CHƯƠNG 1: GIỚI THIỆU VỀ MẠNG DIỆN RỘNG

1.1. Giới thiệu về WAN

WAN (Wide Area Network) là mạng được thiết lập để liên kết các máy tính của hai hay nhiều khu vực khác nhau cách xa về mặt địa lý. Các WAN kết nối các mạng người sử dụng qua một phạm vi địa lý rộng lớn, nên chúng mở ra khả năng cung ứng hoạt động thông tin cự ly xa cho doanh nghiệp. Sử dụng WAN cho phép các máy tính, máy in và các thiết bị khác trên một LAN chia sẻ và được chia sẻ với các vị trí ở xa. WAN cung cấp truyền thông tức thời qua các miền địa lý rộng lớn. Khả năng truyền một thông điệp đến một ai đó ở bất cứ nơi đâu trên thế giới tạo ra một khả năng truyền thông tương tự như dạng truyền thông giữa hai người ở tại một vị trí địa lý. Phần mềm chức năng cung cấp truy xuất thông tin và tài nguyên thời gian thực cho phép hội họp được tổ chức từ xa. Thiết lập mạng diện rộng tạo ra một lớp nhân công mới được gọi là telecommuter, đó là những người làm việc mà chẳng bao giờ rời khỏi nhà. Các WAN được thiết kế để làm các công việc sau:

Hoạt động qua các vùng tách biệt về mặt địa lý.

Cho phép các người sử dụng có khả năng thông tin thời gian thực với người sử dụng khác.

Cung cấp các kết nối liên tục các tài nguyên xa vào các dịch vụ cục bộ.

Cung cấp Email, www, FTP và các dịch vụ thương mại điện tử.

Các công nghệ WAN phổ biến bao gồm:

Modem

ISDL

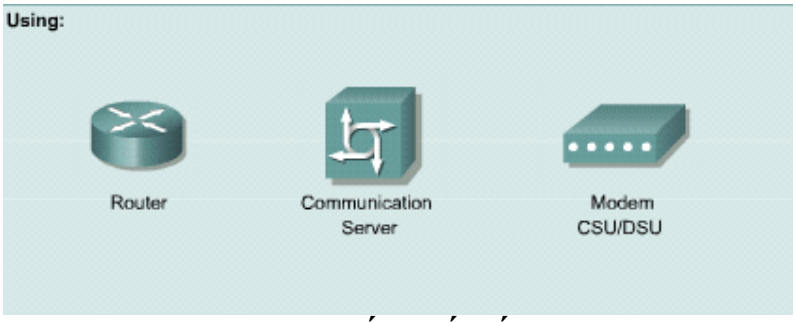
DSL

Frame Relay

Các đường truyền dẫn số theo chuẩn Bắc Mỹ và châu Âu T1, E1, T3, E3

Mạng quang đồng bộ SOả ET.

Các thiết bị WAN bao gồm:



Hình 1.1. Các thiết bị kết nối trong WAN

1.2. Các thiết bị kết nối WAN

1.2.1. Lớp vật lý của WAN

Các thực hiện thực tế lớp vật lý thay đổi tùy vào khoảng cách thiết bị đến dịch vụ, tốc độ và chính bản than dịch vụ. Các kết nối nối tiếp được dùng để hỗ trợ các dịch vụ WAả như các đường dây thuê riêng chạy PPP hay Frame Relay. Tốc độ của các kết nối này trong dải từ 2400 bps đến T1 tốc độ 1,544 Mbps và E1 tốc độ 2,048 Mbps.

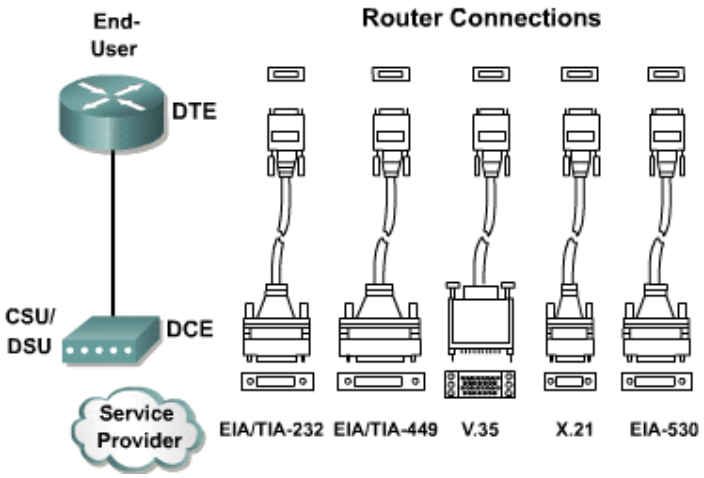
ISDả cung cấp dịch vụ quay số theo yêu cầu. Một dịch vụ giao tiếp tốc độ cơ bản (BRI) được cấu thành từ hai kênh truyền dẫn 64 kbps (kênh B)cho số liệu và một kênh delta tốc độ 16kbps (kênh D) được dùng cho báo hiệu và các tác vụ quản lý liên kết khác. PPP thường được dùng để truyền dẫn số liệu qua kênh D.

Với sự ra tăng nhu cầu về dịch vụ tốc độ cao, băng thông rộng trong khu vực dân cư, các kết nối DSL và modem cáp đang được phổ dụng hơn.

1.2.2. Các kết nối WAN nối tiếp

Trong truyền thông đường dài, các WAả dùng dạng đường dẫn nối tiếp. Đây là quá trình truyền bit số liệu nối tiếp nhau qua một kênh đơn. Tiến trình này cung ứng truyền thông đường dài tin cậy hơn và dùng dải tần số ánh sáng hay điện tử đặc biệt. Các tần số được đo theo số chu kỳ trong một giây và được biểu diễn theo Hz. Kích thước của dải tần được xem như là băng thông và được đo theo số bit được truyền trong một giây. Đối với một Cisco router, kết nối vật lý ở phía khách hàng được cung cấp bởi một hay hai loại kết nối nối tiếp. ả ếu kết nối được nối trực tiếp với nhà cung cấp dịch vụ hay một thiết bị cung cấp tín hiệu định thời như CSU/DSU (Channel Service Unit/Data Service Unit), thì router sẽ là một thiết bị đầu cuối

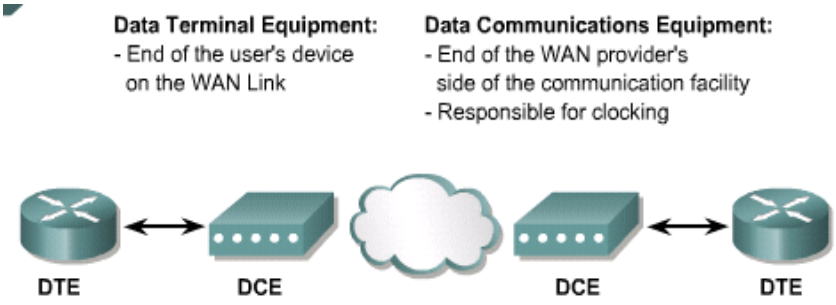
(DTE) và dùng cáp DTE. Tuy nhiên, có một số trường hợp mà router cục bộ được yêu cầu cung cấp tín hiệu định thời và do đó sẽ dùng cáp DCE.



Hình 1.2. Các kết nối WAN nối tiếp

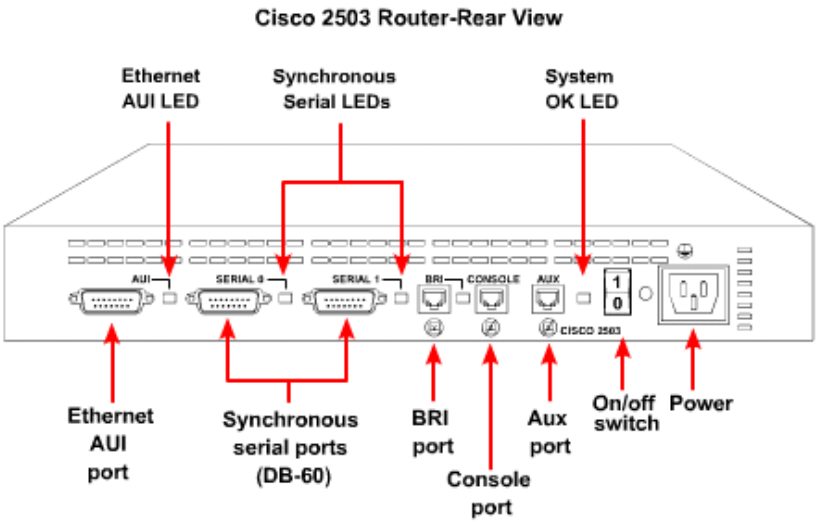
1.2.3. Router và các kết nối nối tiếp

Các router chịu trách nhiệm định tuyến các gói dữ liệu từ nguồn đến đích trong một LAả và để cung cấp kết nối đến WAả . Trong môi trường LAả router chứa broadcast, cung cấp dịch vụ phân dải địa chỉ cục bộ như ARP, RARP và có thể chia mạng bằng cách dùng cấu trúc mạng con. Để cung ứng các dịch vụ này router phải được kết nối LAả và WAả .



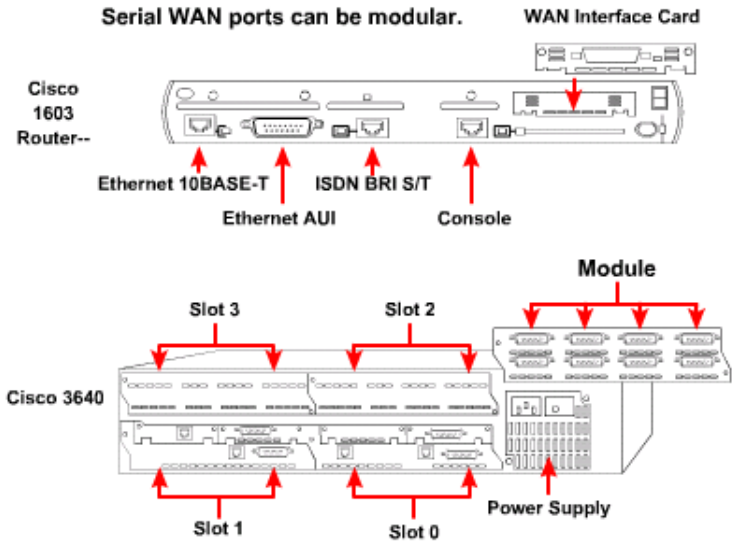
Hình 1.3.1. Kết nối nối tiếp của DTE và DCE

ả hằm xác định loại cáp, cần phải xác định các đầu nối là DTE hay DCE. DTE là điểm của thiết bị người sử dụng trên một liên kết WAả . DCE là một điểm thông thường chịu trách nhiệm chuyển giao số liệu đến nhà cung cấp dịch vụ. Khi nối cáp loại nối tiếp cho router, router sẽ có các port cố định hay gắn linh động (modular port). Các giao tiếp trên router là cố định được đánh nhãn theo loại port và chỉ số port.



Hình 1.3.2 Các giao tiếp cố định

Các giao tiếp trên router là linh động được ghi nhãn theo loại port, khe (slot) và chỉ số port. Khe là vị trí của module. Để cấu hình một port trên một card rời, cần phải chỉ ra giao tiếp bằng cách dùng cú pháp "port type slot number/port number". Dùng nhãn "serial 0/1" khi giao tiếp là nối tiếp, chỉ số khe nơi module được gắn vào là 1 và port đang được tham chiếu đến là 0.

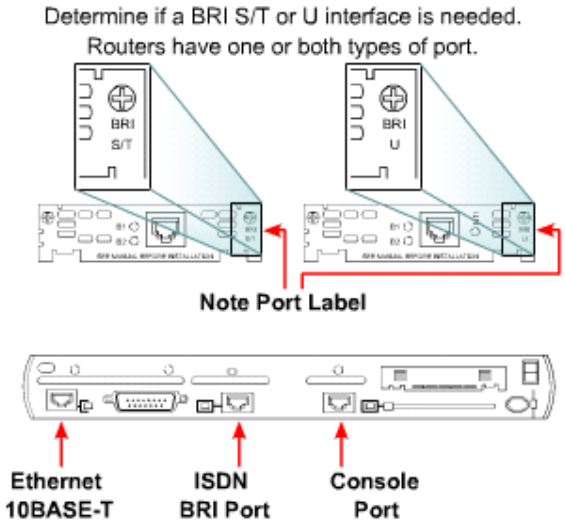


Hình 1.3.3. Các giao tiếp serial port dạng module

1.2.4. Router và các kết nối ISDN BRI

Với ISDả BRI, hai loại giao tiếp có thể được dùng là BRI/S và BRI/U. Xác định ai đang cung cấp thiết bị kết cuối mạng ả T1 để xác định loại giao tiếp cần. ả T1 là một thiết bị trung gian nằm giữa router và tổng đài ISDả của nhà cung cấp

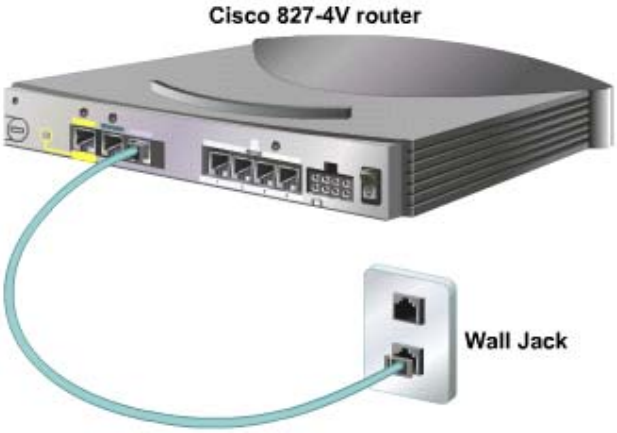
dịch vụ. Để kết nối port ISDẩ BRI đến thiết bị của nhà cung cấp dịch vụ dùng cáp UTP Cat 5 straight-through. Lưu ý, chỉ gắn cáp nối từ ISDẩ BRI port vào một ISDẩ jack hay một tổng đài ISDẩ .



Hình 1.3.4. Nối cáp trên router cho một cầu nối ISDN

1.2.5. Router và các kết nối DSL

Để nối router với dịch vụ DSL, dùng một cáp điện thoại với đầu nối RJ-11. DSL làm việc qua các đường dây điện thoại chuẩn dùng chân 3 và 4 trên đầu nối RJ-11.



Hình 1.5. Kết nối router cho dịch vụ DSL

1.2.6. Thực hiện một kết nối console

Để bắt đầu cấu hình một thiết bị của Cisco, một kết nối quản trị phải được thực hiện trực tiếp đến các thiết bị qua cổng console của thiết bị. Cổng cosonle cho phép giám sát và cấu hình một Cisco hub, switch hay router. Cáp được dùng giữa đầu cuối và cổng console là cáp đảo (rollover cable). Kết nối các thiết bị bằng cáp đảo từ cổng console đến cổng nối tiếp của máy tính làm đầu cuối (cổng COM) sau đó cấu hình ứng dụng mô phỏng đầu cuối với các thông số cài đặt cho cổng nối tiếp (COM) của máy tính như sau:

Speed: 9600 bps

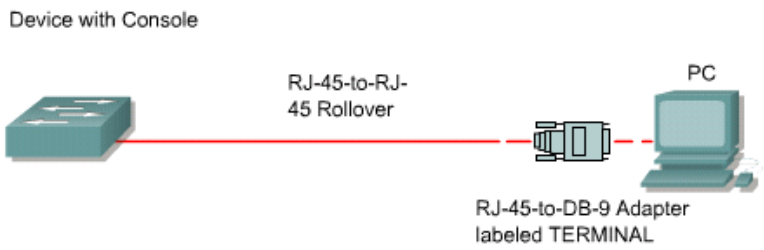
Format: 8 data bit

Parity: no

Stop bits: 1

Flow control: no

Cổng AUX được dùng để cung cấp sự quản lý thông qua modem. Cổng AUX cũng được cấu hình theo cách thức cổng console.



Hình 1.6. Thiết lập một kết nối qua cổng console

1.3. Router trong WAN

Router là một loại máy tính đặc biệt. ả ó cũng có các thành phần cơ bản giống như máy tính: CPU, bộ nhớ, hệ thống Bus và các cổng giao tiếp. Tuy nhiên router được thiết kế để kết nối hai hệ thống mạng và cho phép hai hệ thống này có thể liên lạc với nhau, ngoài ra router còn thực hiện việc chọn đường đi tốt nhất cho dữ liệu. Các thành phần chính bên trong router bao gồm: bộ nhớ RAM, ả VRAM, bộ nhớ flash, ROM và các cổng giao tiếp.

Đặc điểm và chức năng của RAM:

Lưu bảng định tuyến

Lưu bảng ARP

Có vùng bộ nhớ chuyển mạch nhanh

Cung cấp bộ 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 khi router đang hoạt động

Thông tin trên RAM sẽ bị xóa khi router khởi động lại hay mất điện

Đặc điểm và chức năng của NVRAM:

Lưu giữ tập tin cấu hình khởi động của router

ẩ ội dung tập tin vẫn được lưu giữ khi khởi động lại router

Đặc điểm và chức năng của ROM:

Lưu giữ các câu lệnh của chương trình tự kiểm tra khi khởi động _POST (Power-on Self Test)

Lưu chương trình bootstrap và hệ điều hành cơ bản

Để nâng cấp phần mềm trong ROM thì phải thay chip trên mainboard

Đặc điểm và chức năng của cổng giao tiếp:

Kết nối Router vào hệ thống mạng để nhận và chuyển gói dữ liệu

Các cổng có thể được gắn trực tiếp trên mainboard hay dưới dạng card rời

1.4 Đặc điểm vật lý của Router

Cấu trúc của các router rất khác nhau tùy vào từng phiên bản bao gồm các thành phần sau:

CPU – Đơn vị xử lý trung tâm: thực thi các câu lệnh của hệ điều hành để thực hiện các nhiệm vụ như: khởi động hệ thống, định tuyến, điều khiển các cổng giao tiếp mạng.

RAM: Được dùng 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. RAM được chia thành hai phần: phần bộ nhớ xử lý chính và bộ nhớ chia sẻ xuất/nhập. Toàn bộ nội dung trên RAM sẽ bị xóa khi mất điện.

Flash: Bộ nhớ Flash được sử dụng để lưu toàn bộ hệ điều hành Cisco IOS. Mặc định router tìm IOS của nó trong flash.

