TRƯỜNG CAO ĐẲNG NGHỀ CÔNG NGHIỆP HÀ NỘI
Tác giả: Dương Ngọc Việt (chủ biên).
Lê Văn Úy.

GIÁO TRÌNH

Cấu hình và quản trị thiết bị mạng

(Lưu hành nội bộ)

Hà Nội năm 2012

Tuyên bố bản quyền

Giáo trình này sử dụng làm tài liệu giảng dạy nội bộ trong trường cao đẳng nghề Công nghiệp Hà Nội

Trường Cao đẳng nghề Công nghiệp Hà Nội không sử dụng và không cho phép bất kỳ cá nhân hay tổ chức nào sử dụng giáo trình này với mục đích kinh doanh.

Mọi trích dẫn, sử dụng giáo trình này với mục đích khác hay ở nơi khác đều phải được sự đồng ý bằng văn bản của trường Cao đẳng nghề Công nghiệp Hà Nội

LỜI GIỚI THIỆU

Trong những năm qua, dạy nghề đã có những bước tiến vượt bậc cả về số lượng và chất lượng, nhằm thực hiện nhiệm vụ đào tạo nguồn nhân lực kỹ thuật trực tiếp đáp ứng nhu cầu xã hội. Cùng với sự phát triển của khoa học công nghệ trên thế giới, lĩnh vực Công nghệ thông tin nói chung và ngành Quản trị mạng ở Việt Nam nói riêng đã có những bước phát triển đáng kể.

Chương trình dạy nghề Quản trị mạng đã được xây dựng trên cơ sở phân tích nghề, phần kỹ năng nghề được kết cấu theo các môđun. Để tạo điều kiện thuận lợi cho các cơ sở dạy nghề trong quá trình thực hiện, việc biên soạn giáo trình theo các môđun đào tạo nghề là cấp thiết hiện nay.

Mô đun 34: Cấu hình và quản trị thiết bị mạng là mô đun đào tạo chuyên môn nghề được biên soạn theo hình thức tích hợp lý thuyết và thực hành. Trong quá trình thực hiện, nhóm biên soạn đã tham khảo nhiều tài liệu Quản trị mạng trong và ngoài nước, kết hợp với kinh nghiệm trong thực tế.

Mặc dầu có rất nhiều cố gắng, nhưng không tránh khỏi những khiếm khuyết, rất mong nhận được sự đóng góp ý kiến của độc giả để giáo trình được hoàn thiện hơn.

Xin chân thành cảm ơn…

Tháng 02 năm 2012

MỤC LỤC

MÔ ĐUN CẤU HÌNH VÀ QUẢN TRỊ THIẾT BỊ MẠNG

Mã mô đun: MĐ 34

I.VỊ TRÍ, TÍNH CHẤT, Ý NGHĨA VÀ VAI TRÒ CỦA MÔ ĐUN

- Vị trí: Mô đun được bố trí sau khi sinh viên học xong môn, mô đun: Mạng máy tính và Quản trị mạng 1.
- Tính chất: Là mô đun chuyên nghành bắt buộc.
- Ý nghĩa: Đây là mô đun đào tạo chuyên môn nghề, cung cấp cho sinh viên các kỹ năng cơ bản nhất của nghề Quản trị mạng.

II. MỤC TIÊU MÔ ĐUN:

- Giải thích sự khác nhau giữa LAN và WAN;
- Xác định được các thành phần bên trong Router;
- Chuyển đổi giữa các chế độ cấu hình router;
- Thiết lập kết nối bằng HyperTerminal vào router;
- Sử dụng tính năng trợ giúp trong giao tiếp bằng dòng lệnh;
- Nắm được nơi nào mà router lưu các loại tập tin khác nhau;
- Phân biệt các loại giao thức định tuyến;
- Sử dụng được các lệnh định tuyến cho router.
- Bố trí làm việc khoa học đảm bảo an toàn cho người và phương tiện học tập.

III. NỘI DUNG MÔ ĐUN:

1. Nội dung tổng quát và phân phối thời gian :

Số TT	Tên các bài trong mô đun	Thời gian			
		Tổng số	Lý thuyết	Thực hành	Kiểm Tra*
1	WAN và Router	3	3		
2	Giới thiệu về Router	3	3		
3	Cấu hình Router	18	4	13	1
4	Cập nhật thông tin từ các thiết bị khác	11	3	7	1
5	Quản lý phần mềm IOS	13	3	9	1
6	Định tuyến và các giao thức định tuyến	17	5	12	

7	Giao thức định tuyến theo Vector khoảng cách	21	6	15	
8	Thông điệp điều khiển và báo lỗi của TCP/IP	4	3		1
	Cộng	90	30	56	4

BÀI 1: WAN VÀ ROUTER
Mà bài: MĐ34-01

Giới thiệu:

Mạng diện rộng (WAN) là mạng 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.

Mục tiêu:

- Xác định được tổ chức quốc tế chịu trách nhiệm về các chuẩn của WAN.
- Giải thích sự khác nhau giữa LAN và WAN.
- Mô tả vai trò của Router trong WAN.
- Xác định được các thành phần vật lý bên trong Router.
- 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.
- Thực hiện các thao tác an toàn với máy tính.

Nội dung:

1. WAN

Mục tiêu:

- Xác định được tổ chức quốc tế chịu trách nhiệm về các chuẩn của WAN.
- Giải thích sự khác nhau giữa LAN và WAN.
- Mô tả vai trò của Router trong WAN.

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 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 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

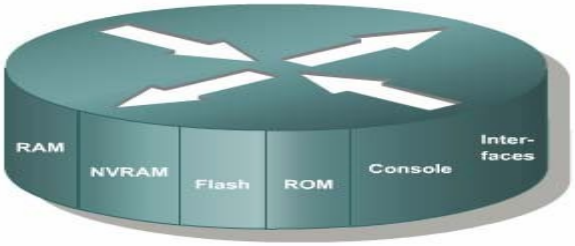
quốc tế - CCITT (Consultative Committee for International Telegraph and Telephone).

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).

1.2. Giới thiệu về router trong mạng WAN



Hình 1.2: Các thành phần Router

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 đặc điểm và chức năng như sau:

Lưu bảng định tuyến.

Lưu bảng ARP.

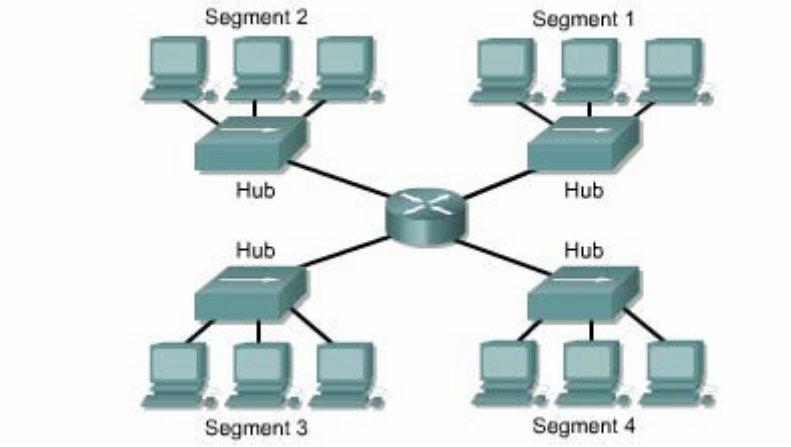
Có vùng bộ nhớ chuyển mạch nhanh.
Cung cấp vùng nhớ đệm cho các gói dữ liệu
Duy trì hàng đợi cho các gói dữ liệu.
Cung cấp bộ nhớ tạm thời cho tập tin cấu hình của router khi router đang hoạt động.
Thông tin trên RAM sẽ bị xoá mất khi router khởi động lại hoặc bị tắt điện.

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 dưới dạng card rời.

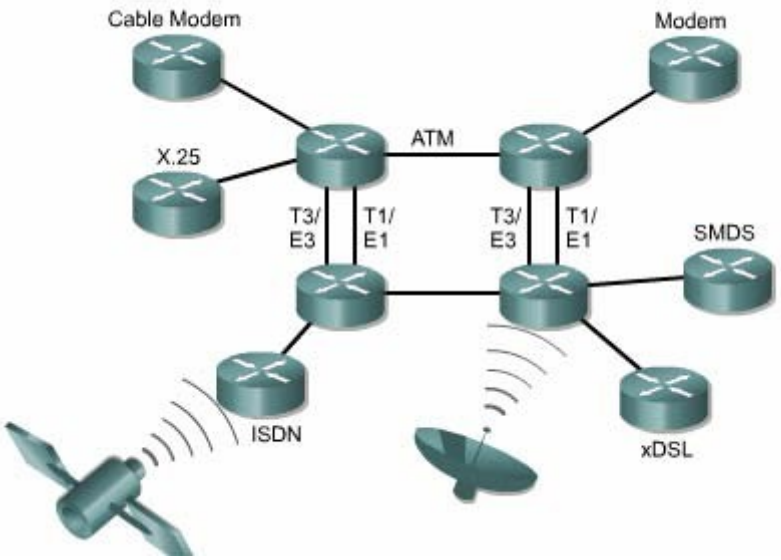
1.3. Router LAN và WAN



Hình 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 1.3b: 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 thì bảng định tuyến được lưu giữ động nhờ các giao thức định tuyến thực hiện trao đổi thông tin mạng giữa các router.

Hình 1.3c

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.

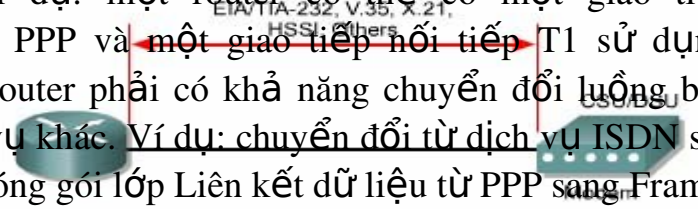
1.4. Vai trò của router trong mạng WAN

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 yêú 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.

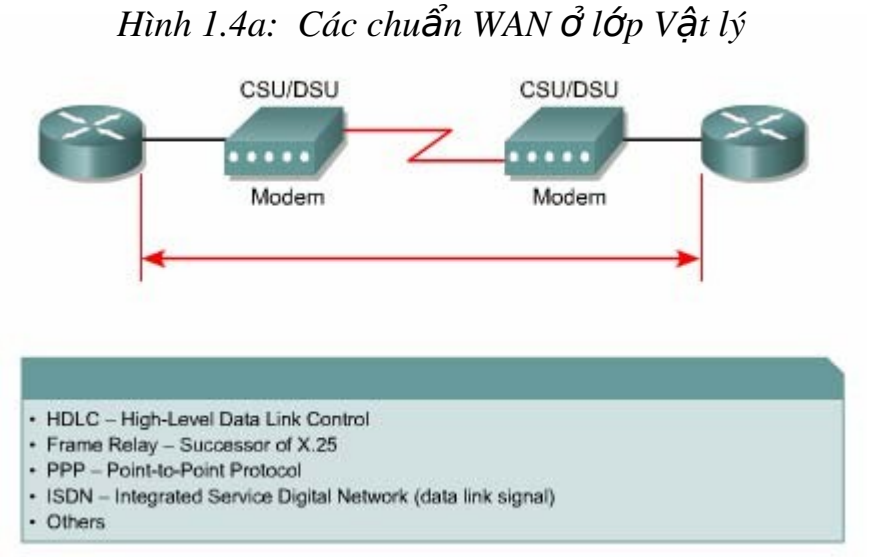


Chi tiết về các giao thức lớp 1 và 2 trong mạng WAN sẽ được đề cập ở

DTE	DCE
Data Terminal Equipment User device with interface connecting to the WAN link	**Data-Circuit Terminating Equipment** End of the WAN provider's side of the communication facility

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 1.4a: Các chuẩn WAN ở lớp Vật lý



Hình 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.

1.5. Các 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).

2. Router

Mục tiêu:

- Xác định được các thành phần vật lý bên trong Router.
- 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.

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.

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 à flash 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

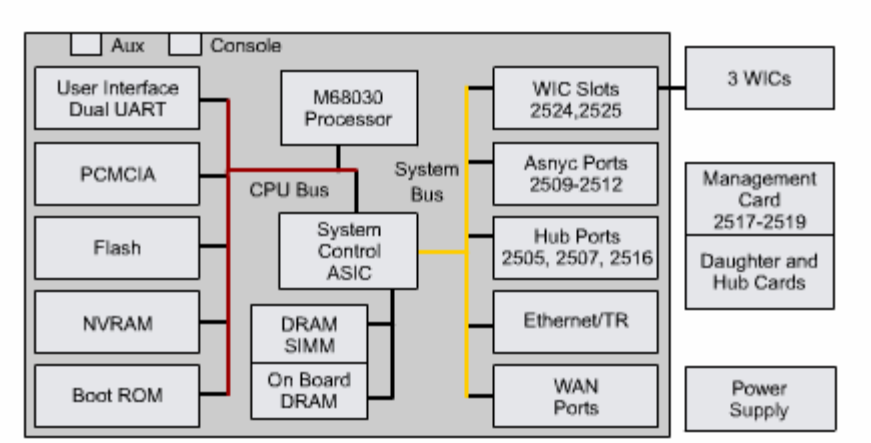
bằng cách thay chip ROM mới.

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.

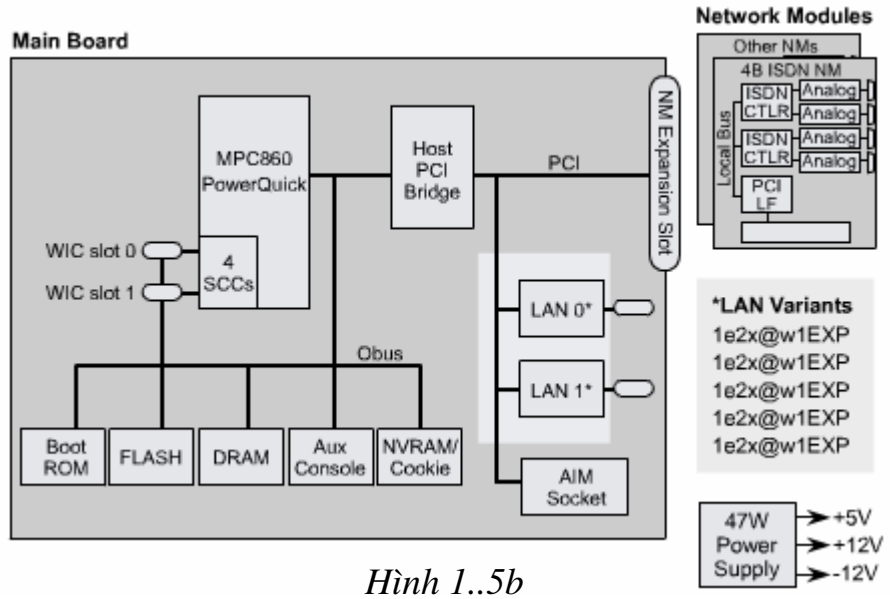
Cổng giao tiếp WAN có thể là cổng Serial, ISDN, cổng tích hợp đơn vị dịch vụ kênh CSU (Chanel Service Unit). Tương tự như cổng giao tiếp LAN, các cổng giao tiếp WAN cũng có chip điều khiển đặc biệt. Cổng giao tiếp WAN có thể định trên router hoặc ở dạng card rời.

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 1.5a

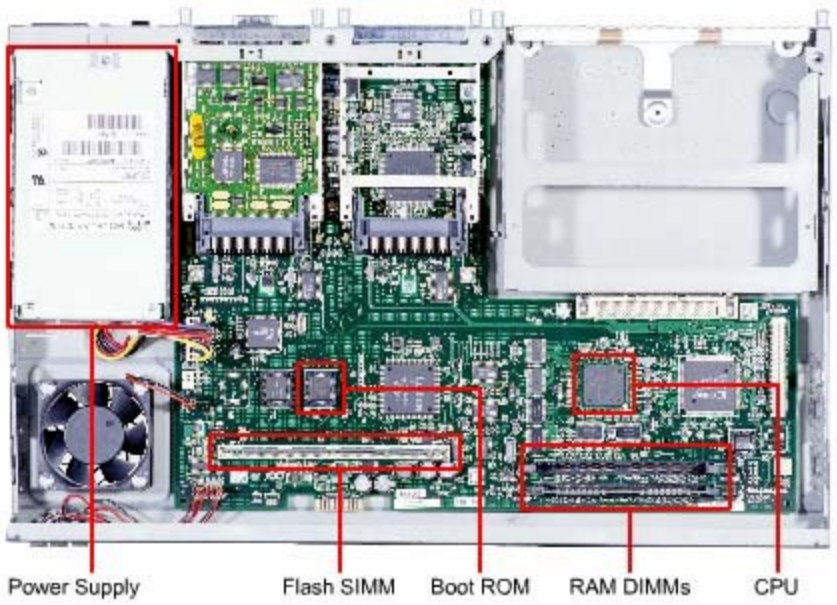


Hình 1..5b

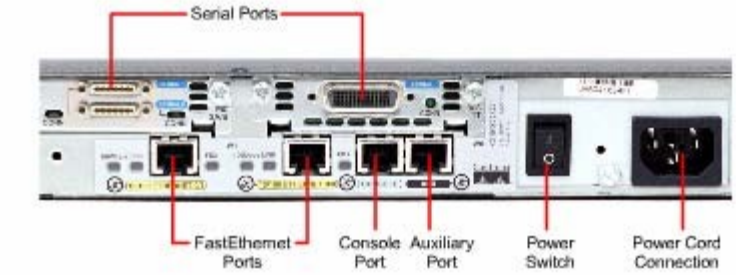
2.2. Đặc điểm vật lý của router

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 1.6a: Cấu trúc bên trong của router 2600



Hình 1.6b: Các loại kết nối bên ngoài của router 2600

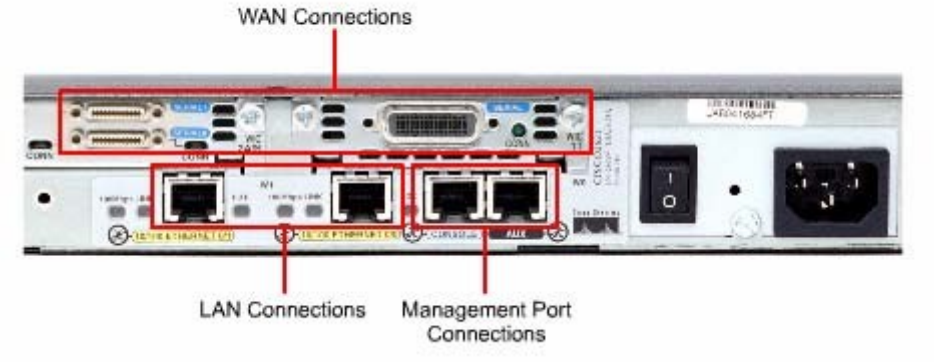
2.3. Các loại kết nối ngoài của router

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.



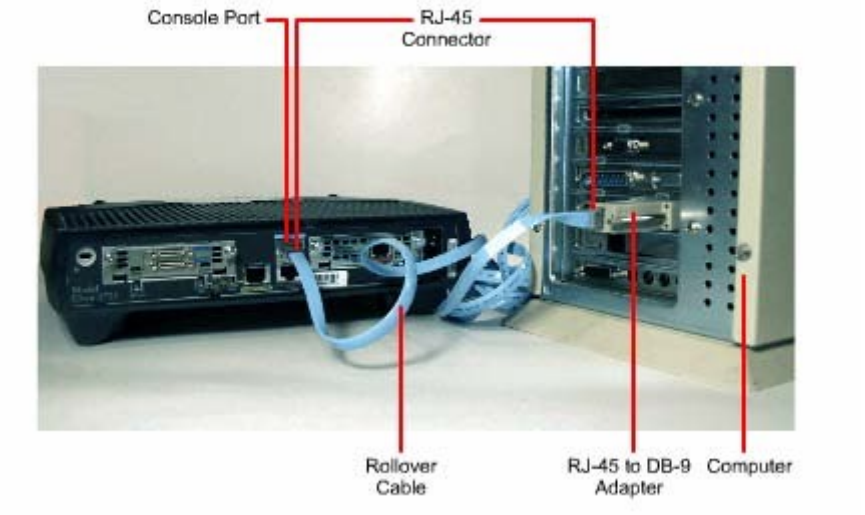
Hình 1.7: Các loại kết nối bên ngoài của router

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 1.8: 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.

2.5. Thiết lập kết nối và cổng console

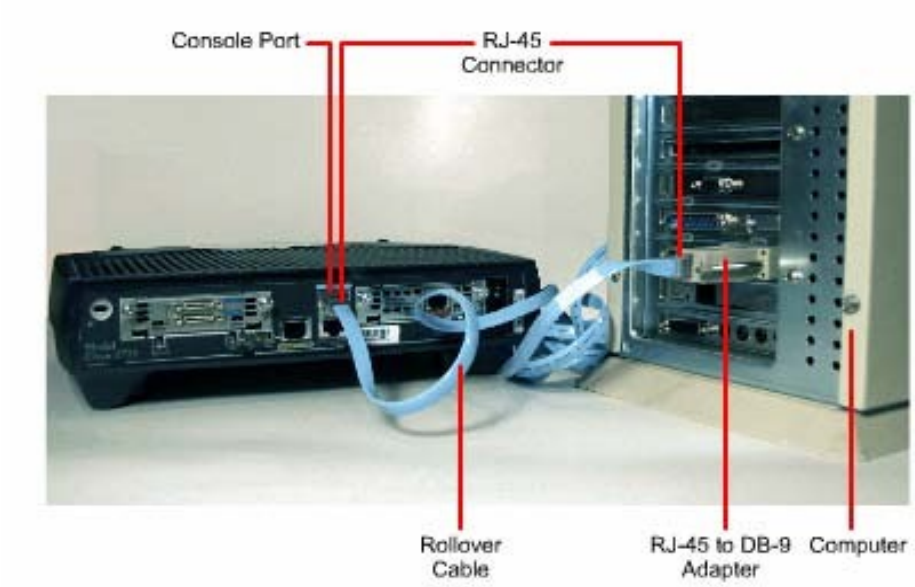
Cổng console là loại cổng quản lý, cung cấp đường kết nối riêng vào router. Cổng này được sử dụng để thiết lập cấu hình cho router, theo dõi hoạt động mạng và khôi phục router khi gặp sự cố nghiêm trọng.

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.

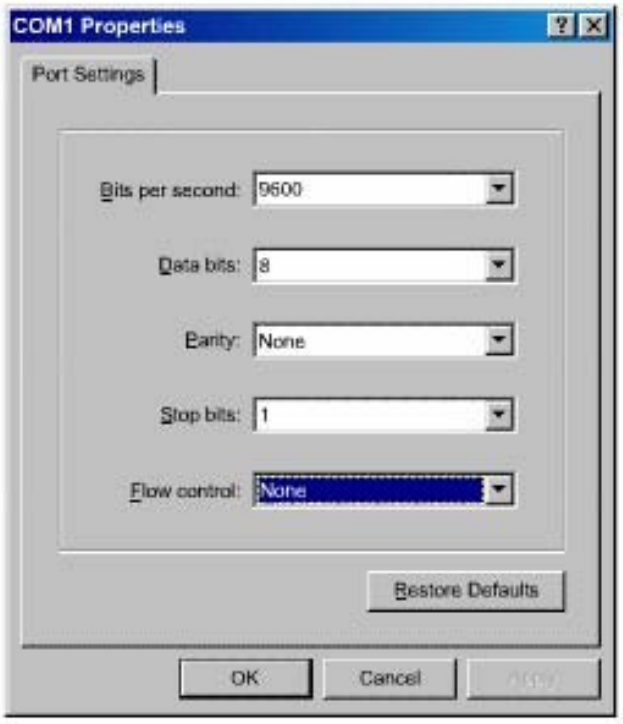
PC hay thiết bị đầu cuối phải có chương trình mô phỏng thiết bị đầu cuối VT100. Thông thường phần mềm này là HyperTerminal.

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
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 1.9a: Kết nối PC vào cổng console trên router



HÌnh 1.9b: Cấu hình hyper terminal để kết nối vào console

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.

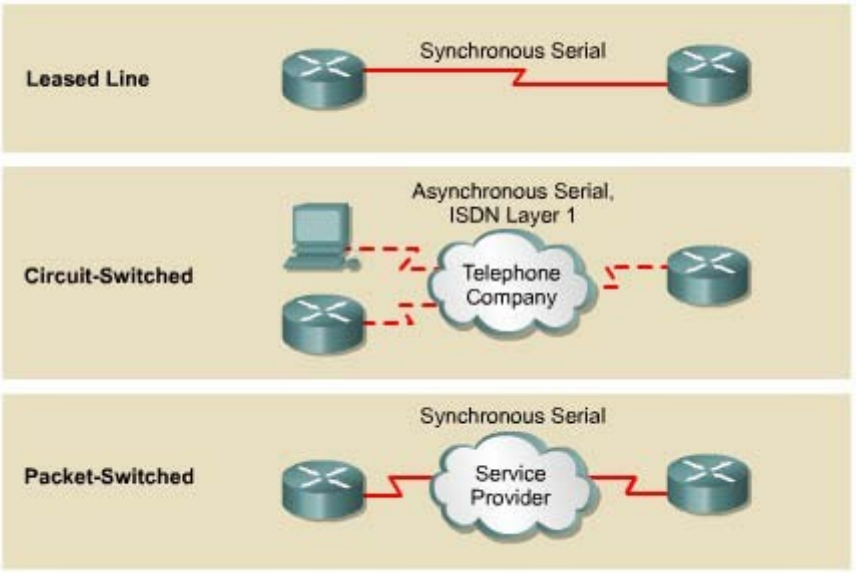
Trong một số trường hợp ta có thể kết nối trực tiếp cổng Ethernet trên router vào máy tính hoặc vào router khác bằng cáp chéo.

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.

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.

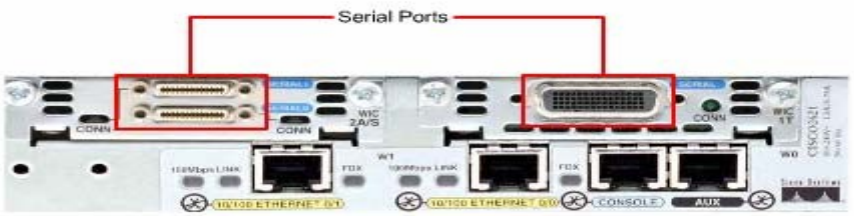


Hình 1.10a: Các loại kết nối WAN

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:

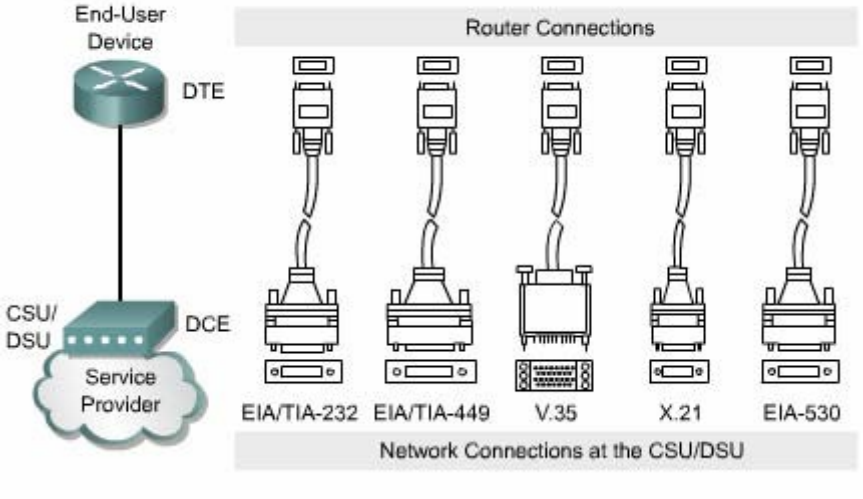
Loại kết nối trên thiết bị Cisco là loại nào? Cisco router sử dụng nhiều loài đầu nối khác nhau cho cổng Serial. Như trong hình 1.2.7b, cổng bên trái là cổng Smart Serial, cổng bên phải là cổng DB-60. Lựa choncáp Serial để kết nối hệ thống mạng là một phần then chốt trong qua trìnhthiết lập WAN.



Hình 1.10b: Các loại đầu nối cho cổng Serial

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.

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 1.10c: Kết nối các thiết bị DTE và DCE

BÀI 2: GIỚI THIỆU VỀ ROUTER

Mà bài: MĐ34-02

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.

Mục tiêu:

- 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.
- Thực hiện các thao tác an toàn với máy tính.

Nội dung:

1. Giới thiệu hệ điều hành IOS

Mục tiêu:

- 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.

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.

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.

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.

