I. Tổng quan về Span Port:

1. SPAN PORT là gì ?

SPAN port (viết tắt của *Switched Port Analyzer*) — còn gọi là port mirroring — là một chức năng/ tính năng của switch cho phép tạo các bản sao(mirror) của các frame Ethernet từ một hoặc nhiều cổng nguồn (source ports) sang một cổng đích (destination port) để phục vụ cho việc giám sát, phân tích hoặc ghi log lưu lượng.

- Nó thường được sử dụng trên switch vì nó ứng dụng để sao chép các frame ethernet trong mạng LAN -> kết nối các máy trong cùng mạng nội bộ. -> Thường được dùng để bổ trợ IDS (NIDS).
- Không dùng trong router vì router không thấy chi tiết từng gói tin giữa các máy trong LAN.Nó chỉ quan tâm đến địa chỉ IP nguồn/đích, route, và chính sách định tuyến ->kết nối giữa mạng LAN với mạng WAN).

2. Cách hoạt động

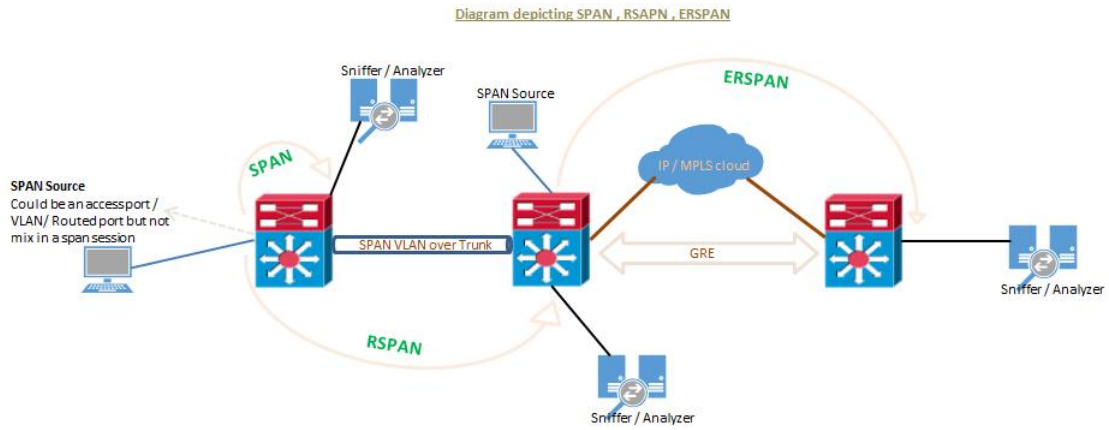
Giả sử bạn có một switch với 24 cổng.

Bạn cấu hình cổng số 24 làm SPAN port.

Sau đó bạn chọn cổng số 1 và 2 là source ports.
- Khi đó, toàn bộ lưu lượng đi vào và đi ra từ cổng 1 và 2 sẽ được sao chép sang cổng 24.
- Tại cổng 24, bạn có thể gắn một thiết bị sniffer (như Wireshark, Security Onion, Zeek, Suricata, v.v.) để phân tích lưu lượng mạng mà không ảnh hưởng tới hoạt động của mạng thật.

3. Các loại SPAN phổ biến

Loại SPAN	Mô tả
Local SPAN	Source và Destination nằm trên cùng switch vật lý.
Remote SPAN (RSPAN)	Source và Destination nằm trên hai switch khác nhau, truyền bản sao qua VLAN đặc biệt.
ERSPAN (*Encapsulated RSPAN*)	Giống RSPAN nhưng dữ liệu được gói trong GRE tunnel để truyền qua IP network (thường dùng trong môi trường ảo hóa hoặc datacenter lớn).



4. Ứng dụng thực tế:

SPAN được sử dụng rộng rãi cho nhiều mục đích:

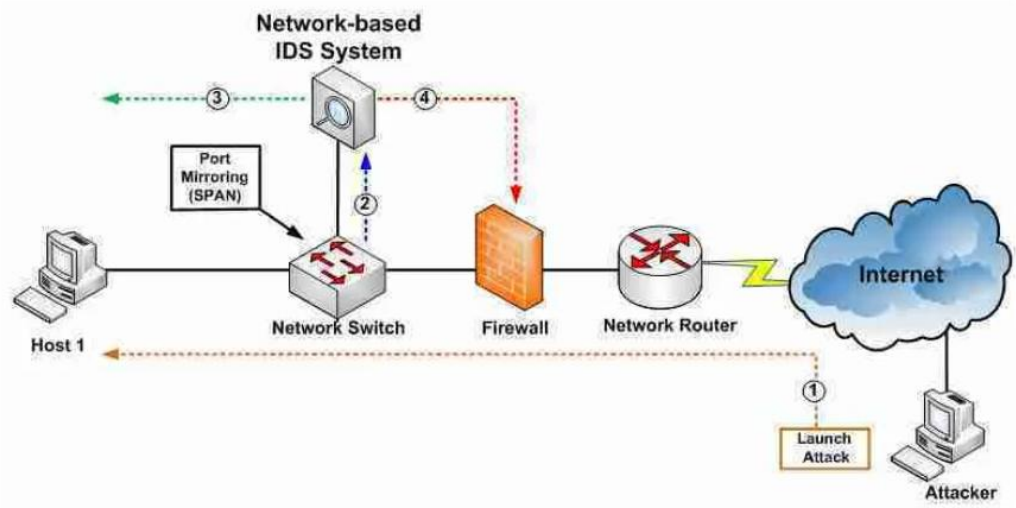
- Xử Lý Sự Cố Mạng: Cho phép các kỹ sư mạng theo dõi và phân tích các gói tin để xác định vấn đề trong mạng.
- Bảo Mật: Các công cụ phát hiện xâm nhập (IDS) có thể sử dụng dữ liệu từ SPAN để phát hiện hoạt động đáng ngờ. VD: NIDS ứng dụng kỹ thuật mirroring (span port).
- Giám Sát Hiệu Suất: Kiểm tra mức sử dụng băng thông và hiệu suất mạng để tối ưu hóa cấu hình.

