



GT.0000023441

CÔNG NGHỆ THÔNG TIN HỮU NGHỊ VIỆT - HÀN

Giáo trình

CHUYỂN MẠCH

VÀ ĐỊNH TUYẾN



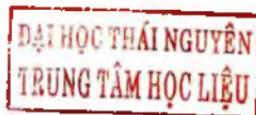
ThS. TRẦN QUỐC VIỆT



NHÀ XUẤT BẢN THÔNG TIN VÀ TRUYỀN THÔNG

TRƯỜNG CAO ĐẲNG CÔNG NGHỆ THÔNG TIN HỮU NGHỊ VIỆT - HÀN

Giáo trình
CHUYỂN MẠCH
VÀ ĐỊNH TUYẾN



NHÀ XUẤT BẢN THÔNG TIN VÀ TRUYỀN THÔNG

LỜI NÓI ĐẦU

Mạng máy tính ngày càng có vai trò quan trọng trong quá trình phát triển kinh tế xã hội của đất nước. Trong đó việc quản trị và cấu hình cho các thiết bị mạng như thiết bị định tuyến, thiết bị chuyển mạch là nhiệm vụ cần thiết khi triển khai các hệ thống mạng.

Các kiến thức về chuyển mạch và định tuyến bao gồm: môi trường làm việc, giao thức, phương thức làm việc của các thiết bị chuyển mạch, cách đánh địa chỉ IP và phân lớp địa chỉ IP; kỹ thuật định tuyến tĩnh, định tuyến động và các giao thức định tuyến động cũng như cách thức cấu hình và quản trị các thiết bị định tuyến trong môi trường mạng...

Với mục đích trang bị cho các sinh viên những kiến thức, kỹ năng và các vấn đề liên quan đến các thiết bị nói trên, Trường Cao đẳng Công nghệ Thông tin Hữu nghị Việt - Hàn phối hợp với Nhà xuất bản Thông tin và Truyền thông xuất bản “Giáo trình chuyển mạch và định tuyến”.

Giáo trình gồm 11 chương được chia thành hai phần cụ thể như sau:

Phần 1: Chuyển mạch

Chương 1: Tổng quan về Mạng nội bộ - LAN

Chương 2: Vận hành thiết bị trong mạng LAN

Chương 3: Mạng nội bộ áo- VLAN

Chương 4: Giao thức cây bao phủ (Spanning Tree Protocols)

Phần 2: Định tuyến

Chương 5: Địa chỉ IP và phân mạng con

Chương 6: Vận hành Router Cisco

Chương 7: Định tuyến tĩnh và con đường kết nối trực tiếp

Chương 8: Chính sách kiểm soát truy cập

Chương 9: Giao thức định tuyến

*Chương 10: Định tuyến trên hệ thống có phân chia mạng con
với mặt nạ mạng thay đổi*

Chương 11: Cấu hình kết nối mạng điện rộng - WAN

Với các kiến thức mà cuốn giáo trình mang lại sẽ giúp cho sinh viên nắm bắt được các nguyên tắc cơ bản về chuyên mạch và định tuyến cũng như cách thức vận hành quản trị cho các thiết bị trong môi trường mạng LAN trên thực tế của các doanh nghiệp.

Mặc dù đã có nhiều cố gắng trong công tác biên soạn, song giáo trình được xuất bản lần đầu sẽ khó tránh khỏi thiếu sót. Rất mong nhận được ý kiến đóng góp của các bạn đồng nghiệp để giáo trình được hoàn thiện hơn trong lần xuất bản tiếp theo.

*Mọi ý kiến đóng góp xin gửi về: Trường Cao đẳng Công nghệ Thông tin
Hữu nghị Việt - Hàn, Điện thoại: (0511) 3962377, Fax: (0511) 3962973.*

Xin trân trọng giới thiệu cùng bạn đọc./.

Đà Nẵng, tháng 01 năm 2011

**TRƯỜNG CAO ĐẲNG CNTT
HỮU NGHỊ VIỆT - HÀN**

PHẦN 1

CHUYỂN MẠCH

Nội dung phần này tập trung các vấn đề liên quan đến kỹ thuật chuyển mạch và vận hành các thiết bị chuyển mạch trong mạng LAN (*Local Area Network – Mạng nội bộ*). Nội dung phần này gồm 4 chương cụ thể như sau:

Chương 1. Tổng quan về mạng nội bộ - LAN: Giới thiệu những kiến thức cơ bản về mạng LAN, bao gồm phương tiện kết nối, thiết bị sử dụng và một số khái niệm cơ bản khác như địa chỉ Ethernet, các thiết bị chuyển mạch và nguyên tắc hoạt động của các thiết bị chuyển mạch.

Chương 2. Vận hành thiết bị trong mạng LAN: Giới thiệu những kiến thức và kỹ năng làm việc trên các thiết bị chuyển mạch như chế độ làm việc theo dòng lệnh, cấu hình chức năng cho thiết bị switch.

Chương 3. Mạng nội bộảo- VLAN:

Khái niệm về VLAN

Cách thức xây dựng trung kế chuyển mạch

Mạng con IP và VLAN

Giao thức trung kế VLAN

Vận hành VTP server, client

Chương 4. Giao thức cây bao phủ (Spanning Tree Protocols): Tìm hiểu về giao thức cây bao phủ, hoạt động và cách thức cấu hình cũng như một số khái niệm khác nhằm giúp cho các thiết bị switch Cisco tránh vòng lặp nội bộ.

Chương 1

TỔNG QUAN VỀ MẠNG NỘI BỘ - LAN

1.1. CƠ SỞ VỀ LAN

Trong một số giáo trình như Mạng máy tính và TCP/IP đã khảo sát một số vấn đề có liên quan đến các giao thức và tiêu chuẩn trong mạng LAN. Các tiêu chuẩn lớp Vật lý và Liên kết dữ liệu hoạt động cùng với nhau để cho phép các máy tính gửi các bit cho nhau thông qua một loại môi trường mạng Vật lý cụ thể nào đó. Lớp Vật lý của mô hình OSI xác định cách thức để gửi các bit qua một môi trường mạng, đảm bảo cho việc chuyển đổi giữa các loại tín hiệu quang, điện, sóng, tần số, các phương pháp điều chế tín hiệu. Lớp Liên kết dữ liệu (Lớp 2) xác định một số quy luật về cách dữ liệu được truyền đi, bao gồm các địa chỉ xác định thiết bị gửi đi và các thiết bị sẽ nhận được và các quy tắc khi nào một thiết bị có thể gửi và nhận các tín hiệu đó.

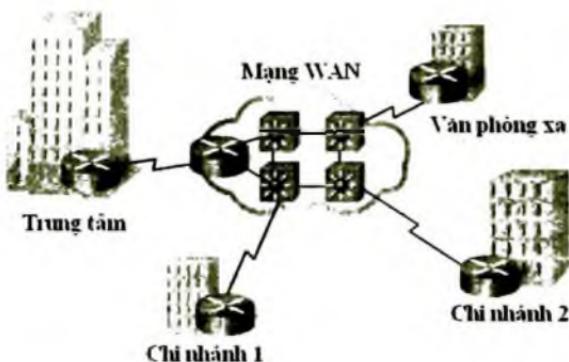
Chương này giải thích một số kiến thức cơ sở về LAN, *là môi trường hoạt động chủ yếu của thiết bị chuyển mạch – switch*. Thuật ngữ LAN ám chỉ đến một tập hợp các tiêu chuẩn lớp 1 và lớp 2 được thiết kế để làm việc với nhau nhằm mục đích là triển khai các mạng con trong phạm vi địa lý nhỏ. Chương này giới thiệu các khái niệm về LAN cụ thể là Ethernet LAN.

1.1.1. Giới thiệu

Một hệ thống mạng máy tính của doanh nghiệp thông thường bao gồm nhiều khu vực khác nhau. Thiết bị người dùng đầu cuối trong một khu vực kết nối với nhau trong một LAN, cho phép các máy tính cục bộ

truyền thông với nhau. Mỗi khu vực có một thiết bị định tuyến - router kết nối mạng LAN của khu vực này với mạng LAN của khu vực khác. Việc sử dụng router và WAN cho phép các máy tính ở các khu vực khác nhau có thể chia sẻ thông tin.

Hình 1.1 cho thấy sơ đồ kết nối trong một mạng máy tính của một doanh nghiệp với nhiều khu vực khác nhau.



Hình 1.1. Sơ đồ kết nối mạng của một doanh nghiệp

Phần nội dung của chương này tập trung vào cách thức xây dựng mạng LAN hiện nay. Trong đó, tập trung vào các công nghệ có sẵn, như là Token Ring, FDDI (Fiber Distributed Data Interface) và ATM (Asynchronous Transfer Mode). Tuy nhiên, phần này sẽ quan tâm chủ yếu đến Ethernet, chuẩn mạng LAN sử dụng rộng rãi nhất, được trở thành chuẩn cho mạng LAN đang được sử dụng.

1.1.2. Tổng quan LAN Ethernet

1.1.2.1. Các chuẩn mạng Ethernet

Thuật ngữ Ethernet xem xét một dòng các tiêu chuẩn xác định các yếu tố liên quan đến vật lý và Liên kết dữ liệu của công nghệ LAN thông dụng nhất trên thế giới. Các chuẩn này khác nhau về tốc độ hỗ trợ, với các tốc độ 10Mbit/s, 100Mbit/s, và 1000Mbit/s (1Gigabit trên giây, hay

Gbit/s). Các chuẩn này cũng khác nhau về loại kết nối cáp và chiều dài đầu cáp cho phép. Ví dụ, các chuẩn sử dụng phổ biến nhất của Ethernet là cáp xoắn đôi không vỏ bọc UTP, với chi phí thấp và các chuẩn khác sử dụng cáp quang đắt tiền hơn. Để thỏa mãn các yêu cầu khác nhau cho việc tạo dựng một LAN như là: tốc độ, giá cả, tính bảo mật và các yếu tố khác, nhiều loại chuẩn Ethernet khác nhau đã được tạo ra.

Học viện Kỹ nghệ và Điện tử Hoa Kì (IEEE - Institute of Electrical and Electronic Engineers) đã định nghĩa nhiều chuẩn Ethernet LAN và nó trở nên phổ biến kể từ đầu những năm 1980. Hầu hết các chuẩn định nghĩa một loại công nghệ khác nhau về Ethernet tại lớp Vật lý, với các khác biệt về tốc độ và loại đầu cáp. Ngoài ra, với lớp Liên kết dữ liệu, IEEE phân chia thành hai lớp con như sau:

- Lớp con điều khiển truy cập đường truyền MAC 802.3
- Lớp con điều khiển liên kết logic LLC 802.2

Mỗi chuẩn Vật lý mới từ IEEE yêu cầu nhiều khác biệt trong lớp Vật lý. Tuy nhiên, chúng kế thừa lại tiêu đề 802.3 trong lớp con điều khiển truy cập đường truyền 802.3 MAC, và lớp con điều khiển liên kết luận lý 802.2 LLC. Bảng 1 – 1 liệt kê các chuẩn lớp Vật lý được sử dụng thông dụng nhất của IEEE.

Bảng 1.1. Các chuẩn Vật lý của công nghệ Ethernet

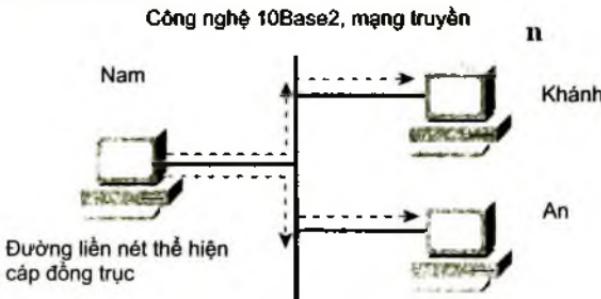
Tên thông dụng	Tốc độ	Tên khác	Tên theo chuẩn IEEE	Loại cáp, chiều dài tối đa
Ethernet	10 Mbit/s	10BASE – T	IEEE 802.3	Đồng, 100m
Fast Ethernet	100 Mbit/s	100BASE-TX	IEEE 802.3u	Đồng, 100m
Giga Ethernet	1000 Mbit/s	1000BASE-LX, 1000BASE-SX	IEEE 802.3z	Quang, 550m (SX) 5km (LX)
Giga Ethernet	1000 Mbit/s	1000BASE-T	IEEE 802.3ab	Đồng, 100m

1.1.2.2. Các chuẩn nguyên thủy của Ethernet: 10Base2 và 10Base5

Chuẩn mạng LAN 10Base2 và 10Base5 là hai chuẩn mạng Ethernet đầu tiên, mô tả chi tiết các lớp Vật lý và Liên kết dữ liệu cho các mạng Ethernet trước dây. Trong hai loại mạng nói trên, yêu cầu cài đặt một

chuỗi cáp đồng trục kết nối mỗi thiết bị trên một mạng Ethernet. Với công nghệ này, việc kết nối mạng không sử dụng các thiết bị mạng nào, mà chỉ đơn giản là tập hợp các NIC (Network Interface Card – các giao tiếp mạng) máy tính và được nối lại bằng cáp đồng trục. Sợi cáp này tạo ra một kênh truyền tín hiệu điện, gọi là một kênh truyền, mỗi trường chia sẻ chung cho tất cả thiết bị trên Ethernet. Khi một máy tính muốn gửi một số bit đến máy tính khác trên kênh truyền, nó gửi một tín hiệu điện, và tín hiệu điện được tái tạo cho tất cả thiết bị khác trên Ethernet đó.

Hình 1.2 thể hiện ý nghĩa cơ bản của một mạng Ethernet 10Base2 truyền thống, sử dụng một kênh truyền điện đơn được tạo với cáp đồng trục và card Ethernet.



Hình 1.2. Sơ đồ mạng Ethernet

Các đường liên kết biểu thị cho việc nối cáp Vật lý. Các đường nét đứt với mũi tên biểu thị cho con đường mà frame của Nam được truyền. Nam gửi một tín hiệu điện từ dọc theo Ethernet NIC của mình để vào cáp. Khi đó cả Khánh, An nhận được tín hiệu, cáp này tạo ra một kênh tín hiệu điện Vật lý, nghĩa là tín hiệu truyền đi sẽ được nhận bởi tất cả các máy trạm trên LAN. Giống như là một điểm dừng xe buýt tại mỗi ngôi nhà của sinh viên dọc theo tuyến đường, tín hiệu điện trên một mạng 10Base2 hay 10Base5 được tái tạo tại mỗi trạm trên LAN.

Bởi vì mạng sử dụng một đường kênh truyền tín hiệu đơn, nếu hai hay nhiều hơn các tín hiệu được gửi tại cùng một thời điểm, chúng sẽ trùng lên nhau và phát sinh xung đột, làm cho cả hai tín hiệu không thể

nhận dạng được. Vì thế, Ethernet định nghĩa cơ chế để đảm bảo rằng chỉ một thiết bị gửi tín hiệu trên Ethernet tại một thời điểm. Nếu không, Ethernet sẽ không thể sử dụng được. Giải thuật này, được biết với tên là giải thuật đa truy cập cảm biến sóng mang với phát hiện xung đột (CSMA/CD), xác định cách thức truy cập đường truyền.

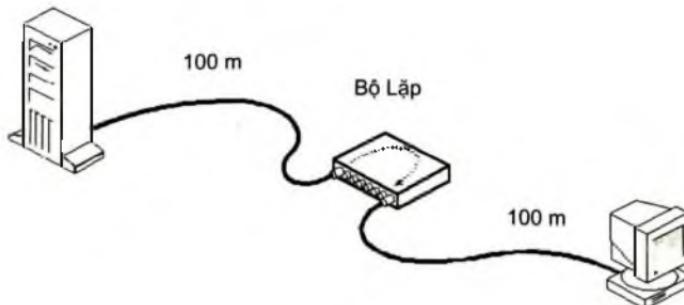
Giải thuật CSMA/CD có thể được tóm tắt như sau:

- Một thiết bị muốn gửi một frame phải đợi cho đến khi LAN rỗi, nói cách khác là không có frame nào đang được gửi đi – trước khi thử gửi một tín hiệu điện.
- Nếu xung đột xảy ra, các thiết bị gây ra xung đột phải đợi một khoảng thời gian ngẫu nhiên và sau đó thử lại lần nữa.

Trong mạng LAN 10Base2 và 10Base5, một xung đột xảy ra bởi vì có nhiều tín hiệu điện được truyền dọc theo toàn thể chiều dài của kênh truyền. Khi hai trạm gửi tại cùng thời điểm, các tín hiệu điện của chúng trùng nhau, dẫn đến xung đột. Vì thế tất cả các thiết bị trên một mạng 10Base2 và 10Base5 sử dụng CSMA/CD để tránh xung đột và để phục hồi khi một xung đột xảy ra.

1.1.2.3. Sử dụng Bộ lặp – Repeater trong mạng 10Base2 và 10Base5

Giống như các loại LAN, 10Base2 và 10Base5 có giới hạn về chiều dài cáp tối đa. Với 10Base5, giới hạn là 500m; với 10Base2, là 185m, tốc độ chung là 10Mbit/s.



Hình 1.3. Sử dụng bộ lặp trong mạng 10Base2 và 10Base5

Trong một số trường hợp, chiều dài cáp lớn hơn chiều dài cáp tối đa, vì thế một thiết bị có tên là bộ lặp được phát triển nhằm giải quyết một trong những vấn đề giới hạn chiều dài của cáp là tín hiệu được gửi bởi một thiết bị có thể suy hao quá nhiều nếu chiều dài cáp lớn hơn 500m hay 185m.

Bộ lặp – Repeater kết nối nhiều phân đoạn cáp lại với nhau, nhận tín hiệu điện trên một cáp, biên dịch thành các bit 0 và 1, và tạo lại một tín hiệu sạch, mới hoàn toàn ra các sợi cáp khác cùng kết nối đến bộ lặp đó. Một bộ lặp không đơn giản là khuếch đại tín hiệu, bởi vì việc khuếch đại tín hiệu có thể cũng khuếch đại nhiễu phát sinh trên đường.

Một số đặc điểm cần ghi nhớ về mạng 10Base2 và 10Base5 là:

- Mạng Ethernet nguyên thủy tạo một kênh truyền tín hiệu điện đến tất cả các thiết bị có kết nối.
- Vì xung đột có thể xảy ra trên kênh truyền này, Ethernet định nghĩa giải thuật CDMA/CD, xác định cách thức để tránh xung đột và thực hiện hành động khi xung đột xảy ra.
- Bộ lặp mở rộng chiều dài của LAN bằng cách nhận tín hiệu điện và tái tạo lại nó – chức năng lớp 1 – nhưng không dịch ra ý nghĩa của tín hiệu điện này.

1.1.2.4. Chuẩn 10BaseT, 100BaseTX và 1000BaseT

Sau đó IEEE định nghĩa các chuẩn Ethernet mới bên cạnh 10Base2 và 10Base5. Chuẩn 10BaseT (xuất hiện năm 1990), 100Base-TX (1995) và 1000Base-T (1999), với đặc điểm chung là sử dụng cáp xoắn đôi. Để hỗ trợ cho các chuẩn mới này, các thiết bị có tên là hub và switch cũng được tạo ra. Phần này giới thiệu cơ bản cách thức các loại mạng Ethernet thông dụng này hoạt động, bao gồm hoạt động cơ bản của hub và switch.

10BaseT giải quyết nhiều vấn đề tồn tại trong các công nghệ 10Base5 và 10Base2 Ethernet. 10BaseT cho phép sử dụng cáp UTP đã có sẵn. Thậm chí nếu cáp UTP mới được cài đặt, thì nó cũng đơn giản và rẻ tiền hơn nhiều so với cáp đồng trục cũ được sử dụng trong công nghệ 10Base2 và 10Base5.

Cài tiến chính khác được giới thiệu với 10BaseT là việc sử dụng một hub (thiết bị tập trung đầu nối) để kết nối các thiết bị mạng lại với nhau. Hình 1.4 cho thấy việc sử dụng hub trong một Ethernet.



Hình 1.4. Mạng Ethernet sử dụng hub

Hub cơ bản là bộ lặp với nhiều cổng. Điều này có nghĩa là hub đơn giản chỉ tái tạo lại tín hiệu điện đến từ một cổng và gửi lại tín hiệu đó ra ngoài mỗi cổng khác. Như thế, với bất kì LAN sử dụng hub, như trong hình 1.4, sẽ tạo một kênh truyền tín hiệu điện, như là 10Base2 và 10Base5. Chính vì thế, xung đột có thể vẫn xảy ra, nên quy tắc truy cập CSMA/ CD tiếp tục được sử dụng.

Các mạng 10Base - T sử dụng hub để giải quyết một số vấn đề với 10Base2 và 10Base5. Trước tiên, LAN sẽ có độ ổn định cao hơn. Vì với một sợi cáp đơn bị hỏng có thể làm đứt mạng LAN 10Base2 và 10Base5, còn với 10Base - T, một cáp kết nối thiết bị với thiết bị tập trung, vì thế một cáp đơn bị hỏng ảnh hưởng đến duy nhất một thiết bị. Ngoài ra việc sử dụng cáp nối UTP, trong một sơ đồ mạng sao (tất cả các cáp chạy trên một thiết bị kết nối tập trung), giảm thiểu chi phí mua sắm và cài đặt cáp.

Ngày nay, hub hiếm khi được sử dụng, thay vào đó là switch. Tuy nhiên, hoạt động của switch về cơ bản là khá giống hub. Các switch thực hiện công việc tốt hơn hub, hỗ trợ nhiều chức năng hơn hub, và thường có giá thấp như hub. Và sau đây là tóm tắt các kiến thức cơ bản về LAN:

- Mạng LAN nguyên thủy tạo một kênh truyền điện đến tất cả các thiết bị có kết nối.

- Bộ lắp 10Base2 và 10Base5 mở rộng độ dài của LAN bằng cách tái tạo lại tín hiệu đến – chức năng lớp 1 – nhưng không dịch ý nghĩa của các tín hiệu điện.
- Hub là bộ lắp cung cấp điểm kết nối tập trung với cáp nối UTP – nhưng chúng cũng vẫn tạo một kênh truyền điện đơn, được chia sẻ bởi nhiều thiết bị khác nhau, như là 10Base2 và 10Base5.

Bởi vì các xung đột có thể xảy ra trong những trường hợp này, Ethernet định nghĩa giải thuật CSMA/CD bảo cho thiết bị cách thúc để cả hai tránh xung đột và thực hiện các hành động khi xung đột xảy ra.

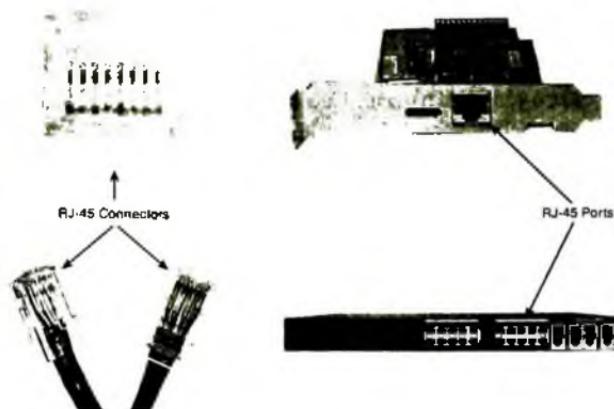
1.1.3. Đầu nối bằng cáp UTP Ethernet

Ba chuẩn Ethernet thông dụng nhất được sử dụng ngày nay là: 10Base-T (Ethernet), 100Base-TX (Fast Ethernet) và 1000Base-T (Gigabit Ethernet) sử dụng cáp UTP. Tuy nhiên có một số khác biệt chính, cụ thể là số cặp dây cần cho mỗi trường hợp, và loại cáp đầu nối. Phần này sẽ xem xét một số chi tiết liên quan đến UTP, chỉ ra những khác biệt giữa những chuẩn này. Cụ thể là mô tả cáp và đầu nối trên cáp, cách sử dụng các cặp dây trong cáp để truyền dữ liệu và chân đầu ra được yêu cầu cho mỗi phương thức hoạt động khác nhau.

1.1.3.1. Cáp UTP và đầu nối RJ-45

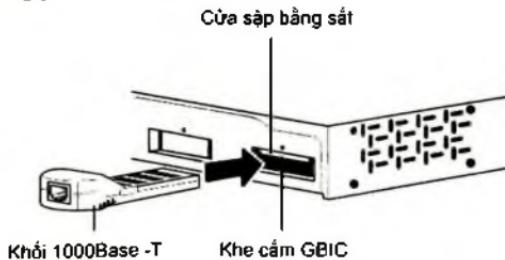
Cáp UTP được sử dụng bởi các chuẩn Ethernet thông dụng bao gồm hai hay bốn sợi dây. Vì các sợi dây bên trong cáp là mảnh, sợi cáp có một lớp bọc nhựa bên ngoài để bảo vệ. Mỗi sợi cáp đồng này cũng có một lớp bọc nhựa khác bên ngoài để bảo vệ sợi dây khỏi bị gãy. Mỗi vỏ bọc trên mỗi sợi cáp có một màu khác nhau, để dễ xem xét trên cả hai đầu cuối của cáp và xác định mỗi đầu cáp với nhau.

Đầu cuối cáp thường có một số dạng đầu nối với các đầu cuối của dây được chèn vào đầu nối này. Đầu nối RJ - 45 có 8 vị trí Vật lý xác định để gắn 8 dây trong cáp có thể được chèn vào, được gọi là vị trí đầu chân, hay đơn giản là chân. Khi đầu nối được thêm vào cuối của cáp, đầu cuối của dây phải được chèn một cách chính xác vào đúng vị trí chân đó.



Hình 1.5. Các đầu nối và cổng RJ-45

Trên hình 1.5 trên cho thấy các chân của đầu nối RJ-45, các cổng RJ-45 trên NIC của máy tính và trên giao tiếp của switch. Ngoài các đầu nối và cổng giao tiếp thông dụng này, có thể sử dụng các cổng khác có thể thay đổi mà không cần phải mua một switch mới. Nhiều switch Cisco có một vài giao tiếp sử dụng hoặc là bộ chuyển đổi giao tiếp Gigabit (GBIC) hay các đầu nối cỡ nhỏ (SFP). Cả hai đều là các thiết bị có thể tháo rời phù hợp với một cổng hay một giao tiếp trên switch. Vì Cisco chế tạo nhiều GBIC và SFP cho mọi chuẩn Ethernet, switch có thể sử dụng nhiều đầu nối cắm cáp và các loại cáp và hỗ trợ các loại cáp có chiều dài khác nhau. Vì vậy có thể lựa chọn các thành phần bổ sung phù hợp mà không phải tốn nhiều tiền để mua các thiết bị mới.



Hình 1.6. Module quang 1Gbit/s bổ sung

1.1.3.2. Truyền tải dữ liệu sử dụng cáp xoắn đôi

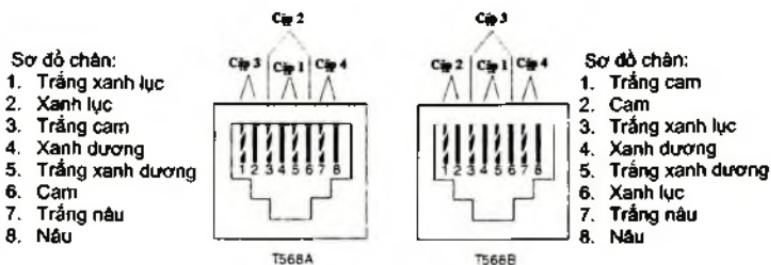
Cáp xoắn đôi thực chất gồm các cặp dây phù hợp được xoắn lại với nhau – vì thế có tên là cáp xoắn. Các thiết bị trên mỗi đầu của cáp có thể tạo một kênh tín hiệu điện sử dụng một cặp sợi dây bằng cách gửi dòng điện trên hai sợi dây, trên hai phía đối diện. Khi dòng điện qua bát kí sợi dây nào, dòng điện tạo ra trường điện từ bên ngoài sợi dây dẫn; trường điện từ có thể làm cho nhiễu điện từ trên hai cặp dây bất kí. Bằng cách xoắn đôi lại với nhau thành từng cặp, với dòng điện trong hai hướng đối diện trên mỗi sợi dây, trường điện từ được tạo ra bởi một sợi hầu như không ảnh hưởng đến trường điện từ được tạo ra bởi sợi kia. Bởi vì đặc tính này, hầu hết cáp mạng sử dụng cáp đồng và cáp điện sử dụng cặp dây xoắn đôi để gửi dữ liệu.

Để gửi dữ liệu qua kênh điện tử được tạo qua cặp dây, thiết bị sử dụng một cơ chế mã hóa xác định cách thức tín hiệu điện tử có thể khác nhau, qua thời gian, có nghĩa là giá trị nhị phân 0 hay 1. Ví dụ, 10BaseT sử dụng cơ chế mã hóa để mã hóa một số nhị phân 0 thành sự chuyển dịch từ điện thế cao hơn xuống điện thế thấp hơn trong khoảng thời gian 1/10.000.000 giây.

1.1.3.3. Sơ đồ đầu chân của 10BaseT và 100BaseTX

Các sợi dây trong cáp UTP phải được kết nối đến đúng vị trí chân trong đầu nối RJ-45 để việc truyền thông được chính xác. Đầu nối RJ-45 có 8 vị trí chân, hay đơn giản là chân, trong đó sợi cáp đồng được cắm vào đầu nối. Sơ đồ đầu chân – mô tả việc lựa chọn màu nào được đi cùng với vị trí chân phù hợp – tuân theo chuẩn Ethernet được mô tả trong phần này.

Thú vị là, IEEE không thực sự định nghĩa chuẩn chính thức cho các nhà sản xuất cáp, cũng như là chi tiết ràng buộc được sử dụng cho sơ đồ chân cáp. Hai tổ chức: TIA (Hiệp hội Công nghiệp Viễn thông) và EIA (Liên minh Công nghiệp Điện tử), định nghĩa các tiêu chuẩn cho đầu cáp UTP, mã màu cho các sợi cáp và chuẩn đầu ra trên các sợi cáp. Hình 1.7 cho thấy hai chuẩn chân đầu ra của EIA/TIA với mã màu và số cặp đã được liệt kê.



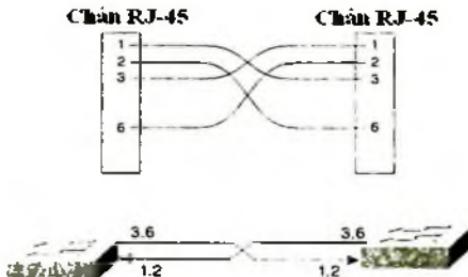
Hình 1.7. Sơ đồ đầu chân cáp chuẩn T568A và T568B

Để hiểu về các từ viết tắt được liệt kê trong hình, chú ý tám sợi dây trong cáp có màu đồng nhất (lục, cam, lam hay nâu) hay màu xen kẽ giữa trắng và bốn màu nói trên. Tương tự, một sợi cáp đơn sử dụng cùng màu cơ bản như vậy. Ví dụ, sợi dây màu lam và trắng lam xen kẽ sẽ là một cặp và được xoắn đôi. Để tạo một LAN Ethernet, phải chọn hay kết nối các cáp sử dụng đúng chân trên mỗi đầu cuối cáp đó. Cáp 10BaseT và 100BaseTX Ethernet xác định mỗi cặp sẽ được sử dụng để gửi dữ liệu trên một hướng, và cặp ngược lại được sử dụng để gửi dữ liệu trên hướng ngược lại. Cụ thể, Ethernet NICs sẽ gửi dữ liệu sử dụng cặp chân có kết nối đến các chân 1 và 2, hay là cặp 3 dựa theo chuẩn chân T568A. Tương tự, Ethernet NICs sẽ nhận dữ liệu sử dụng cặp ở các chân 3 và 6 – cặp 2 theo chuẩn 568A. Còn switch và hub thì ngược lại, chúng nhận dữ liệu trên cặp dây chân 1, 2 (cặp 3 trên T568A), và gửi dữ liệu trên cặp tại chân 3,6 (cặp 2 trên 568A).



Hình 1.8. Truyền tín hiệu trên cáp thẳng

Hình 1.8 cho thấy việc sử dụng cáp thẳng – straight – through. Loại cáp này được sử dụng để kết nối máy tính hoặc router với switch và hub, trong đó chân 1 và 2 kết nối với chân 1 và 2, tương tự cho chân 3 và 6. Cáp thẳng được sử dụng khi các thiết bị trên các đầu cuối khác nhau của cáp sử dụng các chân trái ngược khi truyền dữ liệu. Tuy nhiên, khi kết nối hai thiết bị sử dụng cùng chân để truyền, chân của cáp phải được thiết lập để hoán đổi vị trí cho nhau. Loại cáp này được gọi là cáp chéo – crossover. Các loại cáp này được sử dụng để kết nối các switch với hub hoặc máy tính với router.



Hình 1.9. Truyền tín hiệu trên cáp chéo

Phản đầu của hình 1.9 cho thấy các chân được kết nối. Chân 1 bên trái kết nối với chân 3 bên phải, chân 2 bên trái kết nối chân 6 bên phải, chân 3 bên trái kết nối chân 1 bên phải và chân 6 bên trái kết nối chân 2 bên phải. Bên dưới của hình cho thấy các dây của các chân 3, 6 mỗi bên – các chân mỗi switch sử dụng để truyền – kết nối chân 1, 2 trên mỗi phía, chính vì thế cho phép các thiết bị nhận trên các chân 1 và 2. Hình 1.10 cho thấy các loại cáp thẳng và chéo được dùng trong thực tế.



Hình 1.10. Kết nối thiết bị mạng LAN

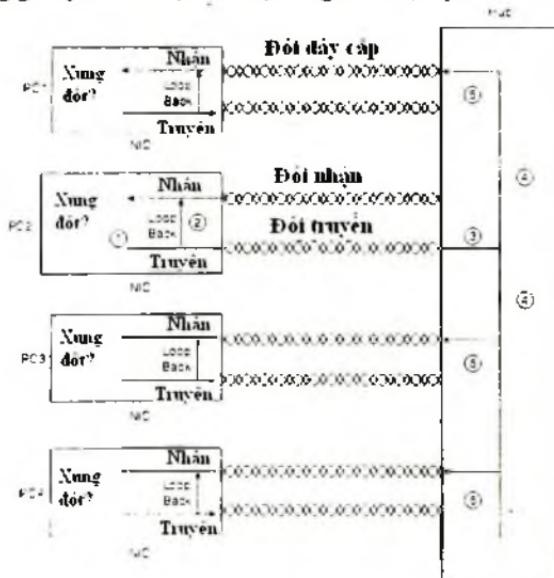
1.1.3.4. Cáp 1000Base – T

Như đã ghi nhận trước đây, cáp 1000BaseT khác so với cáp 10BaseT và 100BaseTX về cách đấu nối và chân. Trước tiên, cáp 1000BaseT yêu cầu bốn cặp dây, tương tự, việc truyền và nhận trên Gigabit Ethernet diễn ra trên bốn cặp dây đồng thời.

Tuy nhiên, Gigabit Ethernet cũng có các loại cáp thẳng và cáp chéo, với một ít khác biệt về các loại cáp chéo. Chân của cáp thẳng 1000Base – T là tương tự 100Base – T, với chân 1 nối với chân 1, chân 2 nối với chân 2... Cáp chéo 1000Base – T tương tự như là Ethernet, cặp dây chân 1, 2 nối với cặp dây chân 3, 6 và cặp dây chân 4, 5 nối với cặp dây chân 7, 8.

1.1.3.5. Sử dụng switch trong LAN

Phần này xem xét một số vấn đề liên quan đến tính khả thi khi sử dụng hub, giải thích cách các switch LAN xử lý hai vấn đề thực thi lớn nhất tồn tại khi sử dụng hub. Để xem xét vấn đề tốt hơn, xem ví dụ hình 1.11, thể hiện những gì xảy ra khi một thiết bị đơn gửi dữ liệu qua hub.



Hình 1.11. Nguyên tắc hoạt động của hub

Hình 1.11 cho thấy cách hub tạo ra một kênh truyền tín hiệu điện, các bước trong hình được mô tả như sau:

Bước 1: Card mạng gửi một frame.

Bước 2: NIC lặp frame đã gửi trong cặp dây nhận bên trong của card đã gửi

Bước 3: Hub nhận tín hiệu điện, biên dịch tín hiệu thành các bit để nó có thể được làm sạch nhiều và lặp lại tín hiệu này.

Bước 4: Hub lặp lại bên trong dây tín hiệu ra tất cả các port khác, nhưng không quay lại port đã gửi tín hiệu mà từ đó nó nhận.

Bước 5: Hub lặp lại tín hiệu đến tất cả các sợi dây nhận trên tất cả các thiết bị khác.

Chú ý rằng một hub luôn lặp lại tín hiệu điện ra tất cả các port, trừ port từ đó tín hiệu đã được nhận. Hình 1.11 không cho thấy trường hợp bị xung đột. Tuy nhiên, nếu PC1 và PC2 gửi một tín hiệu điện cùng lúc, tại bước 4 tín hiệu điện này có thể bị chồng lấp, frame sẽ bị xung đột và cả hai frame có thể không nhận dạng được hay là chúa lỗi.

Giải thuật CSMA/CD giúp ngăn ngừa xung đột và cũng xác định cách để thực hiện khi xung đột xảy ra. Giải thuật này như sau:

Bước 1: Một thiết bị với một frame cần gửi lắng nghe cho đến khi Ethernet không bận

Bước 2: Khi Ethernet không bận, máy gửi bắt đầu gửi frame đi.

Bước 3: Máy gửi lắng nghe để chắc chắn không có xung đột xảy ra.

Bước 4: Nếu có xung đột xảy ra, các thiết bị vừa gửi frame đi gửi một tín hiệu xung đột để đảm bảo rằng tất cả các máy khác ghi nhận được xung đột này

Bước 5: Sau khi tín hiệu xung đột hoàn tất, mỗi máy ngẫu nhiên một thời gian và chờ đợi trước khi thử gửi lại frame đã bị xung đột.

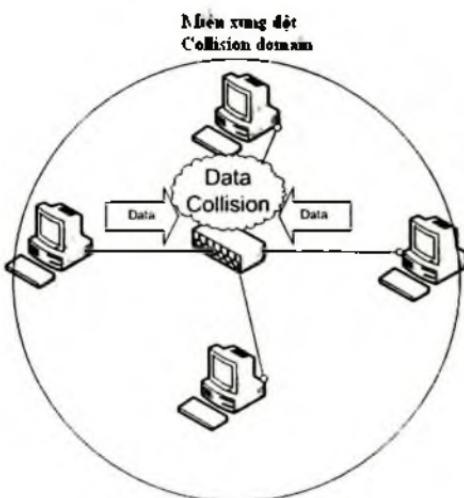
Bước 6: Khi thời gian ngẫu nhiên này kết thúc, tiến trình bắt đầu lại với bước 1.

CSMA/CD không ngăn ngừa xung đột, nhưng nó đảm bảo rằng Ethernet làm việc tốt ngay cả khi xung đột có thể xảy ra. Tuy nhiên, giải thuật CSMA/CD tạo nên vấn đề về thực thi. Trước tiên, CSMA/CD làm cho các thiết bị phải đợi cho đến khi Ethernet rãnh rồi trước khi gửi dữ liệu. Tiến trình này giúp tránh xung đột, nhưng nó có nghĩa là chỉ một thiết bị có thể gửi dữ liệu tại một thời điểm. Kết quả là tất cả các thiết bị được kết nối đến cùng hub chia sẻ chung băng thông có sẵn qua hub. Cơ chế này được gọi là bán song công – half duplex. Điều này ám chỉ rằng thiết bị chỉ gửi hay nhận dữ liệu tại một thời điểm, nhưng không bao giờ thực hiện cả hai tại một thời điểm.

Chức năng chính khác của CSMA/CD xác định điều gì xảy ra khi có xung đột. Khi xung đột xảy ra, mục đích của CSMA/CD là làm cho các thiết bị gửi các frame dữ liệu xung đột chờ đợi trong một khoảng thời gian ngẫu nhiên, và sau đó thử lại. Điều này giúp cho LAN hoạt động được mà không bị xung đột một lần nữa, nhưng lại ảnh hưởng đến khả năng thực thi của hệ thống. Trong quá trình xung đột, không có dữ liệu nào được chuyển qua LAN. Tương tự, các thiết bị tranh chấp phải đợi lâu hơn trước khi thử sử dụng lại LAN. Ngoài ra, khi tải trên Ethernet tăng, khả năng xung đột cũng tăng theo. Thực ra, trong những năm trước khi thiết bị chuyển mạch LAN ra đời và giải quyết các vấn đề liên quan đến thực thi, thì khả năng thực thi của Ethernet bắt đầu suy giảm khi tải bắt đầu vượt quá 30 phần trăm, chủ yếu do sự gia tăng xung đột.

1.1.3.5. Tăng băng thông bằng cách sử dụng thiết bị chuyển mạch

Thuật ngữ miền xung đột xác định một tập hợp các thiết bị chứa các frame có thể xung đột. Tất cả các thiết bị trên mạng 10Base2, 10Base5 hay mạng sử dụng hub có khả năng xung đột giữa các frame mà nó gửi đi, vì thế tất cả các thiết bị trên trong các loại mạng Ethernet này sẽ ở trong cùng một miền xung đột. Ví dụ, tất cả bốn thiết bị có kết nối đến hub trong hình 1.12 là trong cùng một miền xung đột. Để tránh xung đột, và để khôi phục khi nó xảy ra, các thiết bị trong cùng miền xung đột sử dụng CSMA/CD.



Hình 1.12. Miền xung đột

Các thiết bị chuyển mạch LAN giám thiêu đáng kể hay thậm chí ngăn ngừa hiện tượng xung đột trên LAN. Không như hub, switch không tạo một đường truyền chia sẻ đơn, chuyển tiếp các tín hiệu điện nhận được ra tất cả các cổng. Thay vào đó, switch thực hiện công việc như sau:

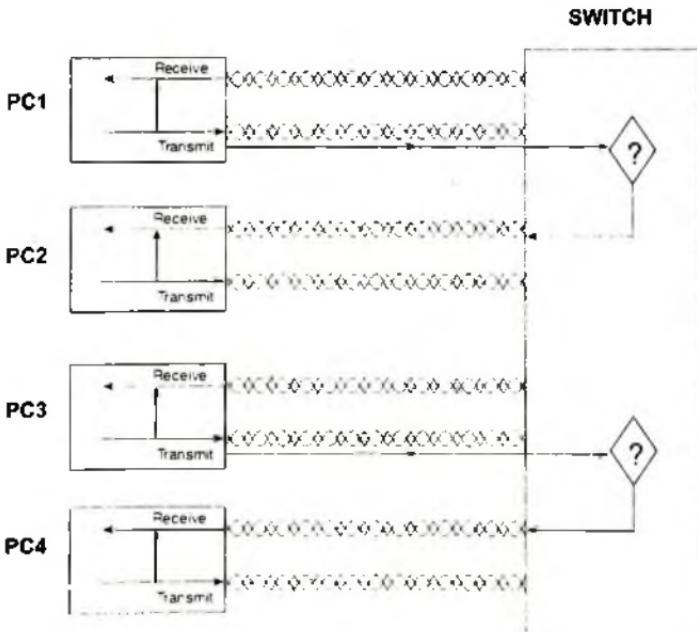
- Switch dịch các bit trong các frame nhận được để nó có thể gửi một cách bình thường các frame ra ngoài một port được yêu cầu, thay vì ra tất cả các port.
- Nếu một switch cần chuyển tiếp nhiều frame ra ngoài cùng một port, switch lưu trữ đệm các frame trong bộ nhớ, rồi gửi cùng lúc, nhằm tránh xung đột.

Hình 1.12 mô tả cách một switch có thể chuyển tiếp hai frame cùng lúc nhằm tránh xung đột, khi cả hai PC1 và PC3 gửi cùng lúc. Trong trường hợp này, PC1 gửi một frame dữ liệu với địa chỉ đích là PC2 và PC3 gửi một frame dữ liệu với địa chỉ đích là PC4. Switch xem xét địa chỉ Ethernet đích và gửi frame từ PC1 đến PC2 cùng lúc với frame được gửi từ PC3 đến PC4. Với một hub được sử dụng, thì có thể xảy ra xung đột; tuy nhiên, switch không gửi các frame ra ngoài tất cả các port khác, nên nó ngăn ngừa xung đột.

Việc lưu trữ đệm cũng giúp ngăn ngừa xung đột. Tưởng tượng rằng PC1 và PC3 cả hai gửi dữ liệu đến PC4 cùng lúc. Switch, biết rằng việc chuyển hai frame đến PC4 cùng lúc sẽ có thể gây ra xung đột. Vì thế nó lưu đệm một frame, cho đến khi frame đầu tiên đã được gửi hoàn toàn cho PC4.

Điều này giúp cải tiến đáng kể khả năng thực thi của hệ thống khi so sánh với việc sử dụng hub. Cụ thể là:

- Nếu chỉ một thiết bị được nối cáp đến mỗi port trên switch, không thể xảy ra xung đột.
- Các thiết bị kết nối đến một port switch không chia sẻ băng thông với các thiết bị kết nối trên các port switch khác. Mỗi port có một băng thông riêng rẽ, nghĩa là một switch với các port 100Mbit/s có băng thông 100Mbit/s cho mỗi port.



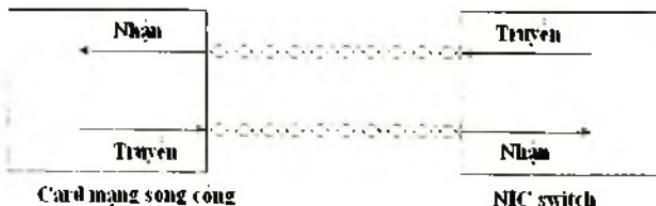
Hình 1.13. Hoạt động của switch

Điểm thứ hai quan tâm đến các khái niệm Ethernet chia sẻ và Ethernet chuyên mạch. Như đã đề cập trong phần trước của chương, Ethernet chia sẻ có nghĩa là băng thông LAN được chia sẻ giữa nhiều thiết bị trên LAN bởi vì chúng thay phiên nhau sử dụng LAN với giải thuật CSMA/CD. Thuật ngữ LAN chuyên mạch có nghĩa là, với các switch, băng thông không phải chia sẻ, cho phép độ thực thi lớn hơn. Ví dụ, một hub với 24 thiết bị Ethernet tốc độ 100Mbit/s có kết nối đến cho phép tối đa theo lý thuyết một đường truyền băng thông 100Mbit/s. Tuy nhiên, một switch với 24 port Ethernet 100Mbit/s được kết nối cho phép hỗ trợ 100Mbit/s mỗi port, hay băng thông theo lý thuyết tối đa là 2400Mbit/s (2,4Gbit/s).

1.1.3.7. Tăng khả năng thực thi bằng cách sử dụng bán song công

Bất kì mạng Ethernet nào sử dụng hub cũng yêu cầu CSMA/CD để có thể hoạt động tốt. Tuy nhiên, CSMA/CD lại khiến cho Ethernet chỉ có thể truyền theo chế độ bán song công, nghĩa là chỉ một thiết bị có thể gửi tại một thời điểm. Vì các switch có thể lưu đệm các frame trong bộ nhớ, switch có thể hoàn toàn ngăn ngừa xung đột trên các port switch có kết nối đến nó. Kết quả là, các LAN switch cho phép sử dụng chế độ song công trên tất cả các port. Song công có nghĩa là các card Ethernet có thể gửi và nhận dữ liệu đồng thời.

Để giải thích vì sao xung đột không thể xảy ra, xem xét hình 1.14, cho thấy một kênh song công được sử dụng với một PC kết nối với LAN switch.



Hình 1.14. Chế độ song công – Full Duplex

Với chỉ một switch và một thiết bị kết nối, xung đột không thể xảy ra. Khi triển khai song công, switch đã bỏ đi chức năng CSMA/CD trên

các thiết bị ở cả hai đầu cáp. Bằng cách này, khả năng thực thi của Ethernet trên cáp đã được nhân đôi bằng cách cho phép truyền đồng thời trên cả hai hướng.

1.1.3.8. Tổng quan về lớp 1 Ethernet

Trong phần này nghiên cứu một cách cơ bản làm thế nào để xây dựng mạng LAN Ethernet lớp 1 sử dụng hub và switch. Phần này cũng đã giải thích cách sử dụng cáp UTP, đầu nối RJ-45, để kết nối các thiết bị đến hub hoặc là switch. Tài liệu cũng đã đề cập đến lý thuyết chung về các thiết bị gửi dữ liệu bằng cách mã hóa nhiều tín hiệu điện tử khác nhau qua một kênh truyền điện, với kênh được tạo ra sử dụng cặp dây bên trong cáp UTP. Quan trọng hơn, phần này đã giải thích cặp dây nào được sử dụng để truyền và nhận dữ liệu. Cuối cùng, hoạt động cơ bản của các switch được giải thích, bao gồm các giới hạn tiềm ẩn về miền xung đột, với kết quả là cải tiến đáng kể khả năng thực thi so với hub.

1.1.4. Giao thức Liên kết dữ liệu Ethernet

Một trong những cải tiến mạnh mẽ của bộ giao thức Ethernet là những giao thức này sử dụng một tập các chuẩn Liên kết dữ liệu nhỏ. Ví dụ, địa chỉ Ethernet làm việc tương tự trên các phiên bản của Ethernet, từ 10Base5 cho đến 10Gbit/s Ethernet – bao gồm các chuẩn Ethernet sử dụng các loại kết nối cáp khác bên cạnh UTP. Tương tự, giải thuật CSMA/CD thường tham gia vào lớp Liên kết dữ liệu, áp dụng cho hầu hết các loại Ethernet, trừ khi nó bị bỏ qua.

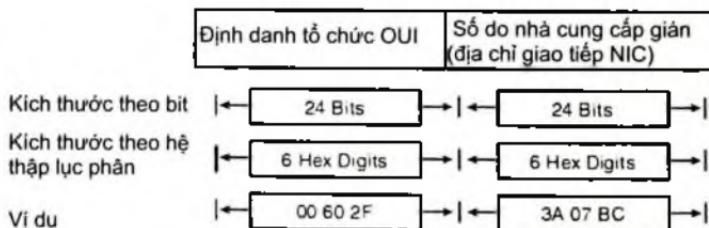
Phần này xem xét hầu hết các chi tiết của bộ giao thức Liên kết dữ liệu Ethernet – cụ thể là địa chỉ Ethernet, xây dựng khung, phát hiện lỗi và xác định loại dữ liệu bên trong frame Ethernet.

1.1.4.1. Địa chỉ Ethernet

Địa chỉ Ethernet xác định hoặc là địa chỉ đơn hay nhóm thiết bị trên một LAN. Mỗi địa chỉ dài 6 byte, thường được viết theo dạng thập lục phân, và trong các thiết bị Cisco, được viết phân tách với các dấu chấm cho mỗi nhóm bốn kí tự thập lục phân. Ví dụ: 0000.1021.3466 là một địa chỉ Ethernet hợp lệ.

Các địa chỉ Ethernet unicast xác định một card LAN đơn. Các máy tính dùng các địa chỉ unicast để xác định máy gửi và nhận của một frame Ethernet. Nếu một máy tính A muốn gửi một frame đến cho máy tính B, nó sẽ sử dụng địa chỉ Ethernet của máy tính A để làm địa chỉ nguồn, địa chỉ Ethernet B của máy tính B làm địa chỉ đích. Gói tin Ethernet được truyền đi trên mạng LAN. Các máy tính khác sẽ nhận và kiểm tra gói tin Ethernet này, nếu địa chỉ Ethernet của nó trùng với địa chỉ Ethernet đích trong gói tin, thì máy tính đó (trường hợp này là B) sẽ xử lý nó. Các máy tính khác đơn giản bỏ qua dữ liệu nhận được.

IEEE định nghĩa và gán cho các địa chỉ LAN Ethernet. IEEE yêu cầu địa chỉ MAC unicast duy nhất toàn cầu trên tất cả các card giao tiếp LAN. IEEE gọi nó là địa chỉ unicast vì các giao thức MAC như là 802.3 định nghĩa các chi tiết cho việc đánh địa chỉ này. Để đảm bảo một địa chỉ MAC duy nhất, nhà sản xuất card Ethernet mã hóa địa chỉ MAC trên mỗi card đó, thường là sử dụng chip ROM. Phần đầu tiên của địa chỉ này xác định nhà sản xuất của card. Mã này, được gán cho mỗi nhà sản xuất bởi IEEE, được gọi là định danh duy nhất của nhà sản xuất OUI (Organization Unique Identifier). Mỗi nhà sản xuất gán một địa chỉ MAC với định danh duy nhất của tổ chức đó là phần đầu tiên của địa chỉ, với phần thứ hai của địa chỉ được gán là một số mà nhà sản xuất không bao giờ sử dụng trên một card khác.



Hình 1.15. Địa chỉ Ethernet

Có nhiều thuật ngữ có thể được sử dụng để mô tả các địa chỉ LAN unicast. Mỗi card LAN đi với một địa chỉ gắn sẵn được ghi vào chip

ROM trên card. Địa chỉ này có thể được xem như là địa chỉ LAN, địa chỉ Ethernet hay là địa chỉ phần cứng Vật lý cho thiết bị.

Các địa chỉ nhóm xác định hơn một địa chỉ MAC Ethernet. IEEE định nghĩa hai nhóm địa chỉ chung cho Ethernet:

- Địa chỉ Broadcast: Được sử dụng thường xuyên nhất bởi các địa chỉ MAC nhóm của IEEE, địa chỉ quảng bá, có giá trị FFFF.FFFF.FFFF. Địa chỉ quảng bá nhấn mạnh rằng tất cả thiết bị trên LAN cần xử lý frame này.
- Địa chỉ multicast: Được sử dụng để cho phép một tập con các thiết bị trên LAN truyền thông với nhau, có định dạng là 0100.5xxx.xxxx

1.1.4.2. Khung Ethernet

Khung Ethernet xác định cách một chuỗi các số nhị phân được dịch. Nói cách khác, khung xác định ý nghĩa của các bit được chuyển đi trên mạng. Lớp Vật lý giúp lấy một chuỗi các bit từ một thiết bị sang một thiết bị khác. Thuật ngữ khung xem xét định nghĩa của các trường trong dữ liệu được nhận.

DIX						
Preamble	Destination	Source	Type	Data and Pad	FCS	
8	6	6	2	46 – 1500	4	

IEEE 802.3 (Original)						
Preamble	SFD	Destination	Source	Length	Data and Pad	FCS
7	1	6	6	2	46 – 1500	4

IEEE 802.3 (Revised 1997)							
Bytes	Preamble	SFD	Destination	Source	Length/ Type 2	Data and Pad	FCS
	7	1	6	6		46 – 1500	4

Hình 1.16. Tiêu đề khung Ethernet

Bảng 1.2 cho thấy một số trường quan trọng trong tiêu đề khung Ethernet

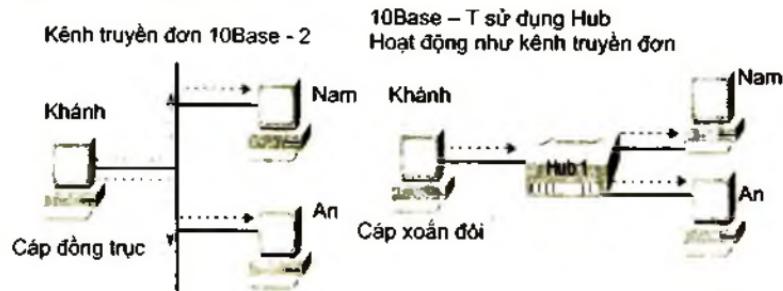
Bảng 1.2. Các trường trong khung Ethernet

Trường	Chiều dài (byte)	Mô tả
Preamble	7	Đồng bộ dữ liệu
Start Frame Delimiter (SFD)	1	Báo hiệu byte kế tiếp bắt đầu với trường MAC đích
Destination MAC address	6	Địa chỉ MAC đích của gói tin
Source MAC Address	6	Địa chỉ MAC nguồn
Length	2	Chiều dài phần dữ liệu của frame (hoặc là chiều dài, hay kiểu được thể hiện, nhưng không cả hai)
Type	2	Xác định loại giao thức được liệt kê bên trong frame
Data and Pad	46-1500	Chứa dữ liệu từ lớp trên, thường là PDU lớp 3 (IP, IPX)
Frame Check Sequence (FCS)	4	Cung cấp phương thức để đầu thu xác định liệu frame nhận được có lỗi

1.2. KHÁI NIỆM VỀ CHUYỂN MẠCH LAN

1.2.1. Giới thiệu các thiết bị LAN

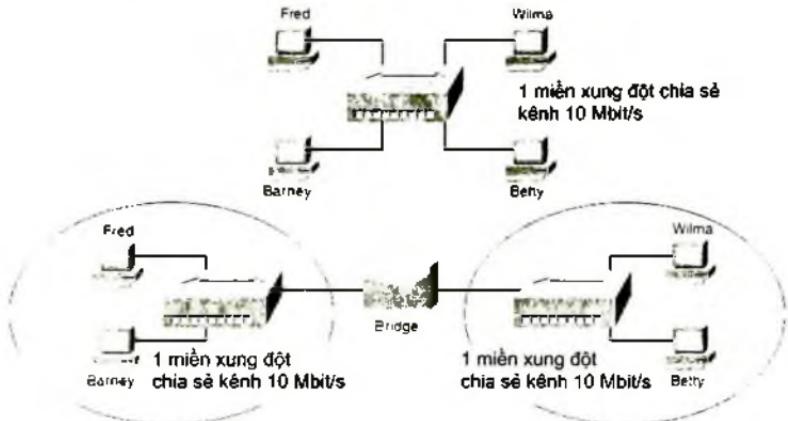
Như đã giới thiệu phần trước, mạng LAN Ethernet bắt đầu với các chuẩn sử dụng cáp điện đồng trục 10Base2. Sau đó là chuẩn 10BaseT, cung cấp khả năng sẵn sàng cao hơn, vì lỗi trên một cáp đơn không ảnh hưởng đến phần còn lại của toàn mạng LAN. 10BaseT cho phép sử dụng cáp xoắn đôi với giá thành rẻ hơn nhiều so với cáp đồng trục. Hình 1.17 mô tả hai loại mạng trên.



Hình 1.17. Mạng 10 BaseC và 10BaseT

Việc sử dụng các thiết bị hub với Ethernet 10Base-T cài tiến nhiều so với 10Base2/5 nhưng cũng có những mặt trái như sau:

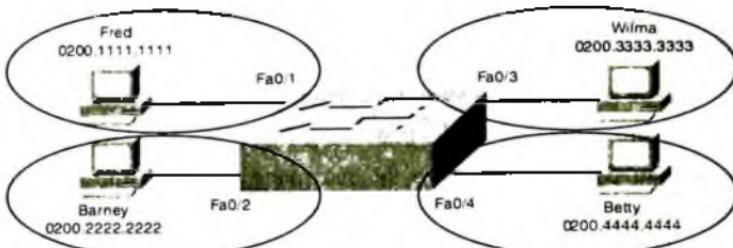
- Hub tạo nên một **miền xung đột** cho tất cả thiết bị trong LAN.
- Băng thông chia sẻ cho toàn mạng chỉ là 10Mbit/s
- Sau đó khả năng thực thi của mạng Ethernet được cải tiến, Ethernet bridge được tạo ra để giải quyết với vấn đề xung đột và tăng băng thông cho mạng.



Hình 1.18. Mạng Ethernet sử dụng hub và bridge

Như hình 1.18 cho thấy, Ethernet Bridge giúp phân mạng LAN thành các miền xung đột khác nhau, với băng thông tống cộng cho LAN lúc này sẽ là tổng băng thông cho hai LAN có kết nối.

Các thiết bị LAN switch được tạo ra với chức năng cốt lõi cơ bản tương tự như là bridge, nhưng với nhiều chức năng có cải tiến. Giống như bridge, switch phân một LAN thành nhiều miền xung đột. Switch còn có nhiều giao tiếp hơn so với bridge, tối ưu hóa phần cứng, cho phép các switch Ethernet nhỏ có thể chuyển hàng triệu Ethernet frame qua mạng đồng thời. Và với khả năng truyền thông song công, băng thông của LAN sử dụng switch được cải tiến rất nhiều so với các loại thiết bị trước đây.



Hình 1.19. Miền xung đột trên switch

Như hình 1.19, có thể thấy switch phân mỗi port của nó thành một miền quang bá, với mỗi miền quang bá đều có khả năng hoạt động song song.

1.2.1.1. Cơ chế chuyển mạch

Vai trò của LAN switch là chuyển tiếp các frame Ethernet. Để đạt được mục tiêu này, switch sử dụng địa chỉ MAC nguồn và đích trong tiêu đề của mỗi frame Ethernet. Công việc chính của switch là nhận và thực hiện quyết định: hoặc là chuyển tiếp frame ra ngoài các port khác, hay là hủy bỏ frame đó đi. Để hoàn thành nhiệm vụ chính này, switch hoặc bridge thực hiện các hành động sau:

- Quyết định khi nào thì chuyển tiếp hay lọc (không chuyển tiếp) một frame, dựa trên địa chỉ MAC đích
- Học địa chỉ MAC bằng cách kiểm tra địa chỉ MAC nguồn của mỗi frame nhận được bởi bridge/switch
- Tạo môi trường không lặp với các bridge khác, sử dụng giao thức cây bao phủ - Spanning Tree Protocol STP.

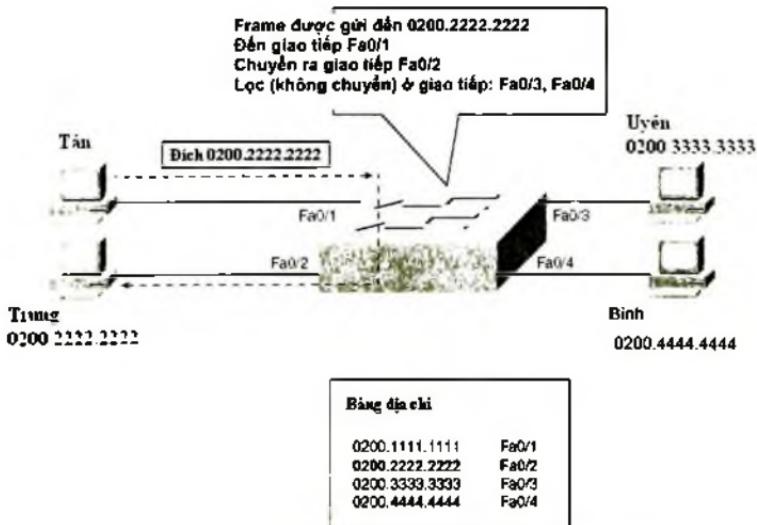
Nhiệm vụ đầu tiên của switch là chuyển tiếp và lọc gói tin, hai nhiệm vụ kia là bổ sung cho nhiệm vụ đầu tiên. Phản sau sẽ kiểm tra mỗi nhiệm vụ này.

1.2.1.2. Quyết định lọc/ chuyển tiếp frame

Để quyết định liệu chuyển tiếp một frame, switch sử dụng một bảng được xây dựng một cách tự động liệt kê các địa chỉ MAC và các giao tiếp đầu ra tương ứng. Switch so sánh địa chỉ MAC đích của frame với bảng này để quyết định liệu có chuyển tiếp các frame hay đơn giản là bỏ qua nó.

Hình 1.20 cho thấy một ví dụ cả hai quyết định chuyển và lọc. Tân gửi một frame với địa chỉ đích 0200.2222.2222 (địa chỉ MAC của Trung). Switch so sánh địa chỉ MAC đích (0200.2222.2222) với bảng địa chỉ MAC, tìm kiếm mục trùng khớp. Đây là giao tiếp ra với một frame sẽ được gửi để chuyển nó đến địa chỉ MAC đã liệt kê (0200.2222.2222). Bởi vì giao tiếp trên đó frame đến là khác với giao tiếp được ra ngoài được liệt kê (Fa0/2), switch quyết định chuyển frame ra ngoài giao tiếp Fa0/2, như thể hiện trong bảng của hình vẽ.

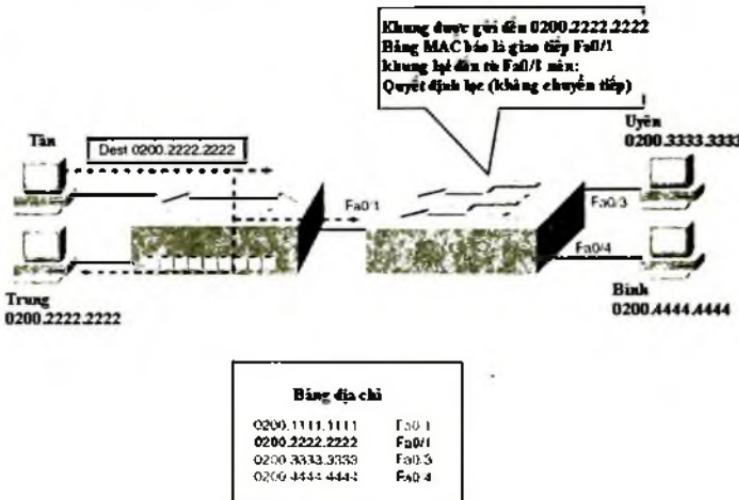
Điều quan trọng để biết liệu một switch sẽ chuyển một frame là kiểm tra và hiểu bảng địa chỉ. Bảng này liệt kê các địa chỉ MAC và giao tiếp sẽ sử dụng khi chuyển các gói tin được gửi đến địa chỉ MAC đó. Hãy ví dụ, bảng này liệt kê 0200.3333.3333 của Fa0/3, đây là giao tiếp ra mà switch sẽ chuyển frame được gửi đến địa chỉ MAC của Uyên (0200.3333.3333).



Hình 1.20. Quyết định chuyển và lọc đơn giản của switch

Hình 1.21 cho thấy một bối cảnh khác, với switch này thực hiện quyết định lọc gói. Trong trường hợp này, các địa chỉ MAC của Tân và

Trung tắt giao tiếp đơn Fa0/1, bởi vì switch sẽ chuyển các frame đến cả hai Tân và Trung ra ngoài giao tiếp FA0/1. Vì thế khi switch nhận một frame được gửi bởi Tân (địa chỉ MAC nguồn là 0200.1111.1111) đến Trung (địa chỉ MAC đến 0200.2222.2222), switch nghĩ rằng: Bởi đi vào giao tiếp Fa0/1 của tôi, và tôi sẽ gửi nó ra ngoài cùng giao tiếp Fa0/1 này, không gửi nó đi (lọc nó), bởi vì gửi nó đi sẽ không có điểm đến.



Hình 1.21. Ví dụ về quyết định lọc gói của switch

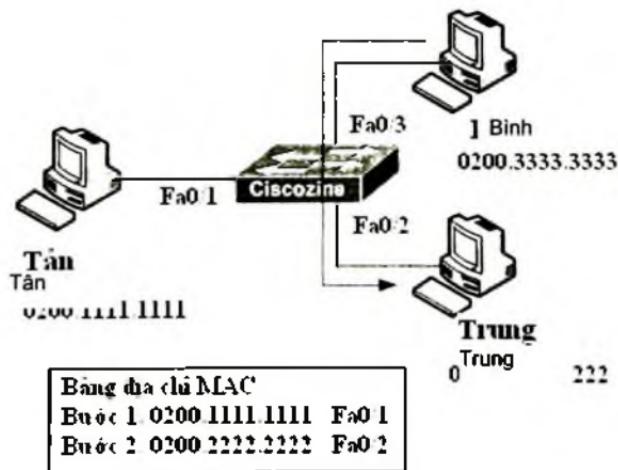
Chú ý rằng hub đơn giản tái tạo lại các tín hiệu điện ra ngoài mỗi giao tiếp, vì thế hub chuyển các tín hiệu điện được gửi bởi Tân đến cả Trung và switch. Switch quyết định lọc (không chuyển) frame, chú ý rằng bảng địa chỉ giao tiếp MAC cho 0200.2222.2222 (Fa0/1) là tương tự như giao tiếp đến.

1.2.1.3. Phương thức các switch học các địa chỉ MAC

Chức năng chính thứ hai của switch là học các địa chỉ MAC và các giao tiếp để đặt nó vào trong bảng địa chỉ giao tiếp của nó. Với một bảng địa chỉ đầy đủ và chính xác, switch có thể tạo chính xác các quyết định chuyển và lọc gói tin.

Các switch xây dựng bảng địa chỉ bằng cách lắng nghe các frame đến và kiểm tra địa chỉ MAC nguồn trên frame này. Nếu một frame đến switch và địa chỉ MAC nguồn không có trong bảng MAC, switch tạo một mục cho bảng này. Địa chỉ MAC được đặt trong bảng, cùng với giao tiếp từ đó frame đến. Switch học địa chỉ luận lý – địa chỉ lớp 3 của các thiết bị theo cách như vậy.

Hình 1.22 mô tả cùng mạng như hình 1.20, nhưng trước khi switch triển khai bắt kí mục nào của bảng địa chỉ. Hình 1.22 cho thấy hai frame được gửi đến đầu tiên trong mạng này – đầu tiên từ Tân, được đánh địa chỉ đến Tân, và sau đó đến đáp ứng của Trung, với địa chỉ đến Tân.



Hình 1.22 Học địa chỉ Ethernet của switch

Như thể hiện trong hình vẽ, sau khi Tân gửi frame đầu tiên của mình đến Trung, switch thêm một bảng ghi cho 0200.1111.1111, địa chỉ MAC của Tân, có liên quan đến giao tiếp Fa0/1. Khi Trung phản hồi tại bước 2, switch thêm một bảng ghi thứ hai, lần này là 0200.2222.2222, địa chỉ MAC của Trung, cùng với giao tiếp Fa0/2, là giao tiếp trong đó mà switch nhận frame này. Việc học luôn luôn xuất hiện bằng cách tìm kiếm địa chỉ MAC trong frame này.

1.2.1.4. Tiến trình Gửi Frame để học các địa chỉ MAC

Bây giờ quay lại tiến trình chuyển các gói tin, sử dụng hình 1.22. xem xét những gì switch sẽ làm với frame đầu tiên của Tân trong hình này, xuất hiện khi không có mục nào trong bảng địa chỉ MAC? Vì nó đi ra ngoài, khi không có giao tiếp đầu ra nào trùng khớp trong bảng địa chỉ MAC, switch chuyển các frame ra ngoài tất cả các giao tiếp (ngoại trừ giao tiếp đến). Các switch chuyển frame unicast không biết này (những frame mà địa chỉ MAC đích đến không có trong bảng địa chỉ MAC) ra ngoài tất cả các giao tiếp khác, với hy vọng rằng thiết bị không biết này sẽ ở trên một phân đoạn Ethernet khác và sẽ đáp ứng, cho phép switch tạo một mục đúng trong bảng địa chỉ.

Lấy ví dụ, trong hình 1.22, switch chuyển frame đầu tiên ra ngoài Fa0/2, Fa0/3, thậm chí dù rằng 0200.2222.2222 (Trung) đang tắt giao tiếp Fa0/2. Switch thực hiện việc chuyển ngược frame trở về Fa0/1, vì switch không bao giờ chuyển một frame ra ngoài cùng giao tiếp mà nó đã đến. Khi Trung phản hồi cho Tân, switch thêm một mục 0200.2222.2222 tương ứng giao tiếp Fa0/2 vào bảng địa chỉ của nó. Sau đó bất kì frame nào được gửi đến địa chỉ đích 0200.2222.2222 sẽ không còn cần thiết để được gửi ra ngoài Fa0/3, mà chỉ được chuyển ra Fa0/2.

Tiến trình chuyển các frame ra ngoài tất cả các giao tiếp, ngoại trừ các giao tiếp trên đó frame đến, được gọi là gửi – Forward. Switch gửi các frame unicast không biết, cũng như các frame broadcast ra tất cả các giao tiếp. Switch cũng gửi các frame multicast LAN ra tất cả các giao tiếp.

Các switch giữ một định thời cho mỗi mục trong bảng địa chỉ MAC, được gọi là bộ định thời chưa kích hoạt. Switch thiết lập bộ định thời *xo้ง 0* cho các mục mới. Mỗi khi switch nhận các frame khác với cùng địa chỉ MAC, bộ định thời được thiết lập lại 0. Bộ định thời đếm tăng lên, vì thế switch có thể báo mục nào đã đi qua thời gian dài nhất kể từ khi nhận một frame từ thiết bị đó. Nếu switch chạy vượt quá gian các mục trong bảng địa chỉ MAC, switch có thể sau đó gỡ bỏ các mục với bộ định chưa kích hoạt cũ nhất.

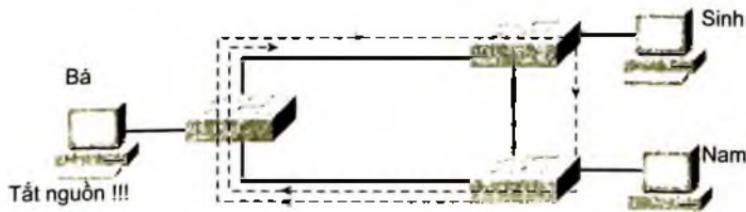
1.2.1.5. Tránh lặp sử dụng giải thuật cây bao trùm – STP (Spanning Tree Protocol)

Chức năng chính thứ ba của LAN switch là ngăn ngừa lặp, khi được triển khai với SPT. Nếu không có SPT, các frame sẽ lặp vô tận trong mạng Ethernet với các liên kết Vật lý dư thừa. Để ngăn ngừa các frame lặp này, STP ngăn một số port không chuyên các frame để chỉ một con đường hoạt động tồn tại giữa bất kỳ cặp phân đoạn LAN nào (các miền xung đột). Kết quả của STP là tốt khi frame không lặp vô hạn, làm cho mạng LAN có thể sử dụng được. Tuy nhiên, dù rằng mạng có thể sử dụng một số liên kết dư thừa trong trường hợp có lỗi, LAN không cân bằng tải lưu lượng.

Để tránh lặp lớp 2, tất cả các switch phải sử dụng STP. STP làm cho mỗi giao tiếp trên một switch thiết lập vào hoặc là trạng thái khóa, hay là trạng thái chuyên tiếp. Khóa có nghĩa rằng giao tiếp không thể chuyên tiếp hay nhận các frame dữ liệu. Chuyên tiếp có nghĩa là giao tiếp có thể gửi và nhận các frame dữ liệu. Nếu một tập hợp con đúng của các giao tiếp bị khóa, tồn tại một con đường luận lý hoạt động giữa các LAN nhằm tránh lặp.

Một ví dụ đơn giản cho thấy nhu cầu cho STP rõ ràng hơn. Nhớ rằng, switch đây các frame được gửi đến với cả hai loại địa chỉ unicast MAC không biết và địa chỉ broadcast.

Hình 1.23 cho thấy một frame đơn, được gửi bởi Nam đến Bá, lặp mãi mãi bởi vì mạng đã dư thừa nhưng không có STP



Hình 1.23. Vòng lặp mạng LAN

Nam gửi một frame unicast đến cho địa chỉ MAC của Bá, nhưng máy của Bá bị tắt, vì thế không có switch nào học được địa chỉ MAC của Bá.

Địa chỉ MAC của Bá sẽ là địa chỉ MAC không biết tại thời điểm này. Chính thế, các frame hướng đến địa chỉ MAC của Bá sẽ không được chuyển bởi mỗi switch ra ngoài mỗi port. Những frame này lặp vô hạn. Bởi vì những switch này không bao giờ biết về địa chỉ MAC của Bá (nguyên nhân vì anh đã tắt máy và không thể gửi các frame đến hoặc đi), chúng tiếp tục chuyển các frame ra ngoài tất cả các port, và bản sao của các frame này lặp vô hạn.

Tương tự, các switch cũng gửi các gói tin quảng bá này, vì thế nếu bắt kì PC nào gửi một broadcast, broadcast sẽ cũng lặp vô hạn.

Một cách để giải quyết vấn đề này là xây dựng một LAN không có các liên kết dự phòng. Tuy nhiên, hầu hết kí sự mạng thiết kế LAN có chủ đích sử dụng các đường liên kết Vật lý dư thừa giữa các switch. Mục đích chính của vấn đề này là tăng khả năng chống lỗi trong trường hợp một liên kết bị lỗi. Giải pháp tốt nhất là sử dụng LAN chuyển mạch với các liên kết dư thừa, trong khi sử dụng STP để khóa động một số giao tiếp để chỉ duy nhất một con đường tồn tại giữa hai điểm cuối tại bất kì thời điểm nào.

1.2.2. Xử lý bên trong các switch Cisco

Trong chương này đã đề cập làm thế nào các switch quyết định liệu chuyển hay lọc một frame. Ngay khi switch Cisco quyết định chuyển một frame, switch có thể sử dụng một hay nhiều loại khác nhau của tiến trình xử lý nội tại. Hầu hết tất cả các switch được phát hành gần đây sử dụng cơ chế xử lý store – and – forward (lưu trữ và chuyển tiếp), nhưng tất cả những loại này xử lý nội tại này được hỗ trợ ít nhất một loại của các switch Cisco có sẵn.

Một số switch, và các bridge trong suốt nói chung, sử dụng tiến trình xử lý store – and – forward. Với store – and – forward, switch phải nhận toàn bộ frame trước khi chuyển bit đầu tiên của frame này. Tuy nhiên Cisco cũng cung cấp hai phương thức xử lý nội bộ khác cho switch: cut – through và fragment – free. Bởi vì địa chỉ MAC xuất hiện sớm trong tiêu đề Ethernet, một switch có thể thực hiện quyết định chuyển gói tin trước khi switch này nhận tất cả các bit của frame đó. Phương thức cut – through và fragment – free cho phép bắt đầu chuyển frame trước khi toàn bộ frame được nhận, giảm thời gian yêu cầu để gửi frame đó (độ trễ, độ trì hoãn).

Với tiến trình xử lý cut – through, switch bắt đầu gửi các frame ra ngoài port ngay khi có thẻ. Dù điều này có thể làm giảm độ trễ, nó cũng tạo ra lỗi. Bởi vì trường kiểm FCS frame này nằm trong hậu đè Ethernet, switch không thể quyết định liệu frame có lỗi gì không trước khi bắt đầu chuyển frame này. Vì thế switch rút ngắn độ trễ frame, nhưng với cái giá của việc được chuyển đi, một số frame có thể bị lỗi.

Fragment – free làm việc tương tự như là cut – through, nhưng nó cố gắng rút số lượng frame lỗi mà nó chuyển. Một sự thật thú vị về Ethernet rằng phương thức CSMA/CD có thể phát hiện lỗi với 64 byte đầu tiên của frame đó. Tiến trình fragment – free làm việc như là cut – through, nhưng nó đợi đê nhận 64 byte đầu tiên trước khi chuyển một frame. Frame ít bị trì hoãn hơn so với store – and – forward và trễ hơn một tí so với cut – through, nhưng frame mà bị lỗi do xung đột không được chuyển đi.

Với nhiều liên kết đến máy tính chạy tốc độ 100Mbit/s, hoặc lên đến 1Gbit/s và các mạch tích hợp đặc trưng cho ứng dụng tốc độ cao hơn, ngày nay các switch thông thường sử dụng tiến trình store and forward, bởi vì độ trễ được cải tiến của hai phương thức chuyển mạch khác là có thể thỏa thuận ở những tốc độ này.

Các thuật ngữ tiến trình xử lý nội tại được sử dụng bởi các switch khác nhau về loại và nhà sản xuất; tùy theo; tiến trình xử lý này có thể được sắp xếp thành một trong các phương thức liệt kê trong bảng 1.3.

Bảng 1.3. Các phương thức chuyển mạch

Phương thức chuyển mạch	Mô tả
Store – and – forward	Switch nhận đầy đủ tất cả các bit trong frame trước khi chuyển tiếp frame đó. Điều này cho phép switch thực hiện kiểm tra FCS trước khi chuyển tiếp frame.
Cut – through	Switch chuyển tiếp các frame ngay khi có thẻ. Điều này rút ngắn thời gian trì hoãn nhưng không cho phép switch kiểm tra lỗi FCS.
Fragment – free	Switch chuyển tiếp frame sau khi nhận 64 byte đầu tiên của frame đó, tránh chuyển tiếp các frame bị lỗi xung đột

1.3. KIẾN THỨC VỀ THIẾT KẾ LAN

Như vậy, giáo trình đã trình bày những kiến thức cơ bản về hoạt động của hệ thống LAN. Nội dung bao gồm cách thức switch chuyển tiếp các frame, cách sử dụng cáp UTP và cách đấu nối, giải thuật CSMA/CD để giải quyết vấn đề xung đột bên trong hệ thống mạng cũng như những khác biệt trong hoạt động và sử dụng hub/switch.

Phần này cung cấp một cái nhìn rộng hơn về LAN: cụ thể, làm thế nào thiết kế hệ thống với LAN lớn hơn. Khi xây dựng một LAN nhỏ, có thể mua một switch, cắm cáp để kết nối một vài thiết bị và hoàn tất. Tuy nhiên, khi xây dựng một mạng LAN từ nhỏ đến lớn, có nhiều sản phẩm hơn để lựa chọn, như là khi nào sử dụng hub, switch và router. Ngoài ra, phải đánh giá lựa chọn loại switch LAN nào (switch khác nhau về kích thước, số port, độ thực thi, chức năng và giá cả). Loại môi trường LAN cũng khác nhau. Ngoài ra, phải đánh giá lợi ích của việc nối cáp UTP, như là chi phí và dễ cài đặt, với cáp quang, hỗ trợ khoảng cách xa hơn và bảo mật tốt hơn. Phần này đánh giá nhiều chủ đề khác nhau có liên quan đến thiết kế LAN theo một số cách. Cụ thể, phần này sẽ bắt đầu trình bày ảnh hưởng của việc lựa chọn hub, switch, và router để kết nối các thành phần của LAN. Sau đó, một số thuật ngữ thiết kế Cisco được xem xét. Kết thúc phần này là bảng tóm lược vấn tắt một số loại Ethernet và cáp thông dụng và hướng dẫn chiêu dài cáp cho mỗi loại.

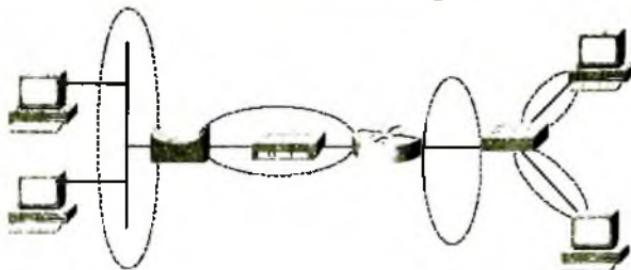
1.3.1. Miền xung đột và miền quảng bá

Khi tạo bất kỳ LAN Ethernet nào, một số loại thiết bị mạng – thông thường là switch, ngày nay là một số router, và có thể là một số hub được sử dụng tùy thuộc vào từng yêu cầu. Những khác biệt này có ảnh hưởng đến quyết định của kỹ sư mạng khi chọn làm thế nào để thiết kế một LAN.

Thuật ngữ miền xung đột và miền quảng bá định nghĩa hai ảnh hưởng quan trọng tiền trinh xử lý việc phân đoạn LAN sử dụng các thiết bị khác nhau. Phần này đánh giá các khái niệm bên dưới các thiết kế LAN Ethernet. Mục tiêu là xác định những thuật ngữ này và để giải thích cách hub, switch và router ảnh hưởng đến miền xung đột và miền quảng bá.

1.3.1.1. Miền xung đột

Nhu đã đề cập trước đây, một miền xung đột là một tập hợp các giao tiếp LAN có các frame có thể xung đột với nhau nhưng không với các frame được gửi bởi bất kì thiết bị nào khác trong mạng. Để xem lại khái niệm cốt lõi này, hình 1.24 mô tả các miền xung đột.



Hình 1.24. Miền xung đột

Chú ý: Thiết kế LAN trong hình 1.24 không phải là một thiết kế thông thường ngày nay. Thay vào đó, nó đơn giản để cung cấp đủ thông tin so sánh với hub, switch và router.

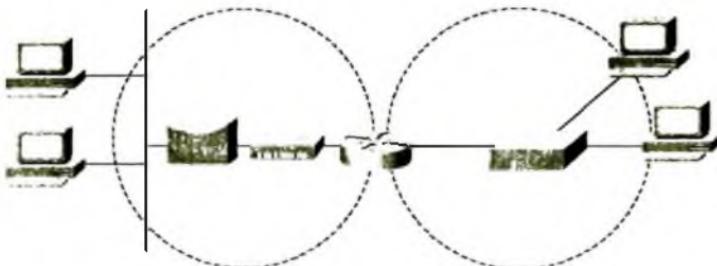
Mỗi phân đoạn riêng biệt, hay miền xung đột, được thể hiện với một vòng tròn gạch dứt trong hình. Switch bên phải tách rời LAN thành hai miền xung đột khác nhau trên mỗi port. Tương tự như vậy, cả hai bridge và router cũng tách mạng LAN thành hai miền xung đột khác nhau. Với tất cả thiết bị trong hình, chỉ hub ở gần trung tâm của mạng không tạo nhiều miền xung đột cho mỗi giao tiếp. Nó lặp lại tất cả các frame ra ngoài tất cả các port mà không có bất kì biện pháp lưu ý và đợi để gửi một frame đến một phân đoạn mạng bận.

1.3.1.2. Miền quảng bá

Thuật ngữ miền quảng bá liên quan đến nơi mà các gói tin quảng bá có thể được chuyển đến. Một miền quảng bá bao gồm một tập hợp các thiết bị mà khi một thiết bị gửi một gói tin quảng bá, tất cả các thiết bị khác nhận được một bản sao của gói tin quảng bá đó. Lấy ví dụ, switch gửi tất cả gói tin broadcast và gói tin multicast ra ngoài tất cả các port. Bởi vì các frame broadcast được gửi ra ngoài tất cả các port, một switch tạo một miền quảng bá đơn.

Ngược lại, chỉ router dùng luồng broadcast này. Hình 1.25 cung cấp các miền quảng bá cho cùng mạng được mô tả trong hình 1.24.

Gói tin quảng bá được gửi bởi một thiết bị trong một miền quảng bá không được chuyển đến các thiết bị trong một miền quảng bá khác. Trong ví dụ này, có hai miền quảng bá. Lấy ví dụ, router không chuyển một broadcast LAN được gửi bởi một PC bên phân đoạn trái của mạng sang phân đoạn phải của mạng này. Trước đây, thuật ngữ broadcast firewall mô tả sự thật rằng router không chuyển các broadcast LAN.



Hình 1.25. Miền quảng bá

Định nghĩa chung cho một miền xung đột và một miền quảng bá như sau:

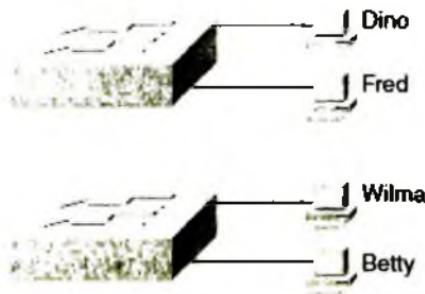
- Một miền xung đột là một tập hợp các card giao tiếp mạng NIC trong đó một frame được gửi bởi một NIC có thể dẫn đến xung đột với một frame được gửi bởi một NIC khác trong cùng miền xung đột đó.
- Một miền quảng bá là một tập hợp các NIC trong đó một frame quảng bá được gửi bởi một NIC được nhận bởi tất cả các NIC khác trong cùng miền quảng bá đó.

1.3.2. LAN ảo (VLAN)

Hầu hết các mạng doanh nghiệp ngày nay sử dụng khái niệm LAN ảo (VLAN). Trước khi tìm hiểu VLANs, cần tìm hiểu định nghĩa của một LAN. Dù rằng có thể hiểu và định nghĩa thuật ngữ LAN từ nhiều bối cảnh khác nhau, một bối cảnh cụ thể trong đó sẽ giúp hiểu về VLAN là:

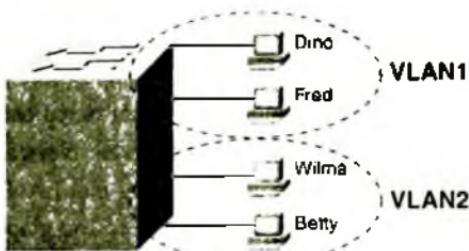
- Một LAN thực chất bao gồm tất cả các thiết bị trong cùng một miền quảng bá.
- Nếu không có VLAN, một switch xem tất cả các giao tiếp trên switch đó thuộc về cùng miền quảng bá. Nói cách khác, tất cả các thiết bị được kết nối đến trên cùng một LAN. (Cisco switch thực hiện điều này bằng cách đặt tất cả các giao tiếp vào trong VLAN 1 theo mặc định) Với VLANs, một switch có thể đặt một số giao tiếp vào một miền quảng bá và một số giao tiếp khác vào VLANs khác dựa trên một số cấu hình đơn giản. Một cách cần thiết, switch tạo nhiều miền quảng bá bằng cách đặt một số giao tiếp vào trong một VLAN và một số giao tiếp khác vào trong các VLAN khác. Những miền quảng bá độc lập này được tạo bởi switch và được gọi là các mạng LAN ảo.

Hình 1.26 so sánh hai LAN nhằm mục đích giải thích một chi tiết về VLAN. Trước tiên, trước khi VLAN tồn tại, nếu một thiết kế xác định hai miền quảng bá riêng biệt, hai switch sẽ được sử dụng – một cho mỗi miền quảng bá, như trong hình này.



Hình 1.26. Hai switch tương ứng cho hai miền quảng bá

Cách khác, có thể tạo nhiều miền quảng bá sử dụng một switch đơn. Hình 1.27 cho thấy hai miền quảng bá giống nhau như hình 1.26, bây giờ được triển khai như là hai VLAN khác nhau trên một switch.



Hình 1.27. Một switch được cấu hình thành 2 VLAN tương ứng hai miền quảng bá

Trong các mạng nhỏ như là mạng trong hình 1.26, có thể không thực sự cần sử dụng VLAN. Tuy nhiên, có nhiều nguyên nhân để sử dụng VLANs, cụ thể:

- Để tạo các thiết kế linh động hơn mà các nhóm người dùng theo phòng ban, hay theo nhóm người dùng làm việc cùng nhau, thay vì vị trí Vật lý của các thiết bị.
- Để phân đoạn các thiết bị thành các LAN nhỏ hơn (broadcast domain) nhằm giảm thiểu độ trễ gây ra bởi mỗi thiết bị trên LAN đó.
- Để bảo mật hơn bằng cách đặt các thiết bị mà làm việc với dữ liệu nhạy cảm trên một VLAN tách biệt.
- Để tách biệt giữa lưu lượng sử dụng điện thoại IP và lưu lượng dữ liệu được gửi từ PC có kết nối đến điện thoại IP đó.

1.4. THUẬT NGỮ THIẾT KẾ MẠNG LAN

Thuật ngữ campus LAN để cập đến LAN được tạo ra để hỗ trợ cho các tòa nhà lớn hơn, hay nhiều tòa nhà. Lấy ví dụ, một công ty có thể đặt các văn phòng trong nhiều tòa nhà trong cùng một khu làm việc. Khi sử dụng có thể xây dựng một campus LAN bao gồm các switch trong mỗi tòa nhà, thêm vào các liên kết Ethernet giữa các switch trong tòa nhà đó, để tạo một campus LAN lớn hơn.

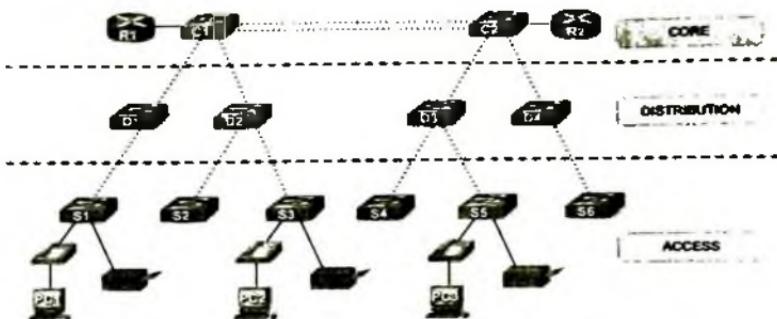
Khi lập kế hoạch và thiết kế một campus LAN, người thiết kế phải xem xét các loại Ethernet có sẵn và chiều dài nối cáp được hỗ trợ cho mỗi loại này. Người thiết kế cũng cần lựa chọn tốc độ được yêu cầu cho mỗi phân đoạn Ethernet. Ngoài ra, cần phải tính đến một số switch được sử dụng để kết nối thiết bị đầu cuối người dùng trong khi một số thiết bị khác được sử dụng để kết nối các thiết bị này lại với nhau. Cuối cùng hầu hết các dự án yêu cầu rằng người người thiết kế xem xét loại thiết bị đã được cài đặt và liệu sự gia tăng tốc độ trong một số phân đoạn là có đáng tiền để mua thiết bị mới hay không.

Lấy ví dụ, phần lớn các PC đã được cài đặt trong mạng ngày nay có các card mạng NICs 10/100/1000 Mbit/s. Giả sử việc nối cáp tương ứng đã được cài đặt, 1 NIC 10/100/1000 có thể sử dụng theo phương thức tự thỏa thuận để sử dụng hoặc là 10Base – T (10Mbit/s), 100 Base – TX (100Mbit/s), hay 1000(Mbit/s) Ethernet. Tuy nhiên, khi mua sắm, cần phải quyết định liệu mua switch hỗ trợ các giao tiếp 10/100 hay hỗ trợ 10/100/1000.

Cisco sử dụng ba thuật ngữ để mô tả vai trò của mỗi switch trong một thiết kế campus: access, distribution và core. Vai trò khác nhau chủ yếu trong hai khái niệm chính:

- Liệu thiết bị có kết nối đến thiết bị đầu cuối người dùng hay không
- Liệu thiết bị có chuyển frame giữa các thiết bị khác bằng cách kết nối nhiều switch khác nhau không

Access switch (switch truy cập) kết nối trực tiếp đến người dùng cuối, cung cấp truy cập đến LAN. Trong những tình huống thông thường, truy cập switch thường gửi lưu lượng đến và đi từ các thiết bị đầu cuối người dùng đến các switch chúng được kết nối đến. Tuy nhiên, xét về mặt thiết kế, được sử dụng để chuyển lưu lượng giữa hai switch khác nhau. Thay vào đó, sử dụng các switch distribution (phân phối) để kết nối đến các access switch, và cuối cùng sử dụng các switch core (lõi) để kết nối các thiết bị switch distribution như sơ đồ trong hình 1.28.



Hình 1.28. Sơ đồ thiết kế LAN theo kiến trúc phân cấp

1.5. MỘT SỐ LOẠI SWITCH CỦA CISCO

Trong phần này sẽ đề cập đến một số loại switch được sử dụng thông dụng trên thị trường hiện nay với các tiêu chí:

- Tiêu chí về vai trò của các thiết bị switch. Theo sơ đồ thiết kế LAN thì một switch có thể đóng một trong các vai trò: Switch truy cập (Access), Switch phân phối (Distribution), Switch lõi (Core)
- Tiêu chí về khả năng thực thi của thiết bị switch đáp ứng cho các mạng với quy mô từ nhỏ, đến trung bình và cỡ lớn.

Bảng 1.4. Một số loại switch của Cisco

Kích thước mạng	Lớp	Catalyst Switch	Tính năng
Dùng chung cho cả ba mạng nhỏ, vừa và lớn	Access	2950	<ul style="list-style-type: none"> • < 50 user • 10/100BASE-T • 100BaseFX or 1000BASE-X uplinks
		3550	<ul style="list-style-type: none"> • < 50 users • 10/100BASE-T • 1000BASE-X uplinks
		4000/4500	<ul style="list-style-type: none"> • < 250 users • 10/100/1000BASE-T • 1000BASE-X uplinks
		6500	<ul style="list-style-type: none"> • 250 users • 10/100/1000Base-T • 1000Base-X uplinks

Nhỏ	Distribution /Core	3550-12T (EMI)	<ul style="list-style-type: none"> • 10 10/100/1000BASE-T • 2 1000BASE-X uplinks; • MLS
		3550-12G (EMI)	<ul style="list-style-type: none"> • 10 1000BASE-X • 2 10/100/1000BASE-T uplinks; • MLS
		4006/4500	<ul style="list-style-type: none"> • 30 1000BASE-X • hoặc 240 10/100/1000BASE-T • MLS
		6500	<ul style="list-style-type: none"> • 100 1000BASE-X • khả năng hoạt động cao. • MLS • Tính mở rộng trong tương lai
Vừa	Distribution	4006/4500	<ul style="list-style-type: none"> • 30 1000BASE-X • hoặc 240 10/100/1000BASE-T • MLS
		6500	<ul style="list-style-type: none"> • 100 1000BASE-X • khả năng hoạt động cao. • MLS • Tính mở rộng trong tương lai
		6500	<ul style="list-style-type: none"> • 100 1000BASE-X • khả năng hoạt động cao. • MLS • Tính mở rộng trong tương lai
		6500	<ul style="list-style-type: none"> • 100 1000BASE-X • khả năng hoạt động cao. • MLS • Tính mở rộng trong tương lai
	Core	6500	<ul style="list-style-type: none"> • 100 1000BASE-X • khả năng hoạt động cao. • MLS • Tính mở rộng trong tương lai
		6500	<ul style="list-style-type: none"> • 100 1000BASE-X • khả năng hoạt động cao. • MLS • Tính mở rộng trong tương lai
Lớn	Core	6500	<ul style="list-style-type: none"> • 100 1000BASE-X • khả năng hoạt động cao. • MLS • Tính mở rộng trong tương lai
		6500	<ul style="list-style-type: none"> • 100 1000BASE-X • khả năng hoạt động cao. • MLS • Tính mở rộng trong tương lai

Trong chương 1 đã tập trung khảo sát một số vấn đề cơ bản sau:

1. Môi trường mạng LAN và các chuẩn Ethernet
2. Hoạt động của các thiết bị như bộ lặp, hub, switch trong LAN
3. Cơ chế chuyển mạch của switch
4. Các đặc tính khác của LAN: STP, VLAN
5. Thiết kế LAN và một số thiết bị switch của Cisco

1.6. CÂU HỎI VÀ BÀI TẬP CHƯƠNG 1

Câu 1. Câu nào sau đây đúng khi kết nối một LAN Ethernet hiện đại thông dụng?

- a. Kết nối mỗi thiết bị theo chuỗi dùng cáp đồng trục
- b. Kết nối mỗi thiết bị theo chuỗi sử dụng cáp UTP
- c. Kết nối mỗi thiết bị tập trung tại hub sử dụng cáp UTP
- d. Kết nối mỗi thiết bị tập trung tại switch sử dụng cáp UTP

Câu 2. Khẳng định nào sau đây đúng về cáp 10Base2 Ethernet LAN?

- a. Kết nối mỗi thiết bị sử dụng cáp đồng trục
- b. Kết nối mỗi thiết bị sử dụng cáp UTP
- c. Kết nối mỗi thiết bị tập trung tại hub sử dụng cáp UTP
- d. Kết nối mỗi thiết bị tập trung tại switch sử dụng cáp UTP

Câu 3. Khẳng định nào sau đây là đúng về cáp chéo

- a. Chân 1 và 2 chéo nhau trên đầu cuối cáp
- b. Chân 1 và 2 trên mỗi đầu cuối kết nối với chân 3 và chân 6 trên đầu kia của cáp
- c. Chân 1 và 2 trên một đầu cuối cáp kết nối với chân 3 và chân 4 trên đầu kia của cáp
- d. Cáp có thể dài đến 1000 mét giữa các tòa nhà
- e. Không có câu nào như trên là đúng

Câu 4. Mỗi câu trả lời bên dưới liệt kê hai loại thiết bị được dùng trong mạng 100BASE-TX. Nếu các thiết bị được kết nối với các UTP Ethernet, cặp nào có thể yêu cầu cáp nối thẳng?

- a. PC – router
- b. PC – switch
- c. Hub – switch
- d. Router – hub
- e. Điểm truy cập không dây – wireless access point và switch

Câu 5. Khẳng định nào sau đây đúng về giải thuật CSMA/CD?

- a. Giải thuật không bao giờ cho phép xung đột xảy ra
- b. Xung đột có thể xảy ra, nhưng giải thuật xác định cách máy tính chú ý xung đột và cách khắc phục
- c. Giải thuật làm việc với chỉ hai thiết bị trên cùng Ethernet.
- d. Không có câu trả lời nào đúng

Câu 6. Điều nào sau đây là một miền xung đột?

- a. Tất cả thiết bị kết nối với một hub Ethernet.
- b. Tất cả thiết bị kết nối với một switch Ethernet
- c. Hai máy tính, với một cáp đến port Ethernet router và đầu kia kết nối PC với một cáp chéo
- d. Không có câu trả lời nào đúng

Câu 7. Điều này sau đây mô tả vấn đề về việc sử dụng hub được cài tiến bằng cách sử dụng switch?

- a. Hub tạo một mạch điện đơn đến tất cả các thiết bị có kết nối khác, làm cho các thiết bị chia sẻ băng thông
- b. Hub giới hạn chiều dài cáp tối đa của các cáp riêng lẻ
- c. Hub cho phép xung đột xảy ra khi hai thiết bị kết nối gửi dữ liệu đồng thời
- d. Hub ngăn số port vật lý kết nối tối đa là 8

Câu 8. Điều này sau đây mô tả cho các địa chỉ Ethernet có thể được sử dụng để truyền thông với hơn một thiết bị tại một thời điểm.

- a. Địa chỉ tạo sẵn
- b. Địa chỉ unicast
- c. Địa chỉ broadcast
- d. Địa chỉ multicast

Câu 9. Cả switch và hub đều được tận dụng trong mạng LAN. Điều nào sau đây là đúng tùy theo việc sử dụng hub và switch trong mạng.

- a. Switch mất ít thời gian để xử lý các frame hơn so với hub
- b. Hub có thể lọc các frame
- c. Switch không chuyển tiếp các gói tin quảng bá
- d. Switch tăng số lượng miền xung đột trong mạng
- e. Sử dụng hub có thể tăng số lượng băng thông có sẵn đến các máy tính
- f. Không phương án nào như trên là đúng

Câu 10. Điều nào sau đây là đúng dựa theo việc sử dụng hub và switch?

- a. Hub có thể có các port được cấu hình với VLAN
- b. Sử dụng hub là đáng giá với khả năng băng thông ổn định
- c. Switch không thể chuyển tiếp các gói tin quảng bá
- d. Switch hữu dụng hơn hub trong khi xử lý các frames
- e. Switch tăng số miền xung đột trong mạng

Câu 11. Khi so sánh và làm nổi bật những tương đồng và khác biệt giữa switch và bridge, khẳng định nào sau đây là đúng

- a. Các bridge nhanh hơn switch do chúng có ít port hơn
- b. Một switch là một bridge nhiều port
- c. Bridge và switch học các địa chỉ MAC bằng cách kiểm tra địa chỉ MAC nguồn của mỗi frame đến
- d. Một bridge sẽ chuyển tiếp một gói tin quảng bá nhưng một switch thì không
- e. Bridge và switch làm tăng kích thước của miền xung đột
- f. Không có khẳng định nào như trên là đúng

Câu 12. Điều nào sau đây mô tả các chức năng khác nhau và đại diện cho một router. (Lựa chọn các phương án phù hợp)

- a. Chuyển mạch gói tin
- b. Ngăn xung đột trên một phân đoạn LAN
- c. Lọc gói tin

- d. Làm tăng miền quảng bá
- e. Chuyển tiếp gói tin quảng bá
- f. Truyền thông liên mạng
- g. Không có phương án đúng

Câu 13. LAN cần được mở rộng trong văn phòng công ty, khi nó phát triển nhanh chóng có thể sử dụng thiết bị lớp 1 nào ? (chọn tất cả phương án)

- a. Một switch
- b. Một router
- c. Một card mạng
- d. Một hub
- e. Một bộ lập

Câu 14. Router Cisco làm nhiệm vụ gì trong số các nhiệm vụ sau đây ? (chọn 2 phương án)

- a. Phân đoạn miền quảng bá
- b. Lựa chọn đường đi
- c. Chuyển mạch gói tin
- d. Làm cầu nối giữa các phân đoạn LAN
- e. Bảo mật lớp truy cập
- f. Gán thành viên của VLAN
- g. Tối ưu hóa ứng dụng

Câu 15. Cả bridge và switch được sử dụng trên mạng LAN, khẳng định nào sau đây là đúng tùy theo switch và bridge trên LAN ? (Lựa chọn 3 phương án đúng)

- a. Switch hoạt động dựa trên phần mềm trong khi switch hoạt động trên phần cứng
- b. Switch thường có số port cao hơn bridge
- c. Bridge thường nhanh hơn switch
- d. Bridge xác định miền quảng bá trong khi switch xác định miền xung đột

- e. Cả bridge và switch chuyển tiếp các gói tin quảng bá lớp 2.
- f. Cả switch và bridge thực hiện quyết định chuyển tiếp dựa trên địa chỉ lớp

Câu 16. Khi quyết định sử dụng thiết bị trên mạng, những thuật lợi nào của switch khi so sánh với hub?

- a. Cho phép chuyển tiếp các frame đồng thời
- b. Tăng kích thước của miền quảng bá
- c. Tăng chiều dài tối đa cáp UTP giữa các thiết bị
- d. Lọc các gói tin dựa trên địa chỉ MAC
- e. Giảm số lượng các miền xung đột.

Câu 17. Khẳng định nào sau đây mô tả các phần của tiến trình trong đó cách một switch quyết định chuyển một frame đến đích với một địa chỉ unicast biết trước?

- a. Nó so sánh địa chỉ đích unicast với bảng MAC address
- b. Nó so sánh địa chỉ nguồn unicast với bảng MAC address
- c. Nó chuyển tiếp frame ra tất cả các giao tiếp trên cùng VLAN trừ giao tiếp đến
- d. Nó so sánh địa chỉ IP đích với địa chỉ MAC đích
- e. Nó so sánh giao tiếp đến của frame với mục MAC nguồn trong bảng MAC address

Câu 18. Khẳng định nào sau đây là đúng về quá trình một LAN switch quyết định chuyển tiếp một frame đến một địa chỉ MAC quảng bá?

- a. Nó so sánh địa chỉ đích unicast với bảng MAC address
- b. Nó so sánh địa chỉ nguồn unicast với bảng MAC address
- c. Nó chuyển tiếp frame ra ngoài tất cả các giao tiếp trên cùng VLAN ngoại trừ giao tiếp ra
- d. Nó so sánh địa chỉ IP đích với địa chỉ MAC đích
- e. Nó so sánh giao tiếp đến của frame với các mục MAC nguồn trong bảng MAC

Câu 19. Khẳng định nào sau đây đúng nhất mô tả những gì switch làm với một frame khi đúng đến là một địa chỉ unicast không biết?

- a. Nó chuyển tiếp ra ngoài tất cả các giao tiếp trên cùng VLAN ngoại trừ giao tiếp đến
- b. Nó chuyển tiếp frame ra ngoài một giao tiếp được xác định bằng cách so sánh với bảng địa chỉ MAC
- c. Nó so sánh địa chỉ IP đích với địa chỉ MAC đích
- d. Nó so sánh giao tiếp đầu ra của frame với địa chỉ MAC nguồn trong bảng địa chỉ MAC.

Câu 20. Switch thực hiện so sánh nào sau đây khi quyết định liệu một địa chỉ MAC mới có được thêm vào bảng định tuyến

- a. Nó so sánh địa chỉ đích đến với bảng địa chỉ MAC
- b. Nó so sánh địa chỉ nguồn unicast với bảng địa chỉ MAC
- c. Nó so sánh giá trị VLAN ID với bảng địa chỉ MAC.
- d. Nó so sánh địa chỉ IP đích của bộ đệm ARP với bảng MAC.

Chương 2

VẬN HÀNH THIẾT BỊ TRONG MẠNG LAN

Các switch *LAN* là các thiết bị mạng thông dụng nhất trong các mạng doanh nghiệp ngày nay. Switch cung cấp điểm kết nối tập trung cho các máy tính và thiết bị văn phòng muốn trao đổi dữ liệu với nhau và kết nối với các hệ thống mạng khác lớn hơn bên ngoài như là mạng *Internet*.

Các thiết bị switch *LAN* hiện nay được phân thành hai loại chính là switch có khả năng quản lý và switch không thể quản lý. Khi mua một thiết bị switch, có thể sử dụng nó được ngay mà không cần thiết phải có bất kì cấu hình nào. Switch sử dụng các thiết lập mặc định vì thế tất cả các giao tiếp sẽ làm việc, giả sử rằng đã lựa chọn đúng cáp và đúng thiết bị để kết nối. Tuy nhiên, với một số doanh nghiệp cần có các yêu cầu cấu hình cao hơn cho switch, như là giám sát các giao tiếp trên switch để theo dõi các truy cập không bảo mật đến switch, cấu hình *VLAN*... Cisco có hai dòng sản phẩm switch chính, dòng *Catalyst* gồm nhiều loại switch khác nhau, được sử dụng chủ yếu cho doanh nghiệp, văn phòng... với các chức năng và kích thước khác nhau. Dòng *Linksys* bao gồm các switch được sử dụng chủ yếu trong nhà hay văn phòng nhỏ. Trong nội dung giáo trình này chỉ đề cập đến các dòng switch *Catalyst* (Cụ thể là switch *Catalyst 2960*). Người dùng có thể sử dụng các loại switch khác của Cisco hoặc sử dụng phần mềm mô phỏng *Packet Tracer* với các chức năng tương tự để tiện theo dõi giáo trình.

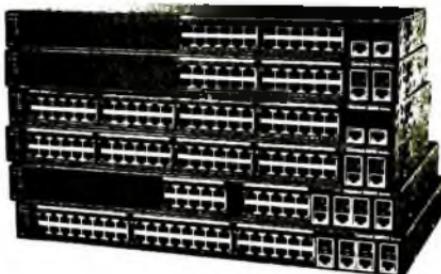
Phần này của giáo trình giải thích chi tiết cách thức truy cập một giao diện người dùng của Cisco, cách sử dụng lệnh để kiểm tra switch nào đang hoạt động, và cách thức cấu hình các switch.

2.1. SWITCH CISCO CATALYST 2960

2.1.1. Giới thiệu

Switch 2960 của Cisco là dòng switch đầy đủ chức năng dành cho doanh nghiệp. Hình 2.1 cho thấy các loại Switch 2960. Các switch này có thể khác nhau đôi chút, ví dụ dòng WS-2960-24TTL có 24 RJ-45 UTP 10/100 port, nghĩa là các port có thể thỏa thuận sử dụng 10BaseT hay 100BaseTX. Dòng SW-2960-24TT-L còn có thêm hai port RJ-45 10/100/1000, thường được sử dụng để kết nối với các switch phía trên.

Cisco xem mỗi đầu nối RJ-45 là một giao tiếp hay một port. Mỗi giao tiếp có một số có dạng x/y, trong đó x và y là hai số khác nhau. Trên 2960, số trước dấu / luôn là 0. Giao tiếp 10/100 đầu tiên của switch 2960 được đánh số bắt đầu với 0/1, thứ hai là 0/2... Giao tiếp này được đặt tên là “interface Fast Ethernet 0/1”. Các giao tiếp gigabit được đặt tên là “Interface Gigabitethernet 0/1”.



Hình 2.1. Thiết bị switch

Các switch Cisco hỗ trợ hai loại hệ điều hành chính:

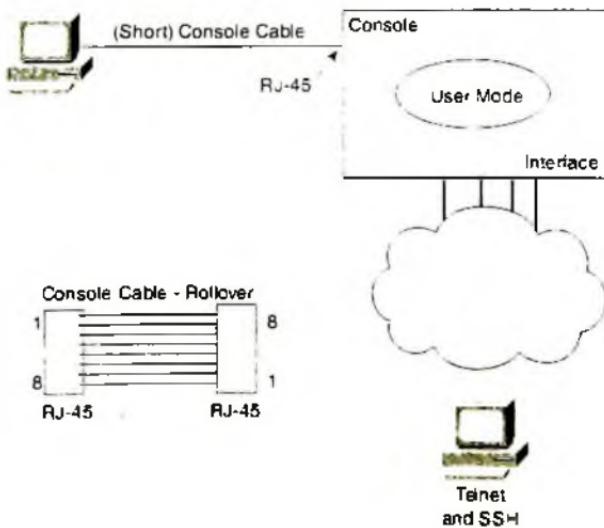
- Hệ điều hành liên mạng - Internetwork Operation System (IOS)
- Hệ điều hành Catalyst - Catalyst Operating System (Cat OS)

Hầu hết các switch Catalyst ngày nay sử dụng Cisco IOS, nhưng một số loại switch cao cấp sử dụng cả hai loại hệ điều hành nói trên. Trong phạm vi giáo trình này chỉ tập trung vào Cisco IOS.

2.1.2. Truy cập giao diện dòng lệnh của Cisco IOS

Phần mềm Cisco IOS cho Catalyst switch triển khai và kiểm soát ý nghĩa và các chức năng được thực hiện bởi một Cisco switch. Bên cạnh việc kiểm soát hoạt động và thuộc tính của switch, Cisco IOS cũng xác định một giao diện cho người dùng được gọi là CLI (Command Line Interface – giao diện dòng lệnh). Phần mềm này cho phép người dùng sử dụng một chương trình mô phỏng đầu cuối, chấp nhận văn bản được nhập từ người dùng. Khi nhấn Enter, bộ mô phỏng gửi văn bản đó cho switch. Switch xử lý văn bản như một lệnh, thực hiện những gì lệnh yêu cầu, và gửi ngược kết quả lại cho người dùng.

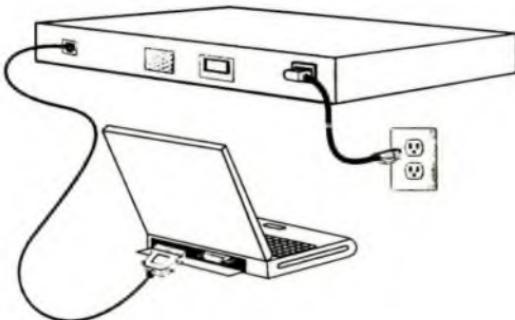
Giao diện này có thể được truy cập qua ba phương pháp thông dụng – console, Telnet và Secure Shell – SSH. Hai trong số các phương pháp này, Telnet và SSH sử dụng mạng IP trong đó switch được đặt để đến switch. Console là port vật lý được xây dựng riêng cho phép truy cập vào CLI.



Hình 2.2. Các phương pháp truy cập switch

2.1.2.1. Truy cập từ Console

Cổng console cho phép truy cập vào Switch CLI thậm chí nếu switch chưa được kết nối vào mạng. Mọi switch Cisco đều có một cổng console, là một cổng RJ-45 vật lý. Một PC kết nối đến cổng console sử dụng cáp UTP rollover, cũng được kết nối đến cổng nối tiếp của PC. Cáp UTP đầu nối RJ-45 trên mỗi phía, với chân 1 trên một phía kết nối đến chân 8 trên phía ngược lại, chân 2 nối với chân 7, chân 3 nối với chân 6, và chân 4 nối với chân 5. Trong một số trường hợp, giao tiếp serial của máy tính không sử dụng port RJ-45, thì một bộ chuyển đổi phải được sử dụng để chuyển từ giao tiếp vật lý của PC – thường hoặc là bộ đầu nối 9 chân hay đầu nối USB sang một cổng RJ-45. Hình sau đây cho thấy đầu cuối RJ-45 của cáp console kết nối đến một switch và đầu cuối DB-9 kết nối đến một laptop.



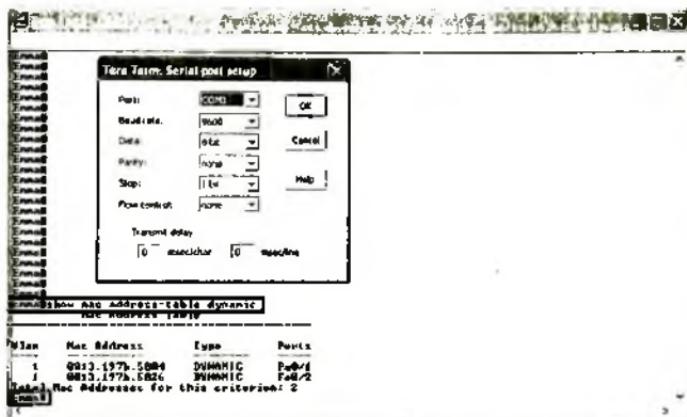
Hình 2.3. Truy cập switch qua console

Khi PC đã kết nối với cổng console, một phần mềm giả lập đầu cuối phải được cài đặt và cấu hình trên PC. Ngày nay, phần mềm giả lập đầu cuối hỗ trợ cho Telnet và SSH, có thể được sử dụng để truy cập switch CLI qua mạng, nhưng không qua console.

Dưới đây là một ví dụ về phần mềm Tera Term được sử dụng để kết nối với switch qua cổng serial. Người dùng có thể sử dụng phần mềm Hyper Terminal thay thế. Cần thiết lập các tham số như sau:

- Tốc độ 9600 bit/ giây
- Không có điều khiển luồng phần cứng

- 8 – bit ASCII
- Không có stop bit
- 1 parity bit



Hình 2.4. Sử dụng Hyper Terminal truy cập switch bằng cổng Console

2.1.2.2. Truy cập CLI với Telnet và SSH

Ứng dụng TCP/IP Telnet cho phép một phần mềm mô phỏng đầu cuối liên lạc với một thiết bị, khá giống những gì xảy ra với một đầu cuối trên PC kết nối với console. Tuy nhiên, Telnet sử dụng một mạng IP để gửi và nhận dữ liệu, hơn là một loại cáp đặc trưng và port vật lý trên thiết bị đó. Giao thức ứng dụng Telnet xem phần mềm mô phỏng đầu cuối là một Telnet Client và thiết bị lắng nghe các lệnh và phản hồi với nó là Telnet server.

Để có thể truy cập được, switch phải có một phần mềm Telnet server đã cài đặt sẵn và phải được cấu hình một địa chỉ IP quản lý cho switch đó. Ngoài ra, mạng giữa PC và switch cần được bật và đang hoạt động để PC và switch có thể trao đổi các gói tin IP.

Việc sử dụng Telnet có thể giúp cho quản trị viên truy cập và cấu hình các switch từ xa thay vì phải đi đến và kết nối vật lý trực tiếp.

Telnet gửi tất cả dữ liệu (bao gồm username và password để đăng nhập vào switch) ở dạng văn bản thô, nên ẩn chứa nguy cơ bảo mật lớn.

SSH cũng thực hiện tương tự như là Telnet, nhưng an toàn hơn bằng cách sử dụng phương pháp mã hóa. Giống như telnet, SSH cũng nhận và truyền dữ liệu sử dụng giao thức TCP qua mạng IP, nhưng SSH truy cập vào port 22 thay vì port 23 như Telnet. SSH server trên switch nhận dữ liệu từ SSH client, xử lý lệnh này và trả kết quả về client. Điểm khác biệt chính giữa Telnet và SSH là thông tin được mã hóa và chính vì thế nó đảm bảo tính riêng tư và ít có nguy cơ hơn.

2.1.2.3. Mã hóa mật khẩu cho truy cập CLI

Mặc định, switch Cisco rất an toàn khi được khóa trong một căn phòng, tương tự, một switch nếu chỉ cho phép truy cập console, không có Telnet hay SSH thì cũng rất an toàn. Tuy nhiên, trong nhiều trường hợp cần cho phép người dùng truy cập thông qua kết nối Telnet/ SSH, thậm chí nếu người khác truy cập trực tiếp qua console cũng không có khả năng thay đổi hoặc xem thông tin cấu hình của switch. Để thực hiện điều này, có thể thiết lập mật khẩu cho các switch, nhằm ngăn ngừa các truy cập trái phép qua console/ Telnet hay SSH như sau:

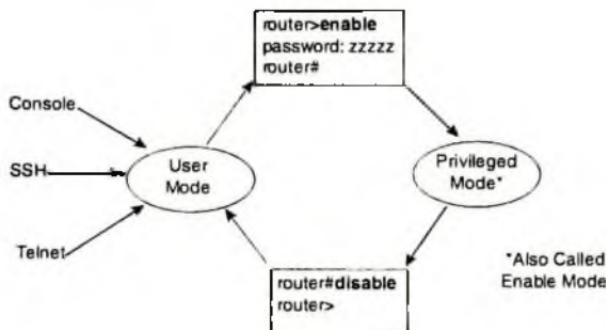
Bảng 2.1. Ví dụ thiết lập mật khẩu cho Switch

Truy cập từ	Loại mật khẩu	Ví dụ câu lệnh
Console	Mật khẩu console	Line console 0 Login Password 2950
Telnet	Mật khẩu vty	Line vty 0 15 Login Password 2960

2.1.2.4. Chế độ người dùng và cấp quyền

Tất cả 3 phương pháp đã xem xét trước đây (console, Telnet và SSH) sẽ cho phép người dùng truy cập vào chế độ “EXEC người dùng”. Chế độ này còn được gọi là chế độ người dùng, cho phép người dùng xem xét thông tin nhưng không ảnh hưởng đến hệ thống.

Cisco IOS hỗ trợ chế độ với nhiều chức năng hơn được gọi là chế độ cấp quyền – enabled mode hay privileged mode.



Hình 2.5. Các chế độ truy cập Cisco IOS

Để chuyển sang chế độ privileged, chỉ đơn giản thực hiện lệnh enable như trên. Để về lại chế độ người dùng, cần dùng lệnh disable.

