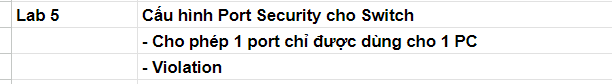
**THỰC HÀNH LAB 5**

**CẤU HÌNH PORT SECURITY SWITCH**

****

**Phần 1: Giới thiệu**

Một trong những phương pháp hay nhất trong bảo mật mạng là thử và ngăn chặn các mối đe dọa bảo mật từ điểm vào của mạng LAN. Port security thường được triển khai để: Ngăn chặn người lạ xâm nhập vào thống mạng nội bộ, **Chặn tấn công MAC Spoofing, Bảo vệ dữ liệu,** **Phát hiện lỗi vi phạm, Tăng cường bảo mật mạng, Chặn chia sẻ cổng không an toàn,** Quản lý tốt các thiết bị truyền ra- vào.

**Phần 2: Chuẩn bị thiết bị**

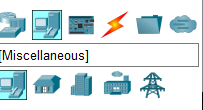
**Mô hình:**

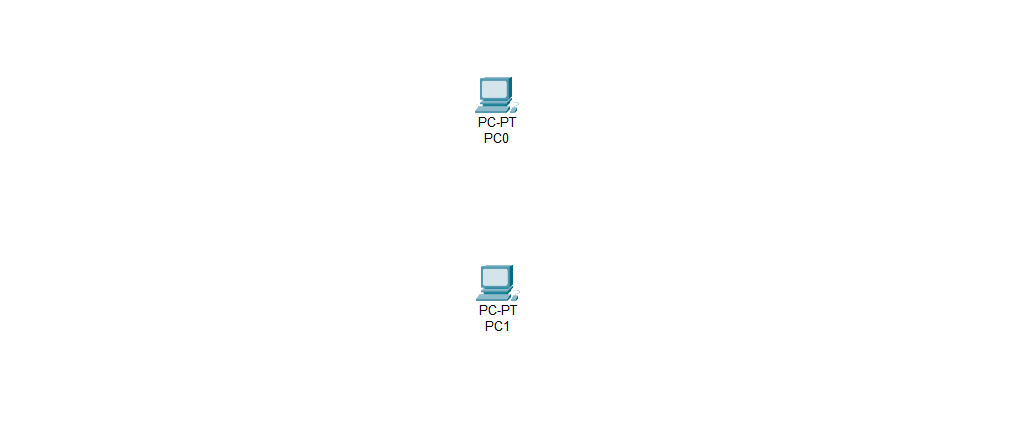
|  |  |  |
| --- | --- | --- |
| **Tên thiết bị** | **Số lượng** | **Ghi chú** |
| Switch  (2960-24TT) | 01 | Dùng để kiểm soát các Port |
| PC-PT  Pc0:  IP: 192.168.1.2  PC1:  IP: 192.168.1.3 | 02 |  |

**Phần 3: Cài đặt thiết bị**

1. PC:

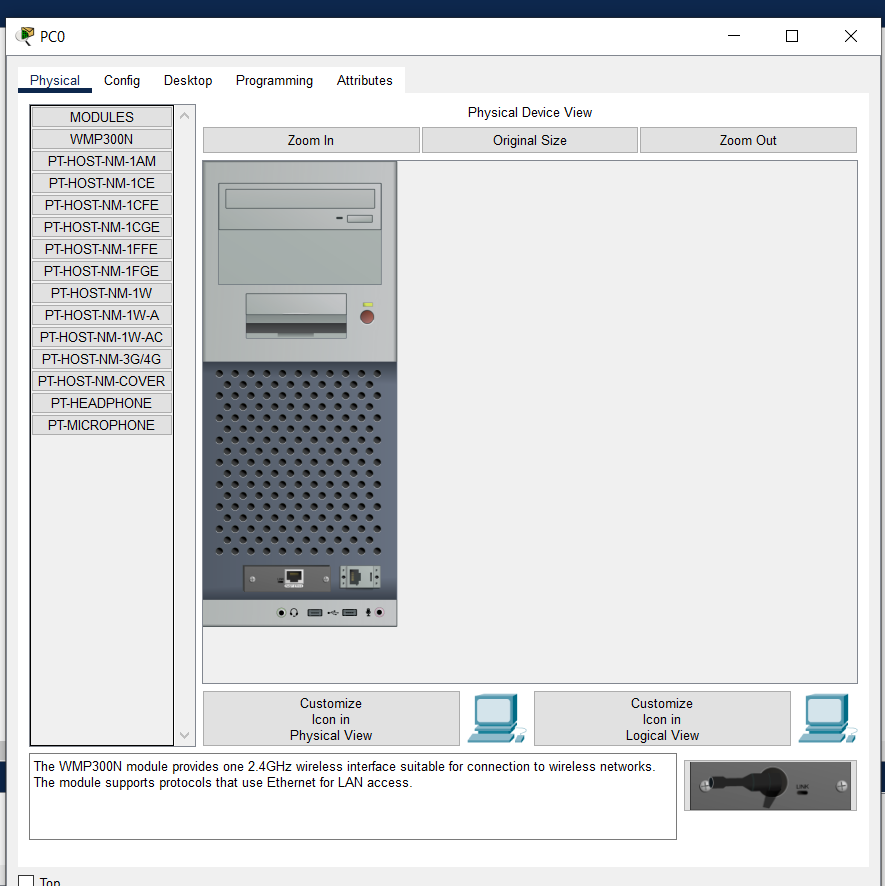
Bước 1: Vào Cisco Packet Tracer tìm vùng PC tạo 2 máy PC.