--> Mục tiêu của span port là " nuôi" traffic cho IDS nội bộ

5. Quy Tắc và Hạn Chế Quan Trọng của Span Port:

- Cổng đích SPAN không nên được cấu hình để mang lưu lượng bình thường, chỉ nên dùng cho giám sát.
- Một session SPAN chỉ có thể có một cổng đích duy nhất.
- Có thể cấu hình tối đa 512 session SPAN trên mỗi thiết bị.
- Khi sao chép lưu lượng từ một cổng tốc độ cao sang một cổng tốc độ thấp hơn, các gói tin dư thừa có thể bị loại bỏ
- Có thể drop packet khi switch quá tải.
- Không phải lúc nào cũng phản ánh lưu lượng thực tế 100%.

II. ỨNG DỤNG MIRRORING (SPAN PORT) VÀO NIDS:



- NIDS chỉ là một mắt xích trong hệ thống phòng thủ nhiều lớp (Defense in Depth). Cụ thể:

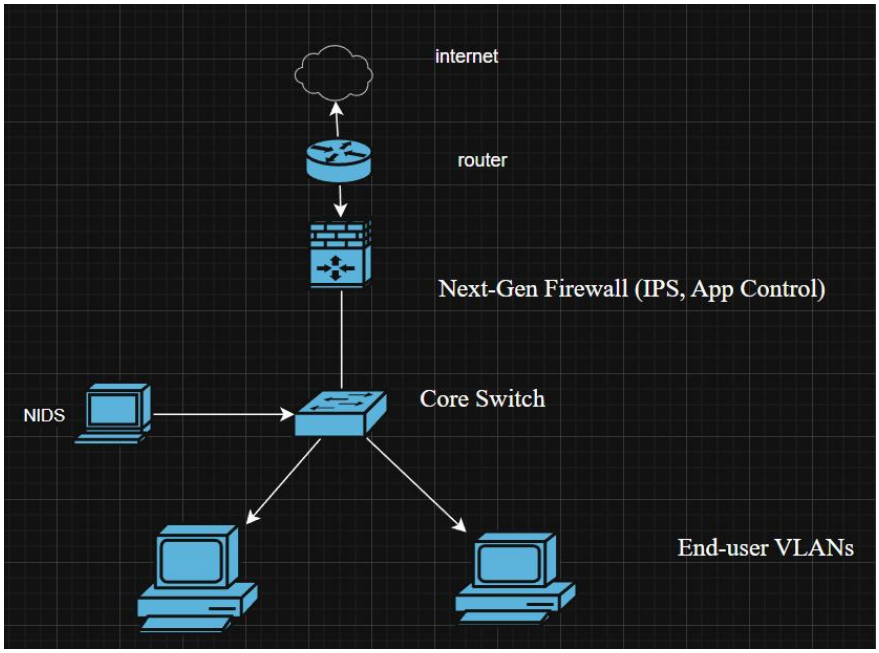
- NIDS kết hợp với:

Thành phần	Chức năng	Mức độ phản ứng
Firewall / NGFW / IPS	Chặn traffic theo rule, port, signature	Real-time chặn
SIEM (Splunk, QRadar, ELK)	Thu log từ NIDS, firewall, endpoint	Phân tích tập trung
SOAR / Automation	Khi thấy cảnh báo nghiêm trọng từ NIDS → tự động chặn IP, cô lập host	Phản ứng tự động
EDR / XDR	Phát hiện & chặn hành vi trên endpoint	Local chặn

→ Nên thông thường chúng ta không cần đặt NIPS riêng (ở internal lan/core switch) vì firewall NGFW đã có module IPS/NIPS rồi.