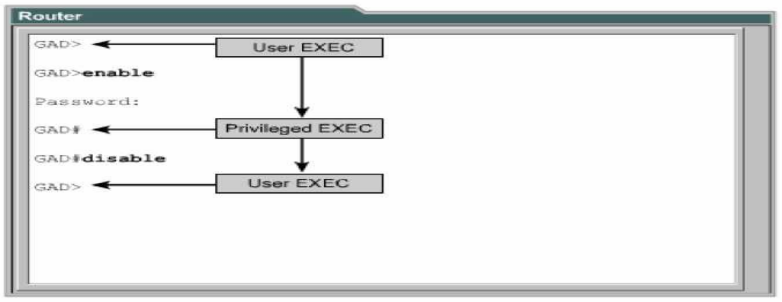
Vì lý do bảo mật nên Cisco IOS chia phiên bản làm việc của EXEC thành hai chế độ là: chế độ EXEC người dùng và chế độ EXEC đặc quyền. Sau đây là các đặc điểm của chế độ EXEC người dùng và chế độ EXEC đặc quyền:

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 Các chế độ cấu hình router

1.4. Các đặc điểm của phần mềm 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 phù 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 2.2: Tên của Cisco IOS

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.

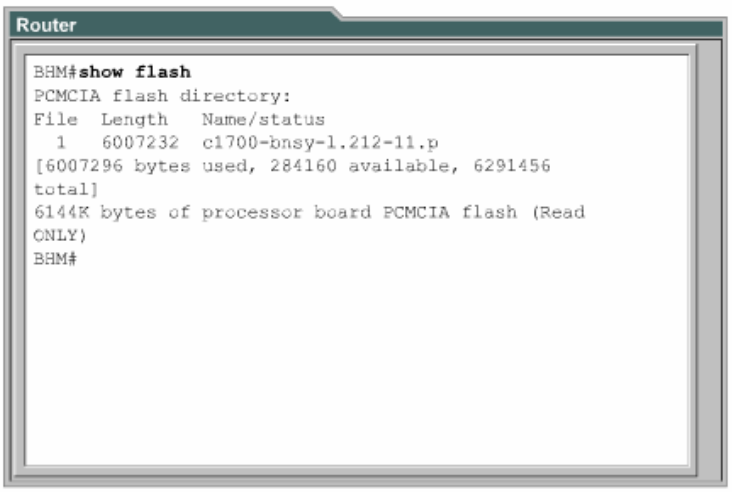
Dòng trên cho biết dung lượng của bộ nhớ chính và bộ nhớ chia sẻ trên router. Có mốt số thiết bị sử dụng một phần DRAM làm bộ nhớ chia sẻ. Tổng hai dung lượng trên là dung lương thật sự của DRAM trên router.

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

GAD#**show flash**

...<*output omitted*>...

1599897 bytes total (10889728 bytes free)



Hình 2.4b: Xem dung lượng bộ nhớ flash

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 2.4a: Router ở chế độ boot ROM

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**.

```
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 2.3: Xem thông tin phần mềm IOS

2. Bắt đầu với router

Mục tiêu:

- Hiểu được quá trình khởi động của 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.

2.1. Khởi động router

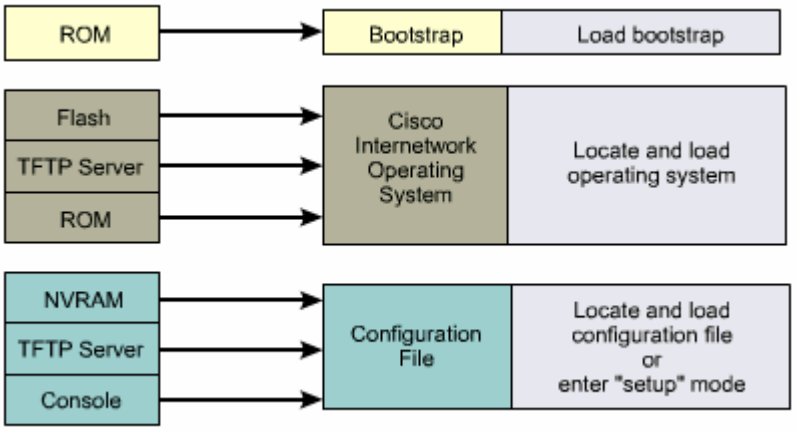
Router khởi động bằng cách tải bootstrap, hệ điều hành và tập tin cấu hình. Nếu router không tìm thấy tập tin cấu hình thí sẽ tự động vào chế độ cài đặt. Khi bạn hoàn tất việc cấu hình trong chế độ cài đặt thì tập tin cấu hình đó sẽ được lưu trong NVRAM.

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 2.5a: 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.

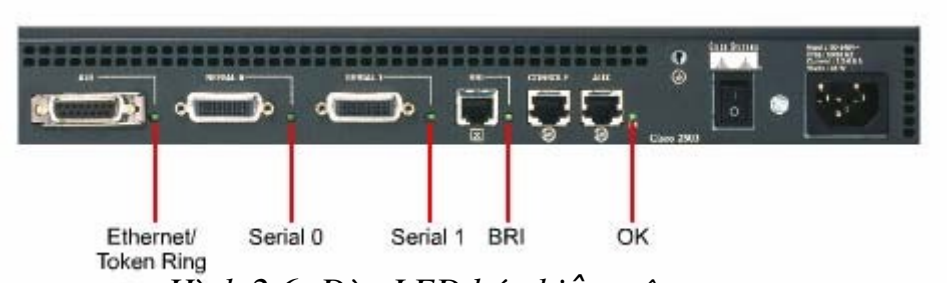
Khi bạn hoàn tất cấu hình trong chế độ cài đặt, bạn sẽ gặp các dòng thông báo như sau:

```
[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]:
```

```
Router#setup
--System Configuration Dialog--
Press Enter at any time to use '?' 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
```

Hình 2.5b: Chế độ cài đặt của router

2.2. Đèn LED báo hiệu trên router



Hình 2.6: Đèn LED báo hiệu trên router

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.

2.3. Khảo sát quá trình khởi động của router

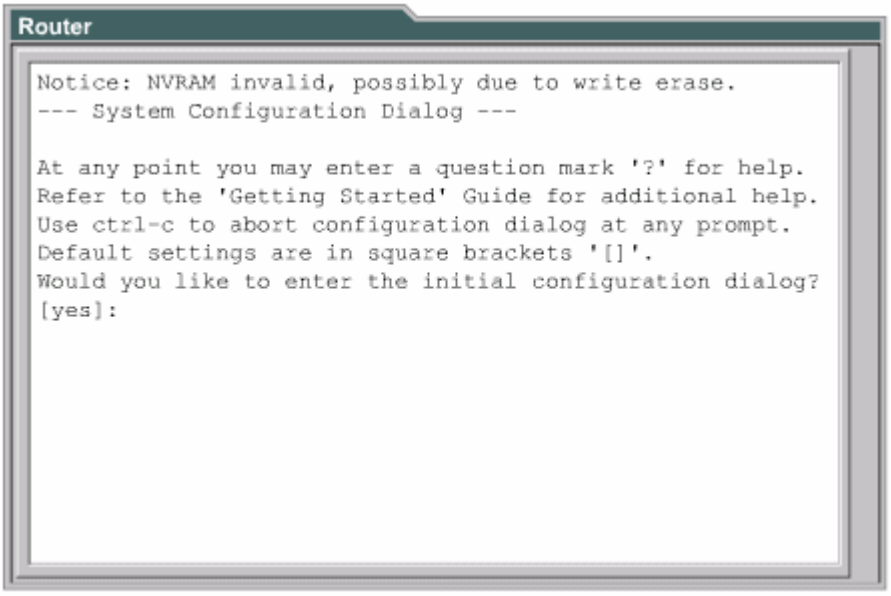
Ví dụ ở hình 2.7a cho thấy nội dung các thông điệp được hiển thị trên màn hình console trong suốt quá trình khởi động của router. Các thông tin này sẽ khác nhau tuỳ theo các loại cổng có trên router và tuỳ theo từng phiên bản Cisco IOS. Do đó hình 2.7a chỉ là một ví dụ để tham khảo chứ không pản ánh chính xác toàn bộ những gì được hiện thị.

Router

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

Notice: NVRAM invalid, possibly due to write erase.

F3: 5797928+162396+258800 at 0x3000060

Restricted Rights Legend

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

Hình 2.7a: Thông tin hiển thị trong quá trình khởi động router

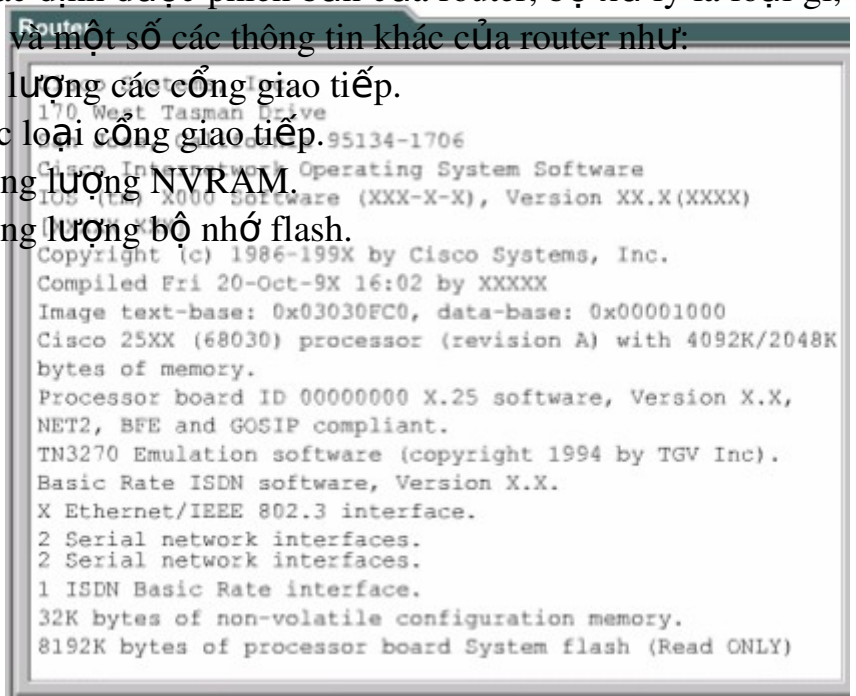
Trong hình 2.7b, câu "VNRAM invalid, possibly due to write erase" cho biết router này chưa được cấu hình hoặc là NVRAM đã bị xoá. Thông thường khi router đã được cấu hình thì tập tin cấu hình được lưu trong NVRAM, sau đó ta phải cấu hình thanh ghi để router sử dụng tập tin cấu hình này. Giá trị mặc định 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 2.7b: Thông tin hiển thị trong quá trình khởi động router

Dựa vào thông tin như hình 2.7c, 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.



Hình 2.7c: Thông tin hiển thị trong quá trình khởi động router

2.4. 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.

2.5. 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.

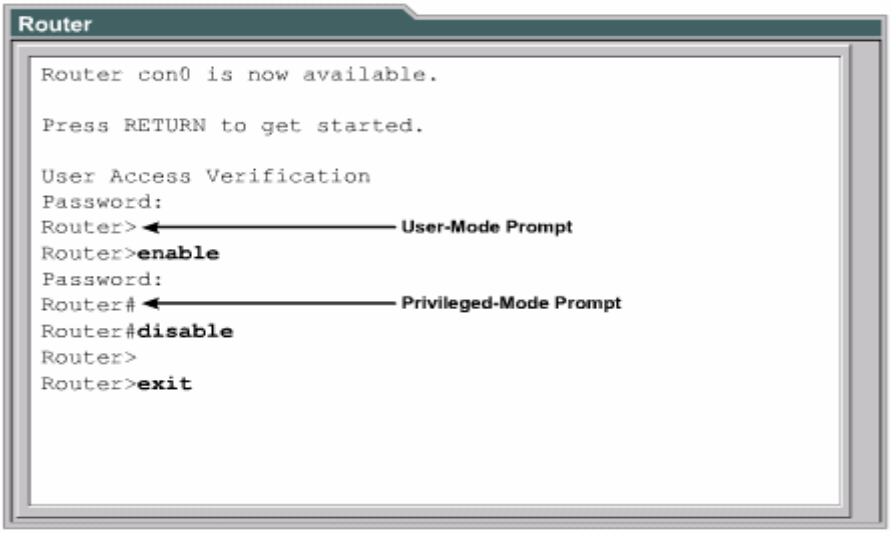
Mức EXEC đặc quyền: bao gồm tất cả các câu lệnh để cấu hình router.

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.

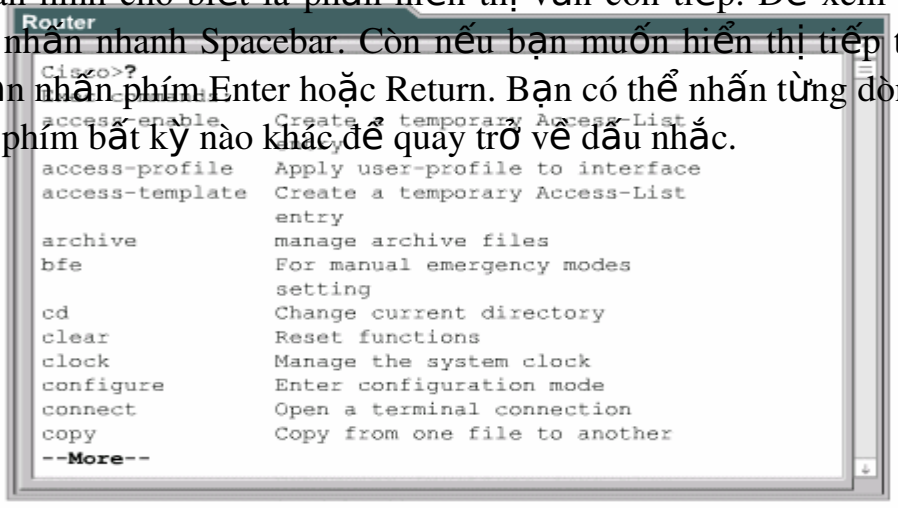
Từ chế độ EXEC đặc quyền, bạn gõ disable hoặc exit để trở về chế độ EXEC người dùng. Để trở về chế độ EXEC đặc quyền từ chế độ cấu hình toàn cục, bạn dùng lệnh exit hoặc Ctrl-Z. Lệnh Ctrl-Z có thể sử dùng để trở về ngay chế độ EXEC đặc quyền từ bất kỳ chế độ cấu hình riêng biệt nào.



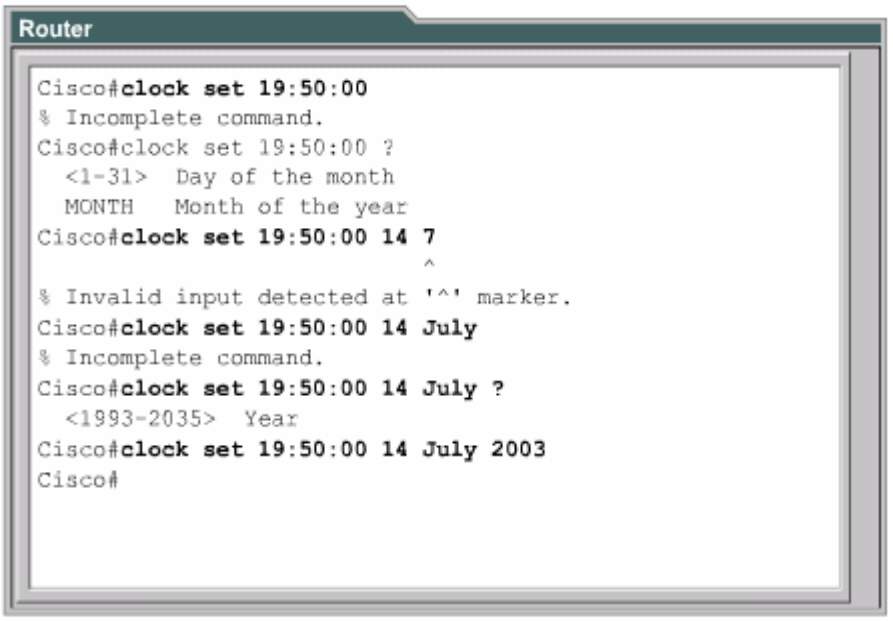
Hình 2.8: Các chế độ truy cập router

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 2.9a: Danh sách lệnh sử dụng ở chế độ EXEC người dùng



Hình 2.9b: Cài đặt đồng hồ cho router

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 2.9b.
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 (^{A}) thì có nghĩa là câu lệnh đã bị nhập sai. Vị trí của dấu (^{A}) sữ cho biết vị trí mà câu lệnh từ đầu cho tới vị trí mà dấu (A) 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.

2.7. 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 2.10a* 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

Hình 2.10a Tổ hợp phím hỗ trợ soạn thảo lệnh trong router

Khi soạn thảo câu lệnh, màn hình sẽ cuộn ngang khi câu lệnh dài quá một hàng. 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 Hình 2.10b là ví dụ khi một câu lệnh dài quá một hàng. 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 2.10b: Câu lệnh dài quá một hàng

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 (ị). 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
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

2.9. 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 (A). Dấu báo lỗi (A) 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 "A" 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>.

2.10. 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 những 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.

BÀI 3: CẤU HÌNH ROUTER
Mà bài: MĐ34-03

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.

Mục tiêu:

- 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.
- 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.
- Thực hiện các thao tác an toàn với máy tính.

Nội dung:

1. Cấu hình router

Mục tiêu:

- 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.

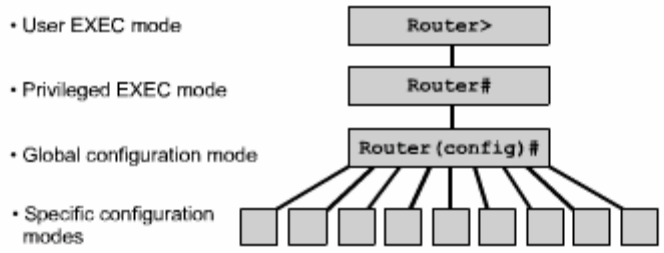
1.1. Chế độ giao tiếp dòng lệnh CLI

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:

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

Router # configure terminal
Router(config)#



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: Chế độ giao tiếp dòng lệnh CLI

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.

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).

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**:

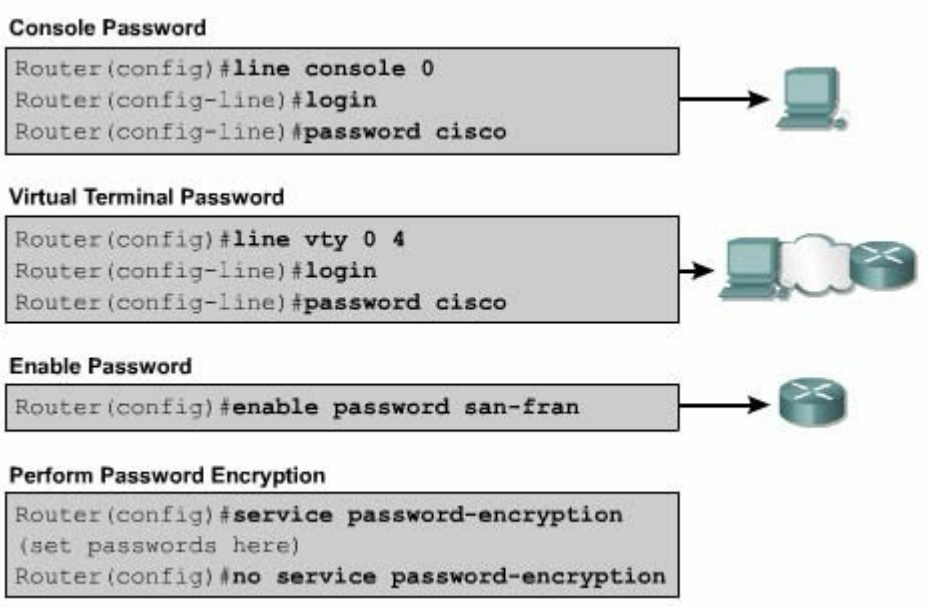
Router(config)#**enable password** <password>

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 mã **enable secret** thì sử dụng một thuật toán mã hoá rất mạnh là MD5



Hình 3.2: Đặt mật mã cho router

1.4. Kiểm tra bằng 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.

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.

Router

```
LAB_A#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(9),
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Mon 24-Jan-00 22:06 by bettyl
Image text-base: 0x030387D0, data-base: 0x00001000

ROM: System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE
BOOTFLASH: 3000 Bootstrap Software (IGS-RXBOOT), Version
10.2(8a), RELEASE SOFTWARE (fc1)

LAB_A uptime is 25 minutes
System restarted by reload
System image file is "flash:c2500-d-l_120-9.bin"
cisco 2500 (68030) processor (revision D) with
8192K/2048K bytes of memory.
Processor board ID 02001682, with hardware revision
00000000
Bridging software.
X.25 software, Version 3.0.0.
2 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read ONLY)
Configuration register is 0x2102
LAB_A#show flash
System flash directory:
File  Length   Name/status
  1   6888660  c2500-d-l_120-9.bin
[6888724 bytes used, 1499884 available, 8388608 total]
8192K bytes of processor board System flash (Read ONLY)
Configuration register is 0x2102
LAB_A#show flash
System flash directory:
File  Length   Name/status
  1   6888660  c2500-d-l_120-9.bin
[6888724 bytes used, 1499884 available, 8388608 total]
8192K bytes of processor board System flash (Read ONLY)
LAB_A#show users
    Line     User      Host(s)            Idle Location
*  0 con 0             idle                 00:00:00

LAB_A#
```

Hình 3.3: Các lệnh kiểm tra thông tin trên router

1.5. Cấu hình cổng serial

Chúng ta có thể 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**

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.

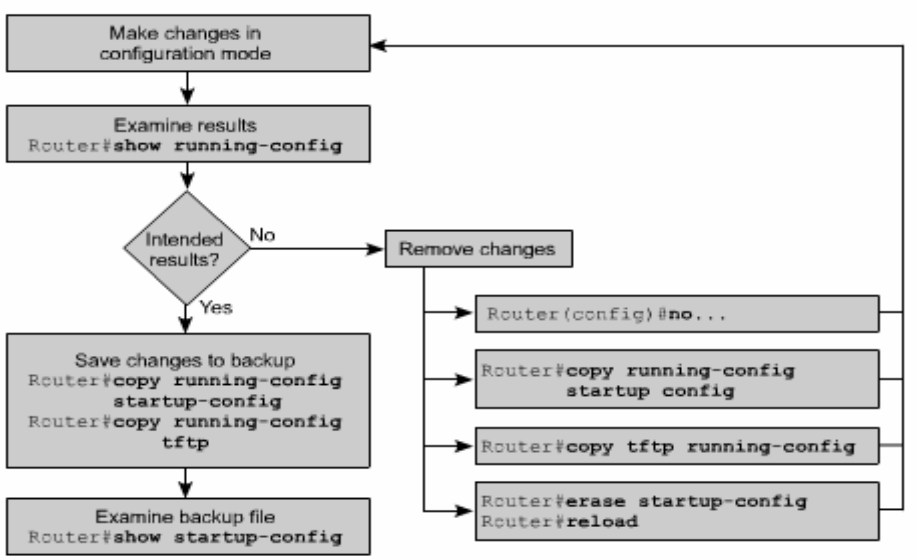
Khởi động lại router với tập tin cấu hình nguyên thuỷ trong NVRAM.

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 3.4: các lệnh liên quan đến tập tin cấu hình trong router

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:

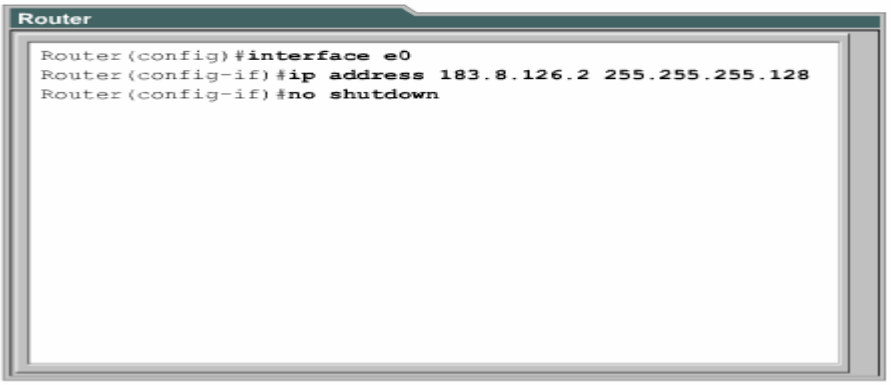
Vào chế độ cấu hình toàn cục.

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 3.5: Cấu hình cổng Ethernet

2. Hoàn chỉnh cấu hình router

Mục tiêu:

- 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.

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

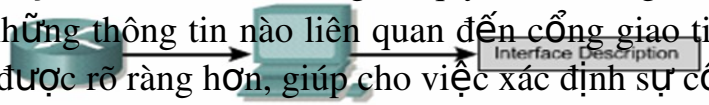
Trong một tổ chức việc phát các quy định dành cho các tập tin cấu hình là rất cần thiết. Từ đó ta có thể kiểm soát được các tập tin nào càn bảo trì, lưu các tập tin ở đâu và như thế nào.

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.

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




