

CCNA

HỌC KỲ 2

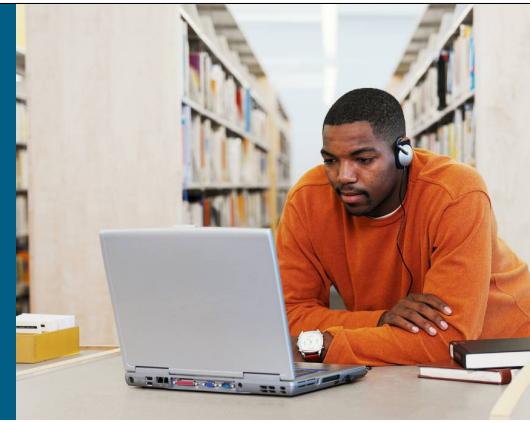
**Tài liệu hướng dẫn
Version 1.0**

Mục Lục

(Học kỳ 2)

<u>Bài 1:</u> Tìm hiểu chức năng định tuyến.....	1-1
<u>Bài 2:</u> Tìm hiểu hệ nhị phân.....	2-1
<u>Bài 3:</u> Cấu trúc địa chỉ mạng.....	3-1
<u>Bài 4:</u> Khởi động một router.....	4-1
<u>Bài 5:</u> Cấu hình Cisco Router.....	5-1
<u>Bài 6:</u> Quá trình phân phối gói dữ liệu.....	6-1
<u>Bài 7:</u> Tìm hiểu về bảo mật trên Cisco Router.....	7-1
<u>Bài 8:</u> Sử dụng Cisco SDM.....	8-1
<u>Bài 9:</u> Sử dụng Cisco Router như là một DHCP server.....	9-1
<u>Bài 10:</u> Truy xuất vào các thiết bị từ xa.....	10-1
<u>Bài 11:</u> Hiểu về các công nghệ mạng diện rộng.....	11-1
<u>Bài 12:</u> Cho phép kết nối Internet.....	12-1
<u>Bài 13:</u> Cấu hình định tuyến tĩnh.....	13-1
<u>Bài 14:</u> Cấu hình đón gói cổng serial.....	14-1
<u>Bài 15:</u> Cấu hình RIP.....	15-1
<u>Bài 16:</u> Discovering neighbors on the network.....	16-1
<u>Bài 17:</u> Quản lý quá trình khởi động và cấu hình của Cisco Router	17-1
<u>Bài 18:</u> Quản lý thiết bị Cisco	18-1

Bài 1: Tìm hiểu chức năng định tuyến



Kết nối LAN

1-1

Tổng quan

Định tuyến (Routing) là quá trình chuyển một gói dữ liệu giữa những mạng hoặc mạng con sử dụng thiết bị lớp 3 – router hay gateway. Tiến trình routing được thực hiện thông qua bảng định tuyến, các giao thức và các thuật toán để định ra con đường tốt nhất để dẫn dữ liệu. Router đóng vai trò to lớn trong việc mở rộng hệ thống mạng bằng cách cách ly các vùng xung đột và các vùng broadcast. Hiểu được quá trình vận hành của router sẽ giúp chúng ta biết rõ hơn về hệ thống mạng được kết nối với nhau như thế nào và quá trình truyền dẫn dữ liệu trong hệ thống mạng được thực thi ra sao. Bài học này sẽ mô tả quá trình vận hành của routing.

Mục tiêu

Bạn sẽ có khả năng mô tả sự vận hành của Cisco router trong việc kết nối nhiều hệ thống mạng sau khi kết thúc bài học này qua những nhiệm vụ sau:

- Mô tả đặc tính vật lý của router và chức năng của router trong quá trình phân phối gói dữ liệu IP
- Mô tả phương pháp được sử dụng trong việc xác định đường truyền tối ưu để truyền dữ liệu

- Liệt kê những đặc tính của bảng định tuyến và chức năng của nó trong việc xác định đường
- Mô tả những đặc tính của những tuyến tĩnh (static route), tuyến động (dynamic route), tuyến kết nối trực tiếp (directly connected route) và tuyến mặc định (default route)
- Liệt kê những đặc điểm của các giao thức định tuyến được dùng để xây dựng và duy trì bảng định tuyến một cách tự động

Routers

Cisco 2800 Series Router



- Router có các thành phần sau:
 - CPU
 - Mạch chủ
 - RAM
 - ROM
- Router có các cổng mạng để gán địa chỉ.
- Router có 2 loại cổng chính sau:
 - Console: Gắn vào đầu cuối để quản lý
 - Network: Những cổng LAN và WAN
- Router chuyển gói dữ liệu dựa trên bảng định tuyến.

1-3

Router hay gateway là thiết bị mạng dùng để định ra con đường tối ưu trong quá trình truyền dữ liệu. Giữa tất cả các router đều có những đặc tính chung cụ thể. Chủ đề này mô tả các đặc tính của router.

Router là một thành phần cần thiết trên một hệ thống mạng lớn sử dụng bộ giao thức TCP/IP bởi router có khả năng cung cấp khả năng mở rộng hệ thống mạng trên các vùng địa lý khác nhau. Những đặc tính sau đây là những đặc tính chung của các router:

• Router có các thành phần sau, cũng là những thành phần cấu tạo nên PC và Switch:

- CPU
- Mạch chủ
- RAM
- ROM

• Router có các card mạng để gán địa chỉ IP

• Router có các loại cổng sau:

- Cổng Console: Các thiết bị đầu cuối có thể sử dụng cổng console để quản lý, cấu hình và điều khiển router. Cổng console có thể được tìm thấy trên hầu hết các router.

- Cổng mạng: Router có rất nhiều cổng mạng, bao gồm cho cả LAN và WAN.

Chức năng router

```
RouterX# show ip route
1 { D 192.168.1.0/24 [90/25789217] via 10.1.1.1
    R 192.168.2.0/24 [120/4] via 10.1.1.2
    O 192.168.3.0/24 [110/229840] via 10.1.1.3 } 2
```

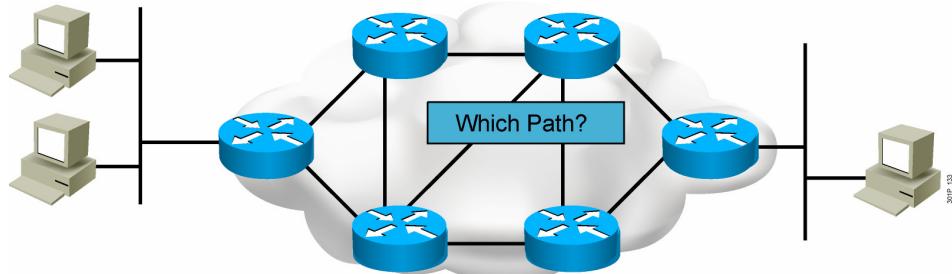
1. Giúp các router khác nhận biết sự thay đổi
2. Định ra nơi để đưa dữ liệu đi

1-4

Router có hai chức năng chính sau:

- Xác định đường: Router phải duy trì bảng định tuyến và đảm bảo rằng tất cả các router khác biết về sự thay đổi trên hệ thống mạng. Router làm được điều này nhờ vào các giao thức định tuyến được dùng để trao đổi về thông tin mạng với các router khác từ bảng định tuyến trên router. Các router có khả năng quảng bá bảng định tuyến theo chu kỳ cố định, nhưng việc này khiến hệ thống mạng khó mở rộng và phát sinh một số vấn đề khi hệ thống mạng thay đổi.
- Chuyển gói dữ liệu: Router sử dụng bảng định tuyến để xác định nơi sẽ gửi gói dữ liệu, router chuyển các gói dữ liệu qua các cổng mạng của mình đến mạng đích dựa trên địa chỉ IP đích được chứa trong gói dữ liệu.

Tìm đường

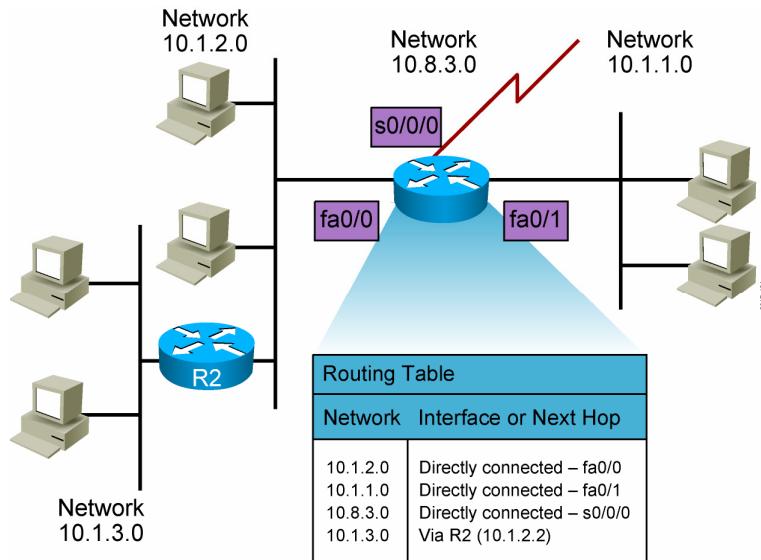


1-5

- Trong suốt quá trình tìm đường trên hệ thống mạng, router ước định những tuyến có khả năng truyền dữ liệu đến đích. Chủ đề này sẽ mô tả vấn đề làm thế nào router có thể xác định được con đường hiệu quả nhất để dẫn dữ liệu.
- Có ba loại tuyến tồn tại trong bảng định tuyến có thể được sử dụng để chọn ra con đường tốt nhất về một mạng nào đó:
 - Định tuyến tĩnh (static routing): loại định tuyến này yêu cầu người quản trị nhập vào các tuyến bằng tay
 - Định tuyến động (dynamic routing): loại định tuyến này tự động xây dựng bảng định tuyến bằng cách sử dụng các thông tin lấy trong các giao thức định tuyến
 - Định tuyến mặc định (default route): sử dụng loại định tuyến này thì không cần phải chỉ rõ các tuyến đến từng mạng cụ thể. Phương pháp định tuyến mặc định có thể được cấu hình bằng tay hay học từ một giao thức định tuyến khác.
- Bảng định tuyến sẽ chứa một tuyến cho một mạng nào đó. Nếu có nhiều hơn một thông tin nguồn chỉ đến nhiều tuyến khác nhau cho cùng một mạng nào đó thì tiến trình định tuyến phải lựa chọn nguồn thông tin nào sẽ được đưa lên bảng định tuyến.

Những nguồn định tuyến này xuất hiện khi ta dùng nhiều giao thức định tuyến, định tuyến tĩnh hay thậm chí là các thông tin định tuyến mặc định cùng chạy đồng thời. Các giao thức định tuyến sử dụng những metric khác nhau để đo khoảng cách trên những tuyến đường đến một mạng nào đó. Do không thể trực tiếp sử dụng các thông tin mạng lại bởi các giao thức định tuyến khác nhau, Cisco đã đưa ra khái niệm trọng số cho mỗi nguồn thông tin định tuyến và trọng số này được biết đến như khoảng cách quản trị (administrative distance). Những nguồn thông tin tin cậy nhất sẽ có khoảng cách quản trị nhỏ nhất.

Bảng định tuyến



1-7

• Như là một phần trong toàn bộ quá trình định tuyến, bảng định tuyến sẽ là nơi dùng để xác định những địa chỉ mạng cụ thể và cách để với về những mạng đó. Chủ đề này sẽ mô tả chức năng của bảng định tuyến trong tiến trình định tuyến.

• Metric trong tiến trình định tuyến sẽ rất khác nhau tùy thuộc vào giao thức định tuyến nào được sử dụng. Hình trên thể hiện cách router giữ bảng thông tin định tuyến dùng để chuyên dữ liệu đi.

Thông tin bảng định tuyến

Bảng định tuyến bao gồm một danh sách có thứ tự những địa chỉ mạng được biết đến thông qua các giao thức định tuyến động, phương pháp định tuyến tĩnh hoặc những mạng kết nối trực tiếp. Bảng định tuyến bao gồm các thông tin địa chỉ mạng đích và các chặng liên quan để với đến những mạng đích đó. Những mối liên quan này sẽ giúp router biết được các địa chỉ mạng đang được gắn trực tiếp vào router hay qua các router khác, các router khác trong trường hợp này được gọi là router chặng kế (next-hop router). Khi nhận được một gói dữ liệu, router sẽ đọc địa chỉ đích gói dữ liệu, tra bảng định tuyến để tìm ra con đường dẫn dữ liệu tốt nhất. Nếu không có tuyến nào tồn tại cho một địa chỉ mạng cụ thể, router sẽ hủy gói dữ liệu và gửi gói thông tin ICMP thông báo về phía gửi.

Ở hình trên, bảng định tuyến chứa thông tin thể hiện: khi router nhận một gói dữ liệu với địa chỉ đích thuộc về mạng 10.1.3.0 router sẽ gửi gói dữ liệu này qua router R2.

Thông tin cập nhật

Các router giao tiếp với nhau và duy trì bảng thông tin định tuyến bằng cách trao đổi cho nhau các gói cập nhật về thông tin định tuyến. Tùy vào những giao thức định tuyến cụ thể, các gói cập nhật này có thể gửi theo chu kỳ hoặc chỉ gửi khi có sự thay đổi xảy ra trên hệ thống mạng. Thông tin chứa trong gói dữ liệu cập nhật bao gồm địa chỉ mạng đích và các metric để đến mạng đó. Bằng cách phân tích các gói cập nhật nhận được từ router bên cạnh, router có thể xây dựng và duy trì bảng thông tin định tuyến của mình.

Các dòng định tuyến

- Kết nối trực tiếp: Router gắn trực tiếp vào mạng này
- Định tuyến tĩnh: Tuyến được đưa vào bởi người quản trị
- Định tuyến động: Học bằng cách trao đổi bảng định tuyến
- Tuyến mặc định: Học tĩnh hay động, được dùng khi không có một mạng nào được chỉ ra

1-9

• Router có thể học các địa chỉ mạng qua những tuyến tĩnh, động, kết nối trực tiếp hay những tuyến mặc định. Chủ đề này mô tả những loại tuyến này.

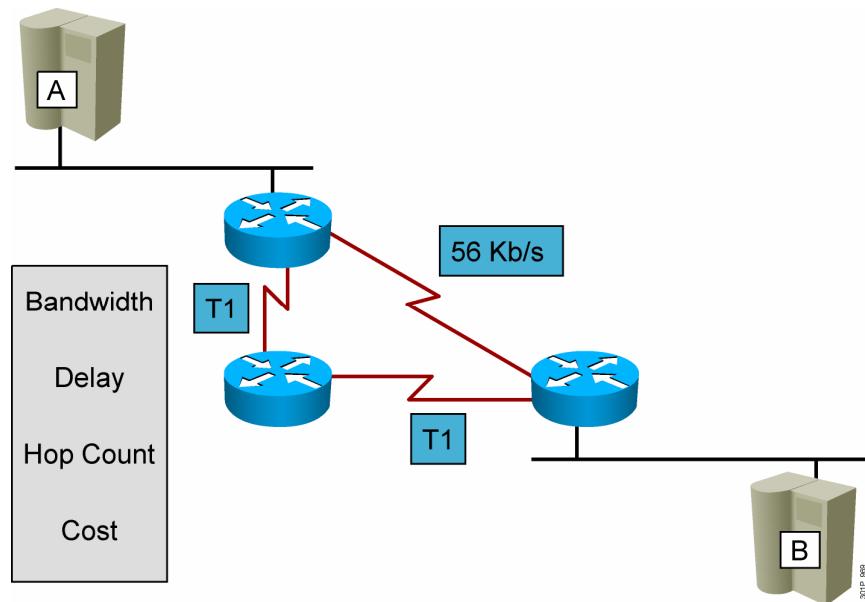
• Tuyến kết nối trực tiếp: những tuyến này có được là do các cổng của router trực tiếp gắn vào những đoạn mạng khác nhau. Đây là phương pháp cụ thể nhất trong việc quảng bá bảng thông tin định tuyến. Nếu một cổng bị lỗi hoặc bị đóng lại bởi người quản trị, dòng tuyến của mạng này sẽ bị xóa khỏi bảng thông tin định tuyến. Khoảng cách quản trị cho những tuyến kết nối trực tiếp bằng 0 do đó đây là những tuyến được tin cậy nhất và sẽ được ưu tiên trên những dòng tuyến khác chỉ cùng về địa chỉ mạng đó.

• Tuyến tĩnh: những tuyến này được cấu hình bằng tay và đưa trực tiếp vào bảng định tuyến của router. Khoản cách quản trị mặc định cho những tuyến tĩnh là 1, do vậy, những tuyến này sẽ được nằm trong bảng định tuyến trừ khi cùng tồn tại các tuyến kết nối trực tiếp cho cùng những địa chỉ mạng này. Phương pháp định tuyến tĩnh phù hợp cho hệ thống mạng nhỏ và các địa chỉ mạng không thay đổi thường xuyên.

• Tuyến động: là những tuyến được học từ các router và được cập nhật theo sự thay đổi của hệ thống mạng. Luôn luôn có một sự chậm pha giữa thời gian bắt đầu xuất hiện thay đổi cho đến khi toàn bộ các router nhận biết sự thay đổi này. Thời gian gián đoạn cho đến khi các router phản ánh đúng sự thay đổi gọi là thời gian hội tụ. Thời gian hội tụ càng nhỏ càng tốt. Phương pháp định tuyến động phù hợp trên những hệ thống mạng lớn bởi vì có rất nhiều địa chỉ mạng tồn tại và có nhiều sự thay đổi diễn ra trên hệ thống này.

•Tuyến mặc định: đây là một tùy chọn được sử dụng khi không có một tuyến cụ thể nào được tìm thấy trong bảng định tuyến. Các tuyến mặc định có thể được đưa vào bảng định tuyến bằng tay hay nhờ vào các giao thức định tuyến động khác.

Routing Metrics



1-11

- Có những giao thức định tuyến sử dụng những các thức và metric riêng của nó để xây dựng và cập nhật bảng định tuyến một cách tự động. Chủ đề này mô tả về giá trị metric và các phương thức mà các giao thức định tuyến dùng.

- Giá trị Metric

Khi một giao thức cập nhật bảng định tuyến, nhiệm vụ chính là phải xác định được thông tin nào tốt nhất bao gồm trong bảng thông tin định tuyến. Thuật toán định tuyến sẽ sinh ra một con số, gọi là metric, cho mỗi tuyến đến một mạng đích. Những giao thức tinh tế có thể chọn đường dẫn dựa trên rất nhiều metric khác nhau và hợp chúng lại thành một metric tổng hợp. Metric càng nhỏ tuyến dẫn đường càng tốt.

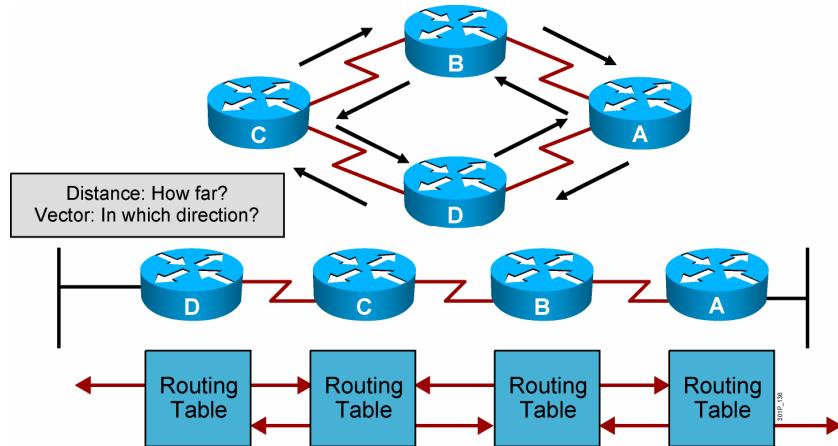
- Metric có thể được tính dựa trên một hoặc nhiều đặc tính của đường truyền. Sau đây là các loại metric được sử dụng phổ biến bởi các giao thức định tuyến:

- Băng thông (bandwidth): dung lượng dữ liệu của đường truyền.
- Độ trễ (delay): thời gian để chuyển gói dữ liệu trên đường truyền từ nguồn đến đích, giá trị này phụ thuộc vào băng thông, hàng đợi trên các router, nghẽn trên hệ thống mạng và khoảng cách đường truyền

- Số chặng (hop count): số lượng router mà gói dữ liệu sẽ phải vượt qua trước khi tới đích (ở hình trên, hop count từ A đến B là 2 chặng)

- Giá (cost): là một giá trị tùy ý được gán bởi người quản trị, thông thường sẽ được tính dựa trên băng thông, sự chủ định của người quản trị, hay sốt số phương pháp tính toán khác.

Giao thức định tuyến Distance Vector



Theo chu kỳ cập nhật nguyên bảng định tuyến cho router lân cận và tích lũy dần về khoảng cách

1-13

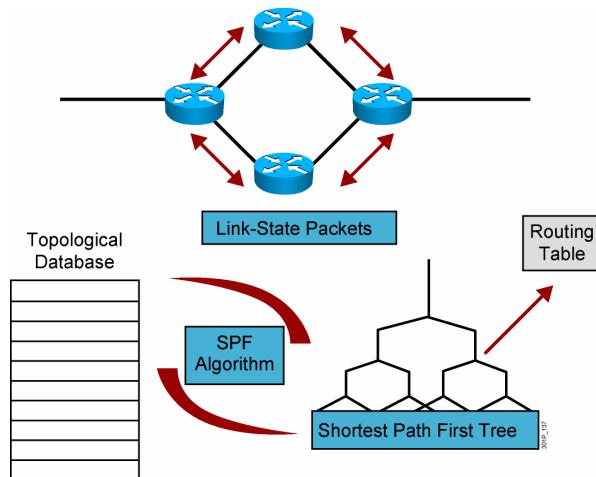
Phương pháp định tuyến

Các giao thức định tuyến được thiết kế dựa trên các phương pháp định tuyến sau:

- Distance Vector Routing: trong phương pháp distance vector, router không cần phải biết tất cả toàn bộ những tuyến đến tất cả các đoạn mạng, router chỉ biết hướng và khoảng cách để gửi gói dữ liệu đến đích. Phương pháp này chỉ định ra hướng (vector) và khoảng cách (distance) để đi đến một đích nào đó. Thuật toán distance vector cứ theo chu kỳ 30s sẽ gửi ra tất cả hoặc một phần thông tin bằng định tuyến cho các router kế cận. Những router chạy thuật toán distance vector sẽ gửi cập nhật theo chu kỳ mà không cần có sự thay đổi nào xảy ra trên hệ thống mạng. Bằng cách nhận thông tin bằng định tuyến từ router kế cận, router có thể kiểm tra tất cả những địa chỉ mạng đã biết và thay đổi bảng thông tin định tuyến của nó dựa trên những thông tin này. Tiến trình như vậy gọi là định tuyến qua lời đồn (Routing by rumor) bởi vì kiến thức về mô hình mạng mà router có được là dựa trên bảng thông tin định tuyến của router kế cận.

Một ví dụ của giao thức định tuyến theo phương pháp distance vector là RIP (Routing Information Protocol) và RIP sử dụng hop count làm metric.

Giao thức định tuyến Link-State



Sau khi tràn ngập dữ liệu lúc đầu, trao đổi thông tin link-state khi xảy ra thay đổi trên hệ thống

1-14

- Link state Routing: với phương pháp định tuyến này, các router có găng tự xây dựng mô hình mạng cho riêng mình. Mỗi router sẽ gửi ra một thông điệp vào hệ thống mạng khi nó được kích hoạt để liệt kê thông tin về những mạng đang được gắn kết trực tiếp và trạng thái của những kết nối này. Router sử dụng các thông tin này để xây dựng mô hình mạng cho chính mình và sau đó sẽ tìm ra những tuyến tốt nhất dựa trên mô hình này. Những giao thức link state sẽ phản ứng khi mô hình mạng thay đổi bằng cách gửi ngay các gói cập nhật cho thông tin thay đổi này. Link state cũng có hình thức gửi cập nhật theo chu kỳ với một chu kỳ dài khoảng vào 30 phút.

Khi một kết nối thay đổi trạng thái, thiết bị phát hiện được sự thay đổi này sẽ tạo ra một thông tin cập nhật liên quan đến kết nối đó và sẽ thông báo cho toàn bộ các router còn lại. Mỗi router nhận được thông tin cập nhật này sẽ cập nhật lại bảng định tuyến và chuyển tiếp thông tin cập nhật này đến các router kế cận khác. Quá trình gửi cập nhật tràn ngập như thế này là cần thiết để đảm bảo rằng tất cả các router sẽ cập nhật được cơ sở dữ liệu trước khi cập nhật lại bảng thông tin định tuyến cho mô hình mạng mới.

Ví dụ cho giao thức kiểu link-state là OSPF (Open Shortest Path First) và IS-IS (Intermediate System – Intermediate System).

Tóm tắt

- Router có các thành phần cụ thể tương tự như máy tính và switch.
- Router có 2 chức năng chính trong việc chuyển gói là duy trì bảng định tuyến và tìm ra đường tốt nhất để đưa dữ liệu đi.
- Router có thể dùng những phương pháp khác nhau để định tuyến: tĩnh, động và tuyến mặc định.
- Bảng định tuyến cung cấp danh sách có thứ tự những tuyến tốt nhất đến các đích.
- Các thuật toán định tuyến xử lý tiến trình cập nhật và phổ biến bảng định tuyến.

1-15

Tóm tắt (tt.)

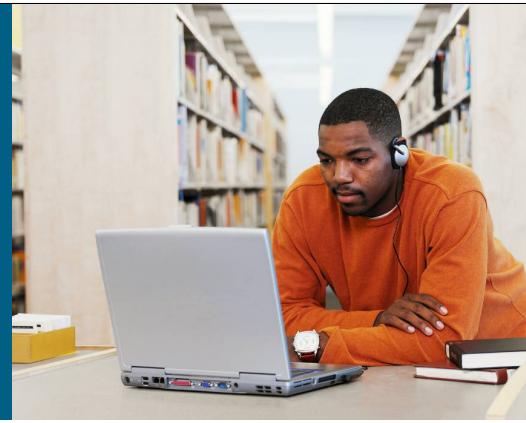
- Những metric phổ biến bao gồm bandwidth, delay, hop count, và cost.
- Giao thức distance vector xây dựng và cập nhật bảng định tuyến một cách tự động bằng cách gửi tất cả hay một phần bảng định tuyến cho router lân cận. Thuật toán định ra hướng và khoản cách đến các mạng đích.
- Giao thức link-state xây dựng và cập nhật bảng định tuyến một cách tự động sử dụng thuật toán của Link-state.
- Cisco phát triển EIGRP là sự kết hợp những đặc tính tốt nhất giữa distance vector và link-state.

1-16



1-17

Bài 2: Tìm hiểu hệ nhị phân



Kết nối LAN

2-1

Tổng quan

Tất cả những hệ thống máy tính đều hoạt động dựa trên quá trình chuyển giữa trạng thái bật và tắt. Đây được gọi là hệ thống nhị phân, trạng thái tắt được đại diện bằng số 0 và trạng thái bật được đại diện bằng số 1. Một số nhị phân chỉ bao gồm hai trường hợp, 0 hoặc 1.

Địa chỉ mạng của thiết bị cũng sử dụng đến hệ thống nhị phân để xác định vị trí của thiết bị đó trên mạng. Địa chỉ IP được biểu diễn theo dạng thập phân được phân cách bởi các dấu chấm. Bài học này mô tả cách tính toán trong hệ nhị phân, cách chuyển đổi từ hệ thập phân sang nhị phân và ngược lại.

Mục tiêu

Cung cấp khả năng giúp chuyển đổi từ số thập phân sang nhị phân và ngược lại thông qua các nhiệm vụ sau:

- Mô tả hệ thập phân và nhị phân
- Mô tả tiến trình lũy thừa 2 (power of 2)
- Chuyển đổi từ số thập phân sang nhị phân
- Chuyển đổi từ số nhị phân sang thập phân

Số thập phân và nhị phân

- Số thập phân bao gồm các con số từ 0 đến 9.
- Số nhị phân được thể hiện bởi các chuỗi 0 và 1.

Decimal	Binary
0	0
1	1
2	10
3	11
4	100
5	101
6	110
7	111
8	1000
9	1001

Decimal	Binary
10	1010
11	1011
12	1100
13	1101
14	1110
15	1111
16	10000
17	10001
18	10010
19	10011

2-2

Hệ thập phân (cơ số 10) là hệ số được sử dụng trong tính toán hằng ngày, trong khi đó hệ nhị phân (cơ số 2) lại là nền tảng của việc tính toán trên các hệ thống điện toán. Chủ đề này mô tả về số thập phân và số nhị phân

Hệ thập phân có các số bao gồm: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Khi cần một số lượng lớn hơn 9, hệ thập phân bắt đầu từ 10 và cứ như thế cho đến 99 rồi lại bắt đầu lại với 100 và cứ thế bằng cách cộng thêm 1.

Hệ nhị phân chỉ dùng hai số 0 và 1. Do vậy số đầu tiên sẽ là 0, kế tiếp là 1. Nếu cần một số lượng lớn hơn 1, hệ nhị phân sẽ bắt đầu từ 10 và kết đến là 11, tiếp tục là 100, 101, 110, 111,... Hình trên thể hiện sự tương ứng giữa các số nhị phân và thập phân từ có giá trị từ 0 đến 19.

Sơ đồ số nhị phân và thập phân

Base-10 Decimal Conversion—63204829

	MSB							LSB
Base ^{exponent}	10^7	10^6	10^5	10^4	10^3	10^2	10^1	10^0
Column Value	6	3	2	0	4	8	2	9
Decimal Weight	10000000	1000000	100000	10000	1000	100	10	1
Column Weight	60000000	3000000	200000	0	4000	800	20	9

$$60000000 + 3000000 + 200000 + 0 + 4000 + 800 + 20 + 9 = 63204829$$

Base-2 Binary Conversion—1110100 (233)

	MSB							LSB
Base ^{exponent}	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Column Value	1	1	1	0	1	0	0	1
Decimal Weight	128	64	32	16	8	4	2	1
Column Value	128	64	32	0	8	0	0	1

$$128 + 64 + 32 + 0 + 8 + 0 + 0 + 1 = 233$$

2-3

- Bit có trọng số nhỏ nhất và bit có trọng số lớn nhất
- Đa số chúng ta thì quen làm việc với hệ thập phân. Những cơ số đóng vai trò quan trọng trong các hệ số. Số 10 được biểu diễn bởi số 1 ở hàng chục và số 0 ở hàng đơn vị. Số 100 được biểu diễn bởi số 1 ở hàng trăm, số 0 ở hàng chục và số 0 ở hàng đơn vị.
- Với hệ nhị phân, số nằm ngoài cùng bên phải được gọi là bit có trọng số nhỏ nhất (LSB – Least Significant Bit) và số nằm ngoài cùng bên trái gọi là bit có trọng số lớn nhất (MSB – Most Significant Bit). Trọng số của các số nhị phân còn lại nằm trong khoảng giữa được tính theo sự kế cận của nó với LSB hay MSB.
- Sự chuyển đổi hệ nhị phân

Hiểu được hệ nhị phân là một điều kiện quan trọng bởi vì địa chỉ IPv4 được tạo thành bao gồm 32 bit nhị phân trong cấu trúc. 32 bit này được chia thành 4 cụm 8 bit, mỗi cụm như vậy được gọi là một bộ tám (octet). Dấu chấm được đặt giữa các octet để cách biệt chúng. (Byte là một tên khác để gọi cho một cụm 8 bit như vậy, nhưng trong module này, cụm 8 bit được gọi là octet).

Có nhiều lớp địa chỉ được tạo ra dựa trên phạm vi của các octet. Việc nhóm cụm 8 bit này lại cũng giúp dễ dàng cho việc chuyển đổi hơn là chuyển đổi với 32 bit. Khi thực hiện chuyển đổi, ta chỉ thực hiện trên từng octet tại một thời điểm. Giá trị nhị phân lớn nhất của octet là 11111111 tương ứng với hệ thập phân là 255.

Lũy thừa 2

Power of 2	Calculation	Value
2^0		1
2^1	2	2
2^2	$2 * 2$	4
2^3	$2 * 2 * 2$	8
2^4	$2 * 2 * 2 * 2$	16
2^5	$2 * 2 * 2 * 2 * 2$	32
2^6	$2 * 2 * 2 * 2 * 2 * 2$	64
2^7	$2 * 2 * 2 * 2 * 2 * 2 * 2$	128

2-4

Để hiểu được số nhị phân được sử dụng như thế nào trong việc đặt địa chỉ, bạn phải hiểu được tiến trình tính toán đổi từ số thập phân sang nhị phân và ngược lại. Chủ đề này mô tả tiến trình của phương pháp lũy thừa 2.

Hình trên sẽ được sử dụng để thuận tiện cho việc chuyển đổi giữa hệ thập phân và nhị phân.

Đổi từ thập phân sang nhị phân

Base ^{Exponent}	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Place Value	128	64	32	16	8	4	2	1
Example: Convert decimal 35 to binary	0	0	1	0	0	0	1	1

$$\begin{aligned}
 35 &= 2^5 + 2^1 + 2^0 \\
 35 &= (32 * 1) + (2 * 1) + (1 * 1) \\
 35 &= 0 + 0 + 1 + 0 + 0 + 0 + 1 + 1 \\
 35 &= \underline{\underline{00100011}}
 \end{aligned}$$

CC BY-SA

2-5

• Một số thập phân có thể chuyển đổi sang số nhị phân theo một tiến trình riêng biệt. Chủ đề này mô tả cách đổi từ một số thập phân sang số nhị phân.

• Hình trên thể hiện quá trình chuyển đổi đơn giản từ số thập phân 35 sang hệ nhị phân. Hàng trên cùng thể hiện cơ số 2 và các hàm mũ của nó. Hàng thứ hai thể hiện giá trị thập phân tương ứng của hàng thứ nhất và hàng thứ ba là các số nhị phân tương ứng. Bảng trên mô tả các bước để xác định các số nhị phân. Chú ý rằng hai bit đầu tiên của số nhị phân là 0, được gọi là những bit 0 đầu tiên. Trên thực tế số thập phân 35 chỉ bao gồm 6 bit nhị phân nhưng do địa chỉ IP được cấu thành từ các cụm 8 bit (octet) do vậy ta phải thêm vào hai bit 0 vào trước 6 bit giá trị của số 35 để đủ một octet.

• Quá trình đổi từ hệ thập phân sang nhị phân

Bước 1: như ví dụ trên, ta bắt đầu nhìn xem lũy thừa 2 nào lớn nhất có giá trị nhỏ hơn hay bằng với 35. Giá trị 128 không rơi vào trường hợp như vậy nên bit nhị phân tương ứng tại vị trí đó là 0.

Bước 2: 64 cũng như 128, không nhỏ hơn hay bằng 35, do vậy bit nhị phân tương ứng tại vị trí này cũng bằng 0

Bước 3: 2^5 (32) nhỏ hơn 35 vậy bit nhị phân tương ứng tại vị trí này bằng 1

Bước 4: giá trị 35 giờ chỉ còn 3 (35-32)

Bước 5: kiểm tra tiếp 16 có thỏa điều kiện nhỏ hơn bằng 3 hay không, trường hợp này không thỏa, do đó bit nhị phân tương ứng tại vị trí này bằng 0

Bước 6: giá trị kế tiếp là 8, ta có bit nhị phân tương ứng tại vị trí này cũng bằng 0

Bước 7: tương tự cho giá trị kế tiếp là 4, bit nhị phân tương ứng tại vị trí này cũng bằng 0

Bước 8: giá trị kế là 2, nhỏ hơn 3 vậy bit nhị phân tương ứng tại vị trí này bằng 1

Bước 9: kết quả của 3-2 ta còn lại 1

Bước 10: bit cuối cùng là 1 khớp với giá trị cuối cùng còn lại, do vậy bit nhị phân tương ứng tại vị trí này bằng 1

Cuối cùng viết lại các số nhị phân trong quá trình tính toán ta có giá trị sau chuyển đổi từ số thập phân 35 là: 00100011

Đổi từ nhị phân sang thập phân

Base ^{Exponent}	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Place Value	128	64	32	16	8	4	2	1
Example: Binary Number	1	0	1	1	1	0	0	1
Decimal Number Total: 185	128	0	32	16	8	0	0	1

$$\begin{aligned}
 10111001 &= (128 * 1) + (64 * 0) + (32 * 1) + (16 * 1) + (8 * 1) + (4 * 0) + (2 * 0) + (1 * 1) \\
 10111001 &= 128 + 0 + 32 + 16 + 8 + 0 + 0 + 1 \\
 10111001 &= \underline{185}
 \end{aligned}$$

2-7

Quá trình chuyển đổi từ hệ nhị phân sang thập phân cũng được thực hiện theo quá trình tương tự như quá trình chuyển đổi từ thập phân sang nhị phân đã thực hiện như trên

Bước 1: tìm vị trí giá trị tương ứng với bất kỳ bit 1 nào trong số nhị phân. Như ví dụ trên bit nhị phân nằm ngay cột 2^7 là 1 do đó giá trị thập phân tương ứng có được là 128

Bước 2: tại cột 2^6 (64) là 0 do vậy giá trị thập phân lúc này là $128 + 0 = 128$

Bước 3: tại cột 2^5 (32) là 1 do vậy giá trị thập phân lúc này là $128 + 32 = 160$

Bước 4: tại cột 2^4 (16) là 1 do vậy giá trị thập phân lúc này là $160 + 16 = 176$

Bước 5: tại cột 2^3 (8) là 1 do vậy giá trị thập phân lúc này là $176 + 8 = 184$

Bước 6: tại cột 2^2 và 2^1 đều là 0 do vậy giá trị thập phân không đổi = $184 + 0 + 0 = 184$

Bước 7: cuối cùng, tại cột còn lại 2^0 (1) là 1 do vậy giá trị thập phân lúc này là $184 + 1 = 185$.

Do đó kết quả cuối cùng ta có giá trị thập phân tương ứng của 10111001 là 185.

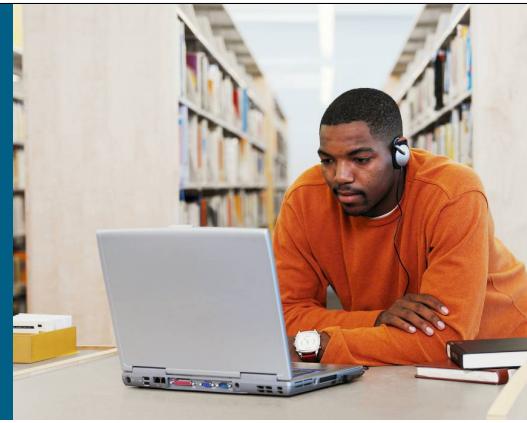
Tóm tắt

- Tất cả máy tính vận hành trên hệ nhị phân.
- Hệ nhị phân chỉ sử dụng các bit 0 và 1.
- Hệ thập phân sử dụng các con số từ 0 đến 9.
- Với hàm lũy thừa 2 ta có thể đổi từ thập phân sang nhị phân và ngược lại.



2-9

Bài 3: Cấu trúc địa chỉ mạng



Kết nối LAN

3-1

Tổng quan

Mạng con (subnet hay subnetwork) là một khái niệm rất phổ biến. Trong môi trường mạng, đó là khái niệm phân đoạn hệ thống mạng thành những bộ phận nhỏ có những địa chỉ riêng của nó. Để tạo ra các subnet, một số bit nằm trong phần host của địa chỉ IP sẽ được mượn để tạo ra các subnet. Bài học sẽ mô tả về chức năng của subnet và cách tính toán các subnet.

Mục tiêu

Cung cấp khả năng tính toán địa chỉ subnet thông qua các nhiệm vụ sau:

Mô tả mục tiêu và chức năng của subnet

Mô tả tiến trình tính toán những địa chỉ subnet và host khả dụng

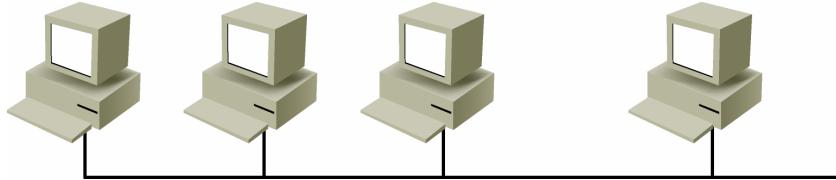
Mô tả làm cách cách thiết bị đầu cuối sử dụng subnet mask để định vị trí thiết bị đích

Mô tả cách router sử dụng subnet mask để định tuyến cho dữ liệu đến đích

Mô tả cơ cấu vận hành của subnet mask

Áp dụng nguyên tắc vận hành này vào các lớp địa chỉ A, B, C

Mạng phẳng



3-15

Vấn đề

- Tất cả các thiết bị chia sẻ cùng băng thông.
- Tất cả các thiết bị cùng nằm trong một broadcast domain.
- Khó để áp dụng các chính sách bảo mật.

3-2

• Quản trị mạng thông thường sẽ chia nhỏ hệ thống mạng, đặc biệt là trong môi trường mạng lớn, thành nhiều subnet khác nhau nhằm tạo ra khả năng phân địa chỉ một cách linh động. Chủ đề này mô tả mục tiêu, chức năng của subnet và cách định ra kế hoạch về địa chỉ.

• Một công ty chiếm hữu 3 tầng lầu của một toàn nhà sẽ có hệ thống mạng được chia theo các tầng, trên mỗi tầng lại được chia nhỏ thành từng văn phòng nhỏ. Suy nghĩ một tòa nhà này như một hệ thống mạng với 3 tầng là 3 subnet và mỗi văn phòng như một host trong hệ thống mạng này.

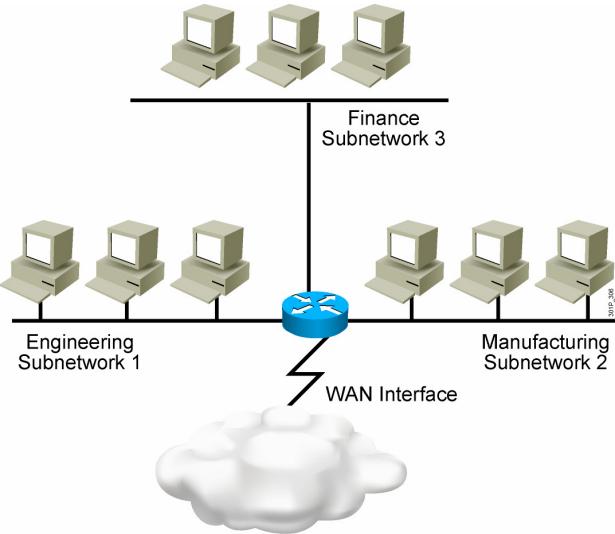
• Subnet sẽ phân đoạn các host trong hệ thống mạng. Nếu không có khái niệm subnet, hệ thống mạng chỉ là một mô hình phẳng. Một mô hình phẳng như vậy sẽ làm bẳng định tuyến của chúng ta ngắn hơn và chỉ dựa trên địa chỉ MAC lớp 2 để phân phối dữ liệu. MAC là dạng địa chỉ không phân cấp và khi hệ thống mạng càng lớn, băng thông của hệ thống mạng sẽ ít dần và trở nên kém hiệu quả.

- Những bất lợi của một mạng phẳng:
 - Tất cả các thiết bị sẽ chia sẻ cùng một băng thông
 - Tất cả các thiết bị chia sẻ cùng một vùng broadcast
 - Rất khó để áp đặt các chính sách bảo mật bởi vì hầu như không tồn tại một sự ngăn cách nào giữa các thiết bị

•Trong hệ thống mạng Ethernet gắn kết với nhau bởi HUB, mỗi host trong môi trường mạng này sẽ thấy tất cả các gói dữ liệu khác trên mạng. Trong môi trường gắn qua hệ thống chuyển mạch (switched-connected network) các host sẽ thấy gói dữ liệu broadcast. Trong trường hợp dữ liệu đưa ra lớn, khả năng va chạm là hoàn toàn có thể khi các thiết bị gửi dữ liệu ra đồng thời. Thiết bị phát hiện được và dụng sẽ phải ngưng truyền và sẽ cố gắng truyền lại trong một khoảng thời gian ngắn nhiên sau đó. Về phía người dùng, họ chỉ có thể cảm nhận được tiến trình này qua sự chậm đi của hệ thống mạng. Router có thể được sử dụng trong trường hợp này để chia cách mạng thành những những subnet khác nhau.

Subnetworks

- Mạng nhỏ hơn thì dễ quản lý hơn.
- Tổng lưu lượng dữ liệu sẽ giảm đi.
- Dễ dàng hơn trong việc áp đặt các chính sách bảo mật.

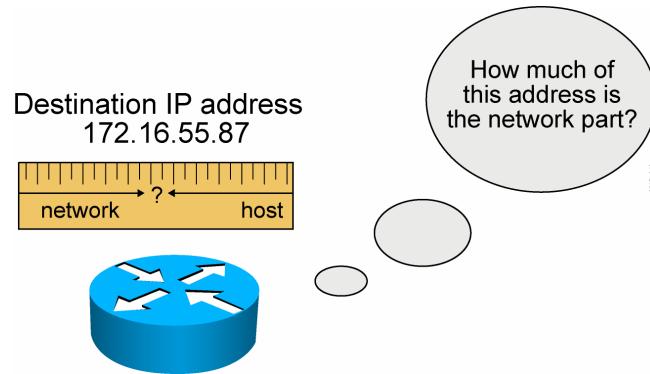


3-4

- Những lợi điểm của việc subnet hệ thống mạng được thể hiện như dưới:
- Hệ thống mạng càng nhỏ càng dễ quản lý và dễ dàng gắn kết với các nhu cầu chức năng cũng như phạm vi địa lý
- Tổng lưu lượng hệ thống mạng sẽ được giảm xuống do đó sẽ làm tăng khả năng hoạt động của hệ thống
- Bạn có thể dễ dàng áp dụng các chính sách bảo mật mạng tại những điểm liên kết nối giữa các subnet thay vì phải đặt trên toàn bộ hệ thống mạng
- Trong môi trường tồn tại nhiều hệ thống mạng, mỗi subnet có thể được gắn vào Internet qua một router như hình trên. Trong ví dụ này, hệ thống mạng được chia nhỏ thành nhiều subnet. Chi tiết bên trong môi trường mạng và làm cách nào hệ thống mạng được chia thành nhiều subnet sẽ trở nên không quan trọng đối với cách nhìn từ hệ thống mạng khác.
- Giá trị subnet mask xác định phần quan trọng trong địa chỉ IP, tầm quan trọng ở đây chính là ranh giới giữa phần network và phần host. Giá trị này sẽ ảnh hưởng đến quá trình định tuyến trong hệ thống mạng.

Chức năng của Subnet Mask

- Nối với router nhìn vào bao nhiêu bit khi thực hiện định tuyến
- Định ra các bit quan trọng
- Được sử dụng như một công cụ đo lường



Địa chỉ 2 cấp và 3 cấp

• Khi phương pháp xác định địa chỉ và các lớp địa chỉ IPv4 được phát triển, địa chỉ 2 lớp (bao gồm network và host) thoát đầu tỏa khá hiệu quả. Mỗi lớp địa chỉ (A, B và C) có giá trị subnet mask mặc định đi liền, và do subnet mask được định nghĩa trước, do vậy không cần phải bắt buộc cấu hình giá trị này.

• Khi số lượng các thiết bị gắn kết vào mạng ngày càng tăng, vấn đề không hiệu quả trong việc sử dụng địa chỉ mạng ngày càng trở nên rõ ràng hơn. Để giải quyết vấn đề này, cấp địa chỉ thứ 3, bao gồm subnet, đã được phát triển.

• Một địa chỉ subnet bao gồm phần mạng đầy đủ của lớp mạng nguyên gốc cộng thêm phần subnet. Đây cũng được xem như là phần mở rộng tiền tố mạng. Vùng subnet và vùng host được tạo ra từ phần host cũ của lớp mạng ban đầu. Để tạo ra các địa chỉ subnet, chúng ta mượn những bit từ vùng host nguyên gốc và phân định chúng thành những bit thuộc vùng subnet.

• Tuy nhiên, subnet sẽ không vận hành được nếu không có cách xác định phần địa chỉ nào giờ đây sẽ thuộc về phần mạng và phần nào là phần host. Do vậy, subnet mask cần phải được cấu hình rõ ràng.

Quá trình tạo subnet

•Địa chỉ subnet được tạo ra bằng cách lấy đi những bit của phần host thuộc về các lớp A, B hay C. Thông thường quản trị mạng sẽ phân định các địa chỉ subnet một cách cục bộ. Và cũng như địa chỉ IP, mỗi subnet phải là duy nhất.

•Khi tạo ra các subnet, một số địa chỉ IP sẽ bị mất đi, do vậy phải lường trước được tỷ lệ địa chỉ bị mất đi khi tạo ra các subnet. Phương pháp được sử dụng để tính toán số lượng của các subnet là lũy thừa của 2. Khi lấy đi một số bit từ vùng host, cần phải chú ý về số lượng subnet mới được tạo ra. Khi mượn 2 bit ta có thể tạo ra 4 subnet ($2^2 = 4$). Mỗi khi có một bit được mượn từ vùng host, số lượng subnet sẽ được tăng lên bằng với lũy thừa 2 số lượng bit mượn được đồng thời số lượng host cũng giảm đi theo công thức lũy thừa 2 như vậy.

Một số ví dụ được đưa ra như sau:

- Sử dụng 3 bit cho vùng subnet sẽ tạo ra 8 subnet ($2^3 = 8$)
- Sử dụng 4 bit cho vùng subnet sẽ tạo ra 16 subnet ($2^4 = 16$)
- Sử dụng 5 bit cho vùng subnet sẽ tạo ra 32 subnet ($2^5 = 32$)
- Sử dụng 6 bit cho vùng subnet sẽ tạo ra 64 subnet ($2^6 = 64$)
- Nói tóm lại, công thức sau đây được sử dụng để tính toán số lượng subnet
 - $\text{Số lượng subnet} = 2^s$ (s là số lượng số bit làm subnet)

Những Subnets và Hosts của lớp C



Number of Bits Borrowed (s)	Number of Subnets Possible (2^s)	Number of Bits Remaining in Host ID ($(8 - s = h)$)	Number of Hosts Possible Per Subnet ($2^h - 2$)
1	2	7	126
2	4	6	62
3	8	5	30
4	16	4	14
5	32	3	6
6	64	2	2
7	128	1	2

3-7

Tính số lượng host cho địa chỉ lớp C

- Mỗi khi 1 bit được mượn từ vùng host, vùng host lại bị giảm đi 1 bit có thể được sử dụng cho các host và số lượng địa chỉ host dùng để gán cho các host bị giảm đi theo công thức lũy thừa 2.
- Như ví dụ trên, xét một địa chỉ lớp C trong đó tất cả 8 bit trong octet cuối được sử dụng cho phần xác định host. Do vậy, có khoảng 256 địa chỉ có thể. Trên thực tế, giá trị thực sự để có thể phân định cho các host là 254 (256 - 2 địa chỉ để dành).
- Hãy tưởng tượng rằng địa chỉ lớp C được chia thành các subnet, nếu 2 bit được mượn từ 8 bit mặc định ban đầu, kích cỡ vùng host sẽ giảm xuống còn 6 bit. Sự kết hợp của tất cả các giá trị bit 0 và bit 1 xảy ra ở 6 bit còn lại sẽ tạo ra các địa chỉ để gán cho host trong mỗi subnet đó. Số lượng này, ban đầu là 256 giờ giảm xuống còn 64. Giá trị thực tế lúc này lại chỉ giảm còn 62 (64 - 2 địa chỉ để dành).
- Trong cùng một mạng lớp C, nếu 3 bit được mượn, kích cỡ vùng host sẽ giảm còn 5 bit và số lượng địa chỉ tổng cộng cho các host là 32 (2^5). Trong đó chỉ có 30 địa chỉ sử dụng được (32-2). Số lượng địa chỉ host có thể sử dụng được để gán cho subnet thì liên quan đến số lượng subnet được tạo ra. Ví dụ trong địa chỉ mạng lớp C số lượng subnet được tạo ra là 8 thì mỗi subnet bao gồm khoảng 30 địa chỉ host.

Những Subnets và Hosts của lớp B

Network . Network . 

Bits to Borrow

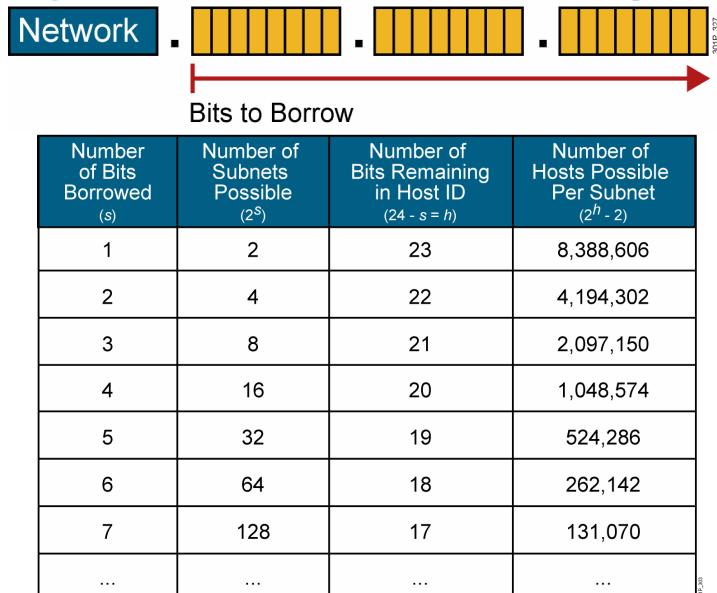
Number of Bits Borrowed (s)	Number of Subnets Possible (2^s)	Number of Bits Remaining in Host ID ($16 - s = h$)	Number of Hosts Possible Per Subnet ($2^h - 2$)
1	2	15	32,766
2	4	14	16,382
3	8	13	8,190
4	16	12	4,094
5	32	11	2,046
6	64	10	1,022
7	128	9	510
...

3-8

Tính số lượng host cho địa chỉ lớp B

- Xét một địa chỉ lớp B trong đó có 16 bit dùng cho phần xác định network và 16 bit sử dụng cho phần xác định host. Do vậy có khoảng 65,536 (2^{16}) địa chỉ có sẵn cho các host (thực tế là 65,534 địa chỉ sử dụng được sau khi trừ đi 2 địa chỉ broadcast và subnet)
- Bây giờ ta chia mạng lớp B thành các subnet. Nếu mượn 2 bit từ 16 bit mặc định, kích cỡ vùng host sẽ giảm xuống còn 14 bit. Sự kết hợp của tất cả các bit 0 và 1 của 14 bit còn lại sẽ tạo ra các địa chỉ cho subnet đó. Do vậy, số lượng host được gán trong subnet là 16,382 (2^{14}) địa chỉ.
- Trong cùng địa chỉ lớp B này, nếu 3 bit được mượn, kích cỡ vùng host sẽ giảm còn 13 bit và tổng số địa chỉ còn lại cho mỗi subnet là 8,192 (2^{13}). Số lượng địa chỉ thực sự sử dụng được là 8,190 ($8,192 - 2$).

Những Subnets và Hosts của lớp A

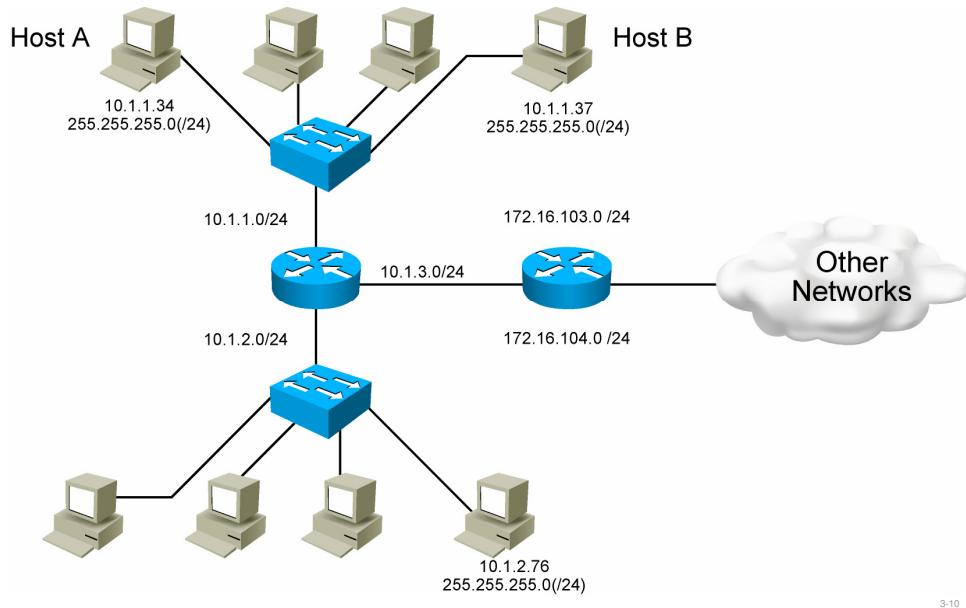


3-9

Tính số lượng host cho địa chỉ lớp A

- Cuối cùng, hãy xét hệ thống mạng lớp A, trong đó ta có 8 bit được dùng cho phần xác định network và 24 bit được sử dụng cho phần xác định host. Do vậy ta có khoảng 16,777,216 (2^{24}) địa chỉ trong trường hợp này dành cho các host (thực tế là 16,777,214 địa chỉ sau khi đã trừ đi 2 địa chỉ broadcast và subnet).
- Nay chia địa chỉ lớp A thành các subnet. Nếu 6 bit được mượn từ giá trị 24 bit mặc định, kích cỡ vùng host sẽ giảm còn 18 bit. Sự kết hợp của tất cả các bit 0 và 1 của 18 bit còn lại sẽ tạo ra các địa chỉ cho subnet đó. Do vậy, số lượng host thực tế được gán trong subnet là 16,777,214 ($2^{18} - 2$) địa chỉ.