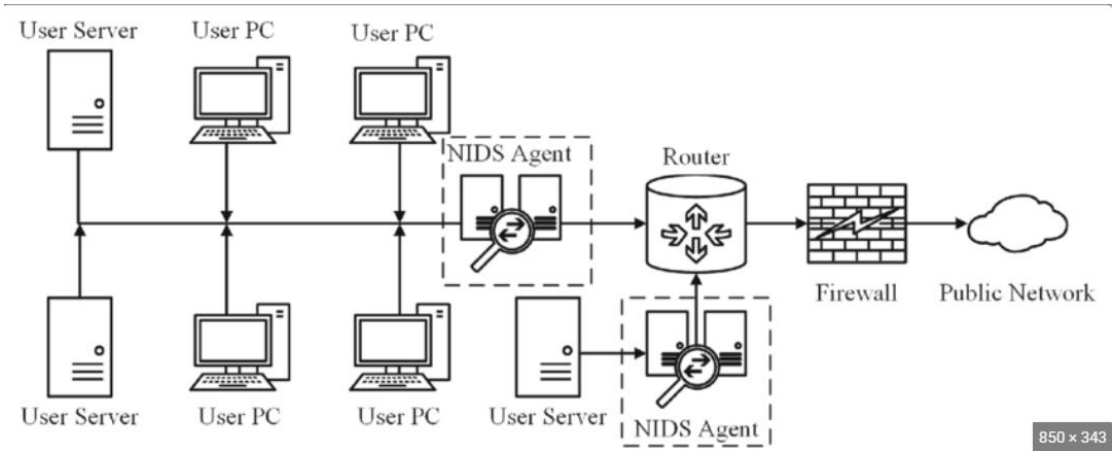
Tình huống thực tế:

Ví dụ trong doanh nghiệp hiện nay:




```
[Internet]
    ↓
[Next-Gen Firewall (IPS, App Control)]
    ↓
[Core Switch]
    ↓
[NIDS Sensor - Giám sát Inter-LAN Traffic]
    ↓
[End-user VLANs / Server VLANs]

⇅
SIEM + SOAR + EDR (phản ứng tự động)
```



Khi NIDS phát hiện một hành vi lạ (ví dụ SMB brute-force):

1. Nó gửi alert lên SIEM.
2. SOAR hoặc Firewall nhận alert đó → tự động chặn IP nguồn, hoặc EDR cô lập host.
→ Vì vậy doanh nghiệp vẫn ngăn chặn được tấn công, nhưng gián tiếp qua hệ thống khác, không phải NIDS tự làm.

✓ Kết luận thực tế:

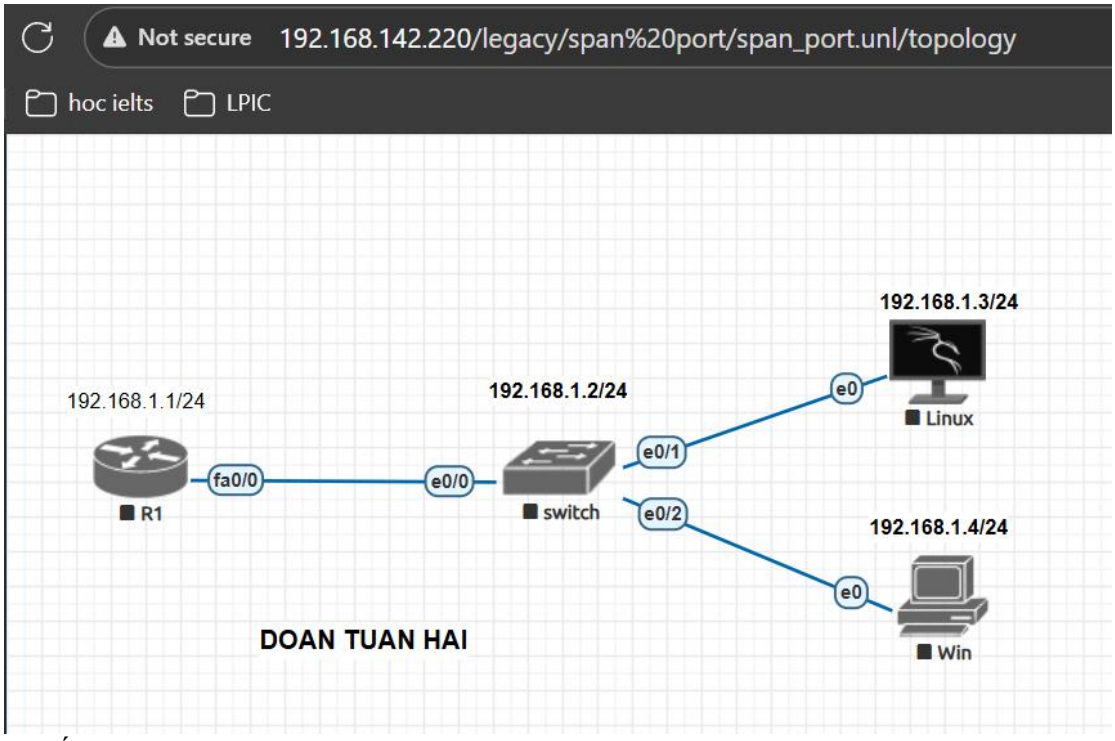
- Trong doanh nghiệp, NIDS ở inter-LAN chỉ là "mắt giám sát", không thể tự chặn.
- Việc ngăn chặn được thực hiện bởi firewall (IPS/NIPS) hoặc qua cơ chế phản ứng tự động (SOAR/EDR).
- Vì vậy, chỉ có NIDS thôi là chưa đủ để bảo vệ mạng nội bộ.

