**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA CÔNG NGHỆ THÔNG TIN 1**

*****

# BÀI THỰC HÀNH CHƯƠNG 5

# HỌC PHẦN:
# MẠNG MÁY TÍNH

**Hà Nội - 2017**

# MỤC LỤC

# BÀI THỰC HÀNH CHƯƠNG 5

## 1. Bài thực hành số 1

Tên bài: Cấu hình switch, VLAN, NAT
- Cấu hình mạng không dây

### ❖ Chuẩn bị:

Sử dụng một máy tính chạy hệ điều hành Windows có kết nối mạng internet hoặc LAN làm môi trường thực hành. Phần mềm PacketTracer.

### ❖ Các bước thực hiện:

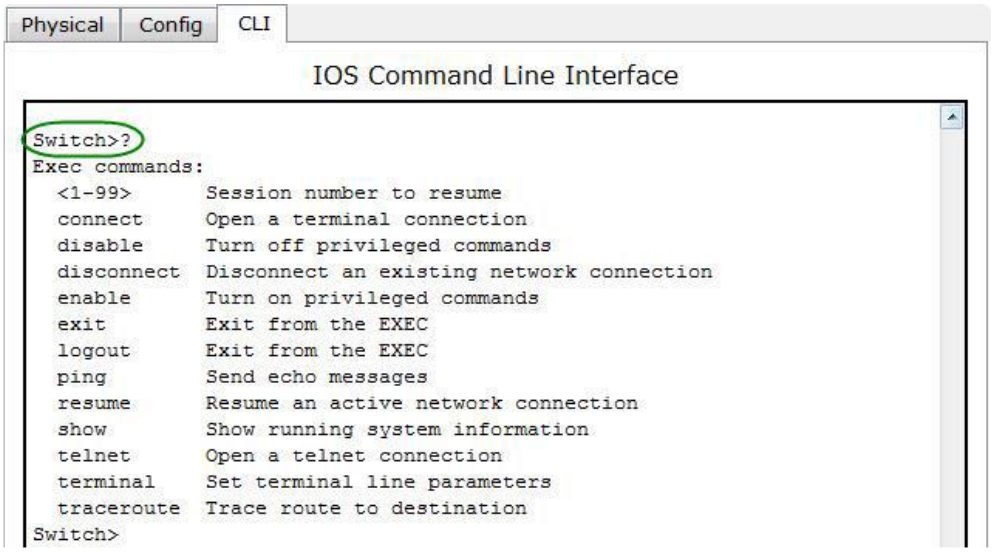
**a) Cấu hình Switch cơ bản với PacketTracert – Giới thiệu các câu lệnh**

Các bước thực hiện trong PacketTracer:

Sử dụng thiết bị switch có tên Switch1.

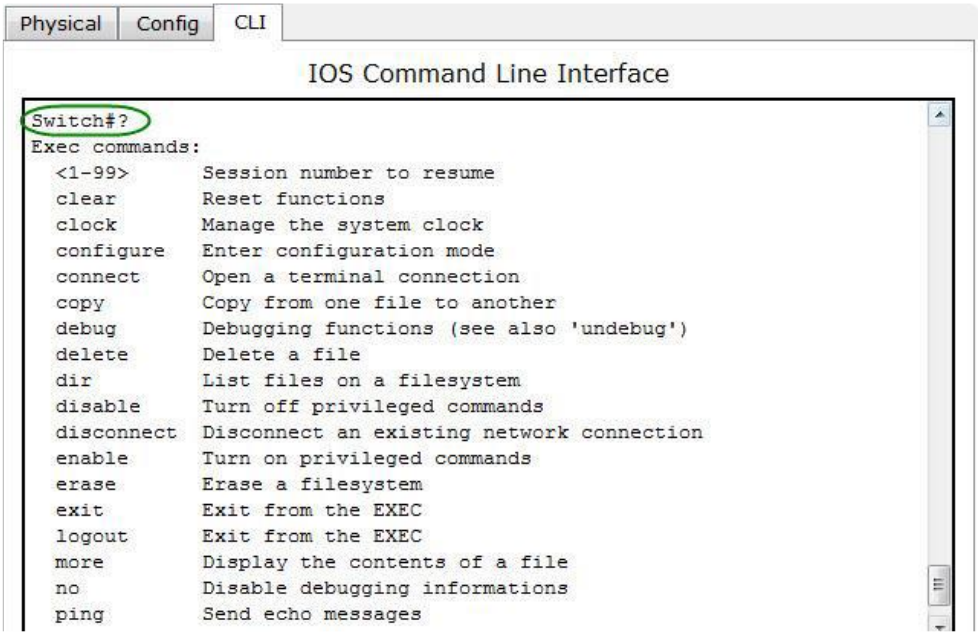
1. Khi truy cập vào Switch1, ta sẽ bắt đầu tại dấu nhắc lệnh cơ bản (đại diện bởi ký tự >), tức user mode

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 (?)



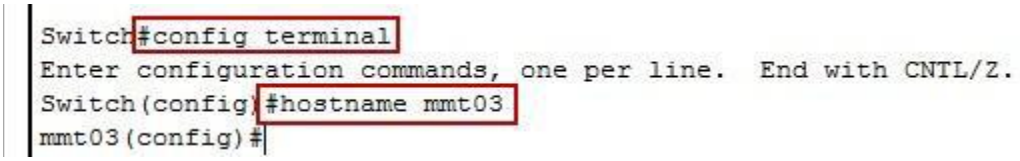
3. Giờ muốn vào Privilege mode (đại diện bởi ký tự #) - chế độ cho phép ta toàn quyền kiểm soát thiết bị thì sử dụng lệnh enable

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




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.

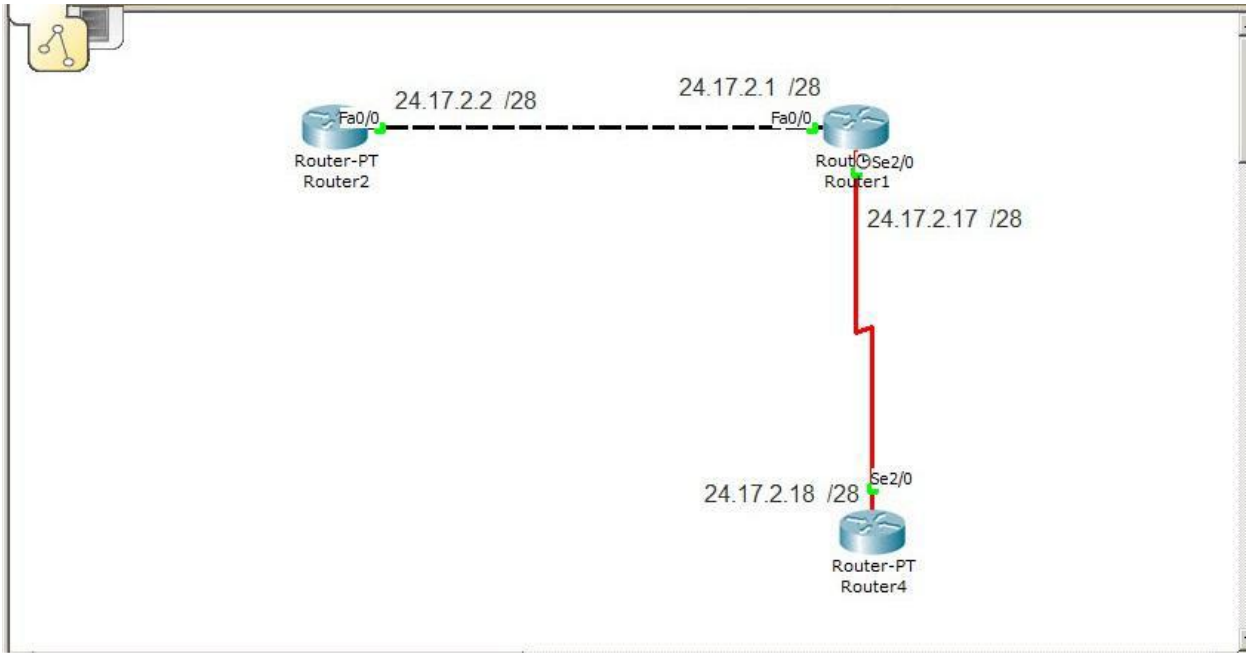
```
mmt03>en
Password: Nhập mật khẩu là cisco
```

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

**b) Cấu hình Switch cơ bản với PacketTracert - Danh sách kiểm soát truy cập chuẩn**

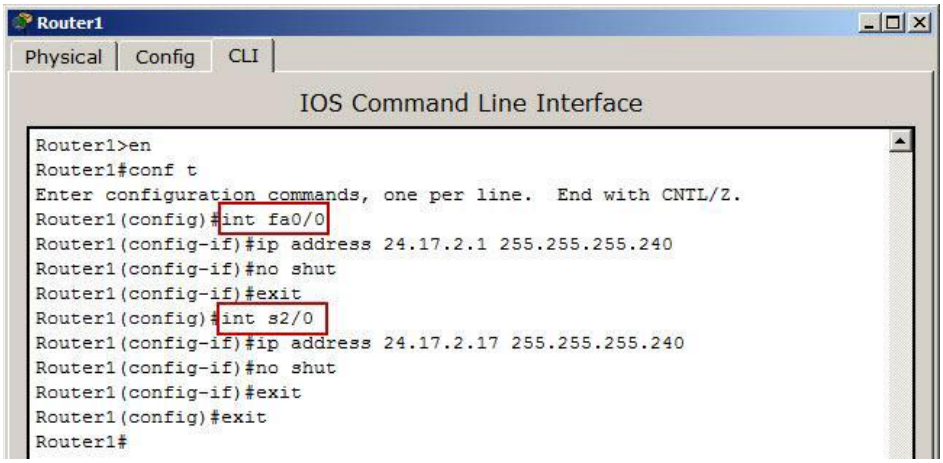
Tìm hiểu và thực hành cấu hình các danh sách kiểm soát truy cập chuẩn (Standard ACL).