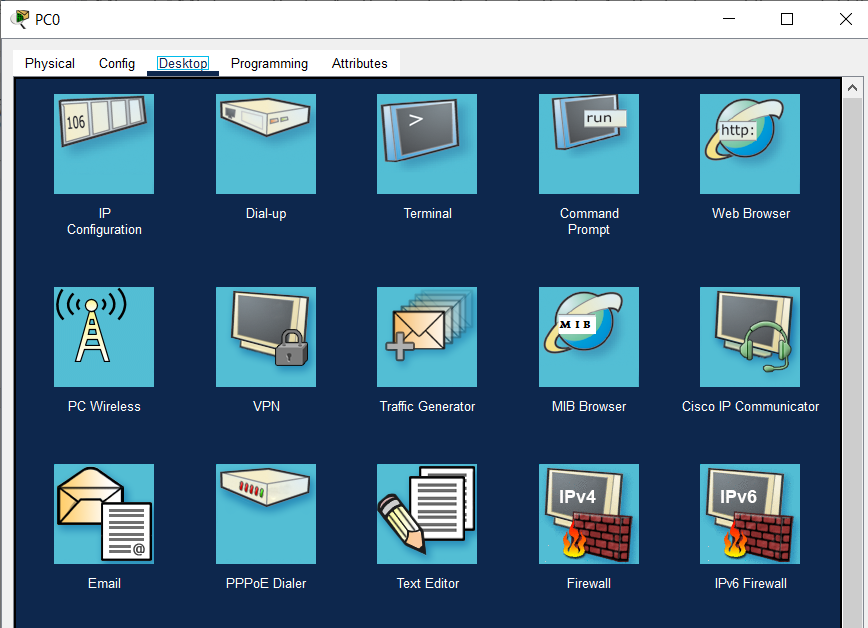


Bước 2: Nhập IP cho máy

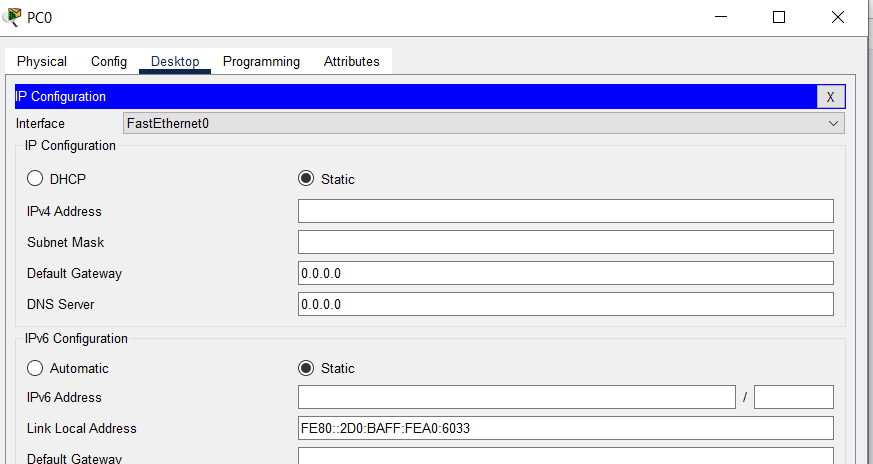
* Bấm chọn vào máy để hiện bảng dữ liệu máy