III. CÁC KĨ THUẬT MIRRORING KHÁC:

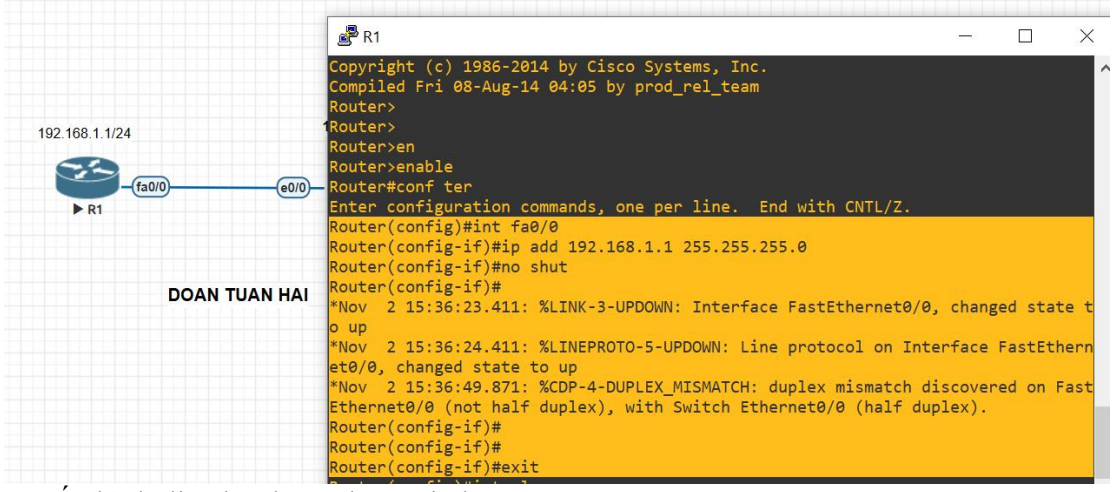
Loại mirroring	Vị trí	Cách thức	Dùng khi
SPAN (Local)	Switch	Mirror trong switch	Lab, mạng nhỏ
RSPAN	Switch	Mirror qua VLAN	IDS ở switch khác
ERSPAN	Switch	Mirror qua GRE tunnel	IDS ở xa, datacenter khác
TAP (Network TAP)	Phần cứng	Sao chép tín hiệu vật lý	Mạng lớn, datacenter
Virtual TAP	Cloud / ảo hóa	Mirror VM / container traffic	Cloud SOC
Inline TAP / Bypass TAP	Giữa thiết bị mạng	Mirror song song với thiết bị inline	SOC lớn, IPS, firewall

