THỰC HÀNH CÁC BÀI LAB CCNA

(CCNA Lab Series)

Mẫn Thắng (manthang)

manvanthang@gmail.com

http://manthang.wordpress.com

HCM, 02/2012

Giới thiệu

Để thực hiện các lab trong tài liệu này, bạn cần chuẩn bị các thứ sau:

1. **Một máy tính có cài đặt Packet Tracer**

Download bản 5.3 của nó ở đây:

`http://www.mediafire.com/?zziz2tziywj`

Các thao tác xây dựng mô hình mạng và cấu hình cho các thiết bị đều được thực hiện trong Packet Tracer.

2. **Standalone Labs for CCNA**

Là ebook tiếng Anh mà tôi dựa vào nội dung trong đó để biên soạn thành tài liệu tiếng Việt này. Bạn có thể tải nó về ở đây:

`http://www.mediafire.com/?3tc66h1n35s4xf3`

Một số ưu điểm trong các bài lab do tôi biên soạn so với ebook trên là:

- Tại các bước thực hiện đều có hình minh họa rõ ràng.
- Nhiều khái niệm, lý thuyết được tôi diễn giải, tóm tắt lại sao cho ngắn gọn và dễ hiểu nhất.
- Ngôn ngữ tiếng Việt nên thích hợp với các bạn chưa bắt kịp khả năng đọc hiểu tài liệu tiếng Anh.

Lưu ý

Trước khi đi vào thực hiện theo các hướng dẫn trong tài liệu này, bạn nên biết là:

1. Các bài lab được thiết kế phù hợp cho những bạn nào đã nắm khá vững chương trình học của chứng chỉ CCNA, thế nên phần lý thuyết về mạng căn bản nói chung cũng như những phần chuyên biệt trong CCNA nói riêng sẽ không được đề cập chi tiết trong các bài lab.

2. Do trên Internet cũng có khá nhiều bài viết hướng dẫn cách cài đặt và sử dụng Packet Tracer rồi nên tôi sẽ không trình bày lại nữa. Dưới đây là một số địa chỉ để bạn tham khảo:

   http://vnexperts.net/index.php?option=com_content&task=view&id=755&Itemid=199

   http://www.scribd.com/doc/4291610/Hng-dn-s-dng-Packet-Tracer-kakalotsai

Mục lục

Lab 1: Connecting and Logging on to a Cisco Router

Kết nối và đăng nhập vào một thiết bị Cisco Router

A. Mục tiêu của bài lab:

Giới thiệu về Cisco Router.

B. Chuẩn bị cho bài lab:

Chúng ta sẽ sử dụng một thiết bị router có tên là Router1.

C. Các bước thực hiện:

1. Khởi động Router1 lên và truy cập vào giao diện cấu hình CLI của nó.

2. Nhấn `Enter` để làm xuất hiện dấu nhắc lệnh (command prompt). Dấu nhắc lệnh này bao gồm 2 thành phần: chuỗi "`Router`" là hostname của Router1 và ký tự ">" cho biết ta đang ở user mode.

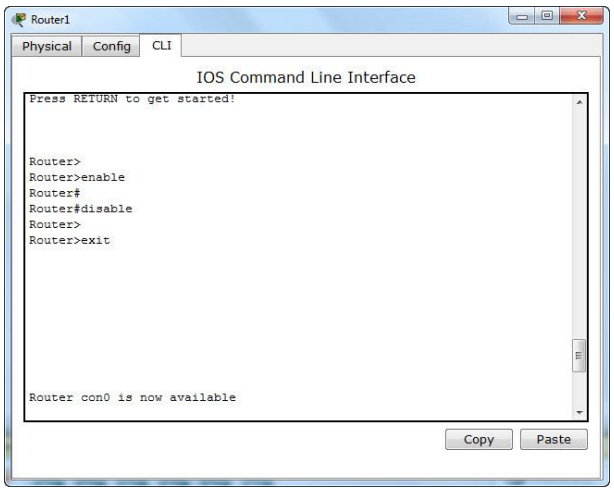
```
Press RETURN to get started!
Router>
```

3. Gõ lệnh `enable` để vào privileged mode và dấu ">" được thay bằng dấu "#".

```
Router>enable
Router#
```

4. Để trở về user mode, ta gõ `disable`. Từ user mode, gõ tiếp `logout` hoặc `exit` để thoát khỏi router.

```
Router>enable
Router#
```



Lab 2: Introduction to the Basic User Interface

Cơ bản về giao diện người dùng

A. Mục tiêu của bài lab:

Giới thiệu về giao diện dòng lệnh (CLI); 2 chế độ là user mode và privileged mode; cơ bản về 2 lệnh `help` và `show`.

B. Chuẩn bị cho bài lab:

Chúng ta sẽ tiếp tục sử dụng Router1.

C. Các bước thực hiện

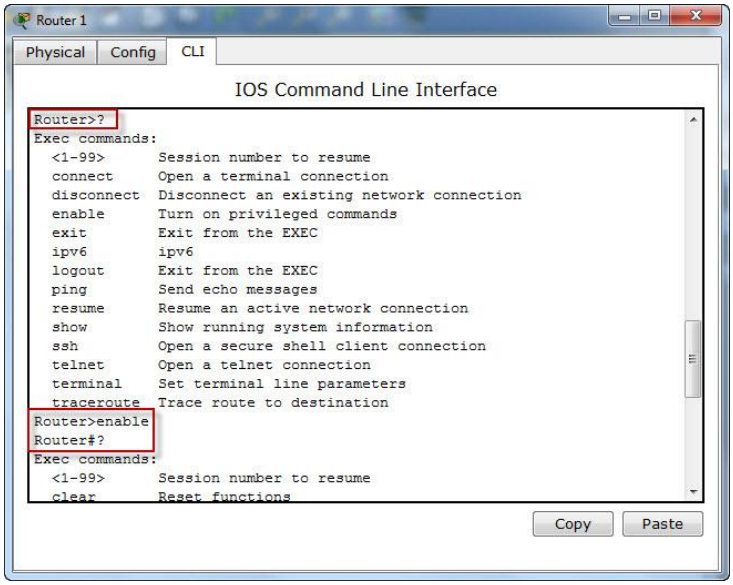
1. Khởi động Router1 lên và truy cập vào giao diện cấu hình CLI của nó. Sau đó, nhấn Enter để hiển thị dấu nhắc lệnh.

2. Hiện ta đang ở User mode (là chế độ chỉ hỗ trợ các câu lệnh cơ bản để xem những thiết lập của thiết bị mà không được phép sử dụng các câu lệnh đặc quyền để thay đổi cấu hình của thiết bị). Gõ vào dấu chấm hỏi (?) để xem tất cả các câu lệnh có thể sử dụng tại dấu nhắc lệnh này.

```
Router>?
```

3. Gõ lệnh sau để vào Privileged mode (là chế độ hỗ trợ nhiều câu lệnh nâng cao hơn để thay đổi các thiết lập của thiết bị).

```
Router> enable

Router#
```



4. Để xem tất cả các câu lệnh có thể sử dụng trong Privileged mode.

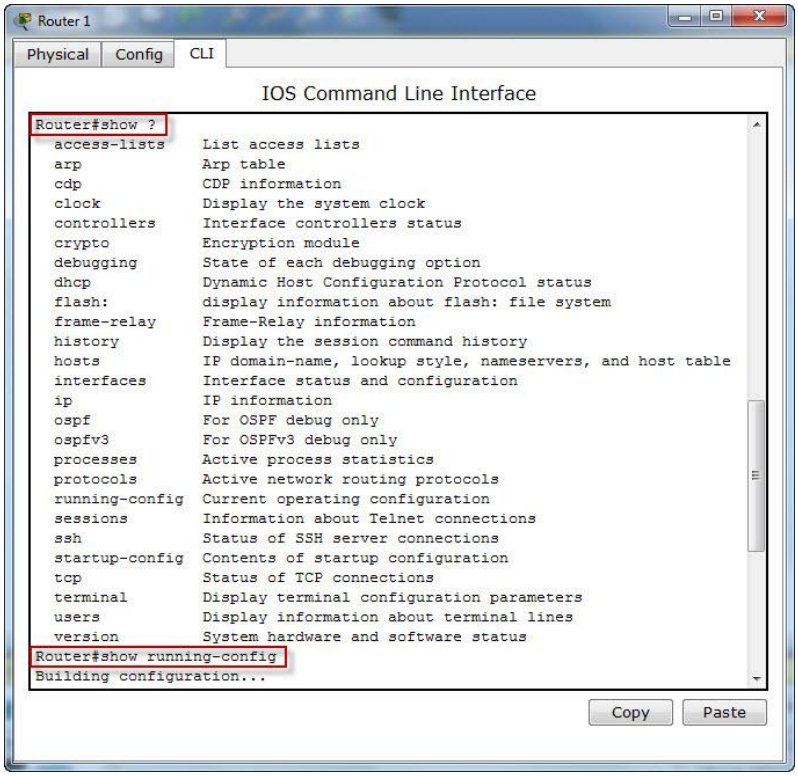
```
Router#?
```

5. Gõ lệnh sau để xem tất cả các câu lệnh show.

```
Router#show ?
```

6. Để xem thông tin về cấu hình hiện tại mà router đang sử dụng (running configuration).

```
Router>show running-config
```



7. Tại dấu nhắc lệnh, gõ phím khoảng trắng để hiển thị trang thông tin kế tiếp

<space bar>

8. Gõ một trong các lệnh sau để đăng xuất khỏi router

```
Router#exit
```

hoặc

```
Router#disable
```

Lab 3: Introduction to Basic Show Commands

Cơ bản về lệnh show

A. Mục tiêu của bài lab:

Làm quen với các câu lệnh show cơ bản

B. Chuẩn bị cho bài lab:

Chúng ta tiếp tục sử dụng Router1.

C. Các bước thực hiện:

1. Hiển thị dấu nhắc lệnh.

```
Router>
```

2. Vào Privileged mode.

```
Router>enable

Router#
```

3. Trong CLI, tập tin nằm trong bộ nhớ RAM chứa các cấu hình mà hiện tại đang được thiết bị (router, switch…) sử dụng được gọi là running-config. Lưu ý là cần vào Privileged mode mới xem được nội dung của running-config.

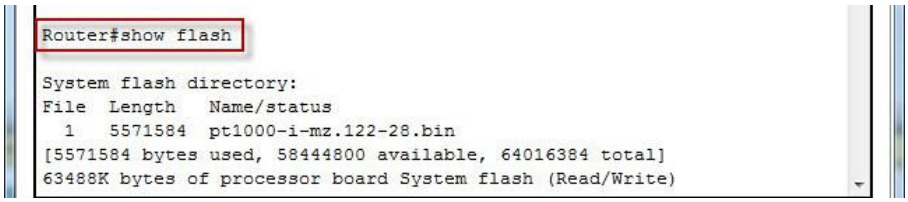
   Đặc biệt, nội dung của running-config không được tự động lưu lại trên Cisco router và sẽ bị mất nếu xảy ra sự cố về nguồn điện cung cấp cho router (như cúp điện đột ngột, điện áp quá tải hoặc quá thấp khiến router không thể hoạt động được…).

   Sau khi ta thay đổi cấu hình cho router, các cấu hình mới này sẽ được cập nhật vào tập tin running-config và để lưu lại nội dung của running-config thì ta cần sử dụng lệnh copy (sẽ được đề cập trong các bài lab sau). Bây giờ, để hiển thị nội dung của running-config ta gõ lệnh sau.

```
Router#show running-config
```

4. Flash là một loại bộ nhớ đặc biệt trên router mà lưu trữ các tập tin hệ điều hành (OS image). Không giống như bộ nhớ thông gặp khác (như RAM), bộ nhớ flash vẫn chứa các OS image ngay cả khi router không được cấp nguồn để hoạt động.

```
Router#show flash
```



5. Mặc định, CLI của các router lưu giữ 10 lệnh gần đây nhất mà được gõ vào trong bộ nhớ. Để xem tất cả các lệnh đã thực hiện vẫn còn được lưu trong bộ nhớ của router.

```
Router#show history
```

6. Hai lệnh sau giúp ta lấy lại lệnh đã gõ trước đó

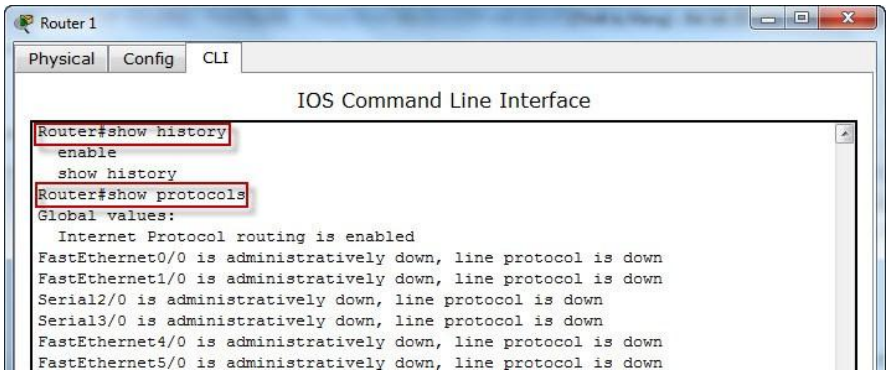
```
Nhấn phím mũi tên đi lên (up) hoặc <ctrl> P
```

7. Còn hai lệnh sau giúp ta sử dụng lệnh kế tiếp trong "history buffer"

```
Nhấn phím mũi tên đi xuống (down) hoặc <ctrl> N
```

8. Để xem trạng thái của các giao thức được định tuyến (routed protocol) ở layer 3 đang chạy trên router

```
Router#show protocols
```



9. Lệnh sau được dùng để nhận về các thông tin quan trọng như: loại "router platform", phiên bản (revision) của OS, lần khởi động cuối và vị trí tập tin image của OS, lượng bộ nhớ, số lượng cổng giao tiếp (interface), và các thanh ghi cấu hình (configuration register)?

```
Router#show version
```

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang
Image text-base: 0x8000808C, data-base: 0x80A1FECC

ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
ROM: PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)

System returned to ROM by reload
System image file is "flash:pt1000-i-mz.122-28.bin"
```

10. Xem ngày giờ được thiết lập trên router

```
Router#show clock
```

11. Để hiển thị danh sách các "hosts" và tất cả các địa chỉ IP của chúng mà được router lưu trữ lại (cache)

```
Router#show hosts
```

12. Xem danh sách các "user" đã kết nối tới router

```
Router#show users
```

13. Để xem thông tin chi tiết về mỗi cổng giao tiếp (interface)

```
Router#show interfaces
```

```
Router#show clock
*0:3:34.96 UTC Mon Mar 1 1993
Router#show hosts
Default Domain is not set
Name/address lookup uses domain service
Name servers are 255.255.255.255

Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
       temp - temporary, perm - permanent
       NA - Not Applicable None - Not defined

Host                      Port  Flags      Age Type   Address(es)
Router#show users
    Line       User       Host(s)              Idle       Location
*  0 con 0                 idle                 00:00:00

  Interface    User               Mode         Idle     Peer Address
Router#show interfaces
FastEthernet0/0 is administratively down, line protocol is down (disabled)
  Hardware is Lance, address is 0060.3e5a.603e (bia 0060.3e5a.603e)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
```

Copy Paste

14. Xem trạng thái tổng quát về các giao thức ở layer 3 cũng như trạng thái của các interface

```
Router#show protocols
```

Lab 4: CDP

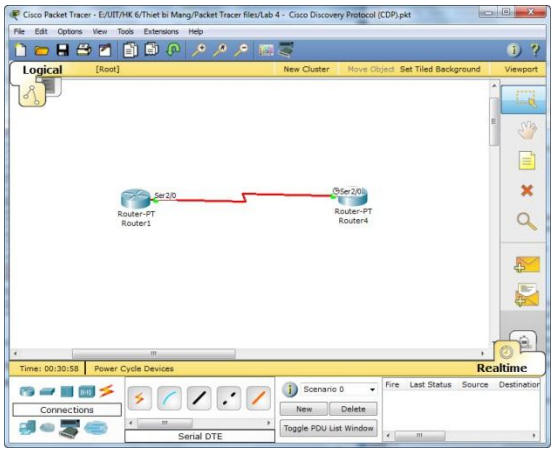
Giao thức CDP (Cisco Discovery Protocol)

A. Mục tiêu của bài lab:

Hiểu được các chức năng của CDP

B. Chuẩn bị cho bài lab:

Chúng ta sẽ sử dụng Router 1 và Router 4.



C. Các bước thực hiện:

1. Trên Router 1, vào chế độ cấu hình toàn cục (global configuration mode)

```
Router>enable

Router#conf t

Router(config)#
```

2. Trên Router 1, thay đổi hostname thành R1

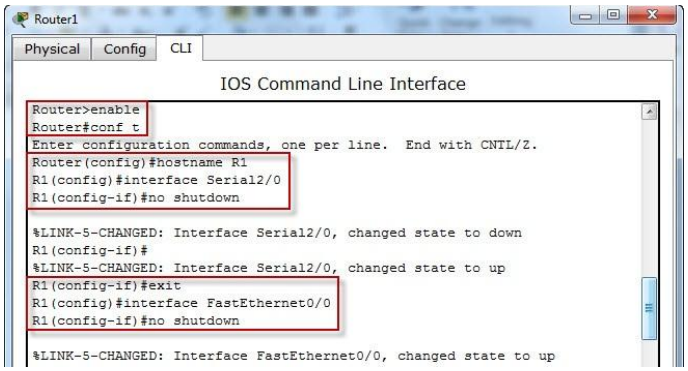
```
Router(config)#hostname R1

R1(config)#
```

3. Thực hiện lại bước 1 và 2 trên Router 4

```
Router>enable

Router#conf t

Router(config)#hostname R4
```

```
R4(config)#
```

Lưu ý: mặc định, tất cả các interface đều bị vô hiệu hóa (không thể sử dụng được)

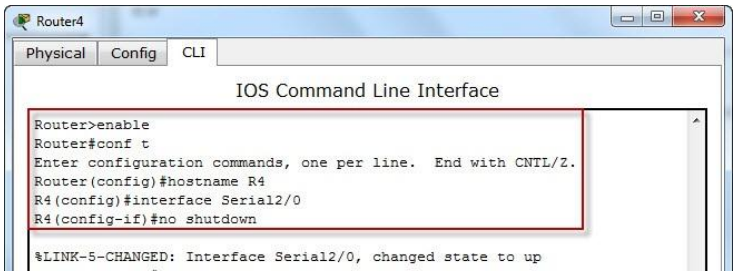


4. Kích hoạt interface Serial2/ 0 trên R1

```
R1(config)#interface Serial2/0
R1(config-if)#no shutdown
```

5. Tương tự, kích hoạt interface Serial2/0 trên R4

```
R4(config)#interface Serial2/0
R4(config-if)#no shutdown
```



6. Kích hoạt interface FastEthernet0/0 trên R1

```
R1(config)#interface FastEthernet0/0
R1(config-if)#no shutdown
```

CDP giúp các thiết bị chia sẻ các thông tin cấu hình cơ bản cho nhau. CDP sẽ hoạt động mà không cần cấu hình gì thêm. CDP được kích hoạt mặc định trên tất cả interface. CDP là một giao thức hoạt động tại layer 2 của mô hình OSI. Vì vậy điều quan trọng cần nắm là CDP không phải là giao thức định tuyến. Nó chỉ có thể giúp các thiết bị được kết nối trực tiếp với nhau trao đổi thông tin cho nhau.

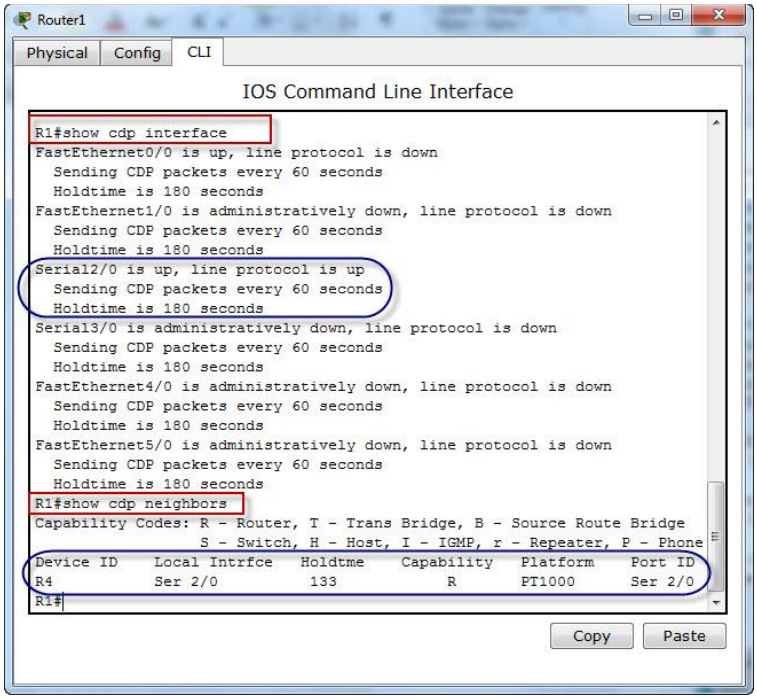
7. Trên R1, gõ lệnh sau để xem trạng thái của tất cả các interface đang chạy CDP.

```
R1(config-if)#exit

R1(config)#exit

R1#show cdp interface
```

Hiện tại, router đang sử dụng CDP để quảng bá đi các thông tin về các interface của nó và đồng thời CDP cũng giúp nó để biết được các router "hàng xóm" được kết nối trực tiếp tới nó.

8. Trên R1, gõ lệnh sau để hiển thị các thông tin về các 'hàng xóm' đang được kết nối trực tiếp tới R1

```
R1#show cdp neighbors
```



Trong hình trên ta thấy, thiết bị đầu tiên trong danh sách các 'hàng xóm' của R1 là router R4 được kết nối trực tiếp tới cổng Serial2/0 trên R1 (cột Local Interface). R1 nhận các gói RDP update từ R4, các gói update này cũng cho ta biết được R1 sẽ nắm giữ các thông tin cập nhật về R4 trong bao lâu. Tại thời điểm gõ câu lệnh trên thì thời gian còn lại là 133 giây (cột Holdtime). R4 là một Cisco router thuộc series 1000 như được thể hiện trong cột platform. Cột cuối cùng, Port ID, là cổng trên trên thiết bị (trong trường hợp này cổng Serial2/0 của R4) mà từ đó các gói update được gửi đi.

9. Trên R1, gõ lệnh sau để xem nhiều thông tin chi tiết hơn về các "hàng xóm" được kết nối trực tiếp tới R1.

```
R1#show cdp neighbors detail
```

Lệnh này sẽ hiện ra cùng lúc thông tin của tất cả các thiết bị 'hàng xóm'. Nó được sử dụng để hiển thị các địa chỉ ở tầng Network. Như hình trên ta thấy R4 có một địa chỉ IP là 192.168.1.4. Ngoài ra, câu lệnh còn cho biết thông tin về phiên bản của IOS. Chú ý rằng các thiết bị 'hàng xóm' được liệt kê theo trình tự. Nếu ta muốn biết thông tin về một thiết bị nằm ở đằng sau nữa thì ta cần cuộn xuống bằng cách nhấn phím khoảng trắng.

10. Trên R1, lệnh sau sẽ chỉ cung cấp thông tin về R4

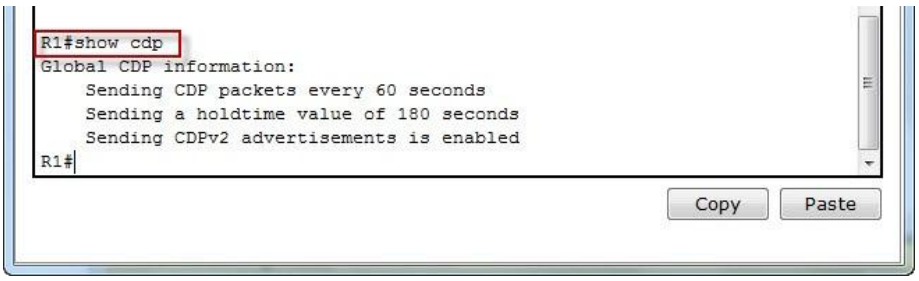
```
R1#show cdp entry R4
```

(thông tin đầu ra của câu lệnh trên giống với trong hình ở bước 9)

Lệnh này cho ta cấu trúc thông tin giống với đầu ra của lệnh show cdp neighbors detail, nhưng khác ở chỗ lệnh này chỉ hiển thị thông tin về R4 mà thôi. Cũng lưu ý thêm rằng đây là một trong những lệnh thuộc loại "case-sensitive", tức là có phân biệt chữ hoa và chữ thường trong câu lệnh.

11. Trên R1, để biết được thời gian định kỳ R1 sẽ gửi đi các gói RDP update và các thông tin CDP mà R1 nhận về sẽ tồn tại trong bao lâu, ta gõ lệnh sau

```
R1#show cdp
```



12. Trên R1, để điều chỉnh số giây thời gian giữa các lần gửi CDP update thành 45, ta gõ

```
R1# conf t

R1(config)#cdp timer 45
```

Ngoài ra, ta cũng có thể điều chỉnh lại giá trị holdtime. Giá trị này cho biết router nhận CDP update sẽ lưu giữ các thông tin trong CDP update (do các router khác gửi tới) trong bao lâu và đây cũng là một tham số toàn cục (global parameter).

13. Trên R1, để điều chỉnh bộ đếm holdtime thành 60 giây, ta gõ

```
R1#conf t

R1(config)#cdp holdtime 60
```

14. Trên R1, gõ lệnh sau để xác nhận lại những thay đổi vừa tạo ra ở trên

```
R1#show cdp
```

Đầu ra của câu lệnh sẽ như sau

```
Global CDP information:

    Sending CDP packets every 45 seconds

    Sending a holdtime value of 60 seconds

    Sending CDPv2 advertisements is enabled
```

Nếu R1 không được kết nối trực tiếp với bất kỳ Cisco router nào trên mạng, hoặc đơn giản để tiết kiệm băng thông, ta cần xem xét việc tắt CDP trên R1.

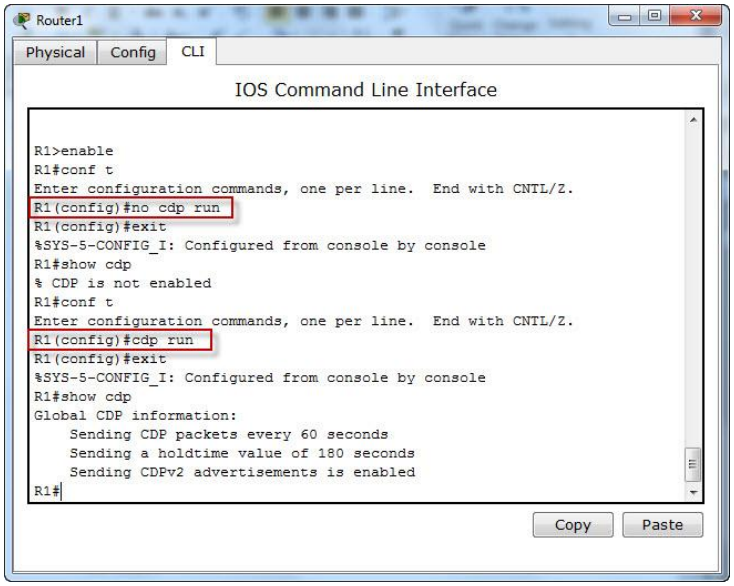
15. Trên R1, để tắt hoàn toàn CDP

```
R1#conf t

R1(config)#no cdp run
```

16. Cũng trên R1, để kích hoạt lại CDP trên tất cả các interface của router

```
R1#conf t

R1(config)#cdp run
```

Lúc này, có thể ta chỉ muốn tắt CDP đối với một số interface cụ thể nào đó, ví dụ các interface có băng thông thấp hoặc vì các lý do bảo mật.



17. Trên R1, để tắt CDP chỉ với interface FastEthernet1/0

```
R1(config)#interface FastEthernet1/0
```

```
R1(config-if)#no cdp enable
```

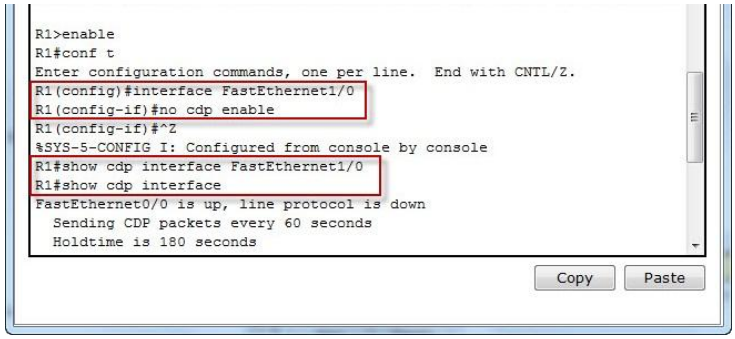
18. Trên R1, để xác nhận interface FastEthernet1/0 không còn gửi đi các gói CDP update nữa, ta gõ

```
R1#show cdp interface
```

hoặc

```
R1#show cdp interface FastEthernet1/0
```

Nếu trong đầu ra không có thông tin về FastEthernet1/0 thì có thể kết luận rằng CDP đã bị vô hiệu hóa trên interface này.



Lab 5: Extended Basics

Ôn tập và mở rộng

A. Mục tiêu của bài lab:

Quan sát và cấu hình một số phần cơ bản của router.

B. Chuẩn bị cho bài lab:

Chúng ta tiếp tục sử dụng Router1.

C. Các bước thực hiện:

1. Truy cập vào CLI của router và hiển thị dấu nhắc lệnh.

```
Router>
```

2. Để xem danh sách tất cả các câu lệnh sẵn có mà ta có thể sử dụng tại dấu nhắc này.

```
Router>?
```

3. Vào Privileged mode. Ở chế độ này thì bạn có toàn quyền điều khiển router.

```
Router>enable

Router#
```

4. Xem các câu lệnh có thể chạy trong Privileged mode

```
Router#?
```

5. Sử dụng lệnh sau để vào Configuration mode để cấu hình cho router.

```
Router#config terminal

Router(config)#
```

6. Hostname của router được dùng để nhận dạng thiết bị trong mạng. Khi đăng nhập vào router, ta sẽ thấy hostname nằm ở đầu dấu nhắc (> hoặc #). Có thể sử dụng hostname để thể hiện vị trí hoặc chức năng của router. Lệnh sau sẽ đặt tên cho Router1 là mmt03

```
Router(config)#hostname mmt

mmt(config)#
```

7. "Enable password" dùng để kiểm soát việc truy cập vào Privileged mode. Đây là loại mật khẩu cực kỳ quan trọng cần bảo mật bởi vì trong Privileged mode bạn có thể thay đổi cấu hình cho router. Để đặt "enable password" thành "network" ta thực hiện lệnh sau

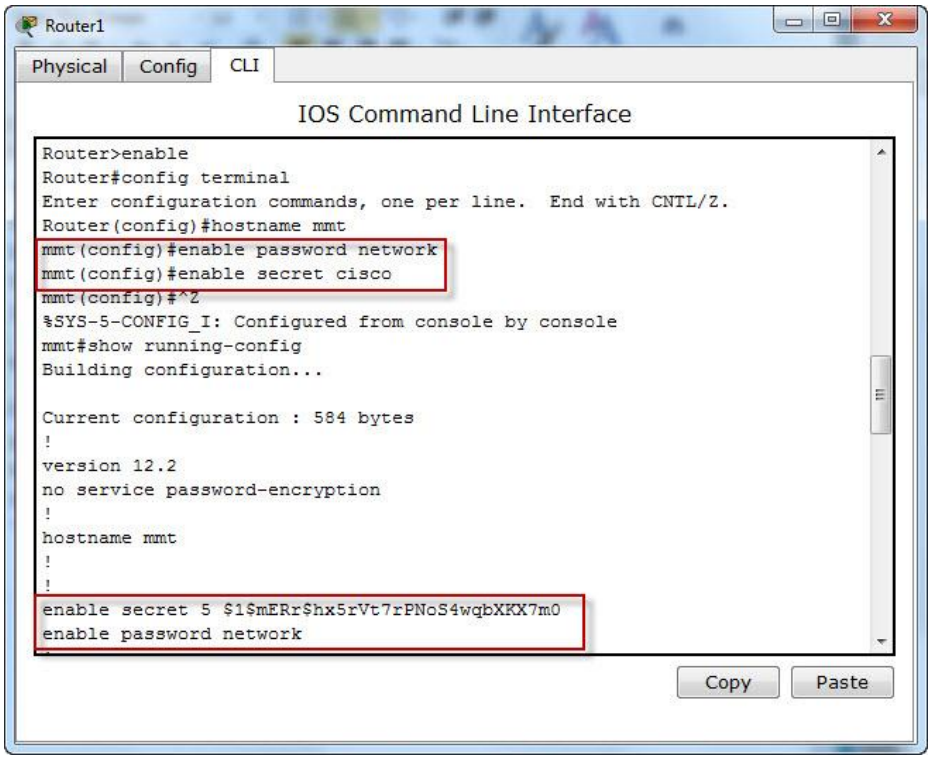
```
mmt(config)#enable password network
```

8. Để kiểm tra password này. Thoát khỏi router và thử vào lại Privileged mode với mật khẩu "network" vừa thiết lập ở trên. Bây giờ, gõ conf term và làm tiếp các hướng dẫn ở bước kế tiếp.

9. Vấn đề duy nhất với "enable password" là nó xuất hiện dưới dạng "plain-text"trong file cấu hình của router. Nếu bạn cần cho ai đó xem file này để họ có thể giúp bạn khắc phục vấn đề nào đó thì vô tình bạn đã để lộ các mật khẩu và điều này đe dọa đến bảo mật của hệ thống của bạn. Vậy làm sao để tạo ra các mật khẩu được mã hóa? Lệnh sau sẽ tạo mật khẩu "cisco" được lưu trữ ở dạng mã hóa.