2.1.2.4.1. Chức năng trợ giúp CLI

Việc nhớ tất cả các câu lệnh của Cisco IOS thường rất khó khăn. Chính vì thế, để trợ giúp người dùng, Cisco giúp cho người sử dụng công cụ nhớ các câu lệnh và tiết kiệm thời gian.

Bảng 2.2. Một số lệnh tóm tắt có trong CLI

Lệnh nhập	Thông tin trợ giúp
?	Trợ giúp tất cả các lệnh có thể trong chế độ này
Help	Mô tả cách có được trợ giúp. Không có lệnh trợ giúp thực sự nào được thực hiện
Command ?	Trợ giúp về các đối số đầu tiên cho lệnh command
Com?	Liệt kê danh sách các lệnh bắt đầu với com
Command param	Nếu nhấn b trong lệnh, CLI dịch phản hồi lại của đối số hay không thực hiện điều gì. Nếu CLI không thực hiện điều gì, nghĩa là có hơn 1 đối số có thể xảy ra.
Command param1 ?	CLI liệt kê tất cả các đối số kế tiếp đối số hiện tại và cho giải thích về mỗi đối số đó.

2.1.2.4.2. Lệnh show và debug

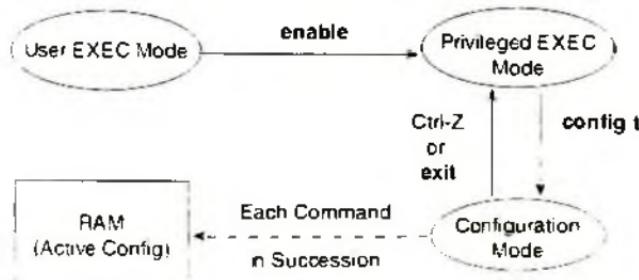
Trong Cisco IOS, lệnh show được sử dụng rất nhiều, cho biết trạng thái của hầu hết mọi chức năng có trong Cisco IOS. Switch phân giải các lệnh show này và thể hiện kết quả cho người dùng.

Một lệnh ít thông dụng hơn là lệnh debug. Giống lệnh show, lệnh debug cũng liệt kê trạng thái của Cisco IOS, tuy nhiên nó không chỉ liệt kê trạng thái hiện tại mà còn yêu cầu switch tiếp tục giám sát các tiến trình khác nhau trong switch. Switch gửi các thông điệp cho người dùng khi có các sự kiện khác nhau xảy ra.

2.1.2.5. Cấu hình phần mềm Cisco IOS

Phần này xem xét tiến trình cấu hình cơ bản, bao gồm khái niệm về file cấu hình và nơi các file cấu hình được lưu trữ. Ngoài ra, sẽ xem xét một số lệnh được sử dụng trong tiến trình cấu hình này.

Chế độ cấu hình là một chế độ khác của Cisco CLI, tương tự như chế độ người dùng và chế độ cấp quyền. Chế độ người dùng cho phép thực hiện các lệnh không ảnh hưởng và thể hiện một số thông tin. Chế độ cấp quyền cho phép các lệnh cao hơn so với chế độ người dùng, bao gồm các lệnh có thể gây hại cho switch. Tuy nhiên, không có lệnh nào trong chế độ người dùng hay cấp quyền thay đổi cấu hình của switch. Chế độ cấu hình cho phép thực hiện các lệnh cấu hình – các lệnh báo cho switch chi tiết những gì phải làm, và cách thực hiện điều đó. Hình 2.6 mô tả chế độ cấu hình và quan hệ với các chế độ trước.



Hình 2.6. Các chế độ cấu hình trong Cisco IOS

Các lệnh nhập vào trong chế độ cấu hình sẽ thay đổi file cấu hình hoạt động của hệ thống. Những thay đổi với cấu hình xảy ra tức thì mỗi khi nhấn phím Enter tại cuối dòng lệnh. Vì thế hãy cẩn thận trước khi nhấn phím Enter tại cuối một lệnh cấu hình.

2.1.2.5.1. Chế độ cấu hình con và các ngữ cảnh

Chế độ cấu hình bản thân nó chưa nhiều chế độ cấu hình con, hay là các ngữ cảnh cấu hình. Các lệnh thiết lập ngữ cảnh cho phép đưa từ một chế độ cấu hình con này sang chế độ cấu hình con khác. Những lệnh thiết lập ngữ cảnh này báo cho switch chủ đề trong đó sẽ vào sau một vài lệnh cấu hình.

Lệnh Interface là một trong các lệnh được sử dụng thường xuyên nhất trong các lệnh cấu hình. Ví dụ, người dùng có thể vào chế độ cấu hình cho giao tiếp Fast Ethernet 0/1 bằng lệnh Interface Fastatethernet 0/1. Lúc đó các trợ giúp trong chế độ cấu hình giao tiếp hiển thị chỉ các lệnh hữu ích khi cấu hình giao tiếp Ethernet. Các lệnh được sử dụng trong trường hợp này được gọi là các lệnh con – hay cụ thể là các lệnh con cho giao tiếp.

Xem xét ví dụ sau đây:

- Chuyển từ chế độ cấp quyền sang chế độ cấu hình sử dụng lệnh `configure terminal`
- Sử dụng lệnh cấu hình thiết bị `name Viethan` để cấu hình tên switch
- Chuyển sang chế độ cấu hình console sử dụng lệnh `line cons 0`
- Thiết lập mật khẩu `mot_diem_tua` cho chế độ console sử dụng lệnh `password mot_diem_tua`
- Chuyển sang chế độ cấu hình giao tiếp sử dụng lệnh `interface` cho giao tiếp `Fa0/0`
- Thiết lập tốc độ 100 Mbit/s cho giao tiếp `Fa0/0` (sử dụng lệnh `speed 100`)
- Chuyển sang chế độ cấu hình bằng lệnh `exit`

```

Switch>en
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#host name Viethan
Viethan(config)#line console 0
Viethan(config-line)#password mot_diem_tua
Viethan(config-line)#interface Fa0/1
Viethan(config-if)#speed 100
Viethan(config-if)#exit
Viethan(config)#

```

Cụm từ bên trong dấu ngoặc của lệnh xác định chế độ cấu hình. Ví dụ lệnh đầu tiên sau khi vào chế độ cấu hình (config), nghĩa là chế độ cấu hình toàn cục. Sau lệnh line console 0, dòng chữ lại là (config-line) nghĩa là chế độ cấu hình dòng. Bảng 2.3 liệt kê các câu lệnh thông dụng nhất trong chế độ cấu hình, tên của những chế độ này và các lệnh thiết lập được sử dụng để vào chế độ cấu hình đó.

Lệnh	Chế độ	Cách để đến chế độ này
Host name(config)#	Cấu hình chung	Lệnh configure terminal
Host name(config-line)#	Cấu hình truy cập qua vty hay console	Line console 0 Line vty 0 15
Host name(config-if)#	Cấu hình giao tiếp	Interface loại_giao tiếp chi_số

Bảng 2.3. Một số lệnh thông dụng trong các chế độ của switch

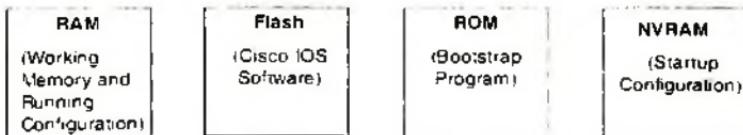
Không có quy tắc nào giúp xác định một lệnh là global (tổng quát) hay subcommands (lệnh con). Thông thường khi nhiều thẻ hiện của một tham số có thể được thiết lập trên một switch đơn, lệnh được sử dụng để thiết lập tham số thường là một lệnh cấu hình con. Các thành phần được thiết lập cho toàn thể switch là các lệnh toàn cục. Ví dụ, lệnh host name là một lệnh cấu hình toàn cục vì chỉ có một tên trên mỗi switch. Ngược lại, lệnh duplex là một lệnh con giao tiếp cho phép switch sử dụng các thiết lập khác nhau trên các giao tiếp khác nhau.

Tổ hợp phím Ctrl-z và lệnh end cho phép thoát khỏi chế độ cấu hình và quay về chế độ cấp quyền. Tương tự, lệnh Exit đưa thoát khỏi chế độ cấu hình con để về chế độ cấu hình trước đó.

2.1.2.5.2. Lưu trữ các file cấu hình switch

Khi cấu hình switch, cần thiết lưu trữ cấu hình hoạt động thiết bị. Cũng cần thiết để duy trì cấu hình trong trường hợp switch mất nguồn. Switch Cisco có RAM để chứa dữ liệu khi Cisco IOS đang sử dụng, nhưng RAM mất thông tin khi switch mất nguồn. Để lưu trữ thông tin có thể được duy trì ngay cả khi mất nguồn, switch Cisco sử dụng nhiều loại bộ nhớ cố định khác nhau, như sau:

- **RAM:** Còn được gọi là DRAM – Dynamic Random Access Memory, RAM được sử dụng trong switch cũng như máy tính: để lưu trữ cấu hình hoạt động. File cấu hình hoạt động được lưu trữ ở đây.
- **ROM:** Read – Only Memory lưu trữ bộ nạp khởi động được nạp lên lần đầu khi switch được bật nguồn. Chương trình này sau đó tìm kiếm Cisco IOS image và quản lý tiến trình nạp Cisco IOS vào RAM, tại thời điểm này, Cisco IOS chiếm quyền điều khiển switch.
- **Bộ nhớ Flash:** hoặc là chip bên trong một switch hay là thẻ nhớ có thể tháo rời được. Bộ nhớ Flash chứa hoàn toàn ảnh Cisco IOS và là nơi lưu trữ mặc định nơi switch lấy Cisco IOS của nó khi khởi động. Bộ nhớ Flash có thể được sử dụng để lưu trữ bất kì file khác, bao gồm các bản sao dự phòng của các file cấu hình.
- **NVRAM:** Nonvolatile RAM lưu trữ file cấu hình khởi động hay ban đầu, được sử dụng khi switch được bật lên lần đầu hay khi switch được tái nạp



Hình 2.7. Các loại bộ nhớ trong thiết bị switch

Cisco IOS lưu trữ tập hợp các lệnh cấu hình trong một file cấu hình. Thực ra, switch sử dụng nhiều file cấu hình – một cho cấu hình khởi tạo được

sử dụng khi được bật, và một cho cấu hình hoạt động, được lưu trữ trong RAM. Bảng 2.4 liệt kê tên của hai file này, mục đích của nó và nơi lưu trữ.

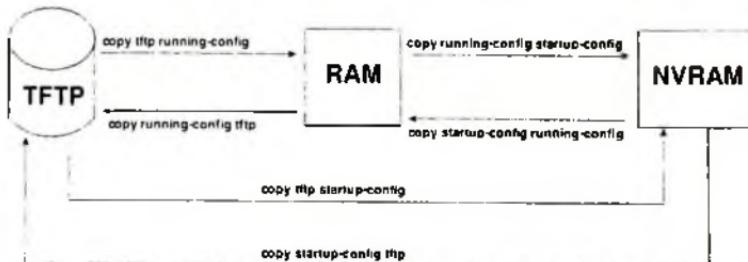
Bảng 2.4. Các tập tin cấu hình

Tập tin cấu hình	Mục đích	Nơi lưu trữ
Startup - config	Lưu trữ cấu hình khởi động được sử dụng khi switch tái nạp IOS	NVRAM
Running - config	Lưu trữ cấu hình hoạt động, nội dung thay đổi khi có lệnh trong chế độ cấu hình	RAM

Khi cập nhật thông tin cấu hình của switch, chỉ cập nhật trong file cấu hình running-config. Tuy nhiên, nếu switch mất nguồn, tắt cả cấu hình có thể mất. Nếu muốn giữ cấu hình này, phải sao chép running-config sang NVRAM, ghi đè lên file cấu hình startup-config cũ.

2.1.2.5.3. Sao chép và xóa các file cấu hình

Để sao chép các tập tin cấu hình, sử dụng lệnh copy, sao chép một file sang file khác trong switch. Thường thì lệnh copy được sử dụng để sao chép giữa RAM, NVRAM trên switch và một TFTP server.



Hình 2.8. Sao lưu tập tin cấu hình

Lệnh được sử dụng để sao chép Cisco IOS được tiến hành như sau:

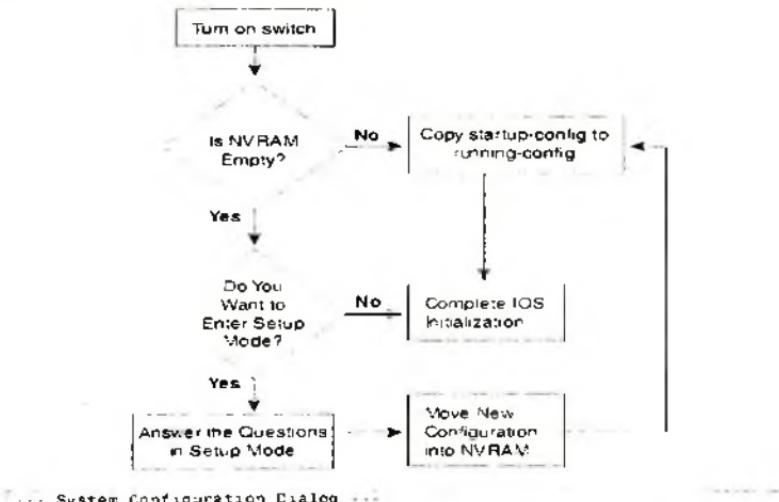
Copy (tftp/running-config/startup-config) (tftp/running-config/ startup-config)

Nội dung trong RAM sẽ mất khi tắt nguồn, trong một số trường hợp cần xóa nội dung trong startup-config của NVRAM. Để thực hiện điều này có thể sử dụng ba lệnh để xóa nội dung của NVRAM: lệnh write

erase, erase startup – config và erase nvram. Tất cả các lệnh này đơn giản xóa nội dung của tập tin startup-config trong NVRAM.

2.1.2.5.4. Cấu hình khởi tạo (Chế độ thiết lập)

Cisco IOS hỗ trợ hai phương pháp chính để tạo cho một switch một cấu hình cơ bản – chế độ cấu hình, đã được xem xét trước đây, và chế độ thiết lập. Chế độ thiết lập cho phép người quản trị viên thiết lập các thông số cấu hình cơ bản bằng cách sử dụng các câu hỏi yêu cầu các thông số cấu hình cơ bản. Vì chế độ cấu hình được yêu cầu cho hầu hết các nhiệm vụ cấu hình, người dùng không sử dụng chế độ thiết lập. Tuy nhiên, những người dùng mới lại thích sử dụng chế độ này hơn, vì nó quen thuộc hơn so với chế độ cấu hình CLI.



... System Configuration Dialog ...

Would you like to enter the initial configuration dialog? [yes no]: yes

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

Basic management setup configures only enough connectivity for management of the system. Extended setup will ask you

to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

Enter host name [Switch]: fred

The enable secret is a password used to protect access to privileged EXEC and configuration modes. This password, after entered, becomes encrypted in the configuration.
Enter enable secret: cisco

The enable password is used when you do not specify an enable secret password, with some older software versions, and some boot images.

Enter enable password: motelscc

The virtual terminal password is used to protect access to the switch over a network interface.

Enter virtual terminal password: wilma

Configure SNMP Network Management? [no]:

Current interface summary

Any interface listed with OK? value NO does not have a valid configuration

Interface	IP-Address	OK? Method	Status	Protocol	
Vlan1	unassigned	NO	unset	up	up
FastEthernet0/1	unassigned	YES	unset	up	up
FastEthernet0/2	unassigned	YES	unset	up	up
FastEthernet0/3	unassigned	YES	unset	up	up

1 lines omitted for brevity

GigabitEthernet0/1	unassigned	YES	unset	down	down
GigabitEthernet0/2	unassigned	YES	unset	down	down

The following configuration command script was created:

```
hostname fred
enable secret 5 $1$NE7S4$ktD3JN14$5Fcc77B217
enable password motelscc
line vty 0 15
password wilma
no snmp-server
```

2.2. CÁU HÌNH SWITCH ETHERNET

Phần này giải thích nhiều vấn đề liên quan đến cấu hình Cisco switch. Một số chủ đề khá quan trọng, như là cấu hình tên người dùng và mật khẩu để truy cập từ xa được bảo mật hơn. Một số chủ đề không quan trọng, nhưng hữu ích, như là gán một thông điệp mô tả cho một giao tiếp

2.2.1. Cấu hình các chức năng thông dụng

2.2.1.1. Bảo mật switch CLI

Để vào chế độ cấp quyền, người dùng phải truy cập vào chế độ người dùng hoặc là từ console hay từ Telnet/SSH, và sử dụng lệnh enable. Với các thiết lập mặc định, một người dùng ở chế độ console không cần phải cung cấp một mật khẩu để truy cập vào chế độ người dùng hay chế độ cấp quyền. Nguyên nhân là bởi vì ai cũng có thể thiết lập lại mật khẩu chưa đầy 5 phút sử dụng tiến trình khôi phục mật khẩu Cisco xuất bản. Vì thế, router và switch mặc định cho phép người dùng sử dụng console truy cập vào chế độ cấp quyền.

Để truy cập vào chế độ cấp quyền từ Telnet hay SSH, switch phải được cấu hình các yêu cầu sau:

- Một địa chỉ IP
- Bảo mật truy cập trên các line vty
- Mật khẩu được kích hoạt

Phần này xem xét cấu hình liên quan đến việc truy cập chế độ cấp quyền trên switch hay router, còn vấn đề chưa được xem xét là cấu hình địa chỉ IP, được xem xét trong phần sau.

2.2.1.1.1. Cấu hình mật khẩu bảo mật đơn giản

Mặc định, switch và router cho phép người dùng sử dụng console truy cập chế độ người dùng sau khi đăng nhập, không cần mật khẩu. Với các thiết lập mặc định, người dùng telnet bị từ chối khi truy cập vào switch, vì mật khẩu vty chưa được thiết lập.

Ví dụ sau đây cho thấy tiến trình cấu hình thiết lập mật khẩu console, mật khẩu vty và kích hoạt mật khẩu, tên cho switch. Ví dụ này cho thấy toàn bộ tiến trình, bao gồm các lệnh, như sau.

```
Switch>en
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#enable secret cisco
Switch(config)#hostname KHMT01
```

```
KHMT01(config)#line console 0
KHMT01(config-line)#password Cisco123
KHMT01(config-line)#login
KHMT01(config-line)#exit
KHMT01(config)#line vty 0 15
KHMT01(config-line)#password Viethan01
KHMT01(config-line)#login
KHMT01(config-line)#exit
KHMT01(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
KHMT01#show running-config
Building configuration...
Current configuration : 1040 bytes
!
version 12.2
no service password-encryption
!
thiết bị name KHMT01
!
enable secret 5 $1$mERr$hx5rVl7rPNoS4wqbXKX7m0
!
!
!
interface Fastatahernet0/1
!
interface Fastatahernet0/2
!
interface Fastatahernet0/3
!
interface Fastatahernet0/4
!
interface Fastatahernet0/5
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Switch(config)#enable secret cisco
Switch(config)#thiết bị name KHMT01
KHMT01(config)#line console 0
KHMT01(config-line)#password Cisco123
KHMT01(config-line)#login
KHMT01(config-line)#exit
KHMT01(config)#line vty 0 15
KHMT01(config-line)#password Viethan01
KHMT01(config-line)#login
KHMT01(config-line)#exit
KHMT01(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
KHMT01#show running-config
Building configuration...
Current configuration : 1040 bytes
!
version 12.2
no service password-encryption
!
thiết bị name KHMT01
!
enable secret 5 $1$mERr$hx5rVt7rPNo$4wqbXKX7m0
!
!
!
!
interface Fastatahernet0/1
!
interface Fastatahernet0/2
!
interface Fastatahernet0/3
!
interface Fastatahernet0/4
!
interface Fastatahernet0/5
!
```

```

interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface Vlan1
  no ip address
  shutdown
!
line con 0
password Cisco123
login
!
line vty 0 4
password Viethan01
login
line vty 5 15
password Viethan01
login
!
!
end

```

Ví dụ này bắt đầu với lệnh `configure terminal` cho phép chuyển người dùng từ chế độ cấp quyền sang chế độ cấu hình. Sau đó thiết lập tên và mật khẩu cho switch sử dụng lệnh `name` và `enable secret`.

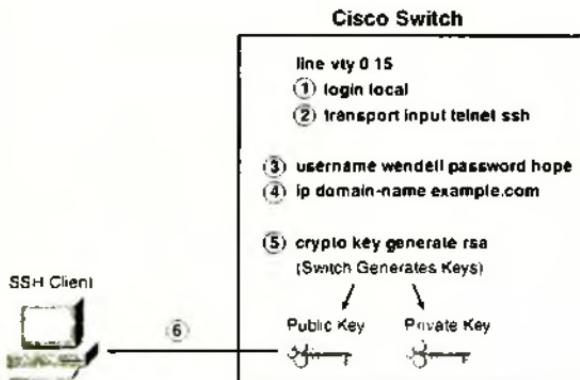
Sau đó, để truy cập vào chế độ console hay chế độ vty, sử dụng các lệnh `line console 0` và `line vty 0 15` tương ứng.

2.2.1.1.2. Cấu hình tài khoản người dùng và SSH

Telnet gửi tất cả dữ liệu, bao gồm mật khẩu được nhập bởi người dùng, ở dạng văn bản thô. Ứng dụng SSH cung cấp cùng chức năng với Telnet, tuy nhiên SSH mã hóa dữ liệu được gửi giữa SSH client và SSH server, nên SSH là phương pháp được ưa thích hơn cho các đăng nhập từ xa đến switch và router.

Để thực hiện, SSH yêu cầu cung cấp nhiều lệnh cấu hình hơn. Ví dụ, SSH yêu cầu người dùng cung cấp cả `username` và `mật khẩu` thay vì chỉ

sử dụng mật khẩu. Vì thế, switch phải được cấu hình lại để sử dụng một trong hai phương thức yêu cầu tài khoản và mật khẩu: một phương thức với tài khoản và mật khẩu được cấu hình trên switch, và phương pháp khác với mật khẩu và tài khoản được cấu hình trên một server bên ngoài được gọi là server Xác thực (Authentication), Xác quyền (Authorization) và Kiểm toán (Accounting), còn gọi là AAA server. Nội dung trong giáo trình này chỉ xem xét đến cấu hình nội bộ sử dụng tài khoản/ mật khẩu. Hình sau đây cho thấy sơ đồ của việc cấu hình và tiến trình được yêu cầu để hỗ trợ SSH.



Hình 2.9. Bảo mật truy cập mạng

Các bước được giải thích như sau:

Bước 1: Thay đổi vty line để sử dụng tài khoản, cục bộ hay trên AAA server. Trong trường hợp này, lệnh con local login xác định sử dụng tài khoản nội bộ, thay thế cho lệnh login trong chế độ cấu hình vty.

Bước 2: Báo với switch chấp nhận cả Telnet và SSH với các lệnh vty con là transport input telnet ssh

Bước 3: Thêm một hay nhiều các giá trị username và password sử dụng các lệnh cấu hình toàn cục tương ứng

Bước 4: Cấu hình một DNS domain name với lệnh cấu hình toàn cục ip domain-name name.

Bước 5: Cấu hình switch để tạo một cặp khóa chung khóa riêng trùng khớp, cũng nhung là một khóa chung chia sẻ, sử dụng lệnh crypto key generate rsa.

Bước 6: sao chép khóa chung của switch cho SSH client trước khi tiến hành kết nối.

```
Emma#  
Emma#configure terminal  
Enter configuration commands, one per line. End with CNTL-Z.  
Emma(config)#line vty 0 15  
! Step 1: a command happens next  
Emma(config) line 1 login local  
! Step 2: a command happens next  
Emma(config) line 1 transport input telnet ssh  
Emma(config) line 1 exec  
! Step 3: a command happens next  
Emma(config) #username wendell password hope  
! Step 4: a command happens next  
Emma(config) ip domain-name example.com  
! Step 5: a command happens next  
Emma(config) #crypto key generate rsa  
The name for the keys will be: Emma.example.com  
Choose the size of the key modulus in the range of 360 to 2048 for your  
General Purpose Keys. Choosing a key modulus greater than 512 may take  
a few minutes.  
  
How many bits in the modulus [512]: 1024  
% Generating 1024 bit RSA keys ...[OK]  
  
00:03:58: SSH 5 ENABLED: SSH 1.99 has been enabled  
Emma(config) ^Z  
: Next, the contents of the public key are listed; the key will be needed by the SSH  
client  
Emma#show crypto key mypubkey rsa  
% Key pair was generated at: 00:03:58 UTC Mar 1 1993  
Key name: Emma.example.com  
Usage: General Purpose Key  
Key is not exportable.  
Key Data:  
20819F30 0006092A B64886F7 0D010101 05000381 80003061 89028181 0005430C  
49C258FA 8E0BEE62 0A6C8688 A00D29CE EAEE6138 456868FD 491A9863 B39A4334  
B6F64E02 1B320256 019J1831 787304A2 720A570A FBB3E75A 94517901 7764C332  
A3A4B2B1 DB4F153E A8477385 5337CE8C B1F5E832 B213E66B 73B77006 8A07820E  
18096609 9A6476D7 C9164ECE 1DCT52B8 955F58D6 F82BFCB2 A273C58C BB020301 00E1  
% Key pair was generated at 00:04:01 UTC Mar 1 '993  
Key name: Emma.example.com.server  
Usage: Encryption Key  
Key is not exportable
```

2.2.1.1.3. Mã hóa mật khẩu

Nhiều lệnh cấu hình được sử dụng để cấu hình mật khẩu. Mật khẩu lưu trữ trong dạng văn bản thô trong file running – config. Các mật khẩu đơn giản được cấu hình trong console và vty line, với lệnh password, được lưu trữ dạng văn bản thô. Để bảo vệ mật khẩu khỏi bị xâm hại trong file cấu hình, hay có thể mã hóa mật khẩu sử dụng lệnh cấu hình service password-encryption.

- Khi lệnh service password – encryption được cấu hình, tất cả các mật khẩu có sẵn được mã hóa.
- Nếu lệnh server password – encryption đã được cấu hình, bất kì thay đổi nào trong tương lai với những mật khẩu này đều được mã hóa.
- Nếu lệnh no service password-encryption được sử dụng sau đó, thì mật khẩu tiếp tục được mã hóa, cho đến khi chúng bị thay đổi.

```
Switch3#show running-config | begin line vty
line vty 0 4
password cisco
login
Switch3#configure terminal
Enter configuration commands, one per line. End with CNTL-Z.
Switch3(config)*#service password-encryption
Switch3(config)*#^Z
Switch3#show running-config | begin line vty
line vty 0 4
password 7 0700285F4C06
login
end
Switch3#configure terminal
Enter configuration commands, one per line. End with CNTL-Z.
Switch3(config)*#no service password-encryption
Switch3(config)*#^Z
Switch3#show running-config | begin line vty
line vty 0 4
password 7 0700285F4C06
login
end
Switch3#configure terminal
Enter configuration commands, one per line. End with CNTL-Z.
Switch3(config-line vty 0 4)
Switch3(config-line)*#password cisco
Switch3(config-line)*#^Z
Switch3#show running-config | begin line vty
line vty 0 4
password cisco
login
```

2.2.1.2. Cấu hình console và vty

2.2.1.2.1. Banners

Router Cisco và switch có thể hiển thị nhiều banner phụ thuộc vào người quản trị. Một banner cho phép hiển thị văn bản xuất hiện trên màn hình người dùng. Có thể cấu hình một router hay một switch để thể hiện nhiều banner, trước và sau khi đăng nhập. Sau đây là một số loại banner thông dụng.

Bảng 2.5. Một số lệnh cấu hình Banner

Banner	Typical Use
Message of the Day (MOTD)	Được thể hiện trước khi login.
Login	Được thể hiện trước khi login nhưng sau thông điệp MOTD
Exec	Được thể hiện sau khi login. Cung cấp các thông tin ẩn với user không được phép

Lệnh banner có thể được dùng để cấu hình tất cả các loại banner này. Trong mỗi trường hợp, loại banner được liệt kê như là tham số đầu tiên, với thiết lập MOTD là thiết lập mặc định. Kí tự không trong đầu tiên sau loại banner được gọi là kí tự giới hạn bắt đầu. Văn bản của banner có thể được cấu hình ngay khi người dùng nhấn Enter tại cuối mỗi dòng. CLI biết rằng banner đã được cấu hình ngay khi người dùng nhập lại cùng kí tự giới hạn.

```

: Below, the three banners are created in configuration mode. Note that any
: delimiter can be used, as long as the character is not part of the message
: text.
Switch#config#banner #
Enter TEXT message. End with the character #.
Switch down for maintenance at 11PM Today #
Switch#config#banner login #
Enter TEXT message. End with the character #.
Unauthorized Access Prohibited!!!!
#
Switch#config#banner exec Z
Enter TEXT message. End with the character Z.
Company picnic at the park on Saturday
Don't tell outsiders!
Z
Switch#config#^Z
: Below, the user of this router quits the console connection, and logs back in
: seeing the MOTD and login banners, then the exec mode prompt, and then the

```

```

! exec banner.
SW1#quit

SW1 con0 is now available

Press RETURN to get started.

Switch down for maintenance at 11PM Today
Unauthorized Access Prohibited!!!!

User Access Verification

Username: fred
Password:
Company picnic at the park on Saturday
don't tell outsiders!
SW1>

```

2.2.1.2.2. Bộ đệm lệnh

Khi nhập các lệnh từ CLI, các lệnh được lưu lại trong bộ đệm. Để thao tác với các bộ đệm này sử dụng các lệnh sau đây:

Bảng 2.6. Một số lệnh trong bộ đệm lệnh

Lệnh	Mô tả
Show history	Liệt kê các lệnh hiện tại được chứa trong bộ nhớ đệm
History size x	Thiết lập kích thước bộ nhớ đệm lệnh cho người dùng khi truy cập từ console hay vty
Terminal history size x	Thiết lập bộ nhớ đệm lệnh trong chế độ EXEC

2.2.2. Cấu hình và vận hành LAN switch

Các thiết bị Cisco switch có thể hoạt động mà không cần thiết phải cấu hình. Các giao tiếp trên switch có thể hoạt động một cách tự động, thiết lập tốc độ và chế độ truyền phù hợp. Tuy nhiên, để thực hiện chức năng quản trị tốt hơn, switch cung cấp cho các cấu hình như sau:

- Cấu hình địa chỉ IP cho switch
- Cấu hình giao tiếp (bao gồm tốc độ và chế độ)
- Cấu hình an ninh công
- Cấu hình VLAN

2.2.2.1. Cấu hình địa chỉ IP cho switch

Để cho phép Telnet hay SSH truy cập switch, hay giao thức quản lý dựa trên IP khác như là SNMP – Simple Network Management Protocol, hay cho phép truy cập các công cụ đồ họa như là Cisco Device Manager CDM, switch cần một địa chỉ IP. Các switch không cần địa chỉ IP để chuyển tiếp các frame Ethernet, mà chỉ để phục vụ chức năng quản lý cho switch đó.

Một switch có địa chỉ IP hoạt động tương tự như là một máy tính với một giao tiếp Ethernet đơn. Switch cần một địa chỉ IP và một mặt nạ phù hợp. Switch cũng cần biết địa chỉ gateway mặc định của nó – nói cách khác, địa chỉ IP trên router gần nhất. Có thể thực hiện điều này thông qua cấu hình địa chỉ IP tĩnh hay sử dụng DHCP để cấp phát IP động.

Các bước cho cấu hình tĩnh địa chỉ IP trên switch như sau:

- **Bước 1:** vào chế độ cấu hình VLAN 1 sử dụng lệnh `interface vlan 1`.
- **Bước 2:** Gán địa chỉ IP và mặt nạ mạng sử dụng lệnh `ip address địa chỉ_IP mặt_nạ_mạng`.
- **Bước 3:** Kích hoạt giao tiếp VLAN 1 sử dụng lệnh `no shutdown`.
- **Bước 4:** Thêm địa chỉ gateway mặc định sử dụng lệnh `ip default-gateway`.

```

Ethernet1#configure terminal
Ethernet1(config)#interface vlan 1
Ethernet1(config-if)#ip address 192.168.1.200 255.255.255.0
Ethernet1(config-if)#no shutdown
00:25:07: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
00:25:08: %LINEPROTO-5-UPDOWN: Line protocol on interface Vlan1, changed
state to up
Ethernet1(config-if)#exit
Ethernet1(config)#ip default-gateway 192.168.1.1

```

Trên Switch có thể có nhiều VLAN khác nhau, nhưng người thường sử dụng VLAN 1 để cấu hình địa chỉ IP cho switch, có thể sử dụng các VLAN khác để cấu hình tương tự. Để xác nhận cấu hình, có thể sử dụng

lại lệnh show running-config để xem thông tin cấu hình và xác nhận đã nhập đúng địa chỉ, маска và gateway mặc định.

Phương pháp thứ hai là sử dụng DHCP cấp phát địa chỉ IP động cho các switch. Sử dụng tương tự các bước như trên, với một số thay đổi bước 2 và bước 4, như sau:

Bước 2: Sử dụng lệnh ip address dhcp, thay vì ip address *địa chỉ_ip* *mặt nạ mạng* như trước.

Bước 4: Không sử dụng lệnh ip default-gateway

```

Enma=configure terminal
Enter configuration commands, one per line. End with CNTL Z.
Enma(config)=interface vlan 1
Enma(config-if)=ip address dhcp
Enma(config-if)=no shutdown
Enma(config-if)=exit
Enma#
00:38:20: HWLINK-3-UPDCON: Interface Vlan1, changed state to up
00:38:21: HWLINKPROTO-5-UPDCON: Line protocol on Interface Vlan1, changed state to up
Enma#
Interface Vlan1 assigned DHCP address 192.168.1.101, mask 255.255.255.0
Enma#show dhcp lease
Tento IP addr: 192.168.1.101 for peer on Interface Vlan1
Tento suo net mask: 255.255.255.0
    DHCP Lease server: 192.168.1.1, state: 3 Bound
    DHCP transaction id: 1966
    Lease: 86400 secs. Renewal: 43200 secs. Recind: 75600 secs
Tento default-gateway addr: 192.168.1.1
    Lease timer fires after: --:59:15
    Retry count: 0 Client-ID: cisco-0019.e86a.6fc0-V11
    Hostname: Enma
Enma#show interface vlan 1
Vlan1 is up. Line protocol is up
    Hardware is EtherS3V1, address is 0019.e86a.6fc0
    Internet address is 192.168.1.101 255.255.255.0
    MTU 1500 bytes, RX 10000000 bytes, TX 10000000 bytes
    Reliability 255/255 txload 1/255 rxload 1/255
    Lines critted for privacy

```

Cuối cùng, để xem địa chỉ IP của switch được cấu hình bằng DHCP, sử dụng lệnh show dhcp lease.

2.2.2.2. Cấu hình các giao tiếp của switch

IOS sử dụng thuật ngữ *giao tiếp* để xem xét các port vật lý được sử dụng để chuyển tiếp dữ liệu đến và đi khỏi một thiết bị. Mỗi giao tiếp có

thì được cấu hình với nhiều tham số khác nhau, mỗi trong số đó có thể khác biệt giữa các giao tiếp.

IOS sử dụng các lệnh con giao tiếp để cấu hình các thiết lập này. Ví dụ, các giao tiếp có thể được cấu hình để hoạt động với các tốc độ và chế độ khác nhau, sử dụng lệnh duplex và speed, hay các giao tiếp có thể thỏa thuận để đạt được tốc độ theo yêu cầu.

```
Emma#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Emma(config)#interface FastEthernet 0/1
Emma(config-if)#duplex full
Emma(config-if)#speed 100
Emma(config-if)#description Server1 connects here
Emma(config-if)#exit
Emma(config)#interface range FastEthernet 0/11 - 28
Emma(config-if-range)#description end-users connect here
Emma(config-if-range)#+Z
Emma#
Emma#show interfaces status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/1	Server1 connects	notconnect	1	full	100	10 100BaseTX
Fa0/2		notconnect	1	auto	auto	10 100BaseTX
Fa0/3		notconnect	1	auto	auto	10 100BaseTX
Fa0/4		connected	1	a-full	a-100	10 100BaseTX
Fa0/5		notconnect	1	auto	auto	10 100BaseTX
Fa0/6		connected	1	a-full	a-100	10 100BaseTX
Fa0/7		notconnect	1	auto	auto	10 100BaseTX
Fa0/8		notconnect	1	auto	auto	10 100BaseTX
Fa0/9		notconnect	1	auto	auto	10 100BaseTX
Fa0/10		notconnect	1	auto	auto	10 100BaseTX
Fa0/11	end-users connect	notconnect	1	auto	auto	10 100BaseTX
Fa0/12	end-users connect	notconnect	1	auto	auto	10 100BaseTX
Fa0/13	end-users connect	notconnect	1	auto	auto	10 100BaseTX
Fa0/14	end-users connect	notconnect	1	auto	auto	10 100BaseTX
Fa0/15	end-users connect	notconnect	1	auto	auto	10 100BaseTX
Fa0/16	end-users connect	notconnect	1	auto	auto	10 100BaseTX
Fa0/17	end-users connect	notconnect	1	auto	auto	10 100BaseTX
Fa0/18	end-users connect	notconnect	1	auto	auto	10 100BaseTX
Fa0/19	end-users connect	notconnect	1	auto	auto	10 100BaseTX
Fa0/20	end-users connect	notconnect	1	auto	auto	10 100BaseTX
Fa0/21		notconnect	1	auto	auto	10 100BaseTX
Fa0/22		notconnect	1	auto	auto	10 100BaseTX
Fa0/23		notconnect	1	auto	auto	10 100BaseTX
Fa0/24		notconnect	1	auto	auto	10 100BaseTX
Gi0/1		notconnect	1	auto	auto	10 100 1000BaseTX
Gi0/2		notconnect	1	auto	auto	10 100 1000BaseTX

2.2.2.3. Cấu hình port security – bảo mật giao tiếp

Nếu muốn giới hạn một giao tiếp trên switch chỉ được kết nối với một thiết bị cụ thể nào đó, có thể sử dụng chức năng port security để giới hạn các thiết bị khác truy cập vào giao tiếp đang sử dụng.

Điều này giúp hạn chế một số lỗ hổng bảo mật khi người khác muốn truy cập trực tiếp vào hệ thống. Khi thiết bị không phù hợp thử gửi dữ liệu qua giao tiếp của switch, switch có thể tạo ra các thông điệp lỗi, hủy bỏ các frame từ thiết bị đó, hay thậm chí ngắt giao tiếp này.

Cấu hình bảo mật giao tiếp bao gồm nhiều bước. Cơ bản là cần chuyển port đó thành một port truy cập, sau đó cần kích hoạt chức năng port security và cấu hình các địa chỉ MAC của các thiết bị được phép sử dụng port đó. Sau đây là các bước cho phép thực hiện, bao gồm các lệnh cấu hình được sử dụng

Bước 1: Chuyển giao tiếp switch sang giao tiếp truy cập sử dụng lệnh con switchport mode access

Bước 2: Kích hoạt bảo mật giao tiếp sử dụng lệnh con switchport port - security

Bước 3: Xác định số địa chỉ MAC tối đa cho phép với giao tiếp sử dụng lệnh switchport port - security số địa chỉ

Bước 4: Xác định hành động thực hiện khi một frame nhận được từ địa chỉ MAC đó khác với địa chỉ đã xác định sử dụng lệnh switchport port - security violation {protect/ restrict/ shutdown}

Bước 5A: Xác định các địa chỉ MAC được cho phép gửi frame vào giao tiếp sử dụng lệnh switchport port-security mac - address địa chỉ mac. Sử dụng nhiều lệnh để xác định nhiều địa chỉ MAC.

Bước 5B: Cách khác, sử dụng phương pháp học tự động địa chỉ MAC bằng lệnh switchport port - security mac - address sticky.

2.3. CÂU HỎI VÀ BÀI TẬP CHƯƠNG 2

Câu 1. Khi thực hiện câu lệnh enable secret, sau đó là enable password, từ console. Sau đó thoát khỏi switch và đăng nhập trở lại vào console. Lệnh nào xác định mật khẩu mà phải nhập vào để truy cập?

- a. Enable password
- b. Enable secret
- c. Không có mật khẩu nào
- d. Lệnh password, nếu nó được cấu hình

Câu 2: Khi cấu hình switch Cisco 2960 cho phép truy cập Telnet với mật khẩu mypassword. Sau đó thay đổi cấu hình để hỗ trợ SSH. Lệnh nào sau đây có thể là một phần của cấu hình mới?

- a. Một lệnh username name password pass trong chế độ cấu hình vtyb
- c. Một lệnh username name password pass trong lệnh cấu hình toàn cục
- d. Một lệnh cấu hình transport input ssh trong chế độ cấu hình vty
- e. Một lệnh cấu hình toàn cục transport input ssh.

Câu 3. Lệnh sau đây đã được sao chép và dán vào chế độ cấu hình khi một người dùng telnet đến một switch Cisco:

“Banner login this is the login banner”

Điều nào sau đây là đúng khi người dùng đăng nhập lần tiếp theo từ console?

- a. Không có văn bản banner nào hiện ra
- b. Văn bản banner “his is” xuất hiện
- c. Văn bản banner “this is the login banner” xuất hiện
- d. Văn bản banner “Login banner configured, no text defined” xuất hiện

Câu 4: Điều nào sau đây không cần yêu cầu khi cấu hình bảo mật port mà không học theo sticky?

- a. Thiết lập số địa chỉ MAC tối đa cho phép trên giao tiếp với lệnh con cấu hình giao tiếp switchport port-security maximum
- b. Cho phép port security với lệnh con giao tiếp switchport port-security
- c. Xác định các địa chỉ MAC được phép sử dụng lệnh con giao tiếp switchport port – security mac – address
- d. Tất cả các phương án trên

Câu 5. Kết nối máy tính với switch tại khu vực chính. Một router tại khu vực chính kết nối đến mỗi văn phòng chi nhánh thông qua một kết nối serial, với một router nhỏ và một switch tại mỗi chi nhánh. Lệnh nào sau đây phải được cấu hình, trong chế độ cấu hình được liệt kê, để cho phép telnet đến các switch văn phòng chi nhánh?

- a. Lệnh ip address trong chế độ cấu hình VLAN 1
- b. Lệnh ip address trong chế độ cấu hình toàn cục
- c. Lệnh ip default – gateway trong chế độ cấu hình VLAN 1
- d. Lệnh ip default – gateway trong chế độ cấu hình toàn cục
- e. Lệnh password trong chế độ cấu hình console line
- f. Lệnh password trong chế độ cấu hình vty line

Câu 6. Lệnh nào sau đây mô tả cách hủy chức năng tự thỏa thuận trên một port 10/100 của switch Cisco?

- a. Lệnh con giao tiếp negotiate disable
- b. Lệnh con giao tiếp no negotiate
- c. Lệnh con giao tiếp speed 100
- d. Lệnh con giao tiếp duplex half
- e. Lệnh con giao tiếp duplex full
- f. Lệnh con giao tiếp speed 100 và duplex full

Câu 7. Trong chế độ cấu hình đây cho phép cấu hình duplex cho giao tiếp fastatethernet 0/5?

- a. Chế độ người dùng
- b. Chế độ Cấp quyền
- c. Chế độ cấu hình toàn cục
- d. Chế độ thiết lập
- e. Chế độ cấu hình giao tiếp

Chương 3

MẠNG NỘI BỘ ẢO (Virtual Local Area Network - VLAN)

Các giao tiếp của switch Cisco được xem như là giao tiếp truy cập hoặc là giao tiếp trung kế. Theo định nghĩa, giao tiếp truy cập gửi và nhận các frame chỉ trên một VLAN đơn, được gọi là VLAN truy cập. Các giao tiếp trung kế gửi và nhận lưu lượng trên nhiều VLAN.

Một thiết bị Cisco Catalyst sử dụng các thiết lập mặc định cho phép nó làm việc mà không phải cấu hình bổ sung. Tuy nhiên, việc cấu hình thiết bị switch hầu hết tập trung ba vấn đề chính sau đây: VLANs, được đề cập trong chương này; Spanning Tree, được đề cập ở chương sau và nhiều thiết lập quản trị khác của switch, đã được giải thích trong các chương trước.

Phần quan trọng đầu tiên của chương này giải thích các khái niệm cốt lõi, bao gồm làm thế nào chuyển dung lượng VLAN giữa các switch sử dụng các trung kế VLAN và làm thế nào để các giao thức trung kế VLAN (VTP) hỗ trợ tiến trình cấu hình VLAN trong một mạng LAN? Làm thế nào để gán các giao tiếp tĩnh cho một VLAN. Phần quan trọng cuối cùng xem xét cấu hình VTP và xử lý sự cố có liên quan.

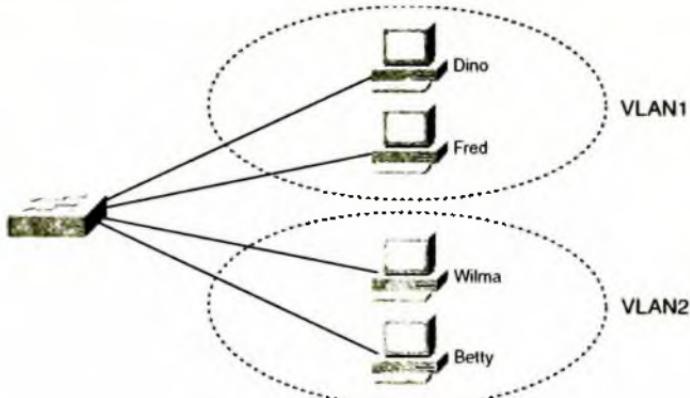
3.1. CÁC KHÁI NIỆM VỀ MẠNG LAN ẢO

Trước khi tìm hiểu về VLANs, cần có kiến thức nhất định về định nghĩa của một mạng LAN. Mặc dù có thể nghĩ về LAN từ các mặt khác nhau, cụ thể một khái niệm có thể giúp hiểu hơn về VLAN là:

- Một LAN bao gồm tất cả các thiết bị trong cùng một miền quang bá.

- Một miền quảng bá bao gồm tập hợp tất cả các thiết bị mạng LAN được kết nối để khi bắt đầu một thiết bị gửi một frame quảng bá, tất cả các thiết bị lấy được bản sao của frame đó. Vì thế có thể xem LAN và miền quảng bá là như nhau.

Nếu không có VLANs, một switch xem tất cả các giao tiếp của nó ở cùng một miền quảng bá; nói cách khác, tất cả các thiết bị được kết nối trên cùng một LAN. Với VLAN, một switch có thể đặt một số giao tiếp vào một miền quảng bá và một số giao tiếp khác vào miền quảng bá khác, để tạo ra nhiều miền quảng bá. Những miền quảng bá cá nhân được tạo ra bởi switch được gọi là mạng LAN ảo. Hình 3.1 cho thấy một ví dụ, hai mạng LAN và hai thiết bị trên một VLAN.



Hình 3.1. Mạng LAN ảo

Việc đặt các thiết bị vào các miền VLAN khác nhau mang lại cho nhiều lợi ích. Thuận lợi lớn nhất là thông tin quảng bá từ một thiết bị trong VLAN sẽ được nhận và xử lý bởi tất cả các thiết bị khác trên VLAN, chứ không phải bởi các thiết bị khác trên một VLAN khác. Càng nhiều thiết bị trên một VLAN đơn, số lượng gói tin quảng bá càng lớn, và thời gian xử lý được yêu cầu càng lớn bởi một thiết bị trên VLAN đó. Ngoài ra, mọi người có thể download nhiều gói phần mềm miễn phí, thường được gọi là các phần mềm phân tích giao thức, ví dụ như là

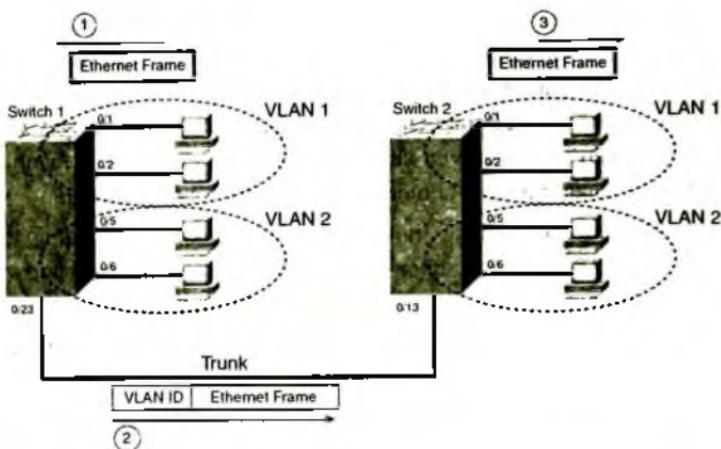
Wireshark để bắt giữ các frame được nhận bởi một thiết bị. Kết quả là, các mạng VLAN lớn hơn tạo ra số lượng lớn và nhiều loại hơn các gói tin quảng bá đến các thiết bị khác, chính vì thế tạo ra các kẽ hở bảo mật giúp cho kẻ tấn công có thể thâm nhập và nghe lén hệ thống. Đây chỉ là một vài nguyên nhân chủ yếu cho việc phân chia các thiết bị thành các VLAN khác nhau. Sau đây là một số nguyên nhân phổ biến nhất:

- Để tạo các thiết kế linh động hơn để nhóm người dùng theo phòng ban, hay các nhóm làm việc cùng nhau, thay vì bằng vị trí địa lý.
- Để phân các thiết bị thành các mạng LAN nhỏ hơn (miền quảng bá) để giảm tắc nghẽn do mỗi thiết bị trên VLAN này
- Để giảm tải cho giao thức STP bằng cách hạn chế một VLAN cho một switch truy cập đơn.
- Để đảm bảo bảo mật tốt hơn bằng cách đặt các thiết bị làm việc với các dữ liệu nhạy cảm trên các VLAN tách rời.
- Để phân tách lưu lượng được gửi bởi một IP Phone từ các lưu lượng được gửi bởi các PC được kết nối đến điện thoại đó.

Chương này tập trung vào làm thế nào các VLANs làm việc qua nhiều switch Cisco, bao gồm cấu hình yêu cầu được triển khai. Phần kế tiếp kiểm tra trung kế VLAN, một chức năng được yêu cầu khi cài đặt VLAN trên hệ thống nhiều switch.

3.2. XÂY DỰNG TRUNG KẾ VỚI ISL VÀ 802.1Q

Khi sử dụng VLAN trong các mạng có nhiều switch được kết nối với nhau, các switch này cần sử dụng trung kế VLAN trên các phân đoạn mạng giữa các switch. Trung kế VLAN thực chất là các switch sử dụng một tiến trình được gọi là VLAN gging, bằng cách switch gửi thêm các tiêu đề khác vào frame trước khi gửi nó ra ngoài giao tiếp trung kế. Điều này làm tăng tải tiêu đề cho VLAN, bao gồm một trường định danh VLAN (VLAN ID) để switch gửi có thể liệt kê VLAN ID, và switch nhận có thể sau đó biết được rằng mỗi frame đó thuộc về VLAN nào. Hình 3.2 cho thấy ý tưởng về trung kế VLAN.



Hình 3.2. Trung kế VLAN giữa hai switch

Sử dụng trung kế cho phép các switch chuyển các frame từ nhiều VLAN qua một kết nối vật lý đơn. Lấy ví dụ, hình 3.2 cho thấy switch 1 đang nhận một frame quảng bá trên giao tiếp Fa0/1 tại bước 1. Để gửi frame này, switch 1 cần chuyển gói tin quảng bá đến switch 2. Tuy nhiên, switch 1 cần cho switch 2 biết rằng frame đó là một phần của VLAN 1. Vì thế, như thể hiện trong bước 2, trước khi gửi frame đi, switch 1 thêm một tiêu đề VLAN vào frame Ethernet gốc, với tiêu đề VLAN liệt kê một ID VLAN của switch 1 trong trường hợp này. Khi switch 2 nhận frame này, nó nhận thấy rằng frame từ một thiết bị trên VLAN 1, vì thế switch 2 biết rằng nó chỉ nên chuyển gói tin quảng bá ra ngoài các giao tiếp trên VLAN 1 của chính bản thân nó. Switch 2 gỡ bỏ tiêu đề VLAN, chuyển tiếp frame gốc này ra ngoài giao tiếp của nó trong VLAN 1 (bước 3).

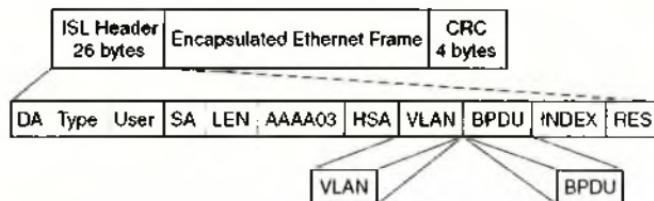
Lấy ví dụ khác, xem xét trong trường hợp khi thiết bị trên giao tiếp Fa0/5 của switch 1 gửi một gói quảng bá. Switch 1 gửi gói tin này ra ngoài port Fa0/6 (vì hai port này trên cùng VLAN 2) và ra ngoài Fa0/23 (bởi vì nó là một trung kế, nghĩa là nó hỗ trợ nhiều VLAN khác nhau). Switch 1 thêm một tiêu đề trung kế vào frame này, liệt kê một VLAN ID 2.

Switch 2 gỡ bỏ tiêu đề trung kế sau khi cảnh báo rằng frame là một phần của VLAN2, vì thế switch 2 biết để chuyển frame này ra ngoài chỉ các port Fa0/5 Fa0/6, chứ không phải Fa0/1 và Fa0/2.

Các cisco switch hỗ trợ hai giao thức trung kế khác nhau: Inter – Switch Link (ISL) và IEEE 802.1Q. Các giao thức trung kế cung cấp nhiều chức năng, quan trọng nhất là chúng xác định tiêu đề đặc trưng cho VLAN ID, như hình 3.2. Chúng còn thực hiện các chức năng khác, như sẽ được đề cập sau.

3.2.1. Phương thức trung kế ISL Inter – Switch Link

Cisco đã tạo ISL nhiều năm trước khi IEEE tạo chuẩn 802.1Q cho giao thức trung kế VLAN. Bởi vì ISL là một chuẩn riêng của Cisco, nó có thể được sử dụng chỉ giữa hai thiết bị switch Cisco hỗ trợ ISL (một số switch Cisco mới không hỗ trợ ISL, thay vào đó chỉ hỗ trợ cho giao thức đã được chuẩn hóa, 802.1Q). ISL đóng gói hoàn toàn mỗi frame Ethernet gốc trong một tiêu đề và hậu đê ISL. Frame Ethernet gốc bên trong tiêu đề và hậu đê của ISL được giữ không thay đổi, như trong hình 3.3.



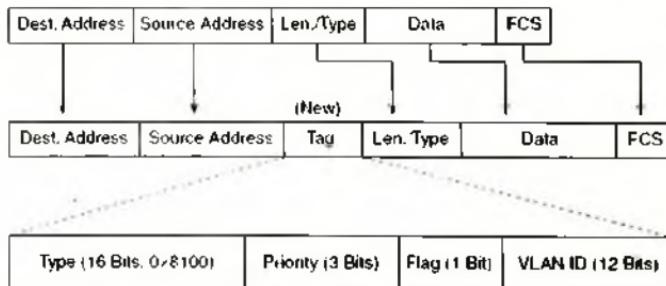
Hình 3.3. Tiêu đề ISL

Tiêu đề ISL bao gồm nhiều trường, nhưng quan trọng nhất, tiêu đề ISL VLAN cung cấp một nơi để giải mã số VLAN ID. Bằng cách đánh dấu một frame với dùng số VLAN bên trong tiêu đề, switch gửi có thể đảm bảo rằng switch nhận biết frame được đóng gói thuộc về VLAN nào. Cũng vậy, các địa chỉ nguồn và đích trong tiêu đề ISL sử dụng các địa chỉ MAC của các switch gửi và nhận, như để xuất cho các thiết bị mà thực sự gửi frame gốc này. Ngoài ra, các chi tiết của tiêu đề ISL là không quan trọng.

3.2.2. Phương thức trung kế IEEE 802.1Q

IEEE chuẩn hóa nhiều giao thức có liên quan đến LAN ngày nay và Trung kế VLAN không phải là ngoại lệ. Nhiều năm sau khi Cisco tạo ISL, IEEE hoàn tất công việc trên chuẩn 802.1Q, xác định một cách khác để thực hiện trung kế VLAN. Ngày nay, 802.1Q trở thành giao thức trung kế phổ biến hơn, vì thế Cisco thậm chí không hỗ trợ ISL trong một số mẫu LAN switch mới sau này, bao gồm switch 2960 được sử dụng trong các ví dụ của giáo trình này.

802.1Q sử dụng kiểu tiêu đề khác ISL để đánh dấu các frame với một số VLAN. Thực ra, 802.1Q không thực sự đóng gói frame gốc trong tiêu đề và phụ đề của Ethernet khác. Thay vào đó, 802.1Q chèn một tiêu đề VLAN 4 byte vào tiêu đề Ethernet gốc. Kết quả là, không giống như ISL, frame vẫn có cùng các địa chỉ MAC nguồn và MAC đích với gói tin gốc. Cũng vậy, bởi vì tiêu đề gốc được mở rộng, cơ chế đóng gói 802.1Q bắt buộc tính toán lại trường FCS của frame gốc trong hậu đề của Ethernet, bởi vì FCS được dựa trên nội dung của toàn bộ frame. Hình 3.4 cho thấy tiêu đề của 802.1Q và việc đóng gói của tiêu đề Ethernet mong muốn.



Hình 3.4. Tiêu đề 802.1Q

3.2.3. So sánh ISL và IEEE 802.1Q

Có thể thấy, phần trên đã mô tả một điểm chung giữa ISL và 802.1Q, với hai khác biệt. Điểm chung là cả hai ISL và 802.1Q định nghĩa một tiêu đề VLAN có một trường VLAN ID. Tuy nhiên, mỗi giao thức trung kế sử dụng một tiêu đề khác nhau hoàn toàn được chuẩn hóa.

802.1Q và chuẩn dành riêng ISL. Phần này chỉ ra một vài điểm so sánh chính giữa hai giao thức.

Cả hai giao thức trung kế hỗ trợ cùng số VLAN, cụ thể là 4094 VLAN. Cả hai giao thức sử dụng 12 bit của tiêu đề VLAN để đánh số VLAN, hỗ trợ 2^{12} (hay 4096 VLAN ID), trừ đi hai giá trị để dành (0 và 4095), trong đó các VLAN ID 1-1005 được xem như là dãy VLAN thông thường, trong khi các giá trị lớn hơn 1005 được gọi là dãy VLAN mở rộng, được sử dụng cho VTP.

ISL và 802.1Q đều hỗ trợ một phương pháp STP cho mỗi VLAN, nhưng việc triển khai chi tiết khác nhau (được giải thích trong chương 2). Các LAN với các liên kết dự phòng, sử dụng chỉ một thực thể của STP có nghĩa rằng một số liên kết rảnh rỗi dưới mức hoạt động thông thường, với các liên kết khác chỉ được sử dụng khi các liên kết này bị lỗi, bằng cách hỗ trợ nhiều thực thể của STP, có thể điều chỉnh các tham số STP để mà dưới các hoạt động thông thường, một số lưu lượng VLAN sử dụng một tập hợp các liên kết và các lưu lượng VLAN khác sử dụng các liên kết khác, thuận lợi trên tất cả các liên kết trong mạng.

Điểm khác biệt chính cuối cùng giữa ISL và 802.1Q được xem xét ở đây liên quan đến một chức năng được gọi là native VLAN. 802.1Q định nghĩa một VLAN trên mỗi trung kế như là một native VLAN, trong khi ISL không sử dụng khái niệm này. Mặc định, 802.1Q native VLAN là VLAN 1. Theo định nghĩa 802.1Q đơn giản không thêm một tiêu đề 802.1Q vào các frame trong native VLAN này. Khi switch ở phía kia của trung kế nhận một frame mà không có một tiêu đề 802.1Q, switch nhận biết rằng frame đó là một phần của native VLAN. Chú ý rằng bởi vì thuộc tính này, cả hai switch phải đồng ý VLAN nào là native VLAN.

802.1Q native VLAN cung cấp một số chức năng lý thú, chủ yếu hỗ trợ các kết nối đến các thiết bị mà không hiểu về trung kế. Lấy ví dụ, một switch Cisco có thể không hiểu về trung kế 802.1Q. Switch này có thể gửi các frame trong native VLAN – có nghĩa là frame không có tiêu đề trung kế – vì thế switch khác sẽ hiểu được frame này với cùng một native VLAN với switch đó. Khái niệm native VLAN cho các switch khả năng chuyển ít nhất lưu lượng trên một VLAN (native VLAN), và cho phép một số chức năng cơ bản khác, như là khả năng có thể telnet đến một switch.

Bảng 3.1. So sánh ISL và 802.1Q

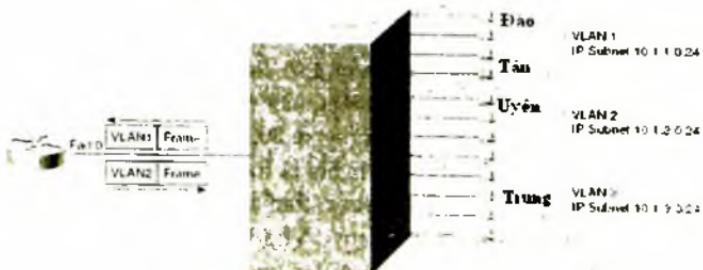
Chức năng	ISL	802.1Q
Định nghĩa bởi	Cisco	IEEE
Chèn thêm bốn byte tiêu đề để hoàn tất đóng gói frame ban đầu	NO	YES
Hỗ trợ các khoảng VLAN thông thường (1 - 1005) và mở rộng (1006 - 4094)	YES	YES
Cho phép nhiều cây bao trùm	YES	YES
Sử dụng native VLAN	NO	YES

3.3. IP SUBNETS VÀ VLAN

Khi xem xét một thiết kế VLAN, các thiết bị bên trong một VLAN cần ở trong cùng một subnet. Tương tự, các thiết bị bên trong các VLAN khác nhau cần ở trong các subnet khác nhau.

Vì những quy tắc thiết kế này, nhiều người nghĩ rằng VLANs là một subnet và rằng một subnet là một VLAN. Dù rằng nó không hoàn toàn đúng bởi vì một VLAN là một khái niệm lớp 2 và một subnet là một khái niệm lớp 3, ý tưởng chung có thể giải thích được vì các thiết bị trong cùng một VLAN đơn là các thiết bị trong cùng một subnet đơn.

Cũng như với tất cả các subnet IP, với một thiết bị trong một subnet để chuyển các gói tin đến một subnet khác, ít nhất cần có một router trung gian. Lấy ví dụ, xem xét hình 3.5, cho thấy một switch với 3 VLANs, được thể hiện trong các đường đứt nét, trong đó có ví dụ khi một thiết bị trong VLAN 1 gửi một gói tin IP đến một thiết bị trong VLAN 2.



Hình 3.5. Mạng con IP và VLANs

Trong trường hợp này, khi Tân gửi một gói tin đến địa chỉ IP của Uyên, Tân gửi gói tin đó đến router mặc định, bởi vì địa chỉ IP của Uyên ở trong subnet khác. Router nhận frame này, với một tiêu đề VLAN nhấn mạnh rằng frame đó là một phần của VLAN 1. Router thực hiện quyết định chuyển gói tin, gửi gói tin ngược lại cho cùng liên kết vật lý đó, tại thời điểm này header Trung kế VLAN liệt kê là VLAN 2. Switch chuyển frame đó trong VLAN 2 cho Uyên.

Kiểu thiết kế này không hiệu quả khi gửi gói tin từ switch đến router, và quay ngược lại switch. Một lựa chọn tương tự trong các mạng LAN hiện nay là sử dụng một switch được gọi là switch đa lớp hay một switch lớp 3. Những switch này có thể hoạt động ở cả lớp 2 chuyển mạch và lớp 3 định tuyến, kết hợp chức năng của router thể hiện trong hình 3.5.

3.4. GIAO THỨC TRUNG KẾ VLAN

Giao thức trung kế VLAN của Cisco cung cấp một phương tiện bằng cách các switch Cisco có thể trao đổi thông tin cấu hình VLAN. Cụ thể là, VTP quảng bá về sự tồn tại của mỗi VLAN dựa trên VLAN ID của nó và VLAN name. Tuy nhiên, VTP không quảng bá chi tiết về giao tiếp nào của switch được gán cho mỗi VLAN.

Vì cuốn sách này không thể hiện cách cấu hình VLAN, để hiểu hơn về VTP, xem xét ví dụ sau đây về những gì VTP có thể làm. Tưởng tượng rằng một mạng có 10 switch được kết nối bằng cách nào đó sử dụng các Trung kế VLAN, và mỗi switch có ít nhất một port được gán cho một VLAN với VLAN ID 3 và tên là Accounting. Nếu không có VTP, có thể phải đăng nhập vào 10 switch và nhập hai câu lệnh cấu hình để tạo VLAN và xác định tên của nó. Với VTP, có thể tạo VLAN 3 trên một switch và trên 9 switch còn lại sẽ học về VLAN 3 đó và tên của nó sử dụng VTP.

VTP định nghĩa một giao thức trao đổi thông điệp lớp 2 mà các switch sử dụng để trao đổi thông tin cấu hình VLAN. Khi một switch thay đổi thông tin cấu hình VLAN của nó – nói cách khác, khi một VLAN được thêm hay xóa hay một VLAN hiện tại bị thay đổi – VTP

làm cho tất cả các switch đồng bộ cấu hình VLAN, bao gồm cùng VLAN ID và VLAN name. Tiến trình này là tương tự như giao thức định tuyến, trong đó mỗi switch gửi các thông điệp VTP theo một khoảng thời gian nhất định. Các switch cũng gửi các thông điệp VTP ngay khi cấu hình VLAN thay đổi. Lấy ví dụ, cấu hình một VLAN 3 mới, với tên Accounting, switch sẽ ngay lập tức gửi các cập nhật VTP ra ngoài tất cả các trung kế, dẫn đến việc phân phối của thông tin VLAN mới cho các switch còn lại.

Mỗi switch sử dụng một trong ba chế độ VTP: server mode, client mode, và transparent mode. Để sử dụng VTP, có thể thiết lập một số switch sử dụng chế độ server và phần còn lại sử dụng chế độ client. Sau đó, cấu hình VLAN có thể được thêm vào trên các server, sau đó tất cả các server và client khác học về những thay đổi với cơ sở dữ liệu VLAN trên VTP server đã thay đổi. Clients không thể được sử dụng để cấu hình thông tin VLAN.

Các switch Cisco không thể bỏ chức năng VTP. Tuy nhiên có thể sử dụng chế độ transparent, làm cho switch bỏ qua các thông điệp VTP, tuy nhiên vẫn chuyển tiếp các thông điệp VTP đến client hoặc server khác.

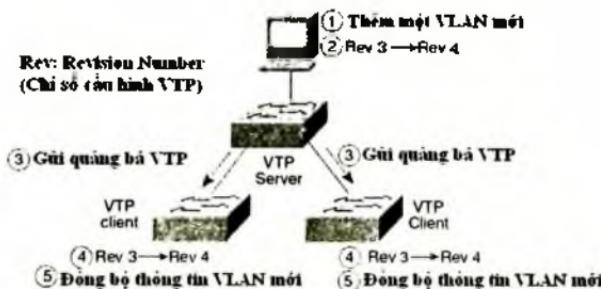
Phản tiếp theo giải thích về các hoạt động thông thường khi sử dụng các chế độ server và client để có được những lợi ích của VTP và cuối cùng là hoạt động của switch ở chế độ VTP transparent.

3.4.1. Hoạt động của VTP sử dụng các chế độ VTP server và client

Tiến trình VTP server bắt đầu với việc tạo VLAN trên một switch được gọi là VTP server. VTP Server sau đó phân phối những thay đổi cấu hình VTP thông qua các bản tin VTP, chỉ được gửi qua các trung kế ISL và 802.1Q, thông qua mạng. Cả hai VTP server và client xử lý các thông điệp VTP nhận được, cập nhật cơ sở dữ liệu cấu hình VTP của chúng dựa trên các thông điệp này và gửi một cách độc lập các cập nhật VTP ra ngoài các trung kế của chúng. Cuối tiến trình này, tất cả các switch học về thông tin VTP mới.

VTP Server và client chọn liệu có tái hoạt động với một cập nhật VTP được nhận, và cập nhật các cấu hình VLAN dựa trên sự gia tăng số

cấu hình cơ sở dữ liệu VLAN (configuration revision number). Mỗi khi một VTP server chỉnh sửa thông tin cấu hình VLAN của nó, VTP server tăng số cấu hình hiện tại lên 1. Các thông điệp cập nhật VTP liệt kê số cấu hình mới này. Khi client hoặc server switch khác nhận một thông điệp VTP với một chi số cấu hình cao hơn của nó, switch cập nhật cấu hình VLAN của nó. Hình 3.6 mô tả làm thế nào VTP hoạt động trên một mạng chuyển mạch.



Hình 3.6. Tạo Trung kế VLAN

Hình 3.6 bắt đầu với tất cả switch có cùng chi số cấu hình VLAN (revision configuration number), nghĩa là chúng có cùng cơ sở dữ liệu cấu hình VLAN: tất cả các switch biết cùng chi số VLAN và VLAN name; tiến trình bắt đầu với mỗi switch biết về chi số cấu hình hiện tại là 3. Các bước thể hiện trong hình 3.6 như sau:

1. Một VLAN mới được cấu hình từ giao diện dòng lệnh CLI của một VTP server.
2. VTP Server cập nhật chi số cấu hình VLAN của nó từ 3 sang 4.
3. Server gửi các thông điệp cập nhật VTP ra ngoài các giao tiếp trung kế của nó, báo rằng chi số cấu hình là 4.
4. Hai client switch VTP nhận được thông điệp VTP với chi số cấu hình cao hơn chi số cấu hình hiện tại của nó, cập nhật từ 3 lên 4.
5. Hai client switch cập nhật cơ sở dữ liệu VLAN của nó dựa trên cập nhật VTP của server.

Ví dụ này cho thấy hoạt động VTP trên một mạng LAN rất nhỏ. Tiền trình VTP cũng làm việc tương tự cho các mạng lớn hơn. Khi một VTP server cập nhật cấu hình VLAN, server ngay lập tức gửi các thông điệp VTP ra ngoài tất cả các trung kế. Các switch lân cận trên các đầu cuối của các trung kế xử lý các thông điệp nhận được và cập nhật các cơ sở dữ liệu VLAN và sau đó chúng gửi các thông điệp VTP đến các switch lân cận của nó. Tiền trình lặp lại trên các lân cận, cho đến khi tất cả các switch đã có được cơ sở dữ liệu VLAN mới này.

Các VTP server và client cũng gửi các thông điệp VTP sau chu kỳ 5 phút, để gửi cho nhau các thông tin VTP. Ngoài ra, khi một trung kế mới được kích hoạt, các switch có thể ngay lập tức gửi một thông điệp VTP hỏi thăm switch lân cận để gửi cơ sở dữ liệu VTP của nó.

Chương này đã đề cập đến các thông điệp VTP như cũng như cách cập nhật hay các thông điệp VTP. Trong thực tế, VTP định nghĩa 3 loại thông điệp: đầu tiên là các quảng bá tóm tắt, liệt kê chi số xem xét, tên miền, và thông tin khác, nhưng không có thông tin VLAN. Các thông điệp VTP định kỳ xảy ra 5 phút mỗi lần là các quảng bá tóm tắt VTP.

Thứ hai, nếu có thay đổi xảy ra với VTP, như là xuất hiện một chi số xem xét lớn hơn, thông điệp quảng bá tóm tắt được theo sau bởi một hay nhiều các quảng bá con, mỗi một thông điệp quảng bá là tập con của cơ sở dữ liệu VLAN.

Thông điệp thứ ba, thông điệp yêu cầu quảng bá, cho phép một switch ngay lập tức yêu cầu các thông điệp VTP từ một switch lân cận ngay khi một trung kế được bật lên.

3.4.2. Ba yêu cầu cho VTP để làm việc giữa các switch

Khi một VTP client hay server kết nối đến một VTP client hay server switch khác, Cisco IOS yêu cầu thỏa mãn ba yêu tố sau trước khi hai switch có thể trao đổi các thông điệp VTP cho nhau:

- Liên kết giữa các switch phải đang hoạt động như là một trung kế VLAN (ISL hay là 802.1Q)
- Hai tên miền VTP đúng kiểu (case – sensitive) của hai switch phải giống nhau

- Nếu được cấu hình trên ít nhất một trong các switch, mật khẩu VTP (đúng kiểu) của hai switch phải giống nhau.

Tên miền VTP cung cấp một cung cấp thiết kế để tạo nhiều nhóm cho VTP switch, được gọi là các miền, cho phép cấu hình tự động VLAN. Để làm như vậy, có thể cấu hình một trong các switch trong một miền VTP và các switch khác trên miền VTP khác. Các switch trên các miền khác sẽ bỏ qua các thông điệp VTP nếu không cùng tên miền. Các miền VTP cho phép các nhà thiết kế phân chia mạng chuyển mạch thành các miền quản trị khác nhau. Lấy ví dụ, trong một tòa nhà lớn với một đội ngũ IT lớn, một nhánh nhân viên IT có thể sử dụng VTP tên miền là Accounting, trong khi nhánh khác của đội ngũ IT có thể sử dụng một tên miền là Sales, cho phép duy trì kiểm soát các cấu hình của hệ thống nhưng tiếp tục chuyển lưu lượng giữa các nhánh thông qua cơ sở hạ tầng LAN.

Cơ chế mật khẩu VTP giúp một switch có thể ngăn ngừa các kẻ xâm nhập có thể thâm nhập và thay đổi cấu hình VLAN. Bản thân mật khẩu không bao giờ được truyền đi dưới dạng văn bản thuần túy.

3.4.3. Tránh VTP bằng cách sử dụng chế độ VTP transparent

Để tránh sử dụng VTP trao đổi thông tin VLAN trong các switch Cisco, các switch không thể hủy bỏ chế độ VTP. Thay vào đó, các switch phải sử dụng phương thức VTP thứ ba: chế độ VTP transparent. Chế độ transparent cho phép bỏ qua trao đổi thông điệp VTP với các switch khác. Giống như VTP server, các switch chế độ VTP transparent có thể cấu hình VLAN. Tuy nhiên, không giống như server, switch chế độ transparent không bao giờ cập nhật cơ sở dữ liệu VLAN của chúng dựa trên các thông điệp VTP đến, và các switch chế độ transparent không bao giờ thử tạo các thông điệp VTP để thông báo cho các switch khác về cấu hình VLAN của nó.

3.4.4. Lưu trữ cấu hình VLAN

Để chuyển lưu lượng cho một VLAN, một switch cần phải biết về VLAN ID của một VLAN và tên VLAN của nó. Công việc của VTP là

để quảng bá các chi tiết này, với tập hợp đầy đủ cấu hình cho tất cả VLAN được gọi là cơ sở dữ liệu cấu hình VLAN, hay đơn giản là cơ sở dữ liệu VLAN.

Cisco IOS lưu trữ thông tin trong cơ sở dữ liệu VLAN theo cách khác so với hầu hết các lệnh cấu hình Cisco IOS khác. Khi một VTP client và server lưu trữ cấu hình VLAN, bao gồm VLAN ID, VLAN name và các thiết lập cấu hình VTP khác – cấu hình này được lưu trữ trong một file gọi là `vlan.dat` trong bộ nhớ flash. Ngoài ra, Cisco IOS không đặt cấu hình VLAN vào trong file cấu hình running – config hay startup – config. Không có câu lệnh nào tồn tại để xem cấu hình VLAN một cách trực tiếp; cần sử dụng nhiều câu lệnh show để liệt kê thông tin về VLAN và cấu hình VTP.

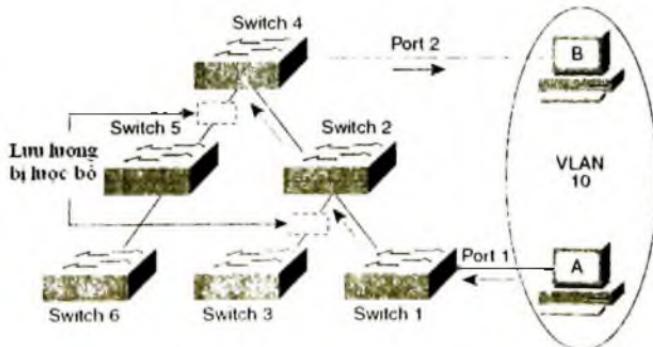
Tiến trình lưu trữ cấu hình VLAN bằng flash trong tập tin `vlan.dat` cho phép cả hai server và client tự động học hỏi về VLANs, và có cấu hình được lưu trữ một cách tự động, chính vì thế làm cho cả server và client được cung cấp đầy đủ thông tin VLAN và VTP cho lần khởi động lại (reload) kế tiếp. Nếu việc cấu hình VLAN chỉ là thêm vào file cấu hình running config, thì mạng LAN có thể bị hư hỏng trong trường hợp tất cả các switch bị mất điện trong cùng thời gian (để dàng xảy ra với một nguồn cấp điện đơn vào một tòa nhà), kết quả là mất tất cả thông tin cấu hình VLAN. Bằng cách lưu trữ tự động trong file `vlan.dat` trong bộ nhớ flash, mỗi switch có ít nhất một cơ sở dữ liệu cấu hình VLAN gần nhất và có thể sau đó dựa trên các cập nhật VTP từ các switch khác nếu bắt ki cấu hình VLAN nào thay đổi gần đây.

Khuyết điểm của tiến trình này là khi sử dụng VTP client hay server switch trong thực tế, và muốn gỡ bỏ tất cả cấu hình để bắt đầu với một switch hoàn toàn không có cấu hình VLAN hay VTP, phải giải sử dụng nhiều câu lệnh khác ngoài câu lệnh `erase startup-config`. Nếu chỉ xóa `startup-config` và khởi động lại switch, switch nhớ tất cả cấu hình VLAN và cấu hình VTP mà nó được lưu trữ trong tập tin `vlan.dat` được đặt trong flash. Để gỡ bỏ chi tiết các cấu hình này trước khi nạp lại switch phải xóa tập tin `vlan.dat` trong flash với câu lệnh là: `delete flash:vlan.dat`.

3.4.5. VTP Pruning (xược bỏ VTP)

Mặc định, các switch Cisco đẩy các gói tin quảng bá (broadcasts) và các gói tin đơn hướng (unicast) không rõ đích trong mỗi VLAN đang hoạt động ra tất cả các trung kế bên ngoài, trong trường hợp sơ đồ STP hiện tại không khóa trung kế này. Tuy nhiên trong hầu hết các mạng campus, nhiều VLAN tồn tại trên chỉ một vài switch, nhưng không phải tất cả các switch. Chính vì thế, lãng phí khi chuyển các gói quảng bá qua tất cả các trung kế là lãng phí.

Các switch hỗ trợ hai phương thức trong đó có thể giới hạn các luồng lưu lượng của VLAN thông qua một trung kế. Phương thức đầu tiên yêu cầu cấu hình thủ công cho danh sách VLAN được phép trên mỗi trung kế; việc cấu hình thủ công này được xem xét ở phần sau của chương. Phương thức thứ hai, VTP Prunning, cho phép VTP xác định một cách một cách động switch nào không cần các frame từ các VLAN nào đó, và sau đó VTP lược bỏ các VLAN này từ các trung kế tương ứng. Việc lược bỏ đơn giản có nghĩa là trên các giao tiếp trung kế trên switch tương ứng không gửi các frame sang VLAN đó. Hình 3.7 cho thấy một ví dụ, với các đường đứt nét chỉ thị các trung kế trong đó VLAN đã được tự động lược bỏ đi.



Hình 3.7. Lược bô VTP

Trong hình 3.7 các switch 1 và 4 có các port trong VLAN 10. Với VTP pruning được cho phép trong toàn thể mạng, các switch 2 và 4 tự động sử dụng VTP để học một trong số các switch trong phần trái dưới của hình có bất kì port nào được gán cho VLAN 10. Kết quả là switch 2 và 4 lược bỏ VLAN 10 từ các trung kế như hình vẽ. Việc lược bỏ dẫn đến các switch 2 và 4 không gửi các frame trong VLAN 10 ra ngoài các trung kế này. Lấy ví dụ, khi trạm A gửi một gói tin quảng bá, switch gửi gói quảng bá, như thể hiện trong các đường mũi tên trong hình 3.7.

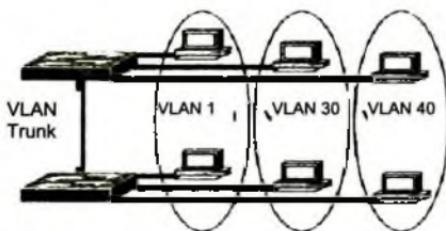
Việc lược bỏ VTP tăng băng thông sẵn sàng cho hệ thống chuyển mạch LAN bằng cách giới hạn lưu lượng được gửi trên mỗi trung kế. Việc lược bỏ VTP là một trong hai nguyên nhân cần thiết nhất để sử dụng VTP, và nguyên nhân khác là để làm cho cấu hình VLAN dễ dàng hơn và nhất quán hơn.

Bảng 3.2.

Chức năng	Server	Client	Transparent
Chỉ gửi các thông điệp VTP ra ngoài trung kế ISL hay 802.1Q	YES	YES	YES
Hỗ trợ cấu hình VLAN CLI	YES	NO	YES
Có thể sử dụng các khoảng VLAN thông thường (1 – 1005)	YES	YES	YES
Có thể sử dụng các khoảng VLAN mở rộng (1006 – 4094)	NO	NO	YES
Đồng bộ cập nhật cơ sở dữ liệu cấu hình của nó khi nhận thông điệp VTP với giá trị chỉ số xem xét cao hơn	YES	YES	NO
Tạo và gửi cập nhật VTP 5 phút một lần	YES	YES	NO
Không xử lý các cập nhật VTP, nhưng chuyển tiếp các cập nhật VTP ra ngoài các trung kế khác	NO	NO	YES
Đặt VLAN ID, VLAN NAME, và cấu hình VTP vào file running – config	NO	NO	YES
Đặt VLAN ID, VLAN NAME và cấu hình VTP vào tập tin vlan.dat trong flash	YES	YES	YES

3.5. CÂU HỎI VÀ BÀI TẬP CHƯƠNG 3

Câu 1. Có bao nhiêu miền quảng bá trong mạng LAN sau đây?



- a. Một
- b. Hai
- c. Ba
- d. Bốn
- e. Năm
- f. Sáu

Câu 2. Trong một LAN, thuật ngữ nào sau đây tương ứng nhất cho thuật ngữ VLAN?

- a. Miền xung đột
- b. Miền quảng bá
- c. Miền mạng con
- d. Switch đơn
- e. Trung kế

Câu 3. Có một switch với ba VLAN được cấu hình. Yêu cầu phải có bao nhiêu mạng con IP, giả sử rằng tất cả các thiết bị trên tất cả VLAN muốn dùng TCP/IP?

- a. 0
- b. 1
- c. 2
- d. 3
- e. Không thể nói gì từ thông tin đã cung cấp

Câu 4. Phương thức nào sau đây đóng gói hoàn toàn frame Ethernet trong một tiêu đề trung kế hơn là chèn thêm một header khác bên trong tiêu đề Ethernet ban đầu?

- a. VTP
- b. ISL
- c. 802.1Q
- d. Cả ISL và 802.1Q
- e. Không có phương án trả lời đúng

Câu 5. Phương thức nào sau đây thêm tiêu đề trung kế cho tất cả các VLAN ngoại trừ một VLAN đặc biệt?

- a. VTP
- b. ISL
- c. 802.1Q
- d. Cả ISL và 802.1Q
- e. Không có câu trả lời nào trên là đúng

Câu 6. Chế độ VTP nào sau đây cho phép VLAN được cấu hình trên một switch?

- a. Client
- b. Server
- c. Transparent
- d. Dynamite
- e. Không có câu trả lời nào chính xác

Câu 7. Giả sử switch 1 được cấu hình với tham số auto cho trung kế trên giao tiếp Fa0/5 của nó, được kết nối đến switch 2. Phải cấu hình switch 2 thiết lập nào sau đây có thể cho phép trung kế làm việc?

- a. Trung kế turned on
- b. Auto
- c. Desirable
- d. Access
- e. Không có câu trả lời nào đúng

Câu 8. Một switch Cisco chưa được cấu hình, muốn vào chế độ cấu hình và thực hiện lệnh vlan 22, sau đó là lệnh name Hannahs-VLAN. Lệnh nào sau đây là đúng?

- a. VLAN 22 được liệt kê trong đầu ra của lệnh show vlan brief
- b. VLAN 22 được liệt kê trong đầu ra của lệnh show running-config
- c. VLAN 22 không được tạo ra bởi tiến trình này
- d. VLAN 22 không tồn tại cho switch cho đến khi ít nhất một giao tiếp được gán cho VLAN đó.

Câu 9. Lệnh nào sau đây liệt kê trạng thái hoạt động của giao tiếp Gigabit 0/1 tương thích với trung kế VLAN?

- a. Show interfaces gi0/1
- b. Show interfaces gi0/1 switchport
- c. Show interfaces gi0/1 trung kế
- d. Show trung kế

Câu 10. Cài đặt bốn switch 2960 mới và kết nối các switch nói trên với nhau sử dụng cáp chéo. Tất cả các giao tiếp đều ở trạng thái up và up. Cấu hình mỗi switch với tên domain VTP là Tân và để tắt cả bốn switch trong chế độ cấu hình VTP server. Thêm một VLAN 33 lúc 9h sáng, và sau đó trong 30 giây, sử dụng lệnh show vlan brief trên ba switch khác, nhưng VLAN33 chưa xuất hiện trên 3 switch còn lại này. Câu trả lời chính xác nhất cho vấn đề này là?

- a. VTP yêu cầu tắt cả các switch có cùng VTP password
- b. Tiếp tục chờ đợi SW1 gửi cập nhật VTP thường kì kế tiếp của nó
- c. Không có liên kết nào giữa trung kế các switch vì chế độ quản trị tự động của 2960
- d. Không có câu trả lời nào đúng.

Câu 11. Các switch SW1 và SW2 kết nối thông qua một liên kết hoạt động, muốn sử dụng VTP để trao đổi các thay đổi cấu hình VLAN. Cấu hình một VLAN mới trên SW1, VLAN 44, nhưng SW2 không

biết về VLAN mới này. Thiết lập cấu hình nào sau đây trên SW1 và SW2 sẽ không là một nguyên nhân tiềm ẩn đe cho SW2 không thể học về VLAN 44?

- a. Tên miền VTP của Lan và LAN, một cách riêng biệt
- b. Mật khẩu VTP của Bá và BÁ, riêng biệt
- c. Lược bỏ VTP được kích hoạt và hủy bỏ, riêng biệt
- d. Chế độ VTP server và client, riêng biệt

Chương 4

GIAO THỨC CÂY BAO PHỦ (Spanning Tree Protocols)

4.1. GIỚI THIỆU

Khi thiết kế LAN với nhiều switch, các phân đoạn Ethernet dự phòng giữa các switch được sử dụng. Mục đích là tăng khả năng chống lỗi cho hệ thống chuyển mạch LAN. Vì một số switch có thể bị lỗi và cáp có thể không được cắm, nhưng nếu các switch dự phòng và cáp được thiết lập, dịch vụ mạng có thể vẫn sẵn sàng cho mọi người làm việc.

Tuy nhiên, LAN với các liên kết dự phòng lại xuất hiện khả năng mà các frame có thể bị lặp vô tận, được gọi là vòng lặp LAN. Những frame bị lặp này có thể gây ra những vấn đề về khả năng thực thi của mạng. Chính vì thế, LAN sử dụng giải thuật STP (Spanning Tree Protocol - Giao thức Cây bao phủ), cho phép các liên kết LAN dự phòng được sử dụng trong khi ngăn ngừa các frame khỏi bị lặp quanh LAN được xác định thông qua những liên kết dự phòng này. Ngoài ra còn xem xét STP, cùng với một vài câu lệnh cấu hình được sử dụng để điều chỉnh cách STP hoạt động.

Chương này xem xét chi tiết STP, cộng với một khác biệt mới có tên là Giải thuật cây bao phủ nhanh (Rapid STP). Phần cuối của chương xem xét cấu hình STP trên switch 2960 cùng với một số lời khuyên làm thế nào giải quyết các vấn đề STP.

4.2. CÁC VẤN ĐỀ LIÊN QUAN ĐẾN STP

Trong chương trước đã xem xét, nếu không có STP, một LAN với một liên kết dự phòng có thể làm cho các frame Ethernet lặp vô hạn. Với STP, một số switch khóa các port để các port này không chuyền các frame Ethernet. STP lựa chọn các port được khóa để chỉ duy nhất một con đường tồn tại giữa hai phân đoạn LAN bất kì (các miền xung đột). Kết quả là, các frame có thể được chuyền đến mỗi thiết bị, mà không gây nên các lỗi khi các frame bị lặp trong mạng.

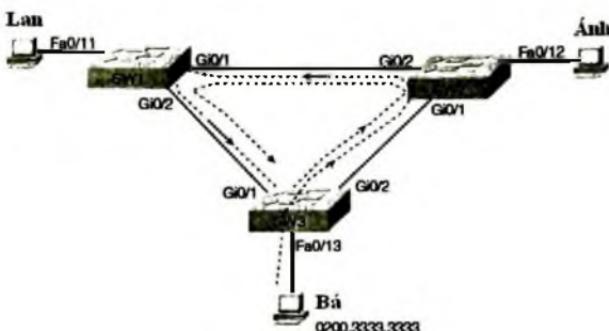
Chương này sẽ bắt đầu với việc giới thiệu nhu cầu cho việc chuẩn hóa IEEE với STP và cách thức chuẩn này làm việc. Phần quan trọng thứ hai giải thích làm thế nào tiêu chuẩn mới và nhanh hơn RSTP làm việc và những so sánh giữa hai chuẩn này với nhau. Hai phần quan trọng cuối cùng kiểm tra việc cấu hình và xử lý sự cố với STP.

4.2.1. Giao thức cây bao phủ STP (802.1d)

802.1d, chuẩn chung đầu tiên cho STP, xác định một giải pháp chấp nhận được cho vấn đề lặp các frame quanh các liên kết dự phòng mãi mãi. Các phần sau đây bắt đầu với mô tả chi tiết hơn cho vấn đề này, theo sau đó là một đặc tả về kết quả cuối cùng cách STP 802.1d giải quyết vấn đề này. Cuối cùng là cách thức STP làm việc, một tiến trình phân tán trên tất cả các LAN switch, để ngăn ngừa vòng lặp.

4.2.1.1. Sự cần thiết của STP

Sử dụng STP có thể giải quyết vấn đề cơ bản nhất là “bão gói tin quang bá”, có thể làm cho các gói tin broadcast (multicast hay unicast không rõ đích) lặp quanh một LAN vô hạn. Kết quả là, một số liên kết có bị tràn ngập các bão sao vô ích của cùng một frame, làm nghẽn các frame có ích, cũng như là ảnh hưởng thấy rõ đến khả năng thực thi của PC người dùng cuối bằng cách làm cho PC xử lý với quá nhiều gói tin loại này. Để thấy làm thế nào điều này xảy ra, hình 4.1 cho thấy một mạng mẫu trong đó Bé gửi một frame broadcast. Các đường đứt nét cho thấy cách switch chuyền frame khi STP không tồn tại.



Hình 4.1. Bão gói tin broadcast

Switch đẩy các gói tin quảng bá này ra ngoài tất cả các giao tiếp trên cùng một VLAN, ngoại trừ giao tiếp đã gửi nó đến. Trong hình này, điều này có nghĩa là SW3 sẽ chuyển frame của Bá đến SW2; SW2 sẽ chuyển đến cho SW1; SW1 sẽ chuyển frame ngược lại cho SW3 và SW3 sẽ bắt đầu chuyển lại cho SW2 như lúc đầu. Frame này lặp vô tận cho đến khi có gì đó xuất hiện – ai đó tắt một giao tiếp, khởi động lại switch, hay làm điều gì đó để tách vòng lặp. Cũng chú ý rằng sự kiện tương tự xảy ra trong phía đối diện. Khi Bá gửi frame gốc, SW3 cũng chuyển một bản sao đến SW1, SW1 chuyển nó đến SW2 và tương tự.

Bảng MAC bắt ôn cũng xuất hiện như là kết quả của các frame bị lặp. Bảng MAC bắt ôn nghĩa là bảng địa chỉ MAC sẽ thay đổi thông tin được liệt kê cho địa chỉ MAC nguồn của frame bị lặp. Lấy ví dụ, SW3 bắt đầu trong hình 4.1 với một bộ địa chỉ MAC như sau:

0200.3333.3333 Fa0/13 VLAN1

Tuy nhiên, xem xét tiến trình học của switch xảy ra khi frame lặp đi đến SW2 sau đó đến SW1, và quay ngược lại giao tiếp Gi0/1 trên SW3. SW3 cho rằng địa chỉ MAC nguồn là 0200.3333.3333 và nó đến giao tiếp Gi0/1. Chính vì thế nó cập nhật bộ này trong bảng MAC trên SW3.

0200.3333.3333 Gi0/1 VLAN 1

Tại thời điểm này, nếu một frame đến tại SW3 – một frame khác với frame gây ra vòng lặp – đến địa chỉ MAC của Bá với 0200.3333.3333,

SW3 sẽ chuyển sai frame đến giao tiếp Gi0/1 đến SW1. Frame mới này cũng có thể lặp, hay frame có thể đơn giản không bao giờ được chuyển đến Bá.

Rắc rối thứ ba có thể gây ra khi không dùng STP trong một mạng có dự phòng là các thiết bị làm việc có nhiều bản sao của cùng frame. Giả sử một trường hợp trong đó Bá gửi một frame đến Lan, nhưng không có switch nào biết địa chỉ MAC của Lan (Các switch đẩy các frame được gửi với các địa chỉ MAC không biết đích). Khi Bá gửi frame (đến địa chỉ MAC của Lan), SW3 gửi một bản sao của nó đến SW1 và SW2. SW1 và SW2 cũng đẩy frame này, dẫn đến các bản sao của frame bị lặp. SW1 cũng gửi một bản sao của mỗi frame ra ngoài giao tiếp Fa0/11 đến Lan. Kết quả là, Lan nhận nhiều bản sao của frame này, có thể dẫn đến một lỗi ứng dụng.

Bảng 4.1 tóm tắt ba loại vấn đề chính xảy ra khi STP không được sử dụng trong LAN có dự phòng.

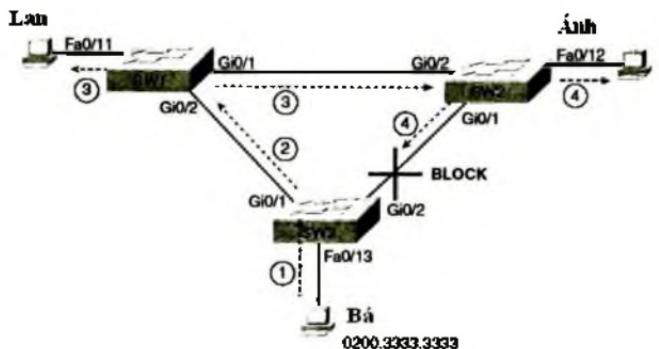
Bảng 4.1. Những vấn đề chính trong mạng LAN không có STP

Lỗi	Mô tả
Bão broadcast	Chuyển tiếp frame lặp lại trên cùng các liên kết, làm giảm đáng kể lưu lượng liên kết
Bảng MAC không ổn định	Tiếp tục cập nhật bảng MAC của switch với các giá trị không chính xác, gây ra do lặp các frame, kết quả là các frame được gửi đến sai địa điểm
Truyền nhiều frame	Ảnh hưởng khác của các frame bị lặp trong đó nhiều bản sao của một frame được chuyển đến máy đích, gây nhầm lẫn máy đích

4.2.1.2. Hoạt động IEEE 802.1d

STP ngăn lặp bằng cách đặt mỗi port trên bridge/switch ở hoặc là Forwarding State – Chế độ Chuyển tiếp hay một Blocking State – Chế độ khóa. Các giao tiếp ở Forwarding State hoạt động thông thường, chuyển và nhận các frame, nhưng các giao ở Blocking State không xử lý bất kì frame nào, ngoại trừ các thông điệp STP. Tất cả các port ở Forwarding State được xem như là cây phủ hiện tại. Tập hợp các port forwarding tạo một con đường đơn qua đó các frame được gửi giữa các phân đoạn

Ethernet. Hình 4.2 cho thấy một cây STP đơn giản giải quyết vấn đề thể hiện trong hình 4.1 bằng cách đặt một port trên SW3 vào chế độ Blocking State.



Hình 4.2. Mạng dự phòng và STP

Bây giờ khi Bá gửi một frame quảng bá, frame không lặp. Bá gửi frame đến SW3 (bước 1), sau đó chỉ chuyển frame đến SW1 (bước 2), bởi vì giao tiếp Gi0/2 SW3 ở trạng thái Blocking State. SW1 dây frame này ra ngoài giao tiếp Fa0/11 và Gi0/1 (bước 3). SW2 dây frame ra ngoài Fa0/12 và Gi0/1 (bước 4). Tuy nhiên, SW3 bỏ qua frame nhận được từ SW2, bởi vì frame này đến giao tiếp Gi0/2 của SW3, ở trạng thái Blocking State.

Với sơ đồ STP trong hình 4.2, switch đơn giản không sử dụng liên kết giữa SW2 và SW3 với các lưu lượng trong VLAN này, cũng là mặt trái khi sử dụng STP. Tuy nhiên, nếu liên kết giữa SW1 và SW3 lỗi, STP thay đổi để SW3 chuyển thay vì khóa trên giao tiếp Gi0/2 của nó.

Chú ý: Thuật ngữ hội tụ STP để cập đến tiến trình trong đó các switch nhận ra rằng có sự thay đổi trong sơ đồ LAN, vì thế switch cần thay đổi các port khóa và port chuyển.

Làm thế nào STP quản lý để làm cho switch khóa hay Chuyển tiếp trên mỗi giao tiếp? Và làm thế nào nó chuyển trạng thái từ Blocking State sang Forwarding State để tận dụng liên kết dự phòng nhằm đáp ứng với những thay đổi của mạng? Mục 4.2.1.3 trả lời cho câu hỏi này.

4.2.1.3. Cách hoạt động của cây bao phủ

Giải thuật STP tạo một cây bao phủ của các giao tiếp chuyên frame. Cấu trúc cây tạo một con đường đơn đi và đến mỗi phân đoạn Ethernet, giống như có thể lùi theo một con đường đơn trên một cây thông thường từ gốc đến mỗi lá.

Tiến trình được sử dụng bởi STP, thỉnh thoảng được gọi là Giải thuật cây bao phủ SPA, chọn các giao tiếp mà sẽ được đặt vào Forwarding State. Với bất kì giao tiếp không được chọn là Forwarding State, SPA đặt những giao tiếp đó vào Blocking State. Nói cách khác, STP đơn giản đặt các giao tiếp được chuyên gói tin đi.

STP sử dụng ba ưu tiên để lựa chọn liệu có đặt một giao tiếp và Forwarding State hay không:

- STP thu thập một gốc switch. STP đặt tất cả các giao tiếp làm việc vào gốc switch trong trạng thái Forwarding State.
- Mỗi switch không phải gốc xem mỗi port của nó có chi phí quản trị ít nhất giữa nó và switch gốc. STP đặt giao tiếp chi phí – gốc – thấp nhất này, gọi tên có là port gốc của switch, trong trạng thái Forwarding State.
- Nhiều switch có thể được kết nối đến cùng một LAN Ethernet. Switch với chi phí quản trị thấp nhất từ nó đến bridge gốc, khi so sánh với các switch được kết nối đến cùng phân đoạn, được đặt vào Forwarding State. Switch chi phí thấp nhất trên mỗi phân đoạn được gọi là bridge được chỉ định, và các giao tiếp của bridge đó, được kết nối đến phân đoạn, được gọi là port được chỉ định.

Chú ý: Nguyên nhân thực sự switch gốc đặt tất cả các giao tiếp làm việc trong Forwarding State là rằng tất cả các giao tiếp của nó sẽ trở thành port được chỉ định (DP), nhưng dễ nhớ hơn rằng tất cả các giao tiếp làm việc của switch gốc sẽ chuyên frame.

Tất cả các giao tiếp khác được đặt ở chế độ Blocking State. Bảng 4.2 tóm tắt các nguyên nhân STP đặt một port vào chế độ Blocking hay Forwarding State.

Bảng 4.2. Nguyên nhân STP đặt một port vào chế độ khóa hay Chuyển tiếp

Đặc tính của port	Trạng thái STP	Mô tả
Tất cả các port của switch root	Chuyển tiếp Forwarding	Switch root luôn là switch dành trên tất cả các phân đoạn có kết nối
Mỗi port của switch không phải là root	Chuyển tiếp Forwarding	Port trên đó switch có chi phí thấp nhất đến switch root
Mỗi port dành riêng trên LAN	Chuyển tiếp Forwarding	Switch chuyển tiếp giá trị BUDU chi phí thấp nhất và phân đoạn là switch dành riêng trên phân đoạn đó
Các port hoạt động khác	Khóa Blocking	Port không được dùng để chuyển tiếp các frame, hoặc là bất kì frame nào nhận được trên các giao tiếp này được xem như là đang chuyển tiếp

Chú ý: STP chỉ xem xét các giao tiếp làm việc. Các giao tiếp lỗi (lấy ví dụ, các giao tiếp không có cáp được cắm) hay các giao tiếp tắt chúc năng quản trị được đặt vào chế độ STP Disabled. Vì thế, phần này nói đến các port hoạt động để đề cập đến các giao tiếp có thể chuyển frame nếu STP đặt giao tiếp đó và Forwarding State.

4.2.1.4. Chỉ số STP và Hello BPDU

SPA bắt đầu với việc bầu cho một switch trở thành switch gốc. Để hiểu rõ hơn về tiến trình bầu chọn này, cần hiểu các thông điệp STP được gửi giữa các switch cũng như khái niệm và định dạng được sử dụng để xác định tính duy nhất cho mỗi switch.

Giá trị STP Bridge ID (BID) là một giá trị 8 byte duy nhất cho mỗi switch. BID thực chất là một trường ưu tiên 2 byte và một ID hệ thống 6 byte, với ID hệ thống được sử dụng dựa trên địa chỉ MAC có sẵn trong mỗi switch. Sử dụng địa chỉ MAC này đảm bảo rằng các BID sẽ là duy nhất.

STP định nghĩa các thông điệp được gọi là đơn vị dữ liệu giao thức bridge (Bridge Protocol Data Units – BPDU), mà bridge và switch sử

dụng để trao đổi thông tin với nhau. Thông điệp thông thường nhất, được gọi là Hello BPDU, liệt kê BID của switch đang trao đổi thông tin. Bằng cách liệt kê giá trị duy nhất BID của nó, switch có thể báo sự khác biệt giữa BPDU được gửi bởi các switch khác nhau. Thông điệp này cũng liệt kê BID của switch gốc hiện tại.

STP định nghĩa nhiều loại thông điệp BPDU khác nhau, với Hello BPDU là thông điệp làm việc nhiều nhất. Hello BPDU bao gồm nhiều trường, nhưng quan trọng nhất, là các trường được liệt kê trong bảng 4.3.

Bảng 4.3. Các trường trong Hello - BPDU

Trường	Mô tả
Định danh root bridge	Định danh cầu nối của switch/bridge mà thiết bị gửi bản tin Hello này đang tin nó là switch root
Định danh bridge của máy phát	Bridge ID của switch/ bridge gửi bản tin Hello BPDU này.
Chi phí đến root	Chi phí STP giữa switch và root hiện tại
Giá trị bộ định thời trên switch root	Bao gồm bộ định thời Hello, MaxAge, Và Forward Delay

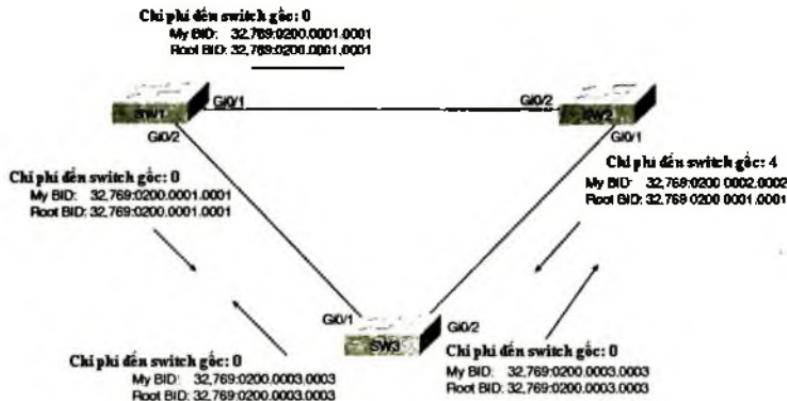
Cần quan tâm đến ba trường đầu tiên trong bảng 4.3 trong phần sau thông qua ba bước trong đó STP lựa chọn các giao tiếp để đặt vào trạng thái Forwarding State. Ké tiếp, kiểm tra ba bước chính trong tiến trình STP.

4.2.1.5. Bầu Switch gốc

Các switch bầu một switch gốc dựa trên BID trong BPDU. Switch gốc là switch với giá trị thấp nhất cho BID đó. Bởi vì hai phần BID bắt đầu với giá trị ưu tiên, lúc đó switch với độ ưu tiên thấp nhất trở thành gốc. Lấy ví dụ, nếu một switch có độ ưu tiên 100, và một switch khác có độ ưu tiên 200, thì switch có độ ưu tiên 100 thắng, tùy theo địa chỉ MAC nào được sử dụng để tạo BID cho mỗi switch/ bridge.

Nếu xảy ra xung đột với phần ưu tiên của BID, switch với phần địa chỉ MAC thấp hơn của BID sẽ là gốc. STP bầu chọn switch gốc trong ngữ cảnh không khác với bầu cử chính trị. Tiến trình bắt đầu với tất cả

switch muốn trở thành gốc. Nếu một switch nhận được một Hello với một BID thấp hơn – gọi là Superior Hello – thì switch này ngừng quảng bá nó là root và bắt đầu chuyên Superior Hello. Điều này giống như bầu cử chính trị trong đó một ứng viên ít phiếu bầu hơn sẽ bỏ cuộc và rời cuộc đua, nhường lại quyền ứng hộ cho một ứng viên khác. Hình 4.3 cho thấy việc bắt đầu của tiến trình bầu cử gốc. Trong trường hợp này, SW1 đã quảng bá chính nó là root, cho SW2 và SW3. Tuy nhiên, SW2 cho rằng SW1 là một gốc tốt hơn, vì thế nó chuyên Hello bắt nguồn từ SW1. Nó chuyên Hello BID của SW1 như là BID gốc. Tuy nhiên, SW1 và SW3 đều đang nghĩ rằng chúng là tốt nhất, vì thế chúng tiếp tục liệt kê BID của mình như là root trên Hello BPDU của nó.

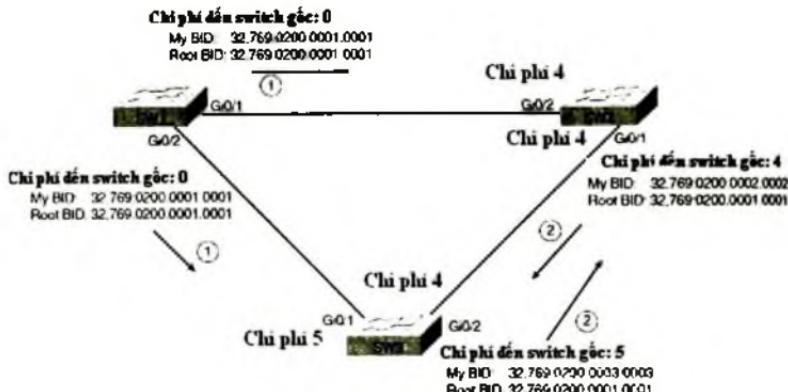


Hình 4.3. Bầu chọn root switch

Hai ứng viên sẽ tiếp tục tồn tại trên hình 4.3: SW1 và SW3. Vậy ai thắng? từ giá trị bridge ID, switch có giá trị ưu tiên thấp hơn sẽ thắng. Nếu xuất hiện xung đột, thì địa chỉ MAC thấp hơn sẽ thắng. Như trong hình vẽ 4.3, SW1 có giá trị bridge ID (32769:0200.0000.0001) thấp hơn SW3 (32769.2000.0003.0003), vì thế SW1 thắng và SW3 bây giờ xem switch sẽ là switch tốt hơn. Hình 4.4 cho thấy kết quả thông điệp Hello được gửi bởi các switch này.

Sau khi việc bầu chọn được hoàn tất, chỉ switch gốc tiếp tục tạo các thông điệp Hello BPDU. Các switch khác nhận các Hello, cập nhật

trường BID nơi gửi (và trường chi phí đến gốc) và chuyển tiếp các Hello này ra ngoài các giao tiếp khác. Hình 4.4 cho thấy yếu tố này, với SW1 gửi các Hello tại bước 1, và SW2 và SW3 chuyển tiếp một cách độc lập Hello đó ra ngoài các giao tiếp khác tại bước 2.



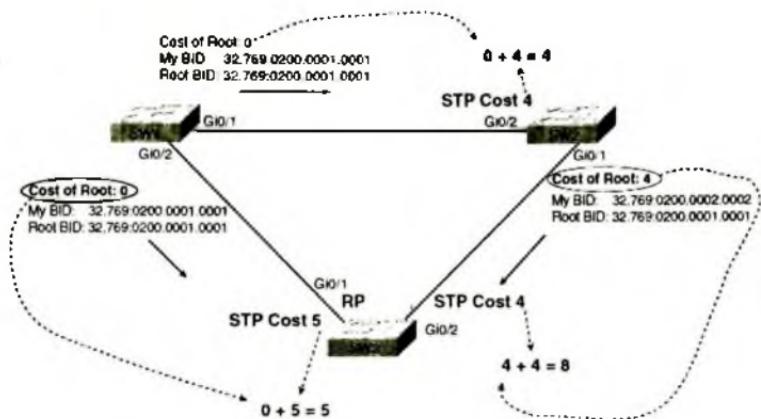
Hình 4.4. Tiến trình bầu chọn root switch (tiếp theo)

4.2.1.6. Chọn mỗi port gốc của switch khác

Phản thứ hai của tiến trình STP xảy ra khi mỗi switch không phải là gốc chọn một và chỉ một port gốc của nó. Một port gốc (RP) của switch là một giao tiếp của nó thông qua đó nó có chi phí STP thấp nhất để đến switch gốc.

Để tính toán chi phí này, một switch thêm vào chi phí được liệt kê trong một Hello nhận được với chi phí port STP được gán cho cùng giao tiếp đó. Chi phí port STP đơn giản là một giá trị nguyên được gán cho mỗi giao tiếp nhằm mục đích cung cấp một tính toán có đối tượng cho phép STP lựa chọn giao tiếp nào được thêm vào sơ đồ STP.

Hình 4.5 cho thấy một ví dụ cách SW3 tính toán chi phí của nó để đến gốc qua hai con đường có thể bằng cách thêm vào một chi phí có quảng bá (trong các thông điệp Hello) vào các chi phí giao tiếp được liệt kê trong hình.



Hình 4.5. Tiến trình bầu chọn root port

Kết quả của tiến trình được mô tả trong hình 4.5, SW3 lựa chọn giao tiếp Gi0/1 là port gốc của nó, vì chi phí để đến switch gốc thông qua port đó (5) là thấp hơn chi phí của các port khác (Gi0/2 chi phí 8). Tương tự, SW2 sẽ chọn port Gi0/2 làm port gốc, với chi phí là 4 (Chi phí quảng bá của SW1 là 0, cộng với chi phí giao tiếp SW2 là 4). Mỗi switch đặt các port gốc của mình sang trạng thái Forwarding State.

Trong các sơ đồ phức tạp hơn, việc lựa chọn port gốc sẽ không rõ ràng như thế. Phần “Xử lý sự cố STP” trong phần sau của chương cho thấy một ví dụ, trong đó việc chọn lựa port gốc yêu cầu ít công sức hơn.

4.2.1.7. Chọn port dành riêng – Designated port (DP) trên mỗi phân đoạn LAN

Bước cuối cùng của STP để chọn sơ đồ STP là chọn cổng dành riêng (Designated port - DP) trên mỗi phân đoạn LAN. Port dành riêng trên mỗi phân đoạn LAN là port của switch quảng bá Hello chi phí thấp nhất vào một phân đoạn LAN đó. Khi một switch không phải là gốc chuyển tiếp một Hello, switch gốc thiết lập trường chi phí trong Hello đó sang chi phí đến đích của switch đó. Kết quả là, switch với chi phí đến đích thấp hơn, trong số tất cả các switch có kết nối đến một phân đoạn, trở thành port dành riêng DP trên phân đoạn đó.

Ví dụ, trong hình 4.4, cả hai SW2 và SW3 chuyển tiếp các thông điệp Hello vào phân đoạn mạng này. Chú ý rằng cả hai SW2 và SW3 liệt kê các chi phí riêng của chúng để đến switch gốc (chi phí 4 trên SW2 và chi phí 5 trên SW3). Kết quả là, port Gi0/2 của SW2 là port dành riêng trên phân đoạn LAN này.

Tất cả các DP được chuyển sang trạng thái Chuyển tiếp, vì thế trong trường hợp này, giao tiếp Gi0/1 của SW2 sẽ chuyển sang trạng thái Chuyển tiếp.

Nếu chi phí quảng bá bị xung đột, các switch phá vỡ xung đột bằng cách chọn switch với chi phí bridge ID thấp hơn. Trong trường hợp này, SW2 sẽ thắng, với BID là 32769:0200.0002.0002 so với 32769:0200.0003.0003 của SW3.

Chú ý: Một switch có thể kết nối hai hay nhiều giao tiếp đến cùng một miền xung đột nếu hub được sử dụng. Trong những trường hợp như thế, một cơ chế bẻ khóa khác được thực hiện: Switch chọn giao tiếp với số giao tiếp nội bộ thấp hơn.

Chi giao tiếp không được chuyển sang trạng thái Forwarding State trên ba switch trong ví dụ được thể hiện trong các hình 4.3, 4.4, 4.5 là port Gi0/2 của SW3. Vì thế tiến trình STP bây giờ kết thúc. Bảng 4.4 liệt kê trạng thái của mỗi port và cho thấy tại sao nó lại ở trong trạng thái đó.

Bảng 4.4. Trạng thái của các port

Switch/ giao tiếp	Trạng thái	Nguyên nhân
SW1, Gi0/1	Chuyển tiếp	Giao tiếp của root switch
SW1, Gi0/2	Chuyển tiếp	Giao tiếp của root switch
SW2, Gi0/2	Chuyển tiếp	Root port
SW1, Gi0/1	Chuyển tiếp	Port dành riêng trên phân đoạn LAN đến SW3
SW3, Gi0/1	Chuyển tiếp	Root port
SW3, Gi0/2	Khóa	Không phải là root port hay port dành riêng

Chi phí cho port có thể được cấu hình, hay có thể sử dụng mặc định. Bảng 4.5 liệt kê các chi phí port mặc định được xác định bởi IEEE;

Cisco sử dụng các giá trị mặc định này. IEEE xem xét lại các giá trị ban đầu này, được thiết lập vào đầu những năm 1980, vì không tương thích với sự phát triển của Ethernet để hỗ trợ Ethernet 10 – Gigabit.

Bảng 4.5. Chi phí cho các port khác nhau

Tốc độ Ethernet	Chi phí IEEE ban đầu	Chi phí IEEE hiện tại
10Mbit/s	100	100
100Mbit/s	10	19
1Gbit/s	1	4
10Gbit/s	1	2

Với việc kích hoạt STP, tất cả các giao tiếp làm việc trên switch sẽ thiết lập sang chế độ STP Forwarding hay Blocking (thậm chí là các port truy cập). Với các giao tiếp có kết nối đến một máy tính hay router, không sử dụng STP, switch sẽ tiếp tục chuyển các Hello đến các giao tiếp này. Giả sử rằng chỉ duy nhất một thiết bị gửi một Hello đến một phân đoạn LAN, switch đang gửi Hello chi phí thấp nhất vào phân đoạn LAN đó, làm cho switch trở thành port dành riêng trên phân đoạn LAN đó. Vì thế STP đặt các giao tiếp truy cập làm việc sang trạng thái Forwarding State như là kết quả của phân port dành riêng của tiến trình STP.

4.2.1.8. Phản ứng với các thay đổi trong mạng

Sau khi sơ đồ STP – tập hợp các giao tiếp trong trạng thái chuyển tiếp – đã được xác định, tập hợp các giao tiếp chuyển tiếp này không thay đổi trừ khi sơ đồ mạng thay đổi. Phản này đánh giá hoạt động của STP khi mạng ổn định và sau đó đánh giá các STP hội tụ sang một sơ đồ mới khi một số thay đổi xảy ra.

Switch gốc gửi một Hello BPDU mới 2 giây mỗi lần theo mặc định. Mỗi switch chuyển tiếp Hello trên tất cả các port dành riêng DP, nhưng chỉ sau khi thay đổi hai mục. Chi phí được thay đổi để phù hợp với chi phí đến gốc, và trường Bridge ID của switch gửi cũng được thay đổi (trường bridge ID của root không thay đổi). Bằng cách chuyển tiếp các

Hello đã nhận (và thay đổi) ra ngoài tất cả các DP, tất cả các switch tiếp tục nhận Hello khoảng 2 giây mỗi lần. Danh sách sau tóm tắt hoạt động trạng thái ổn định khi không có gì thay đổi trong sơ đồ STP.

- Root tạo và gửi một Hello BPDUs, với chi phí là 0, ra ngoài tất cả giao tiếp làm việc của nó (các giao tiếp này trong trạng thái Forwarding State)
- Các switch không phải gốc nhận Hello trên mỗi port gốc của nó. Sau khi thay đổi Hello để liệt kê giá trị bridge ID của nó như là BID của switch gửi, và liệt kê chi phí của switch gốc, switch chuyển tiếp Hello ra ngoài tất cả các port dành riêng này.
- **Bước 1 và 2 được lặp lại cho đến khi có thay đổi xảy ra.**

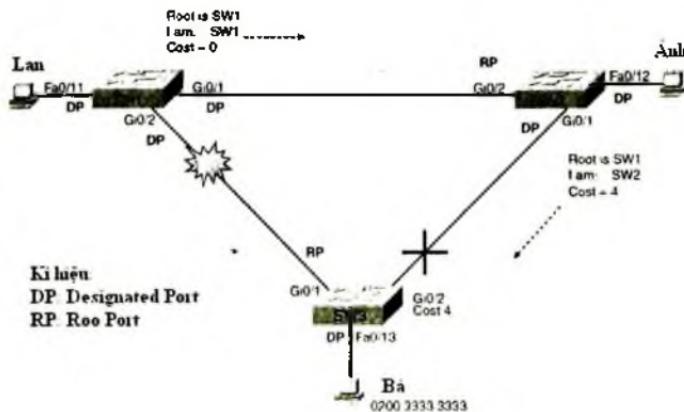
Mỗi switch dựa trên các thông điệp Hello nhận được theo chu kì từ gốc như là cách để biết được rằng con đường của nó đến root vẫn còn làm việc. Khi một switch không thể nhận các Hello, thì có sự cố đã xảy ra, vì thế các switch phản ứng lại và bắt đầu tiến trình thay đổi sơ đồ STP. Với nhiều nguyên nhân khác nhau, tiến trình hội tụ yêu cầu sử dụng ba bộ định thời. Chú ý rằng tất cả các switch sử dụng các bộ định thời này theo yêu cầu bởi switch gốc, mà root liệt kê trong các thông điệp Hello BPDU của nó. Bộ định thời và các mô tả của nó được liệt kê trong bảng 4.6.

Bảng 4.6. Các bộ định thời trong STP

Bộ định thời	Mô tả	Giá trị mặc định
Hello	Chu kì giữa các bản tin Hello được tạo bởi root switch	2 giây
MaxAge	Thời gian switch đợi, sau khi nhận Hello, trước khi thử thay đổi sơ đồ STP	10 lần Hello
Forward Delay	Độ trì hoãn ánh hưởng tiến trình xảy ra khi một giao tiếp chuyển từ trạng thái Khóa sang trạng thái Chuyển tiếp. Một port ở trong trạng thái trung gian Listening sau đó chuyển sang Learning, xác định bởi bộ định thời này	15 giây

Nếu một switch không nhận một Hello BPDU được mong đợi trong khoảng thời gian Hello, switch tiếp tục hoạt động như thông thường. Tuy nhiên, nếu Hello không xuất hiện lại trong khoảng thời gian MaxAge, switch phản ứng bằng cách thực hiện các bước để thay đổi sơ đồ STP. Lúc này, switch cần tính toán lại switch nào sẽ là switch gốc, và nếu nó không phải là switch gốc, thì port nào sẽ là port RP của nó, và port nào sẽ là DP, giả sử rằng các Hello nó thường nhận đã ngưng đến.

Cách tốt nhất để mô tả sự hội tụ STP là cho một ví dụ sử dụng cùng sơ đồ. Hình 4.6 cho thấy cùng một ví dụ tương tự, với giao tiếp SW3 trong trạng thái Blocking, nhưng giao tiếp Gi0/2 của SW1 đã bị lỗi.



Hình 4.6. Tiến trình hội tụ STP

SW3 phản ứng lại với thay đổi vì SW3 lỗi khi nhận các thông điệp Hello nó đang mong đợi trên giao tiếp Gi0/1 của nó. Tuy nhiên, SW2 không cần phải phản ứng lại vì SW2 tiếp tục nhận các thông điệp Hello định kì trên giao tiếp Gi0/2 của nó. Trong trường hợp này, SW3 phản ứng lại hoặc là khi thời gian MaxAge vượt qua mà không nghe thấy Hello nào, hay ngay khi SW3 cảnh báo rằng giao tiếp Gi0/1 đã lỗi. Nếu giao tiếp này lỗi, switch có thể giả sử rằng các Hello sẽ không đến nữa.

Bây giờ SW3 có thể phản ứng lại, nó bắt đầu bằng cách tính toán lại việc lựa chọn switch root. SW3 sẽ nhận Hello từ SW1, được chuyển tiếp

bởi SW2 và SW1 có một giá trị Bridge ID thấp hơn; hay là SW1 có thể không phải là root. Vì thế, SW3 quyết định rằng SW1 sẽ vẫn là switch tốt nhất và SW3 không phải là root.

Ké tiếp, SW3 tính toán lại chọn lựa RP của nó. Lúc này, SW3 chỉ nhận các Hello trên một giao tiếp, Gi0/2. Với bất kì chi phí được tính toán, Gi0/2 sẽ trở thành RP mới của SW3.

SW3 sau đó tính toán lại vai trò của nó như là một DP trên bất kì giao tiếp nào khác. Trong ví dụ này, không có công việc thực tế nào cần được thực thi. SW3 thực sự là DP trên giao tiếp Fa0/13, và nó tiếp tục là DP, vì không có switch nào khác kết nối đến port đó.

Khi STP hội tụ, một switch lựa chọn giao tiếp chuyển dịch từ một trạng thái này sang một trạng thái khác. Tuy nhiên, sự chuyển dịch từ trạng thái khóa sang trạng thái Chuyển tiếp không thể được thực hiện ngay tức thì bởi vì thay đổi tức thì sang chuyển tiếp có thể tạm thời làm cho các frame bị lặp. Để ngăn ngừa những vòng lặp tạm thời này, STP chuyển một giao tiếp qua hai trạng thái giao tiếp trung gian, như sau:

- **Trạng thái Lắng nghe (Listening):** Giống như trạng thái khóa, giao tiếp đó sẽ không chuyển tiếp các frame. Các mục trong bảng MAC cũ và không chính xác bây giờ đã hết hạn trong suốt giai đoạn này, vì các mục trong bảng MAC cũ không chính xác bây giờ có thể là nguyên nhân làm cho lặp tạm thời.
- **Trạng thái Học:** các giao tiếp trong trạng thái này sẽ không chuyển tiếp các frame, nhưng switch bắt đầu học các địa chỉ MAC của frame được nhận trên các giao tiếp đó.

STP chuyển một giao tiếp từ trạng thái Khóa sang trạng thái Lắng nghe, sau đó là trạng thái Học, và sau đó là trạng thái Chuyển Tiếp. STP để cho các giao tiếp trong mỗi trạng thái trung gian một khoảng thời gian bằng với thời gian trì hoãn chuyển tiếp. Kết quả là, một sự kiện hội tụ có thể là cho một giao tiếp thay đổi từ Khóa sang Chuyển Tiếp yêu cầu 30 giây để chuyển từ Khóa sang Chuyển Tiếp. Ngoài ra, một switch có thể phải đợi số giây MaxAge trước khi lựa chọn để chuyển một giao tiếp từ

trạng thái Blocking sang trạng thái Forwarding. Theo các ví dụ được thể hiện trong các hình này, SW3 có thể đợi thời gian MaxAge trước khi quyết định nó không nhận cùng các thông điệp BPDU từ cùng một gốc và trên port gốc của nó (mặc định là 20 giây), và sau đó đợi 15 giây mỗi lần trong các trạng thái lắng Nghe và Học trên giao tiếp Gi0/2, kết quả là thời gian trì hoãn trong khi hội tụ là 50 giây.

Bảng 4.7. Tóm tắt các trạng thái giao tiếp khác nhau cho STP

Trạng thái	Chuyển tiếp Frame?	Học địa chỉ MAC dựa trên frame nhận được	Trạng thái ổn định hay trung gian?
Khóa	No	No	Ôn định
Lắng nghe	No	No	Trung gian
Học	No	Yes	Trung gian
Chuyển tiếp	Yes	Yes	Ôn định
Hùy	No	No	Ôn định

4.2.2. Các chức năng tùy chọn của STP

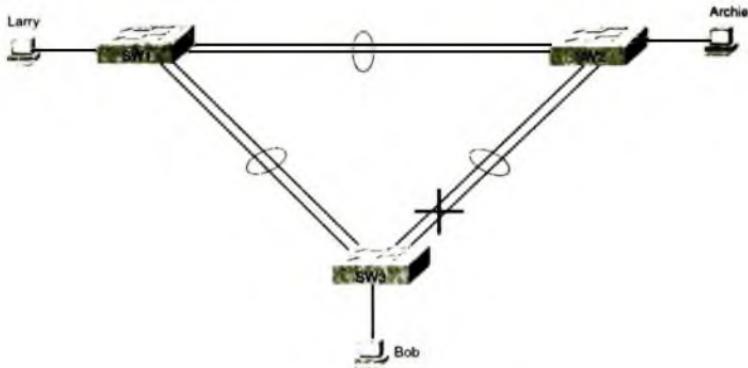
STP đã được phát triển qua hơn 20 năm. Các switch của Cisco triển khai trên chuẩn IEEE 802.1d STP, nhưng qua một số năm cải tiến, Cisco đã thêm các chức năng riêng để cải tiến STP. Trong một số trường hợp, IEEE đã thêm các cải tiến này vào hay những gì tương tự vào các chuẩn IEEE sau này, như là chuẩn 802.1d hay một chuẩn bổ sung. Phần sau đánh giá ba thuộc tính bổ sung cho STP: EtherChannel, PortFast, và BPDU Guard.

Chú ý: Nếu muốn làm việc trong một mạng LAN campus, có thể cần tìm hiểu chi tiết hơn về các chức năng STP so với nội dung giáo trình này. Để thực hiện, theo dõi hướng dẫn cấu hình phần mềm cho các switch 2960 và kiểm tra trong các chương liên quan đến STP, RSTP và các chức năng tùy chọn STP khác. Hướng dẫn trong cuốn sách này liệt kê thông tin về cách để tìm các tài liệu liên quan của Cisco.

4.2.2.1. EtherChannel

Một trong những cách tốt nhất để giảm thiểu thời gian hội tụ của STP là tránh hội tụ lẫn nhau. EtherChannel cung cấp cách để ngăn ngừa sự hội tụ STP được thực hiện khi chỉ một port hay cáp đơn hỏng xuất hiện.

EtherChannel kết hợp nhiều phân đoạn song song hay cùng tốc độ giữa cùng các cặp switch, tạo thành một EtherChannel. Các switch này xem EtherChannel như là một giao tiếp đơn cho tiến trình Chuyển tiếp frame cũng như là STP. Kết quả là, nếu một liên kết bị hỏng, nhưng ít nhất còn một liên kết là hoạt động, sự hội tụ STP không xảy ra. Lấy ví dụ, hình 4.7 cho thấy một mạng với 3 switch tương tự nhau, nhưng bây giờ với hai kết nối Gigabit Ethernet giữa mỗi cặp switch này.



Hình 4.7. Ether-Channel

Với mỗi cặp liên kết Ethernet được cấu hình như là một EtherChannel, STP xem mỗi EtherChannel là một liên kết đơn. Nói cách khác, cả hai liên kết đến cùng một switch phải bị lỗi thì mới làm cho switch hội tụ STP. Nếu không có EtherChannel, nếu có nhiều liên kết song song giữa hai switch, STP khóa tắt cả các liên kết ngoại trừ một. Với EtherChannel, tắt cả các liên kết song song có thể up và làm việc đồng thời, trong khi lại giảm thiểu số thời gian mà STP phải hội tụ, làm cho mạng có khả năng sẵn sàng tốt hơn.

EtherChannel cũng cung cấp nhiều băng thông hơn. Tất cả các trung kế trong một EtherChannel hoặc là Chuyển tiếp hay khóa, vì STP xem tất cả các trung kế trong cùng một EtherChannel là một trung kế. Khi một EtherChannel trong trạng thái Chuyển tiếp, các switch cân bằng tải trên tất cả các trung kế, cung cấp nhiều băng thông hơn.

4.2.2.2. PortFast

PortFast cho phép một switch ngay tức thì đặt một port vào trong trạng thái Chuyển tiếp khi port đó được kích hoạt vật lý, bỏ qua bất kì lựa chọn nào về sơ đồ STP và bỏ qua các trạng thái Lắng nghe và Học. Tuy nhiên, chỉ các port trên đó có thể kích hoạt một cách an toàn chức năng PortFast là các port mà trên đó biết không có bridge, switch hay các thiết bị có khả năng STP khác được kết nối.

PortFast là thích hợp nhất cho các kết nối đến các thiết bị đầu cuối người dùng, nếu kích hoạt PortFast trên các port có kết nối đến thiết bị người dùng, khi một máy tính người dùng khởi động, ngay khi NIC của PC được kích hoạt, port của switch được chuyển sang trạng thái Chuyển tiếp và chuyển tiếp lưu lượng đi. Nếu không có PortFast, mỗi port phải chờ cho đến khi một switch xác nhận rằng port đó là một DP, và sau đó đợi cho đến khi giao tiếp này được đặt vào trạng thái Lắng nghe và Học trước khi chuyển sang trạng thái Chuyển tiếp.

4.2.2.3. Bảo mật STP với BPDU Guard

Các giao tiếp của switch kết nối đến các thiết bị người dùng đầu cuối trong một LAN có các lỗ hổng bảo mật. Một kẻ tấn công có thể kết nối đến một switch trên một trong số các port này, với giá trị ưu tiên STP thấp hơn và trở thành switch root. Tương tự, bằng cách kết nối switch của kẻ tấn công với nhiều switch tương ứng, switch kẻ tấn công có thể kết thúc việc chuyển tiếp các gói tin trên LAN, và kẻ tấn công có thể sử dụng bộ phân tích giao thức LAN để sao chép lượng lớn dữ liệu được gửi qua LAN. Tương tự, người dùng có thể gây hại một cách vô tình đến LAN. Ví dụ, một người dùng có thể mua và kết nối một thiết bị LAN rẻ tiền vào một switch có sẵn, có thể tạo ra vòng lặp hay có thể làm cho một switch mới, với khả năng yếu đã trở thành root.

Chức năng Cisco BPDU Guard giúp chống lại các loại vấn đề này bằng cách hủy một port nếu bất kỳ BPDU được nhận trên port đó. Vì thế chức năng này hữu dụng cụ thể trên các port mà chỉ được sử dụng như là một port truy cập và không bao giờ được kết nối đến switch khác. Ngoài ra, chức năng BPDU Guard thường được sử dụng trên cùng giao tiếp có

chức năng PortFast được kích hoạt, vì port đã kích hoạt PortFast sẽ chắc chắn nằm trong chế độ Chuyển Tiếp, làm tăng khả năng lặp chuyền tiếp.

Chức năng Cisco BPDU Guard giúp chống lại lỗi khi có một switch mới muốn trở thành switch root. Chức năng Root Guard cho phép switch khác được kết nối đến giao tiếp đó và tham gia vào STP bằng cách gửi và nhận BPDU. Tuy nhiên, khi giao tiếp của switch đó với Root Guard được kích hoạt nhận một BPDU cao hơn từ một switch lân cận – một BPDU có giá trị BID tốt hơn/ thấp hơn – switch với chức năng Root Guard phản ứng lại. Switch này không chi bò qua BPDU cao hơn này, mà còn hủy luôn giao tiếp đó, không gửi hay nhận các frame nữa, cũng như tránh cho các BPDU cao hơn tiếp tục đến. Nếu các BPDU cao hơn ngưng đến, switch có thể bắt đầu sử dụng giao tiếp này lại.

4.2.3. STP nhanh (IEEE 802.1w)

Nhu đã đề cập phần đầu chương, IEEE định nghĩa STP trong chuẩn 802.1d. IEEE đã cải tiến giao thức 802.1d với việc định nghĩa thêm Giao thức Cây bao phủ nhanh – RSTP được định nghĩa thành chuẩn 802.1w

RSTP – 802.1w làm việc giống như STP (802.1d) trong nhiều điểm:

- Nó bao switch gốc sử dụng cùng các tham số và cơ chế giải quyết xung đột.
- Nó bao root port trên các switch không phải root với cùng các quy luật.
- Nó bao port dành riêng trên mỗi phân đoạn LAN với cùng các luật
- Nó đặt mỗi port vào trong trạng thái Chuyển tiếp hay Khóa, dù RSTP gọi đó là trạng thái Khóa hay Hủy.
- RSTP có thể được triển khai cùng với các switch 802.1d truyền thống, với các chức năng RSTP làm việc trên các switch có hỗ trợ nó, và các chức năng 802.1d truyền thống làm việc trên các switch chỉ hỗ trợ STP.

Với tất cả các tương đồng này, có thể giải thích vì sao IEEE không tạo RSTP trước. Nguyên nhân là sự hội tụ. STP tồn tại nhiều thời gian để hội tụ (50 giây theo mặc định). RSTP cải tiến sự hội tụ mạng khi sơ

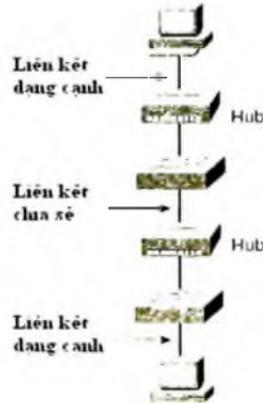
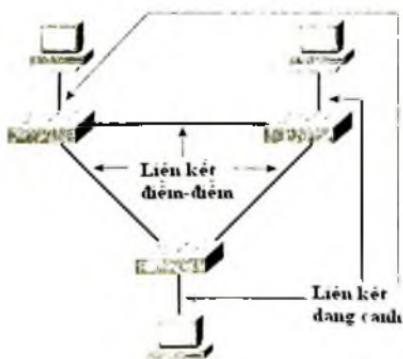
đòi thay đổi xảy ra. RSTP cải tiến hội tụ bằng cách hoặc là giới hạn hay giảm thiểu trống thấy thời gian chờ đợi mà 802.1d cần để tránh lặp trong quá trình hội tụ. 802.1d yêu cầu một thời gian chờ đợi là MaxAge (mặc định là 20 giây) trước khi phản ứng lại với một số sự kiện, trong khi RSTP chỉ đợi 3*Hello (mặc định là 6 giây). Ngoài ra RSTP hạn chế trì hoãn chuyển tiếp (mặc định là 15 giây) trong các trạng thái Lắng nghe và Chuyển tiếp. Hội tụ STP truyền thống cần thiết khoảng thời gian bằng ba lần, mà RSTP cải tiến. Ba khoảng thời gian chờ đợi (mặc định) 20, 15 và 10 giây làm cho STP hội tụ khá chậm và giảm thiểu hay hạn chế những khoảng thời gian chờ đợi này làm cho sự hội tụ RSTP xảy ra nhanh chóng hơn.

Thời gian hội tụ RSTP thường là thấp hơn 10 giây. Trong một số trường hợp, có thể thấp khoảng 1 đến 2 giây. Phần sau đây giải thích thuật ngữ và tiến trình được sử dụng bởi RSTP để vượt qua những hạn chế của 802.1d và cải tiến thời gian hội tụ.

4.2.3.1. Liên kết RSTP và các dạng Edge

RSTP xác định các loại kết nối vật lý trong một LAN thành ba dạng khác nhau như sau:

- Dạng liên kết điểm – điểm
- Dạng liên kết chia sẻ
- Dạng liên kết cạnh



Hình 4.8. Rapid STP

Hình 4.8 thể hiện hai mạng mẫu. Mạng bên trái là một thiết kế mạng ngày nay, không sử dụng hub. Tất cả các switch kết nối cáp Ethernet, và tất cả các thiết bị đầu cuối người dùng cũng kết nối đến cáp Ethernet. IEEE định nghĩa RSTP để cài tiến hội tụ trong những loại mạng này.

Trong mạng bên phải của hình, các hub vẫn được dùng để kết nối giữa các switch, cũng như cho các kết nối với thiết bị người dùng cuối. Ngày nay các mạng không còn sử dụng hub nữa. IEEE không tạo RSTP để hoạt động trong các mạng sử dụng các hub chia sẻ, và RSTP sẽ không cài tiến hội tụ trên mạng bên phải.

RSTP gọi kết nối Ethernet giữa các switch là liên kết điểm – điểm và gọi các kết nối Ethernet đến thiết bị người dùng cuối là liên kết cạnh. Hai dạng liên kết được tồn tại là: điểm – điểm, như phần bên phải trong hình 4.8 và chia sẻ, như phần bên phải trong hình này. RSTP không phân biệt giữa dạng chia sẻ và điểm – điểm cho kết nối cạnh.

RSTP giảm thiểu thời gian hội tụ cho các kết nối dạng liên kết điểm – điểm và kết nối dạng cạnh. Nó không cài tiến thời gian hội tụ qua kết nối dạng chia sẻ. Tuy nhiên, hầu hết các mạng hiện đại không sử dụng hub giữa các switch, chính vì thế sự thiếu sót cho việc cài tiến hội tụ RSTP cho dạng liên kết chia sẻ không thành vấn đề.

4.2.3.2. Trạng thái Port RSTP

Sau đây là một số thuật ngữ liên quan trạng thái port cần làm quen:

Bảng 4.8. Các trạng thái port trong RSTP

Trạng thái hoạt động	Trạng thái STP (802.1d)	Trạng thái RSTP (802.1w)	Chuyển frame dữ liệu?
Bật	Khóa	Hủy	No
Bật	Lắng nghe	Hủy	No
Bật	Học	Học	No
Bật	Chuyển tiếp	Chuyển tiếp	Yes
Tắt	Tắt	Hủy	No

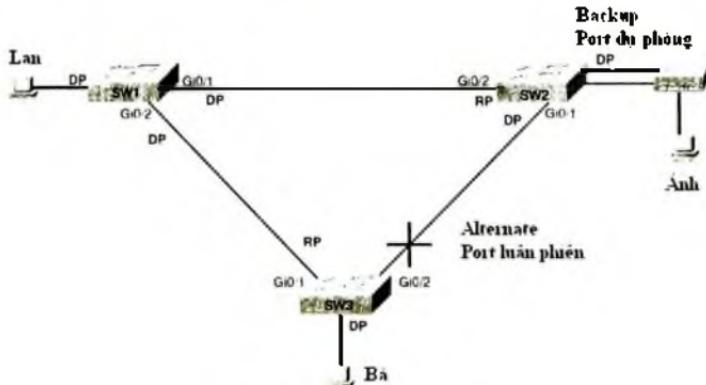
Tương tự STP, RSTP ồn định với tất cả các port hoặc là trong trạng thái Chuyển tiếp, hay trạng thái Hủy. Hủy có nghĩa là port đó không

chuyển tiếp các frame, xử lý frame nhận được hay học các địa chỉ MAC, nhưng nó có lắng nghe các BPDU. Tóm lại, nó hoạt động giống như trạng thái Khóa của STP. RSTP sử dụng một trạng thái đệm Học khi chuyển một giao tiếp từ trạng thái Hủy sang trạng thái Chuyển tiếp. Tuy nhiên, RSTP cần sử dụng trạng thái Học cho chỉ một khoảng thời gian ngắn.

4.2.4. Vai trò Port RSTP

Cả STP (802.1d) và RSTP (802.1w) sử dụng các khái niệm trạng thái port và vai trò port. Tiến trình STP xác định vai trò của mỗi giao tiếp. Lấy ví dụ, STP xác định giao tiếp này hiện tại có vai trò port root hay port dành riêng. Sau đó, STP xác định trạng thái port ỗn định để sử dụng cho các giao tiếp với các vai trò nhất định: trạng thái Chuyển tiếp cho các port RP và DP, trạng thái khóa cho các port khác.

RSTP thêm ba vai trò port khác vào, hai trong số đó được thể hiện trong hình 4.9 (vai trò port thứ ba, disabled) không được thể hiện trong hình, nó đơn giản được ám chỉ như là các giao tiếp đã tắt.



Hình 4.9. Port RSTP

Vai trò port khác của RSTP xác định một port luân phiên tốt nhất cho RP hiện tại của switch đó. Tóm lại, vai trò port luân phiên là một RP luân phiên. Lấy ví dụ, SW3 liệt kê Gi0/1 là RP của nó, nhưng SW3 cũng biết rằng nó nhận các Hello BPDU từ giao tiếp Gi0/2. Switch SW3 có

một port gốc, như là STP. RSTP dành riêng các port nhận các BPDU gần tối ưu (các BPDU không tốt như là các BPDU nhận trên các port root) là các port luân phiên. Nếu SW3 ngừng nhận các Hello từ bridge gốc, RSTP trên SW3 chọn port luân phiên tốt nhất như là port gốc mới của nó để bắt đầu tăng tốc tiến trình hội tụ.

Loại port RSTP mới khác, gọi là port dự phòng, áp dụng chỉ cho một switch đơn có hai liên kết đến cùng một phân đoạn (miền xung đột). Để có hai liên kết đến cùng miền xung đột, switch phải được kết nối đến một hub, được thể hiện trong hình 4.9 mà không có SW2. Trong hình này, switch SW2 đặt một trong hai port vào vai trò port dành riêng (hoặc là sang chế độ Chuyển tiếp) và giao tiếp khác sang vai trò dự phòng (hoặc là sang chế độ Hủy). SW2 chuyển tiếp các BPDU ra ngoài port trong chế độ Chuyển tiếp và nhận cùng BPDU quay ngược lại trên port ở chế độ Hủy. Vì thế SW2 biết nó có thêm một kết nối bổ sung đến phân đoạn đó, được gọi là port dự phòng. Nếu port DP cho trạng thái Chuyển tiếp lỗi, SW2 có thể nhanh chóng chuyển port dự phòng đó từ chế độ Hủy sang chế độ Học Hồi và sau đó là chế độ Chuyển tiếp.

Bảng 4.9. Các port trong RSTP

Vai trò RSTP	Vai trò STP	Định nghĩa
Root port	Root port	Một port đơn trên mỗi switch không phải là root trong đó switch lắng nghe BPDU tốt nhất chuyển ra trên tất cả BPDU được nhận
Port dành riêng	Port dành riêng	Của tất cả switch trên tất cả các switch kết nối đến cùng miền xung đột, port quảng bá BPDU tối ưu
Alternate port	-	Port trên switch nhận một BPDU tối ưu thấp hơn
Backup port	-	Port bị hủy hay nó không thể làm việc vì các nguyên nhân khác
Tắt	-	Một port bị tắt hay không thể làm việc vì nguyên nhân khác

4.2.4.1. Sự hội tụ RSTP

Phản này của RSTP được bắt đầu bằng cách so sánh sự giống nhau giữa RSTP và STP: cách thức cả hai lựa chọn một root sử dụng cùng các quy luật, lựa chọn các port dành riêng, v.v. Nếu RSTP giống như STP thì không cần thiết phải nâng cấp phiên bản 802.1d thành chuẩn mới 802.1w RSTP. Nguyên nhân chính cho tiêu chuẩn mới được cải tiến là cải tiến thời gian hội tụ.

Giải thuật cây bao phủ RSTP làm việc khác một ít so với phiên bản trước đó. Ví dụ, trong điều kiện ổn định, mọi switch độc lập tạo và gửi các thông điệp Hello BPDUs, hơn là chỉ thay đổi và chuyển tiếp các Hello được gửi bởi switch gốc. Tuy nhiên, trong các điều kiện ổn định, các kết quả cuối cùng là giống nhau: Một switch tiếp tục lắng nghe cùng các Hello, với cùng chi phí và giá trị BID switch gốc được liệt kê, bỏ qua sơ đồ STP.

Các thay đổi chính với phiên bản RSTP so với STP khi thay đổi xuất hiện với mạng. RSTP hoạt động khác nhau trên một số giao tiếp dựa trên các đặc tính của RSTP của giao tiếp đó dựa trên những gì được kết nối đến giao tiếp này.

4.2.4.2. Liên kết dạng cạnh và PortFast

RSTP cải tiến hội tụ cho các kết nối dạng cạnh bằng cách ngay tức thì đặt port đó vào chế độ Chuyển tiếp khi một liên kết được kích hoạt về mặt vật lý. Kết quả là, RSTP xem những port này giống như chức năng PortFast của riêng Cisco. Sự thực là trong các switch Cisco, để kích hoạt chức năng RSTP trên các giao tiếp cạnh, đơn giản cấu hình PortFast.

4.2.4.3. Liên kết dạng chia sẻ

RSTP không thực hiện điều gì khác với STP trên các liên kết dạng chia sẻ. Tuy nhiên, bởi vì hầu hết các liên kết giữa các switch ngày nay không được chia sẻ, nhưng thường được kết nối song công điểm - điểm, cho nên điều đó trở nên không quan trọng.

4.2.4.4. Liên kết dạng điểm - điểm

RSTP cải tiến hội tụ qua các liên kết song công giữa các switch – liên kết mà RSTP gọi là liên kết dạng điểm – điểm. Cải tiến đầu tiên được thực hiện bởi RSTP qua những loại liên kết này liên quan đến các STP sử dụng tham số MaxAge. STP yêu cầu rằng một switch khi không nhận các Hello BPDU từ switch gốc nữa phải đợi cho hết thời gian số giây MaxAge trước khi bắt đầu hội tụ. MaxAge mặc định là 20 giây. RSTP nhận thấy việc mất con đường đến bridge gốc, thông qua port root của nó, vào khoảng 3 lần thời gian của Hello, hay 6 giây, với một bộ định thời Hello mặc định có giá trị 2 giây. Vì thế, RSTP nhận thấy một con đường đến gốc bị mất nhanh chóng hơn.

RSTP gỡ bỏ sự cần thiết cho các trạng thái Lắng Nghe và giảm thiểu thời gian được yêu cầu cho trạng thái Lắng nghe bằng cách khám phá chủ động trạng thái mạng mới. STP chờ đợi một cách thụ động các BPDU mới và phản ứng lại với chúng trong suốt chế độ Lắng nghe và Học Hỏi. Với RSTP, các switch thỏa thuận với switch lân cận bằng cách gửi các thông điệp RSTP. Các thông điệp cho phép các switch nhanh chóng xác định liệu một giao tiếp có thể được dịch chuyển tức thời sang trạng thái Chuyển tiếp hay không. Trong nhiều trường hợp, tiến trình đó chỉ tốn một hay hai giây cho toàn thể miền RSTP.

4.2.4.5. Một ví dụ về khả năng tốc độ trong hội tụ RSTP

Ví dụ sau đây cho hiểu rõ hơn về tiến trình làm việc này thông qua hình vẽ 4.10 giải thích sự hội tụ RSTP.



Hình 4.10. Hội tụ RSTP

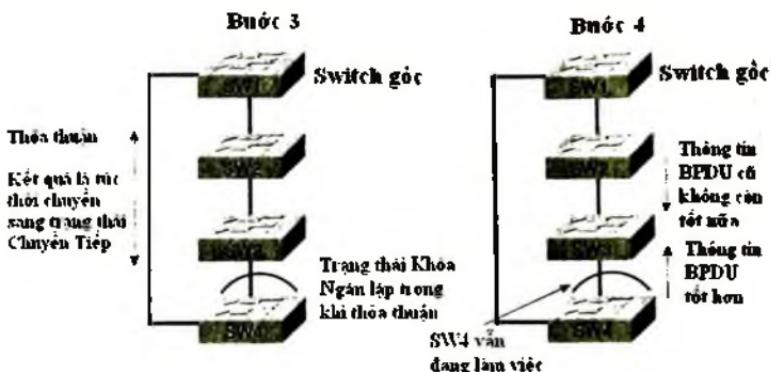
Hình 4.10 cho thấy vẫn đề được xảy ra. Bên trái, trong bước 1, mạng không có liên kết dự phòng nào. RSTP đặt tất cả các liên kết dạng diêm – diêm sang chế độ Chuyển tiếp. Đề thêm dự phòng, cần thêm các liên kết diêm – diêm khác vào giữa SW1 và SW4, được thể hiện như hình bên phải tại bước 2. Vì thế, hội tụ RSTP xảy ra.

Bước đầu tiên của hội tụ xảy ra khi SW4 nhận thấy rằng nó đang nhận một BPDU tốt hơn đến từ SW3. Vì cả hai giá trị BPDU mới và cũ quảng bá cùng một switch, nên SW1, có giá trị BPDU mới, tốt hơn đến từ liên kết trực tiếp từ SW1 phải tốt hơn vì giá trị của nó tốt hơn. Vì nguyên nhân này, SW4 cần chuyển sang chế độ Chuyển tiếp trên liên kết mới đến SW1, vì nó bây giờ là port gốc của SW4.

Lúc này, RSTP hoạt động khác với STP. RSTP trên SW4 lúc này tạm thời khóa tất cả các liên kết khác. Bằng cách làm như vậy, SW4 ngăn vòng lặp có thể xảy ra. Sau đó SW4 thỏa thuận với các switch lân cận của nó về cổng gốc mới này, SW1 sử dụng các thông điệp thỏa thuận RSTP. Kết quả là, SW4 và SW1 đồng ý rằng chúng có thể đặt mỗi phần cuối của liên kết mới này sang chế độ Chuyển tiếp ngay tức thì. Hình 4.11 cho thấy bước thứ ba này.

Tại sao SW1 và SW4 có thể đặt các đầu cuối của liên kết mới này vào chế độ Chuyển tiếp mà không gây ra lặp? Vì SW4 khóa tất cả các port dạng liên kết khác. Nói cách khác, nó khóa trên tất cả các port khác có kết nối đến các switch khác. Đó là điểm cốt lõi để tìm hiểu về sự hội tụ RSTP. Một switch biết nó cần thay đổi sang một root port mới. Nó khóa trên tất cả các liên kết khác và sau đó thỏa thuận để chuyển port root này sang chế độ Chuyển tiếp. SW4 sau đó báo với SW1 rằng tin cậy nó và bắt đầu chuyển tiếp, vì SW4 cam kết khóa trên tất cả các port khác cho đến khi nó chắc chắn nó có thể chuyển một trong số chúng sang trạng thái Chuyển tiếp lại.

Tiến trình này chưa hoàn tất, tuy nhiên, sơ đồ RSTP cho thấy SW4 bị khóa, mà trong ví dụ này không phải là kết thúc, tức là sơ đồ tốt nhất.



Hình 4.11. Tiến trình hội tụ RSTP

SW4 và SW3 lặp lại cùng tiến trình mà SW1 và SW4 vừa thực hiện. Trong bước 4, SW4 vẫn tiếp tục khóa, để ngăn lặp xảy ra. Tuy nhiên, SW4 chuyển tiếp các BPDU root mới đến SW3, vì thế SW3 bây giờ lắng nghe trên hai BPDU. Trong ví dụ này, giả sử rằng SW4 nghĩ rằng BPDU từ SW4 tốt hơn từ SW2; điều này làm cho SW3 lặp lại cùng tiến trình mà SW4 vừa thực hiện. Nó tuân theo luồng công việc chung từ thời điểm này.

- SW3 quyết định thay đổi port root của nó dựa trên BPDU mới này từ SW4.

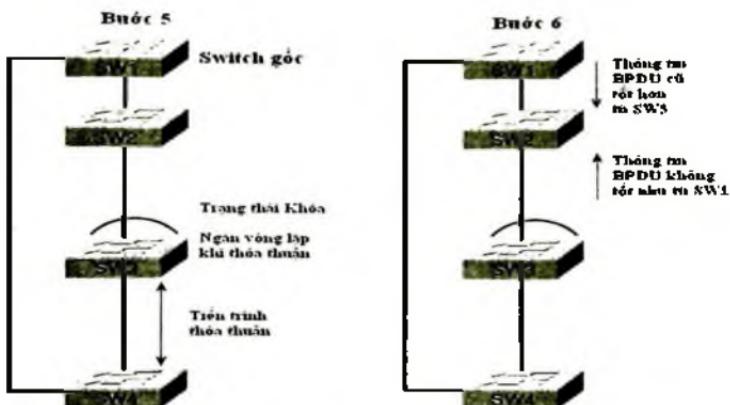
- SW3 khóa tất cả các port dạng liên kết khác (RSTP gọi tiến trình này là đồng bộ hóa).

- SW3 và SW4 thỏa thuận.

Kết quả của tiến trình thỏa thuận, SW3 và SW4 có thể chuyển sang chế độ chuyển tiếp trên các giao tiếp trên các liên kết điểm điểm.

SW3 duy trì trạng thái Khóa trên tất cả các port dạng liên kết khác cho đến khi bước kế tiếp diễn ra.

Hình 4.12 cho thấy một số bước này trong phần bước 5 bên trái và kết quả cuối cùng trong bước 6 bên phải.



Hình 4.12. Tiến trình hội tụ RSTP (tiếp theo)

SW3 vẫn khóa trên các giao tiếp cao hơn tại thời điểm này. Chú ý rằng SW2 bây giờ đang nhận hai BPDUs, nhưng cùng BPDUs cũ nó đang nhận là vẫn có giá trị BPDUs tốt hơn. Vì thế SW2 không làm gì cả. Và RSTP kết thúc sự hội tụ này.

4.3. CÁU HÌNH VÀ XÁC NHẬN STP

Theo mặc định các switch của Cisco sử dụng STP (IEEE 802.1d). Có thể dùng một vài switch và kết nối chúng với cáp Ethernet theo sơ đồ dự phòng, khi đó STP sẽ đảm bảo không có lặp tồn tại. Hệ thống hoạt động mà không cần phải nghĩ đến việc thay đổi bất kì thiết lập nào.

Dù STP làm việc mà không cần cấu hình, nhà thiết kế biết cách STP làm việc, hiểu cách dịch các câu lệnh có liên quan đến STP, và biết cách điều chỉnh STP bằng cách cấu hình các tham số khác nhau. Ví dụ, theo mặc định tất cả các switch sử dụng cùng độ ưu tiên, vì thế switch với giá trị MAC address thấp nhất được tạo sẵn sẽ trở thành root. Thay vào đó, có thể được cấu hình với độ ưu tiên thấp hơn, để luôn biết được switch nào là root, giả sử rằng switch đó là up và đang chạy.

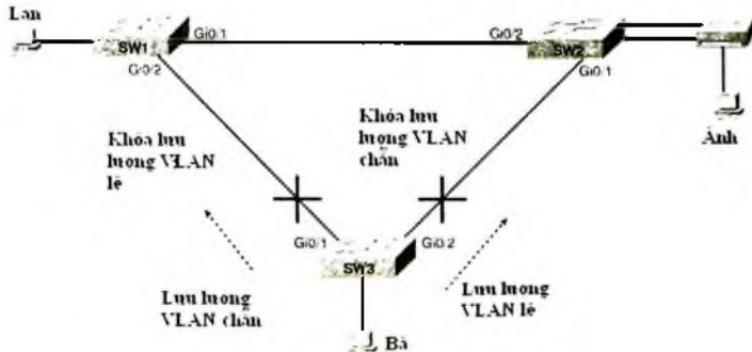
Phản sau bắt đầu bằng việc thảo luận nhiều tham số khác nhau cho cân bằng tải lưu lượng bằng cách sử dụng nhiều thể hiện của STP, sau đó là mô tả cách cấu hình STP để tận dụng các thể hiện này của STP. Phần còn lại của những phần này cho thấy các ví dụ cấu hình khác nhau cho cả STP và RSTP.

4.3.1. Đa thể hiện cho STP

Khi IEEE chuẩn hóa STP, VLAN chưa tồn tại. Khi VLAN được chuẩn hóa sau đó, IEEE không định nghĩa bất kì tiêu chuẩn nào cho phép nhiều hơn một thể hiện của STP, thậm chí với nhiều VLAN. Tại thời điểm đó, nếu một switch chỉ tuân theo các tiêu chuẩn IEEE, switch được áp dụng một thể hiện của STP trên tất cả các VLAN. Nói cách khác, nếu một giao tiếp đang chuyển tiếp, nó cũng như vậy cho tất cả các VLAN, và khi nó bị khóa, nó cũng làm như vậy cho tất cả VLAN đó.

Mặc định, các switch của Cisco sử dụng IEEE 802.1d, chứ không phải là RSTP (802.11w), với chức năng của riêng Cisco được gọi là Per-VLAN Spanning Tree Plus (PVST+). PVST+ (thường gọi tắt là PVST) tạo một thể hiện khác của STP cho mỗi VLAN. Vì thế trước khi xem xét các tham số STP có thể điều chỉnh, cần kiến thức cơ bản về PVST+, bởi vì các thiết lập cấu hình có thể khác nhau cho mỗi thể hiện của STP.

PVST+ cung cấp cho công cụ cân bằng tải. Bằng cách thay đổi một số tham số cấu hình STP trong các VLAN khác nhau, có thể làm cho các switch này lấy các RP và DP khác nhau trên các VLAN khác nhau. Kết quả là, một số lưu lượng trên một số VLAN có thể được chuyển tiếp qua một trung kế, và lưu lượng cho các VLAN khác được chuyển tiếp qua một trung kế khác. Hình 4.13 cho thấy ý tưởng cơ bản, với SW3 chuyển tiếp lưu lượng VLAN số chẵn qua trung kế bên trái (Gi0/2) và các VLAN số lẻ qua trung kế bên phải (Gi0/2).



Hình 4.13. Đa thể hiện STP

Sau đó, khi IEEE giới thiệu 802.1w RSTP, IEEE không có một chuẩn nào cho việc sử dụng đa thể hiện của STP. Vì thế, Cisco đã triển khai một giải pháp riêng khác để hỗ trợ một VLAN trên mỗi cây bao phủ RSTP. Cisco đã gọi nó là Rapid Per – VLAN Spanning Tree (RPVST) và Per – VLAN Rapid Spanning Tree (PVRST). Dù khác nhau nhưng ý tưởng vẫn chỉ là PVST+, nhưng được áp dụng cho RSTP: một thể hiện của RSTP điều khiển mỗi VLAN. Vì thế không chỉ có hội tụ nhanh hơn mà còn có khả năng cân bằng tải như trong hình 4.13.

Sau đó, IEEE tạo một tham số được chuẩn hóa cho nhiều cây bao phủ. Chuẩn IEEE (802.1s) được gọi là Multiple Spanning Trees (MST), hay nhiều thể hiện của Spanning Tree (MIST). MIST cho phép định nghĩa nhiều thể hiện của RSTP với mỗi VLAN có liên quan với một thể hiện cụ thể. Ví dụ, để có khả năng cân bằng tải như trong hình 4.13, MIST sẽ tạo hai thể hiện của RSTP: Một cho các VLAN số chẵn và một cho các VLAN số lẻ. Nếu có 100 VLAN, các switch sẽ vẫn chỉ có hai thể hiện của RSTP, thay vì 100 thể hiện được sử dụng bởi PVRST. Tuy nhiên, MIST yêu cầu cấu hình nhiều hơn trên mỗi switch, chủ yếu để xác định các thể hiện RSTP và liên hệ mỗi VLAN với một thể hiện STP.

Bảng 4.10. Các chế độ đa thể hiện STP

Loại	Hỗ trợ STP	Hỗ trợ RSTP	Công sức cấu hình	Chỉ một thể hiện được yêu cầu cho mỗi tuyến dự phòng
PVST+	Yes	No	ít	No
PVRST	No	Yes	ít	No
MIST	No	Yes	Trung bình	Yes

4.3.2. Cấu hình các tham số ảnh hưởng đến sơ đồ cây bao phủ

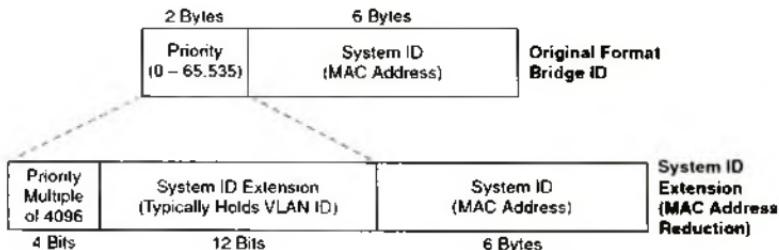
Tùy theo đó là PVST+, PVRST hay MIST được sử dụng, hai tham số cấu hình chính có thể được dùng để lấy được hiệu quả cân bằng tải như mô tả trong hình 4.13: Bridge ID và port cost. Những tham số này ảnh hưởng đến mỗi sơ đồ mạng VLAN STP như sau:

- Các giá trị Bridge ID ảnh hưởng đến việc chọn lựa switch gốc, và các switch không phải root, việc lựa chọn port của nó.
- Mỗi chi phí giao tiếp (mỗi VLAN) để đến root đó, ảnh hưởng đến việc lựa chọn cổng dành riêng trên mỗi phân đoạn LAN này.

Phản sau chỉ ra một vài chi tiết cụ thể cho việc triển khai STP trên các switch Cisco, với các khái niệm chung đã được xem xét trong phần trước của chương này.

4.3.2.1. Bridge ID và System ID

Như đã đề cập trước đây, một switch với BID được tạo thành bằng việc kết hợp trường ưu tiên 2 Byte của switch đó và địa chỉ MAC 6 Byte. Trong thực tế, các switch của Cisco sử dụng một trường BID chi tiết hơn phân tách độ ưu tiên thành hai phần. Hình 4.14 cho thấy định dạng chi tiết này, với trường ưu tiên 16-bit bây giờ bao gồm một trường con 12-bit được gọi là System ID extension.



Hình 4.14. Định dạng BID

Để xây dựng một BID của một switch cho một thể hiện cụ thể của mỗi VLAN STP, switch phải sử dụng một thiết lập ưu tiên cơ sở với giá trị bội số của 4096. ($4096 = 2^{12}$). Để tạo 16 bit đầu tiên của BID đó cho một VLAN cụ thể, switch bắt đầu với phiên bản 16 bit của trường ưu tiên cơ sở, với tất cả các bit là không trong 12 kí số cuối cùng. Switch sau đó thêm vào giá trị ưu tiên cơ sở của nó trường VLAN ID. Kết quả là 12 bit thứ tự thấp của trường ưu tiên nguyên thủy liệt kê giá trị của VLAN ID.

Một tốt của việc sử dụng system ID là PVST+ khi sử dụng một giá trị BID khác trên mỗi VLAN. Lấy ví dụ, một switch được cấu hình với VLAN1 đến 4, với giá trị ưu tiên cơ sở là 32,768, có giá trị ưu tiên STP mặc định là 32,769 trong VLAN 1, 32,770 trong VLAN 2 và 32,771 trong VLAN 3...

4.3.2.2. Chi phí port mỗi VLAN

Mỗi giao tiếp switch mặc định chi phí mỗi STP VLAN với các giá trị được thể hiện trước đây trong bảng 4.11 khi xem xét giá trị chi phí IEEE. Trên các switch Cisco, chi phí STP được dựa trên tốc độ thực sự của giao tiếp đó, vì thế nếu một giao tiếp thỏa thuận sử dụng một tốc độ thấp hơn, chi phí STP mặc định đó thể hiện tốt độ thấp hơn mỗi bảng 4.11. Nếu giao tiếp đó thỏa thuận để sử dụng một tốc độ khác, switch đó cũng tự động thay đổi chi phí port STP.

Mặc khác, chi phí port của mỗi switch có thể cấu hình, hoặc là cho tất cả các VLAN hay cho một VLAN tại một thời điểm. Sau khi được cấu hình xong, switch bỏ qua tốc độ được thỏa thuận trên giao tiếp đó, thay vì sử dụng chi phí được cấu hình.

4.3.2.3. Tóm tắt tham số cấu hình STP

Bảng 4.11 tóm tắt các thiết lập mặc định cho cả hai BID và các chi phí port, cũng như liệt kê các lệnh cấu hình tùy chọn được xem xét trong chương này.

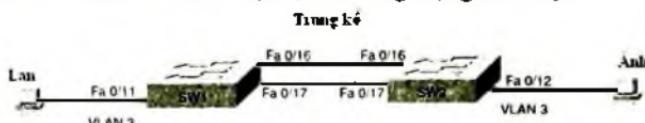
Bảng 4.11 Tóm tắt tham số cấu hình STP

Thiết lập	Mặc định	Lệnh để thay đổi mặc định
Bridge ID	- Ưu tiên: 32.768 + VLAN ID - Hệ thống: Một MAC có sẵn trên switch	Spanning-tree vlan vlan-id root {primary secondary} Spanning-tree vlan vlan-id priority priority
Interface cost	100-10Mbit/s; 19-100 Mbit/s; 4 - 1Gbit/s; 2 - 10Gbit/s	Spanning-tree vlan vlan-id cost cost
PortFast	Không bật	Spanning-tree portfast
BPDU Guard	Không bật	Spanning-tree bpduguard enable

Kế tiếp, phần cấu hình cho thấy cách kiểm tra hoạt động của STP trong một mạng đơn giản, cùng với cách thay đổi những thiết lập tùy chọn này.

4.3.2.4. Xác nhận hoạt động mặc định STP

Các ví dụ sau được thực hiện từ một mạng nhỏ với hai switch, được thể hiện trong hình 4.15. Trong mạng này, sử dụng các thiết lập mặc định, tất cả các giao tiếp sẽ chuyển tiếp ngoại trừ một giao tiếp trên một switch trên các liên kết kết nối đến switch. Ví dụ 4.1 liệt kê nhiều câu lệnh show. Phần văn bản sau ví dụ giải thích cách lệnh show thể hiện chi tiết cho sơ đồ STP được tạo ra trong mạng nhỏ này.



Hình 4.15. Ví dụ về hoạt động STP

Video 4.1:

```

SW1#show spanning-tree vlan 3

VLAN0003
  Spanning tree enabled protocol ieee
  Root ID  Priority  32771
            Address  0019.e859.5380
            Cost       19
            Port      16 (FastEthernet0/16)
            Hello time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID Priority  32771  (priority 32768 sys-id-ekt 3)
  Address  0019.e859.6f80
  Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
  Aging Time 300

  Interface      Role Sts Cost      Prio.Nbr Type
  Fa0/11        Desg Fwd 19        128.11  P2p
  Fa0/16        Root Fwd 19        128.16  P2p
  Fa0/17        Altn Blk 19        128.17  P2p

SW1#show spanning-tree root

          Root      Hello Max Fwd
Vlan      Root ID      Cost      Time Age Dly  Root Port
          32769 0019.e859.5380  19      2 20 15  Fa0/16
VLAN0002  32770 0019.e859.5380  19      2 20 15  Fa0/16
VLAN0003  32771 0019.e859.5380  19      2 20 15  Fa0/16
VLAN0004  32772 0019.e859.5380  19      2 20 15  Fa0/16
! The next command supplies the same information as the show spanning-tree vlan 3
! command about the local switch, but in slightly briefer format
SW1#show span vlan 3 bridge

          Hello Max Fwd
Vlan      Bridge ID      Time Age Dly  Protocol
          32771 (32768. 31 0019.e859.6f80  2 20 15  IEEE
VLAN0003

```

Ví dụ 4.1 bắt đầu với đầu ra của câu lệnh “show spanning-tree vlan 3” trên SW1. Lệnh đầu tiên thể hiện ba nhóm thông điệp chính: một nhóm thông điệp về switch root, được theo sau bởi một nhóm khác về switch cục bộ, và kết thúc với vai trò và trạng thái thông tin giao tiếp. Bằng cách so sánh root ID và bridge ID trong các nhóm thông điệp đầu tiên, có thể biết liệu switch nội bộ có phải là root vì bridge ID và root ID sẽ là giống nhau. Trong ví dụ này, switch nội bộ (SW1) không phải là root.

Nhóm thông điệp thứ ba trong đầu ra lệnh “show spanning-tree vlan 3” xác định phần sơ đồ STP trong ví dụ này bằng cách liệt kê tất cả các giao tiếp trong VLAN (cả các giao tiếp truy cập và trung kế có thể hỗ trợ VLAN), các vai trò port STP của nó, và các trạng thái port STP của nó. Ví dụ, SW1 xác định rằng Fa0/11 đóng vai trò port dành riêng bởi vì không có switch nào khác cạnh tranh để trở thành DP trên port đó, được thể hiện với vai trò “desg” trên đầu ra lệnh. Chính vì thế, SW1 phải quảng bá Hello chi phí thấp nhất trên phân đoạn đó. Kết quả là SW1 đặt Fa0/11 vào trạng thái Chuyển tiếp.

Khi kết quả của lệnh thể hiện rằng SW1 chọn giao tiếp Fa0/16 là RP của nó, mục đích của SW1 khi thực hiện lựa chọn này không khác với đầu ra của lệnh. SW1 nhận các Hello BPDUs từ SW2 trên các port Fast Ethernet 0/16 và 0/17, đều từ SW2. Vì cả Fa0/16 và Fa0/17 mặc định cùng chi phí port, đường đến root của SW1 là giống nhau qua cả hai con đường này. Khi một switch xung đột thì tùy theo chi phí đến switch gốc, switch trước tiên sử dụng độ ưu tiên port của giao tiếp đó để giải quyết xung đột. Nếu các giá trị ưu tiên xung đột, switch sử dụng chi số giao tiếp bên trong thấp nhất. Độ ưu tiên của giao tiếp và chi số port nội bộ được liệt kê trong tiêu đề “Prio.Nbr” trong ví dụ 4.1. Trong trường hợp này, SW1 đang sử dụng độ ưu tiên port mặc định là 128 trên mỗi giao tiếp, vì thế SW1 sử dụng chi số port thấp hơn, Fa0/16, làm root port, chính vì thế nó đặt Fa0/16 vào chế độ Chuyển tiếp.

Chú ý rằng đầu ra lệnh thể hiện rằng Fa0/17 đóng vai trò port root thay thế, được thể hiện với từ viết tắt Altn trong đầu ra của lệnh đó. Trong khi vai trò port thay thế là một khái niệm của RSTP, việc triển khai 802.1d STP cũng sử dụng khái niệm này, vì thế lệnh “show” thể

hiện vai trò port thay thế đó. Tuy nhiên, vì port này hoặc là RP hoặc là DP, SW1 đặt port này vào chế độ Khóa.

Lệnh kê trong ví dụ này, “show spanning – tree root”, liệt kê Bridge ID của switch root trên mỗi VLAN. Chú ý rằng cả hai switch đang sử dụng tất cả thiết lập mặc định, vì thế SW2 trở thành root cho tất cả bốn mạng VLAN có sẵn này. Lệnh này cũng liệt kê phần ưu tiên của bridge ID riêng biệt, thể hiện các giá trị ưu tiên khác nhau (32,769, 31,770, 32,771 và 32,772) dựa trên trường System ID mở rộng được giải thích trước đây trong chương. Lệnh cuối cùng trong ví dụ này “show spanning – tree vlan 3 bridge id” đơn giản liệt kê thông tin bridge ID của switch nội bộ trong VLAN 3.

4.3.3. Cấu hình chi phí port STP và độ ưu tiên của Switch

Ví dụ 4.2 cho thấy cách tác động đến sơ đồ STP bằng cách cấu hình chi phí port và độ ưu tiên của switch. Trước tiên, trên SW1, chi phí port được làm thấp ở Fastatetherne 0/17, làm cho con đường đến root của SW1 qua Fa0/17 tốt hơn con đường qua Fa0/16, chính vì thế thay đổi root port của SW1. Theo đó, ví dụ này cho thấy SW1 trở thành switch root bằng cách thay đổi độ ưu tiên bridge của SW1.

Ví dụ 4.2:

```

S7#debug spanning-tree events
Spanning tree event debugging is on
S7#configure terminal
Enter configuration commands, one per line. End with CNTL-Z.
S7(config)#interface Fa0/17
S7(config-if)#spanning-tree vlan 3 cost 2
00:45:39: STP: VLAN0003 new root port Fa0/17, cost 2
00:45:39: STP: VLAN0003 Fa0/17 -> listening
00:45:39: STP: VLAN0003 send Topology Change Notice on Fa0/17
00:45:39: STP: VLAN0003 Fa0/16 -> blocking
00:45:34: STP: VLAN0003 Fa0/17 -> learning
00:46:09: STP: VLAN0003 send Topology Change Notice on Fa0/17
00:46:09: STP: VLAN0003 Fa0/17 -> forwarding
S7(config-if)#Z
S7#show spanning-tree vlan 3

VLAN0003
  Spanning tree enabled protocol IEEE802.1D
  Root ID    Priority  32769
              Address   0019.6659.5388
              Cost       2
              Port      17 (FastEthernet0/17)
              Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

```

```

Bridge ID Priority 32771 (Priority 32768 sys-id-ext 3)
Address 0019.4f6a.4f80
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 15

Interface Role Sts Cost Prio.Nbr Type
-----+-----+-----+-----+-----+-----+-----+
Fa0/11 Desg FWD 19 128.11 P2p
Fa0/16 Alt BLK 18 128.16 P2p
Fa0/17 Root FWD 2 128.17 P2p
SW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#spanning-tree vlan 3 root primary
00:48:58: Setting bridge id 10 (which=1) prio 24578 prio cfg 24576 sysid 3
  (on id 0003.0019.4f6a.4f80
00:48:58: STP: VLAN0003 we are the spanning tree root
00:48:58: STP: VLAN0003 Fa0/16 -> listening
00:48:58: STP: VLAN0003 Topology Change rcvd on Fa0/16
00:47:13: STP: VLAN0003 Fa0/18 -> learning
00:47:28: STP: VLAN0003 Fa0/18 -> forwarding

```

Ví dụ này bắt đầu với lệnh “debug spanning – tree events” trên SW1. Lệnh này báo cho switch cách giải quyết các thông điệp ghi nhận thông tin nhật ký bắt kí khi nào STP thực hiện các thay đổi với vai trò hay trạng thái của một switch. Những thông điệp này thể hiện trong ví dụ như là kết quả của các câu lệnh được thể hiện trước đây trong đầu ra của ví dụ này.

Kế tiếp, chi phí port của giao tiếp Fastatethernet 0/17 của SW1, trên chi VLAN 3, được thay đổi sử dụng lệnh “spanning – tree vlan 3 cost 2” trong chế độ cấu hình giao tiếp Fa0/17. Theo kết quả lệnh này, SW1 thể hiện các thông điệp debug có ý nghĩa. Những thông điệp này cơ bản thể hiện rằng Fa0/17 bây giờ là root port – RP của SW1, rằng Fa0/16 chuyên dịch tức thì sang trạng thái Khóa, và Fa0/17 chuyên dịch chậm chạp sang trạng thái Chuyển tiếp bằng cách trước tiên đi qua các trạng thái Lắng nghe và Học Hồi. Có thể thấy thời gian ước lượng vào khoảng 15 giây (mỗi thiết lập tri hoãn chuyển tiếp mặc định) trên cả hai chế độ Học Hồi và Lắng nghe như được thể hiện trong nhãn thời gian cố định hình trong ví dụ này.

Chú ý: Hầu hết lệnh cấu hình cho thiết lập các thông số STP có thể ảnh hưởng đến thông số VLAN, chính vì thế làm thay đổi thiết lập cho tất cả các VLAN. Lấy ví dụ, lệnh “spanning – tree cost 2” sẽ làm chi phí STP của một giao tiếp trở thành 2 cho tất cả các VLANs.

Theo tập các câu lệnh debug đầu tiên này, đầu ra của lệnh “show spanning – tree” liệt kê Fastatethernet 0/16 là Khóa và Fastatethernet 0/17 là Chuyển tiếp, với chi phí đến bridge root bây giờ chỉ là 2, dựa trên chi phí có thay đổi của giao tiếp Fastatethernet 0/17.

Thay đổi kế tiếp xảy ra khi lệnh “spanning – tree vlan 3 root primary” được thực hiện trên SW1. Lệnh này thay đổi độ ưu tiên cơ bản sang 24,576, làm cho độ ưu tiên VLAN 3 của SW1 là 24,576 cộng với 3, hay 24,579. Kết quả là, SW1 trở thành switch root, như được thể hiện trong các thông điệp debug bên dưới.

Lệnh “spanning – tree vlan *vlan-id* root primary” cho biết một switch sử dụng một giá trị ưu tiên cụ thể chỉ trên VLAN đó, với switch lựa chọn một giá trị mà sẽ làm cho switch đó trở thành switch root trên VLAN đó. Để làm như vậy, lệnh này thiết lập độ ưu tiên cơ sở - đến một giá trị thấp hơn giá trị ưu tiên cơ sở của switch root. Lệnh này chọn độ ưu tiên cơ sở như sau:

- 24,576 nếu root hiện tại có giá trị ưu tiên cơ sở cao hơn 24,576.
- 4096 thấp hơn độ ưu tiên cơ sở của root hiện tại nếu độ ưu tiên của root hiện tại là 24,576 hay thấp hơn.
- Lệnh “spanning – tree vlan *vlan – id* root secondary” báo cho một switch sử dụng một giá trị độ ưu tiên cơ sở mà switch nội bộ sẽ trở thành root nếu switch root chính bị lỗi. Lệnh này thiết lập độ ưu tiên cơ sở của switch thành 28,672 tùy thuộc theo giá trị độ ưu tiên hiện tại của root hiện tại.

Chú ý: Độ ưu tiên cũng có thể được thiết lập rõ ràng với lệnh cấu hình toàn cục “spanning – tree vlan *vlan-id* priority *value*”, thiết lập độ ưu tiên cơ sở cho switch đó. Tuy nhiên, bởi vì nhiều thiết kế LAN dựa trên chỉ một root, và một dự phòng cho root đó, nên các lệnh khác thường được ưu tiên hơn.

4.3.4. Cấu hình PortFast và BPDU Guard

Các chức năng PortFast và BPDU Guard có thể được cấu hình một cách dễ dàng trên bất kỳ giao tiếp nào. Để cấu hình PortFast, chỉ sử dụng lệnh cấu hình con trên giao tiếp “spanning – tree portfast”. Để cung kích hoạt BPDU Guard, thêm lệnh cấu hình con “spanning – tree bpdu guard enable” vào.

4.3.5. Cấu hình EtherChannel

Cuối cùng, hai switch có kết nối Ethernet song song có thể được cấu hình với EtherChannel. Để làm như thế, STP không khóa trên bất kỳ giao tiếp nào, vì STP xem cả hai giao tiếp trên mỗi switch như là một liên kết. Ví dụ 4.3 cho thấy cấu hình SW1 và lệnh “show” cho EtherChannel mới này.

Ví dụ 4.3:

```
SW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#interface fa 0/16
SW1(config-if)#channel-group 1 mode on
SW1(config-if)#int fa 0/17
SW1(config-if)#channel-group 1 mode on
SW1(config-if)#^Z
00:32:27: STP: VLAN001 Po1 -> learning
00:32:42: STP: VLAN001 Po1 -> forwarding

SW1#show spanning-tree vlan 3

VLAN003
  Spanning tree enabled protocol ieee
  Root ID    Priority    28675
              Address     0019.e859.5388
              Cost         12
              Port        72 (Port-channel)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID Priority    28675 (priority 28672 sys-id-ext 3)
              Address     0019.e86a.6f80
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time   300

  Interface      Role Sts Cost      Prio.Nbr Type
  -----
```

```

Fa0/11      Desg FWD 19      128.11  P2p
Po1        Root PWD 12      128.72  P2p

SW1#show etherchannel 1 summary
Flags: D - down      P - in port-channel
      I - stand-alone S - suspended
      H - Hot standby (LACP only)
      R - Layer3      S - Layer2
      U - in use       f - failed to allocate aggregator
      U - unsuitable for bundling
      W - waiting to be aggregated
      d - default port

Number of channel-groups in use: 1
Number of aggregators: 1

Group  Port-channel  Protocol  Ports
-----+-----+-----+
1      Po1(SU)       -        Fa0/16(P)  Fa0/17(P)

```

Trên các switch 2960, bất kì port nào cũng có thể là thành phần của một EtherChannel, với tối đa tám trên một EtherChannel đơn, vì thế các lệnh EtherChannel là các lệnh giao tiếp con. Các lệnh con giao tiếp **channel – group 1 mode on** kích hoạt EtherChannel trên các giao tiếp Fastatethernet 0/16 và 0/17. Cá hai switch phải đồng ý về chỉ số port cho EtherChannel đó, là 1 trong trường hợp này, vì thế việc cấu hình portchannel cho SW2 là cần thiết với SW1.

Lệnh channel – group cho phép cấu hình một giao tiếp để luôn luôn là một port channel (sử dụng từ khóa **on**), hay được tự động thỏa thuận với các switch khác sử dụng các từ khóa **auto** hay **desirable**. Với từ khóa **on** được sử dụng trên SW1, nếu với một số nguyên nhân SW2 không được cấu hình một cách chính xác với EtherChannel, các lệnh cấu hình **channel – group** trên mỗi switch có thể sử dụng các tham số **auto** hay **desirable** thay vì **on**. Với những tham số khác này, các switch thỏa thuận liệu có sử dụng EtherChannel hay không. Nếu được thỏa thuận, một EtherChannel được tạo dựng. Nếu không, các port có thể được sử

dụng mà không cần xây dựng cơ chế EtherChannel, với việc khóa STP trên một số giao tiếp.

Việc sử dụng các tham số **auto** và **desirable** có thể dễ nhầm lẫn. Nếu cấu hình **auto** trên hai giao tiếp, EtherChannel không bao giờ hoạt động. Từ khóa **auto** báo cho switch biết phải đợi các switch khác để bắt đầu thỏa thuận. Cùng với một trong hai switch được cấu hình với hoặc là **on** hay **desirable**, EtherChannel có thể thỏa thuận một cách thành công.

Trong phần còn lại của ví dụ 4.3, thấy nhiều tham chiếu đến “port – channel” hay là “Po.” Vì STP xem EtherChannel là một liên kết, các switch cần một số cách để hiển thị toàn thể EtherChannel đó. IOS 2960 sử dụng khái niệm Po, viết tắt của Port channel, là cách để đặt tên cho EtherChannel. EtherChannel thỉnh thoảng được gọi tên là port channel. Ví dụ, phần gần cuối của ví dụ này, lệnh **show etherchannel 1 summary** tham chiếu đến Po1, cho port Channel/ EtherChannel 1.

4.3.6. Cấu hình RSTP

Việc cấu hình và xác nhận RSTP là cực kì cần thiết sau khi đã hiểu được cấu hình các tham số STP được xem xét trong chương này. Mỗi switch yêu cầu một lệnh cấu hình đơn, **spanning – tree mode rapid – pvst**. Như có thể nói từ lệnh này, nó không chỉ cho phép RSTP mà còn PVRST, chạy thể hiện RSTP cho tất cả các VLAN đã xác định.

Phần còn lại của các lệnh cấu hình được xem xét trong phần này áp dụng với RSTP và PVRST mà không có thay đổi nào. Các lệnh tương tự ảnh hưởng đến BID, chỉ định port, và EtherChannel. Thực ra, các lệnh giao tiếp con **spanning – tree portfast** thậm chí làm việc tạo giao tiếp một giao tiếp kiểu RSTP edge một cách kỹ thuật, thay vì kiểu liên kết, và ngay tức thì đưa giao tiếp đó sang trạng thái Chuyển tiếp.

Ví dụ 4.4 cho thấy cách tích hợp từ STP và PVST+ sang RSTP và PVRST, và cách để báo liệu một switch đang sử dụng RSTP hay STP.

Ví dụ 4.4:

```

SW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#spanning-tree mode ?
  mst      Multiple spanning tree mode
  pvst     Per-Vlan spanning tree mode
  rapid-pvst Per-Vlan rapid spanning tree mode

! The next line configures this switch to use RSTP and PVRST.
!
SW1(config)#spanning-tree mode rapid-pvst
SW1(config)#^Z
! The 'protocol RSTP' shaded text means that this switch uses RSTP, not IEEE STP.
SW1#show spanning-tree vlan 4

VLAN004
  Spanning tree enabled protocol rstp
  Root ID  Priority 32772
            Address  0019.e859.5388
            Cost      19
            Port      16 (FastEthernet0/16)
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID Priority 32772 (priority 32768 sys-id-ext 4)
            Address  0019.e86a.6f80
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time 300

Interface      Role Sts Cost      Prio.Nbr Type
-----+-----+-----+-----+-----+-----+-----+
Fa0/16        Root FWD 19      120.16  P2p Peer(STP)
Fa0/17        Altn BLK 19      128.17  P2p Peer(STP)

```

Cụ thể, so sánh cụm từ “protocol rstp” được tô bóng mờ trong ví dụ này với đầu ra các ví dụ trước đây từ câu lệnh `show spanning-tree`. Các ví dụ trước đây tất cả đều sử dụng thiết lập mặc định của STP và PVST+, liệt kê dòng chữ “protocol ieee” muốn nói đến chuẩn gốc từ IEEE 802.1d

4.4. XỬ LÝ SỰ CÓ STP

Phần cuối cùng này tập trung vào cách áp dụng thông tin đã xem xét trong các phần trước đây của chương này với các ngữ cảnh mới. Phần này giúp chuẩn bị để xử lý các vấn đề của STP trong các mạng thực tế.

Phần này mô tả và tóm tắt kế hoạch cho việc phân tích và trả lời các dạng vấn đề khác nhau của STP. Để thực hiện, cần tuân theo quy trình cơ bản sau đây:

Bước 1: Xác định switch root

Bước 2: Với mỗi switch không phải là root, xác định một port root, và chi phí để đến switch root thông qua port root đó.

Bước 3: Với mỗi phân đoạn, xác định port dành riêng và chi phí được quảng bá bởi port dành riêng vào phân đoạn đó.

Phản sau xem lại các điểm chính về mỗi một bước này, và sau đó liệt kê một số các hướng dẫn giúp nhanh chóng tìm ra phương án để xử lý sự cố.

4.4.1. Xác định switch root

Việc xác định switch root là đơn giản nếu biết tất cả các BID của switch đó, chỉ lấy giá trị thấp nhất của nó. Nếu các câu hỏi liệt kê độ ưu tiên và địa chỉ MAC riêng biệt, như thường là đầu ra của lệnh show, đặt switch đó với giá trị ưu tiên thấp nhất, hay trong trường hợp xung đột, lấy giá trị địa chỉ MAC thấp hơn.

Khá giống với các mạng trong thực tế, nếu một câu hỏi yêu cầu giải quyết các lệnh show trên nhiều switch để tìm switch root, một chiến lược có tổ chức có thể giúp trả lời các câu hỏi đó nhanh hơn. Trước tiên, nhớ rằng nhiều loại khác nhau của câu lệnh **show spanning – tree** liệt kê BID của root, với độ ưu tiên trên một dòng và địa chỉ MAC trên dòng kế tiếp, trong phần đầu của đầu ra đó; BID của switch cục bộ được liệt kê trong phần tiếp theo. Cũng ghi nhớ rằng các switch Cisco mặc định sử dụng PVST+, vì thế cần thận khi xem xét các chi tiết STP với VLAN đúng. Với những nhận tổ này, danh sách sau đây liệt kê ra một chiến lược tốt:

*Bước 1: Lấy một switch để bắt đầu, và tìm ra giá trị BID của switch root và giá trị BID nội bộ trong VLAN đó trong câu hỏi sử dụng lệnh **show spanning – tree vlan vlan-id***

Bước 2: Nếu BID của root là bằng với BID nội bộ, switch nội bộ là switch root.

Bước 3: Nếu BID root không bằng với BID nội bộ, tuân theo các bước sau:

- Tim giao tiếp RP trên switch nội bộ (cũng sử dụng lệnh **show spanning - tree**)
- Sử dụng giao thức CDP hay giao thức khác, xác định switch nào là đầu cuối phía bên kia của giao tiếp RP được tìm thấy trong bước 3A.
- Đăng nhập vào switch đó bên đầu phía đối diện của giao tiếp RP và lặp lại tiến trình này, bắt đầu với bước 1.

Ví dụ 4.5 cho thấy đầu ra của lệnh **show spanning - tree vlan 1**. Nếu không có kiến thức về sơ đồ LAN, có thể sử dụng các bước nói trên để xác định switch root cho sơ đồ.

Ví dụ 4.5:

```
SW2#show spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID  Priority  32769
            Address   000a.b7dc.b780
            Cost      19
            Port      1 (FastEthernet0/1)
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID Priority  32769 (priority 32768 sys-id-ext 1)
  Address   0011.92b0.f500
  Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
  Aging Time 300

