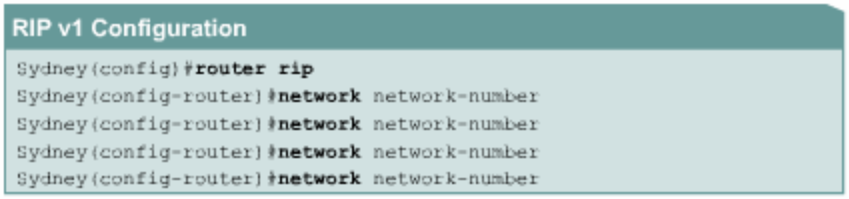
Địa chỉ lớp c có subnet mask mặc định là 255.255.255.0

RIPv1 l à giao th ức đ ịnh tuyến được sử dụng phổ biến vì mọi router IP đều có hỗ trợ giao thức này. RIPv1 được phổ biến vì tính đơn giản và tính tương thích toàn cầu của nó. RIPv1 có thể chia tải ra tối đa là 6 đường có chi phí bằng nhau.

Sau đây là những điểm giới hạn của RIPv1:

- Không gửi thông tin subnet mask trong thông tin định tuyến
- Gửi quảng bá thông tin định tuyến theo địa chỉ 255.255.255.255
- Không hỗ trợ xác minh thông tin định tuyến
- Không hỗ trợ VLSM và CIDR

RIPv1 được cấu hình đơn giản như trong hình 1.2.1



Hình 1.2.1

1.2.2 Đặc điểm của RIP phiên bản 2

RIPv2 được phát triển từ RIPv1 nên nó vẫn có các đặc điểm như RIPv1

- Là một giao thức định tuyến theo vectơ khoảng cách sử dụng số lượng hop làm thông số định tuyến
- Sử dụng thời gian holddown để chống lặp vòng, thời gian này mặc định là 180 giây
- Sử dụng cơ cế split horizon để chống lặp vòng
- Giá trị hop tối đa là 15

RIPv2 có gửi subnet mask đi kèm với các địa chỉ mạng trong thông tin định tuyến. Nhờ đó RIPv2 có thể hỗ trợ VLSM và CIDR

RIPv2 có hỗ trợ việc xác minh thông tin định tuyến. Bạn có thể cấu hình cho RIP gửi và nhận thông tin xác minh trên cổng giao tiếp của router bằng mã hoá MD hay không mã hoá

RIPv2 gửi thông tin định tuyến theo địa chỉ multicast 224.0.0.9

1.2.3 So sánh RIPv1 và RIPv2

RIP sử dụng thuật toán định tuyến theo vectơ khoảng cách. Nếu có nhiều đường đến cùng một đích thì RIP sẽ chọn đường có số hop ít nhất. Chính vì dựa vào số lượng hop để chọn đường nên đôi khi con đường mà RIP chọn không phải là đường nhanh nhất đến đích

RIPv1 cho phép các router cập nhật bảng định tuyến của chúng theo chu kỳ mặc định là 30 giây. Việc gửi thông tin định tuyến cập nhật liên tục như vậy giúp cho topo mạng được xây dụng nhanh chóng. Để tránh bí lặp vòng vô tận. RIP giới hạn số hop tối đa để chuyển gói là 15hop . Nếu tới được và gói dữ liệu đến đó sẽ bị huỷ bỏ. Điều này làm giới hạn khả năng mở rộng của RIP. RIPv1 sử dụng cơ chế split horizon để chống lặp vòng. Với cơ chế này khi gửi thông tin định tuyến ra một cổng giao tiếp RIPv1 router không gửi ngược trở lại các thông tin định tuyến mà nó học được từ chính cổng đó. RIPv1 còn sử dụng thời gian holddown để chống lặp vòng. Khi nhận được một thông báo về một mạng đích bị sự cố router sẽ khởi động thời gian holddown . Trong suốt khoảng thời gian holddown router sẽ không cập nhật tất cả các thong tin có thông số định tuyến xấu hơn về mạng đích đó

RIPv2 được phát triển từ RIPv1 nên nó cũng có các đặc tính như trên. RIPv2 cũng là giao thức

Là một giao thức định tuyến theo vetơ khoảng cách sử dụng số lượng hop làm thông số định tuyến

Sử dụng thời gian holddown để chống lặp vòng thời gian này mặc định là 180 giây

Sử dụng cơ chế spit horizon để chống lặp vòng

Giá trị hop tối đa

RIPv2 có gửi subnet mask đi kèm với cácđịa chỉ mạng trong thông tin định tuyến. Nhờ đó, RIPv2 có thể hỗ trợ VLSM và CIDR

Ripv2 có hỗ trợ việc xác minh thông tin định tuyến. Bạn có thể cấu hình cho RIP gửi và nhận thông tin xác minh trên cổng giao tiếp của router bằng mã hoá MD5 hay không mã hoá

RIPv2 gửi thông tin định tuyến theo địa chỉ multicaskt 224.0.0.9

1.2.3 So sánh RIPv1 và RIPv2

RIP sử dụng thuật toán định tuyến theo vectơ khoảng cách. Nếu có nhiều đường đến cùng một đích thì RIP sẽ chọn đường có số hop ít nhất. Chính vì chỉ dựa vào số lượng hop để chọn đường nên đôi khi con đường mà RIP chọn không phải là đường nhanh nhất đến đích

RIPv1 cho phép các router cập nhật bảng định tuyến của chúng theo chu kỳ mặc định là 30 giây. Việc gửi thông tin định tuyến cập nhật liên tục như vậy giúp cho topo mạng được xây dựng nhanh chóng. Để tránh bị lặp vòng vô tận, RIP giới hạn số hop tối đa để chuyển gói là 15 hop. Nếu một mạng đích xa hơn 15 router thì xem như mạng đích đó không thể tới được và gói dữ liệu. đó sẽ bị huỷ bỏ . Điều này làm giới hạn khả năng mở rộng của RIP , RIPv1 sử dụng cơ chế split horizon để chống lặp vòng. Với cơ chế này khi gửi thông tin định tuyến ra một cổng giao tiếp , RIPv1 router khônggửi ngược trở lại các thông tin định tuyến mà nó học đước từ chính cổng dó, RIPv1 còn sử dụng thời gian holddown để chống lặp vòng. Khi nhận được một thông báo về một mạng đích bị sự cố, router sẽ khởi động thời gian holddown. Trong suốt khoảng thời gian holddown router sẽ không cập nhật tất cả các thông tin có thông số định tuyến xấu hơn về mạng đích đó

RIPv2 được phát triển từ RIPv1 nên nó cũng có các đặc tính như trên RIPv2 cũng là giao thức định tuyến theo vectơ khoảng cách sử dụng số lượng hop làm thông số định tuyến duy nhất . RIPv2 cũng sử dụng thời gian holddown và cơ chế split horizon để tránh lặp vòng

Sau đây là các điểm khác nhau giữa RIPv1 và RIPv2

RIPv1	RIPv2
Cấu hình đơn giản	Cấu hình đơn giản
Định tuyến theo lớp địa chỉ	Định tuyến không theo lớp địa chỉ
Không gửi thông tin về subnet mask trong thông tin định tuyến.	Có gửi thông tin về subnet mask trong thông tin định tuyến.
Không hỗ trợ VLSM. Do đó tất cả các mạng trong hệ thống RIPv1 phải có cùng subnet mask.	Hỗ trợ VLSM. Các mạng trong hệ thống IPv2 có thể có chiều dài subnet mask khác nhau.
Không có cơ chế xác minh thông tin định tuyến.	Có cơ chế xác minh thông tin định tuyến.
Gửi quảng bá theo địa chỉ 255.255.255.255.	Gửi multicast theo địa chỉ 224.0.0.9 nên hiệu quả hơn.

1.2.4. Cấu hình RIPv2

Để cấu hình một giao thức định tuyến động, chúng ta đều thực hiện các bước sau

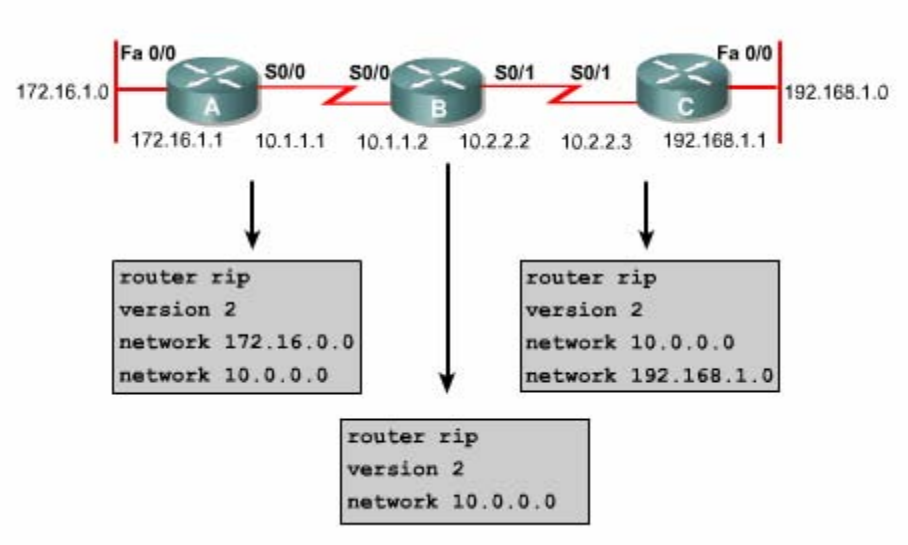
Chọn giao thức định tuyến, ví dụ như RIPv2 chẳng hạn

Khai báo các địa chỉ mạng IP cho giao thức định tuyến không cần khai báo giá trị subnet mask

Khai báo địa chỉ IP và subnet mask cho các cổng router

Lệnh network khai báo địa chỉ mạng IP tham gia và tiến trình định tuyến. Cổng nào của router có địa chỉ IP rơi vào trong địa chỉ mạng được khai báo ở lệnh network thì cổng đó sẽ tham gia vào quá trình gửi và nhận thông tin định tuyến cập nhật. Mặt khác lệnh network cũng khai báo những địa chỉ mạng mà router sẽ thực hiện quảng cáo về mạng đó

Lệnh router rip version 2 xác định RIPv2 được chọn làm giao thức định tuyến chạy trên router



Hình 1.2.4.a

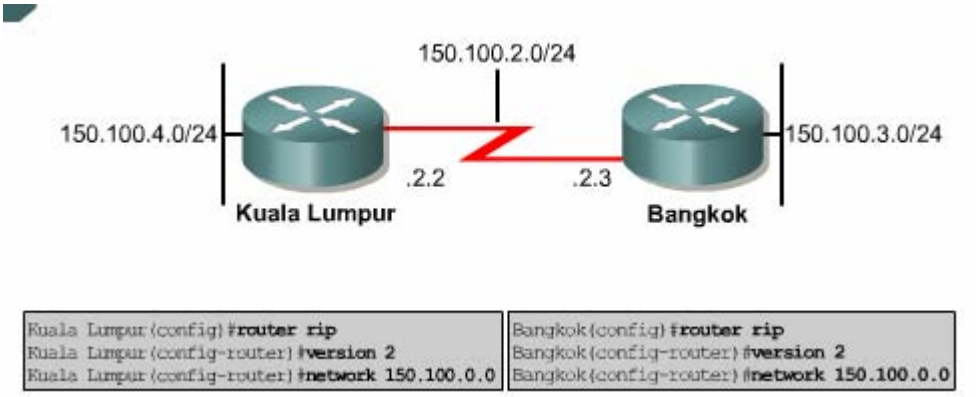
Trong ví dụ ở hình 1.2.4.a router A được cấu hình như sau router rip - chọn rip làm giao thức định tuyến

Version 2 – Xác định ripv2

Network 172.16.0.0 – khai báo địa chỉ mạng kết nối trực tiếp vào router A

Network 10.0.0.0 – Khai báo địa chỉ mạng kết nối trực tiếp vào router A

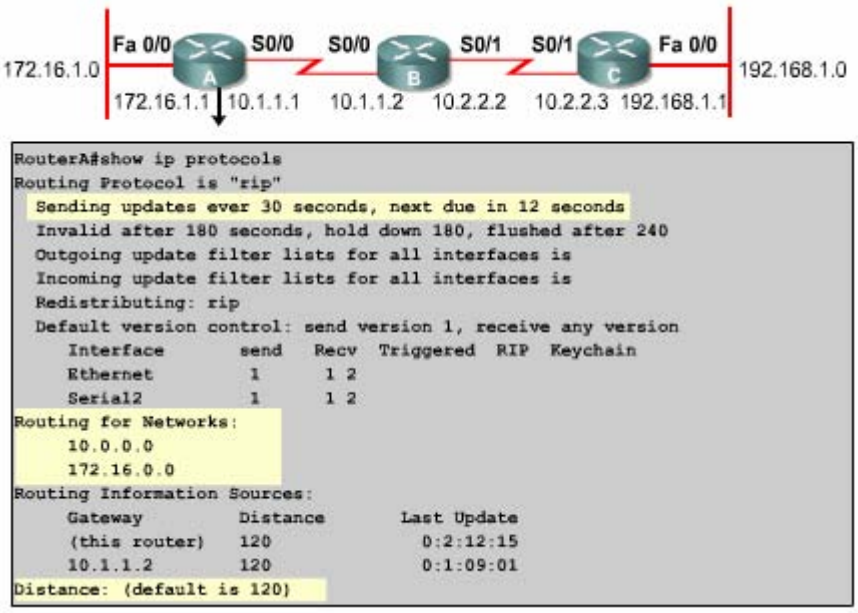
Khi đó tất cả các cổng trên router A kết nối vào mạng hoặc subnet trong 172.16.0.0 và 10.0.0.0 sẽ gửi và nhận thông tin cập nhật RIPv2



Hình 1.2.4.b

1.2.5 Kiểm tra RIPv2

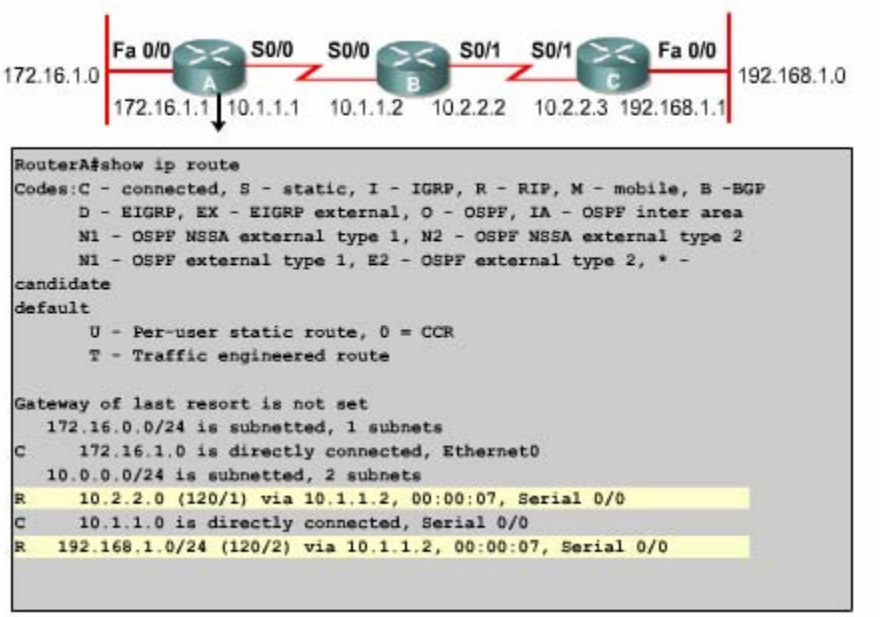
Lênh show ip protocol sẽ hiển thị các giá trị của giao thức định tuyến và các thời gian hoạt động của giao thức đó. Trong ví dụ ở hình 1.2.5.a lệnh này cho thấy router được cấu hình với RIP không nhận được bất kỳ thông tincập nhật nào từ một router láng giềng trong 180 giây hoặc hơn thì những con đường học được từ router láng giềng đó sẽ được xem là không còn giá trị. Nếu vẫn không nhận thông tin cập nhật gì cả thì sau 240 giây, các con đường này sẽ bị xoá khỏi bảng định tuyến . Trong hình router A nhận được cập nhật mới nhấttừ router B cách đây 12 giây. thời gian holddown 180 giây. Khi có một con đường được thông báo là đã b ị ngắt con đường đó sẽđược đặt vào trạng thái holddown trong 180 giây



Hình 1.2.5.a

Router sẽ gửi thông tin về các đường đi trong các mạng được liệt kê sau dòng routing for networks. Router nhận được các thông tin cập nhật từ các router láng giềng được liệt kê sau dòng routing information sources chỉ số độ tin cậy mặc định của rip là 120

Lệnh show ip interface brief được sử dụng để tổng hợp thông tin trạng thái của các cổng trên router



Hình 1.2..5.b

Lệnh show ip route sẽ hiển thị nội dụng bảng định tuyến Ip . Trong bảng định tuyến cho biết về đường đi đến các mạng đích mà router học được đồng thời cho biết các thông tin này được học như thế nào

Nếu thông tin trong bảng định tuyến bị thiếu một đường đi nào thì bạn nên dùng lệnh show running – config hoặc show ip protocols để kiểm tra lại cấu hình định tuyến

1.2.6 Xử lý sự cố RIPv2

Sử dụng lện debug ip rip để hiển thị các thông tin định tuyến RIP khi chúng được gửi đi và nhận vào. Bạn dùng lệnh no debug all hoặc undebug all để tắt mọi debug đang bật

Ta xét ví dụ như hnhf 1.2..6 router A nhận được thông tin về hai mạng đích trên cổng serial 2 từ router láng giềng có địa chỉ IP là 10.11.2 . Router A cũng gửi thông tin cập nhật của nó ra hai cổng ethernel và serial 2 với địa chỉ là địa chỉ quảng bá còng địa chỉ ngoặc là địa chỉ IP nguồn

Đôi khi bạn còn gặp một số câu thông báo trong lệnh debug ip rip như sau

Những câu này xuất hiện khi router mới khởi động lên hoặc khi có một sự cố mới xảy ra như một cổng bị thay đổi trạng thái hay router bị xoá mất bảng định tuyến

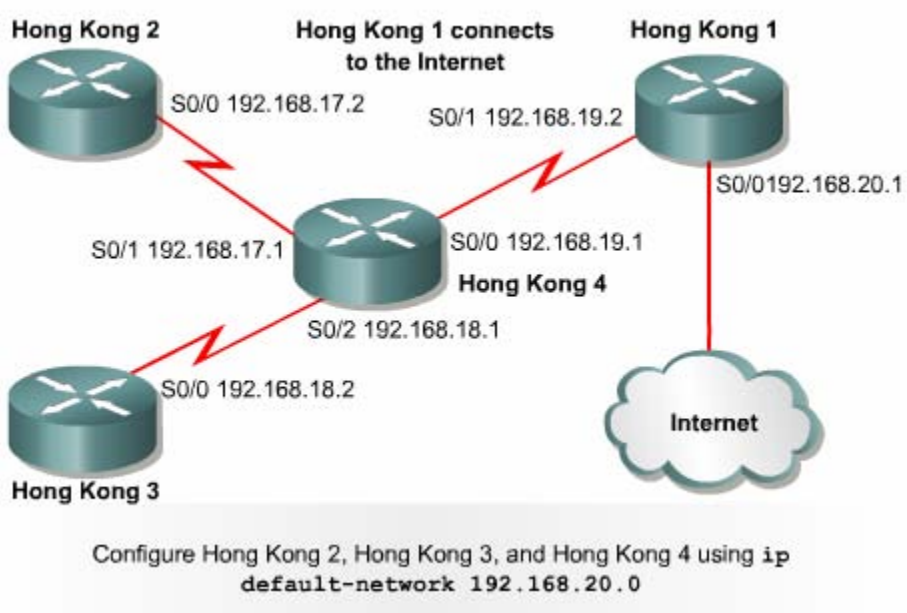
1.2.7 Đường mặc định

Mặc định router học thông tin về đường đến mạng đích bằng 3 cách sau'

Đường cố định – là đường do người quản trị mạng cấu hình bằng tay cho router trong đó chỉ định rõ router kế tiếp để tới mạng đích. Đường cố định có khả năng bảo mật cao vì khong có hoạt động gửi thông tin cập nhật như đường định tuyến động. Đường cố định rất hữu dụng khi chỉ có một đường duy nhất đến đích không còn đường nào khác phải chọn lựa

Đường mặc định cũng do người quản trị mạng cấu hình bằng tay cho router. Trong đó khai báo đường mặc định để sử dụng khi router không biết đường đến đích. Với đường mặc định định tuyến router sẽ dược ngắn gọn hơn. Khi gói dữ liệu có địa chỉ mạng đích mà router sẽ gửi nó ra đường mặc định

Đường định tuyến động là những đường do router học được từ các router khác nhờ giao thức định tuyến động



Hình 1.2.7

giả sử hệ thống mạng này sử dụng giao thức định tuyến động .Router HK1 có kết nối ra internet,kết nối này là đường mặc định của toàn bộ hệ thống mạng bên

trong.Những gói nào khôn gửi đến các mạng bên trong nội bộ mà gửi ra ngoài thì mặc nhiên sẽ được gửi lên đường mặc định ra internet. Để khai báo đường mặc định cho router HK1chúng ta dùng lện sau :I b

HongKong1(config)#ip route 0.0.0.0 0.0.0.0 192.168.20.2

Lệnh trên là lệnh cấu hình đường cố định đặc biệt đại diện cho bất kì mạng đích nào với bất kì subnetmask nào .Xin nhấn mạnh một lần nữa , lệnh trên được sử dụng để khai báo đường măc định cho router nào có kết nối đường mặc định vào nó

Các router còn lại trong hệ thống, ta dùng lệnh ip default-network để khai báo mạng mặc định này cho các router:

Router(config)#ip default-network 192.168.20.0

Các router HK2,HK3,HK4 sẽ sử dụng mang 192.168.20.0 làm mạng đích mặc định .Những gói dữ liệu nào có địa chỉ đích mà các router nào không tìm thấy trên bảng định tuyến của chúng thì chúng sẽ gửi về mạng mặc định 192.168.20.0.Kết quả là các gói dữ lieu này được chuyển tớ i router HK1. Trên router HK1 , với khai báo mặc định la iproute 0.0.0.0 0.0.0.0 192.168.20.2, các gói dữ liệu sẽ được truyền ra đường kết nối với Internet

TỔNG KẾT

Sau đây là các điểm quan trọng trong chương này

VLSM và lí do sử dụng nó

Chia địa chỉ mạng IP thành các subnet có kích thước khác nhau bằng VLSM

cấu hình router sử dụng VLSM

Dặc điểm chính của RIPv1 và RIPv2

Điểm khác nhau quan trọng giữa RIP1và RIPv2

Cấu hình RTPv2

Kiểm tra và xử lí sự cố hoạt động RTPv2

Cấu hình đường mặc định bằng lệnh ip route và ip default-network .

Chương 2: OSPF ĐƠN VÙNG

GIỚI THIỆU

Giao thức định tuyến nội vi (IGP) có 2 loại chính là định tuyến theo vector khoảng cách và định tuyến theo trạng thái đường liên kết. Cả 2 loại giao thức định tuyến này đều thực hiện định tuyến trong phạm vi một hệ tự quản. Chúng sử dụng 2 phương pháp khác nhau để thực hiện cùng một nhiệm vụ.

Thuật toán định tuyến trạng thái theo đường liên kết, hay còn gọi là thuật toán chọn đường ngắn nhất (SPF – Shortest Path First), lưu giữ một cơ sở dữ liệu phức tạp các thông tin về cấu trúc hệ thống mạng. Thuật toán này có đầy đủ thông tin về các router trên đường đi và cấu trúc kết nối của chúng. Ngược lại, thuật toán định tuyến theo vectơ khoảng các không cung cấp thông tin cụ thể về cấu trúc đường đi trong mạng và hoàn toàn không có nhận biết về các router trên đường đi.

Để có thể cấu hình, kiểm tra và xử lý sự cố của các giao thức định tuyến theo trạng thái đường liên kết thì việc hiểu các hoạt động của chúng là điều rất quan trọng. Chương này sẽ giải thích cách làm việc của giao thức định tuyến theo trạng thái đường liên kết, liệt kê các đặc điểm của chúng, mô tả thuật toán mà chúng sử dụng và đồng thời chỉ ra các ưu nhược điểm của loại giao thức này.

Ban đầu, các giao thức định tuyến như RIPv1 đều là các giao thức định tuyến theo vectơ khoảng cách. Ngày nay, có rất nhiều giao thức định tuyến theo vectơ khoảng cách đang được sử dụng như RIPv2. IRGP và giao thức định tuyến lai EIGRP. Khi hệ thống mạng ngày càng phát triển lớn hơn và phức tạp hơn thì những điểm yếu của giao thức định tuyến theo vectơ khoảng cách lại càng bộc lộ rõ hơn. Router sử dụng giao thức định tuyến theo vectơ khoảng cách học thông tin định tuyến bằng cách cập nhật bảng định tuyến từ các router láng giềng kết nối trực tiếp. Hoạt động cập nhật theo định kỳ này chiếm băng thông cao và cách học thông tin định tuyến như vậy làm cho mạng hội tụ chậm.

Giao thức định tuyến theo trạng thái đường liên kết thì khác với giao thức định tuyến theo vectơ khoảng cách. Giao thức này phát các thông tin về đường đi cho mọi router để các router trong mạng đều có cái nhìn đầy đủ về cấu trúc hệ thống mạng. Hoạt động cập nhật chỉ được thực hiện khi có sự kiện thay đổi, do đó băng thông được sử dụng hiệu quả hơn và mạng hội tụ nhanh hơn. Ngay khi có sự thay

đổi trạng thái của một đường liên kết, thông tin được phát ra cho tất cả các router trong mạng.

OSPF là một trong những giao thức quan trọng nhất của loại giao thức định tuyến theo trạng thái đường liên kết. OSPF dựa trên một chuẩn mở nên nó có thể được sử dụng và phát triển bởi các nhà sản xuất khác nhau. Đây là một giao thức phức tạp được triển khai cho các mạng lớn. Các vấn đề cơ bản về OSPF sẽ được đề cập đến trong chương này.

Cấu hình Cisco router cũng tương tự như cấu hình các giao thức định tuyến khác. Đầu tiên OSPF cũng phải được khởi động trên router, sau đó khai báo các mạng mà OSPF được phép hoạt động trên đó. Ngoài ra, OSPF cũng có một số đặc tính riêng và cấu hình riêng. Các đặc tính riêng này đã làm cho OSPF trở thành một giao thức định tuyến mạnh nhưng đồng thời tạo nên những thách thức khi cấu hình OSPF.

Trong hệ thống mạng lớn, OSPF có thể được cấu hình mở rộng trên nhiều vùng khác nhau. Nhưng trước khi có thể thiết kế và triển khai mạng OSPF lớn thì bạn phải nắm được cấu hình OSPF trên một vùng. Do đó chương này sẽ mô tả cấu hình OSPF đơn vùng.

Sau khi hoàn tất chương này, các bạn có thể thực hiện các nhiệm vụ sau:

- Xác định các đặc tính quan trọng của giao thức định tuyến theo trạng thái đường liên kết.
- Giải thích được giao thức định tuyến theo trạng thái đường liên kết xây dựng và duy trì thông tin định tuyến như thế nào.
- Phân tich về thuật toán định tuyến theo trạng thái theo trạng thái đường liên kết.
- Xác định ưu và nhược điểm cua loại giao thức định tuyến theo trạng thái đường liên kết.
- So sánh và phân biệt giao thức định tuyến theo trạng thái đường liên kết với giao thức định tuyến theo vectơ khoảng cách.
- Khởi động OSPF trên router.
- Cấu hình địa chỉ loopback để định quyền ưu tiên cho router.
- Thay đổi thông số chi phí để thay đổi quyết định chọn đường của OSPF.
- Cấu hình cho OSPF thực hiện quá trình xác minh.
- Thay đổi các thông số thời gian của OSPF.

- Mô tả các bước tạo và quảng bá đường mặc định vào OSPF.
- Sử dụng các lệnh show để kiểm tra hoạt động của OSPF.
- Cấu hình tiến trình định tuyến OSPF.
- Định nghĩa các thuật ngữ quan trọng của OSPF.
- Mô tả các loại mạng OSPF.
- Mô tả giao thức OSPF Hello.
- Xác định các bước cơ bản trong hoạt động của OSPF.

2.1. Giao thức định tuyến theo trạng thái đường liên kết

2.1.1. Tổng quan về giao thức định tuyến theo trạng thái đường liên kết

Giao thức định tuyến theo trạng thái đường liên kết hoạt động khác với giao thức định tuyến theo vectơ khoảng cách. Trong phần này sẽ giải thích những điểm khác nhau này. Đây là những kiến thức cực kỳ quan trọng đối với 1 nhà quản trị mạng. Một điểm khác nhau quan trọng mà bạn cần nhớ là giao thức định tuyến theo vectơ khoảng cách sử dụng phương pháp trao đổi thông tin định tuyến đơn giản hơn.

Thuật toán định tuyến theo trạng thai đường liên kết xây dựng và duy trì một cơ sở dữ liệu phức tạp của thông tin về cấu trúc mạng. Trong khi thuật toán định tuyến theo vectơ khoảng cách không cung cấp thông tin cụ thể về đường đi trong mạng và cũng không có nhận biết về các router khác trên đường đi, thì thuật toán định tuyến theo trạng thái đường liên kết có đầy đủ thông tin về các router trên đường đi và cấu trúc kết nối của chúng.

Loại giao thức	Ví dụ	Đặc điểm
Định tuyến theo vectơ khoảng cách	RIPv1 và RIPv2 Intẻio Gateway Routing Protocol (IGRP).	• 1.Copy bảng định tuyến cho router láng giềng. • 2.Cập nhật định kì. • 3.RIPv1 và RIPv2 sử dụng số lượng hop làm thông số định tuyến. • 4.Mỗi router nhìn hệ thống mạng theo sự chi phối của các router láng giềng. • 5.Hội tụ chậm.

		• 6.Dễ bị lặp vòng. • 7.Dễ cấu hình và dễ quản trị. • 8.Tốn nhiều băng thông.
Định tuyến theo trạng thai đương liên kết	Open Shortest Path First (OSPF) Intermediate – System to Intermedia – Sýtem (IS-IS)	• Sử dụng đường ngắn nhất. • Chỉ cập nhật khi có sự kiện xảy ra. • Gửi 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 và năng lượng xử lý hơn so với định tuyến theo vectơ khoảng cách. • Tốn ít băng thông hơn so với định tuyến theo vectơ khoảng cách.

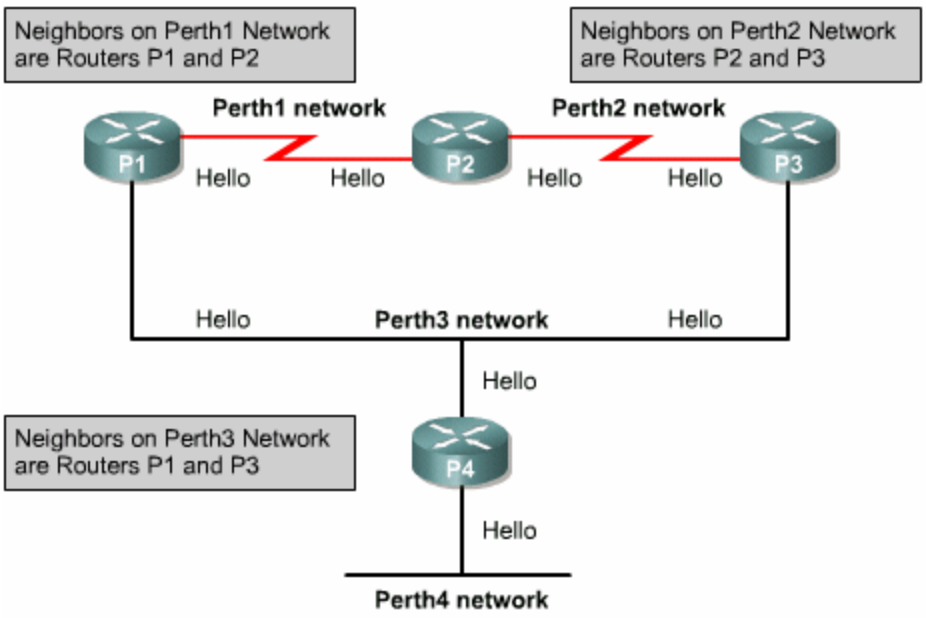
2.1.2. Đặc điểm của giao thức định tuyến theo trạng thái đường liên kết .

Giao thức định tuyến theo trạng thái đường liên kết thu thập thông tin về đường đi từ tất cả các router khác trong cùng hệ thống mạng hay trong cùng một vùng đã được xác định. Khi tất cả các thông tin đã được thu thập đầy đủ thì sau đó mỗi router sẽ tự tính toán để chọn ra đường đi tốt nhất cho nó đến các mạng đích trong hệ thống. Như vậy mỗi router có một cái nhìn riêng và đầy đủ về hệ thông mạng,khi đó chúng sẽ không còn truyền đi các thông tin sai lệch mà chúng nhận được từ các router láng giềng.

Sau đây là một số hoạt động của giao thức định tuyến theo trạng thái đường liên kết:

- Đáp ứng nhanh theo sự thay đổi của hệ thống mạng.
- Gửi cập nhật khi hệ thống mạng có sự thay đổi.
- Gửi cập nhật định kỳ để kiểm tra trạng thái đường liên kết.
- Sử dụng cơ chế hello để xác định router láng giềng có còn kết nối được hay không.

Mỗi router gửi multicast gói hello để giữ liên lạc với các router láng giềng.Gói hello mang thông tin về các mạng kkết nối trực tiếp vào router.Ví dụ như hình 2.1.2, P4 nhận biết các láng giềng của nó trong mạng Perth3 là P1và P3. LSAs cung cấp thông tin cập nhật về trạng thái đường liên kết của các router trong mạng.



Hình 2.1.2. Sử dụng hello để xác định router láng giềng trên từng mạng.

Sau đây là các đặc điểm hoạt đông của router sử dụng giao thức định tuyến theo trạng thái đường liên kết:

1. Sử dụng thông tin từ gói hello và LSAs nhận được từ các router láng giềng để xây dựng cơ sở dữ liệu về cấu trúc hệ thống mạng.
2. Sử dụng thuật toán SPF để xác tính toán ra đường ngắn nhất đến từng mạng.
3. Lưu kết quả chon đường trong bảng định tuyến.

2.1.3. Thông tin định tuyến được duy trì như thế nào

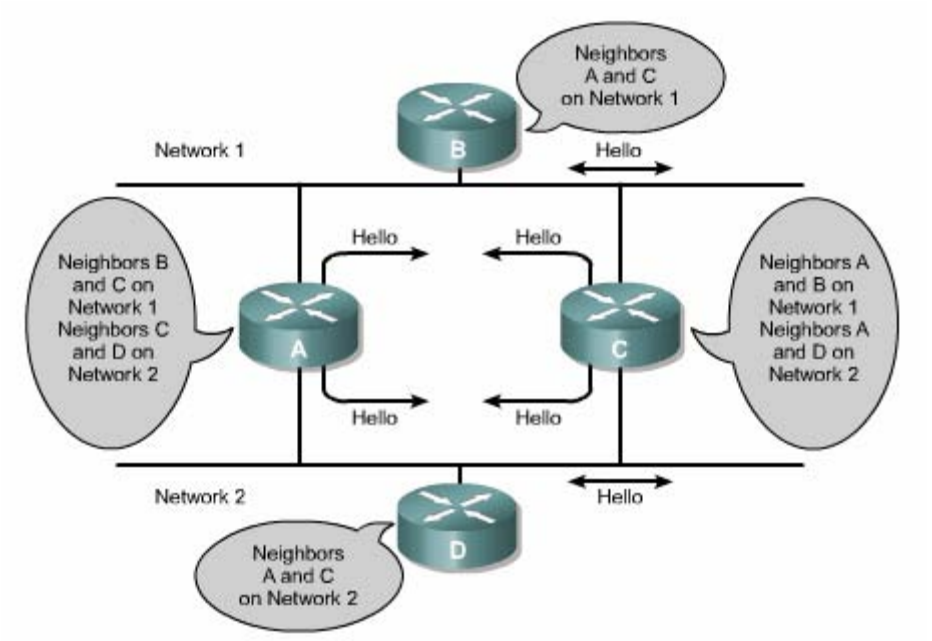
Phần này sẽ giải thích giao thức định tuyến theo trạng thái đường liên kết sử dụng các thành phần sau đây như thế nào:

- LSAs.
- Cơ sở dữ liệu về cấu trúc hệ thống mạng.
- Thuật toán SPF
- Cây SPF
- Bảng định tuyến với đường đi và cổng ra tương ứng để định tuyến cho gói dữ liệu.

Giao thức định tuyến theo trạng thái đường liên kết được thiết kế để khắc phục các nhược điểm của giao thức định tuyến theovectơ khoảng cách. Ví dụ như:giao thức định tuyến theo vectơ khoảng cách chỉ trao đổi thông tin định tuyến với các router kết nối trực tiếp với mình mà thôi, trong khi đó giao thức định tuyến theo trạng thái đường liên kết thực hiện trao đổi thông tin định tuyến trên một vùng rộng lớn.

Khi có một sự cố xảy ra trong mạng, ví dụ như có một router láng giềng bị mất kết nối , giao thức định tuyến theo trạng đường liên kết lập tức phát các gói LSAs ra trên toàn vùng bằng 1 địa chỉ multicast đặc biệt. Tiến trình này thực hiện gửi thông tin ra tất cả các cổng, trừ cổng nhận được thông tin. Mỗi router nhận được một LSA, cập nhật thông tin mới này vào cơ sở dữ liệu về cấu trúc hệ thống mạng. Sau đó router chuyển tiếp gói LSA này cho tất cả các thiết bị làng giềng khác. LSAs làm cho mọi router trong vùng thực hiện tính toán lại đường đi. Chính vì vậy số lượng router trong một vùng nên có giới hạn.

Một kết nối tương ứng với một cổng trên router. Thông tin về trạng thái của một liên kết bao gồm thông tin về một cổng của router và mối quan hệ với các router láng giềng trên cổng đó. Ví dụ như: thông tin về một cổng trên router bao gồm địa chỉ IP, subnet mask, loại mạng kết nối vào cổng đó…Tập hợp tất cả các thông tin trên được lưu lại thành một cơ sở dữ liệu về trạng thái các đường liên kết, hay còn gọi là cơ sở dữ liệu về cấu trúc hệ thống mạng. Cơ sở dữ liệu này được sử dụng để tính toán chọn đường tốt nhất. Router áp dụng thuật toán chọn đường ngắn nhất Dijkstra vào cơ sở dữ liệu về cấu trúc mạng, từ đó xây dựng nên cây SPF với bản thân router là gốc. Từ cây SPF này, router sẽ chọn ra đường ngắn nhất đến từng mạng đích. Kết quả chọn đường được đặt trên bảng định tuyến của router.



Hình 2.1.3

2.1.4 Thuật toán định tuyến theo trạng thái đường liên kết

Thuật toán định tuyến theo trạng thái đường liên kết xây dựng và duy trì một cơ sở dữ liệu phức tạp về cấu trúc hệ thống mạng bằng cách trao đổi các gói quảng cáo trạng thái đường liên kết LSAs(Link – State Advertisements) với tất cả các router khác trong mạng.

Thuật toán định tuyến theo trạng thái đường liên kết có đặc điểm sau:

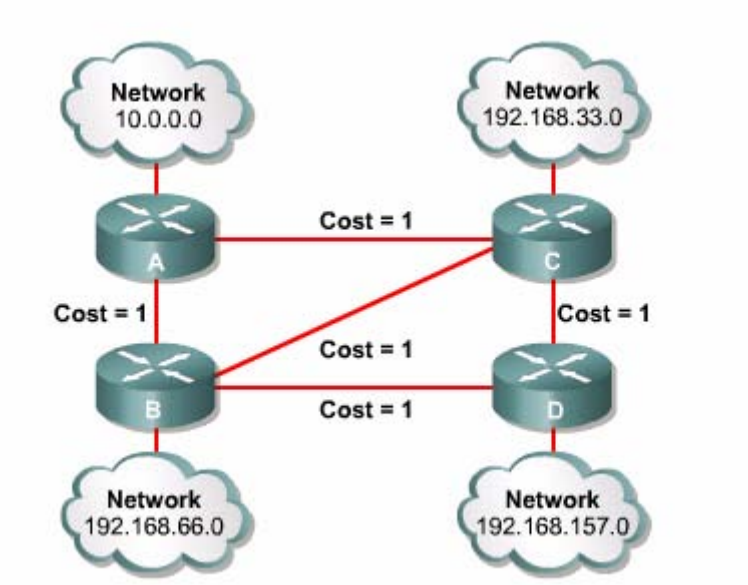
- Chúng được xem như là một tập hợp các giao thức SPF.

- Chúng xây dựng và duy trì một cơ sở dữ liệu phức tạp về cấu trúc hệ thống mạng.
- Chúng dựa trên thuật toán Dijkstra.

Giao thức định tuyến theo trạng thái đường liên kết phát triển và duy trì đầy đủ các thông tin về mọi router trong mạng và cấu trúc kết nối của chúng. Điều này được thực hiện nhờ quá trình trao đổi LSAs với các router khác trong mạng.

Mỗi router xây dựng cơ sở dữ liệu về cấu trúc hệ thống mạng của mình nhờ các thông tin từ các LSA mà nó nhận được. Sau đó router sử dụng thuật toán SP để tính toán chọn đường ngắn nhất đến từng mạng đích. Kết quả chọn đường được đưa lên bảng định tuyến của router. Trong suốt tiến trình hoạt động, mọi sự thay đổi trong cấu trúc hệ thống mạng như một thành phần mạng bị đứt hay mạng phát triển thêm thành phần mới đều được phat hiện và đáp ứng theo.

Việc trao đổi LSA được thực hiện khi có một sự kiện xảy ra trong mạng chứ không được thực hiện theo định kìy. Nhờ vậy tốc độ hội tụ nhanh hơn ví không cần chờ hết thời gian định kỳ các router mới được hội tụ.



Router	Destination	Next Hop	Cost
A	192.168.66.0	B	1
A	192.168.33.0	C	1
A	192.168.157.0	B	2
A	192.168.157.0	C	2
B	10.0.0.0	A	1
B	192.168.33.0	C	1
B	192.168.157.0	D	1
C	10.0.0.0	A	1
C	185.134.0.0	B	1
C	192.168.157.0	D	1
D	10.0.0.0	B	2
D	10.0.0.0	C	2
D	192.168.66.0	B	1
D	192.168.33.0	C	1

Hình 2.1.4

Ví dụ hình 2.1.4: Tùy theo từng giao thức và thông số định tuyến tương ứng, giao thức định tuyến có thể phân biệt được hai đường đến cùng một đích và sử dụng đường tốt nhất. Trong hình 2.1.4, trên bảng định tuyến có hai đường đi từ Router A đến Router D. Hai đường này có chi phí bằng nhau nên giao thức định tuyến ghi nhận cả hai. Có một số giao thức định tuyến theo trạng thái đường liên kết có cách đánh giá khả năng hoạt động của hai đường và chon đường tốt nhất. Ví dụ, nếu đường đi qua Router C gặp trở ngại như bị nghẽn mạch hoặc bị hư hỏng thì giao thức định tuyến theo trạng thái đường liên kết có thể nhận biết được các thay đổi này và chuyển gói di theo đường qua Router B.

2.1.5 Ưu và nhược điểm của giao thức định tuyến theo trạng thái đường liên kết

Sau đây là các ưu điểm của giao thức định tuyến theo trạng thái đường liên kết:

- Sử dụng chi phí làm thông số định tuyến để chọn đường đi trong mạng. Thông số chi phí này có thể phản ánh được dung lượng của đường truyền.
- Thực hiện cập nhật khi có sự kiện xảy ra, phát LSAs ra cho mọi router trong hệ thống mạng. Điều này giúp cho thời gian hội tụ nhanh hơn.
- Mỗi router có một sơ đồ đầy đủ và đồng bộ về toàn bộ cấu trúc hệ thống mạng. Do đó chúng rất khó bị lặp vòng.

- Router sử dụng thông tin mới nhất để quyết định chọn đường đi.
- Cần thiết kế hệ thống mạng một cách cẩn thận để cơ sở dữ liệu về trạng thái các đường liên kết có thể được thu nhỏ lại. Nhờ đó chúng ta có thể tiết kiệm được các tính toán Dijkstra và hội tụ nhanh hơn.
- Mọi router sử dụng sơ đồ cấu trúc mạng của riêng nó để chọn đường. Đặc tính này sẽ giúp chúng ta khi cần xử lý sự cố.
- Giao thức định tuyến theo trạng thái đường liên kết có hỗ trợ CIDR và VLSM.

Sau đây là các nhược điểm của giao thức định tuyến theo trạng thái đường liên kết:

- Chúng đòi hỏi nhiều dung lượng bộ nhớ và năng lực xử lý cao hơn so với giao thức định tuyến theo vectơ khoảng cách. Do đó chúng khá mắc tiền đối với các tổ chức nhỏ, chi phi hạn hẹp và thiết bị cũ.
- Chúng đòi hỏi hệ thống mạng phải được thiết kề theo mô hình phân cấp, hệ thống mạng được chia ra thành nhiều cùng nhỏ để làm giảm bớt độ lớn và độ phức tạp của cơ sở dữ liệu về cấu trúc hệ thống mạng.
- Chúng đòi hỏi nhà quản trị mạng phải nắm vững giao thức.
- Trong suốt quá trình khởi động, các router thu thập thông tin về cấu trúc hệ thống mạng để xây dựng cơ sở dữ liệu, chúng phát các gói LSA ra trên toàn bộ mạng. Do đó tiến trình này có thể làm giảm dung lượng đường truyền dành cho dữ liệu khác.

1.1.4. So sánh và phân biệt giữa định tuyến theo vectơ khoảng cách và định tuyến theo trạng thái đường liên kết

Trước tiên ta xét giao thức định tuyến theo vectơ khoảng cách. Thông tin định tuyến mà các router gửi đi là những thông tin gì và gửi cho ai ? Các router định tuyến theo vectơ khoảng cách thực hiện gửi toàn bộ bảng định tuyến của mình và chỉ gửi cho các router kết nối trực tiếp với mình. Như chúng ta đã biết ,thông tin trên bảng định tuyến rất ngắn gọn,chỉ cho biết tương ứng với một mạng đích là cổng nào của router , router kế tiếp có địa chỉ IP là gì, thông số định tuyến của con đường này là bao nhiêu. Do đó, các router định tuyến theo vectơ khoảng cách không biết được đường đi một cách cụ thể, không biết về các router trung gian trên đường đi và cấu trúc kết nối giữa chúng. Các bạn có thể xem nội dung bảng định tuyến trên router bằng lệnh **show ip route.** Hơn nữa, bảng định tuyến là kết quả chọn đường tốt nhất của mỗi router. Do đó, khi

chúng trao đổi bảng định tuyến với nhau, các router chọn đường dựa trên kết quả đã chọn của router láng giềng. Mỗi router nhìn hệ thống mạng theo sự chi phối của các router láng giềng.

Các router định tuyến theo vectơ khoảng cách thực hiện cập nhật thông tin định tuyến theo định kỳ nên tốn nhiều băng thông đường truyền. Khi có sự thay đổi xảy ra, router nào nhận biết sự thay đổi đầu tiên sẽ cập nhật bảng định tuyến của mình trước rồi chuyển bảng định tuyến bảng định tuyến cập nhật cho router láng giềng. Router láng giềng nhận được thông tin mới, cập nhật vào bảng định tuyến đã được cập nhật cho các router láng giềng kế tiếp. Quá trình cập nhật cứ lần lượt như vậy ra toàn bộ hệ thống. Do đó thời gian bị hội tụ chậm.

Bây giờ ta xét đến giao thức định tuyến theo trạng thái đường liên kết. Thông tin định tuyến mà các router gửi đi là gì và gửi cho ai? Khi bắt đầu hoạt động, mỗi router sẽ gửi thông tin cho biết nó có bao nhiêu kết nối và trạng thái của mỗi đường kết nối như thế nào, và nó gửi cho mọi router khác trong mạng bằng địa chỉ multicast. Do đó mỗi router đều nhận được từ tất cả các router khác thông tin về các kết nối của chúng. Kết quả là mỗi router sẽ có đầy đủ thông tin để xây dựng một cơ sở dữ liệu về trạng thái các đường liên kết, hay còn gọi là cơ sở dữ liệu về cấu trúc mạng. Như vậy, mỗi router đều có một cái nhìn đầy đủ và cụ thể về cấu trúc của hệ thống mạng. Từ đó, mỗi router tự tính toán để chọn đường đi tốt nhất đến từng mạng đích.

Khi các router định tuyến theo trạng thái đường liên kết đã hội tụ xong, không thực hiện cập nhật định kỳ. Chỉ khi nào có sự thay đổi thì thông tin về sự thay đổi đó được truyền đi cho tất cả các router trong mạng. Do đó thời gian hội tụ nhanh và ít tốn băng thông.

Ta thấy ưu điểm nổi trội của định tuyến theo trạng thái đường liên kết so với định tuyến theo vectơ khoảng cách là thời gian hội tụ nhanh hơn và tiết kiệm băng thông đường truyền hơn. Giao thức định tuyến theo trạng thái đường liên kết có hỗ trợ CIDR và VLSM. Do đó, chúng là một lựa chọn tốt cho mạng lớn và phức tạp. Thực chất giao thức định tuyến theo trạng thái đường liên kết thực hiện định tuyến tốt hơn so với giao thức định tuyến theo vectơ khoảng cách ở mọi kích cỡ mạng. Tuy nhiên, giao thức định tuyến theo trạng thái đường liên kết không được triển khai ở mọi hệ thống mạng vì chúng đòi hỏi dung lượng bộ

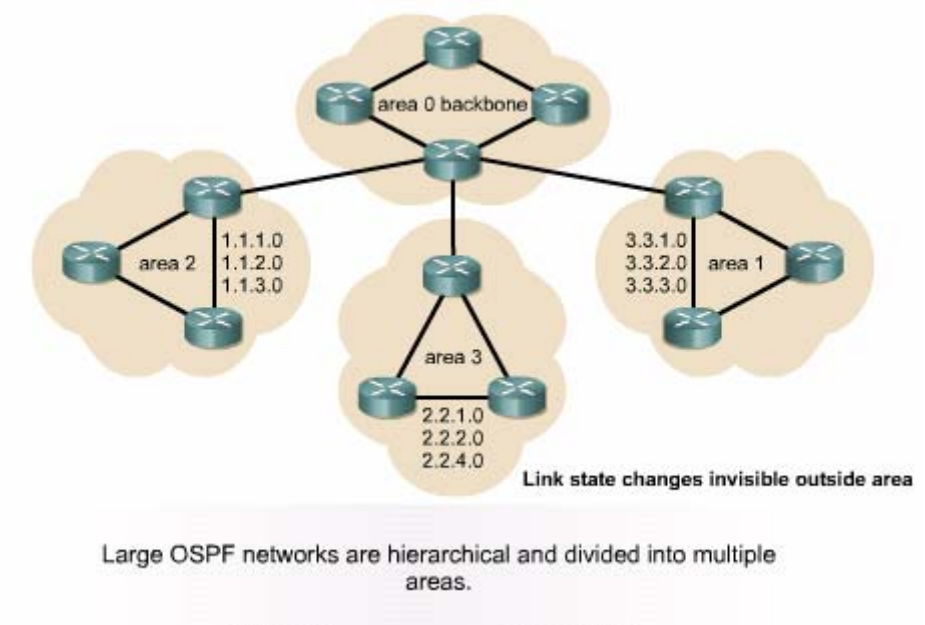
nhớ lớn và năng lực xử lý mạnh hơn, do đó có thể gây quá tải cho các thiết bị xử lý chậm. Một nguyên nhân nữa làm cho chúng không được triển khai rộng rãi là do chúng là một giao thức thực sự phức tạp, đòi hỏi người quản trị mạng phải được đào tạo tốt mới có thể cấu hình đúng và vận hành được.

1.2. Các khái niệm về OSPF đơn vùng

2.2.1. Tổng quát về OSPF

OSPF là một giao thức định tuyến theo trạng thái đường liên kết được triển khai dựa trên các chuẩn mở. OSPF được mô tả trong nhiều chuẩn của IETF (Internet Engineering Task Force). Chuẩn mở ở đây có nghĩa là OSPF hoàn toàn mở đối với công cộng, không có tính độc quyền

Nếu so sánh với RIPv1 và v2 thí OSPF là một giao thức định tuyến nội vi IGP tốt hơn vì khả năng mở rộng của nó. RIP chỉ giới hạn trong 15 hop, hội tụ chậm và đôi khi chọn đường có tốc độ chậm vì khi quyết định chọn đường nó không quan tâm đến các yếu tố quan trọng khác như băng thông chẳng hạn. OSPF khắc phục được các nhược điểm của RIP và nó là một giao thức định tuyến mạnh, có khả năng mở rộng, phù hợp với các hệ thống mạng hiện đại. OSPF có thể được cấu hình đơn vùng để sử dụng cho các mạng nhỏ.



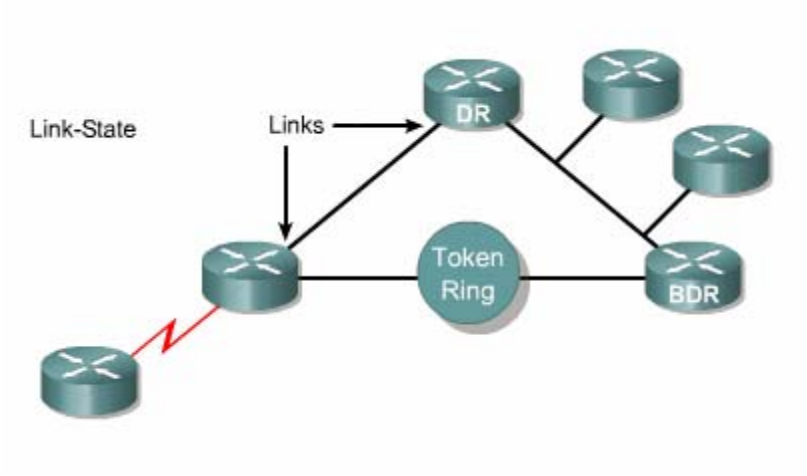
Hình 2.2.1. Mạng OSPF lớn được thiết kế phân cấp và chia thành nhiều vùng

Ví dụ như hình 2.2.1, mạng OSPF lớn cần sử dụng thiết kế phân cấp và chia thành nhiều vùng. Các vùng này đều được kết nối vào cùng phân phối la vùng 0 hay còn gọi là vùng xương sống (backbone). Kiểu thiết kế này cho phép kiểm soát hoạt động cập nhật định tuyến. Việc phân vùng như vậy làm giảm tải của hoạt động định tuyến, tăng tốc độ hội tụ, giới hạn sự thay đổi của hệ thống mạng vào từng vùng và tăng hiệu suất hoạt động.

2.2.2. Thuật ngữ của OSPF

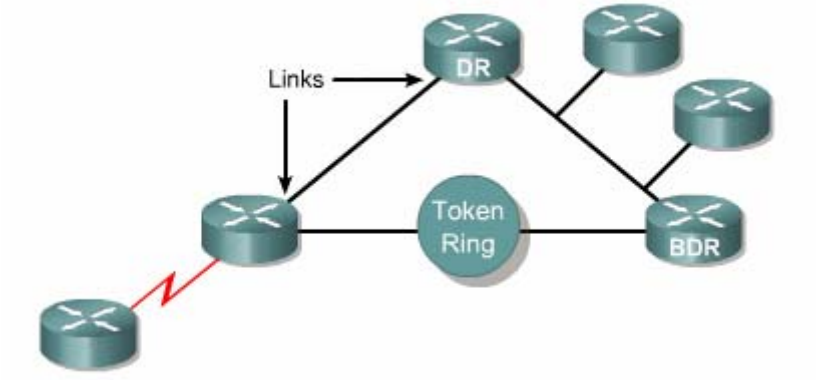
Router định tuyến theo trạng thái đường liên kết xác định các router láng giềng và thiết lập mối quan hệ với các láng giềng này.

OSPF thực hiện thu thập thông tin về trạng thái các đường liên kết từ các router láng giềng. Mỗi router OSPF quảng cáo trạng thái các đường liên kết của nó và chuyển tiếp các thông tin mà nó nhận được cho tất cả các láng giềng khác.

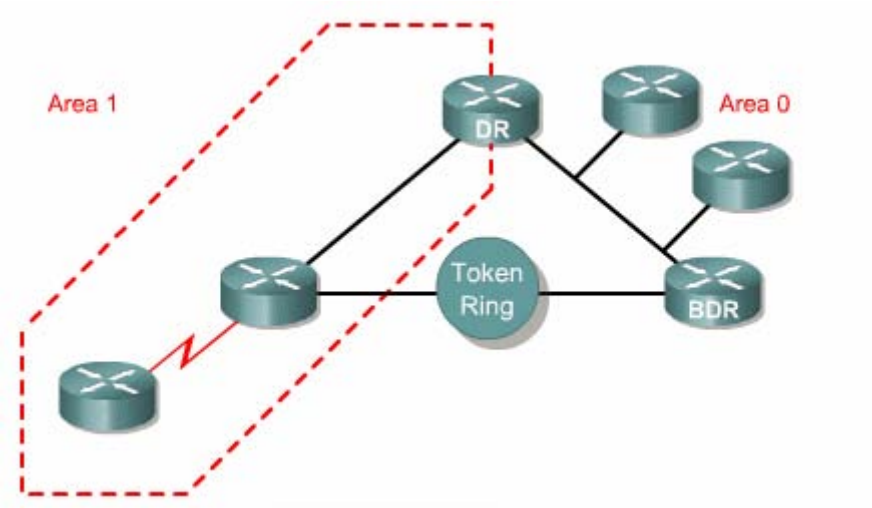


Hình 2.2.2.a. Link – là một cổng trên router. Link-state: trạng thái của một đường liên kết giữa hai router, bao gồm trạng thái của một cổng trên router và mối quan hệ giữa nó với router láng giềng kết nối vào cổng đó.

Router xử lý các thông tin nhận được để xây dựng một cơ sở dữ liệu về trạng thái các đường liên kết trong một vùng. Mọi router trong cùng một vùng OSPF sẽ có cùng một cơ sở dữ liệu này. Do đó mọi router sẽ có thông tin giống nhau về trạng thái của các đường liên kết và láng giềng của các router khác.

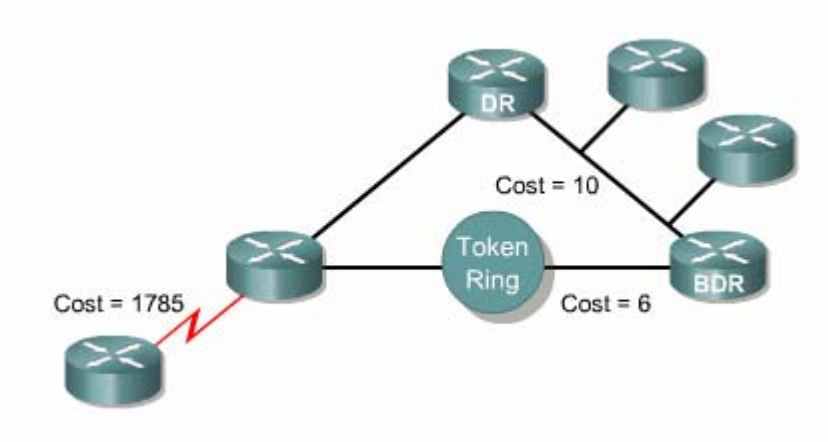


Hình 2.2.2.b.. Link-state database (Topological database) – danh sách các thông tin về mọi đường liên kết trong vùng.

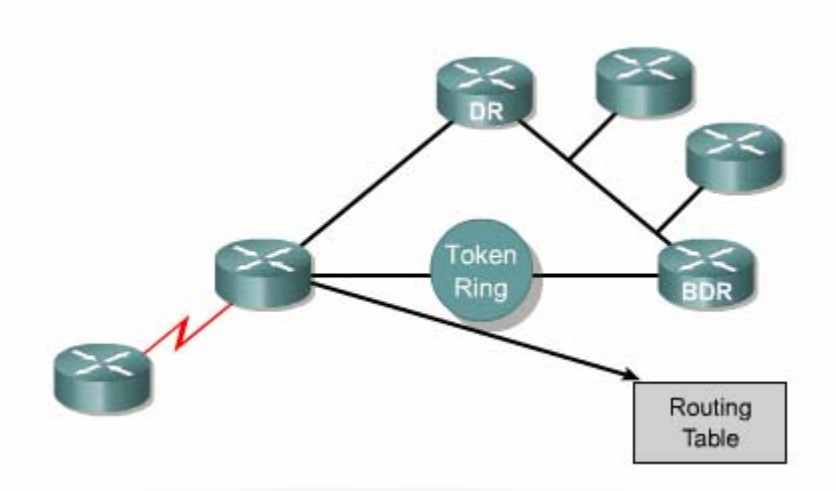


Hình 2.2.2.c.Area - Tập hợp các mạng và các router có cùng chỉ số danh định vùng. Mỗi router trong một vùng chỉ xây dựng cơ sở dữ liệu về trạng thái các đường liên kết trong vùng đó. Do đó, các router trong cùng một vùng sẽ có thông tin giống nhau về trạng thái các đường liên kết. Router nằm trong một vùng được gọi la router nội vùng.

Mỗi router áp dụng thuật toán SPF và cơ sở dữ liệu của nó để tính toán chọn đường tốt nhất đến từng mạng đích. Thuật toán SPF tính toàn chi phí dựa trên băng thông của đường truyền. Đường nào có chi phí nhỏ nhất sẽ được chọn để đưa vào bảng định tuyến.

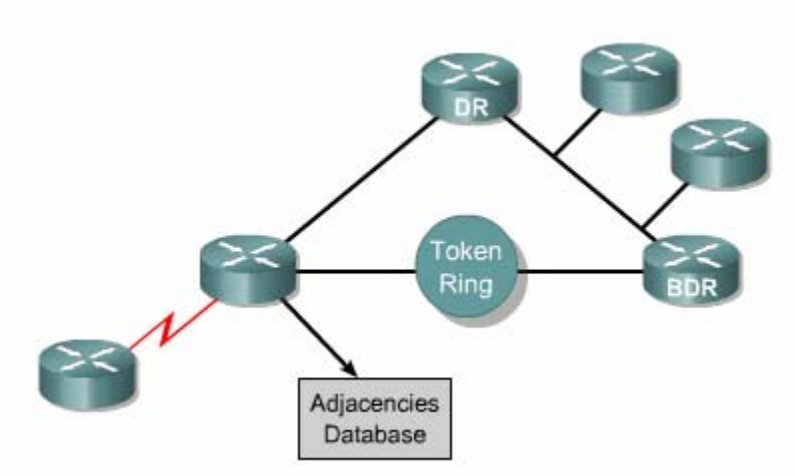


Hình 2.2.2.d. Cost – giá trị chi phí đặt cho một đường liên kết. Giao thức định tuyến theo trạng thái đường liên kết tính chi phí cho một liên kết dựa trên băng thông hoặc tốc độ của đường liên kết đó.



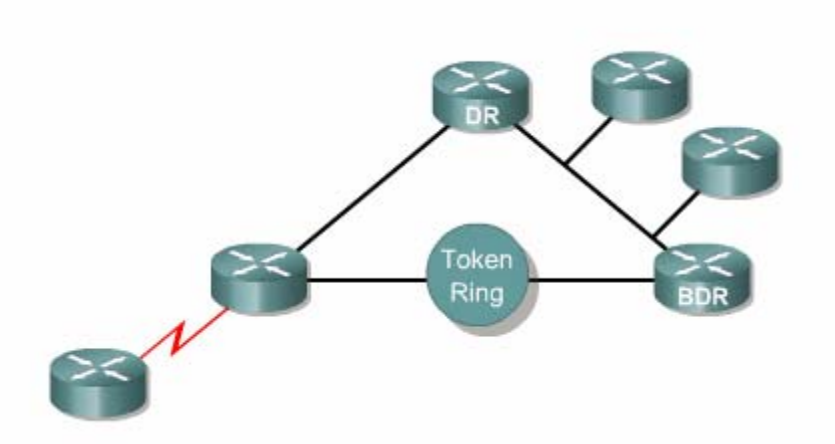
Hình 2.2.2.e. Routing table – hay còn gọi là cơ sở dữ liệu để chuyển gói. Bảng định tuyến là kết quả chọn đường của thuật toán chọn đường địa dựa trên cơ sở dữ liệu về trạng thái các đường liên kết.

Mỗi router giữ một danh sách các láng giềng thân mật, danh sách này gọi là cơ sở dữ liệu các láng giềng thân mật. Các láng giềng được gọi là thân mật là những láng giềng mà router có thiết lập mối quan hệ hai chiều. Một router có thể có nhiều láng giềng nhưng không phải láng giềng nào cũng có mối quan hệ thân mật. Do đó bạn cần lưu ý mối quan hệ láng giềng khác với mối quan hệ láng giềng thân mật, hay gọi tắt là mối quan hệ thân mật. Đối với mỗi router danh sách láng giềng thân mật sẽ khác nhau.



Hình 2.2.2.f. Adjacency database – danh sách các router láng giềng có mối quan hệ hai chiều. Mỗi router sẽ có một danh sách khác nhau.

Để giảm bớt số lượng trao đổi thông tin định tuyến với nhiều router láng giềng trong cùng một mạng, các router OSPF bầu ra một router đại diện gọi là Designated router (DR) và một router đại diện dự phòng gọi là Backup Designated (BDR) làm điểm tập trung các thông tin định tuyến.



Hình 2.2.2.g. Design Router (DR) và Backup Designated Router (BDR) là router được tất cả các router khác trong cùng một mạng LAN bầu ra làm đại diện. Mỗi một mạng sẽ có một DR va BDR riêng.

2.2.3. So sánh OSPF với giao thức định tuyến theo vectơ khoảng cách

Trong phần này chúng ta sẽ so sánh OSPF với một giao thức định tuyến theo vectơ khoảng cách la RIP. Router định tuyến theo trạng thái đường liên kết có một sơ đồ đầy đủ về cấu trúc hệ thống mạng. Chúng chỉ thực hiển trao đổi thông tin về trạng thái các đường liên kết lúc khởi động và khi hệ thống mạng có sự thay đổi. Chúng không phát quảng bá bảng định tuyến theo định kỳ như các router định tuyến theo vectơ khoảng cách. Do đó, các router định tuyến theo trạng thái đường liên kết sử dụng ít băng thông hơn cho hoạt động duy trì bảng định tuyến.

RIP phù hợp cho các mạng nhỏ và đường tốt nhất đối với RIP là đường có số lượng hop ít nhất. OSPF thì phù hợp với mạng lớn, có khả năng mở rộng, đường đi tốt nhất của OSPF được xác định dựa trên tốc độ của đường truyền. RIP cũng như các giao thức định tuyến theo vectơ khoảng cách đều sử dụng thuật toán chọn đường đơn giản. Còn thuật toán SPF thì rất phức tap. Do đó, nếu router chạy giao

thức định tuyến theo vectơ khoảng cách sẽ cần ít bộ nhớ và năng lực xử lý thấp hơn so với khi chạy OSPF.

OSPF chọn đường dựa trên chi phí được tính từ tốc độ của đường truyền. Đường truyền có tốc độ càng cao thì chi phí OSPF tương ứng càng thấp.

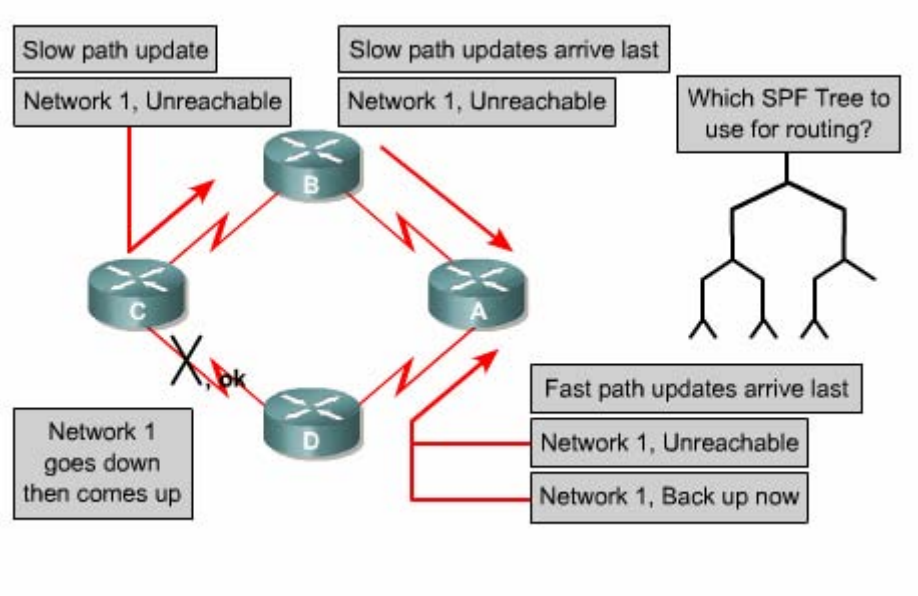
OSPF chọn đường tốt nhất từ cây SPF.

OSPF bảo đảm không bị định tuyến lặp vòng. Còn giao thức định tuyến theo vectơ khoảng cách vẫn có thể bị định tuyến lặp vòng.

Nếu một kết nối không ổn định, chập chờn, việc phát liên tục các thông tin về trang thái của đường liên kết này sẽ dẫn đến tình trạng các thông tin quảng cáo không đồng bộ làm cho kết quả chọn đường của các router bị đảo lộn.

OSPF giải quyết được các vấn đề sau:

- Tốc độ hội tụ.
- Hỗ trợ VLSM (Variable Length Subnet Mask).
- Kích cỡ mạng
- Chọn đường
- Nhóm các thành viên.



Hình 2.2.3. Sự cố xảy ra khi một kết nối không ổn định làm cho việc cập nhật không đồng bộ.

Trong một hệ thống mạng lớn, RIP phải mất vài phút mới có thể hội tụ được vì mỗi router chỉ trao đổi bảng định tuyến với các router láng giềng kết nối trực tiếp với mình mà thôi. Còn đối với OSPF sau khi đã hội tụ vào lúc khởi động, khi có thay đổi thì việc hội tụ sẽ rất nhanh vì chỉ có thông tin về sự thay đổi được phát ra cho mọi router trong vùng.

OSPF có hỗ trợ VLSM nên nó được xem là một giao thức định tuyến không theo lớp địa chỉ. RIPv1 không có hỗ trợ VLSM, tuy nhiên RIPv2 có hỗ trợ VLSM.

Đối với RIP, một mạng đích cách xa hơn 15 router xem như không đến được vì RIP có số lượng hop giới hạn là 15. Điều này làm kích thước mạng của RIP bị giới hạn trong phạm vi nhỏ. OSPF thì không hề có giới hạn về kích thước mạng, OSPF hoàn toàn phù hợp cho các mạng vừa và lớn.

Khi nhận được từ láng giềng các router bao cáo về số lượng hop đến mạng đích, RIP sẽ cộng thêm 1 vào thống số hop này và dựa vào số lượng hop đó để chọn đường đến mạng đích. Đường nào có khoảng cách ngắn nhất hay nói cách khác là có số lượng hop ít nhất sẽ là đường tốt nhất đối với RIP. Chúng ta thấy thuật toán

chọn đường như vậy rất đơn giản và không đòi hỏi nhiều bộ nhớ và năng lượng xử lý của router. RIP không hề quan tâm đến băng thông đường truyền khi quyết định chọn đường.

OSPF thì chọn đường dựa vào chi phí được tính từ băng thông của đường truyền. Mọi OSPF router đều có thông tin đầy đủ về cấu trúc của hệ thống mạng dựa vào đó để tự tính toán chọn đường tốt nhất. Do đó thuật toán chọn đường này rất phức tạp, đòi hỏi nhiều bộ nhớ và năng lực xử lý của router cao hơn so với RIP.

RIP sử dụng cấu trúc mạng dạng ngang hàng. Thông tin định tuyến được truyền lần lượt cho mọi router trong cùng một hệ thống RIP. OSPF sử dụng khái niệm về phân vùng. Một mạng OSPF có thể chia các router thành nhiều nhóm. Bằng cách này, OSPF có thể giới hạn lưu thông trong từng vùng. Thay đổi trong vùng này không ảnh hưởng đến hoạt động của các vùng khác. Cấu trúc phân cấp như vậy cho phép hệ thống mạng có khả năng mở rộng một cách hiệu quả.

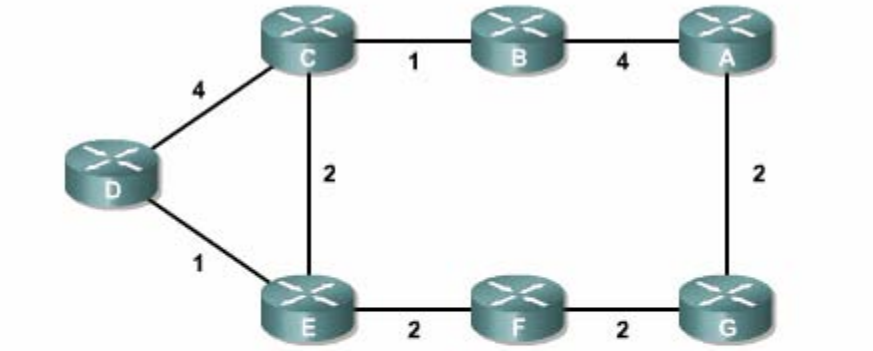
2.2.4. Thuật toán chọn đường ngắn nhất.

Trong phần này sẽ giải thích cách OSPF sử dụng thuật toán chọn đường ngắn nhất như thế nào.

Theo thuật toán này, đường tốt nhất là đường có chi phí thấp nhất. Edsger Wybe Dijkstra, một nhà khoa học máy tính người Hà Lan, đã phát minh thuật toán này nên nó còn có tên là thuật toán Dijkstra. Thuật toán này xem hệ thống mạng là một tập hợp các nodes được kết nối với nhau bằng kết nối điểm-đến-điểm. Mỗi kết nối này có một chi phí. Mỗi node có một cái tên. Mỗi node có đầy đủ cơ sở dữ liệu về trạng thái của các đường liên kết, do đó chúng có đầy đủ thông tin về cấu trúc vật lý của hệ thống mạng. Tất cả các cơ sở dữ liệu này đều giống nhau cho mọi router trong cùng một vùng. Ví dụ như trên hình 2.2.4.a, D có các thông tin là nó kết nối tới node C bằng đường liên kết có chi phí là 4 và nó kết nối đến node E bằng đường liên kết có chi phí là 1.

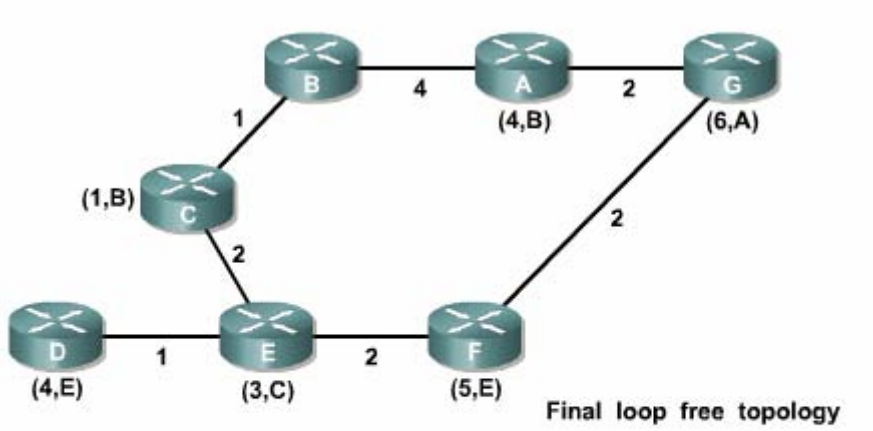
Thuật toán chọn đường ngắn nhất sẽ sữ dụng bản thân node làm điểm xuất phát và kiểm tra các thông tin mà nó có về các node kế cận. Trong hình 2.2.4.b, node B chọn đường đến D. Đường tốt nhất đến D là đi bằng đường của node E có chi phí là 4. Như vậy là gói dữ liệu đi từ B đến D sẽ đi theo đường từ B qua C qua E rồi đến D.

Node B chọn đường đến node F là đường thông qua node C có chi phí là 5. Mọi đường khác đều có thể bị lặp vòng hoặc có chi phí cao hơn.



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		

Hình 2.2.4.a



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		

Hình 2.2.4.b

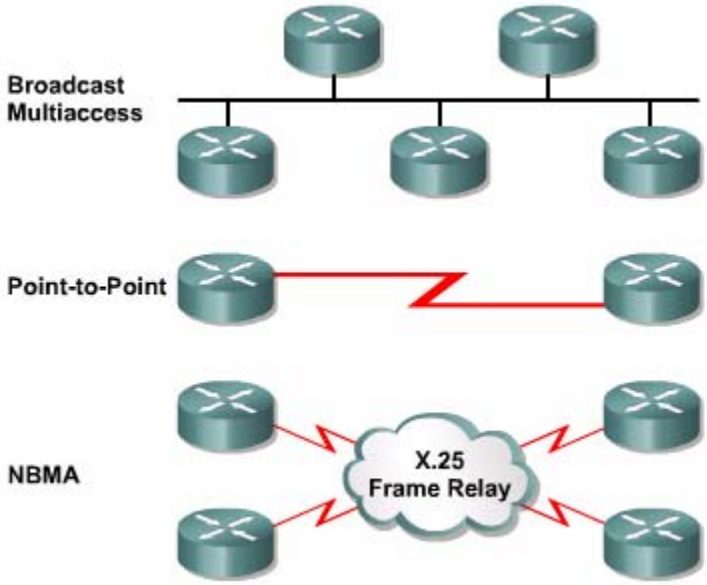
2.2.5. Các loại mạng OSPF

Các OSPF router phải thiết lập mối quan hệ láng giềng để trao đổi thông tin định tuyến. Trong mỗi một mạng IP kết nối vao router, nó đều cố gắng ít nhất là trở thành một láng giềng hoặc là láng giềng thân mật với một router khác. Router OSPF quyết định chọn router nào làm láng giềng thân mật là tuỳ thuộc vào mạng kết nối của nó. Có một số router có thể cố gắng trở thành láng giềng thân mật với mọi router láng giềng khác. Có một số router khác lại có thể chỉ cố gắng trở thành láng giềng thân mật với một hoặc hai router láng giềng thôi. Một khi mối quan hệ láng giềng thân mật đã được thiết lập giữa hai láng giềng với nhau thì thông tin về trạng thái đường liên kết mới được trao đổi.

Giao tiếp OSPF nhận biết ba loại mạng sau:

- Mạng quảng bá đa truy cập, ví dụ như mạng Ethernet.
- Mạng điểm-nối-điểm.
- Mạng không quảng bá đa truy cập (NBMA – Nonbroadcast multi-access), ví dụ như Frame Relay.

Loại mạng thứ 4 là mạng điểm-đến-nhiều điểm có thể được nhà quản trị mạng cấu hình cho một cổng của router.



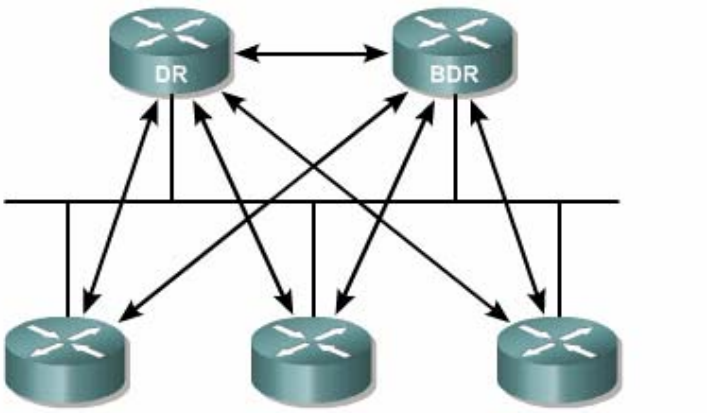
Hình 2.2.5.a. Ba loại mạng của OSPF.

Trong mạng đa truy cập không thể biết được là có bao nhiêu router sẽ có thể kết nối được kết nối vào mạng. Trong mạng điểm-đến-điểm chỉ có hai router kết nối với nhau.

Trong mạng quảng bá đa truy cập có rất nhiều router kết nối vào. Nếu mỗi router đều thiết lập mối quan hệ thân mật với mọi router khác và thực hiện trao đổi thông tin về trạng thái đường liên kết với mọi router láng giềng thì sẽ quá tải. Nếu có 10 router thì sẽ cần 45 mối liên hệ thân mật, nếu có n router thì sẽ có n*(n-1)/2 mối quan hệ láng giềng thân mật cần được thiết lập.

Giải pháp cho vấn đề quá tải trên là bầu ra một router làm đại diện (DR – Designated Router). Router này sẽ thiết lập mối quan hệ thân mật với mọi router khác trong mạng quảng bá. Mọi router còn lại sẽ chỉ gửi thông tin về trạng thái đường liên kết cho DR. Sau đó DR sẽ gửi các thông tin này cho mọi router khác trong mạng bằng địa chỉ mutlticast 224.0.0.5. DR đóng vai trò như một người phát ngôn chung.

Việc bầu DR rất có hiệu quả nhưng cũng có một số nhược điểm. DR trở thành một tâm điểm nhạy cảm đối với sự cố. Do đó, cần có một router thứ hai được bầu ra để làm router đại diện dự phòng (BDR – Backup Designated Router), router này sẽ đảm trách vai trò của DR nếu DR bị sự cố. Để đảm bảo cả DR và BDR đều nhận được các thông tin về trạng thái đường liên kết từ mọi router khác trong cùng một mạng, chúng ta sử dụng địa chỉ multicast 224.0.0.6 cho các router đại diện.



Hình 2.2.5.b. DR và BDR nhận các gói LSAs.

Trong mạng điểm-nối-điểm chỉ có 2 router kết nối với nhau nên không cần bầu ra DR và BDR. Hai router này sẽ thiết lập mối quan hệ láng giềng thân mật với nhau.

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

Hình 2.2.5.c

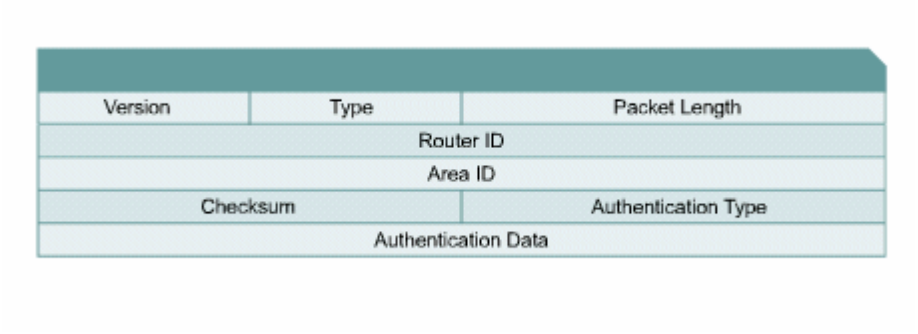
2.2.6. Giao thức OSPF Hello

Khi router bắt đầu khởi động tiến trình định tuyến OSPF trên một cổng nào đó thì nó sẽ gửi một gói hello ra cổng đó và tiếp tục gửi hello theo định kỳ. Giao thức Hello đưa ra các nguyên tắc quản lý việc trao đổi các gói OSPF Hello.

Ở Lớp 3 của mô hình OSI, gói hello mang địa chỉ multicast 224.0.0.5. Địa chỉ này chỉ đến tất cả các OSPF router. OSPF router sử dụng gói hello để thiết lập một quan hệ láng giềng thân mật mới để xác định là router láng giềng có còn hoạt động hay không. Mặc định, hello được gửi đi 10 giây 1 lần trong mạng quảng bá đa truy cập và mạng điểm-nối-điểm. Trên cổng nối vào mạng NBMA, ví dụ như Frame Relay, chu kỳ mặc định của hello là 30 giây.

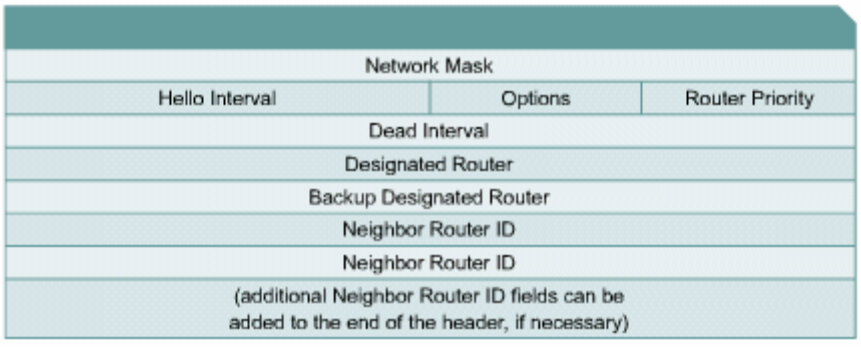
Trong mạng đa truy cập, giao thức hello tiến hành bầu DR và BDR.

Mặc dù gói hello rất nhỏ nhưng nó cũng bao gồm cả phần header của gói OSPF. Cấu trúc của phần header trong gói OSPF được thể hiện trên hình 2.2.6.a. Nếu là gói hello thì trường Type sẽ có giá trị là 1.



Hình 2.2.6.a. Phần header của gói OSPF.

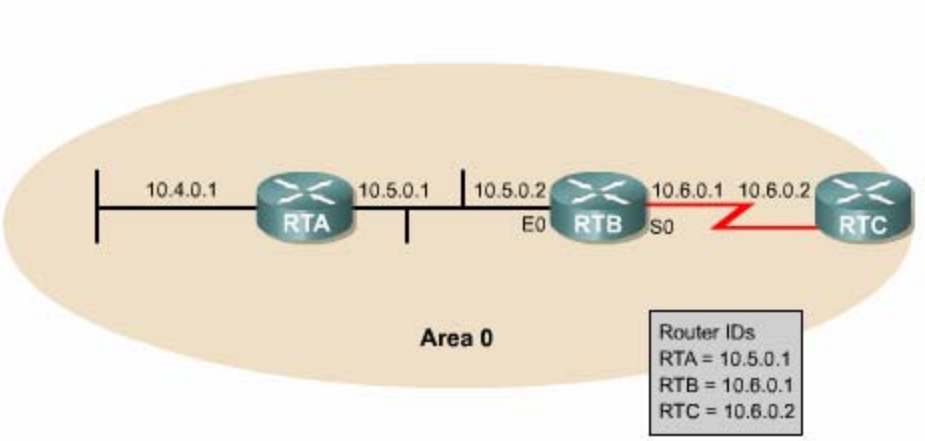
Gói hello mang những thông tin để thống nhất giữa mọi láng giềng với nhau trước khi có thể thiết lập mối quan hệ láng giềng thân mật và trao đổi thông tin về trạng thái các đường liên kết.



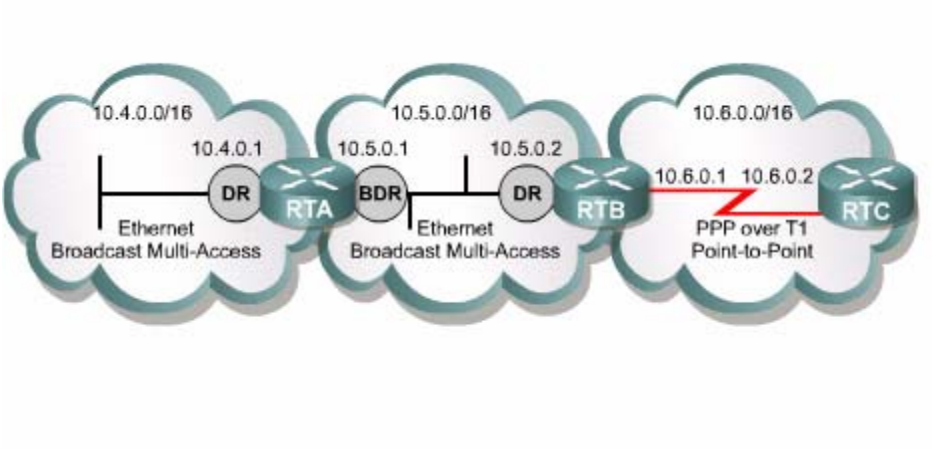
Hình 2.2.6.b. Phần header của gói OSPF Hello. Các thông tin trong phần Hello Interval, Đea Interval và Router ID phải đồng nhất thì các router mới có thể thiết lập mối quan hệ láng giềng thân mật.

2.2.7. Các bước hoạt động của OSPF

Khi bắt đầu khởi động tiến trình định tuyến OSPF trên một cổng nào đó, nó sẽ gửi gói Hello ra cổng đó và tiếp tục gửi hello theo định kỳ. Giao thức Hello là một tập hợp các nguyên tắc quản lý việc trao đổi gói Hello. Gói Hello mang các thông tin cần thống nhất giữa mọi router láng giềng trước khi có thể thiết lập mối quan hệ thân mật và trao đổi thông tin về trạng thái các đường liên kết. Trong mạng đa truy cập, giao thức Hello sẽ bầu ra một DR và BDR. DR và BDR duy trì mối quan hệ thân mật với mọi router OSPF còn lại trong cùng một mạng.



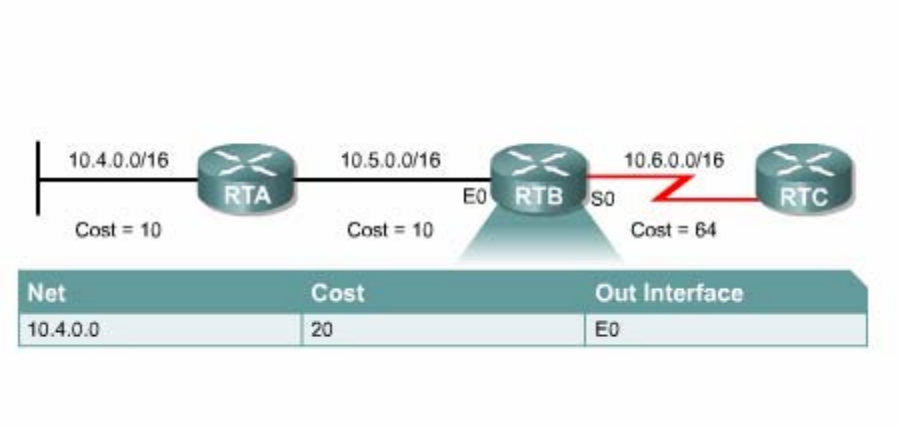
Hình 2.2.7.a. Bước 1: phát hiện các router láng giềng. Trong từng mạng IP kết nối vào router, router cố gắng thiết lập mối quan hệ thân mật với ít nhất một láng giềng.



Hình 2.2.7.b. Bước 2: bầu ra DR và BDR. Quá trình này chỉ được thực hiện trong mạng đa truy cập.

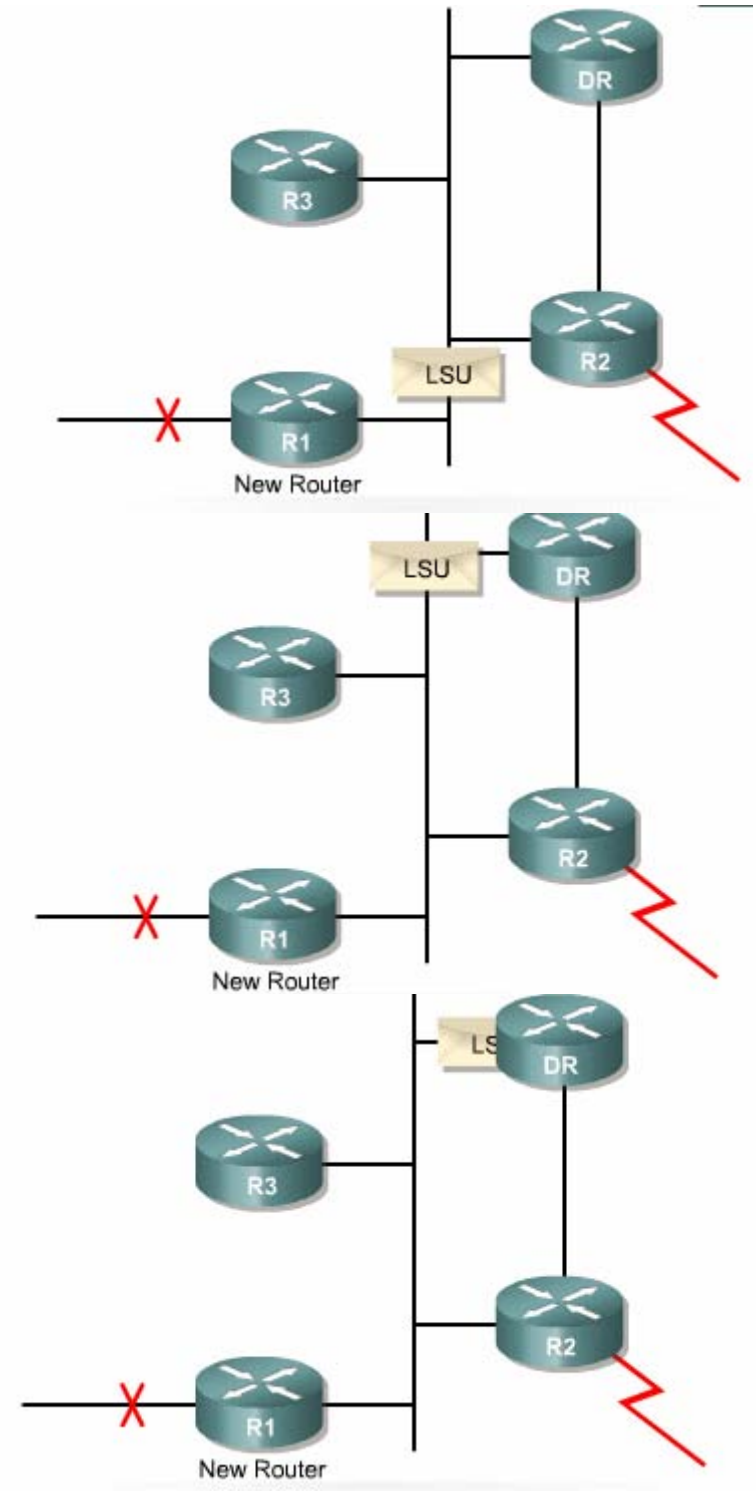
Các router đã có mối quan hệ thân mật lần lượt thực hiên các bước trao đổi thông tin về trạng thái các đường liên kết. Sau khi hoàn tất quá trình này các ở trạng thái gọi la *full state.* Mỗi router gửi thông tin quảng cáo về trạng thái các đường liên kết trong gói LSAs (Link-State Advertisements) và gửi thông tin cập nhật các trạng thái này trong gói LSUs (Link-State Updates). Mỗi router nhận các gói LSAs này từ láng giềng rồi ghi nhận thông tin vào cơ sở dữl iệu của nó. Tiến trình này được lặp lại trên mọi router trong mạng OSPF.

Khi cơ sở dữ liệu về trạng thái các đường liên kết đã đáy đủ, mỗi router áp dụng thuật toán SPF để tự tính toán chọn đường tốt nhất dựa trên cơ sở dữ liệu mà nó có. Đường ngắn nhất là đường có chi phí thấp nhất đến mạng đích.

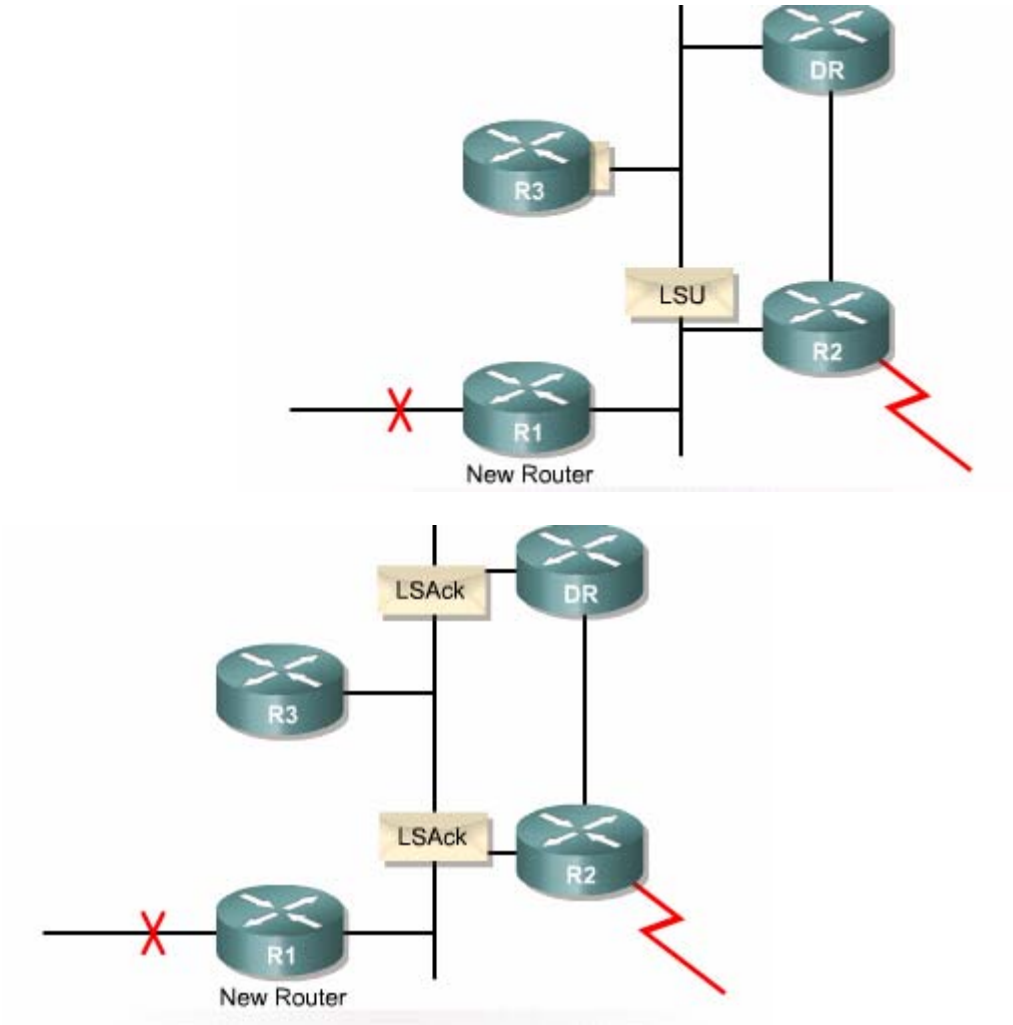


Hình 2.2.7.c. Bước 3: áp dụng thuật toán SPF vào cơ sở dữ liệu về trạng thái các đường liên kết để chọn đường tốt nhất đưa lên bảng định tuyến.

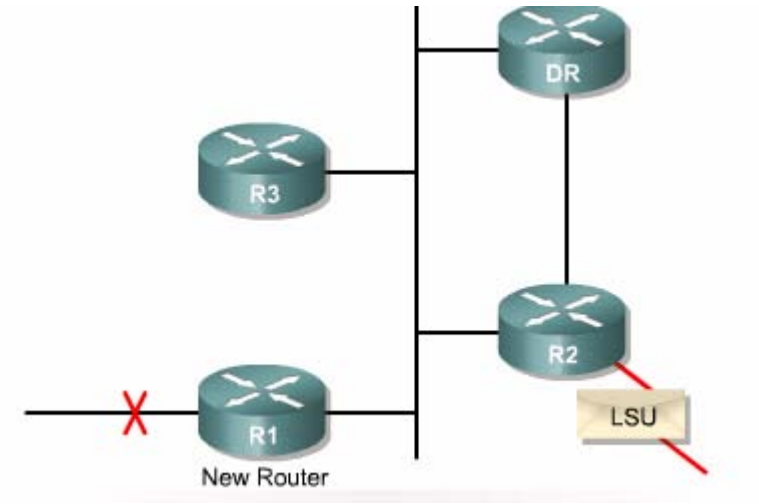
Sau đó các thông tin định tuyến cần phải được bảo trì. Khi có một sự thay đổi nào về trạng thái của đường liên kết, router lập tức phát thông báo cho mọi router khác trong mạng. Thời gian Dead interval trong giao thức Hello là một thông số đơn giản để xác định một router láng giềng thân mật còn hoạt động hay không.


DR
R3
R2
LSU
R1
New Router
LSU
DR
R3
R2
R1
New Router
DR
R3
R2
R1
New Router

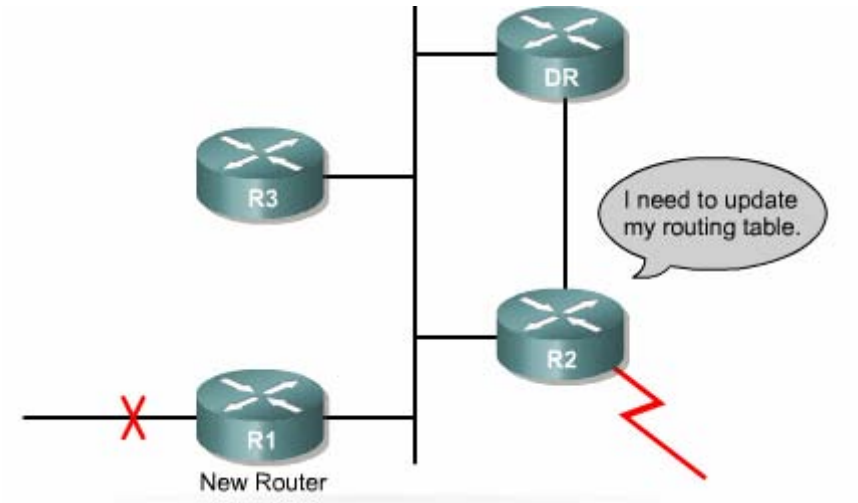
Hình 2.2.7.d. R1 phát hiện một liên kết bị đứt và gửi LSU cho DR bằng địa chỉ multicast 224.0.0.6. DR gửi báo nhận cho R1.



Hình 2.2.7.e. Tiếp theo DR gửi LSU mới nhận cho tất cả các router còn lại trong cùng một mạng bằng địa chỉ multicast 224.0.0.5. Sau khi nhận được LSU, các router gửi báo nhận lại cho DR.



Hình 2.2.7.f. Nếu router OSPF nào còn có kết nối đến mạng khác thì nó sẽ chuyển tiếp LSU ra mạng đó.



Hình 2.2.7.g. Sau khi nhận được LSU với thông tin mới, router OSPF sẽ cập nhật vào cơ sở dữ liệu của nó rồi áp dụng thuật toán SPF với thông tin mới này để tính toán lại bảng định tuyến.

2.3. Cấu hình OSPF đơn vùng

2.3.1. Cấu hình tiến trình định tuyến OSPF

Định tuyến OSPF sử dụng khái niệm về vùng. Mỗi router xây dựng một cơ sở dữ liệu đầy đủ về trạng thái các đường liên kết trong một vùng. Một vùng trong mạng OSPF được cấp số từ 0 đến 65.535. Nếu OSPF đơn vùng thì đó là vùng 0. Trong mạng OSPF đa vùng, tất cả các vùng đều phải kết nối vào vùng 0. Do đó vùng 0 được gọi là vùng xương sống.

Trước tiên, bạn cần khởi động tiến trình định tuyến OSPF trên router, khai báo địa chỉ mạng và chỉ số vùng. Địa chỉ mạng được khai báo kèm theo wildcard mask chứ không phải là subnet mask. Chỉ số danh định (ID) của vùng được viết dưới dạng số hoặc dưới dạng số thập phân có dấu chấm tượng tự như IP.

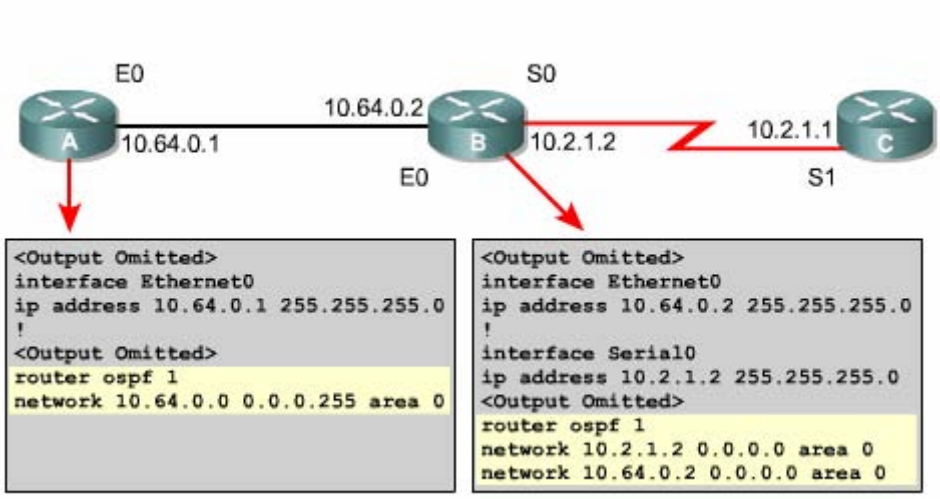
Để khởi động định tuyến OSPF bạn dùng lệnh sau trong chế độ cấu hình toàn cục:

Router (config)#router ospf **process-id**

Process-id là chỉ số xác định tiến trình đing tuyến OSPF trên router. Bạn có thể khởi động nhiều tiến trình OSPF trên cùng một router. Chỉ số này có thể là bất kỳ giá trị nào trong khoảng từ 1 đến 65.535. Đa số các nhà quản trị mạng thường giữ chỉ số *process-id* này giống nhau trong cùng một hệ tự quản, nhưng điều này là không bắt buộc. Rất hiếm khi nào bạn cần chạy nhiều hơn một tiến trình OSPF trên một router. Bạn khai báo địa chỉ mạng cho OSPF như sau:

Router(config-router)#network **address wildcard-mask** area **area-id**

Mỗi mạng được quy ước thuộc về một vùng. Adress có thể là địa chỉ của toàn mạng, hoặc là một subnet hoặc là địa chỉ của một cổng giao tiếp. Wildcard-mask sẽ xác định chuỗi địa chỉ host nằm trong mạng mà bạn cần khai báo.



Hình 2.3.1. Cấu hình OSPF cơ bản.

2.3.2. Cấu hình địa chỉ loopback cho OSPF và quyền ưu tiên cho router

Khi tiến trình OSPF bắt đầu hoạt động, Cisco IOS sử dụng địa chỉ IP lớn nhất đang hoạt động trên router làm router ID. Nếu không có cổng nào đang hoạt động thì tiến trình OSPF không thể bắt đầu được. Khi router đã chọn địa chỉ IP của một cổng làm router ID và sau đó cổng này bị sự cố thì tiến trình sẽ bị mất router ID. Khi đó tiến trình OSPF sẽ bịi ngưng hoạt động cho đến khi cổng đó hoạt động trở lại.

Để đảm bảo cho OSPF hoạt động ổn định chúng ta cần phải có một cổng luôn luôn tồn tại cho tiến trình OSPF. Chính vì vậy cần cấu hình một cổng loopback là một cổng luận lý chứ không phải cổng vật lý. Nếu có một cổng loopback được cấu hình thì OSPF sẽ sử dụng địa chỉ của cổng loopback làm router ID mà không quan tâm đến giá trị của địa chỉ này.

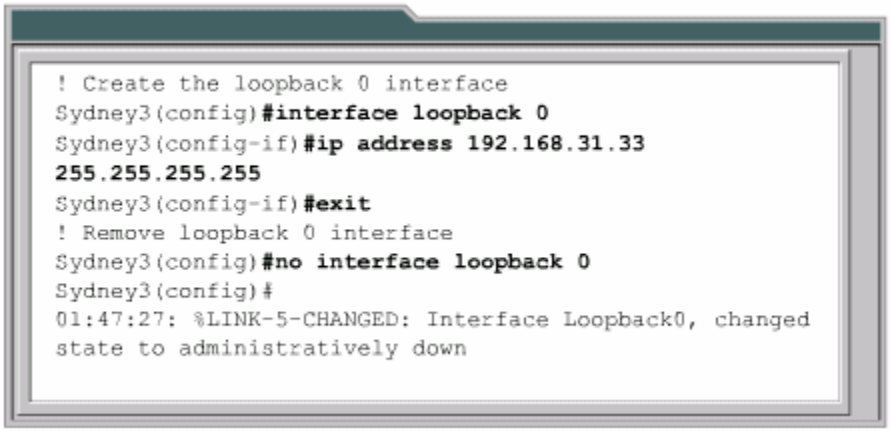
Nếu trên router có nhiều hơn một cổng loopback thì OSPF sẽ chọn địa chỉ IP lớn nhất trong các địa chỉ IP của các cổng loopback làm router ID.

Để tạo cổng loopback và đặt địa chỉ IP cho nó bạn sử dụng các lệnh sau:

Router (config)#interface loopback **number**

Router (config-if)#ip address **ip-address subnet-mask**

Bạn nên sử dụng cổng loopback cho mọi router chạy OSPF. Cổng loopback này nên được cấu hình với địa chỉ có subnet mask là 255.255.255.255. Địa chỉ 32-bit subnet mask như vậy gọi là host mask vì subnet mask này xác định một địa chỉ mạng chỉ có một host. Khi OSPF phát quảng cáo về mạng loopback, OSPF sẽ luôn luôn quảng cáo loopback như là một host với 32-bit mask.



Hình 2.3.2.a. Cổng loopback chỉ là một cổng phần mềm. Để xoá cổng loopback bạn dùng dạng no của câu lệnh tạo cổng.

Trong mạng quảng bá đa truy cập có thể có nhiều hơn hai router. Do đó, OSPF bầu ra một router đại diện (DR – Designated Router) làm điểm tập trung tất cả các thông tin quảng cáo và cập nhật về trạng thái của các đường liên kết. Vì vai trò của DR rất quan trọng nên một router đại diện dự phòng (BDR – Backup Designated Router) cũng được bầu ra để thay thế khi DR bị sự cố.

Đối với cổng kết nối vào mạng quảng bá, giá trị ưu tiên mặc định của OSPF trên cổng đó là 1. Khi giá trị OSPF ưu tiên của các router đều bằng nhau thì OSPF sẽ bầu DR dựa trên router ID. Router ID nào lớn nhất sẽ được chọn.

Bạn có thể quyết định kết quả bầu chọn DR bằng cách đặt giá trị ưu tiên cho cổng cua router kết nối vào mạng đó. Cổng của router nào có giá trị ưu tiên cao nhất thì router đó chắc chắn là DR.

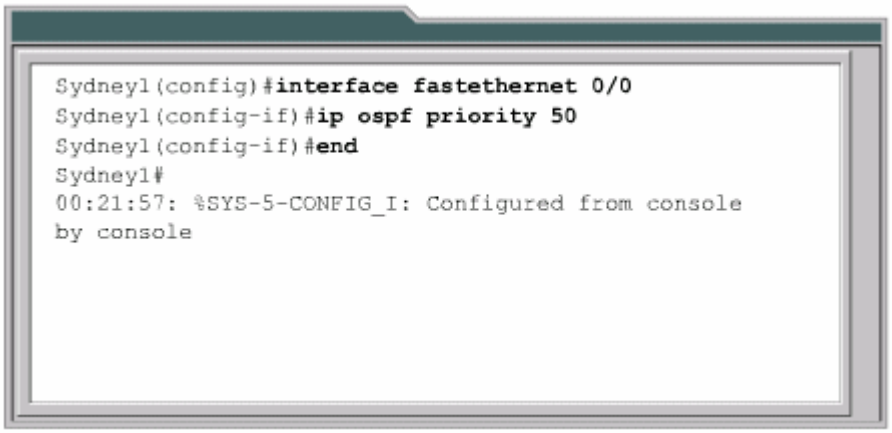
Giá trị ưu tiên có thể đặt bất kỳ giá trị nào nằm trong khoảng từ 0 đến 255. Giá trị 0 sẽ làm cho router đó không bao giờ được bầu chọn. Router nào có giá trị ưu tiên

OSPF cao nhất sẽ được chọn làm DR. Router nào có vị trí ưu tiên thứ 2 sẽ là BDR. Sau khi bầu chọn xong, DR và BDR sẽ giữ luôn vai trò của nó cho dù chúng ta có đặt thêm router mới vào mạng với giá trị ưu tiên OSPF cao hơn.

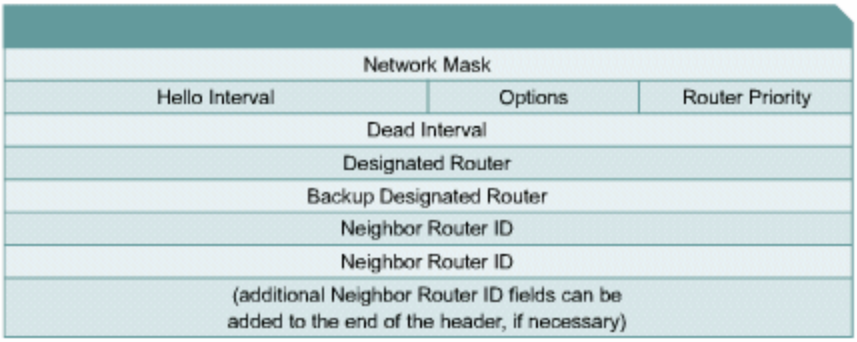
Để thay đổi giá trị ưu tiên OSPF, bạn dùng lệnh **ip ospf priority** trên cổng nào cần thay đổi. Bạn dùng lệnh **showip ospf interface** có thể xem được giá trị ưu tiên của cổng và nhiều thông tin quan trọng khác.

Router(config-if)#ip ospf priority **number**

Router#show ip ospf interfacetype **number**



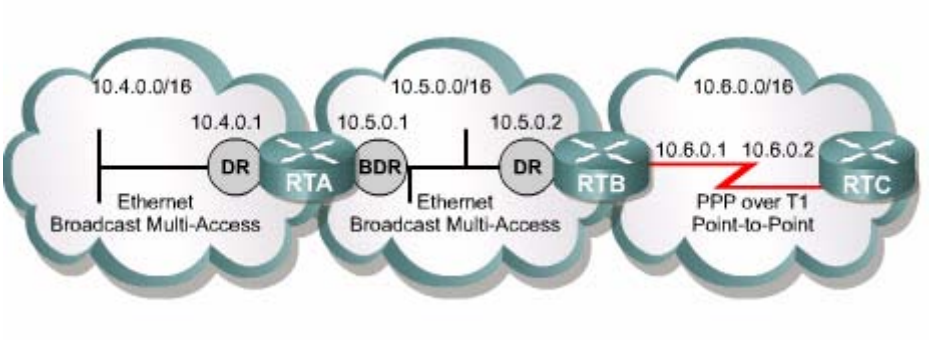
Hình 2.3.2.b. Trong gói hello phát ra cổng Fast Ethernet 0/0, trường Router Priority sẽ có giá trị là 50.



Hình 2.3.2.c. Gói OSPF Hello.

```
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)
```

Hình 2.3.2.d



Hình 2.3.2.e. Bầu DR và BDR trong mạng quảng bá đa truy cập.

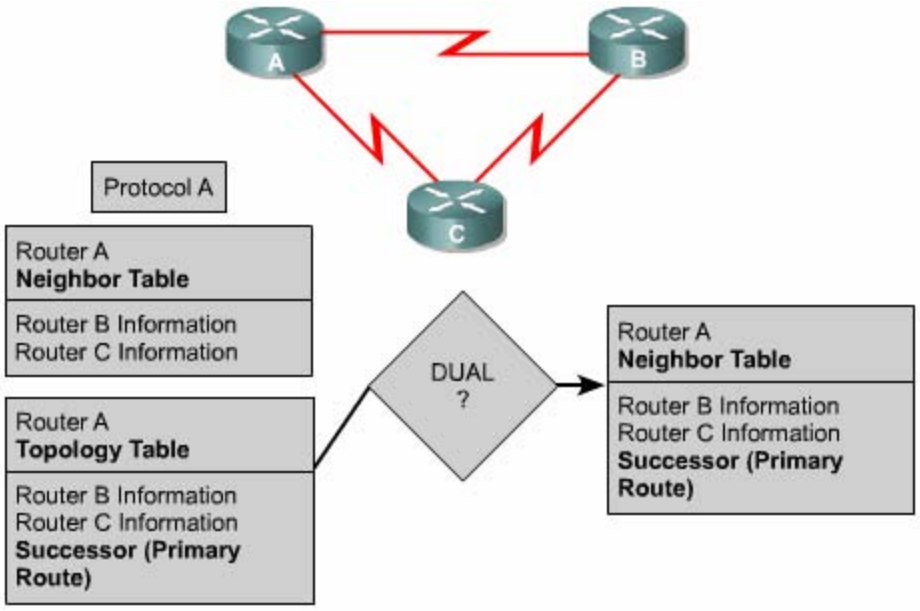
Ta xét ví dụ trong hình 2.3.2.d. RTA va RTB sẽ thực hiện bầu DR và BDR trong hai mạng Ethernet quảng bá đa truy cập. Còn mạng PPP giữa RTB và RTC là mạng điểm-nối-điểm nên không thực hiện bầu DR và BDR. Trong mạng Ethernet 10.4.0.0/16 kết nối giữa RTA và RTB giả sử giá trị ưu tiên trên 2 cổng Ethernet của RTA và RTB đều bằng nhau và bằng giá trị mặc định là 1. Khi đó router nào có router ID lớn nhất trong mạng này sẽ được bầu làm DR. Router ID của RTA là 10.5.0.1, router ID của RTB là 10.6.0.1. Vậy RTB làm DR và RTA làm BDR.

Khong tim thay hinh

Hình 2.3.2.f

Ta xét ví dụ hình 2.3.2.f. Hai mạng 10.2.0.0/30 va 10.2.0.4/30 giữa hai kết nối serial của router HQ – router B, router B – router Remote là hai mạng điểm-nối-điểm nên không bầu DR và BDR trong mạng Ethernet 10.4.0.0/16 kết nối giữa chúng. Tương tự cho mạng 10.5.0.0/16 giữa router A và router Remote. Giả sử giá

trị ưu tiên trên cổng fa0 của router HQ và trên cổng fa1 của router A đều bằng giá trị mặc định là 1. Router HQ có router ID là 10.4.0.2, router A có router ID là 10.5.0.1, router Remote có router ID là 10.5.0.2. Vậy router A sẽ là DR trong mạng này vì router A có router ID lớn hơn router ID của router HQ. Tương tự, router Remote sẽ là DR trong mạng 10.5.0.0/16 và router A làm BDR trong mạng này.



Hình 2.3.2.g

Ta xét ví dụ trong hình 2.3.2.g. R2 và R3 không thực hiện bầu DR và BDR cho mạng điểm-nối-điểm kết nối giữa hai cổng serial của chúng. R1, R2 và R3 sẽ tiến hành bầu DR và BDR cho mạng Ethernet kết nối giữa chúng. Giả sử giá trị ưu tiên của cổng e0 trên các router đều bằng 1. R1 có cổng Loopback0 nên nó sẽ lấy địa cỉ IP của cổng này làm router ID. R2 không có cấu hình cổng Loopback nên nó lấy địa chỉ IP lớn nhất mà nó có để làm router ID. Do đó, router ID của R2 là 192.1.1.2. Tương tự, router ID của R3 là 201.1.1.1. Như vậy R3 có router ID lớn nhất nên nó được bầu làm DR trong mạng Ethernet 192.1.1.0/24, R2 có router ID lớn thứ 2 nên nó được bầu làm BDR trong mạng này.

2.3.3. Thay đổi giá trị chi phí của OSPF.

OSPF sử dụng chi phí làm thông số chọn đường tốt nhất. Giá trị chi phí này liên quan đến đường truyền và dữ liệu nhận vào của một cổng trên router. Nói tóm lại, chi phí của một kết nối được tính theo công thức 10^8/băng thông, trong đó băng thông được tính theo đơn vị bit/s. Người quản trị mạng có thể cấu hình giá trị chi phí bằng nhiều cách. Cổng nào có chi phí thấp thì cổng đó sẽ được chọn để chuyển dữ liệu. Cisco IOS tự động tính chi phí dựa trên băng thông của cổng tương ứng. Do đó, để OSPF hoạt động đúng bạn cần cấu hình băng thông đúng cho cổng của router.

Router (config)#interface serial 0/0

Router(config-if)#bandwidth 64

Giá trị băng thông mặc định của cổng Serial Cisco là 1,544Mbps hay 1544kbs

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

Hình 2.3.3.a. Giá trị chi phí OSPF mặc định của Cisco IOS.

Giá trị chi phí thay đổi sẽ ảnh hưởng đến kết quả tính toán của OSPF. Trong môi trường định tuyến có nhiều hãng khác nhau, bạn sẽ phải thay đổi giá trị chi phí để giá trị chi phí của hãng này tương thích với giá trị chi phí của hãng kia. Một trường hợp khác bạn cần thay đổi giá trị chi phí khi sử dụng Gigabit Ethernet. Giá trị chi phí mặc định thấp nhất, giá trị 1, là tương ứng với kết nối 100Mbs. Do đó, khi trong mạng vừa co 100Mbs va Gigabit Ethernet thì giá trị chi phí mặc định sẽ làm cho việc định tuyến có thể không tối ưu. Giá trị chi phi nằm trong khoảng từ 1 đến 65.535.

Bạn sử dụng câu lệnh sau trong chế độ cấu hình cổng tương ứng để cài đặt giá trị chi phí cho cổng đó:

Router (config-if)#ip ospf cost number

Hình 2.3.3.b. Cấu hình giá trị chi phí cho một cổng của router.

2.3.4. Cấu hình quá trình xác minh cho OSPF.

Các router mặc nhiên tin rằng những thông tin định tuyến mà nó nhận được là do đúng router tin cậy phát ra và những thông tin này không bị can thiệp dọc đường đi.

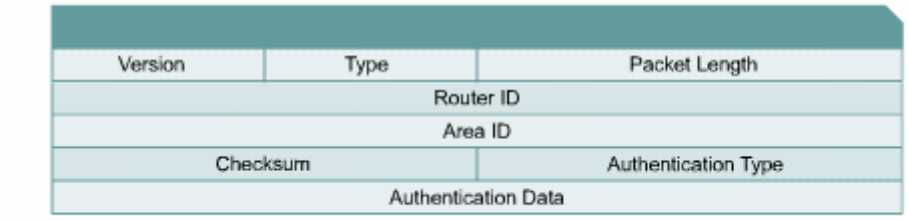
Để đảm bảo điều này, các router trong một vùng cần được cấu hình để thực hiện xác minh với nhau.

Mỗi một cổng OSPF trên router cần có một chìa khoá xác minh để sử dụng khi gửi các thông tin OSPF cho các router khác cùng kết nối với cổng đó. Chìa khóa xác minh, hay còn gọi là mật mã, được chia sẻ giữa hai router. Chìa khoá này sử dụng để tạo ra dữ liệu xác minh (trường Authentication data) đặt trong phần header của gói OSPF. Mật mã này có thể dài đến 8 ký tự. Bạn sử dụng câu lệnh sau để cấu hình mật mã xác minh cho một cổng OSPF:

Router (config-if)#ip ospf authentication-key**password**

Sau khi cấu hình mật mã xong, bạn cần bật chế độ xác minh cho OSPF:

Router(config-router)#area***area-number*** authentication



Hình 2.3.4.a. Phần header của gói OSPF.

Với cơ chế xác minh đơn giản trên, mật mà được gửi đi dưới dạn văn bản. Do đó nó dễ dàng được giải mã nếu gói OSPF bị những kẻ tấn công bắt được.

Chính vì vậy các thông tin xác minh nên được mật mã lại. Để đảm bảo an toàn hơn và thực hiện mật mã thông tin xác minh, bạn nên cấu hình mật mã message-digest bằng câu lệnh sau trên cổng tương ứng của router:

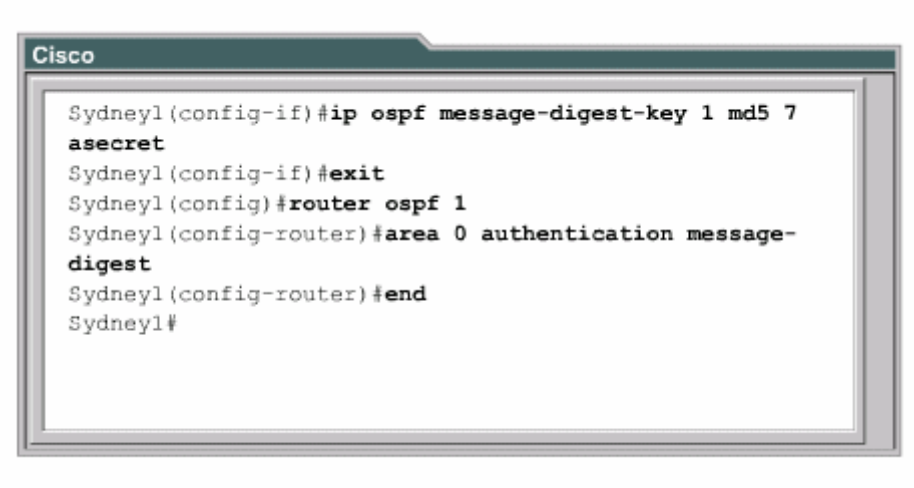
Router(config-ì)#ip ospf message-digest-key **key-**id encryption-type md5 **key**

MD5 là một thuật toán mật mã thông điệp message-digist. Nếu bạn đặt tham số encryption-type giá trị 0 có nghĩa là không thự hiện mật mã, còn giá trị 7 có nghĩa là thực hiện mật mã theo cách độc quyền của Cisco.

Tham số *key-id* là một con số danh định có giá trị từ 1 đến 255. Tham số *key* là phần cho bạn khai báo mật mã, có thể dài đến 16 ký tự. Các router láng giềng bắt buộc phải có cùng số *key-id* cà cùng giá trị *key*.

Sau khi cấu hình mật mã MD5 xong bạn cần bật chế độ xác minh message-digest trong OSPF:

Router (config-router)#area**area-id** authentication message-digest



Hình 2.3.4.b. Cấu hình cơ chế xác minh MD5 cho OSPF.

Từ mật mã và nội dung của gói dữ liệu, thuật toán mất mã MD5 sẽ tạo ra một thông điệp gắn thêm vào gói dữ liệu. Router nhận gói dữ liệu sẽ dùng mật mã mà bản thân router có kết hợp với gói dữ liệu nhận được để tạo ra một thông điệp. Nếu kết quả hai thông điệp này giống nhau thì có nghĩa là là router đã nhận được gói dữ liệu từ đúng nguồn và nội dung gói dữ liệu đã không bị can thiệp. Cấu trúc phần header của gói OSPF như trên hình 2.3.4.a. Trường authentication type cho biết cơ chế xác minh là cơ chế nào. Nếu cơ chế xác minh là message-digest thì trường authentication data sẽ có chứa key-id và thông số cho biết chiều dài của phần thông điệp gắn thêm vào gói dữ liệu. Phần thông điệp này giống như một con dấu không thể làm giả được.

2.3.5. Cấu hình các thông số thời gian của OSPF

Các router OSPF bắt buộc phải có khoảng thời gian hello và khoảng thời gian bất động với nhau mới có thể thực hiện trao đổi thông tin với nhau. Mặc định, khoảng thời gian bất động bằng bốn lần khoảng thời gian hello. Điều này có nghĩa là một router có đến 4 cơ hội để gửi gói hello trước khi nó xác định là đã chết.

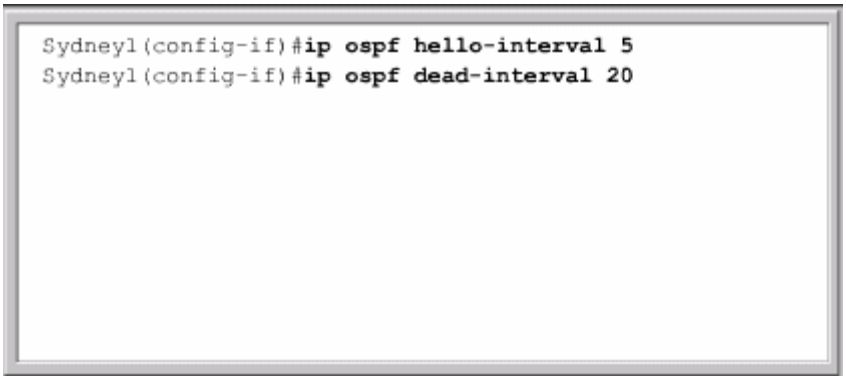
Trong mạng OSPF quảng bá, khoảng thời gian hello mặc định là 10 giây, khoảng thời gian bất động mặc định là 40 giây. Trong mạng không quảng bá, khoảng thời gian hello mặc định là 30 giây và khoảng thời gian bất động mặc định là 120 giây. Các giá trị mặc định này có ảnh hưởng đến hiệu quả hoạt động của OSPF và đôi khi bạn cần phải thay đổi chúng.

Người quản trị mạng được phép lựa chọn giá trị cho hai khoảng thời gian này. Để tăng hiệu quả hoạt động của mạng bạn cần ưu tiên thay đổi giá trị của hai khoảng thời gian này. Tuy nhiên, các giá trị này phải được cấu hình giống nhau cho mọi router láng giềng kết nối với nhau.

Để cấu hình khoảng thời gian hello và khoảng thời gian bất động trên một cổng của router, bạn sử dụng câu lệnh sau:

Router (config-if)#ip ospf hello-interval **seconds**

Router (config-if)#ip ospf dead-interval **seconds**



Hình 2.3.5

2.3.6. OSPF thực hiện quảng bá đường mặc định

Định tuyến OSPF đảm bảo các con đường đến tất cả các mạng đích trong hệ thống không bị lặp vòng. Để đến được các mạng nằm ngoài hệ thống thì OSPF cần phải biết về mạng đó hoặc là phải có đường mặc định. Tốt nhất là sử dụng đường mặc định vì nếu router phải lưu lại từng đường đi cho mọi mạng đích trên thế giới thì sẽ tốn một lượng tài nguyên khổng lồ.

Trên thực tế, chúng ta khai báo đường mặc định cho router OSPF nào kết nối ra ngoài. Sau đó thông tin về đường mặc định này được phân phối vào cho các router khác trong hệ tự quản (AS – autonomous system) thông qua hoạt động cập nhật bình thường của OSPF.

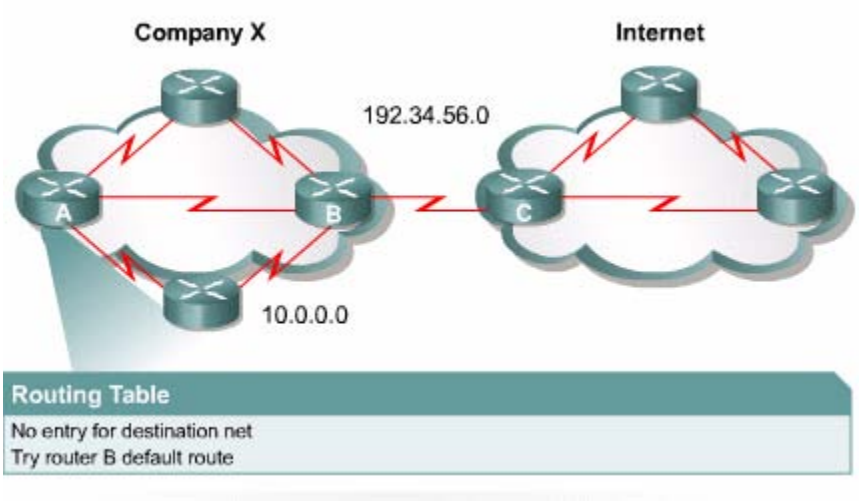
Trên router có cổng kết nối ra ngoài, bạn cấu hình mặc định bằng câu lệnh sau:

Router (config)#ip route 0.0.0.0 0.0.0.0 **[interface | next-hop address]**

Mạng tám số 0 như vậy tương ứng với bất kỳ địa chỉ mạng nào. Sau khi cấu hình đường mặc định xong, bạn cấu hình cho OSPF chuyển thông tin về đường mặc định cho mọi router khác trong vùng OSPF:

Router (config-router) #default – information originate

Mọi router trong hệ thống OSPF sẽ nhận biết được là có đường mặc định trên router biên giới kết nối ra ngoài.



Hình 2.3.6. Đường mặc định chỉ được sử dụng khi không tìm thấy đường nào khác trong bảng định tuyến.

2.3.7. Những lỗi thường gặp trong cấu hình OSPF

OSPF router phải thiết lập mối quan hệ láng giềng hoặc thân mật với OSPF router khác để trao đổi thông tin định tuyến. Mối quan hệ này không thiết lập được có thể do những nguyên nhân sau:

- Cả hai bên láng giềng với nhau đều không gửi Hello.
- Khoảng thời gian Hello và khoảng thời gian bất động không giống nhau giữa các router láng giềng.
- Loại cổng giao tiếp khác nhau giữa các router láng giềng.
- Mật mã xác minh và chìa khoá khác nhau giữa các router láng giềng.

Trong cấu hình định tuyến OSPF việc đảm bảo tính chính xác của các thông tin sau cũng vô cùng quan trọng:

- Tất cả các cổng giao tiếp phải có địa chỉ và subnet mask chính xác.

- Câu lệnh network area phải có wildcard mask chính xác.
- Câu lệnh network area phải khai báo đúng area mà network đó thuộc về.

2.3.8. Kiểm tra cấu hình OSPF

Để kiểm tra cấu hình OSPF bạn có thể dùng các lệnh show được liệt kê trong bảng 2.3.8.a. Bảng 2.3.8.b liệt kê các lệnh show hữu dụng cho bạn khi tìm sự cố của OSPF.

Bảng 2.3.8.a. 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.
Show ip ospf	Lệnh này cho biết số lần đã sử dụng thuật toán SPF, đồng thời cho biết khoảng thời gian cập nhật khi mạng không có gì

	thay đổi.
Show ip ospf neighbor detail	Liệt kê chi tiết các láng giềng, giá trị ưu tiên của chúng và trạng thái của chúng.
Show ip ospf database	Hiển thị nội dung của cơ sở dữ liệu về cấu trúc hệ thống mạng trên router, đồng thời cho biết router ID, ID của tiến trình OSPF.

Bảng 2.3.8.b. 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.

TỔNG KẾT

Sau đây là các điểm quan trọng bạn cầm nắm được trong chương này:

- Các đặc điểm của định tuyến theo trạng thái đường liên kết.
- Thông tin định tuyến theo trạng thái đường liên kết được xây dựng và bảo trì như thế nào.
- Thuật toán định tuyến theo trạng thái đường liên kết.
- Ưu và nhược điểm của định tuyến theo trạng thái đường liên kết.

- So sánh định tuyến theo trạng thái đường liên kết với định tuyến theo vectơ khoảng cách.
- Các thuật ngữ OSPF.
- Các loại mạng OSPF.
- Hoạt động của thuật toán chọn đường ngắn nhất SPF.
- Giao thức OSPF Hello.
- Các bước cơ bản trong hoạt động của OSPF.
- Khởi động OSPF trên router.
- Cấu hình cổng loopback để đặt quyền ưu tiên cho router.
- Thay đổi quyết định chọn đường của OSPF bằng cách thay đổi thông số chi phí.
- Cấu hình quá trình xác minh cho OSPF.
- Thay đổi các thông số thời gian của OSPF.
- Tạo và quảng bá đường mặc định.
- Sử dụng các lệnh **show** để kiểm tra hoạt động của OSPF.

Chương 3: EIGRP

GIỚI THIỆU

Enhanced Interior Gateway Routing Protocol (EIGRP) là một giao thức định tuyến độc quyền của Cisco được phát triển từ Interior Gateway Routing Protocol (IGRP).

Không giống như IGRP là một giao thức định tuyến theo lớp địa chỉ, EIGRP có hỗ trợ định tuyến liên miền không theo lớp địa chỉ (CIDR – Classless Interdomain Routing) và cho phép người thiết kế mạng tối ưu không gian sử dụng địa chỉ bằng VLSM. So với IGRP, EIGRP có thời gian hội tụ nhanh hơn, khả năng mở rộng tốt hơn và khả năng chống lặp vòng cao hơn.

Hơn nữa, EIGRP còn thay thế được cho giao thức Novell Routing Information Protocol (Novell RIP) và Apple Talk Routing Table Maintenance Protocol (RTMP) để phục vụ hiệu quả cho cả hai mạng IPX và Apple Talk.

EIGRP thường được xem là giao thức lai vì nó kết hợp các ưu điểm của cả giao thức định tuyến theo vectơ khoảng cách và giao thức định tuyến theo trạng thái đường liên kết.

EIGRP là một giao thức định tuyến nâng cao hơn dựa trên các đặc điểm cả giao thức định tuyến theo trạng thái đường liên kết. Những ưu điểm tốt nhất của OSPF như thông tin cập nhật một phần, phát hiện router láng giềng…được đưa vào EIGRP. Tuy nhiên, cấu hình EIGRP dễ hơn cấu hình OSPF.

EIGRP là một lựa chọn lý tưởng cho các mạng lớn, đa giao thức được xây dựng dựa trên các Cisco router.

Chương này sẽ đề cập đến các nhiệm vụ cấu hình EIGRP, đặc biết tập trung vào cách EIGRP thiết lập mối quan hệ với các router thân mật, cách tính toán đường chính và đường dự phòng khi cần thiết, cácg đáp ứng với sự cố của một đường đi nào đó.

Một hệ thống mạng được xây dựng bởi nhiều thiết bị, nhiều giao thức và nhiều loại môi trường truyền. Khi một bộ phận nào đó của mạng không hoạt động đúng thì sẽ có một vài người dùng không truy cập được hoặc có thể cả hệ thống mạng cũng không hoạt động được. Cho dù trong trường hợp nào thì khi sự cố xảy ra người

quản trị mạng phải nhanh chóng xác định được sự cố và xử lí chúng. Sự cố mạng thường do những nguyên nhân sau:

- Gõ sai câu lệnh
- Cấu hình danh sách kiểm tra truy cập ACL không đúng hoặc đặt ACL không đúng chỗ
- Các cấu hình cho router, switch và các thiết bị mạng khác
- Kết nối vật lý không tốt

Người quản trị mạng cần tiếp cận với sự cố một cách có phương pháp, sử dụng sơ đồ xử lý sự cố tổng quát. Trước tiên là kiểm tra sự cố ở lớp vật lý trước rồi mới đi dần lên các lớp trên. Mặ dù chương này chỉ tập trung vào xử lý sự cố các hoạt động của giao thức định tuyến ở Lớp 3 nhưng cũng rất quan trong cho các bạn khi cần loại trừ sự cố ở các lớp dưới.

Sau khi hoàn tất chương này, các bạn sẽ thực hiện được những việc sau:

- Mô tả sự khác nhau giữa EIGRP và IGRP
- Mô tả các khái niệm, kĩ thuật và cấu trúc dữ liệu của EIGRP
- Hiểu được quá trình hội tụ của EIGRP và các bước hoạt động cơ bản của thuật toán DUAL (Diffusing Update Algorithm)
- Thực hiện cấu hình EIGRP cơ bản
- Cấu hình đường tổng hợp cho EIGRP
- Mô tả quá trình EIGRP xây dựng và bảo trì bảng định tuyến
- Kiểm tra hoạt động của EIGRP
- Mô tả 8 bước để xử lý sự cố tổng quát
- Áp dụng tiến trình logic để xử lý sự cố định tuyến.
- Xử lý sự cố của hoạt động định tuyến RIP bằng cách sử dụng lệnh show và debug.
- Xử lý sự cố của hoạt động định tuyến IGRP bằng cách sử dụng lệnh show và debug
- Xử lý sự cố của hoạt động định tuyến EIGRP bằng cách sử dụng lệnh show và debug
- Xử lý sự cố của hoạt động định tuyến OSPF bằng cách sử dụng lệnh show và debug

3.1. Các khái niệm của EIGRP

3.1.1. So sánh EIGRP và IGRP

Cisco đưa ra giao thức EIGRP vào năm 1994 như là một phiên bản mới mở rộng và nâng cao hơn của giao thức IGRP. Kĩ thuật vectơ khoảng cách trong IGRP vẫn được sử dụng cho EIGRP

EIGRP cải tiến các đặc tính của quá trình hội tụ, hoạt động hiệu quả hơn IGRP. Điều này cho phép chúng ta mở rộng, cải tiến cấu trúc trong khi vẫn giữ nguyên những gì đã xây dựng trong IGRP

Chúng ta sẽ tập trung so sánh EIGRP và IGRP trong các lĩnh vực sau:

- Tính tương thích
- Cách tính thông số định tuyến
- Số lượng hop
- Hoạt động phân phối thông tin tự động
- Đánh dấu đường đi

IGRP và EIGRP hoàn toàn tương thích với nhau. EIGRP router không có ranh giới khi hoạt động chung với IGRP router. Đặc điểm này rất quan trọng khi người sử dụng muốn tận dụng ưu điểm của cả hai giao thức. EIGRP có thể hỗ trợ nhiều loại giao thức khác nhau còn IGRP thì không.

EIGRP và IGRP có cách tính thông số định tuyến khác nhau. EIGRP tăng thông số định tuyến của IGRP sử dụng thông số 24 bit. Bằng cách nhân lên hoặc chia đi 256 lần, EIGRP có thể dễ dàng chuyển đổi thông số định tuyến của IGRP

EIGRP và IGRP đều sử dụng công thức tính thông số định tuyến như sau:

Thông số định tuyến = [K1 * băng thông + (K2 * băng thông/(256 – độ tải) + (K3 * độ trễ)] * [K5/(độ tin cậy + K4)]

Mặc định: K1=1, K2=0, K3=1, K4=0, K5=0.

Khi K4=K5=0 thì phần [K5/ (độ tin cậy + K4)]trong công thức không còn là một nhân tố khi tính thông số định tuyến nữa. Do đó, công thức tính còn lại như sau:

Thông số định tuyến = băng thông + độ trễ

IGRP và EIGRP sử dụng các biến đổi sau để tính toán thông sô định tuyến:

Băng thông trong công thức trên áp dụng cho IGRP = 10 000 000 / băng

thông thực sự

Băng thông trong công thức trên áp dụng cho EIGRP = (10 000 000 / băng thông thực sự) * 256

Độ trễ trong công thức trên áp dụng cho IGRP = độ trễ thực sự/10

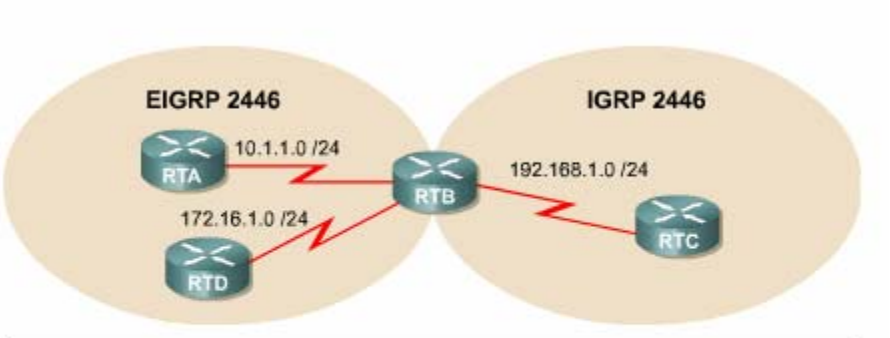
Độ trễ trong công thức trên áp dụng cho EIGRP = (độ trễ thực sự/10) * 256

IGRP có số lượng hop tối đa là 255. EIGRP có số lượng hop tối đa là 224. Con số này dư sức đáp ứng cho một mạng được thiết kế hợp lí lớn nhất.

Để các giao thức định tuyến khác nhau như OSPF và RIP chẳng hạn thực hiện chia sẻ thông tin định tuyến với nhau thì cần phải cấu hình nâng cao hơn. Trong khi đó IGRP và EIGRP có cùng số AS của hệ tự quản sẽ tự động phân phối và chia sẻ thông tin về đường đi với nhau. Trong ví dụ ở hình 3.1.1, RTB tự động phân phối các thông tin về đường đi mà EIGRP học được cho IGRP AS và ngược lại.

EIGRP đánh dấu những đường mà nó học được từ IGRP hay từ bất kì nguồn bên ngoài nào khác là đường ngoại vi vì những con đường này không xuất phát từ EIGRP router. IGRP thì không phân biệt đường ngoại vi và nội vi.

Ví dụ như hình 3.1.1, trong kết quả hiển thị của lệnh **show ip route,** đường EIGRP được đánh dấu bằng chữ D, đường ngoại vi được đánh dấu bằng chữ EX. RTA phân biệt giữa mạng học được từ EIGRP (172.16.0.0) và mạng được phân phối từ IGRP (192.168.1.0). Trong bảng định tuyến của RTC, giao thức IGRP không có sự phân biệt này. RTC chỉ nhận biết tất cả các đường đều là đường IGRP mặc dù 2 mạng 10.1.1.0 và 172.16.0.0 là được phân phối từ EIGRP.




```
RTB(config)#router igrp 2446
RTB(config-router)#network 192.168.1.0
RTB(config)#router eigrp 2446
RTB(config-router)#network 10.1.1.0
RTB(config-router)#network 172.16.1.0
```

3.1.2. Các khái niệm và thuật ngữ của EIGRP

EIGRP router lưu giữ các thông tin về đường đi và cấu trúc mạng trên RAM, nhờ đó chúng đáp ứng nhanh chóng theo sự thay đổi. Giống như OSPF, EIGRP cũng lưu những thông tin này thành từng bảng và từng cơ sở dữ liệu khác nhau.

EIGRP lưu các con đường mà nó học được theo một cách đặc biệt. Mỗi con đường có trạng thái riêng và có đánh dấu để cung cấp thêm nhiều thông tin hữu dụng khác.