IV. BÀI LAB ỨNG DỤNG SPAN PORT LÀM IDS:

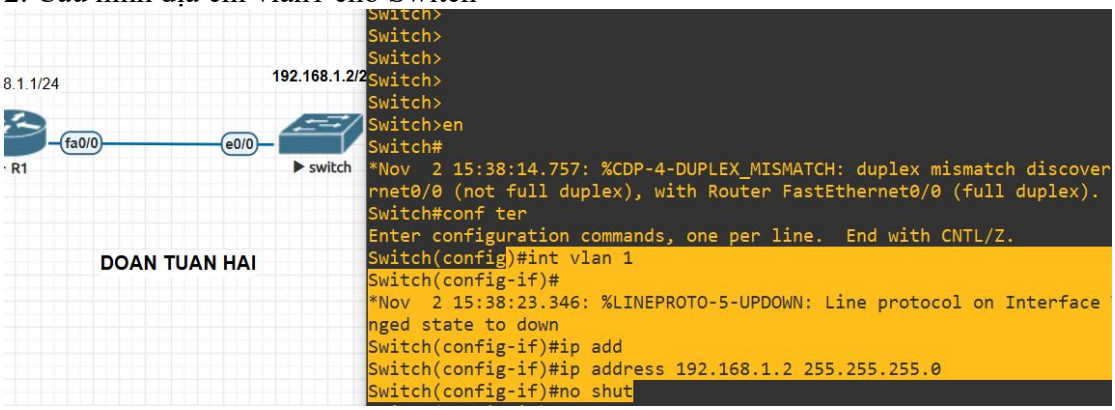
Mô hình



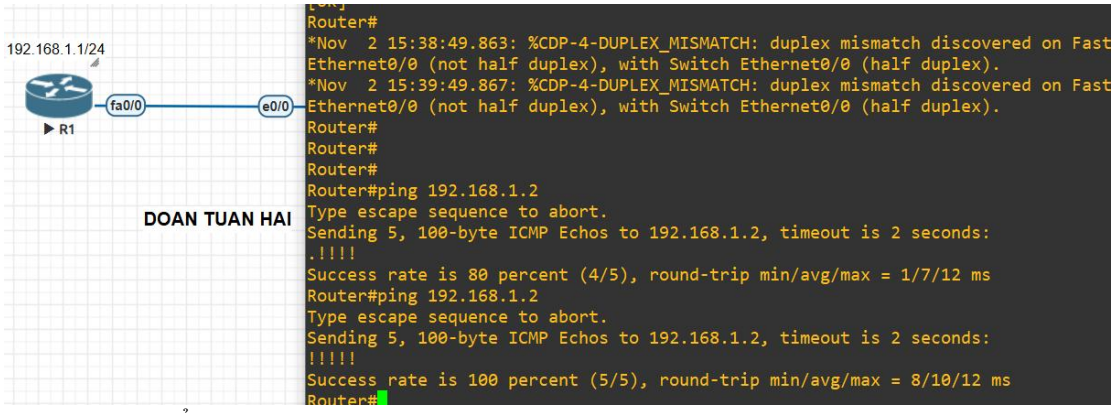
1. Cấu hình địa chỉ router



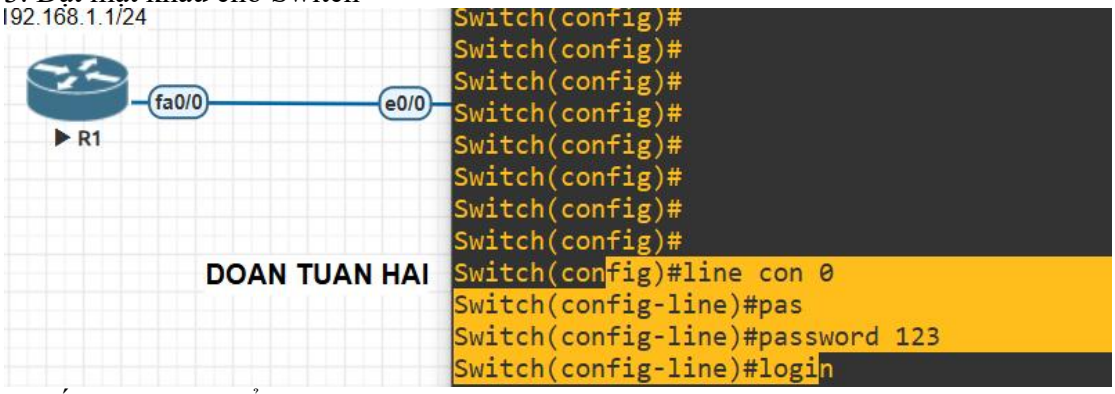
2. Cấu hình địa chỉ vlan1 cho Switch



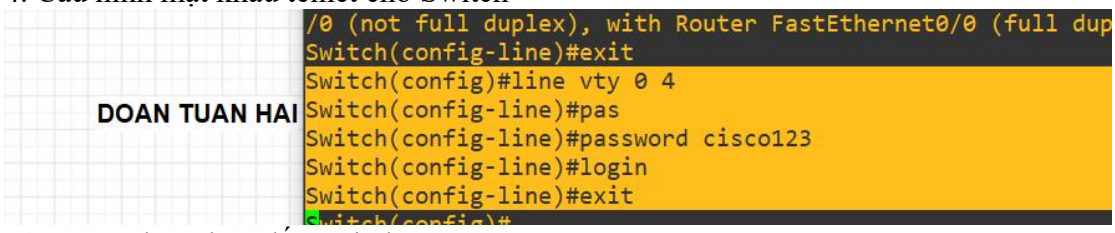
Thử ping router với switch