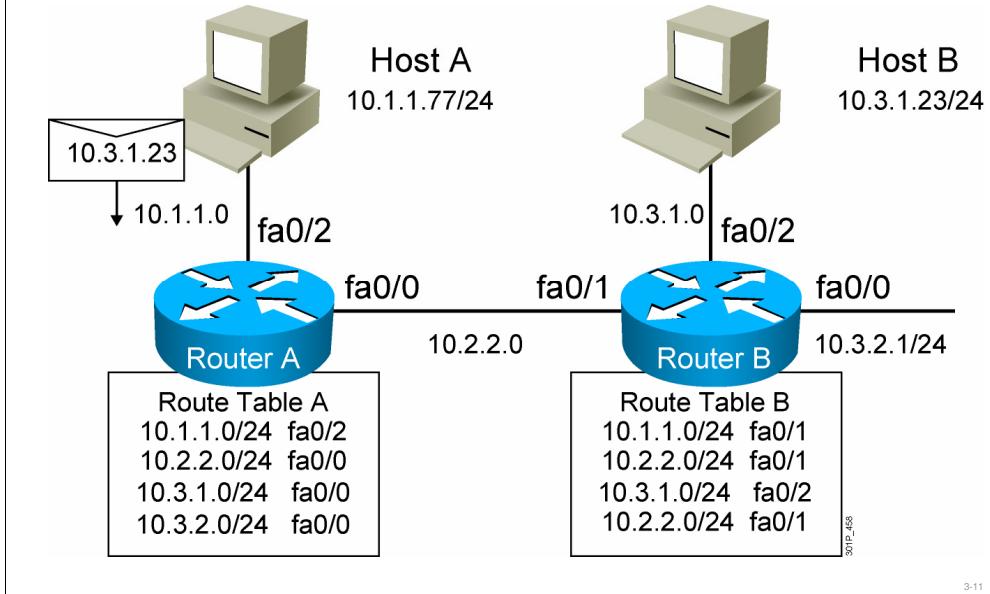
Subnet Mask của thiết bị đầu cuối



Cách sử dụng subnet mask của thiết bị đầu cuối

- Các hệ thống đầu cuối sử dụng subnet mask để so sánh phần địa chỉ mạng của mình với địa chỉ đích của dữ liệu sẽ được gửi. Chủ đề này mô tả tiến trình các thiết bị đầu cuối sử dụng giá trị subnet mask.
- Trước khi một hệ thống đầu cuối gửi một dữ liệu đến đích, đầu tiên nó sẽ xác định xem địa chỉ đích đó có thuộc hệ thống mạng LAN hay không. Nếu đúng, hệ thống sẽ dùng tiến trình ARP để tìm địa chỉ IP với địa chỉ MAC tương ứng của hệ thống đích. Nếu không đúng, dữ liệu sẽ được đưa đến cổng ra mặc định (default gateway) để truyền đến đích.

Router sử dụng Subnet Mask như thế nào



3-11

Cách sử dụng subnet mask của router

• Subnet mask định ra những vùng quan trọng trong địa chỉ IP. Router cần biết thông tin giá trị của subnet mask để xác định cách đưa dữ liệu đến đích. Chủ đề này mô tả cách router sử dụng subnet mask

• Tất cả các router đều có bảng định tuyến của mình. Tùy vào vị trí của router trong cấu trúc phân cấp của địa chỉ mạng, bảng định tuyến này có thể nhỏ, đơn giản hoặc rất lớn và phức tạp. Router sẽ quảng bá bảng định tuyến với những phần về thông tin mạng mà router biết để có thể so sánh với địa chỉ đích của dữ liệu cần được chuyển đi. Nếu địa chỉ mạng không được gắn trực tiếp và router, router sẽ lưu địa chỉ của router chặn kẽ mà qua đó dữ liệu sẽ được chuyển đi. Để router không phải lưu tất cả những network đích trong bảng định tuyến, router có thể sử dụng tuyến mạc định để những dữ liệu đi đến một đích mà không khớp với những dòng tuyến trong bảng định tuyến thì sẽ được dẫn theo tuyến này.

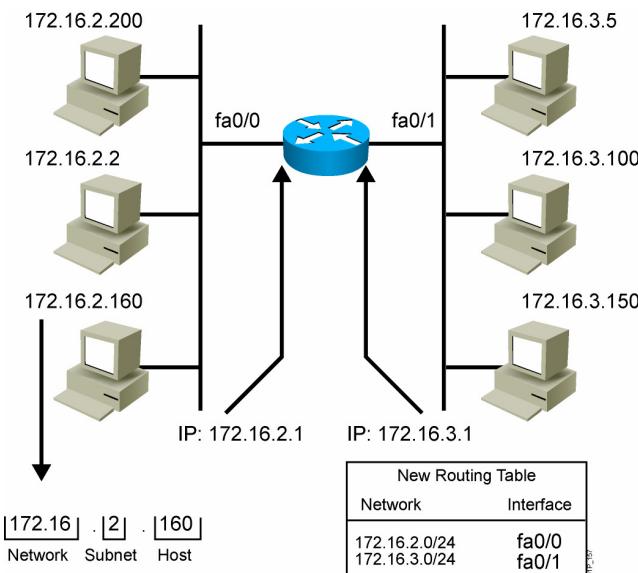
• Tiến trình định tuyến với subnet mask

Bước 1: Host A xác định địa chỉ mạng đích này cần phải được gởi ra default gateway

Bước 2: Router A đã có tuyến đến mạng 10.3.1.0 và sẽ dẫn gói dữ liệu này đến router B

Bước 3: Bởi vì mạng 10.3.1.0 được gắn trực tiếp vào cổng f0/2 của router B, do vậy router B sẽ sử dụng ARP để tìm MAC của host B và gởi dữ liệu đến host B.

Áp dụng Subnet Mask



3-12

Khi cấu hình router, mỗi cổng router sẽ được gắn về các network hay các subnet khác nhau. Những địa chỉ hợp lệ cho các host trong network hay subnet đó sẽ được gán cho các cổng của router trong network tương ứng. Trong ví dụ này, router có 2 cổng Ethernet. Cổng gắn vào network 172.16.2.0 được gán địa chỉ 172.16.2.1 và cổng khác gắn vào mạng 172.16.3.0 có địa chỉ là 172.16.3.1. Tất cả các host gắn vào cần phải có địa chỉ thuộc về dãy địa chỉ của subnet đó. Những host với địa chỉ nằm ngoài dãy sẽ không thể đến được.

Giá trị các Octet của Subnet Mask

128	64	32	16	8	4	2	1	
1	0	0	0	0	0	0	0	= 128
1	1	0	0	0	0	0	0	= 192
1	1	1	0	0	0	0	0	= 224
1	1	1	1	0	0	0	0	= 240
1	1	1	1	1	0	0	0	= 248
1	1	1	1	1	1	0	0	= 252
1	1	1	1	1	1	1	0	= 254
1	1	1	1	1	1	1	1	= 255

Subnet masks, like IP addresses, are represented in the dotted decimal format like 255.255.255.0

3-13

Cơ chế vận hành của subnet mask

- Chúng ta đã biết lý do tồn tại của subnet mask và cách mà router và các hệ thống đầu cuối sử dụng giá trị subnet mask này.
- Chủ đề này mô tả làm thế nào subnet mask được tạo ra và các hoạt động của nó.
- Mặc dù subnet mask sử dụng cùng định dạng như địa chỉ IP, nhưng bản thân nó không phải là địa chỉ IP. Mỗi subnet mask dài 32 bit và được chia làm 4 octet và thường được biểu diễn qua các cụm số thập phân phân cách nhau bằng các dấu chấm. Trong biểu diễn nhị phân, subnet mask sẽ được biểu diễn bằng các bit 1 trong phần network và phần subnet, các bit 0 cho phần host.

Giá trị Octet của subnet mask

- Chỉ có 8 giá trị subnet mask hợp lệ cho mỗi octet. Phần subnet luôn luôn đi liền sau phần địa chỉ mạng. Do đó, những bit được mượn phải là n bit đầu tiên, bắt đầu từ bit có trọng số cao nhất (MSB) của vùng host mặc định, trong đó n là kích cỡ mong muốn của vùng subnet (như hình trên). Subnet mask là công cụ được sử dụng bởi router để xác định bit nào là bit để định tuyến (network và subnet) và bit nào là bit làm host.

- Nếu tất cả 8 bit trong các octet đều là 1, octet sẽ có giá trị thập phân tương ứng lúc này là 255. Do vậy đó là lý do tại sao 255 là giá trị thập phân cho subnet mask mặc định. Ở lớp A, giá trị subnet mask mặc định là 255.0.0.0 hay 11111111.00000000.00000000.00000000. Nếu 3 bit cao nhất trên octet có thứ tự cao nhất kế tiếp được mượn, thì nó sẽ tạo thành 224 hay giá trị subnet mask lúc này là 255.224.0.0 (11111111.11100000.00000000.00000000)

Subnet Masks mặc định

Example Class A address (decimal):	10.0.0.0
Example Class A address (binary):	00001010.00000000.00000000.00000000
Default Class A mask (binary):	11111111.00000000.00000000.00000000
Default Class A mask (decimal):	255.0.0.0
Default classful prefix length:	/8

Example Class B address (decimal):	172.16.0.0
Example Class B address (binary):	10010001.10101000.00000000.00000000
Default Class B mask (binary):	11111111.11111111.00000000.00000000
Default Class B mask (decimal):	255.255.0.0
Default classful prefix length:	/16

Example Class C address (decimal):	192.168.42.0
Example Class C address (binary):	11000000.10101000.00101010.00000000
Default Class C mask (binary):	11111111.11111111.11111111.00000000
Default Class C mask (decimal):	255.255.255.0
Default classful prefix length:	/24

3-15

- Với quá trình phân định địa chỉ IP, subnet mask có vai trò xác định phần thông tin địa chỉ cần thiết để gởi dữ liệu đến đích. Subnet mask xác định bit nào trong địa chỉ IP là phần network và subnet.
- Hình trên thể hiện giá trị subnet mask mặc định của lớp A, B và C.

Tiến trình triển khai Subnet Mask

1. Determine the IP address assigned by the registry authority.
2. Based on the organizational and administrative structure, determine the number of subnets required.
3. Based on the address class and required number of subnets, determine the number of bits you need to borrow from the host ID.
4. Determine the binary and decimal value of the subnet mask.
5. Apply the subnet mask to the network IP address to determine the subnet and host addresses.
6. Assign subnet addresses to specific interfaces.

3-16

Áp dụng sự vận hành của subnet mask

- Hầu hết các quản trị mạng đều làm việc trên hệ thống mạng có sẵn và đã hoàn chỉnh với các giá trị subnet và subnet mask đã được đặt sẵn. Người quản trị mạng cần có khả năng xác định trong hệ thống mạng có sẵn đó phần nào của địa chỉ là phần network, phần nào là subnet. Áp dụng sự vận hành của subnet mask vào hệ thống mạng ta sẽ có được những thông tin này. Chủ đề này mô tả làm cách nào để vận dụng những nguyên tắc hoạt động của subnet mask vào hệ thống mạng.
- Tiến trình mô tả trong hình giải thích các để lựa chọn số lượng subnet cần cho một mạng cụ thể nào đó và sau đó vận dụng vào quá trình triển khai các subnet.

Tiến trình thực thi các subnet

Bước 1: Xác định địa chỉ IP trong hệ thống mạng đã được phân định. Giả sử ta đã được phân định một địa chỉ lớp B là 172.16.0.0

Bước 2: Dựa trên cấu trúc tổ chức và nhu cầu quản trị, xác định số lượng subnet cần thiết cho hệ thống mạng. Chú ý lường trước sự thay đổi của hệ thống mạng trong tương lai. Giải sử bạn quản lý một hệ thống mạng năm tại 25 quốc gia khác nhau. Mỗi quốc gia trung bình có 4 vị trí, do vậy bạn sẽ cần khoảng 100 subnet.

Bước 3: Dựa trên lớp địa chỉ và số lượng subnet đã được lựa chọn, xác định số bit cần mượn từ phân host. Để tạo ra 100 subnet, bạn cần mượn 7 bit ($2^7 - 2 = 126$).

Bước 4: Xác định giá trị nhị phân và thập phân của subnet mask mới được lựa chọn. Với địa chỉ lớp B có 16 bit trong phần network, khi mượn thêm 7 bit cho vùng subnet, giá trị subnet mask lúc này sẽ là /23 có định dạng nhị phân là 11111111.11111111.11111110.00000000 và định dạng thập phân là 255.255.254.0

Bước 5: Áp dụng subnet mask cho phần mạng địa chỉ IP để xác định phần subnet và phần host. Bạn cũng phải định ra địa chỉ network và địa chỉ broadcast cho từng subnet.

Bước 6: Gán các địa chỉ subnet vào các subnet cụ thể trên hệ thống mạng.

8 bước đơn giản để xác định địa chỉ subnet

IP Address: 192.168.221.37 Subnet Mask /29

Step	Description	Example
1.	Write the octet that is being split in binary.	Fourth octet: 00100101
2.	Write the mask or classful prefix length in binary.	Assigned mask: 255.255.255.248 (/29) Fourth octet: 11111000
3.	Draw a line to delineate the significant bits in the assigned IP address. Cross out the mask so you can view the significant bits in the IP address.	Split octet (binary): 00100101 Split mask (binary): 11111000

30
30

3-18

Xác định kế hoạch phân địa chỉ

- Khi làm việc với môi trường mạng classful sử dụng chiều dài subnet mask cố định, bạn có thể xác định kế hoạch phân địa chỉ cho toàn bộ hệ thống mạng dựa trên một địa chỉ IP đơn và subnet mask tương ứng của nó.
- Hình trên thể hiện 3 bước đầu tiên của 8 bước được sử dụng để xác định subnet của một địa chỉ IP. Trong ví dụ này, địa chỉ IP và subnet mask được cho như sau:

Địa chỉ network: 192.168.221.37

Subnet mask: 255.255.255.248

8 bước đơn giản để xác định địa chỉ subnet (tt.)

Step	Description	Example
4.	Copy the significant bits four times.	00100 000 (network address) 00100 001 (first address in subnet) 00100 110 (last address in subnet) 00100 111 (broadcast address)?
5.	In the first line, define the network address by placing all zeros in the significant bits.	
6.	In the last line, define the broadcast address by placing all ones in the significant bits.	
7.	In the middle lines, define the first and last host number.	Completed Subnet Addresses Network address: 192.168.221.32 Subnet mask: 255.255.255.248 First subnet: 192.168.221.32 First host address: 192.168.221.33 Last host address: 192.168.221.38 Broadcast address: 192.168.221.39 Next subnet: 192.168.221.40
8.	Increment the subnet bits by one.	00101 000 (next subnet)

3-19

Hình trên thể hiện 5 bước cuối trong 8 bước được sử dụng để xác định subnet của một địa chỉ IP cho sẵn. Sau khi chuyển đổi địa chỉ từ nhị phân sang thập phân, địa chỉ của subnet được cho như sau

Địa chỉ subnet đầu tiên: 192.168.221.32

Địa chỉ IP đầu tiên: 192.168.221.33

Địa chỉ IP cuối cùng: 192.168.221.38

Địa chỉ broadcast: 192.168.221.39

Địa chỉ subnet kế tiếp: 192.168.221.40

Chú ý dãy địa chỉ của khối địa chỉ từ 192.168.221.32 đến 192.168.221.39 bao gồm cả địa chỉ subnet và địa chỉ broadcast trực tiếp (directed-broadcast).

Ví dụ: Áp dụng Subnet Mask cho địa chỉ lớp C

IP Address 192.168.5.139 Subnet Mask 255.255.255.224

IP Address	192	168	5	139	
IP Address	11000000	10101000	00000101	10001011	
Subnet Mask	11111111	11111111	11111111	11100000	/27
Subnetwork	11000000	10101000	00000101	10000000	
Subnetwork	192	168	5	128	
First Host	192	168	5	10000001=129	
Last Host	192	168	5	10011110=158	
Directed Broadcast	192	168	5	10011111=159	
Next Subnet	192	168	5	10100000=160	

3-20

Ví dụ về địa chỉ lớp C

Cho trước một địa chỉ 192.168.5.139 và subnet mask tương ứng là 255.255.255.224 (11111111.11111111.11111111.11100000 hoặc /27)

Các bước để xác định địa chỉ subnet lớp C

Bước 1: Viết ra các octet được tách biệt ở dạng nhị phân: 10001011

Bước 2: Viết ra giá trị subnet mask hay chiều dài của subnet mask ở dạng nhị phân: 11100000

Bước 3: Vẽ một vạch phân định ra những bit quan trọng (bit phần network) trong địa chỉ IP được gán sẵn, gạch đi phần subnet mask sẽ thấy được những bit quan trọng trong địa chỉ IP đó.

100 | 01011

111 | 00000

Bước 4: Sao chép các bit quan trọng này ra 4 lần

100 00000 (địa chỉ mạng đầu tiên)

100 00001 (địa chỉ host đầu tiên)

100 11110 (địa chỉ mạng cuối cùng)

100 11111 (địa chỉ broadcast)

Bước 5: Bản sao chép đầu tiên xác định địa chỉ mạng bằng cách đặt tất cả bit 0 trong phần host: 100 00000

Bước 6: Bản sao chép cuối cùng xác định địa chỉ broadcast bằng cách đặt tất cả bit 1 trong phần host: 100 1111

Bước 7: Những bản sao chép giữa sẽ xác định địa chỉ IP đầu tiên và cuối cùng cho subnet này

Bước 8: Tăng bit phần subnet lên một đơn vị sẽ xác định địa chỉ subnet kế tiếp: 101 00000. Thực hiện lại từ bước 4 đến bước 8 cho tất cả các subnet.

Ví dụ: Áp dụng Subnet Mask cho địa chỉ lớp B

IP Address 172.16.139.46 Subnet Mask /20

IP Address	172	16	139	46	
IP Address	10101100	00010000	1000 1011	00101110	
Subnet Mask	11111111	11111111	1111 0000	00000000	/20
Subnetwork	10101100	00010000	10000000	00000000	
Subnetwork	172	16	128	0	
First Host	172	16	10000000	00000001=128.1	
Last Host	172	16	10001111	11111110=143.254	
Directed Broadcast	172	16	10001111	11111111=143.255	
Next Subnet	172	16	10010000	00000000=144.0	

3-22

Ví dụ về địa chỉ lớp B

Cho trước một địa chỉ 172.16.139.46 và subnet mask tương ứng là 255.255.240.0 (11111111.11111111.11110000.00000000 hoặc /20)

Các bước để xác định địa chỉ subnet lớp B

Bước 1: Viết ra các octet được tách biệt ở dạng nhị phân: 10001011

Bước 2: Viết ra giá trị subnet mask hay chiều dài của subnet mask ở dạng nhị phân: 11110000

Bước 3: Vẽ một vạch phân định ra những bit quan trọng (bit phần network) trong địa chỉ IP được gán sẵn, gạch đi phần subnet mask sẽ thấy được những bit quan trọng trong địa chỉ IP đó.

1000 | 1011

1111 | 0000

Bước 4: Sao chép các bit quan trọng này ra 4 lần

1000 0000 (địa chỉ mạng đầu tiên)

1000 0001 (địa chỉ host đầu tiên)

1000 1110 (địa chỉ mạng cuối cùng)

1000 1111 (địa chỉ broadcast)

Bước 5: Bản sao chép đầu tiên xác định địa chỉ mạng bằng cách đặt tất cả bit 0 trong phần host: 1000 0000

Bước 6: Bản sao chép cuối cùng xác định địa chỉ broadcast bằng cách đặt tất cả bit 1 trong phần host: 1000 1111

Bước 7: Những bản sao chép giữa sẽ xác định địa chỉ IP đầu tiên và cuối cùng cho subnet này.

Bước 8: Tăng bit phần subnet lên một đơn vị sẽ xác định địa chỉ subnet kế tiếp: 1001 0000. Thực hiện lại từ bước 4 đến bước 8 cho tất cả các subnet.

Ví dụ: Áp dụng Subnet Mask cho địa chỉ lớp A

IP Address 10.172.16.211 Subnet Mask /18

IP Address	10	172	16	211	
IP Address	00001010	10101100	00010000	11010011	
Subnet Mask	11111111	11111111	11000000	00000000	/18
Subnetwork	00001010	10101100	00000000	00000000	
Subnetwork	10	172	0	0	
First Host	10	172	00000000	00000001=0.1	
Last Host	10	172	00111111	11111110=63.254	
Directed Broadcast	10	172	00111111	11111111=63.255	
Next Subnet	10	172	01000000	00000000=64.0	

3-24

Ví dụ về địa chỉ lớp A

Cho trước một địa chỉ 10.172.16.211 và subnet mask tương ứng là 255.255.192.0 (11111111.11111111.11000000.00000000 hoặc /18)

Các bước để xác định địa chỉ subnet lớp A

Bước 1: Viết ra các octet được tách biệt ở dạng nhị phân: 00010000

Bước 2: Viết ra giá trị subnet mask hay chiều dài của subnet mask ở dạng nhị phân: 11000000

Bước 3: Vẽ một vạch phân định ra những bit quan trọng (bit phần network) trong địa chỉ IP được gán sẵn, gạch đi phần subnet mask sẽ thấy được những bit quan trọng trong địa chỉ IP đó.

00 | 010000

11 | 000000

Bước 4: Sao chép các bit quan trọng này ra 4 lần

00 000000 (địa chỉ mạng đầu tiên)

00 000001 (địa chỉ host đầu tiên)

00 111110 (địa chỉ mạng cuối cùng)

00 111111 (địa chỉ broadcast)

Bước 5: Bản sao chép đầu tiên xác định địa chỉ mạng bằng cách đặt tất cả bit 0 trong phần host: 1000 0000

Bước 6: Bản sao chép cuối cùng xác định địa chỉ broadcast bằng cách đặt tất cả bit 1 trong phần host: 1000 1111

Bước 7: Nhũng bản sao chép giữa sẽ xác định địa chỉ IP đầu tiên và cuối cùng cho subnet này.

Bước 8: Tăng bit phần subnet lên một đơn vị sẽ xác định địa chỉ subnet kế tiếp: 01 000000. Thực hiện lại từ bước 4 đến bước 8 cho tất cả các subnet.

Tóm tắt

- Một mạng lớn thường được chia thành các mạng nhỏ hơn gọi là các subnet. Subnet cải thiện quá trình vận hành và điều khiển mạng.
- Địa chỉ subnet mở rộng phần mạng bằng cách mượn những bit từ phần host.
- Xác định số subnet là host tối ưu phục thuộc vào mạng và số lượng host yêu cầu.
- Số subnet được tính theo công thức 2^s , s là số bit làm subnet.

Tóm tắt (tt.)

- Subnet Mask là công cụ router sử dụng để xác định bit nào sẽ được định tuyến (phần mạng) và bit nào làm phần host.
- Thiết bị đầu cuối sử dụng Subnet Mask để so sánh mạng của mình và của địa chỉ đích.
- Router sử dụng Subnet Mask để định ra phần mạng của địa chỉ IP trên băng định tuyến.

Tóm tắt (tt.)

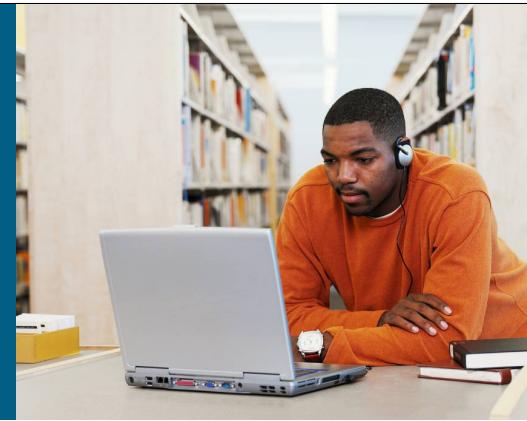
Các bước sau dùng để xác định subnet và host dùng Subnet Mask:

1. Viết octet sẽ bị tách ra ở dạng nhị phân.
2. Viết Subnet Mask dạng nhị phân và vẽ một đường chỉ ra những bit quan trọng.
3. Gạch đi phần Subnet Mask để nhìn thấy những bit quan trọng.
4. Sao chép những bit subnet 4 lần.
5. Định ra địa chỉ mạng bằng cách cho các bit phần host bằng 0.
6. Định ra địa chỉ broadcast bằng cách cho các bit phần host bằng 1.
7. Định ra địa chỉ đầu tiên và cuối cùng.
8. Tăng các bit subnet lên 1.



3-29

Bài 4: Khởi động một Router



Kết nối LAN

4-1

Tổng quan

Khi lần đầu bật lên, Cisco router sẽ trải qua bước khởi động và lúc này sẽ chưa có bất kỳ một cấu hình nào tồn tại. Sau khi quá trình khởi động hoàn tất, ta có thể đưa vào cấu hình ban đầu. Nhận thức đúng về tiến trình khởi động của router là bước đầu tiên trong việc cài đặt thiết bị. Router phải khởi động thành công và có sẵn cấu hình đúng để vận hành trên mạng. Bài học sẽ mô tả quá trình khởi động của một router và cách kiểm tra quá trình vận hành ban đầu.

Mục tiêu

Cung cấp khả năng để khởi động một Cisco router với hệ điều hành IOS và sử dụng giao diện dòng lệnh (CLI) để cấu hình và giám sát router qua các nhiệm vụ sau:

- Khởi động Cisco router
- Khởi động tiến trình thiết lập ban đầu cho Cisco router
- Đăng nhập vào Cisco router
- Hiển thị thông tin phần mềm và phần cứng của Cisco router

Khởi động ban đầu của Cisco Router

- Một chuỗi chuẩn những tiến trình khởi động sẽ kích hoạt hệ điều hành Cisco IOS.
- Router sẽ trở về lại trạng thái khởi động trong một số trường hợp cần thiết.

1. Before you start the router, verify the power, cabling, and console connection.
2. Push the power switch to “on.”
3. Observe the boot sequence:
 - Cisco IOS Software output text appears on the console.



301P_405

4-2

• Quá trình khởi động của Cisco router yêu cầu việc kiểm tra về mặt cài đặt vật lý, bật nguồn router và quan sát những thông tin xuất ra từ hệ điều hành Cisco IOS từ console. Chủ đề này mô tả quá trình khởi động ban đầu của Cisco router.

• Để có thể bắt đầu vận hành, router phải hoàn tất các bước sau:

- Chạy POST (power-on self-test) để kiểm tra các phần cứng
- Tìm và tải hệ điều hành Cisco IOS
- Tìm và sử dụng các cấu hình về một số tính chất riêng của router, chức năng các giao thức và địa chỉ các cổng trên router.

• Khi được bật lên, Cisco router sẽ thực hiện tiến trình POST. Trong suốt quá trình này, router thực hiện quá trình chuẩn đoán để kiểm tra sự vận hành cơ bản của bộ xử lý trung tâm (CPU), bộ nhớ, mạch điện, các cổng.

• Sau khi kiểm tra các phần cứng, router tiếp tục với việc khởi động phần mềm, trong quá trình này, router sẽ tìm và tải tập tin ảnh hệ điều hành và sau đó là tìm và tải tập tin cấu hình (nếu tồn tại).

• Bảng sau sẽ liệt kê các bước yêu cầu cho quá trình khởi động ban đầu

Quá trình khởi động Cisco router

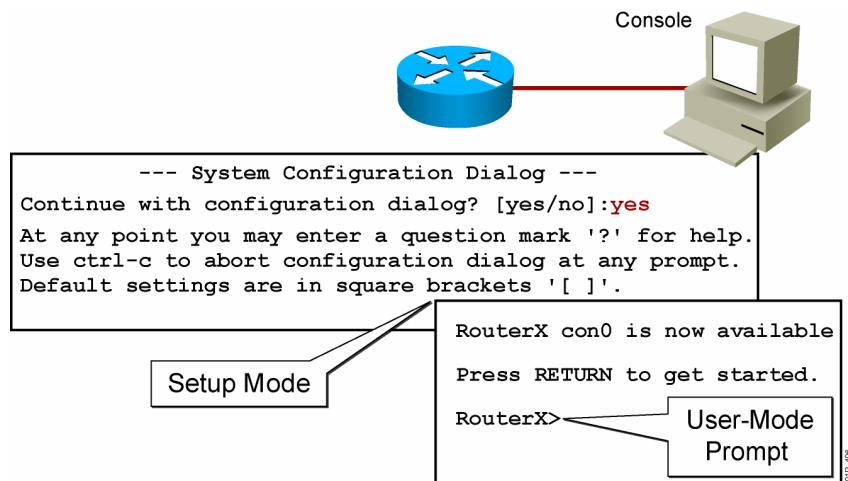
Bước 1: Trước khi khởi động một router, kiểm tra các vấn đề sau:

- Tất cả cáp kết nối đã được bảo vệ
- Thiết bị đầu cuối đã được gắn vào cổng console
- Chương trình ứng dụng đầu cuối, như HyperTerminal, đã được kích hoạt

Bước 2: Bật công tắc sang vị trí “on”

Bước 3: Quan sát thứ tự khởi động và những thông tin xuất ra trên console

Output từ quá trình khởi động



Unconfigured vs. Configured Router

4-4

- Khi được khởi động, router sẽ tìm tập tin cấu hình thiết bị. Nếu không tập tin nào được tìm thấy, router sẽ thực thi một tiến trình giúp hoàn tất cấu hình qua các câu hỏi hướng dẫn, quá trình này gọi là “setup”. Chủ đề này mô tả những câu lệnh ban đầu và giải thích cách để hoàn thành quá trình thiết lập qua kiểu hội thoại
- Sau khi router hoàn tất quá trình POST và tải tập tin ảnh hệ điều hành, router sẽ tìm kiếm tập tin cấu hình trong NVRAM. NVRAM của router là một loại bộ nhớ sẽ vẫn lưu cấu hình thậm chí khi mất nguồn. Nếu như router có tập tin cấu hình trong NVRAM, dấu nhắc user-mode sẽ xuất hiện. Hình trên hiển thị dấu nhắc **RouterX>**
- Khi khởi động một router mới, sẽ không có tập tin cấu hình trong NVRAM. Trong trường hợp này, hệ điều hành sẽ thực thi quá trình cấu hình qua các câu hỏi hướng dẫn, gọi là tiến trình hội thoại hay còn gọi là setup-mode.
- Setup-mode sẽ không được dùng khi muốn cấu hình những giao thức phức tạp trong router. Chỉ sử dụng setup-mode để tạo nên một cấu hình tối thiểu ban đầu.

Setup: Khởi tạo quá trình cấu hình hội thoại

```
Router#setup
```

```
--- System Configuration Dialog ---
```

```
Continue with 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
```

020_296

4-5

- Mục tiêu chính của setup-mode là nhanh chóng đưa lại một cấu hình tối thiểu ban đầu cho các router không có tập tin cấu hình. Ta có thể vào setup-mode khi router khởi động mà không có cấu hình hoặc có thể vào bất cứ khi nào sau khi router đã vận hành bằng cách nhập vào câu lệnh **setup** ở mode đặc quyền (privileged mode).
- Cho hầu hết các dấu nhắc trong setup-mode, câu trả lời mặc định sẽ được đặt nằm trong dấu []. Nhấn **Enter** sẽ cho phép sử dụng giá trị mặc định này.
- Khi được nhắc với “Would you like to enter basic management setup?” bạn có thể ngừng tiến trình cấu hình hội thoại này bằng cách nhấn **no** tại dấu nhắc. Để bắt đầu tiến trình cấu hình nhấn **yes**. Thông thường khi nhấn **no** tại dấu nhắc “basic management setup” ta sẽ vào extended setup và tại đây ta có thể cấu hình một số tham số cụ thể hơn
- Nhấn **Ctrl-C** để kết thúc tiến trình cấu hình setup-mode để trở ra lại EXEC mode tại bất kỳ thời điểm nào.

Thiết lập tóm tắt các interface

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

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	NO	unset	up	up
FastEthernet0/1	unassigned	NO	unset	up	up
Serial0/0/0	unassigned	NO	unset	up	up
Serial0/0/1	unassigned	NO	unset	down	down

Các Interfaces tìm thấy trong quá
trình khởi động

4-6

- Nếu nhấn yes tại dấu nhắc “Would you like to enter basic management setup?” bạn sẽ được nhắc “First, would you like to see the current interface summary?”. Nhấn yes để xem các cổng trên router. Hình trên thể hiện trạng thái hiện tại của mỗi cổng trên router. Thông tin bao gồm địa chỉ IP và cấu hình hiện tại.

Thiết lập các thông số toàn cục

```
Configuring global parameters:
```

```
Enter host name [Router]:RouterX
```

```
The enable secret is a password used to protect access to privileged  
EC and configuration modes. This password, after entered, becomes  
encrypted in the configuration.
```

```
Enter enable secret: Cisco1
```

```
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: SanFran3
```

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

```
Enter virtual terminal password: Sanj0se
```

```
Configure SNMP Network Management? [no]:
```

4-7

- Tiếp tục với setup-mode, bạn sẽ được hỏi về các tham số toàn cục. Nhập vào các tham số toàn cục tại dấu nháy, sử dụng các giá trị cấu hình đã được xác định sẵn cho router. Thông số toàn cục đầu tiên là tên cho router (hostname). Host name này sẽ được đặt trước dấu nháy của hệ điều hành trong tất cả các mode cấu hình. Tên mặc định của router được đặt nằm trong ngoặc vuông là [Router].
- Sử dụng các thông số toàn cục được thể hiện để thiết lập các mật mã khác nhau sử dụng cho router.

Thiết lập các giao thức ban đầu

```
Configure IP? [yes]:  
    Configure RIP routing? [yes]: no  
Configure CLNS? [no]:  
    Configure bridging? [no]:
```

Tùy vào hệ điều hành mà thông tin trên có thể hiện ra.

4-8

Tiếp tục qua các bước trong setup-mode, bạn sẽ được hỏi thêm các thông số toàn cục. Ví dụ trên là dấu nhắc cho phần giao thức định tuyến. Nếu nhấn yes để chỉ ra rằng bạn muốn cấu hình giao thức định tuyến, một số dấu nhắc cấp dưới sẽ xuất hiện để cấu hình cho giao thức đó.

Thiết lập các thông số cho interface

```
Configuring interface parameters:  
Do you want to configure FastEthernet0/0 interface? [yes]:  
    Use the 100 Base-TX (RJ-45) connector? [yes]:  
    Operate in full-duplex mode? [no]:  
    Configure IP on this interface? [yes]:  
        IP address for this interface: 10.2.2.11  
        Subnet mask for this interface [255.0.0.0] : 255.255.255.0  
        Class A network is 10.0.0.0, 24 subnet bits; mask is /24  
  
Do you want to configure FastEthernet0/1 interface? [yes]: no  
  
Do you want to configure Serial0/0/0 interface? [yes]: no  
  
Do you want to configure Serial0/0/1 interface? [yes]: no
```

4-9

Tiếp tục để được hỏi về các thông số cho các cổng đã được cài đặt. Sử dụng các giá trị cấu hình đã định trước cho các cổng để nhập vào.

Cisco AutoSecure

```
Would you like to go through AutoSecure configuration? [yes]: no
AutoSecure dialog can be started later using "auto secure" CLI
```

Tùy thuộc vào hệ điều hành mà phần này có thể xuất hiện.

4-10

Cisco AutoSecure là một đặc tính bảo mật dùng giao diện dòng lệnh (CLI) của hệ điều hành Cisco IOS. Bạn có thể triển khai một trong hai mode sau, tùy vào nhu cầu:

Mode tương tác (Interactive mode): nhắc người dùng với các tính năng tùy chọn để kích hoạt hoặc ngưng kích hoạt các dịch vụ và các đặc tính bảo mật.

Mode không tương tác (Noninteractive mode): tự động thực hiện các câu lệnh AutoSecure với cấu hình bảo mật mặc định mà Cisco khuyến nghị.

Chú ý: Cisco AutoSecure cố gắng đảm bảo khả năng bảo mật tối đa bằng cách ngưng kích hoạt các dịch vụ được sử dụng phổ biến bởi hacker để xâm nhập vào router. Tuy nhiên một số dịch vụ này lại cần thiết để một số chức năng khác vận hành. Do vậy, không nên sử dụng chức năng này cho đến khi hiểu toàn bộ sự vận hành của nó và các nhu cầu trên hệ thống mạng.

Cisco AutoSecure thực hiện những tính năng sau:

Ngưng kích hoạt các dịch vụ toàn cục sau:

- Finger
- Packet assembler/disassembler (PAD)
- Small servers
- BOOTP servers
- HTTP service

- Identification service
- Cisco Discovery Protocol
- Network Time Protocol (NTP)
- Source routing

Kích hoạt cho phép sử dụng các dịch vụ toàn cục:

- Password encryption service
- Tuning of scheduler interval and allocation
- TCP synwait time
- TCP keepalive messages
- Security policy database (SPD) configuration
- Internet Control Message Protocol (ICMP) unreachable messages

Ngưng kích hoạt các dịch vụ sau trên các cổng:

- ICMP
- Proxy Address Resolution Protocol (ARP)
- Directed broadcast
- Maintenance Operation Protocol (MOP) service
- ICMP unreachables
- ICMP mask reply messages

Cung cấp chức năng ghi log, bao gồm các dịch vụ sau:

- Enables sequence numbers and timestamp
- Provides a console log
- Sets log buffered size
- Provides an interactive dialogue to configure the logging server IP address

Bảo vệ truy xuất vào router, bao gồm những chức năng sau:

- Checking for a banner and providing the ability to add text for automatic configuration
- Login and password
- Transport input and output
- exec-timeout** commands
- Local authentication, authorization, and accounting (AAA)
- Secure Shell (SSH) timeouts and **ssh authentication-retries** commands
- Enabling only SSH and Secure Copy Protocol (SCP) for access and file transfers to and from the router
- Disabling Simple Network Management Protocol (SNMP) if not being used

Bảo vệ pha chuyển dữ liệu (forwarding plane), bao gồm những chức năng sau:

- Enabling Cisco Express Forwarding or distributed Cisco Express Forwarding on the router, when available
- Antispoofing
- Blocking all Internet Assigned Numbers Authority (IANA) reserved IP address blocks
- Blocking private address blocks, if customer desires
- Installing a default route to Null0, if a default route is not being used
- Configuring a TCP intercept for a connection timeout, if the TCP intercept feature is available and the user desires
- Starting an interactive configuration for Context-Based Access Control (CBAC) on interfaces facing the Internet, when using a Cisco IOS Firewall image
- Enabling NetFlow on software forwarding platforms

Xem lại và sử dụng đoạn mã thiết lập

```
The following configuration command script was created:  
hostname RouterX  
enable secret 5 $1$aNMG$kV3mxjl1WDRGXmfwjEBNAf1  
enable password cisco  
line vty 0 4  
password sanjose  
no snmp-server  
!  
ip routing  
no c1ns routing  
no bridge 1  
  
interface FastEthernet0/0  
media-type 100BaseX  
half-duplex  
ip address 10.2.2.11 255.255.255.0  
no mop enabled  
!  
interface FastEthernet0/1  
shutdown  
no ip address  
!  
interface Serial0/0/0  
shutdown  
no ip address  
!  
interface Serial0/0/1  
shutdown  
no ip address  
dialer-list 1 protocol ip permit  
!  
end  
[0] Go to the IOS command prompt without saving this config.  
[1] Return back to the setup without saving this config.  
[2] Save this configuration to nvram and exit.  
Enter your selection [2]: 2
```

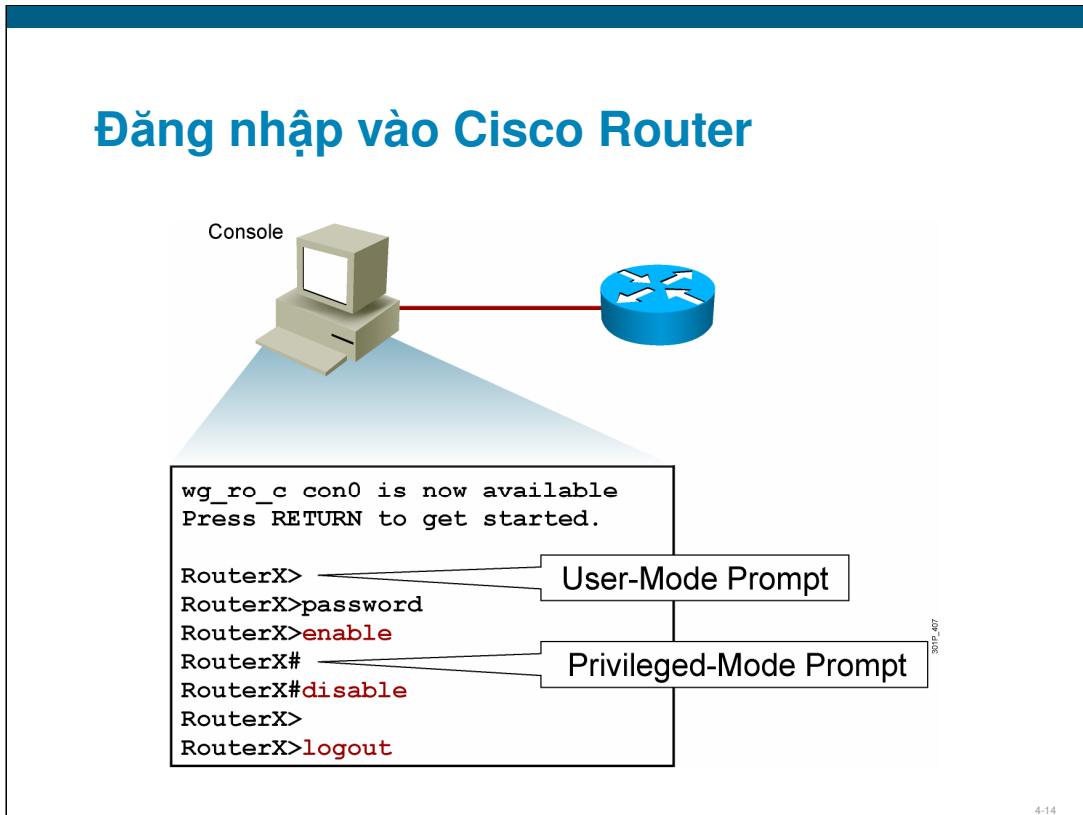
4-13

Khi đã hoàn thành tất cả các cấu hình trên router, câu lệnh **setup** sẽ hiển thị những câu lệnh đã được tạo ra. Câu lệnh setup sẽ mang lại 3 tùy chọn

- [0]: Thoát ra EXEC mode mà không lưu cấu hình đã tạo ra
- [1]: Quay lại lúc khởi đầu của setup mode mà không lưu lại cấu hình
- [2]: Chấp nhận cấu hình, lưu vào NVRAM và thoát ra EXEC mode

Nếu chọn [2], cấu hình sẽ được thực thi và lưu vào NVRAM, hệ thống lúc này đã sẵn sàng để sử dụng. Để chỉnh sửa cấu hình, ta phải cấu hình lại bằng tay.Thêm vào đó, câu lệnh **setup** không hỗ trợ nhiều tính năng cao cấp để cấu hình cho router hoạt động với những tính năng này.

Đăng nhập vào Cisco Router



Khi cấu hình router với giao diện dòng lệnh từ thiết bị đầu cuối qua cổng console, hệ điều hành Cisco IOS cung cấp một interpreter gọi là EXEC. EXEC sẽ diễn dịch các câu lệnh nhập vào và thực thi sự vận hành tương ứng. Chủ đề này mô tả cách truy xuất vào Cisco router để bắt đầu khởi tạo một cấu hình ban đầu.

Sau khi đã cấu hình Cisco router từ setup-mode, ta có thể cấu hình lại hoặc thêm vào cấu hình từ giao diện người dùng chạy trên cổng console hoặc cổng AUX trên router. Ta cũng có thể cấu hình Cisco router sử dụng các ứng dụng truy xuất từ xa như SSH.

EXEC sẽ phiên dịch các câu lệnh được đưa vào và thực thi sự vận hành tương ứng. Ta phải đăng nhập vào router trước khi thực thi những câu lệnh EXEC

Vì lý do bảo mật, EXEC được chia thành 2 cấp độ truy nhập để thực thi các câu lệnh

User mode: Bao gồm các tác vụ để kiểm tra trạng thái router

Privileged mode: Bao gồm các tác vụ dùng để thay đổi cấu hình router

Khi lần đầu đăng nhập vào router, dấu nhắc user mode sẽ được hiển thị. Những câu lệnh EXEC có sẵn trong user mode là những câu lệnh cũng sẽ được bao gồm trong privileged mode, những câu lệnh này chỉ thể hiện những thông tin mà không thể làm thay đổi cấu hình router.

Để truy xuất vào bộ lệnh hoàn chỉnh, ta phải kích hoạt privileged mode bằng câu lệnh **enable** và sẽ được hỏi password để đăng nhập nếu được cấu hình.

Chú ý: enable password để vào privileged mode được hiển thị dạng clear text khi được xem với câu lệnh **show run**. Password dạng secret thì sẽ được mã hóa do vậy sẽ không hiển thị ở dạng clear text. Nếu cả hai dạng password là enable và secret cùng được cấu hình, secret password sẽ được ưu tiên trên enable password

Dấu nhắc sẽ là dấu # (#) khi đang đứng trong privileged mode. Từ privileged mode ta có thể truy xuất vào global configuration mode và các mode chi tiết khác như mode interface, subinterface, line, router, route-map và các mode khác.

Sử dụng câu lệnh **disable** để quay về lại user mode từ privilege mode.

Sử dụng câu lệnh **exit** hoặc **logout** để kết thúc session hiện tại.

Các câu lệnh trong user mode

```
RouterX>?
Exec commands:
  access-enable      Create a temporary Access-List entry
  access-profile     Apply user-profile to interface
  clear              Reset functions
  connect             Open a terminal connection
  disable             Turn off privileged commands
  disconnect          Disconnect an existing network connection
  enable              Turn on privileged commands
  exit                Exit from the EXEC
  help                Description of the interactive help system
  lat                 Open a lat connection
  lock                Lock the terminal
  login               Log in as a particular user
  logout              Exit from the EXEC
-- More --
```

You can abbreviate a command to the fewest characters that make a unique character string.

4-16

Nhập vào dấu hỏi (?) tại dấu nháy user mode hay privilege mode để hiển thị danh sách các câu lệnh có sẵn trong mode đang đứng.

Chú ý: những câu lệnh có sẵn sẽ rất khác nhau tùy vào những version hệ điều hành khác nhau. Khi gặp --More-- tại phía cuối màn hình, dấu hiệu này chỉ ra rằng có nhiều trang màn hình nữa sẽ được xuất ra tùy theo những câu lệnh sau được nhập vào:

- Nhấn Spacebar để hiển thị trang kế tiếp
- Nhấn Return (hay Enter) để hiển thị dòng kế tiếp
- Nhấn phím bất kỳ để trả về dấu nháy

Các câu lệnh trong privilege mode

```
RouterX#?
Exec commands:
  access-enable      Create a temporary Access-List entry
  access-profile     Apply user-profile to interface
  access-template    Create a temporary Access-List entry
  bfe                For manual emergency modes setting
  cd                 Change current directory
  clear              Reset functions
  clock              Manage the system clock
  configure          Enter configuration mode
  connect             Open a terminal connection
  copy               Copy from one file to another
  debug              Debugging functions (see also 'undebug')
  delete              Delete a file
  dir                List files on a filesystem
  disable             Turn off privileged commands
  disconnect          Disconnect an existing network connection
  enable              Turn on privileged commands
  erase              Erase a filesystem
  exit                Exit from the EXEC
  help               Description of the interactive help system
-- More --
```

You can complete a command string by entering the unique character string, then pressing the **Tab** key.

4-17

Nhập vào câu lệnh **enable** từ user mode để truy xuất vào privilege EXEC mode. Thông thường nếu enable password đã được thiết lập, bạn cũng phải nhập vào password này để có thể vào privilege mode

Nhập vào dấu **?** tại dấu nháy của privilege mode để hiển thị danh sách các câu lệnh nằm trong mode này

Chú ý: các câu lệnh sẽ khác nhau tùy thuộc vào các version của hệ điều hành Cisco IOS.

Câu lệnh show version

```
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(12), RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 17-Nov-06 12:02 by prod_rel_team

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)

RouterX uptime is 2 days, 21 hours, 15 minutes
System returned to ROM by power-on
System image file is "flash:c2800nm-adipservicesk9-mz.124-12.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/wlc/export/crypto/tool/stqrg.html

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

Cisco 2811 (revision 53.50) with 249856K/12288K bytes of memory.
Processor board ID FTX1107A6BB
2 FastEthernet interfaces
2 Serial(sync/async) interfaces
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity enabled.
239K bytes of non-volatile configuration memory.
62720K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102

RouterX#
```

4-18

Sau khi đăng nhập vào Cisco router, trạng thái phần cứng và phần mềm có thể được kiểm tra qua các câu lệnh sau: **show version**, **show running-config**, **show startup-config**. Chủ đề này mô tả các câu lệnh trạng thái của router.

Sử dụng câu lệnh **show version** để hiển thị cấu hình phần cứng hệ thống, version phần mềm, dung lượng bộ nhớ và thanh ghi cấu hình.

Trong ví dụ trên, bộ nhớ RAM có dung lượng là 249,856 KB cho bộ nhớ chính và 12,288 KB cho bộ nhớ truy xuất I/O (chia sẻ cho tất cả các cổng của router). Bộ nhớ I/O dùng để giữ dữ liệu trong khi nó đang được định tuyến. Router có 2 cổng Fast Ethernet và 2 cổng serial. Thông tin này hữu dụng để khảng định những cổng vật lý đã được nhận ra sau quá trình khởi động router (POST). Router có 239 KB để chứa cấu hình trong NVRAM và 62,720 KB cho bộ nhớ Flash dùng để chứa tập tin ảnh hệ điều hành.

Tóm tắt

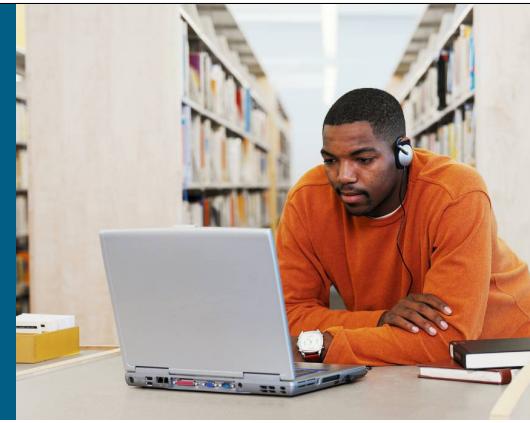
- Các bước khởi động của Cisco router tương tự như Catalyst Switch. Sau quá trình POST, router sẽ tìm và tải hệ điều hành, cuối cùng là tìm và tải cấu hình.
- Sử dụng câu lệnh **enable** để vào privilege mode từ user mode.
- Sau khi đã vào router, ta có thể kiểm tra cấu hình với các câu lệnh : **show version**, **show running-config**, và **show startup-config**

4-19



4-20

Bài 5: Cấu hình Cisco Router



Kết nối LAN

5-1

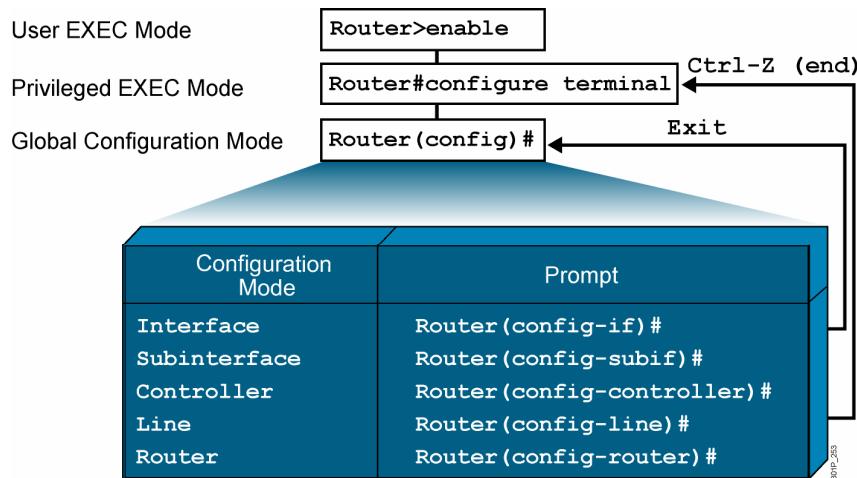
Tổng quan

Sau khi router hoàn tất quá trình khởi động có một cấu hình khởi tạo ban đầu, ta có thể bắt đầu cấu hình router hoạt động cho một hệ thống mạng cụ thể. Để làm được chuyện này, ta phải làm quen với các câu lệnh ở giao diện CLI, các mode vận hành, trước khi cấu hình các đặc tính nâng cao khác như định tuyến IP. Bài học mô tả cách thực thi một cấu hình cơ bản cho Cisco router.

Mục tiêu

- Cung cấp khả năng thực thi một cấu hình cơ bản cho Cisco router qua các nhiệm vụ sau:
 - Mô tả các mode cấu hình của router
 - Cấu hình router từ CLI
 - Cấu hình các cổng (interface) của router
 - Cấu hình địa chỉ IP cho router
 - Kiểm tra cấu hình trên router interface

Tổng quan về các mode của router



5-2

Từ privileged EXEC mode, ta có thể vào global configuration mode, nơi sẽ tiếp tục cung cấp lối vào các mode chuyên dụng khác trên router. Chủ đề mô tả các mode cấu hình cho router và cách để lưu cấu hình.

Bước đầu tiên để cấu hình router là qua setup mode. Mode này cho phép ta tạo ra một cấu hình cơ bản ban đầu. Cho những cấu hình chi tiết và phức tạp hơn, ta có thể sử dụng CLI để thực hiện cấu hình từ thiết bị đầu cuối.

Từ privileged EXEC mode, ta dùng câu lệnh **configure terminal** để vào global configuration mode. Từ global configuration mode, ta có thể tiếp tục vào các mode chuyên dụng sau:

- **Interface:** cung cấp các câu lệnh để cấu hình cho sự vận hành trên từng interface.
- **Subinterface:** cung cấp các câu lệnh để cấu hình nhiều interface ảo trên một interface vật lý
- **Controller:** cung cấp các câu lệnh để cấu hình cho controllers (như E1 và T1 controller)
- **Line:** cung cấp các câu lệnh để cấu hình cho các line, ví dụ như line console, line vty
- **Router:** cung cấp các câu lệnh cấu hình định tuyến IP

Nếu ta đưa vào câu lệnh **exit**, router sẽ thoát trở ra một cấp, cho đến khi thoát ra ngoài. Thông thường ta có thể đưa vào câu lệnh **exit** từ các mode chuyên dụng để thoát trở ra global configuration mode. Nhấn **Ctrl-Z** để hoàn toàn thoát khỏi mode cấu hình và trở ra privileged EXEC mode.

Trong mode cấu hình CLI, mỗi câu lệnh đưa vào sẽ được phân tích bởi bộ biên dịch ngay sau khi nhấn phím **Enter**.

Nếu không có lỗi nào về ngữ pháp trong câu lệnh, câu lệnh sẽ được thực thi và lưu trong running configuration và sẽ có tác động ngay lập tức đến hệ thống.

Những câu lệnh có ảnh hưởng lên toàn bộ router gọi là những câu lệnh global, câu lệnh **hostname** và **enable password** là những ví dụ của các câu lệnh global.

Những câu lệnh dùng để chỉ đến hay chỉ ra một tiến trình, một interface được cấu hình thì gọi là những câu lệnh major. Khi được nhập vào, những câu lệnh major sẽ đưa ta vào những mode cấu hình chuyên dụng. Những câu lệnh major không ảnh hưởng đến hệ thống cho đến khi những câu lệnh cấp dưới (subcommand) được đưa vào. Ví dụ, câu lệnh **interface serial 0** là một câu lệnh major sẽ không ảnh hưởng đến router cho đến khi những subcommand được đưa vào để hoàn tất cấu hình trên interface này.

Bên dưới là ví dụ của các câu lệnh major và các subcommand đi kèm

Router(config)#**interface serial 0** (major command)

Router(config-if)#**shutdown** (subcommand)

Router(config-if)#**line console 0** (major command)

Router(config-line)#**password cisco** (subcommand)

Router(config-line)#**router rip** (major command)

Router(config-router)#**network 10.0.0.0** (subcommand)

Chú ý rằng những câu lệnh major sẽ đưa ta chuyển từ mode này sang mode khác. Và cũng không cần thiết phải quay về global configuration mode trước khi chuyển sang các mode cấu hình khác.

Lưu cấu hình

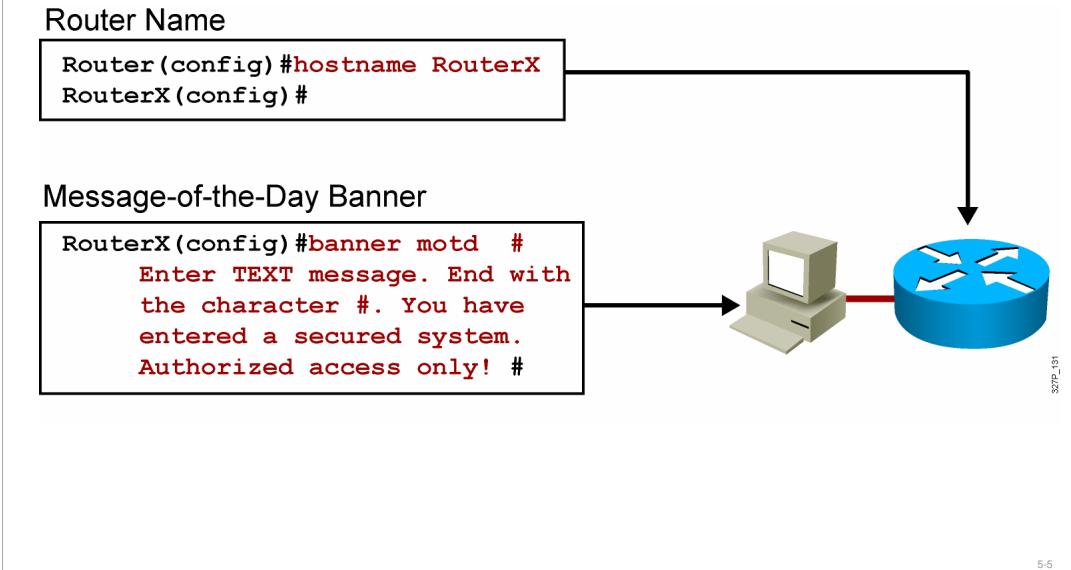
```
RouterX#  
RouterX#copy running-config startup-config  
Destination filename [startup-config]?  
Building configuration...  
  
RouterX#
```

Sao chép cấu hình hiện tại sang NVRAM

5-4

Sau khi đưa vào những câu lệnh để cấu hình router, ta phải lưu cấu hình đang chạy vào NVRAM bằng câu lệnh **copy running-config startip-config**. Nếu như cấu hình cấu hình không được lưu vào NVRAM thì sau khi khởi động lại, cấu hình sẽ mới đưa vào sẽ mất và router sẽ lấy cấu hình gần nhất được lưu trong NVRAM để sử dụng.

