



fit@hcmus

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

KHOA CÔNG NGHỆ THÔNG TIN

BÁO CÁO TÓM TẮT ĐATH SỐ 2: CẤU HÌNH CÁC GIAO THỨC
HỌC PHẦN CSC11005 – THỰC TẬP MẠNG MÁY TÍNH

1. Thông tin nhóm thực hiện

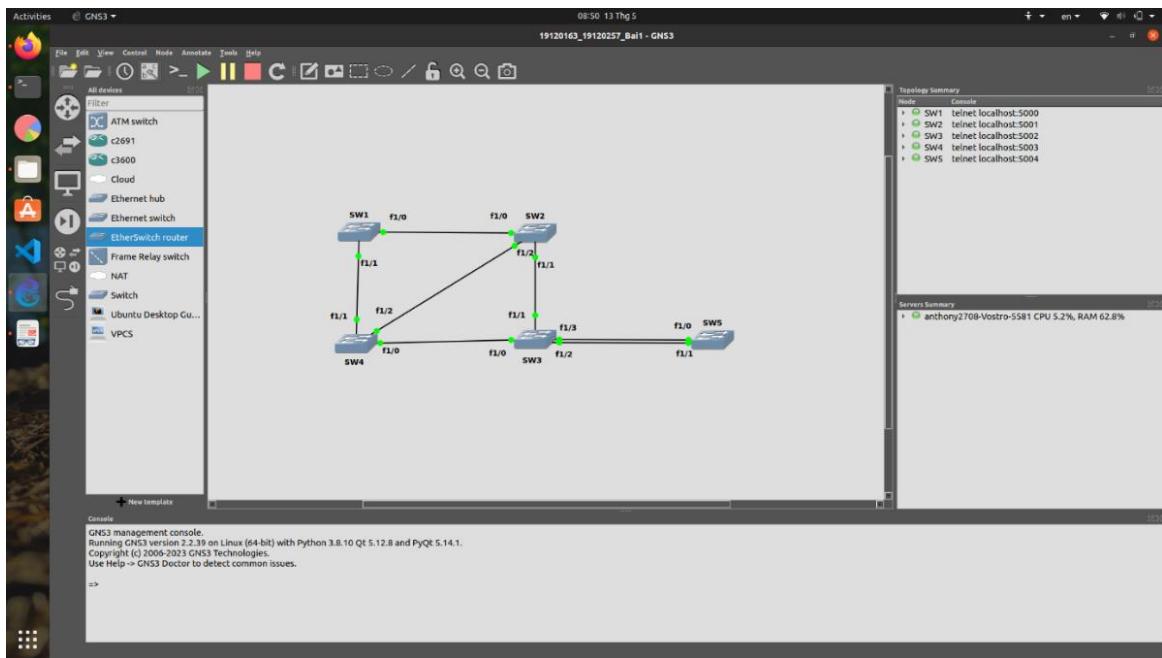
- Bùi Lê Tuấn Anh (**19120163**), đóng góp **50%** tổng bài làm cho đồ án thực hành số 2, sử dụng phiên bản **GNS3 2.2.38** và phiên bản IOS cho bài làm là **c3745-adviservicesk9-mz.124-25d.image**. Tỷ lệ hoàn thành: **100%** yêu cầu đề ra của **bài 1**, trong đó bao gồm các yêu cầu về cấu hình cũng như kiểm tra nội dung gói tin trao đổi giữa các thiết bị với nhau. Hệ điều hành: **Ubuntu 20.04 LTS**
- Phạm Anh Khoa (**19120257**), đóng góp **50%** tổng bài làm cho đồ án thực hành số 2, sử dụng phiên bản **GNS3 2.2.38** và phiên bản IOS cho bài làm là **c3725-adventuresek9-mz.124-25d.image**. Tỷ lệ hoàn thành: **100%** yêu cầu đề ra của **bài 2**, trong đó bao gồm các yêu cầu về cấu hình, định tuyến cũng như kiểm tra nội dung gói tin trao đổi giữa các giao thức với nhau. Hệ điều hành: **Windows 10**

2. Tài liệu tham khảo

- <https://learningnetwork.cisco.com/s/question/0D53i00000Ksy9yCAB/stp-wrong-root-port>
- <https://community.cisco.com/t5/other-network-architecture-subjects/mulitcast-mac-address/td-p/586124>
- <https://study-cvpn.com/virtual-terminal-vty-lines-with-access-control-list/>
- Slides và HDTH STP, Thực tập Mạng máy tính, Khoa CNTT, ĐH KHTN, ĐHQG TPHCM
- Cấu hình EtherSwitch Router trên GNS3 thực hiện dựa trên hướng dẫn ở video sau:
<https://www.youtube.com/watch?v=JINfwm9ywB0>

3. Nội dung thực hiện

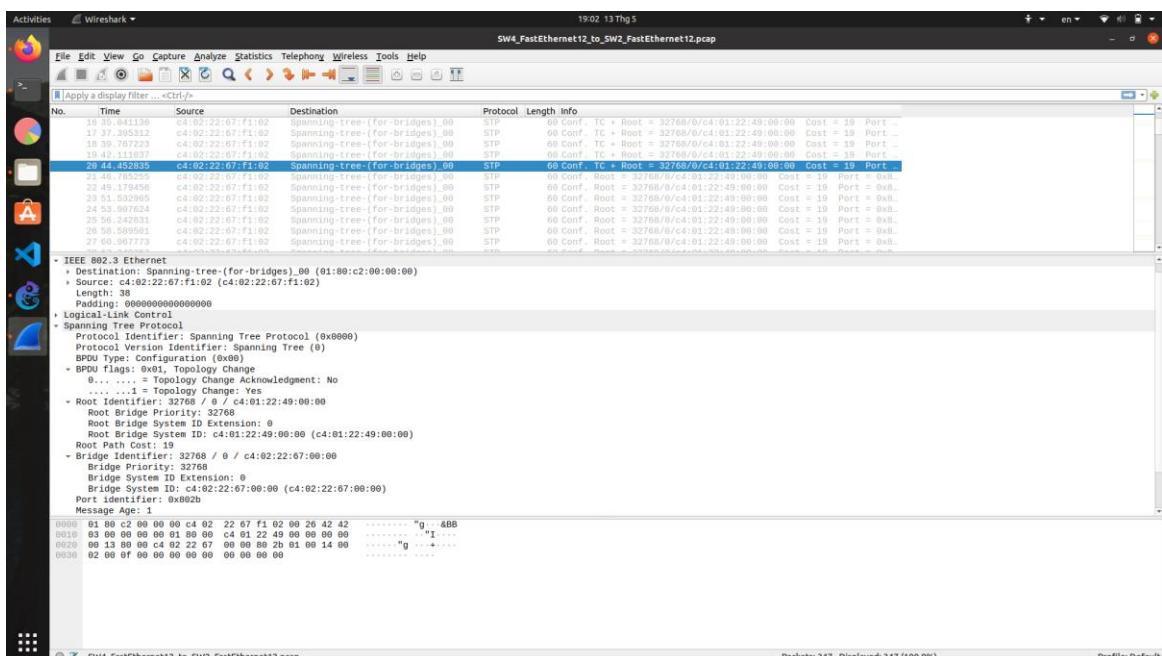
a. Bài 1. Thiết lập mô hình cho giao thức STP



Thứ tự khởi động các switch như sau: **SW1 → SW2 → SW3 → SW4 → SW5**

Sử dụng công cụ bắt gói tin để xác định các thông số kỹ thuật

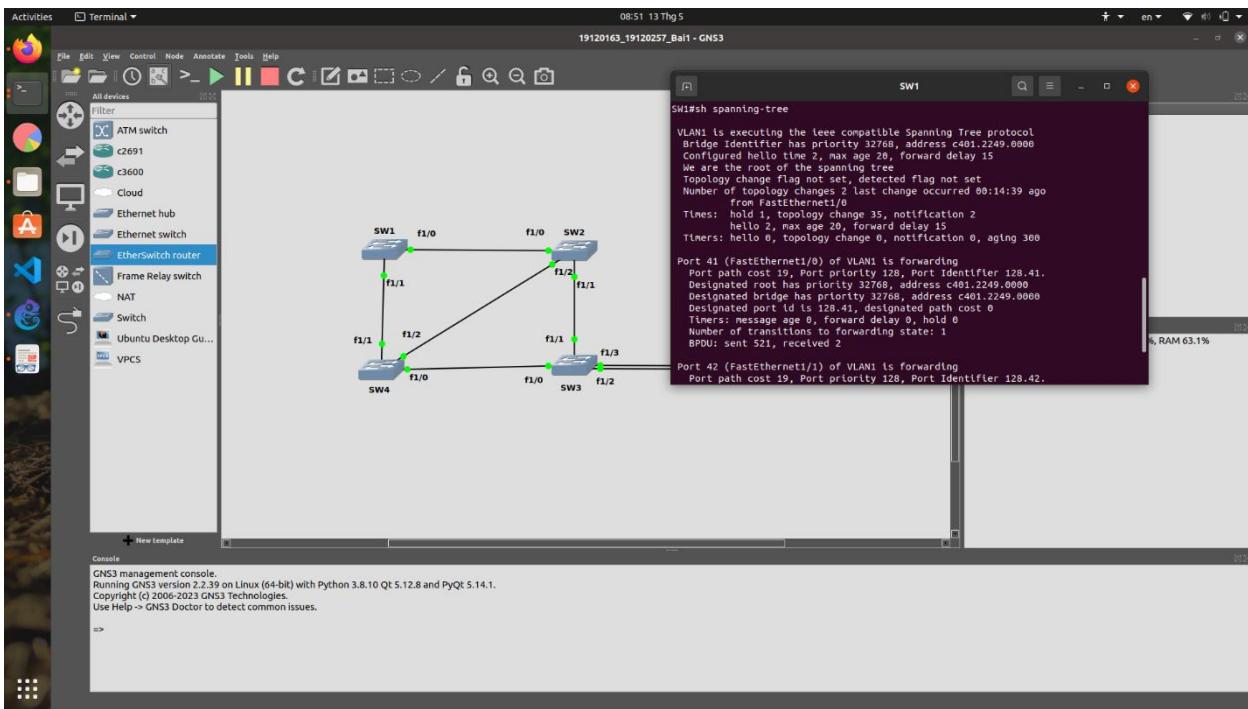
- Đặt công cụ bắt gói tin giữa **SW4 (cổng f1/2)** và **SW2 (cổng f1/2)** và lọc các gói tin STP để cho ra kết quả chi tiết sau đây (với gói tin số 20):



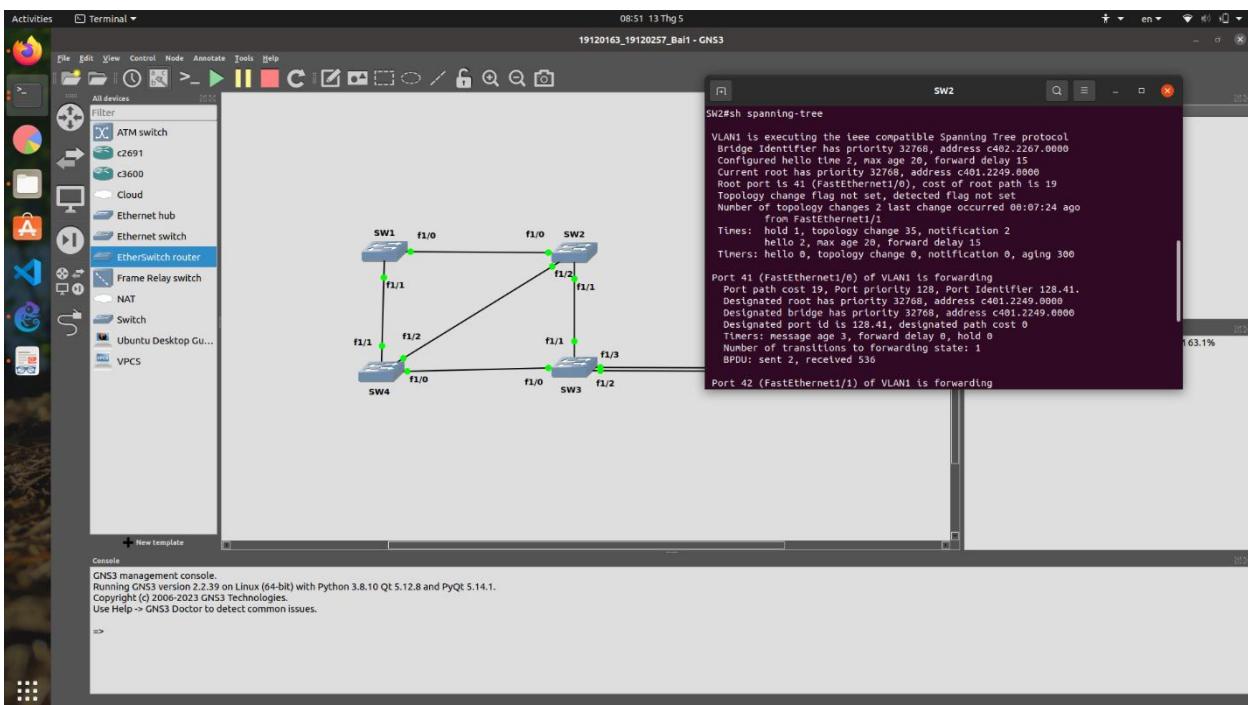
- Source MAC của gói tin: **C402.2267.F102**. Đây có khả năng là địa chỉ SW2 (do phần đầu của Bridge ID tại SW2 cũng là C402.2267)
- Destination MAC của gói tin: **0180.C200.0000**. Đây là địa chỉ của giao thức STP dành riêng cho BPDU sinh ra bởi các thiết bị của Cisco trên các đường trunk và **chỉ dành riêng cho VLAN1**. Đối với các VLAN khác thì địa chỉ này là **0100.0CCC.CCCD**
- BPDU Type: **Configuration (0x00)**
- Root Identifier: **SW1** (Độ ưu tiên: **32768**, Phần mở rộng ID: 0, Root ID: **C401.2249.0000**)
- Root Path Cost: **19**
- Bridge Identifier: **SW2** (Độ ưu tiên: **32768**, Phần mở rộng ID: 0, Bridge ID: **C402.2267.0000**)
- Port Identifier: **0x802B** (Thập phân: **128.43**, tức là cổng f1/2)