```
Tokyo(config)#interface e 0

Tokyo(config-if)#description Engineering LAN, Bldg. 18
```

Hình 3.6: Câu chú thích cho cổng giao tiếp

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 đặc 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:

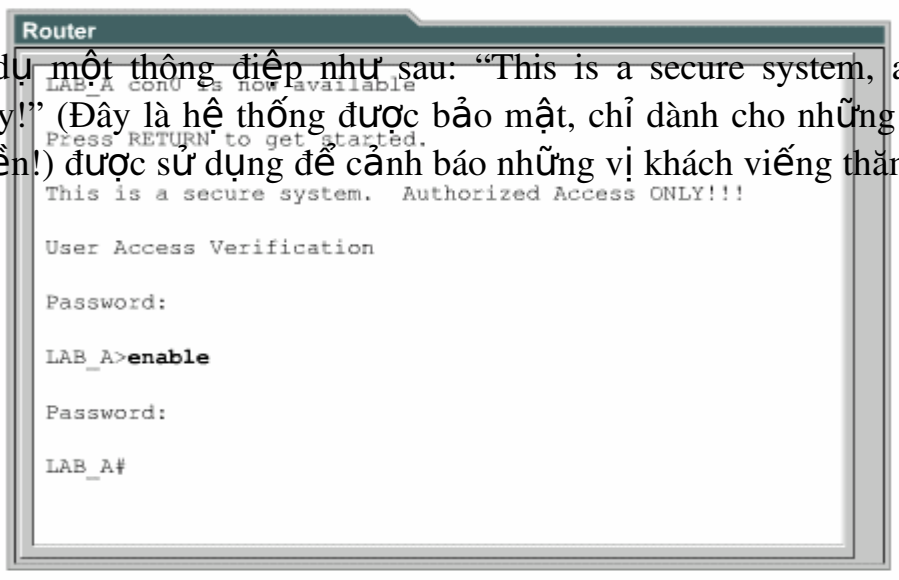
Interface Ethernet 0
Description LAN Engineering, Bldg.2
Interface serial 0
Description ABC network 1, circuit 1

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.

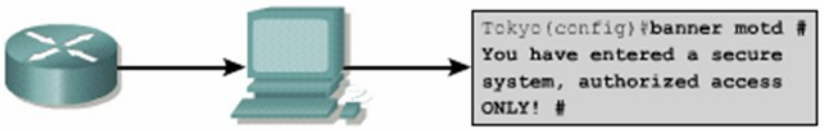
Tất cả mọi người đều có thể nhìn thấy thông điệp đăng nhập. Cho nên bạn nên dùng các thông điệp mạng tính cảnh báo, thu hút sự chú ý. Còn những thông điệp để "chào đón" mọi người đăng nhập vào router là không thích hợp lắm.

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 3.7: Thông điệp đăng nhập router

2.5. Cấu hình thông điệp đăng nhập (MOTD)



Hình 3.8: Cấu hình thông điệp đăng nhập cho router

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**.

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.

Dưới đây là ví dụ cấu hình bảng host trên 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**

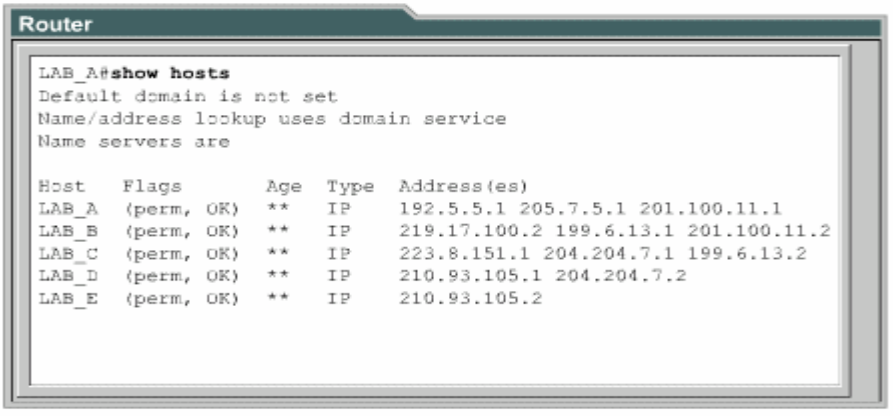
Router(config)#**ip host Denver 10.202.8.1**

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 đây 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 3.8: Thông tin bảng host

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.

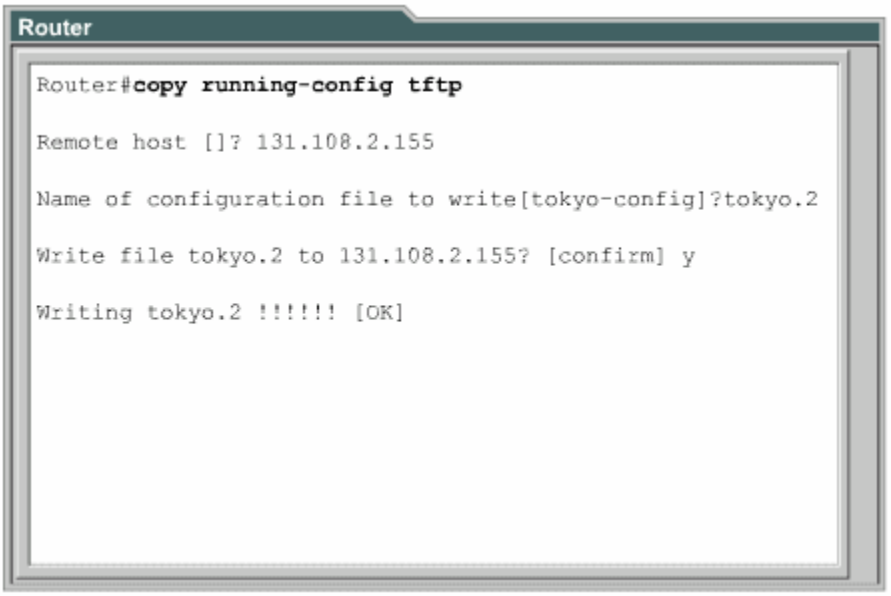
Chúng ta cần lưu dự phòng các tập tin cấu hình để sử dụng trong

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.

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:

1. Nhập lệnh **copy running-config tftp**.
2. Nhập địa chỉ IP của máy mà chúng ta sẽ lưu tập tin cấu hình lên đó.
3. Nhập tên tập tin.
4. Xác nhận lại câu lệnh bằng cách trả lời "yes"



Hình 3.9a: Thay đổi tập tin cấu hình

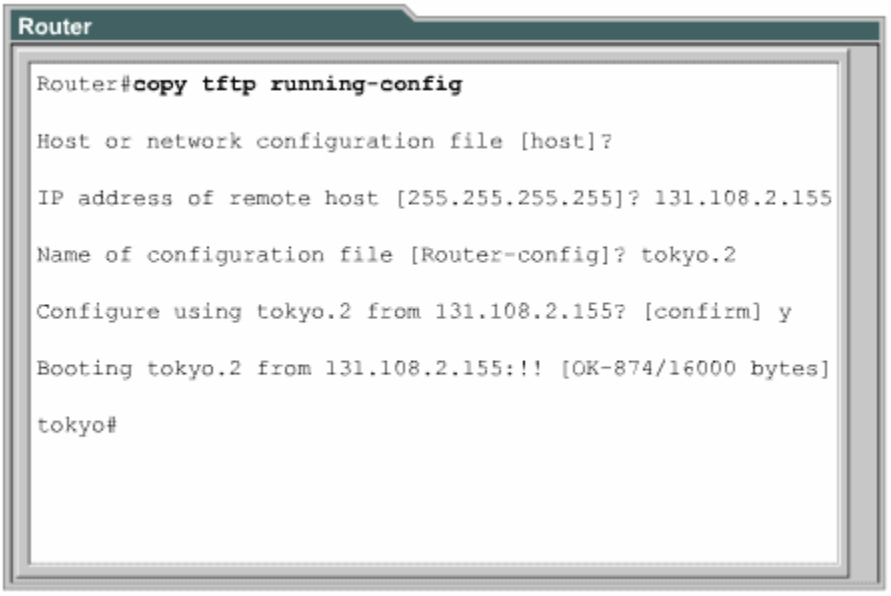
Chúng ta có thể sử dụng tập tin cấu hình lưu trên server mạng để cấu hình cho router.

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 3.9b: Thay đổi tập tin cấu hình

Bài tập và sản phẩm thực hành bài 34.3

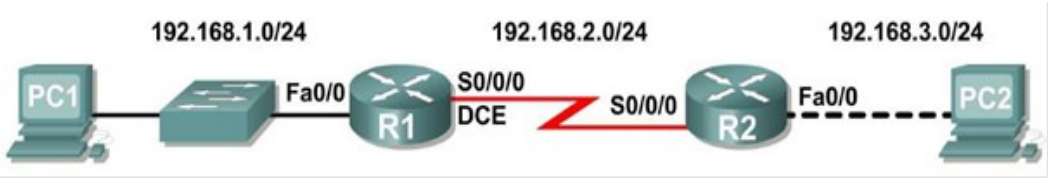
Kiến thức:

Câu 1: Trình bày đặc điểm các chế độ giao tiếp dòng lệnh CLI (*Command Line Interface)* của router?

Câu 2: Nêu các điểm quan trọng khi cấu hình router cơ bản ?

Kỹ năng:

Bài tập ứng dụng: Thực hiện cấu hình cho các router trong mô hình mạng bên dưới ?



- Cấu hình gán IP address cho Interface của Router
- Cấu hình cho phép kết nối tới Router từ xa thông qua Telnet
- Cấu hình bảo mật truy cập router
- Cấu hình các tham số cơ bản khác cho router
- Xem xét các thông số cơ bản của router bằng các lệnh "show"
- Thời gian:….. giờ (kể cả thời gian chuẩn bị và cấu hình)

CHỈ DẪN ĐỐI VỚI HỌC SINH THỰC HIỆN BÀI TẬP ỨNG DỤNG

1. Kết nối cáp cho Router, PC, Switch như hình vẽ.
2. Thực hiện Console tới router bằng cáp console và phần mềm Hyper Terminal.
3. Thực hiện xóa cấu hình khởi động của router và khởi động lại router. Sau khi khởi động lại Router, chọn "NO" để vào User mode.
4. Cấu hình các thông số cơ bản cho Router.
5. Gán IP address cho các PC.
6. Kiểm tra cấu hình, kết nối.
7. Xóa cấu hình startup-config và khởi động lại Router để kết thúc bài thực hành.
8. Tổng điểm và kết cấu điểm của các bài như sau:

    Tổng số điểm tối đa cho bài: 100 điểm, kết cấu như sau:

    a, Điểm ngoại dạng khách quan: Tổng cộng 70 điểm

    b, Điểm tuân thủ các qui định: 30 điểm

- Thời gian thực hiện bài tập vượt quá 25% thời gian cho phép sẽ không được đánh giá.

- Thí sinh phải tuyệt đối tuân thủ các qui định an toàn lao động, các qui định của phòng thực hành, nếu vi phạm sẽ bị đình chỉ thực tập

BÀI 4: CẬP NHẬT THÔNG TIN TỪ CÁC THIẾT BỊ KHÁC
Mà bài: MĐ34-04

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.

Mục tiêu:

- Bật và tắt CDP.
- Sử dụng lệnh *show cdp neighbors*.
- Xác định các thiết bị lân cận kết nối vào các cổng.
- Ghi nhân thông tin và địa chỉ mạng cua các thiết bị lân cận.
- Thiết lập và kiểm tra kết nối Telnet.

- Kết thúc và tạm ngưng một phiên Telnet.
- Thực hiện các kiểm tra kết nối khác.
- Xử lý sự cố với các kết nối từ xa.
- Thực hiện các thao tác an toàn với máy tính.

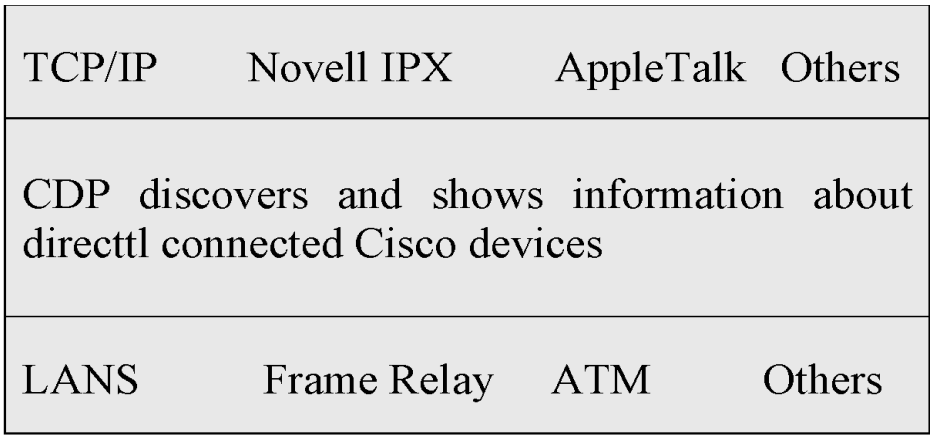
Nội dung:

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

Mục tiêu:

- Bật và tắt CDP.
- Sử dụng lệnh *show cdp neighbors*.
- Xác định các thiết bị lân cận kết nối vào các cổng.
- Ghi nhân thông tin và địa chỉ mạng cua các thiết bị lân cận.

1.1. Giới thiệu về CDP



Hình 4.1

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.

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.

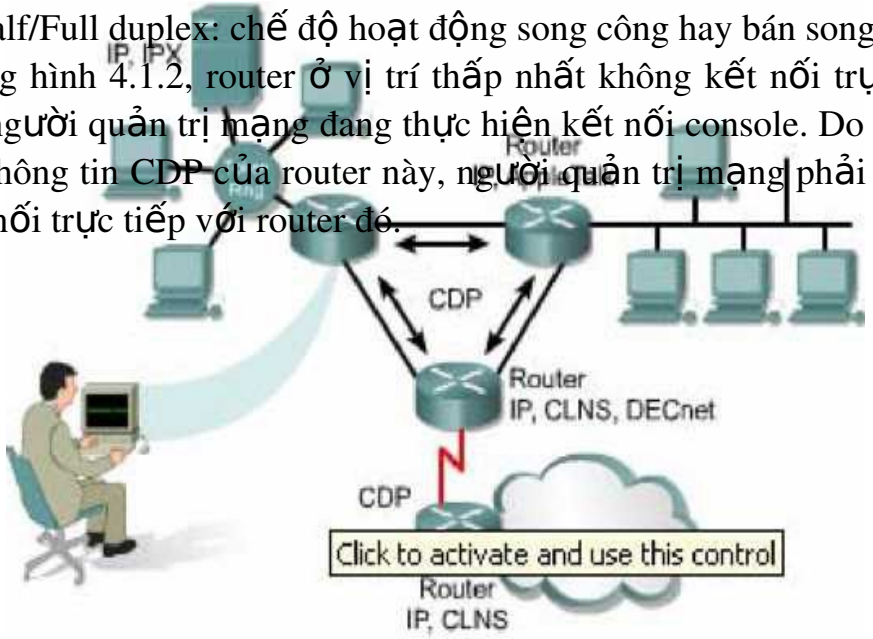
Port ID: chỉ số danh định (ID) của cổng trên thiết bị láng giềng kết nối vào thiết bị của chúng ta.

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 4.2

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
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

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 4.3a

Router

```
CDP Version 1
Rt3#show cdp
Global CDP information:
   Sending CDP packets every 60 seconds
   Sending a holdtime value of 180 seconds
Rt3#
CDP Version 2
Rtl#show cdp
Global CDP information
   Sending CDP packets every 60 seconds
   Sending a holdtime value of 180 seconds
   Sending CDPv2 advertisments is enabled
Rtl#
```

Hình 4.3b

Router

```
Rt1#show cdp entry Rt2
-------------------
Device ID: Rt2
Entry address(es):
IP address: 192.168.2.2
Platform: cisco 2621, Capabilities: Router
Interface: Serial0/0, PortID(outgoing port): Serial0/0
Holdtime: 139 sec

Version:
Cisco Internetwork Operating System Software
IOS (tm)C2600 Software(C2600-DO3S-M), Version 12.0(5)TI,
RELEASE
SOFTWARE(fc1)
Copyright(c) 1986-1999 by cisco System, Inc.
Compiled Tue 17-Aug-99 13:18 bycmong
```

Hình 4.3c

Router

```
Rt1#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

Rt1#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
Rt1#
```

Hình 4.3d

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
Rt1      Ser0/0        121     R        2620      Ser0/0
Rt2#
```

Hình 4.3e

Hình 4.1.3e

```
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

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.

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.

```
Rt1
Rtl#show cdp
Global CDP information
   Sending CDP packets every 60 seconds
   Sending a holdtime value of 180 seconds
   Sending CDPv2 advertisements is enabled
Rtl#configure terminal
Enter configuration commands, one per line. End with
 CNTL/Z
Rtl(config)#no cdp run
Rtl(config)#^Z
Rtl#show cdp
%CDP is not enabled
Rtl#configure terminal
Enter configuration commands, one per line. End with
 CNTL/Z
Rtl(config)#cdp run
Rtl(config)#^Z
```

Hình 4.4

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
Debug cdp	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 định cập nhật và thời gian lưu giữ thông tin

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

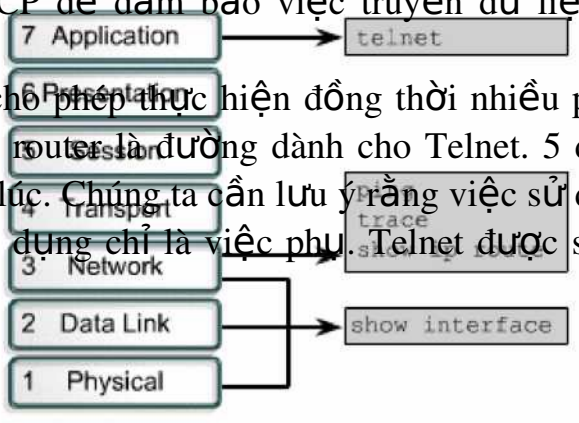
Mục tiêu:

- Thiết lập và kiểm tra kết nối Telnet.
- Kết thúc và tạm ngưng một phiên Telnet.
- Thực hiện các kiểm tra kết nối khác.
- Xử lý sự cố với các kết nối từ xa.

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 4.5

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**.

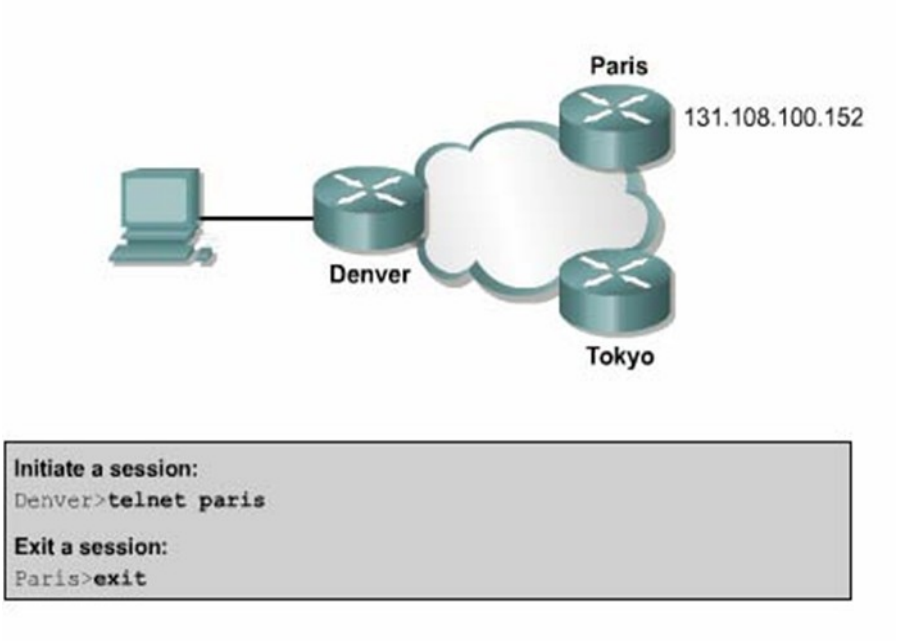
Để thiết lập kết nối Telnet, bạn dùng một trong các lệnh sau:

Denver>**connect paris**

Denver>**paris**

Denver>**131.108.100.152**

Denver>**telnet paris**

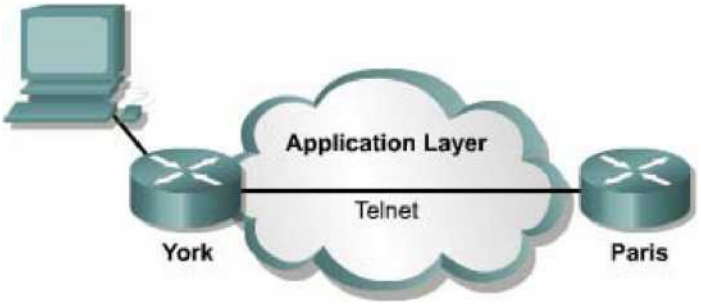


Hình 4.6a

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 4.6b

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**.

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:

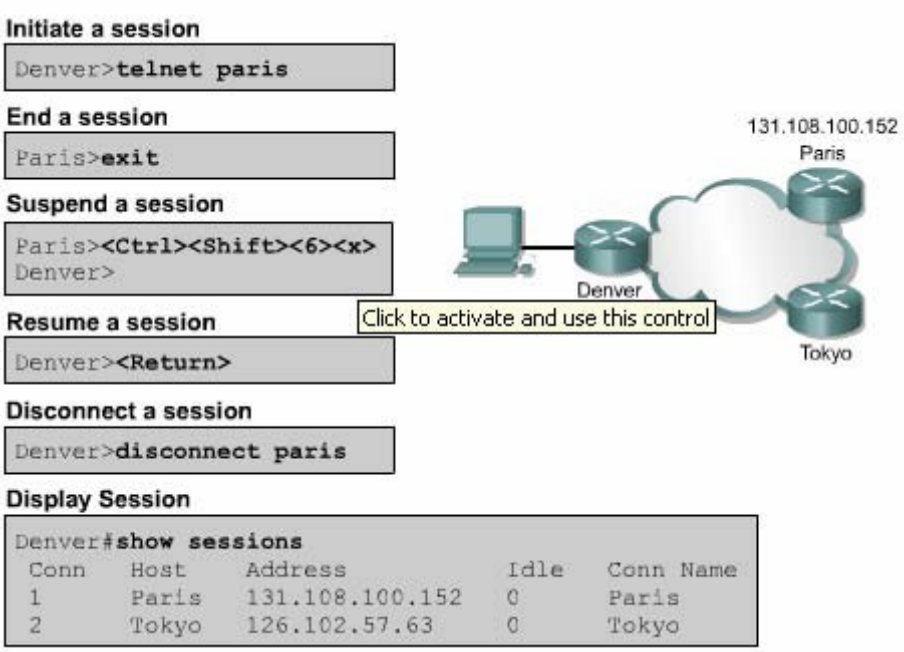
Nhập lệnh disconnect.

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 4.7

2.4. Mở rộng thêm về hoạt động Telnet

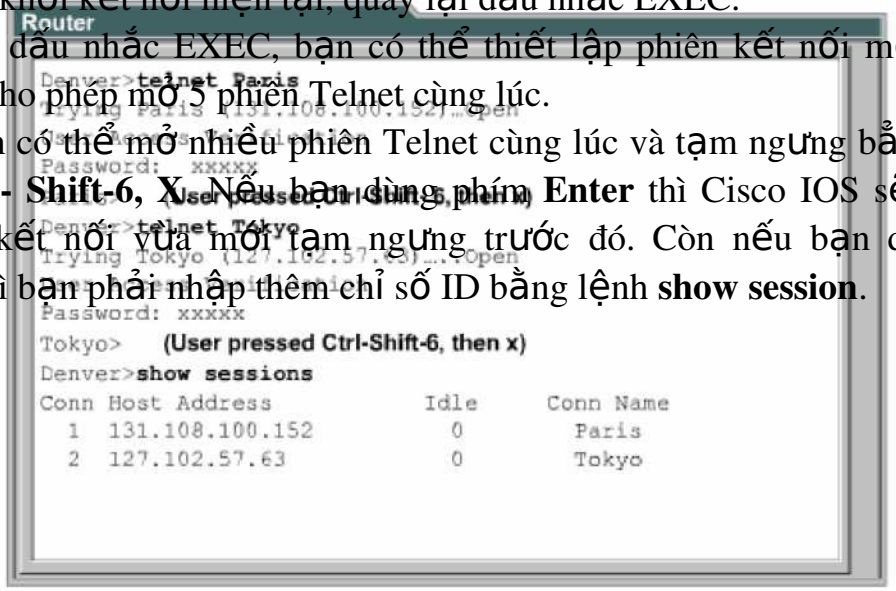
Trên router có thể mở nhiều phiên Telnet cùng lúc. Chúng ta có thể chuyển đổi qua lại giữa các phiên Telnet này. Bạn có thể ấn định số lượng phiên Telnet được phép mở đồng thời trên router bằng lệnh **session limit**.

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**.

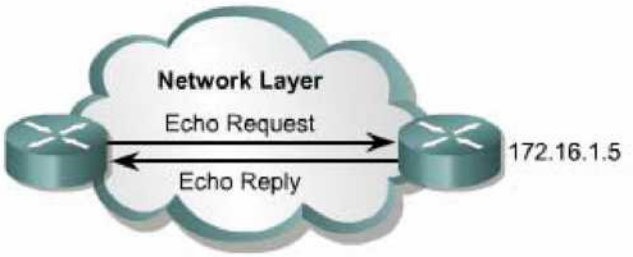


Hình 4.8

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.

Hình 4.9a là ví dụ cho biết phản hồi hành công cho 5 gói gửi đi của lệnh ping 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).

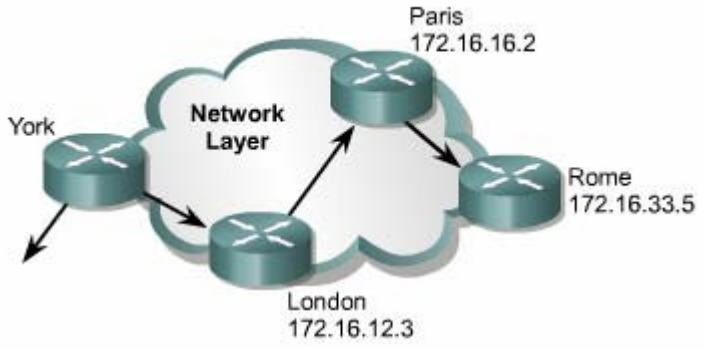



```
Router>ping 172.16.1.5
Type escape sequence to abort.
Sending 5, 100 byte ICMP Echos to 172.16.1.5,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent,
round-trip min/avg/max = 1/3/4 ms
Router>
```

Hình 4.9a

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 4.9b

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.

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.

Bài tập và sản phẩm thực hành bài 34.4

Kiến thức:

Câu 1: Khái niệm CDP ?Trình bày chức năng của các lệnh liên quan đến CDP?

Câu 2:Khái niệm Telnet? So sánh điểm khác nhau giữa VTY (Virtual Terminal) line và TTY (Terminal controller) line ?

Kỹ năng:

Bài tập ứng dụng: Thực hiện cấu hình telnet cho các router. Kết hợp telnet và CDP thu thập thông tin thiết bị trong mô hình mạng bên dưới ?

CHỈ DẪN ĐỐI VỚI HỌC SINH THỰC HIỆN BÀI TẬP ỨNG DỤNG

1. Kết nối các router và dây cáp như hình vẽ.
2. Cấu hình cơ bản cho router.
3. Gán IP cho các router như hình vẽ.
5. Cấu hình telnet.
6. Kiểm tra quá trình kết nối telnet.
4. Kết hợp giao thức telnet và CDP thu thập thông tin thiết bị.
7. Thời gian:….. giờ (kể cả thời gian chuẩn bị và cấu hình)
8. Tổng điểm và kết cấu điểm của các bài như sau:

Tổng số điểm tối đa cho bài: 100 điểm, kết cấu như sau:

a, Điểm ngoại dạng khách quan: Tổng cộng 70 điểm

b, Điểm tuân thủ các qui định: 30 điểm

- Thời gian thực hiện bài tập vượt quá 25% thời gian cho phép sẽ không được đánh giá.

- Thí sinh phải tuyệt đối tuân thủ các qui định an toàn lao động, các qui định của phòng thực hành, nếu vi phạm sẽ bị đình chỉ thực tập

BÀI 5: QUẢN LÝ PHẦN MỀM CISCO IOS

Mà bài: MĐ34-05

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.

Mục tiêu:

- Xác định được router đang ở giai đoạn nào trong quá trình khởi động.
- Xác định các thiết bị Cisco tìm và tải IOS như thế nào.
- Sử dụng các lệnh *boot system*.
- Xác định giá trị thanh ghi cấu hình.
- Mô tả khái quát các tập tin IOS sử dụng và chức năng tương ứng.
- Nắm được nơi nào 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 sử dụng TFTP Server.
- Tải IOS bằng TFTP hoặc Xmodem.
- Kiểm tra tập tin hệ thống bằng các lệnh show.
- Thực hiện các thao tác an toàn với máy tính.

Nội dung:

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

Mục tiêu:

- Xác định được router đang ở giai đoạn nào trong quá trình khởi động.
- Xác định các thiết bị Cisco tìm và tải IOS như thế nào.
- Sử dụng các lệnh *boot system*.
- Xác định giá trị thanh ghi cấu hình.

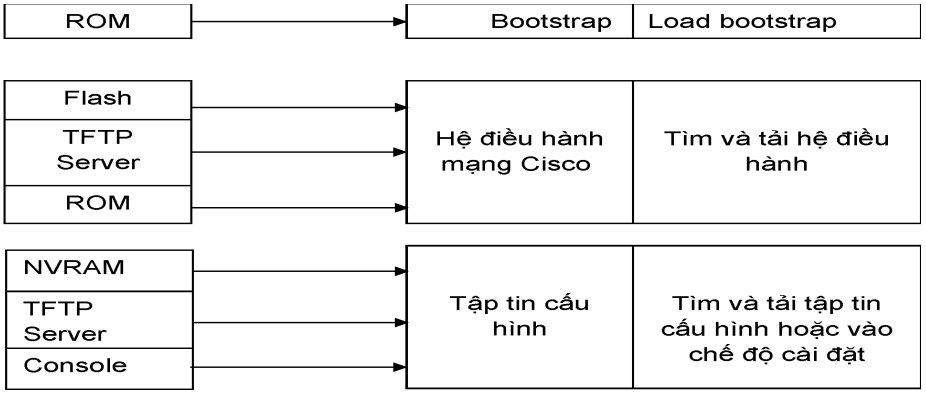
1.1. Các giai đoạn khởi động router khi bắt đầu bật điện

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.



1.2. Thiết bị Cisco tìm và tải như thế nào

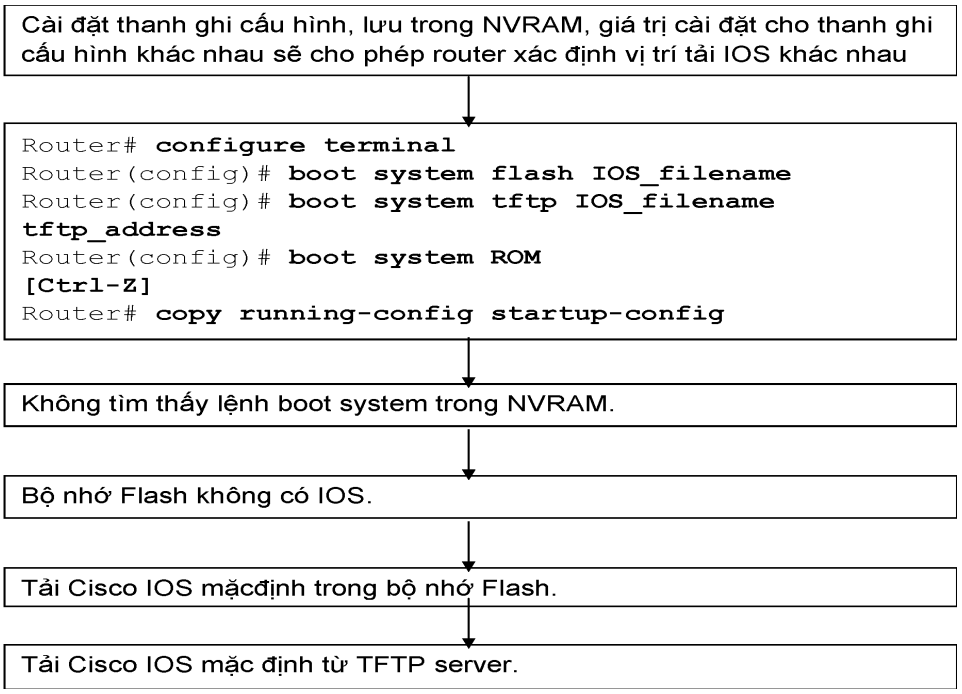
Nguồn mặc định tải phần mềm Cisco IOS thì khác nhau tuỳ theo phiên bản phần cứng của thiết bị, nhưng hầu hết các router đều tìm lệnh boot system lưu trong NVRAM. Phần mềm Cisco IOS có thể được tải từ nhiều nguồn khác nhau. Những nguồn này chúng ta có thể cấu hình hoặc router sẽ sử dụng quá trình tìm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



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 bit 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 **config-register** để thay đổi giá trị cho thanh ghi, ta chỉ cần đổi giá trị của số hex cuối

```
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], REL
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
EASE SOFTWARE fc1)
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.
FastEthernet/IEEE 802.3 interface(s)
Low-speed serial (sync/async) network interface(s)
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.