```
mmt(config)#enable secret cisco
```

10. Giờ ta có thể kiểm tra mật khẩu mới này bằng cách đăng xuất khỏi router và sau đó gõ enable. "Enable secret" là một mật khẩu bổ trợ cao cấp hơn "enable password", thực tế thì nó ghi đè "enable password". Nếu bạn đã thiết lập cả 2 loại mật khẩu này thì "enable secret" mới là mật khẩu mà bạn cần dùng để vào Privileged mode còn "enable password" tuy vẫn hiện diện nhưng hiện tại đã bị vô hiệu hóa.



Lab 6: Setting the Banner MOTD (Message of the Day)

Thiết lập thông báo khi đăng nhập vào router

A. Mục tiêu của bài lab:

MOTD là thông báo được hiển thị khi ai đó đăng nhập vào router. MOTD có thể được sử dụng để cung cấp thông tin về router hoặc hiển thị các thông báo về báo về bảo mật.

B. Chuẩn bị cho bài lab:

Chúng ta tiếp tục sử dụng Router1.

C. Các bước thực hiện:

1. Kết nối tới Router1 và vào Privileged mode

```
Router>

Router>enable

Router#
```

2. Vào Configuration mode

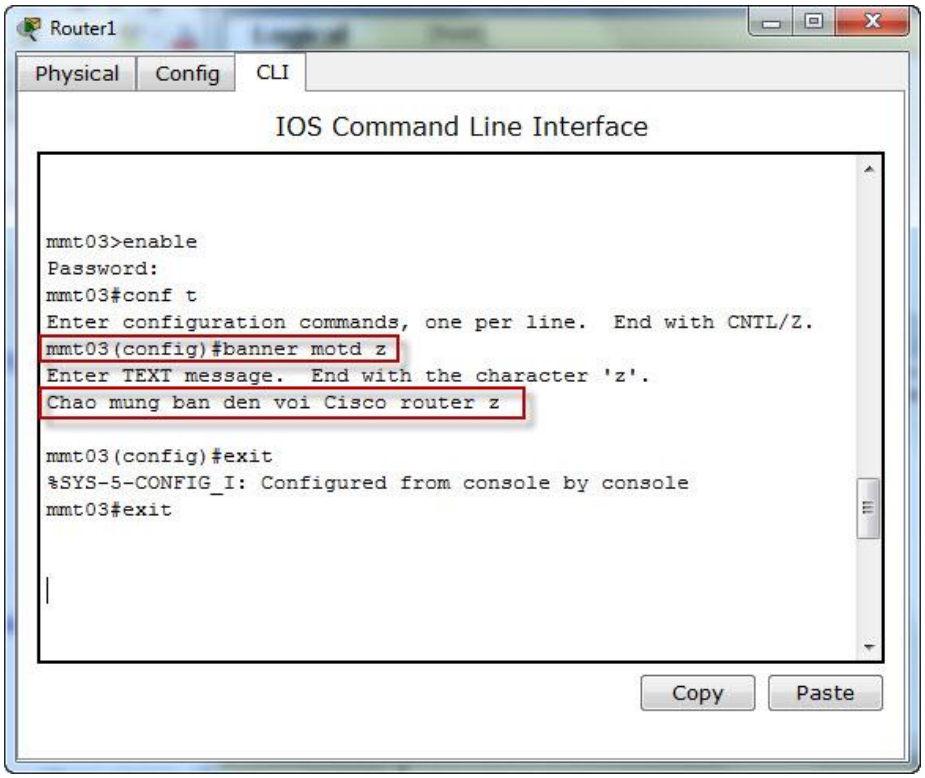
```
Router#config t

Router(config)#
```

3. Gõ vào câu lệnh `banner motd` và tiếp sau đó là một ký tự định giới hạn (delimiting character). Ký tự định giới hạn sẽ được gõ vào tại phần cuối của dòng thông báo để router sẽ biết được là khi nào ta hoàn thành việc gõ vào thông báo. Ký tự thường sử dụng nhất là "z".

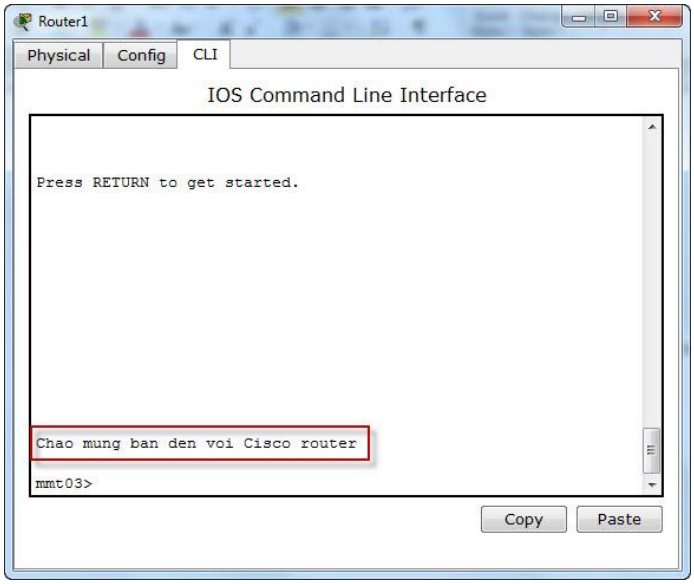
```
Router(config)#banner motd z

Enter TEXT message.  End with the character 'z'.
```

4. Bây giờ, ta sẽ gõ vào thông báo muốn hiển thị lúc đăng nhập vào router, khi cần kết thúc việc gõ thông báo ta sẽ gõ ký tự "z" và nhấn Enter thì lập tức thông báo sẽ được router lưu lại. Ví dụ, để thiết lập MOTD là dòng chữ "Chao mung ban den voi Cisco router" thì gõ

```
Chao mung ban den voi Cisco router z
```



5. Để xem thông báo trên, ta thoát khỏi Configuration mode và sau đó thoát khỏi router. Nhấn Enter để quay trở lại và ta sẽ thấy được thông báo vừa đặt ở trên



Lab 7: Copy command

Lệnh copy

A. Mục tiêu của bài lab:

Giới thiệu về các lệnh copy mà Cisco IOS hỗ trợ

B. Chuẩn bị cho bài lab:

Chúng ta tiếp tục sử dụng Router1.

C. Các bước thực hiện:

1. Hiển thị dấu nhắc lệnh

```
Router>
```

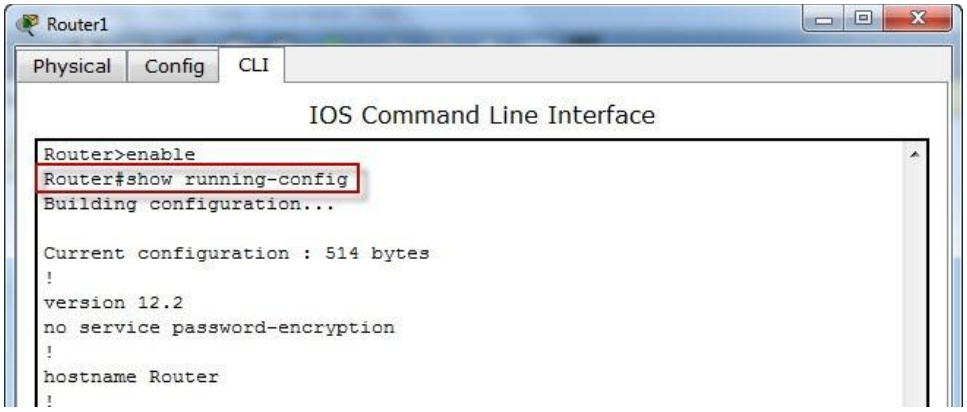
2. Vào Privileged mode

```
Router>enable

Router#
```

3. Hiển thị "running-config" hiện tại được lưu trong bộ nhớ RAM.

```
Router#show running-config
```

4. Thử hiển thị nội dung của file cấu hình được lưu trữ trong bộ nhớ NVRAM (dữ liệu trong NVRAM vẫn còn nguyên vẹn ngay cả khi không có nguồn điện cung cấp cho router), file này được gọi là startup-config. Hiện tại chúng ta chưa lưu cấu hình vào NVRAM nên không có bất kỳ nội dung nào được hiển thị ở đây

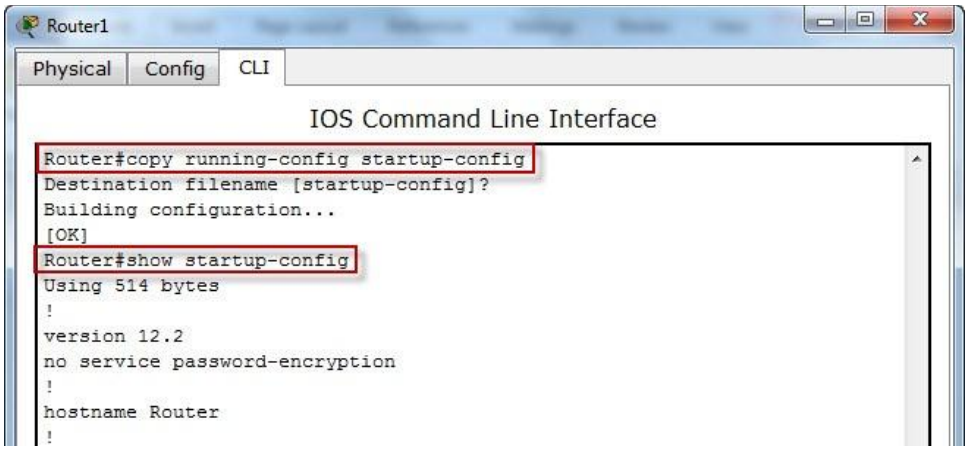


5. Copy nội dung của running-config trong RAM vào NVRAM. Khi router khởi động, nó sẽ nạp cấu hình được lưu trữ trong NVRAM này.

```
Router#copy running-config startup-config
```

6. Bây giờ, hiển thị cấu hình được lưu trong NVRAM.

```
Router#show startup-config
```

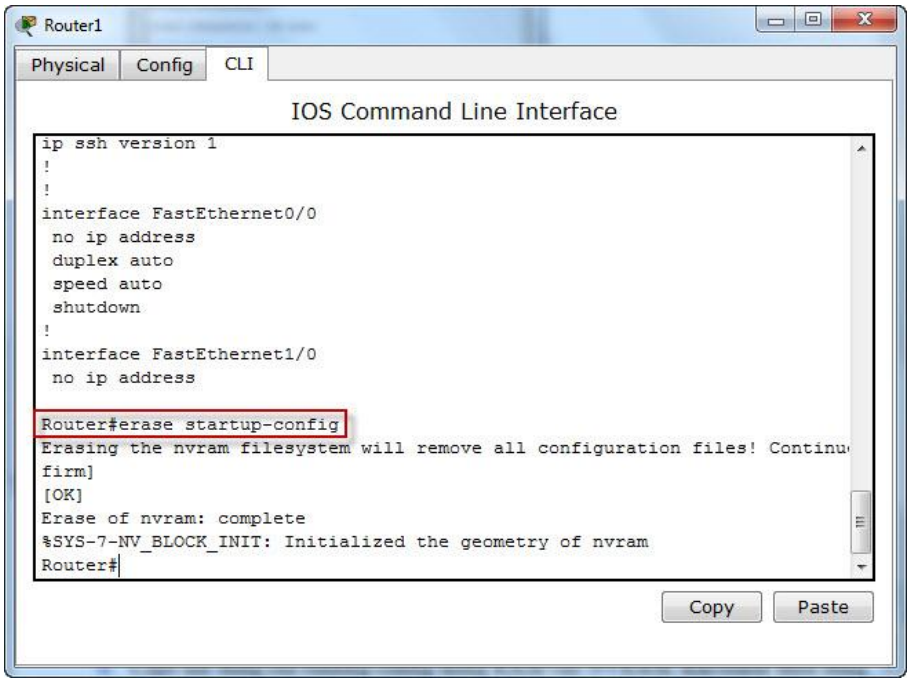


7. Nếu muốn router khởi động lên mà không nạp bất kỳ cấu hình nào (sau đó ta sẽ cấu hình lại cho router từ đầu) thì ta có thể xóa startup-config và nạp lại router. Để xóa cấu hình trong NVRAM, ta gõ

```
Router#erase startup-config
```

8. Giờ ta cần nạp lại router. Router báo cho ta biết là hiện có một cấu hình đang nằm trong RAM và hỏi ta xem có muốn lưu lại cấu hình đó vào NVRAM trước khi nạp lại router không. Vì ta không muốn lưu lại running-config nên ta sẽ chọn no

```
Router#reload
```

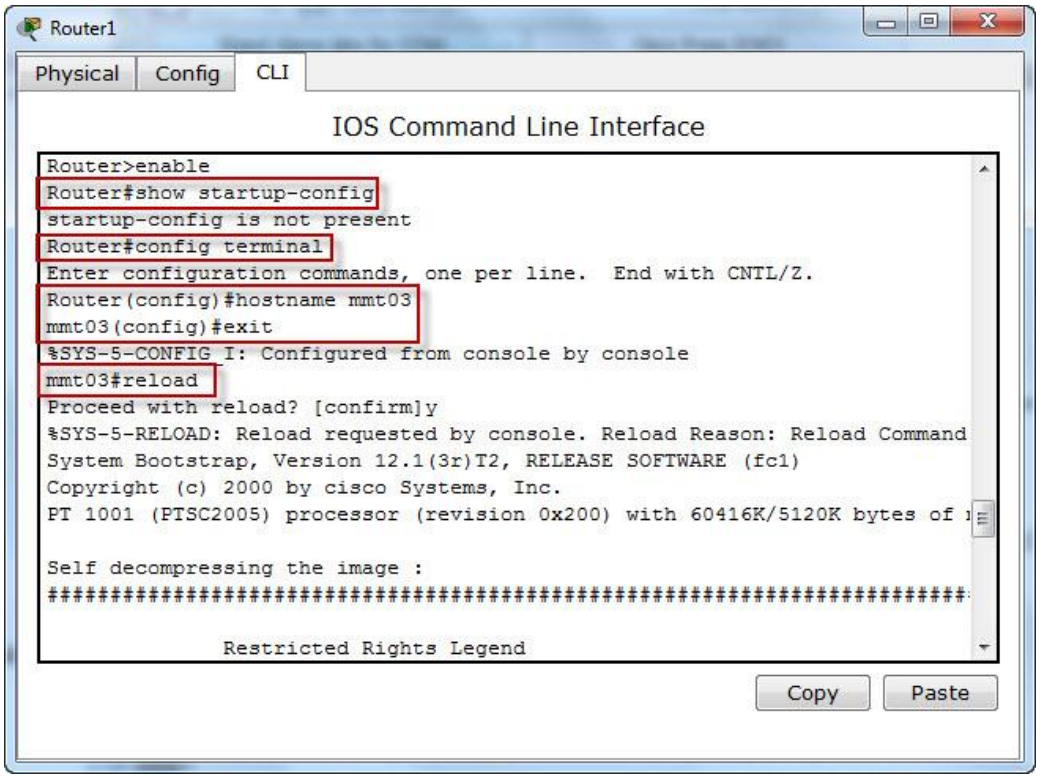


9. Sau router khởi động lại xong, giờ ta xem lại file startup-config. Vì ta đã không lưu lại nó ở bước 8 nên hiện không có thông tin nào trong startup-config cả.

```
Router#show startup-config
```

10. Giờ ta đổi hostname cho router thành mmt03

```
Router#config terminal

Router(config)#hostname mmt03

mmt03(config)#exit

mmt03#
```



11. Sau khi đổi hostname, ta sẽ reload router và khi được hỏi ta sẽ đồng ý lưu lại cấu hình vừa thay đổi này.

```
mmt03#reload
```

12. Sau khi router reload xong, chuỗi mmt03 xuất hiện trong dấu nhắc lệnh.

Lab 8: Introduction to Interface Configuration

Cấu hình các cổng giao tiếp (interface)

A. Mục tiêu của bài lab:

Biết cách kích hoạt và xem thông tin các interface trên một router.

B. Chuẩn bị cho bài lab:

Chúng ta sẽ sử dụng Router1 và Router2.

C. Các bước thực hiện:

1. Trên Router1, vào Global Configuration mode

```
Router>enable

Router#conf t

Router(config)#hostname R1
```

2. Giờ ta sẽ cấu hình cho interface FastEthernet (Fa). Để làm điều này, ta cần truy nhập vào chế độ cấu hình cho interface (Interface Configuration mode – viết tắt là config-if). Gõ lệnh sau để vào "config-if" dành cho Fa0/0

```
R1(config)#interface Fa0/0

R1(config-if)#
```

3. Để xem tất cả các câu lệnh hiện có thể sử dụng trong "config-if"

```
R1(config-if)#?
```

4. Trong đó, lệnh `shutdown` được dùng để tắt/vô hiệu hóa interface

```
shutdown Shutdown the selected interface
```

Để làm điều ngược lại của một lệnh nào đó, ta thêm chữ "no" đằng trước lệnh đó. Vậy lệnh sau sẽ giúp ta kích hoạt lại Fa0/0 trên Router1

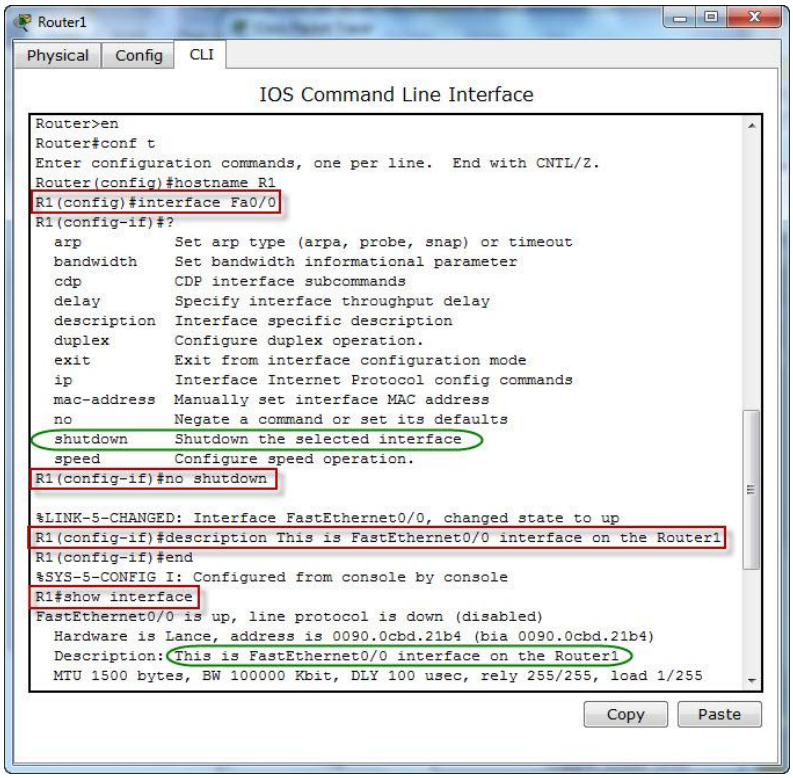
```
R1(config-if)#no shutdown
```

5. Giờ thêm phần mô tả cho interface này

```
R1(config-if)#description This is FastEthernet0/0
interface on the Router1
```

6. Để xem phần mô tả vừa thiết lập ở trên ta trở lại Privileged mode và thực hiện lệnh `show interface`.

```
R1(config-if)#end

R1#show interface
```



7. Bây giờ ta kết nối tới Router2 và vào chế độ "config-if" của Fa0/0

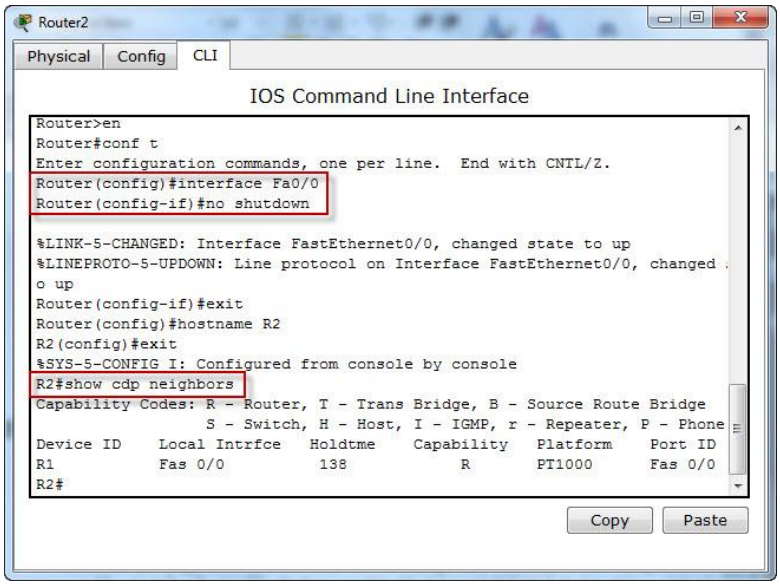
```
Router#conf t

Router(config)#hostname R2

R2(config)#interface Fa0/0
```

8. Kích hoạt interface này lên

```
R2(config-if)#no shutdown
```

9. Hiện tại cổng Fa0/0 trên R1 được nối với cổng Fa0/0 trên R2 và cả 2 cổng Fa0/0 ở 2 đầu của kết nối này đều đã được enable để chúng có thể "thấy" nhau bằng cách sử dụng CDP. Chạy lệnh sau trên R2 để xem tất cả các Cisco router đang được kết nối trực tiếp với nó.

```
R2(config-if)#end

R2#show cdp neighbors
```



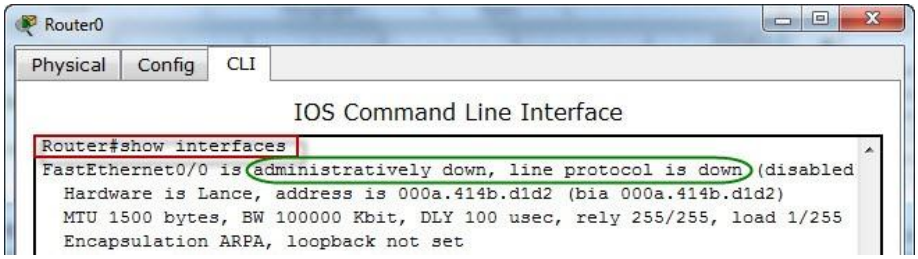
Cấu hình và xem xét thông tin về các interface

Xem xét các interface

Router có thể có nhiều loại interface như token ring, FDDI, Ethernet, Serial, ISDN… Thường ta muốn xem trạng thái về các thiết lập của chúng. Có một vài lệnh quan trọng cần nắm ở đây và show interfaces là một trong những lệnh quan trọng hơn cả

```
Router#show interfaces
```

Lệnh trên sẽ xuất ra các thông tin về mỗi interface. Trong trường hợp này, ta thấy rằng interface Fa0/0 đang bị tạm ngưng hoạt động (administratively down). Điều này có nghĩa là cổng Fa0/0 bị tắt bởi lệnh `shutdown`.



Interface is	Line protocol is	Ý nghĩa
administratively down	Down	Interface bị tắt bởi lệnh `shutdown`
up	Down	Cáp được đấu nối đúng nhưng chưa nhận được keep alive (gói tin cho biết liên kết đang hoạt động tốt) của router ở đầu kết nối bên kia.

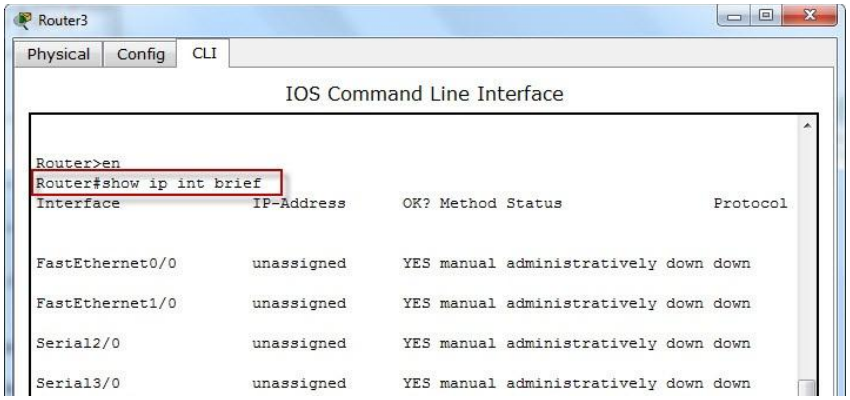
down	Down	Trục trặc ở cáp nối hoặc chưa đặt giá trị clock rate trên DCE hoặc interface của router ở đầu bên kia bị tắt
up	Up	Đây là điều ta muốn: kết nối hoạt động bình thường

Bạn có thể xem thông tin chi tiết về một interface cụ thể nào đó, ví dụ Serial2/0, với lệnh sau:

```
Router#show interface Serial2/0
```

Còn để xem thông tin tóm lược của tất cả các interface, ta có lệnh:

```
Router#show ip int brief
```



Điều này giúp ta nhận diện nhanh chóng trạng thái của tất cả các interface

Xem xét các Controller

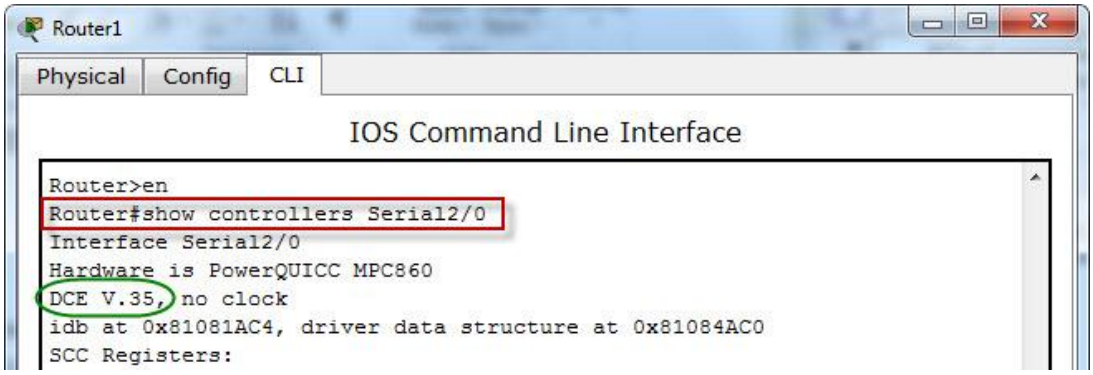
Controller là bộ phận của interface có nhiệm vụ tạo ra các kết nối vật lý. Điều quan trọng nhất mà ta cần biết là loại cáp nào được gắn vào cổng Serial.

Cáp **DTE** (*data terminating equipment*) là loại cáp mà ta thường hay sử dụng. DTE có nghĩa rằng ta đang mong chờ đầu cuối bên kia cung cấp **clocking**.

Cáp **DCE** (*data circuit-terminating equipment*) có nghĩa là thiết bị này sẽ phải cung cấp **clocking** trên đường truyền.

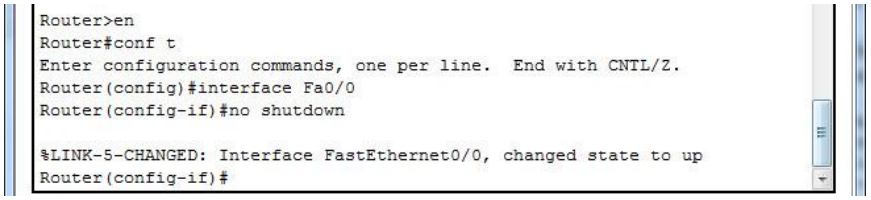
Lệnh `show controllers` sẽ giúp ta biết được interface nào đó là DCE hay DTE.

```
Router#show controllers Serial2/0
```

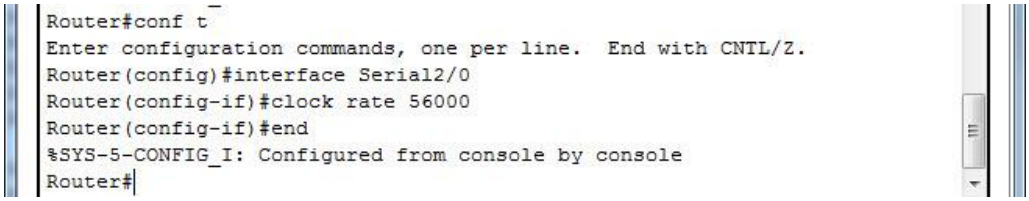


Cấu hình cho interface

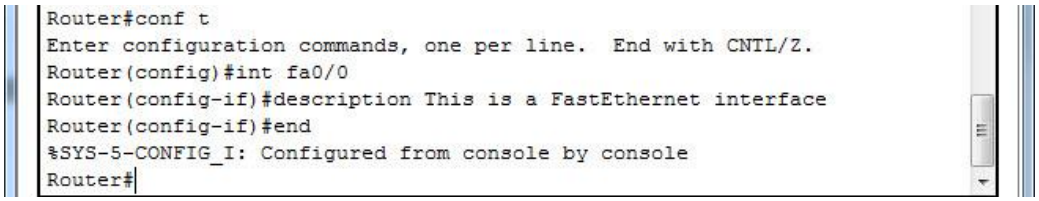
Nếu một interface nào đó bị khóa lại bởi lệnh shutdown (administratively down). Bạn phải vào Configuation mode (config), sau đó truy nhập vào Interface Configuation mode (config-if) dành cho interface đó, và cuối cùng, chạy lệnh `no shutdown`. Dưới đây là hình minh họa cách kích hoạt cho interface Fa0/0 trên Router1.



Nếu interface là DCE, bạn phải cung cấp giá trị clocking sử dụng lệnh clock rate



Thật hữu ích để thêm phần mô tả ý nghĩa của interface sử dụng lệnh `description`



Sử dụng lệnh `show running-config` hoặc `show interfaces` hoặc `show controllers` để xem những thay đổi mà ta vừa tạo ra ở trên.

Lab 9: Introduction to IP (Internet Protocol)

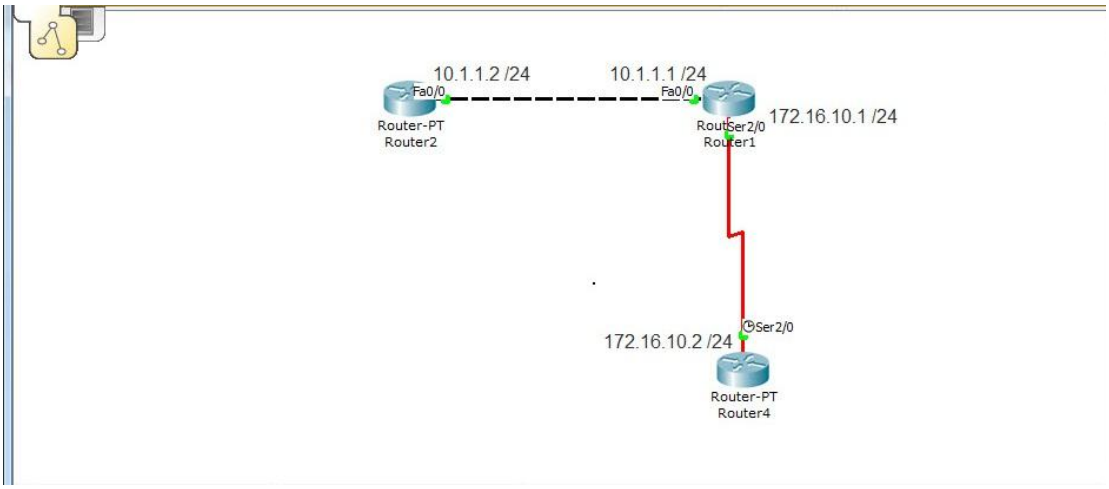
Giao thức IP

A. Mục tiêu của bài lab:

Cấu hình địa chỉ IP cho các Router 1, 2 và 4 và sử dụng lệnh ping để kiểm tra kết nối giữa chúng.

B. Chuẩn bị cho bài lab:

Chúng ta sẽ sử dụng Router1, Router2, Router4.



C. Các bước thực hiện:

Cấu hình các địa chỉ IP

1. Đầu tiên, kết nối tới Router1 và đặt hostname cho nó là R1

```
Router>en
Router#conf t
Router(config)#hostname R1
```

2. Vào chế độ Interface configuration để đặt địa chỉ IP cho cổng fa0/0 trên Router1

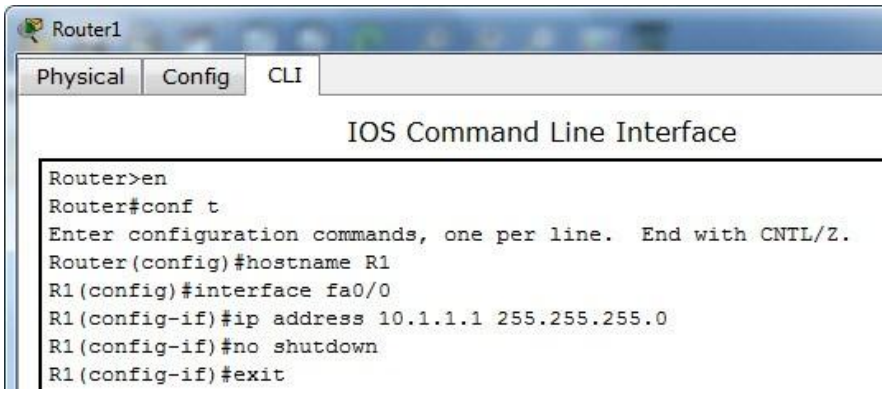
```
R1(config)#interface fa0/0
```

3. Đặt địa chỉ IP cho cho cổng fa0/0 này như sau

```
R1(config-if)#ip address 10.1.1.1 255.255.255.0
```

4. Kích hoạt interface fa0/0 này lên

```
R1(config-if)#no shutdown
```



5. Giờ đặt địa chỉ IP cho interface Serial2/0 trên R1 như sau

```
R1(config)#interface Ser2/0
R1(config-if)#ip address 172.16.10.1 255.255.255.0
R1(config-if)#no shut
```

6. Mở CLI của Router2 lên

7. Gán hostname cho nó là R2

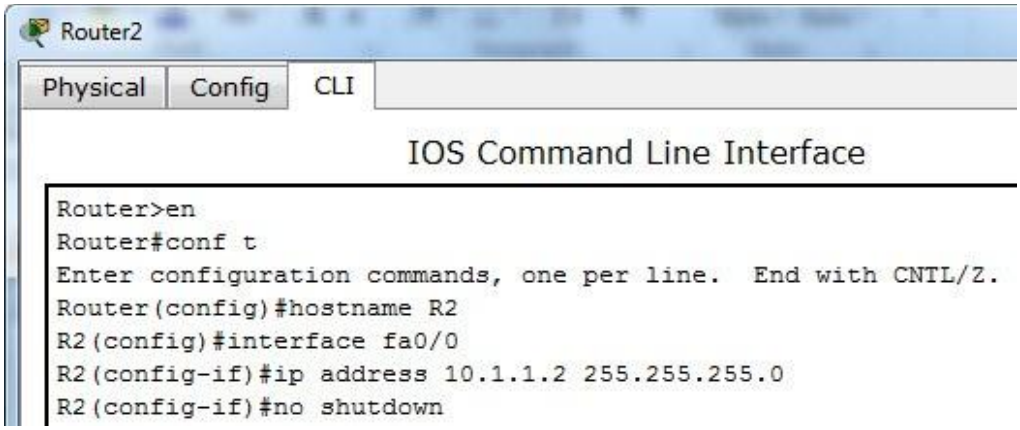
```
Router>en
Router#conf t
Router(config)#hostname R2
```

8. Đặt địa chỉ IP cho cổng fa0/0 trên R2 này như sau

```
R2(config)#interface fa0/0
R2(config-if)#ip address 10.1.1.2 255.255.255.0
```

9. Kích hoạt interface này lên

```
R2(config-if)#no shutdown
```



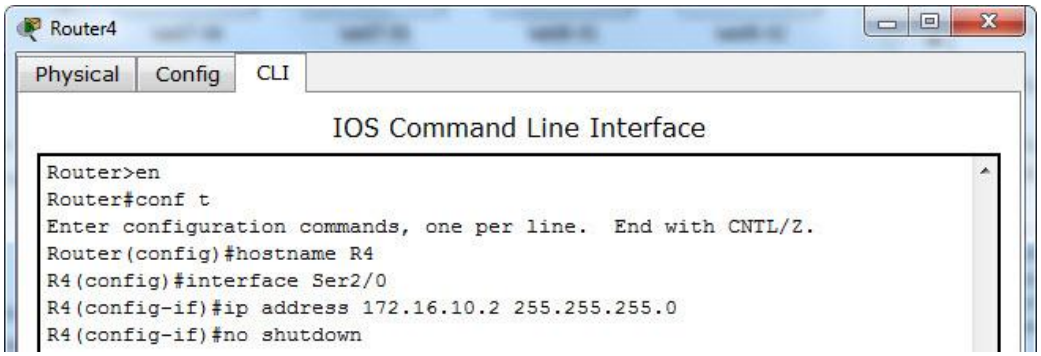
10. Giờ ta truy cập vào CLI của Router4

11. Gán hostname cho Router4 và sau đó đặt địa chỉ IP cho cổng Serial2/0 như sau

```
Router>en

Router#conf t

Router(config)#hostname R4

R4(config)#interface Ser2/0

R4(config-if)#ip address 172.16.10.2 255.255.255.0
```

12. Tiếp tục kích hoạt cổng Serial2/0 trên R4

```
R4(config-if)#no shutdown
```



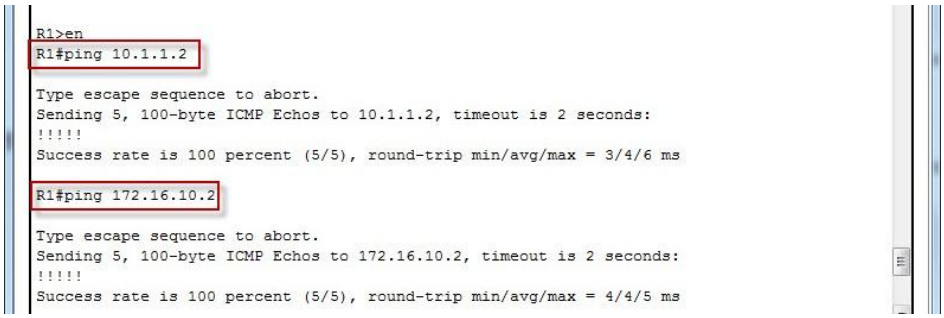
13. Kết nối trở lại tới Router1

14. Thử ping tới cổng fa0/0 trên Router2

```
R1(config-if)#ping 10.1.1.2
```

15. Thử ping tới cổng Serial2/0 trên Router4

```
R1#ping 172.16.10.2
```



16. Kiểm tra và bảo đảm trạng thái đường kết nối và trạng thái giao thức của các interface trên Router đều "UP"

```
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        10.1.1.1        YES manual up                    up

FastEthernet1/0        unassigned      YES manual administratively down down

Serial2/0              172.16.10.1     YES manual up                    up
```

17. Xem nội dung của running-config và kiểm tra xem việc đặt IP đã đúng chưa

```
R1#show running-config
```

18. Xem thông tin chi tiết về IP cho mỗi interface

```
R1#show ip interface
```

```
!
!
interface FastEthernet0/0
 ip address 10.1.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial2/0
 ip address 172.16.10.1 255.255.255.0
!
interface Serial3/0
 no ip address
```

Lab 10: ARP

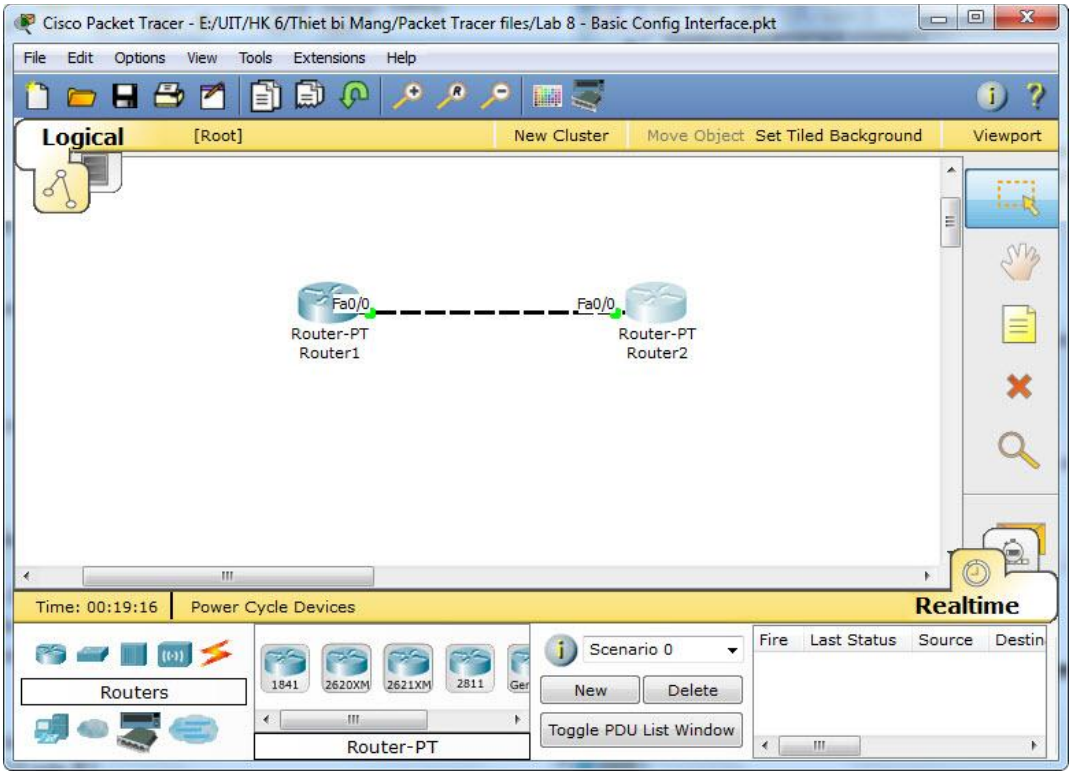
Giao thức ARP

A. Mục tiêu của bài lab:

Xem thông tin trong bảng ARP

B. Chuẩn bị cho bài lab:

Chúng ta sẽ sử dụng Router1 và Router2.



C. Các bước thực hiện:

1. Kết nối tới Router1 (có hostname là R1) và xem bảng ARP của nó.

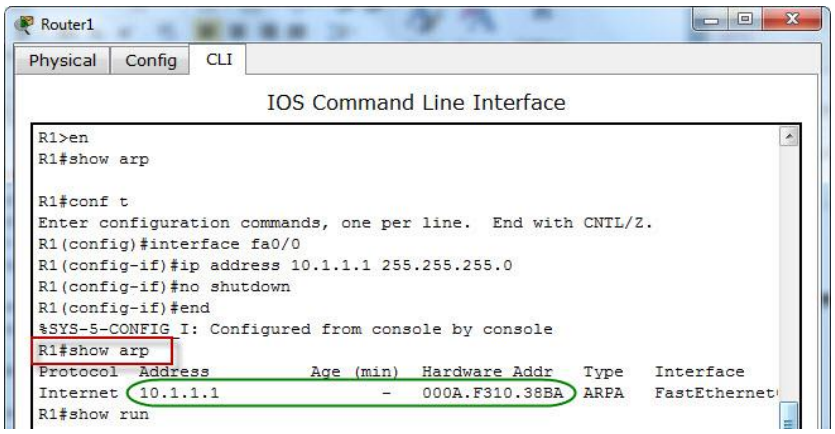
```
R1>en
R1#show arp
```

2. Gán địa chỉ IP cho cổng Fa0/0 trên R1.