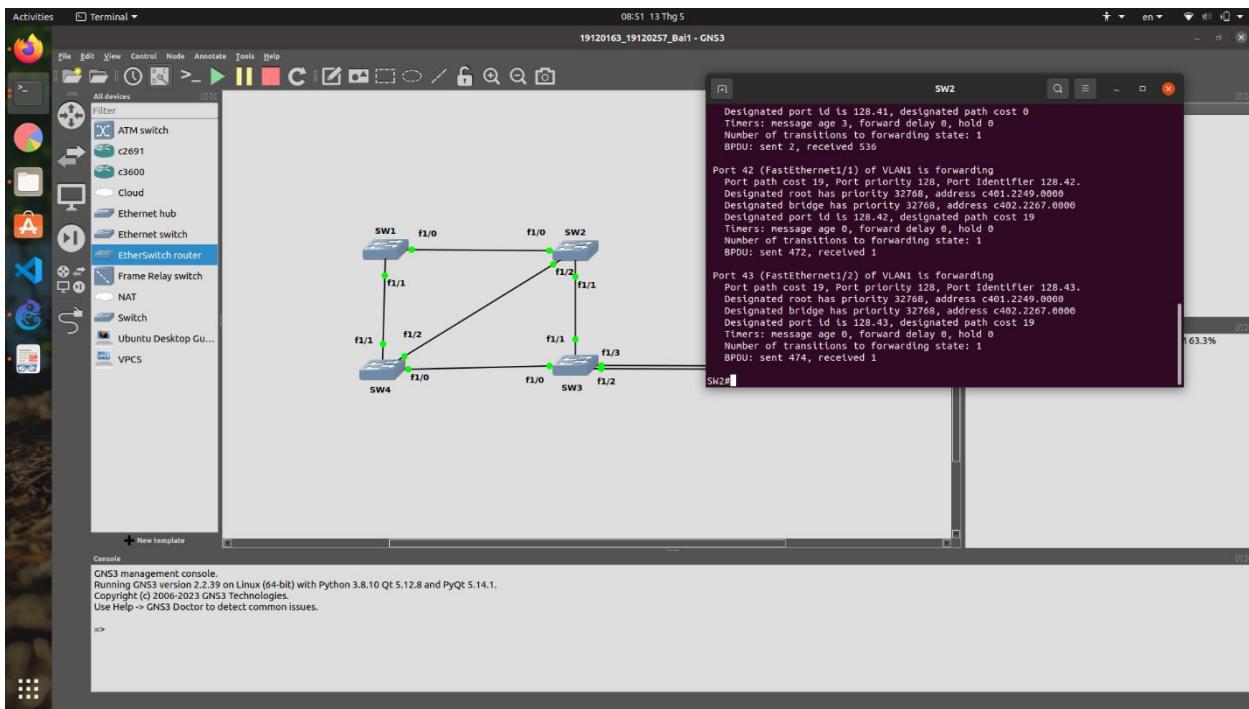
Sử dụng công cụ dòng lệnh để xác định các thông số kỹ thuật

- Sử dụng câu lệnh **Router(config)# show spanning-tree** để xem qua cấu hình hiện thời của giao thức STP.
- Kết quả xác định: Switch SW1 hiện thời đang giữ vai trò là Root của VLAN 1. (Được xác định bởi câu **We are the root of the spanning tree** hoặc **This bridge is the root**). Như vậy chắc chắn hai cổng f1/0 và f1/1 của SW1 là **Designated Ports** (xác định bởi lệnh **Forwarding/FWD**).

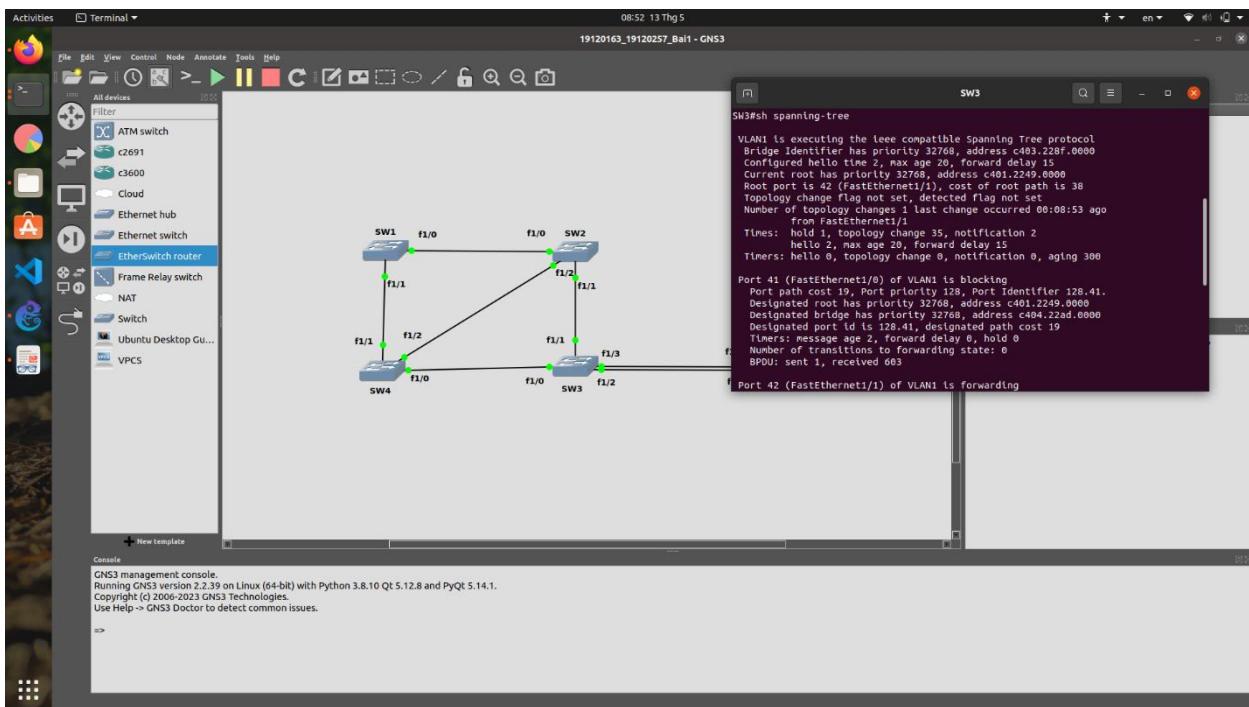


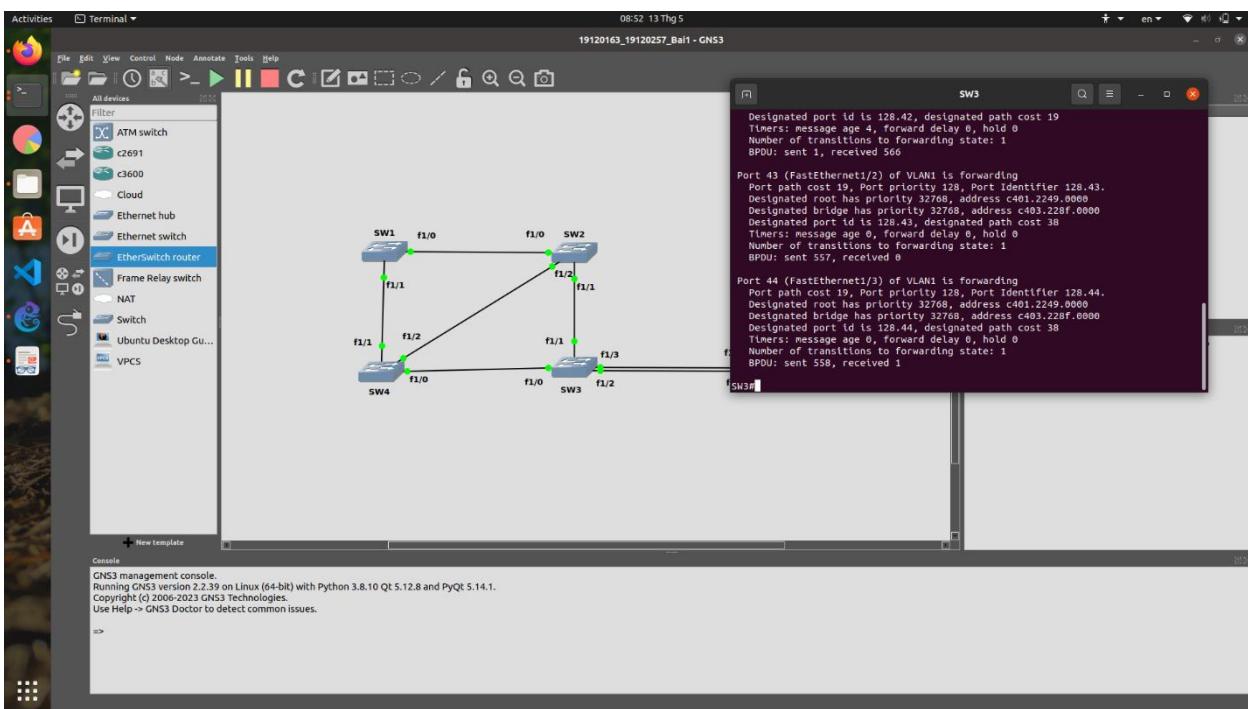
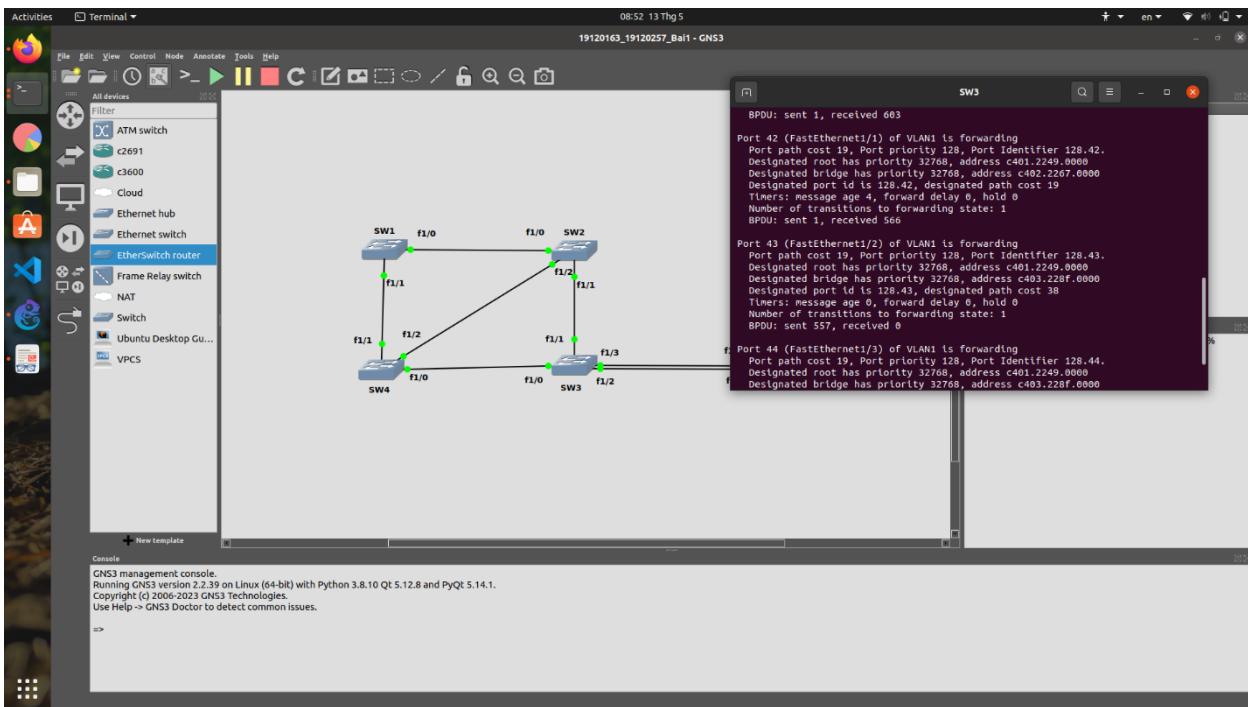
- SW2 có 3 cổng, trong đó như hai hình tiếp theo thì **Root Port** là f1/0. Hai cổng còn lại ở trạng thái Forwarding đều là **Designated Ports**.