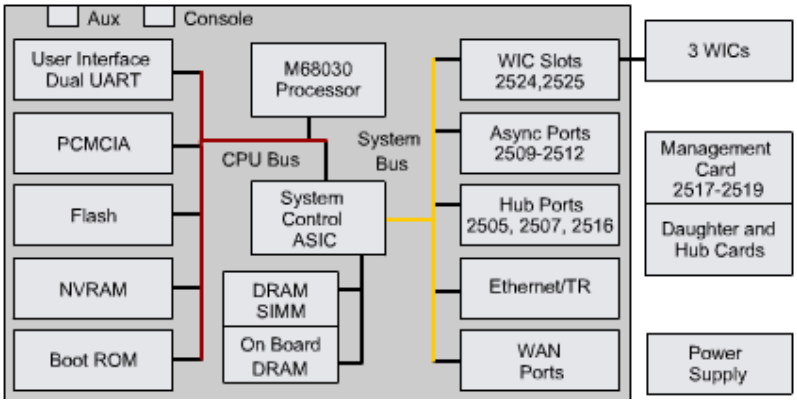
NVRAM (None-volative Random-access Memory): Là bộ nhớ RAM không bị mất thông tin khi mất điện, được sử dụng để lưu tập tin cấu hình.

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.

CPU sử dụng CPU bus để truy xuất các thành phần của router thông qua bộ nhớ trên router.

ROM (Read Only Memory): Là nơi lưu đoạn mã của chương trình kiểm tra khi khởi động. ả hiệm 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.

Các cổng giao tiếp: Là nơi router kết nối với bên ngoài. Router có ba loại cổng: LAả , WAả và console. Cổng giao tiếp LAả thường là cổng Ethernet hoặc Token Ring. Cổng giao tiếp WAả có thể là cổng Serial, ISDả , cổng tích hợp đơn vị dịch vụ kênh CSU (Channel Service Unit). Cổng console/AUX là cổng giao tiếp chủ yếu được sử dụng để cấu hình router.



Hình 1.8. Cấu trúc vật lý của router

1.5 Vai trò của Router trong WAN

Chức năng chủ yếu của router là định tuyến. Hoạt động định tuyến diễn ra ở Lớp 3, cung cấp kết nối giữa các mạng WAả với các chuẩn vật lý và liên kết dữ liệu khác nhau. Ví dụ: một router có thể có một giao tiếp ISDả 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 loại dịch vụ khác. Ví dụ: chuyển đổi từ dịch vụ ISDả sang dạng T1, đồng thời chuyển kiểu đóng gói lớp Liên kết dữ liệu từ PPP sang FrameRelay.

CHƯƠNG 2. CẤU HÌNH ROUTER

2.1 Khái niệm về cấu hình Router.

Cấu hình router là sử dụng các phương pháp khác nhau để định cấu hình cho router thực hiện các chức năng cụ thể: liên kết leased line, liên kết dial-up, firewall, Voice Over IP… trong từng trường hợp cụ thể.

Đối với Cisco Router thường có 03 phương pháp để định cấu hình cho router:

- **Sử dụng CLI:**

CLI là chữ viết tắt của Command Line Interface, là cách cấu hình cơ bản áp dụng cho hầu hết các thiết bị của Cisco. ẩ gười sử dụng có thể dùng các dòng lệnh nhập từ các Terminal (thông qua port Console hay qua các phiên Telnet) để định cấu hình cho Router.

- **Sử dụng Chương trình ConfigMaker:**

ConfigMaker là chương trình hỗ trợ cấu hình cho các Router từ 36xx trở xuống của Cisco. Chương trình này cung cấp một giao diện đồ họa và các Wizard thân thiện, được trình bày dưới dạng "Question – Answer", giúp cho việc cấu hình router trở nên rất đơn giản.

ẩ gười sử dụng có thể không cần nắm vững các câu lệnh của Cisco mà chỉ cần một kiến thức cơ bản về hệ thống là có thể cấu hình được router. Tuy nhiên ngoài hạn chế về số sản phẩm router hỗ trợ như ở trên, chương trình này cũng không cung cấp đầy đủ tất cả các tính năng của router và không có khả năng tuỳ biến theo các yêu cầu cụ thể đặc thù.

Hiện nay version mới nhất của ConfigMaker là ConfigMaker 2.4.

- **Sử dụng chương trình FastStep:**

Khác với chương trình ConfigMaker, FastStep được cung cấp dựa trên từng loại sản phẩm cụ thể của Cisco. Ví dụ như với Cisco router 2509 thì có FastStep for Cisco Router 2509… Chương trình này cung cấp các bước để cấu hình các tính năng cơ bản cho từng loại sản phẩm. Các bước cấu hình cũng được trình bày dưới dạng giao diện đồ họa, "Question – Answer" nên rất dễ sử dụng. Tuy vậy cũng như chương trình ConfigMaker, FastStep chỉ mới hỗ trợ cho một số sản phẩm cấp thấp của Cisco và chỉ giúp cấu hình cho một số chức năng cơ bản của router.

Tóm lại, việc sử dụng CLI để cấu hình Cisco Router tuy phức tạp nhưng vẫn là cách cấu hình router thường gặp nhất. Hiểu biết việc cấu hình bằng CLI sẽ giúp người sử dụng linh hoạt trong việc cấu hình và dễ dàng khắc phục sự cố. Hiện nay việc sử dụng CLI có thể kết hợp với một trong 02 cách cấu hình còn lại để đẩy nhanh tốc độ cấu hình router. Khi đó, các chương trình cấu hình sẽ sử dụng để tạo các file cấu hình thô, phương pháp CLI sẽ được sử dụng sau cùng để tùy biến hay thực hiện các tác vụ mà chương trình không thực hiện được.

Trong tài liệu này các hướng dẫn cấu hình đều là phương pháp CLI – phương pháp dùng dòng lệnh.

2.2 Cấu trúc router.

Cấu trúc router là một trong các vấn đề cơ bản cần biết trước khi cấu hình router. Cấu trúc của router được trình bày trong hình 2.1.

Các thành phần chính của router bao gồm:

 ẩ VRAM:

ẩ VRAM (ẩ onvolatile random-access memory) là loại RAM có thể lưu lại thông tin ngay cả khi không còn nguồn nuôi. Trong Cisco Router ẩ VRAM thường có nhiệm vụ sau:

- Chứa file cấu hình startup cho hầu hết các loại router ngoại trừ router có Flash file system dạng Class A. (7xxx)
- Chứa Software configuration register, sử dụng để xác định IOS image dùng trong quá trình boot của router.

 Flash memory:

Flash memory chứa Cisco IOS software image. Đối với một số loại, Flash memory có thể chứa các file cấu hình hay boot image..

Tùy theo loại mà Flash memory có thể là EPROMs, single in-line memory (SIMM) module hay Flash memory card:

- Internal Flash memory:
  - Internal Flash memory thường chứa system image.
  - Một số loại router có từ 2 Flash memory trở lên dưới dạng single in-line memory modules (SIMM). ẩ ếu như SIMM có 2 bank thì được gọi là *dual-bank Flash memory*. Các bank này có thể được phân thành nhiều phần logic nhỏ
- Bootflash
  - Bootflash thường chứa boot image.
  - Bootflash đôi khi chứa ROM Monitor.
- Flash memory PC card hay PCMCIA card.
  Flash memory card dủng để gắn vào Personal Computer Memory Card International Association (PCMCIA) slot. Card này dùng để chứa system image, boot image và file cấu hình.

  Các loại router sau có PCMCIA slot:
  - Cisco 1600 series router: 01 PCMCIA slot.
  - Cisco 3600 series router: 02 PCMCIA slots.
  - Cisco 7200 series ẩ etwork Processing Engine (ẩ PE): 02 PCMCIA slots
  - Cisco 7000 RSP700 card và 7500 series Route Switch Processor (RSP) card chứa 02 PCMCIA slots.

 DRAM:

Dynamic random-access memory (DRAM) bao gom 02 loại:

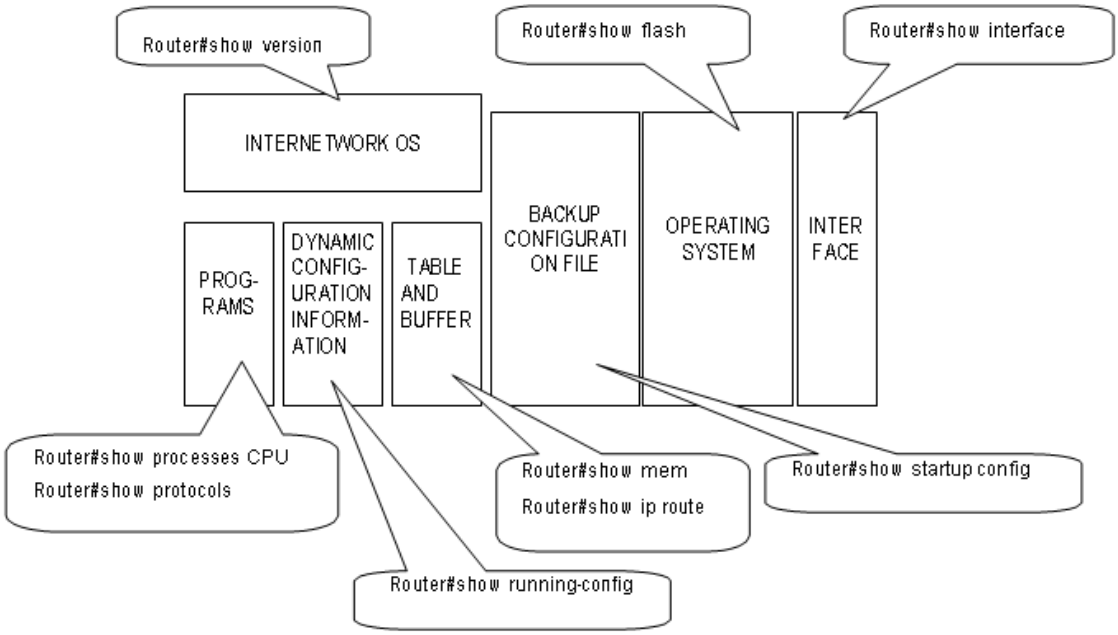
- Primary, main, hay processor memory, dành cho CPU dùng để thực hiện Cisco IOS software và lưu giữ running configuration và các bảng routing table.
- Shared, packet, or I/O memory, which buffers data transmitted or received by the router's network interfaces.

Tùy vào IOS và phần cứng mà có thể phải nâng cấp Flash RAM và DRAM.

 ROM

Read only memory (ROM) thường được sử dụng để chứa các thông tin sau:

- ROM monitor, cung cấp giao diện cho người sử dung khi router không tìm thấy các file image không phù hợp.
- Boot image, giúp router boot khi không tìm thấy IOS image hợp lệ trên flash memoty.



Hình 2.1

2.3 Các mode config

Cisco router có nhiều chế độ (mode) khi config, mỗi chế độ có đặc điểm riêng, cung cấp một số các tính năng xác dịnh để cấu hình router. Các mode của Cisco router được trình bày trong hình 2.2.

- User Mode hay User EXEC Mode:

Đây là mode đầu tiên khi bạn bắt đầu một phiên làm việc với router (qua Console hay Telnet). Ở mode này bạn chỉ có thể thực hiện được một số lệnh thông thường của router. Các lệnh này chỉ có tác dụng một lần như lệnh **show** hay lệnh **clear** một số các counter của router hay interface. Các lệnh này sẽ không được ghi vào file cấu hình của router và do đó không gây ảnh hưởng đến các lần khởi động sau của router.

- Privileged EXEC Mode:

Để vào Privileged EXEC Mode, từ User EXEC mode gõ lệnh **enable** và password (nếu cần). Privileged EXEC Mode cung cấp các lệnh quan trọng để theo dõi hoạt động của router, truy cập vào các file cấu hình, IOS, đặt các password… Privileged EXEC Mode là chìa khóa để vào Configuration Mode, cho phép cấu hình tất cả các chức năng hoạt động

của router.

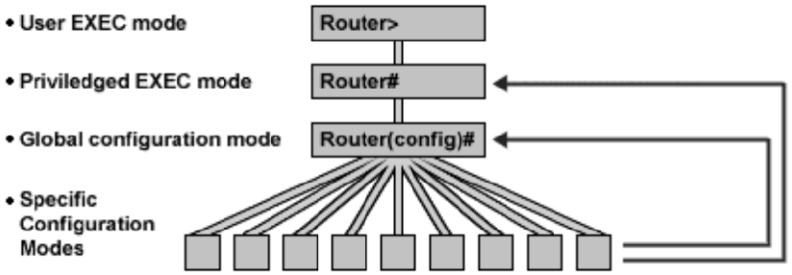
- Configuration Mode:

ả hư trên đã nói, configuration mode cho phép cấu hình tất cả các chức năng của Cisco router bao gồm các interface, các routing protocol, các line console, vty (telnet), tty (async connection). Các lệnh trong configuration mode sẽ ảnh hưởng trực tiếp đến cấu hình hiện hành của router chứa trong RAM (running-configuration). ả ếu cấu hình này được ghi lại vào ả VRAM, các lệnh này sẽ có tác dụng trong những lần khởi động sau của router.

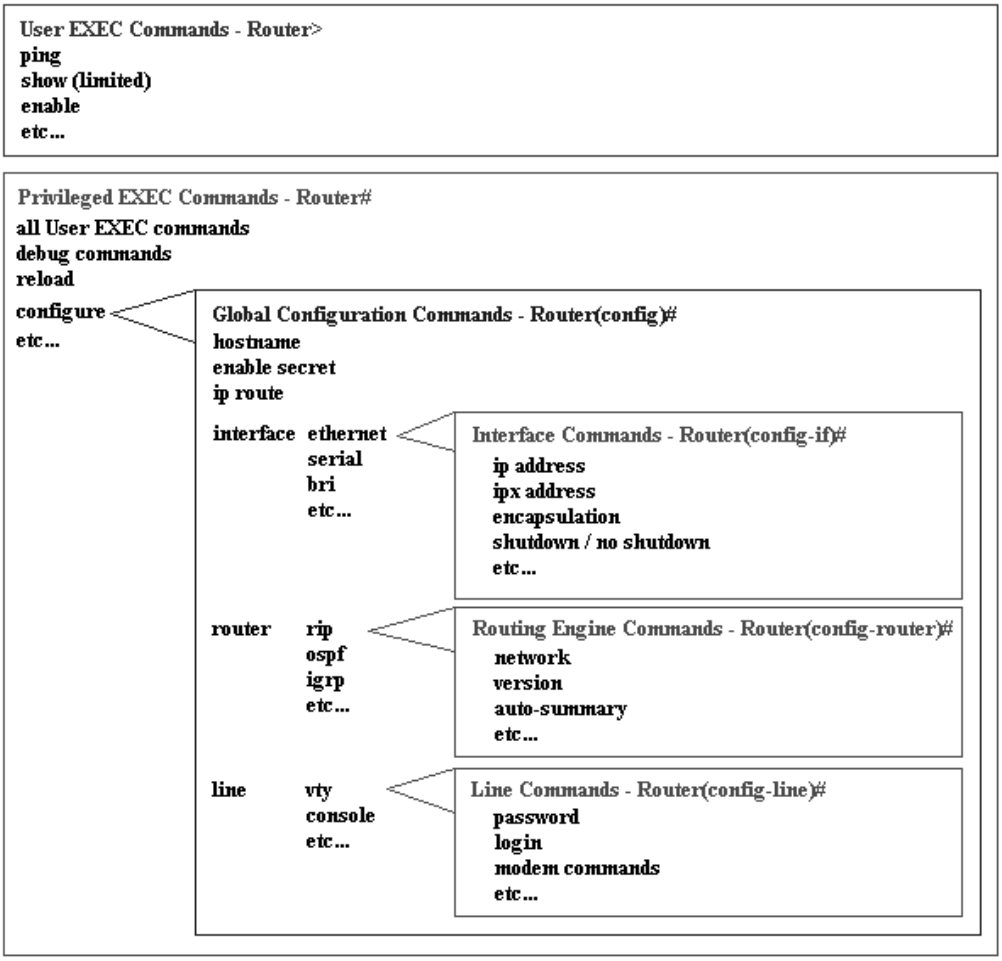
Configurarion mode có nhiều mode nhỏ, ngoài cùng là global configuration mode, sau đó là các interface configration mode, line configuration mode, routing configuration mode.

- ROM Mode

ROM mode dùng cho các tác vụ chuyên biệt, can thiệp trực tiếp vào phần cứng của router như Recovery password, maintenance. Thông thường ngoài các dòng lệnh do người sử dụng bắt buộc router vào ROM mode, router sẽ tự động chuyển vào ROM mode nếu không tìm thấy file IOS hay file IOS bị hỏng trong quá trình khởi động.



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 2.2: Một số mode config của Cisco Router

Bảng 2.1 trình bày các mode cơ bản của Cisco router và một số đặc điểm của chúng:

Mode	Cách thức truy cập	Dấu nhắc	Cách thức thoát
User EXEC	Log in.	Router>	**logout** command.
Privileged EXEC	Từ user EXEC mode, sử dụng lệnh **enable.**	Router#	Để trở về user EXEC mode, dùng lệnh **disable.**. Để vào global configuration mode, dùng lệnh **configure terminal.**
Global configuration	Từ privileged EXEC mode, dùng lệnh **configure terminal**	Router(config)#	Để ra privileged EXEC mode, dùng lệnh **exit** hay **end** hay gõ **Ctrl-Z**. Để vào interface configuration mode, gõ lệnh **interface.**

Interface configuration	Từ global configuration mode, gõ lệnh **interface**.	Router(config-if)#	Để ra global configuration mode, dùng lệnh **exit** Để ra privileged EXEC mode, dùng lệnh **exit** hay gõ **Ctrl-Z.** Để vào subinterface configuration mode, xác định subinterface bằng lệnh **interface**
Subinterface configuration	Từ interface configuration mode, xác định subinterface bằng lệnh **interface.**	Router(config-subif)#	To exit to global configuration mode, use the exit command. To enter privileged EXEC mode, use the end command or press Ctrl-Z.
ROM monitor	Từ privileged EXEC mode, dùng lệnh **reload** nhấn phím Break trong 60s khi router khởi động Dùng lệnh **boot system rom.**	>	Để ra user EXEC mode, gõ lệnh **continue**

2.3 Cấu hình các tính năng chung của router.

2.3.1 Một số quy tắc về trình bày câu lệnh.

Các quy tắc trình bày tại bảng sau được sử dụng trong tài liệu này cũng như trong tất cả các tài liệu khác của Cisco

Cách trình bày	**Ý nghĩa**
^ hay Ctrl	Phím Ctrl.
Screen	Hiểm thị các thông tin sẽ được trình bày trên màn hình.
Boldface	Hiển thị các thông tin (dòng lệnh) mà bạn phải nhập vào từ bàn phím.
< >	Biểu hiện các ký tự không hiển thi trên màn hình, ví dụ như password.
!	Biểu hiện các câu chú thích.
( )	Biểu hiện dấu nhắc hiện tại
[ ]	Biểu hiện các tham số tùy chọn (không bắt buộc) cho câu lệnh.
Italics	Biểu hiện các tham số của dòng lệnh. Các tham số này là bắt buộc phải có và bạn phải chọn giá trị phù hợp cho tham số đó để đưa vào câu lệnh.
{ **x** | **y** | **z** }	Biểu hiện bạn phải chọn một trong các giá trị x, y, z trong câu lệnh.