```
R1#conf t
R1(config)#interface fa0/0
R1(config-if)#ip address 10.1.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#end
```

3. Xem lại bảng ARP của R1. Lúc này ta thấy xuất hiện một dòng (entry) duy nhất là thông tin về cổng Fa0/0 trên R1

```
R1#show arp
```



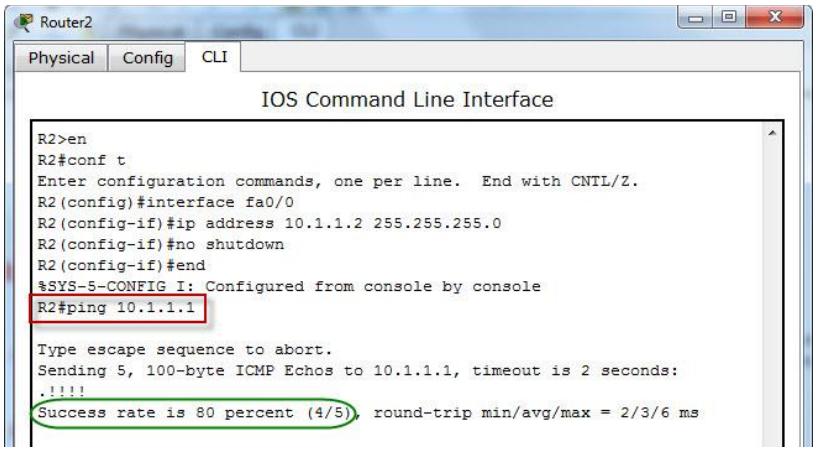
4. Truy cập vào CLI của Router2 (có hostname là R2)

5. Đặt địa chỉ IP cho cổng Fa0/0 trên R2 như sau

```
R2>en
R2#conf t
R2(config)#interface fa0/0
R2(config-if)#ip address 10.1.1.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#end
```

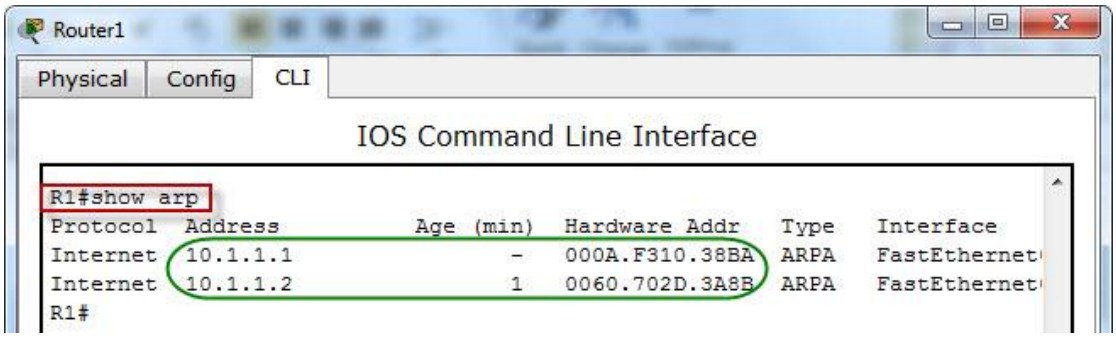
6. Hiện ta đã có một kết nối giữa 2 cổng Fa0/0 trên R1 và R2. Để chắc rằng kết nối này hoạt động tốt, trên R2 ta ping thử tới địa chỉ IP của cổng Fa0/0 trên R1.

```
R2#ping 10.1.1.1
```



7. Giờ xem lại bảng ARP trên R1 và để ý thấy là đã xuất hiện thêm một entry dành cho cổng Fa0/0 trên R2.

```
R1#show arp
```

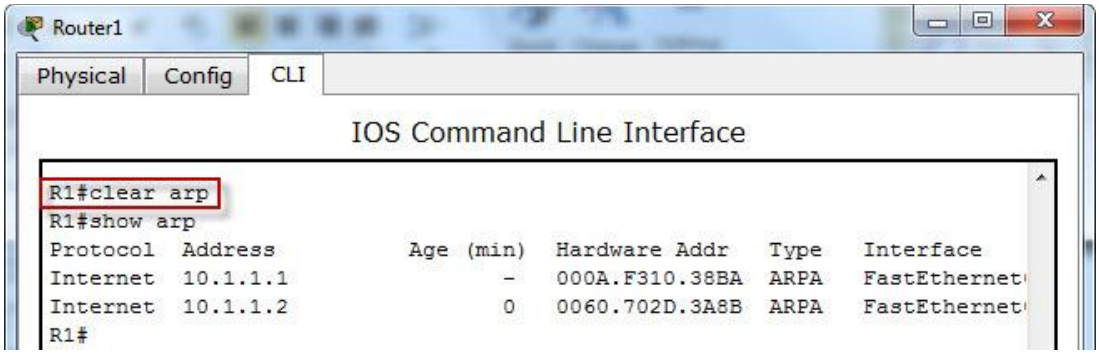


8. Giờ ta sẽ xây dựng lại bảng ARP trên R1, chạy lệnh sau để xóa thông tin trong bảng ARP này.

```
R1#clear arp
```

9. Xem lại bảng ARP của R1 lần cuối và ghi nhận lại các entry trong đó.

```
R1#show arp
```



Lab 11: Creating a Host table

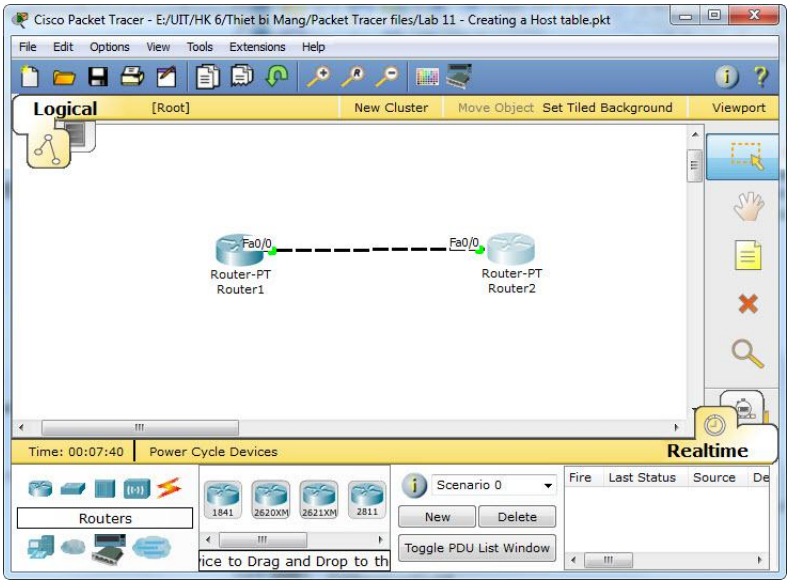
Tạo bảng Host

A. Mục tiêu của bài lab:

Làm quen với bảng host của router. Ta sử dụng bảng host để đặt tên cho địa chỉ IP thường hay sử dụng, tức là ta sẽ có một cặp ánh xạ giữa tên (dạng chuỗi ký tự) và địa chỉ IP (dạng số).

B. Chuẩn bị cho bài lab:

Chúng ta sẽ sử dụng Router1 và Router2. Hai router này được nối lại với nhau (bằng cáp chéo) sử dụng cổng Fa0/0 trên mỗi router như hình sau



C. Các bước thực hiện:

1. Truy cập vào CLI của Router1 và vào Privileged mode

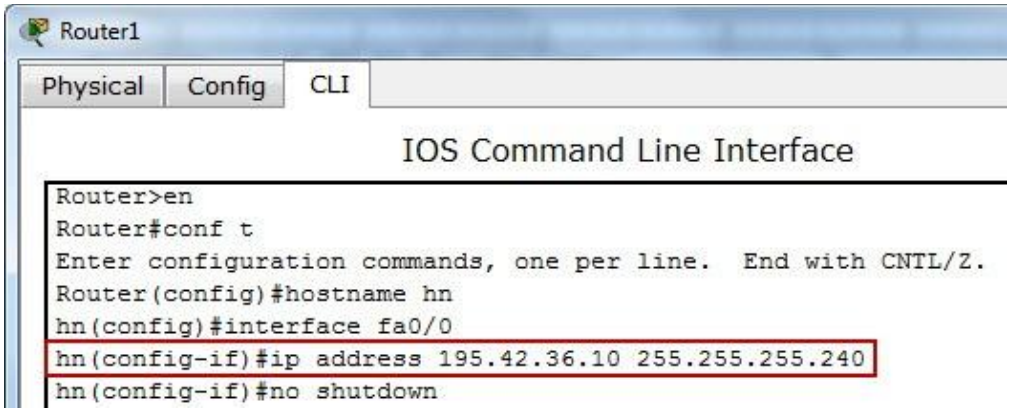
```
Router>enable
Router#
```

2. Vào Configuation mode và đặt hostname cho Router1 là hn

```
Router#conf t
Router(config)#hostname hn
hn(config)#
```

3. Đặt địa chỉ IP cho cổng Fa0/0 trên Router1 và kích hoạt cổng này lên như sau

```
hn(config)#interface fa0/0
hn(config-if)#ip address 195.42.36.10 255.255.255.240
hn(config-if)#no shutdown
```



4. Giờ ta truy cập vào CLI của Router2 và vào Privileged mode

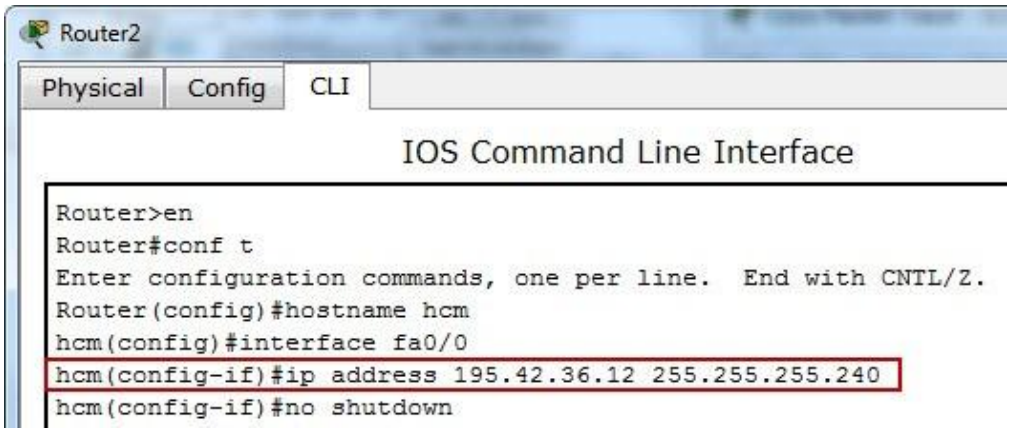
```
Router>enable
Router#
```

5. Vào Configuation mode và đặt hostname cho Router2 là hcm

```
Router#conf t
Router(config)#hostname hcm
hcm(config)#
```

6. Đặt địa chỉ IP cho cổng Fa0/0 trên Router2 và kích hoạt cổng này lên như sau

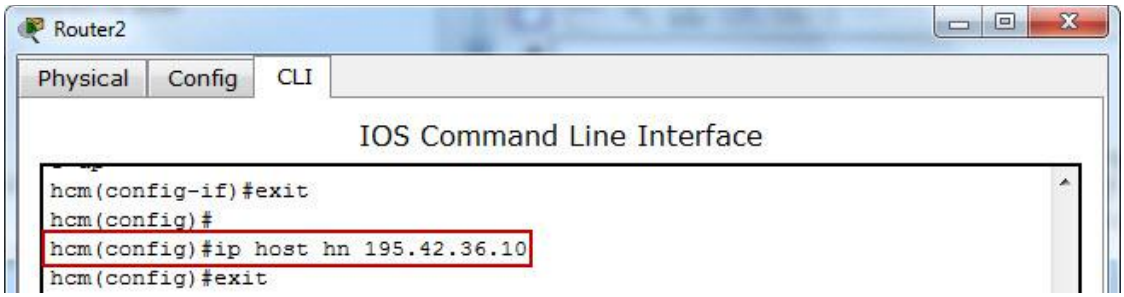
```
hcm(config)#interface fa0/0
hcm(config-if)#ip address 195.42.36.12 255.255.255.240
hcm(config-if)#no shutdown
```



7. Thoát khỏi "config-if" mode. Giờ ta không muốn phải gõ vào địa chỉ IP của cổng Fa0/0 trên Router1 (hn) mỗi lần ta thử ping tới địa chỉ IP đó nên ta sẽ tạo ra một entry

trong bảng host của Router2 (hcm) là ánh xạ giữa hostname của Router1 (là hn, nhưng thật ra bạn chọn một tên khác bất kỳ cũng được) và IP là 195.42.36.10

```
hcm(config-if)#exit
hcm(config)#
hcm(config)#ip host hn 195.42.36.10
```

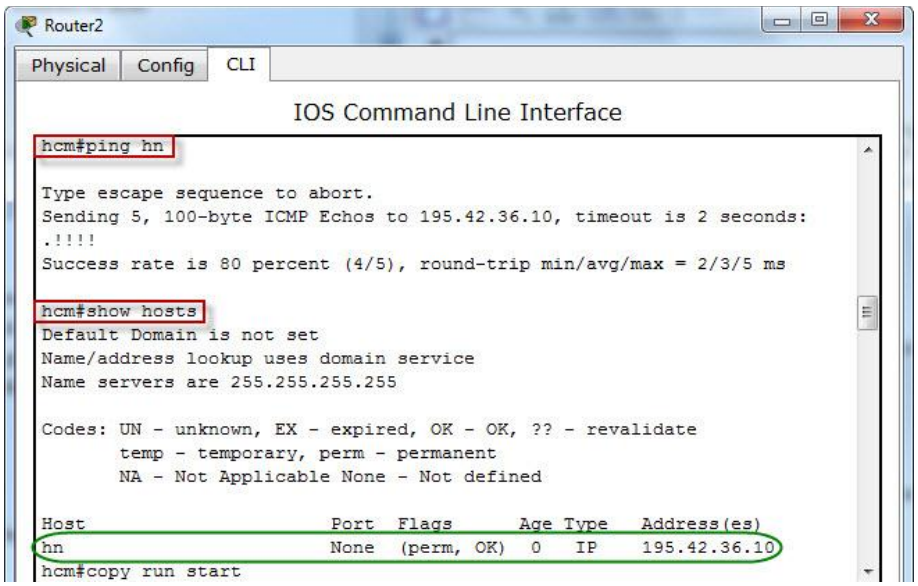


8. Sau đó, ta đã có thể ping tới địa chỉ IP của cổng Fa0/0 trên Router2 sử dụng hostname là hn của nó

```
hcm(config)#exit
hcm#ping hn
```

9. Xác nhận lại rằng entry ở trên đã có trong bảng host của Router1 với lệnh sau

```
hcm#show hosts
```



Lab 12: Static Routes

Cấu hình Static Route

A. Mục tiêu của bài lab:

Đặt địa chỉ IP cho các interface trên các Router 1, 2 và 4 và sau đó thêm các "static route" vào bảng định tuyến trên các router này để chúng có thể liên lạc được với nhau.

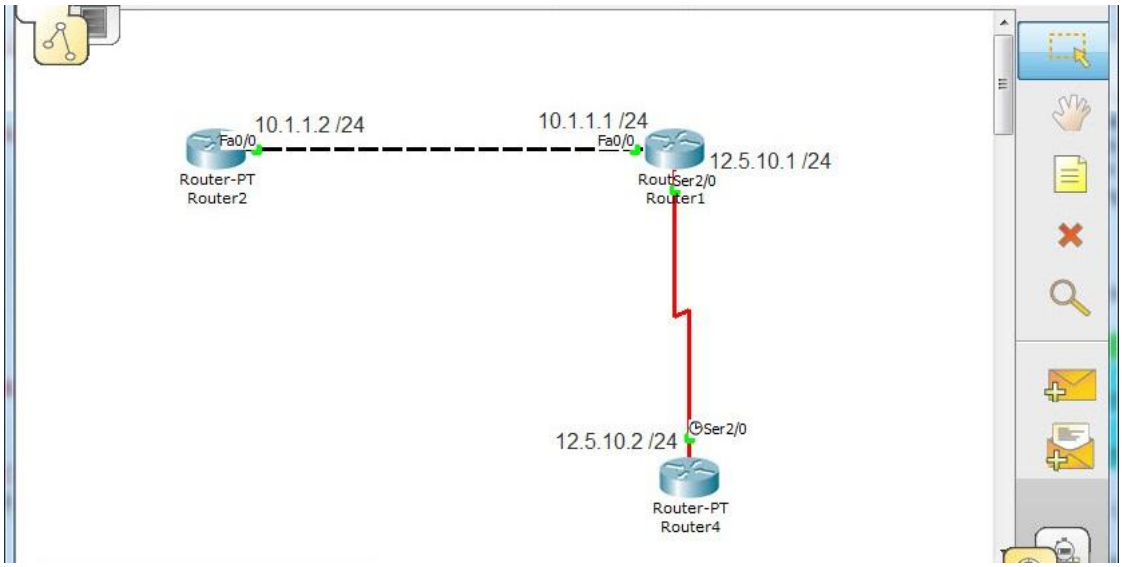
1. Đặt hostname cho các router và kích hoạt các interface của chúng.
2. Ping qua lại giữa các interface được kết nối trực tiếp với nhau.
3. Thiết lập các static route.
4. Xem bảng định tuyến (routing table).
5. Kiểm tra lại là các router có thể ping qua lại lẫn nhau.

B. Chuẩn bị cho bài lab:

Chúng ta sẽ sử dụng Router 1, 2 và 4.

C. Các bước thực hiện:

1. Dưới đây là sơ đồ kết nối giữa các router và các địa chỉ IP được gán cho các interface trên các router.



2. Sau khi cấu hình xong địa chỉ IP trên mỗi interface như trong hình trên, ta sẽ sử dụng lệnh ping để kiểm tra rằng các router được nối trực tiếp nhau thì có thể liên lạc được với nhau. Tức là khi bạn đang ở Router1 thì bạn có thể ping tới cổng Fa0/0 của Router 2 và cổng Ser2/0 của Router 4.

```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface fa0/0
R1(config-if)#ip address 10.1.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface ser2/0
R1(config-if)#ip address 12.5.10.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console
R1#ping 10.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/5 ms

R1#ping 12.5.10.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.5.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/3/4 ms

R1#
```

Trên Router 2: đặt IP cho cổng Fa0/0 và ping thử tới cổng Fa0/0 của Router 1

```
R2>en
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface fa0/0
R2(config-if)#ip address 10.1.1.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console
R2#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 4/4/5 ms

R2#
```

Trên Router 4: đặt IP cho cổng Ser2/0 và ping thử tới cổng Ser2/0 của Router 1

```
R4>en
R4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#interface ser2/0
R4(config-if)#ip address 12.5.10.2 255.255.255.0
R4(config-if)#clock rate 56000
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console
R4#ping 12.5.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.5.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/5 ms

R4#
```

3. Giờ ta bắt đầu cấu hình static route trên mỗi router. Đầu tiên, xem xét R1. Ta cần tạo các static route tới bất kỳ vị trí (node) nào mà chưa được kết nối trực tiếp với R1. Nhưng rõ ràng, R1 hiện đang được kết nối trực tiếp tới cả Router 2 và Router 4 vì thế ta không cần cấu hình bất kỳ static route nào trên R1. Kế tiếp, ta sẽ kết nối tới R4.

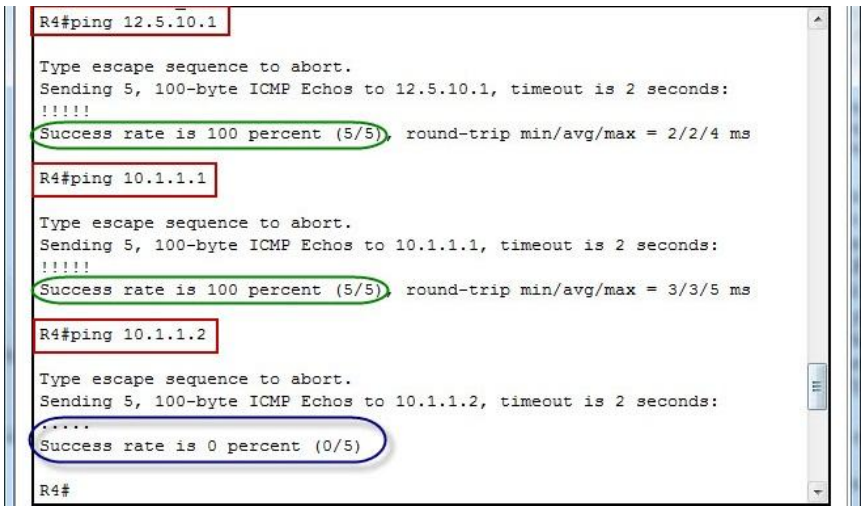
4. Giờ vào Configuration mode trên R4 và nghĩ về câu lệnh nào được dùng để cấu hình static route cho nó? Hiện ta biết được rằng R4 không thể liên lạc với R2 bởi 2 router này không được nối trực tiếp với nhau. Cổng Ser2/0 của R4 có địa chỉ IP thuộc mạng 12.5.10.0 và được nối với cổng Ser2/0 của R1. R1 cũng được kết nối trực tiếp tới mạng 10.1.1.0 là mạng mà ta muốn R4 tới được. Vậy trong trường hợp này ta sẽ cần một static route cho mạng 10.1.1.0. Trên R4, gõ lệnh sau để thiết lập một static route tới mạng 10.1.1.0 này

```
R4(config)#ip route 10.1.1.0 255.255.255.0 12.5.10.1
```

Chúng ta vừa tạo trên R4 một route để tới mạng 10.1.1.0. Giờ thì bất cứ khi nào một gói tin được gửi cho mạng 10.1.1.0 thì nó sẽ được gửi tới router có địa chỉ IP là 12.5.10.1 (ở đây là cổng Ser2/0 của R1).

5. Hãy xem ta đã có được điều gì qua bước 4. Lúc chưa tạo static route trên, ta biết rõ là có thể ping thành công tới cổng Ser2/0 của R1 nhưng lại không thể ping tới cổng Fa0/0 của R1. Giờ ta vừa thiết lập một route tới mạng 10.1.1.0. Để chắc rằng route này hoạt động tốt, ta sẽ thử ping tới cổng Ser2/0 của R1, Fa0/0 của R1 và Fa0/0 của R2.

```
R4#ping 12.5.10.1
R4#ping 10.1.1.1
R4#ping 10.1.1.2
```

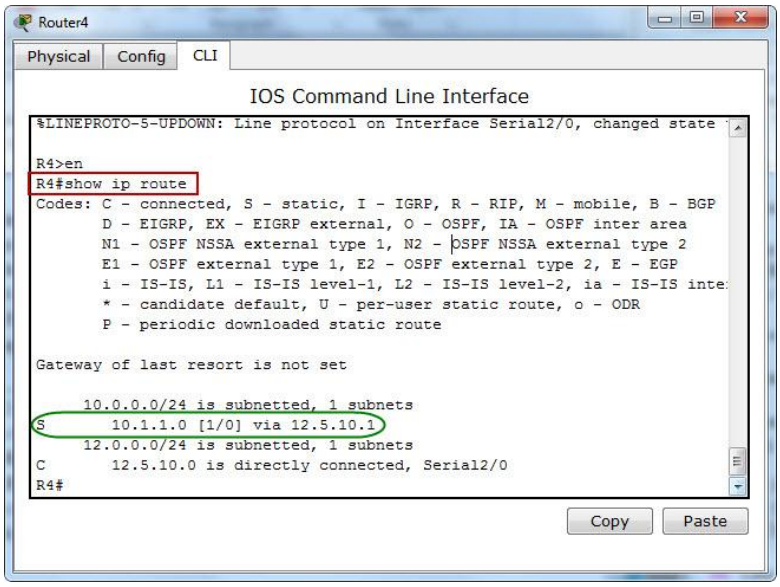


6. Qua kết quả của 3 lệnh ping được thể hiện như trong hình trên ta thấy, chỉ có duy nhất địa chỉ IP 10.1.1.2 (cổng Fa0/0 của R2) là không hề gửi lại bất cứ gói ICMP reply nào cho R4, tại sao lại như vậy?

   Bạn thử hình dung và suy luận thế này: một gói tin luân chuyển trong mạng (trong trường hợp này là gói tin ICMP echo mà R4 gửi tới 10.1.1.2) có địa chỉ **mạng đích** là **10.1.1.0** khi tới R4 thì dựa vào static route (được lưu trong bảng định tuyến của R4) ở trên mà R4 sẽ quyết định đẩy gói tin đó ra ngoài cổng Ser2/0 của nó và chuyển tới cổng Ser2/0 của R1. Và do R1 được kết nối trực tiếp với mạng 10.1.1.0 nên R1 sẽ gửi gói tin ra ngoài cổng Fa0/0 của nó.

   Sau đó, R2 nhận được gói tin mà vừa R1 gửi tới và nó muốn phản hồi lại cho R4 một thông điệp để báo rằng "Này, bạn đã tìm thấy tôi rồi!". R2 bắt đầu kiểm tra gói tin và thấy rằng địa chỉ IP nguồn là 12.5.10.2 (cổng Ser2/0 của R4) nhưng trong bảng định tuyến của R2 hiện chưa có route nào dành cho mạng 12.5.10.0 (mà 12.5.10.2 thuộc về) nên nó đành hủy bỏ (drop) gói tin này và đồng thời không gửi lại gói tin phản hồi cho R4. Đó là lý do tại sao R4 không nhận được gói ICMP reply nào khi ping tới 10.1.1.2.

7. Xem bảng định tuyến của R4 để đảm bảo có tồn tại static route mà ta vừa tạo ở trên

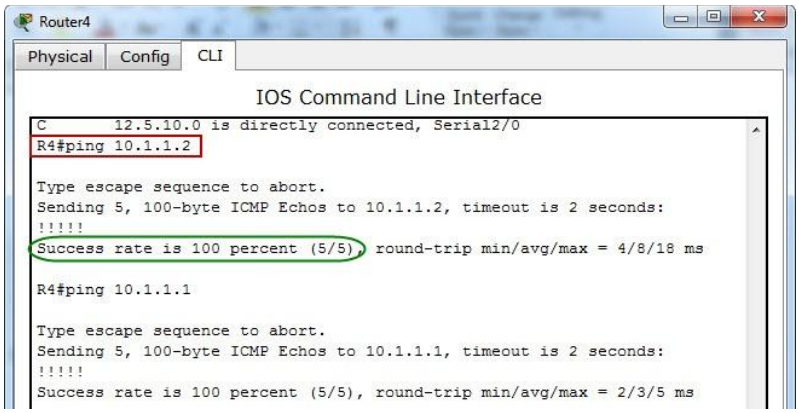


8. Để hoàn tất việc cấu hình static route nhằm đảm bảo 3 router đều liên lạc được với nhau thì ta cần kết nối tới R2 và tạo một static route cho mạng 12.5.10.0 (mạng mà R4 kết nối trực tiếp tới). Gõ lệnh sau trong CLI của R2

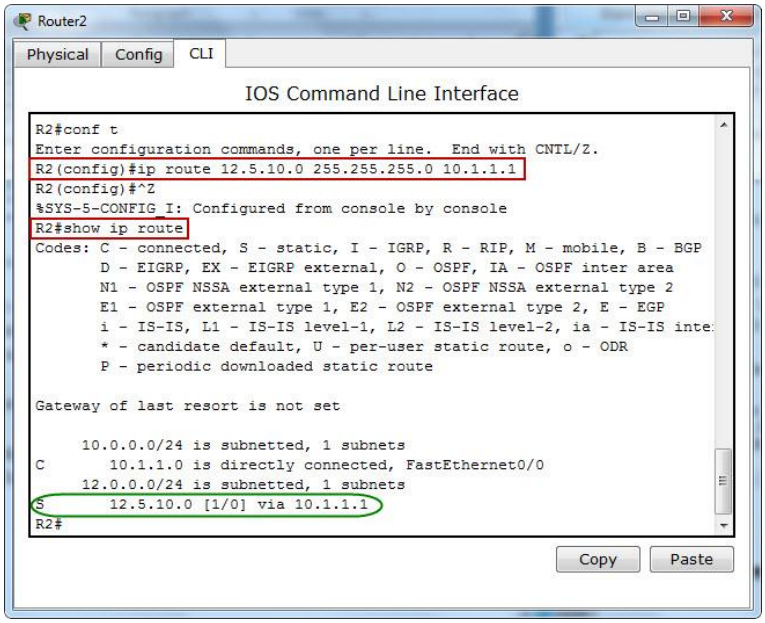
```
R2(config)#ip route 12.5.10.0 255.255.255.0 10.1.1.1
```

Điều này có nghĩa rằng bất cứ gói tin nào R2 gửi tới mạng 12.5.10.0 sẽ phải đi qua 10.1.1.1 (cổng Fa0/0 của R1) trước.

9. Trở lại R4 và chắc rằng ta có thể ping tới tất cả các interface hiện đang hoạt động



10. Xem qua bảng định tuyến của R2



Để ý dòng được khoanh viền màu xanh ta sẽ thấy có ký tự S có nghĩa là static route. Kế tiếp ta xem mạng đích và thông tin về subnet. [1/0] lần lượt cho ta biết giá trị administrative distance (mặc định là "1") và giá trị metric (trong trường hợp là số lượng hop) ở đây là bằng 0. Cuối cùng để đi tới mạng 12.5.10.0 này thì gói tin sẽ cần đi tới địa chỉ 10.1.1.1.

Lab 13: RIP

Cấu hình RIP

A. Mục tiêu của bài lab:

Đặt địa chỉ IP cho các interface trên các Router 1, 2 và 4 và sau đó cấu hình RIP cho các router. Cụ thể ta sẽ làm các công việc sau:

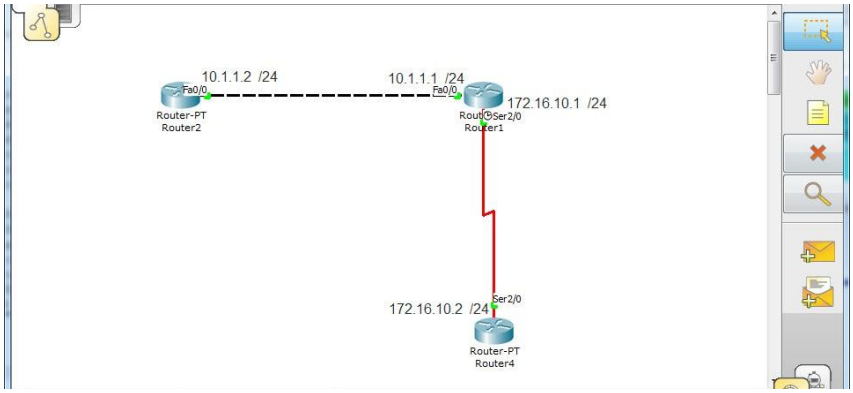
1. Đặt hostname cho các router và kích hoạt các interface của chúng.
2. Cấu hình RIP.
3. Chọn các mạng được kết nối trực tiếp với nhau.
4. Xem bảng định tuyến.
5. Xem thông tin về giao thức RIP.

B. Chuẩn bị cho bài lab:

Chúng ta sẽ sử dụng Router 1, 2 và 4.

C. Các bước thực hiện: *(cách làm của bước 1 và 2 của 2 bài lab 12 và lab 13 này khá giống nhau, chỉ khác nhau ở các địa chỉ IP được gán cho các interface)*

1. Dưới đây là sơ đồ kết nối giữa các router và các địa chỉ IP được gán cho các interface trên các router.



2. Sau khi đã cấu hình xong các địa chỉ IP cho mỗi interface ta cần kiểm tra xem các Router là 'hàng xóm' của nhau (được kết nối trực tiếp với nhau) có thể "thấy" nhau (liên lạc được) hay không.

3. Giờ ta đi vào bước cấu hình RIP làm giao thức định tuyến cho các router. Thật dễ dàng để cấu hình với RIP; đầu tiên ta cần vào Configurarion mode trên R1.

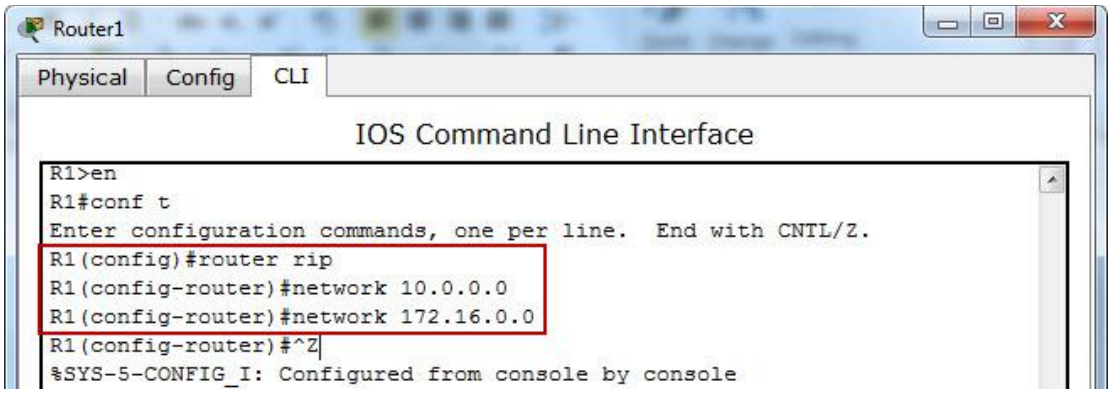
```
R1#
R1#config t
R1(config)#
```

4. Gõ lệnh sau để cấu hình RIP cho R1.