2. Quản lý tập tin hệ thống Cisco

Mục tiêu:

- Mô tả khái quát các tập tin IOS sử dụng và chức năng tương ứng.
- Nắm được nơi nào 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 sử dụng TFTP Server.
- Tải IOS bằng TFTP hoặc Xmodem.
- Kiểm tra tập tin hệ thống bằng các lệnh show.

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.

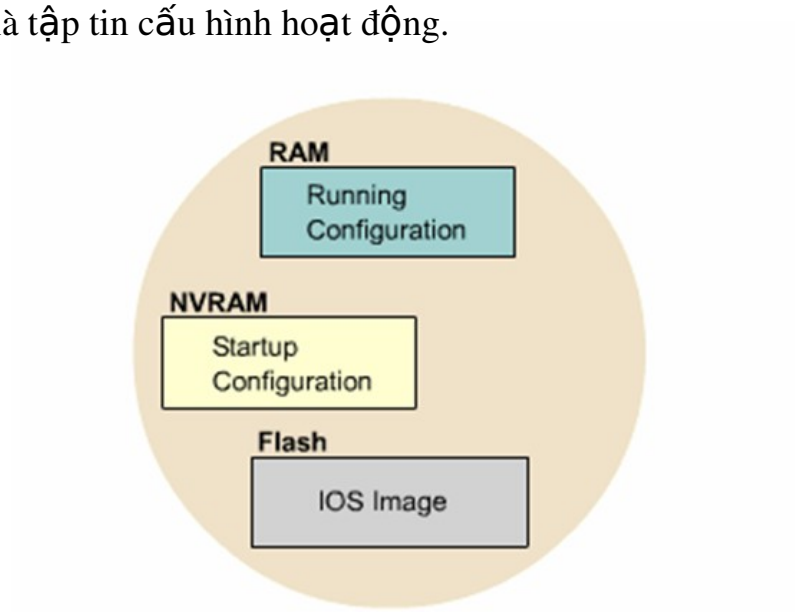
Hệ điều hành được sử dụng cho hầu hết các thiết bị Cisco là hệ điều hành liên mạng Cisco, gọi tắt là Cisco IOS (Internetwork Operating System). Phần mềm Cisco IOS cho phép thiết bị thực hiện các chức năng của router hay switch. Một tập tin IOS khoảng vài megabyte.

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 5.1a: Các tập tin hệ thống Cisco

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 5.1b* 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 5.1b

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 5.1c

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.

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:

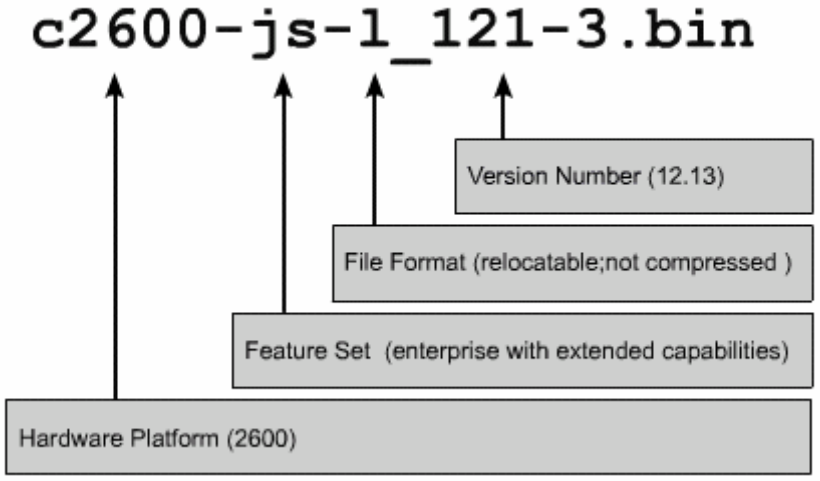
Cơ bản: các đặc tính dành cho từng phiên bản phần cứng, ví dụ: IP, IP/FW.

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.



Hình 5.2: Các thành phần của tập tin IOS

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.

2.3. Quản lý tập tin cấu hình bằng 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.

```
GAD#copy running-config tftp
Address or name of remote host
[]?192.168.119.20
Destination filename [GAD-confg]?
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
624 bytes copied in 7.05 secs
GAD#
```

```
GAD#copy tftp flash
Address or name of remote host []?192.168.119.20
Source filename []? C2600-js-l_121-3.bin
Destination filename [C2600-js-l_121-3.bin]?
Accessing tftp://192.168.119.20/ C2600-js-l_121-3.bin
Erase flash: before copying? [confirm]
Erasing the flash file system will remove all files
Continue? [confirm]
Erasing device eeeeee…eeeeeeeeeeeee…erased
Loading C2600-js-l_121-3.bin from 192.168.119.20 (via
FastEthernet 0/0): !!!!!!!!!!!!!!…!!!!!!!!!!!!!!!!!!
Verifying Check sum ............OK
[OK-8906589 bytes]
8906589 bytes copied in 277.45 secs
GAD#
```

Hình 5.3a: Quản lý tập tin bằng TFTP Server

Hình 5.3b: Quản lý tập tin bằng TFTP Server

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 thêm 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.

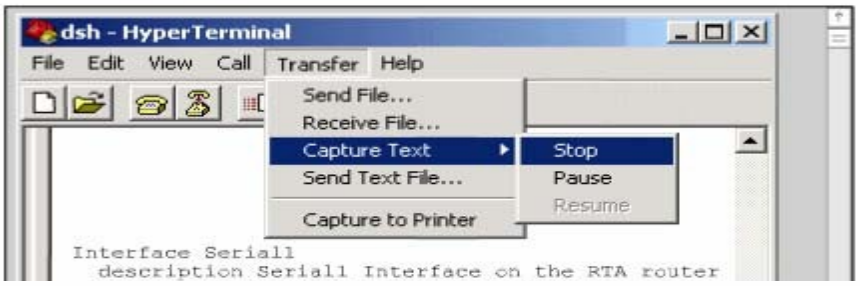
Chọn tên của tập tin cấu hình mà bạn cần chép lên router.

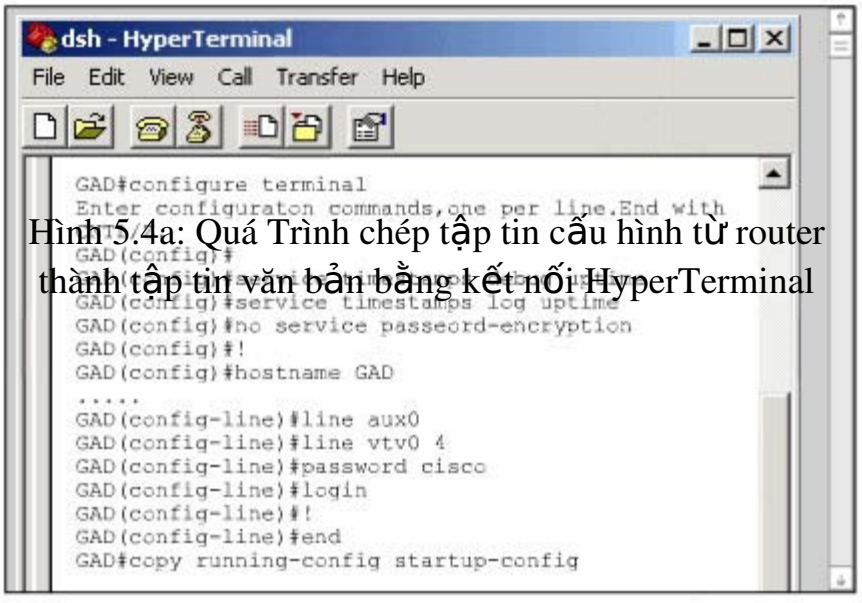
Từng dòng trong tập tin cấu hình sẽ được nhập vào y như lúc bạn gõ lệnh đó vậy.

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 5.4a: Quá Trình chép tập tin cấu hình từ router thành tập tin văn bản bằng kết nối HyperTerminal

Hình 5.4b: Quá trình chép tập tin cấu hình vào router bằng kết nối HyperTerminal

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 chữ "e" trong suốt quá trình xoá flash.

.

```
GAD#copy tftp flash
Address or name of remote host []?192.168.119.20
Source filename []? C2600-js-l_121-3.bin
Destination filename [C2600-js-l_121-3.bin]?
Accessing tftp://192.168.119.20/ C2600-js-l_121-3.bin
Erase flash: before copying? [confirm]
Erasing the flash file system will remove all files
Continue? [confirm]
Erasing device eeeeee…eeeeeeeeeeeee…erased
Loading C2600-js-l_121-3.bin from 192.168.119.20 (via
FastEthernet 0/0): !!!!!!!!!!!!!!…!!!!!!!!!!!!!!!!!!!
Verifying Check sum .............OK
[OK-8906589 bytes]
8906589 bytes copied in 277.45 secs
GAD#
```

Hình 5.5:Quản lý tập tin bằng TFTP Server

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

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**

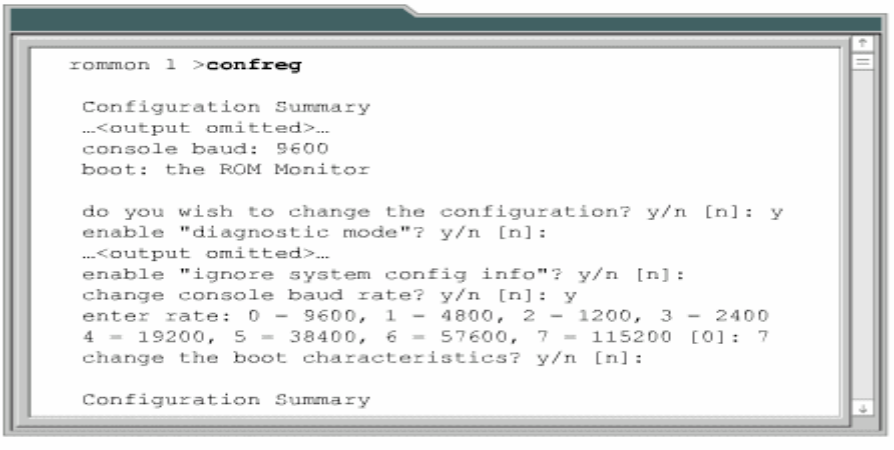
Nếu router khởi động bình thường thì có 2 vấn đề bạn cần kiểm tra xem tại sao router lại khởi động vào chế độ ROMmon mà không khởi động từ IOS trong flash. Đầu tiên, bạn dùng lệnh **show version** để kiểm tra giá trị của thanh ghi cấu hình xem có đúng giá trị mặc định hay không. Nếu giá trị thanh ghi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



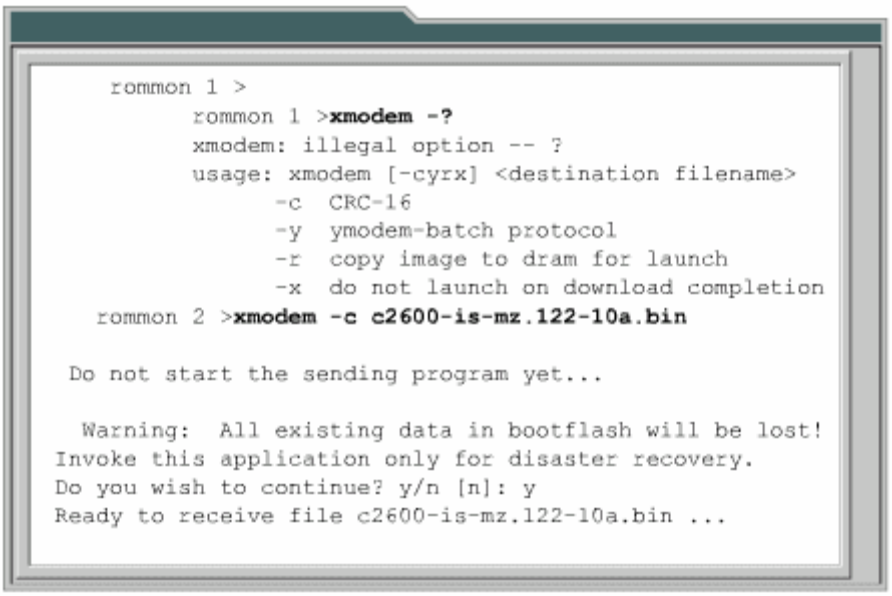
Hình 5.6a

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-i-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 5.6b: 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.

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.

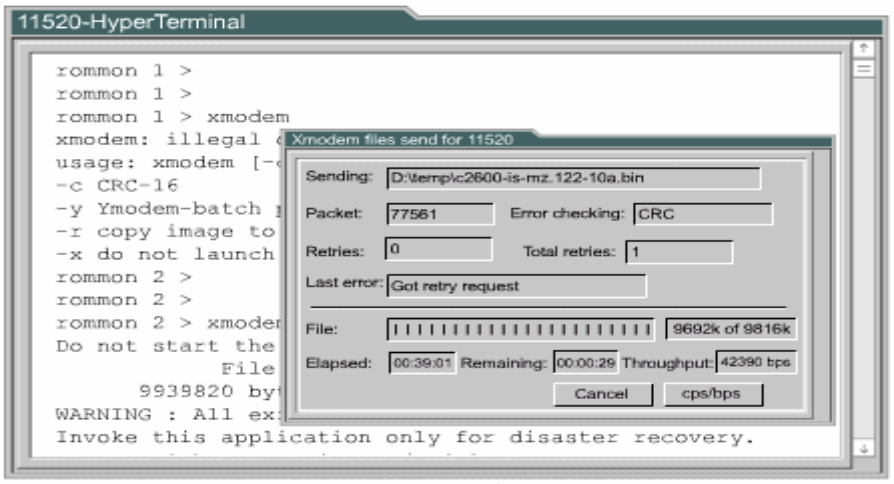
IP_SUBNET_MASK:subnet mask cho cổng LAN.

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 5.7: 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.

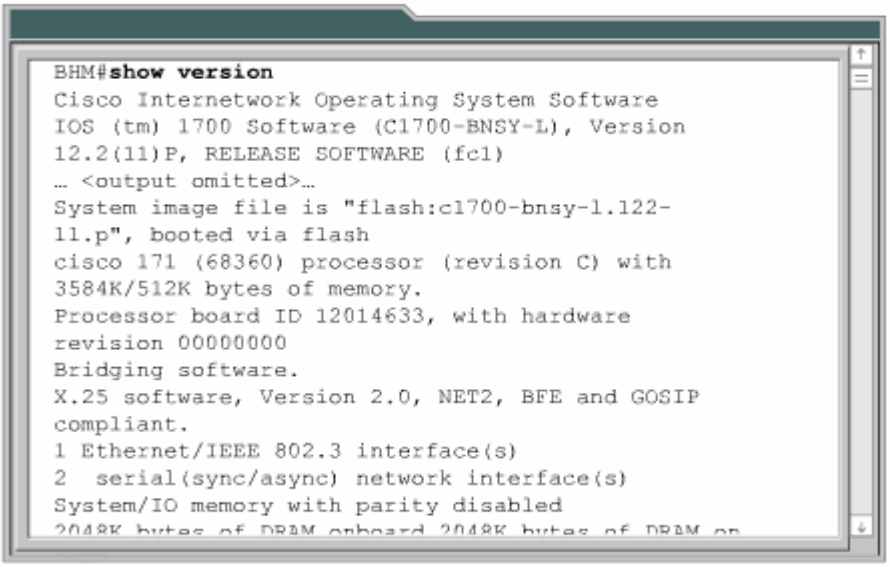
2.8. Kiểm tra tập tin hệ thống

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.



Hình 5.7: Kiểm tra tập tin hệ thống

Bài tập và sản phẩm thực hành bài 34.5

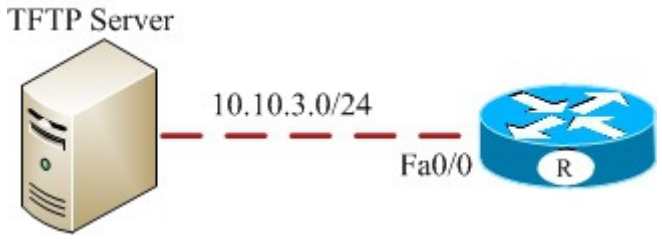
Kiến thức:

Câu 1: Trình bày các giai đoạn trong quá trình khởi động router?

Câu 2: Quá trình router tìm và tải IOS như thế nào ?

Kỹ năng:

Bài tập ứng dụng: Cho mô hình mạng bên dưới. Thực hiện Backup và Recovery các file hệ thống qua TFTP Server.



CHỈ DẪN ĐỐI VỚI HỌC SINH THỰC HIỆN BÀI TẬP ỨNG DỤNG

1. Kết nối Router, PC
   - Kết nối console để cấu hình Router.
   - Kết nối cổng mạng của máy tính với cổng Fa0/0 của Router.
2. Thực hiện gán IP address, subnetmask, default gateway cho PC, gán IP address cho interface của router (nối với PC).
3. Cấu hình các thông số cơ bản cho router.
4. Chạy Cisco TFTP Server trên PC.
5. Kiểm tra kết nối giữa router và TFTP Server.
6. Thực hiện backup file cấu hình của router.
7. Recovery file cấu hình.
8. Kiểm tra phiên bản IOS hiện tại của router. Thực hiện backup file IOS.
9. Recovery IOS.
10. Thời gian:….. giờ (kể cả thời gian chuẩn bị và cấu hình)
11. Tổng điểm và kết cấu điểm của các bài như sau:

    Tổng số điểm tối đa cho bài: 100 điểm, kết cấu như sau:

    a, Điểm ngoại dạng khách quan: Tổng cộng 70 điểm

    b, Điểm tuân thủ các qui định: 30 điểm

- Thời gian thực hiện bài tập vượt quá 25% thời gian cho phép sẽ không được đánh giá.

- Thí sinh phải tuyệt đối tuân thủ các qui định an toàn lao động, các qui định của phòng thực hành, nếu vi phạm sẽ bị đình chỉ thực tập

BÀI 6: ĐỊNH TUYẾN VÀ CÁC GIAO THỨC ĐỊNH TUYẾN
Mà bài: MĐ34-06

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.

Mục tiêu:

- 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.
- Phân biệt giao thức định tuyến theo vecto khoảng cách.
- Nhận biết giao thức định tuyến theo trạng thái đường liên kết.
- Mô tả đặc điểm cơ bản của giao thức định tuyến thông dụng.
- Phân biệt giao thức định tuyến nội bộ.
- Phân biệt giao thức định tuyến ngoại vi.
- Thực hiện các thao tác an toàn với máy tính.

Nội dung:

1. Giới thiệu về định tuyến tĩnh

Mục tiêu:

- 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.

1.1. Giới thiệu về định tuyến tĩnh

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.

1.2. Hoạt động của định tuyến tĩnh.

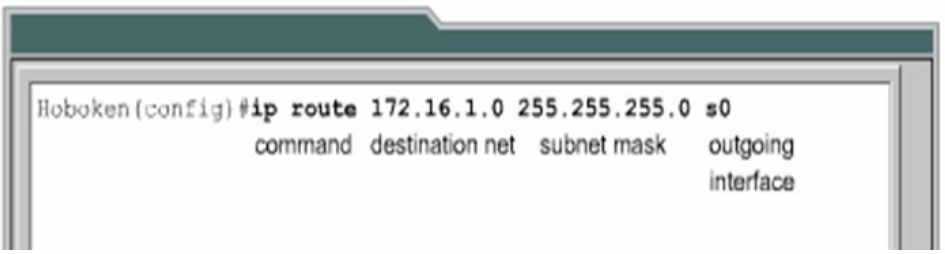
Hoạt động của định tuyến tĩnh có thể chia ra làm 3 bước như sau:

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 .

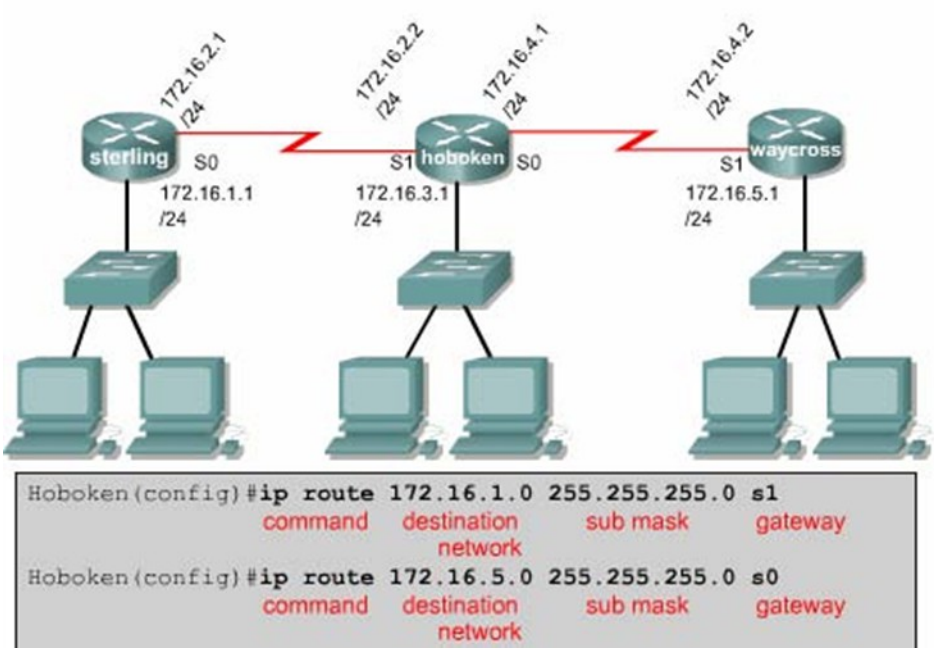
Người quản trị mạng cấu hình đường cố định cho router bằng lệnh iproute. Cú pháp của lệnh iproute như hình 6.1a:



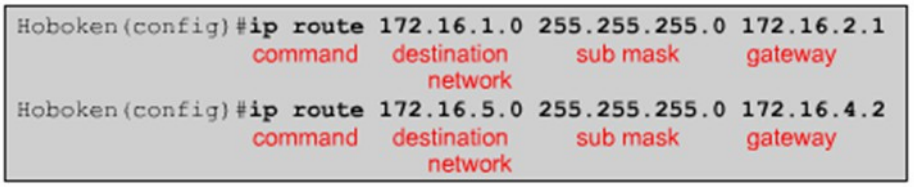
Hình 6.1a

Trong 2 hình 6.1b và 6.1.c là 2 câu lệnh 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 6.1b,câu lệnh này chỉ cho router biết đường đến mạng

đích đi ra bằng cổng giao tiếp nào .Còn ở hình 6.1c ,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 6.1b



Hình 6.1c

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 .

1.3. Cấu hình đường cố định

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

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 .

Bạn vào chế độ cấu hình toàn cục của router .

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 .

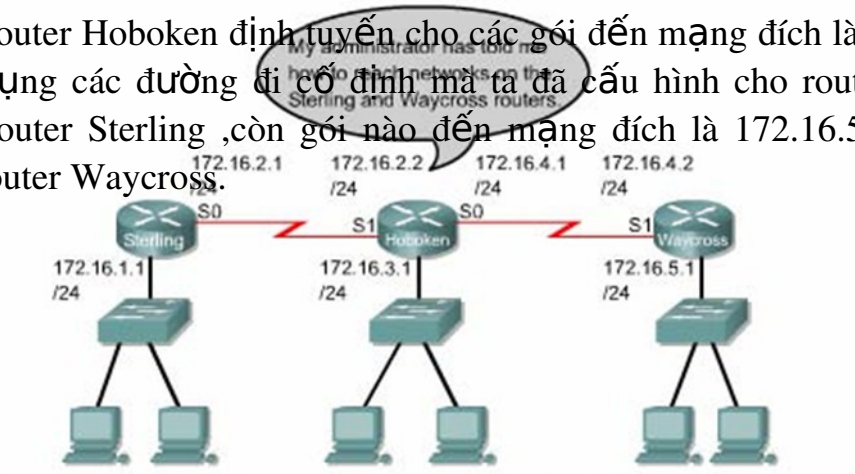
Lặp lại bước 3 cho những mạng đích khác.

Thoát khỏi chế độ cấu hình toàn cục.

Lưu tập tin cấu hình đang hoạt động thành tập tin cấu hình khởi động bằng lệnh copy running -config statup-config.

Hình 6.2 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.




```
Hoboken(config)#ip route 172.16.1.0 255.255.255.0 s1
This command points to the Sterling LAN
Hoboken(config)#ip route 172.16.5.0 255.255.255.0 s0
This command points to the Waycross LAN
```

```
Hoboken(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.1
This command points to the Sterling LAN
Hoboken(config)#ip route 172.16.5.0 255.255.255.0 172.16.4.2
This command points to the Waycross LAN
```

Hình 6.2

Ở khung phía trên của hình 6.2,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 6.2, 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 .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.

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.

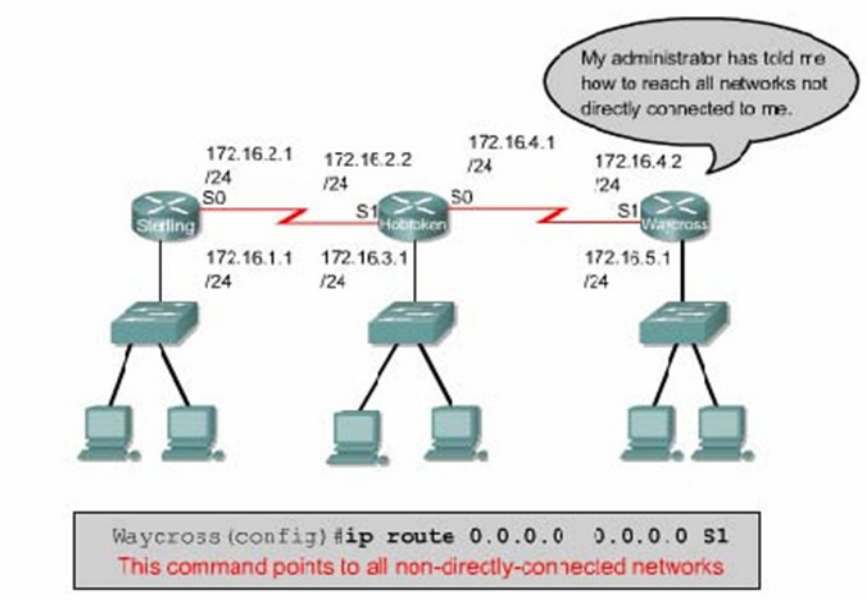
Nhập lệnh ip route với mạng đích là 0.0.0.0 và subnet mask tương ứng là 0.0.0.0. Gateway của đường mặc định có thể là cổng giao tiếp trên router kế tiếp .Thông thường thì chúng ta nên sử dụng địa chỉ IP của router kế tiếp làm gateway .

Thoát khỏi chế độ cấu hình toàn cục.