Bảng 3.1

2.3.2 Các phím tắt cần sử dụng khi cấu hình router

Cisco router được cấu hình bằng chuỗi các lệnh, để thuận tiện và nhanh chóng hơn trong việc nhập lệnh một số các phím tắt thường được sử dụng được trình bày ở bảng 3.2:

Phím	**Công dụng**
Delete	Xóa ký tự bên phải con trỏ
Backspace	Xóa ký tự bên trái con trỏ
Left Arrow hay Ctrl-B	Di chuyển con trỏ về bên trái một ký tự
Right Arrow hay Ctrl-F	Di chuyển con trỏ về bên phải một ký tự
Esc-B	Di chuyển con trỏ về bên trái một từ
Esc-F	Di chuyển con trỏ về bên phải một từ
TAB	Hiển thị toàn bộ lệnh (chỉ có tác dụng khi phần đã gõ của lệnh tương ứng đủ để giúp Cisco IOS xác định lệnh đó là duy nhất)
Ctrl-A	Di chuyển con trỏ lên đầu hàng lệnh.
Ctrl-E	Di chuyển con trỏ về cuối hàng lệnh.
Ctrl-R	Hiển thị lại dòng lệnh.
Ctrl-U	Xóa dòng lệnh.
Ctrl-W	Xóa một từ
Ctrl-Z	Kết thúc Configuration Mode, trở về EXEC mode.
Up Arrow hay Ctrl-P	Hiển thị dòng lệnh trước.
Down Arrow hay Ctr-N	Hiển thị dòng lệnh tiếp theo.

Bảng 3.2

Ngoài ra khi cấu hình router, dấu **?** thường được sử dụng ở tất cả các mode để liệt kê danh sách các câu lệnh có thể sử dụng được tại mode đó.

Ví dụ:

```
Router> ?
Exec commands:
 <1-99>      Session number to resume
 connect     Open a terminal connection
 disconnect  Disconnect an existing telnet session
 enable      Turn on privileged commands
 exit        Exit from the EXEC
 help        Description of the interactive help system
 lat         Open a lat connection
 lock        Lock the terminal
 login       Log in as a particular user
```

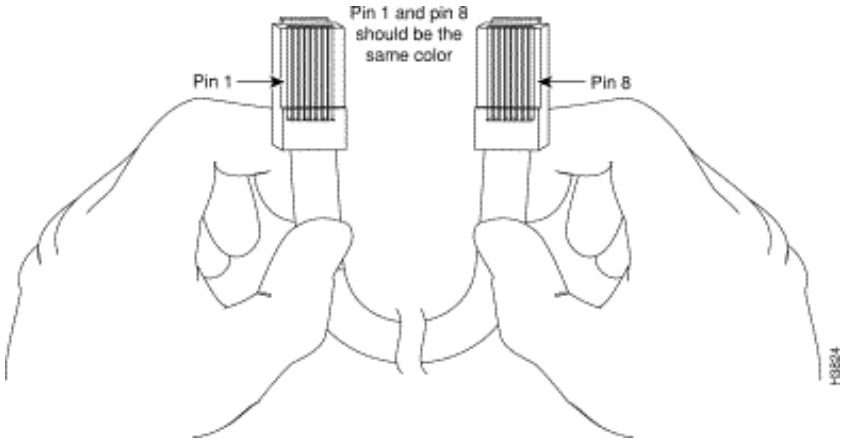
```
  logout              Exit from the EXEC

menuStart         a menu-based user interface
mbranchTrace      multicast route for branch of tree
mrbranchTrace     reverse multicast route to branch of tree
mtrace            Trace multicast route to group
name-connection Name an existing telnet connection pad
                  Open a X.29 PAD connection
ping              Send echo messages
resume            Resume an active telnet connection
show              Show running system information
systat            Display information about terminal lines
telnet            Open a telnet connection
terminal          Set terminal line parameters
tn3270            Open a tn3270 connection trace
Trace route to destination whereList active telnet
connections x3    Set X.3 parameters on PAD
xremote           Enter XRemote mode
```

2.3.3 Các khái niệm về console, telnet. Cách xác định các tên và password cho router.

2.3.3.1 Console port

Console port có trên tất cả các loại router dùng để cho các terminal có thể truy cập vào router để định cấu hình cũng như thực hiện các thao tác khác trên router. Console port thường có dạng lỗ cắm cho RJ-45 connector. Để kết nối vào console port ta cần các thiết bị sau:

- 01 terminal, có thể là terminal chuyên dụng của UNIX hay máy PC Windows chạy chương trình HyperTerminal.
- 01 Roll-over cable: sợi cáp này đi kèm với mỗi router (hình 3.1), là cáp UTP có 4 cặp dây và được bấm RJ-45 đảo thứ tự 2 đầu.



Hình 3.1

- 01 đầu DB-25 hay DB-9 dùng để kết nối vào Terminal. Các đầu nối này có port nối RJ-45 ở phía sau. Các đầu nối này thường được gọi là RJ-45 to DB-9 hay RJ-45 to DB-25 adapter.

Kết nối vào console port được thực hiện như hình 3.2

Khi kết nối đã được thực hiện, chạy chương trình (ví dụ như HyperTerminal) của Windows để truy cập vào router. Một số điểm lưu ý khi sử dụng chương trình là:

- Chọn đúng COM port kết nối (direct to COM1 hay COM2).
- Các thông số của console port là: 9600 baud, 8 data bits, no parity, 2 stop bits. Console port không hỗ trợ cho flow control và modem control.

Nếu không được đặt password cho console port, khi khởi động chương trình HyperTerminal, xác lập đúng các thông số như trên và gõ vài lần **Enter,** bạn sẽ vào ngay user EXEC mode với dấu nhắc "router>". Password với console port là không bắt buộc, tuy nhiên để bảo đảm an toàn cho hệ thống, ta có thể dùng các bước sau đây để xác định password cho console port của router.

Hình 3.2 Kết nối console port vào terminal.

Câu lệnh	**Dấu nhắc ban đầu**	**Dấu nhắc sau khi gõ**	**Giải thích**
enable	Router>	Router#	Vào chế độ Privileged mode, gõ password nếu cần
config terminal	Router#	Router#(config)	Vào global configuration mode
line con0	Router#(config)	Router#(config-line)	Vào line configuration mode.
login	Router#(config-line)	Router#(config-line)	Cho phép login vào router và hiển thị câu hỏi password khi truy cập.
password *password*	Router#(config-line)	Router#(config-line)	Đặt password cho console port.
^ Z	Router#(config-line)	Router#	Trở về Privileged mode.

Bảng 3.3

2.3.3.2 Telnet sesstion

Trong hệ thống mạng sử dụng TCP/IP, Telnet là một dịch vụ rất hữu ích giúp cho người sư dụng có thể truy cập và cấu hình thiết bị từ bất cứ nơi nào trong hệ thống hay thông

qua các dịch vụ remote access. Để sử dụng được Telnet cho việc truy cập và cấu hình cisco router cần phải có các điều kiện sau:

- Hệ thống mạng sử dụng giao thức TCP/IP
- Gán địa chỉ IP cho ít nhất 01 trong các ethernet port của router và kết nối cổng đó vào hệ thống mạng.
- 01 PC kết nối vào mạng thông qua TCP/IP.

Sau khi thỏa mãn các điều kiện trên, tại PC ta có thể gõ lệnh **telnet** *ip address của ethernet port trên router* để có thể truy cập vào router.

Do mức độ dễ dàng và thuận tiện của telnet trong việc truy cập vào router, việc đặt password cho telnet là rất cần thiết và quan trọng. Bảng sau sẽ trình bày các bước để xác lập password cho các đường telnet.

Câu lệnh	**Dấu nhắc ban đầu**	**Dấu nhắc sau khi gõ**	**Giải thích**
enable	Router>	Router#	Vào chế độ Privileged mode, gõ password nếu cần
config terminal	Router#	Router#(config)	Vào global configuration mode
line vty 0 4	Router#(config)	Router#(config-line)	Vào line configuration mode.
login	Router#(config-line)	Router#(config-line)	Cho phép login vào router và hiển thị câu hỏi password khi truy cập.
password *password*	Router#(config-line)	Router#(config-line)	Đặt password cho console port.
^ Z	Router#(config-line)	Router#	Trở về Privileged mode.

Bảng 3.4

Đường telnet trong Cicso router được ký hiệu là **vty.** Cisco router hỗ trợ 05 phiên telnet đồng thời (ký hiệu từ 0 đến 4). Ta có thể xác định password cho từng đường telnet. Tuy nhiên cả 05 đường thường được cấu hình chung 01 password duy nhất để tăng khả năng bảo mật và dễ quản lý.

2.3.3.3 Xác định tên cho router và enable password.

Khi chưa xác định tên cho router, dấu nhắc mặc định của router sẽ là “router>”. Việc xác định tên cho router nhằm mục đích quản lý và làm thay đổi dấu nhắc này. Ngoài ra việc xác đính enable password cho phép ngăn chặn thêm một lần nữa (ngoài password vào console hay telnet) việc truy cập và thay đổi cấu hình router. Bảng sau trình bày các buớc để đặt (hay thay đổi) tên và enable password cho router.

Câu lệnh	**Dấu nhắc ban đầu**	**Dấu nhắc sau khi gõ lệnh**	**Giải thích**
enable	Router>	Router#	Vào chế độ Privileged mode, gõ password nếu cần

config terminal	Router#	Router#(config)	Vào global configuration mode
hostname *name*	Router#(config)	(name)#(config-line)	Xác định tên cho router, dấu nhắc sẽ thay đổi đúng theo tên đã nhập.
enable assword *password*	(name)#(config-line)	(name)#(config-line)	Xác định enable password
enable secret *password*	(name)#(config-line)	(name)#(config-line)	Xác định enable password đồng thời mã hóa password trong file cấu hình. Phải đi chung với lệnh **service password-encryption.**
^ Z	(name)#(config-line)	(name)#	Trở về Privileged mode.

Bảng 3.5

2.3.4 Làm việc với file cấu hình và IOS image.

2.3.4.1 Một số khái niệm cơ bản.

- File cấu hình (configuration file):

Là một file dạng text có cấu trúc, trong đó chứa tất cả các lệnh quan trọng của router, quyết định hoạt động của router. Sau khi cấu hình ban đầu, file cấu hình này được ghi vào NVRAM của router và sẽ được sử dụng trong suốt thời gian hoạt động của router. (trong một số loại router, file này có thể chứa ở bootflash RAM, slot 0 hay slot 1của PCMCIA card). Khi router khởi động file cấu hình này được nạp từ NVRAM vào RAM và thi hành một cách tự động. Việc mất hay hư hỏng file cấu hình này sẽ khiến router rơi vào ROM mode hay setup mode. File cấu hình nằm trong NVRAM được gọi là startup-config còn nằm trong RAM được gọi là running-config. Ngoại trừ trong quá trình cấu hình router, hai file này thường giống nhau.

Ví dụ về một file cấu hình của router:

```
Current configuration:
!
version 11.2
! Version of IOS on router, automatic command
!
no service udp-small-servers no
service tcp-small-servers
!
hostname Critter
prompt Emma
! Prompt overrides the use of the hostname as the prompt
!
enable password lu
! This sets the priviledge exec mode password
!
no ip domain-lookup
! Ignores all names resolutions unless locally defined on the router.
!
ipx routing 0000.3089.b170
! Enables IPX rip routing
!
```

```
interface Serial0
ip address 137.11.12.2 255.255.255.0
ipx network 12
!
interface Serial1
description this is the link to Albuquerque ip
address 137.11.23.2 255.255.255.0
ipx network 23
!
interface TokenRing0
ip address 137.11.2.2 255.255.255.0
ipx network CAFE
ring-speed 16
!
router rip
network 137.11.0.0
!
no ip classless
!
banner motd ^C This Here's the Rootin-est Tootin-est Router in these here Parts! ^C
! Any text between the Ctl-C keystroke is considered part of the banner, including
!the return key.!
line con 0
password cisco
login
! login tells the router to supply a prompt; password defines what the user must type!
!
line aux 0
line vty 0 4
password cisco
login
!
end
```

- IOS image:

IOS là chữ viết tắt của Internetworking Operating System. IOS thực sự là trái tim của Cisco router. Nó quyết định tất cả các chức năng của thiết bị và bao gồm tất cả các dòng lệnh dùng để cấu hình thiết bị đó. IOS image là thuật ngữ dùng để chỉ file chứa IOS, nhờ đó mà ta có thể backup hay upgrade IOS một cách dễ dàng và thuận tiện. Trong Cisco router IOS thường được chứa trong Flash RAM.

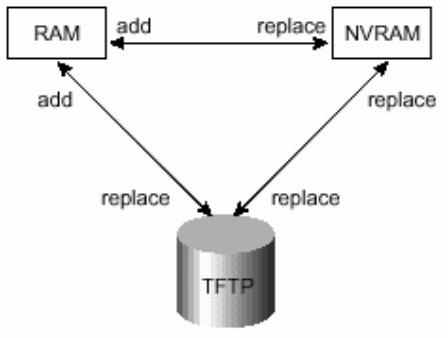
- TFTP server.

TFTP là chữ viết tắt của Trial File Transfer Protocol, một protocol chuẩn của giao thức TCP/IP. TFTP là một connectionless, reliable protocol. TFTP Server có thể là một workstation UNIX hay một PC thường chạy chương trình giả lập TFTP server trên một hệ thống mạng TCP/IP. TFTP Server thường được dùng làm nơi backup các file cấu hình,
IOS image hay ngược lại là nơi chứa các file cấu hình mới, các IOS image mới để update cho router.

2.3.4.2 Làm việc với file cấu hình và IOS.

- Với file cấu hình:

Các quá trình làm việc với file cấu hình được mô tả trong hình 3.3



Hình 3.3

Như hình 3.3 cho thấy, ta có thể chuyển đổi qua lại file cấu hình từ RAM, NVRAM và TFTP Server. Các chuyển đổi đến NVRAM và TFTP thường có nghĩa là thay thế (replace) trong khi các chuyển đổi tới RAM có nghĩa là bổ sung (add).

- Để chuyển đổi file cấu hình trong Cisco router dùng lệnh sau ở privileged mode:

  copy {tftp | running-config | startup-config} {tftp | running-config | startup-config}

Ví dụ:

- Để copy file cấu hình từ RAM vào NVRAM ta dùng lệnh sau:

  copy running-config startup-config

- Để xem một file cấu hình ta dùng lệnh sau:

  show {running-config | startup-config}

- Để xóa một file cấu hình ta dùng lệnh sau:

  erase nvram

Ngoài ra ta còn có thể sử dụng các câu lệnh khác có tác dụng tương tự. Các lệnh này là các lệnh cũ thường được sử dụng trong các IOS version 11.0 trở về trước.

Câu lệnh	**Câu lệnh tương đương (lệnh cũ)**
show running-config	write terminal
show startup-config	show config
copy running-config startup config	write mem
copy running-config tftp	write network
erase nvram	write erase hay erase startup-config.

.

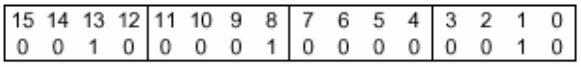
- Xem nội dung của flash RAM

Dùng lệnh **show flash** để xem thông tin về IOS image chứa trong flash RAM Ví dụ:

```
fred#show flash
System flash directory: File
Length Name/status
1 4181132 c2500-i-l.112-7a
[4181196 bytes used, 4207412 available, 8388608 total]
8192K bytes of processor board System flash (Read ONLY)
```

- Chọn IOS image để khởi động router.

Trong mỗi router có 01 thanh ghi gọi là configuration register. Đây là một thanh ghi 16-bit (Hình 3.5) trong đó 4 bit cuối cùng được gọi là boot field quyết định quá trình khởi động của router. Giá trị của boot field cho biết router sẽ khởi động từ ROM hay từ RAM. Can thiệp vào quá trình khởi động của router thông qua configuration register thường dùng trong quá trình password recovery.



Hình 3.5: configuration register.

Một cách khác đơn giản và thường được sử dụng là dùng lệnh **boot system** của IOS. Lệnh này thường được đặt và trong startup-config của router.

Bảng sau sẽ tổng kết lại cả hai phương pháp trên

Giá trị của boot field	**Câu lệnh boot system**	**Kết quả**
0x0	Không ảnh hưởng	ROM monitor mode.
0x1	Không ảnh hưởng	ROM mode.
0x2 đến 0xF	**Boot system rom**	ROM mode
0x2 đến 0xF	**Boot system flash**	IOS đầu tiên trong flash sẽ được dùng để khởi động.
0x2 đến 0xF	**Boot system flash** *filename*	IOS image trong flash được chỉ định sẽ được dùng để khởi động.
0x2 đến 0xF	**Boot system tftp** *ip address filename*	IOS image có tên là *filename* trong TFTP server có địa chỉ *ip address* sẽ được dùng để khởi động.
0x2 đến 0xF	Nhiều lệnh **boot system**	Router sẽ sử dụng các lệnh từ trên xuống dưới cho đến khi có một lệnh được thực

.Bảng 3.7

CHƯƠNG III: GIAO THỨC ĐỊNH TUYẾN

3.1.Giới thiệu về định tuyến

Định tuyến là quá trình mà router thực hiện để chuyển gói dữ liệu tới mạng đích. Tất cả các router dọc theo đường đi đều dựa vào địa chỉ IP đích của gói dữ liệu để chuyển gói theo đúng hướng đến đích cuối cùng. Định tuyến chia làm hai dạng định tuyến động và định tuyến tĩnh.

3.2. Định tuyến tĩnh

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 sự thay đổi nào thì chính người quản trị mạng phải xoá hoặc thêm thông tin về đường đi cho router. những loại đường như vậy gọi là đường cố định.