```
R1(config)#router rip
R1(config-router)#
```

5. Thêm các mạng mà R1 kết nối trực tiếp tới.

```
R1(config-router)#network 10.0.0.0
R1(config-router)#network 172.16.0.0
```



6. Ta vừa cấu hình RIP cho R1, giờ kết nối tới R2 và vào Configuration mode

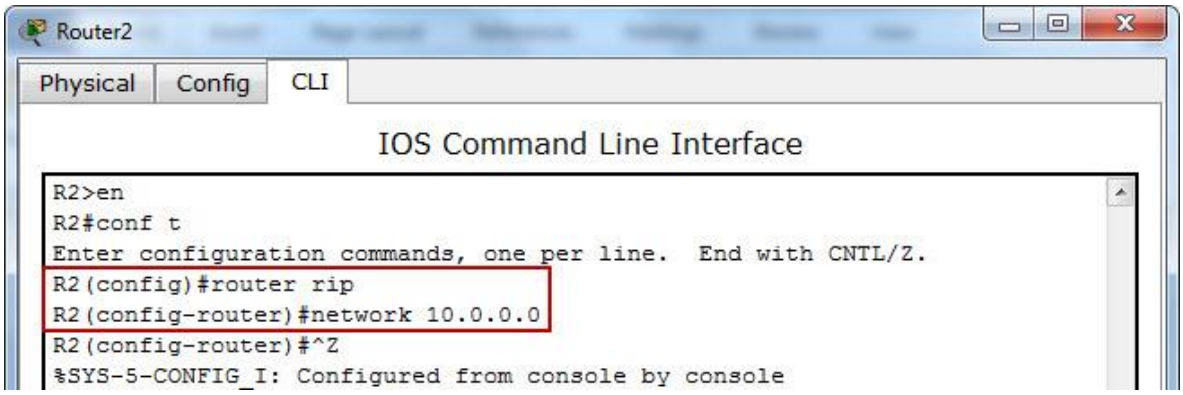
```
R2#
R2#config t
R2(config)#
```

7. Cấu hình RIP cho R2.

```
R2(config)#router rip
R2(config-router)#
```

8. Thêm (các) mạng mà R2 kết nối trực tiếp tới.

```
R2(config-router)#network 10.0.0.0
```



9. Tiếp theo ta sẽ cấu hình RIP cho R4. Kết nối tới R4 và vào Configuration mode

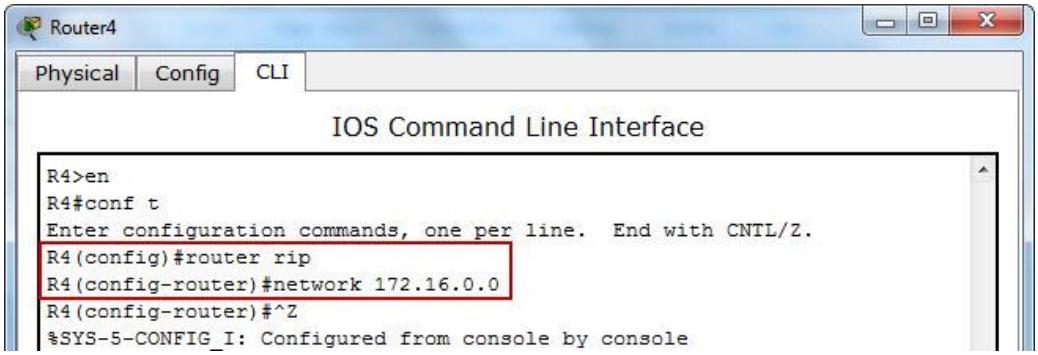
```
R4#
R4#config t
R4(config)#
```

10. Cấu hình RIP cho R4.

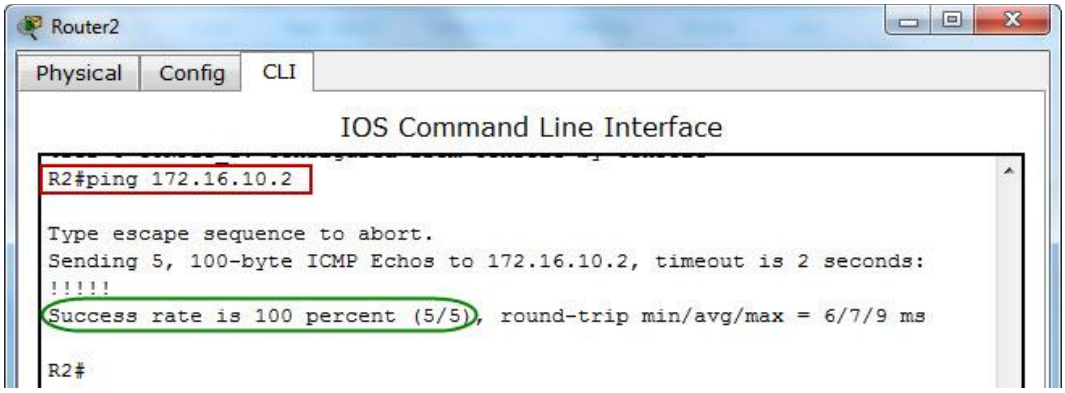
```
R4(config)#router rip
R4(config-router)#
```

11. Thêm (các) mạng mà R4 kết nối trực tiếp tới.

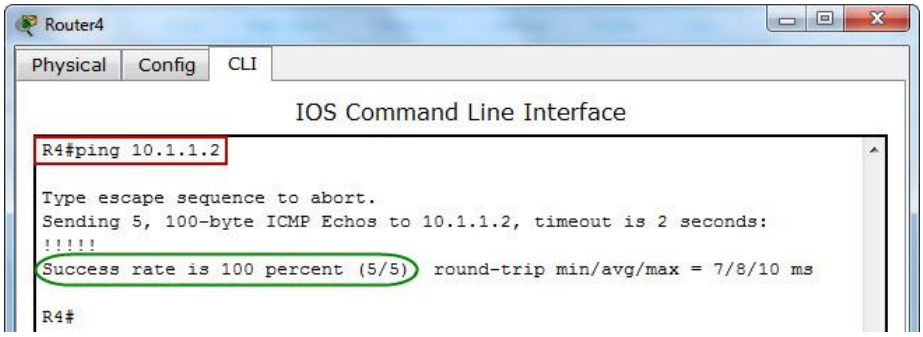
```
R4(config-router)#network 172.16.0.0
```



12. Ta vừa cấu hình RIP cho tất cả các router. Nhấn Ctrl+Z để thoát khỏi Privileged mode và xét xem ta có thể ping tới các router không được kết nối trực tiếp với nhau (giữa R2 và R4) hay không. Từ R2, thử ping tới cổng Ser2/0 của R4 có địa chỉ IP là 172.16.10.2.

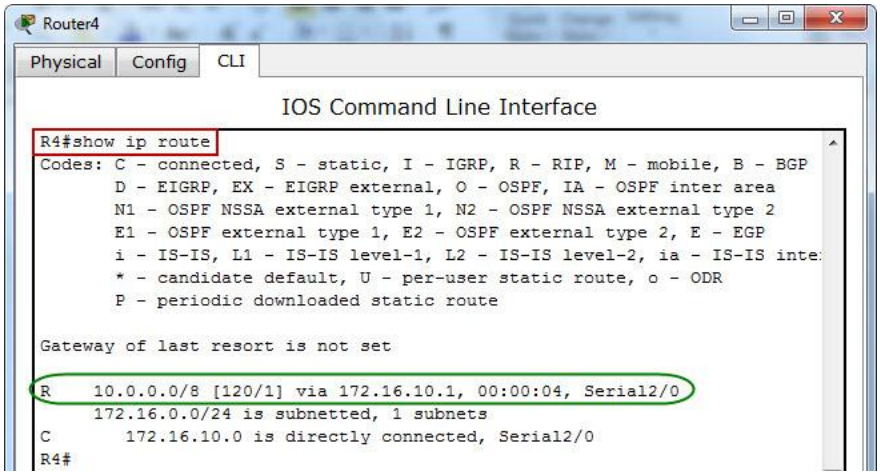


13. Kết nối tới R4 và ping thử tới cổng Fa0/0 của R2 có địa chỉ IP là 10.1.1.2.



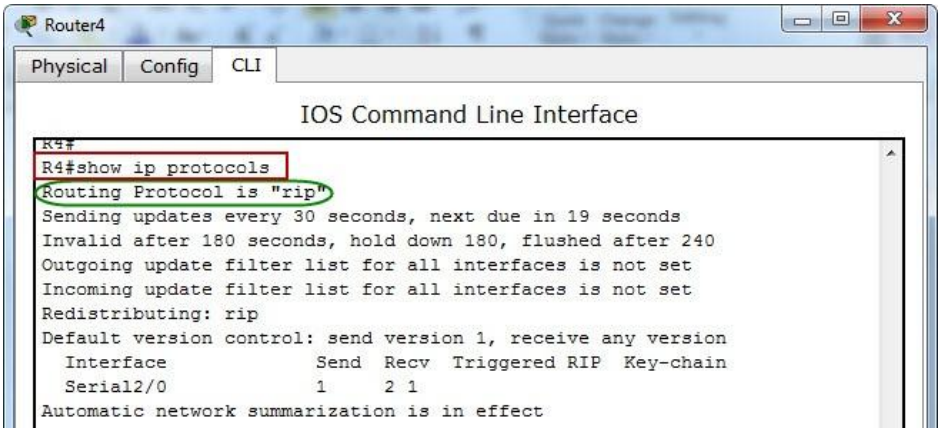
14. Nếu R2 và R4 có thể ping thành công nhau thì ta cũng đã cấu hình định tuyến sử dụng RIP thành công. Giờ ta xem bảng định tuyến của R4

```
R4#show ip route
```



15. Xem thông tin về (các) giao thức định tuyến mà R4 đang sử dụng

```
R4#show ip protocols
```



Lab 14: Troubleshooting RIP

Chẩn đoán và xử lý sự cố với RIP

A. Mục tiêu của bài lab:

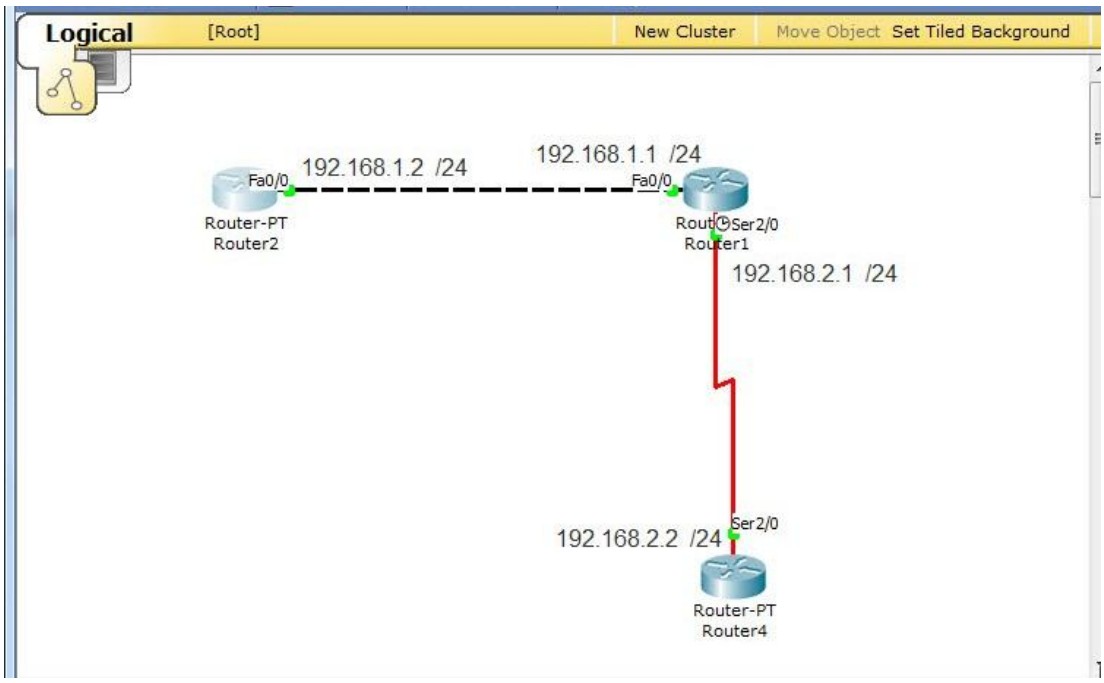
Đặt địa chỉ IP cho các interface trên các Router 1, 2 và 4 và sau đó cấu hình RIP cho các router. Sau đó, ta sẽ quan sát các hoạt động định tuyến sử dụng lệnh debug ip rip. Còn để xem xét các route trong bảng định tuyến ta sử dụng lệnh show ip route.

B. Chuẩn bị cho bài lab:

Chúng ta sẽ sử dụng Router 1, 2 và 4.

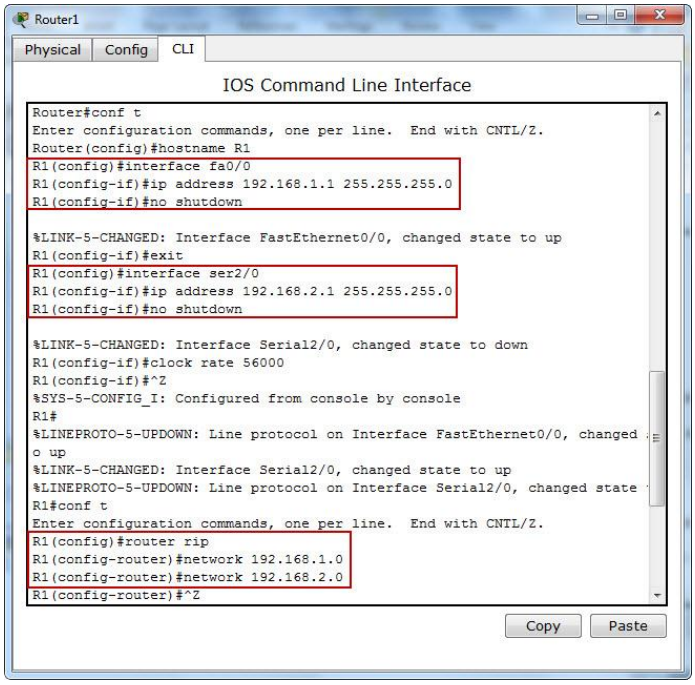
C. Các bước thực hiện:

1. Dưới đây hình mô tả sơ đồ kết nối giữa các router và địa chỉ IP được gán cho các interface.

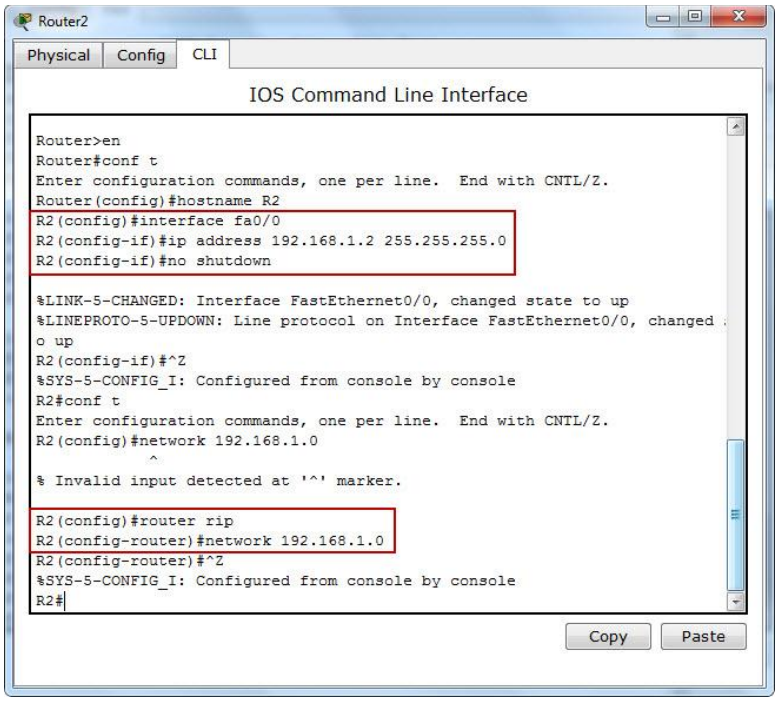


2. Cấu hình giao thức định tuyến RIP trên tất cả các router sử dụng các câu lệnh network thích hợp

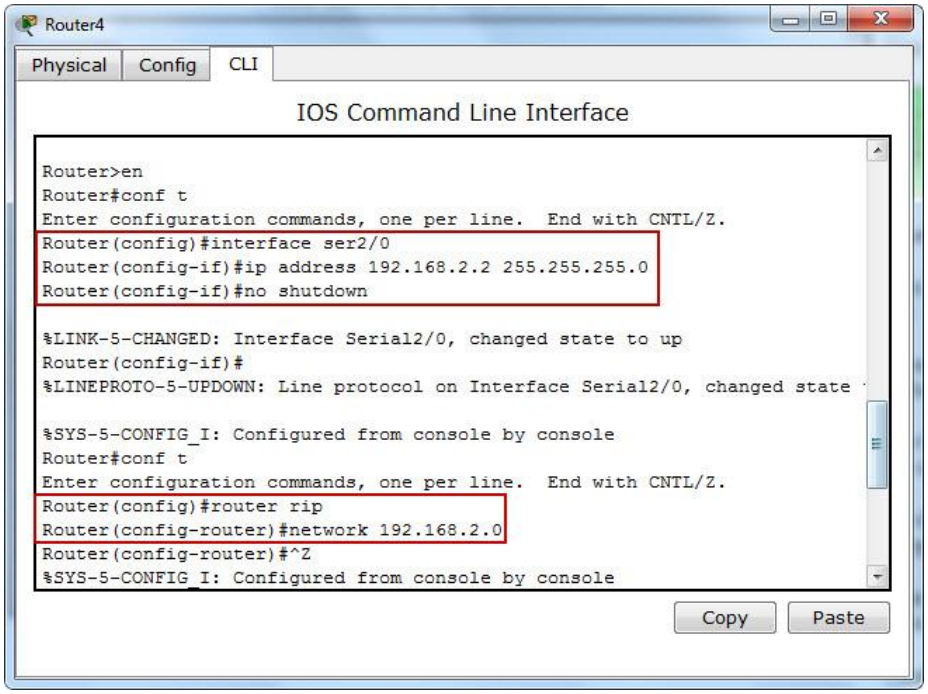
Trên Router1



Trên Router2

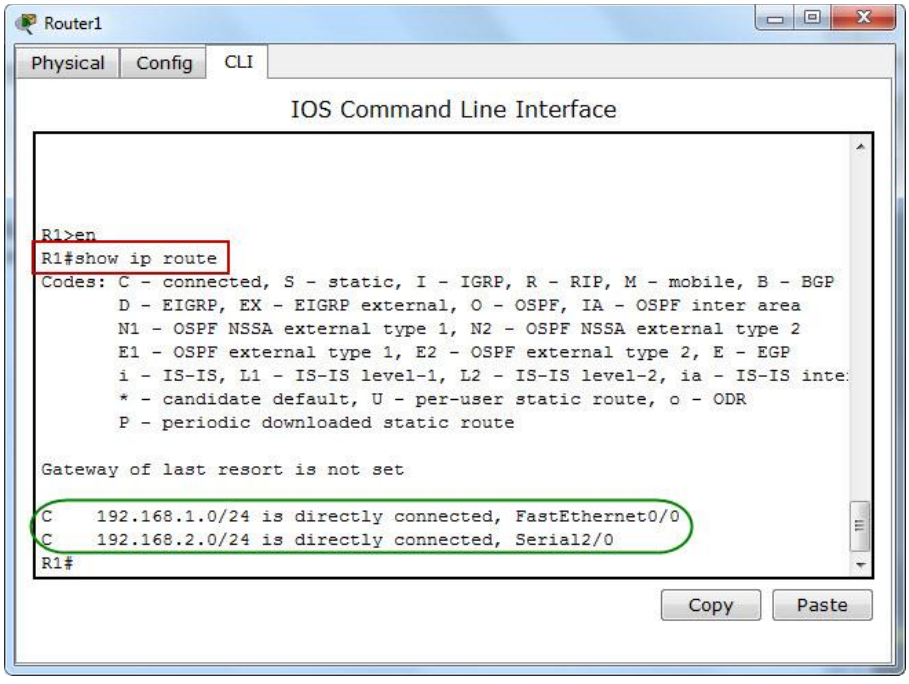


Trên Router4

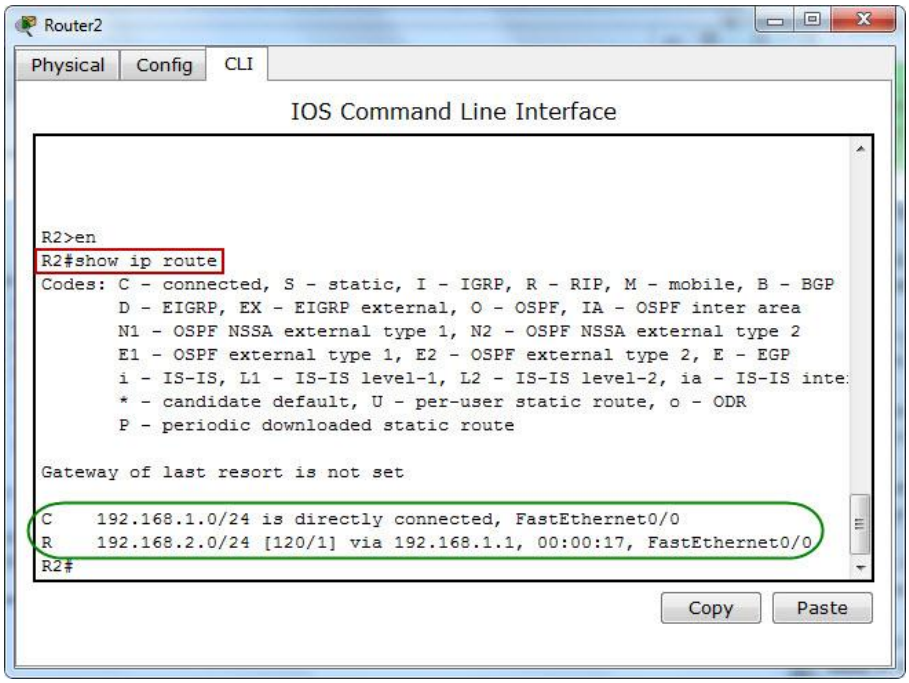


3. Kiểm tra để đảm bảo rằng các route hiện diện đầy đủ trong các bảng định tuyến của tất cả các router với lệnh `show ip route`.

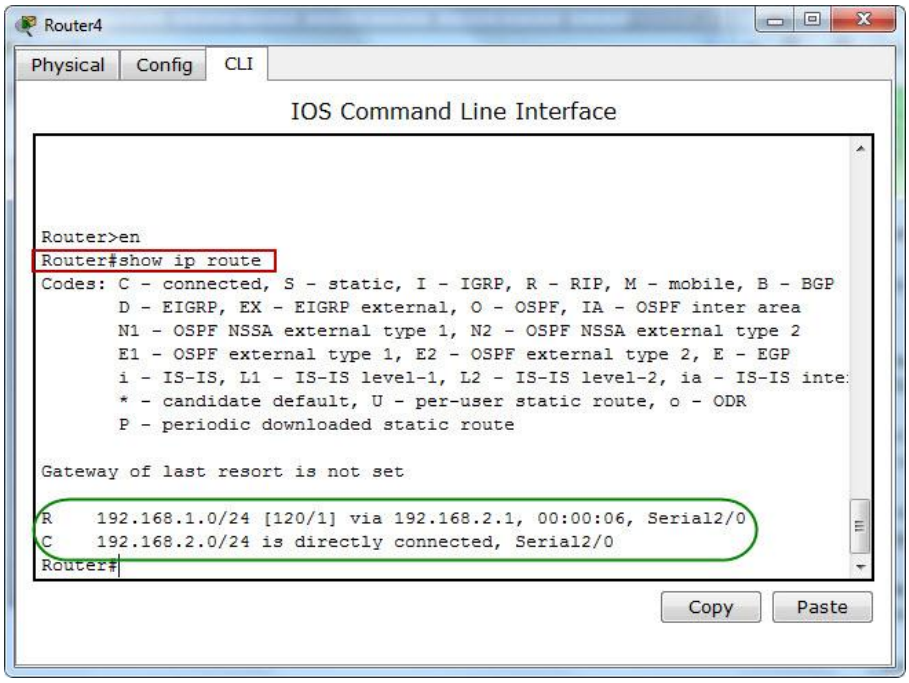
Trên Router1



Trên Router2

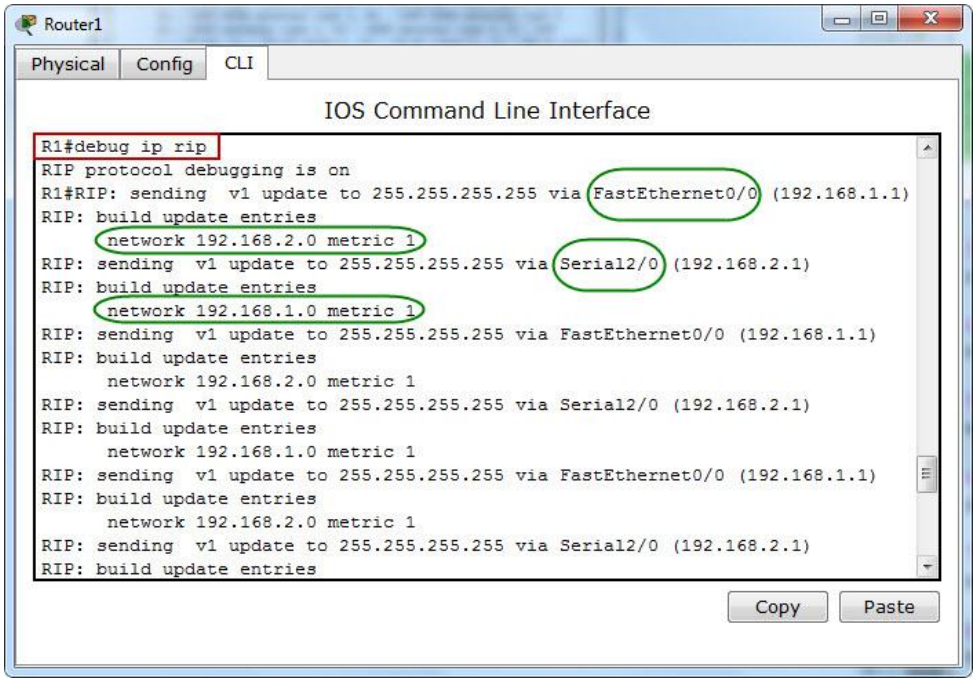


Trên Router4

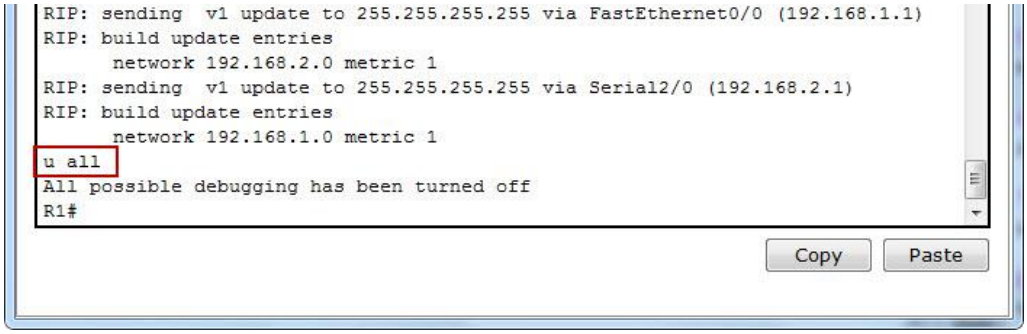


4. Trong Privileged mode của Router1, chạy lệnh `debug ip rip`

5. Quan sát thông tin đầu ra xuất hiện trên màn hình (lưu ý, có thể mất gần 60 giây để các thông tin debug này mới hiện ra)



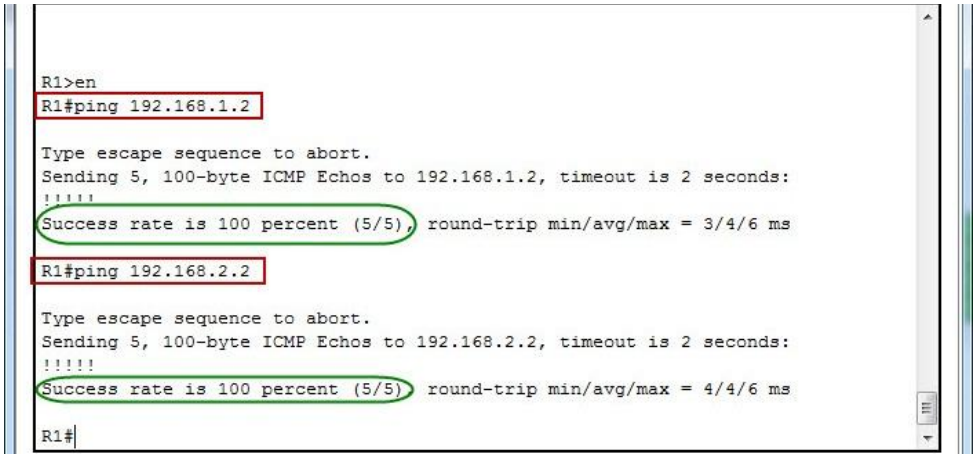
6. Nếu muốn dừng lại quá trình hiển thị thông tin debug của RIP và trả lại cho ta dấu nhắc lệnh, ta cần hủy bỏ lệnh debug. Để làm điều này, gõ vào lệnh "`undebug all`" hoặc "`u all`" và nhấn Enter.



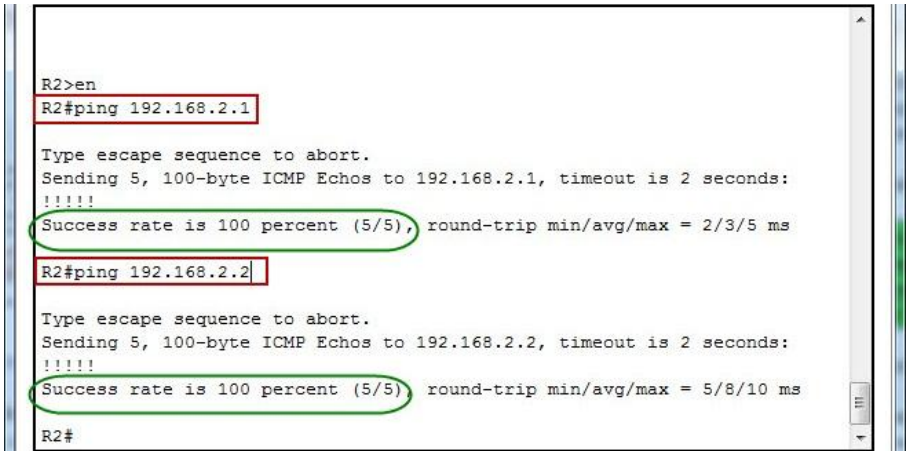
7. Xem bảng định tuyến trên Router2 và 4. Chú ý các giá trị Administrative distance và metrics của các route (xem các hình chụp ở bước 3).

8. Đảm bảo rằng các router có thể ping thành công tới nhau.

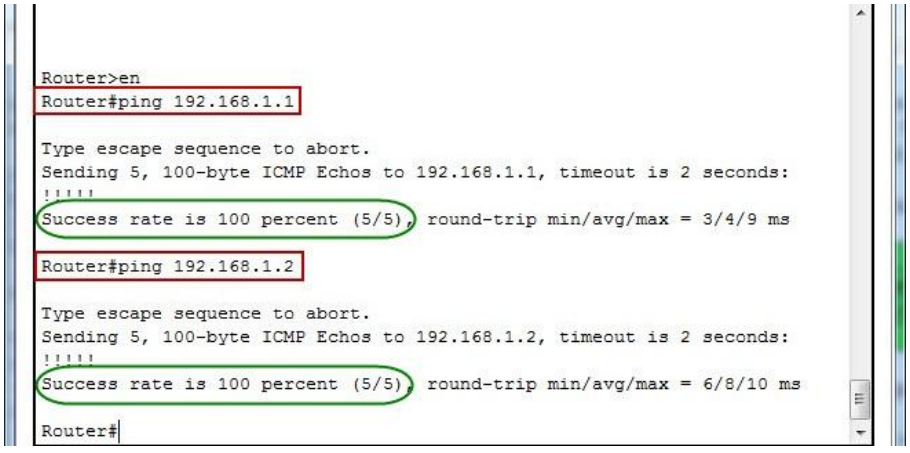
Trên Router1



Trên Router2



Trên Router4



Lab 15: IGRP

Cấu hình IGRP

A. Mục tiêu của bài lab:

Đặt địa chỉ IP cho các interface trên các Router 1, 2 và 4 và sau đó cấu hình giao thức định tuyến IGRP cho các router này. Cụ thể ta sẽ:

1. Đặt hostname cho các router và kích hoạt các interface của chúng.
2. Cấu hình giao thức định tuyến IGRP cho các router.
3. Với từng router, chọn các mạng được kết nối trực tiếp nó.
4. Xem bảng định tuyến của các router.
5. Xem thông tin về giao thức IGRP.

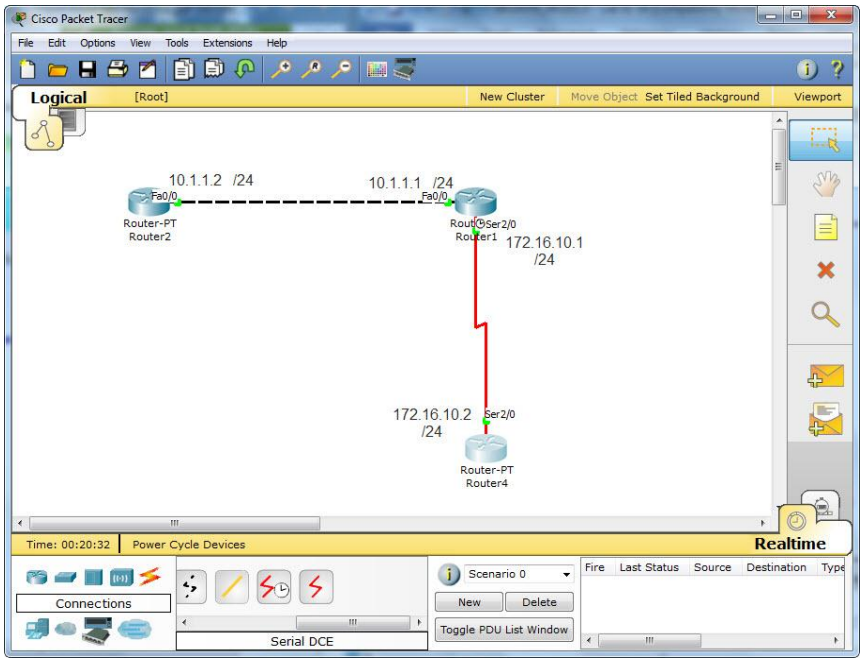
Lưu ý đặc biệt: IGRP là một giao thức đang dần không còn được hỗ trợ trên các thiết bị mạng của Cisco và nó được thay thế bởi EIGRP – một giao thức có nhiều điểm tương đồng và cải tiến hơn IGRP. Phiên bản của IOS mà Packet Tracer 5.1 giả lập không hỗ trợ IGRP nên trong bài lab này ta sẽ cấu hình cho EIGRP làm giao thức định tuyến thay cho IGRP.

B. Chuẩn bị cho bài lab:

Chúng ta sẽ sử dụng Router 1, 2 và 4.

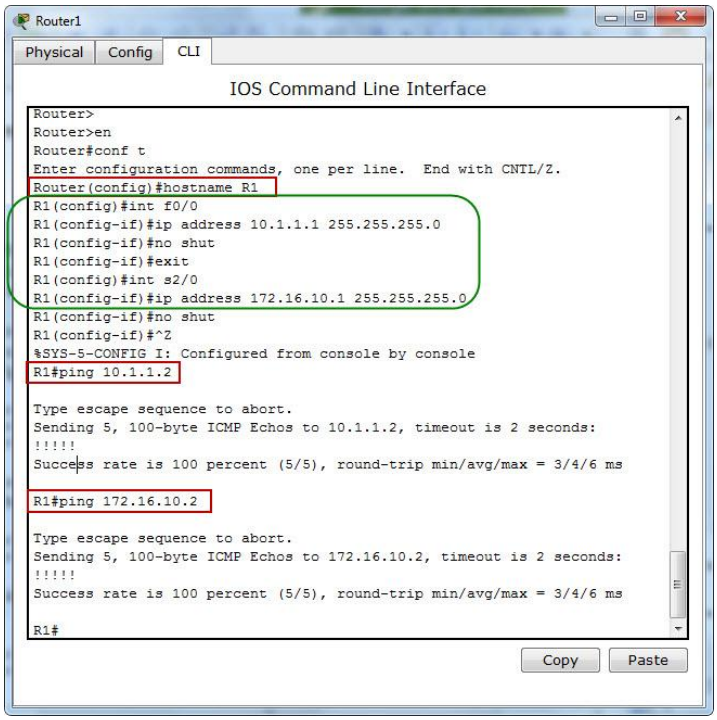
C. Các bước thực hiện:

1. Dưới đây hình mô tả sơ đồ kết nối giữa các router và địa chỉ IP được gán cho các interface.

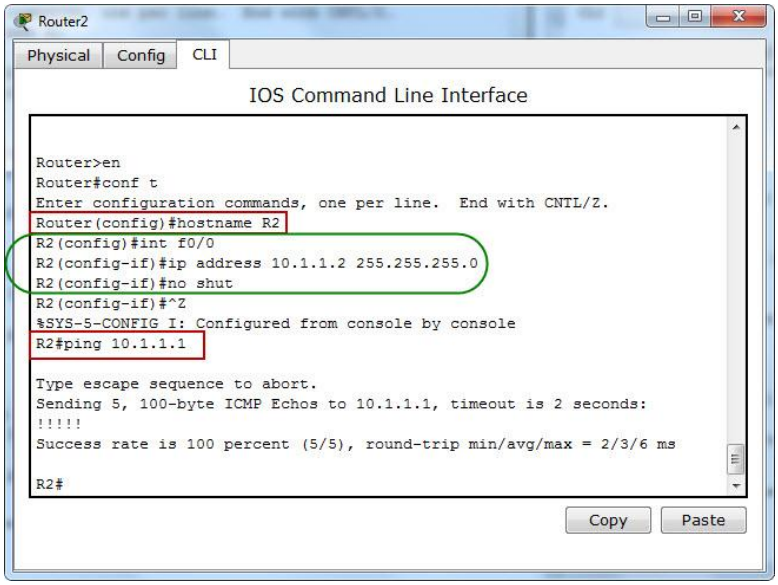


2. Sau khi cấu hình xong địa chỉ IP trên mỗi interface như trong hình trên, ta sẽ sử dụng lệnh ping để kiểm tra rằng các router được nối trực tiếp nhau thì có thể liên lạc được với nhau. Tức là khi bạn đang ở Router1 thì bạn có thể ping tới cổng Fa0/0 của Router 2 và cổng Ser2/0 của Router 4.

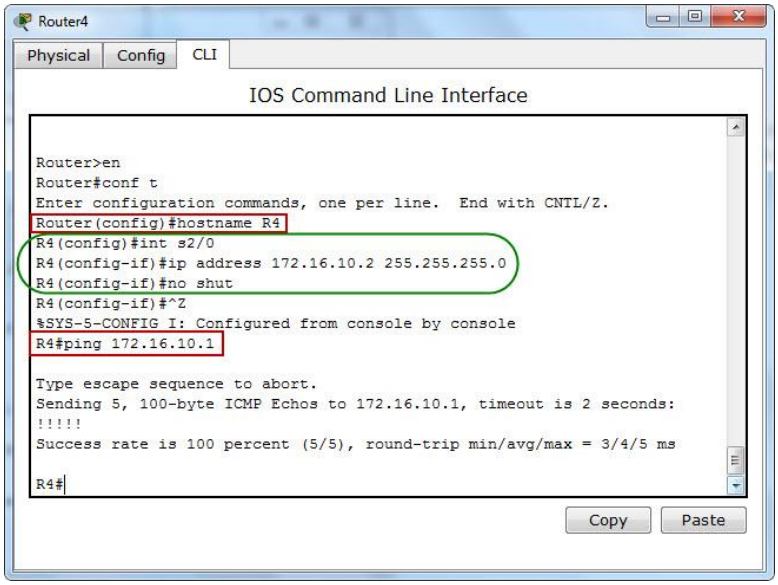
Trên Router1



Trên Router2



Trên Router4



3. Chúng ta vừa cấu hình xong địa chỉ IP cho các interface, tiếp đến ta sẽ đi vào cấu hình EIGRP làm giao thức định tuyến cho các router. Điều này thì rất dễ thực hiện, đầu tiên ta cần vào Configuration mode trên R1

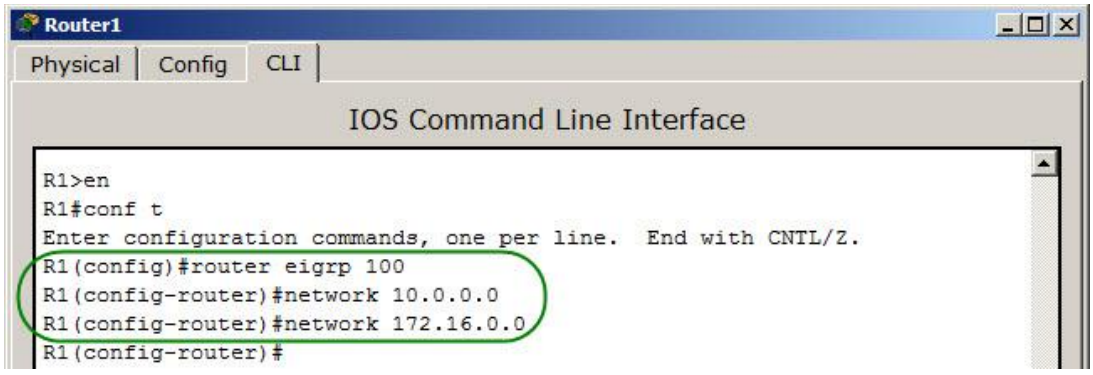
```
R1>en
R1#conf t
```

4. Gõ lệnh sau để cấu hình cho router sử dụng EIGRP với tham số Autonomous system là 100