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:

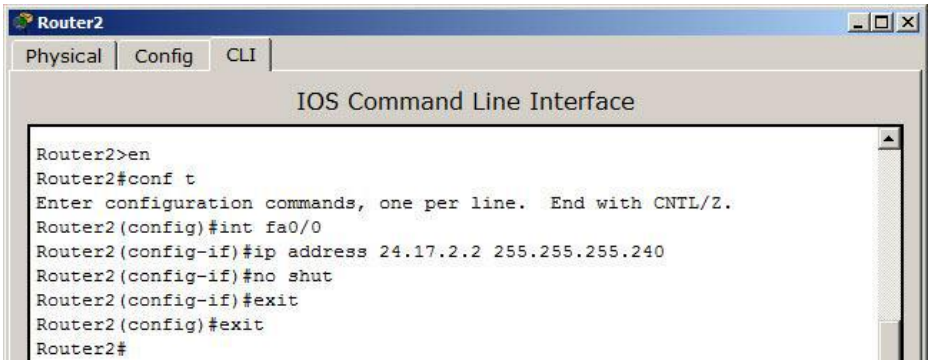



Các bước thực hiện trong PacketTracer:

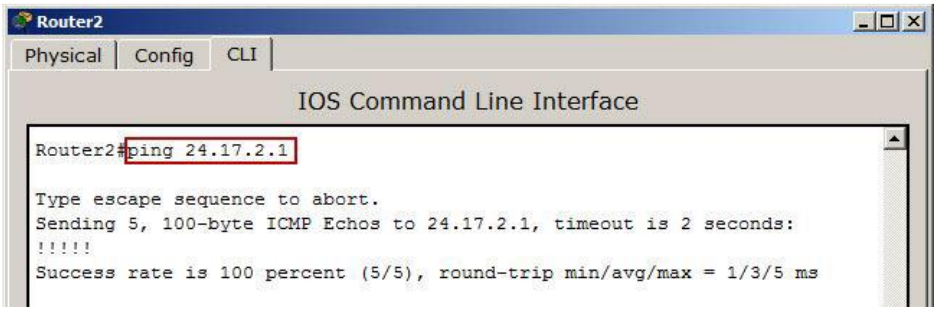
1. Trên Router1, đặt địa chỉ IP cho các cổng Fa0/0 và Ser2/0 như sau:



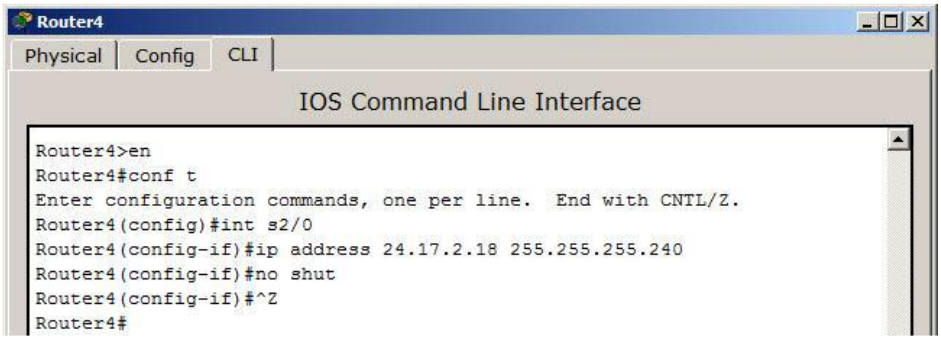

2. Trên Router2, đặt địa chỉ IP cho cổng Fa0/0 như sau:



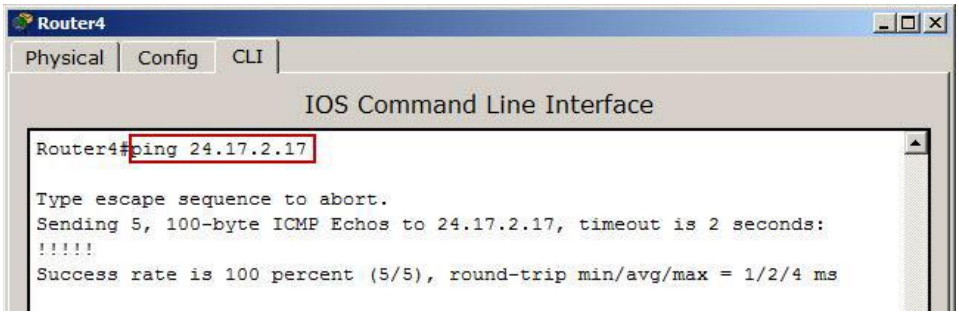

3. Từ Router2, ping tới địa chỉ IP của cổng Fa0/0 của Router1



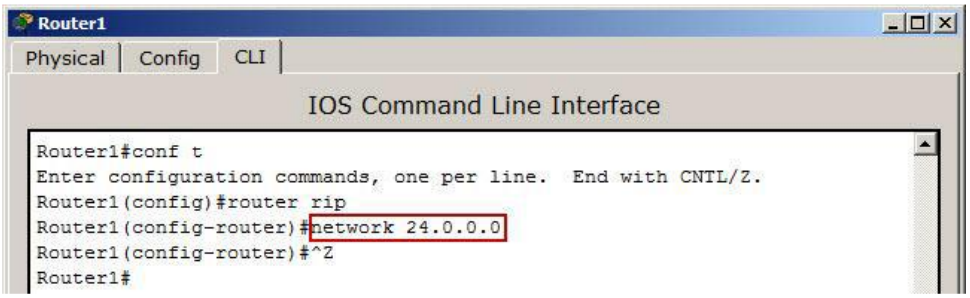

4. Trên Router4, đặt địa chỉ IP cho cổng Ser2/0 như sau:



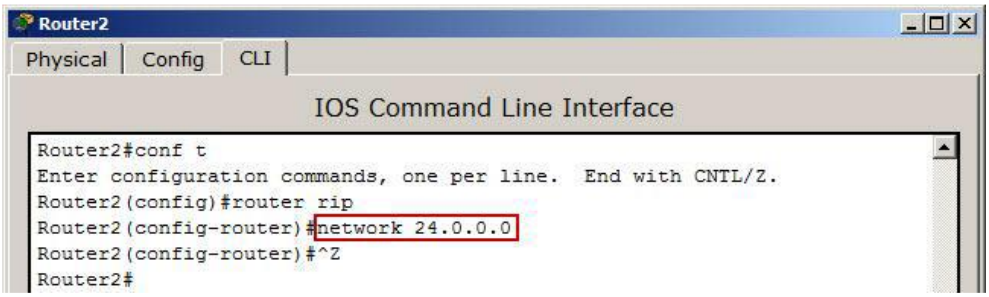

Sau đó ping thử tới địa chỉa IP của cổng Ser2/0 của Router1



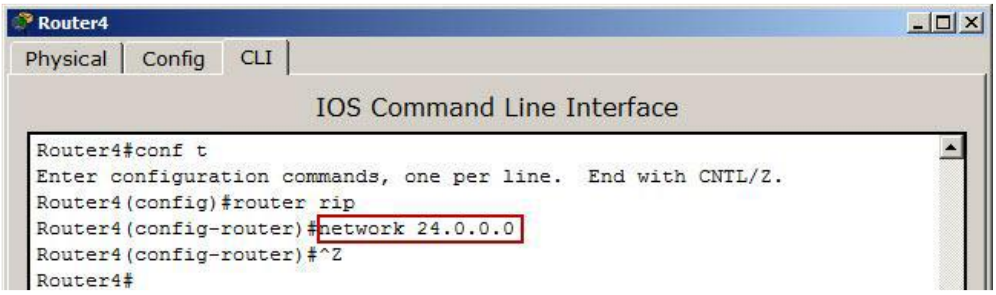

5. Cấu hình RIP cho Router1 và thêm network dành cho các cổng Fa0/0 và Ser2/0



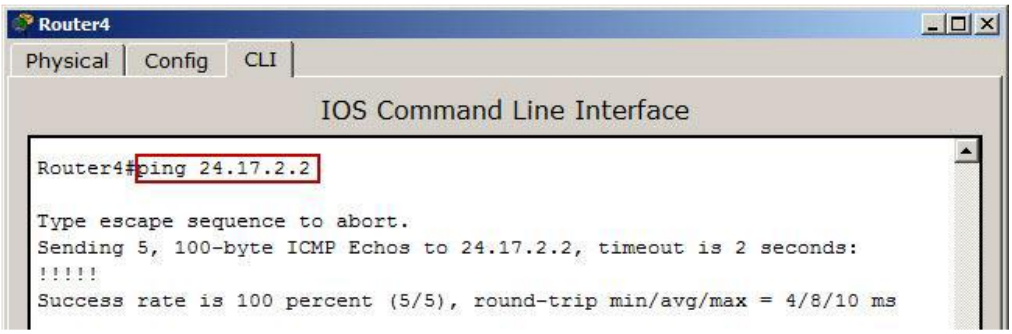

6. Cấu hình RIP cho Router2 và thêm network dành cho cổng Fa0/0



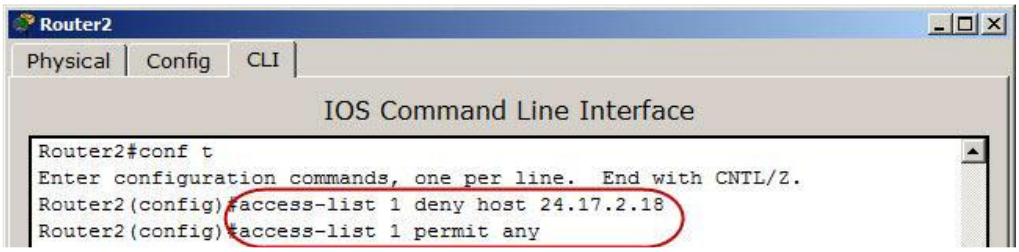

7. Cấu hình RIP cho Router4 và thêm network dành cho cổng Ser2/0




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:

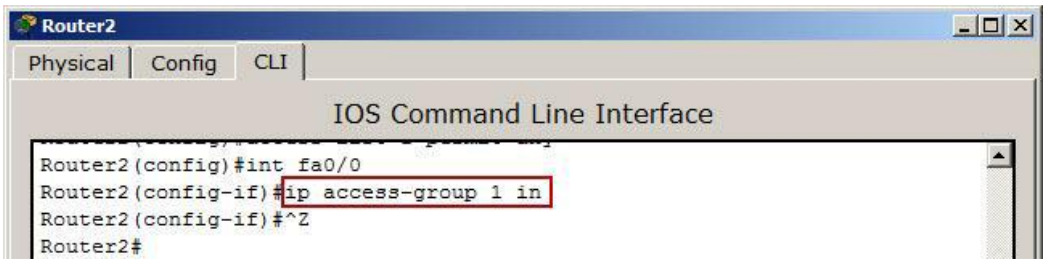
# access-list 1 deny 24.17.2.18 0.0.0.0

và

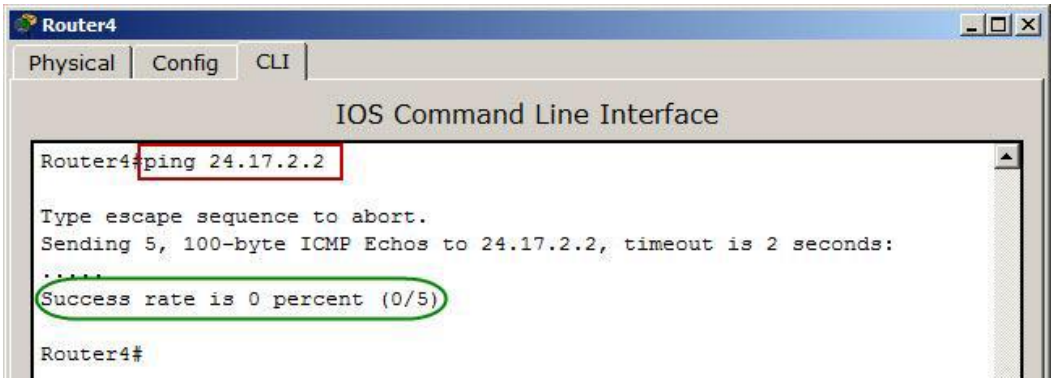
# access-list 1 deny 24.17.2.18

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.