3.2.1.Hoạt động của định tuyến tĩnh

Hoạt động của định tuyến tĩnh có thể được chia ra làm ba bước 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

ẩ gươi quản trị mạng cấu hình đường cố định cho router bằng lệnh **ip route.** Cú pháp của lệnh **ip route** như sau:

Router(config) # ip route *prefix mask {address / interface }* [*distance*] [**tag** *tag*] [**permanent**]

- **prefix**IP của mạng đích.
- **mask** Subnet mask của mạng đích.
- **address** Địa chỉ IP của "next hop" để đi đến mạng đích.
- **interface** Cổng ra trên router đi đến mạng đích
- **distance** (tùy chọn) Khoảng cách quản trị của giao thức.
- **tag** *tag*(tuỳ chọn) Sử dụng làm giá trị so sánh để điều khiển việc phân bố đường qua bản đồ đường đi (trong CCẩ P).

- **Permanent** (tuỳ chọn) Chỉ ra rằng con đường này không bị xoá kể cả khi cổng bị shutdown. (trong CCẩ P)

Một vấn đề cần quan tâm đến đối với định tuyến tĩnh đó là chỉ số tin cậy.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 vậy nếu hai con đường cùng đi đến một đích thì con đường nào có độ tin cậy nhỏ hơn thì đường đó được đặt vào bảng định tuyến của router trước. Ví dụ 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. ẩ ếu ta muốn chỉ định chỉ số tin cậy thay vì sử dụng giá trị mặc định thì ta thêm hông số này vào sau thông số về cổng ra hoặc địa chỉ IP trạm kế của câu lệnh. Giá trị này nằm trong khoảng từ 0 đến 255.

Ví dụ: router(config)# ip route 172.16.2.0 255.255.255.0 172.16.4.1 124

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

3.2.2.Cấu hình đường cố định

+ Khoảng cách quản trị và độ đo đường đi (metric)

Độ đo đường đi của mọi đường tĩnh luôn bằng "0"

Khoảng cách quản trị là độ ưu tiên về thông tin định tuyến.

Khoảng cách quản trị càng nhỏ thì càng có độ ưu tiên càng cao.

ẩ ếu router thấy có nhiều con đường tới cùng một mạng đích từ nhiều nguồn khác nhau thì nó sẽ sử dụng Khoảng cách quản trị để quyết định đưa con đường nào vào Bảng định tuyến.

Khoảng cách quản trị mặc định của đường định tuyến tĩnh là "1"

Route Source	Default Distance Values
Connected interface	0
Static route	1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route	5
External Border Gateway Protocol (BGP)	20
Internal EIGRP	90
IGRP	100
OSPF	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
On Demand Routing (ODR)	160
External EIGRP	170
Internal BGP	200
Unknown*	255

Hình 3.2.1 Khoảng cách quản trị của các giao thức định tuyến

+ ***Các bước cấu hình đường cố định:***

1. Xác định tất cả các mạng đích cần cấu hình, subnet mask tương ứng và gateway tương ứng. Gateway có thể là cổng giao tiếp trên router hoặc là địa chỉ của trạm kế tiếp để đến được mạng đích.

2. Bạn vào chế độ cấu hình toàn cục của router

3. ẩ hập lệnh ip route với địa chỉ mạng đích, subnet mask và gateway tương ứng mà ta đã xác định ở bước một. nếu cần thì thêm thông số về độ tin cậy.

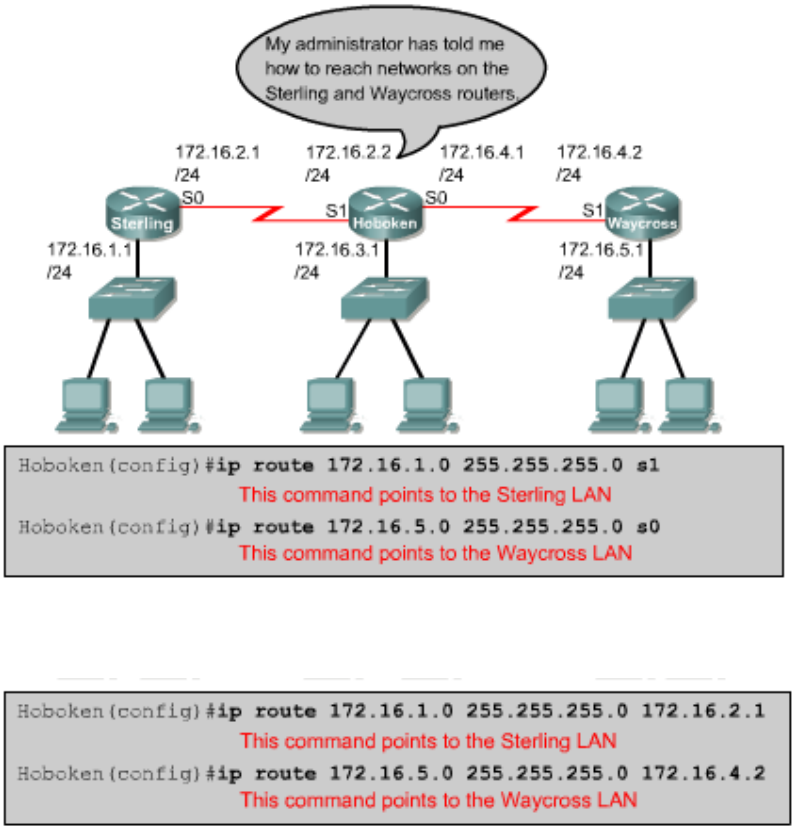
4. Lặp lại bước ba cho những mạng đích khác

5. tháot khỏi chế độ cấu hình toàn cục

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

Ví dụ: Hình 3.2.2 là một minh hoạ về cấu hình đường cố định với cấu trúc mạng có 3 router kết nối đơn giản. trên router Hoboken ta cần cấu hình đường đi tới mạng 172.16.1.0 và mạng 172.16.5.0 cả hai mạng này đều có subnet mask la255.255.255.0

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



Hình 3.2.2: Cấu hình định tuyến tĩnh cho mạng

Ở khung phía trên của hình 3.2.2 cả hai câu lệnh đều chỉ đường cố định cho router thông qua cổng ra trên router. Trong câu lệnh này không chỉ định giá trị cho chỉ số tin cậy nên trên bảng định tuyến hai đường cố định này có chỉ số tin cậy mặc định là 0. Đường có chỉ số tin cậy bằng 0 tương đương với mạng kết nối trực tiếp vào router.

Ở khung bên dưới của hình 6.2.2, hai câu lệnh chỉ đường cố định cho router thông qua địa chỉ router kế tiếp. Đường tới mạng 172.168.1.0 có địa chỉ của router kế tiếp là 172.16.2.1, đường tới mạng 172.16.5.0 có địa chỉ của router kế tiếp là

172.16.4.2. Trong hai câu lệnh này cũng không chỉ định giá trị cho độ tin cậy nên hai đường cố định tương ứng sẽ có cỉ số tin cậy mặc định là 1.

3.2.3.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 cấu hình đường mặc định cho đường ra của Internet của router vì router không cần lưu thông tin định tuyến tới từng mạng trên Internet.

Lệnh cấu hình đường cố định:

Ip route 0.0.0.0 0.0.0.0 [next-hop-address / outging interface]

Subnet 0.0.0.0 khi thực hiện phép toán Aẩ D logic với bất kỳ địa chỉ IP đích nào cũng có kết quả mạng là 0.0.0.0. Do đó nếu gối 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.

Các bước cấu hình đường mặc định:

+ Vào chế độ cấu hình toàn cục

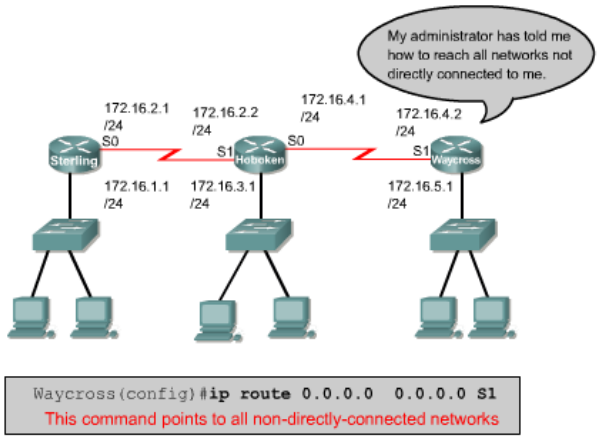
+ ẩ hập lệnh **ip route** với mạng đích là 0.0.0.0 và subnet mask tương ứng là 0.0.0.0. Gateway của đường mặc định có thể là cổng giao tiếp trên router kết nối với mạng bên ngoài hoặc là địa chỉ IP của router kế tiếp. Thông thường ta hay sử dụng địa chỉ IP của router kế tiếp làm gateway.

+ Thoát khỏi chế độ cấu hình toàn cục

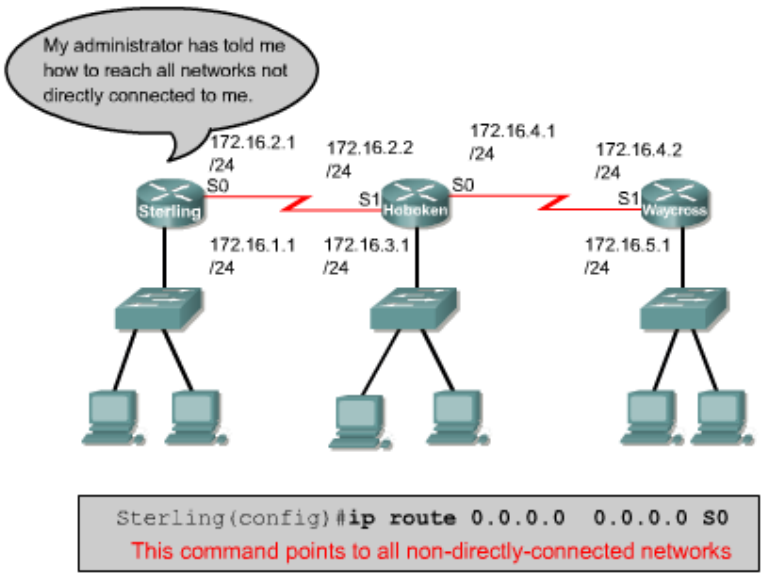
+ Lưu lại tập tin cấu hình khởi động trong ẩ VRAM bằng lệnh:

copy running-config startup-config.

Vi dụ:



Hình 3.2.3a



Hình 3.2.3b

Trong ví dụ của hình 3.2.2 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 Waycross. ẩ hưng cả router Sterling và Waycross đều chưa biết đường đi tới các mạng mà không kết nối trực tiếp với nó. Ta có thể cấu hình đường cố định cho sterling và Waycross để chỉ đường tới từng mạng một. ẩ hưng cách này không phải là một giải pháp hay cho những hệ thống mạng lớn. Trong hình 3.2.3a và 3.2.3b là những ví dụ về cấu hình các đường mặc định cho router sterling và

Waycross. Sterling kết nối đến tất cả các mạng khác thông qua một cổng Serial 0. Tương tự Waycross 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 Waycross thì hai 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 với nó.

3.2.4.Các quy tắc về định tuyến tĩnh

+ Định tuyến tĩnh qua liên kết điểm-điểm.

Tốt nhất là ta nên sử dụng định tuyến tĩnh bằng cổng ra.

Với các cổng serial kết nối kiểu điểm-điểm, router không bao giờ sử dụng địa chỉ trung gian để chuyển tiếp gói dữ liệu.

+ Định tuyến tĩnh qua mạng kiểu quảng bá

Tốt nhất là cấu hình dường định tuyến tĩnh với cả địa chỉ trung gian và cổng ra

+ Chỉ sử dụng địa chỉ trung gian

Khi cấu hình đường định tuyến tĩnh tránh việc các đường đinh jtuyến tĩnh chỉ tham chiếu đến các địa chỉ trung gian vì các đường định tuyến tĩnh không được gán với một cổng nào cả mà phụ thuộc vào việc tìm đường qua các địa chỉ trung gian làm cho tốc độ hội tụ chậm lại. Điều này cũng có thể gây ra vấn đề định tuyến lặp.

3.2.5.Kiểm tra cấu hình đường cố định

Sau khi cấu hình đường cố định, để kiểm tra xem bảng định tuyến đã có đường cố định mà ta đã cấu hình hay chưa, hoạt động định tuyến có đúng hay không. Ta 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 ta dùng lệnh **show ip route** để xem có đường cố định nào trong bảng định tuyến chưa.

Các bước kiểm tra cấu hình đường cố định:

+ Ở chế độ đặc quyền, ta 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. ả ếu không đúng thì ta phải vào lại chế độ cấu hình toàn cục,xoa câu lênh sai và nhập câu lệnh mới.

+ ả hập lệnh **show ip route.**

+ Kiểm tra xem đường cố định mà ta cấu hình có trong bảng định tuyến hay không.

3.2.6.Xử lý sự cố

Dùng lệnh ping để kiểm tra xem các mạng nối với nhau có thông hay không. nếu có sự cố xảy ra ta dùng tiếp lệnh tracerouter để kiểm tra xem mạng bị rớt ở đâu. Sau khi đã xác định được sự cố xảy ra ở router nào thì ta vào các router đó sửa chữa hoặc cấu hình lại cho router đó.

3.3. Định tuyến động

3.3.1.Giới thiệu về định tuyến động

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

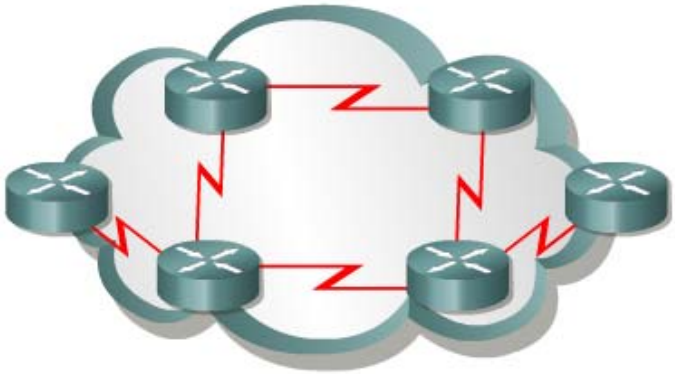
Một số giao thức định tuyến động:

+ RIP (Routing Information Protocol)
+ IPGP (Interior Gateway Routing Protocol)
+ EIGRP (Enhanced Interior Gateway Routing Protocol)
+ OSPF (Open Shortest Path First)

3.3.2.Hệ thống tự quản (Autonomous System) (AS)

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 là nơi quản lý việc cấp số cho mỗi AS. Chỉ số này dài 16 bit.



Hình 3.3.2: Một AS là bao gồm các router hoạt động dưới cùng một cơ chế quản trị

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

Mục đích của giao thức định tuyến động 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 các giao thức định tuyến động 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 cập nhật về tất cả các đường, chọn đường tốt nhất đặt vào bảng định tuyến và xoá đi khi đường đó không được sử dụng nữa. Còn router thì sử dụng thông tin trên bảng định tuyến để chuyển gói dữ liệu của các giao thức đường 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 kiến thức về mạng của các router phải thay đổi theo. Các router phải có kiến thức chính xác về cấu trúc hệ thống mạng.

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

3.3.4.Phân loại các giao thức định tuyến động

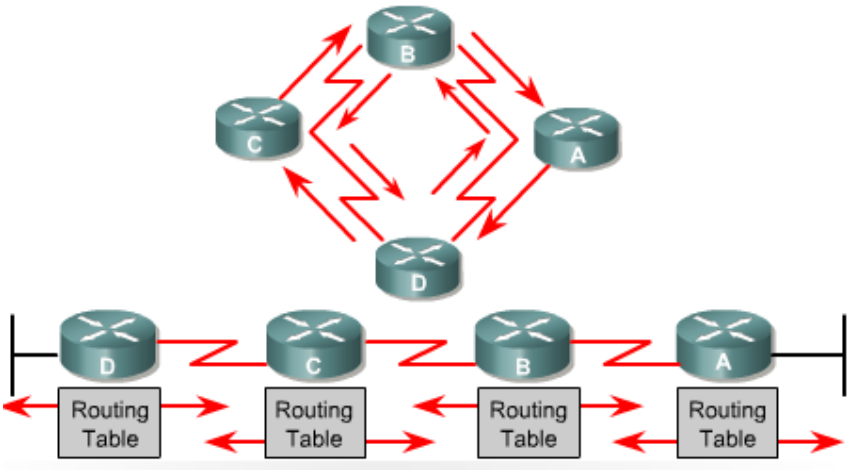
Đa số các thuật toán định tuyến động được xếp vào 2 loại sau:

+ Vectơ khoảng cách

+ Trạng thái đường liên kết

Định tuyến theo vectơ khoảng cách là chọn đường theo hướng và khoảng cách tới đích. Còn định tuyến theo trạng thái đường liên kết thì chọn đường ngắn nhất dựa trên cấu trúc của toàn bộ hệ thống mạng.

3.3.5. Đặc điểm của giao thức định tuyến theo vectơ khoảng cách



Hình 3.3.5

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 véc tơ khoảng cách còn gọi là thuật toán Bellman-Ford.

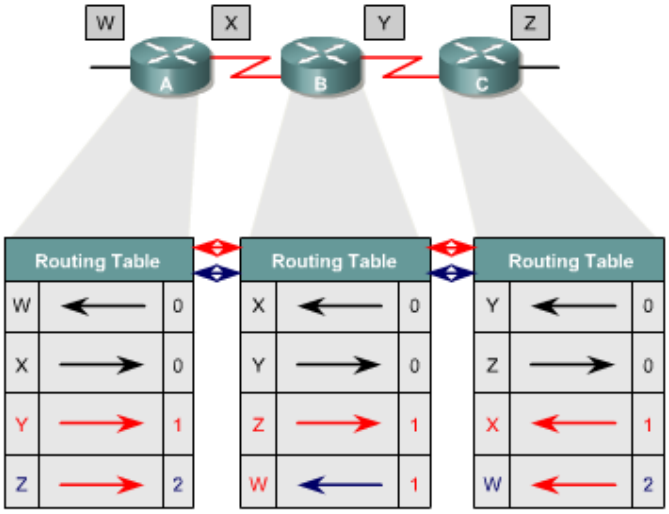
Mỗi router nhận được bảng định tuyến của những router láng giềng kết nối trực tiếp với nó.

Ví dụ ở hình 3.3.5 router B nhận được thông tin từ router A. sau đó router B sẽ cộng thêm khoảng cách từ router B tới router A (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 là router C. Quá trình này xảy ra tương tự cho các router láng giềng khác.

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 khi các router hoạt động theo thuật toán vectơ khoảng cách nó có nhược điểm đó là router sẽ không biết được chính xác cấu trúc của toàn bộ hệ thống mạng mà chỉ biết được các router láng giềng hoạt động cạnh nó mà thôi.

