ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

BÁO CÁO

Lab 3. LAN SECURITY

Họ và tên: Nguyễn Bửu Thạch

MSSV:20120576

Môn học: An ninh máy tính

Thành phố Hồ Chí Minh-2024

1. **Port Security** (1,0 điểm)

Bằng cách giới hạn và kiểm soát các thiết bị gắn vào Switch có thể hạn chế nhiều tấn công trong LAN như:

- Kẻ tấn công dùng công cụ để quét lấy hết IP từ DHCP server
- Kiểm soát các thiết bị người dùng cố định, các server kết nối đến Switch (tránh sự thay đổi tự do trong quá trình vận hành hệ thống)

Topology

00-40-45-19-71-83

Yêu cầu

1. Chỉ có client với địa chỉ MAC: 00-40-45-19-71-83 được sử dụng port fa0/1 trên Switch (tùy vào PC, SV có thể dùng địa chỉ MAC khác).

2. Các client khác gắn vào port fa0/1, port fa0/1 sẽ bị shutdown

3. port fa0/1 sẽ khôi phục lại sau 30 giây (ko lam duoc tren packet tracer).

Cấu hình

1. Cấu hình port security. Chỉ có client với địa chỉ MAC: 00-40-45-19-71-83 được sử dụng port fa0/1 trên Switch.

Switch(config)#interface fa0/1

Switch(config-if)#switchport mode access

Switch(config-if)#switchport port-security

(Switch(config-if)#switchport port-security mac-address 0040.4519.7183)

Switch(config-if)#switchport port-security maximum 1

Switch(config-if)#switchport port-security mac-address sticky

2. Các client khác gắn vào port fa0/1, port fa0/1 sẽ bị shutdown

Switch(config)#interface fa0/1

Switch(config-if)#switchport port-security violation shutdown

```
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#ex
Switch(config)#interface fa0/1
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#
```

3. port fa0/1 sẽ khôi phục lại sau 30 giây *(các lệnh sau không hỗ trợ trên phần mềm giả lập Packet Tracer, – SV không cần làm chức năng này hoặc thử nghiệm trên GNS3)*

Switch(config)#errdisable detect cause all

Switch(config)#errdisable recovery cause all

Switch(config)#errdisable recovery interval 30

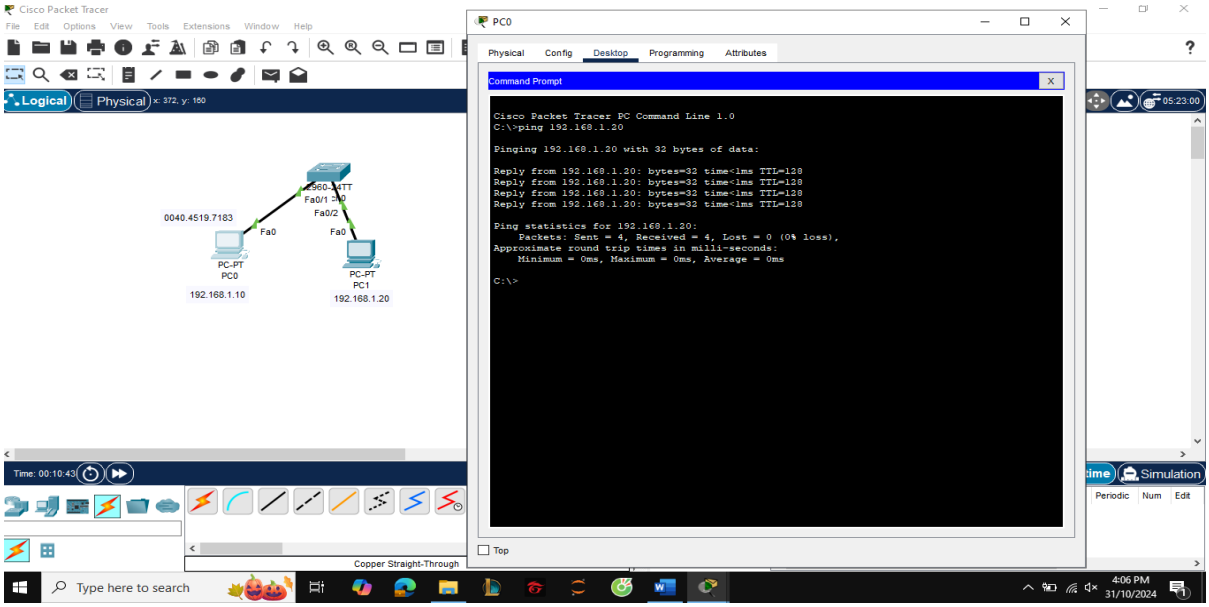
Kiểm tra cấu hình

show interface switchport

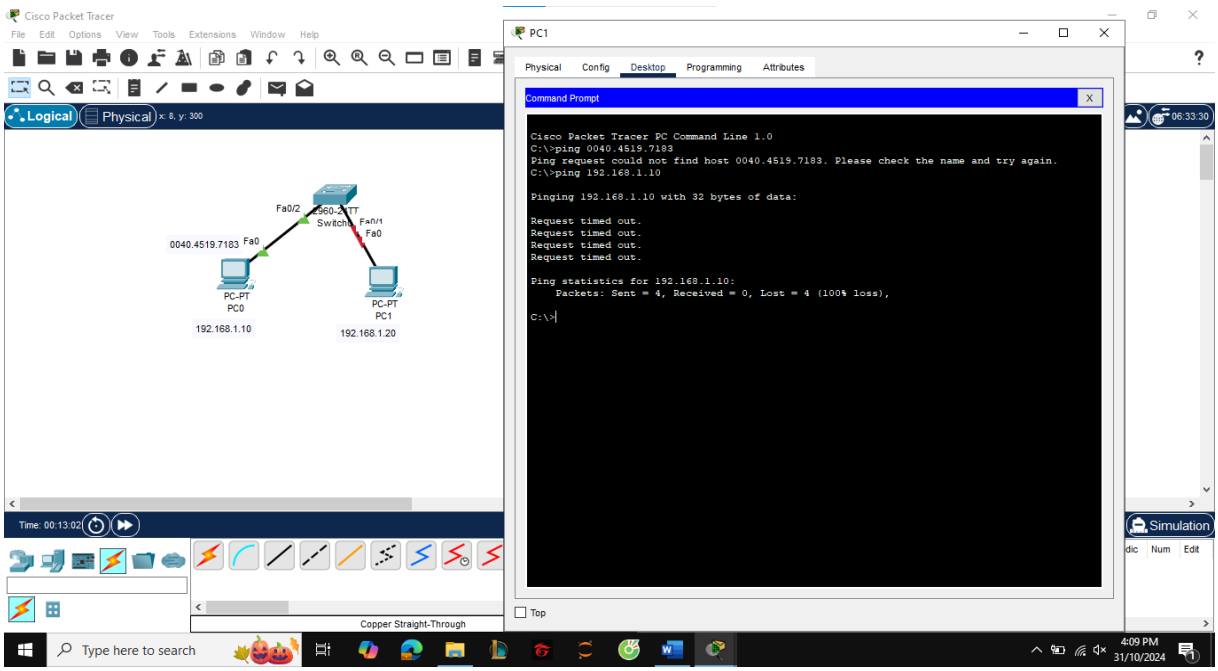
show port-security interface

Kết quả:

PC1 (Địa chỉ MAC: *0040.4519.7183)*



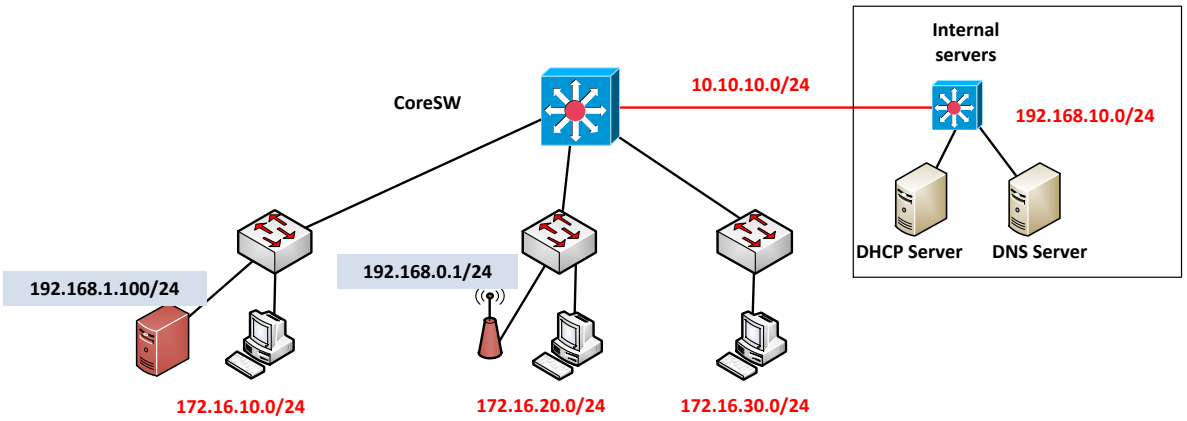
PC2: (Địa chỉ MAC khác *0040.4519.7183)*



⇨ Chỉ có client với địa chỉ MAC: 00-40-45-19-71-83 được sử dụng port fa0/1 trên Switch. Các client khác gắn vào port fa0/1, port fa0/1 sẽ bị shutdown

2. **DHCP snooping** (2,0 điểm)

Chống giả các DHCP server trong hệ thống, chỉ cho phép các client xin IP từ DHCP Server thật *(sử dụng phần mềm giả lập Packet Tracer hoặc EVE)*