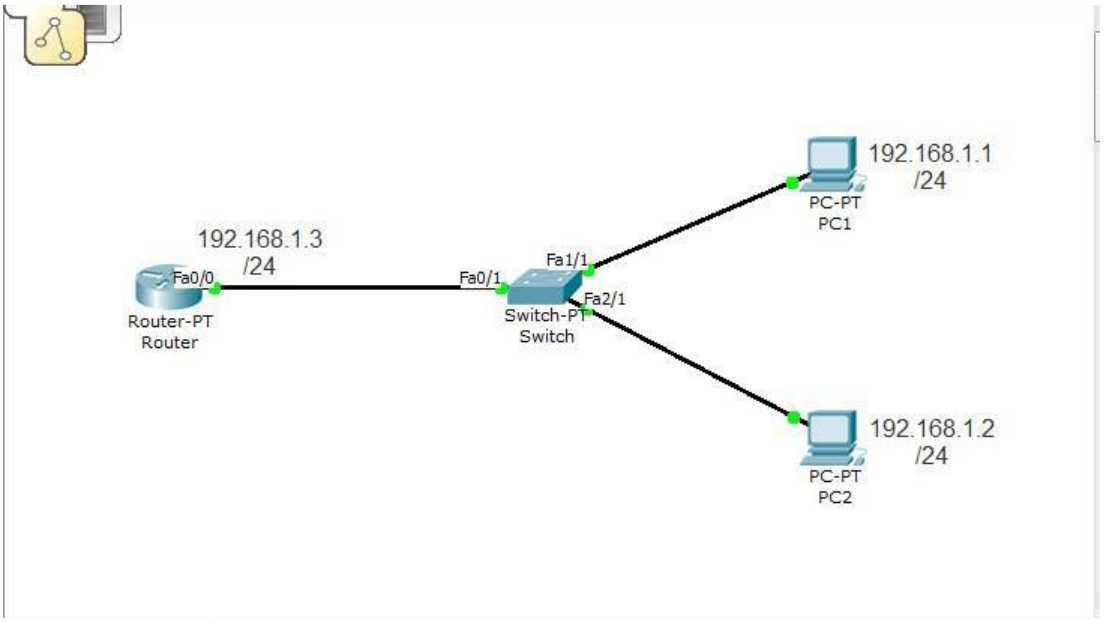



**c) Cấu hình VLAN – Giới thiệu**

Tìm hiểu và thực hành cấu hình VLAN

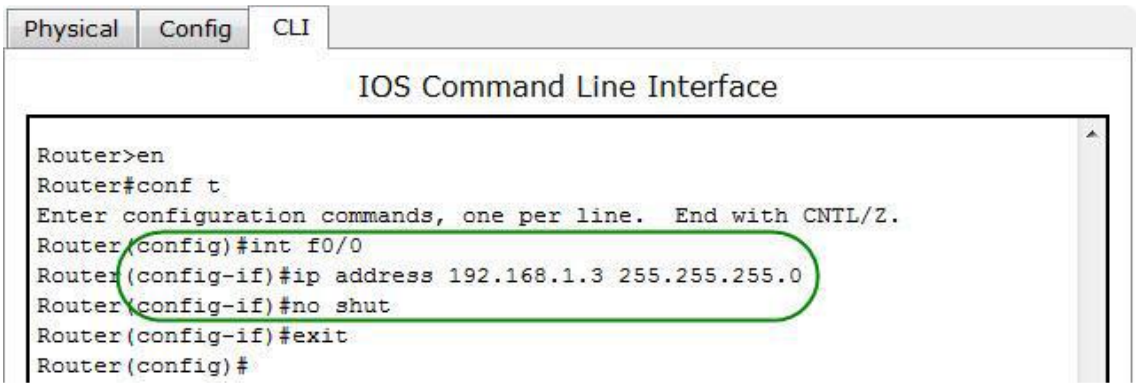
Sử dụng Router, Switch và PC1, PC2 được kết nối và cấu hình IP như hình sau.

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.

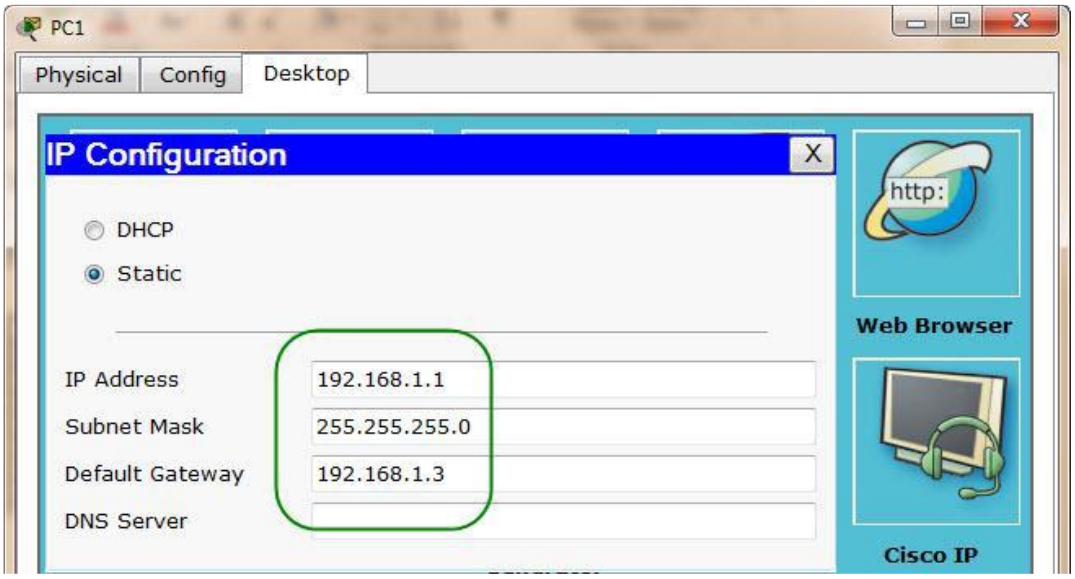



Các bước thực hiện trong PacketTracer:

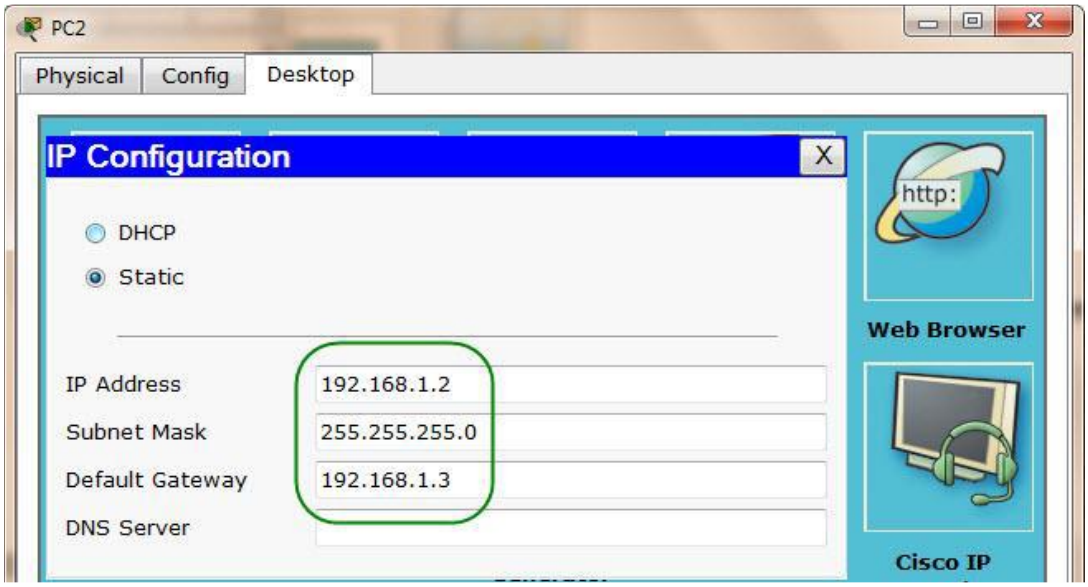
1. Bắt đầu bằng việc cấu hình địa chỉ IP cho cổng Fa0/0 của Router như sau.