EIGRP có ba loại bảng sau:

- Bảng láng giềng (Neighbor table)
- Bảng cấu trúc mạng (Topology table)
- Bảng định tuyến (Routing table)

Bảng láng giềng là bảng quan trọng nhất trong EIGRP. Mỗi router EIGRP lưu giữ một bảng láng giềng, trong đó là danh sách các router thân mật với nó. Bảng này tương tự như cơ sở dữ liệu về các láng giềng của OSPF. Đối với mỗi giao thức mà EIGRP hỗ trợ, EIGRP có một bảng láng giềng riêng tương ứng.

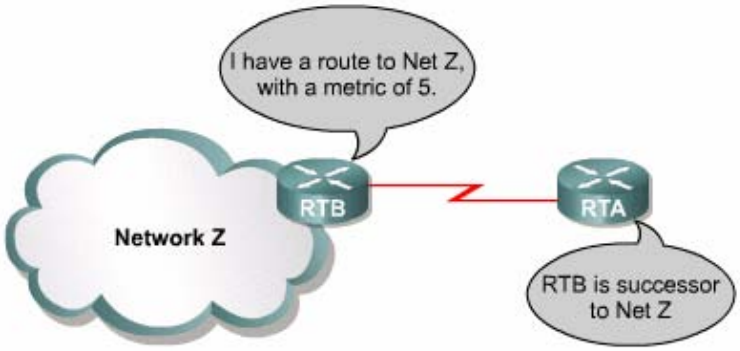
Khi phát hiện một láng giềng mới, router sẽ ghi lại địa chỉ và cổng kết nối của láng giềng đó vào bảng láng giềng. Khi láng giềng gửi gói hello trong đó có thông số về khoảng thời gian lưu giữ. Nếu router không nhận được gói hello khi đến định kì thì khoảng thời gian lưu giữ là khoảng thời gian mà router chờ và vẫn xem là router láng giềng còn kết nối được và còn hoạt động. Khi khoảng thời gian lưu giữ đã hết mà vẫn không còn kết nối được và còn hoạt động. Khi khoảng thời gian lưu giữ đã hết mà vẫn không nhận được hello từ router láng giềng đó, thì xem như router láng giềng đã không còn kết nối được hoặc không còn hoạt động, thuật toán DUAL

(Difusing Update Algorithm) sẽ thông báo sự thay đổi này và thực hiện tính toán lại theo mạng mới.
Bảng cấu trúc mạng là bảng cung cấp dũ liệu để xây dưngj lên mạng định tuyến của EIGRP. DUAL lấy thông tin từ bảng láng giềng và bảng cấu trúc mạng để tính toán chọn đường có chi phí thấp nhất đến từng mạng đích.
Mỗi EIGRP router lưu một bảng cấu trúc mạng riêng tương ứng với từng loại giao thức mạng khác nhau. Bảng cấu trúc mạng chứa thông tin về tất cả các con đường mà router học được. Nhờ những thông tin này mà router có thể xác định đường đi khác để thay thế nhanh chóng khi cần thiết. Thuật tóan DUAL chọn ra đường tốt nhất đến mạng đích gọi là đường kính (successor router).
Sau đây là những thông tin chứa trong bảng cấu trúc mạng:

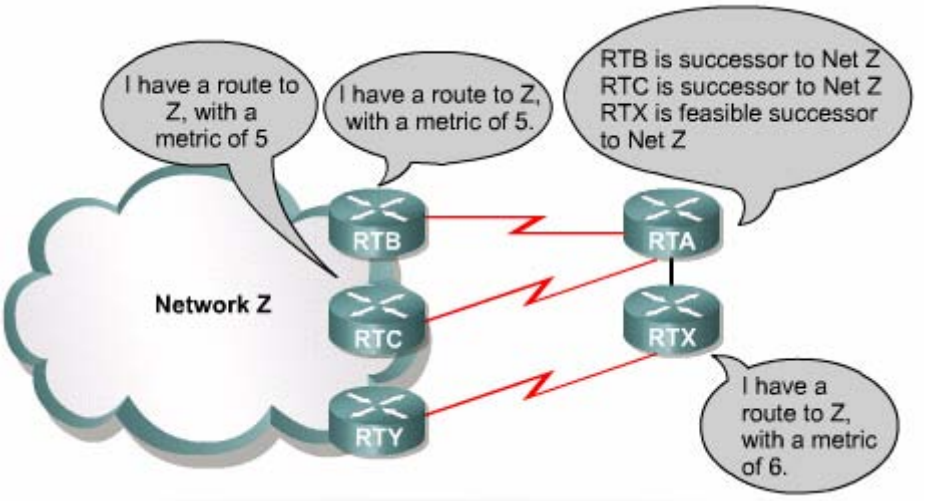
- Feasible distance (FD): là thông tin định tuyến nhỏ nhất mà EIGRP tính được cho từng mạng đích.
- Route source: là nguồn khởi phát thông tin về một con đường nào đó. Phần thông tin này chỉ có với những đường được học từ ngoài mạng EIGRP.
- Reported disdiance (RD): là thông số định tuyến đến một router láng giềng thân mật thông báo qua.
- Thông tin về cổng giao tiếp mà router sử dụng để đi đến mạng đích.
- Trạng thái đường đi: Trạng thái không tác động (P – passive) là trạng thái ổn định, sẵn sàng sử dụng được, trạng thái tác động (A – active) là trạng thái đang trong tiến trình tính toán lại của DUAL.

Bảng định tuyến EIGRP lưu giữ danh sách các đường tốt nhất đến các mạng đích. Những thông tin trong bảng định tuyến được rút ra từ bảng từ cấu trúc mạng. Router EIGRP có bảng định tuyến riêng cho từng giao thức mạng khác nhau.
Con đường được chọn làm đường chính đến mạng đích gọi là successor. Từ thông tin trong bảng láng giềng và bảng cấu trúc mạng, DUAL chọn ra một đường chính và đưa lên mạng định tuyến. Đến một mạng đích có thể có đến 4 successor. Những đường này có chi phí bằng nhau hoặc không bằng nhau. Thông tin về successor cũng được đạt trong bảng cấu trúc mạng.
Đường Feasible successor (FS) là đường dự phòng cho đường successor. Đường này cũng được chọn ra cùng với đường successor nhưng chúng chỉ được lưu trong bảng cấu trúc mạng nhưng điều này không bắt buộc.
Router xem hop kế tiếp của đường Feasible successor dưới nó gần mạng đích hơn nó. Do đó, chi phí của Feasible successor được tính bằng chi phí của chính nó cộng với chi phí vào router láng giềng thông báo qua. Trong trường hợp successor bị sự cố thì router sẽ tìm Feasible successor để thay thế. Một đường Feasible successor bắt buộc phải có chi phí mà router láng giềng thông báo qua thấp hơn chi phí của đường successor hiện tại. Nếu trong bảng cấu trúc mạng không có sẵn đường Feasible successor thì con đường đến mạng đích tương ứng được đưa vào trạng

thái Active và router bắt đầu gửi các gói yêu cầu đến tất cả các láng giềng để tính toán lại cấu trúc mạng. Sau đó với các thông tin mới nhận được, router có thể sẽ chọn ra được successor mới hoặc Feasible successor mới. Đường mới được chọn xong sẽ có trạng thái là Passive.



Hình 3.1.2.a. RTA có thể có nhiều successor đến mạng Z nếu RTB và RTC gửi thông báo về chi phí đến mạng Z như nhau

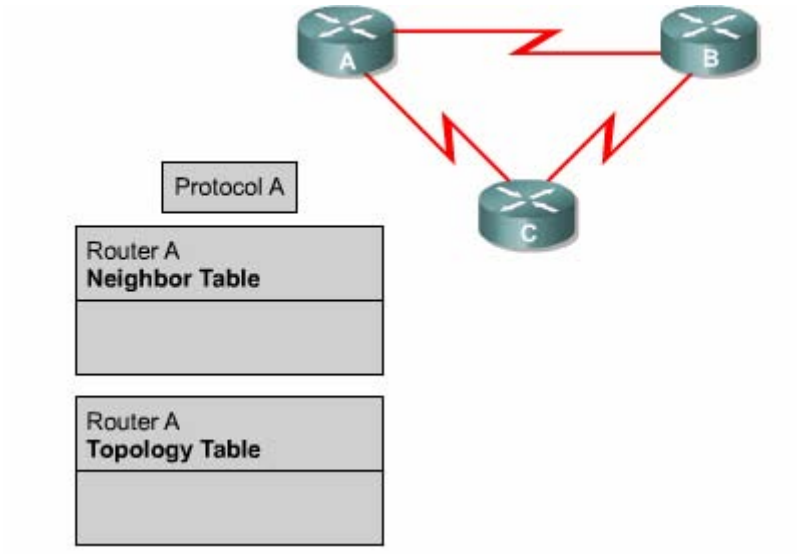


Hình vẽ 3.1.2.b.

Bảng cấu trúc mạng còn lưu nhiều thông tin khác về các đường đi. EIGRP phân loại ra đường nôi vi và đường ngoại vi. Đường nội vi là đường xuất phát từ bên trong hệ tự quản (Á –Autonomous system) của EIGRP. EIGRP có dán nhãn (Administrator tag) với giá trị từ 0 đến 255 để phân biệt đường thuộc loại nào.

Đường ngoại vi là đường xuất phát từ bên ngoài Á của EIGRP. Các đường ngoại vi là những đường được học từ các giao thức định tuyến khác như RIP, OSPF và IGRP. Đường cố định cũng được xem là đường ngoại vi.

```
RTX#show ip eigrp topology 204.100.50.0
IP-EIGRP topology entry for 204.100.50.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s),
FD is 2297856
  Routing Descriptor Blocks:
  10.1.0.1 (Serial0), from 10.1.0.1, Send flag is 0x0
      Composite metric is (2297856/128256), Route is External
      Vector metric:
        Minimum bandwidth is 1544 Kbit
        Total delay is 25000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
      External data:
        Originating router is 192.168.1.1
        AS number of route is 0
        External protocol is Connected, external metric is 0
        Administrator tag is 0 (0x00000000)
```



3.1.3. Các đặc điểm của EIGRP

EIGRP hoạt động khác với IGRP. Về bản chất EIGRP là một giao thức định tuyến theo vectơ khoảng cách nâng cao nhưng khi cập nhật và bảo trì thông tin láng giềng và thông tin định tuyến thì nó làm việc giống như một giao thức định tuyến theo trạng thái đường liên kết. Sau đây là các ưu điểm của EIGRP so với giao thức định tuyến theo vectơ khoảng cách thông thường:

- Tốc độ hội tụ nhanh.
- Sử dụng băng thông hiệu quả.

- Có hỗ trợ VLSM (Variable — Length Subnet Mask) và CIDR (Classless Interdomain Routing). Không giống như IGRP, EIGRP có trao đổi thông tin về subnet mask nên nó hỗ trợ được cho hệ thống IP không theo lớp.
- Hỗ trợ nhiều giao thức mạng khác nhau.
- Không phụ thuộc vào giao thức định tuyến. Nhờ cấu trúc từng phần riêng biệt tương ứng với từng giao thức mà EIGRP không cần phải chỉnh sửa lâu. Ví dụ như khi phát triển để hỗ trợ một giao thức mới như IP chẳng hạn, EIGRP cần phải có thêm phần mới tương ứng cho IP nhưng hoàn toàn không cần phải viết lại EIGRP.

EIGRP router hội tụ nhanh vì chúng sử dụng DUAL. DUAL bảo đảm hoạt động không bị lặp vòng khi tính toán đường đi, cho phép mọi router trong hệ thống mạng thực hiện đồng bộ cùng lúc khi có sự thay đổi xảy ra.

EIGRP sử dụng băng thông hiệu quả vì nó chỉ gửi thông tin cập nhật một phần và giới hạn chứ không gửi toàn bộ bảng định tuyến. Nhờ vậy nó chỉ tốn một lượng băng thông tối thiểu khi hệ thống mạng đã ổn định. Điều này tương tự như hoạt động cập nhật của OSPF, nhưng không giống như router OSPF, router EIGRP chỉ gửi thông tin cập nhật một phần cho router nào cần thông tin đó mà thôi, chứ không gửi cho mọi router khác trong vùng như OSPF. Chính vì vậy mà hoạt động cập nhật của EIGRP gọi là cập nhật giới hạn. Thay vì hoạt động cập nhật theo chu kỳ, các router EIGRP giữ liên lạc với nhau bằng các gói hello rất nhỏ. Việc trao đổi các gói hello theo định kỳ không chiếm nhiều băng thông đường truyền.

EIGRP có thể hỗ trợ cho IP, IPX và Apple Talk nhờ có cấu trúc từng phần theo giao thức (PDMs — Protocol-dependent modules). EIGRP có thể phân phối thông tin của IPX RIP và SAP để cải tiến hoạt động toàn diện. Trên thực tế, EIGRP có thể điều khiển hai giao thức này. Router EIGRP nhận thông tin định tuyến và dịch vụ, chỉ cập nhật cho các router khác khi thông tin trong bảng định tuyến hay bảng SAP thay đổi.

EIGRP còn có thể điều khiển giao thức Apple Talk Routing Table Maintenance Protocol (RTMP). RTMP sử dụng số lượng hop để chọn đường nên khả năng chọn đường không được tốt lắm. Do đó, EIGRP sử dụng thông số định tuyến tổng hợp

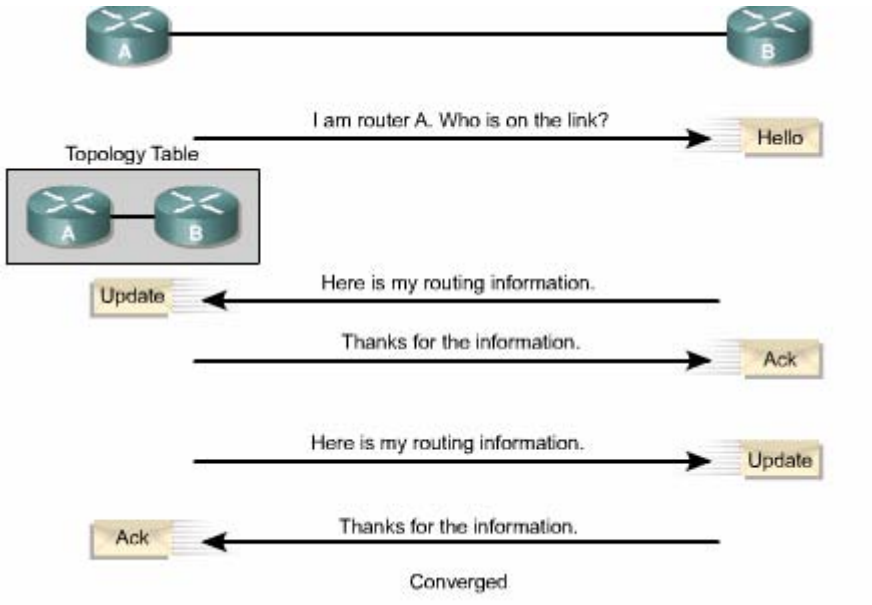
cấu hình được để chọn đường tốt nhất cho mạng Apple Talk. Là một giao thức định tuyến theo vectơ khoảng cách, RTMP thực hiện trao đổi toàn bộ thông tin định tuyến theo chu kỳ. Để giảm bớt sự quá tải này, EIGRP thực hiện phân phối thông tin định tuyến Apple Talk khi có sự kiện thay đổi mà thôi. Tuy nhiên, Apple Talk client cũng muốn nhận thông tin RTMP từ các router nội bộ, do đó EIGRP dùng cho Apple Talk chỉ nên chạy trong mạng không có client, ví dụ như các liên kết WAN chẳng hạn.

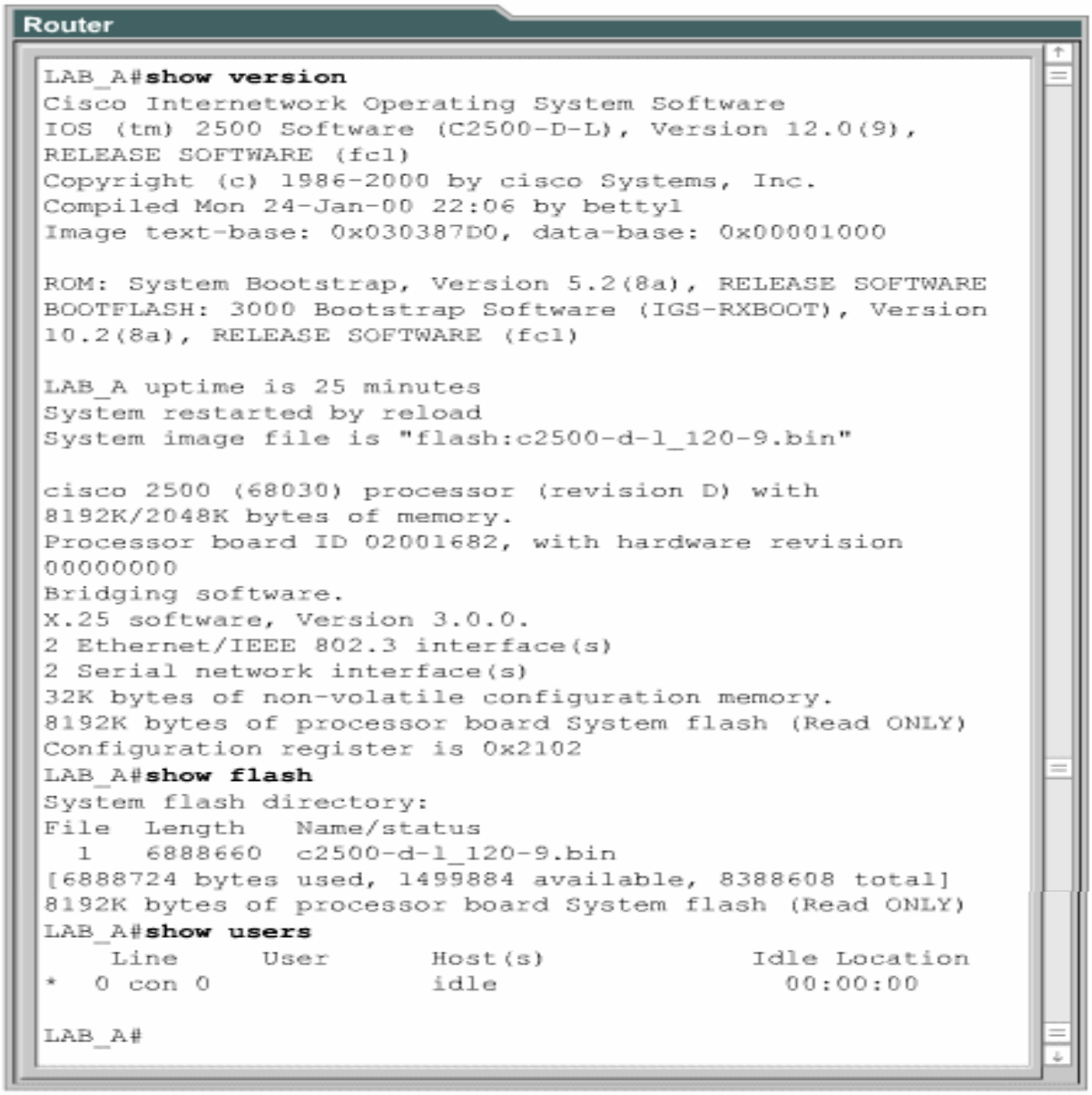
3.1.4. Các kỹ thuật của EIGRP

EIGRP có rất nhiều kỹ thuật mới để cải tiến hiệu quả hoạt động, tốc độ hội tụ và các chức năng so với IGRP và các giao thức định tuyến khác. Các kỹ thuật này được tập trung thành 4 loại như sau:

- Sự phát hiện và tái phát hiện các router láng giềng.
- Giao thức truyền tải tin cậy (RTD — Reliable Transport Protocol).
- Thuật toán DUAL finite — state machine.
- Cấu trúc từng phần theo giao thức (PDMs — Protocol-dependent modules).

Router định tuyến theo vectơ khoảng cách dạng đơn giản không thiết lập mối quan hệ với các láng giềng của nó. RIP và IGRP router chỉ đơn giản là phát quảng bá hay multicast các thông tin cập nhật của nó ra mọi cổng đã được cấu hình. Ngược lại, EIGRP router chủ động thiết lập mối quan hệ với các láng giềng của chúng, tương tự như cách làm của OSPF router.


A
B
I am router A. Who is on the link?
Hello
Topology Table
A
B
Update
Here is my routing information.
Thanks for the information.
Ack
Here is my routing information.
Update
Ack
Thanks for the information.
Converged



Hình 3.1.4

Quá trình EIGRP router thiết lập mối quan hệ thân mật được mô tả trong hình

3.1.4. EIGRP router

Sử dụng các gói hello rất nhỏ để thực hiện việc thiết lập mối quan hệ thân mật với các router láng giềng. Mặc định, hello được gửi đi theo chu kỳ là 5 giây. Nếu router vẫn nhận được hello từ láng giềng thì nó sẽ xem như láng giềng này và các đường đi của nó vẫn hoạt động. Bằng cách thiết lập mối quan hệ này, EIGRP router có thể thực hiện được những việc sau:

- Tự động học được đường mới khi chúng kết nối vào hệ thống mạng.
- Xác định một router không còn kết nối hoặc không còn hoạt động nữa.
- Phát hiện sự hoạt động trở lại của các router.

Giao thức vận chuyển tin cậy RTP (Reliable Transport Protocol) là giao thức ở lớp vận chuyển, thực hiện việc chuyển gói EIGRP một cách tin cậy và có thứ tự đến tất cả các láng giềng. Trong mạng IP, host sử dụng TCP để vận chuyển các gói một cách tuần tự và tin cậy. Tuy nhiên, EIGRP là một giao thức độc lập với giao thức mạng, do đó nó không dựa vào TCP/IP để thực hiện trao đổi thông tin định tuyến giống như RIP, IGRP và OSPF đã làm. Để không bị phụ thuộc vào IP, EIGRP sử dụng RTP làm giao thức vận chuyển riêng độc quyền của nó để đảm bảo việc truyền tin định tuyến.

EIGRP có thể yêu cầu RTP cung cấp dịch vụ truyền tin cậy hoặc không tin cậy tuỳ theo yêu cầu của từng trường hợp. Ví dụ, các gói hello được truyền theo định kỳ và cần phải càng nhỏ càng tốt nên chúng không cần phải dùng chế độ truyền tin cậy. Ngược lại, việc truyền tin cậy các thông tin định tuyến sẽ có thể làm tăng tốc độ hội tụ vì EIGRP router không cần chờ hết thời hạn mới truyền lại.

Với RTP, EIGRP có thể gửi multicast và trực tiếp cho các đối tác khác nhau cùng một lúc, giúp tối ưu hiệu quả hoạt động.

Thành phần trung tâm của EIGRP là thuật toán Diffusing Update Algorithm (DUAL), là bộ máy tính toán đường đi của EIGRP. Tên đầy đủ của kỹ thuật này là DUAL finite-state machine (FSM). FSM là một bộ máy thuật toán nhưng không phải là một thiết bị cơ khí có các thành phần di chuyển được. FSM định nghĩa một tập hợp các trạng thái có thế trải qua, sự kiện nào gây ra trạng thái nào và sẽ có kết quả gì. Người thiết kế sử dụng FSM để lập trình cách mà một thiết bị, một chương trình máy tính hay một thuật toán định tuyến sẽ xử lý như thế nào với một tập hợp các dữ liệu đầu vào. DUAL FSM chứa tất cả các logic được sử dụng để tính toán và so sánh đường đi trong mạng EIGRP.

DUAL lưu tất cả các đường đi mà láng giềng thông báo qua. Dựa trên thông số định tuyến tổng hợp của mỗi đường, DUAL so sánh và chọn ra đường có chi phí thấp nhất đến đích. DUAL đảm bảo mỗi một đường này là không có lặp vòng.

Đường chính được chọn ra gọi là đường successor. Đường successor được lưu trên băng định tuyến và đồng thời cũng được lưu trong bảng cấu trúc mạng.

EIGRP giữ các thông tin quan trọng về đường đi và cấu trúc mạng trong bảng láng giềng và bảng cấu trúc mạng. Hai bảng này cung cấp cho DUAL các thông tin về đường đi khi cần thiết. Nếu có một đường liên kết bị đứt, DUAL sẽ tìm đường thay thế hoặc một feasible successor trong bảng cấu trúc mang.

Một trong những ưu điểm nổi bật của EIGRP là nó được thiết kế thành từng phần riêng biệt theo giao thức. Nhờ cấu trúc này, nó có khả năng mở rộng và tương thích tốt nhất. Các giao thức được định tuyến như IP, IPX và Apple Talk được đưa vào EIGRP thông qua các PDM. EIGRP có thể dễ dàng tương thích với giao thức định tuyến mới hoặc các phiên bản mới của chúng như IPv6 chẳng hạn bằng cách thêm PDM vào.

Mỗi PDM chịu trách nhiệm thực hiện mọi chức năng liên quan đến một giao thức được định tuyến. Ví dụ phần IP- EIGRP chịu trách nhiệm các việc sau:

- Gửi và nhận các gói EIGRP chứa dữ liệu IP.
- Thông báo cho DUAL khi nhận được thông tin định tuyến IP mới.
- Duy trì kết quả chọn đường của DUAL trong bảng định tuyến IP.
- Phân phối thông tin định tuyến mà nó học được từ các giao thức định tuyến IP khác.

3.1.5. Cấu trúc dữ liệu của EIGRP

Giống như OSPF, EIGRP dựa vào nhiều loại gói dữ liệu khác nhau để duy trì các loại bảng của nó và thiết lập mối quan hệ phức tạp với router láng giềng.

Có 5 loại gói EIGRP:

- Hello.
- Báo nhận.
- Cập nhật.
- Yêu cầu.

- Đáp ứng.

EIGRP dựa vào các gói hello để phát hiện, kiểm tra và tái phát hiện các router láng giềng. Tái phát hiện có nghĩa là router EIGRP không nhận được hello từ một router láng giềng trong suốt khoảng thời gian lưu giữ nhưng sau đó router láng giềng này lại tái lập lại thông tin liên lạc.

Chu kỳ gửi hello của EIGRP router có thể cấu hình được. Khoảng thời gian hello mặc định phụ thuộc vào băng thông trên từng cổng của router. Trong mạng IP, EIGRP router gửi hello theo địa multicast 224.0.0.10.

EIGRP router lưu thông tin về các láng giềng trong bảng láng giềng. Bảng láng giềng này có lưu số thứ tự (Seq No) và thời gian lưu giữ của gói EIGRP cuối cùng nhận được từ mỗi router láng giềng. Theo định kỳ và trong giới hạn của khoảng thời gian lưu giữ, router phải nhận được gói EIGRP thì những đường tương ứng mới có trạng thái Passive. Trạng thái Passive có nghĩa là trạng thái hoạt động ổn định.

Nếu router không nghe ngóng được gì về router láng giềng trong suốt khoảng thời gian lưu giữ thì EIGRP sẽ xem như láng giềng đó đã bị sự cố và DUAL phải tính toán lại bảng định tuyến. Mặc định, khoảng thời gian lưu giữ gấp 3 lần chu kỳ hello. Người quản trị mạng có thể cấu hình giá trị cho 2 khoảng thời gian này phù hợp hơn với hệ thống của mình.

Bandwidth	Example Link	Default Hello Interval	Default Hold Time
1.544 Mbps or less	Multipoint Frame Relay	60 seconds	180 seconds
Greater than 1.544 Mbps	T1, Ethernet	5 seconds	15 seconds

Hình 3.1.5

OSPF bắt buộc các router láng giềng với nhau phải có cùng khoảng thời gian hello và khoảng thời gian bất động thì mới có thể thông tin liên lạc với nhau được. EIGRP thì không yêu cầu như vậy. Router sẽ học các khoảng thời gian của router láng giềng thông qua việc trao đổi gói hello. Chúng sẽ dùng thông tin trong đó để

thiết lập mối quan hệ ổn định mà không cần các khoảng thời gian này phải giống nhau giữa chúng.

Gói hello thường được gửi theo chế độ không bảo đảm tin cậy. Điều này có nghĩa là không có báo nhận cho các gói hello.

EIGRP router sử dụng gói báo nhận để xác nhận là đã nhận được gói EIGRP trong quá trình trao đổi tin cậy. Giao thức vận chuyển tin cậy (RTP — Reliable Transport Protocol) cung cấp dịch vụ liên lạc tin cậy giữa hai host EIGRP. Gói báo nhận chính là gói hello mà không có dữ liệu. Không giống như hello được gửi multicast, các gói báo nhận chỉ gửi trực tiếp cho một máy nhận. Báo nhận có thể được kết hợp vào loại gói EIGRP khác như gói trả lời chẳng hạn.

Gói cập nhật được sử dụng khi router phát hiện một láng giềng mới. Router EIGRP sẽ gửi gói cập nhật cho router láng giềng mới này để nó có thể xây dựng bảng cấu trúc mạng. Có thể sẽ cần nhiều gói cập nhật mới có thể truyền tải hết các thông tin cấu trúc mạng cho router láng giềng mới này.

Gói cập nhật còn được sử dụng khi router phát hiện sự thay đổi trong cấu trúc mạng. Trong trường hợp này, EIGRP router sẽ gửi multicast gói cập nhật cho mọi router láng giềng của nó để thông báo về sự thay đổi. Mọi gói cập nhật đều được gửi bảo đảm.

EIGRP router sử dụng gói yêu cầu khi nó cần một thông tin đặc biệt nào đó từ một hay nhiều láng giềng của nó. Gói đáp ứng được sử dụng để trả lời cho các gói yêu cầu.

Nếu một EIGRP router mất successor và nó không tìm được feasible successor để thay thế thì DUAL sẽ đặt con đường đến mạng đích đó vào trạng thái Active. Sau đó router gửi multicast gói yêu cầu đến tất cả các láng giềng để cố gắng tìm successor mới cho mạng đích này. Router láng giềng phải trả lời bằng gói đáp ứng để cung cấp thông tin hoặc cho biết là không có thông tin nào khác có thể khả thi. Gói yêu cầu có thể được gửi multicast hoặc chỉ gửi cho một máy, còn gói đáp ứng thì chỉ gửi cho máy nào gửi yêu cầu mà thôi. Cả hai loại gói này đều được gửi bảo đảm.

3.1.6. Thuật toán EIGRP

Thuật toán DUAL phức tạp giúp cho EIGRP hội tụ nhanh. Để hiểu rõ hơn về quá trình hội tụ với DUAL, ta xét ví dụ ở hình 3.1.6a. Mỗi router xây dựng một bảng cấu trúc mạng chứa các thông tin về đường đi đến mạng A.

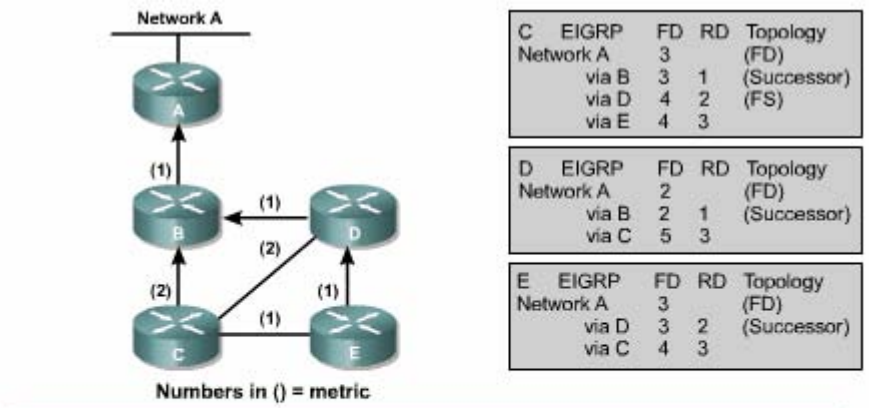
Mỗi bảng cấu trúc mạng trong ví dụ ở các hình 3.1.6.a-f có các thông tin sau:

- Giao thức định tuyến là giao thức EIGRP.
- Chi phí thấp nhất của đường đến một mạng đích gọi là Feasible Distance (FD).
- Chi phí của một đường đến một mạng đích do router láng giềng thông báo qua gọi là Reported Distance (RD).

NGUYÊN TẮC CHỌN ĐƯỜNG FEASIBLE SUCCESSOR:

1. Đường feasible successor là đường dự phòng, thay thế cho đường successor khi đường này bị sự cố.
2. Reported Distance (RD) của một đường đến một đích nào đó là chi phí được thông báo từ một router láng giềng. Chi phí này phải nhỏ hơn Feasible Distance (FD) của đường successor hiện tại.
3. Nếu thoả mãn điều kiện trên thì có nghĩa là không có vòng lặp, đường đó sẽ được chọn làm feasible successor
4. Đường feasible succesor có thể thay thế cho đường successor khi cần thiết.
5. Nếu RD của một đường lớn hơn hoặc bằng FD của successor hiện tại thì đường đó không được chọn làm feasible successor.
6. Router phải tính toán cấu trúc mạng bằng cách thu nhập thông tin từ tất cả các láng giềng.
7. Router gửi gói yêu cầu đến tất cả các láng giềng để tìm thông tin về đường đi và chi phí của đường đó đến mạng đích mà router đang cần .
8. Tất cả các láng giềng phải gửi gói đáp ứng để trả lời cho gói yêu cầu.
9. Router ghi nhận giữ liệu mới nhận được vào bảng cấu trúc mạng của mình.
10. Bây giờ DUAL đã có thể xác định đường successor mới và feasible

successor mới nếu có dựa vào thông tin mới.



Legend	
EIGRP	Protocol Type
FD	Feasible Distance
RD	Reported Distance as advertised by neighbor router
Successor	Primary Route to Destination
FS	Feasible Successor - Backup route to Destination

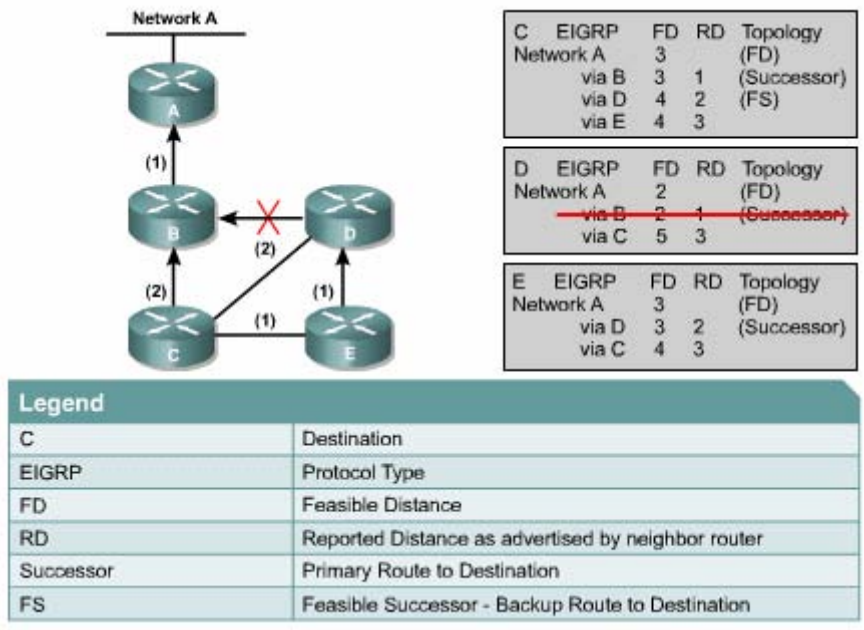
Hình 3.1.6.a

Cột Topology trong hình cho biết đường nào là đường chính hay còn gọi là successor, đường nào là đường dự phòng hay còn gọi là feasible successor (FS). Tuy nhiên, bạn cần lưu ý là không nhất thiết lúc nào cũng phải tìm được feasible successor.

Mạng EIGRP sẽ hoạt động theo các bước mô tả bên dưới để tiến hành hội tụ giữa các router. Hiện tại các router có các thông tin về đường đến mạng A như sau:

- Router C có một đường successor là đường qua Router B.
- Router C có một đường feasible successor là đường qua Router D.
- Router D có một đường successor là đường qua Router B.
- Router D không có đường feasible successor.
- Router E có một đường successor là đường qua Router D.
- Router E không có đường feasible successor.

Sau đây sẽ mô tả mỗi router thực hiện nguyên tắc chọn feasible successor như thế nào khi đường liên kết giữa Router D và Router B bị đứt:



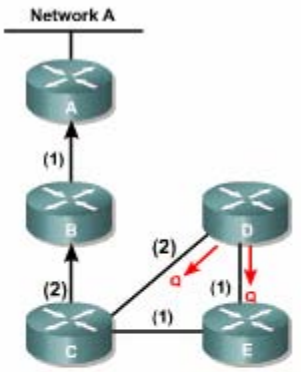
Hình 3.1.6b

Trong Router D (hình 3.1.6b):

- Đường đi qua Router B bị xoá khỏi bảng cấu trúc mạng.
- Đường này là đường successor. Router không xác định được feasible successor trước đó.
- Router D phải tính toán lại đường mới.

Trong Router C:

- Đường đến Mạng A qua Router D bị đứt.
- Đường này bị xoá khỏi bảng.
- Đường này là successor của Router C.



C EIGRP	FD	RD	Topology
Network A	3		(FD)
via B	3	1	(Successor)
via D			
via E	4	3	

D EIGRP		FD	R	Topology
Network A	**ACTIVE**	-1	2	(FD)
via B				(q)
via C		5	3	(q)

E EIGRP	FD	RD	Topology
Network A	3		(FD)
~~via C~~	~~3~~	~~2~~	~~(Successor)~~
via D	4	3	

Legend	
EIGRP	Protocol Type
FD	Feasible Distance
RD	Reported Distance as advertised by neighbor router
Successor	Primary Route to Destination
FS	Feasible Successor - Backup Route to Destination

Hình 3.1.6.c

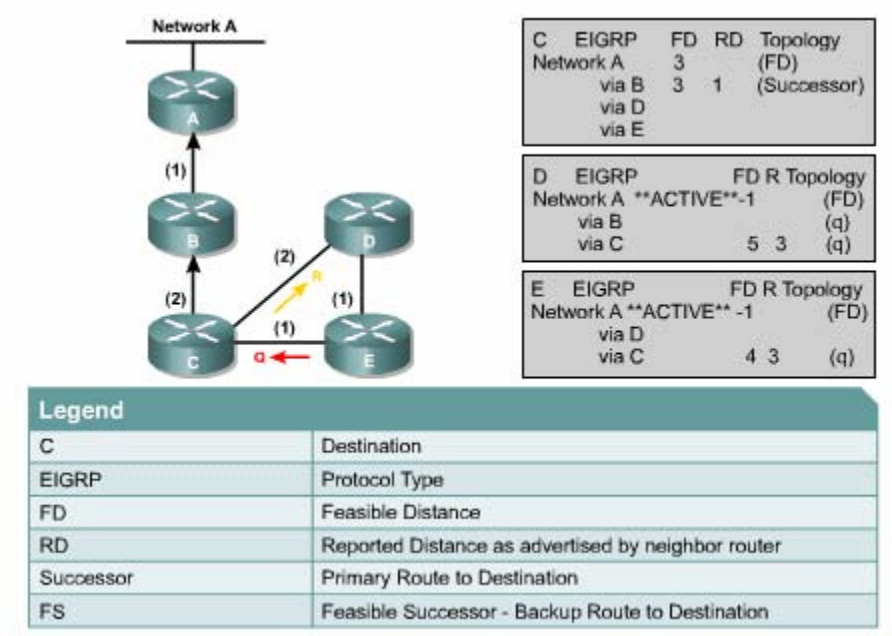
Trong router D (hình 3.1.6.c):

- Router D không có feasible successor. Do đó, nó không thể chuyển qua đường dự phòng được.
- Router D phải tính toán lại cấu trúc mạng. Con đường đến Mạng A được đặt voà trạng thái Active.
- Router D gửi gói yêu cầu cho tất cả các láng giềng kết nối với nó là Router C và Router E để yêu cầu gửi thông tin về mạng.
- Trước đó, Router C có đường qua Router D.
- Trước đó, Router D không có đường qua Router E.

Trong Router E:

- Đường đến Mạng A thông qua Router D bị đứt.
- Đường này là đường successor của Router E.
- Router E không có feasible successor.

- Lưu ý rằng RD của đường thông qua Router C là 3, bằng với chi phí của đường successor qua Router D.



Hình 3.1.6.d

Trong Router C (hình 3.1.6.d):

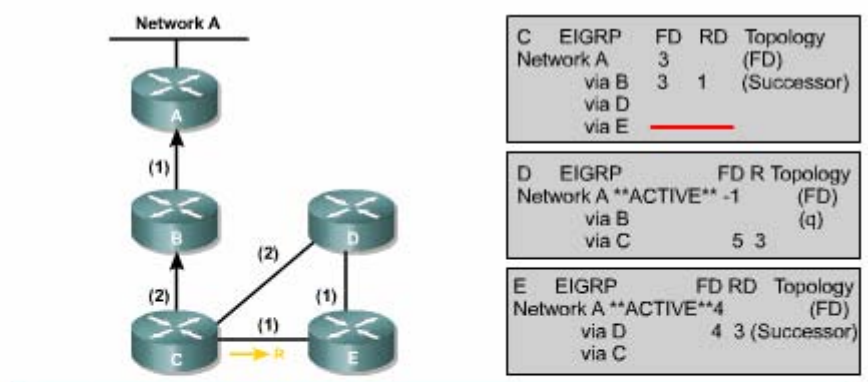
- Router E gửi gói yêu cầu cho Router C.
- Router C xoá đường qua Router E khỏi bảng.
- Router C trả lời cho Router D với thông tin về đường mới đến Mạng A.

Trong Router D:

- Trạng thái của đường đến Mạng A vẫn là Active vì công việc tính toán chưa hoàn tất.
- Router C trả lời cho Router D để xác nhận là đường đến Mạng A đang hoạt động với chi phí là 5.
- Router D vẫn đang chờ đáp ứng từ Router E.

Trong Router E:

- Router E không có feasible successor đến mạng A.
- Do đó, Router E đánh dấu trạng thái con đường đến Mạng A là Active.
- Router E phải tính toán lại cấu trúc mạng.
- Router E xoá đường đi qua Router D ra khỏi bảng.
- Router E gửi gói yêu cầu cho Router C để yêu cầu thông tin về mạng.
- Trước đó, Router E đã có thông tin về đường đi qua Router C. Đường này có chi phí là 3, bằng với chi phí của đường successor.



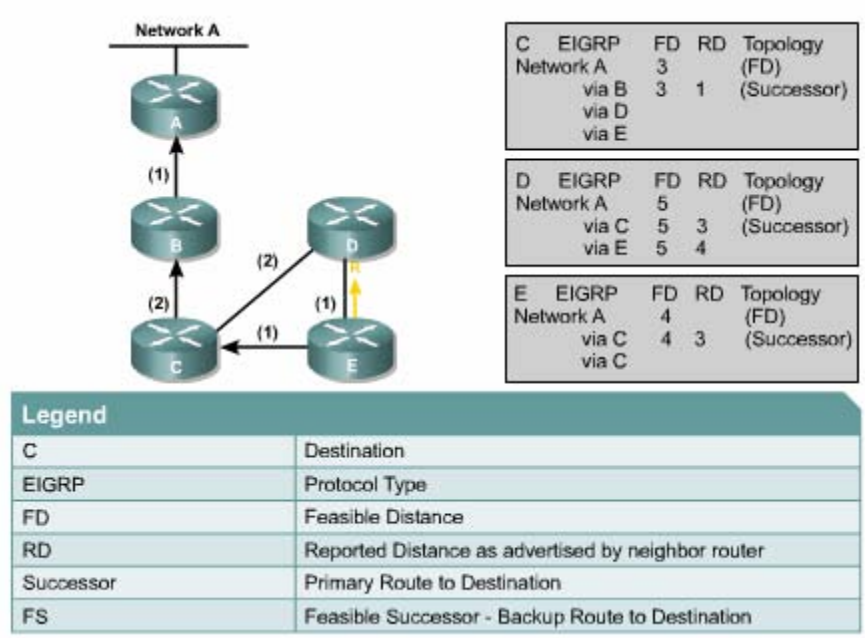
Legend	
C	Destination
EIGRP	Protocol Type
FD	Feasible Distance
RD	Reported Distance as advertised by neighbor router
Successor	Primary Route to Destination
FS	Feasible Successor - Backup Route to Destination

Hình 3.1.6.e

Trong Router E (hình 3.1.6.e):

- Router C trả lời lại thông tin về đường đến Mạng A có RD là 3.
- Bây giờ Router E có thể chọn đường thông qua Router C làm successor mới với FD là 4 và RD là 3.
- Trạng thái của đường đến Mạng A được đổi từ Active sang Passive. Lưu ý: trạng thái Passive là trạng thái mặc định khi router vẫn nhận được gói hello

từ trạng thái đó. Do đó trong ví dụ này chỉ cần đánh dấu trạng thái Active thôi.



Hình 3.1.6.f

Trong Router E (hình 3.1.6.f):

- Router E gửi đáp ứng cho Router D để cung cấp thông tin về mạng của Router E.

Trong Router D:

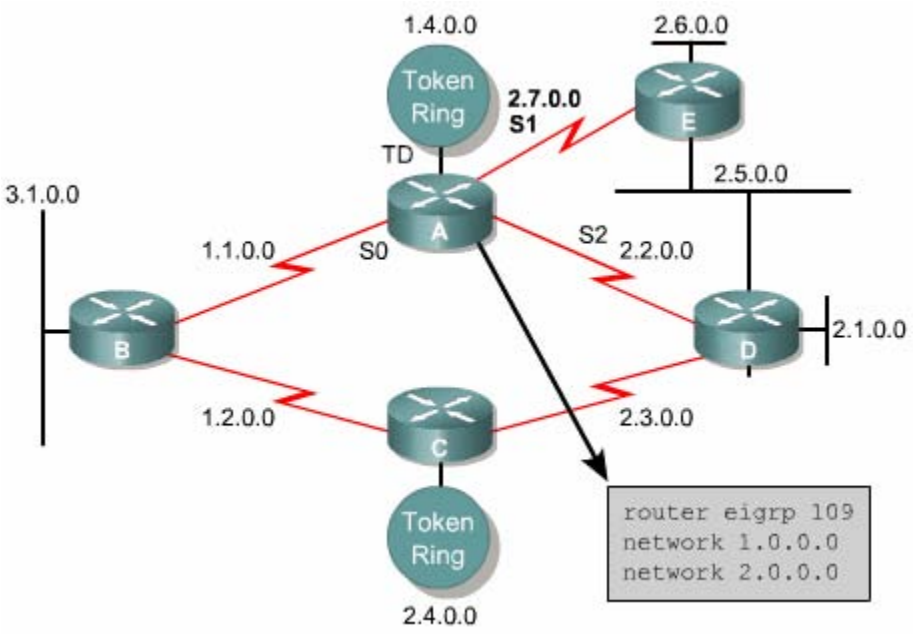
- Router D nhận được gói hồi đáp từ Router E với những thông tin về mạng của Router E.
- Router D ghi nhận con đường đến Mạng A thông qua Router E.
- Con đường này trở thành một đường successor nữa vì nó có chi phí bằng với đường thông qua Router C và nó có RD nhỏ hơn FD của đường thông qua Router C.

Quá trình hội tụ xảy ra giữa mọi router EIGRP sử dụng thuật toán DUAL.

3.2. Cấu hình EIGRP

3.2.1. Cấu hình EIGRP

Trừ thuật toán DUAL là phức tạp, còn cấu hình EIGRP thì khá đơn giản. Tuỳ theo giao thức được định tuyến là IP, IPX hay Apple Talk mà câu lệnh cấu hình EIGRP sẽ khác nhau. Phần sau đây chỉ đề cập đến cấu hình EIGRP cho giao thức IP.



Hình 3.2.1

Sau đây là các bước cấu hình EIGRP cho IP:

1. Sử dụng lệnh sau để khởi động EIGRP và xác định con số của hệ tự quản:

router(config)#router eigrp *autonomous-system-number*

Thông số *autonomous-system-number* xác định các router trong một hệ tự quản. Những router nào trong cùng một hệ thống mạng thì phải có con số này giống nhau.

2. Khai báo những mạng nào của router mà bạn đang cấu hình thuộc về hệ tự quản EIGRP:

router(config-router)#network *network-number*

Thông số *network-number* là địa chỉ mạng của các cổng giao tiếp trên router thuộc về hệ thống mạng EIGRP. Router sẽ thực hiện quảng cáo thông tin về những mạng được khai báo trong câu lệnh network này.

Bạn chỉ khai báo những mạng nào kết nối trực tiếp vào router mà thôi. Ví dụ trên hình 3.2.1, mạng 3.1.0.0 không kết nối vào Router A nên khi cấu hình EIGRP cho Router A chúng ta không khai báo mạng 3.1.0.0.

3. Khi cấu hình cổng serial để sử dụng trong EIGRP, việc quan trọng là cần đặt băng thông cho cổng này. Nếu chúng ta không thay đổi bằng thông của cổng, EIGRP sẽ sử dụng băng thông mặc định của cổng thay vì băng thông thực sự. Nếu đường kết nối thực sự chậm hơn, router có thể không hội tụ được, thông tin định tuyến cập nhật có thể bị mất hoặc là kết quả chọn đường không tối ưu. Để đặt băng thông cho một cổng serial trên router, bạn dùng câu lệnh sau trong chế độ cấu hình của cổng đó:

router(config-if)#bandwidth *kilobits*

Giá trị băng thông khai trong lệnh **bandwidth** chỉ được sử dụng tính toán cho tiến trình định tuyến, giá trị này nên khai đúng với tốc độ của cổng.

4. Cisco còn khuyến cáo nên thêm câu lệnh sau trong cấu hình EIGRP:

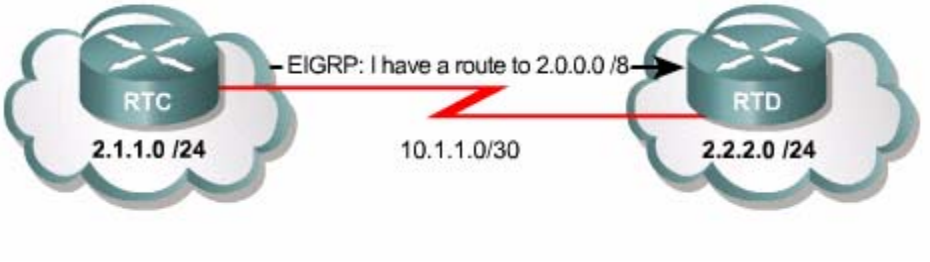
router(config-if)#eigrp log-neighbor-changes

Câu lệnh này sẽ làm cho router xuất ra các câu thông báo mỗi khi có sự thay đổi của các router láng giềng thân mật giúp chúng ta theo dõi sự ổn định của hệ thống định tuyến và phát hiện được sự cố nếu có.

3.2.2. Cấu hình đường tổng hợp cho EIGRP

EIGRP tự động tổng hợp các đường lại theo lớp địa chỉ. Ví dụ như hình 3.2.2a, RTC chỉ kết nối vào mạng con 2.1.1.0 nhưng nó sẽ phát quảng cáo là nó kết nối

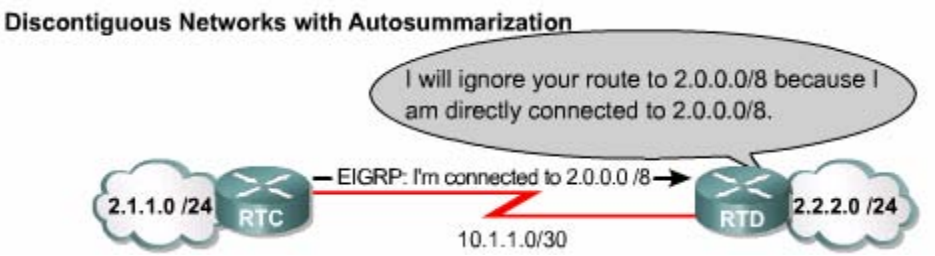
vào mạng lớp A 2.0.0.0. Trong hầu hết các trường hợp, việc tự động tổng hợp này có ưu điểm là giúp cho bảng định tuyến ngắn gọn.



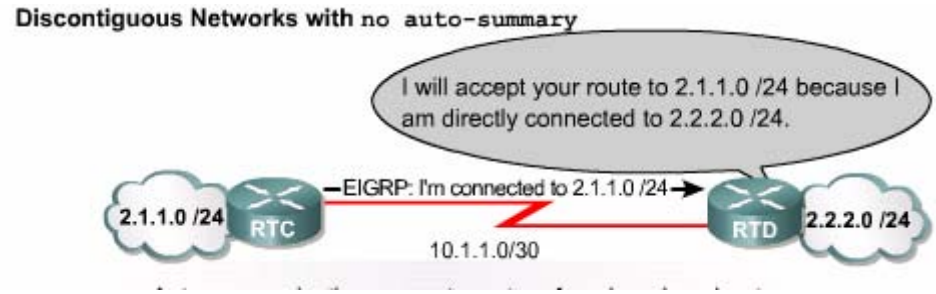
Hình 3.2.2.a. *EIGRP tự động tổng hợp đường đi theo lớp của địa chỉ IP*

Tuy nhiên, trong một số trường hợp bạn không nên sử dụng chế độ tự động tổng hợp đường đi này. Ví dụ trong mạng có sơ đồ địa chỉ không liên tục thì chế độ này phải tắt đi. Để tắt chế độ tự động tổng hợp đường đi, bạn dùng câu lệnh sau:

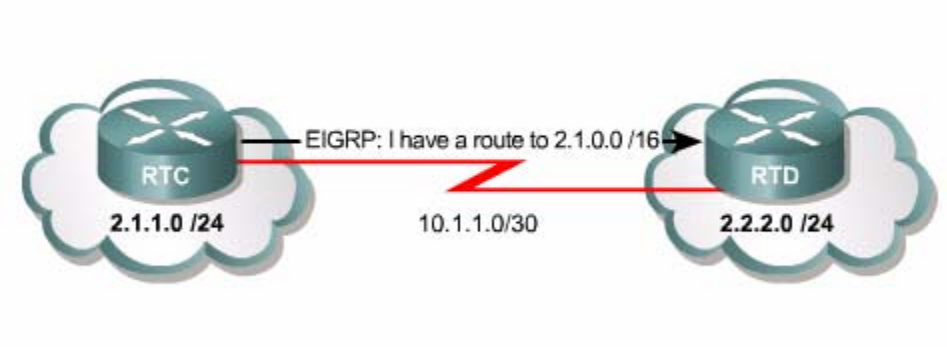
router(config-router)#no auto-summary



Hình 3.2.2.b. *Mạng có sơ đồ địa chỉ không liên tục (hai subnet/24 bị ngắt chính giữa bởi một subnet/30) với chế độ tổng hợp đường đi*



Hình 3.2.2.c. *Mạng có sơ đồ địa chỉ không liên tục có câu lệnh no auto-summary. Khi chế độ tự động tổng hợp đường đi bị tắt, router sẽ quảng cáo từng subnet*



Hình 3.2.2.d. *Việc tổng hợp đường đi của EIGRP có thể được cấu hình trên từng cổng của router*

Với EIGRP, việc tổng hợp đường đi có thể được cấu hình bằng tay trên từng cổng của router với giới hạn tổng hợp mà bạn muốn chứ không tự động tổng hợp theo lớp của địa chỉ IP. Sau khi khai báo địa chỉ tổng hợp cho một cổng của router, router sẽ phát quảng cáo ra cổng đó các địa chỉ được tổng hợp như một câu lệnh đã cài đặt. Địa chỉ tổng hợp được khai báo bằng lệnh **ip summary-address eigrp** như sau:

Router(config-if)**#ip summary-address eigrp** autonomous-system-number ip-address mask administrative-distance

Đường tổng hợp của EIGRP có chỉ số mặc định của độ tin cậy (administrative-distance) là 5. Tuy nhiên, bạn có thể khai báo giá trị cho chỉ số này trong khoảng từ 1 đến 255.

Xét ví dụ như hình 3.2.2.d, RTC được cấu hình như sau:

RTC(config)**#router eigrp 2446**

RTC(config-router)**#no auto-summary**

RTC(config-router)#**exit**

RTC(config)#**interface serial 0/0**

RTC(config-if)#**ip simmary-address ẻigp 2446 2.1.0.0**

255.255.0.0

Khi đó, RTC sẽ thêm vào bảng định tuyến của nó một đường tổng hợp như sau:

D 2.1.0.0/16 is a summary, 00:00:22, Null0

Lưu ý rằng đường tổng hợp có nguồn là Null0 chứ không phải là từ một cổng cụ thể vì đường này chỉ có mục đích để quảng cáo chứ không phải là đại diện cho một đường cụ thể đến mạng đích. Trên RTC, đường tổng hợp này có chỉ số độ tin cậy (administrative distance) là 5.

RTD không hề biết đây là đường tổng hợp nên nó ghi nhận thông tin về đường này từ RTC như một đường EIGRP bình thường với chỉ số tin cậy mặc định của EIGRP là 90.

Trong cấu hình của RTC, chế độ tự động tổng hợp đường đi được tắt đi bằng lệnh **no auto-summary**. Nếu bạn không tắt chế độ tự động tổng hợp này thì RTD sẽ nhận được đồng thời 2 thông tin, một là địa chỉ mạng tổng hợp theo lệnh cài đặt ở trên 2.1.0.0/16 và một là địa chỉ mạng tổng hợp tự động theo lớp của địa chỉ IP 2.0.0.0/8.

Trong đa số các trường hợp, khi bạn muốn cấu hình tổng hợp địa chỉ bằng tay thì bạn nên tắt chế độ tự động tổng hợp bằng lệnh **no auto-summary**.

3.2.3. Kiểm tra hoạt động của EIGRP

Bạn sử dụng các lệnh **show** như trong bảng 3.2.3.a để kiểm tra các hoạt động của EIGRP.

Ngoài ra, các lệnh **debug** là những lệnh giúp bạn theo dõi hoạt động EIGRP khi cần thiết.

Lệnh	Giải thích
Show ip eigrp neighbors [*type number*] [details]	Hiển thị bảng láng giềng của EIGRP. Sử dụng tham số *type number* để xác định cụ thể cổng cần xem. Từ khoá **details** cho phép hiển thị thông tin chi tiết hơn.

Show ip eigrp interfaces [*type number*] [*as-number*] [details]	Hiển thị thông tin EIGRP của các cổng. Sử dụng các tham số in nghiêng cho phép giới hạn phần thông tin hiển thị cho từng cổng hoặc trong từng AS. Từ khoá **details** cho phép hiển thị thông tin chi tiết hơn.
Show ip eigrp topology [*as-number*] [[*ip-address*] mask]	Hiển thị tất cả các feasible successor trong bảng cấu trúc mạng của EIGRP. Sử dụng các tham số in nghiêng để giới hạn thông tin hiển thị theo số AS hay theo địa chỉ mạng cụ thể.
Show ip eigrp topology [active | pending | zero-successors]	Tuỳ theo bạn sử dụng từ khoá nào, router sẽ hiển thị thông tin về các đường đi đang hoạt động, đang chờ xử lý hay không có successor.
Show ip eigrp topology all-links	Hiển thị thông tin về mọi đường đi chứ không chỉ có feasible successor trong bảng cấu trúc EIGRP.
Show ip eigrp traffic [*as-number*]	Hiển thị số gói EIGRP đã gửi đi và nhận được. Bạn sử dụng tham số *as-number* để giới hạn thông tin hiển thị trong một AS cụ thể.

Bảng 3.2.3a. *Các lệnh show dùng cho EIGRP*

Lệnh	**Giải thích**
Debug eigrp fsm	Hiển thị hoạt động của các EIGRP feasible successor giúp chúng ta xác định khi nào tiến trình định tuyến cài đặt và xoá thông tin cập nhật về đường đi.

Debug eigrp packet	Hiển thị các gói EIGRP gửi đi và nhận được. Các gói này có thể là gói hello, cập nhật, báo nhận, yêu cầu hoặc hồi đáp. Số thứ tự của gói và chỉ số báo nhận được sử dụng để gửi bảo đảm các gói EIGRP cũng được hiển thị.

Bảng 3.2.3.b. *Các lệnh EIGRP debug*

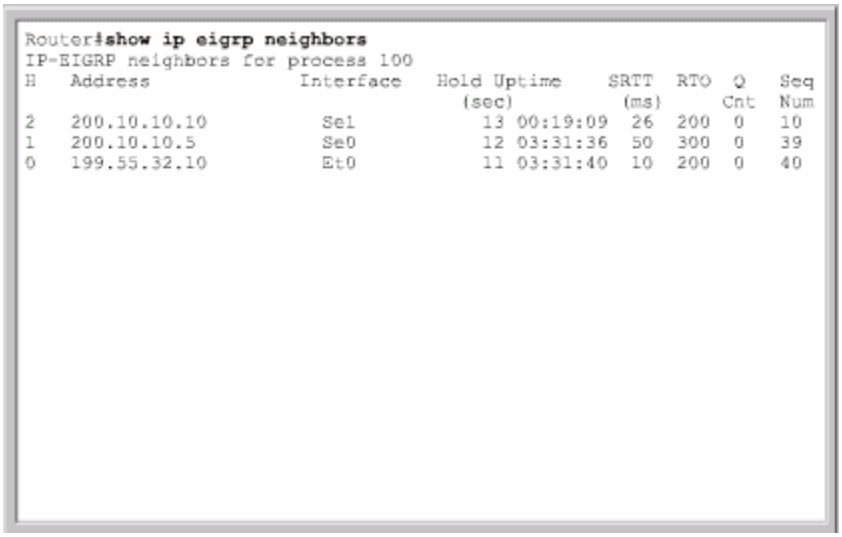
3.2.4. Xây dựng bảng láng giềng.

Router định tuyến theo vectơ khoảng cách dạng đơn giản không thiết lập mối quan hệ với các láng giềng của nó. RIP và IGRP chỉ đơn giản là phát quảng bá hoặc multicast thông tin cập nhật ra các cổng đã được cấu hình. Ngược lại, EIGRP router chủ động thiết lập mối quan hệ với các láng giềng của nó giống như router OSPF đã làm.

Bảng láng giềng là bảng quan trọng nhất trong EIGRP. Mỗi EIGRP lưu một bảng láng giềng, trong đó là danh sách các router láng giềng thân mật. Bảng này tương tự như cơ sở dữ liệu về láng giềng của OSPF. EIGRP có riêng từng bảng láng giềng cho mỗi giao thức mà EIGRP hỗ trợ.

EIGRP router sử dụng các gói hello rất nhỏ để thiết lập mối quan hệ thân mật với các router láng giềng. Mặc định, hello được gửi đi theo chu kỳ 5 giây/lần. Nếu router vẫn nhận được đều đặn các gói hello từ một router láng giềng thì nó vẫn sẽ hiểu rằng router láng giềng đó cùng với các đường đi của nó vẫn còn hoạt động. Bằng cách thiết lập mối quan hệ thân mật như vậy, EIGRP router thực hiện được những việc sau:

- Tự động học được đường mới khi đường này kết nối vào mạng.
- Xác định router láng giềng bị đứt kết nối hay không còn hoạt động nữa.
- Tái phát hiện các router vốn trước đó bị xem là đứt kết nối.



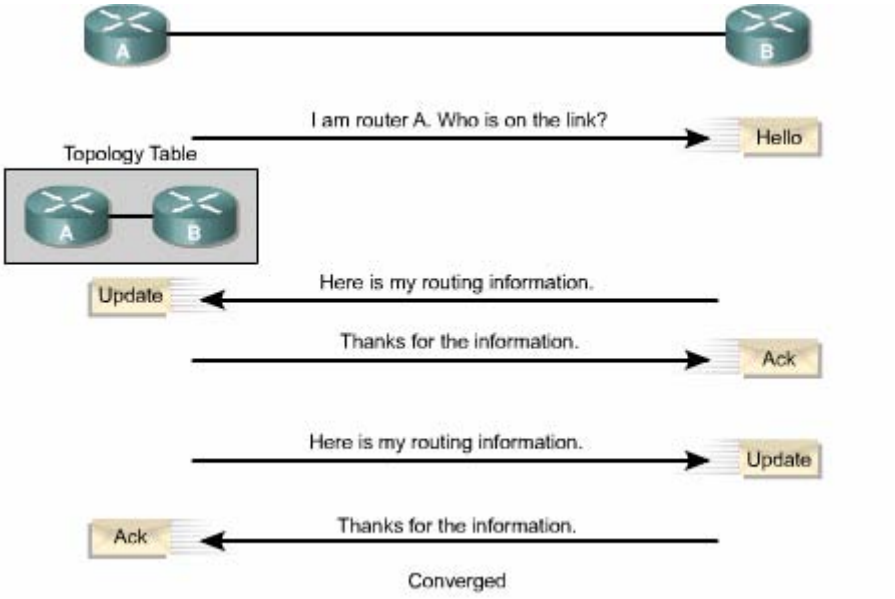
```
Router#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
2   200.10.10.10            Se1              13 00:19:09  26  200  0  10
1   200.10.10.5             Se0              12 03:31:36  50  300  0  39
0   199.55.32.10            Et0              11 03:31:40  10  200  0  40
```

Hình 3.2.4.a. *Bảng láng giềng của EIGRP*

Sau đây là các thông tin trong bảng láng giềng:

- Địa chỉ của router láng giềng.
- **Hold time**: Là khoảng thời gian lưu giữ. Nếu không nhận được bất kỳ cái gì từ router láng giềng trong suốt khoảng thời gian lưu giữ thì khi khoảng thời gian này hết thời hạn, router mới xem kết nối đến láng giềng đó không còn hoạt động. Ban đầu, khoảng thời gian này chỉ áp dụng cho các gói hello, nhưng ở các phiên bản Cisco IOS hiện nay, bất kỳ gói EIGRP nào nhận được sau gói hello đầu tiên đều khởi động lại đồng hồ đo khoảng thời gian này.
- **Smooth Round □ Trip Timer (SRTT):** Là khoảng thời gian trung bình mà router gửi đi một gói và nhận về một gói từ một router láng giềng. Khoảng thời gian này được dùng để xác định thời gian truyền lại (RTO).
- **Queue count (QCnt):** Là số lượng gói dữ liệu đang xếp trong hàng đợi để chờ được chuyển đi. Nếu phần này luôn có giá trị không đổi lớn hơn 0 thì có thể là router đang bị nghẽn mạch. Nếu phần này có giá trị 0 có nghĩa là không có gói EIGRP nào trong hàng đợi.

- **Sequence number (Seq No):** Là số thứ tự của gói nhận được mới nhất từ router láng giềng. EIGRP sử dụng chỉ số này để xác định gói cần truyền lại với router láng giềng. Bảng láng giềng này được sử dụng để hỗ trợ cho việc gửi đảm bảo tin cậy và tuần tự cho các gói dữ liệu EIGRP, tương tự như TCP thực hiện gửi bảo đảm cho các gói IP vậy.



Hình 3.2.4.b. *Quá trình trao đổi thông tin định tuyến giữa hai router láng giềng với nhau*

3.2.5. Phát hiện đường đi

Các router chạy EIGRP giữ các thông tin về đường đi trên RAM, do đó có thể đáp ứng nhanh chóng. Giống như OSPF, EIGRP lưu các thông tin này thành từng bảng hay từng cơ sở dữ liệu.

DUAL là thuật toán vectơ khoảng cách của EIGRP, nó sử dụng thông tin trong bảng láng giềng và bảng cấu trúc mạng để tính toán đường có chi phí thấp nhất đến mạng đích. Đường chính được chọn ra được gọi là đường successor. Sau khi tính

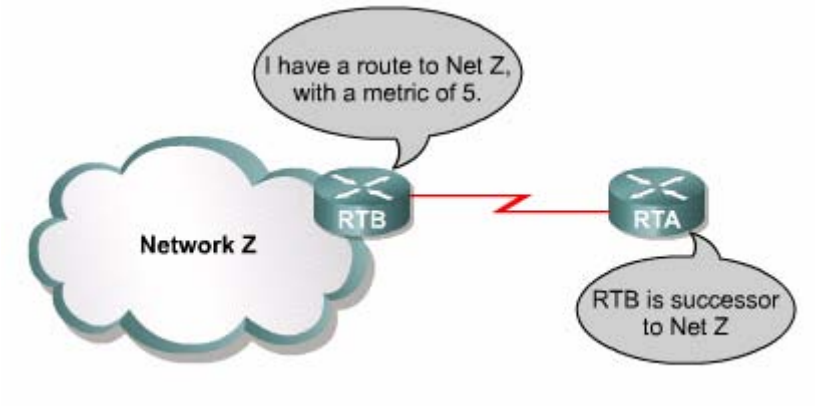
toán, DUAL đặt đường successor lên bảng định tuyến và đồng thời cũng lưu đường này trong bảng cấu trúc mạng.

DUAL còn cố gắng tính đường dự phòng cho trường hợp đường successor bị đứt. Đường dự phòng này được gọi là đường feasible successor. DUAL chỉ lưu đường feasible successor trong bảng cấu trúc mạng. Đường này sẽ được sử dụng thay thế khi đường successor đến mạng đích bị đứt hoặc không bảo đảm tin cậy.

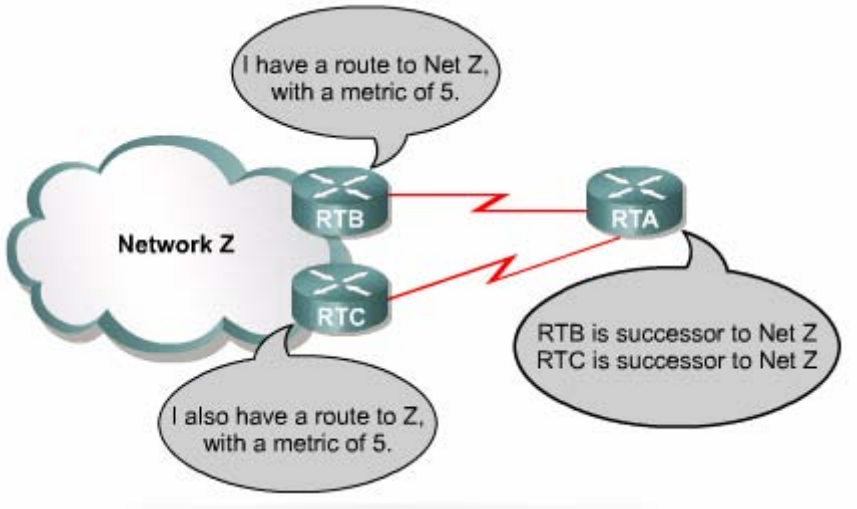
3.2.6. Chọn đường

Nếu có một đường đi đến một mạng đích bị đứt, DUAL sẽ tìm feasible succesor trong bảng cấu trúc mạng để thay thế. Nếu không tìm được feasible successor thì con đường đến mạng đích đó được đánh dấu trạng thái Active. Sau đó, router gửi gói yêu cầu đến tất cả các router láng giềng để yêu cầu cung cấp thông tin về mạng đích đang cần xử lý. DUAL sử dụng các thông tin mới nhận được để tính toán lại successor và feasible successor mới.

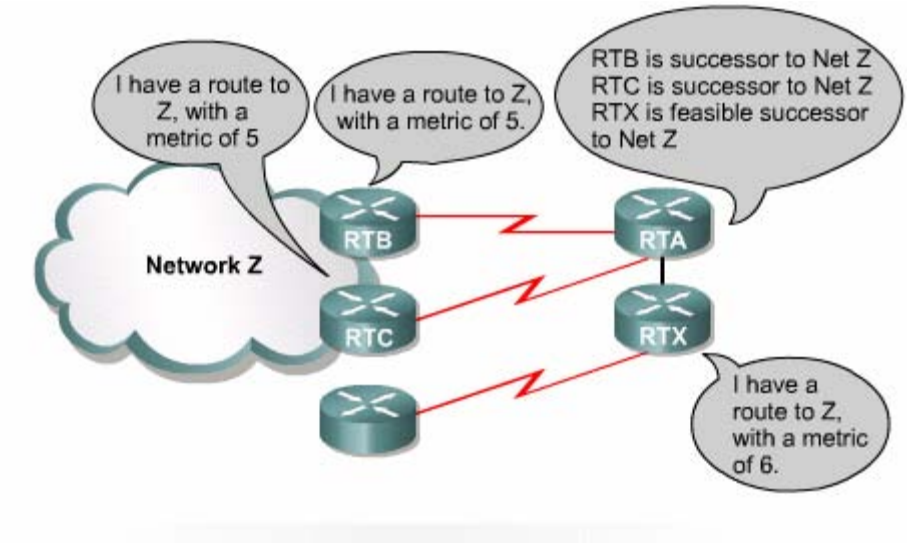
Sau khi DUAL hoàn tất việc tính toán, đường successor được đưa lên bảng định tuyến. Đường successor và feasible successor được lưu trong bảng cấu trúc mạng. Con đường đến mạng đích trên được chuyển từ trạng thái Active sang trạng thái Pasive. Trạng thái này có nghĩa là con đường đến mạng đích đó đã hoạt động và bảo đảm tin cậy.



Hình 3.2.6a. *Đường successor là đường có chi phí thấp nhất đến một mạng đích. Successor là router kế tiếp trên đường đi này*



Hình 3.2.6.b. *RTA có thể cài đặt nhiều đường successor nếu chúng có cùng chi phí*



Hình 3.2.6.c. *Bằng cách xác định đường feasible succesor, EIGRP router có thể tìm được đường thay thế ngay khi đường successor bị đứt.*

3.2.7. Bảo trì bảng định tuyến

DUAL ghi nhận tất cả các đường do láng giềng quảng cáo và sử dụng thông số định tuyến tổng hợp để so sánh giữa chúng. Đồng thời DUAL cũng đảm bảo mỗi đường đi này không bị lặp vòng.

Đường đến một đích có chi phí thấp nhất sẽ được DUAL đưa lên bảng định tuyến. Đường này gọi là đường successor. Đường successor cũng được lưu trong bảng cấu trúc mạng.

EIGRP lưu các thông tin quan trọng về đường đi trong bảng láng giềng và bảng cấu trúc mạng. Hai bảng này cung cấp thông tin đầy đủ cho DUAL. Dựa vào đó DUAL có thể chọn đường thay thế nhanh chóng khi cần thiết.

Khi một đường liên kết bị đứt, DUAL tìm feasible successor trong bảng cấu trúc mạng. Nếu không tìm thấy feasible successor thì đường đi đến mạng đích này được đánh dấu trạng thái Active. Sau đó router gửi gói yêu cầu đến tất cả các router láng giềng của nó để yêu cầu cung cấp thông tin mạng. Với thông tin mới nhận được, DUAL sẽ tính toán lại đường successor và feasible successor mới.

Sau khi DUAL đã tính toán xong, đường successor được đưa vào bảng định tuyến. Đường successor và feasible successor được đặt trong bảng cấu trúc mạng. Trạng thái của con đường đến mạng đích này được chuyển từ Active sang Passive. Trạng thái này có nghĩa là con đường đã hoạt động tin cậy.

EIGRP router sử dụng các gói hello rất nhỏ để thiết lập mối quan hệ thân mật với các router láng giềng. Mặc định, gói hello được gửi theo chu kỳ 5 giây/lần. Nếu EIGRP router vẫn nhận được đều đặn các gói hello theo định kỳ thì có nghĩa là láng giềng đó cùng với các con đường của nó vẫn còn hoạt động bình thường.

Khi phát hiện một láng giềng mới, router sẽ ghi nhận lại địa chỉ và cổng kết nối của láng giềng đó. Thông tin này được lưu trong bảng láng giềng. Khi router láng giềng gửi gói hello, trong đó có thông số về khoảng thời gian lưu giữ. Đây là khoảng thời gian mà router vẫn chờ và xem là router láng giềng vẫn còn hoạt động và kết nối lại được. Hay nói cách khác, nếu router không nhận được gói hello trong suốt khoảng thời gian lưu giữ thì khi khoảng thời gian này kết thúc, router láng giềng xem như không kết nối được nữa hoặc không còn hoạt động nữa. DUAL sẽ thông báo sự thay đổ này và thực hiện tính toán lại với cấu trúc mạng mới.

3.3. Xử lý sự cố giao thức định tuyến

3.3.1. Quá trình xử lý sự cố giao thức định tuyến

Tất cả các quá trình xử lý sự cố giao thức định tuyến đều nên tuân theo một sơ đồ logic tuần tự. Sơ đồ này không phải là một tiến trình bắt buộc cứng nhắc khi xử lý sự cố mạng. Tuy nhiên, nó là một sơ đồ cơ bản để từ đó người quản trị mạng có thể xây dựng một sơ đồ xử lý sự cố phù hợp cho môi trường mạng của mình.

1. Khi khảo sát sự cố mạng, cố gằng làm rõ những mô tả về sự cố.

- Xác định sự cố dựa trên một loạt các hiện tượng và các nguyên nhân có thể gây ra.
- Để phân tích đúng sự cố, bạn xác định các dấu hiện chung và sau đó xác định xem nguyên nhân nào có thể gây ra các hiện tượng như vậy. Ví dụ: host không trả lời dịch vụ khi được yêu cầu từ client, đó là một hiện tượng.
- Những nguyên nhân có thể là cấu hình host bị thiếu, giao tiếp card bị hỏng hoặc thiếu lệnh cấu hình trên router.

2. Xác định nguyên nhân gây ra sự cố

- Thu nhập các sự kiện cần thiết để giúp cho bạn xác định nguyên nhân có thể gây ra sự cố. Hỏi những người dùng bị ảnh hưởng bởi sự cố, hỏi người quản lý, người quản trị mạng và một số người quan trọng khác.
- Thu nhập thông tin từ nhiều nguồn, ví dụ như hệ thống quản lý mạng giao thức phân tích mạng, kết quả hiển thị của một số lệnh khảo sát router hoặc từ các ghi chú của phiên bản phần mềm đang sử dụng.

3. Dựa trên những thông tin đã thu thập được, chúng ta tập trung chú ý vào các nguyên nhân có thể.

- Với các thông tin thu thập được bạn có thể loại trừ một số nguyên nhân. Ví dụ: dựa trên các thông tin này, bạn có thể loại trừ sự cố phần cứng để tập trung vào sự cố phần mềm.
- Trong mọi trường hợp, cố gắng thu nhỏ số lượng nguyên nhân có khả năng gây ra sự cố để chúng ta có thể lên một phương án xử lý hiệu quả.

4. Lên phương án hành động theo các nguyên nhân có khả năng còn lại.

- Bắt đầu với nguyên nhân có khả năng nhiều nhất, bạn đặt ra một phương án trong đó chỉ thay đổi một thông số mạng.

- Chỉ thay đổi một thông số tại một thời điểm. Điều này giúp cho bạn xác định được giải pháp cho từng sự cố cụ thể. Không nên cố thay đổi nhiều hơn một thông số tại một thời điểm. Làm như vậy có thể sẽ giải quyết được sự cố nhưng bạn lại không thể biết được cái nào bạn thay đổi đã giải quyết được hiện tượng nào và như vậy bạn sẽ không rút được kinh nghiệm cho những lần xảy ra sự cố tương tự về sau.

5. Thực hiện phương án đã đưa ra, thực hiện từng bước một cách cẩn thận đồng thời kiểm tra xem các hiện tượng của sự cố đã hết chưa.
6. Khảo sát kết quả để xác nhận là sự cố đã được giải quyết hay chưa. Nếu sự cố đã được giải quyết xong thì quá trình của chúng ta chấm dứt.
7. Nếu sự cố vẫn còn, bạn lên phương án cho nguyên nhân có khả năng cao thứ hai. Quay lại bước 4, thay đổi một thông số khác và lặp lại quá trình cho đến khi giải quyết được sự cố.
8. Một khi nguyên nhân thật sự của sự cố đã được xác định, cố gắng xử lý nó.

- Điều quan trọng ở bước này là ghi lại sự cố và giải pháp tương ứng để có thể sử dụng sau này.
- Nếu đến bước này mà mọi cố gắng vẫn không thành công thì bạn nên yêu cầu hỗ trợ kỹ thuật từ nhà sản xuất thiết bị.
- Một số nguồn hỗ trợ khác có thể giúp cho bạn là các chuyên gia hoặc các kỹ sư về kỹ thuật.
- Cisco router có một số tập lệnh hỗ trợ cho bạn theo dõi và xác định sự cố mạng:
- Tập lệnh **show** cho phép bạn theo dõi các hoạt động bình thường của mạng, giúp bạn khoanh vùng khu vực xảy ra sự cố.
- Tập lệnh **debug** hỗ trợ cho bạn xác định sự cố của giao thức và của cấu hình router.
- Các công cụ TCP/IP như ping, traceroute và telnet.

Tập lệnh **show** là công cụ quan trọng nhất giúp bạn hiểu được trạng thái hoạt động của router, xác định các router láng giềng, theo dõi hoạt động tổng quát và khoanh vùng sự cố mạng.

Tập lệnh **debug** cung cấp các thông tin sống về giao thông trên một cổng, các thông điệp báo lỗi bên trong, phân tích các gói dữ liệu của một giao thức nào đó và nhiều thông tin khác có ích. Chúng ta chỉ dùng lệnh **debug** để xác định sự cố chứ không dùng nó để xem các hoạt độngbình thường của mạng. Chỉ sử dụng **debug** để tìm một giao thông đặc biệt nào đó hay một sự cố nào đó. Bạn nên thu hẹp các nguyên nhân gây ra sự cố trước khi sử dụng lệnh **debug**. Bạn dùng lệnh **show debugging** để xem những **debug** nào đang được bật lên trong router.

Sử dụng tập lệnh show của Cisco IOS cho các công việc sau:

- Xem các đáp ứng của router trong quá trình cài đặt.
- Xem hoạt động bình thường của mạng.
- Xác định sự cố trên cổng giao tiếp, trên máy tinh hay trên một ứng dụng nào.
- Xác định khi nào mạng nghẽn mạch.
- Xác định trạng thái của server, client hoặc các láng giềng.

Các công cụ mạng TCP/IP:

- Lệnh ping mở rộng có thể điều khiển tốt hơn lệnh ping cơ bản.
- Ping kiểm tra nhanh tính kết nối từ đầu cuối - đến — đầu cuối.
- Traceroute có thể được sử dụng để xác định kết nối nào bị nghẽn mạch hay bị đứt.
- Telnet được sử dụng để kiểm tra một kết nối hoạt động hoàn chỉnh từ đầu cuối - đến - đầu cuối.

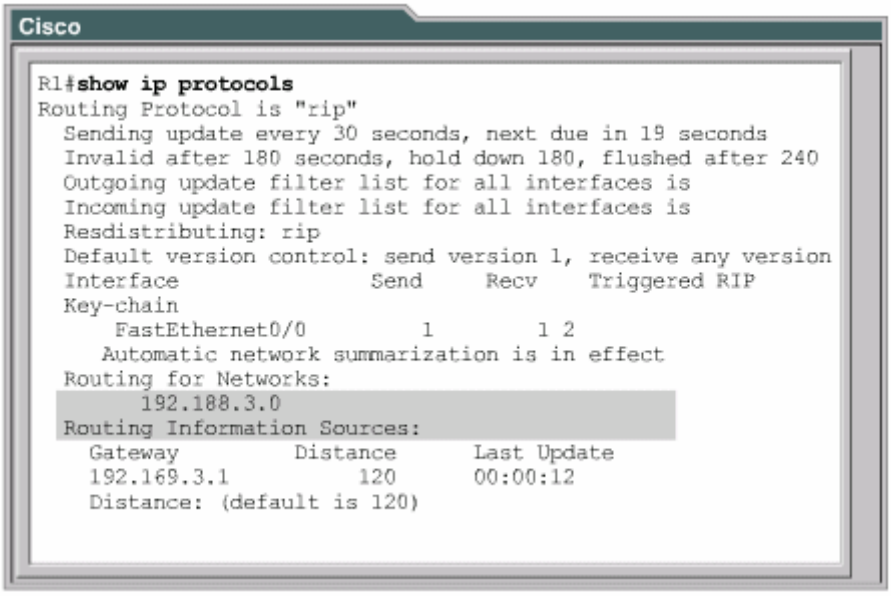
3.3.2. Xử lý sự cố cấu hình RIP

Sự cố thường gặp nhất của RIP làm cho RIP không thực hiện quảng cáo về một đường nào đó là do VLSM (Variable — length subnet mask). RIP phiên bản 1 không hỗ trợ VLSM. Do đó khi RIP không quảng cáo về một đường nào đó, bạn nên kiểm tra những điều sau:

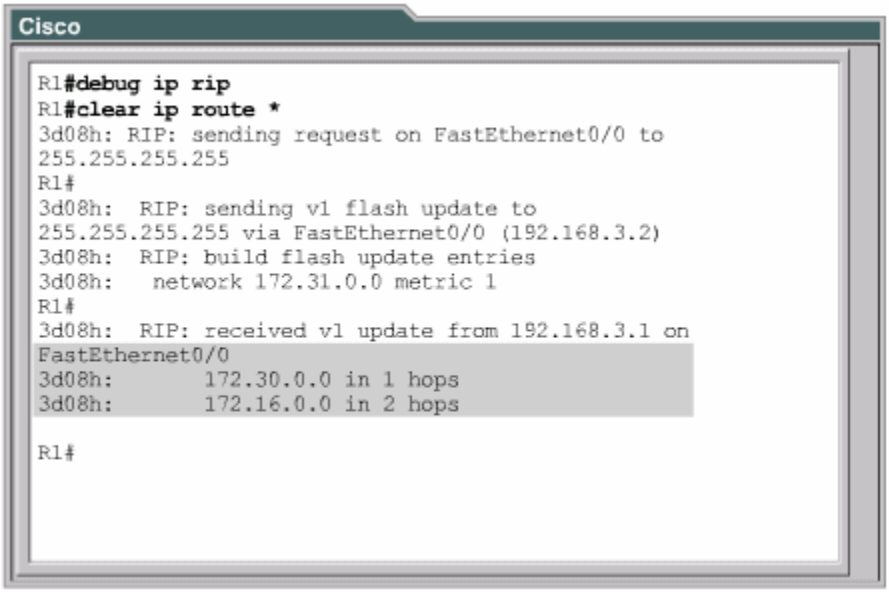
- Có sự cố về kết nối ở Lớp 1 hoặc Lớp 2 hay không.
- Có cấu hình địa chỉ IP theo sơ đồ VLSM hay không. VLSM không thể sử dụng được với RIPv1.
- Cấu hình RIPv1 và RIPv2 có phù hợp với nhau hay không.
- Câu lệnh **network** có bị thiếu hay bị sai không.
- Cổng giao tiếp trên router có hoạt động tốt không.

Lệnh **show ip protocols** cung cấp các thông tin về đặc điểm và trạng thái hiện tại của các giao thức định tuyến đang hoạt động trên router. RIP gửi thông tin định tuyến ra các cổng giao tiếp có địa chỉ IP nằm trong địa chỉ mạng được khai báo trong câu lệnh **network**. Ví dụ: nếu bạn đã cấu hình xong cổng FastEtherrnet 0/1 nhưng bạn không khai báo địa chỉ mạng của cổng này cho RIP bằng lệnh **network** thì RIP sẽ không gửi thông tin định tuyến ra cổng đó và đồng thời cũng không nhận thông báo này từ cổng này.

Bạn có thể dùng lệnh **debug ip rip** để xem các thông tin tức thời về hoạt động của RIP. Sau đó bạn dùng lệnh **no debug ip rip**, **no debug all** hoặc **undebug all** để tắt debug.



Hình 3.3.2.a. *Ví dụ kết quả hiển thị của lệnh show ip protocols*



Hình 3.3.2.b. *Ví dụ hiển thị của lệnh debug ip rip*

Ví dụ trong hình 3.3.2.b, router R1 đang nhận thông tin cập nhật từ một router khác có địa chỉ là 192.168.3.1. Router này gửi thông tin về hai mạng đích là 172.30.0.0 và 172.16.0.0. Router R1 cũng gửi thông tin cập nhật của nó ra cổng FastEthernet 0/0. Cả hai router đều sử dụng địa chỉ quảng bá 255.255.255.255 làm địa chỉ đích

cho các gói thông tin định tuyến của mình. Chỉ số trong ngoặc () là địa chỉ nguồn được đóng gói trong phần IP header.

Bạn có thể sẽ gặp câu thông báo như sau khi router nhận được một gói không đúng dạng chuẩn:

RIP: bad version 128 from 160.89.80.43

3.3.3. Xử lý sự cố cấu hình IGRP

IGRP là một giao thức định tuyến theo vectơ khoảng cách được phát triển bởi Cisco từ giữa thập niên 80. IGRP có nhiều đặc điểm khác với các giao thức định tuyến theo vectơ khoảng cách như RIP chẳng hạn. Các đặc điểm này được liệt kê trong bảng 3.3.3.

Đặc điểm	**Giải thích**
Khả năng mở rộng tăng	IGRP có khả năng định tuyến cho mạng có kích thước lớn hơn nhiều sơ với mạng sử dụng RIP.
Thông số định tuyến phức tạp	IGRP sử dụng thông số định tuyến tổng hợp để chọn đường linh hoạt hơn. Các yếu tố tác động vào việc chọn đường là băng thông, độ trễ, độ tải và độ tin cậy. Mặc định, thông số định tuyến chỉ bao gồm băng thông và độ trễ. IGRP khắc phục được giới hạn 15 hop của RIP. IGRP có giá trị hop tối đa mặc định là 100 nhưng bạn có thể cấu hình cho giá trị này lên tới 255.
Chia tải ra nhiều đường	IGRP có thể duy trì tới 6 đường khác nhau giữa một cặp nguồn và đích. Những đường này giữa một cặp nguồn và đích. Những đường này không bắt buộc phải có chi phí bằng nhau như đối với RIP. Việc sử dụng nhiều đường cho cùng một đích như vậy sẽ tăng được băng thông đường truyền hoặc có thể để dự phòng

Bảng 3.3.3

Bạn dùng lệnh **router igrp autonomous-system** để khởi động tiến trình định tuyến IGRP trên router như sau:

R1 (config)**#router igrp 100**

Sau đó, bạn dùng lệnh **network network-number** để khai báo các địa chỉ của các cổng trên router tham gia vào quá trình cập nhật IGRP.

R1 (config-router)#network 172.30.0.0

R1 (config-router)#network 192.168.3.0

Bạn dùng các lệnh sau để kiểm tra cấu hình và hoạt động của IGRP:

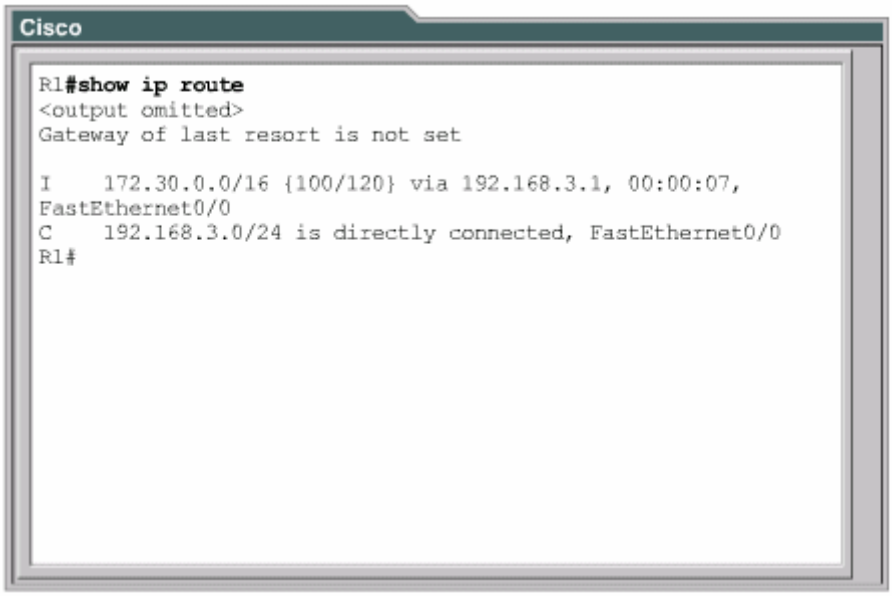
R1**#show ip protocols**

R1**#show ip route**

Cisco

```
R1#show ip protocols
Routing Protocol is "igrp 100"
  Sending update every 90 seconds, next due in 58 seconds
  Invalid after 270 seconds, hold down 280, flushed after 630
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  IGRP maximum hopcount 100
  IGRP maximum metric variance 1
  Redistributing: igrp 100
  Routing for Networks:
        172.30.0.0
        192.168.3.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.3.2          100      00:00:11
    Distance: (default is 100)
R1#
```

Hình 3.3.3.a



Hình 3.3.3.b

3.3.5.Xử lý sự cố cấu hình OSPF

OSPF là 1 giao thức định tuyến theo trạng thái đường liên kết.Một liên kết tương ứng với một cổng giao tiếp trên một router.Trạng thái của một đường liên kết bao gồm thông tin về cổng giao tiếp và mối quan hệ với các router láng giềng kết nối vào cổng đó.Ví dụ : thông tin về một cổng giao tiếp bao gồm địa chỉ IP ,subnet mask và loại mạng kết nối vào cổng đó cũng như các router kết nối vào cổng này.Tập hợp các thông tin như vậy tạo thành cơ sở dữ liệu về trạng thái các đường liên kết.

-Sự cố thường xảy ra với OSPF có liên quan tới quan hệ với các láng giềng thân mật và việc đồng bộ cơ sở dữ liệu về trạng thái các đường liên kết.Lệnh show ip ospf neighbors sẽ cung cấp nhiều thông tin hữu ích cho việc xử lý sự cố liên quan đến việc quan hệ với các router láng giềng thân mật.

-Bạn sử dụng lệnh debug ip ospf events để hiển thị thông tin về các sự kiện liên quan đến OSPF như:

+Mối quan hệ láng giềng thân mật.

+Gửi thông tin định tuyến

+Bầu router đại diện(DR)

+Tính toán chọn đường ngắn nhất(OSPF)

-Nếu router đã được cấu hình định tuyến OSPF mà không thấy được các láng giềng OSPF trên những mạng kết nối trực tuyến của nó thì bạn nên thực hiện các việc sau:

+Kiểm tra xem cả hai router láng giềng với nhau đã được cấu hình IP có cùng subnet mask ,cùng khoảng thời gian hello và khoảng thời gian bất động hay chưa.

+Kiểm tra xem cả hai router láng giềng của nhau có nằm trong cùng một vùng hay không.

Để hiển thị thông tin về mỗi gói OSPF nhận được ,bạn dùng lệnh debug ip ospf packet.Dùng dạng no của câu lệnh này để tắt debug.

Lệnh debug ip ospf packet sẽ hiển thị các thông tin của từng gói OSPF mà router nhận được.Thông tin hiển thị thay đổi một chút tuỳ theo loại cơ chế xác minh đang được sử dụng.

TỔNG KẾT

Sau khi đọc xong chương này ,bạn phải trả lời được các câu hỏi sau:

1. EIGRP là một giao thức lai,kết hợp các ưu điểm của giao thức định tuyến theo vectơ khoảng cách và giao thức định tuyến theo trạng thái đường liên kết.Vậy EIGRP giống giao thức định tuyến theo vectơ khoảng cách ở những điểm nào? Và giống giao thức định tuyến theo trạng thái đường liên kết ở những điểm nào?
2. Bảng cấu trúc mạng của EIGRP và cơ sở dữ liệu về cấu trúc mạng của OSPF khác nhau như thế nào?

Sau đây là những điểm quan trọng trong chương này:

+Điểm khác nhau giữa EIGRP và IGRP

+Các khái niệm chính,kỹ thuật chính và cấu trúc dữ liệu của EIGRP

+Hoạt động hội tụ của EIGRP và hoạt động cơ bản của DUAL

+Cấu hình IEGRP cơ bản

+Cấu hình tổng hợp đường đi cho IEGRP

+Quá trình EIGRP xây dựng và bảo trì bảng định tuyến

+Kiểm tra hoạt động EIGRP

+Tám bước cho quá trình xử lý sự cố nói chung

+Áp dụng sơ đồ logic trên vào quá trình xử lý sự cố định tuyến

+Xử lý sự cố tiến trình định tuyến RIP sử dụng lệnh show và debug.

+Xử lý sự cố tiến trình định tuyến IGRP sử dụng lệnh show và debug

+Xử lý sự cố tiến trình định tuyến EIGRP sử dụng lệnh show và debug

+Xử lý sự cố tiến trình định tuyến OSPF sử dụng lệnh show và debug

CHƯƠNG 4: CÁC KHÁI NIỆM VỀ CHUYỂN MẠCH

GIỚI THIỆU

Việc thiết kế LAN được phát triển và thay đổi nhiều theo thời gian.Cho đến gần đây các nhà thiết kế mạng vẫn còn sử dụng hub,bridge để xây dựng hệ thống mạng.Còn hiện nay ,switch và router là hai thiết bị quan trọng nhất trong LAN,khả năng và hoạt động của hai loại thiết bị này không ngừng được năng cao.

Chương này sẽ quay lại một số nguồn gốc của các phiên bản Ethernet LAN,thảo luận về sự phát triển của Ethernet/802.3 và cấu trúc phát triển nhất của LAN.Một cái nhìn về hoàn cảnh lịch sử của sự phát triển LAN và các thiết bị mạng khác nhau làm việc ở lớp 1, lớp 2, lớp 3 của mô hình OSI sẽ giúp chúng ta hiểu rõ hơn tại sao các thiết bị mạng đã được phát triển như vậy.

Cho đến gần đây hầu hết các mạng Ethernet vẫn còn được sử dụng Repeater. Khi hiệu quả hoạt động của các mạng này trở nên xấu đi vì có quá nhiều thiết bị cùng chia sẻ một môi trường truyền thì các kỹ sư mạng mới lắp thêm Bridge để chia mạng thành nhiều miền đụng độ mạng nhỏ hơn. Khi hệ thống mạng càng phát triển lớn hơn và phức tạp hơn, Bridge được phát triển thành Switch như bây giờ, cho phép phân đoạn cực nhỏ hệ thống mạng. Các mạng ngày nay được xây dựng dựa trên Switch và router, thậm chí có thiết bị bao gồm cả hai chức năng định tuyến và chuyển mạch.

Switch hiện đại có khả năng thực hiện nhiều nhiệm vụ phức tạp khác nhau trong mạng. Chương này sẽ giới thiệu về cách phân đoạn mạng và mô tả hoạt động cơ bản của Switch.

Switch là thiết bị Lớp 2 được sử dụng để tăng băng thông và giảm nghẽn mạch. Một Switch có thể phân mạng LAN thành các đoạn siêu nhỏ, là những đoạn mạng chỉ có Host. Nhờ vậy một miền lớn được chia thành nhiều miền nhỏ ko có đụng độ.Là một thiết bị ở lớp 2 nên LAN Switch có thể tạo được nhiều miền đụng độ nhưng tất cả các Host kết nối vào Switch vẫn nằm trong cùng một miền quảng bá.

Sau khi hoàn tất chương này các bạn có thể thực hiện các việc sau:

+ Mô tả lịch sử và chức năng của Ethernet chia sẻ,bán song công

+ Định nghĩa đụng độ trong mạng Ethernet

+ Định nghĩa phân đoạn cực nhỏ (microsegment)

+ Định nghĩa CSMA/CD

+ Mô tả một số thành phần quan trọng ảnh hưởng đến hiệu quả hoạt động của mạng

+ Mô tả chức năng của Repeater

+ Định nghĩa độ trễ mạng

+ Định nghĩa thời gian truyền

+ Mô tả chức năng cơ bản của Fast Ethernet

+ Xác định đoạn mạng sử dụng Router,Switch và Bridge

+ Mô tả hoạt động cơ bản của Switch

+ Định nghĩa độ trễ của Ethernet Switch

+ Giải thích sự khác nhau giữa chuyển mạch lớp 2 và lớp 3

+ Định nghĩa chuyển mạch đối xứng và bất đối xứng

+ Định nghĩa bộ nhớ hàng đợi

+ So sánh và phân biệt giữa chuyển mạch store-and-forward và cut-through

+ Hiểu được sự khác nhau giữa Hub,Bridge,Switch

+ Mô tả chức năng chính của Switch

+ Liệt kê các chế độ chuyển gói chính của Switch

+ Xác định đoạn mạng LAN

+ Xác định đoạn mạng cực nhỏ sử dụng Switch

+ Mô tả tiến trình lọc tải

+ So sánh và phân biệt miền đụng độ và miền quảng bá

+ Xác định loại cáp cần thiết để kết nối máy trạm vào Switch

+ Xác định loại cáp cần thiết để kết nối Switch vào Switch

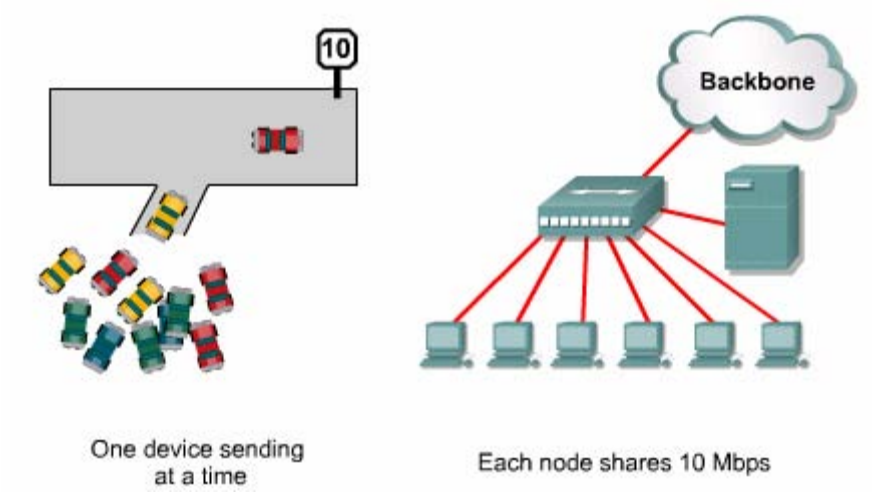
4.1. Giới thiệu Ethernet/802.3 LAN

4.1.1. Sự phát triển của Ethernet/802.3 LAN

- Kỹ thuật LAN đầu tiên sử dụng cấu trúc "thick Ethernet" và "Thin Ethernet". Nắm được các giới hạn của 2 loại cấu trúc này là rất quan trọng để thấy được vị trí của chuyển mạch LAN ngày nay.

- Thêm HUB hay còn gọi là bộ tập trung vào mạng là một cải tiến dựa trên kỹ thuật "thick" và "thin" Ethernet. Hub là thiết bị lớp 1 và đôi khi được coi là một bộ tập trung Ethernet hay Repeater đa port. Sử dụng Hub trong mạng cho phép kết nối được nhiều user hơn. Loại Hub chủ động còn cho phép mở rộng khoảng cách của mạng vì nó thực hiện tái tạo lại tín hiệu dữ liệu.Hub ko hề có quyết định gì đối với tín hiệu dữ liệu mà nó nhận được. Nó chỉ đơn giản là khuếch đại và tái tạo lại tín hiệu mà nó nhận được và chuyển ra cho tất cả các thiết bị nối vào nó.

- Ethernet cơ bản là kỹ thuật chia sẻ cùng 1 băng thông cho mọi người dùng trong 1 phân đoạn LAN. Điều này giống như một xe hơi cùng chạy vào một làn đường vậy. Con đường này chỉ có một làn đường nên tại một thời điểm chỉ có 1 xe hơi chạy trên đó mà thôi. Các user kết nối và cùng một Hub chia sẻ băng thông trên cùng một đường truyền.



Hình 4.1.1.a.Kết nối user dùng Hub.Các user trên cùng một Hub truy suất cùng một băng thông đường truyền cũng giống như nhiều xe hơi cùng rẽ vào một làn đường vậy.Con đường này chỉ có một làn đường nên tại một thời điểm chỉ được một xe rẽ mà thôi.

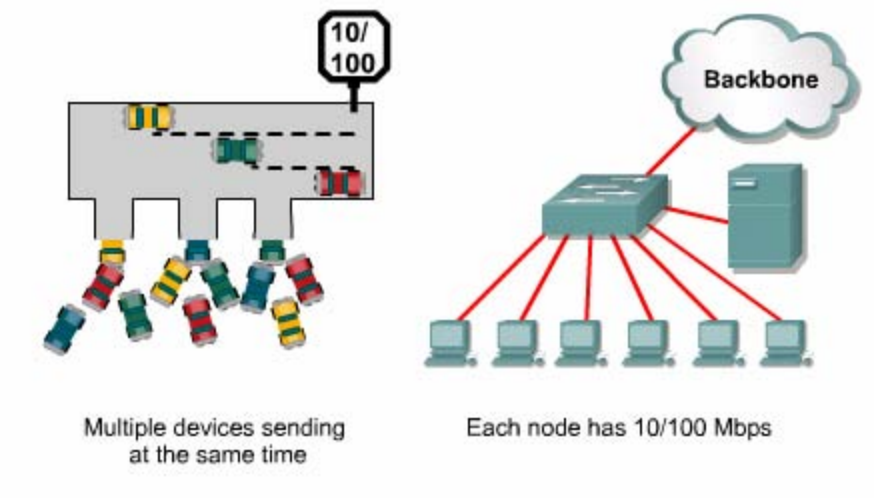
- Đụng độ là một hậu quả tất yếu của mạng Ethernet. Nếu có hai hay nhiều thiết bị cùng truyền cùng một lúc thì đụng độ sẽ xảy ra. Điều này cũng giống như 2 xe cùng tranh giành một làn đường và xảy ra đụng độ. Khi đụng độ xảy ra mọi giao thông trên đường truyền đó sẽ bị ngưng lại cho đến khi sự đụng độ đã được vãn hồi. Khi số lượng đụng độ quá lớn, thời gian đáp ứng của hệ thống mạng sẽ rất chậm. Tình trạng này cho thấy mạng bị nghẽn mạch hoặc có quá nhiều user truy cập cùng lúc vào mạng.

- Thiết bị lớp 2 thông minh hơn thiết bị lớp 1. Thiết bị lớp 2 có quyết định chuyển gói dựa trên địa chỉ MAC (Media access Control) được ghi trong phần đầu của gói.

- Bridge là 1 thiết bị lớp 2 được sử dụng để phân đoạn mạng. Bridge thu thập và chon lựa dữ liệu để chuyển mạch giữa hai đoạn mạng bằng cách học địa chỉ MAC của tất cả các thiết bị nằm trong từng đoạn mạng kết nối vào nó. Dựa vào các địa chỉ MAC, Bridge xây dựng thành bảng chuyển mạch và theo đó để chuyển hoặc chặn gói lại. Nhờ vậy Bridge tách 1 mạng thành nhiều miền đụng độ nhỏ hơn,làm tăng hiệu quả hoạt động của mạng. Tuy nhiên Bridge ko chặn các lưu lượng quảng bá nhưng dù sao thì Bridge cũng điều khiển lưu lượng mạng tốt hơn Hub.

- Switch cũng là 1 thiết bị lớp 2 và được xem là Bridge đa port. Switch có thể quyết định chuyển 1 gói dựa trên địa chỉ MAC được ghi trong gói đó. Switch học địa chỉ MAC của các thiết bị kết nối trên từng port của nó và xây dựng thành bảng chuyển mạch

-Khi hai thiết bị kết nối vào Switch thực hiện trao đổi với nhau, Switch sẽ thiết lập một mạch ảo cung cấp một đường liên lạc riêng giữa hai thiết bị này. Switch có khả năng phân đoạn mạng cực nhỏ, nghĩa là tạo ra môi trường ko đụng độ giữa nguồn và đích,nhờ đó tối đa hoá lượng băng thông khả dụng. Switch có thể tạo nhiều mạch ảo đồng thời giữa các cặp thiết bị khác nhau. Hình ảnh này tương tự như đường cao tốc có thể chia thành nhiều làn đường và mỗi xe có riêng một làn đường cho mình.



Hình 4.1.1.b Kết nối user bằng Switch.Có bao nhiêu thiết bị kết nối vào Switch thf Switch có thể tạo ra bấy nhiêu mạch ảo cho từng thiết bị. Điều này giống như hình minh hoạ về đường cao tốc ở bên trái. Đường cao tốc này có đủ 3 làn đường dành cho 3 nhánh đổ vào nó,mỗi nhánh một làn đường riêng.

- Khuyết điểm của thiết bị lớp 2 là nó chuyển gói quảng bá cho tất cả các thiết bị trong mạng kết nối vào nó.Khi số lượng quảng bá quá nhiều sẽ làm cho thời gian đáp ứng của mạng rất chậm.

- Router là một thiết bị ở lớp 3.Router quyết định chuyển gói dựa trên địa chỉ mạng của gói dữ liệu.Router sử dụng bảng định tuyến để ghi lại địa chỉ lớp 3

của các mạng kết nối trực tiếp vào router và các mạng mà router học được từ các router láng riềng.

- Mục tiêu của router là thực hiện các việc sau:

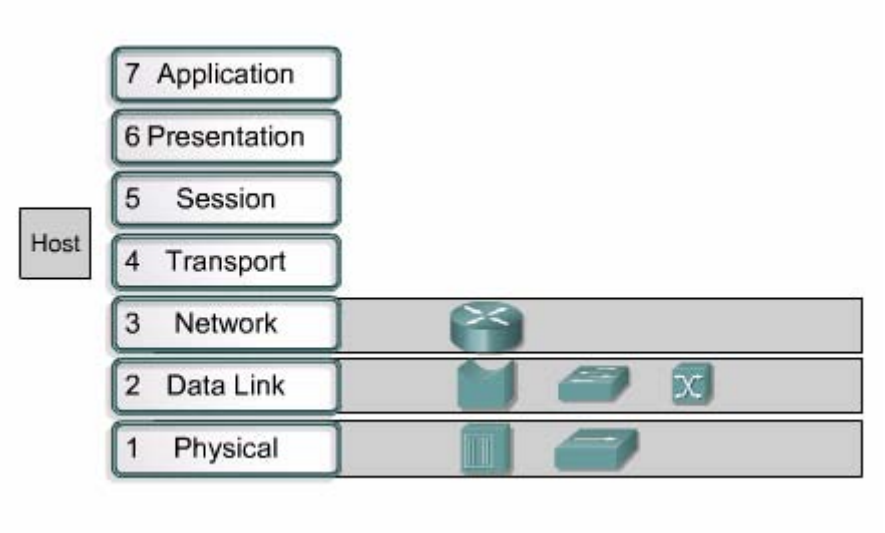
+ Kiểm tra dữ liệu lớp 3 của gói nhận được

+ Chọn đường tốt nhất cho gói dữ liệu

+ Chuyển mạch gói ra cổng tương ứng

- Router ko bị bắt buộc phải chuyển các gói quảng bá. Do đó router có thể làm giảm kích thước miền đụng độ và miền quảng bá trong mạng. Router là thiết bị phân luồng lưu lượng quan trọng nhất trong hệ thống mạng lớn. Chúng giúp cho bất kỳ máy tính nào cũng có thể thông tin liên lạc với bất kỳ máy tính nào khác ở bất cứ đâu trên thế giới.

- LAN kết hợp hoạt động của cả hai thiết bị lớp 1 và lớp 2 và lớp 3. Việc triển khai các thiết bị này như thế nào phụ thuộc vào điều kiện và hoàn cảnh đặc biệt của từng đơn vị tổ chức.



Hinh 4.1.1.c

4.1.2. Các yếu tố ảnh hưởng đến hiệu quả hoạt động của mạng

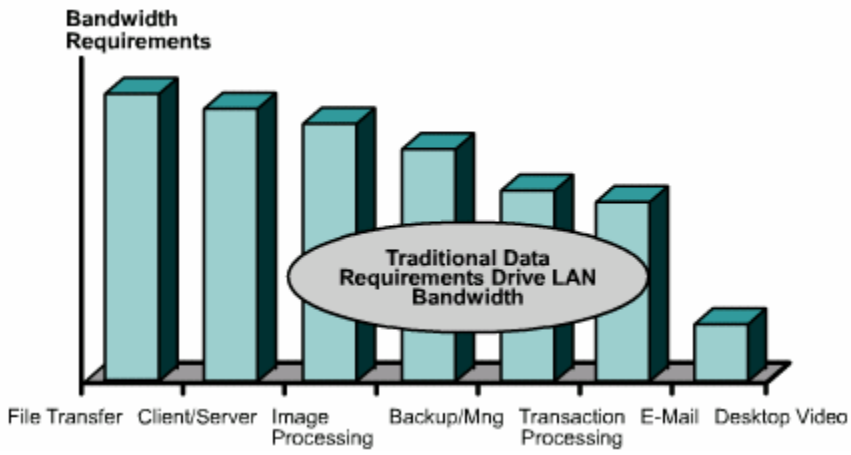
- Mạng LAN ngày nay ngày càng trở nên quá tải và tình trạng nghẽn mạch gia tăng. Thêm vào đó số lượng người dùng mạng tăng lên nhanh chóng cùng với

nhiều yếu tố khác kết hợp lại tạo thành nhiều thử tháchđối với mạng LAN truyền thống.

+Môi trường đa nhiệm hiện nay của các hệ điều hành máy tính như Window, Unix/Linux và MAC cho phép thực hiện đồng thời nhiều phiên giao dịch mạng.Khả năng này càng tăng lên thì yêu cầu về tài nguyên mạng càng tăng.

+Việc sử dụng các ứng dụng chuyên sâu như World Wide Web chẳng hạn gia tăng.Các ứng dụng dạng client/server này cho phép người quản trị mạng có thể tập trung thông tin,dữ liệu lại để dễ bảo trì và bảo vệ dữ liệu.

+Các ứng dụng dạng client/server giải phóng cho các máy trạm gánh nặng của việc lưu trữ dữ liệu và chi phí trang bị đĩa cứng để lưu trữ. Chính vì những ưu điểm này mà việc sử dụng các ứng dụng dạng client/server sẽ càng được sử dụng rộng rãi trong tương lai.



Hình vẽ 4.1.2

+Quá nhiều người trong 1 phân đoạn mạng 10Mbps +Hầu hết mọi người dùng đều truy cập vào 1 hoặc 2 server +Các ứng dụng chuyên ngành như tạo màu, CAD/CAM,xử lý ảnh ,và cơ sở dữ liệu.

4.1.3. Các thành phần của mạng Ethernet/802.3

- Các cấu trúc thông dụng nhất của LAN là Ethernet. Ethernet được dùng để truyền dữ liệu giữa 2 thiết bị trong cùng một mạng nội bộ.Những thiết bị này có thể là máy tính máy in, file server…Tất cả các máy trong cùng một môi trường Ethernet sẽ truyền và nhận dữ liệu theo phương pháp quảng bá. Một số yếu tố sau có thể tác động đến hiệu quả hoạt động của mạng Ethernet/802.3 chia sẻ:

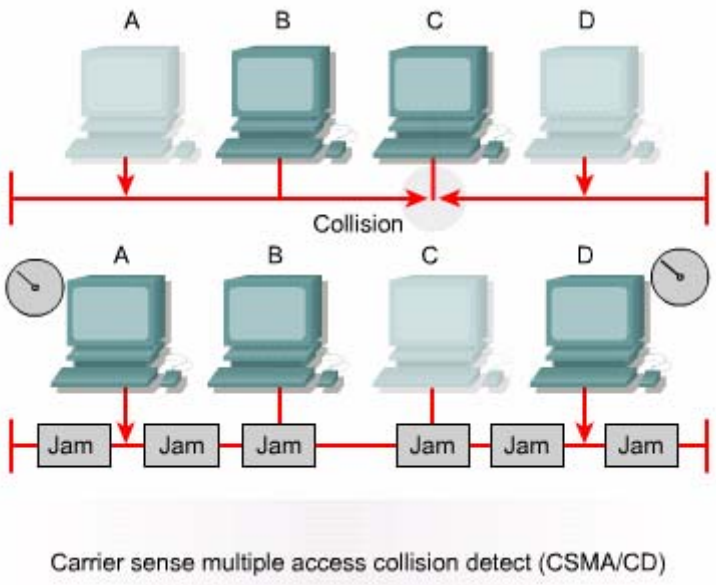
+Việc truyền gói trong mạng Ethernet/802.3 là quảng bá

+Phương pháp đa truy cập cảm nhận sóng mạng phát hiện đụng độ CSMA/CD (carrier sense multiple access/collision detect) chỉ cho phép một máy trạm được truyền tại một thời điểm.

+Nhiều ứng dụng đa truyền thông có yêu cầu băng thông cao như video và internet, cộng với tính chất quảng bá của Ethernet sẽ làm cho mạng nghẽn mạch.

+Thời gian trễ mặc nhiên khi gói di chuyển trên môi trường mạng lớp 1 và đi qua các thiết bị mạng lớp 1 lớp 2 lớp 3.

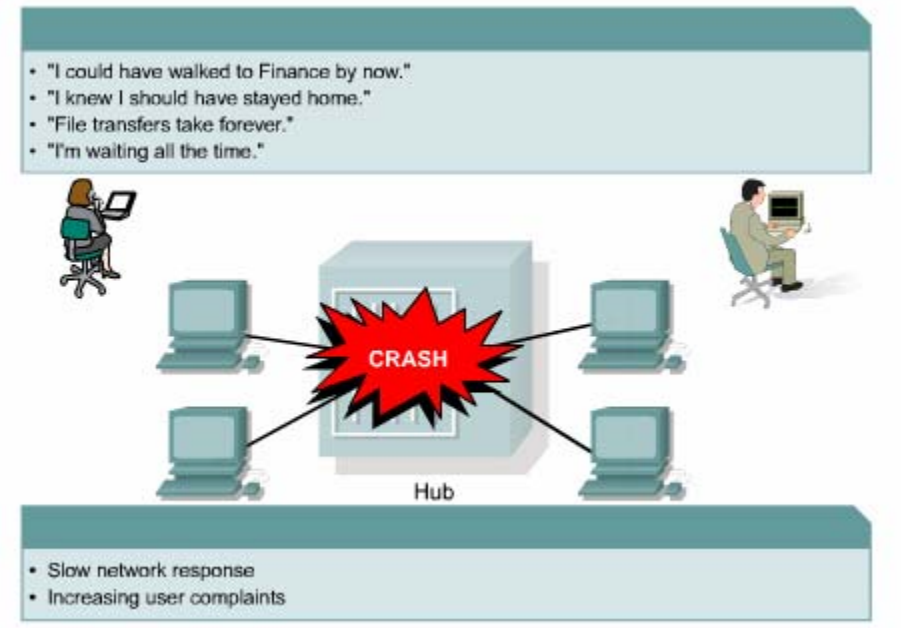
+Sử dụng Repeater để mở rộng khoảng cách và đồng thời cũng làm tăng thời gian trễ của mạng Ethernet/802.3 LAN



Carrier sense multiple access collision detect (CSMA/CD)

Hình 4.1.3.a

-Ethernet sử dụng CSMA/CD và môi trường truyền chia sẻ có thể truyền dữ liệu với tốc độ lên đến 100 Mb/s.CSMA/CD là một phương pháp truy cập cho phép chỉ một máy trạm được truyền dữ liệu tại một thời điểm.Thành công của Ethernet là cung cấp một dịch vụ truyền tổng lực(best-effort) để truyền dữ liệu và cho phép mọi thiết bị trong cùng một môi trường chia sẻ có cơ hội truyền dữ liệu ngang nhau.Tuy nhiên đụng độ là một điều tất yếu trong mạng Ethernet,CSMA/CD



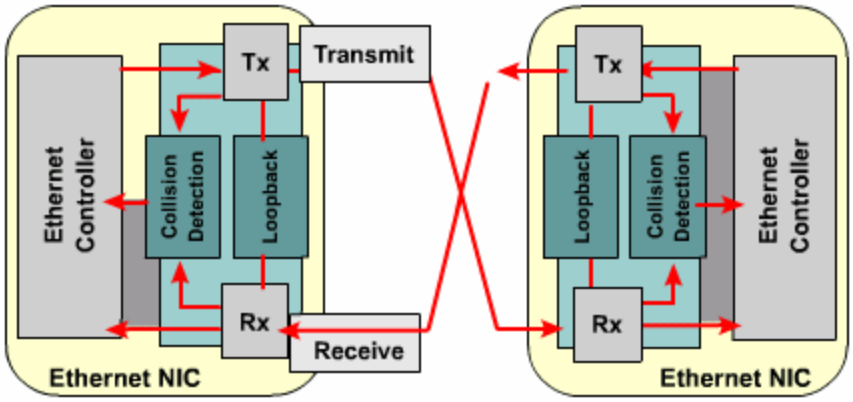
Hình 4.1.3.b

4.1.4.Mạng bán song công

-Ethernet khởi đầu là một kỹ thuật bán song công.Với chế độ truyền bán song công ,host chỉ có thể truyền hoặc nhận tại một thời điểm chứ không thể thực hiện cả hai đồng thời.Mỗi một Ethernet host phải kiểm tra xem có dữ liệu đang truyền trên mạng hay không trước khi thực hiện phát dữ liệu của mình.Nếu mạng đang có người sử dụng thì host phải hoãn lại thì cả hai hay nhiều Ethernet host sẽ có thể truyền dữ liệu cùng một lúc và kết quả là xảy ra đụng độ.Khi đụng độ xảy ra,host nào phát hiện ra đụng độ đầu tiên sẽ phát ra tín hiệu báo

nghẽn cho các host khác.Khi nhận được tín hiệu báo nghẽn ,mỗi host sẽ ngừng việc truyền dữ liệu lại và chờ một thời gian ngẫu nhiên trước khi bắt đầu thực hiện truyền lại.Khoảng thời gian chờ ngẫu nhiên này do thuật toán back-off(vãn hồi đụng độ)tính toán.Càng có nhiều host kết nối vào mạng và bắt đầu truyền dữ liệu thì đụng độ càng nhiều hơn.

-Ethernet LAN ngày càng trở nên bão hoà vì ngwoif dùng sử dụng nhiều phần mềm chuyên sâu,các ứng dụng client/server… là những loại phần mềm yêu cầu host phải thực hiện truyền thường xuyên hơn với thời gian lâu hơn.



Hình 4.1.4:Cấu trúc mạch của card mạng

Ta xét card bên trái ,tín hiệu được phát ra chân Tx(transmit) xuống đường truyền, đồng thời theo mạch hồi tiếp(loopback) đi vào chân Rx(Receive).Tín hiệu xuống đường truyền và được truyền quảng bá đến mọi máy trạm cùng kết nối vào môi trường truyền chia sẻ.Do đó chân Rx của card bên trái cũng đồng thời nhận được tín hiệu của chính nó từ đường truyền lên.Khi đó nó sẽ so sánh giữa hai tín hiệu,một tín hiệu nhận được từ đường truyền và một tín hiệu đi từ chân Tx theo mạch hồi tiếp vòng về Rx.Nếu hai tín hiệu giống nhau nghĩa là bình thường.Nếu có đụng độ xảy ra,tín hiệu nhận được từ đường truyền lên sẽ bị khác với tín hiệu hồi tiếp từ Tx.Nhờ đó nó phát hiện được đụng độ xảy ra

4.1.5.Sự nghẽn mạch trong mạng

-Kỹ thuật phát triển tạo ra các máy tính ngày càng nhanh hơn và thông minh hơn.Khả năng của máy trạm và các ứng dụng mạng chuyên sâu ngày càng phát

triển thì yêu cầu về băng thông của mạng ngày càng tăng.Nhu cầu đã vượt mức 10Mb/s trên mạng chia sẻ Ethernet/802.3

-Ngày nay ,mạng thực hiện truyền rất nhiều các loại dữ liệu như:

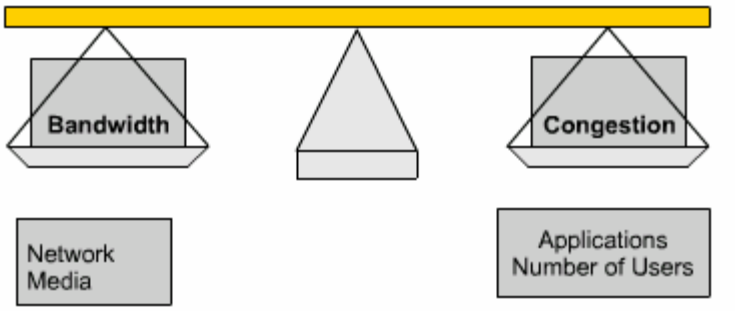
+Tập tin hình ảnh lớn

+Hình ảnh

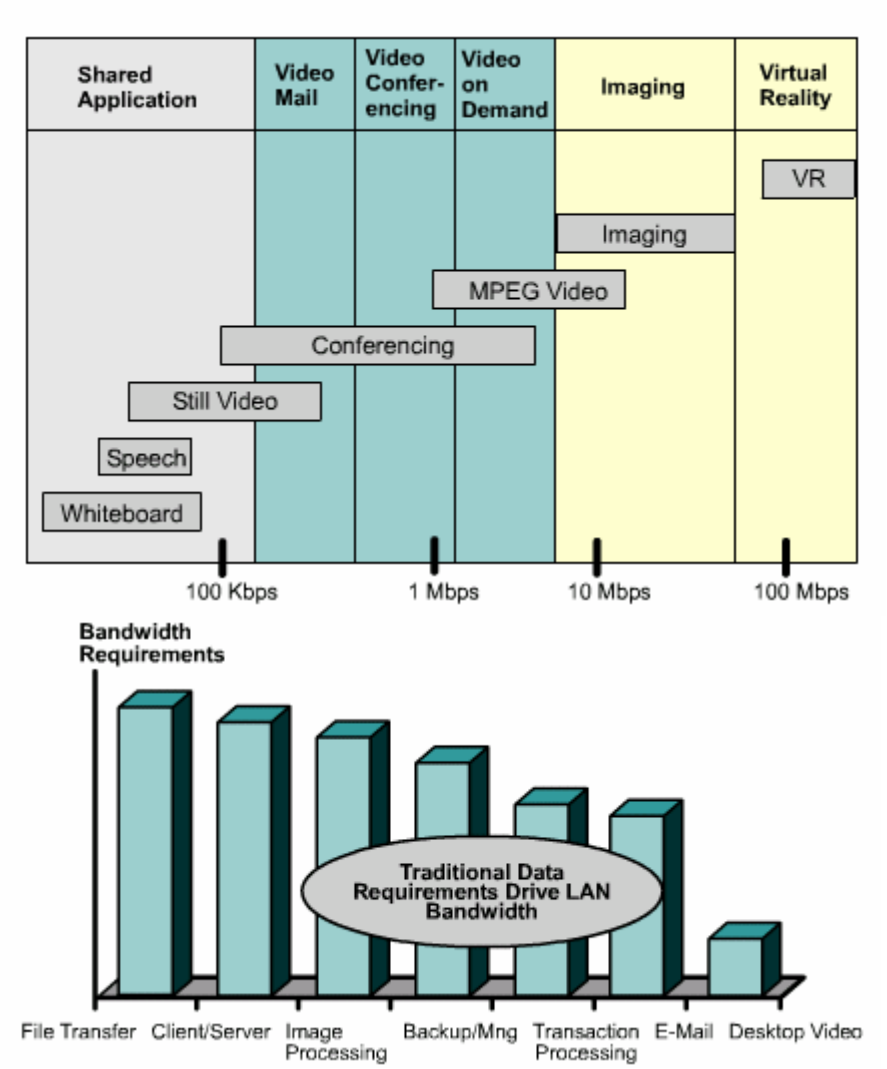
+Hình động(video)

+Ứng dụng đa phương tiện

-Ngoài ra số lượng người dùng trong mạng cũng tăng lên nhanh chóng.Tất cả các yếu tố trên đã đặt một sức ép rất lớn đối với băng thông 10Mb/s.Khi có quá nhiều người cùng thực hiện chia sẻ tập tin,truy cập file server và kết nối Internet thì tình trạng nghẽn mạch sẽ xảy ra.Hậu quả là thời gian đáp ứng của mạng chậm,thời gian tải tập tin lâu hơn và làm giảm năng suất làm việc của người sử dụng. Để giải quyết tình trạng nghẽn mạch này,bạn cần phải có nhiều băng thông hơn hoặc là phải sử dụng lượng băng thông đang có một cách hiệu quả hơn.



Hình 4.1.5.a.Cán cân phải cân bằng giữa băng thông mạng và nhu cầu của người dùng cùng với các ứng dụng chạy trên mạng



Hình 4.1.5.b.Băng thông và các nhu cầu của các ứng dụng khác

4.1.6.Thời gian trễ trên mạng

-Thời gian trễ là khoảng thời gian gói dữ liệu di chuyển từ máy nguồn tới máy đính.Việc xác định thời gian trễ của đường đi giữa nguồn và đính trong LAN và WAN là rất quan trọng.Trong mạng Ethernet LAN ,nắm được thời gian trễ và các tác đọng của nó là rất quan trọng để quyết định thời gian CSMA/CD phát hiện đụng độ và thoả thuận truyền lại.

-Có ít nhất 3 nguồn gây ra trễ:

-Đầu tiên là thời gian mà NIC ở máy nguồn phát tín hiệu điện xuống đường dây và thời gian để NIC ở máy thu nhận biết được các xung điện.Khoảng thời gian này gọi là khoảng thời gian của NIC,khoảng us đối với 10BASE-T NIC.

-Thứ hai là khoảng thời gian tín hiệu lan truyền trên đường dây.Thời gian này khoảng 0,556 us trên 100m cáp UTP CAT5.Cáp càng dài và vận tốc truyền càng chậm thì thời gian trễ này càng lớn.

-Thứ ba là thời gian trễ do các thiết bị mạng lớp 1 lớp 2 lớp 3 dọc trên đường đi giữa hai máy nguồn và đích.

-Thời gian trễ không phụ thuộc hoàn toàn vào khoảng cách và số lượng thiết bị mạng.Ví dụ :Nếu 3 Switch giữa 3 máy trạm được cấu hình đúng thì thời gian trễ giữa hai máy trạm sẽ ít hơn là nếu giữa chúng đặt một Router vì router thực hiện chức năng phức tạp hơn,cần nhiều thơi gian xử lý hơn.Router phải xử lý dữ liệu ở lớp 3 chứ không phải dữ liệu ở lớp 2 như Switch

4.1.7.Thời gian truyền của Ethernet 10Base-T

-Tất cả các mạng đều có một thời bit hay còn gọi là một khe thời gian.Nhiều kỹ thuật LAN như Ethernet chẳng hạn, định nghĩa thời bit là một đơn vị thời gian để truyền đi một bit. Để cho một thiết bị điện hay quang nhận ra được tín hiệu là bit 0 hay bit 1 thì phải có một khoảng thời gian tối thiểu là khoảng thời gian của một bit.

-Thời gian truyền được tính bằng số lượng bit gửi đi nhân với thời bit tương ứng của kỹ thuật mà bạn đang sử dụng.Hay nói cách khác,thời gian truyền là khoảng thời gian truyền hết một gói dữ liệu.Do đó gói dữ liệu càng dài thì khoảng thời gian này càng dài.

-Mỗi một bít trong mạng Ethernet 10Mb/s có thời gian truyền là 100ns. Đây chính là thời bit.Một byte bằng 8 bit .Do đó,một byte cần tối thiểu 800ns để truyền hết.Một frame có 64 byte là frame nhỏ nhất hợp lệ của 10Base-T càn 51.200 ns(51,2us) Như vậy ,nếu truyền một frame có 1000 byte thì máy nguồn cần 800us mới phát xong frame này.Tổng thời gian thực sự để frame đi được tới máy đích còn phụ thuộc vào nhiều nguồn gây trễ khác trên mạng như:

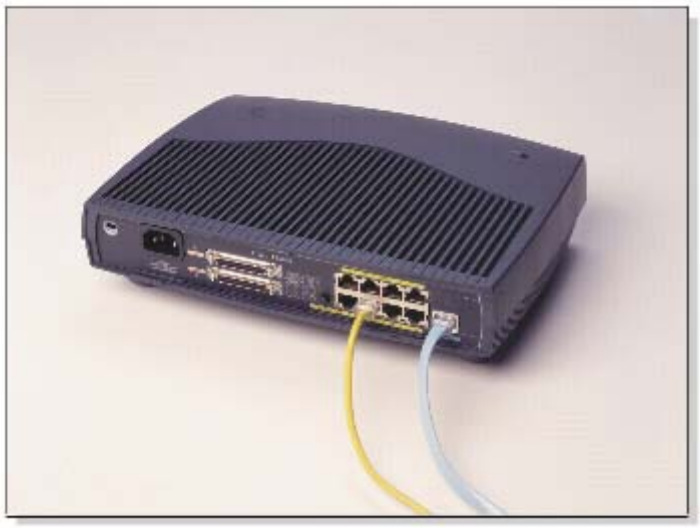
+thơi gian trễ của NIC

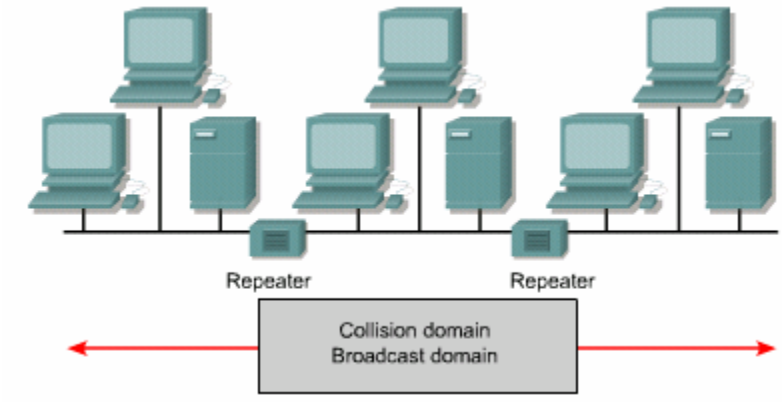
+Thời gian trễ do lan truyền trên đường cáp

+Thời gian trễ do các thiết bị lớp 1,lớp 2 và lớp 3 dọc trên đường đi

4.1.8. Ích lợi của việc sử dụng Repeater

-Khoảng cách mà một mạng LAN có thể bao phủ bị giới hạn và sự suy hao của tín hiệu.Khi tín hiệu di chuyển trên mạng nó sẽ bị suy hao do trở kháng của cáp hay của môi trường truyền làm tiêu hao năng lượng tín hiệu . Ethernet Repeater là một thiết bị hoạt động ở lớp vật lý,nó khuếch đại và tái tạo lại tín hiệu trong Ethernet LAN.Khi bạn sử dụng repeater để mở rộng khoảng cách của một LAN,mạng LAN này có thể bao phủ lênmột phạm vi lớn hơn và có nhiều người dùng hơn cùng chia sẻ mạng này.Tuy nhiên,việc sử dụng repeater và hub lại tạo ra một vấn đề về quảng bá và đụng độ làm giảm hiệu quả hoạt động của mạng LAN có môi trường truyền chia sẻ.





+Repeater là một thiết bị lớp 1 thực hiện khuếch đại,tái tạo lại tín hiệu và truyền đi

+Repeater cho phép kéo dài khoảng cách từ đầu cuối -đến -đầu cuối

+Repeater làm tăng kích thước của miền đụng độ và miền quảng bá

Hình:4.1.8.b.Mở rộng môi trường chia sẻ mạng LAN bằng repeater

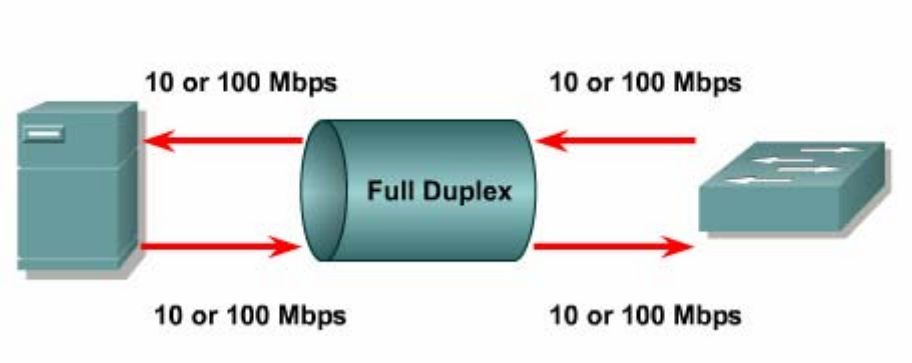
4.1.9.Truyền song công

-Ethernet song công cho phép truyền một gói dữ liệu đồng thời nhận một gói dữ liệu khác tại cùng một thời điểm.Việc truyền và nhận song song đồng thời này yêu cầu sử dụng hai cặp dây khác nhau trong cáp và chuyển mạch kết nối giữa hai máy.Kết nối này phải được xem như kết nối điểm -nối -điểm và hoàn toàn không có đụng độ.Vì cả hai node có thể truyền và nhận đồng thời nên không còn việc thỏa thuận sủ dụng băng thông. Ethernet song công có thể sử dụng cấu trúc cáp đax có nếu như môi trường truyền thỏa mãn được những tiêu chuẩn Ethernet tối thiểu.

Để truyền và nhận đồng thời, mỗi node phải kết nối vào một port riêng trên switch. Kết nối song công có thể sử dụng chuẩn môi trường truyền của 10BASE-T, 100BASE-T hoặc 100BASE-FX để tạo kết nối điiểm-nối-điểm. NIC trên tất cả thiết kế nối vào mạng phải có khả năng song công.

Ethernet switch song công vận dụng ưu điểm của hai cặp dây riêng rẽ trong cáp để tạo kết nối trực tiếp giữa chân truyền (Tx) ở một đầu với chân thu (Rx0 ở đầu kia. Khi hai máy được kết nối như vậy sẽ tạo ra môi trường truyền không có đụng độ, việc truyền và nhận dữ kiệu được thực hiện trên hai mạc điện của hai cặp dây riêng biệt trong sơi cáp.

Trong mạng băng thông 10Mb/s trước đây, Ethernet chỉ sử dụng khoảng 50% - 60% lượng băng thông do đụng độ và thời gian trễ. Ethernet song công có thể sử dụng 100% băng thông trên cả hai chiều, mỗi chiều Tx và Rx bạn có 10Mb/s, tổng cộng là bạn có thông lượng 20Mb/s.



- Gấp đôi băng thông giữa hai node.
- Truyền không có đụng độ.
- Hai đường 10Mb/s hay 100Mb/s.

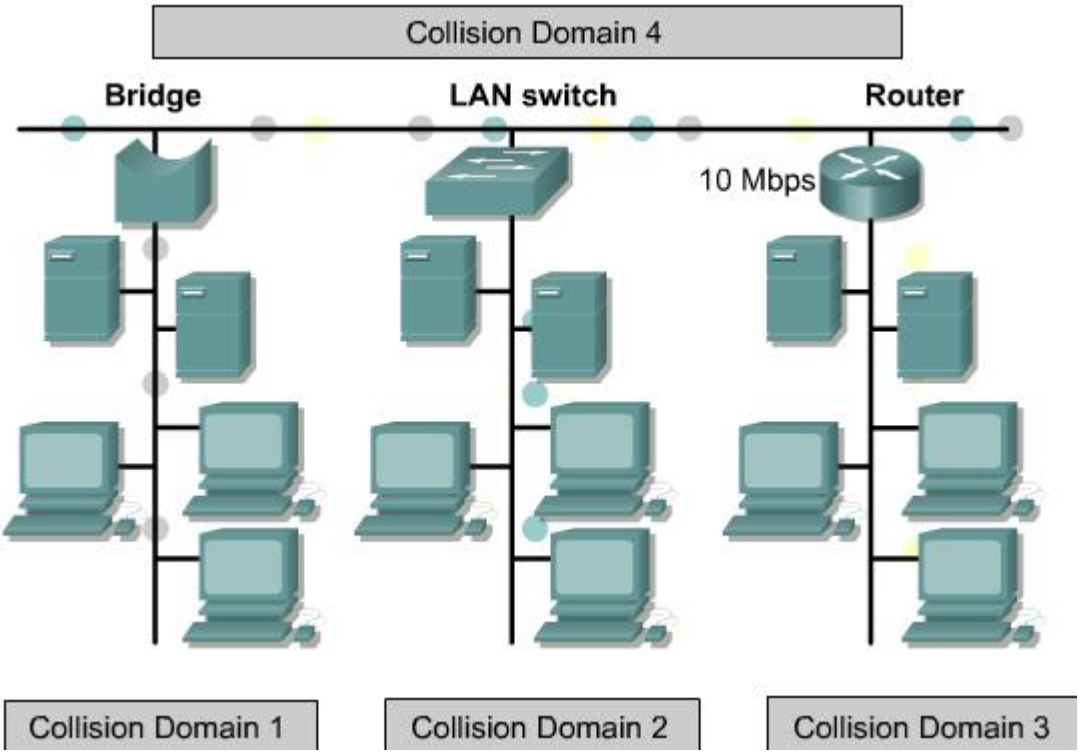
4.2. Giới thiệu về chuyển mạch LAN

4.2.1. Phân đoạn mạng LAN

Một hệ thống mạng có thể chia thành nhiều đơn vị nhỏ hơn gọi là segmnet. Hình 4.2.1. là một ví dụ về phân đoạn Mạng Ethernet. Toàn bộ hệ thống mạng có 15 máy tính, trong đó có 6 server và 9 máy trạm. Mỗi segment sử dụng phương pháp truy cập CSMA/CD và duy trì lưu lượng trong segment đó. Mỗi segment là một miền đụng độ riêng.

Việc phân đoạn mạng cho phép phạm vi nghẽn mạch được thu nhỏ trong phạm vi từng segment. Khi dữ liệu được truyền đi trong một segment, các thiết bị

trong cùng segment đó chia sẻ toàn bộ băng thông của segment đó. Dữ liệu được truyền giữa các segment sẽ được truyền lên đường trục chính của mạng.

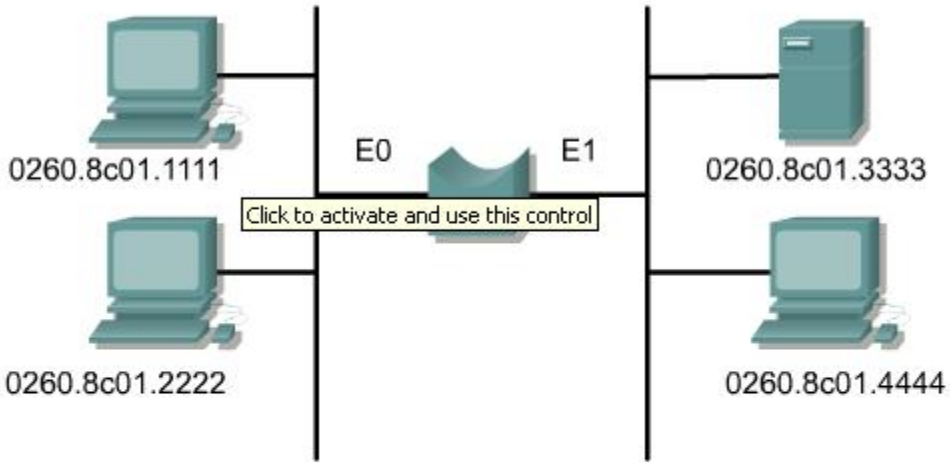


4.2.2. Phân đoạn của mạng bridge

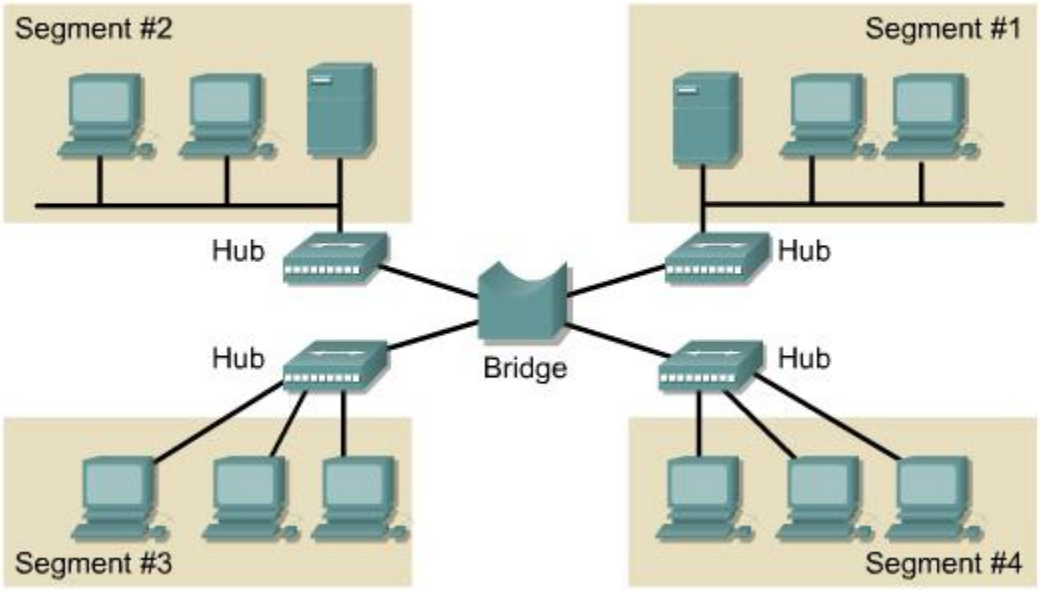
Bridge là một thiết bị Lớp 2 thực hiện chuyển gói dựa trên địa chỉ MAC. Khi bridge nhận frame vào từ một port, bridge sẽ đọc địa chỉ MAC, của máy gửi để nhận biết được thiết bị nàop kết nối với port đó. Từ đó bridge xây dựng được bảng chuyển mạch, trển đó ánh xạ từ địa chỉ MAC ra port tương ứng. Những gói dữ liệu nào không cần chuyển ra segment thì bridge sẽ chặn các gói đó lại.

Mặc dù hoạt động của bridge là trong suốt đối với các thiết bị mạng khác nhưng thời gian trễ vân tăng lên khoảng 10% đến 30% khi sử dụng bridge. Thời gian trễ này là thời gian để bridge xử lý và quyết định chuyển gói. Bridge là một thiết bị chuyển mạch dạng store —and-forward.