```
R1(config)#router eigrp 100
```

5. Thêm các mạng mà R1 được kết nối trực tiếp tới

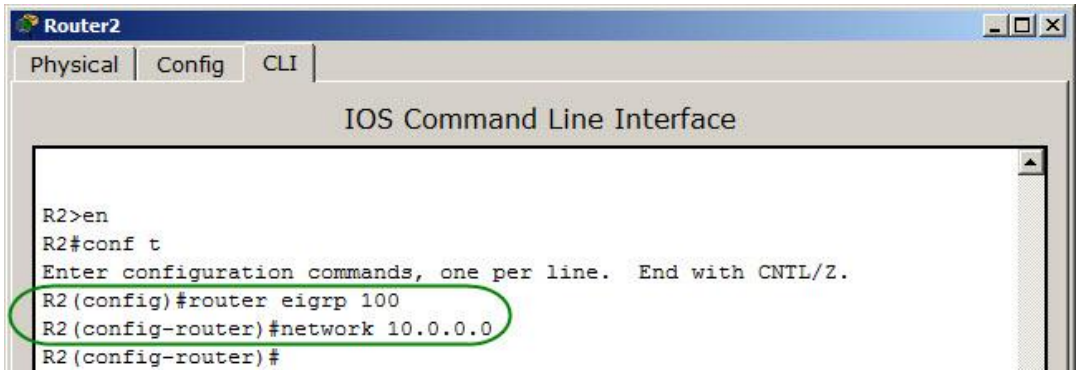
```
R1(config-router)#network 10.0.0.0
R1(config-router)#network 172.16.0.0
```



6. Ta vừa cấu hình xong EIGRP cho R1, giờ ta vào Configuration mode của R2
```
R2>en
R2#conf t
```

7. Chọn EIGRP làm giao thức định tuyến cho R2 và nhớ kèm theo tham số Autonomous system giống với của R1
```
R2(config)#router eigrp 100
```

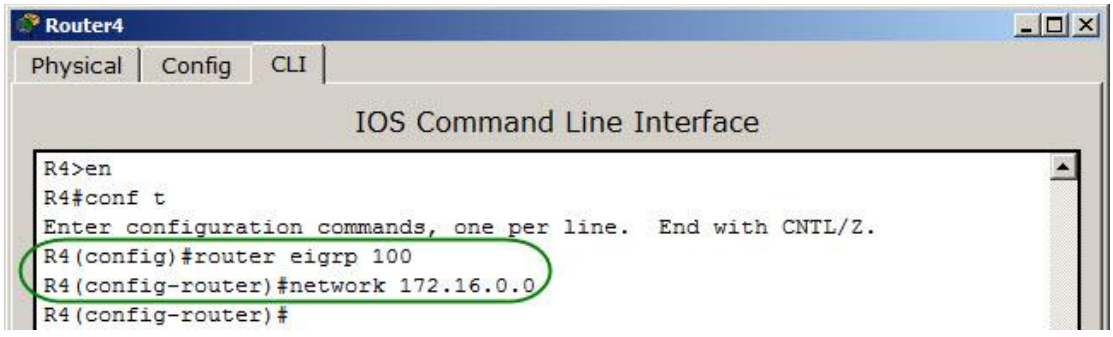
8. Thêm (các) mạng mà R2 đang được kết nối trực tiếp tới
```
R2(config-router)#network 10.0.0.0
```



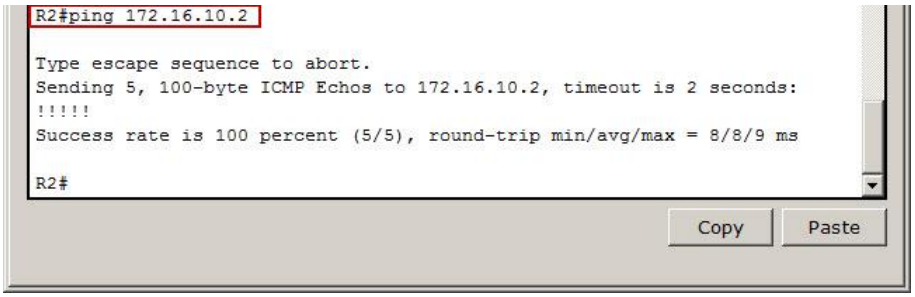
9. Ta vừa cấu hình xong EIGRP cho R2, giờ ta vào Configuration mode của R4
```
R4>en
R4#conf t
```

10. Chọn EIGRP làm giao thức định tuyến cho R4 và nhớ kèm theo tham số Autonomous system giống với của R1
```
R4(config)#router eigrp 100
```

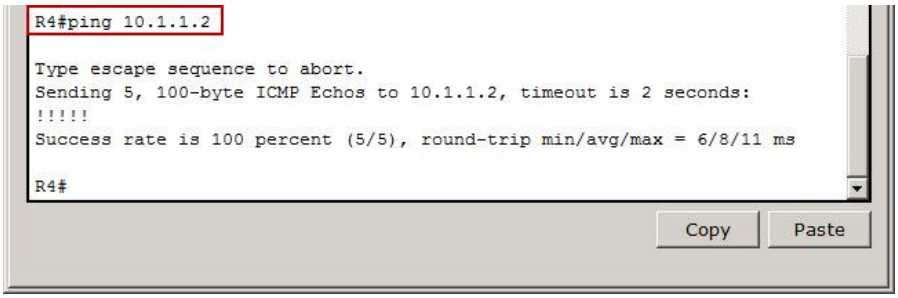
11. Thêm (các) mạng mà R4 đang được kết nối trực tiếp tới
```
R4(config-router)#network 172.16.0.0
```



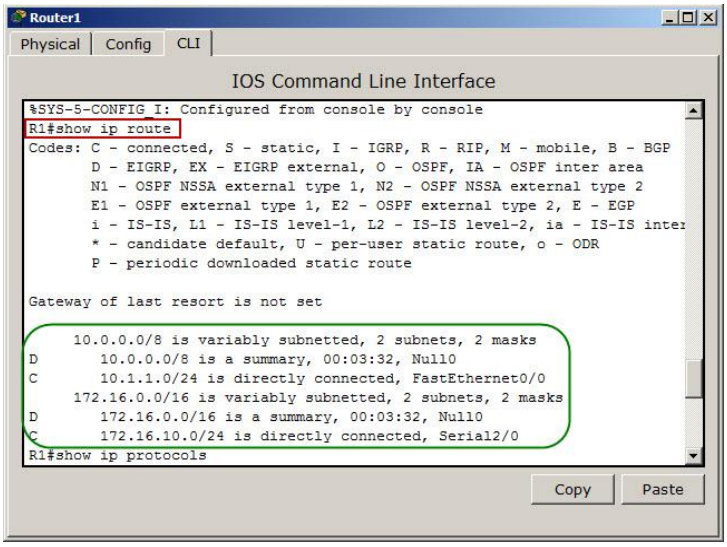
12. Giờ thì ta đã có EIGRP chạy trên cả 3 router. Trở về Privileged mode của R2 và thử sử dụng lệnh ping để kiểm tra xem ta có thể ping tới các router không được kết nối trực tiếp tới R2 hay không. Ở đây ta sẽ thử ping tới cổng Ser2/0 của R4 có địa chỉ là 172.16.10.2



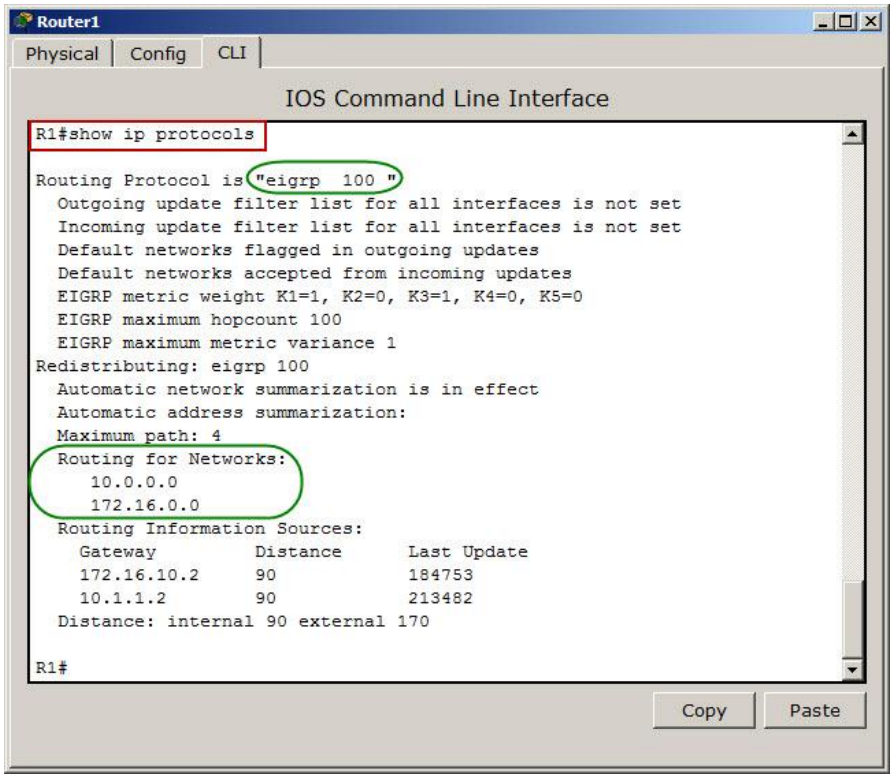
13. Kế tiếp, từ R4 ta sẽ thử ping tới cổng Fa0/0 của R2 có địa chỉ IP là 10.1.1.2



14. Nếu việc ping thành công trên cả R2 và R4 thì coi như ta đã hoàn thành xong việc cấu hình định tuyến cho các router sử dụng EIGRP. Giờ ta sẽ xem qua bảng định tuyến của R1



15. Cuối cùng ta sẽ xem thông tin về giao thức định tuyến mà R1 đang sử dụng để đảm bảo rằng các cấu hình mà ta vừa thực hiện có hiệu lực.



Lab 16: PPP and CHAP

Cấu hình PPP với xác thực CHAP

A. Mục tiêu của bài lab:

Sử dụng PPP làm phương thức đóng gói dữ liệu và các bước cấu hình CHAP làm phương thức xác thực để bảo mật cho kết nối PPP.

B. Chuẩn bị cho bài lab:

Sử dụng Router1 và Router2 được kết nối lại với nhau thông qua cổng Se2/0 trên mỗi router như sau:

C. Các bước thực hiện:

1. Truy cập vào Configuration mode của Router1 và đặt hostname cho nó là R1

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
```

2. Cũng trên R1, chạy lệnh sau để cấu hình các tham số (username và password) dùng để xác thực với R2

```
R1(config)#username R2 password mmt03
```

Trong đó, R2 là hostname của Router2, còn mmt03 là mật khẩu giống nhau cho cả R1 và R2.

3. Tiếp tục, gán địa chỉ IP là 10.1.1.1 với subnet mask là 255.25.255.0 cho cổng S2/0 của R1. Sau đó chọn phương thức đóng gói là PPP với xác thực là CHAP cho cổng này. Cuối cùng, gõ `no shut` để kích hoạt cho nó.

```
R1(config)#int s2/0
R1(config-if)#ip address 10.1.1.1 255.255.255.0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication chap
R1(config-if)#no shut
```

đóng gói với PPP

xác thức bằng CHAP

4. Tương tự như các bước cấu hình cho R1 ở trên, trên Router2 ta cũng thực hiện tuần tự như sau:

- Đặt hostname R2.
- Cấu hình các tham số xác thực: username là R1 (hostname của Router1) và password là mmt03 (giống với mật khẩu ta vừa thiết lập cho R1 ở trên).
- Chọn phương thức xác thực là CHAP và đóng gói là PPP và cho cổng S2/0 của R2
- Kích hoạt cổng S2/0 của R2 lên.

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2
R2(config)#username R1 password mmt03
R2(config)#int s2/0
R2(config-if)#ip address 10.1.1.2 255.255.255.0
R2(config-if)#encapsulation ppp
R2(config-if)#ppp authentication chap
R2(config-if)#no shut
```

5. Cuối cùng, để kiểm tra và xác nhận rằng các cấu hình ở trên làm việc đúng, ta cần đảm bảo là từ R2 có thể ping tới cổng S2/0 của R1

```
R2#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/6 ms
```

Lab 18: Saving Router Configurations

Sao lưu cấu hình của Router

A. Mục tiêu của bài lab:

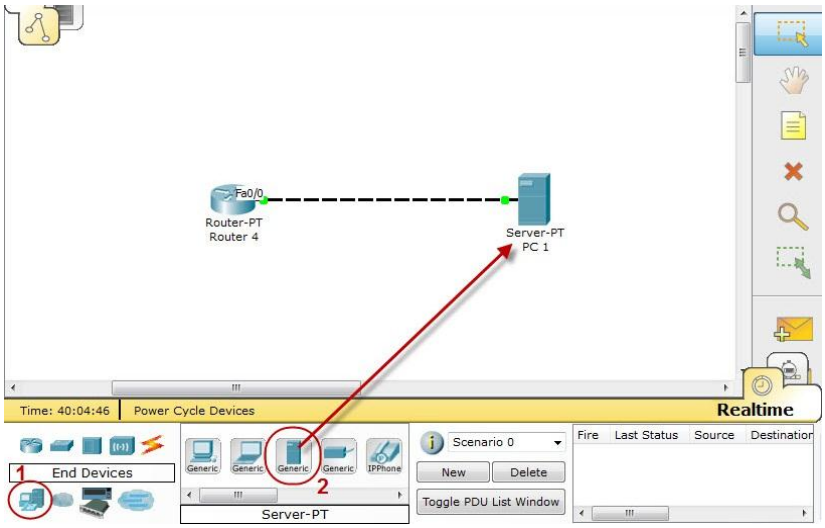
Bài lab này sẽ hướng dẫn bạn cách sao lưu cấu hình của router trong trường hợp bạn vô tình xóa mất cấu hình này hoặc router của bạn bị "chết".

B. Chuẩn bị cho bài lab:

Chúng ta sẽ sử dụng Router 4 và PC1 làm TFTP Server.

Lưu ý: Đối với PC1 thì bạn cần sử dụng thiết bị là *Server-PT* trong mục **End Devices** thì mới có dịch vụ TFTP được hỗ trợ trên PC1.

Mô hình bài lab như hình dưới đây. Cổng Fa0/0 trên Router 4 được kết nối tới card mạng của PC1 sử dụng cáp thẳng (*Copper Straight-Through*)



C. Các bước thực hiện:

1. Kết nối tới Router 4 và vào Configuration mode

```
Router>en
Router#conf t
```

2. Gán hostname là Tampa cho Router 4

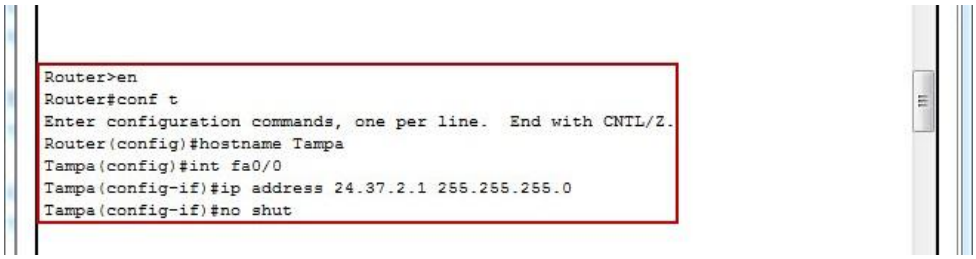
```
Router(config)#hostname Tampa
```

3. Đi vào cổng Fa0/0 của Router 4

```
Tampa(config)#int fa0/0
```

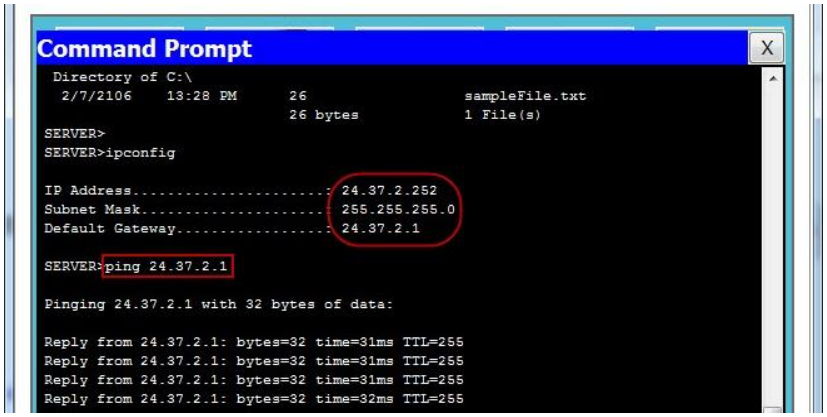
4. Gán địa chỉ IP là 24.37.2.1 với subnet mask là 255.255.255.0 cho cổng Fa0/0 này
```
Tampa(config-if)#ip address 24.37.2.1 255.255.255.0
```

5. Kích hoạt interface Fa0/0 lên
```
Tampa(config-if)#no shut
```



6. Kết nối tới PC 1 và đặt địa chỉ IP là 24.37.2.252 với subnet mask là 255.255.255.0, default gateway là 24.37.2.1 (địa chỉ IP của cổng Fa0/0 trên Router 4)

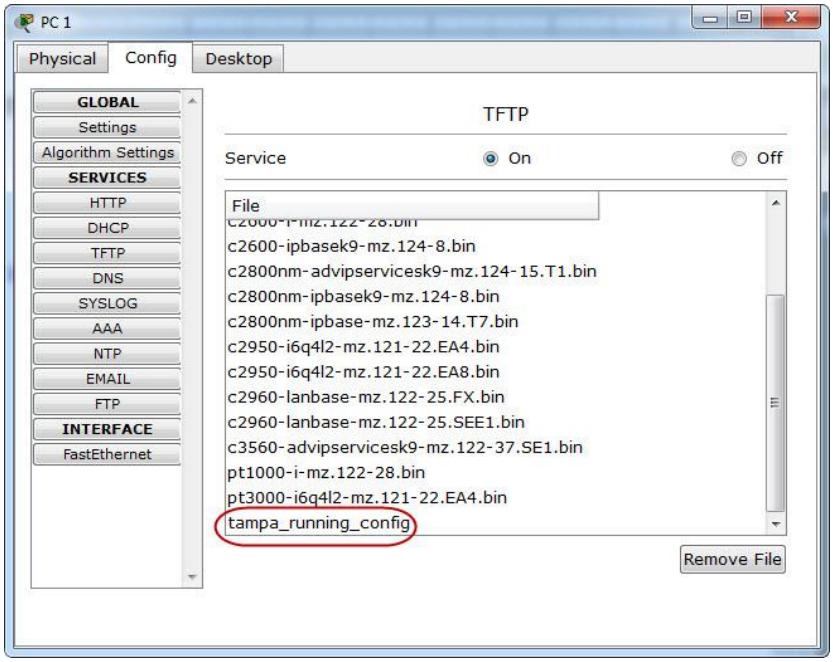
7. Thử ping từ PC tới Router để chắc rằng kết nối giữa 2 thiết bị này hoạt động tốt
```
PC>ping 24.37.2.1
```



8. Kết nối trở lại Router 4 và thoát khỏi interface mode. Sử dụng lệnh copy để chép nội dung trong running-config lên TFTP server là PC1
```
Tampa#copy running-config tftp
```

9. Nhập vào địa chỉ IP của TFTP server và tên của file cấu hình mà ta sẽ lưu trữ nó trên TFTP server

10. Vào PC1 và xác nhận rằng sự tồn tại của file running-config mà ta vừa chép từ Router 4 lên



Lab 19: Loading Router Configurations

Tải về cấu hình của Router

A. Mục tiêu của bài lab:

Bài lab này sẽ hướng dẫn bạn cách tải về và nạp cấu hình của router từ TFTP server.

B. Chuẩn bị cho bài lab:

Chúng ta vẫn sẽ sử dụng tiếp mô hình gồm Router 4 và PC1 như trong bài lab 18. Lưu ý là bạn đã hoàn thành xong các bước trong lab 18.

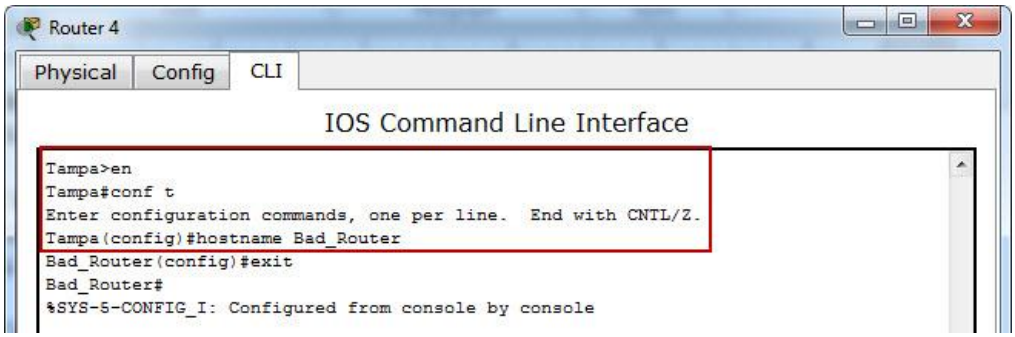
C. Các bước thực hiện:

1. Hiện tại thì file cấu hình của Router 4 đang được lưu trữ trên TFTP server có hostname là *Tampa*. Đăng nhập vào Tampa và vào Configuration mode.

```
Tampa>en
Tampa#conf t
```

2. Đặt lại hostname là *Bad_Router*.

```
Tampa(config)#hostname Bad_Router
```



3. Giờ ta sẽ copy cấu hình được lưu trữ trên TFTP server và ghi đè lên cấu hình hiện tại mà Router 4 đang sử dụng.

```
Bad_Router#copy tftp running-config
```

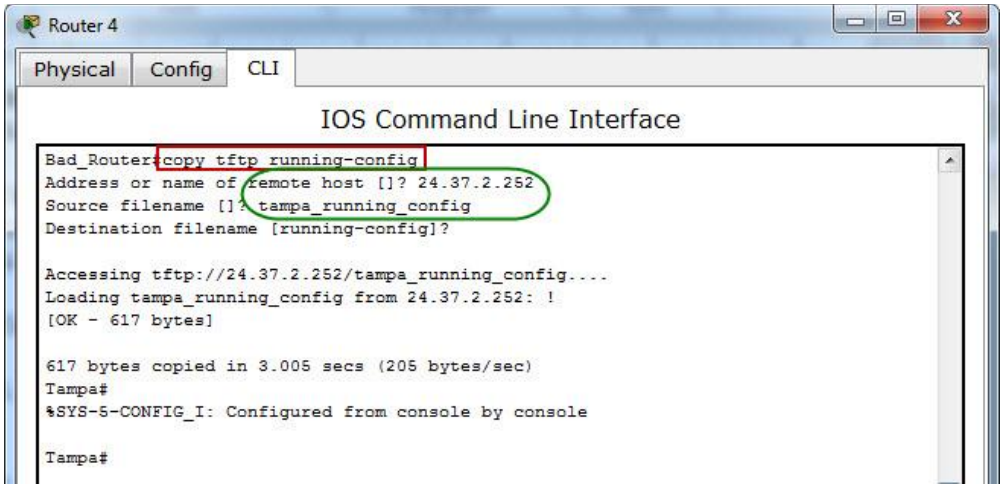
4. Khi được router nhắc nhở về địa chỉ IP của TFTP server, ta nhập vào IP của PC1 như sau

```
Address or name of remote host []? 24.37.2.252
```

5. Kế đến ta cần cung cấp tên của file cấu hình cần nhận về từ TFTP server.

```
Source filename []? tampa_running_config
```

6. Chờ một lát để router tải về cấu hình và nạp nó vào *running-config*


Router 4
Physical
Config
CLI
IOS Command Line Interface
Bad_Router#copy tftp running-config
Address or name of remote host []? 24.37.2.252
Source filename []? tampa_running_config
Destination filename [running-config]?
Accessing tftp://24.37.2.252/tampa_running_config....
Loading tampa_running_config from 24.37.2.252: !
[OK - 617 bytes]
617 bytes copied in 3.005 secs (205 bytes/sec)
Tampa#
%SYS-5-CONFIG_I: Configured from console by console
Tampa#

Lab 20: Frame Relay

Cấu hình Frame Relay

A. Mục tiêu của bài lab:

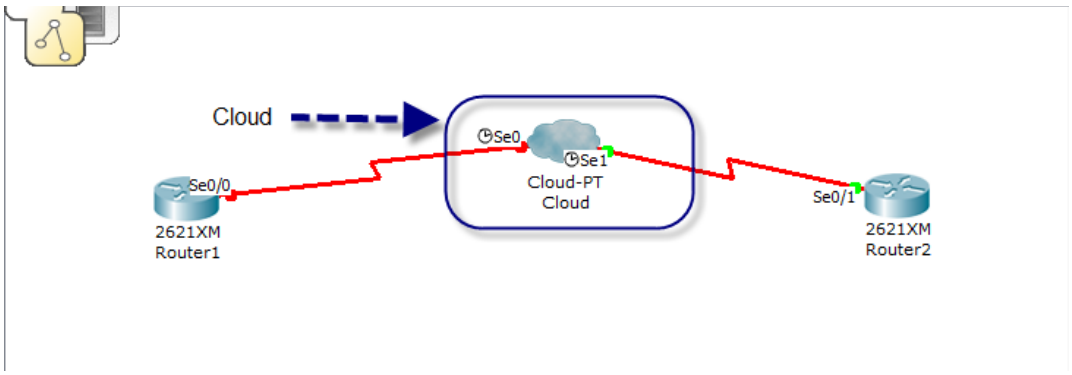
Hiểu được cách thiết lập Frame Relay trong kết nối WAN.

B. Chuẩn bị cho bài lab:

Chúng ta sẽ sử dụng Router1 và Router2.

C. Các bước thực hiện:

1. Trong bài lab này, ta sẽ cấu hình frame relay giữa router 1 và router 2 theo 2 cách: dùng cổng giao tiếp vật lí (physical interface) hoặc là cổng giao tiếp logic (sub interfaces). Lưu ý là cả 2 router đều kết nối tới Cloud bằng đầu DTE



2. **Cách 1:** cấu hình frame relay dùng physical interfaces trên các cổng serial của router. Các bước gồm đặt địa chỉ IP, chỉnh DLCI, và chỉnh Imi-type là ANSI.

Trên Router1:

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hos router2
router2(config)#int s0/1
router2(config-if)#ip add 215.10.1.2 255.255.255.0
router2(config-if)#no shut
router2(config-if)#enca
router2(config-if)#encapsulation fram
router2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state to up
frame map ip 215.10.1.1 501 broadcast
router2(config-if)#frame lmi ansi
router2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state to down
```

Trên Router2:

```
router1>en
router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
router1(config)#int s0/0
router1(config-if)#ip add 215.10.1.1 255.255.255.0
router1(config-if)#no shut

router1(config-if)#
%LINK-5-CHANGED: Interface Serial0/0, changed state to up
en fr
router1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state
fr map ip 215.10.1.2 105 b
router1(config-if)#fr l ansi
router1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state
```

Kiểm tra lại bằng các lệnh show sau

```
# show frame-relay map
# show frame-relay pvc
# show frame-relay
```

Các lệnh trên lần lượt thể hiện các thông tin về Mapping, PVC, LMI

```
router1#sh frame-relay map
Serial0/0 (up): ip 215.10.1.2 dlci 105, static, broadcast, CISCO, status defined
, active
router1#sh fra pvc

PVC Statistics for interface Serial0/0 (Frame Relay DTE)
DLCI = 105, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0

input pkts 14055       output pkts 32795        in bytes 1096228
out bytes 6216155      dropped pkts 0           in FECN pkts 0
in BECN pkts 0         out FECN pkts 0          out BECN pkts 0
in DE pkts 0           out DE pkts 0
out bcast pkts 32795   out bcast bytes 6216155

router1#sh fra lmi
LMI Statistics for interface Serial0/0 (Frame Relay DTE) LMI TYPE = ANSI
 Invalid Unnumbered info 0      Invalid Prot Disc 0
 Invalid dummy Call Ref 0       Invalid Msg Type 0
 Invalid Status Message 0       Invalid Lock Shift 0
 Invalid Information ID 0       Invalid Report IE Len 0
 Invalid Report Request 0       Invalid Keep IE Len 0
 Num Status Enq. Sent 302       Num Status msgs Rcvd 302
 Num Update Status Rcvd 0       Num Status Timeouts 16

router1#
```

3. **Cách 2:** cấu hình frame relay dùng sub interfaces trên các cổng serial của router. Lưu ý do vẫn dùng vài thông số cấu hình cũ nên ta không cần gõ quá nhiều câu lệnh. Ta chỉ cần gõ địa chỉ IP và frame map từ interface để gắn cho sub interface.

Trên Router1

```
router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
router1(config)#int s0/0
router1(config-if)#no ip add
router1(config-if)#no fra map ip 215.10.1.2 105 b
%Can't find address map for ip 215.10.1.2
router1(config-if)#exit
router1(config)#int s0/0.1 p
router1(config-subif)#ip add 215.10.1.1 255.255.255.0
router1(config-subif)#fra int?
interface-dlci
router1(config-subif)#fra int 105
router1(config-subif)#
```

Trên Router2

```
router2>en
router2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
router2(config)#int s0/1
router2(config-if)#no ip add
router2(config-if)#no fra map ip 215.10.1.1 501 b
router2(config-if)#exit
router2(config)#int s0/1.1 p

%LINK-5-CHANGED: Interface Serial0/1.1, changed state to up
router2(config-subif)#ip add 215.10.1.2 255.255.255.0
router2(config-subif)#fra int 501
router2(config-subif)#end

%SYS-5-CONFIG_I: Configured from console by console
router2#ping 215.10.1.1
```

Kiểm tra lại bằng các lệnh show, lệnh ping, kết quả tương tự như cách 1.

Lab 24: Introduction to Basic Switch Commands

Các câu lệnh cấu hình Switch cơ bản

A. Mục tiêu của bài lab:

Cấu hình cơ bản cho switch.