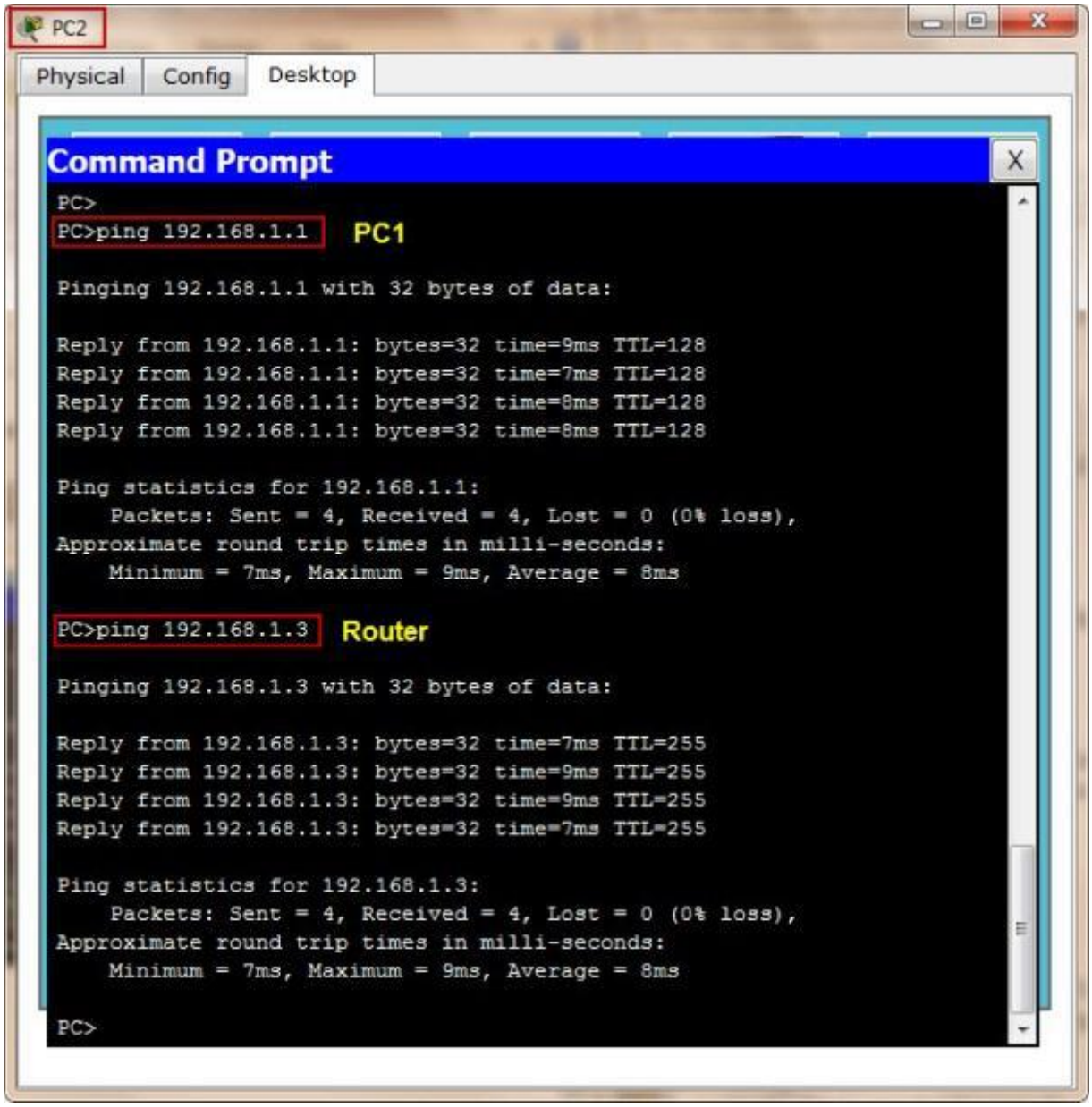

2. Kết nối tới PC1 và đặt IP cho nó như sau



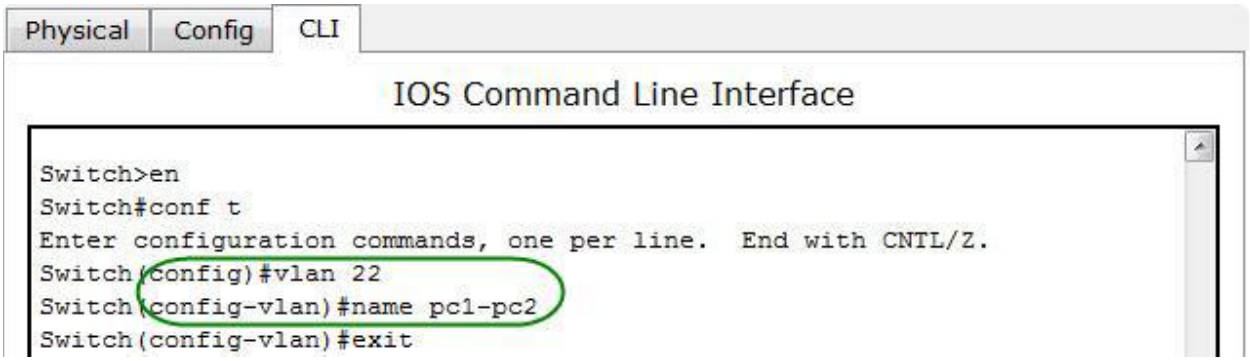

3. Kết nối tới PC2 và đặt IP cho nó như sau




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

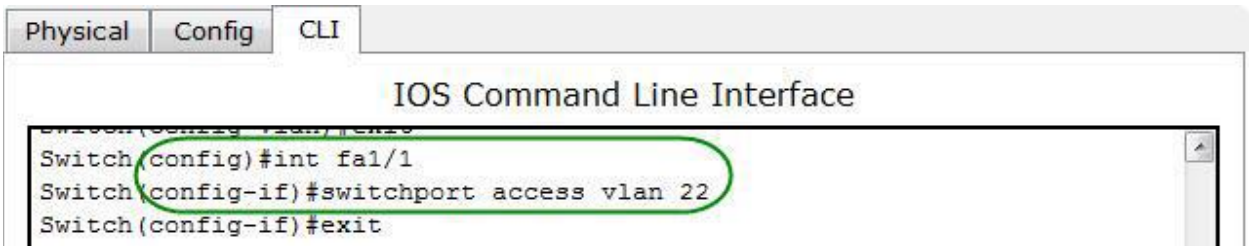



5. Giờ kết nối tới Switch và cấu hình VLAN. Mặc định, thì tất cả các cổng (port) trên switch đều nằm trong cùng VLAN có ID là 1 (VLAN 1). Trong trường hợp này ta sẽ thiết đặt cho port Fa1/1 của switch (hiện đang nối với PC1) vào một VLAN có ID là 22 tách biệt với các port còn lại. Bắt đầu tạo một VLAN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

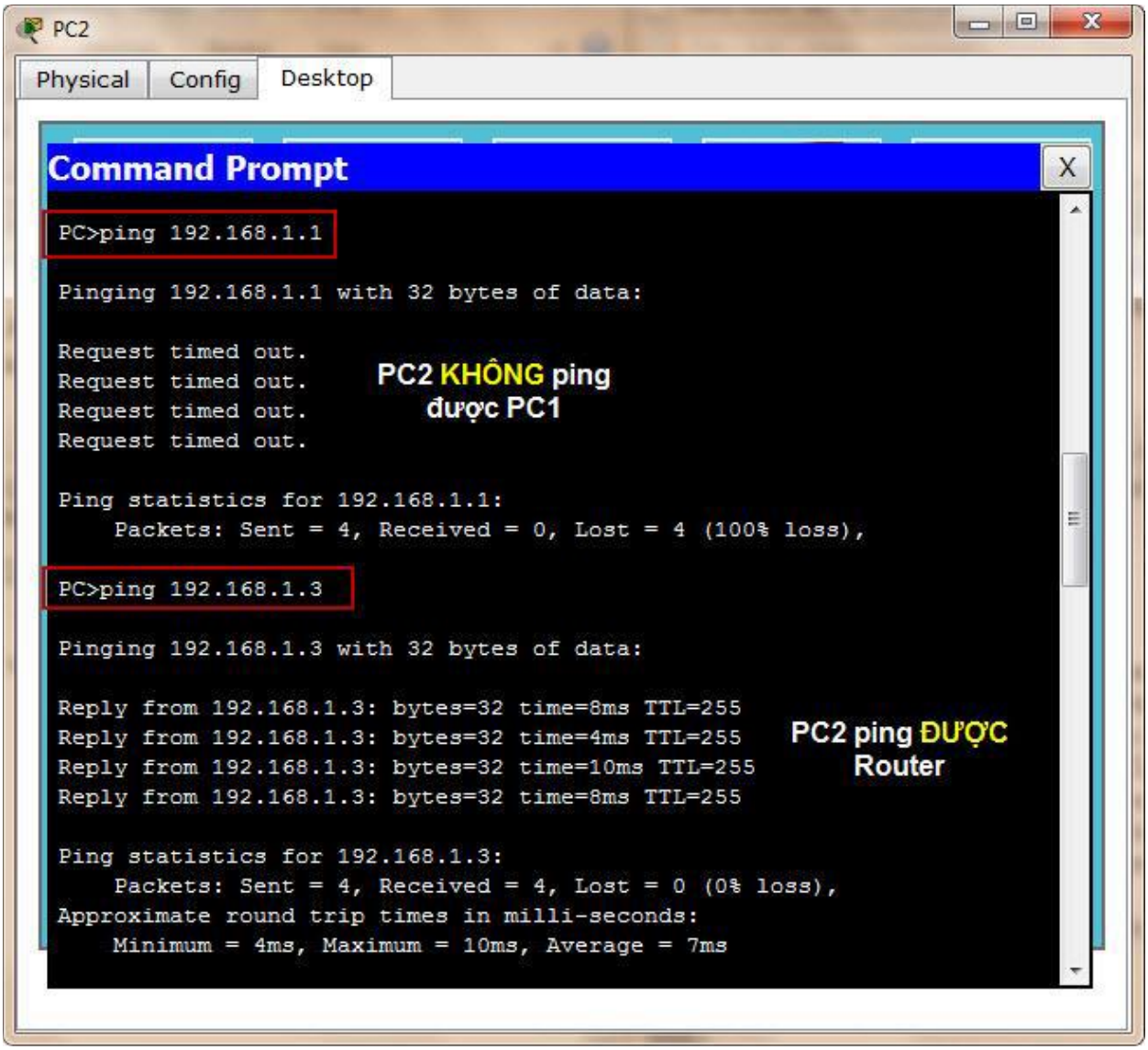



Nếu muốn bạn có thể đặt tên cho VLAN 22 này để giúp nhận dạng và phân biệt dễ dàng hơn giữa các VLAN, như trong hình trên ta đặt là pc1-pc2.

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.



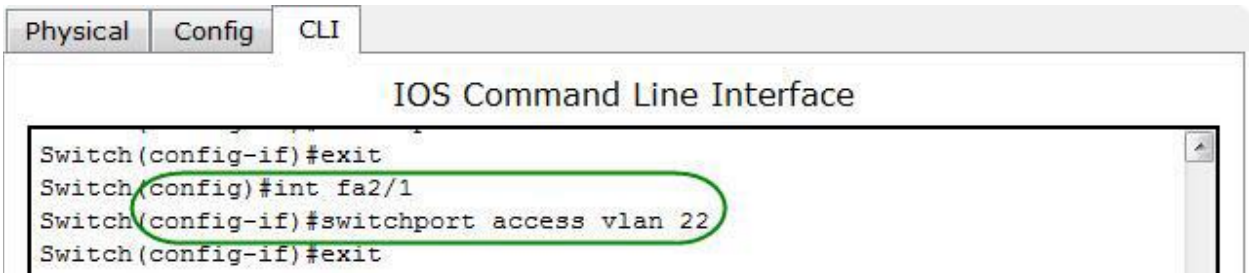

7. Tiếp đến ta kết nối lại vào PC2 và thử ping tới PC1 và Router thì kết quả như sau:



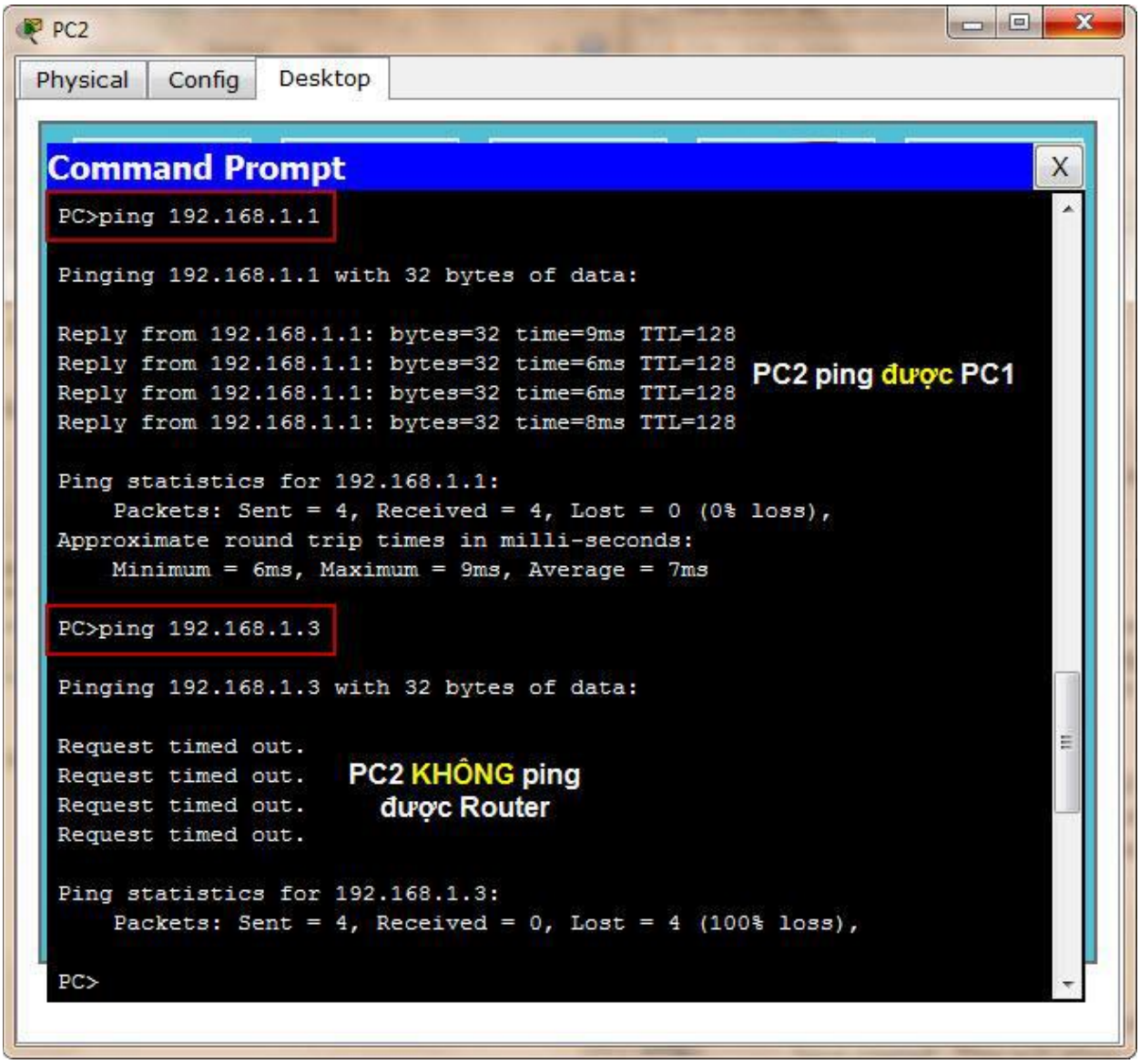

Như hình trên ta thấy, PC2 có thể ping tới Router nhưng PC1 không thể ping được PC1. Tại sao lại như vậy?