Cấu hình định danh router



3/27/P_L31

5-5

- CLI được sử dụng để cấu hình tên, password và các câu lệnh console khác trên router. Chủ đề này mô tả một số nhiệm vụ cấu hình cần thiết bao gồm tên và các password trên router.
- Một trong những bước cấu hình đầu tiên là đặt tên cho router. Việc đặt tên cho router sẽ giúp việc quản lý hệ thống mạng tốt hơn qua việc có thể xác định định danh những thiết bị trên mô hình mạng. Tên của router được gọi là hostname và tên này sẽ được hiển thị tại dấu nhắc của router. Nếu hostname không được cấu hình, mặc định router sẽ lấy tên là **Router**. Tên của router sẽ được cấu hình ở global configuration mode. Như được thể hiện ở ví dụ trên, tên của router được đặt là **RouterX**.
- Ta có thể cấu hình một biểu ngữ MOTD (message-of-the-day) để hiển thị trên thiết bị đầu cuối khi nối vào router. Biểu ngữ này sẽ được hiện khi bắt đầu đăng nhập và sẽ có ích để truyền tải những thông điệp cho người dùng đầu cuối. Theo sau câu lệnh **banner motd** là một hoặc nhiều khoảng cách cùng với ký tự cách ly. Trong ví dụ này, ký tự cách ly được sử dụng là dấu thăng (#). Ký tự cách ly này cũng sẽ được nhập vào sau khi kết thúc đoạn văn bản cho biểu ngữ.
- Ta cũng có thể đưa thêm một vào mô tả cho các interface của router để giúp nhớ một số thông tin riêng biệt cho các interface đó chẩn hạn dịch vụ mang được sử dụng cho interface... Những mô tả này có ý nghĩa duy nhất chỉ để giúp xác định các để sử dụng interface này cho chính xác. Mô tả này sẽ xuất hiện khi xem thông tin trên bộ nhớ RAM của router hay với câu lệnh **show interfaces**.

Câu lệnh trong Console-Line

```
RouterX(config) #line console 0  
RouterX(config-line) #exec-timeout 20 30
```

- Điều chỉnh thời gian timeout trên line console

```
RouterX(config) #line console 0  
RouterX(config-line) #logging synchronous
```

- Hiển thị lại những câu lệnh nhập vào bị ngắt quãng

5-6

• Một câu lệnh hữu dụng khác là **exec-timeout**. Ở hình trên, câu lệnh exec-timeout sẽ thiết lập thời gian tạm ngưng cho phiên làm việc trên cổng console là 20 phút và 30 giây. Giá trị mặc định là 10 phút.

• Câu lệnh **logging synchronous** sẽ hữu ích khi những thông điệp từ cổng console xuất hiện lúc ta đang nhập lệnh vào đồng thời. Thay vì những thông điệp này sẽ gián đoạn đến những câu lệnh nhập vào, câu lệnh sẽ giúp những thông tin đưa vào được chuyển sang một dòng khác sau khi một thông điệp từ cổng console được đưa ra. Việc này giúp việc đọc thông tin vào ra dễ dàng hơn.

Cấu hình Interface

```
RouterX(config)#interface type number  
RouterX(config-if) #
```

- **type** bao gồm serial, ethernet, token ring, fddi, hssi, loopback, dialer, null, async, atm, bri, tunnel...
- **number** dùng để xác định từng interface cụ thể

```
RouterX(config)#interface type slot/port  
RouterX(config-if) #
```

- Với router dạng modular, lựa chọn các interface mong muốn

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

- Thoát khỏi mode interface hiện tại

5-7

Những cấu hình trên các interface sẽ bao gồm những thứ như địa chỉ IP, đóng gói lớp data-link, loại phương tiện truyền, băng thông, tốc độ xung nhịp. Ta có thể cấu hình những đặc tính này trên từng interface một. Khi đưa vào câu lệnh **interface**, ta phải định ra loại và số vị trí của interface đó. Số của các interface phụ thuộc vào vị trí vật lý của nó trên router. Sự xác định này rất quan trọng khi router có nhiều interface cùng loại cùng tồn tại. Ví dụ về loại và số vị trí của interface được cho như dưới:

```
Router(config)#interface serial 0
```

```
Router(config)#interface fa 0/0
```

Một interface trên Cisco router tích hợp dịch vụ dòng 2800 và 3800 hoặc một số router dạng modular khác được xác định qua vị trí slot, số vị trí port trên module của slot đó.

```
Router(config)#interface fa 1/0
```

Để thoát ra khỏi một interface, gõ lệnh **exit** tại dấu nhắc Router(config-if)#.

Cấu hình mô tả Interface

```
RouterX(config-if)# description string
```

- **string** một mô tả giúp nhớ những thông tin về interface này.
- Số lượng ký tự tối đa là 238.

5-8

Để đưa thêm mô tả vào interface, sử dụng câu lệnh **description** trong mode interface. Để tháo gỡ mô tả này, thêm vào **no** trước câu lệnh.

Ngưng và kích hoạt một interface

```
RouterX#configure terminal  
RouterX(config)#interface serial 0  
RouterX(config-if)#shutdown  
%LINK-5-CHANGED: Interface Serial0, changed state to administratively down  
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to down
```

- Ngưng kích hoạt interface

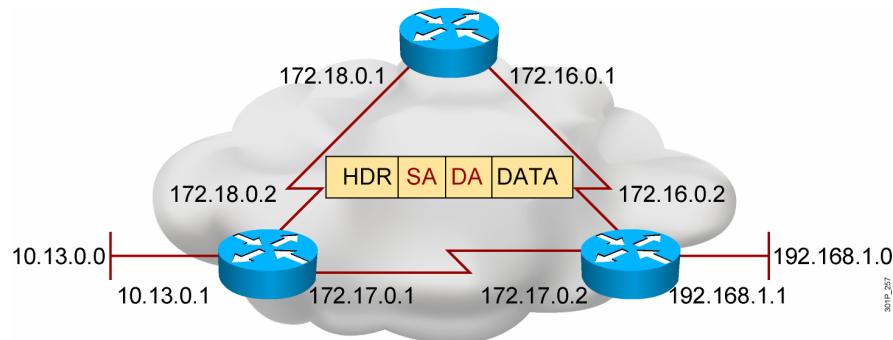
```
RouterX#configure terminal  
RouterX(config)#interface serial 0  
RouterX(config-if)#no shutdown  
%LINK-3-UPDOWN: Interface Serial0, changed state to up  
%LINEPROTO-5-UPDOWN: Line Protocol on Interface Serial0, changed state to up
```

- Kích hoạt interface

5-9

- Ta có thể ngưng kích hoạt (disable) một interface để thực hiện quá trình bảo trì phần cứng trên interface đó hay để phân đoạn hệ thống mạng. Câu lệnh **shutdown** sẽ tắt interface đó theo ý nghĩa quản trị. Để trả lại trạng thái kích hoạt, sử dụng câu lệnh **no shutdown**.
- Khi một interface được cấu hình lần đầu, trừ khi ở setup mode, ta phải kích hoạt interface này trước khi nó có thể được dùng để truyền và nhận dữ liệu. Sử dụng câu lệnh **no shutdown** sẽ cho phép hệ điều hành Cisco IOS sử dụng interface này.

Cấu hình địa chỉ IP



- Có một địa chỉ IP duy nhất cho phép các host giao tiếp với nhau
- Chọn đường dẫn dựa trên địa chỉ IP đích

5-10

Mỗi interface trên Cisco router phải có một địa chỉ IP để xác định nó một cách duy nhất trên mạng. Chủ đề này mô tả cách cấu hình địa chỉ IP cho mỗi interface trên Cisco router.

Câu lệnh show interface

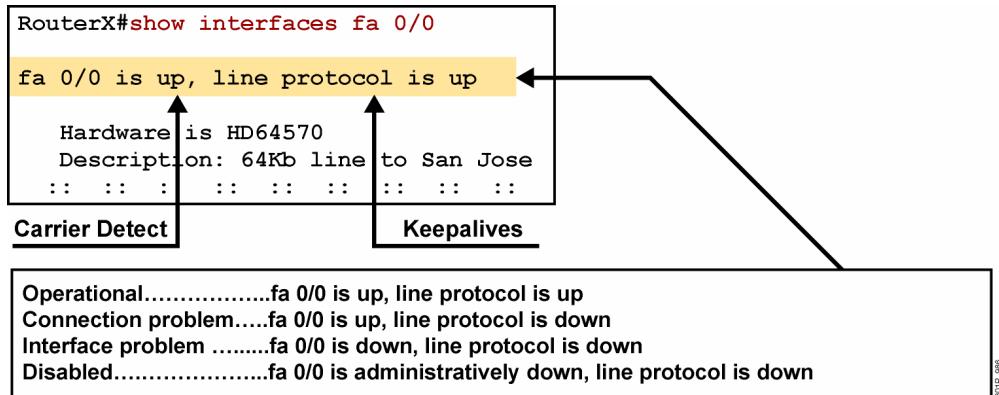
```
RouterX#show interfaces
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 00e0.1e5d.ae2f (bia 00e0.1e5d.ae2f)
  Internet address is 10.1.1.11/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:07, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    81833 packets input, 27556491 bytes, 0 no buffer
    Received 42308 broadcasts, 0 runts, 0 giants, 0 throttles
    1 input errors, 0 CRC, 0 frame, 0 overrun, 1 ignored, 0 abort
    0 input packets with dribble condition detected
    55794 packets output, 3929696 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 babbles, 0 late collision, 4 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

5-11

Sau khi hoàn tất cấu hình trên interface của router, ta có thể kiểm tra lại cấu hình bằng câu lệnh **show interfaces**. Chủ đề này mô tả câu lệnh **show** và các phần thông tin thể hiện để kiểm tra cấu hình.

Câu lệnh **show interfaces** thể hiện trạng thái và các thông kê cho tất cả các interface trên router. Thêm vào đó, những thông tin trên cho từng interface có thể được hiển thị bằng câu lệnh **show interfaces type slot**.

Diễn dịch trạng thái một interface



301P_986

5-12

Một trong những thành phần quan trọng của câu lệnh **show interfaces** là sự hiển thị của line và trạng thái giao thức data-link. Hình trên thể hiện thông tin quan trọng để kiểm tra ý nghĩa trạng thái của cổng serial. Với một số cổng khác, ý nghĩa này có thể hơi khác so với trên cổng serial.

Thông số đầu tiên chỉ về lớp phần cứng và phản ánh cho chúng ta biết interface có nhận được sóng mang từ thiết bị DCE hay không. Thông số thứ hai chỉ về lớp data link và phản ánh thông tin giao thức keepalives ở lớp này có được nhận hay không

Dựa trên thông tin xuất ra từ câu lệnh **show interfaces**, ta có thể khắc phục một số lỗi như sau:

- Nếu **interface is up, line protocol is down** trường hợp này có thể do:
 - Không có tín hiệu keepalives
 - Không khớp về dạng đóng gói
- Nếu **interface is down, line protocol is down**, có thể cáp truyền đã không được kết nối khi router bật lên hoặc một số lỗi về interface là vấn đề này xảy ra. Ví dụ trong kết nối back-to-back, phía router bên kia có thể nằm ở trạng thái **administrative down**
- Nếu **interface is administratively down**, có nghĩa là interface đã bị ngưng kích hoạt (bằng câu lệnh **shutdown**)

Kiểm tra cấu hình trên cổng serial

```
RouterX#show interface serial s0/0/0
Serial0/0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 10.140.4.2/24
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:09, output 00:00:04, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing 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)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
(output omitted)
```

30/P_380

5-13

Sau khi cấu hình cổng serial, sử dụng câu lệnh **show interface serial** để kiểm tra sự thay đổi. Chú ý trong ví dụ này line trên cổn đã up và băng thông đã chuyển sang 64kbps.

Tóm tắt

- Từ privilege mode ta có thể vào global configuration mode và thực hiện tiếp cấu hình cho những mode khác
- Chức năng chính của router là chuyển gói từ một thiết bị mạng sang thiết bị khác. Để làm được chuyện này, đặc tính của interface mà gói dữ liệu sẽ nhận và gửi trên đó phải được xác định, như là địa chỉ, băng thông...

5-14

Từ privilege mode ta có thể vào global configuration mode và thực hiện tiếp cấu hình cho những mode khác

Chức năng chính của router là chuyển gói từ một thiết bị mạng sang thiết bị khác. Để làm được chuyện này, đặc tính của interface mà gói dữ liệu sẽ nhận và gửi trên đó phải được xác định, như là địa chỉ, băng thông...

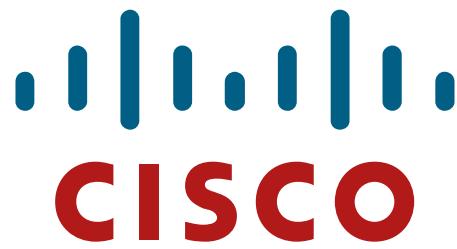
Summary (Cont.)

- Trong môi trường TCP/IP thiết bị đầu cuối cũng được xem như server hay các thiết bị đầu cuối khác. Giao thiệp xảy ra là nhờ vào mỗi host dùng một địa chỉ IP 32bit duy nhất.
- Khi đã hoàn thành cấu hình trên interface, ta có thể dùng lệnh show để kiểm tra các thông số.

5-15

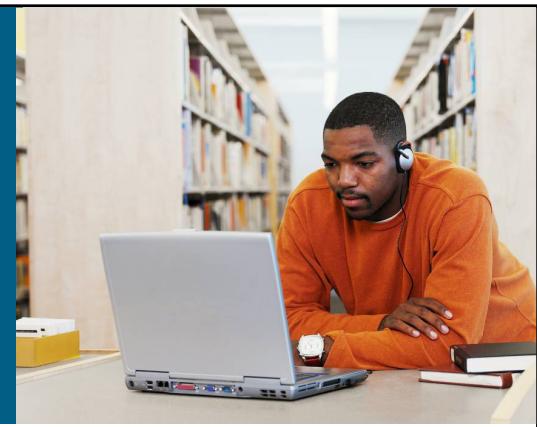
Trong môi trường TCP/IP thiết bị đầu cuối cũng được xem như server hay các thiết bị đầu cuối khác. Giao thiệp xảy ra là nhờ vào mỗi host dùng một địa chỉ IP 32bit duy nhất.

Khi đã hoàn thành cấu hình trên interface, ta có thể dùng lệnh show để kiểm tra các thông số



5-16

Bài 6: Quá trình phân phối gói dữ liệu



Kết nối LAN

6-1

- **Tổng quan**

Hiểu được tiến trình phân phối gói dữ liệu là phần cơ bản trong việc tìm hiểu quá trình hoạt động của các thiết bị Cisco. Ta phải hiểu được quá trình giao tiếp giữa host đến host cùng với router để có thể quản trị hệ thống mạng. Bài học mô tả quá trình giao tiếp giữa host đến host thông qua router.

- **Mục tiêu**

Cung cấp khả năng mô tả cách giữa những host giao tiếp với nhau thông qua các nhiệm vụ sau:

Mô tả địa chỉ lớp 2

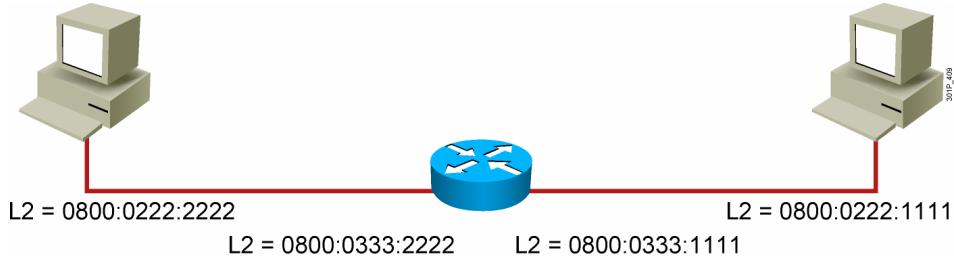
Mô tả địa chỉ lớp 3

Mô tả tiến trình phân phối gói dữ liệu giữa host đến host

Mô tả cách sử dụng câu lệnh **show ip arp**

Mô tả cách sử dụng các công cụ phổ biến của hệ điều hành Cisco IOS để kiểm tra kết nối

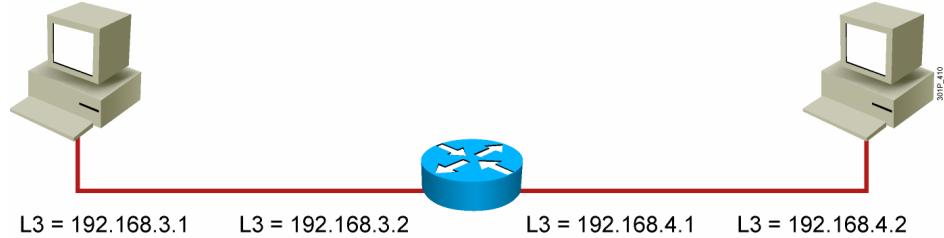
Địa chỉ lớp 2



6-2

- Địa chỉ MAC được gán vào thiết bị đầu cuối như các host. Những interface vật lý trên router cung cấp chức năng lớp 2 và được gán vào các địa chỉ MAC.

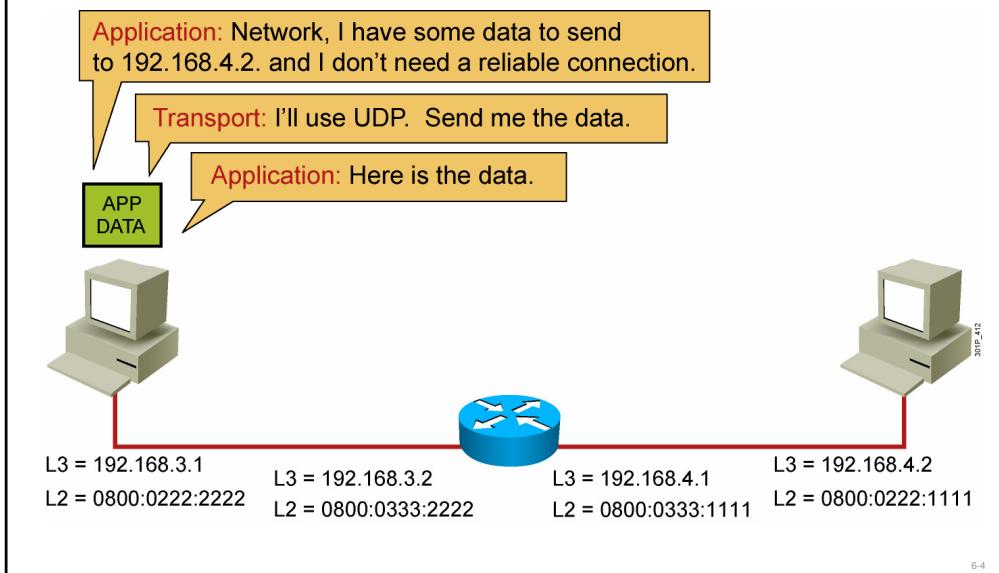
Địa chỉ lớp 3



6-3

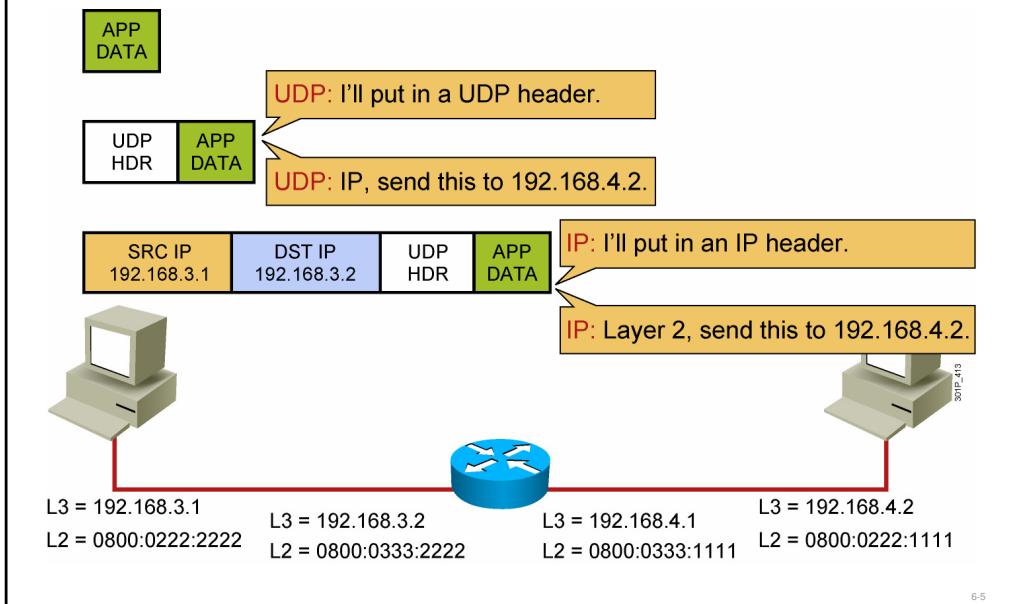
- Chủ đề mô tả địa chỉ lớp 3 trong mô hình giao tiếp host-to-host
- Router có địa chỉ lớp 3 cho mỗi interface

Quá trình phân phối dữ liệu (1 of 17)



- Những bước mô tả quá trình phân phối gói dữ liệu trên hệ thống định tuyến tương tự các bước để gửi một bức thư qua hệ thống bưu điện. Chủ đề sẽ mô tả tiến trình phân phối gói dữ liệu.
- Có nhiều bước được bao gồm trong tiến trình này.
- Host sẽ gửi bất kỳ một gói dữ liệu nào không nằm trong địa chỉ mạng cục bộ hiện tại ra ngoài default gateway. Default gateway là địa chỉ của router cục bộ và phải được cấu hình trên host (PC, server, ...)

Quá trình phân phối dữ liệu(2 of 17)

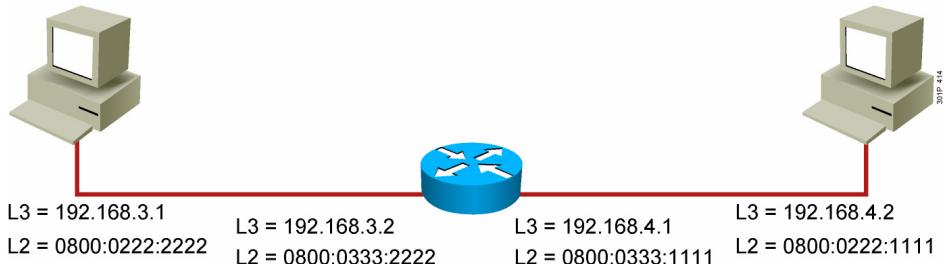


- Trong ví dụ này, host 192.168.2.1 có dữ liệu muốn gửi đến host 192.168.4.2. Các ứng dụng không cần quá trình truyền tin cậy bởi đã sử dụng dịch vụ với giao thức UDP

Quá trình phân phối dữ liệu(3 of 17)

Layer 2: ARP, do you have a mapping for 192.168.4.2?

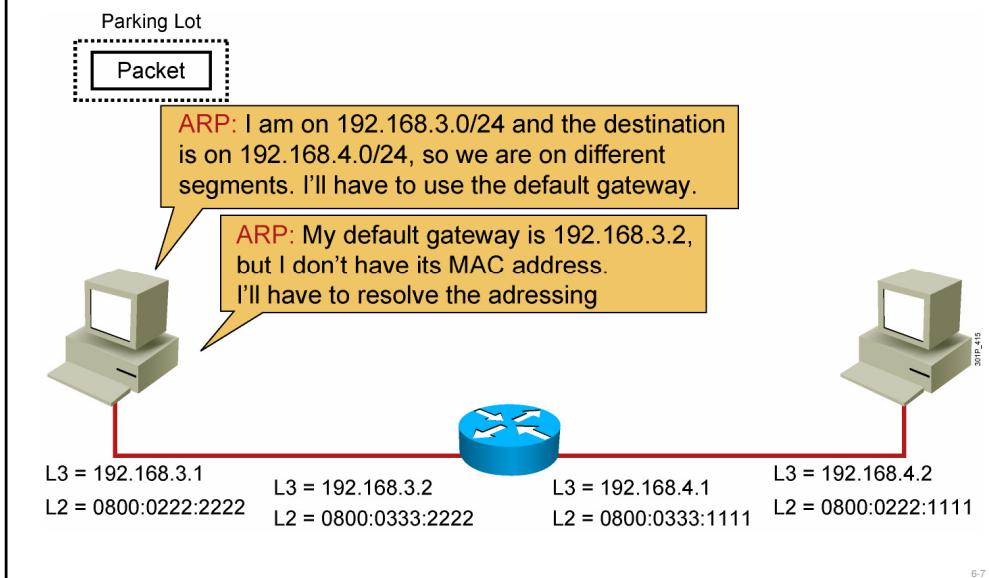
ARP: No, Layer 2 will have to hold the packet while I resolve the addressing.



6-6

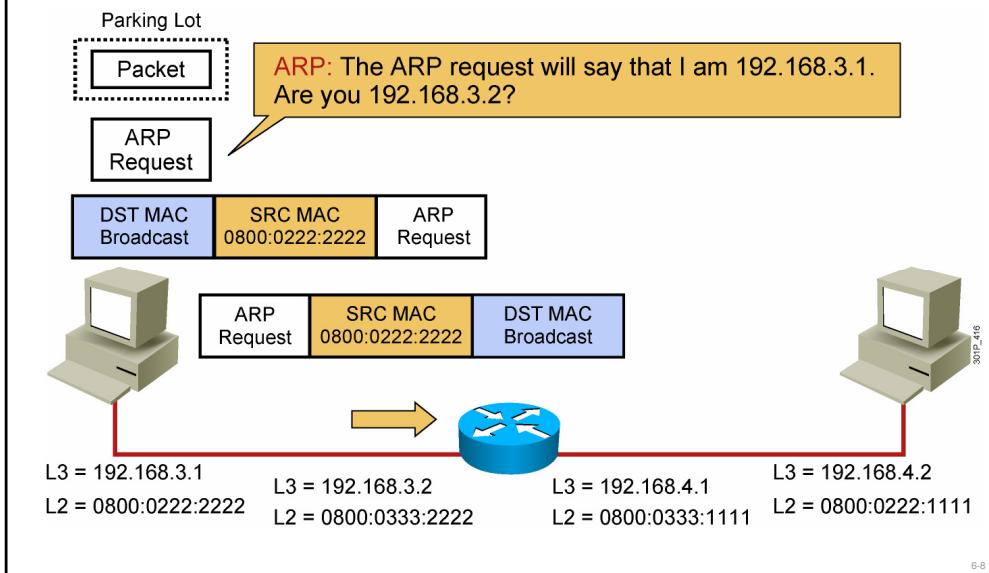
- Bởi vì không cần thiết phải thiết lập các phiên giao dịch, các ứng dụng có thể bắt đầu gửi dữ liệu. UDP chuẩn bị các header và đưa PDU xuống IP (lớp 3) và hướng dẫn cách gửi PDU đến 192.168.4.2. IP đóng gói PDU ở lớp 3 và tiếp tục đưa xuống lớp 2.

Quá trình phân phối dữ liệu(4 of 17)



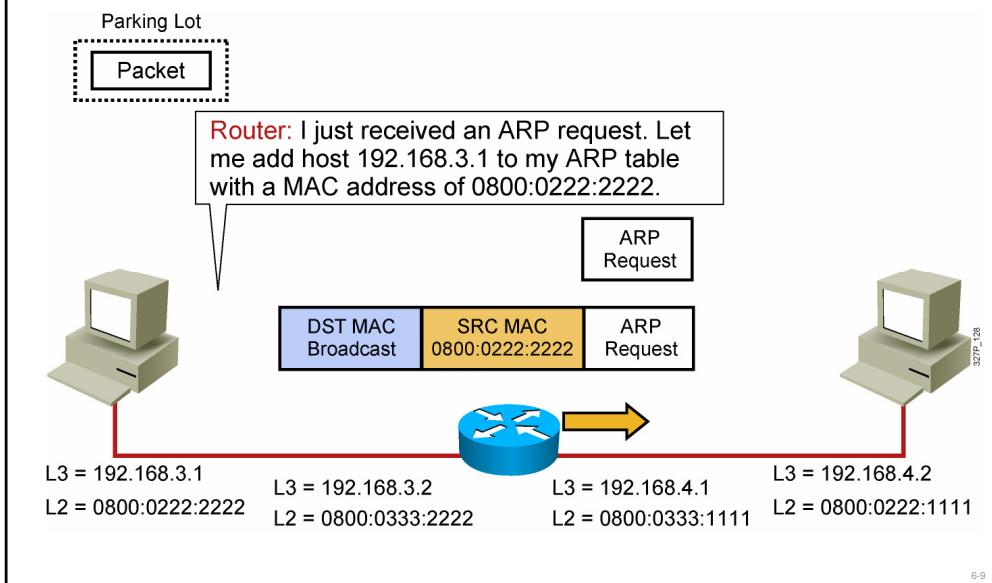
- Bảng ARP hiện tại không có bất kỳ một thông tin nào.

Quá trình phân phối dữ liệu(5 of 17)



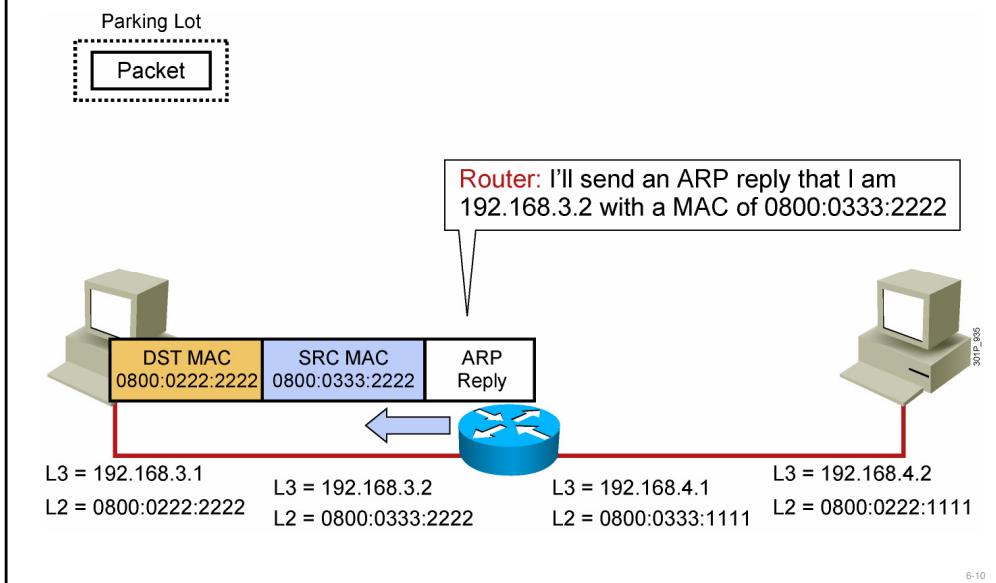
- Ví dụ này khác với ví dụ trước. Hai host nằm trên 2 đoạn mạng khác nhau: 192.168.3.0/24 và 192.168.4.0/24. Bởi vì các host không chạy bất kỳ giao thức định tuyến nào, do vậy nó sẽ không biết các với về đoạn mạng bên kia. Các host sẽ gửi khung dữ liệu đến default gateway, các host này sử dụng tiến trình ARP bình thường để lấy MAC này.

Quá trình phân phối dữ liệu(6 of 17)



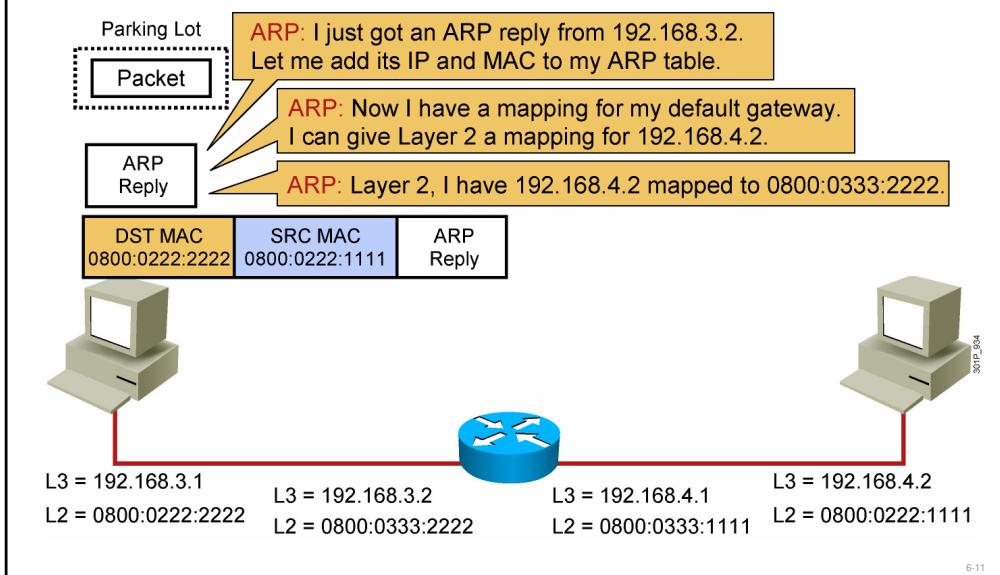
- User đã được cấu hình địa chỉ 192.168.3.2 như một default gateway. Host 192.168.3.1 gửi ra yêu cầu ARP và thông tin này được nhận bởi router.

Quá trình phân phối dữ liệu(7 of 17)



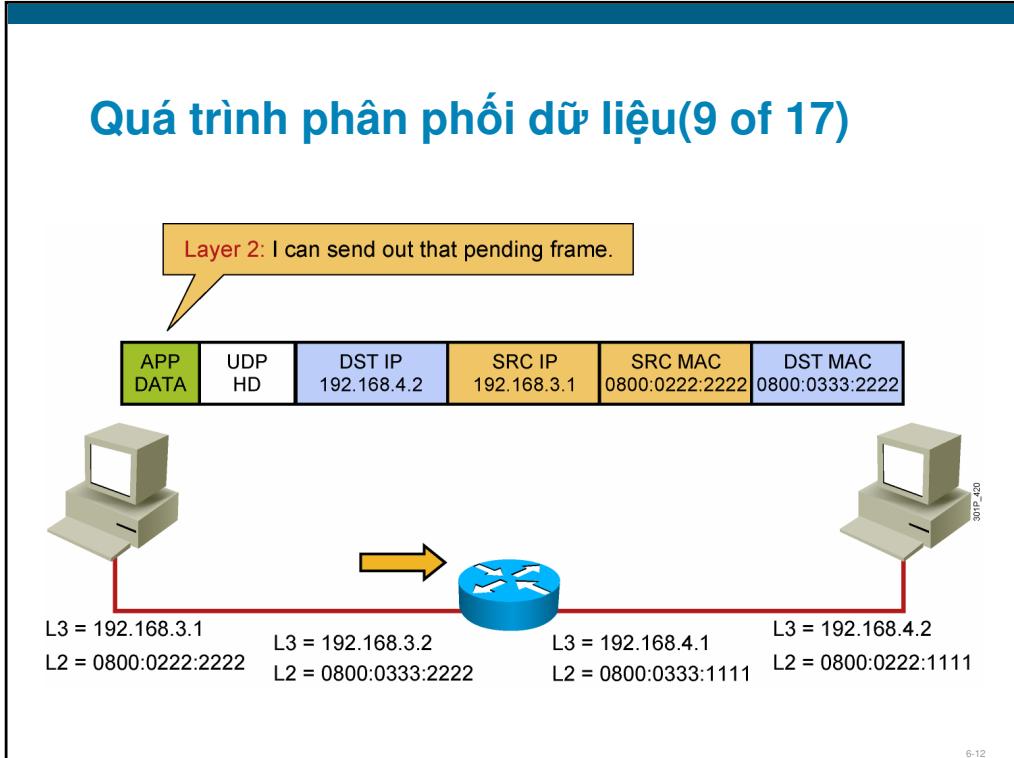
- Router sử lý tiến trình ARP giống như tất cả các host khác.

Quá trình phân phối dữ liệu(8 of 17)



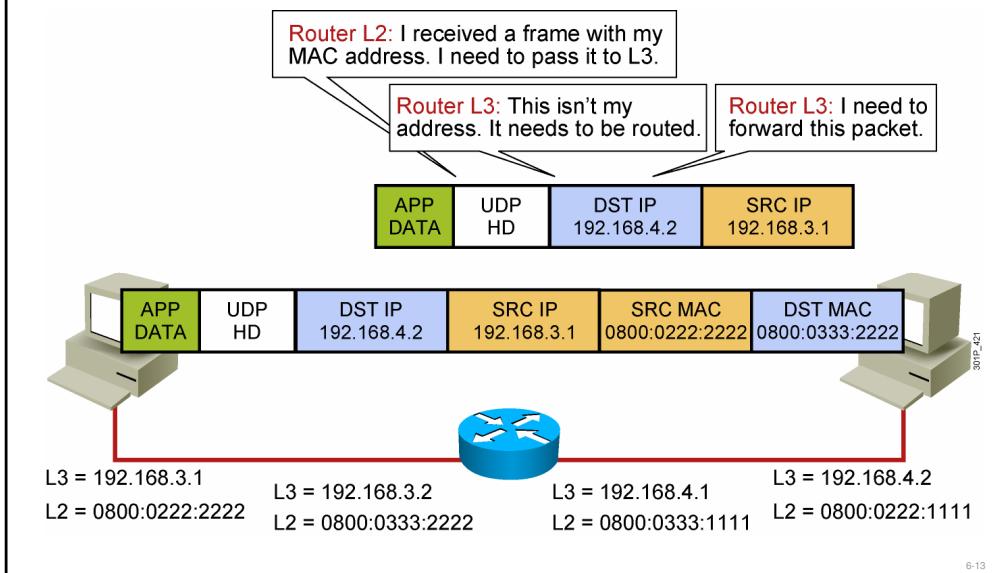
- Phản hồi được gửi lại cho thông tin ARP yêu cầu.

Quá trình phân phối dữ liệu(9 of 17)



- Host đích nhận được yêu cầu ARP. Thông tin lớp 2 lúc này được phản hồi. Chú ý rằng ARP gửi về thông tin ánh xạ giữa địa chỉ IP 192.168.4.2 và địa chỉ MAC của default gateway thay vì địa chỉ MAC thực.

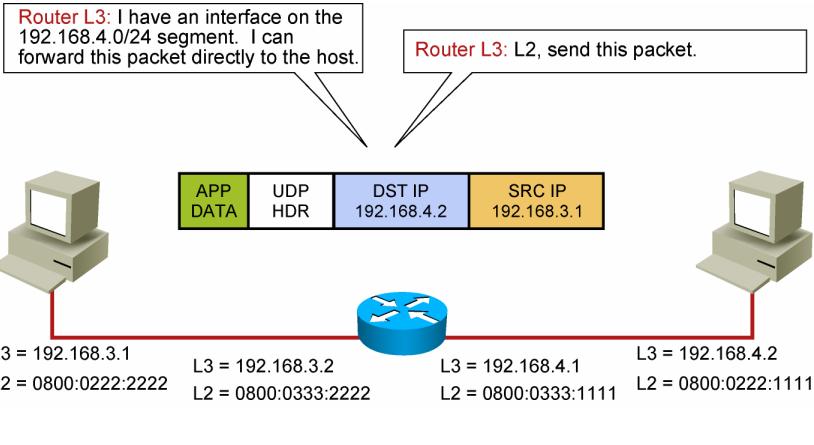
Quá trình phân phối dữ liệu(10 of 17)



- Khung dữ liệu đang chờ giờ sẽ được gửi đi với địa chỉ IP và MAC của nó nằm trong phần địa chỉ nguồn. Tuy nhiên, địa chỉ IP đích là IP của host từ xa, nhưng địa chỉ MAC là địa chỉ của default gateway.

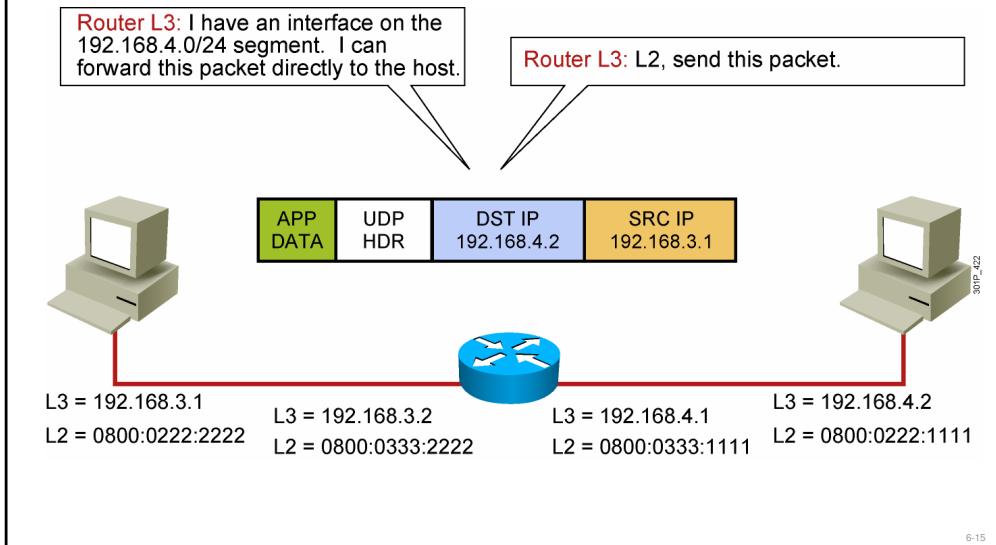
Quá trình phân phối dữ liệu(11 of 17)

Destination	Next Hop	Interface
192.168.3.0/24	Connected	fa 0/0
192.168.4.0/24	Connected	fa 0/1



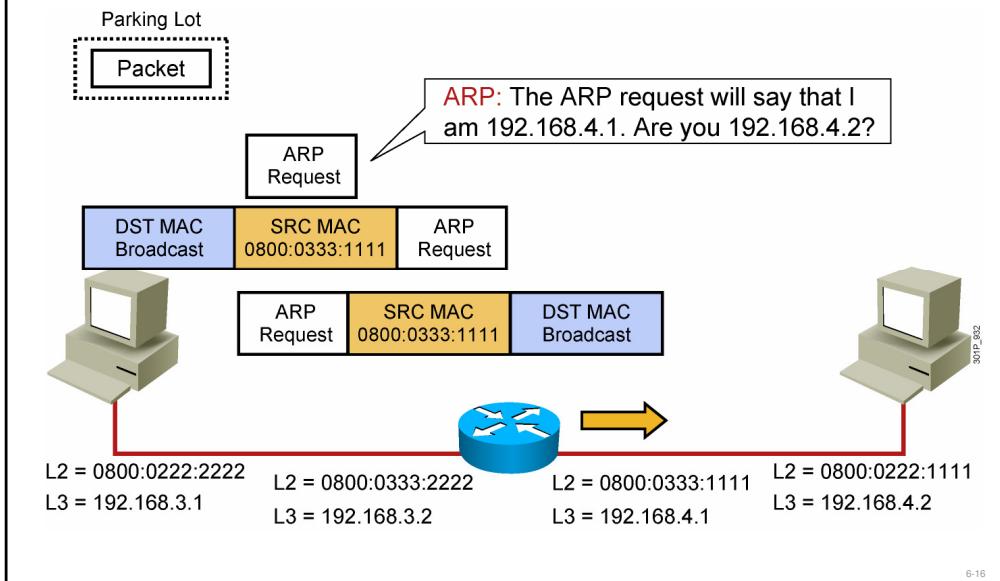
- Khi khung dữ liệu được nhận bởi router, router nhận ra địa chỉ MAC của nó và tiến hành xử lý khung dữ liệu này. Tại lớp 3, router nhận thấy rằng địa chỉ IP đích không phải là địa chỉ của mình. Nếu đây là một host, nó sẽ hủy gói dữ liệu này. Nhưng do là router, gói dữ liệu này sẽ được đưa qua tiến trình xử lý định tuyến.

Quá trình phân phối dữ liệu(12 of 17)



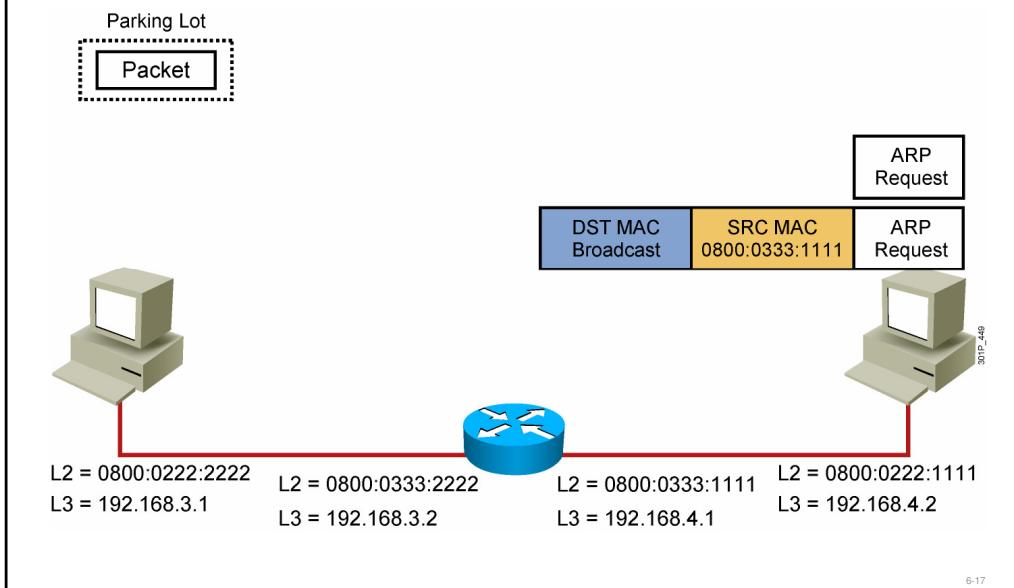
- Tiến trình định tuyến tìm địa chỉ IP đích trong bảng định tuyến (routing table). Trong ví dụ này, địa chỉ mạng đích được gắn trực tiếp vào router. Do vậy, tiến trình định tuyến có thể đẩy gói dữ liệu trực tiếp lớp ở interface phù hợp.

Quá trình phân phối dữ liệu(13 of 17)



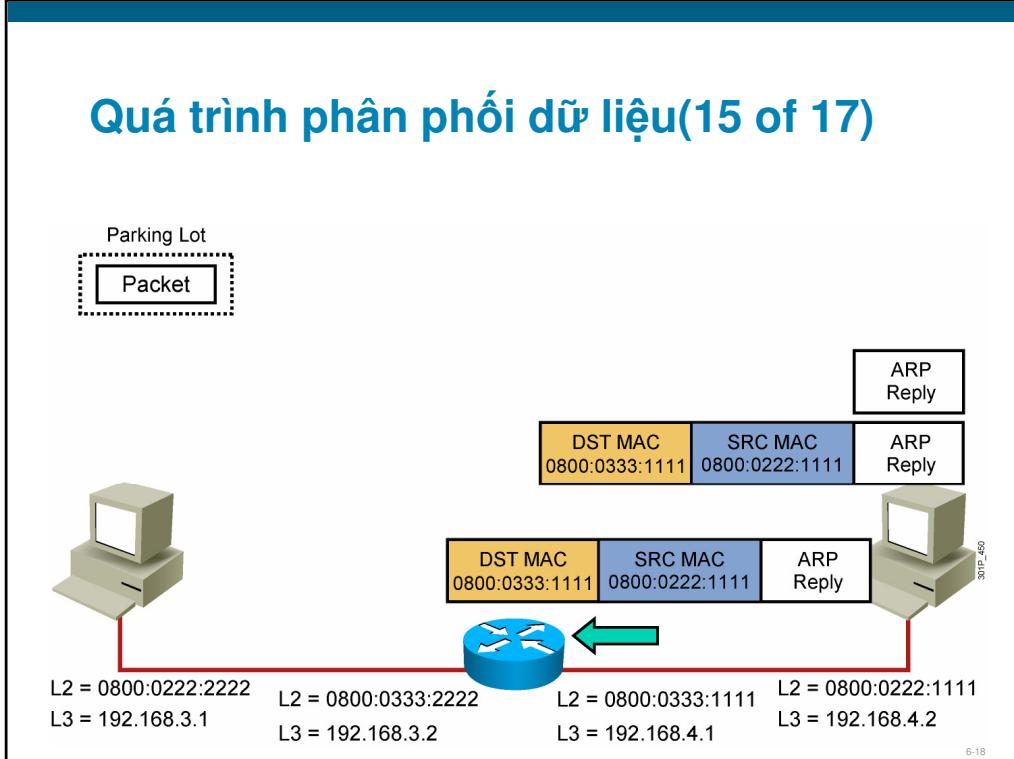
- Lớp 2 sẽ sử dụng tiến trình ARP để có được ánh xạ địa chỉ IP và địa chỉ MAC.

Quá trình phân phối dữ liệu(14 of 17)



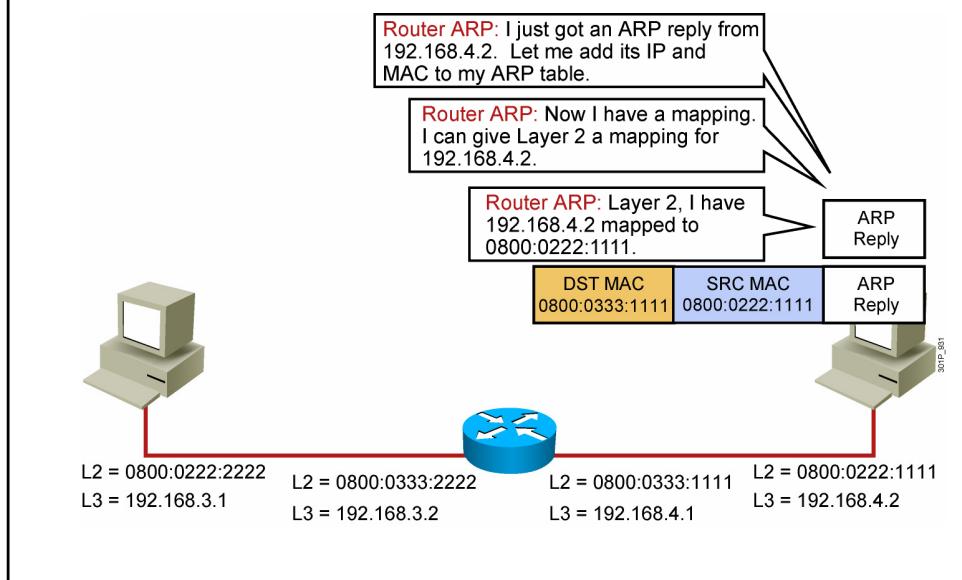
- Bên đích sẽ nhận và xử lý yêu cầu của ARP.

Quá trình phân phối dữ liệu(15 of 17)



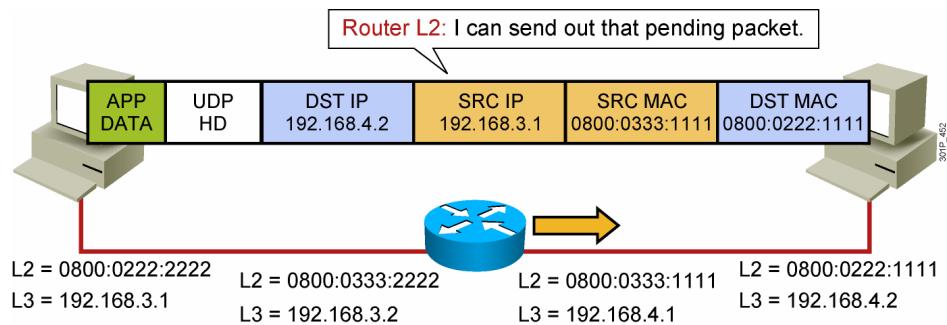
- Host nhận được khung dữ liệu chứa yêu cầu của ARP sẽ đưa yêu cầu này lên tiến trình ARP xử lý.

Quá trình phân phối dữ liệu(16 of 17)



- Host sẽ phản hồi cho yêu cầu ARP.

Quá trình phân phối dữ liệu(17 of 17)



6-20

- Khung dữ liệu sẽ được đưa đến đích.

Dùng câu lệnh show IP

Router# show ip arp					
Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	172.69.233.229	-	0000.0c59.f892	ARPA	Ethernet0/0
Internet	172.69.233.218	-	0000.0c07.ac00	ARPA	Ethernet0/0
Internet	172.69.233.19	-	0000.0c63.1300	ARPA	Ethernet0/0
Internet	172.69.233.309	-	0000.0c36.6965	ARPA	Ethernet0/0
Internet	172.19.168.11	-	0000.0c63.1300	ARPA	Ethernet0/0
Internet	172.19.168.254	9	0000.0c36.6965	ARPA	Ethernet0/0

6-21

Chủ đề sẽ mô tả cách sử dụng câu lệnh **show ip arp**.

Để hiển thị bộ nhớ tạm của ARP, sử dụng câu lệnh **show ip arp** theo cấu trúc sau

show ip arp [ip-address] [host-name] [mac-address] [interface type number]

- **Mô tả cú pháp**

ip-address (Tùy chọn) những dòng thông tin ARP
Khớp với địa chỉ IP này sẽ được thể hiện

host-name (Tùy chọn) tên host

mac-address (Tùy chọn) 48-bit địa chỉ MAC

Interface type number (Tùy chọn) những dòng thông tin ARP học được từ
interface này sẽ được hiển thị

- **Cách sử dụng**

ARP thiết lập sự tương ứng giữa địa chỉ mạng (địa chỉ IP) và địa chỉ phần cứng (địa chỉ Ethernet). Thông tin của sự tương ứng này được lưu trong bộ nhớ tạm thời trong một thời gian được định trước và sau đó sẽ bị hủy đi.

Bảng sau mô tả một ví dụ đưa ra từ câu lệnh **show ip arp**

ping

Router#

```
ping [[protocol {host-name | system-address}]]
```

- Sử dụng câu lệnh ping để chuẩn đoán trạng thái kết nối mạng.

6-22

- Chủ đề này mô tả cách sử dụng một số công cụ phổ biến để kiểm tra kết nối trên router.
- Để chuẩn đoán một kết nối cơ bản, ta có thể sử dụng câu lệnh **ping** trong user mode hay privilege mode

```
ping [[protocol {host-name | system-address}]]
```

Mô tả cú pháp

- protocol* (Tùy chọn) từ khóa giao thức, có thể là **appletalk**, **atm**, **clns**, **decnet**, **ipx**, hay **srn**. Nếu một giao thức cụ thể không được chỉ ra, ping sẽ sử dụng IP (IPv4). Để sử dụng các tùy chọn mở rộng, xem tài liệu cho câu lệnh **ping ip**.

host-name

Tên của hệ thống được dùng để ping, nếu host-name hay system-address không được chỉ ra, ta sẽ sử dụng ping trong mode hội thoại.

systemaddress

Địa chỉ của hệ thống được ping. Nếu host-name hay system-address không được chỉ ra, ta sẽ sử dụng ping trong mode hội thoại.

traceroute

Router#

```
traceroute [protocol] destination
```

- Sử dụng câu lệnh traceroute để xem tuyến đường thực sự dùng để gởi gói dữ liệu.

6-23

- Để khám phá những tuyến là gói dữ liệu sẽ thực sự vượt qua khi đi đến đích, ta có thể sử dụng câu lệnh **traceroute** trong user mode hay privilege mode.

traceroute [vrf vrf-name] [protocol] destination

- **Mô tả cú pháp**

- *protocol* (Tùy chọn) từ khóa giao thức, một trong các giao thức **appletalk**, **clns**, **ip**, **ipv6**, **ipx**, **oldvines**, hoặc **vines**.

Khi không được chỉ ra, thông số giao thức này sẽ được xác định dựa trên định dạng của thông số *destination*.

- *destination* (Tùy chọn ở privileged mode; yêu cầu trong user mode) địa chỉ đích hay hostname ta muốn theo vết. Hệ điều hành

xác định các thông số mặc định cho các giao thức thích hợp và quá trình theo vết sẽ được khởi tạo.

Tóm tắt

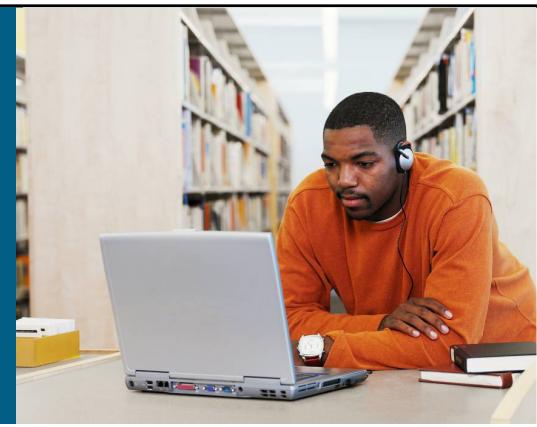
- Nếu các host không cùng nằm trong đoạn mạng, khung dữ liệu sẽ gửi đến default gateway.
- Gói dữ liệu gửi đến default gateway có địa chỉ IP đích và nguồn là không đổi.
- Khung dữ liệu gửi đến default gateway có địa chỉ MAC đích là của default gateway và MAC nguồn là không đổi.
- Router thay đổi thông tin lớp 2 và để nguyên thông tin lớp 3.
- Câu lệnh show ip arp hiển thị thông tin ánh xạ giữa MAC và IP.
- Công cụ kiểm tra kết nối của Cisco IOS bao gồm **ping** và **traceroute**.

6-24



6-25

Bài 7: Tìm hiểu về bảo mật trên Cisco Router



Kết nối LAN

7-41

Tổng quan

- Sau khi bảo vệ về mặt vật lý trên hệ thống mạng, ta phải đảm bảo rằng truy xuất vào router qua cổng console hay vty cũng phải được bảo mật.Thêm vào đó, ta phải chắc rằng những cổng không sử dụng sẽ không trở thành mối nguy cơ trên mạng. Bài học mô tả các vấn đề bảo mật trên router.

Mục tiêu

- Cung cấp khả năng thực thi vấn đề bảo mật cơ bản trên Cisco router qua những nhiệm vụ sau:
- Mô tả cách giảm nhẹ các mối đe dọa liên quan đến phần cứng, môi trường, điện và quá trình bảo trì liên quan đến Cisco router
- Cấu hình password bảo mật
- Cấu hình biểu ngữ đăng nhập
- Mô tả Telnet và SSH cho vấn đề truy xuất từ xa

Các nguy cơ phổ biến trong việc cài đặt vật lý

- Nguy cơ về phần cứng
- Nguy cơ về môi trường
- Nguy cơ về điện
- Nguy cơ về bảo trì



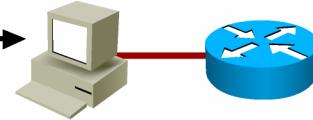
7-2

- Việc thiết lập các thiết bị mạng không đúng và không hoàn chỉnh thường là các mối đe dọa không được chú ý đến. Hệ điều hành hỗ trợ chức năng bảo mật một mình sẽ không thể ngăn được các sự cố liên quan đến một hệ thống được thiết lập một cách nghèo nàn. Chủ đề này mô tả cách để giảm nhẹ các mối đe dọa liên quan đến phần cứng, môi trường, điện và quá trình bảo trì liên quan đến Cisco router.
- Việc thiết lập các thiết bị mạng không đúng dẫn đến nguy cơ bảo mật trên hệ thống mạng được chia thành 4 loại:
 - Mối đe dọa về phần cứng: Các nguy cơ về các sự cố vật lý đối với router và các phần cứng router
 - Mối đe dọa về môi trường: Các nguy cơ về nhiệt độ (quá nóng hoặc quá lạnh) hay do độ ẩm (quá ẩm hoặc quá khô)
 - Mối đe dọa về điện: Các nguy cơ về phân nhánh điện thế, không đủ nguồn cung cấp, nhiễu điện và mất công suất
 - Mối đe dọa về bảo trì: Các nguy cơ về việc sử dụng các công cụ điện, thiếu các thành phần dự phòng, vấn đề về cáp,...

Cấu hình Password cho router

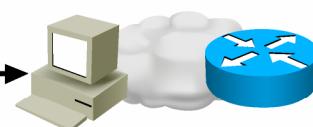
Console Password

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



Virtual Terminal Password

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



Enable Password

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



Secret Password

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

Service Password-Encryption Commands

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

30/10_084

- Ta có thể sử dụng CLI để cấu hình password và các câu lệnh khác. Chủ đề này mô tả quá trình cấu hình password và các nhiệm vụ cấu hình cần thiết.
- Chú ý: Password này chỉ có mục tiêu giảng dạy, password trong thực tế phải là những password mạnh.
- Ta có thể bảo vệ router bằng cách sử dụng password để hạn chế truy xuất vào router. Sử dụng password và gán phân quyền cho router là cách đơn giản nhất để cung cấp truy xuất bảo mật vào router. Password có thể thiết lập trên từng line cụ thể như line console, hay password cho mode đặc quyền. Password phân biệt chữ thường và chữ hoa.
- Mỗi cổng telnet trên một router được xem như là một “vty đầu cuối”. Có tối đa 5 cổng vty trên router cho phép 5 phiên telnet đồng thời vào router. Trên router, các cổng vty được đánh số từ 0 đến 4.
- Ta có thể dùng câu lệnh **line console 0** theo sau với câu lệnh **login** và **password** để yêu cầu password đăng nhập trước khi thiết lập phiên giao dịch trên cổng console. Mặc định, yêu cầu đăng nhập không được kích hoạt trên cổng console hay trên cổng vty.
- Ta có thể dùng câu lệnh **line vty 0 4** theo sau với câu lệnh **login** và **password** để yêu cầu password đăng nhập trước khi thiết lập phiên giao dịch trên cổng vty qua dịch vụ telnet.
- Câu lệnh **login local** cho phép kiểm tra password cho từng người dùng sử dụng thông số username và password cấu hình qua câu lệnh **username** ở global configuration mode. Câu lệnh này sẽ thiết lập quá trình chứng thực username với password được mã hóa.
- Câu lệnh **enable password** tại global mode hạn chế truy xuất vào privilege mode. Ta có thể gán một password được mã hóa qua câu lệnh **enable secret**. Nếu password secret này được cấu hình, nó sẽ được sử dụng thay vì password từ câu lệnh **enable password**.

- Ta cũng có thể thêm vào một lớp bảo mật, điều này sẽ rất hiệu dụng cho những password phải gửi đi trên mạng hay lưu trên các TFTP server. Cisco cung cấp một tính năng cho phép ta mã hóa dữ liệu, câu lệnh được sử dụng cho chức năng này là **service password-encryption** trong global configuration mode.
- Password được thể hiện hay được thiết lập sau khi ta cấu hình câu lệnh **service password-encryption** sẽ được mã hóa.
- Để nhưng kích hoạt câu lệnh này, thêm **no** vào trước câu lệnh. Ví dụ **no service password-encryption** là câu lệnh ngưng kích hoạt chức năng mã hóa password.

Cấu hình login banner

Định nghĩa một biểu ngữ hiện ra trước dấu nhắc để nhập username và password

```
RouterX# banner login " Access for authorized users only. Please enter your  
username and password. "
```



7-5

- Ta có thể sử dụng CLI để cấu hình message-of-the-day và các câu lệnh console khác. Chủ đề này mô tả một số cấu hình cần thiết để kích hoạt chức năng của biểu ngữ đăng nhập (login banner).
- Để định nghĩa một biểu ngữ hiện ra trước dấu nhắc để nhập username và password ta dùng câu lệnh **banner login** ở global configuration mode. Để ngưng chức năng này, ta thêm **no** phía trước câu lệnh.
- Khi nạp vào câu lệnh này, phía sau câu lệnh là một hoặc nhiều khoản trắng cùng ký tự phân cách. Trong ví dụ này ký tự ngăn cách là dấu nháy kép (""). Sau khi nội dung biểu ngữ được điền vào, kết thúc câu lệnh cũng với ký tự ngăn cách tương tự.
- **Chú ý** Các cảnh báo nên được sử dụng khi lựa chọn những từ ngữ được sử dụng trong biểu ngữ đăng nhập. Những từ như “Welcome” có thể ngụ ý rằng quá trình truy cập này thì không bị hạn chế và đây có thể là lý do hacker biện minh cho hành động xâm nhập của mình.

Truy xuất bằng Telnet và SSH

- Telnet
 - Telnet là công cụ phổ biến nhất để truy xuất vào các thiết bị mạng
 - Không bảo mật
- SSH
 - Mã hóa
 - Phải định nghĩa IP domain
 - Khóa phải được tạo ra

```
!--- The username command create the username and password for the SSH session
username cisco password 0 cisco

ip domain-name mydomain.com

crypto key generate rsa

ip ssh version 2

line vty 0 4
login local
transport input ssh
```



7-6

- Chủ đề này mô tả về phương pháp truy cập từ xa Telnet và SSH.
- Telnet là công cụ phổ biến nhất để truy xuất vào các thiết bị mạng. Tuy nhiên, Telnet lại là một cách truy xuất không bảo mật. SSH là một phương pháp bảo mật và dùng thay thế Telnet. Giao tiếp giữa client và server được mã hóa bởi cả SSH phiên bản 1 (SSH1) và phiên bản 2 (SSH2). Nếu có thể, nên sử dụng phiên bản 2 bởi nó sử dụng các thuật toán bảo mật được nâng cấp. Khi quá trình mã hóa được kích hoạt, mã khóa Rivest, Shamir và Adleman (RSA) phải được sinh ra trên router.Thêm vào đó, IP domain name cũng phải được gán trên router.
- Khi thực thi SSH, đầu tiên nên kiểm tra quá trình xác thực mà không có SSH để đảm bảo rằng quá trình xác thực hoạt động trước khi thêm vào SSH. Ví dụ sau đây hiện quá trình xác thực cục bộ cho phép ta telnet vào router với username “cisco” và password “cisco”.
- !--- The username command create the username and password for
the SSH session
username cisco password 0 cisco
ip domain-name mydomain.com
crypto key generate rsa
ip ssh version 2
line vty 0 4
login local
transport input ssh
- Để kiểm tra quá trình xác thực với SSH, ta phải thêm vào những câu lệnh vừa rồi để kích hoạt SSH, sau đó kiểm tra SSH từ PC hay máy trạm UNIX.

- Nếu ta muốn ngăn những kết nối không phải SSH, thêm vào câu lệnh **transport input ssh** để hạn chế router chỉ chấp nhận những kết nối SSH, telnet sẽ bị từ chối

!--- Prevent non-SSH Telnets.