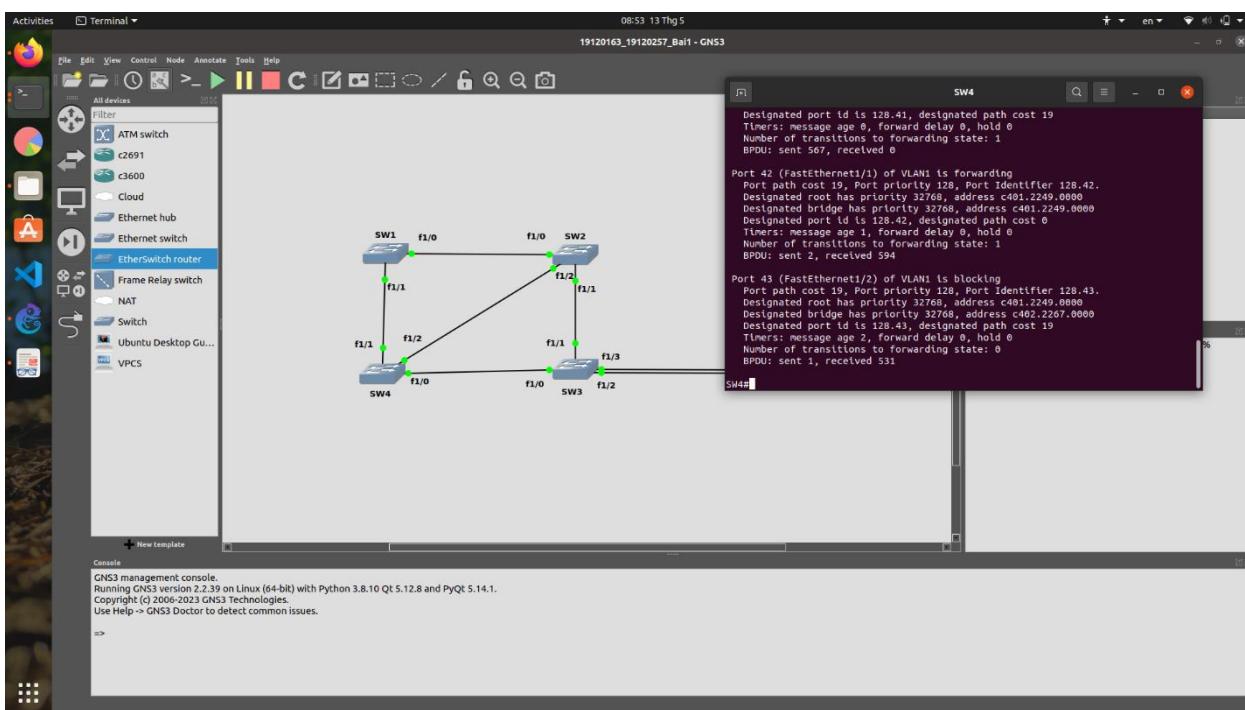
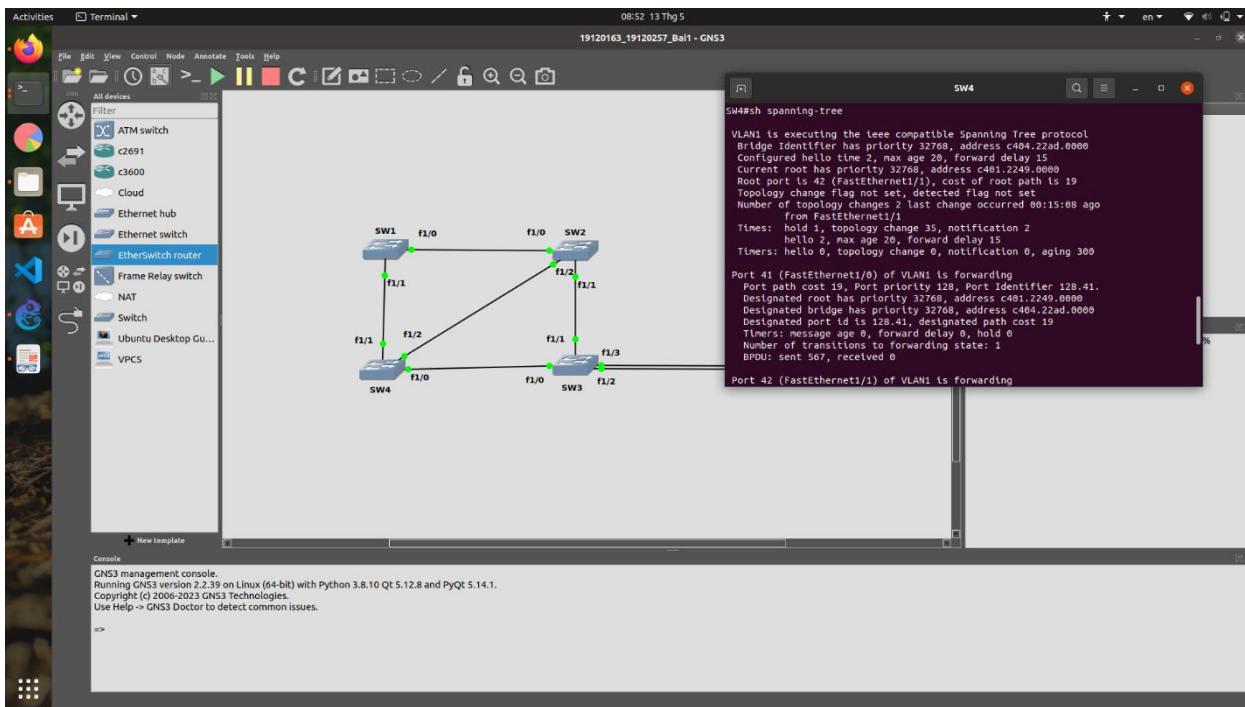


- SW3 có 4 cổng, trong đó, **Root Port** là f1/1. Cổng f1/2 và f1/3 đều ở trạng thái Forwarding là **Designated Ports**. Cổng f1/0 đang ở trạng thái **Blocking**, đồng nghĩa với việc đây là **Non-designated Port**.

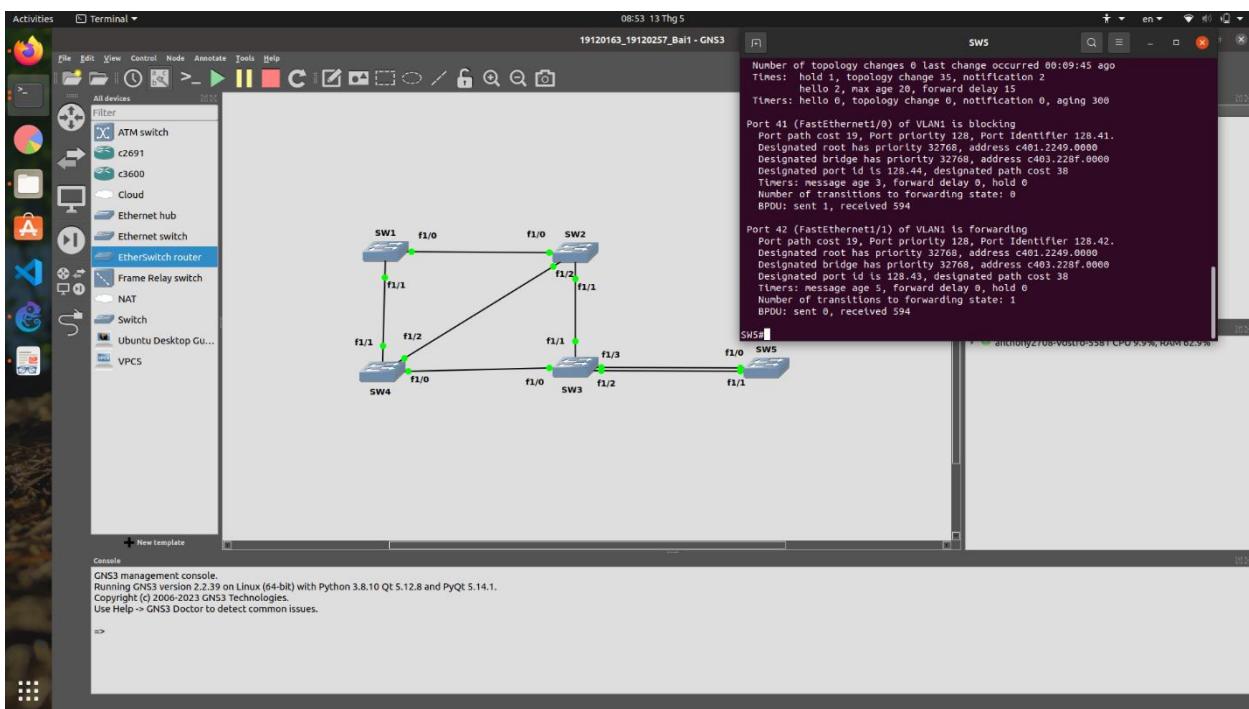
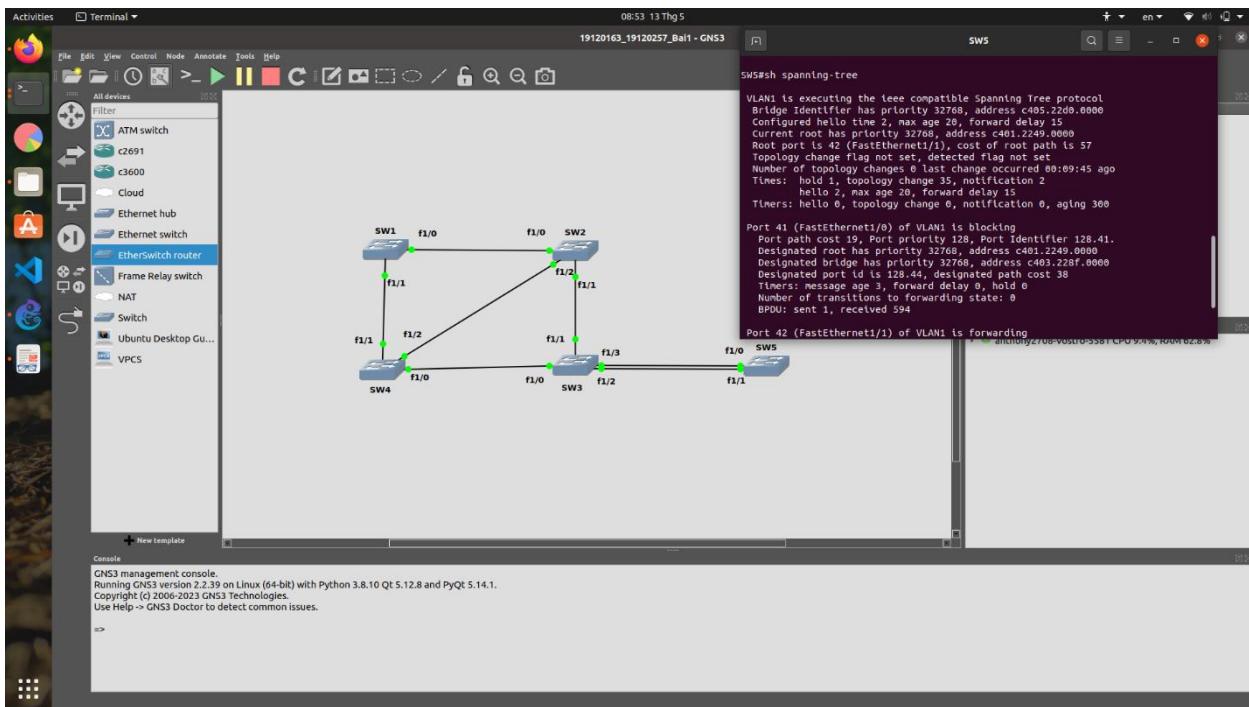




- SW4 có 3 cổng, trong đó duy nhất cổng f1/2 đang ở trạng thái **Blocking**, đồng nghĩa với việc đây là **Non-designated Port**. Cổng f1/1 đang là **Root Port**, còn cổng f1/0 ở trạng thái Forwarding là **Designated Port**.



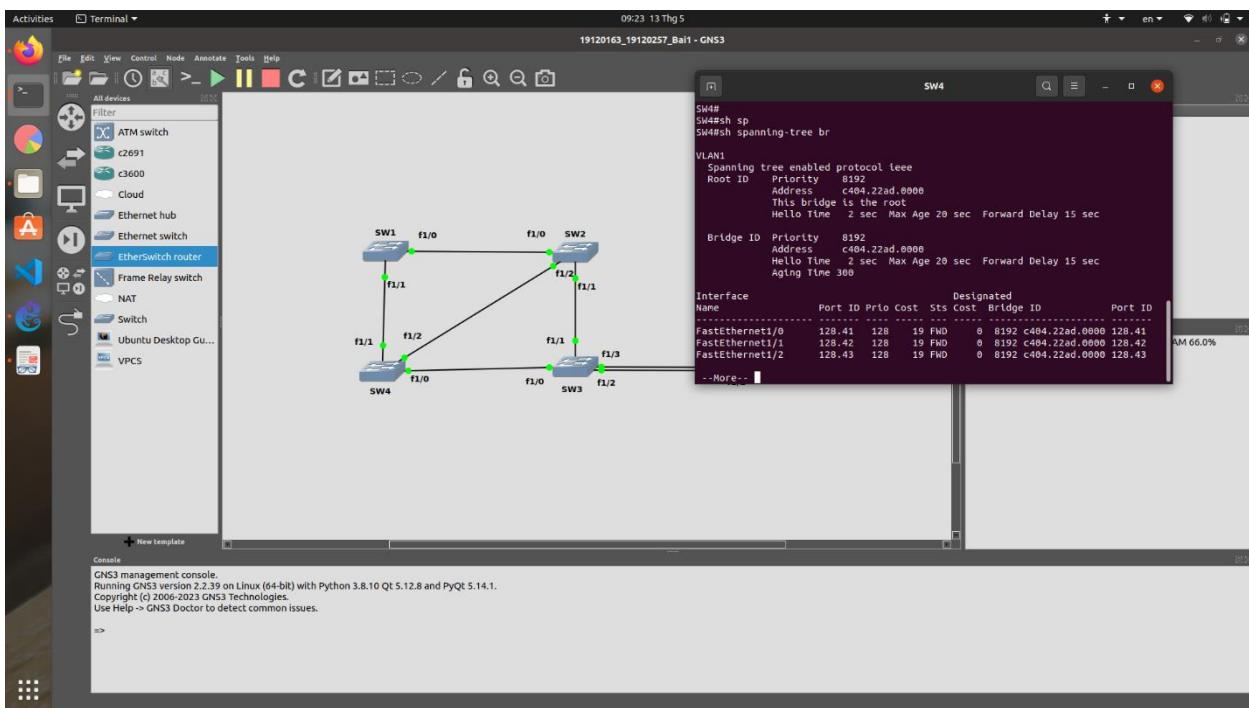
- SW5 có 2 cổng, trong đó cổng f1/1 đang là **Root Port**, còn cổng f1/0 đang ở trạng thái **Blocking**, đồng nghĩa với việc đây là **Non-designated Port**.