  Interface      Role Stg Cost      Prio.Nbr Type
  .....          .....  ..  ..  ..  ..  ..  ..
  Fa0/1          Root FWD 19      128.1    P2P
  Fa0/19         Desg FWD 100    128.19   Shr
  Fa0/20         Desg FWD 100    128.20   Shr
  SW2#show spanning-tree vlan 1 bridge id
  VLAN0001        0001.0011.92b0.f500
```

Phản bông đồ của ví dụ này chỉ ra BID của root (độ ưu tiên và địa chỉ) cũng như là BID khác của SW2. Vì BID switch root là khác, bước tiếp theo sẽ là tìm root port, được liên kê trong hai nơi khác nhau của đầu ra lệnh (Fa0/1). Bước tiếp sẽ là lặp lại tiến trình trên switch ở đầu bên kia của giao tiếp Fa0/1 của SW2, nhưng ví dụ này không xác định switch đó.

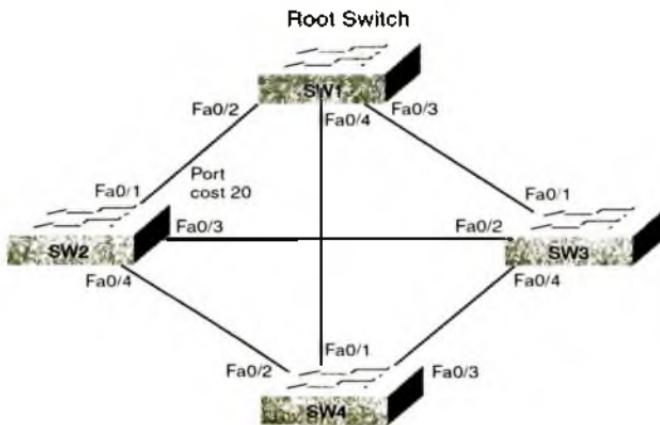
4.4.2. Xác định các root port và không root port của các switch

Mỗi switch không phải là root có chỉ một và duy nhất một root port – RP. (Switch root không có một RP nào). Để chọn RP của nó, một

switch lắng nghe các thông điệp Hello BPDU đến. Với mỗi Hello nhận được, switch thêm chi phí được liệt kê trong Hello BPDU vào chi phí port của switch đó với port mà Hello đã được nhận. Chi phí thấp nhất thắng, trong trường hợp trùng, switch lấy giao tiếp với độ ưu tiên port thấp hơn, và nếu nó trùng, switch lấy số port nội bộ thấp hơn.

Trong khung phân hình vẽ trước thực sự tóm tắt cách thức một switch lấy RP của nó, khi một câu hỏi cung cấp thông tin về switch root và chi phí port của giao tiếp, một tiếp cận khác biệt đôi chút có thể giúp trả lời nhanh hơn. Ví dụ, xem xét câu hỏi sau đây, được hỏi về mạng thể hiện trong hình 4.16.

Trong mạng chuyển mạch hình 4.16, tất cả các switch và phân đoạn đang hoạt động, với STP được kích hoạt trên VLAN 1. SW1 được lựa chọn là root. Giao tiếp Fa0/1 của SW2 sử dụng chi phí được thiết lập là 20, với tất cả các giao tiếp khác sử dụng chi phí STP mặc định. Xác định RP trên SW4.



Hình 4.16. Ví dụ về Root Port trên mạng LAN

Một cách để giải quyết vấn đề cụ thể này là chỉ áp dụng các khái niệm STP như đã tóm tắt trong mục 1.1 của chương này. Ngoài ra có thể tìm thấy giải pháp nhanh hơn một ít với tiến trình sau đây, bắt đầu với một switch không phải là root.

Bước 1: Xác định tất cả con đường có thể qua đó một frame, được gửi bởi một switch không phải là root, có thể đến switch root.

Bước 2: Với mỗi con đường có thể trong bước 1, thêm chi phí của tất cả các giao tiếp ra ngoài trên con đường đó.

Bước 3: Chi phí thấp nhất được tìm thấy là chi phí để đến root, và giao tiếp ra ngoài là RP của switch đó.

Bước 4: Nếu chi phí xung đột, sử dụng độ ưu tiên port để giải quyết xung đột, và nếu nó xung đột tiếp, sử dụng số port thấp nhất để giải quyết.

Bảng 4.12 cho thấy công việc được hoàn thành với Bước 1 và 2 trong tiến trình này, liệt kê các con đường và chi phí riêng rẽ để đến root qua mỗi con đường. Trong mạng này, SW4 có năm con đường có thể đến switch root. Cột chi phí liệt kê các chi phí giao tiếp trên cùng thứ tự như là trong cột đầu tiên, cùng với chi phí tổng cộng.

Bảng 4.12. Kết quả xác định root port

Con đường vật lý (giao tiếp đầu ra)	Chi phí
SW4(Fa0/2) → SW2(Fa0/1) → SW1	19+20=39
SW4(Fa0/3) → SW3(Fa0/1) → SW1	19+19=38
SW4(Fa0/1) → SW1	19=19
SW4(Fa0/2) → SW2(Fa0/3) → SW3(Fa0/1) → SW1	19+19+19=57
SW4(Fa0/3) → SW3(Fa0/2) → SW2(Fa0/1) → SW1	19+19+20=58

Để đảm bảo rằng nội dung của bảng là rõ ràng, kiểm tra việc định tuyến vật lý từ SW4 (Fa0/2) → SW2 (Fa0/1). Với con đường này, các giao tiếp ra là giao tiếp Fa0/2 của SW4, mặc định chi phí là 19, và giao tiếp Fa0/1 của SW2, được cấu hình cho chi phí là 20, vậy tổng cộng là 39.

Chúng ta cũng nên nhận ra chi phí của giao tiếp nào bị bỏ qua trong tiến trình này. Sử dụng cùng ví dụ, frame được gửi bởi SW4 đến root sẽ đi vào giao tiếp Fa0/4 của SW2 và giao tiếp Fa0/2 của SW1. Không còn chi phí nào khác được xem xét.

Trong trường hợp này, RP của SW4 sẽ là giao tiếp Fa0/1 của nó, vì con đường với chi phí thấp nhất (19) bắt đầu với giao tiếp đó.

Cần thận với việc trả lời các câu hỏi yêu cầu tìm một RP của switch. Ví dụ, trong trường hợp này, có thể trực giác để nghĩ rằng RP của SW4 có thể là giao tiếp Fa0/1 của nó, vì nó được kết nối trực tiếp đến root. Tuy nhiên, nếu Fa0/3 của SW4 là Fa0/1 của SW3 được thay đổi chi phí port là 4 cho mỗi giao tiếp đó, thì con đường Fa0/3(SW4) → Fa0/1(SW3) → SW1 sẽ có chi phí tổng cộng là 8, và RP của SW4 sẽ là giao tiếp Fa0/3 của nó. Vì thế, chỉ vì con đường có vẻ tốt hơn trong sơ đồ này, nhớ rằng điểm quyết định là chi phí tổng.

4.4.3. Xác định port dành riêng cho mỗi phân đoạn LAN

Mỗi phân đoạn LAN có một switch đơn hoạt động như là port dành riêng DP cho phân đoạn đó. Trên phân đoạn có kết nối một switch đến một thiết bị không sử dụng STP – ví dụ, các phân đoạn có kết nối một switch đến một PC hay một router – port switch đó được bầu chọn là DP vì chỉ thiết bị đó gửi Hello vào phân đoạn chính là switch đó. Tuy nhiên, phân đoạn mạng kết nối nhiều switch yêu cầu nhiều hơn để phát hiện ra port nào sẽ là DP. Theo định nghĩa, DP cho một phân đoạn được xác định như sau:

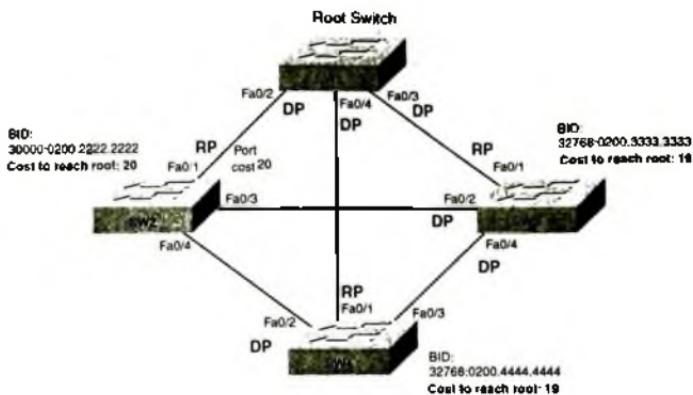
Giao tiếp của switch mà chuyển tiếp Hello BPDU chi phí thấp nhất vào các phân đoạn là DP. Trong trường hợp xung đột, cùng với các switch gửi các Hello với chi phí xung đột, switch với BID thấp nhất chiến thắng.

Theo đó, điều này mô tả cách STP làm việc, và có thể áp dụng khái niệm đó với bất kỳ câu hỏi STP nào. Tuy nhiên, trong ví dụ này, nếu vừa kết thúc việc tìm kiếm RP cho mỗi switch không phải là root, và ghi nhận rằng chi phí để đến root port trên mỗi switch (ví dụ, như thể hiện trong bảng 4.12), có thể dễ dàng tìm thấy DP như sau:

Bước 1: Với các switch có kết nối đến cùng phân đoạn LAN, switch với chi phí thấp nhất để đến root là DP trên phân đoạn đó.

Bước 2: Trong trường hợp xung đột, trong số các switch mà xung đột về chi phí này, switch với BID thấp nhất trở thành DP.

Ví dụ: xem xét **hình 4.17**. Hình này cho thấy cùng mạng chuyển mạch như trong **hình 4.16** nhưng với các RP và DP được ghi chú, cũng như chi phí thấp nhất mỗi switch để đến root qua mỗi RP của nó.



Hình 4.17. Ví dụ về Root Port trên mạng LAN (tiếp theo)

Tập trung vào các phân đoạn kết nối đến switch không phải root. Với phân đoạn SW2 – SW4, SW4 thắng bằng cách giả sử có một con đường chi phí đến root, trong khi con đường tốt nhất của SW2 chi phí là 20. Với cùng nguyên nhân này, SW3 trở thành DP trên phân đoạn SW2 – SW3. Với phân đoạn SW3 – SW4, cả hai SW3 và SW4 xung đột chi phí đến root. Hình này liệt kê BID của switch không phải là root, vì thế có thể thấy rằng BID của SW3 là thấp hơn. Kết quả là, SW3 thắng xung đột, làm cho SW3 là DP trên phân đoạn này.

Chú ý rằng switch root trở thành DP trên tất cả các phân đoạn của nó bằng cách nhấn mạnh sự thật rằng switch root luôn quảng bá Hello với chi phí 0 và chi phí được tính toán của tất cả các switch khác phải ít nhất là 1, vì chi phí port thấp nhất cho phép là 1.

Ví dụ có thể tìm thấy switch root, sau đó RP trên mỗi switch, và DP trên mỗi phân đoạn, sau đó biết về BID, port cost, và sơ đồ mạng LAN. Tại thời điểm này, cũng biết giao tiếp nào chuyển tiếp – những giao tiếp mà là RP hay DP – còn lại là các giao tiếp bị khóa.

4.4.4. Hội tụ STP

Sơ đồ STP – tập hợp các giao tiếp trong trạng thái Chuyển tiếp – nên duy trì sự ổn định cũng như là mạng duy trì sự ổn định của nó. Khi

các giao tiếp và switch hoạt động và ngưng, kết quả sơ đồ STP có thể thay đổi và nói cách khác, sự hội tụ STP xảy ra. Phần này chỉ ra một số chiến lược khá quen thuộc để tìm hiểu các vấn đề nói trên.

Khi sự hội tụ xảy ra, tập trung vào sự thay đổi các giao tiếp từ Chuyển tiếp sang Khóa và từ Khóa sang Chuyển tiếp. Một số vấn đề khác liên quan đến tiến trình dịch chuyển, bao gồm định thời Hello, MaxAge, trì hoãn chuyển tiếp, Trạng thái Học Hồi và Lắng nghe, và sử dụng của chúng, như mô tả trong phần đầu của chương. Với các loại câu hỏi này, hãy nhớ các yếu tố sau đây trong quá trình hội tụ STP:

- Với các giao tiếp ở trong cùng trạng thái STP, không cần thay đổi điều gì
- Với các giao tiếp cần chuyển từ trạng thái Chuyển tiếp sang trạng thái Khóa, switch ngay tức thì chuyển sang trạng thái Khóa.
- Với các giao tiếp cần chuyển từ trạng thái Khóa sang trạng thái Chuyển tiếp, switch trước tiên chuyển giao tiếp sang trạng thái Lắng nghe, sau đó là trạng thái Học Hồi mỗi lần được xác định bởi bộ trì hoãn chuyển tiếp (mặc định 15 giây). Chỉ sau đó, giao tiếp được đặt vào trạng thái Chuyển tiếp.

4.5. CÂU HỎI VÀ BÀI TẬP CHƯƠNG 4

Câu 1: Trạng thái cổng 802.1d nào sau đây là trạng thái ổn định được sử dụng khi STP đã hoàn tất hội tụ

- a. Trạng thái Khóa - Blocking
- b. Trạng thái Chuyển tiếp – Forwarding
- c. Trạng thái Lắng nghe – Listening
- d. Trạng thái Học Hồi – Learning
- e. Trạng thái Hủy – Discarding

Câu 2. Trạng thái cổng 802.1d nào sau đây là chuyển tiếp chỉ sử dụng trong suốt tiến trình hội tụ STP?

- a. Trạng thái Khóa
- b. Trạng thái Chuyển tiếp
- c. Trạng thái Học Hồi
- d. Trạng thái Lắng nghe
- e. Trạng thái Hùy

Câu 3. Giá trị bridge ID nào sau đây sẽ thăng trong bầu cử switch gốc giả sử rằng các switch với những giá trị bridge này ở cùng trên một mạng?

- a. 32768:0200.1111.1111
- b. 32768:0200.2222.2222
- c. 200:0200.1111.1111
- d. 200:0200.2222.2222
- e. 40,000:0200.1111.1111

Câu 4. Yếu tố nào sau đây quyết định bao lâu một bridge hay một switch không phải là gốc gửi một thông điệp Hello BPDU 802.1d STP?

- a. Bộ định thời Hello như được cấu hình trên switch đó
- b. Bộ định thời Hello như được cấu hình trên switch gốc
- c. Nó luôn có giá trị 2 giây
- d. Switch phản ứng lại với BPDU nhận được từ switch gốc bằng cách gửi một BPDU khác 2 giây sau khi nhận được BPDU gốc.

Câu 5. Chức năng STP nào làm cho một giao tiếp đặt sang trạng thái Chuyển tiếp ngay khi giao tiếp được kích hoạt Vật Lý

- a. STP
- b. RSTP
- c. Root Guard
- d. 802.1w
- e. PortFast
- f. EtherChannel

Câu 6. Câu trả lời nào liệt kê tên chuẩn IEEE cài tiến chuẩn STP nguyên thủy và làm giảm thời gian hội tụ

- a. STP
- b. RSTP
- c. Root Guard
- d. 802.1w
- e. PortFast
- f. Trung kế

Câu 7. Trạng thái công RSTP nào có cùng tên như là một Trạng thái công trong STP truyền thống?

- a. Trạng thái Khóa – Blocking
- b. Trạng thái Chuyển tiếp – Forwarding
- c. Trạng thái Lắng nghe – Listatening
- d. Trạng thái Học hỏi – Learning
- e. Trạng thái Hủy - Discarding
- f. Trạng thái bị Hủy - Disabled

Câu 8. Trên một switch 2960, lệnh nào sau đây thay đổi giá trị bridge ID?

- a. spanning – tree bridge – id value
- b. spanning – tree vlan vlan – number root {primary|secondary}
- c. spanning – tree vlan vlan – number priority value
- d. set spanning – tree priority value

Câu 9. Kiểm tra phân giải sau từ lệnh show spanning – tree trên một switch Cisco:

Bridge ID Priority 32771 (priority 32768 sys – id – ext 3)

Address 0019.e86a.6f80

Điều nào sau đây là đúng dựa trên đầu ra của lệnh có được?

- a. Thông tin là về thể hiện STP cho VLAN 1
- b. Thông tin là về thể hiện STP cho VLAN 3

- c. Đầu ra lệnh xác nhận rằng switch này không thể là switch gốc
- d. Đầu ra lệnh xác nhận rằng switch hiện tại là switch gốc

Câu 10. Switch SW3 đang nhận chỉ hai Hello BPDUs, cả hai đều từ cùng switch gốc, được nhận trên hai giao tiếp được liệt kê như sau:

SW3# show interfaces status

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/13		Connected	3	auto	100	10/100 BaseTX
Gi0/1		connected	1	auto	1000	1000 BaseTX

SW3 không có lệnh cấu hình nào liên quan đến STP. Hello được nhận trên Fa0/13 liệt kê chi phí 10, và Hello nhận được trên Gi0/1 liệt kê chi phí 20. Điều nào sau đây là đúng về STP trên SW3?

- a. SW3 sẽ chọn Fa0/13 là port gốc
- b. SW3 sẽ chọn Gi0/1 làm port gốc
- c. Giao tiếp Fa0/13 của SW3 sẽ trở thành port dành riêng
- d. Giao tiếp Gi0/1 của SW3 sẽ trở thành port dành riêng

PHẦN 2

ĐỊNH TUYẾN

Trong phần 1, giáo trình đã tập trung thảo luận các vấn đề có liên quan đến các thiết bị chuyên mạch, môi trường hoạt động của thiết bị chuyên mạch, nguyên tắc hoạt động, cấu tạo và các yếu tố khác có liên quan. Phần 2 của giáo trình sẽ đề cập đến các nội dung liên quan đến các thiết bị định tuyến. Nội dung của phần định tuyến tập trung vào các vấn đề sau:

Chương 5. Địa chỉ IP và phân mạng con: Trong chương này, giáo trình đề cập đến việc đánh địa chỉ IP trong hệ thống mạng và cách phân chia mạng IP con. Nội dung của chương còn đi sâu vào phân tích và giải quyết một số bài toán liên quan đến việc thực hiện và chuyên đổi các phép toán nhị phân, hữu ích khi thực hiện việc đánh số và thiết kế hệ thống mạng IP.

Chương 6. Vận hành router Cisco: Chương này sẽ tìm hiểu về việc cài đặt các router Cisco trong doanh nghiệp và router cho kết nối Internet. Đề cập đến cấu tạo, hoạt động và cách thức truy cập router từ các chế độ khác nhau, cũng như giới thiệu về tiến trình khởi động của router Cisco và việc nâng cấp IOS của router Cisco.

Chương 7. Định tuyến tĩnh và con đường kết nối trực tiếp: Nội dung chương 7 tập trung vào các vấn đề cụ thể sau đây:

- Các vấn đề có liên quan đến định tuyến trên mạng TCP/ IP: DNS, DHCP, ARP, ICMP...
- Các mạng có con đường kết nối trực tiếp
- Định tuyến tĩnh

Chương 8. Chính sách kiểm soát truy cập: Nội dung chương này đề cập chi tiết về việc cấu hình chính sách kiểm soát truy cập – Access List cho các thiết bị router. Trong đó có đề cập đến chính sách truy cập chuẩn, chính sách truy cập mở rộng và quản lý cấu hình chính sách truy cập.

Chương 9. Giao thức định tuyến: Trong chương này, giáo trình tập trung nghiên cứu về đặc điểm, phương thức hoạt động, giải thuật tìm đường cũng như những đặc điểm, tính chất và cách thức cấu hình cho các giao thức định tuyến động như RIP – 1, RIP – 2, OSPF, EIGRP...

Chương 10. Định tuyến trong hệ thống có mặt nạ mạng có chiều dài thay đổi: Nội dung chương 10 đề cập đến các vấn đề sau đây:

- Định tuyến phân lớp và không phân lớp
- Kỹ thuật phân mạng con có chiều dài mặt nạ mạng thay đổi
- Gộp đường cho các mạng con
- Chiến lược gộp đường
- Cấu hình tự động gộp đường trên router Cisco

Chương 11. Kết nối mạng diện rộng - WAN:

- Cấu hình kết nối điểm - điểm
- Cấu hình router kết nối Internet

Trong nội dung của phần này thì kỹ thuật định tuyến tĩnh và định tuyến động là quan trọng nhất. Tuy nhiên, tác giả cố gắng bổ sung thêm các phần có liên quan đến kỹ thuật định tuyến để giải thích và làm rõ nội dung cho độc giả tiện theo dõi.

Chương 5

ĐỊA CHỈ IP VÀ PHÂN MẠNG CON

Chương này tập trung vào tập hợp các khái niệm có liên quan với nhau, thông qua các tiến trình và được sử dụng để giải quyết các câu hỏi về địa chỉ IP, phân chia mạng con. Trong đó tập trung chủ yếu vào làm thế nào để giải quyết các vấn đề có liên quan đến địa chỉ IP và phân chia mạng con.

5.1. ĐỊA CHỈ IP VÀ ĐỊNH TUYẾN

Phần này chủ yếu xem lại các khái niệm về địa chỉ và định tuyến được tìm thấy trong các chương trước đây, cũng như là trong các học phần khác. Trong đó cũng giới thiệu một cách vắn tắt về địa chỉ IP version 6 (IPv6) và khái niệm của mạng địa chỉ IP riêng.

5.1.1. Địa chỉ IP

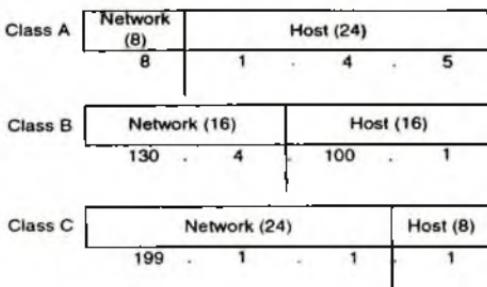
Phần lớn mạng IP ngày nay sử dụng một phiên bản của giao thức IP được gọi là IP Version 4 (IPv4) và trong giáo trình này đơn giản để cập nhật là địa chỉ IP.

Trong IPV4 tồn tại nhiều lớp mạng A, B, C khác nhau. Bảng 5.1 tóm tắt một số mạng có thể, tổng số cho mỗi loại và số lượng thiết bị trên mỗi lớp mạng A, B và C.

Bảng 5.1. Các mạng phân lớp trong địa chỉ IP V4

	Lớp A	Lớp B	Lớp C
Khoảng octet đầu tiên	1 đến 126	128 đến 191	192 đến 223
Số mạng hợp lệ	1.0.0.0 đến 126.0.0.0	128.0.0.0 đến 191.255.0.0	192.0.0.0 đến 223.255.255.0
Số mạng trong lớp	$2^7 - 2$	$2^{14} - 2$	$2^{21} - 2$
Số thiết bị mỗi mạng	$2^{24} - 2$	$2^{16} - 2$	$2^8 - 2$
Kích thước phần địa chỉ mạng (Byte)	1	2	3
Kích thước phần địa chỉ thiết bị (Byte)	3	2	1

Hình 5.1 cho thấy cấu trúc của ba lớp địa chỉ IP, mỗi lớp từ một mạng khác nhau, khi việc phân chia mạng con không được sử dụng. Một địa chỉ trong một mạng lớp A, một trong mạng lớp B, và một trong mạng lớp C.



Hình 5.1. Các mạng IP được sử dụng

Theo định nghĩa, một địa chỉ IP mà bắt đầu với 8 trong octet đầu tiên là trong mạng lớp A, vì thế phần địa chỉ mạng là byte đầu tiên, hay là octet đầu tiên. Một địa chỉ bắt đầu với 130 là một mạng lớp B. Theo định nghĩa, các địa chỉ lớp B có phần mạng 2 byte, như thể hiện trên hình vẽ. Cuối cùng, bắt kí địa chỉ mà bắt đầu với 199 là một mạng lớp C, có phần mạng 3 byte. Cũng theo định nghĩa, một địa chỉ lớp A có phần thiết bị 3 byte, lớp B có phần thiết bị 2 byte, và lớp C có phần thiết bị 1 byte.

Có thể nhớ đơn giản các số trong bảng 5.1 và khái niệm trong hình 5.1 để sau đó nhanh chóng quyết định các phần mạng và phần thiết bị của địa chỉ IP. Tuy nhiên máy tính sử dụng một mặt nạ để định nghĩa kích thước của các phần mạng và thiết bị của một địa chỉ. Ý nghĩa của mặt nạ giống như các khái niệm trong các mạng lớp A, B, C như đã giới thiệu, nhưng máy tính có thể xử lý tốt hơn khi sử dụng mặt nạ mạng ở dạng nhị phân.

Mặt nạ mạng (subnet mask) là một số nhị phân 32 bit, thông thường được viết theo định dạng dấu chấm thập phân. Mục đích của mặt nạ là xác định cấu trúc của một địa chỉ IP. Ngắn gọn hơn, mặt nạ xác định kích thước của phần thiết bị của một địa chỉ IP, biểu diễn cho phần thiết bị của

địa chỉ IP với các bit 0 trong mặt nạ. Phần đầu tiên của mặt nạ chứa các bit 1, giới thiệu cho phần mạng của các địa chỉ (nếu không sử dụng phân chia mạng con), hay cả hai phần mạng và mạng con của các địa chỉ (nếu có sử dụng mạng con).

Khi mạng con không được sử dụng, mỗi lớp địa chỉ IP sử dụng mặt nạ mặc định cho lớp đó. Lấy ví dụ, mặt nạ mặc định lớp A kết thúc với 24 bit 0 nhị phân, có nghĩa rằng ba octet cuối của mặt nạ là 0, đại diện cho phần thiết bị 3 byte của các địa chỉ lớp A. Bảng 5.2 tóm tắt các mặt nạ mặc định và phản ánh kích thước của hai phần của một địa chỉ IP.

Bảng 5.2. Mặt nạ mạng mặc định trong IP V4

Lớp địa chỉ	Kích thước phần địa chỉ tĩnh theo bit	Kích thước phần thiết bị tĩnh theo bit	Mặt nạ mặc định cho mỗi lớp mạng
A	8	24	255.0.0.0
B	16	16	255.255.0.0
C	24	8	255.255.255.0

5.1.2. Địa chỉ công cộng và dành riêng

ICANN (thường gọi là IANA) và các tổ chức thành viên quản lý tiến trình gán số mạng IP, hay thậm chí là khoảng các địa chỉ IP nhỏ hơn, để phù hợp với các nhu cầu muôn kết nối Internet. Sau khi một công ty được gán một khoảng địa chỉ IP, chỉ công ty đó có thể sử dụng khoảng địa chỉ IP của mình. Ngoài ra, các bộ định tuyến trên Internet có thể học các con đường để đến những mạng này, vì thế mọi người trên Internet có thể chuyển các gói tin đến mạng IP đó. Bởi vì những địa chỉ IP này có thể đến được bằng cách gói tin trên mạng Internet công cộng, những mạng này thường được gọi là mạng công cộng và các địa chỉ trên mạng này được gọi là các địa chỉ công cộng.

Một số máy tính sẽ không bao giờ được kết nối Internet. Vì thế, người xây dựng một mạng bao gồm chỉ những máy tính có thể sử dụng các địa chỉ IP trùng với các địa chỉ IP công cộng đã đăng ký trên Internet. Vì thế, khi thiết kế ràng buộc địa chỉ IP cho một mạng như vậy, một tổ chức có thể lấy và sử dụng bất kì số nào mạng nào mà họ muốn, và tất cả

đều làm việc tốt. Ví dụ, có thể mua một vài bộ định tuyến, kết nối chúng trong một văn phòng, và cấu hình các địa chỉ IP trong mạng 1.0.0.0 và làm cho chúng hoạt động, thậm chí một số công ty cũng sử dụng mạng ở lớp A như là địa chỉ mạng IP công cộng đã đăng ký. Các địa chỉ IP sử dụng có thể bị trùng với các địa chỉ IP thực trên Internet, nhưng nếu muôn làm trong phòng thực hành trong văn phòng, thì tất cả đều hoạt động tốt.

Tuy nhiên, sử dụng cùng các địa chỉ IP được sử dụng bởi công ty khác là không cần thiết trong tình huống này, bởi vì khuyến nghị 1918 TCP/IP xác định một tập các mạng riêng có thể được sử dụng cho việc kết nối liên mạng mà không có kết nối Internet. Quan trọng hơn, tập hợp mạng riêng sẽ không bao giờ được gán bởi ICANN cho bất kỳ tổ chức nào cho việc sử dụng như là số mạng công cộng có đăng ký. Vì thế, khi xây dựng một mạng riêng, giống như trong lab, có thể sử dụng các số trong một khoảng mà không được sử dụng bởi bất kỳ ai trên Internet. Bảng 5.3 cho thấy không gian địa chỉ riêng được định nghĩa bởi RFC 1918.

Bảng 5.3. Địa chỉ IP dành riêng

Mạng IP dành riêng	Lớp mạng	Số mạng
10.0.0.0 đến 10.0.0.0	A	1
172.16.0.0. đến 172.31.0.0	B	16
192.168.0.0 đến 192.168.255.0	C	256

Nói cách khác, bất kỳ tổ chức nào cũng có thể sử dụng các số mạng này. Tuy nhiên không tổ chức nào được phép quảng bá những mạng này sử dụng giao thức định tuyến trên Internet.

Nhiều người có thể ngạc nhiên “tại sao lại dành riêng số mạng riêng đặc biệt này trong khi không lo lắng liệu những địa chỉ này có bị trùng không?” Dĩ nhiên, các mạng dành riêng có thể được dùng trong một công ty và công ty này có kết nối Internet, sử dụng một chức năng được gọi là NAT (Network Address Translation – Cơ chế Chuyển đổi địa chỉ mạng).

5.1.3. Địa chỉ IPv6

IPv6 định nghĩa nhiều cải tiến hơn IPv4. Tuy nhiên, mục tiêu chính của IPv6 là để tăng một cách đáng kể số địa chỉ IP có thể. Để làm điều này,

IPv6 sử dụng một địa chỉ IP 128 bit, thay vì 32 bit được định nghĩa bởi IPv4. Để đáp ứng với cấu trúc kích thước địa chỉ, một cấu trúc địa chỉ 128 bit cung cấp hơn 10^{38} địa chỉ IP có thể. Nếu quan tâm đến sự thật rằng dân số Trái Đất hiện thời nhỏ hơn 10^{10} người, có thể thấy rằng số địa chỉ IP mới là rất khổng lồ.

IPv6 đã được xác định từ giữa những năm 1990, nhưng việc tích hợp từ IPv4 lên IPv6 là khá chậm. IPv6 được tạo ra để giải quyết vấn đề thiếu hụt không gian địa chỉ IPv4. Một số giải pháp ngắn hạn (đáng chú ý là NAT) giúp cải thiện địa chỉ IP. Tuy nhiên, trong năm 2007, việc triển khai IPv6 đã được khởi động nhanh chóng. Nhiều nhà cung cấp dịch vụ lớn đã chuyển đổi sang IPv6 để hỗ trợ số lượng lớn hơn các thiết bị di động có thể kết nối Internet, và chính phủ Việt Nam, cụ thể là Bộ Thông tin và Truyền thông đã quan tâm đến việc chuyển đổi sang địa chỉ IPv6 cho các văn phòng thành viên.

Địa chỉ IPv6 128 bit được viết theo cú pháp thập lục phân, với các dấu phẩy giữa mỗi bốn dấu hiệu. Thậm chí, trong thập lục phân, địa chỉ này cũng rất dài. Tuy nhiên, IPv6 cũng cho phép viết tắt, như trong bảng 5.4. Bảng này cũng tóm tắt một số thông tin khi so sánh IPv4 với IPv6.

Bảng 5.4. So sánh địa chỉ IPv4 và IPv6

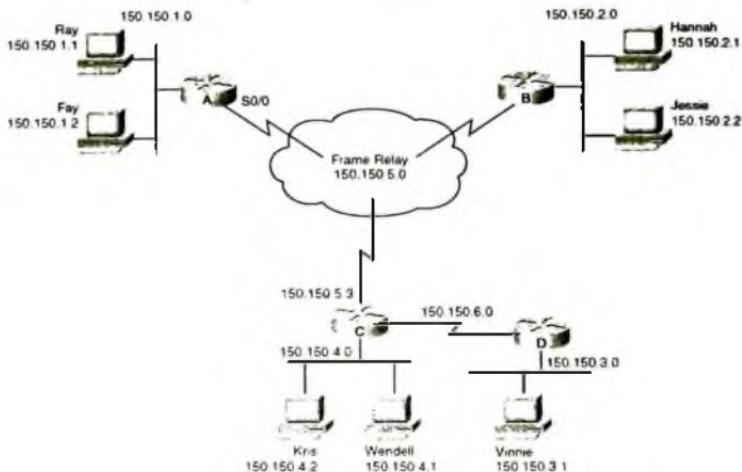
Chức năng	IPv4	IPv6
Kích thước địa chỉ (số bit hay byte mỗi octet)	32 bit, 4 octet	128 bit, 16 octet
Địa chỉ mẫu	10.1.1.1	0000:0000:0000:0000:FFFF:FFFF:0A01:0101
Cùng mạng, được viết tắt	-	::FFFF:FFFF:0A01:0101
Số lượng địa chỉ có thể, bỏ qua giá trị dành riêng	2^{32}	2^{128} hay tương đương 3.4×10^{38}

5.1.4. Phân chia địa chỉ IP

Việc phân chia địa chỉ IP tạo ra một lượng lớn các nhóm nhỏ hơn địa chỉ IP khi so sánh với các quy tắc theo lớp A, B và C. Dù có thể vẫn

nghĩ về các lớp quy tắc lớp A, B và C, nhưng bây giờ một lớp mạng A, B và C đơn có thể phân nhò thành nhiều nhóm nhỏ hơn. Việc phân chia mạng con xem một nhánh nhỏ của một mạng A, B hay C là một mạng con. Bằng cách này, một mạng đơn A, B hay C có thể được phân chia thành nhiều mạng con không trùng lắp.

Hình 5.2 cho thấy làm thế nào phân chia một mạng classful. Hình này cho thấy mạng lớp B 150.150.0.0 với nhu cầu 6 mạng con.



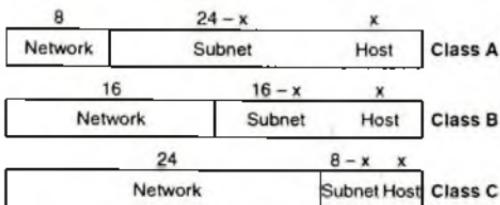
Hình 5.2. Một ví dụ mạng phân lớp trong thực tế

Thiết kế này phân chia lớp mạng B 150.150.0.0. Người thiết kế địa chỉ IP đã chọn mặt nạ 255.255.255.0, octet cuối cùng để làm 8 bit địa chỉ thiết bị. Vì nó là mạng lớp B, có tất cả 16 bit lớp mạng. Chính vì thế, có tất cả 8 bit dành cho các mạng con, từ bit 17 đến 24, trong octet thứ ba.

Các phần mạng (hai octet đầu tiên trong ví dụ này) bắt đầu với 150.150, nghĩa là mỗi một trong 6 mạng con này là một mạng con của mạng lớp B 150.150.0.0

Với việc phân mạng con, phần thứ ba của một địa chỉ IP – phần mạng con – xuất hiện trong chính giữa của địa chỉ. Kích thước của phần mạng của địa chỉ không bao giờ thu hẹp. Nói cách khác, các quy tắc

mạng lớp A, B, và C vẫn áp dụng khi xác định kích thước của phần mạng của một địa chỉ. Tuy nhiên, phần thiết bị của địa chỉ thu hẹp để tạo chỗ cho phần mạng con của địa chỉ này. Hình 5.3 cho thấy định dạng của các địa chỉ khi phân mạng con được sử dụng.



Hình 5.3. Kỹ thuật phân mạng con

5.1.5. Tổng quan định tuyến IP

Định tuyến và địa chỉ IP được thiết kế cùng với nhau ngay từ đầu. Định tuyến IP dựa trên cấu trúc mạng con của IP, trong khoảng của các địa chỉ IP dựa trên một mạng con đơn. Khuyến nghị địa chỉ IP xác định việc phân mạng con để mà các địa chỉ IP được đánh số liên tục có thể được biểu diễn như là một số mạng con (địa chỉ mạng con) và một mặt nạ mạng con. Điều này cho phép bộ định tuyến liệt kê các mạng con trong bảng định tuyến của chúng.

Router cần một cách tốt để liệt kê số mạng con trong bảng định tuyến của nó. Thông tin này bằng cách nào đó ám chỉ các địa chỉ IP trong một mạng con. Lấy ví dụ, mạng con tại đây của hình 5.2, chưa thiết bị Kris, có thể được mô tả như sau:

Tất cả các địa chỉ IP mà bắt đầu với 150.150.4; cụ thể hơn, các số 150.150.4.0 đến 150.150.4.255

Dù rằng đúng, nhưng điều này không dễ hiểu lắm. Thay vào đó bảng định tuyến của router sẽ liệt kê số mạng con và mặt nạ mạng như sau:

150.150.4.0/255.255.255.0

Số mạng con và mặt nạ cùng có nghĩa như câu trên nhưng chỉ sử dụng các số để biểu diễn. Mục này giải thích làm thế nào kiểm tra số mạng con và mặt nạ mạng và chỉ ra khoảng địa chỉ IP liên tục tương ứng với mạng con này.

Một nguyên nhân cần có thể chỉ ra khoảng cách địa chỉ trong một mạng con là để hiểu, phân tích và xử lý các vấn đề định tuyến. Để thấy tại sao, một lần nữa xem xét con đường của router A cho mạng con 150.150.4.0, 255.255.255.0 trong hình 5.2. Mỗi con đường trong bảng định tuyến router liệt kê một đích (số mạng con và mặt nạ), cộng với chỉ dẫn làm cách nào router chuyển gói tin đến mạng con đó. Chỉ dẫn chuyển tiếp thường bao gồm địa chỉ IP của router kế tiếp mà gói tin sẽ được chuyển, và giao tiếp vật lý được dùng khi chuyển tiếp gói tin. Ví dụ, con đường router A đến mạng con đó sẽ giống như thông tin trong bảng 5.5.

Bảng 5.5. Ví dụ về định tuyến

Mạng con và mặt nạ	Router kế tiếp	Giao tiếp đầu ra
150.150.4.0/255.255.255.0	150.150.5.3	S0/0

5.2. CÁC PHÉP TOÁN ĐƯỢC SỬ DỤNG KHI PHÂN CHIA MẠNG CON

Máy tính, đặc biệt là các bộ định tuyến, xem địa chỉ IP như là các con số nhị phân 32 bit. Điều này đúng, vì kỹ thuật này chính là các địa chỉ IP. Tương tự, máy tính sử dụng mặt nạ mạng để xác định cấu trúc của các địa chỉ nhị phân này. Yêu cầu một hiểu biết đầy đủ về điều này có nghĩa là không quá khó với một ít hiểu biết và thực tế. Tuy nhiên, làm quen với toán nhị phân có thể có một ít khó khăn, vì nó ít được sử dụng hằng ngày.

Trong phần này sẽ nghiên cứu về ba phép toán sẽ được sử dụng trong khi thảo luận cho câu trả lời về các câu hỏi liên quan đến địa chỉ và phân mạng con.

- **Chuyển địa chỉ IP và mặt nạ mạng từ nhị phân sang thập phân và ngược lại**
- **Thực hiện phép toán nhị phân được gọi là toán tử nhị phân AND**
- **Chuyển đổi giữa hai định dạng cho các mặt nạ mạng con: thập phân dấu chấm và biểu thức tiền tố**

5.2.1. Chuyển đổi địa chỉ IP và mặt nạ từ thập phân sang nhị phân và ngược lại

Nếu đã từng biết cách số nhị phân làm việc, làm thế nào chuyển đổi từ nhị phân sang thập phân và thập phân sang nhị phân và ngược lại, và làm thế nào để chuyển đổi các địa chỉ IP và mặt nạ từ thập phân sang nhị phân và ngược lại thì bỏ qua phần tiếp theo “Thực hiện phép toán nhị phân AND”

Địa chỉ IP là các số nhị phân 32 bit được biết như là một chuỗi các số thập phân ngăn cách nhau bởi các khoảng (được gọi là định dạng chấm thập phân). Để kiểm tra một địa chỉ có đúng dạng hay không, theo nhị phân, cần chuyển đổi từ nhị phân sang thập phân. Để đặt một số nhị phân 32 bit trong dạng thập phân, cần phải cấu hình một bộ định tuyến, cần chuyển đổi một số 32 bit ngược trở lại số thập phân 8 bit.

Điểm quan trọng để thực hiện tiến trình chuyển đổi cho các địa chỉ IP là nhớ các yếu tố sau:

- Khi chuyển đổi từ một dạng sang dạng khác, mỗi số thập phân đại diện cho 8 bit.
- Khi chuyển đổi từ thập phân sang nhị phân, mỗi số thập phân chuyển đổi sang một số 8 bit.
- Khi chuyển đổi từ nhị phân sang thập phân, mỗi tập hợp 8 bit của các bit liền kề chuyển thành một số thập phân.

Xem xét việc chuyển đổi địa chỉ IP 150.150.2.1 sang nhị phân. Số 150, khi được chuyển sang 8 bit thì bằng với 10010110. Byte kế tiếp là một số thập phân khác 150, được chuyển sang 10010110. Byte thứ ba, số 2 thập phân, được chuyển thành 00000010. Cuối cùng, byte thứ tư, số 1 được chuyển thành 00000001. Chuỗi kết hợp của các số 8 bit là một địa chỉ IP 32 bit – trong trường hợp này là: 10010110 10010110 00000010 00000001

Nếu bắt đầu với phiên bản nhị phân của địa chỉ IP, trước tiên phân tách nó thành bốn tập số 8 kí tự. Sau đó chuyển mỗi tập 8 số nhị phân

thành dạng thập phân tương ứng. Lấy ví dụ, viết một địa chỉ IP như sau là đúng, nhưng không hữu ích lắm:

10010110100101100000001000000001

Để chuyển số này thành dạng thập phân tương ứng, trước tiên phân tách nó thành bốn tập hợp 8 kí tự như sau:

10010110 10010110 00000010 00000001

Sau đó kiểm tra bảng chuyển đổi trong phụ lục, thấy rằng số 8 bit đầu tiên chuyển sang 150, và tương tự cho số thứ hai. Tập hợp 8 bit thứ ba được chuyển sang 2 và tập thứ tư được chuyển sang 1 cho kết quả 150.150.2.1

Sử dụng bảng này trong phụ lục dễ hơn, tuy nhiên có hai lựa chọn khác. Trước tiên, có thể học và thực hành các chuyển đổi. Lựa chọn thứ hai là sử dụng toán thập phân, cần thiết cho việc thực hiện chuyển đổi.

Và nhớ rằng với việc phân mạng, mạng con và phần thiết bị của địa chỉ có thể chỉ trải trên một byte của địa chỉ IP đó. Nhưng khi chuyển từ nhị phân sang thập phân và ngược lại, quy luật chuyển đổi một số 8 bit nhị phân sang số thập phân là luôn đúng. Tuy nhiên, khi xem xét phân mạng, cần bỏ qua biên của byte và xem xét rằng các địa chỉ IP là một số 32 bit mà không có biên của byte cụ thể.

5.2.2. Thực hiện phép toán nhị phân AND

Georg Boole, một nhà toán học sống vào những năm 1800, tạo một nhánh toán học mà được gọi là đại số Boolean. Nó có nhiều ứng dụng trong lý thuyết tính toán. Thực sự, có thể tìm thấy số mạng con được cho bởi một địa chỉ IP và mặt nạ mạng sử dụng một phép Boolean AND.

Phép toán Boolean AND là một phép toán được thực hiện trên một cặp số nhị phân một kí tự. Kết quả là một số nhị phân khác. Danh sách sau cho thấy bốn đầu vào có thể với một phép AND, và kết quả của nó.

0 AND 0 \rightarrow 0

0 AND 1 \rightarrow 0

1 AND 0 \rightarrow 0

1 AND 1 \rightarrow 1

Nói cách khác, đầu vào của biểu thức gồm hai số nhị phân một kí tự, và đầu ra của biểu thức là một số nhị phân một kí tự. Kết quả là một khi tất cả đầu vào đều là 1; ngược lại, kết quả của phép toán AND Boolean là 0.

Có thể thực hiện một phép toán Boolean với các số nhị phân dài hơn, nhưng chỉ thực hiện một phép AND trên mỗi cặp số. Lấy ví dụ, nếu muốn thực hiện phép AND trên các số nhị phân 4 kí tự, phải thực hiện một phép AND trên số đầu tiên của mỗi số và ghi kết quả. Sau đó thực hiện lần lượt cho các số tiếp theo.

Bảng 5.6. Thực hiện phép toán nhị phân

	Bốn số nhị phân	Kí tự đầu	Kí tự hai	Kí tự ba	Kí tự bốn
Số đầu	0110	0	1	1	0
Số thứ hai	0011	0	0	1	1
Phép AND	0010	0	0	1	0

Việc tính toán số mạng con được thực hiện tương tự như trên, chỉ khác là sẽ thực hiện trên chuỗi có độ dài 32 bit.

Để xác định số mạng con của một địa chỉ IP, thực hiện phép AND bit giữa địa chỉ IP và mặt nạ mạng con. Dù có thể tìm kiếm một địa chỉ IP và mặt nạ trong dạng số thập phân và tìm ra được số mạng con, các bộ định tuyến và các máy tính khác sử dụng phép toán AND bit giữa địa chỉ IP và mặt nạ mạng để tìm số mạng con, vì thế cần phải hiểu tiến trình này. Bảng 5.7 cho ví dụ về địa chỉ IP, mặt nạ mạng và mạng con tương ứng.

Bảng 5.7. Thực hiện phép toán nhị phân
giữa địa chỉ IP và mặt nạ mạng

	Thập phân	Nhị phân
Địa chỉ	150.150.2.1	1001 0110 1001 0110 0000 0010 0000 0001
Mặt nạ	255.255.255.0	1111 1111 1111 1111 1111 1111 0000 0000
Kết quả AND	150.150.2.0	1001 0110 1001 0110 0000 0010 0000 0000

Trước tiên tập trung vào cột thứ ba của bảng này. Phiên bản nhị phân của địa chỉ 150.150.2.1 được liệt kê trước. Hàng tiếp theo cho thấy phiên bản nhị phân 32 bit của một mặt nạ mạng (255.255.255.0).

Hàng cuối cho thấy kết quả của phép toán AND bit của hai số này. Nói cách khác, bit đầu tiên của mỗi số được AND, và sau đó là các bit tiếp theo, cho đến khi 32 bit của số đầu tiên được AND với các bit cùng vị trí của số thứ hai.

Kết quả số 32 bit nhị phân hàng thứ ba là số mạng con của địa chỉ IP vừa tìm. Tất cả việc cần phải làm là chuyển đổi số 32 bit này ngược lại số thập phân 8 bit. Kết quả là 150.150.2.0.

5.2.3. Kí hiệu tiền tố

Các mặt nạ mạng thực sự là các số 32 bit, nhưng để thuận tiện, chúng thường được viết dưới dạng số thập phân chấm, lấy ví dụ 255.255.255.0. Tuy nhiên, cách khác để đại diện cho một mặt nạ, được gọi là kí hiệu tiền tố, cung cấp một cách tiện lợi hơn để viết tất cả các mặt nạ có số bit 1 liên tiếp, được sau bởi các số 0. Nói cách khác, một mặt nạ mạng không thể có bit 1 và không liên tiếp nhau trong mặt nạ đó. Mặt nạ luôn có một số bit 1 được sau bởi các bit 0.

Nhằm mục đích ghi hay viết mặt nạ mạng, kí hiệu tiền tố đơn giản ghi nhận lại số nhị phân 1 trong một mặt nạ, theo sau bởi một dấu '/'. Lấy ví dụ, với mặt nạ 255.255.255.0, tương ứng với 11111111 11111111 11111111 00000000, kí hiệu tiền tố tương ứng là /24 bởi vì có 24 bit 1 liên tiếp trong mặt nạ này.

Khi nói về các mặt nạ đó, chúng có thể nói là “mặt nạ sử dụng tiền tố /24” hay mặt nạ có một tiền tố 24 bit thay vì phải nói mạng con sử dụng mặt nạ hai trăm năm lăm chấm hai trăm năm mươi lăm chấm hai trăm năm mươi lăm chấm không – đơn giản là chỉ nói “trên 24”.

5.2.4. Tiền trình nhị phân để chuyển đổi giữa thập phân có chấm và ký hiệu tiền tố

Để có thể làm việc được, cần phải chuyển đổi mặt nạ giữa thập phân có chấm và ký hiệu tiền tố. Các bộ định tuyến thể hiện các mặt nạ trong cả hai định dạng, tùy thuộc vào câu lệnh show, và các lệnh câu hỏi thường yêu cầu kí hiệu chấm thập phân. Cũng vậy, có thể thấy tài liệu

được viết với các định dạng mặt nạ khác nhau. Nói một cách thực tế, cần phải chuyển đổi giữa chúng một cách thường xuyên.

Phần này mô tả tiến trình chuyển đổi giữa hai định dạng, sử dụng toán nhị phân, và phần tiếp theo giải thích làm thế nào để chuyển đổi sử dụng chỉ toán thập phân. Để chuyển từ thập phân có chấm sang kí hiệu tiền tố, có thể tuân theo tiến trình nhị phân đơn giản như sau:

Bước 1: Chuyển đổi mặt nạ thập phân có chấm sang nhị phân

Bước 2: Đếm số nhị phân 1 trong mặt nạ nhị phân 32 bit; đây là giá trị của mặt nạ tiền tố.

Ví dụ, mặt nạ nhị phân 255.255.255.0 chuyển sang 11111111 11111111 11110000 00000000 trong nhị phân. Mặt nạ có 20 bit 1, vì thế kí hiệu tiền tố nhị phân của mặt nạ này là /20.

Để chuyển từ một tiền tố sang số thập phân có chấm, có thể tuân theo tiến trình người như sau:

Bước 1: Viết x các bit 1, trong đó x là giá trị được liệt kê trong tiền tố.

Bước 2: Viết chuỗi bit 0 sau bit 1 cho đến khi đủ 32 bit.

Bước 3: Chuyển số nhị phân này, 8 bit một lần, sang thập phân, để tạo số thập phân có chấm; giá trị này là phiên bản thập phân có chấm của mặt nạ mạng.

Lấy ví dụ, với tiền tố /20, chúng sẽ viết như sau:

1111 1111 1111 1111 1111

Sau đó thêm các số 0 vào cho đủ 32 bit:

1111 1111 1111 1111 1111 0000.

Bây giờ chuyển sang thập phân như sau:

255.255.240.0

5.2.5. Tiến trình thập phân để chuyển giữa số thập phân có chấm và kí hiệu tiền tố

Tiến trình thập phân để chuyển đổi các mặt nạ giữa định dạng thập phân có chấm và định dạng tiền tố là có quan hệ gần gũi, cụ thể để có thể chuyển đổi nhị phân/thập phân một cách nhanh chóng. Để thực hiện, hãy

xem bảng 5.8, liệt kê 9 số thập phân có thể được sử dụng trong một mặt nạ mạng con, cùng với số nhị phân tương ứng.

Bảng 5.8. Chuyển đổi số nhị phân và thập phân tương ứng

Octet thập phân mặt nạ mạng	Nhị phân	Số bit 1	Số bit 0
0	00000000	0	8
128	10000000	1	7
192	11000000	2	6
224	11100000	3	5
240	11110000	4	4
248	11111000	5	3
252	11111100	6	2
254	11111110	7	1
255	11111111	8	0

Để chuyển mặt nạ từ chấm thập phân sang định dạng tiền tố, sử dụng tiền trình sau đây:

Bước 1: Khởi động giá trị tiền tố với 0.

Bước 2: Với mỗi octet thập phân có chấm, thêm số nhị phân 1 được liệt kê cho giá trị thập phân đó trong bảng trên.

Bước 3: Chiều dài tiền tố là /x, trong đó x là tổng được tính tại bước 2.

Ví dụ, với mặt nạ 255.255.240.0 như trên, trong bước 1, bắt đầu với giá trị 0. Tại bước 2, thêm số sau đây vào

- Octet đầu tiên có giá trị là 255, thêm 8
- Octet thứ hai có giá trị 255, thêm 8
- Octet thứ ba có giá trị 240 thêm 4.
- Octet thứ tư là 0, thêm 0.
- Kết quả cuối cùng, là chiều dài tiền tố, được viết là /20.

Chuyển đổi từ định dạng tiền tố sang thập phân có chấm là trực quan, nhưng tiền trình được viết rắc rối hơn một ít so với tiền trình trước đây. Tiền trình này để cập đến giá trị x, tiền trình này như sau:

Bước 1: Chia x cho 8 ($x/8$), ghi nhớ thừa số của x cho 8, gọi là d), và số dư còn lại, gọi là r.

Bước 2: Ghi lại d octet của giá trị 255. (Điều này có được bắt đầu mặt nạ với 8, 16 hay 24 bit 1).

Bước 3: Với octet đầu tiên, tìm số thập phân bắt đầu với r số nhị phân 1, được sau bởi tất cả số nhị phân 0. (Xem thêm bảng 5.8).

Bước 4: Với tất cả octet còn lại, ghi một số thập phân 0.

Các bước trên có thể không rõ ràng như được viết. Nếu chiều dài tiền tố là 20, thì tại bước 1, $20/8$ được thừa số là 2, và số dư là 4. Tại bước 2, viết lại số octet của thập phân 255 là:

255.255

Sau đó, tại bước 3, thấy rằng 240 tương ứng với 4 bit 0 của số dư. Sau đó viết giá trị 240 vào octet thứ ba. Cuối cùng, bước 4, hoàn tất mặt nạ mạng như sau:

255.255.240.0

Nên thực hành các phép chuyển đổi thập phân sang nhị phân thường xuyên để có thể làm việc một cách nhanh chóng và chính xác.

5.3. PHÂN TÍCH VÀ LỰA CHỌN MẶT NẠ MẠNG

Tiến trình phân mạng phân chia một mạng classful – các mạng lớp A, B, và C thành nhiều nhóm địa chỉ nhỏ hơn, được gọi là các mạng con. Khi thiết kế một liên mạng, cần chọn để sử dụng mặt nạ đơn trong một mạng classful cụ thể. Việc lựa chọn mặt nạ mạng liên quan đến các yêu cầu thiết kế – như cầu số lượng mạng con, và số thiết bị cho mỗi mạng. Lựa chọn mặt nạ mạng quyết định có bao nhiêu mặt nạ mạng mà lớp classful đó có thể tồn tại, và bao nhiêu địa chỉ tồn tại trên mỗi mạng con, cũng như là số mạng con cụ thể.

Phần trước tiên của chương này kiểm tra làm thế nào phân tích ý nghĩa của mặt nạ mạng con khi đã lựa chọn mạng classful và mặt nạ được dùng trong một liên mạng. Phần thứ hai mô tả làm thế nào lựa chọn mặt nạ mạng để sử dụng khi thiết kế một liên mạng mới. Chú ý rằng trong thực tế, việc phân tích ý nghĩa của mặt nạ mạng mà có đó lựa chọn là nhiệm vụ khác thường xuyên.

5.3.1. Phân tích mặt nạ mạng trong thiết kế mạng con có sẵn

Việc lựa chọn sử dụng một mạng classful cụ thể, với mặt nạ mạng con đơn cụ thể, quyết định số mạng con có thể và số thiết bị trên mỗi mạng con. Dựa trên số mạng và mặt nạ mạng con, có thể chỉ ra có bao nhiêu mạng, mạng con và các bit thiết bị được sử dụng với cơ chế phân mạng con này. Từ yếu tố đó, có thể dễ dàng chỉ ra rằng có bao nhiêu thiết bị trong mạng con và có bao nhiêu mạng con có thể tạo trong mạng đó sử dụng mặt nạ mạng này.

Phần này bắt đầu với thảo luận chung về cách phân tích một thiết kế phân mạng IP, cụ thể làm thế nào xác định số mạng, mạng con và các bit thiết bị được sử dụng trong thiết kế đó. Sau đó mô tả hai tiến trình thông dụng khác nhau để tìm kiếm các nhân tố này, một sử dụng toán nhị phân và một sử dụng toán thập phân. Thông thường nên đọc cả hai, nhưng nên luyện tập một trong các tiến trình này cho đến khi thuần thục. Cuối cùng, phần này kết thúc với việc mô tả làm thế nào để tìm kiếm số mạng có thể, và số thiết bị có thể trên mỗi mạng con.

5.3.2. Ba thành phần: mạng, mạng con và thiết bị

Như đã biết rằng các mạng lớp A, B và C có 8, 16, 24 bit trong trường mạng của nó. Quy tắc này không thay đổi. Cũng biết rằng, nếu không có mạng con, các địa chỉ lớp A, B và C có 24, 16, 8 bit trong trường thiết bị. Với phân mạng con, phần mạng của địa chỉ không thay đổi hay co giãn, nhưng phần thiết bị co giãn để tạo chỗ trong phần mạng con. Vì thế điểm chính để trả lời cho những loại câu hỏi là để chỉ ra có bao nhiêu bit thiết bị duy trì sau khi triển khai mạng con bằng cách lựa chọn mặt nạ mạng con cụ thể. Sau đó có thể biết kích thước trường mạng con, với phần còn lại của câu trả lời cho hai nhân tố sau.

Nhân tố sau cho biết làm thế nào tìm kích thước của mạng, mạng con và phần thiết bị của một địa chỉ IP.

- Phần mạng của địa chỉ luôn được xác định bởi các quy tắc lớp
- Phần thiết bị của địa chỉ luôn được xác định bởi quy tắc mạng con. Số bit 0 trong mặt nạ (luôn được tìm thấy ở cuối mặt nạ) xác định số bit thiết bị trong phần thiết bị của địa chỉ.

- Phân mạng con của địa chỉ là phần còn lại của địa chỉ 32 bit.

Bảng 5.9 cho một ví dụ, với ba hàng cuối cùng thể hiện phân tích cho ba phần của một địa chỉ IP dựa trên ba quy tắc vừa liệt kê.

Bảng 5.9. Ví dụ phân chia mạng con

Bước	Ví dụ	Quy tắc nhớ
Địa chỉ	8.1.4.5	
Mặt nạ	255.255.0.0	
Số bit mạng	8	Theo lớp A, B, C
Số bit thiết bị	16	Theo số bit 0 có trong mặt nạ
Số bit mạng con	8	32-(số bit mạng+số bit thiết bị)

Ví dụ này có 8 bit mạng vì địa chỉ là mạng lớp A, 8.0.0.0. Có 16 bit thiết bị với vì 255.255.0.0 có 16 bit 0 - 16 bit cuối trong mặt nạ mạng. Kích thước của phần mạng con của địa chỉ này là phần còn lại bên trái, hay 8 bit.

5.3.3. Tiến trình nhị phân: Tìm số mạng, mạng con và số bit thiết bị

Có thể tính toán số bit thiết bị một cách dễ dàng nếu mặt nạ mạng sử dụng chỉ là 255 và 0, bởi vì dễ nhớ rằng 255 đại diện cho 8 bit 1 và 0 đại diện cho 8 bit 0. Vì thế với mỗi số thập phân 0 trong mặt nạ, thì có 8 bit thiết bị. Tuy nhiên khi mặt nạ sử dụng giá trị giữa 0 và 255, xác định số bit thiết bị khó khăn hơn một ít.

Kiểm tra các mặt nạ nhị phân giúp giải quyết khó khăn này bởi vì mặt nạ nhị phân xác định một cách trực tiếp số bit mạng và mạng con kết hợp, và số bit thiết bị như sau:

- Số bit 1 của mặt nạ mạng xác định các phần mạng và mạng con kết hợp của địa chỉ đó.
- Số bit 0 của mặt nạ mạng xác định phần thiết bị của các địa chỉ.
- Quy tắc lớp xác định kích thước của phần mạng.

Áp dụng ba yếu tố này với mặt nạ nhị phân cho phép dễ dàng tìm thấy kích thước của mạng, mạng con và phần thiết bị của địa chỉ trong

một phân mạng con cụ thể. Ví dụ, xem xét các địa chỉ và mặt nạ, bao gồm phiên bản nhị phân của mặt nạ, thể hiện trong bảng 5.10.

Bảng 5.10. Ví dụ mặt nạ thập phân và nhị phân

Mặt nạ thập phân	Mặt nạ nhị phân
130.4.102.1, 255.255.255.0	1111 1111 1111 1111 1100 0000 0000
199.1.1.100m 255.255.255.224	1111 1111 1111 1111 1111 1110 0000

Số bit thiết bị được biểu thị bởi một mặt nạ trở nên rõ ràng hơn sau khi chuyển đổi mặt nạ sang nhị phân. Mặt nạ đầu tiên, 255.255.255.0 có 10 bit 0, biểu thị một trường thiết bị 10 bmoiit. Bởi vì mặt nạ này được sử dụng với một địa chỉ lớp B (130.4.102.1), biểu thị 16 bit trường mạng, vẫn còn 6 bit dành cho trường mạng con. Trong ví dụ thứ hai, mặt nạ chỉ có năm bit 0, dành cho 5 thiết bị bit. Vì mặt nạ được dùng với một địa chỉ lớp C, có 24 bit địa chỉ mạng, còn lại chỉ 3 bit dành cho địa chỉ mạng con.

Đây là các bước cần thực hiện, trong nhị phân để tìm kích thước mạng, mạng con và phần thiết bị của một địa chỉ.

Bước 1: So sánh octet đầu tiên của địa chỉ với các địa chỉ bảng lớp A, B và C; viết số bit mạng tùy thuộc vào lớp địa chỉ đó.

Bước 2: Tìm kiếm số bit thiết bị bằng cách:

- Chuyển đổi mặt nạ mạng sang nhị phân
- Đếm số bit 0 trong mặt nạ

Bước 3: Tính số bit mạng con bằng cách trừ 32 với số bit mạng và bit thiết bị

5.3.4. Tiến trình thập phân: Tìm số bit mạng, mạng con và thiết bị

Rất hợp lý khi sử dụng tiến trình nhị phân để tìm số bit mạng, mạng con và thiết bị của một địa chỉ IP bất kì. Với một ít thực hành, và ít tính toán chuyển đổi thập phân/nhị phân, có thể thực hiện nó dễ dàng. Tuy nhiên, một số trường thích làm việc với tiến trình thập phân hơn. Và sau đây là tiến trình thập phân được sử dụng cho quá trình tìm kiếm nói trên:

Bước 1: (Giống như trong tiến trình nhị phân) So sánh octet đầu tiên của địa chỉ với bảng các địa chỉ lớp A, B và C; ghi lại số bit mạng tùy thuộc vào lớp địa chỉ.

Bước 2: Nếu mặt nạ chứa định dạng dấu chấm, chuyển đổi mặt nạ sang định dạng tiền tố.

Bước 3: Tìm kiếm số bit thiết bị, trừ chiêu đi giá trị chiêu dài tiền tố.

Bước 4: (Giống như bước 4 trong tiến trình nhị phân) Tính số lượng bit mạng con bằng cách trừ 32 với số bit của mạng và thiết bị.

Điều quan trọng của tiến trình này là mặt nạ trong định dạng tiền tố liệt kê số bit nhị phân trong mặt nạ, vì thế nó dễ dàng chỉ ra làm có bao nhiêu bit 0 trong mặt nạ đó. Lấy ví dụ, một mặt nạ 255.255.224.0, được chuyển về dạng tiền tố, là /19. Biết rằng mặt nạ có 32 bit, và biết rằng /19 có nghĩa là 19 bit 1, có thể dễ dàng tính toán số bit 0 là $32 - 19 = 13$ bit thiết bị. Phần còn lại của tiến trình cho phép cùng cách thức được sử dụng trong tiến trình nhị phân, nhưng những bước này không yêu cầu bắt kì tính toán nhị phân nào.

5.3.5. Xác định số mạng con và số thiết bị mỗi mạng con

Cần phải trả lời cho câu hỏi sau đây:

“Cho một địa chỉ (hay là số mạng classful), và một mặt nạ mạng con đơn được sử dụng trong mạng classful đó, có bao nhiêu mạng con tồn tại trong mạng classful này? Và có bao nhiêu thiết bị trong mỗi mạng con?”

Hai công thức đơn giản sau đây cho câu trả lời. Nếu xem số bit mạng con là s và số bit thiết bị là h , công thức sau cho câu trả lời:

- Số subnet = 2^s
- Số thiết bị mỗi subnet = $2^h - 2$.

Cả hai công thức được dựa trên sự thật rằng để tính số có thể được tính sử dụng một số nhị phân, lấy 2 lũy thừa số bit được sử dụng. Lấy ví dụ, với 3 bit, có thể tạo $2^3 = 8$ số nhị phân duy nhất: 000, 001, 010, 011, 100, 101, 110, 111.

Quy tắc đánh địa chỉ IP dành riêng hai địa chỉ IP cho mỗi mạng con: số nhỏ nhất/dầu tiên (với tất cả bit 0 trong phần thiết bị) và số lớn nhất/cuối cùng (với tất cả bit 1 trong phần thiết bị). Số nhỏ nhất được dùng cho số mạng con, và số lớn nhất được dùng như là địa chỉ quảng bá

của mạng con. Bởi vì những số này không thể được gán cho một thiết bị để sử dụng như là một địa chỉ IP, công thức để tính toán số thiết bị trên mỗi mạng con phải trừ đi 2.

5.3.6. Số mạng con: Trừ đi 2, hay không

Trước khi tìm hiểu sâu hơn về toán học, chương này cần giải thích một ít các thông tin có liên quan về toán được sử dụng khi tính toán số mạng con có thể. Trong một số trường hợp, hai mạng con trong một mạng IP classful được để dành, và không được dùng. Trong các trường hợp khác, hai mạng con không được dành riêng và có thể sử dụng. Phần này mô tả hai mạng con này, và giải thích khi nào chúng có thể được dùng, và khi nào không được dùng.

Một trong hai khả năng mạng con để dành được gọi là zero subnet, hay mạng con không. Tất cả các mạng con của mạng classful, có giá trị số nhỏ nhất. Số mạng của mạng con không cũng xuất hiện luôn luôn chính xác cùng với số mạng classful của nó. Lấy ví dụ, với mạng lớp B 150.150.0.0, mạng con không sẽ là 150.150.0.0 – tạo một bit không rõ ràng khi nhìn lướt qua. Điều không rõ ràng này là một trong những nguyên nhân mà mạng con không được để dành đầu tiên.

Khả năng thứ hai với mạng con dành riêng được gọi là broadcast subnet, hay mạng con quảng bá. Đó là mạng con có số mạng lớn nhất trong mạng. Nguyên nhân vì mạng này không được sử dụng tại thời điểm liên quan đến sự thật rằng địa chỉ quảng bá của mạng con đó – được sử dụng để gửi một gói tin đến tất cả các thiết bị trong mạng con đó – xảy ra với cùng số của địa chỉ quảng bá toàn thể mạng. Lấy ví dụ, một gói tin được gửi đến địa chỉ 150.150.255.255 có thể có nghĩa là “gửi gói tin này đến tất cả các thiết bị trong mạng lớp B 150.150.0.0”, nhưng trong các trường hợp khác có nghĩa rằng gói tin đó nên chỉ được chuyển đến tất cả các thiết bị trong một mạng con đơn. Điều mơ hồ này trong ý nghĩa của một địa chỉ quảng bá là nguyên nhân vì sao những mạng như vậy bị bỏ qua.

Cần phải xác định khi nào mạng con không và mạng con quảng bá được dùng. Nếu được phép, công thức cho số mạng của mạng con là 2^s ,

trong đó s là số bit mạng con; nếu không được phép, số mạng con là $2^s - 2$, trừ đi hai mạng đặc biệt. Có ba nhân tố xác định khi nào có thể sử dụng hai mạng con đó, và khi nào không. Trước tiên, nếu giao thức định tuyến là classless, được sử dụng hai mạng này, nhưng nếu giao thức định tuyến là classful, không sử dụng hai mạng này. (Chương giao thức định tuyến và các khái niệm, giải thích các thuật ngữ giao thức định tuyến classless và classful; chi tiết không quan trọng bây giờ). Ngoài ra, nếu câu hỏi sử dụng VLSM Variable Length Subnet Mask mặt nạ mạng con với chiều dài thay đổi – thực hành cho sử dụng các mặt nạ mạng khác nhau trong cùng mạng classful – thì hai mạng đặc biệt này được dùng.

Nhân tố thứ ba xác định liệu hai mặt nạ mạng con nên được sử dụng dựa trên một câu lệnh cấu hình toàn cục: ip subnet zero. Nếu được cấu hình, câu lệnh này báo với bộ định tuyến rằng một địa chỉ IP trong một mạng con không có thể được cấu hình trên một giao tiếp. Nếu ngược lại không cấu hình – câu lệnh no ip subnet zero – thì một địa chỉ IP trong mạng con không không thể được cấu hình.

Chú ý rằng câu lệnh ip subnet zero là thiết lập mặc định trong Cisco IOS, có nghĩa rằng IOS cho phép mạng con không là mặc định. Vì thế nếu câu lệnh ip subnet zero được cấu hình, hay không liệt kê, thì mạng con không và các mạng đặc biệt khác, mạng con quảng bá, không được cho phép.

5.3.7. Ví dụ thực hành phân tích mặt nạ mạng con

Chương này sử dụng 5 địa chỉ IP và các mặt nạ khác nhau như ví dụ cho các phần khác nhau của việc phân tích mạng con. Để thực hành, xác định số bit mạng, mạng con và thiết bị, và số lượng mạng con và số lượng thiết bị trên mỗi mạng con, cho mỗi ví dụ sau đây:

- 8.1.4.5/16
- 130.4.102.1/24
- 199.1.1.100/24
- 130.4.102.1/22
- 199.1.1.100/27

Bảng 5.11. Thực hành phân mạng con

Địa chỉ	8.1.4.5/16	130.4.102.1/24	199.1.1.100/24	130.4.102.1/22	199.1.1.100/27
Mặt nạ	255.255.0.0	255.255.255.0	255.255.255.0	255.255.252.0	255.255.255.224
Số bit mạng	8	16	24	16	24
Số bit thiết bị	16	8	8	10	5
Số bit mạng con	8	8	0	6	3
Số thiết bị mạng con	$2^{16}-2$, hay 65.534	2^8-2 , hay 254	2^8-2 hay 254	$2^{10}-2$ hay 1022	2^5-2 hay 30
Số mạng con	2^8 hay 256	2^8 hay 256	0	2^6 hay 64	2^3 hay 8

5.4. LỰA CHỌN MẠNG CON PHÙ HỢP VỚI YÊU CẦU THIẾT KẾ

Phản thảo luận trước của chương về mặt nạ mạng con giả sử rằng đã lựa chọn mặt nạ mạng. Tuy nhiên, cần phải lựa chọn mặt nạ mạng để dùng. Phần này mô tả các khái niệm liên quan với việc lựa chọn mặt nạ mạng con tương ứng, dựa trên một tập hợp các yêu cầu thiết kế.

Khi thiết kế một liên mạng mới, phải chọn một mặt nạ mạng con để dùng, dựa trên các yêu cầu cho liên mạng mới này. Mặt nạ cần xác định để đủ các bit cần thiết cho phần thiết bị (dựa trên công thức $2^h - 2$) và đủ số mạng con khác nhau (dựa trên công thức 2^s hay $2^s - 2$, tùy thuộc liệu mạng con không và quảng bá có thể được dùng). Xem câu hỏi sau đây.

Hệ thống đang sử dụng mạng X lớp B, và cần 200 mạng con, với hầu hết 200 thiết bị cho mỗi mạng. Mặt nạ mạng nào sau đây có thể được sử dụng?

Để tìm câu trả lời đúng cho những loại câu hỏi dạng này, trước tiên cần quyết định bao nhiêu bit mạng con và thiết bị cần để thỏa mãn nhu cầu. Một cách cơ bản, số thiết bị mỗi mạng con là $2^h - 2$, trong đó h là số bit thiết

bị được xác định bởi mặt nạ mạng con. Giống như vậy, số mạng con trong một mạng, giả sử rằng cùng số mặt nạ mạng con được dùng cho tất cả các mạng, là 2^s , nhưng với s là số bit mạng con. Trường hợp khác, nếu câu hỏi nhấn mạnh rằng hai mạng con đặc biệt (mạng con không và mạng con quảng bá) không được dùng, nên sử dụng công thức $2^s - 2$. Ngay khi biết có bao nhiêu bit mạng con và thiết bị được yêu cầu, có thể chỉ ra mặt nạ phù hợp với mục tiêu thiết kế trong câu hỏi.

Trong một số trường hợp, yêu cầu thiết kế chỉ cho phép có thể một mặt nạ mạng con đơn, trong khi một số trường hợp khác, nhiều mặt nạ có thể phù hợp với yêu cầu thiết kế. Phản tiếp theo thể hiện một ví dụ trong đó chỉ một mặt nạ có thể được sử dụng, được theo bởi một phần sử dụng một ví dụ trong đó nhiều mặt nạ phù hợp với yêu cầu thiết kế.

5.4.1. Tìm mặt nạ mạng có thể

Sau đây ta hãy xem xét câu hỏi sau: điều kiện nào để mặt nạ mạng có thể phù hợp với các yêu cầu:

Mạng có thể sử dụng mạng lớp B 130.1.0.0. Mặt nạ mạng nào thỏa mãn yêu cầu rằng chuẩn bị cho phép đến 200 mạng con, với hầu hết 200 thiết bị mỗi mạng con này?

Trước tiên, cần chỉ ra có bao nhiêu bit mạng con cho phép với 200 mạng con. Có thể sử dụng công thức 2^s và đặt các giá trị s cho đến khi một trong các số ít nhất là 200. Trong trường hợp này, s sẽ là 8, vì 2^7 là 128 và 2^8 là 256, đủ để cung cấp cho các mạng con. Nói cách khác, cần ít nhất 8 bit cho mạng con để cung cấp cho 200 mạng con này.

Tương tự, để tìm số bit thiết bị được yêu cầu, lấy giá trị h trong công thức $2^h - 2$ cho đến khi tìm được giá trị nhỏ nhất của h có kết quả 200 hoặc hơn. Trong trường hợp này, h = 8.

Bảng 5.13 giúp cho ghi nhớ rõ hơn số bit sử dụng và số mạng con, số thiết bị được tạo ra.

Bảng 5.12. Ví dụ xác định địa chỉ mạng con

Số bit trong trường thiết bị hay mạng con	Số thiết bị tối đa ($2^n - 2$)	Số mạng con tối đa (2^8)
1	0	2
2	2	4
3	6	8
4	14	16
5	30	32
6	62	64
7	126	128
8	254	256
9	519	512
10	1022	1024
11	2046	2048
12	4094	4096
13	8190	8192
14	16.382	16.384

Tiếp tục ví dụ này với lớp mạng B 130.1.0.0, cần quyết định mặt nạ mạng nào cần được sử dụng, biết rằng phải có ít nhất 8 bit mạng con và 8 bit thiết bị để thỏa mãn nhu cầu thiết kế. Trong trường hợp này, vì mạng là lớp B, biết rằng nó có 16 bit dành cho mạng. Sử dụng kí tự N biểu diễn cho các bit mạng, S biểu diễn cho các bit mạng con và kí tự H biểu diễn cho các bit thiết bị, phần sau cho thấy kích thước của các trường khác nhau trong mặt nạ mạng này.

NNNNNNNN NNNNNNNN SSSSSSSS HHHHHHHH

Trong ví dụ này, vì có 16 bit mạng, 8 bit mạng con và 8 bit thiết bị được xác định, phải lấy tất cả 32 bit của cấu trúc địa chỉ. Vì thế, chỉ một mặt nạ mạng có thể làm việc. Để chỉ ra mặt nạ này, cần ghi lại mặt nạ mạng con 32 bit, áp dụng cho yếu tố và các mặt nạ mạng con sau đây:

Các bit mặt nạ mạng và mạng con, theo định nghĩa bảng 1. Tương tự, các bit thiết bị trong mặt nạ mạng con, theo định nghĩa tất cả là 0.

Vì thế, chỉ mặt nạ mạng phù hợp trong nhị phân, là:

11111111 11111111 11111111 00000000

Khi được chuyển sang thập phân, đó là 255.255.255.0 hay /24 trong định dạng tiền tố.

5.4.2. Trường hợp nhiều mặt nạ mạng

Trong hầu hết các trường hợp, có nhiều hơn một mặt nạ mạng thỏa mãn nhu cầu thiết kế. Mục này sẽ trình bày một ví dụ, với một số ý tưởng về cách tìm tất cả các mặt nạ mạng có thể. Ngoài ra cũng đưa ra một ví dụ, trong trường hợp này là với nhiều mặt nạ mạng con thỏa yêu cầu chỉ, như sau:

Thiết kế hệ thống liên mạng với yêu cầu 50 mạng con, trong đó mạng con lớn nhất có 200 thiết bị. Hệ thống liên mạng sử dụng mạng lớp B, và sẽ không có mạng nào lớn hơn thế. Một mặt nạ mạng con nào thỏa mãn các yêu cầu này?

Với thiết kế này, cần 16 bit mạng, vì thiết kế sử dụng một mạng lớp B, cần ít nhất 8 bit thiết bị, bởi $2^7 - 2 = 126$ (không đủ), và $2^8 - 2 = 254$, đủ cung cấp số thiết bị cần thiết cho mỗi mạng con. Tương tự, bây giờ chỉ cần 6 bit mạng con, bởi vì 6 bit mạng con cho phép 2^6 hay 64 mạng con, trong khi 5 bit mạng con chỉ cho phép 32 mạng con.

Nếu tuân theo cùng tiền trình xác định số bit của mạng, mạng con và thiết bị với các kí tự N, S và H, có định dạng sau đây:

NNNNNNNN NNNNNNNN SSSSSS__ HHHHHHHH

Định dạng này biểu diễn số bit mạng (16), mạng con (6) và thiết bị (8) tối thiểu. Tuy nhiên, nó để lại hai bit trống, hai bit cuối cùng trong octet thứ ba. Tại các bit này, viết một kí tự X cho bit tự do – các bit mà có thể hoặc là mạng con hay bit thiết bị. Trong ví dụ này, ta có:

NNNNNNNN NNNNNNNN SSSSSSXX HHHHHHHH

Các bit tự do, thể hiện là X, có thể là các bit thiết bị hay mạng con. Có 2 bit, vì thế có thể có 4 câu trả lời có thể tồn tại; tuy nhiên, chỉ

có ba câu trả lời đúng, vì một yếu tố rất quan trọng của các mặt nạ mạng là:

- Tất cả mặt nạ phải bắt đầu với một chuỗi các số 1 liên kề không ngắt quãng, được theo sau bởi một chuỗi các số 0 liên kề không ngắt quãng.
- Có thể thấy điều này thông qua ví dụ sau đây. Tiếp tục ở trên danh sách sau liệt kê các phương án, trong đó có ba phương án đúng, tất cả thể hiện các chuỗi 1 và 0 liên tiếp. Danh sách này cũng bao gồm một kết hợp không hợp lệ của các bit tự do – một câu trả lời thể hiện cho chuỗi các bit 0 và 1 không liên tục. Chú ý rằng các bit tự do được thể hiện đậm nét.

11111111 11111111 11111111 00000000

(8 bit mạng con, 8 thiết bị)

11111111 11111111 11111110 00000000

(7 bit mạng con, 9 thiết bị)

11111111 11111111 11111100 00000000

(6 bit mạng con, 10 thiết bị)

11111111 11111111 11111101 00000000

không hợp lệ.

Ba dòng đầu tiên vẫn thỏa mãn yêu cầu chuỗi các bit 1 được theo sau bởi chuỗi các bit 0 không ngắt quãng. Tuy nhiên, dòng cuối cùng trong danh sách thể hiện 22 bit 1, sau đó là một bit 0 được theo sau bởi một bit 1 khác, nên giá trị này không hợp lệ khi sử dụng làm mặt nạ mạng con.

Câu trả lời cuối cùng cho vấn đề này là danh sách ba mặt nạ mạng con hợp lệ trong thập phân hay định dạng tiền tố, như sau:

255.255.255.0 /24 8 bit mạng con, 8 bit thiết bị

255.255.254.0 /23 7 bit mạng con, 9 bit thiết bị

255.255.252.0 /22 6 bit mạng con, 10 bit thiết bị

5.4.3. Lựa chọn mặt nạ tối đa hóa số mạng con hay thiết bị

Cuối cùng, một câu hỏi đặt ra là làm thế nào để tìm mặt nạ mạng con phù hợp với yêu cầu cho trước, yêu cầu hoặc là cực đại hoặc là cực tiểu số thiết bị trên mỗi mạng con này. Để đơn giản hóa vấn đề, cần ghi nhớ các yêu cầu thiết kế như sau:

- **Mặt nạ với hầu hết các bit là mạng con:** mặt nạ trong đó các bit tự do được thiết lập sang bit 1, chính thế làm cho phần mạng con của địa chỉ lớn hơn, cực đại hóa bit của mạng con và cực tiểu số thiết bị trên mỗi mạng con.
- **Mặt nạ mạng với hầu hết các bit là thiết bị:** Mặt nạ trong đó các bit tự do được thiết lập là 0, chính vì thế làm cho phần thiết bị của địa chỉ lớn hơn, cực đại hóa số thiết bị trên mỗi mạng con và cực tiểu số mạng con.

Trong ví dụ trên, mặt nạ /24 cho số phần mạng con lớn nhất, còn mặt nạ /22 cho số lượng thiết bị lớn nhất. Đây là danh sách tóm tắt các bước lựa chọn một mặt nạ mạng con mới, dựa trên một tập các yêu cầu, giả sử rằng mạng con không và quảng bá có thể được dùng.

Bước 1: tìm số bit mạng (N) dựa trên quy tắc lớp A, B và C

Bước 2: Tìm số bit mạng con (S) dựa trên công thức 2^s , như là: Số lượng mạng con yêu cầu $\leq 2^s$.

Bước 3: Tìm số bit của thiết bị (H), dựa trên công thức $2^h - 2$, như là: Số lượng thiết bị yêu cầu $< 2^h - 2$.

Bước 4: Ghi lại bắt đầu từ trái, N + S bit 1

Bước 5: Ghi lại bắt đầu từ phải, H bit 0.

Bước 6: Nếu tổng số bit 1 và 0 nhỏ hơn 32

- Diền phần bit tự do X còn lại giữa các bit 1 và 0
- Diền tất cả kết hợp của các bit với các vị trí bit tự do phù hợp với yêu cầu cho một chuỗi liên tục không ngắt quảng các bit 1 trong mặt nạ.

Bước 7: Chuyển mặt nạ sang thập phân hay dạng tiền tố tương ứng.

Bước 8: Tìm kiếm mặt nạ cực đại hóa số mạng con, đặt mặt nạ là các bit 1, và mặt nạ mạng cực đại hóa số thiết bị, đặt mặt nạ là các bit 0.

5.5. PHÂN TÍCH CÁC MẠNG CON CÓ SẴN

Một trong những nhiệm vụ có liên quan đến phân mạng con thông thường nhất – là phân tích và hiểu một số yếu tố về các mạng con có sẵn. Có thể cho một địa chỉ IP và mặt nạ mạng con, và cần trả lời các câu hỏi về mạng con trong đó chứa địa chỉ – thỉnh thoảng được xem như là số mạng con dư thừa. Ví dụ như là “Số mạng con nào trong đó địa chỉ này thuộc về?” hay như là địa chỉ nào sau đây cùng mạng con với địa chỉ đã cho?

Phần này sẽ mô tả cách tìm ba yếu tố chính về mạng con bắt kì, khi biết một địa chỉ IP và mặt nạ mạng con cho một thiết bị trên mạng con ấy.

- Số mạng con (địa chỉ mạng con)
- Địa chỉ quảng bá mạng con cho mạng con đó
- Khoảng địa chỉ IP có thể sử dụng trong mạng con đó

Sau đây nghiên cứu tiên trình tìm kiếm ba yếu tố về một mạng con này sử dụng nhị phân. Sau đó là tiến trình tìm kiếm thập phân giúp tìm ra cùng câu trả lời với thời gian ngắn hơn.

5.5.1. Tiến trình nhị phân tìm kiếm số mạng con

Chi số mạng con, hay địa chỉ mạng con được dùng một số thập phân có chấm để biểu diễn. Thường thấy các chi số mạng con được viết trong tài liệu và trong bảng định tuyến của router. Mỗi mạng con có thể chứa hàng trăm các địa chỉ IP liên tiếp, nhưng một router thường giới hạn một khoảng địa chỉ IP như là một chi số mạng con và mặt nạ mạng trong bảng định tuyến IP của nó. Liệt kê chi số mạng con và mặt nạ mạng trong bảng định tuyến cho phép một router xem như đó là một mạng con – tức là một khoảng liên tiếp các địa chỉ IP – mà không phải yêu cầu một mục trong bảng định tuyến cho mỗi địa chỉ thiết bị độc lập.

Phản đầu chương, ta đã biết về các máy tính thực hiện các phép toán Boolean AND của một địa chỉ IP và mặt nạ để tìm chỉ số mặt nạ mạng con. Có thể sử dụng cùng quy trình này, như sau:

Bước 1: Chuyển địa chỉ IP từ thập phân sang nhị phân

Bước 2: Chuyển mặt nạ mạng sang nhị phân, viết số này bên dưới địa chỉ IP từ bước 1.

Bước 3: Thực hiện phép toán bit Boolean AND giữa hai số. Làm như sau:

- AND bit đầu tiên của địa chỉ với bit đầu tiên của mặt nạ mạng, ghi lại kết quả bên dưới các số này.
- AND bit thứ hai của mỗi số, ghi lại kết quả như trên
- Lặp lại mỗi cặp bit, kết quả là số nhị phân 32 bit.

Bước 4: Chuyển số nhị phân kết quả, 8 bit mỗi lần, ngược lại số thập phân. Giá trị này chính là chỉ số mạng con cần tìm.

Bảng sau đây cho thấy các kết quả qua tất cả bốn bước, với 5 ví dụ khác nhau. Bảng này cũng bao gồm phiên bản nhị phân của địa chỉ và mặt nạ và các kết quả của phép toán Boolean AND.

Bảng 5.13. Ví dụ tìm kiếm địa chỉ mạng con sử dụng nhị phân (1)

Địa chỉ	8.1.4.5	00001000 00000001 00000100 00000101
Mặt nạ	255.255.0.0	11111111 11111111 00000000 00000000
Kết quả AND	8.1.0.0	00001000 00000001 00000000 00000000

Bảng 5.14. Ví dụ tìm kiếm địa chỉ mạng con sử dụng nhị phân (2)

Địa chỉ	130.4.102.1	10000010 00000100 01101010 00000001
Mặt nạ	255.255.255.0	11111111 11111111 11111111 00000000
Kết quả AND	130.4.102.0	10000010 00000100 01101010 00000000

Bảng 5.15. Ví dụ tìm kiếm địa chỉ mạng con sử dụng nhị phân (3)

Địa chỉ	199.1.1.100	11000111 00000001 00000001 10101000
Mặt nạ	255.255.255.0	11000111 00000001 00000001 00000000
Kết quả AND	199.1.1.0	11000111 00000001 00000001 00000000

Bảng 5.16. Ví dụ tìm kiếm địa chỉ mạng con sử dụng nhị phân (4)

Địa chỉ	130.4.102.1	10000010 00000100 01100110 00000001
Mặt nạ	255.255.252.0	11111111 11111111 11111100 00000000
Kết quả AND	130.4.100.0	10000010 00000100 01100110 00000000

Bảng 5.17. Ví dụ tìm kiếm địa chỉ mạng con sử dụng nhị phân (5)

Địa chỉ	199.1.1.100	11000111 00000001 00000001 01100100
Mặt nạ	255.255.255.224	11111111 11111111 11111111 11100000
Kết quả AND	199.1.1.96	11000111 00000001 00000001 01100000

Bước cuối cùng của quy trình – chuyển từ số nhị phân ngược lại số thập phân có thể khó khăn với nhiều người mới quen với phân mạng. Rắc rối thường xảy ra khi biên giữa phần mạng con và phần thiết bị của địa chỉ đó là nằm giữa một byte, xảy ra khi mặt nạ mạng có giá trị giữa 0 và 255. Ví dụ, với mạng 130.4.102.1, mặt nạ 255.255.255.0 (bảng 5.16), 6 bit đầu tiên của octet thứ ba ám chỉ trường mạng con, và 2 bit còn lại của octet thứ ba, cộng với toàn thể octet thứ tư, ám chỉ trường thiết bị. Vì những yếu tố này, một số thường chuyển đổi phần mạng con 6 bit từ nhị phân sang thập phân, và sau đó chuyển đổi phần thiết bị 10 sang thập phân. Tuy nhiên, khi chuyển đổi nhị phân sang thập phân, để tìm địa chỉ IP thập phân có chấm, luôn chuyển đổi toàn thể octet, thậm chí nếu phần octet chứa cả phần địa chỉ mạng con và phần thiết bị của địa chỉ đó.

Vì thế trong ví dụ ở bảng trên, chỉ số mạng con (130.4.100.0) trong nhị phân là 1000 (0010 0000 0100 0110 0100 0000 0000). Toàn bộ octet thứ ba được thể hiện in đậm, được chuyển thành 100 trong thập phân. Khi chuyển đổi toàn thể số này, mỗi tập 8 bit được chuyển sang thập phân, cho 130.4.100.0

5.5.2. Tìm kiếm chỉ số mạng con: Dạng nhị phân rút gọn

Có thể tìm thấy một công thức đơn giản hơn để chuyển đổi hai số thập phân có chấm sang nhị phân, thực hiện phép AND Boolean cho 32 bit, sau đó chuyển ngược kết quả lại dạng thập phân có chấm. Tuy nhiên, khi thực hành tiền trình này, nên chú ý một số xu hướng quan trọng, có

thể giúp tối ưu hóa và đơn giản quy trình nhị phân. Phần này chú ý một cách rõ nét đến những xu hướng này và cho thấy cách có thể rút ngắn quy trình Boolean AND xuống.

Trước tiên, xét các octet tách biệt. Bất kì octet tách biệt của bất kì địa chỉ IP nào, khi được AND với một chuỗi nhị phân 8 bit 1 từ mặt nạ, có kết quả là cùng giá trị với nó. Dĩ nhiên, khi mặt nạ có một octet có giá trị thập phân 255, số này biểu diễn cho 8 bit nhị phân 1. Kết quả là với bất kì octet nào trong đó mặt nạ thể hiện số thập phân giá trị 255, kết quả phép AND với địa chỉ IP tương ứng là không thay đổi.

Ví dụ, octet đầu tiên của ví dụ trên 199.1.1.100 mặt nạ 255.255.255.224 có một địa chỉ IP giá trị 199 (11000111), mặt nạ 255 (11111111). Thực hiện phép AND giữa hai octet này, có kết quả vẫn là số 199. Vì vậy, nếu bất kì octet nào của mặt nạ có chứa 255, chỉ việc giữ nguyên giá trị octet tương ứng của địa chỉ IP đó.

Hoàn toàn tương tự cho các octet của mặt nạ có giá trị là 0. Khi đó chỉ việc thay thế octet tương ứng của địa chỉ IP giá trị là 0.

Ví dụ địa chỉ 172.16.1.5 có mặt nạ mạng 255.255.0.0. Nhận xét rằng hai octet cuối cùng của mặt nạ có giá trị thập phân là 0 (nhị phân tương ứng là 00000000) nên khi thực hiện phép AND với bất kì địa chỉ IP nào cũng cho kết quả là 0. Như vậy, có thể xác định kết quả cho hai octet tương ứng trên địa chỉ IP cần tìm đều có giá trị thập phân là 0.

Hai yếu tố này giúp phát triển một quy trình mới như sau:

Bước 1: Ghi lại mặt nạ thập phân trên hàng đầu tiên của bảng và địa chỉ IP thập phân trên hàng thứ hai

Bước 2: Với bất kì octet của mặt nạ có giá trị thập phân 255, chép lại giá trị thập phân octet của địa chỉ IP thành kết quả octet của chỉ số mạng con.

Bước 3: Tương tự, với bất kì octet của mặt nạ có giá trị thập phân là 0, ghi lại giá trị thập phân 0 cho cùng octet của chỉ số mạng con.

Bước 4: Nếu chỉ số mạng con còn có một octet còn lại cần được điền vào, thực hiện như sau:

- a. Chuyển một octet còn lại của địa chỉ IP đó sang nhị phân
- b. Chuyển một octet còn lại của mặt nạ đó sang nhị phân
- c. AND hai số 8 bit đó lại với nhau
- d. Chuyển số nhị phân 8 bit đó sang thập phân, và đặt giá trị trong một octet còn lại vào chỉ số mạng con.

Sử dụng phương pháp này, khi mặt nạ chỉ có 255 và 0, có thể tìm chỉ số nhị phân mà không phải thực hiện bất kì phép toán nhị phân nào. Trong các trường hợp khác, có thể tìm ba octet một cách dễ dàng, và sau đó chỉ thực hiện phép toán AND trên octet còn lại giữa địa chỉ IP và mặt nạ mạng con, để hoàn tất chỉ số mạng con này.

5.5.3. Tìm kiếm nhị phân địa chỉ quảng bá mạng con

Địa chỉ quảng bá mạng con, thỉnh thoảng được gọi là địa chỉ quảng bá trực tiếp, có thể được sử dụng để gửi một gói tin đến mọi thiết bị trong một mạng con đơn. Lấy ví dụ, mạng con 8.1.4.0/24 có một địa chỉ quảng bá mạng con là 8.1.4.255. Một gói tin được gửi đến một địa chỉ đích của 8.1.4.255 sẽ được chuyển qua liên mạng, cho đến khi nó đến router có kết nối đến mạng con đó. Router cuối cùng, khi chuyển gói tin vào mạng con này, đóng gói gói tin trong frame quảng bá liên kết – dữ liệu. Lấy ví dụ, nếu mạng con này tồn tại trên Ethernet LAN, gói tin sẽ được chuyển bên trong một Ethernet frame với địa chỉ Ethernet là FFFF.FFFF.FFFF.

Theo định nghĩa, một địa chỉ quảng bá mạng con có cùng giá trị với chỉ số mạng con trong mạng và phần mạng con của địa chỉ đó, nhưng với tất cả các bit 1 trong phần thiết bị của địa chỉ quảng bá đó. Chỉ số mạng con, theo định nghĩa, xuất hiện với tất cả các bit nhị phân 0 trong phần thiết bị. Nói cách khác, chỉ số mạng con là đầu thấp nhất của các địa chỉ, và địa chỉ quảng bá của mạng con là đầu cao nhất của khoảng địa chỉ đó.

Có một công thức toán học để tính địa chỉ quảng bá của mạng con dựa trên chỉ số mạng con, nhưng có một quy trình dễ hơn, đặc biệt nếu đã quen với chỉ số mạng con trong nhị phân:

Để tính địa chỉ quảng bá mạng con, nếu đã biết phiên bản nhị phân của chỉ số mạng con, thay đổi tất cả giá trị bit thiết bị trong chỉ số mạng con đó sang bit nhị phân 1.

Cũng đã biết cách xác định các bit thiết bị, dựa trên giá trị nhị phân 0 của các bit mặt nạ. Có thể kiểm tra toán đơn giản sau khi tính toán địa chỉ quảng bá mạng con trong bảng sau. Các phần thiết bị của các địa chỉ, mặt nạ, chỉ số mạng con, và các địa chỉ quảng bá được in đậm.

Bảng 5.18. Ví dụ xác định địa chỉ quảng bá (1)

Địa chỉ	8.1.4.5	00001000 00000001 00000100 00000101
Mặt nạ	255.255.255.0	11111111 11111111 11111111 00000000 00000000
Kết quả AND	8.1.0.0	00001000 00000001 00000000 00000000
Quảng bá	8.1.255.255	00001000 00000001 11111111 11111111

Bảng 5.19. Ví dụ xác định địa chỉ quảng bá (2)

Địa chỉ	130.4.102.1	10000010 00000100 01100110 00000001
Mặt nạ	255.255.255.0	11111111 11111111 11111111 00000000 00000000
Kết quả AND	130.4.102.0	10000010 00000100 01100110 00000000
Quảng bá	130.4.102.255	10000010 00000100 01100110 11111111

Bảng 5.20. Ví dụ xác định địa chỉ quảng bá (3)

Địa chỉ	199.1.1.100	11000111 00000001 00000001 01100100
Mặt nạ	255.255.255.0	11111111 11111111 11111111 00000000 00000000
Kết quả AND	199.1.1.0	11000111 00000001 00000001 00000000
Quảng bá	199.1.1.255	11000111 00000001 00000001 11111111

Bảng 5.21. Ví dụ xác định địa chỉ quảng bá (4)

Địa chỉ	130.4.102.1	10000010 00000100 01100110 00000001
Mặt nạ	255.255.252.0	11111111 11111111 11111100 00000000 00000000
Kết quả AND	130.4.100.0	10000010 00000100 01100100 00000000
Quảng bá	130.4.100.255	10000010 00000100 01100100 00000000

Bảng 5.22. Ví dụ xác định địa chỉ quảng bá (5)

Địa chỉ	199.1.1.100	11000111 00000001 00000001 01100100
Mặt nạ	255.255.255.224	11111111 11111111 11111111 11100000 00000000
Kết quả AND	199.1.1.96	11000111 00000001 00000001 01100000
Quảng bá	199.1.1.127	11000111 00000001 00000001 01111111

Bằng cách kiểm tra các địa chỉ quảng bá mạng con trong nhị phân, có thể thấy rằng chúng được xác định với các chỉ số mạng con, ngoại trừ tất cả các bit thiết bị có một giá trị nhị phân 1 thay vì giá trị nhị phân 0.

Để tham khảo, tiến trình sau đây tóm tắt các khái niệm được mô tả hướng dẫn làm thế nào tìm địa chỉ quảng bá mạng con.

Bước 1: Viết chỉ số mạng con (hay địa chỉ IP), và mặt nạ mạng con, trong dạng nhị phân. Chắc chắn rằng kí tự nhị phân đứng thẳng hàng trực tiếp với nhau.

Bước 2: Tách phần thiết bị của những chỉ số này khỏi phần mạng/mạng con bằng các vẽ một đường thẳng đứng. Đặt đường này giữa bit 1 tận cùng phải và bit 0 tận cùng trái.

Bước 3: Để tìm địa chỉ quảng bá mạng con, trong nhị phân:

- Sao chép các bit của chỉ số mạng con (hay địa chỉ IP) đến trái của đường thẳng đứng này.
- Ghi các bit 1 nhị phân sang bên phải của dòng thẳng.

Bước 4: Chuyển đổi địa chỉ quảng bá mạng con nhị phân 32 bit sang thập phân, 8 bit một lần, bỏ qua đường gạch thẳng.

5.5.4. Tìm khoảng địa chỉ IP hợp lệ trong một mạng con

Ngoài ra, cũng cần phải chỉ ra địa chỉ IP nào thuộc mạng con hoặc không. Như đã biết làm thế nào để thực hiện phân chia “cứng” cho câu trả lời đó. Trong mọi mạng con, hai chỉ số ấn định trước và không được sử dụng như là địa chỉ IP cho các thiết bị là chỉ số mạng con và địa chỉ quảng bá cho mạng con đó. Chỉ số mạng con là số nhỏ nhất trong mạng con đó, và địa chỉ quảng bá là số lớn nhất. Vì thế, khoảng địa chỉ IP hợp lệ bắt đầu với địa chỉ IP lớn hơn 1 so với chỉ số mạng con và kết thúc nhỏ hơn 1 so với địa chỉ quảng bá.

Đây là các bước tính địa chỉ IP hợp lệ nếu đã biết trước địa chỉ mạng con và địa chỉ quảng bá cho mạng con đó.

Bước 1: Để tìm kiếm địa chỉ IP đầu tiên, sao chép chỉ số mạng con, nhưng thêm 1 vào octet thứ tư.

Bước 2: Đề tìm địa chỉ IP cuối cùng, sao chép địa chỉ quảng bá mạng con, nhưng trừ đi 1 từ octet thứ tư.

Quy trình toán học khá rõ ràng; tuy nhiên, cần thận với khi thêm (*Bước 1*) và khi trừ (*Bước 2*) chỉ trong octet thứ tư – không quan tâm đến lớp mạng của địa chỉ và mặt nạ mạng con nào được sử dụng. Các bảng sau tóm tắt các câu trả lời cho 5 ví dụ được dùng trong chương này.

Bảng 5.23. Quy trình tìm khoảng địa chỉ cho mạng con(1)

Octet	1	2	3	4
Địa chỉ	8	1	4	5
Mặt nạ	255	255	0	0
Địa chỉ mạng con	8	1	0	0
Địa chỉ đầu tiên	8	1	0	1
Quảng bá	8	1	255	255
Địa chỉ cuối	8	1	255	254

Bảng 5.24. Quy trình tìm khoảng địa chỉ cho mạng con(2)

Octet	1	2	3	4
Địa chỉ	130	41	102	1
Mặt nạ	255	255	255	0
Địa chỉ mạng con	130	4	102	0
Địa chỉ đầu tiên	130	4	102	1
Quảng bá	130	4	102	255
Địa chỉ cuối	130	4	102	254

Bảng 5.25. Quy trình tìm khoảng địa chỉ cho mạng con(3)

Octet	1	2	3	4
Địa chỉ	199	1	1	100
Mặt nạ	255	255	255	0
Địa chỉ mạng con	199	1	1	0
Địa chỉ đầu tiên	199	1	1	1
Quảng bá	199	1	1	255
Địa chỉ cuối	199	1	1	254

Bảng 5.26. Quy trình tìm khoảng địa chỉ cho mạng con(4)

Octet	1	2	3	4
Địa chỉ	130	4	102	1
Mặt nạ	255	255	252	0
Địa chỉ mạng con	130	4	100	0
Địa chỉ đầu tiên	130	4	100	1
Quảng bá	130	4	103	255
Địa chỉ cuối	130	4	103	254

Bảng 5.27. Quy trình tìm khoảng địa chỉ cho mạng con(5)

Octet	1	2	3	4
Địa chỉ	199	1	1	100
Mặt nạ	255	255	255	224
Địa chỉ mạng con	199	1	1	96
Địa chỉ đầu tiên	199	1	1	97
Quảng bá	199	1	1	127
Địa chỉ cuối	199	1	1	126

5.6. TIỀN TRÌNH THẬP PHÂN TÌM KIÉM MẠNG CON, ĐỊA CHỈ QUẢNG BÁ VÀ KHOẢNG ĐỊA CHỈ

Sử dụng toán nhị phân được yêu cầu để tìm kiếm chỉ số mạng con và địa chỉ quảng bá khiếu nại nghĩ về phân mạng con, thực sự giúp hiệu về phân mạng tốt hơn. Tuy nhiên, thông thường việc thực hiện các phép toán thập phân lại quen thuộc và dễ dàng hơn nhiều so với làm việc với toán nhị phân. Phản này mô tả một số quy trình thập phân cho việc tìm kiếm chỉ số mạng và địa chỉ quảng bá mạng con. Từ đó, có thể dễ dàng tìm kiếm khoảng địa chỉ có thể gán trong mạng con đó, như mô tả trong phần trước đây.

5.6.1. Quy trình thập phân với các mặt nạ đơn giản

Có ba mặt nạ mạng đơn giản: 255.0.0.0, 255.255.0.0 và 255.255.255.0 chỉ sử dụng các giá trị 255 và 0. Gọi là các mặt nạ “đơn giản”, bởi vì có thể tìm thấy chỉ số mạng con và địa chỉ quảng bá một cách dễ dàng, mà

không phải thực hiện bất kì phép toán thực sự nào. Nhiều người thấy một cách trực quan làm thế nào tìm câu trả lời với các mặt nạ đơn giản, nếu thế thì bỏ qua phần này để đến phần “Quy trình thập phân với các mặt nạ phức tạp”, nếu đã biết làm thế nào tìm chi số mạng con và địa chỉ quảng bá.

Với ba loại mặt nạ đơn giản này, 255.0.0.0 không dẫn đến bất kì mạng con nào. Chính vì thế, phần này chỉ mô tả làm thế nào sử dụng hai mặt nạ đơn giản có thể được dùng cho phân mạng – 255.255.0.0 và 255.255.255.0.

Tiến trình này khá đơn giản. Để tìm chi số mạng con khi được cho một địa chỉ IP và một mặt nạ của 255.255.0.0 hay 255.255.255.0, thực hiện như sau:

Bước 1: Với mỗi octet mặt nạ mạng con có giá trị 255, sao chép giá trị địa chỉ IP octet đó.

Bước 2: Với các octet còn lại của mặt nạ mạng con có giá trị 0, viết lại thành số 0.

Ngay sau khi biết chi số mạng và địa chỉ quảng bá, có thể dễ dàng tìm thấy các địa chỉ IP đầu tiên và cuối cùng trong mạng con sử dụng cùng ý nghĩa đơn giản như đã xem xét trước đây.

- Để tìm địa chỉ IP hợp lệ đầu tiên trong mạng con đó, sao chép chi số mạng con, nhưng thêm 1 vào octet thứ tư.
- Để tìm địa chỉ IP hợp lệ cuối cùng trong mạng con, sao chép địa chỉ quảng bá, nhưng trừ đi 1 trong octet thứ tư.

5.6.2. Tiến trình thập phân với các mặt nạ phức tạp

Khi mặt nạ mạng không phải là 255.0.0.0, 255.255.0.0 hay 255.255.255.0, nhận thấy mặt nạ này phức tạp hơn, nguyên nhân là vì hầu hết mọi người không thể dễ dàng tìm ra chi số mạng con và địa chỉ quảng bá mà không sử dụng toán nhì phân.

Có thể sử dụng các quy trình nhị phân trước đây trong chương này, vào mọi lúc, khi mặt nạ đơn giản hay phức tạp – và nhất định tìm thấy các câu trả lời đúng. Tuy nhiên, hầu hết mọi người có thể tìm thấy câu trả

lời đúng nhanh chóng hơn nhiều bằng cách bỏ ít thời gian luyện tập quy trình thập phân được mô tả trong phần này.

Quy trình thập phân sử dụng một bảng để giúp tổ chức vấn đề, một ví dụ của nó được tìm thấy trong bảng sau, xem bảng này như là sơ đồ mạng con.

Bảng 5.28. Quy trình thập tìm khoảng địa chỉ cho mạng con

Octet	1	2	3	4
Địa chỉ				
Mặt nạ				
Địa chỉ mạng con				
Địa chỉ đầu tiên				
Quảng bá				
Địa chỉ cuối				

Các bước sau đây liệt kê quy trình thông thường cho việc tìm kiếm chỉ số mạng con, sử dụng quy trình thập phân, giả sử rằng một mặt nạ con phức tạp được dùng.

Bước 1: Ghi lại mặt nạ mạng con trong hàng trống đầu tiên của bảng mạng con và địa chỉ IP vào hàng trống thứ hai.

Bước 2: Tìm octet trong đó giá trị mặt nạ mạng con là 255 hay 0. Octet này được gọi là octet đơn giản. Vẽ một hình vuông đen quanh cột octet đơn giản của bảng này, từ đỉnh xuống đáy.

Bước 3: Ghi lại giá trị chỉ số mạng con cho octet không đơn giản, như sau:

- Với mỗi octet sang trái của hình vuông được vẽ trong bước 2: sao chép giá trị địa chỉ IP cho cùng octet.
- Với mỗi octet sang phải của hình vuông: ghi lại giá trị thập phân 0.

Bước 4: Tại điểm này, hàng chỉ số mạng con của bảng mạng con có ba octet được điền vào, còn lại chỉ octet đơn giản. Để tìm giá trị chỉ số mạng con cho octet đơn giản này:

- Tính toán số bước nhảy bằng cách trừ 256 cho giá trị octet đơn giản của mặt nạ mạng con.
- Tính bội số của số bước nhảy này, bắt đầu từ 0 lên 256.
- Tìm giá trị chỉ số đơn giản của octet mạng con; như sau tìm bội số của bước nhảy, gần nhưng không lớn hơn giá trị octet địa chỉ IP đơn giản.

Như có thể thấy, quy trình này khá chí tiết, nhưng cũng khá phức tạp. Điểm chính của ba bước đầu tiên – vẽ một hình vuông xung quanh octet đơn giản – sử dụng cùng ý nghĩa với mặt nạ đơn giản. Bước thứ tư là chí tiết, nhưng nó có thể được học, làm chủ, và quyên khi thấy các mẫu thập phân sau phân mạng.

Lấy ví dụ sau đây, xem xét địa chỉ 130.4.102.1 với mặt nạ 255.255.252.0 Vì octet thứ ba không phải là 0 hay 255, sẽ tiến hành quy trình thập phân với octet này. Với bước 1, tạo một bảng mạng con và điền mặt nạ và địa chỉ trong hai hàng đầu tiên. Trong bước 2, vẽ một hình vuông quanh cột của octet thứ ba trong bảng mạng con. Trong bước 3, điền vào hai octet đầu tiên của chỉ số mạng con bằng cách sao chép địa chỉ IP của hai octet đầu tiên và ghi 0 vào octet thứ tư. Bảng sau cho thấy kết quả của những bước này.

Bảng 5.29. Ví dụ quy trình thập phân tìm khoảng địa chỉ cho mạng con (1)

Octet	1	2	3	4
Địa chỉ	255	255	252	0
Mặt nạ	130	4	102	1
Số mạng con	130	4		0
Địa chỉ đầu tiên				
Quảng bá				
Địa chỉ cuối				

Bước cuối cùng chỉ là bước nhò, nhưng ít nhất nó cho phép sử dụng toán thập phân, thay vì nhị phân, để tìm kiếm chỉ số mạng con. Trong

trường hợp này, số bước nhảy là $256 - 252 = 4$. Sau đó có thể tìm bội số của số bước nhảy gần với octet của địa chỉ, nhưng nhỏ hơn hay bằng nó. Trong ví dụ này, 100 là bội số của số bước nhảy ($100 = 4 \times 25$), và bội số này nhỏ hơn hay bằng với 102. Bội số cao hơn kế tiếp là số 104, lớn hơn 102, do vậy không phải là số đúng, vì thế cần diền 100 vào octet thứ ba của chỉ số mạng con trong bảng trên.

Ngay sau khi biết chỉ số mạng con, có thể dễ dàng tìm thấy địa chỉ IP hợp lệ đầu tiên trong mạng con:

Để tìm địa chỉ IP hợp lệ đầu tiên, sao chép mặt nạ mạng, nhưng thêm 1 vào octet thứ tư.

Bảng 5.30. Ví dụ quy trình thập phân tìm khoảng địa chỉ cho mạng con (2)

Octet	1	2	3	4	Chú thích
Địa chỉ	130	4	102	1	
Mặt nạ	255	255	252	0	
Địa chỉ mạng con	130	4	100	0	Bước nhảy: $256 - 252 = 4$. 100 là bội số gần nhất của 4, nhưng lại nhỏ hơn 102
Địa chỉ đầu tiên	130	4	100	1	Thêm 1 vào octet cuối cùng
Quảng bá					
Địa chỉ cuối					

5.6.3. Quy trình thập phân tìm kiếm địa chỉ quảng bá

Nếu sử dụng tiến trình thập phân để tìm chỉ số mạng con, tìm địa chỉ quảng bá mạng con cách đơn giản nhất là sử dụng toán thập phân. Khi tìm thấy địa chỉ quảng bá, đã biết làm thế nào để tìm thấy địa chỉ IP có thể sử dụng được trong mạng con đó. Để tìm địa chỉ quảng bá mạng con sau khi tìm chỉ số mạng, giả sử với mạng phức tạp, sử dụng quy trình sau đây:

Bước 1: Diền các octet địa chỉ quảng bá mạng con vào bên trái của hình vuông bằng cách sao chép các octet của cùng chỉ số mạng con.

Bước 2: Diền các octet địa chỉ quảng bá vào bên phải của hình vuông với thập phân 255.

Bước 3: Tìm giá trị cho octet đơn giản bằng cách thêm giá trị chỉ số mạng con vào octet đơn giản với số bước nhảy và trừ đi 1.

Để điền vào octet đang quan tâm địa chỉ quảng bá, sử dụng số bước nhảy. Số bước nhảy là 256 trừ đi octet đang quan tâm của mặt nạ. Trong ví dụ này, số bước nhảy là 4, sau đó thêm số bước nhảy vào giá trị octet đang quan tâm với chỉ số mạng con và trừ đi 1. Kết quả của giá trị địa chỉ quảng bá trong octet đang quan tâm. Trong trường hợp này, giá trị này là:

$$100 \text{ (octet thứ ba của chỉ số mạng)} + 4 \text{ (số bước nhảy)} - 1 = 103$$

Bảng 5.31. Ví dụ quy trình thập phân tìm khoảng địa chỉ cho mạng con (3)

Octet	1	2	3	4	Chú thích
Địa chỉ	130	4	102	1	
Mặt nạ	255	255	252	0	
Địa chỉ mạng con	130	4	100	0	Bước nhảy: $256 - 252 = 4$. 100 là bội số gần nhất của 4, nhưng lại nhỏ hơn 102
Địa chỉ đầu tiên	130	4	100	1	Thêm 1 vào octet cuối cùng
Quảng bá	130	4	103	254	Trừ 1 từ địa chỉ quảng bá của mạng
Địa chỉ cuối	130	4	103	255	Địa chỉ quảng bá mạng con, lấy bước nhảy cộng với địa chỉ mạng, trừ đi 1

5.6.4. Tổng kết quy trình thập phân để tìm mạng con, quảng bá và khoảng địa chỉ IP

Bước 1: Viết mặt nạ mạng con trong hàng trống đầu tiên của bảng mạng con và địa chỉ IP vào hàng thứ hai

Bước 2: Tìm octet trong đó giá trị mặt nạ mạng con không phải là 255 hay 0. Octet này được gọi là octet đang quan tâm. Về một hình chữ nhật đậm quanh cột octet đang quan tâm của bảng này, từ trên xuống dưới

Bước 3: Ghi lại giá trị số mạng con của các octet không quan tâm, như sau:

- Với mỗi octet bên trái của hình chữ nhật được vẽ trong bước 2: Sao chép giá trị địa chỉ IP trong cùng octet đó.
- Với mỗi octet bên phải hình vuông: ghi lại giá trị thập phân 0.

Bước 4: Để tìm giá trị chỉ số mạng con cho octet đang quan tâm:

- Tính chỉ số bước nhảy bằng cách trừ 256 với giá trị octet đang quan tâm của mặt nạ mạng.
- Tính bội số của số bước nhảy, từ 0 đến 256.
- Ghi lại giá trị octet đang quan tâm, được tính như sau: tìm bội số của số bước nhảy, gần với nhưng không lớn hơn giá trị octet đang quan tâm của địa chỉ IP đó.

Bước 5: Tìm kiếm địa chỉ quảng bá mạng con, như sau:

- Với mỗi octet mặt nạ mạng con bên trái của hình chữ nhật: Sao chép giá trị octet của địa chỉ IP
- Với mỗi octet mặt nạ mạng con bên phải của hình chữ nhật: Ghi lại giá trị 255.
- Tìm giá trị của octet đang quan tâm bằng cách thêm giá trị chỉ số mạng con vào octet đang quan tâm với số bước nhảy, và trừ 1.

Bước 6: Để tìm địa chỉ IP đầu tiên, sao chép chỉ số mạng con thập phân mạng con, trừ đi 1 ở octet thứ tư.

Bước 7: Để tìm địa chỉ IP cuối cùng, sao chép địa chỉ quảng bá thập phân mạng con, trừ đi 1 ở octet thứ tư.

5.7. CÂU HỎI VÀ BÀI TẬP CHƯƠNG 5

Câu 1. Mạng nào sau đây là mạng IP dành riêng?

- 172.31.0.0
- 172.32.0.0
- 192.168.255.0
- 192.1.168.0

e. 11.0.0.0

Câu 2. Kết quả phép AND nhị phân giữa địa chỉ IP 150.150.4.100 và mặt nạ 255.255.192.0 là?

- a. 1001 0110 1001 0110 0000 0100 0110 0100
- b. 1001 0110 1001 0110 0000 0000 0000 0000
- c. 1001 0110 1001 0110 0000 0100 0000 0000
- d. 1001 0110 0000 0000 0000 0000 0000 0000

Câu 3. Điều nào sau đây tương ứng mặt nạ mạng con 255.255.248.0, nhưng ở cú pháp tiền tố

- a. /248
- b. /24
- c. /28
- d. /21
- e. /20
- f. /23

Câu 4. Nếu mặt nạ 255.255.255.128 được sử dụng với một mạng lớp B, có bao nhiêu mạng con tồn tại, và có bao nhiêu máy trên mỗi mạng?

- a. 256 và 256
- b. 256 và 254
- c. 62 và 1022
- d. 1022 và 62
- e. 512 và 126
- f. 126 và 510

Câu 5. Một mạng lớp B cần được phân thành 100 mạng con và 100 máy trên/mạng. Với thiết kế này, nếu có nhiều mặt nạ phù hợp cho những yêu cầu thiết kế đó, chọn mặt nạ tối thiểu số máy trên mỗi mạng con. Mặt nạ nào sau đây phù hợp với tiêu chuẩn thiết kế?

- a. 255.225.255.0
- b. /23
- c. /26

d. 255.255.252.0

Câu 8. Nếu mặt nạ 255.255.255.240 được sử dụng với mạng lớp C, có bao nhiêu mạng con tồn tại, với bao nhiêu máy trên mỗi mạng?

- a. 16 và 16
- b. 16 và 14
- c. 16 và 14
- d. 8 và 32
- e. 32 và 8

Câu 7. Mật khẩu mạng con nào sau đây cho phép một mạng lớp B có đến 150 máy trên mỗi mạng con và hỗ trợ 164 mạng con?

- a. 255.0.0.0
- b. 255.255.0.0
- c. 255.255.255.0
- d. 255.255.192.0
- e. 255.255.240.0
- f. 255.255.252.0

Câu 8. Mật khẩu mạng con nào sau đây cho phép một mạng lớp A có đến 150 máy trên mỗi mạng con và hỗ trợ 163 mạng con?

- a. 255.0.0.0
- b. 255.255.0.0
- c. 255.255.255.0
- d. 255.255.192.0
- e. 255.255.252.0
- f. 255.255.255.192

Câu 9. Địa chỉ IP nào sau đây không cùng mạng con với 192.4.80.80, mặt nạ 255.255.255.0?

- a. 190.4.80.1
- b. 190.4.80.1

- c. 190.4.80.50
- d. 190.4.80.100
- e. 190.4.80.200
- f. 190.4.90.1
- g. 10.1.1.1

Câu 10. Địa chỉ IP nào sau đây không cùng mạng con với 190.4.80.80, mặt nạ 255.255.240.0?

- a. 190.4.80.1
- b. 190.4.80.50
- c. 190.4.80.100
- d. 190.4.80.200
- e. 190.4.90.1
- f. 10.1.1.1

Câu 11. Địa chỉ IP nào sau đây không cùng mạng con với 190.4.80.80/25

- a. 190.4.80.1
- b. 190.4.80.50
- c. 190.4.80.100
- d. 190.4.80.200
- e. 190.4.90.1
- f. 10.1.1.1

Câu 12. Mỗi câu trả lời sau đây thể hiện một số thập phân có chấm và một mặt nạ mạng. Số thập phân có chấm phản là một địa chỉ IP hợp lệ có thể sử dụng cho một máy tính hay nó có thể là một số mạng con hay địa chỉ quảng bá. Câu trả lời nào cho một địa chỉ có thể được sử dụng bởi một máy tính?

- a. 10.0.0.0, 255.0.0.0
- b. 192.168.5.160, 255.255.255.192
- c. 172.27.27.27, 255.255.255.252
- d. 172.20.49.0, 255.255.254.0

Câu 13. mạng con nào sau đây là hợp lệ trong mạng 180.1.0.0 khi sử dụng mặt nạ 255.255.248.0?

- a. 180.1.2.0
- b. 180.1.4.0
- c. 180.1.8.0
- d. 180.1.16.0
- e. 180.1.32.0
- f. 180.1.40.0

Câu 14. Mặt nạ nào sau đây không hợp lệ trong mạng 180.1.0.0 khi sử dụng mặt nạ 255.255.255.0?

- a. 180.2.2.0
- b. 180.1.4.0
- c. 180.1.8.0
- d. 180.1.16.0
- e. 180.1.32.0
- f. 180.1.40.0

Chương 6

VẬN HÀNH ROUTER CISCO

Router khác với switch trong mục đích sử dụng của nó. Switch chuyển các frame Ethernet bằng cách so sánh địa chỉ MAC đến của frame với bảng địa chỉ MAC của switch đó, trong khi router chuyển tiếp các gói tin bằng cách so sánh địa chỉ IP đích với bảng định tuyến IP của router. Các Ethernet switch ngày nay thường chỉ có một trong các dạng của giao tiếp Ethernet, trong khi router có nhiều giao tiếp Ethernet, giao tiếp WAN serial, và các giao tiếp khác kết nối thông qua cáp và đường dây kĩ thuật số ra Internet. Router biết làm thế nào để chuyển dữ liệu đến các thiết bị được kết nối đến các loại giao tiếp khác nhau này, trong khi các switch Ethernet tập trung giải quyết việc chuyển các Ethernet frame đến các thiết bị Ethernet. Vì thế trong khi cả hai switch và router chuyển dữ liệu, chi tiết loại dữ liệu có thể được chuyển và đến các thiết bị nào, khác nhau rõ rệt.

Mặc dù mục đích chính của chúng khác nhau, nhưng router và switch Cisco sử dụng cùng giao tiếp dòng lệnh người dùng. Chương này xem xét các chức năng dòng lệnh người dùng trên các router khác với các chức năng trên switch.

6.1. CÀI ĐẶT ROUTER CISCO

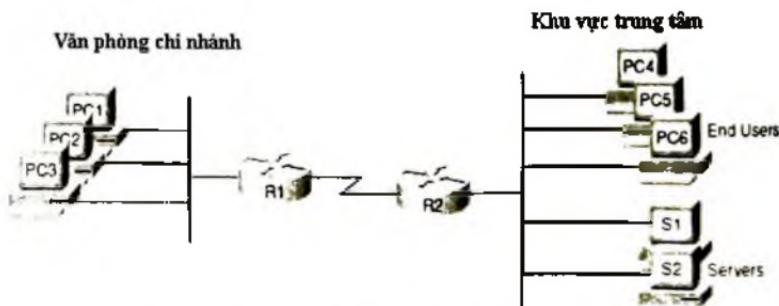
Router chủ yếu cung cấp chức năng của lớp mạng – khả năng chuyển các gói điêm – điêm thông qua mạng. Như đã giới thiệu trong chương 5 “Tổng quan về Địa chỉ IP và định tuyến” router chuyển các gói tin bằng các kết nối với nhiều liên kết vật lý khác nhau, như là Ethernet,

Serial, và Frame Relay, sử dụng ý nghĩa định tuyến lớp 3 để chọn nơi chuyển tiếp cho mỗi gói tin. Phần này kiểm tra chi tiết liên quan đến việc cài đặt và nối cáp router, từ quan điểm doanh nghiệp, và sau đó từ quan điểm của việc kết nối một văn phòng/nhà nhỏ đến ISP sử dụng Internet tốc độ cao.

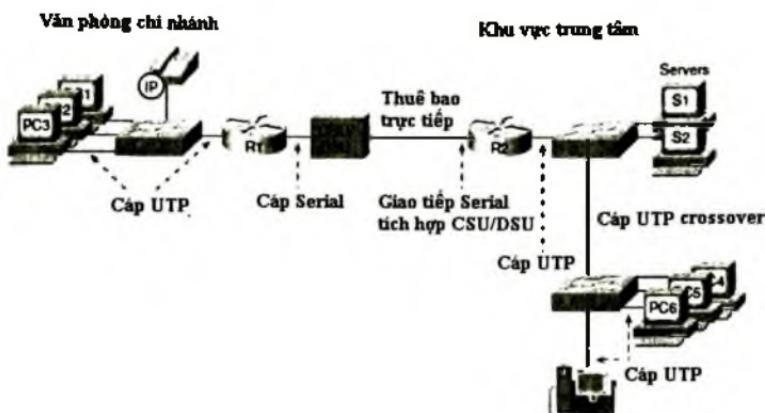
6.1.1. Cài đặt router cho các doanh nghiệp

Một mạng doanh nghiệp thông thường có một vài khu vực tập trung và nhiều khu vực ở xa. Thiết bị tại các khu vực này (máy tính, điện thoại IP, máy in và các thiết bị khác), liên lạc với nhau thông qua ít nhất một switch LAN. Ngoài ra, mỗi khu vực có một router, kết nối đến LAN switch và kết nối đến khu vực khác sử dụng liên kết WAN. Liên kết WAN này cung cấp kết nối từ mỗi khu vực ở xa, quay về khu vực trung tâm và đến các khu vực khác thông qua kết nối đến khu vực trung tâm.

Hình 6.1 cho thấy một phần của mạng doanh nghiệp, trong đó có một chi nhánh văn phòng thông thường bên trái, với một router, một số PC người dùng cuối. Khu vực trung tâm, bên phải có các thành phần cơ bản tương tự, với liên kết serial điểm – điểm kết nối hai router. Khu vực trung tâm bao gồm một dãy server với hai server, với một trong các mục đích chính của việc kết nối nào là cung cấp khả năng truy cập đến dữ liệu được lưu trữ cho các văn phòng ở xa trên các server này.



Hình 6.1. Cấu hình Router điểm - điểm



Hình 6.2. Cấu hình kết nối router điểm - điểm sử dụng CSU/DSU

Hình 6.2 cho thấy các loại cáp LAN (UTP), với một cặp kết nối cáp WAN khác nhau. Các kết nối LAN đều sử dụng cáp thẳng UTP, ngoại trừ với cáp UTP giữa hai switch, sử dụng cáp chéo.

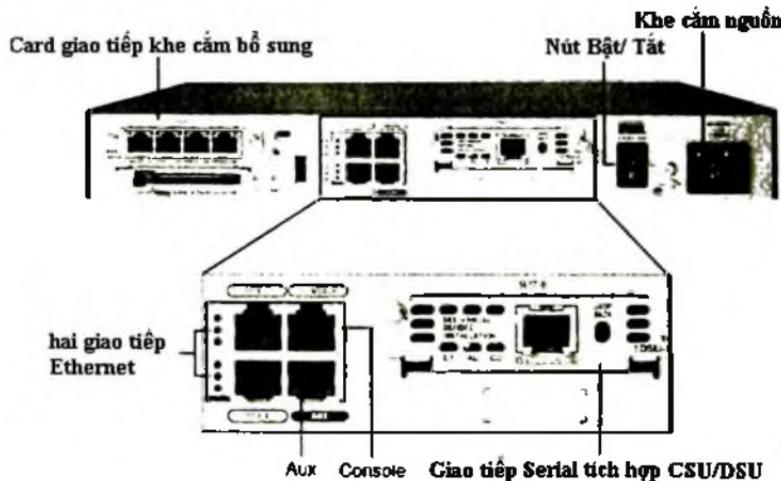
Liên kết serial trong hình cho thấy hai lựa chọn chính cho nơi các đơn vị dịch vụ kênh/dơn vị dịch vụ dữ liệu (CSU/DSU) được đặt; hoặc là bên ngoài router (như thể hiện tại văn phòng trung tâm trong trường hợp này) hay được tích hợp với giao tiếp serial của router (như thể hiện tại khu vực trung tâm). Hầu hết các phiên bản mới ngày nay đã bao gồm các CSU/DSU trong giao tiếp serial của router. Cáp WAN được cài đặt bởi công ty viễn thông thường có đầu nối kiểu RJ – 45, cùng kiểu và kích thước với đầu nối RJ – 45. Cáp công ty viễn thông với đầu nối RJ – 45 chèn vào CSU/DSU, nghĩa là nó kết nối trực tiếp đến router khu vực trung tâm trong trường hợp này, nhưng vào trong bộ CSU/DSU bên ngoài tại router văn phòng chi nhánh. Tại chi nhánh, bộ CSU/DSU bên ngoài sau đó được nối cáp, sử dụng một cáp serial, đến port serial của router văn phòng chi nhánh.

6.1.2. Router dịch vụ tích hợp của Cisco

Các nhà cung cấp sản phẩm, bao gồm Cisco thường cung cấp nhiều loại router khác nhau, bao gồm một số loại chỉ thực hiện việc định tuyến,

với các loại router khác cung cấp các chức năng khác ngoài định tuyến. Một văn phòng chi nhánh doanh nghiệp thường cần một router cho kết nối LAN/WAN và một LAN switch để cung cấp một mạng cục bộ có khả năng thực thi cao và có thể kết nối đến router và WAN. Nhiều chi nhánh cũng cần các thiết bị thoại qua IP mới và nhiều dịch vụ bảo mật khác. Thay vì yêu cầu nhiều thiết bị tách biệt tại một khu vực, như trong hình trên, Cisco cung cấp các thiết bị đơn hoạt động như là cả router và switch, và cung cấp các chức năng khác.

Cisco cung cấp nhiều mẫu router mới trong đó router hỗ trợ cho nhiều chức năng khác nhau, được gọi là các router dịch vụ tích hợp – Integrated Services Routers (ISR), có nghĩa là nhiều chức năng được tích hợp vào một thiết bị duy nhất.



Hình 6.3. Các thành phần router

6.1.3. Cài đặt vật lý

Để cài đặt một router, tuân theo các bước sau:

Bước 1: Kết nối bất kì cáp LAN đến các port LAN

Bước 2: Nếu sử dụng một CSU/DSU ngoại kết nối giao tiếp serial của router với CSU/DSU này, và sau đó kết nối CSU/DSU đến đường dây của công ty viễn thông.

Bước 3: Nếu sử dụng một CSU/DSU nội, kết nối giao tiếp serial của router với đường dây từ công ty viễn thông.

Bước 4: Kết nối cổng console với một PC (sử dụng cáp rollover), nếu cần thiết để cấu hình router.

Bước 5: Kết nối cáp nguồn từ bảng nguồn đến cổng nguồn trên router.

Bước 6: Bật router.

Chú ý rằng các bước trên thường tuân theo cùng các bước được dùng cho việc cài đặt LAN switch – cài đặt cáp cho các giao tiếp, kết nối console (nếu cần) và kết nối nguồn. Tuy nhiên, hầu hết các router Catalyst của Cisco không có nút bật/tắt nguồn được kết nối với nguồn, trong khi switch thì có.

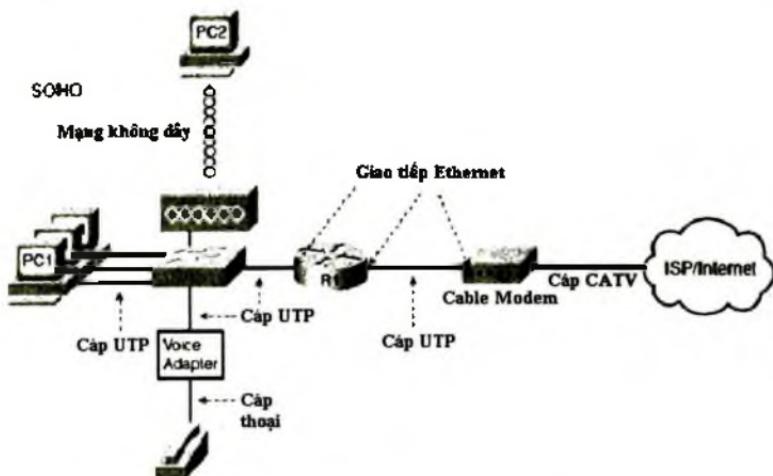
6.2. CÀI ĐẶT CÁC ROUTER TRUY CẬP INTERNET

Router đóng vai trò chính trong các mạng SOHO, được sử dụng để kết nối mạng LAN từ người dùng đến nhà cung cấp truy cập Internet tốc độ cao. Một khi đã kết nối Internet, người dùng SOHO có thể gửi các gói dữ liệu từ và đến các mạng doanh nghiệp tại công ty hay trường học.

Ở thị trường mạng doanh nghiệp, các nhà sản xuất sản phẩm có xu hướng bán các thiết bị mạng tích hợp thực hiện nhiều chức năng. Tuy nhiên, phần này kiểm tra các chức năng mạng khác nhau cần thiết tại một mạng SOHO thông thường, sử dụng một thiết bị tách biệt cho mỗi chức năng. Theo đó, một ví dụ thực tế được thể hiện, với các chức năng kết hợp vào một thiết bị đơn.

6.2.1. Cài đặt SOHO với một switch, router, và cáp modem tách biệt

Hình trên cho thấy một ví dụ về các thiết bị và cáp được dùng trong một mạng SOHO để kết nối Internet sử dụng cáp TV như là dịch vụ Internet tốc độ cao. Bây giờ, nhớ rằng hình trên thể hiện một cách khác cho các thiết bị và cáp, trong khi nhiều biến thể khác là có thể.



Hình 6.4. Cấu hình router kết nối Internet

Hình 6.4 thể hiện kết nối mạng văn phòng doanh nghiệp thông thường. PC người dùng cuối kết nối đến một switch, và switch kết nối đến một giao tiếp Ethernet của router. Router vẫn cung cấp dịch vụ định tuyến, chuyển các gói tin IP. Các chi tiết thoại khác một ít so với hình trên, chủ yếu bởi vì hình này thể hiện một dịch vụ điện thoại Internet thông thường tại nhà, sử dụng điện thoại tương tự thông thường và các bộ thoại để chuyển đổi từ tín hiệu thoại sang IP.

Khác biệt chính giữa kết nối SOHO trong hình 6.4 và mạng doanh nghiệp trong hình 6.2 có liên quan đến kết nối Internet. Một kết nối Internet sử dụng CATV hay DSL cần một thiết bị chuyển đổi giữa các chuẩn lớp 1 và lớp 2 được dùng trong các đường DSL hay CATV, và Ethernet sử dụng bởi router. Những thiết bị này, thông thường được gọi là cáp modem hay DSL modem, chuyển đổi tín hiệu điện giữa cáp Ethernet và cáp CATV hay là DSL.

Thực ra, trong khi chi tiết có vẻ khác biệt lớn, thì mục đích của việc sử dụng cáp modem và DSL modem tương tự như là CSU/DSU trên một liên kết serial. Một CSU/DSU chuyển đổi giữa chuẩn lớp 1 được sử dụng

bởi một kênh WAN của công ty viễn thông và chuẩn lớp 1 cáp serial – và router có thể sử dụng các cáp serial này. Tương tự, một modem cáp chuyển đổi giữa tín hiệu CATV và chuẩn lớp 1 và lớp 2 được dùng bởi router – thông thường là Ethernet. Tương tự, DSL modem chuyển đổi giữa tín hiệu DSL qua đường dây thoại và Ethernet.

Để cài đặt vật lý một mạng SOHO với các thiết bị được thể hiện trong hình 6.4, cần dùng cáp UTP cho các kết nối Ethernet, và hoặc là cáp CATV (cho các dịch vụ cáp Internet) hay đường dây điện thoại (cho các dịch vụ DSL). Chú ý rằng router được dùng trong hình 6.4 đơn giản cần hai giao tiếp Ethernet – một để kết nối đến switch LAN và một để kết nối đến modem cáp.

Cần sử dụng các bước sau để cài đặt router SOHO này:

Bước 1: Kết nối cáp thẳng UTP từ router đến switch

Bước 2: Kết nối cáp thẳng UTP từ router đến modem cáp

Bước 3: Kết nối đến cổng console của router (sử dụng cáp rollover), nếu cần, để cấu hình router

Bước 4: Kết nối cáp nguồn từ bảng nguồn đến cổng nguồn trên router

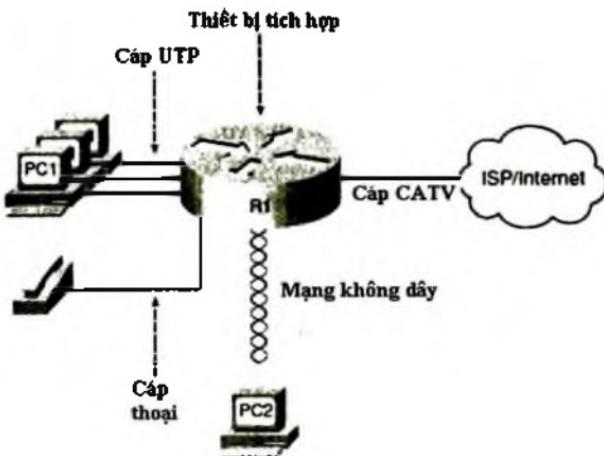
Bước 5: Bật router

6.2.2. Một cài đặt SOHO với switch, router và DSL modem tích hợp

Ngày nay, hầu hết các phiên bản SOHO mới sử dụng một thiết bị được tích hợp hơn là các thiết bị tách rời thể hiện trong hình 6.4. Thực ra, có thể mua các thiết bị SOHO bao gồm các chức năng sau đây:

- Router
- Switch
- Modem cáp hay DSL
- Thiết bị voice
- Bộ truy cập không dây
- Mã hóa phần cứng

Kết nối Internet tốc độ cao SOHO này nay có thể giống như hình 6.5, với một thiết bị tích hợp



Hình 6.5. Cấu hình router kết nối Internet

6.3. GIAO DIỆN DÒNG LỆNH CỦA ROUTER CISCO

Router Cisco sử dụng cùng giao diện dòng lệnh của switch. Tuy nhiên, vì router và switch thực hiện các chức năng khác nhau các câu lệnh thực sự khác nhau trong một số trường hợp. Phần này bắt đầu với việc liệt kê một số chức năng chính làm việc chính xác trên cả hai router và switch, và sau đó liệt kê và mô tả chi tiết một số chức năng khác giữa switch và router.

6.3.1. So sánh giữa dòng lệnh Router và Switch

Danh sách sau đây liệt kê nhiều mục được xem xét trong chương 8 mà dòng lệnh Router có cùng chức năng. Câu lệnh cấu hình được dùng cho các chức năng sau là giống:

- Chế độ Người dùng và cấp quyền
- Vào và thoát chế độ cấu hình, sử dụng các câu lệnh **configure terminal**, **end**, và **exit** và tổ hợp phím **Ctrl - Z**.

- Cấu hình console, telnet, và enable secret password
- Cấu hình khóa mã SSH và định danh người dùng/mật khẩu đăng nhập
- Cấu hình tên thiết bị và mô tả giao tiếp
- Cấu hình các giao tiếp Ethernet có thể thương lượng tốc độ, sử dụng các câu lệnh speed và duplex.
- Cấu hình một giao tiếp tắt chức năng quản trị (shutdown) và bật chức năng quản trị (no shutdown)
- Định hướng qua ngũ cành chế độ cấu hình khác nhau sử dụng câu lệnh như là line console 0 và interface
- Trợ giúp CLI, hiệu chỉnh lệnh, và chức năng gọi lại lệnh.
- Ý nghĩa và sử dụng startup – config (trong NVRAM), running – config (trong RAM), và các server ngoại (TFTP), cùng với cách sử dụng câu lệnh copy để sao chép các file cấu hình và ảnh ISO.
- Tiến trình vào chế độ thiết lập hoặc là bằng cách tái tạo router với startup – config rõ ràng hoặc bằng câu lệnh setup.

Các yếu tố trên là khá giống như khi cấu hình với switch, tuy nhiên, có một số khác biệt khi cấu hình dòng lệnh giữa router và switch như sau:

- Việc cấu hình địa chỉ IP trên các giao tiếp
- Các câu hỏi được đặt ra trong chế độ thiết lập
- Router có một cổng phụ (Auxiliary), được kết nối đến một modem ngoài, cho phép người dùng từ xa kết nối đến router và truy cập vào dòng lệnh, bằng cách quay số đến.

6.3.2. Các giao tiếp của router

Trong nội dung giáo trình này, chỉ nghiên cứu về các giao tiếp serial và Ethernet. Giao tiếp Ethernet để cập đến bất kì giao tiếp Ethernet nào, có tốc độ 10Mbit/s, 100Mbit/s, 1000Mbit/s.

Giao tiếp Serial là loại chính thứ hai của kết nối Internet vật lý. Như đã giới thiệu trong phần trước, các đường truyền đường dây thuê bao leased line diêm diếm và các liên kết truy cập Frame Relay đều sử dụng cùng các

tiêu chuẩn lớp 1 bên dưới. Để hỗ trợ những chuẩn này, router Cisco sử dụng các giao tiếp serial. Sau đó có thể chọn giao thức lớp liên kết dữ liệu được dùng, như là HDLC, PPP cho leased line hay Frame Relay cho các kết nối Frame Relay, và cấu hình router để dùng đúng giao thức liên kết dữ liệu.

Router sử dụng số để phân biệt giữa các giao tiếp khác nhau cùng loại. Trên router, các số giao tiếp có thể là số đơn, hay hai số tách rời bởi dấu gạch chéo, hay ba số tách rời bởi các dấu gạch chéo. Ví dụ, tất cả ba câu lệnh cấu hình sau đều đúng với ít nhất một loại router Cisco:

- Interface Ethernet 0
- Interface fastethernet 0/1
- Interface serial 1/0/1

Có thể xem thông tin về các giao tiếp bằng cách dùng nhiều câu lệnh. Để xem danh sách các giao tiếp vẫn tắt, sử dụng lệnh `show ip interface brief`. Để xem chi tiết về một giao tiếp cụ thể, sử dụng câu lệnh `show protocols type number`. Cũng có thể xem nhiều chi tiết về mỗi giao tiếp, bao gồm thông kê về luồng gói vào và ra của giao tiếp đó, bằng cách sử dụng câu lệnh `show interfaces`. Tùy chọn có thể thêm loại giao tiếp và số trên nhiều câu lệnh, lấy ví dụ `show interface số giao tiếp` để xem chi tiết cho giao tiếp đó. Đây là một ví dụ.

```
Albuquerque#show ip interface brief
Interface          IP Address      OK? Method Status      Protocol
FastEthernet0/0    unassigned     YES unset  up          up
FastEthernet0/1    unassigned     YES unset  administratively down down
Serial0/0/0        unassigned     YES unset  administratively down down
Serial10/0/1       unassigned     YES unset  up          up
Serial10/1/0       unassigned     YES unset  up          up
Serial10/1/1       unassigned     YES unset  administratively down down
Albuquerque#show protocols fast/0
FastEthernet0/0 is up, line protocol is up
Albuquerque#show interfaces serial/0
Serial10/1/0 is up, line protocol is up
  Hardware is GT66K Serial
  MTU 1500 bytes, Rx 1544 Kbit, DLY 20000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:03, output 00:00:01, output hang never
  Last clearing of 'show interface' counters never
  Input queue: 0.75 0 0 (size/max drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0 (size/max total/threshold drops)
    Conversations 0-1.256 (active/max active/max total)
    Reserved Conversations 0 (allocated/max allocated)
    Available Bandwidth: 1158 kbytes/sec
```

6.3.3. Mã trạng thái giao tiếp

Mỗi câu lệnh trong ví dụ trên liệt kê hai mã trạng thái giao tiếp. Với router, để sử dụng một giao tiếp, hai mã trạng thái giao tiếp trên giao tiếp đó phải ở trạng thái “up”. Mã trạng thái đầu tiên ám chỉ đến liệu Lớp 1 có đang hoạt động hay không, và mã trạng thái thứ hai chủ yếu để cập đến liệu giao thức liên kết dữ liệu có đang làm việc. Bảng sau tóm tắt hai mã trạng thái này:

Bảng 6.1. Các trạng thái giao tiếp

Tên	Vị trí	Ý nghĩa chung
Trạng thái đường truyền	Mã trạng thái đầu	Trạng thái lớp 1 – ví dụ đã nối cáp đúng hay chưa, thiết bị đầu kia đã bật?
Trạng thái giao thức	Mã trạng thái thứ hai	Trạng thái lớp 2 – luôn luôn tắt nếu trạng thái đường truyền là tắt. Nếu trạng thái đường truyền là bật, trạng thái giao thức tắt thường do cấu hình lớp liên kết dữ liệu không trùng khớp

Bốn kết hợp của thiết lập có sẵn cho các mã trạng thái được sử dụng khi xử lý sự cố trên một mạng. Bảng 6.1 liệt kê bốn kết hợp này, cùng với giải thích về các nguyên nhân thông thường tại sao một giao tiếp lại ở trong trạng thái đó. Khi xem danh sách, chú ý rằng trạng thái đường truyền (mã trạng thái đầu tiên) không “up”, vì các chức năng lớp liên kết dữ liệu không hoạt động nếu lớp vật lý có vấn đề.

Bảng 6.2. Mã trạng thái giao tiếp

Trạng thái giao thức và đường truyền	Nguyên nhân thông thường
Administrative down, down	Giao tiếp đang tắt với lệnh shutdown
Down, down	Giao tiếp đã có lệnh no shutdown, nhưng có vấn đề với lớp vật lý. Ví dụ không có cáp, hay với Ethernet, giao tiếp switch đầu kia đã tắt hay switch bị tắt
Up, down	Thông thường lỗi của lớp liên kết dữ liệu, liên quan đến cấu hình. Ví dụ, liên kết serial được cấu hình một đầu là HDLC và một đầu là PPP.
Up, up	Hoạt động tốt

6.3.4. Địa chỉ IP cho giao tiếp Router

Router cần một địa chỉ IP trên mỗi giao tiếp. Nếu không có địa chỉ IP nào được cấu hình, thậm chí nếu giao tiếp là ở trạng thái up/up, router

sẽ không thử gửi và nhận các gói IP trên giao tiếp này. Để hoạt động từ mọi giao tiếp một router cần một địa chỉ IP.

Việc cấu hình địa chỉ IP trên một giao tiếp là khá đơn giản. Để cấu hình địa chỉ và mặt nạ, đơn giản sử dụng câu lệnh ip address địa chỉ mặt_nạ. Ví dụ sau cho một ví dụ cấu hình địa chỉ IP trên hai giao tiếp của router, và kết quả khác trên các câu lệnh show ip interface brief và show interface.

```
Albuquerque#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Albuquerque (config)#interface Fa0/0
Albuquerque (config-if)#ip address 10.1.1.1 255.255.255.0
Albuquerque (config-if)#interface Fa0/0/1
Albuquerque (config-if)#ip address 10.1.2.1 255.255.255.0
Albuquerque (config-if)#Z
Albuquerque#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    10.1.1.1        YES manual up          up
FastEthernet0/0/1   unassigned      YES NVRAM administratively down down
Serial0/0/0         unassigned      YES NVRAM administratively down down
Serial0/0/1         10.1.2.1        YES manual up          up
Serial0/1/0         unassigned      YES NVRAM up          up
Serial0/1/1         unassigned      YES NVRAM administratively down down
Albuquerque#show interfaces fa0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt06k FE, address is 0013.197b.5004 (bia 0013.197b.5004)
  Internet address is 10.1.1.1/24
  ! lines omitted for brevity
```

6.3.5. Băng thông và xung đồng hồ trên giao tiếp Serial

Các giao tiếp Ethernet sử dụng tốc độ có thể tự thỏa thuận với nhau. Tuy nhiên, biết các liên kết WAN có thể chạy ở nhiều tốc độ khác nhau. Để xử lý vấn đề này, router, thường sử dụng các bộ CSU/DSU thông qua một tiến trình được gọi là xung đồng hồ. Kết quả là router có thể sử dụng các liên kết serial mà không cần cấu hình hay thỏa thuận bổ sung để cảm nhận tốc độ liên kết serial. Thiết bị CSU/ DSU biết tốc độ đó, CSU/DSU gửi xung đồng hồ qua cáp đến router, và router tái kích hoạt với tín hiệu đồng hồ. Mục đích là CSU/DSU báo cho router biết khi nào gửi bit kế tiếp trên cáp, và khi nào nhận bit kế tiếp đó.

Câu lệnh clock rate kích hoạt tốc độ thực sự được dùng để truyền các bit trên một liên kết serial nhưng chỉ khi liên kết vật lý serial thực sự

được tạo với việc nối cáp trong một phòng thí nghiệm. Đây là một ví dụ cho việc sử dụng câu lệnh **clock rate** trong liên kết serial.

```
Albuquerque#show running-config
! lines omitted for brevity
interface Serial0/0/1
  clock rate 128000
```

continues

```
!
interface Serial0/1/0
  clock rate 128000
  bandwidth 128
!
interface FastEthernet0/0
! lines omitted for brevity
Albuquerque#show controllers serial 0/0/1
Interface Serial0
Hardware is PowerQUICC MPC864
DCE V.35, clock rate 128000
idb at 0x01690020, driver data structure at 0x016A35E4
! Lines omitted for brevity
```

Câu lệnh **clock rate** thiết lập tốc độ bit trên giây trên router có cáp DCE được cắm vào. Nếu không biết router nào có cáp DCE, có thể tìm thấy nhờ câu lệnh **show controllers**, liệt kê cáp được nối là DCE hay DTE. Thủ vị là, IOS chấp nhận lệnh **clock rate** trên một giao tiếp chỉ nếu giao tiếp đã có cáp DCE, hay nếu không có cáp. Nếu một cáp DTE được cắm vào, IOS từ chối câu lệnh này, nghĩa là IOS không cho một thông điệp lỗi, nhưng IOS bỏ qua lệnh này.

Lệnh thứ hai liên quan đến tốc độ của liên kết serial là câu lệnh **bandwidth**, như thể hiện trong ví dụ 6.3. Câu lệnh **bandwidth** báo cho IOS tốc độ của liên kết, trong Kbit/s, tùy theo liệu router được cung cấp xung nhịp. Tuy nhiên, thiết lập băng thông không thay đổi tốc độ bit được gửi và nhận trên liên kết đó. Thay vào đó, router sử dụng nó để làm thông tin tư liệu, trong tính toán liên quan đến tốc độ tối ưu của liên kết, và cho nhiều mục đích khác. Cụ thể, giao thức định tuyến EIGRP và OSPF sử dụng thiết lập băng thông giao tiếp để thiết lập tham số metric mặc định của nó, với các metric này ảnh hưởng đến việc lựa chọn của router cho con đường IP tốt nhất để đến mỗi mạng con.

Mỗi giao tiếp router có một thiết lập mặc định cho câu lệnh **bandwidth** được sử dụng khi không có lệnh **bandwidth** nào được cấu

hình trên giao tiếp đó. Với các liên kết serial, băng thông mặc định là 1544, có nghĩa là 1544 kbit/s (1,544 Mbit/s), hay là tốc độ đường T1. Các giao tiếp Ethernet router thiết lập mặc định đến băng thông phản ánh tốc độ của giao tiếp đó. Ví dụ, nếu một giao tiếp Fast Ethernet chạy ở tốc độ 100 Mbit/s, băng thông là 100,000 kbps; nếu giao tiếp đang chạy tốc độ 10 Mbit/s, router tự động thay đổi băng thông sang 10,000 kbps. Chú ý việc cấu hình câu lệnh bandwidth trên một giao tiếp ghi đè các thiết lập này.

6.4. CÔNG PHỤ (AUXILIARY) CỦA ROUTER

Router có một cổng phụ cho phép truy cập đến dòng lệnh băng cách dùng bộ mô phỏng đầu cuối. Thông thường, cổng phụ Aux được kết nối thông qua cáp (RJ – 45 cáp thẳng) đến một modem số. Modem kết nối đến một đường dây điện thoại. Sau đó, sử dụng PC và modem để quay số đến router từ xa.

Khi đã kết nối, có thể sử dụng bộ giả lập đầu cuối để truy cập đến giao diện dòng lệnh của router, bắt đầu với chế độ người dùng như thông thường.

Cổng phụ có thể được cấu hình bắt đầu với lệnh **line aux 0** để vào chế độ cấu hình cho cổng phụ. Từ đó, tất cả câu lệnh cho chế độ console có thể được sử dụng. Ví dụ, các lệnh **login** và **password** có thể được dùng để thiết lập kiểm tra mật khẩu khi người dùng quay số đến.

Cấu hình khởi tạo (chế độ thiết lập): Các tiến trình có liên quan đến chế độ thiết lập trong router tương tự như các quy tắc dành cho switch. Các câu lệnh sau đây tông kết một số điểm chính, tất cả đều đúng cho cả hai router và switch.

- Chế độ thiết lập cho phép cấu hình cơ bản bởi dòng lệnh người dùng thông qua một loạt các câu hỏi
- Có thể vào chế độ thiết lập hoặc là bằng cách khởi động một router sau khi xóa file cấu hình startup – config hoặc bằng cách sử dụng câu lệnh vào chế độ cho phép EXEC setup.
- Vào cuối tiến trình, có ba lựa chọn (0, 1 hay 2) để hoặc là bỏ qua các câu trả lời và về lại chế độ CLI (0), bỏ qua câu trả lời và quay lại với chế độ thiết lập (1); hay sử dụng kết quả cấu hình.

- Nếu không thích các tiến trình này, sử dụng tổ hợp phím Ctrl - C sẽ bỏ chế độ thiết lập và quay về chế độ CLI trước đó.
- Nếu lựa chọn sử dụng cấu hình kết quả, router ghi cấu hình vào file cấu hình startup - config cũng như là file running - config.

Khác biệt chính giữa chế độ thiết lập trên switch và router liên quan đến thông tin được yêu cầu trong chế độ thiết lập. Lấy ví dụ, router cần biết địa chỉ IP và mặt nạ cho mỗi giao tiếp trên đó muốn cấu hình IP, trong khi switch chỉ có duy nhất một địa chỉ IP. Ví dụ sau mô tả việc sử dụng cho chế độ thiết lập.

```
... System Configuration Dialog ...

Would you like to enter the initial configuration dialog? [yes/no]: yes
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'. Basic management setup configures
only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: no
First, would you like to see the current interface summary? [yes]:
Any interface listed with 'OK?' value 'NO' does not have a valid configuration

Interface          IP-Address      OK? Method Status      Protocol
Ethernet0          unassigned      NO  unset  up          down
Serial0            unassigned      NO  unset  down        down
Serial1            unassigned      NO  unset  down        down

Configuring global parameters:

Enter host name [Router]: R1
The enable secret is a password used to protect access to
privileged EXEC and configuration modes. This password, after
entered, becomes encrypted in the configuration.
Enter enable secret: cisco
The enable password is used when you do not specify an
enable secret password, with some older software versions, and
some boot images.
Enter enable password: fred
The virtual terminal password is used to protect
access to the router over a network interface.
Enter virtual terminal password: borney
Configure SNMP Network Management? [yes]: no
Configure Bridging? [no]:
Configure DECnet? [no]:
Configure AppleTalk? [no]:
Configure IP? [no]:
```

```

Configure IP? [yes]:  

Configure RIP routing? [yes]:  

Configure CLNS? [no]:  

Configure bridging? [no]:  

Configuring interface parameters:  

Do you want to configure Ethernet0 interface? [yes]:  

Configure IP on this interface? [yes]:  

IP address for this interface: 172.16.1.1  

Subnet mask for this interface [255.255.0.0] : 255.255.255.0  

Class B network is 172.16.0.0, 24 subnet bits; mask is /24  

Do you want to configure Serial0 interface? [yes]:  

Configure IP on this interface? [yes]:  

Configure IP unnumbered on this interface? [no]:  

IP address for this interface: 172.16.12.1  

Subnet mask for this interface [255.255.0.0] : 255.255.255.0  

Class B network is 172.16.0.0, 24 subnet bits; mask is /24  

Do you want to configure Serial1 interface? [yes]:  

Configure IP on this interface? [yes]:  

Configure IP unnumbered on this interface? [no]:  

IP address for this interface: 172.16.13.1  

Subnet mask for this interface [255.255.0.0] : 255.255.255.0  

Class B network is 172.16.0.0, 24 subnet bits; mask is /24

```

The following configuration command script was created:

```

hostname R1
enable secret 5 $1$V0Lh$pkle0kjx2sgjgZ/V6Gt1s.
enable password fred
line vty 0 4
password barney
no snmp-server
!
ip routing
!
interface Ethernet0
ip address 172.16.1.1 255.255.255.0
!
interface Serial0
ip address 172.16.12.1 255.255.255.0
!
interface Serial1
ip address 172.16.13.1 255.255.255.0
!
router rip
network 172.16.0.0
!
```

```

end

[6] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
Building configuration...
[OK]Use the enabled mode "configure" command to modify this configuration.
Press RETURN to get started!

```

6.5. NÂNG CẤP PHẦN MỀM IOS CỦA CISCO VÀ TIẾN TRÌNH KHỞI ĐỘNG PHẦN MỀM IOS CỦA CISCO

Cần biết cách nâng cấp IOS để có được các phiên bản sau của nó. Thông thường, một router có một ảnh IOS trên bộ nhớ Flash, và đó là ảnh IOS được dùng. (Thuật ngữ ảnh IOS ám chỉ đến một file chứa IOS). Tiến trình nâng cấp có thể bao gồm các bước như là sao chép một ảnh IOS mới hơn vào bộ nhớ Flash, cấu hình router để báo cho nó biết cần sử dụng ảnh IOS nào, và xóa ảnh cũ khi tin rằng ảnh mới hoạt động tốt. Cách khác, có thể copy một ảnh mới sang TFTP server với một số cấu hình bổ sung trên router để báo nó lấy IOS mới từ TFTP server cho lần tải nạp kế tiếp.

Phần này cho thấy cách nâng cấp IOS bằng cách sao chép một file IOS mới vào bộ nhớ Flash, và báo router biết sử dụng IOS mới này. Vì router quyết định IOS nào được dùng khi router khởi động, đây cũng là một cách tốt để xem lại tiến trình trong đó router khởi động. Các switch tuân theo cùng quy trình cơ bản như mô tả ở trên, với một số khác biệt nhỏ, như đã chú ý một cách cụ thể.

Nâng cấp phần mềm IOS vào bộ nhớ Flash: Router và switch thường lưu trữ ảnh IOS trong bộ nhớ Flash. Bộ nhớ Flash là nơi thông tin có thể được lưu trữ và thay đổi, thích hợp cho việc lưu trữ các file cần được duy trì khi router mất nguồn. Mục đích của Cisco khi sử dụng bộ nhớ Flash thay thế cho các ổ đĩa của nó vì không có thành phần tháo rời nào trong bộ nhớ Flash này. Vì thế nó ít có lỗi hơn so với ổ đĩa thông thường. Ngoài ra, ảnh IOS có thể được đặt vào một TFTP server bên

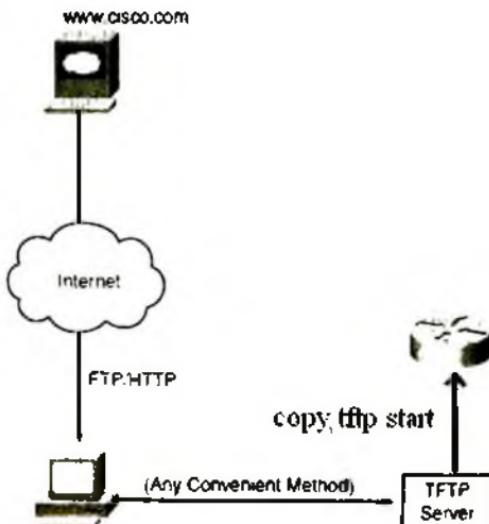
ngoài, nhưng việc sử dụng một TFTP server bên ngoài thường chỉ phù hợp cho việc kiểm tra sản phẩm, còn thông thường mọi router Cisco nạp một ảnh của nó được lưu trữ trong chỉ một dạng bộ nhớ lớn, cố định – bộ nhớ Flash

Các bước cho nâng cấp ảnh IOS từ bộ nhớ Flash

Bước 1: Lấy ảnh IOS từ Cisco, thường bằng cách download ảnh IOS từ Cisco.com sử dụng HTTP hay FTP.

Bước 2: Đặt ảnh IOS này và thư mục mặc định trong server FTFP có khả năng truy cập từ router này.

Bước 3: Sử dụng lệnh copy từ router, sao chép file đó vào bộ nhớ Flash



Hình 6.6. Nâng cấp IOS router Cisco

Ví dụ sau cho thấy bước cuối cùng, sao chép ảnh IOS vào bộ nhớ Flash. Chủ ý rằng lệnh `copy tftp flash` được thể hiện ở đây làm việc giống như lệnh `copy tftp startup-config` có thể được dùng để phục hồi một bản sao của file cấu hình vào NVRAM.

```

Router#copy tftp flash
System flash directory:
File Length Name/status
1 7530768 c4500-d-mz.120.2.bin
[7530824 bytes used, 837764 available, 8388688 total]
Address or name of remote host [255.255.255.255]? 134.141.3.33
Source file name? c4500-d-mz.120.5.bin
Destination file name [c4500-d-mz.120.5.bin]?
Accessing file c4500-d-mz.120.5.bin on 134.141.3.33...
Loading c4500-d-mz.120.5.bin from 134.141.3.33 (via Ethernet0): 1 [OK]

Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]

Copy 'c4500-d-mz.120.5.bin' from server
as 'c4500-d-mz.120.5.bin' into Flash WITH erase? [yes/no]
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeee...erased
Loading c4500-d-mz.120.5.bin from 134.141.3.33 (via Ethernet0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! (leaving out lots of exclamation points)
[OK 7530768/8388688 bytes]

Verifying checksum... OK (0xA93E)
Flash copy took 0:04:26 (hh:mm:ss)

```

Trong suốt tiến trình sao chép ảnh vào bộ nhớ Flash, router cần phải khám phá nhiều nhân tố quan trọng:

1. Địa chỉ IP hay tên của TFTP server?
2. Tên của file cần chép?
3. Không gian trống có sẵn cho file trên bộ nhớ Flash?
4. Liệu server có file với tên như vậy?
5. Muốn router xóa file cũ hay không?

Router sẽ nhắc các câu trả lời, nếu cần thiết. Với mỗi câu hỏi, nên hoặc là đánh câu trả lời hoặc là nhấn Enter nếu đó là câu trả lời mặc định (được thể hiện trong các dấu ngoặc trong cuối câu hỏi). Sau đó, router xóa bộ nhớ Flash, sao chép file và sau đó xác nhận kiểm tra checksum cho file để chắc chắn không có lỗi nào xảy ra trong quá trình truyền. Có thể sử dụng lệnh show Flash để xem nội dung của bộ nhớ Flash, như mô tả trong ví dụ sau đây.

```

Fred@show flash
System flash directory:
File  Length  Name/status
1  1398382  c2500.ds.1.122.1.bin
[12385416 bytes used, 18777218 total]
16384K bytes of processor board System flash (Read ONLY)

```

Dòng bôi đen trong ví dụ trên liệt kê số bộ nhớ Flash, khoảng trống đã dùng, và khoảng trống còn lại. Khi sao chép một ảnh IOS mới vào Flash, lệnh copy sẽ hỏi liệu muốn xóa Flash, với câu trả lời mặc định là yes. Nếu phản hồi với câu trả lời no, và IOS thấy không đủ bộ nhớ để sao chép, tiến trình này dừng lại. Ngoài ra, nếu trả lời yes và xóa tất cả bộ nhớ Flash, ảnh IOS của bộ nhớ Flash phải đủ để được chứa trong bộ nhớ flash, nếu không việc sao chép sẽ bị lỗi.

Khi ảnh IOS mới đã được sao chép vào Flash, router phải được nạp để sử dụng ảnh IOS mới này. Phần kế tiếp, xem xét tiến trình khởi động của IOS, giải thích chi tiết làm thế nào cấu hình một router để nó nạp đúng ảnh IOS.

6.6. TIẾN TRÌNH KHỞI ĐỘNG PHẦN MỀM IOS CỦA CISCO

Các router Cisco thực hiện cùng các loại tác vụ mà một máy tính thông thường thực hiện khi bật hay khởi động lại nó. Hầu hết các máy tính có một hệ điều hành đơn (OS) được cài đặt trên đó và hệ điều hành này khởi động theo mặc định. Tuy nhiên, một router có thể có sẵn nhiều ảnh IOS trên cả bộ nhớ Flash và trên server TFTP, vì thế router cần biết ảnh IOS nào để nạp. Phần này kiểm tra toàn thể tiến trình khởi động, với việc nhấn mạnh cách lựa chọn ảnh IOS cần nạp của một router.

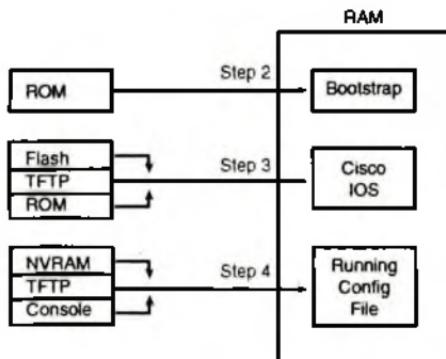
Chú ý: Tiến trình khởi động được mô tả chi tiết trong phần này, cụ thể tùy theo thanh ghi cấu hình và ROMMON OS, khác với switch LAN của Cisco, nhưng chúng được áp dụng cho hầu hết mọi loại router Cisco. Cuốn sách này không xem xét các tham số tương ứng cho switch Cisco.

Khi một router được bật đầu tiên, nó tuân theo bốn bước sau đây:

1. Router thực hiện tiến trình kiểm tra Power – On – Self – Test POST để phát hiện các thành phần phần cứng và xác nhận tất cả thành phần hoạt động tốt.

- Router sao chép một chương trình khởi động mới từ ROM vào RAM và chạy chương trình khởi động mới này.
- Chương trình khởi động mới này quyết định ảnh IOS nào (hay các OS khác) cần nạp vào RAM, và nạp OS đó. Sau khi nạp ảnh IOS đó, chương trình khởi động mới chiếm quyền điều khiển cho phần cứng router với OS vừa được nạp.
- Nếu chương trình khởi động mới đã nạp xong IOS, IOS tìm file cấu hình (thông thường là file startup – config trên NVRAM) và nạp nó vào RAM thành running – config.

Mỗi router thử bốn bước trên mỗi khi router đó được bật lên hay được khởi động lại. Hai bước đầu tiên không có bất kì tham số nào để lựa chọn; những bước này hoặc là làm việc hay router khởi tạo lỗi và như vậy thường cần gọi trung tâm dịch vụ kỹ thuật Cisco để hỗ trợ. Tuy nhiên, bước 3 và 4 có nhiều tham số cấu hình báo cho router biết cần làm gì tiếp theo. Hình 6.7 mô tả các tham số đó, với các bước từ 2 đến 4 được thể hiện như trong tiến trình khởi động.



Hình 6.7. Các bước khởi động Cisco IOS

Như có thể thấy, router có thể lấy ảnh IOS từ ba nơi và có thể lấy cấu hình khởi tạo cũng từ ba nơi đó. Thông thường các router luôn nạp cấu hình thực sự từ NVRAM (file startup – config), khi nó tồn tại. Không có lợi ích nào nếu lưu trữ cấu hình khởi tạo bất kì nơi nào ngoài

NVRAM. Vì thế chương này sẽ không xem xét kĩ hơn tham số của bước 4. Tuy nhiên, có nhiều nguyên nhân cần thiết cho việc đặt nhiều ảnh IOS vào Flash, và giữ cho các ảnh trên các server bên ngoài, vì thế phần còn lại của chương đánh giá bước 3 chi tiết hơn. Cụ thể là, giải thích một ít về các hệ điều hành khác của router bên cạnh IOS, và một chức năng router được gọi là thanh ghi cấu hình, trước khi đi sâu vào cách một router chọn ảnh IOS nào để nạp.

Chú ý: Ảnh IOS thường là một file nén để nó có thể chiếm ít không gian trong bộ nhớ Flash. Router sẽ giải nén ảnh IOS khi nó được nạp vào RAM.

6.6.1. Ba hệ điều hành của Router

Một router thông thường nạp và sử dụng một ảnh IOS cho phép router thực hiện chức năng thông thường của nó cho việc định tuyến các gói tin. Tuy nhiên, router Cisco có thể sử dụng một OS khác để thực hiện một số các xử lý sự cố, để khôi phục lại mật khẩu router, và để sao chép các file IOS mới vào Flash khi Flash đã bị xóa hay bị hư hỏng. Trong các phiên bản mới gần đây của router Cisco (1800 và 2800), router Cisco sử dụng chỉ một OS khác, trong khi các dòng router cũ hơn (như 2500) thực sự có hai hệ điều hành khác nhau để thực hiện các phần khác nhau của cùng chức năng này. Bảng sau liệt kê hai hệ điều hành khác nhau của router, và một số chi tiết về chúng.

Bảng 6.2. Các loại hệ điều hành trong router Cisco

Môi trường	Tên thông thường	Được lưu tại	Được sử dụng
ROM Monitor	ROMMON	ROM	Router đời cũ và mới
Boot ROM	RxBoot, Boot Helper	ROM	Router đời cũ

Vì OS RxBoot chỉ có trên các router cũ và không còn cần thiết trong các router mới, chương này chủ yếu đề cập đến OS còn được tiếp tục cho những mục đích đặc biệt, ROMMON OS.

6.6.2. Thanh ghi cấu hình

Thanh ghi cấu hình là một số 16 bit đặc biệt có thể được thiết lập trên bất kì router nào. Các bit của thanh ghi cấu hình này điều khiển các

thiết lập khác nhau cho một số đặc tính điều hành mức thấp của router. Ví dụ, cổng console hoạt động ở tốc độ 9600bit/s theo mặc định, nhưng tốc độ console đó được dựa trên các thiết lập mặc định của một cặp bit trên thanh ghi cấu hình.

Có thể thiết lập giá trị thanh ghi cấu hình với lệnh cấu hình toàn cục config – register. Thiết lập thanh ghi cấu hình với các giá trị khác nhau vì nhiều nguyên nhân, nhưng thông thường nhất là để giúp báo cho router ảnh IOS nào được nạp, như được giải thích trong phần sau, và trong tiến trình khôi phục mật khẩu router. Ví dụ, lệnh config – registater 0x2100 thiết lập giá trị sang thập lục phân 2100, làm cho router nạp ROMMON OS thay vì IOS – một kinh nghiệm thông dụng khi khôi phục mật khẩu bị mất. Thú vị là, giá trị này được tự động lưu trữ khi nhấn Enter tại cuối câu lệnh config – registater – không cần lưu trữ file running – config vào file startup – config sau khi thay đổi thanh ghi cấu hình. Tuy nhiên, giá trị mới của thanh ghi cấu hình không được sử dụng cho đến khi router được nạp lần tiếp.

6.6.3. Cách router chọn OS để nạp

Một router chọn OS để nạp dựa trên 4 bit thấp trong thanh ghi cấu hình và các chi tiết được cấu hình trong bất kì câu lệnh cấu hình toàn cục boot system nào được tìm thấy trong file startup – config. Bốn bit thấp trong thanh ghi cấu hình được gọi là trường khởi động, *boot field*, với giá trị của các bit này là giá trị đầu tiên một router kiểm tra khi lựa chọn OS nào cần thử và nạp. Giá trị trường khởi động khi router được bật hay được tái nạp báo cho router biết cách để xử lý với việc lựa chọn OS nào cần nạp.

Tiến trình chọn OS để nạp, trên nhiều router hiện đại không có OS RxBoot, xảy ra như sau:

Bước 1: Nếu trường khởi động = 0, sử dụng ROMMON OS

Bước 2: Nếu trường khởi động = 1, sử dụng file IOS đầu tiên được tìm thấy trong bộ nhớ Flash.

Bước 3: Nếu trường khởi động = 2-F:

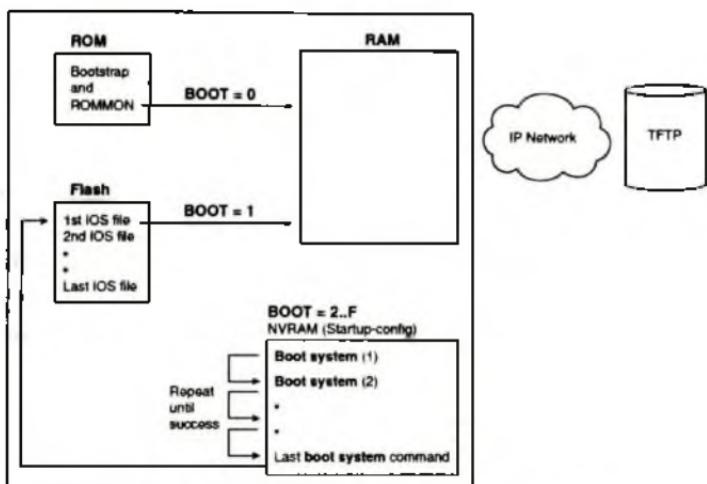
- Thứ mỗi câu lệnh **boot system** trong file **startup – config**, theo thứ tự, cho đến khi một trong đó hoạt động.
- Nếu không có câu lệnh nào của **boot system** hoạt động, nạp file IOS đầu tiên tìm thấy trong bộ nhớ Flash.

Hai bước đầu tiên là khá đơn giản, nhưng bước thứ ba sau khi báo router tìm kiếm phương thức chính thứ hai để báo cho router IOS nào để nạp; câu lệnh cấu hình toàn cục **boot system**. Câu lệnh này có thể được cấu hình nhiều lần trên một router, với các chi tiết về các file trong bộ nhớ Flash, và tên và địa chỉ IP của các server, báo cho router nơi tìm kiếm ảnh IOS để nạp. Router thử nạp các ảnh IOS, theo thứ tự các câu lệnh **boot system** đã được cấu hình. Khi router thành công trong việc nạp một trong số các ảnh IOS, tiến trình kết thúc, và router có thể bỏ qua các câu lệnh **boot system** còn lại. Nếu router gặp lỗi khi nạp một IOS dựa trên các câu lệnh **boot system**, router sau đó thử những gì bước 1 đề nghị, để nạp IOS đầu tiên được tìm thấy trong bộ nhớ Flash.

Cả bước 2 và bước 3 để cập đến khái niệm file IOS đầu tiên, một khái niệm cần được giải thích. Router đánh số file được lưu trữ trong bộ nhớ Flash, với mỗi file mới thông lấy một số cao hơn. Khi một router thử Bước 2 hay bước 3b từ danh sách đang xử lý, router sẽ tìm kiếm trong bộ nhớ Flash, bắt đầu với file số 1, và sau đó là file số 2 v.v, cho đến khi nó tìm thấy file có số thấp nhất là một ảnh IOS, router sẽ nạp ảnh đó.

Hầu hết router kết thúc việc sử dụng bước 3b để tìm ảnh IOS của nó. Router Cisco không có bắt kì câu lệnh **boot system** nào được cấu hình; thực ra, không có bắt kì cấu hình nào trong file **startup – config**. Router nạp bộ nhớ Flash với một hệ điều hành đơn khi nó xây dựng và kiểm tra router, và giá trị thanh ghi cấu hình được thiết lập sang 0x2102, nghĩa là một trường khởi động có giá trị 0x2. Với tất cả các thiết lập này, tiến trình thử bước 3 (vì giá trị trường khởi động = 2), tìm thấy không có câu lệnh **boot system** nào (vì **startup – config** trống) và sau đó tìm file đầu tiên trong bộ nhớ Flash ở bước 3b.

Hình 6.3 cho thấy sơ đồ tóm tắt các khái niệm chính bên dưới cách một router chọn OS để nạp.



Hình 6.3. Tiến trình khởi động Cisco IOS

Các câu lệnh **boot system** cần đề cập đến file chính xác mà router cần nạp. Bảng 6.3 cho thấy nhiều ví dụ của câu lệnh này.

Bảng 6.3. Một số ví dụ lệnh **boot system**

Lệnh khởi động hệ thống	Kết quả
Boot system flash	File đầu tiên của bộ nhớ Flash được nạp
Boot system flash filename	IOS có tên được nạp từ bộ nhớ Flash
Boot system tftp filename 10.1.1.1	IOS có tên được nạp từ TFTP server

Trong một số trường hợp, router gặp lỗi khi nạp OS dựa trên tiến trình ba bước được liệt kê trước đây trong phần này. Ví dụ, một vài người có thể xóa tất cả nội dung của Flash, bao gồm ảnh IOS. Vì thế router cần nhiều tham số hơn để giúp khôi phục từ những lỗi không mong đợi nhưng vẫn có thể xảy ra này. Nếu không có OS này được tìm thấy trong bước 3, router sẽ gửi các gói quảng bá để tìm kiếm TFTP

server, đoán một tên file cho ảnh IOS, và nạp một ảnh IOS (giả sử rằng TFTP server này được tìm thấy). Bước cuối cùng đơn giản nạp ROMMON, được thiết kế để cung cấp các công cụ để khôi phục từ những loại vấn đề không mong đợi như trên. Lấy ví dụ, một ảnh IOS có thể được sao chép vào Flash từ một server TFTP trong khi sử dụng ROMMON.

Với các loại router cũ hơn mà có RxBoot OS trong ROM, tiến trình để chọn OS nào để nạp thường tương tự, với hai khác biệt. Khi trường khởi động là 0x1, router nạp OS RxBoot được lưu trữ trong ROM. Tương tự, trong khi tìm kiếm một OS như được mô tả trong sơ đồ trước, nếu nỗ lực tìm kiếm một ảnh từ một TFTP server bị lỗi, và router có một ảnh RxBoot, router trước tiên thử nạp RxBoot trước khi thử nạp ROM Monitor OS.

6.6.4. Câu lệnh `show version` và tìm kiếm giá trị của thanh ghi cấu hình

Câu lệnh `show version` cung cấp một lượng lớn thông tin về router, bao gồm cả giá trị hiện hành của thanh ghi cấu hình và giá trị mong đợi tại lần nạp kế tiếp của router. Danh sách sau đây liệt kê một số thông tin đáng quan tâm trong câu lệnh này.

1. Phiên bản IOS
2. Thời gian uptime (khoảng thời gian tính từ khi lần tái nạp cuối cùng)
3. Nguyên nhân cho lần tái nạp cuối cùng của IOS (câu lệnh reload, bật tắt nguồn, lỗi phần mềm)
4. Thời gian nạp cuối cùng của IOS (nếu dòng hồ router đã được thiết lập)
5. Nguồn từ đó router nạp IOS hiện tại
6. Số lượng bộ nhớ RAM
7. Số lượng và loại giao tiếp
8. Số lượng bộ nhớ NVRAM
9. Số lượng bộ nhớ Flash
10. Thiết lập hiện tại và tương lai của thanh ghi cấu hình (nếu khác)

Ví dụ sau cho thấy đầu ra của câu lệnh show version, in đậm các thông tin chính. Chủ ý rằng danh sách trên cùng thứ tự với thông tin được làm đậm xuất hiện trong ví dụ này.

