|  |  |
| --- | --- |
|  | **TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**  **KHOA CÔNG NGHỆ THÔNG TIN** |

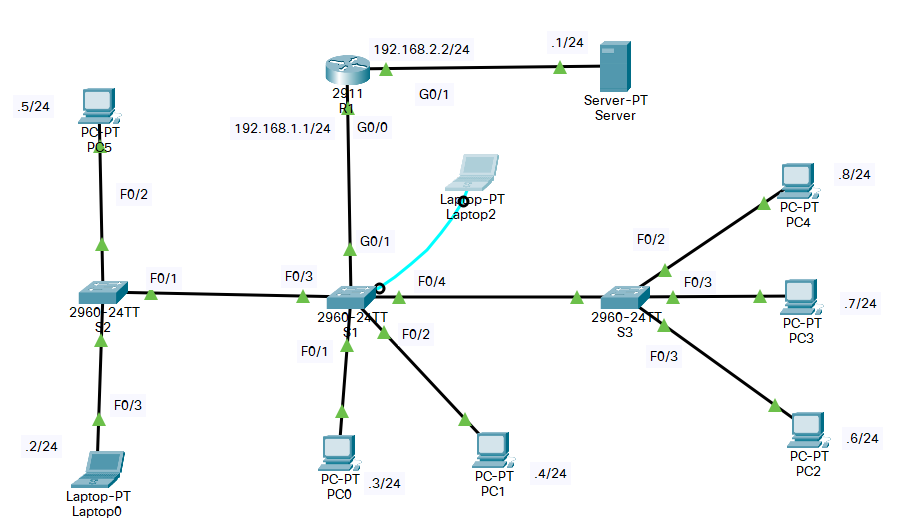
**BÀI TẬP THỰC HÀNH MÔN HỌC WIRELESS AND MOBILE NETWORK SECURITY**

**LAB 3**

* HỌ TÊN: Tạ Văn Trọng (MSV: 51702048)

**NỘI DUNG BÁO CÁO KẾT QUẢ**

**Phần 1: Mô hình**

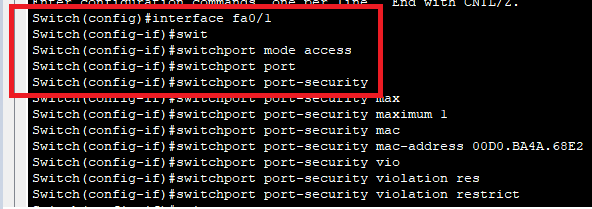


**Phần 2: Cấu hình**

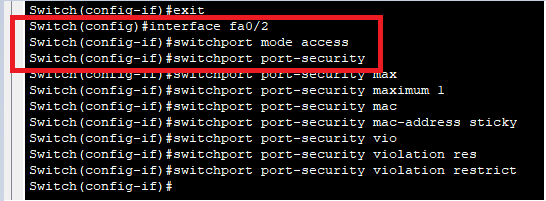
**1: Truy cập vào giao diện dòng lệnh của S1 bằng Labtop2 thực hiện các yêu cầu sau với các cổng Fast Ethernet 0/1 và 0/2.**

**a. Bật bảo mật trên cổng Fast Ethernet 0/1 và 0/2.**

Cấu hình bảo mật trên cổng F0/1 tại Laptop2:

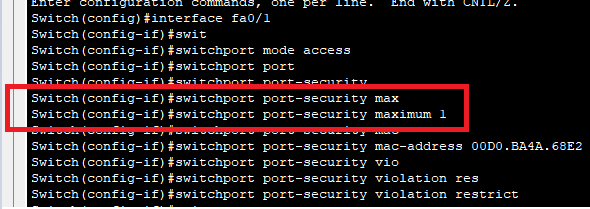


Cấu hình bảo mật trên cổng F0/2 tại Laptop2:

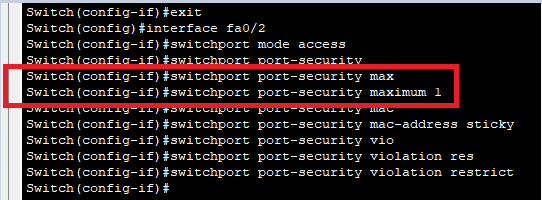


**b. Cấu hình chỉ cho phép tối đa một thiết bị có thể truy cập vào Fast Ethernet 0/1 và 0/2.**

Cấu hình bảo mật trên cổng F0/1 tại Laptop2:

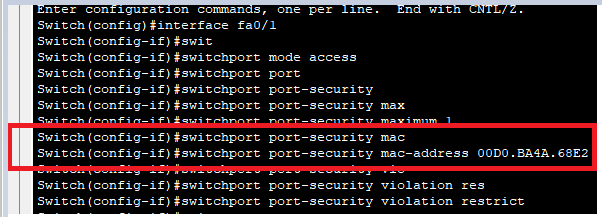


Cấu hình bảo mật trên cổng F0/2 tại Laptop2:

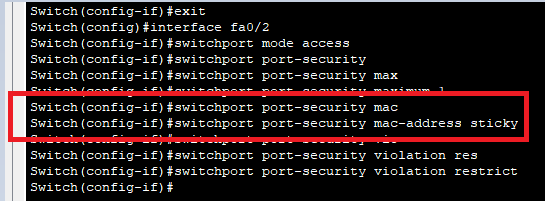


**c. Cấu hình bảo mật các cổng f0/1-2 để địa chỉ MAC của PC0 và PC1 được học tự động và thêm vào cấu hình đang chạy.**

Cấu hình bảo mật trên cổng F0/1 cho phép địa chỉ MAC của PC0 truy cập tại Laptop2:

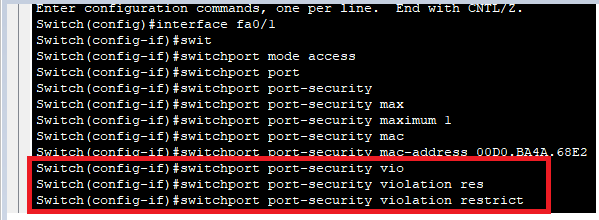


Cấu hình bảo mật trên cổng F0/2 cho phép địa chỉ MAC của PC1 truy cập tại Laptop2:

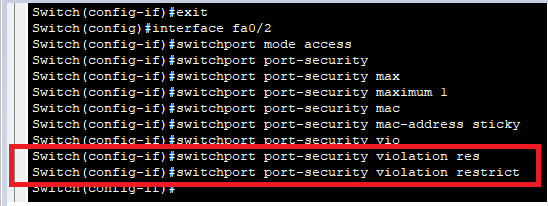


**d. Đặt chế độ vi phạm để các cổng Fast Ethernet 0/1 và 0/2 không bị vô hiệu hóa khi vi phạm xảy ra, nhưng thông báo về vi phạm bảo mật sẽ được tạo và các gói từ nguồn không xác định bị loại bỏ.**

Cổng F0/1:

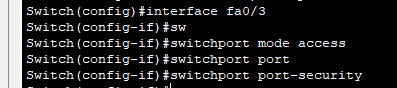


Cổng F0/2:

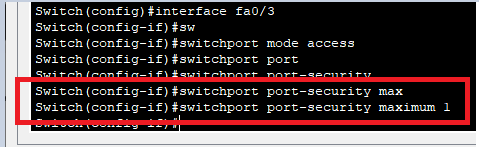


**2: Truy cập vào giao diện dòng lệnh của S1 bằng Labtop2 thực hiện các yêu cầu sau với cổng Fast Ethernet 0/3.**

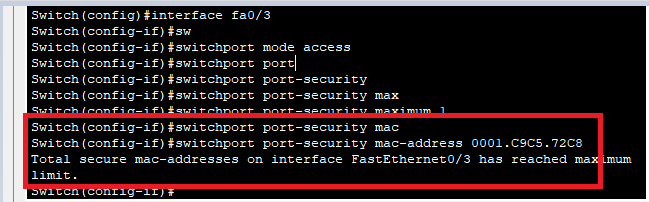
**a. Bật bảo mật trên cổng Fast Ethernet 0/3.**



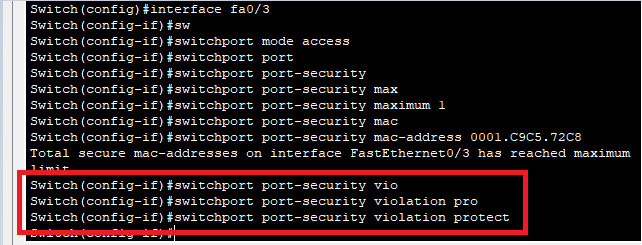
**b. Cấu hình chỉ cho phép tối đa một thiết bị có thể truy cập vào Fast Ethernet 0/3.**