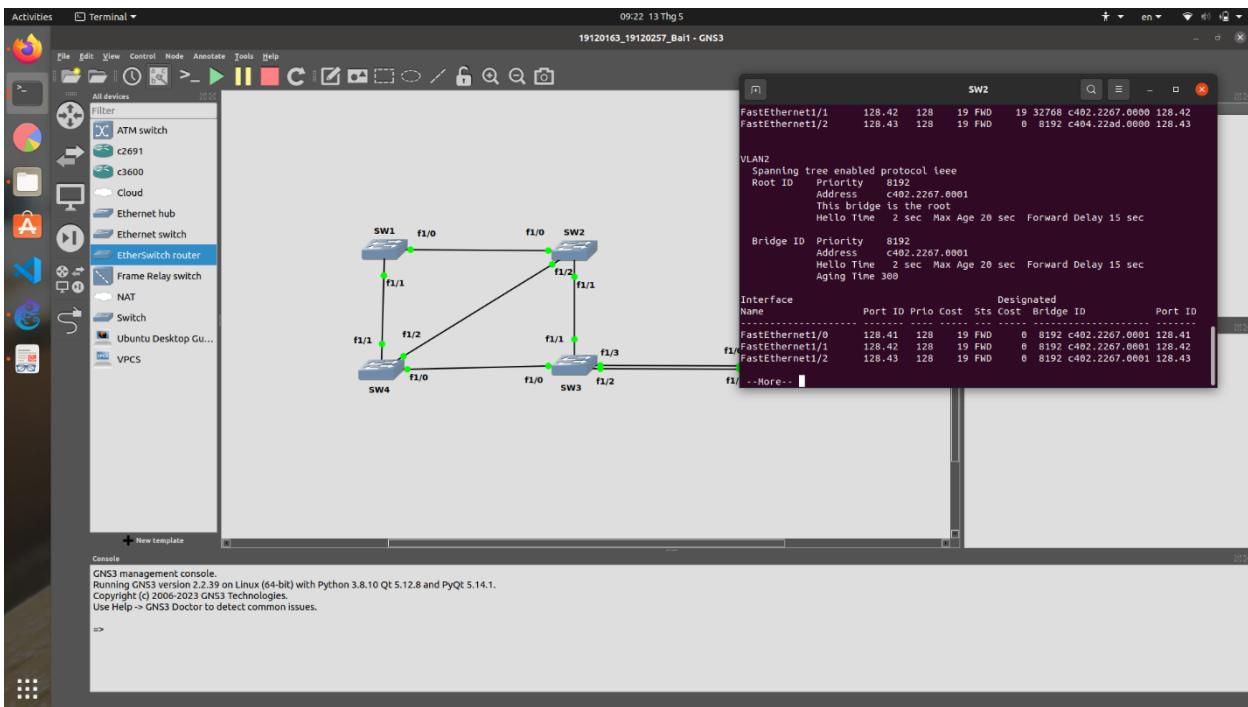
Tạo VLAN và can thiệp vào quá trình bầu chọn Root Bridge

- Sử dụng chùm câu lệnh sau để tạo VLAN trên tất cả các switch:
 - **Router# vlan database**
 - **Router(vlan)# vlan [mã]**
 - **Router(vlan)# apply**

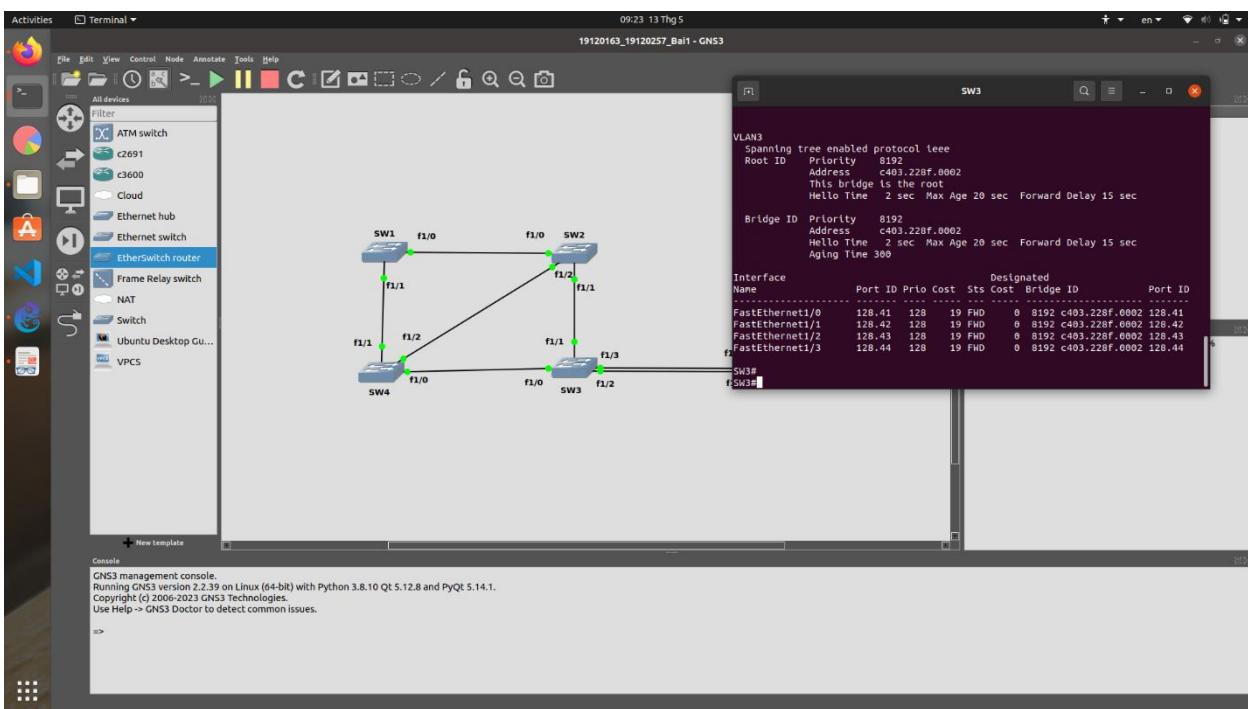
- Tiếp theo, chuyển các cổng thành chế độ trunk để sử dụng nhiều VLAN trên cùng đường truyền bằng câu lệnh **Router(config-if)# switchport mode trunk**.
- Tại các switch tương ứng, can thiệp bầu chọn bằng cách gõ lệnh **Router(config)# spanning-tree vlan [mã] root primary**. Sau đó kiểm tra kết quả tương ứng bằng lệnh: **Router(config)# show spanning-tree vlan [mã] brief**
 - SW4 làm Root cho VLAN1



- SW2 làm Root cho VLAN2

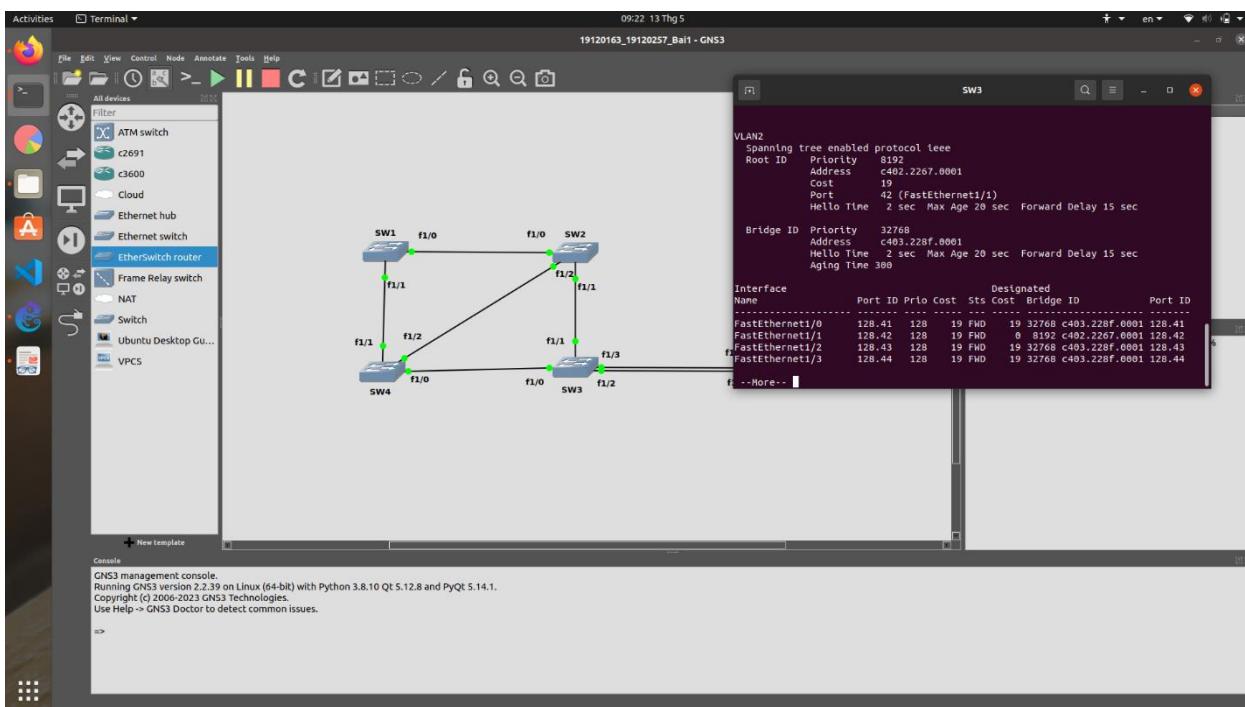
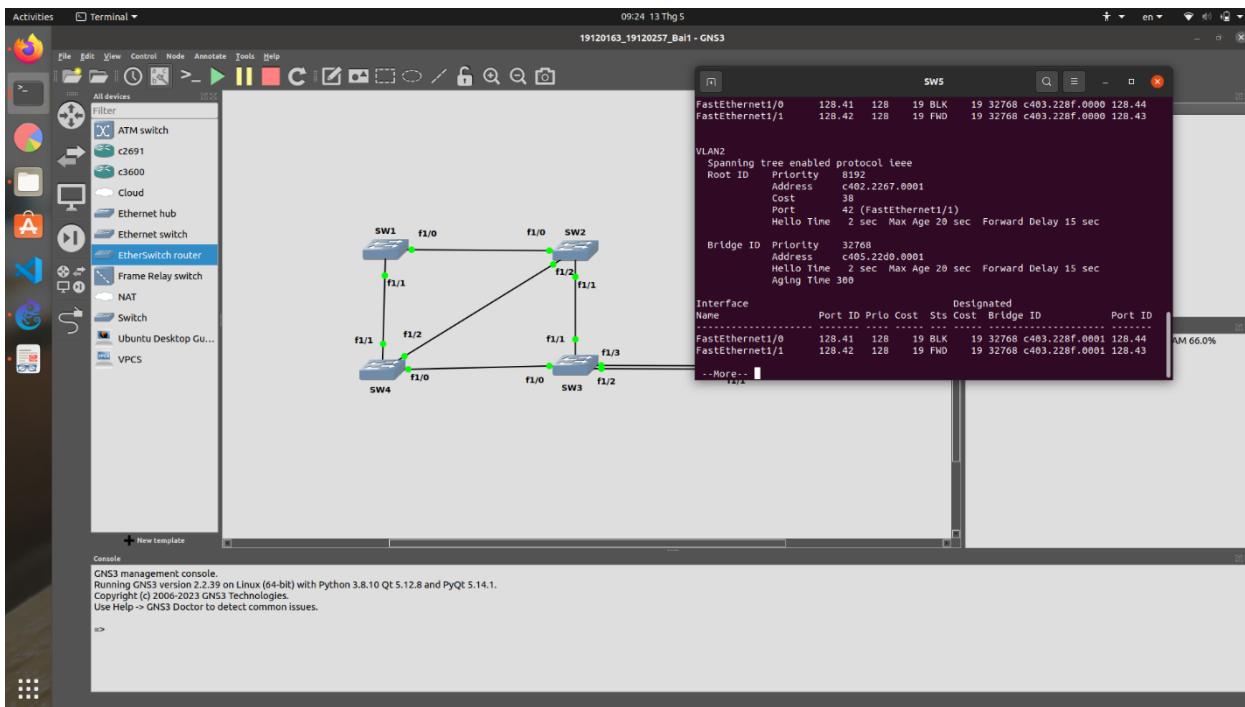


- SW3 làm Root cho VLAN3



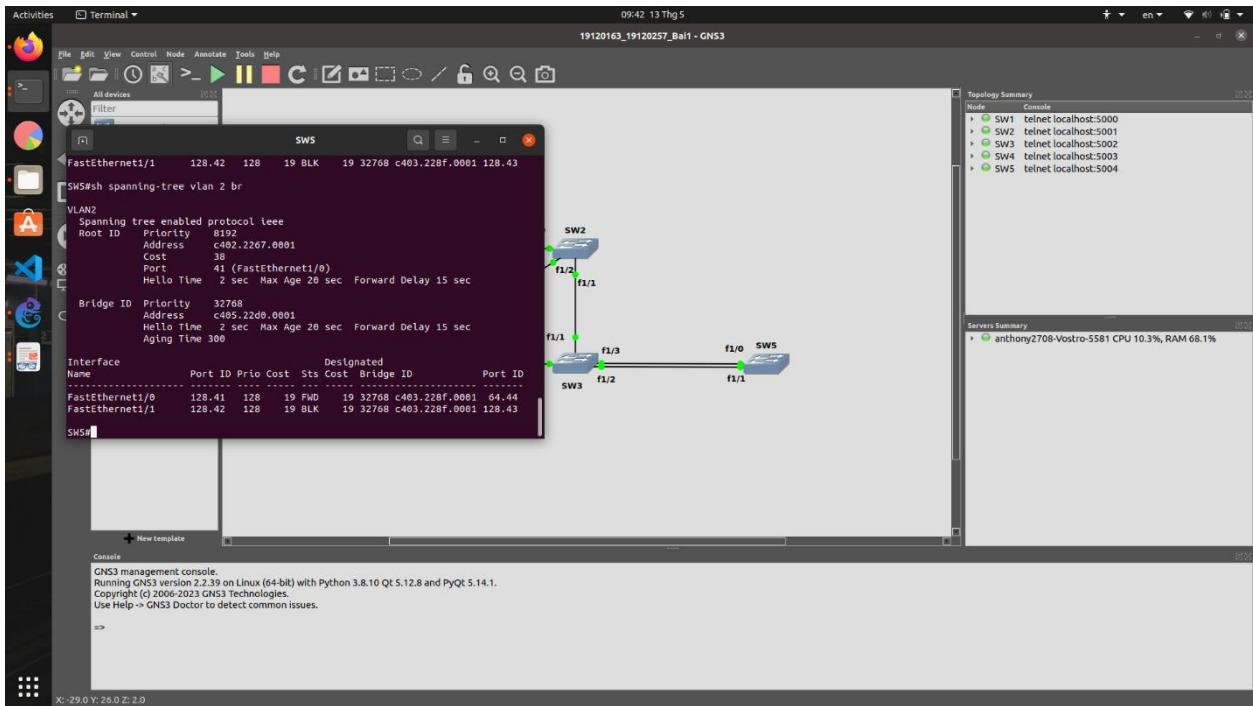
Đổi Root Port cho VLAN trên Switch

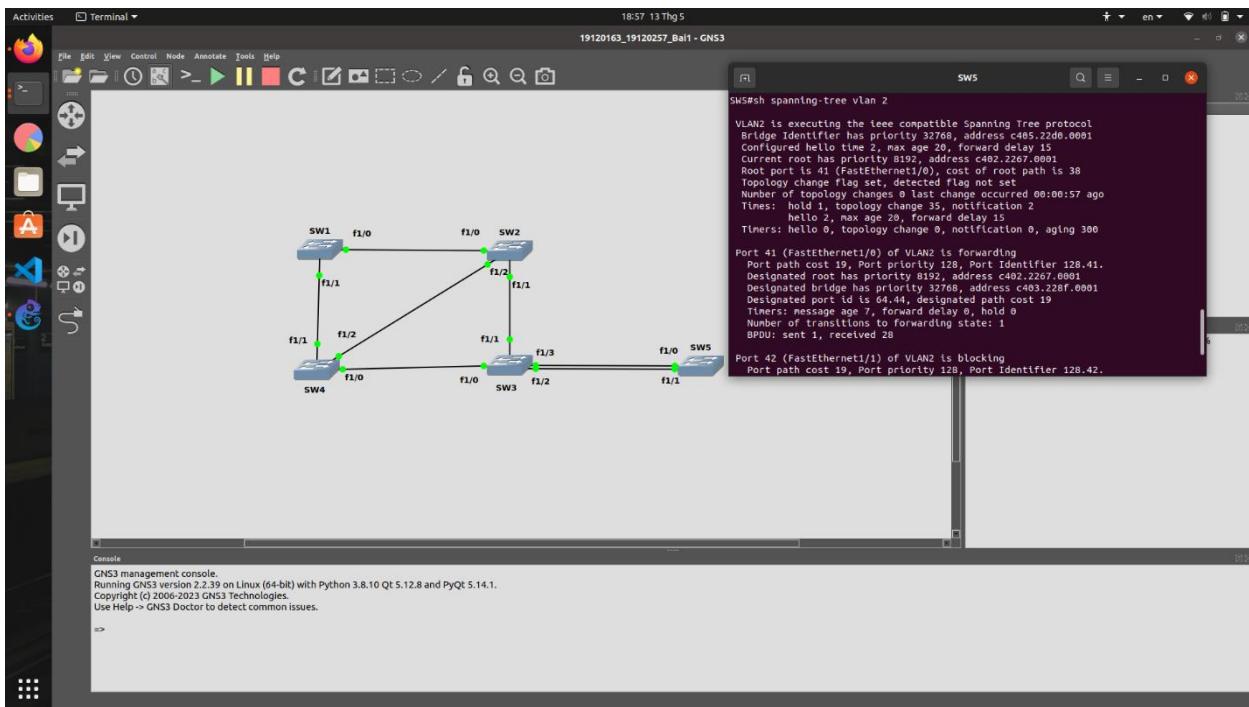
- Kiểm tra VLAN 2 tại SW5, ta thấy cổng f1/0 đang ở trạng thái **Blocking**.