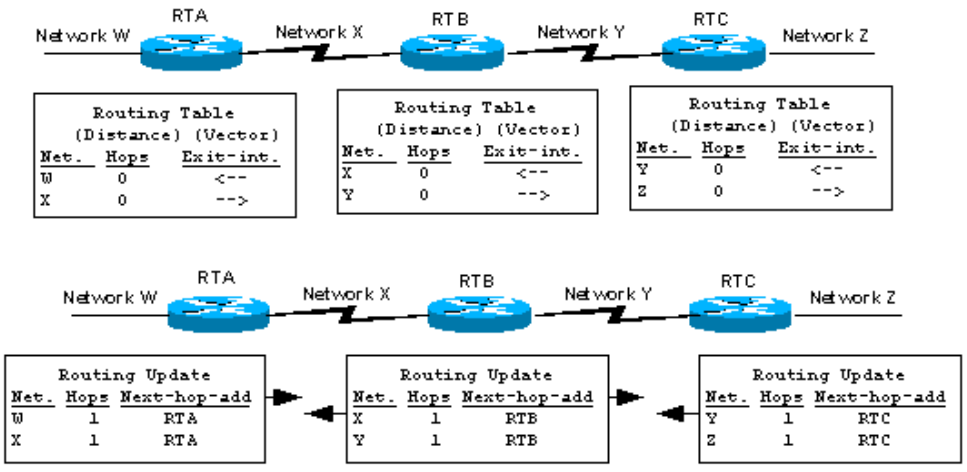
Khi sử dụng định tuyến theo vectơ khoảng cách, bước đầu tiên là router phải xác định các router láng giềng với nó. Các mạng kết nối trực tiếp vào cổng giao tiếp của router sẽ có khoảng cách là 0. còn đường đi tới các mạng không kết nối trực tiếp vào router thì router sẽ chọn đường tốt nhất dựa trên các thông tin mà nó nhận được từ các router láng giềng.

Ví dụ:



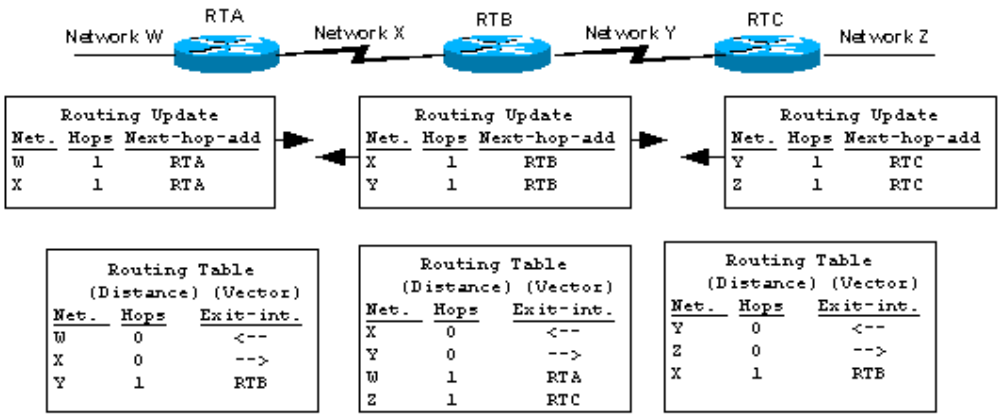
Ta có thể xét quá trình cập nhật bảng định tuyến của các router A,B,C

Đầu tiên trong bảng định tuyến của các router nó sẽ hiển thị đường đi tới các mạng kết nối trực tiếp với nó.



Đối với router A có hai mạng kết nối trực tiếp là W,X do vậy từ router A đến các mạng này có khoảng cách bằng 0.

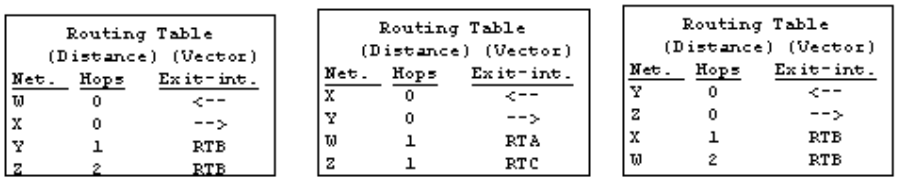
Sau đó router A và B trao đổi thông tin với nhau



Ta thấy router A sẽ học được từ router B mạng Y và đường đi từ router A tới mạng Y phải đi qua router B do vậy khoảng cách tăng lên 1.

Mặt khác router B lại học được từ router A mạng W với khoảng cách là 1 qua router A, và mạng Z với khoảng cách là 1 qua router C.

Sau đó router A và B lại trao đổi thông tin bảng định tuyến với nhau

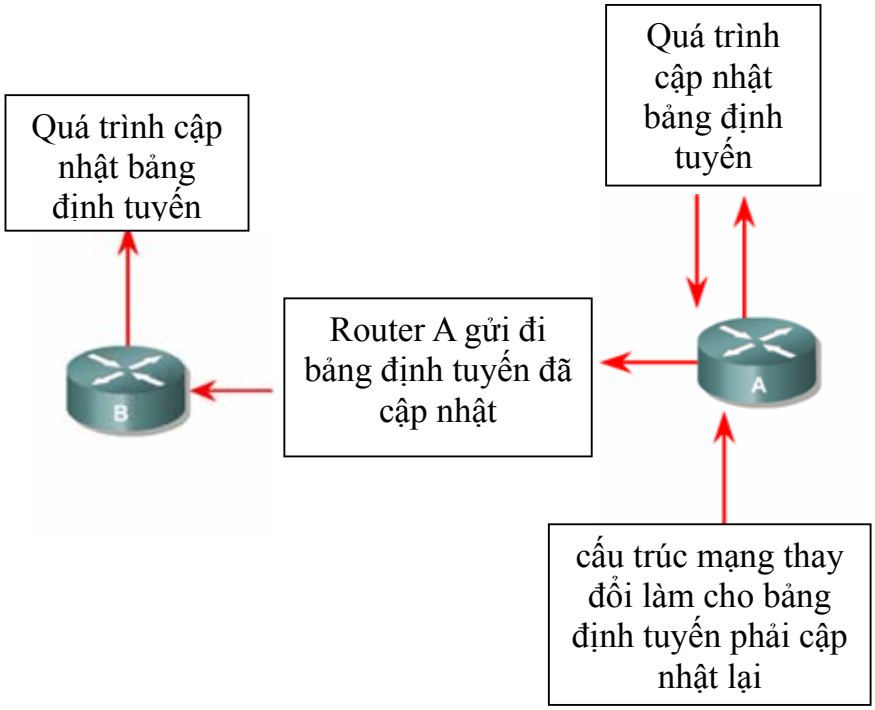


Ta thấy router A lại học được từ router B mạng Z với khoảng cách tăng lên một bằng 2 qua router B.

Tương tự ta cũng xet với các router B và C ta được kết quả của bảng định tuyến của các router này như hình 3.3.5b.

Bảng định tuyến sẽ 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 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.



Hình 3.3.5c

3.3.6. 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 Dijkstrashay 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 các 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 đi ngắn nhất.

+ Bảng định tuyến: chứa danh sách các đường đi đã được chon lựa.

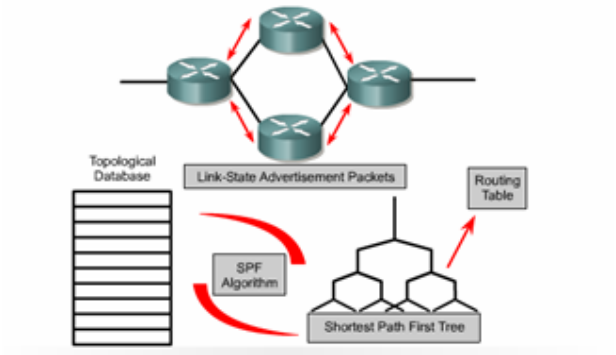
Quá trình thu thập thông tin mạng dể thực hiện định tuyến theo trạng thái đường liên kết:

Mỗi router bắt đầu trao đổi LSA với tất cả các router khác, trong đó LSA mang thông tin về các mạng kết nối trực tiếp của từng router. Sau đó các router tiến hành xây dựng 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 thân 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.

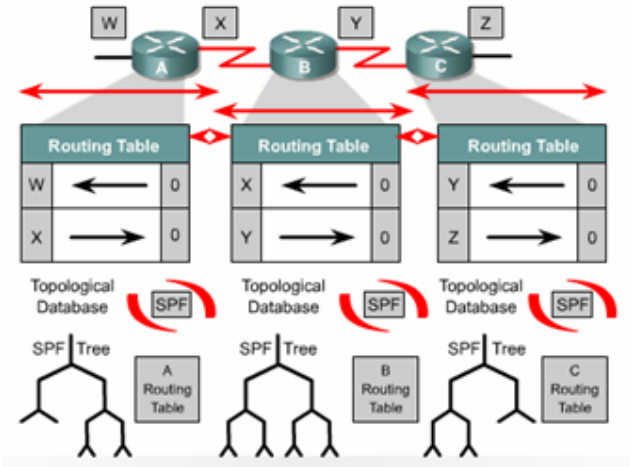
Trên bảng định tuyến sẽ chứa thông tin về các đường đi đã được chọn với cổng ra tương ứng.

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 các thông tin về các router mới, các thay đổi về trạng thái đường liên kết. gói LSA này sẽ được phát cho tất cả các router khác. Khi router nhận được gói LSA này nó sẽ cập nhật lại cơ sử 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.



Router gửi LSAs cho các router khác. Thông tin của LSA được sử dụng để xây dựng cơ sở dỡ liệu đầy đủ về cấu trúc hệ thống mạng.thuật toán SPF tính toán từ đó xây dựng ra bảng định tuyến

Hình 3.3.6a



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

Hình 3.3.6b

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

+ Bộ xử lý trung tâm của router phải tính toán nhiều
+ Đòi hỏi dung lượng bộ nhớ lớn
+ Chiếm dung lượng bằng thông đường truyền

Router sử dụng định tuyến theo trạng thái đường kiên kết sẽ cần nhiều bộ nhớ hơn và hoạt động xử lý nhiều hơn là sử dụng định tuyến theo vectơ khoảng cách. Khi khởi động việc định tuyến, tất cả các router phải gửi các gói LSA cho tất cả các router khác khi đó băng thông đường truyền sẽ bị chiếm dụng làm cho băng thông dành cho truyền dữ liệu của người dùng giảm xuống. ả hưng 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 có sự thay đổi thì router mới phát gói LSA để cập nhật.

3.4.Tổng quát về giao thức định tuyến

3.4.1 Quyết định chọn đường đi

Router có hai 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 đã quyết định đường ra thì router thực hiện việc chuyển mạch để phát gói dữ liệu.

Chuyển mạch là quả trình 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 chuyển bị đi ra.

3.4.2 Cấu hình định tuyến

Để cấu hình giao thức định tuyến, ta 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, ta cần khởi động giao thức định tuyến mà ta muốn, ví dụ như RIP, IGRP, EIGRP, OSPF. Sau đó, trong chế độ cấu hình định tuyến ta phải khai báo địa chỉ IP.

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.

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

3.4.3. 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 vectơ khoảng cách của 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.

* Một số đặc điểm cơ bản của RIP

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

IGRP (Interior Gateway Routing Protocol) là giao thức được phát triển độc quyền của Cisco.

* Một số đặc điểm 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 định tuyến theo trạng thái đường liên kết.

* Một vài đặc điểm chính 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.

EIRGP là giao thức định tuyến nâng cao theo vectơ khoảng cách và là giao thức độc quyền của Cisco.

* Một số đặc điểm của EIRGP

+ Là giao thức nâng cao vectơ khoảng cách.

+ Có chia tải.

+ Có các ưu điểm của định tuyến theo vectơ khoảng cách và định tuyến trạng thái đường liên kết.

+ Sử dụng thuật toán DUAL (Difused Update Algorithm) đẻ tính toán chọn đường đi tôt nhất.

+ Cập nhật theo định kỳ mặc định là 90 giây hoặc cập nhật khi có sự thay đổi về cấu trúc mạng.

BGP (Border Gateway Protocol) là giao thức định tuyến ngoại.

* Vài đặc điểm cơ bản của BGP

+ Là giao thức định tuyến ngoại theo vectơ khoảng cách.

+ Được sử dụng để định tuyến giữa các ISP hoặc ISP và khách hàng.

+ Được sử dụng để định tuyến lưu lượng Internet giữa các hệ tự quản (AS)

Chương 4 GIAO THỨC ĐỊNH TUYẾN THEO VÉC KHOẢNG CÁCH

4.1.Tổng quan về định tuyến theo vectơ khoảng cách

Giao thức định tuyến động giúp cho công việc của người quản trị mạng trở lên đơn giản hơn nhiều. 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 để hiểu rõ hơn, trong chương này ta sẽ đề cập tới các vấn đề của giao thức định tuyến theo vectơ khoảng cách cụ thể là IGRP.

4.2. Định tuyến theo vectơ khoảng cách

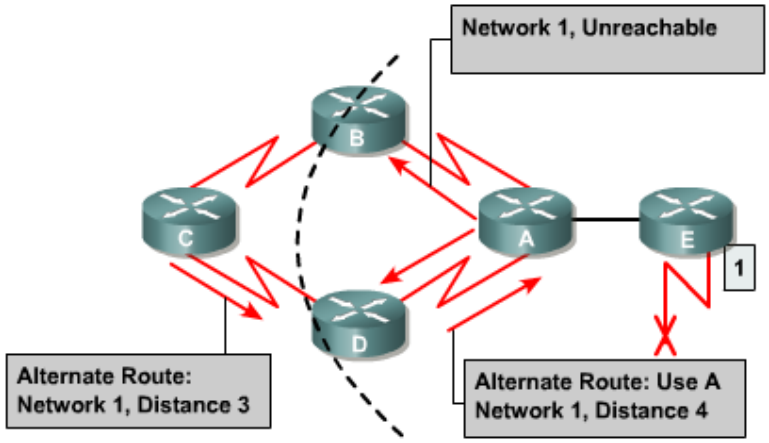
4.2.1.Cập nhật thông tin định tuyến

Bảng định tuyến được cập nhật theo chu kỳ hoặc khi cấu trúc mạng có sự thay đổi. Điểm quan trọng với một giao thức định tuyến là làm sao cập nhật bảng định tuyến một cách hiệu quả. Khi cấu trúc mạng có bất kỳ một sự thay đổi nào 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 tuyến của mình cho các router khác kết nối trực tiếp với nó. Bảng định tuyến bao gồm các thông tin về đường đi tới mạng đích như tổng chi phí (khoảng cách chẳng hạn) tính từ bản thân router tới mạng đích, địa chỉ của trạm kế tiếp trên đường đi.

4.2.2.Lỗi định tuyến lặp

Một vấn đề có thể xảy ra trong quá trình các router cập nhật bảng định tuyến, đó là khi bảng định tuyến trên các router chưa được cập nhật hội tụ do quá trình hội tụ chậm.

Ta có thể xét ví dụ cụ thể sau:



Hình 4.2.2

Ta thấy trước khi mạng một 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. Ta giả sử rằng router C chọn đường đến mạng 1 bằng con đường qua router B. Ta thấy khoảng cách của con đường này từ router C đến mạng 1 là 3 hops.

ả gay khi mạng 1 bị lỗi, router E liền gửi thông tin cập nhật cho router A. router A lập tức ngưng ngay việc định tuyến về mạng 1. ả hưng router B, C ,D vẫn tiếp tục việc này vì chúng vẫn chưa biết mạng 1 bị lỗi. Sau đó router A cập nhật thông tin về việc mạng 1 bị lỗi cho router B, D router B, D lập tức ngưng ngay việc định tuyến về mạng 1. nhưng lúc này router C vẫn chưa được cập nhật thông tin về mạng 1 nên nó vân tiếp tục định tuyến các gói dữ liệu đến mạng 1 qua router B.

Đến thời điểm cập nhật định kỳ của router C.Trong thông tin cập nhật của router C 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 do nó nhận được từ router A lúc nãy. Do đó router D cập nhật lại thông tin này vào bảng định tuyến mà nó không biết rằng như vậy là sai. Lúc này trên bảng định tuyến của router D có đường tới mạng 1 là đi qua router C. Sau đó router D lấy bảng định tuyến vừa cập nhật gửi cho router A. tương tự router A cũng cập nhật lại đường đến mạng 1 qua router D. Rồi gửi cho router B và E. quá trình tương tự tiếp tục xảy ra ở router B và E. khi đó bất kỳ một gói dữ liệu nào gửi tới mạng 1 đều bị gửi lặp vòng từ router C đến B tới router A tới router D rồi lại tới C.

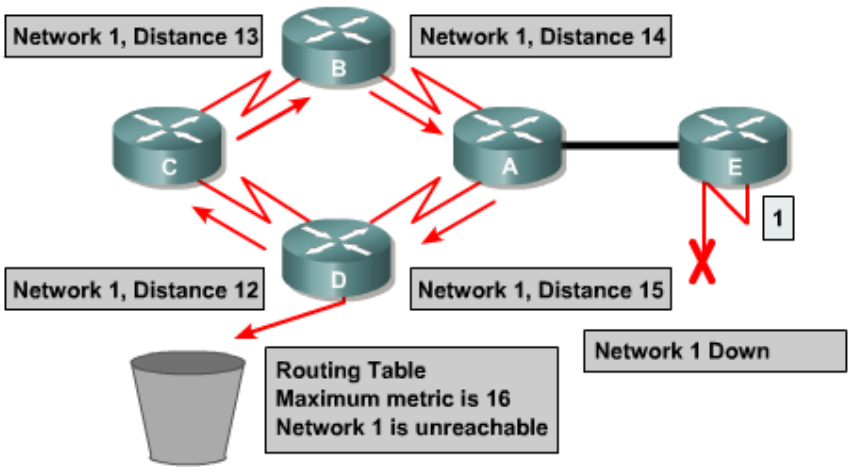
4.2.3. Giá trị tối đa

Ở ví dụ trong mục 4.2.2 việc cập nhật sai về mạng 1 như trên sẽ bị lặp vòng như vậy cho tới khi nào có một tiến trình khác cắt dứt được tiến trình này. Tình trạng như vậy gọi là đếm vô hạn, gói dữ liệu sẽ bị lặp vòng trên mạng trong khi mạng 1 đã bị cắt.

Với vectơ 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. ả ếu ta không có biện pháp khắc phục tình trạng đếm vô hạn, thì cứ như vậy chỉ số hop sẽ tăng lên vô hạn.