```
Albuquerque#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(0)T, RELEASE
  SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.

Compiled Fri 16-Jun-06 21:26 by prod_rel_team

ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

Albuquerque uptime is 5 hours, 20 minutes
System returned to ROM by reload at 13:12:26 UTC Wed Jan 17 2007
System restarted at 13:13:38 UTC Wed Jan 17 2007
System image file is 'flash:c1841-adventerprisek9-mz.124-9.T.bin'

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wl/export/crypto/tool/storg.html

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

Cisco 1841 (revision 4.1) with 354304K/38912K bytes of memory.
Processor board ID FTX0006V03T
2 FastEthernet interfaces
4 Serial(sync/async) interfaces
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity disabled.
192K bytes of NVRAM.
125440K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102 (will be 0x2101 at next reload)
```

continues

Hầu hết thông tin được làm nổi bật trong ví dụ này có thể dễ dàng được tìm thấy trong khi so sánh với danh sách trong ví dụ trên. Tuy nhiên, chú ý rằng bộ nhớ RAM, được liệt kê là 354304K/38912K, thể hiện RAM trong hai phần. Tổng của hai phần này là lượng RAM tổng cộng, khoảng 72MB.

6.7. CÂU HỎI VÀ BÀI TẬP CHƯƠNG 6

Câu 1. Bước cài đặt nào sau đây thường được sử dụng trên router Cisco, nhưng không thường yêu cầu trên switch?

- a. Kết nối cáp Ethernet
- b. Kết nối cáp serial
- c. Kết nối cổng console
- d. Kết nối cáp nguồn
- e. Bật công tắc lên “on”

Câu 2. Vai trò nào sau đây mà một router SOHO thường thực hiện khi gán địa chỉ IP?

- a. DHCP server trên giao tiếp kết nối với phía ISP
- b. DHCP server trên giao tiếp kết nối đến phía các PC ở nhà/ văn phòng
- c. DHCP client trên giao tiếp kết nối với ISP
- d. DHCP client trên giao tiếp kết nối với PCs ở nhà/ văn phòng

Câu 3. Chức năng nào sau đây thường mong đợi có liên quan với router CLI, nhưng không phải với switch CLI?

- a. Lệnh clock rate
- b. Lệnh ip address address mask
- c. Lệnh ip address dhcp
- d. Lệnh interface vlan 1

Câu 4. Mua 2 router Cisco để sử dụng, kết nối mỗi router đến một LAN khác nhau sử dụng giao tiếp Fa0/0 của chúng cũng kết nối hai giao tiếp serial của router sử dụng một cáp back – to – back.

Các bước nào sau đây không được yêu cầu để có thể chuyển IP trên cả hai giao tiếp của router?

- a. Cấu hình một địa chỉ IP trên mỗi giao tiếp serial và FastEthernet của router.
- b. Cấu hình lệnh bandwidth trên một giao tiếp serial của router
- c. Cấu hình lệnh clock rate trên một giao tiếp serial của router
- d. Thiết lập description trên cả hai giao tiếp serial và FastEthernet của mỗi router.

Câu 5. Đầu ra lệnh show ip interface brief trên R1 liệt kê mã trạng thái giao tiếp down và down cho giao tiếp Serial 0/0. Điều nào sau đây có thể đúng?

- a. Lệnh shutdown được cấu hình trên giao tiếp đó
- b. Giao tiếp serial R1 đã được cấu hình sử dụng Frame Relay, nhưng router ở phía đầu kia của liên kết serial được cấu hình sử dụng PPP
- c. Giao tiếp serial của R1 không có cáp serial được cài đặt
- d. Cả hai router đã được nối cáp đến một liên kết serial đang làm việc (chưa có CSU/DSU), nhưng chỉ một router đã được cấu hình với địa chỉ IP.

Câu 6. Lệnh nào sau đây không liệt kê địa chỉ IP và mặt nạ của ít nhất một giao tiếp?

- a. show running – config
- b. show protocols type number
- c. show ip interface brief
- d. show interfaces
- e. show version

Câu 7. Khác biệt nào trên CLI Cisco switch so với CLI Cisco router?

- a. Lệnh được sử dụng cấu hình mật khẩu đơn kiểm tra cho console
- b. Số địa chỉ IP được cấu hình

- c. Loại câu hỏi được đưa ra trong chế độ thiết lập
- d. Cấu hình của tên thiết bị
- e. Cấu hình mô tả một giao tiếp

Câu 8. Điều nào sau đây có thể làm cho một router thay đổi IOS được nạp khi router khởi động?

- a. Lệnh reload EXEC
- b. Lệnh boot EXEC
- c. Lệnh reboot EXEC
- d. Lệnh cấu hình boot system
- e. Lệnh cấu hình reboot system
- f. Thanh ghi cấu hình

Câu 9. Giá trị thập lục phân sau đây trong phần cuối của thanh ghi cấu hình có thể làm cho một router không tìm kiếm IOS trong bộ nhớ Flash

- a. 0
- b. 2
- c. 4
- d. 5
- e. 6

Chương 7

ĐỊNH TUYẾN TĨNH VÀ CON ĐƯỜNG KẾT NỐI TRỰC TIẾP

7.1. ĐỊNH TUYẾN VÀ ĐÁNH ĐỊA CHỈ IP

Việc định tuyến IP tùy thuộc vào các quy tắc về đánh địa chỉ IP, với một trong số các mục đích thiết kế cơ bản cho việc đánh địa chỉ IP trở thành nguyên tắc thiết kế định tuyến IP có hiệu quả. Việc định tuyến IP là xác định con đường đi của một gói tin từ máy tính gửi đến máy tính đích. Các quy tắc đánh địa chỉ IP, nhóm các địa chỉ IP thành các tập hợp địa chỉ đánh số liên tục được gọi là các mạng con, nhằm mục đích chuyển tiếp hay định tuyến IP.

7.2. ĐỊNH TUYẾN IP

Cả máy tính và router tham gia vào tiến trình định tuyến IP. Phản tiếp theo liệt kê tóm tắt hoạt động của một máy tính khi chuyển tiếp một gói tin, giả sử rằng thiết bị này trên một LAN Ethernet hay một LAN không dây:

- Khi gửi một gói tin, so sánh địa chỉ IP đích của gói tin với máy gửi về khoảng địa chỉ trong mạng con có kết nối đó, dựa trên địa chỉ IP và mặt nạ mạng con đó.
- Nếu đích là trên cùng mạng con với máy tính, gửi gói tin một cách trực tiếp đến máy tính đích. Giao thức phân phối địa chỉ ARP cần thiết để tìm kiếm địa chỉ MAC của máy tính đích.
- Nếu đích không cùng mạng con với máy tính gửi, thì gửi gói tin trực tiếp đến cổng định sẵn (default gateway) của máy tính. ARP là cần thiết để tìm địa chỉ MAC của default gateway.

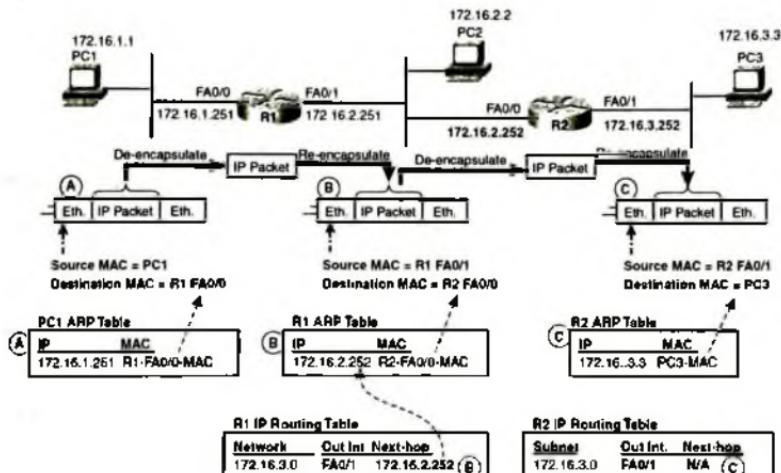
Router sử dụng các bước chung sau đây, chú ý rằng với router, gói tin trước tiên phải được nhận, trong khi thiết bị gửi (được xem xét trước đây) bắt đầu với gói IP trong bộ nhớ:

- Với mỗi frame nhận được, sử dụng trường kiểm tra thứ tự của trailer FCS để đảm bảo rằng frame không có lỗi; nếu lỗi xảy ra, hủy frame đó đi (và không tiếp tục ở bước kế tiếp).
- Kiểm tra địa chỉ lớp liên kết dữ liệu của frame đích, và xử lý chỉ nếu được đưa địa chỉ đến router này hay một địa chỉ quảng bá/quảng bá nhóm.
- Hủy các trường tiêu đề và hậu đê lớp da link của frame đến, để lại gói IP.
- So sánh địa chỉ IP đích của gói tin với bảng định tuyến, và tìm con đường trùng khớp với địa chỉ đến. Con đường này xác định giao tiếp ra ngoài của router, và có thể là router chặng kế tiếp.
- Xác định địa chỉ lớp liên kết dữ liệu đích được sử dụng cho việc chuyển các gói tin đến router hay máy tính kế tiếp (như được định hướng trong bảng định tuyến).
- Đóng gói gói IP bên trong một tiêu đề và hậu đê da link mới; tương ứng với giao tiếp ra, và chuyển tiếp frame ra ngoài giao tiếp đó.

Ví dụ, xem xét hình 7.1, cho thấy một mạng đơn giản với hai router và ba máy tính. Trong trường hợp này, PC1 tạo một gói tin để được gửi đến địa chỉ IP của PC3, có tên là 172.16.3.3. Hình này cho thấy ba bước định tuyến chính, được đánh nhãn là A, B và C; Mục đích định tuyến của PC1 là chuyển tiếp gói tin đến R1, R1 muốn chuyển gói tin đó sang R2 và R2 sẽ chuyển gói tin về PC2.

Trước tiên, xem xét bước A từ hình 7.1. PC1 biết địa chỉ IP của chính nó là 172.16.1.1, mặt nạ 255.255.255.0 (tất cả các giao tiếp sử dụng mặt nạ đơn giản 255.255.255.0 trong ví dụ này) PC1 có thể tính toán số mạng con của nó (172.16.1.0/24) và khoảng địa chỉ (172.16.1.1 – 172.16.1.254) Địa chỉ đích 172.16.3.3 không phải cùng mạng con PC1,

vì thế PC 1 sử dụng bước 1B trong phần tóm tắt về định tuyến, PC1 gửi gói tin đi, bên trong frame Ethernet, đến default gateway của nó là 172.16.1.251.



Hình 7.1. Tiến trình định tuyến qua router và PC

Bước đầu tiên (bước A) khi PC1 gửi gói tin đến default gateway của nó cũng ôn lại hai khái niệm quan trọng. Như có thể thấy từ phần thấp hơn trong hình này, PC1 sử dụng địa chỉ MAC của riêng nó như là địa chỉ MAC nguồn, nhưng nó sử dụng địa chỉ MAC LAN R1 như là địa chỉ MAC đích. Kết quả là bất kỳ switch LAN nào có thể chuyển frame một cách chính xác đến giao tiếp Fa0/0 của R1. Cũng chú ý rằng PC1 tìm kiếm và thấy địa chỉ MAC 172.16.1.251 của R1 trong cache ARP. Nếu địa chỉ MAC này không được tìm thấy, PC1 phải sử dụng ARP để tự động tìm kiếm địa chỉ MAC được sử dụng bởi 172.16.1.251 (R1) trước khi có thể gửi frame đi như thể hiện trong hình 7.1.

Kế tiếp tập trung vào bước B trong hình 7.1, là công việc được thực hiện bởi router để chuyển gói tin đi. Sử dụng sáu định tuyến tóm lược của router để xử lý hình 7.1, xảy ra như sau tại R1. Chú ý rằng hình trên thể hiện nhiều chi tiết với kí tự B.

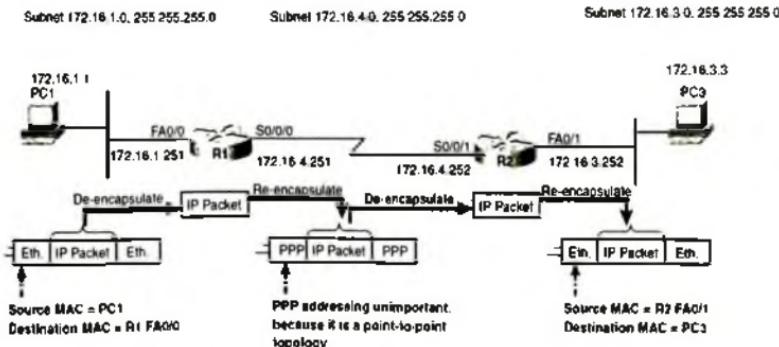
- R1 kiểm tra FCS, và frame đó không có lỗi
- R1 tìm thấy địa chỉ MAC giao tiếp Fa0/0 của nó trong địa chỉ MAC của frame đích, vì thế, R1 sẽ xử lý gói tin được đóng gói này.
- R1 hủy tiêu đề và hậu đê của lớp liên kết dữ liệu cũ, đê lại gói IP (như thể hiện trực tiếp bên dưới biểu tượng R1 trong hình 7.1).
- Trong phần dưới trung tâm của hình 7.1, R1 so sánh địa chỉ IP đích (172.16.3.3) với bảng định tuyến, tìm thấy con đường phù hợp trong hình này, với địa chỉ giao tiếp ra ngoài Fa0/1 và router chặng kế tiếp là 172.16.2.252.
- R1 cần tìm địa chỉ MAC thiết bị chặng kế tiếp (địa chỉ MAC của R2), vì thế R1 tìm kiếm và thấy rằng địa chỉ MAC đó trong bảng ARP của nó.
- R1 đóng gói gói tin IP trong một frame Ethernet mới, với địa chỉ MAC Fa0/1 của R1 là địa chỉ MAC nguồn, và địa chỉ MAC Fa0/0 của R2 là địa chỉ MAC đích. R1 gửi gói tin này đi.

Vấn đề này phức tạp, có thể xem xét các phiên bản đơn giản hơn cho vấn đề này như sau. Ví dụ, khi xử lý định tuyến, tập trung vào bước 4 – tìm địa chỉ IP đích của gói tin trùng khớp trong bảng định tuyến – có thể là một trong các bước quan trọng nhất. Vì thế, phiên bản tóm tắt hơn cho tiến trình định tuyến có thể là: Router nhận một gói tin, so khớp địa chỉ đích gói tin đó với bảng định tuyến và chuyển gói tin dựa trên con đường trùng khớp đó. Và để kết thúc ví dụ này, xem xét ngũ cành chuyển tiếp router 6 bước được áp dụng trên router R2, được liệt kê là kí tự C trong hình 7.1, như sau:

- R2 kiểm tra FCS, và frame không có lỗi
- R2 tìm địa chỉ MAC giao tiếp Fa0/0 của nó trong trường địa chỉ MAC đích của frame, vì thế R2 sẽ xử lý gói tin đã đóng gói này.
- R3 hủy các tiêu đề và hậu đê lớp liên kết dữ liệu cũ, đê lại gói IP, như thể hiện trong biểu tượng R2 hình 7.1.

- Trong phần dưới góc phải của hình 7.1 R2 so sánh địa chỉ IP đích (172.16.3.3) với bảng định tuyến R2, tìm kiếm con đường trùng khớp được thể hiện trong hình, với giao tiếp ra Fa0/1 và không có router chặng kế tiếp được liệt kê.
- Vì không có router chặng kế tồn tại, R2 cần tìm địa chỉ MAC thiết bị đích thực (địa chỉ MAC PC3), vì thế R2 tìm kiếm và thấy địa chỉ MAC đó trong bảng ARP của nó.
- R2 đóng gói gói IP trong một frame Ethernet mới, với địa chỉ MAC Fa0/1 của R2 là địa chỉ MAC nguồn, và địa chỉ MAC của PC3 (mỗi bảng định tuyến ARP) là địa chỉ MAC đích. R1 gửi frame đi.
- Cuối cùng, khi frame này đến PC3, PC3 thấy địa chỉ MAC của nó được liệt kê như là địa chỉ MAC đích, vì thế PC bắt đầu xử lý frame này.

Tiến trình xử lý tương tự cũng làm việc với các liên kết WAN, với một số chi tiết khác biệt. Trên các liên kết điểm – điểm, như thể hiện trong hình 7.2, bảng ARP là không cần thiết. Bị một liên kết điểm – điểm có thể có ít nhất một router kết nối đến nó, có thể bỏ qua địa chỉ liên kết dữ liệu này. Tuy nhiên, với Frame Relay, tiến trình định tuyến quan tâm đến các địa chỉ liên kết dữ liệu này, được gọi là định danh kết nối liên kết dữ liệu (DLCI).



Hình 7.1. Tiến trình định tuyến qua router và PC (tiếp theo)

Tiến trình định tuyến IP trên cả máy tính và router dựa trên khả năng của các thiết bị này để biết địa chỉ IP và dự đoán các địa chỉ IP nào trên mỗi nhóm hay subnet. Phần kế tiếp ôn lại các địa chỉ IP và phân chia mạng con.

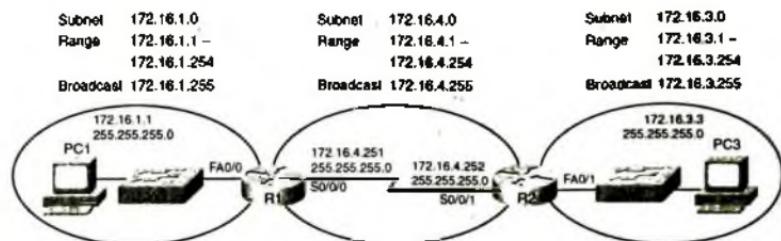
7.2.1. Địa chỉ IP và phân mạng con

Các quy tắc đánh địa chỉ IP cho tiến trình định tuyến IP bằng cách yêu cầu các địa chỉ IP được tổ chức thành các nhóm các địa chỉ IP được đánh số liên tục được gọi là **mạng con**. Để cho phép sử dụng mạng con, việc đánh địa chỉ IP định nghĩa một khái niệm gọi là **số mạng con** và **mặt nạ mạng con**, xác định một cách chính xác khoảng địa chỉ trong một mạng con. Ví dụ, router trong hình 7.1 sử dụng các con đường được đánh số mạng con là 172.16.3.0 khi chuyển tiếp các gói tin đến PC3 (172.16.3.3). Hình trên bỏ qua mặt nạ mạng để giảm bớt rườm rà, nhưng mọi thiết bị có thể nhìn vào số mạng con 172.16.3.0 với mặt nạ mạng là 255.255.255.0 và biết rằng có hai số giới thiệu một cách vắn tắt cho mạng con đó như sau:

- Số mạng con là 172.16.3.0
- Khoảng địa chỉ có thể sử dụng trong mạng con là: 172.16.3.1 – 172.16.3.254
- Địa chỉ quảng bá mạng con (không dùng cho các thiết bị riêng): 172.16.3.255
- Danh sách sau cung cấp sơ qua một số khái niệm địa chỉ IP chính. Chú ý rằng chương này chủ yếu đề cập về các địa chỉ IPV4, và chương 17, đề cập đến IPV6.
- Các địa chỉ IP unicast là các địa chỉ IP có thể được gán cho một giao tiếp đơn để gửi và nhận các gói tin
- Mỗi địa chỉ IP unicast dựa trên một lớp mạng cụ thể A, B, C được gọi là **mạng IP** có phân lớp
- Nếu phân mạng con được sử dụng, điều này hầu như luôn đúng trong thực tế, mỗi địa chỉ IP unicast cũng thuộc về một mạng con cụ thể của một mạng có phân lớp được gọi là **mạng con**

- **Mặt nạ mạng con**, được viết dưới dạng dấu chấm thập phân, ví dụ 255.255.255.0, hay dạng cú pháp tiền tố (ví dụ, /24) xác định cấu trúc địa chỉ IP unicast, và cho phép các thiết bị và người dùng sử dụng số mạng con, khoảng địa chỉ và địa chỉ quảng bá cho một mạng con đó.
- Các thiết bị trên cùng mạng con tất cả sẽ sử dụng cùng mặt nạ mạng con; hay là chúng có các lựa chọn khác về khoảng địa chỉ trên mạng con đó, mà có thể phá vỡ tiến trình định tuyến IP.
- Các thiết bị trên một VLAN đơn nên cùng một mạng con IP đơn.
- Các thiết bị trên các VLAN khác nhau nên ở các mạng con khác nhau.
- Để chuyển gói tin giữa các mạng con, một thiết bị thực hiện chức năng định tuyến được sử dụng. Trong sách này, chỉ router được sử dụng, nhưng với các thiết bị switch đa lớp, các switch thực hiện chức năng định tuyến – có thể được sử dụng.
- Các liên kết điểm – điểm serial sử dụng mạng con khác với mạng con LAN, nhưng những mạng con này chỉ yêu cầu hai địa chỉ IP, một cho mỗi giao tiếp của router trên đầu cuối khác nhau của liên kết đó.
- Các máy tính được phân tách bởi một router phải được đặt trên các mạng con tách rời.

Hình 7.3 cho thấy một ví dụ liên mạng chứa nhiều chức năng này. Switch SW1 mặc định đặt tất cả các giao tiếp vào VLAN 1, vì thế tất cả các máy tính bên trái (gồm PC1) là trên một mạng con đơn. Chú ý rằng địa chỉ IP quản lý của SW1, cũng trên VLAN 1, sẽ từ cùng subnet đó. Tương tự, SW2 mặc định đặt tất cả các port vào trong VLAN 1, yêu cầu một mạng con thứ hai. Liên kết điểm – điểm yêu cầu một mạng con thứ ba. Hình trên cho thấy số mạng con, mặt nạ và khoảng địa chỉ. Chú ý rằng tất cả các địa chỉ và các mạng con là thành phần của cùng mạng con có phân lớp Lớp B 172.16.0.0, và tất cả các mạng con sử dụng cùng mặt nạ 255.255.255.0



Hình 7.3. Tiến trình định tuyến qua router và PC (tiếp theo)

Hình 7.3 liệt kê số mạng con, khoảng địa chỉ, và địa chỉ quảng bá của mỗi mạng con này. Tuy nhiên, mỗi thiết bị trên hình có thể tìm kiếm cùng thông tin chỉ dựa trên địa chỉ IP của nó và cấu hình mặt nạ mạng con, dựa trên chỉ số mạng con, khoảng địa chỉ và địa chỉ quảng và cho mỗi mạng con có kết nối đến này.

7.2.2. Chuyển tiếp IP bằng cách tìm kiếm con đường phù hợp nhất

Bất kì tiến trình định tuyến IP nào của router cũng yêu cầu rằng router đó so sánh địa chỉ IP đích của mỗi gói với nội dung có sẵn trong bảng định tuyến IP của router đó. Thường thì, chỉ có một đường phù hợp với địa chỉ đích cụ thể. Tuy nhiên, trong một số trường hợp, một địa chỉ đích cụ thể có thể phù hợp với nhiều đường của router. Một số nguyên nhân thông thường và xác đáng cho các con đường trùng lắp này trong bảng định tuyến như sau:

- Sử dụng chức năng tự động tóm lược
- Tóm lược con đường thủ công
- Sử dụng các con đường tĩnh
- Phân chia mạng con được thiết kế không chính xác, vì thế mạng con đó trùng lắp khoảng địa chỉ của nó.

Trong chương 9, VLSM và tóm lược con đường, giải thích chi tiết hơn về mỗi nguyên nhân này. Trong một số trường hợp việc trùng lắp con đường phát sinh vẫn đề, trường hợp khác thì hoạt động bình thường từ một số chức năng khác. Phần này tập trung vào cách router chọn con đường trùng lắp nào để sử dụng, với các chức năng có thể làm cho trùng lắp được xem xét trong chương 9.

Phần sau tóm tắt ý nghĩa của một router với các con đường trùng lắp: *Khi một địa chỉ IP đích cụ thể trùng với hơn một con đường trong một bảng định tuyến, router sử dụng con đường cụ thể nhất, nói cách khác, con đường với chiều dài tiền tố lớn nhất.*

Để thấy được điều này có nghĩa là gì, bảng định tuyến liệt kê trong ví dụ 7.1 thể hiện một chuỗi các con đường bị trùng lắp. Trước tiên, trước khi xem xét nó, thử dự đoán con đường nào sẽ được sử dụng để các gói tin được gửi đi đến địa chỉ IP sau: 172.16.1.2, 172.16.1.2, 172.16.1.3 và 172.16.1.4.

```
Router#show ip route rip
172.16.0.0/16 is variably subnetted, 5 subnets, 4 masks
A     172.16.1.0/32 [120/1] via 172.16.25.2, 00:00:04, Serial0/1/1
R     172.16.1.0/24 [120/2] via 172.16.25.129, 00:00:09, Serial0/1/1
R     172.16.0.0/22 [120/1] via 172.16.25.2, 00:00:04, Serial0/1/1
R     172.16.0.0/16 [120/2] via 172.16.25.129, 00:00:09, Serial0/1/0
R     0.0.0.0/0 [120/3] via 172.16.25.129, 00:00:09, Serial0/1/0
Router#show ip route 172.16.4.3
Routing entry for 172.16.0.0/16
  Known via "rip", distance 120, metric 2
  Redistributing via rip
  Last update from 172.16.25.129 on Serial0/1/0, 00:00:19 ago
  Routing Descriptor Blocks:
    * 172.16.25.129, from 172.16.25.129, 00:00:19 ago, via Serial0/1/0
      Route metric is 2, traffic share count is 1
```

Trong khi sơ đồ hệ thống mạng có thể được cung cấp với câu hỏi này, thực sự chỉ cần hai thông tin để xác định con đường nào sẽ được phù hợp: địa chỉ IP đích của gói tin và nội dung của bảng định tuyến trên router. Bằng cách kiểm tra mỗi mạng con và mặt nạ trên bảng định tuyến này, có thể xác định khoảng địa chỉ IP trong mỗi mạng con. Trong trường hợp này, khoảng địa chỉ được xác định bởi mỗi con đường, một cách riêng rẽ, như sau:

- 172.16.1.1 (chỉ một địa chỉ này)
- 172.16.1.0 – 172.16.1.255
- 172.16.0.0 – 172.16.3.255
- 172.16.0.0 – 172.16.255.255
- 255.255.255.255

Con đường được liệt kê là 0.0.0.0/0 là con đường mặc định, phù hợp với tất cả địa chỉ IP và nó được giải thích trong phần sau của chương này.

Như có thể thấy từ những khoảng này, nhiều khoảng địa chỉ của các con đường trùng lặp nhau. Khi trùng hơn một con đường, con đường với chiều dài tiền tố lớn hơn sẽ được sử dụng. Ví dụ:

- 172.16.1.1: trùng với 5 con đường, chiều dài lớn nhất là /32, con đường đến 172.16.1.1/32
- 172.16.1.2: trùng với 4 con đường cuối, tiền tố lớn nhất là /24, con đường đến 172.16.1.0/24
- 172.16.2.3: trùng với ba con đường cuối, tiền tố lớn nhất là /22, con đường đến 172.16.0.0/22
- 172.16.4.3: Trùng với hai con đường cuối, tiền tố lớn nhất là /16, con đường đến 172.16.0.0/16

Bên cạnh việc chỉ thực hiện phép toán phân mạng con trên mỗi con đường trong bảng định tuyến, lệnh `show ip route ip-address` cũng có thể hữu dụng nhất định. Lệnh này liệt kê thông tin chi tiết về con đường mà router phù hợp với địa chỉ IP được liệt kê trong lệnh đó. Nếu nhiều con đường phù hợp với địa chỉ IP đó, lệnh này liệt kê con đường tốt nhất: con đường với chiều dài tiền tố lớn nhất. Ví dụ 7.1 liệt kê đầu ra của lệnh `show ip route 172.16.4.3`. Đầu ra của dòng đầu tiên liệt kê con đường phù hợp: con đường đến 172.16.0.0/16. Phần còn lại của kết quả liệt kê chi tiết về con đường cụ thể đó.

7.2.3. DNS, DHCP, ARP và ICMP

Tiến trình định tuyến sử dụng nhiều giao thức có liên quan, bao gồm giao thức ARP đã đề cập trong chương này. Trước khi đi vào chủ đề mới trong chương này, phần này ôn lại nhiều giao thức có liên quan.

Trước khi một thiết bị có thể gửi bất kỳ gói tin IP nào, thiết bị cần biết nhiều tham số liên quan đến IP. Các máy tính thường sử dụng Dynamic Host Configuration Protocol để tìm hiểu các yếu tố chính sau đây, bao gồm:

- Địa chỉ IP của máy tính
- Mật mã mạng có liên quan
- Địa chỉ IP của gateway mặc định
- Địa chỉ IP của DNS server

Để tìm hiểu thông tin này, máy tính – DHCP client – gửi một gói tin quảng bá đến DHCP Server. Server sau đó có thể cấp phát một địa chỉ IP cho thiết bị đó và cung cấp thông tin khác trong danh sách trước đây. Tại thời điểm này, máy tính có một địa chỉ IP được sử dụng như là địa chỉ IP nguồn, và dù thông tin để thực hiện quyết định định tuyến đơn giản như là sẽ gửi các gói tin trực tiếp đến thiết bị khác (cùng mạng con) hay đến gateway mặc định (mạng con khác).

Thông thường, người dùng hoặc là ám chỉ đến trực tiếp hay gián tiếp tên một máy tính khác, và máy tính này tiếp tục sử dụng tên của máy tính khác để gửi gói tin đi. Ví dụ, mở một trình duyệt web, và gõ vào <http://www.viethanit.edu.vn> như là địa chỉ URL xác định tên máy tính web server của trường CĐ CNTT HN Việt Hàn. Mở một email client như Microsoft Outlook tức là gián tiếp đến đề cập đến tên một máy tính. Email client này được cấu hình để biết tên máy tính của các mail server đi và đến, vì thế người dùng không quan tâm các thiết lập này hàng ngày, phần mềm email client vẫn biết tên máy tính nó sẽ trao đổi mail.

Vì các thiết bị không thể gửi các gói tin đến tên máy tính đích, hầu hết các máy tính sử dụng giao thức DNS để phân giải tên miền sang địa chỉ IP của nó. Máy tính này hoạt động như một DNS client, gửi các gói tin đến địa chỉ IP unicast của DNS server. Yêu cầu DNS liệt kê tên (ví dụ, www.cisco.com), với server phản hồi địa chỉ IP tương ứng với tên thiết bị đó. Sau khi nó đã học xong, máy tính có thể lưu trữ đệm thông tin chuyển đổi tên – sang – địa chỉ, cần thiết để phân giải tên trở lại khi mục đó hết hạn sử dụng. (Trong Windows XP, lệnh `ipconfig/displaydns` liệt kê danh sách tên và địa chỉ các máy tính hiện tại).

ICMP (Internet Control Message Protocol) gồm nhiều chức năng khác nhau, tất cả tập trung vào điều khiển và quản lý IP. ICMP định

nghĩa tập các thông điệp khác nhau với nhiều mục đích khác nhau, bao gồm các thông điệp ICMP Echo Request và ICMP Echo Reply. Lệnh thông dụng ping kiểm tra con đường đến một máy tính ở xa, và trả về con đường đến máy tính ban đầu, bằng cách gửi Echo Request messages đến địa chỉ IP đích và địa chỉ IP đích đó phản hồi lại mỗi thông điệp Echo Request với thông điệp Echo Reply.

Khi lệnh ping nhận các thông điệp Echo Reply, lệnh đó biết rằng con đường giữa hai máy tính đang hoạt động tốt.

Tất cả các giao thức này hoạt động cùng với nhau để hỗ trợ cho tiến trình định tuyến, nhưng DHCP, DNS ICMP và ARP thường không xuất hiện với mọi gói tin. Ví dụ, tưởng tượng một máy tính mới kết nối đến LAN, và người dùng sử dụng lệnh ping www.cisco.com. DHCP có thể được sử dụng khi hệ điều hành khởi động, khi máy tính sử dụng DHCP để tìm hiểu địa chỉ IP và thông tin khác, nhưng sau đó DHCP có thể không được sử dụng trong nhiều ngày. Máy tính sau đó sử dụng DNS để phân giải www.cisco.com thành một địa chỉ IP, nhưng sau đó PC không cần sử dụng DNS lại cho đến khi tên máy tính mới được sử dụng. Nếu máy tính đang ping đến một máy tính ở xa, máy tính cục bộ tạo một gói tin IP, với thông điệp ICMP Echo Request bên trong gói tin này, với địa chỉ IP đích của các địa chỉ IP nó học được bằng yêu cầu DNS trước đó. Cuối cùng, vì máy tính vừa mới hoạt động, nó không có mục ARP nào cho gateway mặc định của nó, vì thế máy tính phải sử dụng ARP để tìm kiếm địa chỉ IP cho gateway mặc định này. Chỉ sau đó thì gói tin có thể được gửi ra đúng địa chỉ máy tính đích, như được miêu tả trong phần đầu của chương. Với các gói tin có thứ tự được gửi đến cùng máy tính, những giao thức này có thể không cần được sử dụng lại, và máy tính nội bộ có thể chỉ gửi gói tin mới này đi.

Danh sách sau đây tóm tắt các bước được sử dụng bởi một máy tính, khi cần thiết cho các giao thức được đề cập trong phần này:

- Nếu nó chưa biết, máy tính sử dụng DHCP để học địa chỉ IP, mặt nạ mạng, địa chỉ IP DNS và gateway mặc định của nó. Nếu đã biết, máy tính bỏ qua bước này.

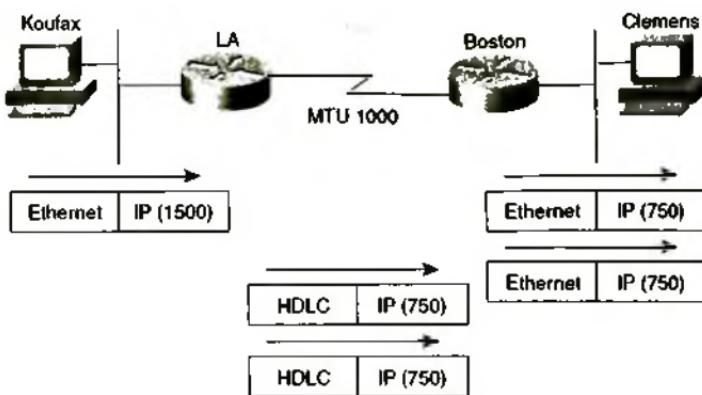
- Nếu người dùng truy cập đến tên một máy tính hiện không có trong bộ nhớ cache của máy tính đó, máy tính thực hiện một yêu cầu DNS để phân giải tên đó thành địa chỉ IP tương ứng. Ngược lại, bước này bỏ qua.
- Nếu người dùng sử dụng lệnh ping, gói IP chứa thông tin của ICMP Echo Request; nếu người dùng thay vào đó sử dụng một ứng dụng TCP/IP thông thường, thì họ sử dụng giao thức tương ứng với ứng dụng đó.
- Để tạo một frame Ethernet, máy tính sử dụng mục cache ARP cho thiết bị chặng kế tiếp – hoặc là gateway mặc định (khi gửi đến một máy tính trên một mạng con khác) hay đúng máy tính đó (khi gửi đến một máy tính trên cùng một mạng). Nếu ARP cache không chứa giá trị này, máy tính sử dụng ARP để tìm kiếm thông tin này.

7.2.4. Phần mảnh và MTU

TCP/IP xác định chiều dài tối đa cho một gói tin IP. Thuật ngữ được sử dụng để miêu tả chiều dài tối đa là đơn vị truyền thông tối đa (MTU).

MTU khác nhau dựa trên cấu hình và đặc tính của giao tiếp. Mặc định một máy tính tính toán MTU của một giao tiếp dựa trên kích thước tối đa của phần dữ liệu của frame liên kết dữ liệu (trong đó gói tin được chứa). Ví dụ, giá trị MTU mặc định trên giao tiếp Ethernet là 1500.

Router, giống như bất kỳ máy tính IP nào, không thể chuyển tiếp một gói tin ra ngoài giao tiếp nếu gói tin đó dài hơn MTU. Nếu một MTU của giao tiếp router nhỏ hơn gói tin phải được chuyển đi, router phân đoạn gói tin thành các gói tin nhỏ hơn. Việc phân đoạn là tiến trình chia nhỏ gói tin thành các gói tin nhỏ hơn, mỗi một gói tin này nhỏ hơn hay bằng với giá trị MTU. Hình 7.4 cho thấy một ví dụ về phân đoạn trong mạng khi MTU trên liên kết serial thấp hơn 1000byte qua cầu hình.



Hình 7.4. Ví dụ về phân đoạn mạng trong định tuyến

Như mô tả trong hình 7.4, Koufax gửi một gói tin 1500 byte đến router LA. LA gỡ tiêu đề Ethernet nhưng không thể chuyển tiếp gói tin đi được, vì nó là 1500 bytes và liên kết HDLC chỉ hỗ trợ MTU với chỉ 1000. Vì thế LA phân gói tin gốc thành hai gói tin, mỗi gói chiều dài 750 byte. Router thực hiện tính toán yêu cầu để chỉ ra số lượng phân mảnh tối thiểu (hai trong trường hợp này) và chia gói tin gốc thành hai gói tin có độ dài như nhau. Vì thế, bất kì router nào khác mà gói tin phải đi qua không cần thiết phải thực hiện phân mảnh. Sau khi chuyển hai gói tin này, Boston nhận các gói tin đó và chuyển tiếp chúng mà không tái hợp lại. Việc tái hợp được thực hiện tại máy tính đầu cuối, trong trường hợp này là Clemens.

Tiêu đề IP chứa các trường hữu ích cho việc tái hợp các phân mảnh thành gói tin ban đầu. Tiêu đề IP chứa một giá trị ID giống nhau cho mỗi gói tin được phân mảnh, cũng như là giá trị offset xác định phần nào của gói tin gốc được giữ trong mỗi phân mảnh. Các gói tin được phân mảnh đi ra ngoài theo thứ tự có thể được xác định như là một phần của cùng gói tin gốc ban đầu và có thể tái hợp lại theo đúng thứ tự sử dụng trường offset trong mỗi phân mảnh này.

Hai lệnh cấu hình có thể được sử dụng để thay đổi kích thước MTU trong một giao tiếp là: lệnh con giao tiếp `mtu` và lệnh con giao tiếp `ip mtu`. Lệnh `mtu` thiết lập MTU cho tất cả các giao thức lớp 3; trừ khi cần thiết tồn tại một thiết lập khác cho mỗi giao thức lớp 3 này, thì lệnh này được ưu tiên. Nếu một thiết lập khác được thực hiện cho IP, lệnh `ip mtu` thiết lập giá trị được sử dụng cho IP. Nếu cả hai được cấu hình trên một giao tiếp, thiết lập IP MTU được ưu tiên hơn trên giao tiếp đó. Tuy nhiên, nếu lệnh `mtu` được cấu hình sau khi lệnh `ip mtu` được cấu hình, giá trị `ip mtu` được thiết lập lại cùng giá trị như là lệnh `mtu`. Nên cẩn thận khi thay đổi giá trị này.

Việc xem xét định tuyến IP và địa chỉ IP đến đây là hoàn tất. Kế tiếp, chương này kiểm tra các con đường có kết nối, bao gồm các con đường có kết nối liên quan đến Trung kế VLAN và địa chỉ IP thứ hai.

7.3. CÁC CON ĐƯỜNG ĐẾN MẠNG CON KẾT NỐI TRỰC TIẾP

Một router tự động thêm một con đường vào bảng định tuyến của nó cho mạng con có kết nối đến mỗi giao tiếp, giả sử rằng hai yếu tố sau đây là đúng:

- Giao tiếp trong trạng thái làm việc, nối cách khác, trạng thái giao tiếp trong lệnh `show interfaces` liệt kê trạng thái `up` và trạng thái giao tiếp cũng là `up`.
- Giao tiếp có một địa chỉ IP được gán, hoặc là thông qua lệnh `ip address` hay sử dụng DHCP client.

Khái niệm các con đường có kết nối khá là cơ bản. Router cần phải biết số mạng con được sử dụng trên mạng vật lý có kết nối đến mỗi giao tiếp của nó, nhưng nếu giao tiếp hiện không làm việc, router cần gỡ bỏ con đường đó khỏi bảng định tuyến của nó. Lệnh `show ip route` liệt kê các con đường này với một mã đường là `c`, nghĩa là có kết nối, và lệnh `show ip route connected` liệt kê chỉ các con đường có kết nối.

Phần sau về các con đường có kết nối tập trung vào hai biến thể trong cấu hình ánh hướng đến các con đường có kết nối, chính vì thế ánh hướng đến cách router chuyên các gói tin. Chủ đề đầu tiên liên quan đến

một công cụ được gọi là địa chỉ IP thứ cấp, trong khi chủ đề thứ hai liên quan đến việc cấu hình của một router khi sử dụng Trung kế VLAN.

7.3.1. Địa chỉ IP thứ cấp

Tưởng tượng rằng lập kế hoạch cho cơ chế đánh địa chỉ IP cho một mạng, sau đó, mạng con của nó phát triển lên, và đã sử dụng tất cả các địa chỉ IP hợp lệ trong mạng con đó. Tiếp theo nên làm gì? Ba lựa chọn chính là:

- Làm cho mạng con hiện tại lớn hơn
- Tích hợp các thiết bị để sử dụng các địa chỉ trong các mạng con khác, lớn hơn.
- Sử dụng cơ chế địa chỉ thứ cấp

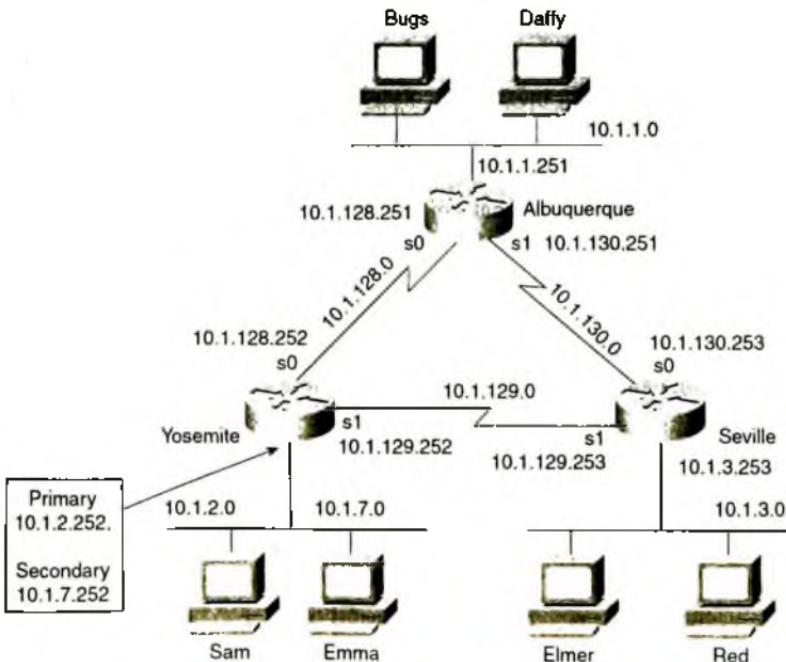
Tất cả ba lựa chọn trên đều có ý nghĩa, nhưng tất cả đều có vấn đề.

Để làm cho mạng con lớn hơn, chỉ cần thay đổi mặt nạ mạng được sử dụng trên mạng con đó. Tuy nhiên, việc thay đổi mặt nạ mạng có thể tạo ra các mạng con trùng lắp. Ví dụ, nếu mạng con 10.1.4.0/24 đang hết địa chỉ, và thực hiện thay đổi mặt nạ thành 255.255.254.0 (9 bit thiết bị, 24 bit mạng con), một mạng con mới chứa các địa chỉ 10.1.4.0 đến 10.1.5.255. Nếu đã gán mạng con 10.1.5.0/24 với các địa chỉ có thể gán 10.1.5.1 đến 10.1.5.253, có thể tạo một mạng con với địa chỉ trùng lắp, điều này không được phép. Tuy nhiên, nếu các địa chỉ 10.1.5.x chưa sử dụng, việc mở rộng mạng con cũ có thể chấp nhận được.

Lựa chọn thứ hai đơn giản là lấy một mạng con mới, lớn hơn, chưa sử dụng. Tất cả các địa chỉ IP sẽ cần phải thay đổi. Đây là một tiến trình khá đơn giản nếu hầu hết hay tất cả các máy tính sử dụng DHCP, nhưng thường không khả thi nếu nhiều máy tính sử dụng các địa chỉ IP cấu hình tĩnh.

Chú ý rằng hai giải pháp đầu này nhấn mạnh chiến thuật sử dụng các mặt nạ khác nhau trong các phần mạng khác nhau. Sử dụng các mặt nạ khác nhau này được gọi là mặt nạ mạng con với chiều dài thay đổi (VLSM), làm cho mạng trở nên phức tạp hơn, cụ thể là cho việc giám sát và xử lý sự cố mạng.

Lựa chọn thứ ba là sử dụng chức năng của router Cisco được gọi là đánh địa chỉ IP thứ cấp. Địa chỉ thứ cấp sử dụng nhiều mạng hay nhiều mạng con trên cùng một liên kết dữ liệu. Bằng cách sử dụng nhiều hơn một mạng con trên cùng một môi trường, làm tăng số địa chỉ IP có thể. Để làm cho nó hoạt động, router cần một địa chỉ IP trên mỗi mạng con để mà các máy tính trên mỗi mạng con này có một địa chỉ IP gateway mặc định trên cùng một mạng con đó. Ví dụ, hình 7.5 có mạng con 10.1.2.0/24, giả sử rằng nó có tất cả các địa chỉ IP đã được gán. Giả sử việc đánh địa chỉ thứ cấp là giải pháp được lựa chọn, mạng con 10.1.7.0 cũng được sử dụng trên cùng Ethernet. Ví dụ 7.2 cho thấy cấu hình cho địa chỉ IP thứ cấp trên Yosemite.



Hình 7.5. Địa chỉ IP thứ cấp trong định tuyến

```

! Excerpt from show running-config follows...
hostname Yosemite
ip domain-lookup
ip name-server 10.1.1.100 10.1.2.100
interface ethernet 0
  ip address 10.1.7.252 255.255.255.0 secondary
  ip address 10.1.2.252 255.255.255.0
interface serial 0
  ip address 10.1.120.252 255.255.255.0
interface serial 1
  ip address 10.1.129.252 255.255.255.0

Yosemite# show ip route connected
  10.0.0.0/24 is subnetted, 4 subnets
C      10.1.2.0 is directly connected, Ethernet0
C      10.1.7.0 is directly connected, Ethernet0
C      10.1.129.0 is directly connected, Serial1
C      10.1.128.0 is directly connected, Serial0

```

Router có con đường có kết nối đến mạng con 10.1.2.0/24 và 10.1.7.0/24, vì thế nó có thể chuyên tiếp các gói tin đến mỗi mạng con này. Các thiết bị trên mỗi mạng con trên cùng LAN có thể sử dụng hoặc là 10.1.2.252 hay 10.1.7.252. như là địa chỉ IP gateway mặc định của nó, tùy thuộc vào mạng con mà nó phụ thuộc vào.

Điều nghịch lý lớn nhất với địa chỉ thứ cấp là các gói tin được gửi giữa các máy tính trên LAN có thể được định tuyến không hiệu quả. Ví dụ, khi máy tính trên mạng con 10.1.2.0 gửi một gói tin đến máy tính 10.1.7.0, mục đích của máy tính gửi là muốn gói tin đến gateway mặc định của nó, vì đích là nằm trên một mạng con khác. Vì thế máy tính gửi gói tin đến router, sau đó gửi ngược lại trên cùng một LAN.

7.3.1.1. Hỗ trợ các con đường có kết nối đến mạng con zero

IOS có thể giới hạn một router khỏi cấu hình ip address với một địa chỉ bên trong mạng con zero. Mạng con zero là một mạng con trong một mạng classful có tất cả các bit 0 trong phần mạng của phiên bản nhị phân của chỉ số mạng con. Trong chỉ số thập phân, mạng con zero đường như cùng chỉ số mạng với chỉ số mạng classful.

Với lệnh ip subnet – zero được cấu hình, IOS cho phép mạng con zero trở thành con đường có kết nối như là kết quả của lệnh ip address

được cấu hình trên một giao tiếp. Lệnh này trở thành thiết lập mặc định kể từ ít nhất phiên bản ISO 12.

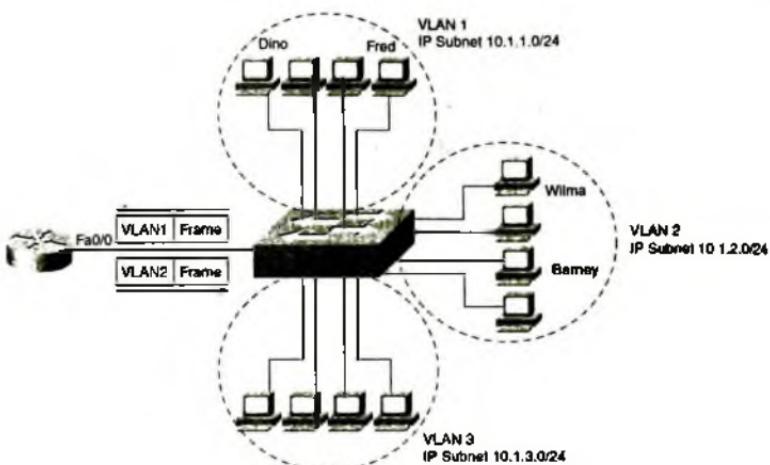
Với lệnh **no ip subnet-zero** được cấu hình trên một router, router đó từ chối bắt kì địa chỉ lệnh **ip address** nào sử dụng kết hợp giữa một địa chỉ/ mặt nạ mạng cho mạng con zero đó. Ví dụ, lệnh con giao tiếp **ip address 10.0.0.1 255.255.255.0** nhấn mạnh mạng con 10.0.0.0/24, vì thế router sẽ từ chối lệnh nếu lệnh thông tin toàn cục **no ip subnet – zero** đã được cấu hình. Chú ý rằng thông điệp lỗi này đơn giản thông báo rằng “mặt nạ sai” hơn là báo về vấn đề với mặt nạ zero.

Lệnh **no ip subnet – zero** trên một router không ảnh hưởng đến các router khác, và nó không ngăn một router khỏi việc học hỏi về một mặt nạ zero qua giao thức định tuyến. Nó đơn giản ngăn router khỏi việc cấu hình một giao tiếp trở thành một mạng con zero.

7.3.1.2. Cấu hình ISL và 802.1Q trên các router

Như đã đề cập trong chương 3, “Mạng LAN ảo”, trung kế VLAN có thể được sử dụng giữa hai switch và giữa một switch và một router. Bằng cách sử dụng trung kế thay vì sử dụng một giao tiếp router thực trên mỗi VLAN, số các giao tiếp router được yêu cầu có thể giảm bớt. Thay vì sử dụng một giao tiếp vật lý đơn trên router cho mỗi VLAN trên switch, một giao tiếp vật lý có thể được sử dụng và router có thể tiếp tục định tuyến các gói tin giữa nhiều VLAN khác nhau.

Hình 7.6 cho thấy một router với một giao tiếp Fast Ethernet đơn và một kết nối đơn đến một switch. Hoặc là ISL hay 802.1Q được sử dụng, với chi các khác biệt nhỏ trong cấu hình cho mỗi phương thức này. Với các frame chứa các gói tin mà router định tuyến giữa hai VLAN, frame đến được đánh dấu bởi switch đó với một VLAN ID, và frame đi được đánh dấu bởi router đó với một VLAN ID khác. Ví dụ 7.3 cho thấy cấu hình được yêu cầu của một router hỗ trợ đóng gói ISL và chuyển tiếp giữa các VLAN này.



Hình 7.6. Định tuyến giữa các VLAN

```

interface fastethernet 0/0.1
ip address 10.1.1.1 255.255.255.0
encapsulation isl 1
!
interface fastethernet 0/0.2
ip address 10.1.2.1 255.255.255.0
encapsulation isl 2
!
interface fastethernet 0/0.3
ip address 10.1.3.1 255.255.255.0
encapsulation isl 3

```

Ví dụ 7.3 cho thấy cấu hình của ba giao tiếp con của giao tiếp Fast Ethernet trên router này. Một giao tiếp con là một phân nhánh con luân lý của giao tiếp vật lý. Router gán mỗi giao tiếp con một địa chỉ IP và gán giao tiếp con một VLAN đơn. Vì thế, thay vì ba giao tiếp vật lý trên router, mỗi giao tiếp kết nối đến một mạng con/VLAN khác, router sử dụng một giao tiếp vật lý của router, với ba giao tiếp con luân lý, mỗi cái kết nối đến một mạng con/ VLAN khác. Lệnh **encapsulation** đánh số các VLANs, phải trùng với cấu hình cho VLAN ID trên switch đó.

Ví dụ này sử dụng số giao tiếp con trùng với VLAN ID trên mỗi giao tiếp con. Không có yêu cầu nào về các số trùng này, nhưng hầu hết

mọi người lựa chọn chúng trùng đê thực hiện cấu hình rõ ràng hơn và xử lý sự cố dễ dàng hơn. Nói cách khác, VLAN ID có thể là 1, 2, và 3, nhưng chỉ số giao tiếp con có thể là 4, 5, và 6, vì số giao tiếp con chỉ được sử dụng bên trong một router.

Ví dụ 7.4 cho thấy cùng một mạng, nhưng lúc này 802.1Q được sử dụng thay vì ISL. IEEE 802.1Q có khái niệm được gọi tên là native VLAN, là một VLAN đặc biệt trên mỗi trung kế mà trong đó trường tiêu đề 802.1Q không cần thêm vào các frame này. Mặc định, VLAN 1 là native VLAN. Ví dụ 7.4 cho thấy sự khác biệt trong cấu hình này.

```
interface FastEthernet 0/0
 ip address 10.1.1.1 255.255.255.0
!
interface FastEthernet 0/0.2
 ip address 10.1.2.1 255.255.255.0
 encapsulation dot1q 2
!
interface FastEthernet 0/0.3
 ip address 10.1.3.1 255.255.255.0
 encapsulation dot1q 3
```

Cấu hình trên tạo ba VLAN trên giao tiếp Fa0/0. Hai trong số VLAN này, VLAN 2 và 3, được cấu hình giống như ví dụ 7.3, ngoại trừ lệnh **encapsulation** liệt kê 802.1Q là loại đóng gói.

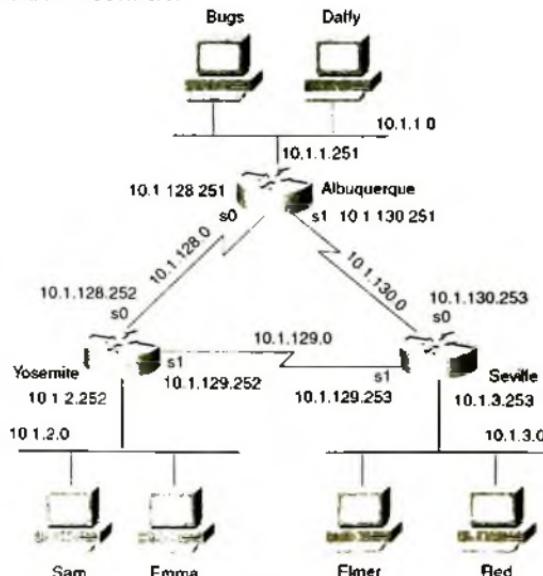
Native VLAN, VLAN 1 trong trường hợp này, có thể được cấu hình với hai kiểu cấu hình. Ví dụ 7.4 cho thấy một kiểu trong đó chỉ IP native VLAN được cấu hình trên giao tiếp vật lý. Kết quả là, router không sử dụng tiêu đề trung kế VLAN trong VLAN này, như được sử dụng cho native VLAN. Cách khác để cấu hình địa chỉ IP native VLAN trên giao tiếp con khác là sử dụng lệnh giao tiếp con **encapsulation dot1q native** với VLAN 1, nhưng từ khóa **native** báo cho router biết không sử dụng bất kỳ tiêu đề 802.1Q nào với giao tiếp con đó.

Router không thực hiện thỏa thuận trung kế động. Vì thế, các switch có kết nối đến một giao tiếp của router phải cấu hình trung kế một cách thủ công, như đã xem xét trong chương 1. Ví dụ, một switch trên đầu cuối giao tiếp Fa0/0 có thể cấu hình lệnh giao tiếp con **switchport mode trunk** (để kích hoạt trung kế thủ công), và nếu switch có khả năng sử dụng cả hai loại trung kế, lệnh con giao tiếp **switchport trunk encapsulation dot1q** để cấu hình tĩnh sử dụng 802.1Q.

7.3.2. Các con đường tĩnh

Router sử dụng ba phương pháp chính để thêm các con đường vào bảng định tuyến của nó: các con đường có kết nối, các con đường tĩnh và các giao thức định tuyến tĩnh. Router luôn thêm một con đường có kết nối khi các giao tiếp có địa chỉ IP được cấu hình và các giao tiếp đang bật và hoạt động. Trong hầu hết các mạng, sử dụng các giao thức định tuyến động có mục đích để làm cho mỗi router học về phần còn lại của các con đường trong một liên mạng. Sử dụng các con đường tĩnh – các con đường được thêm vào một bảng định tuyến thông qua cấu hình trực tiếp là được sử dụng ít nhất trong ba lựa chọn này.

Định tuyến tĩnh thực ra là các câu lệnh cấu hình toàn cục **ip route** độc lập xác định một con đường đến một router. Lệnh cấu hình này bao gồm tham chiếu đến một mạng con – chỉ số mạng con và mặt nạ mạng, cùng với các chỉ dẫn về nơi để chuyển gói tin đến mạng con đó. Để thấy được sự cần thiết cho con đường tĩnh này, và thấy được cấu hình của nó, xem xét ví dụ 7.5, thể hiện hai lệnh ping kiểm tra kết nối IP từ Albuquerque đến Yosemite.



Hình 7.7. Cấu hình định tuyến tĩnh

```

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

Gateway of last resort is not set

  10.0.0.0/24 is subnetted, 3 subnets
      C      10.1.1.0 is directly connected, Ethernet0
      C      10.1.130.0 is directly connected, Serial1
      C      10.1.128.0 is directly connected, Serial0

Albuquerque#ping 10.1.128.252
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.128.252, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms

Albuquerque#ping 10.1.2.252
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.252, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

```

Phần cuối ví dụ này thể hiện hai lệnh **ping** trên router Albuquerque, một đến 10.1.128.252 (địa chỉ IP của Yosemite) và một đến 10.1.2.252 (địa chỉ IP LAN của Yosemite). Lệnh **ping** của IOS gửi 5 gói tin ICMP Echo Request theo mặc định, với đầu ra của lệnh liệt kê một dấu chấm than (!) nghĩa là một Echo Reply được nhận và một dấu(.) nghĩa là không có phản hồi được nhận. Trong ví dụ này, lệnh **ping 10.1.128.252**, thể hiện 5 đáp ứng (100%) và lệnh thứ hai, **ping 10.1.2.252**, thể hiện không có đáp ứng nào được nhận (0%). Lệnh **ping** đầu tiên hoạt động vì Albuquerque có một con đường đến mạng con trong đó 10.1.128.2 được đặt (mạng con 10.1.128.0/24). Tuy nhiên, lệnh **ping** đến 10.1.2.252 không làm việc vì Albuquerque không có con đường nào phù hợp cho địa chỉ 10.1.2.252. Lúc này, Albuquerque chỉ có các con đường cho ba mạng con có kết nối của nó. Vì thế, lệnh **ping 10.1.2.252** tạo các gói tin, nhưng Albuquerque hủy gói tin này vì không có con đường nào tồn tại.

Một giải pháp đơn giản cho lỗi của lệnh **ping 10.1.2.252** là cho phép một giao thức định tuyến trên tất cả ba router. Thực ra, trong một mạng thực

tế, đây là giải pháp thông dụng nhất. Cách khác, có thể cấu hình các con đường tĩnh. Nhiều mạng có một vài con đường tĩnh, vì thế hiếm khi cần cấu hình chúng. Ví dụ 7.6 cho thấy lệnh **ip route** trên Albuquerque, thêm các con đường tĩnh và làm cho lệnh ping lỗi trong ví dụ 7.5 hoạt động.

```
ip route 10.1.2.0 255.255.255.0 10.1.128.252
ip route 10.1.3.0 255.255.255.0 10.1.130.253
```

Lệnh **ip route** xác định một con đường tĩnh bằng cách xác định chỉ số mạng con và địa chỉ IP chặng kế tiếp. Một lệnh **ip route** xác định một con đường đến 10.1.2.0 (mặt nạ 255.255.255.0), được đặt ngoài Yosemite, vì thế địa chỉ IP chặng kế được cấu hình trên Albuquerque là 10.1.128.252, là địa chỉ IP Serial0 của Yosemite. Tương tự, một con đường đến 10.1.3.0, mạng con ngoài Seville, trả đến địa chỉ IP của giao tiếp Serial0 trên Seville, 10.1.130.253. Chú ý rằng địa chỉ IP kế tiếp là một địa chỉ IP trong mạng con có kết nối trực tiếp, mục đích là để xác định router kế tiếp để gửi gói tin đến. Bây giờ Albuquerque có thể chuyển tiếp các gói tin đến các mạng con này.

Lệnh **ip route** có hai định dạng cơ bản. Lệnh có thể ám chỉ đến địa chỉ IP chặng kế, như thể hiện trong ví dụ 7.6. Cách khác, với các con đường tĩnh sử dụng liên kết serial điểm-điểm, lệnh có thể liệt kê giao tiếp ra thay vì địa chỉ IP chặng kế tiếp. Ví dụ 4.6 có thể sử dụng lệnh **ip route 10.1.2.0 255.255.255.0 serial** thay vì lệnh cấu hình **ip route**.

Không may là, việc thêm hai con đường tĩnh trong ví dụ 7.6 cho Albuquerque không giải quyết tất cả các vấn đề định tuyến mạng. Các con đường tĩnh giúp Albuquerque chuyển các gói tin đến hai mạng con, nhưng hai con đường khác đó không có đủ thông tin định tuyến để chuyển các gói tin đến Albuquerque. Ví dụ, PC Bugs không thể ping cho PC Sam trong mạng này, dù đã thêm các lệnh trong ví dụ 7.6. Vấn đề là dù Albuquerque đã có một con đường đến mạng con 10.1.2.0, nơi có SAM, Yosemite không có một con đường đến 10.1.1.0, nơi có Bugs. Các gói tin yêu cầu ping đi từ Bugs đến Sam một cách chính xác nhưng gói tin phản hồi của Sam không thể được định tuyến bởi Yosemite quay lại qua Albuquerque đến Bugs, vì thế lệnh ping có lỗi.

7.3.3. Lệnh ping mở rộng

Trong thực tế, có thể không thể tìm thấy người dùng, như là Bugs, để nhờ anh kiểm tra mạng bằng cách ping. Thay vào đó, có thể sử dụng

lệnh ping trên một router để kiểm tra định tuyến theo cùng cách mà một ping từ Bugs đến Sam để kiểm tra định tuyến. Ví dụ 7.7 cho thấy một ví dụ về Albuquerque với lệnh ping 10.1.2.252 hoạt động, nhưng với một lệnh ping 10.1.2.252 mở rộng, hoạt động tương tự như là một ping từ Bugs đến Sam, một lệnh ping có lỗi trong trường hợp này (chỉ có hai con đường tĩnh được thêm vào tại thời điểm này).

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

Gateway of last resort is not set

      10.0.0.0/24 is subnetted, 5 subnets
S        10.1.3.0 [1/0] via 10.1.128.253
S        10.1.2.0 [1/0] via 10.1.128.252
C        10.1.1.0 is directly connected, Ethernet0
C        10.1.128.0 is directly connected, Serial1
C        10.1.128.0 is directly connected, Serial0
Albuquerque ping 10.1.2.252

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.252, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms

Albuquerque ping
Protocol [ip]:
Target IP address: 10.1.2.252
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.251
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [0]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.252, timeout is 2 seconds:
* * * *
Success rate is 0 percent (0/5)
```

Lệnh **ping** 10.1.2.252 đơn giản hoạt động vì một nguyên nhân rõ ràng và không rõ ràng. Trước tiên, Albuquerque có thể chuyên tiếp một gói tin đến mạng con 10.1.2.0 vì đó là một con đường tĩnh. Gói tin trả về, được gửi bởi Yosemite, được gửi đến địa chỉ 10.1.1.128.251 – địa chỉ IP Serial0 của Albuquerque – và Yosemite có một con đường kết nối để đến mạng con 10.2.128.0. Nhưng tại sao Yosemite gửi một phản hồi Echo Reply đến địa chỉ IP S0 của Albuquerque là 10.1.128.251? Các điểm sau đây là đúng về lệnh **ping** trên một router Cisco.

Lệnh **ping** theo mặc định sử dụng địa chỉ IP giao tiếp đầu ra như là địa chỉ nguồn của gói tin, trừ khi nó được xác định trong một địa chỉ ping mở rộng. Lệnh ping đầu tiên trong ví dụ 4.7 sử dụng địa chỉ nguồn là 10.1.128.251, vì con đường được sử dụng để gửi gói tin đến 10.1.2.252 gửi các gói tin này ra ngoài giao tiếp Serial 0 của Albuquerque, có địa chỉ IP 10.1.128.251.

Các gói tin phản hồi ping (ICMP Echo Replies) đảo ngược địa chỉ IP được sử dụng trong yêu cầu ping nhận được với các địa chỉ chúng phản hồi. Vì thế trong ví dụ này, Echo Reply của Yosemite, phản hồi với lệnh ping đầu tiên trong ví dụ 7.7, sử dụng 10.1.128.251 như là địa chỉ đích và 10.1.2.252 như là địa chỉ IP nguồn

Vì lệnh **ping** 10.1.2.252 trên Albuquerque sử dụng 10.1.128.251 là địa chỉ nguồn của gói tin, Yosemite có thể gửi ngược một phản hồi đến 10.1.128.251, vì Yosemite có một con đường có kết nối đến 10.1.128.0

Vẫn đề nguy hiểm khi xử lý với lệnh **ping** chuẩn là các vấn đề định tuyến có thể tồn tại, nhưng lệnh **ping** 10.1.2.252, lại làm việc, cho cảm giác sai lầm về bảo mật. Một cách khác đơn giản hơn là sử dụng lệnh **ping** mở rộng để hoạt động giống như sử dụng một ping từ một máy tính trên mạng con đó, mà không phải nhờ người này đánh vào lệnh ping giúp từ máy tính của họ. Phiên bản mở rộng của lệnh **ping** có thể được dùng

đề cài tiến vẫn đề bên dưới gây ra khi thay đổi nhiều chi tiết khi lệnh ping gửi trong yêu cầu của nó. Thực ra, khi một ping từ một router hoạt động, như một ping từ một máy tính không hoạt động, lệnh ping mở rộng có thể giúp kiểm lại vấn đề mà không cần phải làm việc với người dùng cuối qua điện thoại.

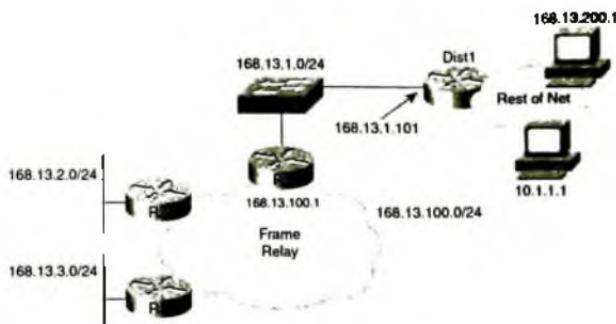
Ví dụ, trong ví dụ 7.7, lệnh ping mở rộng trên Albuquerque gửi một gói tin từ địa chỉ IP nguồn 10.1.1.251 (địa chỉ Ethernet của Albuquerque) đến 10.1.2.252 (Ethernet của Yosemite). Theo đầu ra này, Albuquerque không nhận được một phản hồi. Thông thường, lệnh ping có thể xác định từ địa chỉ IP của giao tiếp ra. Với việc sử dụng địa chỉ nguồn lệnh ping mở rộng, địa chỉ IP nguồn của gói echo được thiết lập thành địa chỉ IP Ethernet của Albuquerque, 10.1.1.251. Vì phản hồi ICMP echo được tạo ra bởi lệnh ping mở rộng từ một địa chỉ trong mạng con 10.1.1.0, gói tin trong khá giống một gói tin từ người dùng cuối trên mạng đó.

Yosemite tạo một Echo Reply, với đích 10.1.1.251, nhưng nó không có con đường đến mạng con đó. Vì thế Yosemite không thể gửi gói tin phản hồi ping đến Albuquerque.

Để giải quyết vấn đề này, tất cả router có thể được cấu hình để sử dụng một giao thức định tuyến. Cách khác, có thể đơn giản xác định các con đường tĩnh trên tất cả các router trên mạng.

7.3.4. Các con đường tĩnh mặc định

Một con đường mặc định là một con đường đặc biệt phù hợp với tất cả các gói tin đích. Các con đường mặc định có thể hữu ích khi chỉ một con đường vật lý tồn tại từ một phần của mạng đến các phần khác của nó, và trong các trường hợp trong đó một router của doanh nghiệp cung cấp kết nối Internet cho doanh nghiệp đó. Ví dụ, trong hình 7.8, R1, R2 và R3 có thể chuyển tiếp các gói tin đến phần còn lại của mạng cũng như các gói tin đến R1, đến lượt nó chuyển tiếp các gói tin đến router Dist1.



Hình 7.8. Con đường tĩnh mặc định

Các phần tiếp theo cho thấy hai lựa chọn cho việc cấu hình các con đường tĩnh mặc định: một sử dụng lệnh `ip route` và một sử dụng lệnh `ip default-network`

7.3.4.1. Các con đường mặc định sử dụng lệnh `ip route`

Bằng cách cấu hình một con đường mặc định trên R1, với router chặng kế là Dist1, và bằng cách cho R1 quảng bá con đường mặc định đến R2 và R3, việc định tuyến mặc định có thể được hoàn tất. Bằng cách sử dụng một con đường mặc định như thế, R1, R2 và R3 có thể không cần các con đường cụ thể đến các mạng con bên phải của router Dist1. Ví dụ 7.8 cho bắt đầu với việc kiểm tra thiết kế bằng cách thể hiện định nghĩa một con đường tĩnh mặc định và dẫn đến thông tin trên bảng định tuyến R1.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 168.13.1.101
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is 168.13.1.101 to network 0.0.0.0

      168.13.0.0/24 is subnetted, 4 subnets
C        168.13.1.0 is directly connected, FastEthernet0/0
R        168.13.3.0 [126/1] via 168.13.100.3, 00:00:05, Serial0.1
R        168.13.2.0 [126/1] via 168.13.100.2, 00:00:21, Serial0.1
C        168.13.100.0 is directly connected, Serial0.1
S*  0.0.0.0/0 [1/0] via 168.13.1.101
```

R1 xác định một con đường tĩnh với lệnh **ip route**, với đích là 0.0.0.0, mặt nạ mạng 0.0.0.0. Kết quả là, lệnh **show ip route** của R1 liệt kê một con đường tĩnh đến 0.0.0.0, mặt nạ là 0.0.0.0 với chặng kế tiếp là 168.13.1.101 – một cách cần thiết, với cùng thông tin trên lệnh cấu hình **ip route 0.0.0.0 0.0.0.0 168.13.1.101**. Dịch của nó là 0.0.0.0, với mặt nạ 0.0.0.0, đại diện cho tất cả các đích theo quy ước. Với cấu hình trên, R1 có một con đường tĩnh trùng với bất kì và tất cả các gói tin IP đích nào.

Chú ý trong ví dụ 7.8 rằng lệnh **show ip route** của R1 liệt kê một “Gateway of last resort” là 168.13.1.101. Khi một router biết ít nhất một con đường mặc định, router ghi nhận con đường đó với một dấu chấm than trên bảng định tuyến. Nếu một router biết nhiều con đường mặc định – hoặc là thông qua cấu hình tĩnh hay từ các giao thức định tuyến – router ghi nhận mỗi con đường mặc định như là một dấu ! trên bảng định tuyến. Sau đó, router lựa chọn con đường mặc định tốt nhất, chú ý rằng lựa chọn như là “gateway or last resort” (khoảng cách quản trị của thông tin định tuyến nguồn, được xác định bởi thiết lập khoảng cách quản trị, có ảnh hưởng đến việc lựa chọn này. Khoảng cách quản trị được xem xét trong chương 9 “Giao thức định tuyến” trong phần “Khoảng cách quản trị”).

Khi cấu hình RIP không được thể hiện, R1 cũng quảng bá con đường mặc định này đến R2 và R3, như thể hiện trong đầu ra của lệnh **show ip route** trên R3 trong ví dụ 7.9.

```
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is 168.13.100.1 to network 0.0.0.0

  168.13.0.0/24 is subnetted, 4 subnets
R    168.13.1.0 [120/1] via 168.13.100.1, 00:00:13, Serial0.1
C    168.13.3.0 is directly connected, Ethernet0
R    168.13.2.0 [120/1] via 168.13.100.2, 00:00:06, Serial0.1
C    168.13.100.0 is directly connected, Serial0.1
```

Các giao thức định tuyến khác nhau quảng bá các con đường mặc định với nhiều cách khác nhau. Ví dụ, khi R3 học một con đường mặc định từ R1 sử dụng RIP, R3 liệt kê đích của con đường mặc định này (0.0.0.0) và router chặng kế, là R1 trong trường hợp này (168.12.100.1), được làm nổi bật trong ví dụ 4.9. Vì thế khi R3 cần sử dụng con đường mặc định của nó, nó chuyển tiếp các gói tin đến R1 (168.13.100.1).

7.3.4.2. Các con đường mặc định sử dụng lệnh ip default – network

Một cách khác để cấu hình con đường mặc định là sử dụng lệnh **ip default – network**. Lệnh này liệt kê địa chỉ IP mạng classful là đối số, báo cho router biết để sử dụng chi tiết định tuyến của con đường cho mạng classful đó như là chi tiết chuyển tiếp cho một con đường mặc định.

Lệnh này hữu dụng nhất khi muốn sử dụng một con đường mặc định để đến mạng bên ngoài mạng được sử dụng trong doanh nghiệp đó. Ví dụ, trong hình 7.8, tường tượng rằng tất cả các mạng con của mạng doanh nghiệp lớp B 168.13.0.0 được biết trước; chúng tồn tại chỉ gần các router R1, R2 và R3; và những con đường này tất cả đều có trong bảng định tuyến của R1, R2 và R3. Cũng vậy không có mạng con nào của 168.1.0.0 bên phải của router Dist1. Nếu muốn sử dụng một con đường mặc định để chuyển tiếp các gói tin đến đích của bên phải của Dist1, lệnh **ip default – network** làm việc tốt.

Để sử dụng lệnh **ip default – network** để cấu hình một con đường mặc định, dựa trên hiểu biết của nó rằng Dist1 đã quảng bá một con đường cho mạng classful 10.0.0.0 đến R1. Con đường của R1 đến mạng 10.0.0.0 chỉ đến địa chỉ 168.13.1.0 của Dist1 như là địa chỉ kế tiếp. Biết rằng, có thể cấu hình lệnh **ip default – network 10.0.0.0** trên R1, điều này báo R1 để xây dựng con đường mặc định của nó dựa trên các con đường đã học được cho mạng 10.0.0.0/8. Ví dụ 7.10 thể hiện nhiều chi tiết về trường hợp này trên R1.

```

R1#configure terminal
R1(config)#ip default-network 10.0.0.0
R1(config)#exit
R1#show ip route
Codes: C - connected, S - static, I - IGMP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is 168.13.1.101 to network 10.0.0.0

  168.13.0.0/24 is subnetted, 5 subnets
R    168.13.200.0 [120/1] via 168.13.1.101, 00:00:12, FastEthernet0/0
C    168.13.1.0 is directly connected, FastEthernet0/0
R    168.13.3.0 [120/1] via 168.13.100.3, 00:00:00, Serial0.1
R    168.13.2.0 [120/1] via 168.13.100.2, 00:00:00, Serial0.1
C    168.13.100.0 is directly connected, Serial0.1
R*  10.0.0.0/8 [120/1] via 168.13.1.101, 00:00:12, FastEthernet0/0

```

R1 thể hiện kết quả học được từ con đường đến mạng 10.0.0.0 thông qua RIP, cộng với kết quả bổ sung của lệnh cấu hình ip default – network 10.0.0.0. Con đường RIP của R1 cho 10.0.0.0 liệt kê địa chỉ IP chặng kế tiếp là 168.13.1.101, địa chỉ IP của Dist1 trên LAN chung của nó. Vì lệnh ip default – network, R1 quyết định sử dụng các chi tiết trong con đường đến 10.0.0.0 như là con đường mặc định của nó. Phần cuối cùng dòng là về gateway of last resort liệt kê mạng mặc định đó, 10.0.0.0. Tương tự, R1 liệt kê một dấu chấm than bên ngoài con đường được tham chiếu đến trong lệnh ip default – network.

7.3.4.3. Tóm tắt về con đường mặc định

Ghi nhớ các chi tiết cấu hình các con đường mặc định và cụ thể là kết quả chi tiết đầu ra của lệnh show ip route có thể là khó khăn. Tuy nhiên, tạo điểm để nhớ về các điểm cốt yếu theo các con đường mặc định:

- Các con đường tĩnh mặc định có thể được cấu hình tĩnh sử dụng lệnh ip route **0.0.0.0 0.0.0.0 địa chỉ chặng kế tiếp hoặc ip default – network net – number**

- Khi một router chỉ so khớp một gói tin với con đường mặc định đó, router sử dụng chi tiết về chuyền tiếp được liệt kê trên dòng gateway of last resort.
- Tùy theo cách con đường mặc định được thể hiện – liệu nó là gateway of last resort, một con đường đến 0.0.0.0, một con đường đến một số mạng khác với dấu * bên cạnh nó trong bảng định tuyến – nó được sử dụng dựa theo quy tắc định tuyến phân lớp hay không phân lớp – như được giải thích trong phần tiếp theo.

7.4. CÂU HỎI VÀ BÀI TẬP CHƯƠNG 7

Câu 1. Một người dùng bật máy tính, sau đó sử dụng trình duyệt để truy cập vào trang web <http://www.ciscopress.com>. Giao thức nào sẽ không được sử dụng bởi PC trong tiến trình này.

- DHCP
- DNS
- ARP
- ICMP

Câu 2. Một người dùng bật máy tính, sau đó thực hiện một lệnh ping 2.2.2.2, và lệnh ping cho thấy kết quả thành công 100%. Địa chỉ IP của máy tính là 1.1.1.1/24. Thiết lập nào sau đây được yêu cầu trên máy tính để hỗ trợ lệnh ping thành công?

- Địa chỉ IP của DNS server
- Địa chỉ IP của default gateway
- Địa chỉ IP của ARP server
- Địa chỉ IP của DHCP server

Câu 3. Router 1 có một giao tiếp Fa0/0 với địa chỉ IP là 10.1.1.1. Giao tiếp được kết nối đến một switch. Kết nối này sau đó được tích hợp để sử dụng trung kế 802.1Q. Lệnh nào sau đây có thể là cấu hình hợp lệ cho giao tiếp Fa0/0 của Router 1?

- interface fastatethernet 0/0.4

- b. dot1q enable
- c. dot1q enable 4
- d. trung kế enable
- e. trung kế enable 4
- f. encapsulation dot1q

Câu 4. Một router được cấu hình với lệnh toàn cục no ip subnet-zero. Lệnh con giao tiếp nào sau đây có thể chấp nhận được với router này.

- a. ip address 10.1.1.1 255.255.255.0
- b. ip address 10.0.0.129 255.255.255.128
- c. ip address 10.1.2.2 255.254.0.0
- d. ip address 10.0.0.5 255.255.255.252

Câu 5. Điều nào sau đây phải đúng trước khi IOS liệt kê một con đường “S” trong đầu ra lệnh “show ip route”

- a. Địa chỉ IP phải được cấu hình trên một giao tiếp
- b. Router phải nhận một cập nhật định tuyến từ các router lân cận
- c. Lệnh ip route phải được thêm vào cấu hình
- d. Lệnh ip address phải sử dụng từ khóa special
- e. Giao tiếp phải ở trạng thái up và up

Câu 6. Lệnh nào sau đây cấu hình đúng về một con đường kết nối tĩnh?

- a. ip route 10.1.3.0 255.255.255.0 10.1.130.253
- b. ip route 10.1.3.0 serial 0
- c. ip route 10.1.3.0/24 10.1.130.253
- d. ip route 10.1.3.0/24 serial 0

Câu 7. Điều nào sau đây bị ảnh hưởng bởi liệu một router được thực hiện định tuyến phân mạng hay không phân mạng?

- a. Khi sử dụng một con đường mặc định
- b. Khi sử dụng mặt nạ trong cập nhật định tuyến

- c. Khi chuyển một địa chỉ IP gói tin đích đến một địa chỉ mạng
- d. Khi thực hiện hàng đợi dựa trên phân loại gói tin vào một hàng đợi cụ thể.

Câu 8. Một router đã được cấu hình với lệnh toàn cục ip address . Router nhận được một gói tin đến địa chỉ IP 168.13.4.1. Đoạn văn sau đây liệt kê nội dung bảng định tuyến của router. Điều nào sau đây là đúng về cách router này chuyển tiếp gói tin?

Gateway of last resort is 168.13.1.101 to network 0.0.0.0

168.13.0.0/24 is subnetted, 2 subnets

C 168.13.1.0 is directly connected, Fastatethernet0/0

R 168.13.3.0 [120/1] via 168.13.100.3, 00:00:05, Serial0.1

- a. Nó được chuyển tiếp đến 168.13.100.3
- b. Nó được chuyển tiếp đến 168.13.1.101
- c. Nó được chuyển ra ngoài giao tiếp Fa0/0, hướng đến máy tính đích
- d. Router hủy bỏ gói tin

Chương 8

CHÍNH SÁCH KIỂM SOÁT TRUY CẬP

Bảo mật mạng là một trong những chủ đề nóng bỏng ngày nay. Dù bảo mật luôn là quan trọng, việc bùng nổ kích thước và phạm vi của Internet đã tạo ra nhiều hơn các lỗ hổng bảo mật. Trong những năm gần đây, hầu hết các công ty đều có kết nối đến mạng toàn cầu – một mạng qua đó người khác có thể thử truy cập trái phép vào mạng của bất kỳ cá nhân hay tổ chức nào.

Các router của Cisco có thể được sử dụng như là một phần của chiến lược bảo mật tổng thể. Một trong những công cụ quan trọng trong phần mềm Cisco IOS được sử dụng như là một phần của chiến lược đó là ACL (Access List – chính sách kiểm soát truy cập). ACL xác định các quy tắc có thể được sử dụng để ngăn một số gói tin qua mạng. IOS ACL có thể là công cụ bảo mật quan trọng như là một phần của chiến lược bảo mật lớn hơn.

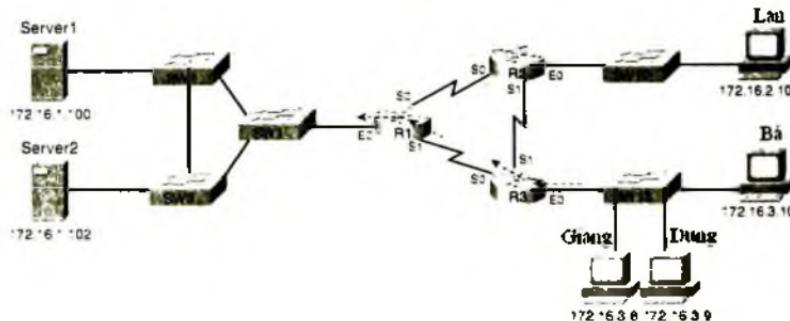
8.1. CHÍNH SÁCH KIỂM SOÁT TRUY CẬP IP CHUẨN

IP ACL làm cho một router hủy bỏ một số gói tin dựa trên các tiêu chuẩn được xác định bởi người quản trị mạng. Mục đích của việc lọc này là ngăn các lưu lượng không mong muốn trên mạng – ngăn ngừa hacker xâm nhập mạng hay chỉ ngăn ngừa người dùng khỏi việc truy cập các hệ thống mà họ không được phép. Chính sách truy cập đơn giản là một phần của chính sách bảo mật cho một tổ chức.

Theo cách đó, chính sách truy cập IP có thể được sử dụng để lọc các cập nhật định tuyến, để so khớp các gói tin với các tiêu chuẩn, VPN tunneling và so khớp các gói tin với việc truyền khai các chức năng chất lượng dịch vụ. Chương này xem xét hai chủ đề chính của IOS IP ACL – chuẩn và mở rộng. ACL chuẩn sử dụng ý nghĩa đơn giản hơn, và ACL mở rộng sử dụng ý nghĩa phức tạp hơn. Phần đầu tiên của chương xem xét IP ACL chuẩn, sau đó là IP ACL mở rộng.

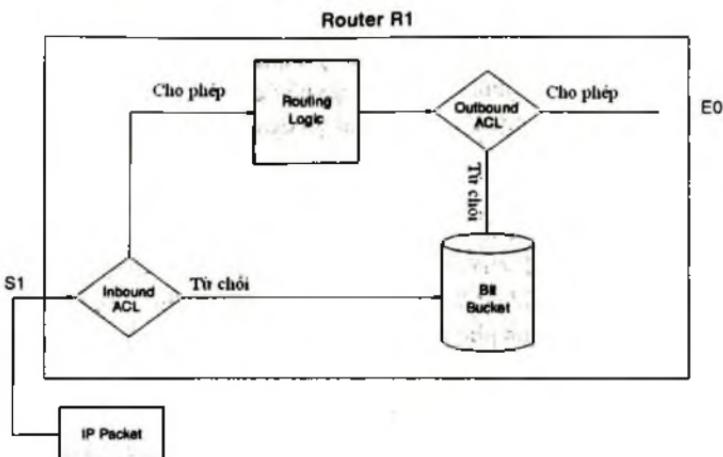
8.1.1. Các khái niệm IP ACL Chuẩn

Cần thực hiện hai lựa chọn chính cho bất kì ACL sẽ lọc các gói tin IP: gói tin nào sẽ lọc, và nơi nào trong mạng được đặt vào ACL. Hình 8.1 xem xét một ví dụ. Trong trường hợp này, tưởng tượng rằng Bá không được phép truy cập vào Server 1, nhưng LAN thì được.



Hình 8.1. Ví dụ về chính sách truy cập chuẩn

Thao tác lọc gói tin như yêu cầu có thể được cấu hình trên bất kì ba router nào và trên bất kì giao tiếp nào của nó. Đường mũi tên nét đứt trong hình cho thấy các điểm tương thích nhất được áp dụng trong một ACL. Vì lưu lượng của Bá cần được lọc, và mục đích là ngăn truy cập Server 1, chính sách truy cập có thể được áp dụng trên hoặc là R1 hay R3. Vì lưu lượng của Bá đến Server không cần qua R2, R2 không phải là một nơi tốt để đặt ACL. Giả sử trong trường hợp này, sử dụng ACL tại R1.



Hình 8.2. Cấu hình chính sách truy cập chuẩn

Việc lọc có thể được áp dụng cho các gói tin vào giao tiếp S1 hay các gói tin ra khỏi giao tiếp E0 trên R1 để so khớp với gói tin được gửi bởi Bá đến Server 1. Thông thường, có thể lọc các gói tin bằng cách tạo và kích hoạt chính sách truy cập cho cả hai gói tin đến và đi trên mỗi giao tiếp. Sau đây là một số đặc tính chính của chính sách truy cập Cisco:

- Các gói tin có thể được lọc khi chúng vào một giao tiếp trước khi thực hiện định tuyến
- Gói tin có thể được lọc trước khi chúng ra khỏi một giao tiếp, sau khi thực hiện quyết định định tuyến.
- Từ chối là thuật ngữ được sử dụng bởi phần mềm Cisco IOS để xác định rằng gói tin đó bị lọc.
- Cho phép là thuật ngữ được sử dụng bởi phần mềm Cisco IOS để xác định rằng gói tin đó không bị lọc.
- Ý nghĩa của lọc gói được cấu hình trong chính sách truy cập.
- Tại cuối của mỗi chính sách truy cập là một lệnh được xác định “deny all traffic”. Chính vì thế, nếu một gói tin không trùng bất kì lệnh chính sách truy cập nào, nó bị khóa.

Ví dụ, có thể tạo một chính sách truy cập trong R1 và kích hoạt nó trên giao tiếp S1 của R1. Chính sách truy cập sẽ tìm kiếm các gói tin đến từ Bá. Chính vì thế, chính sách truy cập nên được kích hoạt trên gói tin đầu vào, bởi vì trong mạng này, các gói tin đến từ Bá vào giao tiếp S2, và ngược lại.

Chính sách truy cập có hai bước chính: so khớp và hành động. So khớp kiểm tra mỗi gói tin và đánh giá liệu nó trùng với lệnh “access-list”. Ví dụ địa chỉ IP của Bá có thể được dùng để so khớp các gói tin được gửi đến từ Bá. IP ACL báo cho router biết thực hiện một trong hai hành động khi một lệnh phù hợp: từ chối hay cho phép. Từ chối có nghĩa là hủy bỏ gói tin và cho phép xác định gói tin có thể tiếp tục trên con đường của nó.

Vì thế chính sách truy cập để ngăn gói tin của Bá đến server có thể được thực hiện như sau:

Tìm kiếm gói tin với địa chỉ IP nguồn là của Bá và địa chỉ IP đích là của server 1. Khi tìm thấy, hủy bỏ nó, nếu không thấy, thì không hủy bỏ.

Tuy nhiên, IP ACL có thể có nhiều khó khăn hơn trong thực tế. Thậm chí một danh sách các tiêu chuẩn phù hợp ngăn có thể tạo các chính sách truy cập phức tạp trên nhiều giao tiếp của nhiều router. Cisco xem các chức năng lọc gói là chính sách kiểm soát truy cập vì mục đích là tạo nhiều lệnh cấu hình được xem xét như là cùng một danh sách. Khi một chính sách truy cập có nhiều mục, IOS tìm kiếm danh sách tuần tự cho đến khi lệnh đầu tiên phù hợp. Lệnh đã phù hợp xác định hành động được thực hiện. Mục đích IOS sử dụng với ACL nhiều mục có thể được tóm lược như sau:

1. Các tham số phù hợp của lệnh access-list được so sánh với gói tin
2. Nếu trùng khớp, hành động được xác định trong lệnh access-list (từ chối hay cho phép) được thực hiện
3. Nếu không trùng khớp, lặp lại bước 1 và 2 cho đến khi có trùng khớp
4. Nếu không có trùng khớp, hành động từ chối được thực hiện

8.1.1.1. Mặt nạ ngược

IP ACL của IOS so khớp các gói tin bằng cách tìm kiếm IP, tiêu đề TCP và UDP của gói tin. Chính sách truy cập mở rộng kiểm tra các địa chỉ IP nguồn và đích, cũng như chỉ số port nguồn và đích, cùng với nhiều trường khác. Tuy nhiên, chính sách truy cập IP chuẩn có thể đánh giá chỉ địa chỉ IP nguồn.

Không tùy thuộc vào liệu sử dụng IP ACL chuẩn hay mở rộng, người quản trị có thể báo router biết để so khớp dựa trên toàn bộ địa chỉ IP hay chỉ một phần của địa chỉ IP đó. Ví dụ nếu muốn chặn Bá gửi gói tin đến Server 1, tìm kiếm toàn bộ địa chỉ IP của Bá và Server 1 trong danh sách. Nhưng điều gì xảy ra nếu điều kiện là ngăn tất cả các máy tính trong mạng con của Bá truy cập đến Server 1? Vì tất cả các máy trong mạng con của Bá có cùng chỉ số trong ba octet đầu tiên, chính sách truy cập có thể chỉ kiểm tra 3 octet đầu tiên của địa chỉ để so khớp tất cả gói tin với một lệnh access – list đơn.

Mặt nạ ngược của Cisco xác định phần địa chỉ IP được kiểm tra. Khi xác định một lệnh ACL, như thấy trong phần trước, người quản trị có thể xác định một mặt nạ ngược cùng với địa chỉ IP. Mặt nạ ngược báo cho router biết phần nào của địa chỉ IP trong lệnh cấu hình phải được so sánh với tiêu đề gói tin.

Ví dụ, giả sử một mặt nạ nhấn mạnh rằng toàn bộ gói tin cần được kiểm tra và mặt nạ khác xác định chỉ 3 octet đầu tiên của các địa chỉ cần được kiểm tra. Để thực hiện so khớp, chính sách truy cập Cisco sử dụng các mặt nạ ngược.

Mặt nạ ngược giống như mặt nạ mạng con, nhưng không hoàn toàn như thế. Mặt nạ ngược đại diện cho một số 32 bit, như là mặt nạ mạng. Tuy nhiên, các bit 0 của mặt nạ ngược báo cho router biết các bit tương ứng trong địa chỉ phải được so sánh khi thực hiện công việc so khớp. Bit 1 trong mặt nạ ngược báo cho router biết những bit này không cần so khớp.

Bảng 8.1. Một số mặt nạ ngược

Mặt nạ ngược	Mặt nạ ngược nhị phân	Mô tả
0.0.0.0	00000000.00000000.00000000.00000000	Toàn bộ địa chỉ IP trùng
0.0.0.255	00000000.00000000.00000000.11111111	Chỉ 24 bit đầu trùng
0.0.255.255	00000000.00000000.11111111.11111111	Chỉ 16 bit đầu trùng
0.255.255.255	00000000.11111111.11111111.11111111	Chỉ 7 bit đầu trùng

Bảng 8.2. Một số mặt nạ ngược (tt)

Mặt nạ ngược	Mặt nạ ngược nhị phân	Mô tả
255.255.255.255	11111111.11111111.11111111.11111111	Xem như là tự động trùng với tất cả và bất kì địa chỉ nào
0.0.15.255	00000000.00000000.00001111.11111111	20 bit đầu tiên trùng
0.0.3.255	00000000.00000000.00000011.11111111	22 bit đầu tiên trùng

8.1.1.2. Tính toán mặt nạ ngược

Cả ACL IP chuẩn (chỉ có địa chỉ IP nguồn) và ACL mở rộng (cả địa chỉ nguồn và đích) có thể được cấu hình để kiểm tra tất cả hay một phần của một địa chỉ IP dựa trên mặt nạ ngược. Tuy nhiên, có thể thực hiện công việc tính toán mặt nạ ngược nhanh hơn.

Trong nhiều trường hợp, một ACL cần so khớp tất cả máy tính trong một mạng cụ thể. Để so khớp một mạng con với một ACL, có thể sử dụng cách vẫn tắt như sau:

- Sử dụng chỉ số mạng con như là giá trị địa chỉ trong lệnh `access-list`
- Sử dụng mặt nạ ngược được tìm thấy bằng cách lấy `255.255.255.255` trừ mặt nạ mạng

Ví dụ, với mạng con `172.16.8.0 255.255.252.0`, sử dụng chỉ số mạng như là tham số địa chỉ và sau đó thực hiện tính toán sau đây để tìm mặt nạ ngược.

$$\begin{array}{r}
 255.255.255.255 \\
 - 255.255.252.0 \\
 \hline
 0.0.0.3.255
 \end{array}$$

Sau đây là các bước cho việc thực hiện cấu hình chính sách truy cập:

Bước 1: Sử dụng địa chỉ trong lệnh access-list là số mạng con

Bước 2: Sử dụng số được tìm thấy bằng cách trừ 255.255.255.255 cho mặt nạ mạng con.

Bước 3: Xem các giá trị từ hai bước đầu tiên như là số mạng con và số mặt nạ mạng, và tìm địa chỉ quảng bá cho mạng con đó. ACL phù hợp với khoảng địa chỉ giữa chỉ số mạng con và địa chỉ mạng.

Khoảng địa chỉ được xác định bằng tiến trình này là giống khoảng địa chỉ được so khớp bởi ACL. Vì thế, nếu đã tìm thấy khoảng địa chỉ mạng con nhanh và dễ dàng, sử dụng tiến trình này để thay đổi một ACL có thể giúp tìm kiếm các giá trị khác nhanh hơn. Ví dụ, với lệnh access-list **permit 172.16.200.0 0.0.7.255**, có thể xác định ngay 172.16.200.0 là số mạng con. Sau đó tính toán mặt nạ mạng là 255.255.248.0 như sau:

$$\begin{array}{r}
 255.255.255.255 \\
 - 0. 0. 7.255 \\
 \hline
 255.255.248.0
 \end{array}$$

Từ đây, có thể thực hiện tiếp các công việc tính toán khác đã được đề cập trong các chương trước đây.

8.1.2. Cấu hình chính sách truy cập IP chuẩn

Cú pháp chung cho việc cấu hình ACL chuẩn như sau:

Access-list access-list-number {deny|permit} source [source-wildcard]

Một chính sách truy cập chuẩn sử dụng một chuỗi các lệnh access-list có chung số. Các lệnh access-list với cùng số được xem như là cùng danh sách, với các lệnh được liệt kê trong cùng thứ tự trong đó chúng được thêm vào cấu hình. Mỗi lệnh access-list có thể trùng với một khoảng địa chỉ IP nguồn. Nếu xảy ra trùng khớp, ACL hoặc là cho phép gói tin đi qua (hành động **permit**, cho phép) hay hủy bỏ gói tin (hành động **deny**, từ chối). Mỗi ACL chuẩn có thể trùng với tất cả hay là chỉ một phần với địa chỉ IP nguồn của gói tin. **Chú ý rằng với ACL IP chuẩn, số khoảng cho ACL là 1 đến 99 và 1300 đến 1999.**

Danh sách sau sơ lược một tiến trình cấu hình được đề nghị. Mặc dù không cần phải nhớ tiến trình này, nhưng nó sẽ giúp nhiều hơn trong khi làm việc với ACL.

Bước 1: Hoạch định nơi (router và giao tiếp) và hướng (vào hay ra) trên giao tiếp đó.

- ACL chuẩn nên được đặt gần đích của gói tin để nó không hủy gói tin một cách vô tình với gói tin không cần hủy
- Vì ACL chuẩn chỉ có thể so khớp một địa chỉ IP nguồn, xác định địa chỉ IP nguồn của các gói tin khi nó đi vào hướng mà ACL đang kiểm tra.

Bước 2: Cấu hình một hay nhiều lệnh access-list để tạo ACL, lưu ý như sau

- Danh sách được tìm kiếm tuần tự, sử dụng trùng khớp đầu tiên. Nói cách khác, khi một gói tin trùng một trong số các lệnh access-list, việc tìm kiếm kết thúc, thậm chí nếu gói tin có thể trùng với lệnh bên dưới
- Hành động mặc định, nếu một gói tin không trùng với bất kỳ lệnh access-list nào, là hủy bỏ gói tin đó.

Bước 3: Kích hoạt ACL trên giao tiếp đã chọn của router, theo đúng hướng, sử dụng lệnh con giao tiếp ip access-group number {in|out}. Bây giờ xem xét hai ví dụ cấu hình ACL.

Ví dụ 8.1: Trong ví dụ này sẽ quay lại hình 8.1. Trong hình này, Bá không được phép truy cập Server 1. Trong đó, việc cấu hình kích hoạt một ACL cho tất cả các gói tin đi ra giao tiếp Ethernet0 của R1. ACL so khớp địa chỉ nguồn trong gói tin với địa chỉ IP của Bá. Chú ý rằng lệnh access-list trong phần cuối của ví dụ này, sau khi thực hiện lệnh show running-config.