**c. Cấu hình bảo mật các cổng F0/3, địa chỉ MAC của Laptop0 được thêm thủ công và cấu hình đang chạy.**

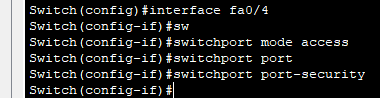


**d. Đặt chế độ vi phạm để các cổng Fast Ethernet 0/3 không bị vô hiệu hóa khi vi phạm xảy ra, nhưng không nhận được bất kỳ thông tin ghi nhật ký nào.**

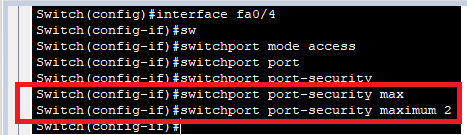


**3: Truy cập vào giao diện dòng lệnh của S1 bằng Labtop2 thực hiện các yêu cầu sau với cổng Fast Ethernet 0/4.**

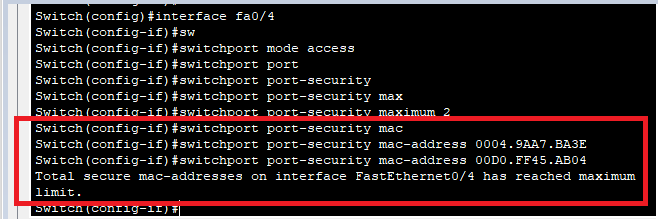
**a. Bật bảo mật trên cổng Fast Ethernet 0/4.**



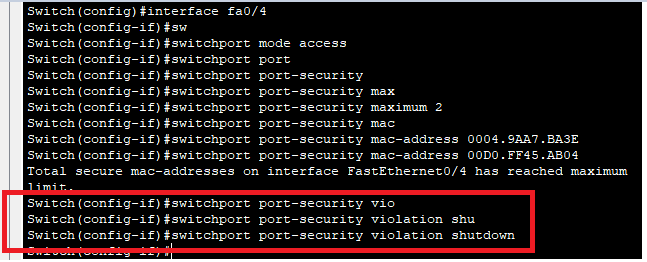
**b. Cấu hình chỉ cho phép tối đa 2 thiết bị có thể truy cập vào Fast Ethernet 0/4**



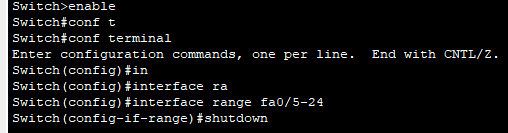
**c. Cấu hình bảo mật cổng F0/4, với địa chỉ MAC của PC2 và PC3 được thêm thủ công vào cấu hình đang chạy.**



**d. Đặt chế độ vi phạm để các cổng Fast Ethernet 0/4 bị vô hiệu hóa khi vi phạm xảy ra, nhưng thông tin ghi nhật ký và bẫy SNMP được gửi đi.**



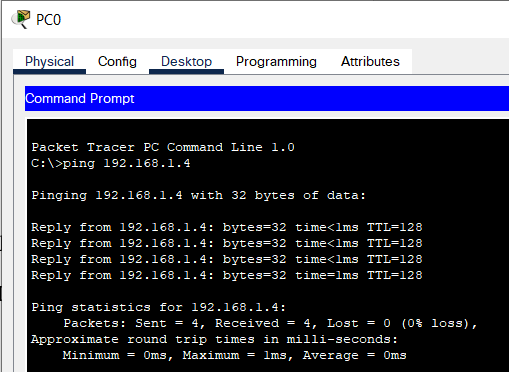
**e. Tắt tất cả các cổng không sử dụng còn lại.**



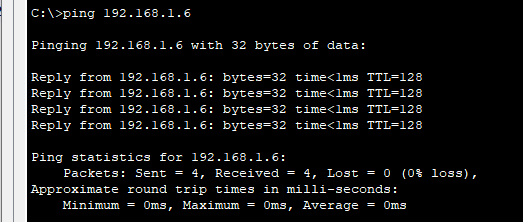
**Phần 3: Xác minh an ninh cổng**

**a. Từ PC0 ping tới PC1,PC2,PC3, Laptop0, Server.**

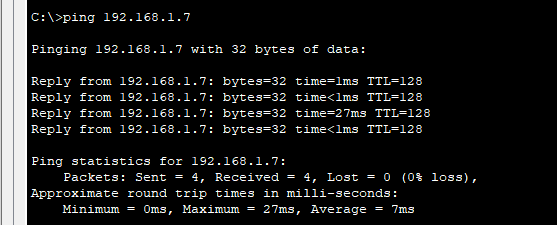
Từ PC0 ping tới PC1:



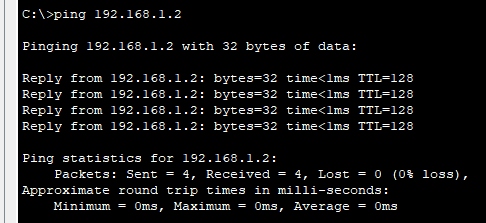
Từ PC0 ping tới PC2:



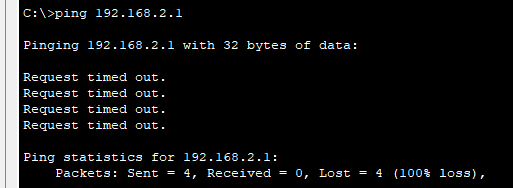
Từ PC0 ping tới PC3:



Từ PC0 ping tới Laptop0:

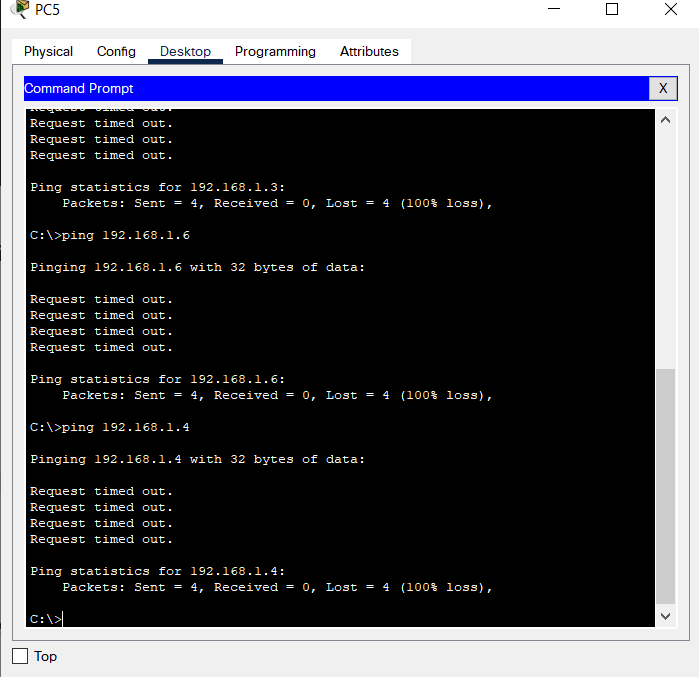


Từ PC0 ping tới Server:



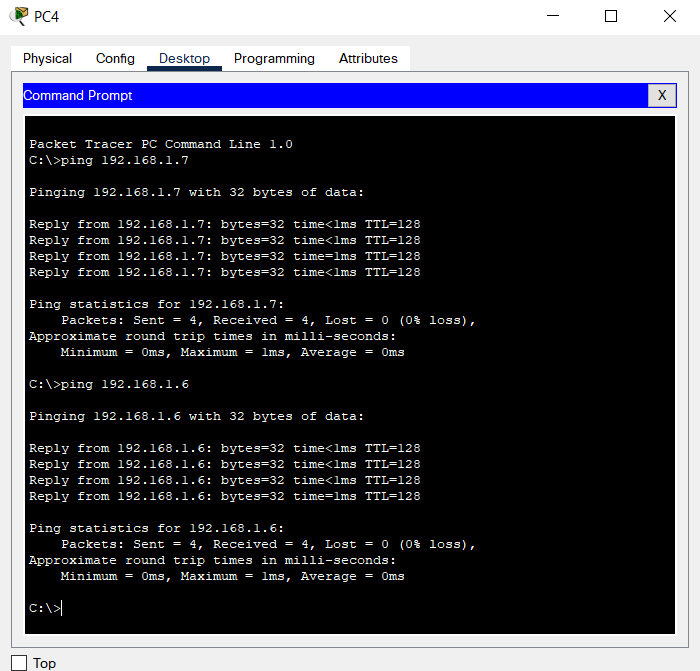
**b. Từ PC5, PC4 ping tới các PC còn lại và Server. Giải thích kết quả xảy ra.**