Bản thân thuật toán định tuyến theo vectơ khoảng cách có thể tự sửa 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 này kéo dài, giao thức định tuyến theo vectơ khoảng cách đã được 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 quá giá trị tối đa.

Ví dụ



KHi thông số định tuyến là 16 hop lớn hơn giá trị tối đa là 15 thì thông tin cập nhật đó sẽ bị huỷ bỏ.

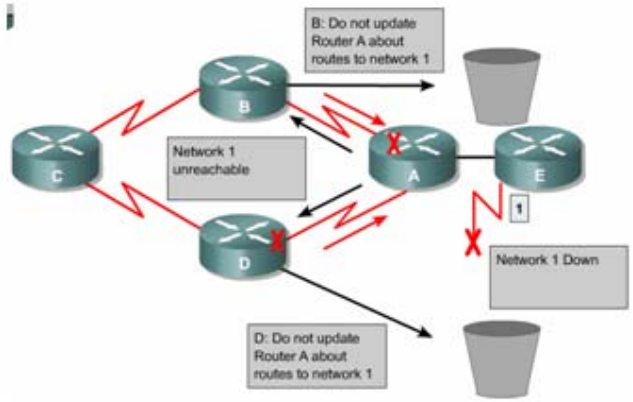
4.2.4.Tránh định tuyến lặp vòng bằng phương pháp slip horizone

Một nguyên nhân khác cũng 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. để hiểu rõ hơn ta xét cơ chế sau:

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 đi tới mạng 1 thông qua router D, khoảng cách đường này là 4.

Khi đó router B tưởng lầm là router C vẫn có đường đến mạng 1 mặc dù con đường này có thông số không tốt bằng con đường cũ của router B lúc trước. sau đó router B cũng cập nhật lại cho router A về đường mới đến mạng 1. Mà router B vừa mới nhận được. 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 mạng 1 qua router C. router C lại định tuyến qua router D kết quả là bất kỳ gói dữ liệu nào đến mạng 1 cũng rơi vào vòng lặp này.

Cơ chế slip-horizon sẽ tránh được tình huống này bằng cách: ả ếu 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 slip-horizonlamf giảm được việc cập nhật thông tin sai và giảm bớt việc xử lý thông tin cập nhật.

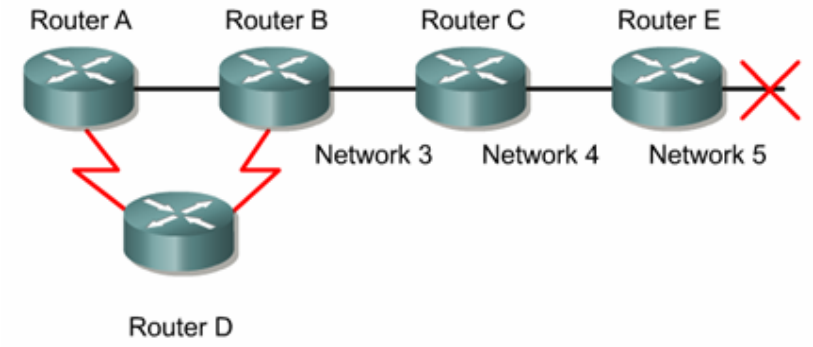


Hình 4.2.4

4.2.5 Router poisoning

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

Ví dụ:



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 được truy cập 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 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 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.

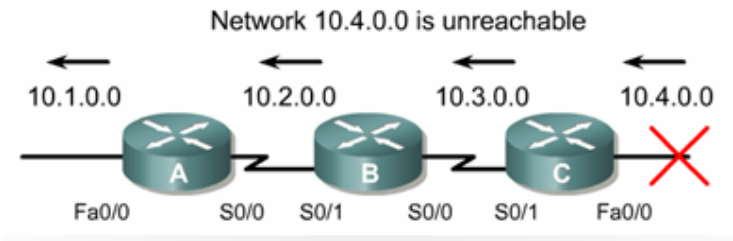
Tóm lại: Route poisoning có nghĩa là khi có một con đường nào đó bị ngắt thì router sẽ thông báo về con đường đó với thông số định tuyến lớn hơn giá trị tối đa. Cơ chế route poisoning không hề gây mâu thuẫn với cơ chế slip-horizon. Slip-horizon có nghĩa là khi router gửi thông tin cập nhật ra một đường liên kết thì router sẽ 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 với thông số định tuyến lớn hơn giá trị tối đa thì kết quả vẫn như vậy. Cơ chế này gọi là cơ chế slip-horizon kết hợp với poison reverse.

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

Khi router phát hiện ra có một thay đổi nào đó trong cấu trúc mạng thì nó lập tức gửi thông điệp cập nhật cho các router láng giềng để thông báo về sự thay đổi đó. ả hất là khi có một đường nào đó bị lỗi hoặc không truy nhập 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 thay đổi trong cấu trúc mạng giúp cho các router cập nhật kịp thời và khởi động thời gian holddown nhanh hơn.

Ví dụ:



Hình 4.2.6

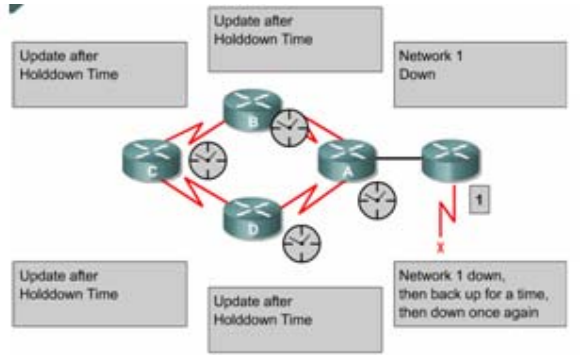
Trong ví dụ trên hình 4.2.6 router C cập nhật tức thời ngay khi mang 10.4.0.0 không truy cập được nữa. Khi nhận được thông tin này, router B cũng phát thông báo về mạng 10.4.0.0 ra cổng S0/1. Đến lượt router A cũng phát thông báo ra cổng Fa0/0.

4.3.7.Tránh lặp vòng với thời gian holddown

Tình trạng lặp vòng đến vô hạn có thể tránh được bàng 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 giềng 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, nếu router nhận được thông tin cập nhật từ một router láng giềng khác (không phải là router láng giềng đã phát thông 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 có trước đó thì nó sẽ cập nhật lại thông tin này và kết thúc thời gian holddown

Trong suốt thời gian holddown, nếu router nhận được thông tin cập nhật từ router láng giềng khác (không phải là router láng giềng đã phát thông tin cập nhật về mạng X lúc nãy) nhưng thông tin nãy cho biết có đường tới mạng X với thông số

định tuyến không tốt bằng con đường mà router có trước đó thì nó sẽ bỏ qua, không cập nhật thông tin này. Cơ chế này giúp cho router tránh được việc cập nhật nhầm lẫn những thông tin cũ do các router láng giềng chưa hay biết gì về mạng X đã không truy cập được nữa. Khoảng 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 mạng đều đã được cập nhật là mạng X không truy cập được nữa, khi đó các router đều có 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 4.3.7

4.4. Giao thức định tuyến RIP

4.4.1. Tiến trình của RIP

IP RIP được mô tả chi tiết trong 2 văn bản. Văn bản đầu tiên là RFC 1058 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 đảm bảo 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 đến vô hạn bằng cách giới hạn số lượng hop tối đa cho phép từ máy gửi đến máy nhận. Số lượng hop tối đa cho mỗi con đường là 15. Đối với các con đường mà router nhận được từ thông tin cập nhật của router láng giềng, router sẽ tăng chỉ số hop lên 1 vì router xem bản thân nó là một hop trên đường đi. ả ếu sau khi tăng chỉ số hop lên 1 mà chỉ số này lớn hơn 15 thì router sẽ xem như mạng đích tương ứng với con đường này không đến được. ả goài ra, RIP cũng có nhiều đặc tính tương tự như các giao thức định tuyến khác. Ví dụ như: RIP cũng có split horizon và thời gian holddown để tránh cập nhật thông tin định tuyến không chính xác

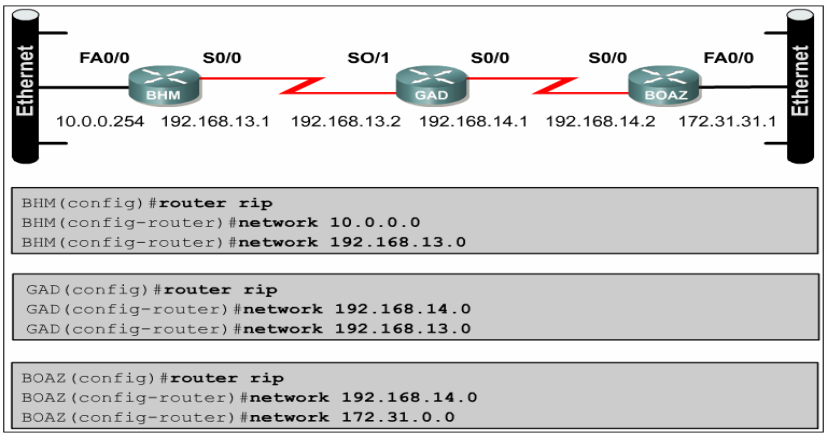
Các đặc điểm chính của RIP

- Là giao thức định tuyến theo vectơ khoảng cách.
- Thông số định tuyến là số lượng hop.
- ả ếu 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.

4.4.2. Cấu hình RIP

Lệnh **router rip** dùng để khởi động RIP. Lệnh **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 đến mạng đích mà router học được từ router láng giềng thì nó sẽ tăng chỉ số hop lên 1, địa chỉ nguồn của thông tin cập nhật này sẽ là địa chỉ của trạm kế tiếp. có thể sử dụng nhiều con đường có chỉ số bằng nhau đến cùng 1 đích. RIP chỉ chọn một con đường tốt nhất đến mạng đích, tuy nhiên nó cũng

Có thể cấu hình cho RIP thực hiện 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 này đầu tiên sẽ cập nhật vào bảng định tuyến của nó trước, sau đó lập tức gửi thông tin cập nhật cho các router khác để thông báo về sự thay đổi đó. Hoạt động này gọi là cập nhật tức thời và nó xẩy ra hoàn toàn độc lập với cập nhật định kỳ. Hình 4.4.1 là một ví dụ về cấu hình RIP:



Hình 4.4.1

- BHM(config)#**router rip -** Chọn RIP làm giao thức định tuyến cho router.
- BHM(config-router)#**network 10.0.0.0** –Khai báo mạng kết nối trực tiếp vào router.
- BHM(config-router)#**network** 192.168.13.0 – Khai báo mạng trực tiếp kết nối 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 ta có thể thực hiện thêm một số cấu hình khác. ả những cấu hình này không bắt buộc phải làm, ta chỉ cấu hình thêm nếu thấy cần thiết:

- Điều chỉnh các thông số cần thiết.
- Điều chỉnh các thông số hoạt động về thời gian của RIP.
- Khai báo phiên bản của RIP mà ta đang sử dụng (RIPv1 hay RIPv2).
- Cấu hình cho RIP thực hiện khi trao đổi thông tin cập nhật.
- Cấu hình cho RIP chỉ gửi thông tin định tuyến rút gọn ra một cổng nào đó.
- Kiểm tra thông tin định tuyến IP rút gọn.
- Cấu hình 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 WAả .

Tóm lại, để cấu hình cho RIP ta bắt đầu chế độ cấu hình toàn cục như sau:

Router(config)#**router rip** - Khởi động giao thức định tuyến RIP.

Router(config-router)#network network-numbur – Khai báo các mạng mà RIP được phép chạy trên đó.

4.4.3. Sử dụng 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 đó nhưng các subnet kết nối trực tiếp vào router lại có cùng supernet với subnet đích của gói dữ liệu. Ví dụ: Một tổ chức sử dụng địa chỉ mạng 10.10.0.0/16, khi đó subnet 10.10.10.0/24 có supernet là 10.10.0.0/16. Trong trường hợp như vậy ta dùng lệnh ip classless để router không huỷ bỏ gói dữ liệu mà sẽ truyền gói ra đường đến địa chỉ supernet, nếu có. Đối với phần mềm Cisco IOS phiên bản 11.3 trở về sau, mặc định là lệnh **ip classless** đã được chạy trong cấu hình của router. ả ếu bạn muốn 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 sẽ bị huỷ bỏ.

Ip classless chỉ có tác động đối với việc chuyển gói đi chứ không tác động đến cách mà router xây dựng bảng định tuyến. Đây chính là đặc điểm quan trọng của giao thức định tuyến theo lớp. ả ếu một địa chỉ mạng lớn được chia thành các subnet con và trên bảng định tuyến của router chỉ có một số 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 huỷ bỏ

Cơ chế này hay bị nhầm lẫn nhất khi router có cấu hình đường mặc định. từ một địa chỉ mạng lớn chia thành nhiều nubnet con. Kết nối trực tiếp vào router chỉ có một 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 subnet đó không tồn tại. Do đó khi router nhận được gói dữ liệu có địa chỉ mạng 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 huỷ bỏ gói dữ liệu cho dù trên bảng định tuyến của router có cấu hình đường mặc định. Lệnh **ip classless** sẽ giải quyết vấn đề này bằng cách cho phép router không cần quan tâm đến địa chỉ đích

nữa. Khi đó nếu router không tìm thấy được củ thể mạng đích trên bảng định tuyến thì nó sử dụng đường mặc định để truyển gói đi.

4.4.4. 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 vectơ khoảng cách. Tất cả các giao thức định tuyến theo vectơ khoảng cách đều có nhược điểm là tốc độ hội tụ chậm. Trạng thái hội tụ là khi tất cả các router trong hệ thống mạng đều có thông tin định tuyến về một 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 nhau những thông tin cũ chưa được cập nhật đúng.

Để giải quyết những vấn đề này, RIP sử dụng những kỹ thuật sau:

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

Có một số kỹ thuật đòi hỏi bạn phải cấu hình, còn có 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 mà có số hop lớn hơn 15 thì xem như mạng đó không đến được. Điều này làm cho RIP bị hạn chế không sử dụng được cho những hệ thống mạng lớn nhưng nó lại giúp 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 đa nhận được từ hướng đó. Trong một số cấu hình mạng thì bạn cần phải tắt cơ chế split horizon.

Sau đây là lệnh để tắt cơ chế split horizon:

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

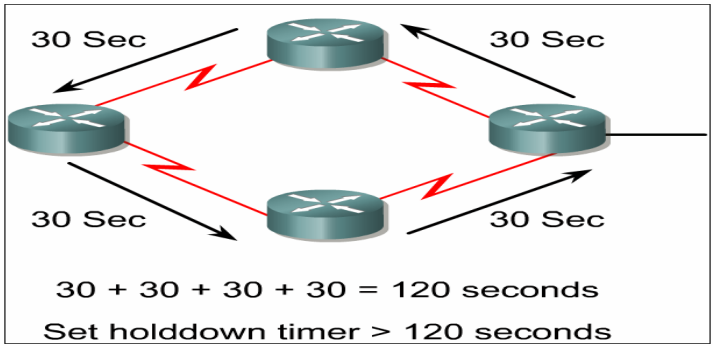
Thời gian holddown là một thông số mà ta có thể thay đổi nếu cần.

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. Ta có thể điều chỉnh cho thời gian ngắn lại để tăng tốc độ hội tụ nhưng ta phải 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 có thể để cho toàn bộ hệ thống cập nhật xong. Ví dụ như hình 4.4.4 ta có 4 router. ả ếu mỗi 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. ả hư vậy thì thời gian holddown phải dài hơn 120 giây.

Để thay đổi thời gian holddown ta dùng lệnh sau:

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



Hình 4.4.4

Một lý do khác làm ảnh hưởng tới tốc độ hội tụ là chu kỳ cập nhật. Chu kỳ cập nhật mặc định của RIP là 30 giây. Ta có thể điều chỉnh cho chu kỳ cập nhật dài hơn để tiết kiệm băng thông đường truyền hoặc là giút ngắn chu kỳ cập nhật để tăng tốc độ hội tụ.

Để thay đổi chu kỳ cập nhật ta dùng lệnh sau:

GAD(config-router)# update-time seconds

Còn một vấn đề ta hay gặp đối với các 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 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 bao. ả hà 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)#neighbor ip address

Phần mềm 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 chỉ gửi gói phiên bản 2 … bằng các lệnh sau:

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

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

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

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

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

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

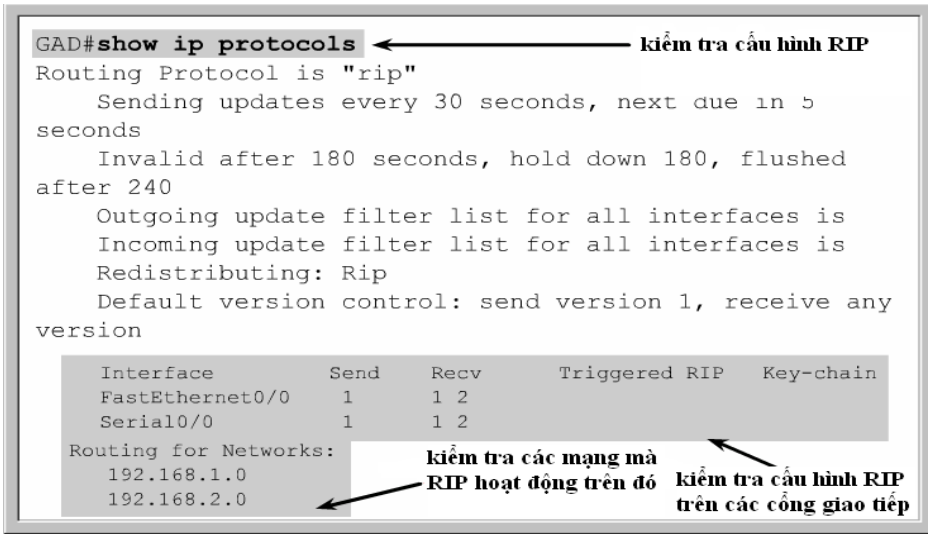
GAD(config-if)#ip rip receive version 1 2

4.5. Kiểm tra cấu hình RIP

Có rất nhiều lệnh có thể kiểm tra cấu hình RIP có đúng hay không. Trong đó 2 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 giúp ta kiểm tra được phần lớn cấu hình của RIP nhưng chưa phải đầy đủ toàn bộ. Sau đây ta cần chú ý một số điểm khi 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 nào có chính xác hay không.
- Các địa chỉ mạng được khai báo trên router để chạy RIP có đúng hay không.