```

interface Ethernet0
  ip address 172.16.1.1 255.255.255.0
  ip access-group 1 out

access-list 1 remark stop all traffic whose source IP is Bob
access-list 1 deny 172.16.3.10 0.0.0.0
access-list 1 permit 0.0.0.0 255.255.255.255

```

Trước tiên, xem xét cú pháp cơ bản của lệnh. Chính sách truy cập IP chuẩn sử dụng số trong khoảng từ 1 đến 99 hay 1300 đến 1999. Ví dụ này sử dụng ACL số 1, nhưng không có nghĩa là 1 hay 99 tốt hơn. Lệnh **access-list** là lệnh cấu hình toàn cục. Để cho phép ACL trên một giao tiếp và xác định hướng gói tin mà ACL được áp dụng, lệnh **ip access-group** được sử dụng. Trong trường hợp này, nó có nghĩa với ACL 1 trên Ethernet 0 với các gói tin đi ra khỏi giao tiếp đó.

ACL giữ các gói tin được gửi bởi Bá trên Ethernet của R1, dựa trên lệnh **access-list 1 deny 172.16.3.10 0.0.0.0**. Mặt nạ ngược 0.0.0.0 có nghĩa là so trùng tất cả 32 bit, vì thế chỉ các gói tin có địa chỉ IP chính xác trùng với 172.16.3.10 trong lệnh này với bị hùy đi. Lệnh **access-list 1 permit 0.0.0.0 255.255.255.255**, lệnh cuối cùng trong này, trùng khớp với tất cả gói tin, vì 255.255.255.255 có nghĩa là không quan tâm tất cả 32 bit đó. Nói cách khác, lệnh này phù hợp cho tất cả các địa chỉ IP nguồn. Tất cả các gói tin đều được phép.

Cuối cùng, chú ý rằng ví dụ đã thêm một lệnh **access-list 1 remark** vào ACL. Lệnh này cho phép thêm một chú thích văn bản, hay một đánh dấu, để có thể theo dõi mục đích của ACL. Đánh dấu này chỉ thể hiện trong cấu hình, không được thể hiện trong đầu ra lệnh **show**.

Ví dụ trên khá đơn giản, trong đó chính sách truy cập 1 ngăn các gói tin của Bá gửi đến Server2. Với cùng sơ đồ trong hình 8-1, một ACL chuẩn trên giao tiếp E0 của R1 không thể ngăn Bá truy cập Server 1 trong khi cho phép truy cập Server2. Để làm điều này, một ACL mở rộng là cần thiết để theo dõi cả địa chỉ IP nguồn và đích.

Nếu các lệnh trong ví dụ 8.1 được nhập vào chế độ cấu hình, IOS thay đổi cú pháp cấu hình của hai lệnh. Đầu ra của lệnh **show running-config** trong ví dụ 8.2 cho thấy khác biệt này.

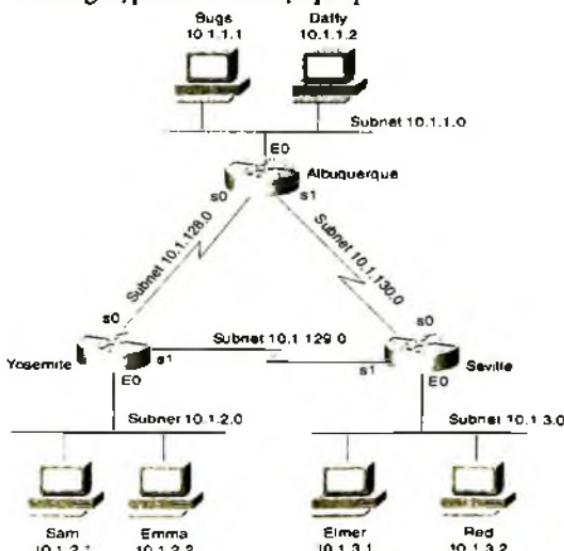
```
interface Ethernet0
  ip address 172.16.1.1 255.255.255.0
  ip access-group 1 out

  access-list 1 remark stop all traffic whose source IP is Bob
  access-list 1 deny host 172.16.3.10
  access-list 1 permit any
```

Các lệnh trong ví dụ 8.1 được thay đổi dựa trên ba yếu tố. Cisco IOS cho phép cả kiểu cấu hình cũ và mới với một số tham số. Ví dụ 8-1 cho thấy kiểu cũ, và router thay đổi cấu hình kiểu mới tương ứng trong ví dụ 8.2. Trước tiên, dùng mặt nạ ngược 0.0.0.0 không có nghĩa là router sẽ so khớp với một địa chỉ IP xác định. Thay đổi khác với cấu hình kiểu mới liên quan đến việc sử dụng mặt nạ ngược 255.255.255.255 nghĩa là phù hợp với tất cả. Cấu hình kiểu mới sử dụng từ khóa `any` để thay thế cho cả địa chỉ IP và mặt nạ ngược 255.255.255.255, `any` đơn giản nghĩa là bất kì địa chỉ IP nào cũng phù hợp.

Ví dụ 8.2: IP ACL chuẩn thứ hai giải thích rõ hơn về ACL. Ví dụ 6.3 và 6.4 cho thấy việc sử dụng cơ bản của chính sách truy cập IP chuẩn, với hai thay đổi như sau:

- Sam không được phép truy cập Bug hay Daffy
- Các máy tính trên Seville Ethernet không được phép truy cập các máy tính trên Yosemite Ethernet.
- Các trường hợp khác đều được phép



Hình 8.3. Chính sách truy cập chuẩn

Ví dụ 8.3:

```
interface serial 0
  ip access-group 3 out
  !
  access-list 3 deny host 10.1.2.1
  access-list 3 permit any
```

Ví dụ 8.4:

```
interface serial 1
  ip access-group 4 out
  !
  access-list 4 deny 10.1.3.0  0.0.0.255
  access-list 4 permit any
```

Trong phần đầu, hai chính sách truy cập đường như thực hiện được chức năng mong muốn. ACL3, cho phép các gói tin ra ngoài giao tiếp S0 của Yosemite, phù hợp với tiêu chuẩn 1, vì ACL 3 phù hợp với địa chỉ IP của Sam. ACL trên Seville, cho phép gói tin ra giao tiếp S1 của nó, phù hợp với tiêu chuẩn 2, vì ACL 4 so khớp tất cả gói tin đến từ mạng con 10.1.3.0/24. Cả hai router phù hợp với tiêu chuẩn 3: một mặt nạ ngược permit all được dùng tại cuối của mỗi chính sách truy cập để ghi đè lên các mặc định, là hủy tất cả các gói tin khác. Vì thế tất cả các tiêu chuẩn đều phù hợp.

Tuy nhiên, khi một liên kết WAN bị lỗi, một số vấn đề sẽ xảy ra với ACL đó. Ví dụ, nếu liên kết từ Albuquerque đến Yosemite bị lỗi, Yosemite học một con đường đến 10.1.1.0/24 qua Seville. Gói tin từ Sam, được chuyển tiếp với Yosemite và hướng đến với các máy tính trên Albuquerque, rời giao tiếp Serial 1 trên Yosemite mà không bị lọc. Vì thế tiêu chuẩn 1 không còn phù hợp nữa. Tương tự, nếu liên kết từ Seville đến Yosemite bị lỗi, Seville đưa các gói tin qua Albuquerque, định tuyến qua chính sách truy cập đã cho phép trên Seville, vì thế tiêu chuẩn 2 cũng không còn phù hợp.

Ví dụ 8.5 mô tả một giải pháp khác, với tất cả cấu hình trên Yosemite – một trường hợp vẫn làm việc thậm chí khi có một số liên kết lỗi.

Ví dụ 8.5:

```

interface serial 0
  ip access-group 3 out
  !
interface serial 1
  ip access-group 3 out
  !
interface ethernet 0
  ip access-group 4 out
  !
access-list 3 remark meets criteria 1
access-list 3 deny host 18.1.2.1
access-list 3 permit any
!
access-list 4 remark meets criteria 2
access-list 4 deny 18.1.3.0 0.0.0.255
access-list 4 permit any

```

Cấu hình trong ví dụ 8.5 giải quyết rắc rối của ví dụ 8.3 và 8.4. ACL 3 kiểm tra địa chỉ IP nguồn của Sam, và nó được cho phép trên cả hai giao tiếp serial với các lưu lượng ra. Vì thế, với lưu lượng được định tuyến lại vì liên kết WAN lỗi, các gói tin từ Sam tiếp tục bị lọc. Để phù hợp với tiêu chuẩn 2, Yosemite lọc tất cả gói tin khi chúng qua giao tiếp Ethernet của nó. Chính thế, không phụ thuộc vào liên kết WAN mà gói tin đi vào, các gói tin từ mạng con của Seville không thể được chuyển tiếp đến Ethernet của Yosemite.

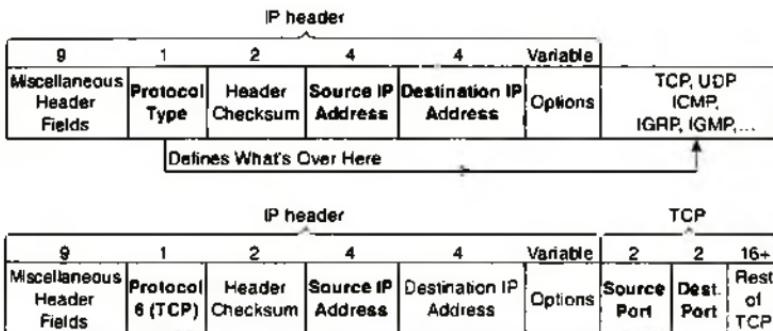
8.2. CHÍNH SÁCH KIỂM SOÁT TRUY CẬP IP MỞ RỘNG

Các chính sách truy cập IP mở rộng có cả phần tương đồng và khác biệt so sánh với IP ACL chuẩn. Giống như danh sách chuẩn, người quản trị cho phép chính sách truy cập mở rộng trên các giao tiếp với các gói tin hoặc là đến hay đi khỏi giao tiếp. IOS tìm kiếm danh sách tuần tự. Lệnh trùng khớp đầu tiên ngưng việc tìm kiếm lại và xác định hành động cần thực hiện. Tất cả chức năng khác đều dùng cho chính sách truy cập chuẩn.

Một khác biệt chính giữa hai loại là số trường trong gói tin có thể được so sánh để khớp bởi các chính sách truy cập mở rộng. Một ACL mở rộng đơn có thể kiểm tra nhiều phần của một tiêu đề gói tin, yêu cầu tất cả các tham số phải trùng khớp để phù hợp với một ACL. Việc so khớp này làm cho chính sách truy cập mở rộng vừa hữu dụng vừa phức tạp hơn so với IPACL chuẩn.

8.2.1. Các khái niệm IP ACL mở rộng

Chính sách truy cập mở rộng tạo một khả năng so khớp mạnh mẽ bằng cách kiểm tra nhiều phần của một gói tin. Hình 8.4 cho thấy nhiều trường trong tiêu đề gói tin có thể trùng khớp.



Hình 8.4. Chính sách truy cập mở rộng

Tập trên cùng của tiêu đề cho thấy loại của giao thức IP, xác định tiêu đề nào tuân theo tiêu đề IP. Người quản trị có thể xác định tất cả các gói tin IP, hay tất cả với tiêu đề TCP, UDP, ICMP, vv, bằng cách kiểm tra trường Protocol. Cũng có thể kiểm tra cả các địa chỉ IP nguồn và đích, như thể hiện. Phần thấp hơn của hình cho thấy một ví dụ với tiêu đề TCP theo sau tiêu đề IP, chỉ ra vị trí của số port TCP nguồn và đích. Những số port này xác định loại ứng dụng đang sử dụng. Ví dụ, web sử dụng port mặc định là 80. Nếu xác định một giao thức là TCP hay UDP, cũng có thể kiểm tra số port. Bảng sau đây tóm tắt một số trường được sử dụng thường xuyên nhất có thể được so khớp với một IP ACL mở rộng, khi so sánh với một IP ACL chuẩn.

Bảng 8.3. Các loại chính sách truy cập

Loại chính sách truy cập	Có thể trùng với
Các chính sách truy cập chuẩn và mở rộng	Địa chỉ IP nguồn
	Phản địa chỉ IP nguồn sử dụng mặt nạ ngược
	Địa chỉ IP đích
	Phản địa chỉ IP đích sử dụng mặt nạ ngược
	Loại giao thức (TCP, UDP, ICMP, IGRP,...)
Chính sách ACL mở rộng	Các port nguồn
	Các port đích
	Tất cả luồng TCP trừ luồng đầu tiên
	IP TOS
	Địa chỉ IP theo ý thích

IOS kiểm tra tất cả thông tin cấu hình phù hợp trong lệnh **acces-list** đơn. Mọi thứ phải phù hợp trong một lệnh đơn được xem là một trùng khớp và hành động xác định được thực hiện. Phản tham số bắt đầu với loại giao thức (IP, UDP, TCP, ICMP...), được theo sau bởi địa chỉ IP nguồn, port nguồn, địa chỉ IP đích, và port đích. Bảng sau đây liệt kê nhiều lệnh **access – list** mẫu, với nhiều tham số được cấu hình và một số giải thích.

Bảng 8.4. Một số lệnh access-list

Lệnh access – list	Trùng khớp với
Access-list 101 deny ip any thiết bị 10.1.1.1	Bất kì gói IP nào, bất kì địa chỉ IP nguồn, với địa chỉ IP đích là 10.1.1.1
Access-list 101 deny tcp any gt 1023 thiết bị 10.1.1.1 eq 23	Các gói tin tiêu đề TCP, bất kì địa chỉ IP nào, với địa chỉ port lớn hơn (gt) 1023, địa chỉ IP đích là 10.1.1.1 và địa chỉ IP nguồn bằng (eq) 23.
Access-list 101 deny tcp any thiết bị 10.1.1.1 eq 23	Cùng với ví dụ trên, nhưng tất cả gói TCP từ thiết bị 10.1.1.1 đến thiết bị 10.1.1.1 đều bị chặn, vì tham số đó bị bỏ qua trong trường hợp này.
Access-list 101 deny any thiết bị 10.1.1.1 eq telnet	Cùng ví dụ trên, từ khóa telnet thay thế cho port 23
Access-list 101 deny udp 1.0.0.0 0.255.255.255 lt 1023 any	Một gói tin với địa chỉ nguồn trong mạng 1.0.0.0, sử dụng UDP với địa chỉ port nhỏ hơn (lt) 1023, với bất kì địa chỉ IP đích nào

8.2.2. So khớp số port TCP và UDP

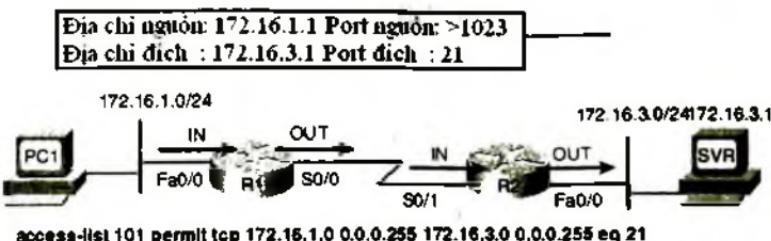
IP ACL mở rộng cho phép so khớp trường giao thức tiêu đề IP, cũng như là so khớp số port TCP và UDP nguồn và đích. Tuy nhiên, nhiều người gặp khó khăn khi lần đầu cấu hình ACL phù hợp với số port, cụ thể là so khớp số port nguồn.

Khi xem xét bất kì câu hỏi có liên quan đến TCP hay UDP port, luôn ghi nhớ:

- Lệnh access – list phải sử dụng từ khóa giao thức tcp để cho phép so khớp port TCP và từ khóa udp để cho phép so khớp port UDP. Từ khóa ip không cho phép so khớp số port.
- Các đối số port nguồn và đích trong lệnh access – list là tùy ý. Nói cách khác, vị trí của chúng trong lệnh xác định liệu đối số kiểm tra là port nguồn hay đích.
- Ghi nhớ rằng ACL có thể so khớp các gói tin được gửi đến một server bằng cách so sánh port đích với một số port biết trước. Tuy nhiên, ACL cần phải so khớp port nguồn với các gói tin được gửi bởi server.
- Cần thiết phải nhớ các ứng dụng TCP và UDP thông dụng nhất và các port biết trước của nó, được liệt kê trong bảng 8.5.

Ví dụ, xem xét sơ đồ mạng đơn giản trong hình. FTP server ở bên phải và client ở bên trái. Hình này cho thấy cú pháp của một ACL phù hợp với:

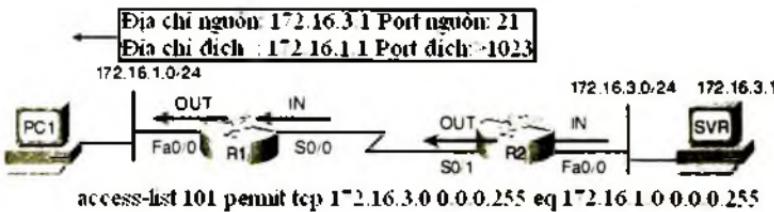
- Gói tin chứa tiêu đề TCP
- Gói tin được gửi đến một mạng con của client
- Gói tin được gửi đến mạng con server
- Gói tin với port đích là 21



Hình 8.5. Chính sách truy cập mở rộng

Xem xét gói tin di chuyển từ trái sang phải, từ PC1 sang server. Nếu server sử dụng port biết trước 21 (port điều khiển của FTP), gói tin được gửi bởi PC1, trong tiêu đề TCP, có port đích có giá trị 21. Cú pháp ACL bao gồm đối số **eq 21** sau địa chỉ IP đích với vị trí trong câu lệnh nhấn mạnh rằng đối số này phù hợp với port đích. Kết quả là, lệnh ACL được thể hiện trong hình sẽ phù hợp với gói tin này, và port đích là 21, nếu được sử dụng trong bất kỳ vị trí nào của bốn vị trí được nhấn mạnh bởi đường mũi tên đậm trong hình.

Ngược lại, hình sau đây cho thấy một hình ảnh ngược lại, với một gói tin được gửi bởi server ngược lại PC1. Trong trường hợp này, tiêu đề TCP của gói tin có port nguồn là 21, vì thế ACL phải kiểm tra giá trị port nguồn 21, và ACL phải được đặt trên các giao tiếp khác nhau.



Hình 8.6. Chính sách truy cập mở rộng (tiếp theo)

Bảng 8.5 liệt kê các số port thông dụng nhất và lớp giao vận, ứng dụng tương ứng của nó. Chú ý rằng cú pháp của lệnh **access - list** chấp nhận cả số port và phiên bản ngắn tắt của tên ứng dụng.

Bảng 8.5. Một số ứng dụng và các cổng – port tương ứng

Chi số port	Giao thức	Ứng dụng	Tên từ khóa ứng dụng trong lệnh
20	TCP	FTP Da	ftp-da
21	TCP	FTP Control	ftp
22	TCP	SSH	-
23	TCP	Telnet	Telnet
25	TCP	SMTP	Smtp
53	UDP,TCP	DNS	Domain
67,68	UDP	DHCP	Nameserver
69	UDP	TFTP	Tftp
80	TCP	HTTP(WWW)	www
110	TCP	POP3	Pop3
161	UDP	SNMP	Snmp
443	TCP	SSL	-
16.384-32.767	UDP	Thoại trên RTP (VoIP) và video	-

8.2.3. Cấu hình IP ACL mở rộng

Vì ACL mở rộng có thể so khớp quá nhiều trường khác nhau trong tiêu đề của gói tin IP, cú pháp lệnh không thể dễ dàng tóm tắt trong một số lệnh đơn chung. Để tham khảo, bảng 8.6 liệt kê cú pháp của hai câu lệnh chung phổ biến nhất.

Bảng 8.6. Hai lệnh access-list phổ biến nhất

Lệnh	Chế độ cấu hình và mô tả
Access-list access-list-number {deny permit} protocol source source-wildcard destination destination destination-wildcard [log log-input]	Lệnh cấu hình toàn cục với danh sách địa chỉ IP mở rộng. Sử dụng số giữa 100 và 199 hay 2000 và 2699.
Access-list access-list-number {deny permit} {tcp udp} source source-wildcard [operator port] destination destination-wildcard [operator port] [established][log]	Phiên bản của lệnh access-list với tham số TCP xác định

Tiến trình cấu hình cho ACL mở rộng hầu hết giống với tiến trình được sử dụng cho ACL chuẩn. Vị trí và hướng nên được chọn trước tiên để các đối số của ACL có thể được hoạch định dựa trên thông tin trên gói tin tuân theo hướng đó. ACL nên được cấu hình với lệnh **access – list**. Sau đó ACL nên được kích hoạt với cùng lệnh **ip access – group** được sử dụng với ACL chuẩn. Tất cả những bước này tương tự như ACL chuẩn. Tuy nhiên, những khác biệt trong cấu hình được tóm tắt như sau:

- ACL mở rộng nên được đặt càng gần càng tốt với nguồn gói tin được lọc, vì ACL mở rộng có thể được cấu hình để mà chúng không thể hủy gói tin mà nó không nên hủy. Vì thế việc lọc gói tin gần với nguồn của nó tiết kiệm nhiều băng thông hơn.
- Tất cả các trường trong lệnh **access – list** phải so khớp một gói tin với gói tin được xem xét trong lệnh **access – list**.
- Lệnh **access – list** mở rộng sử dụng số giữa 100 – 199 và 2000 – 2699.

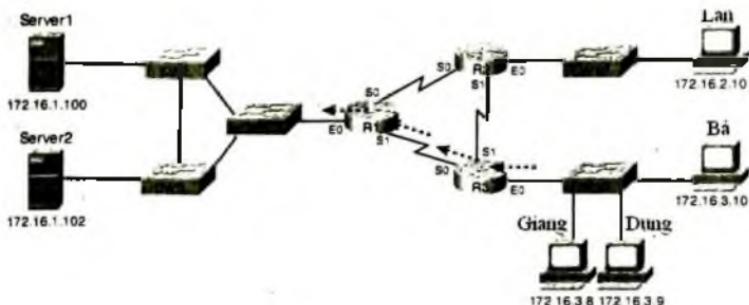
Phiên bản mở rộng của lệnh **access – list** cho phép so khớp số port sử dụng nhiều hoạt động cơ bản, như là bằng và nhỏ hơn. Tuy nhiên, các lệnh sử dụng các cú pháp vẫn tắt, như sau:

Bảng 8.7. Toán tử trong lệnh access-list

Toán tử trong lệnh access-list	Ý nghĩa
Eq	Equal to – bằng với
Neq	Not equal to – không bằng với
Lt	Less than – Nhỏ hơn
Gr	Greater than – Lớn hơn
Range	Khoảng chỉ số port

8.2.3.1. Chính sách truy cập IP mở rộng: ví dụ 8.6

Ví dụ này tập trung vào tìm hiểu cú pháp cơ bản. Trong trường hợp này, Bán bị từ chối truy cập vào tất cả FTP server trên Ethernet của R1. Và Lan bị từ chối truy cập vào Web server của Server1.



Hình 8.7. ví dụ chính sách truy cập mở rộng

Ví dụ 8.6:

```

interface Serial0
  ip address 172.16.12.1 255.255.255.0
  ip access-group 101 in
  !
interface Serial1
  ip address 172.16.13.1 255.255.255.0
  ip access-group 101 in
  !
access-list 101 remark Stop Bob to FTP servers, and Larry to Server1 web
access-list 101 deny tcp host 172.16.3.10 172.16.1.0 0.0.0.255 eq ftp
access-list 101 deny tcp host 172.16.2.10 host 172.16.1.100 eq www
access-list 101 permit ip any any
  
```

Trong ví dụ 8.6, lệnh ACL đầu tiên ngăn truy cập của Bá đến FTP server trong mạng con 172.16.1.0. Lệnh thứ hai ngăn truy cập của Lan đến dịch vụ web trên Server 1. Lệnh cuối cùng cho phép tất cả các lưu lượng khác.

Tập trung vào cú pháp, có nhiều mục mới cần quan tâm. Trước tiên, số chính sách truy cập rơi vào khoảng 100 đến 199 hay 2000 đến 2699. Tùy theo hành động *permit* hay *deny*, đổi số *protocol* xác định liệu muốn kiểm tra cho tất cả gói tin IP hay chỉ với các gói tin chứa tiêu đề TCP hay UDP. Khi kiểm tra số port TCP và UDP, phải xác định giao thức là TCP hay UDP.

Ví dụ này sử dụng đổi số *eq*, nghĩa là bằng với “equal”, để kiểm tra số port đích cho điều khiển FTP (từ khóa *ftp*) và lưu lượng HTTP (từ

khóa http). có thể sử dụng giá trị số - hay các tham số khác thông dụng hơn, ví dụ như eq 80, hay eq www.

Trong ví dụ ACL mở rộng đầu tiên này, chính sách truy cập có thể được thay thế trên R2 và R3 thay vì R1. Như đã được đề cập, Cisco đưa một số khuyến nghị về nơi đặt IP ACL. Với IP ACL mở rộng, Cisco đề nghị nên đặt càng gần có thể nguồn của gói tin. Chính thế, ví dụ 8-7 có cùng kết quả với ví dụ 8.6, ngăn truy cập của Bá đến FTP server tại khu vực chính, và nó thực hiện bằng một ACL trên R3.

Ví dụ 8.7:

```
interface Ethernet0
 ip address 172.16.3.1 255.255.255.0
 ip access-group 101 in

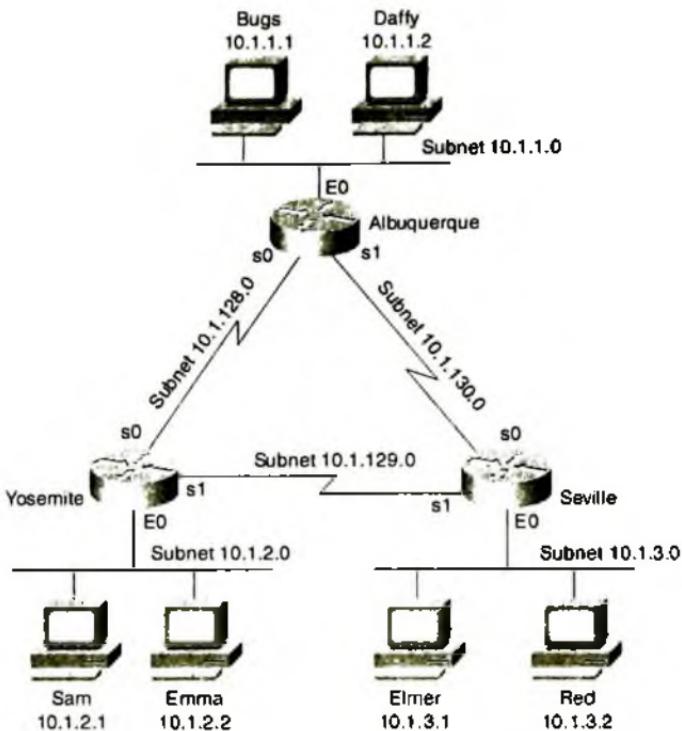
access-list 101 remark deny Bob to FTP servers in subnet 172.16.1.0/24
access-list 101 deny tcp host 172.16.3.18 172.16.1.0 0.0.0.255 eq ftp
access-list 101 permit ip any any
```

ACL 101 trông khá giống như ACL 101 ở ví dụ 8.6, nhưng lần này ACL không quan tâm kiểm tra tiêu chuẩn phù hợp với lưu lượng của Lan, vì lưu lượng của Lan sẽ không bao giờ vào giao tiếp Ethernet 0 của R3. Vì ACL được đặt trên R3, gần Bá, nó tìm kiếm các gói tin Bá gửi đi vào giao tiếp Ethernet0 của nó. Vì ACL đó, lưu lượng FTP của Bá đến 172.16.1.0/24 bị từ chối, với tất cả các lưu lượng khác vào giao tiếp E0 của R3 được đi vào mạng.

8.2.4.2. Chính sách truy cập IP mở rộng: ví dụ 2

Ví dụ 8.8, dựa trên mạng được thể hiện trong hình 8.8, cho thấy một ví dụ khác về cách sử dụng chính sách truy cập IP mở rộng. Ví dụ này sử dụng cùng các tiêu chuẩn và sơ đồ mạng như ví dụ IP ACL chuẩn thứ hai, như sau:

- Sam không được phép truy cập Bugs hay Daffy
- Các máy tính trên Seville Ethernet không được phép truy cập đến các máy tính trên Yosemite Ethernet
- Các trường hợp khác đều được phép



Hình 8.8. Cấu hình chính sách truy cập mở rộng

Ví dụ 8.8:

```

interface ethernet 0
ip access-group 110 in
!
access-list 110 deny ip host 10.1.2.1 10.1.1.0 0.0.0.255
access-list 110 deny ip 10.1.2.0 0.0.0.255 10.1.3.0 0.0.0.255
access-list 110 permit ip any any

```

Cấu hình này giải quyết vấn đề với một vài lệnh trong khi vẫn giữ những hướng dẫn thiết kế của Cisco khi đặt ACL mở rộng càng gần càng tốt nguồn lưu lượng. ACL lọc các gói tin vào giao tiếp E0 của Yosemite, là giao tiếp router đầu tiên mà gói tin được gửi bởi Sam đi vào.

8.2.4. Quản lý cấu hình ACL

Giờ đã có một hiểu biết tốt về những khái niệm cốt yếu trong IP ACL của IOS, phần tiếp theo xem xét các cải tiến của IOS để hỗ trợ ACL: ACL có tên và số thứ tự ACL. Dù hai chức năng này là hữu dụng và quan trọng, chúng không bổ sung bất kì chức năng nào để router có thể hay không thể lọc, khi so sánh ACL được đánh số được xem xét trong chương này. Thay vào đó, ACL có tên và số thứ tự ACL cung cấp khả năng cấu hình làm cho nó dễ nhớ các tên ACL hơn và dễ hiệu chỉnh các ACL có sẵn hơn khi một ACL cần thay đổi.

8.2.4.1. Chính sách truy cập IP có tên

Các ACL có tên, được giới thiệu với IOS phiên bản 11.2 có thể được dùng để so khớp cùng các gói tin với cùng các tham số, và sử dụng với ACL IP chuẩn cũng như mở rộng. Các ACL IP có tên có một số khác biệt, tuy nhiên, một vài trong số chúng làm cho chúng dễ dàng hơn để làm việc. Khác biệt rõ ràng nhất là ở IOS xác định định ACL có tên sử dụng tên đã tạo ra, khác với sử dụng số.

Ngoài ra là sử dụng các tên có tính gợi nhớ hơn, thuận lợi chính của ACL có tên so với ACL đánh số, có thể xóa các dòng độc lập trong một chính sách truy cập IP có tên. Qua lịch sử của IP ACL đánh số và lệnh toàn cục ip access – list cho đến khi xuất hiện IOS 12.3, một dòng đơn trong ACL đánh số không thể bị xóa. Ví dụ, nếu đã cấu hình trước đây với lệnh ip access – list 101 permit tcp any any eq 80, sau đó nhập tiếp lệnh no ip access – list 101 permit tcp any any eq 80, thì ACL 101 không thể bị xóa. Lợi ích của ACL đặt tên là có thể nhập một lệnh xóa các dòng độc lập trong một ACL.

Cú pháp cấu hình là rất giống giữa các chính sách truy cập có tên và đánh số. Các mục có thể so khớp với một chính sách truy cập IP chuẩn đánh số là xác định với các mục có thể được so khớp với một chính sách

truy cập IP chuẩn có tên. Giống như vậy, các mục được xác định với cá chính sách truy cập IP có tên và được đánh số.

Hai khác biệt cấu hình quan trọng tồn tại giữa ACL đánh số kiểu cũ và chính sách truy cập có tên kiểu mới hơn. Khác biệt chính đầu tiên là chính sách truy cập có tên sử dụng một lệnh toàn cục đóng vai trò người dùng trong chế độ con chính sách truy cập IP có tên, trong đó việc từ chối/ cho phép (permit/ deny) được cấu hình. Điểm khác biệt chính khác là khi một lệnh so khớp bị xóa, chỉ một lệnh đó bị xóa.

Ví dụ 8.9 cho thấy trường hợp sử dụng IP ACL có tên. Nó thể hiện dấu nhắc lệnh thay đổi trong chế độ cấu hình, thể hiện rằng người dùng được đặt trong chế độ cấu hình ACL. Nó cũng liệt kê phần thích hợp của đầu ra của lệnh **show running - configuration**. Nó kết thúc với một ví dụ về cách người quản trị có thể xóa các dòng độc lập trong một ACL có tên.

Ví dụ 8.9:

```
conf t
Enter configuration commands, one per line. End with Ctrl-Z.
Router(config)#ip access-list extended barney
Router(config-ext-nacl)#permit tcp host 10.1.1.2 eq www any
Router(config-ext-nacl)#deny udp host 10.1.1.1 10.1.2.0 0.0.0.255
Router(config-ext-nacl)#deny ip 10.1.3.0 0.0.0.255 10.1.2.0 0.0.0.255
! The next statement is purposefully wrong so that the process of changing
! the list can be seen.
Router(config-ext-nacl)#deny ip 10.1.2.0 0.0.0.255 10.2.3.0 0.0.0.255

Router(config-ext-nacl)#deny ip host 10.1.1.199 host 10.1.3.2
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#interface serial1
Router(config-if)#ip access-group barney out
Router(config-if)##^Z
Router#show running-config
Building configuration...
```

Current configuration:

```

.
. (unimportant statements omitted)

interface serial 1
 ip access-group barney out
!
ip access-list extended barney
 permit tcp host 10.1.1.2 eq www any
 deny   udp host 10.1.1.1 10.1.2.0 0.0.0.255
 deny   ip 10.1.3.0 0.0.0.255 10.1.2.0 0.0.0.255
 deny   ip 10.1.2.0 0.0.0.255 10.2.3.0 0.0.0.255
 deny   ip host 10.1.1.130 host 10.1.3.2
 deny   ip host 10.1.1.28 host 10.1.3.2
 permit ip any any
Router#conf t
Enter configuration commands, one per line.  End with Ctrl-Z.
Router(config)#ip access-list extended barney
Router(config-ext-nacl)#no deny ip 10.1.2.0 0.0.0.255 10.2.3.0 0.0.0.255
Router(config-ext-nacl)##Z
Router#show access-list

Extended IP access list barney
 10 permit tcp host 10.1.1.2 eq www any
 20 deny   udp host 10.1.1.1 10.1.2.0 0.0.0.255
 30 deny   ip 10.1.3.0 0.0.0.255 10.1.2.0 0.0.0.255
 50 deny   ip host 10.1.1.130 host 10.1.3.2
 60 deny   ip host 10.1.1.28 host 10.1.3.2
 70 permit ip any any

```

Ví dụ này bắt đầu với việc tạo một ACL có tên là **barney**. Lệnh **ip access - list extended barney** tạo ACL, đặt tên là **barney** và đặt người dùng trong chế độ cấu hình ACL. Lệnh này cũng báo cho IOS biết rằng **barney** là một ACL mở rộng. Kế tiếp, bảy lệnh **permit** và **deny** sử dụng cùng cú pháp mà lệnh **access - list** đánh số sử dụng, bắt đầu với từ khóa **deny** hay **permit**. Trong ví dụ này một chú thích được bổ sung chỉ trước khi lệnh được xóa sau đó.

Kết quả lệnh **show running - config** liệt kê cấu hình có tên ACL trước khi một mục đơn bị xóa. Kế tiếp, lệnh **no deny ip ...** xóa một mục đơn từ ACL. Chú ý rằng đầu ra của lệnh **show running - config** vẫn liệt kê ACL, với sáu lệnh **permit** và **deny** vì bảy.

8.2.4.2. Hiệu chỉnh ACL sử dụng số thứ tự

Các ACL được đánh số đã tồn tại trong IOS kể từ những ngày đầu của router Cisco. Kể từ khi tạo ra nó, cho đến phiên bản IOS 12.2, cách duy nhất để chỉnh sửa ACL đánh số có sẵn là xóa một dòng trong ACL – tức là xóa toàn bộ ACL và sau đó cấu hình lại toàn bộ ACL. Bên cạnh việc bất tiện, tiến trình này cũng gây ra một số mặt nhược điểm. Khi xóa ACL, quan trọng là phải hủy ACL từ tất cả các giao tiếp, và sau đó xóa chúng, cấu hình lại và kích hoạt nó trên giao tiếp đó. Ngược lại, trong suốt tiến trình cấu hình lại này, trước khi tắt cả các lệnh được cấu hình lại, ACL sẽ không thực hiện tất cả các kiểm tra cần thiết, thỉnh thoảng gây ra lỗi, hay tạo ra lỗ hổng mạng cho nhiều hình thức tấn công khác nhau.

Như đã đề cập, phiên bản nguyên thủy IOS hỗ trợ cho các ACL có tên, được giới thiệu trong IOS 11.2, giải quyết một số vấn đề hiệu chỉnh. Các lệnh nguyên thủy cho ACL có tên cho phép xóa một dòng trong một ACL. Tuy nhiên, các lệnh cấu hình không cho phép chèn một lệnh permit hay deny mới vào danh sách. Tất cả các lệnh mới được thêm vào cuối của ACL.

Với IOS 12.3, Cisco giới thiệu nhiều các tham số cấu hình cho ACLs – các lựa chọn được áp dụng cho cả IP ACL có tên và đánh số. Những lựa chọn này tận dụng những ưu điểm của một số thứ tự của ACL được thêm vào mỗi lệnh permit hay deny ACL, với số đại diện cho thứ tự lệnh trong ACL. Số thứ tự ACL cung cấp các chức năng sau đây cho cả các ACL có tên và đánh số:

- Một lệnh ACL permit hay deny đơn có thể được xóa chỉ bởi tham chiếu số thứ tự, mà không phải xóa toàn bộ phần còn lại của ACL.
- Các lệnh permit và deny mới được thêm vào có thể được cấu hình với một số thứ tự, xác định vị trí của lệnh bên trong ACL.
- Các lệnh permit và deny mới được thêm vào có thể được cấu hình mà không có số thứ tự, với IOS tạo một số thứ tự và đặt nó vào cuối của ACL.

Để tận dụng khả năng xóa và chèn các dòng vào trong một ACL, cả ACL đánh số và đặt tên phải sử dụng cùng kiểu cấu hình và lệnh được dùng cho ACL có tên. Khác biệt duy nhất trong cú pháp là liệu tên hay số được sử dụng. Ví dụ 8.10 cho thấy một cấu hình của IP ACL đánh số chuẩn.

Bước 1: ACL số 24 được cấu hình, sử dụng phương pháp cấu hình kiểu mới, với ba lệnh permit

Bước 2: Lệnh show ip access – list thể hiện ba lệnh permit, với số thứ tự là 10, 20 và 30.

Bước 3: Xóa chỉ lệnh permit thứ hai, sử dụng lệnh con no 20

Bước 4: Lệnh show ip access – list xác nhận rằng ACL bây giờ chỉ có hai dòng (thứ tự 10 và 30)

Bước 5: Thêm một lệnh permit mới vào phần đầu của ACL, sử dụng lệnh 5 deny 10.1.1.1

Bước 6: Lệnh show ip access – list một lần nữa xác nhận thay đổi, lần này liệt kê ba lệnh permit, thứ tự 5, 10 và 30.

Ví dụ 8.10:

```
! Step 1: The 3-line Standard Numbered IP ACL is configured.
R1#configure terminal
Enter configuration commands, one per line. End with Ctrl-Z.
R1(config)#ip access-list standard 24
R1(config-std-nacl)#permit 10.1.1.0 0.0.0.255
R1(config-std-nacl)#permit 10.1.2.0 0.0.0.255
R1(config-std-nacl)#permit 10.1.3.0 0.0.0.255
! Step 2: Displaying the ACL's contents, without leaving configuration mode.
R1(config-std-nacl)#do show ip access-list 24
Standard IP access list 24
    10 permit 10.1.1.0, wildcard bits 0 0.0.255
    20 permit 10.1.2.0, wildcard bits 0 0.0.255
    30 permit 10.1.3.0, wildcard bits 0 0.0.255
! Step 3: Still in ACL 24 configuration mode, the line with sequence number 20 is deleted.
R1(config-std-nacl)#no 20
! Step 4: Displaying the ACL's contents again, without leaving configuration mode.
! Note that line number 20 is no longer listed.
R1(config-std-nacl)#do show ip access-list 24
Standard IP access list 24
    10 permit 10.1.1.0, wildcard bits 0 0.0.255
    30 permit 10.1.3.0, wildcard bits 0 0.0.255
! Step 5: Inserting a new first line in the ACL.
R1(config-std-nacl)#5 deny 10.1.1.1
! Step 6: Displaying the ACL's contents one last time, with the new statement (sequence
! number 5) listed first.
R1(config-std-nacl)#do show ip access-list 24
Standard IP access list 24
    5 deny 10.1.1.1
    10 permit 10.1.1.0, wildcard bits 0 0.0.255
    30 permit 10.1.3.0, wildcard bits 0 0.0.255
```

Thú vị là, các ACL đánh số có thể được cấu hình với kiểu mới, hay kiểu cũ, sử dụng lệnh cấu hình access – list, như thể hiện trong nhiều ví dụ đầu tiên trong chương. Thực ra, có thể sử dụng cả hai loại cấu hình trên một ACL đơn. Tuy nhiên, không quan tâm đến loại cấu hình được sử dụng, đều ra lệnh **show running – config** vẫn thể hiện các lệnh cấu hình kiểu cũ. Ví dụ 8.11 mô tả các yếu tố này, thực hiện khi ví dụ 8.10 kết thúc, với các bước bổ sung sau đây:

Bước 7: Liệt kê cấu hình (show running – config), liệt kê lệnh cấu hình kiểu cũ – thậm chí dù ACL được tạo với cấu hình kiểu mới.

Bước 8: Thêm một lệnh mới vào cuối ACL, sử dụng lệnh cấu hình kiểu cũ access – list 24 permit 10.1.4.0 0.0.0.255

Bước 9: Lệnh **show ip access – list** xác nhận rằng lệnh kiểu cũ access – list từ bước trước tuân theo quy tắc được thêm vào cuối của ACL.

Bước 10: Thể hiện cấu hình để xác nhận rằng các thành phần của ACL 24 được cấu hình với cả kiểu cũ và mới được liệt kê trong cùng ACL kiểu cũ.

Ví dụ 8.11:

```
! Step 7: A configuration snippet for ACL 24.
R1#show running-config
! The only lines shown are the lines from ACL 24
access-list 24 deny 10.1.1.1
access-list 24 permit 10.1.1.0 0.0.0.255
access-list 24 permit 10.1.3.0 0.0.0.255

! Step 8: Adding a new access-list 24 command
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 24 permit 10.1.4.0 0.0.0.255
R1(config)#^Z
! Step 9: Displaying the ACL's contents again, with sequence numbers. Note that even
! the new statement has been automatically assigned a sequence number.
R1#show ip access-list 24
Standard IP access list 24
  5 deny 10.1.1.1
  10 permit 10.1.1.0, wildcard bits 0.0.0.255
  30 permit 10.1.3.0, wildcard bits 0.0.0.255
  40 permit 10.1.4.0, wildcard bits 0.0.0.255
```

```

I Step 10: The numbered ACL configuration remains in old-style configuration commands.
R1#show running-config
! The only lines shown are the lines from ACL 24
access-list 24 deny 10.1.1.1
access-list 24 permit 10.1.1.0 0.0.0.255
access-list 24 permit 10.1.3.0 0.0.0.255
access-list 24 permit 10.1.4.0 0.0.0.255

```

8.3. BÀI TẬP VÀ CÂU HỎI CHƯƠNG 8

Câu 1: Hai nguyên nhân nào sau đây mà một quản trị viên cần sử dụng chính sách kiểm soát truy cập?

- a. Để điều khiển truy cập vty vào một router
- b. Để điều khiển lưu lượng gói tin quảng bá qua một router
- c. Để lọc gói tin khi nó đi qua một router.
- d. Để lọc gói tin bắt nguồn từ router đó.
- e. Để thay thế mật khẩu để chống lại các nguy cơ bảo mật.

Câu 2: Trung là một máy tính có địa chỉ IP 10.1.1.1 trong mạng con 10.1.1.0/24. Điều nào sau đây là chuẩn IP ACL có thể được cấu hình để thực hiện công việc?

- a. So khớp với địa chỉ IP nguồn
- b. So khớp các địa chỉ IP 10.1.1.1 thông qua 10.1.1.4 với một lệnh access-list mà không so khớp với các địa chỉ IP khác.
- c. So khớp tất cả địa chỉ IP trong mạng con Trung với một lệnh access-list mà không phải so khớp với các địa chỉ IP khác.
- d. So khớp chỉ địa chỉ IP đích.

Câu 3: Địa chỉ mặt nạ mạng con ngược nào sau đây là hữu dụng khi so khớp tất cả các gói tin IP trong mạng con 10.1.128.0/24?

- a. 0.0.0.0
- b. 0.0.0.31
- c. 0.0.0.240
- d. 0.0.0.255
- e. 0.0.15.0
- f. 0.0.248.255

Câu 4: Mặt nạ mạng con ngược nào sau đây là hữu dụng cho việc so khớp tất cả các địa chỉ IP trong mạng con 10.1.128.0, mặt nạ 255.255.240.0?

- a. 0.0.0.0
- b. 0.0.0.31
- c. 0.0.0.240
- d. 0.0.0.255
- e. 0.0.15.255
- f. 0.0.248.255

Câu 5: Trường nào sau đây không thể so sánh dựa trên một IP ACL mở rộng?

- a. Giao thức
- b. Địa chỉ IP nguồn
- c. Địa chỉ IP đích
- d. Byte TOS
- e. URL
- f. Tên file cho việc truyền FTP

Câu 6: Lệnh access-list nào sau đây cho phép lưu lượng có thể so khớp các gói tin đi ra từ máy tính 10.1.1.1 đến tất cả web server có địa chỉ IP bắt đầu với 172.16.5?

- a. access-list 101 permit tcp thiết bị 10.1.1.1 172.16.5.0 0.0.0.255 eq www
- b. access-list 1951 permit ip thiết bị 10.1.1.1 172.16.5.0 0.0.0.255 eq www
- c. access-list 2523 permit ip thiết bị 10.1.1.1 eq www 172.16.5.0 0.0.0.255
- d. access-list 2523 permit tcp thiết bị 10.1.1.1 eq www 172.16.5.0 0.0.0.255
- e. access-list 2523 permit tcp thiết bị 10.1.1.1 172.16.5.0 0.0.0.255 eq www

Câu 7: Lệnh access – list nào sau đây cho phép lưu lượng có thể so khớp các gói tin đi ra từ bất kì web client nào từ bất kì web server có địa chỉ IP bắt đầu với 172.16.5?

- A. access-list 101 permit tcp thiết bị 10.1.1.1 172.16.5.0 0.0.0.255 eq www
- B. access-list 1951 permit ip thiết bị 10.1.1.1 172.16.5.0 0.0.0.255 eq www
- C. access-list 2523 permit tcp any eq www 172.16.5.0 0.0.0.255
- D. access-list 2523 permit tcp 172.16.5.0 0.0.0.255 eq www 172.16.5.0 0.0.0.255
- E. access-list 2523 permit tcp 172.16.5.0 0.0.0.255 eq www any

Câu 8: Trường nào sau đây có thể được so sánh với một tên IP ACL mở rộng nhưng không phải là một IP ACL mở rộng có đánh số

- Giao thức
- Địa chỉ IP nguồn
- Địa chỉ IP đích
- Byte TOS
- Không có câu trả lời nào đúng

Câu 9: Trong một router chạy IOS 12.3, một kỹ sư cần xóa dòng thứ hai trong ACL 101, bây giờ đã có bốn câu lệnh đã được cấu hình. Tham số nào sau đây có thể được sử dụng?

- Xóa toàn bộ ACL và cấu hình lại ba lệnh ACL còn lại trong ACL
- Xóa một dòng trong ACL sử dụng lệnh no access – list
- Xóa một dòng trong ACL bằng cách vào chế độ cấu hình ACL và sau đó xóa chỉ dòng thứ hai dựa trên số thứ tự của nó
- Xóa ba dòng cuối trong ACL trong chế độ cấu hình ACL, và sau đó thêm hai dòng lệnh cuối lại vào ACL

Câu 10: Hướng dẫn chung nào có thể cho phép khi đặt các IP ACL mở rộng?

- a. Thực hiện tất cả các lọc đầu vào nếu có thể
- b. Đặt các lệnh tổng quan hơn vào ACL
- c. Lọc các gói tin gần nguồn nhất có thể
- d. Sắp xếp các lệnh ACL dựa trên địa chỉ IP nguồn, từ thấp nhất đến cao nhất, để cài tiến khả năng thực thi

Câu 11: Công cụ nào sau đây yêu cầu người dùng cuối để telnet vào một router để lấy truy cập đến các máy tính ở bên kia router?

- a. ACL có tên
- b. ACL có liên quan
- c. ACL động
- d. ACL dựa theo thời gian

Chương 9

GIAO THỨC ĐỊNH TUYẾN

Các giao thức định tuyến xác định nhiều cách thức khác nhau mà router trao đổi thông tin với nhau để xác định con đường tốt nhất cho mỗi đích. Khi mạng phát triển phức tạp hơn qua thời gian, các router tiêu tốn nhiều xử lý trong RAM. Kết quả là, các giao thức định tuyến mới hơn được thiết kế, tận dụng các liên kết nhanh hơn và router nhanh hơn. Trong chương này bắt đầu với giới thiệu về các giao thức định tuyến. Sau đó lý thuyết về giao thức định tuyến *distance vector* và *link-state*.

9.1. TỔNG QUAN VỀ GIAO THỨC ĐỊNH TUYẾN ĐỘNG

Router thêm các con đường IP vào bảng định tuyến của nó sử dụng ba phương pháp: các con đường kết nối trực tiếp, các con đường tĩnh và các con đường được học từ các giao thức định tuyến động. Trước tiên, xem xét một số thuật ngữ liên quan đến giao thức định tuyến, giao thức được định tuyến và giao thức có thể định tuyến, như sau:

Giao thức định tuyến: Một tập hợp các thông điệp, và giải thuật được sử dụng bởi router để mục đích chung là học về các con đường. Tiến trình này bao gồm việc trao đổi và phân tích thông tin định tuyến. Mỗi router lựa chọn con đường tốt nhất đến mỗi mạng con (lựa chọn đường) và cuối cùng đặt những con đường tốt nhất này vào trong bảng định tuyến của nó. Ví dụ gồm có RIP, EIGRP, OSPF, BGP.

Giao thức được định tuyến và giao thức có thể định tuyến: Cả hai thuật ngữ này đề cập đến một giao thức xác định cấu trúc gói tin và địa chỉ luận lý, cho phép router có thể chuyển tiếp hay định tuyến các gói tin này đi. Router chuyển tiếp hay định tuyến các gói tin được xác định bởi các giao thức được định tuyến và có thể định tuyến. Ví dụ gồm có IP và IPX.

Dù rằng giao thức định tuyến (RIP) là khác với giao thức được định tuyến (IP), chúng lại làm việc cùng nhau. Tiến trình định tuyến chuyển tiếp các gói tin IP, nhưng nếu một router không có bắt kì con đường nào trong bảng định tuyến phù hợp với địa chỉ đích của gói tin, router hủy gói tin đi. Router cần giao thức định tuyến để router học tất cả các con đường có thể và thêm chúng vào bảng định tuyến để tiến trình định tuyến có thể chuyển tiếp (định tuyến) các giao thức định tuyến như là IP.

9.1.1. Chức năng giao thức định tuyến

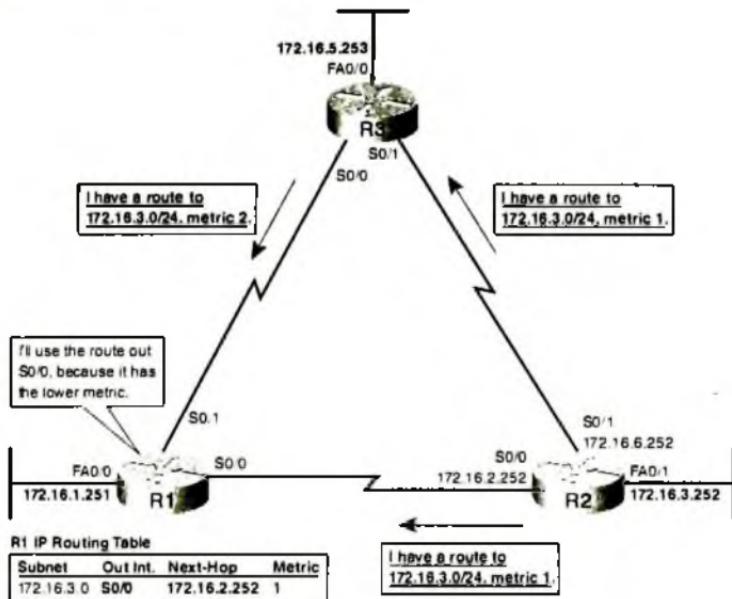
Phần mềm Cisco IOS hỗ trợ nhiều giao thức định tuyến IP, thực hiện cùng chức năng chung:

- Học thông tin định tuyến về các mạng con IP từ các router lân cận kề cận
- Quảng bá thông tin định tuyến về các mạng con IP đến các router kề cận khác.
- Nếu hơn một con đường tồn tại đến một mạng con, lấy con đường tốt nhất dựa vào trọng số.
- Nếu sơ đồ mạng thay đổi, ví dụ liên kết hỏng – tái kích hoạt bằng cách quảng bá rằng một số con đường đã lỗi, và lấy lại con đường tốt nhất hiện tại. Tiến trình này được gọi là hội tụ định tuyến.

Hình 9.1 cho thấy một ví dụ với ba trong bốn chức năng trong danh sách trên. Cả R1 và R3 học về một con đường đến mạng con 172.16.3.0/24 từ R2 (chức năng 1). Sau khi R3 học về con đường đến 172.16.3.0/24 từ R2, R3 quảng bá con đường đó đến R1 (chức năng 2). Sau đó R1 phải lựa chọn một con đường được học từ hai con đường trên để đến mạng con 172.16.3.0/24: một với trọng số 1 từ R2 và một với trọng số 2 từ R3. R1 chọn con đường có trọng số thấp hơn qua R2 (chức năng 3).

Hội tụ là chức năng thứ tư của giao thức định tuyến được xem xét. Thuật ngữ hội tụ đề cập đến tiến trình xảy ra khi sơ đồ mạng thay đổi, khi hoặc là một router hay một liên kết hỏng, hay khi nó hoạt động trở lại. Khi thay đổi xảy ra, con đường tốt nhất trên mạng có thể thay đổi. Hội tụ đơn giản đề cập đến tiến trình trong đó tất cả các router phân tích

để xác định điều gì đã xảy ra, quảng bá thông tin về những thay đổi cho tất cả các router khác, và tất cả các router khác đó sau đó chọn con đường tốt nhất hiện tại cho mỗi mạng con. Khả năng hội tụ nhanh, mà không gây ra vòng lặp, một trong những nhân tố quan trọng khi lựa chọn giao thức định tuyến IP nào được sử dụng.



Hình 9.1. Giao thức định tuyến

Trong hình 9.1, hội tụ có thể xảy ra nếu liên kết giữa R1 và R2 bị hỏng. Trong trường hợp đó, R1 có thể ngưng sử dụng con đường cũ của nó với mạng con 172.16.3.0/24 (trực tiếp qua R2), thay vì gửi gói tin đến R3.

9.1.2. Giao thức định tuyến nội và ngoại

Các giao thức định tuyến IP được chia làm hai loại chính: Giao thức định tuyến nội – Interior Gateway Protocols (IGP) hay giao thức định tuyến ngoại – Exterior Gateway Protocols (EGP). Định nghĩa cho mỗi giao thức như sau:

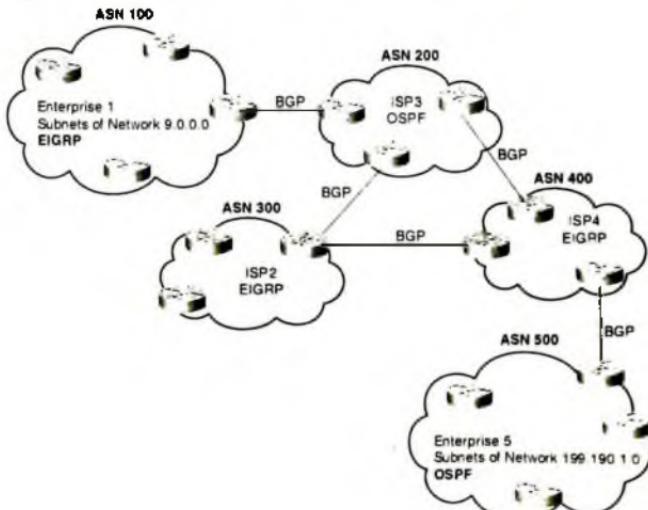
IGP: Giao thức định tuyến được thiết kế và nhằm mục đích sử dụng trong một hệ thống tự động (AS – autonomous system) đơn.

EGP: Giao thức định tuyến được thiết kế và nhằm mục đích sử dụng giữa các hệ thống tự động đơn khác nhau.

Hệ thống tự động (AS – autonomous system): là một mạng dưới sự kiểm soát của một tổ chức đơn. Ví dụ, một mạng được tạo và trả tiền bởi một công ty đơn có thể là một AS đơn, mạng của một chính phủ quốc gia cũng có thể là một AS đơn. Mỗi ISP cũng thường là một AS đơn.

Một số giao thức định tuyến hoạt động tốt bên trong một AS đơn theo thiết kế, vì thế những giao thức định tuyến này được gọi là IGP. Ngược lại, các giao thức định tuyến được thiết kế để trao đổi các con đường giữa các router trong nhiều AS khác nhau được gọi là EGP.

Mỗi AS có thể được gán một con số gọi là chi số AS. Giống như địa chỉ IP công cộng, ICANN đảm nhận việc gán ASN trên toàn cầu. Hình 9.2 cho thấy một hệ thống mạng Internet toàn cầu. Hình này cho thấy hai mạng và ba ISP sử dụng IGP (OSPF và EIGRP) bên trong mạng và BGP giữa các ASN.



Hình 9.2. Định tuyến giữa các ASN

9.1.3. So sánh các IGP

Ngày nay, không có nhiều lựa chọn cho EGP: chỉ đơn giản sử dụng BGP. Tuy nhiên, khi lựa chọn một IGP để sử dụng trong một tổ chức đơn, có nhiều lựa chọn hơn. Lựa chọn hợp lý nhất là RIP – 2, EIGRP và OSPF. Phần này tập trung giới thiệu một số điểm so sánh chính giữa các giao thức IGP, còn chi tiết sẽ được đề cập sau.

9.1.3.1. Giải thuật giao thức định tuyến IGP

Giải thuật bên dưới giao thức định tuyến xác định cách giao thức định tuyến thực hiện công việc của nó. Thuật ngữ giao thức định tuyến đề cập đến ý nghĩa và các tiến trình được sử dụng bởi các giao thức định tuyến khác nhau để giải quyết các vấn đề cho việc học các con đường, lựa chọn con đường tốt nhất cho mỗi mạng con và hội tụ khi phản ứng với những thay đổi trong mạng. Ba nhánh chính của giải thuật giao thức định tuyến trong giao thức IGP gồm:

- Distance Vector
- Link state
- Lai cân bằng (còn gọi là Distance vector cải tiến)

Theo lịch sử, các giao thức định tuyến distance vector được phát minh đầu tiên, chủ yếu vào đầu những năm 1980. RIP là giao thức nổi tiếng đầu tiên được sử dụng giao thức IP distance vector, với giao thức riêng của Cisco là Interior Gateway Routing Protocol IGRP được giới thiệu ít lâu sau. Vào những năm đầu 1990, các giao thức định tuyến distance vector hội tụ chậm và có nguy cơ bị lặp. Chính vì thế, giao thức định tuyến mới hơn được ra đời, sử dụng giải thuật mới. Giao thức định tuyến link – state, cụ thể là OSPF và Integrated IS – IS, giải quyết những tồn động chính của giao thức định tuyến distance vector, nhưng chúng yêu cầu thời gian để hoạch định nhiều hơn với những mạng kích thước từ trung bình đến lớn.

Cùng thời gian xuất hiện OSPF, Cisco tạo một giao thức định tuyến riêng có tên là Enhanced Interior Gateway Routing Protocol EIGRP, sử dụng một số đặc tính của giao thức IGRP trước đó. EIGRP giải quyết cùng vấn đề mà link state đã thực hiện, nhưng yêu cầu hoạch định ít hơn khi triển khai trên mạng. Thời gian qua đi, EIGRP được phân làm loại giao thức định tuyến duy nhất, không thuộc distance vector cũng như link state – vì thế EIGRP được gọi là giao thức lai cân bằng hay giao thức distance vector cải tiến.

Những phần tiếp theo trong chương sẽ đề cập chi tiết về giao thức distance vector và link state cũng như EIGRP.

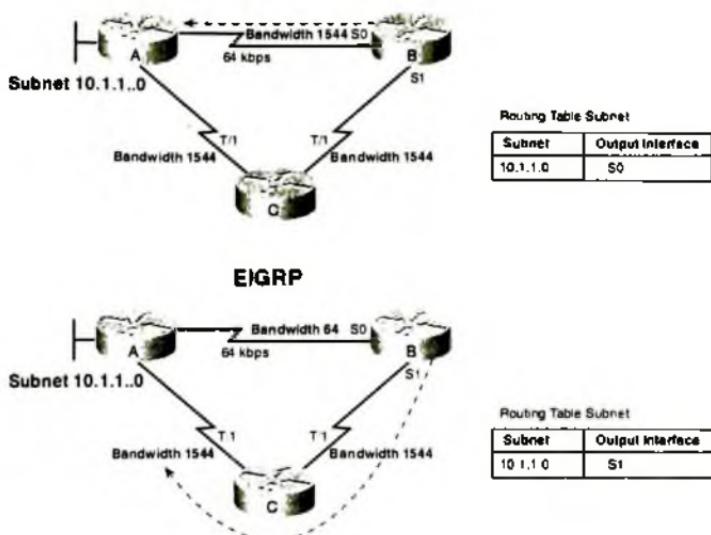
9.1.3.2. Trọng số

Các giao thức định tuyến chọn con đường tốt nhất để đến một mạng con bằng cách lựa chọn con đường với trọng số thấp nhất. Ví dụ, RIP sử dụng bộ đếm số router giữa một router và mạng con đích. Bảng sau đây liệt kê các giao thức định tuyến quan trọng nhất và một số chi tiết về trọng số trong mỗi trường hợp.

Bảng 9.1. Trọng số của các giao thức định tuyến

IGP	Trọng số	Mô tả
RIP – 1, RIP – 2	Số chặng	Số router (số chặng) giữa một router và mạng con đích
OSPF	Chi phí	Tổng tất cả các thiết lập chi phí cho tất cả các liên kết trên một con đường, với chi phí mặc định được dựa trên băng thông giao tiếp
EIGRP	Kết hợp băng thông và độ trễ	Được tính toán dựa trên thời gian chờ nhất của con đường và độ trì hoãn ước lượng liên quan đến mỗi giao tiếp trên con đường đó

Không như RIP – 1 hay RIP – 2, cả trọng số OSPF và EIGRP bị ảnh hưởng bởi nhiều sự thiết lập băng thông giao tiếp. Hình 9.3 so sánh ảnh hưởng của các trọng số được sử dụng bởi RIP và EIGRP.



Hình 9.3. Trọng số định tuyến

Như thể hiện trong phần đầu của hình, con đường RIP của router B đến 10.1.1.0 chỉ đến router A bởi vì con đường đó có số chặng thấp hơn (1) so với con đường qua router C (2). Tuy nhiên, trong phần dưới của hình 9.3, Router B chọn con đường qua hai chặng qua Router C khi sử dụng EIGRP vì băng thông của hai liên kết trong con đường là nhanh hơn (tốt hơn) so với con đường một chặng. Chú ý rằng để EIGRP lựa chọn đúng đường, cần cấu hình chính xác băng thông giao tiếp phù hợp với tốc độ thực sự, để EIGRP có thể chọn con đường nhanh hơn. (Lệnh giao tiếp bandwidth không ảnh hưởng đến tốc độ vật lý thực sự trên giao tiếp. Nó chỉ báo cho IOS biết tốc độ giả sử dụng mà giao tiếp đang sử dụng).

9.1.3.3. Tóm tắt so sánh các IGP

Bảng sau đây liệt kê nhiều đặc tính được hỗ trợ bởi nhiều IGP khác nhau. Bảng này chứa các mục được đề cập một cách chi tiết trong chương này.

Bảng 9.2. *Chức năng của một số giao thức định tuyến*

Chức năng	RIP1	RIP2	EIGRP	OSPF	IS-IS
Classless – định tuyến không phân lớp	No	Yes	Yes	Yes	Yes
Hỗ trợ VLSM	No	Yes	Yes	Yes	Yes
Gửi-mail nạp trong cập nhật	No	Yes	Yes	Yes	Yes
Vector Khoảng cách	Yes	Yes	No	No	No
Link – State	No	No	No	Yes	Yes
Hỗ trợ tự động gộp đường	No	Yes	Yes	No	No
Hỗ trợ gộp đường thủ công	No	Yes	Yes	Yes	Yes
Các cập nhật quảng bá được gửi đến một địa chỉ quảng bá nhóm	No	Yes	Yes	Yes	-
Hỗ trợ xác thực	No	Yes	Yes	Yes	Yes
Hội tụ	Chậm	Chậm	Rất Nhanh	Nhanh	Nhanh

Bảng 9.3. đây liệt kê nhiều chủ đề khác về RIP – 2, OSPF, và EIGRP. Các chủ đề trong bảng được giải thích đầy đủ hơn trong phần sau.

Bảng 9.3. *Đặc tính của một số giao thức định tuyến*

Chức năng	RIP – 2	OSPF	EIGRP
Trọng số	Số chẵng	Chi phí liên kết	Kết hợp băng thông và độ trì hoàn
Gửi cập nhật chu kỳ	Yes (30 giây)	No	No
Cập nhật định tuyến một phần hay đầy đủ	Full	Partial	Partial
Các cập nhật được gửi tại	(224.0.0.9)	(224.0.0.5,224.0.0.6)	(224.0.0.10)
Trọng số được xem là vô hạn	16	(224-1)	(232-1)
Hỗ trợ cân bằng tải trên các con đường chi phí không bằng	No	No	Yes

9.1.3.4. Khoảng cách quản trị

Nhiều công ty và tổ chức sử dụng một giao thức định tuyến đơn. Tuy nhiên, trong một số trường hợp, một công ty cần sử dụng nhiều giao thức định tuyến. Ví dụ, nếu hai công ty kết nối mạng của họ để trao đổi một số thông tin định tuyến. Nếu một công ty sử dụng RIP và một số khác sử dụng EIGRP, ít nhất trên router, cả RIP và EIGRP phải được sử dụng. Sau đó router này có thể lấy các con đường đã được học bằng RIP và quảng bá nó sang EIGRP, và ngược lại, thông qua tiến trình gọi là tái phân phối con đường.

Tùy theo sơ đồ mạng, hai giao thức định tuyến có thể học các con đường đến cùng mạng con. Khi một giao thức định tuyến đơn học nhiều con đường đến cùng một mạng con, trọng số báo cho nó biết con đường nào là tốt nhất, tuy nhiên, khi hai giao thức định tuyến khác nhau học các con đường đến một mạng đơn, vì trọng số mỗi giao thức định tuyến dựa trên thông tin khác nhau, IOS không thể so sánh nó. Ví dụ, RIP có thể học một con đường đến mạng con 10.1.1.0 với trọng số 1, và EIGRP có thể học một con đường đến 10.1.1.0 với trọng số 2.192.416, nhưng EIGRP có thể là con đường tốt hơn, hoặc không. Đơn giản là không có cơ sở nào để so sánh giữa hai trọng số đó.

Khi IOS phải lựa chọn giữa hai con đường học được sử dụng các giao thức định tuyến khác nhau, IOS sử dụng khái niệm là khoảng cách quản trị (administrative distance). Khoảng cách quản trị là số cho biết khả năng tin cậy về giao thức định tuyến trên một router đơn. Số càng thấp thì càng thấp hay càng đáng tin. Ví dụ, RIP có khoảng cách quản trị là 120, và EIGRP là 90, nên EIGRP đáng tin hơn RIP. Vì thế khi cả hai giao thức định tuyến học các con đường về cùng mạng con, router chỉ thêm con đường EIGRP vào bảng định tuyến đó. Giá trị khoảng cách quản trị được cấu hình trên một router và không thể trao đổi với router khác. Bảng sau liệt kê các thông tin định tuyến khác nhau và khoảng cách quản trị mặc định

Bảng 9.4. Khoảng cách quản trị của một số giao thức định tuyến

Loại con đường	Khoảng cách quản trị
Kết nối	0
Tĩnh	1
BGP (con đường ngoại mạng)	20
EIGRP (con đường nội mạng)	90
IGRP	100
OSPF	110
IS – IS	115
RIP	120
EIGRP (con đường ngoại mạng)	170
BGP (con đường nội mạng)	200
Không dùng	255

Bảng trên cho thấy các giá trị khoảng cách quản trị mặc định, nhưng IOS có thể được cấu hình để thay đổi khoảng cách quản trị cho một giao thức định tuyến cụ thể, một con đường cụ thể hay thậm chí là một con đường tĩnh. Ví dụ, lệnh `ip route 10.1.3.0 255.255.255.0 10.1.130.253` xác định một con đường tĩnh với khoảng cách quản trị là 1, nhưng với lệnh `ip route 10.1.3.0 255.255.255.0 10.1.130.253 210` xác định cùng một con đường tĩnh với khoảng cách quản trị là 210.

9.2. GIAO THỨC ĐỊNH TUYẾN DISTANCE VECTOR

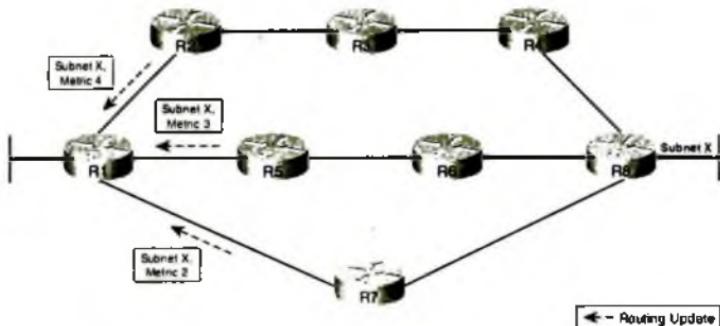
Phần này tập trung vào cơ sở cho giao thức định tuyến distance vector, sử dụng RIP như một ví dụ. Phần này bắt đầu bằng việc kiểm tra hoạt động thông thường của giao thức distance vector, sau đó là giải thích về chức năng chống lặp.

9.2.1. Khái niệm

Thuật ngữ *distance vector* mô tả những gì router biết về mỗi con đường. Tại cuối của tiến trình, khi một router họ về một con đường đến mạng con, tất cả những gì router biết là độ đo khoảng cách (trọng số) và router chặng kế vào giao tiếp đầu ra được sử dụng cho con đường đó (mô vector, hay hướng). Để cho thấy chính xác hơn những gì mà một giao thức

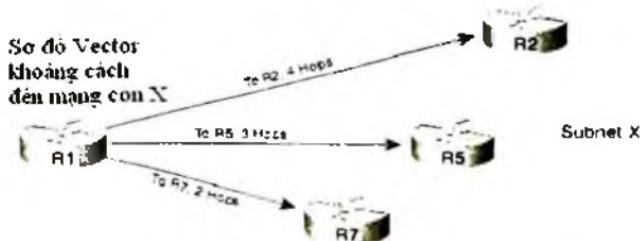
định tuyến distance vector thực hiện, hình 9.4 thể hiện những gì một router học với một giao thức định tuyến distance vector. Hình cho thấy một mạng trong đó router R1 học về ba con đường đến mạng con X:

- Con đường bốn chặng qua R2
- Con đường ba chặng qua R5
- Con đường hai chặng qua R7



Hình 9.4. Cập nhật trọng số định tuyến

R1 học về mạng con và trọng số có liên quan đến mạng con đó, và không gì khác. R1 phải lấy con đường tốt nhất để đến mạng con X. Trong trường hợp này, nó lấy con đường hai chặng qua R7, vì con đường đó có trọng số thấp nhất. Để xem xét kĩ hơn ý nghĩa của thuật ngữ vector khoảng cách (distance vector), xem xét hình 9.5, thể hiện những gì R1 biết về mạng con X trong hình trên.

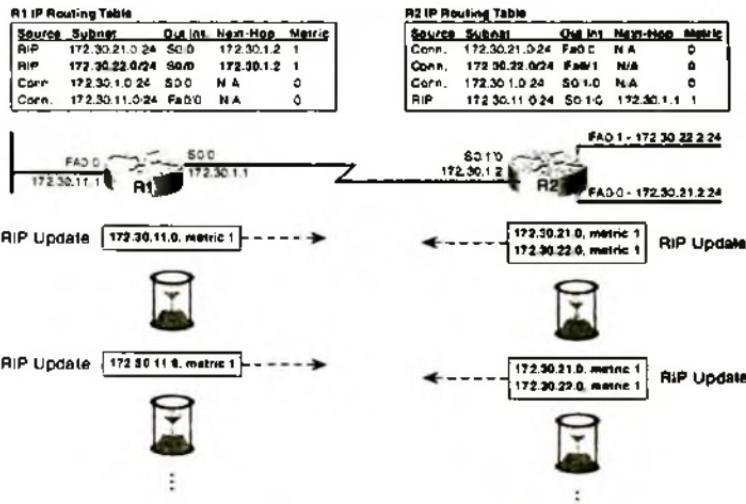


Hình 9.5. Định tuyến Distance Vector

Tất cả những gì R1 biết về mạng con X là ba vector. Chiều dài của vector là trọng số, mô tả con đường đó tốt hay xấu. Hướng của vector thể hiện router chặng kế tiếp. Vì thế, với ý nghĩa khoảng cách quản trị, giao thức định tuyến không học nhiều về mạng khi chúng nhận các cập nhật định tuyến. Tất cả những gì mà giao thức định tuyến biết là một khái niệm về vector: chiều dài vector là khoảng cách (trọng số) đến mạng con, và hướng vector là thông qua router lân cận quảng bá về con đường.

9.2.2. Hoạt động của distance vector trong mạng ổn định

Giao thức định tuyến distance vector gửi các cập nhật định tuyến theo chu kỳ. Hình 9.6 mô tả khái niệm này trong một mạng với hai router, ba mạng con LAN và một mạng con WAN. Hình này thể hiện cả hai bảng cập nhật định tuyến đầy đủ, liệt kê tất cả bốn con đường, và cập nhật đầy đủ định kì được gửi bởi mỗi router.



Hình 9.6. Hoạt động của giao thức Distance Vector

Để hiểu đầy đủ hơn hoạt động distance vector trong hình này, tập trung vào một số yếu tố quan trọng hơn về những gì một router học cho mạng con 172.30.22.0/24, là mạng con có kết nối đến giao tiếp Fa0/1 của R2.

1. R2 xem bàn thân nó có một con đường số chặng là 0 đến mạng con 172.30.22.0/24, vì thế trong cập nhật định tuyến được gửi bởi R2, R2 quảng bá một con đường có trọng số là 1 (số chặng là 1).
2. R1 nhận được cập nhật RIP từ R2, và vì R1 chưa học được con đường nào đến mạng 172.30.22.0/24, con đường này là con đường tốt nhất của R1 đến mạng con đó.
3. R1 thêm mạng con này vào bảng định tuyến của nó, xem nó như là một con đường được học bằng RIP.
4. Với con đường đã học, R1 sử dụng giao tiếp ra S0/0, vì R1 nhận cập nhật định tuyến của R2 trên giao tiếp S0/0 của R1.
5. Với con đường đã học, R1 sử dụng một router chặng kế là 172.30.1.2 vì R1 đã học con đường này từ cập nhật RIP từ địa chỉ IP là 172.30.1.2

Tại cuối của tiến trình này, R1 đã được học một con đường mới. Phần còn lại của RIP học các con đường trong ví dụ này với cùng tiến trình như trên.

Bên cạnh việc học và quảng bá các con đường, một số yếu tố quan trọng cụ thể khác về giao thức distance vector như sau:

- Tính chu kỳ: RIP mặc định gửi các cập nhật định kỳ 30 giây mỗi lần theo mặc định
- Cập nhật đầy đủ: Router gửi các cập nhật đầy đủ mỗi lần thay vì chỉ gửi các cập nhật mới hay thông tin định tuyến đã thay đổi
- Cập nhật đầy đủ bị giới hạn bởi quy tắc phân tách miền: Giao thức định tuyến giới hạn một số con đường khỏi việc cập nhật đầy đủ theo quy tắc phân tách miền. Miền phân tách là chức năng chống vòng lặp được xem xét sau

9.2.3. Ngăn vòng lặp Distance Vector

Như đã đề cập, tiến trình distance vector thực sự khá đơn giản. Nhưng không may là, điều này lại dẫn đến khả năng vòng lặp định tuyến. Vòng lặp định tuyến xảy ra khi router chuyển tiếp các gói tin trên cùng

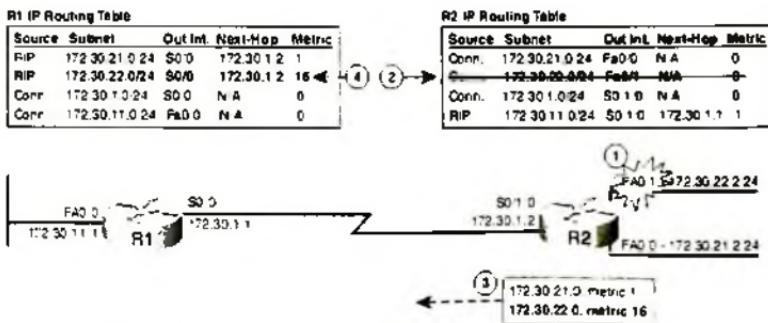
một con đường lặp đi lặp lại, làm tiêu tốn băng thông và không bao giờ chuyển tiếp gói tin đi được. Trong mạng thực tế, số lượng gói tin vòng lặp có thể làm cho mạng tắc nghẽn đến mức không thể sử dụng được, vì thế lặp định tuyến phải được tránh đến mức có thể. Phần còn lại sẽ khảo sát giao thức distance vector với chức năng ngăn vòng lặp.

9.2.3.1. Con đường bị lỗi

Khi một con đường bị lỗi, giao thức định tuyến distance vector gây nên vòng lặp định tuyến cho đến khi mọi router trên mạng tin và biết rằng con đường ban đầu đó đã lỗi. Kết quả là, giao thức distance vector cần một cách thức để xác định cụ thể con đường nào đã bị lỗi.

Các giao thức distance vector truyền thông tin về một con đường lỗi bằng cách đánh dấu con đường đó. Đánh dấu con đường tức là quảng bá con đường, nhưng với một giá trị trọng số đặc biệt được gọi là vô hạn. Bằng cách đơn giản đặt con đường trọng số vô hạn, router xem con đường đó đã bị lỗi. Chú ý rằng mỗi giao thức distance vector sử dụng khái niệm giá trị trọng số thực sự biểu diễn cho giá trị vô hạn. RIP xem giá trị vô hạn là 16.

Hình sau đây cho một ví dụ về đánh dấu con đường với RIP, với giao tiếp Fa0/1 của R2 bị lỗi, nghĩa là con đường của R2 đến 172.30.22.0/24 đã lỗi.



Hình 9.7. Con đường đánh dấu trong Distance Vector

Tiến trình như sau:

- Giao tiếp Fa0/1 của R2 lỗi
- R2 gỡ bỏ con đường kết nối của nó cho 172.30.22.0/24 ra khỏi bảng định tuyến
- R2 quảng bá 172.30.22.0 với trọng số vô hạn, đối với RIP là 16.
- R1 giữ con đường này trong bảng định tuyến của nó, với một trọng số vô hạn, cho đến khi nó gỡ bỏ con đường đó ra khỏi bảng định tuyến.

Bất kì giá trị trọng số nào dưới vô hạn có thể được sử dụng như là giá trị trọng số hợp lệ cho một con đường hợp lệ. Với RIP, điều này có nghĩa là một con đường 15 chặng sẽ là một con đường hợp lệ. Một số mạng lớn trên thế giới có ít nhất bốn hay năm router trên con đường dài nhất giữa hai mạng con. Vì thế, trọng số tối đa hợp lệ 15 chặng là đủ.

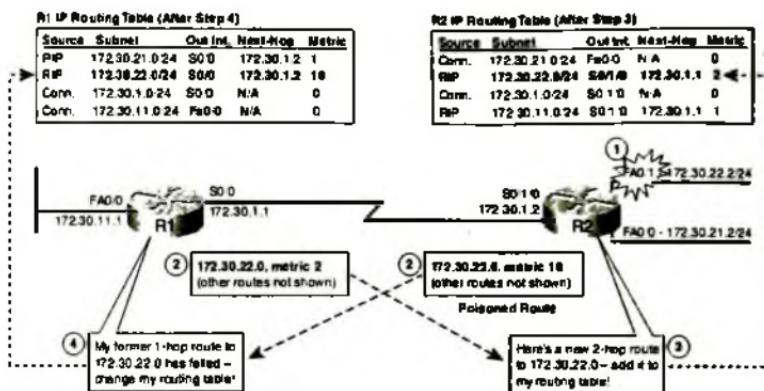
9.2.3.2. Lỗi giá trị vô hạn qua liên kết đơn

Giao thức định tuyến distance vector có thể gây ra lỗi vòng lặp định tuyến trong thời gian khi router đầu tiên nhận ra một con đường bị lỗi cho đến khi tất cả router biết con đường đó đã bị lỗi. Nếu không có cơ chế ngăn lỗi vòng lặp định tuyến được giải thích trong phần này, giao thức định tuyến distance vector có thể gặp vấn đề được gọi là đếm đến vô hạn. Dĩ nhiên, router có thể không bao giờ đếm đến vô hạn theo lý thuyết, nhưng chúng có thể đếm đến vô hạn, ví dụ với RIP là 16.

Đếm đến vô hạn gây ra hai vấn đề có liên quan. Nhiều chức năng ngăn lặp distance vector tập trung vào ngăn ngừa những vấn đề sau:

- Các gói tin có thể lặp quanh một mạng trong khi router đếm đến vô hạn, với bảng thông tin tiêu tồn vì các gói tin lặp quan trọng đó.
- Tiến trình đếm đến vô hạn có thể tồn nhiều thời gian, nghĩa là vòng lặp có thể làm cho người dùng tin rằng mạng đã lỗi.

Hình 9.8. cho thấy một ví dụ về lỗi đếm đến vô hạn

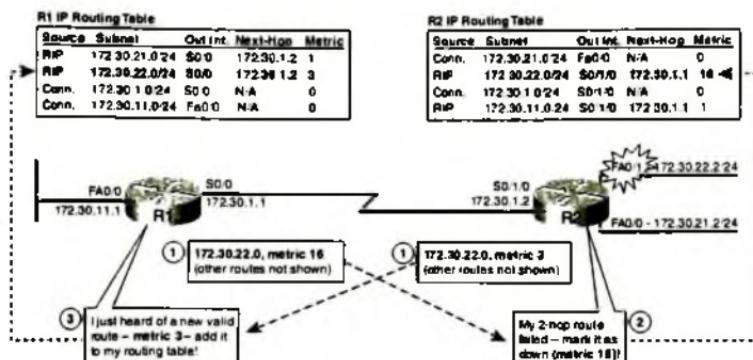


Hình 9.8. *Lỗi đếm đến vô hạn của Distance Vector*

Điểm chính trong ví dụ được biết rằng cập nhật định kì của R1 đến R2 (từ trái qua phải) xảy ra trong hầu hết cùng một thời điểm vì các quảng bá đánh dấu của R2 đến R1. Tiến trình như sau:

1. Giao tiếp Fa0/1 của R2 lỗi, vì thế R2 gỡ bỏ con đường có kết nối 172.30.22.0/24 của nó khỏi bảng định tuyến.
2. R2 gửi một bản tin quảng bá đánh dấu (trọng số 16 với RIP) đến R1, nhưng cùng lúc, thời gian cập nhật định kì của R1 hết hạn, vì thế nó gửi đi một cập nhật thông thường của nó, bao gồm một quảng bá về 172.30.22.0/24, trọng số 2.
3. R2 nhận được con đường 172.30.22.0 có trọng số là 2 từ R1. Vì R2 không còn con đường cho mạng con 172.30.22.0, vì thế nó thêm con đường trọng số 2 đó vào bảng định tuyến, router chặng kế là R1.
4. Cùng thời điểm 3, R1 nhận được cập nhật từ R2, báo R1 rằng con đường cũ đến 172.30.22.0 qua R2 đã lỗi. Kết quả là R1 thay đổi bảng định tuyến của nó thành 16 cho con đường 172.30.22.0.

Tại thời điểm này, R1 và R2 chuyển tiếp các gói tin hướng đến 172.30.22.0/24 tới và lui cho nhau. R2 có một con đường đến 172.30.22.0/24, hướng đến R1 và R1 cũng ngược lại. Vòng lặp xảy ra cho đến khi cả hai, R1 và R2 đếm đến vô hạn.



Hình 9.9. Lỗi đếm đến vô hạn trong Distance Vector (tiếp theo)

Hình trên cho thấy cập nhật định kỳ kế tiếp của hai router, như sau:

- Cả hai bộ định thời cập nhật của R1 và R2 hết hạn cùng lúc, R1 gửi một con đường đánh dấu (trọng số 16), và R2 gửi một con đường trọng số 3.
- R2 nhận cập nhật của R1, vì thế R2 thay đổi con đường của nó đến 172.30.22.0 sang giá trị trọng số 16.
- Cùng thời điểm bước 2, R1 nhận cập nhật của R2, vì thế R1 thay đổi con đường của nó đến 172.30.22.0 sang trọng số là 3.

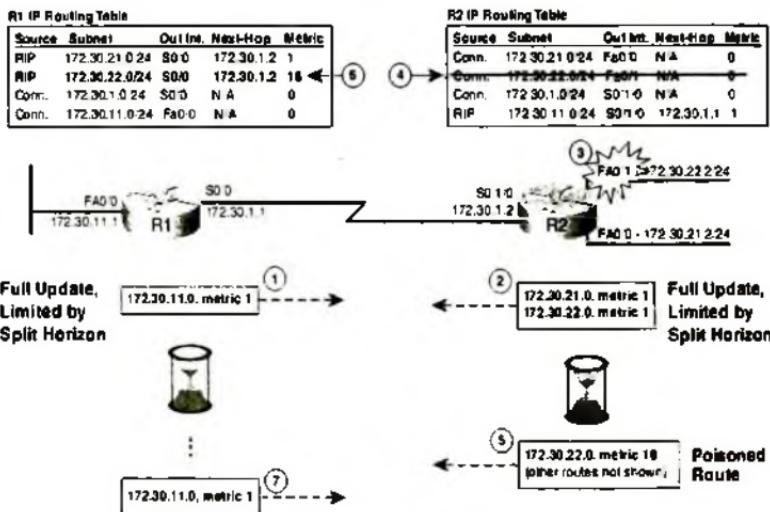
Tiến trình tiếp tục cho đến khi cả hai router đạt đến trọng số 16. Lúc này, router có thể hết hạn với con đường đó và gỡ bỏ nó ra khỏi bảng định tuyến.

9.2.3.3. Miền phân tách – split horizon

Trong ví dụ thể hiện ở hai hình trên, Router R2 có một con đường kết nối đến 172.30.22.0, và R1 học con đường đó vì một cập nhật định tuyến được gửi bởi R2. Tuy nhiên, không cần thiết cho R1 để quảng bá lại cùng một con đường đến R2, vì R1 đã học con đường đó từ R2. Vì thế, một cách để ngăn lỗi đếm đến vô hạn là để R1 không quảng bá mạng con 172.30.22.0, sử dụng chức năng miền phân tách (split horizon). Miền phân tách được định nghĩa như sau:

“Trong cập nhật định tuyến được gửi ra ngoài giao tiếp X, không chứa thông tin định tuyến về các con đường xem giao tiếp X đó như là giao tiếp đầu ra”.

Miền phân tách nghĩa là khi router R1 nhận một con đường từ R2, R1 không cần quảng bá con đường đó ngược lại R2. Hình 9.10 cho thấy hiệu quả của miền phân tách trên các router R1 và R2 trên cùng một mạng. Bảng định tuyến của R1 liệt kê bốn con đường, ba trong số chúng xem giao tiếp S0/0 của R1 là giao tiếp đầu ra. Vì thế miền phân tách ngăn R1 không chứa những con đường này trong bảng định tuyến được gửi bởi R1 ra ngoài giao tiếp S0/0 của nó.



Hình 9.10 Miền phân tách

Các bước trong tiến trình như sau:

1. R1 gửi cập nhật đầy đủ định kỳ thông thường của nó, vì quy tắc miền phân tách, nó chỉ chứa một con đường.
2. R2 gửi cập nhật đầy đủ định kỳ của nó, chứa chỉ hai con đường.

3. Giao tiếp Fa0/1 của R2 lỗi
4. R2 gỡ bỏ con đường kết nối của 172.30.22.0/24 khỏi bảng định tuyến
5. R2 quảng bá 172.30.22.0 với trọng số vô hạn, RIP là 16
6. R1 tạm thời giữ con đường 172.30.22.0 trong bảng định tuyến, gỡ bỏ con đường đó khỏi bảng định tuyến sau
7. Trong cập nhật thông thường kế tiếp, R1, theo quy tắc miền phân tách, vẫn không quảng bá con đường cho 172.30.22.0

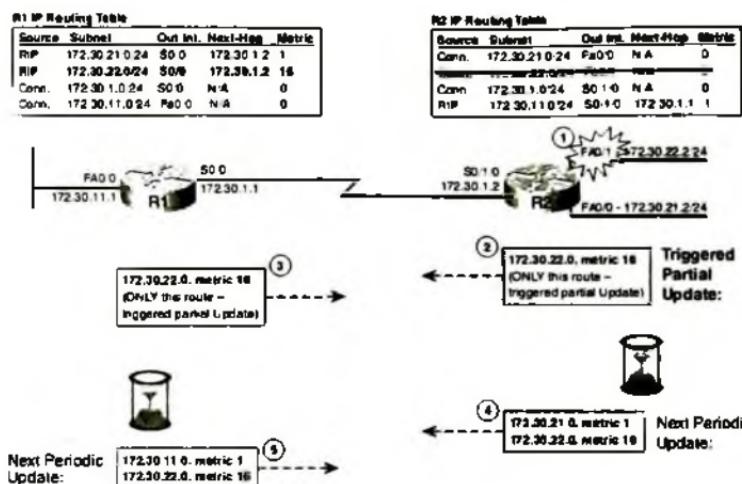
Miền phân tách ngăn lỗi đếm vô hạn vì R1 không quảng bá 172.30.22.0 sang R2. Kết quả là, R2 không bao giờ nhận một con đường khác về 172.30.22.0. Cisco IOS mặc định sử dụng miền phân tách trên hầu hết các giao tiếp.

9.2.3.4. Đánh dấu ngược (poison reverse) và theo dõi cập nhật (triggered update)

Giao thức distance vector có thể giải quyết lỗi đếm đến vô hạn bằng cách đảm bảo rằng mọi router học được con đường đã lỗi, thông qua mọi phương tiện có thể, càng nhanh càng tốt. Chứa năng ngăn lặp kế tiếp được xác định như sau:

- Theo dõi cập nhật: Khi con đường lỗi, không đợi cập nhật định kì kế tiếp. Thay vào đó, gửi một cập nhật theo dõi tức thì đến liệt kê con đường đánh dấu
- Đánh dấu ngược: Khi học được con đường lỗi, sử dụng quy tắc miền phân tách cho con đường đó và quảng bá con đường đánh dấu.

Hình 9.11 cho thấy một ví dụ về một trong các chức năng này, với giao tiếp Fa0/1 của R2 lại bị lỗi. Chú ý rằng hình này bắt đầu với tất cả giao tiếp đang làm việc, và tất cả con đường đều xác định.



Hình 9.11. Cập nhật con đường trong miền phân tách

Tiến trình như sau:

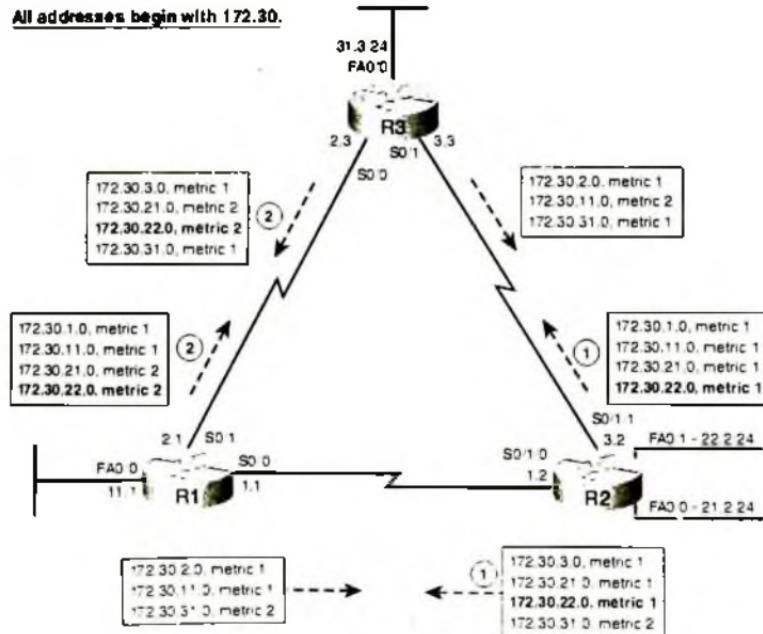
1. Giao tiếp Fa0/1 của R2 bị lỗi
2. R2 ngay tức thì gửi một cập nhật một phần có theo dõi với chỉ thông tin đã thay đổi – trong trường hợp này, là con đường đánh dấu cho 172.30.22.0
3. R1 phản hồi bằng cách thay đổi bảng định tuyến và gửi ngược một cập nhật một phần có theo dõi tức thì, với giá trị 172.30.22.0 với trọng số vô hạn. Đây là một con đường đánh dấu ngược.
4. Trong cập nhật định kì kế tiếp của R2, R2 quảng bá tất cả các con đường thông thường, bao gồm con đường đánh dấu cho 172.30.22.0, một lần.
5. Trên cập nhật định kì kế tiếp trên R1, R1 quảng bá tất cả các con đường chung, kể cả con đường đánh dấu ngược của 172.30.22.0, một lần.

Trong ví dụ này, R2 phản ứng tức thì bằng cách gửi một cập nhật theo dõi. R1 cũng phản ứng tức thì, sử dụng quy tắc miền phân tách cho

con đường lỗi và gửi một con đường đánh dấu ngược. Thực ra, con đường đánh dấu của R2 không được xem như là con đường đánh dấu ngược, vì R2 đã thực sự quảng bá con đường 172.30.22.0. Tuy nhiên, con đường đánh dấu của R1 là con đường đánh dấu ngược bởi vì nó được quảng bá ngược lại cho router từ R1 đã học được con đường lỗi đó.

9.2.3.5. Lỗi vô hạn trên con đường dự phòng

Miền phân tách ngăn lỗi đếm đến vô hạn xảy ra giữa hai router. Tuy nhiên, trên các con đường dự phòng trong một mạng, thường được sử dụng trong hầu hết các mạng ngày nay, miền phân tách một mình không ngăn ngừa được lỗi đếm đến vô hạn. Để xem xét, hình sau đây cho thấy một mạng mới đang làm việc trong chế độ thông thường, ổn định.

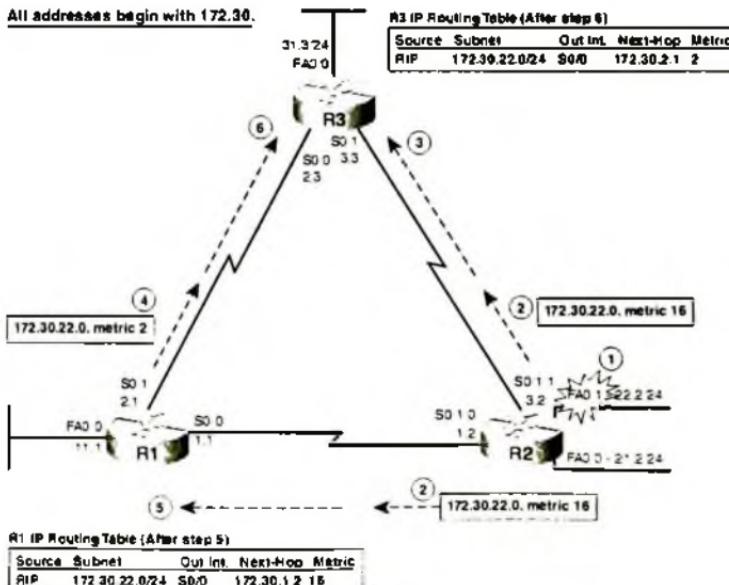


Hình 9.12. Lỗi cập nhật vô hạn

Bên cạnh việc cho thấy hoạt động thông thường như mạng khác, hình 9.12 cho một ví dụ về cách miền phân tách làm việc. Một lần nữa sử dụng mạng con 172.30.22.0 làm ví dụ, tiến trình sau xảy ra trong mạng:

- R2 quảng bá một con đường trọng số 1 trong cập nhật của nó đến cả R1 và R2.
- R1 sau đó quảng bá một con đường trọng số 2 cho mạng 172.30.22.0 cho R3, và R3 quảng bá một con đường trọng số 2 cho mạng 172.30.22.0 đến R2.
- Cả R1 và R3 thêm con đường trọng số 1, được học trực tiếp từ R2, vào bảng định tuyến của nó, và bỏ qua con đường hai chặng chúng học được từ nhau. Ví dụ, R1 đặt con đường 172.30.22.0, sử dụng giao tiếp đầu ra S0/0, router chặng kế 172.30.1.2 (R1) trong bảng định tuyến.

Xem xét tiếp hình 9.13 với giao tiếp Fa0/1 của R2 bị lỗi.



Hình 9.13. Lỗi cập nhật vô hạn (tiếp theo)

Các bước của tiến trình được thể hiện như sau:

1. Giao tiếp Fa0/1 của R2 bị lỗi.
2. R2 ngay tức thì gửi cập nhật một phần có theo dõi, đánh dấu con đường 172.30.22.0. R2 gửi cập nhật đó ra ngoài tất cả các giao tiếp còn làm việc.
3. R3 nhận cập nhật đã theo dõi của R2 có đánh dấu con đường 172.30.22.0, vì thế R3 cập nhật bảng định tuyến của nó thành trọng số 16 cho con đường này.
4. Trước khi cập nhật được mô tả trong bước 2 đến R1, R1 gửi cập nhật định kì thông thường của nó đến R3, lấy 172.30.22.0, trọng số 2 như bình thường.
5. R1 nhận cập nhật đã theo dõi của R2 đánh dấu con đường 172.30.22.0, vì thế R1 cập nhật bảng định tuyến cho con đường này trọng số là 16.
6. R3 nhận cập nhật định kì được gửi bởi R1, lấy giá trị trọng số 2 cho 172.30.22.0. Kết quả là, R3 cập nhật bảng định tuyến của nó với giá trị trọng số là 2 cho con đường này, thông qua R1 là router chặng kế, với giao tiếp ra là S0/0.

Lúc này, R3 có một con đường sai trọng số là 2 cho 172.30.22.0, trả ngược lại R1. Tùy thuộc vào thời gian khi giá trị này vào và ra khỏi bảng định tuyến, router có thể kết thúc việc chuyển tiếp các gói tin được gửi đến mạng con 172.30.22.0/24 qua mạng đó, có thể lặp một số gói tin trên mạng nhiều lần, trong khi tiến trình đếm đến vô hạn tiếp tục.

9.2.3.6. Tiến trình Holddown và Bộ định thời Holddown

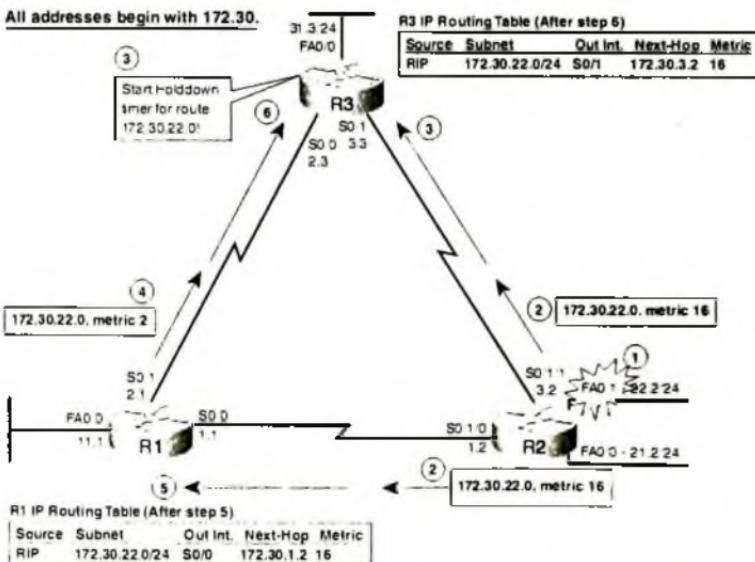
Chức năng ngăn vòng lặp cuối cùng được xem xét trong chương này, một tiến trình được gọi là holddown, ngăn vòng lặp và lỗi đếm đến vô hạn được thể hiện trong hình vẽ sau. Giao thức distance vector sử dụng bộ định thời holddown để ngăn vòng lặp được tạo ra bởi lỗi đếm đến vô hạn xảy ra trên một mạng dự phòng. Thuật ngữ holddown có ý nghĩa như sau:

“Ngay khi con đường được xem là tắt, giữ nó tắt một lúc để cho router thời gian để đảm bảo mọi router biết rằng con đường đó đã lỗi”.

Tiến trình holddown báo cho router biết để bỏ qua các thông tin mới về con đường đã lỗi, trong một khoảng thời gian được gọi là thời gian holddown, hay gọi là bộ định thời holddown. Tiến trình đó tóm tắt như sau:

“Sau khi nhận được một con đường đánh dấu, khởi động bộ định thời holddown cho con đường đó. Cho đến khi bộ định thời hết hạn, không tin vào bắt kè thông tin định tuyến nào về con đường đã lỗi, vì lảng nghe nó có thể gây ra vòng lặp. Tuy nhiên, thông tin được học từ các lân cận được quảng bá từ con đường hoạt động có thể tin tưởng trước khi bộ định thời holddown hết hạn”.

Để hiểu rõ hơn, xem xét ví dụ sau đây. Hình 9.14 cho thấy một ví dụ giống ví dụ trên, nhưng với tiến trình holddown ngăn lỗi đếm đến vô hạn. Hình này cho thấy các R3 bỏ qua bắt kè thông tin mới về mạng con 172.30.22.0 vì holddown. Như thông thường, ví dụ bắt đầu với tất cả giao tiếp bắt và làm việc, và tất cả con đường đều biết, và bước 1 bắt đầu với lỗi trên cùng giao tiếp của router R2.



Hình 9.14. Tiến trình Holddown và bộ định thời Holddown

Tiến trình diễn ra như sau, với các bước từ 3 – 6 khác với ví dụ trước.

1. Giao tiếp Fa0/1 của R2 lỗi
2. R2 ngay tức thì gửi cập nhật một phần có theo dõi, đánh dấu con đường 172.30.22.0. R2 gửi cập nhật ra ngoài tất cả các giao tiếp còn làm việc
3. R3 nhận cập nhật có theo dõi của R2 có đánh dấu con đường 172.30.22.0, vì thế R3 cập nhật bằng định tuyến của nó với giá trị 16 cho con đường. R3 cũng đặt con đường 173.30.22.0 holddown và bắt đầu bộ định thời holddown cho con đường đó, mặc định là 180 giây cho RIP
4. Trước khi cập nhật như đã mô tả ở bước 2 đến R1, R1 gửi cập nhật định kì thông thường của nó đến R3, đặt 172.30.22.0 có trọng số là 2, như thông thường
5. R1 nhận cập nhật có theo dõi của R2 (như mô tả trong bước 2) có đánh dấu con đường 172.30.22.0, vì thế R1 cập nhật bằng định tuyến giá trị trọng số 16 cho con đường đó
6. R3 nhận cập nhật từ R1 (như mô tả trong bước 4), lấy giá trị trọng số là 2 cho con đường 172.30.22.0. Vì R3 đã đặt con đường này vào chế độ holddown, vào mục mới trọng số 2 này đã được được học từ một router khác (R1) thay vì con đường ban đầu (R2), R3 bỏ qua thông tin định tuyến mới này.

Kết quả holddown của R3 được mô tả trong bước 6, tất cả 3 router có một con đường 172.30.22.0 trọng số 16. Lúc này, bất kì cập nhật định tuyến nào trong tương lai sẽ liệt kê con đường trọng số 16 cho mạng con đó – ít nhất cho đến khi con đường thực sự đến mạng con đó trở nên sẵn sàng trở lại.

Định nghĩa của holddown cho phép router tin cùng router đã gửi con đường ban đầu, thậm chí trước khi bộ định thời holddown hết hạn. Ví dụ, toàn thể tiến trình của hình trên có thể xảy ra chỉ trong một vài giây vì tất cả các cập nhật có theo dõi. Nếu giao tiếp bật trở lại, R2 khi đó quảng bá lại con đường trọng số 1 cho 172.30.22.0. Nếu R1 và R3 tin lại quảng bá của R2, chúng có thể tránh phải đợi hầu hết phút cho bộ định thời

holddown của nó hết hạn với mạng con 172.30.22.0. Vì thế, việc lắng nghe cập nhật định tuyến từ cùng một router đã quảng bá con đường đó không tạo ra vòng lặp. Chính thế, holddown cho phép các router lắng nghe các quảng bá của R2.

9.2.4 Tổng kết về Distance Vector

Trước khi kết thúc việc xem xét khả năng tránh lặp của distance vector, cần thiết xem lại các khái niệm sau đây. Phần này quan tâm đến nhiều lý thuyết, tập trung vào các chủ đề chính sau đây:

- Trong suốt thời gian ổn định, router gửi các cập nhật đầy đủ định kì dựa trên một bộ định thời ngắn (mặc định RIP là 30 giây). Cập nhật đó liệt kê tất cả các con đường đã biết ngoại trừ con đường bị giới hạn bởi quy tắc miền phân tách
- Khi thay đổi xảy ra làm cho một con đường lỗi, router báo lỗi phản ứng bằng cách gửi ngay tức thì cập nhật một phần, chưa chỉ con đường đã đánh dấu, với trọng số vô hạn
- Các router khác lắng nghe con đường đánh dấu cũng gửi các cập nhật một phần có theo dõi, đánh dấu con đường bị lỗi đó.
- Các router áp dụng quy tắc miền phân tách với con đường lỗi bằng cách gửi một con đường đánh dấu ngược đến router từ con đường đánh dấu đã học.
- Tất cả router đặt con đường vào trạng thái holddown và bắt đầu bộ định thời holddown cho con đường sau khi đã biết con đường đó bị lỗi. Mỗi router bỏ qua tất cả thông tin mới về con đường đó cho đến khi bộ định thời holddown hết hạn, trừ khi thông tin đó đến từ cùng router đã quảng bá con đường cho mạng con bị lỗi trước đó.

9.3. GIAO THỨC ĐỊNH TUYẾN LINK – STATE

Giống distance vector, giao thức link – state gửi cập nhật định tuyến đến các router kế cận, rồi lại tiếp tục... Tại cuối của tiến trình, giống giao thức distance vector, router sử dụng giao thức link – state thêm con đường tốt nhất vào bảng định tuyến của nó, dựa trên trọng số. Phần này

Xem xét cơ chế cơ bản nhất cách giao thức link – state làm việc, với ví dụ là OSPF – Open Shortest Path First, giao thức định tuyến IP link – state đầu tiên. Bắt đầu với việc giới thiệu cách giao thức link – state đầy các thông tin định tuyến trên mạng. Sau đó sẽ mô tả cách giao thức link state xử lý thông tin định tuyến để chọn con đường tốt nhất.

9.3.1. Xây dựng cùng LSDB trên mọi router

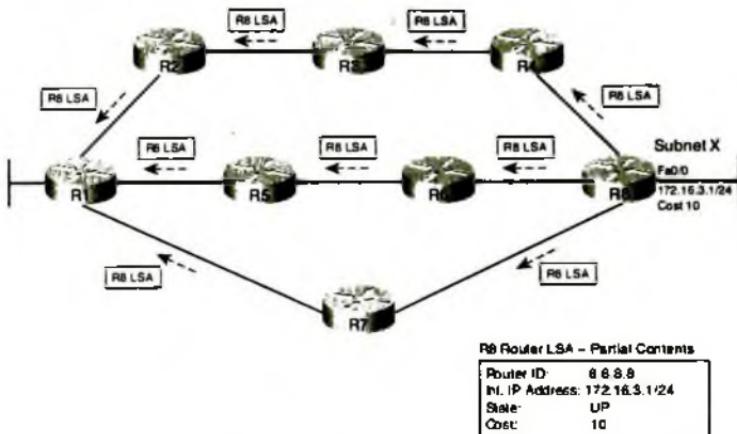
Các router sử dụng giao thức link – state cần quảng bá mọi chi tiết về mạng cho tất cả các router khác. Tại cuối tiến trình này, mọi router trên mạng đều có chính xác cùng thông tin về mạng. Router sử dụng thông tin này, được lưu trữ trong RAM bên trong cấu trúc dữ liệu gọi là cơ sở dữ liệu Link – state Database (LSDB), để thực hiện tiến trình link – state chính xác để tính toán con đường tốt nhất hiện tại đến mọi mạng con.

OSPF quảng bá thông tin trong các thông điệp cập nhật định tuyến ở nhiều loại, với cập nhật chứa thông tin được gọi là quảng bá link – state (LSA). LSA tồn tại trong nhiều dạng, bao gồm hai loại chính sau đây:

- Router LSA: Chứa một số định danh về router (Router ID), địa chỉ IP và mặt nạ của các giao tiếp của router, trạng thái (bật hay tắt) của mỗi giao tiếp, và chi phí có liên quan với giao tiếp đó.
- Link LSA: Xác định mỗi liên kết (mạng con) và router có kết nối đến liên kết đó. Nó cũng xác định trạng thái liên kết (bật hay tắt)

Một số router trước tiên phải tạo router và link LSA, và sau đó đầy các LSA này đến tất cả các router khác. Mỗi router tạo một router LSA cho chính nó và sau đó đầy LSA đó đến các router khác trong thông điệp cập nhật định tuyến. Để đầy một LSA, router gửi LSA đó đến lân cận của nó. Những lân cận này đến lượt chuyển tiếp LSA đó cho lân cận của nó, cho đến khi tất cả các router đều học về các LSA đó. Với link LSA, một router có kết nối đến một mạng con cũng tạo và đầy một link LSA cho mạng con đó. Vào cuối tiến trình, mọi router có mọi LSA của các router khác vào bàn sao của tất cả các link LSA.

Hình 9.15 mô tả ý tưởng chung cho tiến trình đầy các thông tin định tuyến, với R8 tạo và đầy các LSA của nó.



Hình 9.15. Định tuyến Link State

Hình 9.15 cho thấy tiến trình gửi thông tin cơ bản, với R8 gửi LSA ban đầu cho chính nó, và router khác đầy LSA này bằng cách chuyển tiếp nó cho đến khi mọi router có một bản sao của nó. Để ngăn ngừa lặp quảng bá LSA, một router biết về LSA trước tiên hỏi các lân cận của nó nếu router này đã biết về LSA đó. Ví dụ R8 trước tiên bắt đầu bằng cách hỏi R4, R6, R7 liệu chúng biết về router LSA cho R8. Những router này sẽ phản hồi, thông báo rằng chúng không biết về router LSA của R8. Chỉ tại thời điểm đó, R8 gửi LSA này đến các router lân cận của mình. Tiến trình lặp lại với mọi lân cận. Nếu một router đã học về LSA đó – không quan tâm về con đường nào – nó có thể thông báo rằng đã có LSA đó – vì thế ngăn LSA khỏi bị quảng bá lặp trên mạng.

Nguồn gốc của thuật ngữ *link-state* có thể được giải thích bằng cách xem xét nội dung của router LSA trong hình. Hình 9.15 cho thấy một trong bốn địa chỉ IP của giao tiếp được liệt kê trong router LSA của R8, cùng với trạng thái của giao tiếp đó. Giao thức link state lấy tên của nó từ yêu tố mà LSA quảng bá mỗi giao tiếp và trạng thái của giao tiếp đó là bật hay tắt. Vì thế, LSDB chứa thông tin về không chỉ router đang

bật và làm việc và các liên kết, giao tiếp của nó, mà còn tắt cả các router và giao tiếp hay liên kết của nó, dù cho giao tiếp đó tắt.

Sau khi LSA được đẩy đi, dù LSA không thay đổi, giao thức link-state yêu cầu việc quảng bá các LSA định kì, tương tự như cập nhật định kì được gửi bởi giao thức distance vector. Tuy nhiên, giao thức distance vector thường sử dụng bộ định thời ngắn hơn, ví dụ như RIP là 30 giây và RIP gửi một cập nhật đầy đủ liệt kê tất cả các con đường đã quảng bá bình thường. OSPF gửi lại mỗi LSA dựa trên bộ định thời riêng rẽ trên mỗi LSA (mặc định là 30 phút). Kết quả là, trong một mạng ổn định, giao thức link-state sử dụng ít băng thông mạng hơn để gửi các thông tin định tuyến so với giao thức distance vector. Nếu một LSA thay đổi, router ngay lập tức gửi đi LSA thay đổi đó. Ví dụ, nếu giao tiếp LAN của R8 lỗi, R8 cần gửi lại các LSA của R8, báo rằng giao tiếp bây giờ đã tắt.

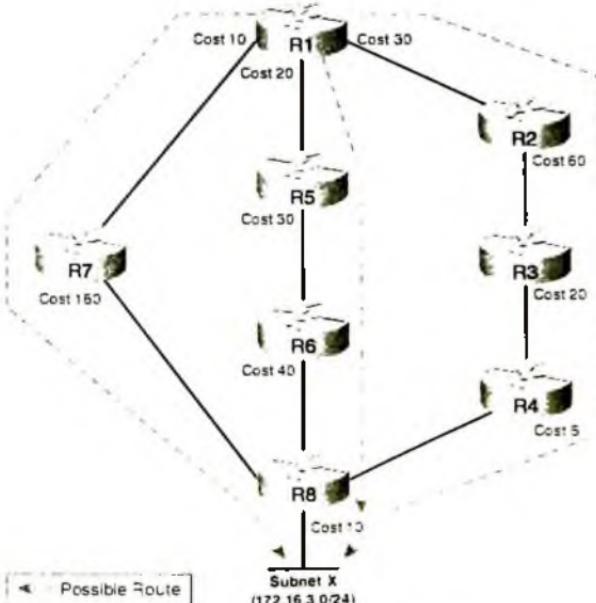
9.3.2. Thuật toán Dijkstra để tìm đường đi tốt nhất

Tiến trình gửi link-state có kết quả là mọi router có một bản sao giống nhau về LSDB trong bộ nhớ nhưng tiến trình này bản thân nó không thể làm cho router biết về các con đường cần được thêm vào bảng định tuyến IP. Dù rằng rất chi tiết và hữu ích, thông tin trong LSDB không thể diễn tả rõ ràng con đường tốt nhất của mỗi router để đến đích. Giao thức link state phải sử dụng một phần quan trọng khác của giải thuật link state để tìm kiếm và thêm các con đường vào bảng định tuyến IP – các con đường liệt kê số mạng con và mặt nạ và giao tiếp đầu ra, và địa chỉ IP router chặng kế tiếp. Tiến trình này sử dụng giải thuật Dijkstra Shortest Path First (SPF).

Giải thuật SPF có thể được so sánh với các thường làm khi đi du lịch sử dụng bản đồ. Mọi người có thể mua cùng bản đồ, vì thế mọi người có thể biết thông tin về các con đường. Tuy nhiên, khi nhìn bản đồ, trước tiên tìm điểm bắt đầu và kết thúc, và sau đó phân tích bản đồ để tìm các con đường có thể. Nếu nhiều con đường có vẻ giống nhau về độ dài, có thể quyết định sử dụng con đường dài hơn nếu con đường đó là cao tốc thay vì đường thông thường. Một số người có thể sở hữu cùng bản đồ, nhưng họ có điểm bắt đầu và kết thúc có thể khác, vì thế họ có thể chọn một con đường hoàn toàn khác.

Về mặt phân tích, LSDB hoạt động giống như là bản đồ và giải thuật SPF hoạt động giống như con người xem xét bản đồ. LSDB chứa tất cả thông tin về mọi router và liên kết. Giải thuật SPF xác định cách một router xử lý LSDB, với mỗi router xem bản thân nó là điểm bắt đầu cho con đường. Mỗi router sử dụng chính nó như là điểm xuất phát vì mỗi router cần đặt các con đường vào trong bảng định tuyến của chính nó. Giải thuật SPF tính toán tất cả các con đường có thể để đến một mạng con, và trọng số tương thích cho toàn bộ con đường, với mỗi mạng con đích có thể. Tóm lại, mỗi router phải xem bản thân nó như là điểm xuất phát, và mỗi mạng con là đích, và sử dụng giải thuật SPF để tìm con đường phù hợp nhất và tốt nhất cho mỗi mạng con.

Hình 9.16 cho thấy một ví dụ về kết quả giải thuật SPF được thực hiện bởi R1 khi thử tìm con đường tốt nhất đến mạng con 172.16.3.0/24. Hình này tương tự như một cây với gốc là R1 và các nút lá là mạng con muôn đến.



Hình 9.16. Cập nhật định tuyến Link State

Hình 9.16 không thể hiện thuật toán SPF, nhưng nó thể hiện hình vẽ của dạng phân tích được thực hiện bởi giải thuật SPF trên R1. Thông thường, mỗi router thực hiện tiến trình SPF để tìm kiếm tất cả các con đường đến mỗi mạng con, và sau đó giải thuật SPF có thể lấy con đường tốt nhất. Để lấy con đường tốt nhất đó, giải thuật SPF của một router thêm chi phí liên quan với mỗi con đường giữa nó và mạng con dịch, thông qua mỗi con đường có thể. Hình trên cho thấy chi phí liên quan với mỗi con đường bên ngoài các liên kết đó, với các đường gạch đứt cho thấy ba con đường R1 tìm thấy giữa nó và mạng con X (172.16.3.0/24).

Bảng 9.17. Các con đường trong ví dụ định tuyến OSPF

Con đường	Vị trí trong hình 9.16	Chi phí ước lượng
R1-R7-R8	Trái	$10+180+10=200$
R1-R5-R6-R8	Giữa	$20+30+40+10=100$
R1-R2-R3-R4-R8	Phải	$30+60+20+5=125$

Bảng 9.17 cho thấy ba con đường với các chi phí liên quan, thể hiện con đường tốt nhất của R1 đến 172.16.3.0 bắt đầu bằng cách đi qua R5.

Kết quả của giải thuật SPF phân tích LSDB, R1 thêm một con đường đến mạng con 172.16.3.0/24 vào bảng định tuyến của nó, với router chặng kế là R5.

9.3.3. Hội tụ với giao thức Link – State

Sau khi mạng ổn định, giao thức link – state gửi lại mỗi LSA theo chu kỳ (mặc định OSPF là 30 phút). Tuy nhiên, khi một LSA thay đổi, các giao thức link – state phản ứng lại với thay đổi đó, hội tụ mạng và sử dụng các con đường tốt nhất hiện tại nhanh nhất có thể. Ví dụ, tưởng tượng rằng liên kết giữa R5 và R6 lỗi trong mạng của hình trên. Danh sách sau đây giải thích tiến trình R1 sử dụng để chuyển sang một con đường khác. (Các bước tương tự có thể xảy ra với các thay đổi với các router và con đường khác).

1. R5 và R6 gửi các LSA thông báo giao tiếp của nó ở trạng thái “down”
2. Tất cả router chạy giải thuật SPF lại để xem xét liệu tất cả các con đường đã thay đổi

3. Tất cả các router thay thế các con đường, như có thể, dựa trên kết quả của SPF. Ví dụ, R1 thay đổi con đường đến mạng con X (172.16.3.0/24) để sử dụng R2 như là router chặng kế

Những bước này cho phép giao thức định tuyến link – state hội tụ nhanh chóng, nhanh hơn nhiều so với giao thức định tuyến distance vector.

9.3.4. Tóm tắt và so sánh với giao thức Distance Vector

Giao thức định tuyến link – state cung cấp khả năng hội tụ nhanh, có thể là chức năng quan trọng nhất của một giao thức định tuyến với chức năng tránh lặp. Giao thức định tuyến link – state không cần sử dụng nhiều chức năng chống lặp được sử dụng bởi giao thức distance vector, nên giảm thiểu đáng kể thời gian hội tụ. Chức năng chính của giao thức định tuyến như sau:

- Tất cả router học về cùng thông tin chi tiết của các router và mạng con trong hệ thống mạng.
- Mỗi phần sơ đồ thông tin độc lập được gọi là LSA. Tất cả các LSA được lưu trữ trong RAM dưới cấu trúc dữ liệu được gọi là LSDB.
- Router gửi các LSA khi: thứ nhất chúng được tạo ra, thứ hai theo chu kỳ (nếu LSA không thay đổi thì mặc định là 30 phút), cuối cùng khi LSA thay đổi.
- LSDB không chứa con đường nào, nhưng chứa thông tin có thể được xử lý bởi thuật toán Dijkstra để tìm con đường tốt nhất của một router đến mạng con.
- Mỗi router chạy giải thuật SPF, với LSDB là đầu vào, kết quả là các con đường tốt nhất được thêm vào bảng định tuyến.
- Giao thức link – state hội tụ nhanh bằng cách gửi lại tức thì các LSA thay đổi và chạy lại giải thuật SPF trên mỗi router.

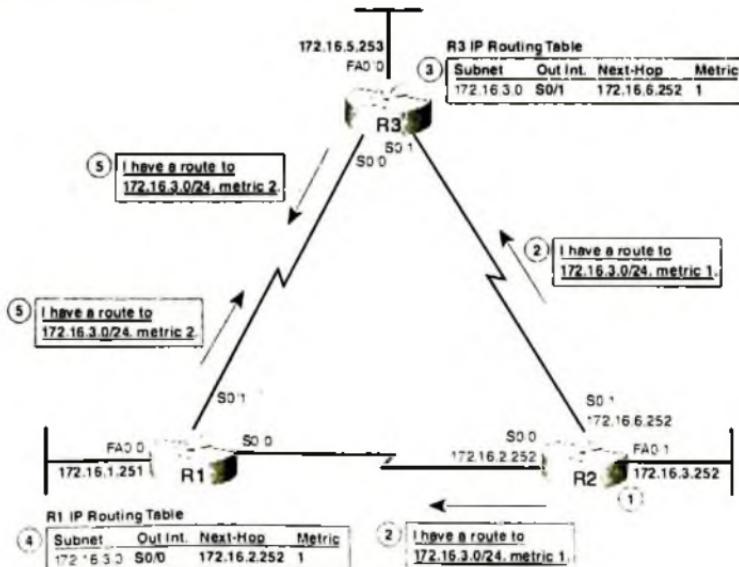
Một trong những điểm so sánh quan trọng giữa các giao thức định tuyến khác nhau là tốc độ hội tụ của mỗi giao thức đó. Dĩ nhiên, giao thức định tuyến link – state hội tụ nhanh hơn nhiều giao thức định tuyến distance vector. Danh sách sau đây tóm tắt một số điểm so sánh chính cho các giao thức khác nhau, đánh giá sức mạnh của giải thuật bên dưới.

- Độ hội tụ: Giao thức link – state nhanh hơn nhiều
- CPU và RAM: Giao thức link – state tốn nhiều CPU và nhiều bộ nhớ hơn giao thức distance vector, dù rằng với mạng được thiết kế hoàn chỉnh, điều bất tiện này có thể được giảm thiểu.
- Tránh lặp định tuyến: Giao thức link – state tránh lặp tốt, trong khi distance vector yêu cầu nhiều chức năng bổ sung (ví dụ, miền phân tách)
- Cấu hình: Distance vector yêu cầu ít cấu hình hơn, link state yêu cầu sử dụng nhiều chức năng cấu hình hơn.

9.4. GIAO THỨC ĐỊNH TUYẾN RIP – 2

9.4.1. Khái niệm cơ bản

Router sử dụng RIP – 2 để quảng bá lượng thông tin nhỏ đơn giản về mỗi mạng con đến các lân cận. Những lân cận này đến lượt nó quảng bá thông tin đó cho các lân cận khác, và tiếp tục cho đến khi tất cả router đã học về thông tin đó.



Hình 9.17. Định tuyến RIP - 2

Ví dụ về RIP – 2 quảng bá các con đường

Hình vẽ 9.17 cho thấy cách router quảng bá và học các con đường với mạng con 172.16.3.0/24, thực tế router sẽ quảng bá các con đường khác nữa. Các bước như sau:

1. Router R2 học một con đường có kết nối đến mạng con 172.16.3.0/24
2. R2 gửi một cập nhật định tuyến đến một lân cận, liệt kê mạng con (172.16.3.0), mặt nạ (/24) và khoảng cách, hay trọng số (1)
3. R3 lắng nghe các cập nhật định tuyến, và thêm một con đường vào bảng định tuyến của nó với mạng con 172.16.3.0/24, xem R2 là router chặng kế.
4. Trong cùng thời gian đó, R1 cũng lắng nghe cập nhật định tuyến được gửi trực tiếp đến R1 bởi R2. R1 sau đó thêm một con đường vào bảng định tuyến của nó với mạng con 172.16.3.0/24, xem R2 là router chặng kế.
5. R1 và R3 sau đó gửi một cập nhật định tuyến cho nhau, với mạng con 172.16.3.0/24 có trọng số là 2.

Cuối tiên trình này, cả R1 và R2 đều nghe về hai con đường có thể đến mạng con 172.16.3.0 – một trọng số là 1 và một trọng số là 2. Mỗi router sử dụng trọng số thấp hơn của chính nó (1) để đến 172.16.3.0.

9.4.2. Cấu hình và xác nhận RIP – 2

Cấu hình RIP – 2 thực sự đơn giản khi so sánh với các khái niệm khác về giao thức định tuyến. Tiên trình cấu hình sử dụng ba lệnh được yêu cầu, với chỉ một lệnh, network, cần thiết phải có suy nghĩ có thể cũng biết các câu lệnh show thông dụng hơn để giúp phân tích và xử lý sự cố.

9.4.2.1. Cấu hình RIP – 2

Tiền trình cấu hình RIP – 2 yêu cầu chỉ ba bước đơn giản như sau, trong đó bước thứ ba có thể lặp lại

Bước 1: Sử dụng lệnh cấu hình router rip để vào chế độ cấu hình RIP

Bước 2: Sử dụng lệnh con cấu hình RIP version 2 để vào chế độ cấu hình RIP -2

Bước 3: sử dụng một trong các lệnh con cấu hình RIP network net-number để bật RIO trên các giao tiếp chính xác,

Bước 4: (tùy chọn) tùy nhu cầu, bỏ RIP trên một giao tiếp sử dụng lệnh con RIP passive – interface type number

Trong ba bước được yêu cầu đầu tiên, chỉ bước thứ ba – lệnh **network**, cần xem xét. Mỗi lệnh **network** RIP chỉ sử dụng một mạng phân lớp như là một đối số của nó. Với bất kì địa chỉ IP của giao tiếp router trong một mạng phân lớp hoàn toàn, router cần thực những công việc sau đây:

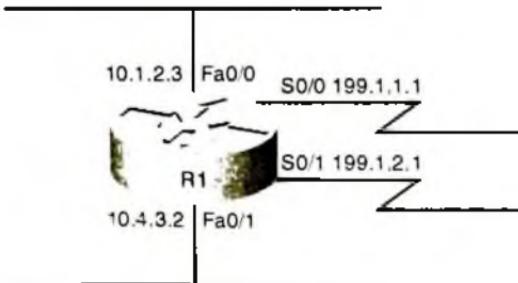
Router quảng bá nhóm các cập nhật định tuyến đến một địa chỉ IP quảng bá dành riêng, 244.0.0.9.

Router lắng nghe các cập nhật đến trên cùng giao tiếp đó.

Router quảng bá về mạng con có kết nối đến giao tiếp đó.

9.4.2.2. Cấu hình RIP mẫu

Ghi nhớ các yếu tố này, và xem xét cách cấu hình RIP trên một router đơn. Kiểm tra hình vẽ sau đây và thử áp dụng ba bước cấu hình đầu tiên trên router này.



Hình 9.18. Ví dụ định tuyến RIP - 2

Hai lệnh cấu hình đầu tiên là đơn giản, **router rip**, sau đó là **version 2**, không cần đổi số. Sau đó cần chọn lệnh **network** để cấu hình tại bước 3. Để trùng khớp với giao tiếp S0/0, phải chỉ ra địa chỉ 199.1.1.1 là địa chỉ IP mạng lớp C 199.1.1.0, nghĩa là cần một lệnh con **network 199.1.1.0**. Tương tự, để trùng khớp với giao tiếp S0/1, cần một lệnh **network 199.1.2.0** vì địa chỉ IP 199.1.2.1 trong mạng lớp C 199.1.2.0. Cuối cùng, cả hai giao tiếp LAN có một địa chỉ trong mạng lớp A 10.0.0.0, nên một lệnh **network 10.0.0.0** phù hợp với cả hai giao tiếp trên. Ví dụ sau đây cho thấy tiến trình cấu hình toàn thể với tất cả năm lệnh cấu hình trên.

Ví dụ 9.1:

```
R1#configure terminal
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 199.1.1.0
R1(config-router)#network 199.1.2.0
R1(config-router)#network 10.0.0.0
```

Với cấu hình này, R1 bắt đầu sử dụng RIP – gửi các cập nhật RIP, lắng nghe các cập nhập RIP đến và quảng bá về mạng con có kết nối – trên mỗi một bốn giao tiếp trên. Tuy nhiên, tưởng tượng rằng muốn bật RIP trên giao tiếp Fa0/0 trên R1, nhưng không muốn bật RIP trên giao tiếp Fa0/1. Cả hai giao tiếp này đều trên mạng 10.0.0.0 vì thế cả hai đều phù hợp với mạng con bằng lệnh **network 10.0.0.0**.

Cấu hình RIP không cung cấp cách thức bật RIP trên chỉ một số giao tiếp trên các mạng con lớp A, B, C. Vì thế, nếu muốn kích hoạt RIP trên chỉ giao tiếp Fa0/0 của R1, và không có trên giao tiếp Fa0/1, sẽ thực sự cần sử dụng lệnh **network 10.0.0.0** để bật RIP trên cả hai giao tiếp, và sau đó tắt việc gửi các cập nhật RIP trên Fa0/1 sử dụng lệnh con **passive-interface type number**. Ví dụ, bật RIP trên tất cả giao tiếp của router R1 trên hình đó, ngoại trừ Fa0/1, có thể sử dụng cùng cấu hình trong ví dụ trên, nhưng sau đó cũng thêm lệnh con **passive-interface fa0/1** trong khi cấu hình RIP. Lệnh này báo cho R1 biết ngưng gửi các cập nhật RIP ra ngoài giao tiếp Fa0/1 của nó, tắt một trong số chức năng chính của RIP.

Một trong số chú ý cuối của lệnh **network**: IOS sẽ thực sự chấp nhận một đối số bên cạnh số mạng phân lớp trên mạng đó, và IOS sẽ

không thông báo lỗi nào. Tuy nhiên, IOS luôn xem đối số đó là chỉ số mạng con phân lớp. Ví dụ, nếu gõ lệnh **network 10.1.2.3** trong cấu hình RIP, IOS sẽ chấp nhận lệnh này mà không có lỗi. Tuy nhiên, khi xem xét cấu hình, sẽ thấy mạng con 10.0.0.0, và mạng 10.1.2.3 mà nhập vào không tồn tại ở đây. Lệnh **network 10.0.0.0** sẽ phù hợp với tất cả giao tiếp trên mạng 10.0.0.0.

9.4.2.3. Xác nhận RIP – 2

IOS chứa ba lệnh **show** chính hữu ích để xác nhận cách RIP – 2 làm việc tốt. Bảng 9.18 liệt kê các lệnh và mục đích của chúng.

Bảng 9.18. Các lệnh **show** trong RIP-2

Command	Purpose
Show ip interface brief	Liệt kê các giao tiếp trên router, gồm địa chỉ IP và trạng thái. Một router cần có địa chỉ IP và trạng thái "up/up", trước khi RIP có thể hoạt động trên giao tiếp đó
Show ip route [rip]	Liệt kê bảng định tuyến, bao gồm các con đường học theo RIP và tùy chọn các con đường chỉ học theo RIP
Show ip protocols	Liệt kê tất cả thông tin về cấu hình RIP, cộng với địa chỉ IP của các router RIP lân cận từ đó router đã học được con đường

9.4.2.4. Kiểm tra các thông điệp RIP với lệnh **debug**

Cách tốt nhất để hiểu liệu RIP có hoạt động tốt hay không là sử dụng lệnh **debug ip rip**. Lệnh này bật chức năng debug thông báo cho router biết tạo một thông điệp nhật ký mỗi khi router gửi và nhận một cập nhật RIP. Những thông điệp đó chứa thông tin về mọi mạng con được liệt kê trong các quảng bá và ý nghĩa của các thông điệp khá rõ ràng.

Ví dụ 9.2 mô tả kết quả được tạo bởi lệnh **debug ip rip** trên router Albuquerque. Chú ý rằng để thấy các thông điệp này người dùng cần kết nối đến chế độ console của router hay sử dụng lệnh **terminal monitor** trong chế độ cấp quyền nếu việc sử dụng Telnet hay SSH để kết nối đến router đó. Chú ý bên trong ví dụ mô tả một số ý nghĩa của các thông điệp, trong năm nhóm khác nhau. Ba nhóm đầu tiên của thông điệp mô tả cập nhật của Albuquerque được gửi trên mỗi ba giao tiếp đã bật RIP của nó; nhóm thứ tư chứa các thông điệp được tạo khi Albuquerque nhận một cập nhật từ Seville, và nhóm thứ năm mô tả cập nhật nhận được từ Yosemite.

Ví dụ 9.2:

```

Albuquerque>#debug ip rip
RIP protocol debugging is on
Albuquerque

: Update sent by Albuquerque out Fa0/0:
! The next two messages tell you that the local router is sending a version 2 update
! on Fa0/0, to the 224.0.0.9 multicast IP address. Following that, 5 lines list the
! 5 subnets listed in the advertisement.
*Jun 9 14:35:08.855: RIP: sending v2 update to 224.0.0.9 via FastEthernet0 0 (10.1.1.251)
*Jun 9 14:35:08.855: RIP: build update entries
*Jun 9 14:35:08.866: 10.1.2.0/24 via 0.0.0.0, metric 2, tag 0
*Jun 9 14:35:08.855: 10.1.3.0/24 via 0.0.0.0, metric 2, tag 0
*Jun 9 14:35:08.855: 10.1.128.0/24 via 0.0.0.0, metric 1, tag 0
*Jun 9 14:35:08.855: 10.1.128.0/24 via 0.0.0.0, metric 2, tag 0
*Jun 9 14:35:08.855: 10.1.130.0/24 via 0.0.0.0, metric 1, tag 0

! The next 5 debug messages state that this local router is sending an update on its
! S0/0/1 interface, listing 3 subnets/masks
*Jun 9 14:35:10.351: RIP: sending v2 update to 224.0.0.9 via Serial0/1 0 (10.1.130.251)
*Jun 9 14:35:10.351: RIP: build update entries
*Jun 9 14:35:10.351: 10.1.1.0/24 via 0.0.0.0, metric 1, tag 0
*Jun 9 14:35:10.351: 10.1.2.0/24 via 0.0.0.0, metric 2, tag 0
*Jun 9 14:35:10.351: 10.1.128.0/24 via 0.0.0.0, metric 1, tag 0

! The next 5 debug messages state that this local router is sending an update on its
! S0/0/1 interface, listing 3 subnets/masks
*Jun 9 14:35:12.443: RIP: sending v2 update to 224.0.0.9 via Serial0/0 1 (10.1.128.251)
*Jun 9 14:35:12.443: RIP: build update entries
*Jun 9 14:35:12.443: 10.1.1.0/24 via 0.0.0.0, metric 1, tag 0
*Jun 9 14:35:12.443: 10.1.3.0/24 via 0.0.0.0, metric 2, tag 0
*Jun 9 14:35:12.443: 10.1.130.0/24 via 0.0.0.0, metric 1, tag 0

! The next 4 messages are about a RIP version 2 (v2) update received by Albuquerque
! from Seville (S0/0/0), listing three subnets. Note the mask is listed as /24.
*Jun 9 14:35:13.819: RIP: received v2 update from 10.1.130.253 on Serial0/0 0
*Jun 9 14:35:13.819: 10.1.2.0/24 via 0.0.0.0 in 2 hops
*Jun 9 14:35:13.819: 10.1.3.0/24 via 0.0.0.0 in 1 hops
*Jun 9 14:35:13.819: 10.1.129.0/24 via 0.0.0.0 in 1 hops

! The next 4 messages are about a RIP version 2 (v2) update received by Albuquerque
! from Yosemite (S0/0/1), listing three subnets. Note the mask is listed as /24.
*Jun 9 14:35:16.911: RIP: received v2 update from 10.1.128.252 on Serial0/0 1
*Jun 9 14:35:16.915: 10.1.2.0/24 via 0.0.0.0 in 1 hops
*Jun 9 14:35:16.915: 10.1.3.0/24 via 0.0.0.0 in 2 hops
*Jun 9 14:35:16.915: 10.1.129.0/24 via 0.0.0.0 in 1 hops