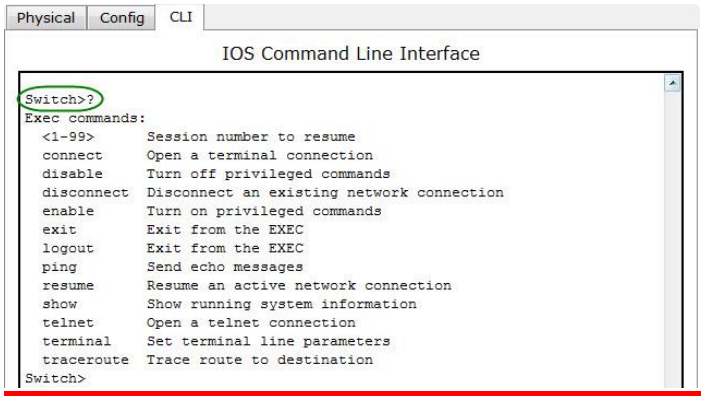
B. Chuẩn bị cho bài lab:

Sử dụng thiết bị switch có tên Switch1.

C. Các bước thực hiện:

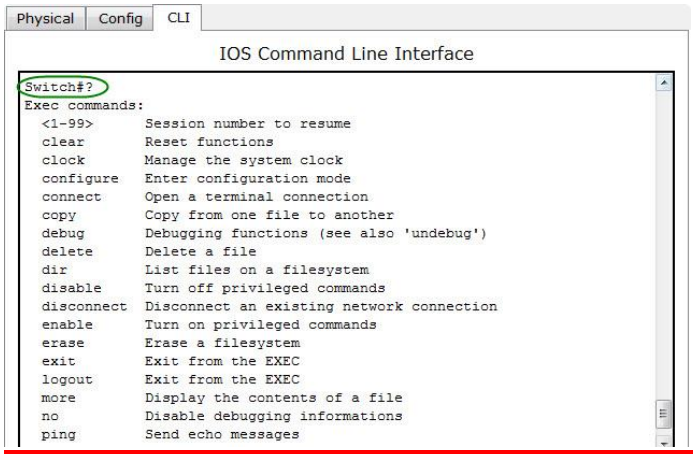
1. Khi truy cập vào Switch1, ta sẽ bắt đầu tại dấu nhắc lệnh cơ bản (đại diện bởi ký tự >), tức user mode

2. Để xem danh sách tất cả các câu lệnh hiện có thể sử dụng tại chế độ cơ bản này, ta gõ dấu hỏi chấm (?)



3. Giờ muốn vào Privilege mode (đại diện bởi ký tự #) - chế độ cho phép ta toàn quyền kiểm soát thiết bị thì sử dụng lệnh `enable`

4. Tiếp tục, để xem các câu lệnh sẵn dùng trong Privilege mode, ta lại gõ ?



5. Nếu muốn cấu hình cho switch. Gõ tiếp lệnh `config terminal` để vào Configuration mode

6. Host name được sử dụng để nhận dạng thiết bị. Khi đăng nhập vào switch, bạn sẽ thấy Host name nằm đằng trước dấu nhắc lệnh (> hoặc #). Bạn có thể thay đổi Host name để chỉ ra vị trí hoặc chức năng của switch. Lệnh `hostname` sau đây sẽ đặt tên cho Switch1 là mmt03

```
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname mmt03
mmt03(config)#
```

7. Sử dụng lệnh `enable password` để thiết lập mật khẩu truy cập cho Privilege mode. Điều này thực sự rất quan trọng vì trong Privilege mode, bạn có thể tạo ra nhiều thay đổi cấu hình của switch nên bạn cần giới hạn chỉ để những người biết được mật khẩu mới có thể đăng nhập vào switch để cấu hình cho thiết bị.

   Có một chút khác biệt về cú pháp lệnh khi đặt mật khẩu cho switch và router. Trên các thiết bị mạng Cisco, có nhiều mức quyền hạn - **privilege level**, và thường có 16 level được đánh số từ 0 đến 15. Mỗi level có một tập các lệnh và bạn có thể điều chỉnh lại tập các lệnh trong từng level, mặc định thì User mode là level 1 và level 15 là Privileged mode. Sau đó bạn có thể thiết lập cho một (nhóm) người dùng nào đó chỉ được phép sử dụng các câu lệnh thuộc level nào đó.

   Để đặt mật khẩu là *uit* cho Privileged mode có level là 15 (tức giữ nguyên cấu hình mặc định) ta thực hiện như sau

```
mmt03#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
mmt03(config)#enable password level 15 uit
% Converting to a secret.  Please use "enable secret" in the future
mmt03(config)#exit
mmt03#
%SYS-5-CONFIG_I: Configured from console by console

mmt03#exit
```

8. Giờ kiểm tra mật khẩu này, ta trở về User mode (lệnh `exit`) và thử vào lại Privileged mode (lệnh `enable`), sau đó nhập vào mật khẩu là *uit* tại dấu nhắc Password:

```
mmt03>en
Password:Nhập mật khẩu là uit
mmt03#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
mmt03(config)#
```

Gõ tiếp `conf term` để tiếp tục các bước sau của bài lab

9. Vấn đề duy nhất đối với `enable password` là nó xuất hiện trong file cấu hình của switch dưới dạng không mã hóa (plain-text). Nếu bạn cần cho ai đó xem file này để họ có thể giúp bạn khắc phục vấn đề nào đó thì có thể bạn đã vô tình để tự phá vỡ cơ chế bảo vệ của hệ thống bằng việc để lộ mật khẩu truy nhập vào Privileged mode của switch.

Lệnh `enable secret` dưới đây sẽ thiết lập mật khẩu được lưu trữ ở dạng mã hóa trong file cấu hình của thiết bị. Đừng quên tham số lệnh `level` có giá trị là 15 và ở đây chuỗi mật khẩu ở dạng plain-text mà người dùng cần nhập khi muốn vào Privileged mode là *cisco*.

```
mmt03#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
mmt03(config)#enable secret level 15 cisco
mmt03(config)#exit
mmt03#
%SYS-5-CONFIG_I: Configured from console by console
e
% Ambiguous command: "e"
mmt03#exit
```

10. Bây giờ ta thử kiểm tra mật khẩu enable secret này bằng cách trở về User mode và sau đó gõ enable. Lưu ý là khi tồn tại cả 2 loại mật khẩu là enable password và enable secret thì enable secret sẽ được ưu tiên sử để truy nhập vào Privileged mode. Do vậy, ở đây ta cần nhập vào chuỗi mật khẩu là *cisco*.

```
mmt03>en
Password:Nhập mật khẩu là cisco
```

Như vậy ta đã tìm hiểu xong các lệnh cấu hình căn bản cho Switch.

Lab 28: Standard Access Lists

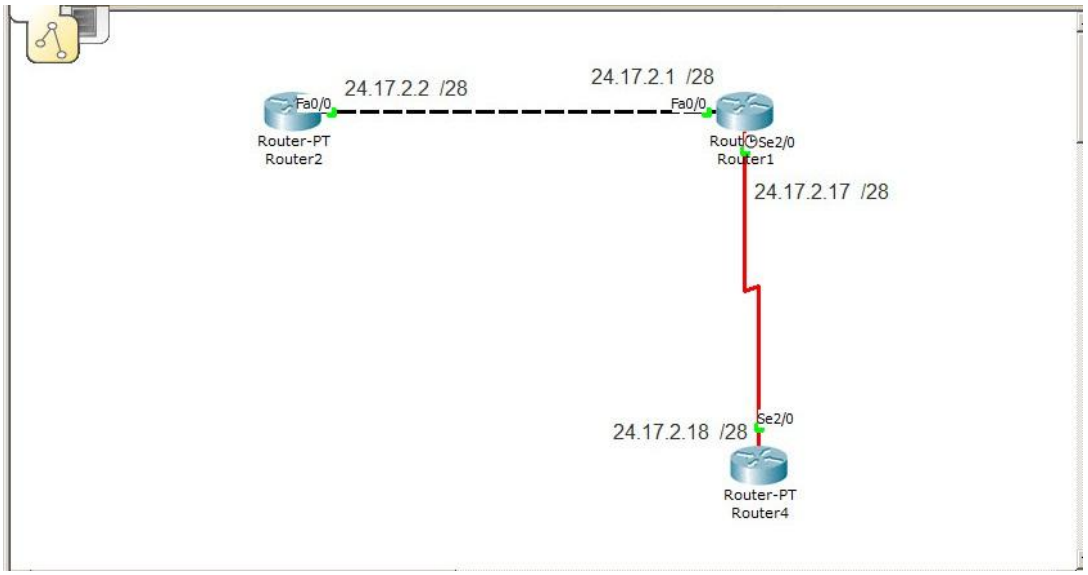
Danh sách kiểm soát truy cập chuẩn

A. Mục tiêu của bài lab:

Tìm hiểu và thực hành cấu hình các danh sách kiểm soát truy cập chuẩn (Standard ACL).

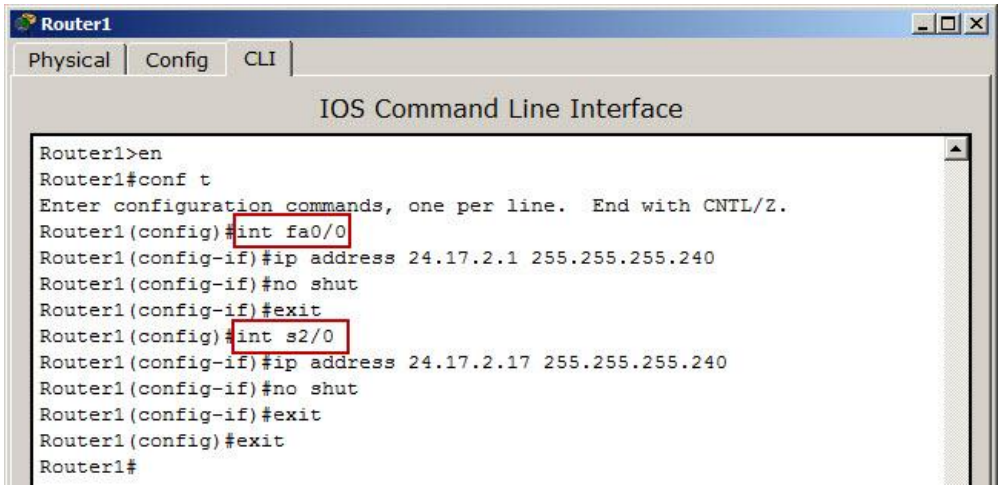
B. Chuẩn bị cho bài lab:

Chúng ta sẽ sử dụng Router 1, 2 và 4 với các cổng được kết nối và đặt địa chỉ IP theo mô hình như sau:

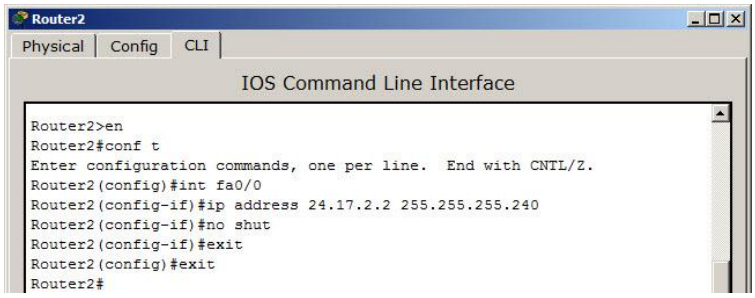


C. Các bước thực hiện:

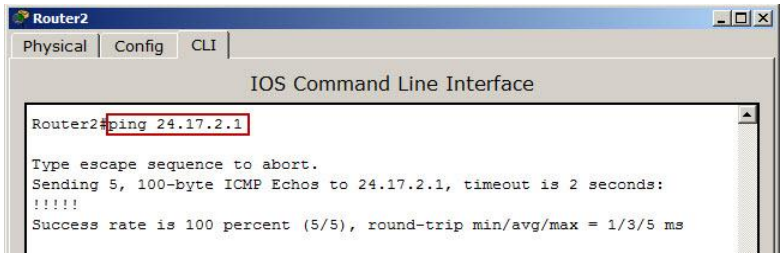
1. Trên Router1, đặt địa chỉ IP cho các cổng Fa0/0 và Ser2/0 như sau:



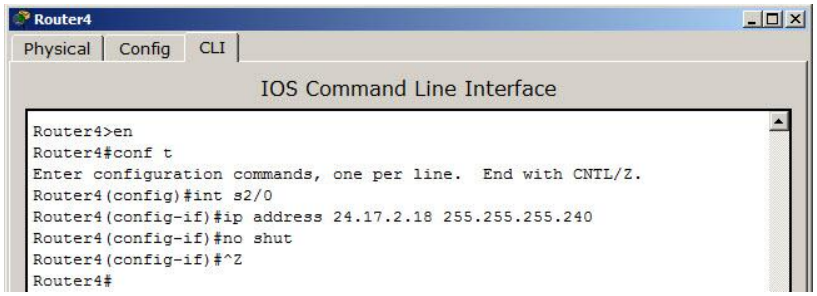
2. Trên Router2, đặt địa chỉ IP cho cổng Fa0/0 như sau:



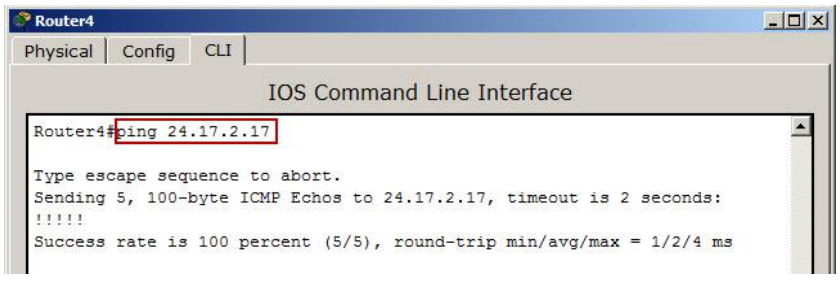
3. Từ Router2, ping tới địa chỉ IP của cổng Fa0/0 của Router1



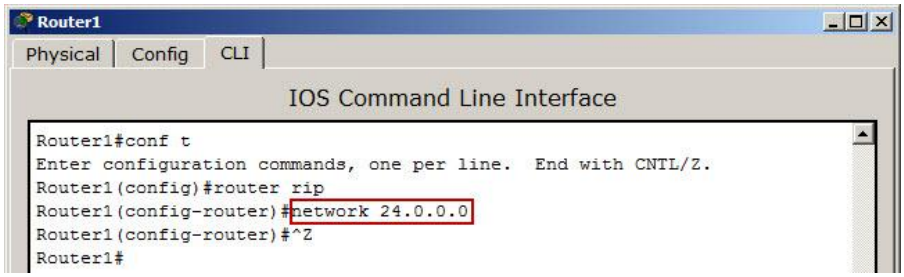
4. Trên Router4, đặt địa chỉ IP cho cổng Ser2/0 như sau:



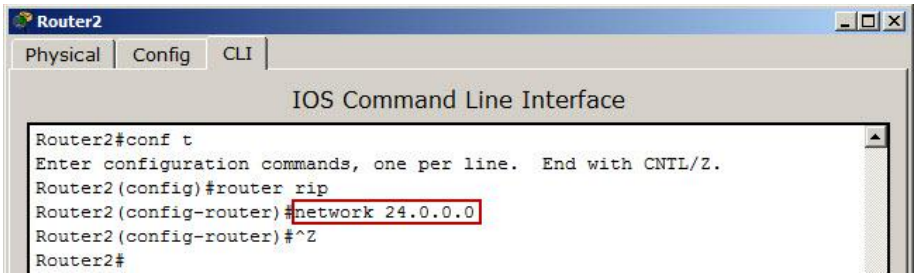
Sau đó ping thử tới địa chỉa IP của cổng Ser2/0 của Router1



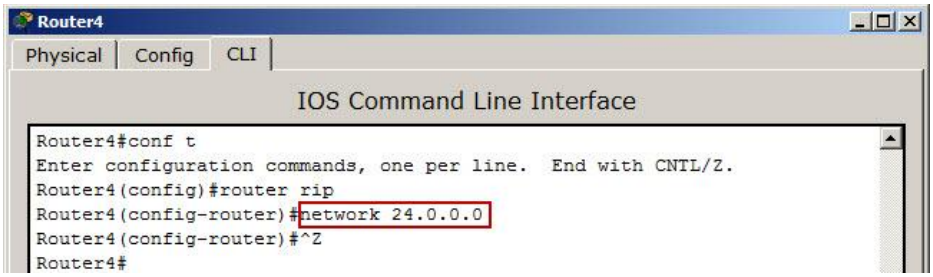
5. Cấu hình RIP cho Router1 và thêm network dành cho các cổng Fa0/0 và Ser2/0



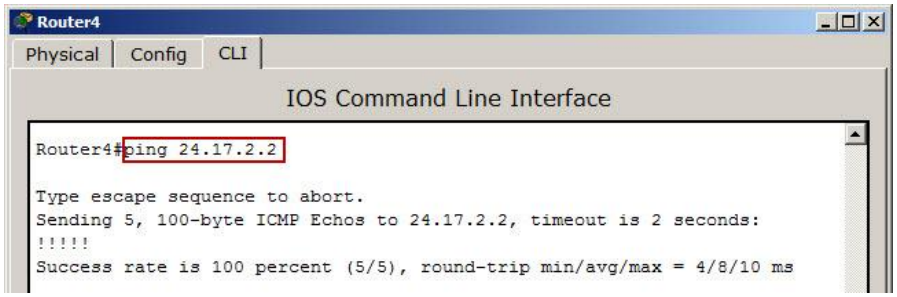
6. Cấu hình RIP cho Router2 và thêm network dành cho cổng Fa0/0



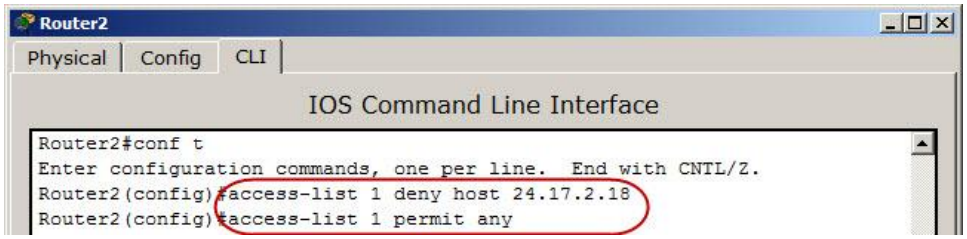
7. Cấu hình RIP cho Router4 và thêm network dành cho cổng Ser2/0



8. Từ Router4, ping thử tới địa chỉ IP của cổng Fa0/0 của Router2



9. Giờ ta sẽ cấu hình ACL trên Router2 để chặn khả năng Router4 ping tới Router2. Vào chế độ Configuration. Sau đó, tạo một access-list 1 chỉ để chặn địa chỉ IP 24.17.2.18 (cổng Ser2/0 của Router4) theo sau đó là lệnh `access-list permit any` để cho phép tất cả các địa chỉ IP khác được gửi gói tin tới cổng Fa0/0 của Router2.



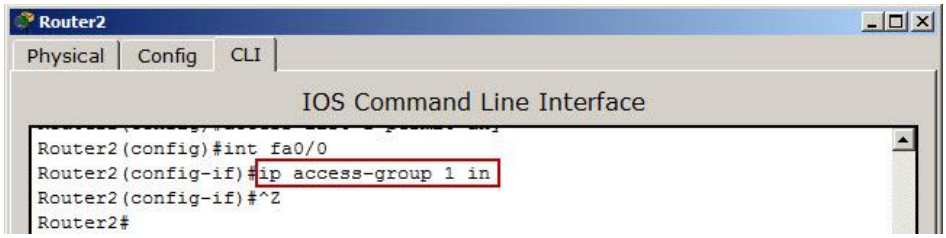
Ngoài lệnh `access-list 1 deny host 24.17.2.18`, ta còn có thể sử dụng hai lệnh tương đương sau:

```
# access-list 1 deny 24.17.2.18 0.0.0.0
```

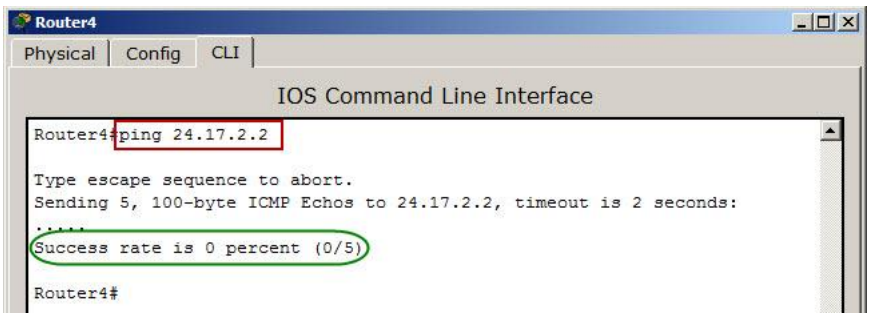
và

```
# access-list 1 deny 24.17.2.18
```

10. Sau khi tạo xong access-list ở trên, ta cần gán nó cho cổng Fa0/0 của Router2 đồng thời chỉ ra hướng đi của gói tin mà access-list này sẽ kiểm soát (đi vào hay đi ra từ cổng Fa0/0 của Router2). "in" có nghĩa là các gói tin đến từ mạng và sẽ đi vào router và "out" có nghĩa rằng các gói tin đi ra khỏi router và đi vào mạng.



11. Kiểm tra lại rằng bây giờ Router4 không thể ping tới cổng Fa0/0 của Router2 nữa.



Lab 29: Verify Standard Access Lists

Kiểm tra lại cấu hình Standard ACL

A. Mục tiêu của bài lab:

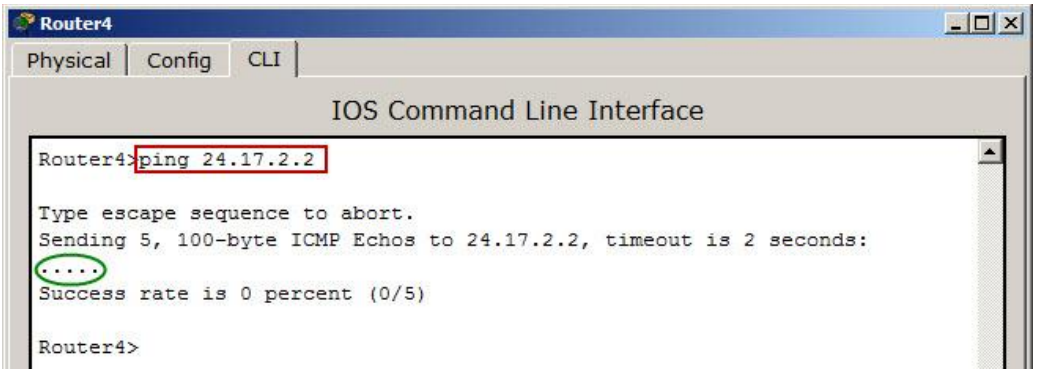
Kiểm tra xem access-list đã được cấu hình đúng hay chưa.

B. Chuẩn bị cho bài lab:

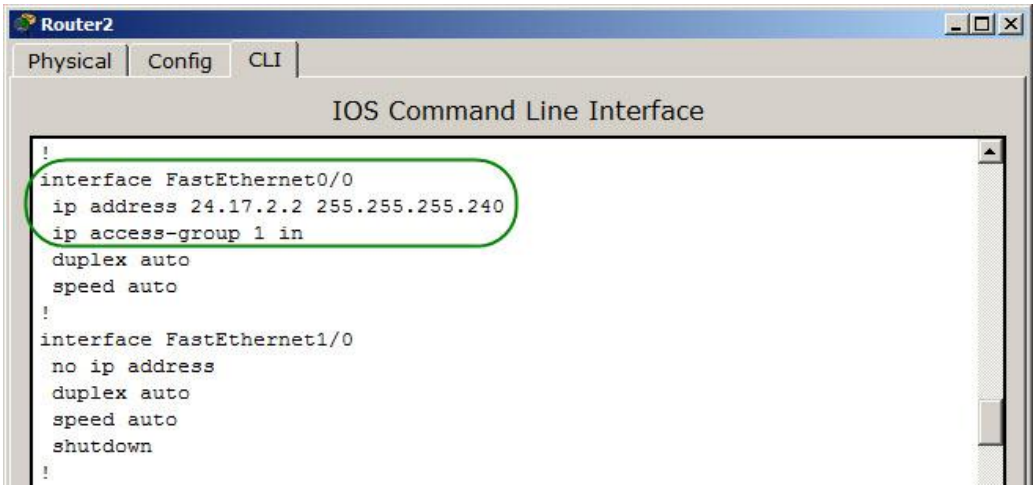
- Yêu cầu: đã hoàn thành xong lab 28 (Standard Access List)
- Chúng ta sẽ tiếp tục làm việc với mô hình của lab 28.

C. Các bước thực hiện:

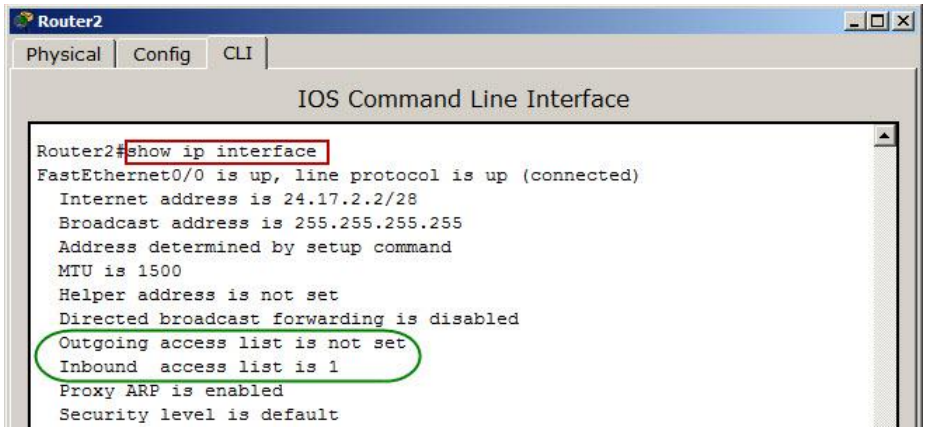
1. Ở bước đầu tiên này ta sẽ xem xét xem có thể ping tới Router2 từ Router4 không. Kết nối tới Router4 và thử ping tới cổng Fa0/0 của Router2 (có địa chỉ IP là 24.17.2.2). Nếu bạn nhận được 5 dấu chấm như hình sau thì access-list mà ta đã tạo ở lab 28 đã làm việc đúng.



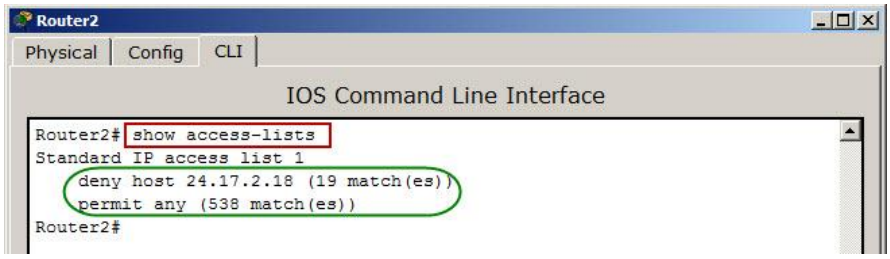
2. Truy cập vào Router2 và thẩm tra xem các access-list của ta đang chạy trên các interface nào, xem nội dung của running-config



3. Ta cũng có thể xem các access-list được áp dụng cho các interface nào bằng lệnh `show ip interface`



4. Lệnh `show access-lists` sẽ cho ta biết các access-list nào mà ta đã tạo trên router. Nó cũng sẽ cho ta biết các entry nào trong access-list đã được sử dụng và số lượng gói tin mà router cho phép hoặc bị chặn.



Lab 30: Extended Access Lists

Danh sách kiểm soát truy cập mở rộng

A. Mục tiêu của bài lab:

Tìm hiểu và thực hành cấu hình các danh sách kiểm soát truy cập mở rộng (Extended ACL).

B. Chuẩn bị cho bài lab:

Sử dụng lại mô hình cũng như các bước cấu hình địa chỉ IP cho các interface và RIP trên các router tượng tự bài lab 28.

Lưu ý: Nếu bạn đã thực hiện cấu hình Standard ACL ở lab 28 thì trước khi đi vào các bước của lab 29 này, bạn cần thực hiện lệnh `no ip access-group 1` trên cổng Fa0/0 của Router2 (hoặc sử dụng lệnh `no ip access-list standard 1` trong chế độ Configuration của Router2)

C. Các bước thực hiện: (từ bước 1 -> 8, thực hiện giống lab 28)

9. Hai extended access list mà ta sẽ tạo ra sau đây có 2 tác dụng khác nhau. Đầu tiên, ta sẽ chỉ cho phép subnet nối trực tiếp với cổng S2/0 của Router1 được telnet tới cổng S2/0 của Router1. Để làm điều này ta chạy lệnh sau trong chế độ Configuration của Router1.

```
Router1(config)#access-list 101 permit tcp 24.17.2.16
0.0.0.15 any eq telnet
```

10. Tiếp đến ta sẽ cho phép bất kỳ gói tin nào từ subnet 24.17.2.0 bằng lệnh sau

```
Router1(config)#access-list 102 permit ip 24.17.2.0
0.0.0.15 any
```

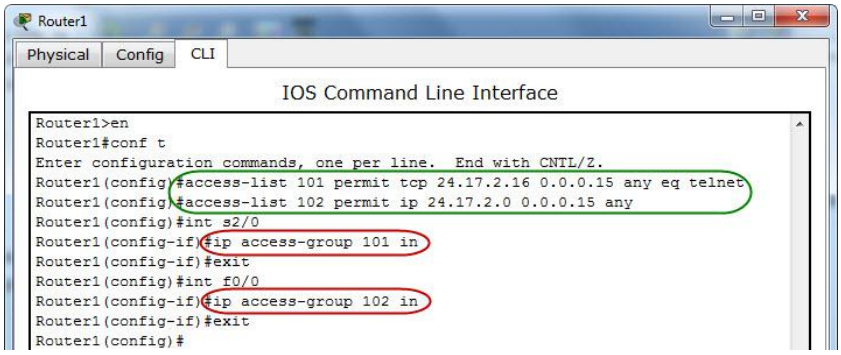
11. Giờ ta cần gán các access-list này cho các interface. Dưới đây là các lệnh dùng để gán `access-list 101` cho cổng S2/0 của Router1 theo hướng inbound (các gói tin đi vào cổng này sẽ chịu sự kiểm soát).

```
Router1(config)#int S2/0
Router1(config)#ip access-group 101 in
Router1(config)#exit
```

12. Với cổng Fa0/0 thì ta cần gán `access-list 102` hướng inbound.

```
Router1(config)#int F0/0
Router1(config)#ip access-group 102 in
```

```
Router1(config)#exit
```



13. Như vậy là ta đã hoàn thành xong các yêu cầu của bài lab này. Ở bài lab kế tiếp ta sẽ thực hiện các bước để thẩm định rằng các access-list trong bài này được cấu hình chuẩn xác.

Lab 31: Verify Extended Access Lists

Kiểm tra Extended Access Lists

A. Mục tiêu của bài lab:

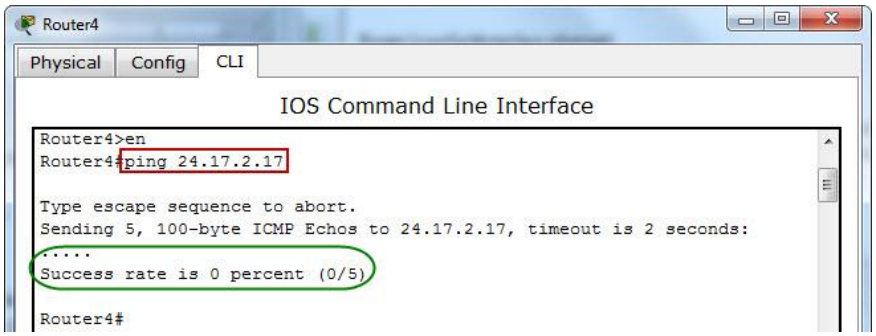
Kiểm tra lại các cấu hình access-list ở bài lab 30.

B. Chuẩn bị cho bài lab:

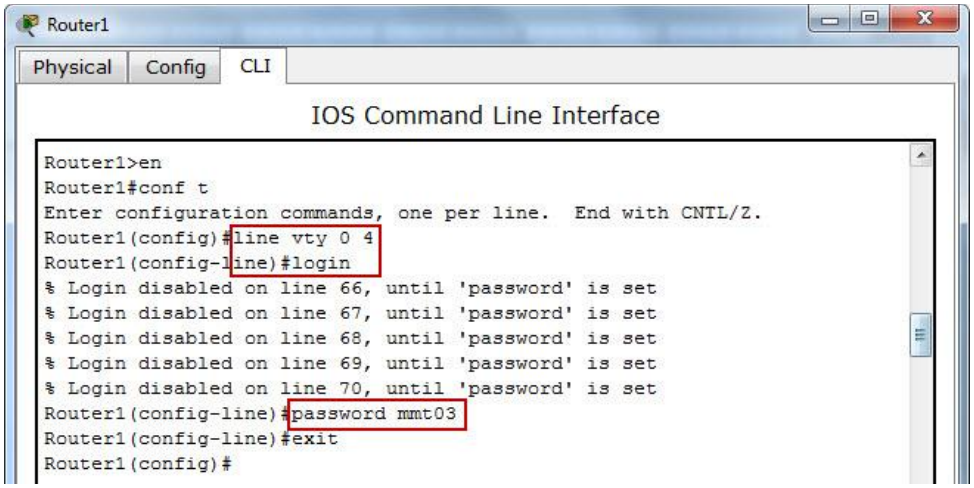
- Sử dụng lại mô hình cũng như các bước cấu hình địa chỉ IP cho các interface và RIP trên các router tượng tự bài lab 28.
- Đã hoàn thành cấu hình extended access list trong bài lab 30.

C. Các bước thực hiện:

1. Giờ ta sẽ kiểm tra xem các access-list ở lab 30 có được cấu hình đúng chưa. Kết nối tới Router4 và thử ping tới cổng S2/0 của Router1. Nếu ping không thành công thì `access-list 101` đang làm việc đúng.



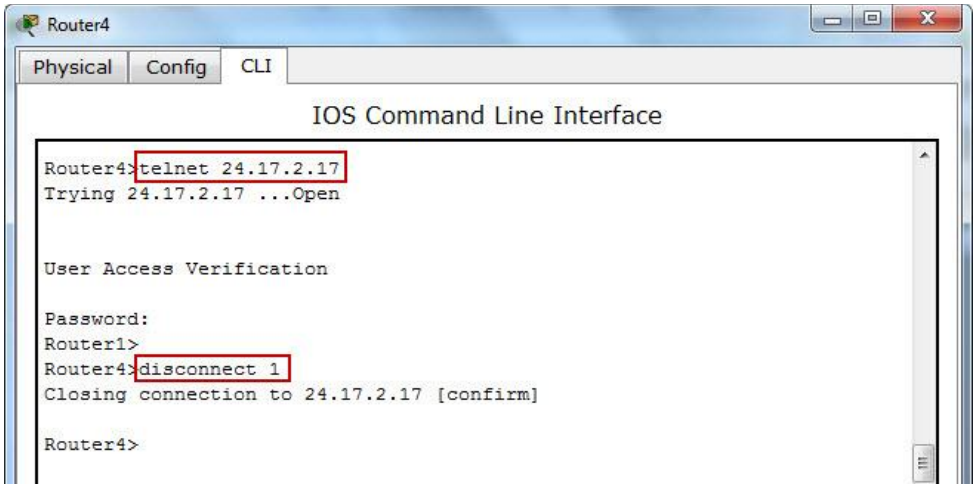
2. Tiếp đến ta cần kiểm tra xem từ Router4 có được phép telnet tới Router1 chưa. Kết nối tới Router1 và cho phép truy cập bằng telnet, sau đó thiết lập mật khẩu cho kết nối telnet là mmt03.



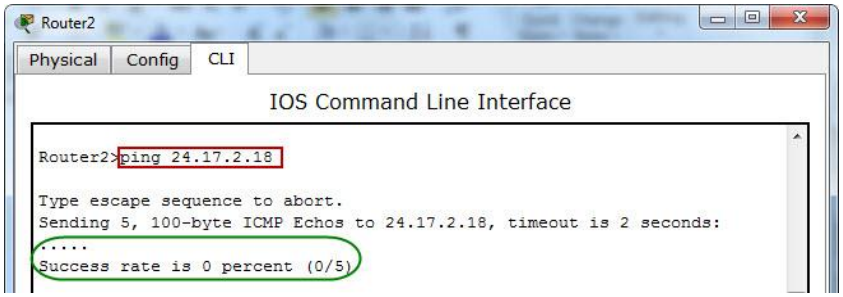
3. Giờ kết nối trở lại Router4 và thử telnet tới Router1

```
Router4#telnet 24.17.2.17
```

4. Nếu thấy dấu nhắc lệnh của router đổi thành Router1 thì tức là ta đã telnet thành công tới Router1. Giờ chạy lệnh exit hoặc nhấn giữ tổ hợp phím `control+shift+6+x` để trở lại Router4. Sau đó, gõ tiếp lệnh `disconnect 1` để đóng kết nối telnet tới Router1. Như vậy, ta đã cấu hình đúng cho access-list.