Với kiểu chuyển mạch này, bridge phải kiểm tra địa chỉ đích và tính toán CRC (Cyclic Redundancy Check) để kiểm tra lỗi frame rồi mới chuyển frame đi. Nếu port đích đang bận thì bridge có thể tạm thời lâu frame cho đến khi port đích được giải phóng.



Interface	MAC address
E0	0260.8c01.1111
E0	0260.8c01.2222
E1	0260.8c01.3333
E1	0260.8c01.4444



Phân đoạn mạng bằng bridge giúp giảm số lượng người dùng trên một segment.

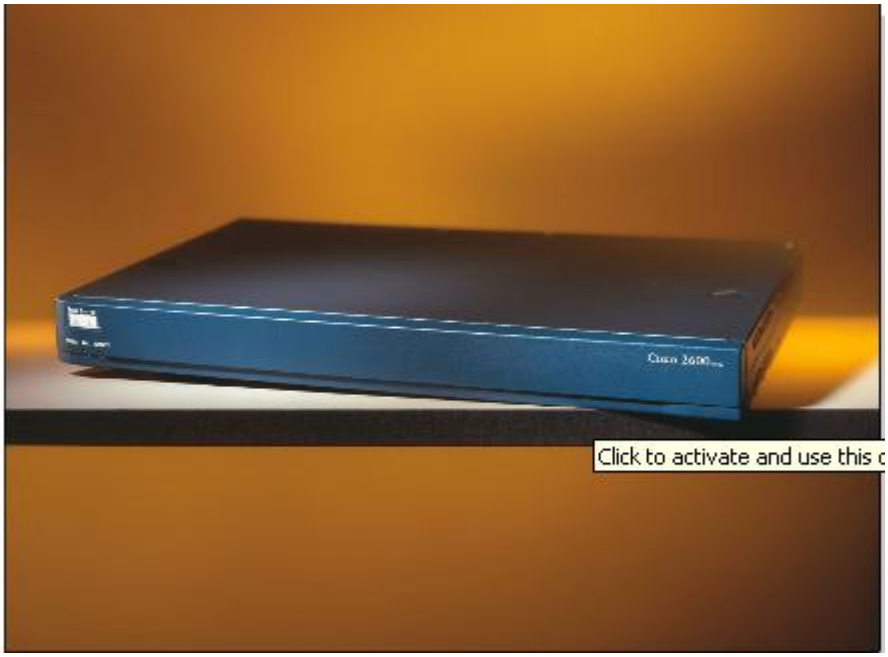
bridge nhận frame, giữ frame rồi chuyển frame đi dựa theo địa chỉ Lớp 2.

Không phụ thuộc vào giao thức Lớp 3

Tăng thời gian trễ trên mạng.

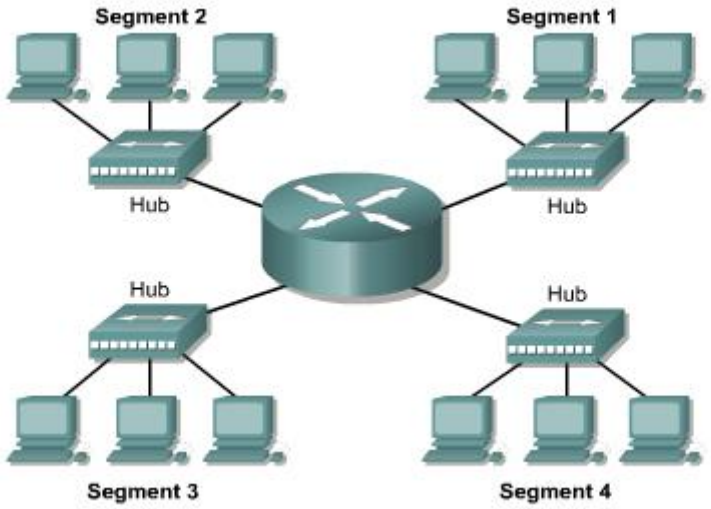
4.2.3. Phân đoạn mạng bằng router.

Phân đoạn mạng bằng router sẽ làm tăng thời gian trễ của mạng lên 20% đến 30%. Thời gian trễ này cao hơn bridge vì router hoạt động ở lớp Mạng và sử dụng địa chỉ IP để quyết định chọn đường tốt nhất đến máy đích.



Bridge và switch chỉ phân đoạn mạng trong một mạng đơn nay trong một subnet thôi. Còn router cung cấp kết nối giữa các mạng và các subnet với nhau.

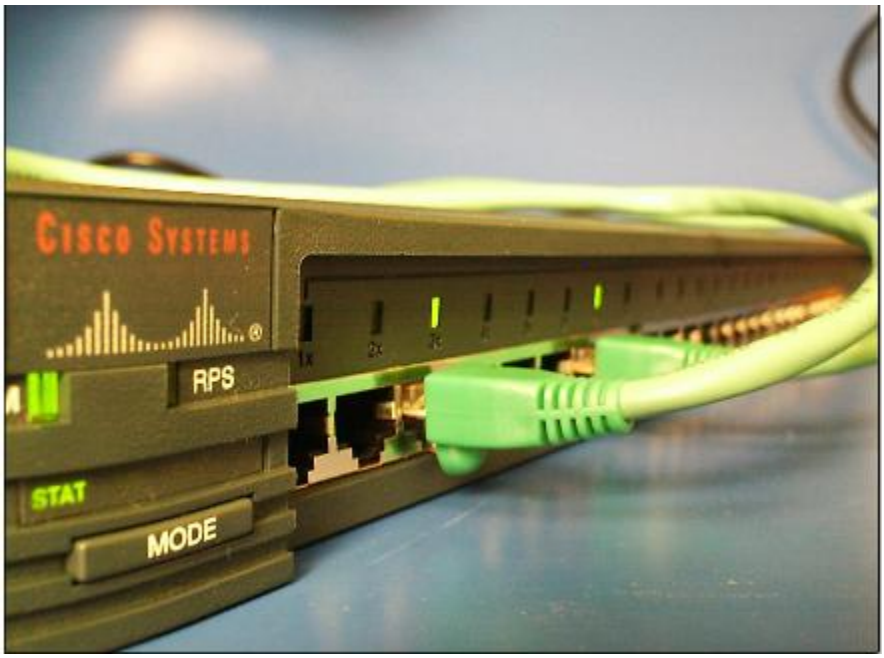
Router không chuyển gói quảng bá trong khi swich và bridge bắt buộc phải chuyển gói quảng cáo.



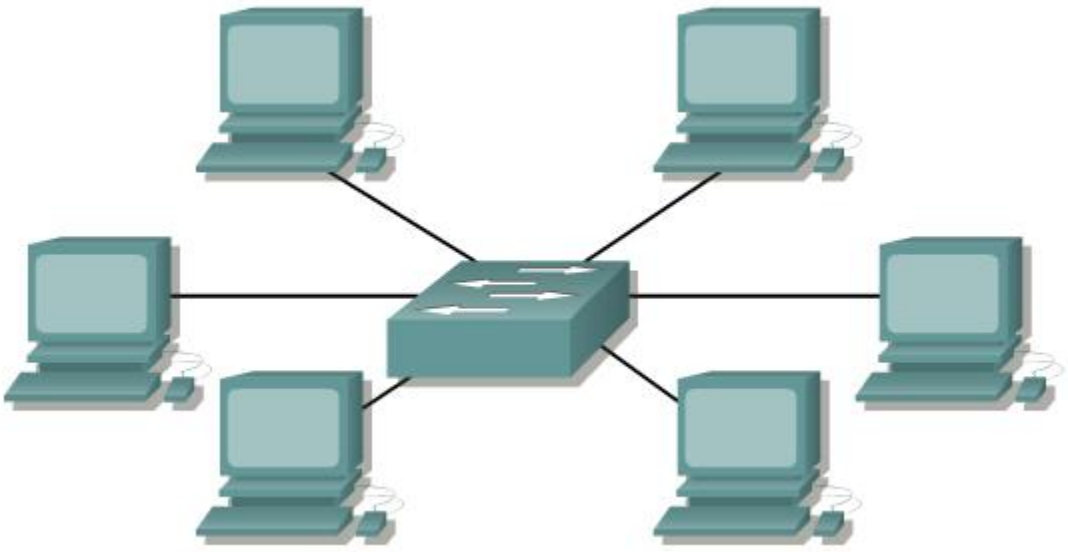
- Dễ quản lý hơn, chức năng nhiều hơn, nhiều đường đi hơn
- Thu nhỏ khích thước miền quảng bá
- Hoạt động ở lớp 3

4.2.4. Phân đoạn mạng bằng switch

Chuyển mạch LAN giúp giảm đi tình trạng thiếu hụt băng thông và nghẽn mạch. Switchsẽ phân đoạn mạng LAN thành các vi đoạn (microsegment), thu nhỏ tối đa kích thước miền đụng độ. Tuy nhiên tất cả các host kết nối vào một switch vẫn nằm trong cùng một miền quảng bá.



Trong mạng Ethernet LAN thuần chuyển mạch, các node thực hiện chức năng truyền và nhận giống như là trong mạng chỉ có duy nhất mình nó vậy. Khi hai node thiết lập kế nối, một mạch ảo được thiết lập giữa chúng và cuing cấp toàn bộ băng thông mạng. Mạch ảo này chỉ tồn tại trong switch khi các node cần trao đổi. Các kết nối bằng switch cung cấp nhiều thông lượng hơ so với Ethernet LAN kết nối bằng bridge hay hub.



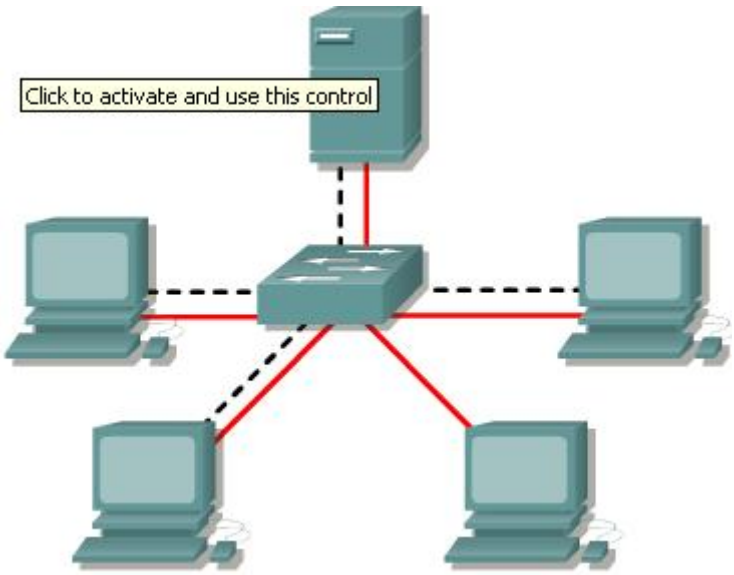
- Swithc loại trừ đụng độ bằng cách phân đoạn cực nhỏ (microsegement).
- Tời gian trễ thấp và tốc độ chuyển trang frame cao trên mỗi port.
- Hoạt động tốt với card mạng và cáp có sẵn của chuẩn 802.3 (CSMA/CD).

4.2.5. Hoạt động cơ bản của switch.

Chuyển mạch là một kỹ thuật giúp giảm tắc nghẽn trọng mạng Ethernet, Token Ring và FDDI (Fiber Distributed Data Inteface). Chuyển mạch thực hiện được việc này bằng cách giảm giao thông và tăng băng thông. LAN switch thường được sử dụng để thay thế cho hub và vẫn hoạt động tốt với các cấu trúc cáp có sẵn.

Switch thực hiện hoạt động chính sau:

- Chuyển mạch frame
- Bảo trì hoạt động chuyển mạch.



- Khả năng truy cập riêng biệt trên port

- Loại trừ được đụng độ và tăng thông lượng đường truyền

- Hỗ trợ được nhiều phiên giao dịch cùng một lúc

- Chuyển frame dựa trên bảng chuyển mạch

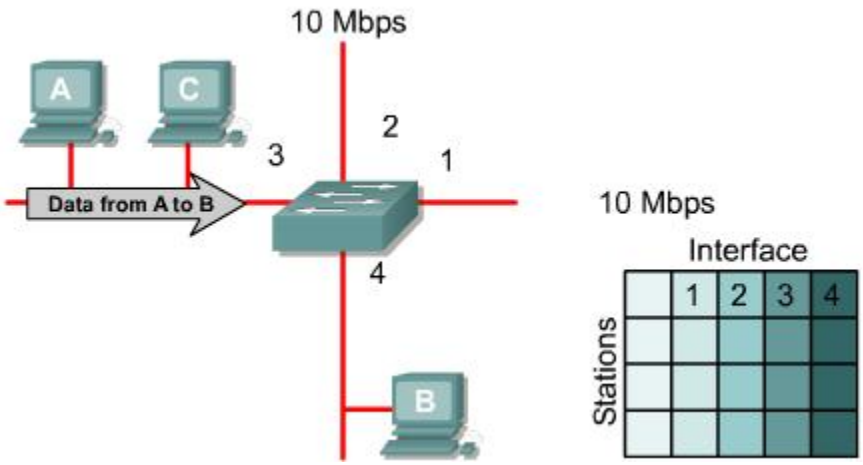
+ Chuyển frame dựa theo địa chỉ MAC (Lớp 2).

- Hoạt động ở Lớp 2 của mô hình OSI.

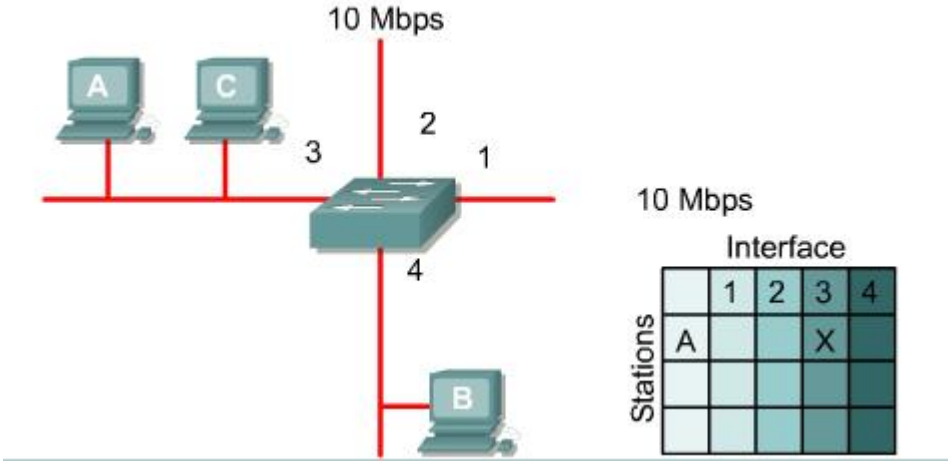
- Học vị trí kết nối của từng máy trạm bằng cách ghi nhận địa chỉ nguồn trên frame nhận vào.

+ Chuyển frame ra tất cả các port khi địa chỉ đích là quảng bá, multicast hoặc là một địa chỉ mà switch không biết.

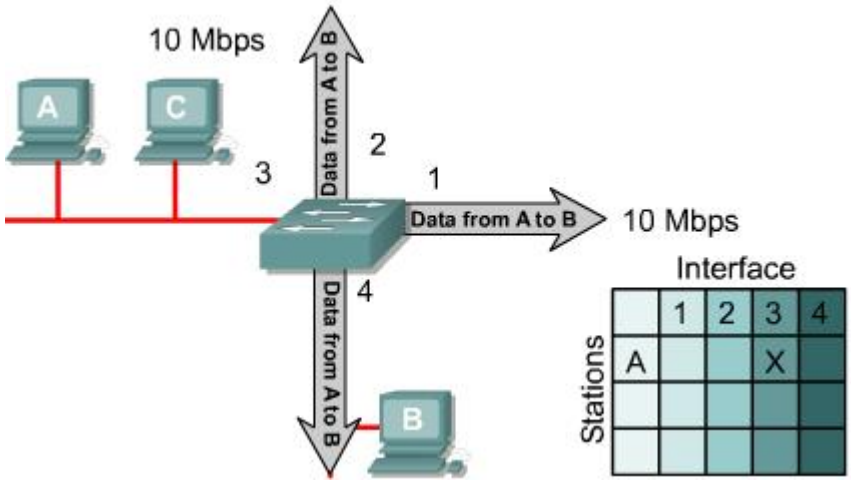
+ Chỉ chuyển frame ra port khác khi địa chỉ đích nằm ở port khác với port nhận vào.



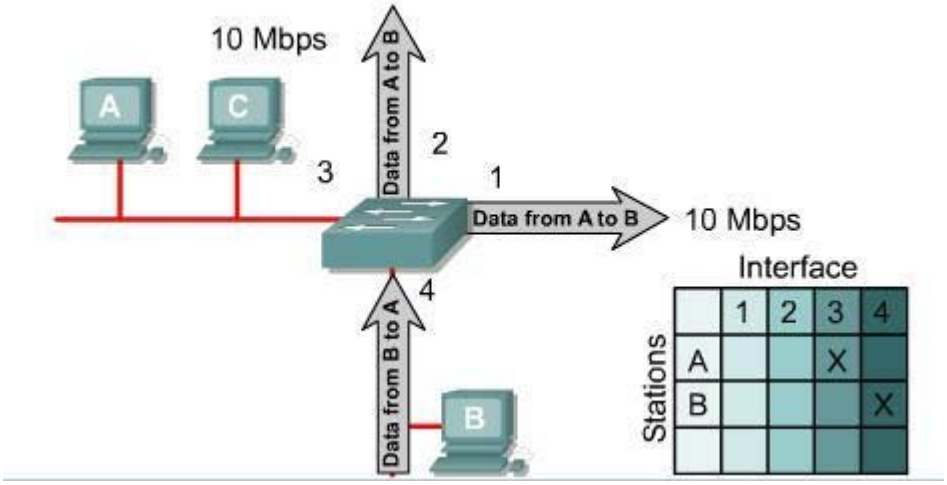
Hình 4.2.5.b. Hoạt động cơ bản của switch. Ta xét hoạt động của switch từ lúc ban đầu chưa có thông tin gì trong bảng chuyển mạch. ở hình này, máy A thực hiện gửi gói dữ liệu cho máy B.



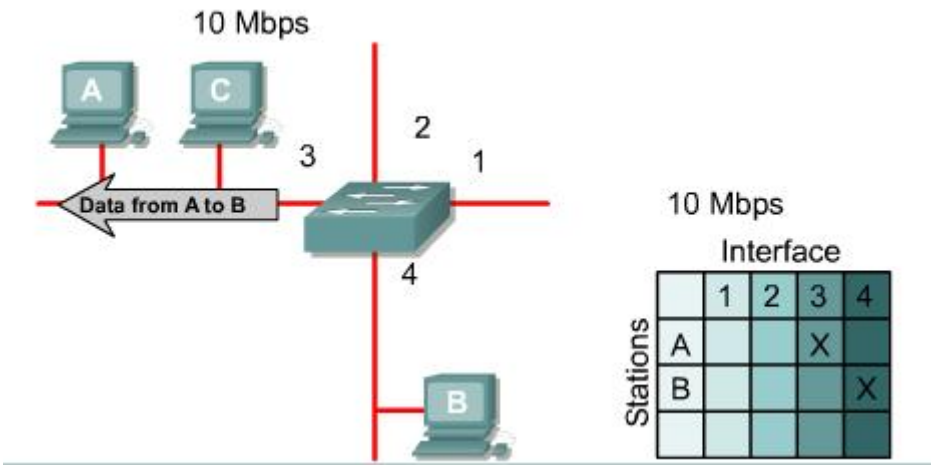
Hình 4.2.5.c. Switch nhận được frame từ máy A vào port số 3. Switch kiểm tra địa chỉ nguồn trong frame nhân được và ghi nhận vào bảng chuyển mạch: địa chỉ MAC của máy A tương ứng với port số 3.



Hình 4.2.5.d. ở thời điểm này, trên bảng chuyển mạch của switch chưa có thông tin gì về địa chỉ đích là địa chỉ MAC của máy B. Do đó, switch chuyển frame ra tất cả các port từ port số 3 là port nhận frame vào.



Hình 4.2.5.e. Máy B nhận được dữ liệu máy A gửi cho nó, nó gửi dữ liệu của nó lại cho máy A



Lúc này, switch nhận vào từ port số 4 gói dữ liệu của máy B gửi cho máy A. Cũng bằng cách học địa chỉ nguồn trong frame nhận vào, switch sẽ ghi nhận được vào bảng chuyển mạch: địa chỉ MAC của máy B là tương ứng với port số 4. Địa chỉ đích của frame này là địa chỉ MAC của máy A mà swithc đã học trước đó. Do đó, switch chỉ chuyển frame ra port số 3.

4.2.6. Thời gian trễ của Ethernet switch.

Thời gian trễ là khoảng thời gian từ lúc switch bắt đầu nhận frame cho đến khi switch đã chuyển hết frame ra port đích. Thời gian trễ này phụ thuộc vào cấu hình chuyển mạch và lượng giao thông qua switch.

Thời gian trễ được đo đơn vị nhỏ hơn giây. Đối với thiết bị mạng hoạt động với tốc độ cao thì mỗi một nano giây (ns) trễ hơn là một ảnh hưởng lớn đến hoạt động mạng.

4.2.7. Chuyển mạch Lớp 2 và Lớp 3.

Chuyển mạch là tiến trình nhận frame vào từ một cổng và chuyển frame ra một cổng khác. Router sử dụng chuyển mạch Lớp 3 để chuyển mạch các gói đã được định tuyến xong. Switch sử dụng chuyển mạch Lớp 2 để chuyển frame.

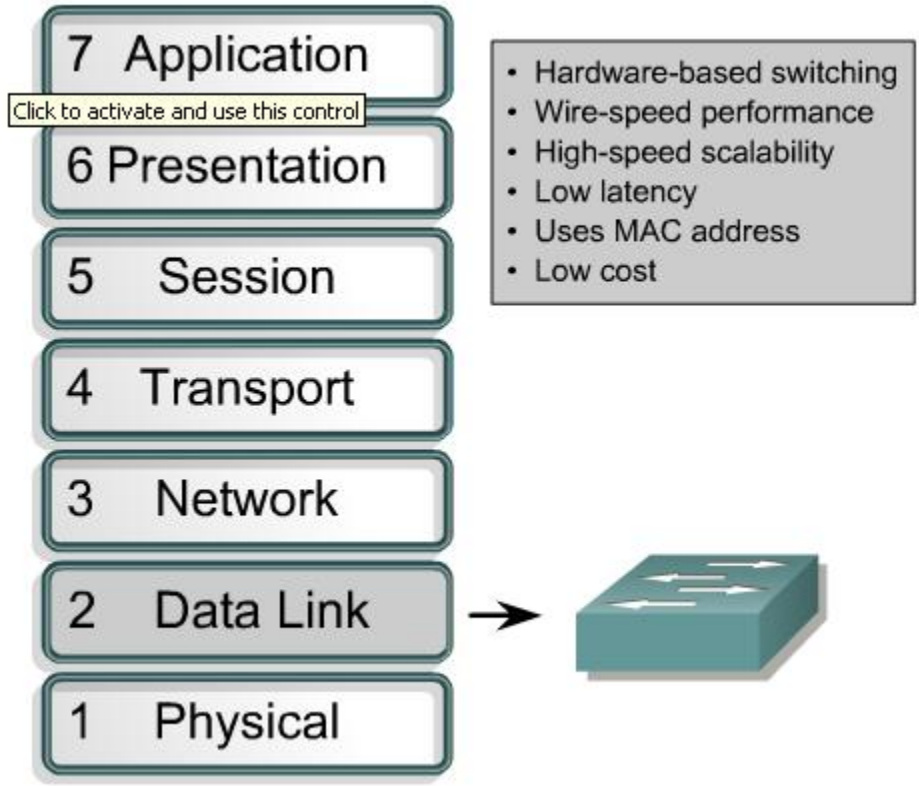
Sự khác nhau giữa chuyển mạch Lớp 2 và Lớp 3 là loại thông tin nằm trong frame được sử dụng để quyết định chọn cổng ra là khác nhau. Chuyển mạch Lớp 2 dựa trên thông tin về địa chỉ MAC. Còn chuyển mạch Lớp 3 thì dựa và địa chỉ lớp Mạng ví dụ như địa chỉ IP.

Chuyển mạch Lớp 2 nhìn vào địa chỉ MAC đích trong phần header của frame và chuyển frame ra đúng port dựa theo thông tin về địa chỉ MAC trên bảng chuyển

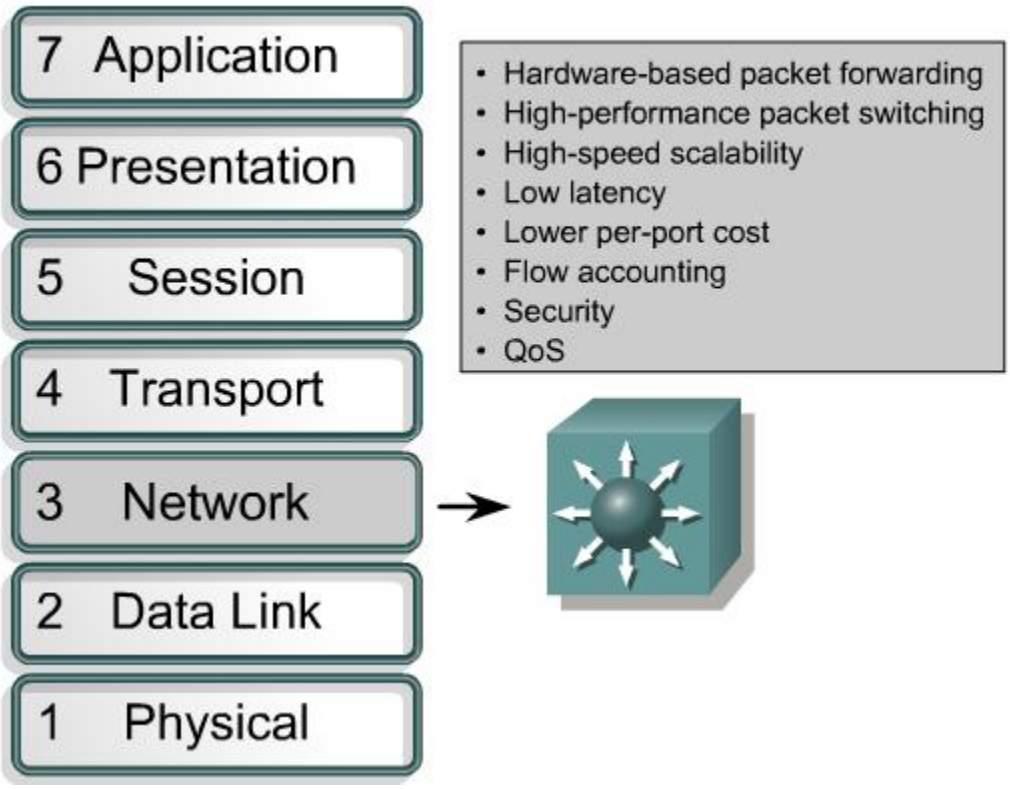
mạch. Bảng chuyển mạch được lưu trong bộ nhớ địa chỉ CAM (Content Addressable Memory). Nếu switch Lớp 2 không biết phải gửi frame ra port nào cụ thể thì đơn giản là nó quảng bá frame ra tất cả các port của nó. Khi nhận được gói trả lời về, switch sẽ ghi nhận địa chỉ mới vào CAM.

Chuyển mạch Lớp 3 là một chức năng của Lớp Mạng. Chuyển mạch Lớp 3 kiểm tra thông tin nằm trong phần header của Lớp 3 và dựa vào địa chỉ IP trong đó để chuyển gói.

Dòng giao thông trong mạng chuyển mạch hay mạng ngang hàng hoàn toàn khác với dòng giao thông trong mạng định tuyến hay mạng phân cấp. Trong mạng phân cấp, dòng giao thông được uyển chuyển hơn trong mạng ngang hàng.



Hình 4.2.7.a. Chuyển mạch lớp 2



Hình 4.2.7.b. Chuyển mạch lớp 3

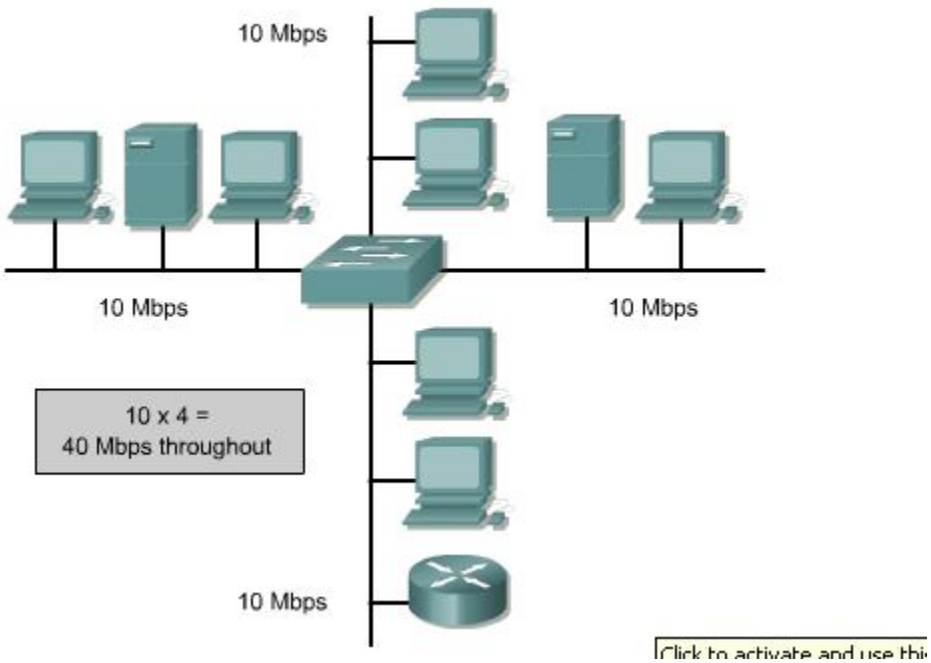
4.2.8. Chuyển mạch đối xứng và bất đối xứng.

Chuyển mạch LAN được phân loại thành đối xứng và bất đối xứng dựa trên bảng thông của mỗi Port trên switch. Chuyển mạch đối xứng là chuyển mạch giữa các port có cùng băng thông. Chuyển mạch bất đối xứng là chuyển mạch giữa các port có băng thông khác nhau, ví dụ như giữa các port 10 Mb/s và port 100 Mb/s.

Chuyển mạch bất đối xứng cho phép dành nhiều băng thông hơn cho port nối vào server để tránh nghẽn mạch trên đường này khi có nhiều client cùng truy cập vào server cùng một lúc. Chuyển mạch bất đối xứng cần phải có bộ nhớ đệm để giữ frame được liên tục giữa hai tốc độ khác nhau của hai port.

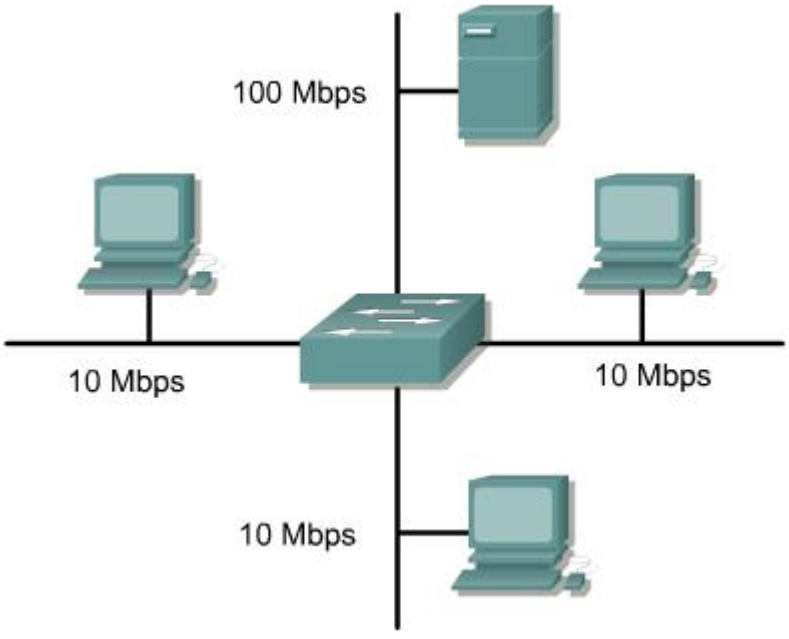
- Chuyển mạch giữa hai port có cùng băng thông (10/10 Mb/s hay 100/100 Mb/s).

- Thông lượng càng tăng khi số lượng thông tin liên lạc đồng thời tại một thời điểm càng tăng.



Hình 4.2.8.a . Chuyển mạch đối xứng.

- Chuyển mạch giữa hai port không cùng băng thông (10/100 Mb/s)
- Đòi hỏi phải có bộ nhớ đệm.



Hình 4.2.8.b. Chuyển mạch bất đối xứng.

4.2.9. Bộ đệm.

Ethernet switch sử dụng bộ đệm để giữ và chuyển frame. Bộ đệm còn được sử dụng khi port đích đang bận. Có hai loại bộ đệm có thể sử dụng để chuyển frame là bộ đệm theo port và bộ đệm chia sẻ.

Trong bộ đệm theo port, frame được lưu thành từng hàng đợi tương ứng với từng port nhận vào. Sau đó frame chỉ được chuyển sang hàng đợi của port đích khi tất cả các frame trước nó trong hàng đợi đã được chuyển hết. Như vậy một frame có thể làm cho tất cả các frame còn lại trong hàng đợi phải hoãn lại vì port đích của frame này đang bận. Ngay cả khi port đích đang trống thì cũng vẫn phải chờ một khoảng thời gian để chuyển hết frame đó.

Bộ đệm được chia sẻ để tất cả các frame vào chung một bộ nhớ. Tất cả các port của switch chia sẻ cùng một bộ đệm. Dung lượng bộ đệm được tự động phân bổ theo nhu cầu của mỗi port ở mỗi thời điểm. Frame được tự động phân bổ theo nhu cầu của mỗi port ở mỗi thời điểm. Frame trong bộ đệm được tự động đưa ra port phát. Nhờ cơ chế chia sẻ này, một frame nhận được từ port này không cần phải chuyển hàng đợi để phát ra port khác.

Switch giữ một sơ đồ cho biết frame nào tương ứng với port nào và sơ đồ này sẽ được xoá đi sau khi đã truyền frame thành công. Bộ đệm được sử dụng theo dạng chia sẻ. Do đó lượng frame lưu trong bộ đệm bị giới hạn bởi tổng dung lượng của bộ của bộ đệm chứ không phụ thuộc vào vùng đệm của từng port như dạng bộ đệm theo port. Do đó frame lớn có thể chuyển đi được và ít bị rớt gói hơn. Điều này rất quan trọng đối với chuyển mạch bất đồng bộ vì frame được chuyển mạch giữa hai port có tốc độ khác nhau.

- Bộ đệm theo port lưu các frame theo hàng đợi tương ứng với từng port nhận vào.

- Bộ đệm chia sẻ lưu tất cả các frame vào chung một bộ nhớ. Tất cả các port trên switch chia sẻ cùng một vùng nhớ này.

4.2.10. Hai phương pháp chuyển mạch.

Sau đây là hai phương pháp chuyển mạch dành cho frame:

- Store-and-forwad: Nhận vào toàn bộ frame xong rồi mới bắt đầu chuyển đi. Switch đọc địa chỉ nguồn, đích và lọc frame nếu cần trước khi quyết định chuyển frame ra. Vì switch phải nhận xong toàn bộ frame rồi mới bắt đầu tiến trình chuyển

mạch frame nên thời gian trễ sẽ càng lớn đối với frame càng lớn. Tuy nhiên nhờ vậy switch mới có thể kiểm tra lỗi cho toàn bộ frame giúp khả năng phát hiện lỗi cao hơn.

- Cut-through: Frame được chuyển đi trước khi nhận xong toàn bộ frame. Chỉ cần địa chỉ đích có thể đọc được rồi là đã có thể chuyển frame ra. Phương pháp này làm giảm thời gian trễ nhưng đồng thời cũng làm giảm khả năng phát hiện lỗi frame.

Sau đây là hai chế độ chuyển mạch cụ thể theo phương pháp cut-through:

- Fast-forward: Chuyển mạch nhanh có thời gian trễ thấp nhất. Chuyển mạch nhanh sẽ chuyển frame ra ngay sau khi đọc được địa chỉ đích của frame mà không cần phải chờ nhận hết frame. Do đó cơ chế này không kiểm tra được frame nhận vào có bị lỗi hay không mặc dù điều này không xảy ra thường xuyên và máy đích sẽ huỷ gói nếu gói bị lỗi. Trong chế độ chuyển mạch nhanh, thời gian trễ được tính từ lúc switch nhận vào bit đầu tiên cho đến khi switch phát ra bit đầu tiên.

- Fragment-free: Cơ chế chuyển mạch này sẽ lọc bỏ cách mảnh gãydo đụng độ gây ra trước khi bắt đầu chuyển gói. Hầu hết những frame bị lỗi trong mạng là những mảnh gãy của frame do bị đụng độ. Trong mạn hoạt động bình thường, một mảnh frame gãy do đụng độ gây ra nhất phải nhỏ hơn 64 byte. Bất kỳ frame nào lớn hơn 64 byte đều được xem là hợp lệ và thường không có lỗi. Do cơ chế chuyển mạch khiông mảnh gãy sẽ chờ nhận đủ 64 byte đầu tiên của frame để đảm bảo frame nhận được không phải là một mảnh gãy do bị đụng độ rồi mới bắt đầu chuyển frame đi. Trong chế độ chuyển mạch này, thời gian trễ cũng được tính từ lúc switch nhận được bit đầu tiên cho đến khi switch phát đi bit đầu tiên đó.

Thời gian trễ của mỗi chế độ chuyển mạch phụ thuộc vào cách mà switch chuyền frame như thế nào. Đẻ chuyển frame được nhanh hơn, switch đã bớt thời gian kiểm tra lỗi frame đi nhưng làm như vậy lại làm tăng lượng dữ liệu cần truyền lại.

4.3. Hoạt động của switch.

4.3.1. Chức năng của Ethernet switch.

Switch là một thiết bị mạng chọn lựa đường dãn để gửi frame đến đích, Cả switch và bridge đều hoạt động ở Lớp 2 của mô hình OSI.

Đôi khi switch còn được gọi là bridge đa port hay hub chuyển mạch. Swich quyết định chuyển frame dựa trên địa chỉ MAC, do đó nó được xếp ào thiết bị Lớp 2. Ngược lại, hub chỉ tái tạo lại tín hiệu Lớp 1 và phát tín hiệu đó ra tất cả các port của nó mà không hề thực hiện một sự chọn lựa nào. Chính nhờ switch có khả năng chọn lựa dường dẫn để quyết định chuyển frame nên mạng Lan có thẻ hoạt động hiệu quả hơn. Switch nhận biết host nào kết nối vào port của nó bằng cách đọca địa chỉ MAC nguồn trong frame mà nó nhận được. Khi hai host thực hiện liên lạc với nhau, switch chỉ thiết lập một mạch ảo giữa hai port tương ứng và không làm ảnh hưởng đến lưu thông trên các port khác. Trong khi đó, hub chuyển dữ liệu ra tất cả các port của nó nên mọi host đều nhận được dữ liệu và phải xử lý dữ liệu cho dù những dữ liệu này không phải gửi cho chúng. Do đó, mạng Lan có hiệu suất hoạt động cao thường sử dụng chuyển mạch toàn bộ.

- Switch tập trung các kết nối và quyết định chọn đường dẫn để chuyển dữ liệu hiệu quả. Frame được chuyển mạch từ port nhận vào đến port phát ra. Mỗi port là một kết nối cung cấp chọn băng thông cho host.

- Trong Ethernet hub, tất cả các port kết nối vào một mạch chính, hay nói cách khác, tất cả các thiết bị kết nối hub sẽ cùng chia sẻ băng thông mạng. Nếu có hai máy trạm được thiết lập phiên kết nối thì chúng sẽ sử dụng một lượng băng thông đáng kể và hoạt động của các thiết bị còn lại kết nối vào hub sẽ bị giảm xuống.

- Để giải quyết tình trạng trên, switch xử lý mỗi port là một segment riêng biệt. Khi các máy ở các port khác nhau cần liên lạc với nhau, switch sẽ chuyển từ frame từ port này sang port kia và đảm bảo cung cấp chon băng thông cho mỗi phiên kết nối.

Để chuyển frame hiệu quả giữa các port, switch lưu giữ một bảng địa chỉ. Khi switch nhận vào một frame, nó sẽ ghi nhận địa chỉ MAC của máy gửi tương ứng với port mà nó nhận frame đó vào.

Sau đây là các đặc điểm chính của Ethernet switch

- Tách biệt giao thông trên từng segment

- Tăng nhiều hơn lượng băng thông dành cho mỗi user bằng cách tạo miền đụng độ nhỏ hơn.

Đặc điểm đầu tiên: Tách biệt giao thông trên từng segment. Ethernet switch chia hệ thống mạng thành các đơn vị cực nhỏ gọi là microsegment. Các segment

như vậy cho phép các user trên segment khác nhau có thể gửi dữ liệu cùng một lúc mà không làm chậm lại các hoạt động của mạng.

Bằng cách chia nhỏ hệ thống mạng, bạn sẽ làm giảm lượng user và thiết bị cùng chia sẻ một băng thông. Mỗi segment là một miền đụng độ riêng biệt. Ethernet switch giới hạn lưu thông bằng chỉ chuyển gói đến đúng port cần thiết dựa trên địa chỉa MAC Lớp 2.

Đặc điểm thứ hai của Ethernet switch là đảm bảo cung cấp băng thông nhiều hơn cho user bằng cách tạo các miền đụng độ nhỏ hơn. Ethernet và Fast Ethernet switch chia nhỏ mạng LAN thành nhiều segment nhỏ. Mỗi segment này là một kết nối riêng giống như là một làn đường riêng 100 Mb/s vậy. Mỗi serer có thể đặt trên một kết nối 100 Mb/s riêng. Trong các hệ thống mang hiện nay, Fast Ethernet switch được sử dụng làm đường trục chính cho LAN, còn Ethernet hub, Ethernet switch hoặc Fast Ethernet hub được sử dụng để kết nối xuống các máy tính. Khi các ứng dụng mới như truyền thông đa phương tiện, video hội nghị ... ngày càng trở nên phổ biến hơn thì mỗi máy tính sẽ được một kết nối 100 Mb/s riêng vào switch.

4.3.2. Các chế độ chuyển mạch frame

Có 3 chế độ chuyển mạch frame:

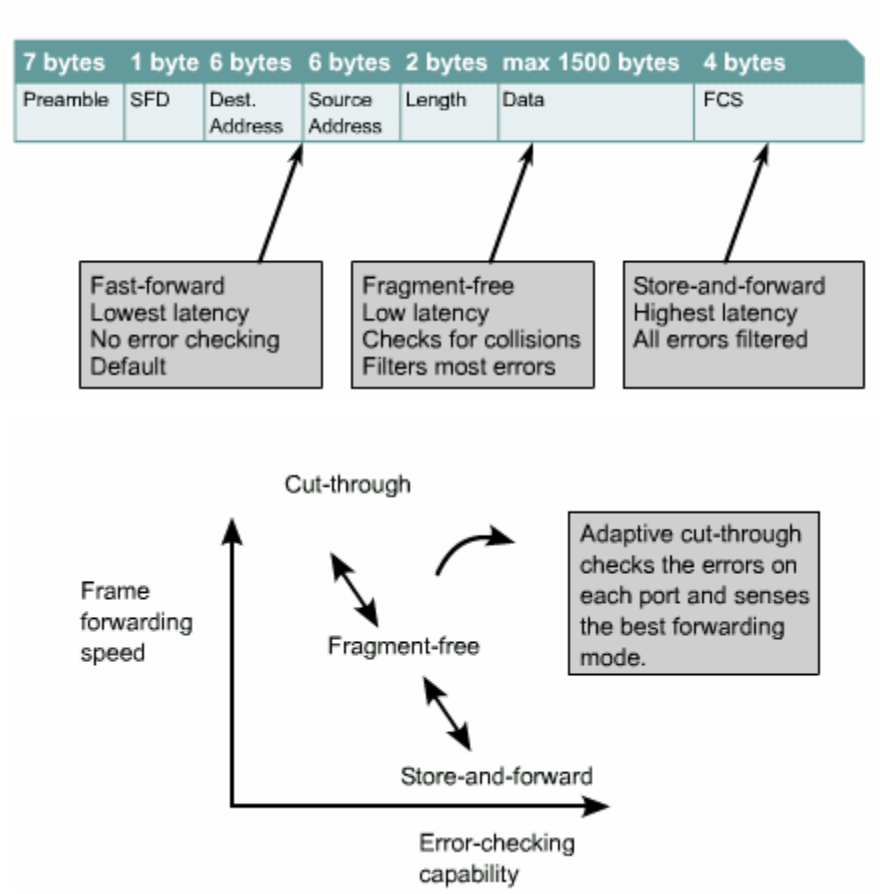
- Fast-forwad: switch đọc được địa chỉ của frame là bắt đầu chuyển frame đi luôn mà không cần chờ nhận được hết frame. Như vậy, frame được chuyển đi trước khi nhận hết toàn bộ frame.. Do đó, thời gian trễ giảm xuống nhưng khả năng phát hiện lỗi kém. Fast-forward là một thuật ngữ được sử dụng để chỉ switch đang ở chế độ chuyển mạch cut-through.

- Store —and-forward: Nhận vào toàn bộ frame rồi mới bắt đầu chuyển frame đi. Switch đọc địa chỉ nguồn, đích và thực hiện lọc bỏ frame nếu cần rồi mới quyết định chuyển frame đi. Thời gian switch nhận frame vào sẽ gây ra thời gian trễ. Frame càng lớn thì thời gian trễ càng vì switch phải nhận xong toàn bộ frame rồi mới tiến hành chuyển mạch cho frame. Nhưng như vậy thì switch mới có đủ thời gian và dữ liệu để kiểm tra lỗi frame, nên khả năng phát hiện lỗi cao hơn.

- Fragment-free: Nhận vào hết 64 byte đầu tiên của Ethernet frame rồi mới bắt đầu chuyển frame đi. Fragement-free là một thuật ngữ được sử dụng để chỉ switch đang sử dụng một dạng cải biên của chuyển mạch cut-through.

Một chế độ chuyển mạch khác được kết hợp giữa cut-through và store-and-forward. Kiểu kết hợp này gọi là cut-through thích nghi (adaptive cut-through).

Trong chế độ này, switch sẽ sử dụng chuyển mạch cut-through cho đến khi nào nó phát hiện ra một lượng frame bị lỗi nhất định. Khi số lượng frame bị lỗi vượt quá mức ngưỡng thì khi đó switch sẽ chuyển dùng chuyển mạch store-and-forwad.



4.3.3. Bridge và switch học địa chỉ như thế nào

Bridge và switch chỉ chuyển từ segment này sang segment khác khi cần thiết. Để thực hiện nhiệm vụ này, bridge và switch phải biết thiết bị nào kết nối vào segment nào.

Bridge được xem là một thiết bị thông minh vì nó có thể quyết định chuyển frame dựa trên địa chỉ MAC. Để thực hiện công việc này, bridge xây dựng một bảng địa chỉ. Khi bridge bắt đầu được bật lên, nó sẽ quảng bá một thông điệp cho mọi máy trạm trong segment kết nối vào nó để yêu cầu các máy này trả lời. Khi

các máy trạm trả lời cho thông điệp quảng bá, bridge sẽ ghi nhận lại địa chỉ của các máy vào bảng địa chỉ của mình. Quá trình này được gọi là quá trình học địa chỉ.

Bridge và switch học địa chỉ theo các cách sau:

* Đọc địa chỉ MAC nguồn trong mỗi frame nhận được.

* Ghi nhận lại số port mà switch sẽ học được địa chỉ nào thuộc về thiết bị kết nối vào port nào của bridge hoặc switch.

* Địa chỉ học được và số port tương ứng sẽ lưu trong bảng địa chỉ. Bridge sẽ kiểm tra địa chỉ đích nằm trong frame nhận được rồi dò tìm địa chỉ đích này trong bảng địa chỉ để tìm port tương ứng.

CAM (Content Addressable Memory) được sử dụng cho các hoạt động sau:

* Lấy ra thông tin địa chỉ trong gói dữ liệu nhận được và xử lý chúng

* So sánh địa chỉ đích của frame với các địa chỉ trong bảng của nó

CAM lưu giữ bảng địa chỉ MAC và số port tương ứng. CAM sẽ so sánh địa chỉ MAC nhận được với nội dung của bảng CAM. Nếu tìm thấy đúng địa chỉ đích thì số port tương ứng sẽ được chọn để chuyển gói ra.

Ethernet switch học địa chỉ của từng thiết bị trong mạng kết nối vào nó bằng cách đọc địa chỉ nguồn của từng frame mà nó nhận được và ghi nhớ số port mà nó vừa nhận frame đó vào. Những thông tin học được sẽ lưu trong CAM. Mỗi khi nó đọc được một địa chỉ mới chưa có trong CAM thì nó sẽ tự động học và lưu lại địa chỉ đó để sử dụng cho lần sau. Mỗi địa chỉ như vậy được đánh dấu thời gian cho phép địa chỉ có được lưu giữ trong một khoảng thời gian.

Sau đó mỗi khi switch đọc một địa chỉ nguồn trong frame, địa chỉ tương ứng trong CAM sẽ được đánh dấu thời gian mới. Nếu trong suốt khoảng thời gian đánh

dấu mà switch không có ghi nhận gì nữa về địa chỉ đó thì nó sẽ xoá địa chỉ đó ra khỏi bảng. Nhờ vậy CAM luôn giữ được thông tin của mình chính xác và kịp thời.

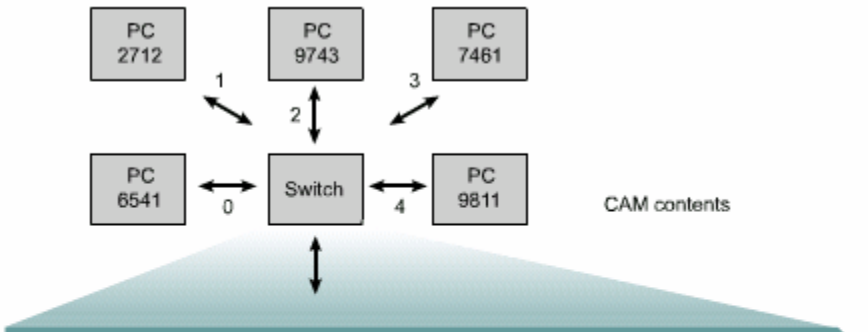
Sau đây là quá trình xử lý của CAM:

1. Nếu bridge không tìm thấy địa chỉ đích trong bảng của nó thì nó sẽ chuyển frame ra tất cả các port trừ port nhận frame vào.

2. Bảng địa chỉ của bridge có thể bị xoá do bridge khởi động lại hoặc một địa chỉ nào đó đã bị xoá vì đã hết thời gian đánh dấu mà bridge vẫn không nhận được thông tin nào về địa chỉ đó nữa. Khi bridge không biết chọn port nào để chuyển frame thì nó gửi frame ra tất cả các port từ port nhận frame vào. Đương nhiên là không cần phải gửi lại frame ra port mà nó vừa được nhận vào nữa vì các thiết bị khác nằm trong segment kết nối vào port đó cũng đã nhận được frame rồi.

3. Nếu bridge tìm thấy địa chỉ trong bảng nhưng port tương ứng cũng chính là port mà nó vừa nhận frame vào, lúc này bridge sẽ huỷ bỏ gói dữ liệu đó vì máy đích nằm cùng segment với máy nguồn và nó đã nhận được frame rồi.

4. Nếu bridge tìm thấy địa chỉ trong bảng và port tương ứng là port khác với port nhận frame vào thì bridge sẽ chuyển frame ra đúng port tương ứng với địa chỉ đích.



Port	Host MAC address
0	6541
1	2712
2	9743
3	7461
4	9811

4.3.4. Bridge và switch thực hiện lọc frame như thế nào

Bridge có khả năng lọc frame dựa trên bất kỳ thông tin Lớp 2 nào trong frame. Ví dụ: bridge có thể được cấu hình để từ chối không chuyển tất cả các frame có địa chỉ nguồn từ một mạng nào đó. Các thông tin lớp 2 thường có phản ánh giao thức lớp trên nên bridge có thể lọc frame dựa vào đặc điểm này. Hơn nữa việc lọc frame cũng rất có ích đối với các gói quảng bá và multicast không cần thiết.

Một khi bridge đã xây dựng xong bảng địa chỉ của nó thì có nghĩa là nó đã sẵn sàng hoạt động. Khi nó nhận vào frame, nó kiểm tra địa chỉ đích. Nếu địa chỉ đích nằm cùng phía với port nhận frame thì bridge sẽ huỷ frame đi. Động tác này được gọi là lọc frame. Nếu địa chỉ đích nằm trên segment khác thì bridge sẽ chuyển frame ra segment đó.

Về cơ bản, bridge chỉ lọc bỏ những frame được gửi trong nội bộ một segment và chỉ chuyển các frame gửi sang segment khác.

Còn lọc frame đặc biệt theo địa chỉ nguồn và đích thì có các dạng sau:

* Không cho một máy nào đó được gửi frame ra ngoài segment của máy đó.

* Không cho tất cả các frame từ bên ngoài gửi frame đến một máy nào đó. Nhờ vậy có thể ngăn không cho các máy khác có thể thông tin liên lạc với một máy nào đó.

Cả hai loại lọc frame trên đều giúp kiểm soát giao thông mạng và tăng khả năng bảo mật.

Hầu hết Ethernet bridge đều có khả năng lọc gói quảng bá và multicast. Đôi khi có một thiết bị nào đó hoạt động không bình thường và liên tục phát ra các gói quảng bá đi khắp mạng. Một cơn bão quảng bá có thể làm cho hoạt động mạng trở thành con số 0. Do đó nếu bridge không thể lọc bỏ các gói quảng bá thì cơn bão quảng bá sẽ có khả năng xảy ra.

Ngày nay, bridge còn có thể lọc frame tuỳ theo giao thức lớp mạng ở trên. Điều này làm giảm đi ranh giới giữa bridge và router. Router hoạt động ở lớp

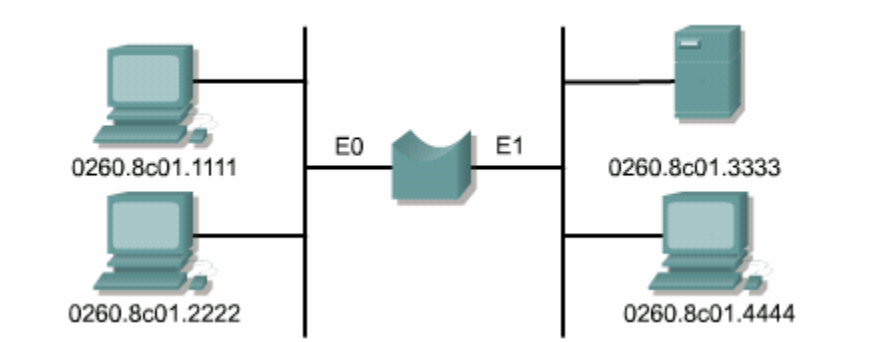
mạng, sử dụng giao thức định tuyến để phân luồng giao thông trên mạng. Còn bridge sử dụng kỹ thuật lọc cải tiến dựa trên thông tin lớp mạng được gọi là brouter. Brouter khác với router ở chỗ là không sử dụng giao thức định tuyến.

4.3.5. Phân đoạn mạng LAN bằng bridge

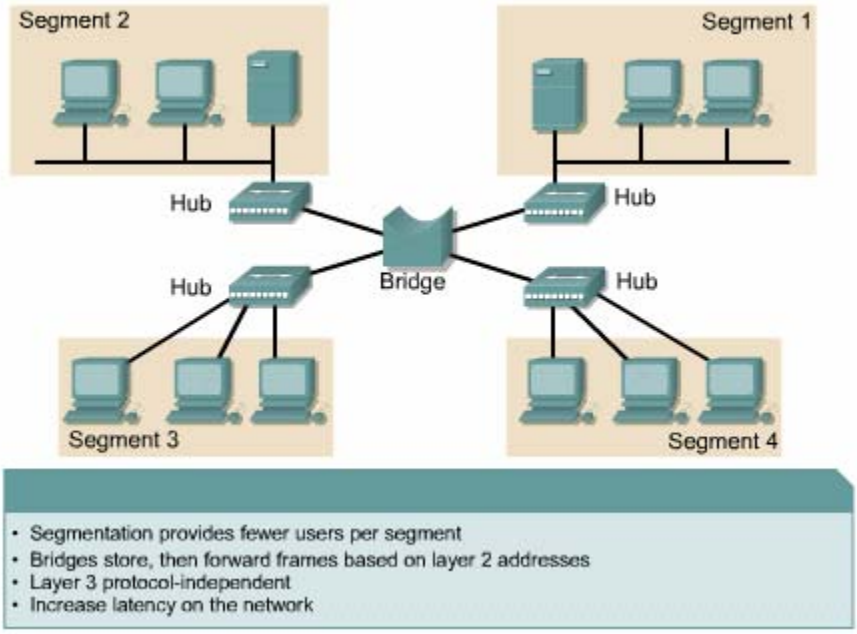
Mạng Ethernet LAN được phân đoạn bằng bridge làm giảm số lượng user trên mỗi segment, do đó sẽ tăng được lượng băng thông dành cho mỗi user.

Bridge chia mạng ra bằng cách xây dựng bảng địa chỉ trong đó cho biết địa chỉ của từng thiết bị mạng nằm trong segment nào. Khi đó, dựa vào địa chỉ MAC của frame bridge sẽ có thể quyết định chuyển frame hay không. Ngoài ra, bridge còn được xem là trong suốt đối với các thiết bị khác trong mạng.

Bridge làm tăng thời gian trễ trong mạng lên khoảng 10% đến 30%, thời gian trễ này là thời gian để bridge quyết định và thực hiện chuyển mạch dữ liệu. Bridge chuyển mạch theo dạng nhận — rồi chuyển nên nó phải nhận hết toàn bộ frame, kiểm tra địa chỉ nguồn và đích, tính toán CRC để kiểm tra lỗi frame rồi mới chuyển frame đi. Nếu port đích đang bận thì bridge sẽ tạm thời lưu frame lại cho đến khi port đích được giải phóng. Chính những khoảng thời gian này làm tăng thời gian trễ và làm chậm quá trình truyền trên mạng.



Interface	MAC address
E0	0260.8c01.1111
E0	0260.8c01.2222
E1	0260.8c01.3333
E1	0260.8c01.4444

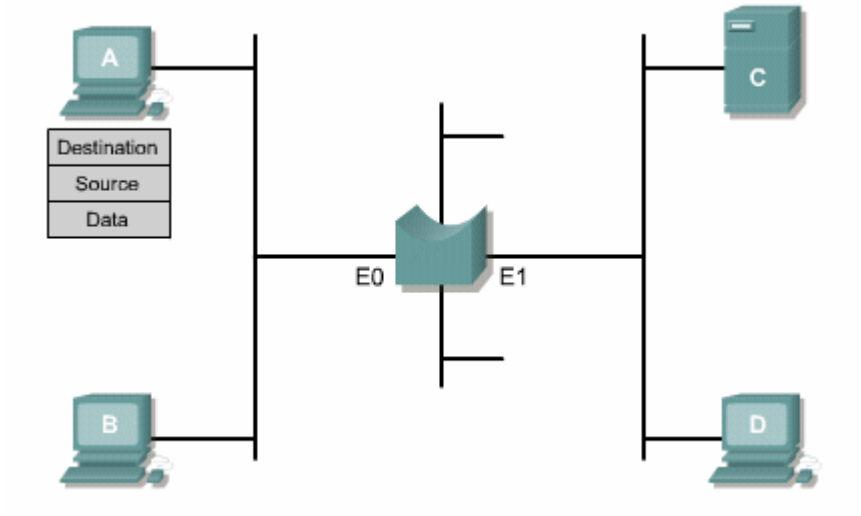


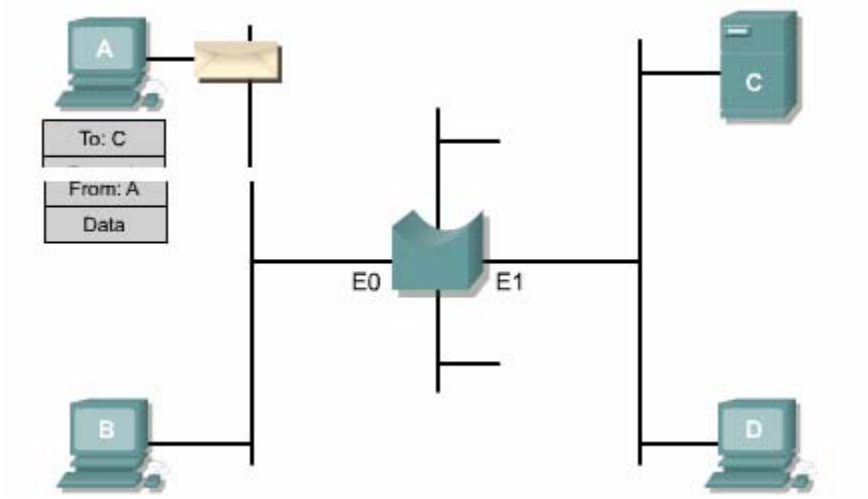
* Chia nhỏ mạng làm giảm số lượng user trên một segment.

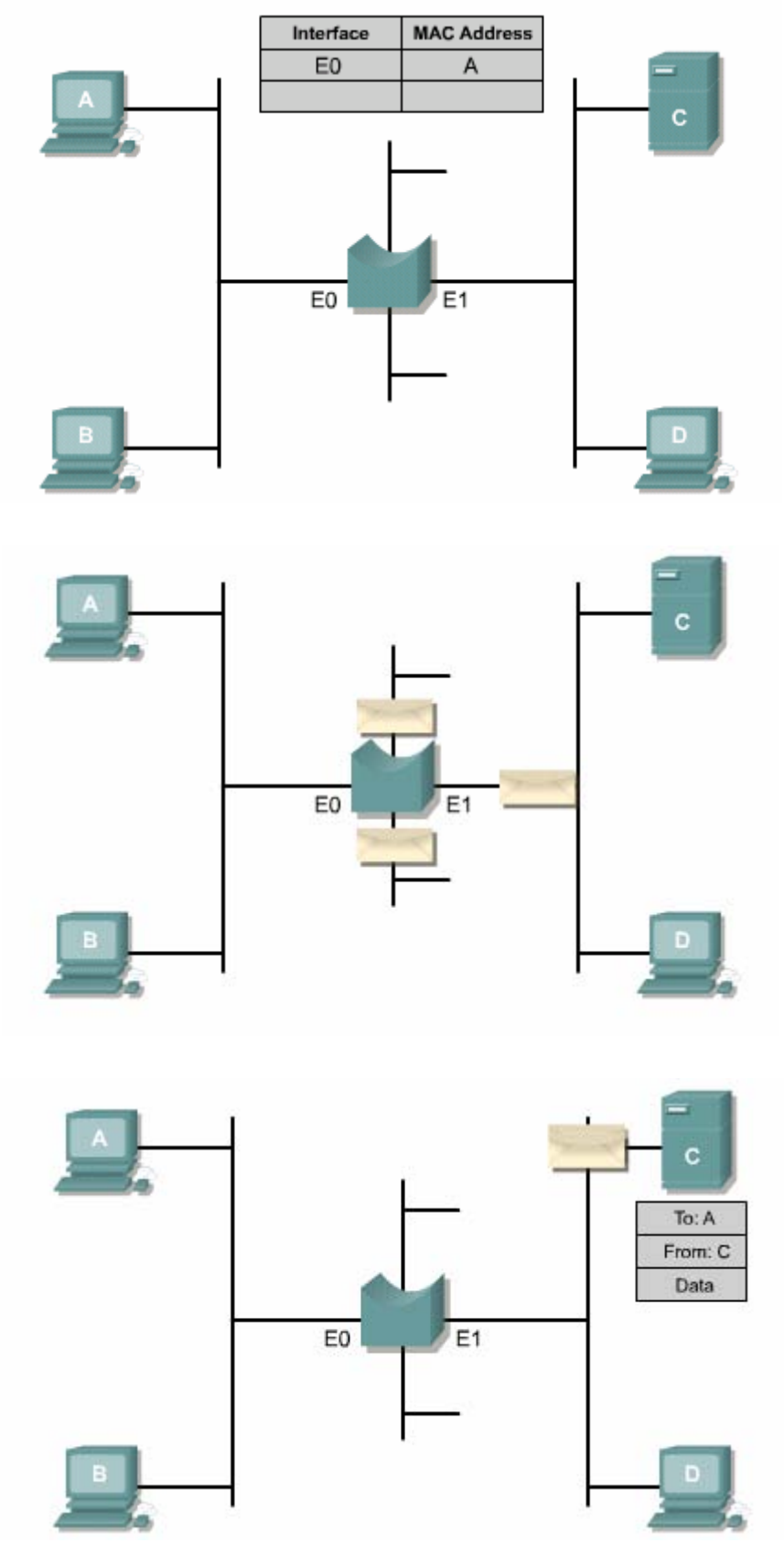
* Bridge nhận rồi chuyển frame dựa trên địa chỉ lớp 2

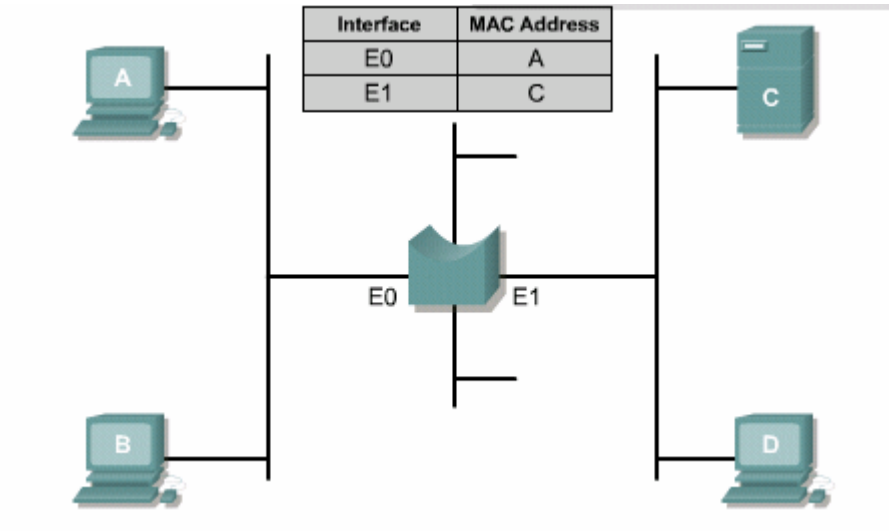
* Độc lập với giao thức lớp 3

* Làm tăng thời gian trễ trong mạng.






Interface
MAC Address
E0
A
A
C
E0
E1
B
D
A
C
E0
E1
B
D
A
C
To: A
From: C
Data
E0
E1
B
D



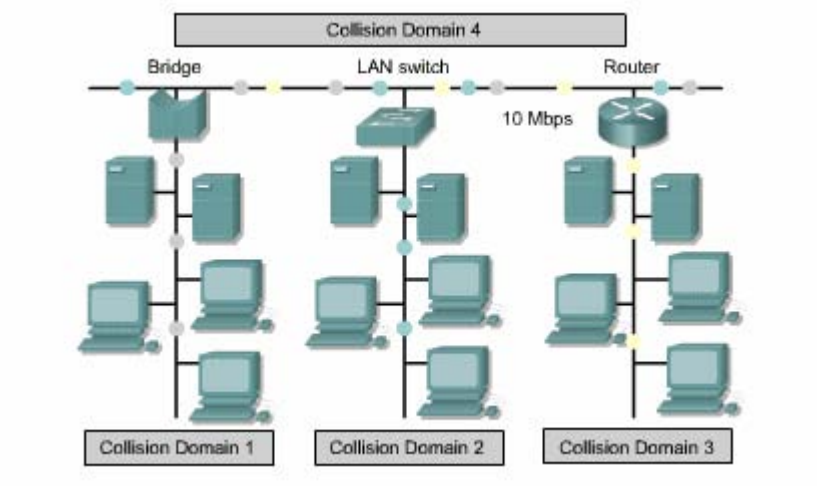
4.3.6. Tại sao phải phân đoạn mạng LAN

Có hai nguyên nhân chính để chúng ta phân đoạn mạng LAN, thứ nhất là để phân luồng giao thông giữa các segment. Thứ hai là để tăng lượng băng thông cho mỗi user bằng cách tạo miền đụng độ nhỏ hơn.

Nếu không phân đoạn mạng LAN, mạng LAN lớn nhanh chóng bị nghẽn mạch vì mật độ giao thông và đụng độ quá nhiều.

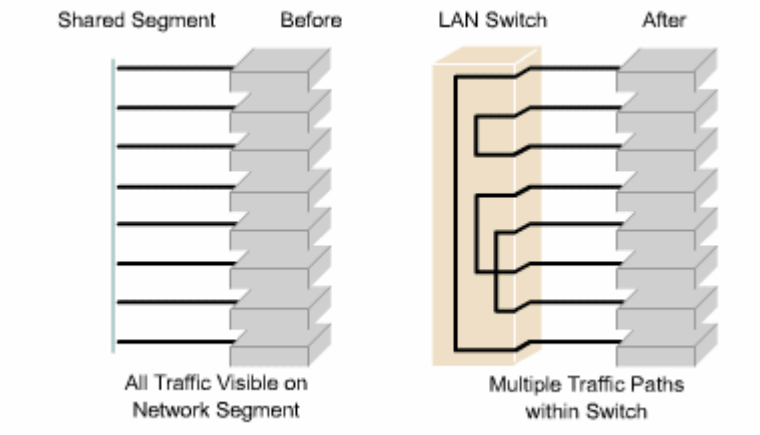
Bạn có thể sử dụng bridge, switch và router để chia nhỏ mạng LAN thành nhiều segment. Mỗi segment là một miền đụng độ riêng biệt.

Bridge và switch có nhiều ưu điểm khi sử dụng để chia một mạng lớn thành nhiều đơn vị độc lập. Bridge và switch sẽ giảm bớt lượng giao thông trên tất cả các segment vì chúng chỉ chuyển một tỉ lệ giao thông nhất định ra ngoài một segment chứ không phải toàn bộ. Tuy bridge và switch có thể thu hẹp miền đụng độ nhưng lại không thu hẹp được miền quảng bá.



Mỗi một cổng trên router kết nối vào một mạng riêng. Do đó, router sẽ chia một mạng LAN thành nhiều miền đụng độ nhỏ hơn và đồng thời thành nhiều miền quảng bá nhỏ hơn vì router không chuyển gói quảng bá trừ phi nó được cấu hình để làm như vậy.

Switch chia mạng LAN thành các miền cực nhỏ gọi là microsegment. Mỗi segment như vậy là một kết nối điểm - đến - điểm riêng biệt. Khi có hai máy cần liên lạc với nhau, switch sẽ thiết lập một mạch ảo giữa hai port của hai máy đó và mạch ảo này chỉ tồn tại trong khoảng thời gian cần thiết cho hai máy liên lạc với nhau thôi.



4.3.7. Thực hiện phân đoạn cực nhỏ (microsegment)

LAN switch được xem là bridge đa port không có miền đụng độ vì nó có thể phân đoạn cực nhỏ. Bằng cách đọc địa chỉ MAC đích, switch có thể chuyển mạch frame với tốc độ cao như bridge. Tuy nhiên switch có thể chuyển mạch frame ra port đích trước khi nhận hết toàn bộ frame giúp giảm thời gian trễ và tăng tốc độ chuyển frame.

Ethernet switch chia mạng LAN thành nhiều segment, mỗi segment là một kết nối điểm - đến - điểm và switch kết nối các segment này bằng mạch ảo. Mạch ảo chỉ được thiết lập bên trong switch và tồn tại khi hai máy cần liên lạc với nhau thôi. Nhờ vậy chuyển mạch Ethernet có thể làm tăng băng thông khả dụng trên mạng.

Mặc dù LAN switch có thể thu nhỏ kích thước miền đụng độ nhưng tất cả các host kết nối vào switch vẫn nằm trong cùng một miền quảng bá. Do đó, một gói quảng bá từ một máy vẫn được gửi đến tất cả các máy khác thông qua switch.

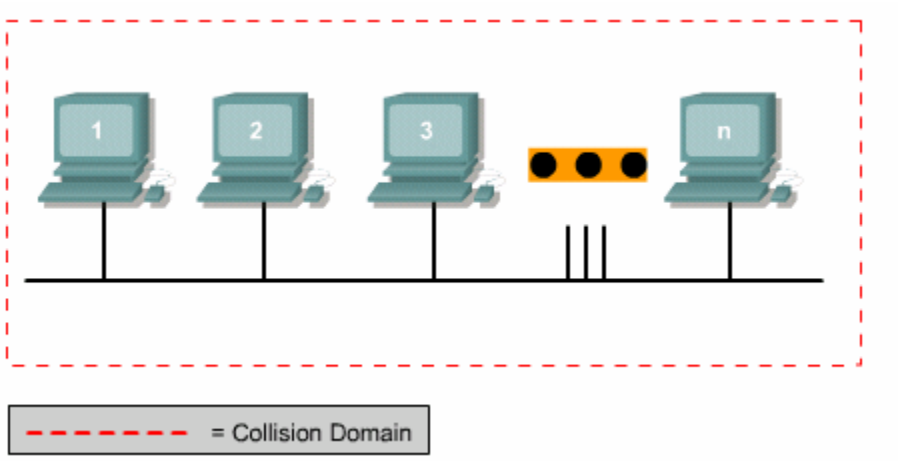
Switch là một thiết bị lớn liên kết dữ liệu giống như brige, cho phép kết nối nhiều segment LAN vật lý với nhau thành một mạng lớn. Tương tự như bridge, switch cũng chuyển gói dựa trên địa chỉ MAC. Nhưng switch chuyển mạch phần cứng chứ không chuyển mạch bằng phần mềm nên nó có tốc độ nhanh hơn. Mỗi một port của switch có thể được xem là một brige riêng biệt với trọn băng thông dành cho mỗi port đó.

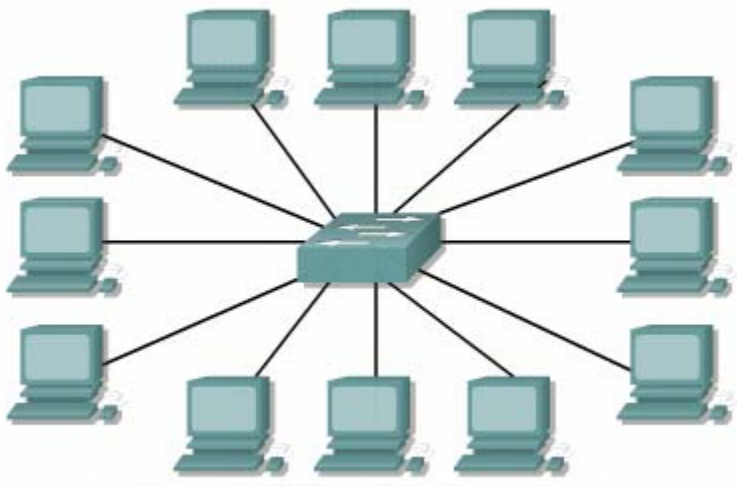
4.3.8. Switch và miền đụng độ

Nhược điểm lớn nhất của mạng Ethernet 802.3 là đụng độ. Đụng độ xảy ra khi có hai máy truyền dữ liệu đồng thời. Khi đụng độ xảy ra, mọi frame đang được truyền đều bị phá huỷ. Các máy đang truyền sẽ ngưng việc truyền dữ liệu lại và chờ

một khoảng thời gian ngẫu nhiên theo quy luật của CSMA/CD. Nếu đụng độ nhiều quá mức sẽ làm cho mạng không hoạt động được.

Miền đụng độ là khu vực mà frame được phát ra có thể bị đụng độ. Tất cả các môi trường mạng chia sẻ với nhau là các miền đụng độ. Khi kết nối một máy vào một port của switch, switch sẽ tạo một kết nối riêng biệt băng thông 10Mb/s cho máy đó. Kết nối này là một miền đụng độ riêng. Ví dụ: nếu ta kết nối máy vào một port của một switch 12 port thì ta sẽ tạo ra 12 miền đụng độ riêng biệt.

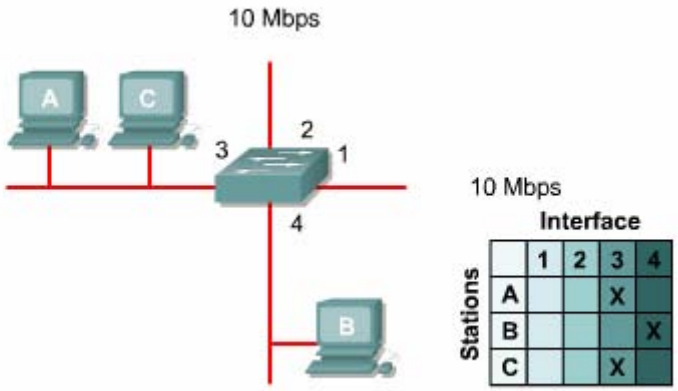




Switch xây dựng bảng chuyển mạch bằng cách địa chỉ MAC của các host kết nối trên mỗi port của switch. Khi hai host kết nối vào switch muốn liên lạc với nhau, switch sẽ tìm trong bảng chuyển mạch của nó và thiết lập kết nối ảo giữa hai port của hai host đó. Kết nối ảo này được duy trì cho đến khi phiên giao dịch kết thúc.

Trong ví dụ hình 4.3.8. c, Host B và Host C muốn liên lạc với nhau switch sẽ thiết lập một kết nối ảo giữa hai port của Host B và Host C tạo thành một microsegment. Microsegment hoạt động như một mạng chỉ có hai host duy nhất, một host gửi và một host nhận, do đó nó sử dụng được toàn bộ băng thông khả dụng trong mạng.

Switch giảm đụng độ và tăng băng thông mạng vì nó cung cấp băng thông dành riêng cho mỗi segment.



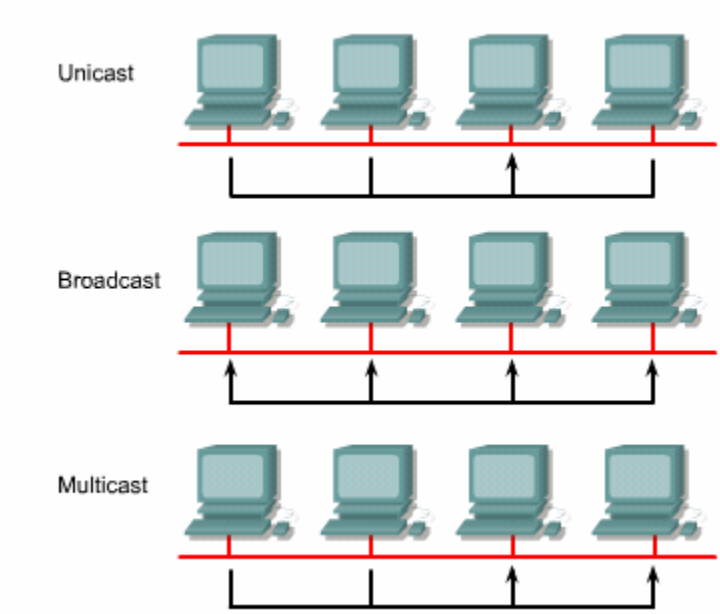
4.3.9. Switch và miền quảng bá

Thông tin liên lạc trong mạng được thực hiện theo 3 cách. Cách thông dụng nhất là gửi trực tiếp từ một máy phát đến một máy thu.

Cách thứ 2 là truyền multicast. Truyền multicast được thực hiện khi một máy muốn gửi gói cho một mạng con, hay cho một nhóm nằm trong segment.

Cách thứ 3 là truyền quảng bá. Truyền quảng bá được thực hiện khi một máy muốn gửi cho tất cả các máy khác trong mạng. Ví dụ như server giử đi một thông điệp và tất cả các máy khác trong cùng segment đều nhận được thông điệp này.

Khi một thiết bị muốn gửi một gói quảng bá lớp 2 thì địa chỉ MAC đích của frame đó sẽ là FF:FF:FF:FF:FF:FF theo số thập lục phân. Với địa chỉ đích như vậy, mọi thiết bị đều phải nhận và xử lý gói quảng bá.



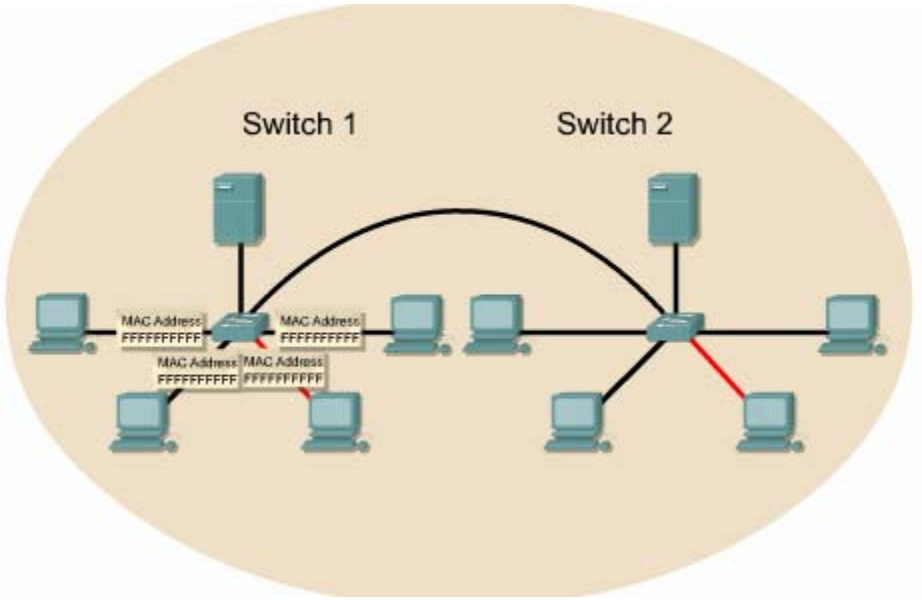
Miền quảng lớp 2 còn được xem miền quảng bá MAC. Miền quảng bá MAC bao gồm tất cả các thiết bị trong LAN có thể nhận được frame quảng bá từ một host trong LAN đó.

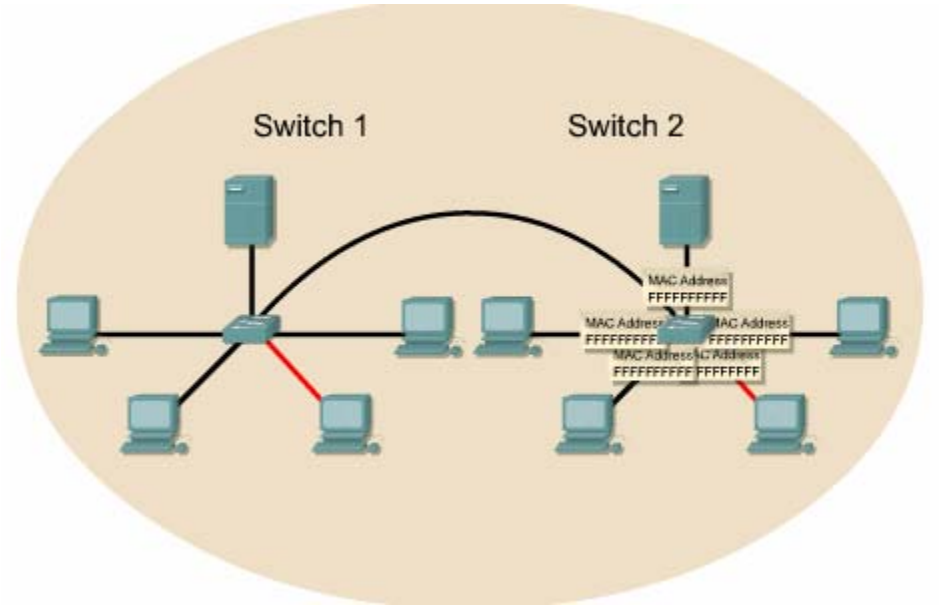
Switch là một thiết bị lớp 2. Khi switch nhận được gói quảng bá thì nó sẽ gửi ra tất cả các port của nó trừ port nhận gói vào. Mỗi thiết bị nhận được gói quảng bá

đều phải xử lý thông tin nằm trong đó. Điều này làm giảm hiệu quả hoạt động của mạng vì tốn băng thông cho mục đích quảng bá.

Khi hai switch kết nối với nhau, kích thước miền quảng bá được tăng lên. Ví dụ như hình 4.3.9.b-c, gói quảng bá được gửi ra tất cả các port của Switch. 1 Switch 1 kết nối với Switch 2. Do đó gói quảng bá cũng được truyền cho tất cả các thiết bị kết nối vào Switch 2.

Hậu quả là lượng băng thông khả dụng giảm xuống vì tất cả các thiết bị trong cùng một miền quảng bá đều phải nhận và xử lý gói quảng bá.





Router là thiết bị lớp 3. Router không chuyển tiếp các gói quảng bá. Do đó Router được sử dụng để chia mạng thành nhiều miền đụng độ và nhiều miền quảng bá.

4.3.10. Thông tin liên lạc giữa Switch và máy trạm

Khi một máy trạm được kết nối vào một LAN, nó không cần quan tâm đến các thiết bị khác cùng kết nối vào LAN đó. Máy trạm chỉ đơn giản là sử dụng NIC để truyền dữ liệu xuống môi trường truyền.

Máy trạm có thể được kết nối trực tiếp với một máy trạm khác bằng cáp chéo hoặc là kết nối vào một thiết bị mạng như hub, switch hoặc router bằng cáp thẳng.

Switch là thiết bị lớp 2 thông minh, có thể học địa chỉ MAC của các thiết bị kết nối vào port của nó. Chỉ đến khi thiết bị bắt đầu truyền dữ liệu đến switch thì nó mới học được địa chỉ MAC của thiết bị vào bảng chuyển mạch. Còn trước đó nếu thiết bị chưa hề gửi dữ liệu gì đến switch thì switch chưa nhận biết gì về thiết bị này.

Tổng kết

Sau khi kết thúc chương này, bạn cần nắm được các ý quan trọng sau:

* Lịch sử và chức năng của Ethernet chia sẻ, bán song công.

* Đụng độ trong mạng Ethernet

* Microsegment.

* CSMA/CD

* Các yếu tố ảnh hưởng đến hoạt động mạng

* Chức năng của repeater

* Thời gian truyền

* Chức năng cơ bản của Fast Ethernet

* Phân đoạn mạng bằng router, switch, và bridge

* Hoạt động cơ bản của switch

* Thời gian trễ của Ethernet switch

* Sự khác nhau giữa chuyển mạch lớp 2 và lớp 3

* Chuyển mạch đối xứng và bất đối xứng

* Bộ đệm

* Chuyển mạch kiểu store — and — forward và kiểu cut — through.

* Sự khác nhau giữa hub, bridge và switch

* Chức năng chính của switch

* Các chế độ chuyển mạch chính của switch

* Tiến trình học địa chỉ của switch

* Tiến trình lọc frame

* Miền đụng độ va miền quảng bá.

CHƯƠNG 5: Switch

Giới thiệu

Thiết kế mạng là một công việc đầy thách thức chứ không chỉ đơn giản là kết nối các máy tính lại với nhau. Một hệ thống mạng phải có nhiều đặc điểm như độ tin cậy cao, dễ dàng quản lý và có khả năng mở rộng. Để thiết kế một hệ thống mạng với đầy đủ những đặc điểm như vậy thì người thiết kế mạng cần phải biết được rằng mỗi thành phần chính trong mạng có một yêu cầu thiết kế riêng biệt.

Sự cải tiến hoạt động của các thiết bị mạng và khả năng của môi trường mạng đã làm cho công việc thiết kế mạng ngày càng trở nên khó khăn hơn. Việc sử dụng nhiều loại môi trường truyền khác nhau và kết nối LAN với nhiều mạng bên ngoài đã làm cho môi trường mạng trở nên phức tạp. Một mạng được thiết kế tốt là mạng đó phải tăng hiệu quả hoạt động hơn và ít có trở ngại khi mạng phát triển lớn hơn.

Một mạng LAN có thể trải rộng trong một phòng, trong một toà nhà hay trên nhiều toà nhà. Một nhóm các toà nhà thuộc về một tc, một đơn vị thì được xem như là một trường đại học vậy. Việc thiết kế các mạng LAN lớn cần xác định các tầng như sau:

* *Tầng truy cập*: kết nối người dùng đầu cuối vào LAN

* *Tầng phân phối*: cung cấp các chính sách kết nối giữa các người dùng đầu cuối LAN

* *Tầng trục chính*: cung cấp kết nối nhanh nhất giữa các điểm phân phối.

Mỗi một tầng trên khi thiết kế cần phải chọn lựa switch phù hợp nhất để có thể thực hiện những nhiệm vụ đặc biệt của tầng đó. Các đặc điểm, chức năng và yêu

cầu kỹ thuật của mỗi switch tuỳ thuộc vào thiết kế của mỗi tầng trong LAN. Do đó bạn cần nắm được vai trò của mỗi tầng và chọn lựa switch như thế nào cho phù hợp với từng tầng để bảo đảm hoạt động tối ưu cho người dùng trong LAN.

Sau khi hoàn tất chương trình này, các bạn có thể thực hiện được những việc sau:

* Mô tả 4 mục tiêu chính trong thiết kế LAN.

* Liệt kê các điểm quan trọng cần lưu ý khi thiết kế LAN.

* Hiểu được các bước thiết kế hệ thống LAN

* *Hiểu được các vấn đề nảy sinh trong thiết kế cấu trúc 1,2 và 3.*

* Mô tả mô hình thiết kế 3 tầng.

* Xác định chức năng của từng tầng trong mô hình 3 tầng này.

* Liệt kê các Cisco switch sử dụng cho tầng truy cập và các đặc điểm của chúng.

* Liệt kê các Cisco switch sử dụng cho tầng phân phối và các đặc điểm của chúng.

* Liệt kê các Cisco switch sử dụng cho tầng trục chính và các đặc điểm của chúng.

5.1. Thiết kế LAN

5.1.1. Các mục tiêu khi thiết kế LAN

Bước đầu tiên trong thiết kế LAN là thiết lập và ghi lại các mục tiêu của việc thiết kế. Mỗi một trường hợp hay mỗi một tổ chức sẽ có những mục tiêu riêng. Còn những yêu cầu sau là những yêu cầu thường gặp trong hầu hết các thiết kế mạng:

* **Khả năng hoạt động được**: đương nhiên yêu cầu trước nhất là mạng phải hoạt động được. Mạng phải đáp ứng được những yêu cầu công việc của người dùng, cung cấp kết nối giữa user và user, giữa user với các ứng dụng

* **Khả năng mở rộng**: mạng phải có khả năng lớn hơn nữa. Thiết kế ban đầu có thể phát triển lớn hơn nữa mà không cần những thay đổi cơ bản của toàn bộ thiết kế.

* **Khả năng thích ứng**: mạng phải được thiết kế với một cái nhìn về những kỹ thuật phát triển trong tương lai. Mạng không nên có những thành phần làm giới hạn việc triển khai các công nghệ kỹ thuật mới về sau này.

* **Khả năng quản lý**: mạng phải được thiết kế để dễ dàng quản lý và theo dõi nhằm đảm bảo hoạt động ổn định của hệ thống.

5.1.2. Những điều cần quan tâm khi thiết kế LAN

Có nhiều tổ chức muốn nâng cấp mạng LAN đã có của mình hoặc lập kế hoạch thiết kế và triển khai mạng LAN mới. Sự mở rộng trong thiết kế LAN là do sự phát triển với một tốc độ nhanh chóng của các công nghệ mới như Asynchoronous. Transfer Mode (ATM) chẳng hạn, sự mở rộng này còn là do cấu trúc phức tạp của LAN khi sử dụng chuyển mạch LAN và mạng LAN ảo (VLAN).

Để tối đa hiệu quả hoạt động và lượng băng thông khả dụng, bàn cần quan tâm những vấn đề sau khi thiết kế LAN:

* Chức năng và vị trí đặt server

* Vấn đề phát hiện đụng độ

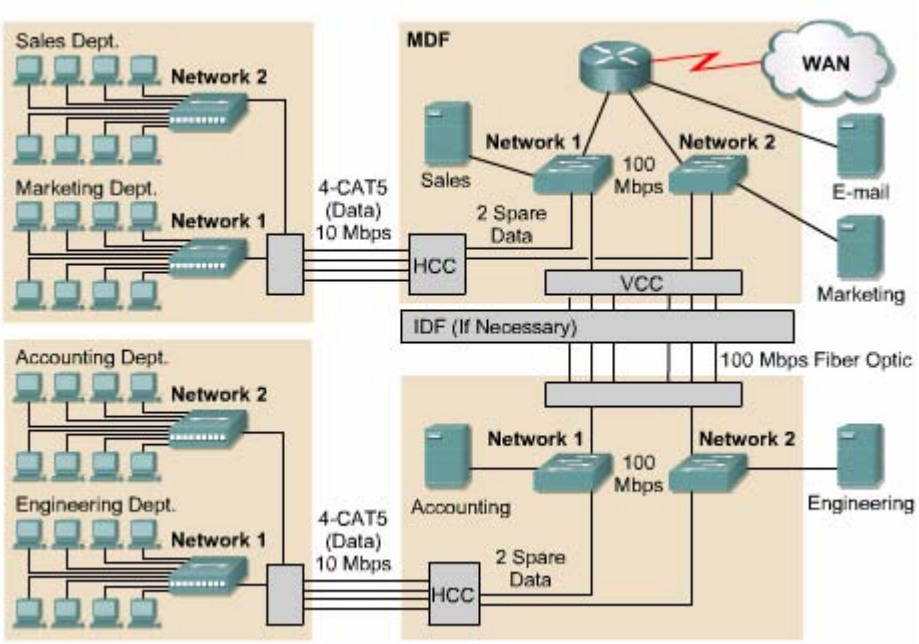
* Phân đoạn mạng

* Miền quảng bá

Server cung cấp dịch vụ chia sẻ tập tin, máy in, thông tin liên lạc và nhiều dịch vụ ứng dụng khác, server không thực hiện chức năng như một máy trạm thông thường. Server chạy các hệ điều hành đặc biệt như NetWare, Windows NT, UNIX, và Linux. Mỗi server thường giành cho một chức năng riêng như Emai hoặc chia sẻ tập tin.

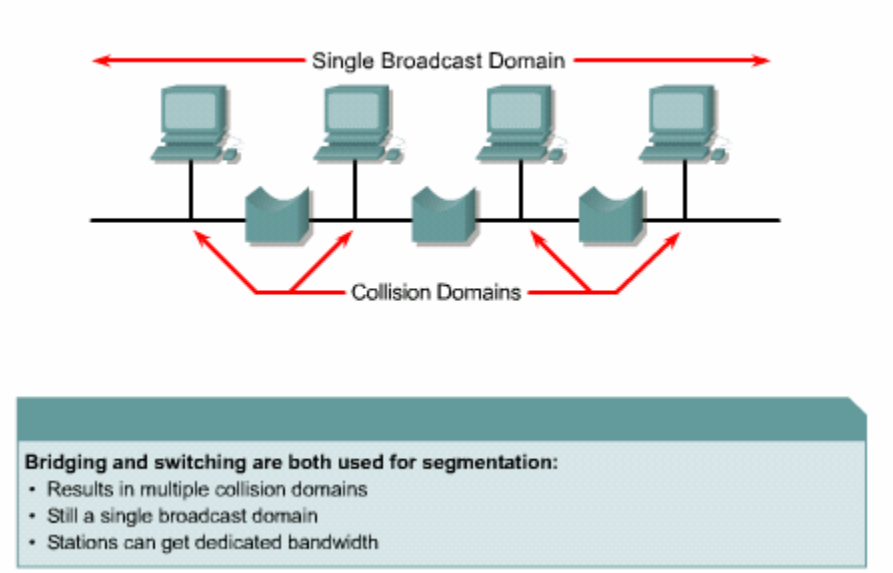
Server có thể được phân thành hai loại: Server toàn hệ thống và server nhóm. Server toàn hệ thống cung cấp dịch vụ của nó để dùng cho mọi người dùng trong hệ thống mạng. Ví dụ như Email hay DNS là những dịch vụ mà mọi người trong tổ chức đều cần sử dụng vì tính chất tập trung của những dịch vụ này. Còn server nhóm thì chỉ cung cấp dịch vụ để phục vụ cho một nhóm người dùng cụ thể. Ví dụ như những dịch vụ xử lý và chia sẻ tập tin có thể chỉ phục vụ cho một nhóm người dùng nào đó thôi.

Server toàn hệ thống nên đặt ở trạm phân phối chính (MDF — Main distribution facility). Giao thông hướng đến server toàn hệ thống chỉ đi qua MDF thôi chứ không đi qua các mạng khác. Nơi đặt lý tưởng cho các server nhóm là ở trạm phân phối trung gian gần nhóm người dùng mà nó phục vụ nhất. Như vậy giao thông đến các server này chỉ đi trong mạng riêng của IDF đó mà không ảnh hưởng đến các mạng khác. LAN switch lớp 2 đặt trong MDF và các IDF nên có đường 100 Mb/s hoặc hơn dành cho các server.



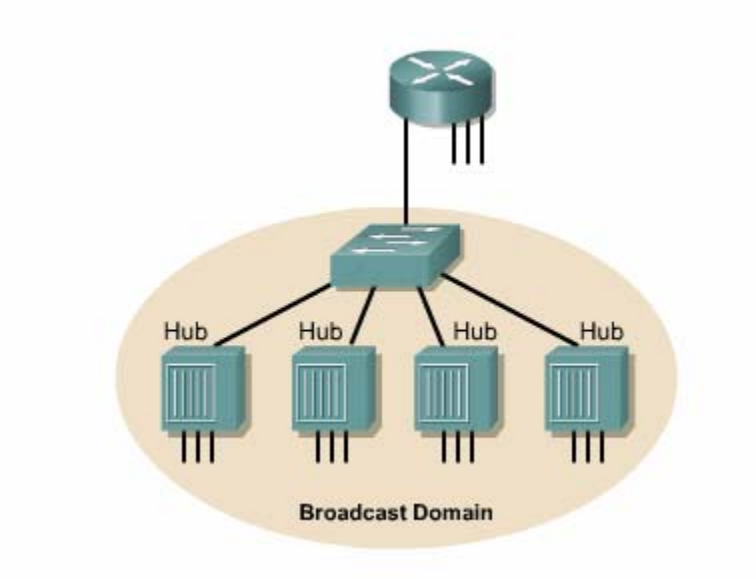
Ethernet node sử dụng CSMA/CD. Mỗi node đều phải chú ý đến tất cả các node khác khi truy cập vào môi trường chia sẻ hay còn gọi là miền đụng độ. Nếu hai node truyền dữ liệu cùng một lúc thì đụng độ sẽ xảy ra. Khi đụng độ xảy ra, những dữ liệu đang trên đường truyền sẽ bị huỷ bỏ và một tín hiệu báo nghẽn được phát ra trong mọi máy trong miền đụng độ. Sau đó các node phải chờ trong một khoảng thời gian ngẫu nhiên rồi mới truyền lại dữ liệu của mình. Đụng độ xảy ra nhiều quá có thể giảm lượng băng thông khả dung trong mạng xuống khoảng 35 — 40%.

Do đó chúng ta cần chia nhỏ một miền đụng độ thành nhiều miền đụng độ nhỏ hơn, giúp giảm miền đụng độ trên mỗi miền và tăng lượng băng thông khả dụng cho mỗi user. Bạn có thể sử dụng các thiết bị lớp 2 như brigde và switch để chia 1 LAN thành nhiều miền đụng độ nhỏ, còn router được sử dụng để chia nhỏ mạng ở lớp 3.



Gói quảng bá là gói dữ liệu có địa chỉ MAC đích là: FF: FF: FF:FF:FF:FF. Miền quảng bá là tập hợp các thiết bị có thể nhận được gói quảng bá xuất phát từ bất kỳ thiết bị nào trong tập hợp đó. Tất cả các thiết bị nhận được đều phải xử lý thông tin trong đó, việc xử lý gói quảng bá này làm giảm lượng băng thông của mỗi host.

Thiết bị lớp 2 có thể thu nhỏ kích thước miền đụng độ nhưng khôngthể thu nhỏ kích thước của miền quảng bá. Chỉ có router mới có thể vừa thu nhỏ kích thước miền đụng độ vừa thu nhỏ kích thước miền quảng bá ở lớp 3.



5.1.3. Phương pháp thiết kế LAN

Để có 1 mạng LAN hoạt động hiệu quả và đáp ứng được nhu cầu của người sử dụng, LAN cần được thiết kế và triển khai theo 1 kế hoạch với đầy đủ hệ thống các bước sau:

* Thu thập các yêu cầu và mong đợi của người sử dụng mạng

* Phân tích các dữ liệu và các yêu cầu thu thập được

* Thiết kế cấu trúc LAN lớp 1, 2 và 3

* Ghi nhận lại các bước triển khai mạng vật lý và logic

Quá trình thu thập thông tin sẽ giúp cho bạn xác định và làm sáng tỏ những vấn đề hiện tại của hệ thống mạng. Những thông tin này có thể bao gồm lịch sử phát triển tổ chức, tình trạng hiện tại, dự án phát triển, chính sách hoạt động và quản lý, hệ thống văn phòng và phương thức làm việc, quan điểm của những người sẽ sử dụng mạng LAN. Sau đây là những câu bạn nên hỏi khi thu thập thông tin:

* Những người nào sẽ sử dụng hệ thống mạng

* Kỹ năng của họ ở mức nào?

* Quan điểm của họ về máy tính và các ứng dụng máy tính là gì?

* Các văn bản chính sách về tổ chức được phát triển như thế nào?

* Có dữ liệu nào cần công bố trong phạm vi giới hạn không?

* Có hoạt động nào cần giới hạn không?

* Những giao thức nào được phép chạy trên mạng?

* Cần hỗ trợc các máy tính để bàn không?

* Ai là người chịu trách nhiệm về địa chỉ LAN? Đặt tên, thiết kế cấu trúc và cấu hình?

* Tài nguyên về nhân lực, phần cứng và phần mềm của tổ chức là những gì?

Những nguồn tài nguyên này hiện đang được liên kết và chia sẻ như thế nào?

Nguồn tài chính mà tổ chức có thể dành cho mạng là bao nhiêu?

Ghi nhận lại toàn bộ các yêu cầu trên cho phép chúng ta ước lượng được chi phí và khoảng thời gian để triển khai dự án thiết kế LAN. Một điểm rất quan trọng mà bạn cần nắm được là những vấn đề hoạt động đang tồn tại trong hệ thống mạng đã có.

Tính khả dụng đo lường mức độ hữu ích của hệ thống mạng, có nhiều yếu tố ảnh hưởng đến tính khả dụng, bao gồm những yếu tố sau:

* Thông lượng

* Thời gian đáp ứng

* Khả năng truy cập vào tài nguyên mạng

Mỗi khách hàng đều có định nghĩa khác nhau về tính khả dụng của mạng. Ví dụ: khách hàng cần truyền thoại và video trên mạng. Những dịch vụ này đòi hỏi nhiều băng thông hơn lượng băng thông đang có trên mạng. Để tăng lượng băng thông khả dụng, cần phải thêm nhiều tài nguyên vào mạng nhưng như vậy thì chi phí sẽ tăng theo. Do đó thiết kế mạng phải làm sao cung cấp được khả năng sử dụng lớn nhất với chi phí thấp nhất.

Sau khi phân tích về tính khả dụng, bước tiếp theo là phân tích các yêu cầu của hệ thống mạng và người sử dụng mạng đó. Ví dụ khi càng có nhiều ứng dụng mạng về thoại và video thì nhu cầu về băng thông mạng càng tăng lên nhiều hơn.

Một thành phần nữa trong bước phân tích này là đánh giá yêu cầu của người dùng. Một mạng LAN mà không thể cung cấp thông tin nhanh chóng và chính xác cho người sử dụng là một mạng LAN vô dụng. Do đó yêu cầu của tổ chức và yêu cầu của các nhân viên trong tổ chức đó phải gặp nhau.

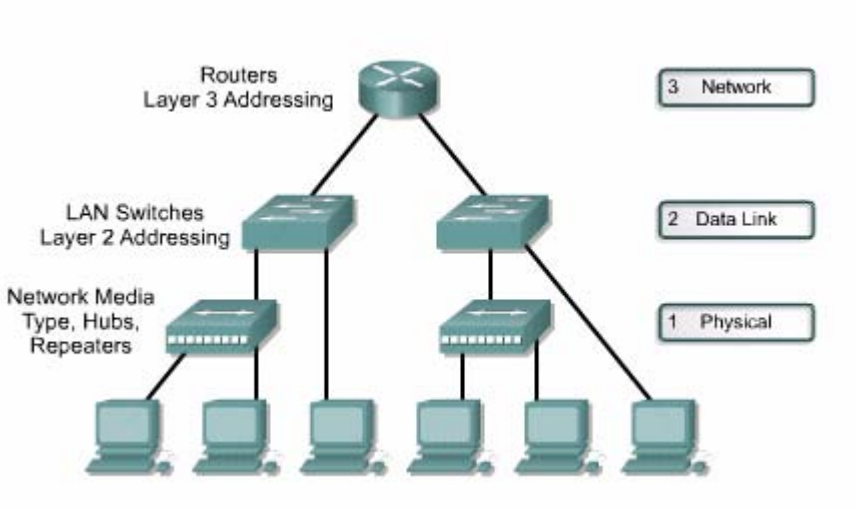
Bước kế tiếp là quyết định cấu trúc tổng thể của LAN thể thoả mãn mọi yêu cầu của người sử dụng. Trong giáo trình này, chúng ta chỉ tập trung vào cấu trúc hình Sao và hình sao mở rộng. Cấu trúc hình Sao và hình sao mở rộng sử dụng kỹ thuật Ethernet 802,3 CSMA/CD. Cấu trúc hình Sao CSMA/CD đang là cấu hình thống trị hiện nay.

Thiết kế cấu trúc LAN có thể được phân thành 3 bước theo 3 mô hình OSI như sau:

- Lớp Mạng
- Lớp liên kết dữ liệu
- Lớp vật lý

Bước cuối cùng trong thiết kế LAN là ghi nhận lại các cấu trúc vật lý và luận lý của hệ thống mạng. Cấu trúc vật lý của mạng là sơ đồ kết nối vật lý của các

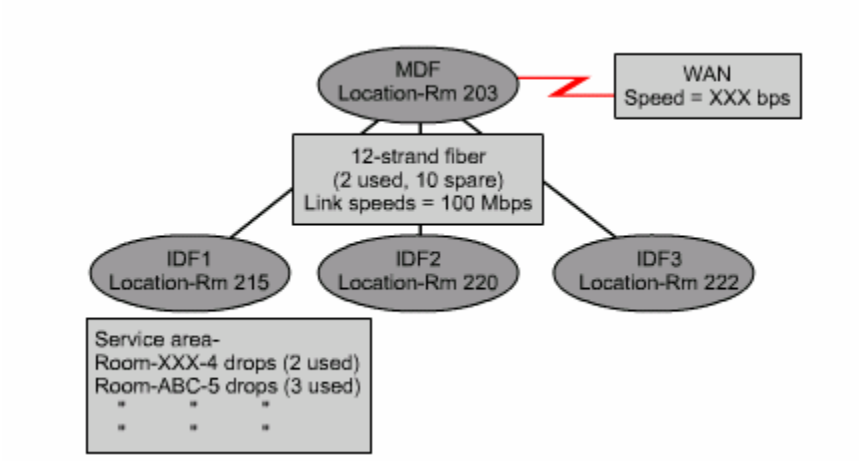
thành phần trong mạng LAN. Còn thiết kế luận lý là cách phân dòng dữ liệu trong mạng. Nó cũng bao gồm cả sơ đồ tên và địa chỉ được sử dụng trong thiết kế LAN.

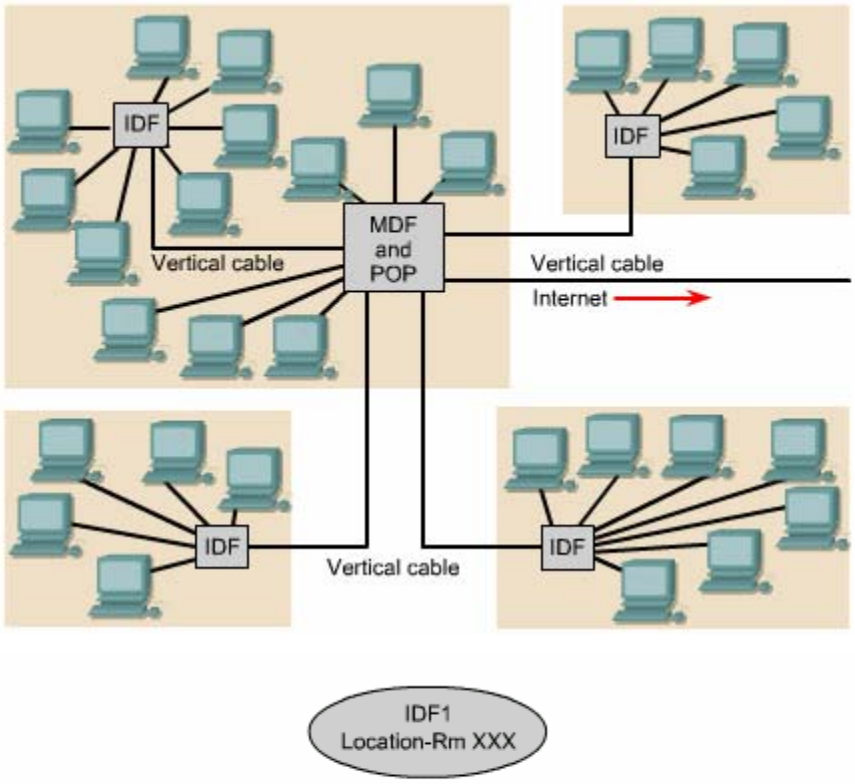


Sơ đồ thiết kế LAN

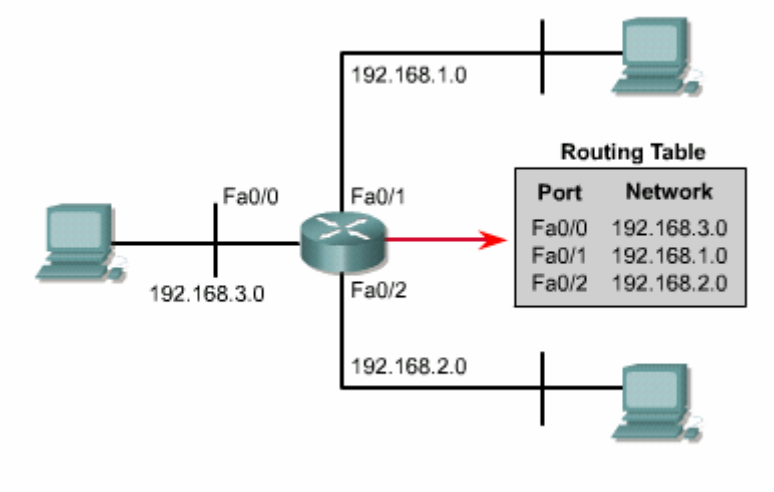
Hồ sơ thiết kế LAN bao gồm những thành phần quan trọng sau:

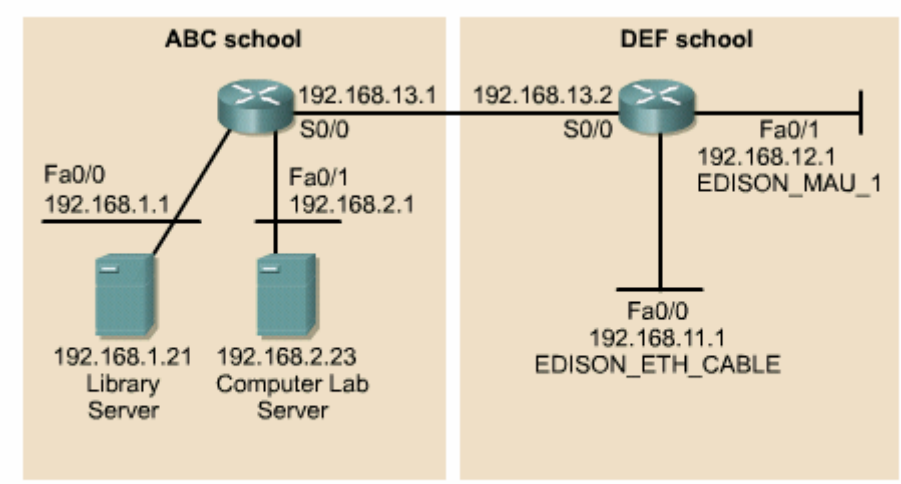
- Sơ đồ cấu trúc theo lớp OSI
- Sơ đồ LAN luận lý
- Sơ đồ LAN vật lý
- Bảng ánh xạ vị trí, địa chỉ và tình trạng sử dụng của từng thiết bị trong LAN (cut - sheet)
- Sơ đồ VLAN luận lý
- Sơ đồ luận lý lớp 3
- Sơ đồ địa chỉ





Connection	Cable ID	Cross Connection Paired#/Port#	Type of Cable	Status
IDF1 to Rm 203	203-1	HCC1/Port 13	Category 5 UTP	Used
IDF1 to Rm 203	203-2	HCC1/Port 14	Category 5 UTP	Not Used
IDF1 to Rm 203	203-3	HCC2/Port 3	Category 5 UTP	Not Used
IDF1 to MDF	IDF1-1	VCC1/Port 1	Multimode fiber	Used
IDF1 to MDF	IDF1-2	VCC1/Port 2	Multimode fiber	Used



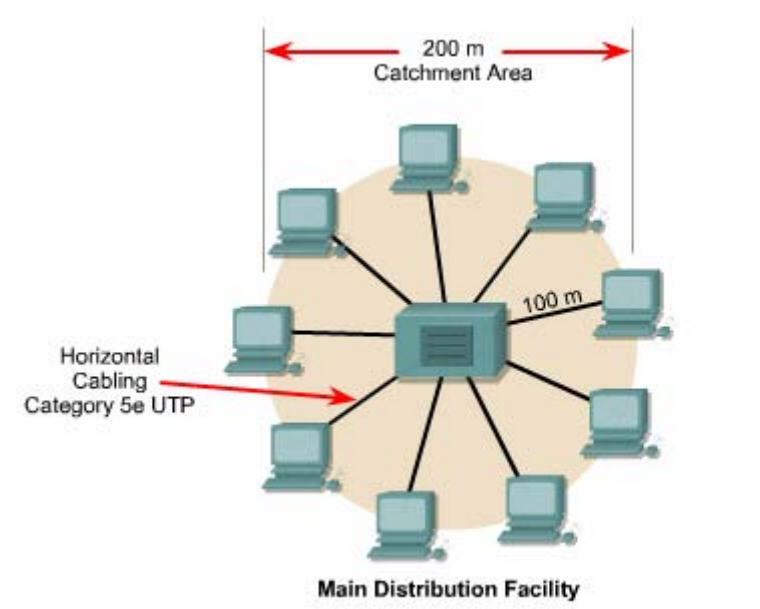


Một trong những phần quan trọng nhất mà bạn cần quan tâm khi thiết kế mạng là cáp vật lý. Hiện nay, hầu hết cáp sử dụng cho LAN đều dựa trên công nghệ Fast Ethernet. Fast Ethernet là Ethernet được nâng cấp từ 10Mb/s lên 100 Mb/s và có khả năng hoạt động song công. Fast Ethernet vẫn sử dụng cấu trúc luận lý hình bus hướng quảng bá chuẩn Ethernet của 10BASE — T và phương pháp CSMA/CD cho địa chỉ MAC.

Những vấn đề trong thiết kế lớp 1 bao gồm loại cáp sử dụng, thường là cáp đồng hay cáp quang và cấu trúc tổng thể của hệ thống cáp. Mỗi trường cáp lớp 1 có nhiều loại như 10/100 BASE — TX CAT5, 5e hoặc 6 UTP, STP, 100 BASE — FX cáp quang và chuẩn TIA/EIA — 568 — A về cách bố trí và kết nối dây.

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

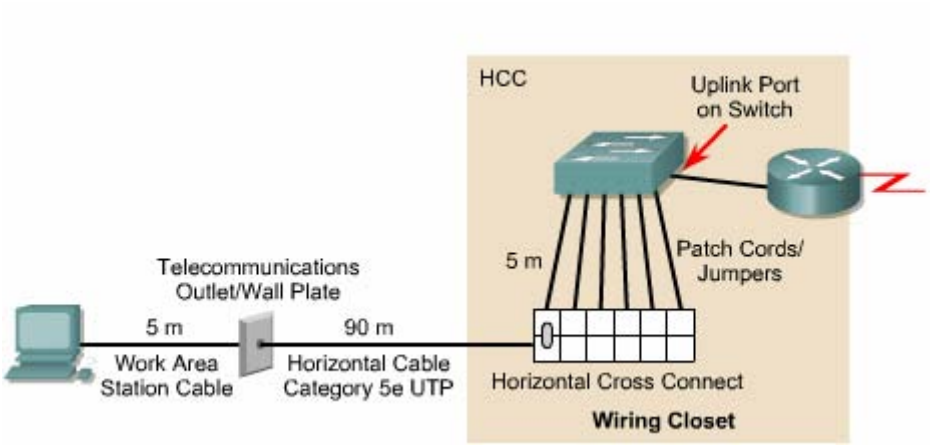
Bạn nên đánh giá cẩn thận điểm mạnh điểm mạnh và yếu của cấu trúc mạng vì một hệ thống mạng tồn tại với chính hệ thống cáp bên dưới của nó. Hầu hết các sự cố mạng đều xảy ra ở lớp 1. Do đó khi có bất kỳ dự định thay đổi quan trọng nào thì bạn cần kiểm tra toàn bộ hệ thống cáp để xác định khu vực cần nâng cấp hoặc đi dây lại.



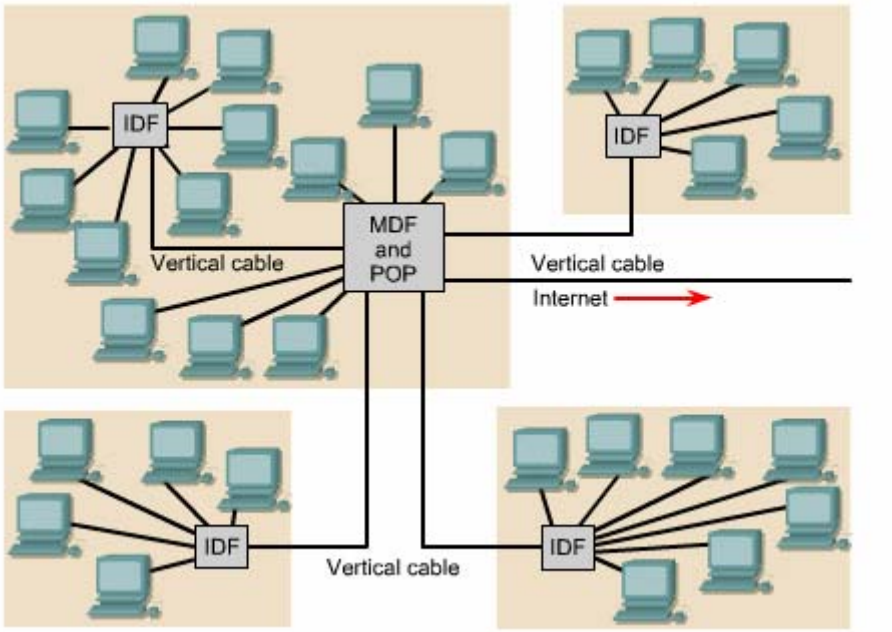
Bạn nên sử dụng cáp quang cho các đường trục chính trong thiết kế cáp UTP CAT 5e nên sử dụng cho đường cáp horizotal, là những đường cáp nối từ hộp cắm dây của mỗi host kéo về trạm tập trung dây. Việc nâng cấp cáp cần phải được thực hiện ưu tiên so với các thay đổi cần thiết khác. Ngoài ra bạn cần đảm bảo là toàn bộ hệ thống cáp tương thích với chuẩn công nghiệp như chuẩn TIA/EIA — 568 — A chẳng hạn.

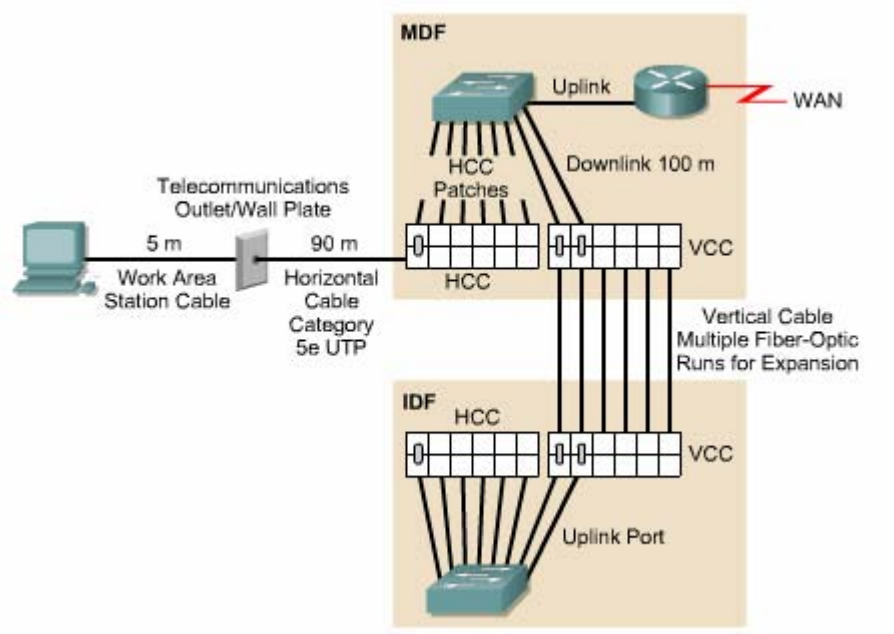
Chuẩn TIA/EIA — 568 — A quy định rằng mọi thiết bị trong mạng cần được kết nối vào một vị trí trung tâm bằng cáp horizontal. Khoảng cách giới hạn của cáp CAT 5e là UTP là 100m.

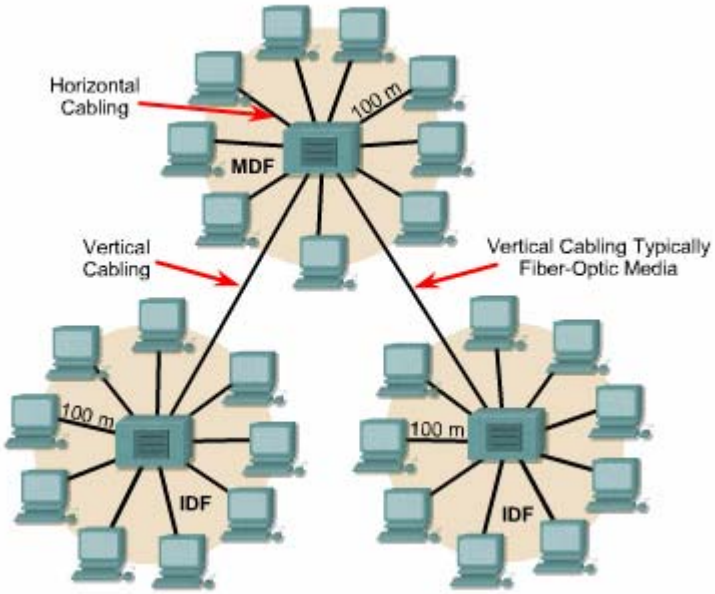
Trong cấu trúc hình sao đơn chỉ có một tủ nối dây là MDF. Từ hộp cắm dây của mỗi host (Outlet) ta kép cáp horizaontal về MDF rồi kết nối vào các bộ tập trung dây HCC (Horizontal Cross Connect patch panel) đặt trong MDF. Patch cord là những sợi cáp ngắn được sử dụng để kết nối cáp horizontal vào por của switch lớp 2. Tuỳ theo phiên bản switch, đường uplink sẽ kết nối từ switch vào cổng Ethernet của router lớp 3 bằng cáp patch cord. Như vậy là host đầu cuối đã có kết nối vật lý hoàn chỉnh vào cổng của router.

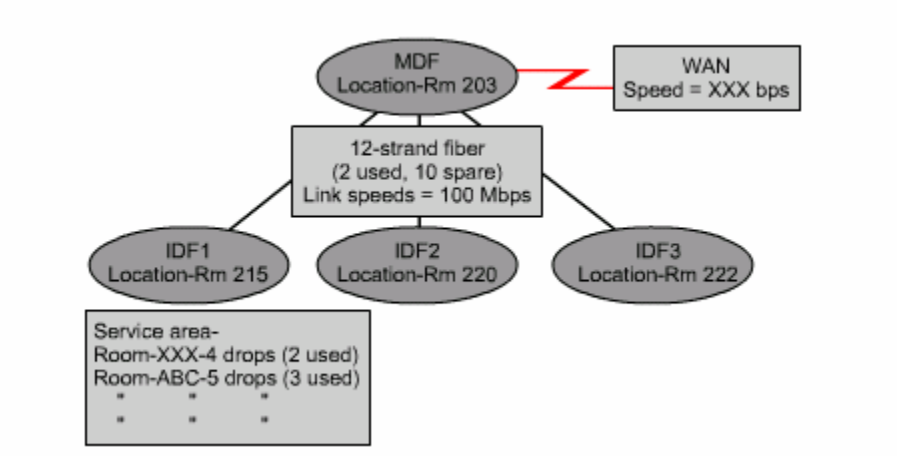


Khi hệ thống mạng lớn, có nhiều host nằm ngoài giới hạn 100m của cáp CAT 5e UTP thì bạn cần có nhiều hơn một tủ nối dây. Bằng cách thiết lập nhiều tủ nối dây bạn sẽ tạo ra nhiều vùng bao phủ. Tủ nối dây thứ hai được gọi là trạm phân phối trung gian IDF (Intermediate distribution facilities). Chuẩn TIA/EIA — 568 — A quy định rằng IDF được kết nối vào MDF bằng cáp vertical hay còn gọi là cáp trục chính (backbone). Cáp vertical được kéo từ IDF đến MDF và được kết nối vào bộ tập trung cáp VCC (Vertical Cros Connect patch panel) đặt trong MDF. Chúng ta thường sử dụng cáp quang cho đường cáp vertical vì đường cáp này thường dài hơn giới hạn 10 m của cáp CAT 5e UTP.




MDF
Uplink
WAN
HCC
Patches
Downlink 100 m
Telecommunications
Outlet/Wall Plate
5 m
Work Area
Station Cable
90 m
Horizontal
Cable
Category
5e UTP
HCC
VCC
Vertical Cable
Multiple Fiber-Optic
Runs for Expansion
IDF
HCC
VCC
Uplink Port


Horizontal
Cabling
100 m
MDF
Vertical
Cabling
Vertical Cabling Typically
Fiber-Optic Media
100 m
IDF
100 m
IDF



Connection	Cable ID	Cross Connection Paired#/Port#	Type of Cable	Status
IDF1 to Rm 203	203-1	HCC1/Port 13	Category 5e UTP	Used
IDF1 to Rm 203	203-2	HCC1/Port 14	Category 5e UTP	Not Used
IDF1 to Rm 203	203-3	HCC2/Port 3	Category 5e UTP	Not Used
IDF1 to MDF	IDF1-1	VCC1/Port 1	Multimode fiber	Used
IDF1 to MDF	IDF1-2	VCC1/Port 2	Multimode fiber	Used

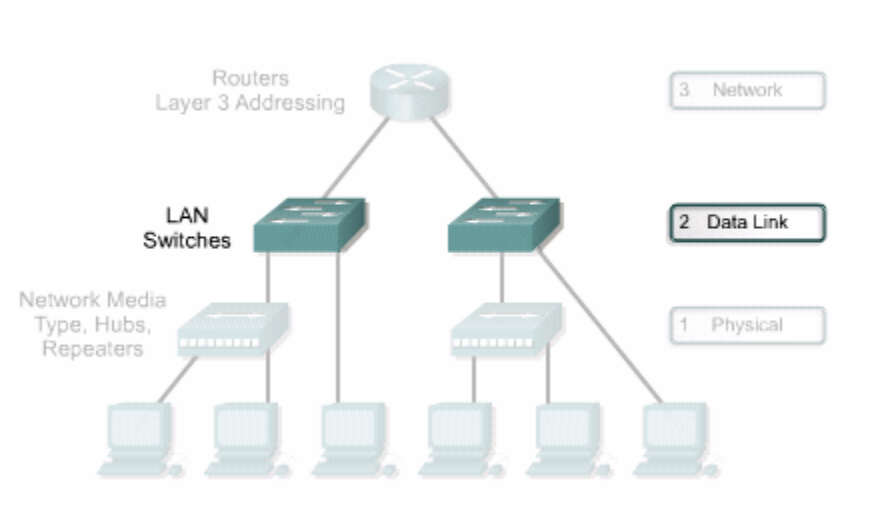
Sơ đồ luận lý là sơ đồ cấu trúc mạng nhưng không mô tả chính xác các chi tiết lắp đặt đường cáp. Sơ đồ luận lý chỉ là sơ đồ đường đi cơ bản của LAN bao gồm những thành phần sau:

- Xác định vị trí đặt MDF và IDF
- Ghi lại loại cáp và số lượng sử dụng để kết nối các IDF và MDF
- Ghi lại số lượng cáp để dành để tăng băng thông giữa các tủ nối dây. Ví dụ: nếu cáp vertical giữa IDF 1 và MDF chạy hết 80% thì sẽ sử dụng thêm 2 cặp cáp nữa để tăng gấp đôi bằng thông.
- Cung cấp hồ sơ chi tiết về tất cả các cáp trong hệ thống, chỉ số danh định và số port của chúng trên HCC hoặc VCC.

Sơ đồ luận lý rất quan trọng khi xử lý sự cố về kết nối mạng. Ví dụ như trên hình 5.1.4.h-i: nếu phòng 203 bị mất kết nối thì bằng cách kiểm tra trong cut sheet chúng ta sẽ xác định được cáp nối từ phòng nay đến IDF là cáp số 203 — 1 và kết nối vào port số 13 trên HCC trong IDF. Sử dụng đồng hồ đo cáp chúng ta sẽ xác định đoạn cáp này có bị hư hỏng về mặt vật lý hay không. Nếu có thì chúng ta có thể sử dụng 2 sơi cáp dự phòng còn lại là 203 — 2 hoặc 203 —3 để thiết lập lại kết nối trong thời gian chờ sửa chữa cáp 203 — 1.

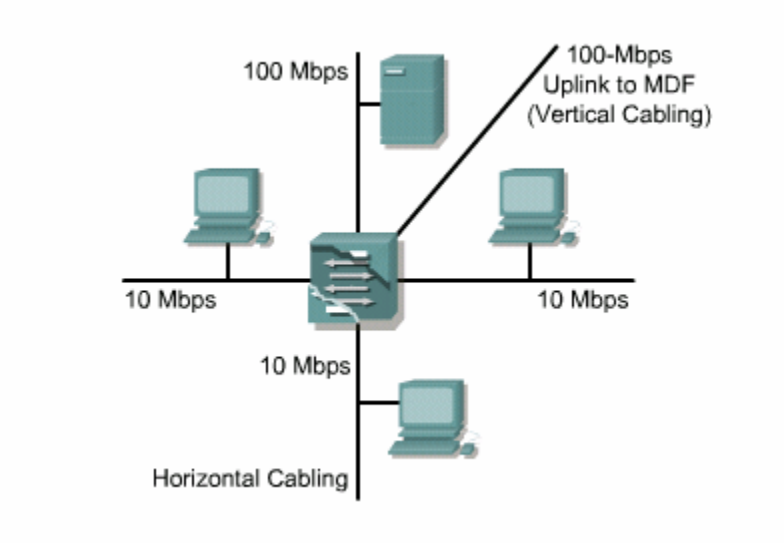
5.1.5. Thiết kế lớp 2.

Mục đích của thiết bị lớp 2 trong mạng là điều khiển luồng, phát hiện lỗi, sửa lỗi và giảm nghẽn mạch. Hai thiết bị lớp 2 phổ biến nhất là bridge và switch. Thiết bị lớp 2 sẽ quyết định kích thước miền đụng độ.

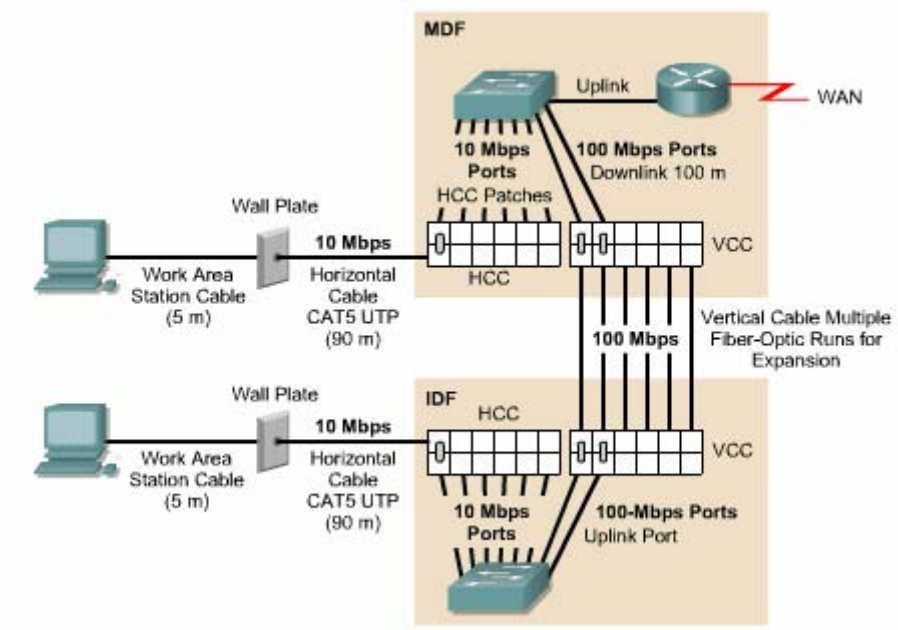


Đụng độ và kích thước miền đụng độ là hai yếu tố ảnh hưởng xấu đến hiệu quả hoạt động của mạng. Do đó chúng ta nên chia nhỏ mạng thành các miền đụng độ của mạng. Do đó chúng ta nên chia nhỏ mạng thành các miền đụng độ cực nhỏ (microsegment) bằng switch và bridge để giảm đụng độ và kích thước miền đụng độ. Chúng ta có thể sử dụng switch kết hợp với hub để cung cấp mức độ hoạt động hợp lý cho mỗi nhóm user và server khác nhau.

Một đặc điểm quan trọng của LAN switch là nó có thể phân bổ băng thông trên từng port. Nhờ đó nó có thể dành nhiều băng thông hơn cho đường vertical, uplink hoặc đường kết nối vào server. Loại chuyển mạch như vậy gọi là chuyển mạch bất đối xứng . Chuyển mạch bất đối xứng thực hiện chuyển mạch giữa các port có băng thông không bằng nhau, ví dụ từ port 10Mb/s sang port 100Mb/s.

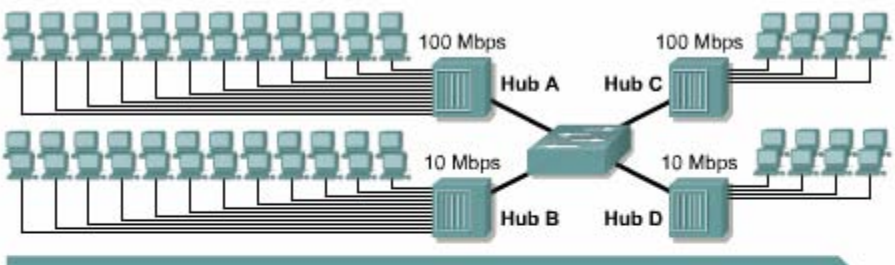


Đường vertical kết nối từ IDF đến MDF để truyền dữ liệu giữa MDF và IDF. Dung lượng đường vertical thường lớn hơn đường horizontal. Đường horizontal nối giữa IDF và máy trạm thường sử dụng cáp CAT 5e UTP và dài không quá 100mét. Trong môi trường mạng thông thường, đường horizontal có băng thông 10 Mb/s và sử dụng switch chuyển mạch bất đối xứng để kết hợp port 10 Mb/s và 100 Mb/s.



Nhiệm vụ tiếp theo là quyết định số lượng port 10Mb/s và 100 Mb/s cần sử dụng trong MDF và mỗi IDF. Ta có thể quyết định số lượng này dựa vào yêu cầu của user về số lượng cáp horizontal đi vào mỗi phòng và tổng số lượng cáp đổ vào mỗi vùng bao phủ. Đồng thời chúng ta cũng tính luôn số lượng đường vertical cần thiết . Ví dụ: user yêu cầu phải có 4 đường horizontal đi vào mỗi phòng. Mỗi một IDF phục vụ cho một vùng bao phủ gồm 18 phòng. Như vậy cần tổng cộng là 4* 18 = 72 port trên LAN switch trong mỗi IDF.

Kích thước miền đụng độ xác định bởi số lượng host được kết nối vật lý vào cùng một port của switch. Từ đó ta có thể xác định lượng băng thông khả dụng cho từng host. Trong điều kiện lý tưởng là ta kết nối một host vào một port của switch tạo thành một microsegment chỉ bao gồm host nguồn và host đích khi có bất kỳ hai host nào thực hiện thông tin liên lạc với nhau. Do đó, không có đụng độ trong microsegment. Nếu không đủ điều kiện để làm vậy thì bạn có thể sử dụng hub để kết nối nhiều host vào một port của switch. Như vậy tất cả các host kết nối vào hub trên cùng một port của switch chia sẻ cùng một băng thông và cùng một miền đụng độ. Do đó đụng độ có thể xảy ra.



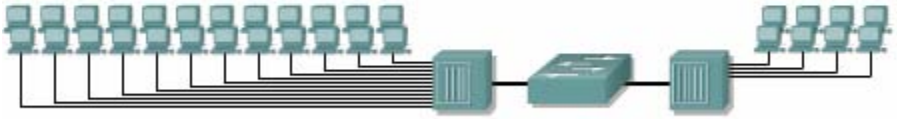
Hub A:
- Collision domain = 24 hosts
- Bandwidth average = 100 Mbps/24 hosts = 4.167 Mbps per host

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

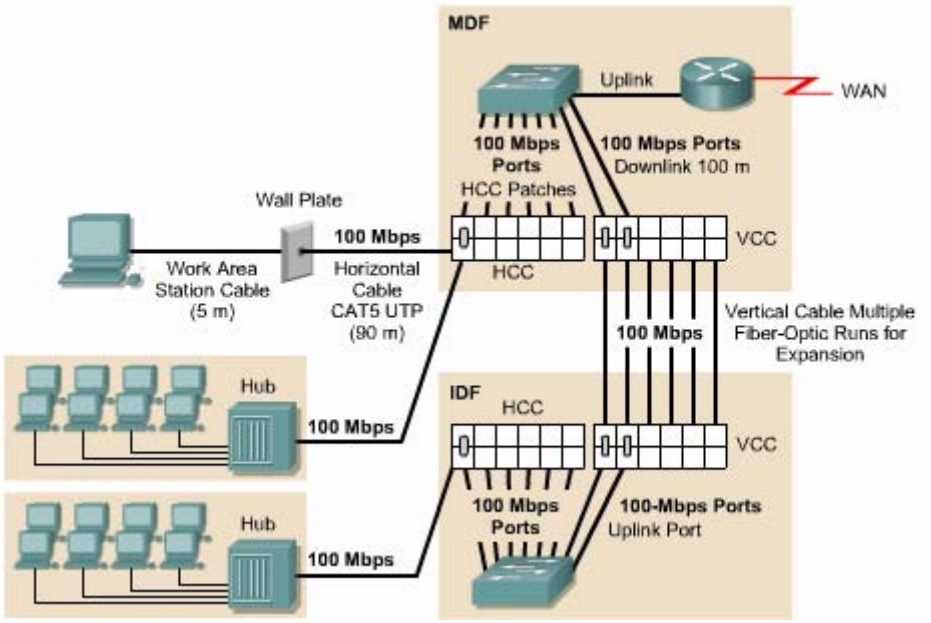
Switched LAN

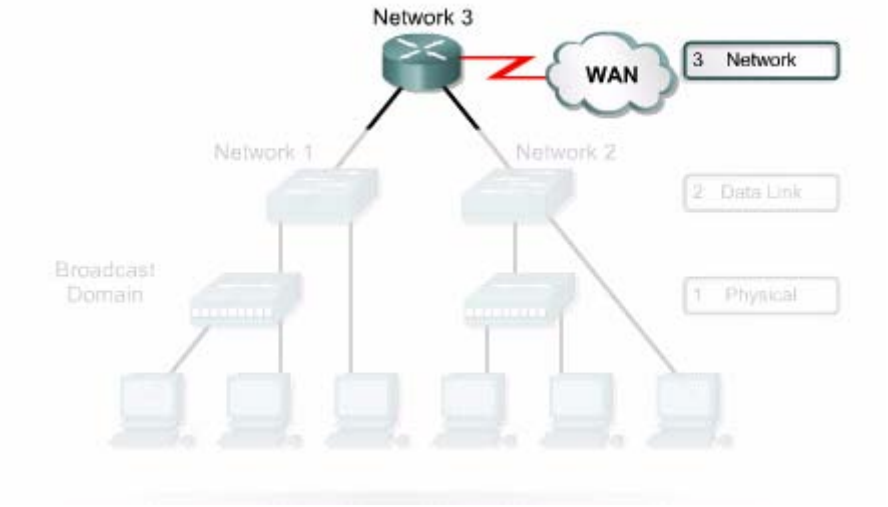


LAN with Hubs

Một số switch đời cũ như Catalyst 1700 chẳng hạn không hỗ trợ chia sẻ băng thông và miền đụng độ. Switch đời cũ không lưu được nhiều địa chỉ MAC cho một port nên hậu quả là sinh ra nhiều quảng bá và các yêu cầu ARP.

Ta thường sử dụng hub để tạo nhiều điểm kết nối đầu cuối vào một đường cáp horizontal. Biện pháp này có thể chấp nhận được nhưng nên cẩn thận vì miền đụng độ nên giữ ổ kích thước nhỏ để cung cấp đủ lượng băng thông cho host theo yêu cầu của thiết kế.





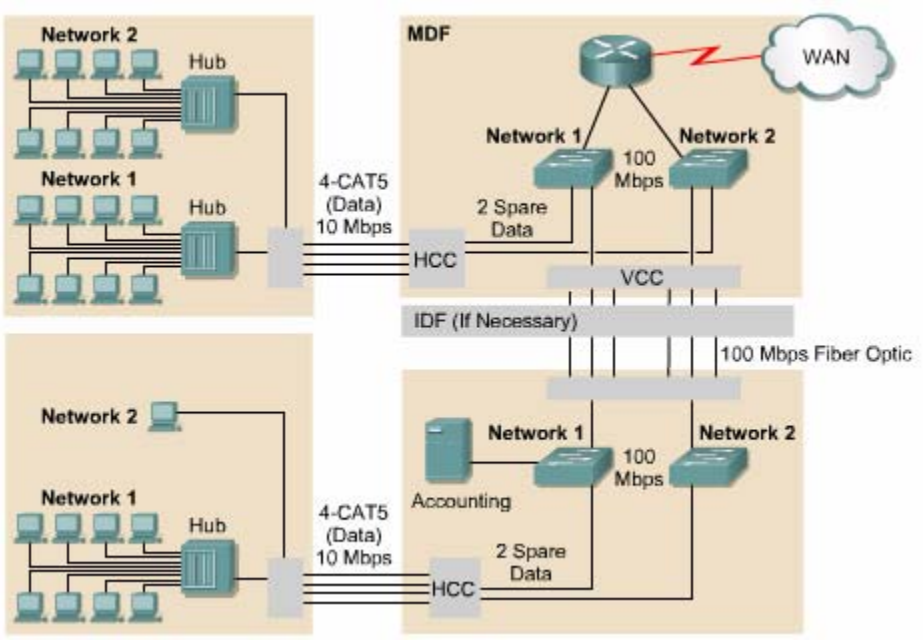
Router là thiết bị lớp 3 và được coi là một trong những thiết bị mạnh nhất trong cấu trúc mạng.

Thiết bị lớp 3 được sử dụng để chia mạng LAN thành nhiều mạng riêng biệt. Thiết bị lớp 3 cho phép thông tin liên lạc giữa 2 mạng thông qua địa chỉ lớp 3, ví dụ như địa chỉ IP. Triển khai thiết bị lớp 3 cho phép chia nhỏ mạng LAN về mặt vật lý và luận lý. Router còn có thể kết nối WAN như nối ra Internet chẳng hạn.

Định tuyến lớp 3 phân luồng giao thông giữa các mạng vật lý dựa trên địa chỉ lớp 3. Router không chuyển tiếp các gói quảng bá ví dụ như gói yêu cầu ARP chẳng hạn. Do đó mỗi cổng trên router được xem là cửa vào và cửa ra của một miền quảng bá, là nơi kết thúc của quảng bá, ngăn không cho quảng bá sang các mạng khác.

Router được xem là bức tường lửa đối với gói quảng bá. Ngoài ra router còn chia hệ thống mạng thành các subnet theo địa chỉ lớp 3.