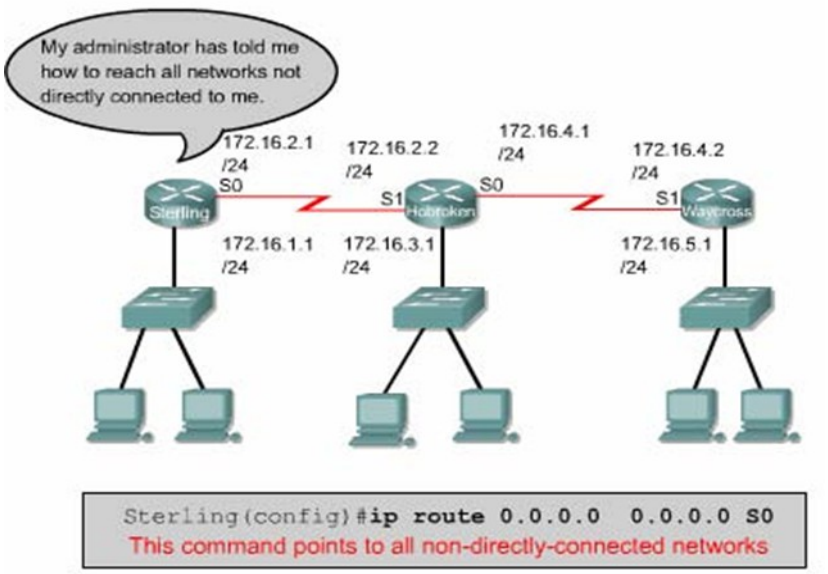
Lưu lại thành tập tin cấu hình khởi động trong NVRAM bằng lệnh

copy running -config.

Tiếp tục xét ví dụ trong phần 6.3: router Hoboken đã được cấu hình để định tuyến dữ liệu tới mạng 172.16.1.0 trên router Sterling và tới mạng 172.16.5.0 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.



Hình 6.3a



Hình 6.3b

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 .

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 route**.

Kiểm tra xem đường cố định mà bạn đã cấu hình có trong bảng định tuyến hay không

1.6. Xử lý sự cố

Xét ví dụ trong phần 6.3: 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.

2 Tổng quan về định tuyến động

Mục tiêu:

- Phân biệt các loại giao thức định tuyến.
- Phân biệt giao thức định tuyến theo vectơ khoảng cách.
- Nhận biết giao thức định tuyến theo trạng thái đường liên kết.

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:

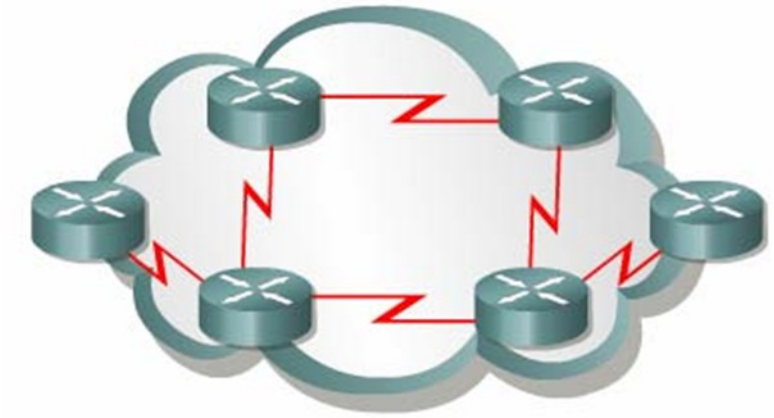
Internet Protocol (IP)

Internetwork Packet Exchange(IPX)

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

2.3. Mục đích của giao thức định tuyến và hệ thống tự quản

Mục 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, để 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 .

2.5. Phân loại các giao thức định tuyến

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

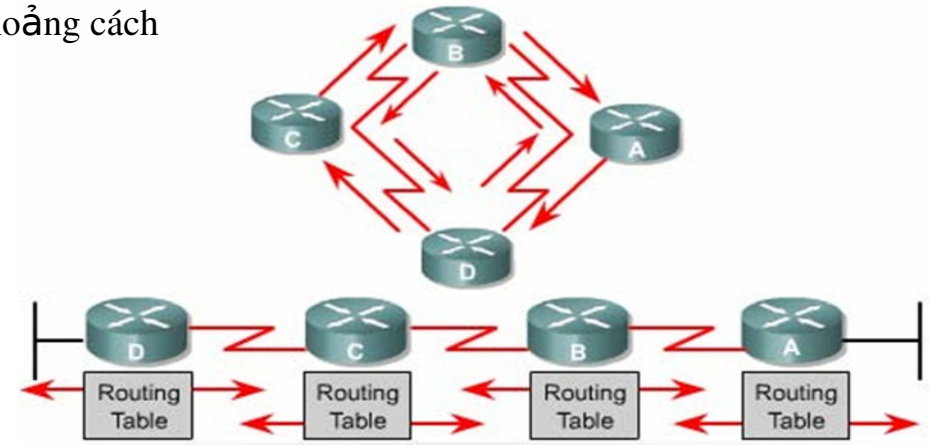
Vectơ khoảng cách.

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 láng giềng theo định kỳ và tính lại vectơ khoảng cách



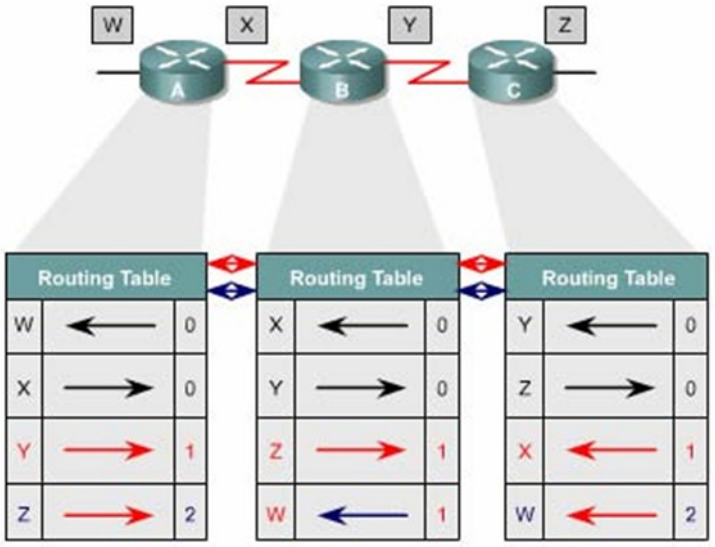
Pass periodic copies of a routing table to neighbor routers and accumulate distance vectors.

Hình 6.5a: Bảng định tuyến theo vectơ khoảng cách

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 6.5b: Cập nhật thông tin bảng định tuyến

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.

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 .

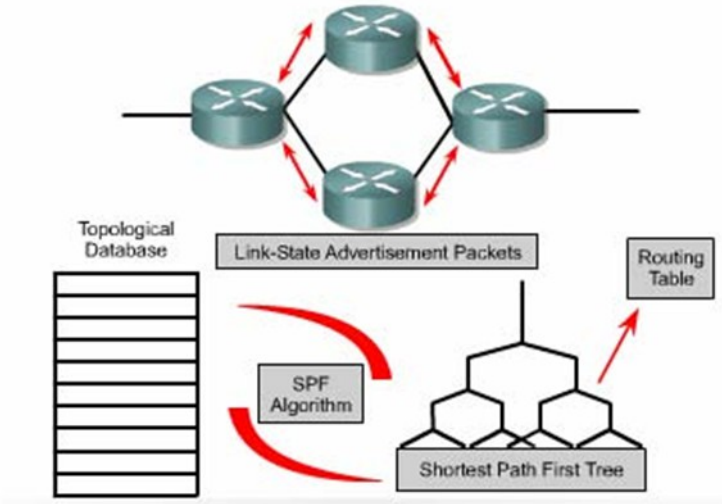
Thuật toán SPF :dựa trên cơ sở dữ liệu về cấu trúc mạng ,thuật toán SPF sẽ tính toán để tìm đường ngắn nhất .

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.

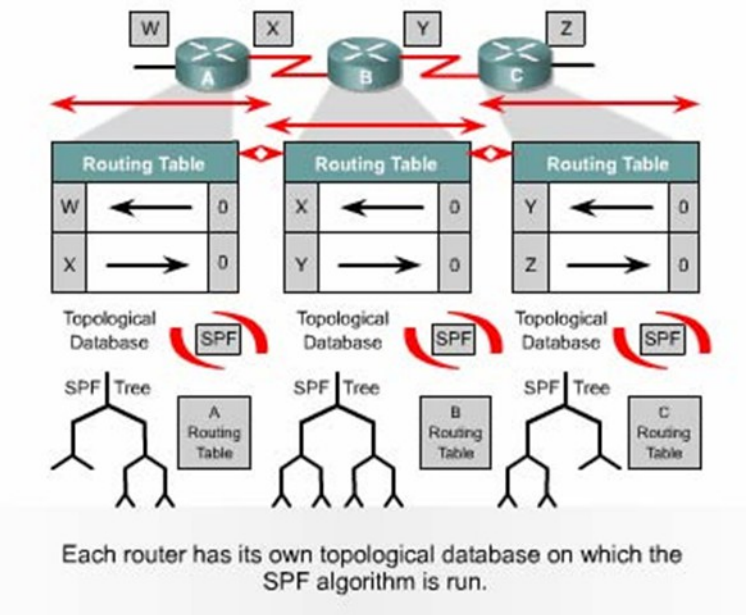
Mỗi router tiến hành xây dựng lại cấu trúc mạng theo dạng hình cây với bản than nó là gốc ,từ đó router vẽ ra tất cả các đường đi tới tất cả các mạng trong hệ thống .Sau đó thuật toán SPF chọn đường ngắn nhất để đưa vào bảng định tuyến. Trên bảng định tuyến sẽ chứa thông tin về các đường đi đã được chọn 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 6.6a

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 .



Hình 6.6b

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 xử 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 .

3. Tổng quát về giao thức định tuyến

Mục tiêu:

- Mô tả đặc điểm cơ bản của giao thức định tuyến thông dụng.
- Phân biệt giao thức định tuyến nội bộ.
- Phân biệt giao thức định tuyến ngoại vi.

3.1. Quyết định chọn đường đi

Router có 2 chức năng chính là :

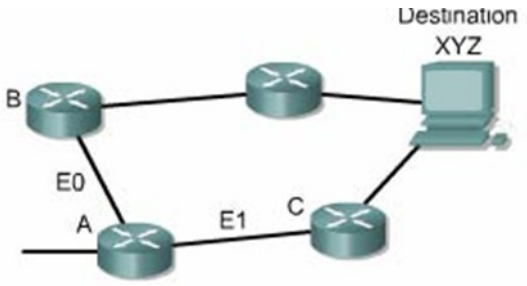
Quyết định chọn đường đi.

Chuyển mạch.

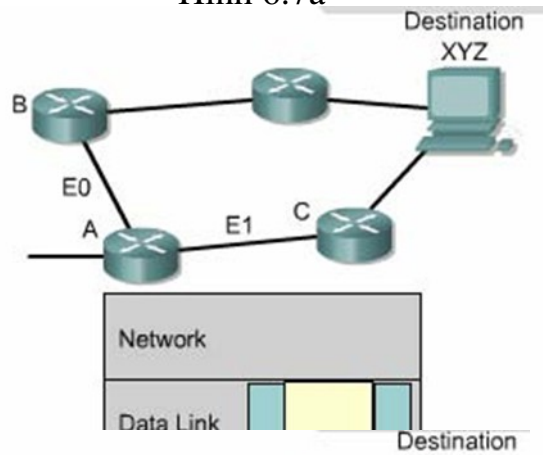
Quá trình chọn đường đi được thực hiện ở lớp Mạng. Router dựa vào bảng định tuyến để chọn đường cho gói dữ liệu ,sau khi quyết định đường ra thì router thực hiện việc chuyển mạch để phát gói dữ liệu .

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

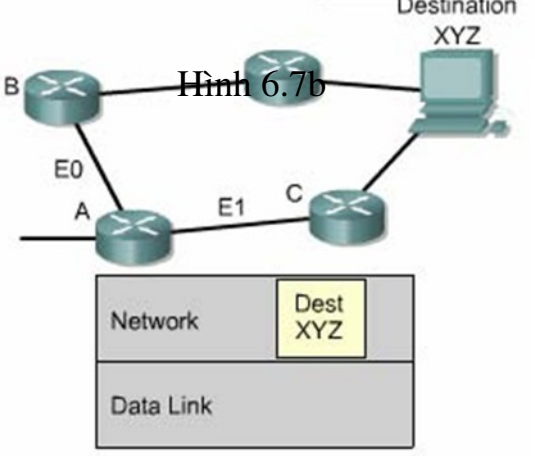
Trong các hình 6.7a-6.7e cho thấy cách mà router sử dụng địa chỉ mạng để quyết định chọn đường cho gói dữ liệu .



Hình 6.7a



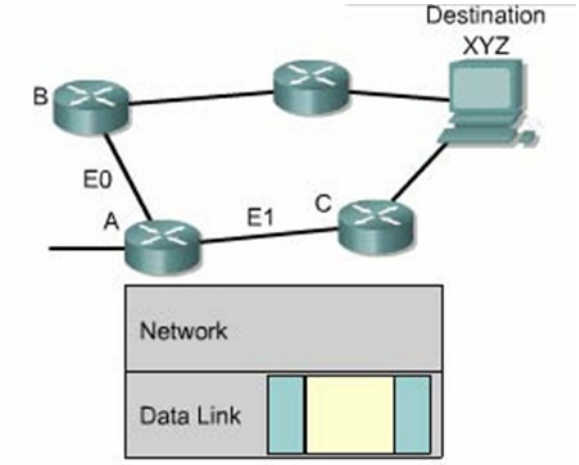
Hình 6.7b



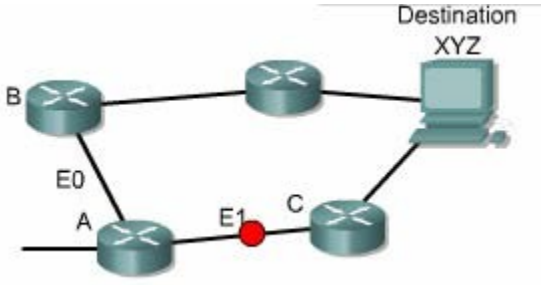
Hình 6.7c

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

Hình 6.7d



Hình 6.7e



Hình 6.7f

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.

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).

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 :

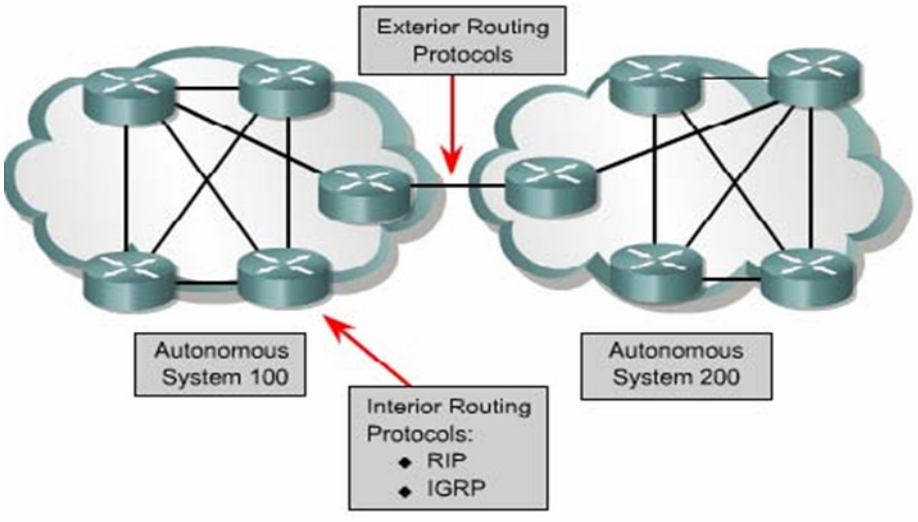
Danh sách các router láng giềng để trao đổi thông tin định tuyến.

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



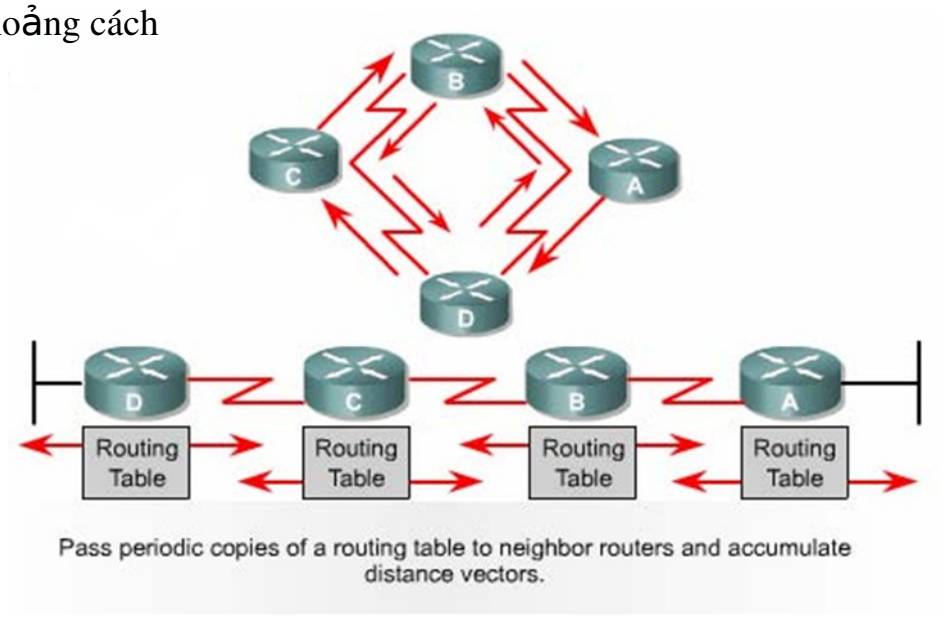
Hình 6.8: Hệ tự quản

3.5. Vectơ khoảng cách

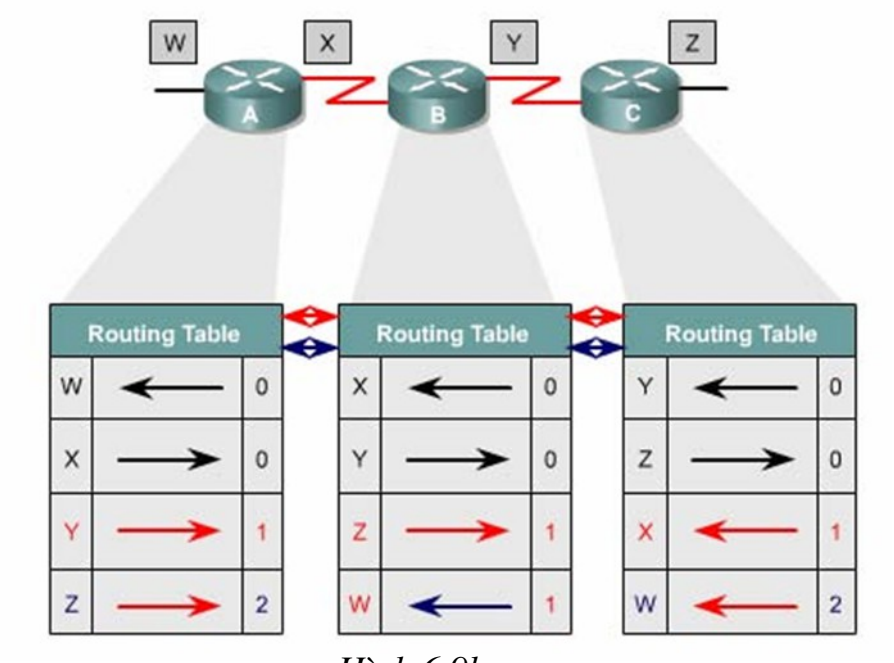
Thuật toán vectơ khoảng cách (hay còn gọi là thuật toán Bellman-Ford)yêu cầu mỗi router gửi một phần hoặc toàn bộ bảng định tuyến cho các router láng giềng kết nối trực tiếp với nó .Dựa vào thông tin cung cấp bởi các router láng giềng ,thuật toán vectơ khoảng cách sẽ lựa chọn đường đi tốt nhất .

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 6.9a



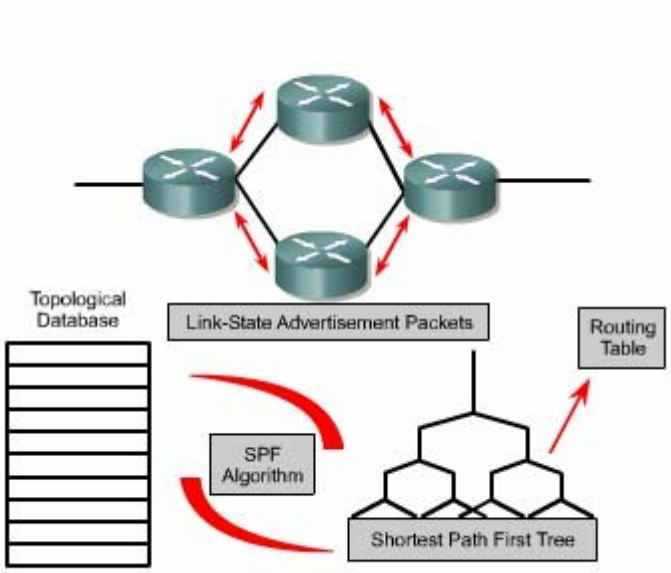
Hình 6.9b

3.6. Trạng thái đường liên kết

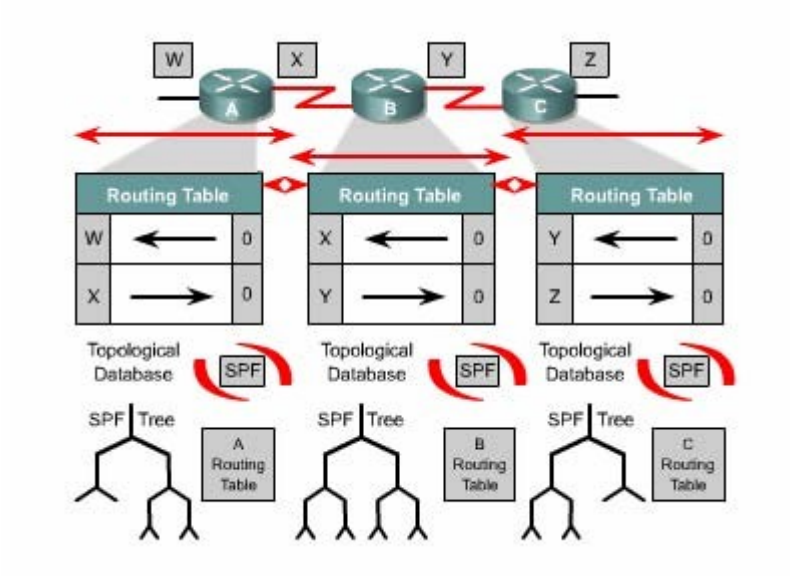
Thuật toán chọn đường theo trạng thái đường liên kết (hay còn gọi là thuật toán chọn đường ngắn nhất) thực hiện trao đổi thông tin định tuyến cho tất cả các router khi bắt đầu chạy để xây dựng một bản đồ đầy đủ về cấu trúc hệ thống mạng .Mỗi router sẽ gửi gói thông tin tới tất cả các router còn lại .Các 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 6.10a: Thuật toán chọn đường theo trạng thái đường liên kết



Hình 6.10b: Cập nhật thông tin cho bảng định tuyến

Bài tập và sản phẩm thực hành bài 34.6

Kiến thức:

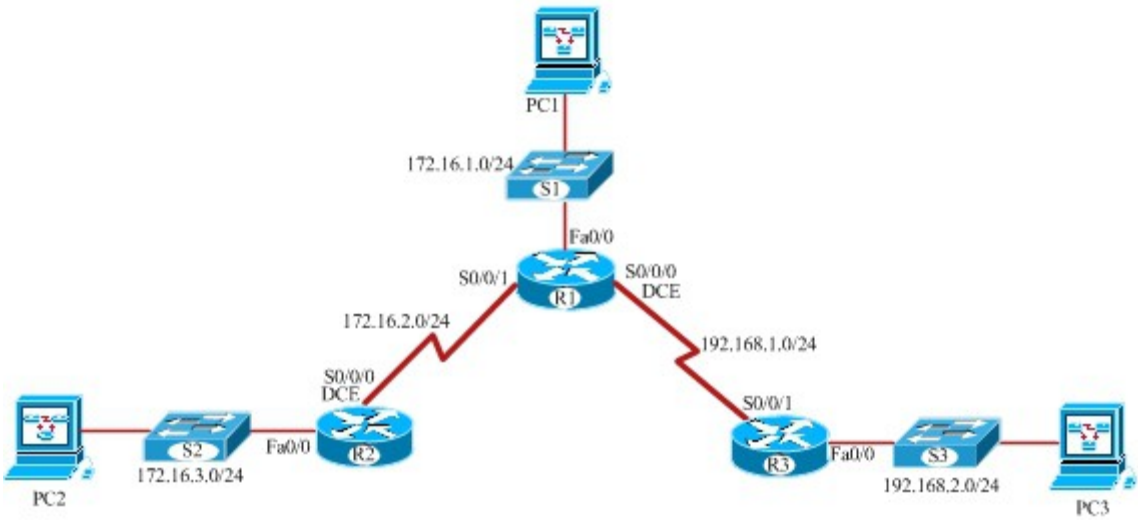
Câu 1: Trình bày chức năng chính của router?

Câu 1: So sánh sự khác nhau giữa định tuyến tĩnh và định tuyến động?

Câu 2: Trình bày các bước cấu hình đường cố định và cấu hình đường đi mặc định cho router ?

Kỹ năng:

Bài tập ứng dụng: Thực hiện cấu hình định tuyến tĩnh cho hệ thống mạng bên dưới.



CHỈ DẪN ĐỐI VỚI HỌC SINH THỰC HIỆN BÀI TẬP ỨNG DỤNG

1. Kết nối cáp cho Router, PC, Switch như hình vẽ.
2. Thực hiện gán IP address, subnetmask, default gateway cho PC, gán IP address cho interface của router (nối với PC).
3. Cấu hình các thông số cơ bản cho router.
4. Thực hiện kiểm tra kết nối giữa PC-PC, PC-Router, Router-Router.
5. Kiểm tra thông tin bảng định tuyến các router.
6. Cấu hình định tuyến tĩnh trên router.
7. Kiểm tra thông tin bảng định tuyến trên các router.
8. Kiểm tra lại kết nối.
9. Thời gian:….. giờ (kể cả thời gian chuẩn bị và cấu hình)
10. Tổng điểm và kết cấu điểm của các bài như sau:

    Tổng số điểm tối đa cho bài: 100 điểm, kết cấu như sau:

    a, Điểm ngoại dạng khách quan: Tổng cộng 70 điểm

    b, Điểm tuân thủ các qui định: 30 điểm

- Thời gian thực hiện bài tập vượt quá 25% thời gian cho phép sẽ không được đánh giá.

- Thí sinh phải tuyệt đối tuân thủ các qui định an toàn lao động, các qui định của phòng thực hành, nếu vi phạm sẽ bị đình chỉ thực tập

BÀI 7: GIAO THỨC ĐỊNH TUYẾN THEO VECTƠ KHOẢNG CÁCH
Mà bài: MĐ34-07

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.

Mục tiêu:

- Mô tả được tại sao định tuyến vòng lặp lại xảy ra đối với định tuyến theo vectơ khoảng cách.
- Mô tả được các phương pháp được sử dụng để bảo đảm cho các giao thức định tuyến theo vector khoảng cách định tuyến đúng.
- Cấu hình RIP.
- Sử dụng lệnh ip classless.
- Xử lý sự cố của RIP.
- Cấu hình RIP để 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.
- Thực hiện các thao tác an toàn với máy tính.

Nội dung:

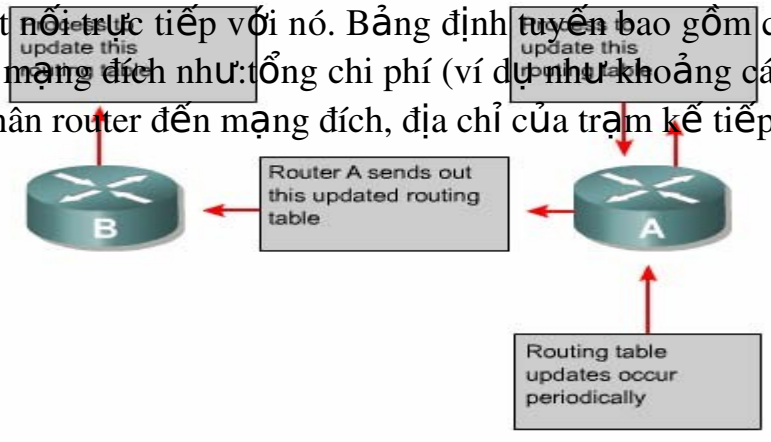
1. Định tuyến theo vectơ khoảng cách

Mục tiêu:

- Mô tả được tại sao định tuyến vòng lặp lại xảy ra đối với định tuyến theo vectơ khoảng cách.
- Mô tả được các phương pháp được sử dụng để bảo đảm cho các giao thức định tuyến theo vector khoảng cách định tuyến đúng.