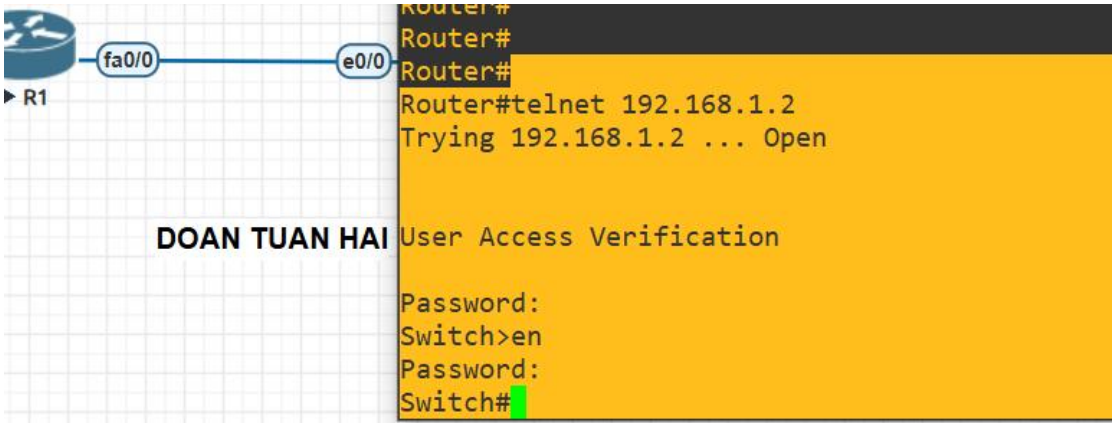
3. Đặt mật khẩu cho Switch



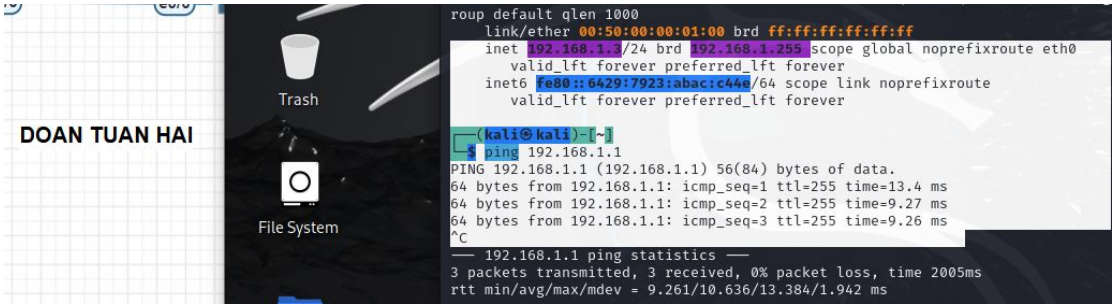
4. Cấu hình mật khẩu telnet cho Switch



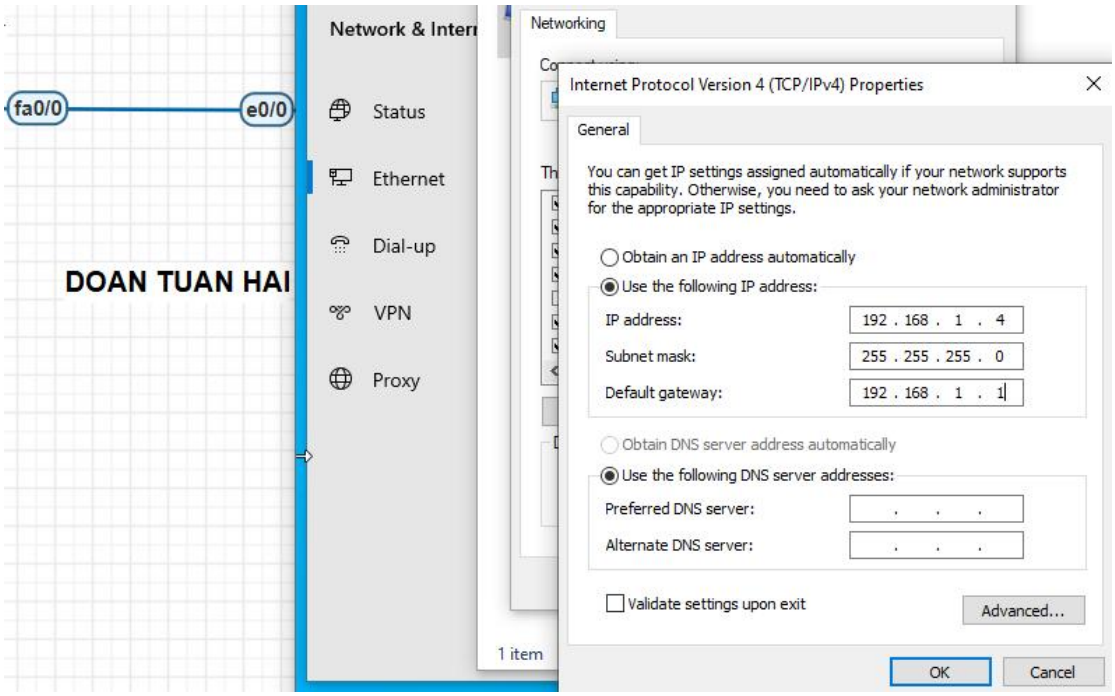
Từ router thử telnet đến switch



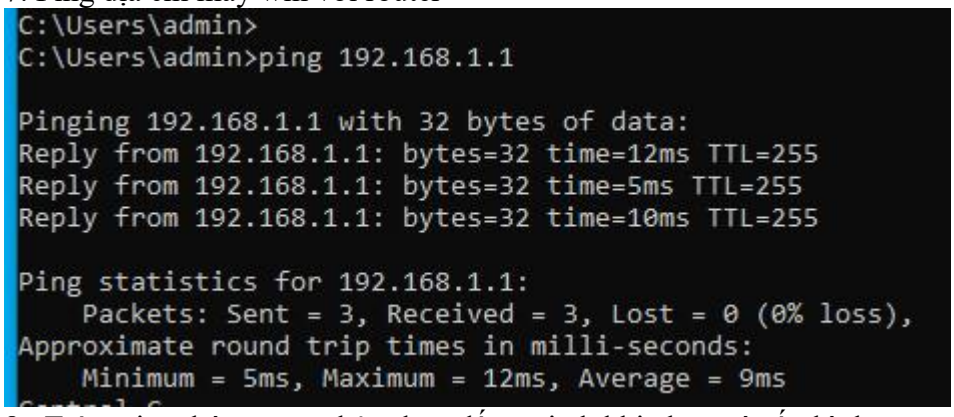
5. Ping thử kết nối giữa kali và router.