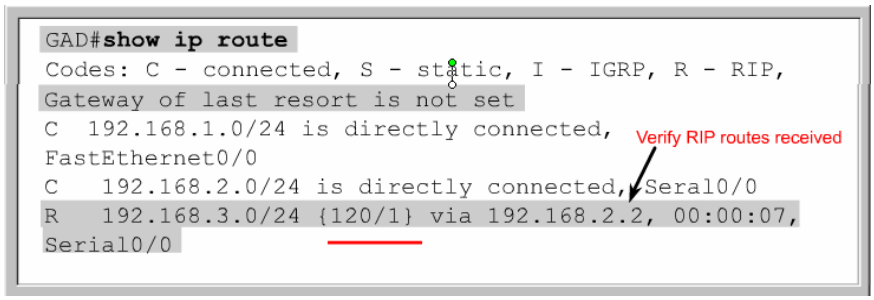


Hình 4.5 a

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 kết quả hiển thị bảng định tuyến, ta kiểm tra các đường có đánh dấu bằng chữ R ở đầu dòng mà những đương router học được từ các router rip láng giềng. Ta nên nhớ rằng các router 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.

ẩ goài ra còn có một số lệnh khác mà ta có thể sử dụng để kiểm tra cấu hình RIP:

- show interface *interface*
- show ip interface *interface*
- show running config

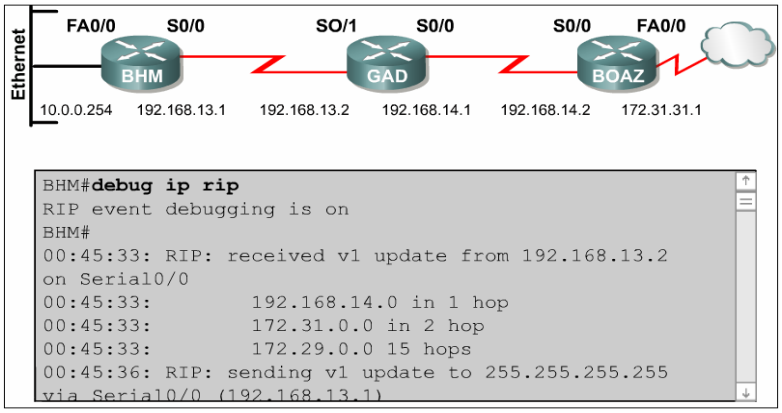


Hình 4.5b

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

Hầu hết các lỗi về cấu hình RIP đều do khai báo câu lệnh network sau, 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 3.2.6 cho ta thấy kết quả hiển thị của lệnh debug ip rip. Sauk hi 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 cho ta thấy router chạy rip v1 và rip 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 nhật RIP.



Hình 4.6

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

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

- show ip rip database
- show ip protocols (summary)
- show ip route
- debug ip rip (events)
- show ip interface brief

4.7. 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 router sử dụng giao thức định tuyến theo trạng thái đường liên kết thì cơ chế trên không hiệu quả vì các giao thức này quyết định chọn đường đi 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 sau chỉ sử dụng cho giao thức định tuyến theo vectơ khoảng cách nh RIP, IGRP thôi.

Ta 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, lệnh passive interface sẽ làm cho router ngừng gửi thông tin cập nhật về định tuyến cho 1 router láng giềng nào đó, nhưng router vẫn tiếp tục lắng nghe và nhận thông tin cập nhật từ router láng giềng đó

4.8. Chia tải với RIP

Router có thể chia tải theo nhiều đường khi có nhiều đường tốt đến cùng một đích.Bạn có thể cấu hình bằng tay cho route chia tải ra các đường hoặc la route các giao thức định tuyến độngcó thểtự động tính toán để chia tải. RIP có khả năng chia tải ra tối đa là 6 đường, có chi phí bằng nhau, còn mạc định thì rip chỉ chia tải ra 4 đường. RIP thực hiện chia tải bằng cách sử dụng lần lượt và luân phiên từng đường.

4.9. Chia tải cho nhiều đường

Router có khả năng chia tải ra nhiều đường để chuyển các gói dữ liệu đến cùng một 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(Administrative distance) nhỏ nhất để đặt vào bảng định tuyến. Trong trường hợp các đường này có cùng chỉ số tin cậy thì router thì router sẽ chọn đường nào có chi phí thấp nhất hoặc có thông số định tuyến nhỏ

nhất. Mỗi giao thức định tuyến có cách tính chi phí khác nhau và ta cần phải cấu hình các chi phí này để router thực hiện chia tai.

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 đường có cùng chi phí (thói 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 co phép tối đa là 4 đương.

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 một đường đến một đích.

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

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

IGRP có thể chia tải lên tối đa 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.

Khi định tuyến IP, Cisco IOS có 2 cơ chế chia tải là: Chia tải theo gói dữ liệu và chia tải theo địa chỉ đích. ẩ ếu router chuyển mạng theo tiến chình 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 các gói dữ liệu đến cùng một đích ra 1 đường. Các gói dữ liệu đến hop khác nhưng trong cùng một mạng đích thì sẽ tải ra đường kế tiếp. Cách này gọi là chia tải theo địa chỉ đích.

4.10. Tích hợp đường cố định với RIP

Đường cố định là do người quản trị cấu hình cho router chuyển gói tơi mạng đích theo đường mà mình muốn. Mặt khác, lệnh để cấu hình đường cố định cũng như 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 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.

Ta có thể xoá đường cố định bằng lệnh **no ip router** 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) mặc định. ẩ gười quản trị mạng có thể cấu hình một đường cố định tới một 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 số AD nhỏ hơn nên 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 cố định để chuyển gói dữ liệu đến mạng đích.

ẩ ếu ta cấu hình đường cố định chỉ ra một cổng 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 được xem như là kết nối trực tiếp vào router nên nó không còn bản chất là một đường cố định nữa. ẩ ếu ta cấu hình đường cố định chỉ ra một cổng mà RIP không chạy trên cổng đó thì RIP không gửi thông tin cập nhật về đường cố định đó, chừ khi ta phải cấu hình thêm lệnh **redistribute static** cho RIP.

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

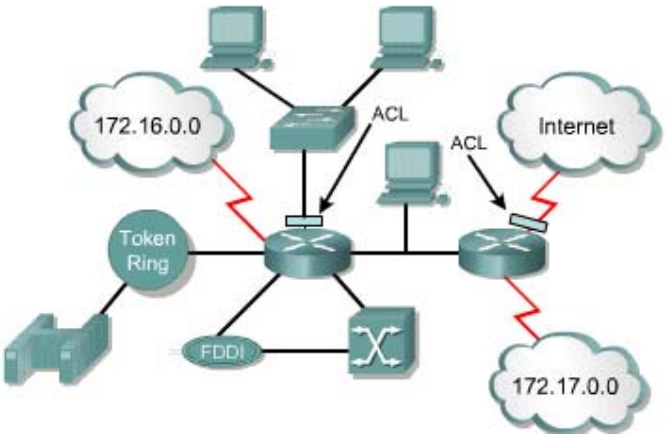
CHƯƠNG 5: DANH SÁCH TRUY CẬP ACLs

5.1. Cơ bản về Danh sách kiểm tra truy cập

5.1.1. ACL là gì ?

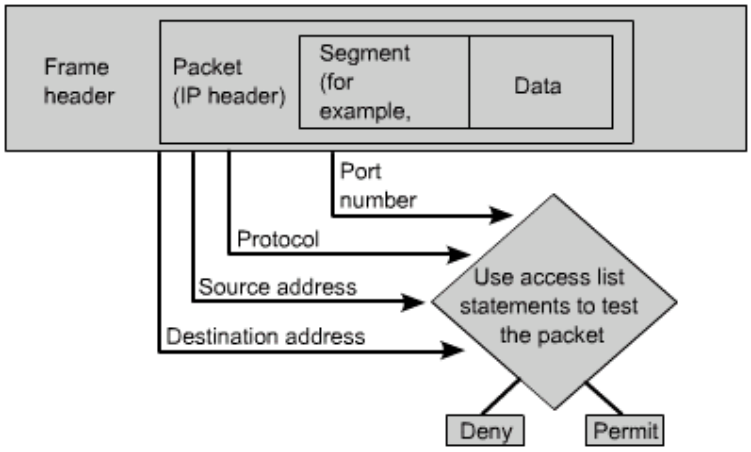
ACLs là một danh sách các điều kiện được áp dụng cho lưu lượng đi qua một cổng của Router. Danh sách này cho phép Router biết loại gói nào được chấp nhận hay bị từ chối dựa trên các điều kiện cụ thể. ACL được sử dụng để quản lý lưu lượng mạng và bảo vệ sự truy cập ra hoặc vào hệ thống mạng.

ACL có thể được tạo ra cho tất cả các giao thức được định tuyến như IP (Internet Protocol) và IPX (Internetwork Packet Exchange). ACL có thể được cấu hình trên router để kiểm tra việc truy cập và một mạng hay một subnet nào đó.



Hình 5.1. Ví dụ về ACL

ACL lọc tải bằng cách kiểm tra việc chuyển đi các gói đã được định tuyến xong hoặc là chặn ngay các gói vào cổng của router. Router kiểm tra từng gói một để quyết định là chuyển gói đi hay hủy bỏ gói đó tùy vào các điều kiện trong ACL như: địa chỉ nguồn và đích, giao thức và số port của lớp trên.



Hình 5.2. Cấu trúc về gói dữ liệu

Một số nguyên nhân chính để tạo ACLs:

Giới hạn lưu lượng mạng để tăng hiệu xuất hoạt động của mạng. Ví dụ, bằng cách giới hạn lưu lượng truyền video, ACLs đã làm giảm tải đáng kể và làm tăng hiệu suất của mạng.

Kiểm tra dòng lưu lượng. ACLs có thể giới hạn thông tin truy cập định tuyến.

Cung cấp chế độ bảo vệ truy cập cơ bản. ACLs có thể cho phép một host truy cập vào một phần nào đó của hệ thống mạng và ngăn không cho các host khác truy cập vào khu vực đó.

Quyết định loại lưu lượng được phép cho qua hay chặn lại trên các công của router. Ví dụ, lưu lượng của Email được phép cho qua nhưng tất cả lưu lượng của telnet đều bị chặn lại.

Cho phép người quản trị mạng điều khiển được các phạm vi mà các Client được quyền truy cập vào trong hệ thống mạng.

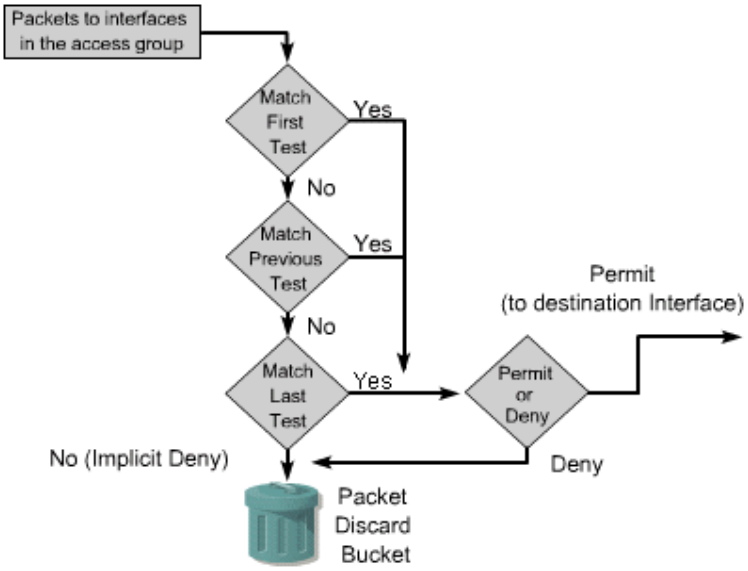
Kiểm tra host để cho phép hay từ chối không cho truy cập vào một khu vực nào đó trong hệ thống. ấ ếu trên router không có cấu hình ACLs thì tất cả các gói được chuyển đi đến mọi vị trí trong hệ thống mạng.

5.1.2. ACLs làm việc như thế nào

Mỗi ACLs là một danh sách các câu lệnh trong đó xác định gói dữ liệu nào được chấp nhận hay từ chối tại chiều ra hay chiều vào của một cổng trên Router. Mỗi một câu lệnh có các điều kiện và kết quả chấp nhận hay từ chối tương ứng. ấ ếu thoả điều kiện trong câu lệnh thì quyết định chấp nhận hay từ chối sẽ được thực hiện.

Thứ tự đặt các câu lệnh trong ACLs rất quan trọng.Phần mềm Cisco IOS sẽ kiểm tra gói dữ liệu với từng câu lệnh một theo đúng thứ tự từ trên xuống dưới. ấ ếu thoả điều kiện của một câu lệnh thì gói dữ liệu sẽ được chấp nhận hay từ chối ngay và toàn bộ các câu lệnh còn lại trong ACLs đó sẽ không phải kiểm tra nữa. ấ ếu không thoả điều kiện của tất cả các câu lệnh trong ACLs thì mặc định là cuối danh sách luôn có một câu lệnh ẩn "deny any" (từ chối tất cả).

ấ ếu bạn cần thêm một câu lệnh vào ACLs thì bạn phải xoá toàn bộ ACLs đi rồi tạo lại ACLs mới có câu lệnh mới.



Hình 5.3. Sơ đồ làm việc của ACLs

5.1.3. Tạo ACLs

ACLs được tạo trong chế độ cấu hình toàn cục. Có rất nhiều loại ACLs khác nhau, bao gồm: ACL cơ bản, ACL mở rộng, ACL cho IPX, AppleTalk và các giao thức khác. Khi cấu hình ACLs trên router mỗi ACL có một số xác định.

Protocol	Range
IP	1-99, 1300-1999
Extended IP	100-199, 2000-2699
AppleTalk	600-699
IPX	800-899
Extended IPX	900-999
IPX Service Advertising Protocol	1000-1099

Hình 5.4. Các thông số cấu hình ACL

Bắt đầu tạo ACLs bằng từ khóa *access-list*, theo sau là các tham số tương ứng của lệnh này. Trong chế độ chế độ cấu hình cổng của router, dùng lệnh *access-group* để gán

ACL tương ứng vào cổng đó. Khi gán ACL cho một cổng , cần xác định cụ thể ACL đó áp dụng cho chiều ra hay vào trên cổng của router. Để thay đổi ACL, dùng lệnh *no access-list list-number* để xóa tất cả các câu lệnh *access-list* có cùng *list-number*.

Các nguyên tắc cơ bản khi tạo và gán ACLs:

Một ACL cho một giao thức trên một chiều của một cổng.

ACL cơ bản nên đặt ở vị trí gần mạng đích nhất.

ACL mở rộng nên đặt ở gần mạng nguồn nhất

Đứng trong router để xác định chiều đi ra hay đi vào trên một cổng của router đó

Các câu lệnh trong một ACL sẽ được kiểm tra tuần tự từ trên xuống cho đến khi có một câu lệnh được thỏa. ẩ gược lại, nếu không có câu lệnh trong ACL thì gói dữ liệu đó sẽ bị từ chối.

```
Router(config)#access-list 2 deny 172.16.1.1
Router(config)#access-list 2 permit 172.16.1.0 0.0.0.255
Router(config)#access-list 2 deny 172.16.0.0 0.0.255.255
Router(config)#access-list 2 permit 172.0.0.0
0.255.255.255
Router(config)#interface e0
Router(config-if)#ip access-group 2 in
```

Hình 5.5. Cấu hình ACL cho một router

Trong thực tế, các lệnh của danh sách truy cập có thể là các xâu kí tự dài. Các danh sách truy cập có thể phức tạp khi nhập vào hoặc dịch ra.Tuy nhiên, bạn có thể đơn giản hoá các lệnh định cấu hình cho danh sách truy cập chung bằng cách giảm các lệnh bởi hai phần tử chung.

Mô hình tạo ACL:

Bước 1: Tạo các thông số cho câu lệnh kiểm tra danh sách truy cập này (có thể là một hoặc vài câu lệnh):

Router(config)#**access-list** *access-list-number {permit | deny} {test condition}*

***Bước 2*:** Cho phép một giao diện trở thành một phần của nhóm, nhóm mà sử dụng danh sách truy cập đã được xác định (kích hoạt access list trên interface).

Router(config-ip)#{protocol} **access-group** *access-list-number {in | out}*

access-list-number là số hiệu phân biệt các access list với nhau, đồng thời cũng cho biết là loại access list nào (standard hay extended)

Cập nhật các danh sách truy cập:

ả ếu các câu lệnh điều kiện thêm vào là cần thiết trong một danh sách truy cập thì cập nhật toàn bộ.

ACL phải được xoá và tạo lại với các câu lệnh điều kiện mới.

Xác định ACLs như thế nào?

Mỗi ACL được xác định duy nhất bằng cách gán một số (hoặc một tên) cho nó.

Số này xác định kiểu của danh sách truy cập được tạo và phải nằm trong phạm vi giới hạn đặc biệt của các chỉ số:

```
Rio(config)# access-list ?
  <1-99>        IP standard access list
  <100-199>     IP extended access list
  <200-299>     Protocol type-code access list
  <300-399>     DECnet access list
  <600-699>     Appletalk access list
  <700-799>     48-bit MAC address access list
  <800-899>     IPX standard access list
  <900-999>     IPX extended access list
 <1000-1099>    IPX SAP access list
 <1100-1199>    Extended 48-bit MAC address access list
 <1200-1299>    IPX summary address access list
 <1300-1999>    IP standard access list (expanded range)
 <2000-2699>    IP extended access list (expanded range)
```

Một ACL được số hoá không thể bị hiệu chỉnh trên router.

Để hiệu chỉnh một ACL:

Bước 1: Copy nó tới một file văn bản.

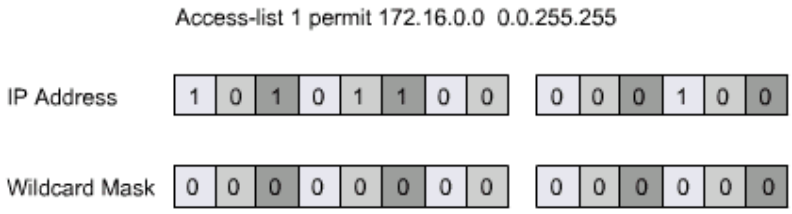
Bước 2: Gỡ bỏ từ cấu hình router với 'no' hình dạng của câu lệnh ACL

Bước 3: Tạo những thay đổi cần thiết cho lile văn bản.

Bước 4: Dán trở lại chế độ cấu hình chung.