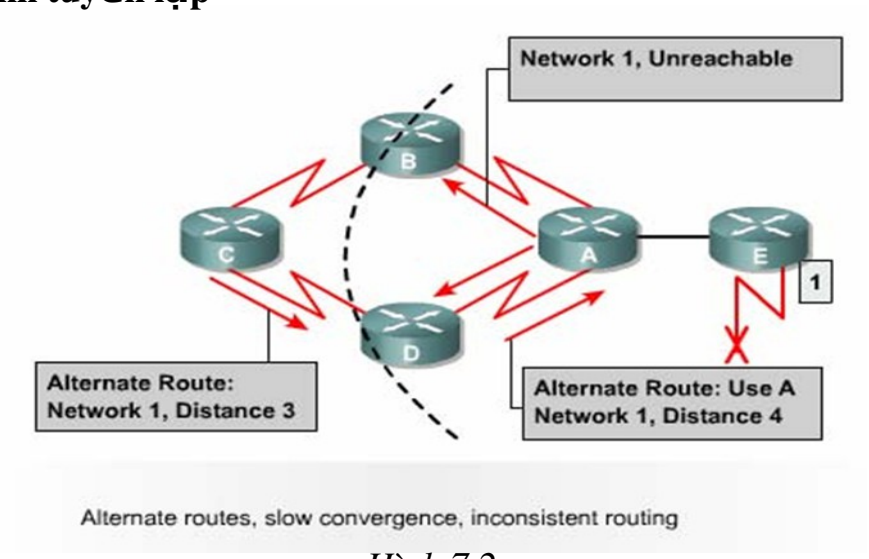
1.1. Cập nhật thông tin định tuyến

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

1.2. Lỗi định tuyến lặp



Hình 7.2

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.

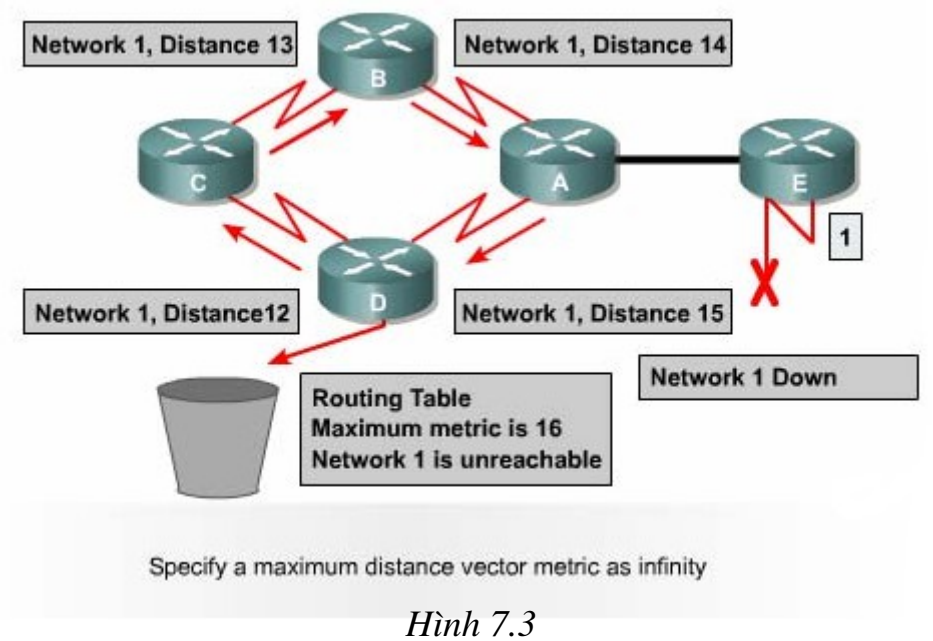
1.3. Định nghĩa giá trị tối đa

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.

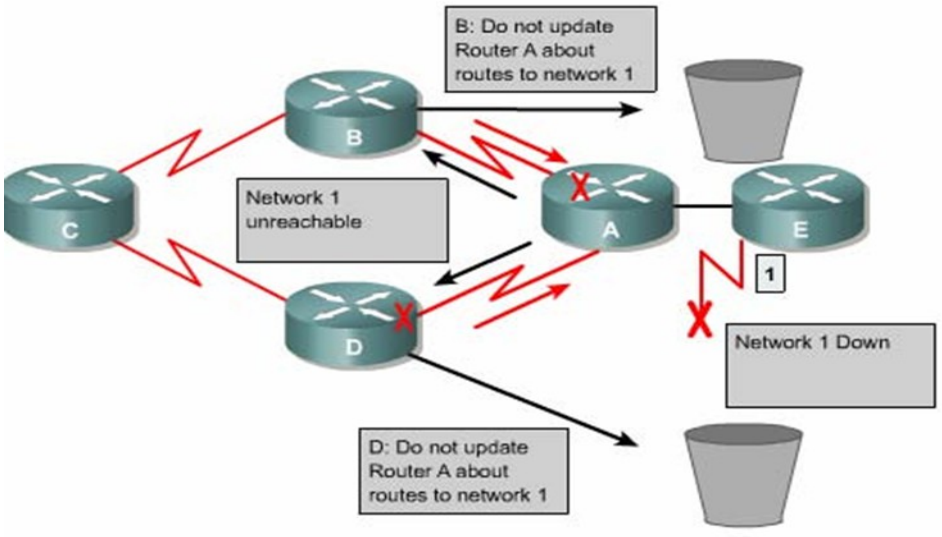


Hình 7.3

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 7.4

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.

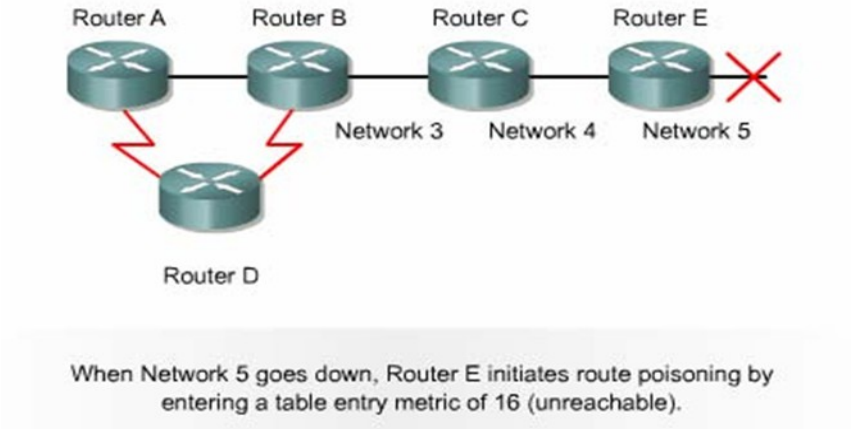
Ví dụ như hình 7.5: khi Mạng 5 bị ngắt thì trên bảng định tuyến của

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 7.5

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

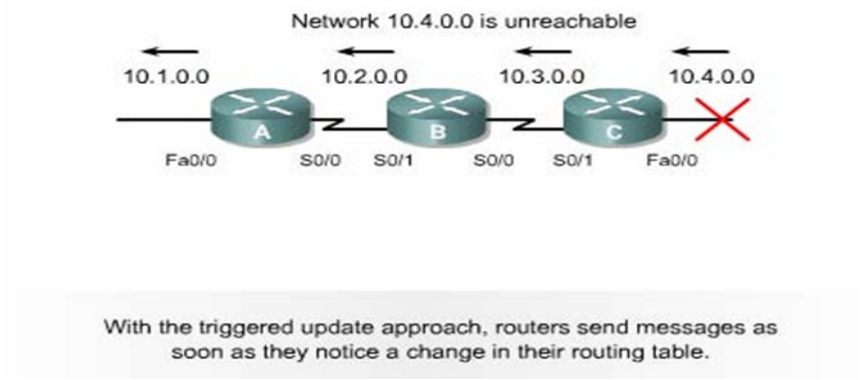
Hoạt động cập nhật bảng định tuyến giữa các router láng giềng được thực hiện theo chu kỳ .Ví dụ :cứ sau 30 giây RIP thực hiện cập nhật một lần .Ngoài ra còn có cơ chế cập nhật tức thời để thông báo về một thay đổi nào đó trong bảng định tuyến .Khi router phát hiện ra có một thay đổi nào đó trong cấu 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 7.6: 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 lượt router A cũng sẽ phát thông báo ra cổng Fa0/0. NetWork 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



Hình 7.6

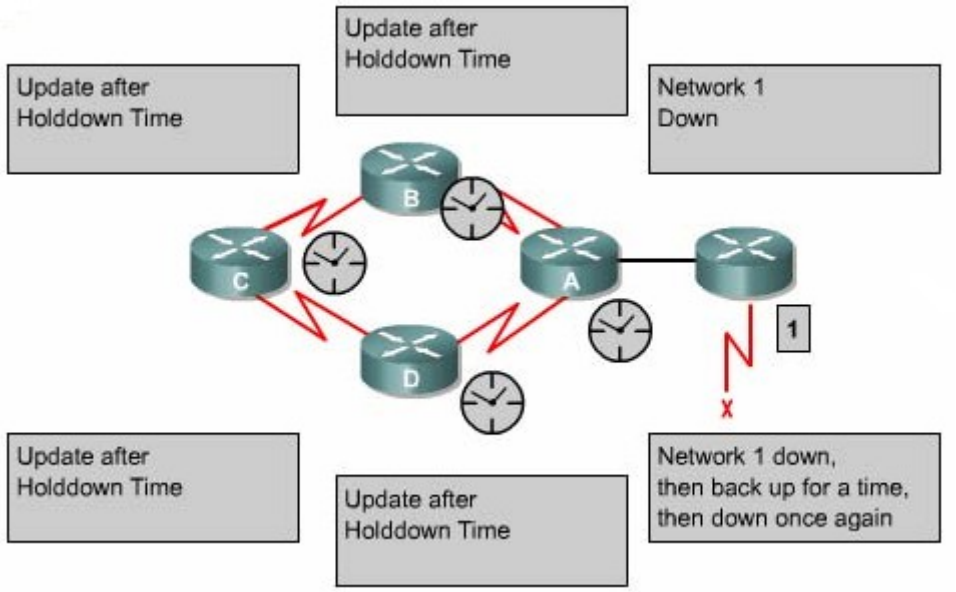
1.7. Tránh lặp vòng với thời gian holddown

Tình trạng lặp vòng đến vô hạn như đã đề cập ở phần 7.6 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 7.7

2.RIP

Mục tiêu:

- Cấu hình RIP.
- Sử dụng lệnh ip classless.
- Xử lý sự cố của RIP.
- Cấu hình RIP để chia tải.
- Cấu hình đường cố định cho RIP.
- Kiểm tra cấu hình RIP.

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 lượng hop.

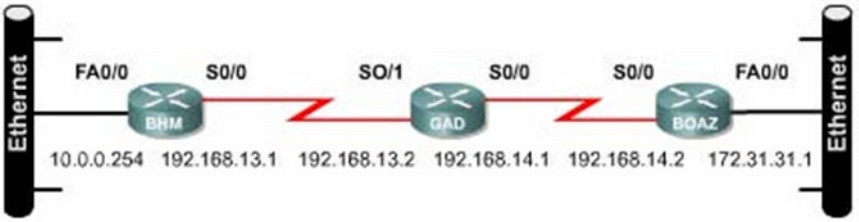
Nếu gói dữ liệu đến mạng đích có số lượng hop lớn hơn 15 thì gói dữ liệu đó sẽ bị huỷ bỏ.

Chu kỳ cập nhật mặc định là 30 giây.

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 7.8 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
```

Hình 7.8

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.

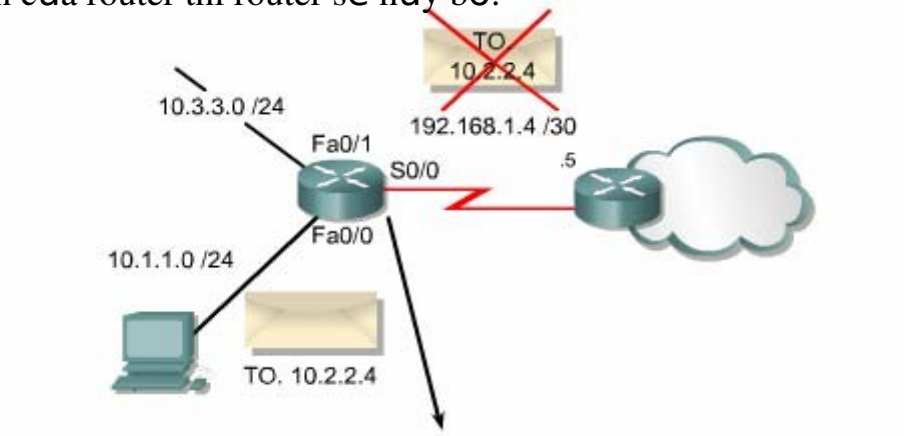
Router(config- router)#network network- number- khai báo các mạng mà RIP được phép chạy trên đó.

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 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.

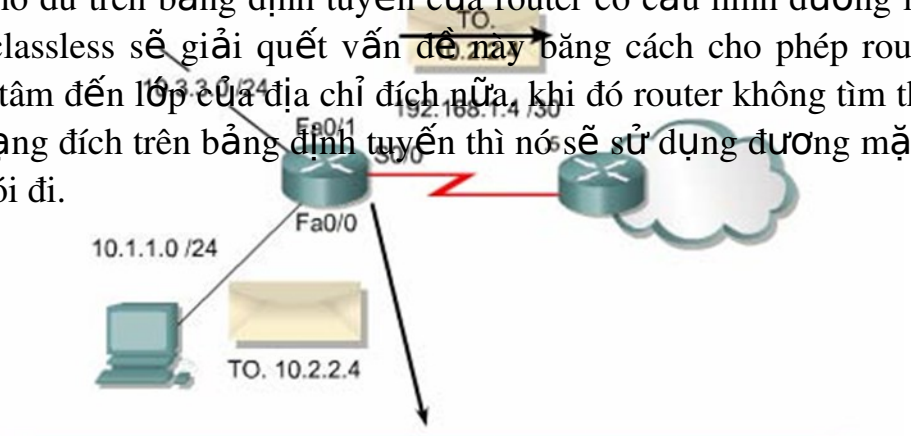
Tuy nhiên, nếu không có chức năng này thì tất cả các gói có địa chỉ đích là một subnet có cùng supernet với các địa chỉ mạng khác của router nhưng lại không có trong bảng định tuyến. Đây chính là đặc điểm quan trọng của giao thức định tuyến theo lớp. Nếu một địa chỉ mạng lớn được chia thành các subnet 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 7.9a: 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 bằng 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 7.9b: Khi có lệnh ip classless.

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 là: 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:

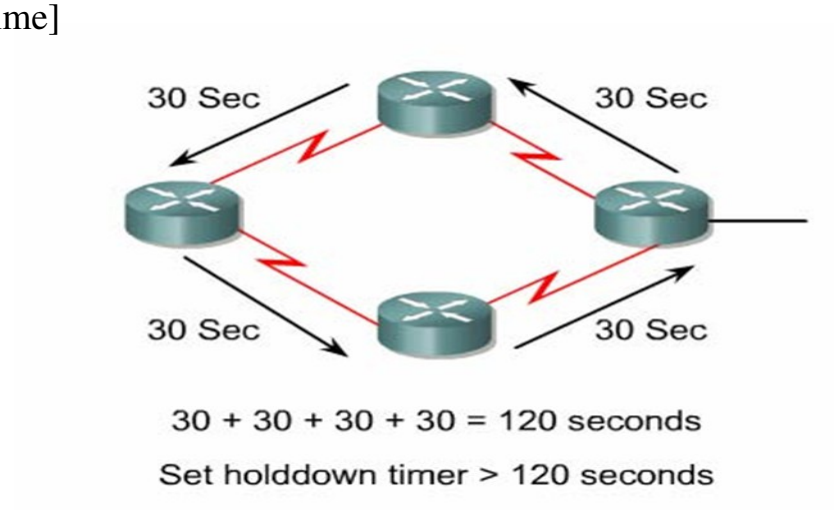
GAD (config-if)#no ip split- horizon

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.

Để thay đổi thời gian holddown bạn dùng lệnh sau:

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



Hình 7.10

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 bảng 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

2.5. Kiểm tra cấu hình RIP

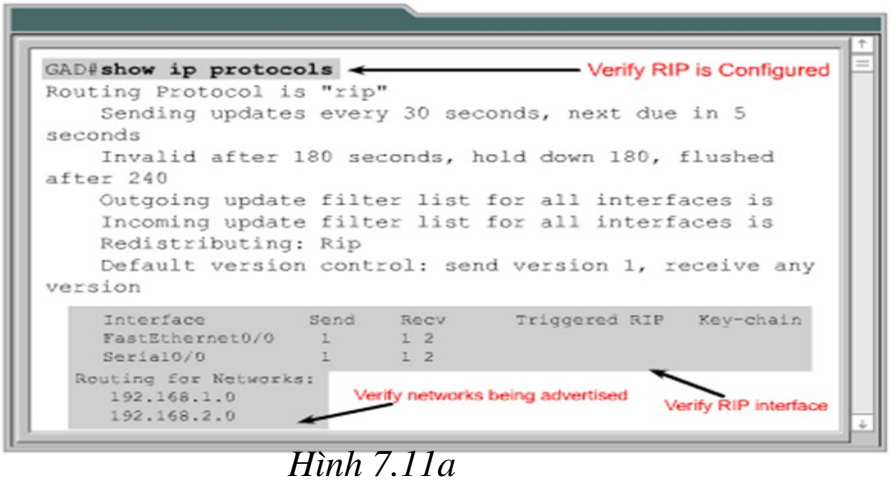
Có nhiều lệnh có thể sử dụng để kiểm tra cấu hình RIP có đúng hay không. Trong đó hai lệnh thường được sử dụng nhiều nhất là **Show ip route và show ip protocols.**

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 7.11a

Lệnh **show ip route** 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.

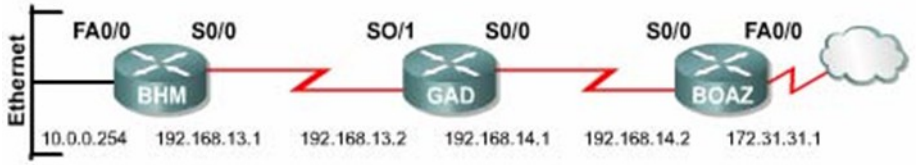
```
GAD#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP,
M - mobile, B - BGP
           D - EIGRP, EX - EIGRP external, O - OSPF,
IA - OSPF inter area
           N1 - OSPF NSSA external type 1, N2 - OSPF
NSSA external type2
           E1 - OSPF external type 1, E2 - OSPF
external type 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 download static route

Gateway of last resort is not set
```

Hình 7.11b

2.6. Xử lý sư 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

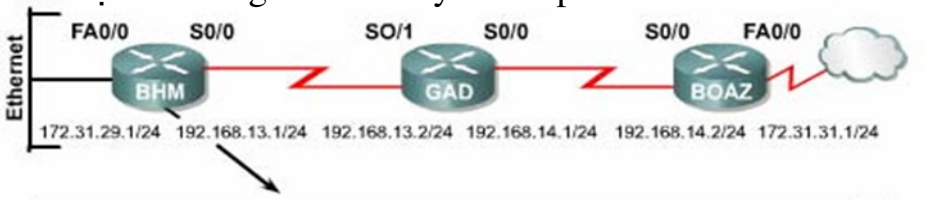
Lệnh debug ip rip sẽ hiển thị tất cả các thông tin định tuyến mà RIP gửi và nhận. Ví dụ trong hình 7.12a cho thấy kết quả hiển thị của lệnh debug ip rip. Sau khi nhận được thông tin cập nhật , router sẽ xử lý thông tin đó rồi sau đó gửi thông tin mới vừa cập nhật ra các cổng. Trong hình 7.12a cho thấy 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 nguồn của gói thông tin cập nhâth RIP.




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

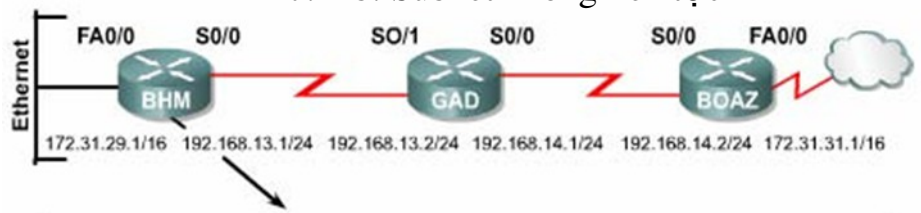
Hình 7.12a: Kiểm tra các thông tin được quảng bá qua Rip

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.




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

Hình 7.12b: Subnet không liên tục




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

Hình 7.12c: 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}.

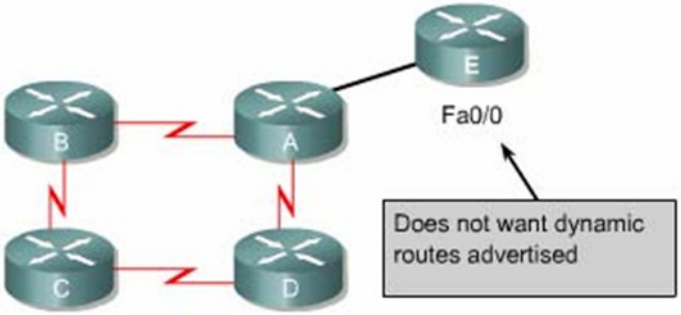
Show ip interface brief.

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.




```
RouterE(config-router)#passive-interface Fa0/0
```

Hình 7.13

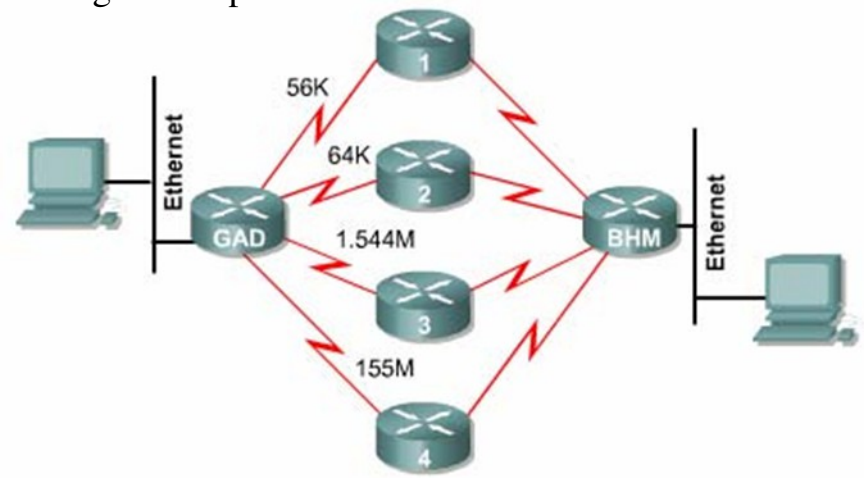
2.8. Chia tải với RIP

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 taỉ 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 hình 7.14a 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 7.14a

Trong hình 7.14b 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 7.14b

2.9. Chia tải cho nhiều đường

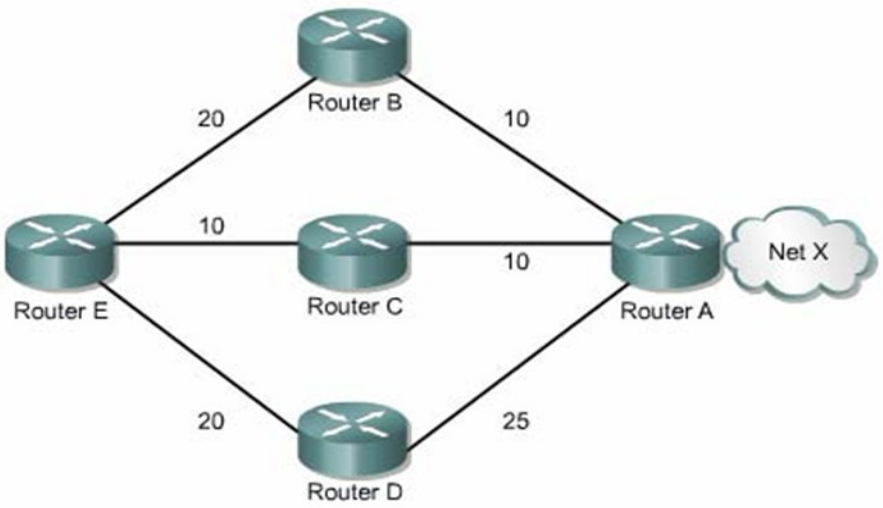
Router có khả năng chia tải ra nhiều đường để chuyển các gói dữ liệu đến cùng mục đích. Chúng ta có thể cấu hình bằng tay cho router thực hiện

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 đừơng 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 7.15a

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 7.15a, 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 7.15b

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 đường 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 7.16a và 7.16b 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 đừng 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#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 7.16a

```
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 7.16b

3.EIGRP

Mục tiêu:

- Cấu hình EIGRP.
- Kiểm tra hoạt động của EIGRP.
- Xử lý sự cố EIGRP.

3.1. Giới thiệu giao thức định tuyến EIGRP

EIGRP là giao thức riêng của Cisco, được đưa ra vào năm 1994 với IOS 9.2.1, được phát triển từ giao thức IGRP.

Không giống 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 địa chỉ bằng VLSM. So với IGRP, EIGRP có thời gian hội tụ nhanh hơn, có khả năng mở rộng tốt hơn và khả năng chống loop cao hơn.

Và đặc biệt hơn, 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 tốt cho cả 2 mạng IPX và Apple Talk.

EIGRP là giao thức định tuyến nâng cao theo vectơ khoảng cách (distance vector). 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. Ví dụ như 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. Cho nên EIGRP còn được xem là giao thức định tuyến lai (hybrid routing protocol). EIGRP là một lựa chọn lý tưởng cho các mạng lớn, đa giao thức được xây dựng dựa trên các Cisco router.

3.2. Tìm hiểu giao thức định tuyến EIGRP

3.2.1. 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.

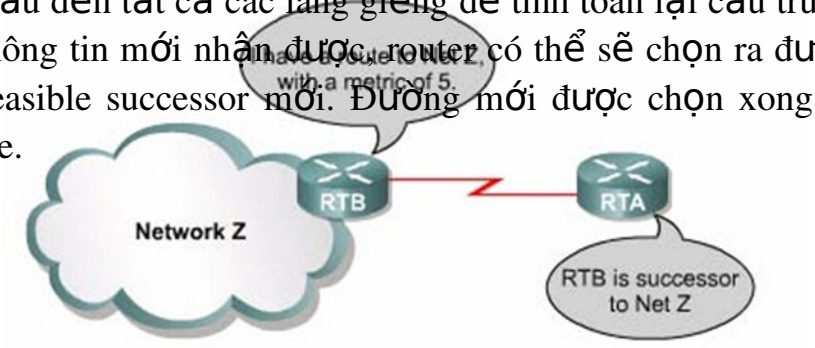
Trạng thái đường đi: Trạng thái không tác động (P - passive) là trạng thái ổn định, sẵn sàng sử dụng được, trạng thái tác động (A - active) là trạng thái đang trong tiến trình tính toán lại của DUAL.

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.