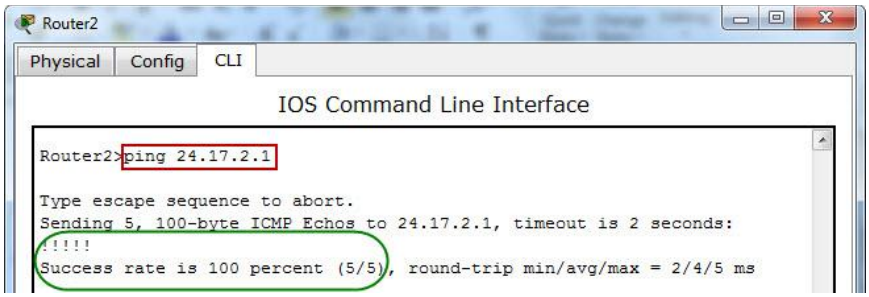


5. Giờ kết nối tới Router2 và kiểm tra xem ta có thể ping tới cổng S2/0 của Router4 hay không

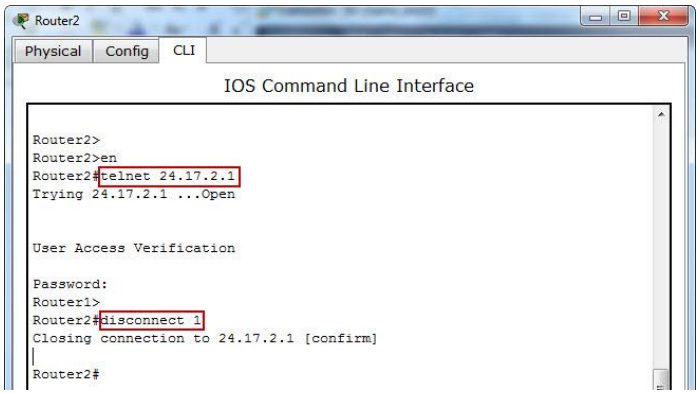


6. Kết quả cho thấy ta không thể lệnh ping ở bước 5 không thành công, tại sao lại như vậy? Hãy mường tượng ra quá trình mà gói tin lưu chuyển trong mạng. Gói tin bắt đầu tại Router2, đi qua Router1 và được chuyển tới Router4. Sau đó, tại Router4, gói tin được đóng gói lại và gửi trả về cho Router1. Khi Router4 đóng gói lại gói tin, IP nguồn của gói tin trở thành IP đích và IP đích trở thành IP nguồn. Khi gói tin gặp phải access-list trên cổng S2/0 của Router1 thì nó bị chặn lại bởi vì IP nguồn của gói tin là địa chỉ của cổng S2/0 của Router4.

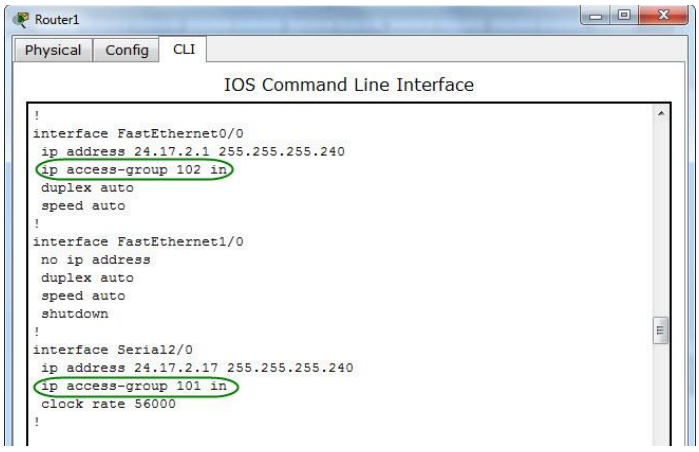
7. Giờ ta kiểm tra xem từ Router2 có thể ping tới cổng Fa0/0 của Router1 (24.17.2.1) hay không



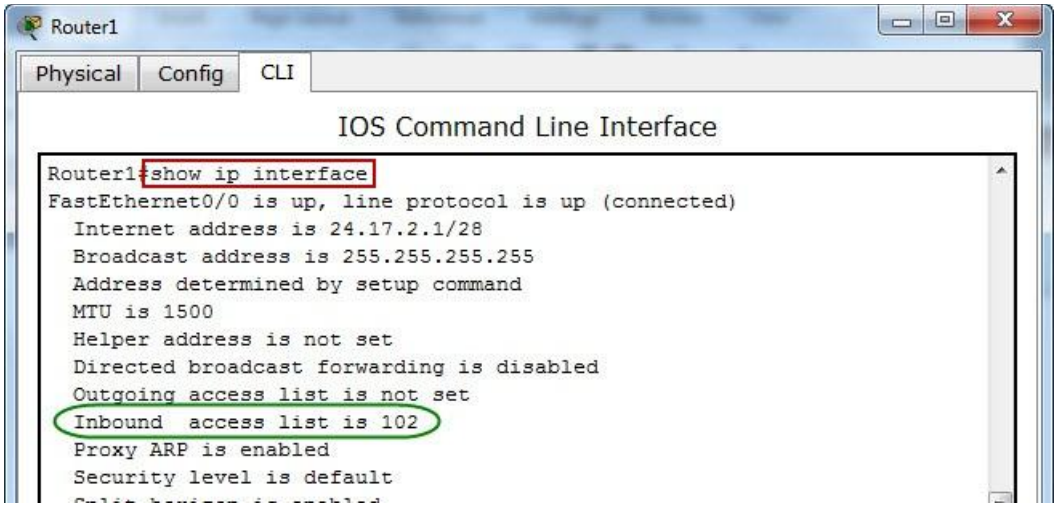
8. Nếu ping được thì ta có thể kiểm tra thêm khả năng telnet tới Router1 như sau:



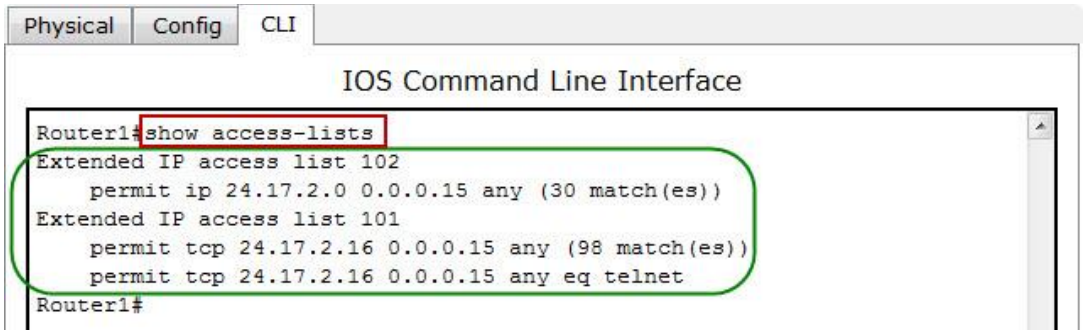
9. Để thẩm tra access-list nào được gán cho interface nào, ta sẽ xem nội dung của running-config



10. Ngoài ra, ta cũng có thể sử dụng lệnh `show ip interface` để đạt được mục đích như bước 9



11. Lệnh `show access-lists` sẽ cho biết các access-list nào được tạo trên router. Nó cũng cho ta biết các entry nào của access-list đã được sử dụng và có bao nhiêu gói tin được phép hoặc bị từ chối bởi access-list.



Lab 32: Named Access Control Lists

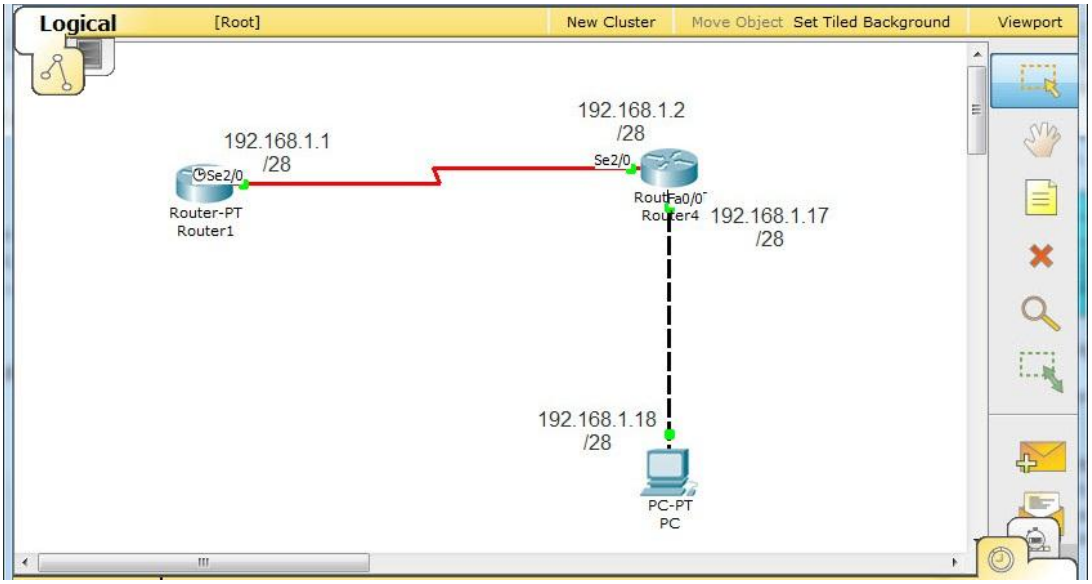
Named Access Control Lists

A. Mục tiêu của bài lab:

Tạo một ACL được gán tên (thay vì được nhận dạng bởi con số như trong các bài lab trước) để cấm tất cả các gói ping từ PC tới Router1 nhưng cho phép truy cập từ Router4 tới Router1. Ta sẽ cấu hình các ACL này trên Router1

B. Chuẩn bị cho bài lab:

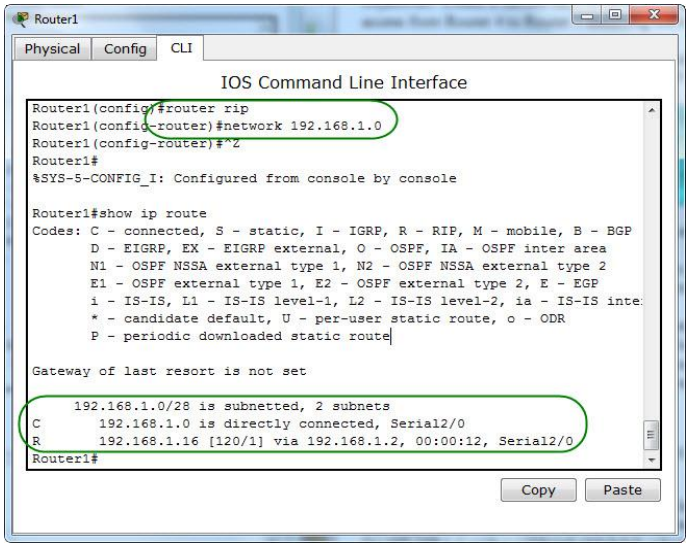
Xây dựng mô hình kết nối giữa PC và các router và cấu hình IP cho các thiết đó như hình dưới đây:



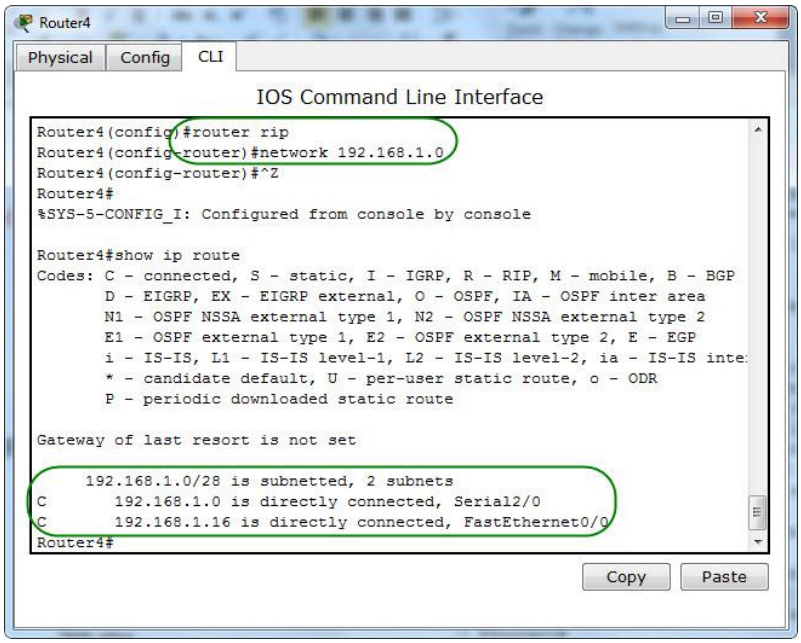
C. Các bước thực hiện:

1. Cấu hình giao thức định tuyến RIP trên cả 2 router sử dụng các lệnh `network` thích hợp (xem lại lab 13)
2. Chạy lệnh `show ip route` để đảm bảo các tuyến đường trong bảng định tuyến của các router là đầy đủ và chính xác. Sau đó kiểm tra kết nối giữa các thiết bị bằng lệnh ping.

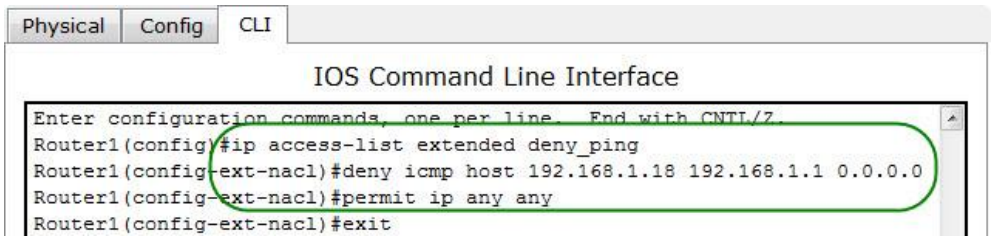
Trên Router1



Trên Router4



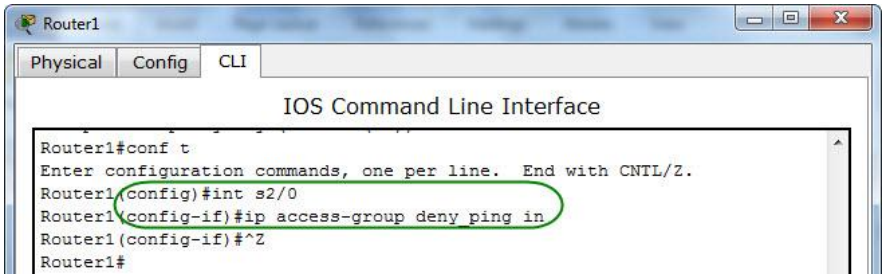
3. Giờ ta sẽ ngăn chặn tất cả các lưu lượng ping xuất phát từ PC và được gửi cho Router1. Access list này có thể nằm trên Router4 hoặc Router1. Thường thì ta sẽ có access list được đặt trên router mà nằm gần nguồn (gửi gói tin) nhất có thể vì điều này giúp loại bỏ nguy cơ các lưu lượng không cần thiết di chuyển trong mạng. Nhưng ở ví dụ này, ta sẽ đặt access list trên Router1 với hướng inbound như sau:



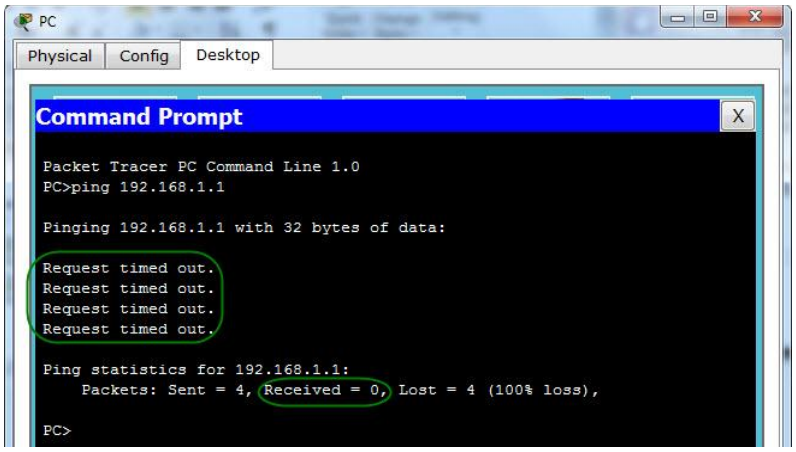
Theo hình trên thì:

- Câu lệnh đầu tiên chỉ rõ kiểu của access list là extended.
- Dòng lệnh thứ hai có tác dụng từ chối bất kỳ gói ICMP nào được gửi từ host có IP là 192.168.1.1 và đích đến là host có IP là 192.168.1.1. Để ý rằng ta đã dùng tham số lệnh host cho phần đầu (source address) của access list và dùng wildcard 0.0.0.0 cho phần hai (destination address) của access list. Cả host và wildcard ở đây đều có tác dụng giống nhau là xác định địa chỉ IP của một host cụ thể (chứ không phải một tập các IP).
- Lệnh thứ ba cho biết rằng tất cả các lưu lượng khác đều ***không*** bị chặn bởi access list.

4. Kế tiếp ta sẽ gán access list vừa tạo ở trên cho cổng S2/0 của Router1 và access list này sẽ dành cho hướng inbound.

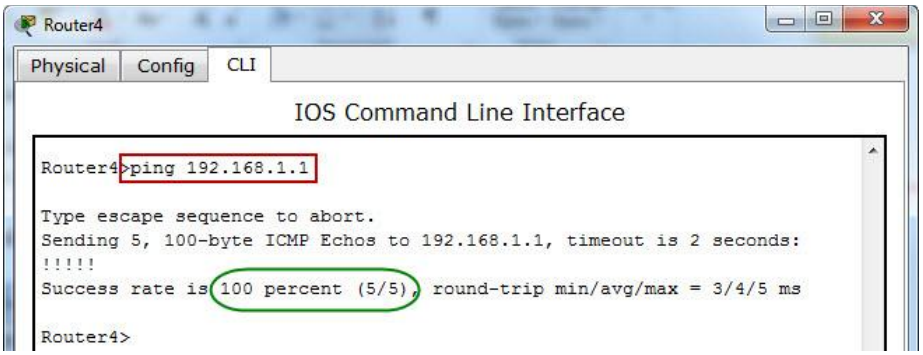


5. Giờ kết nối tới PC và thử ping tới cổng S2/0 của Router1 như sau



Ta thấy, PC có IP là 192.168.1.18 không thể ping tới IP 192.168.1.1, Như vậy, access list của ta đã làm việc đúng theo yêu cầu.

Xác nhận rằng từ Router4 có thể ping thành công tới Router1 như sau



Lab 33: Advanced Extended Access List

Nâng cao về Extended Access List

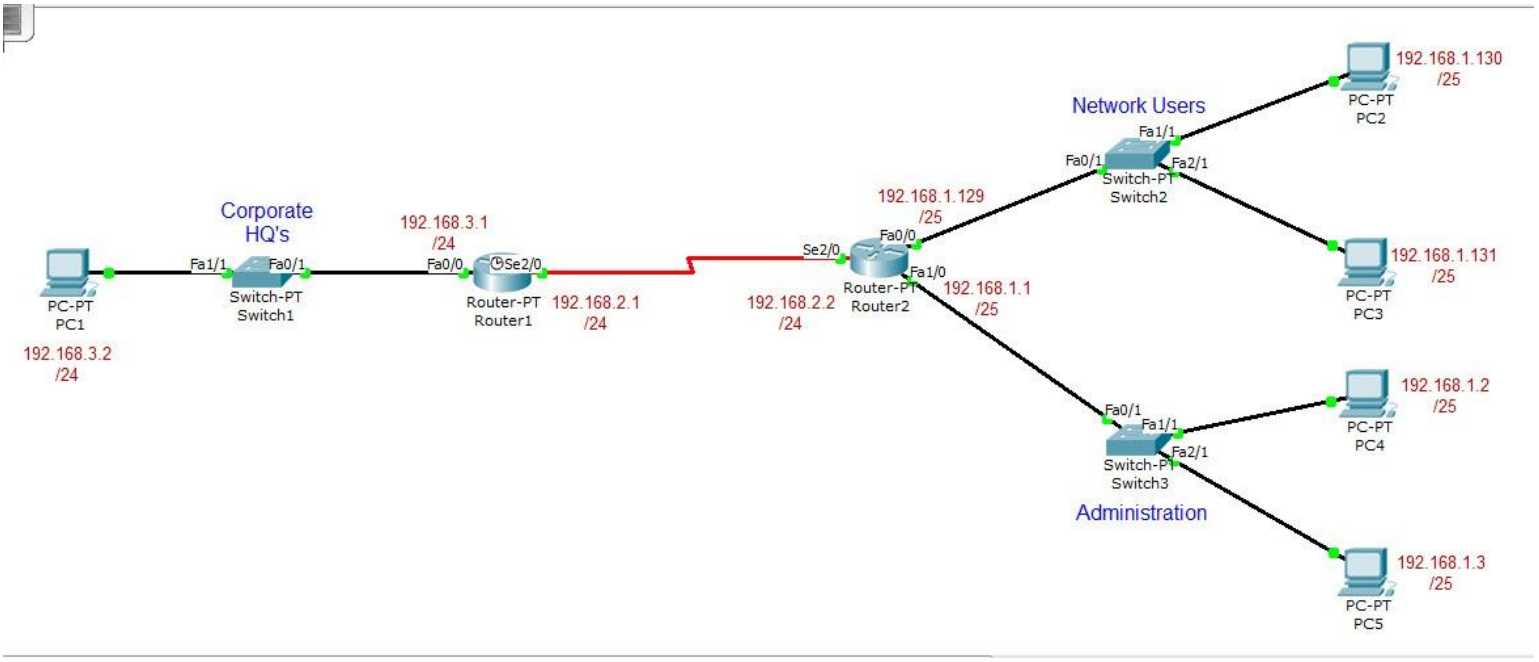
A. Mục tiêu của bài lab:

Cấu hình Extended Access List để lọc nhiều loại lưu lượng mạng (traffic) khác nhau như:

- Lọc các traffic gửi từ network này tới network kia.
- Lọc các traffic gửi từ host tới network.
- Lọc các traffic gửi từ network tới host.

B. Chuẩn bị cho bài lab:

1. Xây dựng sơ đồ mạng và cấu hình IP cho các thiết bị như hình sau:



2. Cấu hình RIP cho tất cả các router sử dụng các câu lệnh network thích hợp.
3. Đảm bảo rằng các route trong bảng định tuyến của các router được tạo ra đầy đủ và chính xác với lệnh `show ip route`.
4. Kiểm tra kết nối giữa các thiết bị bằng lệnh `ping`.

C. Các bước thực hiện:

✓ **Kiểm soát traffic gửi từ network này tới network kia.**

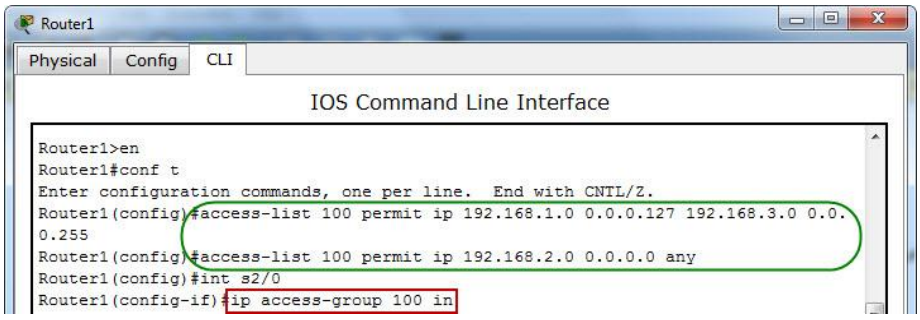
1. Access list đầu tiên ta tạo ra sẽ chỉ cho phép các traffic (sử dụng protocol bất kỳ) từ mạng Administration (gồm PC4 và PC5) gửi tới mạng Corporate HQ (gồm PC1). Để làm điều này ta sẽ sử dụng extended access list như sau:

```
access-list 100 permit ip 192.168.1.0 0.0.0.127
192.168.3.0 0.0.0.255
access-list 100 permit ip 192.168.2.0 0.0.0.0 any
```

- Câu lệnh đầu có nghĩa rằng các IP nằm trong dải (192.168.1.0 -> 192.168.1.127) được phép gửi bất kỳ traffic nào tới các IP thuộc mạng 192.168.3.0/24.

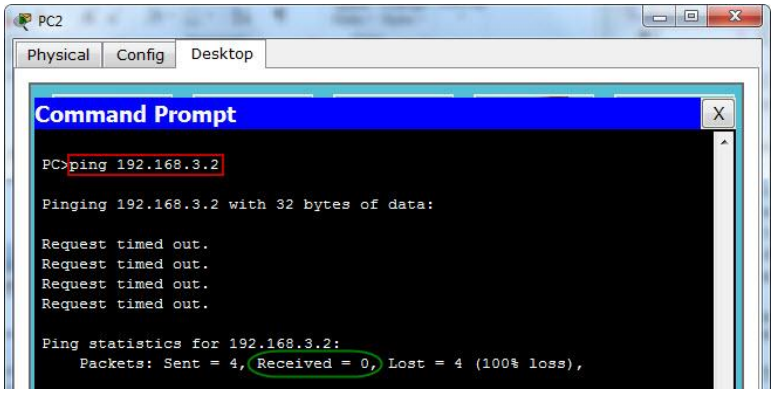
- Câu lệnh thứ hai có nghĩa rằng các các IP thuộc mạng 192.168.2.0/24 được phép gửi bất kỳ traffic nào tới bất kỳ mạng nào. Vì ngầm định, ở dưới cùng access list luôn có một entry mang nghĩa cấm tất cả các traffic vào/ra nên ta cần tới lệnh này để các router1 và router2 có thể trao đổi (dạng broadcast) các thông tin định tuyến (RIP) cho nhau.

2. Vì traffic xuất phát từ Router2 và đi đến Router1 nên ta sẽ cấu hình và gán access list cho cổng S2/0 của Router1 để kiểm tra tất cả các traffic gửi đến cổng này (hướng inbound).

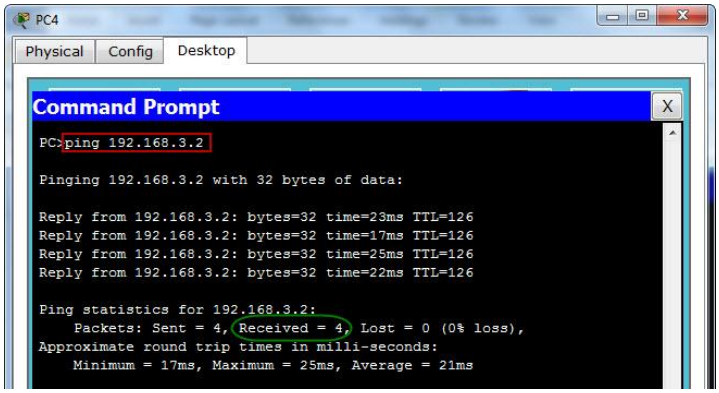


3. Để kiểm tra access list này, thử ping PC1 từ PC2, PC3, PC4 và PC5. Nếu PC2 và PC3 không thể ping tới PC1 nhưng PC4 và PC5 thì có thể thì ta đã access list đã làm việc đúng theo yêu cầu.

Trên PC2

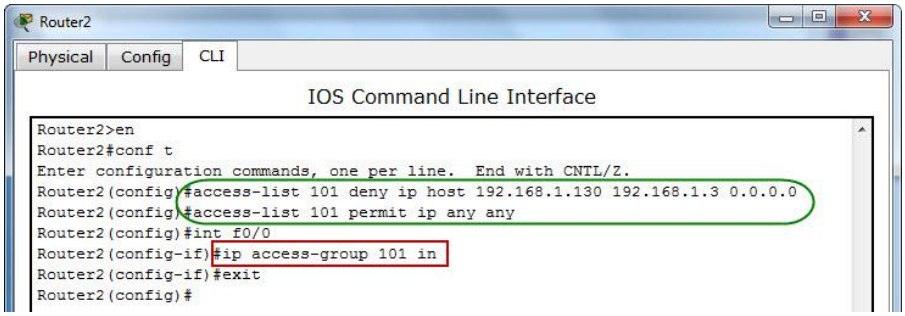


Trên PC4



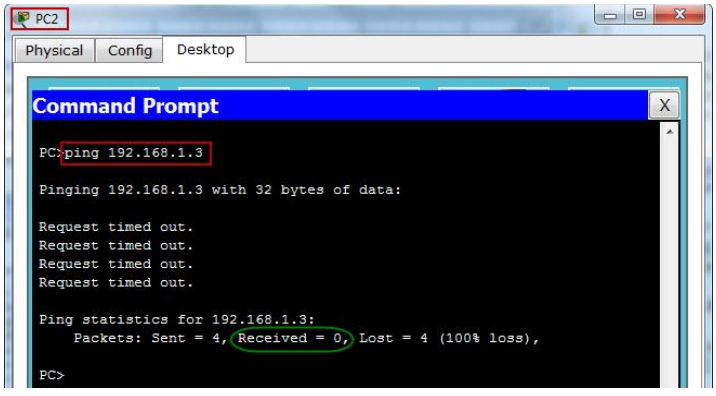
✓ **Kiểm soát traffic gửi từ host này tới host kia**

1. Phần tiếp theo của bài lab này, ta sẽ khóa việc truy cập đến file server (PC5) từ một máy trạm cụ thể (PC2). Để thực hiện điều này, ta sẽ tạo một access list trên Router2 có tác dụng chặn tất cả các traffic gửi từ PC2 đến PC5. Sau đó gán access list này cho cổng Fa0/0 của Router2.

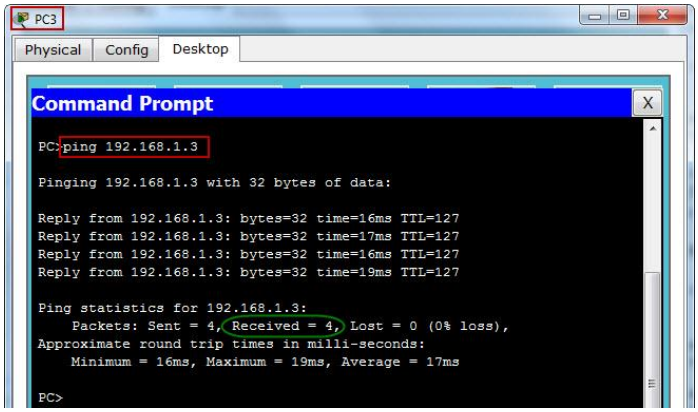


2. Giờ kết nối tới PC2 và xác nhận rằng ta không thể ping tới PC5 nhưng từ PC3 ta có thể ping tới PC5

Trên PC2



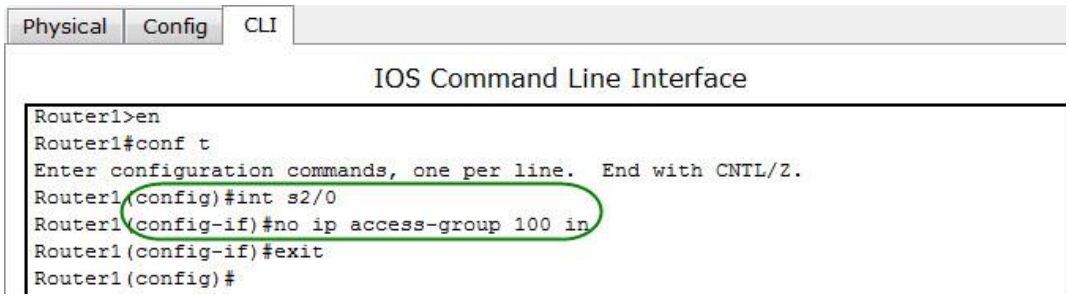
Trên PC3



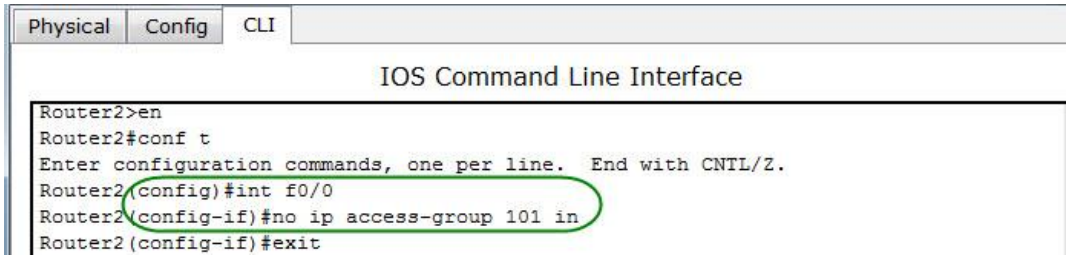
✓ **Kiểm soát traffic gửi từ network cho host**

1. Trước khi bắt đầu cấu hình cho access list mới này, ta cần loại bỏ các access list trên Router1 và Router2 vừa tạo ở trên như sau:

Trên Router1



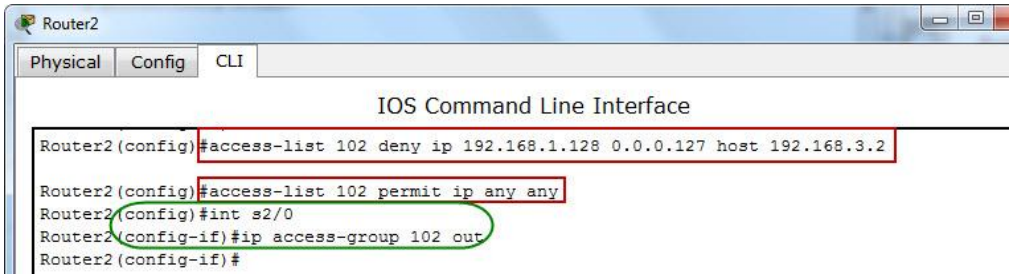
Trên Router2



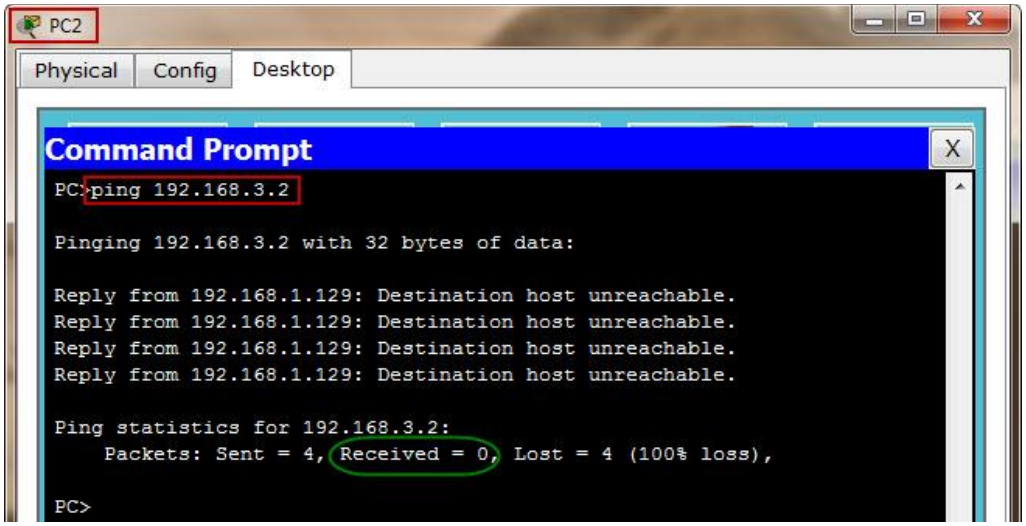
2. Ở kịch bản cuối cùng này, ta sẽ chặn tất cả các traffic gửi đến PC1 từ vùng Network Users như trong sơ đồ mạng ở trên. Để làm điều này, ta sẽ viết một extended access list như sau:

```
access-list 102 deny ip 192.168.1.128 0.0.0.127 host
192.168.3.2
access-list 102 permit ip any any
```

Rồi gán access list 102 này cho cổng S2/0 của Router2 với hướng outbound.



Để kiểm tra access list có làm việc đúng chưa, thử ping PC1 từ PC2 hoặc PC2, nếu ping thất bại thì chúc mừng, ta đã hoàn thành xong bài lab 33 này.