```
transport input ssh
```

- Kiểm tra để chắc rằng những người dùng không sử dụng SSH không thể truy xuất vào router

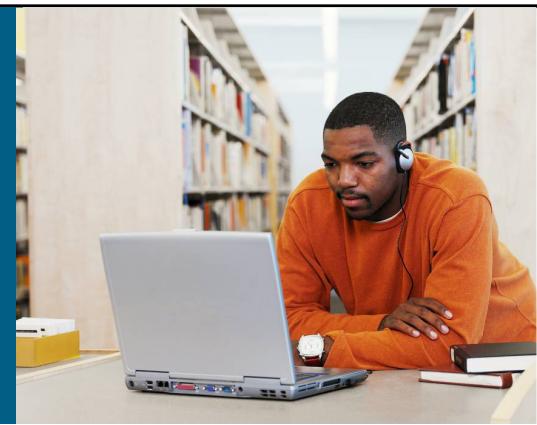
Tóm tắt

- Cấp độ bảo mật đầu tiên là mặt vật lý.
- Password được dùng để hạn chế truy cập.
- Login banner được hiện ra trước dấu nhắc để nhập username và password .
- Telnet gởi dữ liệu ở dạng clear text; SSH mã hóa dữ liệu.



7-9

Bài 8: Sử dụng Cisco SDM

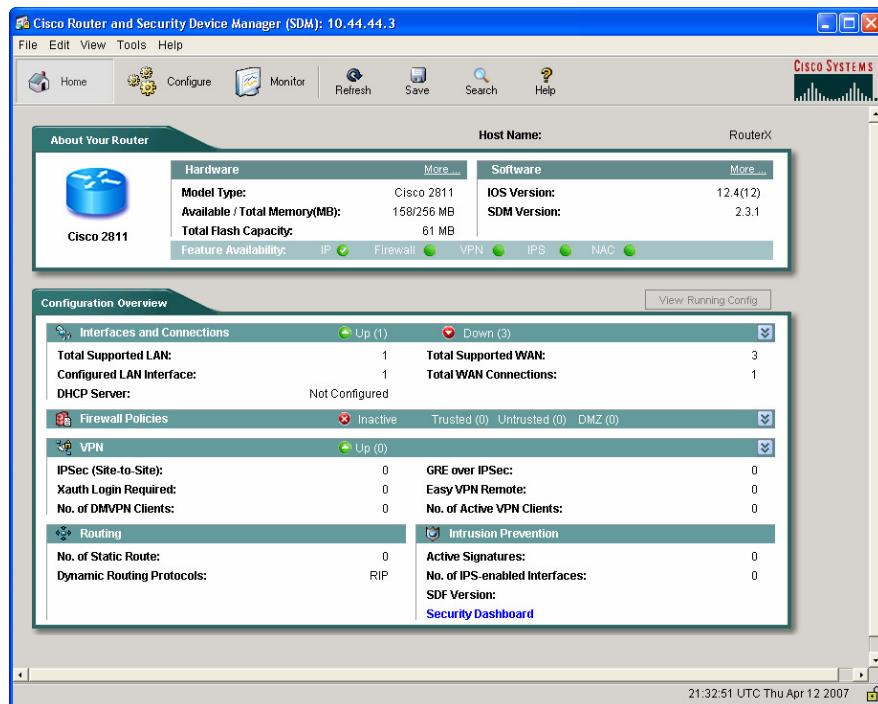


Kết nối LAN

8-1

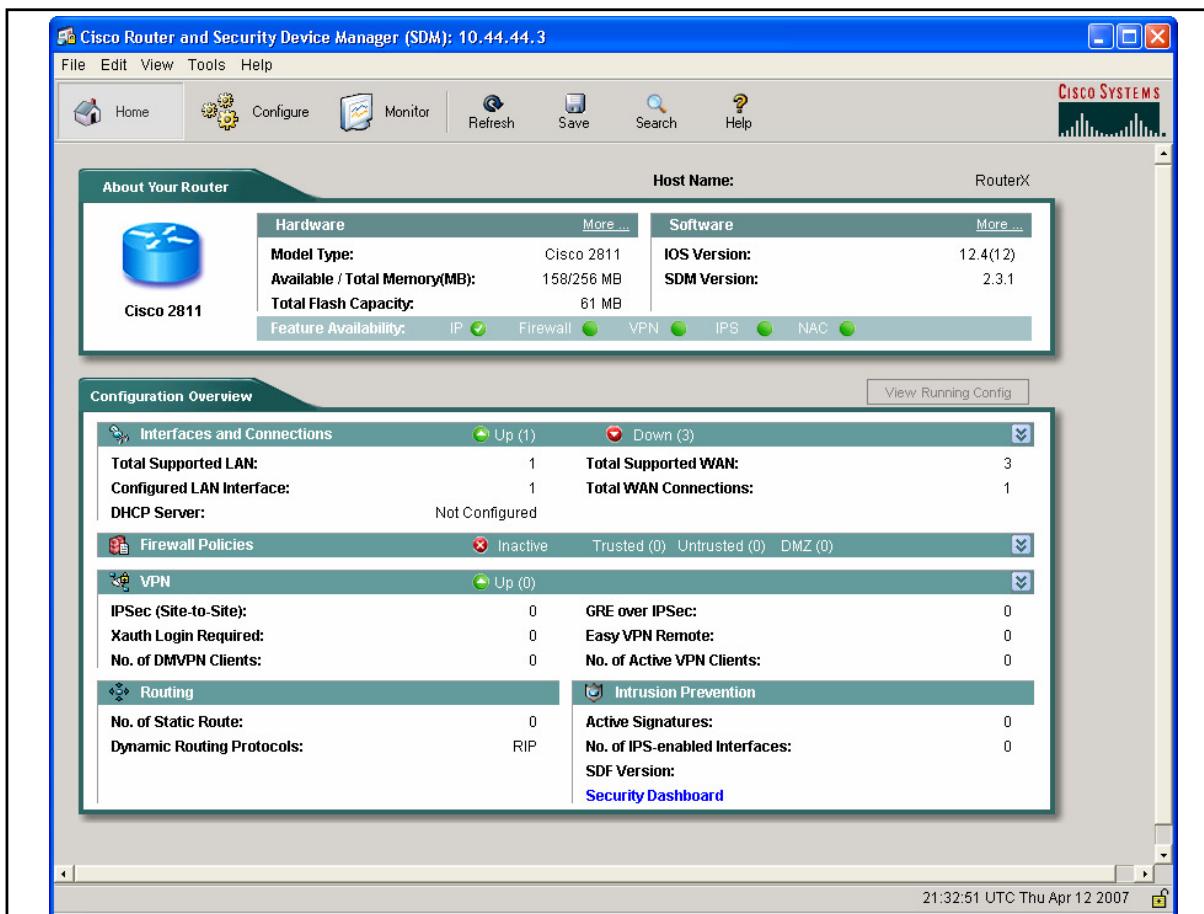
- **Tổng quan**
 - Cisco router và SDM (Security Device Manager) là một công cụ quản lý thiết bị dựa vào Java để sử dụng được thiết kế để cấu hình cho LAN, WAN và các tính năng bảo mật cho router. Bài học mô tả cách sử dụng Cisco SDM
- **Mục tiêu**
 - Cung cấp khả năng mô tả các đặc tính của Cisco SDM qua các nhiệm vụ sau:
 - Mô tả tính năng của Cisco SDM
 - Mô tả các sử dụng các thành phần trong giao diện Cisco SDM

Cisco router và SDM



8-2

- Cisco SDM là một công cụ trực quan để quản lý thiết bị dựa trên giao diện web. Cisco SDM đơn giản hóa việc cấu hình router và các tính năng bảo mật bằng cách sử dụng các wizards cho phép ta nhanh chóng để triển khai, cấu hình và giám sát Cisco router mà không cần phải có các kiến thức cho các câu lệnh ở CLI. Cisco SDM được hỗ trợ trên các dòng router 830, 1700, 1800, 2600XM, 2800, 3600, 3700, 3800, 7200 và 7301



Cisco SDM là gì?

- Một công cụ quản lý nhúng dựa trên web
- Cung cấp những wizard thông minh giúp nhanh chóng và dễ dàng cấu hình mà không cần phải có kiến thức về CLI
- Các công cụ nâng cao cho người dùng
 - ACL editor
 - VPN crypto map editor
 - Cisco IOS CLI preview

8-4

- Cisco SDM cho phép ta dễ dàng cấu hình định tuyến, chuyển mạch, bảo mật hay chất lượng dịch vụ (QoS) trong khi vẫn quản lý thiết bị qua chức năng quan sát. Khi ta triển khai một router mới hay cài đặt Cisco SDM trên một router có sẵn, ta có thể ngay lập tức cấu hình và quan sát những router này từ xa mà không cần dùng đến câu lệnh CLI. Giao diện đồ họa của Cisco SDM giúp cho những người không phải là chuyên gia có thể điều khiển, vận hành thiết bị hàng ngày.
- Wizards thông minh của Cisco SDM hướng dẫn ta từng bước qua việc cấu hình router và các tính năng bảo mật một cách có hệ thống qua việc cấu hình các cổng LAN, WAN, tường lửa, hệ thống ngăn chặn xâm nhập (IPS) hay hệ thống mạng riêng ảo (VPN). Cisco SDM có thể phát hiện các cấu hình không đúng một cách thông minh và đưa ra những đề xuất để chỉnh sửa, ví dụ như cho phép DHCP chạy qua tường lửa nếu như cổng WAN có địa chỉ của DHCP. Tài liệu giúp đỡ trực tuyến bao gồm những thông tin nền tảng và hướng dẫn từng bước để ta có thể đưa vào thông tin một cách chính xác. Những thuật ngữ về mạng, bảo mật và các định nghĩa khác đều được liệt kê trên bảng chú giải trực tuyến.

- Cho những chuyên gia đã quen với hệ điều hành Cisco IOS và các tính năng bảo mật của nó, Cisco SDM mang lại những công cụ cấu hình nâng cao cho phép ta nhanh chóng cấu hình và tinh chỉnh các đặc tính bảo mật trên router và đồng thời cũng cho phép ta xem lại những câu lệnh được sinh ra bởi Cisco SDM trước khi chuyển xuống cho router.
- Cisco SDM giúp ta cấu hình và giám sát router từ xa sử dụng SSL và SSH v2. Công nghệ này giúp ta tạo ra một kênh truyền bảo mật trên Internet giữa trình duyệt của người dùng và router. Khi được triển khai tại văn phòng chi nhánh, router có SDM cho phép ta cấu hình và quan sát chúng từ văn phòng chính, việc này giúp giảm thiểu yêu cầu phải có những người quản trị có kinh nghiệm tại văn phòng chi nhánh.
- Một công cụ quản lý nhúng dựa trên web
- Cung cấp những wizard thông minh giúp nhanh chóng và dễ dàng cấu hình mà không cần phải có kiến thức về CLI

Supported Cisco Routers and Cisco IOS Software Releases

- Cisco SDM được hỗ trợ trên các Cisco router và các hệ điều hành Cisco IOS liên quan.
- Luôn kiểm tra thông tin về Cisco SDM tại địa chỉ <http://www.cisco.com/go/sdm>

8-6

- Cisco SDM được hỗ trợ trên các Cisco router và các hệ điều hành Cisco IOS liên quan.
- Luôn nhớ kiểm tra thông tin về Cisco SDM tại địa chỉ <http://www.cisco.com/go/sdm>
- Cisco SDM được cài đặt sẵn trên một số router sản xuất trong tháng 6 năm 2003 hoặc sau này khi được mua kèm với gói VPN
- Nếu ta có router mà không có Cisco SDM được cài đặt sẵn và ta muốn sử dụng Cisco SDM, ta phải tải về chương trình này tại cisco.com và cài đặt vào router. Chắc chắn rằng router của ta phải có đủ bộ nhớ flash để hỗ trợ thêm các file của SDM. Thông tin để cài đặt SDM cho Cisco router không thuộc phạm vi của khóa học này.

Configuring Your Router to Support SDM

1. Kích hoạt HTTP và HTTPS server trên router.
2. Tạo tài khoản người dùng định nghĩa với đặc quyền mức 15.
3. Cấu hình SSH và Telnet cho việc đăng nhập cục bộ và mức đặc quyền là 15.

8-7

- **Cấu hình router để hỗ trợ Cisco SDM**

- Ta có thể cài đặt và chạy Cisco SDM trên router đang được sử dụng mà không làm ảnh hưởng đến dữ liệu đang chạy trên mạng. Tuy nhiên ta cũng phải đảm bảo rằng đã có một vài thông số có sẵn trong cấu hình.
- Truy xuất vào CLI sử dụng Telnet hoặc qua console để hiệu chỉnh một số cấu hình trước khi cài đặt Cisco SDM trên router

- **Bước 1** Kích hoạt HTTP và HTTPS server trên router bằng các câu lệnh sau:

- Router# configure terminal
- Enter configuration commands, one per line. End with CNTL/Z.
- Router(config)# ip http server
- Router(config)# ip http secure-server
- Router(config)# ip http authentication local
- Router(config)# ip http timeout-policy idle 600 life 86400
- requests 10000

- **Chú ý** Nếu router hỗ trợ HTTPS, HTTPS server sẽ được kích hoạt, nếu không, HTTP server sẽ được kích hoạt. HTTPS được hỗ trợ trên tất cả các hệ điều hành hỗ trợ tính năng IPSec, bắt đầu từ phiên bản 12.25(T).

- **Bước 2** Tạo tài khoản người dùng định nghĩa với đặc quyền mức 15 qua câu lệnh sau:
 - Router(config)# **username username privilege 15 secret 0 password**
 - Ví dụ, cho username là “tomato” và password là “vegetable” ta đưa vào câu lệnh
 - Router(config)# **username tomato privilege 15 secret 0 vegetable**
 - Ta sẽ sử dụng tài khoản này để đăng nhập vào Cisco SDM
- **Bước 3** Cấu hình SSH và Telnet cho việc đăng nhập cục bộ và mức đặc quyền là 15. Sử dụng câu lệnh sau
 - Router(config)# **line vty 0 4**
 - Router(config-line)# **privilege level 15**
 - Router(config-line)# **login local**
 - Router(config-line)# **transport input telnet ssh**
 - Router(config-line)# **exit**

Khởi động SDM



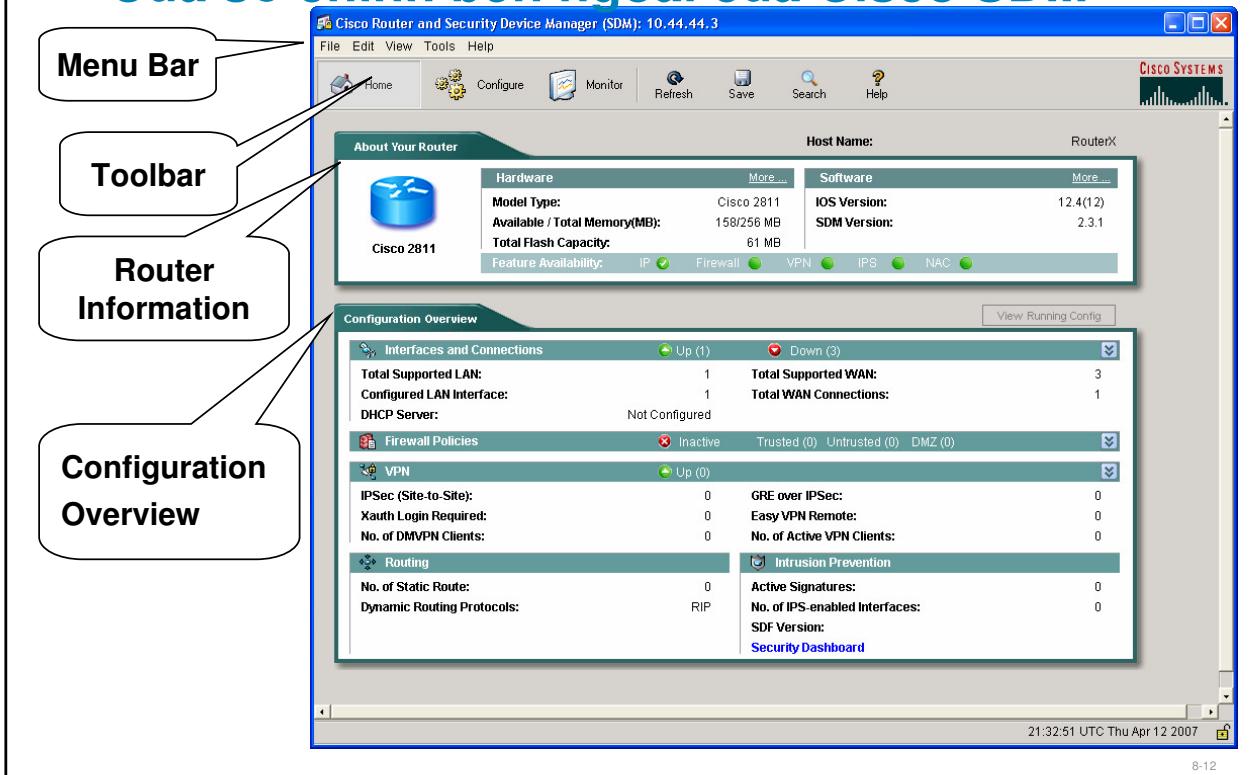
8-9

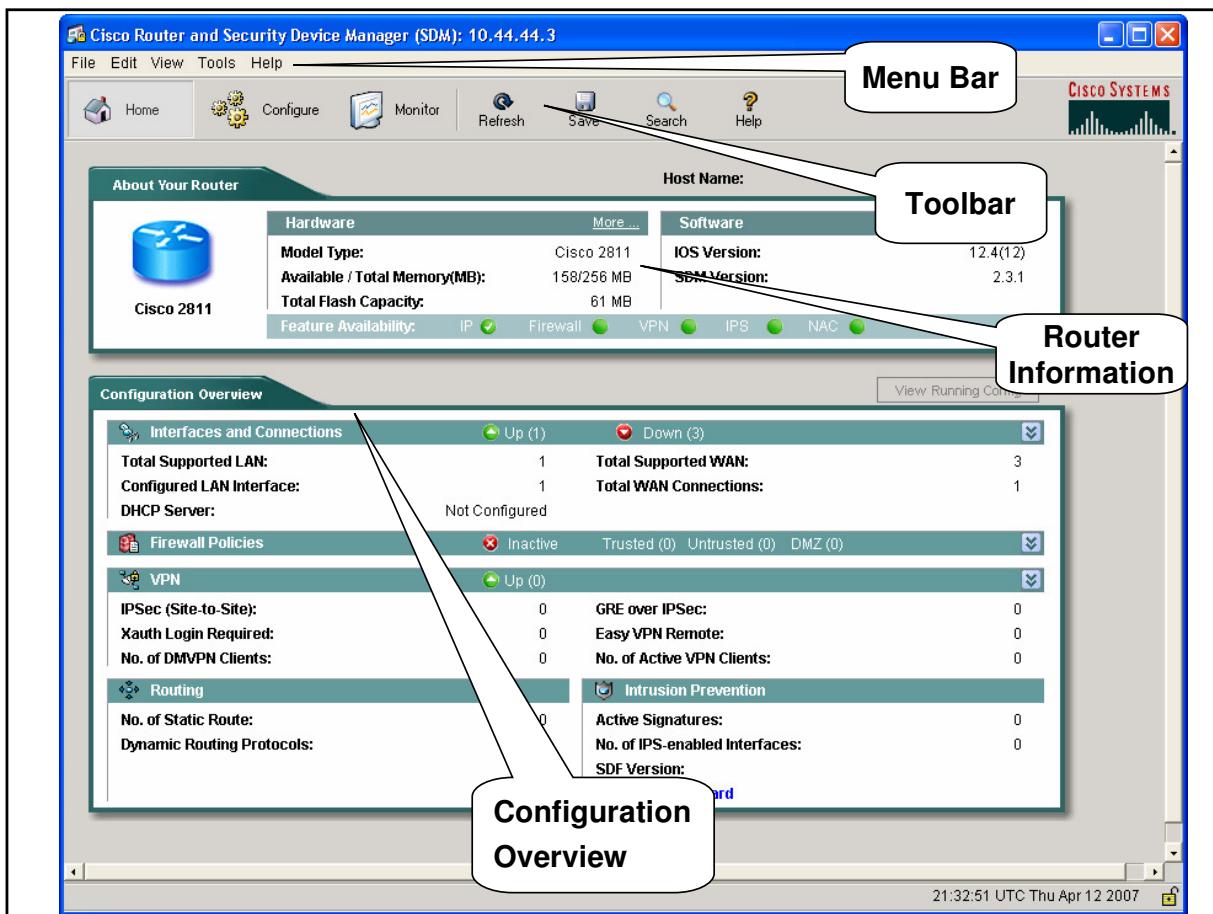
- **Khởi động Cisco SDM**
- Cisco SDM được lưu trong bộ nhớ flash. Nó được gọi bằng cách thực thi một tập tin HTML trên router, sau đó sẽ tải một tập tin Cisco SDM Java đã được đăng ký. Để chạy Cisco SDM, hoàn thành các bước sau:
 - **Bước 1** Từ trình duyệt, nhập vào địa chỉ URL như sau:
 - **https://router IP address**
 - https:// chỉ ra rằng SSL sẽ được sử dụng
 - http:// có thể được sử dụng trong trường hợp không có SSL
 - **Bước 2** Trang chủ của Cisco SDM sẽ xuất hiện trong cửa sổ trình duyệt. Ô hội thoại username và password sẽ hiện ra. Loại và hình dáng của hộp hội thoại sẽ khác nhau tùy thuộc vào trình duyệt sử dụng. Nhập vào username và password ở mức đặc quyền 15 trên router. Java Applet của Cisco SDM sẽ bắt đầu tải về PC từ router.
 - **Bước 3** Cisco SDM là một Java Applet đã được đăng ký. Cái này sẽ làm cho trình duyệt hiện lên một thông tin cảnh báo. Chấp nhận trình Java Applet này.

- **Bước 4** Cisco SDM hiển thị trang Lauch
- Khi cửa sổ Lauch xuất hiện, Cisco SDM hiển thị trang chủ Cisco SDM. Trang chủ này sẽ cung cấp một hình ảnh sơ lược của việc cấu hình và tính năng mà hệ điều hành Cisco IOS hỗ trợ. Cisco SDM bắt đầu với mode Wizard, theo đó ta có thể thực hiện quá trình cấu hình sử dụng thứ tự các cửa sổ xuất hiện để chia nhiệm vụ cấu hình ra thành từng bước có thể quản lý được.



Cửa sổ chính bên ngoài của Cisco SDM





- Trang chủ cung cấp những thông tin cơ bản về phần cứng, phần mềm, cấu hình và bao gồm những phần sau:
- Host Name: Tên cấu hình của router
- About Your Router: Khu vực này thể hiện thông tin phần cứng, phần mềm và các phần khác được thể hiện trong bảng trên
- Hardware
 - Model Type: Thể hiện đời của router
 - Available/ Total Memmory: RAM còn lại để sử dụng và tổng RAM
 - Total Flash Capability Flash cộng với bộ nhớ webflash (nếu có)
- Software
 - IOS version: Phiên bản của hệ điều hành Cisco IOS đang chạy trên router
 - Cisco SDM Version: Phiên bản của Cisco SDM đang chạy trên router
 - Feature Avaiability: Tính năng có sẵn trên hệ điều hành Cisco IOS mà router đang sử dụng. Những đặc tính được kiểm tra đó là IP, tường lửa, VPN, IPS.
- More Link
 - More link hiển thị một cửa sổ pop-up nhằm cung cấp thêm một số thông tin chi tiết cho phần cứng và phần mềm như sau:

- **Hardware Detail:** thể hiện thêm các thông tin đang được thể hiện trong cửa sổ About Your Router, thẻ này hiển thị các thông tin về:
 - Router khởi động từ đâu: flash, hay tập tin cấu hình
 - Router có các phần tăng tốc hay không, ví dụ như phần tăng tốc cho VPN
 - Mô hình cấu hình phần cứng
- **Software Detail:** thể hiện thêm các thông tin đang được thể hiện trong cửa sổ About Your Router, thẻ này hiển thị thông tin về đặc tính trong hệ điều hành Cisco IOS

• Configuration Overview

- Phần này tóm tắt những cấu hình đã được thiết lập. Nếu muốn xem cấu hình đang chạy, nhấp vào View Running Config
- **Interface and Connections**
- Khu vực này thể hiện các thông tin sau
 - Up: Số lượng kết nối đang up
 - Down: Số lượng các kết nối đang down
 - Double Arrow: Nhấp vào để hiển thị hay ẩn đi chi tiết
 - Total Supported LAN: Hiển thị tổng số các cổng LAN hiện diện trên router
 - Total Supported WAN: Hiển thị tổng số các cổng WAN hiện diện trên router
- **Configured LAN Interface:** Số lượng các cổng LAN đã được cấu hình trên
- **Total WAN Connections:** Tổng số lượng kết nối WAN hỗ trợ Cisco SDM hiện diện trên
- **DHCP Server:** Đã hoặc chưa được cấu hình
- **DHCP Pool (Detail View):** Nếu đã có một pool nào đó đã cấu hình, khu vực này sẽ hiển thị địa chỉ đầu và cuối của pool. Nếu có nhiều pool được cấu hình khu vực này sẽ hiển thị danh sách tên các pool được cấu hình
- **Number of DHCP Clients (Detail View):** Các client hiện tại đang sử dụng địa chỉ
- **Interface:** Tên các cổng đã được cấu hình
 - Type: loại cổng
 - IP Mask: địa chỉ IP và subnet mask
 - Description: mô tả cho các cổng
- **Firewall Policies**
- Khu vực này thể hiện các thông tin sau
 - Active: Tường lửa đang vận hành
 - Inactive: Không có tường lửa nào chạy
 - Trusted: Số lượng các cổng được tin cậy (bên trong)
 - Untrusted: Số lượng các cổng không được tin cậy (bên ngoài)
 - DMZ: Số lượng các cổng DMZ

- **Double Arrow:** Nhấp vào để hiện và ẩn chi tiết
- **Interface:** Tên của cổng được áp dụng tường lửa
- **Firewall Icon:** Cổng đang được phân định như là cổng trong hay cổng ngoài
- **NAT:** Số lượng các luật NAT áp dụng trên cổng này
- **Inspection Rule:** Tên hoặc số lượng của các luật inspection chiều bên trong và bên ngoài
- Access Rule: Tên hoặc số lượng các luật truy xuất chiều bên trong và ngoài

- VPN
- **Khu vực này thể hiện các thông tin sau**
- **Up:** Số lượng các kết nối VPN đang tồn tại
- **Double Arrow:** Nhấp vào để hiện hoặc ẩn chi tiết
- **IPSec (Site-to-Site):** Số lượng kết nối VPN site-to-site được cấu hình
- **GRE over IPSec:** Số lượng GRE trên kết nối IPSec
- XAUTH Login Required: Số lượng kết nối của Cisco Easy VPN đang đợi một tiến trình đăng nhập XAUTH
- Chú ý: một số VPN server hoặc Concentrator client sử dụng XAUTH. Phần này thể hiện số lượng các tunnel VPN chờ xác thực XAUTH. Nếu bất kỳ tunnel Cisco Easy VPN nào đang chờ cho tiến trình XAUTH, những cửa sổ thông điệp riêng biệt được thể hiện với nút Login. Nhấp vào Login để được ủy nhiệm vào tunnel
- Chú ý: nếu XAUTH được cấu hình cho tunnel nó sẽ không thể hiện chức năng cho đến khi đăng nhập và password được cung cấp. Không có thời hạn mà XAUTH ngưng chờ.
- Easy VPN Remote: Số lượng kết nối từ xa của Cisco Easy VPN
- No. of DMVPN: Nếu router được cấu hình với DMVPN hub, đây là số lượng DMVPN client
- No. of Active VPN Client: Nếu router được cấu hình như Easy VPN server, đây là số lượng Cisco Easy VPN Client trên những kết nối đang được kích hoạt
- Interface: Tên của Interface được cấu hình kết nối VPN
- IPSec Policy: Tên của chính sách IPSec liên quan đến kết nối VPN

- Routing
- Khu vực này thể hiện các thông tin sau:
- No. of Static Routers: Số lượng tuyến tĩnh được cấu hình trên router
- Dynamic Routing Protocols: Liệt kê bất kỳ một giao thức định tuyến động được cấu hình trên router

- Intrusion Prevention
- Khu vực này bao gồm các thông tin sau:
- Active Signature: Số lượng những signature đang hoạt động mà router sử dụng. Nó có thể là được tích hợp sẵn hoặc được tải từ một nơi nào đó
- **No. of IPS-Enables Interface:** Số lượng các cổng trên router mà IPS được kích hoạt.

Cisco SDM Wizards



- LAN wizard: Được dùng để cấu hình các cổng LAN và DHCP
- WAN wizard: Được sử dụng để cấu hình PPP, FrameRelay, HDLC
- Firewall
- VPN
- Security audit: Thực hiện quá trình giám sát bảo mật trên router
- IPS: Hệ thống ngăn ngừa xâm nhập
- QoS: Chất lượng dịch vụ

8-16

- Cisco SDM chứa một vài wizard tùy chọn được thể hiện như trên:
- LAN wizard: Được dùng để cấu hình các cổng LAN và DHCP
- WAN wizard: Được sử dụng để cấu hình PPP, FrameRelay, HDLC, kiểm tra trên <http://www.cisco.com/go/sdm> để có thông tin mới nhất về các wizard và các cổng được hỗ trợ.
- Firewall wizard:
- VPN wizard
- Security Audit wizard: Có hai tùy chọn
 - The router security audit wizard
 - An easy one-step router security lockdown wizard
- Qos: wizard cho chất lượng dịch vụ
- Chú ý: Tại cuối cùng của mỗi wizard, tất cả sự thay đổi sẽ tự động được phân phối xuống router sử dụng phần tự động phát sinh câu lệnh của Cisco SDM. Ta có thể chọn xem hoặc không xem lại những câu lệnh sẽ được gửi đi. Mặc định sẽ làm không xem lại những câu lệnh này.

The screenshot shows a software interface with a sidebar titled "Tasks" on the left. The sidebar contains nine items, each with an icon and a label:

- Interfaces and Connections
- Firewall and ACL
- VPN
- Security Audit
- Routing
- NAT
- Intrusion Prevention
- Quality of Service
- Additional Tasks

To the right of the sidebar, there is a large white area where a bulleted list of features is displayed:

- LAN wizard: Được dùng để cấu hình các cổng LAN và DHCP
- WAN wizard: Được sử dụng để cấu hình PPP, FrameRelay, HDLC
- Firewall
- VPN
- Security audit: Thực hiện quá trình giám sát bảo mật trên router
- IPS: Hệ thống ngăn ngừa xâm nhập
- QoS: Chất lượng dịch vụ

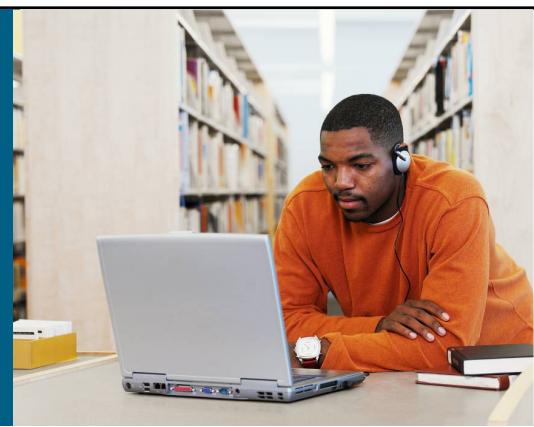
Tóm tắt

- Cisco SDM là công cụ hữu ích để cấu hình ban đầu cho router.
- Cisco SDM bao gồm các wizard dễ dàng sử dụng.
- Cisco SDM cho phép chỉnh những thông số cho các cấu hình nâng cao.



8-19

Bài 9: Sử dụng Cisco Router như một DHCP server



Kết nối LAN

9-1

- **Tổng quan**
 - Ban đầu, người quản trị mạng sẽ cấu hình địa chỉ, giá trị default gateway, hay các thông số mạng khác cho các máy bảng tay. Tuy nhiên DHCP (Dynamic Host Configuration Protocol) sẽ cung cấp các thông số cấu hình cho các host trên Internet. DHCP bao gồm các hai thành phần sau:
 - Giao thức để phân phát những thông số cụ thể cho từng host giữa DHCP server đến DHCP client
 - Phương pháp để cấp phát địa chỉ mạng cho host
 - Bài học sẽ mô tả cách sử dụng Cisco router như DHCP server
- **Mục tiêu**
 - Cung cấp khả năng cấu hình Cisco router như một DHCP server sử dụng Cisco SDM qua các nhiệm vụ sau:
 - Mô tả tính năng của DHCP
 - Mô tả cách sử dụng router như một DHCP server
 - Mô tả cách sử dụng Cisco SDM để kích hoạt chức năng DHCP server trên router
 - Mô tả cách quan sát chức năng của DHCP server

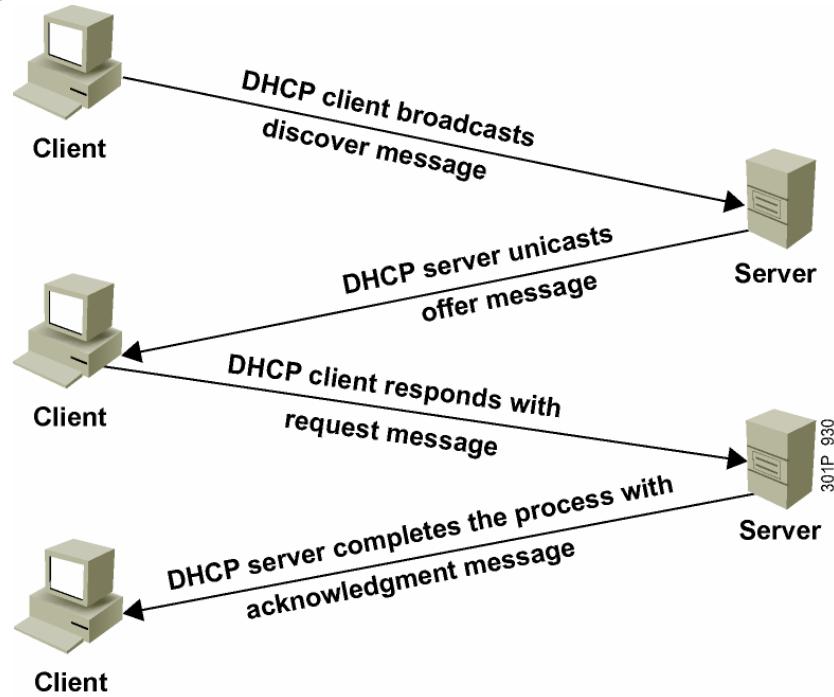
Tìm hiểu về DHCP

- DHCP được xây dựng trên kiến trúc client và server như sau:
 - DHCP server sẽ cấp phát địa chỉ mạng và phân phát thông số cấu hình.
 - Khái niệm client là những host yêu cầu những thông số ban đầu từ DHCP server.
- DHCP hỗ trợ ba phương pháp cấp phát địa chỉ :
 - Cấp phát tự động: DHCP gán một địa chỉ cố định cho client.
 - Cấp phát động: DHCP gán một địa chỉ cho client để sử dụng trong một khoảng thời gian nào đó.
 - Cấp phát bằng tay: địa chỉ IP của client sẽ được gán bởi người quản trị, DHCP chỉ đơn giản được sử dụng để chia địa chỉ được phân định đến client.
- Phương pháp cấp phát động là phương pháp duy nhất cho phép sử dụng lại địa chỉ mà không còn được dùng bởi client nào đó nữa.

9-2

- DHCP được xây dựng trên kiến trúc client và server. Host làm DHCP server sẽ cấp phát địa chỉ mạng và phân phát thông số cấu hình xuống các client. Khái niệm client là những host yêu cầu những thông số ban đầu từ DHCP server.
- DHCP hỗ trợ ba phương pháp cấp phát địa chỉ
- Cấp phát tự động: DHCP gán một địa chỉ cố định cho client
- Cấp phát động : DHCP gán một địa chỉ cho client để sử dụng trong một khoảng thời gian nào đó
- Cấp phát bằng tay : địa chỉ IP của client sẽ được gán bởi người quản trị, DHCP chỉ đơn giản được sử dụng để chia địa chỉ được phân định đến client
- Phương pháp cấp phát động là phương pháp duy nhất cho phép sử dụng lại địa chỉ mà không còn được dùng bởi client nào đó nữa. Phương pháp này hiệu quả để gán địa chỉ cho những client chỉ kết nối vào hệ thống mạng tạm thời hay chia sẻ một pool địa chỉ hạn chế giữa các nhóm client không cần phải có địa chỉ cố định.

DHCP



9-3

• DHCPDISCOVER

- Khi một client bật lên lần đầu, nó sẽ phát ra thông điệp DHCPDISCOVER trên subnet của mình. Bởi vì client không có cách nào biết được subnet nó thuộc về, do vậy DHCPDISCOVER là một all-subnet broadcast (IP đích là 255.255.255.255). Địa chỉ IP nguồn lúc này do chưa có se là 0.0.0.0

• DHCPOFFER

- Một DHCP server nhận được thông điệp DHCPDISCOVER sẽ phản hồi với thông điệp DHCPOFFER chứa cấu hình ban đầu cho client. Ví dụ như địa chỉ IP yêu cầu. Subnet mask và default gateway được chỉ ra trong trường tùy chọn subnet mask, và trường tùy chọn router. Một số thông tin phổ biến khác trong thông điệp DHCPOFFER bao gồm thời gian thuê địa chỉ, thời gian thay mới địa chỉ, địa chỉ server tên miền và tên dịch vụ NetBIOS

• DHCPREQUEST

- Sau khi client nhận được thông điệp DHCPOFFER, nó sẽ phản hồi với thông điệp DHCPREQUEST chỉ ra rằng client dự định sử dụng các thông số trong thông điệp DHCPOFFER nhận được

• DHCPACK

- Sau khi DHCP server nhận được thông điệp DHCPREQUEST, nó sẽ phản hồi thông điệp này với thông điệp DHCPACK và hoàn thành thiến trình DHCP

Sử dụng router như một DHCP server

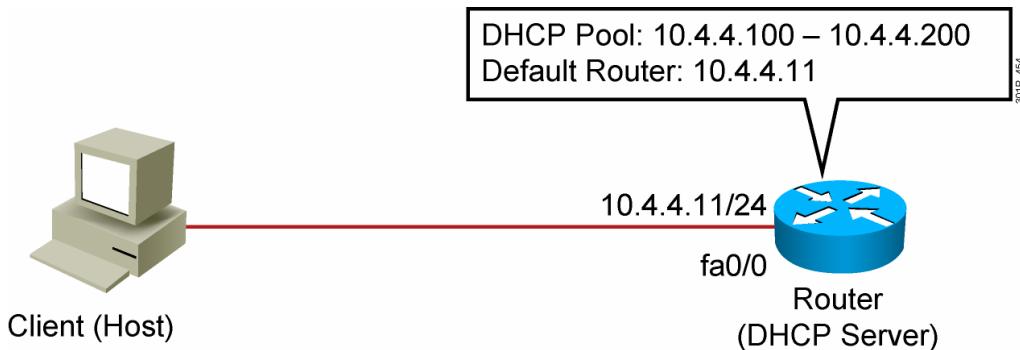
Cisco router với hệ điều hành Cisco IOS cung cấp đủ các tính năng giúp router trở thành một DHCP server :

- Server này có thể cung cấp và quản lý địa chỉ IP từ một pool địa chỉ cụ thể nào đó.
- Ta có thể cấu hình DHCP server để cung cấp thêm một vài thông số :
 - Địa chỉ của DNS server
 - Default router

9-4

- Cisco router với hệ điều hành Cisco IOS cung cấp đủ các tính năng giúp router trở thành một DHCP server. Server này có thể cung cấp và quản lý địa chỉ IP từ một pool địa chỉ cụ thể nào đó. Ta có thể cấu hình DHCP server để cung cấp thêm một vài thông số như địa chỉ của DNS server hay default router
- Cisco Router DHCP server cấp nhận những yêu cầu phân định và làm mới địa chỉ và gán địa chỉ từ những địa chỉ được định nghĩa sẵn trong một pool địa chỉ. Những pool địa chỉ này có thể được cấu hình để cung cấp thêm các thông tin mà client yêu cầu như địa chỉ IP của DNS server, default router, và các thông số khác. Cisco DHCP server có thể chấp nhận broadcast từ đoạn mạng LAN hay yêu cầu DHCP được chuyển tới từ DHCP relay agent

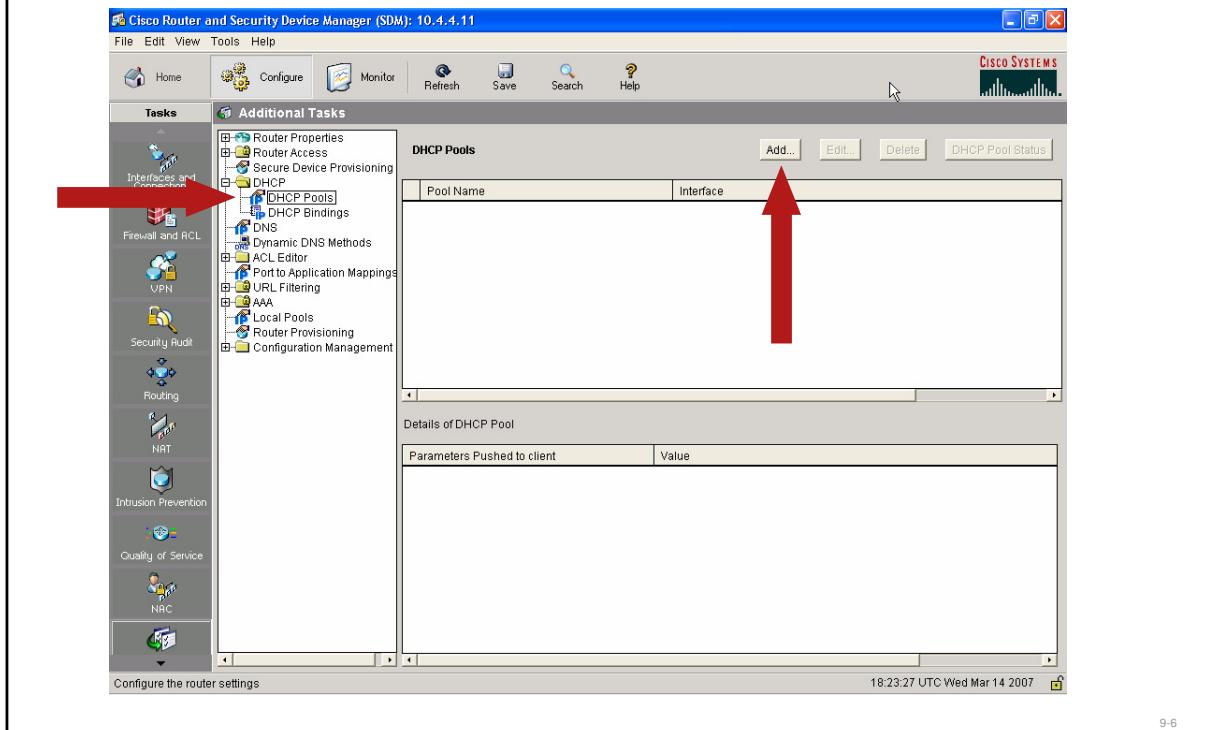
DHCP server sử dụng Router



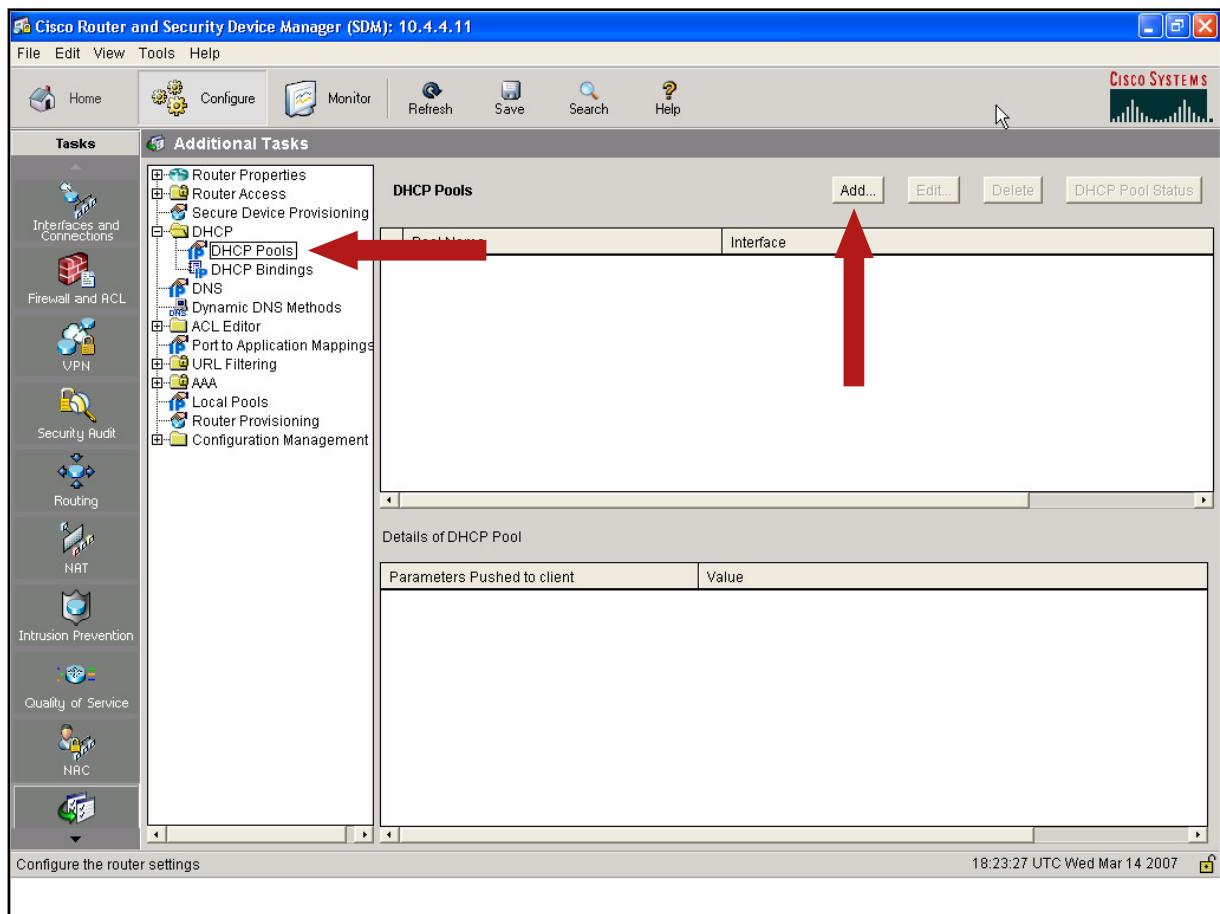
9-5

- Chủ đề này mô tả các sử dụng Cisco SDM để kích hoạt chức năng DHCP server trên router.
- Trong ví dụ này, ta kích hoạt DHCP server trên cổng địa chỉ 10.4.4.11/24 sử dụng pool địa chỉ từ 10.4.4.100 đến 10.4.4.200. Router này sẽ quản lý như là một default router (default gateway của các host)

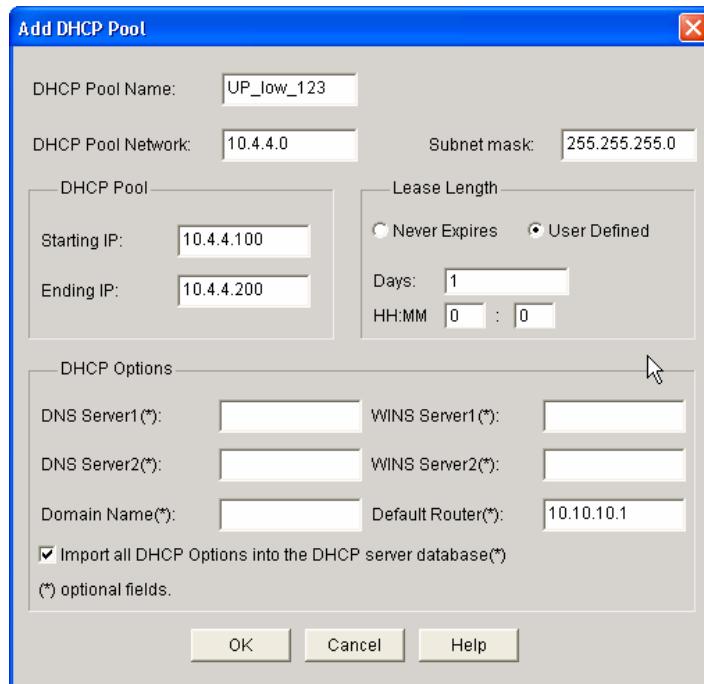
Additional Tasks



- Chức năng cấu DHCP server được kích hoạt dưới thẻ Additional Task. Nhập vào DHCP Pools trong thực mục. Sau đó nhấp vào Add để tạo một pool địa chỉ mới



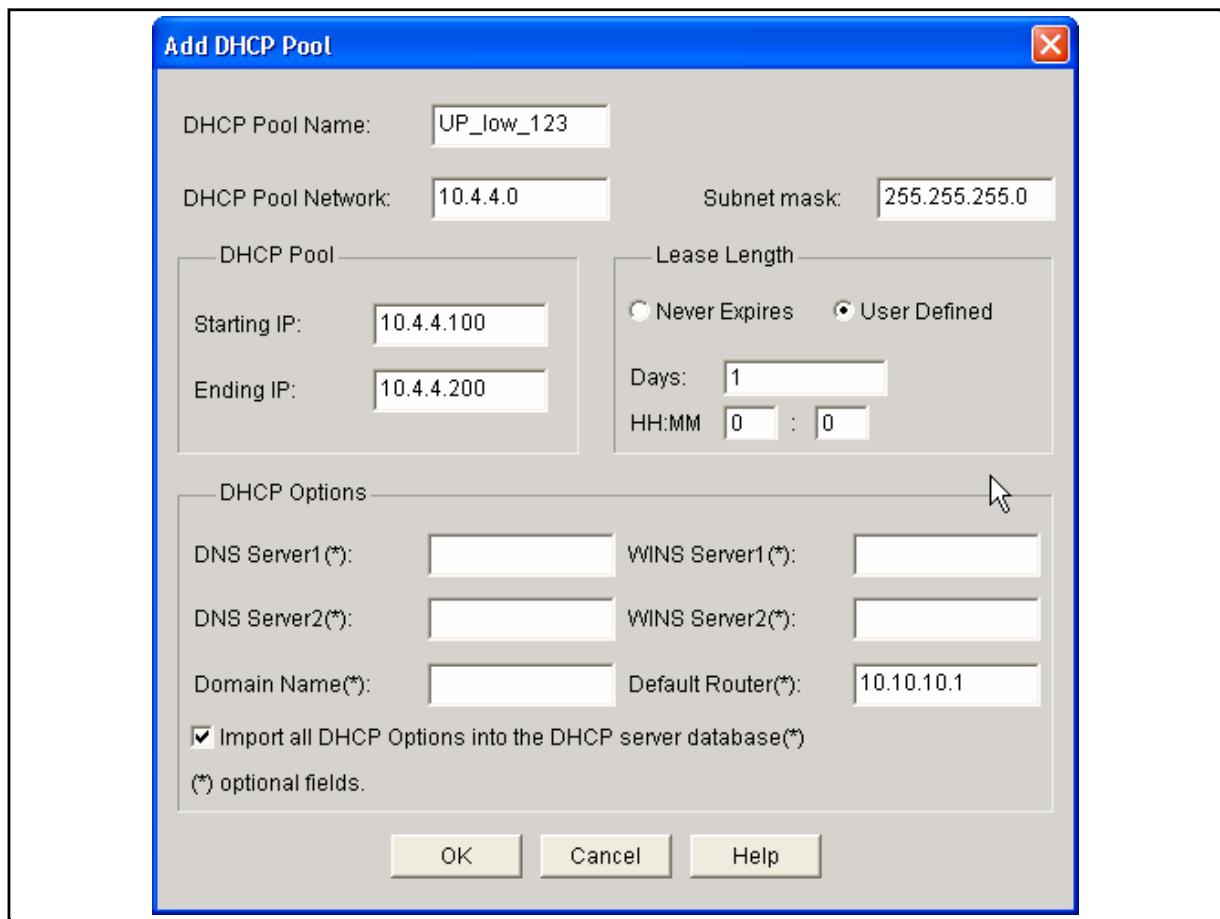
DHCP Pool



9-8

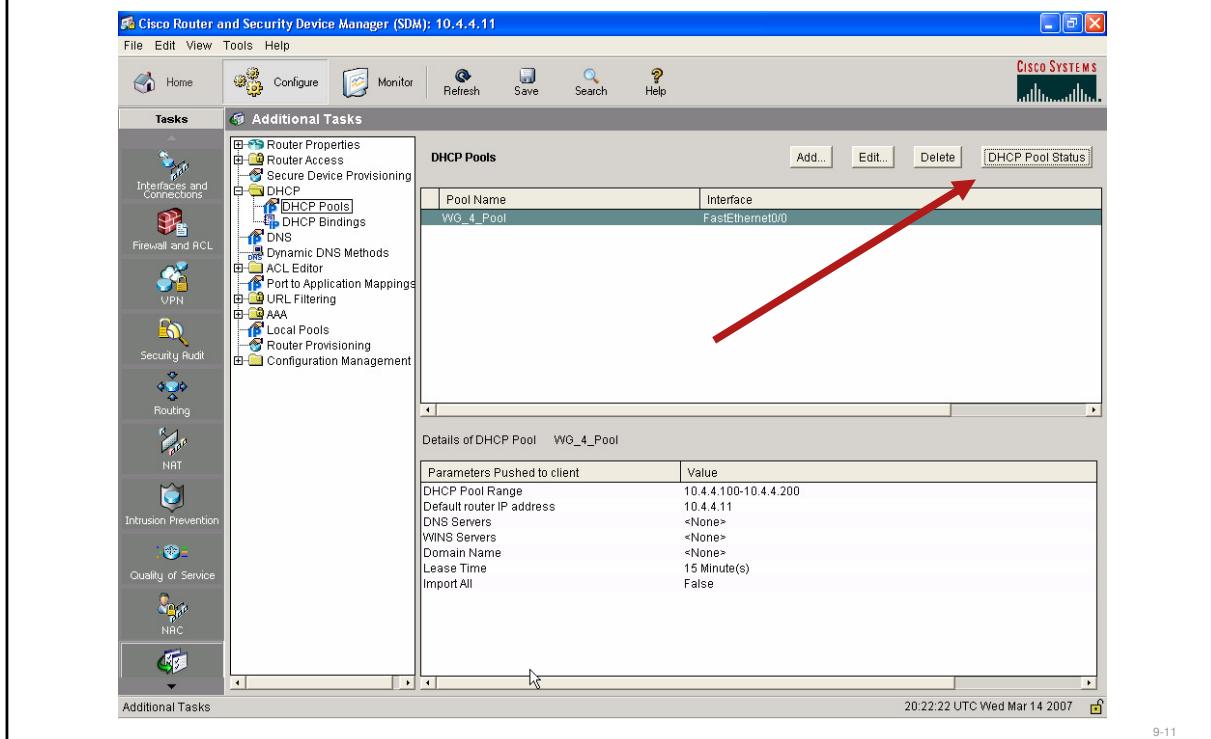
- Cửa sổ Add DHCP Pool cho phép ta cấu hình pool địa chỉ DHCP. Địa chỉ IP mà DHCP server gán sẽ được lấy từ pool địa chỉ được tạo ra bằng dãy địa chỉ bắt đầu và kết thúc. Cửa sổ này thể hiện các trường sau:
 - **DHCP Pool Name:** chuỗi ký tự xác định DHCP pool
 - **DHCP Pool Network và Subnet Mask:** Địa chỉ IP mà DHCP server cấp phát sẽ được lấy từ dãy địa chỉ này
 - Những địa chỉ được chỉ ra nên nằm trong dãy địa chỉ riêng:
 - 10.0.0.0 đến 10.255.255.255
 - 172.16.0.0 đến 172.31.255.255
 - 192.168.0.0 đến 192.168.255.255
 - Dãy địa chỉ được chỉ ra phải nằm trong subnet của cổng LAN. Dãy địa chỉ có thể có tối đa 254 địa chỉ. Những ví dụ sau đây là hợp lệ
 - 10.1.1.1 đến 10.1.1.254 (giả sử địa chỉ mạng LAN thuộc subnet 10.1.1.0)
 - 172.16.1.1 đến 172.16.1.254 (giả sử địa chỉ mạng LAN thuộc subnet 172.16.1.0)
 - Cisco SDM sẽ cấu hình để router tự động trừ đi địa chỉ cổng LAN trong pool
 - Không được sử dụng những địa chỉ để dành sau trong dãy địa chỉ
 - Địa chỉ Network hoặc địa chỉ subnet
 - Địa chỉ broadcast
- **Starting IP:** Nhập vào địa chỉ IP bắt đầu của dãy địa chỉ, đây là địa chỉ nhỏ nhất trong dãy
- **Ending IP:** Nhập vào địa chỉ IP cuối của dãy địa chỉ, đây là địa chỉ lớn nhất trong dãy.

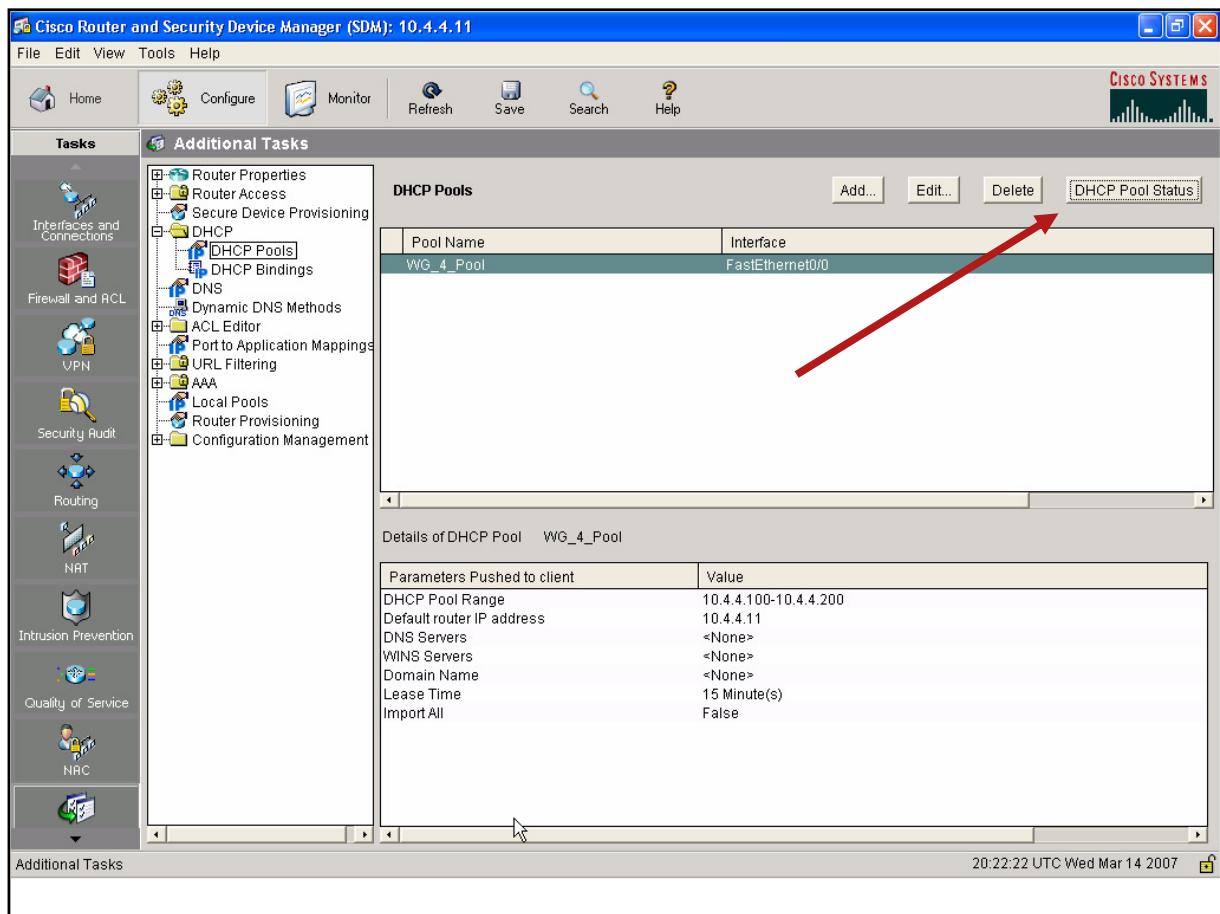
- **Lease Length:** Thời gian client sử dụng địa chỉ được phân định trước khi xin địa chỉ mới
- **DHCP Options:** Sử dụng ô này để cấu hình các tùy chọn DHCP sẽ được gửi đến các host trên LAN
- **DNS Server1:** Nhập vào địa chỉ của DNS server, đây là server có chức năng chuyển đổi tên miền thành địa chỉ IP
- **DNS Server2:** Nếu có thêm DNS server trên mạng ta có thể đưa thêm địa chỉ DNS server này vào đây
- **Domain Name:** Tên của miền hệ thống mạng
- **WINS Server1:** Một số client sẽ yêu cầu Microsoft WINS để kết nối vào các thiết bị trên Internet, đây chính là địa chỉ của WINS server
- **WINS Server2:** Địa chỉ thứ 2 của WINS server
- **Default Router:** Địa chỉ IP được cung cấp cho client sử dụng như default gateway
- **Import All DHCP Options into the DHCP Server Database:** Check box này cho phép cá tùy chọn DHCP sẽ được đưa vào từ server cấp cao hơn và hay được sử dụng trong kết nối với DHCP server trên Internet



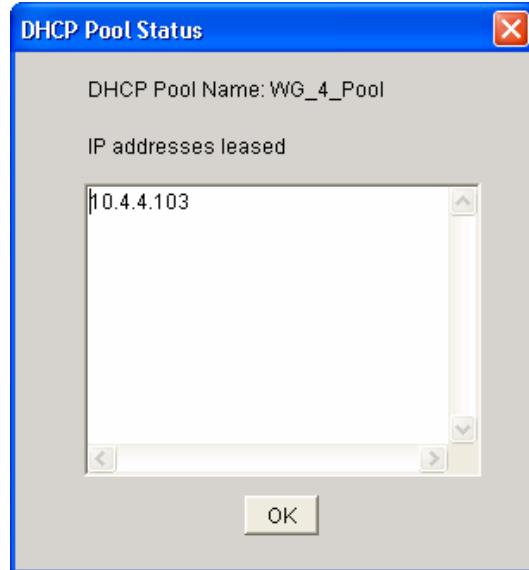
- Ta có thể kiểm tra các thông số cấu hình DHCP từ thẻ DHCP pool. Ta cũng có thể xem thêm một số thông tin cho những địa chỉ đang được dùng bằng cách nhập vào DHCP Pool Status.

Kiểm tra cấu hình DHCP





Trạng thái DHCP Pool



9-13

- Cửa sổ DHCP Pool Status thể hiện danh sách các địa chỉ đang được sử dụng

DHCP Pool Status



DHCP Pool Name: WG_4_Pool

IP addresses leased

10.4.4.103



OK

show ip dhcp conflict