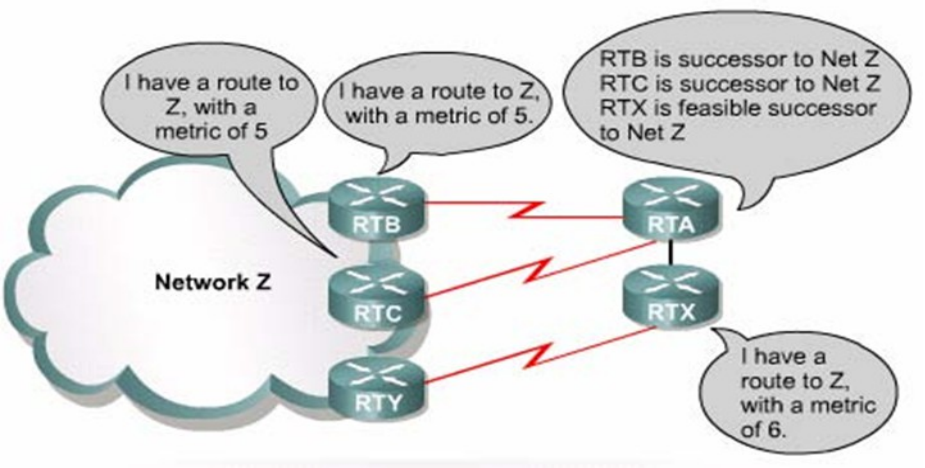
Con đường được chọn làm đường chính đến mạng đích gọi là successor. Từ thông tin trong bảng láng giềng và bảng cấu trúc mạng, DUAL chọn ra một đường chính và đưa lên mạng định tuyến. Đến một mạng đích có thể có đến 4 successor. Những đường này có chi phí bằng nhau hoặc không bằng nhau. Thông tin về successor 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 7.17a: RTA có thể có nhiều successor đến mạng Z nếu RTB và RTC gửi thông báo về chi phí đến mạng Z như nhau