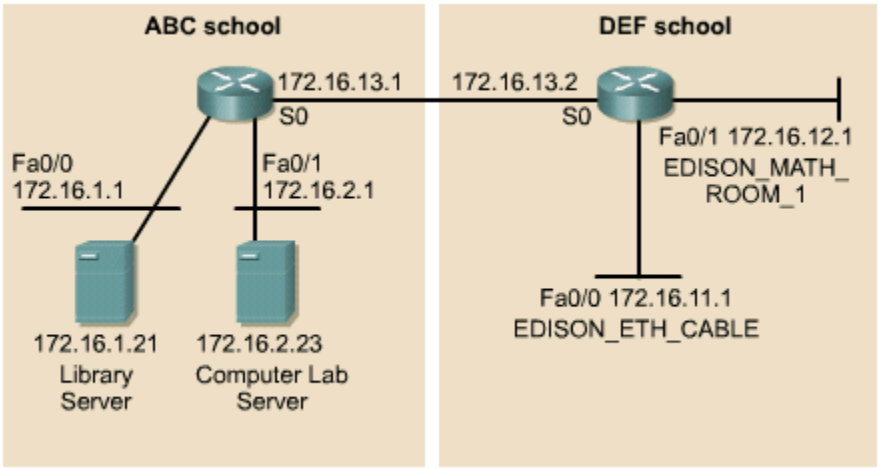
Khi bạn muốn quyết định sử dụng router hay switch ở đâu thì bạn nên nhớ câu hỏi sau: “Vấn đề mà bạn đang cần giải quyết ở đó là gì?” Nếu vấn đề liên quan đến giao thức hơn là sự tranh chấp thì router là giải pháp phù hợp. Router có thể giải quyết các vấn đề liên quan đến mức độ quảng bá quá nhiều, giao thức không cân đối, các vấn đề về bảo mật và địa chỉ lớp mạng. Router mắc tiền hơn và khó cấu hình hơn so với switch.



Hình 5.1.5.b là một ví dụ về hệ thống mạng có nhiều mạng vật lý khác nhau. Mọi dữ liệu từ Mạng 1 đến Mạng 2 đều phải đi qua router. Trong hình này, chúng ta có hai miền quảng bá. Mỗi miền có một sơ đồ địa chỉ lớp 3 riêng biệt. Trong sơ đồ đi dây các lớp 1, mỗi mạng vật lý được tạo ra dễ dàng bằng cách kết nối cáp horizontal và vertical vào switch lớp 2. Sau đó các mạng vật lý này được kết nối vào router làm tăng khả năng bảo mật hơn vì mọi giao thông đi vào hoặc đi ra một LAN đều phải qua router.

Sau khi bạn đã chia sơ đồ IP cho client xong thì bạn nên lập hồ sơ để ghi nhận lại một cách rõ ràng và đầy đủ. Bạn nên đặt một số quy ước chung cho những địa chỉ của các host quan trọng trong mạng. Sơ đồ địa chỉ cần được thống nhất và hoà hợp trên toàn bộ hệ thống mạng. Bạn nên lập hồ sơ địa chỉ để có một cái nhìn tổng quát về hệ thống mạng và ánh xạ chúng vào sơ đồ vật lý để sử dụng khi xử lý sự cố.

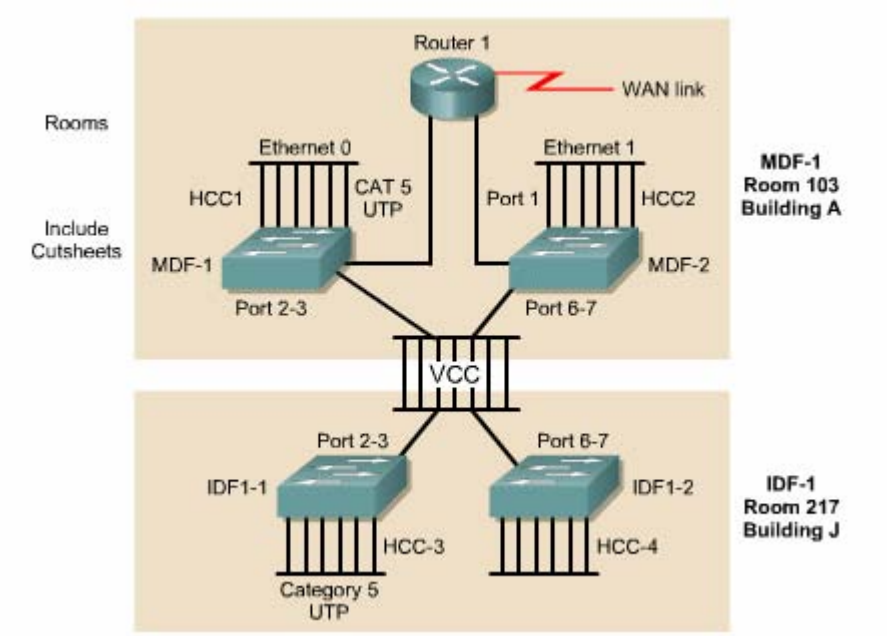
Logical Address	Physical Network Devices
x.x.x.1-x.x.x.10	Router, LAN, and WAN ports
x.x.x.11-x.x.x.20	LAN switches
x.x.x.21-x.x.x.30	Enterprise servers
x.x.x.31-x.x.x.80	Workgroup servers
x.x.x.81-x.x.x.254	Hosts



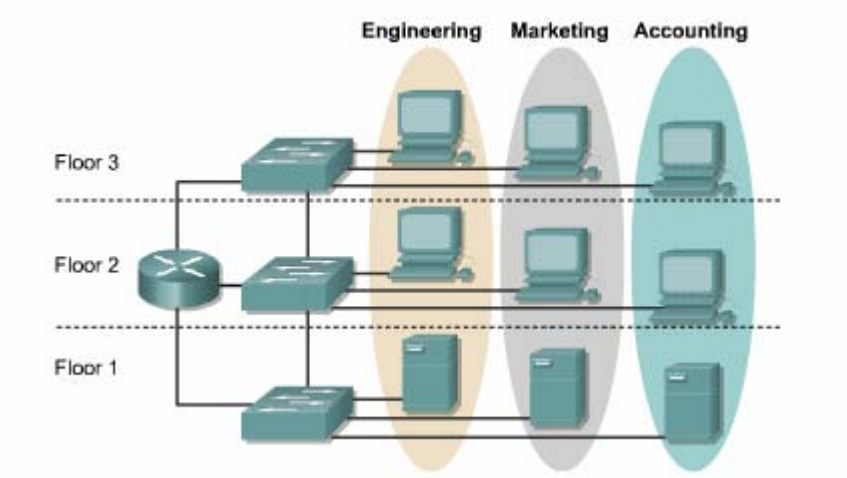
IP Network 172.16.0.0
Subnet Mask = 255.255.255.0

XYZ school district

ABC school	DEF school
172.16.1.0 through 172.16.10.0	172.16.11.0 through 172.16.21.0
Subnet mask = 255.255.255.0	Subnet mask = 255.255.255.0
Router name = ABC Router	Router name = DEF Router
Fa0/0 = 172.16.1.1	Fa0/0 = 172.16.11.1
Fa0/1 = 172.16.2.1	Fa0/1 = 172.16.12.1

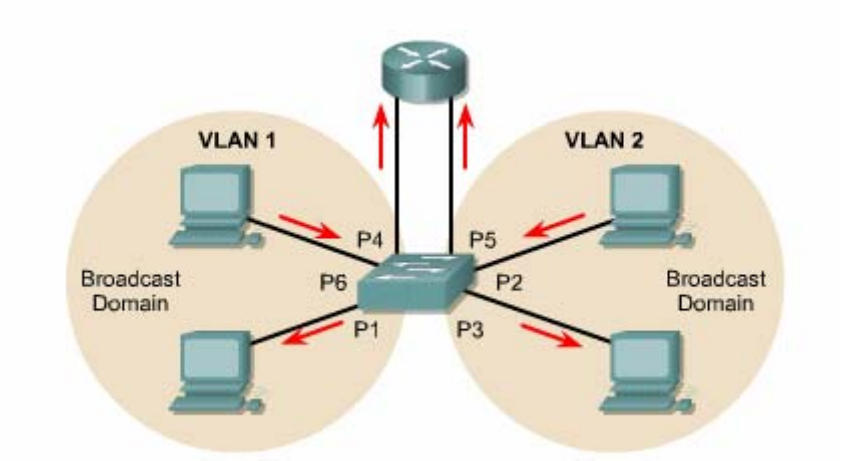


VLAN là một kỹ thuật kết hợp chuyển mạch lớp 2 và định tuyến lớp 3 để giới hạn miền đụng độ và miền quảng bá. VLAN còn được sử dụng để bảo mật giữa các nhóm VLAN theo chức năng của mỗi nhóm.



- Phân nhóm user theo phòng ban, đội nhóm và các ứng dụng thường dùng.
- Router cung cấp thông tin liên lạc giữa các VLAN với nhau.

Các port vật lý được nhóm vào một VLAN. Ví dụ như hình 5.1.5.h, port P1, P4, P5 được nhóm vào VLAN.1. VLAN.2 có các port P2, P3, P5. Thông tin liên lạc giữa VLAN.1. VLAN.2 bắt buộc phải thông qua router. Nhờ vậy kích thước miền đụng độ giảm xuống và router là nơi quyết định cho VLAN.1. và VLAN.2 có thể nói chuyện với nhau.

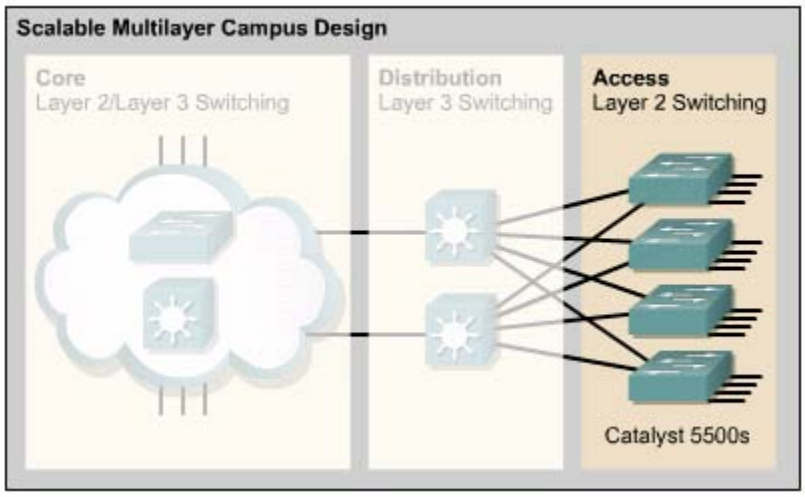


5.2. LAN switch

5.2.1. Chuyển mạch LAN và tổng quát về tầng truy cập

Để xây dựng một mạng LAN thoả mãn được các yêu cầu của một tổ chức vừa và lớn, bạn cần sử dụng mô hình thiết kế phân cấp. Mô hình thiết kế phân cấp sẽ làm cho thiết kế mạng thay đổi dễ dàng khi tổ chức phát triển lớn hơn nữa. Mô hình này có 3 tầng như sau:

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

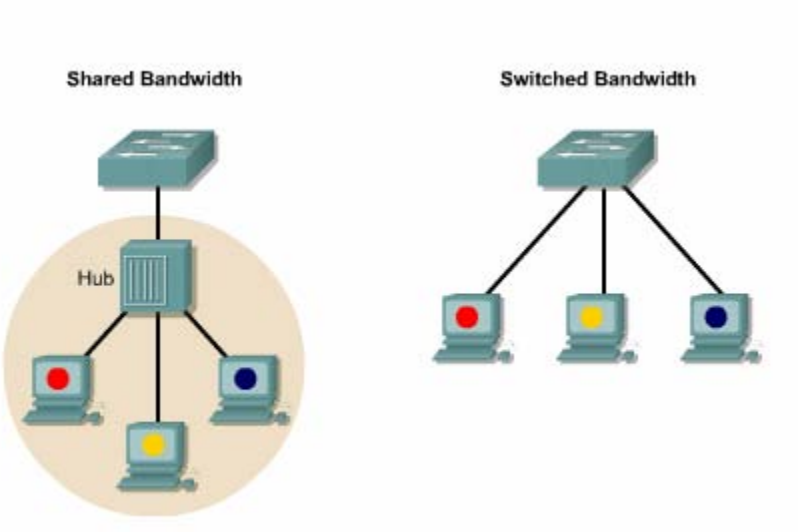


Mô hình phân cấp này có thể áp dụng cho bất kỳ thiết kế mạng nào. Điều quan trọng làm bạn cần thấy rằng 3 tầng này tồn tại với thành phần vật lý riêng biệt, rõ ràng. Mỗi tầng được định nghĩa để đại diện cho những chức năng mà chúng thực hiện trong mạng.

Tầng truy cập là điểm kết nối vào mạng của máy trạm và server. Trong LAN, thiết bị được sử dụng ở tầng truy cập có thể là switch hoặc hub.

Nếu sử dụng hub thì băng thông sẽ bị chia sẻ. Nếu sử dụng switch thì băng thông sẽ được dành riêng cho mỗi port. Nếu chúng ta nối một máy trạm hoặc một server vào một port của switch thì máy tính đó sẽ được dành trọn băng thông trên kết nối của port đó. Nếu kết nối hub vào một port của switch thì băng thông trên port đó sẽ chia sẻ cho mọi thiết bị kết nối vào hub đó.

Chức năng của tầng truy cập còn bao gồm cả lọc lớp MAC và thực hiện phân đoạn cực nhỏ. Lọc lớp MAC có nghĩa là switch chỉ chuyển frame ra đúng port kết nối vào thiết bị đích mà thôi. Switch còn có thể tạo ra các segment lớp 2 rất nhỏ gọi là microsegment. Mỗi segment như vậy chỉ có 2 thiết bị. Đây là kích thước nhỏ nhất có thể được của một miền đụng độ.



5.2.2. Switch sử dụng ở tầng truy cập

Switch tầng truy cập hoạt động ở lớp 2 của mô hình OSI và cung cấp một số dịch vụ như VLAN chẳng hạn. Mục tiêu chính của switch tầng truy cập là cho phép người dùng đầu cuối truy cập vào mạng. Bạn nên chọn switch tầng truy cập thực hiện chức năng này với chi phí thấp và độ cảm nhận trên port cao.

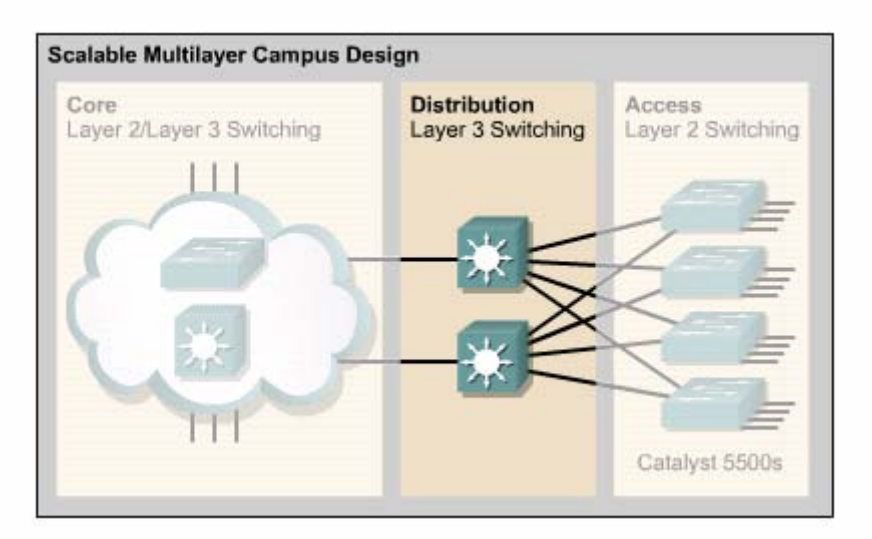
Sau đây là một số dòng switch của Cisco thường được dùng ở tầng truy cập:

- Catalyst 1900
- Catalyst 2820
- Catalyst 2950
- Catalyst 4000
- Catalyst 5000

Dòng Catalyst 1900 và 2820 là những thiết bị truy cập hiệu quả cho hệ thống mạng vừa và nhỏ. Dòng switch Catalyst 2950 cung cấp đường truy cập hiệu quả hơn cho server và nhiều băng thông hơn cho người dùng nhờ các port Fast Ethernet. Dòng Catalyst 4000 và 5000 có port Gigabit Ethernet là thiết bị để truy cập hiệu quả cho các mạng lớn.

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

Fast Ethernet Ports	Gigabit Ethernet	Enterprise Size
2	0	Small to medium
2	0	Small to medium
12 or 24 speed configurable	0 or 2	Small to medium
Configurable ports- up to 240	Configurable ports - up to 240	Varies with options chosen
Configurable ports- up to 266	Configurable ports - up to 38	Varies with options chosen



Tầng phân phối nằm giữa tầng truy cập và tầng trục chính giúp xác định và phân biệt với hệ thống trục chính. Mục tiêu của tầng phân phối là cung cấp giới hạn cho phép các gói dữ liệu được di chuyển trong đó. ở tầng này, hệ thống mạng được chia thành nhiều miền quảng bá, đồng thời áp dụng các chính sách về truy cập, lọc gói dữ liệu tại đây. Tầng phân phối giúp cô lập sự cố trong phạm vi một nhóm và ngăn không cho sự cố tác động vào tầng trục chính. Switch trong tầng này hoạt động ở lớp 2 và 3 của mô hình OSI. Tóm lại, tầng phân phối thực hiện các chức năng sau:

- Xác định miền quảng bá hay miền multicast
- Định tuyến VLAN

- Chuyển đổi môi trường mạng nếu cần
- Bảo mật.

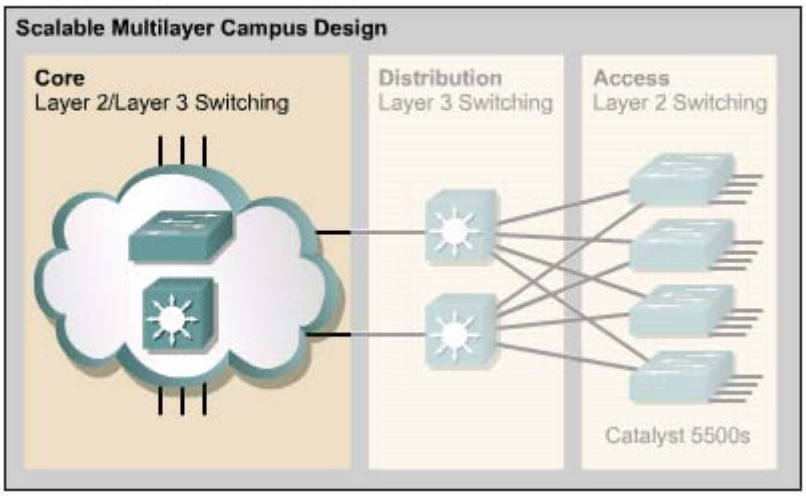
5.2.4. Switch sử dụng ở tầng phân phối:

Switch tầng phân phối là điểm tập trung cho các switch tầng truy cập. Do đó, các switch tầng này phải gánh toàn bộ lượng giao thông từ các thiết bị tầng truy cập nên chúng phải có năng lực hoạt động cao. Switch tầng phân phối là điểm kết thúc cho miền quảng bá. Tầng này tập trung giao thông của VLAN và các chính sách để quyết định dòng chảy của giao thông. Do đó, switch của tầng phân phối hoạt động ở cả lớp 2 và 3 trong mô hình OSI. Switch trong tầng này thường là switch đa lớp. Switch đa lớp là sự kết hợp chức năng của router và switch vào chung trong một thiết bị. Chúng được thiết kế để chuyển mạch giao thông với hiệu suất hoạt động cao hơn một router thông thường. Nếu các switch này không có router module gắn trong nó thì bạn có thể sử dụng một router riêng bên ngoài để thực hiện chức năng lớp 3.

Sau đây là các dòng switch của Cisco phù hợp với tầng phân phối:

- Catalyst 2926G
- Catalyst 5000
- Catalyst 6000

4.1.1. Tổng quát về tầng trục chính:



Tầng trục chính được chuyển mạch tốc độ cao. Nếu switch tầng này không có router module gắn trong thì bạn có thể sử dụng router riêng bên ngoài để thực hiện các chức năng lớp 3. Tầng này được thiết kế là không thực hiện bất kỳ hoạt động cản trở gói nào vì những hoạt động cản trở gói dữ liệu như danh sách kiểm tra truy cập chẳng hạn sẽ làm chậm tốc độ chuyển mạch gói. Cấu trúc tầng trục chính nên có các đường dự phòng để ổn định hoạt động mạng, tránh tình trạng chỉ có một điểm trung tâm duy nhất.

Tầng trục chính được thiết kế sử dụng chuyển mạch lớp 2 hoặc lớp 3. Bạn có thể sử dụng switch ATM hoặc Ethernet cho tầng này.

5.2.6. Switch sử dụng ở tầng trục chính.

Tầng trục chính là xương sống của hệ thống mạng. Switch trong tầng này có thể sử dụng một số công nghệ lớp 2. Nếu khoảng cách giữa các switch có thể sử dụng công nghệ Ethernet. Một số công nghệ lớp 2 khác như chuyển mạch tế bào ATM (Asynchoronous Transfer Mode) cũng có thể được sử dụng. Trong thiết kế mạng, tầng trục chính cũng có thể định tuyến lớp 3 nếu cần thiết. Khi chọn lựa switch cho tầng này bạn cần quan tâm đến những yếu tố như sự cần thiết, giá cả và khả năng hoạt động.

Sau đây là một số dòng Switch của Cosco phù hợp cho tầng trục chính:

- Catalyst 6500
- Catalyst 8500
- IGX 8400
- Lighstream 1010

Tổng kết

Sau khi kết thúc chương trình này, bạn cần nắm được các điểm quan trọng sau:

- Bốn mục tiêu chính trong thiết kế LAN
- Các vấn đề cần quan tâm chính yếu trong thiết kế LAN.
- Các bước trong thiết kế LAN
- Những vấn đề trong thiết kế Lớp 1, 2 và 3.
- Mô hình thiết kế 3 tầng
- Chức năng của mỗi tầng trong mô hình 3 tầng này
- Cisco switch trong tầng truy cập và các đặc điểm của chúng.
- Cisco switch trong tầng phân phối và các đặc điểm của chúng
- Cisco switch trong tầng trục chính và các đặc điểm của chúng

- Kiểm tra các hiển thị của quá trình khởi động switch bằng HyperTerminal.
- Sử dụng tính năng trợ giúp của giao tiếp dòng lệnh.
- Liệt kê các chế độ dòng lệnh cơ bản của switch.
- Kiểm tra cấu hình mặc định của Catalyst switch.

- Đặt địa chỉ IP và cổng mặc định cho switch để cho phép kết nối và quản lý switch qua mạng.
- Xem các cài đặt trên switch bằng một trình duyệt Web.
- Cài đặt tốc độ và hoạt động song công trên port của switch.
- Kiểm tra và quản lý bảng địa chỉ MAC của switch
- Cấu hình bảo vệ port.
- Quản lý tập tin cấu hình và IOS.
- Thực hiện khôi phục mật mã trên switch
- Nâng cấp IOS của switch.

6.1. Bắt đầu với switch

6.1.1. Bắt đầu với phần vật lý của switch

Switch là một máy tính đặc biệt cũng có bộ xử lý trung tâm (CPU), RAM (Random access memory), và hệ điều hành. Switch có các port dành cho mục đích kết nối host và có một số port đặc biệt chỉ dành cho mục đích quản lý switch. Bạn có thể xem và thay đổi cấu hình switch bằng cách kết nối vào cổng console.

Switch thường không có công tắc điện để bật tắt mà nó chỉ có cắm dây điện hay không cắm dây điện mà thôi.

6.1.2. Đèn báo hiệu LED trên switch

Mặt trước của switch có một sô đèn báo hiệu LED (Light-Emitting Diode) giúp bạn theo dõi switchự hoạt động của switch :

- System LED: LED hệ thống.
- Remote Power Supply (RPS): LED nguồn điện từ xa.
- Port Mode LED: LED chế độ port.
- Port Status LED: LED trạng thái port. Mỗi port của switch có một đèn LED nằm ở phía trên port, hiển thị trạng thái của port đó tùy theo chế độ hiển thị được cài đặt ở nút Mode.

LED hệ thống cho biết hệ thống đã được cấp nguồn và hoạt động tốt,

RPS LED cho biết switch có sử dụng bộ nguồn bên ngoài hay không.

LED chế độ port cho biết chế độ hiển thị hiện tại của các LED trạng thái port. Để chọn các chế độ hiển thị trạng thái khác nhau, bạn nhấn nút Mode một hoặc nhiều lần cho đến khi LED chế độ port hiển thị đúng chế độ mà bạn muốn.

LED trạng thái port hiển thị các giá trị khác nhau tùy theo chế độ được cài đặt trên nút Mode.

LED chế độ port	**Màu của các LED trạng thái trên từng port**	**Mô tả**
STAT (Trạng thái hoạt động)	Tắt	Không có kết nối
	Màu xanh	Kết nối đang hoạt động
	Màu xanh nhấp nháy	Port đang truyền và nhận dữ liệu

	Lúc màu xanh lúc màu cam	Kết nối đang bị lỗi
	Màu cam	Port không thực hiện chuyển gói vì nó đã bị tắt chức năng này, hoặc có địa chỉ bị vi phạm cấu hình, hoặc bị khóa do giao thức Spanning Tree.
UTL (mức độ hoạt động của switch)	Tắt	Cứ mỗi một LED trên mỗi port bị tắt có nghĩa là tổng băng thông sử dụng giảm xuống một nửa. Các đèn LED sẽ được tắt lần lượt từ phải sang trái. Nếu một LED đầu tiên bên phải bị tắt có nghĩa là switch đang sử dụng dưới 50% tổng băng thông. Nếu 2 LED đầu tiên bên phải bị tắt có nghĩa là switch đang sử dụng dưới 25% tổng băng thông.
	Màu xanh	Nếu tất cả các LED trên port đều xanh có nghĩa là switch đang sử dụng >= 50% tổng băng thông
FDUP (Full-duplex)	Tắt	Port tương ứng đang ở chế độ bán song công (half-dupplex)
	Màu xanh	Port tương ứng đang ở chế độ song công
100 (Tốc độ)	Tắt	Port tương ứng đang hoạt động ở tốc độ 10Mb/s
	Màu xanh	Port tương ứng đang hoạt động ở tốc độ 100Mb/s

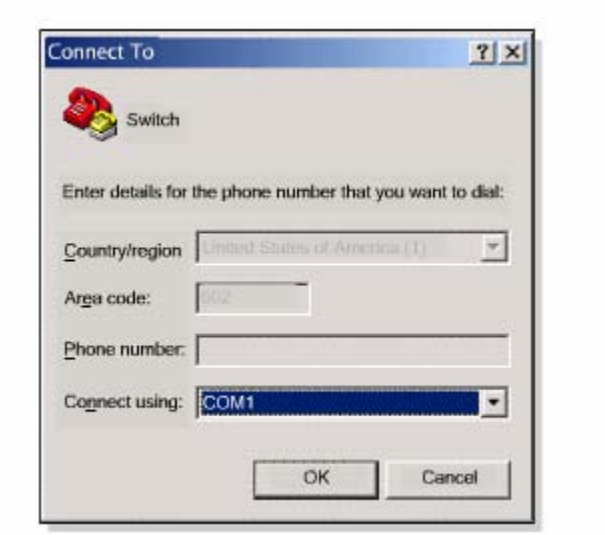
6.1.3. Kiểm tra LED trong suốt quá trình khởi động switch

Khi bắt đầu cắm điện, switch sẽ tiến hành một loạt các bước kiểm tra gọi là tự kiểm tra khi bật nguồn POST (Power-On Self Test). POST tự động kiểm tra các thành phần phần cứng để đảm bảo switch hoạt động đúng. LED hệ thống sẽ cho biết quá trình POST kết thúc thành công hay bị lỗi. Khi switch mới được cắm điện, quá trình POST đang chạy thì LED hệ thống còn tắt. Nếu sau đó LED hệ thống bật lên màu xanh có nghĩa là quá trình POST đã kết thúc thành công. Nếu LED hệ thống bật lên màu vàng có nghĩa là quá trình POST đã gặp lỗi. POST gặp lỗi thường là những lỗi vật lý nghiêm trọng. switch không thể hoạt động tin cậy nếu POST bị lỗi.

LED trạng thái của các port cũng thay đổi trong suốt quá trình POST. LED trạng thái trên mỗi port sẽ bật lên màu cam trong khoảng 30 giây là quá trinhd switch đang phát hiện cấu trúc mạng và dò tìm vòng lặp. Nếu sau đó LED trạng thái trên port chuyển sang màu xanh có nghĩa switch đã thiết lập được kết nối trên port đó với hệ thống mạng. Nếu LED trạng thái trên port tắt có nghĩa là switch nhận thấy không có gì cắm vào port này cả.

6.1.4. Xem các thông tin hiển thị trong quá trình khởi động switch

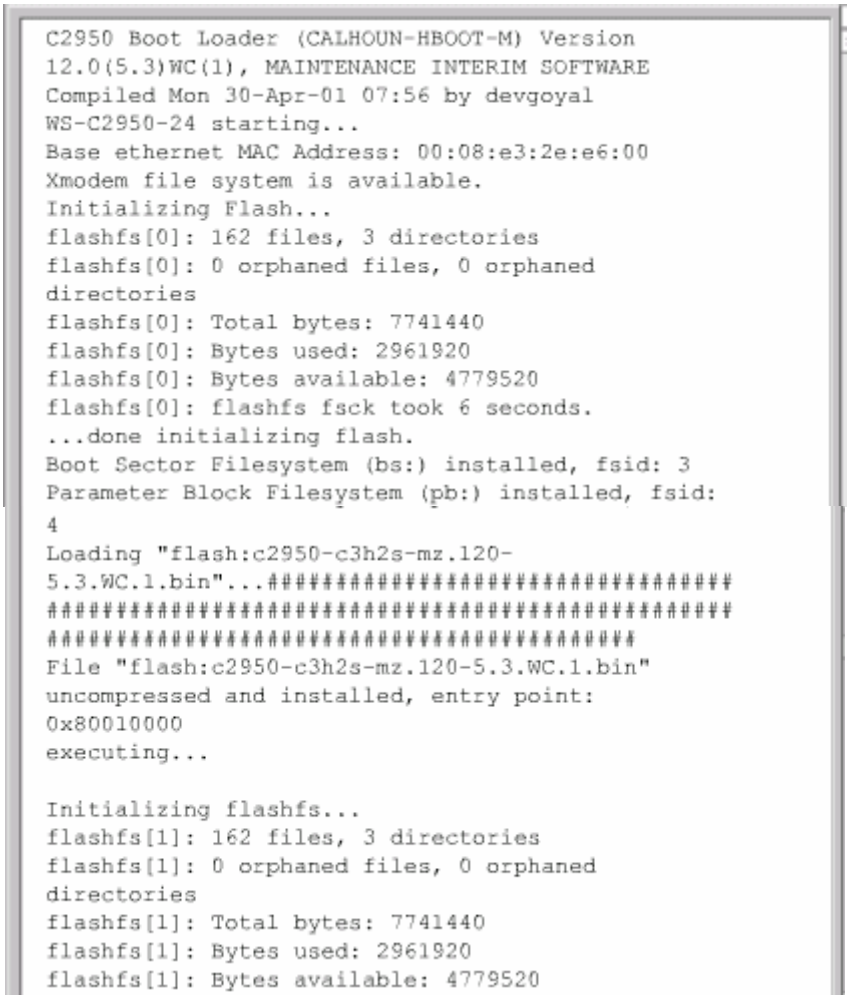
Để cấu hình hoặc kiểm tra trạng thái của switch, bạn cần kết nối một máy tính vào switch để thiết lập phiên giao tiếp. Bạn có thể dùng cáp rollover để nối từ cổng console ở mặt sau của switch vào cổng COM trên máy tính.

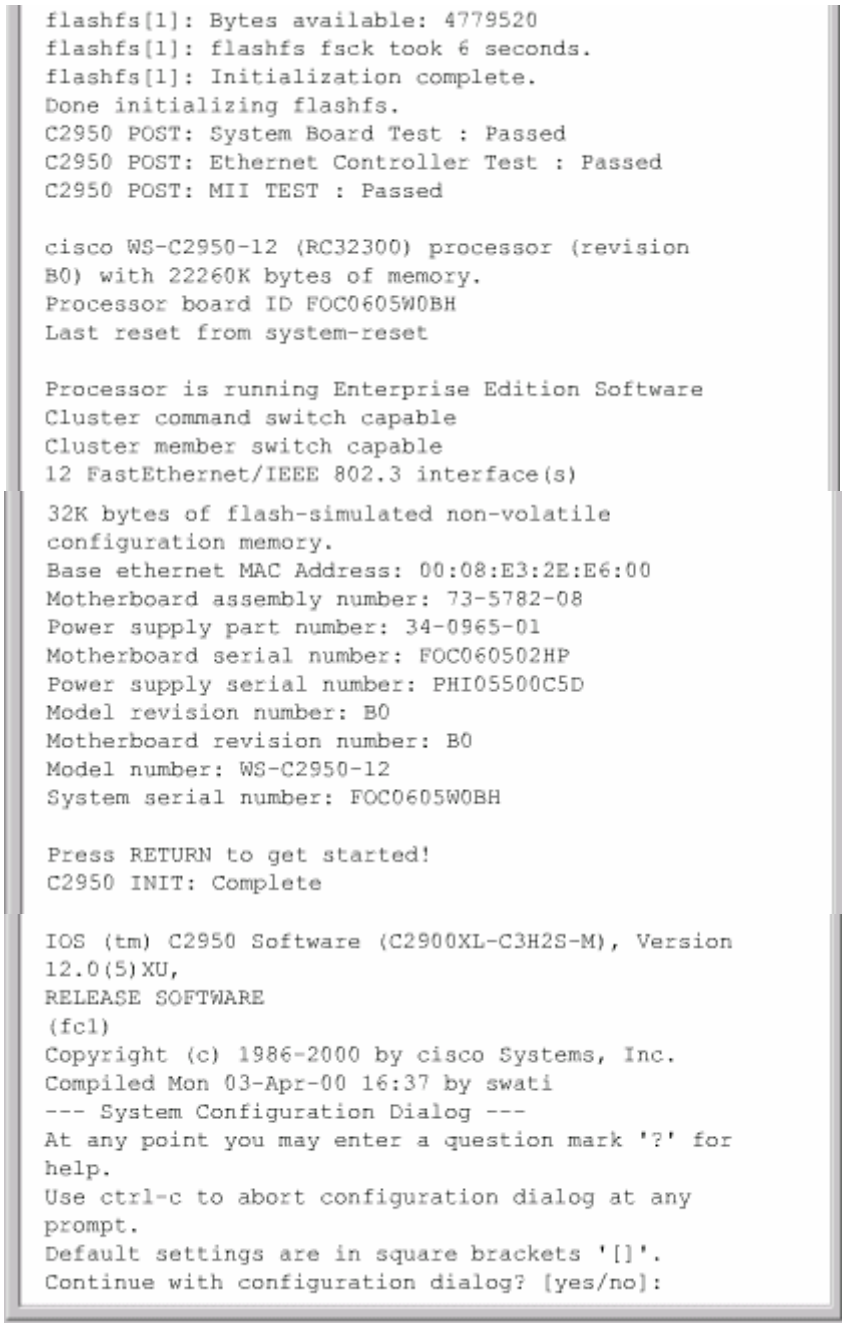


Hình 6.1.4.a. Kết nối máy tính vào cổng console của switch

Hình 6.1.4.b

Sau đó bạn chạy HyperTerminal trên máy tính. Trước tiên, bạn phải đặt tên cho kết nối để bắt đầu cấu hình phiên giao tiếp HyperTerminal với switch. Sau đó bạn gặp hộp thoại như hình 6.1.4.b, chọn cổng COM mà bạn kết nối máy tính vào switch rồi nhấn nút OK. Bạn gặp một hộp thoại tiếp theo như hình 6.1.4.c, chọn các thông số như trên hình rồi ấn nút OK.

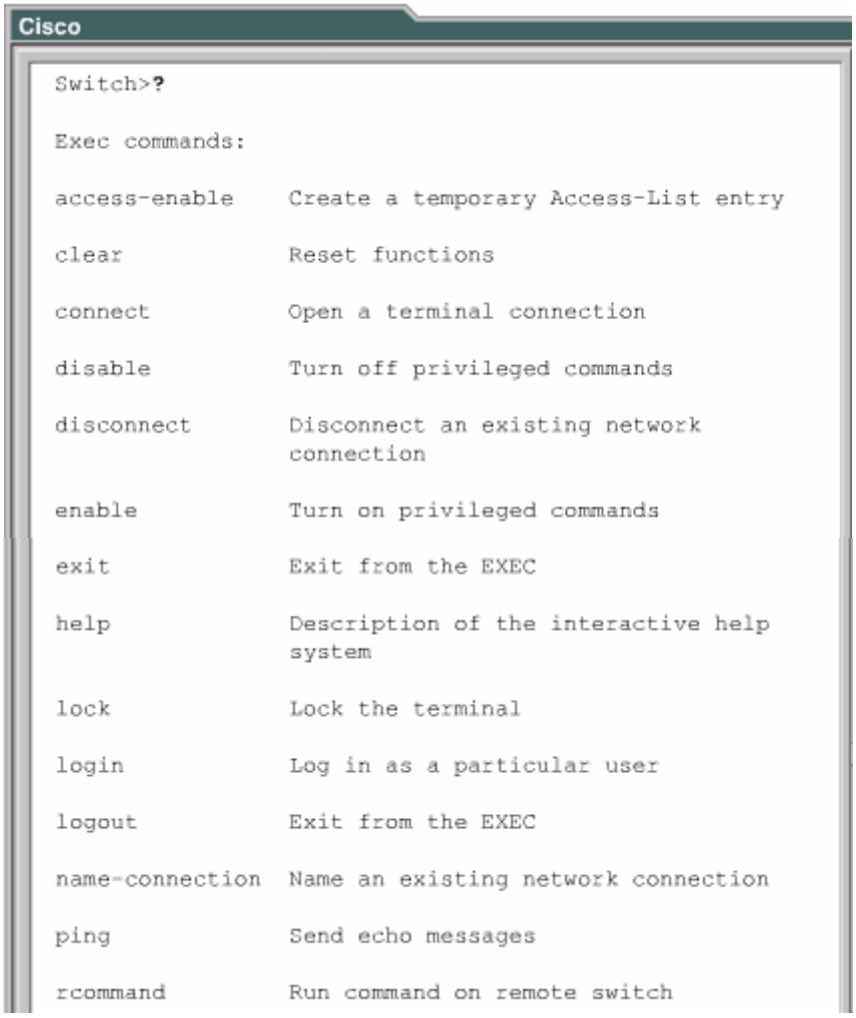


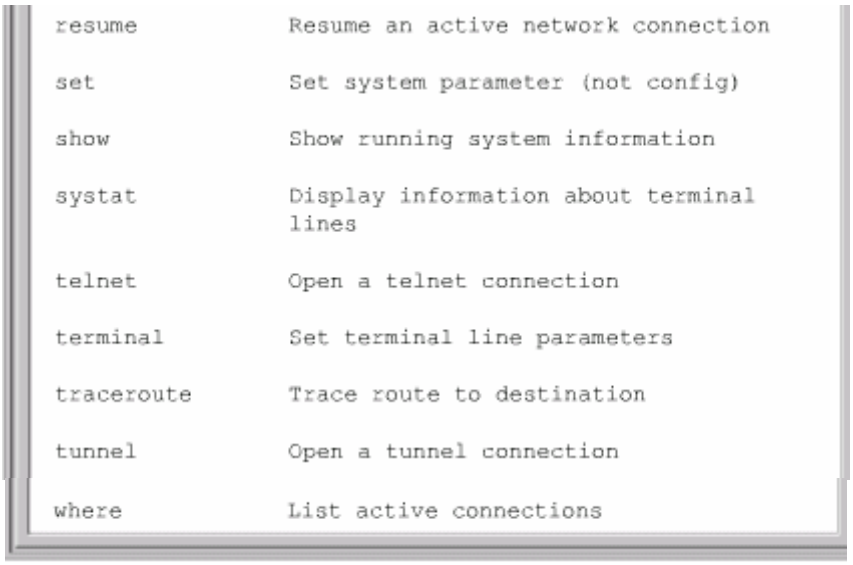


Hình 6.1.4.c. Cài đặt thông số cho HyperTerminal

Cắm điện cho switch. Các thông tin về quá trình khởi động switch sẽ hiện ra trên màn hình HyperTerminal. Những thông tin này bao gồm thông tin về switch, chi tiết về trạng thái POST và dữ liệu về phần cứng của switch.

Sau khi switch hoàn tất quá trình POST và khởi động xong, dấu nhắc của phần đối thoại cấu hình hệ thông sẽ xuất hiện. Bạn có thể cấu hình switch bằng tay hoặc với sự trợ giúp của phần đối thoại cấu hình. Phần đối thoại cấu hình trên switch đơn giản hơn trên router.





Hình 6.1.4.d. Thông tin hiển thị của quá trình khởi động switch .

6.1.5. Chức năng trợ giúp của giao tiếp CLI trên switch

Giao tiếp dòng lệnh (CLI-Command-Line Interface) của Cisco switch rất giống với giao tiếp dòng lệnh của Cisco router.

Lệnh help có thể được gọi một cách ngắn gọn bằng dấu chấm hỏi (?). Khi bạn nhập dấu chấm hỏi tại dấu nhắc của hệ thống, switch sẽ hiển thị danh sách các lệnh mà bạn có thể sử dụng trong chế độ dòng lệnh hiện tại bạn đang ở.

Hình 6.1.5. Lệnh help trong chế độ EXEC người dùng.

Lệnh help có thể được sử dụng một cách linh hoạt. Để tìm danh sách các lệnh bắt đầu với các ký tự mà bạn cần, bạn nhập các ký tự đó rồi liền tiếp sau đó là dấu chấm hỏi (?), không chừa khoảng trắng giữa các ký tự với dấu chấm hỏi. Khi đó bạn sẽ có kết quả hiển thị là danh sách các câu lệnh bắt đầu bằng các ký tự mà bạn vừa mới nhập vào.

Để hiện thị các từ khóa hoặc các tham số của một lệnh nào đó, bạn nhập câu lệnh đó, cách một khoảng trắng rồi điền dấu chấm hỏi (?). switch sẽ hiện thị các từ khóa hoặc tham số được sử dụng tại vị trí của dấu chấm hỏi trong câu lệnh đó.

6.1.6. Các chế độ dòng lệnh của switch

Switch có một chế độ dòng lệnh. Chế độ mặc định là chế độ EXEC người dùng. Chế độ này có dấu nhắc đại diện lớn hơn (>). Các lệnh trong chế độ EXEC người dùng rất giới hạn trong việc thay đổi cài đặt đầu cuối, kiểm tra cơ bản và hiện thị thông tin hệ thống.

Lệnh enable được sử dụng để di chuyển từ chế độ EXEC người dùng sang chế độ EXEC đặc quyền. Chế độ EXEC đặc quyền có dấu nhắc là dấu thăng (#). Các lệnh sử dụng được trong chế độ này cũng bao gồm tất cả các lệnh của chế độ EXEC người dùng và còn có thêm lệnh configure. Lệnh configure cho phép bạn truy cập vào các chế độ cấu hình sâu hơn. Bắt đầu từ chế độ EXEC đặc quyền là bạn có thể cấu hình switch , do đó chế độ này cần được bảo vệ bằng mật mã để cấm việc sử dụng ngoài ý muốn. Nếu người quản trị mạng đặt mật mã thì bạn sẽ được yêu cầu nhập mật mã trước khi vào được chế độ EXEC đặc quyền. Khi bạn nhập mật mã, mật mã se không hiển thị trên màn hình.

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)

6.2. Cấu hình switch

6.2.1. Kiểm tra cấu hình mặc định của Catalyst switch

Khi mới cắm điện lần đầu tiên, switch chỉ có tập tin cấu hình mặc định. Tên mặc định của switch là Switch . Không mật mã nào được cài đặt ở đường console và vty.

```
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
```

Hình 6.2.1.a. Cấu hình mặc định của switch

Bạn nên đặt một địa chỉ IP cho switch trên cổng giả lập VLAN 1 để quản lý switch. Mặc định là switch không có địa chỉ IP nào cả.

Tất cả các port của switch được đặt ở chế độ tự động và đều nằm trong VLAN 1. VLAN 1 và VLAN quản lý theo mặc định của switch.

Mặc định, trong thư mục flash lưu IOS, có một file tên là env_vars và một thư mục con tên là html. Sau khi switch đã được cấu hình, trong thư mục này sẽ có thêm tập tin config.text và vlan.dat là tập tin cơ sở dữ liệu của VLAN.

```
Switch#show interface FastEthernet0/1
FastEthernet0/1 is down, line protocol is down
  Hardware is Fast Ethernet, address is
0008.e32e.e501 (bia 0008.e32.e.e601)
  MTU 1500 bytes, BW 0 Kbit, DLY 100 usec,
    reliability 255/25, txlead 1/255, rxlead 1/255
  Encapulation ARPA, Loopback not set
  Keepalive not set
  Auto-duplex, AutoSpeed , 100BaseTX/TX
  ARP type: ARPA, ARP TImeout 04:00:00
  Last Input never, output 00:31:54, output hang
never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue o/75, 0
drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1 packets input, 54 bytes
     Recieved 0 broadcasts, 0 runts, 0 giants, 0
throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0
ignored
     0 watchdaog, 0 multicast
     0 input packets with dribble condition detected
     5 packets output, 495 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface
resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
```

Hình 6.2.1.b. Đặc điểm mặc định của các port trên switch

Catalyst 2950

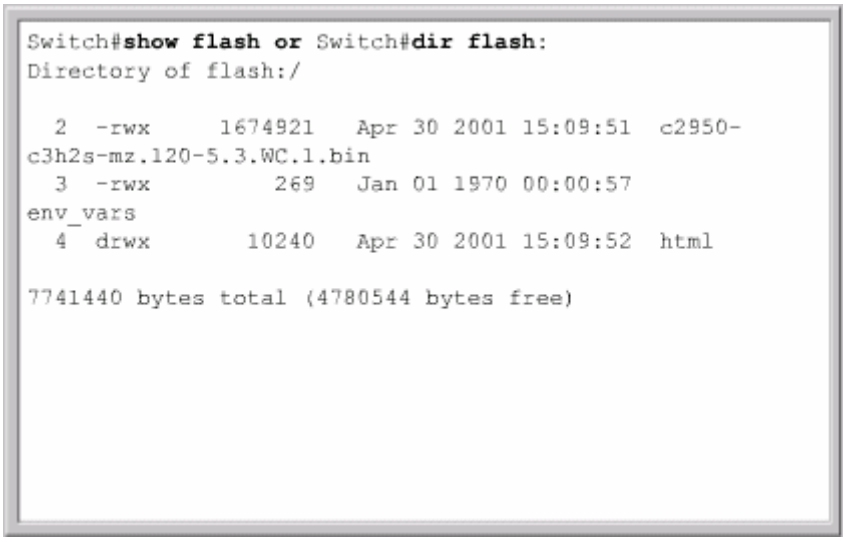
```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash:vlan.dat? [confirm]
Switch#erase startup-config
<output omitted>
Switch#reload
```

Catalyst 1900

```
Switch#delete nvram
```

Hình 6.2.1.c. 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
```



Hình 6.2.1.d. Nội dung mặc định của thư mục flash.

Bạn có thể kiểm tra phiên bản IOS và giá trị cho thanh ghi cấu hình bằng lệnh show version.

Mặc định, switch chỉ có một miền quảng bá và chúng ta chỉ có thể quản lý và cấu hình switch thông qua cổng console. Giao thức Spanning-Tree cũng mặc nhiên chạy tự động trên switch cho phép switch xây dựng cấu trúc không vòng lặp trên toàn bộ mạng LAN.

```
Switch#show interface FastEthernet0/1
FastEthernet0/1 is down, line protocol is down
  Hardware is Fast Ethernet, address is
0008.e32e.e501 (bia 0008.e32.e.e601)
  MTU 1500 bytes, BW 0 Kbit, DLY 100 usec,
    reliability 255/25, txlead 1/255, rxlead 1/255
  Encapulation ARPA, Loopback not set
  Keepalive not set
  Auto-duplex, AutoSpeed , 100BaseTX/TX
  ARP type: ARPA, ARP TImeout 04:00:00
  Last Input never, output 00:31:54, output hang
never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue o/75, 0
drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1 packets input, 54 bytes
     Recieved 0 broadcasts, 0 runts, 0 giants, 0
throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0
ignored
     0 watchdaog, 0 multicast
     0 input packets with dribble condition detected
     5 packets output, 495 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface
resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
```

Hình 6.2.1.e

Đối với mạng nhỏ thì cấu hình mặc đinh là đủ. Switch vẫn thực hiện microsegment ngay, không cần cấu hình gì thêm.

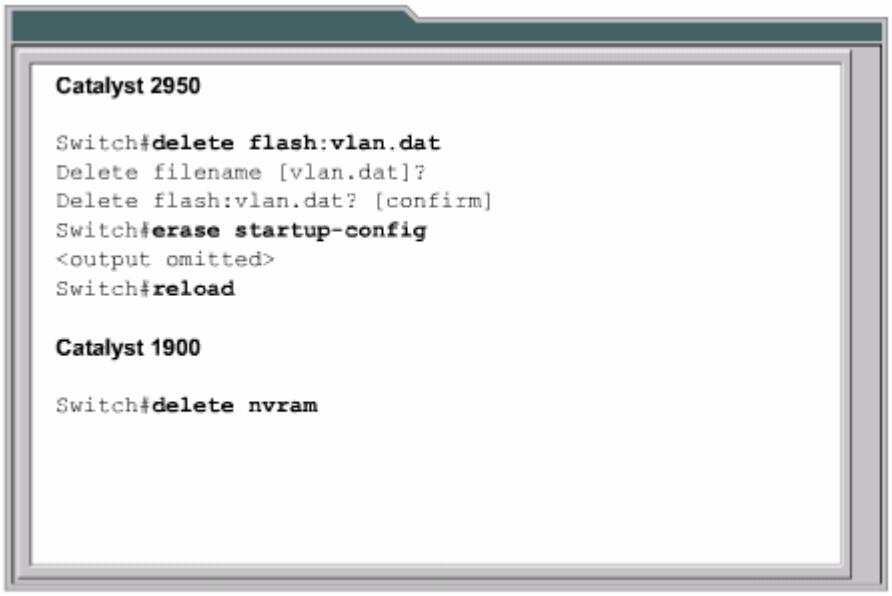
6.2.2. Cấu hình Catalyst switch

Switch có thể đã được cấu hình trước đó và chúng ta có thể cần phải có mật mã để vào được chế đô EXEC người dùng hoặc chế độ EXEC đặc quyền. Để có thể cấu hình switch chúng ta phải bắt đầu từ chế độ EXEC đặc quyền.

Trong giao tiếp dòng lệnh (CLI), dấu nhắc mặc định của chế độ EXEC đặc quyền là Switch#, còn của chế độ EXEC người dùng là Switch>.

Sau đây là các bước bạn cần thực hiện để đảm bảo là cấu hình mới sẽ được thay thế cho cấu hình cũ:

- Xóa mọi thông tin về cơ sở dữ liệu đang có của VLAN bằng các xóa tập tin vlan.dat trong thư mục flash.
- Xóa tập tin cấu hình dự phòng của switch bằng cách xóa tập tin startup-config.
- Khởi động lại switch .

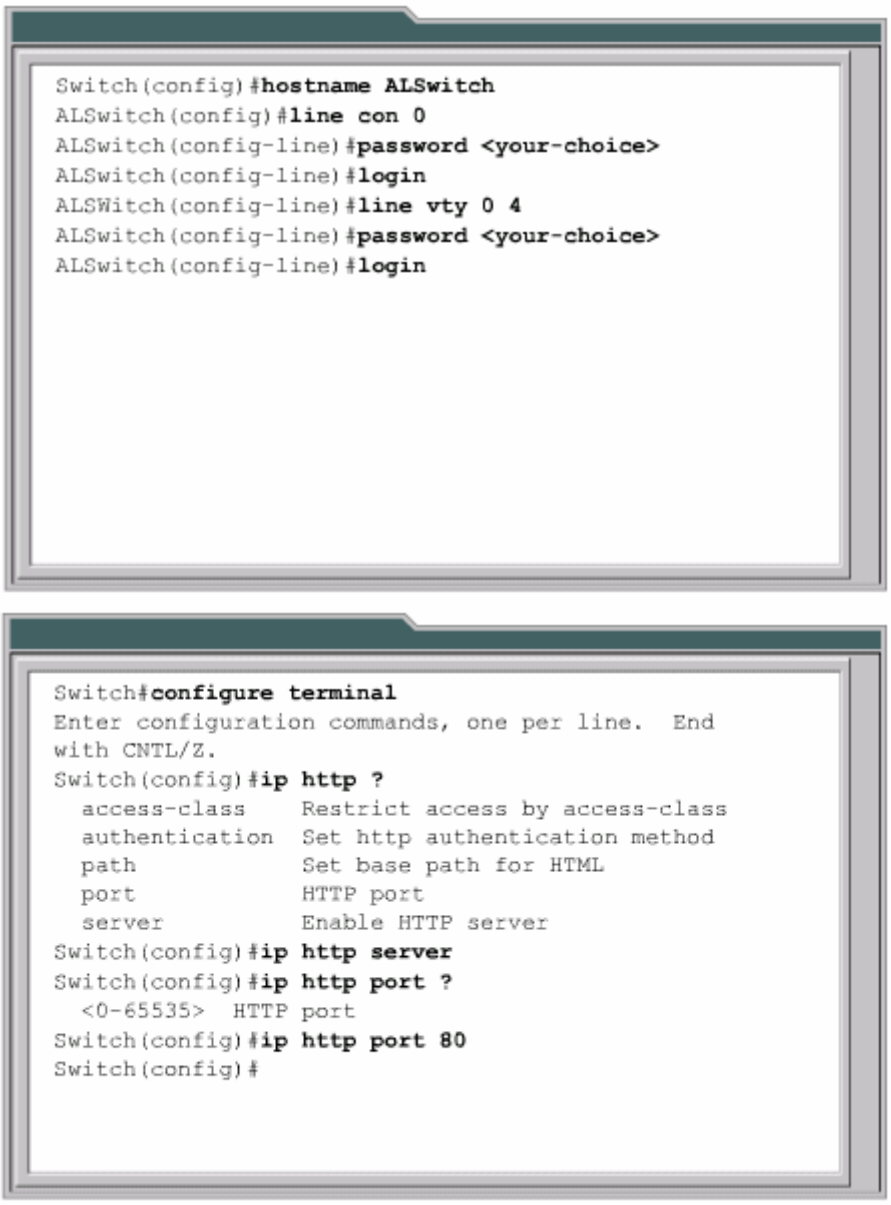


Hình 6.2.2.a Xóa mọi cấu hình cũ trên switch

Ghi hồ sơ, bảo mật và quản lý là những công việc hết sức quan trọng đối với mọi thiết bị mạng.

Chúng ta nên đặt tên cho switch và đặt mật mã cho đường console và vty.

Để có thể truy cập vào switch bằng Telnet hay bằng các ứng dụng TCP/IP khác thì bạn cần đặt một địa chỉ IP và khai báodefault gateway cho switch . VLAN 1 là VLAN quản lý mặc định của switch. Tất cả các thiết bị mạng đều được đặt trong VLAN quản lý. Nhờ đó, từ một máy trạm quản lý bạn có thể truy cập, cấu hình và quản lý tất cả các thiết bị liên mạng.



Hình 6.2.2.b. Đặt tên và mật mã trên đường console và vty, đặt địa chỉ IP và default gateway.

Mặc định, Fast Ethernet Port được đặt ở chế độ tự động về tốc độ và song công. Do đó các port này sẽ tự động thỏa thuận các thông số với thiết bị kết nối vào nó. Nếu người quản trị mạng muốn chắc chắn một port nào đó có tốc độ và chế độ song công như ý mình muốn thì có thể cấu hình bằng tay cho port đó.

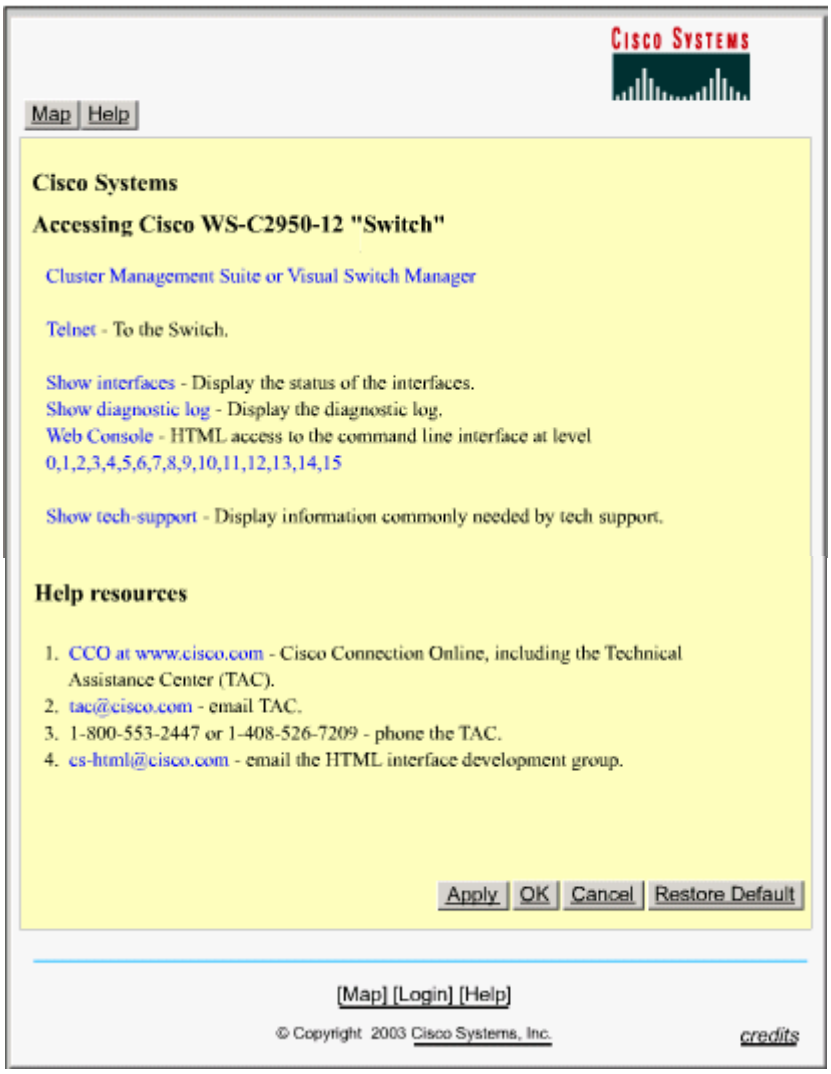
Các thiết bị mạng thông minh có thể giao tiếp được bằng Web để cấu hình và quản lý chúng. Sau khi switch đã được cấu hình địa chỉ IP và gateway, chúng ta có thể truy cập vào switch bằng web. Trình duyệt web truy cập và dịch vụ này trên switch bằng địa chỉ IP của switch và port 80 là port mặc định của HTTP. Bạn có thể mở hoặc tắt dịch vụ HTTP trên switch và có thể chọn port khác cho dịch vụ này.

```
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
```

Hình 6.2.2.c. Cấu hình tốc độ và chế độ song công cho port cho

```
Switch#configure terminal
Enter configuration commands, one per line.  End
with CNTL/Z.
Switch(config)#ip http ?
  access-class    Restrict access by access-class
  authentication  Set http authentication method
  path            Set base path for HTML
  port            HTTP port
  server          Enable HTTP server
Switch(config)#ip http server
Switch(config)#ip http port ?
  <0-65535>  HTTP port
Switch(config)#ip http port 80
Switch(config)#
```

Hình 6.2.2.d. Mở dịch vụ HTTP và chọn port cho dịch vụ này trên switch.



Hình 6.2.2.e. Giao diện web của switch.

Hình 6.2.2.f. Giao diện quản lý web.

6.2.3. Quản lý bằng địa chỉ MAC

Switch học địa chỉ MAC của các thiết bị kết nối vào port của nó bằng cách kiểm tra địa chỉ nguồn của gói dữ liệu mà nó nhận vào từ mỗi port . Các địa chỉ MAC học được sẽ được ghi vào bảng địa chỉ MAC. Những gói dữ liệu nào có địa chỉ MAC đích nằm trong bảng này sẽ được chuyển mạch ra đúng port đích.

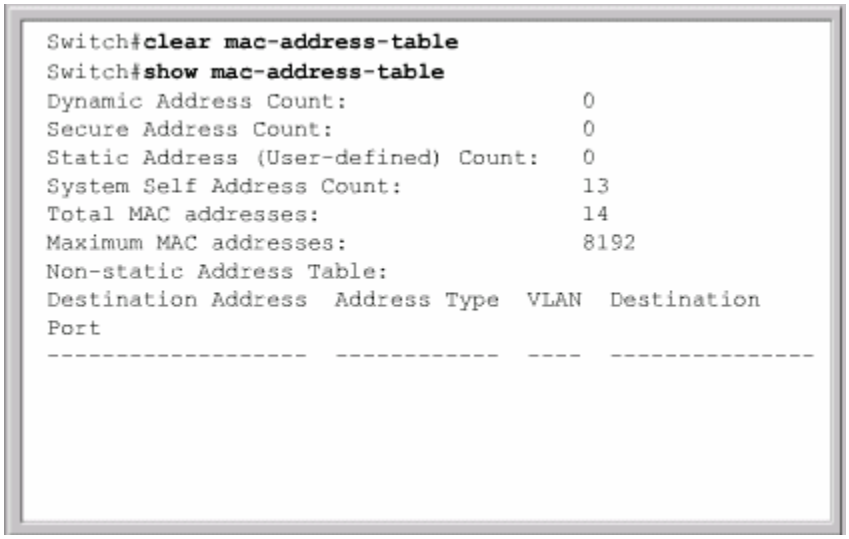
```
Switch#show mac-address-table
Dynamic Address Count:                  2
Secure Address Count:                   0
Static Address (User-defined) Count:    0
System Self Address Count:              13
Total MAC addresses:                    15
Maximum MAC addresses:                  8192
Non-static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

Hình 6.2.3.a

Để kiểm tra các địa chỉ mà switch đã học được, bạn dùng lệnh show mac-address-table trong chế độ EXEC đặc quyền.

Switch có thể tự động học vào bảo trì hàng ngàn địa chỉ MAC. Để tiết kiệm bộ nhớ giúp tối ưu hóa hoạt động của switch, các địa chỉ MAC học được nên xóa đi khi thiết bị tương ứng đã bị ngắt kết nối khỏi port, hoặc bị tắt điện hoặc đã được chuyển sang port khác trên cùng switch đó hoặc trên switch khác. Cho dù vì lý do gì đi nữa, nếu có một địa chỉ MAC nào đó trong bảng mà switch không nhận được gói dữ liệu nào có địa chỉ MAC đó nữa thì switch sẽ tự động xóa địa chỉ đó sau 300 giây.

Thay vì chờ bảng địa chỉ tự động bị xóa vì hết thời hạn thì người quản trị mạng có thể xóa bảng địa chỉ MAC bằng lệnh clear mac-address-table trong chế độ EXEC đặc quyền. Ngay cả những địa chỉ MAC do chính người quản trị mạng cấu hình trước đó cũng bị xóa bằng lệnh này.



Hình 6.2.3.b

6.2.4. Cấu hình địa chỉ MAC cố định

Bạn có thể quyết đinh gán một địa chỉ MAC cố định cho một port nào đó của switch. Lý do để gán cố định một địa chỉ MAC cho một port có thể là một trong những lý do sau:

- Giúp cho địa chỉ MAC không bị xóa tự động do hết thời hạn trên bằng địa chỉ
- Một server hay một máy trạm đặc biệt nào đó của user đươc kết nối vào một port trên switch và địa chỉ MAC của máy này không đổi.
- Tăng khả năng bảo mật.

Để khai báo một địa chỉ MAC cố định cho switch, bạn dùng lệnh sau:

Switch (config)#mac-address-table static <mac-address of host> interface FastEthernet <Ethernet number> vlan

Để xóa một địa chỉ MAC cố định đã được khai báo bạn dùng dạng **no** của câu lênh trên

6.2.5. Cấu hình port bảo vệ

Bảo vệ hệ thống mạng là một trách nhiệm quan trọng của người quản trị mạng. switch tầng truy cập là có khả năng truy cập dễ dàng nhất từ các ổ cắm dây đặt ở các phòng. Bất kỳ người nào cũng có thể cắm PC hoặc máy tính xách tay của mình vào một trong những ổ cắm dây này. Do đó trên switch có một đặc tính gọi là port bảo vệ giúp giới hạn số lượng địa chỉ mà switch có thể học trên một port. Bạn có thể cấu hình cho switch thực hiện một động tác nào đó khi số lượng địa chỉ học được trên port đó vượt quá giới hạn cho phép. Địa chỉ MAC bảo vệ có thể được khai báo cố định. Tuy nhiên việc khai báo cố định địa chỉ MAC bảo vệ rất phức tạp và dễ gây ra lỗi.

Thay vì khai báo địa chỉ MAC bảo vệ cố định thì bạn có thể thực hiện như sau. Trước tiên là bật chế độ port bảo vệ trên port mà bạn muốn. Số lượng địa chỉ MAC trên port đó giới hạn là 1 thôi. Như vậy địa chỉ MAC đầu tiên mà switch tự động học được sẽ trở thành địa chỉ cần bảo vệ.

Để kiểm tra mạng trạng thái của port bảo vệ, bạn dùng lệnh show port security.

Hình 6.2.5

Các bước cơ bản để cấu hình port bảo vệ:

1. Vào chế độ cấu hình của port mà bạn cần.
2. mở chế độ truy cập cho port đó.
3. mở chế độ port bảo vệ.
4. Giới hạn số lượng địa chỉ MAC bảo vệ trên port đó (thường giới hạn 1 địa chỉ MAC)
5. Chỉ định loại địa chỉ MAC bảo vệ là địa chỉ cố định (static), học tự động (dynamic) hay sticky.
    - Static: là địa chỉ MAC do người quản trị mạng khai báo cố định bằng tay. Sau khi khai báo xong, địa chỉ này được lưu cố định trong bảng địa chỉ và không có giới hạn về thời hạn lưu giữ. Ngay cả khi switch bị mất điện, khởi động lại cũng không xóa mất địa chỉ cố định.
    - Dynamic: là địa chỉ MAC do switch tư động học được. Loại địa chỉ động này được lưu có thời hạn trên switch . Nếu trong một khoảng thời gian nhất định mà switch không nhận được gói dữ liệu nào có địa chỉ MAC đó nữa thì nó sẽ xóa địa chỉ này ra khỏi bảng.

- Sticky: là địa chỉ MAC do switch học được tự động nhưng sau khi học xong thì switch ghi địa chỉ này cố đinh vào bảng luôn và không xóa địa chỉ đó nữa ngay cả khi switch bị tắt điện và khởi động lại.

6. Cấu hình cho switch thực hiện động tác đóng port (Shutdown) hoặc treo port (Restrict) khi số lượng địa chỉ MAC học được trên port đó vượt quá giới hạn cho phép.

Câu lệnh cụ thể để cấu hình port bảo vệ trên mỗi dòng switch khác nhau sẽ khác nhau nhưng nhìn chung đều theo các bước cơ bản như trên.

Sau đây là ví dụ về cấu hình port bảo vệ trên switch 2950:

ALSwitch (config)#interface fastethernet 0/4

ALSwitch (config-if)# switchport port-security ?

Aging Port-security aging commands

Mac-address Secure mac address

Maximum Max secure addrs

Violation Security Violation Mode

<cr>

ALSwitch (config-if)# switchport mode access

ALSwitch (config-if)# switchport port-security

ALSwitch (config-if)# switchport port-security maximum 1

ALSwitch (config-if)# switchport port-security mac-address sticky

ALSwitch (config-if)# switchport port-security violation shutdown

6.2.6. Thêm, bớt, chuyển đổi switch

Khi thêm một switch mới vào hệ thống mạng, bạn cần cấu hình các thông tin sau cho switch :

- Tên switch
- Địa chỉ IP của switch trong VLAN quản lý.
- Default gateway.

- Mật mã cho các đường truy cập switch.

Khi chuyển một host từ port này sang port khác hoặc sang switch khác, bạn cũng nên xóa một số cấu hình có thể gây tác động không tốt ở vị trí cũ và thêm cấu hình mới cho vi trí mới của host. Ví dụ khi chuyển một host đang kết nối vào một port có chế độ bảo vệ sang port khác hoặc switch khác, thì ở port cũ bạn nên xóa cấu hình port bảo vệ và cấu hình port bảo vệ cho port mới của host đó.

6.2.7. Quản lý tập tin hoạt động hệ thống của switch

Nhà quản trị mạng luôn phải lập hồ sơ và bảo trì các tập tin hoạt động hệ thống của các thiết bị mạng. Tập tin cấu hình hoạt động mới nhất nên được lưu dự phòng ra server hoặc ra đĩa. Tập tin này không chỉ là thông tin nhạy cảm mà còn rất hữu dụng khi cần khôi phục lại cấu hình cho thiết bị mạng.

IOS cũng nên được lưu dự phòng trên một server nội bộ để sau đó có thể tải về bộ nhớ flash khi cần thiết.

6.2.8. Khôi phục mật mã trên switch 1900/2950

Vì lý do quản lý và bảo mật, switch thường được đặt mật mã trên đường console và vty. Ngoài ra còn có mật mã của chế độ EXEC đặc quyền được cài đặt bằng lênh enable password hoặc enable secret password. Mật mã này giúp đảm bảo chỉ có nhưng user được phép mới có thể truy cập vào chế độ EXEC người dùng và đặc quyền trên switch.

Tuy nhiên có một số tình huống bạn cần truy cập vào switch nhưng bạn truy cập về mặt vật lý được nhưng lại không thể vào được chế độ EXEC người dùng hoặc đặc quyền vì không biết hoặc quên mật mã. Trong những trường hợp như vậy bạn cần phải khôi phục lại mật mã trên switch .

Sau đây là các bước thực hiện để khôi phục mật mã trên switch 2900:

1. Đảm bảo rằng bạn đã kết nối PC của mình vào cổng console trên switch và đã mở xong màn hình HyperTerminal.
2. Tắt điện của switch đi. Sau đó bạn vừa nhấn nút Mode ở mặt trước của switch vừa cắm điện lại cho switch. Khi nào LED STAT trên switch tắt đi thì bạn mới buông nút Mode ra.
3. Khi đó trên màn hình HyperTerminal sẽ có hiện thị như sau:

C2950 Boot Loader (C2950-HBOOT-MAC) Version

12.1 (11r) EA1, RELEASE

SOFT (fc1)

Compiled Mon 22-Jul-02 18:57 by antonio

WS-C2950-24 starting…

Base ethernet MAC Address: 00:0a:b7:72:2b:40

Xmodem file system is available.

The system has been interrupted prior to initializing the flash files

System. The following commands will initialize the flash files system.

And finish loading the operating system software:

Flash_init

Load_helper

Boot

4. Để khởi động tập tin hệ thống và kết thúc quá trình tải hệ điều hành, bạn nhập các lệnh sau theo thứ tự như sau:

Flash_init

Load_helper

Dir flash:

Chú ý: Không được quên dấu hai chấm (:) ở liền sau chữ flash trong câu lệnh thứ 3 ở trên.

Kết quả hiện thị của lệnh dir flash: sẽ cho biết nội dung của thư mục flash. Mặc định, tên của tập tin cấu hình switch lưu trong thư mục flash sẽ có tên là config.text.

5. Bạn đổi định dạng tên của tập tin cấu hình như sau:

Rename flash:config.text flash:config.old

6. Sau đó bạn gõ lệnh boot để khởi động lại switch

Lúc này tập tin cấu hình của switch đã bị đổi định dạng nên switch không tải được tập tin cấu hình. Do đó sau khi khởi động xong bạn sẽ gặp câu thoại cấu hình của switch như sau, bạn nhập ký tự N cho câu hỏi này:

Continue with the configuration dialog? [yes/no] : N

Sau đó bạn sẽ vào được chế độ EXEC người dùng và đặc quyền mà không gặp mật mã nữa.

7. Bạn trả lại tên cũ cho tập tin cấu hình bằng lệnh như sau:

Rename flash:config.old flash:config.text

8. Sau đó cho switch chạy tập tin cấu hình này bằng cách copy tập tin cấu hình này lên RAM:

Switch#copy flash:config.text system:ruinning-config

Source filename [config.text]?[enter]

Destination filename [ruinning-config] [enter]

9. Lúc náy switch sẽ tải tập tin cấu hình xuống RAM để chạy. Khi đó bạn có thể thay đổi mật mã nếu muốn:

AlSwitch#configure terminal

AlSwitch (config)#no enable secret

AlSwitch (config)#enable password cisco

AlSwitch (config)#line console 0

AlSwitch (config-line)#password cisco

AlSwitch (config-line)#exit

AlSwitch (config)#exit

AlSwitch#copy ruinning-config startup-config

Destination filename [startup-config]?[enter]

Building configuration….

[OK]

AlSwitch#

10. Bạn tắt điện cho switch rồi bật lại để kiểm tra xem mật mã mới đã được áp dụng đúng chưa. Nếu chưa đúng thì bạn thực hiện quá trình trên lại từ đầu.

6.2.9. Nâng cấp firmware 1900/2950

IOS và firmware thường xuyên được phát hành phiên bản mới với các khắc phục lỗ hổng cũ, thêm các đặc tính mới và tăng khả năng hoạt động. Nếu bạn muốn hệ thống mạng được bảo vệ tốt hơn, hoạt động hiệu quả hơn với phiên bản mới hơn của IOS thì bạn nên nâng cấp IOS.

Bạn có thể tải phiên bản IOS về server nội bộ của mình từ Trung tâm phần mềm kết nối trực tuyến Cisco (CCO- Cisco Connection Online).

TỔNG KẾT

Sau khi hoàn tất chương này, bạn cần nắm được các ý chính sau:

- Thành phần cơ bản của Catalyst switch .
- Theo dõi trạng thái và hoạt động cảu switch thông qua đèn báo hiệu LED
- Kiểm tra thông tin xuất ra của quá trình khởi động switch bằng HyperTerminal.
- Sử dụng tính năng trợ giúp của giao tiếp dòng lệnh.
- Các chế độ mặc định của switch
- Đặt địa chỉ IP và default gateway cho switch để có thể kết nối và quản lý switch qua mạng.
- Xem cấu hình switch với trình duyệt Web.
- Cài đặt tốc độ và chế độ song công cho port của switch .
- Kiểm tra và quản lý bảng địa chỉ MAC của switch .
- Cấu hình port bảo vệ.
- Quản lý tập tin cấu hình IOS.
- Thực hiện khôi phục mật mã cho switch
- Nâng cấp IOS cho switch

CHƯƠNG 6: Cấu hình switch

Giới thiệu

Switch là một thiết bị mạng Lớp 2 hoạt động như một điểm tập trung kết nối của máy trạm, server, router, hub và các switch khác.

Hub là một thiết bị tập trung kết nối loại cũ, cấp thấp hơn switch vì tất cả các thiết bị kết nối vào hub chia sẻ cùng một băng thông và có thể xảy ra tranh chấp. Hub chỉ có thể chạy bán song công, nghĩa là tại một thời điểm hub hoặc truyền hoặc nhận dữ liệu chứ không thể thực hiện đồng thời cả hai. Còn switch thì có thể chạy song công, truyền và nhận dữ liệu song song đồng thời.

Switch là một brigde đa port: Chuyển mạch đang là một công nghệ chuẩn hiện nay trong cấu trúc hình sao của Ethernet LAN. Khi hai thiết bị kết nối vào switch muốn liên lạc với nhau thì switch thiết lập một mạch ảo điểm đến - điểm dành riêng cho hai thiết bị đó nên không có khả năng xảy ra đụng độ.

Chính vì vai trò quan trọng của switch trong hệ thống mạng hiện nay nên việc tìm hiểu và cấu hình switch là rất quan trọng đối với người làm về mạng.

Một switch hoàn toàn mới luôn có một cấu hình mặc định của nhà sản xuất. Cấu hình này thường không đáp ứng đủ các yêu cầu của nhà quản trị mạng với switch. Một trong những tác vụ này là bảo trì switch và hệ điều hành IOS (Internetworking Oprating System) của nó. Một số tác vụ khác liên quan đến việc quản lý các cổng giao tiếp của switch, tối ưu hoá bảng hoạt động của switch để đảm bảo độ tin cậy và bảo mật. Những kỹ năng về cấu hình switch, nâng cấp IOS, khôi phục mật mã là những kỹ năng rất quan trọng của người quản trị mạng.

Sau khi hoàn tất chương này, bạn có thể thực hiện những công việc sau:

- Xác định các thành phần chính của Catalyst switch.
- Theo dõi hoạt động và trạng thái của switch thông qua các báo cáo hiệu LED.
- Xác định lợi ích và những nguy cơ của cấu trúc dự phòng.
- Mô tả vai tro của Spanning - Tree trong mạng chuyển mạch có dự phòng.
- Xác định các thành phần quan trọng trong hoạt động của Spanning — Tree.
- Mô tả quá trình bầu bridge gốc.
- Liệt kê các trạng thái Spanning — Tree.
- So sánh giao thức Spanning — Tree.

7.1. Cấu trúc dự phòng.

7.1.1. Sự dự phòng.

Rất nhiều công ty và tổ chức đã phát triển hoạt động của họ dựa trên mạng máy tính. Việc truy cập vào file server, cơ sở dữ liệu, Internet, Intranet và Extranet đóng vai trò quan trọng cho sự thành công trong kinh doanh vì nếu mạng bị đứt, năng suất giảm và khách hàng không hài lòng.

Do đó các công ty luôn mong muốn hệ thống mạng may tính của họ luôn hoạt động suốt 24 giờ, 7 ngày một tuần. Việc thực hiện 100% thời gian hoạt động thì có thể không khả thi nhưng mục tiêu đặt ra là phải bảo đảm được 99,999% thời gian hoạt động. Tỉ lệ này có nghĩa là chỉ cho phép mạng ngưng hoạt động trung bình một ngày trong 30 năm, hay 1 giờ trong 4000 ngày, hay 5,25 phút trong một năm.

Nếu có thể thực hiện được mục tiêu trên thì hệ thống mạng sẽ thực sự hoạt động rất tin cậy. Độ tin cậy của hệ thống mạng được đảm bảo từ việc trang bị các thiết bị có độ tin cậy cao đến việc thiết kế hệ thống mạng có dự phòng, có khả năng chịu được lỗi, hội tụ nhanh để vượt qua sự cố.

Mạng có khả năng chịu được lỗi nhờ có sự dự phòng. Dự phòng ở đây có nghĩa là chuẩn bị những gì nhiều hơn mức cần thiết bình thường. Nhưng dự phòng giúp tăng độ tin cậy của mạng như thế nào?

Giả sử như bạn chỉ có một cách duy nhất để đi làm là đi làm bằng xe hơi của bạn, vậy nếu chiếc xe hơi này bị hư có nghĩa là bạn không thể đi làm cho đến khi chiếc xe hơi này được sửa chữa xong.

Nếu chiếc xe này cứ trung binh 10 ngày lại hư mất 1 ngày thì khả năng sử dụng của nó là 90%. Điều này có nghĩa là cứ 10 ngày thì bạn chỉ đi làm được 9 ngày. Do đó độ tin cậy đạt được 90%.

Nếu bạn mua thêm một xe hơi nữa để đi là. Đúng là không cần thiết phải có đến 2 chiếc xe hơi chỉ để đi làm nhưng bạn lại có xe dự phòng khi chiếc xe chính bị hư. Như vậy việc đi làm của bạn sẽ không còn bị phụ thuộc vào một chiếc xe nữa.

Cả hai chiếc xe cũng có thể bị hư cùng một lúc, khoảng 100 ngày thì có một ngày như thế. Như vậy bạn mua thêm chiếc xe thứ 2 để dự phòng, độ tin cậy đã tăng lên 99%.

Hình 7.1.1

7.1.2. Cấu trúc dự phòng.

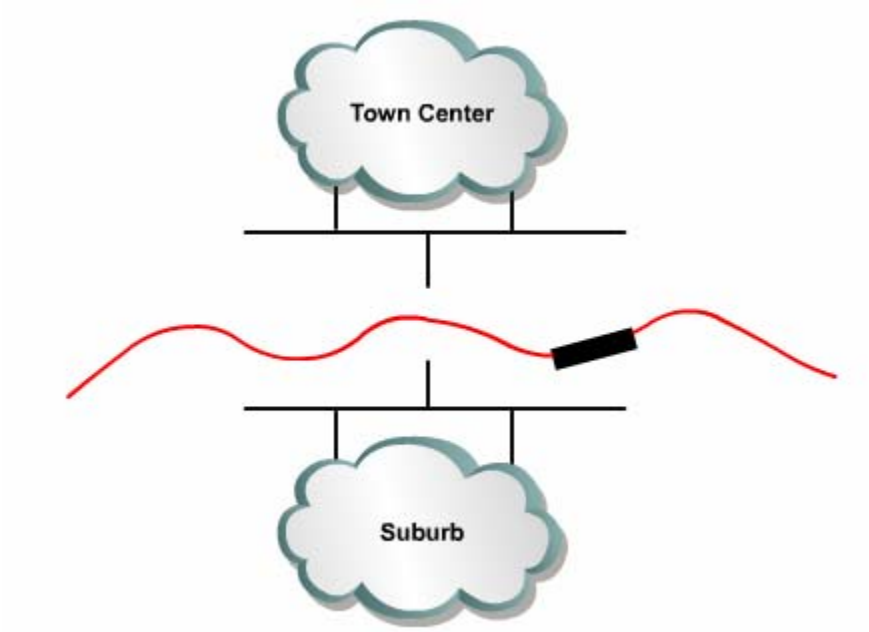
Mục tiêu của cấu trúc dự phòng là loại bỏ điểm tập trung của sự cố. Tất cả các hệ thống mạng cần phải có dự phòng để nâng mức độ bảo đảm.

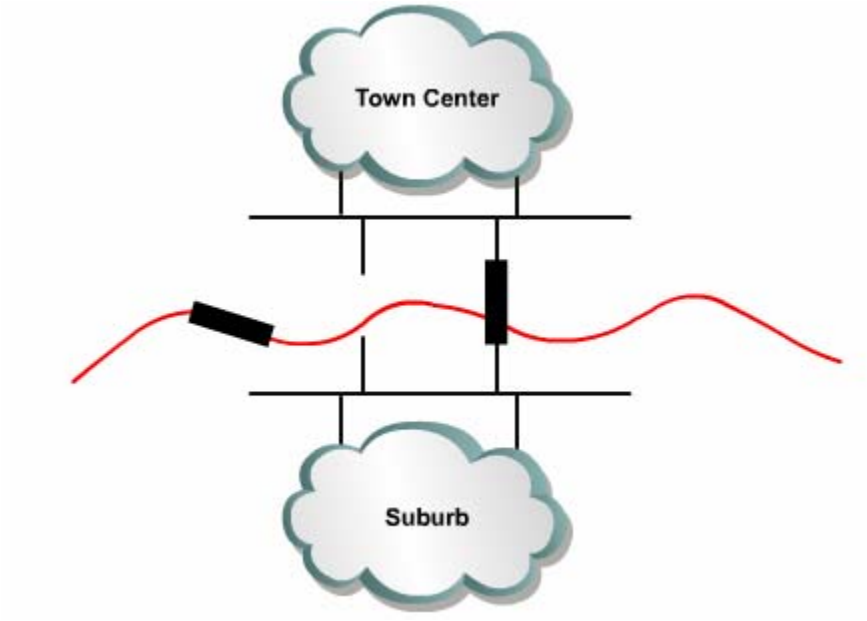
Hệ thống đường giao thông là một ví dụ về cấu trúc có tính dự phòng. Nếu có một con đường bị đóng lại để sửa chữa thì sẽ luôn có đường khác để đi đến đích.

Ví dụ có một công đồng cách trung tâm thị trấn bởi có một con sông. Nếu chỉ bắc một chiếc cầu qua sông đó thì có nghĩa là chỉ có một con đường đi vào thị trấn. Cấu trúc như vậy là không có sự dự phòng.

Nếu cây cầu này bị ngập hoặc bị hư hỏng do tai nạn thì sẽ không thể đi vào thị trấn bằng chiếc cầu này được nữa.

Bắc thêm một chiếc cầu thứ hai qua sông để tạo cấu trúc có dự phòng. Khi đó người dân ở ngoại ô sẽ không còn bị cắt đứt với trung tâm thị trấn khi một cây cầu bị hư hỏng nữa.





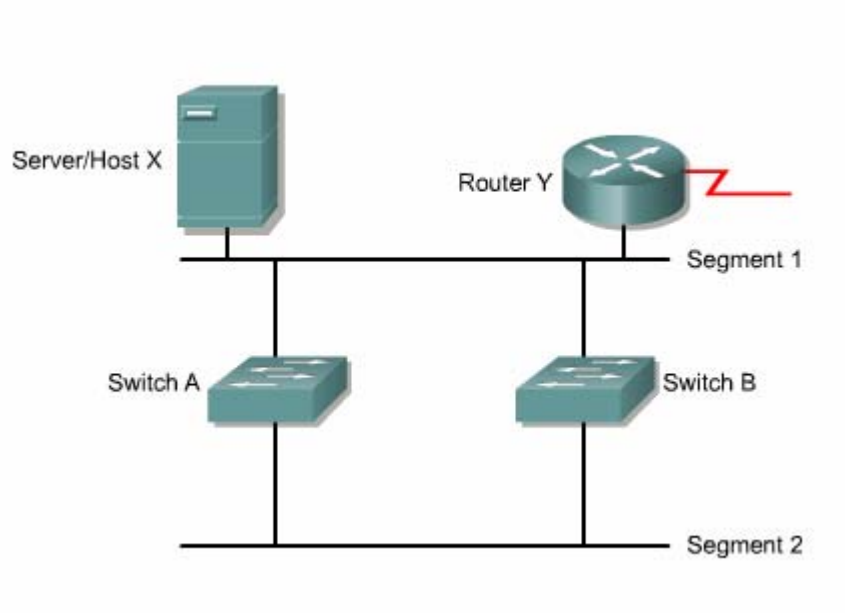
Hình 7.1.2. mô hình có dự phòng và không có dự phòng.

7.1.3. Cấu trúc chuyển mạch dự phòng.

Hệ thống mạng có thiết bị và đường dự phòng sẽ có khả năng tồn tại cao hơn, tránh được mô hình chỉ có một điểm trung tâm của sự cố vì nếu một đường kết nối hoặc một thiết bị gặp sự cố thì đường dự phòng hoặc thiết bị dự phòng sẽ lãnh trách nhiệm thay thế.

Ví dụ như hình 7.1.3, nếu Switch A bị hư, lưu lượng từ segment 2 sang segment 1 và sang router vẫn có thể đi qua Switch B.

Nếu port 1 trên Switch A bị hư thi giao thông vẫn có thể đi qua port 1 trên Switch B.



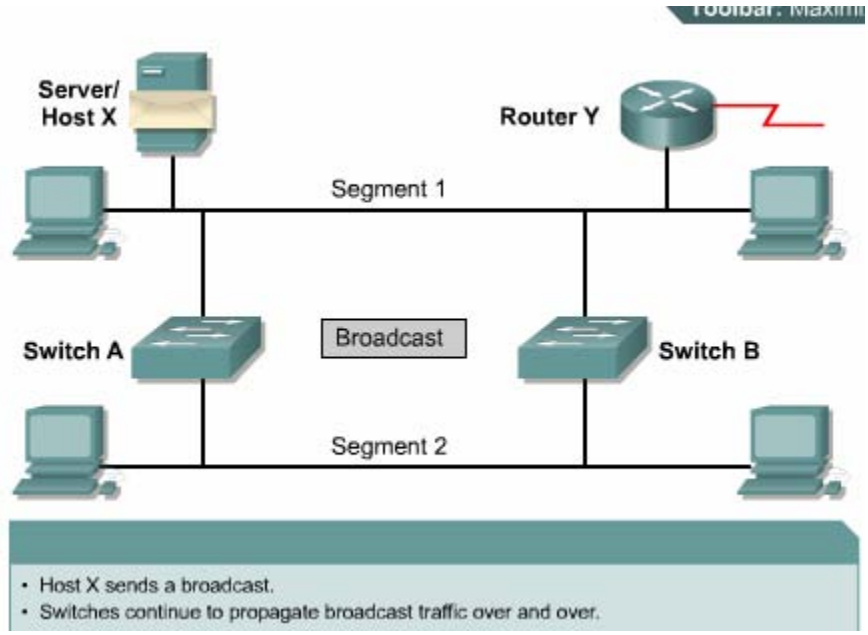
Hình 7.1.3

Switch học địa chỉ MAC của thiết bị kết nối vào port của nó, nhờ đó nó có thể chuyển dữ liệu đến đúng đích. Nếu switch không biết gì về địa chỉ của máy đích thì nó sẽ chuyển gói ra tất cả các port cho đến khi nào nó học được địa chỉ MAC của thiết bị này. Gói quảng bá và multicast cũng được chuyển ra tất cả các port của switch.

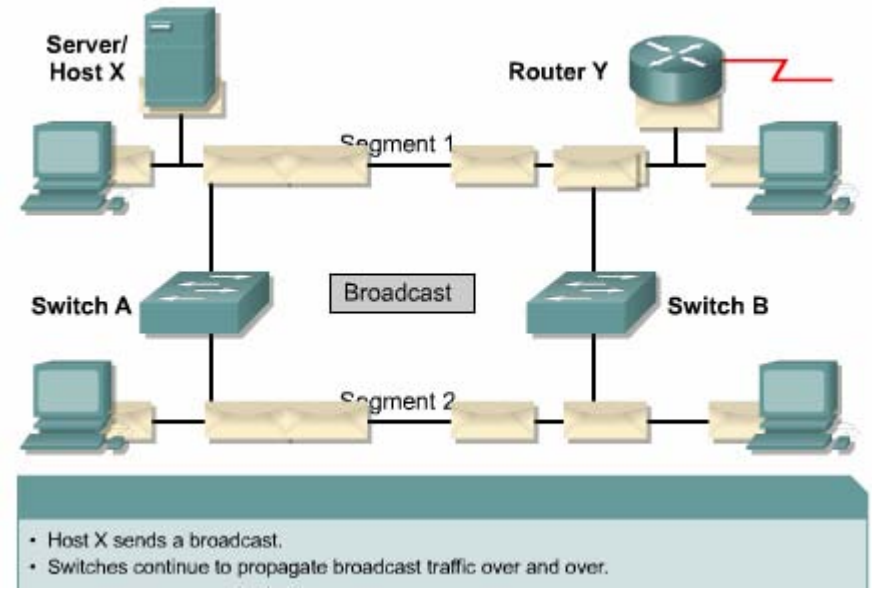
Chính vì vậy, cấu trúc chuyển mạch dự phòng như hình 7.1.3 có thể sẽ gây ra trận bão quảng bá, chuyển nhiều lượt frame và bảng địa chỉ MAC không ổn định.

7.1.4. Trận bão quảng bá.

Gói multicast cũng được switch sử lý giống như gói quảng bá là chuyển ra tất cả các port trừ port nhận gói vào.



Hình 7.1.4.a



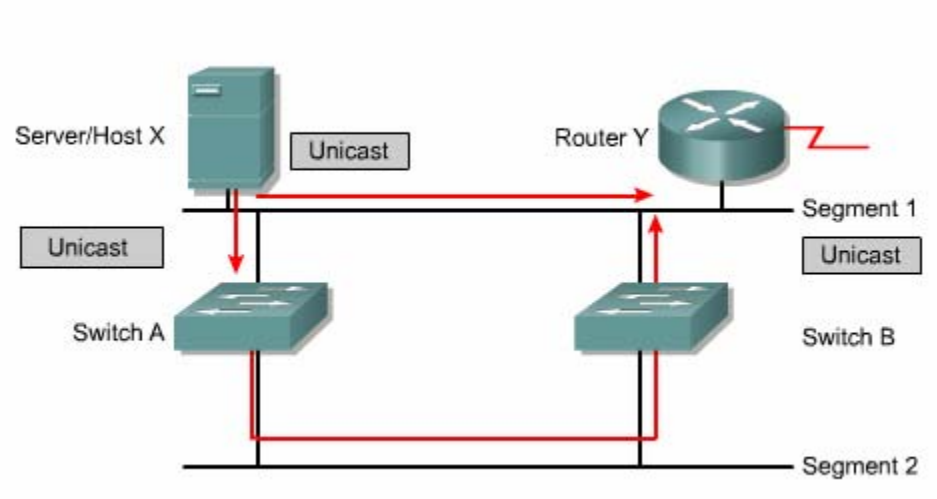
Hình 7.1.4.b. Hậu quả là gây ra một trận bão quảng bá trên mạng.

Ta xét ví dụ trên hình 7.1.4.a: giả sử Host X gửi một gói quảng bá và gói yêu cầu ARP để hỏi địa chỉ lớp 2 của router chẳng hạn. Khí đó switch A nhận được gói quảng bá này sẽ chuyển gói quảng bá này sẽ chuyển gói ra tất cả các port. Switch B cũng thực hiện như vậy. Kết quả là Switch B sẽ nhận lại các gói quảng bá được gửi từ Switch A và ngược lại, Switch A cũng nhận lại các gói quảng bá được gửi từ Switch B. Cả hai Switch này nhận được gói quảng bá của nhau và lại chuyển tiếp ra tất cả các port.

Cứ như vậy, mỗi một gói quảng bá mà switch nhận vào sẽ được nhân ra tất cả các port gây lên trận bão quảng bá trên mạng. Trận bão quảng bá này sẽ được tiếp tục cho đến khi nào một trong hai switch bị ngắt kết nối ra. Switch và các thiết bị đầu cuối sẽ bị quá tải vì phải sử lý quá nhiều các gói quảng bá và không thể sử lý được các gói dữ liệu khác của user. Khi đó hệ thống mạng xem như bị tê liệt.

7.1.5. Truyền nhiều lượt frame.

Cấu trúc mạng chuyển mạch dự phòng có thể làm cho thiết bị đầu cuối nhận được nhiều frame trung lặp nhau.



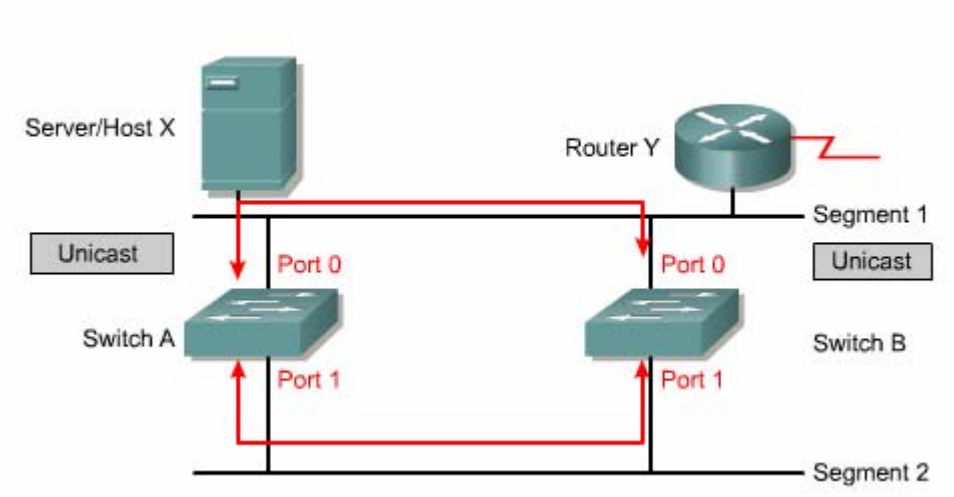
Hình 7.1.5

Ta xét ví dụ trên hình 7.1.5: giả sử rằng cả hai switch vừa mới xoá địa chỉ MAC của Router Y trên bảng địa chỉ vì hết thời hạn và giả sử rằng Host X vẫn còn giữ địa chỉ MAC của router Y trong bảng ARP của mình lên nó gửi một frame trực tiếp tới Router Y. Router Y nhận được gói giữ liệu này vì nó nằm trong cùng segment với Host X.

Switch A cũng nhận được frame này nhưng không có địa chỉ MAC của Router Y trên bảng địa chỉ nên nó chuyển frame ra tất cả các port của nó. Tương tự trên switch B cũng vậy. Kết quả là Router Y nhận được nhiều frame trùng nhau. Điều này làm cho các thiết bị tốn tài nguyên để xử lý nhiều frame không cần thiết.

7.1.6. Cơ sở dữ liệu địa chỉ MAC không ổn định.

Cấu trúc mạng chuyển mạch dự phong có thể làm cho các switch học được thông tin sai về địa chỉ, switch sẽ học được một địa chỉ MAC trên một port mà trong khi địa chỉ MAC này thật sự nằm trên port khác.



Hình 7.1.6

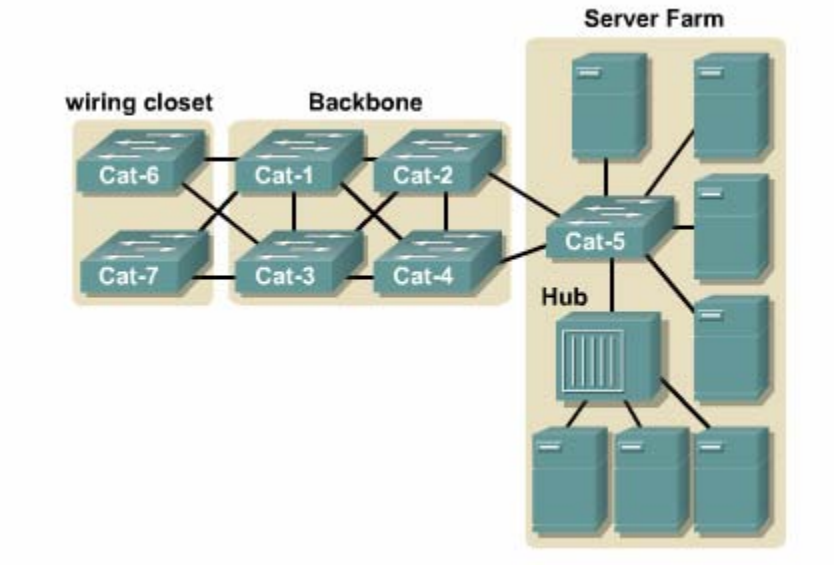
Ta xét ví dụ như trên hình 7.1.6: giả sử địa chỉ MAC của Router Y không có trong bảng địa chỉ của cả hai switch.

Giả sử host X gửi một gói dữ liệu trực tiếp đến Router Y. Switch A và B đều nhận được gói gữi liệu này và học được địa chỉ MAC của Host X là nằm trên port 0. Sau khi đó dữ liệu này được hai switch chuyển ra tất cả các port vì trên hai switch đều chưa có địa chỉ MAC của Router Y. Kết quả là switch A nhận lại gói dữ liệu này từ switch B vào port 1 và ngược lại, Switch B cũng nhận lại dữ liệu từ Switch A vào port 1. Khi đó Switch A và B học lại là địa chỉ MAC của Host X nằm trên port 1, kế tiếp, khi Router Y gửi một gói dữ liệu cho Host X, Switch Avà B cũng đều nhận được gói dữ liệu từ Router Y đến Host X sẽ bị rơi vào vòng lặp.

7.2. Giao thức Spanning □ Tree (Giao thức phân nhánh cây).

7.2.1. Cấu trúc dự phòng và Spanning □ Tree.

Cấu trúc mạng dự phòng được thiết kế để bảo đảm mạng tiếp hoạt động khi có một sự cố xảy ra, user sẽ ít bị gián đoạn công việc của họ hơn. Mọi sự gián đoạn do sự cố gây ra càng ngắn càng tốt.



Hình 7.2.1.a. Một ví dụ về cấu trúc dự phòng.

Trong hệ thống mạng, chúng ta tạo nhiều kết nối giữa các switch và bridge để dự phòng. Các kết nồi này sẽ tạo ra các vòng lặp vật lý trong mạng nhưng nếu có một kết nối bị đứt thi lưu lượng có thể được chuyền sang kết nối khác.

Switch hoạt động ở lớp 2 của môi hình OSI và thực hiện quyết định chuyển gói ở lớp này. Khi Switch không xác định được port đích thì nó sẽ chuyển gói ra tất cả các port. Gói quảng bá và multicast cũng được gửi ra tất cả các port trừ port nhận gói vào. Do đó, mạng chuyển mạch không được có vòng lặp, vì như vậy sẽ gây ra nhiều sự cố như đã phân tích ở các phần trên.

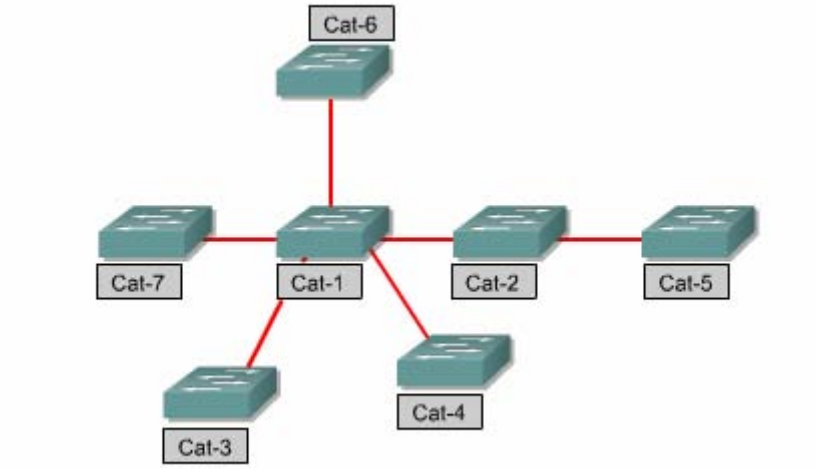
Ở lớp 3, mỗi khi gói dữ liệu đi qua một Router, trường thời gian sống (Time To Live — TTL) sẽ giảm đi một giá trị và gói dữ liệu sẽ bị huỷ bỏ khi trường TTL đạt đến giá trị 0. Trong khi đó, phần thông tin lớp 2 trong gói dữ liệu không có trương TTL. Do đó, nếu frame bị rơi vào vòng lặp lớp 2 của cấu trúc mạng chuyển mạch, nó sẽ bị lặp vòng đến vô tận vì không có thông tin nào trong frame giúp loại bỏ frame khi bị lặp vòng. Điều đó làm hệ thống mạng tiêu tốn băng thông và có thể dẫn đến bị tê liệt.

Tóm lại, mạng chuyển mạch với switch và bridge không thể có vòng lặp nhưng chúng ta vẫn cần xây dựng cấu trúc mạng vật lý có vòng lắp để dự phòng khi xảy ra sự cố, nhằm đảm bảo hoạt động của hệ thống mạng.

Vậy giải pháp là vẫn cho phép cấu trúc vật lý có vòng lặp nhưng chúng ta sẽ tạo cấu trúc luận lý không có vòng lặp. Ví dụ như trên hình 7.2.1.a, giao thông từ các user kết nối vào Cat - 4 đến server Farm kết nối vào Cat - 5 sẽ đi qua đường kết nối giữa Cat - 1 và Cat - 2 mặc dù có tồn tại đường kết nối vật lý giữa Cat - 4 và Cat - 5.

Cấu trúc luận lý không vòng lặp là một cấu trúc dạng phân nhánh cây, tương tự như cấu trúc luận lý hình sao hay hình sao mở rộng.

Thuật toán được sử dụng để tạo cấu trúc luận lý không vòng lặp là thuật toán spanning - tree. Thuật toán này tồn tại khá nhiều thời gian để hội tụ. Do đó có một thuật toán mới hơi gọi là rapid spanning - tree với thời gian tinh toán cấu trúc luận lý không vòng lặp rút ngắn hơn.

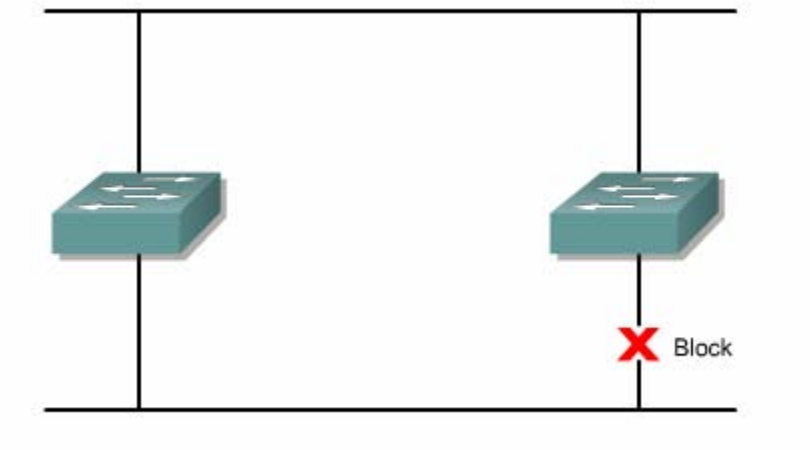


Hình 7.2.1.b. Cấu trúc luận lý không vòng lặp được tạo ra bởi Spanning - Tree. Cấu trúc này theo dạng phân nhánh hình cây, tương tự như cấu trúc luận lý hình sao mở rộng.

7.2.2. Giao thức Spanning - Tree.

Ethernet bridge và switch có thể triển khai giao thức Spanning - Tree IEEE802.1D và sử dụng thuật toán spanning - tree để xây dựng cấu trúc mạng ngắn nhất không vòng lặp.

Để xây dựng mạng theo dạng phân nhánh hình cây, trước tiên giao thức Spanning - Tree phải chọn một điểm làm gốc (root bridge). Xuất phát từ một bridge gốc này, các đường liên kết được xem xét và tính toán để phân nhánh ra tạo cấu trúc mạng theo dạng hình cây, bảo đảm rằng chỉ có một đường duy nhất đi từ gốc đến từng node trong mạng. Những đường kết nối nào dư thừa trong cấu trúc hình cây sẽ bị khoá lại. Tất cả các gói dữ liệu nhận được từ đường liên kết bị khoá này sẽ bị huỷ bỏ.



Hình 7.2.2.a. Giao thức Spanning - Tree xây dựng mạng hình luận lý hình cây. Kết nối nào dư thừa, tạo thành vòng lặp sẽ bị khoá lại.

Giao thức Spanning - Tree đòi hỏi thiết bị mạng phải trao đổi thông tin với nhau để có thể phát hiện ra vòng lặp trong mạng. Thông điệp trao đổi này được gọi là Bridge Protocol Data Unit (BPDU). Kết nối nào tạo thành vòng lặp sẽ bị đặt vào trạng thái khoá. Trên kết nối này không nhận gói dữ liệu nhưng vẫn nhận các gói BPDU để xác định kết nối đó còn hoạt động hay không. Nếu có một kết nối bị đứt hay một thiết bị hư hỏng thì một cấu trúc hình cây mới sẽ được tính toán lại.

BPDU chứa đầy đủ các thông tin giúp cho switch thực hiện được các việc sau:

• Chọn một switch làm gốc cho cấu trúc hình cây.

• Tính toán đường ngắn nhất từ mỗi node đến switch gốc. Đường ngắn nhất là đường có chi phí thấp nhất. Chi phí của đường kết nối được tính toán dựa trên tốc độ của đường kết nối đó.

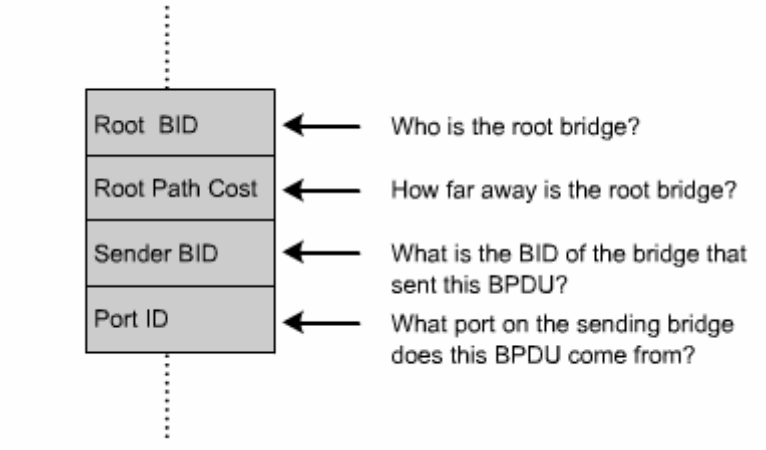
• Trong từng LAN segment, chỉ định ra một switch gần nhất với switch gốc. Switch được chỉ định (designated switch) sẽ lắm giữ mọi thông tin liên lạc giữa LAN và switch gốc.

• Trên mỗi switch không phải là gốc chọn một port làm port gốc (root port) là port có đường kết nối ngắn nhất về gốc.

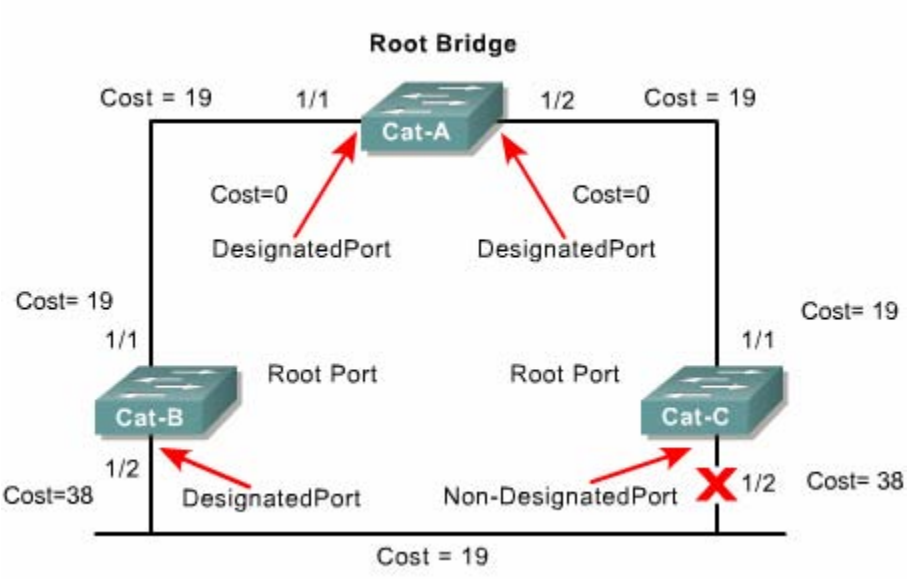
• Các port còn lại được xem xét để làm port chỉ định (designated port). Những port nào không được chỉ định đều bị khoá lại.

Link Speed	Cost(Revised IEEE Spec)	Cost (Previous IEEE Spec)
10 Gbps	2	1
1 Gbps	4	1
100 Mbps	19	10
10 Mbps	100	100

Hình 7.2.2.b. Giá trị chi phí mặc đinh tương ứng với tốc độ của đường kết nối.



Hình 7.2.2.c. Các thông tin nằm trong gói BPDU.



Hình 7.2.2.d. Một ví dụ để kết quả tính toán của giao thức Spanning - Tree. Sau khi tính toán xong, về mặt luận lý, cấu trúc mạng sẽ có dạng rẽ nhánh cây, không còn vòng lặp nữa.

Ta xét ví dụ như hình 7.2.2.c. Ba switch Cat - A, Cat - B và Cat - C được nối thành vòng tròn với nhau. Như vậy là tồn tại một vòng lặp về mặt vật lý. Đầu tiên, quá trình bầu chọn bridge gốc đã chọn Cat - A làm gốc. Từ bridge gốc, hai nhánh từ port 1/1, 1/2 được mở lên để kết nối xuống hai switch Cat - B và Cat - C. Trên Cat - B, port 1/1 có chi phí nối về gốc thấp nhất nên port này được chọn làm port gốc. Tương tự trên Cat - C, port 1/1 được chọn làm port gốc để nối về gốc. Sau khi đã xác định xong port gốc để thiết lập kết nối về bridge gốc, Cat - B và Cat - C sẽ xem xét các port còn lại. Chúng nhận thấy port 1/2 của chúng cùng nối vào một segment LAN. Để tạo cấu trúc hình cây, trong mỗi segment LAN chỉ có một switch được mở một đường để kết nối từ gốc vào segment LAN đó. Do đó, Cat - B và Cat - C sẽ chỉ định ra một switch được truy xuất vào segment LAN này. Kết quả, Cat - B được chọn và port 1/2 của nó được chỉ định mở kết nối vào segment LAN. Cat - C không được chỉ đinh nên port 1/2 của nó bị khoá lại.

7.2.3. Hoạt động của spanning - tree.

Khi mạng đã ổn định và hội tụ chỉ có một cây duy nhất trong một mạng.

Để đạt được kết quả này, các switch trong mạng tuân theo các nguyên tắc sau:

• Chỉ có một bridge gốc duy nhất cho một mạng.

• Trên mỗi bridge không phải là gốc chỉ có một port duy nhất làm port gốc là port kết nối về gốc ngắn nhất.

• Trong từng segment LAN, chỉ được duy nhất một port đi vào segment LAN đó.

• Không sử dụng các port nào không được chỉ định.

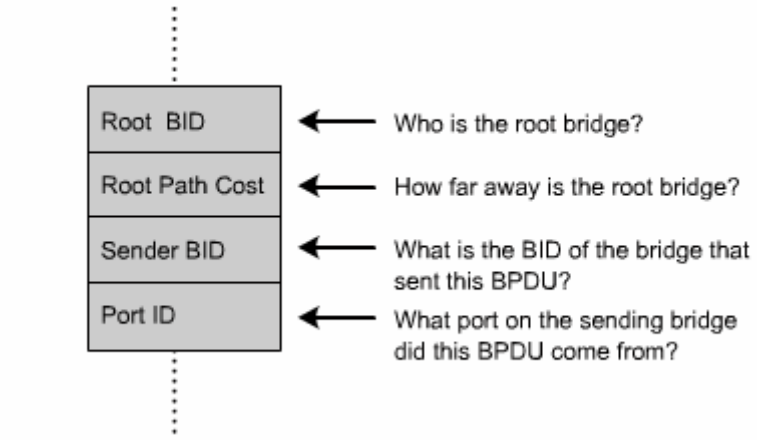
Port gốc và port được chỉ định làm các port được sử dụng để chuyển dữ liệu.

Các port không được chỉ định sẽ huỷ bỏ dữ liệu. Các port này được gọi là port khoá (B - Bloking).

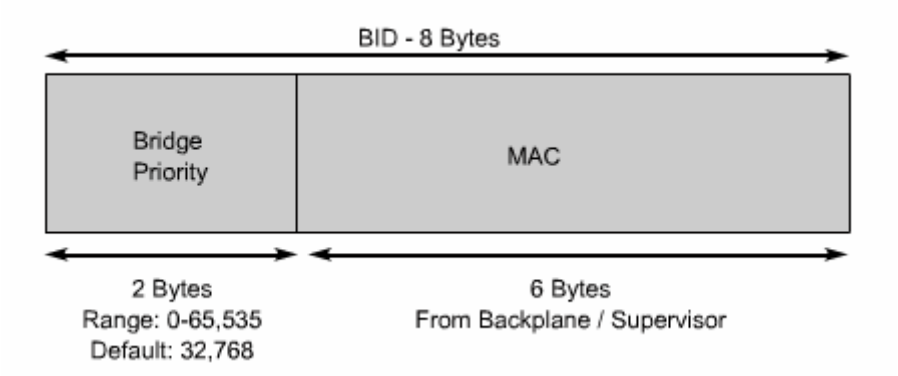
7.2.4. Quá trình chọn bridge gốc.

Muốn xây dựng cấu trúc hình cây thì trước tiên phải có một điểm làm gốc để từ đó phân nhánh cho cây. Do đó việc đầu tiên là tất cả các switch trong mạng phải chọn ra một bridge gốc sẽ tác động đến dòng giao thông trong mạng.

Khi các switch mới được bật điện, chúng sẽ trao đổi các gói BPDU với nhau và dựa vào thông tin bridge ID (BID) trong các gói này để chọn ra bridge gốc. Trường BID bao gồm giá trị độ ưu tiên của switch và địa chỉ MAC của switch đó. Giá trị ưu tiên mặc định của switch là 32768. Mặc định, các gói BPDU được gưi đi 2 giây/lần.

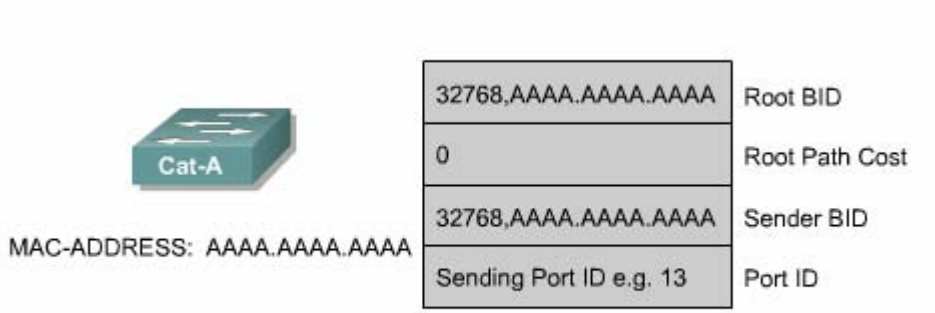


Hình 7.2.4.a. Nội dung gói BPDU.



Hình 7.2.4.b. Cấu trúc của trường BID. 2 byte đầu là giá trị ưu tiên của switch. Giá trị này nằm trong khoảng từ 0 - 65535, giá trị mặc định là 32768. 6 byte sau là địa chỉ MAC của switch.

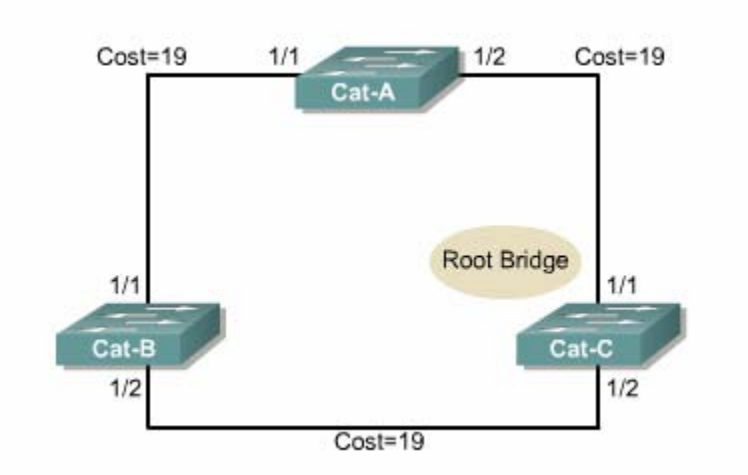
Đầu tiên mỗi switch đều tự cho nó là gốc. Do đó trong gói BPDU đầu tiên mà mỗi switch gửi đi, trường Root BID và sender BID đều có giá trị ưu tiên và địa chỉ MAC của chính nó. Sau đó mỗi switch sẽ lần lượt nhận được các goi BPDU từ những switch khác. Mỗi khi switch nhận được một gói BPDU có trường Root BID thấp hơn Root BID nó đang có thì nó sẽ thay thế Root BID thấp hơn vào gói BPDU rồi gửi đi. Cứ như vậy, cuối cùng các switch sẽ thống nhất được với nhau switch nào có BID thấp nhất làm bridge gốc.



Hình 7.2.4.c. Một ví dụ về nội dung gói BPDU đầu tiên của Cat - A gửi đi.

Nếu không cấu hình gì cả, giá trị mặc định trên các switch đều bằng nhau và bằng 32768. Do vậy switch nào nào có địa chỉ MAC nhỏ nhất (địa chỉ MAC thì không bao giờ trùng nhau giữa các switch) sẽ có BID nhỏ nhất và switch đó sẽ làm gốc. Người quản trị mạng muốn tác động vào việc quyết định chọn bridge gốc thì

có thể cài đặt giá trị ưu tiên của switch nhỏ hơn giá trị mặc định, khi đó BID của switch sẽ có giá trị nhỏ hơn. Tuy nhiên bạn chỉ lên làm điều này khi bạn nắm rõ luồng giao thông trong mạng của mình.



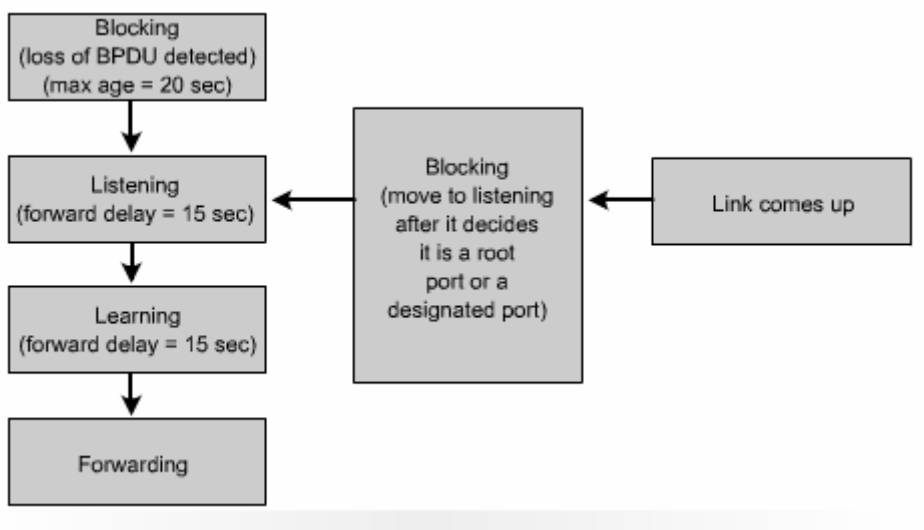
Hình 7.2.4.d. Sau một quá trinh trao đổi gói BPDU, các switch sẽ chọn ra được switch nào có BID nhỏ nhất làm gốc.

7.2.5. Các trạng thái port Spanning - Tree.

Thông tin trao đổi của các giao thức phải mất một khoảng thời gian mới truyền đi hết cho toàn bộ hệ thống mạng. Khi một phân nào đó của cấu trúc mạng bị thay đổi thì cả hệ thống không thể nhận biết được điều này cùng một lúc và ngay lập tức mà phải lần lượt sau đó một khoảng thời gian. Đó chính là thời gian trễ lan truyền. Chính vì vậy, nếu switch đổi trạng thái của một port từ thụ động sang hoạt động ngay lập tức có thể sẽ gây ra vòng lặp.

Trên switch sử dụng giao thức Spanning - Tree, mỗi port sẽ ở một trong năm trạng thái như hình 7.2.5.a.

ở trạng thái khoá, port chỉ nhận gói BPDU. Các gói dữ liệu khác sẽ bị huỷ bỏ và không hề có học địa chỉ ở trạng thái này. Mất khoảng 20 giây để chuyển từ trạng thái này sang trạng thái kế tiếp là trạng thái nghe.



Hình 7.2.5.a. Các trạng thái port Spanning - Tree. Khi kết nối bắt đầu được mở lên, trạng thái đầu tiên của port là trạng thái khoá (Blocking). Sau khi thuật toán Spanning - Tree tính toán xong và chọn port đó là port gốc hay là port chỉ định của một segment LAN thì port sẽ được lần lượt chuyển sang trạng thái nghe (Listenning), trạng thái học (Learning) và cuối cùng trạng thái truyền dữ liệu (Forwarding).

ở trạng thái nghe, switch chỉ xác định xem port này có kết nối về gốc với chi phí thấp nhất hay không, có tạo vòng lặp hay không. Nếu kết quả port này không được chọn làm port gốc và cũng không được chỉ định làm port nối vào một segment LAN nào thì port sẽ được đưa trở về trạng thái khoá. Trạng thái nghe kéo dài khoảng 15 giây, khoảng thời gian này gọi là thời gian chờ chuyển trạng thái (Forward delay). Trong trạng thái nghe, port vẫn không chuyển gói dữ liệu, chưa học địa chỉ MAC, vẫn chỉ xử lý gói BPDU thôi.

Sau đó, port chuyển từ trạng thái nghe sang trạng thái học. ở trạng thái này, port chưa chuyển dữ liệu của user nhưng đã bắt đầu học địa chỉ MAC từ các gói dữ liệu nhận được và vẫn xử lý gói BPDU. Trạng thái học kéo dài khoảng 15 giây và khoảng thời gian này cũng được gọi thời gian chờ chuyển trạng thái (Forward delay).

Sau cùng, port chuyển từ trạng thái học sang trạng thái truyền dữ liệu. ở trạng thái này, port thực hiện truyền dữ liệu của user, học địa chỉ MAC đồng thời vẫn xử lý gọi BPDU.

Một port có thể rơi vào trạng thái không hoạt động (disable). Trạng thái này là do người quản trị cài đặt cho port bằng lệnh shutdown hoặc do chính bản thân port không có kết nối hoặc bị hư, không hoạt động được.

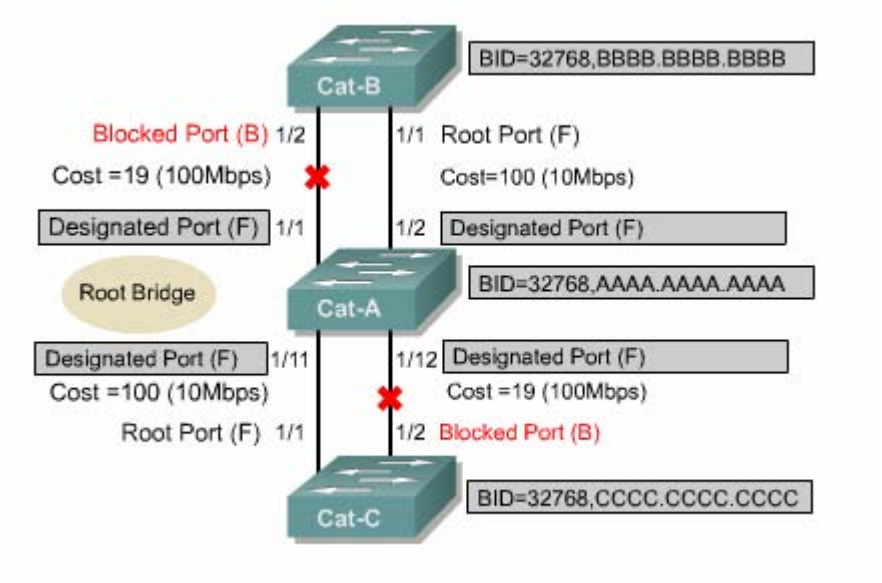
Khoảng thời gian của mỗi trạng thái như đã nêu ở trên là khoảng thời gian mặc định được tính cho một hệ thống mạng có tối đa 7 switch trên một nhánh tính từ gốc.

7.2.6. Spanning - Tree tính toán lại.

Sau khi hệ thống mạng chuyển mạch đã hội tụ, tất cả các port trên mọi switch và bridge đều ở trạng thái truyền dữ liệu hoặc trạng thái khoá. Port truyền dữ liệu là port có thể truyền , nhận dữ liệu và BPDU. Port khoá là port chỉ nhận gói BPDU mà thôi.

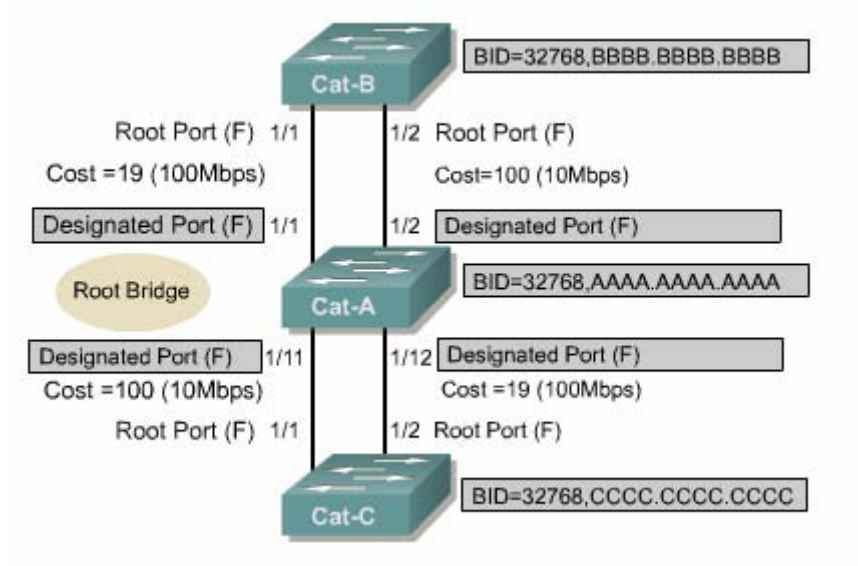
Khi cấu trúc mạng có sự thay đổi, switch và bridge sẽ tính toán lại cấu trúc hình cây và có thể gây cản trở cho giao thông mạng của user khi đang trong quá trình tính toán.

Thời gian hội tụ theo chuẩn IEEE 801.1D cho cấu trúc hình cây mới là khoảng 50 giây. Khi cấu trúc mạng có sự thay đổi xảy ra, sau thời gian chờ tối đa (max - age) là 20 giây để xác định sự thay đổi đó, Spanning - Tree mới bắt đầu tính lại và chuyển trạng thái cho port. Từ trạng thái khoá, port được chuyển sang trạng thái nghe. Sau đó ở trạng thái nghe 15 giây rồi mới chuyển sang trạng thái học và ở trạng thái học 15 giây rồi mới chuyển sang trạng thái truyền dữ liệu. Như vậy tổng cộng là 50 giây để cấu trúc mạng chuyển sang cấu hình cây mới đáp ứng theo sự thay đổi.



Hình 7.2.6.a

Ví dụ một cấu trúc mạng chuyển mạch đã hội tụ như trên. Theo chu kỳ mặc định, cứ 20 giây các switch lại thực hiện trao đổi gói BPDU một lần. Giả sử kết nối trên port 1/1 của Cat - B bị đứt. Khi đó Cat - B không còn nhận được gói BPDU theo định kỳ trên port 1/1 nữa. Trong khi đó Cat - B vẫn nhận được gói BPDU đều đặn trên port 1/2. Cat - B đợi hết thời gian chờ tối đa (max - age) là 20 giây mới xác định kết nối trên port 1/1 đã chết và bắt đầu chuyển sang trạng thái cho port 1/2. Port 1/2 không thể chuyển ngay từ trạng thái khoá sang trạng thái chuyền dữ liệu được mà phải trải qua 2 trạng thái trung gian là trạng thái nghe và trạng thái học, mỗi trạng thái trung gian này kéo dài 15 giây. Như vậy tổng cộng là 50 giây kể từ lúc kết nối trên port 1/1 của Cat - B bị đứt, mạng mới chuyển xong sang cấu trúc mới để đáp ứng theo sự cố này.



Hình 7.2.6.b. Kết quả tính lại là cấu trúc mới như hình vẽ.

7.2.7. Giao thức Rapid Spanning - Tree.

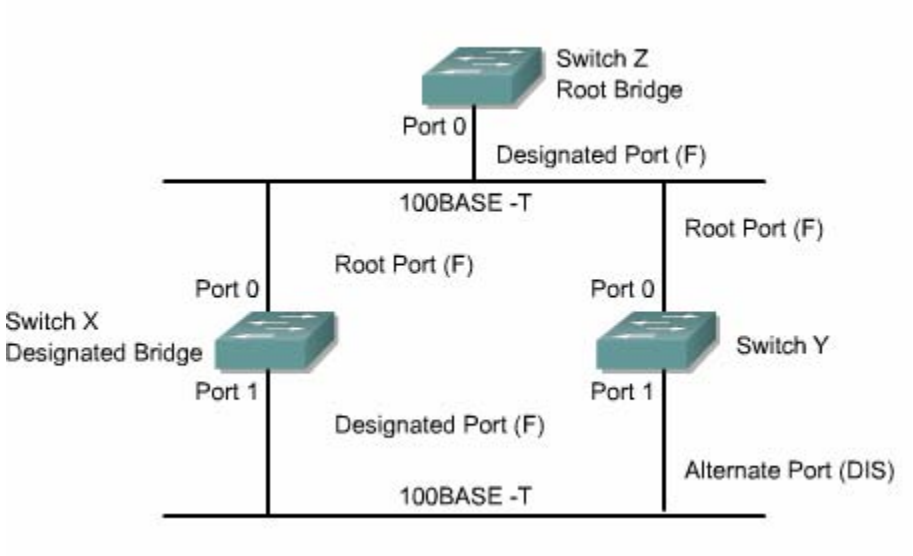
Giao thức Rapid Spanning - Tree được định nghĩa trong chuẩn IEEE 802.1w. Giao thức này giới thiệu các vấn đề mới sau:

• Làm rõ hơn vai trò và trạng thái của port.

• Định nghĩa các loại kết nối có thể chuyển nhanh sang trạng thái truyền dữ liệu.

• Cho phép các switch trong mạng đã hội tụ tự gửi các gói BPDU của nó chứ không chỉ riêng gói BPDU của bridge gốc.

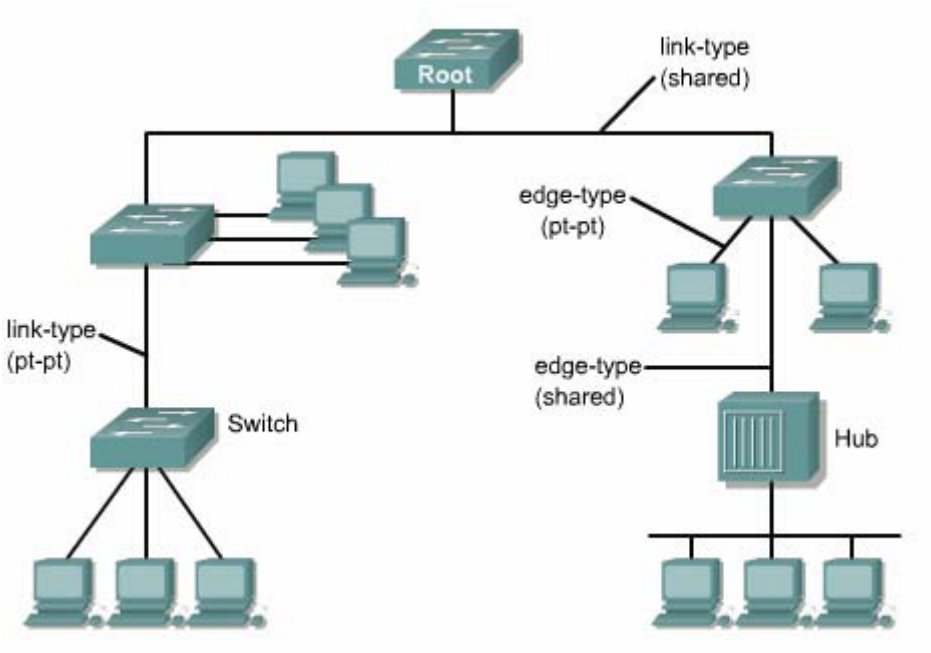
Trạng thái khoá (bloocking) được đổi tên thành trạng loại bỏ (discarding). Port loại bỏ đóng vai trò là một port dự phòng. Trong mỗi segment có một port được chỉ định (designated port) để kết nối vào segment đó. Nếu port chỉ định này bị sự cố thì port loại bỏ tương ứng sẽ được thay thế ngay cho port đó.



Hình 7.2.7.a. Port 1 trên Switch Y là port thay thế cho port 1 trên Switch X.

Các kết nối được phân thành các loại như kết nối điểm - đến - điểm, kết nối chia sẻ và kết nối biên cuối (edge - link). Kết nối điểm - đến - điểm là kết nối giữa hai switch. Kết nối chia sẻ là kết nối có nhiều switch cùng kết nối vào. Kết nối biên cuối là kết nối từ switch xuống host, không còn switch nào khác xen giữa. Phân biệt thành nhiều loại kết nối cụ thể như vậy, việc nhận biết sự thay đổi cấu trúc mạng sẽ nhanh hơn.

Kết nối điểm - đến - điểm và kết nối biên cuối sẽ được chuyển vào trạng thái truyền dữ liệu ngay lập tức vì không hề có vòng lặp trên những kết nối dạng này.



Hình 7.2.7.b. Các loại kết nối trong Rapid Spanning - Tree.

Thời gian hội tụ sẽ không lâu hơn 15 giây kể từ khi có sự thay đổi.

Giao thức Rapid Spanning - Tree, hay IEEE 802.1w sẽ thực sự thay thế cho giao thức Spanning - Tree, hay IEEE 802.1D.

TổNG kết

Sau khi hoàn tất chương này, bạn cần nắm được các ý quan trọng sau:

- Sự dự phòng và vai trò quan trọng của nó trong hệ thống mạng.
- Các thành phần chính trong cấu trúc mạng dự phòng.
- Trận bão quảng bá và tác hại của nó trong mạng chuyển mạch.
- Truyền nhiều lượt frame và tác hại của nó lên mạng chuyển mạch.
- Nguyên nhân và hậu quả của việc cơ sở dữ liệu địa chỉ MAC không ổn định.
- Lợi ích và nguy cơ của cấu trúc mạng dự phòng.

- Vai trò của Spanning - Tree trong cấu trúc mạng dự phòng.
- Các hoạt động cơ bản của Spanning - Tree.
- Quá trình bầu bridge gốc.
- Các trạng thái Spanning - Tree.
- So sánh giao thức Spanning - Tree và giao thức Rapid Spanning - Tree.

CHƯƠNG 8 : VLAN

GIỚI THIỆU

Một đặc tính quan trọng của mạng chuyển mạch Ethernet là mạng LAN ảo(VLAN).VLAN là một nhóm lôgic các thiết bị mạng hoặc các usur. Các thiết bị mạng hoặc user được nhóm lại theo chức năng, phòng ban hoặc theo ứng dụng chứ không theo vị trí vật lý nữa. Các thiết bị trong một VLAN được giới hạn chỉ thông tin liên lạc với các thiết bị trong cùng VLAN. Chỉ có router mới cung cấp kết nối giữa các VLAN khác nhau. Cisco đang cố gắng hướng tới sự tương thích với các nhà sản xuất khác nhau nhưng mỗi nhà sản xuất đã phát triển sản phẩm VLAN riêng độc quyền của họ cho nên chúng có thể không hoàn toàn tương thích với nhau.

VLAN với cách phân nguồn tài nguyên và user theo lôgic đã làm tăng hiệu quả hoạt động của toàn bộ hệ thống mạng. Các công ty, tổ chức thường sử dụng VLAN để phân nhóm user theo lôgic mà không cần quan tâm đến vị trí vật lý của họ. Nhờ đó, user trong phòng Maketing sẽ được nhóm vào Maketing VLAN, user trong phòng Kĩ thuật được đặt vào VLAN kĩ thuật.

Với VLAN,mạng có khả năng phát triển, bảo mật và quản lý tốt hơn vì router trong cấu trúc VLAN có thể ngăn gói quảng bá, bảo mật và quản lý dòng lưu lượng mạng.

VLAN là một công cụ mạnh trong thiết kế và cấu hình mạng. Với VLAN các công việc thêm bớt, chuyển đổi trong cấu trúc mạng khi cần thiết trở nên đơn giản hơn rất nhiều. VLAN còn giúp gia tăng bảo mật và kiểm soát quảng bá Lớp 3. Tuy nhiên nếuVLAN được cấu hình không đúng sẽ làm cho mạng hoạt động kém hoặc có khi không hoạt động được. Do đó, khi thiết kế mạng, việc nắm được cách triển khai VLAN trên nhiều switch khác nhau là rất quan trọng.

Sau khi hoàn tất chương trình này, các bạn có thể thực hiện được những việc sau:

+Định nghĩa VLAN

+Liệt kê các ích lợi của VLAN

+Giải thích VLAN được sử dụng để tạo miền quảng bá như thế nào.

+Giải thích router được sử dụng để thông tin liên lạc giữa các VLAN như thế nào.

+Liệt kê các loại VLAN

+Định nghĩa ISL và 802.1Q

+Giải thích các khái niệm VLAN theo địa lý.

+Cấu hình VLAN có cố định trên dòng Catalyst 29xx switch.

+Kiểm tra và lưu cấu hình VLAN

+Xoá VLAN khỏi cấu hình switch.

8.1 Khái niệm về VLAN

8.1.1 Giới thiệu về VLAN

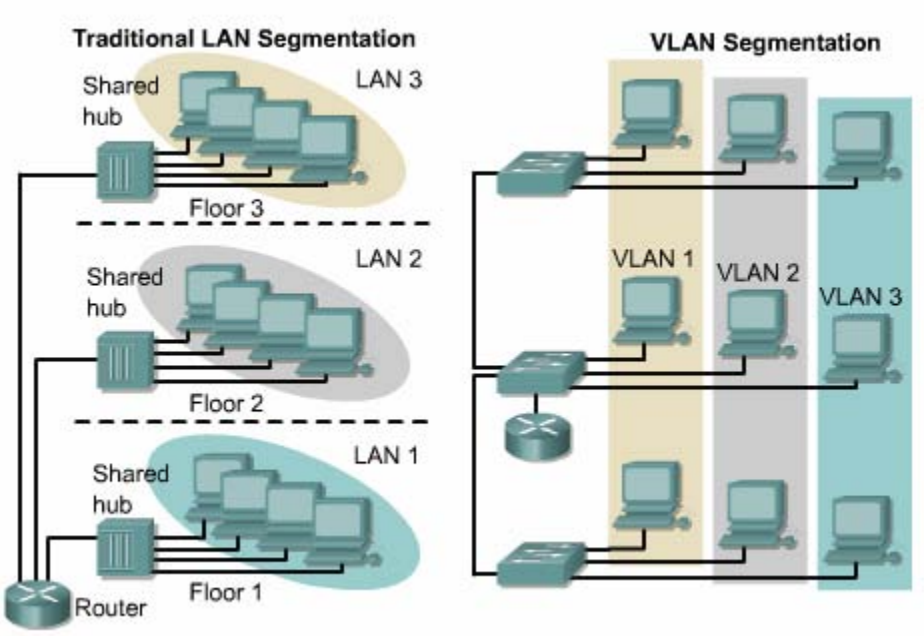
VLAN là một nhóm các thiết bị mạng không bị giới hạn theo vị trí vật lý hoặc theo LAN switch mà chúng kết nối vào.

VLAN là một segment mạng theo lôgic dựa trên chức năng, đội nhóm hoặc ứng dụng của một tổ chức chứ không phụ thuộc vị trí vật lý hay kết nối vật lý trong mạng. Tất cả các máy trạm và server được sử dụng bởi cùng một nhóm làm việc sẽ được đặt trong cùng VLAN bất kể vị trí hay kết nối vật lý của chúng.

Mọi công việc cấu hình VLAN hoặc thay đổi cấu hình VLAN đều được thực hiện trên phần mềm mà không cần thay đổi cáp và thiết bị vật lý.

Một máy trạm trong một VLAN chỉ được liên lạc với file server trong cùng VLAN với nó. VLAN được nhóm theo chức năng lôgic và mỗi VLAN là một miền quảng bá, do đó gói dữ liệu chỉ được chuyển mạch trong cùng một VLAN.

VLAN có khả năng mở rộng, bảo mật và quản lý mạng tốt hơn. Router trong cấu trúc VLAN thực hiện ngăn chặn quảng bá, bảo mật và quản lý nguồn giao thông mạng. Switch không thể chuyển mạch giao thông giữa các VLAN khác nhau. Giao thông giữa các VLAN phải được định tuyến qua router.

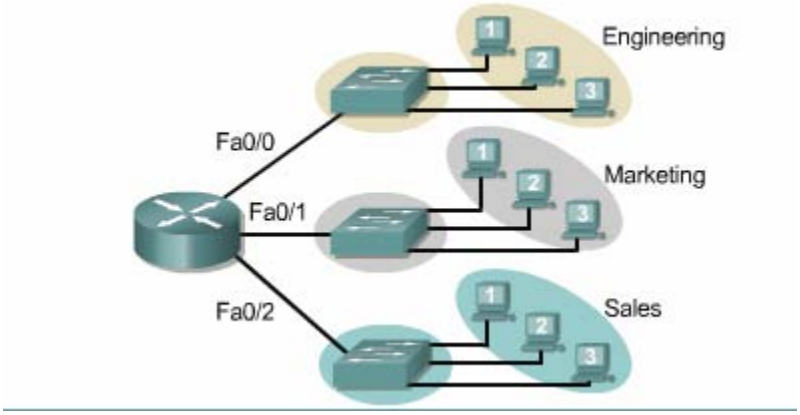


Hình 8.1.1 Phân đoạn mạng LAN theo kiểu truyền thống và theo VLAN.

8.2.1 Miền quảng bá với VLAN và router

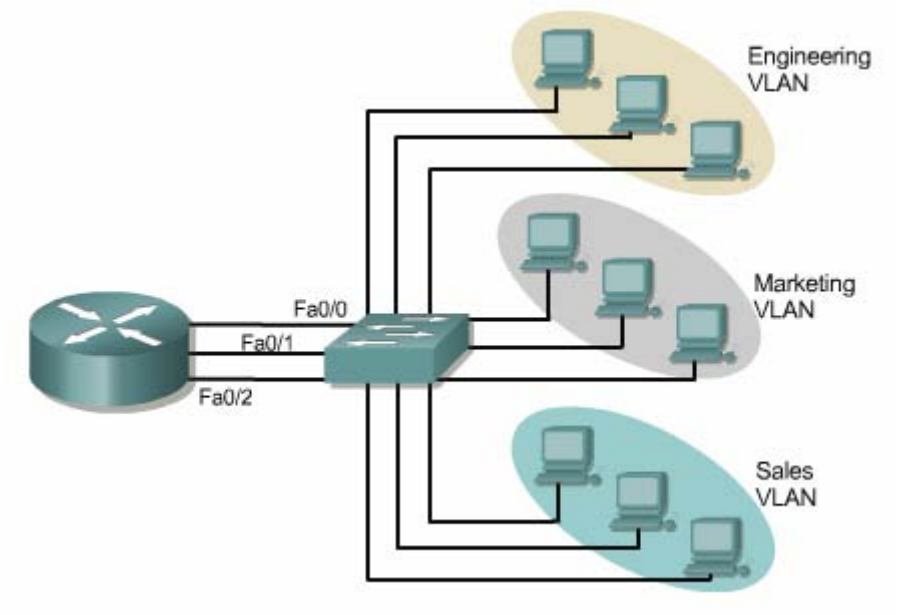
Một VLAN là một miền quảng bá được tạo nên bởi một hay nhiều switch.