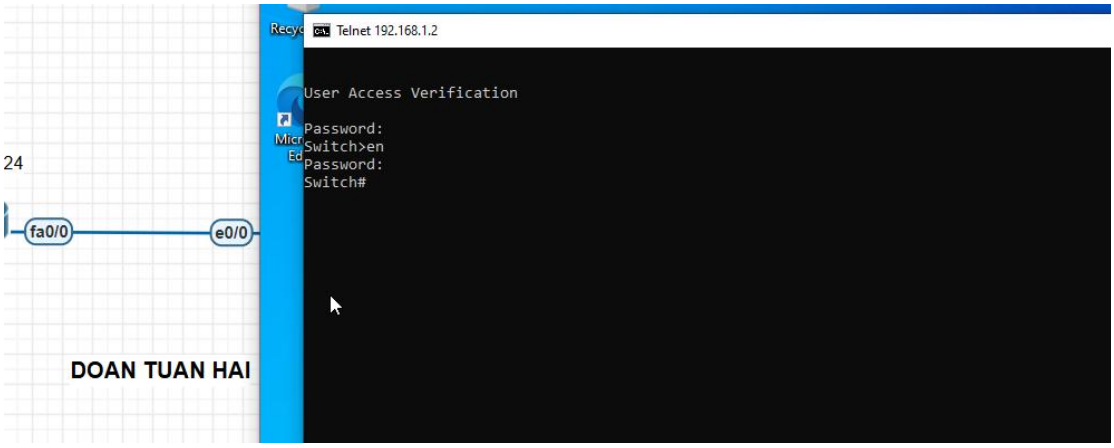
6. Chỉnh địa chỉ ip cho win



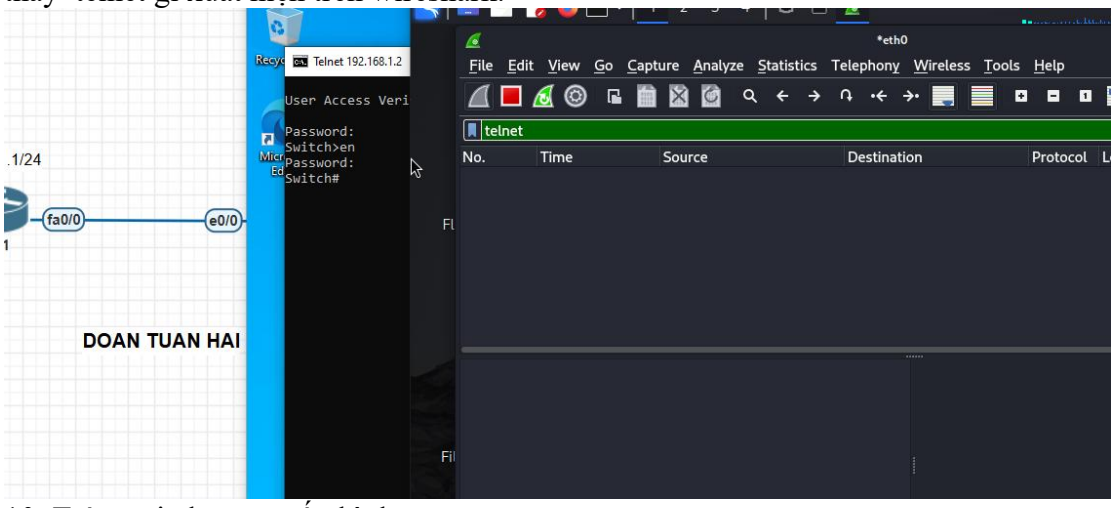
7. Ping địa chỉ máy win với router



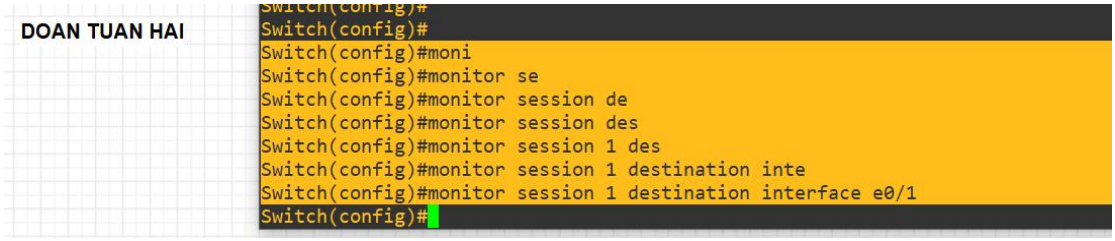
8. Trên win, chúng ta sẽ thử telnet đến switch khi chưa có cấu hình span port trên switch.