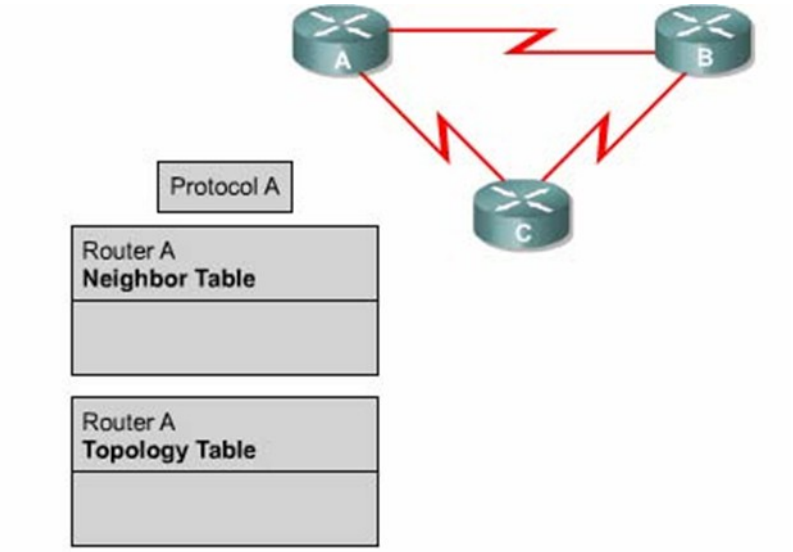


Hình 7.17b

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)
```

Hình 7.17c



Hình 7.17d

3.2.2. Các đặc điểm 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 hê 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.

3.2.3. 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:

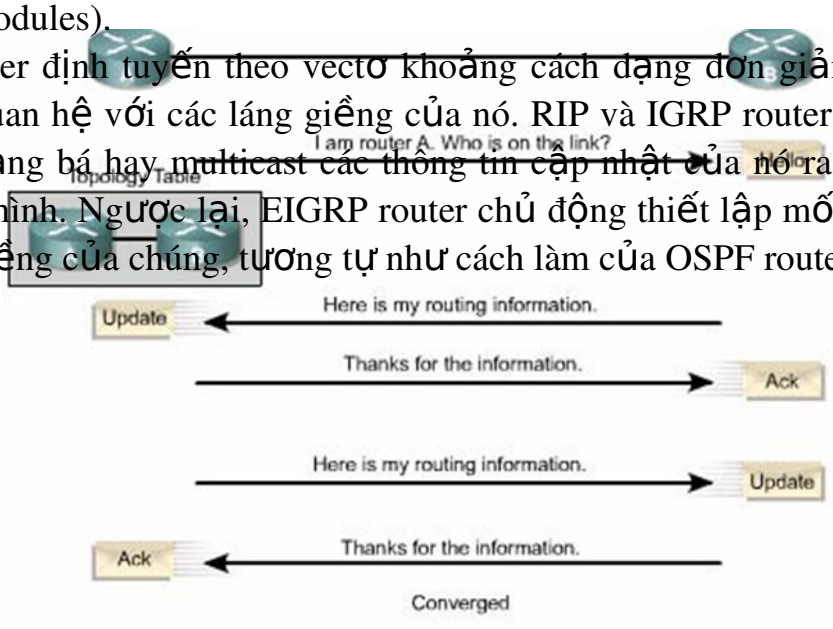
Sự phát hiện và tái phát hiện các router láng giềng.

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.



Hình 7.18

Quá trình EIGRP router thiết lập mối quan hê thân mật được mô tả trong *hình 7.18* EIGRP router sử dụng các gói hello rất nhỏ để thực hiên việc thiết lập mối quan hê 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 đông. 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 thể 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 dịnh 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.

3.2.4. Cấu trúc dữ liêu 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 hiên, kiểm tra và tái phát hiên các router láng giềng. Tái phát hiên có nghĩa là router EIGRP không nhân 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 nhân được từ mỗi router láng giềng. Theo định kỳ và trong giới hạn của khoảng thời gian lưu giữ, router phải nhân 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 hê 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 7.19

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 vây. 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 cây. Điều này có nghĩa là không có báo nhân cho các gói hello.

EIGRP router sử dụng gói báo nhân để xác nhân là đã nhân được gói EIGRP trong quá trình trao đổi tin cây. Giao thức vân chuyển tin cây (RTP — Reliable Transport Protocol) cung cấp dịch vụ liên lạc tin cây giữa hai host

EIGRP. Gói báo nhân chính là gói hello mà không có dữ liệu. Không giống như hello được gửi multicast, các gói báo nhân chỉ gửi trực tiếp cho một máy nhân. Báo nhân 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 câp nhât cho router láng giềng mới này để nó có thể xây dựng bảng cấu trúc mạng. Có thể sẽ cần nhiều gói câp nhât 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 câp nhât cho mọi router láng giềng của nó để thông báo về sự thay đổi. Mọi gói câp nhât 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.

3.2.5. 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 7.20a. 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 7.20a-f có các thông tin sau:

Giao thức định tuyến là giao thức EIGRP.

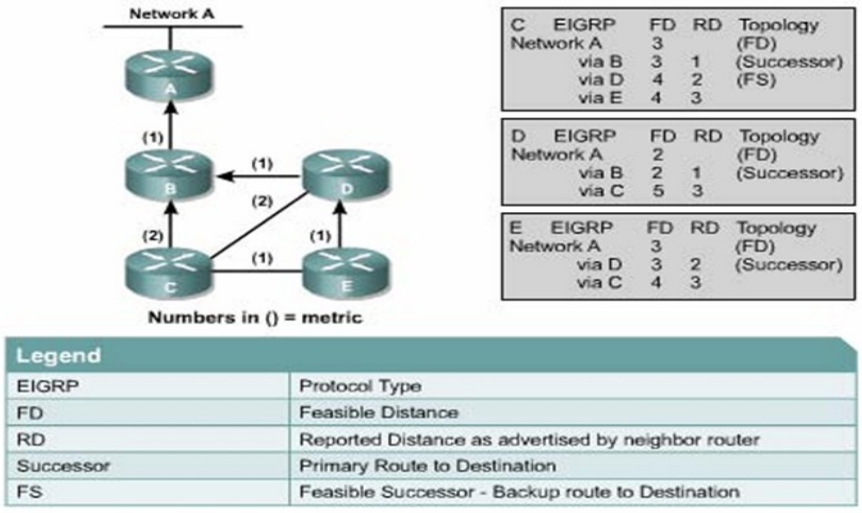
Chi phí thấp nhất của đường đến một mạng đích gọi là Feasible Distance (FD).

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.



Hình 7.20a

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. Hiên 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.

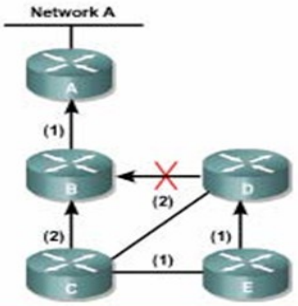
Router D có một đường successor là đường qua Router B.

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 hiên nguyên tắc chọn feasible successor như thế nào khi đường liên kết giữa Router D và Router B bị đứt:



C EIGRP Network A	FD	RD	Topology
	3		(FD)
via B	3	1	(Successor)
via D	4	2	(FS)
via E	4	3	

D EIGRP Network A	FD	RD	Topology
	2		(FD)
~~via B~~	~~2~~	~~1~~	~~(Successor)~~
via C	5	3	

E EIGRP Network A	FD	RD	Topology
	3		(FD)
via D	3	2	(Successor)
via C	4	3	

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 7.20b

Trong Router D (hình 7.20b):

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.

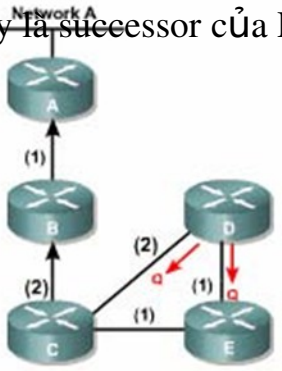
Router D phải tính toán lại đường mới.

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 Network A	FD	RD	Topology
	3		(FD)
via B	3	1	(Successor)
via D			
via E	4	3	

D EIGRP Network A	FD	R	Topology
ACTIVE	-1	2	(FD)
via B			(q)
via C	5	3	(q)

E EIGRP Network A	FD	RD	Topology
	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 7.20c

Trong router D (hình 7.20c):

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.

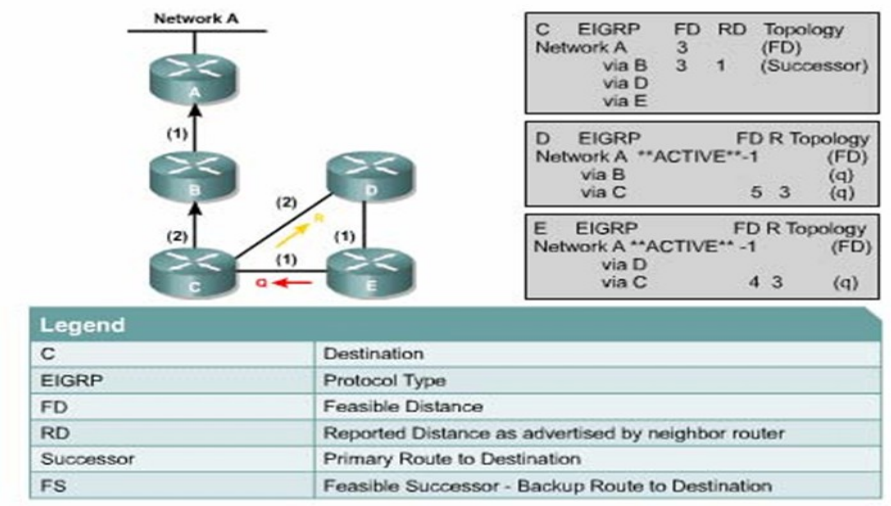
Trong Router E:

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 7.20d

Trong Router C (hình 7.20d):

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 nhân là đường đến Mạng A đang hoạt đông 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.

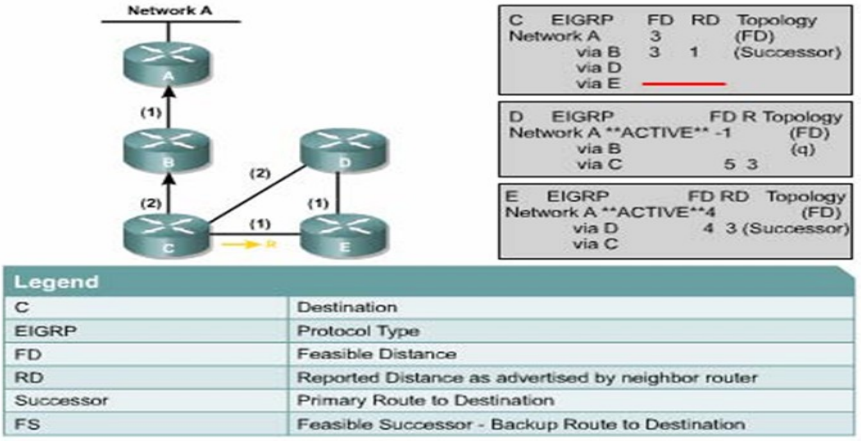
Do đó, Router E đánh dấu trạng thái con đường đến Mạng A là Active.

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 7.20e

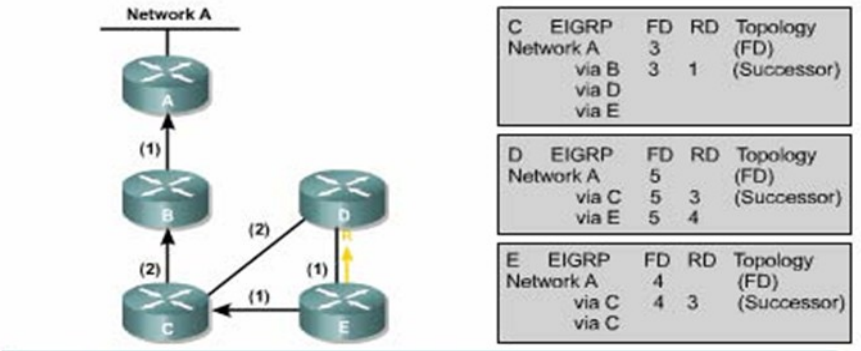
Trong Router E (hình 7.20e):

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 nhân được gói hello từ trạng thái đó. Do đó trong ví dụ này chỉ cần đánh dấu trạng thái Active thôi.



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 7.20f

Trong Router E (hình 7.20f):

Router E gửi đáp ứng cho Router D để cung cấp thông tin về mạng của Router E.

Trong Router D:

Router D nhân được gói hồi đáp từ Router E với những thông tin về mạng của Router E.

Router D ghi nhân 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 cơ bản và kiểm tra cấu hình EIGPR

3.2.1. Cấu hình EIGRP cơ bản

Trừ thuật toán DUAL là phức tạp, còn cấu hình EIGRP thì khá đơn giản, Tùy theo giao thức được định tuyến là IP,IPX hay Apple Talk mà câu lệnh cấu hình EIGRP sẽ khác nhau. Ở đây chỉ đề cập đến cấu hình EIGRP cho giao thức IP.

Việc kích hoạt giao thức EIGRP ta thực hiện trong Privileged EXEC mode. Sử dụng lệnh sau để khởi động EIGRP và xác định con số của hệ thống tự quản (autonomous system number- AS number).

router(config)# **router eigrp autonomous-system-number**

Thông số autonomous-system-number xác định các router trong một hệ thống tự trị. Những router nào trong cùng một hệ thống mạng thì phải có con số này giống nhau để có thể thực hiện việc gửi các gói cập nhật thông tin định tuyến cho nhau.

Khai báo những mạng của router mà bạn đang cấu hình có cùng EIGRP AS number, ta sử dụng câu lệnh sau:

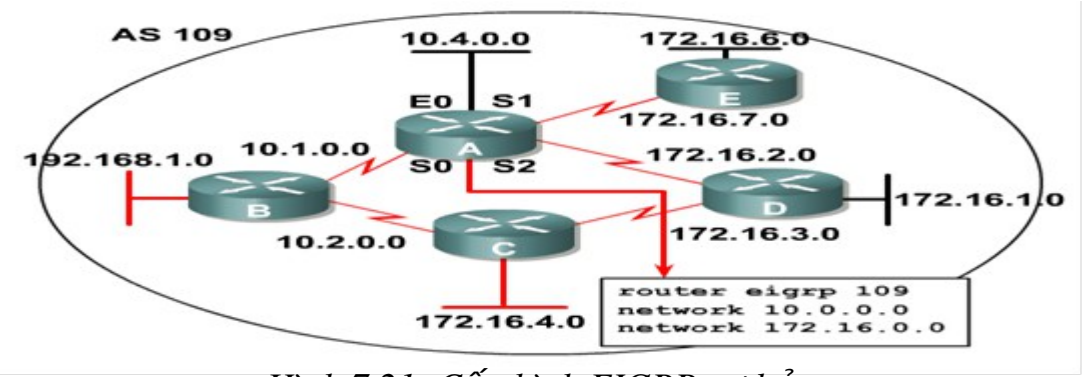
router(config-router)#**network network-number [wildcard-mask]**

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.

Thông số wildcard-mask được sử dụng từ IOS 12.0 trở lên, tham số này có thể sử dụng hoặc không. Tham số wildcard-mask được sử dụng để xác định các mạng con của các mạng classful và có thể được nhập như là một định dạng mặt nạ nghịch đảo hoặc trong mặt nạ mạng.

Wildcard mask = 255.255.255.255 – network's subnet mask

* Lưu ý: Chỉ khai báo những mạng nào kết nối trực tiếp vào router mà thôi.



Hình 7.21: Cấu hình EIGRP cơ bản

Câu lệnh khai báo các mạng trên Router A (không chứa tham số wildcard mask) như sau:

router eigrp 109
network 10.1.0.0
network 10.4.0.0
network 172.16.7.0
network 172.16.2.0

Router A sẽ thay đổi câu lệnh network để có địa chỉ mạng dạng classful, kết quả của quá trình cấu hình sẽ như sau:

router eigrp 109
network 10.0.0.0
network 172.16.0.0

Theo mặc định EIGRP sẽ nhóm các mạng với nhau theo dạng địa classful. Do đó chỉ có 2 mạng được quảng bá trong EIGRP.

Câu lệnh khai báo các mạng trên Router A (không chứa tham số wildcard mask) như sau:

router eigrp 109
network 10.1.0.0 0.0.255.255
network 10.4.0.0 0.0.255.255
network 172.16.2.0 0.0.0.255
network 172.16.7.0 0.0.0.255

Trong trường hợp này, router A sử dụng wildcard mask để xác định các giao diện kết nối trực tiếp tham gia vào quá trình định tuyến EIGRP với AS 109. Tất cả các mạng 10.1.0.0/16, 10.4.0.0/16, 172.16.2.0/24, 172.16.7.0/24 đều tham gia vào quá trình định tuyến EIGRP với AS 109.

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 băng 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 (Bandwidth) cho một cổng serial trên router, dùng câu lệnh sau chế độ cấu hình của cổng đó:

Router(config-if)# bandwidth kilobits

Giá trí băng thông khai báo 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.

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 liên kết trực tiếp giúp chúng ta theo dõi sự ổn định của hệ thống định tuyến và phát hiện sự cố nếu có.

3.2.2. Kiểm tra cấu hình EIGRP

Câu lệnh **show ip eigrp neighbors** hiển thị thông tin về các router láng giềng trong cùng AS number.

Hình 7.22a: Bảng thông tin về các router láng giềng

Các thông tin trong bảng láng giềng:

H (handle): Là một dạng số được sử dụng trong phần mềm Cisco IOS để theo dõi một router láng giềng. Nó ghi thứ tự những router hàng xóm đã học được.

Address: Địa chỉ mạng của router láng giềng.

Interface: Giao diện cổng mạng mà router sử dụng để truyền thông với router láng giềng.

Hold (hold time): Là khoảng thời gian lưu giữ(được tính theo giây). 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 router 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.

Uptime: Là khoảng thời gian đã qua tính theo giờ, phút, giây tính từ khi router láng giềng được thêm vào bảng định tuyến.

SRTT (smoothed round-trip time): Là khoảng thời gian trung bình theo mili giây mà router sử dụng để gửi gói tin EIGRP đến router láng giềng và nhận về gói tin báo nhận. Khoảng thời gian này xác

định thời gian truyền lại - retransmission timeout (RTO).

RTO (retransmission timeout): Là giá trị thời gian tính theo mili giây mà router phải chờ sự xác nhận trước khi truyền một gói tin cậy từ hàng đợi đến router láng giềng. Nếu một bản cập nhật EIGRP, một truy vấn, hoặc trả lời được gửi, một bản sao của gói tin sẽ được xếp vào hàng đợi. Nếu RTOs hết hạn trước khi nhận được sự xác nhận, một bản sao của gói xếp hàng đợi sẽ được gửi.

Q Cnt (queue count): Số lượng các gói tin chờ trong hàng đợi để được gửi ra ngoài. Nếu giá trị này luôn cao hơn 0, vấn đề ùn tắc có thể xảy ra. Giá trị 0 chỉ ra rằng không có các gói tin EIGRP nào trong hàng đợi.

Seq Num: 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 bảo đảm 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.

Lệnh **show ip route eigrp** chỉ hiển thị các tuyến EIGRP trong bảng định tuyến IP. EIGRP hỗ trợ các loại đường sau: bên trong, bên ngoài, và đường tổng hợp. Tuyến EIGRP bên trong được xác định ký hiệu D ở cột bên trái; tuyến đường EIGRP bên ngoài (khác thông số AS number) được xác định bởi ký hiệu EX D.

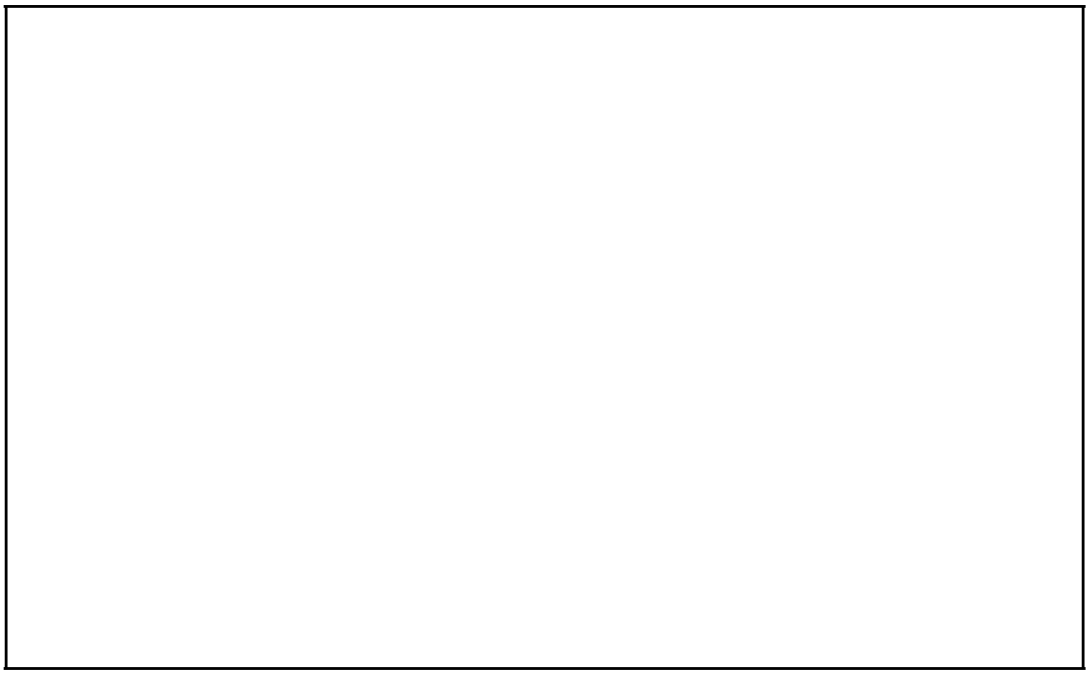
Hình 7.22b: Câu lệnh show ip route eigrp

Administrative Distance (AD): Là một trọng số được router sử dụng để đánh giá độ trung thực của thông tin định tuyến. AD càng nhỏ thì độ ưu tiên càng cao.

Next-hop: Là địa chỉ router láng giềng, từ đó gói tin được chuyển tiếp tới mạng đích.

Output Interface: Là giao diện cổng ra của router, từ đây gói tin bắt đầu được gửi đến mạng đích.

Lệnh **show ip protocols** đưa ra thông tin về tất cả các giao thức định tuyến động chạy trên router.



Hình 7.22c: Câu lệnh Show ip protocols

Trong hình trên câu lệnh cung cấp các thông tin về giao thức eigrp như:

Danh sách bộ lọc cho các gói cập nhật ra hoặc vào. Nó cũng chỉ ra EIGRP đang tạo một mạng mặc định hay nhận một mạng mặc định từ gói cập nhật.

Hiển thị thông tin về cấu hình mặc định của giao thức EIGRP như giá trị của K, số hop và phương sai.Bởi vì các router EIGRP lân cận phải được cấu hình cùng giá trị K, câu lệnh show ip protocols giúp ta xác định được giá trị K hiện thời trước khi cấu hình cho các router kế cận khác.

Cung cấp trạng thái của chức năng tự động tổng hợp đường được bật hay tắt (chế độ này mặc định là bật).

Hiển thị số con đường tối đa mà router được phép cân bằng tải (có thể lên tới sáu con đường nếu được cấu hình bằng câu lệnh maximum-path)

Hiển thị các mạng được router định tuyến.

Câu lệnh **show ip eigrp interfaces** hiển thị thông tin về tất cả các giao diện (cổng) đã được cấu hình EIGRP.

Hình 7.22d: Câu lệnh Show ip eigrp interfaces

Câu lệnh cung cấp các thông tin như:

Interface: Các giao diện đã được cấu hình giao thức định tuyến EIGRP.

Peers: Số láng giềng kết nối trực tiếp với EIGRP trên mỗi giao diện..

Xmit Queue Un/Reliable: Số lượng gói tin còn lại trong hàng đợi truyền tin cậy và không tin cậy.

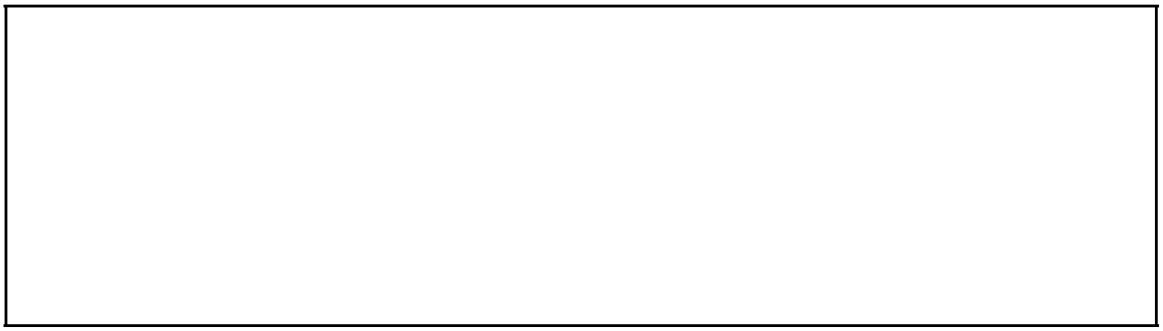
Mean SRTT: Khoảng thời gian SRTT trung bình (tính theo mili giây).

Pacing Time Un/Reliable: Nhịp thời gian được sử dụng để xác định khi nào các gói tin EIGRP được gửi qua các giao diện.

Multicast Flow Timer: Khoảng thời gian tối đa (tính theo giây) mà router gửi các gói tin EIGRP.

Pending Routes: Số tuyến đường trong các gói tin ở hàng đợi truyền đang chờ được gửi đi.

Câu lệnh **Show ip eigrp topology** hiển thị danh sách các mạng đã được router học qua EIGRP.



Hình 7.22e: Câu lệnh Show ip eigrp topology

Câu lệnh hiển thị các thông tin sau:

P (Passive): Mạng ở trạng thái hoạt động ổn định nhất, hoàn toàn có thể được cài đặt trong bảng định tuyến.

A (Active): Hiện thời mạng không sử được, mạng này không thể cài đặt trong bảng định tuyến và đang được thuật toán DUAL tính toán lại.

U (Update): Mạng này đang được cập nhật (được đặt trong một gói cập nhật). Mã này cũng được áp dụng nếu router đang chờ sự xác nhận cho gói cập nhật này.

Q (Query): Mạng này đang được gói tin truy vấn dò hỏi. Mã này cũng áp dụng nếu các bộ định tuyến đang chờ xác nhận cho một gói tin truy vấn. Về cơ bản, mã này chỉ ra rằng các router đã gửi một gói tin

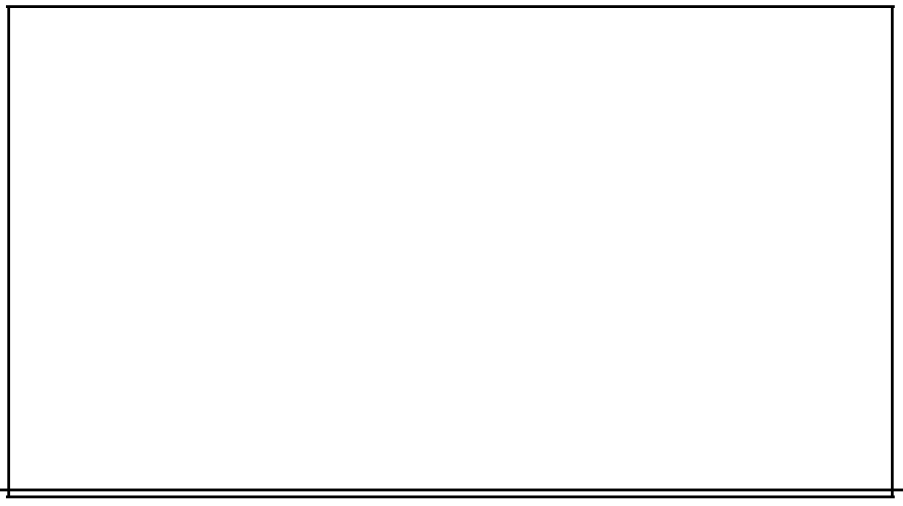
truy vấn đến một router láng giềng.

R (Reply status): Router đang trả lời cho mạng này hoặc đang chờ sự xác nhận cho gói tin trả lời.

S (Stuck-in-active status): EIGRP tập hợp những vấn đề cho mạng mà nó có liên quan.

Số lượng successors có thể sử dụng cho mỗi tuyến đường được thể hiện kết quả hiển thị. Trong hình trên tất cả các mạng đều có một successor, nếu chúng có giá trị đường đi bằng nhau và tới cùng một mạng thì sẽ có tối đa sáu con đường sẽ được hiển thị. Số successors lân cận sẽ tương ứng với số tuyến đường đi tốt nhất và có giá trị đường đi bằng nhau.

Câu lệnh **Show ip eigrp traffic** hiển thị thông tin về số lượng các gói tin EIGRP đã được gửi và nhận.



Hình 7.22f: Câu lệnh Show ip eigrp traffic

Câu lệnh Debug eigrp fsm (Finite State Machines – FSM) hiển thị hoạt động của các EIGRP Feasible Successor giúp chúng ta xác định khi nào tiến trình định tuyến cài đặt và xóa thông tin cập nhật về đường đi

Hình 7.22g: Câu lệnh debug eigrp fsm

Câu lệnh debug eigrp packet hiển thị thông tin về các gói EIGRP gửi đi và nhận được. Các gói tin này có thể là gói hello, báo nhận, cập nhật, yêu cầu, đáp ứng. Số thự tự của gói và chỉ số báo nhận được sử dụng để bảo đảm các gói EIGRP được hiển thị.

3.3. Các tính năng nâng cao của EIGRP

3.3.1. Route Summarization – tổng hợp tuyến đường

.

Hình 7.23a: Tính năng tổng hợp tuyến đường trong EIGRP

Chế độ tự động tổng hợp các tuyến đường về dạng classful là đặc trưng của hoạt động định tuyến theo vectơ khoảng cách. Ở các giao thức vectơ khoảng cách truyền thông như RIPv1 đều là giao thức định tuyến dạng classful và không thể xác định lớp mặt nạ (mask) cho các mạng không kết nối trực tiếp, bởi vì nó không trao đổi lớp mặt nạ trong bản cập nhật định tuyến.

Trong hình 7.23a mạng 2.1.1.0/24 được kết nối trực tiếp với RTC, khi tuyến đường này được RTC quảng bá cho RTD đã được đưa về dạng classful với địa chỉ là 2.0.0.0/8.

Chế độ tổng hợp tuyến đường nhằm mục đích là làm cho dung lượng gói cập nhật định tuyến và bảng định tuyến nhỏ hơn nhằm tiết kiệm băng thông đường truyền và tăng tốc độ truyền tin. Tuy nhiên chúng ta có thể tắt chế độ này và tạo ra một hay nhiều tuyến đường tổng hợp trong mạng tại bất kỳ ranh giới của bit nào đó miễn là có một tuyến đường cụ thể tồn tại trong bảng định tuyến. Khi một tuyến đường cụ thể không còn tồn tại thì tuyến đường tổng hợp sẽ bị gỡ ra khỏi bảng định tuyến.

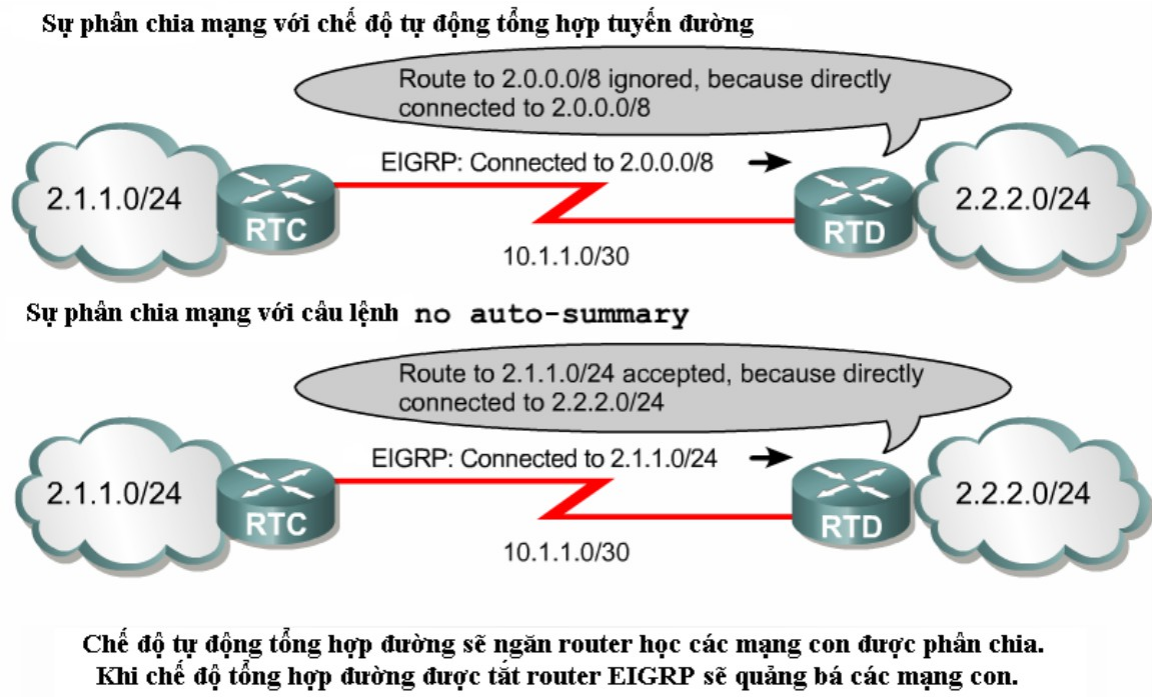
Giá trị metric nhỏ nhất của tuyến đường cụ thể sẽ được sử dụng làm metric của tuyến đường tổng hợp.

Giao diện (cổng) Null0: Khi thực hiện tổng hợp đường tự động hoặc cấu hình thủ công, thì router chạy EIGRP tự động sinh ra một tuyến đường trỏ đến Null0. Đây là cổng ảo, tác dụng của cổng Null0 chính là để ngăn định tuyến lặp. Trong trường hợp chúng ta tổng hợp đường một cách không tối ưu thì sẽ có tuyến Null0 để hỗ trợ.Các gói tin mà không trỏ đến mạng đó được thì sẽ có khả năng bị lặp quay ngược trở lại. Và ở đây tuyến Null0 đóng vai trò: Nếu tuyến gói tin đó đến không tồn tại thì gói tin sẽ bị đưa đến tuyến Null 0 và bị triệt tiêu.

Có hai chế độ tổng hợp đường là chế độ tổng hợp tự động (Automatic summarization) và chế độ tổng hợp thủ công (Manual summarization).

Mặc định chế độ tự động tổng hợp tuyến đường được bật cho EIGRP. Để
tắt chế độ này ta sử dụng câu lệnh no auto-summary

RouterA(config-router)#no auto-summary



Hình 7.23b

Trong hình 7.23b sau khi chế độ tự động tổng hợp tuyến đường được tắt router RTD bây giờ đã chập nhận các tuyến đường được quảng bá từ router RTC.

Để cấu hình thủ công chế độ tổng hợp tuyến đường ta sử dụng lệnh sau: Router(config-if)#ip summary-address eigrp autonomous-system-number ip-address mask [AD]

Giá trị của tham số AD trong lệnh sẽ được gán cho tuyến đường tổng hợp này. Giá trị này không bắt buộc phải cấu hình.

Hình 7.23c: Cấu hình thủ công chế độ tổng hợp tuyến đường trong EIGRP.

Trong hình 7.23c ta thấy mạng 2.1.1.0/24 khi được router RTC quảng bá đến router RTD đã được định tuyến bởi tuyến đường tổng hợp 2.1.0.0/16

Mặc định tuyến đường tổng hợp trên ở router RTC sẽ có giá trị là 5, trên router RTD sẽ có giá trị là 90.

3.3.2. Load Balancing – Cân bằng tải

3.3.2.1. Load Balancing Across Equal Cost Paths – Cân bằng tải trên những tuyến đường có cùng giá trị

Cân bằng tải cùng giá trị là khả năng của một bộ định tuyến để phân phối lưu lượng dữ liệu trên tất cả các cổng mạng của mình khi có cùng thông số định tuyến (metric) từ địa chỉ đích. EIGRP sẽ tự động cân bằng tải trên tuyến đường có giá trị bằng nhau.

Cân bằng tải làm tăng việc sử dụng các phân đoạn mạng và tăng hiệu quả sử dụng băng thông mạng.

Đối với IP, phần mềm Cisco IOS theo mặc định sẽ cài đặt tối đa bốn tuyến đường cùng giá trị trong bảng định tuyến cho hầu hết các giao thức định tuyến. Dòng lệnh maximum-paths maximum-path có thể được sử dụng để tăng số tuyến đường cùng giá trị lên sáu. (Thiết lập maximum-path là 1 đường sẽ vô hiệu hóa chế độ cân bằng tải.)

3.3.2.2 Load Balancing Across Unequal Cost Paths – Cân bằng tải trên những tuyến đường không cùng giá trị

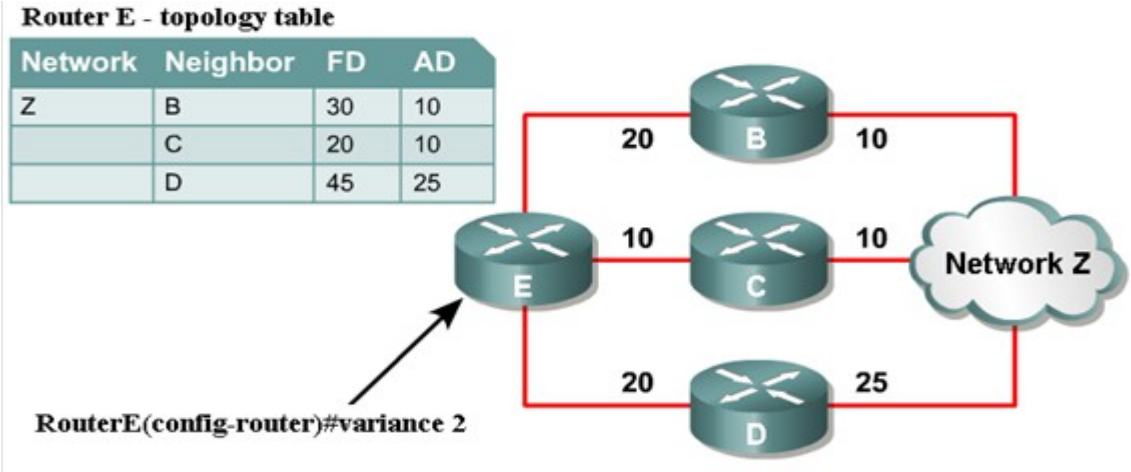
EIGRP cũng có thể cân bằng lưu lượng dữ liệu trên nhiều tuyến đường khác thông số định tuyến. Cấp độ mà EIGRP thực hiện cân bằng tải được điều khiển bằng câu lệnh variance

Router (config-router)# variance multiplier

Câu lệnh cho phép router thêm những tuyến đường có metric nhỏ hơn multiplier lần giá trị metric nhỏ nhất của tuyến đường tới đích.

Tham số multiplier có giá trị từ 1 đến 128, giá trị mặc định là 1 đồng nghĩa với việc router chạy chế độ cân bằng tải cùng giá trị.

Tham số multipier xác định phạm vi của giá trị metric được tiến trình EIGRP cho phép tham gia cân bằng tải.



Hình 7.24: Cân bằng tải trên những tuyến đường không cùng giá trị

Router E chọn con đường qua router C để đến mạng Z vì có giá trị FD

nhỏ nhất bằng 20.

Với giá trị variance bằng 2, router E tiếp tục chọn con đường đi qua router B để đến mạng Z vì có FD bằng 30 < [2*lowest FD = 2*20 = 40].

Router D không được lựa chọn vì có AD = 25 > 20.

Bài tập và sản phẩm thực hành bài 34.7

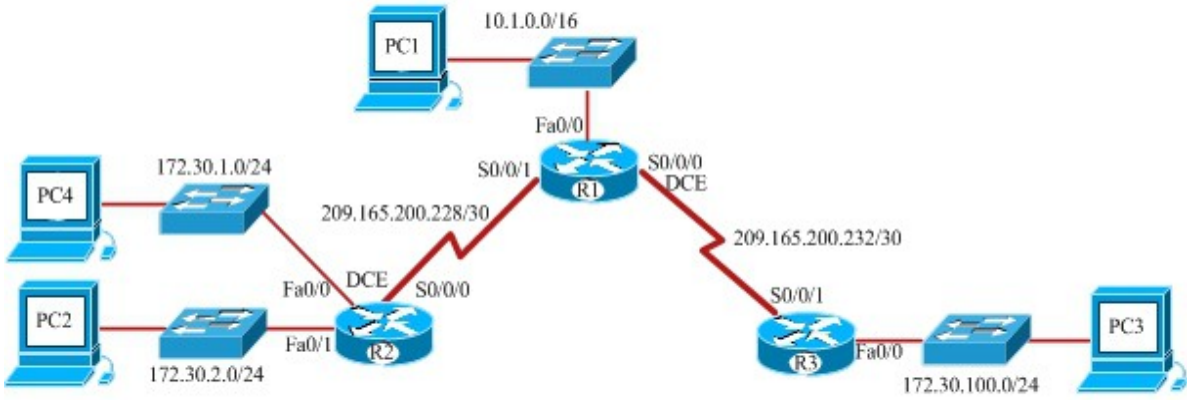
Kiến thức:

Câu 1: Trình bày các phương pháp đảm bảo cho các giao thức định tuyến theo vector khoảng cách định tuyến đúng?

Câu 2: So sánh sự khác nhau giữa Ripv1 và Ripv2?

Kỹ năng:

Bài tập ứng dụng: Thực hiện cấu hình định tuyến RIP trong hệ thống mạng bên dưới.



CHỈ DẪN ĐỐI VỚI HỌC SINH THỰC HIỆN BÀI TẬP ỨNG DỤNG

1. Kết nối cáp cho Router, PC, Switch như hình vẽ.
2. Thực hiện gán IP address, subnetmask, default gateway cho PC, gán IP address cho interface của router (nối với PC).
3. Cấu hình các thông số cơ bản cho router.
4. Thực hiện kiểm tra kết nối giữa PC-PC, PC-Router, Router-Router.
5. Cấu hình định tuyến Ripv1 trên router.
6. Kiểm tra thông tin bảng định tuyến và kết nối mạng.
6. Cấu hình định tuyến Ripv2 trên router.
8. Kiểm tra lại thông tin bảng định tuyến và kết nối mạng.
9. Thời gian:….. giờ (kể cả thời gian chuẩn bị và cấu hình)
10. Tổng điểm và kết cấu điểm của các bài như sau:

    Tổng số điểm tối đa cho bài: 100 điểm, kết cấu như sau:

    a, Điểm ngoại dạng khách quan: Tổng cộng 70 điểm

    b, Điểm tuân thủ các qui định: 30 điểm

- Thời gian thực hiện bài tập vượt quá 25% thời gian cho phép sẽ không được đánh giá.

- Thí sinh phải tuyệt đối tuân thủ các qui định an toàn lao động, các qui định của phòng thực hành, nếu vi phạm sẽ bị đình chỉ thực tập

BÀI 8: THÔNG ĐIỆP ĐIỀU KHIỂN VÀ BÁO LỖI CỦA TCP/IP
Mà bài: MĐ34-08

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.

Mục tiêu:

- Mô tả ICMP.
- Mô tả cấu truc 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 các loại thông điệp điều khiển ICMP được sử dụng trong mạng ngày nay.
- Thực hiện các thao tác an toàn với máy tính.

Nội dung:

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

Mục tiêu:

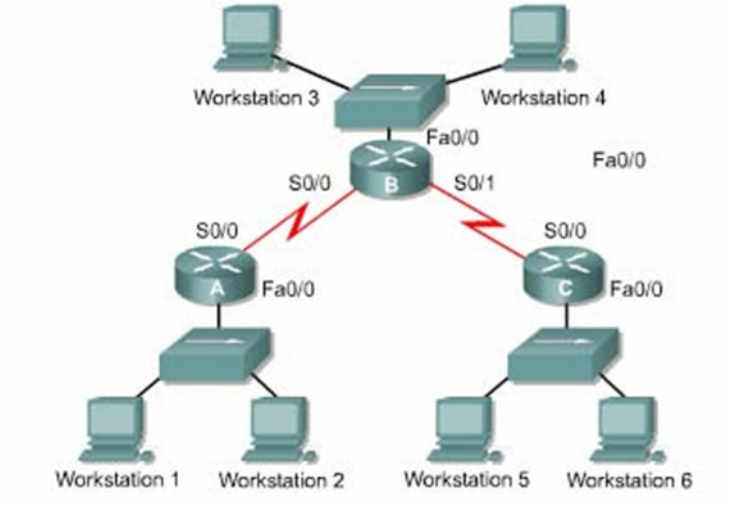
- Mô tả ICMP.
- Mô tả cấu truc thông điệp ICMP.
- Xác định loại thông điệp báo lỗi ICMP.
- Xác định nguyên nhân liên quan đến từng loại thông điệp báo lỗi ICMP.

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.

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 8.1* 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 8.1

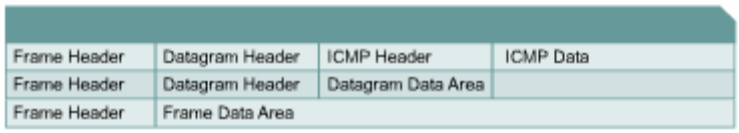
Router C nhận được gói dữ liệu từ Máy 1, nó chỉ biết được địa chỉ IP

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.

1.3. Truyền thông điệp ICMP

Thông điệp ICMP được đóng gói giống như các dữ liệu khác khi truyền đi bằng IP. Hình 8.2 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.



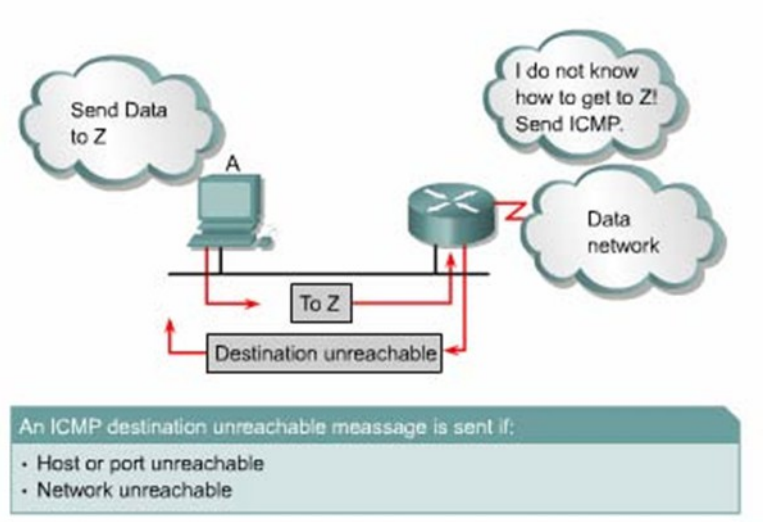
Hình 8.2

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 8.3 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 .

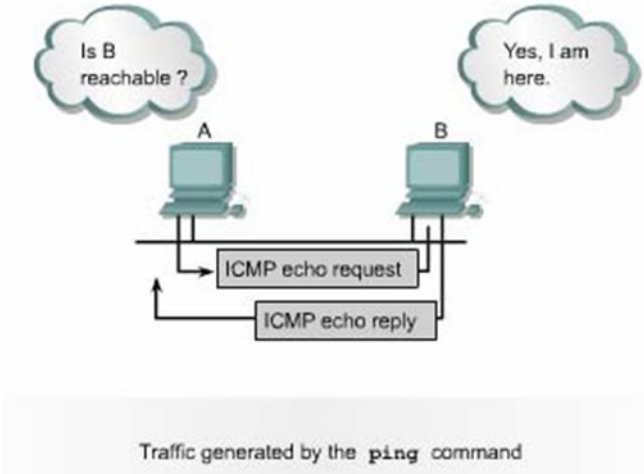


Hình 8.3

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 khẳng 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 8.4a và 8.4b ,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 8.4a

Hình 8.4b

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 .

1.7. Thông điệp echo

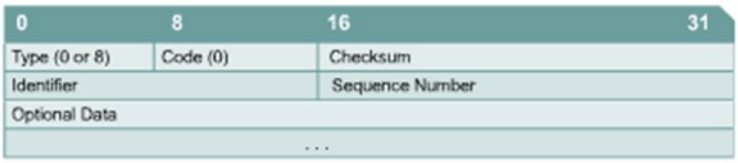
Như bất kỳ các loại gói dữ liệu khác ,thông điệp ICMP cũng có định dạng riêng .Mỗi một loại thông điệp ICMP có một đặc điểm riêng nhưng tất cả các gói ICMP đều bắt đầu bằng 3 phần :

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 8.5a 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 8.5a

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

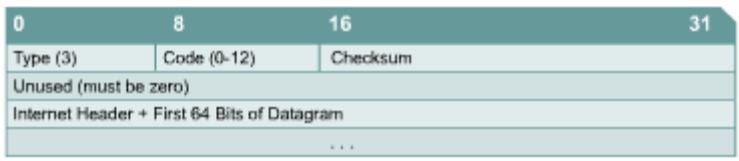
Hình 8.5b

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 8.6a 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 8.6a

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 8.6b

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".

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 8.7 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 8.6

2. Thông điệp điều khiển của TCP/IP

Mục tiêu:

- Mô tả thông điệp điều khiển ICMP.
- Xác định được các loại thông điệp điều khiển ICMP được sử dụng trong mạng ngày nay.
- Xác định nguyên nhân liên quan đến thông điệp điều khiển ICMP.

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	
3	Destination Unreachable
8	Echo Request
10	Router Selection
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply

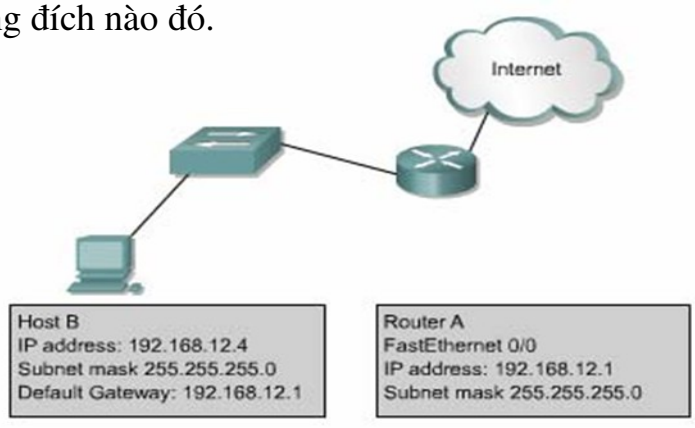
Hình 8.8

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 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 8.8.

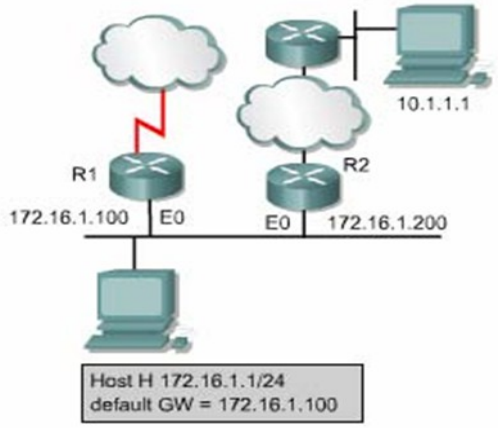
2.2. Thông điệp ICMP redirect/change request

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 8.9a ,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 ost biết về một gateway khác tốt hơn để đến một mạng đích nào đó.



Hình 8.9a

Trong hình 8.9b 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 8.9b

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 .

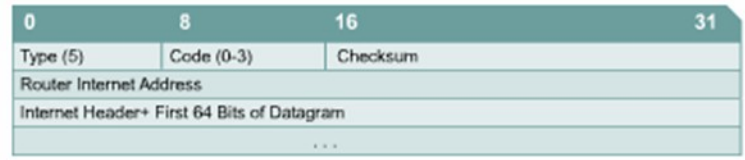
Con đường mà router thực hiện thông báo cho host không phải là đường mặc định của router và cũng không phải là của một ICMP redirect nào khác.

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 8.9c. 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			
. . .			

8.9c

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.

8.9d

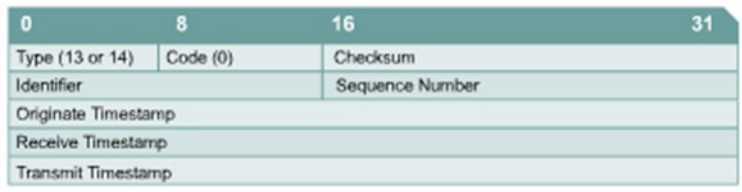
2.3. Đồng bộ đồng hồ và ước tính thời gian truyền dữ liệu

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).



0	8	16	31
Type (13 or 14)	Code (0)	Checksum	
Identifier		Sequence Number	
Originate Timestamp			
Receive Timestamp			
Transmit Timestamp			

Hình 8.10

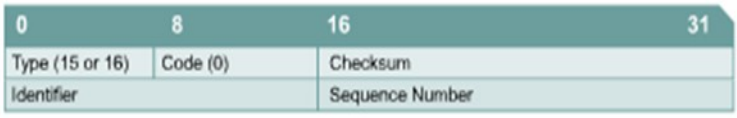
Tất cả các thông tin ICMP timestamp reply đều có đầy đủ 3 thông số :thời điểm gửi gói request ,thời điểm nhận được request và thời điểm gửi gói reply .Dựa vào 3 thông số này host có thể ước lượng được khoảng thời gian dữ liệu truyền trên mạng từ máy nguồn đến máy đích bằng cách lấy giá trị

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.

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 8.11 là cấu trúc của loại thông điệp này.



Hình 8.11

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.

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

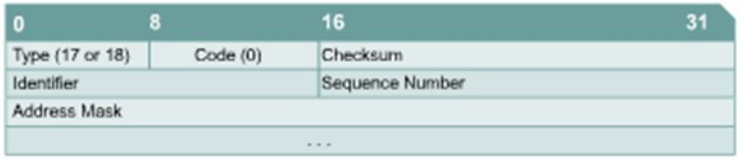
Protocol :ICMP =-1

Type :Address

Mask Request =AM2 Code :0

Mask:255.255.255.0

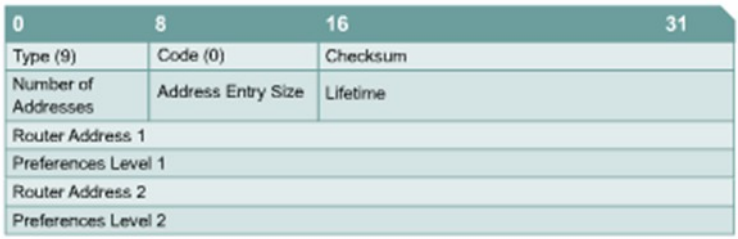
Cấu trúc của thông điệp Address Mask Request và reply được thể hiện ở hình 8.12. Thông điệp Address Mask Request và reply có cấu trúc hoàn toàn như nhau ,chỉ khác nhau giá trị phần Type .Phần Type có giá trị 17 là tương ứng với request ,còn giá trị 18 là tương ứng với reply .Phần Identifier và Sequênc 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 8.12

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 8.13.



Hình 8.13

2.7. Thông điệp Router solicitation

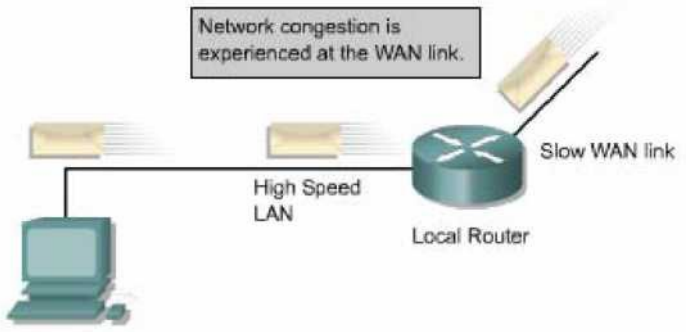
Host gửi thông điệp Router solicitation trong trường hợp bị mất Default gateway.Thông điệp này được gửi multicast và đây chính là bước đầu tiên của quá trình tìm router đã đề cập ở phần 8.13 .Router sẽ trả lời lại bằng thông điệp Router Advertisement,trong đó có cung cấp Default gateway cho host .Hình 8.14 là cấu trúc của thông điệp Router solicitation:

Hình 8.14

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 8.15

TÀI LIỆU THAM KHẢO

[1]. Nguyễn Hồng Sơn, Hoàng Đức Hải, Giáo trình hệ thống mạng máy tính
, Nhà xuất bản Lao động - Xã hội, 2006.

[2]. Đặng Quang Minh. Bùi Nguyễn Hoàng Long. Phạm Đình, CCNA Labpro 2012, Nhà xuất bản Thông tin và truyền thông, 2012.

[3]. Wendell Odom, CCNA Official Exam Certification Library, Cisco Press, 2007.

[4]. Todd Lammle, CCNA: Cisco® Certified Network Associate Study Guide, Wiley, 2007.