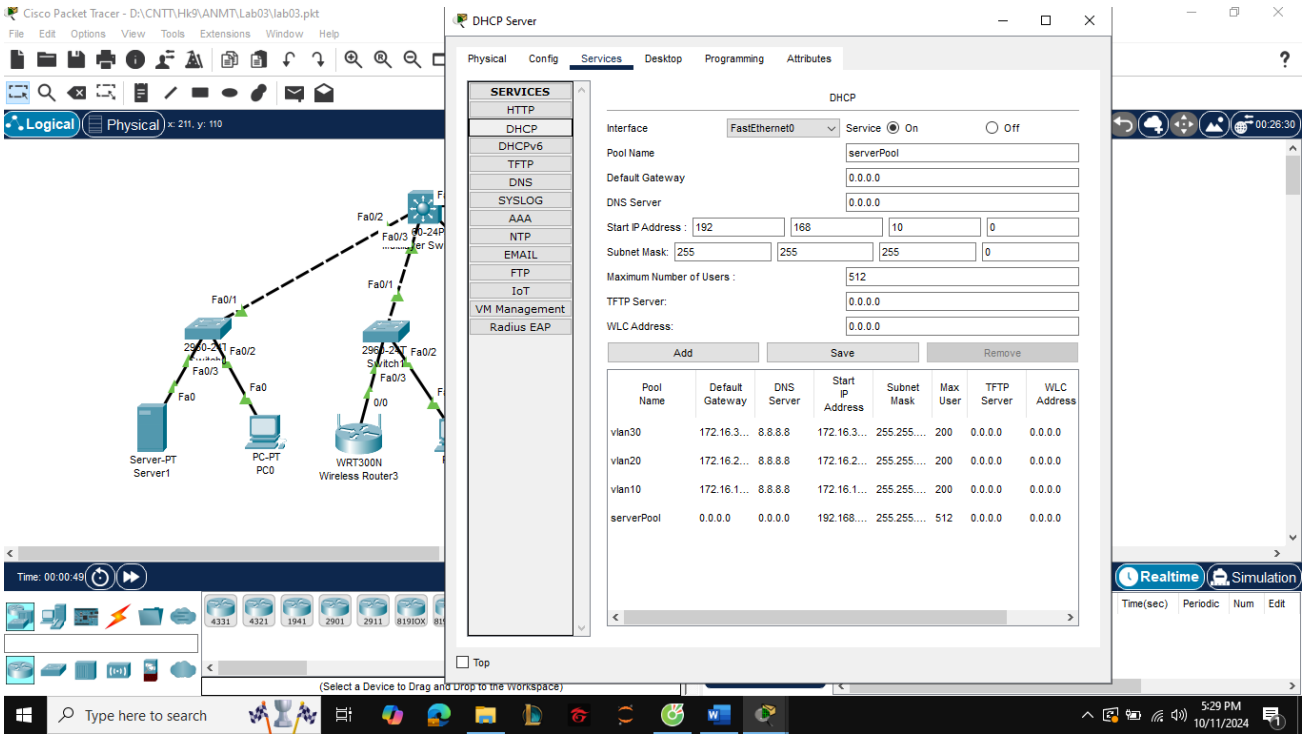
Topology

Yêu cầu

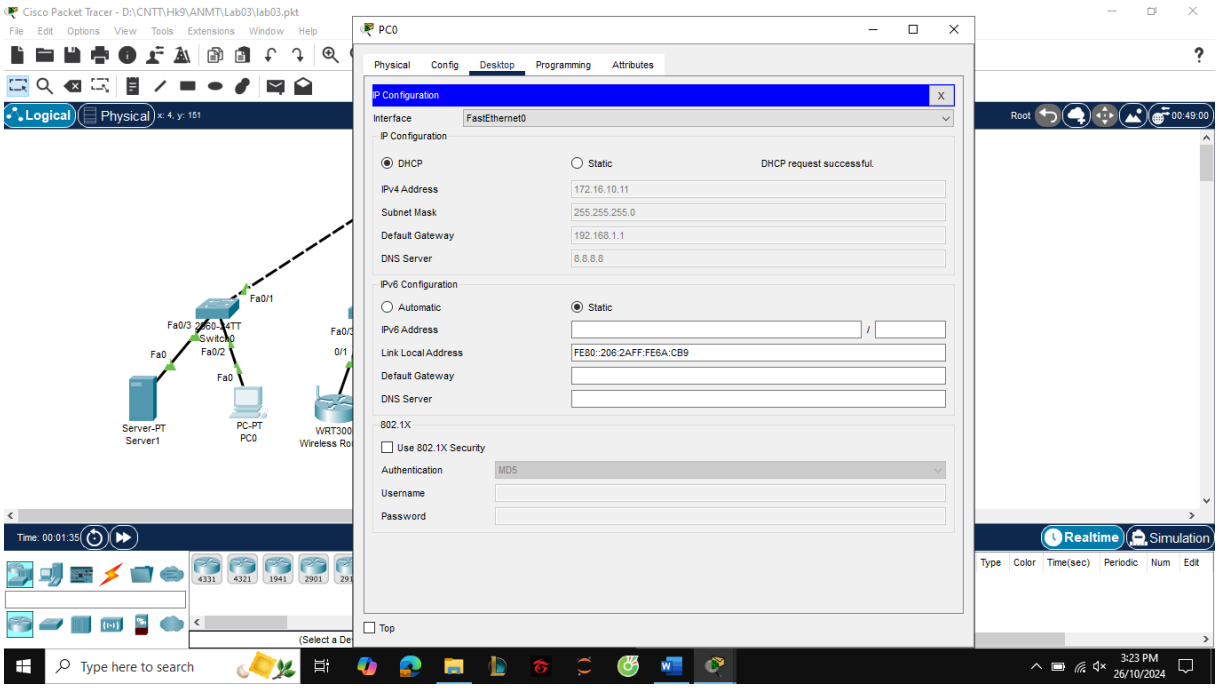
1. Cấu hình theo sơ đồ mạng trên

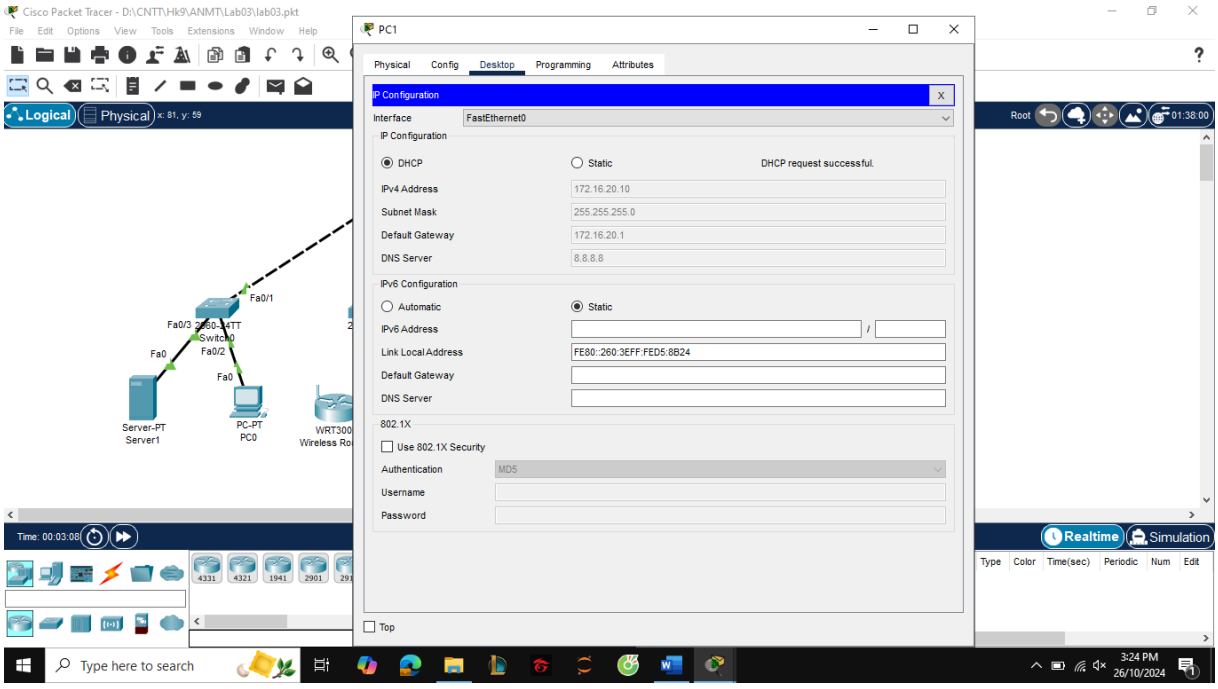
- Cấu hình định tuyến
- Cấu hình cho DHCP server cấp phát địa chỉ IP động cho các PC ở các mạng 172.16.10.0/24, 172.16.20.0/24, 172.16.30.0/24

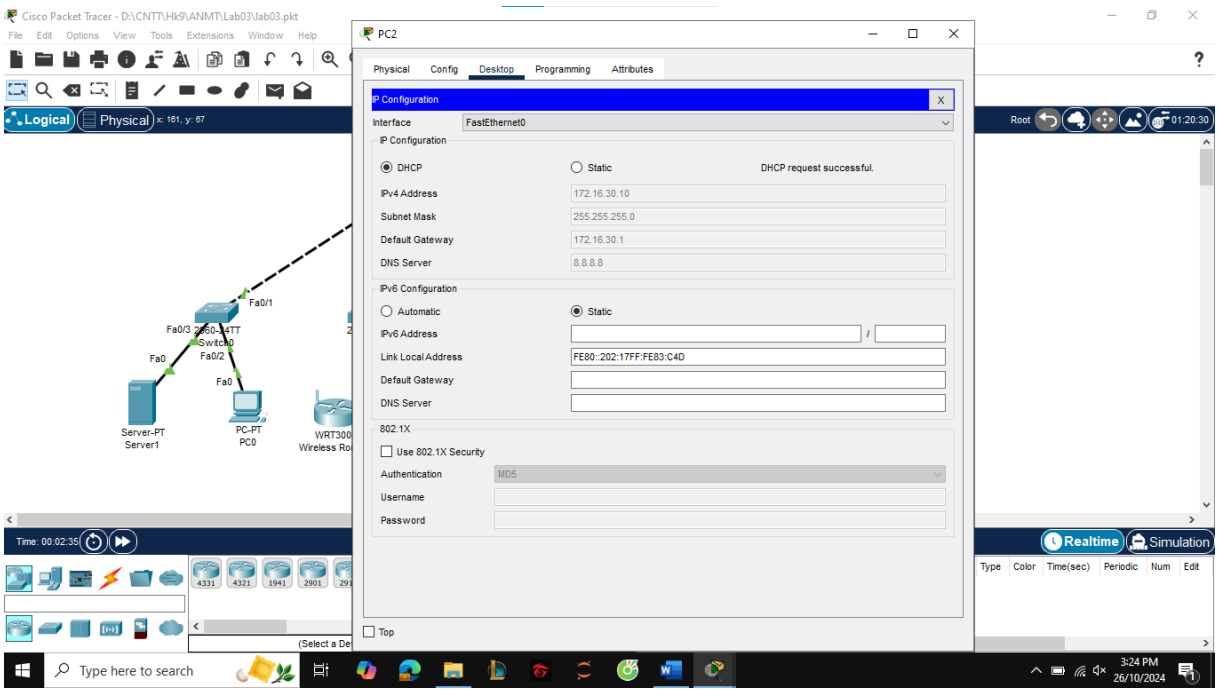
Cấu hình cho DHCP server cấp phát IP động:



Kết quả:


Cisco Packet Tracer - D:\CNTT\Hk9\ANMT\Lab03\lab03.pkt
PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
DHCP
Static
DHCP request successful.
IPv4 Address
172.16.10.11
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
8.8.8.8
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::206:2AFF:FE6A:CB9
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top
Server-PT Server1
PC-PT PC0
Type here to search
3:23 PM
26/10/2024