Albuquerque>#debug all
All possible debugging has been turned off
Albuquerque>show process
CPU utilization for five seconds: 0% CPU: one minute: 0% five minutes: 0%
PID CPUT CPU Runtime (ms) Inlocked JSecs Stacks TTY Process
 1 0% 60.82488 0 1 0 5608 6000 0 Chunk Manager

```

Trước tiên, nếu nhìn rộng hơn về năm tập thông điệp này, nó giúp thiết lập lại các thông điệp được mong đợi mà Albuquerque nên nhận và gửi. Các thông điệp báo rằng Albuquerque đang gửi các cập nhật trên Fa0/0, S0/0/1 và S0/1/0, trên đó RIP được bật. Ngoài ra, các thông điệp khác thông báo rằng router đã nhận các cập nhật trên giao tiếp S0/1/0, là liên kết kết nối đến Seville, và S0/0/1, là liên kết kết nối đến Yosemite.

Hầu hết các chi tiết trong thông điệp có thể dễ dàng đoán ra. Một số thông điệp đề cập đến "v2", có nghĩa là RIP version 2, và các thông điệp được gửi đến địa chỉ IP quảng bá nhóm 224.0.0.9. (RIP – 1 gửi các cập nhật đến địa chỉ IP quảng bá 255.255.255.255). Phần lớn các thông điệp trong ví dụ mô tả thông tin định tuyến được liệt kê trong mỗi cập nhật, cụ thể là mạng con và chiều dài tiền tố (mặt nạ), và trọng số.

Một đánh giá gần hơn về số mạng con trong mỗi cập nhật định tuyến cho thấy rằng các router không quảng bá tất cả các con đường trong cập nhật. Trong sơ đồ có sáu con đường. Tuy nhiên, các cập nhật trong ví dụ trên có hoặc là ba hoặc là năm con đường được thể hiện. Nguyên nhân là miền phân tách, chức năng này giúp tránh lặp, giới hạn số mạng con được quảng bá trên mỗi cập nhật để tránh lặp định tuyến.

Cuối cùng, khi sử dụng lệnh **debug** thì khả năng sử dụng router là rất cao, có thể lên đến 30 – 40 phần trăm, và rất chú ý đến khi bật chức năng này lên vì nó có thể ảnh hưởng đến việc chuyển tiếp các gói tin. Có thể sử dụng lệnh **show process** để thấy rõ hơn về yếu tố này.

9.5. GIAO THỨC ĐỊNH TUYẾN OSPF

Giao thức định tuyến Link – state được phát triển vào đầu những năm 1990. Những người thiết kế giao thức tính toán rằng tốc độ liên kết, CPU và bộ nhớ router sẽ tiếp tục cải tiến qua thời gian, vì thế giao thức được thiết kế để cung cấp nhiều chức năng mạnh mẽ bằng cách tận dụng những cải tiến này. Bằng cách gửi nhiều thông tin hơn, và yêu cầu router thực hiện nhiều xử lý hơn, giao thức link state có được một số lợi điểm quan trọng hơn giao thức distance vector – cụ thể là, hội tụ nhanh hơn. Mục tiêu thì vẫn như cũ, thêm các con đường tốt nhất hiện tại vào bảng

định tuyến, nhưng những giao thức này sử dụng các phương thức khác nhau để tìm và thêm những con đường đó.

Phần này giải thích giao thức link – state được sử dụng phổ biến nhất OSPF (Open Shortest Path First). Giao thức link – state khác là IS – IS thường bị bỏ qua.

9.5.1. Giao thức OSPF và hoạt động

Giao thức OSPF có nhiều chức năng phức tạp. Với tiến trình học đường, các chức năng của OSPF có thể được phân thành ba loại chính: neighbors, Database exchange – trao đổi cơ sở dữ liệu và tính toán con đường. Các router OSPF trước tiên tạo dựng một mối quan hệ lân cận – neighbor cung cấp cơ sở cho việc trao đổi thông tin OSPF. Sau khi các router đã thành lân cận, chúng trao đổi nội dung về các LSDB của chúng, thông qua tiến trình được gọi là trao đổi cơ sở dữ liệu – Database exchange. Cuối cùng, sau khi router đã có thông tin sơ đồ trong cơ sở dữ liệu LSDB của nó, nó sử dụng giải thuật Dijkstra Shortest Path First SPF để tính toán con đường tốt nhất hiện tại và thêm chúng vào bảng định tuyến IP.

Câu lệnh show của IOS cũng hỗ trợ cho các chức năng này. IOS có một bảng neighbor OSPF (`show ip ospf neighbor`) một OSPF LSDB (`show ip ospf Database`) và bảng định tuyến IP (`show ip route`) sẽ khảo sát kĩ hơn các phần trên trong các mục dưới đây.

9.5.1.1. Các lân cận OSPF – OSPF neighbors

Định nghĩa: OSPF neighbor của một router là một router khác kết nối đến cùng liên kết dữ liệu mà trong đó router có thể trao đổi thông tin định tuyến cho nhau sử dụng OSPF.

Đầu tiên, các lân cận kiểm tra và xác nhận các thiết lập OSPF cơ bản trước khi trao đổi thông tin định tuyến – các thiết lập phải trùng khớp để OSPF hoạt động chính xác. Thứ hai, tiến trình đầu ra của một router biết khi nào router đó là tốt, và khi nào kết nối đến một lân cận bị mất, báo cho router khi nào nó tính toán lại toàn bộ các mục trong bảng định tuyến để tái hội tụ với các tập con đường mới. Ngoài ra, tiến trình OSPF

Hello xác định cách thức các lân cận có thể được phát hiện tự động, nghĩa là các router mới có thể được thêm vào mạng mà không yêu cầu mọi router phải cấu hình lại.

Tiền trình OSPF Hello trong đó mỗi quan hệ lân cận được định hình làm việc tương tự như là khi đến một nơi ở mới và gặp gỡ nhiều lân cận. Khi thấy họ, có thể đến chào và hỏi thăm tên tuổi. Sau khi nói chuyện, sẽ có một ít ân tượng về họ. Tương tự, với OSPF, tiền trình bắt đầu với thông điệp được gọi là OSPF Hello. Hello liệt kê Router ID của mỗi router (RID), được xem như là tên duy nhất hay định danh của mỗi router trong OSPF. Cuối cùng OSPF thực hiện nhiều kiểm tra thông tin trong thông điệp OSPF để đảm bảo rằng hai router đó có thể là lân cận của nhau.

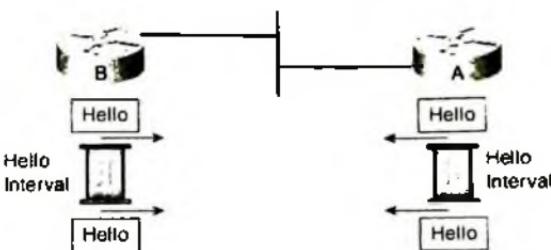
9.5.1.1.1. Xác định OSPF router với một Router ID

Vì nhiều nguyên nhân, OSPF cần một định danh duy nhất cho nhiều router. Trước tiên, các lân cận cần một cách để biết router nào gửi một thông điệp OSPF cụ thể. Ngoài ra, OSPF LSDB liệt kê tập hợp các LSA (Link State Advertisement), mô tả mỗi router trong một hệ thống mạng, vì thế LSDB cần một định danh duy nhất cho mỗi router. Để thực hiện, OSPF sử dụng khái niệm có tên là OSPF Router ID, viết tắt là RID.

OSPF RID là một số 32 bit được viết dạng thập phân có chấm, vì thế sử dụng một địa chỉ IP là cách thuận tiện để xác định một RID. Ngoài ra, OSPF RID có thể được cấu hình trực tiếp, được xem xét trong phần Cấu hình Router ID OSPF.

9.5.1.1.2. Tìm lân cận bằng trao đổi Hello

Ngay sau khi router đã chọn OSPF Router ID của nó, và một số giao tiếp đã bật, router sẵn sàng để tìm lân cận OSPF của nó. Các router OSPF có thể trở thành lân cận nếu chúng được kết nối đến cùng mạng con. Để tìm các router OSPF khác, router gửi các gói tin Hello OSPF multicast đến mỗi giao tiếp và chờ để nhận các gói tin Hello OSPF từ các router khác có kết nối đến các giao tiếp này.



Hình 9.19. Giao thức định tuyến OSPF

Trong hình trên, cả router A và B gửi các thông điệp Hello đến LAN. Chúng tiếp tục gửi các Hello dựa trên các thiết lập Hello Timer. Ngay sau đó, hai router có thể bắt đầu trao đổi thông tin sơ đồ cho nhau. Sau đó chúng thực hiện giải thuật Dijkstra để điền vào bảng định tuyến các con đường tốt nhất. Các thông điệp Hello bao gồm có các chức năng sau đây:

- Thông điệp Hello tuân theo tiêu chuẩn gói tin IP, với loại giao thức gói tin IP 89.
- Các gói tin Hello được gửi đến địa chỉ IP multicast 224.0.0.5, một địa chỉ IP multicast được sử dụng cho OSPF.
- Các router OSPF lắng nghe các gói tin được gửi đến địa chỉ multicast 224.0.0.5, và chờ để nhận các gói tin Hello và tìm các lân cận mới.

Các router học nhiều thông tin quan trọng khác từ việc xem xét các gói tin Hello nhận được. Thông điệp Hello chứa RID của router gửi, Areald – mã vùng, Hello Interval – khoảng thời gian Hello, dead interval – khoảng thời gian dead, độ ưu tiên router, RID của router dành riêng (designated router DR), RID của router dành riêng dự phòng (Backup Designated Router – BDR), và danh sách các lân cận mà router đang gửi đã biết về mạng con đó.

Danh sách lân cận quan trọng với tiến trình Hello. Ví dụ, khi Router A nhận được một Hello từ Router B, Router A cần cách nào đó để báo cho Router B biết rằng Router A có Hello đó. Để thực hiện, router A

thêm RID của router B vào danh sách lân cận OSPF bên trong Hello kế tiếp (và tương lai) mà Router A quảng bá trên mạng đó. Tương tự, khi Router B nhận Hello của router A, các Hello kế tiếp của router B chưa có RID của router A trong danh sách lân cận này.

Ngay khi một router thấy RID của nó trong Hello nhận được, router tin rằng truyền thông hai chiều đã được thiết lập với lân cận đó. Truyền thông hai chiều với một lân cận rất quan trọng, vì lý này, các thông tin chi tiết hơn, như là LSA có thể được trao đổi. Tương tự, trong một số trường hợp trên LAN, các lân cận có thể đạt trạng thái hai chiều và dừng lại. Thông tin chi tiết cho vấn đề này được đề cập trong phần (Lựa chọn một router dành riêng).

9.5.1.1.3. Các vấn đề tiềm ẩn khi trở thành một lân cận

Việc nhận một Hello từ một router trên cùng một mạng con không phải luôn luôn cho kết quả hai router trở thành lân cận của nhau. Với OSPF, các router trên cùng một mạng con phải đồng ý về nhiều tham số được trao đổi trong Hello; ngược lại, router đơn giản không thể trở thành lân cận. Cụ thể, những điều sau đây phải trùng khớp trước khi một cặp router trở thành lân cận.

- Mặt nạ được sử dụng trên mạng con
- Chỉ số mạng con (được kế thừa sử dụng mặt nạ mạng con và địa chỉ IP giao tiếp của router)
- Chu kỳ Hello
- Chu kỳ Dead
- Phải vượt qua kiểm tra xác thực (nếu được sử dụng)
- Giá trị của cờ stub area.

Nếu một trong nhiều các tham số này khác nhau, các router không thể trở thành lân cận. Tóm lại, nếu chúng ra xử lý các sự cố liên quan đến lân cận OSPF, kiểm tra các thông tin trên.

Một số thông tin ở trên cần được giải thích rõ hơn. Trước tiên, một router muốn là lân cận phải xác nhận rằng nó ở trên cùng mạng con bằng cách so sánh địa chỉ IP và mặt nạ mạng con của router kế cận, được thể

hiện trong thông điệp Hello, với địa chỉ và mặt nạ của nó. Nếu chúng cùng mặt nạ, với cùng khoảng địa chỉ, thì kiểm tra này được vượt qua.

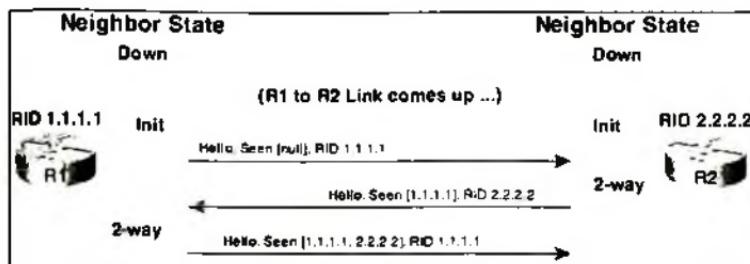
Kế tiếp, hai thiếp lập định thời, chu kỳ Hello và chu kỳ Dead, phải trùng khớp. Các router OSPF gửi các thông điệp Hello mỗi chu kỳ Hello. Khi một router không còn nhận được một Hello từ một lân cận trong khoảng thời gian xác định bởi chu kỳ Dead, router tin rằng lân cận đó không thể đến được nữa, và router phản ứng lại và tái hội tụ mạng. Ví dụ, trên giao tiếp Ethernet, Cisco router mặc định chu kỳ Hello là 10 giây và chu kỳ dead là 4 lần chu kỳ Hello, hay 40 giây, nó đánh dấu router yên lặng là “down” trong bảng lân cận của nó. Tại thời điểm này, router có thể phản ứng lại và hội tụ để sử dụng con đường tốt nhất hiện tại.

9.5.1.1.4. Trạng thái lân cận

OSPF xác định một tập hợp lớn các hành động tiềm ẩn mà hai router sử dụng để truyền thông với nhau. Để theo dõi tiến trình này, router OSPF thiết lập mỗi lân cận của nó một trong nhiều trạng thái lân cận OSPF. Một trạng thái lân cận OSPF là một hiểu biết của router về cách làm việc được hoàn tất trong tiến trình thông thường được thực hiện bởi hai router lân cận. Ví dụ, nếu router R1 và R2 kết nối đến cùng LAN và trở thành lân cận, R1 liệt kê trạng thái lân cận cho R2, trong đó hiểu biết của R1 là những gì xảy ra giữa hai router là quá xa. Tương tự, R2 thể hiện trạng thái lân cận cho R1, thể hiện cách nhìn của R2 về những gì xảy ra giữa R2 và R1.

Vì trạng thái lân cận phản ánh các điểm khác nhau trong các tiến trình OSPF thông thường được sử dụng giữa hai router, cần thiết nghiên cứu trạng thái lân cận cùng với những tiến trình và thông điệp OSPF. Tương tự, bằng cách tìm hiểu trạng thái lân cận OSPF và ý nghĩa của chúng, có thể dễ dàng xác định liệu một lân cận OSPF đang hoạt động bình thường, hay có vấn đề xảy ra.

Hình sau đây thể hiện nhiều trạng thái lân cận được sử dụng bởi định dạng trước đây trong mỗi quan hệ lân cận. Hình này thể hiện thông điệp Hello và kết quả trong trạng thái của các lân cận này.



Hình 9.20. Cập nhật định tuyến OSPF

Hai trạng thái đầu tiên, trạng thái Down và Init, khá đơn giản. Trong các trường hợp khi một router biết về một lân cận của nó, nhưng giao tiếp đó lỗi, lân cận được liệt kê ở trạng thái Down. Ngay khi giao tiếp bắt lại, router có thể gửi các Hello, chuyển lân cận đó sang trạng thái Init. Trạng thái này có nghĩa là mối quan hệ lân cận đang được khởi tạo.

Một router chuyển từ Init sang trạng thái two-way khi hai yếu tố sau đây là đúng: một Hello nhận được báo rằng RID của đó router đã được thấy, và router đó đã kiểm tra tất cả các tham số cho lân cận và chúng đã tốt đẹp. Những yếu tố này có nghĩa là router đang sẵn sàng để truyền thông với lân cận. Để làm cho tiến trình này hoạt động, khi mỗi router nhận một Hello từ một lân cận mới, router kiểm tra chi tiết cấu hình của lân cận, như mô tả trước đây. Nếu tất cả đều tốt, thông điệp Hello kế tiếp của router thể hiện RID của lân cận trong danh sách router đã nhìn thấy. Sau khi cả hai router đã kiểm tra các tham số và gửi một Hello liệt kê RID của router khác là “đã nhìn thấy”, cả hai router đã đạt đến trạng thái two-way.

9.5.1.2. Trao đổi cơ sở dữ liệu sơ đồ OSPF

Các router OSPF trao đổi các nội dung về LSDB của nó để cả hai lân cận có bản sao chính xác về cùng LSDB tại cuối của tiến trình trao đổi cơ sở dữ liệu – lý thuyết nền tảng về cách giao thức định tuyến link-state làm việc. Tiến trình có nhiều bước, với nhiều chi tiết hơn được mô tả tại đây. Phần này bắt đầu với việc đánh giá tổng quan về toàn bộ tiến trình, sau đó là chi tiết sâu hơn về mỗi bước.

9.5.1.2.1. Tổng quan về tiến trình trao đổi cơ sở dữ liệu OSPF

Sau khi hai router OSPF đã trở thành lân cận và đạt đến trạng thái two – way, bước kế tiếp có thể không phải là trao đổi thông tin sơ đồ. Trước tiên, dựa trên nhiều yếu tố, router phải quyết định liệu nó trao đổi một cách trực tiếp thông tin sơ đồ, hay hai lân cận sẽ học thông tin sơ đồ lẫn nhau, trong dạng LSA, một cách gián tiếp. Ngay khi một cặp lân cận OSPF biết rằng chúng có thể chia sẻ thông tin sơ đồ trực tiếp, chúng trao đổi dữ liệu sơ đồ (LSA). Sau khi hoàn tất, tiến trình chuyển sang trạng thái duy trì khá yên tĩnh trong đó các router hiếm khi gửi lại các LSA và theo dõi các thay đổi trên mạng.

Tiến trình chung tuân theo như sau, với mỗi bước được giải thích trong phần sau:

Bước 1: Dựa trên loại giao tiếp OSPF, router có thể hoặc không bầu chọn một Designated Router – DR và Backup Designated Router – BDR

Bước 2: Với mỗi cặp router cần trở thành lân cận đầy đủ, trao đổi lẫn nhau các nội dung LSDB của nhau.

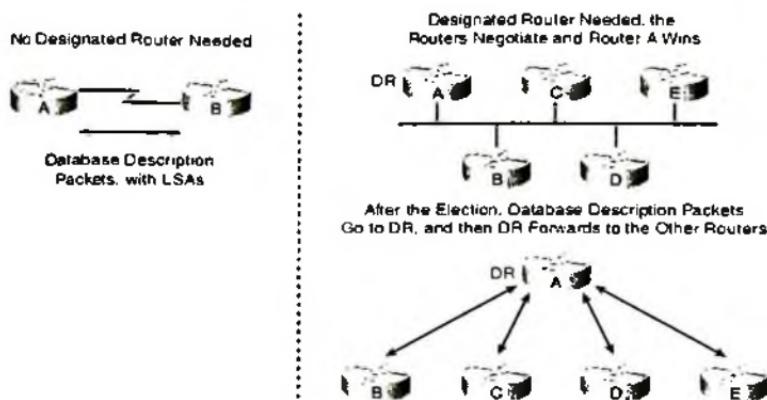
Bước 3: Khi hoàn tất, các lân cận giám sát thay đổi và gửi lại định kì LSA trong trạng thái lân cận đầy đủ.

9.5.1.2.2. Lựa chọn router dành riêng – DR

OSPF xác định rằng một mạng con hoặc là nên hay không nên sử dụng một DR và BDR dựa trên loại giao tiếp OSPF (thỉnh thoảng còn được gọi là loại mạng OSPF). Nhiều loại giao tiếp OSPF tồn tại, nhưng quan tâm đến hai loại: diêm – diêm và quảng bá. (Những loại này có thể được cấu hình với lệnh `ip ospf network type`). Những loại giao tiếp OSPF này tạo nên một tham chiếu chung đến loại giao thức liên kết dữ liệu được sử dụng. Loại liên kết diêm – diêm có mục đích sử dụng trong các liên kết diêm – diêm, và loại quảng bá được sử dụng trong các liên kết dữ liệu hỗ trợ các frame quảng bá, như là LANs.

Hình 9.21 cho thấy một ví dụ điển hình về hai tập lân cận – một sử dụng loại giao tiếp mặc định OSPF diêm – diêm trên một liên kết serial, và một sử dụng liên kết quảng bá trên LAN. Kết quả cuối cùng cho bầu

chọn DR là thông tin sơ đồ được trao đổi chỉ giữa các lân cận với các đường mũi tên trong hình.



Hình 9.21. Các lân cận trong OSPF

Khi không cần DR, các lân cận có thể bắt đầu ngay tiến trình trao đổi sơ đồ, như được thể hiện bên trái. Trong thuật ngữ OSPF, hai router bên trái sẽ tiếp tục làm việc để trao đổi thông tin sơ đồ và trở thành lân cận đầy đủ. Bên phải của hình, phần đầu tiên cho thấy một sơ đồ LAN trong đó việc bầu chọn DR đã được thực hiện, với router A là DR. Với DR, tiến trình trao đổi sơ đồ xảy ra giữa DR và mọi router khác, nhưng không giữa bất kỳ cặp router nào. Kết quả là, tất cả các cập nhật định tuyến đến và đi từ Router A, với router A cần thiết phân phối lại thông tin sơ đồ cho các router khác. Tất cả các router học được tất cả thông tin sơ đồ từ tất cả router khác, nhưng tiến trình chỉ tạo ra sự trao đổi thông tin định tuyến trực tiếp giữa DR và các router không phải DR.

Khái niệm DR ngăn quá tải một mạng con với quá nhiều lưu lượng OSPF khi nhiều router tham gia vào một mạng con. Dĩ nhiên, nhiều router có thể được kết nối vào một LAN, điều này giải thích vì sao DR được yêu cầu cho các router kết nối đến LAN. Ví dụ, nếu 10 router được kết nối đến cùng mạng con LAN, và chúng buộc chuyển các cập nhật OSPF đến 9 router khác, các cập nhập sơ đồ có thể chuyển đi giữa 45 cặp

lân cận khác nhau – với hầu hết tất cả thông tin là dư thừa. Với khái niệm DR, như thể hiện trong hình trên, LAN này yêu cầu các cập nhật định tuyến chỉ giữa DR và chín router khác, giảm thiểu đáng kể việc gửi các thông tin OSPF trên LAN.

Vì DR quan trọng cho trao đổi thông tin định tuyến, việc mất DR có thể làm trì hoãn trong khi hội tụ. OSPF có khái niệm về BDR trên mỗi mạng con, vì thế khi DR lỗi hay mất kết nối đến mạng con, BDR có thể lấy quyền của DR.

Khi cần DR, các router lân cận thực hiện bầu chọn. Để bầu một DR, các router lân cận tìm kiếm hai trường bên trong gói tin Hello chúng nhận và chọn DR dựa trên tiêu chuẩn sau:

- Router gửi Hello với độ ưu tiên OSPF cao nhất trở thành DR.
- Nếu hai hay nhiều router xung đột thiết lập độ ưu tiên cao nhất, router gửi Hello với RID cao nhất chiến thắng.
- Không phải luôn luôn đúng, nhưng thông thường router với độ ưu tiên cao thứ nhì trở thành BDR.
- Thiết lập ưu tiên 0 có nghĩa là router không tham gia vào bầu chọn và có thể không bao giờ trở thành DR hay BDR.
- Khoảng giá trị ưu tiên cho phép router là một ứng viên là 1 đến 255.
- Nếu một ứng viên mới tốt hơn xuất hiện sau khi DR và BDR đã được bầu, ứng viên mới này không thay thế cho DR và BDR hiện tại.

9.5.1.2.3. *Trao đổi cơ sở dữ liệu*

Tiến trình trao đổi cơ sở dữ liệu có thể ít liên quan đến nhiều thông điệp OSPF. Chi tiết của tiến trình có thể được bỏ qua vì mục đích của tài liệu, nhưng tổng quan sơ lược cho một số khái niệm về tiến trình tổng quan.

Sau khi hai router quyết định trao đổi thông tin, chúng không đơn giản gửi nội dung toàn thể cơ sở dữ liệu. Trước tiên, chúng báo cho nhau

danh sách các LSA trong cơ sở dữ liệu riêng của nó – không phải tất cả chi tiết về các LSA, chỉ là danh sách. Mỗi router sau đó so sánh danh sách của router khác với LSDB của riêng nó. Với bất kì LSA mà router không có bản sao đó, router yêu cầu lân cận cung cấp cho bản sao LSA đó, và lân cận gửi LSA đầy đủ cho router.

Khi hai router hoàn tất tiến trình này, chúng được xem như là hoàn tất đầy đủ tiến trình trao đổi cơ sở dữ liệu. Vì thế OSPF sử dụng trạng thái lân cận Full để diễn đạt rằng tiến trình trao đổi cơ sở dữ liệu đã kết thúc.

9.5.1.2.4. Duy trì LSDB trong khi là lân cận đầy đủ

Các lân cận trong trạng thái **Đầy Đủ** vẫn tiếp tục duy trì công việc. Chúng tiếp tục gửi các Hello mỗi chu kì Hello. Số lượng Hello vắng mặt trong thời gian bằng với chu kì Dead nghĩa là kết nối đến lân cận đã bị lỗi. Tương tự, nếu bất kì sơ đồ thay đổi xảy ra, lân cận gửi các bản sao LSA thay đổi mới đến mỗi lân cận để lân cận có thể thay đổi LSDB của nó. Ví dụ, nếu mạng con lỗi, một router cập nhật LSA cho lân cận của nó, và đến lượt các lân cận khác, cho đến khi tất cả mọi router có được bản sao giống nhau về LSDB. Mỗi router có thể sau đó sử dụng SPF để tính toán lại bất kì con đường bị ảnh hưởng bởi mạng con lỗi.

Router tạo mỗi LSA cũng đảm nhận việc gửi lại LSA mỗi 30 phút (mặc định), dù không có thay đổi xảy ra. Tiến trình này khác so với khái niệm distance vector về chu kì cập nhật. Giao thức distance vector gửi các cập nhật đầy đủ trong chu kì ngắn hơn, liệt kê tất cả các con đường (ngoại trừ những con đường do chức năng tránh lặp, như là miền phân tách). OSPF không gửi tất cả các con đường mỗi 30 phút. Thay vào đó, mỗi LSA có một bộ định thời riêng, dựa trên khi LSA được tạo ra. Vì thế, không có thời điểm nào OSPF gửi nhiều thông điệp để gửi lại tất cả LSA. Thay vào đó, mỗi LSA được gửi bởi router đã tạo LSA đó, 30 phút mỗi lần.

Như đã nói, một số router không thử trở thành lân cận đầy đủ. Cụ thể, trên các giao tiếp trong đó DR được bầu, router hoặc là DR hay BDR trở

thành lân cận, nhưng chúng không trở thành lân cận đầy đủ. Những router lân cận không đầy đủ này không trao đổi LSA trực tiếp. Tương tự, lệnh `show ip ospf neighbor` trên một router như vậy liệt kê những router này trong trạng thái two-way như là trạng thái lân cận ổn định thông thường.

9.5.1.2.5. Tổng kết về các trạng thái lân cận

Bảng sau đây liệt kê và mô tả vắn tắt các trạng thái lân cận được đề cập trong chương.

Bảng 9.19. Các trạng thái lân cận

Trạng thái lân cận	Ý nghĩa
Down	Một lân cận đã biết không thể đến được, thường do lỗi bên dưới giao tiếp
Init	Trạng thái trung gian trong đó Hello được nghe từ lân cận, nhưng Hello không thể liệt RID của router đó như đã có
Two-way	Lân cận đã gửi một Hello liệt kê RID của router nội bộ trong danh sách các router đã thấy, cũng báo rằng việc kiểm tra xác nhận lân cận đó đã thành công
Đầy đủ	Cả hai con đường biết chính xác cùng các chi tiết LSDB được điều chỉnh đầy đủ

9.5.1.3. Xây dựng bảng định tuyến IP

Các router OSPF gửi các thông điệp để học hỏi về các lân cận, liệt kê những lân cận này trong bảng lân cận OSPF. Các router OSPF sau đó gửi các thông điệp này để trao đổi dữ liệu sơ đồ với cùng các lân cận đó, lưu trữ thông tin trong bảng sơ đồ OSPF, thông thường được gọi là LSDB hay cơ sở dữ liệu OSPF. Để dienen bảng chính thứ ba được sử dụng bởi OSPF, bảng định tuyến IP, OSPF không gửi bất kỳ thông điệp nào. Mỗi router chạy giải thuật Dijkstra SPF với cơ sở dữ liệu OSPF, lựa chọn các con đường tốt nhất dựa trên tiến trình đó.

Cơ sở dữ liệu sơ đồ OSPF chứa danh sách các chi số mạng con (được gọi là các liên kết, còn gọi là cơ sở dữ liệu link-state). Nó cũng chứa danh sách các router, cùng với liên kết đến mỗi router được kết nối. Mục đích với việc hiểu biết về liên kết và router, một router có thể chạy giải thuật SPF để tính toán các con đường tốt nhất đến tất cả mạng con.

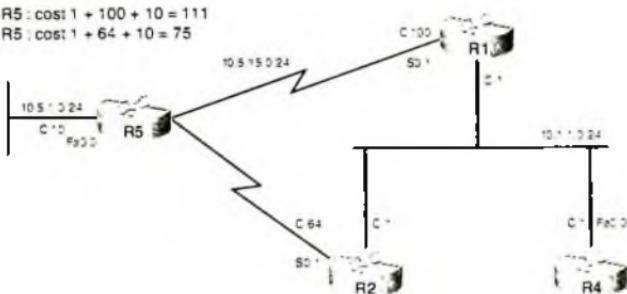
Mỗi router độc lập sử dụng giải thuật SPF Dijkstra, như áp dụng với OSPF LSDB để tìm con đường tốt nhất mà router đó đến mỗi mạng con. Giải thuật tìm đường ngắn nhất từ router đó đến mỗi mạng con trong LSDB. Sau đó router đặt con đường tốt nhất đến mạng con vào bảng định tuyến IP.

OSPF chọn con đường chi phí thấp nhất giữa router và mạng con bằng cách thêm chi phí giao tiếp đầu ra. Mỗi giao tiếp có một chi phí OSPF liên quan với nó. Router tìm kiếm mỗi con đường có thể, thêm chi phí trên giao tiếp ra mà gói tin được chuyển đi trên con đường đó, và sau đó lấy con đường chi phí thấp nhất. Ví dụ, hình sau đây cho thấy một hệ thống mạng với các giá trị chi phí OSPF được liệt kê bên cạnh mỗi giao tiếp. Trong hình này, R4 có hai con đường có thể đến mạng con 10.1.5.0/24. Các con đường như sau, liệt kê mỗi router và giao tiếp ra tương ứng

R4 Fa0/0 – R1 S0/1 – R5 Fa0/0

R4 Fa0/0 – R2 S0/1 – R5 Fa0/0

Route R4 – R1 – R5 : cost 1 + 100 + 10 = 111
 Route R4 – R2 – R5 : cost 1 + 64 + 10 = 75



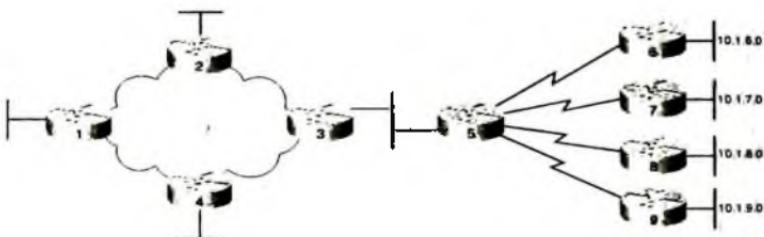
Hình 9.22. Các con đường trong OSPF

Nếu cộng dồn chi phí liên quan đến mỗi giao tiếp, con đường đầu tiên có chi phí 111, con đường thứ hai có tổng cộng 75. Vì thế R4 thêm con đường qua R1 như là con đường tốt nhất và liệt kê địa chỉ IP R1 là địa chỉ IP chặng kế tiếp.

Bây giờ đã thấy cách router OSPF thực hiện chức năng cơ bản nhất của OSPF, phần sau xem xét OSPF rõ hơn, cụ thể là một số điểm thiết kế quan trọng.

9.5.1.4. Thiết kế phân lớp OSPF

OSPF có thể được sử dụng trong một số mạng với rất ít bận tâm về vấn đề thiết kế, chỉ bật OSPF trên tất cả router và nó sẽ hoạt động. Tuy nhiên, trong các mạng lớn, cần hoạch định để có thể sử dụng nhiều chức năng OSPF cho phép làm việc trên các mạng lớn hơn. Xem xét ví dụ sau



Hình 9.23. Phân lớp trong OSPF

Trong mạng này có tất cả 9 router, sơ đồ cơ sở dữ liệu là giống sơ đồ hình vẽ. Với những mạng đơn giản như vậy, có thể chỉ kích hoạt OSPF và nó sẽ hoạt động tốt. Nhưng tương tự một mạng với 900 router thay vì chỉ 9, và hàng ngàn mạng con. Với những mạng như thế, thời gian xử lý yêu cầu để thực hiện SPF có thể làm cho thời gian hội tụ chậm, và router có thể tồn tại nhiều bộ nhớ. Vấn đề trên có thể tóm tắt như sau:

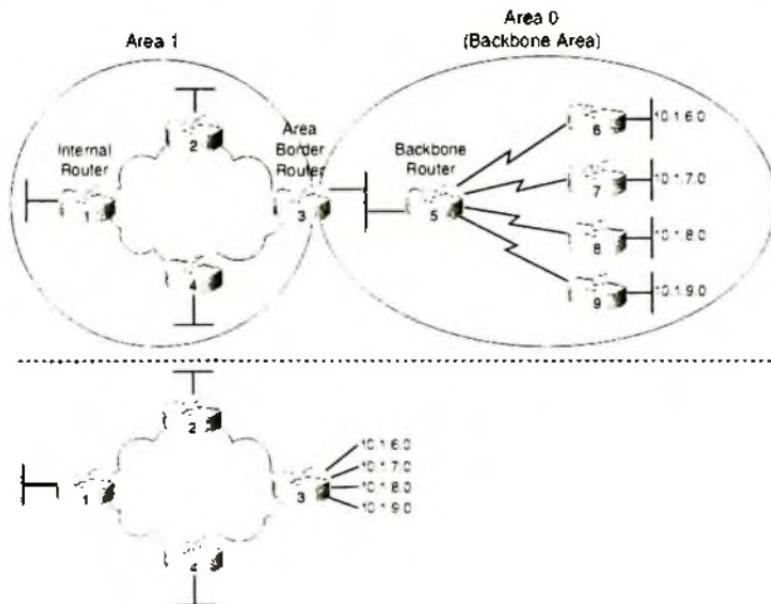
- Một cơ sở dữ liệu sơ đồ lớn hơn cần nhiều bộ nhớ hơn trên mỗi router.
- Xử lý cơ sở dữ liệu sơ đồ lớn hơn với giải thuật SPF yêu cầu xử lý nhiều hơn.
- Một giao tiếp đơn thay đổi, khiến cho mọi router phải chạy SPF lại.

9.5.1.4.1. Vùng OSPF

Sử dụng các vùng (area) OSPF giải quyết nhiều, nhưng không phải tất cả, các vấn đề thông thường nhất khi thực hiện OSPF trên các mạng lớn hơn. Các vùng OSPF phân mạng để các router trên mỗi vùng biết ít thông tin hơn về các mạng con trong các vùng khác – và chúng không biết về các router trong các khu vực khác. Với cơ sở dữ liệu sơ đồ nhỏ

hơn, router tiêu tốn ít bộ nhớ và thời gian xử lý hơn để chạy SPF. Hình 9.24 cho thấy cùng mạng như trên nhưng với hai vùng OSPF, đánh nhãn là Area 1 và Area 0.

Phần dưới của hình vẽ này cho thấy cơ sở dữ liệu sơ đồ trong router 1, 2 và 4. Bằng cách đặt một phần của mạng trong các vùng khác nhau, router bên trong Area 1 được bao bọc khỏi một số chi tiết. Router 3 được xem như là OSPF Area Border Router (ABR), vì nó là biên giữa hai vùng khác nhau. Router 3 không quảng bá thông tin sơ đồ đầy đủ về các phần của mạng trong Area 0 sang router 1, 2 và 4. Thay vào đó, router 3 quảng bá thông tin tóm lược về các mạng con trong Area 0, tác dụng làm cho router 1, 2 và 4 nghĩ sơ đồ trong giống như phần dưới của hình vẽ. Chính vì thế, router 1, 2 và 4 xem mạng có ít router hơn. Kết quả là giải thuật SPF tốn ít thời gian hơn, và cơ sở dữ liệu sơ đồ tốn ít bộ nhớ hơn.



Hình 9.24. Thiết kế phân lớp trong OSPF

Bảng 9.20. Các thuật ngữ trong thiết kế phân lớp OSPF

Thuật ngữ	Mô tả
Area Border Router (ABR)	Một router OSPF với các giao tiếp được kết nối đến khu vực đường trực và đến ít nhất một khu vực khác
Autonomous System Border Router	Một router OSPF kết nối đến các router khác không sử dụng OSPF vì mục đích trao đổi các con đường ngoại mạng đến và ra miền OSPF đó
Router đường trực	Một router trong miền trực
Internal router	Một router trong miền đơn không phải trực
Area	Một tập hợp các router và liên kết chia sẻ cùng thông tin chi tiết LSDB, nhưng không với các router trong các khu vực khác, vì hiệu quả cao hơn
Backbone Area	Một miền OSPF đặc biệt trong đó tất cả các khu vực khác phải kết nối đến, gọi là miền 0.
Con đường ngoại	Một con đường được học từ bên ngoài miền OSPF và sau đó được quảng bá vào trong miền OSPF
Con đường nội miền	Một con đường đến một mạng con bên trong cùng khu vực với router đó
Con đường liên miền	Một con đường đến một mạng con trong một khu vực trong đó router là một phần của mạng con này
Hệ thống tự động	Trong OSPF, điều này tương ứng với một tập các router sử dụng OSPF

9.5.1.4.2. Lợi ích thiết kế vùng OSPF

- Sử dụng các vùng cài tiến hoạt động OSPF theo nhiều cách, cụ thể là trong hệ thống mạng lớn hơn.
- Bộ nhớ yêu cầu LSDB cho mỗi vùng nhỏ hơn
- Router yêu cầu ít CPU để xử lý LSDB nhỏ hơn mỗi vùng với giải thuật SPF, giảm thiểu tiêu tốn CPU và cài tiến thời gian hội tụ
- Giải thuật SPF phải chạy trên các router nội chỉ khi một LSA bên trong vùng thay đổi, vì thế router phải chạy SPF ít thường xuyên hơn.

- Ít thông tin hơn được quảng bá giữa các vùng, giảm thiểu băng thông yêu cầu để gửi LSA.
- Tóm lược thù công có thể chỉ được cấu hình trên ABR và ASBR, vì thế các vùng cho phép bảng định tuyến nhỏ hơn bằng cách cho phép cấu hình tóm lược thù công.

9.5.2. Cấu hình OSPF

Việc cấu hình OSPF chỉ chứa một vài bước yêu cầu, nhưng nó có nhiều bước lựa chọn. Sau khi một thiết kế OSPF đã được lựa chọn – một tác vụ có thể phức tạp trong hệ thống mạng IP lớn hơn – việc cấu hình cũng có thể là đơn giản như kích hoạt OSPF trên mỗi giao tiếp router và đặt giao tiếp đó vào đúng vùng OSPF.

Trong phần này xem xét nhiều ví dụ cấu hình, bắt đầu với mạng OSPF miền đơn, và sau đó là mạng OSPF đa miền. Sau những ví dụ này, cho phép xem xét nhiều thiết lập cấu hình bổ sung. Sau đây là các bước cấu hình tham khảo:

Bước 1: Vào chế độ cấu hình OSPF sử dụng lệnh:

router ospf process-id

Bước 2 (Tùy chọn): Cấu hình router ID bằng:

- Cấu hình lệnh con router – id id – value
- Cấu hình địa chỉ IP trên giao tiếp loopback

Bước 3: Cấu hình một hay nhiều lệnh con network ip – address wildcard-mask area area-id, với bất kì giao tiếp trùng khớp nào được thêm vào vùng.

Bước 4 (Tùy chọn): Thay đổi chu kỳ Hello và Dead giao tiếp sử dụng lệnh con ip ospf hello – interval time và ip ospf dead – interval time

Bước 5 (Tùy chọn): Tác động lựa chọn định tuyến bằng cách thay đổi chi phí trên giao tiếp

- Cấu hình chi phí trực tiếp sử dụng lệnh con:

ip ospf cost value

- Thay đổi băng thông giao tiếp sử dụng lệnh con:

bandwidth value

- Thay đổi kết quả trong công thức để tính chi phí dựa trên băng thông giao tiếp, sử dụng lệnh con:

auto – cost reference – bandwidth value

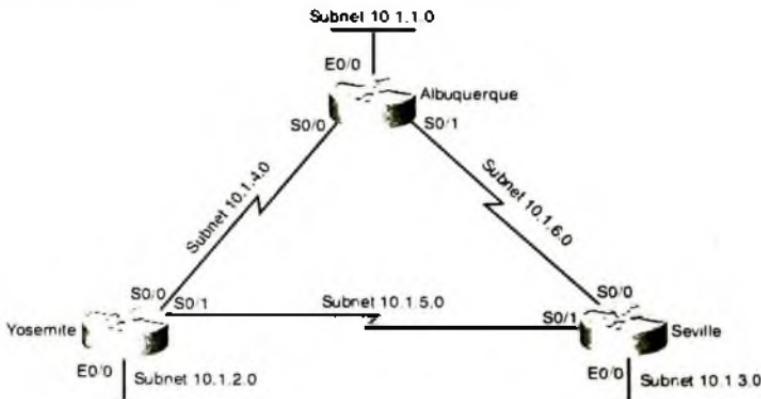
Bước 6 (Tùy chọn): Cấu hình xác thực OSPF

- Trên mỗi giao tiếp sử dụng lệnh con ip ospf authentication
- Với tất cả các giao tiếp trong vùng sử dụng lệnh con area authentication

Bước 7 (Tùy chọn): Cấu hình hỗ trợ cho nhiều con đường cân bằng tải sử dụng lệnh con maximum – paths number

9.5.2.1. Cấu hình vùng đơn OSPF

Cấu hình OSPF khác biệt một ít so với cấu hình RIP khi một vùng đơn OSPF được sử dụng. Cách tốt nhất để mô tả cấu hình và những khác biệt trong cấu hình là sử dụng ví dụ như hình 9.25.



Hình 9.25. Vùng OSPF đơn

Ví dụ 9.3:

```

Interface ethernet 0/0
 ip address 10.1.1.1 255.255.255.0
Interface serial 0/0
 ip address 10.1.4.1 255.255.255.0
Interface serial 0/1
 ip address 10.1.6.1 255.255.255.0

```

```

1
router ospf 1
network 10.0.0.0 0.255.255.255 area 0

```

Việc cấu hình cho phép OSPF trên tất cả ba giao tiếp của Albuquerque. Trước tiên, lệnh **router ospf 1** đặt người dùng vào chế độ cấu hình OSPF. Lệnh **router ospf** có một tham số được gọi là **OSPF process – id**. Trong một số ví dụ, có thể muốn chạy nhiều tiến trình OSPF trên một router đơn, vì thế lệnh **router** sử dụng **process – id** để phân biệt giữa các tiến trình đó. **Process – id** không trùng khớp trên mỗi router, và nó có thể là số nguyên bất kì từ 1 đến 65.535.

Lệnh **network** báo cho router kích hoạt OSPF trên mỗi giao tiếp phù hợp, khám phá các lân cận của giao tiếp đó, giàn giao tiếp vào vùng đó, và quảng bá mạng con có kết nối với mỗi giao tiếp. Trong trường hợp này, lệnh **network 10.0.0.0 0.255.255.255 area 0** phù hợp tất cả ba giao tiếp của Albuquerque.

Ví dụ sau đây cho thấy một cấu hình khác của Albuquerque cũng kích hoạt OSPF trên mọi giao tiếp. Trong trường hợp này, địa chỉ IP cho mỗi giao tiếp là trùng hợp với một lệnh **network**.

Ví dụ 9.4:

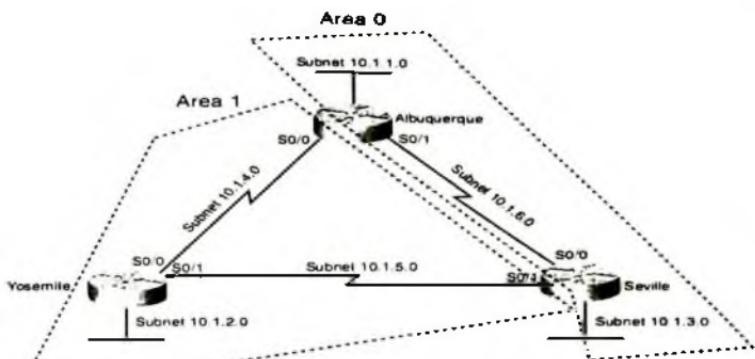
```

interface ethernet 0/0
ip address 10.1.1.1 255.255.255.0
interface serial 0/0
ip address 10.1.4.1 255.255.255.0
interface serial 0/1
ip address 10.1.6.1 255.255.255.0
!
router ospf 1
network 10.1.1.1 0.0.0.0 area 0
network 10.1.4.1 0.0.0.0 area 0
network 10.1.6.1 0.0.0.0 area 0

```

9.5.2.2. Cấu hình OSPF trên nhiều vùng

Cấu hình OSPF trên nhiều vùng là đơn giản khi hiểu cấu hình OSPF trên một vùng đơn. Thiết kế mạng OSPF bằng cách thực hiện các lựa chọn đúng về mạng con nào nên được đặt trong mỗi vùng trước tiên. Sau khi thiết kế hoàn tất, việc cấu hình là khá dễ dàng. Ví dụ, trong hình 9.26 có các mạng con trong Area 1 và Area 0.



Hình 9.26. Cấu hình OSPF trên nhiều vùng

Nhiều vùng là không cần thiết trong những mạng con nhỏ như vậy, nhưng hai vùng được sử dụng trong ví dụ này thể hiện cho cấu hình theo mong muốn.

Ví dụ 9.5:

```

Only the OSPF configuration is shown to conserve space

router ospf 1
  network 10.1.1.1 0.0.0.0 area 0
  network 10.1.4.1 0.0.0.0 area 1
  network 10.1.6.1 0.0.0.0 area 0
Albuquerque#show ip route
Codes: C - connected, S - static, R - RIP, B - mobile, E - BGP
       0 - EIGRP, EX - EIGRP external, G - OSPF, T - OSPF inter area
       41 - OSPF NSSA external type 1, 42 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       1 - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - GDR
       P - periodic downloaded static route

Gateway of last resort is not set

  10.0.0.0/24 is subnetted, 6 subnets
  0    10.1.3.0 [110/65] via 10.1.6.3, 00:01:04, Serial0/1
  0    10.1.2.0 [110/65] via 10.1.4.2, 00:00:39, Serial0/0
  C    10.1.1.0 is directly connected, Ethernet0/0
  0    10.1.5.0 [110/128] via 10.1.4.2, 00:00:39, Serial0/0
  0    10.1.4.0 is directly connected, Serial0/0

Albuquerque#show ip route ospf
  10.0.0.0/24 is subnetted, 6 subnets
  0    10.1.3.0 [110/65] via 10.1.6.3, 00:01:08, Serial0/1
  0    10.1.2.0 [110/65] via 10.1.4.2, 00:00:43, Serial0/0
  C    10.1.1.0 [110/128] via 10.1.4.2, 00:00:43, Serial0/0

```

```
| Only the OSPF configuration is shown to conserve space
router ospf 1
  network 10.0.0.0 0.255.255.255 area 1
Yosemite#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

  10.0.0.0/24 is subnetted, 6 subnets
IA  10.1.0.0 [110/65] via 10.1.6.1, 00:00:34, Serial0/1
IA  10.1.1.0 [110/65] via 10.1.4.1, 00:00:49, Serial0/0
C   10.1.2.0 is directly connected, Ethernet0/0
C   10.1.5.0 is directly connected, Serial0/1
IA  10.1.6.0 [110/128] via 10.1.4.1, 00:00:38, Serial0/0
C   10.1.4.0 is directly connected, Serial0/2
```

Việc cấu hình cần thiết lập đúng chỉ số vùng trên các giao tiếp tương ứng. Ví dụ, lệnh **network 10.1.4.1 0.0.0.0 area 1** phần đầu của ví dụ trước phù hợp với địa chỉ IP của giao tiếp Serial 0/0 Albuquerque, đặt giao tiếp đó vào Area 1. Lệnh **network 10.1.6.1 0.0.0.0 area 0** và **network 10.1.1.1 0.0.0.0 area 0** đặt các giao tiếp Serial 0/0 và Ethernet 0/0 riêng rẽ vào Area 0. Khác với ví dụ ban đầu, Albuquerque không thể cấu hình để phù hợp với tất cả ba giao tiếp với một lệnh con đơn, vì một giao tiếp là ở vùng khác hai giao tiếp còn lại.

Tiếp tục với ví dụ 9.3 lệnh **show ip route ospf** chi tiết kê các con đường học bằng OSPF, trong toàn thể bảng định tuyến. Lệnh **show ip route** liệt kê tất cả ba con đường kết nối, cũng như là các ba con đường học bằng OSPF. Chú ý rằng con đường đến 10.1.2.0 của Albuquerque có O bên cạnh, nghĩa là *intra-area, nội vùng*, vì rằng mạng con bên trong Area 1 và Albuquerque là một phần của Area 1 và Area 0.

Trong ví dụ 9.4, chú ý rằng cấu hình OSPF trên Yosemite yêu cầu chỉ lệnh con đơn **network** vì tất cả các giao tiếp trên Yosemite là ở Area 1.

9.5.2.3. Cấu hình Router ID OSPF

Các router OSPF phải có một Router ID – RID. Để tìm nó, router Cisco sử dụng tiến trình sau đây khi router khởi động lại và bật tiến trình

OSPF. Chú ý rằng khi một trong các bước này xác định RID, tiến trình chấm dứt.

1. Nếu lệnh **con OSPF router-id rid** được cấu hình, giá trị này được sử dụng làm RID
2. Nếu bất kì giao tiếp loopback có một địa chỉ IP được cấu hình và giao tiếp có trạng thái giao tiếp và trạng thái đường truyền là up/up, router lấy giá trị địa chỉ IP cao nhất trong số các giao tiếp loopback up/up đó.
3. Router lấy địa chỉ IP cao nhất trong số tất cả các giao tiếp làm việc

Tiêu chuẩn đầu tiên và thứ ba có nghĩa như sau: RID hoặc là được cấu hình hay được lấy từ địa chỉ IP của giao tiếp làm việc. Còn giao tiếp loopback là một giao tiếp ảo có thể được cấu hình với lệnh **interface loopback 0**, sau đó là lệnh **ip address 192.168.200.1 255.255.255.0**, để tạo một giao tiếp loopback và gán nó một địa chỉ IP. Vì các giao tiếp loopback không phản hồi lại bất kì phản ứng nào, những giao tiếp này có thể là up/up bất kì khi nào IOS hoạt động.

Mỗi router chọn RID OSPF của nó khi OSPF khởi tạo. Việc khởi tạo xảy ra trong suốt quá trình nạp khởi động của IOS. Vì thế khi OSPF bắt đầu, các giao tiếp khác bắt đầu có địa chỉ IP cao hơn, OSPF RID không thay đổi cho đến khi tiến trình OSPF được khởi động lại. OSPF có thể khởi động lại với lệnh **clear ip ospf process**, nhưng tùy thuộc vào tình huống, IOS có thể không thay đổi RID OSPF của nó cho đến lần nạp IOS kế tiếp.

Nhiều lệnh liệt kê OSPF RID của các router khác nhau. Ví dụ, trong ví dụ sau, lần cận đầu tiên của đầu ra lệnh **show ip ospf neighbor** liệt kê Router ID 10.1.5.2, là RID của Yosemite. Sau đó, lệnh **show ip ospf** liệt kê RID của Albuquerque.

Ví dụ 9.6:

```
Albuquerque#show ip ospf neighbor
*
Neighbor ID      Pri  State      Dead Time    Address      Interface
10.1.6.3          1    FULL      00:00:35    10.1.6.3      Serial0
10.1.5.2          1    FULL      00:00:37    10.1.4.2      Serial0/0
Albuquerque#show ip ospf neighbor
Routing Process  ospf 1  with ID 10.1.6.1
! lines omitted for brevity
```

9.5.2.4. Bộ định thời Hello và Dead

Thiết lập mặc định cho bộ định thời Hello và Dead thường làm việc tốt. Tuy nhiên, quan trọng cần chú ý là một sai lệch trên một trong hai thiết lập làm cho hai router gần nhau không trở thành láng cận – hay đạt đến trạng thái two-way. Ví dụ sau liệt kê các chung để thấy thiết lập hiện tại sử dụng lệnh `show ip ospf interface`, được thực hiện từ Albuquerque, khi được cấu hình trong ví dụ da miền OSPF như sau:

Ví dụ 9.7:

```
Albuquerque#show ip ospf interface
Serial0/1 is up, line protocol is up
  Internet Address 10.1.6.1/24, Area 0
  Process ID 1, Router ID 10.1.6.1, Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT.
  Timer intervals configured. Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Index 2/3, flood queue length 8
  Next 0x8(0)/0x0(0)
  Last flood scan length is 2, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.6.3
  Suppress hello for 0 neighbor(s)
Ethernet0/0 is up, line protocol is up
  Internet Address 10.1.1.1/24, Area 0
  Process ID 1, Router ID 10.1.6.1, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router:10.1.6.1, Interface address 10.1.1.1
  No backup designated router on this network
  Timer intervals configured. Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Serial0/0 is up, line protocol is up
  Internet Address 10.1.4.1/24, Area 1
  Process ID 1, Router ID 10.1.6.1, Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT.
  Timer intervals configured. Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Index 1/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.5.2
  Suppress hello for 0 neighbor(s)
```

Chú ý rằng lệnh **show ip ospf interface** liệt kê nhiều chi tiết hơn về hoạt động của OSPF trên mỗi giao tiếp. Ví dụ, lệnh này liệt kê số miền, chi phí OSPF, và bất kì lân cận được biết trên mỗi giao tiếp. Bộ định thời được sử dụng trên giao tiếp đó, bao gồm bộ định thời Dead và Hello, cũng được thể hiện.

Để cấu hình chu kỳ Hello và Dead, có thể sử dụng lệnh **con ip ospf hello - interval value** và **ip ospf dead-interval value**. Chú ý, nếu bộ định thời Hello được cấu hình, IOS tự động cấu hình lại chu kỳ dead của giao tiếp bằng bốn lần chu kỳ Hello.

9.5.2.5. Trọng số (chi phí) OSPF

OSPF tính toán trọng số cho mỗi con đường có thể bằng cách thêm chi phí OSPF cho giao tiếp đầu ra. Chi phí OSPF cho một giao tiếp có thể được cấu hình, hay một router có thể tính toán chi phí dựa trên thiết lập băng thông của giao tiếp đó.

Như đã đề cập, thiết lập băng thông trên một giao tiếp có thể được cấu hình sử dụng lệnh **con bandwidth**. Lệnh này thiết lập tốc độ của giao tiếp router, đơn vị tính là Kbps. Chú ý rằng thiết lập băng thông giao tiếp không phải trùng khớp với thiết lập vật lý giao tiếp. Trên các giao tiếp Ethernet, băng thông phản ánh tốc độ đã thỏa thuận – 10000 (nghĩa là 10.000Kbps hay 10Mbit/s) cho Ethernet 10Mbit/s, và 100.000 (nghĩa là 100.000kbps hay 100Mbit/s) hay 100Mbit/s. Với liên kết serial, mặc định băng thông là 1544 (1544kbps hay tốc độ T1), nhưng IOS không thể điều chỉnh thiết lập này tự động.

IOS chọn chi phí của một giao tiếp dựa trên quy tắc sau đây:

1. Chi phí có thể được thiết lập rõ ràng sử dụng lệnh **con giao tiếp ip ospf cost x**, với giá trị 1 đến 65.535
2. IOS có thể tính toán giá trị dựa trên công thức chung $Ref-BW/Int-BW$, trong đó $Ref-BW$ là băng thông tham khảo mặc định là 100Mbit/s, và $Int-BW$ là thiết lập băng thông giao tiếp.
3. Băng thông tham khảo có thể được cấu hình từ thiết lập mặc định của nó là 100Mbit/s, sử dụng lệnh **con router OSPF auto-cost reference-bandwidth ref-bw**, ảnh hưởng đến tính chi phí giao tiếp mặc định.

Công thức đơn giản để tính chi phí OSPF mặc định có một phần mâu thuẫn. Việc tính toán yêu cầu từ số và mẫu số cùng đơn vị, trong đó **bandwidth** và **auto-cost reference-bandwidth** sử dụng các đơn vị khác nhau. Ví dụ, giao tiếp Ethernet mặc định của phần mềm Cisco sử dụng băng thông 10.000, 10Mbit/s. Băng thông tham khảo mặc định giá trị là 100, nghĩa là 100Mbit/s. Vì thế, chi phí mặc định OSPF trên một giao tiếp Ethernet có thể là 100Mbit/s / 10Mbit/s, sau khi thực hiện cả hai giá trị sử dụng đơn vịMbit/s. Các giao tiếp serial tốc độ cao hơn mặc định băng thông là 1544Mbit/s, với chi phí mặc định là $10^8 / 1544.000\text{bps}$, được làm tròn xuống là khoảng 64, như thể hiện trong giao tiếp S0/1 của hình 9.6. Nếu băng thông tham khảo thay đổi sang 1000, sử dụng lệnh con router OSPF **auto-cost reference bandwidth 1000**, trọng số được tính toán sẽ là 647.

Nguyên nhân chính cho việc thay đổi băng thông tham chiếu là vì router có thể có các giá trị chi phí khác nhau cho các giao tiếp chạy ở các tốc độ 100Mbit/s và cao hơn. Với thiết lập mặc định, một giao tiếp với thiết lập băng thông 100Mbit/s (ví dụ, một giao tiếp FE) và một giao tiếp băng thông 1000Mbit/s (ví dụ, giao tiếp GE). Bằng cách thay đổi băng thông tham chiếu lên 1000, nghĩa là 1000Mbit/s, chi phí mặc định trên giao tiếp băng thông 100Mbit/s sẽ là 10, so với chi phí mặc định là 1 trên một giao tiếp với băng thông là 1000Mbit/s.

9.5.2.6. Xác thực OSPF

Việc xác thực là một trong số các chức năng cấu hình tùy chọn quan trọng nhất cho OSPF. Thiếu xác thực có thể làm cho mạng bị tấn công với một kẻ tấn công kết nối đến mạng đó, làm cho router tin vào dữ liệu OSPF đến từ router “bẩn”. Kết quả, kẻ tấn công có thể dễ dàng thực hiện tấn công từ chối dịch vụ bằng cách làm cho tất cả router gỡ các con đường có sẵn đến tất cả các mạng con, thay vào đó sử dụng các con đường để chuyền các gói tin đến router tấn công. Kẻ tấn công cũng có thể thực hiện tấn công xâm nhập, tìm kiếm thông tin về mạng bằng cách lắng nghe và diễn dịch các thông điệp OSPF.

OSPF hỗ trợ ba dạng xác thực – một được gọi là xác thực **rõ ràng** (nghĩa là không xác thực), một sử dụng mật khẩu văn bản đơn giản và

chính vì thế dễ phá vỡ và một sử dụng MD5, trong đó MD5 là lựa chọn tin cậy nhất. Ngay khi router cấu hình xác thực OSPF trên một giao tiếp, router phải vượt qua tiến trình xác thực cho mọi thông điệp OSPF, với mọi router lân cận trên giao tiếp đó. Điều này nghĩa là mỗi router lân cận trên giao tiếp đó phải có cùng dạng xác thực và cùng mật khẩu xác thực được cấu hình.

Cấu hình có thể sử dụng hai lệnh con giao tiếp trên mỗi giao tiếp – một để kích hoạt một dạng xác thực cụ thể, và một để thiết lập mật khẩu được dùng cho xác thực.

Ví dụ 9.8 cho thấy một ví dụ cấu hình với xác thực mật khẩu đơn giản trên giao tiếp Fa0/0, và xác thực MD5 được thực hiện trên Fa0/1.

Ví dụ 9.8:

```

! The following commands enable OSPF simple password authentication and
! set the password to a value of 'key-t1'
R1#show running-config
! lines omitted for brevity
interface FastEthernet0/0
  ip ospf authentication
  ip ospf authentication-key key-t1
! Below, the neighbor relationship formed, proving that authentication worked.
R1# show ip ospf neighbor fa 0/0
Neighbor ID      Pri  State          Dead Time    Address          Interface
2.2.2.2          1    FULL/BDR      00:00:37    10.1.1.2        FastEthernet0/0
! Next, each interface's OSPF authentication type can be seen in the last line
! or two in the output of the show ip ospf interface command.
R1# show ip ospf interface fa 0/0
! Lines omitted for brevity
Simple password authentication enabled

! Below, R1's Fa0/1 interface is configured to use type 2 authentication.
! Note that the key must be defined with
! the ip ospf message-digest-key interface subcommand.
R1#show running-config
! lines omitted for brevity
interface FastEthernet0/1
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 key-t2
! Below, the command confirms type 2 (MD5) authentication, key number 1.
R1# show ip ospf interface fa 0/1
! Lines omitted for brevity
Message digest authentication enabled
Youngest key id is 1

```

Phản khó khăn nhất khi cấu hình là nhớ cú pháp lệnh được dùng trên hai lệnh con giao tiếp. Chú ý rằng lệnh con giao tiếp được sử dụng để cấu hình các khóa xác thực, với cú pháp khác nhau tùy thuộc vào loại xác thực. Bảng sau đây liệt kê ba loại xác thực OSPF và các lệnh tương ứng.

Bảng 9.21. Xác thực OSPF

Loại	Ý nghĩa	Lệnh để đặt xác thực	Mật khẩu được cấu hình với
0	None	<code>ip ospf authentication null</code>	-
1	Văn bản thuần	<code>ip ospf authentication</code>	<code>ip ospf authentication-key key-value</code>
2	MD5	<code>ip ospf authentication message-digest</code>	<code>ip ospf message-digest-key key-number md5 key-value</code>

Chú ý rằng mật khẩu hay khóa xác thực, được giữ ở văn bản thuần trong cấu hình, trừ khi thêm lệnh cấu hình toàn cục `service password-encryption`.

Thiết lập mặc định sử dụng loại xác thực 0 – có nghĩa là không xác thực có thể được ghi đè trên một miền – đến – miền bằng sử dụng lệnh `area authentication` của router. Ví dụ, router R1 ở trên có thể được cấu hình với lệnh con router `authentication message-digest`, làm cho router mặc định sử dụng xác thực MD5 trên tất cả giao tiếp của nó trong Area 1. Tương tự, lệnh con router `area 1 authentication` cho phép xác thực mật khẩu đơn cho tất cả giao tiếp trên Area 1, làm cho lệnh con giao tiếp `ip ospf authentication` không cần thiết. Chú ý rằng khóa xác thực (mật khẩu) phải vẫn được cấu hình với lệnh con giao tiếp đã xem xét trong bảng trên.

9.5.2.7. Cân bằng tải OSPF

Khi OSPF sử dụng SPF để tính trọng số cho một trong nhiều con đường để đến một mạng con, một con đường có thể có trọng số thấp nhất, vì thế OSPF đặt con đường đó vào bảng định tuyến. Tuy nhiên, khi trọng số xung đột, router có thể đặt đến 16 con đường chỉ bằng nhau khác nhau vào bảng định tuyến (mặc định là bốn con đường) dựa trên thiết lập lệnh con router `maximum-paths`. Ví dụ, nếu một mạng có sáu

con đường giữa các phần của mạng, và muốn tất cả các con đường được sử dụng, các router có thể được cấu hình với lệnh **maximum – paths 6** dưới lệnh **router ospf**.

Khái niệm khác có liên quan đến các router sử dụng các con đường này đó là cơ chế cân bằng tải. Một router có thể cân bằng tải các gói tin trên mỗi gói. Ví dụ, nếu router có ba con đường OSPF chỉ phi bằng nhau cho cùng mạng con trong bảng định tuyến, router có thể gửi gói tin kế tiếp qua con đường đầu tiên, gói tin tiếp theo qua con đường thứ hai, gói tin tiếp theo qua con đường thứ ba, và sau đó bắt đầu lại với con đường đầu tiên cho gói tin kế tiếp.

EIGRP cung cấp một tập các chức năng và thuộc tính mạnh mẽ với mục đích chính là học các con đường IP. EIGRP hội tụ rất nhanh, và loại bỏ một số nhược điểm của OSPF. Cụ thể, EIGRP yêu cầu ít thời gian xử lý hơn, ít bộ nhớ hơn và ít thiết kế hơn OSPF. Điểm yếu duy nhất của EIGRP và nó dành riêng cho Cisco, vì thế nếu hệ thống mạng sử dụng một số router không phải là Cisco, EIGRP không thể sử dụng được trên các router đó.

EIGRP không được xếp vào loại giao thức distance vector hay link – state. Cisco đôi lúc nói EIGRP là giao thức định tuyến distance vector nâng cao, nhưng trong một số trường hợp khác, Cisco lại nói EIGRP là một loại khác: đó là giao thức định tuyến lai cân bằng.

Chương này bắt đầu bằng cách đánh giá một số khái niệm chính về cách EIGRP thực hiện công việc. Phần thứ hai của chương giải thích cấu hình EIGRP.

9.6.1. Hoạt động và khái niệm EIGRP

Giống OSPF, EIGRP tuân theo ba bước chung để có thể thêm các con đường vào bảng định tuyến IP:

1. *Tìm các lân cận*: EIGRP router gửi thông điệp Hello để tìm các lân cận và thực hiện các kiểm tra thông số cơ bản để xác định router nào sẽ trở thành lân cận.

2. *Trao đổi sơ đồ*: Các lân cận trao đổi các cập nhật sơ đồ đầy đủ trong khi mỗi quan hệ lân cận được tạo lập, và chỉ các cập nhật một phần cần thiết dựa trên các thay đổi của sơ đồ mạng.
3. *Lựa chọn đường*: Mỗi router phân tích bảng sơ đồ EIGRP của riêng nó, lựa chọn con đường có trọng số thấp nhất để đến mỗi mạng con.

Kết quả của những bước này, IOS duy trì ba bảng EIGRP quan trọng.

- Bảng lân cận EIGRP liệt kê các router lân cận và được xem với lệnh `show ip eigrp neighbor`.
- Bảng sơ đồ EIGRP chứa tất cả thông tin được học từ các lân cận EIGRP và được thể hiện với lệnh `show ip eigrp topology`.
- Cuối cùng, bảng định tuyến IP chứa tất cả các con đường tốt nhất và được thể hiện với lệnh `show ip route`.

Phản tiếp theo mô tả một số chi tiết về cách EIGRP xây dựng mối quan hệ lân cận, trao đổi các con đường, và thêm các mục vào bảng định tuyến IP. Ngoài những bước này, phần này giải thích một số thuật ngữ EIGRP duy nhất được sử dụng khi hội tụ và phản ứng lại với những thay đổi trong một hệ thống mạng – những ý nghĩa không bao giờ được thấy với các loại giao thức định tuyến khác.

9.6.1.1. Lân cận EIGRP

Một lân cận EIGRP là một router sử dụng EIGRP khác, được kết nối đến cùng mạng con, với router đó sẵn sàng trao đổi thông tin sơ đồ EIGRP. EIGRP sử dụng các thông điệp EIGRP, gửi đến địa chỉ quảng bá nhóm 224.0.0.10, để khám phá tự động các lân cận. Một router học các lân cận bằng cách nhận Hello EIGRP này.

Yêu cầu lân cận: Các router thực hiện một số kiểm tra cơ bản về mỗi lân cận trước khi router đó trở thành một lân cận EIGRP. Một lân cận EIGRP là router đã được nhận một Hello EIGRP. Sau đó router kiểm tra các thiết lập sau đây để xác định liệu router đó có được cho phép trở thành một lân cận:

- Nó phải vượt qua tiến trình xác thực
- Nó phải sử dụng cùng số AS được cấu hình
- Địa chỉ IP nguồn được sử dụng bởi Hello của các lân cận phải cùng mạng con.

Việc kiểm tra xác thực khá là rõ ràng. Nếu xác thực được cấu hình, hai router phải sử dụng *cùng loại xác thực* và *cùng khóa xác thực*. Cấu hình EIGRP bao gồm các tham số được gọi là *số hệ thống tự động (ASN)*, phải giống nhau trên hai router lân cận. Cuối cùng, địa chỉ IP được sử dụng để gửi các thông điệp Hello EIGRP – địa chỉ IP giao tiếp riêng của router – phải trong khoảng địa chỉ trên đó mạng con của router khác có kết nối đến.

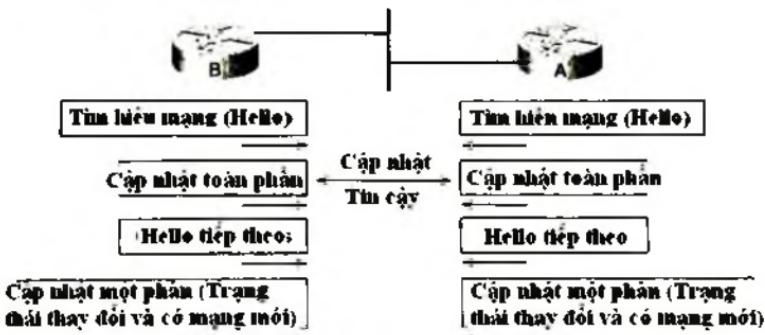
Quan hệ lân cận EIGRP đơn giản hơn nhiều so với OSPF. EIGRP không có khái niệm bổ sung về lân cận đầy đủ như là OSPF, và không có trạng thái lân cận như OSPF. Ngay khi một lân cận EIGRP được phát hiện và vượt qua kiểm tra xác thực cơ bản, router đó trở thành lân cận. Lúc này, hai router có thể bắt đầu trao đổi cho nhau các thông tin sơ đồ. Các lân cận gửi các Hello qua mỗi chu kì EIGRP Hello. Một router xem một lân cận EIGRP của nó không thể đến được nữa sau khi Hello của lân cận đó không thể xuất hiện trong khoảng thời gian được xác định bởi *bộ định thời Hold EIGRP* – thời gian tương ứng với bộ định thời *OSPF Dead*.

9.6.1.2. Trao đổi sơ đồ thông tin EIGRP

EIGRP sử dụng các thông điệp cập nhật EIGRP để gửi thông tin sơ đồ đến các lân cận. Những thông điệp cập nhật này có thể được gửi đến địa chỉ IP quảng bá nhóm 224.0.0.10, nếu router gửi cần cập nhật nhiều router trên cùng một mạng con; ngược lại các cập nhật được gửi đến địa chỉ IP riêng của mỗi lân cận cụ thể. (Thông điệp Hello luôn được gửi đến 224.0.0.10). Không như OSPF, không có khái niệm về router dành riêng – DR hay BDR, nhưng sử dụng các gói tin quảng bá nhóm trên LAN cho phép EIGRP trao đổi thông tin định tuyến với tất cả các lân cận trên LAN một cách hiệu quả.

Các lân cận sử dụng các cập nhật định tuyến đầy đủ hay một phần, như thể hiện trong hình 9.27. Một cập nhật đầy đủ nghĩa là một router gửi

thông tin về tất cả các con đường biết trước, trong khi cập nhật một phần chưa chỉ thông tin về các con đường thay đổi gần nhất. Cập nhật đầy đủ xuất hiện khi các lân cận được thiết lập lần đầu. Sau đó, các lân cận gửi chỉ cập nhật một phần để phản ứng với thay đổi của một con đường.



Hình 9.27. Hoạt động của định tuyến EIGRP

9.6.1.3. Tính toán con đường tốt nhất cho bảng định tuyến

Tính toán trọng số là một trong những chức năng thú vị nhất của EIGRP. EIGRP sử dụng một trọng số phức hợp, được tính toán như là hàm của băng thông và độ trì hoãn. Việc tính toán cũng chứa tài giao tiếp và độ tin cậy giao tiếp. EIGRP tính trọng số cho mỗi con đường có thể bằng cách chèn giá trị trong số phức hợp và một công thức.

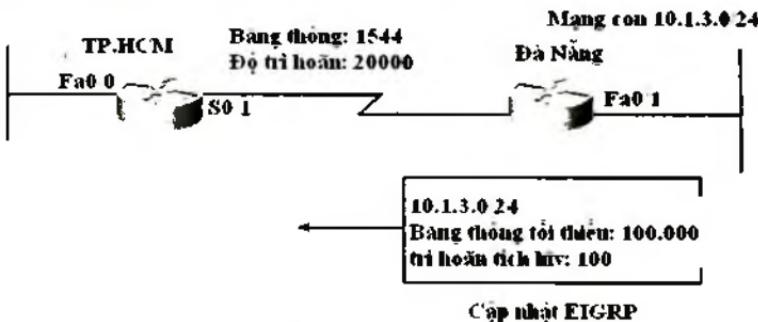
Công thức tính trọng số của EIGRP như sau:

$$\text{Metric} = \left(\left(\frac{10^7}{\text{bảng tần thấp nhất}} \right) + \text{giá trị trung bình} \right) * 256$$

Trong công thức này, thuật ngữ băng thông thấp nhất đại diện cho liên kết băng thông thấp nhất trong con đường, sử dụng đơn vị kbps. Ví dụ, nếu liên kết thấp nhất trong một con đường là 10Mbit/s, phần đầu tiên của công thức là $10^7/10^4$, bằng với 1000. Sử dụng 10^4 trong công thức vì 10Mbit/s tương ứng với 10.000kbps (10^4). Giá trị trì hoãn tích lũy được sử dụng trong công thức là tổng của tất cả các giá trị trì hoãn trên

tất cả các liên kết trong con đường đó, sử dụng đơn vị là “10 lần μ s”. Có thể thiết lập cả băng thông và trì hoãn cho mỗi liên kết, sử dụng lệnh con giao tiếp **bandwidth** và **delay**.

Các cập nhật EIGRP liệt kê mặt nạ và chỉ số mạng con, cùng với độ trì hoãn tích lũy, băng thông tối thiểu, cùng với các phần không sử dụng thông thường khác của trọng số phức hợp. Router sau đó xem các thiết lập băng thông và độ trì hoãn trên giao tiếp trong đó cập nhật được nhận và tính toán một trọng số mới. Ví dụ hình 9.28 cho thấy Albuquerque học từ mạng con 10.1.3.0/24 từ Seville. Cập nhật liệt kê một băng thông tối thiểu là 100.000 kbps và độ trì hoãn tích lũy là 100 μ s. RI có một băng thông giao tiếp được thiết lập là 1544 kbps – băng thông mặc định trên giao tiếp serial – và độ trì hoãn là 20.000 μ s.



Hình 9.28. Cập nhật định tuyến EIGRP

Trong trường hợp này, Albuquerque phát hiện rằng băng thông giao tiếp S0/1 của nó là thấp hơn băng thông tối thiểu đã quảng bá 100.000, vì thế Albuquerque sử dụng băng thông mới, thấp hơn này trong tính toán trọng số. (Nếu giao tiếp S0/1 của Albuquerque có băng thông 100.000 hay hơn trong trường hợp này), Albuquerque sẽ thay vì sử dụng băng thông tối thiểu liệt kê trong cập nhật EIGRP từ Seville). Albuquerque cũng thêm độ trì hoãn giao tiếp S0/1 (20.000 μ s, được chuyển thành 2000 lần 10 μ s trong công thức) sang trì hoãn tích lũy nhận được từ Seville trong cập nhật đó. Kết quả trong tính toán trọng số như sau:

$$\text{Metric} = \left(\left\lceil \frac{10^7}{1544} \right\rceil + (10 + 2000) \right) * 256 = 2,172,416$$

Nếu tồn tại nhiều con đường đến mạng con 10.1.3.0/24, Albuquerque sẽ cùng tính trọng số cho những con đường này và sẽ chọn con đường với trọng số thấp nhất (tốt nhất) để thêm vào bảng định tuyến. Nếu trọng số xung đột, mặc định router đặt bốn con đường trọng số bằng nhau vào bảng định tuyến, gửi lưu lượng qua mỗi con đường. Phần tiếp theo "Con đường EIGRP tối đa" giải thích một ít chi tiết về cách EIGRP có thể thêm nhiều con đường trọng số bằng nhau, và nhiều con đường trọng số không bằng nhau vào bảng định tuyến.

9.6.1.4. Khoảng cách khả thi và khoảng cách được báo cáo

Ví dụ trên cho thấy một số điều cơ sở thuận tiện để xác định hai khái niệm EIGRP như sau:

- Khoảng cách khả thi (FD – Feasible Distance): trọng số của con đường tốt nhất đến mỗi mạng con, được tính toán trên một router.
- Khoảng cách báo cáo (RD – Reported Distance): Trọng số được tính toán trên router lân cận và sau đó được báo cáo và được học trong cập nhật EIGRP

Ví dụ, trong hình trên Albuquerque tính toán khoảng cách có thể là 2.195.631 để đến mạng con 10.1.3.0/24 qua Seville. Seville cũng tính trọng số của nó để đến mạng con 10.1.3.0/24. Seville cũng liệt kê trọng số đó trong cập nhật EIGRP được gửi đến Albuquerque. Thực ra, dựa trên thông tin của hình trên, FD của Seville để đến mạng con 10.1.3.0/24, sau đó được biết bởi Albuquerque như là RD của Seville để đến 10.1.3.0/24, có thể dễ dàng tính được như sau:

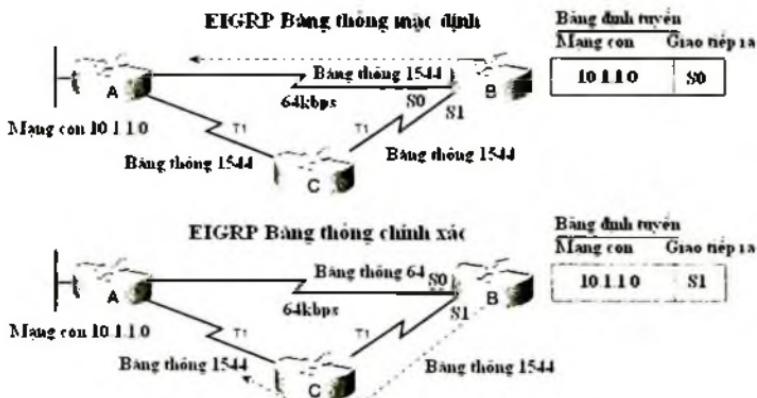
$$\left(\left\lceil \frac{10^7}{100.000} \right\rceil + (10) \right) * 256 = 28.160$$

RD và FD được đề cập trong phần thảo luận kế tiếp về cách EIGRP phản ứng và hội tụ khi một thay đổi xảy ra trong hệ thống mạng.

9.6.1.5. *Khả năng thông báo trước về băng thông trên các liên kết Serial*

Trong số tin cậy của EIGRP cho nó khả năng lựa chọn con đường chứa nhiều router hơn nhưng với liên kết nhanh hơn. Tuy nhiên, để đảm bảo rằng các con đường đúng được chọn, phải thực hiện việc cấu hình thiết lập băng thông và trì hoãn đầy đủ. Cụ thể các liên kết serial mặc định băng thông là 1544kbps và độ trì hoãn 20000μs. Tuy nhiên, IOS không thể tự động thay đổi thiết lập băng thông và trì hoãn dựa trên tốc độ liên kết Serial lớp 1. Vì thế, sử dụng thiết lập băng thông mặc định trên liên kết Serial có thể gây ra các lỗi.

Hình 9.29 cho thấy thiết lập mặc định của băng thông và cách EIGRP sử dụng con đường tốt hơn (nhanh hơn) khi băng thông được thiết lập chính xác. Hình trên tập trung vào con đường đến mạng con 10.1.1.0/24 của router B. Trong phần đầu của hình, tất cả các liên kết serial sử dụng liên kết mặc định 64kbps.



Hình 9.29. Trọng số cập nhật EIGRP

9.6.1.6. *Hội tụ EIGRP*

Tránh lặp là một trong những vấn đề khó khăn nhất với bất kỳ giao thức định tuyến nào. Giao thức định tuyến distance vector vượt qua vấn đề này với nhiều công cụ, một số trong đó làm cho thời gian hội tụ lớn sau khi liên kết hỏng. Giao thức link-state vượt qua vấn đề bằng cách

mỗi router giữ một sơ đồ đầy đủ của mạng, vì thế bằng cách chạy một mô hình toán học, router có thể tránh bất kì vòng lặp nào.

EIGRP tránh lặp bằng cách giữ một số thông tin sơ đồ cơ bản, nhưng nó tránh tốn quá nhiều CPU và bộ nhớ bằng cách giữ những thông tin tắt. Khi một router học nhiều con đường đến mạng con, nó đặt con đường tốt nhất vào bảng định tuyến IP. EIGRP giữ một số thông tin sơ đồ vì cùng nguyên nhân với OSPF – để nó có thể hội tụ rất nhanh và sử dụng một con đường mới không gây nên lặp. Điều cần thiết là, EIGRP giữ một bản ghi của mỗi router chặng kế tiếp, và một số chi tiết có liên quan đến những con đường này, nhưng không có thông tin về sơ đồ bên dưới router chặng kế. Thông tin sơ đồ này không yêu cầu giải thuật SPF phức tạp, nên hội tụ nhanh và ít tốn thời gian, và không có vòng lặp.

Tiến trình hội tụ EIGRP sử dụng một trong hai nhánh ngữ nghĩa của nó, dựa trên liệu con đường lỗi có hay không một con đường có thể thành công. Nếu có một con đường có thể thành công, router có thể ngay tức thì sử dụng con đường đó. Nếu không, router phải sử dụng một tiến trình hội và trả lời để tìm con đường khác không có lặp. Cả hai tiến trình làm cho hội tụ nhanh hơn, thường là nhanh hơn 10 giây, nhưng tiến trình yêu cầu và phản hồi mất thời gian hơn.

9.6.1.6.1. Con đường có thể kế nhiệm EIGRP

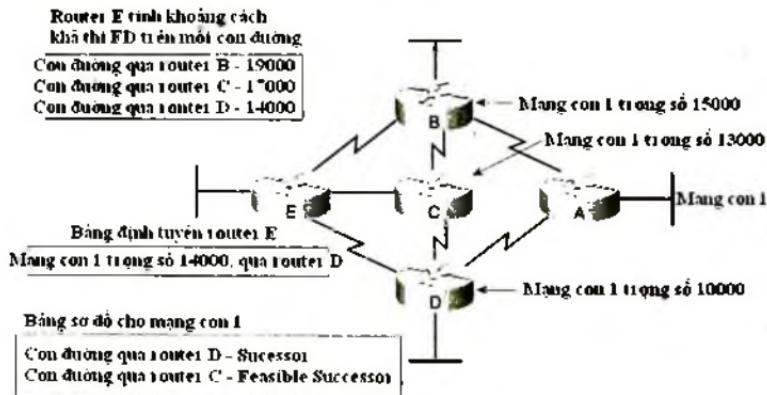
EIGRP tính toán trọng số cho mỗi con đường đến mỗi mạng con. Với một mạng con cụ thể, con đường với trọng số tốt nhất được gọi là kế nhiệm, khi đó router điền vào bảng định tuyến với con đường này.

Các con đường khác đến cùng mạng con đó – các con đường có trọng số cao hơn FD, trọng số khác thi cho con đường đó – EIGRP cần xác định con đường nào được sử dụng tức thi nếu con đường hiện tại lỗi, mà không tạo ra vòng lặp. EIGRP chạy một giải thuật đơn giản để xác định con đường nào có thể sử dụng, lưu con đường dự phòng không lặp đó trong bảng sơ đồ và sử dụng chúng nếu con đường tốt nhất hiện tại gặp lỗi. Những con đường có thể được sử dụng tức thi được gọi là con đường có thể kế nhiệm, vì chúng có thể được sử dụng tức thi khi con

đường hiện tại lỗi. Một router xác định liệu một con đường là có thể kế nhiệm dựa trên điều kiện khả thi như sau:

“Nếu RD của một con đường là nhỏ hơn con đường khả thi FD, con đường này là con đường kế nhiệm khả thi”

Dù rằng về kĩ thuật là đúng, định nghĩa này dễ hiểu hơn nhiều so với ví dụ trên. Hình vẽ đó mô tả cách EIGRP chỉ ra con đường nào là có thể kế nhiệm với mạng con 1. Trong hình đó, router E học ba con đường đến mạng con 1, từ router B, C và D. Sau khi tính toán trọng số mỗi con đường, dựa trên băng thông và thông tin trì hoãn nhận được từ cập nhật định tuyến và trên giao tiếp đầu ra tương ứng của router E, router E thấy rằng con đường qua router D có trọng số thấp nhất, vì thế router E thêm con đường đó vào trong bảng định tuyến của nó, như thế hiện. Khoảng cách khả thi FD là trọng số được tính cho con đường này, giá trị là 14.000 trong trường hợp đó.



Hình 9.30. Con đường kế nhiệm trong EIGRP

EIGRP xác định liệu một con đường có thể kế nhiệm nếu khoảng cách được báo cho con đường đó (trọng số được tính toán trên lân cận đó) là nhỏ hơn trọng số được tính toán tốt nhất của nó (FD). Khi lân cận có trọng số thấp hơn cho con đường của nó đến mạng con trong câu hỏi, con đường đó được trả lời là phù hợp với điều kiện có thể. Ví dụ, router

E tính toán một trọng số khả thi (FD) là 14.000 trên con đường tốt nhất của nó (qua router D). Trọng số được tính của router E – khoảng cách được báo cáo của con đường đó – thấp hơn 14.000. Kết quả là E biết rằng con đường tốt nhất của C cho mạng con đó có thể không trỏ đến router E, vì thế Router R tin rằng nó có thể bắt đầu sử dụng con đường đó qua router C và không gây ra lặp. Kết quả, router E thêm một con đường qua router C vào bảng sơ đồ như là một con đường có thể kế nhiệm. Ngược lại, khoảng cách được báo cáo của router B là 15000, lớn hơn FD của router E là 14000, vì thế router E không nhận ra con đường qua router B là một con đường có thể kế nhiệm.

Nếu con đường đến mạng con 1 qua router D lỗi, router E có thể tức thì đặt con đường qua router C vào bảng định tuyến mà không gây ra lặp. Sự hội tụ có thể ngay tức thì trong trường hợp này.

9.6.1.6.2. Tiến trình truy vấn và phản hồi

Khi một con đường lỗi và không có kế nhiệm khả thi, EIGRP sử dụng một giải thuật phân tán được gọi là Diffusing Update Algorithm (DUAL). DUAL gửi các truy vấn tìm kiếm một con đường không lặp để đến một mạng con trong câu hỏi. Khi một con đường mới được tìm thấy, DUAL thêm nó vào bảng định tuyến.

Tiến trình EIGRP DUAL đơn giản sử dụng các thông điệp để xác nhận rằng một con đường tồn tại và và không thể tạo ra lặp, trước khi quyết định thay thế con đường lỗi với một con đường khác. Ví dụ trong hình 9.30, tường tượng rằng cả hai router C và D bị lỗi. Router E không có một con đường kế nhiệm khả thi đến mạng con 1, nhưng có một con đường vật lý có thể qua router B. Để sử dụng con đường này, router E gửi thông điệp truy vấn EIGRP đến các lân cận đang làm việc của nó. Con đường của router B đến mạng con 1 vẫn đang làm việc tốt, vì thế router B phản hồi cho router E với thông điệp phản hồi EIGRP, đơn giản thông báo chi tiết về con đường đang hoạt động đến mạng con 1 và xác nhận con đường đó vẫn sẵn sàng. Router E có thể sau đó thêm một con đường mới đến mạng con 1 vào bảng định tuyến của nó, mà không sợ lặp.

Thay một con đường lỗi với một kế nhiệm khác thi mất một khoảng thời gian rất ngắn, thường là nhỏ hơn một hay hai giây. Khi các truy vấn và phản hồi được yêu cầu, sự hội tụ có thể tốn ít thời gian hơn, nhưng trong hầu hết các mạng, hội tụ có thể xảy ra trong khoảng thời gian nhỏ hơn 10 giây.

9.6.1.6.3. *Tóm tắt về EIGRP và so sánh với OSPF*

EIGRP là một giao thức định tuyến nội vì nhiều nguyên nhân. Nó làm việc tốt, hội tụ nhanh trong khi tránh lặp bên cạnh hiệu quả như là khả năng cân bằng tải không đều. Nó không yêu cầu nhiều cấu hình hay nhiều hoạch định, thậm chí khi sử dụng để hỗ trợ cho các mạng lớn hơn.

EIGRP có thể có thuận lợi khác không quan trọng như trong những năm gần đây: hỗ trợ Novell's IPX và Apple AppIlk. Router có thể sử dụng EIGRP để học các con đường IP, IPX, và AppleTalk, với cùng chức năng thực thi.

Bảng 9.22. So sánh EIGRP và OSPF

Chức năng	EIGRP	OSPF
Hội tụ nhanh	Yes	Yes
Ngăn vòng lặp	Yes	Yes
Gửi cập nhật định tuyến một phần, quảng bá chỉ các thông tin thay đổi hoặc mới	Yes	Yes
Không phân lớp; vì thế hỗ trợ gộp đường tự động và VLSM	Yes	Yes
Cho phép gộp đường thủ công tại bất kì router nào	Yes	No
Gửi thông tin định tuyến sử dụng IP quảng bá nhóm trên LAN		
Sử dụng khái niệm router dành riêng trên LAN	No	Yes
Thiết kế mạng linh động mà không cần tạo các khu vực	Yes	No
Hỗ trợ cân bằng tải trọng số giống và không giống nhau	Yes	No
Trọng số tin cậy dựa trên băng thông và độ trì hoãn	Yes	No
Có thể quảng bá con đường IP, IPX, Applelk	Yes	No
Chuẩn chung	No	Yes

9.6.2. Cấu hình và xác nhận EIGRP

Cấu hình EIGRP căn bản khá giống RIP và OSPF. Lệnh **router eigrp** kích hoạt cấu hình EIGRP và đưa người dùng vào chế độ cấu hình EIGRP, trong đó một hay nhiều lệnh **network** được cấu hình. Với mỗi giao tiếp phù hợp với một lệnh **network**, EIGRP thử phát hiện các lân cận trên giao tiếp đó, và EIGRP quảng bá mạng con được kết nối với giao tiếp đó.

Phần này đánh giá cấu hình EIGRP, bao gồm nhiều chức năng tùy chọn. Nó cũng giải thích ý nghĩa của đầu ra của nhiều lệnh **show** để trợ giúp kết nối phần lý thuyết được xem xét trong phần đầu của chương với việc triển khai thực tế EIGRP trong IOS. Danh sách cấu hình sau đây liệt kê các tác vụ cấu hình chính được xem xét trong chương này.

Bước 1: Vào chế độ cấu hình EIGRP, và xác định EIGRP ASN bằng cách sử dụng lệnh **router eigrp as-number**

Bước 2: Cấu hình một hay nhiều lệnh **network ip-address**. Điều này kích hoạt EIGRP trên bất kì giao tiếp phù hợp nào và làm cho EIGRP có thể quảng bá các mạng con có kết nối.

Bước 3: (Tùy chọn) Thay đổi bộ định thời Hello và Hold sử dụng lệnh **ip hello-interval eigrp asn time** và **ip hold-time eigrp asn time**.

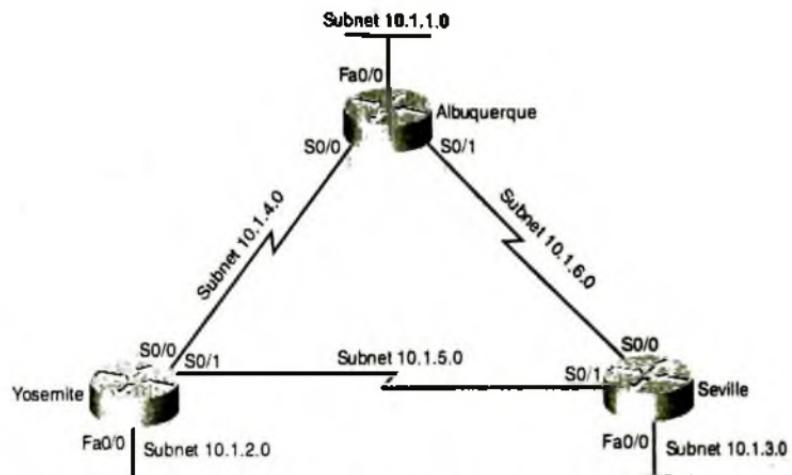
Bước 4: (Tùy chọn) Tác động đến việc tính toán trọng số bằng cách điều chỉnh băng thông và trì hoãn sử dụng lệnh **bandwidth value** và **delay value**.

Bước 5: (Tùy chọn) Cấu hình xác thực EIGRP

Bước 6: (Tùy chọn) Cấu hình hỗ trợ cân bằng tải nhiều con đường sử dụng lệnh **maximum-paths number** và **variance multiplier**.

9.6.2.1. Cấu hình EIGRP cơ bản

Ví dụ 9.31 cho thấy một ví dụ cấu hình EIGRP, cùng với lệnh **show**, trên Albuquerque. Cấu hình yêu cầu trên Yosemite và Seville tương tự như trên Albuquerque.



Hình 9.31. Cấu hình EIGRP cơ bản

Ví dụ 9.9:

```

router eigrp 1
network 10.0.0.0
Albuquerque>show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/24 is subnetted, 6 subnets
C    10.1.3.0 [90/2172416] via 10.1.6.3, 00:00:43, Serial0/1
C    10.1.2.0 [90/2172416] via 10.1.4.2, 00:00:43, Serial0/0
C    10.1.1.0 is directly connected, FastEthernet0/0
C    10.1.6.0 is directly connected, Serial0/1

```

```

0      10.1.5.0 [90/2681856] via 10.1.6.3, 00:00:45, Serial10.1
      [90/2681856] via 10.1.4.2, 00:00:45, Serial10.0
C      10.1.4.0 is directly connected, Serial10.0

```

```

Albuquerque#show ip route eigrp
  10.0.0.0/24 is subnetted, 6 subnets
0      10.1.3.0 [98/2172416] via 10.1.6.3, 00:00:47, Serial10.1
0      10.1.2.0 [98/2172416] via 10.1.4.2, 00:00:47, Serial10.0
0      10.1.5.0 [98/2681856] via 10.1.6.3, 00:00:49, Serial10.1
      [98/2681856] via 10.1.4.2, 00:00:49, Serial10.0

```

```
Albuquerque#show ip eigrp neighbors
```

```
IP-EIGRP neighbors for process 1
```

N	Address	Interface	Hold	Uptime	SRTT	RTO	D	Seq	Type			
									(sec)	(ms)	Cnt	Num
0	10.1.4.2	Se0/0	11	00:00:54	32	200	0	4				
1	10.1.6.3	Se0/1	12	00:00:36	20	200	0	24				

```
Albuquerque#show ip eigrp interfaces
```

```
IP-EIGRP interfaces for process 1
```

Interface	Peers	Xmit Queue	Mean	Pacing Type	Multicast	Pending	
						Un.Reliable	SRTT
Fe0/0	0	0.0	0	0.10	0	0	0
Se0/0	1	0.0	32	0.15	50	0	0
Se0/1	+	0.0	20	0.15	95	0	0

```
Albuquerque#show ip eigrp topology summary
```

```
IP-EIGRP Topology Table for AS(1)/ID(10.1.6.1)
```

```
Head serial 1, next serial 9
```

```
6 routes, 0 pending replies, 0 dummies
```

```
IP-EIGRP(0) enabled on 3 interfaces, 2 neighbors present on 2 interfaces
```

```
Duiscent interfaces: Se0/1/0 Se0/0/1
```

Trong cấu hình EIGRP, tất cả ba router phải sử dụng cùng số AS trong lệnh cấu hình router eigrp. Ví dụ, tất cả sử dụng lệnh **router eigrp 1** trong ví dụ này. Số được sử dụng không thực sự quan trọng, miễn là chúng phải giống nhau trên tất cả ba router. (Giá trị hợp lệ trong khoảng từ 1 đến 65535, như là khoảng hợp lệ của ProcessID tổng cấu hình router ospf). Lệnh cấu hình network 10.0.0.0 kích hoạt EIGRP trên tất cả giao tiếp có địa chỉ IP trong mạng 10.0.0.0, chưa tất cả ba giao tiếp trên Albuquerque. Với hai lệnh cấu hình EIGRP xác định trên hai router khác, EIGRP được kích hoạt trên tất cả ba giao tiếp của những router này, bởi vì những giao tiếp này cùng trên mạng 10.0.0.0.

Các lệnh **show ip route** và **show ip route eigrp** liệt kê các con đường học bằng EIGRP với kí tự “D” bên cạnh. Có thể có thông tin về các lân cận với lệnh **show ip eigrp neighbors** và thông tin về số các lân cận hoạt động với lệnh **show ip eigrp interfaces**.

Cuối cùng, phần cuối của ví dụ thể hiện RID của Albuquerque. EIGRP xác định RID của nó giống OSPF – dựa trên giá trị được cấu hình, hay địa chỉ IP cao nhất của giao tiếp loopback, hay địa chỉ IP cao nhất của giao tiếp không phải là loopback.

Lệnh **network** EIGRP có thể được cấu hình mà không có cú pháp mặt nạ ngược, như đã thấy. Nếu không có mặt nạ, lệnh **network** phải sử dụng mạng phân lớp làm tham số, và tất cả giao tiếp trên mạng phân lớp đều phù hợp. Ví dụ sau cho thấy cấu hình khác sử dụng lệnh **network** với địa chỉ và mặt nạ ngược. Trong trường hợp này, lệnh so khớp một địa chỉ IP của giao tiếp mà có thể trùng khớp nếu địa chỉ và mặt nạ trong lệnh **network** là một phần của ACL.

Ví dụ 9.10:

```
Albuquerque#router eigrp 1
Albuquerque(config-router)#network 10.1.1.0 0.0.0.255
Albuquerque(config-router)#network 10.1.4.0 0.0.0.255
Albuquerque(config-router)#network 10.1.6.0 0.0.0.255
```

9.6.2.2. Trọng số EIGRP, con đường hiện tại và con đường có thể kế nhiệm

Như đã đề cập trước đây, một con đường EIGRP hiện tại là con đường có trọng số tốt nhất đến một mạng con, và con đường có thể kế nhiệm là con đường có thể được sử dụng nếu con đường hiện tại lỗi. Phản này đánh giá cách sử dụng con đường hiện tại và con đường có thể kế nhiệm trong EIGRP, cùng với trọng số tính toán. Cuối cùng, ví dụ sau thể hiện con đường đơn tốt nhất của Albuquerque để đến mạng con 10.1.3.0/24, cả trên bảng định tuyến và cũng như con đường hiện tại trong bảng sơ đồ EIGRP. Nó cũng liệt kê hai con đường hiện tại bằng trọng số trong bảng sơ đồ EIGRP.

Ví dụ 9.11:

```

! Below, note the single route to subnet 10.1.3.0, and the two
! equal-metric routes to 10.1.5.0.
Albuquerque#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/24 is subnetted, 6 subnets
D  10.1.3.0 [90/2172416] via 10.1.6.3, 00:00:57, Serial0/1
D  10.1.2.0 [90/2172416] via 10.1.4.2, 00:00:57, Serial0/0
C  10.1.1.0 is directly connected, Ethernet0/0
C  10.1.6.0 is directly connected, Serial0/1
D  10.1.5.0 [90/2681856] via 10.1.4.2, 00:00:57, Serial0/0
      [90/2690856] via 10.1.6.3, 00:00:57, Serial0/1
C  10.1.4.0 is directly connected, Serial0/0
! Next, the EIGRP topology table shows one successor for the route to 10.1.3.0,
! and two successors for 10.1.5.0, reconfirming that EIGRP installs successor
! routes (not feasible successor routes) into the IP routing table.
Albuquerque#show ip eigrp topology
IP-EIGRP Topology Table for AS(1)/ID(10.1.6.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       R - reply Status, S - sia Status

P 10.1.3.0/24, 1 successors, FD is 2172416
      via 10.1.6.3 (2172416/28160), Serial0/1
P 10.1.2.0 24, 1 successors, FD is 2172416
      via 10.1.4.2 (2172416/28160), Serial0/0
P 10.1.1.0 24, 1 successors, FD is 281600
      via Connected, Ethernet0/0
P 10.1.6.0 24, 1 successors, FD is 2169856
      via Connected, Serial0/1
P 10.1.5.0 24, 2 successors, FD is 2681856
      via 10.1.4.2 (2681856/2169856), Serial0/0
      via 10.1.6.3 (2681856/2169856), Serial0/1
P 10.1.4.0 24, 1 successors, FD is 2169856
      via Connected, Serial0/0

```

Trước tiên, tập trung vào bảng sơ đồ EIGRP liệt kê một số con đường hiện tại. Mục 10.1.3.0/24 báo có một con đường hiện tại, vì thế

bảng định tuyến IP liệt kê một con đường được học EIGRP cho mạng con 10.1.3.0/24. Nếu so sánh, thì bảng sơ đồ EIGRP cho mạng con 10.1.5.0/24 báo có hai con đường hiện tại, vì thế mạng bảng định tuyến IP thể hiện hai con đường học được học bằng EIGRP cho mạng con đó.

Kế tiếp, tập trung vào số trong ngoặc đơn cho bảng sơ đồ EIGRP với mạng con 10.1.3.0/24. Số đầu tiên là trọng số được tính bởi Albuquerque với mỗi con đường. Số thứ hai là RD – trọng số được tính toán trên router lân cận 10.1.6.3 (Seville) và được báo cáo cho Albuquerque. Vì những router này có thiết lập băng thông và trì hoãn mặc định, vì thế giá trị trọng số phù hợp với tính toán trọng số mẫu được thể hiện trong phần trước đây “Tính toán con đường tốt nhất cho bảng định tuyến”.

9.6.2.2.1. Tạo và xem một con đường có thể kế nhiệm.

Với tất cả thiết lập mặc định trong hệ thống mạng này, không có con đường Albuquerque nào phù hợp với điều kiện khả thi, trong đó RD của một con đường là nhỏ hơn hoặc bằng với FD (trọng số con đường tốt nhất). Ví dụ sau đây thay đổi băng thông của một trong các giao tiếp của Yosemite, làm giảm FD của Yosemite để đến mạng con 10.1.3.0/24. Sau đó, RD của Yosemite cho cùng mạng con, như được báo cáo với Albuquerque, phù hợp với điều kiện khả thi, vì thế Albuquerque bây giờ sẽ có một con đường có thể kế nhiệm FS.

Ví dụ 9.12:

```
! Below, the bandwidth of Yosemite's link to Seville (Yosemite's S0/1 interface)
! is changed from 1544 to 2000, which lowers Yosemite's metric for
! subnet 10.1.3.0.
Yosemite(config)#interface S0/1
Yosemite(config-if)#bandwidth 2000
! Moving back to Albuquerque
! Below, the EIGRP topology table shows a single successor route for 10.1.3.0.
! but two entries listed - the new entry is a feasible successor route. The new
! entry shows a route to 10.1.3.0 through 10.1.4.2 (which is Yosemite).
Albuquerque#show ip eigrp topology
IP-EIGRP Topology Table for AS-11 ID(10.1.6.1)
```

```

Codes P - Passive, A - Active, U - Update, Q - Query, R - Reply,
    I - reply Status, S - sia Status

P 10.1.3.0/24, 1 successors, FD is 2172416
    via 10.1.6.3 (2172416/28160), Serial0/1
    via 10.1.4.2 (2684416/1794560), Serial0/0
! the rest of the lines omitted for brevity
! Moving back to Yosemite here
Yosemite#show ip route eigrp
    10.0.0.0/24 is subnetted, 5 subnets
D    10.1.3.0 [90/1794560] via 10.1.6.3, 00:40:14, Serial0/1
D    10.1.1.0 [90/2195456] via 10.1.4.1, 00:42:19, Serial0/0

```

Để thấy con đường có thể kế nhiệm, và tại sao nó là một con đường có thể kế nhiệm, xem xét các số trong ngoặc vuông trong dòng được bôi đen thứ hai trong lệnh `show ip eigrp topology` trên Albuquerque. Lệnh đầu tiên là tính toán trọng số của các router của Albuquerque cho một con đường, và lệnh thứ hai là số RD của các lân cận. Với hai con đường có thể trên – một qua 10.1.6.3 (Seville) và một qua 10.1.4.2 (Yosemite) – con đường qua Seville có trọng số thấp nhất (2.172.416) nên nó là con đường hiện tại và làm cho FD cũng là 2.172.416. Albuquerque đặt con đường này vào bảng định tuyến IP. Tuy nhiên, chú ý RD của hai con đường (con đường qua Yosemite), với giá trị RD là 1.794.560. Điều kiện khả thi là RD của router phải nhỏ hơn trọng số được tính toán tốt nhất – FD của nó – với cùng mạng con địch. Vì thế con đường qua Yosemite thỏa mãn điều kiện này, để làm một con đường có thể kế nhiệm. Các điểm sau đây tóm tắt thông tin chính về con đường hiện tại và con đường có thể kế nhiệm trong ví dụ này.

Con đường đến 10.1.3.0 qua 10.1.6.3 (Seville) là một con đường hiện tại, vì trọng số tính toán (2.172.416), được thể hiện là phần đầu tiên của hai số trong ngoặc kép, là trọng số tính toán tốt nhất.

Con đường đến 10.1.3.0 qua 10.1.4.2 (Yosemite) là con đường có thể kế nhiệm, vì khoảng các báo cáo của lân cận thấp hơn FD của Albuquerque.

Dù rằng cả con đường hiện tại và con đường có thể kế nhiệm trong bảng sơ đồ EIGRP, chỉ con đường hiện tại được thêm vào bảng định tuyến IP.

9.6.2.2.2. Hội tụ sử dụng con đường có thể kế nhiệm

Một trong những lợi ích của EIGRP là hội tụ rất nhanh. Ví dụ sau cho thấy điều này, sử dụng thông điệp debug để thể hiện tiến trình này. Trong ví dụ này, liên kết giữa Albuquerque và Seville bị tắt. Thông điệp debug trên Albuquerque thể hiện ý nghĩa của EIGRP khi thay đổi từ con đường ban đầu sang con đường 10.1.3.0/24 sang con đường mới qua Yosemite. Chú ý vào dấu thời gian, thể hiện tiến trình hội tụ chỉ tốn chưa đầy 1 giây.

Ví dụ 9.13:

```

: Below, debug eigrp fsm is enabled, and then Seville's link to Albuquerque
: (Seville's S0/0 interface) will be disabled, but not shown in the example text.
: SOME DEBUG MESSAGES are omitted to improve readability.

Albuquerque#debug eigrp fsm
EIGRP FSM Events/Actions debugging is on
Albuquerque#
*Mar 1 02:35:31.836: %LINK-3-UPDOWN: Interface Serial0/1, changed state to down
*Mar 1 02:35:31.848: DUAL: rcvupdate: '0.1.6.0/24 via Connected Metric 4294967295
95 4294967295
*Mar 1 02:35:31.848: DUAL: Find FS for dest 10.1.6.0/24. FD is 2169856, RD is 2
169856
*Mar 1 02:35:31.848: DUAL: 0.0.0.0 metric 4294967295 4294967295 not found 0
RD is 4294967295
*Mar 1 02:35:31.848: DUAL: Peer total-stub 2.0 template:full-stub 2.0
*Mar 1 02:35:31.848: DUAL: Dest '0.1.6.0/24' entering active state.
*Mar 1 02:35:31.852: DUAL: Set reply-status table. Count is 2.
*Mar 1 02:35:31.852: DUAL: Not doing split horizon

: Next, Albuquerque realizes that neighbor 10.1.6.3 (Seville) is down, so
: Albuquerque can react.

*Mar 1 02:35:31.852: %DUAL-5-NERCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.6.3
(Serial0/1) is down; interface down

: The next two highlighted messages imply that the old route to '0.1.3.0/24
: is removed, and the new successor route (previously the feasible successor route)
: is added to the RT (routing table..)