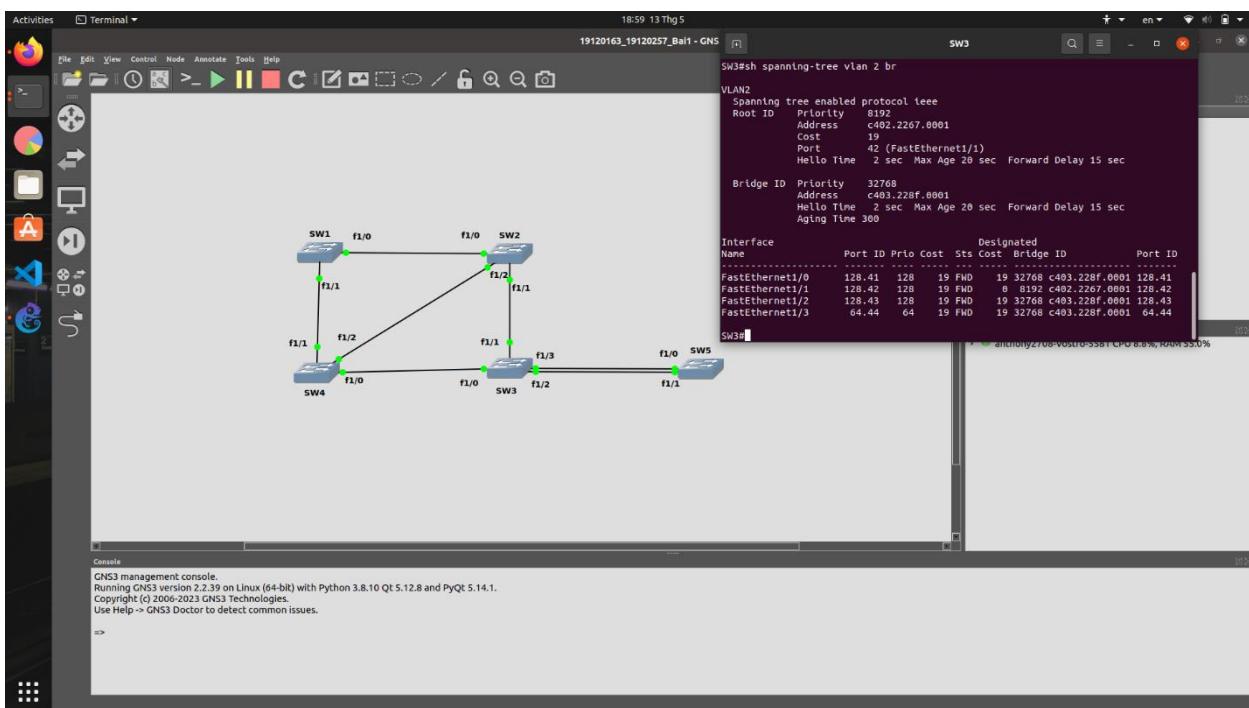
- Giữa SW3 và SW5 đang tồn tại 1 cặp đường dẫn, hai cổng đối diện với hai cổng f1/0 và f1/1 của SW5 lần lượt là f1/3 và f1/2 của SW3. Hai cổng f1/3 và f1/2 đều có địa chỉ Designated Bridge ID khớp với Bridge ID của SW3 nên đều là **Designated Ports**. Theo nguyên tắc lựa chọn Root Port, các tiêu chí sau đây sẽ được ưu tiên theo thứ tự từ cao xuống thấp:

- Chi phí Root Path nhỏ nhất
 - Designated Bridge ID nhỏ nhất
 - Designated Port ID nhỏ nhất: Gồm hai tiêu chí phụ là:
 - Độ ưu tiên nhỏ nhất
 - Số hiệu cổng nhỏ nhất
- Hiện thời thì cổng f1/1 của SW5 đang đối diện với f1/2 của SW3 có Port ID là **128.43** nhỏ hơn **128.44** (128 là độ ưu tiên, số còn lại là số hiệu cổng). Để chỉnh cho f1/0 của SW5 trở thành Root Port của VLAN 2 thì có hai lựa chọn, một là giảm chi phí Root Path xuống **nhỏ hơn 19** như hình, hai là hạ độ ưu tiên của cổng xuống **thấp hơn 128**. Ở đây ta chọn cách thứ 2:
- Vào SW3 và truy cập vào cổng f1/0, sau đó gõ câu lệnh sau: **Router(config-if)# spanning-tree vlan 2 port-priority 64**. Sau đó kết thúc bằng lệnh **end** và kiểm tra lại bằng lệnh **Router(config)# show spanning-tree vlan 2 brief**

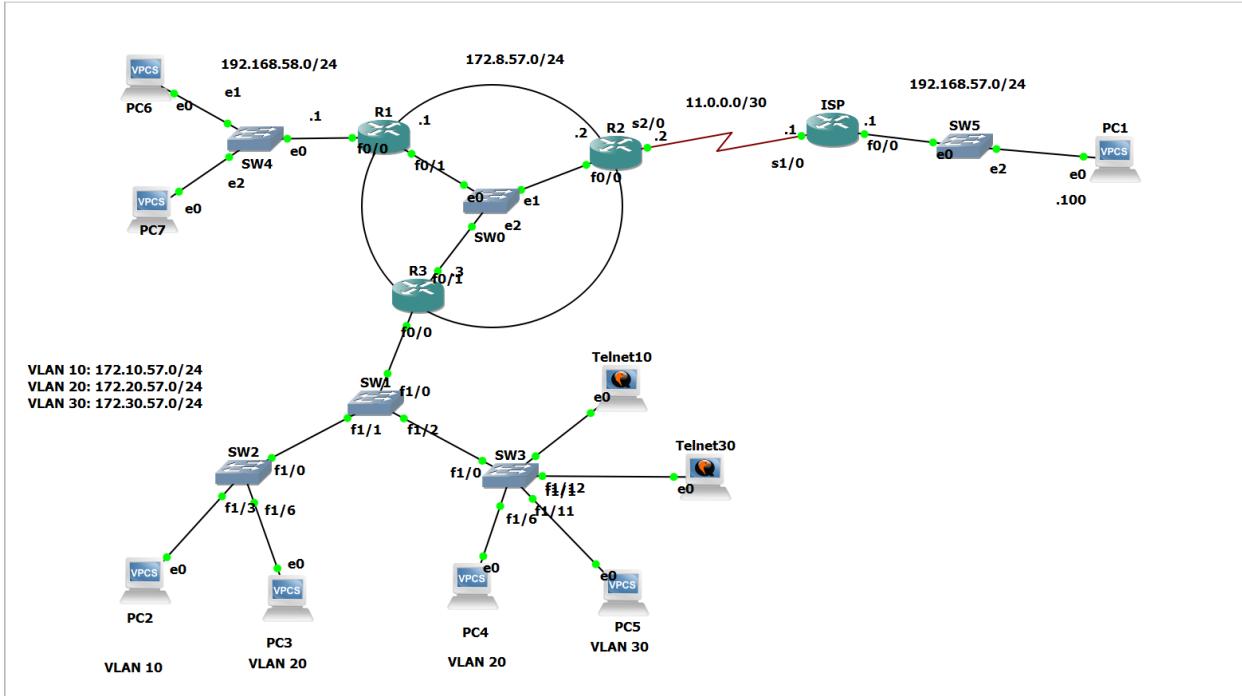




- Hình ảnh cho thấy, cổng f1/0 chuyển sang trạng thái **Forwarding**, đảo ngược kết quả hoàn toàn với thời điểm trước khi thực hiện. Như vậy, cổng f1/0 trở thành Root Port của VLAN 2 tại SW5. Ta cũng tiến hành kiểm tra kết quả sau khi thay đổi Root Port tại SW3.



b. Bài 2: Cấu hình VLAN, VTP, NAT, ACL



Cấu hình đúng địa chỉ IP cho các thiết bị với X=57 đúng với yêu cầu đề bài, riêng các địa chỉ của các máy tính trong đồ hình là:

- **PC2: 172.10.57.20/24, PC3: 172.20.57.30/24**
- **PC4: 172.20.57.40/24, PC5: 172.20.57.50/24**
- **PC6: 192.168.58.60/24, PC7: 192.168.58.70/24**

Ngoài ra còn nhóm cho thêm 2 máy tính chạy hệ điều hành Windows XP vào hai mạng con VLAN 10 và VLAN 20 có địa chỉ lần lượt là 172.10.57.100/24 và 172.30.57.100/24 để thực hiện kiểm tra ACL của telnet sau này.

Cấu hình VLAN, VTP

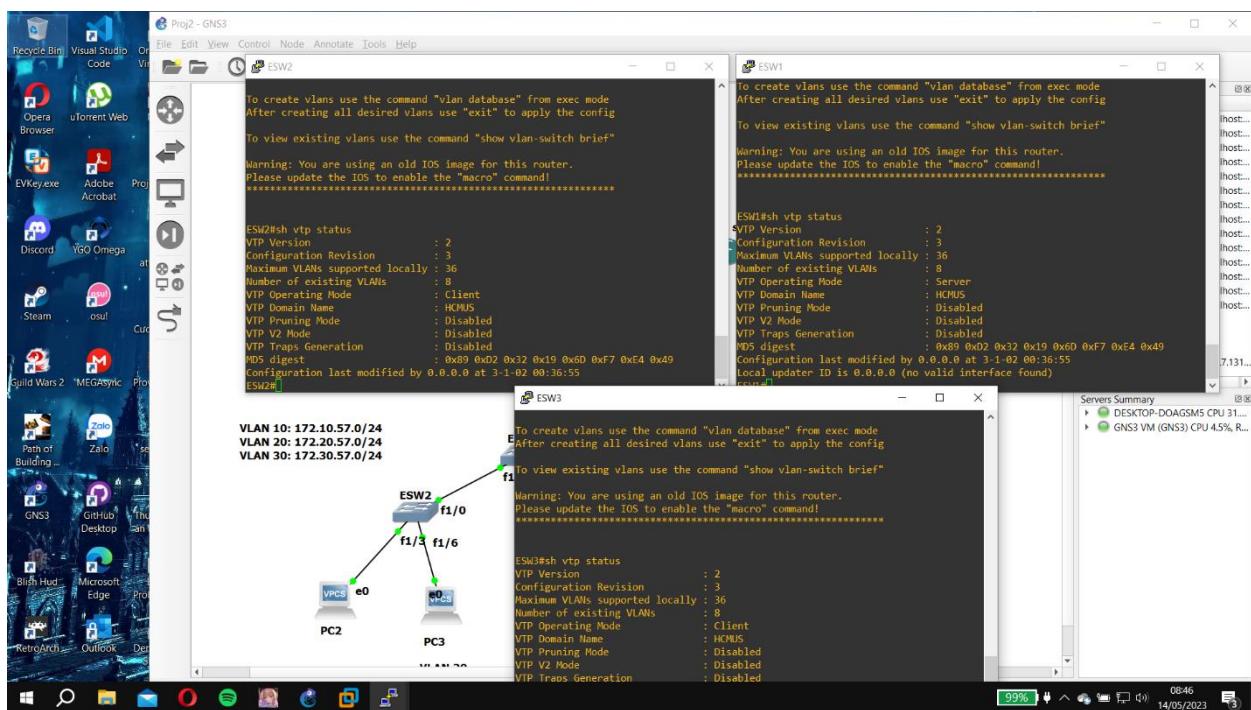
Ở trên SW1, ta sẽ tiến hành cài đặt trở thành VTP Server với các lệnh

- **SW1# vlan database**
- **SW1(vlan)# vtp server**
- **SW1(vlan)# vtp domain HCMUS**