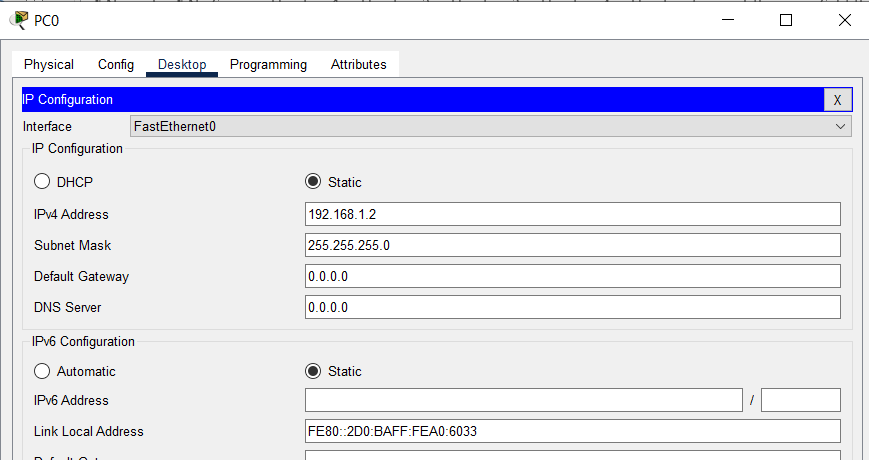
* Chọn Desktop



* Chọn IP Configuration



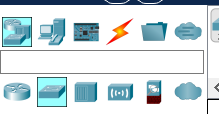
* Ngay tại Ipv4 Address nhập IP của máy -> máy sẽ tự động ghi SubnetMask



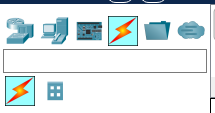
* Ta đã tạo ra máy PC0 với IP: 192.168.1.2
* Thoát ra (vì máy tự lưu nên ta không cần phải lo lắng về việc mất địa chỉ IP của máy PC0)
* Làm tương tự với máy PC1 với IP của PC1

1. Switch:

* Ta vào lại bảng thiết bị tìm Switch và tạo 1 Switch

* Vào lại bảng thiết bị để tìm dây nối:

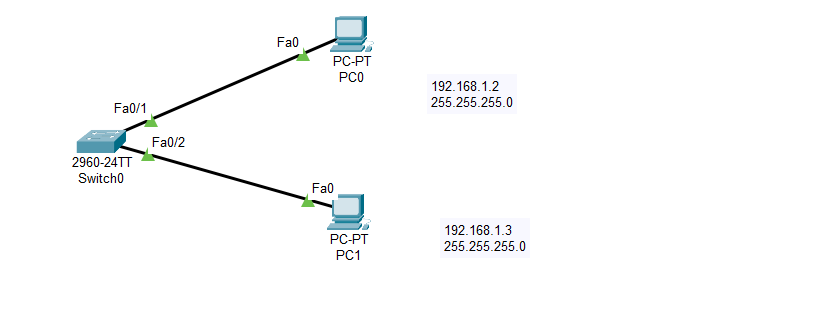
 

Lúc này nhóm em chọn dây đỏ, ngoài ra vẫn có thể dùng được dây đen 

**Phần 4: Thực hành dựng Lap**

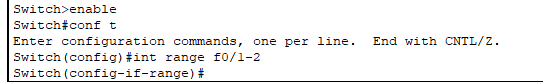
**Phần 1: Cấu hình Port Security cho Switch**

Bước1: Tạo 1 switch( cho giả định nối với 2 PC)



Muốn tạo tính năng ta phải bật tính năng lên trên Switch

Bước 2: Port vào cấu hình



Bước 3: Đưa Port vào chế đồ access để kết nối với end user



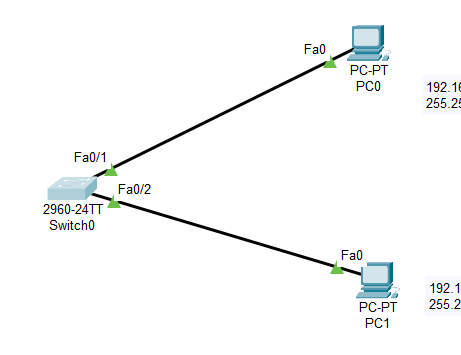
Bước 4: Khởi động Port security



Bước 5: Cho mỗi cổng chỉ ghi nhớ 1 thiết bị chỉ gắn vào đó



Ta thấy, trên swich đang gắn 2 pc:



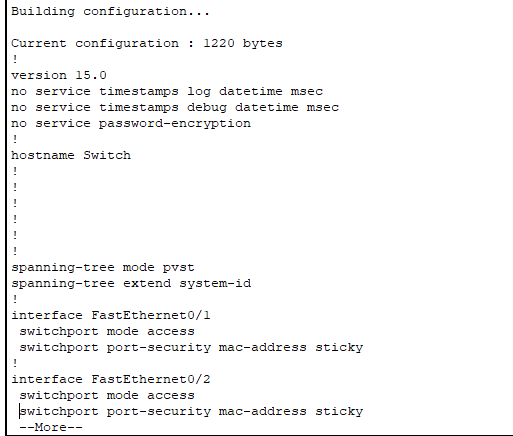
Bước 6: Ta cho hỏng địa chỉ MAC của 2 máy ( nếu như kết nối lớn hơn Maximum thì cả 2 máy đều hỏng luôn) này:



Bước 7: Kiểm tra:



**Kết quả:**

****

Ta thấy: cả 2 máy đều đã bị hỏng:

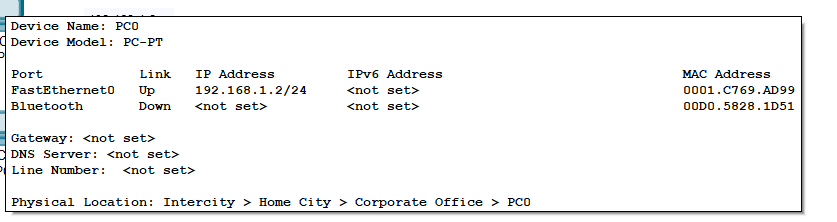




**Ngoài ra, nếu ta muốn chỉ định 1 máy kết nối thay vì bị hòng thì ta làm theo các buóc dưới thây thay cho bước 6:**

Bước 6.2: Gán tĩnh địa chỉ MAC của PC0 đến Port được kết nối đến Switch0

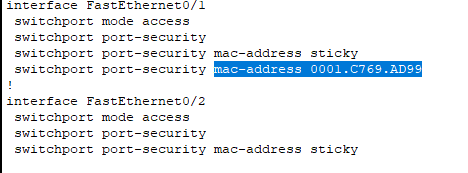
Ta có thể thay thế bằng PC1 cách gắn MAC của PC1 ( tuỳ theo chỉ định người dùng)



Mac:0001.C769.AD99



Bước 7: Kiểm tra



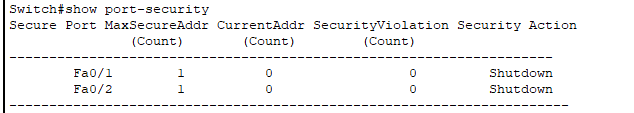
**Phần 2: Violation**

Bình thường khi vi phạm điều kiện, cổng sẽ bị tắt (shutdown) và đưa vào trạng thái lỗi:

Thưởng hay sử dụng ở cách 2 như trên và 1 số cồng ko cần thiết như sơ đồ trên thì cổng từ fa0/3-24…

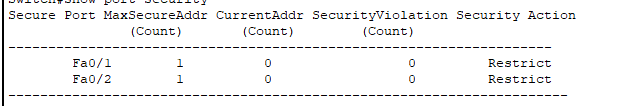
**shutdown**: khi vi phạm điều kiện port ngay lập tức bị shutdown và đưa vào trạng thái lỗi. Ta phải phục hồi lại bằng tay (dùng lệnh **shutdown** và **no shutdown**) hoặc tự động bằng tính năng errdisable recovery (xem lab).





**restrict**: khi vi phạm cổng vẫn hoạt động, tuy nhiên tất cả những khung (frame) từ địa chỉ MAC vi phạm điều kiện đều bị đánh rớt và một thông điệp bẫy SNMP, syslog được gởi ra.





**protect:**khi vi phạm port vẫn hoạt động, giống với **restrict**, tuy nhiên sẽ không gởi thông điệp bẫy SNMP và syslog không được gởi ra.

Đây là trường hợp gắn 1 Mac chạy cho Switch

(cú pháp thì vẫn vậy nhưng ta xem kết quả)