```
RouterX# show ip dhcp conflict
```

IP address	Detection Method	Detection time
172.16.1.32	Ping	Feb 16 2007 12:28 PM
172.16.1.64	Gratuitous ARP	Feb 23 2007 08:12 AM

9-15

- Để hiển thị những địa chỉ bị tranh chấp bởi DHCP server khi địa chỉ được cho các client, sử dụng câu lệnh **show ip dhcp conflict**.
- Server sẽ dùng ping để kiểm tra tranh chấp. Client sử dụng gratuitous ARP để phát hiện. Nếu quá trình tranh chấp địa chỉ được phát hiện, địa chỉ sẽ bị xóa khỏi pool và địa chỉ sẽ không được phân định cho đến khi người quản trị giải quyết vấn đề tranh chấp này
- Ví dụ sau hiển thị phương pháp và thời gian phát hiện cho tất cả các địa IP mang lại bởi DHCP server có tranh chấp với các thiết bị khác

- Router# show ip dhcp conflict
- IP address Detection Method Detection time
• 172.16.1.32 Ping Feb 16 1998 12:28 PM
• 172.16.1.64 Gratuitous ARP Feb 23 1998 08:12 AM

- Mô tả câu lệnh**

- IP address: Địa chỉ IP của những host được ghi lại trên DHCP server.
- The Detection Method: Cách mà địa chỉ của host được tìm thấy trên DHCP server, có thể là do ping hay gratuitous ARP.
- Detection time: Ngày giờ phát hiện tranh chấp

Tóm tắt

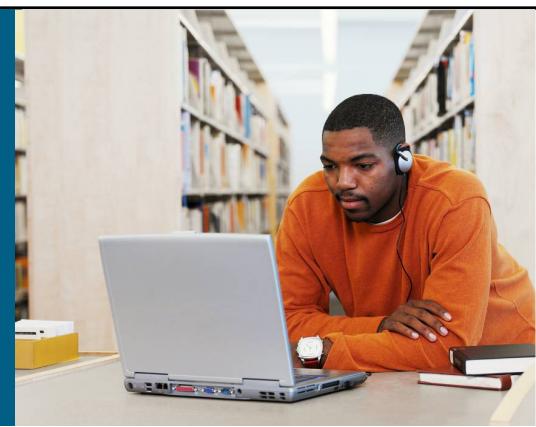
- DHCP được xây dựng trên kiến trúc client và server như sau.
- DHCP server sẽ cấp phát địa chỉ mạng và phân phát thông số cấu hình.
- Hệ điều hành Cisco IOS bao gồm chức năng DHCP server.
- Có thể sử dụng Cisco SDM để cấu hình DHCP server trên router.
- Các bước cần cấu hình như sau:
 - Tên Pool
 - Pool network and subnet
 - Địa chỉ bắt đầu và kết thúc
- Cisco SDM có thể được sử dụng để quan sát DHCP server trên router.
- Câu lệnh **show ip dhcp conflict** dùng để tìm tranh chấp về địa chỉ

9-16



9-17

Bài 10: Truy xuất vào các thiết bị từ xa

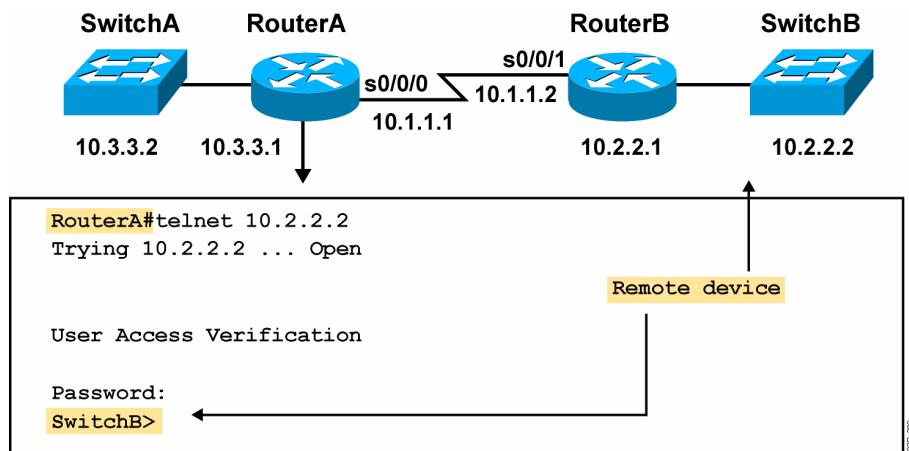


Kết nối LAN

10-1

- **Tổng quan**
 - Trong suốt quá trình duy trì hệ thống, có đôi khi ta phải truy xuất vào một thiết bị từ thiết bị khác. Cisco IOS cung cấp một bộ công cụ cho mục đích này. Bài học mô tả phương pháp có thể sử dụng để truy xuất vào thiết bị từ xa
- **Mục tiêu**
 - Cung cấp khả năng sử dụng các cung cụ hệ điều hành Cisco IOS để truy xuất vào thiết bị từ xa qua các nhiệm vụ sau:
 - Sử dụng Telnet và SSH để kết nối vào thiết bị từ xa
 - Tạm treo và cách quay lại một phiên giao dịch Telnet
 - Đóng phiên giao dịch Telnet
 - Sử dụng câu lệnh Cisco IOS để kiểm tra kết nối

Sử dụng Telnet để kết nối đến thiết bị từ xa



© 2007 Cisco Systems, Inc. All rights reserved.

10-2

- Ứng dụng Telnet hay SSH rất hữu ích cho việc kết nối đến thiết bị từ xa. Chủ đề này mô tả Telnet và SSH, đồng thời giải thích các để thiết lập một kết nối từ xa.
 - Một cách để lấy thông tin của thiết bị từ xa là kết nối với nó qua ứng dụng Telnet hay SSH. Telnet và SSH là một giao thức đầu cuối ảo nằm trong một phần của bộ giao thức TCP/IP. Các giao thức này cho phép kết nối từ một thiết bị mạng đến một hay nhiều các thiết bị từ xa khác.

- Telnet

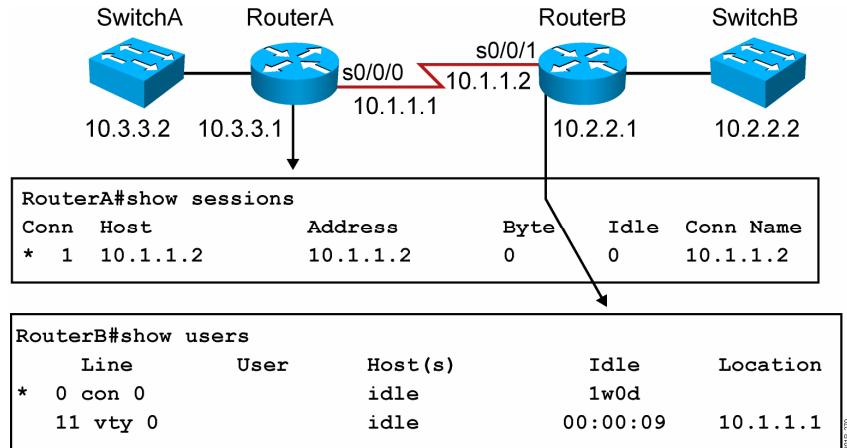
Để truy xuất vào một host hỗ trợ Telnet, sử dụng câu lệnh **telnet**.

telnet host

Mô tả cú pháp

host tên hay địa chỉ IP

Xem kết nối Telnet



© 2007 Cisco Systems, Inc. All rights reserved.

10-3

- **SSH**

- Để khởi tạo một phiên giao dịch mã hóa với thiết bị mạng từ xa, sử dụng câu lệnh `ssh`

`ssh {ipaddr | hostname} [command]`

- **Mô tả cú pháp**

Ipaddr | hostname

Chỉ ra địa chỉ hay tên của thiết bị

muốn truy xuất

- Với hệ điều hành Cisco IOS trên router, địa chỉ IP hay tên của thiết bị cần truy xuất là tất cả để thiết lập nên phiên giao dịch. Câu lệnh `telnet` đặt trước địa chỉ IP hay tên đích. Một khi đã đăng nhập được vào thiết bị từ xa, dấu nhắc console sẽ chỉ ra thiết bị nào đang được cấu hình. Dấu nhắc console chính là tên thiết bị.
- Sử dụng câu lệnh `show sessions` trên router ban đầu để kiểm tra các kết nối Telnet và để hiển thị danh sách các host hiện đang thiết lập kết nối. Câu lệnh này hiển thị tên, địa chỉ IP, số lượng byte, thời gian thiết bị tạm ngưng và tên kết nối của phiên giao dịch. Nếu có nhiều tiến trình phiên giao dịch, dấu * chỉ ra phiên giao dịch nào là cuối cùng và đó sẽ là phiên giao dịch mà router sẽ quay lại khi nhấn `enter`.

Xem kết nối SSH

```
RouterB# show ssh
```

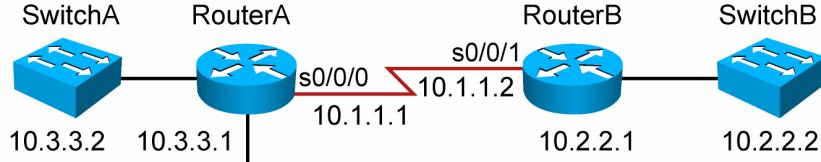
Connection	Version	Encryption	State	Username
0	1.5	3DES	Session Started	guest

© 2007 Cisco Systems, Inc. All rights reserved.

10-4

- Ở hình trên, sử dụng câu lệnh show session trên routerA, phần xuất ra chỉ ra rằng routerA có treo một kết nối với routerB. Sau đó câu lệnh **show users** trên routerB sẽ xác định phiên giao dịch cuối cùng đang được kích hoạt. Phần xuất ra nói rằng người dùng đã có kết nối vào cổng console là phiên giao dịch cuối cùng đang được kích hoạt.
- Dùng câu lệnh **show users** để xem cổng console hiện có đang được kích hoạt và để liệt kê tất cả những phiên giao dịch Telnet bằng địa chỉ IP hay IP alias của thiết bị tạo ra kết nối đến thiết bị này. Trong phần hiện ra của **show users**, dòng “con” hiển thị cổng console và dòng “vty” hiển thị kết nối từ xa. Số “11” ngay tại vty chỉ ra số line, không phải số cổng. Nếu có nhiều người dùng, dấu * chỉ ra kết nối của người dùng cuối cùng.
- Để hiển thị trạng thái của kết nối SSH server, dùng câu lệnh **show ssh** tại mode đặc quyền

Treo và quay lại một phiên Telnet



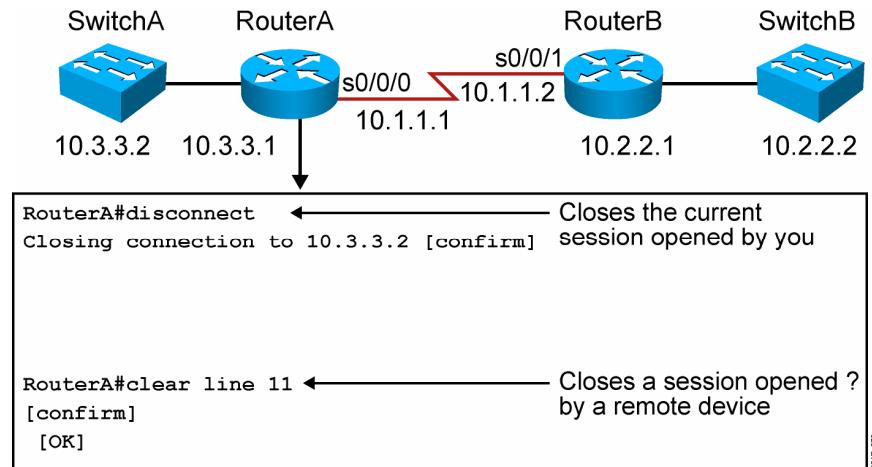
```
RouterB#<Ctrl-Shift-6>x
RouterA#show sessions
Conn Host Address Byte Idle Conn Name
* 1 10.1.1.2 10.1.1.2 0 1 10.1.1.2
RouterA#resume 1
RouterB#
```

© 2007 Cisco Systems, Inc. All rights reserved.

10-5

- Một khi đã kết nối vào thiết bị từ xa, ta có thể muốn quay về lại thiết bị của mình mà không phải ngắt kết nối. Telnet cho phép ta tạm thời treo kết nối và có thể dùng để quay lại sau.
- Chủ đề này mô tả cách để treo một kết nối và quay lại kết nối đó.
- Hình trên hiển thị phiên Telnet từ routerA đến routerB. Tổ hợp phím trên được nhập vào để treo một kết nối. Dấu nhắc chỉ ra rằng ta đã quay về thiết bị của mình và kết nối đã tạm thời được treo.
- Để treo một kết nối như vậy, sử dụng tổ hợp phím sau: **Ctrl-Shift-6** hay **Ctrl-^** (tùy vào bàn phím) theo sau là phím **x**.
- Phương pháp để thiết lập lại kết nối:
Nhấn **Enter**
Nhập lệnh **resume** nếu chỉ có duy nhất một phiên Telnet
Nhập lệnh **resume session number** để quay lại một phiên Telnet cụ thể

Đóng một phiên Telnet



© 2007 Cisco Systems, Inc. All rights reserved.

10-6

- Ta có thể kết thúc phiên Telnet bằng các câu lệnh **exit**, **logout**, **disconnect**, hay **clear**. Chủ đề này mô tả các cách khác nhau để đóng một phiên Telnet
- Ta có thể đóng một phiên Telnet bằng một trong các cách sau:
Từ thiết bị từ xa, dùng câu lệnh **exit** hay **logout** để trở về thiết bị của mình và ngắt kết nối với thiết bị từ xa
Từ thiết bị của mình, dùng câu lệnh **disconnect**, khi có nhiều phiên Telnet, ta phải chỉ ra *session number* sau câu lệnh này.
- Để đóng một phiên telnet truy xuất vào từ thiết bị khác, dùng câu lệnh **clear line line number**, line này tương ứng với số line vty đang được truy xuất vào. Cuối của câu lệnh này, người dùng sẽ thấy một thông báo “closed by a foreign host”

Sử dụng câu lệnh ping và traceroute

```
RouterX#ping 10.1.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

RouterX#trace 192.168.101.101
Type escape sequence to abort.
Tracing the route to 192.168.101.101