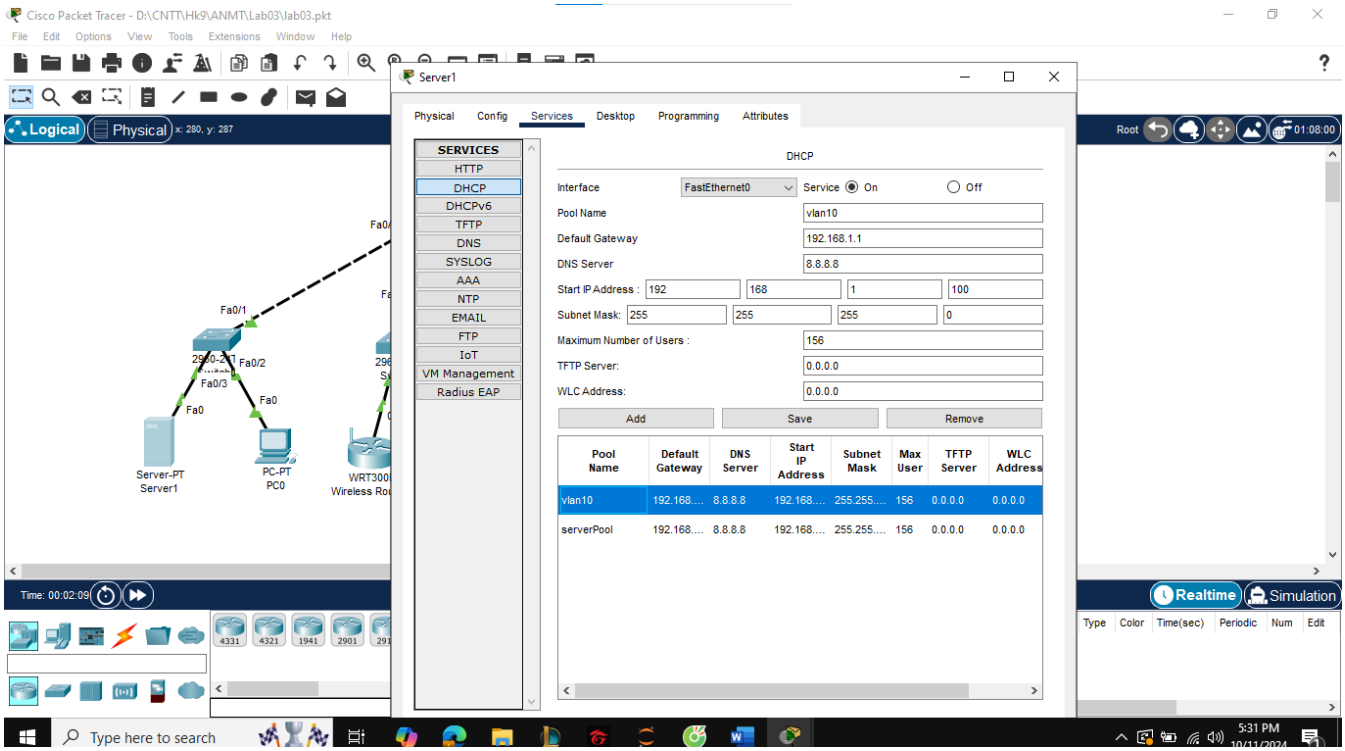

Cisco Packet Tracer - D:\CNTT\Hk9\ANMT\Lab03\lab03.pkt
PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
DHCP
Static
DHCP request successful.
IPv4 Address
172.16.20.10
Subnet Mask
255.255.255.0
Default Gateway
172.16.20.1
DNS Server
8.8.8.8
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::260:3EFF:FED5:8B24
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top
Server-PT Server1
PC-PT PC0
Type here to search
3:24 PM
26/10/2024

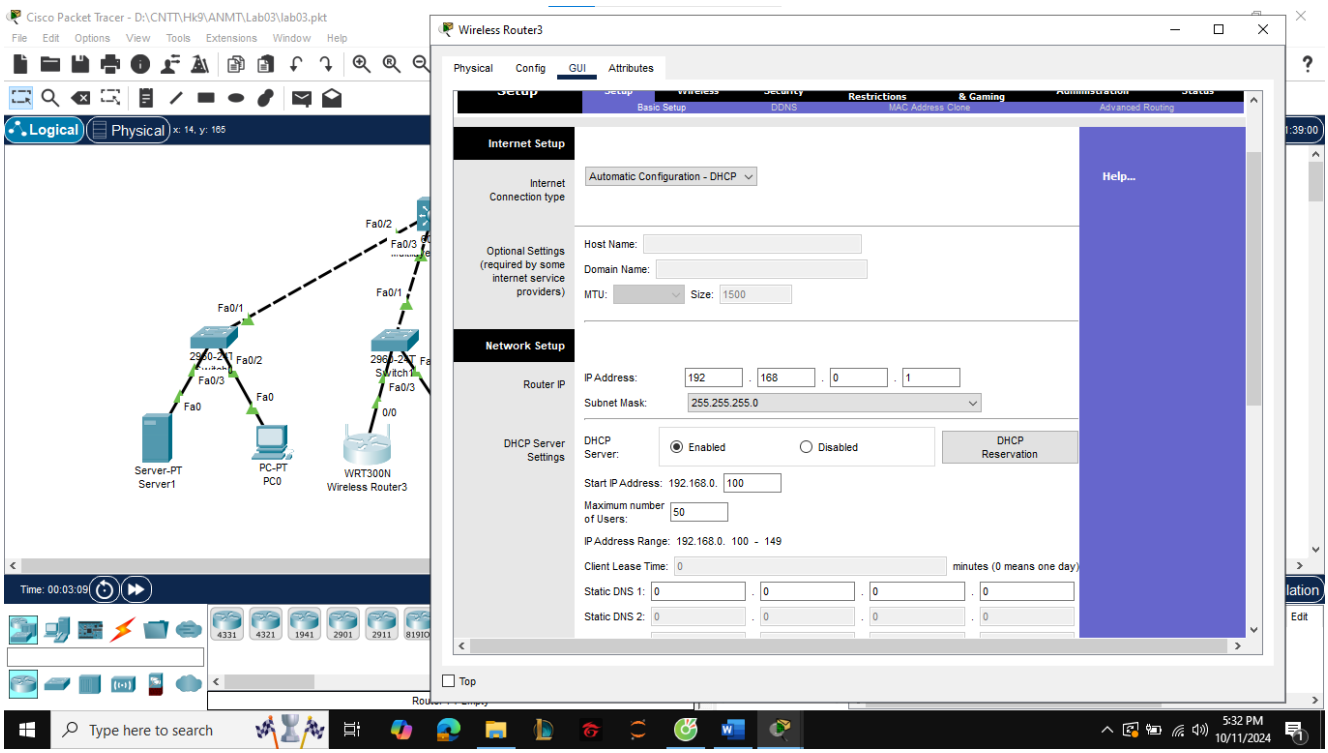


⇨ PC0,PC1,PC2 sẽ nhận địa chỉ IP do DHCP server cấp phát.

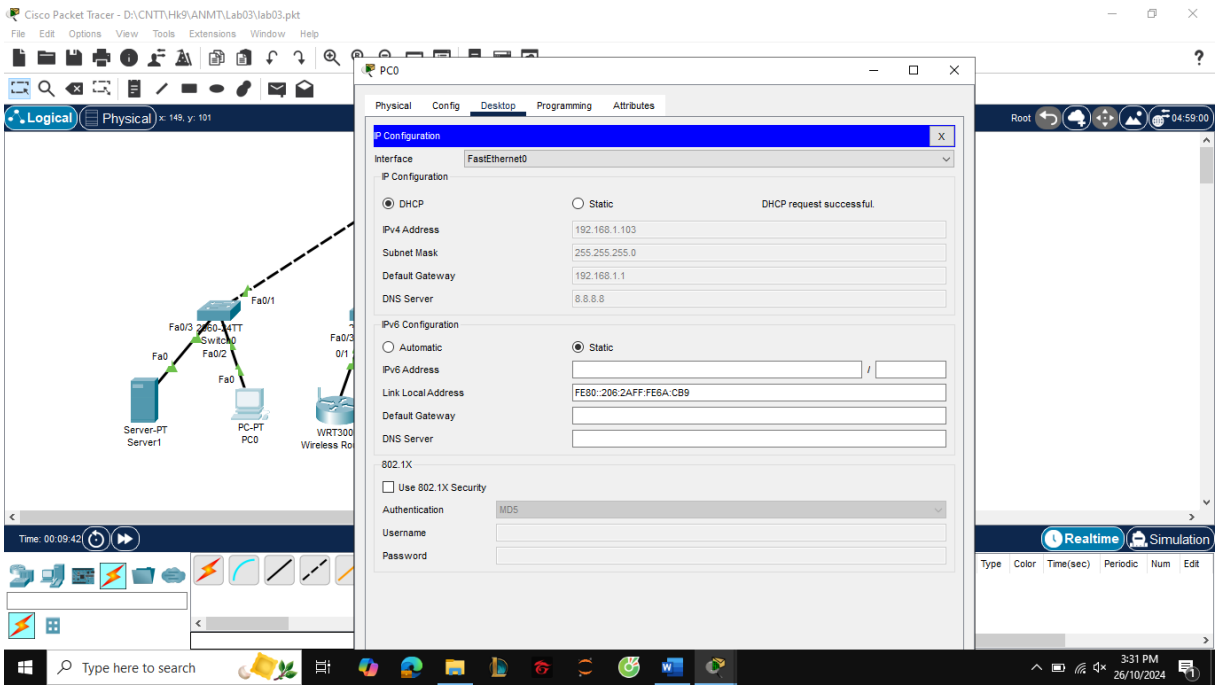
2. Thử trường hợp với các DHCP server giả và AP cấp IP động