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

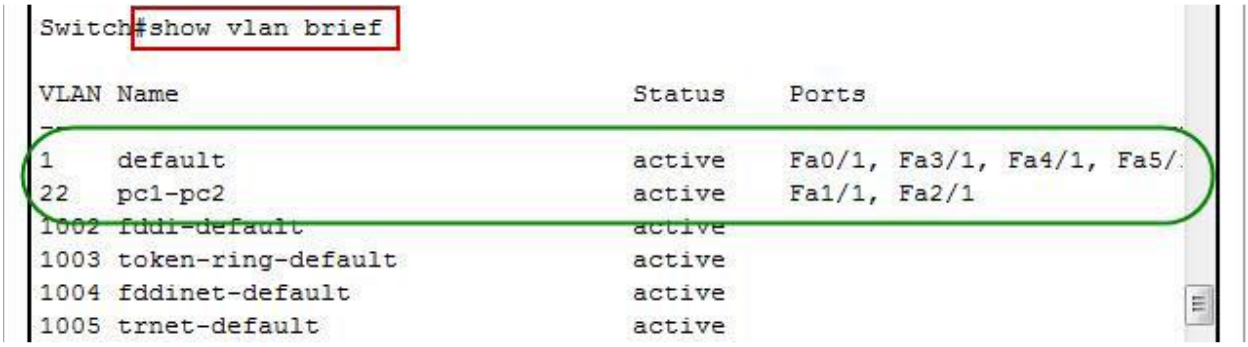



9. Giờ kết nối lại với PC2 và thử ping lại tới Router và PC1



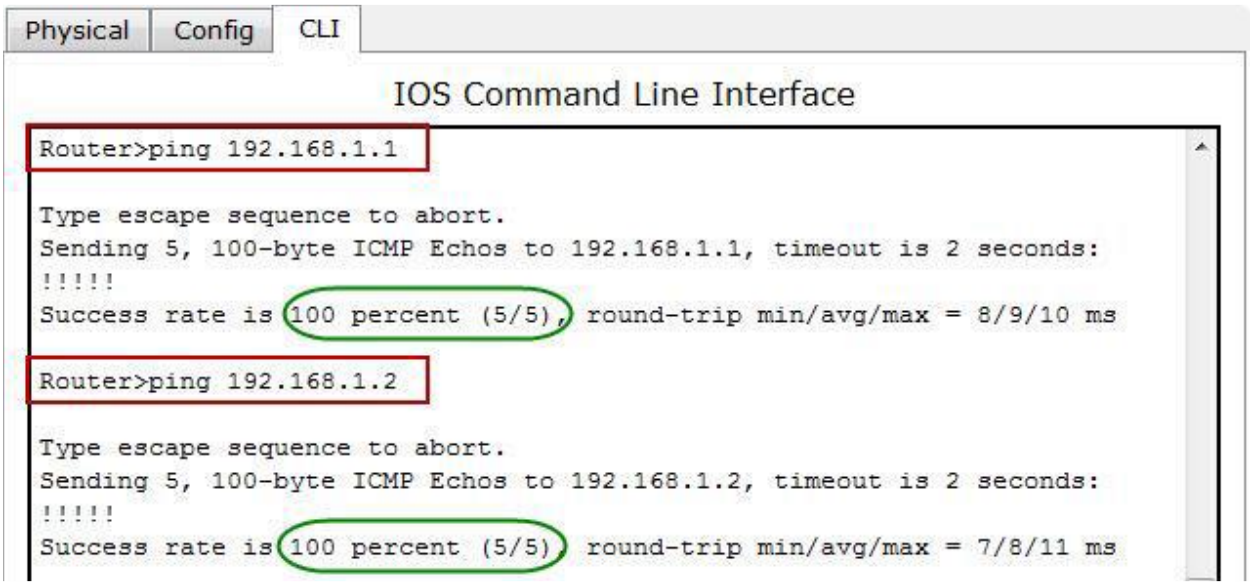
Sự khác lạ ở đây là gì? Hiện PC2 đã có thể ping tới PC1 nhưng vẫn không thể ping tới Router. Lý do là vì lúc này gói tin ping từ PC2 được đánh dấu là VLAN 22, tức là nó chỉ có thể đi ra khỏi port Fa0/1 đang được nối với PC1 và cũng thuộc VLAN 22. Đây cũng chính là mục đích của bài lab mà ta muốn thực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

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




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.


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




**d) Cấu hình VLAN – Trunking protocol**

Mục tiêu bao gồm:

- 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.

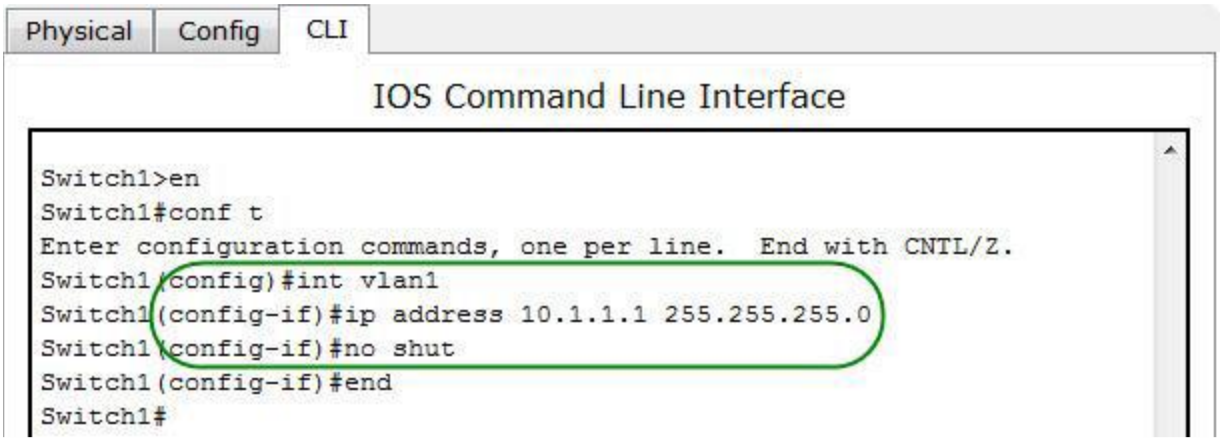
- Tạo một đường trunk giữa 2 switch để làm kênh truyền dẫn giúp đồng bộ thông tin về VLAN giữa các switch.

- Kiểm tra cấu hình của VLAN và VTP.

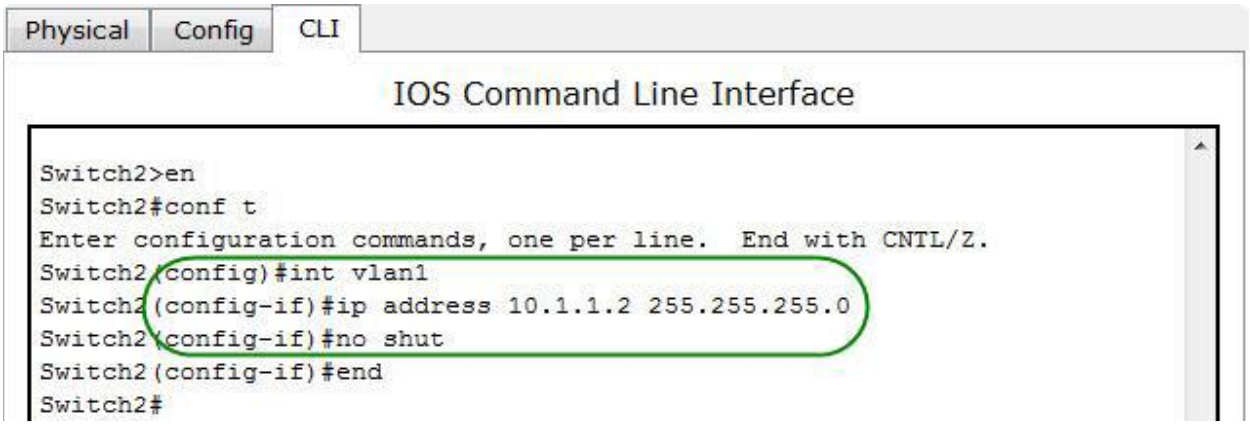
Trong Packet Tracer, sử dụng 2 switch 2950-24 và chúng được kết nối như sau


**Các bước thực hiện:**

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

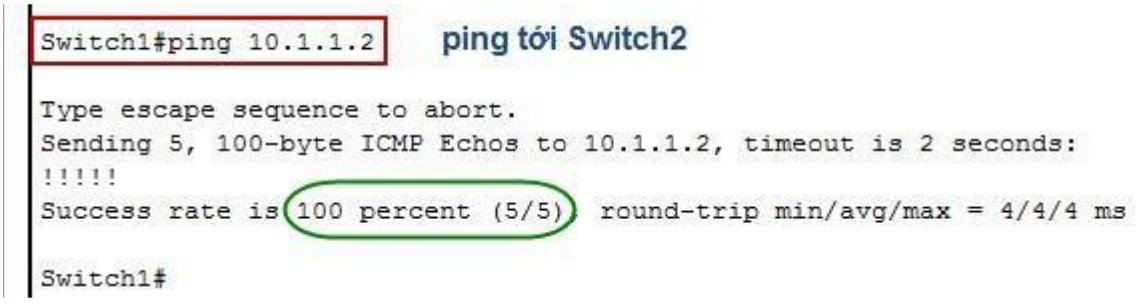



2. Đặt địa chỉ IP cho interface VLAN1 của Switch2 như sau




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

Từ Switch1 ping tới Switch2




Từ Switch2 ping tới Switch1

```
Switch2#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 = 4/4/4 ms

Switch2#
```