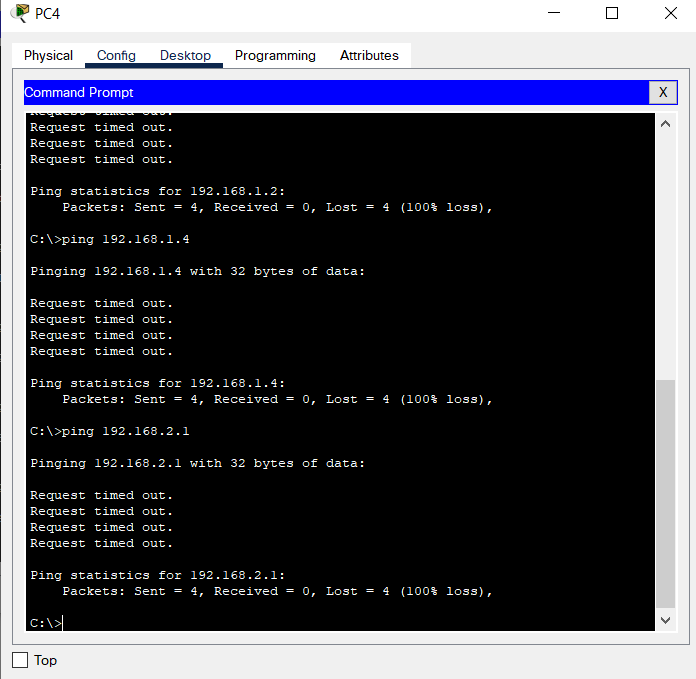
Từ PC5 ping tới các PC còn lại và Server:

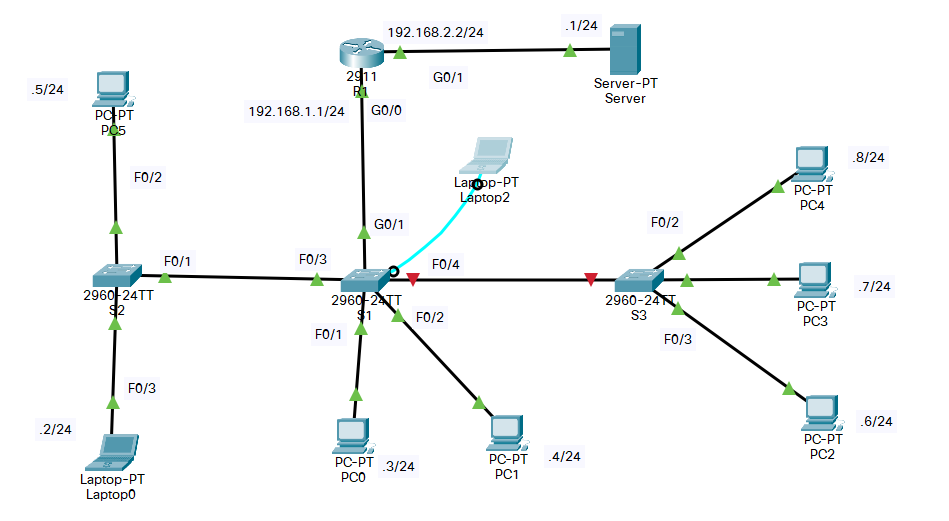


🡺PC5 không thể ping tới server hay các pc còn lại vì cổng fa0/3 chỉ nhận truy cập của địa chỉ MAC: 0001.C9C5.72C8 (Laptop0).

Từ PC4 ping tới các PC còn lại và Server:







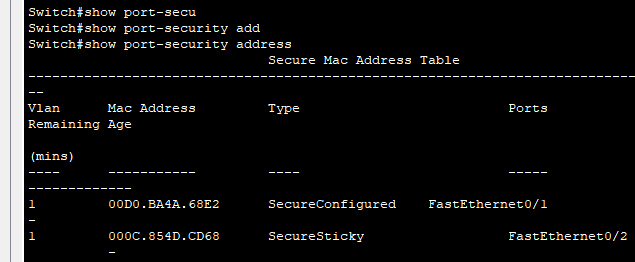
🡺 PC4 chỉ ping được cho PC2, PC3. Tất cả PC còn lại và Server đều không ping được.