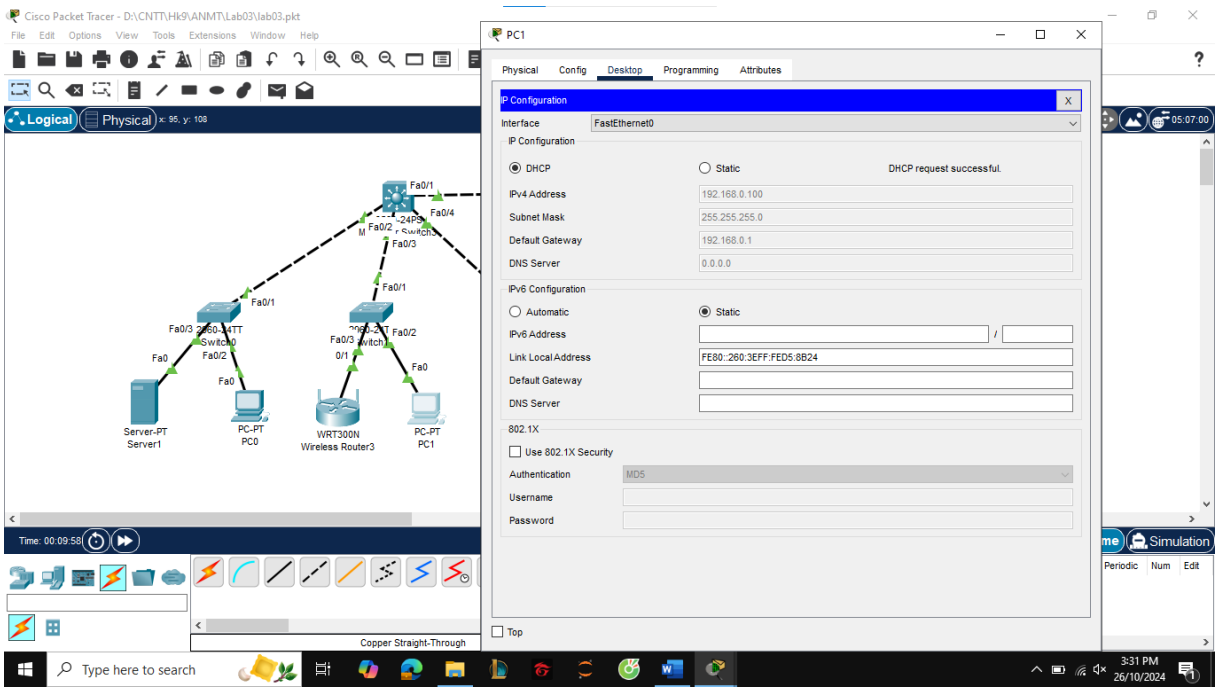
Cấu hình cho DHCP server giả và AP cấp phát IP giả cho các PC




Cisco Packet Tracer - D:\CNTT\Hk9\ANMT\Lab03\lab03.pkt
Wireless Router3
Physical
Config
GUI
Attributes
Internet Setup
Internet Connection type
Automatic Configuration - DHCP
Optional Settings (required by some internet service providers)
Host Name:
Domain Name:
MTU:
Size:
1500
Network Setup
Router IP
IP Address:
192
168
0
1
Subnet Mask:
255.255.255.0
DHCP Server Settings
DHCP Server:
Enabled
Disabled
DHCP Reservation
Start IP Address: 192.168.0. 100
Maximum number of Users:
50
IP Address Range: 192.168.0. 100 - 149
Client Lease Time:
minutes (0 means one day)
Static DNS 1:
Static DNS 2:
Help...
Top
Server-PT Server1
PC-PT PC0
WRT300N Wireless Router3
Time: 00:03:09
5:32 PM
10/11/2024

Kết quả:


Cisco Packet Tracer - D:\CNTT\Hk9\ANMT\Lab03\lab03.pkt
PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
DHCP
Static
DHCP request successful.
IPv4 Address
192.168.1.103
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
8.8.8.8
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::206:2AFF:FE6A:CB9
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Realtime
Simulation
Server-PT Server1
PC-PT PC0
Time: 00:09:42
3:31 PM
26/10/2024



⇨ PC0 sẽ nhận địa chỉ IP do DHCP server giả cấp phát, PC1 sẽ nhận được địa chỉ IP do AP cấp phát.

3. Cấu hình DHCP snooping trên Switch, sao cho các client chỉ xin địa chỉ IP từ DHCP trên DHCP Server thật.

Các lệnh cấu hình:

Switch(config)#ip dhcp snooping

Switch(config)#ip dhcp snooping vlan 1

Switch(config)#no ipdhcp snooping information option

Switch(config)#interface <*interface*> (port kết nối hoặc port hướng kết nối về DHCP thật)

Switch(config-if)#ip dhcp snooping trust

Switch(config-if)#exit

Cấu hình DHCP trên Switch0

```
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 10
Switch(config)#no ipdhcp snooping information option
                ^
% Invalid input detected at '^' marker.

Switch(config)#no ip dhcp snooping information option
Switch(config)#int fa0/1
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#ex
```

Cấu hình DHCP trên Switch1

```
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 20
Switch(config)#no ipdhcp snooping information option
                ^
% Invalid input detected at '^' marker.

Switch(config)#no ip dhcp snooping information option
Switch(config)#int fa0/1
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#ex
```