ping tới Switch1

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#
```

**e) Cấu hình NAT**

Mục tiêu: cung cấp những thông tin và các câu lệnh có liên quan đến những chủ đề sau:

- Địa chỉ IP Private: RFC 1918

- Cấu hình NAT động: Một địa chỉ IP Private chuyển đổi sang một địa chỉ IP Public

- Cấu hình Port Address Translation (PAT): Nhiều địa chỉ IP Private được chuyển đổi sang một địa chỉ IP Public

- Cấu hình Static NAT: Một địa chỉ IP Private được chuyển đổi cố định sang một địa chỉ IP Public

- Kiểm tra cấu hình NAT và PAT

- Xử lý lỗi với cấu hình NAT và PAT

- Cấu hình ví dụ: PAT

1. Địa chỉ IP Private: RFC 1918

- Bảng bên dưới sẽ hiển thị danh sách dải địa chỉ được chỉ định trong cuốn RFC 1918 được sử dụng bởi các quản trị mạng như một địa chỉ IP Private. Những địa chỉ IP này sẽ là những địa chỉ được gán cho các thiết bị nằm trong mạng LAN và được chuyển đổi thành địa chỉ IP Public để có thể được định tuyến trên Internet. Rất nhiều mạng có thể được cho phép để sử dụng những địa chỉ IP này; tuy nhiên, những địa chỉ này không được phép định tuyến trên Internet.

| **Private Addresses** | | |
|---|---|---|
| **Class** | **RFC 1918 Internal Address Range** | **CIDR Prefix** |
| **A** | 10.0.0.0–10.255.255.255 | 10.0.0.0/8 |
| **B** | 172.16.0.0–172.31.255.255 | 172.16.0.0/12 |
| **C** | 192.168.0.0–192.168.255.255 | 192.168.0.0/16 |

2. Cấu hình NAT động: Một địa chỉ IP Private chuyển đổi sang một địa chỉ IP Public

* Chú ý: Để hoàn thành việc cấu hình NAT/PAT với sự trợ giúp của sơ đồ bên dưới, các bạn có thể nhìn vào ví dụ đơn giản ở cuối chương này.

Các bước như sau:

Bước 1: Định nghĩa một static route trên một router remote, ở đó địa chỉ IP Public của bạn đã được định tuyến

ISP(config)#ip route 64.64.64.64 255.255.255.128 s0/0/0

Thông báo cho router của ISP, nơi mà bạn sẽ gửi các gói tin với địa chỉ đích là 64.64.64.64 255.255.255.128.

Bước 2: Định nghĩa một dải địa chỉ IP Public sẽ được sử dụng trên router của bạn để thực thi NAT

Địa chỉ IP Private sẽ nhận địa chỉ IP Public đầu tiên của dải đã được bạn định nghĩa để chuyển đổi.

Corp(config)#ip nat pool scott 64.64.64.70 64.64.64.126 netmask 255.255.255.128

Định nghĩa tên cho dải địa chỉ IP Public là scott. Địa chỉ IP đầu tiên của dải đó là: 64.64.64.70. Địa chỉ IP cuối cùng của dải đó là: 64.64.64.126. Subnet mask của dải đó là: 255.255.255.128.

Bước 3: Tạo một ACL sẽ được dùng để cho phép những địa chỉ IP Private nào sẽ được phép chuyển đổi.

Corp(config)#access-list 1 permit 172.16.10.0 0.0.0.255

Bước 4 : Tạo mối quan hệ giữa ACL với dải địa chỉ IP Public đã tạo Bước 2.

Corp(config)#ip nat inside source list 1 pool scott

Bước 5 : Định nghĩa các interface đóng vai trò là interface inside (sẽ là những interface kết nối vào mạng LAN)

Router(config)#interface fastethernet 0/0

Chuyển cấu hình vào chế độ Interface fa0/0

Router(config-if)#ip nat inside

Bạn có thể có nhiều hơn một interface inside trên một router. Những địa chỉ của mỗi một interface inside sau đó cũng sẽ được chuyển đổi thành địa chỉ IP Public.

Router(config-if)#exit

Trở về chế độ cấu hình Global Configuration.

Bước 6 : Định nghĩa ra interface với vai trò là interface outside (interface sẽ được dùng để để kết nối ra ngoài mạng Interface hoặc WAN)

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

Router(config-if)#ip nat outside

3. Cấu hình PAT : Nhiều địa chỉ IP Private được chuyển đổi sang một địa chỉ IP Public

- Tất cả các địa chỉ IP Private sẽ sử dụng duy nhất một địa chỉ IP Public và các chỉ số port sẽ được dùng cho quá trình chuyển đổi.

Bước 1: Định nghĩa một static route trên một router remote, ở đó địa chỉ IP Public của bạn đã được định tuyến

ISP(config)#ip route 64.64.64.64 255.255.255.128 s0/0/0

Thông báo cho router của ISP, nơi mà bạn sẽ gửi các gói tin với địa chỉ đích là 64.64.64.64 255.255.255.128.

Bước 2: Định nghĩa một dải địa chỉ IP Public sẽ được sử dụng trên router của bạn để thực thi NAT

Sử dụng bước này nếu bạn có nhiều địa chỉ IP Private để chuyển đổi. Một địa chỉ IP Public có thể điều khiển hàng ngàn địa chỉ IP Private. Không sử dụng một dải địa chỉ, bạn có thể chuyển đổi tất cả các địa chỉ IP Private thành một địa chỉ IP đã tồn tại trên interface được dùng để kết nối đến ISP.

Corp(config)#ip nat pool scott 64.64.64.70 64.64.64.70 netmask 255.255.255.128

Định nghĩa tên cho dải địa chỉ IP Public là scott.

Địa chỉ IP đầu tiên của dải đó là: 64.64.64.70

Địa chỉ IP cuối cùng của dải đó là: 64.64.64.7

Subnet mask của dải đó là: 255.255.255.128.

Bước 3: Tạo một ACL sẽ được dùng để cho phép những địa chỉ IP Private nào sẽ được phép chuyển đổi.