PC4 không ping được cho các PC khác vì cổng Fa0/4 chỉ nhận truy cập của địa chỉ MAC của PC2, PC3.

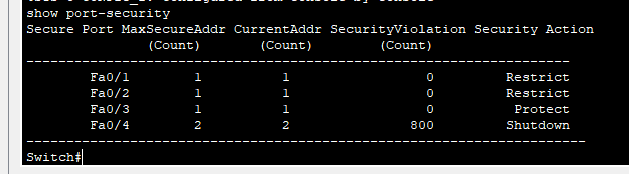
**c. Xác minh rằng bảo mật cổng đã được bật và địa chỉ MAC của PC0 và PC1 đã được thêm vào cấu hình đang chạy.**

MAC address của PC0: 00D0.BA4A.68E2

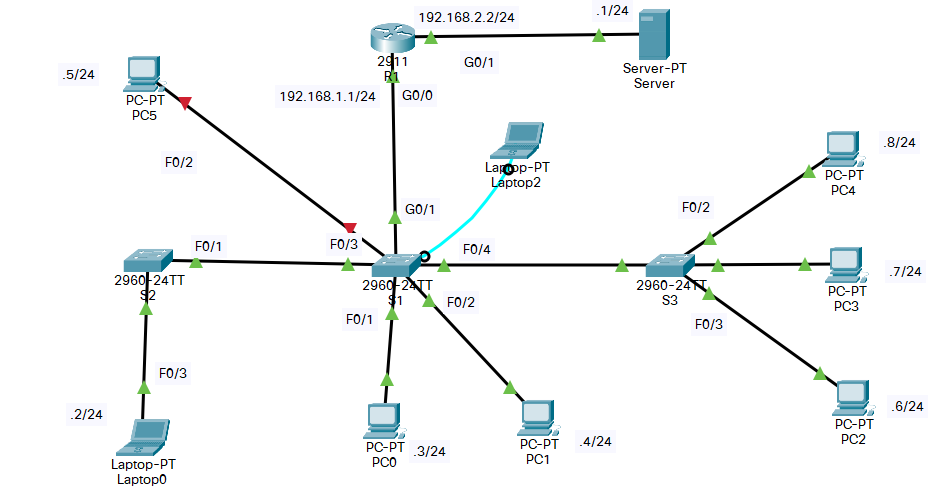
MAC address của PC1: 000C.854D.CD68



**d. Sử dụng các lệnh hiển thị bảo mật cổng để hiển thị thông tin cấu hình.**



**e. Kết nối PC5 vào bất kỳ cổng nào không dụng của S1 và kiểm tra đèn liên kết có mầu gì? Giải thích lý do.**



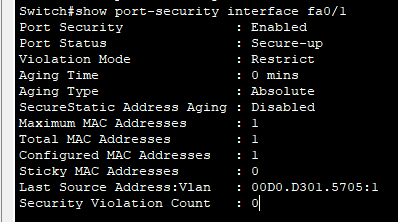
🡺Kết nối PC5 với cổng Fa0/5 của S1 thì có đèn màu đỏ. Vì từ cổng fa0/5 đến fa0/24 đã tắt.

**f. Kết nối PC5 và cổng F0/1, sau đó ping tới các máy còn lại, giải thích kết quả thu được.**

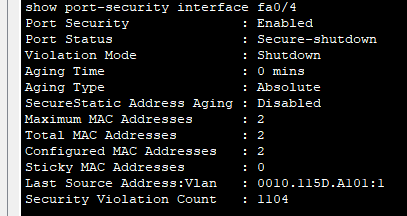
🡺PC5 không thể ping đến các máy còn lại vì cổng F0/1 đã cấu hình cố định truy cập địa chỉ MAC của PC0.

**g. Hiển thị các vi phạm bảo mật cổng đối với cổng mà PC0 và PC2 được kết nối vào. Có bao nhiêu vi phạm đã xảy ra?**

PC0 từ cổng Fa0/1 có 0 lần vi phạm.



PC2 từ cổng Fa0/4 có 1104 lần vi phạm.



**Kết luận:**

Sau khi hoàn thành lab3 thì em đã cấu hình được bảo mật trên Switch.