 1 p1r1 (192.168.1.49) 20 msec 16 msec 16 msec
 2 p1r2 (192.168.1.18) 48 msec * 44 msec
RouterX
```

Kiểm tra kết nối và đường truyền

© 2007 Cisco Systems, Inc. All rights reserved.

10-7

- Câu lệnh **ping** và **trace** cung cấp thông tin về kết nối và đường truyền. Chủ đề này mô tả cách sử dụng câu lệnh **ping** và **traceroute**.
- Câu lệnh **ping** dùng kiểm tra kết nối mạng, ping báo cho ta biết thời gian tối thiểu, trung bình và tối đa để gửi gói dữ liệu thăm dò đi và về. Điều này có thể dùng để đo độ tin cậy đến một hệ thống nào đó.
- Bảng sau liệt kê các trường hợp có thể có của câu lệnh **ping**
- **Mô tả đặc tính**
 - ! Nhận được gói phản hồi
 - . Hết thời gian chờ gói dữ liệu phản hồi
 - U Đích đến không thể với tới
 - Q Đích đến quá bận
 - M Không thể phân đoạn Could not fragment
 - ? Không hiểu loại gói dữ liệu
 - & Quá thời gian sống của gói dữ liệu

- Câu lệnh **traceroute** hiển thị những tuyến thực sự mà gói dữ liệu đã dùng giữa các thiết bị mạng. Một thiết bị, như router hay switch gửi ra một gói UDP đến một port không có giá trị tại thiết bị từ xa. Có ba gói được gửi ra, mỗi gói với giá trị TTL = 1. Điều này sẽ làm cho các gói sẽ bị hết thời gian sống khi tới router đầu tiên trên đường truyền. Router sau đó sẽ phản hồi một ICMP với TEM (Time Exceeded Message) chỉ ra rằng những gói này đã hết hạn.
- Ba gói UDP khác sẽ lại được gửi ra với TTL = 2 khiến cho router thứ 2 sẽ gửi về ICMP TEM. Tiến trình này sẽ tiếp tục cho đến khi các gói với về được đích. Thông điệp ICMP Port Unreachable sẽ được nhận để báo rằng quá trình đã hoàn thành. Mục tiêu là nhằm ghi lại của mỗi ICMP TEM để cung cấp vết của một con đường gói dữ liệu phải đi để với về đích.
- Bảng dưới liệt kê các đặc tính xuất hiện trong câu lệnh **traceroute**.
- **Mô tả đặc tính**

• nn	mili giây, chỉ ra thời gian đi và về của gói thăm dò
• *	Hết thời gian chờ gói thăm dò
• A	Bị cấm bởi người quản trị (ví dụ như bởi access-list)
• Q	Dích đến quá bận
• I	Bị thử can thiệp bởi người dùng
• U	Port không với tới được
• H	Host không với tới được
• N	Mạng không với tới được
• P	Giao thức không với tới được
• T	Hết giờ
• ?	Không hiểu loại gói
- **Chú ý** Nếu chức năng tìm tên miền được kích hoạt, router sẽ cố gắng phân giải mỗi địa chỉ IP thành tên, và có thể làm cho câu lệnh của chúng ta chậm lại.

Tóm tắt

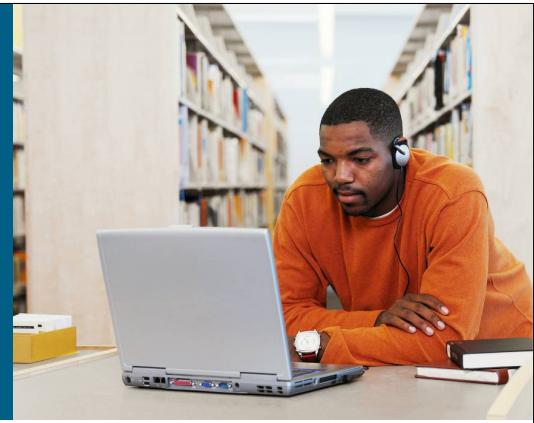
- Một khi đã kết nối vào thiết bị từ xa, ta có thể muốn quay về lại thiết bị của mình mà không phải ngắt kết nối. Telnet cho phép ta tạm thời treo kết nối đó và có thể quay lại sau.
- Ta có thể kết thúc phiên Telnet bằng các câu lệnh **exit**, **logout**, **disconnect**, hay **clear**.
- Câu lệnh **ping** và **trace** cung cấp thông tin về kết nối và đường truyền.



© 2007 Cisco Systems, Inc. All rights reserved.

10-10

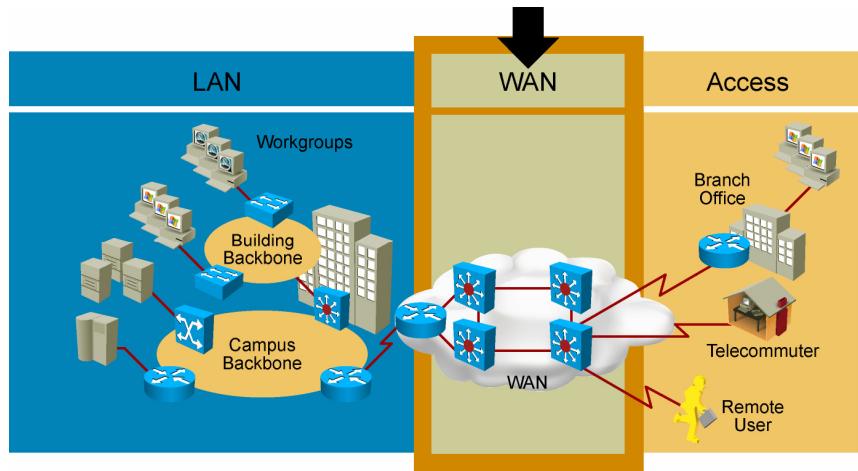
Bài 11: Hiểu về các công nghệ mạng diệu rộng



Kết nối mạng diệu rộng

12-1

Mạng diện rộng



11-2

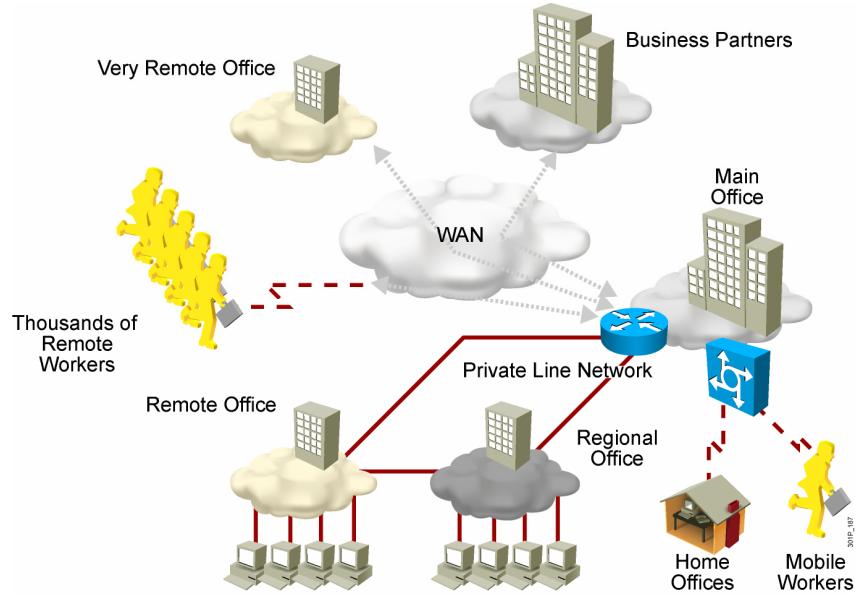
Mạng diện rộng là một mạng truyền dữ liệu mà hoạt động trên một phạm vi địa lý rộng. Phần này mô tả các đặc điểm của mạng này.

Mạng diện rộng sử dụng cơ sở được cung cấp bởi các nhà cung cấp dịch vụ như công ty điện thoại hoặc công ty cáp. Chúng kết nối các vị trí của đơn vị lại với nhau, kết nối từ vị trí của đơn vị này với đơn vị khác, kết nối tới các dịch vụ bên ngoài hoặc tới các người sử dụng từ xa. Mạng diện rộng nói chung mang nhiều kiểu dữ liệu khác nhau như thoại, dữ liệu và hình ảnh.

Có ba đặc điểm chính của mạng diện rộng:

- Mạng diện rộng kết nối các thiết bị mà cách ly nhau bởi vùng địa lý rộng
- Mạng diện rộng sử dụng dịch vụ của nhà cung cấp đường truyền, như công ty điện thoại, công ty truyền hình cáp, hệ thống vệ tinh và các nhà cung cấp dịch vụ mạng
- Mạng diện rộng sử dụng kết nối serial của vài kiểu khác nhau để kết nối vào hệ thống dịch vụ đường truyền

Sự cần thiết của mạng điện rộng



11-3

Các công nghệ mạng cục bộ cung cấp cả về tốc độ và hiệu quả cho việc truyền dữ liệu trong một đơn vị mà trong một vùng địa lý tương đối nhỏ. Tuy nhiên có những nhu cầu công việc khác cần thông tin với những người sử dụng từ xa, như:

- Nhân viên làm việc tại các chi nhánh của đơn vị cần trao đổi và chia sẻ thông tin.
- Đơn vị có khi cần chia sẻ thông tin với các đơn vị khác qua khoảng cách xa. Ví dụ: nhà máy phân mềm thường xuyên thông tin về sản phẩm và chương trình khuyến mãi tới các đơn vị phân phối mà bán sản phẩm của họ tới người sử dụng.
- Nhân viên mà thường xuyên phải đi công tác xa cần truy cập thông tin nằm bên trong đơn vị

Thêm vào đó, người làm việc tại nhà cần gửi nhận dữ liệu qua một khoảng cách lớn, ví dụ:

- Nhiều gia đình hiện nay liên lạc qua máy tính với ngân hàng, siêu thị và các người cung cấp hàng hóa và dịch vụ.
- Sinh viên nghiên cứu truy nhập thư viện và nhà xuất bản ở mọi nơi trên thế giới

Rõ ràng khó có khả năng kết nối các máy tính trên khắp thế giới qua các cáp, do đó nhiều công nghệ khác nhau đã tham gia hỗ trợ cho nhu cầu này. Mạng điện rộng cho phép các đơn vị và cá nhân giải quyết nhu cầu thông tin trên những vùng rộng lớn.

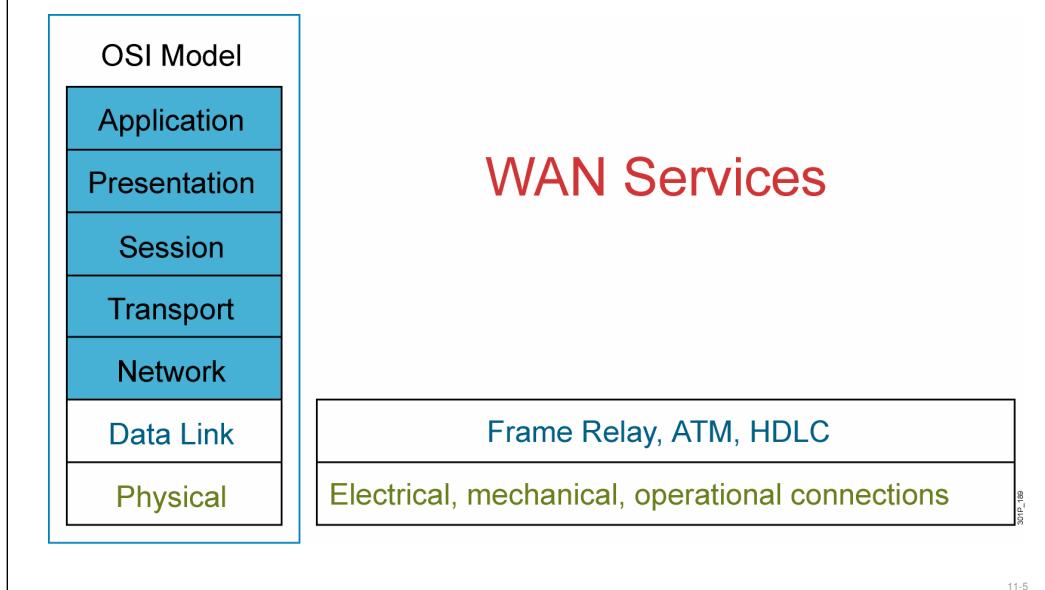
Mạng diện rộng và mạng cục bộ

	WANs	LANs
Area	Wide geographic area	Single building or small geographic area
Ownership	Subscription to outside service provider	Owned by Organization

11-4

Mạng cục bộ kết nối các máy tính, thiết bị ngoại vi, và các thiết bị khác trong một tòa nhà hoặc trong vùng địa lý nhỏ. Mạng diện rộng cho phép truyền dữ liệu qua những khoảng cách địa lý rộng hơn. Hơn nữa, một công ty hay đơn vị phải là một thuê bao của một nhà cung cấp dịch vụ mạng diện rộng để sử dụng dịch vụ truyền dẫn của nó. Trong khi, mạng cục bộ nói chung được sở hữu bởi công ty hay đơn vị sử dụng nó.

Mạng điện rộng tương ứng với mô hình tham khảo OSI



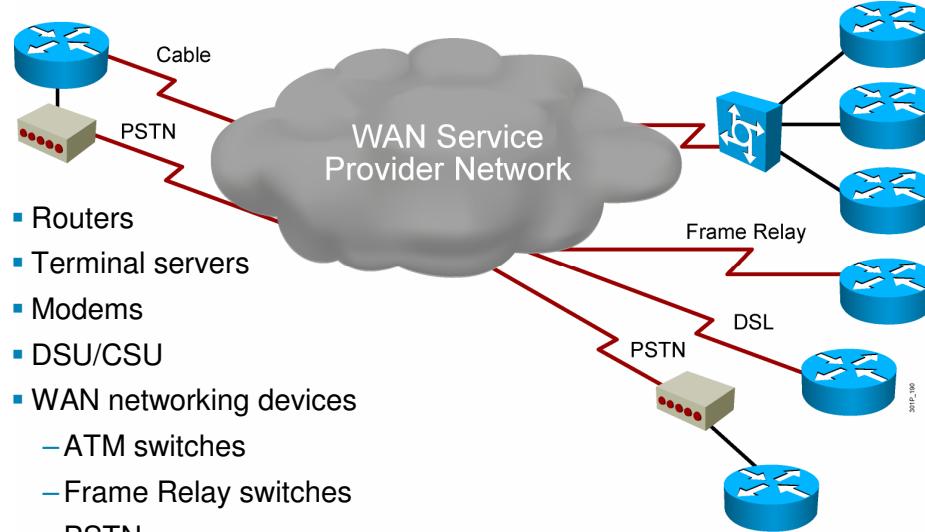
11-5

Các chuẩn truy nhập thường mô tả các phương thức trao đổi lớp vật lý và các yêu cầu ở lớp liên kết dữ liệu như địa chỉ vật lý, kiểm soát dòng, và đóng gói. Các chuẩn truy cập mạng điện rộng được định nghĩa và quản lý bởi vài tổ chức có thẩm quyền như ISO, TIA và EIA.

Các giao thức lớp vật lý (1) mô tả các đặc điểm về điện tử, các cơ chế, các vận hành và chức năng của kết nối tới các dịch vụ của nhà cung cấp.

Các giao thức lớp liên kết dữ liệu (2) định nghĩa làm thế nào để dữ liệu được đóng gói để truyền tới đầu bên kia và cơ chế để truyền các gói trả về. Có nhiều công nghệ được sử dụng, như Fram Relay và ATM. Một số trong các giao thức đó sử dụng cơ chế đóng khung cơ bản giống nhau, đó là HDLC, một chuẩn ISO hoặc các biến thể của nó.

Thiết bị cho mạng diện rộng

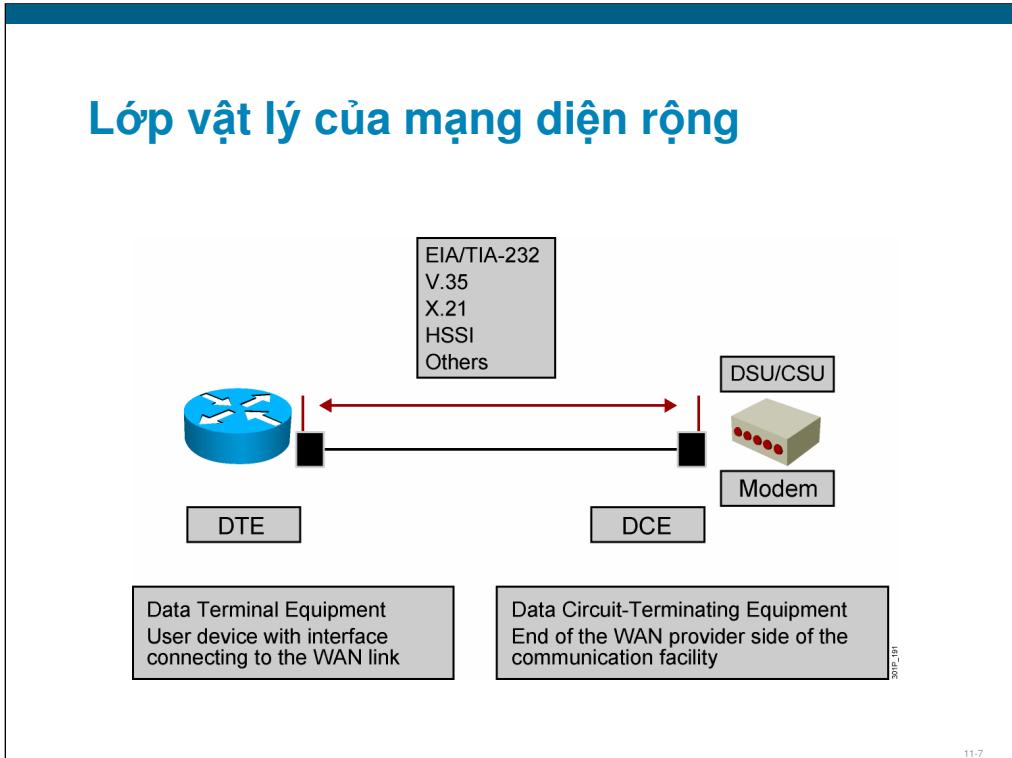


11-6

Các thiết bị sau đây thường được sử dụng để truy cập mạng diện rộng:

- Router: Cung cấp kết nối liên mạng và cổng truy cập mạng diện rộng
- Communication servers: Tập trung các cuộc gọi vào và ra từ người sử dụng truy cập từ xa.
- Modem hoặc DSU/CSU: Trong các đường truyền analog, modem chuyển tín hiệu số thành tín hiệu analog để truyền trên đường analog sau đó được chuyển ngược lại ở modem nhận, trước khi gởi tới thiết bị nhận. Trong các đường truyền digital, DSU/CSU được sử dụng và có thể được hiện thực bên trong các thẻ giao tiếp của router.
- WAN networking device: Là các thiết bị khác như các chuyển mạch ATM, chuyển mạch Frame Relay, tổng đài điện thoại, các router trên mạng đường trực...

Lớp vật lý của mạng điện rộng

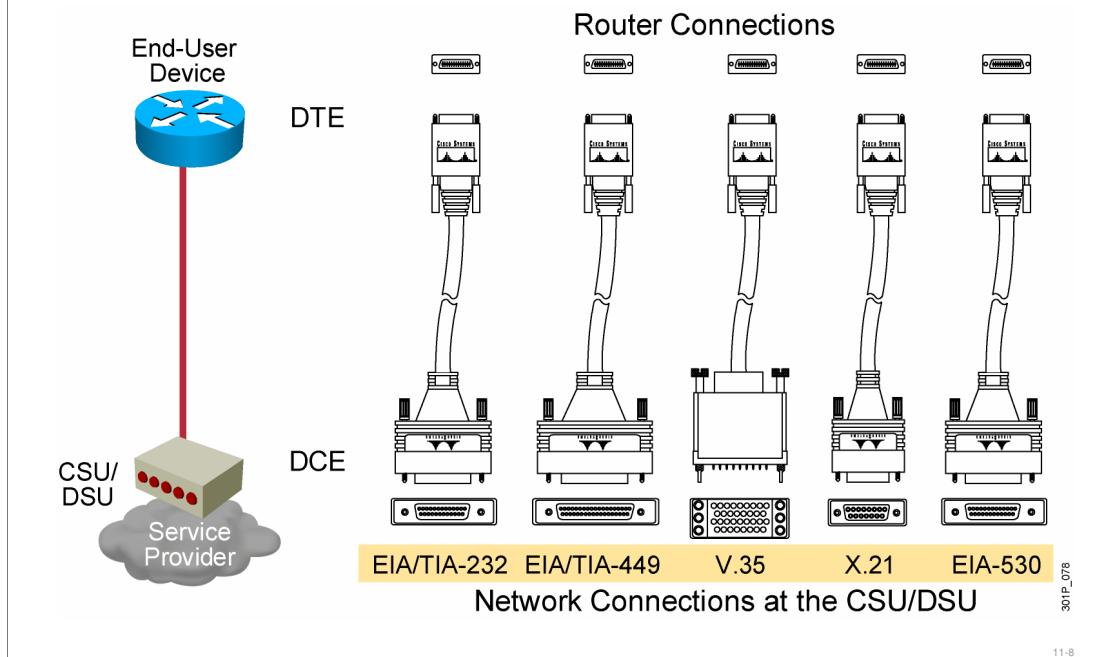


Các thiết bị về phía nhà sử dụng (thuê bao) được gọi là customer premises equipment (CPE). Thuê bao làm chủ các CPE hoặc thuê CPE từ nhà cung cấp. Dây đồng hoặc dây cáp quang kết nối CPE đến tổng đài gần nhất hoặc điểm kết nối gần nhất của nhà cung cấp dịch vụ. Kết nối cáp này thường được gọi là “local loop” hay là “last mile”. Sự truyền dẫn dữ liệu analog được kết nối cục bộ tới một local loop khác hoặc không cục bộ thông qua một trung kế tới một trung tâm chính. Dữ liệu analog sau đó đi tới trung tâm của khu vực, tới các truyền dẫn khu vực, truyền dẫn quốc tế, giống như một cuộc gọi điện thoại bình thường.

Đối với các local loop để mang dữ liệu, cần một thiết bị như modem hoặc DSU/CSU để chuẩn bị dữ liệu trước khi truyền. Thiết bị mà gởi dữ liệu xuống local loop gọi là Data Circuit-terminating Equipment hay Data Communications Equipment (DCE). Thiết bị của thuê bao mà gởi dữ liệu tới DCE được gọi là Data Terminal Equipment (DTE). DCE nhiệm vụ chính để cung cấp giao tiếp cho DTE có thể truyền thông bên trong kiến trúc mạng điện rộng.

Lớp vật lý của truy cập mạng điện rộng mô tả giao tiếp giữa DTE và DCE.

Kết nối tuần tự điểm nối điểm



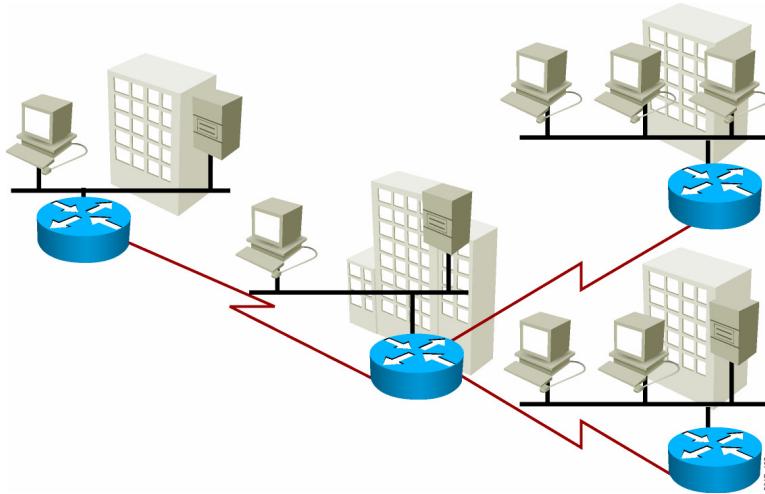
11-8

Các router Cisco hỗ trợ các chuẩn giao tiếp EIA/TIA-232, EIA/TIA-449, V.35, X.21, và EIA/TIA-530 trên kết nối serial.

Khi chúng ta đặt mua cáp, chúng ta sẽ nhận được cáp chuyển tiếp serial bọc giáp theo chuẩn mà ta đặt hàng. Đầu về phía router có một kết nối DB-60, mà sẽ kết nối tới một đầu DB-60 trên thẻ giao tiếp mạng điện rộng của router. Bởi có thể 5 loại cáp khác nhau trên một cổng giao tiếp loại này, nên đôi khi nó được gọi là cổng giao tiếp 5 trong 1. Đầu kia của cáp là kết nối tương ứng với chuẩn mà ta sử dụng. Tài liệu của thiết bị mà ta muốn kết nối tới router sẽ cho biết chuẩn của cáp này.

Thiết bị thuộc sở hữu của thuê bao như router là thiết bị DTE. Các thiết bị DCE như modem hay DSU/CSU là thiết bị mà được sử dụng để chuyển đổi dữ liệu của người sử dụng từ DTE thành dạng có thể được chấp nhận bởi nhà cung cấp dịch vụ kết nối mạng điện rộng. Các cổng giao tiếp đồng bộ trong router có thể được cấu hình như DTE hoặc DCE (trừ chuẩn EIA/TIA-530 chỉ cấu hình như DTE) phụ thuộc và cáp gắn vào. Nếu cổng yêu cầu là DTE (mặc định), nó sẽ yêu cầu một nguồn phát đồng hồ đồng bộ bên ngoài từ thiết bị DCE kết nối với nó.

Mạng điện rộng – Nhiều mạng cục bộ



11-9

Router có cả các cổng LAN và WAN, trong khi router được sử dụng để phân đoạn mạng cục bộ, nó cũng được sử dụng như thiết bị truy xuất mạng điện rộng. Chức năng và vai trò của router trong việc truy cập mạng điện rộng có thể được biết rõ bởi xem các kiểu kết nối có thể sử dụng trong router. Có 3 kiểu cơ bản của kết nối trong router: Giao tiếp LAN, giao tiếp WAN, và các cổng để quản lý. Giao tiếp LAN cho phép router kết nối tới mạng cục bộ qua Ethernet hay các công nghệ LAN khác như Token Ring hay ATM.

Kết nối mạng điện rộng giữa một giao tiếp WAN trên router qua nhà cung cấp dịch vụ để kết nối tới các địa điểm khác hoặc Internet. Có thể thông qua cổng serial hoặc các giao tiếp WAN khác. Với một số kiểu giao tiếp WAN, một thiết bị bên ngoài như DSU/CSU hoặc modem (như một modem analog, modem truyền hình cáp, hoặc một modem DSL) để kết nối router tới POP của nhà cung cấp dịch vụ.

Một điểm phân trách (demarcation point) vật lý được sử dụng để phân chia trách nhiệm của người sử dụng và nhà cung cấp dịch vụ. Điểm này quan trọng vì khi có sự cố xảy ra cả hai phía đều cần chứng minh trách nhiệm xử lý thuộc về ai.

Các cổng để quản lý cung cấp một kết nối giao diện text để cho phép cấu hình và xử lý sự cố. Các giao tiếp quản lý là cổng console và cổng auxiliary. Các cổng này được kết nối tới một cổng thông tin của máy tính (COM). Máy tính phải chạy một chương trình giả lập terminal để cung cấp các phiên giao tiếp dạng text với router, từ đó cho ta quản lý thiết bị.

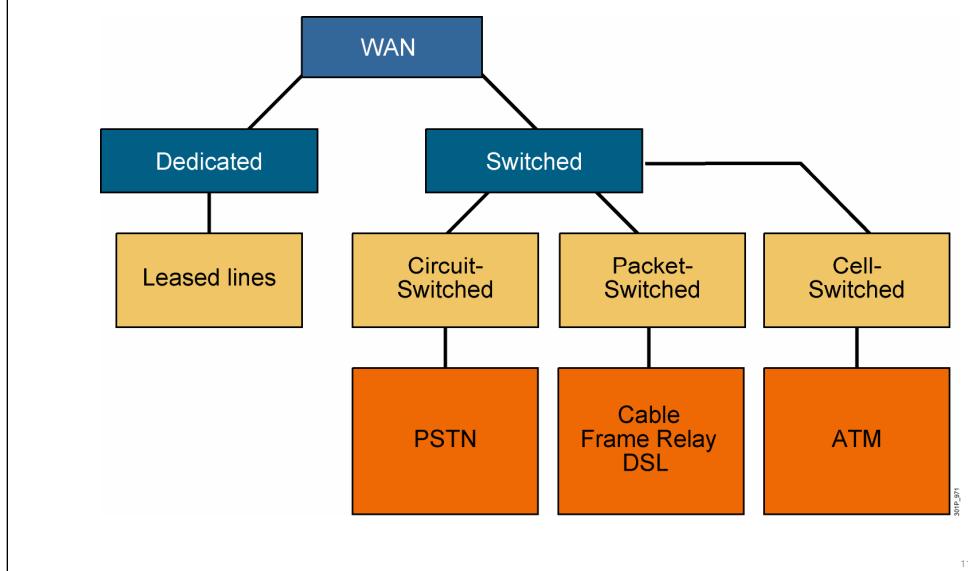
Các giao thức lớp liên kết dữ liệu mạng điện rộng

- HDLC
- PPP
- Frame Relay (LAPF)
- ATM

11-10

Các giao thức lớp liên kết dữ liệu định nghĩa làm thế nào dữ liệu được đóng gói để truyền tới đầu bên kia và cơ chế để truyền gói. Có nhiều công nghệ khác nhau như ISDN, Frame Relay, hoặc ATM. Nhiều giao thức trong đó sử dụng cùng một cơ chế đóng khung cơ bản là HDLC, là một chuẩn ISO, hoặc một phần hoặc các cải biến thế của nó. ATM thì khác biệt hơn, bởi nó sử dụng các gói nhỏ kích thước cố định là 53 bytes (48 byte là dữ liệu)

Các loại liên kết mạng điện rộng



Có hai loại chính của liên kết mạng điện rộng là: liên kết dành riêng và liên kết chuyên mạch.

Trong mỗi loại có các kiểu riêng biệt của liên kết mạng như sau:

- Kết nối thông tin dành riêng: Khi cần một kết nối điểm nối điểm dành riêng vĩnh viễn với dung lượng chỉ bị hạn chế loại truyền dẫn và chi phí thuê đường. Kết nối điểm nối điểm này cung cấp một sự truyền thông mạng điện rộng được thiết lập sẵn từ khách hàng thông qua nhà cung cấp đến đầu khách hàng bên kia. Do thường được thuê từ các cty về truyền dẫn nên được gọi là leased line.
- Kết nối thông tin chuyên mạch: Sự chuyên mạch tự động thiết lập một kết nối ảo dành riêng để trao đổi thoại và dữ liệu giữa người gửi và người nhận. Trước khi sự truyền thông có thể xảy ra, cần thiết phải thiết lập một kết nối thông qua mạng của nhà cung cấp
- Kết nối thông tin chuyển gói: Đối với một số người sử dụng, việc sử dụng các đường truyền cố định như đường dành riêng hay chuyên mạch không có hiệu quả sử dụng cao do tính chất bất thường của dữ liệu. Các nhà cung cấp có những mạng dữ liệu dành cho những người sử dụng này. Trong môi trường chuyển gói, dữ liệu được truyền trong dạng “tế bào”, “khung” hoặc “gói”.

Tóm tắt

- Có 3 đặc điểm chính của mạng diện rộng: kết nối các thiết bị mà xa nhau về vị trí địa lý, sử dụng các dịch vụ của nhà cung cấp, như cty điện thoại, cty truyền hình cáp, hệ thống vệ tinh, nhà cung cấp dịch vụ mạng, và sử dụng kết nối serial với vài kiểu khác nhau
- Nhiều tổ chức và gia đình muốn có sự kết nối với người sử dụng từ xa, như kết nối giữa người sử dụng ở xa với cty, chia sẻ dữ liệu giữa các cty, truy cập internet ...

Tóm tắt (tiếp)

- Mạng cục bộ kết nối các máy tính, thiết bị ngoại vi, và các thiết bị khác trong một tòa nhà hoặc không gian địa lý giới hạn. Mạng diện rộng để kết nối qua một khoảng cách địa lý rộng
- Một cty, tổ chức hoặc cá nhân phải là thuê bao của một nhà cung cấp dịch vụ để sử dụng dịch vụ mạng diện rộng, trong khi mạng cục bộ được làm chủ bởi thực thể đó
- Mạng diện rộng hoạt động tương ứng với lớp 1 và lớp 2 của mô hình OSI

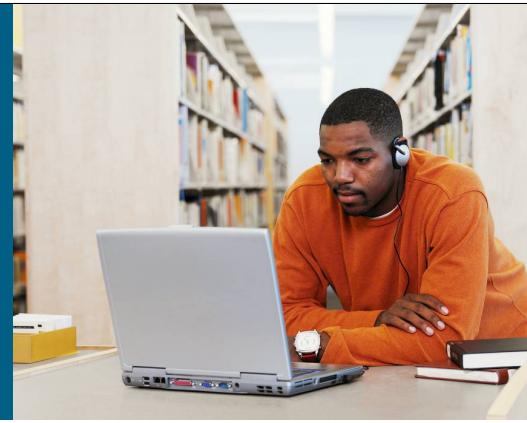
Tóm tắt (tiếp)

- Các kiểu thiết bị chính sử dụng trong truy cập mạng diện rộng là router, communication servers, modem (DSU/CSU) và các thiết bị khác như Frame-Relay và tổng đài điện thoại
- Router có các giao tiếp LAN và WAN, ngoài việc sử dụng để phân đoạn mạng LAN, nó còn sử dụng để kết nối WAN
- Các giao thức lớp liên kết dữ liệu định nghĩa làm thế nào dữ liệu được đóng gói để truyền đi. Có nhiều công nghệ như ISDN, Frame Relay hoặc ATM



11-15

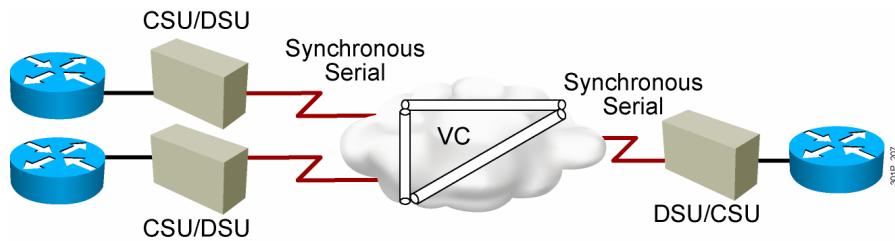
Bài 12: Cho phép kết nối Internet



Kết nối mạng điện rộng

12-1

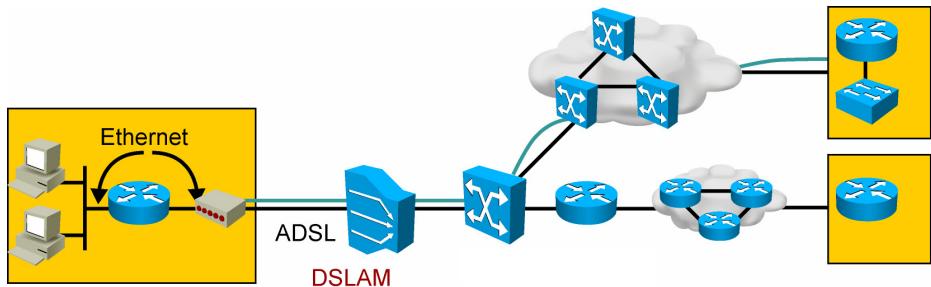
Chuyển gói



12-2

- Là phương pháp mà trong đó không có một đường dành riêng từ nguồn tới đích, cho phép chia sẻ các kết nối và tài nguyên của kênh truyền.
- Chuyển gói cho phép gởi dữ liệu trên các đường khác nhau trên một mạng công cộng dùng chung tới cùng một đích. Thay vì cung cấp một đường thông tin dành riêng, nhà cung cấp cung cấp một mạng tới thuê bao và đảm bảo dữ liệu nhận ở một đầu, sẽ được gởi ra một đầu khác. Tuy nhiên, đường đi để tới đích có thể thay đổi. Khi gói đến đích, giao thức có trách nhiệm đảm bảo chúng được lắp ráp đúng trật tự ban đầu.
- Chuyển gói cho phép giảm số lượng đường link trên mạng và cho phép nhà cung cấp tăng được hiệu quả sử dụng cơ sở hạ tầng và do đó nói chung chi phí thấp hơn so với kết nối điểm đến điểm hoặc leased line. Trong môi trường chuyển gói, nhiều mạng khách hàng kết nối tới nhà cung cấp, nhà cung cấp tạo các mạch ảo giữa những địa điểm của khách hàng. Khi khách hàng không sử dụng hoàn toàn băng thông của mạch ảo, nhà cung cấp có thể cấp băng thông dư thừa này cho khách hàng khác.

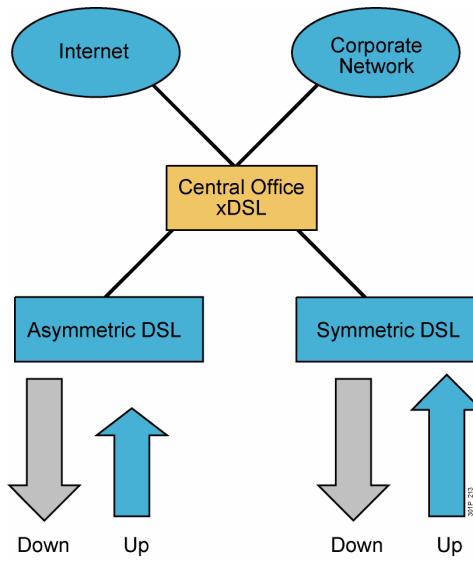
DSL



12-3

- Công nghệ DSL là công nghệ kết nối liên tục mà sử dụng trên cáp điện thoại hiện tại. Một thiết bị là DSL modem được sử dụng để đổi tín hiệu Ethernet từ người sử dụng tới tín hiệu DSL của nhà cung cấp
- Công nghệ DSL cho phép dịch vụ mạng tốc độ cao, cở E1/T1, trên cáp đồng điện thoại. Cho phép đường dây vẫn sử dụng điện thoại hiện tại và kết nối mạng liên tục. Phía nhà cung cấp, nhiều thuê bao DSL được kết nối tới một đường truyền dung lượng cao qua một thiết bị là DSLAM. DSLAM là một thiết bị ghép kênh theo thời gian để gom nhiều kết nối thuê bao vào trong phương tiện đơn dung lượng cao hơn. Hiện tại DSL có thể sử dụng đến 8.192Mb/s với các kỹ thuật mã hóa và điều chế tinh vi.
- Kênh thoại trên kết nối thuê bao sử dụng tần số từ 330 tới 3.3 kHz như truyền thống. Như vậy dãy tần số 4 kHz là được dành cho thoại trên đường cáp. Công nghệ DSL sử dụng các tần số mang dữ liệu tải lên và tải xuống ở khoảng trên dãy tần số này cho phép có thể tải thoại và dữ liệu đồng thời trên cáp này.
- DSL được sử dụng rộng rãi ngày nay và bao gồm nhiều biến thể khác nhau. Công nghệ này được lựa chọn phổ biến để làm việc tại nhà.

Các kiểu dịch vụ DSL



12-4

Kiểu và chuẩn DSL

- **Asymmetric DSL (ADSL):** Bất đối xứng - Cho phép băng thông tải về cao hơn nhiều băng thông tải lên
- **Symmetric DSL (SDSL):** Đối xứng - Cho phép băng thông tải lên và về bằng nhau

Các dạng dịch vụ DSL là được phân loại là đối xứng và bất đối xứng, nhưng có nhiều biến thể khác nhau”

- ADSL:
 - Consumer DSL (CDSL), also called G.Lite or G.992.2
 - Very-high-data-rate DSL (VDSL)
- SDSL:
 - High-data-rate DSL (HDSL)
 - ISDN DSL (IDSL)
 - Symmetric high bit rate DSL (G.shdsl)

Xem xét về DSL

Ưu điểm

- Tốt độ
- Đồng thời thoại và dữ liệu
- Nhiều lợi ích thêm vào
- Khả năng luôn kết nối
- Tương thích với mạng điện thoại

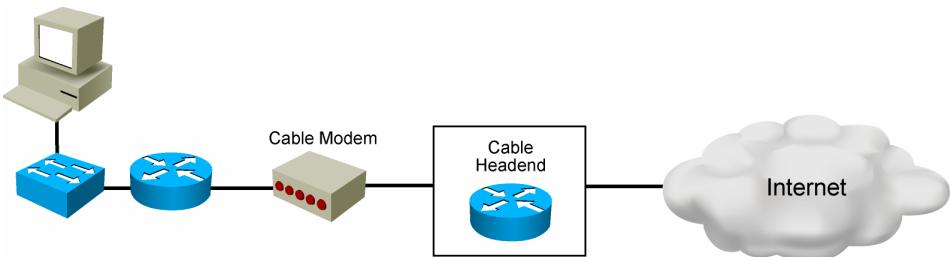
Khuyết điểm

- Khoảng cách giới hạn
- Yêu cầu công ty điện thoại địa phương
- Có rủi ro về an ninh mạng

12-5

Đa số các dịch vụ DSL thường yêu cầu thuê bao không cách xa qua 5,5km từ nhà cung cấp.

Kết nối qua mạng truyền hình cáp

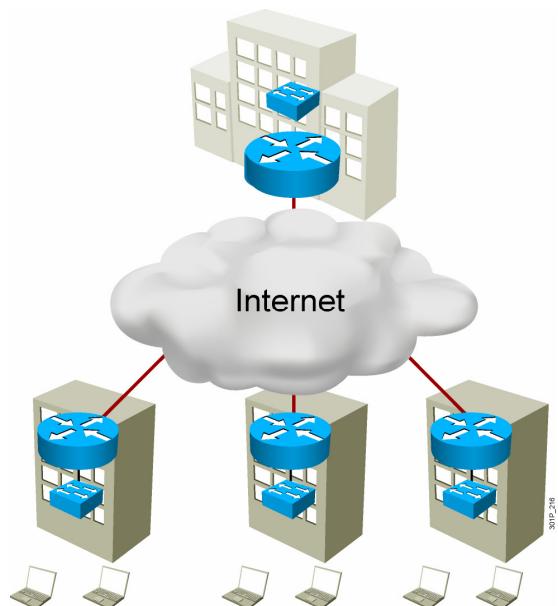


30/10/14

12-6

Ban đầu cáp truyền hình là phương tiện truyền đơn hướng để cung cấp các tín hiệu truyền hình tới thuê bao. Về sau được cải tiến để mang tín hiệu IP-over-Ethernet tới thuê bao. Nhưng từ những năm 1990, phương thức này đã bị thách thức bởi công nghệ DSL.

Mạng toàn cầu Internet



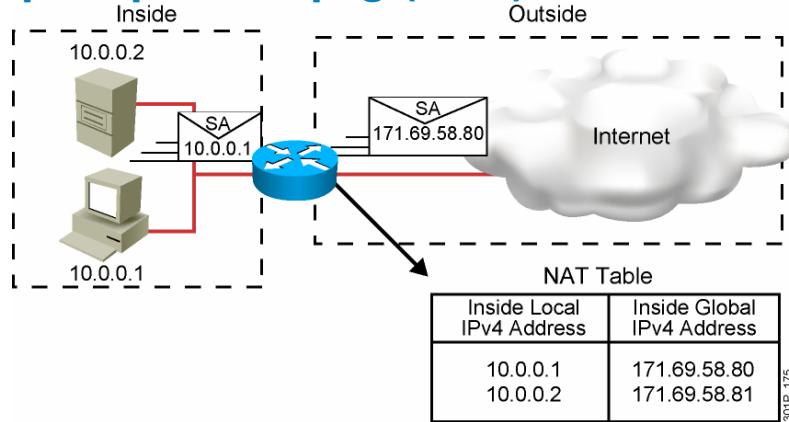
12-7

Cấp địa chỉ từ DHCP server

- Không phải cấu hình thủ công
- Một router có thể làm việc như là một DHCP client.
- Trong kết nối Internet, ISP cung cấp thông tin DHCP

12-8

Dịch địa chỉ mạng (NAT)



- Địa chỉ IP hoặc là local hoặc là global.
- Địa chỉ Local là địa chỉ thấy từ mạng trong
- Địa chỉ Global là địa chỉ thấy từ mạng ngoài
- Việc gán có thể tĩnh hoặc động

12-9

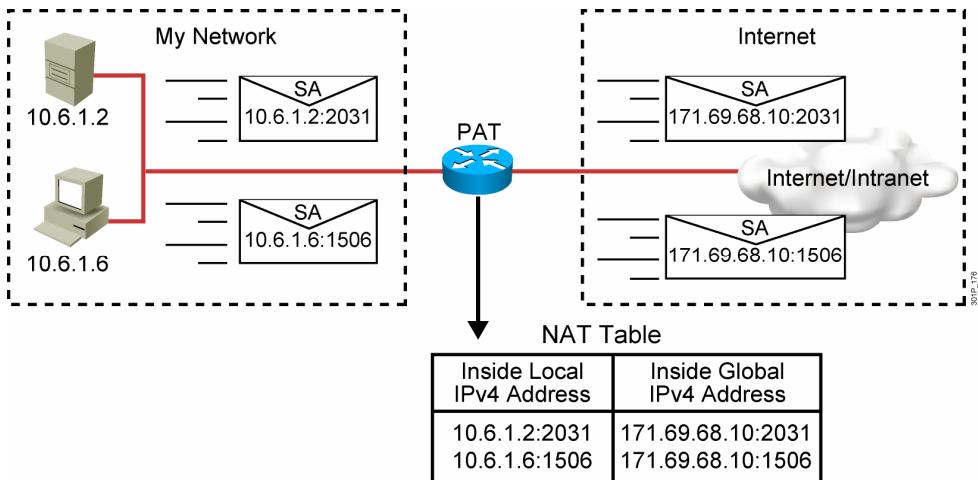
Các mạng nhỏ nói chung thường sử dụng địa chỉ IP riêng. Khi kết nối tới Internet, cần phải có cách để đổi địa chỉ IP riêng tới IP công cộng. NAT hoạt động trong router Cisco và nó cho phép các mạng sử dụng IP riêng hoặc không đăng ký kết nối tới Internet. Thường NAT kết nối 2 mạng với nhau và dịch các địa chỉ riêng thành các địa chỉ công cộng trước khi chuyển ra ngoài mạng khác. Có thể cấu hình NAT để chỉ cần một địa chỉ đại diện cho toàn bộ mạng để ra ngoài. Quảng bá một địa chỉ che dấu một các hiệu quả mạng trong trước bên ngoài, và do đó tăng khả năng an ninh mạng.

Bất kỳ thiết bị nào giữa mạng trong và ngoài như firewall, router hoặc máy tính đều có thể sử dụng như NAT.

Trong thuật ngữ NAT, khái niệm inside để chỉ nhóm mạng mà cần dịch địa chỉ. Khái niệm outside để chỉ các địa chỉ khác, như các địa chỉ ngoài Internet

- **Inside local address:** Địa chỉ gán tới host trong mạng trong.
- **Inside global address:** Địa chỉ công cộng để đại diện cho một hoặc nhiều địa chỉ bên trong
- **Outside local address:** Địa chỉ của một host bên ngoài, như khi nó xuất hiện bên trong mạng trong
- **Outside global address:** Địa chỉ được cấp tới một host bên ngoài bởi người quản lý host đó

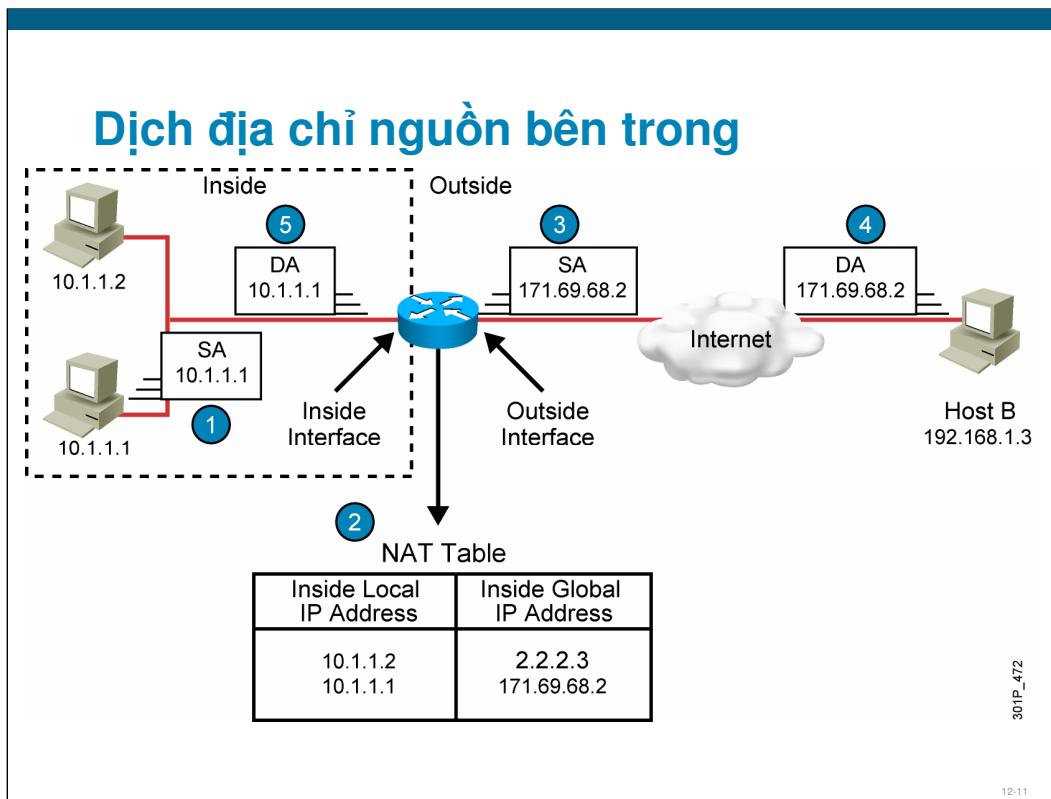
Dịch địa chỉ cổng (PAT)



12-10

Một trong những khả năng chính của NAT là static PAT. PAT cho phép nhiều địa chỉ ở mạng bên trong có thể được dịch thành một hoặc một vài địa chỉ bên ngoài.

PAT sử dụng số port duy nhất để phân biệt các phiên dịch của các địa chỉ bên trong khác nhau. Bởi port có 16 bit do đó tổng số địa chỉ bên trong có thể dịch với một địa chỉ bên ngoài về lý thuyết là 65536. PAT hoạt động sẽ giữ lại giá trị port gửi, nếu port đã sử dụng, PAT sẽ tìm port đầu tiên còn rảnh để sử dụng bắt đầu từ địa chỉ đầu tiên của nhóm port tương ứng 0-511, 512-1023 hoặc 1024-65535. Nếu PAT không tìm được port còn rảnh và nếu nhiều hơn một IP công cộng được sử dụng, PAT sẽ cấp phát port gửi trên IP kế tiếp giống như IP ban đầu.



Trong hình router dịch địa chỉ nguồn bên trong thành địa chỉ nguồn bên ngoài mạng, các bước như sau:

Bước 1: Người dùng ở địa chỉ 10.1.1.1 mở kết nối tới máy B

Bước 2: Gói đầu tiên mà router nhận, sẽ làm router kiểm tra bảng NAT:

Nếu có một sự dịch địa chỉ tĩnh, chuyển qua bước 3

Nếu không có sự dịch địa chỉ tĩnh, router xác định địa chỉ 10.1.1.1 cần dịch động. Router chọn một địa chỉ công cộng phù hợp trong dãy địa chỉ động và tạo một dòng trong bảng NAT mô tả việc dịch này.

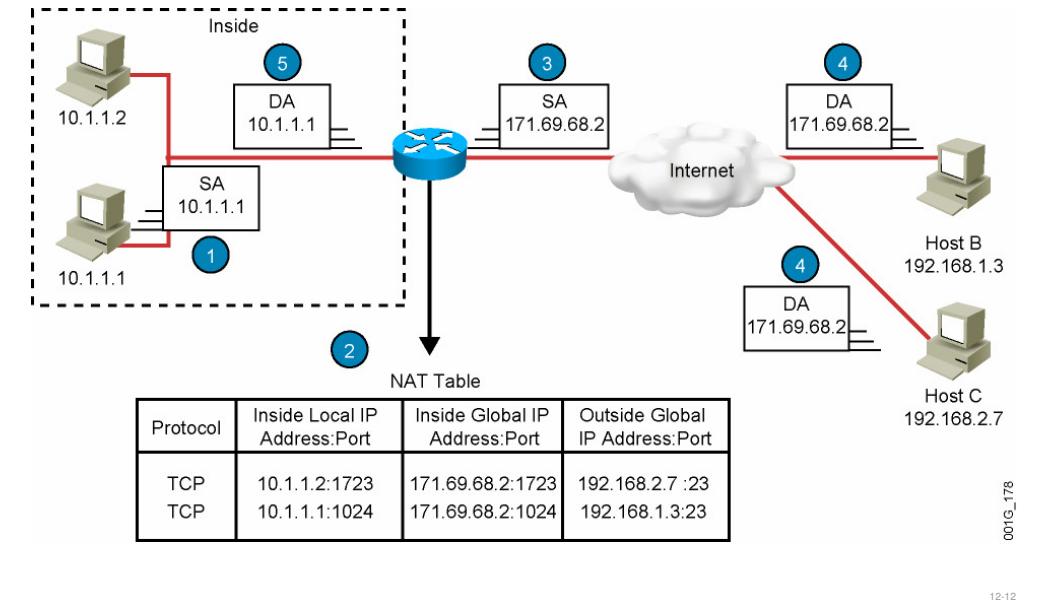
Bước 3: Router thay địa chỉ nguồn trong gói tin với địa chỉ công cộng theo mô tả dòng NAT trong bảng và gửi gói ra ngoài.

Bước 4: Máy B nhận gói và trả lời về địa chỉ công cộng trong địa chỉ nguồn gói ban đầu (171.69.68.2)

Bước 5: Router nhận gói từ B và tìm trong bảng NAT xem có dòng dịch địa chỉ tương ứng không. Tìm thấy, router sẽ thay địa chỉ đích của gói tin bằng địa chỉ ban đầu.

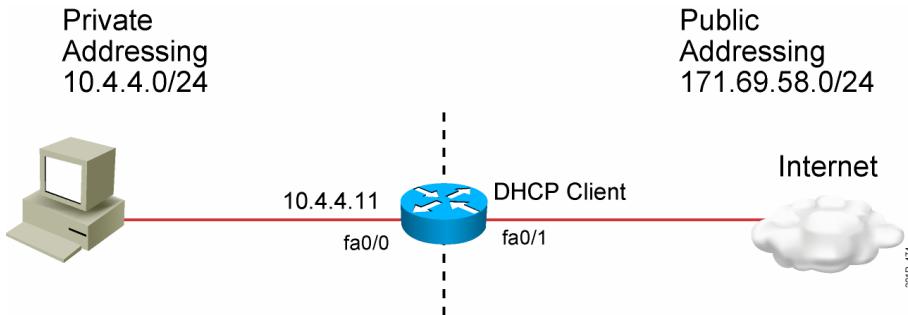
Bước 6: Máy 10.1.1.1 nhận được gói và tiếp tục gửi các gói tin khác

Dịch địa chỉ port



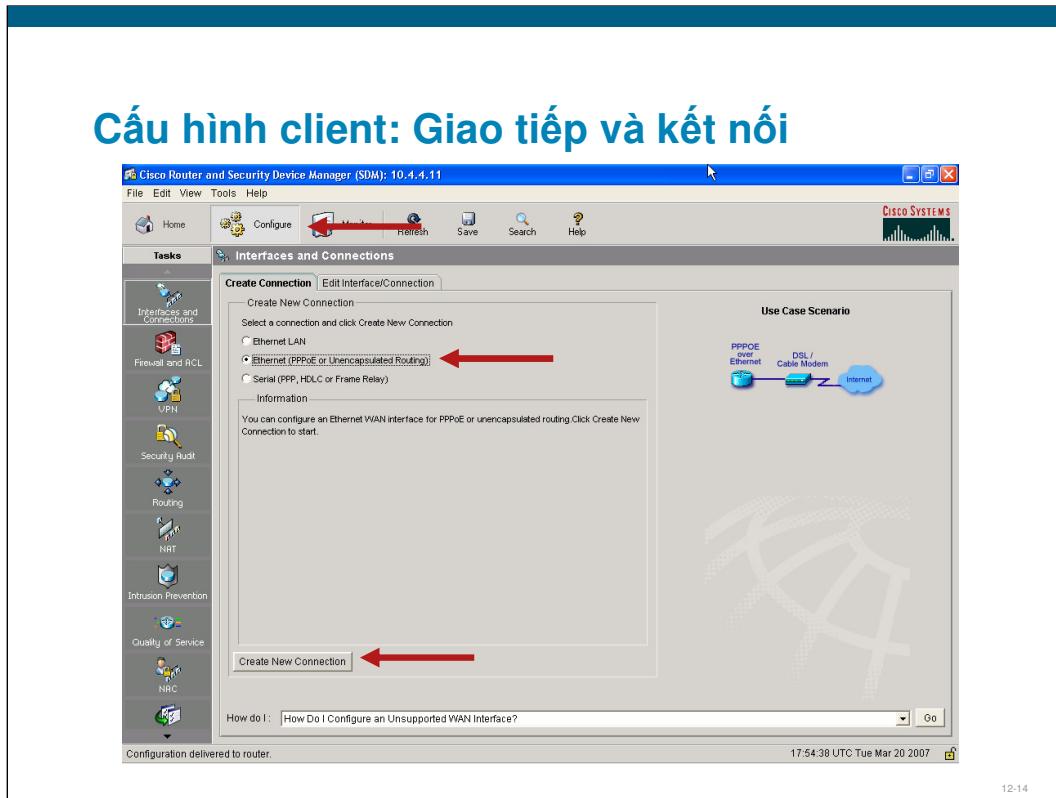
Chúng ta có thể tiết kiệm địa chỉ công cộng bằng việc sử dụng NAT nhiều địa chỉ bên trong thành một hoặc một vài địa chỉ bên ngoài. Khi được cấu hình router sử dụng các thông tin ở protocol con hơn là port trong các gói TCP và UDP để phân biệt các phiên dịch khác nhau.

Tập hợp các thông tin yêu cầu



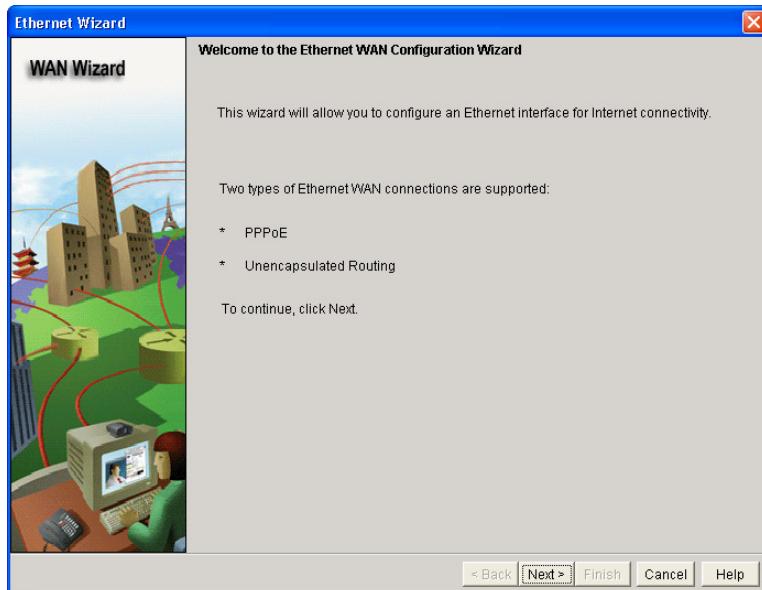
12-13

Khi thực hiện chúng ta cấu hình Fa0/1 như là DHCP client để lấy địa chỉ IP, default gateway và default routing từ DHCP server bên Internet. Sau đó cấu hình PAT để dịch địa chỉ mạng trong tới địa chỉ mạng ngoài



Để cấu hình DHCP client, chọn **Interfaces and Connections tab**.
 Chọn **Ethernet (PPPoE or Unencapsulated Routing)** radio button
 Chọn **Create New Connection button**.

Cấu hình client: WAN Wizard



12-15

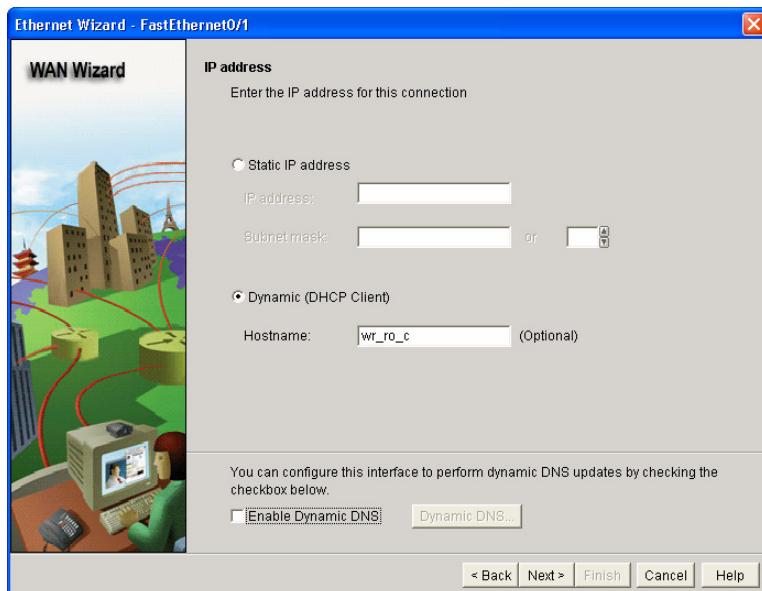
Cấu hình client: Đóng gói



12-16

Nếu nhà cung cấp sử dụng PPPoE, chọn vào hộp chọn này

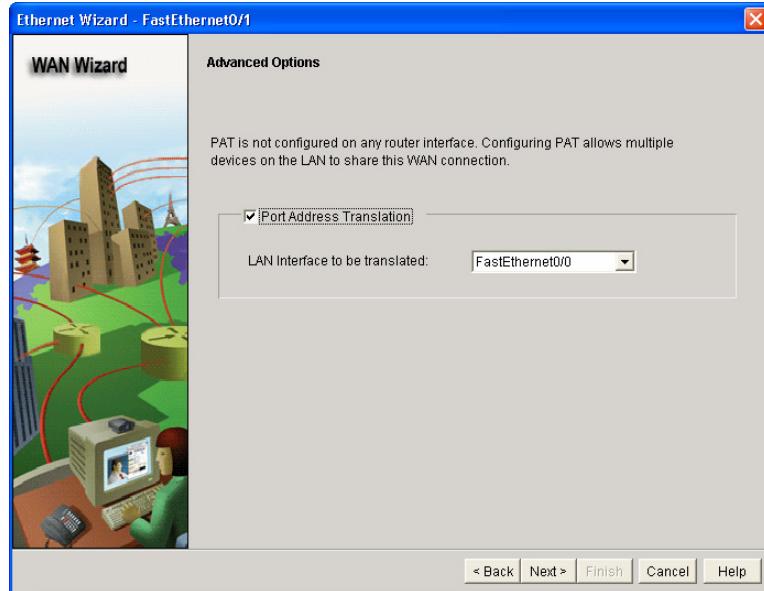
Cấu hình client: IP Addressing



12-17

Chọn Dynamic (DHCP Client) radio button và nhập hostname.

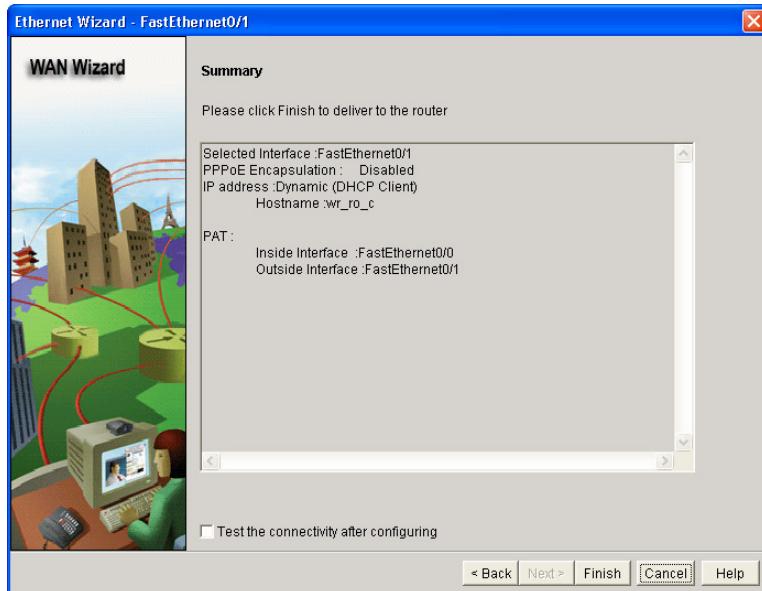
Cấu hình PAT: các tùy chọn nâng cao



12-18

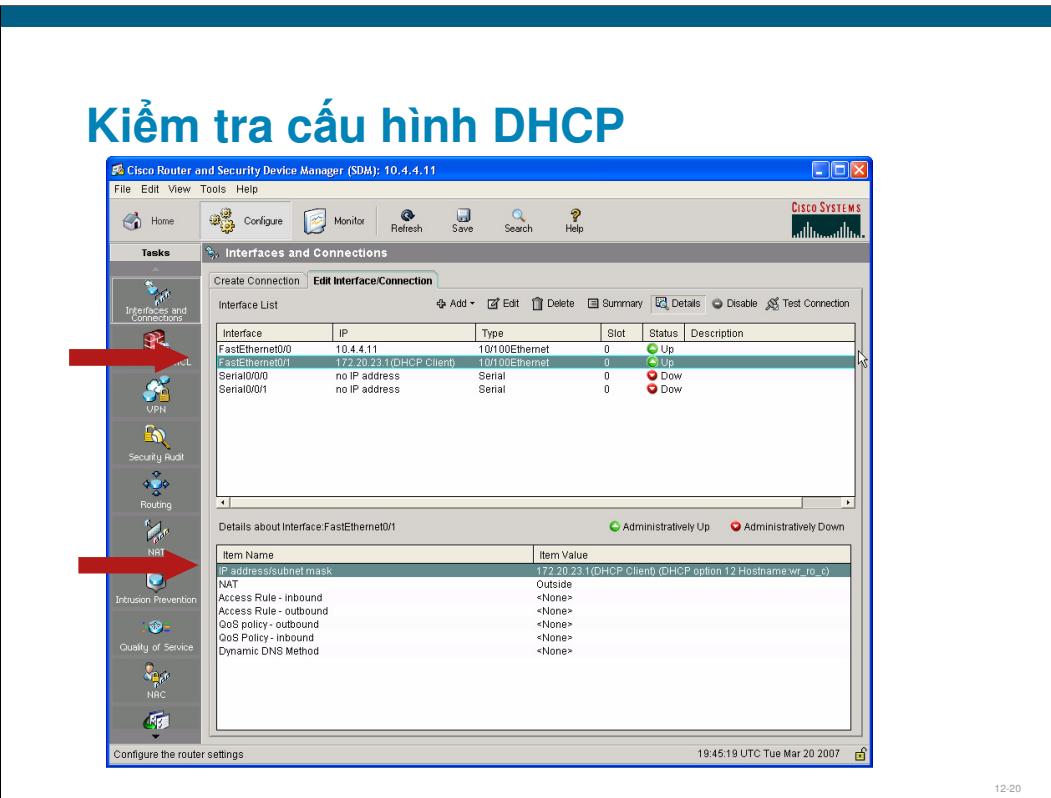
Chọn **Port Address Translation** và chọn **inside interface** trong **drop-down list**.

Configuring PAT: Summary



12-19

This window provides a summary of the configuration.



Sử dụng Interfaces and Connections window để kiểm tra rằng DHCP đã chọn được một địa chỉ IP

Hiển thị thông tin với lệnh show

```
RouterX# show ip nat translation
      Pro Inside global      Inside local        Outside
local      Outside global
      --- 172.16.131.1      10.10.10.1      ---
```

- Displays active translations

```
RouterX# clear ip nat translation *
```

- Clears all dynamic address translation entries

12-21

Các phiên dịch địa chỉ động sẽ quá hạn trong bảng NAT sau một chu kỳ thời gian nhất định. Một phiên dịch NAT sẽ hết hạn sau 24h. Chúng ta có thể xóa nó với lệnh trên

Tóm tắt

- Mạng chuyển gói gửi dữ liệu trên các đường khác nhau tới mạng đích trên một mạng công cộng dùng chung được quản lý bởi các nhà cung cấp dịch vụ
- Có vài kiểu DSL khác nhau như ADSL, SDSL, HDSL, IDSL, và CDSL.
- Mạng truy cập Internet qua truyền hình cáp là một lựa chọn khác bên cạnh DSL và serial link.
- Mạng Internet toàn cầu phát triển từ mạng của bộ Quốc Phòng Mỹ. Hiện nay nó là mạng điện rộng lớn nhất trên thế giới với nhiều các truy cập khác nhau cho thông tin, nghiên cứu và thương mại
- Một giao tiếp có thể lấy địa chỉ IP từ một DHCP server

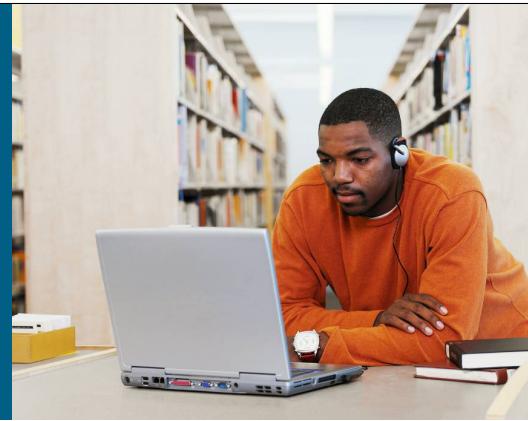
Tóm tắt (Tiếp)

- NAT cho phép một địa chỉ dùng riêng có thể kết nối tới Internet. PAT là một khả năng của NAT cho phép nhiều địa chỉ bên trong có thể sử dụng cùng một vài địa chỉ công cộng để ra ngoài
- Overloading là một dạng của NAT động cho phép ánh xạ nhiều địa chỉ IP không đăng ký bên trong ra một IP đã đăng ký bên ngoài, còn được gọi là PAT.
- Sau khi NAT được cấu hình, dùng lệnh clear và show để kiểm tra hoạt động.

12-23



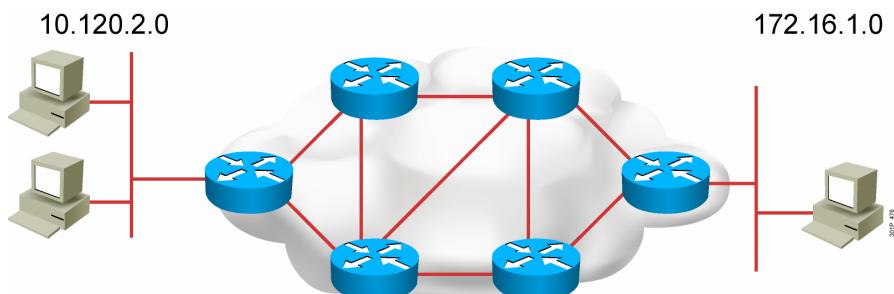
Bài 13: Cấu hình định tuyến tĩnh



Kết nối mạng diện rộng

13-1

Hoạt động của router



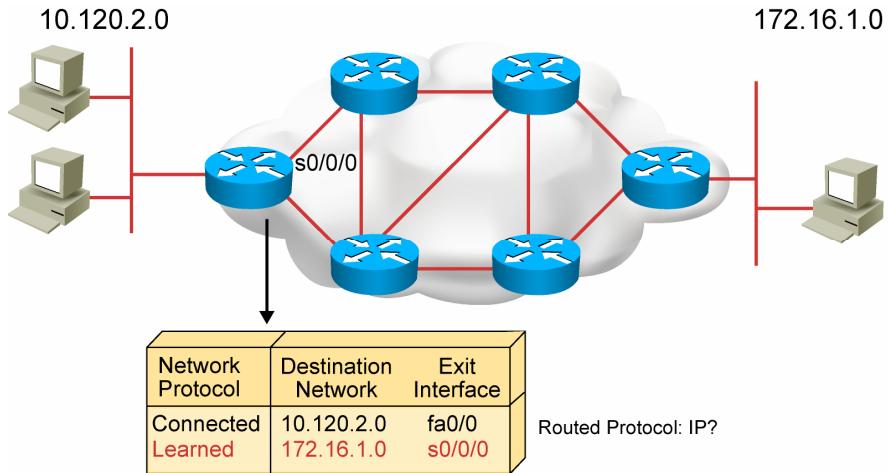
Router cần làm các việc sau:

- Biết các địa chỉ đích.
- Xác định nguồn mà router có thể học.
- Khám phá các tuyến có thể tới các đích mong muốn
- Chọn tuyến tốt nhất.
- Duy trì bảng định tuyến.

13-2

Định tuyến là quá trình mà một gói tin từ một vị trí này tới một vị trí khác. Trong mạng, một router là thiết bị để định tuyến dữ liệu

Hoạt động của router (Tiếp)



- Router phải học các địa chỉ đích mà không kết nối trực tiếp

13-3

Thông tin định tuyến mà một router có được từ các router khác được đặt vào bảng định tuyến. Router sẽ dựa vào bảng định tuyến này để chỉ ra cổng giao tiếp nào được sử dụng để gửi một gói tin ra.

Nếu một mạng đích là kết nối trực tiếp, router biết cổng giao tiếp nào sử dụng để gửi gói tin ra. Nếu mạng đích không kết nối trực tiếp, router phải học tuyến tốt nhất để gửi gói tin đi.

Có 2 cách để học thông tin về mạng đích:

- Nhập các tuyến vào bằng lệnh
- Tập hợp thông tin định tuyến qua một quá trình định tuyến động chạy trong router.

Tuyến tĩnh và tuyến động

Tuyến tĩnh

- Tuyến mà người quản trị nhập vào bằng lệnh

Tuyến động

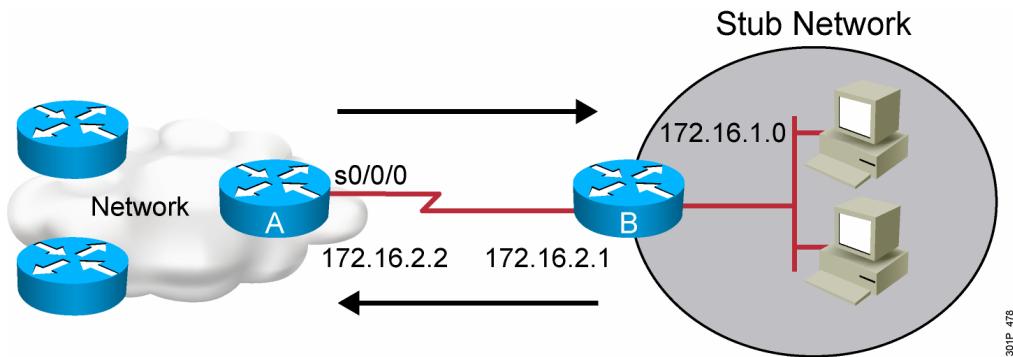
- Tuyến do các giao thức định tuyến đưa ra dựa vào tình trạng mạng hiện tại

13-4

Static route: Người quản trị phải cập nhật thủ công tuyến tĩnh này bất cứ khi nào mạng thay đổi.

Dynamic route: Sau khi người quản trị cho phép định tuyến động, quá trình định tuyến tự động cập nhật kiến thức về tuyến bất kỳ khi nào mạng bị thay đổi. Router học và duy trì các tuyến tới mạng đích bằng cách trao đổi các cập nhật tuyến với các router khác trên mạng

Các tuyến tĩnh



Cấu hình các tuyến tĩnh đơn hướng tới và từ một mạng ngõ cút để cho phép kết nối

30

13-5

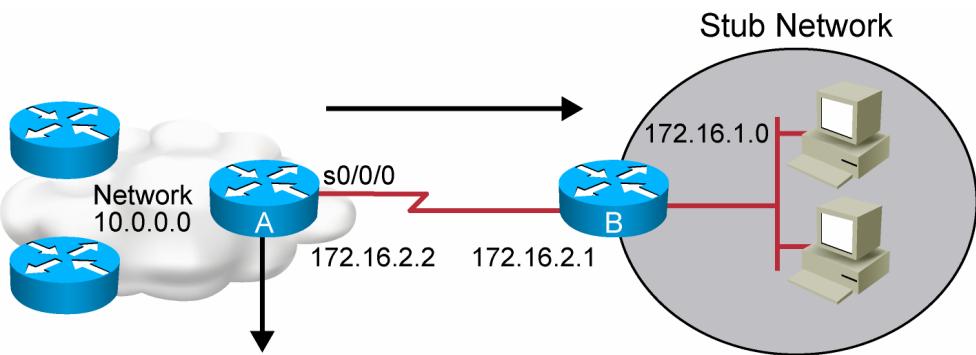
Tuyến tĩnh nói chung được sử dụng khi định tuyến từ một mạng tới một mạng ngõ cút (stub ☺). Đó là mạng có một truy cập đơn ra bên ngoài. Tuyến tĩnh có thể định nghĩa như một tuyến mặc định mà cho phép định tuyến bất kỳ mạng nào ra ngoài.

Static Route Configuration

```
RouterX(config)# ip route network [mask]
{address | interface} [distance] [permanent]
```

- Defines a path to an IP destination network or subnet or host
- Address = IP address of the next hop router
- Interface = outbound interface of the local router

Ví dụ định tuyến tĩnh



```
RouterX(config)# ip route 172.16.1.0 255.255.255.0 172.16.2.1
```

or

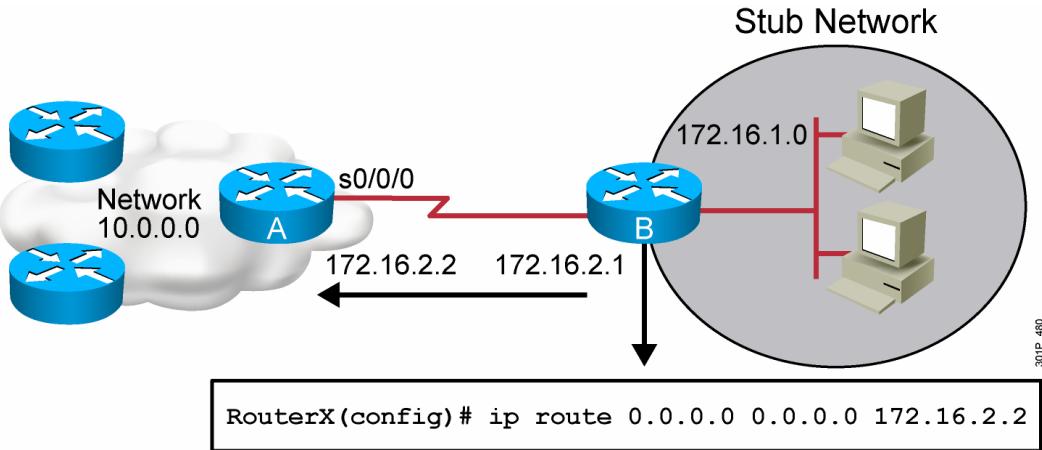
```
Router(config)#ip route 172.16.1.0 255.255.255.0 s0/0/0
```

- Đây là tuyến đơn hướng. Chúng ta phải có một tuyến cấu hình trong hướng ngược lại

30IP_479

13-7

Tuyến mặc định



- Tuyến này cho phép các mạng ngõ cự kết nối đến tất cả các mạng khác ngoài router A

Sử dụng tuyến mặc định trong tình huống khi router gửi một gói tới một mạng đích không biết hoặc khi không có khả năng cho router duyệt trình qua nhiều tuyến trong bảng định tuyến

Kiểm tra cấu hình tuyến tĩnh

```
RouterX# 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
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
      U - per-user static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

      10.0.0.0/8 is subnetted, 1 subnets
C        10.1.1.0 is directly connected, Serial0/0/0
S*      0.0.0.0/0 is directly connected, Serial0
```

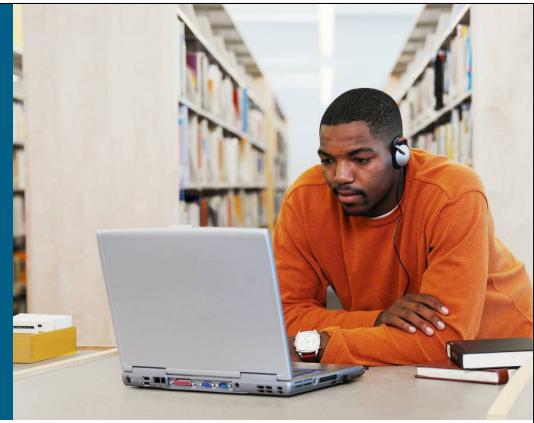
13-9

Tóm tắt

- Định tuyến là quá trình mà một phần tử được chuyển từ chỗ này sang chỗ khác. Router là thiết bị được sử dụng để định tuyến dữ liệu. Router có thể chuyển gói qua các tuyến tĩnh hoặc tuyến động tùy vào cấu hình
- Tuyến tĩnh là tuyến mà người quản trị nhập vào router qua lệnh. Tuyến động là tuyến được học từ các giao thức định tuyến và tự động cập nhật khi mạng thay đổi
- Các tuyến tĩnh đơn hướng phải được cấu hình đến và từ một mạng ngõ cụt (stub ☺) để cho phép mạng được kết nối
- Lệnh **ip route** có thể dùng để cấu hình các tuyến mặc định.
- Lệnh **show ip route** dùng để kiểm tra rằng tuyến tĩnh đã được cấu hình đúng. Tuyến tĩnh được ký hiệu bằng chữ S

13-10

Bài 14: Cấu hình đóng gói cổng serial



Kết nối mạng diện rộng

14-1

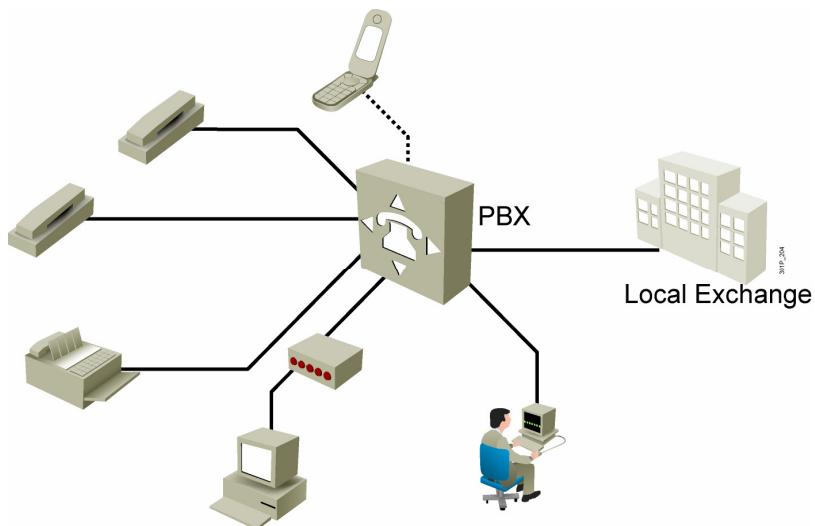
Chuyển mạch



14-2

Chuyển mạch cho phép khởi tạo kết nối trước khi truyền và hủy bỏ kết nối sau khi hoàn thành việc truyền.

Mạng điện thoại công cộng



14-3

Thỉnh thoảng, cần truyền dữ liệu với dung lượng thấp thì có thể sử dụng các modem bất đồng bộ và đường dây điện thoại. Dịch vụ này cung cấp kết nối theo nhu cầu, dung lượng thấp, thông qua các chuyên mạch dành riêng. Mạng điện thoại điện thoại sử dụng dây đồng được gọi là local loop để nối máy điện thoại với tổng đài. Khi gọi tín hiệu trong local loop là tín hiệu điện liên tục biến thiên để thể hiện âm thoại. Đường dây này không thích hợp để truyền dữ liệu, do đó một modem được sử dụng để đổi tín hiệu sang dạng có thể truyền trên local loop.

Băng thông trên các kết nối này là giới hạn, khoảng 33kb/s là tối đa. Tốc độ có thể lên tới khoảng 56kb/s nếu kết nối tới một kết nối digital.

Xem xét về PSTN

Thuận lợi

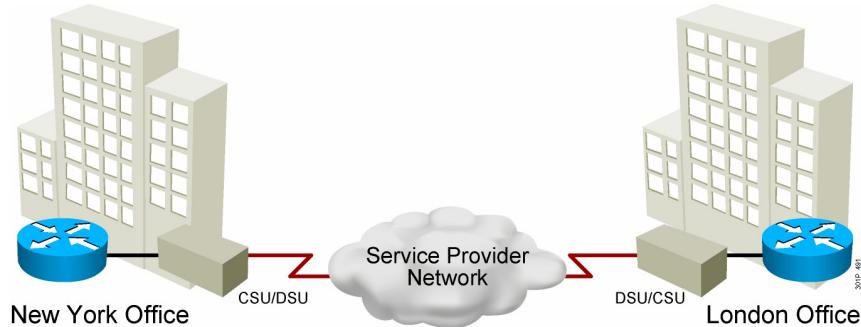
- Đơn giản
- Sẵn sàng
- Chi phí

Khuyết điểm

- Tốc độ thấp
- Thời gian thiết lập kết nối tương đối lâu

14-4

Đường thuê riêng

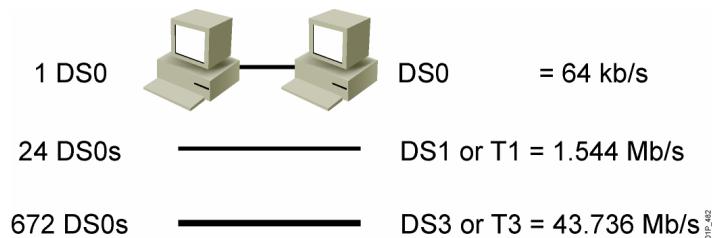


14-5

Liên kết điểm nối điểm cho phép thiết lập thông tin mạng điện rộng cho các thuê bao thông qua nhà cung cấp dịch vụ.

Kết nối điểm nối điểm này thường được thuê từ các nhà cung cấp nên gọi là đường thuê riêng. Nhà cung cấp dành riêng một băng thông cố định cho thuê bao. Nói chung phương pháp này có chi phí cao theo băng thông và khoảng cách giữa các thuê bao.

Bảng thông kê nối mạng điện rộng



14-6

Bảng thông để chỉ tốc độ dữ liệu truyền trên đường truyền. Có hai phân biệt giữa hệ Bắc Mỹ và Âu Châu. Tại Bắc Mỹ, bảng thông thường được tính theo DS0, DS1, ... Với tốc độ cơ sở là DS0 = 64Kbps. 24 DS0 = DS1 = T1 = 1.544Mbps. 28 DS1 = DS3 = T3 = 43.736Mbps.

In similar, E1 = 2.048Mbps và E3 = 34.368Mbps là các chuẩn Âu Châu.

Cấu hình cổng Serial

Enter global configuration mode.

```
RouterX#configure terminal  
RouterX(config)#[/pre]
```

Specify interface.

```
RouterX(config)#interface serial 0/0/0  
RouterX(config-if)#[/pre]
```

Set clock rate (on DCE interfaces only).

```
RouterX(config-if)#clock rate 64000  
RouterX(config-if)#[/pre]
```

Set bandwidth (recommended).