Đối với các SW2 cài đặt trở thành VTP Client và cài đặt tương tự trên SW3

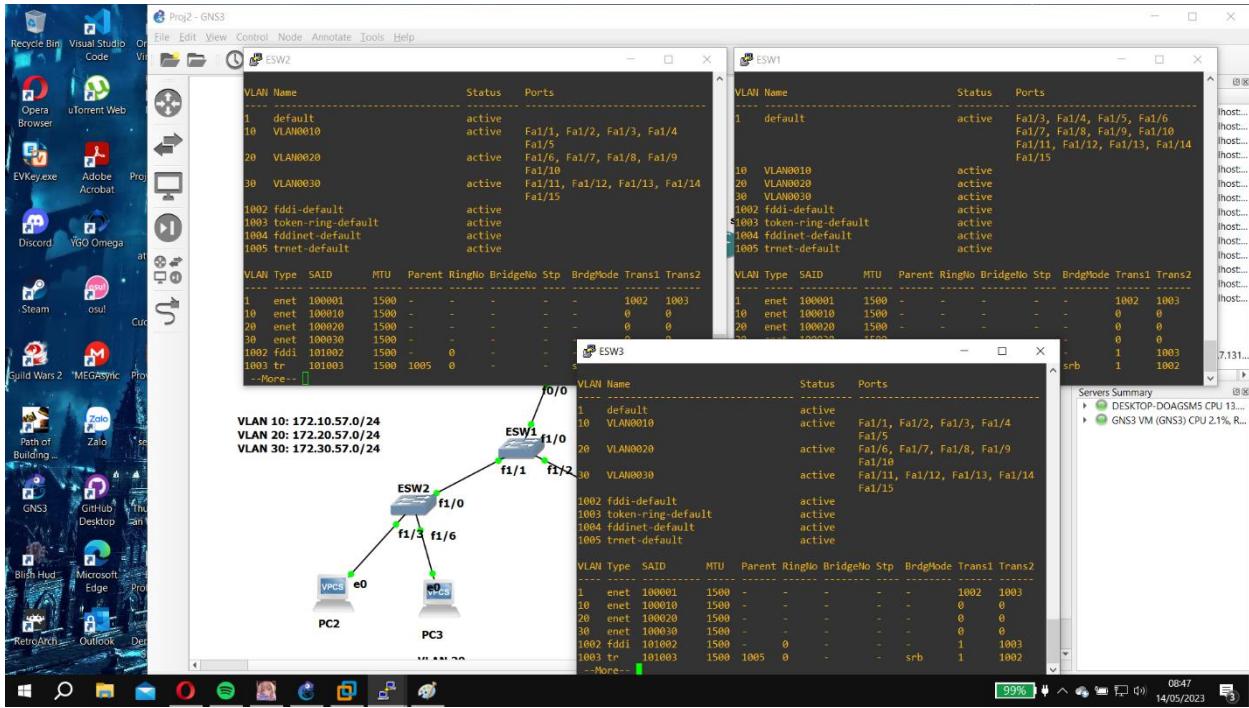
- **SW2# vlan database**
- **SW2(vlan)# vtp client**
- **SW2(vlan)# vtp domain HCMUS**

Để các thông tin VTP truyền cho nhau thì tất cả các cổng kết nối giữa 3 switch SW1, SW2 và SW3 được cấu hình công trunk bằng lệnh: **switchport mode trunk** và **switchport trunk encapsulation dot1q**. Sau khi cài đặt dùng lệnh **show vtp status** để kiểm tra:



Khi này việc khởi tạo 3 VLAN 10, 20 và 30 trên SW1 cũng sẽ tạo ra các VLAN trên các SW2, 3 với lệnh **SW1(vlan)# vlan [mã]**. Lệnh **SW1(vlan)# exit** dùng để switch ghi nhớ lại database sau khi chỉnh sửa

Cuối cùng sử dụng lệnh **show vlan-switch** để kiểm tra tình trạng VLAN trên các switch.



Để đưa các cổng lân lượt vào các VLAN ta sử dụng các lệnh sau

- **SW2(config)#int range f1/1 – 5**
- **SW2(config-if-range)# switchport access vlan 10**
- **SW2(config)#int range f1/6 – 10**
- **SW2(config-if-range)# switchport access vlan 20**
- **SW2(config)#int range f1/11 – 15**
- **SW2(config-if-range)# switchport access vlan 30**

Cấu hình định tuyến OSPF và NAT

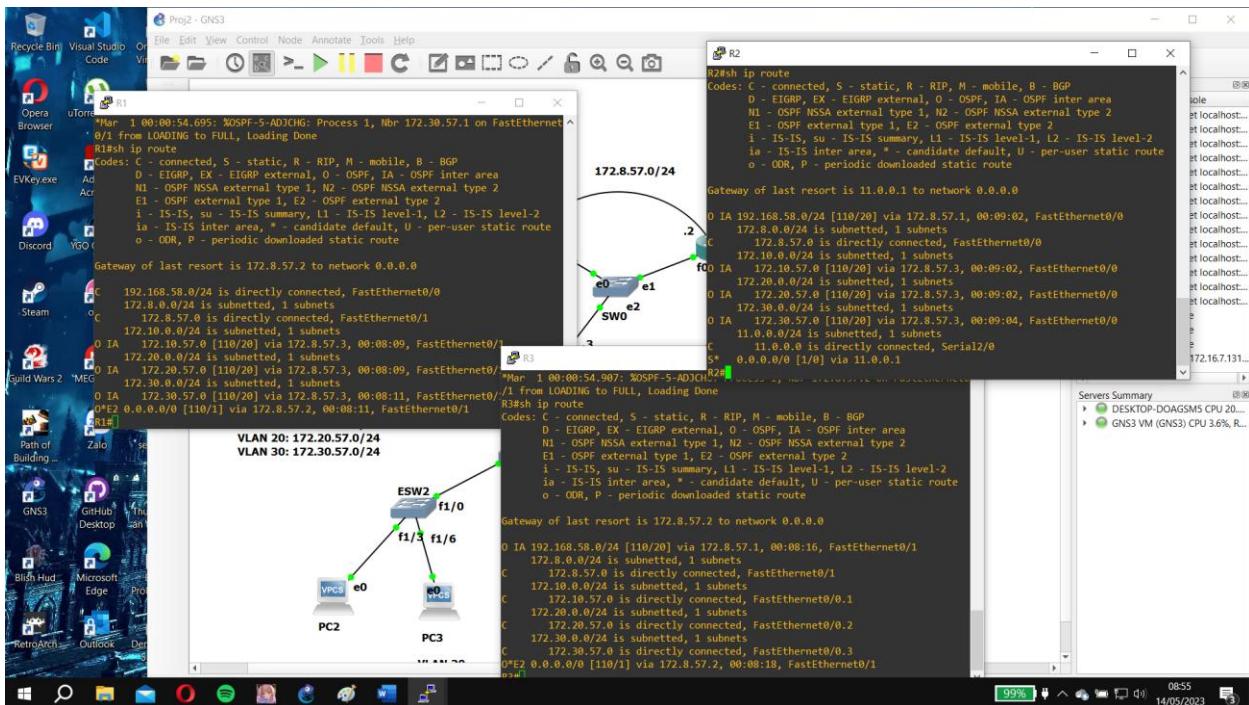
Cấu hình OSPF để định tuyến trên các router R1, R2 và R3 như sau:

- Trên Router R1:
 - o **R1(config)# router ospf 1**
 - o **R1(config-router) # network 172.8.57.0 0.0.0.255 area 0**
 - o **R1(config-router) # network 192.168.58.0 0.0.0.255 area 1**
- Trên Router R2:
 - o **R1(config)# router ospf 1**
 - o **R1(config-router) # network 172.8.57.0 0.0.0.255 area 0**

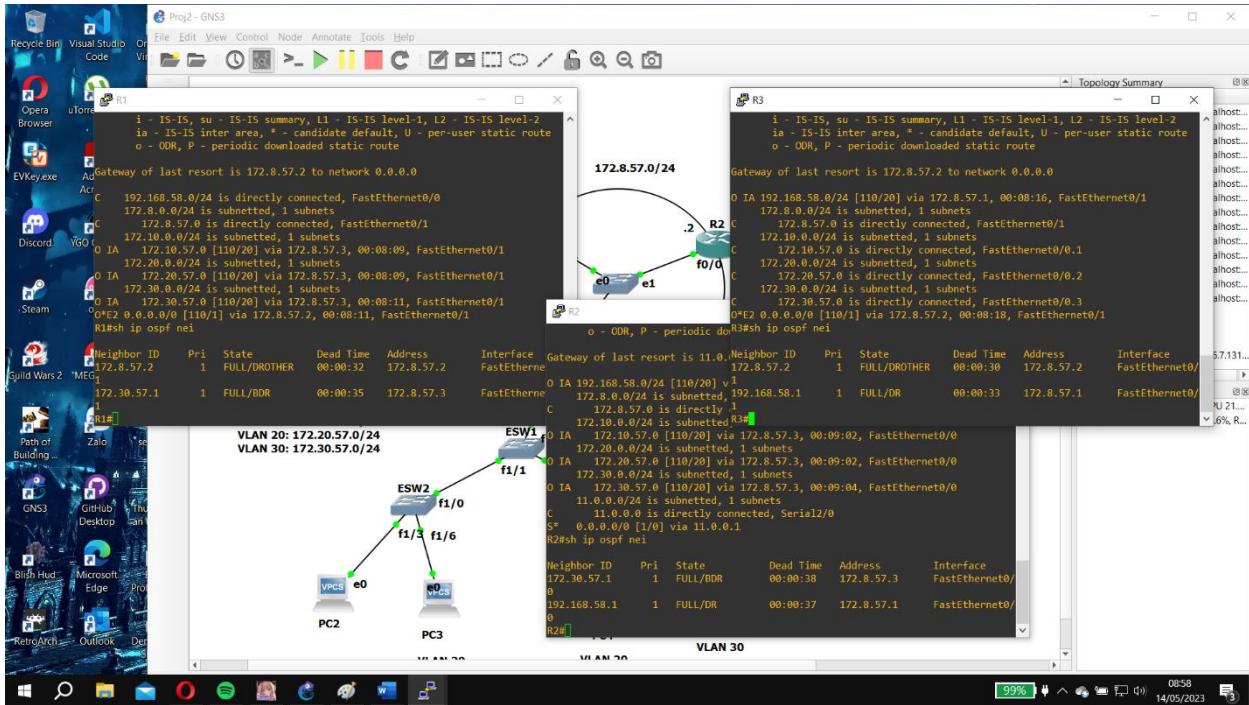
- Trên Router R3:

- **R3(config)# router ospf 1**
- **R3(config-router) # network 172.8.57.0 0.0.0.255 area 0**
- **R3(config-router) # network 172.0.0.0 0.255.255.255 area 2**

Kiểm tra lại bảng định tuyến của các Router sau khi cấu hình



Trong cấu hình trên, các Router kết nối tạo thành một Multiaccess network nên DR cũng như BDR được bầu chọn. Trong đó DR sẽ là Router 1 vì có địa chỉ **192.168.58.1/24** là địa chỉ lớn nhất trong các cổng và BDR sẽ là Router 3 vì có địa chỉ sub-interface cho VLAN 3 là **172.30.57.1/24** là địa chỉ lớn thứ hai



Để cấu hình cho các VLAN có thể trao đổi thông tin với nhau, ta sẽ chuyển đường kết nối từ SW1 lên R3 thành đường trunk và tiến hành tạo các sub-interface cho f0/0 của R3 bằng các lệnh:

- **R3(config)# interface f0/0.1**
- **R3(config-subif)# ip address 172.10.57.1 255.255.255.0**
- **R3(config-subif)# encapsulation dot1q 10**
- **R3(config-subif)# interface f0/0.2**
- **R3(config-subif)# ip address 172.20.57.1 255.255.255.0**
- **R3(config-subif)# encapsulation dot1q 20**
- **R3(config-subif)# interface f0/0.3**
- **R3(config-subif)# ip address 172.30.57.1 255.255.255.0**
- **R3(config-subif)# encapsulation dot1q 30**

Để cấu hình NAT (**chuyển địa chỉ khi kết nối ra ngoài mạng Internet**) trước tiên ta cần cấu hình 1 access-list cho phép dữ liệu từ bên trong mạng nội bộ ra ngoài thông qua Router biên R2 như sau:

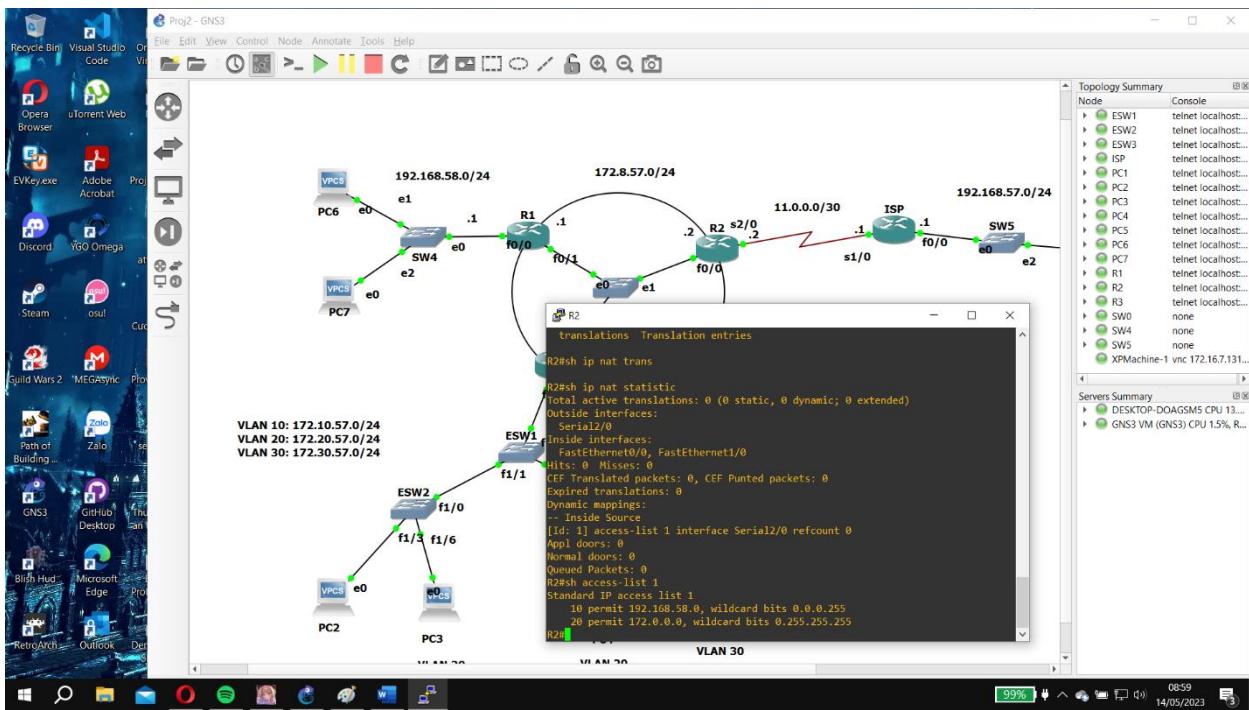
- **R2(config)# access-list 1 permit 192.168.58.0 0.0.0.255**

- **R2(config)# access-list 1 permit 172.0.0.0 0.255.255.255**

Access-list này sẽ cho phép các thiết bị bên trong mạng nội bộ đi ra ngoài Internet. Tiếp theo, ta sẽ cài đặt NAT Overload dựa trên access-list vừa tạo

- **R2(config)# ip nat inside source list 1 interface Serial2/0 overload**
- **R2(config)# interface f0/0**
- **R2(config-if)# ip nat inside**
- **R2(config-if)# interface s2/0**
- **R2(config-if)# ip nat outside**