Hình 8.1.2.a cho thấy tạo 3 miền quảng bá riêng biệt trên ba switch như thế nào. Định tuyến Lớp 3 cho phép router chuyển gói giữa các miền quảng bá với nhau.



Hình 8.1.2.a.3 miền quảng bá trên 3 switch khác nhau.

Trong hình 8.1.2.b chúng ta thấy 3 VLAN tức là 3 miền quảng bá khác nhau được tạo ra trên một switch và một router. Router sẽ sử dụng định tuyến Lớp 3 để chuyển giao thông giữa 3 VLAN.



Hình 8.1.2.b. 3 VLAN □ 3 miền quảng bá trên một switch.

Switch trong hình 8.1.2.b sẽ truyền frame lên cổng giao tiếp của router khi:

+Gói dữ liệu là gói quảng bá.

+Gói dữ liệu có địa chỉ MAC đích là một trong các địa chỉ MAC của router.

Nếu máy trạm 1 trong VLAN kĩ thuật muốn gửi dữ liệu cho máy trạm 2 trong VLAN Bán hàng, hai máy này nằm trong hai miền quảng bá khác nhau, thuộc hai mạng khác nhau, do đó địa chỉ MAC đích trong gói dữ liệu sẽ là địa chỉ MAC của default gateway của máy trạm 1. Vì vậy địa chỉ MAC đích của gói dữ liệu này sẽ là địa chỉ MAC của tổng Fa0/0 trên router. Gói dữ liệu được chuyển đến router, bằng định tuyến IP, router sẽ chuyển gói đến đúng VLAN Bán hàng.

Nếu máy trạm 1 trong VLAN kĩ thuật muốn gửi gói dữ liệu cho máy trạm 2 trong cùng VLAN thì địa chỉ MAC đích của gói dữ liệu sẽ chính là địa chỉ MAC của máy trạm 2.

Tóm lại, switch sẽ xử lý chuyển mạch gói dữ liệu khi có chia VLAN như sau:

+Đối với mỗi VLAN switch có một bảng chuyển mạch riêng tương ứng

+Nếu switch nhận được gói dữ liệu từ một port nằm trong VLAN 1 chẳng hạn, thì switch sẽ chỉ tìm địa chỉ MAC đích trong bảng chuyển mạch của VLAN 1 mà thôi.

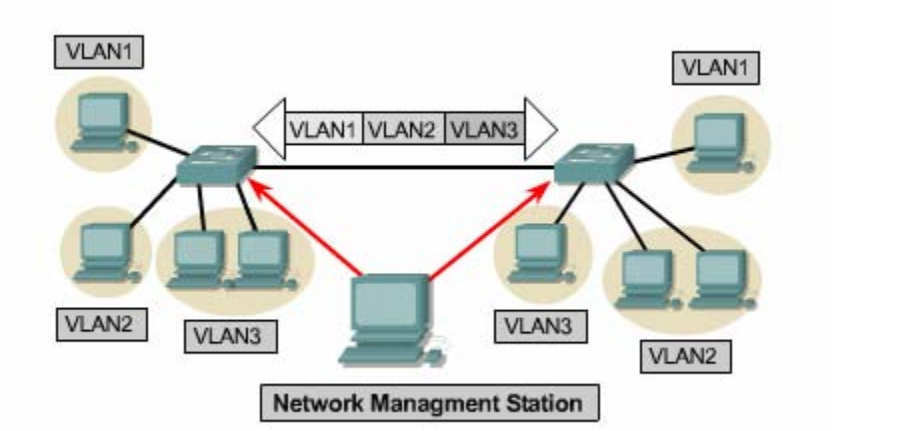
+Đồng thới switch sẽ học địa chỉ MAC nguồn trong gói dữ liệu và ghi vào bảng chuyển mạch của VLAN 1 nếu địa chỉ MAC này chưa được biết.

+Sau đó switch quyết định chuyển gói dữ liệu.

+Switch nhận frame vào từ VLAN nào thì switch chỉ học địa chỉ nguồn của frame và tìm địa chỉ đích cho frame trong một bảng chuyển mạch tương ứng với VLAN đó.

8.1.3 Hoạt động của VLAN

Mỗi port trên switch có thể gán cho một VLAN khác nhau. Các port nằm trong cùng một VLAN sẽ chia sẻ gói quảng bá với nhau. Các port không nằm trong cùng VLAN sẽ không chia sẻ gói quảng bá với nhau. Nhờ đó mạng LAN hoạt động hiệu quả hơn.



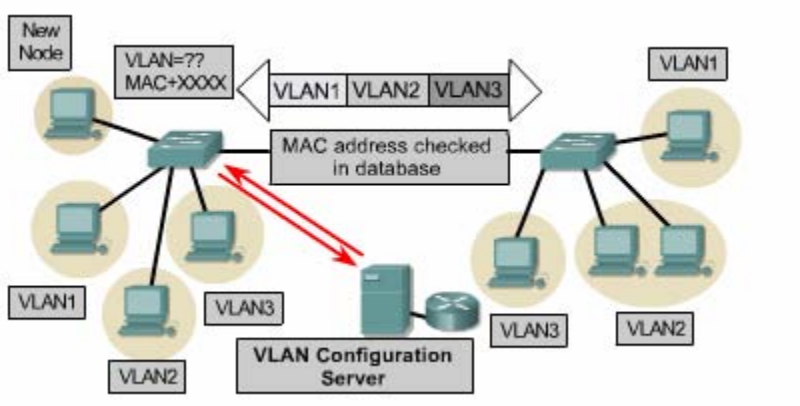
Hình 8.1.3.a VLAN cố định.

Thành viên cố định của VLAN được xác định theo port. Khi thiết bị kết nối vào một port của switch, tuỳ theo port thuộc loại VLAN nào thì thiết bị sẽ nằm trong VLAN đó.

Mặc định, tất cả các port trên một switch đều nằm trong VLAN quản lý. VLAN quản lý luôn luôn là VLAN 1 và chúng ta không thể xoá VLAN này được.

Sau đó chúng ta có thể cấu hình gán port vào các VLAN khác. VLAN cung cấp băng thông tin nhiều hơn cho user so với mạng chia sẻ. Trong mạng chia sẻ, các user cùng chia sẻ một băng thông trong mạng đó, càng nhiều user trong một mạng chia sẻ thì lượng băng thông càng thấp hơn và hiệu suất hoạt động càng giảm đi.

Thành viên động của VLAN được cấu hình bằng phần mềm quản lý mạng. Bạn có thể sử dụng CiscoWorks 2000 hoặc CiscoWorks for Switch Internetworks để tạo VLAN động. VLAN động cho phép các định thành viên dựa theo địa chỉ MAC của thiết bị kết nối vào switch chứ không còn xác định theo port nữa. Khi thiết bị kết nối vào switch, switch sẽ tìm trong cơ sở dữ liệu của nó để xác định thiết bị này thuộc loại VLAN nào.



Hình 8.1.3.b VLAN động

**Cấu hình VLAN bằng các phần mềm VLAN quản lý tập trung.*

**Có thể chia VLAN theo địa chỉ MAC, địa chỉ lôgic hoặc theo loại giao thức.*

**Không cần quản lý nhiều ở các tủ nối dây nữa vì thiết bị kết nối vào mạng thuộc VLAN nào là tuỳ theo địa chỉ của thiết bị đó đã được gán vào VLAN.*

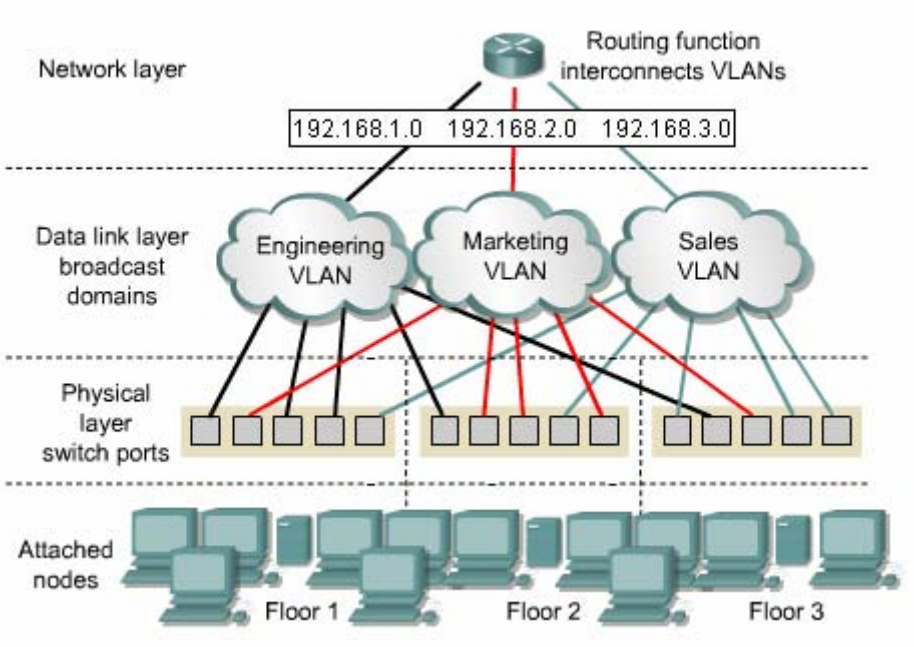
**Có khả năng thông báo cho quản trị mạng khi có một user lạ, không có trong cơ sở dữ liệu kết nối vào mạng.*

Xác định thành viên VLAN theo port tức là port đã được gán vào VLAN nào thì thiết bị kết nối vào port đó thuộc VLAN đó, không phụ thuộc vào thiết bị kết nối là thiết bị gì, địa chỉ bao nhiêu. Với cách chia VLAN theo port như vậy, tất cả các user kết nối vào cùng một port sẽ nằm trong cùng một VLAN. Một user hay nhiều user có thể kết nối vào một port và sẽ không nhận thấy là có sự tồn tại của

VLAN. Cách chia VLAN này giúp việc quản lý đơn giản hơn vì không cần tìm trong cơ sở dữ liệu phức tạp để xác định thành viên của mỗi VLAN.

Người quản trị mạng có trách nhiệm cấu hình VLAN bằng tay và cố định.

Mỗi một port trên switch cũng hoạt động giống như một port trên bridge. Bridge sẽ chặn luồng lưu lượng nếu nó không cần thiết phải đi ra ngoài segment. Nếu gói dữ liệu cần phải chuyển qua bridge và switch không biết địa chỉ đích hoặc gói nhận được là gói quảng bá thì mới chuyển ra tất cả các port nằm trong cùng miền quảng bá với port nhận gói dữ liệu vào.



Hình 8.1.3.c. Chia VLAN theo port.

8.1.4 ích lợi của VLAN

Lợi ích của VLAN là cho phép người quản trị mạng tổ chức mạng theo lôgíc chứ không theo vật lý nữa. Nhờ đó những công việc sau có thể thực hiện dễ dàng hơn:

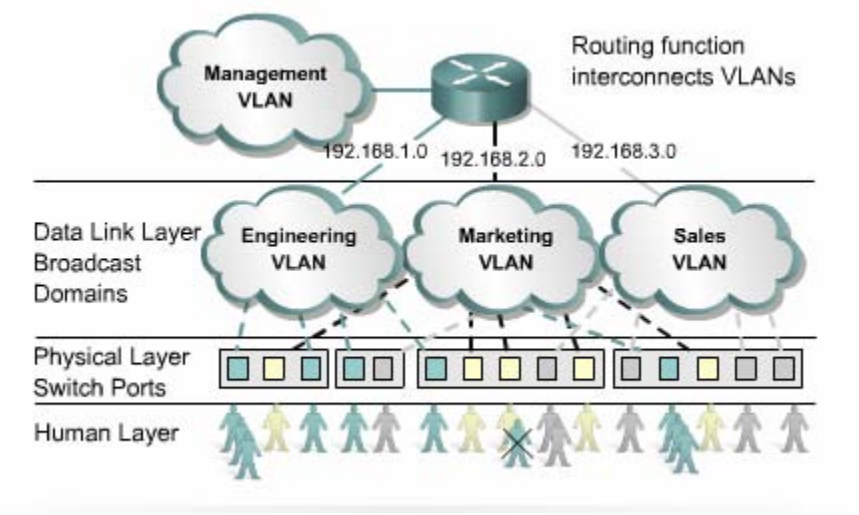
*Di chuyển máy trạm trong LAN dễ dàng.

* 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.



Tất cả các user được gắn vào cùng port là cùng một VLAN.

Hình 8.1.4

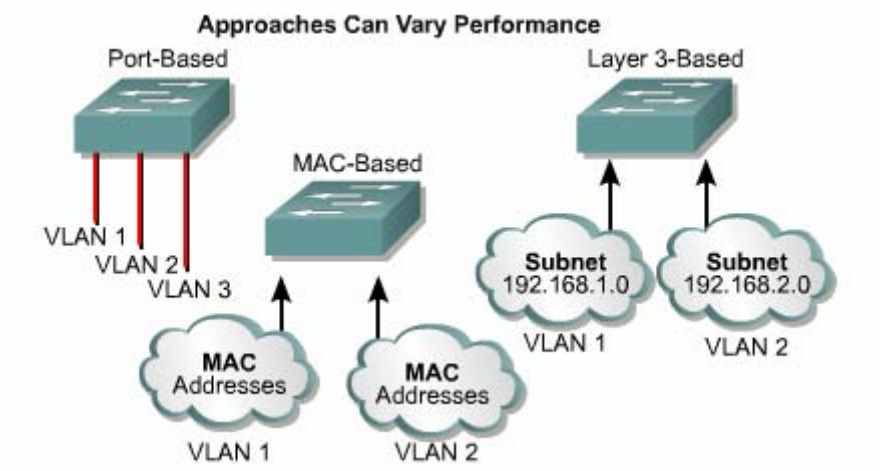
8.1.5 Các loại VLAN

Có 3 loại thành viên VLAN để xác định và kiểm soát việc sử lý các gói dữ liệu:

*VLAN theo port

*VLAN theo địa chỉ MAC

*VLAN theo giao thức



Hình 8.1.5.1. 3 loại thành viên VLAN

*User thuộc loại VLAN nào là tuỳ thuộc vào port kết nối của user đó.

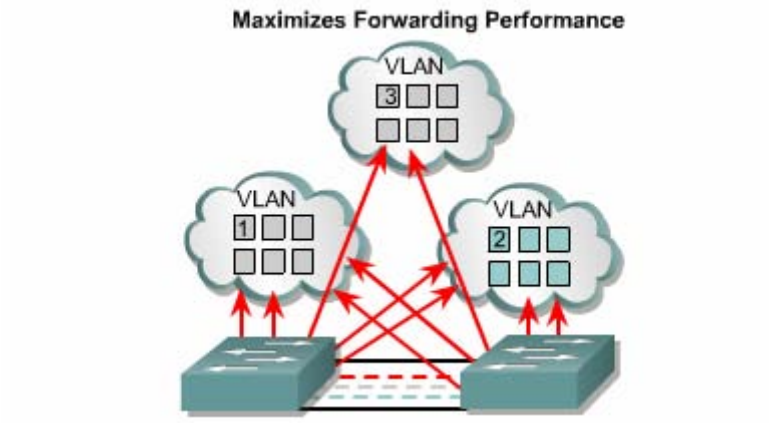
*Không cần tìm trong cơ sở dữ liệu khi xác định thành viên VLAN

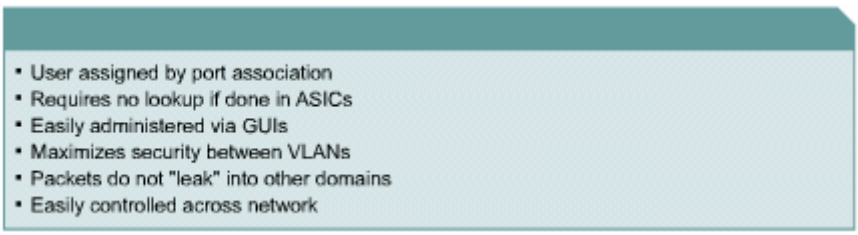
*Dễ dàng quản lý bằng giao diện đồ hoạ(GUIs). Quản lý thành viên của VLAN theo port cũng dễ dàng và đơn giản.

*Bảo mật tối đa giữa các VLAN

*Gói dữ liệu không bị "rò rỉ" sang các miền khác.

*Dễ dàng kiểm soát qua mạng





Hình 8.1.5.b.Xác định thành viên VLAN theo port.

*User thuộc loại VLAN nào là tuỳ thuộc vào địa chỉ MAC của user đó

*Linh hoạt hơn nhưng tăng độ tải lên giao thông mạng và công việc quản trị mạng.

*ảnh hưởng đến hiệu suất hoạt động, khả năng mở rộng và khả năng quản trị vì quản lý thành viên của VLAN theo địa chỉ MAC là một việc phức tạp.

*Tiến trình xử lý gần giống như các lớp trên.

Hình 8.1.5.c Xác định thành viên VLAN theo địa chỉ MAC.

Số lượng VLAN trên một switch phụ thuộc vào các yếu tố sau:

+Dòng giao thông

+Loại ứng dụng

+Sự quản lý mạng

+Sự phân nhóm

Ngoài ra một yếu tố quan trọng mà chúng ta cần quan tâm là kích thước của switch và sơ đồ chia địa chỉ IP

Ví dụ: Một mạng sử dụng địa chỉ mạng có 24 bít subnet mask, như vậy mỗi subnet có tổng cộng 254 địa chỉ host. Chúng ta nên sử dụng mối tương quan một- một giữa VLAN và IP subnet. Do đó, mỗi VLAN tương ứng với một IP subnet, có tối đa 254 thiết bị.

Thieu hinh ve ko co hinh

Phần header của frame sẽ được đóng gói lại và điều chỉnh để có thêm thông tin về VLAN ID trước khi frame được truyền lên đường truyền kết nối giữa các switch. Công việc này gọi là dán nhãn cho frame. Sau đó, phần header của frame được trả lại như cũ trước khi truyền xuống cho thiết bị đích.

Có hai phương pháp chủ yếu để dán nhãn frame là Intr — Switch Link(ISL) và 802.1Q.ISL từng được sử dụng phổ biến nhưng bây giờ đang thay thế bởi 802.1Q.

Xét ví dụ trên hình 8.1.5.d: Switch lưu riêng từng bảng chuyển mạch tương ứng với mỗi VLAN. Switch nhận frame vào từ VLAN nào thì chỉ học địa chỉ nguồn và tìm địa chỉ đích trong bảng chuyển mạch của VLAN đó. Nhờ đó switch bảo đảm chỉ thực hiện chuyển mạch trong cùng một VLAN. Bây giờ giả sử máy trạm trong VLAN1 của switch A gửi gói dữ liệu cho máy trạm trong VLAN 1 của switch B. Switch A nhận được gói dữ liệu này vào từ port nằm trong VLAN1, do đó nó tìm địa chỉ đích trong bảng chuyển mạch của VLAN1. Sau đó switch xác định là phải chuyển frame này lên đường backbone. Trước khi chuyển frame lên đường

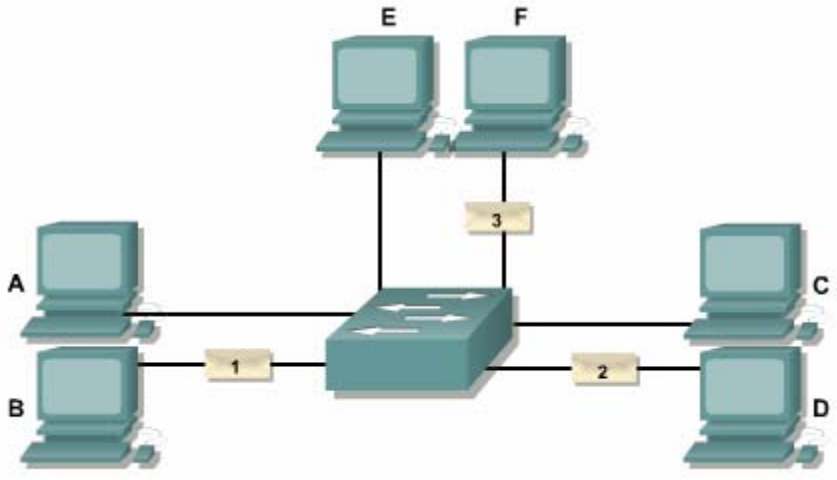
backbone thì Switch A sẽ đóng gói lại cho frame, trong đó phần header của frame có thêm thông tin về VLAN ID cho biết gói dữ liệu này thuộc VLAN1. Công việc này gọi là dán nhãn frame. Sau đó Switch B nhận được gói dữ liệu từ đường backbone xuống, dựa vào VLAN ID trong gói, Switch xác định gói dữ liệu này từ VLAN1 nên nó tìm địa chỉ đích trong bảng chuyển mạch của VLAN1. Switch B tìm được port đích của gói dữ liệu. Trước khi chuyển gói xuống máy đích, Switch tìm được port đích của gói dữ liệu. Trước khi chuyển gói xuống máy đích, Switch B trả lại định dạng ban đầu của phần header trong gói dữ liệu, hay còn gọi là gỡ nhãn frame.

Mô phỏng LAN (LANE — LAN Emulation) làm cho mạng ATM(Asynchronous Transfer Mode) bắt chước giống mạng Ethernet. Trong LANE, không có dán nhãn frame mà sử dụng kết nối ảo để biểu thị choVLAN ID.

8.2 Cấu hình VLAN

8.2.1. Cấu hình VLAN cơ bản

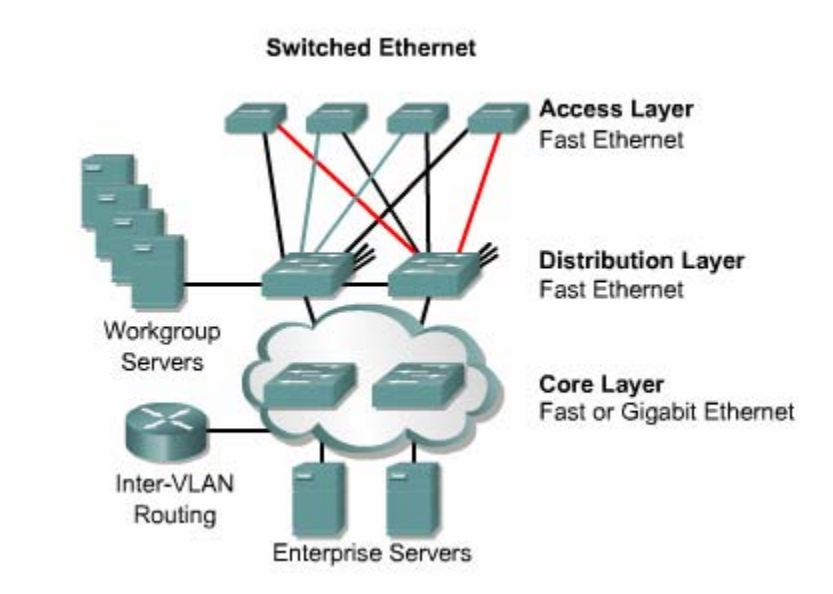
Trong môi trường chuyển mạch, một máy trạm chỉ nhận được giao thông nào gửi đến nó. Nhờ đó, mỗi máy trạm được dành riêng và trọn vẹn băng thông cho đường truyền và nhận. Không giống như hệ thống hus chia sẻ chỉ có một máy trạm được phép truyền tại một thời điểm, mạng chuyển mạch có thể cho phép nhiều phiên giao dịch cùng một lúc trong một miền quảng bá mà không làm ảnh hưởng đến các máy trạm khác bên trong cũng như bên ngoài miền quảng bá. Ví dụ như trên hình 8.2.1.a, cặp A/B, C/D, E/F có thể đồng thời liên lạc với nhau mà không ảnh hưởng đến các cặp máy khác.



Hình 8.2.1.a

Mỗi VLAN có một địa chỉ mạng Lớp 3 riêng: Nhờ đó router có thể chuyển gói giữa các VLAN với nhau.

Chúng ta có thể xây dựng VLAN cho mạng từ đầu cuối - đến - đầu cuối hoặc theo giới hạn địa lý.



Hình 8.2.1.b VLAN từ đầu cuối- đến - đầu cuối.

Một mạng VLAN từ đầu cuối - đến - đầu cuối có các đặc điểm như sau:

*User được phân nhóm vào VLAN hoàn toàn không phụ thuộc vào vị trí vật lý, chỉ phụ thuộc vào chức năng công việc của nhóm.

*Mọi user trong cùng một VLAN đều có chung tỉ lệ giao thông 80/20(80% giao thông trong VLAN, 20% giao thông ra ngoài VLAN)

*Khi user di chuyển trong hệ thống mạng vẫn không thay đổi VLAN của user đó.

*Mỗi VLAN có những yêu cầu bảo mật riêng cho mọi thành viên của VLAN đó.

Bắt đầu từ tầng truy cập, port trên switch được cấp xuống cho mỗi user. Người sử dụng di chuyển trong toàn bộ hệ thống mạng ở mọi thời điểm nên mỗi switch đều

là thành viên của mọi VLAN. Switch phải dán nhãn frame khi chuyển frame giữa các switch tầng truy cập với switch phân phối.

ISL là giao thức độc quyền của Cisco để dán nhãn cho frame khi truyền frame giữa các switch với nhau và với router. CònIEEE802.1Q là một chuẩn để dán nhãn frame. Catalyst 2950 không hỗ trợ ISL trunking.

Các server hoạt động theo chế độ client/server. Do đó các server theo nhóm nên đặt trong cùng VLAN với nhóm user mà server đó phục vụ, như vậy sẽ giữ cho dòng lưu lượng tập trung trong VLAN, giúp tối ưu hoá hoạt động chuyển mạch lớp 2.

Router ở tầng trục chính được sử dụng để định tuyến giữa các subnet. Toàn bộ hệ thống này có tỉ lệ lưu lượng là 80% lưu lượng trong nội bộ mỗi VLAN, 20% giao thông đi qua router đến các server toàn bộ hệ thống và đi ra internet, WAN.

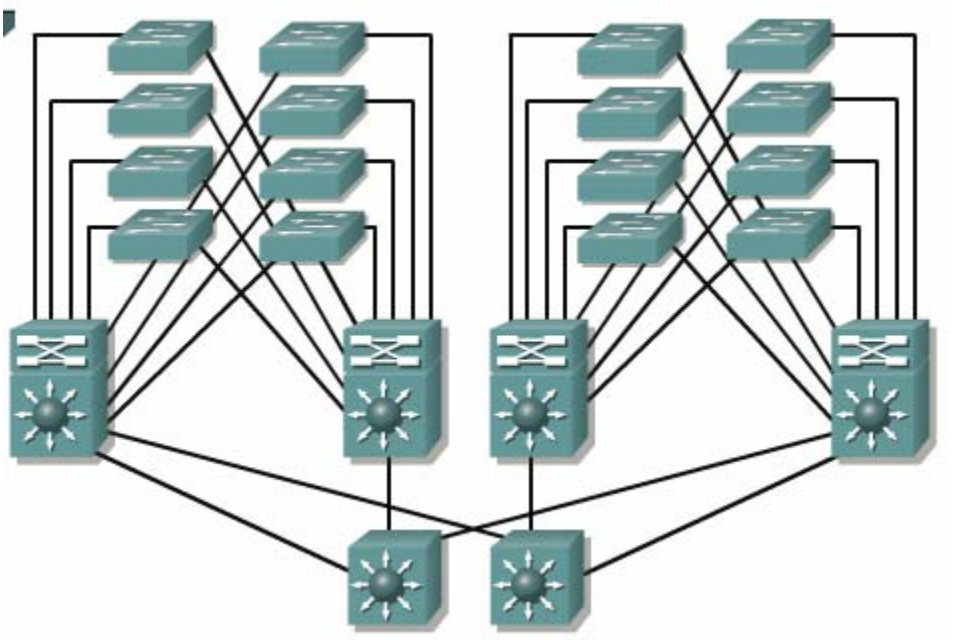
8.2.2. Vlan theo địa lý.

VLAN từ đầu cuối - đến - đầu cuối cho phép phân nhóm nguồn tài nguyên sử dụng, ví dụ như phân nhóm user theo server sử dụng, nhóm dự án và theo phòng ban... Mục tiêu của VLAN từ đầu đến cuối - đến - đầu cuối là giữ 80% giao thông trong nội bộ của VLAN.

Khi các hệ thống mạng tập đoàn thực hiện tập trung tài nguyên mạng thì VLAN từ đầu cuối - đến - đầu cuối rất khó thực hiện mục tiêu của mình. Khi đó user cần phải sử dụng nhiều nguồn tài nguyên khác nhau không nằm trong cùng VLAN với user. Chính vì xu hướng sử dụng và phân bố tài nguyên mạng khác đi nên hiện nay VLAN thường được tạo ra theo giới hạn của địa lý.

Phạm vi địa lý có thể lớn bằng cả một toà nhà hoặc cũng có thể chỉ nhỏ với một switch. Trong cấu trúc VLAN này. Tỷ lệ lưu lượng sẽ là 20/80, 20% giao thông trong nội bộ VLAN và 80% giao thông đi ra ngoài VLAN.

Điểm này có nghĩa là lưu lượng phải đi qua thiết bị lớp 3 mới đến được 80% nguồn tài nguyên. Kiểu thiết kế này cho phép việc truy cập nguồn tài nguyên được thống nhất.



Hình 8.2.2

8.2.3 Cấu hinh VLAN cố định.

VLAN cố định là VLAN được cấu hình theo port trên switch bằng các phần mềm quản lý hoặc cấu hình trực tiếp trên switch. Các port đã được gán vào VLAN nào thì nó sẽ giữ nguyên cấu hình VLAN đó cho đến khi được thay đổi bằng lệnh. Đây là cấu trúc VLAN theo địa lý, các user phải đi qua thiết bị lớp 3 mới truy cập 80% tài nguyên mạng. Loại VLAN cố định hoạt động tốt trong những mạng có đặc điểm như sau:

- Sự di chuyển trong mạng được quản lý và kiểm soát.
- Có phần mềm quản lý VLAN mạnh để cấu hình port trên switch.
- Không dành nhiều tải cho hoạt động duy tri địa chỉ MAC của thiết bị đầu cuối và điều chỉnh bảng địa chỉ.

VLAN động thì không phụ thuộc vào port trên switch.

Sau đây là các hướng dẫn khi bạn cấu hình VLAN trên Cisco 29xx switch:

- Số lượng VLAN tối đa phụ thuộc vào switch.
- VLAN 1 là VLAN mặc định của nhà sản xuất.

• VLAN 1 là VLAN Ethernet mặc định.

• Giao thức phát hiện thiết bị Cisco (Cisco Discovery Protocol — CDP) và giao thức VLAN Trunking (VTP) đều giử gói quảng bá của mình trong VLAN 1.

• Địa chỉ IP của Catalyst 29xx mặc định nằm trong miền quảng bá VLAN 1.

• Switch phải ở chế độ VTP server để tạo, thêm hoặc xoá VLAN.

Việc tạo VLAN trên switch rất đơn giản và rõ ràng. Nếu bạn sử dụng switch với cisco IOS, bạn vào chế độ cấu hình VLAN bằng lệnh vlan database ở chế độ EXEC đặc quyền, sau đó bạn tạo VLAN:

Switch # vlan database.

Switch (vlan) # vlan vlan_number.

Switch (vlan) # exit.

Sau khi đã có VLAN trên switch, bước tiếp theo là các bạn gán port vào VLAN:

Switch (config) # interfase fastethernet 0/9.

Switch (config-if)#switchport access vlan vlan_number.

8.2.4. Kiểm tra cấu hình VLAN.

Bạn dùng các lệnh sau để kiểm tra cấu hình VLAN: show vlan, show vlan brief, show vlan id id_number.

Bạn nên nhớ 2 điều kiện sau:

• Tất cả các VLAN được tạo ra chỉ bắt đầu được sử dụng khi đã có port được phân cho nó.

• Mặc định, tất cả các port ethernet đều nằm trong VLAN 1.

```
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
3    enet 100003 1500  -      -      -        -    -     0      0
1002 fddi 101002 1500  -      -      -        -    -     1      1003
1003 tr   101003 1500  1005   0      -        -    srb   1      1002
1004 fdnet 101004 1500  -      -      1        ibm  -     0      0
1005 trnet 101005 1500  -      -      1        bm   -     0      0
```

Hình 8.2.4.a

Cisco

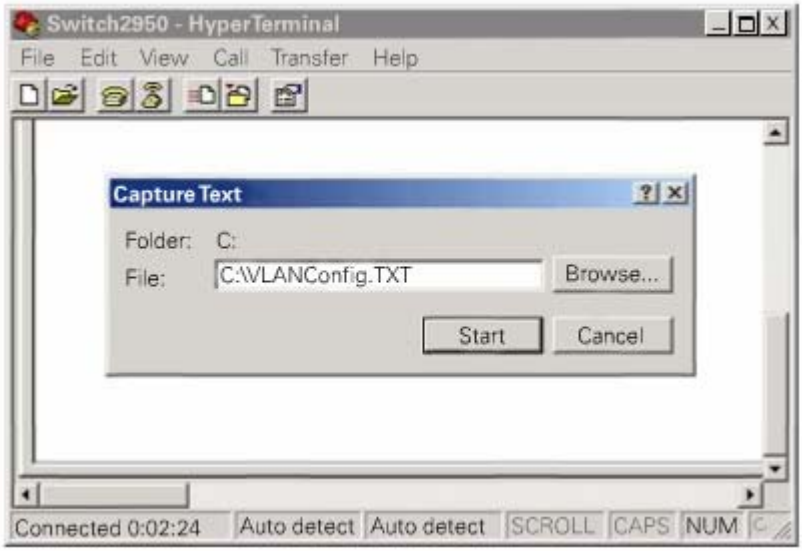
```
---- ------------------- ------- -------------------------------
1    default             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
2    VLAN2               active    Fa0/5, Fa0/6, Fa0/7
3    VLAN3               active    Fa0/8, Fa0/9, Fa0/10, Fa0/11,
                                   Fa0/12
1002 fddi-default        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
3    enet 100003 1500  -      -      -        -    -     0      0
1002 fddi 101002 1500  -      -      -        -    -     1      1003
1003 tr   101003 1500  1005   0      -        -    srb   1      1002
1004 fdnet 101004 1500  -      -      1        ibm  -     0      0
1005 trnet 101005 1500  -      -      1        bm   -     0      0
```

Hình 8.2.4.b

8.2.5. Lưu cấu hình VLAN.

Bạn nên lưu cấu hình VLAN thành một tập tin văn bản để có thể biên tập lại hoặc để dự phòng.

Bạn có thể lưu cấu hình switch bằng lệnh copy running-config tftp hoặc bằng chức năng ghi lại văn bản (capture text) của HyperTerminal.



Hình 8.2.5

8.2.6. Xoá VLAN.

Xoá một VLAN trên switch cũng giống như một dòng lệnh xoá trong cấu hình router vậy. Đơn giản là bạn tạo VLAN bằng lệnh nào thì bạn dùng dạng đó của câu lệnh đó để xoá VLAN.

Khi một VLAN đã bị xoá đi thì tất cả các port của VLAN đó sẽ ở trạng thái không hoạt động nhưng vẫn thuộc về VLAN đã bị xoá cho đến khi nào các port này được cấu hình sang VLAN khác.

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

Hình 8.2.6. Xoá port 0/9 khỏi VLAN 300.

8.3. Xử lý sự cố VLAN.

8.3.1. Giới thiệu chung.

Hiện nay VLAN được sử dụng phổ biến. Với VLAN, người kỹ sư mạng có thể linh hoạt hơn trong thiết kế và triển khai hệ thống mạng. VLAN giúp giới hạn miền quảng bá, gia tăng khả năng bảo mật và phân nhóm theo logic. Tuy nhiên, với cơ bản chuyển mạch LAN, sự cố có thể xay ra khi chúng ta triển khai VLAN. Trong bài này sẽ cho thấy một vài sự cố có thể xảy ra với VLAN và cung cấp cho các bạn một số công cụ và kỹ thuật sử lý sự cố.

Sau khi hoàn tất bài này các bạn có thể thực hiện các việc sau:

- Phân tích hệ thống để tiếp xúc với sự cố của VLAN.
- Giải thích các bước xử lý sự cố nói chung trong mạng chuyển mạch.
- Mô tả sự cố Spanning — Tree dẫn đến trận bão quảng bá như thế nào.
- Sử dụng lệnh show và debug để xử lý sự cố VLAN.

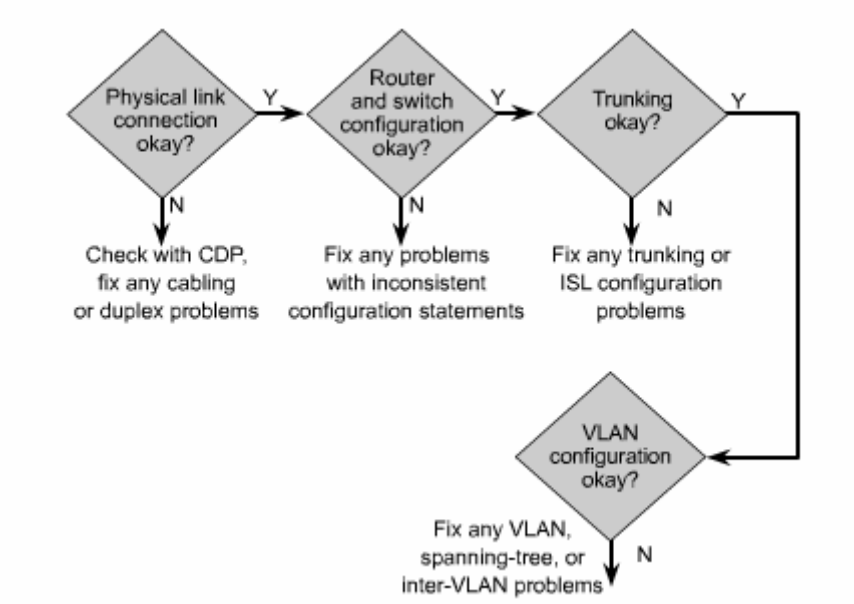
8.3.2. Tiến trình xử lý sự cố VLAN.

Điều quan trọng là bạn phải phát triển các bước xử lý sự cố trên switch một cách có hệ thống. Sau đây là các bước có thể giúp cho bạn xác định sự cố trong mạng chuyển mạch:

1. Kiểm tra các biểu hiện vật lý, như trạng thái LED.
2. Bắt đầu từ một cấu hình trên một switch và kiêm tra dần ra.
3. Kiểm tra kết nối lớp 1.
4. Kiểm tra kết nối lớp 2.
5. Xử lý sự cố VLAN xảy ra trên nhiều switch.

Khi xay ra sự cố, bạn nên kiểm tra xem đây là một sự cố lặp đi lặp lại hay là sự cố biệt lập. Một số sự cố lặp đi lặp lại có thể là do sự gia tăng của các dịch vụ phục vụ cho máy trạm, làm vượt qua khả năng cấu hình, khả năng đường trunking và khả năng truy cập tài nguyên trên server.

Ví dụ: Việc sử dụng các công nghệ web và các ứng dụng truyền thống như truyền tải file, email...sẽ làm gia tăng mật độ giao thông làm cho toàn bộ hệ thống bị trì trệ.



Hình 8.3.1

Hiện nay rất nhiều mạng LAN phải đối mặt với mô hình giao thông chưa được tính trước, là kết quả của sự gia tăng giao thông trong intranet, ít phân nhóm server hơn và tăng sử dụng multicast. Nguyên tắc 80/20 với chỉ có 20% giao thông đi lên các đường trục chính đã trở lên lạc hậu. Ngày nay, các trình duyệt web nội bộ có thể cho phép user xác định và truy cập thông tin ở bất kỳ đâu trong mạng nội bộ của tập đoàn.

Nếu mạng thường xuyên bị nghẽn mạch, quá tải, rớt gói và truyền lại nhiều lần thì nghĩa là có quá nhiều port cho một đương trunk hoặc có quá nhiều yêu cầu truy suất vào các nguồn tài nguyên của toàn hệ thông và các server intranet.

Nghẽn mạch cũng có thể do phần lớn giao thông đều được truyền lên đường trục chính, hoặc là do user mở ra nhiều tài nguyên và nhiêu ứng dụng đa phương tiện. Trong trường hợp này thị hệ thống mạng nên nâng cấp để đáp ứng nhu cầu phát triển.

8.3.3. Ngăn trặn cơn bão quảng bá.

Trận bão quảng bá xảy ra khi có quá nhiều gói quảng bá được nhận vào trên một port. Việc sử lý chuyển mạch các gói này cho hệ thống mạng châm đi. Chúng ta có thể cấu hình cho switch kiểm soát bão trên từng port. Mặc định, chế độ kiểm soát bão trên switch bị tắt đi.

Để ngăn chặn bão quảng bá, chúng ta đặt một giá trị ngưỡng cho port để huỷ gói dữ liệu và đóng port khi giá trị ngưỡng này bị vướt qua.

STP (Spanning - Tree Protocol) có một số sự cố bao gồm trận bão quảng bá, lặp vòng, rớt gói BPDU va gói dữ liệu. Chức năng của STP là bảo đảm không có vòng lặp tồn tại trong mạng bằng cách chọn ra một bridge gốc. Bridge gốc này là điểm gốc của cấu trúc hình cây và nơi kiểm soát hoạt động của giao thức STP.

Nếu cần phải giảm lượng giao thông BPDU thì bạn sẽ cài đặt giá trị tối đa cho các khoảng thời gian hoạt động của bridge gốc. Đặc biệt là bạn nên đặt giá trị tối đa 30 giây cho khoảng thời gian chuyển trạng thái (Forward delay) và thời gian chờ tối đa (max - age) là 40 giây.

Một port vật lý trên router hoặc switch có thể là thành viên của một hoặc nhiều cấu trúc hình cây nếu port này kết nối vào đường trunk.

Lưu ý: VTP chỉ chạy trên Catalyst switch chứ không chạy trên router.

Trên switch kết nối vào router, bạn nên cấu hình cho switch đó chạy ở chế độ VTP transparent cho đến khi nào Cisco hỗ trợ VTP trên router của họ.

Giao thức Spanning - Tree được xem là một trong những giao thức lớp 2 quan trọng nhất trên Catalyst switch. bằng cách ngăn chặn các vòng luận lý trong mạng chuyển mạch, STP cho phép cấu trúc lớp 2 vẫn có các đường dư để dự phòng mà không gây ra trân bão quảng bá.

TẬP 4

CHƯƠNG I:PHÂN CHIA ĐỊA CHỈ IP

GIỚI THIỆU

Sự phát triển không ngừng của Internet đã làm cho những nhà nghiên cứu bất ngờ. Một trong những nguyên nhân làm cho Internet phát triển nhanh chóng như vậy là do sự linh hoạt, uyển chuyển của thiết kế ban đầu. Nếu chúng ta không có các biện pháp phân phối địa chỉ IP thì sự phát triển của Internet sẽ làm cạn kiệt nguồn địa chỉ IP. Để giải quyết vấn đề thiếu hụt địa chỉ IP, nhiều biện pháp đã được triển khai. Trong đó, một biện pháp đã được triển khai rộng rãi là chuyển đổi địa chỉ mạng (Network Address Translation – NAT).

NAT là một cơ chế để tiết kiệm địa chỉ IP đăng kí trong một mạng lớn và giúp đơn giản hóa việc quản lý địa chỉ IP. Khi một gói dữ liệu được định tuyến trong một thiết bị mạng, thường là firewall hoặc các router biên, địa chỉ IP nguồn sẽ được chuyển đổi từ địa chỉ mạng riêng thành địa chỉ IP công cộng định tuyến được. Điều này cho phép gói dữ liệu được truyền đi trong trong mạng công cộng, ví dụ như Internet. Sau đó, địa chỉ công cộng trong gói trả lời lại được chuyển đổi thành địa chỉ riêng để phát vào trong mạng nội bộ. Một dạng của NAT, được gọi là PAT (Port Address Translation), cho phép nhiều địa chỉ riêng được dịch sang một địa chỉ công cộng duy nhất.

Router, server và các thiết bị quan trọng khác trong mạng thường đòi hỏi phải được cấu hình bằng tay địa chỉ IP cố định. Trong khi đó, các máy tính client không cần thiết phải đặt cố định một địa chỉ mà chỉ cần xác định một dải địa chỉ cho nó. Dải địa chỉ này thường là một subnet IP. Một máy tính nằm trong subnet có thể được phân phối bất kì địa chỉ nào nằm trong subnet đó.

Giao thức DHCP (Dynamic Host Configuration Protocol) được thiết kế để phân phối địa chỉ IP và đồng thời cung cấp các thông tin cấu hình mạng quan trọng một cách tự động cho máy tính. Số lượng máy client chiếm phần lớn trong hệ thống mạng, do đó DHCP thực sự là công cụ tiết kiệm thời gian cho người quản trị mạng.

Sau khi hoàn tất chương này, các bạn có thể:

- Xác định địa chỉ IP riêng được mô tả trong RFC 1918.
- Nắm được các đặc điểm của NAT và PAT.
- Phân tích các lợi điểm của NAT.
- Phân tích cách cấu hình NAT và PAT, bao gồm cả chuyển đổi cố định, chuyển đổi động và chuyển đổi overloading.
- Xác định các lệnh dùng để kiểm tra cấu hình NAT và PAT.
- Liệt kê các bước xử lý sự cố NAT và PAT.
- Nắm được các ưu điểm và nhược điểm của NAT.
- Mô tả các đặc điểm của DHCP.
- Phân tích sự khác nhau giữa BOOTP và DHCP.
- Phân tích quá trình cấu hình DHCP client.
- Cấu hình DHCP server.
- Xử lý sự cố DHCP.
- Phân tích yêu cầu đặt lại DHCP.

1.1. Chia địa chỉ mạng với NAT và PAT

1.1.1. Địa chỉ riêng

RFC 1918 dành riêng 3 dải địa chỉ IP sau:

- 1 địa chỉ lớp A: 10.0.0.0/8.
- 16 địa chỉ lớp B: 172.16.0.0 – 172.31.255.255 (172.16.0.0/12).

- 256 địa chỉ lớp C: 192.168.0.0-192.168.255.255 (192.168.0.0/16).

Những địa chỉ trên chỉ dùng cho mạng riêng, mạng nội bộ. Các gói dữ liệu có địa chỉ như trên sẽ không định tuyến được trên Internet.

Địa chỉ Internet công cộng phải được đăng ký với một công ty có thẩm quyền Internet, ví dụ như American Registry for Internet Numbers (ARIN) hoặc Réseaux IP Européens (RIPE) và The Regional Internet Registry phụ trách khu vực Châu Âu và Bắc Phi. Địa chỉ IP công cộng còn có thể được thuê từ một nhà cung cấp dịch vụ Internet (ISP). Địa chỉ IP riêng được dành riêng và có thể được sử dụng bởi bất kỳ ai. Điều này có nghĩa là có thể có 2 mạng hoặc 2 triệu mạng sử dụng cùng một địa chỉ mạng riêng. Router trên Internet sẽ không định tuyến các địa chỉ RFC 1918.ISP cấu hình Router biên ngăn không cho các lưu lượng của địa chỉ riêng được phát ra ngoài.

NAT mang đến rất nhiều lợi ích cho các công ty và Internet. Trước đây, khi không có NAT, một máy tính không thể truy cập Internet với địa chỉ riêng. Bây giờ, sau khi có NAT, các công ty có thể cấu hình địa chỉ riêng cho một hoặc tất cả các máy tính và sử dụng NAT để truy cập Internet.

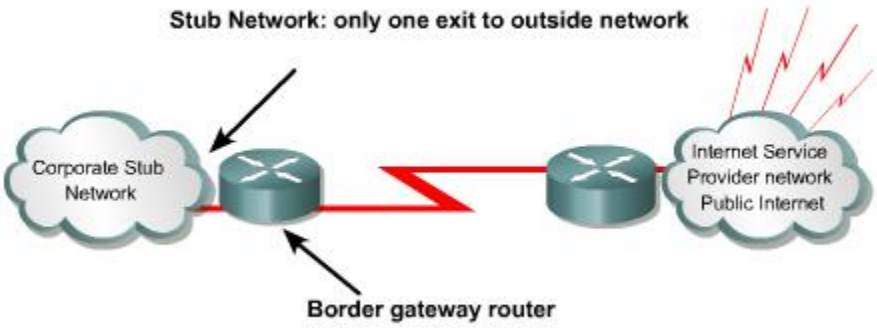
1.1.2. Giới thiệu NAT và PAT

NAT được thiết kế để tiết kiệm địa chỉ IP và cho phép mạng nội bộ sử dụng địa chỉ IP riêng. Các địa chỉ IP riêng sẽ được chuyển đổi sang địa chỉ công cộng định tuyến được bằng cách chạy phần mềm NAT đặc biệt trên thiết bị mạng. Điều này giúp cho mạng riêng càng được tách biệt và giấu được địa chỉ IP nội bộ.

NAT thường được sử dụng trên Router biên của mạng một cửa. Mạng một cửa là mạng chỉ có một kết nối duy nhất ra bên ngoài. Khi một host nằm trong mạng một cửa muốn truyền dữ liệu cho một host nằm bên ngoài nó sẽ truyền gói dữ liệu đến Router biên giới. Router biên giới sẽ thực hiện tiến trình NAT, chuyển đổi địa chỉ

riêng của host nguồn sang một địa chỉ công cộng định tuyến được. Trong thuật ngữ NAT, mạng nội bộ có nghĩa là tập hợp các địa chỉ mạng cần chuyển đổi địa chỉ. Mạng bên ngoài là tất cả các địa chỉ khác còn lai.

Mạng cục bộ chỉ có một cửa ra mạng bên ngoài.



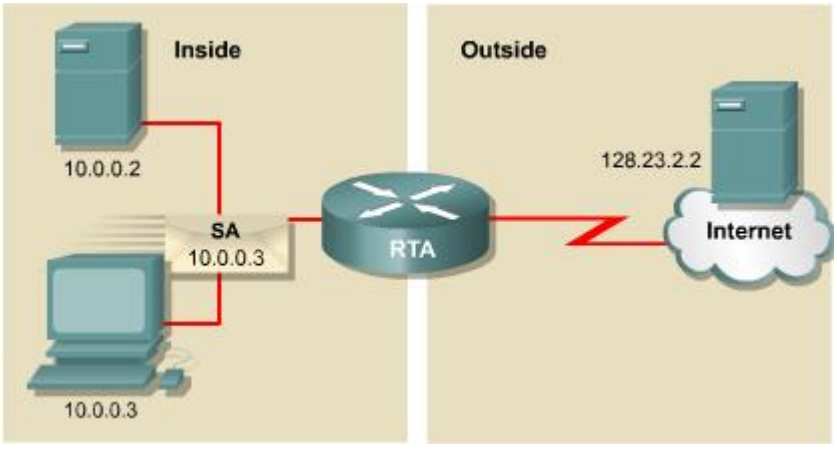
Hình 1.1.2.a. *Mạng một cửa*

Cisco định nghĩa các thuật ngữ NAT như sau:

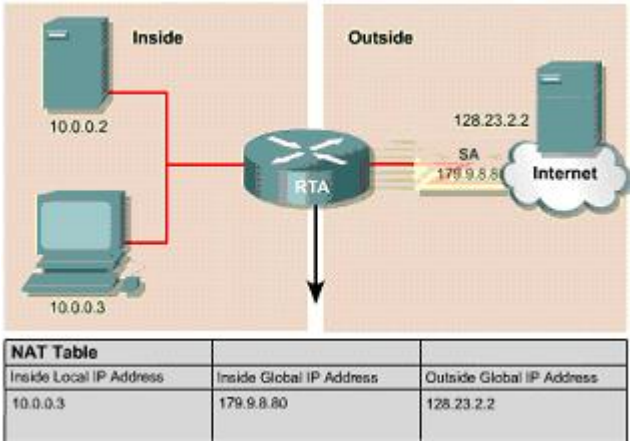
- **Địa chỉ cục bộ bên trong (Inside local address):** là địa chỉ được phân phối cho các host bên trong mạng nội bộ. Các địa chỉ này thường không phải là địa chỉ được cung cấp bởi InterNIC (Internet Network Information Center) hoặc bởi nhà cung cấp dịch vụ Internet. Địa chỉ này thường là địa chỉ riêng RFC 1918.

- **Địa chỉ toàn cục bên trong (Inside global address):** là địa chỉ IP hợp pháp được cung cấp bởi InterNIC hoặc bởi nhà cung cấp dịch vụ Internet. Địa chỉ này đại diện cho một hoặc nhiều địa chỉ nội bộ bên trong đối với thế giới bên ngoài.

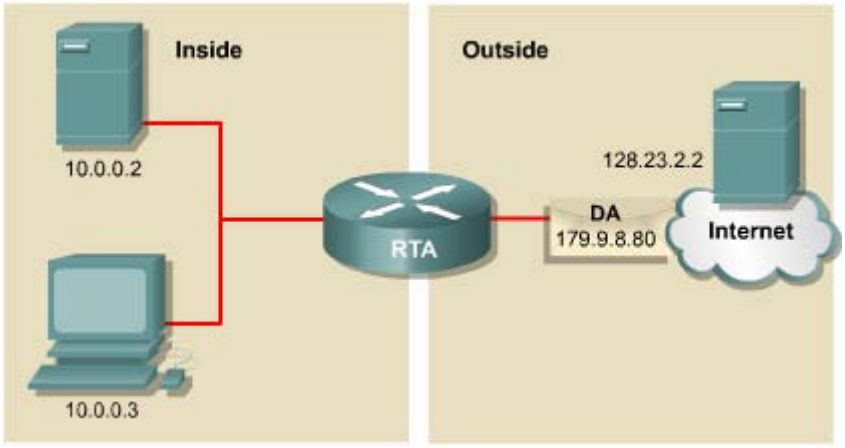
- **Địa chỉ cục bộ bên ngoài (Outside local address):** là địa chỉ riêng của host nằm bên ngoài mạng nội bộ.
- **Địa chỉ toàn cục bên ngoài (Outside global address):** là địa chỉ công cộng hợp pháp của host nằm bên ngoài mạng nội bộ.



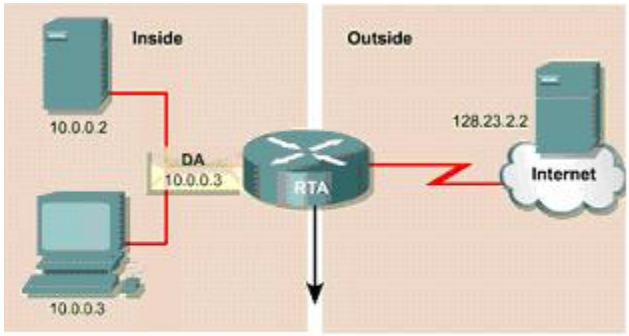
Hình 1.1.2.b. *Host nội bộ 10.0.0.3 muốn gửi gói dữ liệu cho một host nằm ngoài 128.23.2.2. Gói dữ liệu được gửi tới router biên giới RTA.*



Hình 1.1.2.c. *RTA nhận thấy gói dữ liệu này đươc gửi ra ngoài internet nên nó thực hiên tiến trình NAT, chuyến đổi địa chỉ nguồn 10.0.0.3 thành địa chỉ công cộng là 179.9.8.80. Sauk hi thực hiện NAT xong, gói dữ liệu từ RTA đi ra sẽ có địa chỉ nguồn là một địa chỉ công cộng hợp pháp 179.9.8.80.*



Hình 1.1.2.d. *Sau đó server 128..23.2.2 có thể gửi lại một gói trả lời. Khi đó gói trả lời sẽ có địa chỉ đích là 179.9.8.80.*



NAT Table		
Inside Local IP Address	Inside Global IP Address	Outside Global IP Address
10.0.0.3	179.9.8.80	128.23.2.2

Hình 1.1.2.e. *RTA nhận thấy gói dữ liệu này được gửi từ bên ngoài vào trong mạng nội bộ. RTA sẽ tìm trong bảng NAT để ánh xạ từ địa chỉ đích công cộng sang địa chỉ riêng tương ứng. Sau khi thực hiên NAT xong, gói dữ liệu từ RTA phát vào trong mạng nội bộ sẽ có địa chỉ đích là địa chỉ riêng của host đích 10.0.0.3.*

Xét ví dụ hình 1.1.2.b, đối với RTA:

- Địa chỉ nội bộ bên trong là 10.0.0.3.
- Địa chỉ toàn cục bên trong là: 179.9.8.80.
- Địa chỉ toàn cục bên ngoài là: 128.23.2.2.

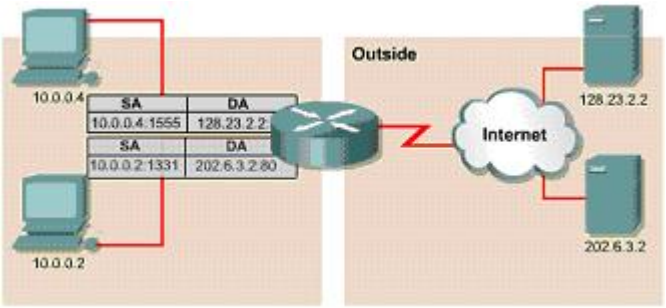
1.1.3. Các đặc điểm của NAT và PAT

Chuyển đổi NAT rất hữu ích cho nhiều mục đích khác nhau và có thể chuyển đổi động hoặc cố định. NAT cố định được thiết kế để ánh xạ **một-một,** từ **một** địa chỉ nội bộ sang **một** địa chỉ công cộng tương ứng duy nhất. Điều này rất tốt đối với những host cần phải có địa chỉ nhất định để truy cập từ Internet. Những host này có thể là các server toàn hệ thống hoặc các thiết bị mạng.

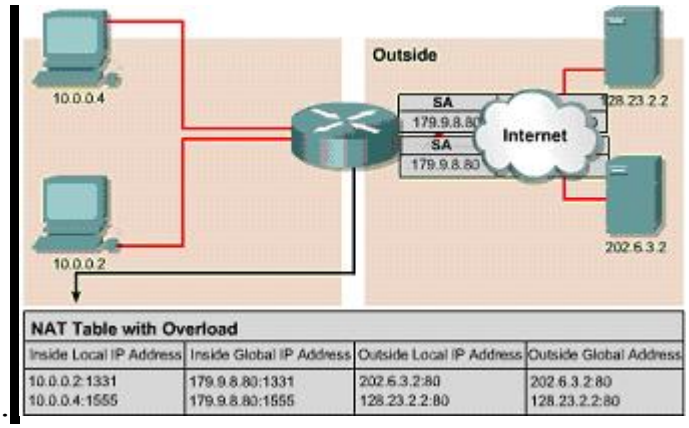
NAT động được thiết kế để ánh xạ **một** địa chỉ IP riêng sang **một** địa chỉ công cộng một cách tự động. Bất kỳ địa chỉ IP nào nằm trong dải địa chỉ IP công cộng đã được định trước đều có thể được gán cho một host bên trong mạng. Overloading hoặc PAT có thể ánh xạ **nhiều** địa chỉ IP riêng sang **một** địa chỉ IP công cộng vì mỗi địa chỉ riêng được phân biệt bằng số port.

PAT sử dụng số port nguồn cùng với địa chỉ IP riêng bên trong để phân biệt khi chuyển đổi. Số port được mã hóa 16 bit. Do đó có tới 65.536 địa chỉ nội bộ có thể được chuyển đổi sang một địa chỉ công cộng. Thực tế thì số lượng port có thể gán cho một địa chỉ IP là khoảng 4000 port. PAT sẽ cố gắng giữ nguyên số port nguồn ban đầu. Nhưng nếu số port này đã bị sử dụng thi PAT sẽ lấy số port còn trống đầu tiên trong các nhóm port 0-511, 512-1023, 1024-65535.

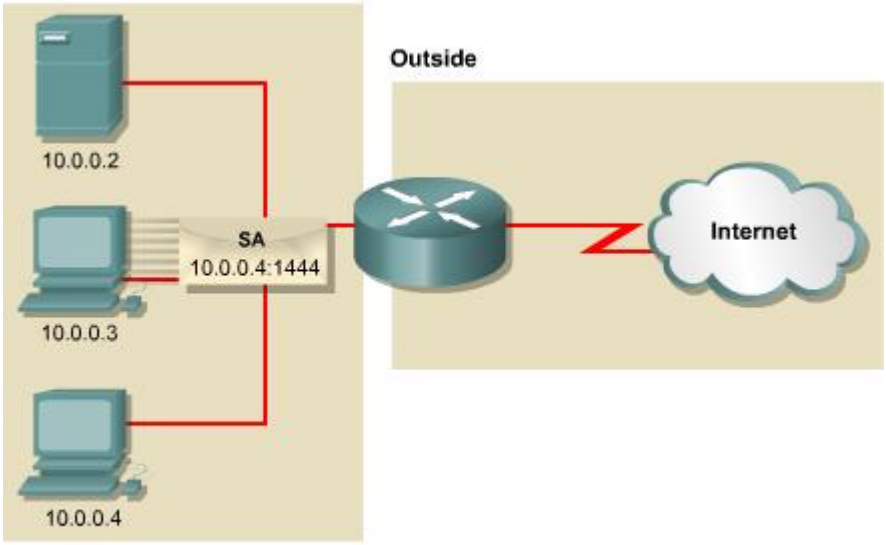
Khi không còn số port nào còn trống và vẫn còn địa chỉ IP công cộng khác đã được cấu hình thì PAT sẽ chuyển sang địa chỉ IP công cộng kế tiếp và bắt đàu xác định số port nguồn như trên. Quá trình này sẽ được thực hiện cho đến khi nào hết số port và địa chỉ IP công cộng còn trống.



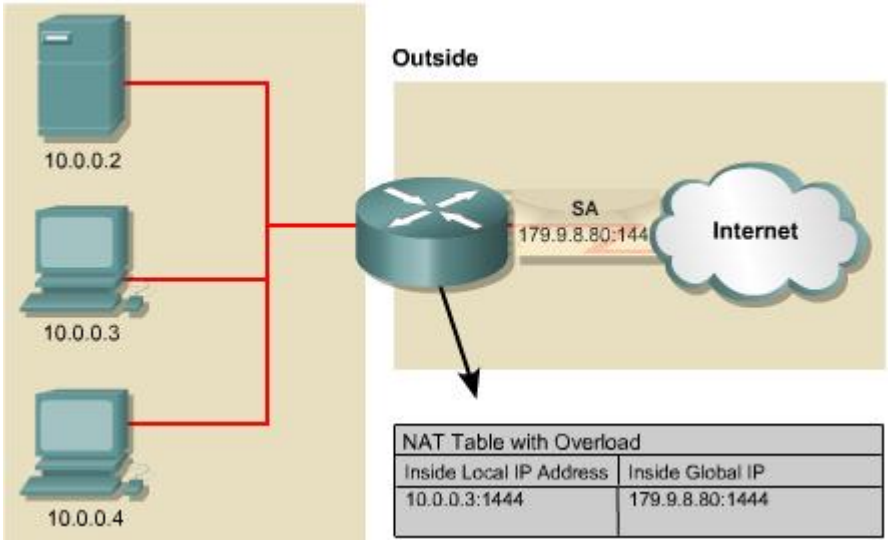
Hình 1.1.3.a.



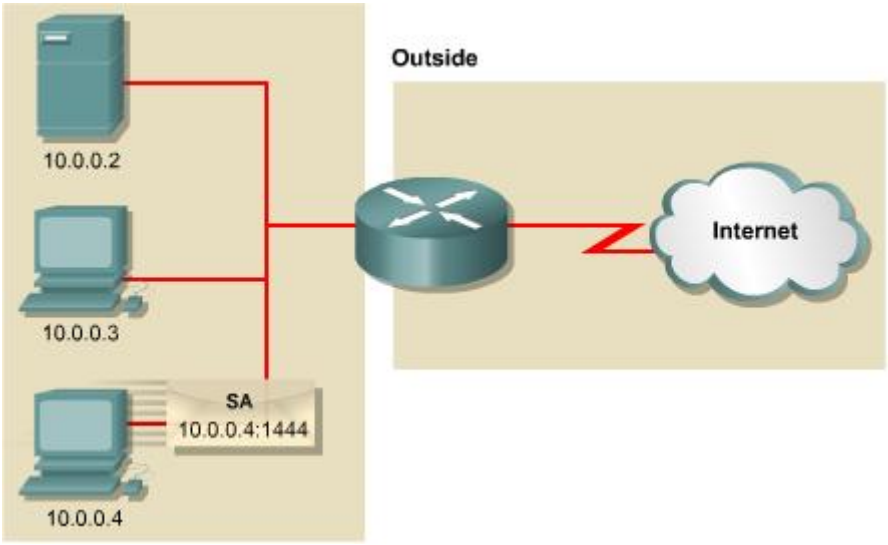
Hình 1.1.3.b.



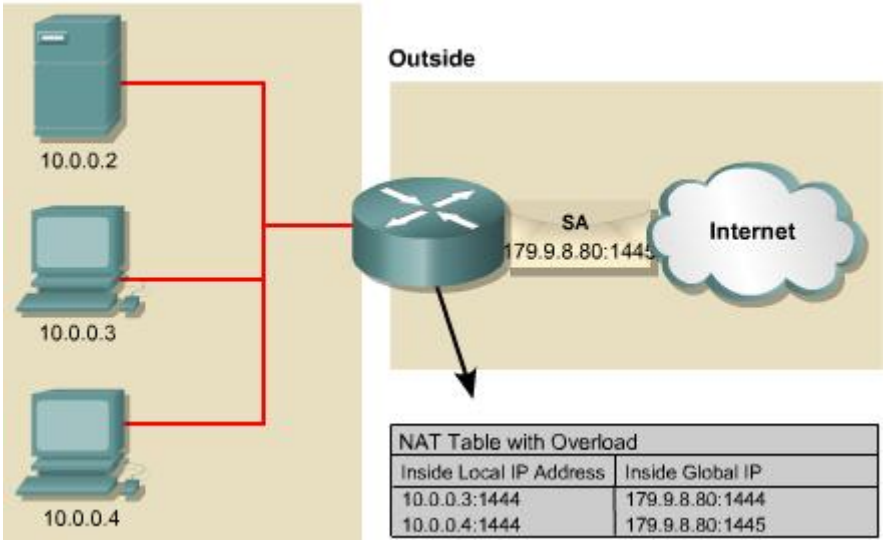
Hình 1.1.3.c. *Host 10.0.0.3 gửi gói dữ liệu ra internet. Trong gói dữ liệu này, địa chỉ IP nguồn là 10.0.0.3, port là* ***1444***



Hình 1.1.3.d. *Router thực hiện chuyển đổi địa chỉ IP nguồn từ 10.0.0.3 sang địa chỉ 179.9.8.80, port nguồn vẫn giữ nguyên là 1444.*



Hình 1.1.3.e. *Bây giờ Host 10.0.0.4 cũng gửi gói dữ liệu ra internet với địa chỉ nguồn là 10.0.0.4, port nguồn là 1444*



Hình 1.1.3.f. *Router thực hiện chuyển đổi địa chỉ IP nguồn từ 10.0.0.4 sang 179.9.8.80. Port nguồn là 1444 lúc này phải đổi sang 1445. Như vậy theo như bảng NAT trong hình ta thấy địa chỉ công cộng 179.9.8.80: 1444 là tương ứng với 10.0.0.3:1444, 179.9.8.80:1445 tương ứng với 10.0.0.4:1444. Bằng cách sử dụng kết hợp với số port như vậy, PAT có thể ánh xạ một địa chỉ IP công cộng cho nhiều địa chỉ riêng bên trong.*

NAT cung cấp những lợi điểm sau:

- Không cần phải gán địa chỉ IP mới cho từng host khi thay đổi sang một ISP mới. Nhờ đó có thể tiết kiệm được thời gian và tiền bạc.
- Tiết kiệm địa chỉ thông qua ứng dụng ghép kênh cấp độ port. Với PAT, các host bên trong có thể chia sẻ một địa chỉ IP công cộng để giao tiếp với bên ngoài. Với cách cấu hình này, chúng ta cần rất ít địa chỉ công cộng, nhờ đó có thể tiết kiệm địa chỉ IP.
- Bảo vệ mạng an toàn vì mạng nội bộ không để lộ địa chỉ và cấu trúc bên trong ra ngoài.

1.1.4. Cấu hình NAT và PAT

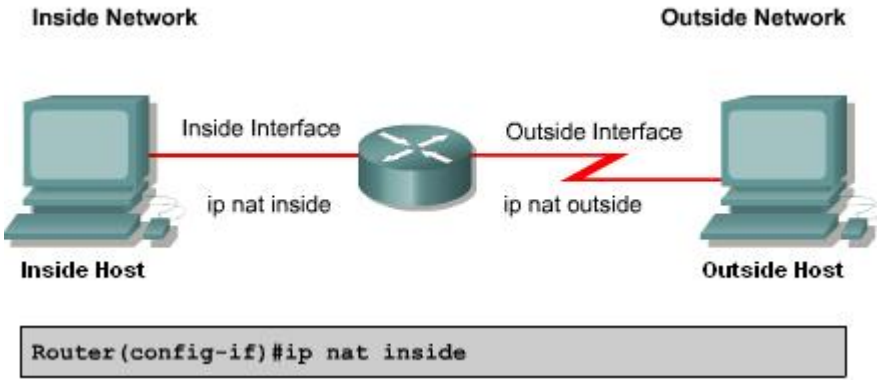
1.1.4.1. Chuyển đổi cố định

Để cấu hình chuyển đổi cố định địa chỉ nguồn bên trong, chúng ta cấu hình các bước như sau:

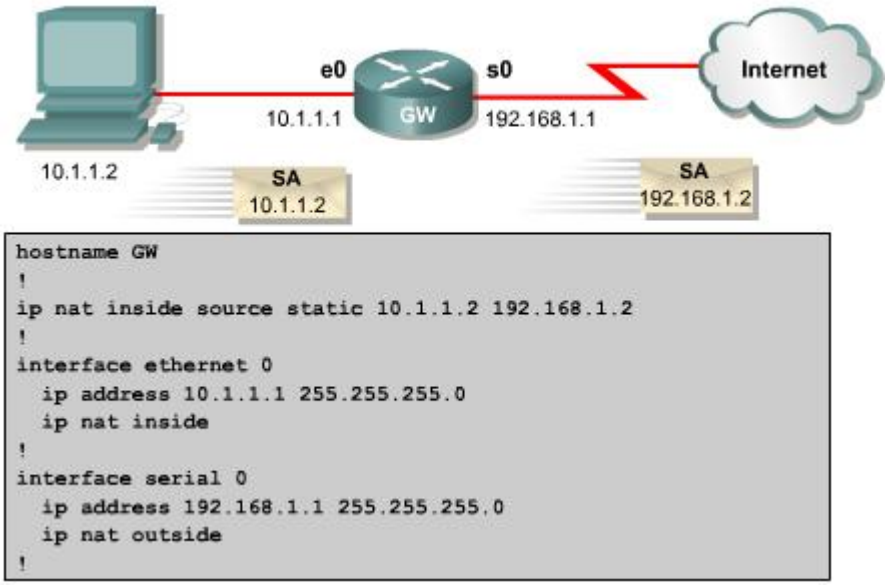
Bước	Thực hiện	Ghi chú
1	Thiết lập mối quan hệ chuyển đổi giữa địa chỉ nội bộ bên trong và địa chỉ đại diện bên ngoài *Router (config) #* **ip nat inside** **source static** *local-ip global-ip*	Trong chế độ cấu hình toàn cục, bạn dùng câu lệnh **no ip nat inside source static** để xóa sụ chuyển đổi địa chỉ cố định.
2	Xác định cổng kết nối vòa mạng bên trong. *Router (config) #* **interface** *type number*	Sau khi gõ lệnh **interface**, dấu nhắc của dòng lệnh sẽ chuyển từ (config) # sang (config-if) #
3	Đánh dấu cổng này là cổng kết nối vào mạng nội bộ bên trong. *Router (config-if) #* **ip nat inside**	
4	Thóat khỏi chế độ cấu hình cổng hiện tại. *Router (config-if) #* **exit**	
5	Xác định cổng kết nối ra mạng công cộng bên ngoài. *Router (config) #* **interface** *type number*	

6	Đánh dấu cổng này là cổng kết nối ra mạng công cộng bên ngoài. *Router (config-if) #* **ip nat outside**	

Hình vẽ - 2 hình



Hình 1.1.4.a *Sự chuyển đổi địa chỉ sẽ được thực hiện giữa hai cổng inside và outside*



Hình 1.1.4.b. *Cấu hình NAT chuyển đổi cố định từ địa chỉ 10.1.1.2 sang 192.168.1.2. Khi có một gói dữ liệu từ host 10.1.1.2 được gửi ra ngoài internet, router GW sẽ chuyển đổi địa chỉ nguồn 10.1.1.2 của gói dữ liệu sang địa chỉ 192.168.1.2 trước khi phát gói ra cổng s0.*

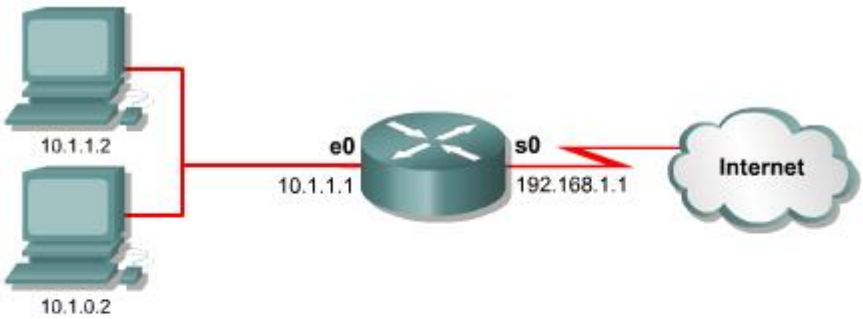
1.1.4.2. Chuyển đổi động

Để Chuyển đổi động địa chỉ nguồn bên trong, chúng ta cấu hình theo các bước như sau:

Bước	**Thực hiện**	**Ghi chú**
1	Xác định dải địa chỉ đại diện bên ngoài *Rourter (config) #* **ip nat pool** *name start-ip end-ip* [**netmask** *netmask* /**prefix-length** *prefix-length*]	Trong chế độ cấu hình toàn cục, gõ lệnh **no ip nat pool** *name* để xóa dải địa chỉ đại diên bên ngoài.
2	Thiết lập ACL cơ bản cho phép những địa chỉ nội bộ bên trong nào được chuyển đổi. *Router (config) #* **access-list** *access-list-number* **permit** *source [source-wildcard]*	Trong chế độ cấu hình toàn cục, gõ lệnh **no access-list** *access-list-number* để xóa ACL đó.
3	Thiết lập mối liên quan giữa địa chỉ nguồn đã được xác định trong ACL ở bước trên với dải địa chỉ đại diện bên ngoài: *Router (config) #* **ip nat inside source list** *access-list-number* **pool** *name*	Trong chế độ cấu hình toàn cục, gõ lênh **no ip nat inside source** để xóa sự chuyển đổi động này
4	Xác định cổng kết nối vào mạng nội bộ	Sau khi gõ xong lệnh

	Router (config) # **interface** *type number*	**interface**, dấu nhắc của dòng lệnh sẽ chuyển đổi từ config sang (config-if)#
5	Đánh dấu cổng này là cổng kết nối vào mạng nội bộ. *Router (config-if) #* ***ip nat inside***	
6	Thóat khỏi chế độ cổng hiện tại. *Router (config) #* **exit**	
7	Xác định cổng kết nối ra bên ngoài. *Router (config) #* **interface** *type number*	
8	Đánh dấu cổng này là cổng kết nối ra bên ngoài. *Router (config) #* **ip nat outside**	

Danh sách điều khiển truy cập (ACL – Access Control List) cho phép khai báo những địa chỉ nào được chuyển đổi. Bạn nên nhớ là kết thúc một ACL luôn có câu lệnh ẩn cấm tuyệt đối để tránh những kết quả không dự tính được khi một ACL có quá nhiều điều kiện cho phép. Cisco khuyến cáo là không nên dùng điều kiện cho phép tất cả **permit any** trong ACL sử dụng cho NAT vì câu lệnh này làm hao tốn quá nhiều tài nguyên của Router và do đó có thể gây ra sự cố mạng.




```
ip nat pool nat-pool1 179.9.8.80 179.9.8.95 netmask 255.255.255.0
ip nat inside source list 1 pool nat-pool1
!
interface ethernet 0
  ip address 10.1.1.1 255.255.0.0
  ip nat inside
!
interface serial 0
  ip address 192.168.1.1 255.255.255.0
  ip nat outside
!
access-list 1 permit 10.1.0.0 0.0.0.255
```

Hình 1.1.4.c

Xét ví dụ hình 1.1.4.c: Dải địa chỉ công cộng đại diện ben ngoài có tên là nat-pool1, bao gồm các địa chỉ từ 179.9.8.80 đến 179.9.95. Địa chỉ nội bộ bên trong được phép chuyển đổi được định nghĩa trong access-list 1 là 10.1.0.0 – 10.1.0.255. Như vậy, gói dữ liệu nào trong mạng nội bộ đi ra ngoài Internet có địa chỉ nguồn nằm trong dải địa chỉ 10.1.0.0 – 10.1.0.255 sẽ được chuyển đổi địa chỉ nguồn sang một trong bất kỳ địa chỉ nào còn trống trong dải địa chỉ công cộng 179.9.8.80 – 179.9.8.95. Host 10.1.1.2 sẽ không được chuyển đổi địa chỉ vì địa chỉ của nó không được cho phép trong acces-list 1, do đó nó không truy cập được Internet.

Overloading hay PAT

Overloading được cấu hình theo hai cách tùy theo địa chỉ IP công cộng được cấp phát như thể nào. Một ISP có thể cho một hệ thống mạng của khách hàng sử dụng chung một địa chỉ IP công cộng duy nhất, đia jchỉ IP công cộng này chính là địa chỉ của cổng giao tiếp trên Router nối về ISP. Sau đây là ví dụ cấu hình cho tình huống này:

Router (config) # access-list 1 permit 10.0.0.0 0.0.255.255

Router (config) ip nat inside source list 1 interface serial0/0 overload

Bước	Thực hiện	Ghi chú
1	Tạo ACL để cho phép những địa chỉ nội bộ nào được chuyển đổi. *Router(config) #* **access-list** *acl-number* **permit** *source [source-wildcard]*	Trong chế độ cấu hình toàn cục, gõ lệnh **no access-list** *access-list-number* để xóa access-list tương ứng.
2A	Thiết lập mối liên quan giữa địa chỉ nguồn đã được xác định trong access-list ở bước trên với địa chỉ đại diện là địa chỉ của cổng kết nối với bên ngoài. *Router (config) #* **ip nat inside source list** *acl-number* **interface** *interface* **overload**	Trong chế độ cấu hình toàn cục, gõ lệnh **no ip nat inside source** để xóa sự chuyển đổi động này. Từ khóa **overload** để cho phép chạy PAT
Hoặc 2B	Khai báo dải địa chỉ đại diện bên ngoài dùng overload. *Router (config)* **ip nat pool** *name start-ip end-ip* *[***netmask** *netmask / **prefix-length** prefix-length]* Thiết lập chuyển đổi overload giữa địa chỉ nội bộ đã được xác định trong ACL ở bước 1 với dải địa chỉ đại diện bên ngoài mới khai báo ở	

	trên. Router (config) # **ip nat inside source list** *acl-number* **pool** *name* **overload**	
3	Xác định cổng kết nối với mạng nội bộ. Router (config) # **interface** *type number* Router (config-if) # **ip nat inside**	Sau khi gõ lệnh **interface**, dấu nhắc của dòng lệnh sẽ được đổi từ (config)# sang (config-if)#
4	Xác định cổng kết nối với bên ngoài. Router (config) # **interface** *type number* Router (config-if) # **ip nat outside.**	

Một cách khác để cấu hình Overload là khi ISP cung cấp một hoặc nhiều địa chỉ IP công cộng để cho hệ thống mạng khách hàng sử dụng làm dải địa chỉ chuyển đổi PAT. Cấu hình ví dụ cho tình huống này như sau:

- Xác định địa chỉ nội bộ được phép chuyển đổi là 10.0.0.0/16:

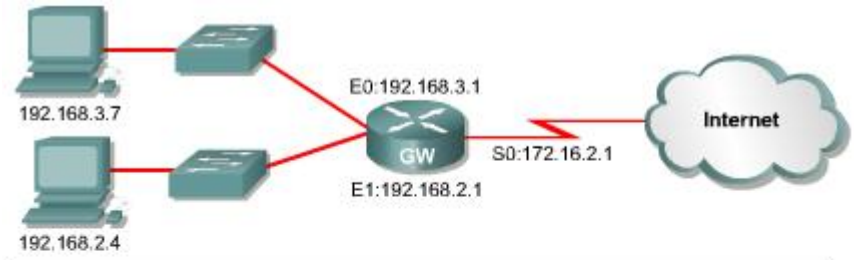
Router (config) # access-list 1 permit 10.0.0.0.0.0.255.255

- Khai báo dải địa chỉ đại diện bên ngoài với tên là nat-pool2, bao gồm các địa chỉ trong subnet 179.9.8.20/28:

  Router (config) # ip nat pool nat-pool2 179.9.8.20 netmask 255.255.255.240

- Thiết lập sự chuyển đổi Overload địa chỉ nội bộ được xác định trong access-list 1 với dải địa chỉ đại diện nat pool2:

  Router (config) # ip nat inside source list 1 pool nat-pool2 overload




```
interface ethernet 0
  ip address 192.168.3.1 255.255.255.0
  ip nat inside
!
interface ethernet 1
  ip address 192.168.2.1 255.255.255.0
  ip nat inside
!
interface serial 0
  ip address 172.16.2.1 255.255.255.0
  ip nat outside
!
ip nat inside source list 1 interface serial 0 overload
!
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 1 permit 192.168.3.0 0.0.0.255
```

Hình 1.1.4.d.

Xét ví dụ hình 1.1.4.d: địa chỉ nội bộ bên trong được phép chuyển đổi được xác định trong access-list 1 là 192.168.2.0/24 và 192.168.3.0/24. Địa chỉ đại diện bên ngoài là địa chỉ của cổng serial 0, cổng kết nối ra Internet. Như vậy phải toàn bộ địa chỉ bên trong được chuyển đổi PAT với một địa chỉ IP đại diện duy nhất là địa chỉ của cổng kết nối ra Internet, cổng serial 0.

1.1.5. Kiểm tra cấu hình PAT

Sau khi NAT đã được cấu hình, chúng ta có thể dùng lệnh clear và show để kiểm tra hoạt động của NAT.

Mặc định, trong bảng chuyển đổi NAT động, mỗi một cặp chuyển đổi địa chỉ sẽ bị xóa đi sau một khoảng thời gian không sử dụng. Với chuyển đổi không sử dụng chỉ số Port thì khoảng thời gian mặc định là 24 giờ. Chúng ta có thể thay đổi khoảng thời gian này bằng lệnh **ip nat translation timeout** *timeout_seconds* trong chế độ cấu hình toàn cục.

Các thông tin về sự chuyển đổi có thể được hiển thị bằng các lệnh sau:

Lệnh	**Giải Thích**
Clear ip nat translation *	Xóa mọi cặp chuyển đổi địa chỉ động trong bảng NAT.
Clear ip nat translation inside *global-ip local-ip* [**outside** *local-ip global-ip*]	Xóa một cặp chuyển đổi địa chỉ động bên trong hoặc cả bên trong và bên ngoài tương ứng với địa chỉ cụ thể được khai báo trong câu lệnh.
Clear ip nat translation *protocol* **inside** *global-ip global-port local-ip local-port* [**outside** *local-ip local-port global-ip global-port*]	Xóa một cặp chuyển đổi địa chỉ động mở rộng.
Show ip nat translations	Hiển thị bảng NAT đang hoạt động.
Show ip nat statistics	Hiển thị trạng thái hoạt động của NAT.

```
Router#show ip nat translations
Pro Inside global     Inside local       Outside local      Outside global
172.16.131.1          10.10.10.1         ---                ---
```

Hình 1.1.5.a

```
Router#show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces:
Serial0
Inside interfaces:
Ethernet0, Ethernet1
Hits: 5 Misses:0
```

Hình 1.1.5.b

Chúng ta có thể dùng lệnh **show run** để kiểm tra lại các giá trị cần khai báo trong các câu lệnh cấu hình NAT, access-list, interface.

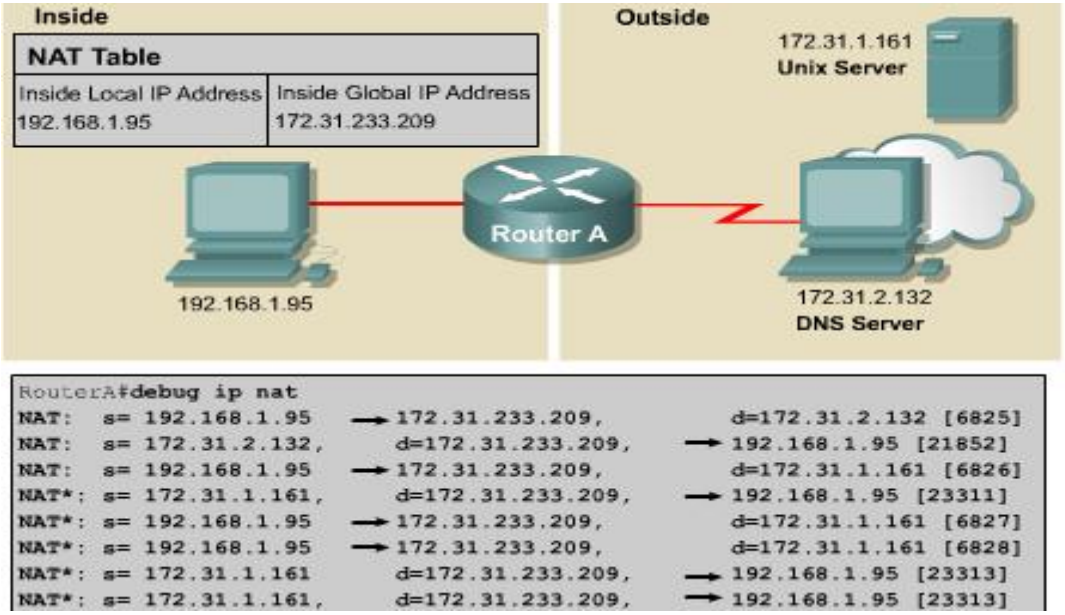
1.1.6. Xử lý sự cố cấu hình NAT và PAT

Thường rất khó xác định nguyên nhân của sự cố khi kết nối IP bị sự cố trong môi trường NAT. Nhiều khi chúng ta nhầm lẫn là do NAT gây ra nhưng thực sự nguyên nhân lại nằm ở chỗ khác.

Khi cố gắng xác định nguyên nhân sự cố của một kết nối IP, chung ta nên cố gắng xác định loại trừ khả năng từ NAT trước. Sau đay là các bước để kiểm tra hoạt động của NAT:

1. Dựa vào tập tin cấu hình, xác định rõ ràng NAT thực hiện những gì.
2. Kiểm tra bảng NAT xem các chuyển đổi địa chỉ có đúng không.
3. Kiểm tra hoạt động NAT xảy ra như thế nào bằng các lệnh **show** và **debug.**
4. Xem chi tiết những gì xảy ra cho một gói dữ liệu và kiểm tra xem router có định tuyến đúng cho gói dữ liệu hay không.

Sử dụng lệnh **debug ip nat** để kiểm tra hoạt động của NAT, hiển thị các thông tin về mỗi gói được chuyển đổi NAT bởi router. Lệnh **debug ip nat** *detal* còn cung cấp thêm một số thông tin liên quan đến sự chuyển của mỗi gói giúp chúng ta xác định lỗi, ví dụ như lỗi không xác định được địa chỉ đại diện bên ngoài.



Hình 1.1.6

Xét ví dụ hình 1.1.6. Hai dòng đầu tiên cho thấy các gói yêu cầu và trả lời DNS được phát đi. Những dòng còn lại cho biết về một kết nối Telnet từ một host bên trong tới một host bên ngoài mạng.

Để giải mã những thông tin hiển thị của lệnh **debug**, chúng ta dựa vào những điểm mấu chốt sau:

- Dấu * kế bên từ NAT cho biết sự chuyển đổi đang được thực hiện trên đường chuyển mạch nhanh. Gói dữ liệu đầu tiên của một phiên đối thoại luôn được xử lý chuyển mạch nên chuyển mạch chậm. Các gói dữ liệu tiếp theo được truyền chuyển mạch nhanh với bộ đệm, không cần xử lý nhiều như gói đầu tiên.

- S= a.b.c.d là địa chỉ nguồn.
- Địa chỉ nguồn a.b.c.d được dịch sang w.x.y.z.
- D=e.f.g.h là địa chỉ đích.
- Giá trị trong giấu ngoặc vuông là chỉ số danh đinh IP. Thông tin này có thể sẽ hữu dụng vì dựa vào đó chúng ta sẽ tìm được những gói dữ liệu tương ứng được phân tích từ những phần mền phân tích giao thức khác.

1.1.7. Những vấn đề của NAT

NAT có những ưu điểm sau:

- Tiết kiệm địa chỉ đăng ký hợp pháp bằng cách cho phép sử dụng địa chỉ riêng.
- Tăng tính linh hoạt của các kết nối ra mạng công cộng. Chúng ta có thể triển khai nhiều dải địa chỉ chia tải để đảm bảo độ tin cậy của kết nối mạng công cộng.
- Nhất quán hồ sơ địa chỉ mạng nội bộ. Nếu mạng không sử dụng địa chỉ IP riêng và NAT mà sử dụng địa chỉ công cộng thì khi thay đổi địa chỉ công cộng, toàn bộ hệ thống mạng phải đặt lại địa chỉ. Chi phí cho việc đặt lại địa chỉ toàn bộ các thiết bịi mạng nội bộ được giữ nguyên khi thay đổi địa chỉ công cộng.

NAT cũng không phải là không có nhược điểm. Khi chuyển đổi địa chỉ như vậy sẽ làm mất đi một số chức năng đặc biệt của giao thức và ứng dụng có cần đến các thông tin địa chỉ IP trong gói IP. Do đó cần phải có thêm các hỗ trợ khác cho thiết bị NAT.

NAT làm tăng thời gian trễ. Thời gian trễ chuyển mạch sẽ lớn hươn do đó phải chuyển đổi từng địa chỉ IP trong mỗi dữ liệu. Gói dữ liệu đầu tiên luôn phải sử lý chuyển mạch nên thời gian chuyển mạch nhanh hơnnếu có bộ đệm.

Hiệu suất hoạt động cũng là một vấn đề cần được quan tâm vì NAT được thực hiện trong tiến trình chuyển mạch. CPU phải được kiểm tra từng gói dữ liệu để quyết định gói dữ liệu đó có cần chuyển đổiđịa chỉ hay không. CPU phải thay đổi phần gói IP của gói dữ liệu và cũng có htể phải thay cả phần đóng gói TCP hoặc UDP.

Một nhược điểm đáng kể khi sử dụng NAT là sự mất đi khả nặng truy tìm địa chỉ IP đầu cuối-đến-đầu cuối. Việc truy theo gói dữ liệu sẽ trở nên khó hơn do gói dữ liệu thay đổi địa chỉ nhiều lần qua nhiều trạm NAT. Hacker sẽ rất khó khăn khi muốn xác định địa chỉ nguồn hoặc đích của gói dữ liệu.

NAT cũng làm cho một số ứng dụng sử dụng địa chỉ IP không hoạt động được vì nó giấu địa chỉ IP đầu cuối-đến-đầu cuối. Những ứng dụng sử dụng địa chỉ vật lý thay vì sử dụng tên miền sẽ không đến được đích nằm sau router NAT. Đôi khi, sự cố này có thể tránh được bằng cách ánh xạ NAT cố định.

Cisco IOS NAT hỗ trợ các loại lưu lượng sau:

- ICMP
- File Transfer Protocol (FTP), bao gồm lệnh PPRRT và PÁV.
- Dịch vụ NetBIOS qua TCP/IP, gói dự liệu, tên và phiên giao tiếp.
- RealNetworks’ RealAudio
- White Pines’ CUSeeMe
- Xing Technologies’ StreamWorks
- DNS “A” and “PTR” queries
- H.323/Microsoft NetMeeting, IOS versions 12.0(1)/ 12.0(1) T và sau đó.
- VDOnet’s VDOLive, IOS version 11.3(4)11.3(4)T và sau đó.
- VXtreme’s Web Theater, IOS versions 11.3(4)11.3(4)T và sau đó.
- IP Multicast, IOS version 12.0(1)T chỉ chuyển đổi địa chỉ nguồn.

Cisco IOS NAT không hỗ trợ các loại giao thức sau:

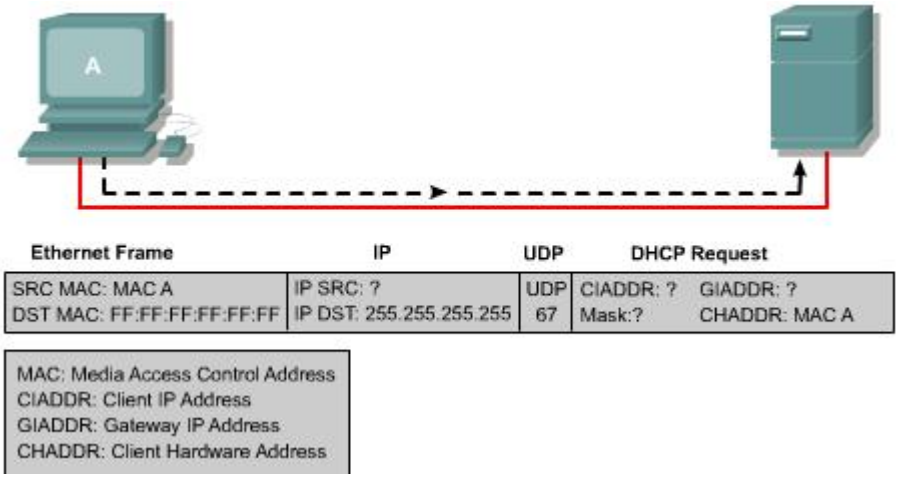
- Thông tin cập nhật bảng định tuyến.
- Chuyển đổi vùng DNS.
- BOOTP
- Giao thức talk and ntalk.
- Giao thức quản lý mạng đơn giản – Simple Network Management Protocol (SNMP)

1.2. DHCP

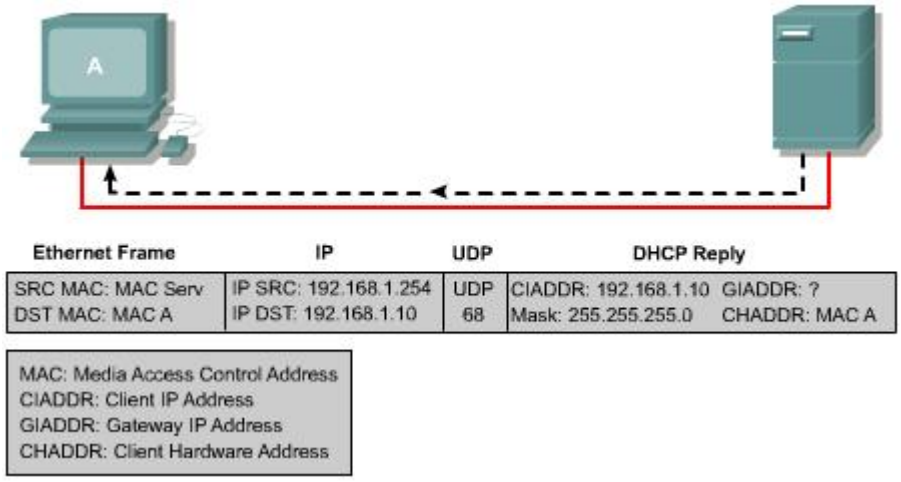
1.2.1. Giới thiệu DHCP

Giao thức cấu hình hoạt động (DHCP – Dynamic Host Configuration Protocol) làm việc theo chế độ client-server. DHCP cho phép các DHCP client trong một mạng IP nhận cấu hình IP của mình từ một DHCP server. Khi sử dụng DHCP thì công việc quản lý mạng IP sẽ ít hơn vì phần lớn cấu hình IP của client được lấy về từ server. Giao thức DHCP được mô tả trong RFC 2131.

Một DHCP client có thể chạy hầu hết các hệ điều hành Windows, Netvell Netửae, Sun Solaris, Linux và MAC OS. Client yêu cầu server DHCP cấp một địa chỉ cho nó. Server này quản lý việc cấp phát địa chỉ IP, sẽ gửi trả lời cấu hình IP cho client. Một DHCP có thể phục vụ cho nhiều subnet khác nhau nhưng không phục vụ cho cấu hình router, switch và các server khác vì những thiết bị này cần phải có địa chỉ IP cố định.



Hình 1.2.1.a. *Client gửi trực tiếp quảng bá một yêu cầu DHCP. Trường hợp đơn giản nhất là có DHCP server nằm trong cùng subnet với client, server DHCP này sẽ nhận được gói yêu cầu. Server thấy phần GIADDR bỏ trống thì biết client nằm trong cùng subnet với server. Đồng thời server sẽ đọc địa chỉ vật lý (địa chỉ MAC) của client.*



Hình 1.2.1.b. *Server sẽ lấy một địa chỉ IP trong dải địa chỉ tương ứng để cấp cho client. Sau đó server dùng địa chỉ của vật lý của client để gửi gói trả lời lại cho client.*

Hình 1.2.1.c. *Hệ điều hành trên DHCP client sẽ dùng những thông tin nhận được trong gói trả lời server để cấu hình IP cho client đó.*

Server chạy DHCP thực hiện tiến trình xác định địa chỉ IP cấp cho client. Client sử dụng địa chỉ được cấp từ server trong một khoảng thời gian nhất định do người quản trị mạng quy định. Khi thời này hết hạn thì client phải yêu cầu cấp lại địa chỉ mới mặc dù thông thường client sẽ vẫn được cấp lại địa chỉ cũ.

Các nhà quản trị mạng thường sử dụng dịch vụ DHCP vì giải pháp này giúp quản lý hệ thống mạng dễ và có khả năng mở rộng. Cisco router có thể sử dụng Cisco IOS có hỗ trợ Easy IP để làm DHCP server. Mặc định , Easy IP cấp cấu hình IP cho client sử dụng trong 24 tiếng. Cơ chế này rất tiện lợi cho các văn phòng nhỏ hoặc những văn phòng tại nhà, người sử dụgn tại nhà có thể tận dụng diạhc vụ DHCP và NAT của router mà không cần phải có thêm một server NT hoặc UNIX. Người quản trị mạng cài đặt dải địa chỉ cho DHCP server còn có thể cung cấp nhiều thông tin khác như địa chỉ DNS server, địa chỉ WINS server và tên miền. Hầu hết các DHCP server đều cho phép người quản trị mạng khai báo những địa chỉ MAC nào cần phục vụ và tự động cấp cho những địa chỉ MAC này địa chỉ IP không thay đổi mỗi lần chúng yêu cầu.

DHCP sử dụng giao thức UDP (User Datagram Protocol) làm giao thức vận chuyển của nó. Client gửi thông điệp cho server trên port 67. Server gửi thông điệp cho client trên port 68.

1.2.2. Những điểm khác nhau giữa BOOTP và DHCP

Đầu tiên cộng đồng Internet phát triển giao thức BOOTP để cấu hình cho máy trạm không có ổ đĩa. BOOTP được định nghĩa trong RFC 951 vào năm 1985. Là một phiên bản đi trước của DHCP nên BOOTP cũng có nhiều đặc điểm hoạt động tương tự như DHCP. Cả hai giao thức này đêgu dựa trên cơ sở client-server và sử dụng port UDP 67, 68. Hai port này hiện vẫn được biết đến như là port BOOTP.

Một cấu hình IP cơ bản bao gồm 4 thông tin sau:

- Địa chỉ IP.
- Địa chỉ Gateway.
- Subnet mask.
- Địa chỉ DNS server.

BOOTP không tự động cấp phát địa chỉ IP cho một host. Khi client yêu cầu một địa chỉ IP, BOOTP server tìm trong bảng đã được cấu hình trước xem có hàng nào tương ứng với địa chỉ MAC của client hay không.Nếu có thì địa chỉ IP tương ứng sẽ được cung cấp cho client. Điều này có nghĩa là địa chỉ MAC và địa chỉ IP tương ứng phải được cấu hình trước trên BOOTP server.

Sau đây là hai điểm khác nhau cơ bản giữa BOOTP và DHCP:

- DHCP cấp một địa chỉ IP cho một client trong một khoảng thời gian nhất định. Hết khoảng thời gian này địa chỉ IP có thể được cấp cho client khác. Client có thể lấy địa chỉ mới hoặc vẫn có thể tiếp tục giữ địa chỉ cũ.
- DHCP cung cấp cho client nhiều thông tin cấu hình IP khác như địa chỉ WINS server, tên miền.

BOOTP	DHCP
Ánh xạ cố định giữ địa chỉ MAC và địa chỉ IP	Ánh xạ tự động giữa địa chỉ MAC và dải địa chỉ IP tương ứng.
Cấp cố định	Cấp trong một khoảng thời gian nhất định
Chỉ cung cấp 4 thông tin cơ bản của cấu hình IP	Có thể cung cấp hơn 30 thông tin cấu hình IP

1.2.3. Những điểm chính của DHCP

Có 3 cơ chế dùng để cấp phaqst một địa chỉ IP cho client:

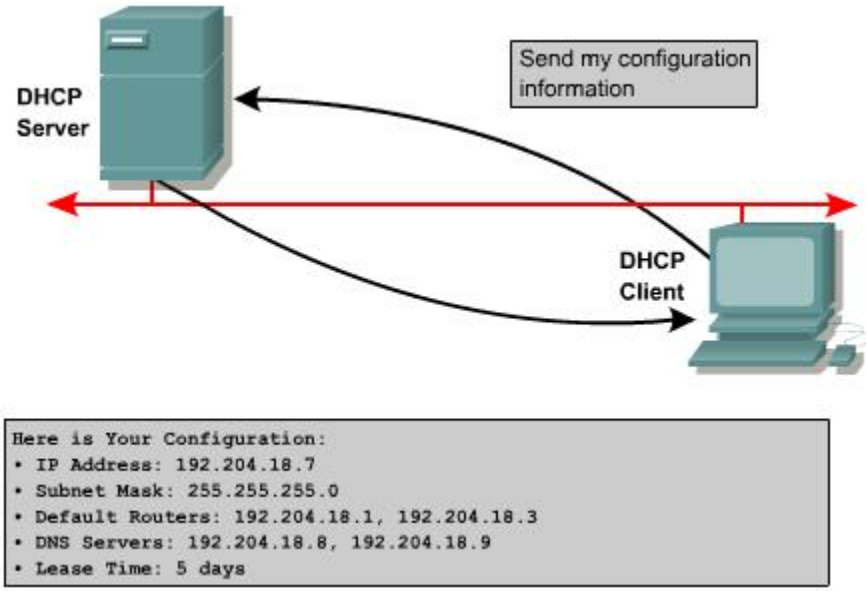
- Cấp phát tự động – DHCP tự động chọn một địa chỉ IP trong dải địachỉ được cấu hình và cấp địa chỉ IP đó cố định, không thay đổi cho một client.
- Cấp phát cố định – Địa chỉ IP của một client do người quản trị mạng quyết định. DHCP chỉ truyền địa chỉ này cho client đó.
- Cấp phát động – DHCP cấp và thu hồi lại một địa chỉ IP của client theo một khoảng thời gian giới hạn.

Trong phần này chúng ta tập trung vào cơ chế cấp phát động. Một số thông số cấu hình được liệt kê trong IÈT RFC 1533 là:

- Subnet mask
- Router
- Tên miền
- Server DNS
- WINS server

Chúng ta có thể tạo trên DHCP server nhiều dải địa chỉ IP và thông số như trên tương ứng. Mỗi một dải địa chỉ dành riêng cho một subnet IP. Điều này cho phép

có thể có nhiều DHCP cùng trả lời và IP client có thể di động. Nếu có nhiều server cùng trả lời thì client có thể chọn một trả lời duy nhất.



Hình 1.2.3

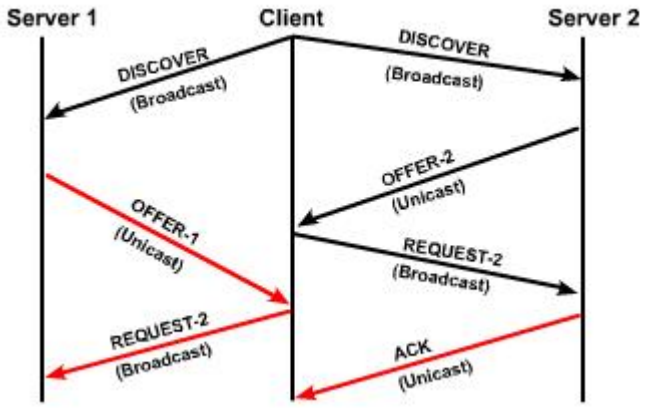
1.2.4. Hoạt động của DHCP

Quá trình DHCP client lấy cấu hình DHCP diễn ra theo các bước sau:

1. Client phải có cấu hình DHCP khi bắt đầu tiến trình tìm các thành viên trong mạng. Client gửi một yêu cầu cho server để yêu cầu cấu hình IP. Đôi khi client có thể đề nghị trước địa chỉ IP mà nó muốn, ví dụ như khi nó hết thời gian sử dụng địa chỉ IP hiện tại và muốn gia hạn thêm thời gian. Client sẽ xác định được DHCP server bằng cách gửi gói quảng bá gọi là DHCPDISCOVER.
2. Khi server nhận được gói quảng bá, nó sẽ tìm trong cơ sở dữ liệu của nó và quyết định là có trả lời được yêu cầu này không. Nếu server không trả lời yêu cầu thì nó sẽ gửi gói trả lời trực tiếp bằng DHCPOFFER về cho client, trong đó mời client sử dụng cấu hình IP của server. Trong DHCPOFER có

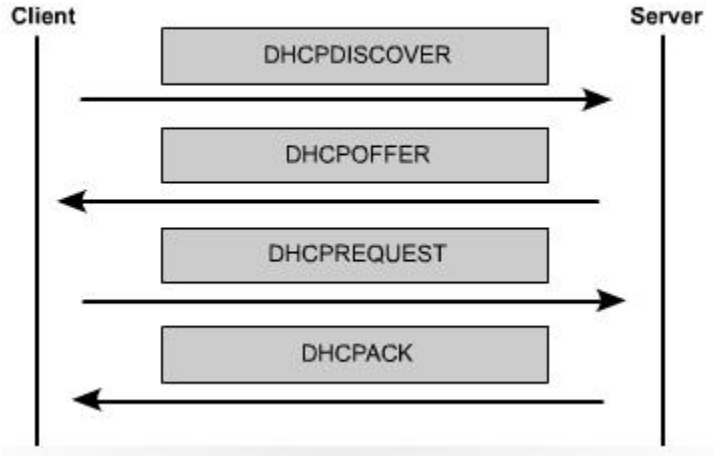
thể có các thôngtin cho client về địa chỉ IP, địa chỉ DNS server và thời gian sử dụng địa chỉ này.

3. Nếu client nhận thấy lời mời của server phù hợp thì nó sẽ gửi quảng bá một DHCPREQUEST để yêu cầu cung cấp những thông cố cụ thể của cấu hình IP. Tại sao lúc này client lại gửi quảng bá mà nó không gửi trực tiếp cho server? Do thông điệp đầu tiên là DHCPDISCOVER đã được gửi quảng bá nên thông điệp này có thể sẽ đến được nhiều server DHCP khác nhau. Khi đó, có thể sẽ có nhiều server cùng mời một client chấp nhận. Thông thường lời mời mà client nhận được đầu tiên sẽ được chấp nhận.
4. Server nào nhận được DHCPREQUEST cho biết client đã chấp nhận sử dụng cấu hình IP mà server đã mời thì server đó sẽ gửi trả lời trực tiếp cho client một gói DHCPACK. Rất hiếm khi nhưng cũng có thể server sẽ không gửi DHCPACK vì có thể cấu hình IP đó đã được cấp cho client khác rồi.
5. Sau khi client nhận được DHCPACK thì có thể bắt đầu sử dụng địa chỉ IP ngay.
6. Nếu client phát hiện rằng địa chỉ IP này đã được sử dụng trong cùng mạng nội bộ với nó thì client sẽ gửi thông điệp DHCPDECLINE và bắt đầu tiến trình DHCP lại từ đầu. Hoặc nếu client nhận được thông điệp DHCPNAK từ server trả lời cho thông điệp DHCPREQUEST thì sau đso client cũng bắt đầu tiến trình lại từ đầu.
7. Nếu client không cần sủ dụng địa chỉ IP này nữa thì client guiử thống điệp DHCPRELEASE cho server.



Hình 1.2.4.a. *Tiến trình hoạt động DHCP*

Tùy theo quy định của mỗi tổ chức, công ty, người quản trị mạng có thể cấp cố định cho một địa chỉ IP nằm trong dải địa chỉ của một DHCP server. Cisco IOS DHCP server luôn luôn phải kiểm tra một địa chỉ IP đã được sử dụng trong mạng hay chưa trước khi mời client sử dụng địa chỉ IP đó. Server sẽ phát một yêu cầu ICMP echo, hay còn gọi là ping, đến các địa chỉ IP nằm trong dải địa chỉ của mình trước khi gửi DHCPOFFER cho client. Số lượng ping mặc định được sủ dụng để kiểm tra một địa chỉ IP là 2 gói và chúng ta có thể cấu hình con số này được.



Hình 1.2.4.b. *Thứ tự các thông điệp DHCP được gửi đi trong tiến trình DHCP.*

1.2.5. Cấu hình DHCP

Tương tự như NAT, DHCP server cũng yêu cầu người quản trị mạng phải khai báo trước dải địa chỉ. Câu lệnh **ip dhcp pool** dùng để khai báo dải địa chỉ mà server có thể cấp pháp cho host.

Câu lệnh đầu tiên, **ip dhcp pool**, tạo dải địa chỉ với một tên cụ thể và đặt router vào chế độ cấu hình DHCP. Trong chế độ cấu hình DHCP, lệnh **network** được dùng để xác định dải địa chỉ được cấp phát. Nếu trong mạng đã có sử dụng cố định một số địa chỉ IP nằm trong dải đã khai báo thì chúng ra quay trở lại chế độ cấu hình toàn cục.

Chúng ra sử dụng lệnh **ip dhcp excluded-address** để cấu hình cho Router loại trừ một số hoặc một dải địa chỉ khi phân phối địa chỉ cho client. Những địa chỉ dành riêng này thường được cấu hình cố định cho những host quan trọng và cho các cổng của Router.

```
Router(config)#ip dhcp excluded-address low-address [high-address]
```

```
Router(config)#ip dhcp excluded-address 172.16.1.1 172.16.1.10
Router(config)#ip dhcp excluded-address 172.16.1.254
```

```
Router(config)#ip dhcp pool subnet12
Router(dhcp-config)#network 172.16.12.0 255.255.255.0
Router(dhcp-config)#default-router 172.16.12.254
Router(dhcp-config)#dns-server 172.16.1.2
Router(dhcp-config)#netbios-name-server 172.16.1.3
Router(dhcp-config)#domain-name foo.com
```

Hình 1.2.5. *Cấu hình ví dụ một DHCP server trên router*

Thông thường, chúng ta còn có thể cấu hình thêm nhiều thông tin khác ngoài thông tin về địa chỉ IP cho một DHCP server. Trong chế độ cấu hình DHCP, chúng ta dùng lệnh **default-router** để khai báo cổng mặc định gateway, lệnh **dns-server** để khai báo địa chỉ của DNS server, lệnh netbios-name-server dùng để khai báo cho WINS server.

Dịch vụ DHCP được chạy mặc định trên các phiên bản Cisco IOS có hỗ trợ dịch vụ này. Để tắt dịch vụ này, chúng ta dùng lệnh **no service dhcp** và dùng lệnh **ip service dhcp** để chạy lại dịch vụ này.

Lệnh	Giải thích
network network-number [mask / /prefix-length]	Khai báo địa chỉ mạng và subnet mask tương ứng cho dải địa chỉ DHCP. Chiều dài bit thuộc phần network có thể được khai báo bằng subnet mask hoặc bằng con số thể hiện số lượng bit, con số này luôn có dấu xổ phải (/) đứng trước.
Default-router Addresss [address2 … Address8]	Khai báo địa chỉ của cổng mặc định gateway cho DHCP client. Mặc dù chỉ cần một địa chỉ những trong cấu lệnh này bạn có thể khai báo tới 8 địa chỉ.
Dns-server Address [address2 … Address8]	Khai báo địa chỉ của DNS server cho DHCP client. Mặc dù chỉ cần một địa chỉ những trong câu lệnh này bạn có thể khai báo tối đa 8 địa chỉ.
Netbios-name- **Server** address [address2…	Khai báo địa chỉ NetBios WINS server cho các Microsoft DHCP client. Mặc dù chỉ cần một địa chỉ những trong câu lệnh này bạn có thể khai báo tới 8 địa chỉ.

Address8]	
Domain-name Name	Khai báo tên miền cho client.
Lease [days [hours} [minutes] / infinite]	Khai báo khoảng thời gian cho phép client được sử dụng một địa chỉ IP. Thời gian mặc định là một ngày.

1.2.6. Kiểm tra hoạt động DHCP

Để kiểm tra hoạt động DHCP, bạn dùng lệnh show ip dhcp binding. Lệnh này sẽ hiển thị danh sách các địa chỉ IP đã được dịch vụ DHCP cấp phát cho các host nào tương ứng.

Để xem các thông điệp DHCP mà router đã gửi đi và nhận vào, chúng ta dùng lệnh show ip dhcp server statistics. Lệnh này sẽ hiển thị các thông tin về số lượng các thông điệp DHCP mà Router đã gửi đi và nhận vào.

```
Router#show ip dhcp binding
```

```
Router#show ip dhcp binding
IP address      Hardware address    Lease expiration       Type
172.16.12.11    0100.10a4.97f4.6d   Mar 02 1993 12:38 AM   Automatic
Router#
```

Hình 1.2.6

1.2.7. Xử lý sự cố DHCP

Để xử lý sự cố của hoạt động DHCP server chúng ta có thể dùng lệnh **debug ig dhcp server events**. Lệnh này sẽ cho biết chu kỳ kiểm tra của server để xem địa chỉ IP nào đã hết thời hạn được sử dụng và tiến trình lấy lại hoặc cấp phát một địa chỉ IP.

```
Router#debug ip dhcp server events
```

```
Router#debug ip dhcp server events
Router#
00:22:53: DHCPD:checking for expired leases.
00:22:23: DHCPD: assigned IP address 172.16.13.11 to client
0100.10a4.97f4.6d
00:22:49: DHCPD:retured 172.16.13.11 to address pool remote.
00:22:59: DHCPD: assigned IP address 172.16.13.11 to client
0100.10a497f4.6d.
```

Hình 1.2.7.

1.2.8. Chuyển tiếp DHCP

DHCP client sử dụng IP quảng bá để tìm DHCP server trong mạng nội bộ. Điều gì sẽ xảy ra khi server và client không nằm trong cùng một mạng và bị ngăn cách nhau bởi Router? Router không hề chuyển tiếp gói quảng bá.

DHCP không phải là một dịch vụ quan trọng duy nhất sử dụng quảng bá Cisco router và các thiết bị khác cũng sử dụng quảng bá để tìm TFTP server. Một số client cần sử dụng quảng bá để tìm TACACS server. TACACS server là một server bảo vệ. Thông thường, trong cấu trúc mạng phân cấp phức tạp, client này phát quảng bá để tim server thì mặc định là router sẽ không chuyển các gói quảng bá ra ngoài subnet của client.

Tuy nhiên có nhiều client sẽ không thể hoạt động được nếu không có những dịc vụ như DHCP chẳng hạn, khi đó phải chon lựa một trong hai giải pháp. Người quả trị mạng có thể đặt server cho mọi subnet trong mạng hoặc là sử dụng đặc tính giúp

đỡ địa chỉ của Cisco IOS. Việc chạy các dịch vụ như DHCP hay DNS trên nhiều máy tính sẽ tạo sự quá tải và khó quản trị nên giải pháp đầu không hiệu quả. Nếu có thể thì người quản trị mạng nên sử dụng giải pháp thứ hai là dùng lệnh **ip helper-address** để chuyển tiếp yêu cầu quảng bá cho những dịch vụ UDP quan trọng này.

Khi sử dụng đặc tính giúp đỡ địa chỉ, router sẽ có thể được cấu hình để tiếp nhận yêu cầu quảng bá của một dịch vụ UDP và sau đó chuyển tiếp yêu cầu đó một cách trực tiếp đến một địa chỉ IP cụ thể. Mặc định, **lệnh ip helper-address** có thể cho phép chuyển tiếp yêu cầu của 8 dịch vụ UDP sau:

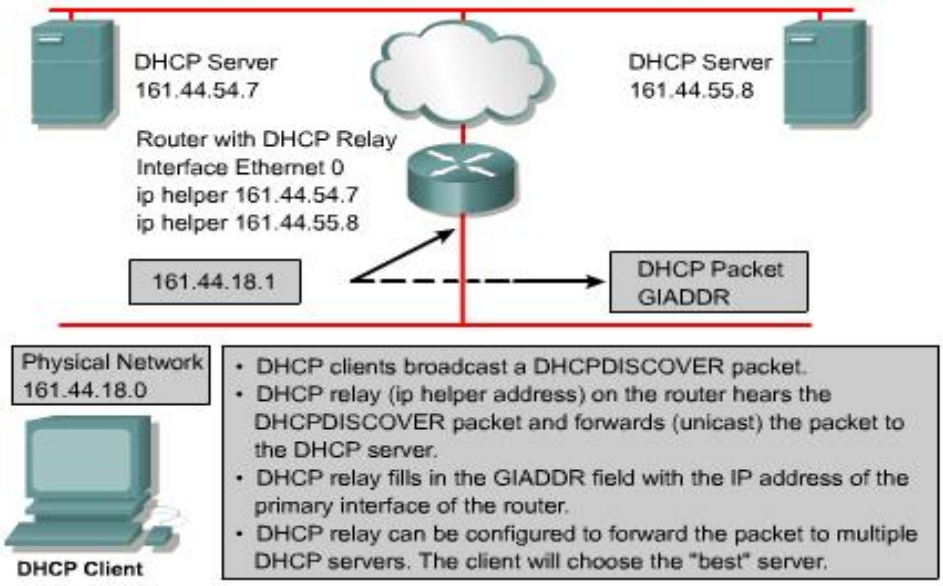
- Time
- TACES
- DNS
- BOOTP/DHCP server
- BOOTP/DHCP client
- TFTP
- Dịch vụ NetBIOS name
- Dịch vụ NetBIOS datagram

Chúng ta xét cụ thể dịch vụ DHCP, client phát quảng bá gói DHCPDISCOVER ra mạng nội bộ của nó. Gói quảng bá này sẽ đến được Gateway chính là router. Nếu trên router có cấu hình lệnh ip helper-address thì gói DHCP này sẽ dược chuyển tiếp cho một địa chỉ IP xác định. Trước khi chuyển tiếp gói yêu cầu này, Router sẽ điền địa chỉ của cổng Router kết nối với client vào phần GIADDR của gói DHCPDISCOVER. Địa chỉ này sẽ là địa chỉ Gateway cho DHCP client sau khi client lấy được địa chỉ IP.

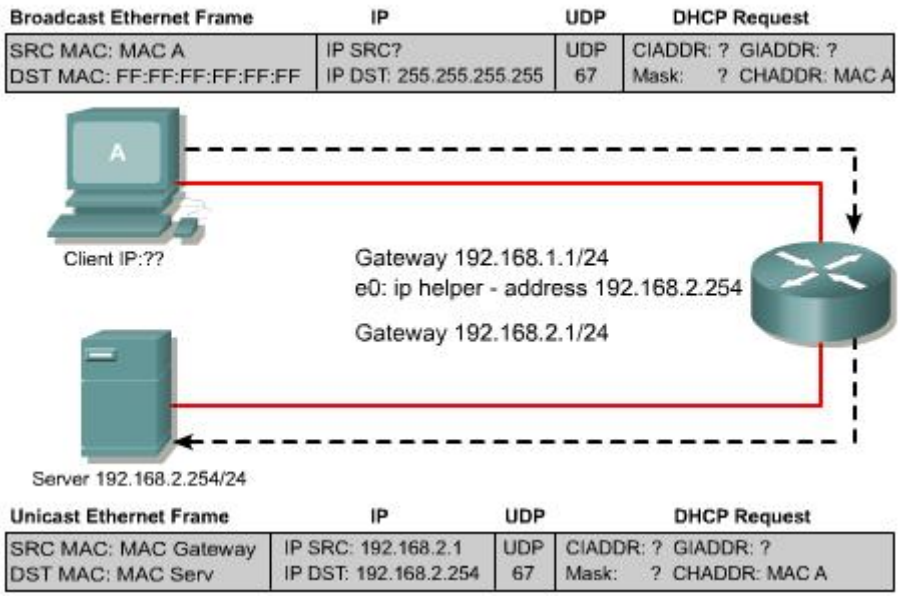
DHCP server nhận được gói DHCPDISCOVER. Đựa vào địa chỉ nằm trong phần GIADDR server sẽ xác định được Gateway này tương ứng với dải địa chỉ nào. Sau đó server sẽ lấy một địa chỉ IP còn trống trong dải để cấp cho client.

OP Code (1)	Hardware Type (1)	Hardware Length (1)	Hops (1)
Transaction ID (XID) - 4 bytes			
Seconds - 2 bytes		Flags - 2 bytes	
Client IP Address (CIADDR) - 4 bytes			
Your IP Address (YIADDR) - 4 bytes			
Server IP Address (SIADDR) - 4 bytes			
Gateway IP Address (GIADDR) - 4 bytes			
Client Hardware Address (CHADDR) - 16 bytes			
Server Name (SNAME) - 64 bytes			
Filename - 128 bytes			
DHCP Options - 312 bytes			

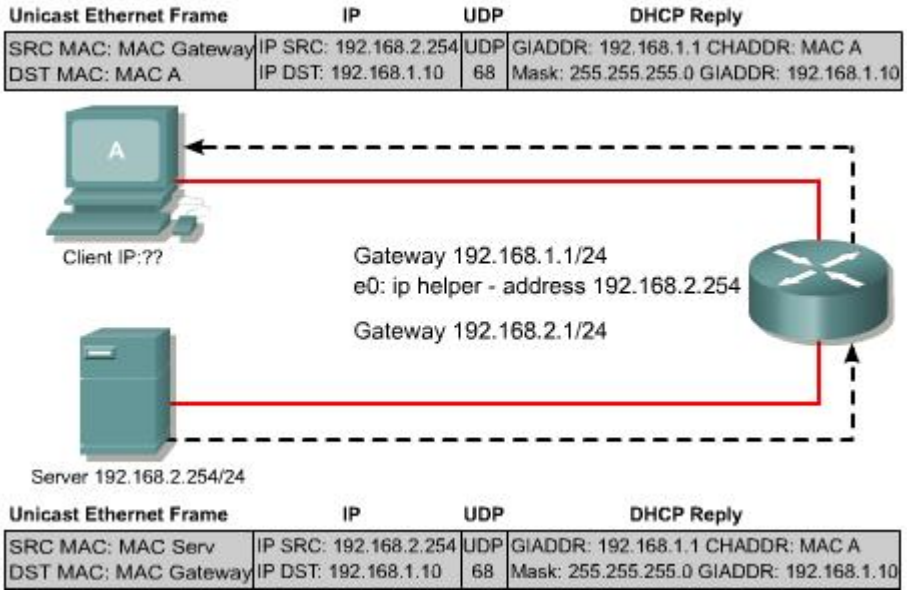
Hình 1.2.8.a. *Cấu trúc gói DHCP*



Hình 1.2.8.b. *Chuyển tiếp DHCP*



Hình 1.2.8.c. *Client A gửi quảng bá DHCPDISCOVER và router chuyển tiếp yêu cầu này cho server DHCP 192.168.2.254. Trước khi chuyển tiếp yêu cầu này router điền địa chỉ của cổng kết nối với client A là 192.168.1.1 vào phần GIADDP của gói DHCPDISCOVER.*



Hình 1.2.8.d. *DHCP server nhận được gói yêu cầu DHCP từ router. Dựa vào địa chỉ 192.168.1.1 trong phần GIADDR, server sẽ xác định được client A nằm trong subnet nào và chọn một địa chỉ IP còn trống trong giải địa chỉ tương ứng để cấp cho client A.. Trong gói trả lời của DHCP server chúng ta thấy client A được cấp địa chỉ 192.168.1.10.*

TỔNG KẾT

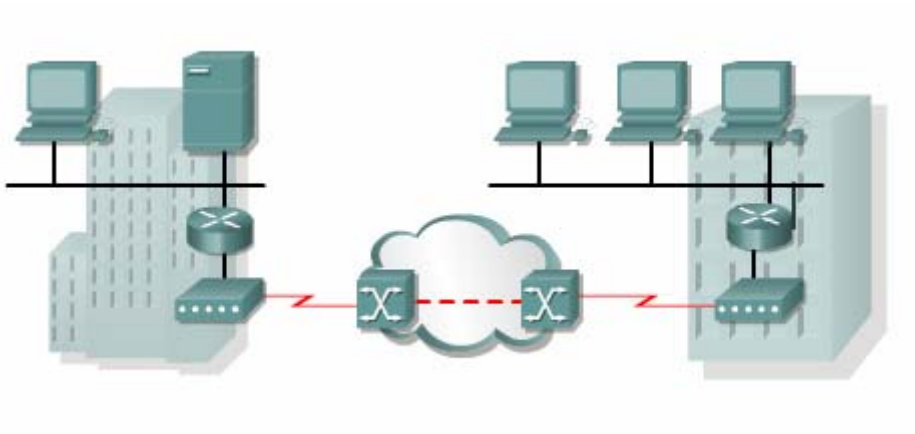
Sau đây là những điểm quan trọng cần nắm trong chương này:

- Địa chỉ riêng được sử dụng cho các mạng riêng, nội bộ và không bao giờ được định tuyến trên các Router Internet công cộng.
- NAT thay đổi phần IP header của gói dữ liệu để chuyển đổi địa chỉ nguồn hoặc đích hoặc cả hai.
- PAT sử dụng một địa chỉ IP công cộng duy nhất cùng với số port để ánh xạ cho nhiều địa chỉ nội bộ bên trong.
- Chuyển đổi NAT có thể được thực hiện cố định hoặc tự động tùy theo mục đích sử dụng.
- NAT và PAT có thể được cấu hình để chuyển đổi cố định, chuyển đổi động và chuyển đổi overloading.
- Lệnh clear và show được sử dụng để kiểm tra hoạt động của NAT và PAT.
- Lệnh debug ip nat được sử dụng để tìm sự cố của cấu hình NAT và PAT.
- Những ưu điểm và nhược điểm của NAT
- DHCP làm việc theo chế độ client-server, cho phép client lấy cấu hình IP từ một DHCP server.
- BOOTP là một phiên bản trước của DHCP và cũng có nhiều đặc điểm hoạt động giống DHCP nhưng BOOTP chỉ cấp phát địa chỉ cố định.
- DHCP server quản lý dải địa chỉ IP và các thông số tương ứng kèm theo. Mỗi một dải địa chỉ tương ứng với một subnet IP.
- DHCP client thực hiện 4 bước để lấy cấu hình IP từ server.
- DHCP server thường được cấu hình để phân phối nhiều địa chỉ IP.
- Lệnh show ip dhcp binding dùng để kiểm tra hoạt động của DHCP.

- Lệnh debug ip dhcp server events được dùng để tìm sự cố của DHCP.
- Khi DHCP server và client không nằm trong cùng một mạng và bị ngăn cách bởi Router, chúng ta dùng lệnh ip helper-address để router chuyển tiếp yêu cầu DHCP.

2.2. Các công nghệ WAN

2.2.1.Kênh quay số (dial-up)



Hình 2.2.1. *Kết nối WAN thông qua modem và mạng điện thoại.*

Modem và đường điện thoại quay số dùng tín hiệu tương tự cung cấp kết nối chuyển mạch, dung lượng thấp, phù hợp cho nhu cầu truyền dữ liệu tốc độ thấp, rẻ tiền.

Điện thoại truyền thống sử dụng cáp đồng kết nối từ máy điện thoại của thuê bao đến tổng đài mạng điện thoại chuyển mạch công cộng (PSTN – Public switched telephone network). Tín hiệu truyền đi trên đường truyền này là tín hiệu tương tự biến đổi liên tục để truyền tiếng nói. Do đó, đường truyền này không phù hợp với tín hiệu số nhị phân của máy tính. Modem tại đầu phát phải thực hiện điều chế tín nhị phân sang tính hiệu tương tự rồi mới đưa tín hiệu xuống đường truyền. Modem tại đầu thu giải điều chế tín hiệu tương tự thành tín hiệu nhị phân như ban đầu.

Đặc điểm vật lý của đường truyền và kết nối PSTN khiến tốc độ của tín hiệu bị hạn chế. Giới hạn trên khoảng 33 kb/giây. Tốc độ này có thể tăng lên khoảng 56 kb/giây nếu tín hiệu được truyền trực tiếp qua một kết nối số.

Đối với nhưng doanh nhiệp nhỏ thì đường truyền này phù hợp vì họ chỉ cần trao đổi các thông tin về bảng lương, giá cả, các báo cáo thông thường và email. Hơn nữa, họ có thể sử dụng cách quay số tự động vào ban đêm hoặc vào ngày nghỉ cuối tuần để truyền tải dữ liệu có dung lượng lớn và lưu dữ liệu dự phòng, vì trong nhưng khoảng thời gian này mức giá cước thấp hơn bình thường. Tổng chi phí cước phụ thuộc và khoảng cách giữa các điểm kết nối, thời gian trễ và thời gian thực hiện cuộc gọi.

Ưu điểm của modem và đường truyền tương tự là thực hiện đơn giản ở mọi nơi, chi phí thấp. Nhược điểm là tốc độ thấp, thời gian thực hiện kết nối lâu, có thời gian trễ và nghẽn mạch, việc truyền thoại và video không được tốt với tốc độ thấp như vậy.

2.2.2. ISDN

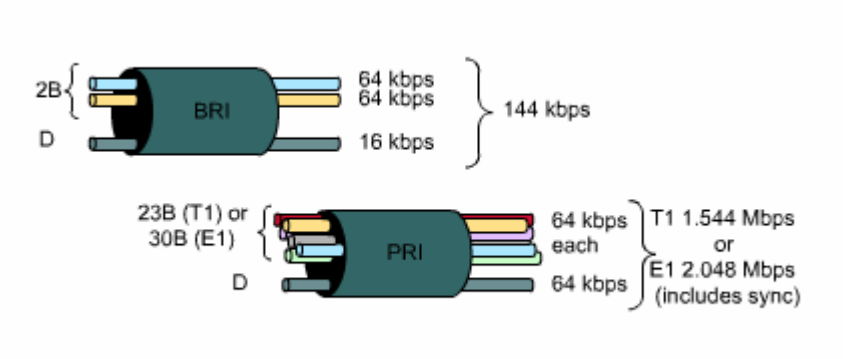
Các đường trung kế của PSTN được thay đổi từ tín hiệu tương tự phân kênh theo tần số sang tín hiệu số phân kênh theo thời gian (TDM). Bước tiếp theo là mạch vọng nội bộ kết nối từ tổng đài đến thuê bao cũng truyền tín hiệu số. Do đó, đường truyền này có dung lượng cao hơn.

ISDN (Integrated Services Digital Network) là kết nối số TDM. Kết nối này sử dụng các kênh B (Bearer) 64 Kb/giây để truyền thoại hoặc dữ liệu và một kênh báo hiệu D (Delta) dùng để thiết lập cuộc gọi và nhiều mục đích khác.

Giao tiếp tốc độ cơ bản BRI ISDN cung cấp hai kênh B 64 Kb/giây và một kênh D 16 Kb/giây phù hợp cho cá nhân, gia đình và các công ty nhỏ. Nếu nhu cầu lớn hơn nữa thì chúng ta có giao tiếp PRI ISDN. PRI cung cấp 23 kênh B 64 Kb/giây và một kenh Điểm 64 Kb/giây ở Bắc Mỹ, tổng tốc độ bit lên tới 1.544 Mb/giây. Ở Châu Âu, Australia và nhiều nơi khác trên thế giới, ISDN PRI cung cấp 30 kênh B và một kênh D, tổng tốc độ bit lên tới 2,048 Mb/giây. Kết nối T1 có tốc độ PRI ở Bắc Mỹ, kết nối E1 có tốc độ PRI quốc tế.

Kênh Điểm BRI không được tận dụng hết khả năng vì nó chỉ được sử dụng để điều khiển cho 2 kênh B. Một số nhà cung cấp dịch vụ cho phép kênk D truyền dữ liệu ở tốc độ thấp, ví dụ như kết nối X.25 với tốc độ 9,6 kb/giây.

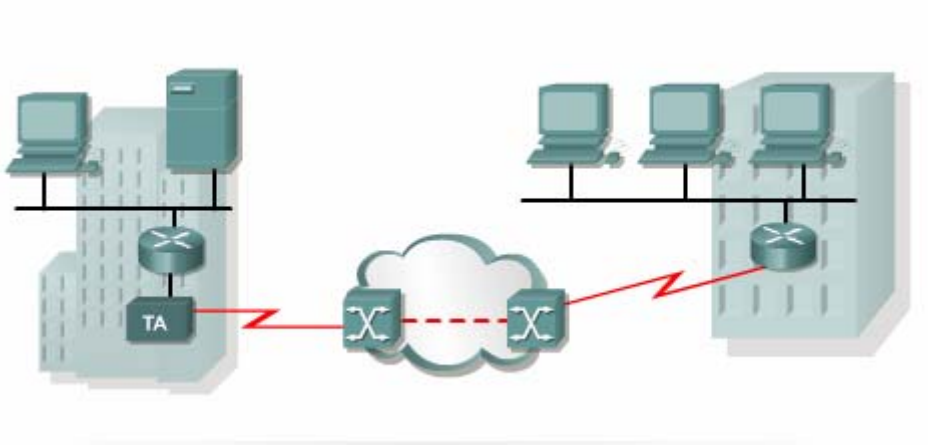
Đối với mạng WAN nhỏ thì kết nối BRI ISDN là một kết nối lý tưởng . BRI có thời gian thiết lập cuộc gọi nhỏ hơn một giây, kênh B 64 kb/giây cung cấy dung lượng lớn hơn một kết nối tương tự với modem. Nếu nhu cầu dung lương cao hơn thì kênh B thứ 2 sẽ được kích hoạt để cung cấp tốc độ 128 kb/giây. Mặc dù như vậy vẫn chưa phù hợp cho truyền video nhưng cũng đã cho phép thực hiện cùng lúc nhiều cuộc đối thoại cùng với các luồng lưu lượng khác.



Hình 2.2.a. *ISDN*

Một ứng dụng thông thường của ISDN là cung cấp thêm dung lượng truyền cho đường truyền thuê riêng. Đường truyền thuê riêng được sử dụng chính, trong những thời điểm nhu cầu dung lượng tăng cao thì ISDN được kích hoạt để hỗ trợ thêm. Ngoài ra, ISDN còn được sử dụng làm đường truyền dự phòng trong trường hợp đường truyền thuê riêng gặp sự cố. Chi phí cước của ISDN được tính trên từng kênh B và cũng tương tự như kết nối thoại quay số.

Với PRI ISDN, ta có thể kết nối hai điểm với nhau bằng nhiều kênh B. Do đó, ta có thể thực hiện được hội nghị truyền hình (video conference), kết nối dữ liệu tốc độ cao, không có thời gian trễ và nghẽn mạch, nhưng chi phí sẽ cao khi khoảng cách giữa các điểm khá lớn



Hình 2.2.2.b. *Cấu trúc chung của mạng WAN với ISDN, Router cần phải có cổng giao tiếp ISDN hoặc phải kết nối thông qua bộ chuyển đổi giao tiếp.*

2.2.3.Đường truyền thuê riêng (leased line)

Khi cần phải có một kết nối dành riêng cố định thì sử dụng đường truyền thuê riêng với dung lượng có thể lên tới 2,5 Gb/giây.

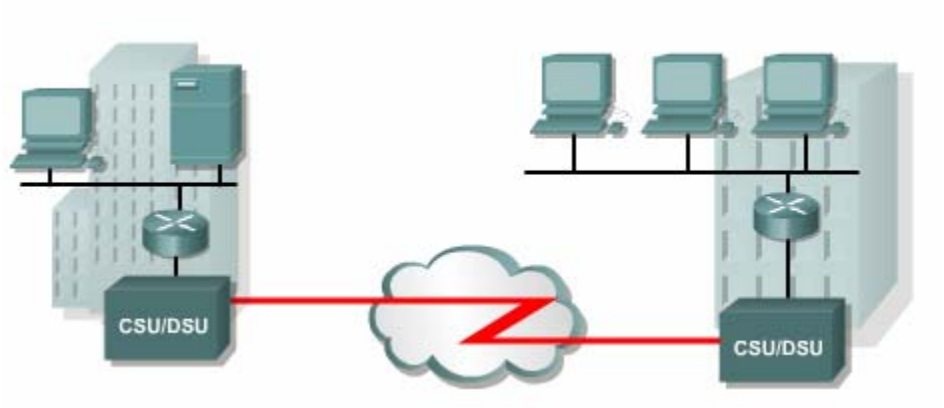
Loại	Chuẩn	Dung lượng
56	DS0	56 Kbps
64	DS0	64 Kbps
T1	DS1	1.544 Mbps
E1	ZM	2.048 Mbps
E3	M3	34.064 Mbps
J1	Y1	2.048 Mbps
T3	DS3	44.736 Mbps
OC-1	SONET	51.84 Mbps
OC-3	SONET	155.54 Mbps
OC-9	SONET	466.56 Mbps
OC-12	SONET	622.08 Mbps
OC-18	SONET	933.12 Mbps
OC-24	SONET	1244.16 Mbps
OC-36	SONET	1866.24 Mbps
OC-48	SONET	2488.32 Mbps

Hình 2.2.3.a. *Các đường truyền WAN và băng thông tương ứng.*

Một kết nối điểm-đến-điểm thiết lập một đường truyền WAN từ vị trí của thuê bao thông qua mạng của nhà cung cấp dịch vụ đến điểm đích. Đườn truyền điểm-đến-điểm này thườn được thuê từ nhà cung cấp dịch vụ nên được gọi là đường truyền thuê riêng. Đường truyền thuê riêng có thể được cung cấp với nhiều mức dung

lượng khác nhau. Giá cả phụ thuộc vào mức băng thông yêu cầu và khoảng cách giữa hai điểm kết nối. Đương nhiên, giá thuê một đường truyền riêng điểm-đến-điểm sẽ cao hơn nhiều so với các đường chia sẻ khác như Frame Relay. Đôi khi chi phí cho đường thuê riêng quá cao so với nhu cầu mà ta sử dụng được. Chi phí này sẽ hiệu quả hơn nếu các kết nối này được sử dụng để nối nhiều vị trí trung tâm. Dung lượng cố định có ưu điểm là không có thời gian trễ và nghẽn mạch giữa hai điểm cuối, phù hợp cho nhiều ứng dụng như thương mại điện tử.

Để thực hiện kết nối thuê riêng ta cần phải có CSU/DSU và đường truyền từ nhà cung cấp dịch vụ, router phải có cổng Serial, mỗi cổng tương ứng với một kết nối.



Hình 2.3.b. *Mạng WAN với đường truyền thuê riêng.*

Đường kết nối trực tiếp thường được sử dụng để kết nối giữa các toà nhà, cung cấp dung lượng truyền cố định. Đường truyền thuê riêng là một chọn lựa truyền thống từ trước tới nay, tuy nhiên nó cũng có nhiều nhược điểm. Lưu lượng WAN luôn biến đổi nhưng dung lượng đường truyền cố định. Do đó, băng thông đường truyền ít khi nào bằng với lưu lượng thực tế. Mỗi router tại mỗi điểm cuối cần phải có một

cổng Serial cho một kết nối, do đó chi phí cho thiết bị sẽ tăng thêm. Mỗi lần muốn thay đổi dung lượng đường truyền ta cần phải liên hệ với nhà cung cấp dịch vụ.

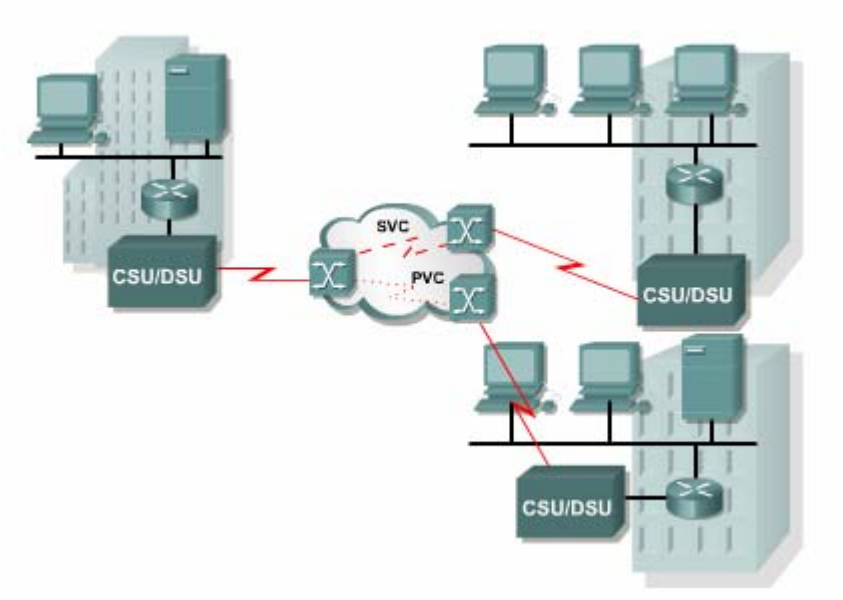
Đường truyền thuê riêng cung cấp kết nối trực tiếp điểm-đến-điểm giữa các LAN và kết nối nhiều chi nhánh riêng lẻ vào mạng chuyển mạch gói.

2.2.4.X.25

Do đường truyền thuê riêng có chi phí cao nên các nhà cung cấp dịch vụ đã giới thiệu mạng chuyển mạch gói sử dụng đường truyền chia sẻ để giảm bớt chi phí. Mạng chuyển mạch gói đầu tiên là mạng X.25. X.25 cung cấp tốc độ bit thấp, dung lượng chia sẻ qua dịch vụ chuyển mạch hoặc cố định.

X.25 là một giao thức lớp Mạng và các thuê bao được cung cấp một địa chỉ mạng. Khi có yêu cầu từ một tập hợp các địa chỉ, mạch ảo SVC sẽ được thiết lập, mỗi SVC được phân biệt bằng một địa chỉ số kênh. Các gói dữ liệu được dán nhãn theo chỉ số kênh này, dựa vào đó các gói dữ liệu được truyền đến đúng địa chỉ mạng đích. Trên một kết nối vật lý có thể thiết lập nhiều kênh truyền.

Thuê bao có thể kết nối vào mạng X.25 bằng kết nối thuê riêng hoặc bằng kết nối quay số. Mạng X.25 cũng có thể cung cấp kênh truyền cố định PVC cho các thuê bao.



Hình 2.2.4. *Mạng X25*

X.25 có chi phí thấp và hiệu quả vì chi phí cước được tính theo lưu lượng dữ liệu chứ không tính theo thời gian kết nối và khoảng cách của kết nối. Dữ liệu được truyền đi với bất kỳ tốc độ nào lên tới mức độ tối đa của đường truyền. Nhưng mạng X.25 thường có dung lượng thấp, tối đa là 48 Kb/giây. Ngoài ra thời gian truyền gói dữ liệu cũng bị trễ do đặc trưng của mạng chia sẻ.

Công nghệ X.25 từ lâu đã không còn được sử dụng rộng rãi. Frame Relay đã thay thế cho X.25

Ứng dụng thường thấy của X.25 là trên các máy đọc thẻ tín dụng. Tại các trung tâm thương mại, siêu thị, khi khach hàng sử dụng thẻ để thanh toán thì các máy đọc thẻ sẽ sử dụng X.25 để liên hệ với máy tính trung tâm xác định giá trị của thẻ, thực hiện giao dịch thanh toán. Một số công ty còn sử dụng X.25 trên mạng VAN (Value-add network). VAN là một mạng riêng được các công ty thuê từ nhà cung cấp dịch vụ để thực hiện trao đổi dữ liệu về tài chính và nhiều thông tin thương mại

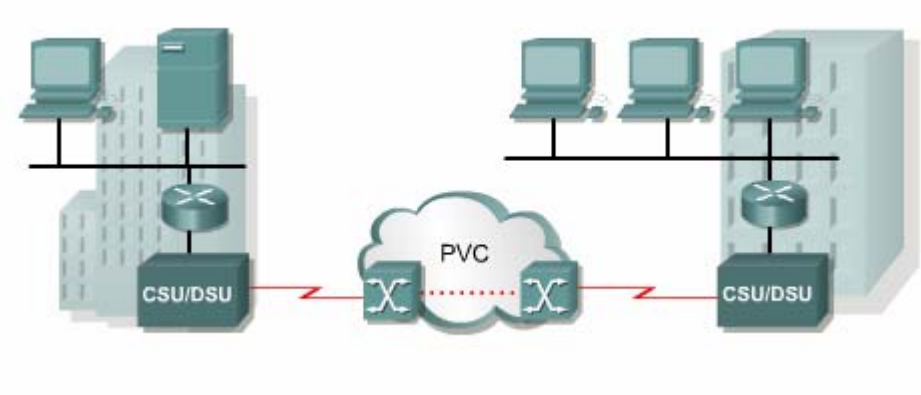
khác. Đối với những ứng dụng này, băng thông thấp và thời gian trễ cao không phải là vấn đề lớn, trong khi đó chi phí thấp lại là một ưu điểm của X.25.