Kiểm tra cấu hình

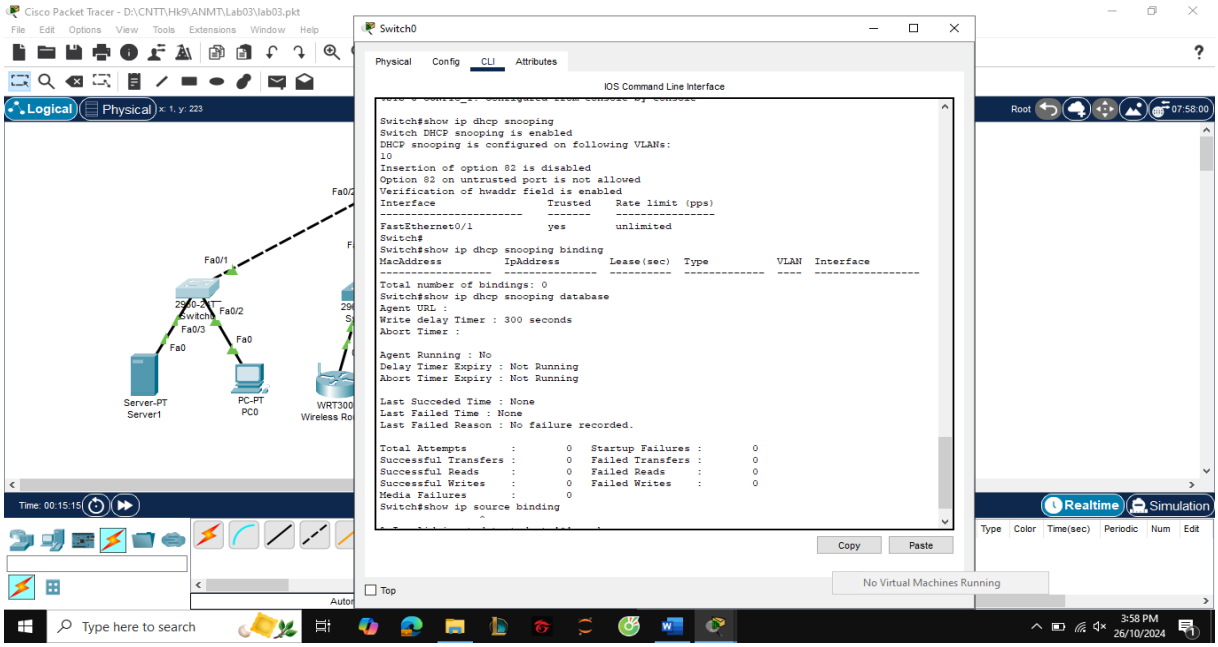
show ip dhcp snooping

show ip dhcp snooping binding

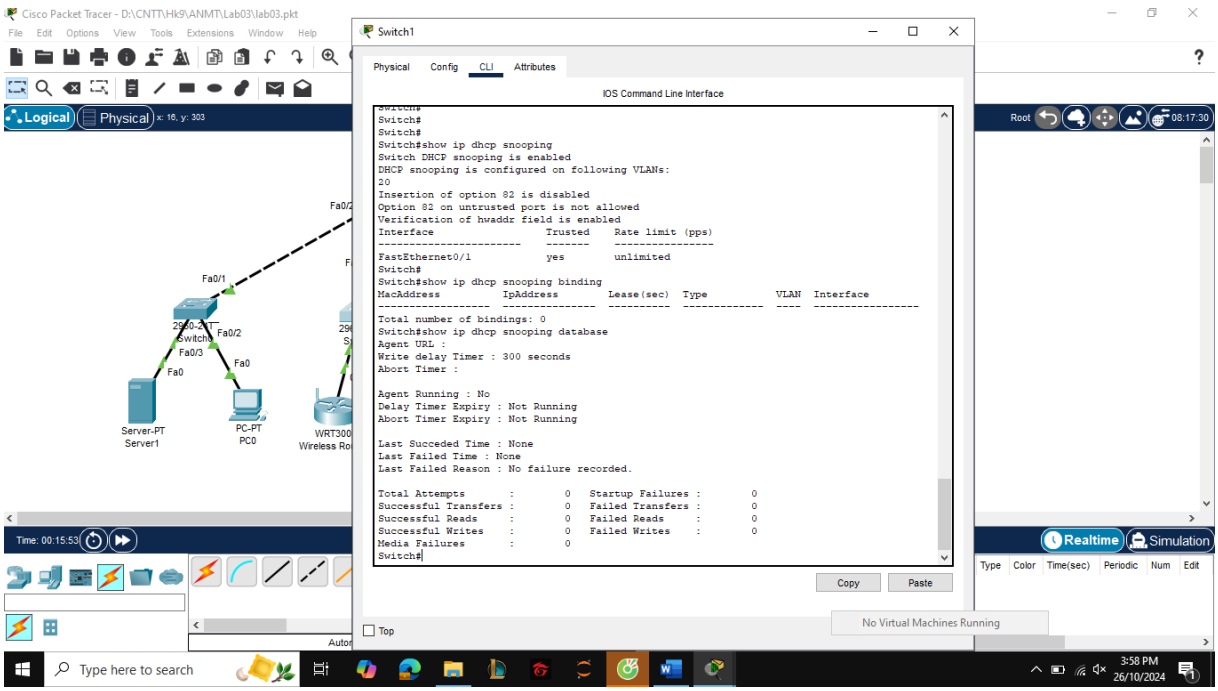
show ip dhcp snooping database

show ip source binding

Switch0

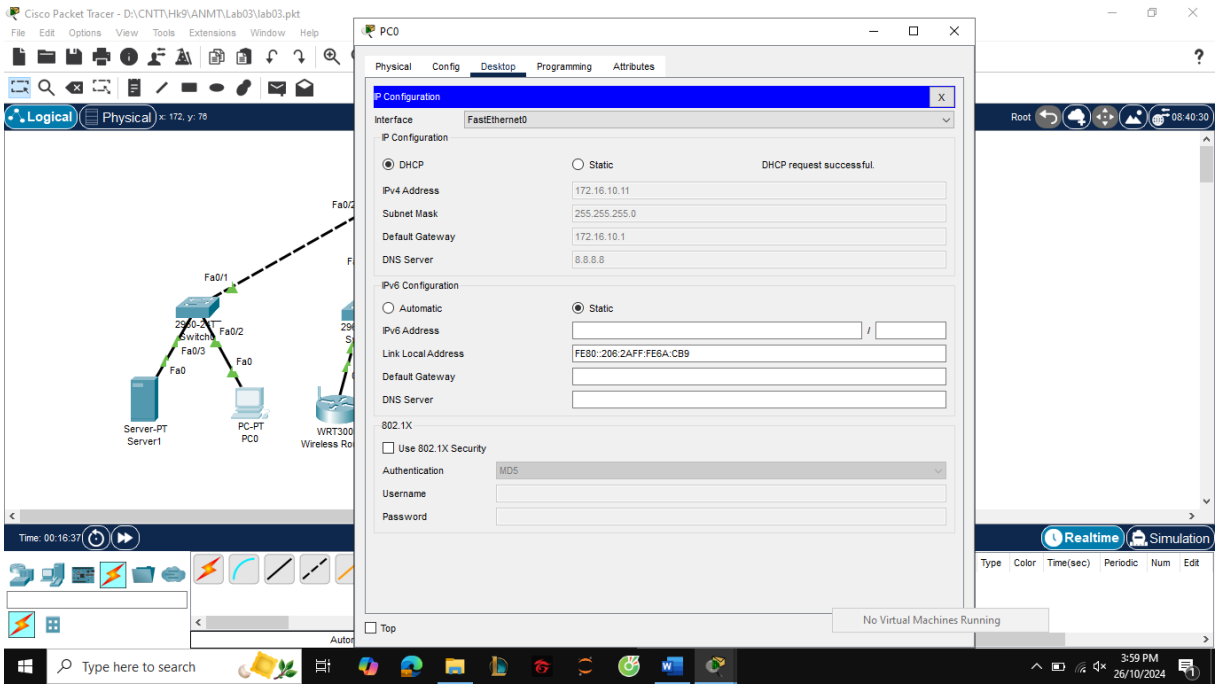


Switch1

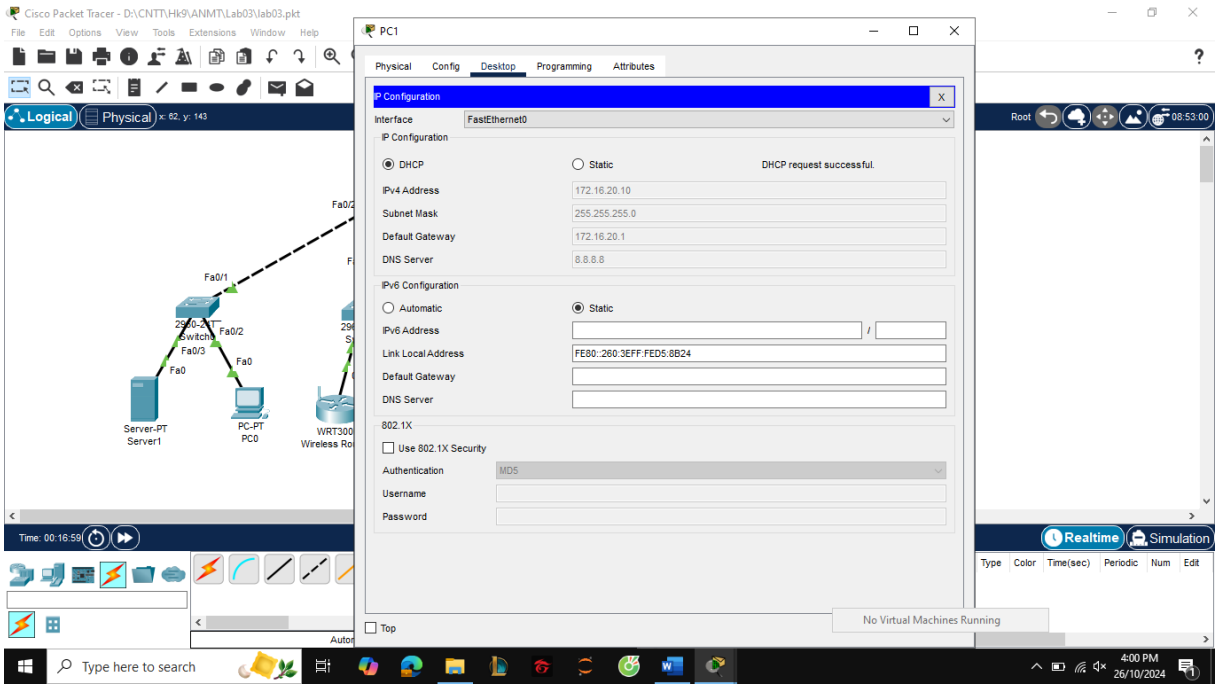


Kết quả:

PC0:



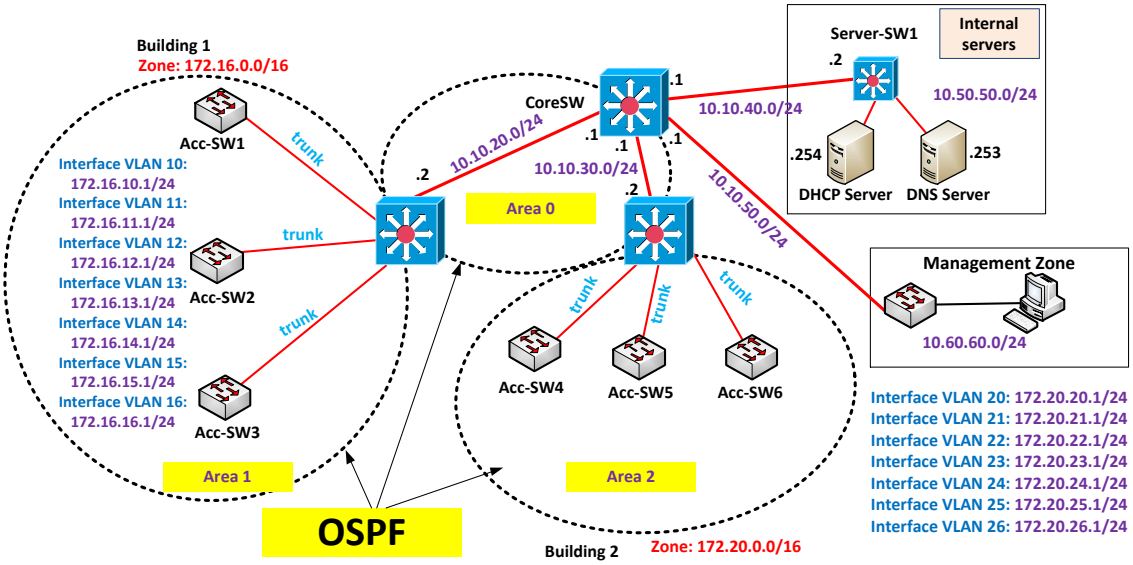
PC1:



⇨ PC0 và PC1 đã xin đúng IP từ DHCP server thật

3. **Access Control List** (2,0 điểm)

Cho sơ đồ mạng



Sử dụng lại bài Lab 01, có bổ sung thêm khu vực quản trị (Management zone)

a) Định tuyến cho khu vực Management Zone
Mở line telnet/SSH trên các thiết bị mạng: CoreSW, Dist-SW1, Dist-SW2, Access-SW1 → Access-SW6)
Trong đó:

- IP của các Acc-Sw1 → Acc-SW3: 172.16.1.1/24 → 172.16.1.3/24
- IP của các Acc-Sw4 → Acc-SW6: 172.16.2.4/24 → 172.16.2.6/24

b) Cấu hình ACL:

- Cấm các PC thuộc VLAN 10 và VLAN 20 ping tới các server trong khu vực Internal Server
- Chỉ cho phép các PC trong khu vực quản trị được phép quản trị từ xa các thiết bị mạng (CoreSW, Dist-SW1, Dist-SW2, Access-SW1 → Access-SW6)

Các bước thực hiện:

a) Định tuyến cho khu vực Management Zone
Mở line telnet/SSH trên các thiết bị mạng: CoreSW, Dist-SW1, Dist-SW2, Access-SW1 → Access-SW6)
Trong đó:

- IP của các Acc-Sw1 → Acc-SW3: 172.16.1.1/24 → 172.16.1.3/24

1. Cấu hình và định tuyến cho khu vực Management Zone:

- Cấu hình L3 EtherChannel giữa Core-SW và Management Zone (đặt tên channel là Po 14)

Core-SW

1. Chuyển các cổng vật lý sang chế độ Layer 3.

```
Core-SW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Core-SW(config)#int range fa0/8-9
Core-SW(config-if-range)#no switchport
```

2. Tạo và cấu hình Etherchannel trên cổng: (Sử dụng chế độ PAgP)

```
Core-SW(config-if-range)#channel-protocol pagp
Core-SW(config-if-range)#channel-group 14 mode desirable
Core-SW(config-if-range)#
%LINK-3-UPDOWN: Interface Port-channel14, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel14, changed state to down

Core-SW(config-if-range)#ex
```

3. Cấu hình giao diện Port-channel 14 với địa chỉ IP

```
Core-SW(config)#int port-channel 14
Core-SW(config-if)#ip address 10.10.50.1 255.255.255.0
Core-SW(config-if)#no shutdown
Core-SW(config-if)#
%LINK-5-CHANGED: Interface Port-channel14, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel14, changed state to up

Core-SW(config-if)#ex
```

Management Zone

1. Chuyển các cổng vật lý sang chế độ Layer 3.

```
Switch(config)#int range fa0/1-2
Switch(config-if-range)#no switchport
```

2. Tạo và cấu hình Etherchannel trên cổng: (Sử dụng chế độ PAgP)

```
Switch(config-if-range)#channel-protocol pagp
Switch(config-if-range)#channel-group 14 mode desirable
Switch(config-if-range)#
%LINK-3-UPDOWN: Interface Port-channel14, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel14, changed state to down

Switch(config-if-range)#ex
```

3. Cấu hình giao diện Port-channel 14 với địa chỉ IP:

```
Switch(config)#int port-channel 14
Switch(config-if)#ip address 10.10.50.2 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#e
%LINK-5-CHANGED: Interface Port-channel14, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel14, changed state to up
Switch(config-if)#ex
```

- Định tuyến cho khu vực Management Zone:

Management Zone:

```
Switch(config)#ip routing
Switch(config)#ip route 172.16.0.0 255.255.0.0 10.10.50.1
Switch(config)#ip route 172.20.0.0 255.255.0.0 10.10.50.1
Switch(config)#ip route 0.0.0.0 0.0.0.0 10.10.50.1
```