```
RouterX(config-if)#bandwidth 64  
RouterX(config-if)#exit  
RouterX(config)#exit  
RouterX#[/pre]
```

14-7

Nếu là cổng serial DCE lưu ý phải chọn đúng clock. Mặc định router là thiết bị DTE nhưng có thể cấu hình làm thiết bị DCE. Trong cấu hình back-to-back trong đó modem không được sử dụng, một trong các cổng phải cấu hình là DCE để cung cấp clock.

Chúng ta cũng nên cấu hình băng thông cho các cổng giao tiếp để được sử dụng trong các giao thức định tuyến hoặc RSVP. Băng thông mặc định trong cổng serial là T1. Băng thông này không ảnh hưởng đến băng thông thực sự của kết nối

Lệnh show controller

```
RouterX#show controller serial 0/0/0
HD unit 0, idb = 0x121C04, driver structure at 0x127078
buffer size 1524  HD unit 0, V.35 DTE cable
.
.
.
```

Xem kiểu cổng serial

0222-261

14-8

Xem thông tin về cổng vật lý. Thường được sử dụng để xem kiểm cáp kết nối vào cổng giao tiếp.

Xem xét kết nối điểm nối điểm

Thuận lợi

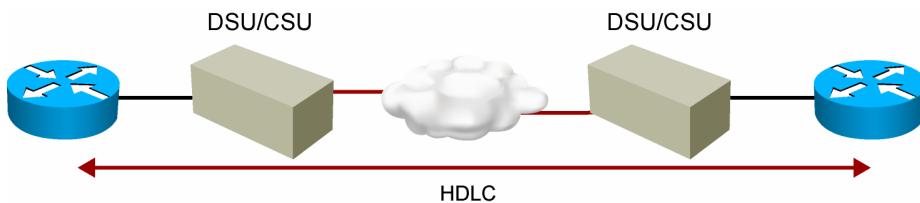
- Đơn giản
- Chất lượng
- Sẵn sàng

Khuyết điểm

- Giá cao
- Giới hạn sự linh hoạt

14-9

HDLC và Cisco HDLC



HDLC

Flag	Address	Control	Data	FCS	Flag
------	---------	---------	------	-----	------

Cisco HDLC

Flag	Address	Control	Proprietary	Data	FCS	Flag
------	---------	---------	-------------	------	-----	------

FCS = Frame Check Sequence

14-10

Chỉ định một phương pháp đóng gói khung dữ liệu trên kết nối bất đồng bộ. Hỗ trợ cả điểm nối điểm và đa điểm. HDLC có thể không tương thích giữa các thiết bị của các nhà sản xuất khác nhau. Cisco HDLC không định nghĩa cơ chế đáp trả theo kiểu cửa sổ trượt và điều khiển dòng, chỉ hỗ trợ điểm nối điểm. Ngoài ra, Cisco HDLC bổ sung một trường mở rộng, cho phép hỗ trợ nhiều giao thức lớp mạng. Do các thay đổi này, Cisco HDLC không thể tương tác với các hiện thực HDLC khác. Trong môi trường như vậy, nên dùng PPP.

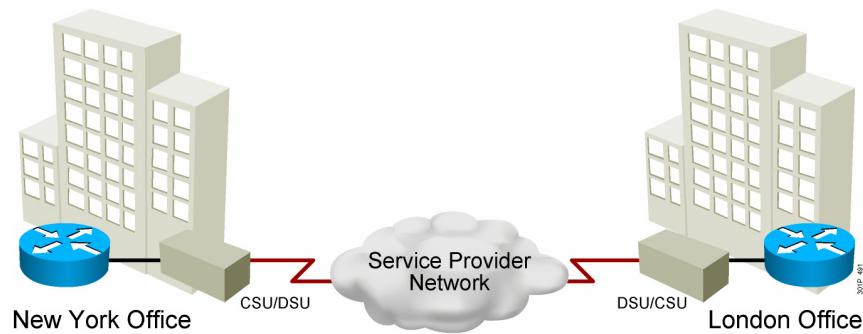
Cấu hình đóng gói HDLC

```
RouterX(config-if)# encapsulation hdlc
```

- Cho phép đóng gói HDLC
- Đây là kiểu đóng gói mặc định trong các cổng serial

14-11

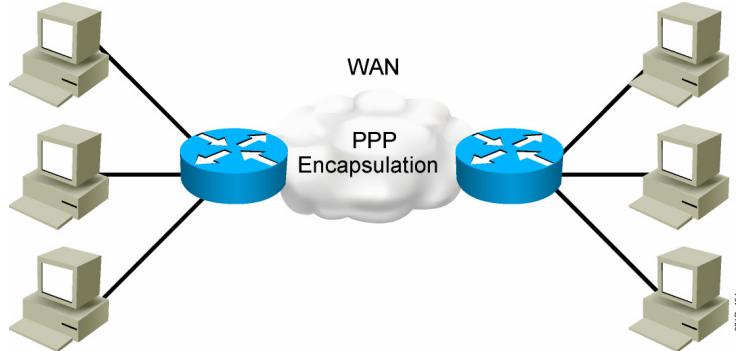
Đường thuê riêng



14-12

Cisco HDLC là một giao thức điểm nối điểm có thể sử dụng trong đường thuê riêng giữa hai Cisco router. Để thông tin với thiết bị của hãng khác, nên dùng PPP thì tốt hơn.

PPP



14-13

Là một giao thức đóng gói ban đầu để mang gói IP trên kết nối điểm đến điểm. PPP cũng thiết lập một chuẩn để gán và quản lý IP địa chỉ, đóng gói đồng bộ hoặc bất đồng bộ, ghép kênh nhiều giao thức lớp mạng, cấu hình đường liên kết, kiểm tra chất lượng đường liên kết, phát hiện lỗi, thỏa thuận các tùy chọn như khả năng thỏa thuận địa chỉ lớp mạng và cơ chế nén.

Ba thành phần chính:

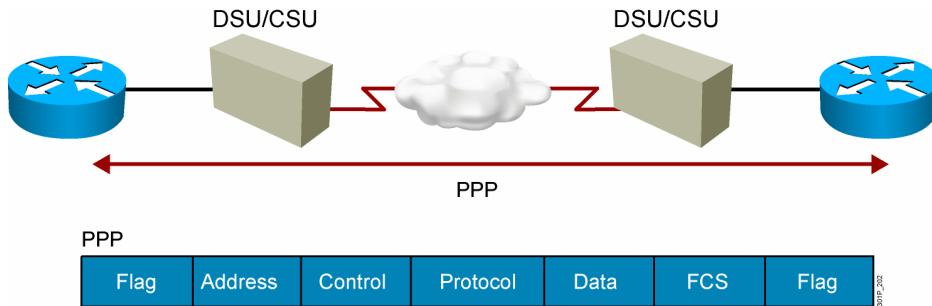
Phương pháp đóng gói nhiều giao thức lớp mạng

Định nghĩa LCP (link control protocol) để tạo, cấu hình, kiểm tra kết nối dữ liệu

Một tập các NCP (network control programs) để tạo và cấu hình các giao thức lớp mạng khác nhau

Xác thực là một chức năng tùy chọn trong PPP. Sau khi liên kết được tạo và chức năng xác thực được chọn. Bên kết nối sẽ cung cấp các thông tin để xác thực để đảm bảo người dùng có thẩm quyền tạo được kết nối

Tổng quan về PPP



- PPP có thể mang gói của nhiều giao thức mạng sử dụng NCP
- PPP kiểm soát và thiết lập các tùy chọn trên liên kết qua LCP

14-14

PPP được thiết kế để tạo các liên kết điểm nối điểm. Mô tả trong RFC 1661 và 1332. RFC 1661 được cập nhật bằng RFC 2153, *PPP Vendor Extensions*.

Chúng ta có thể cấu hình PPP trong các kiểu kết nối vật lý sau:

- Asynchronous serial
- Synchronous serial
- High-Speed Serial Interface (HSSI)

Cho phép đóng gói PPP

```
RouterX(config-if)# encapsulation ppp
```

- Cho phép đóng gói PPP

Cấu hình ví dụ PPP



```
hostname left
!
int serial 0
ip address 10.0.1.1 255.255.255.0
encapsulation ppp
```

```
hostname right
!
int serial 0
ip address 10.0.1.2 255.255.255.0
encapsulation ppp
```

Kiểm tra cấu hình serial

```
RouterX# show interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 10.140.1.2/24
    MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
    Encapsulation PPP, loopback not set, keepalive set (10 sec)
      LCP Open
      Open: IPCP, CDP/PCP
      Last input 00:00:05, output 00:00:05, output hang never
      Last clearing of "show interface" counters never
      Queueing strategy: fifo
      Output queue 0/40, 0 drops; input queue 0/75, 0 drops
      5 minute input rate 0 bits/sec, 0 packets/sec
      5 minute output rate 0 bits/sec, 0 packets/sec
        38021 packets input, 5656110 bytes, 0 no buffer
        Received 23488 broadcasts, 0 runts, 0 giants, 0 throttles
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        38097 packets output, 2135697 bytes, 0 underruns
        0 output errors, 0 collisions, 6045 interface resets
        0 output buffer failures, 0 output buffers swapped out
        482 carrier transitions
      DCD=up  DSR=up  RTS=up  CTS=up
```

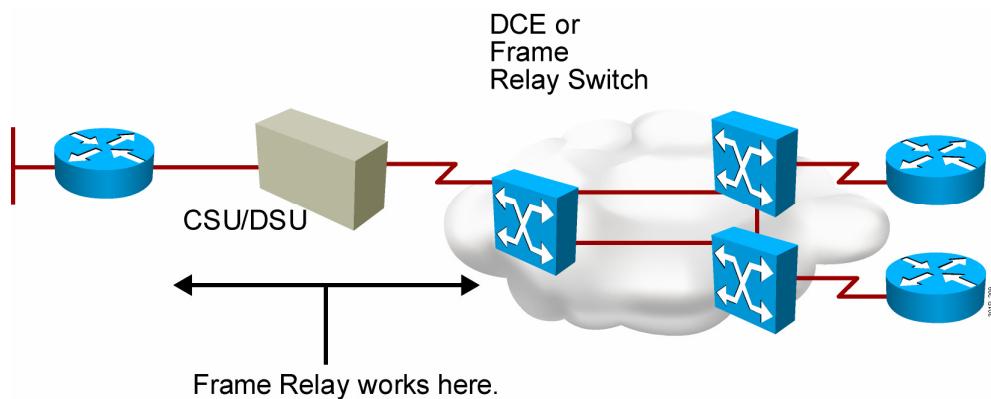
14-17

Kiểm tra đóng gói HDLC và PPP

```
RouterX# show interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is HD64570
    Internet address is 10.140.1.2/24
      MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
      Encapsulation PPP, loopback not set, keepalive set (10 sec)
        LCP Open
          Open: IPCP, CDPCP
          Last input 00:00:05, output 00:00:05, output hang never
          Last clearing of "show interface" counters never
          Queueing strategy: fifo
          Output queue 0/40, 0 drops; input queue 0/75, 0 drops
          5 minute input rate 0 bits/sec, 0 packets/sec
          5 minute output rate 0 bits/sec, 0 packets/sec
            38021 packets input, 5656110 bytes, 0 no buffer
            Received 23488 broadcasts, 0 runts, 0 giants, 0 throttles
            0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
            38097 packets output, 2135697 bytes, 0 underruns
            0 output errors, 0 collisions, 6045 interface resets
            0 output buffer failures, 0 output buffers swapped out
            482 carrier transitions
          DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

14-18

Frame Relay



14-19

Frame Relay là một giao thức chuyển gói được phát triển phổ biến do hiệu quả về chi phí và thay thế các kỹ thuật trước đây là X.25 và đường thuê riêng.

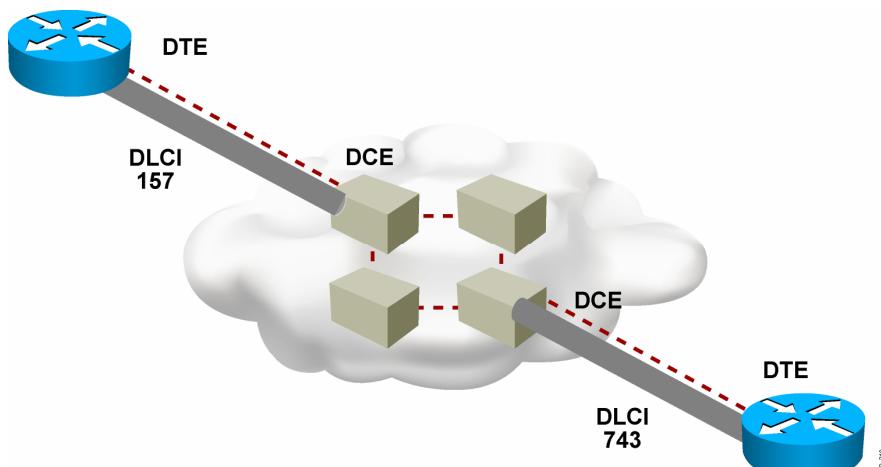
Frame Relay cung cấp các dịch vụ mạch ảo vĩnh viễn (PVC) và mạch ảo chuyên mạch (SVC) trên các kết nối chia sẻ băng thông mang cả thoại và dữ liệu. Tốc độ nói chung lên đến 4Mbps, một số nhà cung cấp còn cho tốc độ cao hơn. Ngoài ra Frame Relay phải đơn giản hóa việc ở lớp liên kết dữ liệu, thay vì ở lớp mạng.

Frame Relay không có cơ chế kiểm tra lỗi và điều khiển dòng. Việc sử lý đơn giản hóa ở đầu khung cho phép giảm thời gian trễ và tránh khung bị tạo lại ở các chuyên mạch trung gian.

Đa số các kết nối Frame Relay là PVC. Kết nối tới các thuê bao từ nhà cung cấp thường là đường thuê riêng, tuy vậy kết nối qua đường điện thoại cũng được sử dụng qua ISDN hoặc xDSL.

Frame Relay lý tưởng cho kết nối các mạng cục bộ doanh nghiệp với nhau bởi vì các router trong mạng cục bộ chỉ cần một cổng serial ngay khi có nhiều mạch ảo tồn tại. Đường dành riêng từ cạnh của nhà cung cấp tới thuê bao cho phép một kết nối hiệu quả về chi phí.

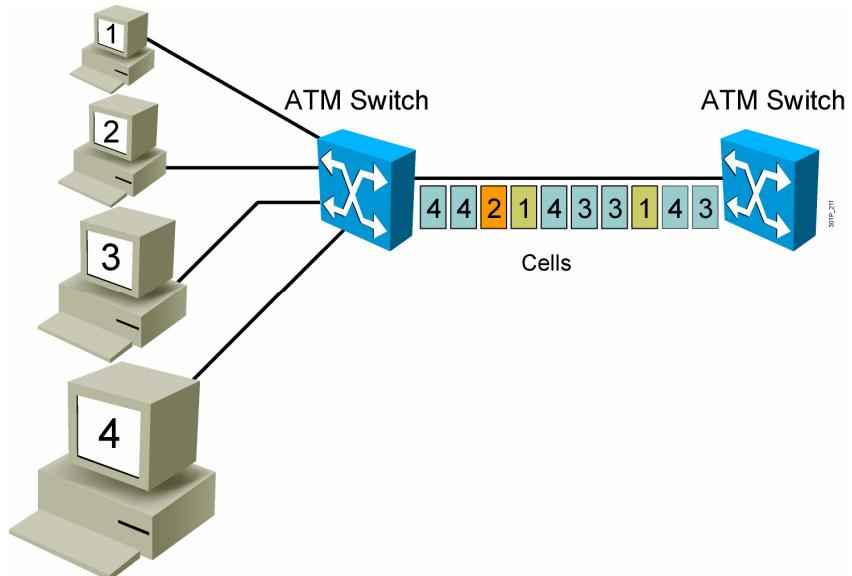
Thiết bị và mạch ảo Frame Relay



14-20

Frame Relay hoạt động trên các mạch ảo trên đó các kết nối logic được tạo và cho phép thông tin giữa hai thiết bị đầu xa với nhau. Mạch ảo là một đường truyền thông song hướng từ một thiết bị DTE này đến một thiết bị DTE khác. DLCI (data-link connection identifier) trong trường địa chỉ của đầu khung Frame Relay dùng để định danh mạch ảo này. Giá trị DLCI này được sử dụng chỉ cho router nơi nó được cấu hình. Mạch ảo có thể băng qua nhiều thiết bị trung giang DCE trong mạng. Nhiều mạch ảo có thể ghép kênh vào trong một đường vật lý tới thuê bao.

ATM và Cell Switching



14-21

ATM là một công nghệ kiểu chuyển gói tế bào mà cho phép truyền thoại, hình ảnh và dữ liệu qua mạng riêng hoặc mạng công cộng. ATM được sử dụng chính trong xương sống mạng doanh nghiệp hoặc trên mạng diện rộng.

ATM có tốc độ lên trên 155Mbps. Về sơ đồ hình học, ATM không khác so với các công nghệ dùng chung khác như X.25 và Frame Relay. ATM dựa trên kiến trúc khung nhỏ như tế bào. Tế bào ATM có kích thước 53 bytes bao gồm 5 bytes đầu khung và 48 bytes dữ liệu. Kích thước nhỏ và cố định thích hợp cho truyền thoại và hình ảnh động bởi các dữ liệu này nhạy cảm với sự trễ.

Kích thước 53 bytes là ít hiệu quả hơn Frame Relay và X.25. Hơn nữa ATM có 5 bytes thêm vào làm đầu khung, khi mang các gói lớp mạng thực chất các byte thêm vào còn lớn hơn vì phần dữ liệu 48 bytes sẽ không phù hợp với kích thước gói (64 bytes). Do đó ATM cần nhiều hơn 20% băng thông so với Frame Relay khi mang cùng một số lượng dữ liệu.

Giống như Frame Relay, ATM sử dụng các mạch ảo và có thể là PVC hoặc SVC. Trong đầu tế bào, chứa một trường gọi là VPI/VCI (virtual path identifier/virtual channel identifier) để xác định mạch ảo nào mà tế bào sử dụng. Ở lớp vật lý, ATM chạy trên nhiều phương tiện như SONET/SDH hoặc cáp đồng trục.

Tóm tắt

- Đường điểm nối điểm có thể kết nối 2 vị trí xa nhau. Đường này thường là đường thuê từ nhà cung cấp, nên được gọi là đường thuê riêng.
- Băng thông để chỉ tốc độ truyền trên một liên kết truyền thông Ở Bắc Mỹ, băng thông thường chỉ định bằng các ký hiệu DS0, DS1...
- Giao thức HDLC là một trong các giao thức lớp liên kết dữ liệu chính sử dụng cho kết nối điểm nối điểm
- Lệnh **encapsulation hdlc** sử dụng để cấu hình HDLC.
- PPP có thể sử dụng trên kết nối đồng bộ hoặc bất đồng bộ và hỗ trợ mang nhiều loại giao thức lớp mạng

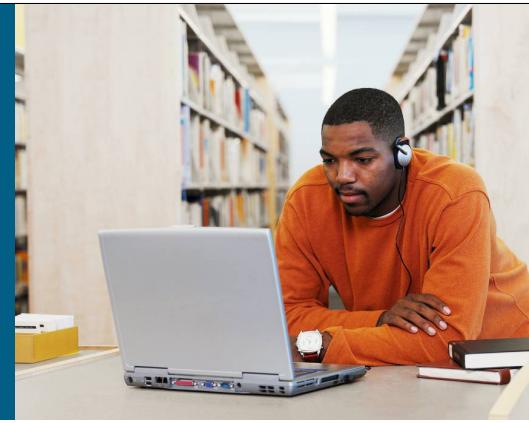
Tóm tắt (Tiếp)

- Lệnh **encapsulation ppp** để cấu hình PPP
- Lệnh **show interface** sử dụng để kiểm tra cấu hình PPP hoặc HDLC.
- Tốc độ Frame Relay có thể lên đến 4 Mb/s hoặc cao hơn. Frame Relay là giao thức đơn giản làm việc ở lớp liên kết dữ liệu.
- ATM là kiểu liên kết chuyển gói kiểu tế bào có khả năng truyền thoại, hình ảnh động và dữ liệu. ATM được sử dụng chính trong mạng của các nhà cung cấp và xương sống mạng doanh nghiệp.
- Các mạch ảo trong ATM hoặc là PVCs hoặc là SVCs.

14-23



Bài 15: Cấu hình RIP

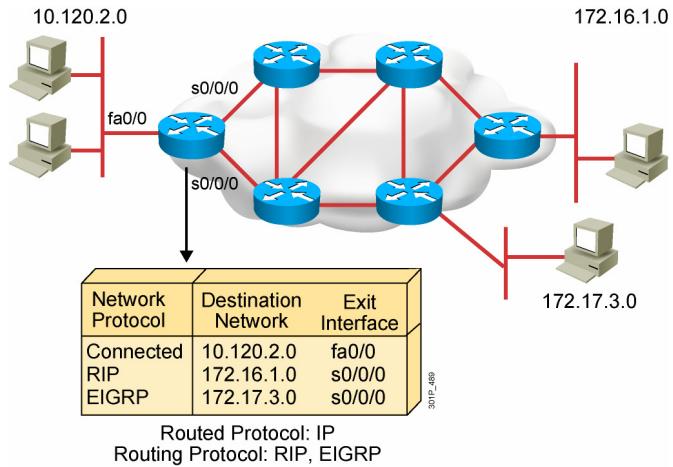


Kết nối mạng diện rộng

15-1

Giao thức định tuyến là gì?

- Giao thức định tuyến được sử dụng giữa các router để xác định đường đi và duy trì bản định tuyến
- Sau khi đường đi đã được xác định, một router có thể định tuyến các gói của giao thức lớp mạng

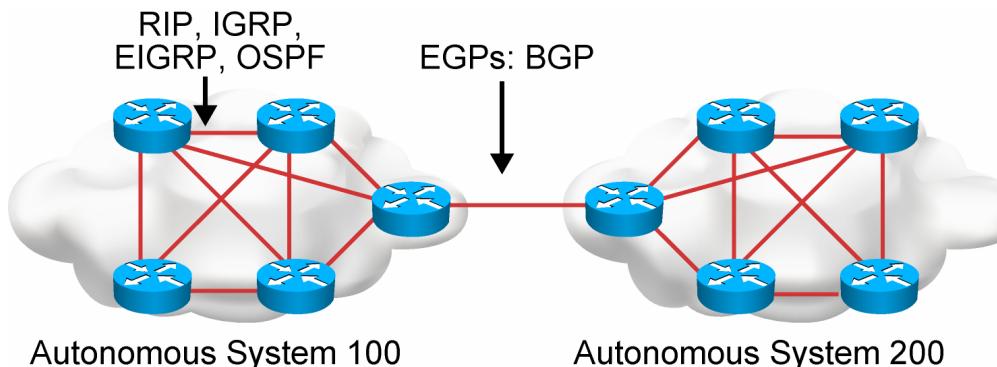


15-2

Giao thức định tuyến mô tả các nguyên tắc để router có thể thông tin với các router khác. Việc định tuyến động dựa vào các giao thức định tuyến. Thông tin mà giao thức định tuyến xác định có thể bao gồm:

- Làm thế nào cập nhật được thực hiện
- Thông tin cập nhật bao gồm những gì
- Khi nào thì việc cập nhật xảy ra
- Việc cập nhật này gửi tới ai

Autonomous Systems: Interior or Exterior Routing Protocols



001G_194

- Một Autonomous System là một tập những mạng dưới một vùng quản trị chung
- IGPs hoạt động bên trong một autonomous system.
- EGPs kết nối các autonomous systems khác nhau.

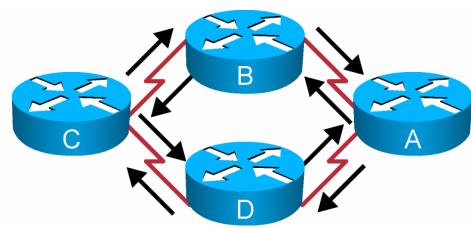
15-3

Có hai kiểu giao thức định tuyến:

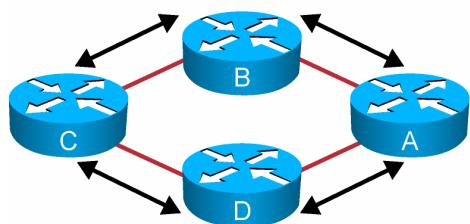
- Interior gateway protocols (IGPs):** như RIPv1, RIPv2, EIGRP, OSPF, IS-IS.
- Exterior gateway protocols (EGPs):** như BGP4

Lớp các giao thức định tuyến

Distance Vector



Hybrid Routing



Link-State

301P_196

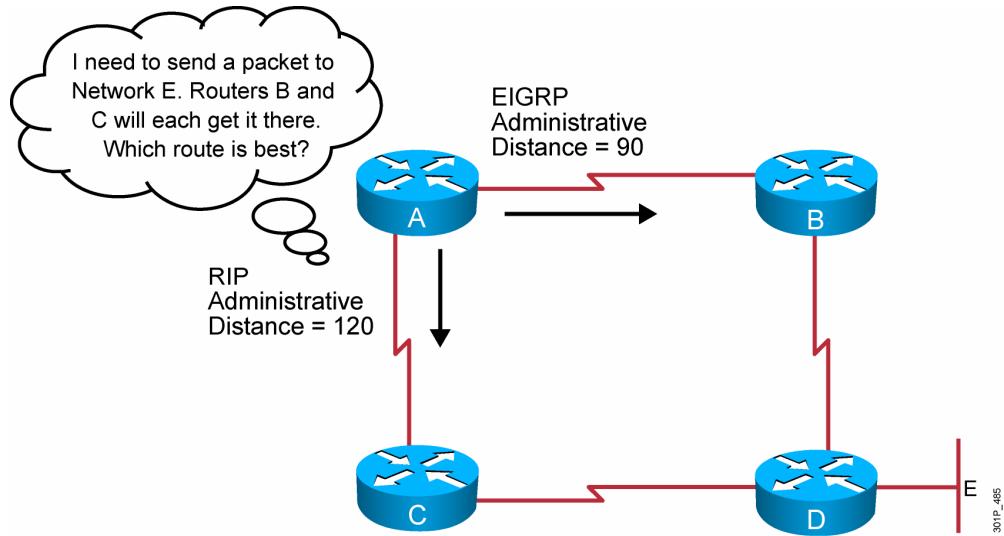
Trong một Autonomous Systems các giao thức định tuyến phân làm các lớp theo thuật giải như sau:

Distance vector: Xác định hướng và khoảng cách tới các liên kết trong mạng.

Link state: còn gọi là thuật toán tìm đường đi ngắn nhất, tạo một cơ sở dữ liệu phản ánh chính xác toàn bộ hoặc một phần sơ đồ hình học của mạng.

Balanced hybrid: Tối ưu hóa các ưu điểm của link-state và distance vector.

Administrative Distance: Đánh giá các tuyến



Administrative distance để đánh giá mức độ tin tưởng đến một nguồn cung cấp thông tin định tuyến, như một router riêng lẽ hay một nhóm router. Giá trị mặc định cho định tuyến tĩnh và một vài giao thức là hiện diện trong Student Guide. Giá trị AD càng thấp thì tuyến đó càng được tin tưởng.

Giao thức định tuyến kiểu Classful

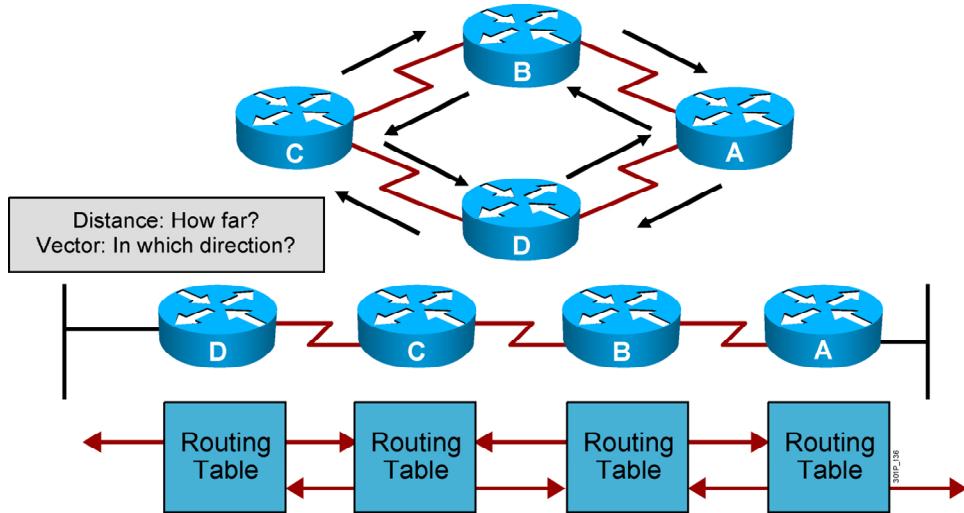
- Giao thức định tuyến kiểu Classful không bao gồm subnet mask trong quảng bá các tuyến
- Trong cùng một major network cần các subnet mask giống nhau.
- Việc nhóm các tuyến là mặc định khi gởi ra ngoài.
- Các hai giao thức:
 - RIPv1
 - IGRP

76

Khi nhận một gói tin cận nhật tuyến, một router chạy giao thức định tuyến theo kiểu classful thực hiện các hoạt động sau để xác định phần địa chỉ mạng của một tuyến:

- Nếu thông tin cập nhật chứa tuyến cùng một địa chỉ mạng chính với địa chỉ cấu hình ở cổng giao tiếp nơi nó nhận cập nhật. Router sử dụng subnet mask của cổng nhận được.
- Nếu thông tin cập nhật chứa tuyến có địa chỉ mạng chính khác với địa chỉ mạng chính của cổng giao tiếp nhận, thì router sẽ sử dụng subnet mask mặc định của lớp mạng địa chỉ đó:
 - Nếu địa chỉ lớp A, mask mặc định là 255.0.0.0.
 - Nếu địa chỉ lớp B, mask mặc định là 255.255.0.0.
 - Nếu địa chỉ lớp C, mask mặc định là 255.255.255.0.

Giao thức định tuyến Distance Vector



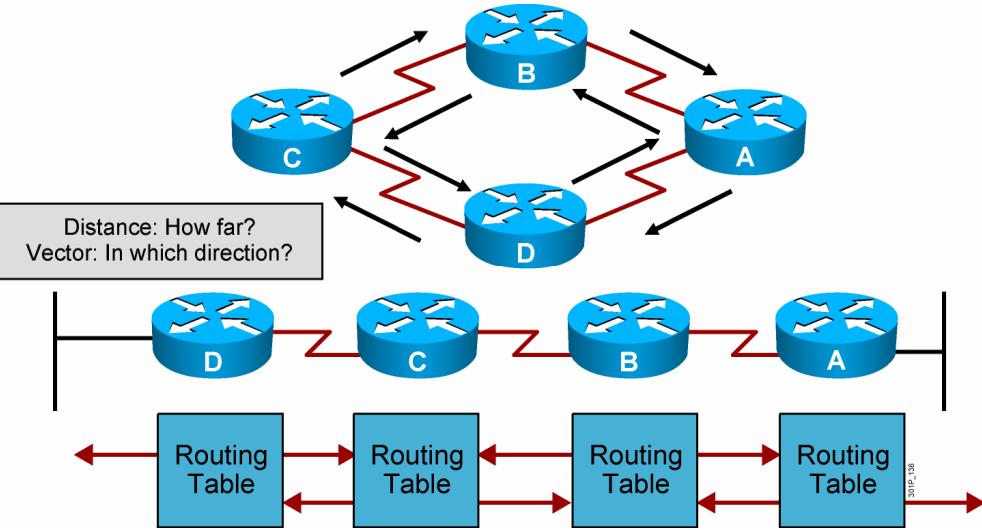
- Routers pass periodic copies of their routing table to neighboring routers and accumulate distance vectors

78

Đây có thể được xem như các giao thức định tuyến thế hệ thứ 2 bởi vì nó được thiết kế để khắc phục các giới hạn của giao thức định tuyến classful trước đây. Giới hạn chính là buộc phải dùng các subnet mask giống nhau cho cùng một địa chỉ mạng chính và khả năng điều khiển việc nhóm các tuyến bị giới hạn ở tự động nhóm tại biên của địa chỉ mạng chính.

Trong môi trường classless, quá trình nhóm được điều khiển dễ dàng và có thể thực hiện ở bất kỳ vị trí bit nào trong địa chỉ. Bởi vì các tuyến subnet được lan truyền qua suốt vùng định tuyến, khả năng nhóm thủ công có phép giữ kích thước của bảng định tuyến ở mức có thể quản lý được.

Giao thức định tuyến Distance Vector



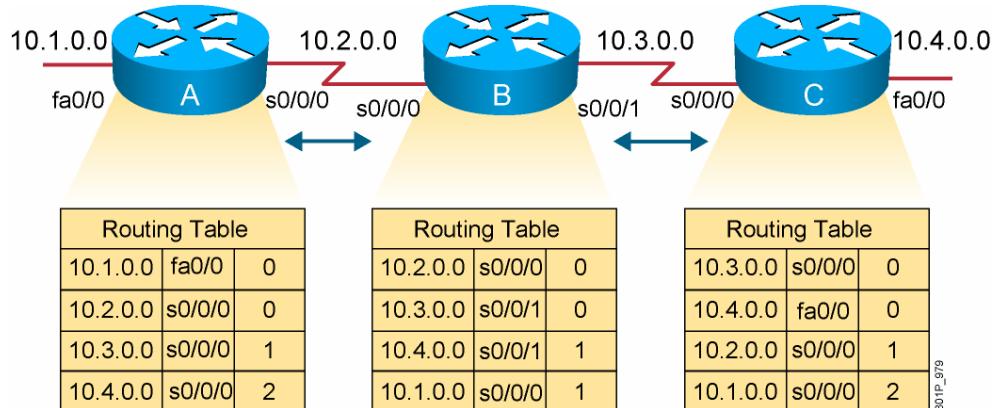
- Routers pass periodic copies of their routing table to neighboring routers and accumulate distance vectors

15-8

Giao thức định tuyến distance vector gửi các cập nhật theo chu kỳ thời gian tới các router kết nối trực tiếp. Địa chỉ mà đa số các router sử dụng để gửi là địa chỉ quảng bá (broadcast). Nó vẫn gửi các cập nhật theo chu kỳ ngay cả khi nó không có sự thay đổi nào. Cập nhật bao gồm toàn bộ bảng định tuyến.

Khi nhận một bảng định tuyến của router kế cận, router sẽ kiểm tra để xem tất cả các tuyến mình đã biết hay chưa và tiến hành cập nhật bảng định tuyến của mình dựa trên các thông tin đó. Quá trình này còn được gọi là “định tuyến theo tin đồn” bởi router hiểu được mạng thông qua router láng giềng.

Hoạt động của Distance Vector



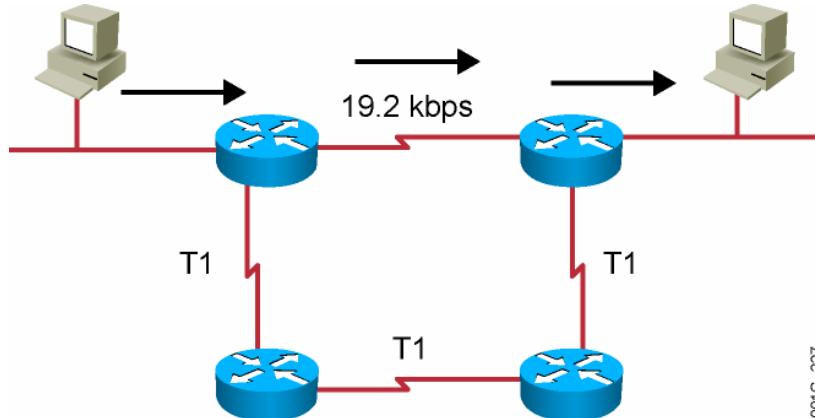
- Router xác định đường tốt nhất tới mạng đích từ mỗi láng giềng

15-9

Trong hình, các mạng kết nối trực tiếp tới các cổng có khoảng cách là 0

Do quá trình hoạt động liên tục của distance vector, router sẽ khám phá ra các đường đi tới các mạng không kết nối trực tiếp khác từ tổng tích lũy metric từ các router láng giềng.

Tổng quan RIP



001G_227

- Số đường đi bằng metric nhau tối đa 16 (mặc định = 4)
- Metric là số router tuyến đó đi qua
- Router gửi cập nhật theo chu kỳ 30 giây

15-10

Các đặc điểm của RIP như sau:

- RIP là giao thức loại distance vector.
- Metric là số router tuyến đi qua.
- Số router một tuyến đi qua tối đa là 15.
- Các cập nhật gửi theo chu kỳ 30 giây.
- Có khả năng chạy cân tải trên lớn nhất 16 đường bằng metric, mặc định là 4.

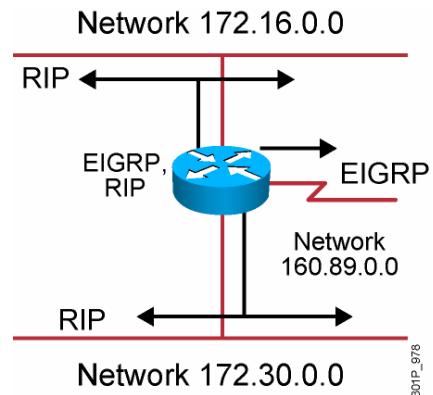
So sánh RIPv1 và RIPv2

	RIPv1	RIPv2
Routing protocol	Classful	Classless
Supports variable-length subnet mask?	No	Yes
Sends the subnet mask along with the routing update?	No	Yes
Addressing type	Broadcast	Multicast
Defined in ...	RFC 1058	RFCs 1721, 1722, and 2453
Supports manual route summarization?	No	Yes
Authentication support?	No	Yes

15-11

Các bước cấu hình định tuyến

- Cấu hình router:
 - Chọn giao thức định tuyến
 - Chọn mạng và giao tiếp



15-12

Cấu hình RIP

```
RouterX(config)# router rip
```

- Bắt đầu một quá trình RIP

```
RouterX(config-router)# version 2
```

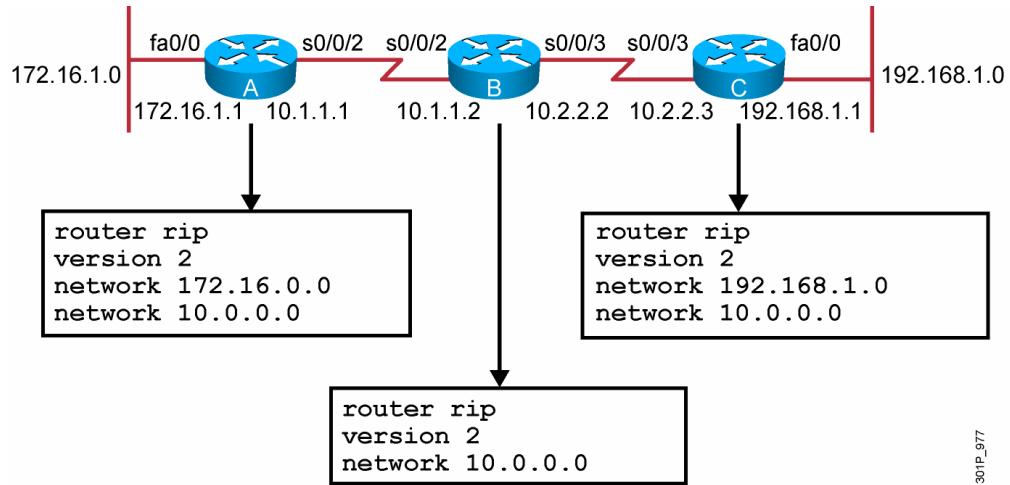
- Cho phép version 2

```
RouterX(config-router)# network network-number
```

- Chọn các mạng thành viên tương ứng các cổng
- Chỉ chọn địa chỉ mạng chính

15-13

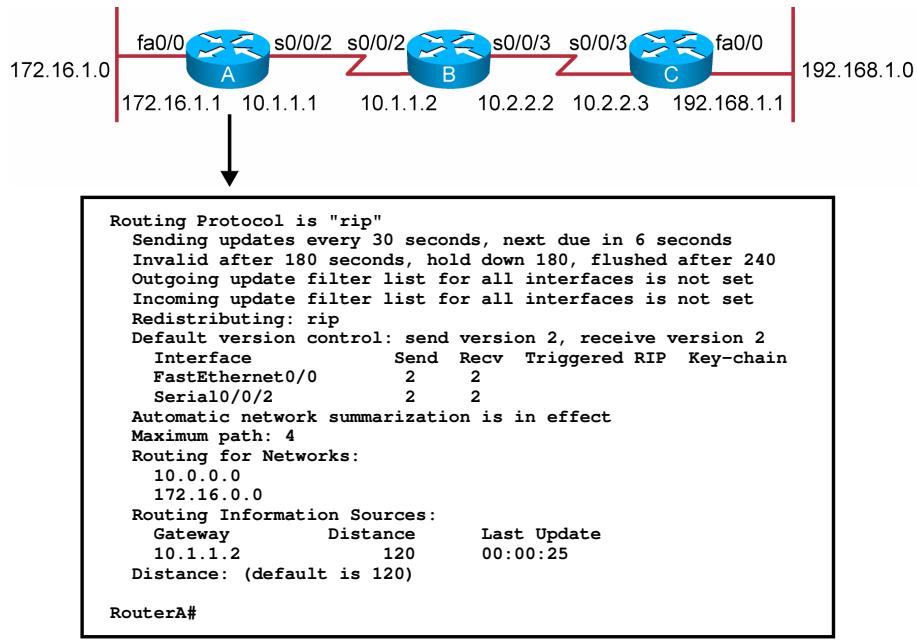
Ví dụ cấu hình RIP



301IP_977

15-14

Kiểm tra cấu hình RIP

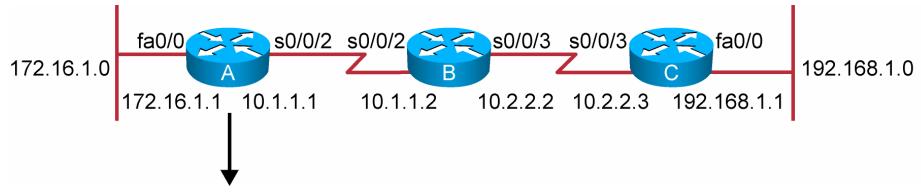


SC/P-376

15-15

Router A được cấu hình để gửi nhận RIP theo chu kỳ 30 giây. Nếu router không nhận được một cập nhật của một tuyến trong khoảng 180 giây, nó sẽ đánh dấu tuyến này là invalid. Hold-down là 180 giây, có nghĩa là nếu một cập nhật của một tuyến đang bị invalid, nó phải đợi cho hết thời gian này nếu cập nhật mới có metric lớn hơn hay bằng metric đang bị invalid đó. Nếu vẫn không có cập nhật trong 240 giây, router sẽ loại tuyến này ra khỏi bảng định tuyến

Xem bảng định tuyến



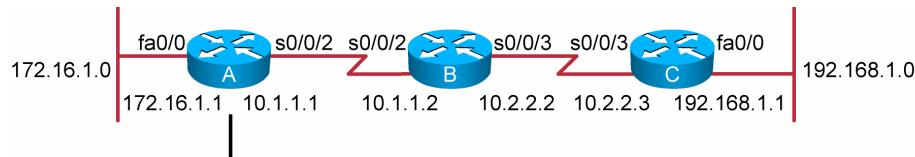
```
RouterA# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E -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

Gateway of last resort is not set

      172.16.0.0/24 is subnetted, 1 subnets
C        172.16.1.0 is directly connected, fastethernet0/0
          10.0.0.0/24 is subnetted, 2 subnets
R        10.1.1.0 [120/1] via 10.1.1.2, 00:00:07, Serial0/0/2
C        10.1.1.0 is directly connected, Serial0/0/2
R        192.168.1.0/24 [120/2] via 10.1.1.2, 00:00:07, Serial0/0/2
```

15-16

Lệnh debug ip rip



```
RouterA# debug ip rip
RIP protocol debugging is on
RouterA#
00:06:24: RIP: received v1 update from 10.1.1.2 on Serial0/0/2
00:06:24:   10.2.2.0 in 1 hops
00:06:24:   192.168.1.0 in 2 hops
00:06:33: RIP: sending v1 update to 255.255.255.255 via FastEthernet0/0 (172.16.1.1)
00:06:34:   network 10.0.0.0, metric 1
00:06:34:   network 192.168.1.0, metric 3
00:06:34: RIP: sending v1 update to 255.255.255.255 via Serial0/0/2 (10.1.1.1)
00:06:34:   network 172.16.0.0, metric 1
```

15-17

Tóm tắt

- Định tuyến là quá trình mà chuyển một gói tin từ vị trí này sang vị trí khác trên môi trường liên mạng.
- Các giao thức định tuyến động xác định làm thế nào các cập nhật được chuyển đi, kiến thức gì được chuyển đi, xác định ai sẽ nhận và khi nào sẽ chuyển đi.
- Giao thức định tuyến có AD càng nhỏ thì càng được tin cậy.
- Có 3 lớp giao thức định tuyến: distance vector, link-state, và balanced hybrid.
- Lệnh **ip classless** có thể được sử dụng để ngăn chặn một router hủy một gói tin mà gửi tới một mạng con không được biết nếu một tuyến mặc định tồn tại.

15-18

Tóm tắt (tiếp)

- RIP là một giao thức định tuyến theo lớp distance vector mà sử dụng metric là số router mà tuyến đi qua và quảng bá các cập nhật 30 giây một lần.
- RIPv1 là loại classful; RIPv2 là loại classless. RIPv2 hỗ trợ VLSM, nhóm tuyến nhân công, xà xác thực; trong khi RIPv1 không hỗ trợ
- Cho phép định tuyến động, đầu tiên phải chọn một giao thức sau đó cấu hình các địa chỉ mạng của các cổng giao tiếp của router.
- Lệnh **router** để tạo một quá trình định tuyến. Lệnh **network** để cho phép quá trình định tuyến xác định cổng giao tiếp nào sẽ tham gia việc gởi nhận các cập nhật định tuyến.

15-19

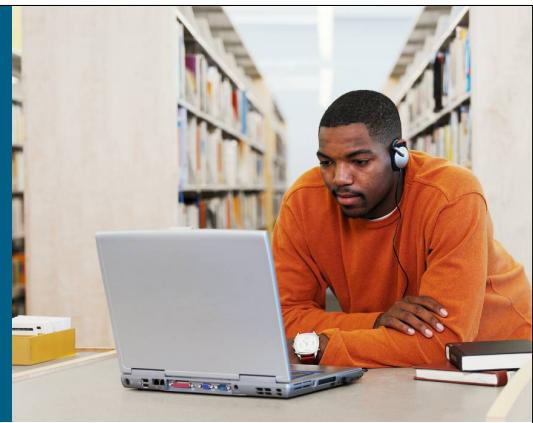
Tóm tắt (tiếp)

- Lệnh **router RIP** để chọn RIP làm giao thức định tuyến. Lệnh **network** để chỉ định sự tham gia của một mạng thành viên.
- Lệnh **show ip** hiển thị thông tin về giao thức định tuyến và bảng định tuyến.
- Lệnh **debug ip rip** hiển thị các thông tin về quá trình định tuyến làm việc

15-20



Bài 16: Discovering Neighbors on the Network



Network Environment Management

16-1

Cisco Discovery Protocol

Upper-Layer Entry Addresses	TCP/IP	Novell IPX	AppleTalk	Others
Cisco Proprietary Data-Link Protocol	Cisco Discovery Protocol discovers and displays information about directly connected Cisco devices.			
Media Supporting SNAP	LANs	Frame Relay	ATM	Others

- Cisco Discovery Protocol is a proprietary utility that provides a summary of directly connected switches, routers, and other Cisco devices.
- Cisco Discovery Protocol discovers neighboring devices, regardless of which protocol suite they are running.
- Physical media must support the SNAP encapsulation.

16-2

Cisco Discovery Protocol (CDP) là một công cụ mà người quản trị mạng sử dụng để thu thập thông tin về các thiết bị Cisco kết nối trực tiếp. Phần này mô tả mục đích và tính năng của CDP

CDP là một công cụ thích hợp cho phép bạn thu thập những thông tin tóm tắt về giao thức (protocol) và địa chỉ của các thiết bị Cisco mà chúng kết nối trực tiếp với thiết bị Cisco ta đang gõ những lệnh CDP.

CDP hoạt động ở tầng Data Link. Vì thế hai hay nhiều thiết bị mạng, ví dụ như router hỗ trợ nhiều giao thức tầng network (IP, Novel IPX), có thể biết về cái khác.

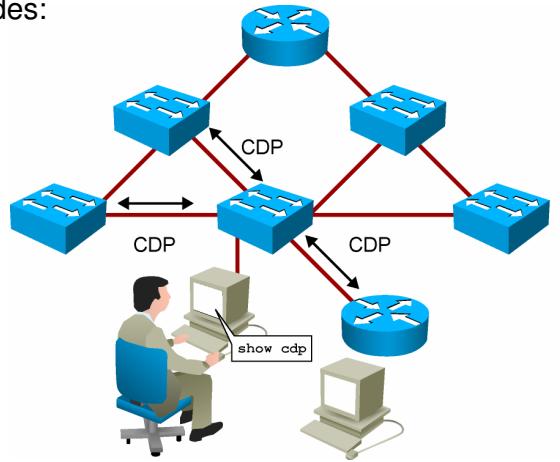
Phương tiện vật lý mà kết nối những thiết bị CDP phải hỗ trợ cách đóng gói dữ liệu Subnetwork Access Protocol (SNAP). Những mạng hỗ trợ bao gồm LANs, Frame Relay, WANs khác và ATM

Khi một thiết bị Cisco khởi động, mặc định CDP đã được start, và phát hiện những thiết bị Cisco đang chạy CDP kết nối trực tiếp với nó một cách tự động, bắt cháp những họ protocol đang chạy

Chú ý: CDP gửi frame theo dạng multicast với địa chỉ 0100.0ccc.cccc.

Discovering Neighbors with Cisco Discovery Protocol

- Cisco Discovery Protocol runs on Cisco IOS devices.
- Summary information includes:
 - Device identifiers
 - Address list
 - Port identifier
 - Capabilities list
 - Platform



16-3

Hình vẽ hiển thị một ví dụ về cách thức CDP trao đổi thông tin với những thiết bị kết nối trực tiếp (neighbor). Bạn có thể hiển thị kết quả của sự trao đổi này thông qua cổng console kết nối đến thiết bị mạng đang chạy CDP

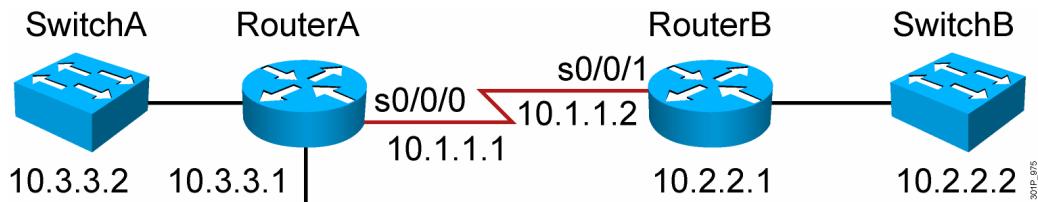
CDP cung cấp những thông tin của neighbor như sau:

- Device identifiers: ví dụ, tên của switch hay router
- Address list: địa chỉ tầng network tương ứng với protocol được hỗ trợ
- Port identifier: tên của port cục bộ và port ở xa dưới hình thức ASCII, ví dụ ethernet0
- Capabilities list: những tính năng được hỗ trợ; ví dụ, thiết bị đang hoạt động như một source-route bridge hay như một router
- Platform: phần cứng của thiết bị; ví dụ, cisco 7200 Series Router

Chú ý, router trong hình vẽ không được kết nối đến cổng console của người quản trị. Để biết về những thông tin của router, người quản trị sẽ telnet đến switch nối trực tiếp với router.

CDP version 2 là phiên bản mới nhất và cung cấp nhiều tính năng thông minh theo dõi thiết bị. Những tính năng này gồm một cơ chế báo cáo (report), mà nó cho phép theo dõi lỗi nhanh hơn, vì thế giảm thời gian down. Những message thông báo lỗi có thể gửi đến console hay logging server.

Using Cisco Discovery Protocol



```
RouterA#show cdp ?
  entry      Information for specific neighbor entry
  interface   CDP interface status and configuration
  neighbors   CDP neighbors entries
  traffic    CDP statistics
  <cr>
RouterA(config)#no cdp run
RouterA(config)#interface serial0/0/0
RouterA(config-if)#no cdp enable
```

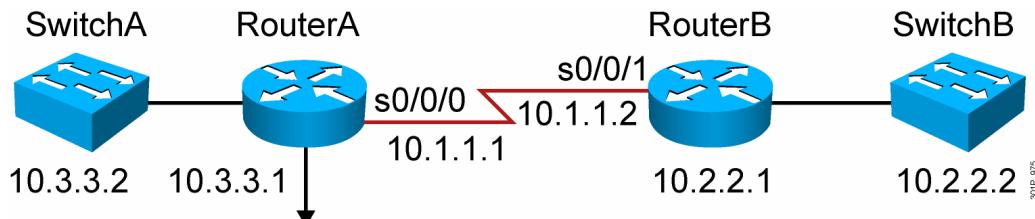
16-4

Note: một vài lệnh CDP không có trên Catalyst 1900 switch, như **cdp run**, **show cdp traffic**, và **show cdp entry**.

Bạn có thể hiển thị thông tin CDP với lệnh **show cdp**. CDP có nhiều từ khóa cho phép truy cập những loại thông tin và mức độ chi tiết khác nhau. Nó được thiết kế và triển khai như là một protocol rất đơn giản, chi phí thấp. Một CDP packet có thể nhỏ bằng 80byte, hầu hết được biểu diễn dạng chuỗi ASCII mà nó được hiển thị như trong hình vẽ.

CDP được cấu hình mặc định trên tất cả interface (ngoại trừ subinterface của Frame Relay multipoint), nhưng có thể loại bỏ tại tầng thiết bị. Tuy nhiên một vài interface, như ATM, không hỗ trợ CDP. Để ngăn chặn những thiết bị khác thu thập thông tin về thiết bị chỉ định, dùng lệnh **no cdp run** ở global configuration . Để loại bỏ CDP ở interface dùng lệnh **no cdp enable**. Để cho phép CDP trên interface dùng lệnh **cdp enable** ở interface configuration.

Using Cisco Discovery Protocol

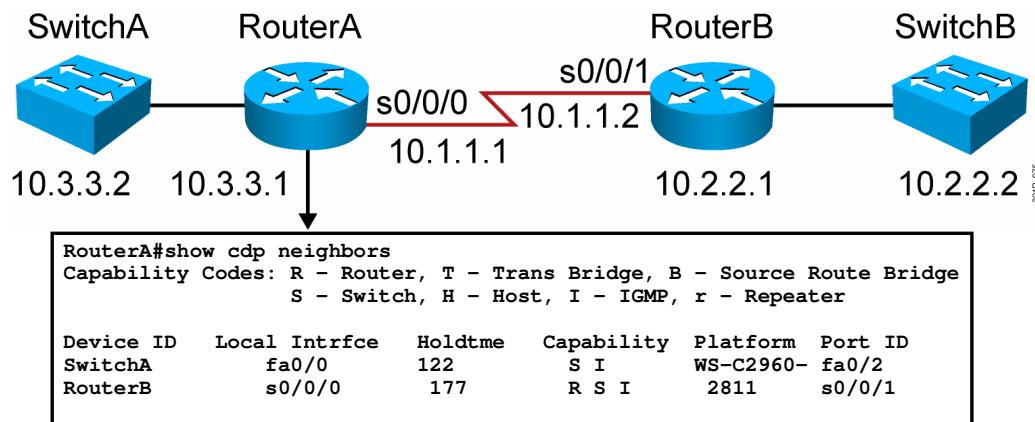


```
RouterA#show cdp ?
  entry      Information for specific neighbor entry
  interface  CDP interface status and configuration
  neighbors  CDP neighbor entries
  traffic    CDP statistics
  ...
RouterA(config)#no cdp run
! Disable CDP Globally
RouterA(config)#interface serial0/0/0
RouterA(config-if)#no cdp enable
! Disable CDP on just this interface
```

16-5

Note: một vài lệnh CDP không có trên Catalyst 1900 switch, như **cdp run**, **show cdp traffic**, và **show cdp entry**.

Using the show cdp neighbors Command



Hình vẽ hiển thị kết quả của lệnh **show cdp neighbors** trên router A. mỗi neighbor gồm những thông tin sau:

- Mã nhận diện thiết bị
- Interface cục bộ
- Giá trị holdtime, tính bằng giây
- Mã khả năng của thiết bị
- Phản ứng của thiết bị
- Mã nhận diện port ở xa

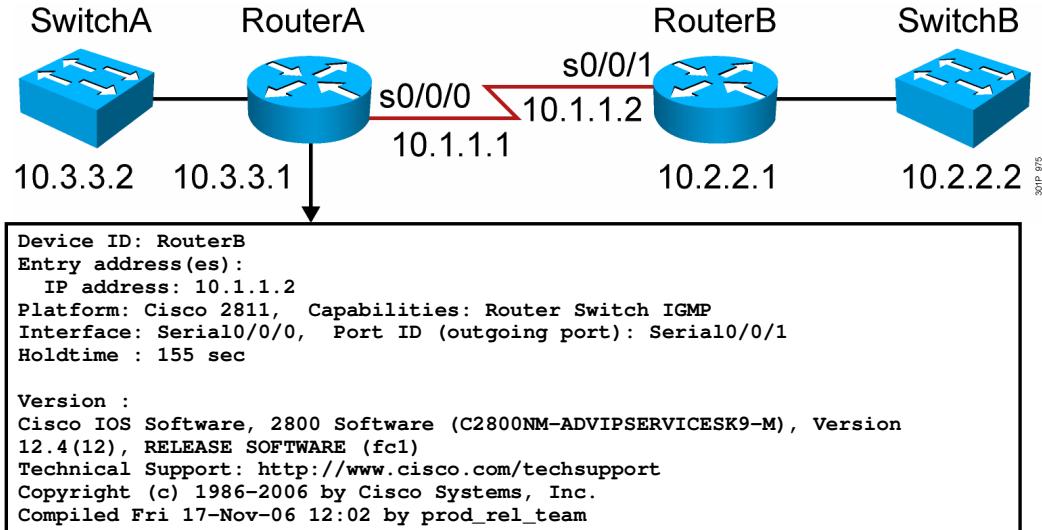
Giá trị holdtime chỉ ra sẽ giữ CDP packet trong bao lâu nữa trước khi hủy nó

Định dạng của kết quả lệnh **show cdp neighbors** khác nhau giữa những loại thiết bị khác nhau, nhưng những thông tin có sẵn thường cố định.