2.2.5. Frame Relay.

Do nhu cầu băng thông ngày càng cao và yêu cầu thời gian chuyển mạch gói nhanh hơn, nhà cung cấp dịch vụ đã giới thiệu Frame Relay, Frame Relay cũng hoạt động như X.25 nhưng có tốc độ cao hơn, lên đến 4 Mb/giây hoặc hơn nữa.

Frame Relay có một số đặc điểm khác với X.25. Trong đó, điểm khác biệt quan trọng nhất là: Frame Relay là giao thức đơn giản hơn, hoạt động ở lớp liên kết dữ liệu thay vì ở lớp Mạng.

Frame Relay không thực hiện điều khiển luồng và kiểm tra lỗi. Do đó, thời gian trễ do chuyển mạch frame giảm đi.



Hình 2.2.5. *Mạng Frame Relay*

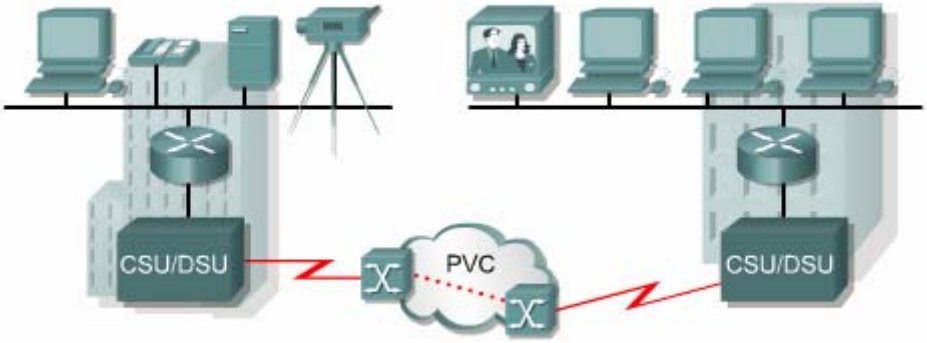
Hầu hết các kết nối Frame Relay đều là kết nối PVC, chứ không phải là SVC. Kết nối từ mạng của khách hàng vào mạng của nhà cung cấp dịch vụ thường là kết nối thuê riêng hoặc cũng có thể là kết nối quay số nếu nhà cung cấp dịch vụ có sử dụng đường ISDN, Kênh D ISDN được sử dụng để thiết lập kết nối SVC trên một hay

nhiều kênh B. Giá cước Frame Relay được tính theo dung lượng kết nối và dung lượng thoả thuận trên các PVC>

Frame Relay cung cấp kết nối chia sẻ có băng thông truyền cố định, có thể truyền được cả tiếng nói. Frame Relay là một chọn lựa lý tưởng cho kết nối giữa các LAN. Router trong LAN chỉ cần một cổng vật lý, trên đó cầu hình nhiều kết nối ảo VC. Kết nối thuê riêng để kết nối vào mạng Frame Relay khá ngắn nên chi phí cũng tương đối hiệu quả khi nối giữa các LAN.

2.2.6. ATM

Các nhà cung cấp dịch vụ đã nhìn thấy nhu cầu cần phải có công nghệ cung cấp mạng chi sẻ cố định với thời gian trễ thấp, ít nghẽn mạch và băng thông cao. Giải pháp của họ chính là ATM (Asychronous Transfer Mode) với tốc độ 155 Mb/giây. So với các công nghệ chia sẻ khác như X.25, Frame Relay thì sơ đồ mạng WAN ATM cũng tương tự.



Hình 2.2.6. *ATM.*

ATM là một công nghệ có khả năng truyền thoại, video và dữ liệu thông qua mạng riêng và mạng công cộng. ATM được xây dựng dựa trên cấu trúc tế bào (cell) chứ không dựa trên cấu trúc frame. Gói dữ liệu được truyền đi trên mạng ATM không được gọi là frame mà gọi là tế bào (cell). Mỗi tế bào ATM luôn có chiều dài cố định là 53 byte. Tế bào ATM 53 byte này chứa 5 byte phần ATM header, tiếp theo

sau là 48 byte của phần dữ liệu. Tất cả các tế bào ATM đều có kích thước nhỏ, cố định như nhau. Do đó, không có các gói dữ liệu khác lơn hơn trên đường truyền, mọi tế bào đều không phải chờ lâu. Thời gian truyền của mỗi gói là như nhau. Do đó, các gói đến đích cách nhau đều đặn, không có gói nào đến quá chậm so với gói trước. Cơ chế này rất phù hợp cho truyền thoại và video vì những tín hiệu này vốn rất nhạy cảm với vấn đề thời gian trễ.

So với các frame lơn hơn của Frame Relay và X.25 thì tế bào ATM 53 byte không được hiệu quả bằng. Khi có một packet lớn của lớp Mạng cần phải phân đoạn nhỏ hơn thì cữ mỗi 48 byte phải có 5 byte cho phần ATM header. Công việc ráp các phân đoạn lại thành packet ban đầu ở ATM switch đầu thu sẽ phức tạp hơn. Hơn nữa, việc đóng gói như vậy làm cho đường truyền ATM phải tốn nhiều hơn 20% băng thông so với Frame Relay để truyền cùng một lượng dữ liệu lớp Mạng.

ATM cung cấp cả kết nối PVC và SVC mặc dù PVC được sử dụng nhiều hơn trong WAN. Cũng như các công nghệ chia sẻ khác, ATM cho phép thiết lập kết nối ảo trên một kết nối vật lí.

2.2.7. DSL

Digital Subscriber Line – DSL là một công nghệ truyền băng rộng sử dụng đường truyền hai dây xoắn của hệ thống điện thoại để truyền dữ liệu với băng thông lớn đến thuê bao dùng dịch vụ. Kỹ thuật truyền băng rộng ghép nhiều dải tần số khác nhau trên cùng một đường truyền vật lý để truyền dữ liệu xDSL bao gồm các công nghệ DSL như sau:

Asymmetric DSL (ADSL)

Symmetric DSL (SDSL)

High Bit Rate DSL (HDSL)

ISDN DSL (IDSL)

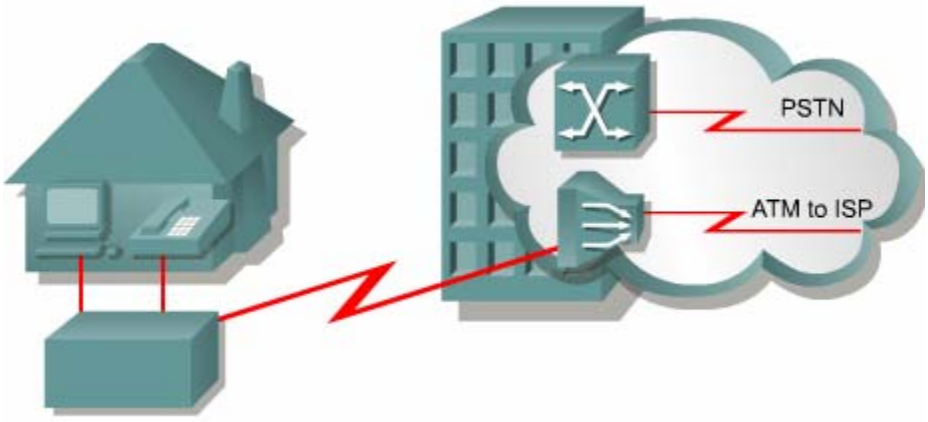
Consumer DSL (CDSL), cũng được gọi là DSL-lite hay G.lite

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

Hình 2.2.7.a.

Với công nghệ DSL, các nhà cung cấp dịch vụ có thể cung cấp cho khách hàng dịch vụ mạng tốc độ cao trên đường dây thoại cáp đồng. Công nghệ DSL cho phép đường dây này thực hiện song song đồng thời chức năng của một kết nối điện thoại và một kết nối mạng thường trực cố định. Nhiều kết nối của thuê bao DSL được ghép kênh vào một đường kết nối có dung lượng cao tại trung tâm cung cấp dịch vụ thông qua thiết bị ghép kênh truy cập DSL (DSLAM – DSL Access Multiplexer). Nhiều kết nối DSL của thuê bao được DSLAM tích hợp vào một kết nối T3/DS3 duy nhất. Các công nghệ DSL hiện nay sử dụng nhiều kỹ thuật mã hoá và điều chế phức tạp để đạt được tốc độ dữ liệu lên đến 8,192 Mb/giây.

Kênh truyền thoại chuẩn trên đường dây điện thoại nằm trong dải tần 300 Hz đến 3,3 KHz. Như vậy, dải tần số 4 KHz được dành để truyền thoại trên đường dây điện thoại. Công nghệ DSL sử dụng dải tần cao hơn 4 KHz để truyền tải dữ liệu. Bằng cách này thoại và dữ liệu có thể được truyền tải song song đồng thời trên cùng một đường truyền.



Hình 2.2.7.b. *Mạch vòng nội bộ của hệ thống điện thoại kết nối modem DSL của từng thuê bao đến DSLAM đặt tại trung tâm cung cấp dịch vụ. Thoại và dữ liệu sử dụng hai dải tần số riêng biệt.*

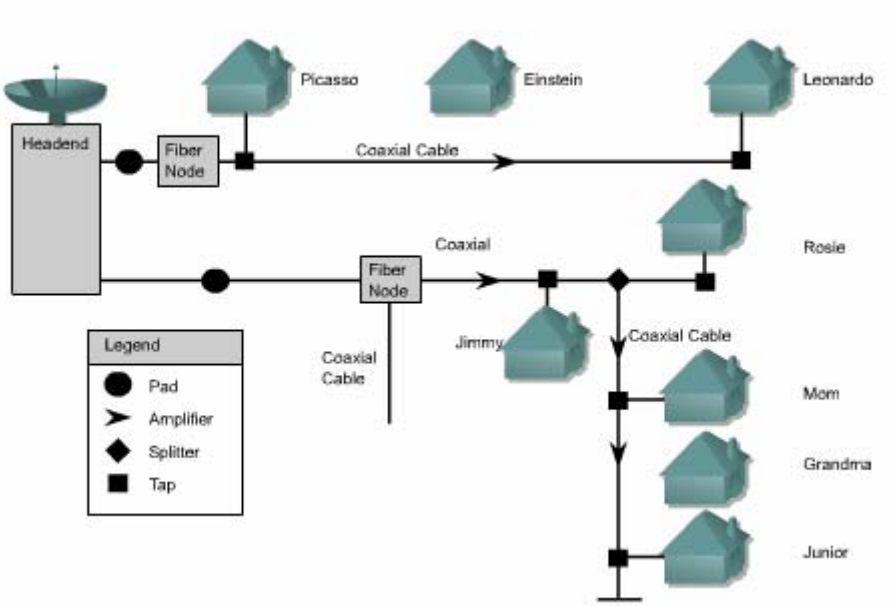
Có 2 loại công nghệ DSL cơ bản là ADSL (Asymmetric DSL – DSL bất đối xứng) và SDSL (Symmetric DSL – DSL đối xứng). Dịch vụ bất đối xứng cung cấp kênh tải dữ liệu (download) lớn hơn kênh truyền dữ liệu (upload). Dịch vụ đối xứng cung cấp cả hai kênh truyền này có dung lượng như nhau.

Không phải tất cả các công nghệ DSL đều cho phép sử dụng đường dây điện thoại. Ví dụ SDSL không cung cấp dịch vụ điện thoại trên cùng một đường truyền. Do đó phải có riêng một đường truyền cho SDSL.

Các loại DSL khác nhau cung cấp băng thông khác nhau với dung lượng có thể vượt qua đường thuê riêng T1 hoặc E1. Tốc độ truyền phụ thuộc vào chiều dài thực tế của mạch vòng nội bộ, loại cáp và điều kiện đi dây cáp. Để dịch vụ được cung cấp tốt thì mạch vòng nội bộ nên ngắn hơn 5,5 km. DSL thường không được chọn làm kết nối giữa nhà riêng và hệ thống mạng trong công ty vì thuê bao không thể từ nhà riêng kết nối trực tiếp vào mạng trung tâm của công ty, mà phải thông qua một nhà cung cấp dịch vụ Internet (ISP – Internet Service Provider). Từ đây, một kết nối IP mới được thực hiện thông qua Internet để đến mạng trung tâm của công ty. Như vậy rất nguy hiêm về mặt bảo mật. Để đảm bảo tính an toàn, dịch vụ DSL có cung cấp khả năng sử dụng mạng riêng ảo VPN (Virtual Private Network) để kết nối vào server VPN đặt tại công ty.

2.2.8. Cable modem

Cáp đồng trục được sử dụng rộng rãi trong các thành phố để truyền tín hiệu truyền hình. Hệ thống mạng được xây dựng dựa trên hệ thống cáp đồng trục này có băng thông cao hơn so với hệ thống mạng trên cáp đồng điện thoại.



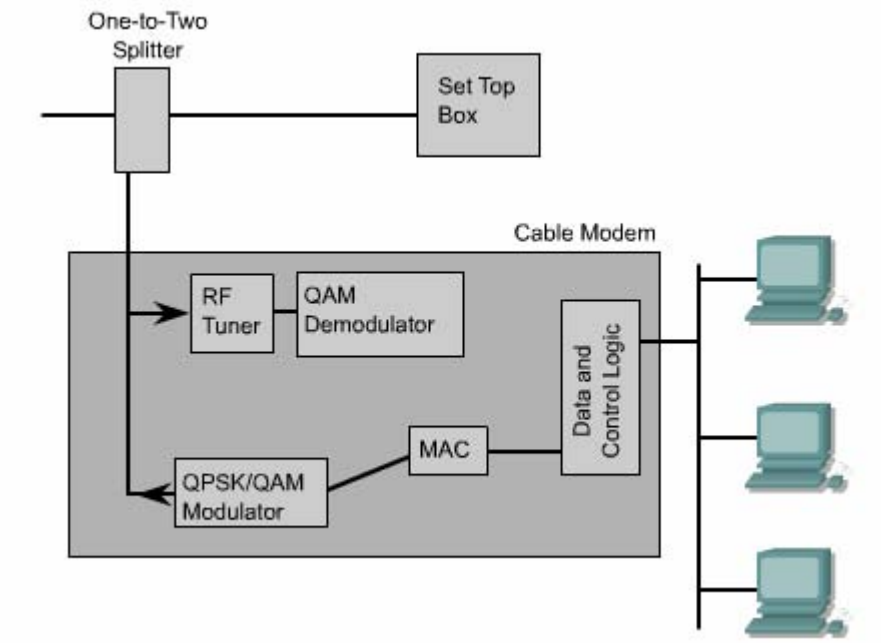
Hình 2.2.8.a. *Cable modem*

Cable modem thực hiện truyền dữ liệu hai chiều tốc độ cao, sử dụng cáp đồng trục trong hệ thống mạng cáp truyền hình. Một số nhà cung cấp dịch vụ còn cam kết tốc độ truyền dữ liệu cao gấp 6,5 lần đường thuê riêng T1. Tốc độ này cho phép truyền được nhanh chóng một lượng lớn thông tin số bao gồm video clip, audio… Lượng thông tin cần phải mất 2 phút nếu tải bằng đường truyền ISDN BRI thì bây giờ chỉ mất 2 giây thông qua kết nối cable modem.

Cable modem cũng cung cấp kết nối thường trực và lắp đặt kết nối này đơn giản. Một kết nối thường trực cũng có nghĩa là máy tính luôn luôn đứng trước mối nguy hiểm về mặt bảo mật, do đó cần phải được bảo vệ bằng bức tường lửa (firewalls). Để đảm bảo về mặt an toàn, dịch vụ cable modem cũng cho phép sử dụng mạng riêng ảo VPN để kết nối vào VPN server đặt tại mạng trung tâm của một công ty.

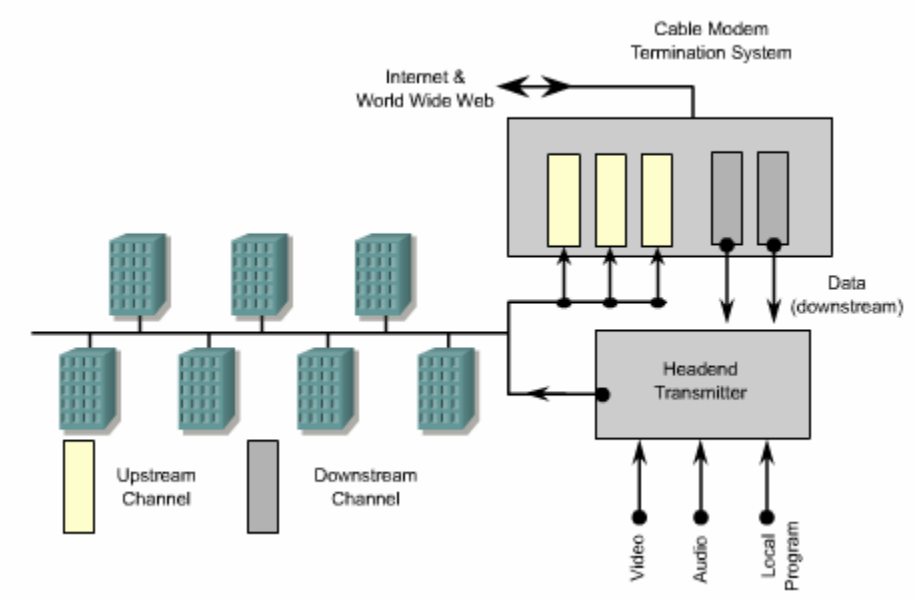
Một kết nối cable modem có dung lượng có thể lên đến 30 – 40 Mb/giây trên kênh truyền 6 MHz. Đường truyền này nhanh gần gấp 500 lần so với đường truyền modem thường (56 Kb/giây).

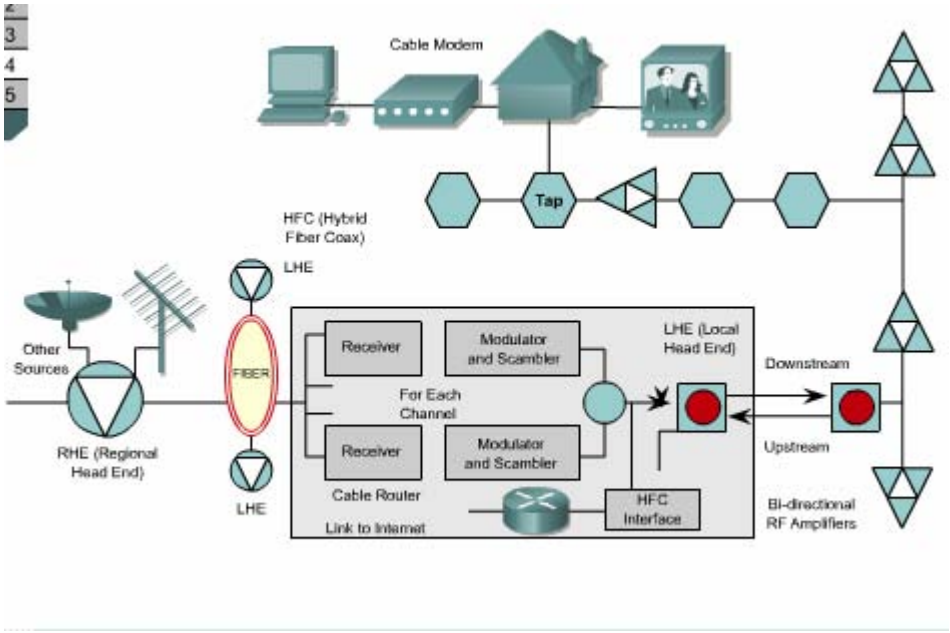
Với cable modem, thuê bao vẫn có thể nhận song song đồng thời dịch vụ truyền hình cáp và dữ liệu cho máy tính thông qua một bộ phân giải 1-2 đơn giản.

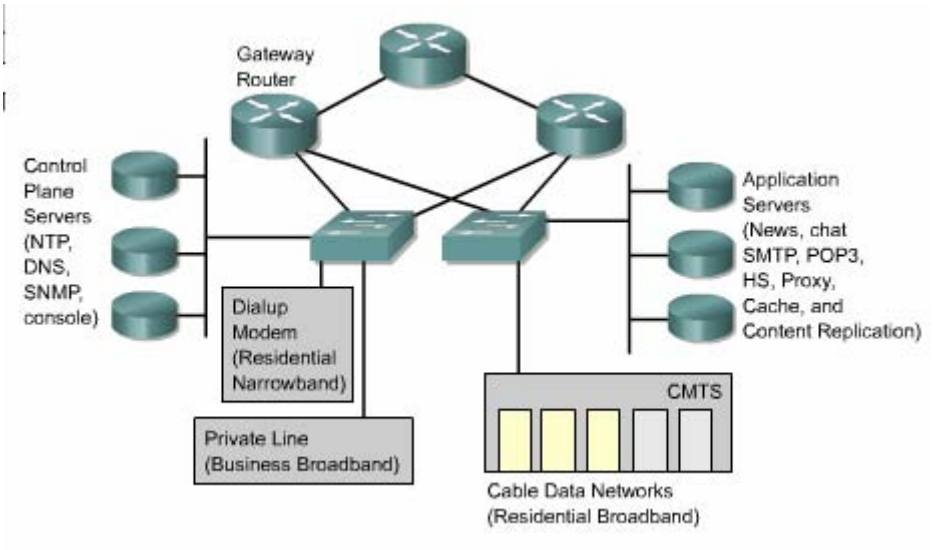


Hình 2.2.8.b. *Cấu trúc bộ phân giải 1-2.*

Thuê bao cable modem phải sử dụng ISP liên kết với nhà cung cấp dịch vụ truyền hình cáp. Tất cả các thuê bao nội bộ đều chia sẻ cùng một băng thông cáp. Do đó càng nhiều người tham gia vào dịch vụ thì lượng băng thông cho mỗi người sẽ giảm xuống.


Cable Modem
Termination System
Internet &
World Wide Web
Data
(downstream)
Headend
Transmitter
Upstream
Channel
Downstream
Channel
Video
Audio
Local
Program


Cable Modem
Tap
HFC (Hybrid
Fiber Coax)
LHE
Other
Sources
FIBER
Receiver
Modulator
and Scambler
LHE (Local
Head End)
Downstream
For Each
Channel
Receiver
Modulator
and Scambler
Upstream
RHE (Regional
Head End)
Cable Router
HFC
Interface
LHE
Link to Internet
Bi-directional
RF Amplifiers



Hình 2.2.8.c. *Cấu trúc mạng cable modem*.

2.3. Thiết kế WAN

2.3.1. Thông tin liên lạc bằng WAN

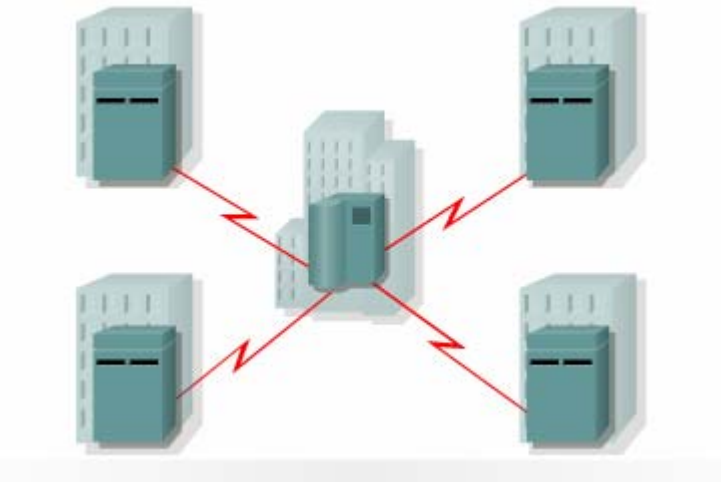
WAN là một tập hợp các đường liên kết dữ liệu kết nối các router trong các LAN khác nhau.

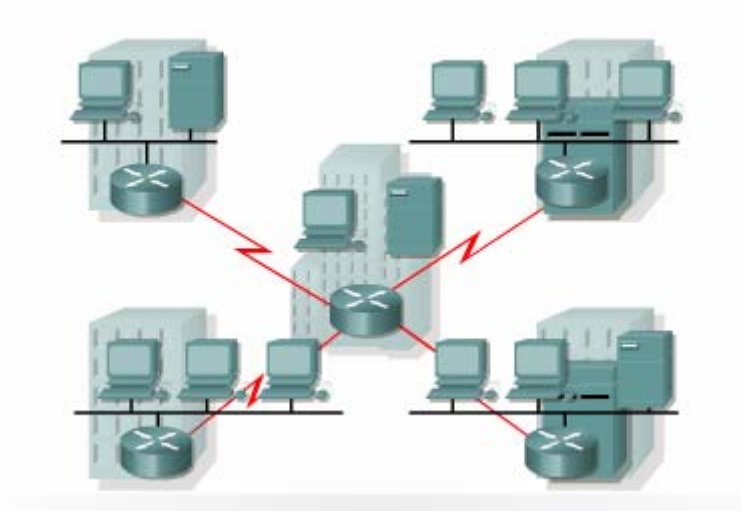
Vì lý do chi phí và pháp định nên chỉ có các nhà cung cấp dịch vụ thông tin liên lạc - viễn thông mới sở hữu các đường truyền dữ liệu của WAN. Khách hàng thuê các đường liên kết này để kết nối các mạng LAN của mình hoặc kết nối đến các mạng ở xa. Tốc độ truyền dữ liệu trong WAN thường thấp hơn tốc độ 100 Mb/giây trong LAN. Chi phí thuê bao đường truyền là chi phí lớn nhất cho một mạng WAN. Do đó, việc thiết kế WAN phải đảm bảo cung cấp băng thông lớn nhất trong khả năng chi trả chấp nhận được. Đối với người sử dụng, việc cân đối giữa chi phí và nhu cầu dịch vụ tốc độ cao là một điều không dễ dàng.

WAN truyền tải rất nhiều loại lưu lượng khác nhau như dữ liệu, thoại và video. Do đó thiết kế được đưa ra phải cung cấp đủ dung lượng, thời gian truyền đáp ứng được với yêu cầu của toàn bộ hệ thống. Ngoài ra, người thiết kế còn phải quan tâm đến cấu trúc của mạng nối giữa các trung tâm với nhau, về đặc tính tự nhiên, về băng thông và khả năng của các kết nối này.

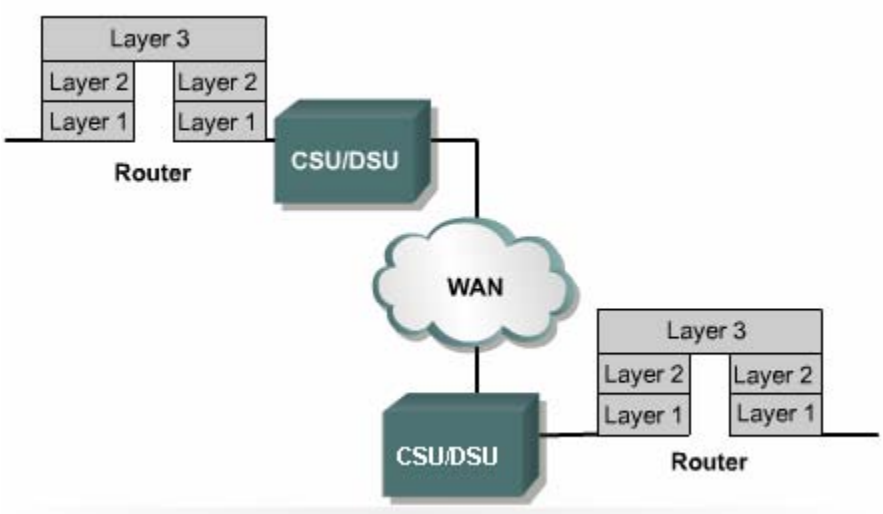
Mạng WAN cũ trước đây thường bao gồm các đường kết nối giữa các máy tính lớn (mainframe) ở cách xa nhau. Mạng WAN ngày nay kết nối các LAN ở xa lại với nhau. Tất cả các máy tính đầu cuối, server và router nằm trong cùng một phạm vi được kết nối với nhau thông qua LAN và WAN kết nối các router của từng LAN lại với nhau. Thông qua sự trao đổi thông tin địa chỉ lớp 3 router có thể định tuyến cho mọi luồng dữ liệu. Ngoài ra, router còn cung cấp chế độ quản lý chất lượng dịch vụ (QoS) cho phép định tuyến và chuyển mạch các luồng dữ liệu khác nhau với các mức ưu tiên khác nhau.

WAN thường chỉ là tập hợp các kết nối giữa các router để liên kết các LAN với nhau, do đó không có dịch vụ nào thực hiện trên WAN. WAN hoạt động ở 3 lớp dưới của mô hình OSI. Router quyết định chọn đường đến đích cho dữ liệu từ thông tin lớp Mạng nằm trong gói dữ liệu rồi sau đó chuyển gói dữ liệu xuống kết nối vật lý tương ứng.





Hình 2.3.1.a. *Mạng WAN trước đây và hiện nay.*



Hình 2.3.1.b. *Các công nghệ WAN hoạt động ở 3 lớp dưới của mô hình OSI.*

2.3.2. Các bước trong thiết kế WAN

Thiết kế WAN là một công việc đầy thử thách, nhưng nếu thiết kế theo một cách có hệ thống thì chúng ta sẽ xây dựng được một mạng WAN có hiệu suất hoạt động cao với chi phí thấp. Mỗi khi cần thay đổi một mạng WAN đã có sẵn thì chũng ta nên đi theo các bước được đề nghị dưới đây trong phần này.

Chúng ta thường phải thay đổi mạng WAN mỗi khi cần mở rộng server WAN, công việc kinh doanh thực tế có sự thay đổi…

Các công ty lắp đặt mạng WAN để thực hiện trao đổi dữ liệu giữa các chi nhánh. Mạng WAN này phục vụ cho toàn bộ hệ thống mạng của công ty. Chi phí bao gồm nhiều phần, ví dụ trong đó có chi phí cho thiết bị và cho việc quản lý đường truyền.

Trong thiết kế WAN, chúng ta cần biết trong mạng WAN đó truyền những loại lưu lượng nào, từ đâu đến đâu. WAN có thể truyền tải nhiều loại dữ liệu khác nhau với yêu cầu băng thông, độ trễ và nghẽ mạch khác nhau.

Traffic	Latency	Jitter	Bandwidth
Voice	Low	Low	Medium
Transaction data (for example, SNA)	Medium	Medium	Medium
Messaging (e-mail)	High	High	High
File transfer	High	High	High
Batch data	High	High	High
Network management	High	High	Low
Videoconferencing	Low	Low	High

Hình 2.3.2.a. *So sánh giữa các loại lưu lượng trong WAN.*

Chúng ta càn biết thông tin về các đặc điểm của mỗi loại lưu lượng trên mỗi hướng. Quyết định về những đặc điểm này tuỳ thuộc vào sự sử dụng của user. Việc thiết kế WAN thường là nâng cấp, mở rộng hoặc thay đổi một mạng WAN đã có sẵn. Do đó, có rất nhiều dữ liệu mà chúng ta cần đã có trong hồ sơ quản lý của mạng cũ.

Các đặc điểm của lưu lượng mạng:

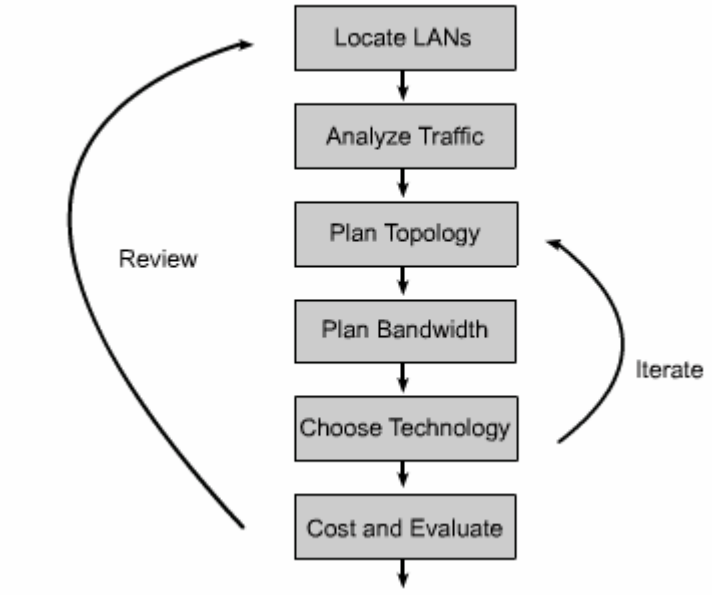
- Kết nối và mức độ dòng lưu lượng.
- Dữ liệu Client/Server.
- Hướng kết nối hay không hướng kết nối.
- Khả năng kéo dài thời gian trễ.
- Khả năng hoạt động của mạng.

- Tỉ lệ lỗi.
- Mức độ ưu tiên.
- Loại giao thức.
- Chiều dài trung bình của gói dữ liệu.

Việc xác định vị trí các điểm cuối của kết nối sẽ giúp chúng ta xây dựng sơ đồ cấu trúc WAN. Cấu trúc này phải thoả mãn các điều kiện về địa lý cũng như các điều kiện hoạt động. Nếu điều kiện hoạt động đòi hỏi cao thì cần phải có thêm các kết nối để dự phòng và chia sẻ tải.

Cuối cung, chúng ta phải quyết đình chi phí lắp đặt và hoạt động cho WAN, so sánh chi phí đó với những lợi ích mà WAN mang lại.

Trong thực tế các bước được đưa ra dưới đây rất ít khi là một quá trình xuyên suốt liên tục. Sẽ có thể có nhiều thay đổi cần thiết trước khi kết thúc thiết kế. Sau khi lắp đặt WAN xong chúng ta cũng luôn phả theo dõi và đánh giá lại mạng WAN để đảm bảo hiệu quả hoạt động của nó.



Hình 2.3.2.b. *Các bước trong thiết kế WAN*

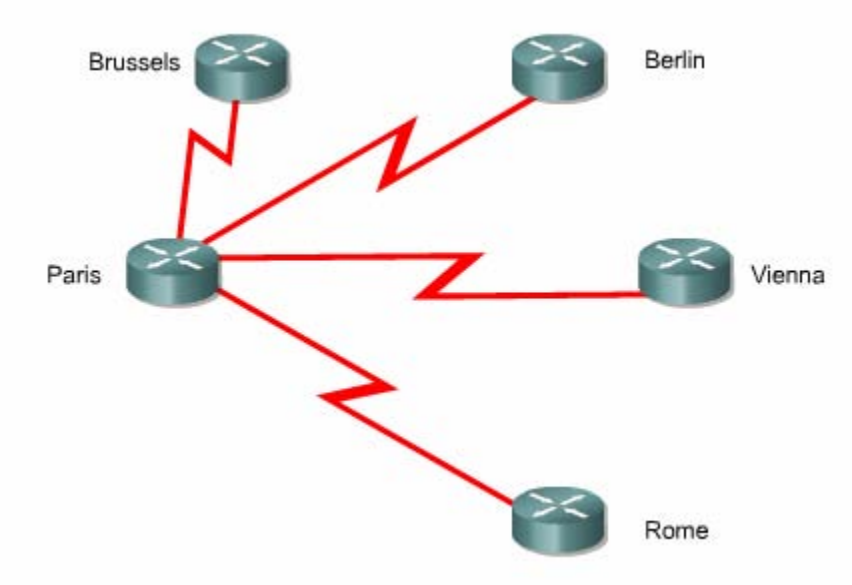
Xác định và lựa chọn dung lượng mạng như thế nào

Thiết kế WAN thực chất bao gồm các công việc sau:

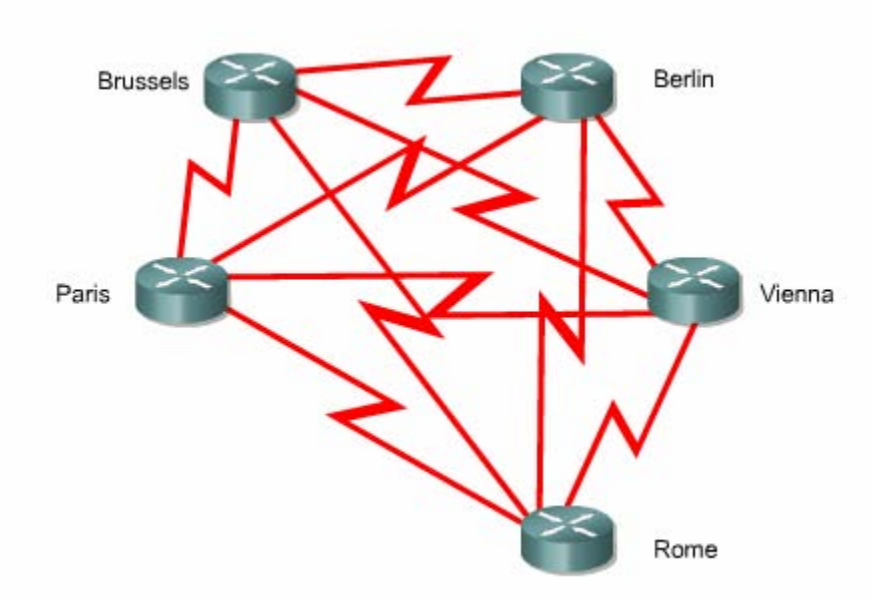
Lựa chọn cấu trúc kết nối giữa các vị trí khác nhau.

Lựa chọn công nghệ cho các kết nối này sao cho phù hợp với yêu cầu của toàn bộ hệ thống và chi phí chấp nhận được.

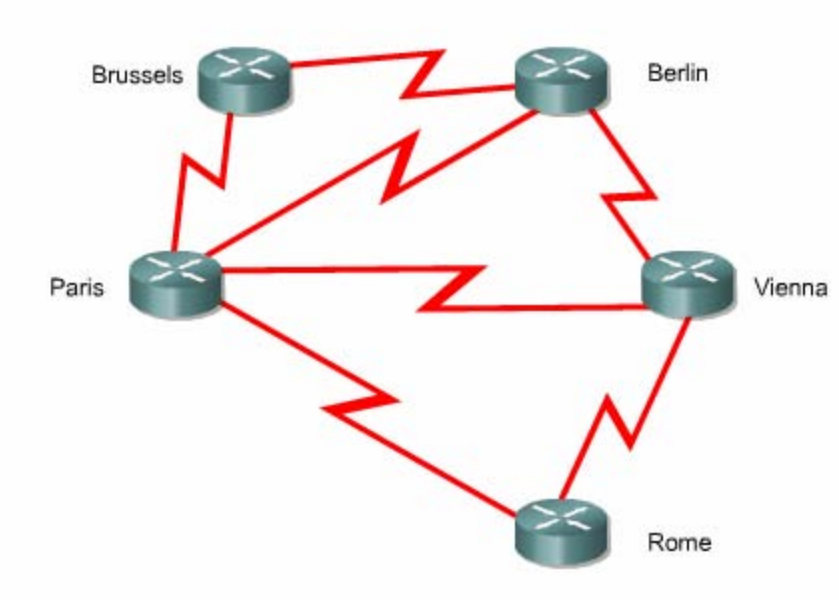
Có rất nhiều mạng WAN sử dụng cấu trúc hình sao. Khi tổ chức phát triển hơn, thêm một chi nhánh cần kết nối vào trung tâm thì khi đó triển khai thêm một nhánh cho cấu trúc hình sao. Đôi khi các điểm cuối của hình sao được kết nối chéo với nhau để tạo thành mạng lưới, tạo thêm nhiều khả năng kết nối. Khi thiết kế, đánh giá lại hoặc thay đổi mạng WAN chúng ta cần chọn ra một cấu trúc phù hợp với yêu cầu.



Hình 2.3.3.a. *Cấu trúc hình sao.*



Hình 2.3.3.b. *Cấu trúc hình lưới toàn phần.*



Hình 2.3.3.c. *Cấu trúc hình lưới một phần.*

Khi lựa chọn cấu trúc, chúng ta cần quan tâm đến một số yếu tố. Càng nhiều kết nối thì chi phí càng tăng cao, nhưng càng có nhiều đường kết nối giữa các điểm thì độ tin cậy của mạng càng cao. Càng đặt thêm nhiều thiết bị trên đường truyền dữ liệu càng làm tăng thêm thời gian trễ và làm giảm độ tin cậy. Chúng ta có rất nhiều

công nghệ khác nhau với những đặc điểm khác nhau để chọn lựa cho kết nối dữ liệu.

Công nghệ	Yếu tố tính cước phí	Tốc độ bit tối đa	Đặc điểm khác
Đường thuê riêng	Khoảng cách, dung lượng	Không giới hạn	Dung lượng cố định.
Đường điện thoại	Khoảng cách, thời gian	33 – 56 kb/giây	Quay số, kết nối chậm.
ISDN	Khoảng cách, dung lượng	64 hoặc 128 Kb/giây <2 Mb/giây PRI	Quay số, kết nối nhanh.
X.25	Dung lượng.	<48 Kb/giây	Dung lượng cố định
ATM	Dung lượng.	>155 Mb/giây	Dung lượng thay đổi.

Những công nghệ đòi hỏi phải thiết lập kết nối trước khi truyền dữ liệu, ví dụ như đường điện thoại, ISDN, X.25, không phù hợp cho mạng WAN cần thời gian đáp ứng nhanh hoặc thời gian trễ thấp. Một khi đã được thiết lập kết nối thì ISDN và các dịch vụ quay số khác có thời gian trễ thấp, ít nghẽn mạch. ISDN thường được chọn để kết nối các văn phòng nhỏ vào mạng trung tâm vì nó cung cấp kết nối tin cậy, băng thông phù hợp. ISDN còn được sử dụng làm đường dự phòng cho đường kết nối chính và là kết nối được thiết lập theo yêu cầu để chia sẻ tải với đường kết nối chính. Một ưu điểm của công nghệ này là thuê bao chỉ phải trả cước phí cho thời gian đường truyền được thiết lập.

Các chi nhánh của một công ty có thể kết nối trực tiếp với nhau bằng đường thuê riêng hoặc kết nối vào mạng chia sẻ như X.25, Frame Relay và ATM. Đường truyền thuê kênh riêng kéo được xa hơn và đương nhiên cũng đắt hơn nhưng nó có thể cung cấp mọi băng thông chúng ta muốn, thời gian trễ và nghẽn mạch rất thấp.

Mạng ATM, Frame Relay và X.25 truyền lưu lượng của nhiều khách hàng khác nhau trong cùng một kết nối. Khách hàng không kiểm soát được số lượng đường kết nối, số lượng trạm trung gian mà dữ liệu phải đi qua trong mạng chia sẻ, cũng như không thể điều khiển được thời gian chờ tại mỗi trạm. Chính vì nhược điểm về thời gian trễ và nghẽn mạch mà các công nghệ này không phù hợp với một số loại lưu lượng mạng. Tuy nhiên, nhược điểm này vẫn thường được chấp nhận vì các mạng chia sẻ này lại có ưu điểm lớn là chi phí rẻ. Khi có nhiều khách hàng cùng chia sẻ một đường kết nối thì đương nhiên chi phí sẽ thấp hơn nhiều so với chi phí cho một đường thuê kênh riêng có cùng dung lượng.

Mặc dù ATM cũng là một mạng chia sẻ nhưng nó được thiết kế để giảm thiểu tối đa thời gian trễ và nghẽn mạch bằng cách sử dụng các kết nối tốc độ cao với một đơn vị dữ liệu thống nhất, dễ quản lý, gọi là tế bào. Mỗi một tế bào ATM (chính là mỗi gói dữ liệu trong mạng ATM) có chiều dài cố định là 53 byte, trong đó 48 byte dữ liệu và 5 byte cho phần Header. Các tế bào có chiều dài nhỏ và như nhau, không có gói nào khác lớn hơn trong mạng ATM nên không có thời gian trễ lớn hơn giữa các gói. Do đó, ATM được sử dụng rộng rãi cho các loại lưu lượng nhạy cảm với thời gian trễ. Frame Relay cũng có thể được sử dụng cho những loại lưu lượng nhạy cảm với thời gian trễ nhưng thường phải sử dụng thêm cơ chế QoS để cấu hình độ ưu tiên cho những loại dữ liệu này.

Việc chọn lựa các công nghệ cho WAN thường dựa trên loại lưu lượng và dung lượng của chúng. ISDN, DSL, Frame Relay hoặc đường thuê riêng thường được sử dụng để kết nối các chi nhánh vào một trung tâm. Frame Relay, ATM hoặc đường thuê riêng thường được sử dụng để kết nối các vùng mở rộng vào đường trục chính. ATM hoặc đường thuê kênh riêng được sử dụng làm đường trục chính cho WAN.

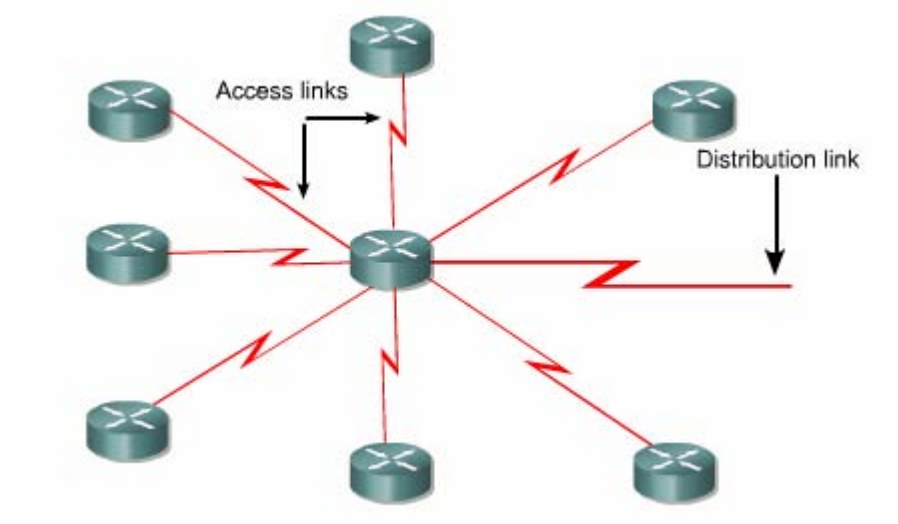
2.3.4. Mô hình thiết kế 3 lớp

Việc kết hợp một cách có hệ thống là rất cần thiết khi chúng ta cần liên kết nhiều vị trí lại với nhau. Giải pháp phân cấp với mô hình 3 lớp cho chúng ta rất nhiều ưu điểm được nêu trong bảng sau.

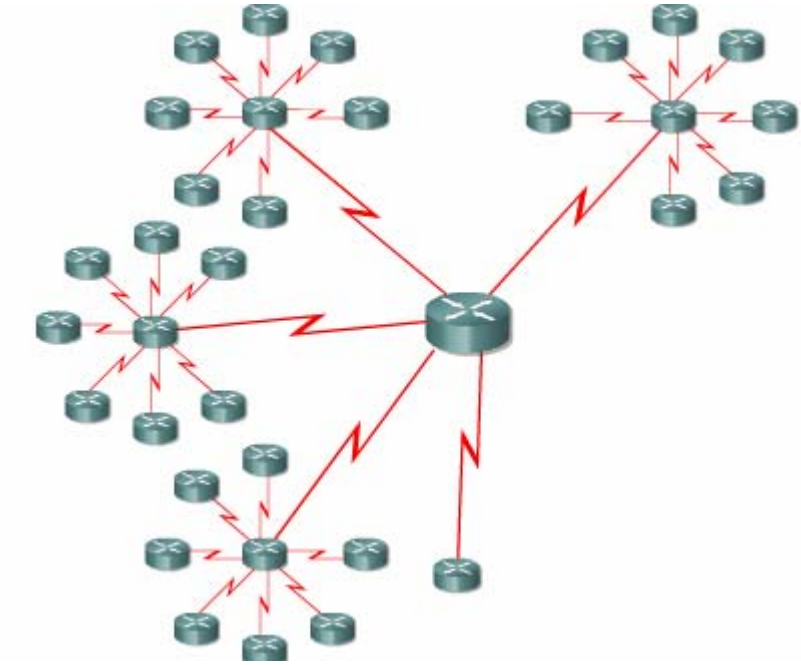
Khả năng mở rộng	Mạng được thiết kế theo mô hình phân cấp có thể mở rộng hơn nhiều mà không hề làm giảm bớt mức độ kiểm soát và quản lý hệ thống. Các chức năng của hệ thống đã mang tính tập trung và các lỗi tiềm ẩn sẽ được phát hiện dễ dàng hơn. Hệ thống mạng chuyển mạch điện thoại là một ví dụ cho kiểu cấu trúc mạng phân cấp lớn.
Dễ triển khai	Cấu trúc phân cấp có chức năng rõ ràng cho từng lớp nên công việc triển khai cũng được thực hiện dễ dàng hơn.
Dễ dàng xử lý sự cố	Việc phân chi chức năng rõ ràng cho mỗi lớp cho phép việc xác định sự cố dễ dàng hơn. Việc chia hệ thống mạng ra thành nhiều phân đoạn giúp giảm thiểu phạm vi ảnh hưởng của sự cố.
Khả năng dự đoán	Phản ứng của hệ thống mạng có cấu trúc phân lớp hoàn toàn có thể dự đoán được, do đó việc nâng cấp hệ thống cũng sẽ tạo được thuận lợi hơn.
Khả năng hỗ trợ các giao thức	Đối với cấu trúc mạng có phân cấp thì việc tích hợp các ứng dụng và giao thức hiện tại với tương lai có thể thực hiện dễ dàng vì cơ sở hạ tầng mạng được tổ chức theo logic.
Khả năng quản lý	Tất cả các ưu điểm được liệt kê ở trên đều nhằm cung cấp khả năng quản lý tốt hơn cho hệ thống mạng.

Chúng ta thử tưởng tượng một công ty lớn hoạt động trên mọi quốc gia ở Châu Âu và có chi nhán ở mọi thành phố có dân số hơn 10.000 người. Mỗi chi nhánh là một LAN và chúng ta cần liên kết các chi nhánh với nhau. Mạng hình lưới rõ ràng là không khả thi vì chúng ta cần tới gần 500.000 liên kết cho 900 điểm. Mạng hình sao đơn cũng không thực hiện được vì chúng ta cần phải có một router tại vị trí trung tâm hình sao với 900 cổng hoặc 1 cổng vật lý có khả năng thiết lập 900 giao tiếp ảo.

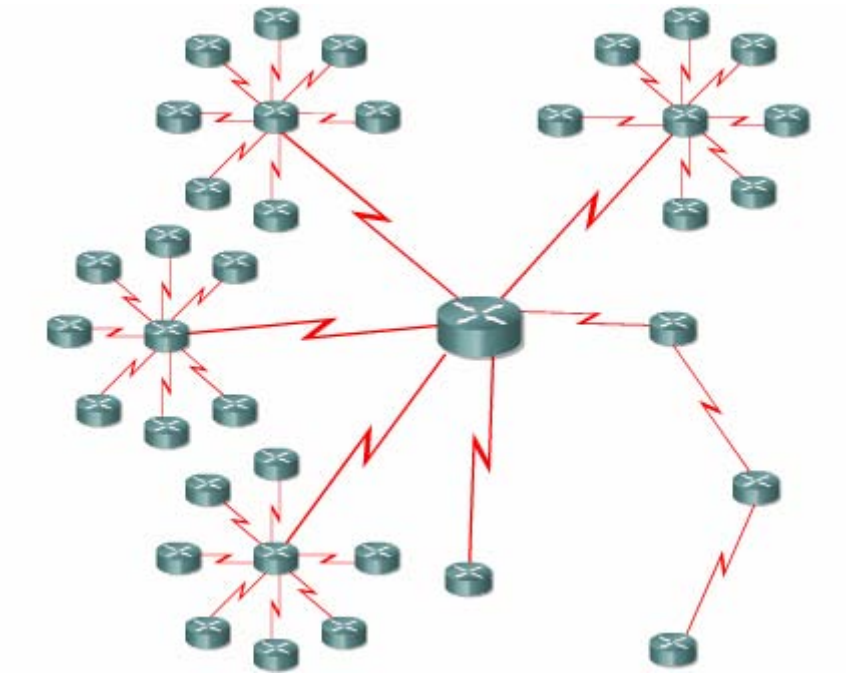
Thay vào đó chúng ta sẽ thiết kết theo mô hình phân cấp. Các mạng LAN trong cùng một vùng địa lý sẽ được liên kết lại với nhau thành một vùng. Các vùng sẽ được kết nối với nhau tạo thành một khu vực. Các khu vực kết nối với nhau và đóng vai trò là trục chính của mạng WAN.



Hình 2.3.4.a. *Các LAN trong một vùng được kết nối lại theo hình sao và từ router ở trung tâm hình sao kết nối ra khu vực.*



Hình 2.3.4.b. *Một mạng khu vực.*



Hình 2.3.4.c. *Kết nối mạng khu vực vào đường trục chính.*

Số lượng các địa điểm được kết nối với nhau trong một vùng được giới hạn trong khoảng từ 30 đến 50. Mỗi vùng có cấu trúc hình sao, thiết bị tại trung tâm hình sao sẽ kết nối ra khu vực. Mạng khu vực có phạm vi địa lý lớn, kết nối khoảng 3 đến 10 vùng với nhau. Thiết bị trung tâm của mạng khu vực sẽ kết nối ra trục chính, các kết nối này có thể là kết nối điểm-đến-điểm.

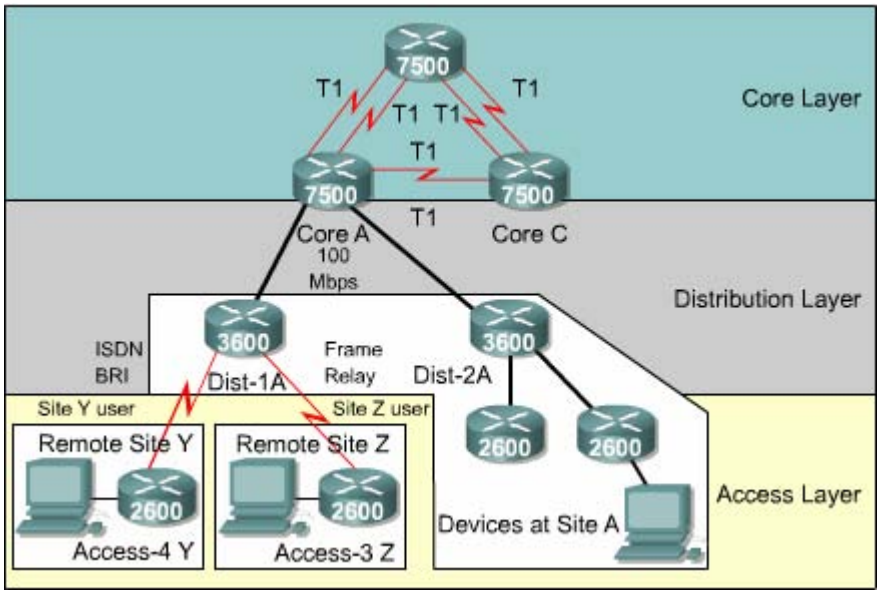
Mô hình 3 lớp này dựa theo thiết kế phân cấp được sử dụng trong hệ thống điện thoại. Lớp truy cập là lớp kết nối các điểm trong cùng một vùng và đây là điểm truy cập vào hệ thống mạng. Lưu lượng giữa các vùng được phân phối bởi các kết nối trong lớp phân phối và chỉ được chuyển lên đường trục chính sang khu vực khác khi cần thiết.

Cấu trúc này rất hữu dụng khi công ty có cấu trúc chi nhánh và được chia thành khu vực, vùng, chi nhánh. Cấu trúc này cũng rất phù hợp khi có một trung tâm dịch vụ mà tất cả các chi nhánh đều cần phải truy cập vào nhưng cấp độ lưu lượng không đủ để phân phối trực tiếp cho từng kết nối của từng chi nhánh.

Trong mạng LAN ở trung tâm của mỗi vùng, chúng ta có thể đặt các server để cung cấp dịch vụ nội bộ. Tuỳ theo mức độ và loại lưu lượng mà kết nối truy cập có thể là quay số, thuê riêng hoặc Frame Relay. Cấu trúc Frame Relay cho phép thực hiên dạng mạng lưới để dự phòng mà không cần phải thêm kết nối vật lý. Các kết nối ở lớp Phân phối (Distribution Layer) có thể là Frame Relay hoặc ATM và kết nối trục chính (Core Layer) có thể là ATM hoặc đường thuê riêng.

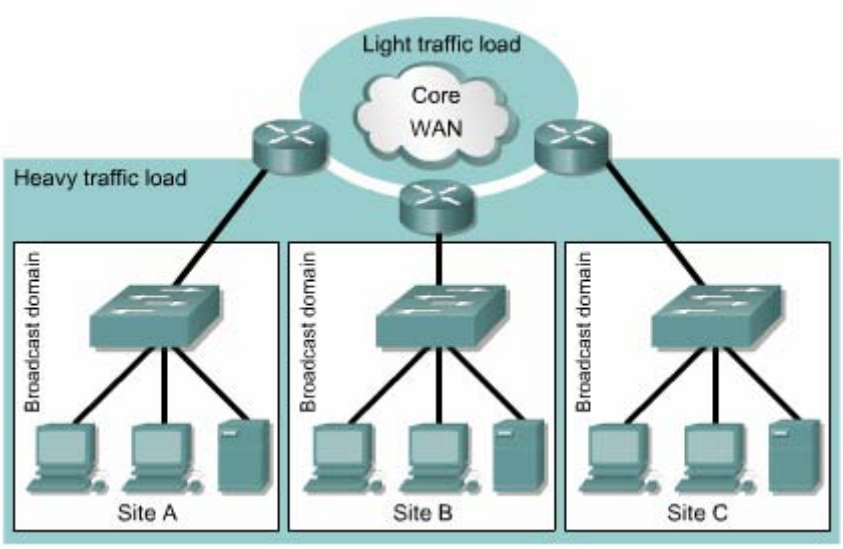
2.3.5. Các mô hình phân lớp khác

Có nhiều hệ thống mạng lại không đòi hỏi phải có cấu trúc phân cấp phức tạp đủ 3 lớp. Do đó, chúng ta có thể sử dụng dạng phân cấp đơn giản hơn.



Hình 2.3.5.a. *Mô hình phân cấp 3 lớp.*

Một công ty có một số chi nhánh nhỏ với mức độ lưu lượng thấp thì có thể thiết kết theo một lớp. Trước đây, mô hình này không được phổ biến vì chiều dài của đường thuê riêng là một yếu tố đáng kể. Ngày nay, với Frame Relay chúng ta không trả cước phí theo chiều dài thì giải pháp thiết kế này có thể thực hiện được.



Hình 2.3.5.b. *Mô hình phân cấp một lớp.*

Nếu do yêu cầu địa lý cần phải tập trung thành một số điểm thì chúng ta có thể áp dụng mô hình thiết kế 2 lớp.

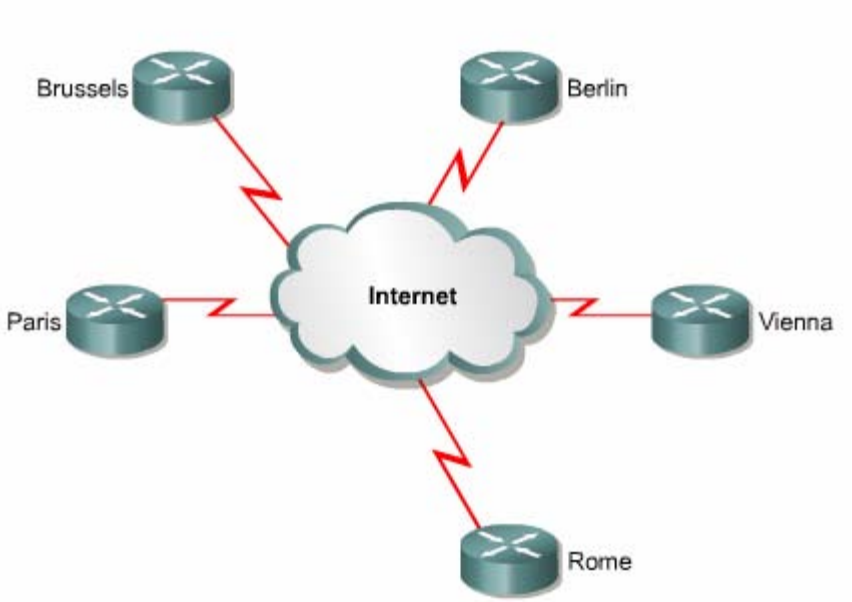
Khi thiết kế mạng đơn giản chúng ta vẫn dựa theo mô hình ba lớp để mạng có khả năng mở rộng về sau. Các thiết bị tại trung tâm của lớp 2 được coi là trục chính mặc dù không có router nào ở lớp trục chính (core layer) kết nối vào nó. Tương tự, trong thiết kế một lớp, thiết bị trung tâm cũng đồng thời là thiết bị khu vực và thiết bị trục chính. Với cách thiết kế phân lớp như vậy hệ thống có thể được mở rộng dễ dàng sau này.

2.3.6. Một số điểm cần lưu ý khác khi thiết kế WAN.

Nhiều mạng WAN có kết nối ra Internet. Đây là một giải pháp có nhiều vấn đề về bảo mật nhưng lại là một cách tốt để kết nối các chi nhánh ở nhiều quốc gia khác nhau.

Trong quá trình thiết kế, chúng ta phải quant tâm đến thành phần đi ra và đi vào từ Internet. Từ khi Internet được triển khai khắp nơi, các mạng LAN của công ty có thể trao đổi dữ liệu theo hai cách. Mỗi LAN có một kết nối đến ISP trong vùng của nó hoặc là từ router trung tâm củ vùng thực hiện một kết nối đến một ISP. Cách thứ nhất có ưu điểm là luồng lưu lượng được truyền đi trong mạng Internet chứ

không phải trong mạng của công ty, do đó kết nối WAN có thể có dung lượng nhỏ hơn. Nhưng cách này có một nhược điểm là cả hệ thống mạng công ty được phơi ra cho các tấn công từ Internet. Khi có nhiều kết nối như vậy thì việc theo dõi và quản lý cũng gặp khó khăn. Một kết nối đơn từ router trung tâm của vùng ra Internet sẽ dễ dàng theo dõi và bảo vệ hơn và như vậy mạng WAN của công ty sẽ phải thực hiện truyền tải lưu lượng nhiều hơn.



Hình 2.3.6. *Sử dụng Internet như mạng WAN của công ty.*

Nếu mỗi LAN trong mạng có một kết nối Internet riêng thì Internet có thể được sử dụng như mạng WAN của công ty đó, trong đó lưu lượng giữa các chi nhánh được truyền đi trong Internet. Việc bảo vệ các mạng LAN sẽ là một vấn đề nhưng chi phí tiết kiệm được do không phải xây dựng mạng WAN riêng sẽ được dành để chi trả cho vấn đề bảo mật.

Server nên được đặt ở gần nơi thường xuyên truy cập vào nó nhất. Các thông tin trả lời, cập nhật của server sẽ làm giảm dung lượng hiệu dụng của đường truyền. Vị trí đặt dịch vụ truy cập Internet phụ thuộc vào đặc tính của bản thân mỗi dịch vụ, mỗi loại lưu lượng và yêu cầu về bảo mật. Lĩnh vực này là một chủ đề đặc biệt nằm ngoài phạm vi của giáo trình này.

TỔNG KẾT

Sau đay là các điểm chính của chương này:

- Sự khác nhau về phạm vi địa lý giữa WAN và LAN.
- Các lớp hoạt động của WAN và LAN trong mô hình OSI.

CHƯƠNG 3: GIAO THỨC ĐIỂM NỐI ĐIỂM

(Point – to – Point Protocol)

GIỚI THIỆU

Chương này cung cấp cho bạn đọc một cái nhìn tổng quát về công nghệ WAN. Trong đó chúng tôi giới thiệu và giải thích các thuật ngữ WAN như truyền nối tiếp, phân kênh theo thời gian (TDM – Time Division Multiplexing), điểm ranh giới, DTE –Data Terminal Equipment, DCE – Data Circuit – terminating Equipment. Sự phát triển và ứng dụng của giao thức đóng gói HDLC (High-level Data Link Control) cũng như phương pháp cấu hình và xử lý sự cố cổng Serial trên router được trình bày trong chương trình này.

PPP (Point – to – Point Protcol) là một giao thức thường được chọn để triển khai trên một kết nối WAN nối tiếp. PPP có thể thực hiện được

Thong tin lien lien lạc thông tin liên lạc đồng bộ, bất đồng bộ và phát hiện lỗi. Quan trọng nhất là PPP có quá trình xác minh sử dụng CHAP hoặc PAP. PPP có thể sử dụng được trên nhiều môi trường vật lý khác nhau bao gồm cáp xoắn, cáp quan và truyền qua vệ tinh.

Trong chương này chúng ta sẽ tìm hiểu về quá trình cấu hình và xử lý sự cố cho PPP

Sau khi hoàn t ất ch ương n ày các b ạn c ó th ể th ực hi ện đ ư ợc:

Gi ải th ích s ự truy ền n ối ti ếp

M ô t ả v à cho v í d ụ v ề TDM

x ác định đi ểm ranh giới trong mạng WAN

M ô t ả ch ức n ăng c ủa DTE v à DCE

Tr ình b ày s ự ph át tri ển c ủa giao th ức đ óng g ói HDLC

S ử d ụng s ự ph át tri ển c ủa giao th ức đ óng g ói HDLC

S ử d ụng l ệnh encapsulation hdlc đ ể c ấu h ình HDLC

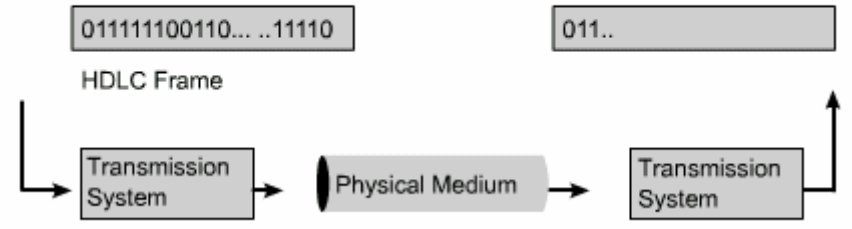
X ử l ý s ự c ố tr ên c ổng S erial b ằng l ệnh sh ow int erface v à sh ow c ontroller

X ác đ ịnh nh ững ưu đi ểm khi s ử d ụng PPP

- Gi ải th ích ch ức n ăng c ủa hai th ành ph ần trong PPP :LCP (Link C ontrol Protocol) v à NCP (Net work C ontrol Protocol)
- M ô t ả c ấu tr úc frame PPP
- X ác đ ịnh 3 qu á tr ình c ủa m ột phi ên giao ti ếp PPP
- Gi ải th ích s ự kh ác nhau gi ữa PAP v à CHAP
- Li ệt k ê c ác b ư ớc c ủa qu á tr ình x ác minh PPP
- C ấu h ình PPP v ới nhi ều ch ọn l ựa kh ác nhau
- C ấu h ình ki ểu đ óng g ói PPP
- C ấu h ình qu á tr ình x ác minh Chap va PAP
- S ử d ụng l ệnh Sh ow int erface đ ể ki ểm tra ki ểu đ óng g ói tr ên c ổng S erial
- X ử l ý c ác sự cố liên quan đến cấu hình PPP bằng lệnh debug PPP

3.1. Liên kết nối tiếp điểm-đến-điểệ

3.1.1.Giới thiệu về truyền nối tiếp



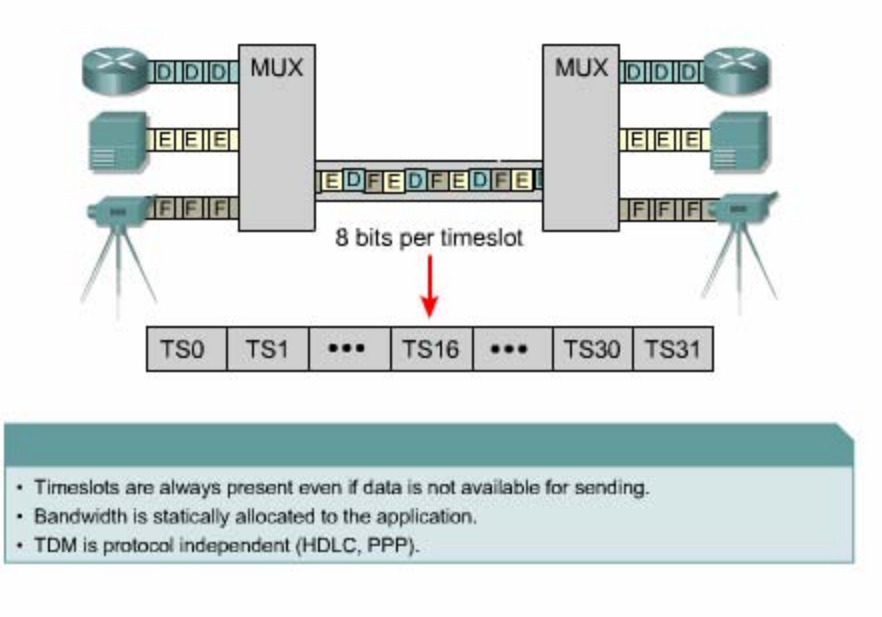
Các công nghệ WAN đều dựa trên cơ sở truyền nối tiếp ở lớp Vật lý. Điều này có ý nghĩa là các bit trong một frame được truyền lần lượt trên đường truyền vật lý

- Mỗi bit trong frame Lớp 2 được mã hoá thành tín hiệu và được truyền lần lượt xuống môi trường tryền vật lý. Các phương pháp mã hoá ín hiệu lớp Vật lý bao gồm NRZ-L (Nonreturn to Zezo Level), HDB3(High Density Binary) và AMI (các phương pháp mã hoá tín hiệu khác nhau. Sau đây là một số các chuẩn truyền nối tiếp khác nhau

- RS-232-E
- V.35
- High Speed Serial Interface (HSSI)

3.1.2 Phân kênh theo thời gian (TDM- Time Division Multiplexing)

Phân kênh theo thời gian TDM là truyền nhiều nguồn thong tin trên cùng một tín hiệu, sau đó lại tách ra thành các nguồn riêng biệt như ban đầu tại điểm cuối



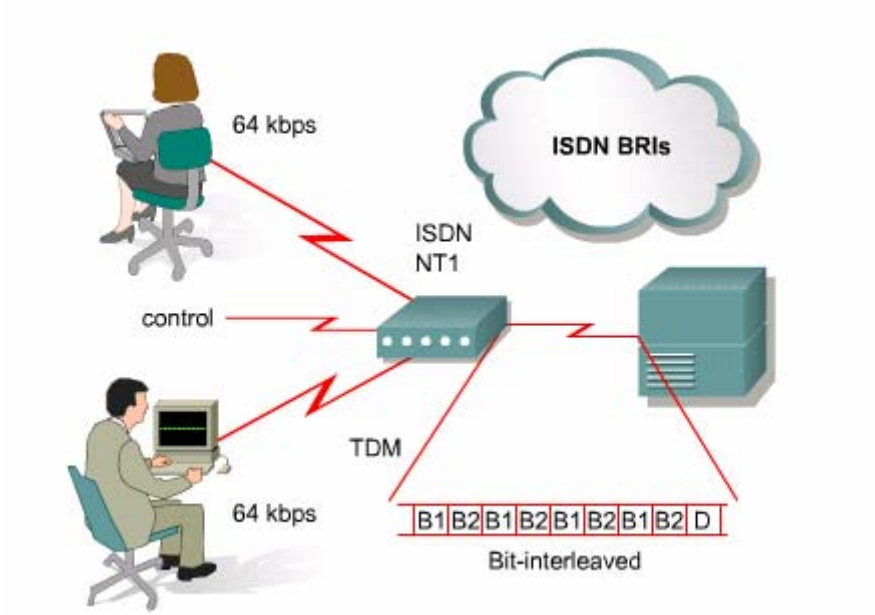
Ví dụ như hình 3.1.2.a chúng ta có 3 nguồn thong tin khác nhau đưa vào cùng một kênh. Mỗi nguồn thông tin được truyền luân phiên, đơn vị dữ liệu. Đơn vị dữ liệu này có thể là một bit hoặc một byte. Tuỳ theo đơn vị là bit hay byte mà loại TDM này được gọi là chèn bit hay chèn byte.

Mỗi nguồn thông tin ở đầu vào có một dung ượng riêng của nó. Để có thể truyền thông tin cho cả 3 nguồn thì dung lượng của kênh truyền không được thấp hơn tổng dung lượng của 3 đầu vào.

Trong TDM các khe thời gian luôn luôn tồn tại cho dù không có dữ liệu truyền vào. TDM có thể được ví như một xe lửa có 3 toa xe. mỗi toa xe thuộc sở hữu của một công ty và mỗi ngày xe lửa đều cạy với 32 toa. Nêu công ty nào có hang gởi đi thì toa xe của công ty đó đầy. Nếu công ty nào không có gì gởi đi thì toa xe đó để trống nhưng vẫn hiện diện trong đoàn tàu

TDM là một khái niệm ở lớp Vật lý, nó không phụ thuộc vào bản chất của thông tin được ghép vào kênh truyền và cũng không phụ thuộc vào các giao thức lớp 2 được sử dụng trên các đầu vào.

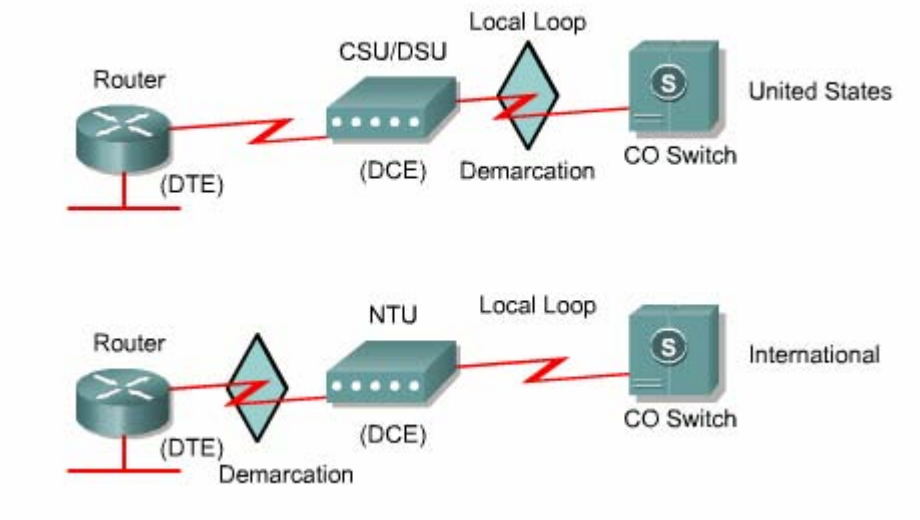
Một ví dụ cho TDM là ISDN (Integrated Services Digital Network). ISDN BRI có 3 kênh truyền, bao gồm 2 kênh B 64Kb/giây và một kênh D 16Kb/giây. TDM có 9 khe thời gian được chia ra như trong hình3.1.2b.



3.1.3 Điểm ranh giới

Điểm ranh giới là điểm mà trách nhiệm của nhà cung cấp dịch vụ trong mạng kết thúc. Ở Mỹ nhà cung cấp dịch vụ cung cấp mạng vòng nội bộ đến vị trí của khách hang và khách hang kết nối thiết bị của mình như CSU/DSU vào điểm cuối của mạch vòng dữ liệu này. Khách hang phải chịu trách nhiệm bảo trì, thay thể hay sửa chữa thiết bị của mình

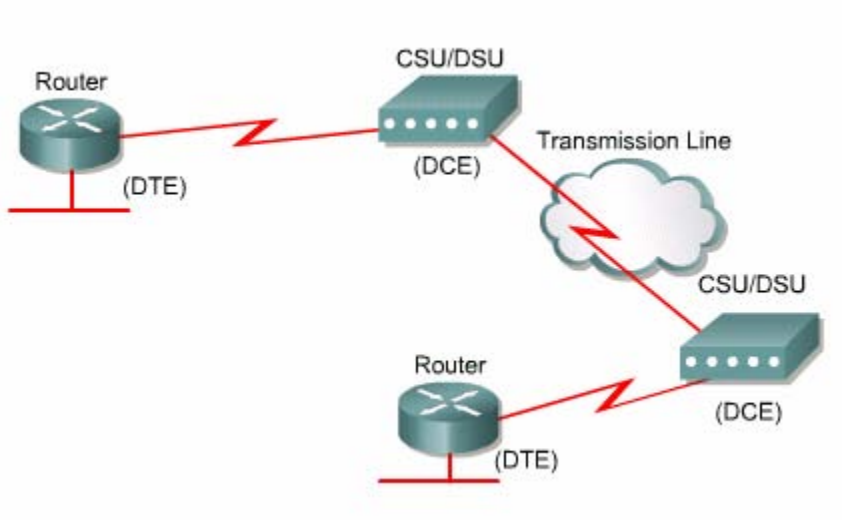
Ở các nước khác trên thế giới thì công ty khai thác dịch vụ sẽ cung cấp và quản lý đơn vị kết cuối mạng NTU (network terminating unit). Như vậy nhà cung cấp dịch vụ có thể quản lý và xử lý sự cố với điểm ranh giới nằm sau NTU. Khách hàng kết nối thiết bị CPE của mình, ví dụ như router, thiết bị truy cập Frame Relay vào NTU bằng cổng Serial V3.5 hoặc RS -232



3.1.4 DTE/DCE

Một kết nối tiếp có một đầu là thiết bị DTE và đầu kia là thiết bị DCE. Kết nối giữa hai DCE chính là mạng WAN của nhà cung cấp dịch vụ CPE thông thường là router của khách hang đóng vai trò là DTE

Máy tính, máy in, máy fax cũng là những ví dụ cho thiết bị DTE, DCE, thông thường là moderm hoặc CSU/DSU là thiết bị chuyển đổi tín hiệu từ DTE sang dạng tín hiệu phù hợp với đường truyền trong mạng WAN của nhà cung cấp dịch vụ. Tín hiệu này được thiết bị DCE ở đầu bên kia nhận được và lại được chuyển đổi thành dạng tín hiệu phù hợp với DTE và được truyền cho DTE



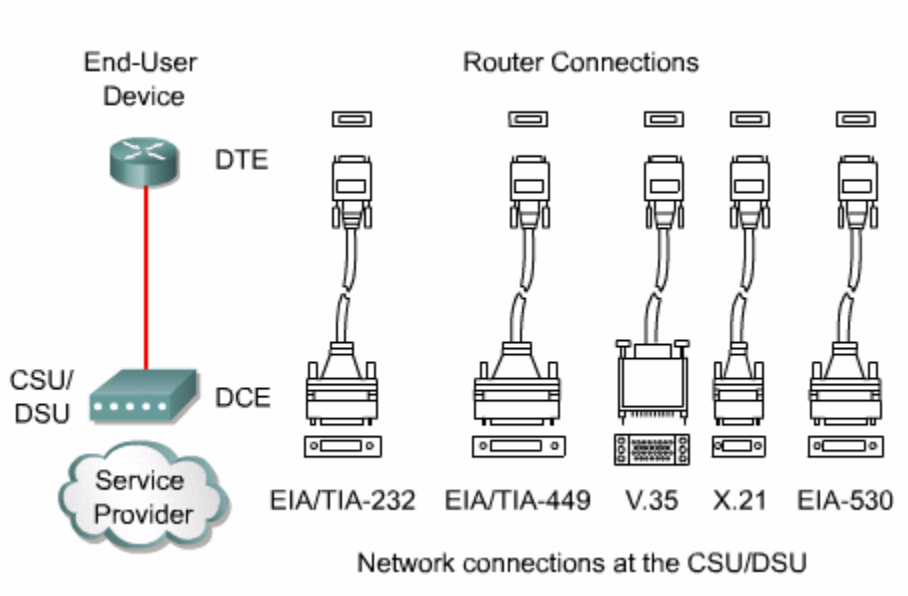
Chuyển giao tiếp DTE/DCE định nghĩa các đặc điểm sau:

- Cấu trúc vật lý: số lượng chân và hình dạng của đầu kết nối
- Điện : định nghĩa mức điện thế cho tín hiệu 0 và 1
- Chức năng: quy ước chức năng ý nghĩa của từng đường tín hiệu trong cổng kết nối
- Thủ tục: quy ước thứ tự các bước trong truyền dữ liệu

Nếu hai DTE cần phải kết nối trực tiếp với nhau giống như hai máy tính hoặc hai router thì chúng ta cần sử dụng một loại cáp đặc biệt gọi là cáp null-moderm để thay thế cho DCE. Đối với kết nối đồng bộ thì cần phải có tín hiệu đồng bộ, khi đó chúng ta cần phải có thêm một thiết bị bên ngoài hoặc một trong hai thiết bị DTE phải phát được tín hiệu đồng bộ

Cổng Serial đồng bộ trên router được cấu hình là DTE hay DCE là tuỳ theo đầu cáp cắm vào cổng đó là DTE hay DCE. Cấu hình mặc định của cổng Serial là DTE. Nếu cổng Serial được cấu hình là DTE thì CSU/DSU hoặc thiết bị DCE kết nối vào cổng này phải phát tín hiệu đồng bộ

Cáp cho kết nối DTE – DCE là cáp nối tiếp có lớp bọc chống nhiều. Đầu cáp kết nối vào cổng Serial trên Router là đầu DB-60. Đầukia của cáp theo chuẩn nào là tuỳ theo CSU/DSU hay nhà cung cấp dịch vụ WAN. Thiết bị Cisso có hỗ trợ các chuẩn kết nối sau: EIA/TIA-32, EIA/TIA-449, V.35, X.21 và EIA/TIA-530



Cisso cũng đã giới thiệu loại cáp Smart Serial với độ nhạy cao hơn và kiểu dáng nhỏ gọn hơn . Đầu cáp Smart Serial cắm vào cổng Serial trên router chỉ có 26 chân tín hiệu nhỏ gọn hơn so với đầu DB-60

3.1.5 Đóng gói HDLC

- Truyền nối tiếp đặt cơ sở trên giao thức hướng bit. Giao thức hướng bit tuy có hiệu quả hơn nhưng thường mang tính độc quyền. Năm 1979, ISO đã chấp thuận HDLC là giao thức chuẩn hướng bit của lớp Liên kết dữ liệu) cho ISDN

Link Aceess Procedure f or Mod emsthực hiện đóng gói dữ liệu cho đường truyền nối tiếp đồng bộ. Sự chuẩn hoá này đã giúp cho các tổ chức khác áp dụng và mở rộng giao thức này. Từ năm 1981, ITU-T đã phát triển một loạt các phiên bản của HDLC. Sau đâ là một ví dụ, những giao thức này được gọi là giao thức truy cập đường liên kết:

- Link Aceess Procedure, Balanced (LAPB) cho X.25\
- Link Aceess Procedure on the D channel (LAPD) cho ISDN(
- Link Aceess Procedure f or Mod ems (LAPM) and PPP cho mod ems
- Link Acc ess Proced ure f or Frame Relay (L APF) cho Frame Relay

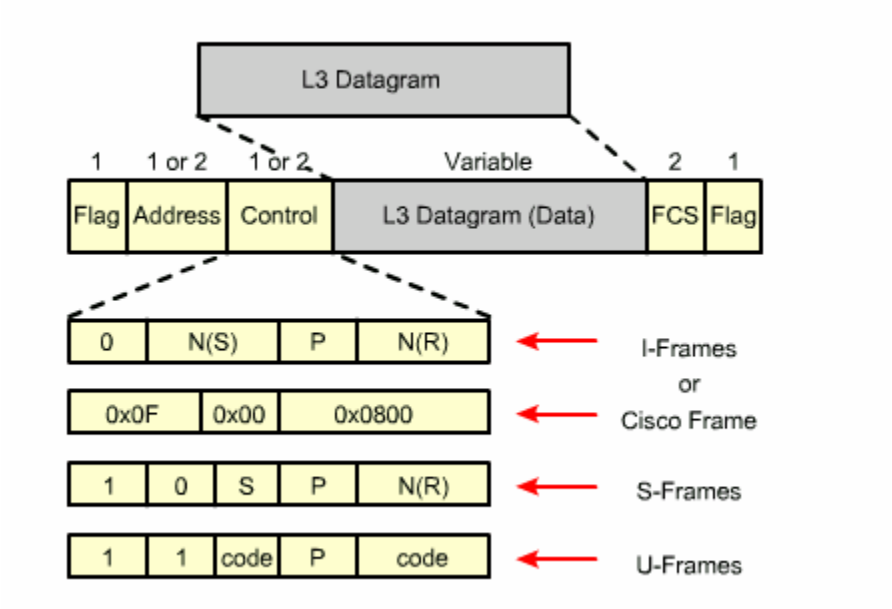
HDLC cung c ấp c ơ ch ế truyền đồng bộ không có lỗi giữa hai điểm. HDLC định nghĩa cấu trúc frame Lớp 2 cho phép điều khiển luồng theo cơ chế cửa sổ trượt, kiểm tra lỗi và báo nhận. Frame dữ liệu hay frame điều khiển đều có cùng một định dạng frame

Chuẩn HDLC không hỗ trợ nhiều giao thức trên một đường kết nối, đồng thời cũng không có thông tin cho biết giao thức lớp trên nào đang được truyền trên đường truyền. Cisso có giới thiệu một phiên bản HDLC độc quyền riêng. Frame Cisso HDLC có phần "type" cho biết giao thức lớp trên của của frame. Nhờ có phần này mà nhiều giao thức lớp Mạng có thể chia sẻ cùng một đường truyền nối tiếp . HDLC là giao thức Lớp 2 mặc định trên cổng Serial của Cisso router

HDLC định nghĩa 3 loại frame mỗi loại có định dạng phần điều khiển khác nhau

- Frame thông tin (I-Frames– Information frames): là frame mạng dữ liệu của máy truyền. Trong frame thông tin có chèn thêm phần điều khiển luồng và lỗi.
- Frame giám sát (S-Frames – Supervisory frames): cung cấp cơ chế hỏi đáp khi cơ chế chèn thông tin trong I-Frame không được sử dụng.
- Frame không đánh số (U-Frames – Unnumbered frames):thực hiện chức năng bổ sung điều khiển kết nối như thiết lập kết nối. Phần "code" trong frame sẽ xác định loại frame là U-frame

Một hoặc hai bit đầu tiên của phần "Cotrol" cho biết loại frame. Trong frame thông tin phần nay có chỉ số của gói gủi kế tiếp và gói nhận kế tiếp. Trong frame phát đi của máy gửi và máy nhận đều có hai chỉ số này



3.1.6 Cấu hình đóng gói HDLC

Kiểu đóng gói mặc định trên cổng Serial đồng bộ của thiết bị Cisco là Cisco HDLC. Nếu cổng Serial đã được cấu hình kiểu đóng gói khác và bây giờ cần quay lại kiểu đóng gói HDLC thì chúng ta vào chế độ cấu hình cổng Serial tương ứng. Sau đó dung lệnh encapsulation để khai báo giao thức đóng gói HDLC cho cổng đó

Router (config – if)# encapsulation hdlc

Cisso HDLC là giao thức điểm nối điểm được sử dụng trên đường truyền nối tiếp giữa hai thiết bị Cisso. Nếu kết nối với một thiết bị không phải của Cisco thì chúng ta nên chọn PPP

3.1.7 Xử lý sự cố trên cổng Serial

Kết quả hiển thị của lệnh show interfaces serial cho biết các thông tin về cổng serial. Khi cổng serial được cấu hình kiểu đóng gói HDLC thì chúng ta sẽ đọc thấy dòng “Encapsulation HDLC” trong kết quả hiển thị của lệnh này

```
Router#show interfaces s0/0
Serial 0 is up, line protocol is up
  Hardware is MCI Serial
  Internet address is 131.108.156.98, subnet mask is
255.255.255.240
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely
255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set
(10 sec)
  Last input 0:00:00, output 0:00:00, output hang never
  Last clearing of "show interface" counters never
  Output queue 0/40, 5762 drops; input queue 0/75, 301
drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     38021 packets input, 5656110 bytes, 0 no buffer
     Received 23488 broadcasts, 0 runts, 0 giants, 0
throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0
ignored, 0 abort
     38097 packets output, 2135697 bytes, 0 underruns
     0 output errors, 0 collisions, 6045 interface
resets
     0 output buffer failures, 0 output buffers swapped
out
     482 carrier transitions
        DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Nếu cổng serial đã được cấu hình PPP thì chúng ta sẽ đọc thấy dòng “Encapsulation PPP” như trong hình 3.1.7b

```
Router#show interfaces serial s0/0
Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 10.140.1.2/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely
255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive set (10
sec)
  LCP Open
  Open: IPCP, CDPCP
  Last input 00:00:05, output 00:00:05, output hang
never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     38021 packets input, 5656110 bytes, 0 no buffer
     Received 23488 broadcasts, 0 runts, 0 giants, 0
throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0
ignored, 0 abort
     38097 packets output, 2135697 bytes, 0 underruns
     0 output errors, 0 collisions, 6045 interface
resets
     0 output buffer failures, 0 output buffers swapped
out
     482 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Sau đây là 5 trạng thái sự cố mà chúng ta có thể xác định được thông qua kết quả hiển thị của lệnh show interfaces serial"

- Serial x is down, line protocol is down
- Serial x is up, line protocol is down
- Serial x is up, line protocol is up (looped)
- Serial x is up, line protocol is down (disabled)
- Serial x is administratively down, line protocol is down

Trạng thái đường kết nối	**Điều kiện có thể xảy ra**	**Sự cố/ Giải pháp**
Serial x is up, line protocol is up	Đây là trạng thái hoạt động tốt của đường truyền	Không cần phải làm gì cả
Serial x is down, line	Router không gửi tín hiệu CD, có nghĩa CD	1.Kiểm tra LED trên CSU/DSU xem CD có hoạt động hay không, hoặc

protocol is down (dầu DTE)	không hoạt động. Có thể sự cố xảy ra do phía nhà cung cấp dịch vụ WAN, kết nối không thực hiện hoặc chưa được kết nối vào CSU/DSU Cáp bị lỗi hoặc kết nối không đúng Lỗi phần cứng (CSU/DSU)	sử dụng thiết bị đo trên đường dây xem có tín hiệu CD hay không. 2. Kiểm tra cáp và kết nối có theo đúng hướng dẫn lắp đặt hay không 3. Sử dụng thiết ị kiểm tra mọi dây cáp. 4. Liên hệ với nhà cung cấp dịch vụ để kiểm tra vị trí xảy ra sự cố. 5. Thay thế phần bị sự cố. 6. Nếu nghi ngờ phần cứng router bị hư hỏng thì nên chuyển kết nối sang cổng khác. Nếu sự cố không xảy ra nữa thì có nghĩa là cổng kết nối trước đó đã bị hư.
Serial x is up, line protocol is down (dầu DTE)	Router nội bộ hoặc router ở đầu bên kia bị cấu hình sai. Router đầu bên kia không gửi thông điệp Keepalives Có thể sự cố xảy ra do phía nhà cung cấp dịch vụ, đường truyền bị nhiễu hoặc switch bị cấu hình sai. Vấn đề về đồng bộ xảy ra trên cáp, SCTE – Serial clock transmit	1. Đặt modem, CSU hoặc DSU vào chế độ loopback và dùng lệnh show interfaces serial để xem line protocol is up, có nghĩa là sự cố do phía nhà cung cấp dịch vụ WAN hoặc router ở đầu bên kia bị sự cố. 2. Nếu có vẻ như sự cố xảy ra ở đâù bên kia thì chúng ta lặp lại bước 1 ở đầu bên kia 3. Kiểm tra mọi dây cáp, chúng ta cần chắc chắn rằng mọi dây cáp đã được kết nối vào đúng cổng, đúng CSU/DSU vào đúng điểm cuối của mạng WAN của nhà cung cấp dịch vụ.Chúng ta sử dụng lệnh show

	external chưa được cài đặt trên CSU/DSU. SCTE được thiết kế để bổ xung cho sự lệch phạ đồng hồ trên cáp dài. Thiết bị DCE sử dụng SCTE thay vì xung đồng hồ bầu bên trong thiết bị DCE CSU/DSU nội bộ hoặc ở đầu bên kia bị sự cố. Phần cứng của router nội bộ hoặc router đầu bên kia bị hư	controllers để xác định cáp nào đang được cắm vào cổng nào 4. Sử dụng lệnh debug serial interface. 5. Nếu vẫn còn trạng thái line protocol is down trong chế độ loopback ở bước 1 và kết quả hiển thị của lệnh debug serial interface cho thấy số lượng Keepalive không tăng lên thì khả năng lớn là lỗi phần cứng của router . Kết nối loopback cho cổng đang kết nối trên router 6. Nếu line protocol is up, số lượng Keepalive tăng lên thì sự cố không nằm trên router nội bộ 7. Nếu nghi ngờ sự cố do phần cứng router thì chúng ta đổi kết nối lên cổng khác còn trống. Nếu kết nối hoạt động được có nghĩa là cổng trước đó bị hư
Serial x is up line protocol is down (dầu DCE)	Thiếu lệnh cấu hình clokrate cho cổng. Thiết bị DTE không hỗ trợ hoặc chưa được cấu hình cho chế độ SCTE .CSU hoặc DSU ở đầu bên kia bị hư	1.Thêm lệnh cấu hình clokrate cho cấu hình cổng serial 2. Clockrate bps 3. Tham số bps có thể là : 1200,2400,4800,9600,19200,38400, 56000,64000,72000,125000,148000, 250000,500000,800000,1000000, 1300000,2000000,8000000.

		4. Nếu có vẻ như sự cố xảy ra ở đầu bên kia kết nối thì chúng ta thực hiện lại bước 1 ở modem, CSU hoặc DSU ở đầu bên kia 5. Kiểm tra xem cáp có kết nối đúng không. 6. Nếu vẫn còn trạng thái line protocol is down, sự cố có thể là phần cứng hoặc do cáp Chúng ta sử dụng thiết bị kiểm tra cáp 7. Thay thế phần bị hư khi cần thiết
Serial x is up line protocol is up (looped)	Tồn tại mạch lặp vòng. Khi mạch lặp vòng bắt đầu được phát hiện, chỉ số thứ tự của gói Keepalive thay đổi ngẫu nhiên. Nếu chỉ số nhận lại cũng giống với chỉ số gửi đi thì có nghĩa là đang tồn tại mạch lặp vòng	1. Sử dụng lệnh show running-confif để kiểm tra xem có lệnh nào cấu hình cho cổng làm loopback hay không 2. Nếu có lệnh loopback trong cấu hình của cổng giao tiếp thì chúng ta dùng lệnh no loopback để xoá lệnh này khỏi cấu hình 3. Nếu không có lệnh cấu hình loopback thì chúng ta kiểm tra CSU/DSU xem thiết bị này có bị cấu hình bằng tay vào chế độ loopback hay không. Nếu có thì chúng ta tắt chế độ này đi 4.Sau khi tắt chế độ loopback trên CSU/DSU, chúng ta khởi động lại CSU/DSU và xem lại trạng thái

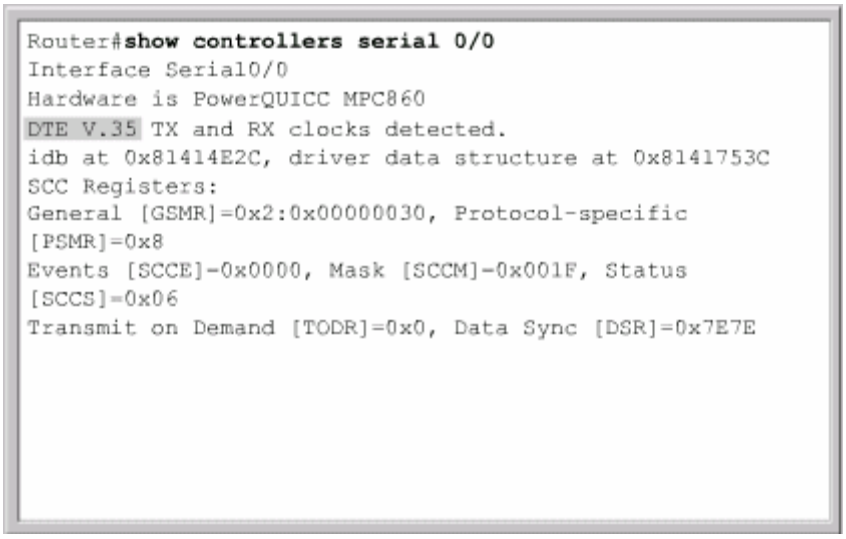
		đường liên kết. Nếu Line protocol is up thì không cần làm gì nữa 5. Nếu CSU/DSU không thể cấu hình bằng tay được thì chúng ta nên liên hệ với nhà cung cấp dịch vụ để yêu cầu hỗ trợ xử lý sự cố trên đường truyền
Serial x is up line protocol is down (disable)	Tỉ lệ lỗi cao đang xảy ra do sự cố phía nhà cung cấp dịch vụ. Sự cố phần cứng của CSU hoặc DSU. Phần cứng router không tốt	1.Sử dụng thiết bị kiểm tra và phân tích đường truyền. Kiểm tra tín hiệu CTS và DSR 2. Ngắn mạch CSU/DSU. Nếu sự cố vẫn còn thì có nghĩa là sự cố phần cứng. Nếu không còn sự cố thì sự cố là do phía nhà cung cấp dịch vụ. 3. Thay thế những thiết bị có sự cố (CSU, DSU, Switch, router)
Serial x is administratively down, line protocol is down	Trong cấu hình cổng của router có lệnh shutdown. Bị trùng địa chỉ IP	1. Kiểm tra cấu hình cổng router xem có lệnh shutdown hay không 2. Nếu có thì dùng lệnh no shutdown để xoá bỏ lệnh này ra khỏi cấu hình 3. Kiểm tra cấu hình địa chỉ IP bằng lệnh show running – config hoặc show interfaces 4. Nếu có trùng địa chỉ thì thay thế địa chỉ IP khác

Lệnh show controllers là một công cụ rất hữu ích khi xử lý sự cố trên kết nối serial. Kết quả hiển thị của lệnh show controllers cho biết trạng thái của cổng, cáp nào hiện đang kết nối vào cổng. Ví dụ như trong hình 3.1.7.c cổng Serial 0/0 được kết

nối với đầu cáp V.35 DTE. Tuỳ theo các phiên bản router khác nhau mà cấu trúc câu lệnh này có khác nhau

Ví dụ khi chúng ta cần xem thông tin về cổng Serial trên router Cisco 7000 thì dùng lệnh show controllers cbus

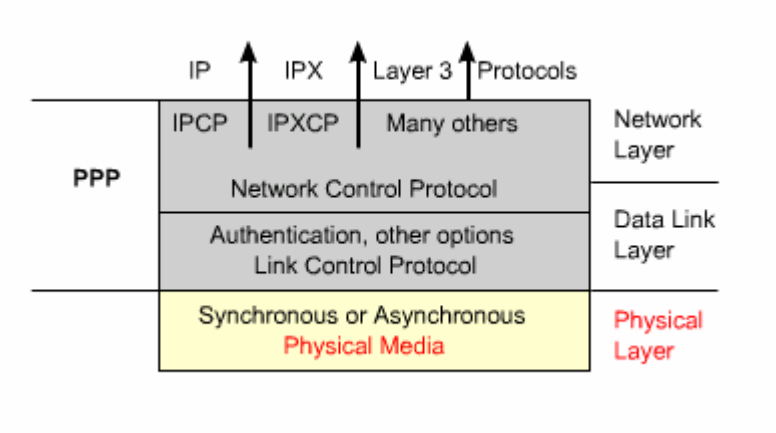
Nếu trong kết quả hiển thị của câu lện này cho thấy cổng giao tiếp là UNKNOWN thay vì là V.35, EIA/TIA – 449 hay một chuẩn cụ thể nào khác, thì sự cố có thể là do kết nối cáp không đúng, Khi đó kết quả hiển thị của lệnh show interfaces serial (X) sẽ cho thấy interface is down, line protocol is down.



3.2 Quá trình xác minh trong PPP

3.2.1. Cấu trúc phân lớp của PPP

PPP sử dụng cấu trúc phân lớp. Cấu trúc phân lớp là mô hình giao tiếp logic giữa các lớp. Mô hình OSI là một ví dụ về mô hình phân lớp trong mạng. PPP cung cấp cách đóng gói phù hợp cho nhiều gói dữ liệu của nhiều giao thức khác nhau để truyền trên một đường truyền điểm-nối-điểm, đồng thời PPP sử dụng lớp liên kết dữ liệu để kiểm tra kết nối. Do đó PPP được chia thành hai giao thức con:



- Giao thức điều khiển đường truyền LCP (Link Control Protocol): được sử dụng để thiết lập kết nối điểm - nối - điểm
- Giao thức điều khiển lớp mạng NCP (Network Control Protocol): được sử dụng để cấu hình cho nhiều giao thức lớp Mạng khác nhau

PPP có thể được cấu hình trên nhiều loại cổng vật lý như sau:

- Cổng truyền nối tiếp bất đồng bộ (Asynchronous serial)
- Cổng truyền nối tiếp đồng bộ (Synchronous serial)
- High – Speed Serial Interface (HSSI).
- Integrated Services Digital Network (ISDN)

LCP nằm ngay trên lớp Vật lý, được sử dụng để thiết lập, cấu hình và kiểm tra kết nối theo những yêu cầu sau

Thực hiện xác minh: Yêu cầu nay đòi bên thiết lập kết nối phải cung cấp thông tin cho biết có được phép của người quản trị mạng để thiết lập kết nối hay không. Hai router ở hai đầu kết nối sẽ thực hiện quá trình xác minh bằng PAP hoặc Chap

- **Nén**: Thực hiện yêu cầu nén frame khi truyền kết nối PPP sẽ giúp tăng thông lượng của đường truyền, giảm lượng dữ liệu phải truyền trên đường dây. Tại đầu nhận frame dữ liệu sẽ được giải nén. Router Cisco có hỗ trợ hai giao thức nén là Stacker và Predictor
- **Phát hiện lỗi:** Cơ chế phát hiện lỗi của PPP thực hiện quá trình kiểm tra điều kiện đường truyền. Chỉ số Quality Magic giúp xác định vòng lặp và độ tin cậy của đường truyền.
- **Ghép kênh (Multilink PPP):**Cisco IOS phiên bản 11.1 trở đi cho phép thực hiện ghép kênh PPP trên cổng của router để thực hienẹ chia sẻ tải
- **PPP Callback:** Để gia tăng khả năng bảo mật, Cisco IOS phiên bản 11.1 trở đi đã cho phép thực hiện chức năng gọi lại trên kết nối PPP. Cisco router đóng vai trò là callback client hoặc callback server. Callback client thiết lập

một cuộc gọi yêu cầu callback server gọi lại cho nó rồi kết thúc ngay cuộc gọi này. Sau đó callback server thực hiện gọi lại cho client dựa trên cấu hình của nó.

LCP còn thực hiện những việc sau:

- Kiểm soat các giới hạn khác nhau về kích thước gói dữ lieu
- Phát hiện lỗi cấu hình
- Kết thúc đường truyền
- Kiểm tra xem đường truyền hoạt động tốt hay bị hư hỏng

PPP cho phép nhiều giao thức lớp mạng khác nhau hoạt động trên cùng một đường truyền. Đối với mỗi giao thức lớp Mạng được sử dụng, PPP cung cấp một NCP riêng biệt. Ví dụ : IPCP (IP Control Protocol) sử dụng cho giao thức IP, IPXCP (Novell IPX control Protocol) sử dụng cho IPX. NCP có mã số chuẩn cho biết giao thức lớp mạng nào đang được đóng gói trong frame PPP

Value (in hex)	Protocol Name
8021	Internet Protocol Control Protocol
8023	OSI Network Layer Control Protocol
8029	Appletalk Control Protocol
802b	Novell IPX Control Protocol
c021	Link Control Protocol
c023	Password Authentication Protocol
c223	Challenge Handshake Authentication Protocol

Sau đây là các phần trong frame PPP

- **Cờ:** Cho biết bắt đầu kết thúc một frame, phần này bao gồm chuỗi nhị phân 0111110
- **Địa chỉ:** Chứa địa chỉ quảng bá 11111111. PPP không ấn định địa chỉ riêng cho trạm đích vì kết nối PPP là kết nối điểm-nối-điểm
- **Điều khiển** : Chiều gài 1 byte có giá trị là 00000011,thực hiện dịch vụ truyền thông kết nối, tương tự như LLC (Logical Link Control) loại 1, truyền dữ liệu không theo thứ tự frame
- **Giao thức:**Chiều gài 2 bte cho biết giao thức lớp trên nào có dữ liệu được đóng gói trong frame
- **Dữ liệu:** Có chiều dài >= 0 byte, chứa toàn bộ dữ liệu của lớp trên. Kết thúc phần dữ liệu là cờ kết thúc và tiếp theo sau là 2 byte của phần FCS. Chiều dài tối đa mặc định của phần dữ liệu là 1500 byte
- **FCS:** Thường dài 2 byte được sử dụng để kiểm tra lỗi frame

3.2.2. Thiết lập một phiên kết nối PPP

Một phiên kết nối PPP được thiết lấp sau 3 giai đoạn: giai đoạn thiết lập kết nối, giai đoạn xác minh và giai đoạn cấu hình giao thức lớp Mạng. Frame LCP được sử dụng để thực hiện các công việc trong mỗi giai đoạn. Sau đây là các loại frame LCP được sử dụng trong phiên kết nối PPP

- Frame thiết lập kết nối: được sử dụng để thiết lập và cấu hình kết nối
- Frame kết thúc kết nối : được sử dụng để kết thúc kết nối
- Frame duy trì kết nối được sử dụng để quản lý và điều chỉnh đường truyền

Sau đây là 3 giai đoạn thiết lập một phiên kết nối PPP:

- **Giai đoạn thiết lập kết nối;**Trong giai đoạn này mỗi thiết bị PPP gửi đi frame LCP để cấu hình và kiểm tra kết nối.Trong frame LCP có chứa các thông tin để các thiết bị có thể thoả thuận và thực hiện các cấu hình cho đường truyền, ví dụ: đơn vị truyền tối đa (MTU – Maximum transmission unit), nén dữ liệu và giao thức xác minh. Nếu không có thông tin gì nằm trong gói LCP thì đường truyền sẽ được thiết lập theo các thông số mặc định. Đường truyền phải được mở lên và cấu ình xong trước khi có thể truyền các gói dữ liệu lớp Mạng. Quá trình này dược kết thúc khi thông tin xác nhận cấu hình được gửi và nhận xong.
- **Giai đoạn xác minh:**(Giai đoạn này không bắt buộc phải có) Sauk hi đường truyền đã được thiết lập và giao thức xác minh đã được chọn xong, thiết bị ở hai đầu kết nối thực hiện xác mnh với nhau. Quá trình xác minh được thực hiện trước khi chuyển sang giai đoạn cấu hình giao thức lớp Mạng. Trong giai đoạn này LCP cũng thực hiện kiểm tra chất lượng đường truyền.
- **Giai đoạn câu hình giao thức lớp mang** Trong giai đoạn này các thiết bị PPP gửi gói NCP để chọn lựa và cấu hình cho một hay nhiều giao thức lớp Mạng, ví dụ như giao thức IP. Khi mỗi giao thức lớp Mạng được cấu hình xong thì gói dữ liệu của giao thức đó có thể được truyền đi trên đường truyền. Kết quả của lệnh show interfaces sẽ cho biết trạng thái của LCP và NCP trong cấu hình PPP

Một kết nối PPP sẽ được duy trì cho đến khi:
Frame LCP hay LCP đóng đường truyền

- Thời gian chờ đã hết hạn
- Sự can thiệp của người sử dụng

3.2.3 Giao thức xác minh PPP

Giai đoạn xác minh của một phiên kết nối PPP là không bắt buộc. Sauk hi đường truyền đã được thiết lập và giao thức xác minh đã được chọn thì hai thiết bị ở hai đầu kết nối thực hiện xác minh với nhau. Quá trình xác minh được thực hiện trước khi giai đoạn cấu hình giao thức lớp Mạng bắt đầu.

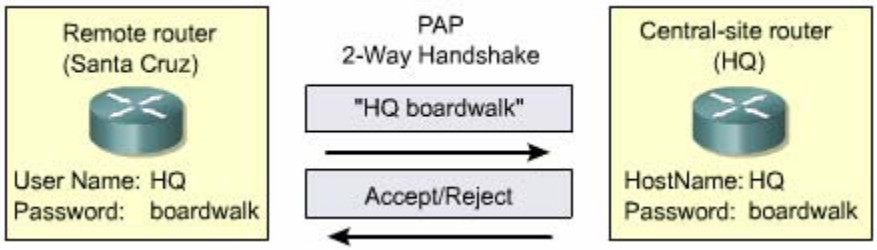
Khi thực hiện xác minh, bên thiết lập kết nối được yêu cầu cung cấp các thông tin để xác minh quyền thiết lập kết nối. Hai router ở hai đầu kêt nối sẽ trao đổi với nhau các thông điệp xác minh

Khi cấu hình quá trình xác minh PPP, người quản trị mạng có thể chọn giao thức PAP (Password Authentication Protocol) hay CHAP (Challenge Handshake Authentication Protocol). Nói chung Chap là giao thức thường được đề nghị hơn

3.2.4 PAP (Password Authentication Protocol)

PAP cung cấp một cơ chế xác minh đơn giản sử dụng quá trình bắt tay 2 bước. Sauk hi giai đoạn thiết lập kết nối PPP hoàn tất, cặp username/password được router ở đầu xa gửi đi nhiêu lần trên đường truyền cho đến khi đã được xác nhận hoặc kết nối bị xóa.

PAP không phải là một giao thức xác minh manh. Password được gửi đi nguyên mẫu trên đường truyền. Do đó không có gì khó khăn đối với các loại tấn công Playback hoặc repeated trial-and-error. Router đầu xa chỉ được kiểm tra một lần khi truy nhập

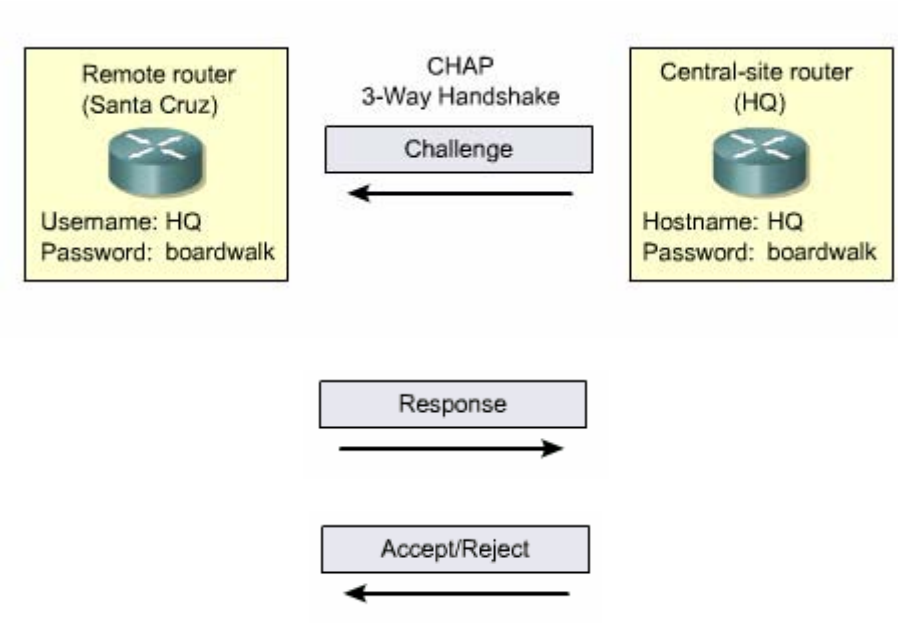


3.2.5 CHAP (Challenge Handshake Authentication Protocol)

Chap được sử dụng khi khởi động đường truyền và sau đó kiểm tra router đầu xa theo định kỳ với quá trình bắt tay 3 bước. CHAP được thực hiện ở lúc bắt đầu thiết lập kết nối và luôn được lặp lai trong suốt quá trình kết nối được duy trì.

Sau khi giai đoạn thiết lập kết nối PPP hoàn tất, router trung tâm gửi một thông điệp "thử thách" cho router đầu xa. Router đầu xa sử dụng thông điệp này với password của nó thông qua thuật toán MD5 (Message Digest) tạo ra một thông điệp trả lời. Router đầu xa gửi thông điệp trả lời này cho router trung tâm. Router trung tâm sử dụng thông điệp trả lời để tính toan ra một giá trị. Nếu giá trị này đúng với thông điệp "thử thách" ban đầu thì thông tin xác minh được xác nhận nếu khong thì kết nối sẽ bị xoá ngay

Chap chống được kiểu tấn công Playback vì giá trị của thông điệp "thử thách" là ngẫu nhiên hoàn toàn khác nhau giữa mỗi lần gửi và không thể đoán được. Do đó giá trị của thông điệp trả lời cũng ngẫu nhiên và riêng biệt. Việc xác minh được thực hiện lặp đi lặp lại để giới hạn thời gian tìm ra mật mã của các đợt tấn công đơn lẻ

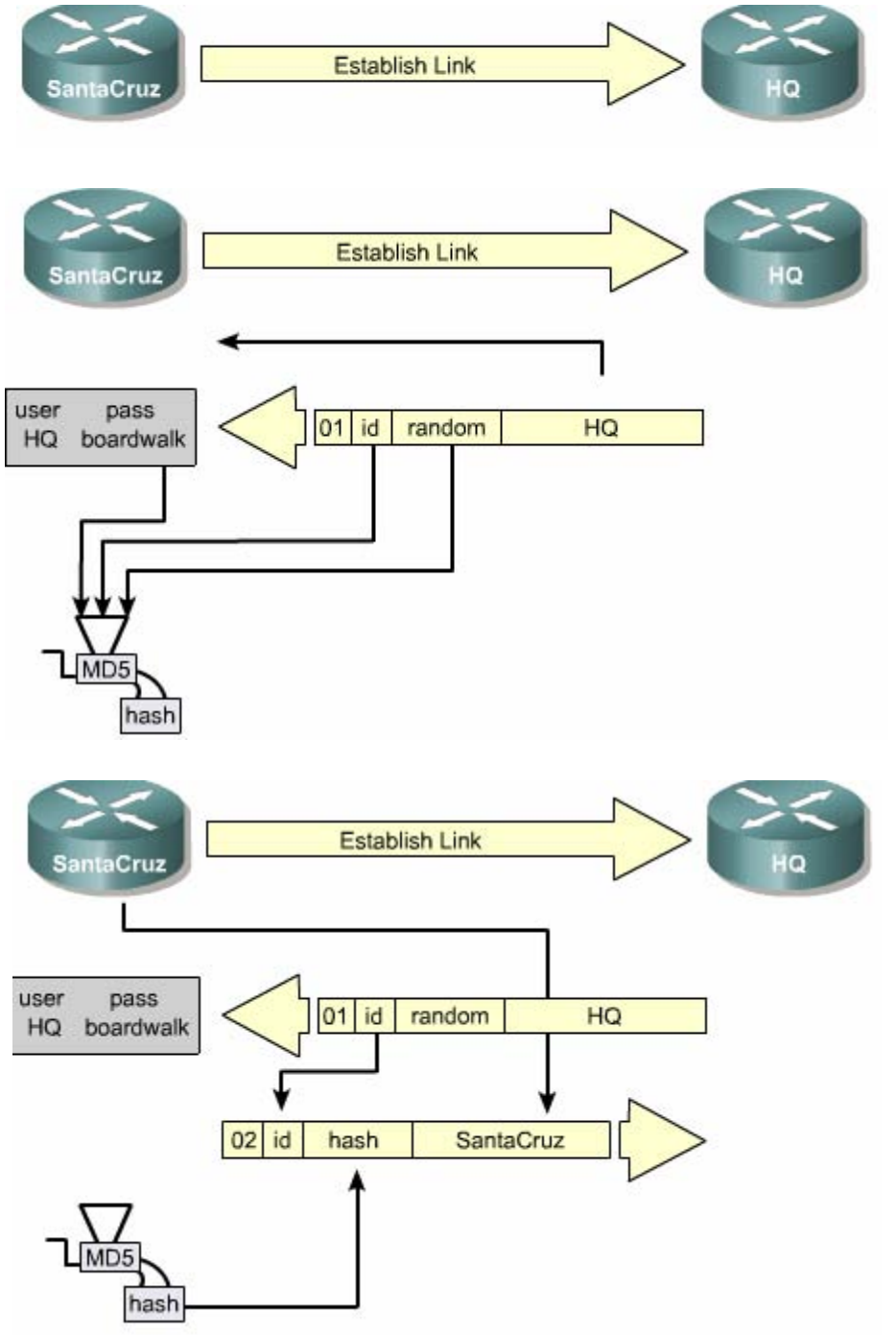


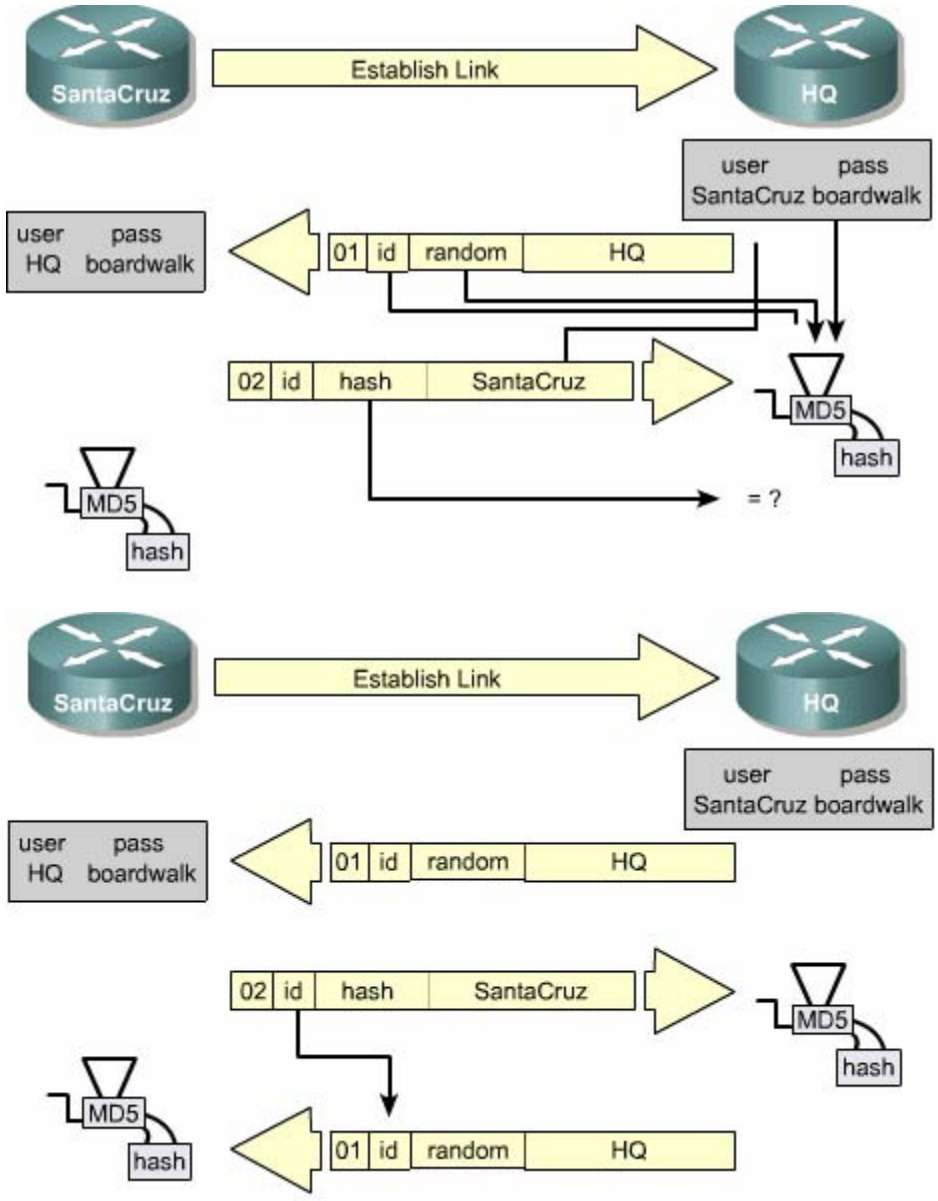
3.2.6 Quá trình thực hiện xác minh PPP

Sauk hi nhập lệnh encapsulation ppp thi bạn có thể thêm cấu hình cho quá trình xác minh PAP hoặc Chap. Nếu không cấu hình quá trình xác minh thì phiên kết nối PPP được bắt đầu ngay . Nếu bạn có cấu hình cho quá trình xác minh thì sẽ diễn ra như sau:

- Xác định giao thức xác minh
- Kiểm tra cơ sở dữ liệu để tìm cặp username/password tương ứng

- Nếu tín hiệu trả lời từ cơ sở dữ liệu là đúng thì phiên kết nối PPP được bắt đầu nếu không thì sẽ bị xoá ngay





3.3 Cấu hình PPP

3.3.1 Giới thiệu cấu hình PPP

Cấu hình PPP bao gồm các thông tin về : phương pháp xác minh, nén dữ liệu phát hiện lỗi có ghép kênh hay không

Các thành phần cấu hinh PPP	Chức năng	Giao thức	Lệnh cấu hình

Quá trình xác minh	Quá trình xác minh yêu cầu bên thiết lập kết nối cung cấp thông tin để xác minh quyền thực hiện kết nối . Hai router ở hai bên đầu kết nối trao đổi thông điệp xác minh. Có hai giao thức thực hiện xác minh là PAP và CHAP	PAP CHAP	Ppp Authentication Pap Ppp Authentication Chap
Nén dữ liệu	Nén dữ liệu giúp tăng thông lượng đường truyền PPP bằng cách giảm lượng dữ liệu được truyền đi trên đường truyền. Frame sẽ được giải nén ở đầu nhận. Hai giao thức nén dữ liệu chạy trên router Cisco là Stacker và Preditor	Stacker Predictor	Compress stac Compress Predictor
Phát hiện lỗi	Cơ chế phát hiện lỗi của PPP thực hiện quá trình kiểm tra điều kiện đường truyền. Chỉ số Quality Magic giúp xác định vòng lặp và độ tin cập của đường truyền		
Multilink	Phiên bản Cisco IOS 11.1 trở đi có hỗ trợ giao thức ghép kênh MP (Multilink protocol) Giao thức này cho phép chia sẻ tải trên các cổng của router đang sử dụng PPP. MP cắt gói dữ liệu thành nhiều phân đoạn có đánh số thứ tự và truyền trên các kênh song song. Các kênh PPP này hoạt	MP	Ppp multilink

	động như một kênh logic, giúp tăng thông lượng và giảm thời gian trễ giữa hai router		

3.3.2 Cấu hình PPP

Sau đây là ví dụ cho cấu hình đóng gói PPP trên cổng Serial (pp)

- Router # configure terminal
- Router (config) # interface serial 0/0
- Router (config –if)#encapsulation ppp

Chúng ta cũng có thể cấu hình phần mềm nén dữ liệu trên cổng Serial đang sử dụng đóng gói PPP. Nén dữ liệu được thực hiện bằng phần mềm. Chúng ta không nên sử dụng nén dữ liệu lần nữa khi bản than phần lớn dữ liệu được truyền đi trên cổng này đã được nén rồi.

- Router (config)#interface serial 0/0
- Router (config – if)#encapsulation ppp
- Router (config – if)# compress (predictor stac)

Chúng ta nhập lệnh sau để có thể theo dõi mức đọ rớt gói dữ liệu trên đường truyền và tránh bị vòng lặp:

- Router (config)#interface serial 0/0
- Router (config – if)#encapsulation ppp
- Router (config – if)#ppp quality p ercentage

Ch úng ta s ử d ụng c ác l ệnh sau đ ể cho ph ép th ực hi ện chia t ải tr ên nhi ều đ ư ờng k ết n ối:

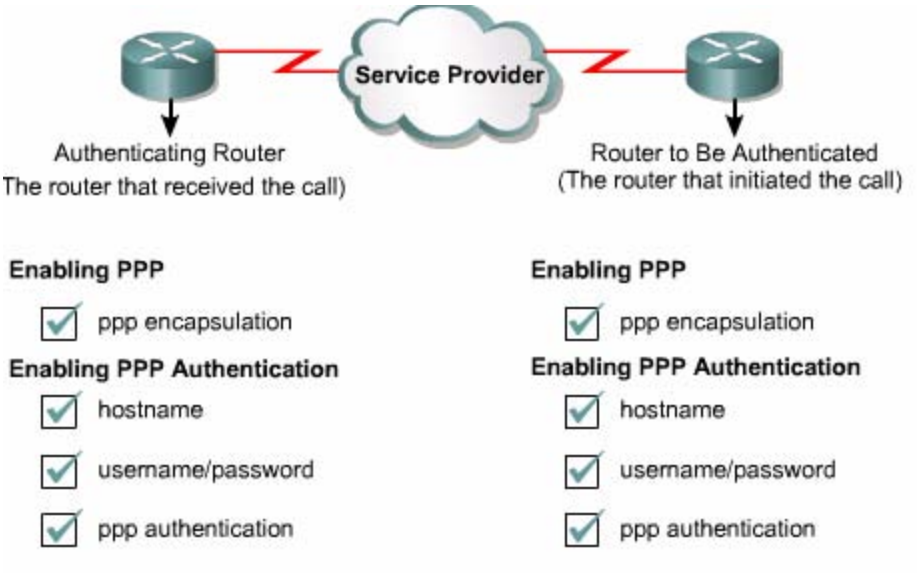
- Router (config)#interface serial 0/0
- Router (config – if)#encapsulation pp
- Rot er (c onfig – if) # ppp multilink

3.3.3 Cấu hình quá trình xác minh PPP

Bước	Mô tả
Bước 1	Trên mỗi router khai báo username và password của router kết nối vào nó

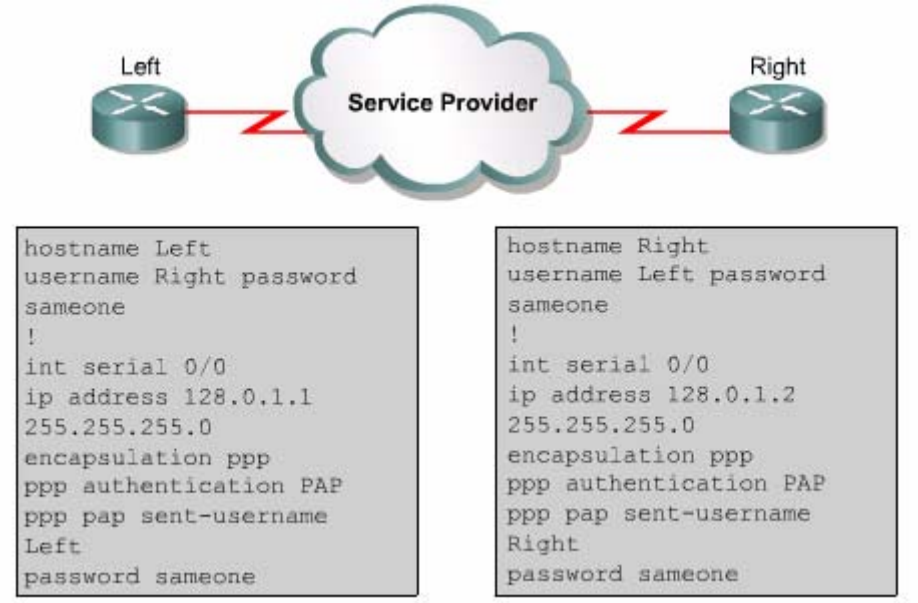
	Router (config)# username name password secret Name là tên của router kết nối vào router đang cấu hình
Bước 2	Vào chế độ câú hình của cổng tương ứng
Bước 3	Cấu hình đóng gói PPP cho cổng: Router (config – if) # encapsulation ppp
Bước 4	Cấu hình quá trình xác minh PPP
Bước 5	Nếu bạn khai báo cả CHAP và PAP thì tên nào được đặt trước sẽ được sử dụng trước. Nếu router đầu bên kia yêu cầu sử dụng phương thức thứ hai hoặc đơn giản là từ chối phương thức thứ nhất thì phương thức thứ hai sẽ được áp dụng.
Bước 6	Bắt đầu từ phiên bản Cisso IOS 11.1 trở đi bạn phải khởi động PAP trên cổng cần thiết mặc định là PAP không chạy trên router

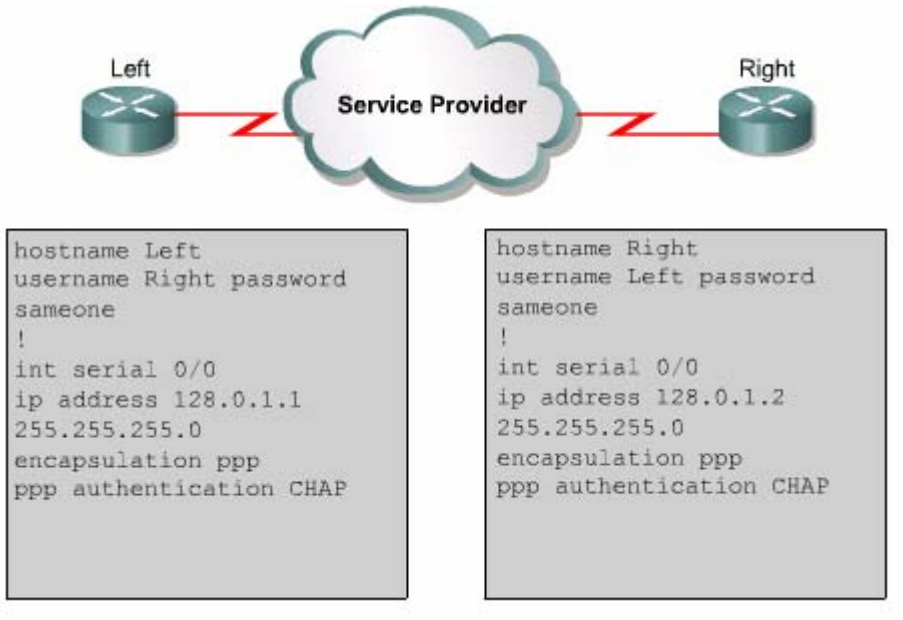
Hình 3.3..3.a là tóm tắt quá trình cấu hình PAP trên hai router kết nối với nhau. Cặp username/password trên mỗi router phải phù hợp với hostname và password được khai báo trên router kia.