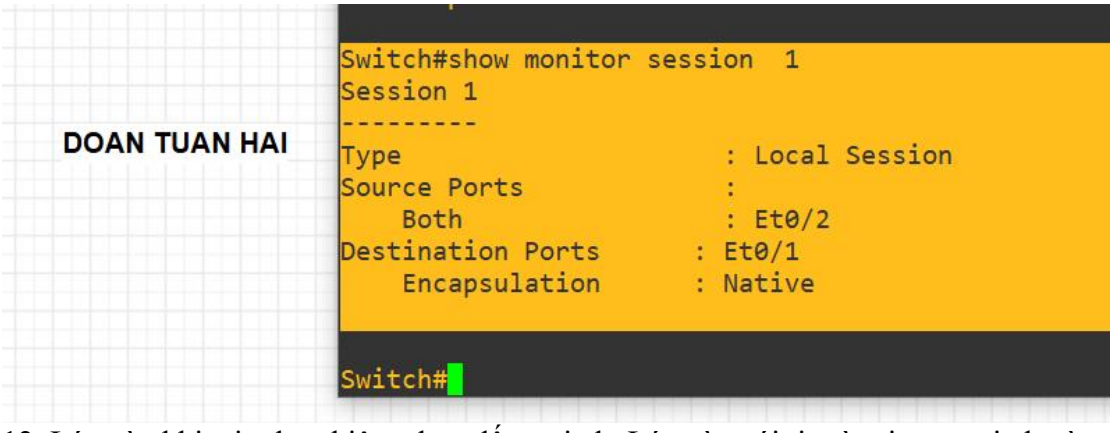
9. Trên kali, ta sẽ đóng vai trò là IDS, giám sát traffic trên switch. Và kết quả không thấy telnet gì xuất hiện trên wireshark.



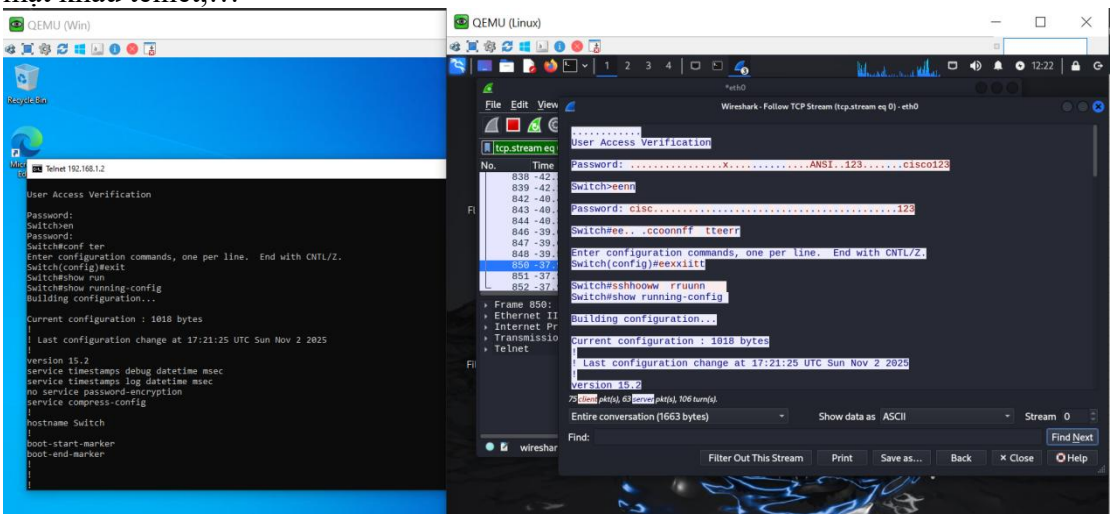
10. Trên switch, ta sẽ cấu hình span port



11. Kiểm tra span port



12. Lúc này khi win thực hiện telnet đến switch. Lúc này gói tin từ win -> switch và cũng copy những gói tin đó chuyển đến kali(IDS) đồng thời. Lúc này trên kali(IDS) chúng ta thực hiện mở wireshark và bắt được các gói tin telnet. Chúng ta : Follow -> TCP Stream để thấy chi tiết gói tin. Ở đây chúng ta có thể thấy được mật khẩu switch, mật khẩu telnet,…



Lưu ý: Sau khi cấu hình SPAN PORT thì cổng destination SPAN bị tách hoàn toàn khỏi hoạt động Layer2/Layer3

Nó chỉ nhận gói mirrored, không gửi bất kỳ traffic nào ra

Nó bị loại khỏi VLAN, không còn học địa chỉ MAC, không xử lý STP, không có IP, không chạy Telnet/SSH

Port destination của SPAN "chết" về mặt logic, chỉ còn để ghi traffic