Lệnh **show cdp neighbors** có thể được sử dụng trên Cisco switch để hiển thị những CDP packet được nhận trên interface cục bộ. Chú ý trên switch, interface cục bộ được xem như là local port

Nếu bạn thêm **detail** vào lệnh **show cdp neighbors**, kết quả hiển thị sẽ có thêm những thông tin, như địa chỉ tầng network của neighbor. Kết quả lệnh **show cdp neighbors detail** giống lệnh **show cdp entry ***

Using the show cdp entry Command



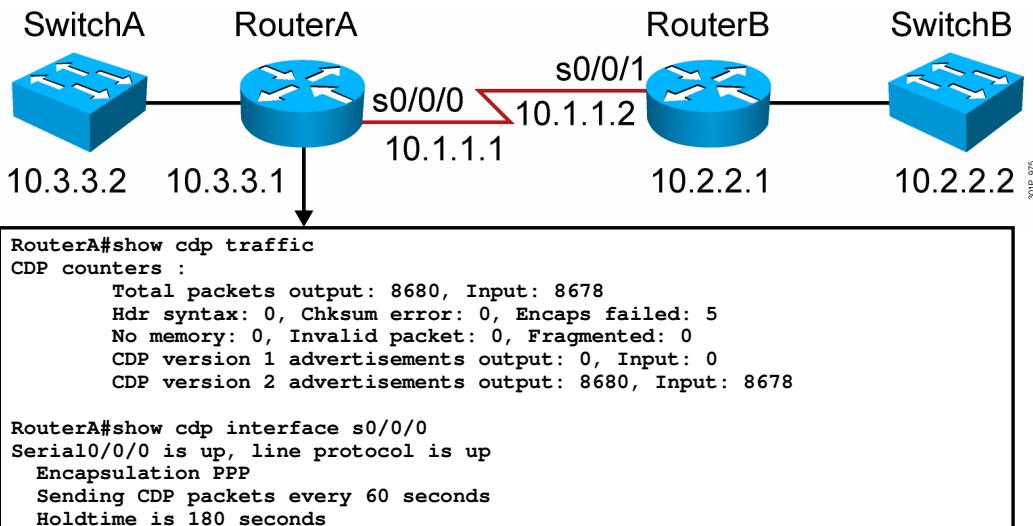
16-7

Lệnh **show cdp entry** hiển thị thông tin chi tiết về những thiết bị neighbor. Để hiển thị thông tin của một neighbor chỉ định, phải thêm địa chỉ IP hoặc device ID của neighbor vào lệnh. Dấu (*) được sử dụng để hiển thị thông tin của tất cả neighbor. Kết quả của lệnh **show cdp entry** như sau:

- Mã nhận dạng neighbor
- Thông tin về protocol tầng network (ví dụ địa chỉ IP)
- Phần cứng thiết bị
- Khả năng thiết bị
- Loại interface cục bộ và mã nhận diện port ở xa
- Giá trị holdtime, tính bằng giây
- Loại Cisco IOS software và phiên bản

Kết quả của lệnh bao gồm tất cả địa chỉ tầng network của các interface của neighbor (một địa chỉ trên một protocol)

Additional Cisco Discovery Protocol Commands



16-8

Note: giá trị holdtime chỉ ra thông tin của neighbor sẽ được giữ bao lâu trong bảng CDP.

Lệnh **show cdp traffic** hiển thị thông tin về sự vận chuyển thông tin của interface. Nó chỉ ra số CDP packet đã gửi và nhận. Nó cũng hiển thị packet bị lỗi với những lỗi sau:

- Syntax (cấu trúc)
- Checksum
- Encapsulation (đóng gói)
- Vượt khỏi bộ nhớ
- Packet không giá trị
- Packet bị phân đoạn
- Số CDP packet version 1 đã gửi
- Số CDP packet version 2 đã gửi

Lưu ý: lệnh show cdp traffic không có trên Catalyst 1900 switch

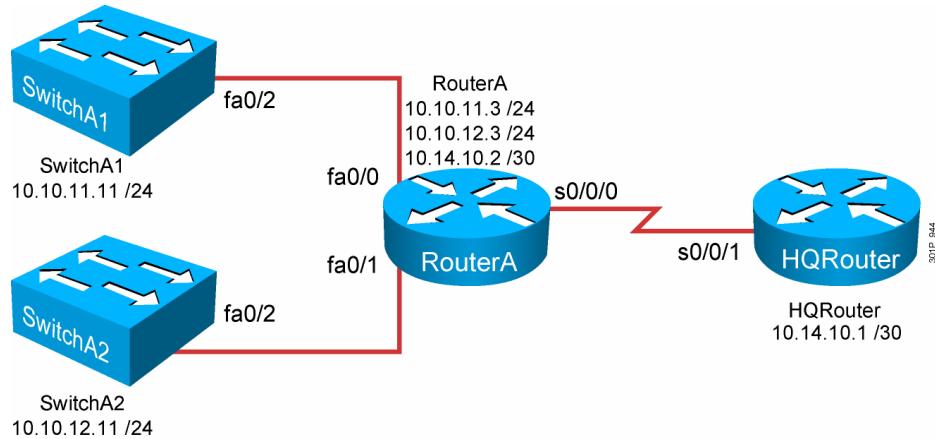
Lệnh **show cdp interface** hiển thị thông tin trạng thái và cấu hình về interface của thiết bị cục bộ:

- Trạng thái tầng physical và data-link của interface
- Loại encapsulation của interface

- Tần suất CDP packet được gửi (mặc định 60 giây)
- Giá trị holdtime, tính bằng giây (mặc định 180 giây)

CDP chỉ giới hạn thu thập thông tin của các thiết bị Cisco nối trực tiếp. Công cụ khác, như telnet, cho phép thu thập thông tin của các thiết bị ở xa mà không kết nối trực tiếp.

Creating a Network Map



16-10

Tài liệu về Sơ đồ mạng được sử dụng để hướng dẫn thiết kế hợp lý và để giúp đỡ thiết kế, thay đổi, và xử lý lỗi trong tương lai. Sơ đồ mạng bao gồm sơ đồ vật lý và sơ đồ logic gồm những thông tin sau:

- Cách kết nối
- Địa chỉ
- Loại môi trường truyền
- Thiết bị
- Sắp xếp rack
- Gán card
- Định tuyến cáp
- Nhận dạng cáp
- Điểm ngắt
- Thông tin nguồn

Duy trì tài liệu về sơ đồ mạng chính xác là chìa khóa để quản lý cấu hình thành công. Cisco khuyên rằng cập nhật tài liệu về sơ đồ mạng mỗi khi một thay đổi về mạng xảy ra

Tóm tắt

- Cisco Discovery Protocol is an information-gathering tool used by network administrators to obtain information about directly connected devices.
- Cisco Discovery Protocol exchanges hardware and software device information with its directly connected Cisco Discovery Protocol neighbors.
- Cisco Discovery Protocol on a router can be enabled or disabled as a whole or on a port-by-port basis.
- The **show cdp neighbors** command displays information about the Cisco Discovery Protocol neighbors of a router.
- The **show cdp entry**, **show cdp traffic**, and **show cdp interface** commands display detailed Cisco Discovery Protocol information on a Cisco device.
- Using the information obtained from the **show cdp** command output, a network topology map can be created to aid troubleshooting.

16-11

- CDP là một công cụ thu thập thông tin được người quản trị sử dụng để biết thông tin về những thiết bị đang kết nối trực tiếp
- CDP trao đổi thông tin về phần cứng và phần mềm với những neighbor chạy CDP kết nối trực tiếp
- Trên router, CDP được cấu hình hay hủy bỏ toàn bộ hay trên port
- Lệnh show cdp neighbors hiển thị thông tin về neighbor của router
- Lệnh show cdp entry, show cdp traffic, và lệnh show cdp interface hiển thị thông tin CDP chi tiết
- Sử dụng thông tin từ lệnh show cdp, một sơ đồ mạng có thể được tạo ra để hỗ trợ cho việc troubleshooting



16-12

Bài 17: Quản lý quá trình khởi động và cấu hình của Cisco Router



Network Environment Management

17-1

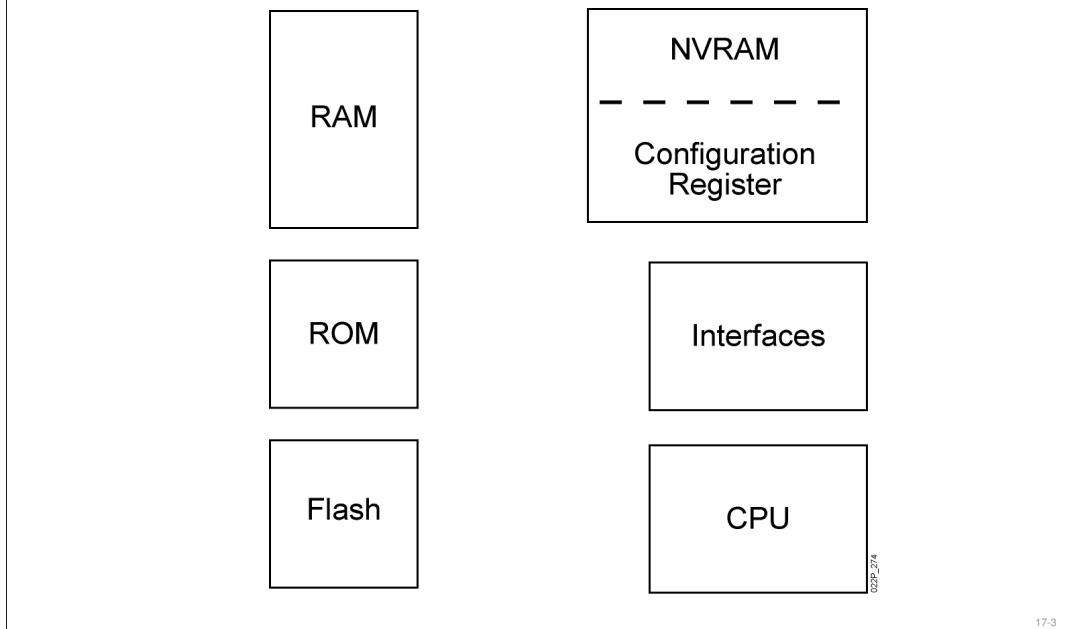
Router Power-On Boot Sequence

1. Perform power-on self-test (POST).
2. Load and run bootstrap code.
3. Find the Cisco IOS Software.
4. Load the Cisco IOS Software.
5. Find the configuration.
6. Load the configuration.
7. Run the configured Cisco IOS Software.

17-2

- Khi router được bật nguồn, thứ tự xảy ra các sự kiện là quan trọng. Biết những thứ tự này sẽ giúp hoàn thành các thao tác và khắc phục lỗi của router. Thứ tự các sự kiện như sau:
 1. Kiểm tra phần cứng (POST): đây là một chuỗi kiểm tra phần cứng để khảng định tất cả phần cứng của router hoạt động tốt. Trong quá trình kiểm tra, router cũng quyết định phần cứng nào được hiển thị. POST thực thi từ một đoạn chương trình nhỏ trong ROM
 2. Tải và chạy đoạn mã bootstrap: đoạn mã bootstrap được sử dụng để thực hiện những sự kiện xảy ra sau này, như tìm IOS, tải nó, và sau đó chạy IOS. Khi IOS được tải và đang chạy, đoạn mã bootstrap không được sử dụng cho đến khi router khởi động lần kế tiếp
 3. Tìm phần mềm(IOS): đoạn mã bootstrap quyết định tìm IOS ở đâu. Thông thường, IOS image được lưu trong bộ nhớ flash. Cấu hình thanh ghi và file cấu hình quyết định tìm IOS image ở đâu và image nào được sử dụng
 4. Tải IOS: khi bootstrap tìm được image phù hợp, sau đó sẽ tải image này vào RAM và khởi động IOS. Một vài router không tải IOS image vào RAM, mà chạy trực tiếp từ flash
 5. Tìm cấu hình: mặc định tìm trong NVRAM nếu file cấu hình (còn gọi là startup-config) được save hợp lý,
 6. Tải cấu hình: file cấu hình được tải và thực thi. Nếu không tồn tại cấu hình, router sẽ đưa vào tiện ích setup hoặc cố gắng tìm file cấu hình từ TFTP Server
 7. Chạy phần mềm đã được cấu hình: bây giờ router đang chạy với IOS đã được cấu hình

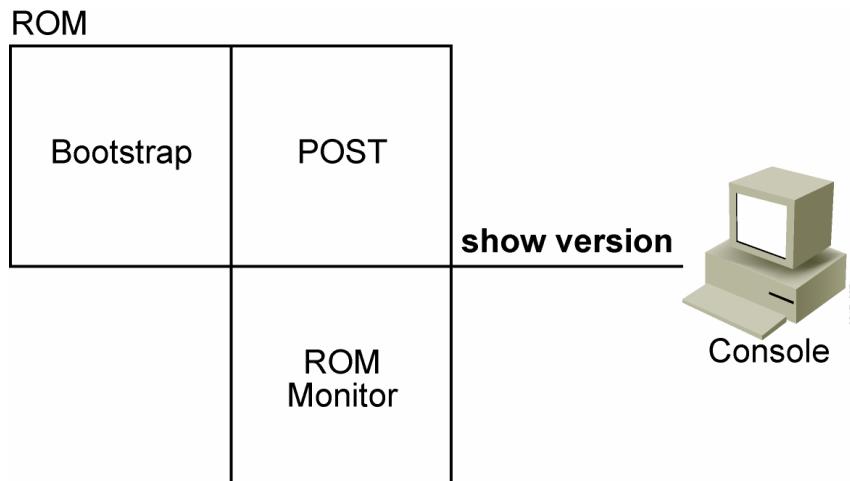
Router Internal Components



Router có các thành phần chính được chỉ ra trong hình vẽ. Hầu hết các thành phần này là phần cứng

- RAM: bộ nhớ có thể đọc/viết, nó chứa IOS và cấu trúc dữ liệu mà cho phép router hoạt động. IOS chính đang chạy trong RAM là Cisco IOS image và cấu hình đang chạy. RAM cũng lưu giữ bảng định tuyến và vùng đệm packet. Bộ nhớ RAM thì thay đổi, nội dung bộ nhớ sẽ bị mất khi tắt nguồn router
- ROM: chứa đoạn mã nhỏ cho phép router hoạt động và duy trì một cách cơ bản, gồm bootstrap và POST. ROM chứa ROM monitor (ROMMON), được sử dụng để khôi phục lỗi của router, như khôi phục password. ROM cũng chứa một IOS image cơ bản (một tập hợp con của IOS), được sử dụng để khôi phục image file, chẳng hạn khi IOS image trong flash bị xóa. ROM ko thay đổi, nội dung ROM không bị mất khi tắt nguồn router
- Flash: bộ nhớ có thể đọc/ghi được sử dụng để lưu IOS image. Một vài router chạy IOS image trực tiếp từ flash và không cần phải tải vào RAM. Một vài router lưu IOS image cơ bản trong flash hơn là ROM. Flash không thay đổi, nội dung flash không bị mất khi tắt nguồn router
- NVRAM: bộ nhớ có thể đọc/ghi được sử dụng để lưu file cấu hình, được gọi là startup-config. NVRAM sử dụng nguồn điện từ pin có sẵn để duy trì dữ liệu khi router tắt nguồn.
- Configuration register: thanh ghi được sử dụng để điều khiển quá trình khởi động router. Thanh ghi là một phần của NVRAM
- Interfaces: là những cổng giao tiếp kết nối router với với thế giới bên ngoài, gồm những loại sau: Ethernet, fast ethernet, gigabit ethernet,...

ROM Functions

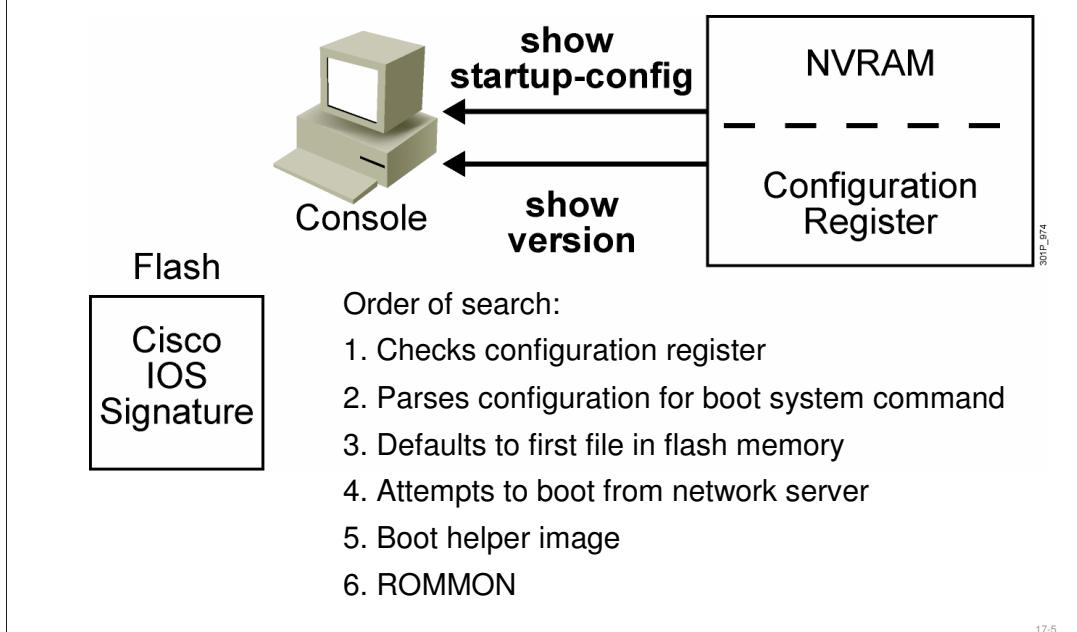


17-4

Đây là 3 microcode được lưu trong ROM:

- Bootstrap: được sử dụng để làm cho router bật lên trong quá trình khởi động. Nó đọc thanh ghi để quyết định cách boot, và sau đó, nếu được chỉ dẫn, tải IOS image
- POST: được sử dụng để kiểm tra tính năng cơ bản của phần cứng router và quyết định phần cứng nào được biểu diễn
- ROMMON: đây là hệ điều hành tàn thấp thường được nhà sản xuất sử dụng, kiểm tra, troubleshooting, và khôi phục password. Trong ROMMON mode, router không có khả năng IP và định tuyến.

Finding the Cisco IOS Image



Bootstrap có nhiệm vụ tìm IOS image. Nó tìm kiếm image theo trật tự sau:

- Bootstrap kiểm tra cột boot trong thanh ghi. Cột Boot là 4 bit thấp của thanh ghi và được sử dụng để chỉ ra cách khởi động của router. Giá trị của cột boot có thể trỏ đến flash, tập tin startup-config, hoặc TFTP Server, hoặc giá trị của cột boot chỉ ra rằng không có IOS image và chỉ khởi động với IOS image cơ bản trong ROM. Những bit trong thanh ghi thực hiện những vai trò khác nhau, như chọn tốc độ của console và có hay không sử dụng file cấu hình được lưu trong NVRAM.

Ví dụ, một thanh ghi có giá trị 0x2102 (0x chỉ ra giá trị này biểu diễn dưới dạng hexa), trong đó giá trị của cột boot là 0x2(số bên phải nhất của thanh ghi và biểu diễn 4 bit thấp của thanh ghi)

- Nếu cột boot trong thanh ghi có giá trị từ 0x2 đến 0xF, bootstrap sẽ phân tích tập tin startup-config trong NVRAM có những lệnh **boot system** hay không, lệnh boot system chỉ ra vị trí và tên của IOS image để tải. Có thể cấu hình nhiều lệnh boot system để cung cấp kế hoạch fault-tolerant boot

lệnh **boot system** là một lệnh global configuration mà cho phép bạn chỉ ra vị trí để tải IOS image. Cấu trúc lệnh boot system

boot system flash [tên file]

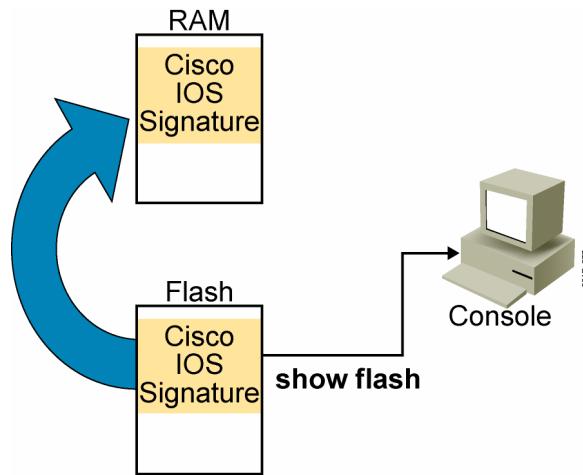
boot system tftp [tên file] [địa chỉ server]

boot system rom

- Nếu không có lệnh **boot system** trong file cấu hình. Mặc định router sẽ tải IOS image trong flash và chạy nó

- Nếu không có IOS image được tìm thấy trong flash, router cố gắng boot từ tftp server bằng cách sử dụng giá trị cột boot như là một phần của tên IOS image
- Mặc định, nếu boot từ TFTP Server bị lỗi sau 5 lần cố gắng, router sẽ boot IOS image cơ bản trong ROM. Người dùng có thể xét bit 13 của thanh ghi có giá trị là 0 để router boot từ TFTP Server một cách liên tục sau 5 lần cố gắng không thành công
- Nếu không có IOS image cơ bản hoặc nếu nó bị lỗi, router sẽ boot ROMMON từ ROM

Loading the Cisco IOS Image from Flash Memory



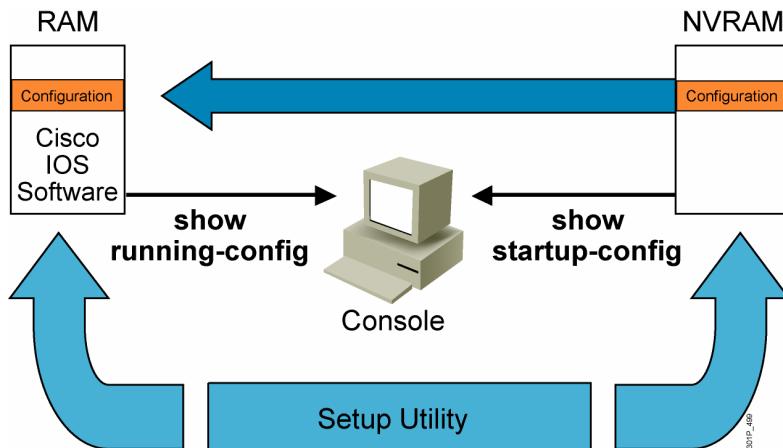
The flash memory file is loaded into RAM.

17-7

Khi router tìm được một IOS image trong flash, IOS image thường được tải vào NVRAM để chạy. Một vài router, gồm Cisco 2500 Series Routers, không có đủ RAM để lưu IOS image, vì thế chạy IOS image trực tiếp từ flash

Nếu image được tải từ flash vào RAM, đầu tiên nó phải được giải nén. Sau khi file đã được giải nén vào RAM, nó start. IOS image chạy từ flash không được nén.

Loading the Configuration



- Load and execute the configuration from NVRAM
- If no configuration is present in NVRAM, enter setup mode

17-8

Sau khi IOS image được tải và chạy, router phải được cấu hình để sử dụng. Nếu có một file cấu hình đã tồn tại trong NVRAM, nó sẽ thực thi file cấu hình này. Nếu không có file cấu hình trong NVRAM, Router bắt đầu AutoInstall hoặc vào tiện ích setup

Autoinstall có găng download một cấu hình từ TFTP Server. Autoinstall yêu cầu một kết nối mạng và một tftp server đã được cấu hình trước.

Tiện ích setup hướng dẫn người dùng nhập những cấu hình cơ bản cho router tại console

show running-config and show startup-config Commands

In RAM

```
RouterX#show running-config
Building configuration...??
Current configuration:?
!?
version 12.2
!
-- More --
```

In NVRAM

```
RouterX#show startup-config
Using 1359 out of 32762 bytes
!
version 12.2
!
-- More --
```

Displays the current and saved configuration

2012-203

Lệnh **show running-config** dùng để xem cấu hình hiện hành trong RAM, và **show startup-config** dùng để xem file cấu hình startup-config trong NVRAM mà router sẽ sử dụng trong lần khởi động lại kế tiếp

Nếu xuất hiện “Current configuration”, cấu hình đang chạy từ RAM đang được hiển thị

Nếu có một message tại đỉnh chỉ ra có bao nhiêu nonvolatile memory được sử dụng, startup-config trong NVRAM đang được hiển thị

Determining the Current Configuration Register Value

```
Cisco IOS Software, 2800 Software (C2800NM-IPBASE-M), Version  
12.4(5a), RELEASE SOFTWARE (fc3)  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2006 by Cisco Systems, Inc.  
Compiled Sat 14-Jan-06 03:19 by alnguyen

ROM: System Bootstrap, Version 12.4(1r) [hqluong 1r], RELEASE  
SOFTWARE (fc1)

RouterX uptime is 1 week, 5 days, 21 hours, 30 minutes  
System returned to ROM by reload at 23:04:40 UTC Tue Mar 13 2007  
System image file is "flash:c2800nm-ipbase-mz.124-5a.bin"

Cisco 2811 (revision 53.51) with 251904K/10240K bytes of memory.  
Processor board ID FTX1013A1DJ
2 FastEthernet interfaces
2 Serial(sync/async) interfaces
DRAM configuration is 64 bits wide with parity enabled.
239K bytes of non-volatile configuration memory.
62720K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102
```

17-10

Trước khi thay đổi giá trị thanh ghi, bạn nên quyết định hiện tại router đang tải IOS image như thế nào. Lệnh **show version** sẽ cho biết giá trị thanh ghi hiện hành. Dòng cuối cùng chứa giá trị thanh ghi.

Configuration Register Values

```
Router#configure terminal  
Router(config)#config-register 0x2104  
[Ctrl-Z]  
Router#
```

- Configuration register bits 3, 2, 1, and 0 set boot option

Configuration Register Boot Field Value	Meaning
0x0	Use ROMMON mode (manually boot using the boot command).
0x1	Automatically boot up from ROM (provides Cisco IOS software subset).
0x2 to 0xF	Examine NVRAM for boot system commands (0x2 default if router has flash).

- Check the configuration register value with the **show version** command

17-11

Bạn có thể thay đổi giá trị mặc định của thanh ghi với lệnh **config-register** trong global configuration. Thanh ghi có kích thước 16 bit. 4 bit thấp của thanh ghi biểu diễn giá trị của cột boot. Giá trị thanh ghi được biểu diễn dưới dạng số hexa. Giá trị mặc định của thanh ghi là 0x2102

Những hướng dẫn thay đổi giá trị của cột boot như sau:

- Cột boot có giá trị 0, router sẽ tự động vào ROMMON mode. Giá trị của 4 bit cột boot là 0000. Trong ROMMON mode, bạn có thể sử dụng lệnh **boot** để khởi động router bằng tay
- Cột boot có giá trị 1, router sẽ khởi động IOS image cơ bản từ ROM. Giá trị của 4 bit cột boot là 0001. Trong mode này router hiển thị dấu nhắc Router(boot)>
- Cột boot có giá trị bất kỳ trong khoảng 0x2 đến 0xF, router sử dụng lệnh **boot system** trong file startup-config trong NVRAM. Mặc định là 0x2. Giá trị của 4 bit cột boot là 0010 đến 1111

show version Command

```
Cisco IOS Software, 2800 Software (C2800NM-IPBASE-M), Version  
12.4(5a), RELEASE SOFTWARE (fc3)  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2006 by Cisco Systems, Inc.  
Compiled Sat 14-Jan-06 03:19 by alnguyen  
  
ROM: System Bootstrap, Version 12.4(1r) [hqluong 1r], RELEASE  
SOFTWARE (fc1)  
  
RouterX uptime is 1 week, 5 days, 21 hours, 30 minutes  
System returned to ROM by reload at 23:04:40 UTC Tue Mar 13 2007  
System image file is "flash:c2800nm-ipbase-mz.124-5a.bin"  
  
Cisco 2811 (revision 53.51) with 251904K/10240K bytes of memory.  
Processor board ID FTX1013A1DJ  
2 FastEthernet interfaces  
2 Serial(sync/async) interfaces  
DRAM configuration is 64 bits wide with parity enabled.  
239K bytes of non-volatile configuration memory.  
62720K bytes of ATA CompactFlash (Read/Write)  
  
Configuration register is 0x2102 (will be 2104 at next reload)
```

17-12

Lệnh **show version** được sử dụng để kiểm tra những thay đổi của thanh ghi. Giá trị cấu hình thanh ghi mới chỉ ảnh hưởng khi router khởi động lại

Trong ví dụ, lệnh **show version** chỉ ra thanh ghi hiện hành có giá trị là 0x2104 sẽ được sử dụng trong lần khởi động lại kế tiếp

show flash Command

```
RouterX#sh flash
--length-- -----date/time----- path
1      14951648 Feb 22 2007 21:38:56 +00:00 c2800nm-ipbase-mz.124-5a.bin
2          1823 Dec 14 2006 08:24:54 +00:00 sdmconfig-2811.cfg
3          4734464 Dec 14 2006 08:25:24 +00:00 sdm.tar
4          833024 Dec 14 2006 08:25:38 +00:00 es.tar
5          1052160 Dec 14 2006 08:25:54 +00:00 common.tar
6          1038 Dec 14 2006 08:26:08 +00:00 home.shtml
7          102400 Dec 14 2006 08:26:22 +00:00 home.tar
8          491213 Dec 14 2006 08:26:40 +00:00 128MB.sdf

41836544 bytes available (22179840 bytes used)
```

17-13

Lệnh **show flash** hiển thị nội dung của bộ nhớ flash, bao gồm tên và kích thước của các image.

Trong ví dụ, dòng cuối cùng cho biết bộ nhớ flash còn trống bao nhiêu. Bộ nhớ flash luôn luôn là read-only

Tóm tắt

- When a router boots, it performs tests, finds, and loads software, finds and loads configurations, and finally runs the software.
- The major internal components of a router include RAM, ROM, flash memory, NVRAM, and the configuration register.
- When a router boots, it searches for the Cisco IOS Software image in a specific sequence: location specified in the configuration register, flash memory, a TFTP server, and ROM.
- The configuration register includes boot information specifying where to locate the Cisco IOS Software image. The register can be examined with a **show** command and change the register value with the **config-register** global configuration command.

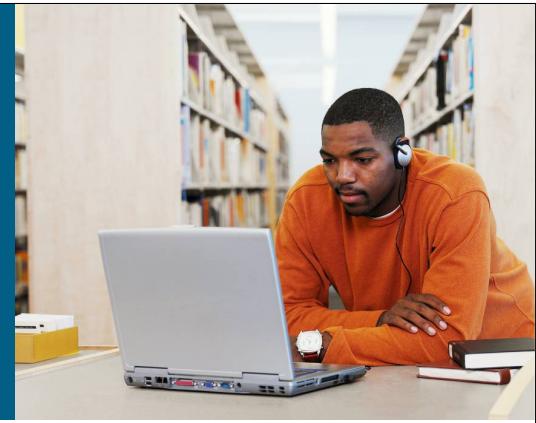
17-14

- Khi router khởi động, nó thi hành kiểm tra, tìm kiếm, và tải IOS image và tải cấu hình, và chạy IOS image
- Những thành phần chính của router gồm RAM, ROM, Flash, NVRAM, và thanh ghi
- Khi router khởi động, nó tìm kiếm IOS image theo một thứ tự cụ thể: vị trí tìm kiếm được ghi rõ trong thanh ghi, flash, tftp server, và ROM
- Thanh ghi gồm thông tin boot chỉ ra nơi tìm kiếm IOS image. Có thể dùng lệnh **show** để kiểm tra giá trị thanh ghi và lệnh **config-register** trong global configuration để thay đổi giá trị thanh ghi



17-15

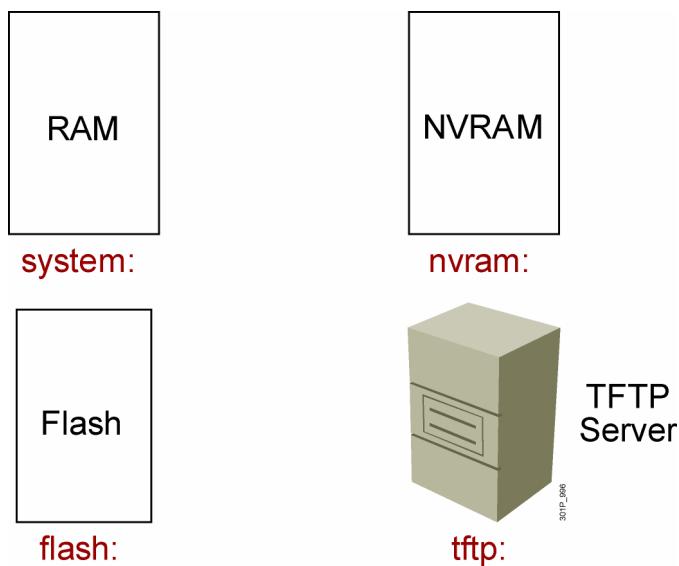
Bài 18: Managing Cisco Devices



Network Environment Management

18-1

Cisco IOS File System and Devices



18-2

Hệ thống tập tin của Cisco IOS (Cisco IFS) cung cấp một cách giao tiếp đến tất cả các hệ thống tập tin mà Router hỗ trợ, gồm:

- Flash memory
- Network: tftp, Remote Copy Protocol (RCP), và FTP
- Bất kỳ nơi nào khác cho phép đọc hoặc ghi dữ liệu (NVRAM, running-config trong RAM, và ...)

Một tính năng chính của Cisco IFS là sử dụng qui ước đặt tên URL để chỉ ra những file trên thiết bị mạng và mạng

Bảng sau đây liệt kê một số tiếp đầu ngữ URL thường sử dụng

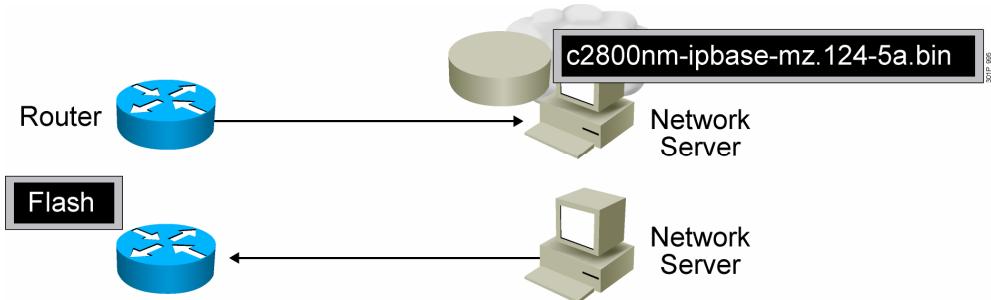
- Bootflash: bộ nhớ bootflash
- Flash: bộ nhớ flash. Tiếp đầu ngữ này có hiệu lực trên tất cả platform. Platform không có thiết bị tên là flash, tiếp đầu ngữ flash: là bí danh của slot0. vì thế, tiếp đầu ngữ flash: có thể được sử dụng để tham chiếu đến vùng lưu trữ bộ nhớ flash chính trên tất cả platform
- Flh: flash load helper log file
- ftp: FTP network server
- Nvram: NVRAM
- Rcp: RCP network server
- Slot0: first PCMCIA flash memory card
- Slot1: second PCMCIA flash memory card

- System: chứa bộ nhớ hệ thống, gồm running-config

- Tftp: TFTP network server

Với Cisco IOS release 12.0, những lệnh được sử dụng để copy và truyền cấu hình và hệ thống tập tin được thay đổi trong những kỹ thuật Cisco IFS.

Managing Cisco IOS Images



18-4

Mạng Production thường được mở rộng ra nhiều vùng và gồm nhiều router. Trong bất kỳ network nào, cần thận trọng việc tạo một bản copy của IOS image để dự phòng trong trường hợp hệ thống bị lỗi hay lỡ xóa IOS image.

Những router trong mạng phân tán cần có một nguồn hay nơi backup IOS image. Sử dụng TFTP server để cho phép upload và download IOS image và file cấu hình. TFTP server có thể là 1 router khác, một workstation, hay một host system

Trước khi copy IOS image từ flash của router đến TFTP server, bạn nên thực hiện những bước sau:

- Step 1: chắc chắn rằng có thể truy cập đến TFTP Server, bạn có thể ping đến tftp server để kiểm tra kết nối
- Step 2: kiểm tra đĩa cứng TFTP server còn vùng trống để lưu backup. Sử dụng lệnh **show flash**: trên router để biết kích thước của IOS image
- Step 3: kiểm tra yêu cầu về filename trên TFTP server. Cái này có thể khác, phụ thuộc vào server đang chạy Microsoft windows, UNIX, hay hệ điều hành khác
- Step 4: tạo file đích để nhận upload, nếu yêu cầu. Bước này phụ thuộc vào hệ điều hành trên server

Verifying Memory and Deciphering Image Filenames

```
RouterX#sh flash
--length-- -----date/time----- path
1      14951648 Feb 22 2007 21:38:56 +00:00 c2800nm-ipbase-mz.124-5a.bin
2          1823 Dec 14 2006 08:24:54 +00:00 sdmconfig-2811.cfg
3      4734464 Dec 14 2006 08:25:24 +00:00 sdm.tar
4      833024 Dec 14 2006 08:25:38 +00:00 es.tar
5      1052160 Dec 14 2006 08:25:54 +00:00 common.tar
6          1038 Dec 14 2006 08:26:08 +00:00 home.shtml
7      102400 Dec 14 2006 08:26:22 +00:00 home.tar
8      491213 Dec 14 2006 08:26:40 +00:00 128MB.sdf

41836544 bytes available (22179840 bytes used)
```

Verify that flash memory has room for the Cisco IOS image.

18-5

Lệnh **show flash** là một công cụ quan trọng để biết thông tin về bộ nhớ và IOS image. Lệnh này cho biết những thông tin sau:

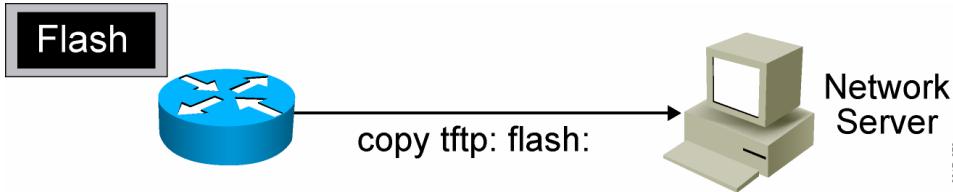
- Tổng dung lượng bộ nhớ flash của router
- Dung lượng bộ nhớ flash còn trống
- Tên của tất cả các file lưu trong flash

Tên IOS image gồm nhiều phần, mỗi phần có một nghĩa khác nhau. Ví dụ, tên “c2800nm-ipbase-mz.124-5a.bin” trong hình chứa những thông tin sau:

- Phần đầu tiên của tên chỉ ra platform mà image này có thể chạy. Trong ví dụ, platform là c2800
- Phân thứ 2 chỉ ra nơi mà image này chạy và nếu file này được nén. Trong ví dụ, “mz” chỉ ra rằng file này chạy từ RAM và được nén.
- Phần thứ 3 của tên chỉ ra version. Trong ví dụ, version là 124-5a
- Phần cuối cùng của tên là mở rộng của file. Trong ví dụ, “.bin” chỉ ra rằng file này là thực thi có dạng binary

Qui ước đặt tên IOS image, ý nghĩa các field, nội dung image, và những chi tiết khác là những đối tượng thay đổi. Bạn có thể liên lạc với sale hay những kênh phân phối để cập nhật, hoặc vào cisco.com

Creating a Software Image Backup



30HP_973

```
RouterX#copy flash tftp:  
Source filename []? c2800nm-ipbase-mz.124-5a.bin  
Address or name of remote host []? 10.1.1.1  
Destination filename [c2800nm-ipbase-mz.124-5a.bin]  
!!!!!!!!!!!!!!<output omitted>  
12094416 bytes copied in 98.858 secs (122341 bytes/sec)  
RouterX#
```

Back up current files prior to updating flash memory.

18-6

Backup image được tạo bằng cách copy tập tin image từ router đến tftp server. Để copy sử dụng lệnh sau

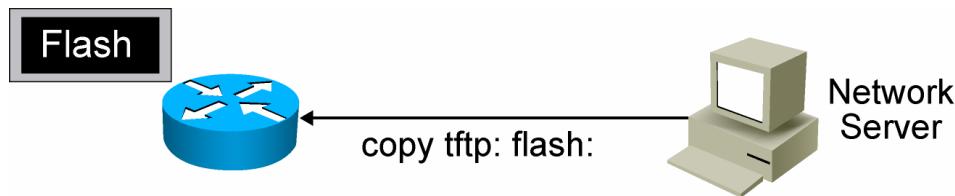
Router#copy flash: tftp:

Lệnh này yêu cầu bạn cung cấp địa chỉ IP của tftp server và tên nguồn và đích của tập tin image

Dấu (!!!....) chỉ ra tiến trình copy tập tin image từ flash đến tftp server. Dấu này có nghĩa là UDP segment được truyền thành công

Trước khi cập nhật flash với IOS image mới, bạn nên backup IOS image hiện hành đến tftp server để dự phòng trong trường hợp flash chỉ đủ kích thước lưu một IOS image

Upgrading the Image from the Network



```
RouterX#copy tftp flash:  
Address or name of remote host [10.1.1.1]?  
Source filename []? c2800nm-ipbase-mz.124-5a.bin  
Destination filename [c2800nm-ipbase-mz.124-5a.bin]  
Accessing tftp://10.1.1.1/c2600-js-mz.122-21a.bin...  
Erase flash: before copying? [confirm]  
Erasing the flash filesystem will remove all files! Continue? [confirm]  
Erasing device... eeeeeeee (output omitted) ...erased  
Erase of flash: complete  
Loading c2800nm-ipbase-mz.124-5a.bin from 10.1.1.1 (via Ethernet0/0): !!!!!!!!  
(output omitted)  
[OK - 12094416 bytes]  
Verifying checksum... OK (0x45E2)  
12094416 bytes copied in 120.465 secs (100398 bytes/sec)  
RouterX
```

3011P_873

18-7

Nâng cấp hệ thống với một phiên bản IOS mới hơn yêu cầu một tập tin IOS image mới tải vào router. Sử dụng lệnh sau để copy image mới từ tftp server vào router:

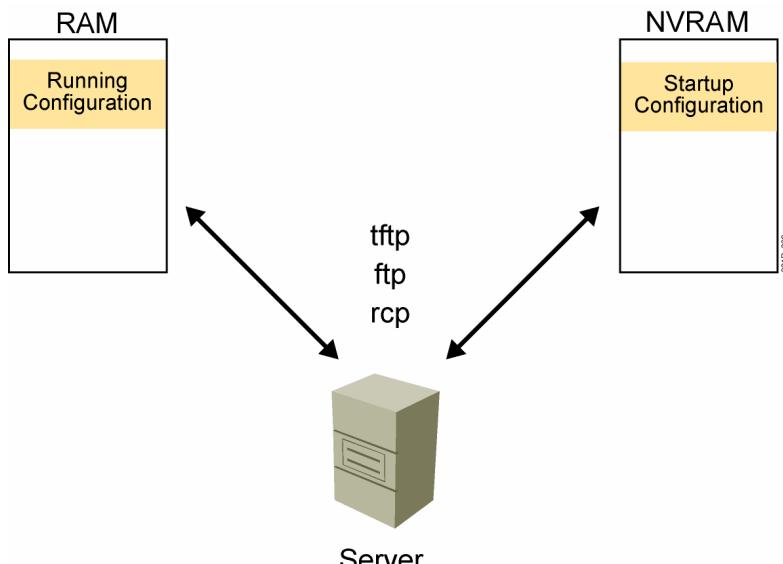
Router#copy tftp: flash:

Lệnh yêu cầu bạn nhập vào địa chỉ IP của tftp server và tên nguồn và đích của tập tin image.

Sau khi confirm tất cả các yêu cầu, nhắc xóa flash xuất hiện. Xóa flash để chép IOS image mới. Xóa flash chỉ khi flash không đủ kích thước để lưu nhiều hơn 1 IOS image. Hệ thống sẽ thông báo cho bạn biết những điều kiện và yêu cầu bạn trả lời

Mỗi dấu (!) nghĩa rằng một UDP segment đã được truyền thành công

Device Configuration Files



18-8

Tập tin cấu hình chứa những câu lệnh nhằm mục đích cấu hình tính năng của thiết bị, như router, access server, switch, và v.v... Việc phân tích, biên dịch và thực thi những lệnh được thực hiện khi hệ thống khởi động, IOS sẽ đọc những lệnh được lưu trong startup-config hoặc khi bạn gõ những lệnh tại CLI trong global configuration mode.

Tập tin cấu hình được lưu ở những vị trí sau:

- Running-config được lưu trong RAM
- Startup-config được lưu trong NVRAM

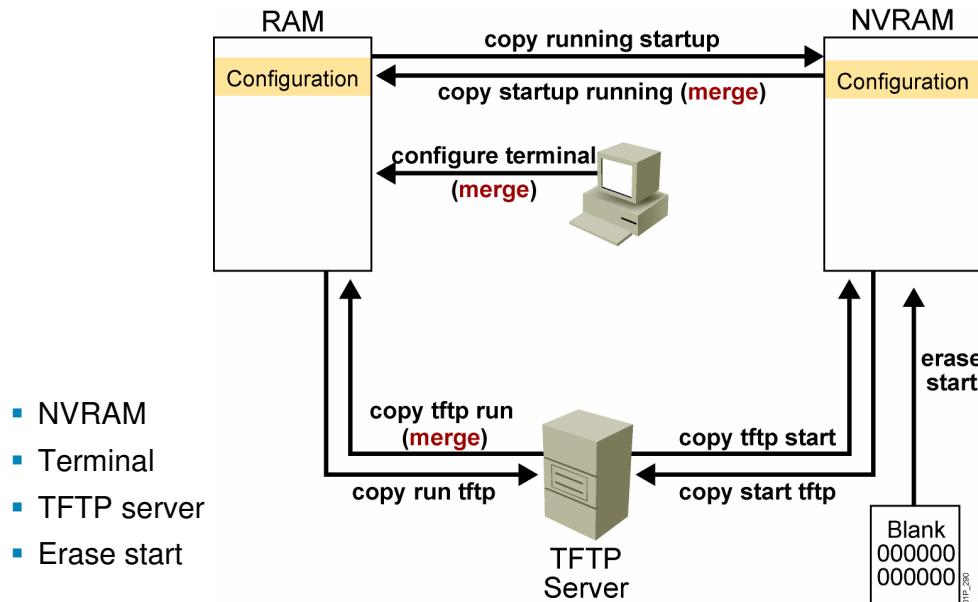
Bạn có thể copy file cấu hình từ router đến file server dùng ftp, rcp, tftp. Ví dụ, copy file cấu hình đến server để backup file cấu hình trước khi bạn thay đổi nội dung của nó, bằng cách này bạn có thể phục hồi file cấu hình cũ từ server. Protocol nào được sử dụng phụ thuộc vào loại server.

Bạn có thể copy file cấu hình từ một tftp, rcp, hoặc ftp server vào running-config trong RAM hoặc startup-config trong NVRAM của router với những lý do sau:

- Phục hồi lại file cấu hình đã backup
- Sử dụng file cấu hình của một router khác. Ví dụ, bạn thêm một router vào mạng và muốn router này có cấu hình tương tự những router gốc. Bằng cách copy file cấu hình từ server và sau đó thay đổi theo yêu cầu của router mới, bạn có thể tiết kiệm thời gian vì không phải tạo toàn bộ file cấu hình

- Để tải những lệnh cấu hình giống nhau vào tất cả router trong mạng vì thế tất cả router có cấu hình tương tự nhau.

Cisco IOS copy Command



18-10

Bạn có nhiều cách khác nhau để cấu hình thiết bị

Bạn có thể sử dụng lệnh **copy** để di chuyển một cấu hình từ thành phần hay thiết bị này đến chỗ khác. Cú pháp lệnh **copy** gồm biến đầu tiên chỉ ra nguồn, biến thứ 2 chỉ ra đích. Ví dụ, **copy running-config: tftp:**, copy cấu hình từ RAM đến TFTP Server

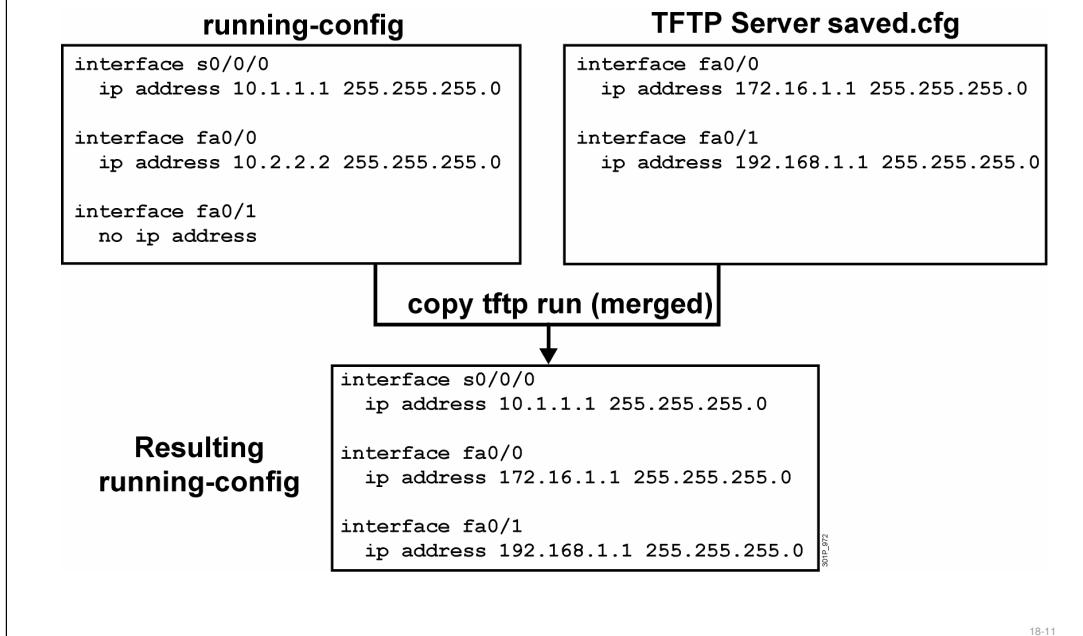
Sử dụng lệnh **copy running-config: startup-config:** sau khi thay đổi cấu hình trong RAM và phải được lưu vào startup-config trong NVRAM. Tương tự, copy từ startup-config vào running-config với lệnh **copy start running**. Bạn có thể viết tắt những lệnh.

Tồn tại những lệnh tương tự để copy giữa tftp server và RAM hoặc NVRAM

Sử dụng lệnh **configure terminal**: để tạo những cấu hình trong RAM từ console và remote terminal

Sử dụng lệnh **erase startup-config** để xóa nội dung file cấu hình trong NVRAM

Cisco IOS copy Command Example



18-11

Hình vẽ chỉ ra cách sử dụng lệnh **copy tftp run**

copy run tftp and copy tftp run Commands

```
RouterX#copy running-config: tftp:  
Address or name of remote host []? 10.1.1.1  
Destination filename [running-config]? wgroa.cfg  
.!!  
1684 bytes copied in 13.300 secs (129 bytes/sec)  
  
RouterX#copy tftp: running-config:  
Address or name of remote host []? 10.1.1.1  
Source filename []? wgroa.cfg  
Destination filename [running-config]?  
Accessing tftp://10.1.1.1/wgroa.cfg...  
Loading wgroa.cfg from 10.1.1.1 (via Ethernet0): !  
[OK - 1684/3072 bytes]  
  
1684 bytes copied in 17.692 secs (99 bytes/sec)
```

18-12

Bạn có thể dùng tftp server để lưu tập trung các file cấu hình, cho phép quản lý và cập nhật tập trung. Với bất kỳ kích thước mạng như thế nào, nên tạo một tập tin backup cấu hình hiện hành

Lệnh **copy running-config: tftp:** cho phép upload cấu hình hiện hành lên tftp server. Địa chỉ IP hoặc tên tftp server và tên file đích phải được cung cấp. Trên hình vẽ một chuỗi các dấu (!) chỉ ra quá trình upload.

Lệnh **copy tftp: running-config:** download file cấu hình từ tftp server vào running-config trong RAM. Địa chỉ hoặc tên tftp server và tên file đích và nguồn phải được cung cấp. Trong trường hợp này, bởi vì bạn đang copy file đến running-config nên tên file đích phải là running-config. Đây là tiến trình kết hợp, không phải là viết đè.

show and debug Commands

	show	debug
Processing characteristic	Static	Dynamic
Processing load	Low overhead	High overhead
Primary use	Gather facts	Observe processes

CCNP_200

18-13

Lệnh **show** và **debug** có những tính năng sau:

- Show: cung cấp một hình ảnh về những vấn đề liên quan tới interface, media, network performance
- Debug: kiểm tra lưu lượng dữ liệu của các protocol về các vấn đề, lỗi protocol hoặc lỗi cấu hình

Bảng sau mô tả sự khác nhau chính giữa lệnh **show** và **debug**:

- Show: cung cấp một tập hợp thông tin tĩnh về trạng thái của thiết bị mạng, những thiết bị neighbor, và network performance. Sử dụng lệnh **show** khi thu thập những sự kiện về những vấn đề độc lập trong một mạng; gồm những vấn đề với interface, node, media, server, client, hay ứng dụng
- Debug: cung cấp dòng thông tin về traffic đang thấy (hoặc không thấy) trên một interface, message lỗi được tạo ra bởi những node trên mạng. Sử dụng lệnh debug khi muốn xem những hoạt động đang diễn ra trên mạng hoặc router để biết xem những sự kiện hay packet có làm việc đúng hay không.

Considerations When Using debug Commands

- May generate output in a variety of formats that may not identify the problem
- Require high overhead, possibly disrupting network device operation
- Useful for obtaining information about network traffic and router status

18-14

Sử dụng lệnh **debug** để cô lập những vấn đề, không phải để theo dõi hoạt động mạng bình thường. Bởi vì tải của lệnh debug cao có thể làm gián đoạn hoạt động của router, lệnh **debug** chỉ nên được dùng khi tìm những loại traffic hoặc những vấn đề chỉ định và những vấn đề đã được thu hẹp nguyên nhân.

Sau đây là một vài cân nhắc khi dùng lệnh **debug**:

- Nhận thức rằng lệnh **debug** có thể tạo ra quá nhiều dữ liệu mà sẽ ít được sử dụng. Một cách thông thường, biết về protocol hoặc những protocol đang debug được yêu cầu thông dịch kết quả thích hợp
- Bởi vì chi phí CPU của lệnh debug cao nên có thể làm gián đoạn hoạt động của thiết bị mạng. Lệnh debug chỉ sử dụng khi tìm một loại traffic hoặc vấn đề chỉ định
- Khi sử dụng công cụ debug để chẩn đoán và sửa lỗi, định dạng kết quả xuất ra sẽ khác nhau phụ thuộc vào mỗi protocol. Có thể tạo ra một dòng đơn hoặc nhiều dòng cho mỗi packet
- Một vài lệnh debug tạo ra khối lượng dữ liệu lớn; những cái khác chỉ tạo ra kết quả theo sự kiện. Một vài tạo ra những dòng text, và cái khác tạo ra thông tin theo định dạng theo cột
- Sử dụng lệnh debug là một gợi ý để thu thập thông tin về network traffic và trạng thái router. Sử dụng lệnh này với tính cẩn thận cao.
- Nếu bạn không chắc chắn về ảnh hưởng của lệnh debug, kiểm tra trong site <http://www.cisco.com>

Commands Related to debug

```
RouteX(config)#
  service timestamps debug datetime msec
    ▪ Adds a time stamp to a debug or log message
RouteX#
  show processes
    ▪ Displays the CPU utilization for each process
RouteX#
  no debug all
    ▪ Disables all debug commands
RouteX#
  terminal monitor
    ▪ Displays debug output on your current vty session
```

18-15

Bảng sau đây liệt kê những lệnh mà bạn có thể sử dụng với lệnh debug

- Service timestamps: để thêm một time stamp vào một debug hoặc log message. Tính năng này có thể cung cấp thông tin quan trọng về khi những thành phần debug xảy ra và trong khoảng thời gian giữa các event
- Show processes: hiển thị việc sử dụng CPU của mỗi process. Dữ liệu này có thể có ảnh hưởng đến quyết định sử dụng lệnh debug, nếu nó chỉ ra hệ thống quá tải khi sử dụng lệnh debug.
- No debug all: tắt tất cả lệnh debug. Lệnh này giải phóng tài nguyên hệ thống sau khi bạn hoàn thành lệnh debug.
- Terminal monitor: hiển thị kết quả của lệnh debug và những message lỗi ra terminal và giao dịch hiện hành.

Để sử dụng công cụ debug hiệu quả, bạn phải xem xét những điều sau:

- Công cụ này có ảnh hưởng đến performance của router.
- Có lựa chọn và sử dụng công cụ nhận dạng
- Làm thế nào để giảm ảnh hưởng của công cụ đến những process khác mà chúng đang tranh giành tài nguyên của thiết bị mạng
- Làm cách nào để dừng công cụ khi việc nhận dạng hoàn thành để router có thể lại bắt đầu công việc hiệu quả nhất

Sử dụng lệnh debug thích hợp, bạn có thể thu thập được những thông tin hữu ích mà không cần một protocol analyzer hoặc một công cụ nào khác

Những xem xét khác khi sử dụng lệnh debug:

- Nó là một lệnh lý tưởng được dùng khi network traffic thấp và ít người dùng. Nó sẽ làm giảm ảnh hưởng đến những user khác

- Khi thông tin bạn cần từ lệnh debug được làm sáng tỏ và lệnh debug chưa hoàn thành, router có thể bắt đầu sử dụng lại nhanh hơn. Cách giải quyết vấn đề có thể lại tiếp tục, một kế hoạch hành động đã được tạo, và vấn đề mạng có thể giải quyết

Tất cả các lệnh debug được gõ tại privileged EXEC mode, và hầu hết các lệnh debug không có biến

Để liệt kê và thấy những mô tả về tất cả các lệnh debug, gõ lệnh debug ?

Mặc định kết quả của lệnh debug và những message lỗi sẽ được gởi ra cổng console. Khi sử dụng mặc định này, bạn nên monitor kết quả debug bằng vty hơn là console. Để đổi hướng xuất của lệnh debug dùng tùy chọn logging trong configuration mode. Những đích có thể gồm console, cty, internal buffer, và những host UNIX đang chạy syslog server. Định dạng của syslog tương thích với 4.3 BSD UNIX và những bắt nguồn từ nó.

Tóm tắt

- The Cisco IFS feature provides a single interface to all the file systems (NVRAM, RAM, TFTP, flash) that a router uses.
- As a network grows, storage of the Cisco IOS Software and configuration files on a central server enables control of the number and revision level of software images and configuration files that must be maintained.
- Having proper backup of the current device configuration stored in a TFTP server can help reduce device downtime.

18-17

Tóm tắt (tiếp theo)

- The Cisco IOS Software **copy** commands can be used to move configurations from one component or device to another, such as RAM, NVRAM, or a file server.
- The **show** and **debug** commands are built-in tools for troubleshooting. The **show** command is used to display static information, while the **debug** command is used to display dynamic data.



18-19