Corp(config)#access-list 1 permit 172.16.10.0 0.0.0.255

Bước 4 : Tạo mối quan hệ giữa ACL với dải địa chỉ IP Public đã tạo Bước 2

Corp(config)#ip nat inside source list 1 pool scott

Bước 5 : Định nghĩa các interface đóng vai trò là interface inside (sẽ là những interface kết nối vào mạng LAN)

Router(config)#interface fastethernet 0/0

Chuyển cấu hình vào chế độ Interface fa0/0

Router(config-if)#ip nat inside

Bạn có thể có nhiều hơn một interface inside trên một router. Những địa chỉ của mỗi một interface inside sau đó cũng sẽ được chuyển đổi thành địa chỉ IP Public.

Router(config-if)#exit

Trở về chế độ cấu hình Global Configuration.

Bước 6 : Định nghĩa ra interface với vai trò là interface outside (interface sẽ được dùng để để kết nối ra ngoài mạng Interface hoặc WAN)

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

Router(config-if)#ip nat outside

* Chú ý: bạn có thể có một dải IP NAT nhiều hơn một địa chỉ IP, nếu cần thiết. Câu lệnh bên dưới có thể là một ví dụ:

Corp(config)#ip nat pool scott 64.64.64.70 74.64.64.128 netmask 255.255.255.128

- Với dải địa chỉ IP trên bạn có tất cả là 63 địa chỉ IP có thể được sử dụng để chuyển đổi.

4. Cấu hình Static NAT: Một địa chỉ IP Private được chuyển đổi cố định sang một địa chỉ IP Public

Bước 1: Định nghĩa một static route trên một router ở xa, ở đó địa chỉ IP Public của bạn đã được định tuyến

ISP(config)#ip route 64.64.64.64 255.255.255.128 s0/0/0

Thông báo cho router của ISP, nơi mà bạn sẽ gửi các gói tin với địa chỉ đích là 64.64.64.64 255.255.255.128.

Bước 2: Tạo một Static mapping trên router của bạn sẽ được sử dụng để thực thi NAT.

Corp(config)#ip nat inside source static 172.16.10.5 64.64.64.65

Thực hiện chuyển đổi cố định địa chỉ IP bên trong 172.16.10.5 thành một địa chỉ IP Public 64.64.64.65.

Bạn sẽ phải sử dụng câu lệnh cho mỗi một địa chỉ IP Private mà bạn muốn ánh xạ tĩnh với một địa chỉ IP Public.

Bước 3: Định nghĩa ra những interface có vai trò là interface inside

Corp(config)#interface fastethernet 0/0

Chuyển cấu hình vào chế độ interface fa0/0.

Corp(config-if)#ip nat inside

Bạn có thể có nhiều hơn một interface inside trên một router.

Bước 4: Định nghĩa những interface với vai trò là interface outside

Corp(config-if)#interface serial 0/0/0

Chuyển cấu hình vào chế độ interface s0/0/0.

Corp(config-if)#ip nat outside

Định nghĩa interface s0/0/0 là interface có vai trò là outside.

5. Kiểm tra cấu hình NAT và PAT

Hiển thị bảng chuyển đổi

Router#show ip nat translations

Hiển thị những thông tin của NAT.

Router#show ip nat statistics

Xóa thông tin chuyển đổi của bảng NAT trước khi thông tin đó bị times out.

Router#clear ip nat translations inside a.b.c.d outside e.f.g.h

Xóa toàn bộ bảng chuyển đổi trước khi thông tin đó bị time oute.

Router#clear ip nat translations*

6. Xử lý lỗi với cấu hình NAT và PAT

Hiển thị thông tin về những gói tin đã được chuyển đổi.

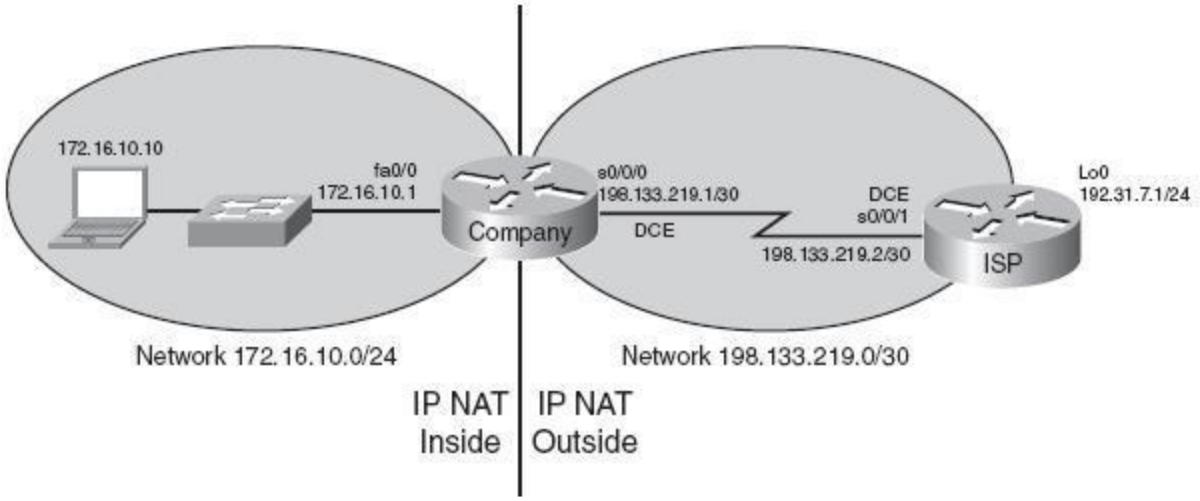
Router#debug ip nat

Hiển thị chi tiết về những gói tin đã được chuyển đổi.

Router#debug ip nat detailed

7. Cấu hình ví dụ: PAT

- Hình dưới là sơ đồ mạng được sử dụng cho việc cấu hình PAT.




**ISP Router**

Chuyển cấu hình vào chế độ Privileged

router>enable

Chuyển cấu hình vào chế độ Global Configuration.

router#configure terminal

Đặt tên cho Router là ISP.

router(config)#host ISP

Tắt tính năng tự động phân giải khi bạn nhập câu lệnh sai.

ISP(config)#no ip domain-lookup

Đặt mật khẩu enable secret là Cisco.

ISP(config)#enable secret cisco

Chuyển cấu hình vào chế độ line console.

ISP(config)#line console 0

Người dùng sẽ phải được yêu cầu nhập thông tin truy cập khi kết nối vào router thông qua port console.

ISP(config-line)#login

Đặt mật khẩu cho truy cập console là class.

ISP(config-line)#password class

Không cho phép ngắt câu lệnh sang dòng mới khi có log hiển thị trên màn hình console.

ISP(config-line)#logging synchronous

Trở về chế độ Global Configuration.

ISP(config-line)#exit

Chuyển cấu hình vào chế độ interface s0/0/1.

ISP(config)#interface serial 0/0/1

Gán địa chỉ IP và subnet mask cho interface s0/0/1

ISP(config-if)#ip address 198.133.219.2 255.255.255.252

Gán giá trị clock rate cho cáp DCE gắn vào interface s0/0/1 của router.

ISP(config-if)#clock rate 56000

Bật interface.

ISP(config-if)#no shutdown

Tạo interface loopback 0 và đồng thời chuyển cấu hình vào chế độ interface loopback 0.

ISP(config-if)#interface loopback 0

Gán địa chỉ IP và Subnet mask cho interface loopback 0.

ISP(config-if)#ip address 192.31.7.1255.255.255.255

Trở về chế độ cấu hình Global Configuration.