Lab 34: Introduction to Telnet

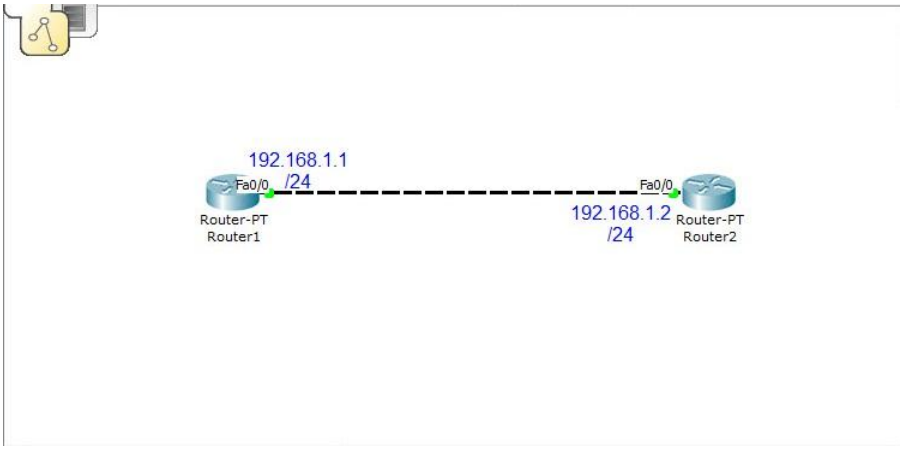
Làm quen với Telnet trên Router

A. Mục tiêu của bài lab:

Tìm hiểu việc thiết lập phiên kết nối Telnet giữa 2 router.

B. Chuẩn bị cho bài lab:

- Sử dụng Router1 và Router2 được kết nối trực tiếp với nhau thông qua cổng Ethernet trên 2 router này.

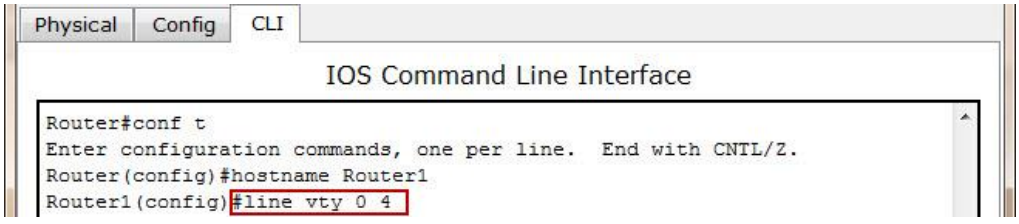


- Cấu hình địa chỉ IP cho các cổng Fa0/0 trên 2 router như sơ đồ trên. Sau đó kiểm tra kết nối giữa chúng bằng lệnh ping.

C. Các bước thực hiện:

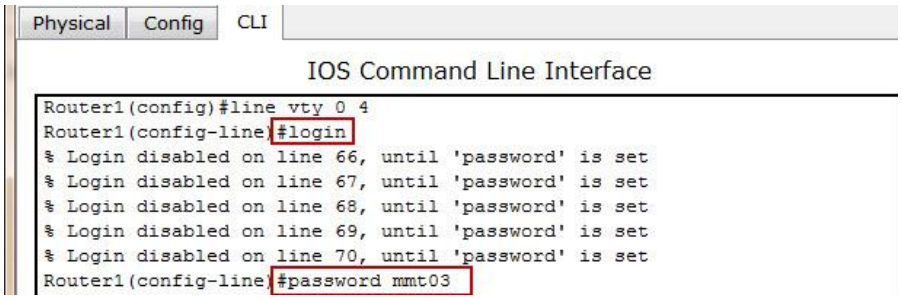
1. Kết nối vào Router1. Ở đây, Router1 đóng vai trò làm thiết bị tiếp nhận các yêu cầu thiết lập phiên telnet và quy định mật khẩu mà các thiết bị khác cần sử dụng nếu muốn telnet vào nó.

- Vào chế độ Configuration của Router1.
- Truy cập vào các line vty (virtual terminal). Mỗi vty đại diện cho một phiên telnet đang hoạt động và thường có tối đa 15 line vty trên router. Để Router1 hỗ trợ cùng lúc 5 phiên telnet (tương ứng với 5 vty) thì câu lệnh mà ta cần gõ vào ở đây là `line vty 0 4`

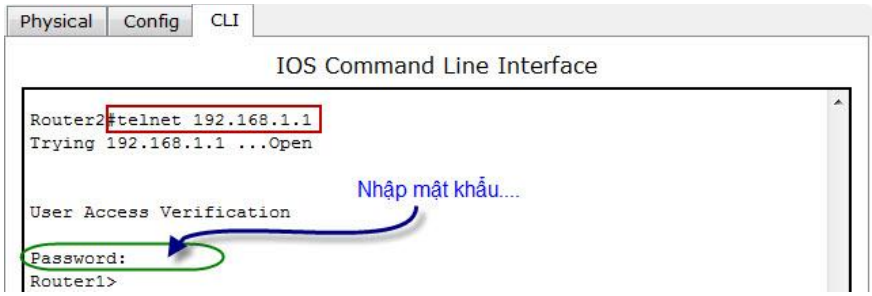


2. Giờ ta cần báo cho Router1 biết rằng ta sẽ đòi hỏi người dùng cung cấp mật khẩu đăng nhập khi họ muốn telnet vào Router1 sử dụng lệnh `login`.

3. Gõ vào mật khẩu được sử dụng để thiết lập phiên telnet, ở đây ta chọn mật khẩu là mmt03

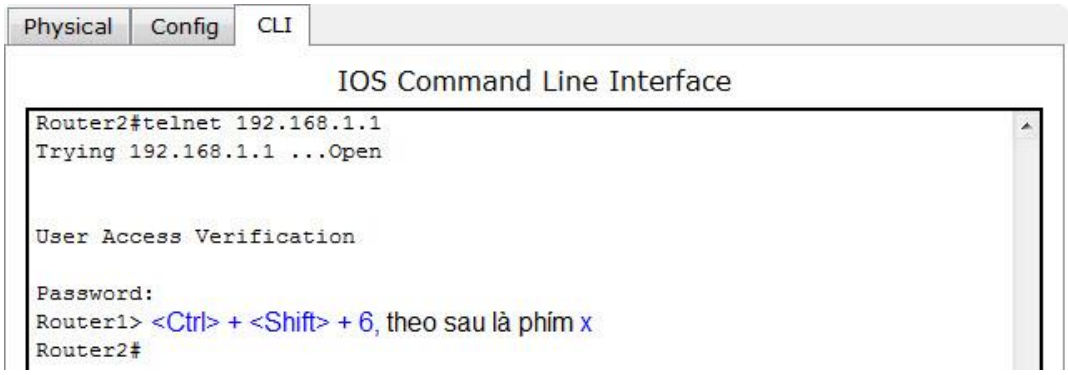


4. Vào Router2. Gõ lệnh sau để kết nối telnet đến Router1 sử dụng địa chỉ IP của cổng Fa0/0 trên Router1.



Sau đó, gõ vào mật khẩu là mmt03 để đăng nhập. Nếu dấu nhắc lệnh trả về là Router1> thì ta đã telnet thành công vào Router1.

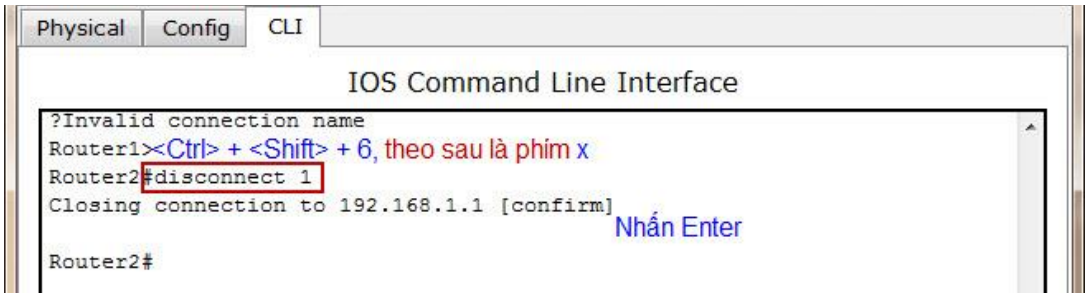
5. Giờ nhấn đồng thời tổ hợp phím `Ctrl+Shift+6`, sau đó thả ra và ngay lập tức nhấn phím `x`. Bạn sẽ nhận thấy rằng dấu nhắc lệnh (hostname) đã đổi thành Router2 tức là giờ ta quay lại làm việc với Router2 (và phiên telnet vừa tạo vẫn được duy trì).



6. Tiếp tục, gõ lệnh `show sessions` để xem tất cả các phiên telnet đang hoạt động. Để trở lại làm việc với phiên telnet nào đó, xác định con số đại diện cho phiên telnet đó rồi sử dụng lệnh resume như sau:

Ở đây, số 1 tương ứng với phiên telnet tới IP 192.168.1.1 (Router1) và ta thấy rằng dấu nhắc lệnh đã quay về lại là Router1.

7. Giờ nhấn tổ hợp phím `Ctrl+Shift+6` theo sau đó là phím x để lại quay về Router2. Cuối cùng gõ lệnh `disconnect 1` để kết thúc phiên telnet tới Router1



Lab 35: Introduction to VLAN

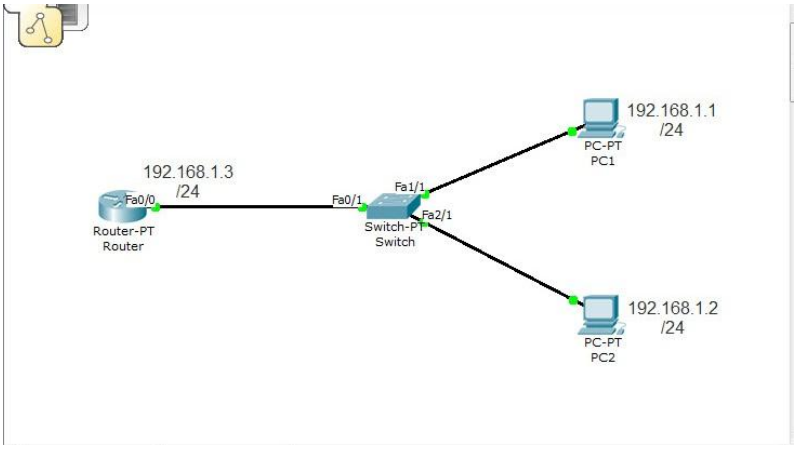
Giới thiệu về VLAN

A. Mục tiêu của bài lab:

Biết được những ưu điểm của VLAN.

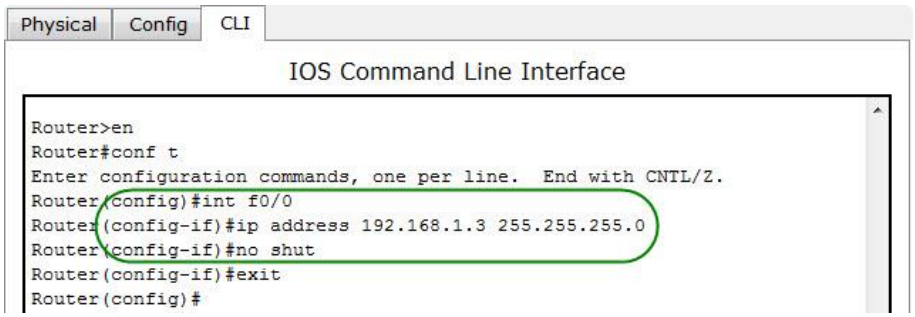
B. Chuẩn bị cho bài lab:

Sử dụng Router, Switch và PC1, PC2 được kết nối và cấu hình IP như hình sau.
Chúng ta sẽ cấu hình cho Router và Switch để hỗ trợ VLAN. Mục đích của lab này là thiết lập các PC1 và PC2 có thể ping được cho nhau thông qua switch. Sau đó ta sẽ thay đổi các VLAN trên switch để chúng không thể ping cho nhau cũng như không thể ping tới router được nữa. Cuối cùng ta sẽ thay đổi cấu hình trên Switch để các PC thuộc cùng VLAN và xem xét rằng chúng lại có thể ping cho nhau.

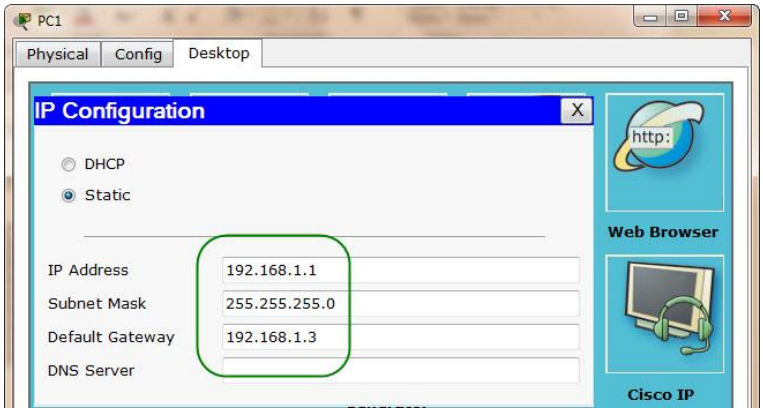


C. Các bước thực hiện:

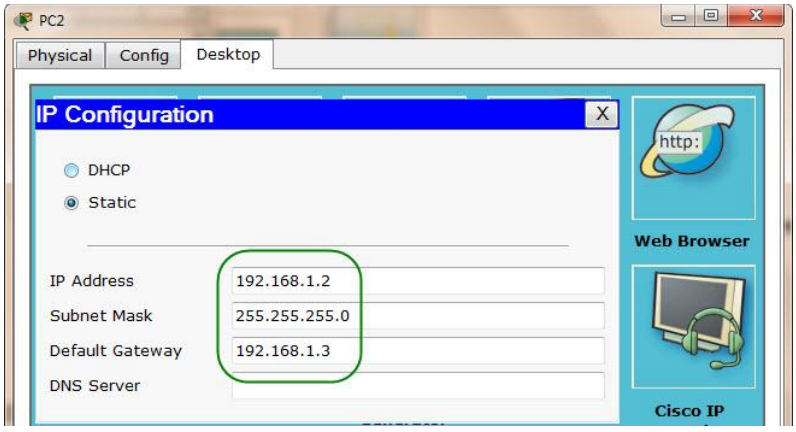
1. Bắt đầu bằng việc cấu hình địa chỉ IP cho cổng Fa0/0 của Router như sau.



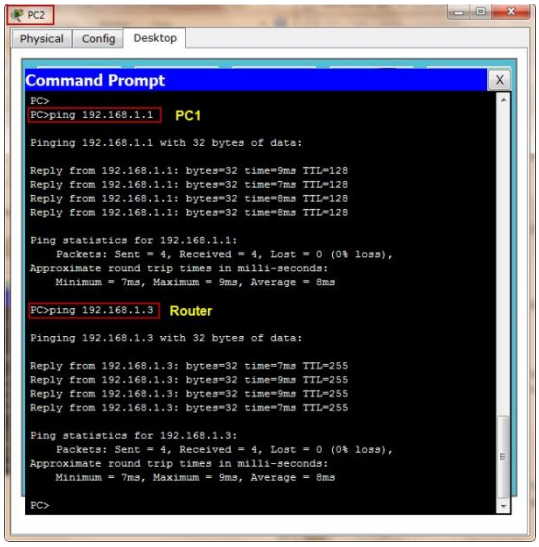
2. Kết nối tới PC1 và đặt IP cho nó như sau



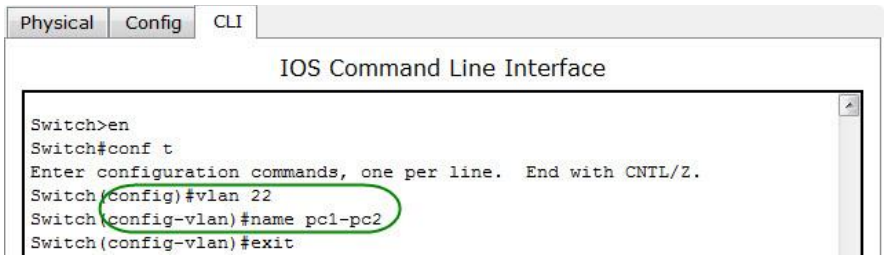
3. Kết nối tới PC2 và đặt IP cho nó như sau



4. Từ PC2, kiểm tra ping thành công tới PC1 và Router

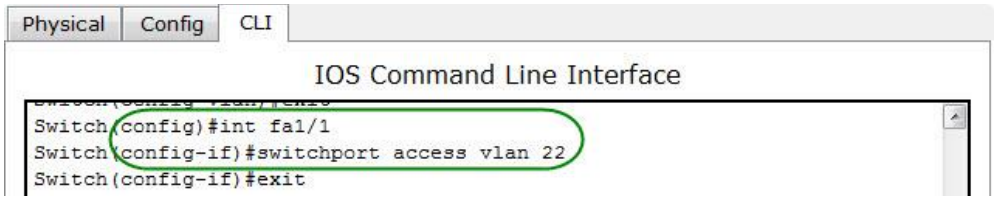


5. Giờ kết nối tới Switch và cấu hình VLAN. Mặc định, thì tất cả các cổng (port) trên switch đều nằm trong cùng VLAN có ID là 1 (VLAN 1). Trong trường hợp này ta sẽ thiết đặt cho port Fa1/1 của switch (hiện đang nối với PC1) vào một VLAN có ID là 22 tách biệt với các port còn lại. Bắt đầu tạo một VLAN mới có ID là 22 như sau:

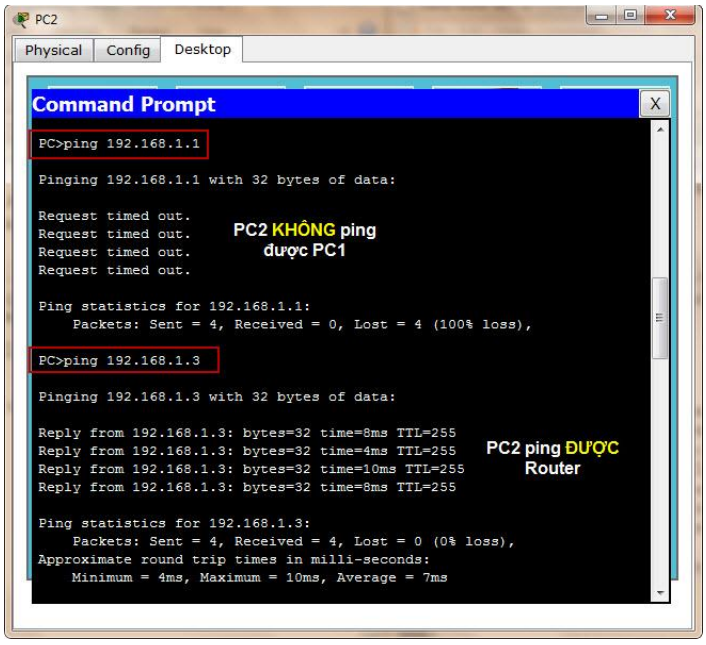


Nếu muốn bạn có thể đặt tên cho VLAN 22 này để giúp nhận dạng và phân biệt dễ dàng hơn giữa các VLAN, như trong hình trên ta đặt là *pc1-pc2*.

6. Giờ ta cần gán các port vào VLAN 22 vừa tạo ở bước 5. Dưới đây sẽ gán port Fa1/1 của Switch đang nối với PC1 vào VLAN 22.



7. Tiếp đến ta kết nối lại vào PC2 và thử ping tới PC1 và Router thì kết quả như sau:

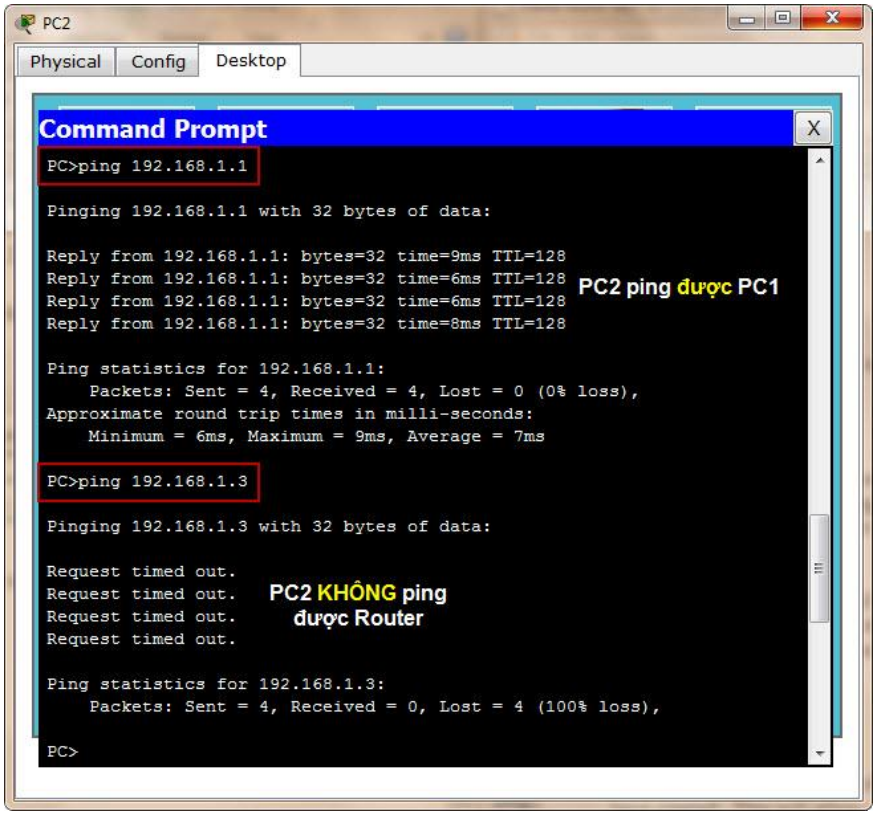


Như hình trên ta thấy, PC2 có thể ping tới Router nhưng PC1 không thể ping được PC1. Tại sao lại như vậy?

Trên Switch, ta đã cấu hình cho VLAN 22 chỉ gồm port Fa1/1. Điều này có nghĩa rằng tất cả các port còn lại (Fa0/1, Fa2/1 -> Fa5/1) vẫn còn nằm trong VLAN 1. Vì thế, khi PC2 (hiện đang nối với port Fa2/1) gửi gói tin ping tới Switch thì các gói tin đó được đánh dấu là VLAN 1 và cũng đồng nghĩa với việc chúng chỉ có thể đi ra khỏi các port thuộc VLAN 1 mà thôi. Và kết quả là chúng (các gói tin ping từ PC2) không thể đi ra khỏi port Fa0/1 thuộc VLAN 22 để tới PC1.

8. Giờ ta lại kết nối trở lại Switch và cấu hình VLAN cho port Fa2/1 (hiện đang nối với PC2) nằm trong VLAN 22 như sau

9. Giờ kết nối lại với PC2 và thử ping lại tới Router và PC1



Sự khác lạ ở đây là gì? Hiện PC2 đã có thể ping tới PC1 nhưng vẫn không thể ping tới Router. Lý do là vì lúc này gói tin ping từ PC2 được đánh dấu là VLAN 22, tức là nó chỉ có thể đi ra khỏi port Fa0/1 đang được nối với PC1 và cũng thuộc VLAN 22. Đây cũng chính là mục đích của bài lab mà ta muốn thực hiện.

10. Kết nối trở lại Switch và sử dụng lệnh `show vlan` (hoặc `show vlan brief`) để xem xét việc phân định VLAN

```
Switch#show vlan brief

VLAN Name                              Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa3/1, Fa4/1, Fa5/
22   pc1-pc2                          active    Fa1/1, Fa2/1
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

11. Cuối cùng, kết nối lại vào Switch và gán port Fa0/1 vào VLAN 22 để cho phép cả 3 thiết bị (Router, PC1, PC2) có thể ping được lẫn nhau.

Physical | Config | CLI

IOS Command Line Interface

```
Switch(config)#int fa0/1
Switch(config-if)#switchport access vlan 22
Switch(config-if)#exit
Switch(config)#
```

12. Kiểm tra lại việc ping thành công giữa Router, PC1 và PC2 bằng cách từ Router ping tới PC1 và PC2

Physical | Config | CLI

IOS Command Line Interface

```
Router>ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/9/10 ms

Router>ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 7/8/11 ms
```

Lab 36: VLAN Trunking Protocol

Cấu hình VLAN Trunking Protocol (VTP)

A. Mục tiêu của bài lab:

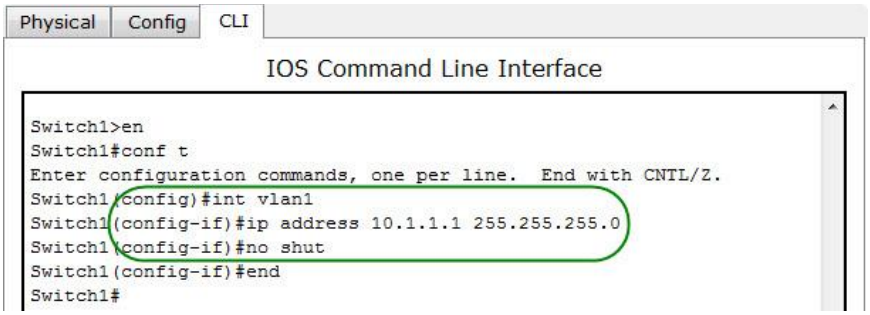
- Tạo các VLAN trên switch Catalyst 2950.
- Gán cùng lúc nhiều port vào các VLAN
- Cấu hình giao thức VTP để thiết lập kết nối giữa VTP server và VTP client.
- Tạo một đường trunk giữa 2 switch để làm kênh truyền dẫn giúp đồng bộ thông tin về VLAN giữa các switch.
- Kiểm tra cấu hình của VLAN và VTP.

B. Chuẩn bị cho bài lab:

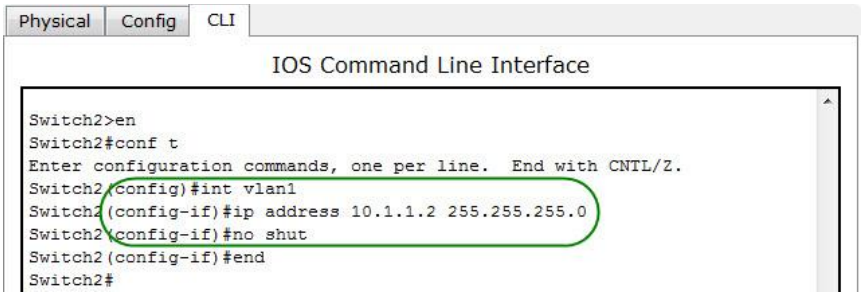
Trong Packet Tracer, sử dụng 2 switch 2950-24 và chúng được kết nối như sau

C. Các bước thực hiện:

1. Đặt địa chỉ IP cho interface VLAN1 của Switch1 như sau



2. Đặt địa chỉ IP cho interface VLAN1 của Switch2 như sau



3. Kiểm tra kết nối thành công giữa 2 switch bằng cách ping qua lại giữa chúng

Từ Switch1 ping tới Switch2

```
Switch1#ping 10.1.1.2
```

ping tới Switch2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

Switch1#
```

Từ Switch2 ping tới Switch1

```
Switch2#ping 10.1.1.1
```

ping tới Switch1

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

Switch2#
```

4. Tại Switch1, tạo vlan 18 và vlan 14. Sau đó gán các port 0/2-0/5 cho vlan 8 và các port 0/6-0/10 cho vlan 14

Physical | Config | CLI

IOS Command Line Interface

```
Switch1>en
Switch1#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

Switch1(vlan)#vlan 8
VLAN 8 added:
    Name: VLAN0008
Switch1(vlan)#vlan 14
VLAN 14 added:
    Name: VLAN0014
Switch1(vlan)#exit
APPLY completed.
Exiting....
Switch1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#int range fa0/2-5
Switch1(config-if-range)#switchport access vlan 8
Switch1(config-if-range)#exit
Switch1(config)#int range fa0/6-10
Switch1(config-if-range)#switchport access vlan 14
Switch1(config-if-range)#exit
Switch1(config)#
```

5. Sử dụng lệnh `show vlan` để xác nhận cấu hình vlan vừa tạo ở trên là chính xác

```
Switch1#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24
8    VLAN0008                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
14   VLAN0014                          active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
```

6. Mặc định thì Catalyst switch được cấu hình làm VTP Server. Giờ ta muốn thiết lập cho Switch1 làm VTP Server còn Switch2 làm VTP Client. Ngoài ra thay đổi VTP domain thành UIT và VTP password là mmt03

Trên Switch1 thực hiện các lệnh sau

```
Switch1#
Switch1#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

Switch1(vlan)#vtp server
Device mode already VTP SERVER.
Switch1(vlan)#vtp domain UIT
Changing VTP domain name from NULL to UIT
Switch1(vlan)#vtp password mmt03
Setting device VLAN database password to mmt03
Switch1(vlan)#exit
APPLY completed.
Exiting....
Switch1#
```

Trên Switch2 thực hiện các lệnh sau

```
Switch2#
Switch2#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

Switch2(vlan)#vtp client
Setting device to VTP CLIENT mode.
Switch2(vlan)#vtp domain UIT
Changing VTP domain name from NULL to UIT
Switch2(vlan)#vtp password mmt03
Setting device VLAN database password to mmt03
Switch2(vlan)#exit
APPLY completed.
Exiting....
Switch2#
```

7. Kế tiếp ta cần tạo một đường trunk để truyền tải các thông tin cấu hình vlan từ Switch1 sang Switch2. Để làm điều này, ta sẽ bật trunking trên các port nối giữa 2 switch, ở đây là 2 port Fa0/1 của mỗi switch. Phương thức đóng gói (encapsulation) được sử dụng là 802.1q.

Trên Switch1, thực hiện các lệnh sau

```
Switch1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#int fa0/1
Switch1(config-if)#switchport mode trunk
Switch1(config-if)#end
Switch1#
```

Trên Switch2, thực hiện các lệnh sau

```
Switch2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch2(config)#int fa0/1
Switch2(config-if)#switchport mode trunk
Switch2(config-if)#end
Switch2#
```

8. Cuối cùng, để xem thông tin về các VLAN mà Switch2 cập nhật từ Switch1 thì tại Switch2 gõ lệnh show vlan

```
Switch2#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24
8    VLAN0008                          active
14   VLAN0014                          active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
```

Còn để xem thông tin trạng thái làm việc của VTP ta gõ

```
Switch2#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 7
VTP Operating Mode              : Client
VTP Domain Name                 : UIT
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x66 0xB8 0x32 0xB8 0x69 0x88 0xD6 0xF5
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:46
Switch2#
```

Lab 37: OSPF Single Area Configuration and Testing

Cấu hình OSPF (Single Area)

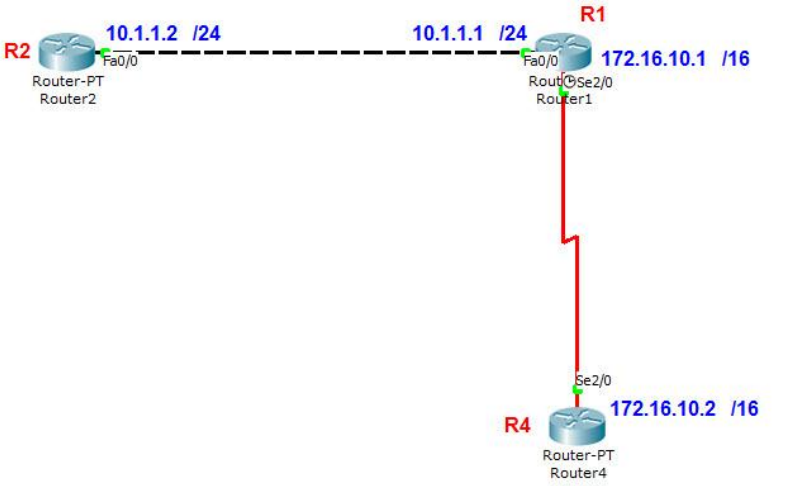
A. Mục tiêu của bài lab:

Cấu hình và kiểm tra hoạt động của giao thức định tuyến OSPF trên router với các bước cơ bản sau:

1. Đặt hostname cho các router và kích hoạt các interface cần được sử dụng.
2. Cấu hình OSPF trên các router.
3. Chọn các mạng được kết nối trực tiếp với nhau.
4. Xem xét bảng định tuyến.
5. Xem thông tin về giao thức OSPF.

B. Chuẩn bị cho bài lab:

Sử dụng các Router1, 2 và 4 có các interface được kết nối như sau:



C. Các bước thực hiện:

1. Sau khi cấu hình địa chỉ IP cho các interface của các router như mô hình trên và xác nhận rằng các router được nối trực tiếp với nhau có thể ping thành công tới nhau, tức là R1 có thể ping tới cổng Fa0/0 của R2 và cổng Se2/0 của R4.

2. Tiếp đến ta sẽ cấu hình OSPF làm giao thức định tuyến trên các router. Điều này rất dễ thực hiện, đầu tiên ta cần vào Configuration mode trên R1. Sau đó chạy lệnh sau:

```
#router ospf 100
```

(với 100 là Process ID)

```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ospf 100
R1(config-router)#
```

3. Thêm vào địa chỉ mạng của các mạng đang được kết nối trực tiếp với R1 sử dụng lệnh sau:

```
R1(config-router)#
R1(config-router)#network 10.1.1.0 0.0.0.255 area 0
R1(config-router)#network 172.16.0.0 0.0.255.255 area 0
R1(config-router)#exit
```

4. Giờ vào Configuration mode của R2, sau đó chọn OSPF làm giao thức định tuyến và thêm vào (các) mạng được kết nối trực tiếp với R2 bằng cách thực hiện tuần tự các lệnh sau:

```
R2>en
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router ospf 100
R2(config-router)#network 10.1.1.0 0.0.0.255 area 0
R2(config-router)#exit
R2(config)#
```

5. Tương tự, ta vào Configuration mode của R4, sau đó chọn OSPF làm giao thức định tuyến và thêm vào (các) mạng được kết nối trực tiếp với R4 bằng cách thực hiện tuần tự các lệnh sau

```
R4>en
R4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#router ospf 100
R4(config-router)#network 172.16.0.0 0.0.255.255 area 0
R4(config-router)#
```

6. Hiện tại thì OSPF đang chạy trên cả 3 router. Nhấn <Ctr>l + Z để thoát khỏi Privileged mode và kiểm tra xem ta giữa các router không được kết nối trực tiếp có thể ping thành công tới nhau hay không. Từ R2 thử ping tới cổng Se2/0 của R4 có IP là 172.16.10.2

```
R2#ping 172.16.10.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/9 ms

R2#
```

7. Kế đến kết nối vào R4 và thử ping tới cổng Fa0/0 của R2 với IP là 10.1.1.2

```
R4#ping 10.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/7/9 ms
```

8. Nếu kết quả của 2 lệnh ping trên thành công thì ta đã hoàn thành xong cấu hình định tuyến sử dụng OSPF cho các router. Giờ xem qua bảng định tuyến trên R2 với lệnh sau

```
R2>en
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0
O    172.16.0.0/16 [110/782] via 10.1.1.1, 00:42:46, FastEthernet0/0
R2#
```

9. Trên R1, để biết thông tin về giao thức định tuyến mà router đang sử dụng, ta chạy lệnh sau

```
R1#show ip protocols

Routing Protocol is "ospf 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.16.10.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.1.1.0 0.0.0.255 area 0
    172.16.0.0 0.0.255.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.1.1.2              110      00:16:00
    172.16.10.2           110      00:16:00
  Distance: (default is 110)

R1#
```

10. Lệnh sau sẽ hiển thị nội dung cơ sở dữ liệu của OSPF

```
R1#show ip ospf database
            OSPF Router with ID (172.16.10.1) (Process ID 100)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
172.16.10.1     172.16.10.1     1099        0x80000005 0x00feff 3
10.1.1.2        10.1.1.2        1188        0x80000003 0x00feff 1
172.16.10.2     172.16.10.2     1100        0x80000003 0x00feff 2

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
10.1.1.1        172.16.10.1     1188        0x80000002 0x00ff77
R1#
```

11. Để hiển thị tất cả các router kế cận với R1, gõ lệnh sau

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.1.2          1   FULL/BDR        00:00:34    10.1.1.2        FastEthernet0/
0
172.16.10.2       0   FULL/  -        00:00:39    172.16.10.2     Serial2/0
R1#
```

12. Cuối cùng, để hiển thị tất cả các interface của router đang sử dụng OSPF, ta chạy lệnh sau:

```
R1#
R1#show ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 10.1.1.1/24, Area 0
  Process ID 100, Router ID 172.16.10.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.10.1, Interface address 10.1.1.1
  Backup Designated Router (ID) 10.1.1.2, Interface address 10.1.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.1.2  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
Serial2/0 is up, line protocol is up
  Internet address is 172.16.10.1/16, Area 0
  Process ID 100, Router ID 172.16.10.1, Network Type POINT-TO-POINT, Cost: 781
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
```

-- Hết --