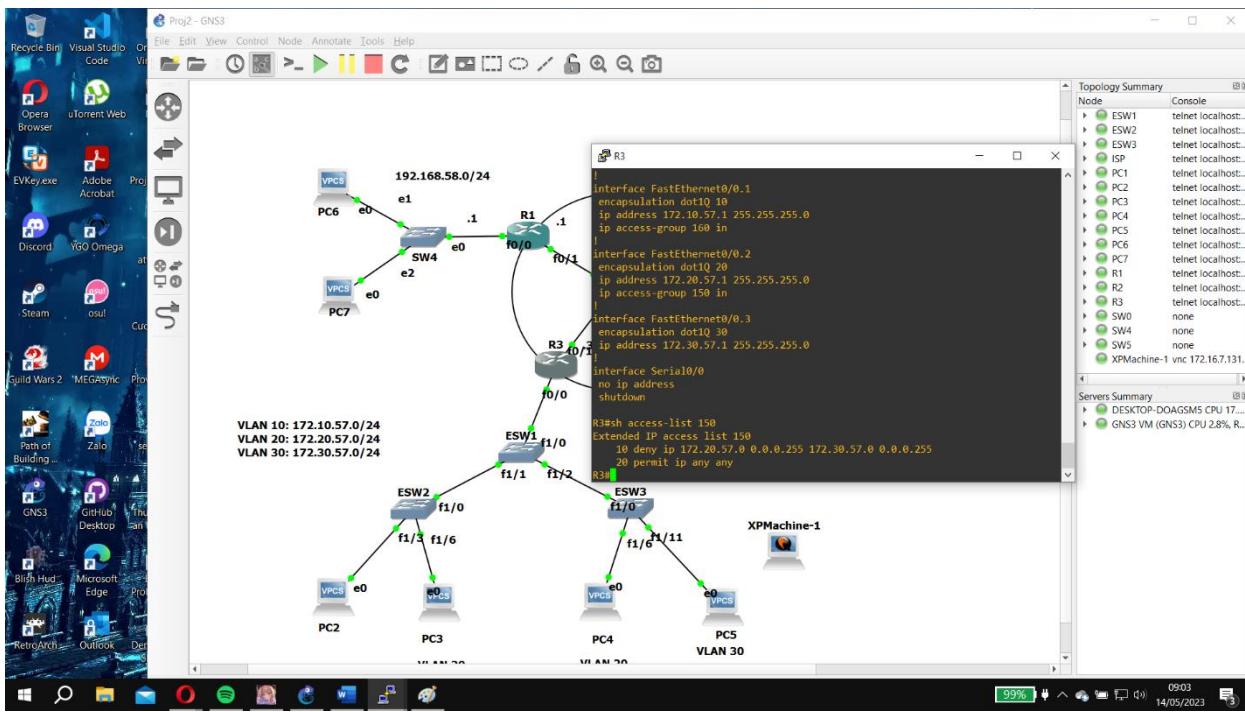
Kiểm tra lại cấu hình vừa cài đặt bằng lệnh **show ip nat statistics**



Cấu hình ACL

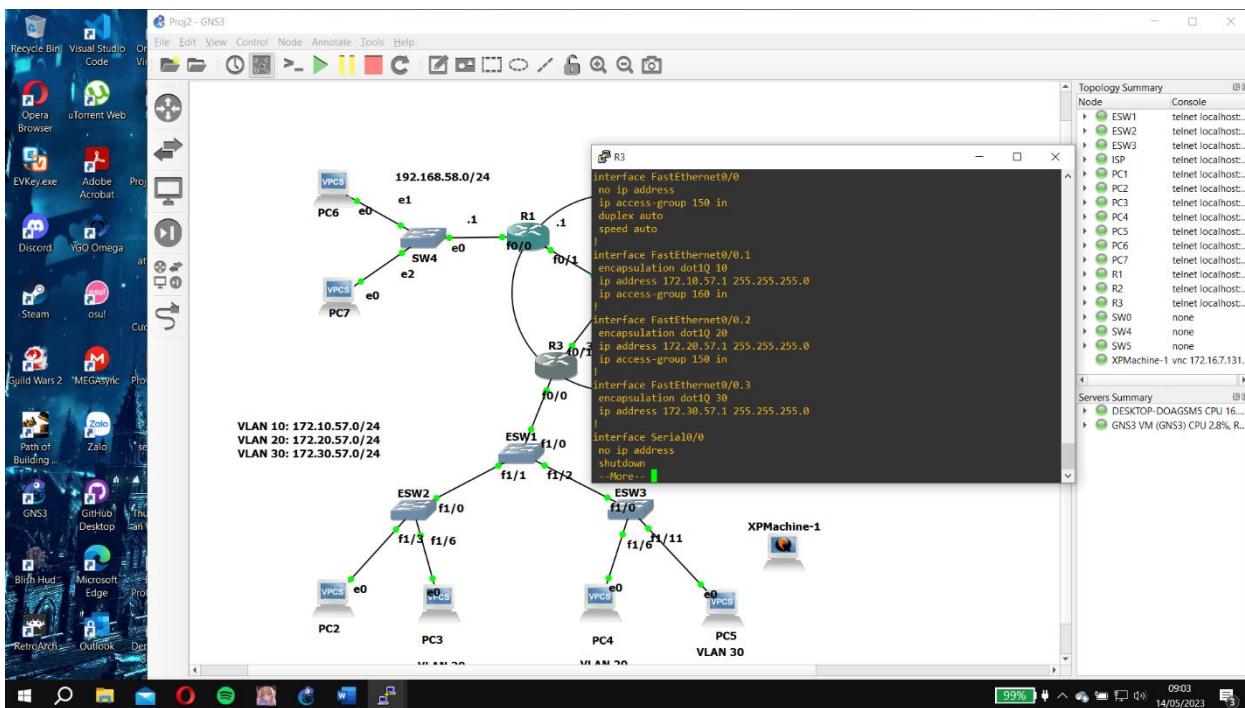
Cấu hình để các host trên VLAN 20 không truy cập được các host trên VLAN 30. Ta sẽ cấu hình ACL chặn các kết nối có nguồn xuất phát từ VLAN 20 và đích đến VLAN 30

- **R3(config)# access-list 150 deny ip 172.20.57.0 0.0.0.255 172.30.57.0 0.0.0.255**
- **R3(config)# access-list 150 permit ip any any**



Tiếp theo ta sẽ đặt access-list này tại cổng vào sub-interface f0/0.2 vì để có thể định tuyến sang các VLAN khác các thiết bị cần phải đi qua các sub-interface của R3 ứng với VLAN của host

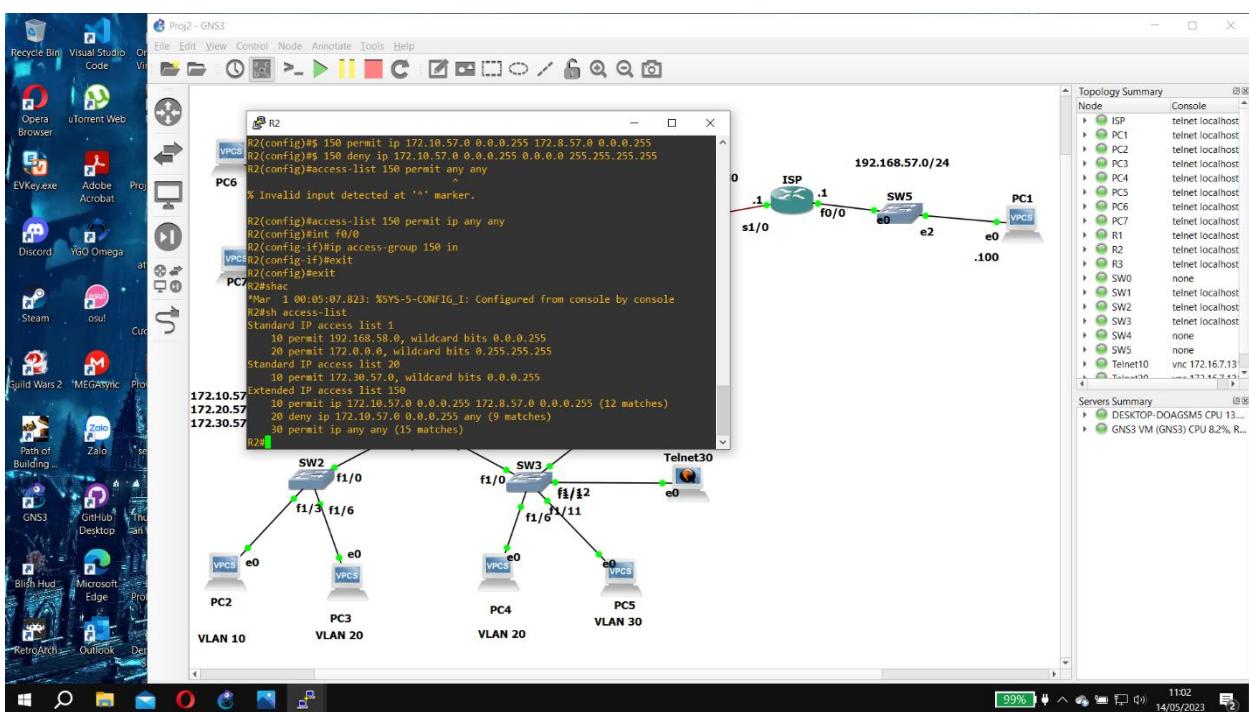
- **R3(config)# int f0/0.3**
- **R3(config-subif)# ip access-group 150 in**



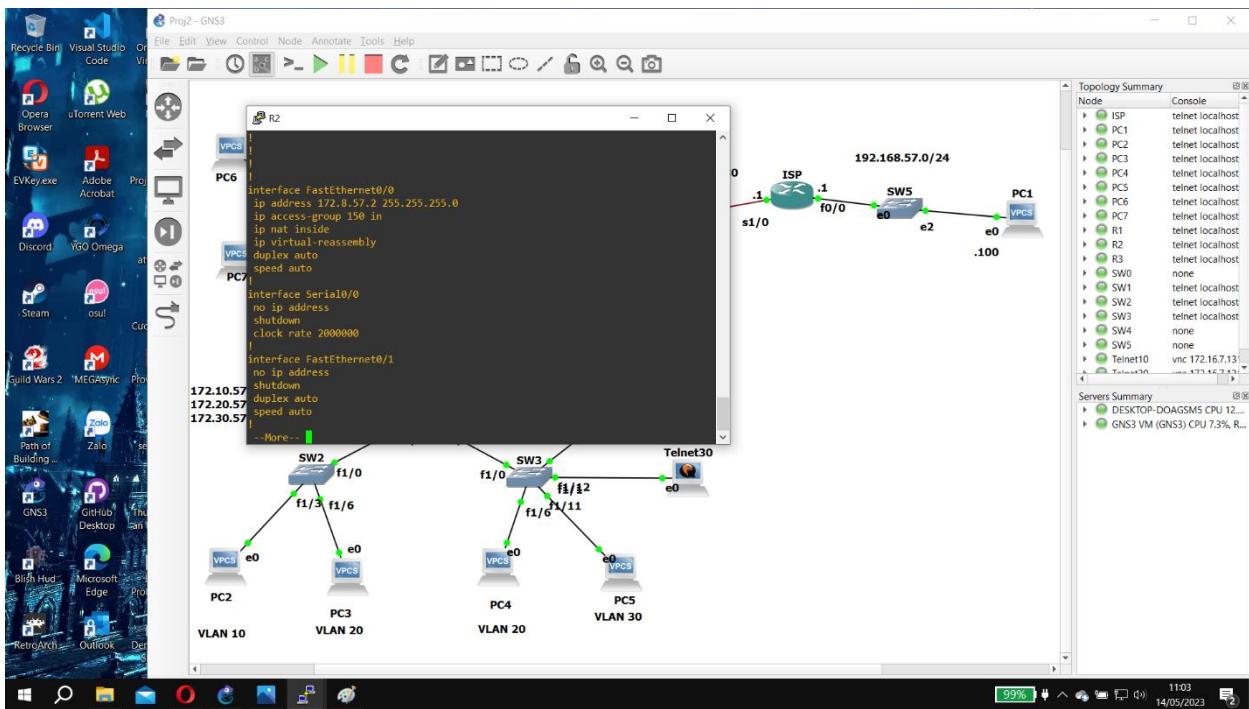
Cấu hình để các host thuộc VLAN 10 không truy cập được Internet. Vì Router biên R2 là thiết bị kết nối đến ISP ra Internet nên ta sẽ đặt ACL trên Router R2:

- R2(config)# access-list 150 permit ip 172.10.57.0 0.0.0.255 172.8.57.0 0.0.0.255
 - R2(config)# access-list 150 deny ip 172.10.57.0 0.0.0.255 any
 - R2(config)# access-list 150 permit ip any any

Trong này dòng đầu tiên sẽ cho phép VLAN vẫn có thể truy cập đến R2 cũng như các kết nối cần đi qua cổng f0/0 của R2 tuy nhiên không thể truy cập ra ngoài Internet



Đặt access-list trên tại hướng vào của cổng 0/0 để nhận dạng vào loại gói tin từ VLAN 10 muốn ra ngoài Internet