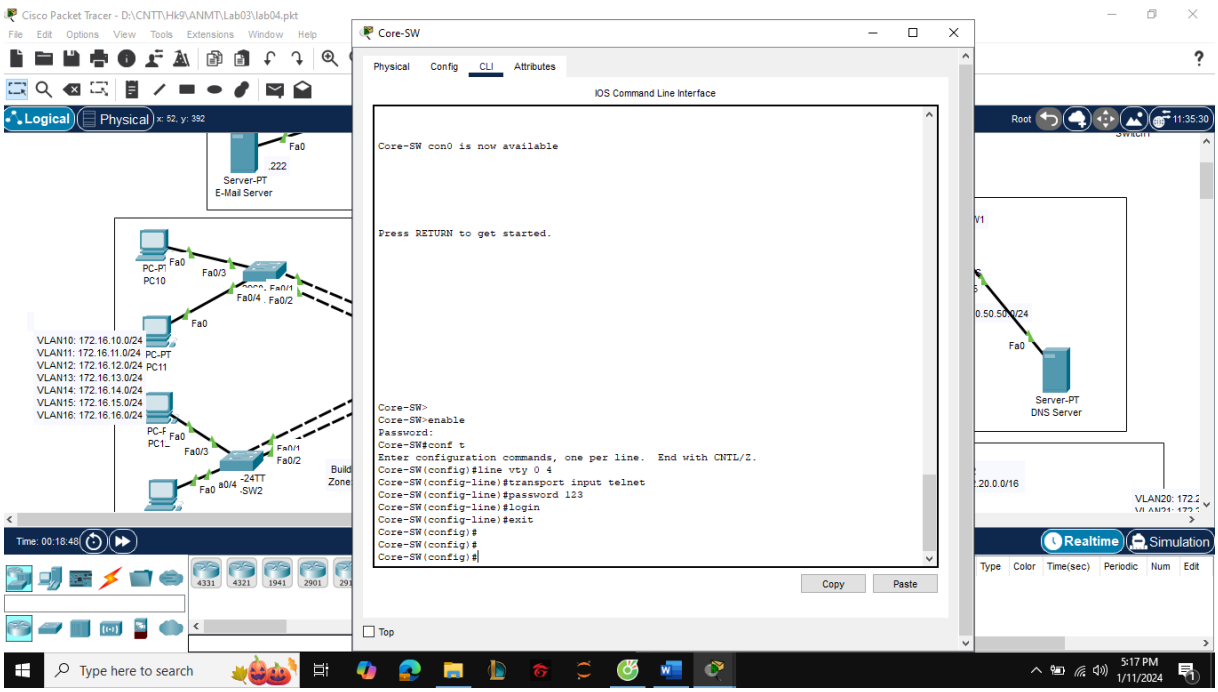
Core-SW:

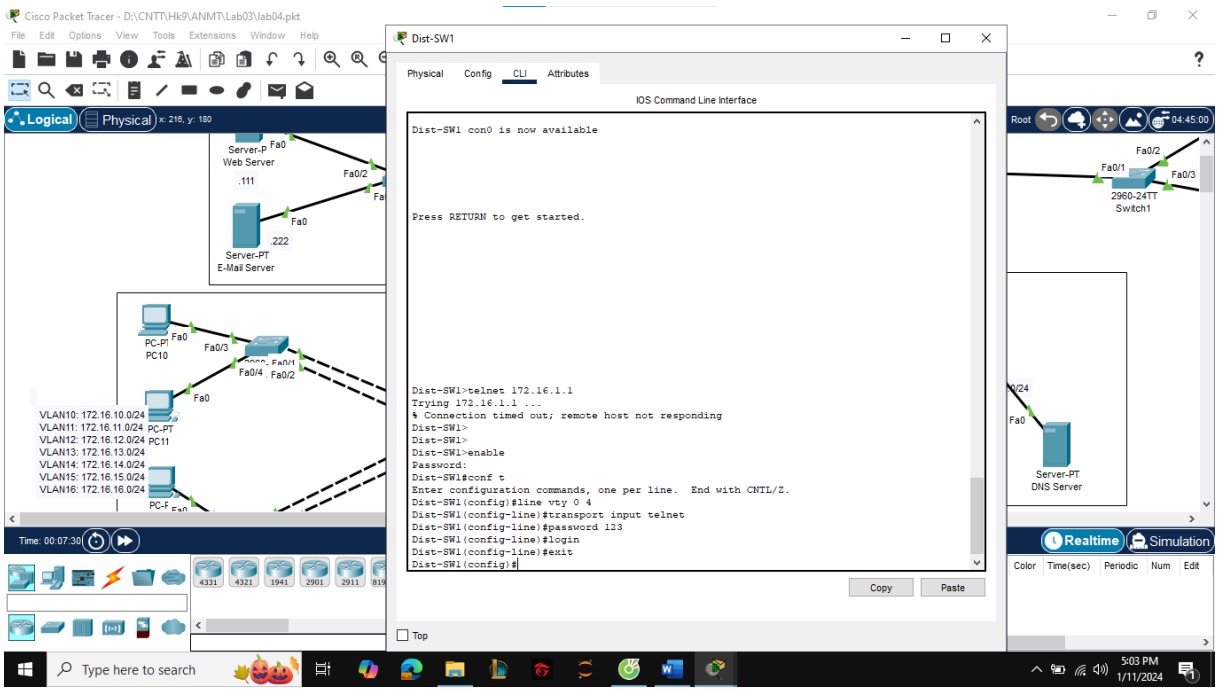
```
Core-SW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Core-SW(config)#ip route 10.60.60.0 255.255.255.0 10.10.50.2
```

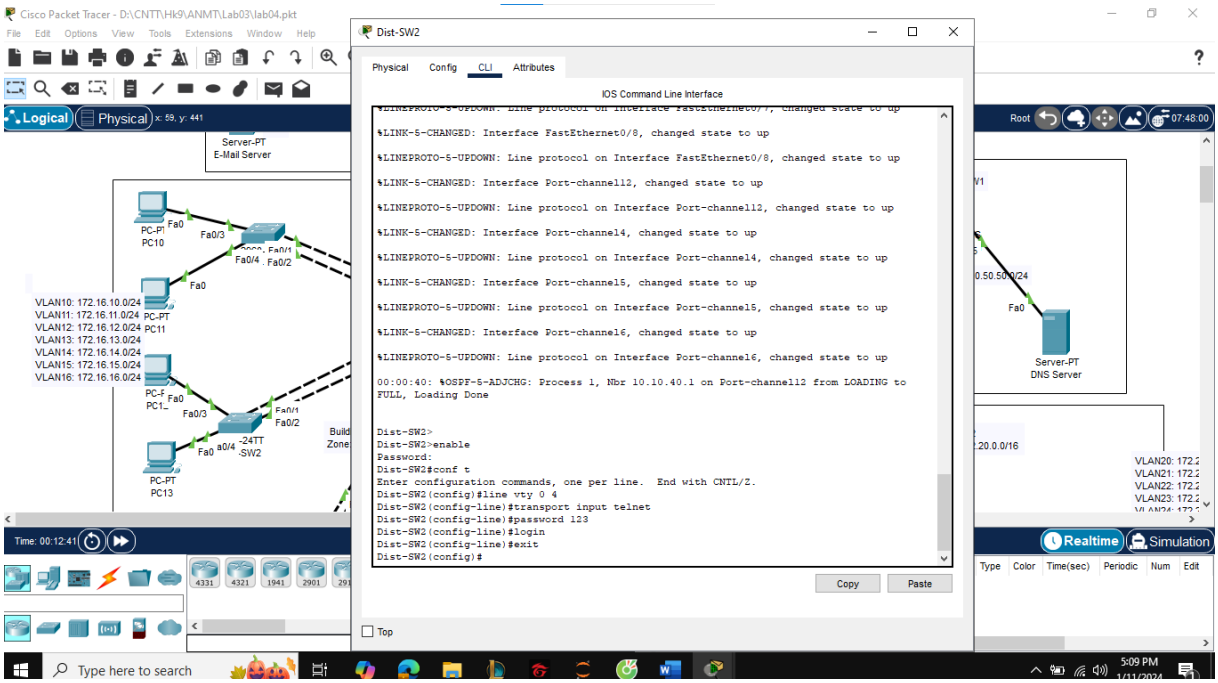
Firewall:

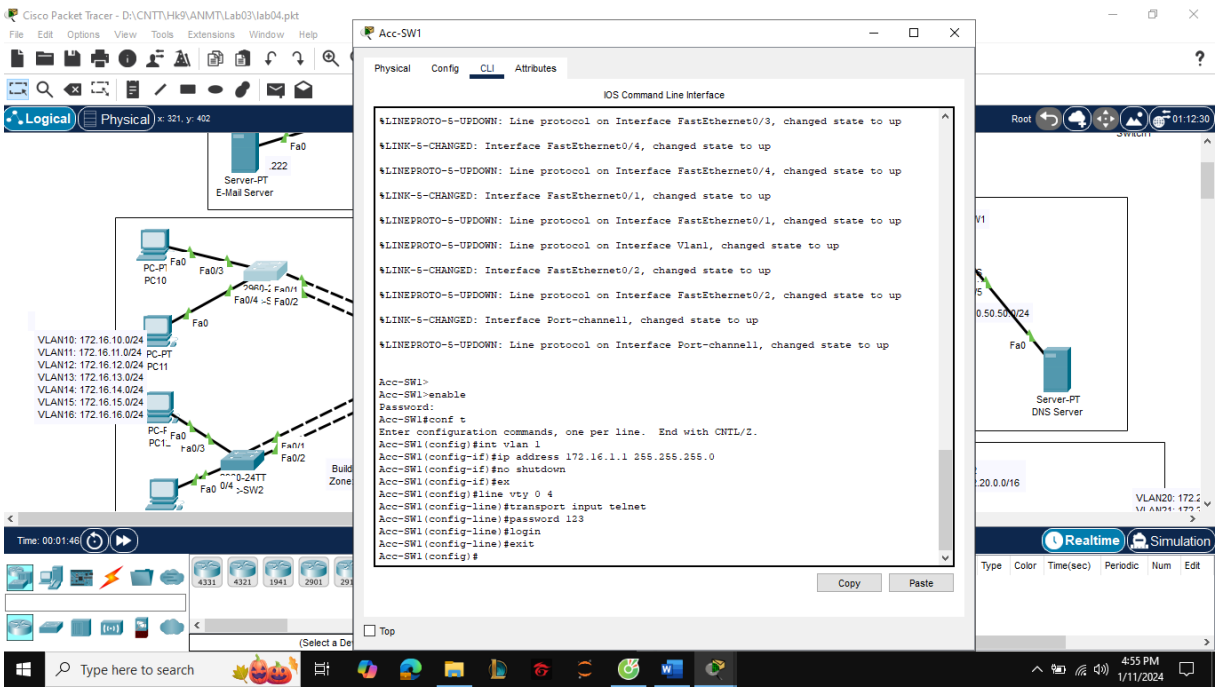
```
ciscoasa#conf t
ciscoasa(config)#route inside 10.60.60.0 255.255.255.0 10.10.10.2
ciscoasa(config)#
ciscoasa(config)#ex
```