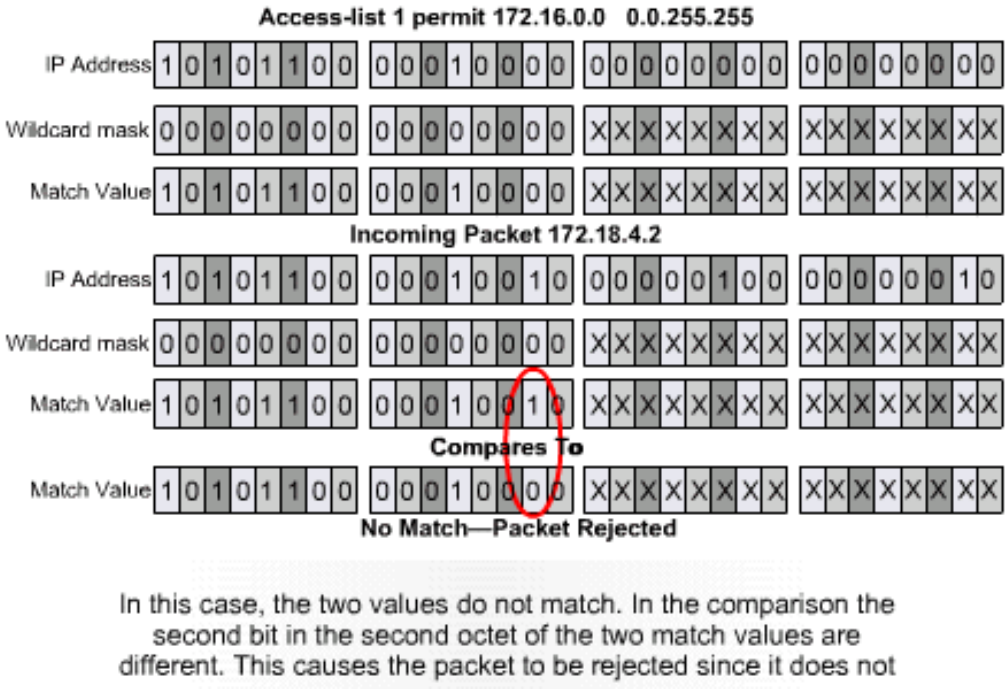
5.1.4. Chức năng của wildcard mask

Một wildcard mask dài 32 bit được chia làm 4 Octet. Mỗi một wildcard mask đi cùng với một địa chỉ IP. Số bit *0* và *1* trong wildcard mask được sử dụng để xác định cách xử lý bit tương ứng trong địa chỉ IP.



Hình 5.6. Cấu trúc của wildcard mask và địa chỉ IP

Subnet mask có chuỗi bit 1 bắt đầu từ trái kéo dài sang phải để xác định phần host và phần mạng trong một địa chỉ IP. Trong khi đó wildcard mask được thiết kế để lọc ra một địa chỉ IP riêng lẻ hay một nhóm địa chỉ IP để cho phép hay từ chối truy cập dựa trên địa chỉ IP. Giá trị *0* và *1* trong wildcard mask có ý nghĩa khác với bit *0* và *1* trong subnet mask. Để tránh nhầm lẫn, chữ x được sử dụng để thay thế bit 1 trong wildcard mask. Ví dụ, wildcard mask là 0.0.255.255. Bit 0 có nghĩa là bit tương ứng trong địa chỉ IP phải kiểm tra, còn bit x (bit 1) có nghĩa là bit tương ứng trong địa chỉ IP có thể bỏ qua không cần kiểm tra. Trong quá trình wildcard mask, địa chỉ IP trong mỗi câu lệnh được kết hợp với wildcard mask trong câu lệnh đó để tính ra giá trị chuẩn. Giá trị này dùng để so sánh với địa chỉ của các gói dữ liệu đang được kiểm tra bởi câu lệnh ACL. ả ếu hai giá trị này giống nhau thì có nghĩa là điều kiện về địa chỉ đã được thỏa mãn. Có hai từ khóa đặc biệt được sử dụng trong ACLs là *any* và *host*. Any đại diện cho IP 0.0.0.0 và wildcard mask là 255.255.255.255, host đại diện cho wildcard mask 0.0.0.0.



Hình 5.7. Quá trình kết hợp IP và wildcard mask

5.1.5. Kiểm tra ACLs

Có rất nhiều lệnh *show* được sử dụng và kiểm tra nội dung và vị trí đặt ACLs trên router. Lệnh *show ip interface* hiển thị thông tin của các cổng IP trên router và cho biết có ACLs được đặt trên các cổng hay không. Lệnh *show access-lists* sẽ hiển thị nội dung của tất cả các ACLs trên router. Để xem cụ thể một ACL nào thì cần thêm tên hoặc số vào sau câu lệnh *show access-lists*

```
Router#show access-lists
Standard IP access list 2
 deny   172.16.1.1
 permit 172.16.1.0, wildcard bits 0.0.0.255
 deny   172.16.0.0, wildcard bits 0.0.255.255
 permit 172.0.0.0, wildcard bits 0.255.255.255
Extended IP access list 101
 permit tcp 192.168.6.0 0.0.0.255 any eq telnet
 permit tcp 192.168.6.0 0.0.0.255 any eq ftp
 permit tcp 192.168.0.0 0.0.0.255 any eq ftp-data
Router#
```

Hình 5.8. Ví dụ về một lệnh show

5.2. Danh sách kiểm tra truy cập

5.2.1. ACLs cơ bản

ACLs cơ bản thực hiện kiểm tra địa chỉ IP nguồn của gói dữ liệu. Kết quả kiểm tra sẽ dẫn đến kết quả là cho phép hay từ chối truy cập toàn bộ các giao thức dựa trên địa chỉ mạng, subnet hay host. Trong chế độ cấu hình toàn cục, lệnh *access-list* được sử dụng để tạo ACL cơ bản với số ACL nằm trong khoảng từ 1 đến 99.

Ví dụ:

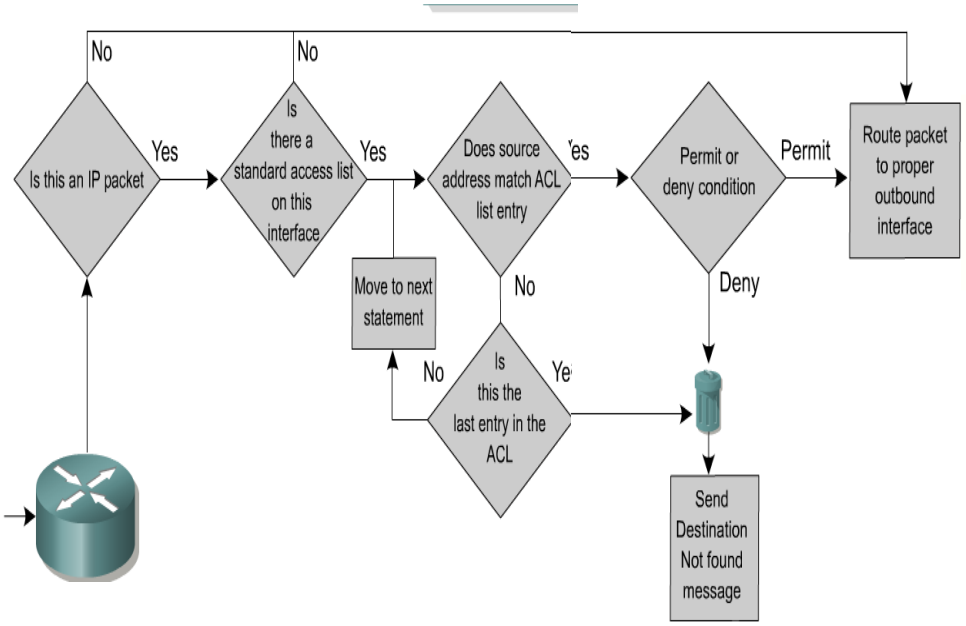
Access-list 2 deny 172.16.1.1

Access-list 2 permit 172.16.1.0 0.0.0.255

Access-list 2 deny 172.16.0.0 0.0.255.255

Access-list 2 permit 172.0.0.0 0.255.255.255

Câu lệnh ACL đầu tiên không có wildcard mask, trong trường hợp này wildcard mask mặc định được sử dụng là 0.0.0.0. Điều này có nghĩa là toàn bộ địa chỉ 172.16.1.1 phải được thỏa, nếu không thì router sẽ phải kiểm tra câu lệnh kế tiếp trong ACL.



Hình 5.9. Hoạt động của ACL cơ bản

Cấu trúc đầy đủ của lệnh ACL cơ bản:

Router(config)#access-list access-list-number {deny / permit}

Source [source wildcard] [log]

Dạng *no* của câu lệnh được sử dụng để xóa ACLs:

Router(config)#no access-list access-list-number

5.2.2. ACLs mở rộng

ACLs mở rộng thường được sử dụng nhiều hơn ACLs cơ bản vì nó có khả năng kiểm soát lớn hơn nhiều. ACLs mở rộng kiểm tra địa chỉ nguồn và đích của gói dữ liệu, kiểm tra cả giao thức với số cổng. Do đó rất thuận tiện trong việc cấu hình các điều kiện kiểm tra cho ACL. Gói dữ liệu được chấp nhận hay từ chối là dựa trên vị trí xuất phát và đích đến của gói dữ liệu cùng với loại giao thức và số cổng của nó. Ví dụ, một ACL mở rộng có thể cho phép lưu lượng của Email từ cổng Fa0/0 ra cổng S0/0 và từ chối các lưu lượng của Web và FTP. Khi gói dữ liệu bị hủy bỏ vì bị từ chối, một số giao thức sẽ gửi thông điệp phản hồi về cho máy gửi để thông báo là dữ liệu không đến đích được.

Trong một ACL có thể có nhiều câu lệnh. Các câu lệnh có cùng số ACL là nằm trong cùng một danh sách ACL. Có thể cấu hình số lượng ACL với số lượng không hạn chế và chỉ phụ thuộc vào dung lượng bộ nhớ của router.

Ví dụ:

Access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq telnet

Access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp

Access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp-data

Ở cuối câu lệnh ACL mở rộng có thông số về số port TCP và UDP để xác định chính xác hơn loại gói dữ liệu. Có thể xác định số port bằng các tham số *eq* (equal: bằng), *neq* (not equal: không bằng), *gt* (greater: lớn hơn), *lt* (less than: nhỏ hơn). ACL mở rộng sử dụng số ACL từ 100 đến 199 (và từ 2000 đến 2699 đối với các IOS gần đây).

Lệnh ip *access-group* được sử dụng để gán một ACL mở rộng đã có vào một cổng của router. Một ACL cho một giao thức cho một chiều trên một cổng.

Ví dụ:

Router(config-if)#**ip access-group** *access-list-number {in | out}*

5.2.3. Đặt tên ACLs

Đặt tên ACLs có những ưu điểm sau:

Xác định ACL bằng tên sẽ mang tính trực giác hơn

ACLs đặt tên có thể chỉnh sửa mà không cần phải xóa toàn bộ ACLs rồi viết lại từ đầu như ACLs đặt theo số.

Không còn bị giới hạn tối đa 798 ACLs cơ bản và 799 ACLs mở rộng.

Ví dụ về cấu hình đặt tên ACL:

Tả (config)#***ip access-list*** *extended server-access*

Tả (config-ext-nacl)#***permit TCP any host 131.108.101.99 eq mstp***

Tả (config-ext-nacl)#***permit UDP any host 131.108.101.99 eq domain***

Tả (config-ext-nacl)#***deny ip any any***

Tả (config-ext-nacl)#^Z

Applying the name list:

Tả (config)#***interface*** *fastethernet 0/0*

Tả (config-if)#***ip access-group*** *server-access out*

Tả (config-if)#^Z

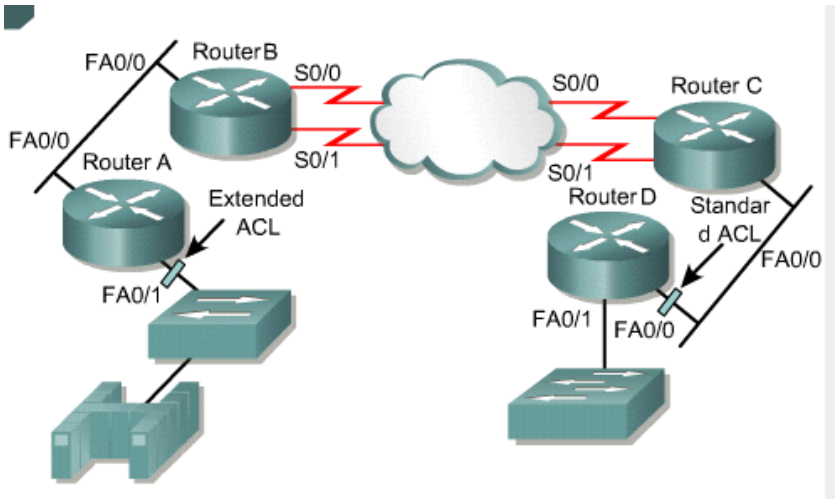
<u>Những điểm cần lưu ý khi thực hiện đặt tên ACLs:</u>

ACLs đặt tên không tương thích với các Cisco IOS phiên bản trước 11.2,

Không sử dụng chung một tên cho nhiều ACLs khác nhau. Ví dụ, không thể có một ACL cơ bản và một ACLs mở rộng có cùng tên là Tả .

5.2.4. Vị trí đặt ACLs

ACLs được sử dụng để kiểm soát lưu lượng bằng cách lọc gói dữ liệu và loại bỏ các lưu lượng không mong muốn trên mạng. Vị trí đặt ACLs rất quan trọng, nó giúp cho hoạt động của toàn bộ hệ thống mạng được hiệu quả.

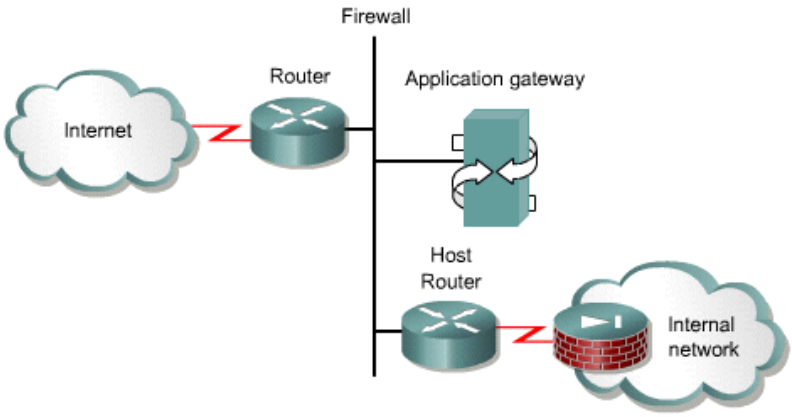


Hình 5.10. Vị trí đặt ACLs

ả guyên tắc chung là: Đặt ACLs mở rộng càng gần nguồn của nguồn lưu lượng mà ta muốn chặn lại càng tốt. ACLs cơ bản không xác định địa chỉ đích nên đặt chúng ở càng gần đích càng tốt.

5.2.5. Bức tường lửa

Bức tường lửa là một cấu trúc ngăn giữa người dùng bên trong hệ thống mạng với hệ thống bên ngoài để tránh những kẻ xâm nhập bất hợp pháp. Một bức tường lửa bao gồm nhiều thiết bị làm việc cùng nhau để ngăn chặn các truy cập không mong muốn.



Hình 5.11. Cấu trúc bức tường lửa

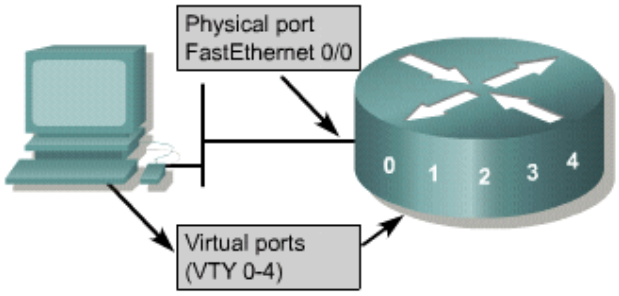
Trong cấu trúc này, router kết nối ra Internet được gọi là router ngoại vi, sẽ đưa tất cả các lưu lượng nhận vào đến Application gateway. Kết quả là gateway có thể kiểm soát việc phân phối các dịch vụ đi ra và đi vào hệ thống mạng. Khi đó, chỉ những user nào được phép mới có thể kết nối ra Internet hoặc là chỉ những ứng dụng nào được phép mới có

thể thiết lập kết nối cho host bên trong và bên ngoài. Điều này giúp bảo vệ Application gateway và tránh cho nó bị quá tải bởi những gói dữ liệu vốn là sẽ bị hủy bỏ.

Do đó ACLs đặt trên router đóng vai trò như bức tường lửa, đó là những router ở vị trí trung gian giữa mạng bên trong và mạng bên ngoài. Router bức tường lửa này sẽ cách ly cho toàn bộ hệ thống mạng bên trong tránh bị tấn công. ACLs cũng nên sử dụng trên router ở vị trí trung gian kết nối giữa hai phần của hệ thống mạng và kiểm soát hoạt động giữa hai phần này.

5.2.6. Giới hạn truy cập vào đường vty trên router

ACLs cơ bản và mở rộng đều có hiệu quả đối với các gói dữ liệu đi qua router. ả hưng chúng không chặn được các gói dữ liệu xuất phát từ chính bản thân router đó. Do đó một ACL mở rộng ngăn hướng Telnet ra sẽ không thể ngăn chặn được các phiên Telnet xuất phát từ chính router đó.



Hình 5.12. Truy cập vào đường vty trên router

Trên router có các cổng vật lý như cổng Fa0/0 và S0/0 cũng có các cổng ảo. Các cổng này gọi là đường vty được đánh số từ 0 đến 4. Giới hạn truy cập vào đường vty sẽ tăng khả năng bảo vệ cho hệ thống mạng. Quá trình tạo vty ACLs cũng giống như tạo các ACL khác, nhưng khi đặt ACLs vào đường vty thì dùng lệnh *access-class* thay vì dùng lệnh *access-group*

Ví du:

Creating the standard list:

Router1(config)#*access-list 2 permit 172.16.1.0 0.0.0.255*

Router1(config)#*access-list 2 permit 172.16.2.0 0.0.0.255*

Router1(config)#*access-list 2 deny any*

Applying the access list:

Router1(config)#*line vty 0 4*

Router1(config-line)#*password secret*

Router1(config-line)#*access-class 2 in*

Router1(config-line)#*login*

TÀI LIỆU THAM KHẢO

[1]. Cisco Certified ả etwork Associate – Semester 2 – Cisco Press

[2]. Interconnecting Cisco ả etwork Devices - Cisco Press

[3]. www.cisco.com