*Mar 1 02:35:31.852: DUAL: Destination 10.1.3.0/24
*Mar 1 02:35:31.852: DUAL: Find FS for dest 10.1.3.0/24. FD is 2172416,
RD is 2172416

```

```

*Mar 1 02:35:31.856: DUAL: 10.1.6.3 metric 4294967295:4294967295
*Mar 1 02:35:31.856: DUAL: 10.1.4.2 metric 2684416:1794568 found Dmru 16 2684416
:
: The next two highlighted messages state that the old route is removed, and the
: new route through Yosemite is added to the "RT" (routing table).
:
*Mar 1 02:35:31.856: DUAL: Removing dest 10.1.3.0/24, nexthop 10.1.6.3
*Mar 1 02:35:31.856: DUAL: RT installed 10.1.3.0/24 via 10.1.4.2
*Mar 1 02:35:31.856: DUAL: Send update about 10.1.3.0/24. Reason: metric chg
*Mar 1 02:35:31.860: DUAL: Send update about 10.1.3.0/24. Reason: new if

```

9.6.2.3. Xác thực EIGRP

EIGRP hỗ trợ một loại xác thực: MD5. Cấu hình xác thực MD5 yêu cầu nhiều bước:

Bước 1: Tạo vòng khóa xác thực

- Tạo một khóa và đặt tên với lệnh `key chain name`
- Tạo một hay nhiều số khóa sử dụng lệnh `key number` trong chế độ cấu hình khóa
- Xác định giá trị khóa xác thực sử dụng lệnh `key-string value` trong chế độ cấu hình khóa
- (Tùy chọn) Xác định chu kỳ cho cả việc gửi và chấp nhận khóa này.

Bước 2: Kích hoạt xác thực MD5 trên một giao tiếp, cho một EIGRP ASN cụ thể, sử dụng lệnh `con giao tiếp ip authentication mode eigrp asn md5`.

Bước 3: Đặt khóa đúng được sử dụng trên một giao tiếp sử dụng lệnh `con giao tiếp authentication key-chain asn name-of-chain`.

Cấu hình bước 1 khá chi tiết, nhưng bước 2 và bước 3 khá đơn giản. Cần thiết là, IOS cấu hình các giá trị khóa riêng biệt, sau đó yêu cầu một lệnh `con giao tiếp` để `đặt` đến các giá trị khóa. Để hỗ trợ khả năng có nhiều khóa, và thậm chí nhiều tập khóa, việc `cấu hình` bao gồm khái niệm `vòng khóa` và `nhiều khóa` trên `mỗi vòng khóa`.

Khái niệm vòng khóa tương tự vòng khóa và khóa được sử dụng hằng ngày. Hầu hết mọi người có ít nhất một vòng khóa, với nhiều khóa được sử dụng hằng ngày. Nếu có nhiều khóa ở nhà và nơi làm việc, có thể có hai khóa để dễ tìm đúng khóa. Có thể có một vòng khóa với các khóa ít được sử dụng được lưu giữ một nơi nào đó. Tương tự, IOS cho phép cấu hình nhiều vòng khóa để nhiều các vòng khóa khác nhau có thể được sử dụng trên các giao tiếp khác nhau. Mỗi vòng khóa có thể chứa nhiều khóa. Có nhiều khóa trong một vòng khóa cho phép các lân cận có thể tiếp tục bật và làm việc trong khi các khóa được thay đổi. (Việc thay đổi khóa thường xuyên giúp tăng cường bảo mật). Để cấu hình các chi tiết chính này, làm theo các bước 1A, 1B, 1C để tạo vòng khóa, tạo một hay nhiều khóa và gán mã khóa (mật khẩu).

Phần tùy chọn và cuối cùng có thể được cấu hình cho xác thực EIGRP là thời gian hữu dụng của mỗi khóa. Nếu không được cấu hình, khóa hợp lệ mãi mãi. Tuy nhiên, nếu được cấu hình, router sử dụng khóa chỉ trong thời gian được liệt kê. Chức năng này cho phép vòng khóa chứa nhiều khóa, mỗi khóa với thời gian hữu dụng khác nhau. Ví dụ, 12 khóa có thể được xác định, một cho một tháng trong năm. Router sau đó tự động sử dụng khóa có chỉ số thấp nhất có khoảng thời gian hợp lệ, việc thay đổi khóa tự động mỗi tháng như trong ví dụ. Chức năng này cho phép cấu hình các khóa một lần cho router sử dụng các khóa mới, tăng cường khả năng bảo mật.

Để hỗ trợ khái niệm vòng đời hữu dụng, router phải biết về thời gian và ngày. Router có thể thiết lập thời gian và ngày với lệnh EXEC **clock set**. Router có thể sử dụng Network Time Protocol – NTP, một giao thức cho phép router đồng bộ thời gian đồng hồ trong ngày của nó.

Cách tốt nhất để hiểu cấu hình là xem xét ví dụ sau. Ví dụ sau đây thể hiện cấu hình mảng sử dụng hai vòng khóa. Vòng khóa “Fred” có hai khóa, một với chu kỳ khác nhau, vì thế router sẽ sử dụng các khóa mới một cách tự động qua thời gian. Nó cũng thể hiện hai vòng khóa được tham chiếu trên hai giao tiếp khác nhau.

Ví dụ 9.14:

```

! Chain carkeys will be used on R1's Fa0/0 interface. R1 will use key 'fred'
! for about a month and then start using 'wilma.'
!
key chain carkeys
  key 1
  key-string fred
  accept-lifetime 00:00:00 Jan 11 2005 00:00:00 Feb 11 2005
  send-lifetime 00:00:00 Jan 11 2005 00:00:00 Feb 11 2005
key 2
  key-string wilma
  accept-lifetime 00:00:00 Feb 10 2005 00:00:00 Mar 11 2005
  send-lifetime 00:00:00 Feb 10 2005 00:00:00 Mar 11 2005
! Next, key chain 'anothersetofkeys' defines the key to be used on
! interface Fa0/1.
key chain anothersetofkeys
  key 1
  key-string barney
!
! Next, R1's interface subcommands are shown. First, the key chain is referenced
! using the ip authentication key-chain command, and the ip authentication mode eigrp
! command causes the router to use an MD5 digest of the key string.
interface FastEthernet0/0
  ip address 172.91.11.1 255.255.255.0
  ip authentication mode eigrp 1 md5
  ip authentication key-chain eigrp 1 carkeys
!
! Below, R1 enables EIGRP authentication on interface Fa0/1,
! using the other key chain
interface FastEthernet0/1
  ip address 172.91.12.1 255.255.255.0
  ip authentication eigrp 1 md5
  ip authentication key-chain eigrp 1 anothersetofkeys

```

Để xác thực làm việc, các router lân cận cần phải được kích hoạt EIGRP MD5, và chuỗi khóa đang dùng phải trùng. Chú ý rằng vòng khóa không cần thiết phải trùng khớp. Vẫn đề thông thường nhất liên quan đến khi nào thiết lập vòng đời hữu dụng không còn trùng khớp, hay một trong số đồng hồ router bị sai. Để triển khai thực tế, NTP cần được bật và sử dụng trước khi các khóa giới hạn cho một khung thời gian cụ thể.

Để xác nhận rằng việc xác thực hoạt động tốt, sử dụng lệnh `show ip eigrp`. Nếu việc xác thực có lỗi, mối quan hệ lân cận không được hình thành. Tương tự, nếu thấy các con đường được học từ một lân cận trên giao tiếp đó, nó cũng chứng minh rằng xác thực đã làm việc. Có thể thấy

nhiều chi tiết hơn về tiến trình xác thực sử dụng lệnh `debug eigrp packets`, cụ thể nếu xác thực lỗi.

9.6.2.4. Số con đường EIGRP tối đa và khác nhau

Giống như OSPF, EIGRP hỗ trợ khả năng đặt các con đường trọng số bằng nhau trong bảng định tuyến. Giống OSPF, EIGRP mặc định hỗ trợ bốn con đường cho mỗi mạng con, và có thể cấu hình để hỗ trợ đến 16 sử dụng lệnh `con maximum-paths number`. Tuy nhiên, việc tính toán trọng số EIGRP ngăn các con đường cạnh tranh có cùng một trọng số giống nhau.

IOS có khái niệm *biến* EIGRP để giải quyết vấn đề này. Các biến cho phép các con đường có các trọng số khác nhau về giá trị được xem như bằng nhau, cho phép nhiều con đường có trọng số không cân bằng đến cùng mạng con được thêm vào bảng định tuyến.

Lệnh `con router EIGRP variance multiplier` xác định một số nguyên giữa 1 và 128. Router sau đó nhân *biến* lần với FD của con đường – trọng số tốt nhất để đến mạng con đó. Bất kì con đường FS nào có trọng số nhỏ hơn kết quả của giá trị trên được xem như là con đường giá trị bằng và có thể được đặt vào bảng định tuyến, tùy thuộc vào thiết lập của lệnh `maximum-paths`.

Một ví dụ về *biến* có thể giải thích khái niệm này rõ hơn. Để giữ cho số này rõ ràng hơn, bảng 9.3 liệt kê một ví dụ về các giá trị trọng số nhỏ. Bảng sau liệt kê trọng số cho ba con đường đến cùng mạng con, như được tính toán trên router R4. Bảng này cũng liệt kê RD của các router lân cận, và quyết định thêm các con đường vào bảng định tuyến dựa trên các thiết lập *biến* khác nhau.

Bảng 9.23. Các biến trong EIGRP

Chặng kế	Trọng số	RD	Được thêm vào RT tại biến 1	Được thêm vào RT tại biến 2	Được thêm vào RT tại biến 3
R1	50	30	Yes	Yes	Yes
R2	90	5	No	Yes	Yes
R3	120	60	No	No	No

Bên cạnh việc xem xét *biến*, chú ý rằng trong trường hợp này, con đường qua R2 là một con đường hiện tại vì nó có giá trị trọng số nhỏ nhất. Điều này có nghĩa là trọng số cho con đường đó thông qua R1, 50 là FD. Con đường qua R2 là một con đường FS vì RD của nó là 40 nhỏ hơn FD giá trị 50. Con đường qua R3 không phải là con đường FS, vì RD của R3 là 60 lớn hơn FD giá trị 50.

Với thiết lập mặc định biến là 1, các trọng số phải bằng chính xác được xem là bằng, vì thế chỉ con đường hiện tại được thêm vào bảng định tuyến. Với biến là 2, FD (50) được nhân với *biến* (2) cho kết quả là 100. Con đường qua R2, với FD 90 là nhỏ hơn 100, vì thế R4 thêm con đường qua R2 vào bảng định tuyến. Router sau đó có thể thực hiện cân bằng tải lưu lượng trên ba router này.

Trong trường hợp thứ ba, với *biến* 3, kết quả của FD nhân 3 là 150, và tất cả ba con đường được tính toán có trọng số nhỏ hơn 150. Tuy nhiên, con đường qua R3 không phải là một con đường FS, vì thế nó không thể được thêm vào bảng định tuyến nên không lo gây ra vòng lặp định tuyến.

Danh sách sau đây tóm tắt một số điểm quan trọng về *biến*:

- Các biến được nhân với giá trị FD hiện tại (trọng số của con đường tốt nhất đến một mạng con)
- Bất kì con đường FS nào có trọng số tính toán nhỏ hơn hay bằng với tích của biến nhân với FD đều được thêm vào bảng định tuyến, giả sử rằng thiết lập maximum – paths cho phép nhiều con đường
- Các con đường hoặc là hiện tại hoặc là có thể kế nhiệm có thể không bao giờ được thêm vào bảng định tuyến, tùy theo thiết lập biến

Ngay khi các con đường được thêm vào bảng định tuyến, router hỗ trợ nhiều lựa chọn về cách cân bằng tải lưu lượng trên các con đường

này. Router có thể cân bằng tải lưu lượng từng phần với các trọng số, nghĩa là các con đường có trọng số thấp hơn gửi nhiều gói tin hơn. Các router có thể gửi tất cả gói tin qua con đường trọng số thấp nhất, với các con đường khác trong bảng định tuyến để hội tụ nhanh hơn trong trường hợp con đường tốt nhất lỗi. Tuy nhiên, chi tiết của tiến trình cân bằng tải yêu cầu hiểu biết sâu hơn về xử lý bên trong của tiến trình chuyển tiếp và chủ đề này sẽ được đề cập trong phần khác.

9.6.2.5. Điều chỉnh tính toán trọng số EIGRP

Mặc định, EIGRP tính toán một trọng số nguyên dựa trên trọng số phức hợp của băng thông và độ trì hoãn. Cả hai thiết lập này có thể được thay đổi trên bất kỳ giao tiếp nào sử dụng các lệnh **con giao tiếp bandwidth value** và **delay value**.

Cisco khuyên nghị các thiết lập băng thông của mỗi giao tiếp một giá trị chính xác, hơn là thiết lập băng thông để thay đổi tính toán trọng số EIGRP. Dù rằng các giao tiếp LAN mặc định chính xác với thiết lập băng thông, các liên kết serial của router nên được cấu hình với lệnh **bandwidth speed**, với giá trị tốc độ trong kbps, phù hợp với tốc độ thực sự của giao tiếp đó.

Vì quá ít chức năng đáp ứng dựa trên thiết lập trì hoãn giao tiếp, Cisco khuyên rằng nếu muốn điều chỉnh trọng số EIGRP, thay đổi thiết lập trì hoãn giao tiếp. Để thay đổi thiết lập trì hoãn giao tiếp, sử dụng lệnh **delay value** trong đó giá trị trì hoãn là thiết lập với một đơn vị không thông dụng: 10 lần μ s; tuy nhiên, lệnh **show interfaces** liệt kê trì hoãn với đơn vị μ s. Xem xét ví dụ sau đây:

1. Fa0/0 của router có thiết lập trì hoãn mặc định là 100 μ s
2. Lệnh **delay 123** được cấu hình trên giao tiếp đó, nghĩa là 123 lần 10 μ s
3. lệnh **show interfaces fa0/0** bây giờ liệt kê độ trì hoãn 1230 μ s

Ví dụ 9.15:

```

Yosemite#show interfaces fa0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is GT98k FE, address is 0013.1970.5026 (bia 0013.1970.5026)
  Internet address is 10.1.2.252/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
  ! lines omitted for brevity

Yosemite#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Yosemite(config)#interface fa0/0
Yosemite(config-if)#delay 123
Yosemite(config-if)#^Z

Yosemite#show interfaces fa0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is GT98k FE, address is 0013.1970.5026 (bia 0013.1970.5026)
  Internet address is 10.1.2.252/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1236 usec,
  ! lines omitted for brevity

```

CÂU HỎI VÀ BÀI TẬP CHƯƠNG 9

Câu 1. Giao thức định tuyến nào sau đây được xem như là sử dụng lý thuyết distance vector?

- RIP – 1
- RIP – 2
- EIGRP
- OSPF
- BGP
- IS – IS tích hợp

Câu 2. Giao thức định tuyến nào sau đây được xem như là sử dụng lý thuyết link – state?

- RIP – 1
- RIP – 2
- EIGRP
- OSPF
- BGP
- IS – IS tích hợp

Câu 3. Giao thức định tuyến nào sau đây sử dụng một trọng số, theo mặc định, ít nhất có ảnh hưởng phần nào bởi băng thông liên kết?

- a. RIP – 1
- b. RIP – 2
- c. EIGRP
- d. OSPF
- e. BGP

Câu 4. Giao thức định tuyến nội nào sau đây hỗ trợ VLSM?

- a. RIP – 1
- b. RIP – 2
- c. EIGRP
- d. OSPF
- e. IS – IS tích hợp

Câu 5. Trong những tình huống cụ thể nào sau đây có thể làm cho một router sử dụng RIP gỡ bỏ tất cả các con đường đã học từ một router lân cận cụ thể?

- a. Lỗi “keepalive” của RIP
- b. Không nhận cập nhật từ các lân cận nữa
- c. Các cập nhật được hơn 5 giây sau khi cập nhật cuối cùng được gửi đến lân cận đó
- d. Các cập nhật từ lân cận đó có cờ “đường xấu” toàn cục

Câu 6. Chức năng nào sau đây của distance vector ngăn lặp định tuyến bằng cách làm cho giao thức định tuyến quảng bá chỉ một phần con của các con đường đã biết, khi liên quan đến băng định tuyến đầy đủ, dưới điều kiện ôn định thông thường

- a. Đếm đến vô hạn
- b. Poison Reverse
- c. Holddown
- d. Miền phân tách
- e. Con đường đang đánh dấu

Câu 7. Chức năng nào của distance vector ngăn lặp định tuyến bằng cách quảng bá một con đường trọng số vô hạn khi một con đường lỗi?

- a. Holddown

- b. Cập nhật đầy đủ
- c. Miền phân tách
- d. Con đường đang đánh dấu

Câu 8. Một router sử dụng giao thức distance vector vừa nhận một cập nhật định tuyến liệt kê một con đường có trọng số vô hạn. Cập nhật định tuyến trước đó từ lân cận này được xem như là một trọng số phù hợp. Điều nào sau đây không phải là một phản ứng thông thường với trường hợp này?

- a. Ngay lập tức gửi một cập nhật một phần chưa con đường đánh dấu cho con đường đã bị lỗi
- b. Đặt con đường vào trạng thái holddown
- c. Ngưng miền phân tách từ con đường đó và gửi một con đường đánh dấu dự phòng
- d. Gửi một cập nhật đầy đủ liệt kê con đường đánh dấu cho con đường lỗi

Câu 9. Một liên mạng sử dụng giao thức định tuyến link – state. Router đã gửi tất cả các LSA, và mạng là ổn định. Điều nào sau đây mô tả những gì các router phải làm để gửi lại các LSA đó?

- a. Mỗi router gửi lại mỗi LSA sử dụng một bộ định thời định kì có thời gian tương tự với bộ định thời cập nhật distance vector
- b. Mỗi router gửi lại một LSA mới sử dụng một bộ định thời chu kì dài hơn bộ định thời cập nhật distance vector
- c. Router không bao giờ gửi lại LSA vì LSA không thể thay đổi.
- d. Router gửi lại tất cả LSA bất kì khi nào một LSA thay đổi

Câu 10. Điều nào sau đây là đúng về cách một router sử dụng một giao thức định tuyến link – state khi chọn con đường tốt nhất đến một mạng con?

- a. Router tìm thấy con đường tốt nhất trong cơ sở dữ liệu link – state.
- b. Router tính toán con đường tốt nhất bằng các chạy giải thuật SPF với thông tin trong cơ sở dữ liệu link – state
- c. Router so sánh trọng số được liệt kê với mạng con trong cập nhật nhận được từ mỗi lân cận và chọn con đường trọng số tốt nhất.

Câu 11. Điều nào sau đây ảnh hưởng đến việc tính toán các con đường OSPF khi tất cả giá trị mặc định có thể được sử dụng?

- a. Băng thông
- b. Độ trì hoàn
- c. Tài
- d. Độ tin cậy
- e. MTU
- f. Số chặng

Câu 12. OSPF chạy một giải thuật để tính con đường tốt nhất hiện tại. Thuật ngữ nào sau đây để cập đến giải thuật đó?

- a. SPF
- b. DUAL
- c. Feasible successor
- d. Dijkstra

Câu 13. Hai router OSPF kết nối đến cùng một VLAN sử dụng giao tiếp Fa0/0 của nó. Thiết lập nào sau đây trên các giao tiếp này của hai router lân cận tiềm ẩn ngăn chúng trở thành lân cận OSPF?

- a. Địa chỉ IP 10.1.1.1/24 và 10.1.1.254/25
- b. Địa chỉ IP thứ hai trên một giao tiếp router, nhưng không với router kia
- c. Các giao tiếp cả hai router được gán miền là 3.
- d. Một router được cấu hình sử dụng xác thực MD5 và router còn lại thì không cấu hình xác thực

Câu 14. Trạng thái lân cận OSPF nào sau đây được mong đợi khi việc trao đổi thông tin cấu hình hoàn tất để mà các router lân cận có cùng LSDB?

- a. Hai chiều
- b. Đầy đủ
- c. Trao đổi
- d. Đang nạp

Câu 15. Điều nào sau đây là đúng về router dành riêng OSPF có sẵn?

- a. Một router mới kết nối trên cùng một mạng con, với độ ưu tiên OSPF cao hơn, chuyên một DR hiện tại thành một DR mới.

- b. Một router mới kết nối trên cùng một mạng con, với độ ưu tiên OSPF thấp hơn, chuyển một DR hiện tại thành một DR mới.
- c. DR có thể được bầu dựa trên chỉ số Router ID OSPF thấp nhất.
- d. DR có thể được bầu dựa trên chỉ số Router ID OSPF cao nhất.
- e. DR thử trở thành một lân cận đầy đủ với mọi lân cận khác trên mạng con.

Câu 16. Lệnh nào sau đây, theo sau lệnh **router ospf 1**, báo router bắt đầu sử dụng OSPF trên các giao tiếp có địa chỉ IP 10.1.1.1, 10.1.100.1 và 10.1.120.1?

- a. **network 10.0.0.0 255.0.0.0 area 0**
- b. **network 10.0.0.0 0.255.255.255 area 0**
- c. **network 10.0.0.1 255.0.0.255 area 0**
- d. **network 10.0.0.1 0.255.255.0 area 0**

Câu 17. Lệnh **network** nào sau đây, theo sau lệnh **router ospf 1**, báo cho router bắt đầu sử dụng OSPF trên các giao tiếp có địa chỉ IP là 10.1.1.1, 10.1.100.1 và 10.1.120.1?

- a. **network 0.0.0.0 255.255.255.255 area 0**
- b. **network 10.0.0.0 0.255.255.0 area 0**
- c. **network 10.1.1.0 0.x.1x.0 area 0**
- d. **network 10.1.1.0 255.0.0.0 area 0**
- e. **network 10.0.0.0 255.0.0.0 area 0**

Câu 18. Lệnh nào sau đây liệt kê các lân cận OSPF trên giao tiếp Serial 0/0?

- a. **show ip ospf neighbor**
- b. **show ip ospf interface**
- c. **show ip neighbor**
- d. **show ip interface**
- e. **show ip ospf neighbor interface serial 0/0**

Câu 19. Router OSPF R1, R2, R3 kết nối trên cùng VLAN. R2 đã được cấu hình với lệnh con giao tiếp ip ospf authentication message – digest trên giao tiếp LAN kết nối đến VLAN thông thường. Lệnh **show ip ospf** liệt kê R1 và R3 là lân cận, trong trạng thái Init và Full riêng biệt. Điều nào sau đây là đúng?

- a. R3 phải có một lệnh con giao tiếp ip ospf authentication message – digest được cấu hình
- b. R3 phải có một lệnh con giao tiếp ip ospf authentication message – digest được cấu hình
- c. Phải là lỗi của R1 vì có một cấu hình xác thực loại OSPF không chính xác
- d. Lỗi trên R1 có thể hoặc không thể liên quan đến xác thực

Câu 20. Một router OSPF học về sáu con đường có thể đến mạng con 10.1.1.0/24. Tất cả 6 con đường có chi phí 55, và tất cả đều là 6 con đường liên khu vực. Mặc định, có bao nhiêu con đường được đặt vào bảng định tuyến?

- a. 1
- b. 2
- c. 3
- d. 4
- e. 5
- f. 6

Câu 21. Điều nào sau đây ảnh hưởng đến việc tính toán các trọng số EIGRP khi tất cả các giá trị mặc định được sử dụng?

- a. Băng thông
- b. Độ trì hoãn
- c. Tài
- d. Độ tin cậy
- e. MTU
- f. Đếm số chặng

Câu 22. EIGRP cảnh báo như thế nào khi một router lân cận lỗi?

- a. Lân cận lỗi gửi một thông điệp cảnh báo trước khi lỗi
- b. Lân cận lỗi gửi một thông điệp “dying gasp”
- c. Router cảnh báo thiết lập nhật định tuyến trong một khoảng thời gian
- d. Router cảnh báo thiết thông điệp Hello trong một khoảng thời gian

Câu 23. Điều nào sau đây là đúng về khái niệm chức năng khoảng cách EIGRP?

- a. Khoảng cách có thể của một con đường là trọng số được tính toán về một con đường có thể đến thành công
- b. Khoảng cách có thể của một con đường là trọng số được tính toán về con đường thành công
- c. Khoảng cách có thể là trọng số của một con đường từ một router lân cận
- d. Khoảng cách có thể là trọng số EIGRP có liên quan đến mỗi con đường có thể để đến một mạng con

Câu 24. Điều nào sau đây đúng về khái niệm khoảng cách báo cáo của EIGRP?

- a. Khoảng cách báo cáo của một con đường là trọng số được tính toán của một con đường có thể thành công
- b. Khoảng cách báo cáo của một con đường là trọng số được tính toán của con đường thành công
- c. Khoảng cách báo cáo của một con đường là trọng số của một con đường từ một router lân cận
- d. Khoảng cách báo cáo là một trọng số có liên quan đến mỗi con đường có thể để đến mạng con

Câu 25. Lệnh **network** nào sau đây, theo sau lệnh **router eigrp 1**, báo cho router bắt đầu sử dụng EIGRP trên các giao tiếp có địa chỉ IP là 10.1.1.1, 10.1.100.1 và 10.1.120.1?

- a. network 10.0.0.0
- b. network 10.1.1x.0
- c. network 10.0.0.0 0.255.255.255
- d. network 10.0.0.0 255.255.255.0

Câu 26. Router R1 và R2 kết nối đến cùng VLAN với các địa chỉ IP 10.0.0.1 và 10.0.0.2 riêng rẽ. R1 được cấu hình với lệnh **router eigrp 99** và **network 10.0.0.0**. Lệnh nào sau đây có thể là một phần của cấu hình hoạt động EIGRP trên R2 đảm bảo rằng hai router trở thành lân cận và trao đổi các con đường?

- a. network 10

- b. router eigrp 98
- c. network 10.0.0.2 0.0.0.0
- d. network 10.0.0.0

Câu 27. Kiểm tra kết quả sau đây từ giao diện dòng lệnh router

```
P 10.1.1.0/24, 1 successors, FD is 2172416
via 10.1.6.3 (2172416/28160), Serial0/1
via 10.1.4.2 (2684416/2284156), Serial0/0
via 10.1.5.4 (2684416/2165432), Serial1/0
```

Điều nào sau đây xác định địa chỉ IP chặng kè trên một con đường có thể thành công?

- a. 10.1.6.3
- b. 10.1.4.2
- c. 10.1.5.4
- d. Không thể xác định từ đầu ra của lệnh này

Câu 28. Điều nào sau đây phải xảy ra để cấu hình xác thực MD5 cho EIGRP?

- a. Thiết lập khóa xác thực MD5 thông qua một số lệnh con giao tiếp
- b. Cấu hình ít nhất một xâu khóa
- c. Xác định khoảng thời gian hợp lệ cho một khóa
- d. Cho phép xác thực EIGRP MD5 trên giao tiếp đó

Câu 29. Trong lệnh `show ip route`, mã dành riêng nào nhấn mạnh rằng một con đường đã được học với EIGRP?

- a. E
- b. I
- c. G
- d. R
- e. P
- f. D

Chương 10

ĐỊNH TUYẾN TRÊN HỆ THỐNG CÓ PHÂN CHIA MẠNG CON VỚI MẶT NẠ MẠNG THAY ĐỔI

10.1. ĐỊNH TUYẾN PHÂN LỚP VÀ KHÔNG PHÂN LỚP

Các router Cisco có hai lựa chọn có thể cấu hình cho các router sử dụng con đường mặc định có sẵn này: định tuyến phân lớp và không phân lớp. Định tuyến không phân lớp làm cho router sử dụng các con đường mặc định của nó với bất kì gói tin nào không trùng khớp với một số con đường khác. Định tuyến phân lớp đặt một giới hạn trên một router khi nó có thể sử dụng một con đường mặc định theo lớp A, B, C. Kết quả là trong các trường hợp trong đó một router có một con đường mặc định nhưng router đó chọn để hủy gói tin thay vì chuyển tiếp gói tin dựa trên con đường mặc định đó.

Thuật ngữ phân lớp và không phân lớp cũng được dùng cho cả địa chỉ IP và giao thức định tuyến IP. Trước khi giải thích chi tiết về định tuyến phân lớp và không phân lớp, phần sau tóm tắt việc sử dụng các khái niệm này.

10.1.1. Tóm tắt việc sử dụng các thuật ngữ Classless và Classful

Các thuật ngữ địa chỉ phân lớp và không phân lớp đề cập đến hai cách khác nhau để xem xét các địa chỉ IP. Cá hai thuật ngữ trên đề cập đến mặt cấu trúc của một địa chỉ IP có phân mạng con. Các địa chỉ không phân lớp sử dụng một địa chỉ IP hai phần, và địa chỉ phân lớp có cấu trúc ba phần. Với địa chỉ phân lớp, địa chỉ đó luôn có một trường mạng 8, 16, 32 bit,

dựa trên quy tắc đánh địa chỉ lớp A, B và C. Phần cuối của địa chỉ có phần máy tính xác định duy nhất mỗi máy tính bên trong một mạng con. Các bit giữa phần mạng và máy tính kết hợp nên phần thứ ba, có tên là phần mạng con của địa chỉ. Với địa chỉ không phân lớp, các phần mạng và mạng con từ địa chỉ phân lớp được kết hợp thành một phần đơn, thường được gọi là mạng con hay tiền tố, với địa chỉ kết thúc trong phần thiết bị.

Thuật ngữ giao thức định tuyến phân lớp và không phân lớp đề cập đến các đặc tính của các giao thức định tuyến IP khác nhau. Các đặc tính này có thể được cho phép hay không; một giao thức định tuyến là, theo nghĩa tự nhiên có thể là phân lớp hoặc không phân lớp. Cụ thể, các giao thức định tuyến không phân lớp quảng bá thông tin mặt nạ cho mỗi mạng con, cung cấp cho các giao thức không phân lớp khả năng hỗ trợ cả VLSM và tóm lược con đường. Các giao thức định tuyến phân lớp không quảng bá thông tin mặt nạ vì thế không hỗ trợ VLSM và tóm lược con đường.

Mục đích sử dụng thứ ba của các thuật ngữ phân lớp và không phân lớp – các thuật ngữ định tuyến phân lớp và không phân lớp phải làm là cách tiền trình định tuyến IP sử dụng con đường mặc định này. Thú vị là, đây chỉ là một trong ba mục đích sử dụng của các thuật ngữ có thể được thay đổi dựa trên thông tin định tuyến. Bảng 10.1 liệt kê ba mục đích sử dụng của các thuật ngữ phân lớp và không phân lớp, với giải thích ngắn gọn. Giải thích đầy đủ phức tạp hơn về định tuyến phân lớp và không phân lớp theo sau bảng này. Chương 9 giải thích thông tin cơ sở về các khái niệm giao thức định tuyến phân lớp và không phân lớp.

Bảng 10.1. Các khái niệm phân lớp và không phân lớp

Được áp dụng cho	Phân lớp	Không phân lớp
Địa chỉ	Các địa chỉ có ba thành phần: mạng, mạng con và thiết bị	Địa chỉ với hai phần: mạng con hay tiền tố và máy tính
Giao thức định tuyến	Giao thức định tuyến không quảng bá mặt nạ hay hỗ trợ VLSM, RIP1 và IGRP	Giao thức định tuyến quảng bá mặt nạ và hỗ trợ VLSM: RIP2, EIGRP, OSPF
Định tuyến	Tiền trình chuyển tiếp IP bị giới hạn theo cách sử dụng con đường mặc định	Tiền trình chuyển tiếp IP không giới hạn sử dụng con đường mặc định

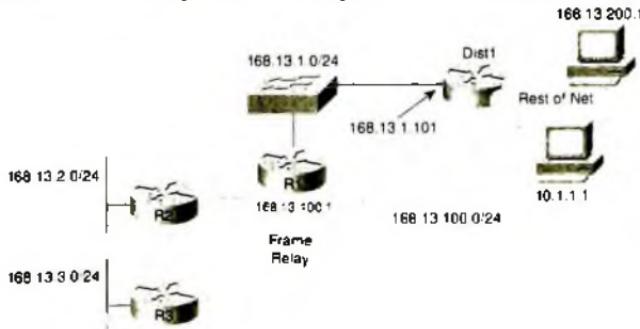
10.1.2. So sánh định tuyến phân lớp và không phân lớp

Định tuyến không phân lớp IP là định tuyến IP sẽ làm việc khi một router biết một con đường mặc định. So sánh với định tuyến phân lớp, khái niệm cốt lõi của định tuyến không phân lớp là rõ ràng. Định tuyến phân lớp giới hạn việc sử dụng con đường mặc định. Hai khái định sau đây cho mô tả chung về mỗi loại, với một ví dụ theo sau các định nghĩa:

Định tuyến không phân lớp: Khi đích của một gói tin chỉ trùng với con đường mặc định của router, và không trùng với bất kì con đường nào khác, chuyên tiếp gói tin sử dụng con đường mặc định đó.

Định tuyến phân lớp: Khi đích một gói tin chỉ trùng khớp với một con đường mặc định của router, và không trùng với bất kì con đường nào khác, chỉ sử dụng con đường mặc định nếu router đó không biết bất kì con đường nào khác trong mạng phân lớp mà địa chỉ IP đích tồn tại.

Việc sử dụng thuật ngữ phân lớp để cập đến sự thật rằng ý nghĩa đó bao gồm việc xem xét quy tắc đánh địa chỉ IP phân lớp – có tên là mạng phân lớp (Lớp A, B hay C) của địa chỉ đích gói tin đó. Để hiểu được khái niệm này, ví dụ 10.1 cho thấy một router với một con đường mặc định, nhưng định tuyến phân lớp cho phép sử dụng con đường mặc định trong một trường hợp, không phải trường hợp khác. Ví dụ này sử dụng cùng các con đường mặc định từ trước trong chương này, dựa trên hình 10.1. Cả R3 và R1 có một con đường mặc định có thể chuyên tiếp các gói tin đến Router Dist1. Tuy nhiên, như đã thấy trong ví dụ 4.1, trên R3 lệnh ping 10.1.1.1 hoạt động tốt, như lệnh ping 168.13.200.1 lỗi.



Hình 10.1. Định tuyến phân lớp và không phân lớp

Ví dụ 10.1:

```
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is 168.13.100.1 to network 0.0.0.0

  168.13.0.0/24 is subnetted, 4 subnets
R    168.13.1.0 [120/1] via 168.13.100.1, 00:00:13, Serial0.1
C    168.13.3.0 is directly connected, Ethernet0
R    168.13.2.0 [120/1] via 168.13.100.2, 00:00:06, Serial0.1
C    168.13.100.0 is directly connected, Serial0.1
R3#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 84/89/114 ms
R3#
R3#ping 168.13.200.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 168.13.200.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Trước tiên, xem xét nỗ lực của R3 thử so sánh cả hai đích (10.1.1.1 và 168.13.200.1) với các con đường trong bảng định tuyến của nó. Bảng định tuyến của R3 không có bất kì con đường nào trùng với cả hai địa chỉ IP đích đó, với con đường mặc định. Vì thế chỉ lựa chọn của R3 là để sử dụng con đường mặc định của nó.

R3 được cấu hình để sử dụng định tuyến phân lớp. Với định tuyến phân lớp, router trước tiên so khớp chỉ số mạng lớp A, B, C với một đích bên trong. Nếu mạng lớp A, B, C được tìm thấy, phần mềm IOS Cisco sẽ tìm kiếm chỉ số mạng con cụ thể. Nếu không tìm thấy, gói tin bị hủy, là trường hợp với các echo ICMP được gửi với lệnh ping 168.13.200.1. Tuy nhiên, với định tuyến phân lớp, nếu gói tin không trùng với mạng lớp A, B, C trong bảng định tuyến, và một con đường mặc định có sẵn, con đường

mặc định được sử dụng thay thế - đó là nguyên nhân vì sao R3 có thể chuyển tiếp các echo ICMP được gửi bởi lệnh ping 10.1.1.1 thành công.

Tóm lại, với định tuyến phân lớp, con đường mặc định chỉ được sử dụng khi router không biết về bất kì mạng con nào của các địa chỉ gói tin lớp mạng A, B hay C.

Có thể chuyển đổi giữa định tuyến phân lớp và không phân lớp với các lệnh cấu hình `ip classless` và `no ip classless`. Với định tuyến không phân lớp, Cisco IOS tìm kiếm con đường phù hợp nhất, bỏ qua quy tắc về lớp. Nếu con đường mặc định tồn tại, với định tuyến không phân lớp, gói tin luôn ít nhất trùng với con đường mặc định đó. Nếu một con đường cụ thể hơn trùng với đích gói tin, con đường này được sử dụng. Ví dụ 10.2 cho thấy R3 thay đổi để sử dụng định tuyến không phân lớp, và ping thành công 168.13.200.1.

Ví dụ 10.2:

```
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ip classless
R3(config)#^Z
R3#ping 168.13.200.1

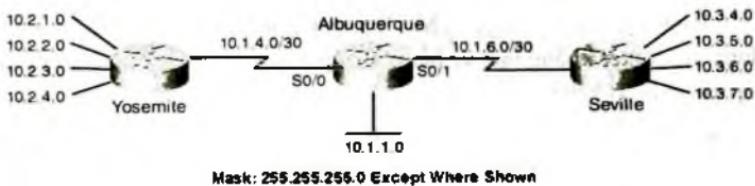
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 168.13.200.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 00/08/112 ms
```

10.2. MẶT NẠ MẠNG CÓ CHIỀU DÀI THAY ĐỔI VLSM VARIABLE LENGTH SUBNET MASK (VLSM)

10.2.1. Giới thiệu

Mặt nạ mạng có chiều dài thay đổi xảy ra khi một hệ thống mạng sử dụng hơn một mặt nạ mạng trong các mạng con khác nhau của một mạng đơn lớp A, B, hay C. VLSM cho phép giảm thiểu số lượng IP lãng phí trên mỗi mạng con, cho phép có nhiều mạng con hơn và tránh việc lấy các mạng địa chỉ IP đã đăng ký từ các cơ quan cấp phát địa chỉ IP trong khu vực. Tương tự, thậm chí khi sử dụng mạng IP dành riêng, nhiều tổ chức có thể vẫn phải cần tiết kiệm địa chỉ IP, chính là cần sử dụng VLSM.

Hình 10.2 cho thấy việc sử dụng VLSM trong một mạng lớp A 10.0.0.0.



Hình 10.2. Cấu hình VLSM trong mạng lớp A

Hình trên cho thấy một lựa chọn thông thường khi sử dụng tiền tố /30 cho một liên kết serial điểm đến và một mặt nạ /24 trên các mạng LAN con. Tất cả các mạng con là mạng lớp A 10.0.0.0, với hai mặt nạ được sử dụng VLSM. Đây chính là định nghĩa về VLSM.

Một điểm thường gây ngộ nhận chính là mọi người thường nghĩ rằng VLSM có nghĩa là “sử dụng hơn một mặt nạ mạng” thay vì “sử dụng hơn một mặt nạ trên một mạng con đơn có phân lớp”

Ví dụ, nếu trong một hệ thống mạng, tất cả các mạng 10.0.0.0 sử dụng một mặt nạ 255.255.240.0 và tất cả các mạng con của mạng 11.0.0.0 sử dụng mặt nạ 255.255.255.0, nên hai mặt nạ khác nhau được sử dụng. Tuy nhiên, chỉ một mặt nạ được sử dụng bên trong một mạng con phân lớp riêng biệt, chính vì thế thiết kế này không phải là sử dụng VLSM.

10.2.2. Giao thức định tuyến phân lớp và không phân lớp

Với một giao thức định tuyến hỗ trợ VLSM, giao thức định tuyến đó phải quảng bá không chỉ là chỉ số mạng con mà còn là mặt nạ mạng khi quảng bá các con đường. Ngoài ra, một giao thức định tuyến phải chứa mặt nạ mạng bên trong các cập nhật bảng định tuyến để hỗ trợ tóm lược các con đường thù công.

Mỗi giao thức định tuyến IP được xem như là phân lớp hay không phân lớp, dựa trên liệu giao thức đó có gửi (không phân lớp) hay không gửi (phân lớp) mặt nạ mạng trong các cập nhật bảng định tuyến hay không. Mỗi giao thức định tuyến hoặc là phân lớp hay không phân lớp một cách tự nhiên; không thể thiết lập qua lệnh hay kích hoạt giao thức

đó là phân lớp hay không phân lớp. Bảng 10.2 đây liệt kê các giao thức định tuyến, cho thấy liệu giao thức đó có phải là phân lớp hay không phân lớp, trong đó quan tâm hai đặc tính (VLSM và tóm lược con đường) của mỗi giao thức định tuyến.

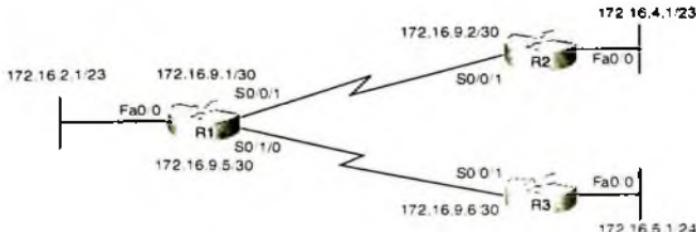
Bảng 10.2. *Khả năng hỗ trợ VLSM của các giao thức định tuyến*

Giao thức định tuyến	Không phân lớp	Gửi mặt nạ trong các cập nhập	Hỗ trợ VLSM	Hỗ trợ tự động gấp đường
RIP1	No	No	No	No
IGRP	No	No	No	No
RIP2	Yes	Yes	Yes	Yes
EIGRP	Yes	Yes	Yes	Yes
OSPF	Yes	Yes	Yes	Yes

10.2.3. Trùng lắp mạng con VLSM

Các mạng con được lựa chọn để sử dụng trong bất kì thiết kế hệ thống mạng IP nào cũng không được trùng lắp khoảng địa chỉ của nó. Với một mặt nạ mạng con đơn trong một mạng, việc trùng lắp là rõ ràng. Tuy nhiên, với VLSM, trùng lắp mạng con có thể không rõ ràng. Khi nhiều mạng con trùng lắp, một mục bảng định tuyến router trùng lắp. Kết quả là, việc định tuyến trở nên không lường được, và một số máy tính có thể không đến được một phần cụ thể nào đó của mạng. Tóm lại, thiết kế sử dụng mạng con trùng lắp được xem như là một thiết kế sai, và không nên được sử dụng.

Hai loại lỗi thông thường nhất tồn tại liên quan đến trùng lắp mạng con VLSM: phân tích một thiết kế có sẵn để tìm trùng lắp và chọn mặt nạ mạng VLSM mới để không tạo ra một mạng con trùng lắp.



Hình 10.3. *Trùng lắp mạng con*

Xem xét hình bên trên với thiết kế VLSM có thể trùng lắp, để việc tính toán VLSM không trùng lắp, thực hiện các bước đơn giản như sau:

Bước 1: Tính toán chỉ số mạng còn và địa chỉ quảng bá của mạng con cho mỗi mạng con; điều này cho biết khoảng địa chỉ trong mạng con đó.

Bước 2: So sánh khoảng địa chỉ trong mỗi mạng con và tìm kiếm trường hợp trong đó khoảng địa chỉ là trùng lắp.

Ví dụ, trong hình bên trên, xem xét 5 mạng con, sử dụng bước 1, tính toán chỉ số mạng con, các địa chỉ quảng bá, khoảng địa chỉ, với các câu trả lời được liệt kê trong bảng sau.

Bảng 10.3. Ví dụ trùng lắp mạng con

Vị trí mạng con	Chi số mạng con	Địa chỉ đầu tiên	Địa chỉ cuối	Địa chỉ quảng bá
R1LAN	172.16.2.0	172.16.2.1	172.16.3.254	172.16.3.255
R2LAN	172.16.4.0	172.16.4.1	172.16.5.254	172.16.5.255
R3LAN	172.16.5.0	172.16.5.1	172.16.5.254	172.16.5.255
R1-R2Serial	172.16.9.0	172.16.9.1	172.16.9.2	172.16.9.3
R1-R3Serial	172.16.9.4	172.16.9.5	172.16.9.6	172.16.9.7

Bước 2 xác định liệu có xảy ra trùng lắp địa chỉ hay không bằng cách so sánh khoảng địa chỉ với nhau. Như vậy là mạng con R2 LAN và R3 LAN đã bị trùng lắp.

Thiết kế sơ đồ mạng con sử dụng VLSM: Trong phần phân chia và đánh địa chỉ IP đã đề cập đến cách thiết kế mạng con sử dụng phân mạng bằng cách sử dụng mặt nạ mạng con đơn quan một mạng con phân lớp. Để thực hiện, tiến trình trước tiên phân tích yêu cầu thiết kế để xác định số mạng con và số máy tính trong mạng con lớn nhất. Sau đó lựa chọn mặt nạ mạng phù hợp. Cuối cùng, tất cả các mạng con có thể trong mạng, sử dụng mặt nạ trên, được xác định và sau đó tất cả các mạng con thực tế được sử dụng trong thiết kế được lấy từ danh sách này.

Khi sử dụng VLSM, tiến trình thiết kế bắt đầu với việc xác định có bao nhiêu mạng con cho mỗi loại được yêu cầu. Ví dụ, hầu hết các mạng con sử

dung tiền tố /30 cho liên kết serial vì những mạng con này hỗ trợ chỉ hai địa chỉ IP, cho các liên kết điểm – điểm. Các mạng con LAN thường có các yêu cầu khác nhau, với chiều dài tiền tố nhỏ hơn (nghĩa là nhiều bit thiết bị hơn) với số lượng máy tính lớn hơn và chiều dài tiền tố dài hơn (nghĩa là ít bit thiết bị hơn) với số lượng máy tính/ mạng con ít hơn.

Sau khi số lượng mạng con với mỗi mặt nạ mạng đã được xác định, bước kế tiếp là tìm kiếm số mạng con phù hợp yêu cầu thiết kế. Nhiệm vụ này thực hiện qua các bước sau đây:

Bước 1: Xác định số mạng con cần thiết cho mỗi mặt nạ/ tiền tố dựa trên các yêu cầu thiết kế.

Bước 2: sử dụng chiều dài tiền tố ngắn nhất (số lượng thiết bị lớn nhất), phù hợp với mạng con của mạng phân lớp khi sử dụng mặt nạ đó, cho đến khi số mạng con được yêu cầu đã được xác định.

Bước 3: Xác định chỉ số mạng con kế tiếp sử dụng cùng mặt nạ mạng trong bước trước.

Bước 4: Bắt đầu với chỉ số mạng con được xác định trong bước trước đây, xác định mạng con nhỏ hơn dựa trên chiều dài tiền tố lớn nhất kế tiếp được yêu cầu cho thiết kế, cho đến khi số mạng con được yêu cầu đã xác định.

Bước 5: Lặp lại bước 3 và 4 cho đến khi tất cả mạng con đã được xác định.

Ví dụ sau đây cho thấy rõ điều này hơn. Trong ví dụ này sử dụng mạng con lớp B 172.16.0.0 có:

- Ba mạng con với mặt nạ /24 (255.255.255.0)
- Ba mạng con với mặt nạ /26 (255.255.255.192)
- Bốn mạng con với mặt nạ /30 (255.255.255.252)

Bước 2, trong trường hợp này nghĩa là ba mạng con của mạng 172.16.0.0 cần được xác định với mặt nạ /24, vì /24 là chiều dài tiền tố ngắn nhất của ba chiều dài tiền tố được liệt kê trong yêu cầu thiết kế.

Sử dụng các công thức đã học trong phần trước, xác định được ba mạng con này phải là 172.16.0.0/24, 172.16.1.0/24 và 172.16.2.0/24

Bước 3, trong trường hợp này là xác định hơn một mạng con sử dụng mặt nạ /24, vì thế mạng con kế tiếp phải là 172.16.3.0/24

Để tìm được mạng con tại bước 4, bắt đầu với chỉ số mạng con chưa được cấp phát được tìm thấy tại bước 3 (172.16.3.0), nhưng với bước 4 áp dụng chiều dài tiền tố lớn hơn, /26 trong ví dụ này.

Tiến trình cũng thực hiện tương tự trong các bước như sau:

172.16.3.0/26: Khoảng địa chỉ IP 172.16.3.1 – 172.16.3.62

172.16.3.64/26: Khoảng địa chỉ IP 172.16.3.65 – 172.16.3.126

172.16.3.128/26: Khoảng địa chỉ 172.16.3.129 – 172.16.3.190

Cuối cùng bước 5 lặp lại bước 3 và 4 cho đến khi tất cả các mạng con đã được tìm thấy.

10.2.4. Gộp các con đường

Các mạng nhỏ có thể chỉ có một vài con đường trong bảng định tuyến. Mạng càng lớn, số con đường càng nhiều. Các router Internet có hơn 100.000 con đường trong bảng định tuyến.

Bảng định tuyến có thể trở nên quá lớn trong không gian mạng IP. Khi các bảng định tuyến tăng lên, chúng tiêu tốn nhiều bộ nhớ trong router. Tương tự, mỗi router có thể mất nhiều thời gian hơn để định tuyến một gói tin, bởi vì router phải so khớp một con đường trong bảng định tuyến, và tìm kiếm một bảng lớn hơn thường tốn nhiều thời gian hơn. Và với một bảng định tuyến lớn, có thể mất nhiều thời gian để xử lý các sự cố, vì router cần sử dụng nhiều thông tin hơn.

Việc tóm lược con đường giảm bớt kích thước của bảng định tuyến trong khi vẫn duy trì các con đường đến tất cả các đích trong mạng. Kết quả là, khả năng thực thi định tuyến có thể được cải tiến, vì các router tóm lược con đường không cần thông báo thay đổi về trạng thái của mỗi

mạng riêng lẻ. Bằng cách quảng bá chỉ con đường chung là up hay down, router có con đường chung này không phải tái hội tụ mỗi khi một trong các mạng con thành phần up hay down.

Chương này đề cập đến việc gộp con đường theo cách gộp thủ công, tương phản với phần chính còn lại của chương, gộp tự động. Thuật ngữ thủ công xem xét yếu tố việc gộp con đường thủ công chỉ xảy ra khi cấu hình một hay nhiều lệnh. Việc gộp đường tự động xảy ra một cách hoàn toàn tự động mà không cần một lệnh cấu hình xác định.

Phản tiếp theo trước tiên kiểm tra các khái niệm bên dưới việc gộp con đường, đi cùng với một số gợi ý về cách xác định các con đường gộp tốt.

10.2.4.1.. Khái niệm về gộp đường

Gộp đường được sử dụng để giảm thiểu kích thước của bảng định tuyến trong mạng. Gộp đường khiến cho một số các con đường cụ thể hơn được thay thế với một con đường đơn chứa tất cả địa chỉ IP được xem xét bởi tất cả các mạng trong các con đường ban đầu.

Con đường gộp, thay thế nhiều con đường khác, phải được cấu hình thủ công. Dù rằng lệnh cấu hình không chính xác như lệnh **static route** nhưng thông tin thì hoàn toàn tương tự. Sau đó giao thức định tuyến chỉ việc quảng bá về cho đường gộp, như là với con đường ban đầu.

Việc gộp đường làm việc tốt hơn nhiều với những mạng được thiết kế với ý định gộp đường ban đầu. Ví dụ, hình 10.2, như trong chương này, cho thấy kết quả của việc hoạch định tốt cho gộp đường. Trong mạng này, hệ thống được thiết kế với số mạng con có liên quan với mục đích là sử dụng chức năng gộp đường. Tất cả các mạng con trong khu vực chính (Albuquerque), bao gồm liên kết WAN, bắt đầu với 10.1. Tất cả các LAN con bên trong Yosemite bắt đầu với 10.2, và tương tự, mạng con LAN bên trong Seville bắt đầu với 10.3.

Trước đó, bảng sau cho thấy bản sao của bảng định tuyến router Albuquerque mà không có gộp đường. Trong đó cho thấy có bốn con

đường đến các mạng con bắt đầu với 10.2, tất cả trả ra giao tiếp Serial 0/0 của Yosemite. Tương tự, Albuquerque cho thấy bốn con đường đến mạng con bắt đầu với 10.3, tất cả trả ra giao tiếp Serial 0/1 của Seville. Thiết kế này cho phép router Yosemite và Seville quảng bá một con đường gộp đơn thay vì bốn con đường đang được quảng bá trong Albuquerque một cách riêng biệt.

Ví dụ sau cho thấy kết quả cấu hình gộp đường thủ công trên cả hai router Yosemite và Seville. Trong trường hợp này, Yosemite quảng bá con đường gộp của 10.2.0.0/16, đại diện cho mạng trong khoảng 10.2.0.0 – 10.2.255.255 (tất cả các địa chỉ bắt đầu với 10.2) Seville quảng bá một con đường gộp cho 10.3.0.0/16 (đại diện cho khoảng địa chỉ 10.3.0.0 – 10.3.255.255, tất cả địa chỉ bắt đầu với 10.3).

Ví dụ 10.3:

Albuquerque# show ip route

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

Gateway of last resort is not set

```
10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
D 10.2.0.0/16 [90/2172416] via 10.1.4.2, 00:05:59, Serial0/0
D 10.3.0.0/16 [90/2172416] via 10.1.6.3, 00:05:40, Serial0/1
C 10.1.1.0/24 is directly connected, Ethernet0/0
C 10.1.6.0/30 is directly connected, Serial0/1
C 10.1.4.0/30 is directly connected, Serial0/0
```

Kết quả bảng định tuyến trong Albuquerque tiếp tục định tuyến các gói tin một cách chính xác, nhưng hiệu quả hơn và tốn ít bộ nhớ hơn. Việc cài tiền với số lượng địa chỉ ít như thế này thường không giúp được gì nhiều, nhưng với một mạng lớn, điều này đem lại những hiệu quả tích cực.

Ví dụ 10.4:

Yosemite>configure terminal

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

Yosemite(config)#interface serial 0/0

Yosemite(config-if)#ip summary-address eigrp 1 10.2.0.0 255.255.0.0

Yosemite(config-if)#^Z

Yosemite#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 9 subnets, 3 masks

D 10.2.0.0/16 is a summary, 00:04:57, Null0

D 10.3.0.0/16 [90/2684416] via 10.1.4.1, 00:04:30, Serial0/0

C 10.2.1.0/24 is directly connected, FastEthernet0/0

D 10.1.1.0/24 [90/2195456] via 10.1.4.1, 00:04:52, Serial0/0

C 10.2.2.0/24 is directly connected, Loopback2

C 10.2.3.0/24 is directly connected, Loopback3

C 10.2.4.0/24 is directly connected, Loopback4

D 10.1.6.0/30 [90/2681856] via 10.1.4.1, 00:04:53, Serial0/0

C 10.1.4.0/30 is directly connected, Serial0/0

Seville>configure terminal

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

Seville(config)#interface serial 0/0

Seville(config-if)#ip summary-address eigrp 1 10.3.0.0 255.255.0.0

Seville(config-if)#^Z

Seville#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 9 subnets, 3 masks

D 10.2.0.0/16 [90/2684416] via 10.1.6.1, 00:00:36, Serial0/0

D 10.3.0.0/16 is a summary, 00:00:36, Null0

D 10.1.1.0/24 [90/2195456] via 10.1.6.1, 00:00:36, Serial0/0

C 10.3.0.0/24 is directly connected, Loopback5

C 10.3.4.0/24 is directly connected, FastEthernet0/0

C 10.1.6.0/30 is directly connected, Serial0/0

C 10.3.7.0/24 is directly connected, Loopback7

D 10.1.4.0/30 [90/2681856] via 10.1.6.1, 00:00:36, Serial0/0

C 10.3.6.0/24 is directly connected, Loopback6

Việc cấu hình gộp đường khác nhau với mỗi giao thức định tuyến: trong ví dụ trên sử dụng EIGRP. Việc gộp đường cho EIGRP được thực hiện bởi lệnh `ip summary – address` trên cả hai router Yosemite và Seville trong trường hợp này. Mỗi lệnh xác định một con đường gộp mới và báo cho EIGRP chỉ quảng bá con đường gộp ra ngoài giao tiếp này mà không quảng bá bất kì con đường nào chứa trong con đường gộp lớn hơn. Ví dụ, Yosemite xác định một con đường gộp đến 10.2.0.0, mặt nạ là 255.255.0.0, xác định một con đường đến tất cả các máy tính có địa chỉ IP bắt đầu với 10.2. Kết quả là, lệnh này làm cho Yosemite và Seville quảng bá con đường 10.2.0.0 255.255.0.0 và 10.3.0.0 255.255.0.0 một cách riêng biệt và không quảng bá bốn mạng con ban đầu.

Quay lại ví dụ trên, bảng định tuyến Albuquerque bây giờ có một con đường đến 10.2.0.0 255.255.0.0 (mặt nạ được liệt kê trong cú pháp tiền tố là /16), nhưng không có bốn mạng con ban đầu nào bắt đầu với 10.2. Điều tương tự cũng xảy ra với con đường 10.3.0.0/16.

Bảng định tuyến trên Yosemite và Seville khác một ít so với Albuquerque. Chú ý ở Yosemite, bốn con đường đến các mạng con bắt đầu với 10.2 đều bắt vì chúng đều là các con đường kết nối trực tiếp. Yosemite không thấy bốn con đường 10.3. Thay vào đó, nó thấy một con đường gộp, vì Albuquerque bây giờ quảng bá chỉ con đường gộp 10.3.0.0 này. Điều ngược lại đúng trên Seville, liệt kê bốn con đường có kết nối bắt đầu với 10.3 và con đường gộp cho 10.2.0.0/16.

Phản ứng của bảng định tuyến Yosemite là con đường đến 10.2.0.0/16, với giao tiếp đầu ra được thiết lập là `null0`. Các con đường đang xem xét đến giao tiếp đầu ra là `null0` có nghĩa là gói tin trùng với con đường này bị hủy. EIGRP đã thêm con đường này, với giao tiếp `null0`, là kết quả của lệnh `ip summary – address`. Ý nghĩa của nó như sau:

Yosemite cần con đường này vì nó có thể nhận các gói tin đến từ địa chỉ 10.2 khác bên ngoài bốn mạng 10.2 đã có sẵn. Nếu một gói tin được đến từ một trong bốn mạng con đường có sẵn 10.2.x, Yosemite có một con đường đúng, phù hợp hơn với gói tin. Nếu một gói tin có đích bắt đầu với 10.2, nhưng nó không phải là trong một trong bốn mạng con nối

trên, con đường rỗng phù hợp với gói tin đó – điều này làm cho Yosemite hủy bỏ gói tin đó đi.

Bảng định tuyến trên Seville tương tự với Yosemite trong các mục của bảng và nguyên nhân chúng ở trong bảng đó.

10.2.4.2. Chiến lược gộp đường

Như đã đề cập trước đây, việc gộp đường thủ công sẽ làm việc tốt nhất khi mạng được hoạch định cho các mạng con tham gia vào việc gộp các con đường. Ví dụ trước đây giả sử rằng một hoạch định tốt, trong đó chỉ sử dụng các mạng con bắt đầu với 10.2 cho tất cả mạng con ngoài router Yosemite. Điều này cho phép tạo con đường gộp cho tất cả địa chỉ bắt đầu với 10.2 bằng cách sử dụng Yosemite quảng bá một con đường mô tả cho mạng con 10.2.0.0, mặt nạ 255.255.0.0

Một số con đường đã gộp kết hợp nhiều con đường thành một, nhưng điều đó không có nghĩa là con đường tốt nhất. Thuật ngữ tốt nhất, khi được áp dụng để lựa chọn con đường gộp để cấu hình, nghĩa là con đường gộp đó bao gồm tất cả các mạng con được xác định trong câu hỏi trên, nhưng có thể với một vài địa chỉ khác. Ví dụ, trong ví dụ gộp đường trước đây, Yosemite gộp bốn mạng con (10.2.1.0; 10.2.2.0; 10.2.3.0; 10.2.4.0, mặt nạ 255.255.255.0) thành một con đường gộp là 10.2.0.0/16. Tuy nhiên, việc gộp này bao gồm nhiều địa chỉ IP không ở trong bốn mạng con đó. Liệu việc thiết kế có đạt được mục tiêu như ban đầu? Chắc chắn. Tuy nhiên, thay vì chỉ định nghĩa một con đường gộp chứa nhiều địa chỉ khác không có trên mạng, chúng chỉ có thể thay vào đó chỉ muốn cấu hình con đường nhỏ nhất, hay phù hợp nhất, hay gộp tốt nhất: con đường gộp chứa tất cả các mạng con nhưng không có các con đường khác như có thể. Phần này mô tả chiến lược cho việc tìm kiếm con đường gộp phù hợp nhất.

Danh sách sau đây mô tả tiến trình nhị phân trong đó có thể tìm ra con đường gộp cho một nhóm các mạng con.

Bước 1: Liệt kê tất cả các số mạng con có thể gộp trong dạng nhị phân

Bước 2: Tìm N bit đầu tiên cho số mạng con với mọi mạng con có cùng giá trị, đi từ trái sang phải, gọi là giai đoạn tìm bit chung.

Bước 3: Để tìm kiếm số mạng con gộp của router, ghi lại trong dạng nhị phân từ bước 2 và phần bit 0 cho các bit còn lại. Chuyển ngược sang dạng thập phân, 8 bit một lần, khi kết thúc.

Bước 4: Để tìm mặt nạ mạng cho con đường gộp, ghi lại N bit 1, với N là số bit chung được tìm thấy trong bước 2. Hoàn tất mặt nạ mạng với các bit 0 ở sau. Chuyển ngược lại thập phân, 8 bit mỗi lần, khi hoàn tất.

Bước 5: Kiểm tra bằng cách tính khoảng địa chỉ IP hợp lệ được cung cấp bằng con đường gộp mới, so sánh khoảng địa chỉ này với các mạng con gộp. Mạng con gộp mới nên chứa tất cả địa chỉ IP trong mạng con đã gộp.

Bằng cách xem xét số mạng con theo nhị phân, có thể dễ dàng phát hiện các bit chung trong tất cả các số mạng con. Bằng cách sử dụng số lớn nhất trong bit chung, có thể tìm thấy con đường gộp tốt nhất. Hai phân kề tiếp cho thấy hai ví dụ sử dụng tiến trình này để tìm con đường nhỏ nhất, phù hợp nhất cho mạng trong hình vẽ trên.

Seville có các mạng con 10.3.4.0, 10.3.5.0, 10.3.6.0 và 10.3.7.0 với mặt nạ là 255.255.255.0, có thể bắt đầu tiên trình bằng cách ghi lại tất cả các số mạng con dạng nhị phân:

0000 1010 0000 0011 0000 01 00 0000 0000 - 10.3.4.0
0000 1010 0000 0011 0000 01 01 0000 0000 - 10.3.5.0
0000 1010 0000 0011 0000 01 10 0000 0000 - 10.3.6.0
0000 1010 0000 0011 0000 01 11 0000 0000 - 10.3.7.0

Bước 2 yêu cầu tìm tất cả các bit chung tại phần đầu của tất cả mạng con. Có thể nhận thấy ngay trước khi bắt đầu tính toán có hai byte đầu tiên là giống nhau trong tất cả bốn byte. Vì thế, xác định ngay các bit chung chứa ít nhất 16 bit đầu tiên của tất cả các mạng con. Chính xác hơn, dựa theo phân tích nhị phân như trên, có thể thấy các mạng con có phần bit chung là 22 bit đầu tiên.

Bước 3 xác định số mạng cho con đường gộp bằng cách lấy cùng số bit trong phần bit chung, và ghi lại số bit 0 cho phần còn lại. Trong trường hợp này là:

0000 1010 0000 0011 0000 01| 00 0000 0000 \leftrightarrow 10.3.4.0

Bước 4 tạo mặt nạ mạng cho con đường gộp bằng cách sử dụng các bit 1 cho cùng các bit trong phần chung, với 22 bit trong trường hợp trên, và sau đó thêm các bit 0 vào phần bit còn lại, như sau;

1111 1111 1111 1111 1111 11| 00 0000 0000 \leftrightarrow
255.255.252.0

Vì thế, con đường gộp bây giờ sử dụng mặt nạ 10.3.4.0, mặt nạ 255.255.252.0

Bước 5 yêu cầu kiểm tra lại kết quả. Con đường gộp nên chứa tất cả địa chỉ IP của tất cả các con đường đã được gộp. trong trường hợp này, khoảng địa chỉ của con đường gộp bắt đầu với 10.3.4.0. Địa chỉ IP hợp lệ đầu tiên là 10.3.4.1, địa chỉ IP hợp lệ cuối cùng là 10.3.7.254, địa chỉ quảng bá là 10.3.7.255. trong trường hợp này con đường gộp chứa tất cả địa chỉ IP trong bốn con đường nó gộp chứa địa chỉ IP phụ trội nào bên ngoài.

10.2.5. Tự động gộp đường và các mạng phân lớp không liên tục

Như đã xem xét trong phần trước, việc gộp đường thủ công có thể cải tiến hiệu quả định tuyến, giảm thiểu thời gian tiêu tốn và cải tiến khả năng hội tụ bằng cách giảm thiểu độ lớn bằng định tuyến. Phần cuối của chương đánh giá việc gộp đường tự động tại các biên của mạng phân lớp, sử dụng chức năng được gọi là tự động gộp đường.

Vì các giao thức định tuyến phân lớp không quảng bá thông tin về mặt nạ mạng con, các cập nhật định tuyến đơn giản liệt kê các chỉ số mạng con mà không có mặt nạ liên quan. Một router nhận một cập nhật định tuyến với một giao thức định tuyến phân lớp tìm kiếm chỉ số mạng con trong cập nhật đó, nhưng router phải thực hiện một số dự đoán về mặt nạ có liên quan đến mạng con này. Ví dụ, với router Cisco, nếu R1 và R2 có các mạng kết nối đến cùng một mạng con lớp A, B hay C, và

nếu R2 nhận một cập nhật từ R1, R2 giả sử rằng con đường được mô tả trong cập nhật của R1 sử dụng cùng mặt nạ mà R2 đã sử dụng. Nói cách khác, giao thức định tuyến phân lớp yêu cầu một mặt nạ mạng con có độ dài cố định qua nhiều mạng con phân lớp để mà mỗi router có thể giả sử một cách hợp lý rằng mặt nạ đó được cấu hình cho các giao tiếp của chính nó là cùng mặt nạ được sử dụng qua mạng phân lớp này.

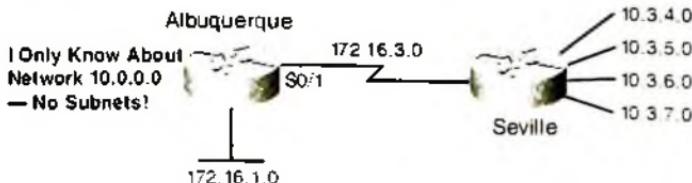
Khi một router có hơn một giao tiếp mạng lớp A, B hay C, nó có thể quảng bá một con đường đơn đến cho toàn bộ mạng lớp A, B hay C vào một mạng phân lớp khác. Chức năng này được gọi là tự động gộp đường. Nó có thể được xác định như sau:

“Khi được quảng bá trên một giao tiếp có địa chỉ IP không nằm trên mạng X, các con đường có liên quan đến các mạng con trên mạng X được gộp và được quảng bá thành một con đường. Con đường này là toàn thể mạng X lớp A, B hay C”.

Nói cách khác, nếu R3 có giao tiếp trên các mạng 10.0.0.0 và 11.0.0.0 khi R3 quảng bá cập nhật định tuyến ra ngoài các giao tiếp với địa chỉ IP bắt đầu với 11, cập nhật quảng bá một con đường đơn cho mạng 10.0.0.0. Tương tự, R3 quảng bá một con đường đơn đến 11.0.0.0 ra ngoài các giao tiếp của nó có địa chỉ IP bắt đầu với 10.

10.2.5.1. Một ví dụ về tự động gộp đường

Xem xét hình sau đây, cho thấy hai mạng được sử dụng: 10.0.0.0 và 172.16.0.0, Seville có bốn con đường có kết nối đến mạng con của mạng 10.0.0.0. Ví dụ này cho thấy kết quả của lệnh `show ip route` trên Albuquerque, cũng như kết quả của lệnh `debug ip rip RIP-1`.



Hình 10.4. Gộp đường thù công

Ví dụ 10.5:

Albuquerque#show ip route

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

Gateway of last resort is not set

```
172.16.0.0/24 is subnetted, 2 subnets
C    172.16.1.0 is directly connected, Ethernet0/0
C    172.16.3.0 is directly connected, Serial0/1
R  10.0.0.0/8 [120/1] via 172.16.3.3, 00:00:20, Serial0/1
```

Albuquerque#debug ip rip

RIP protocol debugging is on

```
00:05:36: RIP: received v1 update from 172.16.3.3 on Serial0/1
00:05:36:      10.0.0.0 in 1 hops
```

Như thể hiện trong ví dụ trên, Albuquerque nhận các cập nhật trên giao tiếp Serial 0/1 từ các quảng bá Seville chi toàn bộ mạng lớp A 10.0.0.0 bởi vì việc tự động gộp đường được kích hoạt bởi Seville theo mặc định. Kết quả là, bảng định tuyến IP của Albuquerque liệt kê chỉ một con đường đến mạng 10.0.0.0.

Ví dụ này cũng chỉ ra một chức năng khác về cách các giao thức định tuyến thực hiện các dự báo. Albuquerque không có bất kì giao tiếp nào trong mạng 10.0.0.0. Vì thế, khi Albuquerque nhận cập nhật định tuyến, nó giả sử rằng mặt nạ được sử dụng với 10.0.0.0 là 255.0.0.0, mặt nạ mặc định cho mạng lớp A. Nói cách khác, các giao thức định tuyến phân lớp mong việc tự động gộp đường xảy ra.

10.2.5.2. Các mạng phân lớp không liên tục

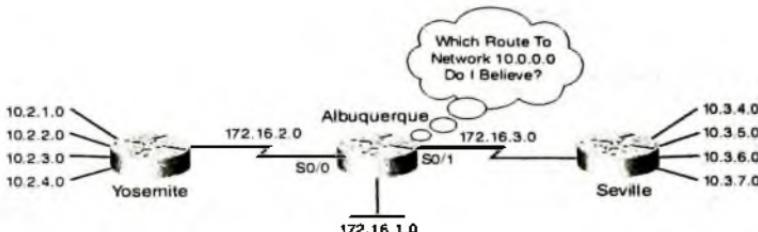
Việc tự động gộp đường không nên bắt kì vấn đề nào ngay cả khi mạng được gộp là liên tục hay không liên tục. Để hiểu rõ hơn về thuật ngữ liên tục và không liên tục là gì, xem xét hai định nghĩa sau đây:

Mạng liên tục: Một mạng phân lớp trong đó các gói tin giữa mỗi cặp mạng con có thể chuyển chỉ thông qua các mạng con của cùng mạng

phân lớp đó, mà không phải chuyển qua các mạng con của bất kì mạng phân lớp nào khác.

Mạng không liên tục: Một mạng phân lớp trong đó gói tin được gửi giữa ít nhất một cặp mạng con phải chuyển qua các mạng con của các mạng con phân lớp khác nhau.

Hình 10.5 cho thấy mạng không liên tục 10.0.0.0. Trong trường hợp này, các gói tin được gửi từ các mạng con của mạng 10.0.0.0 bên trái, gần Yosemite, đến các mạng con của mạng 10.0.0.0 bên phải, gần Seville, phải đi qua các mạng con của mạng 172.16.0.0.



Hình 10.5. Gộp đường cho các mạng không liên tục

Việc tự động gộp đường ngăn ngừa một liên mạng với một mạng không liên tục khỏi hoạt động hoàn toàn. Ví dụ sau cho thấy kết quả của việc sử dụng tự động gộp đường trong liên mạng của hình 10.5, trong trường hợp này sử dụng giao thức định tuyến RIP – 1.

Ví dụ 10.6:

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

Gateway of last resort is not set

      172.16.0.0 255.255.0.0 [1/0] subnetted, 3 subnets
C        172.16.1.0 255.255.0.0 is directly connected, Ethernet0/0
C        172.16.2.0 255.255.0.0 is directly connected, Serial0/0
C        172.16.3.0 255.255.0.0 is directly connected, Serial0/1
R        10.0.0.0 255.255.0.0 [1/120] via 172.16.3.3, 00:00:13, Serial0/1
                           [1/120] via 172.16.2.2, 00:00:04, Serial0/0
```

Như đã thấy, Albuquerque bây giờ có hai con đường đến mạng 10.0.0.0/8: một trả sang bên trái đến Yosemite và một trả sang phải đến Seville. Thay vì gửi các gói tin đến mạng con Yosemite với Serial0/0, Albuquerque gửi một số gói tin ra ngoài S0/1 đến Seville. Albuquerque đơn giản cân bằng các gói tin thông qua hai con đường, vì hai con đường trên đơn giản là cân bằng chi phí đến cùng một đích: toàn bộ mạng 10.0.0.0. Vì thế, các ứng dụng có thể hoạt động không đúng trong mạng này.

Giải pháp cho vấn đề này là hủy chức năng tự động gộp đường. Vì giao thức định tuyến phân lớp phải sử dụng chức năng tự động gộp đường, giải pháp yêu cầu tích hợp một giao thức định tuyến không phân lớp và hủy chức năng tự động gộp đường. Ví dụ sau cho thấy một mạng tương tự như trên nhưng với chức năng tự động gộp đường bị hủy, sử dụng EIGRP.

Ví dụ 10.7:

Albuquerque>show ip route

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

Gateway of last resort is not set

```

172.16.0.0/24 is subnetted, 3 subnets
C    172.16.1.0/24 is directly connected, Ethernet0/0
C    172.16.2.0/24 is directly connected, Serial0/0
C    172.16.3.0/24 is directly connected, Serial0/1
10.0.0.0/24 is subnetted, 8 subnets
D    10.2.1.0/24 [90/2172416] via 172.16.2.2, 00:00:01, Serial0/0
D    10.2.2.0/24 [90/2297856] via 172.16.2.2, 00:00:01, Serial0/0
D    10.2.3.0/24 [90/2297856] via 172.16.2.2, 00:00:01, Serial0/0
D    10.2.4.0/24 [90/2297856] via 172.16.2.2, 00:00:01, Serial0/0
D    10.3.5.0/24 [90/2297856] via 172.16.3.3, 00:00:29, Serial0/1
D    10.3.4.0/24 [90/2172416] via 172.16.3.3, 00:00:29, Serial0/1
C    10.3.7.0/24 [90/2297856] via 172.16.3.3, 00:00:29, Serial0/1
D    10.3.6.0/24 [90/2297856] via 172.16.3.3, 00:00:29, Serial0/1

```

Khi tự động gộp đường bị hủy trên cả Yosemite và Seville, không có router nào quảng bá về con đường gộp tự động của mạng 10.0.0.0/8

đến Albuquerque. Thay vào đó, mỗi router quảng bá các mạng con của nó, vì thế bây giờ Albuquerque biết về bốn mạng con LAN bên ngoài Yosemite cũng như là bốn mạng con bên ngoài Seville.

10.2.5.3. Hỗ trợ và cấu hình tự động gộp đường

Các giao thức định tuyến phân lớp phải sử dụng tự động gộp đường. Một số giao thức định tuyến không phân lớp hỗ trợ tự động gộp đường, mặc định là sử dụng nó, nhưng có khả năng hủy bỏ nó với lệnh con router `no autosummary`. Các giao thức định tuyến không phân lớp khác, đáng chú ý là OSPF, đơn giản không hỗ trợ tự động gộp đường. Bảng 10.4 tóm tắt các yếu tố về tự động gộp đường trên router Cisco.

Bảng 10.4. *Chức năng tự động gộp đường trên các giao thức định tuyến*

Giao thức định tuyến	Không phân lớp	Hỗ trợ tự động gộp đường	Mặc định sử dụng tự động gộp đường	Có thể tắt tự động gộp đường
RIP-1	No	Yes	Yes	No
RIP-2	Yes	Yes	Yes	Yes
EIGRP	Yes	Yes	Yes	Yes
OSPF	Yes	No	-	-

Cũng chú ý rằng tự động gộp đường ảnh hưởng đến các router kết nối trực tiếp đến các phần của hơn một mạng phân lớp, nhưng không có ảnh hưởng đến các router chứa các giao tiếp đều có kết nối đến cùng một mạng con phân lớp đơn.

CÂU HỎI VÀ BÀI TẬP CHƯƠNG 10

Câu 1. Giao thức định tuyến nào sau đây hỗ trợ VLSM?

- RIP – 1
- RIP – 2
- EIGRP
- OSPF

Câu 2. Thuật ngữ VLSM viết tắt cho?

- a. Variable-length subnet mask
- b. Very long subnet mask
- c. Vocious longitudinal subnet mask
- d. Vector-length subnet mask
- e. Vector loop subnet mask

Câu 3. R1 đã được cấu hình giao tiếp Fa0/0 với lệnh ip address 10.5.48.1 255.255.240.0. Mạng con nào sau đây, khi được cấu hình trên một giao tiếp khác của R1, có thể được xem như là một mạng con VLSM trùng lặp?

- a. 10.5.0.0 255.255.240.0
- b. 10.4.0.0 255.254.0.0
- c. 10.5.32.0 255.255.224.0
- d. 10.5.0.0 255.255.128.0

Câu 4. Mạng con được tóm lược nào sau đây là mạng con nhỏ nhất (khoảng địa chỉ nhỏ nhất) tóm lược con đường chứa mạng con 10.3.95.0 10.3.96.0 và 10.3.97.0, mặt nạ 255.255.255.0?

- a. 10.0.0.0 255.255.255.0
- b. 10.3.0.0 255.255.0.0
- c. 10.3.64.0 255.255.192.0
- d. 10.3.64.0 255.255.225.0

Câu 5. Mặt nạ mạng con được tóm lược nào sau đây không phải là mặt nạ tóm lược chứa các mạng con 10.1.55.0, 10.1.56.0, 10.1.57.0, mặt nạ 255.255.255.0?

- a. 10.0.0.0 255.0.0.0
- b. 10.1.0.0 255.255.0.0
- c. 10.1.55.0 255.255.255.0
- d. 10.1.48.0 255.255.248.0
- e. 10.1.32.0 255.255.254.0

Câu 6. Giao thức định tuyến nào sau đây hỗ trợ tóm lược con đường thủ công?

- a. RIP 1
- b. RIP 2
- c. EIGRP
- d. OSPF

Câu 7. Giao thức định tuyến nào thực hiện tự động tóm lược con đường theo mặc định?

- a. RIP 1
- b. RIP 2
- c. EIGRP
- d. OSPF

Câu 8. Một mạng có mạng con không liên tục, và nó có lỗ. Tất cả các router sử dụng RIP 1 với tất cả cấu hình mặc định. Câu trả lời nào sau đây liệt kê một thao tác, sẽ xử lý vấn đề trên và cho phép các mạng không liên tục này?

- a. Tích hợp tất cả các router sử dụng OSPF, sử dụng nhiều mặc định như có thể
- b. Hủy bỏ tự động gộp đường với lệnh cấu hình no auto - summarization
- c. Tích hợp với EIGRP, sử dụng nhiều mặc định có thể
- d. Vấn đề không thể giải quyết mà không thực hiện trước tiên với mạng liên tục 10.0.0.0

Chương 11

CẤU HÌNH KẾT NỐI MẠNG DIỆN RỘNG - WAN

11.1. CẤU HÌNH KẾT NỐI WAN ĐIỀM – ĐIỀM

Phần này giải thích vắn tắt cách cấu hình các kênh thuê riêng giữa hai router, sử dụng cả HDLC và PPP. Cấu hình yêu cầu khá đơn giản, với HDLC, không cần thực hiện gì và với PPP, thêm một lệnh con giao tiếp trên mỗi liên kết serial (**encapsulation ppp**). Tuy nhiên, nhiều bước cấu hình tùy chọn khác cũng được giới thiệu và ảnh hưởng của chúng trên các liên kết.

11.1.1. Cấu hình HDLC

Xem xét ba mức thấp nhất của mô hình tham chiếu OSI trên các giao tiếp Ethernet của router, thì không yêu cầu lệnh cấu hình nào liên quan đến lớp 1 và lớp 2 để giao tiếp đó bật và làm việc, chuyển tiếp các gói tin IP. Các chi tiếp lớp 1 xảy ra một lần theo mặc định khi nối cáp được cài đặt đúng. Router IOS mặc định sử dụng Ethernet như là giao thức liên kết dữ liệu cho các giao tiếp loại Ethernet, vì thế lớp 2 không cần yêu cầu lệnh nào. Để cho giao tiếp có thể chuyển tiếp các gói tin IP, router cần một lệnh để cấu hình một địa chỉ IP trên giao tiếp đó, và có thể chỉ cần một lệnh **no shutdown** trên giao tiếp nếu trạng thái quản trị là “administrative down”.

Tương tự, các giao tiếp serial trên các router Cisco sử dụng HDLC thường không cần lệnh cấu hình lớp 1 và lớp 2. Việc nối cáp được hoàn tất và không có lệnh cấu hình nào cho lớp 1. IOS mặc định sử dụng HDLC là giao thức liên kết dữ liệu vì thế không cần lệnh cấu hình liên

quan đến lớp 2. Như trên các giao tiếp Ethernet, chỉ có một lệnh được yêu cầu để thiết lập địa chỉ IP trên các giao tiếp và làm cho giao tiếp hoạt động qua các lệnh **ip address** và **no shutdown**.

Tuy nhiên nhiều lệnh cấu hình tùy chọn khác có trên liên kết serial. Danh sách sau đây liệt kê các bước cấu hình, các điều kiện trong đó các lệnh cần, cộng với các lệnh hoàn toàn tự chọn:

Bước 1: Cấu hình địa chỉ IP giao tiếp sử dụng lệnh **con ip address**

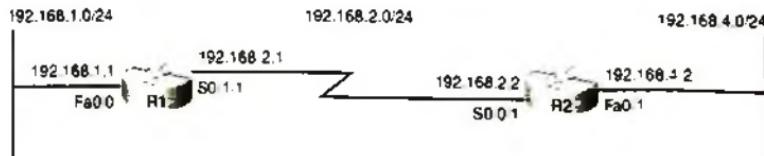
Bước 2: Tác vụ sau đây được yêu cầu khi chỉ các điều kiện sau là đúng:

- Nếu một lệnh con giao tiếp **encapsulation protocol** xác định một giao thức ngoài HDLC, sử dụng **encapsulation hdlc** để bật HDLC trên giao tiếp đó.
- Nếu trạng thái giao tiếp là **administratively down**, bật giao tiếp sử dụng lệnh **no shutdown**.
- Nếu liên kết serial là DCE, sử dụng lệnh **cấu hình clock rate speed** để xác định tốc độ giao tiếp.

Bước 3: Các bước sau đây là tùy chọn và không có ảnh hưởng đến liệu liên kết có hoạt động và có chuyên tiếp các gói tin IP.

- Cấu hình tốc độ liên kết sử dụng lệnh **bandwidth speed – in - kbps**
- Cấu hình mô tả cho một liên kết sử dụng lệnh **description text**.

Trong thực tế, khi cấu hình một router Cisco mà không có cấu hình trước đó, và cài đặt một sản phẩm liên kết serial thông thường với CSU/DSU, lệnh cấu hình **ip address** gần như là lệnh mà cần. Hình sau đây thể hiện một mạng mẫu, với ví dụ bên dưới cho thấy cấu hình của nó. Trong trường hợp này, liên kết serial được cài đặt, yêu cầu các bước 1 (**ip address**) bước 2c (**clock rate**) và bước 3b (**description**).



Hình 11.1. Cấu hình kết nối điểm - điểm HDLC

Ví dụ 11.1:

```
R1#show running-config
! Note - only the related lines are shown
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Serial0/1/1
 ip address 192.168.2.1 255.255.255.0
 description link to R2
 clockrate 1536000
!
router rip
 version 2
 network 192.168.1.0
 network 192.168.2.0
!
R1#show controllers serial 0/1/1
Interface Serial0/1/1
Hardware is GT96K
DCE V.35, clock rate 1536000
1 lines omitted for brevity
R1#show interfaces s0/1/1
Serial0/1/1 is up, line protocol is up
 Hardware is GT96K Serial
 Description: link to R2
 Internet address is 192.168.2.1/24
 MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
 reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation HDLC, loopback not set
 Keepalive set (10 sec)
Last input 00:00:06, output 00:00:03, output hang never
Last clearing of "show interface" counters never
Input queue: 0 75:0 (size:max drops:flushes); Total output drops: 0
Queuing strategy: weighted fair
Output queue: 0:1000:64/0 (size max total threshold:drops)
 Conversations: 0/1/256 (active/max active/max total)
 Reserved Conversations: 0/0 (allocated/max allocated)
 Available Bandwidth: 158 kilobauds/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
 76 packets input, 4446 bytes, 0 no buffer
 Received 56 broadcasts, 0 runts, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 73 packets output, 5280 bytes, 0 underruns
 0 output errors, 0 collisions, 0 interface resets
 0 output buffer failures, 0 output buffers swapped out
 0 carrier transitions
 DCD=up DSR=up DTR=up RTS=up CTS=up
R1#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    192.168.1.1    YES manual up       up
FastEthernet0/1    unassigned      YES NVRAM administratively down down
Serial0/0/0        unassigned      YES NVRAM administratively down down
Serial0/0/1        unassigned      YES manual administratively down down
Serial0/1/1        192.168.2.1    YES manual up       up
```

Ví dụ 11.2:

R1#show interfaces description		
Interface	Status	Protocol Description
Fa0/0	up	up
Fa0/1	admin down	down
Se0/0/0	admin down	down
Se0/0/1	admin down	down
Se0/1/0	admin down	down
Se0/1/1	up	up link to R2

Cấu hình trên R1 khá đơn giản. Cấu hình phù trên giao tiếp S0/0/1 của R2 cũng cần lệnh cấu hình đơn giản **ip address**, cộng với thiết lập mặc định **encapsulation hdlc** và **no shutdown**. Lệnh **clock rate** không nên được thêm vào R2, khi R1 có cấp DCE, vì thế R2 phải được kết nối đến cấp DTE.

Phần còn lại của ví dụ liệt kê đầu ra của một vài lệnh **show**. Trước tiên, đầu ra từ lệnh **show controllers** của S0/1/1 xác nhận rằng R1 thực sự có một cấp DCE được cài đặt sẵn. Lệnh **show interfaces S0/1/1** liệt kê nhiều thiết lập cấu hình khác nhau, bao gồm giá trị đóng gói mặc định (HDLC) và thiết lập băng thông mặc định trên giao tiếp serial (1544, nghĩa là 1544kbps, hay 1,544Mbit/s). Phần cuối của ví dụ, lệnh **show ip interface brief** và **show interfaces description** thể hiện trạng thái ngắn gọn của các giao tiếp, với trạng thái đường truyền và trạng thái giao thức.

11.1.2. Cấu hình PPP

Cấu hình cơ bản của PPP đơn giản như là HDLC, ngoại trừ một điều HDLC là giao thức liên kết dữ liệu mặc định và không cần cấu hình bổ sung thì PPP cần lệnh cấu hình **encapsulation ppp**. Còn lại, danh sách các bước cấu hình có thể và tùy chọn tương tự như HDLC. Vì thế để chuyển từ một liên kết làm việc HDLC sang một liên kết làm việc PPP, lệnh duy nhất cần thiết là lệnh **encapsulation ppp** trên mỗi giao tiếp serial của hai router. Ví dụ sau cho thấy cấu hình giao tiếp serial trên cả hai router R1 và R2 trên ví dụ trên, sử dụng PPP.

Ví dụ 11.3:

```
R1#show running-config interface s0/1/1
Building configuration...

Current configuration : 129 bytes
!
interface Serial0/1/1
  description link to R2
  ip address 192.168.2.1 255.255.255.0
  encapsulation ppp
  clockrate 1536000
end

! R2's configuration next
R2#show run interface s0/0/1
Building configuration...

Current configuration : 86 bytes
!
interface Serial0/0/1
  ip address 192.168.2.2 255.255.255.0
  encapsulation ppp
end
```

Ví dụ trên cho thấy một lệnh **show running-config** cũng như là cấu hình có liên quan đến PPP. Lệnh **show running - config interface S0/1/1** trên R1 cho thấy cấu hình giao tiếp cho giao tiếp S0/1/1, và chú ý đến phần còn lại của cấu hình. Chú ý trên cả hai router, lệnh **encapsulation ppp** đã được thêm vào, điều này quan trọng vì cả hai router cần sử dụng cùng giao thức liên kết dữ liệu, nếu không liên kết sẽ không làm việc.

11.2. CÁU HÌNH ROUTER TRUY CẬP INTERNET

Router truy cập Internet thường kết nối Internet sử dụng một giao tiếp LAN, và đến mạng LAN nội bộ sử dụng một giao tiếp khác. Router được tạo ra dành riêng cho khách hàng kết nối Internet thường được chuyển từ nhà cung cấp đến với dịch vụ DHCP client đã được bật trên giao tiếp kết nối Internet, chức năng DHCP server được bật trên giao tiếp nội bộ, và chức năng PAT được bật. Với các dòng router này, Cisco hỗ trợ phương thức cấu hình khác ngoài CLI, gọi là Cisco Router và Security Device Manager (SDM). Thay vì sử dụng telnet hay SSH, người

dùng kết nối sử dụng trình duyệt web. Từ đó, SDM cho phép người dùng cấu hình nhiều chức năng khác của router, bao gồm DHCP client, DHCP Server và PAT.

11.2.1. Các bước cấu hình router truy cập Internet

Bước 1: Thiết lập kết nối IP. Hoạch định và cấu hình (từ CLI) địa chỉ IP trên mạng LAN cục bộ để một PC trên LAN đó có thể ping và giao tiếp LAN của router.

Bước 2: Cài đặt và truy cập SDM. Cài đặt SDM trên router và truy cập giao diện SDM của router sử dụng một PC có thể ping đến địa chỉ giao tiếp LAN của router đó.

Bước 3: Cấu hình DHCP và PAT. Sử dụng SDM để cấu hình cả DHCP client và PAT trên router.

Bước 4: Hoặc định cho dịch vụ DHCP. Hoạch định địa chỉ IP được gán bởi router trên các máy tính trên LAN nội bộ, cùng với địa chỉ IP DNS, tên miền và gateway mặc định mà router sẽ quảng bá.

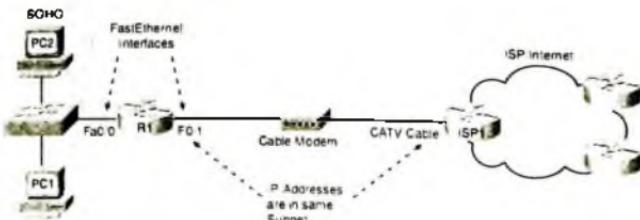
Bước 5: Cấu hình DHCP Server. Sử dụng SDM để cấu hình chức năng DHCP server trên router.

Cụ thể từng bước được mô tả như sau:

11.2.1.1. Bước 1 - Thiết lập kết nối IP

Router Internet cần sử dụng một địa chỉ IP dành riêng trên mạng LAN nội bộ, trong bước này, chọn các chi tiết sau đây:

- **Bước 1:** Chọn số mạng địa chỉ IP dành riêng.
- **Bước 2:** Chọn một mặt nạ cho phép đủ các máy tính
- **Bước 3:** Chọn một địa chỉ IP từ mạng đó

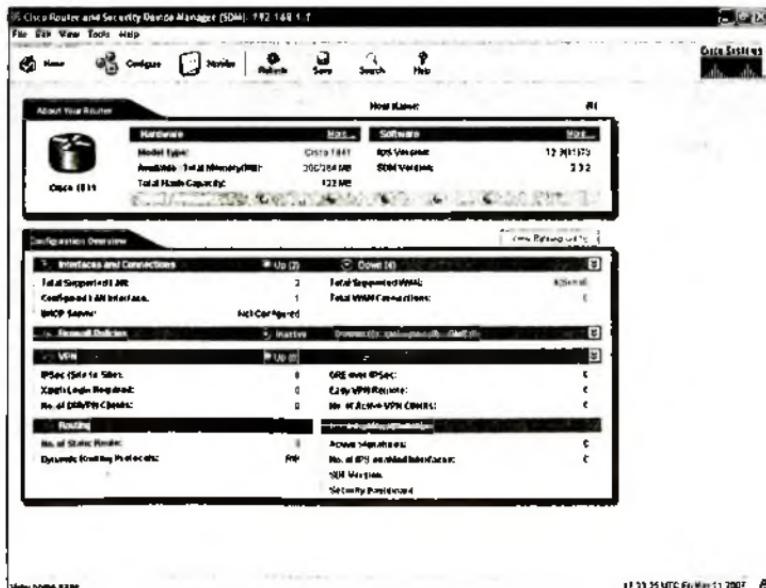


Hình 11.2. Thiết lập kết nối Internet

11.2.1.2. Bước 2 - Cài đặt và truy cập SDM

Để có thể cài đặt phần mềm SDM trên router, và cho phép các máy tính truy cập router sử dụng trình duyệt, cần sử dụng một máy tính với kết nối IP để đến router đó. Thông thường, sử dụng máy tính trên LAN nội bộ, cấu hình giao tiếp LAN nội bộ của router với một địa chỉ IP đã hoạch định bước 1, và cấu hình máy tính với một địa chỉ IP khác cùng mạng đó. Chú ý rằng SDM không sử dụng Telnet hay SSH, và PC phải được kết nối qua một mạng IP.

Cần phải cấu hình nhiều lệnh bổ sung trên router trước khi một người dùng có thể truy cập và sử dụng nó, tuy nhiên vấn đề này nằm ngoài phạm vi của giáo trình. Nếu quan tâm, có thể tìm hiểu trong tài liệu “SDM Installation”. Ở đây, đơn giản chỉ sử dụng một trình duyệt web để kết nối đến router và xem xét trang SDM home page của router đó, như sau.



Hình 11.3. Truy cập SDM

11.2.1.3. Bước 3 - Cấu hình DHCP và PAT

Giao diện người dùng SDM có nhiều chức năng cấu hình wizard cho phép cấu hình qua nhiều trang web, khi nó yêu cầu dữ liệu vào. Vào cuối tiến trình này, SDM nạp lệnh cấu hình tương ứng vào router.

Một tiến trình như vậy cho phép cấu hình chức năng DHCP client trên giao tiếp kết nối Internet và có thể là cấu hình chức năng PAT. Phần này cho thấy các cửa sổ mẫu được sử dụng để cấu hình trên router R1.

Từ trang SDM Home Page, có thể cấu hình tiếp như sau

1. Nhấn **Configure** gần đầu cửa sổ.
2. Nhấn **Interfaces and Connections** tại đầu của thanh sk bên trái của cửa sổ.



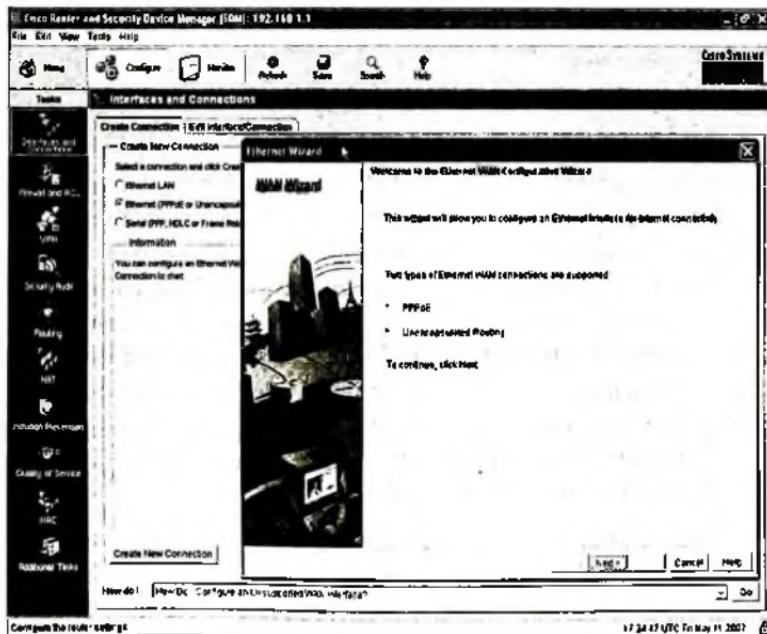
Hình 11.4. Cấu hình DHCP và PAT trên SDM

Sơ đồ mạng bên phải của thẻ trống khá đơn giản, với một router kết nối đến một modem DSL hay cáp. Trên thẻ Create Connection, thực hiện như sau:

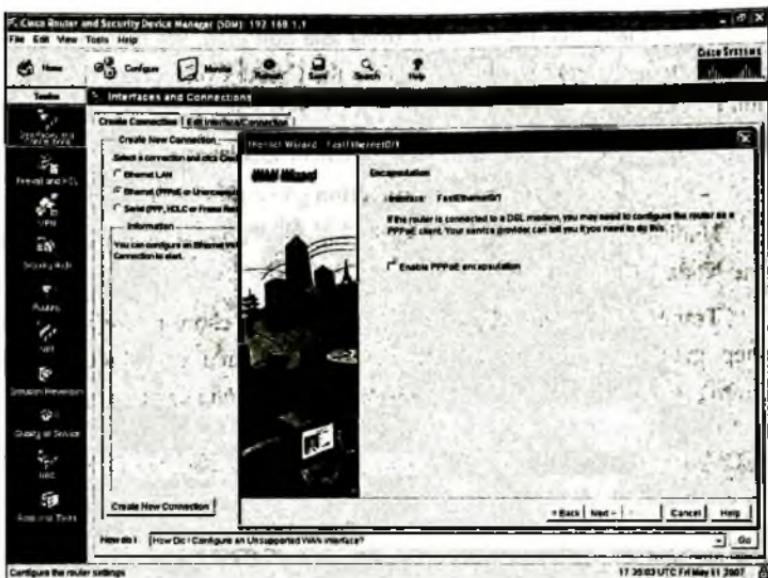
1. Chọn nút Ethernet (PPPoE hay Unencapsulated Routing)
2. Nhấn nút **Create New Connection** gần cuối của thẻ

Hành động này sẽ mở một SDM Ethernet Wizard, như trong hình sau. Nhấn **Next** để tiếp tục.

Trang kế tiếp của tiến trình, có chỉ một lựa chọn, nếu bật thì cho phép giao thức PPP Over Ethernet (PPPoE), nếu cần thiết. Thông thường, bỏ không đánh dấu, nghĩa là định tuyến không cần đóng gói.



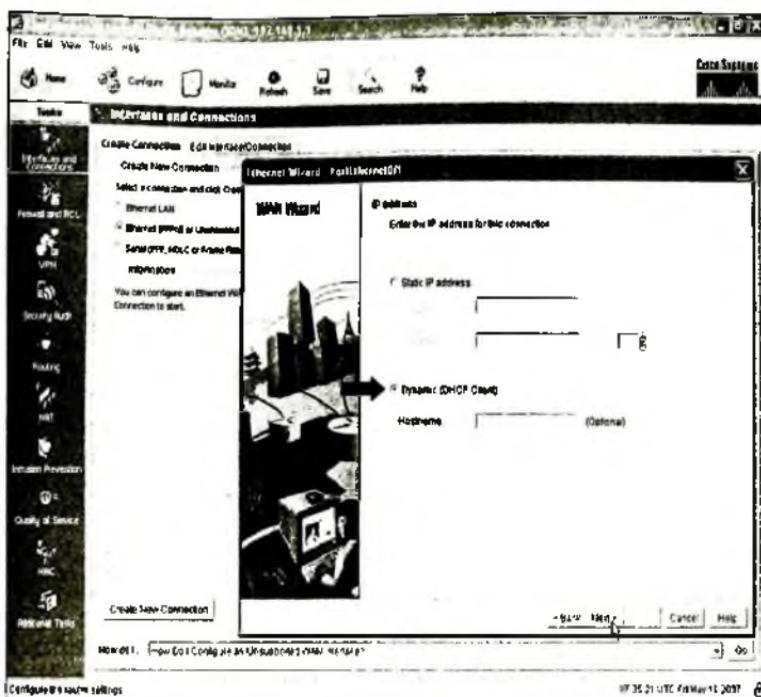
Hình 11.5. Thiết lập phương thức đóng gói PPPoE



Hình 11.6. Cấu hình giao tiếp mạng LAN

Như có thể thấy ở phần đầu của hình trên, tiến trình lấy một giao tiếp Fast Ethernet Fa0/1, làm giao tiếp để cấu hình. Router được sử dụng trong ví dụ này có hai giao tiếp LAN, một trong số chúng đã có địa chỉ IP được gán trong bước 1 (Fa0/0). Vì tiến trình này sẽ cấu hình dịch vụ DHCP client trên router, tiến trình lấy chỉ giao tiếp LAN mà chưa được cấu hình địa chỉ IP, có tên Fa0/1, là giao tiếp trên đó nó sẽ bật chức năng DHCP client. Lựa chọn này quan trọng khi xử lý sự cố với một cài đặt mới, vì nó phải là giao tiếp LAN kết nối đến modem cáp hay DSL. Đây cũng là giao tiếp NAT/ PAT ra ngoài.

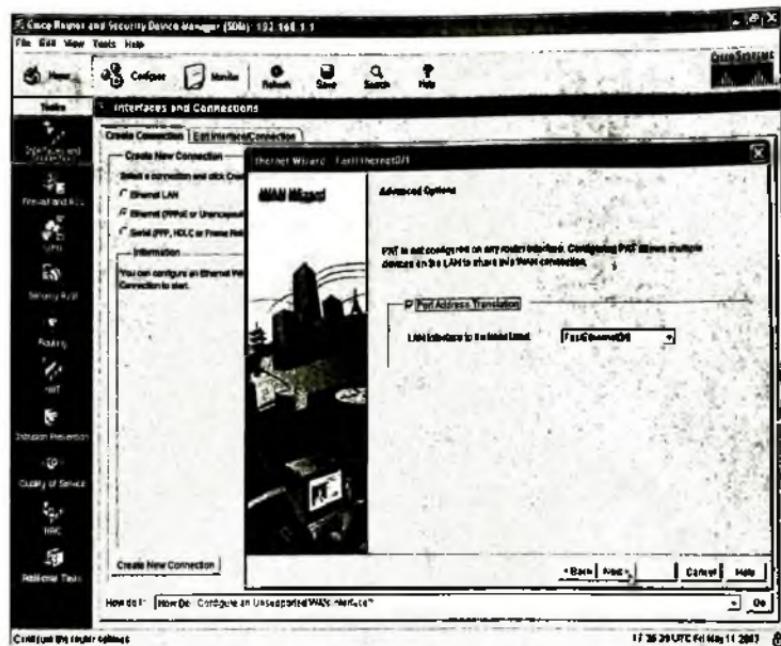
Nhấn Next, hình sau sẽ hiện trang kế tiếp của tiến trình, trang địa chỉ IP. Trang này cho lựa chọn cấu hình địa chỉ IP giao tiếp tĩnh. Tuy nhiên, có thể lấy địa chỉ IP động từ ISP – một địa chỉ IP công cộng có thể truy cập và định tuyến trên Internet. Vì thế muốn sử dụng nút Dynamic.



Hình 11.7. Cấu hình cung cấp địa chỉ IP động

Nhấn **Next** để sang trang cấu hình Advanced Options, như trong hình 11.8. Trang này yêu cầu bật chức năng PAT, dù nhiên phải có khi là một router truy cập Internet. Đơn giản nhấn vào nút chọn **Port Address Translation**. Nếu không muốn bật PAT vì nguyên nhân nào đó, đơn giản đừng chọn nó.

Quan trọng cần chú ý với là chọn LAN Interface to Be Translated ở hộp chọn thả gần cuối trang. Trong thuật ngữ NAT, hộp này liệt kê các giao tiếp bên trong, nghĩa là nó liệt kê giao tiếp kết nối đến LAN nội bộ. Ví dụ này thể hiện Fastatethernet 0/0 là giao tiếp bên trong.



Hình 11.8. Cấu hình PAT

Nhấn **Next** để sang trang **Summary** như hình vẽ sau, tóm lược các lựa chọn đã thực hiện trong tiến trình này. Các dòng chữ trên màn hình là hữu ích, báo biết:

- Giao tiếp được cấu hình là Fastatethernet 0/1
- Fastatethernet 0/1 sẽ sử dụng dịch vụ DHCP Client để tìm địa chỉ IP của nó.
- Đóng gói PPPoE bị tắt, nghĩa là định tuyến không đóng gói được sử dụng
- PAT được bật, với Fastatethernet 0/0 là giao tiếp trong, và Fastatethernet 0/1 là giao tiếp ngoài



Hình 11.9. Hoàn tất cấu hình SDM

Nhấn Finish. SDM sẽ tạo cấu hình và tải nó vào running – config của router. Nếu muốn lưu cấu hình, nhấn vào nút save gần cuối của SDM home page để router thực hiện lệnh **copy running – config startup – config** để lưu cấu hình đó. Tuy nhiên, nếu không có hành động bổ sung, cấu hình sẽ chỉ được thêm vào file cấu hình running – config.

Lúc này, chức năng DHCP client và PAT đã được cấu hình. Các tác vụ còn lại được hoạch định chi tiết những gì cần cấu hình cho chức năng DHCP server trên router với LAN nội bộ, và sử dụng SDM để cấu hình chức năng này.

11.2.1.4. Bước 4 - Cấu hình dịch vụ DHCP

Trước khi cấu hình chức năng DHCP server trên router, để hỗ trợ LAN nội bộ, cần hoạch định một vài giá trị được cấu hình trên server. Cụ thể, cần chọn mạng con của mạng IP riêng trên LAN nội bộ muốn ch

phép sử dụng địa chỉ IP được gán với DHCP. Ví dụ trong chương này, phần mạng làm việc tại bước 1 được chọn mạng IP riêng là 192.168.1.0, và mặt nạ mạng mặc định là 255.255.255.0. Chỉ cần cấu hình một vài địa chỉ IP tĩnh, còn lại tất cả các máy tính khác sẽ được cấp phát địa chỉ IP tự động. Ví dụ giao tiếp Fa0/0 của R1, kết nối đến LAN nội bộ, đã được cấu hình địa chỉ IP 192.168.1.1, vì thế địa chỉ trên không chứa trong khoảng địa chỉ cho phép gán trên DHCP server.

Sau đây là các yếu tố quan trọng mà cần thu thập trước khi cấu hình router như là DHCP server. Hai mục đầu tiên trong danh sách liên quan đến việc hoạch định trên LAN nội bộ và hai mục cuối chỉ là giá trị được học từ ISP cần được chuyển qua trên các máy tính trên LAN nội bộ.

1. Nhắc lại mạng IP dành riêng và mặt nạ được sử dụng trên LAN nội bộ và sau đó chọn một tập con của mạng có thể được gán cho máy tính sử dụng DHCP.

2. Thực hiện một ghi chú về địa chỉ IP của router trên mạng đó, địa chỉ này sẽ là địa chỉ gateway mặc định của máy tính nội bộ.

3. Tìm địa chỉ IP Server DNS đã học bởi router bằng cách sử dụng dịch vụ DHCP client, sử dụng lệnh `show dhcp server`. Router khi đó được bật để thông báo cho các DHCP Client trên LAN nội bộ về các địa chỉ IP DNS server.

4. Tìm tên miền, thực hiện lại lệnh `show dhcp server`.

Với ví dụ trong chương này, hai mục đầu tiên, mạng IP 192.168.1.0 với mặt nạ /24 đã được chọn trong bước 1 của tiến trình cấu hình. Khoảng địa chỉ IP là 192.168.1.101 – 192.168.1.254 được dành riêng cho các DHCP client, để dành khoảng 192.168.1.1 – 192.168.1.100 cho các địa chỉ IP tĩnh.

Với hai mục cuối trong danh sách hoạch định, địa chỉ IP của server DNS và tên miền, ví dụ sau cho thấy cách tìm các giá trị này sử dụng lệnh `show dhcp server`. Lệnh này liệt kê thông tin trên một router hoạt

động như là một DHCP client, các thông tin được học từ mỗi DHCP server trong đó các router đã học về một địa chỉ IP.

```
R1#show dhcp server
DHCP server: ANY (255.255.255.255)
Leases: 8
Offers: 8      Requests: 8      Acks: 8      NAKs: 0
Declines: 0    Releases: 21    Bad: 0
DNS0: 198.133.219.2,  DNS1: 0.0.0.0
Subnet: 255.255.255.252  DNS Domain: example.com
```

11.2.1.5. Bước 5 - Cấu hình DHCP Server

Để cấu hình DHCP Server với SDM, nhấn nút **Configure** gần đầu của hình SDM và nhấn **Additional Tasks** tại cuối của thanh sk để mở cửa sổ Additional sks, như trong hình sau.



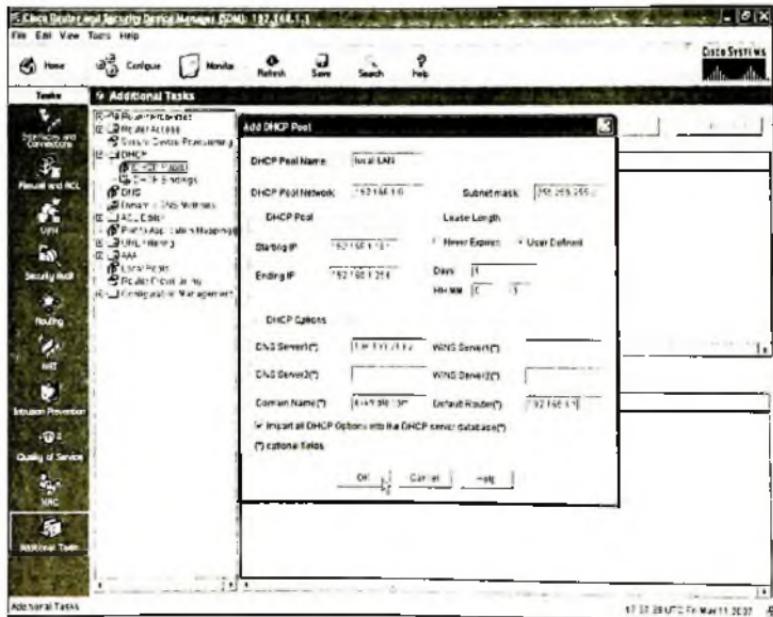
Hình 11.10. Cấu hình DHCP server

Lựa chọn **DHCP Pools** bên trái và sau đó nhấn nút **Add** để mở hộp thoại **Add DHCP Pool**, như hình vẽ sau. Hộp thoại chứa tất cả thông tin

cần thiết trong bước trước, cùng với các thiết lập khác. Hình này cho thấy màn hình được sử dụng để cấu hình router R1 trong ví dụ tiếp theo của chương.

Bốn loại hoạch định được đề cập trong bước cấu hình trước như sau.

- Khoảng địa chỉ được gán với DHCP.
- Địa chỉ IP Server DNS
- Tên miền
- Thiết lập mặc định của router.



Hình 11.11. Thiết lập dãy địa chỉ IP

Ngoài ra, hộp thoại muốn biết về chỉ số mạng con và mặt nạ mạng được sử dụng trong mạng con mà các địa chỉ sẽ được gán. Tương tự, cần tạo một tên cho yêu cầu địa chỉ DHCP này, cần thiết cho việc cài đặt.

11.2.2. Xác nhận router truy cập Internet

Lựa chọn xem xét cấu hình SDM cho DCHP và NAT/ PAT, thay vì các lệnh cấu hình CLI, có những điểm tích cực và tiêu cực. Điểm tích cực là có thể xem xét một số chức năng phổ biến được kiểm tra trên router truy cập, thường được sử dụng bởi các công ty nhỏ dễ dàng hơn. Điểm tiêu cực cho việc sử dụng SDM là việc xử lý sự cố khó khăn hơn vì cấu hình không được xem xét chi tiết. Kết quả là, các sự cố thật sự yêu cầu thông tin khi chỉ sử dụng SDM không giải quyết một cách triệt để. Thay vì thể hiện tất cả các màn hình cấu hình SDM như trên, phần này chỉ một số khó khăn thường thường nhất khi sử dụng SDM để cấu hình DHCP và PAT.

Để thực hiện một số xác nhận cơ bản nhất về cài đặt router truy cập, sử dụng các bước sau đây:

Bước 1: Đến PC trên một LAN nội bộ và mở một trình duyệt. Thủ truy cập vào một trang web trên Internet.

Bước 2: Từ PC nội bộ với hệ điều hành của Microsoft, mở cửa sổ lệnh và sử dụng lệnh ipconfig /all để tìm các địa chỉ IP, mặt nạ, gateway mặc định và địa chỉ IP server DNS được cấu hình trên router.

Bước 3: Kiểm tra nối cáp giữa router và LAN nội bộ và giữa router và modem DSL hay cáp, chú ý giao tiếp nào của router kết nối đến phần nào của mạng. Sau đó kiểm tra cấu hình SDM để đảm bảo các giao tiếp bên trong cấu hình PAT là giao tiếp được kết nối đến LAN nội bộ, và giao tiếp bên ngoài của cấu hình PAT được kết nối đến modem DSL hay cáp.

Bước 4: Kiểm tra chức năng PAT bằng cách tạo một lưu lượng từ PC nội bộ đến một máy tính trên Internet.

Có thể sử dụng các câu lệnh để kiểm tra đầu ra có liên quan đến cấu hình router, như sau.

Ví dụ 11.4:

```

R1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address Client-ID/Hardware address User name Lease expiration Type
192.168.1.101 0003-6873-636f 2d May 12 2007 08:24 PM Automatic
192.168.1.111 0100-1517-1973.2c May 12 2007 08:26 PM Automatic
R1#show ip nat translations
Pro Inside global Inside local Outside local Outside global
tcp 64.100.1.1:36486 192.168.1.101:36486 192.168.7.1:80 192.168.7.1:80
udp 64.100.1.1:1027 192.168.1.111:1027 198.133.219.2:53 198.133.219.2:53
R1#clear ip nat translation *
R1#show ip nat translations
R1#

```

Đầu ra lệnh **show ip dhcp binding** liệt kê thông tin về các địa chỉ IP được gán cho các máy tính trên LAN nội bộ bằng chức năng DHCP server trên router truy cập. Đầu ra của lệnh có thể được so sánh với kết quả khi thử lấy các máy tính trên LAN nội bộ yêu cầu địa chỉ IP từ chức năng DHCP server của router.

Lệnh **show ip nat translations** cung cấp thông tin xác nhận hoạt động của NAT và PAT.

Lệnh cuối cùng, **clear ip nat translation *** được sử dụng để xóa tất cả các thông tin trong bảng NAT, và sau đó router tạo một bảng NAT mới với các máy tính khác. Chú ý rằng lệnh này có thể ảnh hưởng đến các tiến trình đang thực thi khác trên router.

11.3. CÂU HỎI VÀ BÀI TẬP CHƯƠNG 11

Câu 1. Router R1 và R2 kết nối sử dụng thuê bao riêng, với cả hai router sử dụng các giao tiếp Se0/0 riêng của nó. Các router có thể hiện thời định tuyến các gói tin thông qua liên kết đó, sử dụng HDLC. Lệnh nào sau đây yêu cầu tích hợp cấu hình sử dụng PPP?

- encapsulation ppp
- no encapsulation hdlc
- clock rate 128000
- bandwidth 128000

Câu 2. Hai router R1 và R2 được kết nối với nhau sử dụng liên kết Se0/0.

Điều nào sau đây là đúng về cách cài đặt và cấu hình kết nối này?

- Nếu cáp DCE được nối trên R1, thực hiện lệnh clock rate trên R2
- Nếu cáp DTE được nối trên R1, thực hiện lệnh clock rate trên R2
- Nếu lệnh clock rate 128000 được cấu hình trên R1, lệnh bandwidth phải được cấu hình trên R2
- Không có phương án nào đúng

Câu 3. Hai router Cisco mới được kết nối trên hai khu vực khác nhau cách 100 dặm. Một liên kết dành riêng 768kbps đã được cấu hình giữa hai router này. Lệnh nào sau đây được yêu cầu trên ít nhất một router để chuyển tiếp các gói tin qua liên kết dành riêng trên, sử dụng PPP làm giao thức liên kết dữ liệu

- no encapsulation hdlc
- encapsulation ppp
- clock rate 768000
- bandwidth 768
- description this is the link

Câu 4. Khi cấu hình một DHCP server trên một router truy cập Internet sử dụng SDM, thiết lập nào sau đây thường được cấu hình trên router truy cập Internet?

- Địa chỉ MAC của PC trên LAN nội bộ
- Địa chỉ IP của router ISP trên cáp hay liên kết DSL
- Khoảng địa chỉ IP được cấp phát cho máy tính trên LAN nội bộ
- Địa chỉ IP của DNS Server được học thông qua DHCP từ ISP

Câu 5. Khi cấu hình một router truy cập với SDM, để sử dụng dịch vụ DHCP để học một địa chỉ IP từ một ISP, và cấu hình PAT tại cùng thời điểm, điều nào sau đây là đúng?

- a. Tiến trình cấu hình SDM yêu cầu PAT được cấu hình nếu DHCP chức năng client được chọn để cấu hình
- b. Tiến trình cấu hình SDM xem bắt kì giao tiếp nào đã có địa chỉ IP được cấu hình như là một ứng viên để trở thành giao tiếp nội cho PAT
- c. Tiến trình cấu hình SDM già sử giao tiếp trên đó DHCP client đã được bật và sẽ là một giao tiếp nội
- d. Không có câu trả lời nào như trên là đúng

Câu 6. Điều nào sau đây là đúng về tiến trình cấu hình sử dụng SDM?

- a. SDM sử dụng một kết nối SSH thông qua console hay một mạng IP để cấu hình router
- b. SDM sử dụng một giao tiếp web từ mạng IP hay từ console
- c. SDM nạp các lệnh cấu hình vào một router tại cuối mỗi tiến trình (sau khi người dùng nhấn nút Finish), lưu lại cấu hình trong các file running – config và startup – config
- d. Không có phương án nào như trên là đúng

Câu 7. Lỗi nào hay xảy ra khi cấu hình một router truy cập Internet có chức năng lớp 3?

- a. Thường được sử dụng bò qua nhưng một số thông tin tùy chọn từ DHCP server như là địa chỉ IP của DNS server
- b. Thiết lập sai giao tiếp như là giao tiếp NAT bên trong và bên ngoài
- c. Quên cấu hình cùng giao thức định tuyến mà ISP sử dụng
- d. Quên bật CDP trên giao tiếp ra ngoài Internet.

DANH MỤC CÁC TỪ VIỆT TẮT

ABR	Area Border Router	Bộ định tuyến vùng biên
ACL	Access List	Chính sách truy cập
ARP	Address Resolution Protocol	Giao thức phân giải địa chỉ
AS	Autonomous System	Hệ tự quản hay miền tự quản
BDR	Backup Designated Router	Bộ định tuyến được chỉ định dự phòng
BGP	Border Gateway Protocols	Giao thức cổng biên
CLI	Command Line Interface	Giao diện dòng lệnh
CSMA/CD	Carrier Sense Multiple Access with Collision Detection	Đa truy cập cảm biến sóng mang với phát hiện xung đột
CSU	Channel Service Unit	Khối dịch vụ kênh
DCE	Data Communication Equipment	Thiết bị truy truyền dữ liệu
DHCP	Dynamic Host Control Protocol	Giao thức điều khiển host động
DNS	Domain Name System	Hệ thống tên miền
DR	Designated Router	Bộ định tuyến được chỉ định
DSL	Digital Subscriber Line	Đường dây thuê bao số
DSU	Data Service Unit	Khối dịch vụ dữ liệu
DTE	Data Terminal Equipment	Thiết bị đầu cuối dữ liệu
EGP	Exterior Gateway Protocols	Giao thức cổng nối ngoài
EIGRP	Enhanced Interior Gateway Routing Protocol	Giao thức định tuyến nâng cao theo khoảng cách
FTP	File Transfer Protocol	Giao thức truyền tập tin
HTTP	Hyper Text Transfer Protocol	Giao thức truyền tài liệu siêu văn bản
ICANN	Internet Corporation for Assigned Names and Numbers	Tổ chức quản lý tên miền và địa chỉ IP quốc tế
ICMP	Internet Control Message Protocol	Giao thức kiểm soát thông điệp Internet
IGP	Interior Gateway Protocols	Giao thức cổng nối nội bộ
IGRP	Interior Gateway Routing Protocol	Giao thức định tuyến cổng nối nội bộ
IOS	Internetwork Operating System	Hệ điều hành mạng
IP	Internet Protocol	Giao thức Internet
ISL	Inter - Switch Link	Giao thức trung kế ISL

ISP	Internet Service Provider	Nhà cung cấp dịch vụ Internet
LAN	Local Area Network	Mạng cục bộ
LSA	Link-State Advertisement	Quảng bá trạng thái kết nối
LSDB	Link-State DataBase	Cơ sở dữ liệu trạng thái kết nối
MAC	Media Access Control	Kiểm soát truy cập môi trường
MTU	Maximum Transfer Unit	Kích thước dữ liệu tối đa của đường truyền
OS	Operating System	Hệ điều hành
OSPF	Open Shortest Path First	Ưu tiên đường ngắn nhất mở
PC	Personal Computer	Máy tính cá nhân
POST	Power On Self Test	Quá trình tự chẩn đoán khi bật nguồn
RID	Router Identifier	Định danh Router
RIP	Routing Information Protocol	Giao thức thông tin định tuyến
SOHO	Small Office/Home Office	Văn phòng/Gia đình
SPF	Shortest Path First	Ưu tiên đường đi ngắn nhất
STP	Shielded Twister Pair	Cáp xoắn dài có vỏ bọc
TFTP	Trivial File Transfer Protocol	Giao thức truyền tập tin bình thường
UTP	Unshielded Twister Pair	Cáp xoắn dài không vỏ bọc
VLAN	Virtual Local Area Network	Mạng cục bộ ảo
VLSM	Variable Length Subnet Mask	Mặt nạ mạng có độ dài thay đổi
VPN	Virtual Private Network	Mạng riêng ảo
VTP	VLAN Trunking Protocol	Giao thức mạch nối các mạng nội bộ ảo
WAN	Wide Area Network	Mạng diện rộng

TÀI LIỆU THAM KHẢO

- [1] **Wendell Odom (2007)**, ICND 1 & 2, *Cisco Press*.
- [2] **Alex Zinin**, Cisco IP Routing (2005), *Cisco Press*.
- [3] **Giáo trình CCNA Exploration v4.0 (2008)**, *Cisco Press*.
- [4] Một số tài liệu trên Internet.

MỤC LỤC

<i>Lời nói đầu</i>	3
PHẦN I: CHUYỀN MẠCH	5
Chương 1: TỔNG QUAN VỀ MẠNG NỘI BỘ - LAN	7
<i>1.1. Cơ sở về LAN</i>	7
1.1.1. Giới thiệu	7
1.1.2. Tổng quan LAN Ethernet.....	8
1.1.3. Đầu nối bằng cáp UTP Ethernet	14
1.1.4. Giao thức liên kết dữ liệu Ethernet	25
<i>1.2. Khái niệm về chuyển mạch LAN</i>	28
1.2.1. Giới thiệu các thiết bị LAN.....	28
1.2.2. Xử lý bên trong các switch Cisco	36
<i>1.3. Kiến thức về thiết kế LAN</i>	38
1.3.1. Miền xung đột và miền quảng bá.....	38
1.3.2. LAN ảo (VLAN).....	40
<i>1.4. Thuật ngữ thiết kế mạng LAN</i>	42
<i>1.5. Một số loại Switch của Cisco</i>	44
Câu hỏi và bài tập chương 1	46
Chương 2: VẬN HÀNH THIẾT BỊ TRONG MẠNG LAN	53
<i>2.1. Switch Cisco Catalyst 2960</i>	54
2.1.1. Giới thiệu	54
2.1.2. Truy cập giao diện dòng lệnh của Cisco IOS.....	55
<i>2.2. Cấu hình switch Ethernet</i>	66
2.2.1. Cấu hình các chức năng thông dụng	67
2.2.2. Cấu hình và vận hành LAN switch	75

Câu hỏi và bài tập chương 2.....	79
Chương 3: MẠNG NỘI BỘ ẢO (Virtual Local Area Network - VLAN)	83
3.1. Các khái niệm về mạng LAN ảo.....	83
3.2. Xây dựng trung kế với ISL và 802.1Q.....	85
3.2.1. Phương thức trung kế ISL Inter – Switch Link.....	87
3.2.2. Phương thức trung kế IEEE 802.1Q	88
3.2.3. So sánh ISL và IEEE 802.1Q.....	88
3.3. IP Subnets và VLAN.....	90
3.4. Giao thức trung kế VLAN.....	91
3.4.1. Hoạt động của VTP sử dụng các chế độ VTP server và client ...	92
3.4.2. Ba yêu cầu cho VTP để làm việc giữa các switch	94
3.4.3. Tránh VTP bằng cách sử dụng chế độ VTP transparent.....	95
3.4.4. Lưu trữ cấu hình VLAN.....	95
3.4.5. VTP Pruning (lược bỏ VTP).....	97
Câu hỏi và bài tập chương 3.....	99
Chương 4: GIAO THÚC CÂY BAO PHỦ SPANNING TREE PROTOCOLS	103
4.1. Giới thiệu	103
4.2. Các vấn đề liên quan đến STP	104
4.2.1. Giao thức cây bao phủ STP (802.1d).....	104
4.2.2. Các chức năng tùy chọn của STP	119
4.2.3. STP nhanh (IEEE 802.1w).....	122
4.2.4. Vai trò Port RSTP	125
4.3. Cấu hình và xác nhận STP	131
4.3.1. Đa thể hiện cho STP.....	132
4.3.2. Cấu hình các tham số ảnh hưởng đến sơ đồ cây bao phủ	133
4.3.3. Cấu hình chi phí port STP và độ ưu tiên của Switch	138
4.3.4. Cấu hình PortFast và BPDUGuard	141

4.3.5. Cấu hình EtherChannel	141
4.3.6. Cấu hình RSTP.....	143
4.4. Xử lý sự cố STP	144
4.4.1. Xác định switch root	145
4.4.2. Xác định các root port và không root port của các switch	146
4.4.3. Xác định port dành riêng cho mỗi phân đoạn LAN.....	149
4.4.4. Hội tụ STP.....	150
Câu hỏi và bài tập chương 4.....	151
PHẦN II: ĐỊNH TUYỀN	155
Chương 5: ĐỊA CHỈ IP VÀ PHÂN MẠNG CON.....	157
5.1. Địa chỉ IP và định tuyến	157
5.1.1. Địa chỉ IP	157
5.1.2. Địa chỉ công cộng và dành riêng.....	159
5.1.3. Địa chỉ IP phiên bản 6.....	160
5.1.4. Phân chia địa chỉ IP.....	161
5.1.5. Tổng quan định tuyến IP	163
5.2. Các phép toán được sử dụng khi phân chia mạng con	164
5.2.1. Chuyển đổi địa chỉ IP và mặt nạ từ thập phân sang nhị phân và ngược lại	165
5.2.2. Thực hiện phép toán nhị phân AND	166
5.2.3. Kí hiệu tiền tố.....	168
5.2.4. Tiền trình nhị phân để chuyển đổi giữa thập phân có chấm và ký hiệu tiền tố	168
5.2.5. Tiền trình thập phân để chuyển đổi giữa số thập phân có chấm và ký hiệu tiền tố	169
5.3. Phân tích và lựa chọn mặt nạ mạng	171
5.3.1. Phân tích mặt nạ mạng trong thiết kế mạng con có sẵn.....	172
5.3.2. Ba thành phần: mạng, mạng con và thiết bị.....	172
5.3.3. Tiền trình nhị phân: Tìm số mạng, mạng con và số bit thiết bị	173

5.3.4. Tiến trình thập phân: Tìm số bit mạng, mạng con và thiết bị...	174
5.3.5. Xác định số mạng con và số thiết bị mỗi mạng con	175
5.3.6. Số mạng con: Trừ đi 2, hay không.....	176
5.3.7. Ví dụ thực hành phân tích mặt nạ mạng con.....	177
5.4. Lựa chọn mạng con phù hợp với yêu cầu thiết kế.....	178
5.4.1. Tìm mặt nạ mạng có thể.....	179
5.4.2. Trường hợp nhiều mặt nạ mạng.....	181
5.4.3. Lựa chọn mặt nạ tối đa hóa số mạng con hay thiết bị.....	183
5.5. Phân tích các mạng con có sẵn	184
5.5.1. Tiến trình nhị phân tìm kiếm số mạng con	184
5.5.2. Tìm kiếm chỉ số mạng con: Dạng nhị phân rút gọn.....	186
5.5.3. Tìm kiếm nhị phân địa chỉ quảng bá mạng con	188
5.5.4. Tìm khoảng địa chỉ IP hợp lệ trong một mạng con.....	190
5.6. Tiến trình thập phân tìm kiếm mạng con, địa chỉ quảng bá và khoảng địa chỉ	192
5.6.1. Quy trình thập phân với các mặt nạ đơn giản	192
5.6.2. Tiến trình thập phân với các mặt nạ phức tạp	193
5.6.3. Quy trình thập phân tìm kiếm địa chỉ quảng bá.....	196
5.6.4. Tông kết quy trình thập phân để tìm mạng con, quảng bá và khoảng địa chỉ IP	197
Câu hỏi và bài tập chương 5.....	198
Chương 6: VẬN HÀNH ROUTER CISCO	203
6.1. Cài đặt router Cisco	203
6.1.1. Cài đặt router cho các doanh nghiệp	204
6.1.2. Router dịch vụ tích hợp của Cisco	205
6.1.3. Cài đặt vật lý	206
6.2. Cài đặt các router truy cập Internet	207
6.2.1. Cài đặt SOHO với một switch, router và cáp modem tách biệt.....	207
6.2.2. Một cài đặt SOHO với switch, router và DSL modem tích hợp.....	209

6.3. Giao diện dòng lệnh của router Cisco	2
6.3.1. So sánh giữa dòng lệnh Router và Switch	2
6.3.2. Các giao tiếp của router	2
6.3.3. Mã trạng thái giao tiếp	2
6.3.4. Địa chỉ IP cho giao tiếp Router	2
6.3.5. Băng thông và xung đồng hồ trên giao tiếp Serial.....	2
6.4. Cổng phụ (auxiliary) của router.....	2
6.5. Nâng cấp phần mềm IOS của Cisco và tiến trình khởi động phần mềm IOS của Cisco	2
6.6. Tiến trình khởi động phần mềm IOS của Cisco	2
6.6.1. Ba hệ điều hành của Router	2
6.6.2. Thanh ghi cấu hình.....	2
6.6.3. Cách router chọn OS để nạp	2
6.6.4. Câu lệnh show version và tìm kiếm giá trị của thanh ghi cấu hình	2
Câu hỏi và bài tập chương 6.....	2
Chương 7: ĐỊNH TUYẾN TÌNH VÀ CON ĐƯỜNG KẾT NỐI TRỰC TIẾP	2
7.1. Định tuyến và đánh địa chỉ IP	2
7.2. Định tuyến IP	2
7.2.1. Địa chỉ IP và phân mạng con	2
7.2.2. Chuyển tiếp IP bằng cách tìm kiếm con đường phù hợp nhất ..	2
7.2.3. DNS, DHCP, ARP và ICMP	2
7.2.4. Phân mảnh và MTU	2
7.3. Các con đường đến mạng con kết nối trực tiếp	2
7.3.1. Địa chỉ IP thứ cấp.....	2
7.3.2. Các con đường tĩnh	2
7.3.3. Lệnh ping mở rộng	2
7.3.4. Các con đường tĩnh mặc định	2
Câu hỏi và bài tập chương 7.....	2

Chương 8: VẬN HÀNH ROUTER CISCO	26
8.1. Chính sách kiểm soát truy cập IP chuẩn	26
8.1.1. Các khái niệm IP ACL Chuẩn.....	26
8.1.2. Cấu hình chính sách truy cập IP chuẩn	27
8.2. Chính sách kiểm soát truy cập IP mở rộng	27
8.2.1. Các khái niệm IP ACL mở rộng	27
8.2.2. So khớp số port TCP và UDP	28
8.2.3. Cấu hình IP ACL mở rộng	28
8.2.4. Quản lý cấu hình ACL	28
Câu hỏi và bài tập chương 8.....	29
Chương 9: GIAO THỨC ĐỊNH TUYẾN	29
9.1. Tổng quan về giao thức định tuyến động.....	29
9.1.1. Chức năng giao thức định tuyến	30
9.1.2. Giao thức định tuyến nội và ngoại	30
9.1.3. So sánh các IGP	30
9.2. Giao thức định tuyến Distance Vector	30
9.2.1. Khái niệm	30
9.2.2. Hoạt động của distance vector trong mạng ôn định.....	31
9.2.3. Ngăn vòng lặp Distance Vector	31
9.2.4. Tông kết về Distance Vector.....	32
9.3. Giao thức định tuyến Link – State	32
9.3.1. Xây dựng cùng LSDB trên mọi router.....	32
9.3.2. Thuật toán Dijkstra để tìm đường đi tốt nhất.....	32
9.3.3. Hội tụ với giao thức Link – State	32
9.3.4. Tóm tắt và so sánh với giao thức Distance Vector	32
9.4. Giao thức định tuyến RIP – 2	33
9.4.1. Khái niệm cơ bản	33
9.4.2. Cấu hình và xác nhận RIP – 2	33
9.5. Giao thức định tuyến OSPF	33

9.5.1. Giao thức OSPF và hoạt động.....	3
9.5.2. Cấu hình OSPF.....	3
9.6. Giao thức định tuyến EIGRP	2
9.6.1. Hoạt động và khái niệm EIGRP.....	2
9.6.2. Cấu hình và xác nhận EIGRP	2
Câu hỏi và bài tập chương 9.....	2
Chương 10: ĐỊNH TUYẾN TRÊN HỆ THỐNG CÓ PHÂN CHIA MẠNG CON VỚI MẶT NẠ MẠNG THAY ĐỔI.....	2
10.1. Định tuyến phân lớp và không phân lớp.....	2
10.1.1. Tóm tắt việc sử dụng các thuật ngữ Classless và Classful.....	2
10.1.2. So sánh định tuyến phân lớp và không phân lớp	2
10.2. Mặt nạ mạng có chiều dài thay đổi VLSM Variable Length Subnet Mask (VLSM)	4
10.2.1. Giới thiệu	4
10.2.2. Giao thức định tuyến phân lớp và không phân lớp	4
10.2.3. Trùng lắp mạng con VLSM	4
10.2.4. Gộp các con đường	4
10.2.5. Tự động gộp đường và các mạng phân lớp không liên tục.....	4
Câu hỏi và bài tập chương 10.....	4
Chương 11: CÁU HÌNH KẾT NỐI MẠNG DIỆN RỘNG - WAN	4
11.1.Cấu hình kết nối WAN điểm – điểm.....	4
11.1.1. Cấu hình HDLC	4
11.1.2. Cấu hình PPP	4
11.2. Cấu hình router truy cập Internet	4
11.2.1. Các bước cấu hình router truy cập Internet.....	4
11.2.2. Xác nhận router truy cập Internet	4
Câu hỏi và bài tập chương 11.....	4
Danh mục các từ viết tắt.....	4
Tài liệu tham khảo	4

GIÁO TRÌNH
CHUYÊN MẠCH VÀ ĐỊNH TUYÉN

Chịu trách nhiệm xuất bản
NGUYỄN THỊ THU HÀ

Biên tập: NGÔ MỸ HẠNH
NGUYỄN TIỀN SỸ
Trình bày sách: NGUYỄN THANH HƯƠNG
Sửa bản in: NGUYỄN TIỀN SỸ
TRỊNH THU CHÂU

Thiết kế bìa: TRẦN HỒNG MINH

In 400 bản, khổ 17x24 cm tại Trung tâm In, Kỹ thuật và Dịch vụ Ánh
Cơ quan Đại diện Thông tấn xã Việt Nam tại Đà Nẵng

Số đăng ký kế hoạch xuất bản 750-2010/CXB/1-550/TTTT

Số quyết định xuất bản: 463/QĐ-NXB TTTT ngày 31 tháng 12 năm 2010

In xong nộp liên chiểu tháng 01 năm 2011