PAP là phương thức xác minh đơn giản sử dụng hai bước bắt tay và được thực hiện khi thiết lập kết nối. Quá trình xác minh PAP thực hiện và đường truyền được thiết lập

CHAP thực hiện kiểm tra router kết nối ở đầu xa sử dụng ba bước bắt tay và được lặp lại theo định kì. Quá trình này được thực hiện xong lần đầu tiên. Đường truyền được thiết lập và luôn được lặp lại trong suốt quá trình kết nối





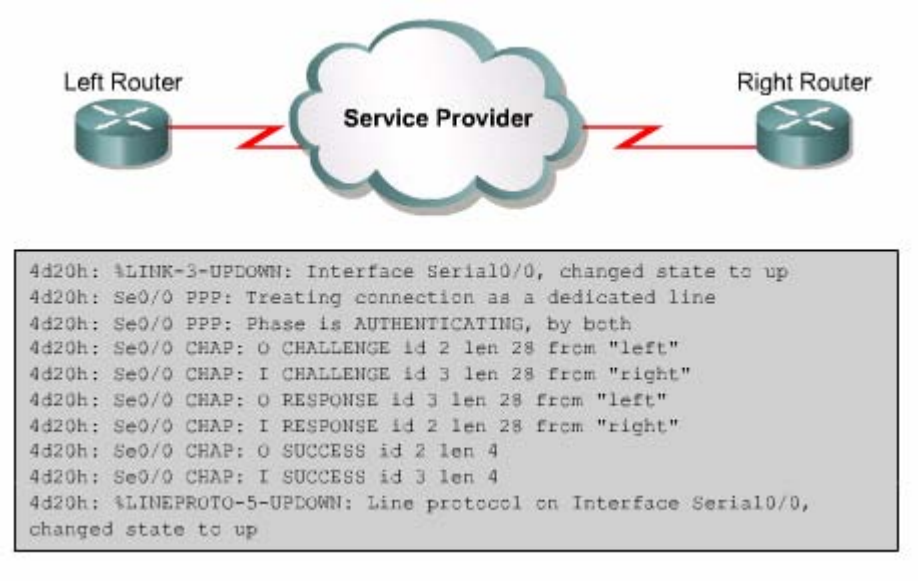
3.3.4 Kiểm tra cấu hình PPP trên cổng Serial

Chúng ta sử dụng lệnh show interfaces serial để kiểm tra cấu hình đóng gói HDLC hoặc PPP trên cổng Serial. Nếu cổng được cấu hinh đóng gói HDLC thì trong kết quả hiển thị có dòng “Encapsulation HDLC”. Ví dụ như trên hình 3.3.4 chúng ta thấy dòng “Encapsulation PPP” như vậy là cổng serial 0/0 đã được cấu hình đóng gói PPP. Sauk hi đã cấu hình PPP, chúng ta có thể kiểm tra trạng thái của LCP (Link Control Protocol) và NCP (Network Control Protocol) cũng bằng lệnh Show interfaces serial

```
Router#show interfaces serial0/0
Serial0/0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 10.140.1.2/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive
set (10 sec)
  LCP Open
  Open: IPCP, CDPCP
  Last input 00:00:05, output 00:00:05, output
hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0
drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     38021 packets input, 5656110 bytes, 0 no
buffer
     Received 23488 broadcasts, 0 runts, 0 giants,
0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0
ignored, 0 abort
     38097 packets output, 2135697 bytes, 0
underruns
     0 output errors, 0 collisions, 6045 interface
resets
     0 output buffer failures, 0 output buffers
swapped out
     482 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

3.3.5 Xử lý sự cố trên cổng Serial

lệnh debug ppp authentication hiển thị các hoạt động xảy ra của qúa trình xác minh. Ví dụ như trên hình 3.3..5.a là kết quả cho thấy quá trình hoạt động của CHAP trên router Left Router Left và router Right được cấu hình thực hiện xác minh hai chiều, do đó hai router này thực hiện xác minh lẫn nhau



Hìn 3.3.5. Kết quả hiển thị của lệnh debug ppp authentication trên router Left.

Kết quả hiển thị	Giải thích
Se0/0 PPP: Phase is AUTHENTICATION by both	Xác minh hai chiều
Se0/0 PAP: O AUTH-REQ id 4 ‘len 18 from “left”	Yêu cầu xác minh được gửi ra cổng Serial 0/0.
Se0/0 PAP: I AUTH-REQ id 1 ‘len 18 from “left”	Yêu cầu xác minh nhận được từ cổng Serial 0/0.
Se0/0 PAP: Authentication peer right	Nhận được thông điệp trả lời của yêu cầu xác minh.
Se0/0 PAP: O AUTH-ACK id 1 len 5	Gửi thông điệp xác nhận
Se0/0 PAP: I AUTH-ACK id 4 len 5	Nhận được thông điệp xác nhận

Bảng 3.3.5. Giải thích kết quả hiển thị của lệnh debig ppp authentiacation

Lệnh debug ppp được sử dụng để hiển thị các hoạt động của PPP . Chúng ta có thể dungdạng no của câu lệnh này để kết thúc quá trình hiển thị của lệnh

Tổng kết

Sau đây là những điểm quan trọng trong chương này mà các bạn cần nắm được:

- Ghép kênh theo thời gian
- Điểm ranh giới trong mạng WAN
- Định nghĩa chức năng của DTE và DCE
- Quá trình phát triển của giao thức đóng gói HDLC
- Sử dụng lệnh encapsulation hdlc để cấu hình HDLC
- Sử dụng lệnh show interface và show controllers khi xác định sự cố trên cổng serial
- Ưu điểm của giao thức PPP
- Chức năng của LCP và NCP trong PPP
- Cấu trúc frame PPP
- Ba giai đoạn thiết lập một phiên kết nối PPP
- Sự khác nhau giữa PAP và CHAP
- Cấu hình PPP
- Cấu hình PAP và Chap
- Sử dụng lệnh show interface serial để kiểm tra cấu ình đóng gói trên cổng serial
- Sử dụng lệnh debug ppp để xác định sự cố ppp

CHƯƠNG 4: ISDN và DDR

GIỚI THIỆU

ISDN là mạng cung cấp kết nối toàn số từ đầu đến cuối để thực hiện dịch vụ truyền thoại và số liệu

ISDN cho phép nhiều kênh kỹ thuật số cùng hoạt động đồng thời trên một đường cáp điện thoại thông thường, nhưng ISDN truyền tín hiệu số chứ không truyền tín hiệu tương tự. Thời gian trễ trên đương ISDN cũng thấp hơn so với đường truyền tín hiệu tương tự

Khi chúng a không có nhu cầu cần một đường truyền thường trực thì nên sử dụng DDR để tiết kiệm chi phi. DDR định nghĩa một tiến trình cho router thực hiện kết nối với mạng quay số khi có dữ liệu cầu truyền đi và ngắt kết nối khi việc truyền dữ liệu đã hoàn tất

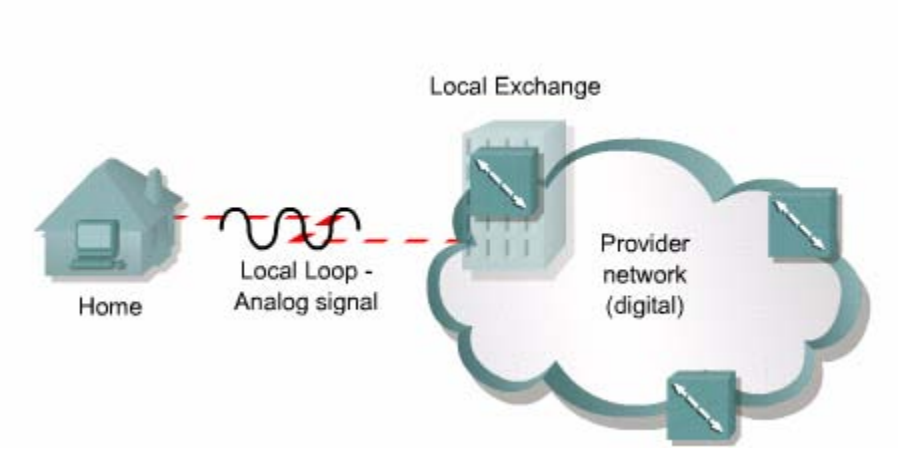
Sau khi kết thúc chương này các bạn có thể thực hiện những việc sau:

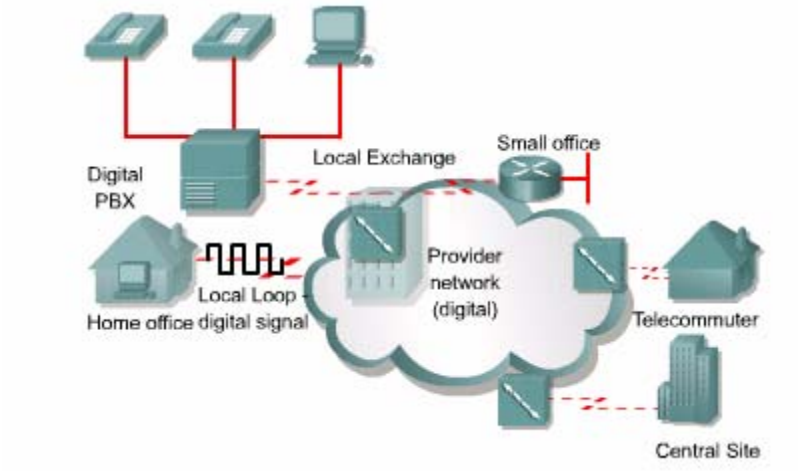
- Định nghĩa các chuẩn ISDN về địa chỉ, tín hiệu
- Mô tả ISDN sử dụng lớp Vật lys và lớp Liên kết dữ liệu như thế nào
- Liệt kê các điểm kết nối và các giao tiếp được sử dụng trong ISDN
- Cấu hình cổng trên router để sử dụng ISDN
- Xác định các lưu lượng được phép truyền đi khi cấu hình DDR
- Cấu hình định tuyến cố định cho DDR
- Xác định và áp dụng danh sách kiểm tra truy cập ACL, cho các lưu lượng DDR
- Cấu hình cổng quay số

4.1 Các định nghĩa của ISDN

4.1.1 Giới thiệu ISDN

Có rất nhiều công nghệ WAN cung cấp đường truy cập mạng từ xa. Một trong những công nghệ đó là ISDN. Những người sử dụng riêng lẻ hay những văn phòng nhỏ chỉ có đường điện thoại truyền thông băng thông thấp. ISDN là giải pháp dành cho những đối tượng này





Đường điện thoại truyền thông PSTN truyền tín hiệu tương tự trên mạch vòng nội bộ kết nối giữa thuê bao và mạng của công ty điện thoại. Mạch tín hiệu tương tự có giới hạn băng thông không được lớn hơn 3000Hz. Công nghệ ISDN cho phép truyền tín hiệu số trên mạch vòng nội bộ này tốc độ truy cập cao hơn. Các côngty điện thoại chỉ cần nâng cấp các bộ chuyển mạch để có thể xử lý được tín hiệu số. ISDN thường được các văn phòng nhỏ ở xa sử dụng để kết nối vào mạng LAN ở trung tâm

Các công ty điện thoại cũng đã phát triển các chuẩn cho ISDN. Các chuẩn ISDN định nghĩa về thiết bị phần cứng và quá trình thiết lập cuộc gọi. Những chuẩn này giúp cho mạng ISDN giao tiếp dễ dàng với các mạng khác trên toàn cầu. Trong mạng ISDN việc số hoá tín hiệu được thực hiện ngay bên phía thuê bao thay vì được thực hiện bên phía nhà cung cấp dịch vụ như trước đây

Sau đây là một số ưu điểm của ISDN:

- Truyền nhiều loại lưu lượng khác nhau bao gồm dữ liệu thoại và và video
- Tốc độ thiết lập cuộc gọi nhanh hơn modem
- Kênh B cung cấp tốc độ truyền dữ liệu nhanh hơn modem
- Kênh B phù hợp với kết nối PPP

ISDN là một dịch vụ linh hoạt có thể truyền dữ liệu thoại và video cho phép truyền nhiều loại lưu lượng trên nhiều kênh khác nhau trên cùng một kết nối

ISDN sử dụng một kênh riêng được gọi là kênh D để truyền tín hiệu điều khiển. Khi cần thiết lập cuộc gọi thuê bao nhấn số cần gọi . Khi tất cả các chữ số đã được nhận đầy đủ thì cuộc gọi được thực hiện. ISDN truyền các số này trên kênh D do đó thời gian thiết lập cuộc gọi nhanh hơn

Mỗi kênh B có thể kết nối đến một điểm khác nhau trong mạng ISDN. PPP có thể hoạt động cả trên kết nối đồng bộ và bất đồng bộ do đó đường truyền ISDN có thể sử dụng kết hợp với đóng gói PPP

4.1.2 Các chuẩn ISDN và phương pháp truy cập

Công việc chuẩn hoá ISDN được bắt đầu từ cuối thập niên 60. Các bộ chuẩn đề nghị của ISDN được xuất bản năm 1994 và sau đó liên tục được cập nhật bởi ITU-T. Các chuẩn ISDN là một tập hợp các giao thức về điện thoại kỹ thuật số và truyền số liệu. Các giao thức ISDN được phân theo các chủ đề chính sau:

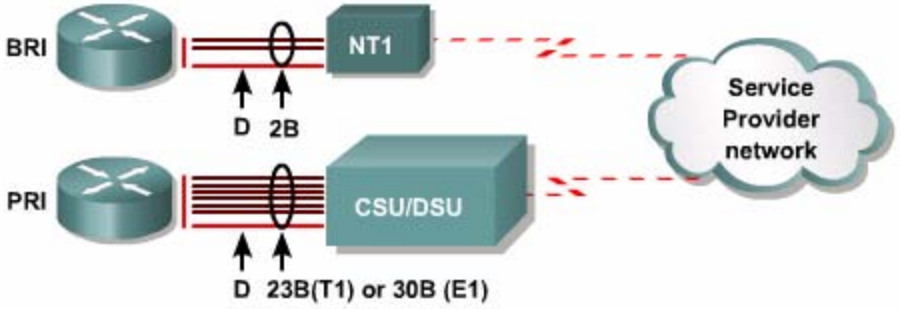
- Bộ giao thức E- các chuẩn về mạng điện thoại cho ISDN. Ví dụ: E:164 là giao thức mô tả địa chỉ quốc tế cho ISDN
- Bộ giao thức I- Liên quan đến các khái niệm thuật ngữ ví dụ I.100 bao gồm các khái niệm chung của ISDN và cấu trúc các giao thức I khác I:200 đề cập đến mặt dịch vụ của ISDN
- Bộ giao thức Q - Đề cập đến hoạt động tín hiệu và chuyển mạch. Hoạt động tín hiệu ở đây có nghĩa là quá trình thiết lập cuộc gọi ISDN

Chuẩn ISDN định nghĩa hai loại kênh chính, mỗi loại có tốc độ truyền khác nhau Kênh B, 64Kb/giây, được sử dụng để truyền mọi dữ liệu số với chế độ truyền song công. Loại kênh thứ hai được gọi là kênh D

Khi thiết lập một kết nối TCP 2 bên trao đổi các thông tin điều khiển để thiết lập kết nối. Các thông tin điều khiển này truyền trên kênh truyền mà sau đó cũng được sử dụng để truyền dữ liệu. Thông tin điều khiển và dữ liệu chia sẻ cùng một kênh truyền. Dạng truyền như vậy được gọi là in-band signaling. ISDN thì không thực

hiện truyền như vậy, mà sử dụng một kênh riêng chính là kênh D, để truyền tín hiệu điều khiển. Dạng truyền như vậy gọi là out – of – band signaling

ISDN định nghĩa hai phương pháp truy cập chuẩn là BRI và PRI. Một cổng BRI hay PRI cung cấp một kênh D và nhiều kênh B



Channel	Capacity	Mostly Used for
B	64 kbps	Circuit-switched data (HDLC, PPP)
D	16/64 kbps	Signaling information (LAPD)

BRI sử dụng hai kênh B 64kb/giây và một kênh D 16kb/giây. BRI hoạt động được trên nhiều Cisco router và đôi khi được ký hiệu là 2B+D

Kênh B có thể được sử dụng để truyền thoại . Khi đó tín hiệu thoại được mã hoá theo cách đặc biệt. Khi kênh B được sử dụng để truyền số liệu thì thông tin được đóng thành frame, sử dụng giao thức đóng gói HDLC hoặc PPP ở lớp 2. PPP phức tạp hơn HDLC vì nó cung cáp cơ chế xác minh, thoả thuận cấu hình kết nối và giao thức phù hợp

ISDN được xem là một kết nối chuyển mạch .Kênh D mang các thông điệp điều khiển để thiết lập cuộc gọi ngắt cuộc gọi và điều khiển cuộc gọi cho kênh B. Lưu lượng trên kênh D sử dụng giao thức LAPD. LAPD là một giao thức lớn liên kết dữ liệu dựa trên cơ sở của HDLC.

Ở Bắc mỹ và Nhật, PRI cung cấp 23 kênh B 64kb/giây và một kênh D 64kb/giây. Một PRI này cung cấp dịch vụ tương đương với một kết nối T hay DSL. Ở Châu âu và phần còn lại trên thế giới , PRI cung cấp 30 kênh B và một kênh D, tương đương với một kết nối E1. PRI sử dụng CSU/DSU cho kết nối T1/E1

4.1.3 Mô hình 3 lớp ISDN và các giao thức tương ứng

OSI Layer	D-Channel	B-Channel
3	Q.931 - ISDN Network Layer between Terminal and Switch	IP
2	Q.921 – LAPD (Link Access Procedure on the D channel)	PPP HDLC
1	I.430/I.431 – ISDN physical-layer interface: • I.430 for the basic interface • I.431 for the primary interface	

ISDN hoạt đọng theo các chuẩn ITU-T tương úng với lớp Vật lý lớp liên kết dữ liệu và lớp Mạng trong mô hình OSI

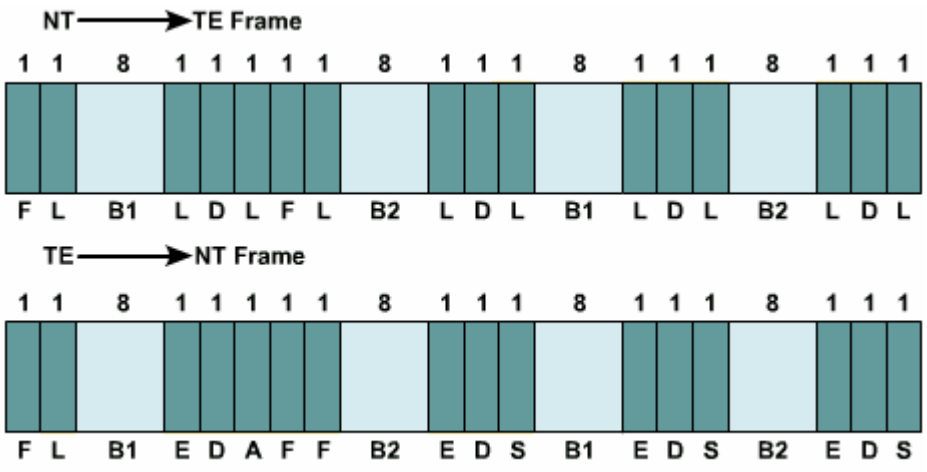
- Chuẩn lớp Vật ly của ISDN BRI và PRI được định nghĩa trong ITU –T I.430 và I..431
- Chuẩn lớp liên kế dữ liệu của ISDN dựa trên cơ sở LAPD và được định nghĩa trong:

- ITU-T Q.920
- ITU-T Q.921
- ITU-T Q.922
- ITU-T Q.923

- Chu ẩn l ớp M ạng của ISDN được định nghĩa trong ITU-T Q.930 hay I.450 và ITU-T Q.931 hay I.451. Các chuẩn này quy ước về kết nối từ user đến user chuyển mạch và chuyển mạch gói.

Dịch vụ BRI được thực hiện trên cáp điện thoại truyền thông. Mặc dù chỉ có một đường truyền vật lý cho một BRI nhưng bên trong là ba kênh truyền thông tin khác nhau 2B+D

Định dạng frame ở lớp Vật lý ISDN khác nhau tuỳ theo frame đi vào hay frame đi ra. Nếu là frame đi ra có nghĩa là frame được truyền từ thiết bị đầu cuối đến mạng ISDN thì sử dụng định dạng frame TE. Nếu là frame đi vào có nghĩa là frame được truyền từ mạng ISDN đến thiết bị đầu cuối thì sử dụng định dạng frame NT



Hình 4.1.3.b

Mỗi frame ISDN BRI chứa hai frame con trong đó mỗi frame con có:

- 8 bit của kênh B1
- 8 bit của kênh B2
- 2 bit của kênh D
- 6 bit chèn thêm

Do đó mỗi frame ISDN BRI có 48 bit , 4000 frame được truyền đi mỗi giây. Mỗi kênh B có dung lượng là 8*4000*2=64kb/giây trong khi đó kênh D có dung lượng là 2*4000*2=16kb/giây. Dung lượng tổng cộng (B1+b2+D) là 144kb/giây, trên một cổng vật lý ISDN có dung lượng là 192kb/giây. Phần dung lượng chênh lệch còn lại là của các bit chèn thêm:6*4000*2=48kb/giây

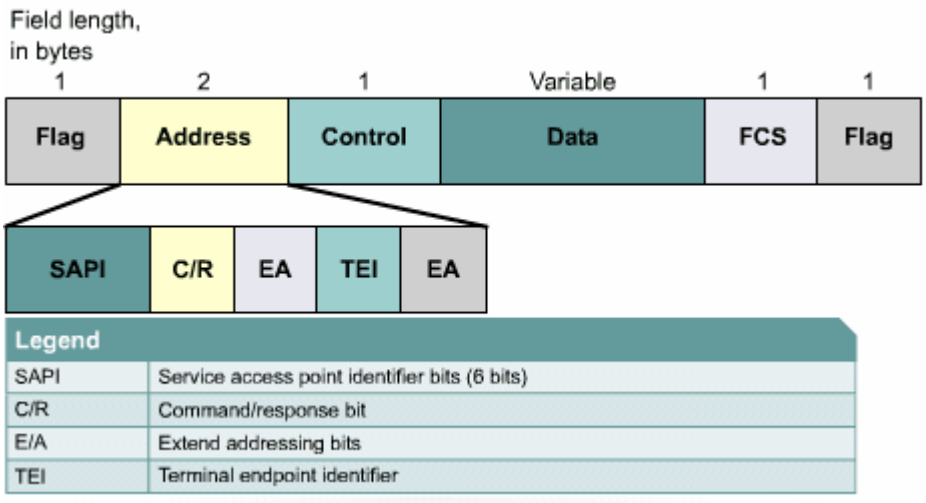
Các bit chèn thêm trong mỗi frame con ISDN có chức năng như sau

- Framing bit - thực hiện chức năng đồng bộ
- Load balancing bit – điêu chỉnh giá trị bit trung bình
- Echo of previous D channel bit- giúp phân biệt tín hiệu của từng thiết bị khi có nhiều thiết bị đầu cuối kết nối vào một đường truyền
- Activation bit- kích hoạt thiết bị
- Spare bit- bit để dành, chưa có chức năng nào được gắn cho bit này

Chúng ta cần lưu ý rằng: tốc độ vật lý của , cổng BRI là 48*4000=192kb/giây, tốc độ truyền dữ liệu là 144kb/giây=64kb/giây+64kb/giây+16kb/giây(2B+D)

Giao thức lớp 2 của kênh tín hiệu ISDN là LAPD. LAPD tương ứng như HDLC. LAPD được sử dụng trên kênh D để đảm bảo cho việc truyền và nhận tín hiệu điều khiển

Phần Cờ và phần điều khiển của LAPD tương ứng như HDLC, phần địa chỉ của LAPD dài 2 byte. Trong đó byte đầu tiên chứa chỉ số xác định điểm truy cập dịch vụ, là chỉ số port giao tiếp giữa dịch vụ LAPD và Lớp 3 . Bit yêu cầu/ đáp ứng (C/R) cho biết frame này là frame yêu cầu hay frame đáp ứng. Byte thứ 2 chứa chỉ số xác định điểm cuối (TEI). Mỗi thiết bị đầu cuối của khách hang cần phải có một chỉ số riêng biệt. Chỉ số TEI này có thể được cấu hình cố định khi cài đặt hoặc được switch cung cấp động mỗi khi thiết bị này khởi động. Nếu TEI được cấu hình cố định khi cài đặt thì chỉ số này nằm trong khoảng từ o đến 63. Chỉ số TEI cấp động nằm trong khoảng từ 64 đến 126. Chỉ số TEI 127 là địa chỉ quảng bá

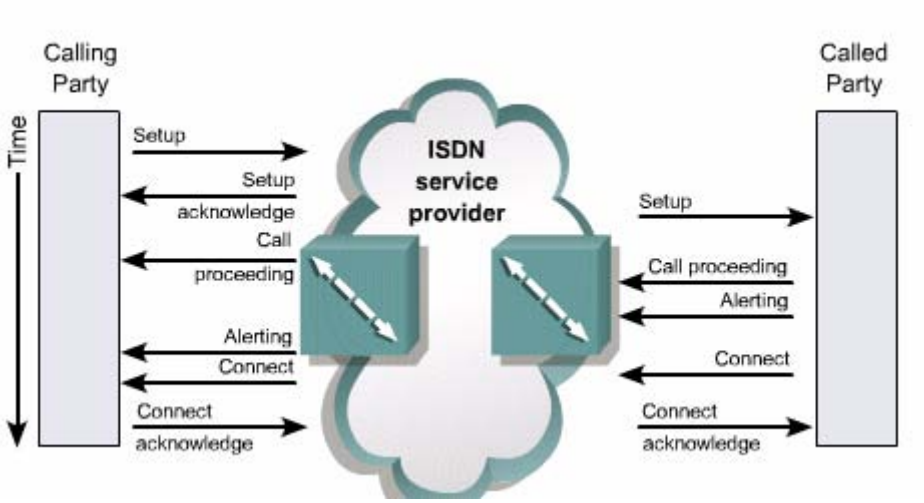


4.1.4 Các hoạt động trong ISDN

Có nhiều hoạt động trao đổi thông tin diễn ra khi một router sử dụng ISDN để kết nối đến router khác. Kênh D được sử dụng để thiết lập kết nối giữa router và ISDN switch. Tín hiệu SS7 được sử dụng giữa các switch trong mạng của nhà cung cấp dịch vụ

Kênh D giữa router và ISDN switch luôn luôn trong trạng thái hoạt động. Q.921 mô tả tiến trình hoạt động của LAPD ở lớp 2 của mô hình OSI. Kênh D được sử dụng để truyền tín hiệu khiển như thiết lập cuộc gọi kết thúc cuộc gọi điều khiển

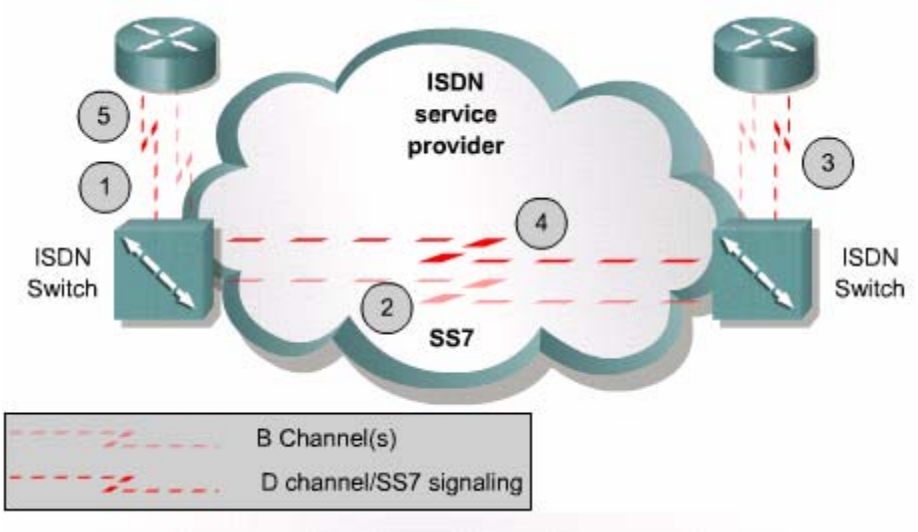
cuộc gọi. Những chức năng này định nghĩa trong giao thức Q.931 ở lớp 3 của mô hình OSI.Q.931 định nghĩa kết nối mạng giữa thiết bị đầu cuối và ISDN switch nhung không định nghĩa kết nối đầu cuối -đến-đầu cuối. Có nhiều ISDN switch đã được phát triển trước khi Q.931 được chuẩn hoá, do đó có nhiều nhà cungcấp dịch vụ ISDN và nhiều loại ISDN switch triển khai Q.931 khác nhau. Cũng chính vì không có chuẩn chungcho loại ISDN switch nên trong cấu hình router phải có câu lệnh khai báo ISDN switch mà router kết nối đến.



Hình 4.1.4.a

Sau đây là thứ tự các bước diễn ra trong quá trình thiết lập một cuộc gọi BRI hoặc PRI

1. Kênh D gửi số cần gọi đến cho ISDN switch nội bộ
2. Switch nội bộ sử dụng giao thức tín hiệu SS7 để thiết lập đường truyền và chuyển số cần gọi cho ISDN switch đầu xa
3. ISDN switch đầu xa chuyển tín hệu đến cho máy đích trên kênh D
4. Thiết bị đích ISDN NT – 1 gửi thông điệp kết nối cuộc gọi cho ISDN switch đầu xa
5. ISDN switch đầu xa sử dụng SS7 để gửi thông điệp kết nối cuộc gọi cho switch nội bộ
6. ISDN switch nội bộ thực hiện kết nối một kênh B, kênh B còn lại dành cho kết nối mới. Cả hai kênh B cũng có thể được sử dụng đồng thời.



Hình 4.1.4b

4.1.5 Các điểm liên kết trong ISDN

Chuẩn ISDN định nghĩa các nhóm chức năng là các nhóm thiết bị phần cứng cho phép user truy cập dịch PRI. Các hang sản xuất có thể tạo ra một thi bị phần cứng thực hiện một hoặc nhiều chức năng. Chuẩn ISDN cũng định nghĩa bốn điểm liên kết giữa các thiết bị ISDN. Mỗi thiết bị trong mạng ISDN thực hiện một nhiệm vụ để tạo nên một kết nối đầu cuối - đến - đầu cuối

Để kết nối các thiết bị khác nhau với các chức năng khác nhau các điểm giao tiếp giữa hai thiết bị phải được chuẩn hoá. Các điểm giao tiếp bên phía khách hang trong kết nối ISDN bao gồm những điểm sau:

- R – là điểm liên kết giữa thiết bị đầu cuối loại 2 (TE2 – Terminal Equipment (ty

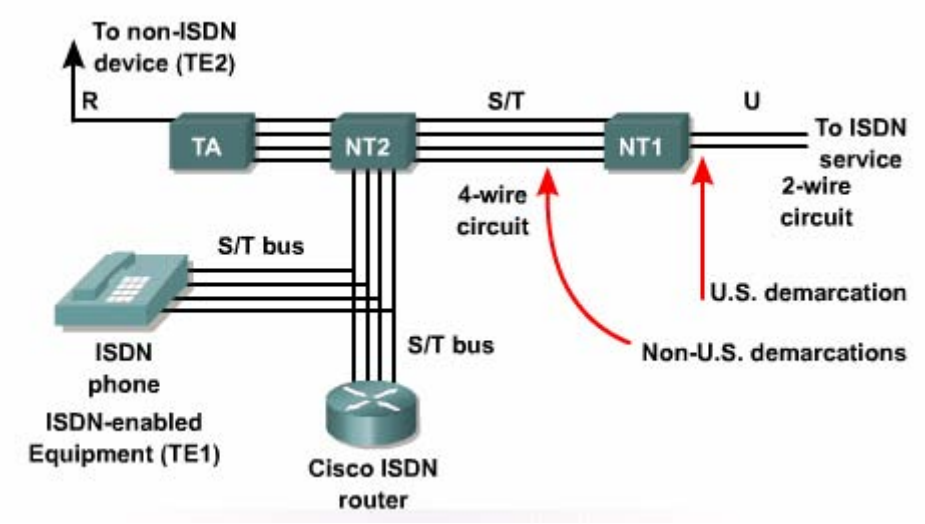
Pe 2) không tương thích với ISDN và thiết bị chuyển đổi TA (Terminal Adapter)

- S – là điểm kết nối vào thiết bị chuyển mạch của khách hang NT2 (Network Termination 2) và cho phép thực hiện cuộc gọi giữa nhiều loại thiết bị khác nhau của khách hang
- T - Tương tự như giao tiếp S về mặt tín hiệu điện. Đây là điểm kết nối từ NT2 vào mạng ISDN hay cho NT1 (Network Termination type 1)
- U – là điểm kết nối giữa NT1 và mạng ISDN của nhà cung cấp dịch vụ

Điểm giao tiếp S và T tương tự nhau về mặt tín hiệu điện nên có nhiều cổng giao tiếp dán nhã là S/T. Mặc dù hai giao tiếp này thực hiện chức năng khác nhau

nhưng do tương tự nhau về mặt tín hiệu điện nên có thể dùng chung cho cả hai chức năng.

Thiết bị	Loại thiết bị	Chức năng của thiết bị
TE1	Terminal Equipment 1 - Thiết bị đầu cuối loại 1	Thiết bị đầu cuối có cổng tương thích với ISDN, ví dụ như ISDN router, điện thoại ISDN
TE2	Terminal Equipment 2 - Thiết bị đầu cuối loại 2	Thiết bị đầu cuối không có cổng tương thích với ISDN. Để kết nối loại thiết bị đầu cuối này vào mạng ISDN thì cần phải có thiết bị chuyển đổi TA
TA	Terminal Adapter - Thiếtbị chuyển đổi	Chuyển đổi tín hiệu EIA/TIA – 232, V.35 và các loại tín hiệu khác sang tín hiệu BRI
NT2	Network Termination 2 - Thiết bị kết cuối mạng loại 2	Là điểm tập trung mọi đường dâyISDN phia khách hang và thực hiện chuyển mạch giữa các thiết bị đầu cuối bằng switch của khách hang
NT1	Network Termination 1 - thiết bị kết cuối mạng loại 1	Điều khiển kết cuối về mặt vật lý và tín hiệu điện phía khách hang Chuyển đổi tín hiệu BRI dây sang tín hiệu 2 dây



4.1.6. Xác định cổng ISDN trên router

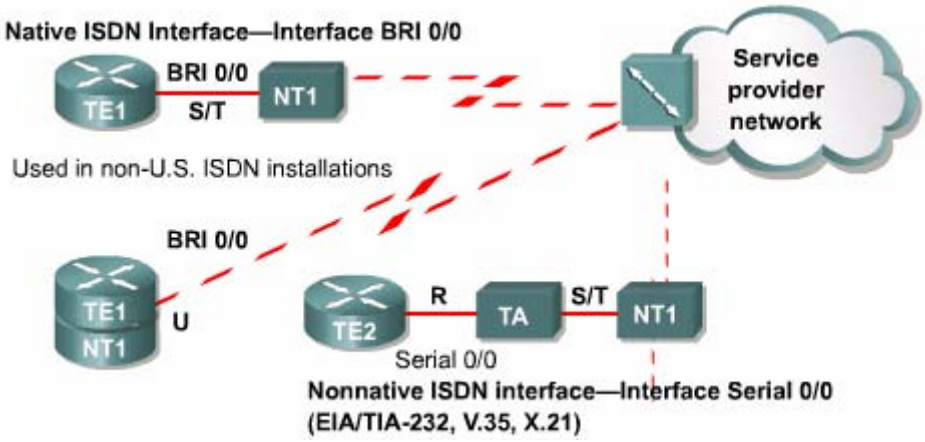
Ở BẮC Mỹ, NT1 là thiết bị thuộc sở hữu của khách hang. Điều này có nghĩa là khách hang phải cung cấp thiết bị có tích hợp chức năng của NT1. Do đó ở Bắc Mỹ các router ISDN thường có cổng ISDN BRI U trong đó có tích hợ chức năng của NT1. Ở Châu Âu , nhà cung cấp dich vụ cung cấp thiết bị NT1 riêng. Do đó, phía khách hàng chỉ cần cung cấp thiết bị có thể kết nối vào NT1, ví dụ như router có cổng ISDN BRI S/T.

Để chọn Cisco router có cổng ISDN phù hợp, các bạn cần đi theo các bước sau:

1. Xác định vị trí cổng ISDN BRI trên router. Chúng ta nhìn phía sau router để xách định vị trị cổng BRI hoặc vị trí để gắn BRI WAN Interface (WIC).

2. Xác định ai là người cung cấp NT1. NT1 là điểm kết nối của mạch vòng nội bộ đến tổng đài trung tâm của nhà cung cấp dich vụ. Ở Bắc Mỹ, NT1 thuộc phần sở hữu của khách hàng. Còn ở Châu Âu, nhà cung cấp dịch vụ sẽ cung cấp thiết bị NT1 riêng.

3. Nếu NT1 thuộc phía khách hàng thì nên chọn router có cổng U. Nếu router có cổng S/T thì cần phải có NT1 bên ngoài để kết nối router vào mạng ISDN của nhà cung cấp dich vụ.



Hình 4.1.6

Nếu router có cổng BRI thì có nghĩa là nó đã sẵn sàng để sử dụng ISDN Router như vậy chính là TE1 và có thể kết nối trực tiếp vào NT1. Nếu trên router đã có cổng U có nghĩa là đã tích hợp luôn NT1 bên trong

Nếu router không có cổng BRI và thuộc loại cấu trúc cố định, không thể gắn thêm card bên ngoài vào thì chúng ta bắt buộc phải sử dụng cổng Serial. Khi đó chúng ta cần phải có thêm thiết bị đổi TA bên ngoài để có thể thực hiện kết nối BRI trên cổng Serial. Nếu router có khả năng gắn thêm card bên ngoài thì chúng ta có thể gắn thêm card BRI WIC cho router

4.1.7 Các loại ISDN switch

Router cần phải có được khai báo loại switch mà nó giao tiếp. Có rất nhiều loại ISDN switch khác nhau tuỳ theo từng nơi. Do sự triển khai Q.931 khác nhau nên giao thức tín hiệu kênh D trên mỗi loại switch của mỗi hang cũng khác nhau

Dịch vụ được cungcấp bởi các nhà cung cấp dịch vụ ISDN rất khác nhau theo từng quốc gia và từng vùng trên thế giới. Giống như modem mỗi loại switch hoạt động khác nhau và có yêu cầu thiết lập cuộc gọi khác nhau. Trước khi router có thể kết nối vào dịch vụ ISDN nó cần phải được khai báo loại switch đang được sử dụng ở tổng đài của nhà cung cấp dịch vụ. Thông tin này phải được khai báo khi cấu hình router sau đó router có thể giao tiếp với switch để thiết lập cuộc gọi và gửi dữ liệu

Country	Switch Type
United States and Canada	AT&T 5ESS and 4ESS; Northern Telecom DMS-100
France	VN2, VN3
Japan	NTT
United Kingdom	Net3 and Net5
Europe	Net3

Hình 4.1.7

Ngoài việc xác định loại switch của nhà cungcấp dịch vụ, chúng ta còn phải biết số SPID là chỉ số được cung cấp bởi nhà cung cấp dịch vụ ISDN, được dùng để xác định cấu hình dịch vụ BRI cho mỗi kết nối.SPID cho phép thực hiện nhiều thiết bị ISDN cùng chia sẻ một kết nối. Switch DMS – 100 và National ISD- 1 thường yêu cầu phải có số SPID

SPID chỉ được sử dụng ở Bắc Mỹ và Nhật. Nhà cung cấp dịch vụ ISDN cung cấp số SPID để xác định cấu hình dịch vụ ISDN trên mỗi kết nố. Do đó trong nhiều trường hợp chúng ta cần phải nhập số SPID khi cấu hình router

Mỗi số SPID tương ứng với một cấu hình cho một kết nối. Số SPID bao gồm nhiều ký tự thường hay giống như số điện thoại. Mỗi số SPID xác định một kênh B cho switch ở tổng đài trung tâm. Một khi đã được xác định, switch sẽ cung cấp dịch vụ cho kết nối. Các bạn nên nhớ ISDN là loại kết nối quay số. Số SPID được xử lý khi router thiết lập kết nối với ISDN switch. nếu loại switch này yêu cầu phải có số SPID mà số SPID lại không được khai báo đúng thì quá trình thiết lập kết nối sẽ không thực hiện được, dịch vụ ISDN cũng không sử dụng được

4.2 Cấu hình ISDN

4.2.1 Cấu hình ISDN BRI

Lệnh ISDN switch type là câu lệnh khai báo loại ISDN switch mà router cần kết nối đến. Câu lệnh này có thể sử dụng ở chế độ cấu hình toàn cục hay ở chế độ cấu hình cổng BRI. Nếu khai báo câu lệnh này ở chế độ cấu hình toàn cục thì mọi cổng ISDN trên router đều sẽ có áp dụng loại ISDN switch được khai báo. Chúng ta cũng có thể khai báo loại ISDN switch riêng tương ứng cho từng cổng BRI. Sau

đây là ví dụ về câu lệnh khai báo loại switch National ISDN – 1 ở chế độ cấu hình toàn cục:

Sau khi lắp đặt dịch vụ ISDN xong, nhà cung cấp dịch vụ sẽ cho biết các thông tin về loại ISDN switch và số SPID. Mỗi số SPID định nghĩa một cấu hình dịch vụ tương ứng cho mỗi khác thuê báo. Tuy theo từng loại switch mà ta có thể cần hoặc không cần khai báo số SPID trong cấu hình router. Switch loại National ISDN – 1 và DMS – 100 đòi hỏi phải có số SPID nhưng switch AT&T 5ESS thì không cần số SPID

Định dạng của số SPID cũng phụ thuộc vào loại ISDN switch và quy ước của nhà cung cấp dịch vụ. Chúng ta sử dụng lệnh ISDN Spidl và ISDN Spid trong chế độ cấu hình cổng BRI để khai báo số SPID

Tham số ldn định nghĩa số danh bạ nội bộ. Thông số khai báo cho ldn phải đúng với thông số khai báo trên ISDN switch. Tham số này không bắt buộc phải khai báo

```
isdn switch-type basic-ni
!
<Output Omitted>
!
interface BRI0/0
 isdn switch-type basic-ni
 isdn spid1 51055540000001 5554000
 isdn spid2 51055540010001 5554001
!
```

Hình 4.2.1

4.2.2 Cấu ình ISDN PRI

ISDN PRI chạy trên đường T1 hay E1. Sau đây là ba nhiệm vụ chính khi cấu hinh PRI

1. Xác định loại switch PRI mà router kết nối đến
2. Xác định T1/E1 controller, loại framing loại mã hoá trên đường truyền
3. Nhóm các timeslot PRI

Router kết nối PRI thông qua T1/E1 do đó không có lệnh "interface pri". Cổng vật lý trên router thực hiện kết nối này được gọi là T1 controller hay E1 controller tuỳ theo chúng ta sử dụng T1 hay E1. Chúng ta phải cấu hình các controller này hoàn chỉnh thì router mới có thể giao tiếp được với mạng của nhà cungcấp dịch vụ. còn kênh B và D của ISDN được cấu hình riêng bên dưới controller bằng lệnh interface serial

Tương tự như BRI chínta cũng dùng lệnh ISDN switch – type để khai báo loại ISDN switch mà router kết nối đến Router (config) # isdn switch-ttype primary-net5

Switch Type	Description
primary-5ess	AT&T basic rate switches (USA)
primary-dms100	Northern Telecom DMS-100 (North America)
primary-ni	National ISDN (North America)
primary-net5	Switch type for Net5 in United Kingdom, Europe, and Australia
primary-ntt	NTT ISDN switch (Japan)

Hình 4.2.2.a

Sau đây là 4 bước cấu hình T1 hay E1 controller

1. Từ chế độ cấu hình toàn cục xác định controller và slot/port của card PRI
2. Cấu hình framing, line codin, cloking theo hướng dẫn của nhà cung cấp dịch vụ. Nếu bạn dùng T1 thì khai báo một trong các tham số sau

Lệnh linecode xác định phương pháp mã hoá tín hiệu ở lớp Vật lý của nhà cung cấp dịch vụ

Router (config – controller) # linecode (ami/b8zs/ hđb3)

Ở Bắc Mỹ phương pháp mã hoá tín hiệu b8zs được sử dụng cho T1. Ở Châu âu thì sử dụng HDB3

1. Nhóm các timeslot vào một cổng PRI

Đối với T1 chúng ta sử dụng timeslot trong khoảng 1 -24. Còn đối với E1 thì chúng ta sử dụng các timeslot trong khoảng 1 – 31

2.Cấu hình một cổng giao tiếp tương ứng cho kênh D PRI hoạt động

Trong thiết bị E1 hay T1 số kênh được bắt đầu từ 1 và kết thúc ở 31 đối với E1 hay kết thúc 24 đối với T1. Trong khi đó số cổng Serial trên Cisco router lại bắt đầu từ 0. Do đó kênh 16 kênh truyền tín hiệu điều khiển của E1, sẽ tương ứng với cổng 15. Kênh 24 kênh truyền tín hiệu điều khiển của T1, sẽ tương ứng với cổng 23. Như vậy cổng Serial 0/0:23 tương ứng với kênh D của T1 PRI

Các bạn không được nhầm lẫn giữa các kênh của T1/E1 với các cổng con thường được sử dụng cho frame Relay. Các cổng con thường được ký hiệu bằng dấu chấm, còn các kênh được ký hiệu bằng dấu hai chấm:

- S0/0.23 là cổng con của cổng S0/0
- S0/0:23: tương ứng với kênh 24 của T1

```
Router(config)#controller t1 1/0
Router(config-controller)#framing esf
Router(config-controller)#linecode b8zs
Router(config-controller)#pri-group timeslots 1-24

Router(config-controller)#interface serial1/0:23
Router(config-if)#isdn switch-type primary-5ess
Router(config-if)#no cdp enable
```

Hình 4.2.2.b

```
Router(config)#controller e1 1/0
Router(config-controller)#framing crc4
Router(config-controller)#linecode hdb3
Router(config-controller)#pri-group timeslots 1-31

Router(config-controller)#interface serial1/0:15
Router(config-if)#isdn switch-type primary-net5
Router(config-if)#no cdp enable
```

Hình 4.2.c

4.2.3 Kiểm tra cấu hình ISDN

Chúng ta có thể sử dụng nhiều lệnh show khác nhau để kiểm tra cấu hình ISDN

Để xác định trạng thái hoạt động của BRI chúng ta dùng lệnh show ISDN status. Chúng ta sử dụng lệnh này sau khi đã cấu hình xong ISDN BRI để kiểm tra xem router đã giao tiếp được với ISDN switch hay chưa. Trong ví dụ ở hình 4.2.3.a cho thấy router đã giao tiếp thành công và ISDN Lớp 3 cũng đã sẵn sang để thực hiện hay nhận cuộc gọi. Trong kết quả hiển thị của lệnh show isdn status chúng ta nên lưu ý đến trạng thái của lớp 1 và lớp 2 Layer 1 Status: Active, layer 2 status Multiple _ Frame _ Established

```
Cork#show isdn status
Global ISDN Switchtype = basic-ni
ISDN BRI0/0 interface
dsl 0, interface ISDN Switchtype = basic-ni
    Layer 1 Status:
ACTIVE
    Layer 2 Status:
TEI = 64, Ces = 1, SAPI = 0, State =
MULTIPLE_FRAME_ESTABLISHED
TEI = 65, Ces = 2, SAPI = 0, State =
MULTIPLE_FRAME_ESTABLISHED
    Spid Status:
TEI 64, ces = 1, state = 5(init)
    spid1 configured, no LDN, spid1 sent, spid1 valid
    Endpoint ID Info: epsf = 0, usid = 70, tid = 1
TEI 65, ces = 2, state = 5(init)
    spid2 configured, no LDN, spid2 sent, spid2 valid
    Endpoint ID Info: epsf = 0, usid = 70, tid = 2
    Layer 3 Status:
```

Hình 4.2.3.a

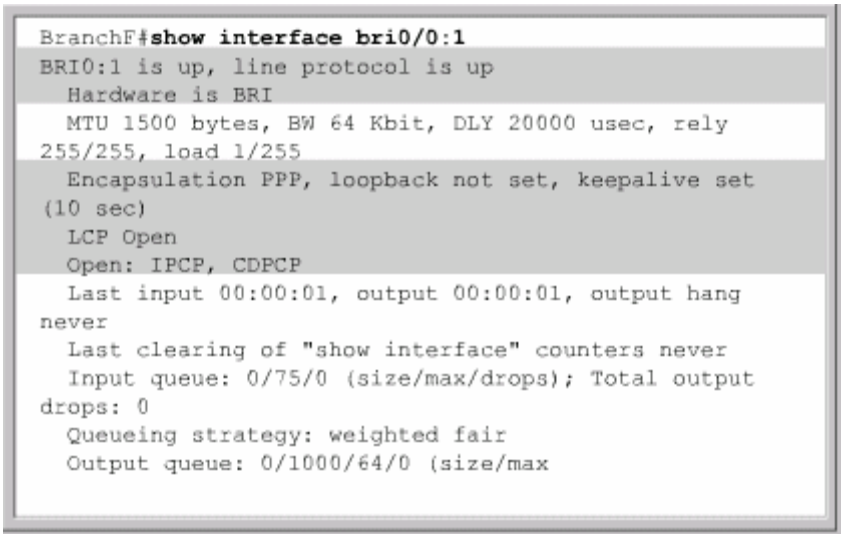
Lệnh show isdn active cho biết các thông tin về những cuộc gọi đang thực hiện bao gồm

- Số gọi đến
- Thời gian gọi
- Cước phí
- Đơn vị tính cước phí trong suốt cuộc gọi
- Thông tin về thiết bị kết nối ở đầu bên kia

Lệnh show interface bri0/0 cho biết trạng thái của cổng BRI trên router. Bạn muốn xem thông tin của từng lệnh thì khai báo thêm số kênh ở cuối câu lệnh này. Ví dụ lệnh show interface br0/0:1 cho biết:

- Kênh B sử dụng đóng gọi PPP

- LCP đã được thoả thuận và hoạt động
- Có hai NCP đang chạy là IPCP và CDPCP



Hình 4.2.3.b

4.2.4 Xử lý sự cố ISDN

Sau đây là các lệnh được dùng để theo dõi và phát hiện sự cố trong cấu hình ISDN:

- Lệnh debug isdn q921 hiển thị các thông tin về lớp liên kết dữ liệu các thông điệp trên kênh D giữa router và ISDN switch. Chúng ta nên sử dụng lệnh này khi trong kết quả hiển thị của lệnh show isdn status không cho thấy là : Layer 1 :Active Layer 2 Multiple_Frame-Established
- Lệnh debug isdn q931 cho biết thông tin về các thông điệp Lớp 3 trong quá trình thiết lập và kết thúc cuộc gọi.
- Lệnh debug ppp authentication hiển thị các thông điệp trao đổi của giao thức xác minh PAP hoặc Chap
- Lệnh debub ppp negotiation hiển thị các thông tin về lưu lượng PPP khi các thành phần trong PPP đang thực hiện việc thoả thuận cấu hình. Trong đó có quá trình thoả thuận của LCP quá trình xác minh và quá trình thoả thuận của NCP
- lệnh debug ppp error hiển thị các lỗi của giao thức và lỗi trạng thái của kết nối PPP. Chúng ta nên sử dụng các lệnh debug ppp để tìm sự cố ở lớp 2 khi kết quả hiển thị của lệnh show isdn status không cho thấy có sự cố của ISDN

4.3. Cấu hình DDR

4.3.1. Hoạt động của DDR

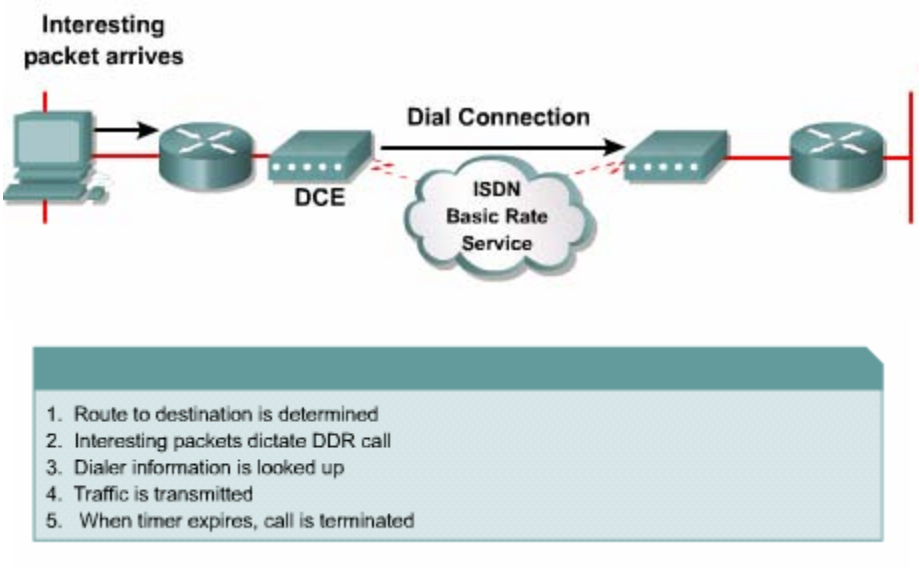
Trên cổng có cấu hình DDR nếu có một dòng dữ liệu nào cần gửi ra cổng này và phù hợp với những tiêu chuẩn đã được định nghĩa trước đó thì DDR sẽ được kích hoạt để thực hiện truyền dữ liệu. Nhưng loại dữ liệu có thể kích hoạt DDR được gọi là lưu lượng đặc biệt. Sau khi router đã truyền xong nhưng lưu lượng đặc biệt này nó sẽ ngắt kết nối.

Điểm quan trọng nhất để DDR hoạt động hiệu quả là việc định nghĩa lưu lượng đặc biệt. . Lưu lượng đặc biệt được định nghĩa bằng lệnh dialer-list . Các lưu lượng của các giao thức được định nghĩa trong dialer – list có thể thực hiện kết nối DDR. Tuy nhiên bạn cần lưu ý rằng dialer – list không ngăn chặn lưu lượng đi qua cổng . Một khi lưu lượng đặc biệt đã kích hoạt kết nối DDR và kết nối này đang còn hoạt động thì mọi lưu lượng khác đều có thể đi qua

Sau đây là các bước hoạt động của DDR trên Cisco router

1. Router nhận luồng lưu lượng vào từ một cổng, kiểm tra bảng định tuyến để xác định cổng ra cho lưu lượng đó.
2. Nếu cổng đi ra có cấu hình DDR thì router sẽ xác định xem lưu lượng này có phải là loại lưu lượng đặc biệt hay không
3. Router xác định các thông tin quay số cần thiết để thực hiện cuộc gọi cho router kế tiếp
4. Nếu cổng ra đang có kết nối thì lưu lượng được chuyển ran gay. nếu cổng ra chưa có kết nối thì router sẽ gửi thông tin thiết lập kết nối trên kênh D BRI
5. Sau khi kếtnối đã được thiết lập thì mọi lưu lượng đặc biệt hay không đặc biệt đều được truyền đi
6. Đồng hồ đếm thời gian chờ bắt đầu được khởi động. Sau một khoảng thời gian định trước mà không có lưu lượng đặc biệt nào đi qua nữa thì kết nối sẽ bị ngắt

Thời gian chờ là khoảng thời gian router duy trì kếtnối khi không có lưu lượng đặc biệt nào truyền đi trên kết nối đó. Một khi kết nối DDR đã được thiết lập thì mọi lưu lượng đều được phép đi qua. Tuy nhiên chỉ có lưu lượng đặc biêt mới có thể khởi động lại đồng hồ đếm thời gian chờ



Hình 4.3.1

4.3.2 Cấu hình DDR

Cấu hình DDR cơ bản chỉ có một tập hợp các thông tin quay số được áp dụng cho một cổng. nếu cần có nhiều cấu hình quay số khác nhau áp dụng cho một cổng thì khi đó chúng ta nên sử dụng dialer profile

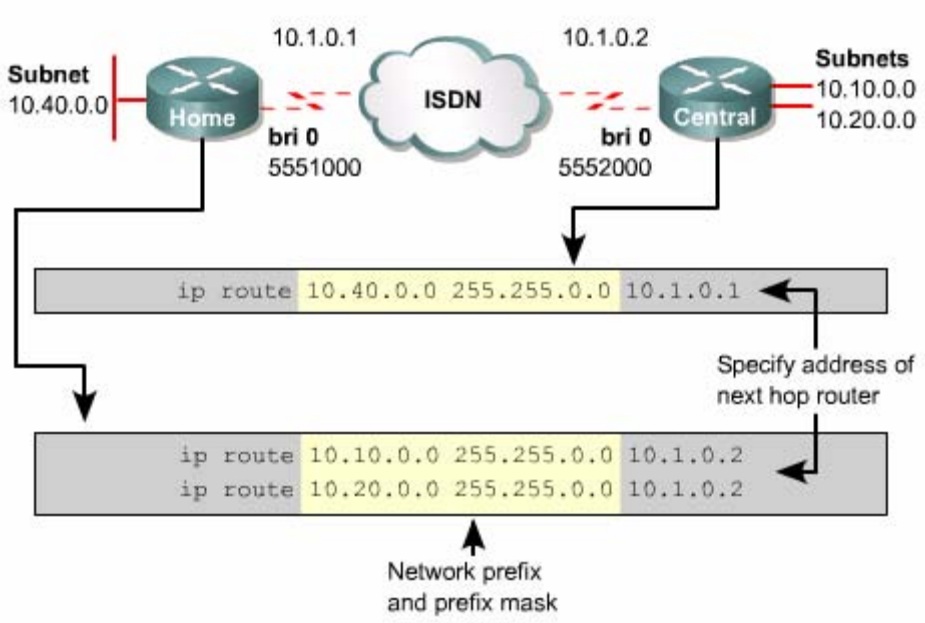
Để cấu hình DDR chúng ta thực hiện các bước sau:

- Cấu hình định tuyến cố định
- Xác định lưu lượng đặc biệt
- Cấu hình các thông tin quay số

4.3.3 Cấu hình định tuyến cố định cho DDR

Để chuyển tiếp dữ liệu router cần phải biết con đường nào tương ứng với mỗi luồng lưu lượng nhận được . Nếu chúng ta sử dụng giao thức định tuyến động và lưu lượng của giao thức định tuyến này được định nghĩa là lưu lượng đặc biệt thì cổng DDR sẽ thực hiện quay số mỗi khi đến chu kỳ cập nhật thông tin định tuyến. Do đó để tránh vấn đề này chúng ta cần cấu hình định tuyến cố định cho DDR

Để cấu hình định tuyến cố định cho IP chúng ta dùng lệnh sau:



Hình 4.3.3

Xét ví dụ hình 4.3.3 router Central có định tuyến cố định đến mạng 10.40.0.0 của router Home. Router Home có hai định tuyến cố định đến hai mạng LAN trên router Central. Nếu mạng kết nối trên router Home là stub network thì mọi lưu lượng đi ra ngoài đều gửi cho router Central

Do đó trên router Home trong trường hợp nà chỉ cần một định tuyến mặc định là đủ

Khi cấu hình định tuyến cố định, các bạn nên nhớ

Mặc định định tuyến cố định luôn được ưu tiên trước định tuyến vì nó có chỉ số tin cậy nhỏ hơn. Nếu không có thêm cấu hình gì đặc biệt thì định tuyến động sẽ bị bỏ qua nếu có định tuyến cố định đến cùng một mục đích

Để giảm bớt số lượng định tuyến cố định chúng ta nên sử dụng định tuyến mặc định hoặc tổng hợp địa chỉ mạng

4.3.4 Định nghĩa lưu lượng đặc biệt cho DDR

Cuộc gọi DDR được kích hoạt lưu lượng đặc biêt. Lưu lượng đặc biệt có thể được định nghĩa theo một trong những tiêu chuẩn sau

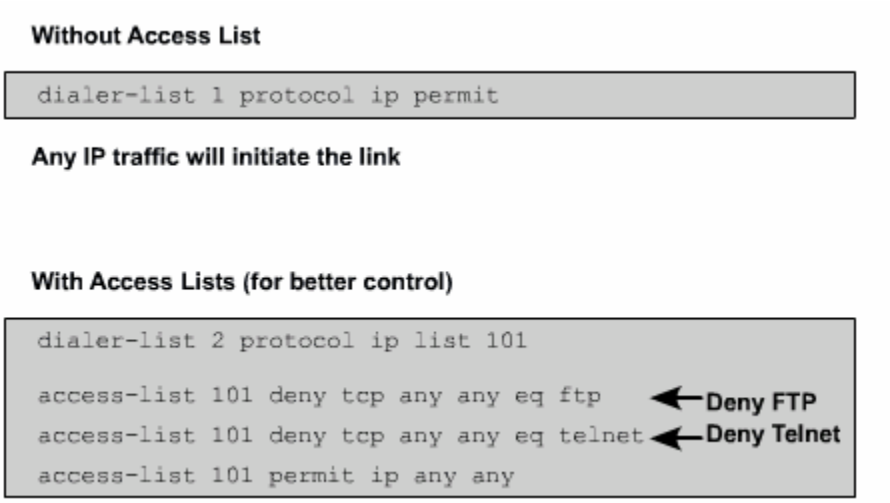
- Theo loại giao thức

- Theo địa chỉ nguồn hoặc đích của gói dữ liệu
- Các tiêu chuẩn khác được định nghĩa do nhà quản trị mạng

Lệnh dialer – list được sử dụng để xác định lưu lượng đặc biêt

Router (config)#dialer – list dialer – group- number protocol protocol – name (permit deny list aceess – list – number)

Dialer – group – number là chỉ số nằm trong khoảng từ 1 đến 10 giúp phân biệt giữa các dialer – list. Lệnh dialer – list 1 protocol ip permit sẽ cho phép mọi lưu lượng IP kích hoạt cuộc gọi. Thay vì cho phép mọi lưu lượng IP như vậy, dialer – list có thể chỉ đến một danh sách kiểm tra truy cập ACL để xác định chính xác hơn loại lưu lượng nào được phép thực hiện kết nối . Như ví dụ trên hình 4.3.4 dialer – list 2 chỉ kích hoạt kết nối DDR mọi gói IP khác đều được xem là lưu lượng đặc biệt và được phép khởi động kết nối DDR



4.3.5 Cấu hình thông tin quay số cho DDR

Để cấu hình DDR chúng ta phải thực hiện qua nhiều bước. Trước tiên là cấu hình PPP cho cổng quay số chúng ta cũng phải sử dụng các lệnh tương tự như khi cấu hình PPP cho cổng serial. HDLC là giao thức đóng gói mặc đinh trên cổng ISDN của Cisco router. Nhưng hầu hết các mạng đều sử dụng PPP cho kết nối chuyển mạch . PPP phức tạp hơn dễ tương thích và có nhiều chức năng hơn. Ví dụ như có quá trình xác minh nên PPP là giao thức liên kết dữ liệu được sử dụng trên kênh B trên hầu hết mọi router. Để cấu hình PPP trên cổng DDR chúng ta xem ví dụ sau

Home (config)# username Central password Cisco

Home (config)#interface bri0/0

Home (config – if)#encapsulation ppp

Home (config – if)# ppp authentication chap

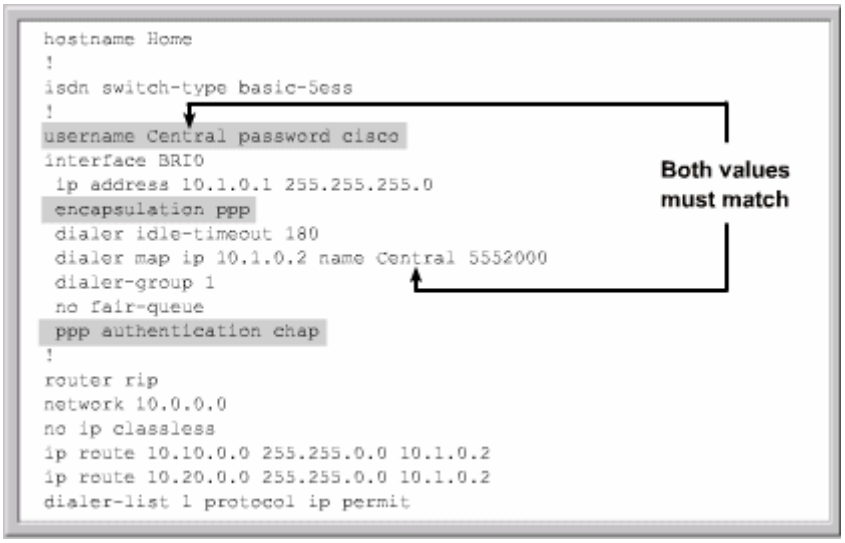
Home (config – if) #ip addres 10.1.0.1

255.255.255.0

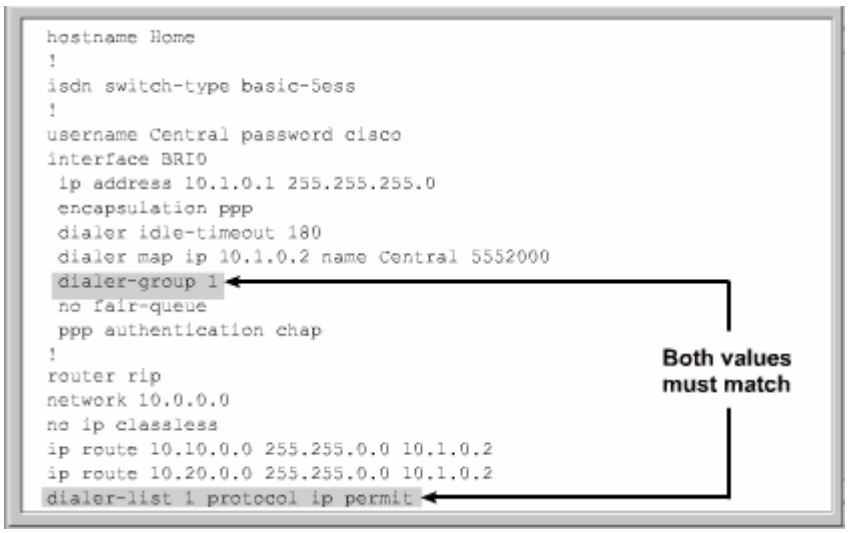
Dialer – list xác định lưu lượng đặc biệt cho cổng DDR. Do đóchúng ta cần liên kết cổng DDR với một dialer – list tương ứng bằng lệnh đialer-group group – number;

Home (config – if)#dialer – group1.

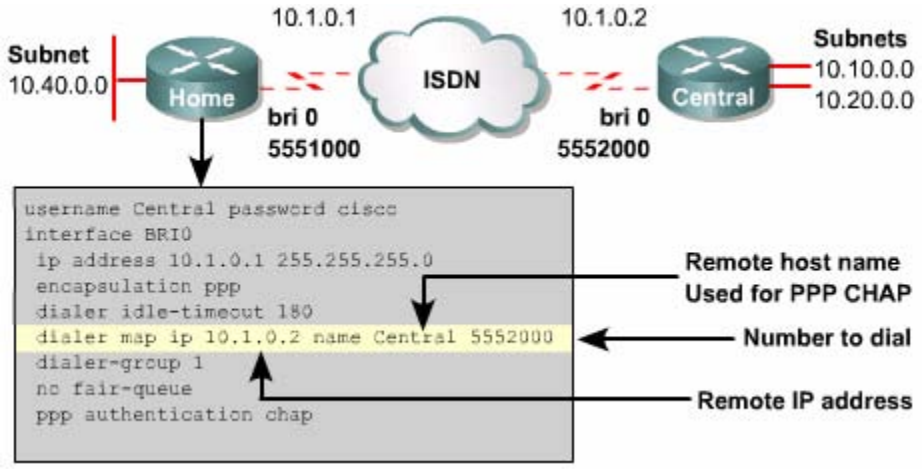
Trong đó group number xác định số thứ tự của dialer – list tương ứng. Do đó chỉ số này phải giống với chỉ số của dialer – list group number. Mỗi một cổng chỉ có một dialer – group nhưng một dialer- list có thể tương ứng cho nhiều cổng khác nhau



Hình 4.3.5a



Hình 4.3.5b



Hình 4.3.5c

Sau đó chúng ta cấu hình thông tin quay số cho DDR bằng lệnh dialer map

Lệnh dialer map ánh xạ địa chỉ của trạm kế tiếp với một số điện thoại

Nếu bạn chỉ cần gọi đến một số duy nhất thì bạn có thể dùng lệnh dialer string. Với lệnh dialer string router sẽ luôn luôn gọi đến số điện thoại khai báo trong lệnh này bất kể địa chỉ đích của dữ liệu

Lệnh dialer idle timeỏu seconds cho phép cấu hình khoảng thời gian chờ tính theo giây trước khi ngắt kết nối, second là số giây chờ tính lúc gói dữ liệu đặc biệt cuối cùng được gửi đi. Thời gian chờ mặc định là 120

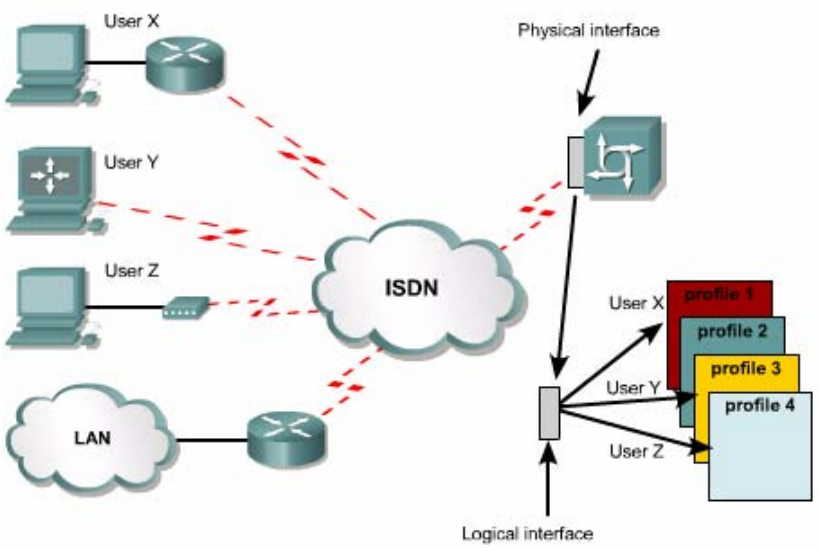
```
hostname Home
!
isdn switch-type basic-5ess
!
username Central password cisco
interface BRI0
 ip address 10.1.0.1 255.255.255.0
 encapsulation ppp
 dialer idle-timeout 180
 dialer map ip 10.1.0.2 name Central 5552000
 dialer-group 1
 no fair-queue
 ppp authentication chap
!
router rip
```

c

Hình .4.3.5.d

4.3.6 Dialer profiles

DDR có một hạn chế là chỉ có một cấu hình quay số áp dụng trực tiếp cho một cổng vật lý. Địa chỉ IP được gán trực tiếp cho cổng vật lý do đó chỉ có hai cổng có hai địa chỉ nằm trong cùng một subnet mới có thể thực hiện kết nối DDR với nhau. Điều này có nghĩa là một cổng DDR ở đầu này chỉa có thể kết nối được với một DR ở đầu bên kia



Hình 4.3.6a

Dialer profile giải quyết được giới hạn này của DDR. Dialer profile tách được mối rang buộc cố định giữa cổng vật lý vàcấu hình quay số , nó cho phép cổng vật lý có thể tự động chọn lựa cấu hình tương ứng với mỗi cuộc gọi. Dialer profile có thể thực hiện được những việc sau

- Định nghĩa giao thức đóng gói và danh sách kiểm tra truy cập ACL
- Định nghĩa số lượng cuộc gọi tối thiểu và tối đa
- Bật hoặc tắt các đặc tính đã được định trước

Dialer profile giúp cho việc thiết kế và phát triển hệ thống mạng được linh hoạt hơn, khả năng mở rộng lớn hơn. Dialer profile tách phần logic của DDR, ví dụ như: phần lớp Mạng đóng gói và các đặc tính về quay số ra khỏi cổng vật lý

Khi sử dụng dialer profile chúng ta thực hiện được những việc sau

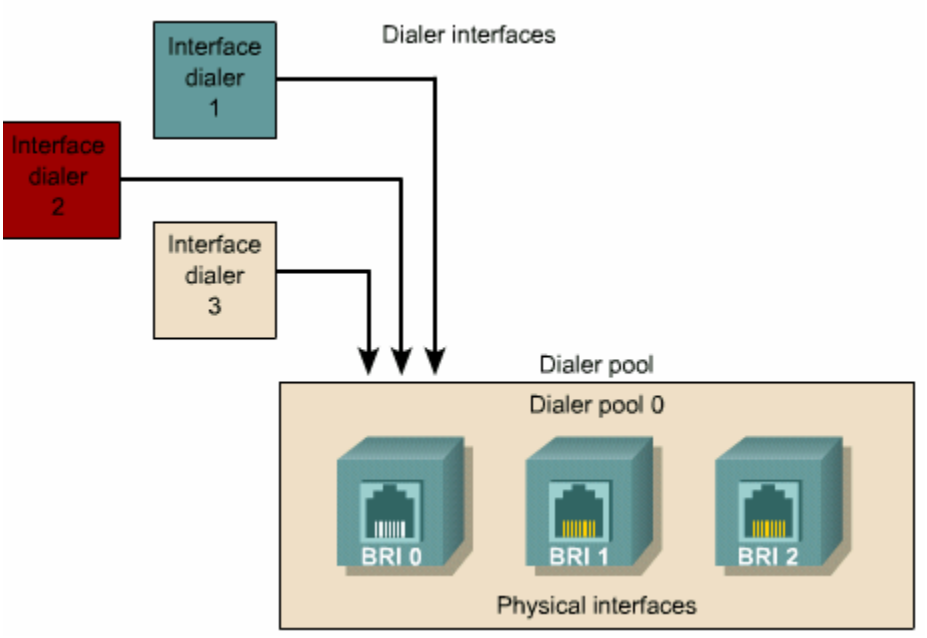
- Cấu hình kênh B của cổng ISDN với nhiều IP subnet khác nhau
- Sử dụng nhiều kiểu đóng gói khác nhau trên kênh B của cổng ISDN
- Khai báo nhiều đặc tính DDR khác nhau cho kênh B của cổng ISDN
- Tận dụng kênh B bằng cách gán một ISDN BRI với nhiêù dialer pools khác nhau

Một dialer profile bao gồm những thành phần sau

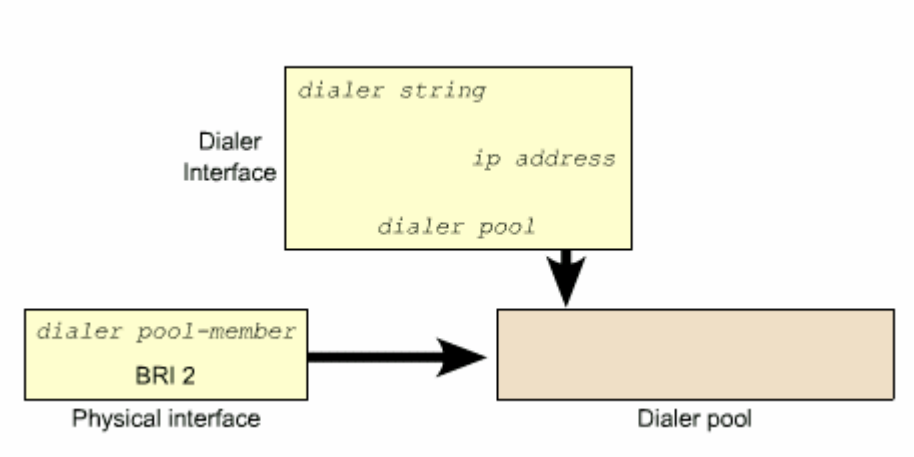
Cổng quay số (Dialer interface) - cổng logic tương ứng với một mạng đích của dialer profile

- Dialer pool - mỗi một cổng quay số tương ứng với một dialer pool điều này có nghĩa là một hay nhiều cổng vật lý tươngứng với một dialer profile

Cổng vật lý - cấu hình các đặc tính về đóng goi quá trình xác minh PPP. Multilink PPP và xác định cổng này tương ứng với dialer profile



Hình 4.3.6.b



Hình 4.3.6.c

DDR hay dialer profile đều kích hoạt đường truyền khi cần truyền lưu lượng đặc biệt ra cổng DDR. Trước tiên lưu lượng đặc biệt được định tuyến đến trạm DDR kế tiếp. Sau đó router tìm cổng quay số có địa chỉ IP nằm trong cùng subnet với địa chỉ IP của trạm DDR kế tiếp. Nếu có router tiếp tục tìm trong dialer pool một cổng vật ý DDR còn trống. Sau đó cấu hình của dialer profile được áp dụng cho cổng

được chọn và tạo kết nối DDR. Sauk hi kết nối DDR kết thúc cổng vật lý được trả về cho dialer pools để sử dụng cho lần sau..

4.3.7 Cấu hình dialer profiles

Chúng ta có thể cấu hnhf nhiều cổng quay số trên một router.Mỗi cổng quay số là một cấu hình hoàn chỉnh cho một điểm đích. Lệnh interface dialer được sử dụng để tạo cổng quay số và vào chế độ cấu hình của cổng này

Sau đây là những công việc cần thực hiện khi cấu hình cổng quay số:

1. Cấu hình một hay nhiều cổng quay số với những lệnh tương tự như cấu hình DDR cơ bản:

Địa chỉ IP

Kiểu đóng gói và giao thức xác minh

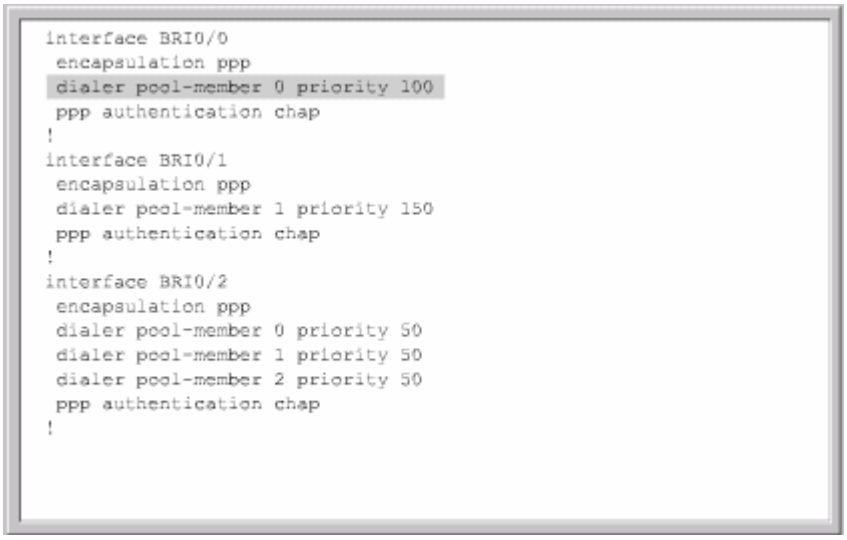
Thời giam chờ

Dialer group

2. Khai báo tên và số điện thoại của router đầu bên kia bằng lệnh dialer string và dialer remote name. Khai báo nhóm các cổng vật lý tương ứng với cổng logic này bằng lệnh dialer pool
3. Cấu hình cổng vật lý và gán cổng này vào dialer pool bằng lệnh dialer pool – member

```
interface dialer1
 ip address 10.1.1.1 255.255.255.0
 encapsulation ppp
 dialer remote-name Smalluser
 dialer string 5554540
 dialer idle-timer 240
 dialer pool 1
 dialer-group 1
 ppp authentication chap
!
interface dialer2
 ip address 10.2.2.1 255.255.255.0
 encapsulation ppp
 dialer remote-name Mediumuser
 dialer string 5551234
 dialer idle-timer 9999
 dialer pool 1
 dialer-group 2
```

Hình 4.3.7.a



Hình 4.3.7.b

Một cổng có thể gán vào nhiều dialer pool khác nhau bằng cách dùng nhiều lần lệnh dialer pool – member. Nếu có nhiều cổng vật lý trong một dialer pool thìchúng ta có thể sử dụng thông số ưu tiên priority trong lệnh dialer poole-member để định mức độ ưu tiên cho các cổng trong dialer pool

Một hoặc nhiều cổng sau đây có thể sử dụng được với dialer pool

- Cổng serial đồng bộ
- Cổng serial bất đồng bộ
- BRI
- PRI

4.3.8 Kiểm tra cấu hình DDR

Lệnh show dialer interface (BRI) hiển thị thông tin về các cuộc gọi vào và ra của DDR

Thông lệnh “Dialer state is data link layer up. Interface bound to profile Dialer1” cho biết cuộc gọi thực hiện tốt và cổng BRI o/0:1 được gán với dialer profile 1i

```
sydney#show dialer

BRI0/0 - dialer type = ISDN

Dial String      Successes   Failures    Last DNIS   Last
status
0 incoming call(s) have been screened.
0 incoming call(s) rejected for callback.

BRI0/0:1 - dialer type = ISDN
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is data link layer up
Interface bound to profile Dialer1
Time until disconnect 83 secs
Current call connected never
Connected to 5552000 (perth)

BRI0/0:2 - dialer type = ISDN
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle
```

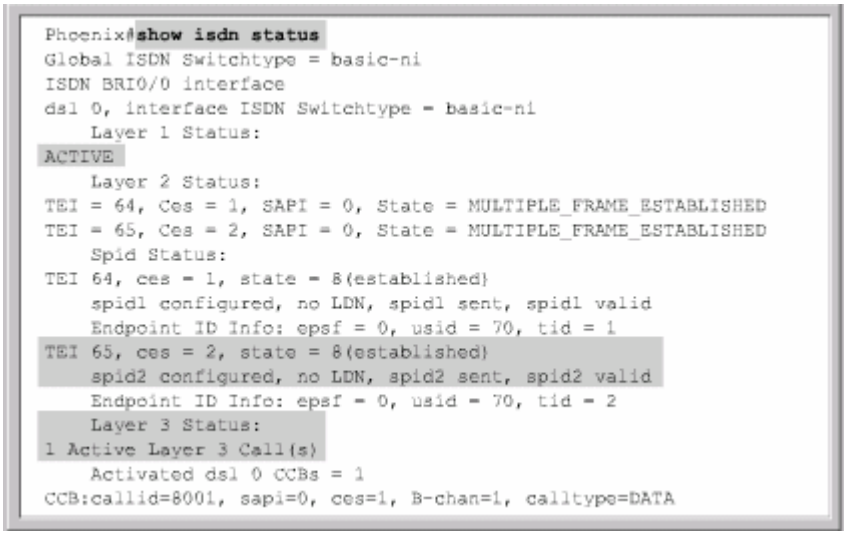
Hình 4.3.8a

Lệnh show ISDN active hiển thị thông tin về các cuộc gọi ISDN đang thực hiện. Trong ví dụ hình 4.3.8.b chúng ta thấy đang có cuộc gọi ra đến router Seatle

```
Phoenix#show isdn active
-------------------------------------------------------------------------
-------------
                                ISDN ACTIVE CALLS
-------------------------------------------------------------------------
-------------
History table has a maximum of 100 entries.
History table data is retained for a maximum of 15 Minutes.
-------------------------------------------------------------------------
-------------
Call Calling Called  Remote Seconds Seconds Seconds Charges
Type Number  Number  Name   Used    Left    Idle    Units/Currency
-------------------------------------------------------------------------
Out          5551000 Seattle      87      41      78      0
-------------------------------------------------------------------------
```

Hình 4.3.8.b

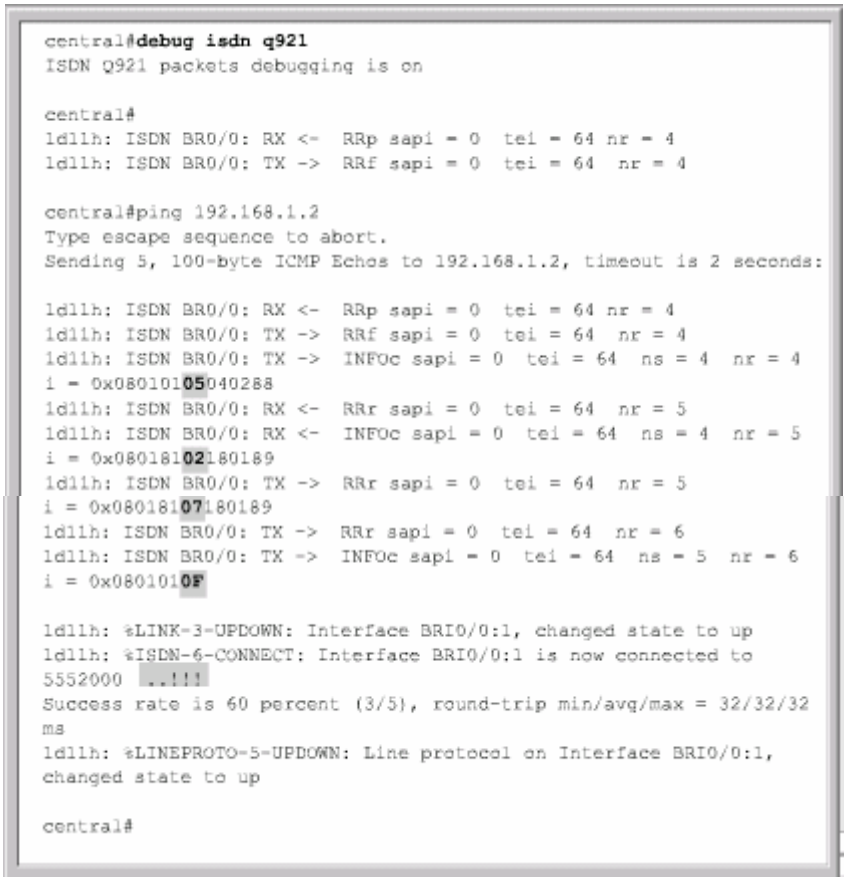
Lệnh show ISDN status hiển thị các thông tin 3 lớp của cổng BRI. Trong ví dụ hình 4.3.8. c chúng ta thấy ISDN Lớp 1 đã hoạt động ISDN Lớp 2 đã được thiết lập với số SP1D1 và SP1D2 và đang có một kết nối ở Lớp 3



Hình 4.3.8.c

4.3.9 Xác định sự cố trong cấu hình DDR

Có hai loại sự cố chíng trong DDR. Một là router không thực hiện quay số khi cần thiết hai là router liên tục gọi đi khi không cần thiết. Các lệnh debug sẽ rất hữu dụng khi chúng ta xác định sự cố trong cấu hình DDR



```
central#debug isdn q921
ISDN Q921 packets debugging is on

central#
ldllh: ISDN BR0/0: RX <-  RRp sapi = 0  tei = 64 nr = 4
ldllh: ISDN BR0/0: TX ->  RRf sapi = 0  tei = 64  nr = 4

central#ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:

ldllh: ISDN BR0/0: RX <-  RRp sapi = 0  tei = 64 nr = 4
ldllh: ISDN BR0/0: TX ->  RRf sapi = 0  tei = 64  nr = 4
ldllh: ISDN BR0/0: TX ->  INFOc sapi = 0  tei = 64  ns = 4  nr = 4
i = 0x08010105040288
ldllh: ISDN BR0/0: RX <-  RRr sapi = 0  tei = 64  nr = 5
ldllh: ISDN BR0/0: RX <-  INFOc sapi = 0  tei = 64  ns = 4  nr = 5
i = 0x08018102180189
ldllh: ISDN BR0/0: TX ->  RRr sapi = 0  tei = 64  nr = 5
i = 0x08018107180189
ldllh: ISDN BR0/0: TX ->  RRr sapi = 0  tei = 64  nr = 6
ldllh: ISDN BR0/0: TX ->  INFOc sapi = 0  tei = 64  ns = 5  nr = 6
i = 0x0801010F

ldllh: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to up
ldllh: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected to
5552000 ..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 32/32/32
ms
ldllh: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0/0:1,
changed state to up

central#
```

Hình 4.3.9.a

Trong ví dụ hình 4.3.9.a hai chữ số Hex đứng vị trí thứ 7 và thứ 8 cho biết loại thông điệp:\

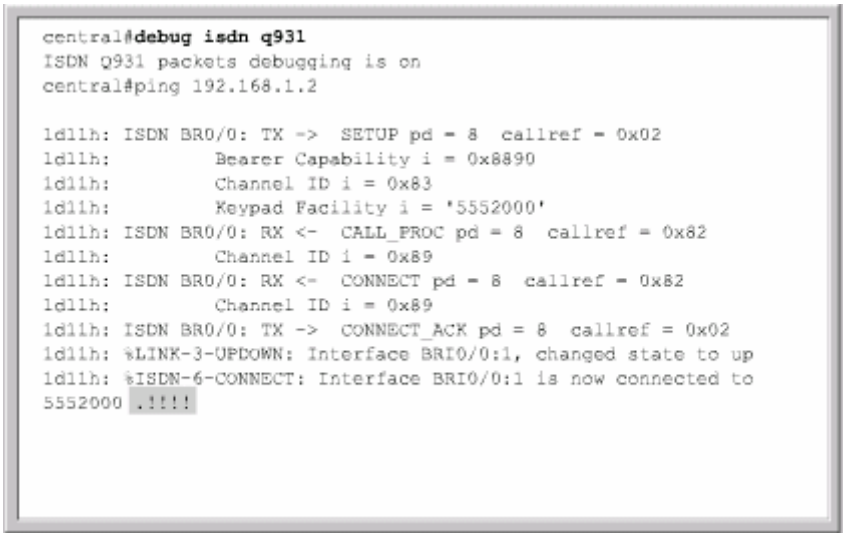
0*05:Thông điệp thiết lập cuộc phí

0*02:Thông điệp triển khai cuộc gọi

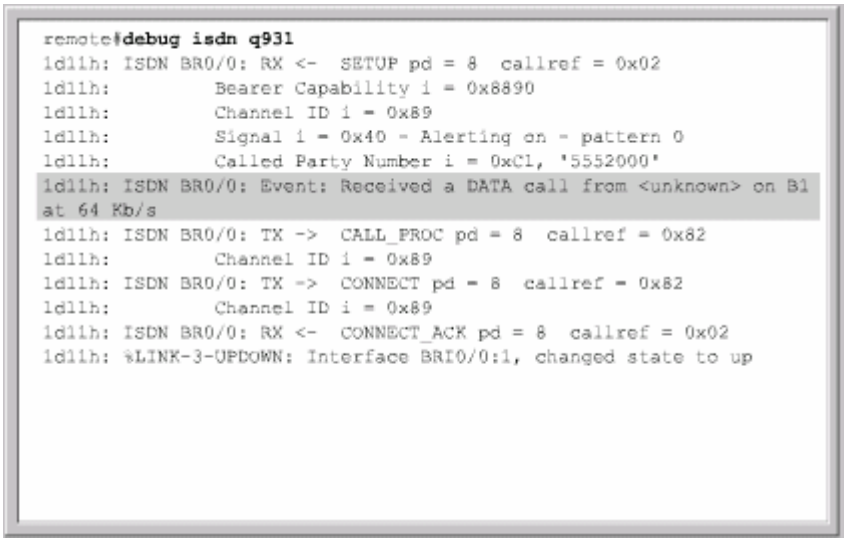
0*07 Thông điệp kết nối

0*0F: Thông điệp xác nhận kết nối

Lệnh debug ISDN q931 cho chúng ta xem các thông tin trao đổi Lớp 2 của ISDN khi cuộc gọi ra hoặc vào được thiết lập. Các chỉ số “i=” là chỉ số Hex của các thông điệp Q931

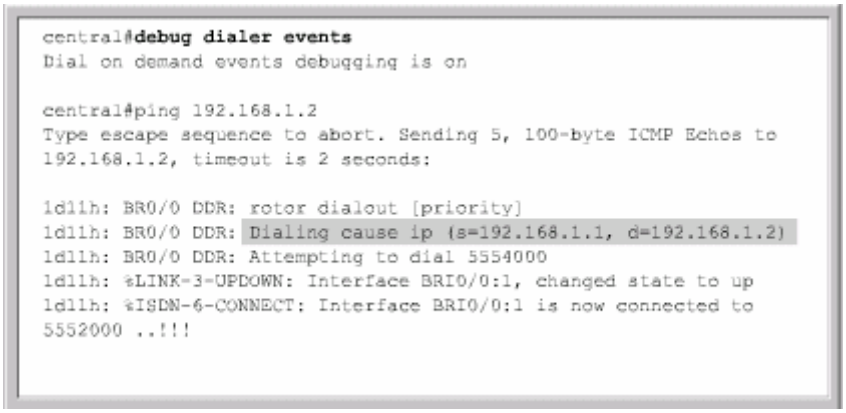


Hình 4.3.9b



Hình 4.3.9c

Lệnh debug dialer (event packer) được sử dụng để xác định sụ cố kết nối DDR. Lệnh debug dialer events hiển thị các thông điệp cho biết kết nối DDR đã được thực hiện chưa lưu lượng nào đã kích hoạt kết nối. Nếu router bị cấu hình DDR không đúng thì lệnh này sẽ chỉ ra được nguồn gốc của sự cố. Nếu không có thông điệp nào được hiển thị thì ra có nghĩa là router chưa nhận được lưu lượng đặc biệt nào. Như vậy nguyên nhân có thể là do cấu hình dialer – list hoặc ACL không đúng

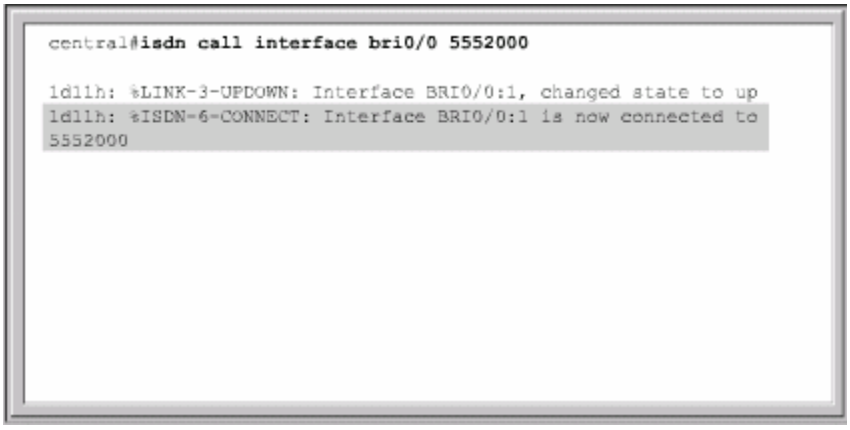


Hình 4.3.9d

Không phải lỗi cấu hình DDR nào cũng dẫn đến việc quay số không đúng. Giao thức định tuyến động cũng có thể làm cho router quay số liên tục mặc dù không có dữ liệu của người dùng cần truyền đi. Lệnh debug dialer packets sẽ hiển thị thông điệp mỗi khi có một gói dữ liệu được truyền ra cổng DDR. Do đó chúng ta có thể dùng lệnh này để xác định chính xác loại lưu lượng nào đã kích hoạt liên tục cổng DDR

Nếu router không thực hiện kết nối được khi cần thiết thì có thể là do lỗi của ISDN hoặc DDR. Có thể router đầu bên kia được cấu hình không đúng hoặc là mạng ISDN của nhà cung cấp dịch vụ có sự cố. Chúng ta dùng lệnh ISDN call interface để ép router quay số đến router đầu bên kia. Nếu hai router không thể giao tiếp được với nhau thì sự cố thuộc về ISDN chứ không phải sự cố DDR. Nhưng nếu hai router có thể giao tiếp được với nhau thì có nghĩa là cấu hình ISDN ở cả hai đầu đều không có vấn đề. Trong trường hợp nay thì khả năng lớn là lỗi của cấu hình DDR trên hai router

Trong một số trường hợp việc khởi động lại kết nối giữa router và ISDN switch cũng rất hiệu quả. Lệnh clear interface bri sẽ xoá hết kết nối hiện tại.trên cổng BRI và khởi động lại kết nối hiện tại trên cổng BRI và khởi động lại ket nối mới với ISDN switch. Và đôi khi chúng ta cũng nên kiểm tra lại chỉ số SP1D1 và SP1D2



Hình 4.3.9.e

TỔNG KẾT

ISDN được xem là một tập hợp các giao thức được thực hiện các công ty điện thoại để cho phép mạng điện thoại có thể tích hợp dịch vụ truyền thoại, video và dữ liệu. ISDN cho phép thông tin liên lạc tốc độ cao chất lượng tốt

DDR được sử dụng để tiết kiệm chi phí khi một công ty hay tổ chức không có nhu cầu cần một đường kết nối WAN cố định. Đường truyền này cũng được sử dụng làm đường dự phòng cho kết nối chính.

- Sau đây là các điểm quan trọng mà bạn cần nắm trong chương này: ISDN truyền dữ liệu thoại và video
- ISDN có sử dụng các chuẩn về địa chỉ tín hiệu
- ISDN hoạt động ở lớp Vật lý và lớp liên kết dữ liệu
- Các điểm liên kết trong ISDN
- Cấu hình ISDN trên router
- Cấu hình những lưu lượng nào được phép kích hoạt DDR
- Cấu hình định tuyến cố định cho DDR
- Cấu hình kiểu đóng gói cho DDR
- Cấu hình ACL cho DDR
- Cấu hình cổng quay số

Một hệ thống mạng được xây dựng bởi nhiều thiết bị nhiều giao thức và nhiều loại môi trường truyền. Khi một bộ phận nào đó của mạng không hoạt động đúng thì sẽ có một vài người dùng không truy cập được hoặc có thể cả hệ thống mạng cũng không hoạt động được. Cho dù trong trường hợp nào thì khi sự cố xảy ra người

quản trị mạng phải nhanh chóng xác định sự cố và xử lýchúng. Sự cố mạng thường do những nguyên nhân sau

- Gõ sai câu lệnh
- Cấu hình danh sách kiểm tra truy cập ACL không đúng hoặc đặt ACL không đúng chỗ
- Cấu hình thiếu cho router switch và các thiết bị mạng khác
- Kết nối vật lý không tốt

Người quản trị mạng cần tiếp cận với sụ cố một cách có phương pháp, sử dụng sơ đò xử lý sự cố tổng quát. Trước tiên là kiểm tra sự cố ở lớp Vật lý trước rồi mới đi dẫn lên các lớp trên. Mặc dù chương này chỉ tập trung vào xử lý sự cố các hoạt động của giao thức định tuyến ở lớp 3 nhưng cũng rất quan trọng cho các bạn khi cần loại trừ ở các lớp dưới

Sauk hi hoàn tất chương này các bạn sẽ thực hiện được những việc sau

- Mô tả sự khác nhau giữa EIGRP và IGRP
- Mô tả các khái niệm kỹ thuật và cấu trúc dữ liệu EIGRP
- Hiểu được quá trình hội tụ của EIGRP và các bước hoạt động cơ bản của thuật toán DUAL
- Thực hiện cấu hình EIGRP cơ bản
- Cấu hinh được tổng hợp cho EIGRP
- Mô tả quá trình EIGRP xây dựng và bảo trì bảng định tuyến
- Kiểm tra hoạt động của EIGRP
- Mô tả tám bước để xử lý sự cố tổng quát
- Áp dụng tiến hành logic để xử lý sự cố định tuyến
- Xử lý sự cố của hoạt động định tuyến RIP bằng cách sử dụng lệnh show và debug
- Xử lý sự cố của hoạt động định tuyến IGRP bằng cách sử dụng lệnh show và debug
- Xử lý sự cố của hoạt động định tuyến EIGRP bằng cách sử dụng lệnh show và debug
- Xử lý sự cố của hoạt động định tuyến OSPF bằng cách sử dụng lệnh show và debug

3.1C ác kh ái ni ệm c ủa EIGRP

3.1.1 So sánh EIGRP và IGRP

Cisco đưa ra giao thức EIGRP vào năm 1994 như là một phiên bản mới mở rộng và nâng cao hơn của giao thức IGRP. Kỹ thuật vectơ khoảng cách trong IGRP vẫn được sử dụng cho EIGRP

EIGRP cải tiến các đặc tính của quá trình hội tụ, hoạt động hiệu quả hơn IGRP. Điều này cho phép chúng ta mở rộng cải tiến cấu trúc trong khi vẫn giữ nguyên những gì đã xây dựng trong IGRP

Chúng ta sẽ tập trung so sánh EIGRP và IGRP trong lĩnh vực sau

- Tính tương thích
- Cách tính thông số định tuyến
- Số lượng họp
- Hoạt động phân phối thông tin tự động
- Đánh dấu đường đi

IGRP và EIGRP hoàn toàn tương thích với nhau EIGRP router không có ranh giới khi hoạt động chung với IGRP router. Đặc điểm này rấtquan trọng khi người sử dụng muốn tận dụng ưu điểm của cả hai giao thức EIGRP có thể hỗ trợ nhiều loại giao thức khác nhau còn IGRP thì không

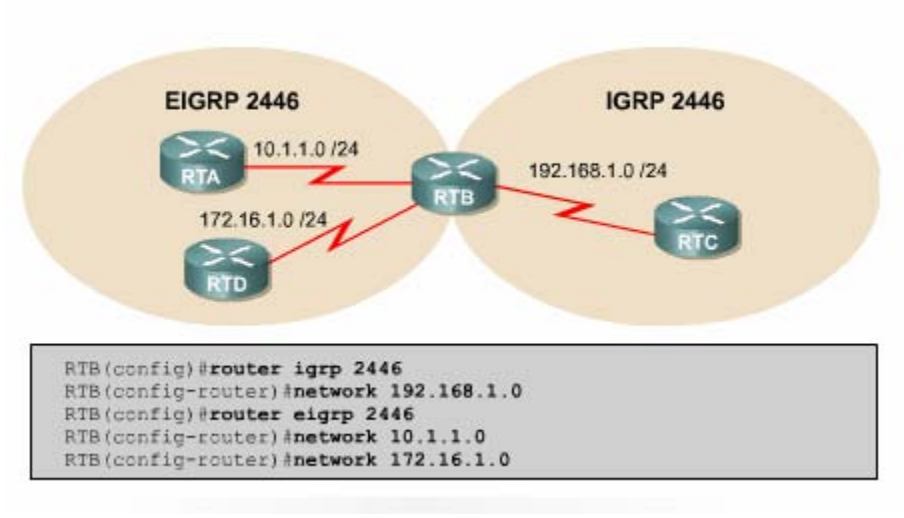
EIGRP và IGRP có cách tính thông số định tuyến khác nhau. EIGRP tăng thông số định tuyến của IGRP lên 256 lần vì EIGRP sử dụng thông số 32 bit còn IGRP sử dụng thông số 24 bit. Bằng cách nhân lên hoặc chia đi 256 lần , EIGRP có thể dễ dàng chuyển đổi thông số định tuyến của IGRP

IGRP có số lượng hợp tối đa là 255. EIGRP có số lượng họp tối đa là 224 Con số này dư sức đáp ứng cho một mạng được thiết lập hợp lý lớn nhất

Để các giao thức định tuyến khác nhau như GSPF và RIP chẳng hạn thực hiện chia sẻ thông tin định tuyến với nhau thì cần phải cấu ình nâng cao hơn. Trong khi đó IGRP và EIGRP có cùng số AS của hệ tự quản sẽ tự động phân phối và chia sẻ thông tin về đường đi với nhau. Trong ví dụ ở hình 3.1.1, RTB tự động phân phối các thông tin về đường đi mà EIGRP học được cho IGRP AS và ngược lại

EIGRP đánh dấu những đường mà nó hoạc được từ IGRP hay từ bất kỳ nguồn bên ngoài nào khác là đường ngoại vi vì những con đường này không xuất phát từ các EIGRP router, IGRP thì không phân biệt đường ngoại vi và nội vi

Ví dụ như hình 3.1.1 trong kết quả hiển thị của lệnh show ip route đường EIGRP được đánh dấu bằng chữ D đường ngoại vi được đánh dấu bằng chữ EX. RTA phân biệt giữa mạng học được từ EIGRP và mạng được phân phối từ IGRP. Trong bảng định tuyến của RTC giao thức IGRP không có sự phân biệt này. RTC chỉ nhận biết tất cả các đường đều là đường IGRP mặc dù hai mạng 10.1.1.0 và 172.16.0.0 là phân phối từ EIGRP




```
RTA#show ip route
<output omitted>
C    10.1.1.0 is directly connected, Serial0
D    172.16.1.0 [90/2681856] via 10.1.1.1, Serial0
D EX 192.168.1.0 [170/2681856] via 10.1.1.1,
00:00:04, Serial0
```

```
RTC#show ip route
<output omitted>
C    192.168.1.0 is directly connected, Serial0
I    10.0.0.0 [100/10476] via 192.168.1.1,
00:00:04, Serial0
I    172.16.0.0 [100/10476] via 192.168.1.1,
00:00:04, Serial0
```

Hình 3.1.1

3.1.2 Các khái niệm và thuật ngữ của EIGRP

EIGRP router lưu giữ các thông tin về đường đi và cấu trúc mạng trên RAM nhờ đó chúng đáp ứng nhanh chóng theo sự thay đổi. Giống như OSPF EIGRP cũng lưu những thông tin này thành từng bảng và từng cơ sở dữ liệu khác nhau

EIGRP lưu các con đường mà nó học được theo một cách đặc biệt. Mỗi con đường có trạng thái riêng và có đánh dấu để cung cấp thêm nhiều thông tin hữu dụng khác.

EIGRP có ba loại bảng sau

- Bảng láng giềng
- Bảng cấu trúc mạng
- Bảng định tuyến

Bảng láng giềng là bảng quan trọng nhất trong EIGRP. Mỗi router EIGRP lưu giữ một bảng láng giềng, trong đó là danh sách các router than mật với nó. Bảng này tương tự như cơ sở dữ liệu về các láng giềng của OSPF. Đỗi với mỗi giao thức mà EIGRP hỗ trợ, EIGRP có một bảng láng giềng tương ứng

Khi phát hiện một láng giềng mới router sẽ ghi lại địa chỉ và cổng kết nối của láng giềng đó vào bảng láng giềng. Khi láng giềng gửi gói hello. Trong đó có thông số về khoảng thời gian lưu giữ. nếu router không nhận được gói hello khi đến định ký thì khoảng thời gian lưu giữ là khoảng thời gian mà router chờ và vẫn xem là router láng giềng còn kếtnối được nhận được hello từ router láng giềng đó thì xem như router láng giềng đã không còn kết nối được hoặc không còn hoạt động thuật toán DUAL sẽ thông báo sự thay đổi này và thực hiện tính toán lại theo mạng mới

Bảng cấu trúc mạng là bảng cung cấp dữ liệu để xây dựng nên bảng định tuyến của EIGRP. DUAL lấy thông tin từ bảng láng giềng và bảng cấu trúc mạng để tính toán chọn đường có chi phí thấp nhất đến từng mạng đích

Mỗi EIGRP router lưu một bảng cấu trúc mạng riêng tương ứng với từng loại giao thức mạng khác nhau. Bảng cấu trúc mạng chứa thông tin về tất cả các con đương mà router học được. Nhờ những thông tin này mà router có thể xác định đường đi khác để thay thế nhanh chóng khi cần thiết. Thuật toán DUAL chọn ra đường tốt nhất đến mạng đích gọi là đường chính

Sau đây là những thông tin chứa trongbảng cấu trúc mạng:

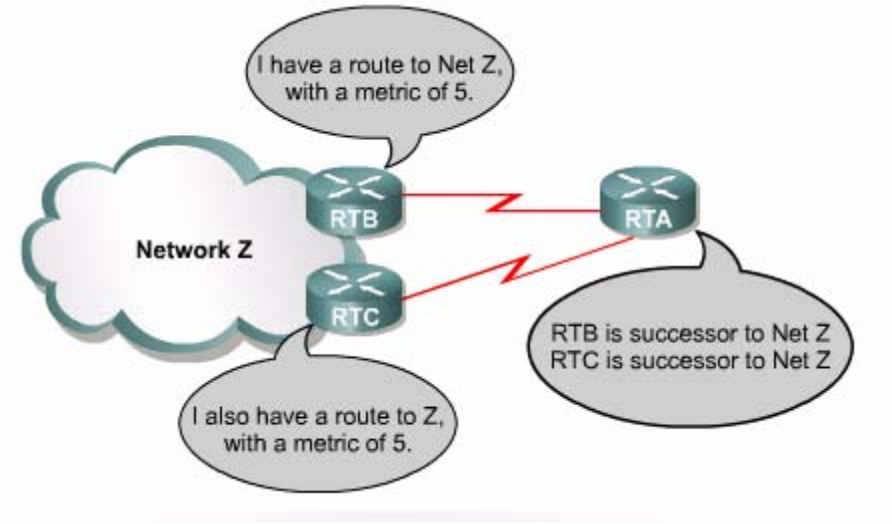
- Feasible distance (FD): là thông số định tuyến nhỏ nhất mà EIGRP tính được cho từng mạng đích
- Route source là nguồn khởi phát thông tin về một con đường nào đó. Phần thông tin này chỉ có đối với những đường được học từ ngoài mạng EIGRP
- Reported distance (RD) là thông số định tuyến đến một mạng đích do router láng giềng thân mật thông báo qua
- Thông tin về cổng giao tiếp mà route sử dụng để đi đến mạng đích
- Trạng thái đường đi: trạng thái không tác động là trạng thái ổn định, sẵn sang sử dụng được trạng thái tác động là trạng thái đang trong tiến trình tính toán lại của DUAL

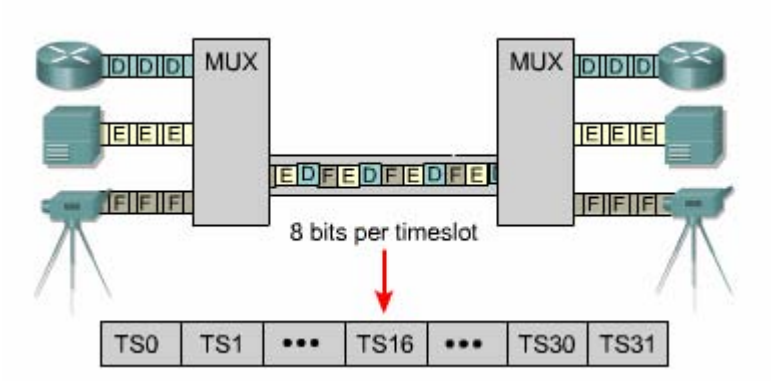
Bảng định tuyến EIGRP lưu giữ danh sách các đường tốt nhất đến các mạng đích. Những thông tin trong bảng định tuyến được rút ra từ bảng cấu trúc mạng. Router EIGRP có bảng định tuyến riêng cho ừng giao thức mạng khác nhau

Con đường được chọn làm đường chính đến mạng đích gọi là đường successor. Từ thông tin trong bảng láng giềng và bảng cấu trúc mạng, DUAL chọn ra một đường chính và đưa lên bảng định tuyến. Đến một mạng đích có thể có đến 4 successor. Những đường này có chi phí bằng nhau hoặc không bằng nhau. Thông tin về successor cũng được đặt trong bảng cấu trúc mạng

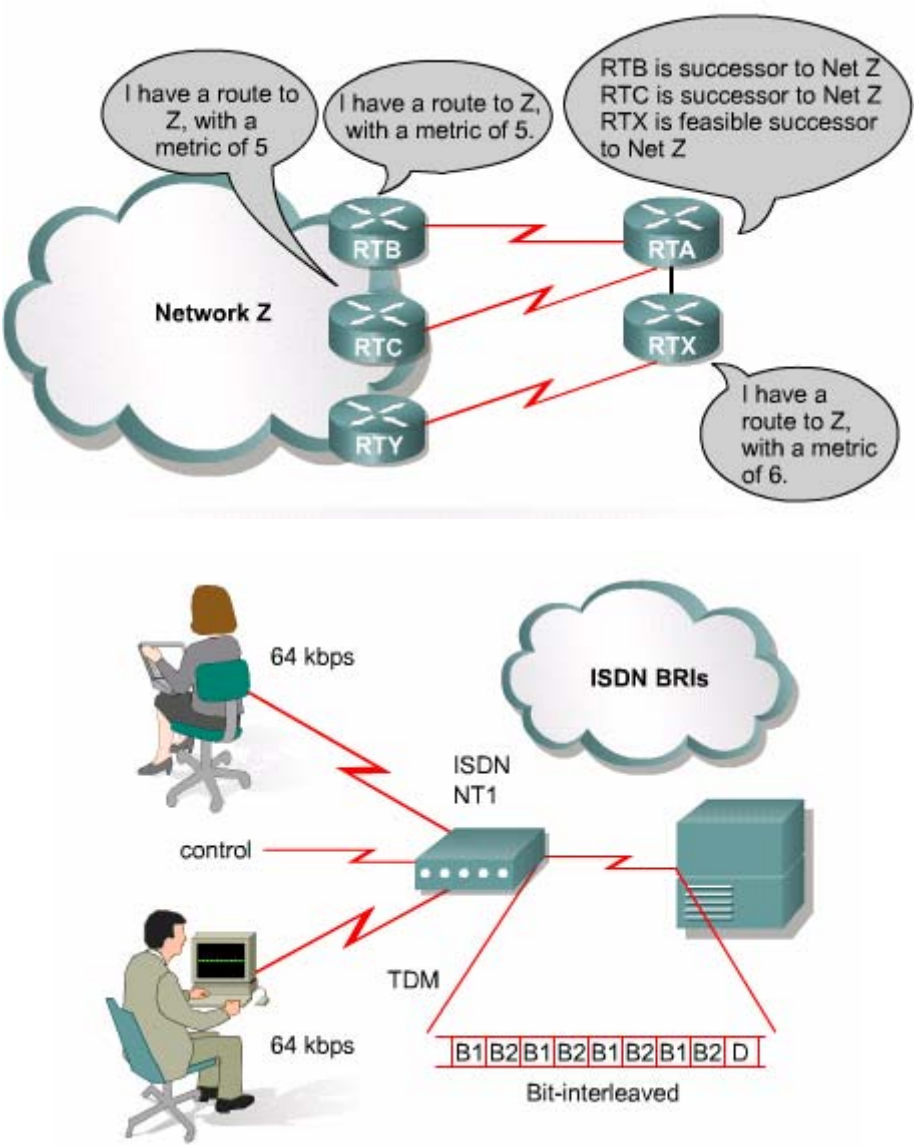
Đường Feasible sucessor (FS) là đường dự phòng cho đường successor. Đường này cũng được hcọn ra cùng với đường successor nhưng chúng chỉ được lưu lượng trong b ảng cấu trúc mạng. Đến một mạng đích có thể có nhiều feasible successor được lưu trong bảng cấu trúc mạng nhưng điều này không bắt buộc

Router xem hợp kế tiếp của đường feasible successor là hop dưới nó, gần mạng đích hơn nó. Do đó chi phí của feasible successor được tính bằng chi phí của chính nó cộng với chi phí mà router láng giềng thông báo qua. Trong trường hợp successor bị sự cố thì router sẽ tìm feasible successor để thay thế. Một đường feasible successor bắt buộc phải có chi phí mà route láng giềng thông báo qua thấp hơn chi phí của đường successor hiện tại. Nếu trong bảng cấu trúc mạng không có sẵn đường feasible successor thì con đường đến mạng đích tương ứng được đưa vào trạng thái Active và route bắt đầu gửi các gói yêu cầu đến tất cả các láng giềng để tính toán lại cấu trúc mạng . Sau đó với các thông tin mới nhận được router có thể sẽ chọn ra được successor mới hoặc feasible successor mới. Đường mới được chọn xong sẽ có trạng thái là Passive


I have a route to Net Z, with a metric of 5.
RTB
RTA
Network Z
RTC
RTB is successor to Net Z
RTC is successor to Net Z
I also have a route to Z, with a metric of 5.


MUX
MUX
8 bits per timeslot
TS0
TS1
TS16
TS30
TS31

Hình 3.1.2.a



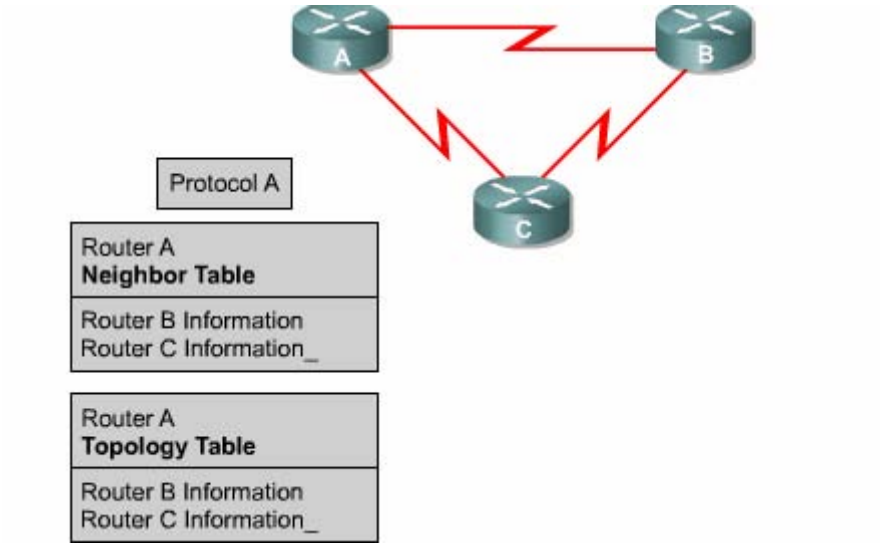
Hình 3.1.2.b

Bảng cấu trúc mạng còn lưu nhiều thông tin khác về các đường đi. EIGRP phân loại ra đường nội vi và đường ngoại vi. Đường nội vi là đường xuất phát từ bên trong hệ tự quản EIGRP, EIGRP có dãn nhãn với giá trị từ 0 đến 255 để phân biệt đường thuộc loại nào

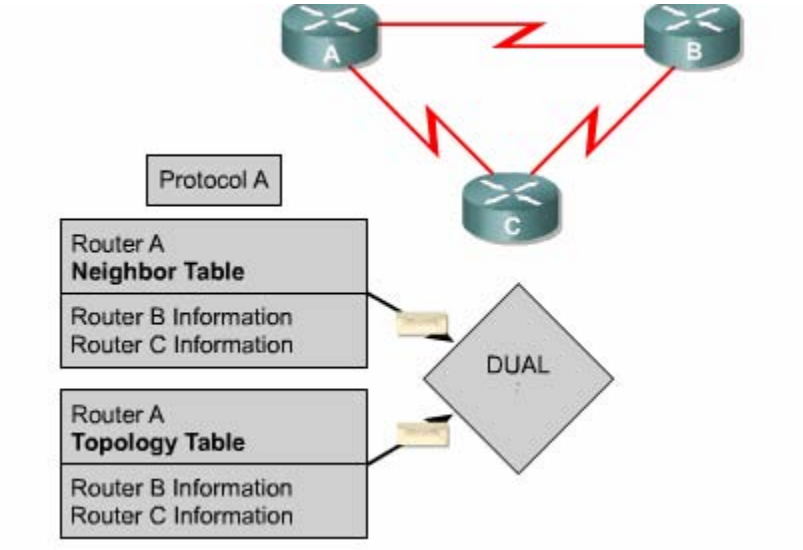
Đường ngoại vi là đường xuất phát từ bên ngoài AS của EIGRP. Các đường ngoại vi là nững đường được học từ các giao thức định tuyến khác như RIP, OSPF và IGRP. Đường cố định cũng được xem là đường ngoại vi