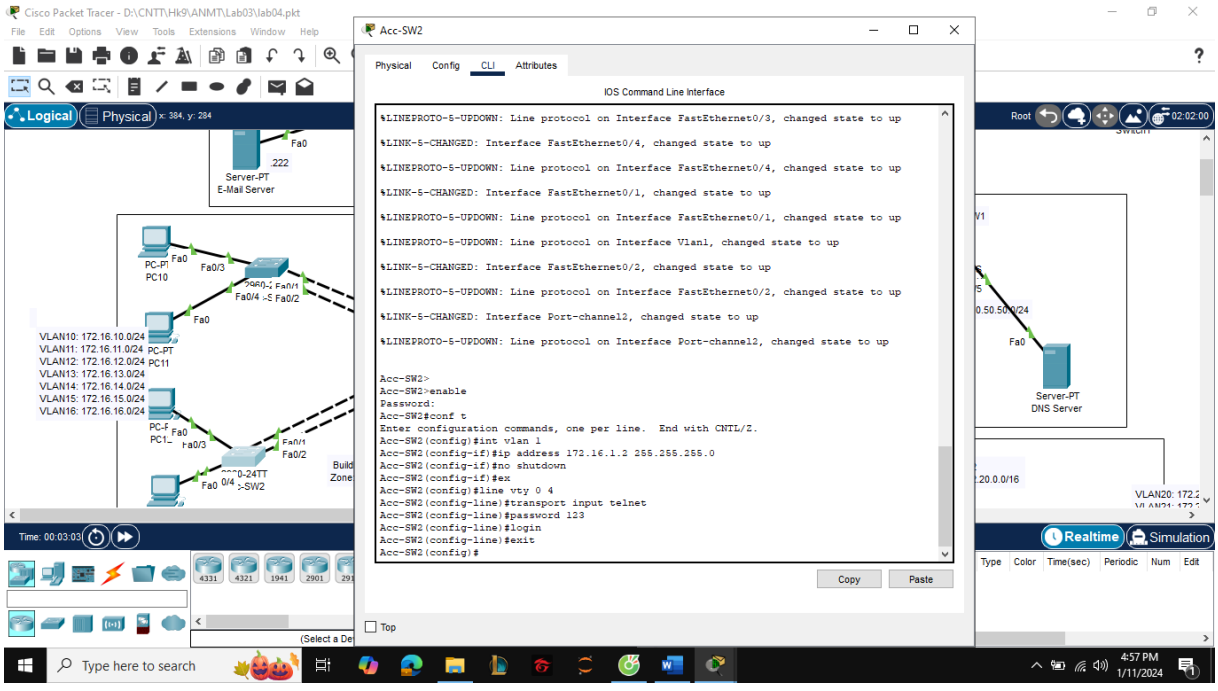
2. Mở line telnet trên tất cả các thiết bị mạng

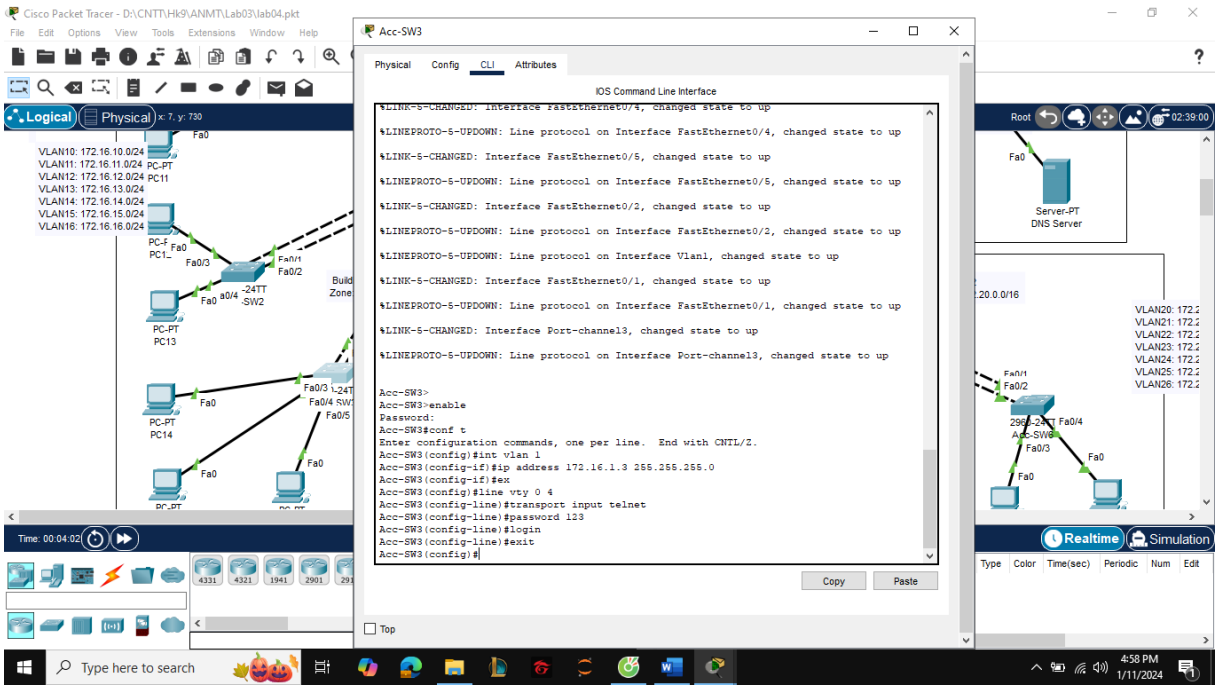


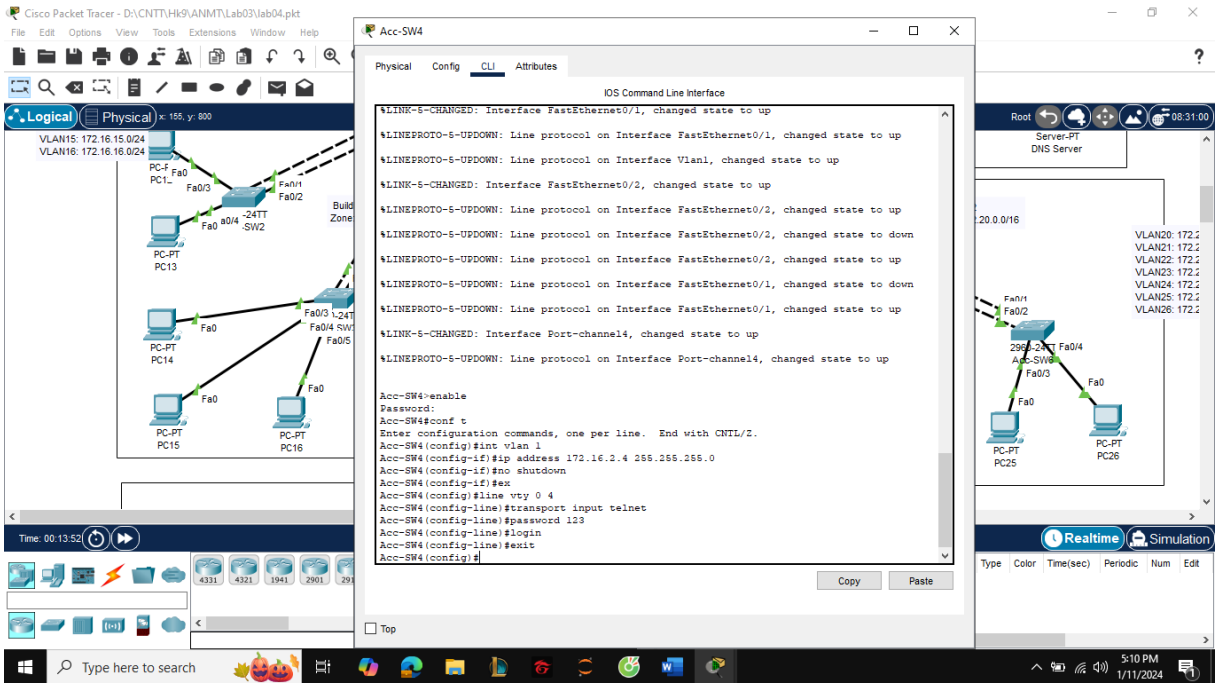

Cisco Packet Tracer - D:\CNTT\Hk9\ANMT\Lab03\lab04.pkt
Dist-SW1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Dist-SW1 con0 is now available
Press RETURN to get started.
Dist-SW1>telnet 172.16.1.1
Trying 172.16.1.1 ...
% Connection timed out; remote host not responding
Dist-SW1>
Dist-SW1>enable
Password:
Dist-SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Dist-SW1(config)#line vty 0 4
Dist-SW1(config-line)#transport input telnet
Dist-SW1(config-line)#password 123
Dist-SW1(config-line)#login
Dist-SW1(config-line)#exit
Dist-SW1(config)#
Copy
Paste
Top
Server-PT Web Server
Server-PT E-Mail Server
2960-24TT Switch1
Server-PT DNS Server
VLAN10: 172.16.10.0/24
VLAN11: 172.16.11.0/24
VLAN12: 172.16.12.0/24
VLAN13: 172.16.13.0/24
VLAN14: 172.16.14.0/24
VLAN15: 172.16.15.0/24
VLAN16: 172.16.16.0/24
Realtime
Simulation
Type here to search
5:03 PM
1/11/2024