ISP(config-if)#exit

Trở về chế độ cấu hình Privileged.

ISP(config)#exit

Lưu file cấu hình đang chạy trên RAM vào NVRAM.

ISP#copy running-config startupconfig

**Company Router**

Chuyển cấu hình vào chế độ privileged.

router>enable

Chuyển cấu hình vào chế độ Global Configuration.

router#configure terminal

Đặt tên cho router là Company.

router(config)#host Company

Tắt tính năng tự động phân giải câu lệnh khi bạn nhập sai.

Company(config)#no ip domain-lookup

Đặt mật khẩu cho enable secret là cisco

Company(config)#enable secret cisco

Chuyển cấu hình vào chế độ line console

Company(config)#line console 0

Yêu cầu người dùng phải nhập thông tin truy cập khi thực hiện kết nối vào router thông qua port console.

Company(config-line)#login

Đặt mật khẩu cho việc truy cập vào router thông qua console là class.

Company(config-line)#password class

Không cho phép ngắt câu lệnh sang dòng mới khi có log hiển thị trên màn hình console.

Company(config-line)#logging Synchronous

Trở về chế độ cấu hình Global Configuration.

Company(config-line)#exit

Chuyển cấu hình vào chế độ interface fa0/0.

Company(config)#interface fastethernet 0/0

Gán địa chỉ IP và subnet mask cho interface.

Company(config-if)#ip address 172.16.10.1 255.255.255.0

Bật interface.

Company(config-if)#no shutdown

Chuyển cấu hình vào chế độ interface s0/0/0.

Company(config-if)#interface serial 0/0/0

Gán địa chỉ IP và subnet mask cho interface s0/0/0

Company(config-if)#ip address 198.133.219.1 255.255.255.252

Bật interface.

Company(config-if)#no shutdown

Trở về chế độ cấu hình Global Configuration.

Company(config-if)#exit

Cấu hình default route static.

Company(config)#ip route 0.0.0.0 0.0.0.0 198.133.219.2

Tạo một ACL để cho phép địa chỉ IP Private có thể được NAT.

Company(config)#access-list 1 permit 172.16.10.0 0.0.0.255

Tạo Nat bằng cách gán list 1 với interface s0/0/0. Phương pháp Overloading sẽ được thực thi.

Company(config)#ip nat inside source list 1 interface serial 0/0/0 overload

Chuyển cấu hình vào chế độ interface fa0/0.

Company(config)#interface fastethernet 0/0

Gán vai trò cho interface fa0/0 là interface inside.

Company(config-if)#ip nat inside

Chuyển cấu hình vào chế độ interface s0/0/0.

Company(config-if)#interface serial 0/0/0

Gán vai trò cho interface s0/0/0 là interface outside.

Company(config-if)#ip nat outside

Trở về chế độ cấu hình Privileged.

Company(config-if)# ctrl –Z

Lưu file cấu hình đang chạy trên RAM vào NVRAM.

Company#copy running-config startup-config

## 2. Bài thực hành số 2

Tên bài: Cấu hình mạng không dây

### ❖ Chuẩn bị:

Sử dụng một máy tính chạy hệ điều hành Windows có kết nối mạng internet hoặc LAN làm môi trường thực hành. Phần mềm PacketTracer.

### ❖ Các bước thực hiện:

Topo mạng được mô tả như sau:


Có 3 PC kết nối với router không dây Linksys.

Ta cần cấu hình IP tĩnh trên PC và Router không dây. Đặt sẵn IP của router là 192.168.0.1.

Đặt SSID là MotherNetwork

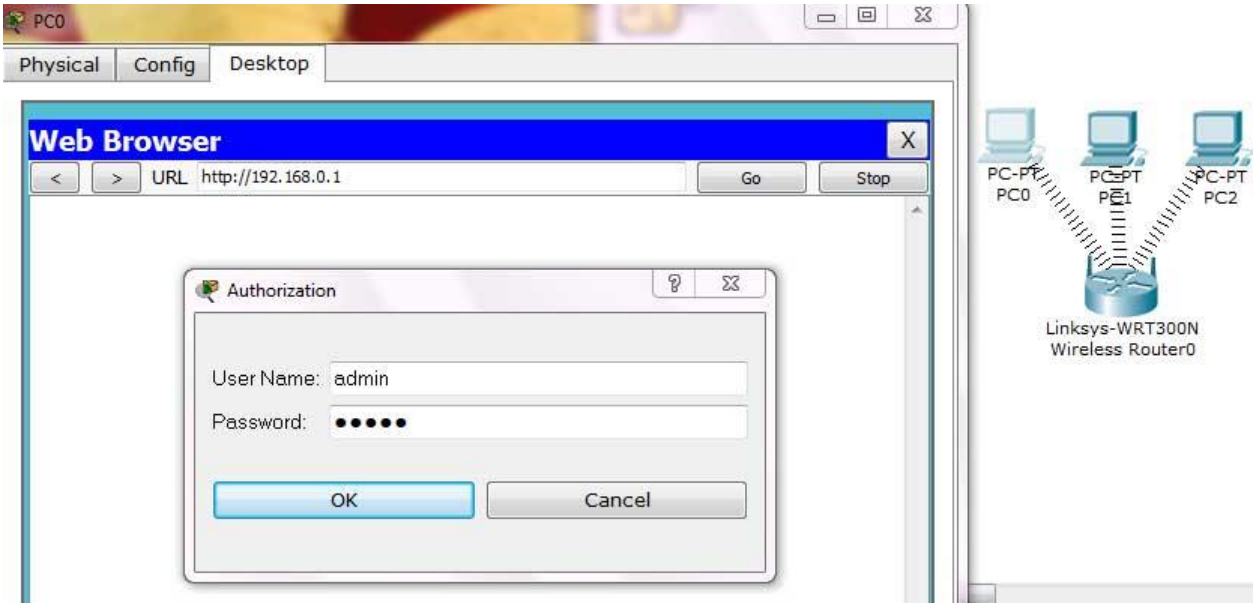
Đổi IP address của router thành 10.0.0.1 và 10.0.0.2 cho PC0, 10.0.0.3 cho PC1, 10.0.0.4 cho PC2

Cấu hình WAP key trên Router

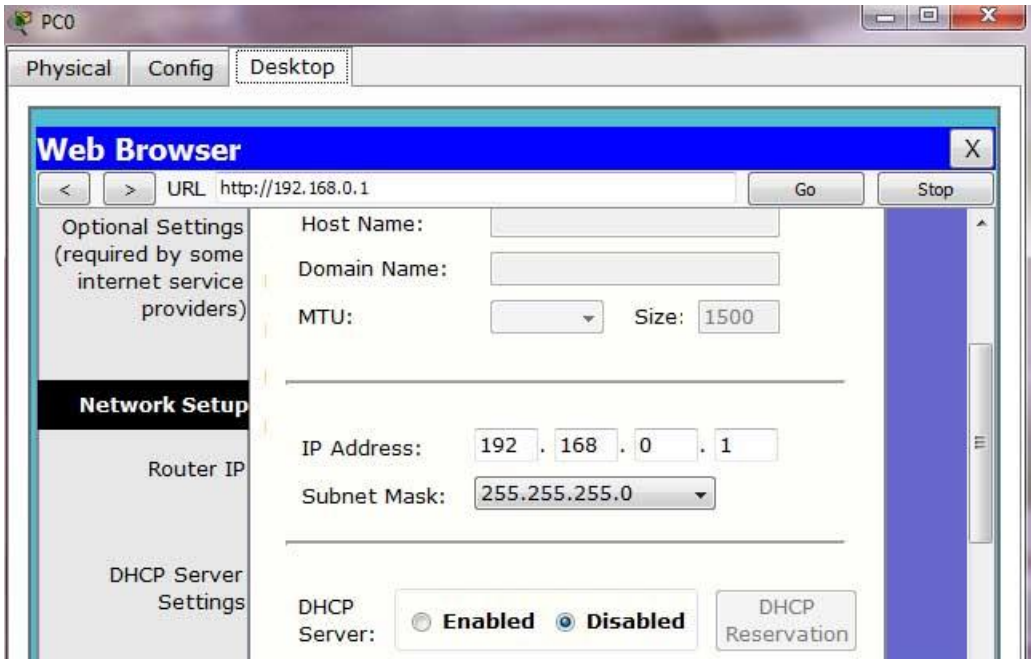
Kết nối mạng cho PC sử dụng WAP key

**Bắt đầu thực hiện như sau:**

Bấm đúp vào PC và chọn Web Browser. Gõ IP là 192.168.0.1 và điền username là admin và Password là admin

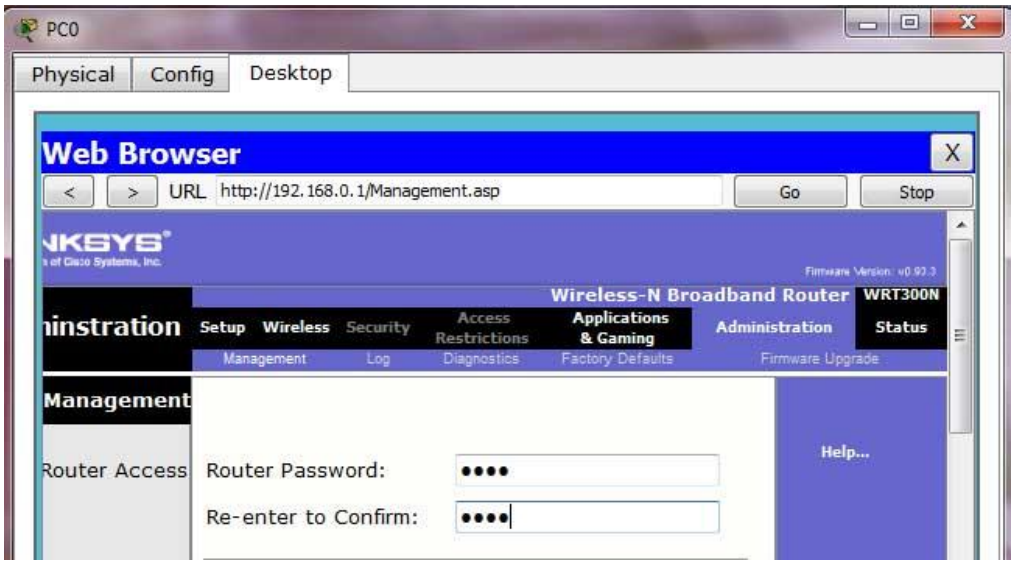



Chọn Disable DHCP

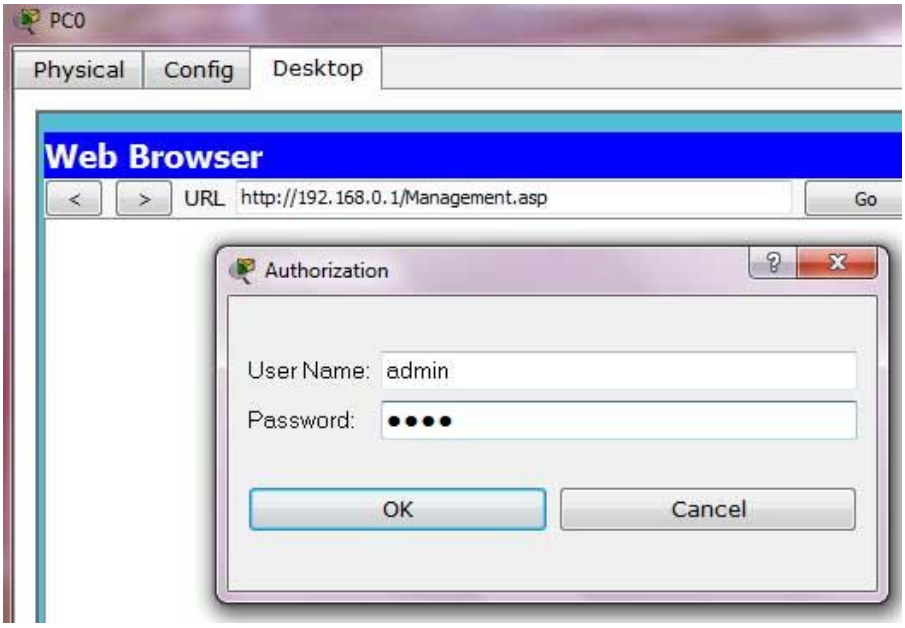



Rồi bấm Save.

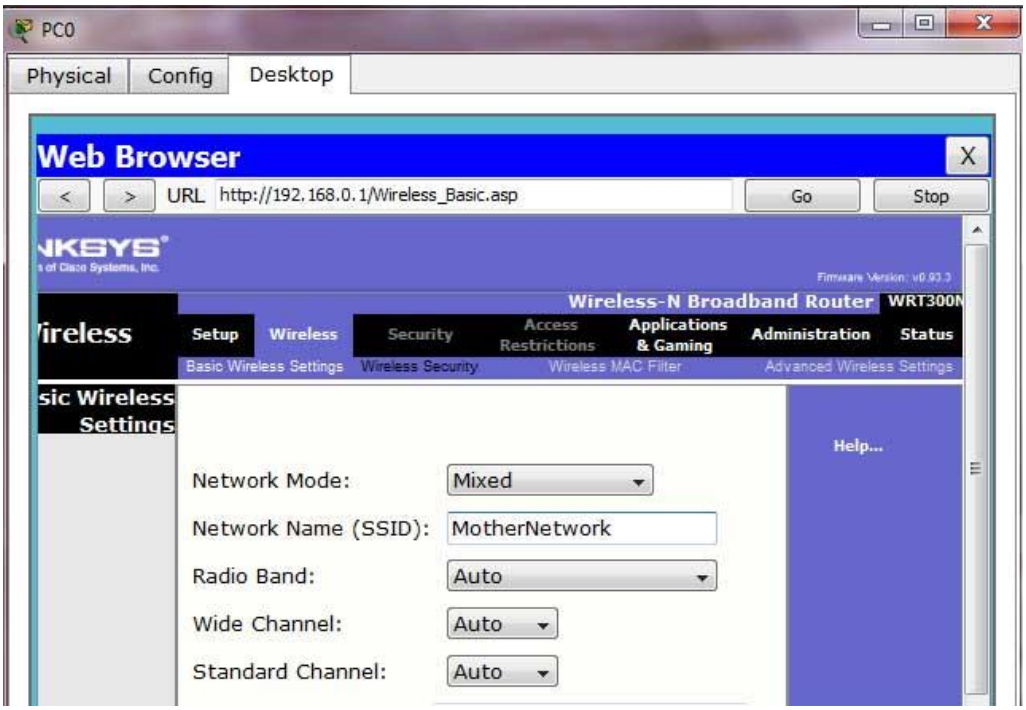

Chọn Administration từ Menu chính và đổi password thành test , bấm Save Setting



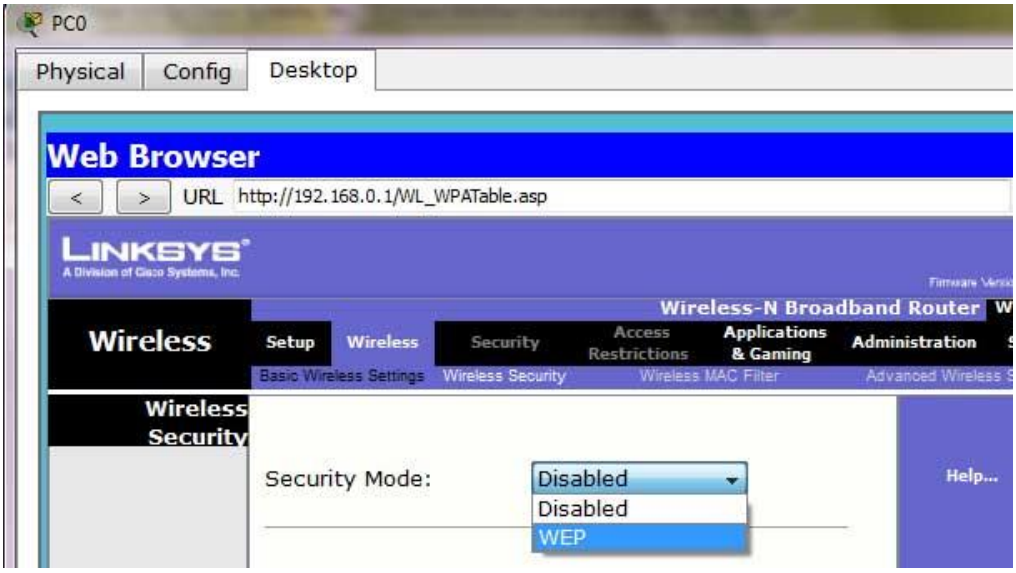

Bấm continue để tiếp tục. Đăng nhập lại với mật khẩu mới đặt.




Chọn tab wireless và đặt SSID thành MotherNetwork




Chọn wireless security và đặt Security Mode thành WEP



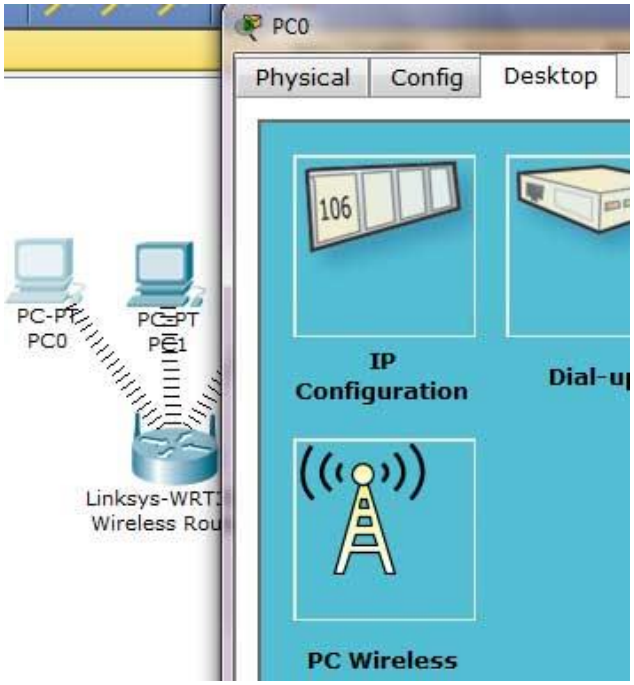

Đặt Key1 là 0123456789


Bấm Save Setting.

Bấm đúp vào pc và chọn tab Desktop tab, chọn IP configuration và Static IP, rồi đặt IP như sau:

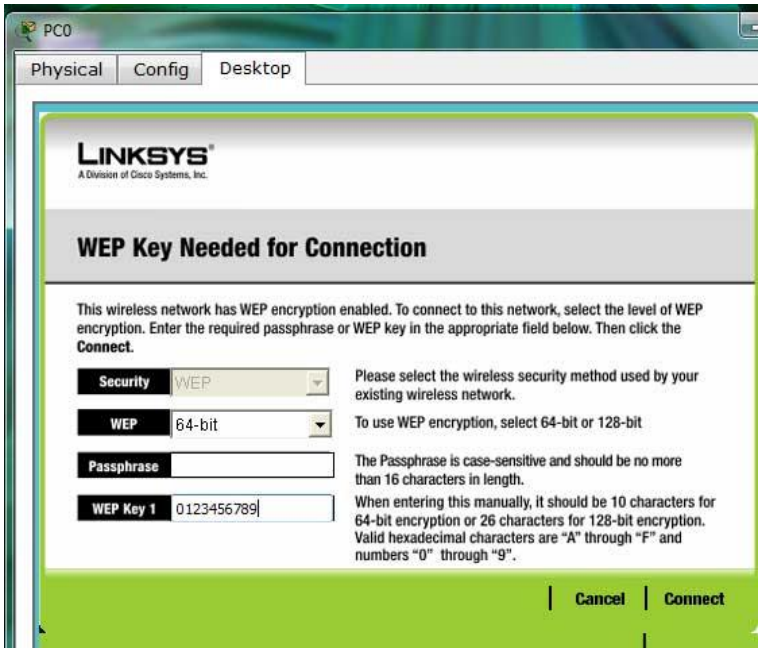
| PC | IP | Subnet Mask | Default Gateway |
|---|---|---|---|
| PC0 | 192.168.0.2 | 255.255.255.0 | 192.168.0.1 |
| PC1 | 192.168.0.3 | 255.255.255.0 | 192.168.0.1 |
| PC2 | 192.168.0.4 | 255.255.255.0 | 192.168.0.1 |

Để kết nối PC tới router không dây. Bấm đúp vào PC, chọn Desktop, rồi PC Wireless

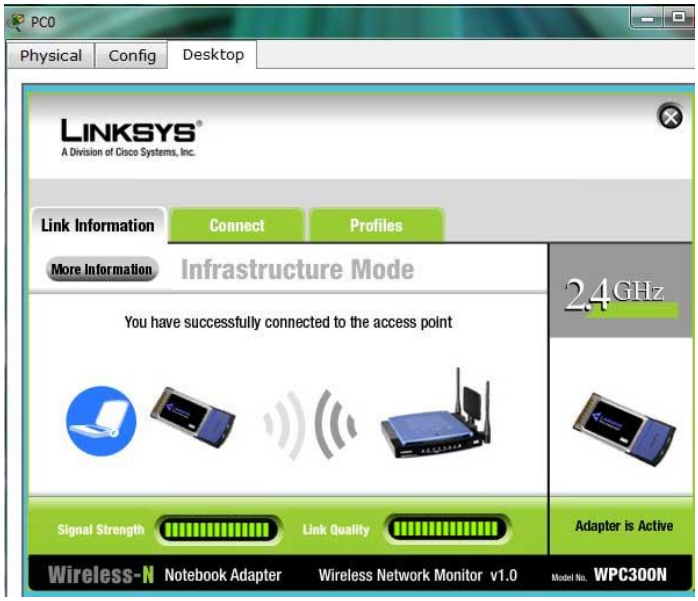



Bấm vào tab connect và nút Refresh.

Bấm vào nút connect để kết nối MotherNetwork, và nhập WAP key là 0123456789 rồi connect.




Nhìn hình dưới ta thấy hệ thống đã kết nối và card PCI card được active.




Làm tương tự với PC1 và PC2.