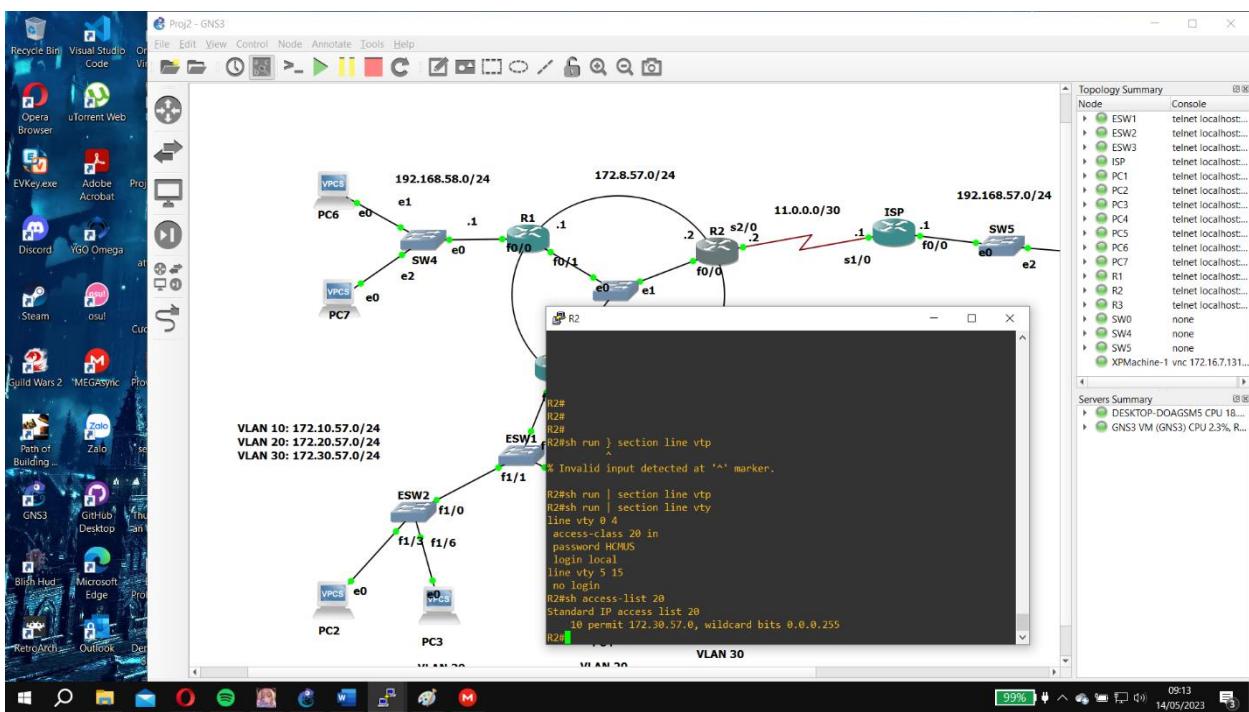
Cấu hình ACL chỉ cho phép VLAN 30 được telnet đến Router R2. Để cấu hình ACL trên ta sẽ tiến hành cài đặt telnet cho R2

- **R2(config)# line vty 0 4**
- **R2(config-line)# password HCMUS**
- **R2(config-line)# login**
- **R2(config-line)# line vty 5 15**
- **R2(config-line)# no login**

Sau khi cài đặt xong cấu hình telnet ta sẽ cài đặt access list cho phép VLAN 30 truy cập bằng telnet thông qua lệnh: **R2(config)# access-list 20 permit 172.30.57.0 0.0.0.255**

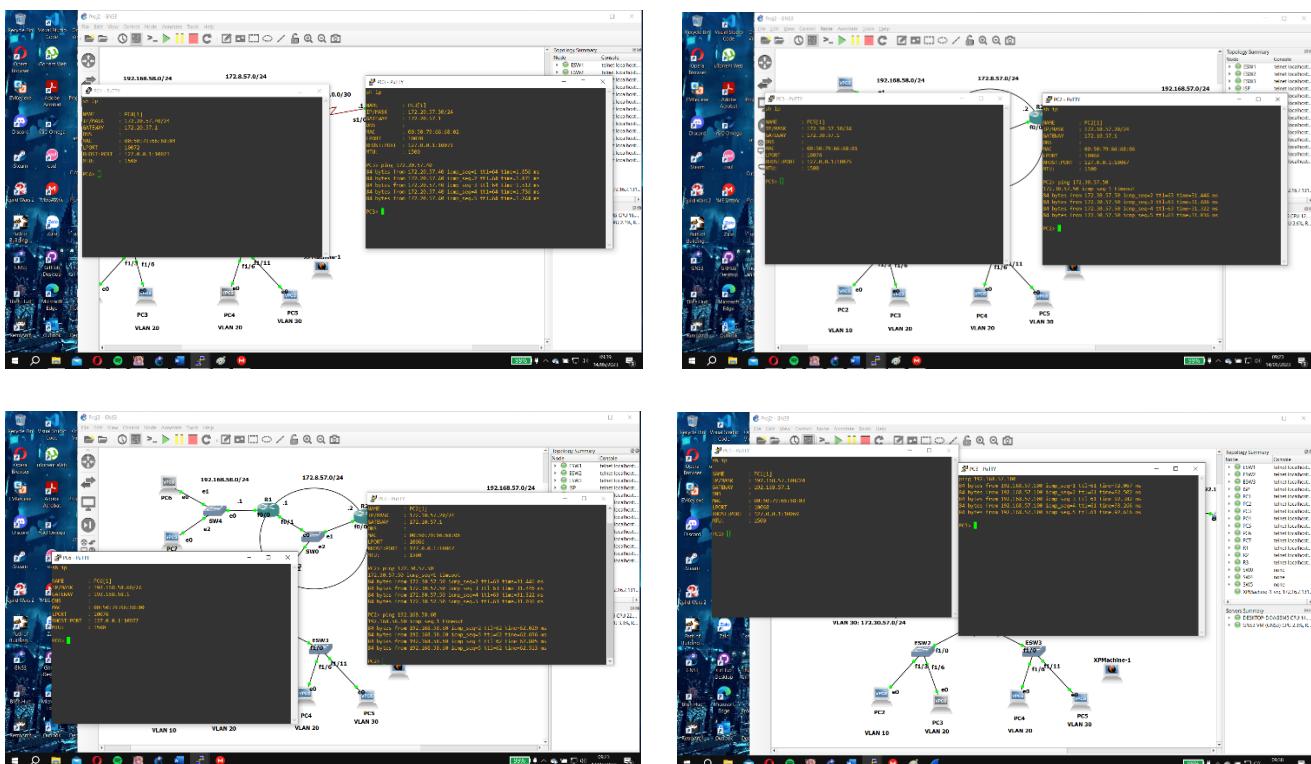
Khi đặt access list trên vào **line vty 0 4** là đường dùng để kết nối telnet khi ấy chỉ các host từ VLAN 30 mới có thể qua được access list truy cập đến R2 bằng telnet

- **R2(config)# line vty 0 4**
- **R2(config-line)# access-class 20 in**

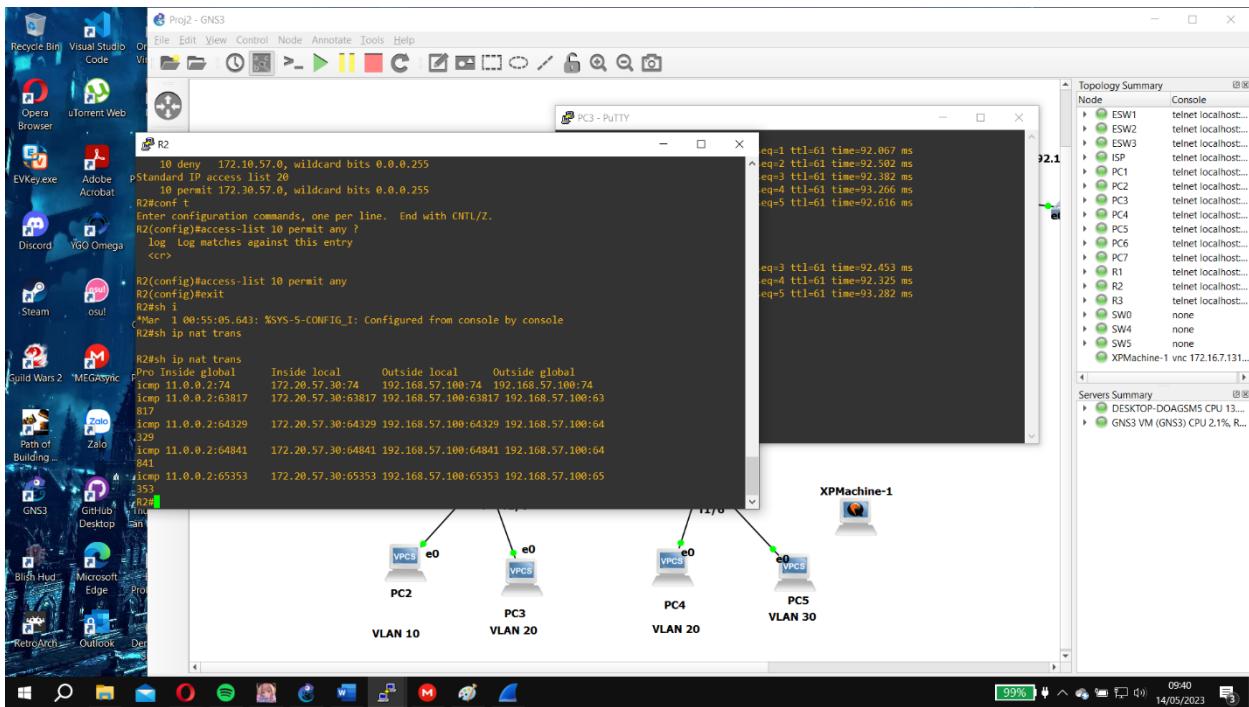


Kiểm tra toàn bộ kết quả

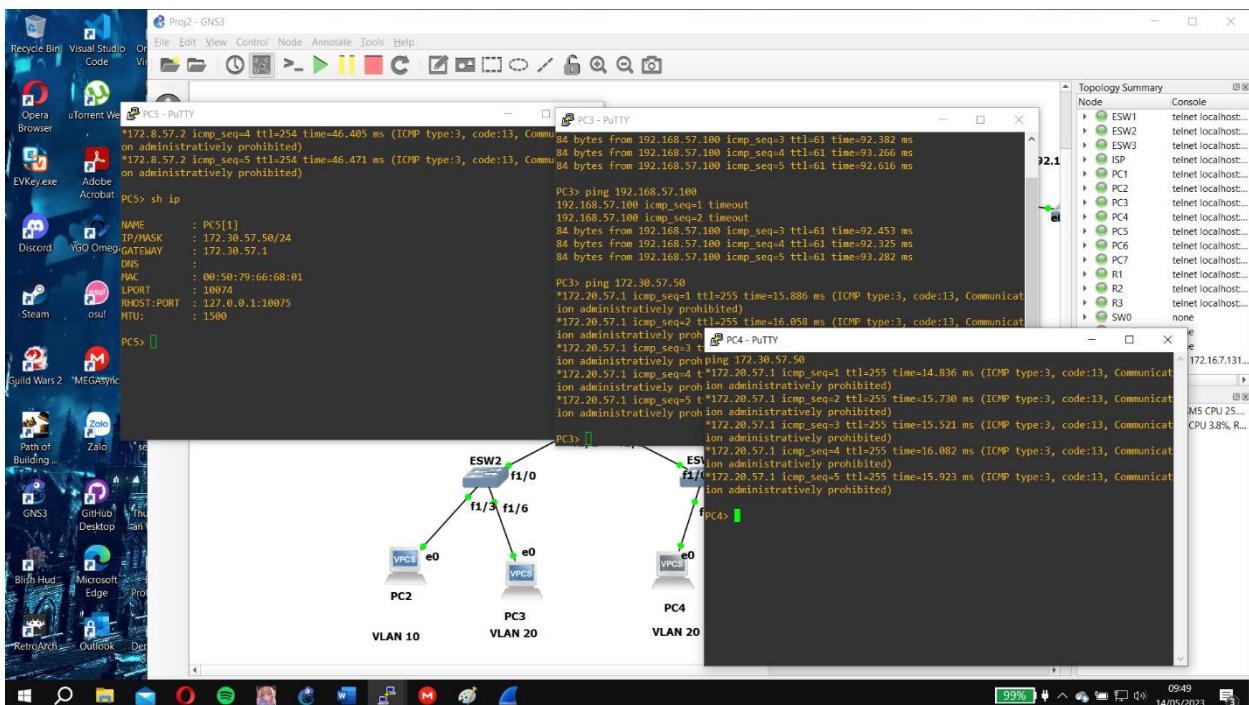
Các host ở trong cùng 1 VLAN, khác VLAN, trong mạng nội bộ có thể ping lẫn nhau và ping ra Internet trừ VLAN 10



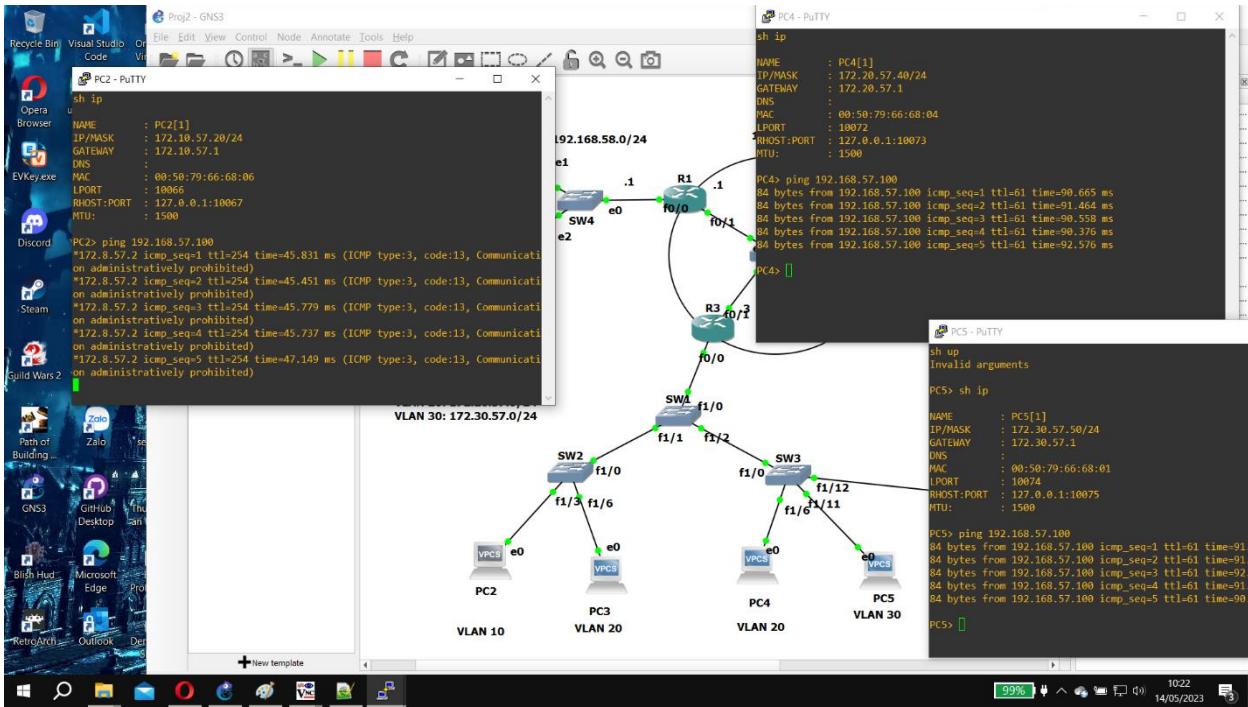
Kết quả NAT từ kết nối trên



VLAN 20 không ping được VLAN 30



VLAN 10 không ping được ra ngoài Internet



Chỉ các host kết nối vào VLAN 30 mới có thể telnet vào R2