```
RTX#show ip eigrp topology 204.100.50.0
IP-EIGRP topology entry for 204.100.50.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s),
FD is 2297856
  Routing Descriptor Blocks:
  10.1.0.1 (Serial0), from 10.1.0.1, Send flag is 0x0
      Composite metric is (2297856/128256), Route is External
      Vector metric:
        Minimum bandwidth is 1544 Kbit
        Total delay is 25000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
      External data:
        Originating router is 192.168.1.1
        AS number of route is 0
        External protocol is Connected, external metric is 0
        Administrator tag is 0 (0x00000000)
```

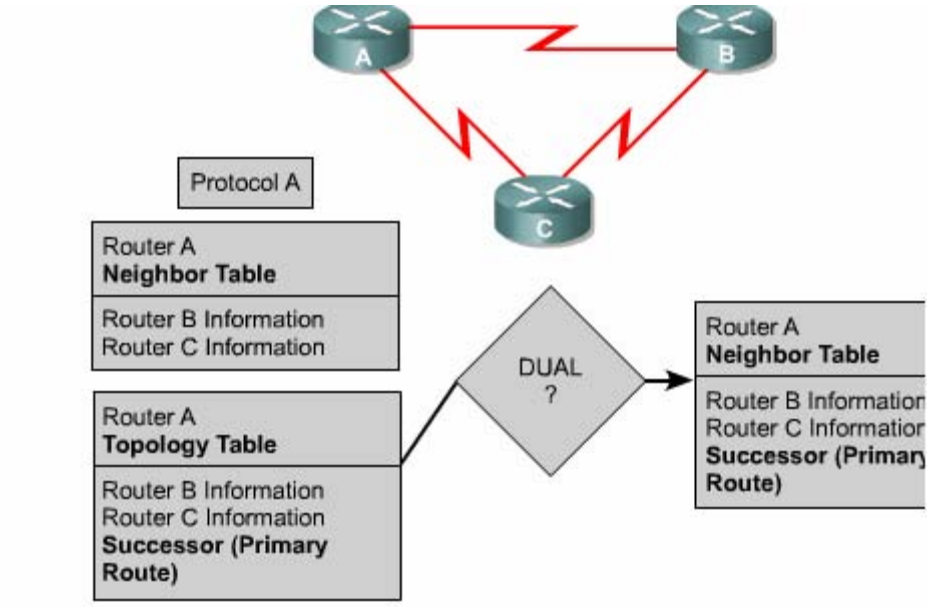
Hình 3.1.2.c



Hình 3.1.2.d



Hình 3.1.2.e



Hình 3.1.2.f

3.1.3 Các đặc điểm của EIGRP

EIGRP hoạt động khác với IGRP, về bản chất EIGRP là một giao thức định tuyến theo vectơ khoảng cách nâng cao nhưng khi cập nhật và bảo trì thông tin láng giềng và thông tin định tuyến thì nó làm việc giống như một giao thức định tuyến theo trạng thái đường liên kết . Sau đây là các ưu điểm của EIGRP so với giao thức định tuyến theo vectơ khoảng cách thông thường

- Tốc độ hội tụ nhanh
- Sử dụng băng thông hiệu quả
- Có hỗ trợ VLSM và CIDR. Không giống như IGRP EIGRP có trao đổi thông tin về subnet mask nên nó hỗ trợ được cho hệ thống IP không theo lớp
- Hỗ trợ cho nhiều giao thức mạng khác nhau
- Không phụ thuộc vào giao thức được định tuyến. Nhờ cấu trúc từng phần riêng biệt tương ứng với từng giao thứ mà EIGRP không cần phải chỉnh sửa lâu. Ví dụ như khi phát triển để hỗ trợ một giao thức mới như IP chẳng hạn. EIGRP cần phải có thêm phần mới tương ứng cho IP nhưng hoàn toàn không cần phải viết lại EIGRP

EIGRP router hội tụ nhanh vì chúng sử dụng DUAL, DUAL bảo đảm hoạt động không bị lặp vòng khi tính toán đường đi cho phép mọi router trong hệ thống mạng thực hiện đồng bộ cùng lúc khi có sự thay đổi xảy ra

EIGRP sử dụng băng thông hiệu quả vì nó chỉ gửi thông tin cập nhật một phần và giới hạn chứ không gửi toàn bộ bảng định tuyến. Nhờ vậy nó chỉ tổn một lượng băng thông tối thiểu khi hệ thống mạng đã ổn định. điều này tương tự như hoạt động cập nhật OSPF nhưng không giống như router OSPF router EIGRP chỉ gửi thông tin cập nhật một router khác trong vùng như OSPF Chính vì vậy mà hoạt động cập nhật của EIGRP gọi là cập nhật giới hạn. Thay vì hoạt động cập nhật theo chu kỳ các router EIGRP giữ liên lạc với nhau bằng các gói hello rất nhỏ. Việc trao đôi các gói hello theo định kỳ không chiếm nhiều băng thông đường truyền

EIGRP có thể hỗ trợ cho IP, IPX và Apple talk nhờ có cấu trúc từng phần theo giao thức, EIGRP có thể phân phối thông tin của IPX RIP và SAP để cải tiến hoạt động toàn diện. Trên thực tế EIGRP có thể điều khiển hai giao thức này Router EIGRP nhận thông tin định tuyến dịch vụ, chỉ cập nhật cho các router khác nhau khi thông tin trong bảng định tuyến hay bảng SAP thay đổi

EIGRP còn có thể điều khiển giao thức Alpha talk routing table maintenance Protocol (RTMP) RTMP sử dụng số lượng để chọn đường nên khả năng chọn đường khôngđược tốt lắm. Do đó, EIGRP sử dụng thông số định tuyến tổng hợp cấu hình được để chọn đường tốt nhất cho mạng Apple talk. Là một giao thức định tuyến theo vectơ khoảng cách RTMP thực hiện trao đổi toàn bộ thông tin định tuyến theo chu kỳ. Để giảm bớt sự quá tải này EIGRP thực iện phân phối thông tin định tuyến Apple talk khi có sự kiện thay đổi mà thôi. Tuy nhiên apple talk client cũng muốn nhận thông tin RTMP từ các router nội bộ do đó EIGRP dùng

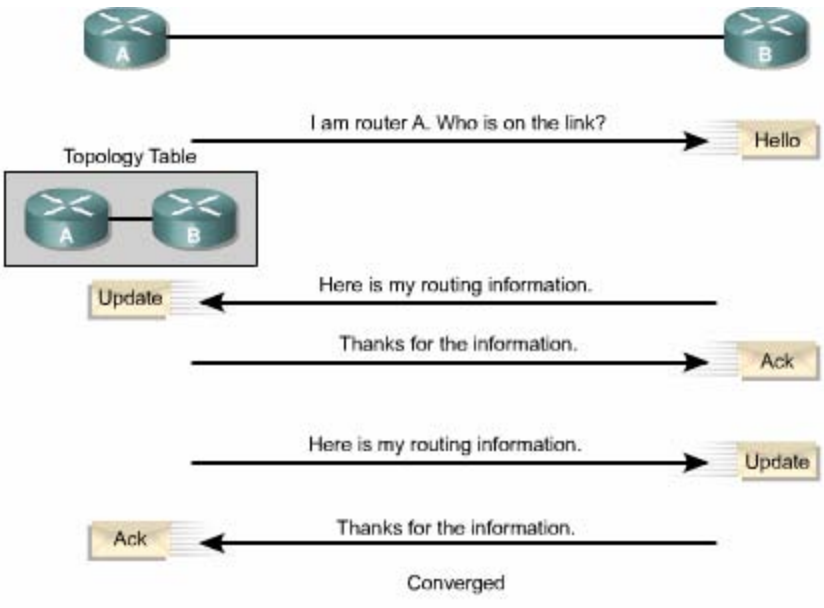
cho Apple talk chỉ nên chạy trong mạng không có client ví dụ nhưcác liên kết WAN chẳng hạn

3.1.4 Các kỹ thuậtcủa EIGRP

EIGRP có rất nhiều kỹ thuật mới để cải tiến hiệu quả hoạt động tốc độ hội tụ và các chức năng so với IGRP và các giao thức định tuyến khác. Các kỹ thuật này được tập trung thành 4 loại như sau:

- Sự phát hiện và tái phát hiện các router láng giềng
- Giao thức truyền tải tin cậy
- thuật toán DUAL finite – sate machine
- Cấu trúc từng phần theo giao thức

Router định tuyến theo vectơ khoảng cách dạng đơn giản không thiết lập mối quan hệ với các láng giềng của nó. RIP và IGRP route chỉ đơn giản là phát quảng bá hay multicast các thông tin cập nhật của nó ra mọi cổng đã được cấu hình. Ngược lại, EIGRP router chủ động thiết lập mối quan hệ với các láng giềng của chúng tương tự như cách làm của OSPF router



Hình 3.1.4

Quá trình EIGRP router thiết lập mối quan hệ than mật được mô tả trong hình 3.1.4. EIGRP route sử dụng các gói hello rất nhỏ để thực hiện việc thiết lập mối

quan hệ than mật với các router láng giềng. Mặc định hello được gửi đi theo chu kỳ là 5 giây. Nếu router vẫn nhận được hello từ láng giềng thì nó sẽ xem như láng giềng này và các đường đi của nó vẫn còn hoạt động . Bằng cách thiết lập mối quan hệ này, EIGRP router có thể thực hiện được những việc sau
- Tự động học được đường mới khi chúng kết nối vào hệ thống mạng

- Xác định một router không còn kết nối hoặc không còn hoạt động nữa
- Phát hiện sự hoạt động trở lại của các router

Giao thức vận chuyển tin cậy RTP là giao thức ở lớp vận chuyển thực hiện chuyển gói EIGRP một cách tin cậy và có thứ tự đến tất cả các láng giềng. Trong mạng IP host sử dụng TCP để vận chuyển các gói một cách tuần tự và tin cậy. Tuy nhiên EIGRP là một giao thức độc lập với giao thức mạng do đó nó không dựa vào TCP/IP để thực hiện trao đổi thông tin định tuyến giống như RIP, IGRP và OSPF đã làm . Để không bị phụ thuộc vào IP, ẺIGP sử dụng RTP làm giao thức vận chuyển riêng độc quyền của nó để đảm bảo việc truyền thông tin định tuyến

EIGRP có thể yêu cầu RTP cung cấp dịch vụ truyền tin cậy hoặc không tin cậy tuỳ theo yêu cầu của từng trường hợp. Ví dụ các gói hello được truyền theo định kỳ và cần phải càng nhỏ càng tốt nên chúng không cần phải dùng chế độ truyền tin cậy. Ngược lại việc truyền tin cậy các thông tin định tuyến sẽ có thể làm tăng tốc độ hội tụ vì EIGRP router không cần hết thời hạn mới truyền lại

Với RTP, EIGRP có thể gửi multicast và trực tiếp cho các đối tác khác nhau cùng một lúc giúp tối ưu hiệu quả hoạt động

Thành phần trung tâm của EIGRP là thuật toán DUAL là bộ máy tính toán đường đi cuả EIGRP. Tên đầy đủ của kỹ thuật này là DUAL finite - state machine . FMS là một bộ máy thuật toán nhưng không phải là một thiết bị cơ khí có các thành phần di chuyển được. FSM định nghĩa một tập hợp các trạng thái có thể trải qua, sự kiện nào gây ra trạng thái nào và sẽ có kết quả là gì. Người thiết kế sử dụng FSM để lập trình cách mà một thiết bị một chương trình máy tính hay một thuật toán định tuyến sẽ xử lý như thế nào với một tập hợp các dữ kiện đầu vào. DUAL FSM chứa tất cả các logic được sử dụng để tính toán và so sánh đường đi trong mạch EIGRP

DUAL lưu tất cả các đường mà láng giềng thông báo qua. Dựa trên thông số định tuyến tổng hợp của mỗi đường, DUAL so sánh và chọn ra đường có chi phí thấp

nhất đến đích. DUAL đảm bảo mỗi một đường này là không có lặp vòng. Đường chính được chọn ra gọi là đường successor. Đường successor được lưu trên bảng định tuyến và đồng thời cũng được lưu trong bảng cấu trúc mạng

EIGRP giữ các thông tin quan trọng về đường đi và cấu trúc mạng trong bảng láng giềng và bảng cấu trúc mạng. Hai bảng này cung cấp cho DUAL các thông tin về đường đi khi cần thiết. Nếu có một đường liên kết bị đứt, DUAL sẽ tìm đường thay thế hoặc một feasible successor trong bảng cấu trúc mạng

Một trong những ưu điểm nổi bật của EIGRP là nó được thiết kế thành từng phần riêng biệt theo giao thức. Nhờ cấu trúc này, nó có khả năng mở rộng và tương thích tốt nhất. Các giao thức được định tuyến như IP, IPX và Apple Talk được đưa vào EIGRP thông qua các PDM EIGRP có thể dễ dàng tương thích với giao thức được định tuyến mới hoặc các phiên bản mới của chúng như IPv6 chẳng hạn bằng cách thêm PDM vào.

Mỗi PDM chịu trách nhiệm thực hiện mọi chức năng liên qan đến một giao thức được định tuyến. Ví dụ phần IP – EIGRP chịu trách nhiệm các việc sau:

- Gửi và nhận các gói EIGRP chứa dữ liệu IP
- Thông báo cho DUAL khi nhận được thông tin định tuyến IP mới
- Duy trì kết quả chọn đường của DUAL trong bảng định tuyến IP
- Phân phối thông tin định tuyến mà nó học được từ các giao thức định tuyến IP khác

3.1.5 Cấu trúc dữ liệu của EIGRP

Giống như OSPF EIGRP dựa vào nhiều loại gói dữ liệu khác nhau để duy trì các loại bảng của nó và thiết lập mối quan hệ phức tạp với router láng giềng

Có 5 loại gói EIGRP

- Hello
- Báo nhận
- Cập nhật
- Yêu cầu
- Đáp úng

EIGRP dựa vào các gói hello để phát hiện, kiểm tra và tái phát hiện các router láng giềng. Tái phát hiện có nghĩa là router EIGRP không nhận được hello từ một router

láng giềng trong suốt khoảng thời gian lưu giữ nhưng sau đó router láng giềng này lại tái lập lại thông tin liên lạc

Chu kỳ gửi hello của EIGRP router có thể cấu hình được. Khoảng thời gian hello mặc định phụ thuộc vào băng thông trên từng cổng của router. Trong mạng IP, EIGRP router gửi hello theo địa chỉ multicast 224.0.0.10

EIGRP router lưu thông tin về các láng giềng trong bảng láng giềng. Bảng láng giềng này có lưu số thứ tự và thời gian lưu giữ của gói EIGRP cuối nhận được từ mỗi router láng giềng. Theo định kỳ và trong giới hạn củak hoảng thời gian lưu giữ. Router phải nhận được gói EIGRP thì những đường tương ứng mới có trạng thái Pasive. Trạng thái Passive có nghĩa là trạng thái hoạt động ổn định

Nếu roter không nghe ngóng được gì về router láng giềng trong suốt khoảng thời gian lưu giữ thì EIGRP sẽ xem như láng giềng đó đã bị sự cố và DUAL phải tính oná lại bảng định tuyến. Mặc định khoảng thời gian lưu giữ gấp 3 lần chu kỳ hello. Người quản trị mạng có thể cấu hình giá trị cho 2 khoảng thời gian này phù hợp hơn với hệ thống của mình

Bandwidth	Example Link	Default Hello Interval	Default Hold Time
1.544 Mbps or less	Multipoint Frame Relay	60 seconds	180 seconds
Greater than 1.544 Mbps	T1, Ethernet	5 seconds	15 seconds

Hình 3.1.5

OSPF bắt buộc các router láng giềng với nhau phải có cùng khoảng thời gian hello và khoảng thời gian bất đọng thì mới có thể thông tin liên lác với nhau được. EIGRP thì không yêu cầu như vậy. Router sẽ học các khoảng thời gian của router láng giềng thông qua việc trao đổi gói hello. Chúng sẽ dùng thông tin trong đó thiết lập mối quan hệ ổn định mà không cần các khoảng thời gian này phải giống nhau giữa chúng.

Gói hello thường được gửi theo chế độ không bảo đảm tin cậy. Điều này có nghĩa là không có báo nhận cho các gói hello

EIGRP router sử dụng gói báo nhận để xác nhận là đã nhận được gói EIGRP trong quá trình trao đổi tin cậy. Giao thức vận chuyển tin cậy cung cấp dịch vụ liên lạc tin cậy giữa hai host EIGRP. Gói báo nhận chính là gói hello mà không có dữ liệu. Không giống như hello được gửi multicast các gói báo nhận chỉ gửi trực tiếp cho một máy nhận. Báo nhận có thể được kết hợp vào loại gói EIGRP khác như gói trả lời chẳng hạn

Gói cập nhật được sử dụng khi router phát hiện một láng giềng mới. Router EIGRP sẽ gửi gói cập nhật cho router láng giềng mới này để nó có thể xây dựng bảng cấu trúc mạng. Có thể sẽ cần nhiều gói cập nhật mới có thể truyền tải hết các thông tin cấu trúc to

Gói cập nhật còn được sử dụng khi router phát hiện sự thay đổi trong cấu trúc mạng. Trong trường hợp này EIGRP router sẽ gửi multicast gói cập nhật cho mọi router láng giềng của nó để thông báo về sự thay đổi . Mọi gói cập nhật đều được gửi bảo đảm

EIGRP router sử dụng gói yêu cầu khi nó cần một thông tin đặc biệt nào đó từ một hay nhiều láng giềng của nó. Gói đáp ứng được sử dụng để trả lời cho các gói yêu cầu

Nếu một EIGRP router mất successor và nó không tìm được feasible successor để thay thế thì DUAL sẽ đặt con đường đến mạng đích đó vào trạng thái Active. Sau đó route gửi multicast gói yêu cầu đến tất cả các láng giềng để cố gắng tìm successor mới cho mạng đích này. Router láng giềng phải trả lời bằng gói đáp ứng để cung cấp thông tin hoặc cho biết là không có thông tin nào khác có thể khả thi. Gói yêu cầu có thể được gửi multicast hoặc chỉ gửi cho một máy, còn gói đáp ứng thì chỉ gửi cho máy nào gửi yêu cầu mà thôi. Cả hai loại gói này đều được gửi bảo đảm

3.1.6 Thuật toán EIGRP

Thuật toán DUAL phức tạp giúp co EIGRP hội tụ nhanh. Để hiểu rõ hơn về quá trình hội tụ với DUAL ta étt ví dụ ở hình 3.1.6.a. Mỗi router xấy dựng một bảng cấu trúc mạng chứa các thông tin về đường đi đến mạng A

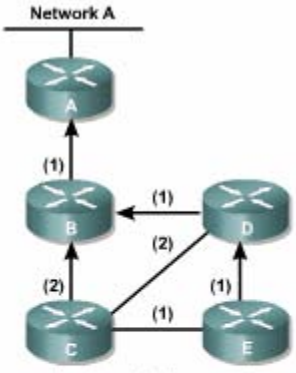
Mỗi bảng cấu trúc mạng trong ví dụ ở các hình 3.1.6.a – f có các thông tin sau

- Giao thức định tuyến là giao thức EIGRP

- Chi phí thấp nhất của đường đến một mạng đích gọi là Feasible Distance
- Chi phí của đường đến một mạng đích do router láng giềng thông báo qua gọi là Reported Distance

Nguyên tắc chọn đường feasible successor

1. Đường feasible successor là đường dự phòng thay thế cho đường successor khi đường này bị sự cố
2. Reported Distance của một đường đến một đích nào đó là chi phí được thông báo từ router láng giềng. Chi phí này phải nhỏ hơn Feasible Distance của đường successor hiện tại
3. Nếu thoả điều kiện trên thì có nghĩa là không có vòng lặp đường đó sẽ được chọn làm feasible successor
4. Đường feasible successor có thể thay thế cho đường successor khi cần thiết
5. Nếu RD của mộ đường lớn hơn hoặc bằng FD của successor hiện tại đường đó không được chọn làm feasible successor
6. Router phải tính toán cấu trúc mạng bằng cách thu thập thông tin từ tất cả các láng giềng
7. Router gửi gói các yêu cầu đến tất cả các láng giềng để tìm thông tin về đường đi và chi phí của đường đó đến mạng đích mà router đang cần
8. Tất cả các láng giềng phải gửi gói đáp ứng để trả lời cho gói yêu cầu
9. Router ghi nhận dữ liệu mới nhận được vào bảng cấu trúc mạngcủa mình
10. Bây giờ DUAL đã có thể xác định đường successor mới và feasible successor mới nếu có dựa vào thông tin mới



Numbers in () = metric

C EIGRP	FD	RD	Topology
Network A	3		(FD)
via B	3	1	(Successor)
via D	4	2	(FS)
via E	4	3	

D EIGRP	FD	RD	Topology
Network A	2		(FD)
via B	2	1	(Successor)
via C	5	3	

E EIGRP	FD	RD	Topology
Network A	3		(FD)
via D	3	2	(Successor)
via C	4	3	

Legend	
EIGRP	Protocol Type
FD	Feasible Distance
RD	Reported Distance as advertised by neighbor router
Successor	Primary Route to Destination
FS	Feasible Successor - Backup route to Destination

Hình 3.1.6.a

Cột Topology trong hình cho biết đường nào là đường chính hay còn gọi là successor, đường nào là đường dự phòng hay còn gọi là feasible successor. Tuy nhiên bạn cần lưu ý là không nhất thiết lúc nào cũng phải tìm được feasible successor

Mạng EIGRP sẽ hoạt động theo các bước mô tả bên dưới để tiến hành hội tụ giữa các router. Hiện tại các router có các thông tin về đường đến Mạng A như sau"

Router C có một đường successor là đường qua Router B

Router C có một đường f easible succ esor là đường qua Router B

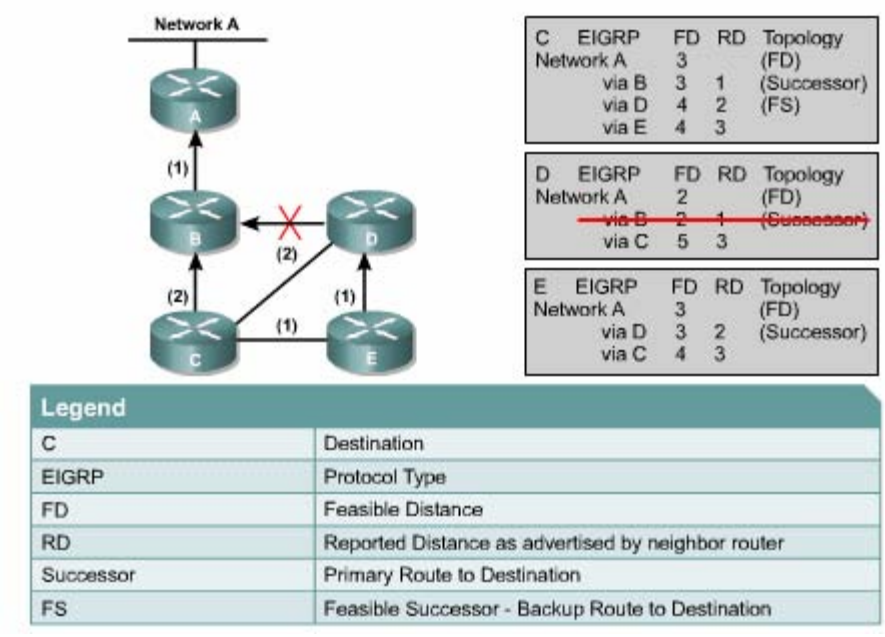
Router D có một đường successor là đường qua Router B

Router D không có đường feasible successor

Router E có một đường successor là đường qua router D

Router E không có đường feasible successor

Sau đây sẽ mô tả mỗi router thực hiện nguyên tắc chọn feasible successor như thế nào khi đường liên kết giữa router D và router B bị đứt



Legend	
C	Destination
EIGRP	Protocol Type
FD	Feasible Distance
RD	Reported Distance as advertised by neighbor router
Successor	Primary Route to Destination
FS	Feasible Successor - Backup Route to Destination

Hình 3.1.6.b

Trong router D (hình 3.1.6.B)

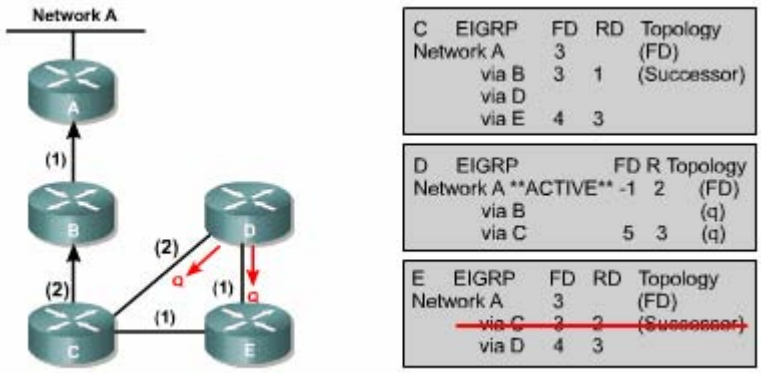
- Đường đi qua router B bị xoá khỏi bảng cấu trúc mạng
- Đường này là đường successor. Router không xác định được feasible successor trước đó
- Router D phải tính toán lại đường mới

Trong Router C:

Đường đến mạng A qua router D bị đứt

Đường này bị xoá khỏi bảng

Đường này là successor của router C



Hình 3.1.6.c

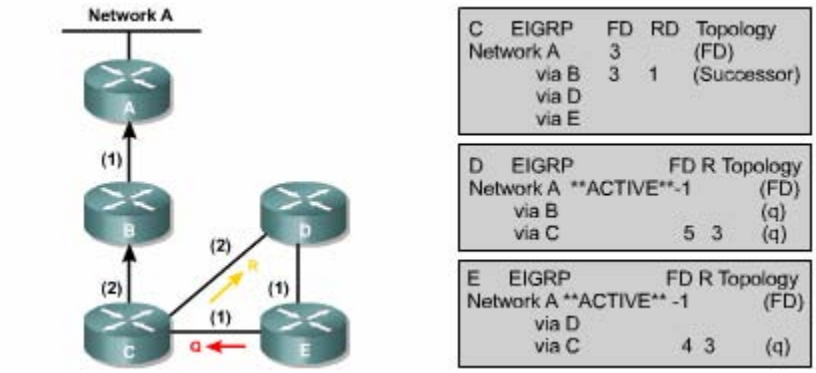
Trong router D

- Router D không có feasible successor. Do đó nó không thể chuyển qua đường dự phòng được
- Router D phải tính toán lại cấu trúc mạng. Con đường đến Mạng A được đặt vào trạng thái Active
- Router D gửi gói yêu cầu cho tất cả các láng giềng kết nối với nó là router C và router R để yêu cầu gửi thông tin về mạng
- Trước đó router C có đường qua router D
- Trước đó router D không có đường qua router E

Trong router E:

- Đường đến Mạng A thông qua router D bị đứt
- Đường này là đường successor của router E
- Router E không có feasible successor

- Lưu ý rằng RD của đường thông qua Router C là 3 bằng với chi phí của đường successor qua router D



Hình 3.1..6.d

Trong router C

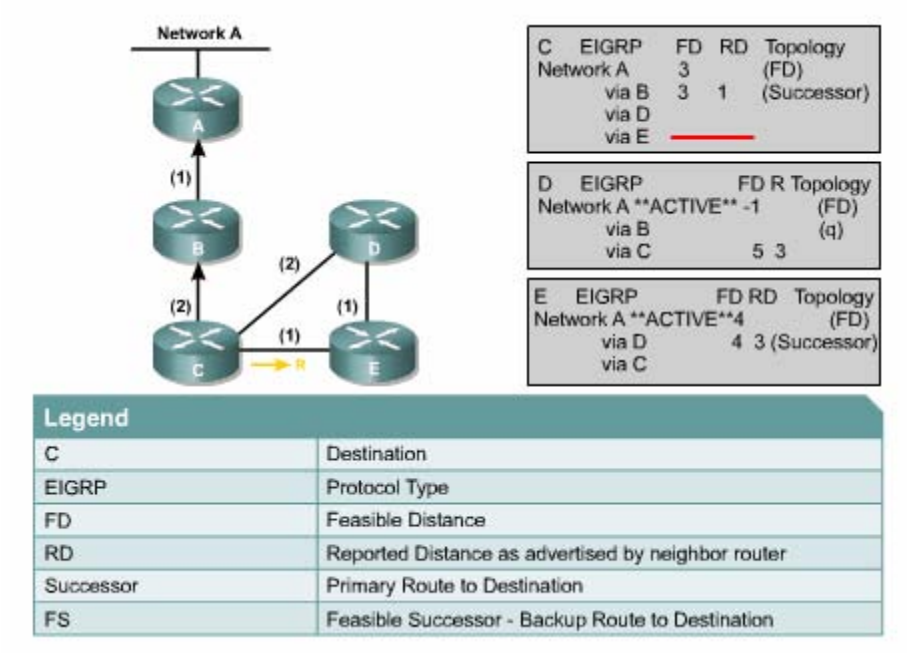
- Router E gửi gói yêu câud cho Router C
- Router C xoá đường qua Router khỏi bảng
- Router C trả lời cho Router với thông tin về đường mới đến Mạng A

Trong Router D

- Trạng thái của đường đến Mạng A vẫn là Active vì công việc tính toán lại chưa hoàn tất
- Router C trả lời cho Router D để xác nhận là đường đến mạng A đang hoạt động với chi phí là 5
- Router D vẫn đangchờ đáp ứng từ router E

Trong router E

- Router E không có feasible successor đến Mạng A
- Do đó, router E đánh dấu trạng thái con đường đến mạng A là Active
- Router E phải tính toán lại cấu trúc mạng
- Router E xoá đường đi qua Router D ra khỏi bảng
- Router E gửi gói yêu cầu cho router C để yêu cầu thông tin về mạng
- Trước đó, router E đã có thông tin về đường đi qua router C. Đường này có chi phí là 3 , bằng với chi phí của đường successor

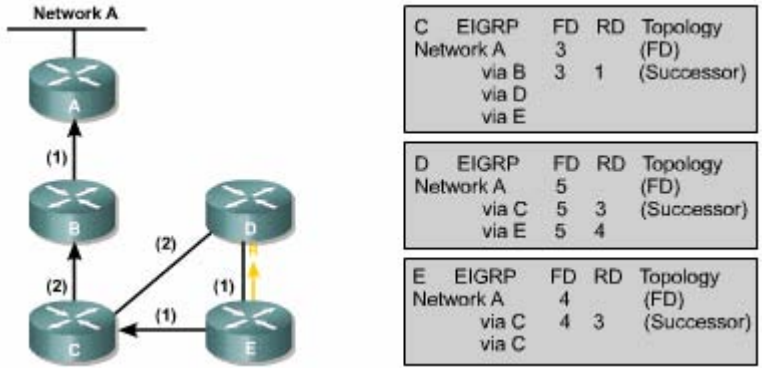


Legend	
C	Destination
EIGRP	Protocol Type
FD	Feasible Distance
RD	Reported Distance as advertised by neighbor router
Successor	Primary Route to Destination
FS	Feasible Successor - Backup Route to Destination

Hình 3.1.6.e

Trong router E (hình 3.1.6.e)

- Router C trả lời lại thông tin về đường đến Mạng A có RD là 3
- Bây giờ router E có thể chọn đường qua router C làm successor mới với FD là 4 và RD là 3
- Trạng thái của đường đến Mạng A được đổi từ Active sang Pasive. Lưu ý trạng thái Passive là trạng thái mặc định khi router vẫn nhận được gói hello từ đường đó. Do đó trong ví dụ này chỉ cần đánh dấu trạng thái Active thôi



Hình 3.1.6.f

Trong router E (hình 3.1.6f)

- Router E gửi đáp ứng cho Router D để cung cấp thông tin về mạng của router E

Trong router D

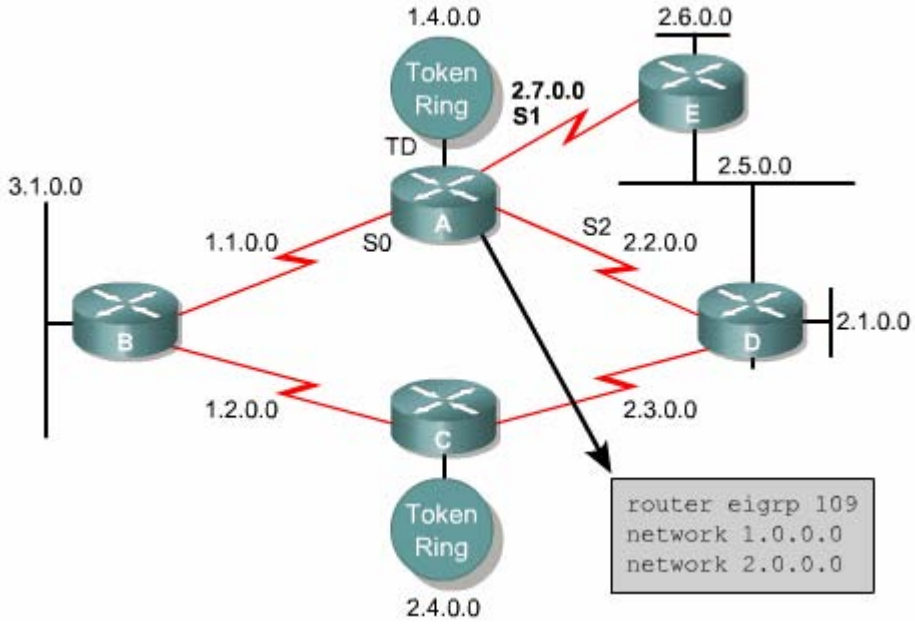
- Router D nhận được gói hồi đáp từ router E với những thông tin về mạng của router E
- Router D ghi nhận con đường đến Mạng A thông qua router E
- Con đường này trở thành một đường successor nữa vì nó có chi phí bằng với đường thông qua router C và nó có RD nhỏ hơn FD của đường thông qua router

Quá trình hội tụ xảy ra giữa mọi router EIGRP sử dụng thuật toán DUAL

3.2Cấu hình EIGRP

3.2.1 Cấu hình EIGRP

Trù thuật toán DUAL là phức tạp còn cấu hình EIGRP thì khá đơn giản tuỳ theo giao thức được định tuyến là IP, IPX hay Apple Talk mà câu lệnh cấu hình EIGRP sẽ khác nhau. Phần sau đây chỉ đề cập đếncấu hình EIGRP cho giao thức IP



Hình 3.2.1

Sau đây là các bước cấu hình EIGRP cho ip

1. Sử dụng lệnh sau khởi động EIGRP và xác định con số của hệ tự quản

Thông số autonomous system number xác định các router trong một hệ tự quản. Những router nào trong cùng một hệ thống mạng thì phải có con số này giống nhau

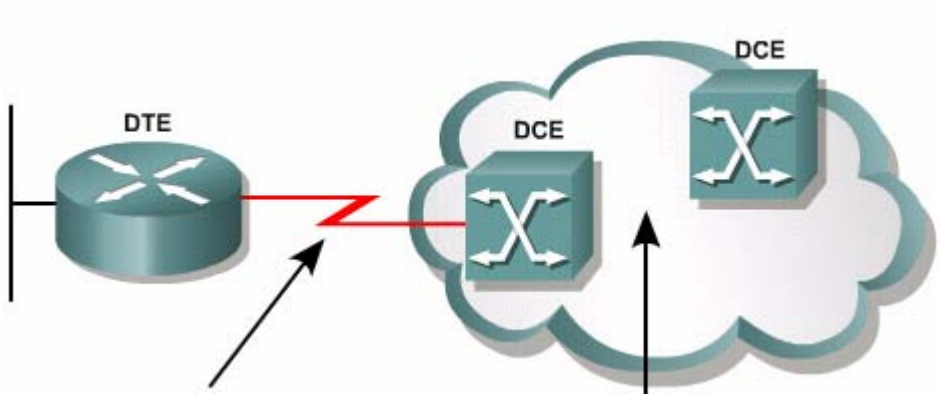
2. Khai báo những mạng nào của router mà bạn đang cấu hình thuộc về hệ tự quản

Thông số network number là địa chỉ mạng của các cổng giao tiếp trên router thuộc về hệ thống mạng EIGRP. Router sẽ thực hiện

5.1 *Các khái niệm về Frame Relay*:

5.1.1 Giới thiệu Frame Relay:

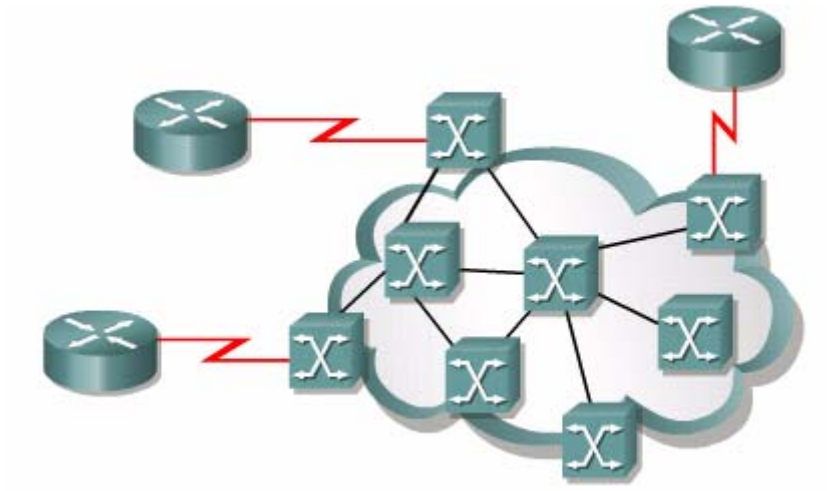
Frame Relay là chuẩn của ITU-T(International Telecômunication Union Telcommunication Stanđardization Sector) và WASI (American Natịonal Standards Institute). Frame Relay là dịch vụ WAN chuyển mạch gói theo hướng kết nối. Frame Relay hoạt động ở lớp Liên kết dữ liệu của mô hình OSI. Frame Relay sử dụng một phần giao thức HDLC làm giao thức LAPF (Link Access Procedure for Frame Relay). Frame Relay thực hiện truyền frame giữa thiết bị của người dùng DTE và thiết bị DCE tại danh giới của mạng WAN.

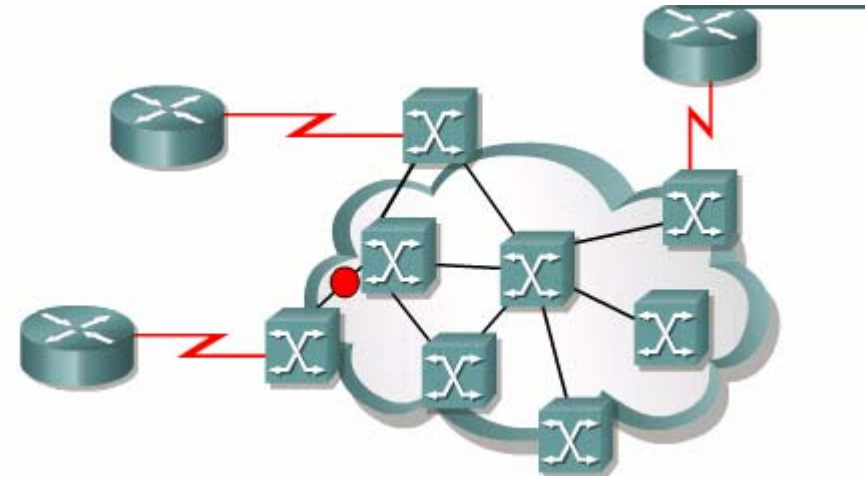


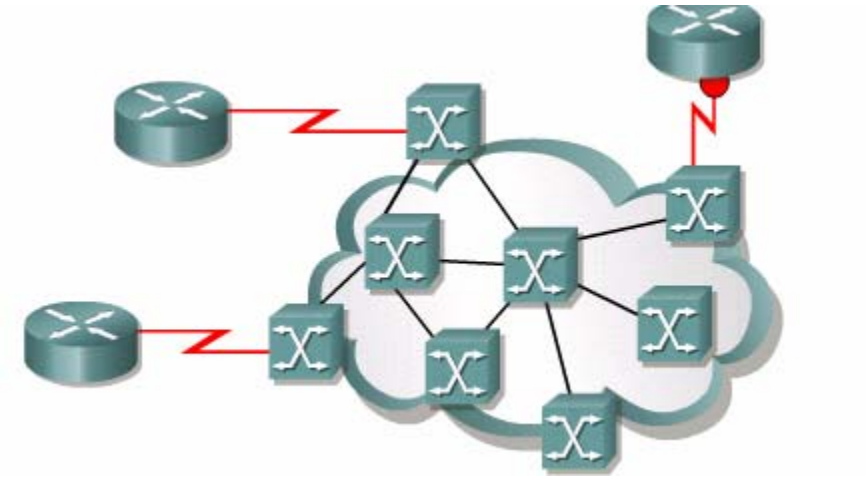
Ban đầu Frane Relay được thiết kế để cho phép thiết bị ISDN có thể truy cập vào dịch vụ chuyển mạch gói trên kênh B. Nhưng bây giờ Frame Relay đã là một công nghệ hoàn toàn độc lập.

Mạng Frame Relay có thể thuộc sở hữu riêng của người dùng nhưng thông thường là được cung cấp bởi các công ty dịch vụ viễn thông.

Frame Realay thường được sử dụng để kết nối các mạng LAN. Mỗi Router biên giới của một mạng LAN là một DTE. Một kết nối nối tiếp, ví dụ như E1/T1, sẽ kết nối vào Frame Relay switch gần nhất của nhà cung cấp dịch vụ. Frame Relay switch chính là thiết bị DCE.





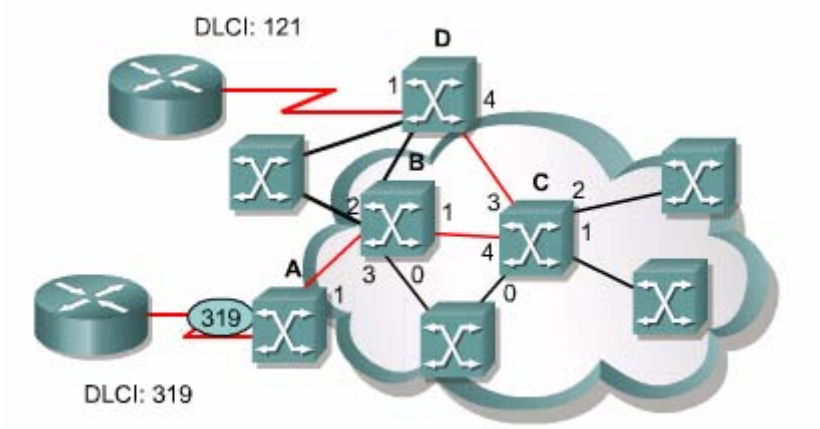


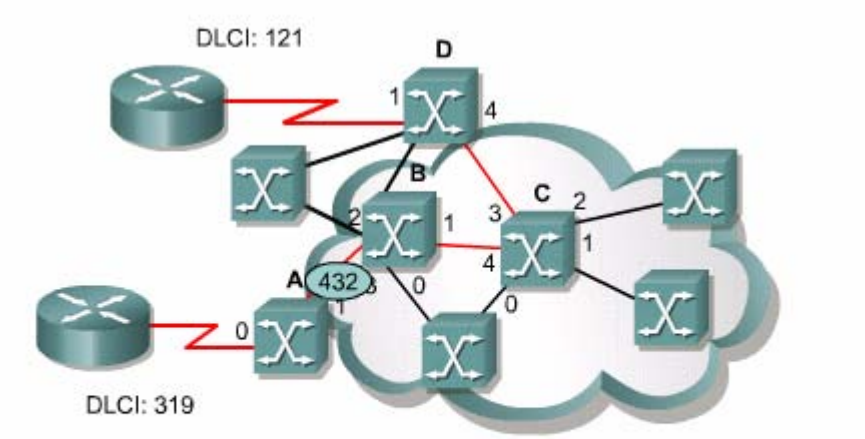
Thiết bị máy tính không nằm trong một mạng LAN cũng có thể gửi dữ liệu qua mạng Frame Relay. Thiết bị máy tính này sử dụng thiết bị truy cập Frame Relay (FRAD) làm DTE.

5.1.2 Các thuật ngữ của Frame Relay:

Kết nối giữa hai DTE qua mạng Frame Relay được gọi là kết nối ảo (VC — Virtual Circuit). Các kết nối ảo chuyển mạch (SVC — Switched virtual

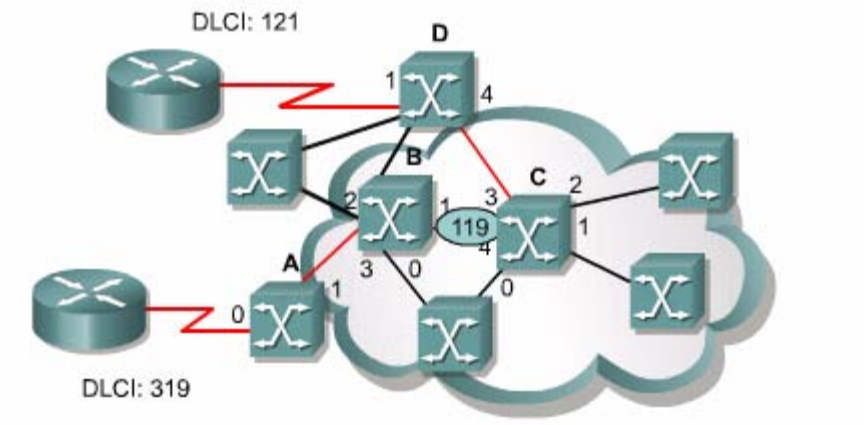
Circuit) có thể được thiết lập tự động bằng cách gửi đi các thông điệp báo hiệu. Tuy nhiên SVC không được sử dụng phổ biến lắm.Kết nối ảo cố định PVC (Permanent virtual circuit) được sử dụng nhiều hơn với cấu hình dịnh trươc của nhà cung cấp. Trên mỗi Frame Relay switch có lưu giữ sơ đồ ánh xạ giữa port vào và port ra tương ứng với mỗi VC. Do đó mỗi kết nối VC được thiết lập từ một điểm cuối thông qua các switch đeens điểm cuối được xác định duy nhất.





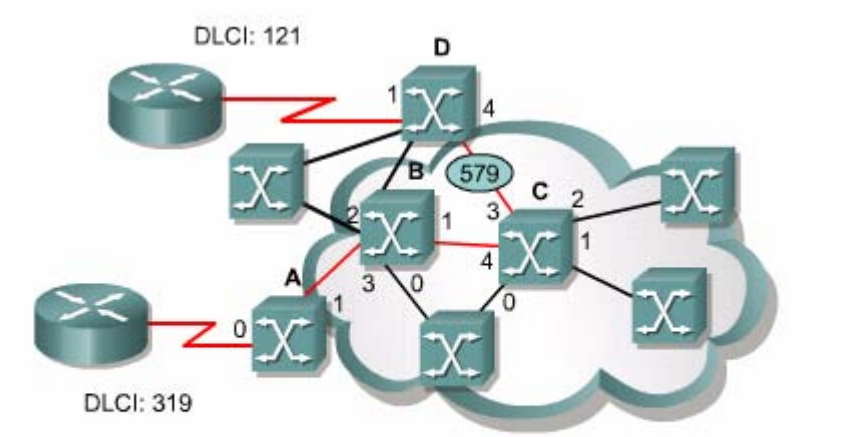
A

VC	Port	VC	Port
319	0	432	1



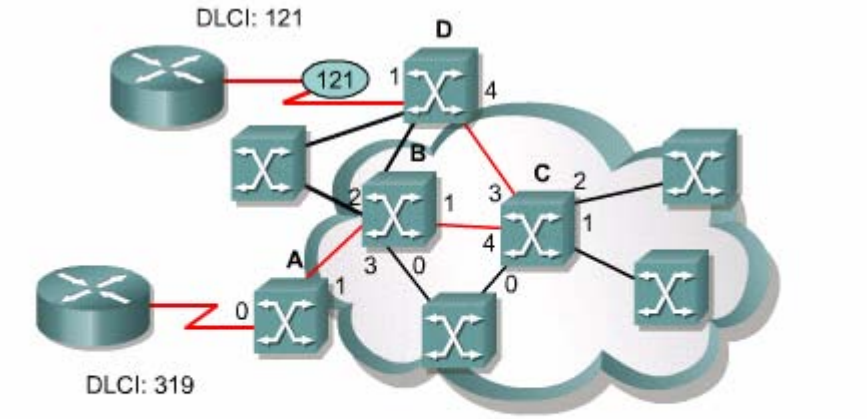
B

VC	Port	VC	Port
432	3	119	1



C

VC	Port	VC	Port
119	4	579	3



D

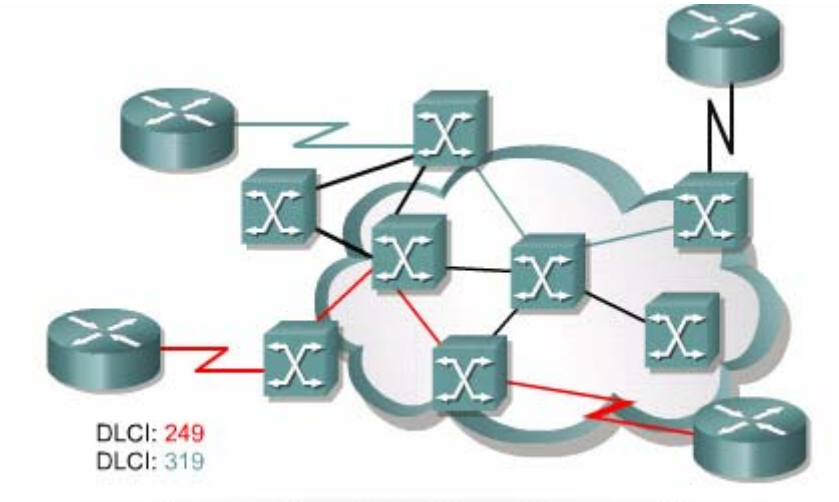
VC	Port	VC	Port
579	0	121	1

Frame Relay được thiết kế để hoạt động trên đường truyền số chất lượng cao, Frame Realy không có cơ chế khắc phục lỗi. Nừu thiết bị nào trên đường truyền phát hiện frame bị lỗi thì hủy bỏ frame đó mà không cần thông báo.

Mỗi router hay FRAD kết nối ảo vào mạng Frame Relay đều có thể có nhiều kết nối ảo đến nhiều điểm cuối khác nhau. Mỗi kết nối đầu cuối chỉ cần có một cổng vật lý và một kết nối vật lý, trên đó thiết lập được nhiều kết nối ảo đến nhiều điểm đích khác nhau. Do đó mạng Frame Relay giảm được nhiều chi phí lắp đặt vì không cần tạo mạng hình lưới với nhiều đường truyền vật lý. Hơn nữa chúng ta còn

tiết kiệm được tiền thuê bao vì dung lượng của đường truyền vật lý phụ htuộc vào băng thông trung bình của các VC thay vì phụ thuộc vào chu cầu tổng băng thông tối đa.

Các kết nối ảo VC trên cùng một đường truyền vật lý vẫn được phân biệt với nhau vì mỗi VC có một chỉ số DLCI riêng. Chỉ số DLCI (Dât Link Connection Identifier) được ghi trong mỗi frame dữ liệu truyền đi. Chỉ sốDLCI chỉ co ý nghĩa nội bộ, có nghĩa là no chỉ có duy nhất đối với kênh vật lý mà nó thuộc về mà thôi. Do đó thiết bị ở đầu bên kia có thể sử dụng một chỉ số khác để quy ước cho cùng một kết nối ảo VC.



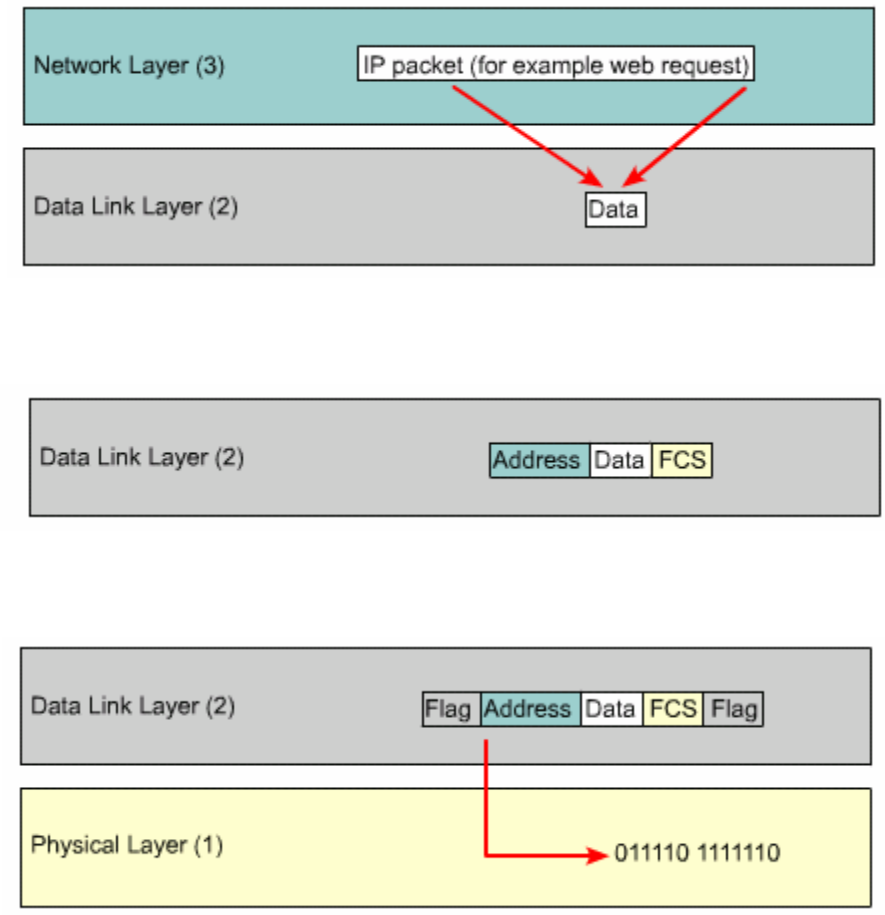
5.1.3 Đóng gói Frame Relay:

Đóng gói Frame Relay thực hiện theo phân lớp như sau:

- Nhận gói dữ liệu từ lớp Mạng, ví dụ gói IP hay IPX.
- Đóng gói thàng frame của Frame Relay.
- Chuyển frame xuống lớp Vật lý để truyền xuống đường truyền.

Lớp vật lý thườnglà EIA/TIA-232, 449 hay 530, V.35, X.21. Frame của Frame Relay sử dụng một phần định dạng của frame HDLC. Dođó cũng có phần cờ 01111110. Phần FCS (Frame Check Sequence) được sử dụng để kểim tra lỗi của frame.Giá trị FCSđược tính ra trước khi truyền frame đivà được ghi vào phần FCS của frame. Thiết bị nhận frame cũng tính lại giá trị FCS và so sánh với giá trị FCS ghi trong frame nhận được. Nừu hai giá trị giống nhau thi frame được tiếp tục xử

lý. Nừu hai giá trị khác nhau có nghĩ la frmae bị lỗi, lập tức frame bị hủy bỏ và không hề thông báo cho thiết bị nguồn. Viện kiểm soát lỗi được giao cho các lớp trên của mô hình OSI đảm trách.



5.1.4 Băng thông và điều khiển luồng trong Frame Relay:

Tốc độ đường truyền nối tiếp trong mạng Frame Relay chính là tốc độ truy cập hay tốc độ port. Tốc độ port thường nằm trong khoảng từ 64 kb/giây đến 4 Mb/giây. Một số nhà cung cấp dịch vụ còn cung cấp tốc độ lên đến 45 Mb/giây.

Tren một đường truyền vật lý hoạt động đồng thời nhiều kết nối ảo PVC, mỗi VC co một lượng băng thông riêng nhất định. Băng thông này chính là băng thông cam kết của nhà cung cấp dịch vụ, gọi la CIR (Commited Information Rate). Nhà cung cấp dịch vụ đồng ý chấp nhận lượng bít này trên một VC.

Mỗi CIR có giá trị nhỏ hơn tốc đọ port. Nhưng tổng các CIR trên mọt port lại lớn hơn tốc độ port, thường là lớn hơn khoảng 2 hay 3 lần,vì các kênh ảo hoạt

động với dung lượng khác nhau tại mỗi thới điểm và không đồng thời sử dụng tối đa băng thông của mình.

Khi truyền frame ,mỗi bít được phát đi với tốc độ port. Do đó nếu lượng bít trung bình trên VC đã bằng với CIR thì sẽ phải có khoảng thời gian nghỉ giữa hai frame.

Frame Relay switch cũng chấp nhận frame được gửi từ DTE với tốc độ cao hơn CIR. Như vậy mỗi VC có thể sử dụng băng thông theo nhu cầulên đến mức tối đa là tốc độ port. Một số nhà cung cấp có thể quy ước mức độ tối đa này thấp hơn tốc độ port. Mức chênh lệch giữa CIR và mức tối đa gọi là ERI (Ecs Information Rate).

Khoảng thời gian (chu kỳ) để tính tốc độ được gọi la Tc (Committed Time). Số lượng bit trong một chu kỳ được gọi la Bc (Committed Burst). Số lượng bit chênh lệch giữa Bc và mức tối đa (là tốc độ vật lý của đường truyền) được gọi la Be (Ecs Burst).

Mặc dù switch vẫn chấp nhận các frame được truyền với tốc độ vượt quá CIR,nhưng mỗi frame vượt tiêu chuẩn này được switch đánh dấu bằng cách đặt bit DE của frame (Discard Eligible) lên 1.

Switch co một đồng hồ đếm bit tương ứng với mỗi VC. Khi switch nhận frame vao, nếu frame này vượt quá số lượng Bc thì frame sẽ đượ đánh dấu bit DE. Frame nhận vào sẽ bị hủy bỏ khi số lượng bit vượt quá Bc + Be. Cuối mỗi chu kỳ Tc switch sẽ khởi động lại đồng hồ đếm bit.

Frame sau khi được nhận vào switch sẽ được xếp hàng đợi chuyển ra. Tuy nhiên nếu số lượng fame quá nhiều sẽ làm tràn hàng đợi, thời gian trễ sẽ tăng lên. Một số giao thức lớp trên có yêu cầu truyền lại khi không nhận được dữ liệu sau một thời gian nhất định. Nhưng do thời gian trễ quá lớn, yêu cầu truyền lại không thể thực hiện được. Trường hợp này sẽ làm tụp giảm thông lượng mạng nghiêm trọng

Để tránh sự cố này, Frame Relay switch có chính sách hủy bớt frame trong hàng đợi để giữ hàng đợi không quá dài. Những frame nào có bit DE sẽ được đặt lên hủy bỏ trước tiên.

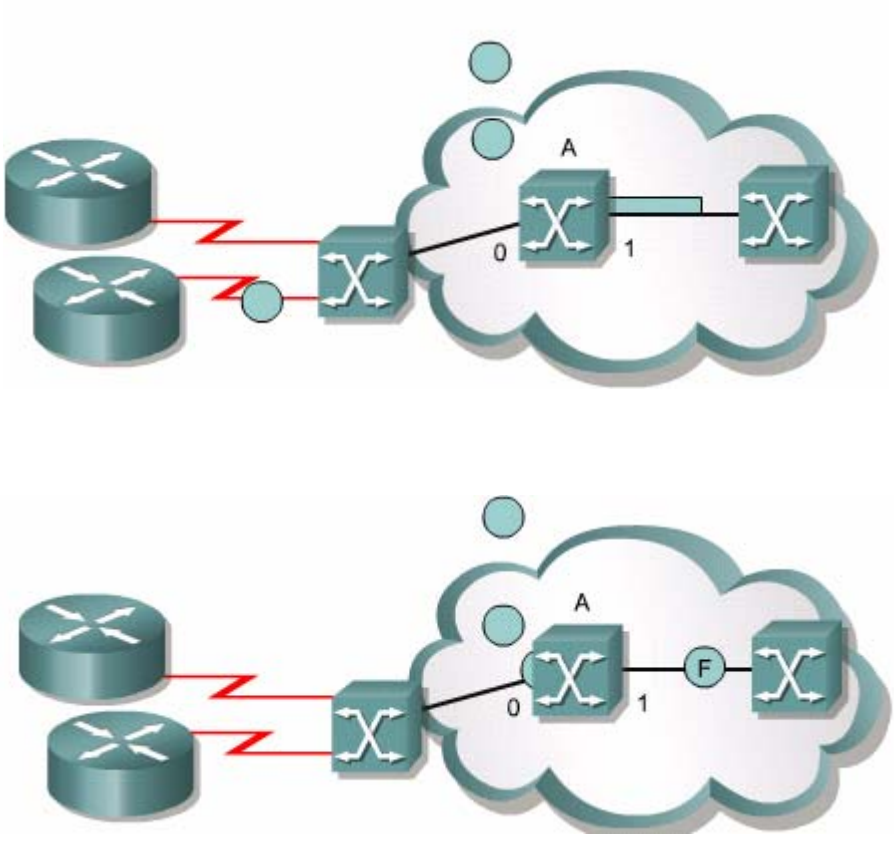
Khi switch nhận hàng đợi của nó đang tăng lên thì nó sẽ cố gắng tìm cách làm giảm dòng truyền frame từ DTE đến nó. Switch thực hiện đặt bit báo nghẽn

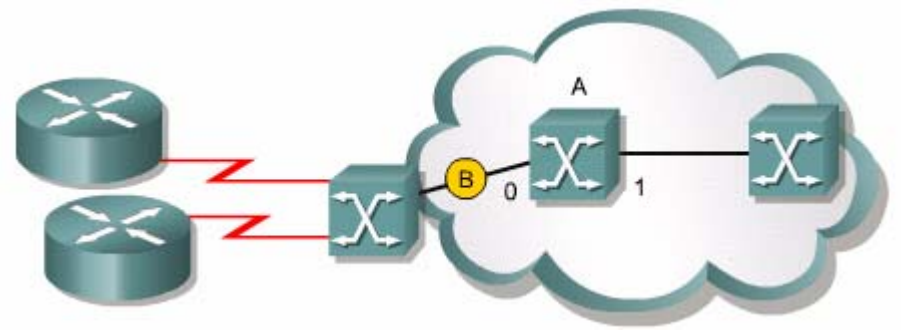
ECN (Explicit Congestion Notification) vào phần địa chỉcủa frame mà switch sẽ truyền lại cho DTE.

Bit FECN (Forward ECN) đượ cài đặt vào mỗi frame mà siwtch sẽ gửi ra đường truyền đang bị nghẽn để thông báo nghẽn cho các thiết bị kế tiếp. Bit BECN (Back ECN) được cài đặt trong mỗi frame mà switch sẽ gửi ngược lại cho thiết bị trước nó. DTE sẽ nhận được các frame có bit ECN được cài đặt trong đó và sau đo sẽ giảm dòng truyền frame lai cho đến khi không còn nghẽn mạch nữa.

Nếu nghẽn mạch xảy ra trên đường kết nối giữa các switch thì DTE bên dưới cũng có thể nhận được thông báo nghẽn mạch mặc dù nó không phải là thiết bị gây ra nghẽn mạch.

Các bit DEM, FECN, BECN là những bit nằm trong phần địa chỉ của frame LAPP.



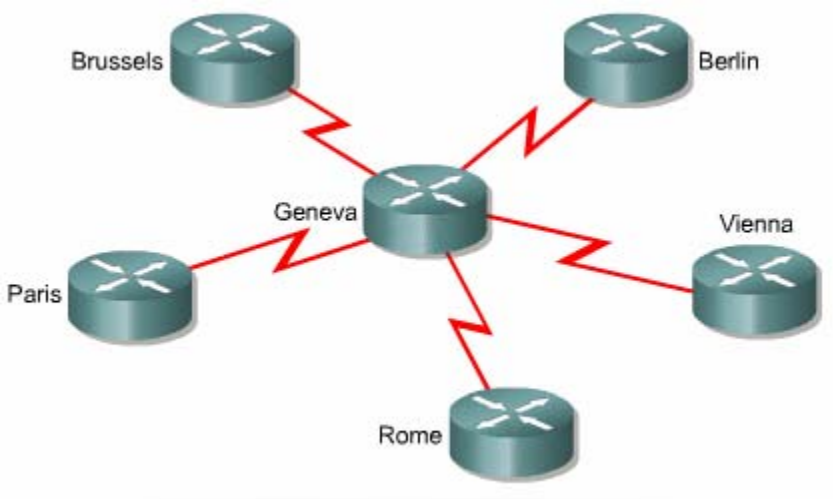


5.1.5 ánh xa đia chỉ và mô hình mang Frame Realy:

Khi chúng ta cần liên kết nhiều mạng với nhau thì chúng ta cần quan tâm đến mô hình kết nối giữa các mạng.

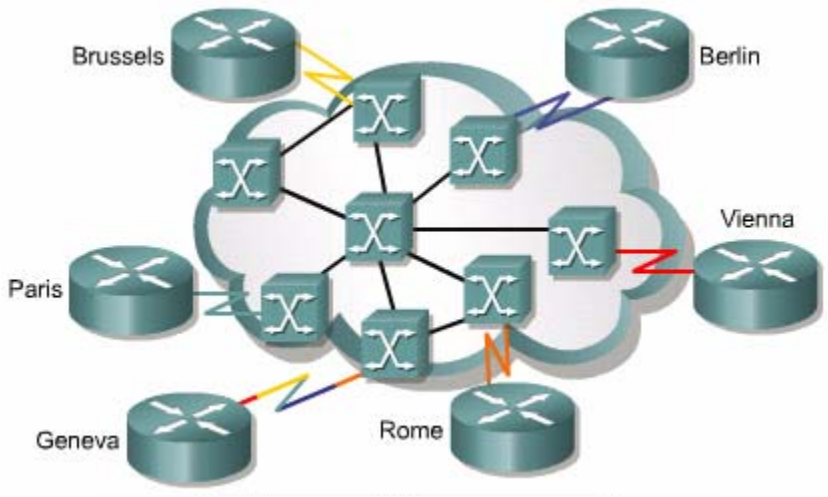
Nừu chúng ta chỉ cần kết nối hai mạng với nhau bằng kết nối điểm-nối-điểm thì lợi thế chi phí thấp của Frame Relay không đáng kể. Frame Relay sẽ rất có lợi về mặt chi phí nếu chúng ta liên kết nhiều mạng với nhau.

WAN thường được liên kết theo cấu trúc hình sao. Dịch vụ chính được đặt ơ một mạng trung tâm và mỗi mạng ở xa cần truy cập dịch vụ thì kết nối vào mạng trung tam. Với cách kết nối hình sao như vậy cho đường thue riêng, chi phí sẽ được giảm tối đa.



Nừu chúng ta kết nối mạng hình sao cho Frame Relay, mỗi mạng ở xa sẽ có một kết nối váo đám mây Frame Relay với một kết nối VC. Mạng trung tâm cũng

có một kết nối vào đám mây Frame Relay nhưng trên đó có nhiều VC kết nối đến các mạng xa. Tiền cước của mạng Frame Relay không tính theo khoảng cách kéo cáp nên vị trí địa lý của mạng trung tâm không nhất thiết phải nằm ở giữa.



Chúng ta nên chọn mô hình mạng hình lưới nếu các điểm truy cập dịch vụ bị phân tán về mặt địa lý và đường truy cập có yêu cầu cao về độ tin cậy. Với mạng lưới, mỗi mạng lưới phải có đường kết nối đến tất cả các mạng còn lại. Tuy nhiên, không giống như đường truyền thuê riêng, chúng ta có thể triển khai mạng hình lưới trong Frame Relay mà không cần phải tăng thêm nhiều VC trên một đường truyền vật lý là có thể nâng cấp mạng hình sao thành mạng hình lưới. Khi ghép nhiều kênh VC vào một đường truyền, chúng ta cungc tận dụng băng thông đường truyền tốt hơn so với việc chỉ cấu hình một VC.

Đối với hệ thống mạng quy mô lớn rất ít khi chúng ta sử dụng mạng hình lưới vì số lượng kết nối cần cho mạng hình lưới quá lớn, tăng theo tỉ lệ bình phương của số vị trí cần kết nối. Các thiết bị có giới hạn dưới 1000VC trên một kết nối. Nhưng trên thực tế thì giới hạn này còn thấp

hơn nữa. Do đó đối với hệ thống mạng lớn chúng ta nên sử dụng mạng hình lứi bán phần. Với mạng hình lưới bán phần chúng ta vẫn cần nhiều kết nối hơn so với mạng hình sao cũng không nhiều bằng bằng mạng hình lưới toàn phần. Việc kết nối mạng hình lưới bán phần như thế nào tùy thuộc vào nhu cầu của dòng chảy dữ liệu.

Trong bất kỳ cấu trúc Frame Relay nào, khi chung ta sử dụng một cổng để kết nối nhiều mạng khác nhau thì có thể gặp phải sự cố không đến được mạng đích. Sự cố này do đặc tính đa truy cập không quảng bá(NBMA- nonbroadcast

multiaccess) của Frame Relay gây ra. Như chúng ta đã học được ở giáo trinh trước, các giao thức định tuyến động sử dụng kỹ thuật Split horizon để tránh gây ra vòng lặp. Split horizon không cho phếp truyền ra một cổng những thông tin định tuyến vừa nhận vào từ cổng đó. Khi co nhiều PVC trên cùng một cổng vật lý thi Split horizon lại gây ra một rắc rối về mặt cập nhật định tuyến. Chúng ta sẽ bàn về vấn đề này kỹ hơn trong phần sau của trương. Frame Relay ở lớp Liên kết dữ liệu với địa chỉ lớp Mạng, ví dụ địa chỉ IP. Router luôn cần biết tương ứng với địa chỉ mạng đích là cổng nào. đối với đường kết nối trực tiếp thì đầu kia chỉ kết nối đến một router duy nhất. Nhưng franme đi từ DTE đền Frame Relay swich và sau đó được ánh xạ với một địa chỉ mạng của router đầu xa. Những thông tin này có thể ssược cấu hình bằng cấu hình bằng lệnh Map hoặc cấu hình tự động bằng cách dùng Inverse ARP.

5.1.6. Frame Relay LMI:

Frame Relay được thiết kế để truyền dữ liệu chuyển mạch gói với thời gian trễ tối thiểu. Bất kỳ yếu tố nào góp phần vào thời gian trễ đều được bỏ qua. Nhưng khi các hãng muốn trển khai Frame Relay như là một công nghệ độc lập chứ không còn là một thành phần của ISDN nữa thì họ quyết định rằng DTE cần được cung cấp thông tin động về trạng thái hoạt động của mạng. Cơ chế này không có trong thiết kế ban đầu của Frame Relay và LMI

(Local Mângemaent Interface) đã được thêm vào sau này để truyền thông tin về trạng thái hoạt động mạng.

Phần DLCI 10 bit cho phép xác định VC từ 0 đến 1023.Trong đó có dành riêng lại một số chỉ số làm giới hạn của VC giảm xuống.Các thông điệp LMI được trao đổi giữa DTE và DCE và sử dụng những chỉ số DLCI dành riêng này

Chỉ số VC	Loại VC
0	LMI (ÁNI, ITU)
1..15	Để dành cho việc sử dụng ở tương lai
992..1007	CLLM

1008..1022	Để dành cho việc sử dụng ở tương lai (ÁNI, ITU)
1019..1020	Multicasting (Cisco)
1023	LMI (Cisco)

LMI baogồm những thông tin sau:

- Cơ chế keepalive để kiểm tra một vòng VC còn hoạt động.
- Cơ chế multicast.
- Điều khiển luồng.
- Có DLCI nào được gán thành giá trị toàn cục hay không.
- Trạng thái VC.

Có nhiều loại LMI khác nhau và các loại này không tương thích với nhau. Do đó chúng ta cần cấu hình loại LMI tên router phù hợp với loại LMI mà nhà cung cấp dịch vụ đang sử dụng. Sau đay là 3 loại lMI mà Cisco router có hỗ trợ:

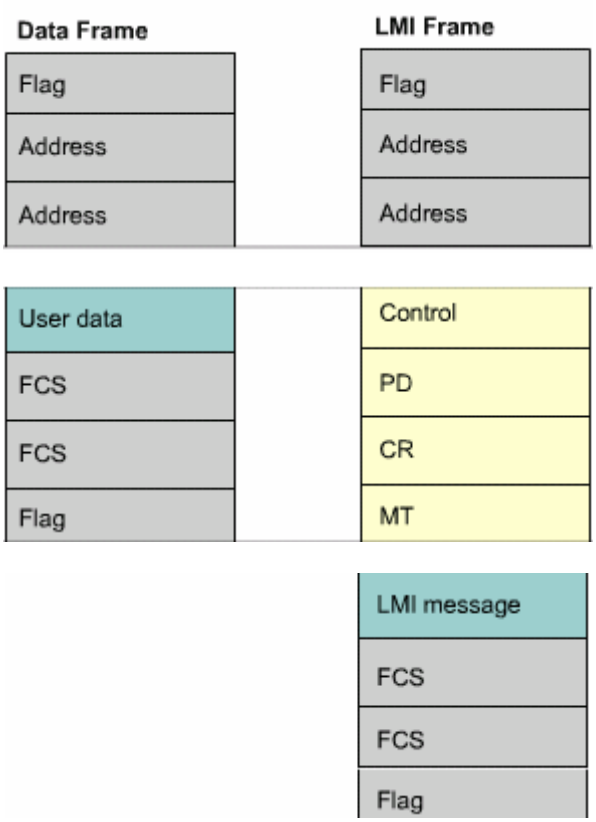
- Cisco - LMI gốc.
- Ansi — theo chuẩn ANSI T1.617 Phụ chương D.
- Q933a — theo chuẩn ITU Q933 phụ chương A.

Thông điệp LMI được lồng trong frame LAPF.Tong đó có thêm 4 phần mằn trong phần Header của frame để có thể tương thích với frame LAPD sử dụng trong ISDN, trong đó phần thứ 4 cho biết loại trông điệp LMI.

Theo sau phần Header là một hoặc nhiều thông tin khác nhau, bao gồm:

- 1 byte chứa chỉ số danh định của thông tin.
- Phần cho biết chiều dài của phần thông tin tương ứng.
- Một hoặc nhiều byte chứ thông tin thực sự về trạng thái của một DLCI.

Thông điệp trạng thái giúp kiểm tra kết nối logic và vật lý. Những thông tin này rất quan trọng trong môi trường định tuyến vì các giao thức định tuyến quyết định dựa trên những thông tin về trạng thái đường kết nối.



- Control: 0x30 (unnumbered info)
- Protocol Discriminator (PD): 0x09
- Call Reference (CR): 0
- Message Type (MT): 0x7D Status Enquiry
  0x75 Status Enquiry
  0x7B Status Update
- LMI Message: 0 or more Information Elements

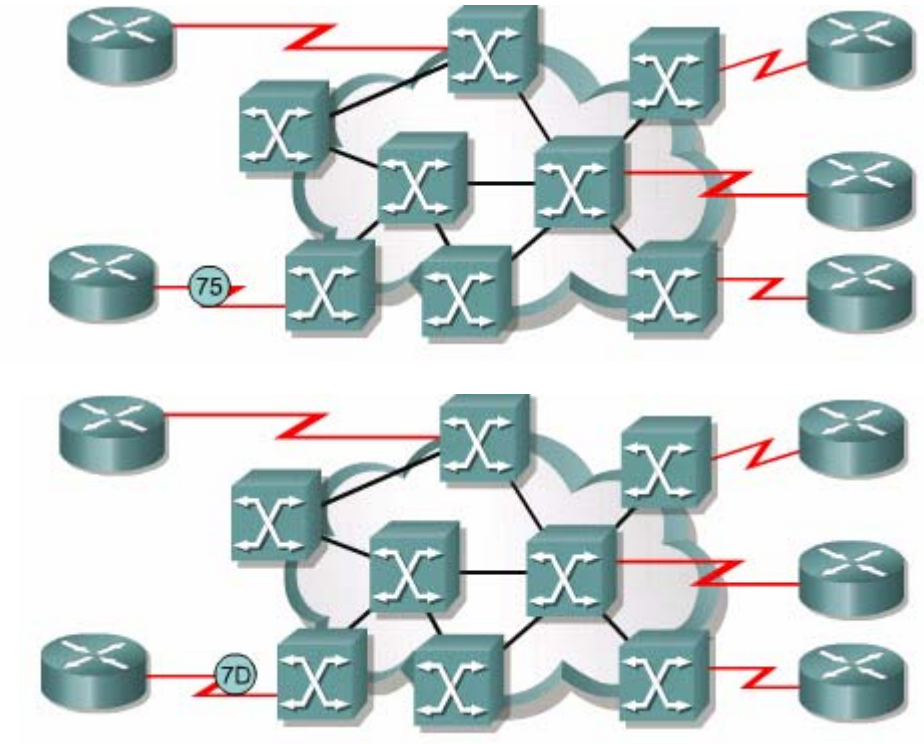
5.1.7 Hoạt động của Inerse ARP và LMI:

Thông điệp trạng thái LMI kết hợp với thông điệp Inverse ARP cho phép router liên kết được địa chỉ lớp mạng và địa chỉ lớp Liên kết dữ liệu.

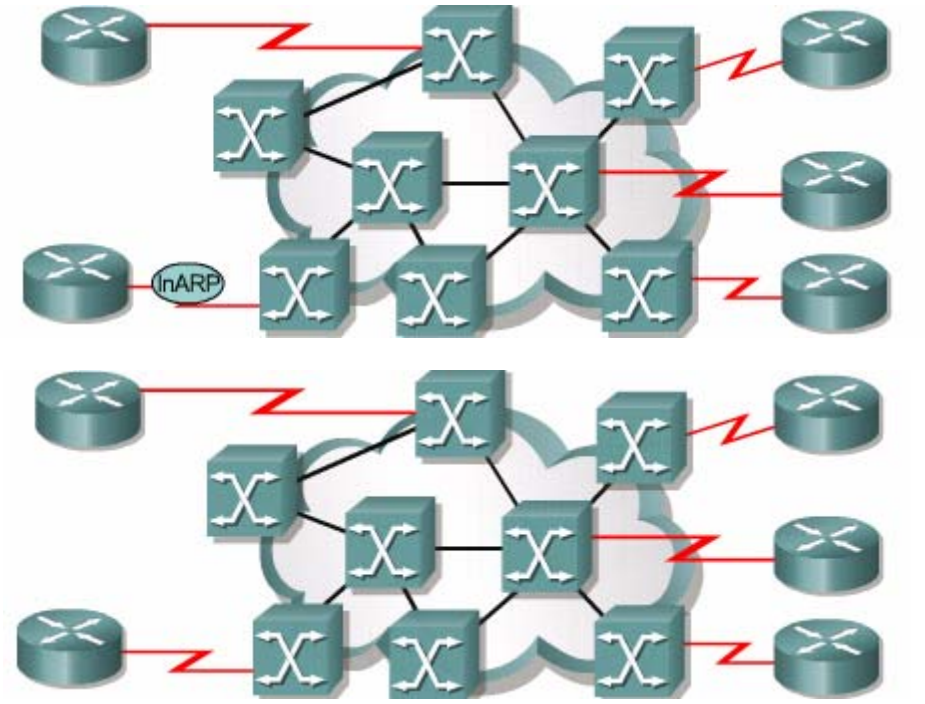
Khi router trong mạng Frame Relay bắt đầu khởi động, nó sẽ gửi các thông điệp LMI để hỏi về trạng thái của hệ thống mạng. Hệ thống mạng sẽ trả lời lại bằng thông điệp LMI,trong đó có các thông tin chi tiết về mọi VC được cấu hình trên một đường kết nối.

Theo chu kỳ router lặp lại việc hỏi thông tin trạng thái của mạng nhưng những lần sau này nò chỉ nhận được trả lời về những thay đổi trạng thái mới xảy ra. Sau một số lần nhất định như vậy mạng lại gửi một lần đầy đủ các thông tin về trạng thaí mạng.

Nêú router cần ánh xạ giữa VC và địa chỉ lớp mạng thì nó sẽ gửi thông tin điệp Inverse ARP ra mỗi VC. Thông điệp Inverse ARP trả lời sẽ cho phép router co thể ánh xạ giữa địa chỉ mạng va DLCI tương ứng. Nừu trong mạng có chạy nhiều giao thức lớp Mạng khác nhau thì thông điệp Inverse ARP được gửi đi nhiều lần tương ứng với mỗi giao thức lớp Mạng khác nhau.



DLCI	Status
101	Active
102	Active
103	Active
104	Active



5.2 Cấu hình Frame Relay:

5.2.1. Cấu hình Frame Relay cơ bản

Phần này sẽ giải thich cấu hình cơ bản của một Frame Relay PVC, Frame Relay đượoc cấu hình trên cổng serial. Giao thức đóng gói mặc định trên cổng này là HDLC. Để chuyên sang kiểu đóng gói Frame Relay chung ta dùng lệnh "encapsulation Frame - Relay {cisco/ietf}."

Cisco: sử dụng kiểu đóng gói độc quyền của cisco cho Frame Relay. Chúng ta sử dụng kiểu đóng gói này nếu thiết bị đầu bên kia cũng la một cisco router. Có nhiều thiết bị không phải của cisco cũng có hỗ trợ kiểu đóng gói này. cisco là trọn lựa mạc định của câu lệnh này, do đo bạn chỉ cần nhấp lệnh này "encapsulation Frame - Relay {cisco/ietf}."là đủ.

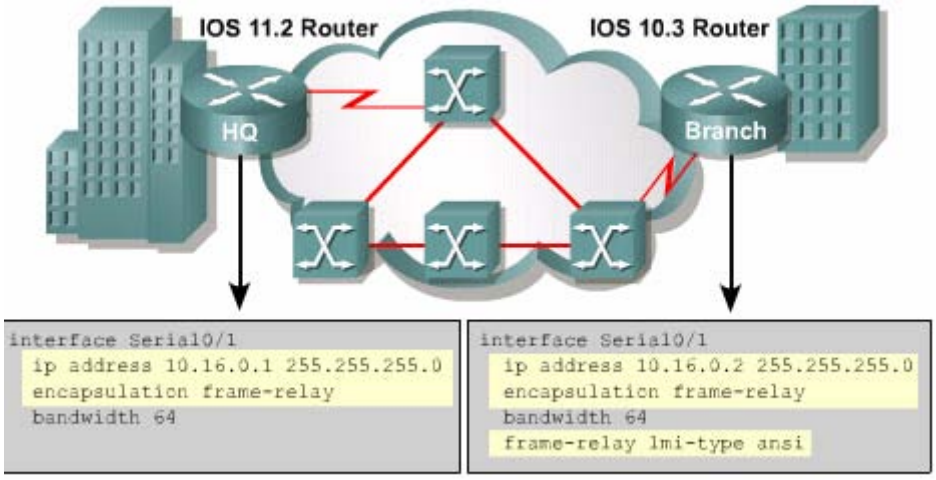
Ietf: kiểu đóng gói phù hợp với chuẩn RFC 1490 của IETF. Chúng ta nên chon kiểu đóng gói này nếu thiết bị ở đầu bên kia kết nối không phải la Cisco router.

Kiểu đóng gói độc quyền của Cisco cho Frame - Relay sử dụng 2 byte phần header, trong đó 2byte xác định chỉ số DLCI và 2byte xác định loại gói dữ kiệu.

Như đã học ở giáo trình trước: chúng ta dùng lệnh ip address để khai báo địa chỉ IP cho cổng Serial. Lệnh Bandwidth để cài đặt băng thông cho cổng Serial, băng thông này tính theo đơn vị (kb/giây). chúng ta sử dụng lệnh này để cài đặt băng thông cố định cho các giao thức định tuyến. Các giao thức định tuyến như IGRP, EIGRP và OFPS sẽ sử dụng giá trị băng thông trong câu lệnh này để tinh toan đường đi.

Kết nối LMI được thiết lập và cấu hình bởi lệnh Frame — Relay Lmi-type{ansi/cisco/q933a}. chúng ta chỉ sử dụng lệnh này nếu phiên bản Cisco IOS phiên bản 11.2 trở về sau, loại LMI mặc định là Cisco và được cài dặt trên cổng Serial. Chúng ta có thể xem thông tin về loại LMI bằng lệnh show interfaces.

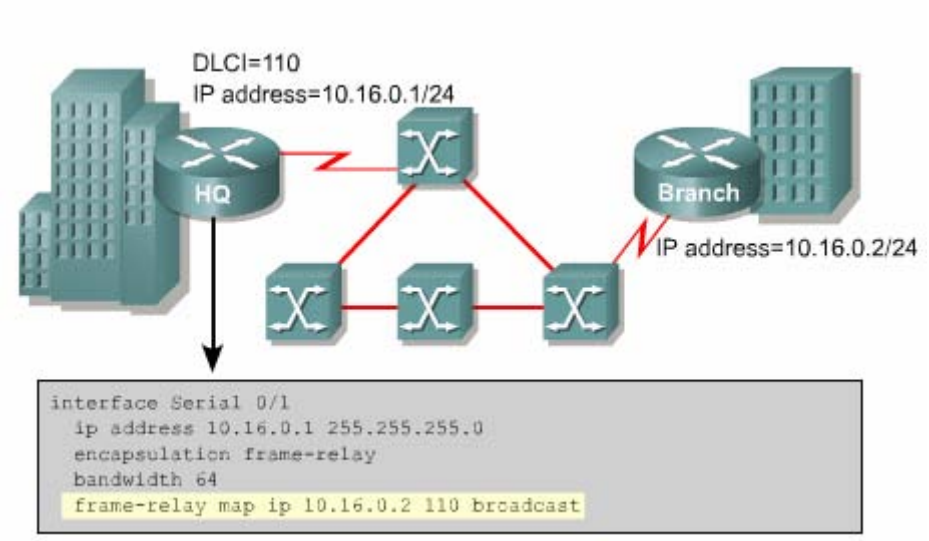
Các bước cấu hình trên không phụ thuộc vào giao thức lớp mạng nào đang chạy trên mạng.



5.2.2. Cấu hình sơ đồ ánh xạ cố đinh cho Frame Relay:

Mỗi chỉ số của DLCI nội bộ phải được ánh xạ cố định đến một địa chỉ lớp mạng của router đầu xa khi router đầu xa không có hỗ trợ Invêrse ARP. Tương tự, khi lưu lượng quảng bá và multicast trên PVC bị kiển sóat thì chúng ta cũng phải cấu hình sơ đò ánh xạ cố định cho Frame — Relay bằng lệnh: Frame — Relay map protocol — address dlci {broadcast}.

Broadcast: cho phép lưu lượng quảng bá vào multicast trên VC , cho phép sử dụng giao thức định tuyến động trên VC. Tham số này không bắt buộc phải cố khi khai báo lệnh.



5.2.3. Sự cố không đến được mạng đích do quá trình cập nhật thông tin định tuyến gây ra trong mạng đa truy cập không quảng bá NBMA (Non -broadcast multi - access).

Mặc định, mạng Frame — Relay là môi trường đa truy cập không quảng bá NBMA. Môi trương NBMA cũng được xem tương tự như các môi trường đa truy cập khác , ví dụ như Ethernet. Tất cả các router kết nối vào một Ethernet đều năm trong cùng mạng. Nhưng để giảm chi phí phần cứng , mạng NBMA lại được xây dựng thieo cấu trúc hình sao, do đo khả năng đa truy cập không bằng Enthernet.

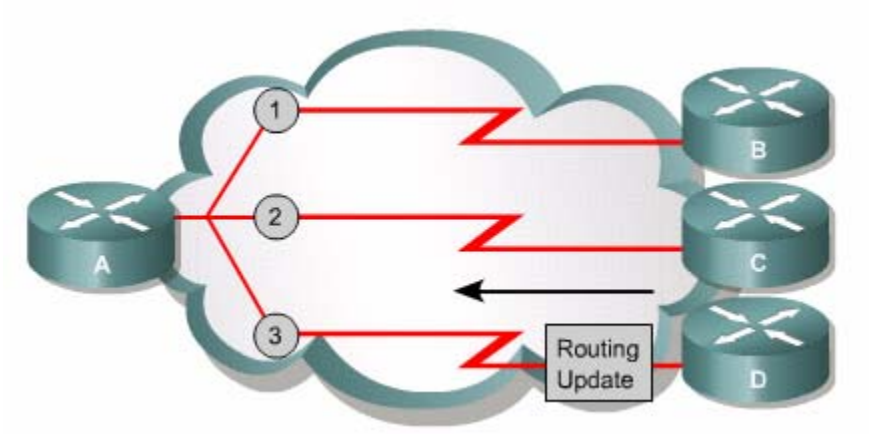
Cờu trúc Frame — Relay NBMA có thể gây ra 2 vấn đề sau:

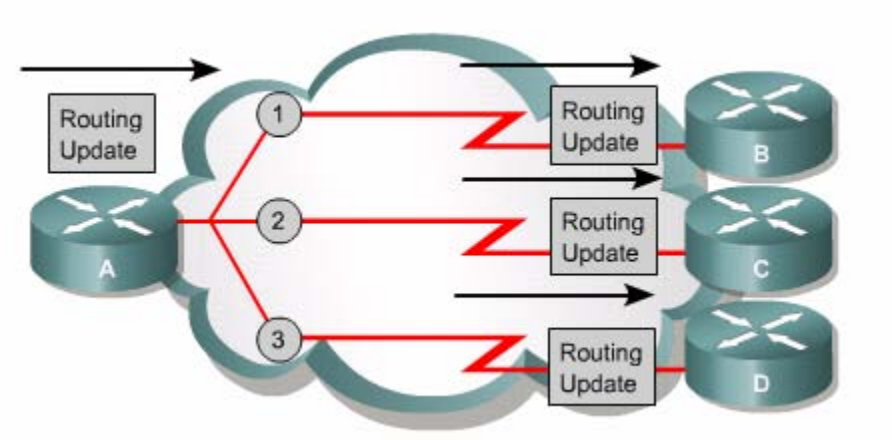
- Sự cố không đến được mạng đích do quá trình cập nhật thông tin định tuyến gây ra.
- Phải lập lại các mạng quảng bá trên mỗi PVC khi trên một cổng vật lý có nhiều PVC.

Các giao thức định tuyến động sử dụng kỹ thuật Split-horizon để ngăn chặn vòng lặp xảy ra. Khi đó những thông tin định tuyến vừa được nhận vào từ một cổng của router sẽ không được phep phát ngược ra cổng đó. Bây giờ chúng ta sét một ví dụ như hính 5.2.3a. Nừu router D gửi một thông tin quản bá đến cho router A, trong đó có chứa thông tin cập nhật định tuyến. Router A la ruoter trung tâm nên có nhiều kết nối PVC trên một cổng vật lý. Nhưng router A không thể phát ngược trở ra

những thông tin cập nhật mà nó vừa nhận được từ router D. kết quả là router B và C không nhận được những thông tin đó . như vậy router B,C không thể gửi gói dữ liệu đên các mạng router D. do đó router Bvà C không có chức năng Split-horizon thì các thông tin cập nhật định tuyến mới có thể phát nhược trở lại trên cổng mà chúng vừa nhận vào. Split-horizon sẽ khong gây ra rác rối nếu chúng ta chỉ có một PVC trên một cổng vật lý, đó chính là kết nối Frame Relay

Điểm- nối - điểm.





Một router có thể có nhiều kết nối PVC trên một cổng vật lý và mỗi PVC kết nối đến một router riêng. khi đó router phỉa lặp các gói dữ liệu quảng bá trên mỗi PVC , ví dụ như các gói cập nhật thông tin định tuyến để đảm bảo mỗi router đầu bên kia đều nhận được đầy đủ thông tin.

Nhưng việc lặp lại các thông tin quảng bá này lại chiếm nhiều băng thông đường truyền và làm cho các lưu lượng khác của người dùng bị chậm lại.

Như vạy chúng ta thấy rằng, để giải quyết sự cố Split-horizon gây ra thì tốt hơn là nên tắt Split-horizon đi. nhưng không phải giao thức lớp mạng nào cũng cho phép chung ta tắt chức năng Split-horizon và việc tắt chức năng Split-horizon cũng đồng nghĩa với khả năng xảy ra lặp vòng trong mạng xẽ cao hơn.

Còn một cách khác để giải quyết vấn đề Split-horizon là sử dụng cấu trúc lưới nối đủ. Nhưng cấu trúch này lại làm tăng chi phí và cần nhiều kết nối hơn.

Cuối cùng, giải pháp mà chung tôi đề nghị là giải pháp sử dụng Subinterface được trình bày trong phần kế tiếp.

5.2.4. Subinterface trong Frame Relay:

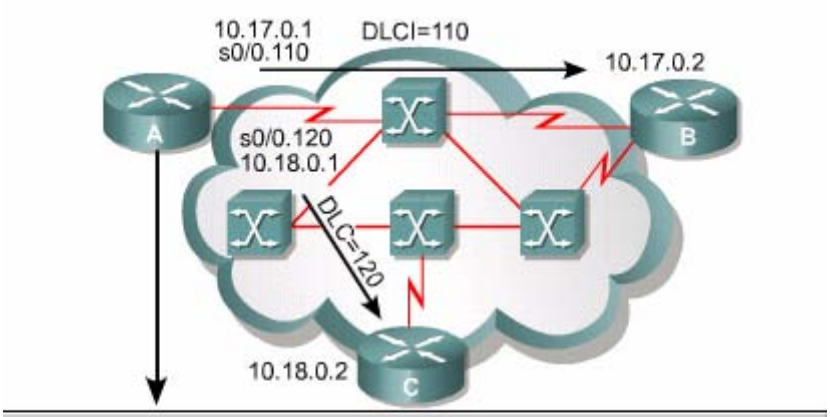
Theo phần trên thì khi một cổng vật lý có nhiều PVC kết nối đến các router đầu xa sẽ xảy ra sự cố Split-horizon.Trong môi trường định truyến Split-horizon, các thông tin cập nhập định tuyến được nhận vào từ cổng nào thì không được phát ngược ra cổng đó. Bây giờ chúng ta chia một cổng vật lý thành nhiều subinterface poin-to-point. Mỗi một subinterface poin-topint thiết lập một PVC đến một cổng vật lý hay một subinterface khác trên router đầu bên kia. Như vậy, mỗi cặp router điểm-nối-điểm này nằm trong cùng một subnet và mỗi cổng subinterface poin-to-point có một DLCI riêng. Mỗi một subinterface poin-topint hoạt động như một cổng riêng biệt, do đó Split-horizon khôngcòn là vấn đề rắc rối nữa. Dạng subinterface poin-topint được ứng dụng cho cấu trúc Frame Relay hình sao.

Cổng subinterface Frame Relay còn có thể cấu hình làm cổng đa điểm (Multipoint). Một subinterface multipoint thiết lập nhiều kết nối PVC đến nhiều router khác nhau. Tất cả các router kết nối dều nằm trong cùng một subnet. Do đó chúng ta tiết kiệm được nhiều địa chỉ mạng và điều này hết sức có ý nghĩa nếu trong trường hợp chúng ta không sử dụng VLSM (Variable Length Subnet Masking). Tuy nhiên, subinterface multipoint lại không giải quyết được vấn đề Split-horizon. Chúng ta ứng dụng subinterface multipoint cho mạng Frame Relay hình lưới nối đủ hoặc nối bán phần.

Lệnh **encapsulation frame-relay** được sử dụng để cấu hình cho cổng vật lý. Còn tất cả các thông tin cấu hình khác của cổng, ví dụ như địa chỉ lớp Mạng, DLCI, chúng ta sẽ cấu hình cho mỗi subinterface. Phần kế tiếp sẽ trình bầy cụ thể cấu hình subinterface cho Frame Relay.

5.2.5 Cấu hình subinterface cho Frame Relay:

Nhà cung cấp có trách nhiệm cấp số DLCI. Chỉ số DLCI thường nằm trong khoảng từ 16 đến 992 và có giá trị cục bộ.Số lượng tối đa của chỉ số DLCI còn phụ thuộc vào loại LMI đang sử được dụng. Chỉ số DLCI cũng có thể có giá trị toàn cầu nhưng chúng ta không bàn đến vấn đề này trong phạm vi của giáo trình này.




```
interface Serial0/0
  no ip address
  encapsulation frame-relay
  !
  interface Serial0/0.110 point-to-point
   ip address 10.17.0.1 255.255.255.0
   bandwidth 64
   frame-relay interface-dlci 110
  !
  interface Serial0/0.120 point-to-point
   ip address 10.18.0.1 255.255.255.0
   bandwidth 64
   frame-relay interface-dci 120
  !
```

Chúng ta xét ví dụ như hình 5.2.5. Router A có hai subinterface poin-to-point: cổng s0/0.120 kết nói đến router C. Mỗi subinterface nằm trong một subnet riêng. Sau đây là các bước thực hiện để cấu hình subinterface trên một cổng vật lý:

- Cấu hình đóng gói Frame Relay cho cổng vật lý bằng lệnh **encapsulation frame-relay.**
- Định nghĩa PVC bằng cách tạo subinterface.

Để tạo subinterface chúng ta sử dụng lệnh sau:

Router (config-if) #**interface**

Serial*number.subinterface-number* **[multipoint | piont-to-point]**

Thông thường chúng ta lấy chỉ số DLCI gán cho chỉ số của subinteface (subinteface-number) để dễ nhận biết khi kiểm tra cấu hình. Kông có chế độ mặc định cho subinteface,do đó chúng ta bắt buộc phải khai báo tham số **multipoint** hay **piont-to-point.**

Nừu subinteface được cấu hình poin-to-point,sau đó chúng ta phải cấu hình DLCI cho cổng đó để phân biệt với cổng vật lý. Đối với subinteface được cấu hình multipiont và có hỗ trợ Inverse ARP thì không cần khai báo DLCI và cấu hình sơ đồ ánh xạ địa chỉ — DLCI cố định.

5.2.6 Kiểm tra cấu hình Frame Relay:

Lệnh show interfaces sẽ cung cấp các thông tin về cấu hình đóng gói, trạng thái Lớp 1 và Lớp 2. Ngoài ra , lệnh này còn hiển thị các thông tin sau:

- Loại LMI.
- LMI DLCI.
- Loại Frame Relay DTE hay DCE.

Thông thường thì router được xem là thiết bị DTE. Tuy nhiên, chúng ta có thể sử dụng một Cisco router để cấu hình làm Frame Relay switch. Khi đó router này trở thàng thiết bị DCE.

Chúng ta sử dụng lệnh **show frame-relay lmi** để xem trạng thái của các hoạt động LMI. Ví dụ: lệnh này sẽ cho biết số lượng các gói LMI được trao đổi giữa router và Frame Relay switch.

```
Router#show interface s0/0
Serial0/0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 10.140.1.2/24
  MTU 150 bytes, BW 1544 Kbit, DLY 20000 usec, relay
  255/255, load 1/255
  Encapsulation FRAME-RELAY, loopback not set, keepalive
  set (10 sec)
  LMI enq sent 19, LMI stat recvd 20, LMI upd recvd 0,
  DTE LMI up
  LMI enq recvd 0, LMI stat sent 0, LMI upd sent 0
  LMI DLCI 1023 LMI type is CISCO frame relay DTE
  FR SVC disabled, LAPF state down
  Broadcast queue 0/64, broadcasts sent/dropped 8/0,
  interface broadcasts 5
  Last clearing of "show interface" counters never

  Queueing startagy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, o drops
  <Output omitted>
```

```
Router#show frame-relay lmi

LMI Statistics for interface Serial0/0 (Frame Relay DTE)
LMI TYPE = CISCO
  Invalid Unnumbered info 0 Invalid Prot Disc 0
  Invalid dummy Call Ref 0 Invalid Msg Type 0
  Invalid Status Message 0 Invalid Lock Shift 0
  Invalid Information ID 0 Invalid Report IE Len 0
  Invalid Report Request 0 Invalid Keep IE Len 0
  Num Status Enq. Sent 113100 Num Status msgs Rcvd
  113100
  Num Update Status Revd 0 Num Status Timeouts 0
```

Lệnh **show frame-relay pvc** [interface *interface*] [dlci] hiển thị trạng thái của mỗi PVC tương ứng đã được cấu hình và thông tin về các lưu lượng trên PVC đó. Một PVC có thể ở trạng thái hoạt động (active), không hoạt động (inactive) hay đã bị xóa (deleted). Bằng lệnh này chúng ta còn có thể xem được số lượng các gói BECN và FECN được nhận vào bởi router.

Lệnh **show frame-relay pvc** được sử dụng để xem trạng thái của tất cả các PVC đã được cấu hình trên router. Nừu chúgn ta khai báo thêm chỉ số của một

PVC thì lệnh sẽ hiển thị thông tin của một PVC đó. Trong ví dụ 5.2.6.c là kết quả hiển thị trạng thái của PVC 100.

```
Router#show frame-relay pvc 100

PVC Statistics for interface Serial0/0 (Frame Relay DTE)

DLCI - 100, DLCI USAGE - LOCAL, PVC STATUS - ACTIVE,
INTERFACE - Serial0/0

 input pkts 28      output pkts 10      in bytes 8398
 out bytes 1198     dropped pkts 0      in FECN pkts 0
 in BECN pkts 0     out FECN pkts 0     out BECN pkts 0
 in DE pkts 0       out DE pkts 0
 out bcast pkts 10 out bcast bytes 1198
 pvc create time 00:03:46, last time pvc status changed
 00:03:47
```

```
Router#show frame-relay map
Serial0/0 (up) : ip 10.140.1.1 dlci 100 (0x64,0x1840),
                 dynamic, broadcast, status defined, active
```

Chúng ta sử dụng lệnh **show frame-relay map** để xem sơ đồ ánh xạ hiện tại và thông itn về các kết nối. Ví dụ như hình 5.2.6.d là kết quả hiển thị của lệnh **show frame-relay map:**

- 10.140.1.1 là địa chỉ IP của router đầu xa. Địa chỉ này đượ học tự động thông qua quá trình Inverse ARP.
- 100 là giá trị của DLCI tính theo số thập phân.
- 0x64 là giá trị hẽ của DLCI, 0x64 = 100.
- 0x1840 là giá trị của DLCI được thể hiện trên đường truyền do các bit được đặt trong địa chỉ của frame (Frame Relay).

- Broadcast/multicast được cho phép trên PVC.
- Trạng thái PVC là đang hoạt động.

Để xóa sơ đồ ánh xạ Frame Relay được tạo ra tự động do quá trình ARP,chúng ta sử dụng lệnh **clear frame-relay-inarp**. Ngay sau đó chung s ta dùng lại lệnh **show frame-relay** thì sẽ không thấy gì nữa. Sau một khoảng thời gian nhất định, quá trình ARP sẽ cập nhập lại bảng này một cách tự động.

5.2.7 Xác định sự cố trong cấu hình Frame Relay:

```
Router#debug frame-relay lmi
Frame Relay LMI debugging is on
Displaying all Frame Relay LMI data
Router#
1w2d: Serial0/0(out):StENq,myseq 140, yourseen 139, DTE up
1w2d: datagramstart = 0xE008SEC, datagramsize = 13
1w2d: FR encap - 0xFCF10309
1w2d: 00 75 01 01 03 02 8C 8B
1w2d:
1w2d: Serial0/0 (in): Status, myseq 140
1w2d: RT IE 1, length 1, type 1
1w2d: KA IE 3, length 2, yourseq 140, myseq 140
1w2d: Serial0/0(out):STEng,myseq 141, yourseen 140, DTE up
1w2d: datagremstart = 0xE008EC,, datagresize = 13
1w2d: FR encap = 0xFCF10309
1w2d: 00 75 01 01 03 02 8D 8C
1w2d:
1w2d: Serial0/0 (in): Status, myseq 142
1w2d: RT IE 1, length 1 type 0
1w2d: KA IE 3, length 2 yourseq 142, myseq 142
1w2d: PVC IE 0x7, length 0x6, dlci 100, status 0x2, bw0
```

Chúng ta sử dụng lệnh **debug frame-relay lmi** để xác định router nào va Frame Relay switch nào gửi nhận các gói tin một cách bình thường. “Out” là những thông điệp LMI được gửi đi bởi router, “in” là những thông điệp LMI nhận được từ Frame Relay switch. Thông điệp trạng thái LMI đầy đủ có “type 0”, “type 1” là một phiên giao dịch trao đổi LMI. Sau đây là ý nghĩa của các thông số trạng thái:

- 0x0: đã nhận biết nhưng không hoạt động. Điều này có nghĩa là switch đã được cấu hình DLCI nhưng vì lý do nào đó không sử dụng được DLCI này. Nguyên nhân có thể là do đầu bên kia của PVC chưa hoạt động .
- 0x2: đã nhận biết là đang hoạt động. Điều này có nghĩa là Frame Relay switch đã có DLCI và mọi cái hoạt động tốt.
- 0x4: đã xóa. Điều này có nghĩa là hiện tại Frame Relay switch không còn DLCI này nữa nhưng trước đó DLCI này đã được cấu hình cho

switch. Nguyên nhân có thể do số DLCI được lưu trên router hoặc nhà cung cấp đã xóa PVC tương ứng trong mạng Frame Relay.

TỔNG KẾT

Sau đây là những điểm chính trong chương trình mà các bạn cần nắm được:

- Phạm vi hoạt động và mục đích của Frame Relay.
- Công nghệ Frame Relay.
- Cấu trúc điểm-nối-điểm và điểm-nối-đa điểm.
- Cấu trúc mạng Frame Relay.
- Cách cấu hình Frame Relay PVC.
- Các cấu hình sơ đồ ánh xạ địa chỉ cho Frame Relay.
- Những vấn đề về định truyến trong mạng đa truy cập không quảng bá.
- Tại sao phải cần subinterface và cấu hình chúng như thế nào.
- Kiểm tra và xác định sự cố kết nối Frame Relay.

CHƯƠNG 6: GIỚI THIỆU VỀ QUẢN TRỊ MẠNG

GIỚI THIỆU:

PC được thiết kế là một máy tính để bàn độc lập. Phần hệ điều hành lúc đó chỉ cho phéptại một thời điểm một use truy cập sử dụng tài nguyên hệ thống. Khi mạng máy tính trở nên phổ biến thì các công ty phần mềm bắt đầu phát triển hệ điều hành mạng, gọi tắt là NOS (Network Operating System). NOS được thiết kếđể cung cấp khả năngbảo mật tập tin, phân quyền use và chia sẻ tài nguyên hệ thống cho nhiều use. Sự phát triển nhanh chóng của Internet đã đòi hỏi các nhà thiết kế phải phát triển NOS ngày nay theo các công nghệ của Internet, ví dụ như World Wide Web (WWW).

Kết nối mạng trở thành nhu cầu thiết yếu với máy tính để bàn. Ranh giới giữa hệ điều hành Desktop và NOS đã trở nên rất mờ nhạt. Ngày nay, hầu hết các hệ điều hành thông dụng như Microsoft Windows 2000 vá Linux đều có thể tìm thấy trên server trên mạng cấu hình mạnh và trên cả desktop của user.

Hiểu biết về các hệ điều hành khác nhau sẽ giúp chúng ta chon lựa đúng hệ điều hành để cung cấp đầy đủ các dịch vụ cần thiết. Trong chương này sẽ giới thiệu về UNIX, Linux, Mac OS X và các hệ điều hành Windows.

Việc quản trị mạng LAN và WAN hiệu quả là một điều kiện then chốt trong việc duy trì một môi trường hoạt động tốt trong thế giới mạng. Càng nhiều dịch vụ đáp ứng cho càng nhiều người dùng, hiệu suất mạng càng cao. Người quản trị mạng thông qua việc theo dõi thường trực, phải phát hiện và sử lý ngay các sự cố trước khi những sự cố có tác động đến người sử dụng.

Có rất nhiều công cụ và giao thức khác nhau để thực hiện việc theo dõi hoạt động mạng. Thành thạo về các công cụ này là rất quan trọng để có thể quản trị mạng một cách hiệu quả.

Sau khi hoàn tất chương chình này, các bạn có thể thực hiện những việc sau:

- Xác định những nhiệm vụ được thực hiện bởi máy trạm.
- Xác định những chức năng của server.
- Mô tả vai trò client/server.
- Mô tả sự khác nhau giữa NOS và hệ điều hành desktop.

- Liệt kê các hệ điều hành Windows và các đặc điểm của chúng.
- Liệt kê các hệ điều hành khác và các đặc điểm của chúng.
- Xác định các công cụ quản trị mạng.
- Mô tả OSI và mô hình quản trị mạng.
- Mô tả SNMP (Simple Network Management Protocol) và CMIP (Common Management Information Protocol).
- Mô tả cách thu nhập thông tin và lưu lại sự cố các phần mềm quản trị mạng.

6.1. Máy trạm và Server:

6.1.1. Máy trạm:

Máy trạm client được sử dụng để chạy các trình ứng dụng và kết nói đến server. Server là máy tính chạy hệ điều hành mạng NOS, là nơi lưu dữ liệu chia sẻ giữa các máy tính. Máy trạm sử dụng phần mềm đặc biệt để thực hiện những nhiệm vụ sau:

- Tiếp nhận dữ liệu của user và lệnh của chương trình ừng dụng.
- Xác định xem lệnh nhận được là cho hệ điều hành nội bộ hay là cho NOS.
- Chuyển lệnh đến hệ điều hành nội bộ hoặc ra card mạng (NIC) để truyền vào mạng.
- Thực hiện việc truyền dữ liệu giữa mạng và phần mềm ứng dụng đang chạy trên máy trạm

Một số hệ điều hành Windows có thể cài đặt được cả trên máy trạm và server. Windows NT/2000/XP có cung cấp khả năng Server mạng. Windớ 9x và ME chỉ có thể sử dụng cho máy trạm.

UNIX và Linux cũng thường được sử dụng trên các máy desktop cấu hình mạnh. Những máy trạm này thường được sử dụng cho các ứng dụng về khoa học kỹ thuật đòi hỏi cấu hình máy tính mạnh. Sau đây là những phần mềm đặc biệt thường được chạy trên các máy trạm UNIX:

- Computer-aiđe desing (CAD).
- Phần mềm thiết kế mạch điện tử.
- Phần mềm phân tích dữ liệu thời tiết.
- Phần mềm thiết kế hình ảnh động.
- Phần mềm quản lý thiết bị viễn thông.

Hầu hết các hệ điều hành desktop hiện nay đều có khả năng mạng và hỗ trợ nhiều user truy cập. Chính vì vậy,việc phân loại máy tính và hệ điều hành không chỉ dựa trên các loại trình ứng dụng chạy trên máy mà còn dựa tren vai trò của máy tính trong mạng, là máy trạm hay server. Các trình ứng dụng thường chạy trên máy trạm thông thường gồm có:trình sử lý văn bản, bảng tính, quản lý chi tiêu, Những trình ứng dụng chạy trên máy trạm công nghệ cao bao gồm: thiết kế đồ họa, quản lý thiết bị và những phần mềm đã được liệt kê ở trên.

Máy trạm không ổ đĩa là một loại máy đặc biệt để thiết kế chạy trong mạng. Máy tính này không có ổ đĩa nhưng vẫn có màn hình, bàn phím, RAM, ROM và NIC. Phần mềm thiết lập kết nối mạng được tải từ chip ROM trên NIC. Loại máy trạm này không có ổ đĩa nên phải chép mọi dữ liệu từ máy trạm lên server và ngược lại, tải mọi dữ liệu từ trên server xuống. Do đó, máy trạm không ổ đĩa không thể phát virut vào mạng và đồng thời cũng không thể lưu dữ liệu từ mạng vào ổ đĩa. Chính vì vậy, máy trạm không ổ an toàn hơn so với máy trạm thông thường. Do đó loại máy trạm không ổ đĩa thường được sử dụng trong những mạng có yêu cầu bảo vệ cao

Laptop cũng là một máy trạm trong mạng LAN và được kết nối mạng thông qua PCMCIA card.

6.1.2. Server:

Trong môi trường mạng, nhiều client cùng truy cập và chia sẻ tài nguyên trên một hay nhiều server. Máy client được trang bị bộ nhớ, ổ đĩa và các thiết bị ngoại vi như bàn phím, màn hình. Còn server phaỉ được trang bị để có thể hỗ trợ cho nhiều user, nhiều tác vụ của nhiều client cùng lúc trên server.

Nhiều công cụ quản lý mạng được thiết kế trong NOS để hỗ trợ cho nhiều user cùng lúc truy cập vào hệ thống. NOS còn được cài đặt trên server và các client cùng chia sẻ những server này. Server thườngdược trang bị ổ đĩa tốc độ cao và dung lượng lớn, bộ nhớ RAM lớn, NIC tốcđộ cao và trong nhiều trường hợp còn được trng bị nhiều CPU. Các server được cấu hình bộ giao thức TCP/IP và cung cấp một hoặc nhiều dịch vụ TCP/IP.

Server cần có dung lượng bộ nhớ lớn hơn nhiều so với máy trạm vì server phải thực hiện nhiều tác vụ cùng một lúc. Server cũng cần dung lượng ổ đĩa lớn để lưu các file chi sẻ và sử dụng ổ đĩa làm bộ nhớ ngoài hỗ trợ cho RAM. Trên mainboard của server cũng cần nhiều slot hơn để có thể gắn nhiều card mạng và kết nối nhiều thiết bị chia sẻ như máy in□

Một đặc điểm nữa của hệ thống server là năng lực sử lý. Nguyên thủy ban đầu server chỉ có một CPU để thực hiện các tác vụ và tiến trình trên máy tính. Để hoạt động hiệu quả hơn và đáp ứng nhanh hơn các yêu cầucủa client, server đòi hỏi phải có CPU mạnh hơn để thực hiện nhiều tác vụ cùng lúc. Trong một số trường hợp một CPU tốc độ cao cũng chưa đáp ứng đủ thì hệ thống cần trng bị thêm CPU. Hệ thống nhiều CPU có khả năng chia các tác vụ cho nhiều CPU khác nhau. Nhờ đó lượng công việc mà server có thể xử lý trong cùng một khoảng thời gian tăng lên rất nhiều.

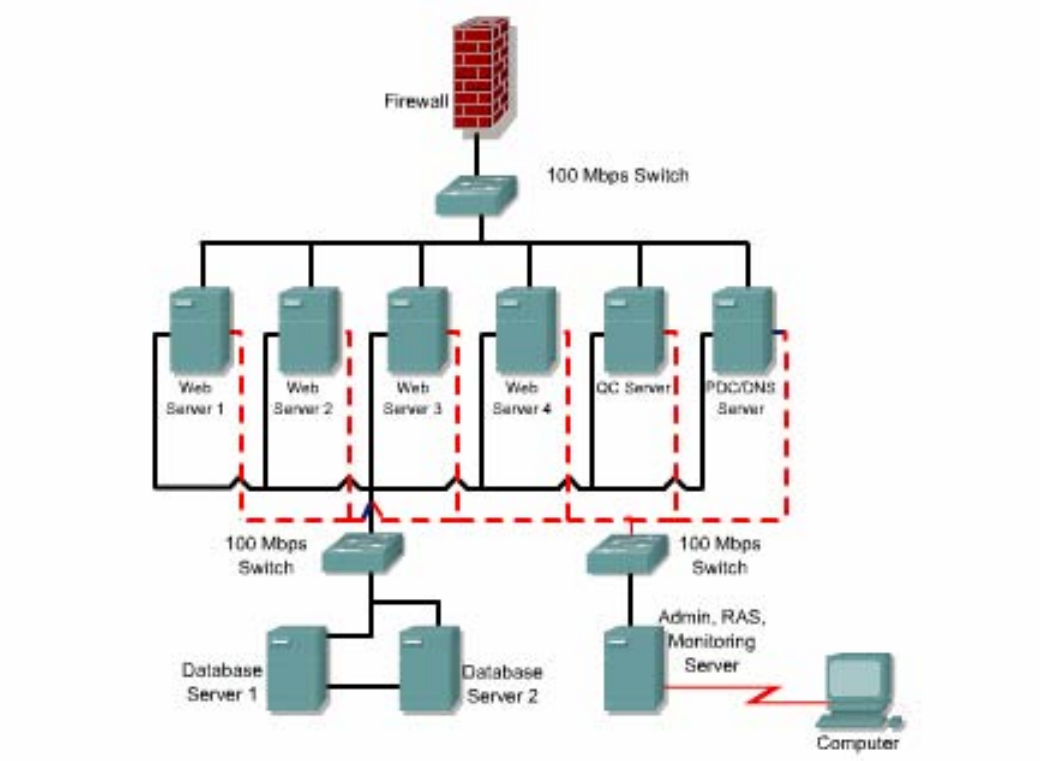
Serverlaf trung tâm tài nguyên và cũng là trung tâm hoạt động của client nên server phải hoạt động hiệu quả và bền vững. Hiệu qủa lớn ở đây có nghĩa là server phải hoạt động hiệu quả với áp lực công việc lớn và có khả năng khôi phục lỗi ở một hay nhiều thành phần của server mà không cần phải tắt toàn bộ hệ thống. Để đáp ứng nhu cầu này, server phải có các phần cứng dự phòng để hoạt động thay thế khi một thành phần nào đó bị hư. Việc sử dụng hệ thống dự phòng giup server vẫn hoạt động liên tục khi sự cố xảy ra và trong khoảng thời gian chờ sửa chữa thành phần bị hư hỏng.

Một số dịch vụ thường được chạy trên server là dịch vụ web HTTP, FTP, DNS, các dịch vụ về email như SMTP, POP3, IMAP, dịch vụ chia sẻ thông file như NFS của Sun Microsystem, SMB của Microsoft, dịch vụ chia sẻ máy in, dịch vụ DHCP để cugn cấpđịa chỉ IP động cho máy trạm.

Ngoài ra, server còn được cài đặt làm fierwall cho hệ thống mạng bằng cách sử dụng proxy hoặc NAT để che giấu địa chỉ mạng riêng bên trong.

Mỗi server chỉ có thể phục vụ cho một lượng client nhất định. Do đó chúng ta có thể triển khai nhiều server để tăng hiệu quả hoạt động. Thông thường người ta phân chia các dịch vụ cho mỗi server, ví dụ một server chịu trách nhiệm về email, một server chịu trách nhiệm về chia sẻ file và một server khác chịu trách nhiệm về FPT.

Việc tập chugn nguồn tài nguyên và các dịch vụ trên server giúpcho truy cập, quản lý và dự phòng dữ liệu tốt hơn. Mỗi client được cung cấp một t6ài khoản với user name/pasword và sẽ xác minh trước khi truy được phép truy cập vào server.

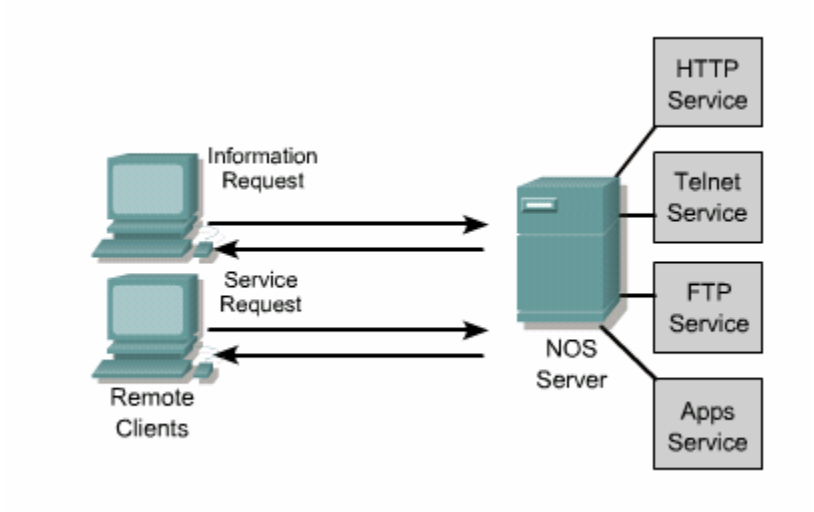


6.1.3. Mối quan hệ client server:

Mô hình client server phân chia mọt tiến trình sử lý lên nhiều maý tính khác nhau. Việc phân chia một tiến trình sử lý cho phép truy cập hệ thống từ xa để chia sẻ thông tin và tài nguyên mạng. Trong môi trường client server client và server cùng chia sẻ, hay nói cách khác là phân chia nhau một tiến trình sử lý.

Một phiên kết nối FTP là một ví dụ về mối quan hệ client server. FTP là một phương pháp để truyền file từ máy tính này sang máy tính khác. Để client có thể tải file từ server hoặc cho phép chép file lên server, trên server phải có chạy dịch vụ

FTP. Khi đó, client yêu cầu truyền file, server cung cấp dịch vụ tương ứng để truyền hoặc nhận file.



Internet cũng là một ví dụ điển hình về quan hệ chia sẻ một tiến trình sử lý giữa client server. Client hay điểm cuối giao tiếp với user là nơi trình duyệt internet explorer hay netscape trình bày dữ liệu với user tình duyệt web gửi yêu cầu đến web server. Server chả lời và trinh duyệt web nhận được dữ liệu HTTP từ server và trình bày trang web đò cho user.

Một ví dụ nữa cho mốt quan hệ slient server là server cung ứng dịch vụ về cơ sở dử liệu và client trong LAN. Trên client, chạy một ứng dụng được viết bằng C hay Java. Trên server, chạy ORACLA hay một phần mềm quản lý dữ liệu. Trong trường hợp này, client thực hiện việc định dạng và trình bày các tác vụ đối với dữ liệu cho user, còn server cung cấp nơi lưu dữ liệu và dịch vụ tìm dữ liệu.

Một máy tính đôi khi phaỉ truy vấn một dữ liệu cần thiết nào đó trong một cơ sở dữ liệu rất lờn. Với mô hình client server, client chỉ cần gửi yêu cầu tìm dữ liệu cho server. Sau đó server có thể xử lý với hơn 100000 hồ sơ dữ liệu mới tìm ra dữ liệu thỏa mãn yêu cầu của client.

Như vậy, việc lưu trữ một lượng lớn dữ liệu và việc sử lý tìm kiếm trên lượng dữ liệu đó đều được thực hiện tại server. Clinet chỉ cần phát đi một yêu cầu nhỏ và chờ nhận kết quả mong muốn. Do đó lượng thông tin chao đổi được truyền đi qua mạng sẽ nhỏ đi ít tốn băng thông hơn.

Việc phân chia sử lý một tiến trình giữa client và server như trên đem lại nhiều ưu điểm, nhưng cũng có nhược điểm về mặt chi phí. Việc tập chung tài nguyên trên server giúp cho việc truy cập đơng giản, kiểm soát tập chung và khả năng bảo vệ tốt hơn nhưng server lại trở thành điểm nhạy cảm duy nhất. Nừu server bị sự cố, không hoạt động được thì kể như toàn bộ hệ thống cũng không hoạt động được nữa. Ngoài ra, để bảo trì và quản trị server còn đòi hỏi phải có những phần cứng dự phòng, những phần mềm đặc biệt và những chuyên gia trình độ cao trong lĩnh vực này. Tất cả những yếu tố đó làm tăng thêm chi phí vận hành mạng.

6.1.4. Giới thiệu về hệ điều hành mạng, gọi tắt là NOS (Networld Operating System):

Hệ điều hành là một phần mềm làm nền cho tất cả các ứng dụng và dịch vụ chạy trên một máy tính. Tương tự, NOS cho phép nhiều thiết bị thông tin liên lạc với nhau để chia sẻ tài nguyên qua mạng. NOS thường được chạy trên các server Unix, Microsoft Windows NT, Windows 2000.

Các chức năng thông thường của một hệ điều hành trên máy trạm gồm điều khiển phần cứng, chạy chương trình và cung cấpgiao diện tiếp với user. Nhiều user có thể chia sẻ cùng một máy tính nhưng không thể sử dụng một máy tính cùng lúc. Trong khi đó, NOS phân chia chức năng trên nhiều máy tính khác nhau, cho phép chia sẻ dữ liệu bởi nhiều user cùng lúc.

Một client trong môi trường NOS có thể cho phép người sử ụng truy cập đến nguồn tài nguyên trên máy khác như chính nguồn tài nguyên nội bộ nằm trên máy vậy.

Một NOS server nhiều người dùng có khả nănh hỗ trợ nhiều user cùng lúc. Nhà quản trị mạng tạo tài khoản cho mỗi user, cho phép server kiểm tra và xác minh user mỗi khi truy cập, đồng thời tùy theo mỗi tài khoản mà user có thể truy cập những tài nguyên nào được phép.

NOS server là một hệ thống đa nhiệm, có khả năng thực hiện nhiều nhiệm vụ cùng lúc. Phần mềm NOS phân phối thời gian xử lý, bộ nhớ và các thành phần khác củu hệ thống cho các tác vụ khác nhau, cho phép nhiều tác vụ cùng chia sẻ tài nguyên hệ thống. Mỗi user trong hệ thống nhiều người dùng được hỗ trợ bởi một tiến trình riêng trong server. Mỗi tiến trình này được tạo ra tự động bên trong server mỗi khi user kết nối vào hệ thống và được xóa đi khi user ngắt kết nối.

Khi chọn lựa NOS chúng ta cần quan tâm đến các đặc điểm sau: khả năng hoạt động, công cụ quản lý và theo dõi, khả năng bảo mật, khả năng mở rộng, độ bền vững và khả năng khắc phục lỗi.

Khả năng hoạt động: NOS phải thực hiện đọc và ghi các file dược truyền qua mạng giữa client và server. Server phải có khả năng hoạt động tốt với áp lực cao khi có nhiều client cùng gửi yêu cầu cùng một lúc. Yêu cầu hoạt động tốt dưới áp lực cao là một tiêu chuẩn hàng đầu cho một NOS.

Khả năng quản lý và theo dõi: Giao diện quản lý của NOS cung cấp công cụ để theo dõi, quản lý client và ổ đĩa. Giao diện quản lý của NOS còn cung cấp công cụ để cài đặt và cấu hình dịch vụ mới. Ngoài ra, server còn đòi hỏi phải được thường xuyên theo dõi và điều chỉnh.

Khả năng bảo mật: NOS phải bảo vệ nguồn tài nguyên chia sẻ. Việc bảo mật bao gồm xác minh user, mã hóa để bảo vệ thông tin khi truyền đi giữa client và server.

Khả năng mở rộng: Là khả năng phát triển mạng mà không làm giảm hiệu quả hoạt động của NOS . NOS phải có khả năng chấp nhận thêm user và server mới.

Độ bền vững và khả năng khắc phục lỗi: Độ bền được xác định thông qua khả năng cung cấp dịch vụ khi co sự cố xảy ra. Chúng ta nên sử dụng ổ đĩa dự phòng và chia tải cho nhiều server để tăng độ bền vững cho NOS.

Novell	UNIX	Windows	Linux
Netware	HP-UX	NT	Red Hat
IntraNetWare	Sun Solaris	Server 2000	Caldera
GroupWise	BSD	.NET Server	SuSE
	SCO	Server 2003	Debian
	AIX		Slackware

6.1.5. Microsoft NT, 2000 và .NET:

Kể từ khi phiên bản Windows 1.0 được phát hành tháng 11năm 1985 đến nay, Microsoft đã phát hành nhiều phiên bản hệ điều hành Windows khác nhau với nhiều cải cách và thay đổi để hỗ trợ cho nhiều mục đích khác nhau.

Windows NT 4.0 được thiết kế để cung cấp một môi trường hoạt động ổn định hơn và có Windows NT 4.0 cho desktop (NT 4.0 Workstation) và cho server (NT 4.0 Server). Ưu điểmcủa Windows NT 4.0 là DOS và các chương trình Windows cũ có chạy trong môi trường giả lập. Lỗi chương trình được cô lập và không cần phải khởi động mại máy.

Windows NT cung cấp cấu trúc miền để kiểm soát user và client truy cập vào tài nguyên server. Mỗi miền NT phải có một primary domain controller lưu cơ sở dữ liệu quản lý tài khoản (SAM — Security Accounts Management Database) và có một hoặc nhiều backup domain controller, trên đó lưu bản copy read-only của SAM. Khi user muốn truy cập vào hệ thống, thông tin tài khoản được gửi đến SAM. Nừu thông tin tài khoản này có lưu trong SAM thì user sẽ được xác minh vào miền NT và truy cập được vào tài nguyên hệ thống.

Kế thừa Windows NT, Windows 2000 được phát triển cho cả Desktop và server, Windows 2000 có kỹ thuật Plug-and — play, nghĩa là các thiết bị mới được cài đặt vào hệ thống mà không cần khởi động lại. Windows2000 còn có hệ thống mã hóa File để bảo mật dữ liệu trên đĩa cứng.

Windows2000 đặt các đối tượng như User, tài nguyên vào một đơn vị như là Organizational units (Ous). Việc xác minh quản trị trên mỗi OU được ủy thác cho một User hoặc một nhóm User đặc điểm này cho phếp quản lý chi tiết hơn so với Windows NT 4.0.

Windows2000 Prossional không được thiết kế để làm một NOS hoàn chỉnh. Nó không cung cấp domain controller, DNS Server, DHCP Server hay bất kỳ dich vụ nào khác như windows2000 Server.

Mục đích chính của windows2000 Prossional là tham gia vào domain với tư cách là một hệ điều hành phía client. Các loại phần cứng có thể cài trên hệ thống cũng bị giới hạn windows2000 Prossional cũng có thể cung cấp một vài khả năng Server cho mạng nhỏ hoặc mạng ngang hàng, ví dụ như File server, FPT server, web server, print server nhưng chỉ tối đa 10 kết nối cùng lúc. windows2000 Server bổ sung thêm nhiều chức năng server cho windows2000 Prossional. windows2000 Server có thể hoạt động như một File server, nhóm user và tài nguyên mạng.

windows2000 Server có thẻ sử dụng cho mạng có kichs thước vừa và nhỏ. Nó cung cấp kết nối tương thích với hệ thống Novell Netware, UNIX và Apple. Nó có thể được cấu hình làm communication server để cung cấp dịch vụ quay số cho các

server ở xa. windows2000 Advance Server hỗ trợ thêm nhiều phần cứng và phần mềm khác cho các mạng lớn và cực lớn.

Microsoft cũng đã phát triển windows.NET Server cung cấp khả năng bảo mật cũng như độ tin cậy cao để chạy các Wed và các FPT sites cực lớn, cạnh tranh với linux, UNIX và novels's One NET. Windows.NET Server cung cấp dịch vụ XML Wed cho các công ty, tổ chức có mức độ lưu lượng web vừa và cao.

6.1.6. UNIX, Sun, HP và LINUX:

6.1.6.1. Nguồn gốc của UNIX:

UNIX là tên của một nhóm các hệ điều hành có nguồn gốc từ năm 1969 ở Bell Labs. Ngay từ ban đầu UNIX đã được thiết kế để hỗ trợ đa người dùng và đa tác dụng. UNIX là hệ điều hành đầu tiên có hỗ trợ các giao thức mạng Internet. lịch sử phát triển có hơn 35 năm của UNIX là một quá trình phức tạp, trong đó có rất nhiều công ty và tổ chức đóng góp vào sự phát triển của nó.

Đầu tiên, UNIX được viết bằng hợp ngữ (assembly language) và UNIX chỉ chạy được trên một loại máy tính đặc biệt. Vào năm 1971, Dennis Ritchie cho ra đời ngôn ngữ lập trình C. Năm 1973, Ritchie cùng với một thành viên của Bell Lasb là nhà lập trình Fen Thompson viết lại chương trình UNIX vời ngôn ngữ C. C là một ngôn ngữ lập trình bậc cao, do đó UNIX đã co thể chuyển sang chạy trên các loại máy tính khác. Quyết định phát triển hệ điều hành mới này là chìa khóa thành công của UNIX. Trong suốt thập niên 70, UNIX được phát triển bởi các nhà lập trình ở Bell Labs và một số trường đại học như University of California ở Berkeley.

Khi UNIX lần đầu tiên trở thành một thương hiệu trên thị trường trong thập niên 80, UNIX chỉ được sử dụng trên các server mạng loại mạnh chứ không sử dụng trên máy tính để bàn. Ngày nay, UNIX đã có nhiều phiên bản khác nhau như:

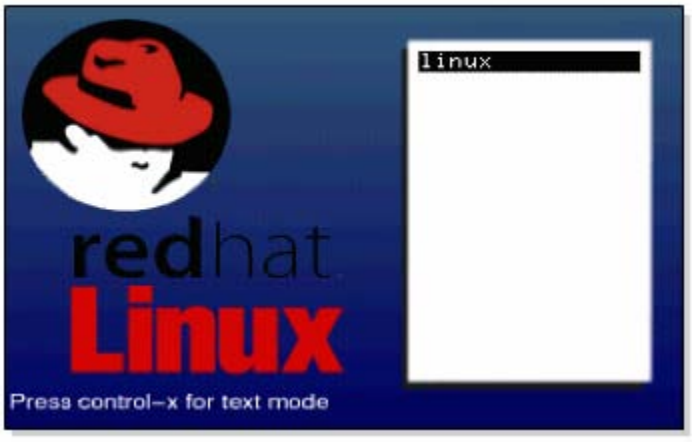
- Hewlett Packard UNIX (HP-UX).
- Berkeley Software Design, Inc. (BSD UNIX), có các sản phẩm như FreeBSD.
- Sânt Cruz Operation (SCO) UNIX.
- Sun Solaris.
- IBM UNIX (AIX).

UNIX tiếp tục khẳng định vị trí của nó là một hệ điều hành đáng tin cậy, an toàn cho các ứng dụng quan trọng, then chốt của một doanh nghiệp hay tổ chức. UNIX cũng thích hợp với TCP/IP vì chúng cần cho LAN và WAN.

Môi trường hệ điều hành Sun Microsystem Solaris là cốt lõi của nó, hệ điều hành SunOS là một phiên bản 64 bit, linh hoạt và hiệu suất hoạt động cao của UNIX. Solaris có thể chạy trên nhiều loại máy tính khác nhau, từ máy tính cá nhân Intel cho đến các máy tính cực mạnh. Hiện nay Solaris là phiên bản được sử dụng rộng rãi nhất của UNIX trong các hệ thống mạng lớn và các Internet website. Sun còn là nhà phát triển công nghệ Java "Write Once, Run Anywhere".

Nếu như Microsoft Windows được sử dụng phổ biến trong LAN thi UNIX được chạy rất nhiều trên Internet. UNIX thường gắn kiền với những phần cứng đắt tiền, không thân thiện với người sử dụng. Tuy nhiên trong những phát triển gần đây, kể cả Linux, người ta đang cố gắng thay đổi hình ảnh này.

6.1.6.2. Nguồn gốc của Linux:



Vào năm 1991, một sinh viên người Phần Lan tên là Linus Torvalds bắt tay nghiên cứu hệ điều hành cho máy tính Intel 80386. Torvalds đã không bằng lòng với trạng thái hoạt động của các hệ điều hành desktop, ví dụ như DOS và sự tốn kém bởi chi phí bản quyền của UNIX. Torvalds đã phát triển hệ điều hành hoạt động giống UNIX nhưng sử dụng mã phần mềm mở hoàn toàn miễn phí cho mọi người sử dụng.

Việc làm của Torvalds đã dẫn đến một hiệu ứng cộng tác toàn cầu, cùng phát triển Linux làm một hệ điều hành mã nguồn mở, có hình thức và cách sử dụng tương tự như UNIX. Vào cuối thập niên 90, Linux đã trở thanh kẻ có thể thay thế cho UNIX trên server và cho Windows trên desktop.

Các phiên bản của Linux hiện nay có thể chạy trên hầu hết các bộ xử lý 32 bit, bao gồm Intel 80386, Motorola 68000, Alpha và PowerPC.

Cũng như UNIX Linux cũng có nhiều phiên bản khác nhau. Một số phiên bản có thể tải miễn phí từ web và một số được bán. Sau đây là một số phiên bản thông dụng nhất của Linux:

- Red Hat Linux — phân phối bởi Red Hat Software.
- OpenLinux - phân phối bởi Caldera.
- Corel Linux.
- Slackware.
- Debian GNU/Linux.
- SúE Linux.

Linux là một trong những hệ điều hành mạnh nhất và đáng tin cậy nhất trên thế giới hiện nay. Chính vì vậy Linux cũng chỉ dành cho những người dùng chuyên nghiệp được sử dụng nhiều cho các server mạnh và ít được triển khai làm hệ điều hành desktop. Mặc dù Linux cũng có giao diện đồ họa thân thiện với người dùng nhưng người dùng không chuyên nghiệp vẫn cảm thấy sử dụng Linux khó hơn so với Mac OS hay Windows. Hiện nay một số công ty như Red Hat, SuSE, Corel và Caldera cũng đang cố gắng làm cho Linux cũng phổ biến như một hệ điều hành cho desktop.

Khi triển khai Linux trên máy tính để bàn, chúng ta cần quan tâm đến khả năng hỗ trợ các trình ứng dụng của Linux. Có một số chương trình ứng dụng chỉ tương ứng với Windows. Tuy nhiên một số hãng như WABI và WINE chuyên cung cấp phần mềm mô phỏng Windows đã giúp cho nhiều ứng dụng Windows có thể chạy trên Linux. Ngoài ra, một số công ty như Corel cũng đang làm phiên bản Linux phù hợp với hệ thống của họ cùng với các phần mềm thông dụng khác.

6.1.6.3.nối mạng với linux:

Hiện nay trong Linux đã có các thành phần về mạng, cho phép kết nối LAN và thiết lập kết nối quay số ra Internet TCP/IP được tích hợp vào nhân của Linux chứ không triển khai thành một hệ thống con riêng biệt.

Sau đây là một số ưu điểm của Linux khi được sử dụng trên desktop:

- Nó thực sự là hệ điều hành 32 bit
- Nó hỗ trợ đa tác vụ và bộ nhớ ảo
- Mã nguồn mở nên bất kỳ ai cũng có thể vận dụng và phát triển

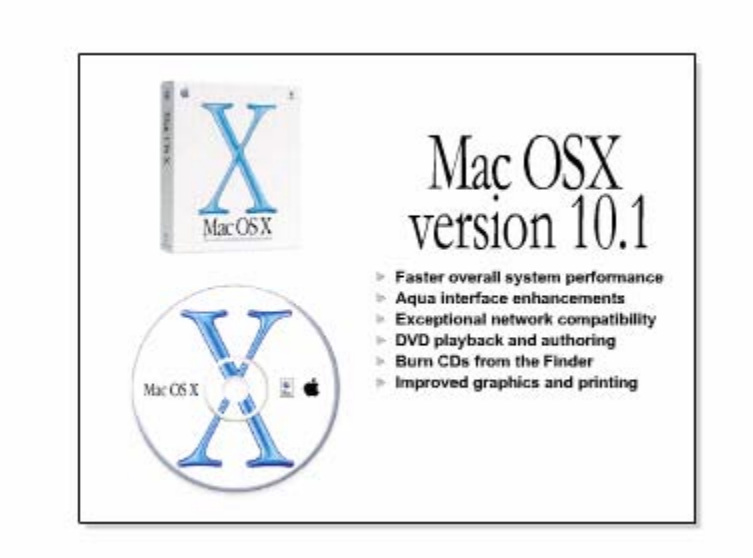
6.1.7 Apple:

Máy tính apple macintosh được thiết kế cho mạng ngang hàng hay một nhóm máy tính nhỏ. Cổng nối mạng cũng được bao gồm luôn trong phần cứng của máy tính, các thnàh phần mạng được xây dựng trong hệ điều hành macintosh. Máy tính macintosh cũng có thể sử dụng bộ chuyển đổi ethrnet hay token ring.

Máy tính macintosh hay gọi tắt là Mac, được sử dụng phổ biến trong các học viện và các bộ phận đồ họa. Mac có thể kết nối với một máy tính khác trong nhóm và có thể truy cập vào file server appleshare. Mac cũng có thể kết nối với các PC trong LAN và các server Microsft, NetWare, UNIX.

Mas OSX(10)

Hệ điều hành Macintosh, Mac OSX, đôi khi còn được gọi là Apple system 10.



Giao diện đồ hạo Aqua của Mac OS X tập hợp những đặc điểm của Microsoft Windows XP và Linux X-Windosw. Mac OS X đươc thiết kế để cung cấp các chức năng cho một máy tính gia đình, ví dụ như chình duyệt Internet, biên tập hình và Video, Game, đồng thời cũng cung cấp những công cụ mạnh, cấu hình chuyên nghiệp mà một chuyên gia IT cần có trong hệ nđiều hành.

Mac OS X tương thích hoàn toàn với các phiên bản cũ của Mac. Mac OS X còn cung cấp nhiều chức năng mới cho phép kết nối với Apple talk và Windows. Hệ điều hành xương sống của Mac OS X được gọi là Darwin. Darwwin là một hệ thống mạnh, dựa trên cơ sở của Unix, hoạt đọng ổn định và hiệu suất cao. Mac OS X cũng hỗ trợ bộ nhớ ảo, quản lý bộ nhớ bậc cao, thực hiên da tác vụ và sử lý đồng bộ. Tất cả những ưu điểm này làm cho Mac OS X cũng là một đối thủ cạnh tranh với các hệ điều hành khác.

6.1.8. Khái niệm về các dịch vụ trên Server:

NOS được thiết kế để cung cấp các hoạt động mạnh cho client. Các dịch vụ mạng bao gồm WWW, chia sẻ tập tin, Mail, quản lý từ xa, in từ xa □□.quản lý từ xa là một dịch vụ mạnh , cho phép người quản trị mạng có thể cấu hình hệ thống mạng từ xa. Mỗi hoạt động mạng trên các hệ điều hành khác nhau có chức năng giống nhau nhưng cách hoạt động sẽ khác nhau.

Tùy theo từng NOS mà một số các hoạt động chủ yếu sẽ được kích hoạt mặc định trong quá trình cài đặt NOS. hầu hết các hoạt dộng mạng thông dụng đều dựa trên bộ giao thức TCP/IP. Nhưng TCP/IP là bộ giao thức mở và nổi tiếng lên các

dịch vụ dựa trên TCP/IP cũng đứng trướca các nguy cơ bị tấn công. tán công DOS (Denian of service), virut, Worm đã buộc người thiết kế NOS quan tâm nhiều hơn đến việc khởi động tự động một dịch vụ mạng.

Những phiên bản thông dụng ngần đây của NOS, ví dụ như Windows và Red Hat Linux, đã giới hạn số dịch vụ mạng được kích hoạt mặc định do đó, khi sử dụng NOS, chúng ta phải khởi động các dịch vụ mạng bằng tay .

Khi một urer muốn in trong mạng có dịch vụ in chia sẻ, yêu cầu in được gửi đến hàng đợi của máy in và máy in phục vụ các yêu cầu này theo thứ tự "đến trước, in trước". Do đó thời gian chờ in có thể sẽ lâu, tùy theo số lượng cần in đang nằn ttrong hàng đợi. Với dịch vụ in qua mạng, người quản trị hệ thống có thể quản lý số lượng lớn công việc công việc lớn in ấn qua mạng, bao gồm cài đặt độ ưu tiên, thời gian chờ và xóa những yêu cầu in đang trong hàng chờ.

Chia sẻ tập in

Chia sẻ tập in là một dịch vụ mạng quan trọng. Hiện nay có rất nhiều giao thức và ứng dụng cho chia sẻ tập tin. Trong phạm vi mạng nhỏ huặc mạng gia đình, tập tin được chia sẻ bằng Windows file sharing hay giao thức NFS khi đó người sử dụng thậm chí cũng không nhận thấy sự khác biệt của tập tin đang nằm trên đãi cứng hay trên server. Windows file sharing và NFS cho phép người sử dụng dễ dàng di chuyển, tạo mới hay xóa tệp tin trong thư mục hay trên máy ở xa.

FTP

Rất nhiều lơi sử dụng FTP để tạo tệp tin có thể truy cập từ xa, điều chỉnh và phát hành ra cộng đồng. dịch vụ FTP kết hợp với dịch vụ WEB được sử dụng rất dộng dãi. ví dụ: một User đọc thông tin về một phần mềm mới trên trang Web và tải phần mềm đó về bằng FTP. Các công ty nhỏ có thể dùng một Server cung cáp cả hai dịch vụ FTP và HTTP, còn cán công ty lớn có thể dành riêng một Server cho FTP.

FTP client phải truy nhập vào FTP Server và chúng ta có thể cấu hình FTP Server cho phép truy nhập vô danh. Khi User truy nhập váo Server dưới dạng vô danh, User không bắt buộc phải có tài sản trong hệ thống. Giao thức FTP còn cho phép User chép tập tin nên Server thay đổi tên và xáo tệp tin. Do đó người quản trị hệ thống cần cẩn thận khi cấu hình quyền truy cập.

FTP là một giao thức hạot động theo phiên truy cập. Client phải mở phiên giao tiếp ở lớp ứng dụng với Server, thực hiện xác minh và sau đó tải huặc chép tệp tin nên Server. Nếu phiên kết nối không hoạt động trong một khoảng thời gian nhất định thì Server sẽ ngắt kết nối đó. Thời gian chờ cho mỗi phiên kết nối tùy thuộc từng phần mềm khác nhau.

Dịch vụ Web

Wornd wide web là dịch vụ mạng phổ biến nhất hiện nay. ệtong vòng không đầy một thập niên Wornd wide web đã chở thành mạng toàn cầu cho thông tin, buôn bán, giáo dục và giải trí. Hàng tỷ các công ty tổ chức và cá nhân đặt trang Web của mình trên Internet Web site là một tập hợp các trang Web với nhau.

Wornd wide web dựa trên các mô hình client/ server. Client thiết lập phiên bản kết nối TCB với Web server. Khi kết nối đã được thiết lập song, client có thể yêu cầu nhận dữ liệu từ server HTTP. Thực hiện các giao thức truyền dưc liệu giữa client và server. Phần mềm Web/client là các trình duyệt Web ví dụ Netscape, Internet explorer.

Trang Web được trên Server có chạy phần mềm dịch vụ Web. Hai phần mềm Web server thông dụng nhất là ernet explorer.

Trang Web được trên Server có chạy phần mềm dịch vụ Web. Hai phần mềm Web server thông dụng nhất là Microsoft Internet information Services (IIS) và Apache Web Server. Microsoft (IIS) chạy trên Windows Apache Web Server chạy trên UNIX và Linnux.

DNS

Giao thức DNS dich trên phần mềm Internet, ví dụ như www.cisco.com, thành đại chỉ IP. Giao thức DNS cho phép client gửi yêu cầu đến DNS server để thực hiện dịch tên miền sang đại chỉ IP. Sau đó chương trình ứng dụng có thể sử dụng địa chỉ IP này để gửi dữ liệu. Nếu không có dịch vụ này có lẽ Internet đã không thể phát triển như ngày nay.

DHCP

Mục đích của DHCP là cho phép mỗi máy tính trong mạng IP được cấu hình TCP/IP từ một hay nhiều DHCP server. DHCP cung cấp đại chỉ IP cho một máy tính trong một khoản thời gian nhất định, sau đó lấy lại đại chỉ IP đó và có thể cấp

một đại chỉ IP mới. Tất cả các công việc này được thực hiện bởi một DHCP server. Nhờ đó công việc quản lý mạng IP lớn được giảm bớt rất nhiều.

Service	TCP/IP Protocol
World Wide Web	HTTP
File Transfer	FTP, TFTP
File Sharing	NFS
Internet Mail	SMTP, POP3, IMAP
Remote Administration	Telnet
Directory Services (Internet)	DNS, LDAP
Automatic Network Address Configuration	DHCP
Network Administration	SNMP

6.2. Quản trị mạng:

6.2.1. Giới thiệu về quản trị mạng:

Khi một hệ thống mạng ngày càng phát triển thì trong đó càng có nhiều tài nguyên quan trọng hơn. khi càng có nhiều tài nguyên phục vụ cho User thì mạng lại càng trở nên phức tạp, công việc quản trị mạng càng trở nên khó khăn hơn. việc thiếu hụt tài nguyên và hiệu suất hoạt động kếm là hậu quả của việc phát triển không hoạch định và các User không thể chấp nhận điều này. do đó người quản trị mạng phải tự động quản lý hệ thống của mình, xác định sự cố và ngăn ngừa sự cố xẩy ra, tạo hiệu suất hoạt động tốt nhất cho User. Mặt khác khi hệ thống mạng chở nên quá lớn, người quản trị có thể không quản lý nổi nếu không có sự trợ giúp của các công cụ quản lý mạng tự động.

Công việc quản trị mạng bao gồm:

- Theo dõi hoạt động mạng.
- Tăng cường khả năng tự động.
- Theo dõi thời gian đáp ứng trong mạng.
- Bảo mật.
- định tuyến lưu lượng mạng.
- Cung cấp khả năng lưu trữ dữ liệu.
- Đăng ký user.

Công việc quản trị mạng chịu những trách nhiệm sau:

- **Kiểm soát tái sản chung:** Nếu tài nguyên mạng không được kiểm soát hiệu quả thì hoạt động của hệ thống mạn sẽ không đạt như mong muốn.

- **Kiểm soát độ phức tạp:** Sự phát triển bùng nổ số lượng thiết bị mạng, user, giao thức và các nhà cung cấp dịch vụ, thiết bị là những điều gây khó khăn cho công việc quản trị mạng
- **Phát triển dịch vụ:** Người sử dụng luôn mong chờ những dịch vụ mới hơn, tốt hơn khi hệ thống mạng phát triển hơn.
- **Cân bằng các nhu cầu khác nhau:** Người sử dụng luôn đòi hỏi các phần mềm ứng dụng khác nhau với những mức hỗ trợ khác nhau và yêu cầu khác nhau về mức độ hoạt động, khả năng bảo mật
- **Giảm tối đa thời gian ngừng hoạt động do sự cố:** Sử dụng các biện pháp dự phòng để đảm bảo khả năng cung cấp dịch vụ và tài nguyên mạng.
- **Kiểm soát chi phí:** Theo dõi và kiểm soát mức độ sử dụng tài nguyên để phù hợp với mức chi phí chấp nhận được.

6.2.2. OSI và mô hình quản trị mạng:

ISO (International Standards Organization) đưa ra mô hình quản trị mạng với 4 phần:

- Tổ chức.
- Thông tin.
- Liên lạc.
- Chức năng.

Phần tổ chức mô tả các thàn phần quản trị mạng, bao gồm các thành phần quản lý, các chi nhánh và mối quan hệ giữa chúng. Việc bố trí các thành phần này sẽ dẫn đến các loại cấu trúc mà chúng ta sẽ bàn đến trong phần sau của chương.

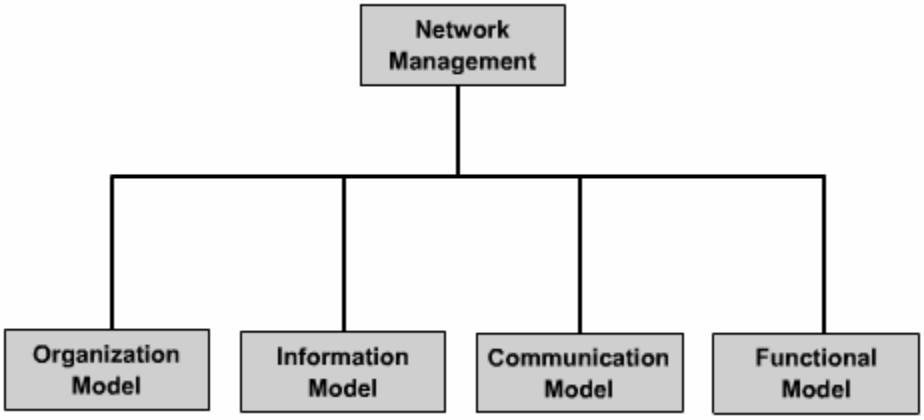
Phần thông tin liên quan đến cấu trúc và lưu trữ thông tin quản trị mạng. Những thông tin này được lưu trữ trong một cơ sở dữ liệu gọi là MIB (Management Information Base). ISO định nghĩa cấu trúc của thông tin quản trị SMI (Structure of Management Information) để định nghĩa cú pháp và thông tin quản trị lưu trong MIB. MIB và SIM sẽ được đề cập trong phần sâu hơn trong phần sau của chương.

Phần liên lạc liên quan đến thông tin quản trị được liên lạc như thế nào giữa trạm quản lý và các chi nhánh. Phần này liên quan đến các giao thức vận chuyển, gioa thức ứng dụng, yêu cầu và đáp ứng giữa 2 bên giao dịch.

Phần chức năng phân chia việc quản trị mạng theo 5 lĩnh vực chức năng như sau:

- Khắc phục lỗi.

- Cấu hình.
- Tính toán chi phí.
- Hiệu suất hoạt động.
- Bảo mật.



6.2.3. SNMP và CMPI:

Để việc quản trị mạng có thể thực hiên liên thông trên nhiều hệ thống mạng khác nhau, chúng ta cần phải có các chuẩn về quản trị mạng. Sau đây là 2 chuẩn chính nổi bật:

- SNMP (Simple Network Management Protocol): chuẩn của IèT.
- CIMP (Common Management Information Protocol): chuẩn của Teltcommunications.

SNMP là tập hợp các chuẩn về quản trị mạng, bao gồm giao thức và cấu trúc cơ sở dữ liệu. SNMP được công nhận là một chuẩn cho TCP/IP vào năm 1989 và sau đó trở nên rất phổ biến. Phiên bản nâng cấp SNMPv2c được công bố năm 1993. SNMPv2c tập chung và phân phối việc quản trị mạng, phát triển SMI, hoạt động giao thức, cấu trúc quản lý và bảo mật. SNMP được thiết kế để chạy trong mạng óI cũng như mạng TCP/IP. Kể từ SNMPv3c, việc truy cập MIB được bảo vệ bằng việc xác minh và mã hóa gói dữ liệu khi truyền qua mạng.

CMIP là một giao thức quản trị mạng OSI, do SIO tạo ra và chuẩn hóa. CMIP thực hiên theo dõi và kiểm soát hệ thống mạng.

6.2.4. Hoạt động của SNMP:

SNMP là một giao thức lớp ứng dụngđược thiết kế để thực hiện các thông tin quản trị mạng giữa các thiết bị mạng. Với SNMP chúng ta sẽ có được các dữ liệu về thông tin quản trị, ví dụ: số lượng gói được gửi đi qua cổng trong mỗi giây, số lượng kết nối TCP đang mở, qua đó nhà quản trị mạng có thể dễ dàng quản lý hoạt động của hệ thống mạng,tìm và xử lý nó.

Hiện nay SNMP là giao thức về quản trị mạng được sử dụng phổ biến nhất trong mạng các doanh nghiệp, trường đại học□

SNMP là một giao thức đơn giản nhưng nó có khả năng xử lý hiệu quả nhiều sự cố khó khâun trong những hệ thống mạng phức tạp.

Mô hình tổ chức của mạng quản lý bằng SNMP bao gồm 4 thành phần:

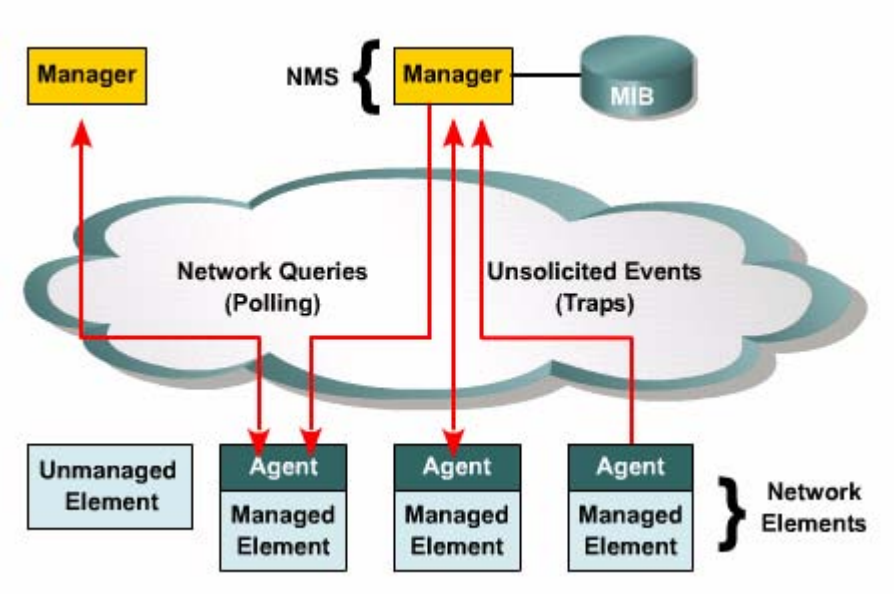
- Trạm quản lý NMS (Network Management Station).
- Chi nhánh quản lý (Management Agent).
- Cơ sở dữ liệu thông tin quản trị MIB (Management Information Base).
- Giao thức quản trị mạng.

NMS thường là một máy trạm độc lập nhưng nó thực hiện nhiệm vụ cho toàn bộ hệ thống. Trên đó cài đặt một số phần mềm quản trị mạng NMA (Network Management Application). Trên NMA có giao diện giao tiếp với user, cho phép người quản trị có thể thông qua đó để quản lý mạng. Các phần mềm này có thể trả lời các yêu cầu của user qua mạng. Chi nhánh quản lý là các phần mềm quản trị mạng được cài đặt trên các thiết bị mạng then chốt như router, bridge, hub, host. Các phần mềm này cung cấp thông tin quan trọng cho NMS. Tất cả các thông tin quản trị mạng được lưu trữ trong cơ sở dữ liệuđặt tịa bản thân mỗi thiết bị. Mỗi thiết bị chi nhánh quản lý lưu các thông tin sau:

- Số lượng và trạng thái các kết nối ảo của thiết bị đó.
- Số lượng các thông điệp báo lỗi mà thiết bị đó nhận được.
- Số lượng bytevà gói dữ liệu được thiết bị nhận vào và chuyển ra.
- Chiều dài tối đa của hàng đợi chờ xuất ra.
- Các thông điệp quảng bá nhận được và gửi đi.
- Số lần các cổng bị tắt và hoạt động trở lại.

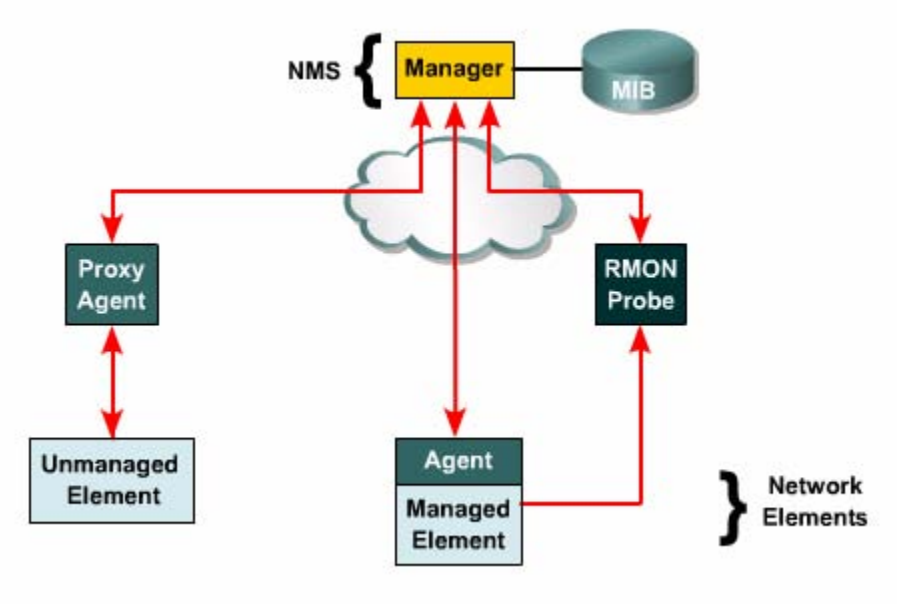
NMS thực hiện chức năng theo dõi bằng cách nhận các thông tin từ MIB. Việc thông tin liên lạc giữa trạm quản lý các chi nhành được thực hiện bởi giao thức quản trị mạng lớp ứng dụng. SNMP sử dụng UDP và post 161, 162. Chúng trao đổi ba loại thông điệp sau:

- Get: Trạm quản lý lấy thông tin của MIB trên chi nhánh.
- Set: Trạm quản lý cài đặt giá trị thông tin của MIB trên chi nhánh.
- Trap: Chi nhánh thông báo cho trạm quản lý khi có một sự kiện xảy ra.

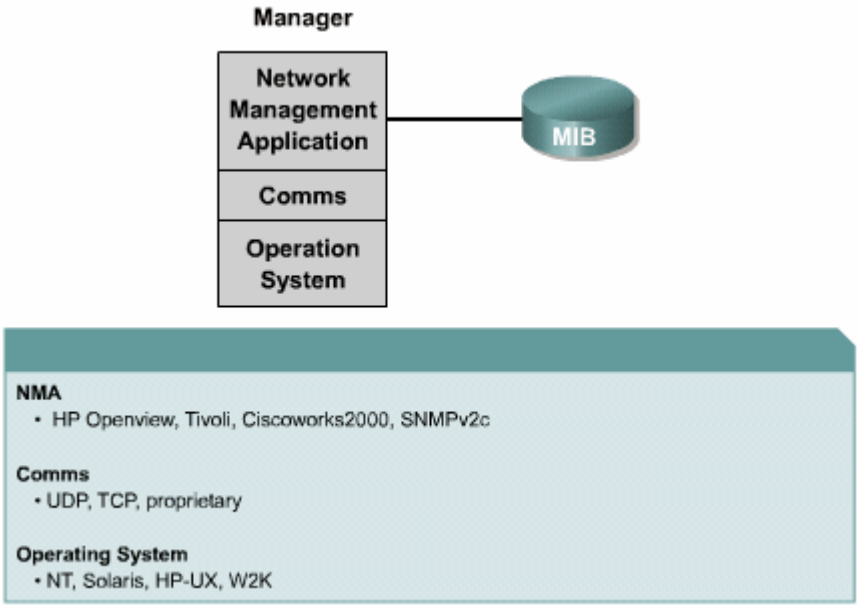


Mô hình thông tin liên lạc như trên được xem là mô hình hai tầng, xem hình 6.2.4.a. Mọi thành phần trong mạng đều được quản lý bởi SNMP. Trong một vài trường hợp, một số thiết bị có quyền ưu tiên quản trị cao hơn, chúng ta cần có mô hình ba tầng. Trạm quản lý mạng thu thập thông tin và kiểm soát những thiết bị có quyền ưu tiên này thông qua một chi nhánh proxy. Chi nhánh proxy dịch các yêu cầu SNMP từ trạm quản lý sang dạng phù hợp với hệ thống bên dưới nó và sử dụng một giao thức quản trị mạng riêng, phù hợp với hệ thống bên dưới. Proxy nhận được trả lời từ hệ thống bên dưới, sau đó dịch các trả lời này sang thông điệp SNMP và gửi lại cho trạm quản lý.

Phần mềm quản trị mạng thường chuyển một số chức năng quản trị mạng cho máy dò RMON(remote monitor) . máy dò RMON thu nhập thông tin quản trị mạng nội bộ , sau đó gửi thông tin tổng hợp theo định kỳ cho trạm quản lý.

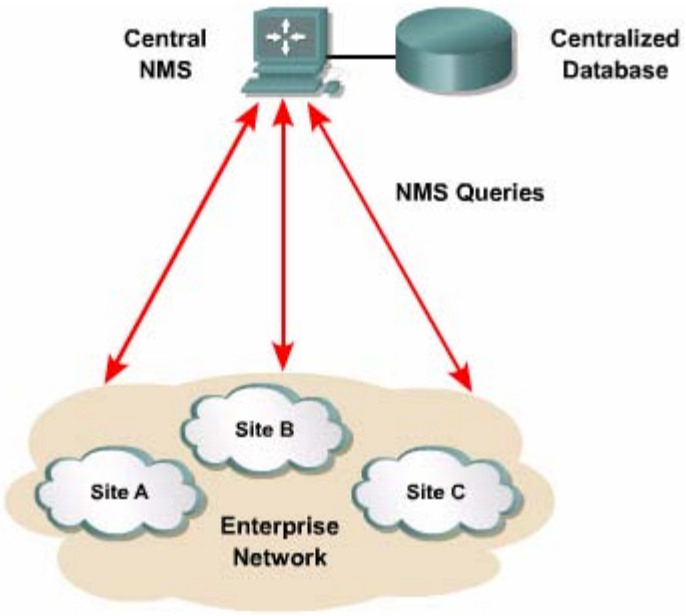


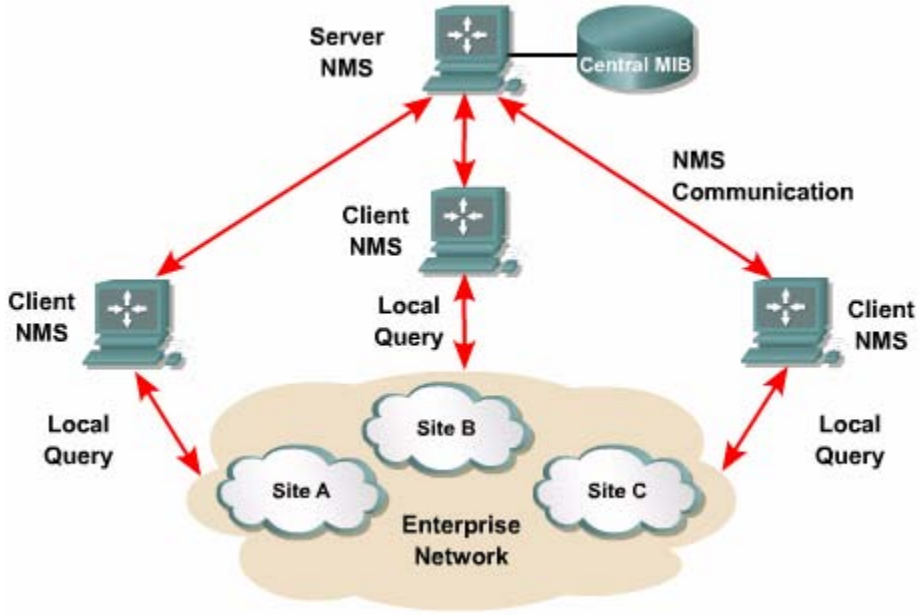
NMS là một máy trạm bình thường chạy một hệ điều hành đặc trưng NMS có dung lượng RAM lớn để có thể chạy mọi trình ứng dụng quản trị mạng cùng một lúc. Một số chương trình quản trị mạng Ciscoworks2000, HP Openview.

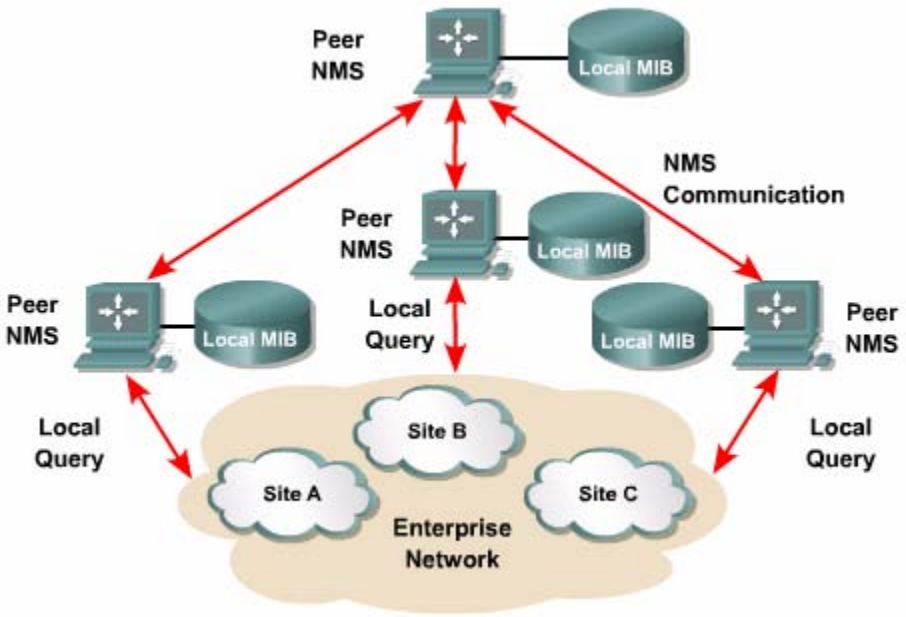


Như vậy nói ở trên, trạm quản lý có thể là một máy trạm độc lập chuyên gửi các yêu cầu đến mọi chi nhánh mà không cần biết chúng nằm ở đâu (hình 6.2.4.d). trong một số hệ thống mạng được phân chia thành nhiều site, thì mỗi site nên có một NMS nội bộ. Tất cả các NMS liên lạc với nhau theo mô hình client-server. Một NMS đóng vai trò là server, các NMS còn lại là client. Các client gửi dữ liệu của nó

cho server để tập chung lưu trữ tại đó (hình 6.2.4.e). một mô hình khác là tất cả NMS đều có chách nhiệm ngang nhau, mỗi NMS quản lý cơ sở dữ liệu riêng của nó, như vậy thông tin quản trị được phân phối trên nhiều NMS(hình 6.2.4.f)







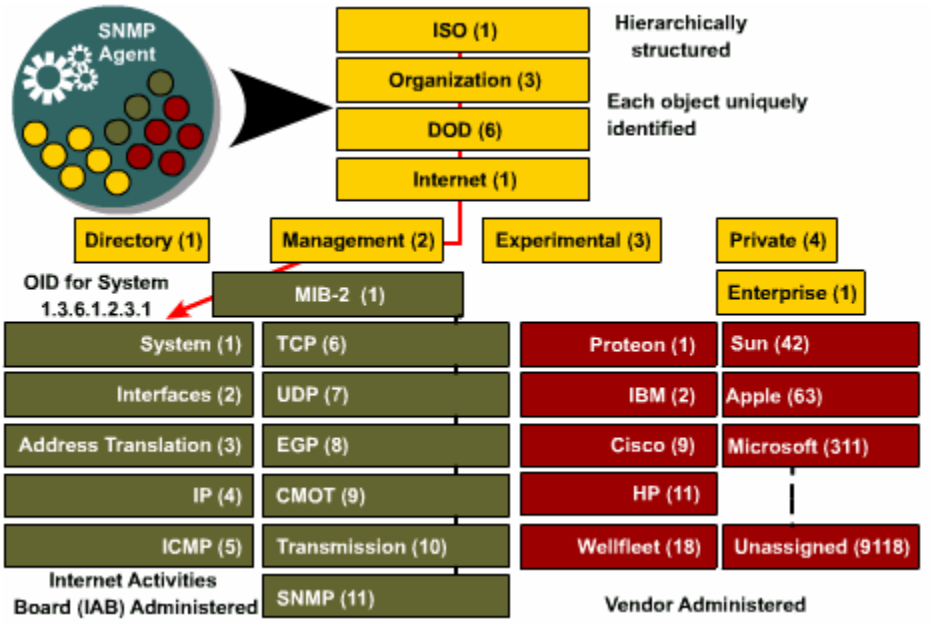
6.2.5 cấu trúc của thông tin quản trị và MIB:

MIB được sử dụng để lưu thông tin về các thành phần mạng và những chi tiết của chúng. Các thông tin này được lưu theo một cấu trúc nhất định trong MIB. Cấu trúc này được định nghĩa theo chuẩn SMI trong đó định nghĩa loại dữ liệu cho mỗi đối tượng, cách đặt tên cho đối tượng và mã hoá đối tượng như thế nào khi chuyền qua mạng.

MIB là nơi lưu trữ thông tin cấu trúc cao cấp. Có rất nhiều chuẩn MIB nhưng cũng có nhiều MIB độc quyền cho thiết bị cho một hãng nào đó. Ban đầu SMI MIB được phân loại thành 8 nhóm khác nhau với tổn cộng 114 đối tượng được định nghĩa và quản lý. Trong MIB —II thay thế cho MIB-I, có thêm nhiều nhóm mới được định nghĩa (185 đối tượng được định nghĩa).

Tất cả các đối tượng quản lý trong môi trường SNMP được sắp xếp theo cấu trúc hình cây phân cấp. Những đối tượng nằm phía dưới sơ đồ là những đối tượng được quản lý thực sự. Mỗi đối tượng này được quản lý thông qua các thông tin về tài nguyên, hoạt động các thông tin có liên quan khác . mỗi đối tượng được quản lý có một chỉ số danh định riêng SNMP chỉ dụng chỉ số này để xác định các giá trị

cần tìm hay cần sửa đổi trong MIB. Chúng ta có thể tham khảo thêm về các đối tượng này trong www.ietf.org.



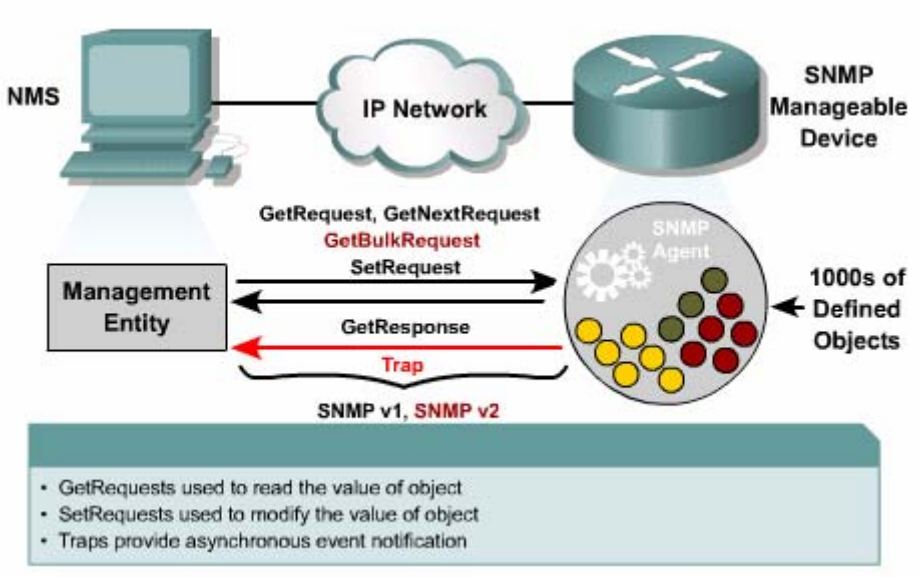
6.2.6. giao thức SNMP:

Các chi nhánh quản trị mạng là các thiết bị mạng như router, switch, hub, máy in, server, trên đó cài một phần mềm có chức năng quản trị mạng. phần mềm này chịu trách nhiệm xử lý các yêu cầu SNMP nhận được từ trạm quản lý, đồng thời bảo trì các thông tin về các đối tượng được quản lý lưu trong MIB.

Sự thông tin liên lạc giữa trạm quản lý và các chi nhánh được thực hiện bởi SNMP. Trong phiên bản đầu tiên SNMP V1 có 3 loại thông điệp được trạm quản lý NMS gửi đi: Getrequest, GetnextRequest và Setquest. Cả ba thông điệp này đều được các chi nhánh hồi đáp bằng thông điệp GetReponse. Khi có sự thay đổi xảy ra làm thay đổi thông tin trong MIB thì các chi nhánh sẽ gửi thông điệp trap báo cho NMS.

Phiên bản SNMP v2 khắc phục một số nhược điểm của SNMP V1. trong đó, bước cải tiến quan trọng nhất là có thêm loại thông điệp GetBulkRequest và bộ

đếm 64 bit cho MIB. Việc thu nhập thông tin bằng GetBulkRequest và GetnextRequest không được hiệu quả vì chỉ lấy được một giá trị cho một cho mỗi lần gửi. Với GetnextRequest trạm quản lý có thể nhận được nhiều thông tin. Bộ đếm 64 khắc phục được nhược điểm bị tràn quá nhanh của bộ đếm trước đây,nhatá là với đường truyền tốc độ cao hiện nay như Gigabit Ethernet.

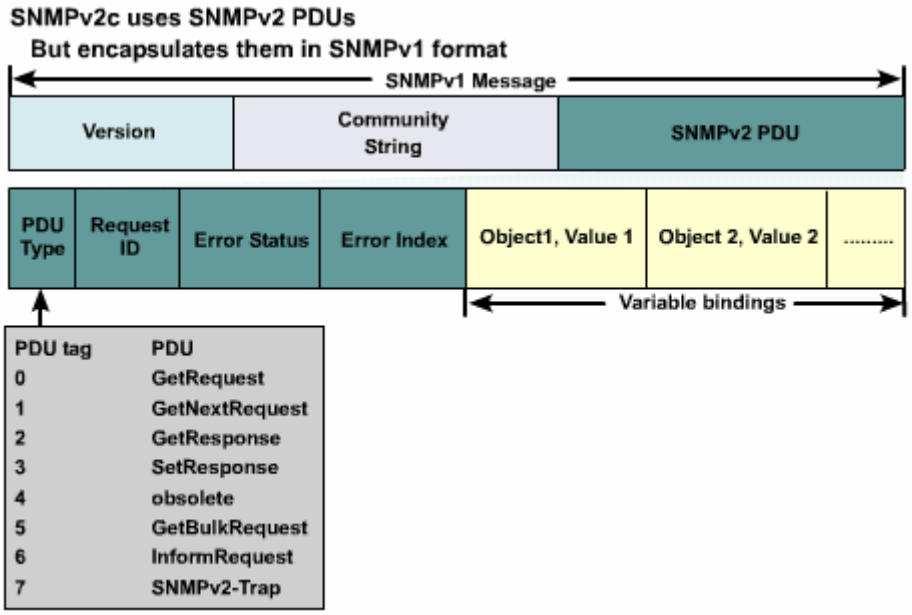


Trạm quản lý xử lý thông tin thu nhập được từ các trạm chi nhánh với nhiều cách khác nhau. Các thông tin này có thể được truy cập, hiển thị và so sánh với các giá trị được cấu hình trước đó để kiểm tra điều kiện hoạt động có được thoả mãn hay không. Nhà quản trị mạng vẫn có khả năng cấu hình, thay đổi các giá trị trong trạm quản lý.

Việc trao đổi thông tin giữa trạm quản lý và các chi nhánh làm tăng thêm lưu lượng mạng. đây là điểm cần lưu ý mỗi khi đặt trạm quản lý vào mạng. việc theo dõi hệ thống quá chi tiết đôi khi lại có tác dụng ngược đối với hiệu suất hoạt động của mạng vì các thiết bị được theo dõi phải xử lý thêm các thông tin trao đổi theo định kỳ càng ít càng tốt. Chúng ta càn xác định những thiết bị và những đường kết nối nào là quan trọng và chúng ta cần những thông tin nào nhất.

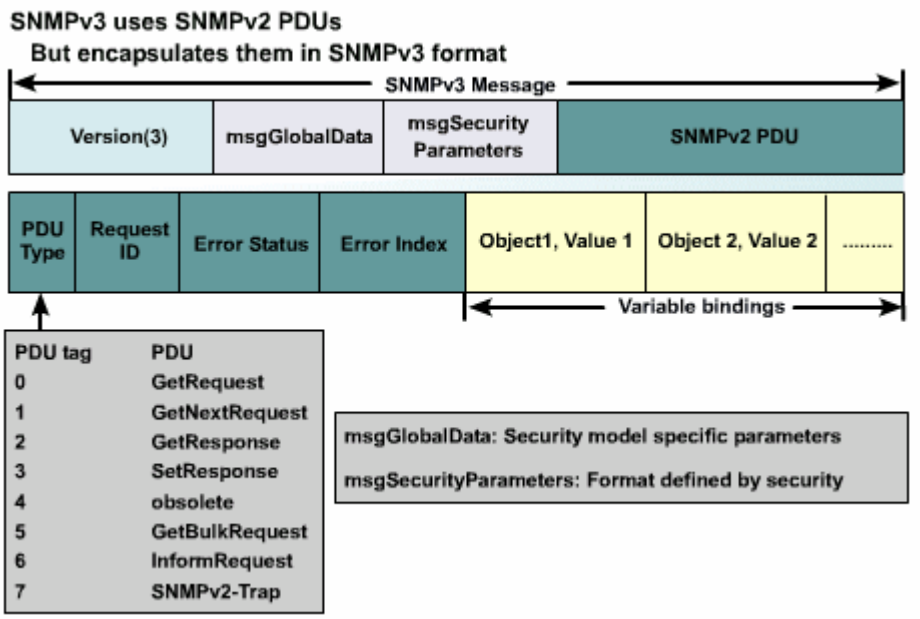
SNMP sử dụng UDP làm giao thức không theo hướng kết nối và không tin cậy, do đó SNMP có thể bị mất thông điệp. Bản thân SNMP cũng không có cơ chế bảo đảm việc truyền dữ liệu do đó các ứng dụng sử dụng SNMP phải có trách nhiệm kiểm soát việc mất mát các thông điệp.

Mỗi thông điệp SNMP có chứa một chuỗi ký tự không mã được gọi là community string. Community string được sử dụng như là password để truy cập vào trạm quản lý, trong hình 6.2.6.b là cấu trúc của thông điệp SNMPv2c. chi tiết hơn về các thnàh phần này các bạn có thể xem thêm trong RFC1905.



SNMPv2c dùng SNMPv2 PDUs

Nhưng gói chúng trong SNMPv1 format



Community string là lỗ hổng bảo mật tồn tại cho đến khi nhóm phát triển SNMPv2 thông qua một cơ chế bảo vệ với kết quả là SNMPv3 ra đời. Tất cả các ứng dụng quản trị dựa trên SNMP đều cần phải cấu hình giá trị phù hợp cho Community string. Có nhiều công ty tổ chức thay đổi thường xuyên giá trị của Community string để giảm bớt nguy cơ tồn tại hoạt động phá hoại thông qua việc sử dụng dịch vụ SNMP bất hợp pháp.

Thiết bị Cisco đã hỗ trợ SNMPv3 nhưng đa số các phần mềmquản trị vẫn còn chưa hỗ trợ SNMPv3. SNMPv3 hỗ trợ nhiều mô hình bảo mật khác nhau đang được sử dụng hiện nay.

6.2.7 cấu hình SNMP:

Để NMS có thể giao tiếp với các thiết bị mạng thì SNMP phải được cấu hình trên các thiết bị với SNMP Community string.

6.2.8. RMON:

RMON là một bước tiến quan trọng trong việc quản trị hệ thống mạng nó định nghĩa một MIB theo dõi từ xa chính là MIB-II và cung cấp cho nhà quản trị một lượng thông tin lớn về hệ thống mạng. ưu điểm chính của RMON là nó mở rộng chức năng cuae SNMP mà không hề thay đổi nền tảng bên dưới của giao thức SNMP. RMON đơn giản chỉ là một dạng đặc biệt của MIB.

Chuẩn RMON đầu tiên được thiết kế theo IETF RFC 1271 hiện nay là RFC 1757. RMON được thiết kế để cung cấp khả năng theo dõi và phân tích linh động. Các thiết bị đươc theo dõi chính là các chi nhánh nằm trong các mạng con có thể báo động cho người sử dụng và thu thập thông tin về các trạng thái hoạt động bằng cách phân tích mọi frame trong mạng đó.

Chuẩn RMON chia các chức năng theo dõi thành 9 nhóm hỗ trợ cho mô hình Ethernet và nhóm thứ 10 trong RFC 1513 hỗ trợ thêm cho các đặc tính riêng của Token ring. Sau đay là các nhóm RMON đã được định nghĩa

Statistics group: bảo trì các thông tin về hoạt động và các lỗi xảy ra trong một mạng đang được theo dõi . ví dụ các thông tin về lượng băng thông đang sử dụng lượng broadcast, multicast lỗi CRC mảnh frame gãy

History group: theo định kỳ lấy các thông tin từ Statistics group ra làm mẫu và lưu lại để sau đó có thể tìm lại được: ví dụ số lượng lỗi, số lượng gói dữ liệu

Alarm group: cho phép nhà quản trị mạng cài đặt chu kỳ lấy mẫu và mức ngưỡng cho các giá trị được lưu bởi các chi nhánh , ví dụ giá trị tuyệt đối và giá trị tương đối mức ngưỡng trên và mức ngưỡng dưới .

Host group: định nghĩa đơn vị đo cho các laọi lưu lượng đến và đi từ các host trong mạng ví dụ: số gói gửi và nhận số byte gửi và nhận, số byte lỗi số gói broadcast và multicast.

Host topN group: cung cấp báo cáo về trạng thái của nhóm Top N host trong Statistic group.

Traffic matrix group: lưu các trạng thái hoạt động và lối giữa các cặp hai node giao tiếp với nahu trong mạng ví dụ số lượng lỗi, số lượng gói byte giữa hai node.

Filter group: lọc các gói dưc liệu từ frame thoả mãn với mẫu của user dã định trước.

Packet capture group: định nghĩa các packet nào phù hợp với tiêu chuẩn nào định trước để lưu lại.

Event group: cho phép hiển thị các sự kiện xảy ra cùng thời gian xảy ra sự kiện đó.

6.2.9. syslog

Tính năng syslog của cisco dựa trên tính năng syslog của UNIX các sự kiện của hệ thống được hiển thị ra màn hình console của hệ thống trừ khi tính năng này bị tắt đi. Tính năng syslog là cơ chế cho phép các ứng dụng, các tiến trình và hoạt động hệ thống của thiết bị Cisco thông báo các hoạt động và lỗi.

Các thông điệp syslog có 8 mức độ khác nhau, từ 0 đến 7, trong đó mức 0 là mức nguy cấp nhất:

0 Emergencies

1 Alerts

2 Critical

3 Erros

4 Warnings

5 Notifications

6 Informational

7 Debugging

Để NMS có thể nhận và nghi lại các thông điệp hệ thống từ các thiết bị thì trên các thiết bị phải được cấu hình syslog. Sau đây là các lệnh để cấu hình cho các thiết bị này.

Để mở chế độ logging:

Router (config) #logging on

Để gửi thông điệp log cho một syslog server:

Router (config) #logging *hostname* | *ip address*

Cài đặt mức độ cho các thông điệp, ví dụ mức độ 6 (mức độ 6 la mức độ mặc định của Cisco IOS):

Router (config) #logging trap informational

Để thông điệp syslog có kèm theo thời gian của sự kiện:

Router (config) #service timestamps log datetime

TỔNG KẾT

Sau đây là những điểm quan trọng mà các bạn cần nắm vững trong chương này:

- Chức năng của máy trạm và server.
- Vai trò của cá thiết bị khác nhau trong môi trường client/server.
- Sự phát triển của hệ điều hành mạng Nó.
- Cái nhìn tổng quát về hệ điều hành Windows và các hệ điều hành khác.
- Nguyên nhân tại sao cần phải quản trị hệ thống mạng.
- Mô hình OSI và mô hình quản trị mạng.
- Các loại công cụ quản trị mạng và các loại ứng dụng của nó.
- Vai trò của SNMP và CMIP trong việc theo dõi hệ thống mạng.
- Các phần mềm quản trị mạng thu thập thông tin và ghi lại các sự cố như thế nào.
- Việc thu thập các thông tin về hoạt động mạng được thực hiện như thế nào.