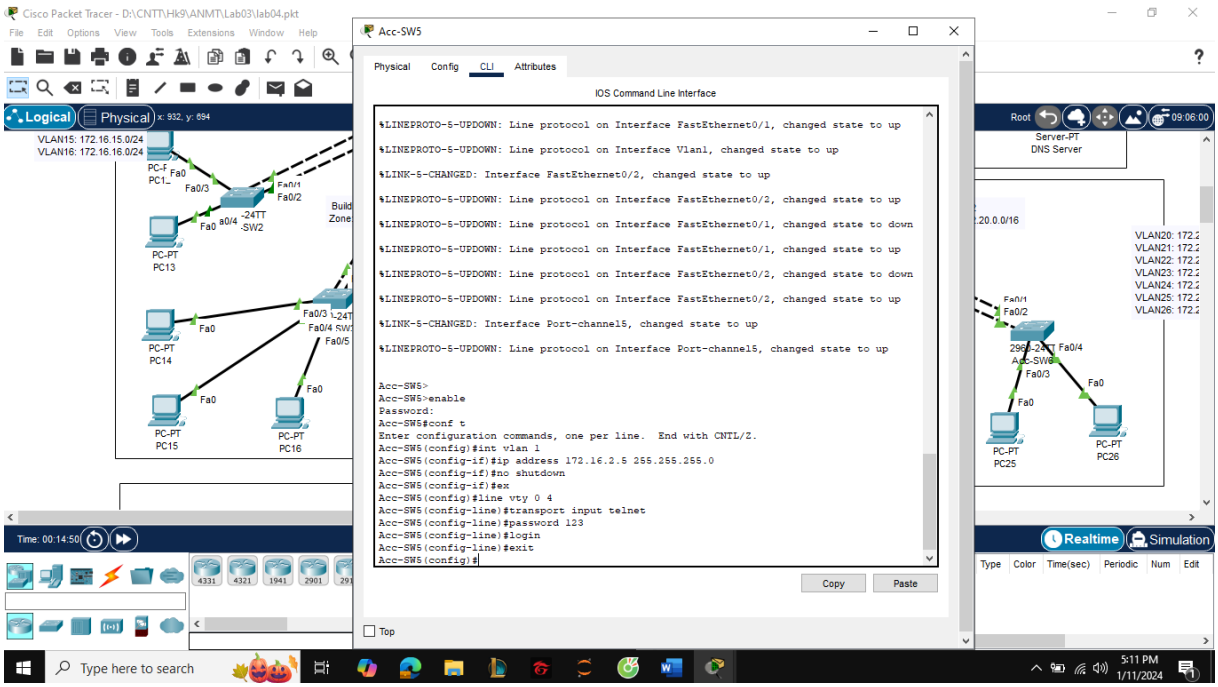

Cisco Packet Tracer - D:\CNTT\Hk9\ANMT\Lab03\lab04.pkt
Dist-SW2
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to up
%LINK-5-CHANGED: Interface Port-channel12, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel12, changed state to up
%LINK-5-CHANGED: Interface Port-channel4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel4, changed state to up
%LINK-5-CHANGED: Interface Port-channel5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel5, changed state to up
%LINK-5-CHANGED: Interface Port-channel6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel6, changed state to up
00:00:40: %OSPF-5-ADJCHG: Process 1, Nbr 10.10.40.1 on Port-channel12 from LOADING to FULL, Loading Done
Dist-SW2>
Dist-SW2>enable
Password:
Dist-SW2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Dist-SW2(config)#line vty 0 4
Dist-SW2(config-line)#transport input telnet
Dist-SW2(config-line)#password 123
Dist-SW2(config-line)#login
Dist-SW2(config-line)#exit
Dist-SW2(config)#
Copy
Paste
Top
Server-PT E-Mail Server
Server-PT DNS Server
VLAN10: 172.16.10.0/24
VLAN11: 172.16.11.0/24
VLAN12: 172.16.12.0/24
VLAN13: 172.16.13.0/24
VLAN14: 172.16.14.0/24
VLAN15: 172.16.15.0/24
VLAN16: 172.16.16.0/24
Realtime
Simulation
Type here to search
5:09 PM

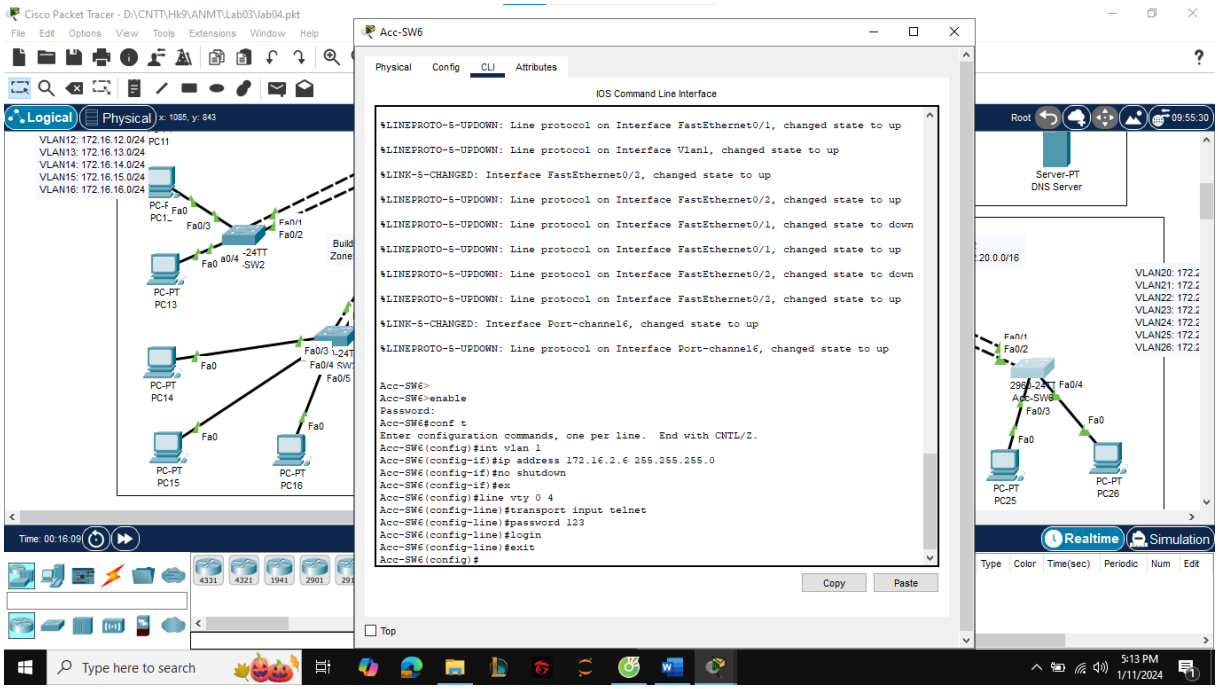

Acc-SW1
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
%LINK-5-CHANGED: Interface Port-channel1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up
Acc-SW1>
Acc-SW1>enable
Password:
Acc-SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Acc-SW1(config)#int vlan 1
Acc-SW1(config-if)#ip address 172.16.1.1 255.255.255.0
Acc-SW1(config-if)#no shutdown
Acc-SW1(config-if)#ex
Acc-SW1(config)#line vty 0 4
Acc-SW1(config-line)#transport input telnet
Acc-SW1(config-line)#password 123
Acc-SW1(config-line)#login
Acc-SW1(config-line)#exit
Acc-SW1(config)#
Copy
Paste
Top
Server-PT
E-Mail Server
Server-PT
DNS Server
VLAN10: 172.16.10.0/24
VLAN11: 172.16.11.0/24
VLAN12: 172.16.12.0/24
VLAN13: 172.16.13.0/24
VLAN14: 172.16.14.0/24
VLAN15: 172.16.15.0/24
VLAN16: 172.16.16.0/24
Realtime
Simulation
Type here to search
4:55 PM
1/11/2024


Acc-SW2
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
%LINK-5-CHANGED: Interface Port-channel2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel2, changed state to up
Acc-SW2>
Acc-SW2>enable
Password:
Acc-SW2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Acc-SW2(config)#int vlan 1
Acc-SW2(config-if)#ip address 172.16.1.2 255.255.255.0
Acc-SW2(config-if)#no shutdown
Acc-SW2(config-if)#ex
Acc-SW2(config)#line vty 0 4
Acc-SW2(config-line)#transport input telnet
Acc-SW2(config-line)#password 123
Acc-SW2(config-line)#login
Acc-SW2(config-line)#exit
Acc-SW2(config)#
Copy
Paste
Top
Server-PT
E-Mail Server
Server-PT
DNS Server
VLAN10: 172.16.10.0/24
VLAN11: 172.16.11.0/24
VLAN12: 172.16.12.0/24
VLAN13: 172.16.13.0/24
VLAN14: 172.16.14.0/24
VLAN15: 172.16.15.0/24
VLAN16: 172.16.16.0/24
Realtime
Simulation
Type here to search
4:57 PM
1/11/2024


Acc-SW3
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface Port-channel3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel3, changed state to up
Acc-SW3>
Acc-SW3>enable
Password:
Acc-SW3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Acc-SW3(config)#int vlan 1
Acc-SW3(config-if)#ip address 172.16.1.3 255.255.255.0
Acc-SW3(config-if)#ex
Acc-SW3(config)#line vty 0 4
Acc-SW3(config-line)#transport input telnet
Acc-SW3(config-line)#password 123
Acc-SW3(config-line)#login
Acc-SW3(config-line)#exit
Acc-SW3(config)#
Copy
Paste
Top
Server-PT
DNS Server
Realtime
Simulation
Type here to search
4:58 PM
1/11/2024

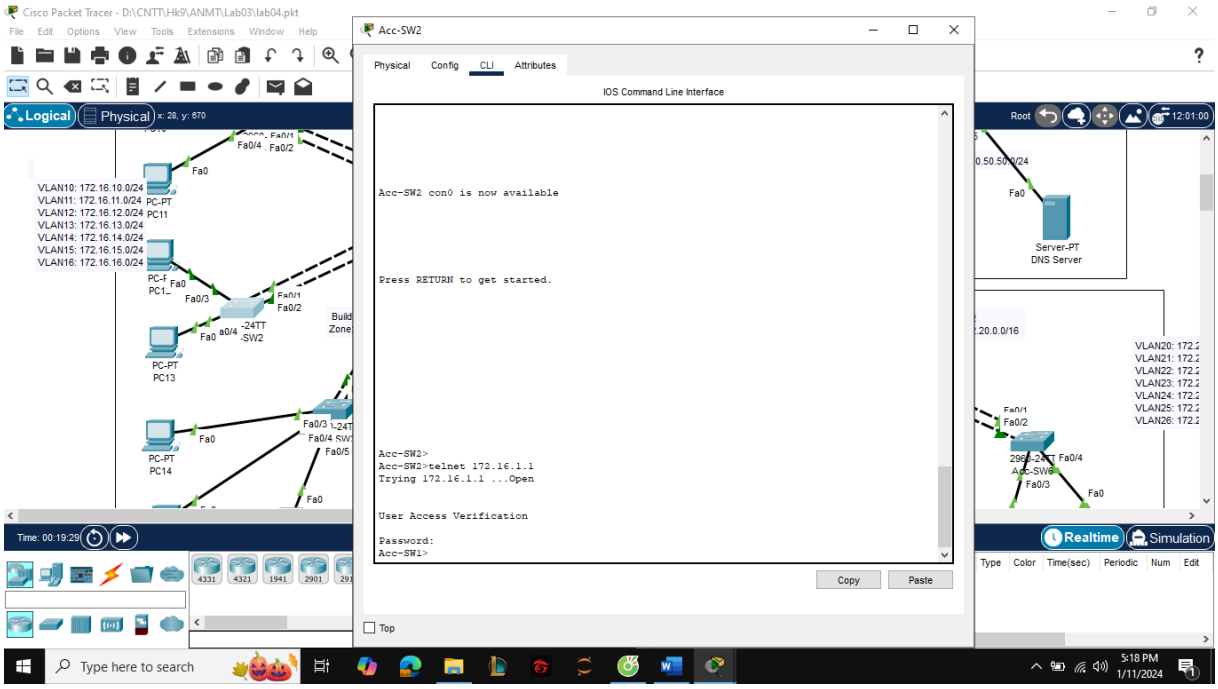

Acc-SW4
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface Port-channel4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel4, changed state to up
Acc-SW4>enable
Password:
Acc-SW4#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Acc-SW4(config)#int vlan 1
Acc-SW4(config-if)#ip address 172.16.2.4 255.255.255.0
Acc-SW4(config-if)#no shutdown
Acc-SW4(config-if)#ex
Acc-SW4(config)#line vty 0 4
Acc-SW4(config-line)#transport input telnet
Acc-SW4(config-line)#password 123
Acc-SW4(config-line)#login
Acc-SW4(config-line)#exit
Acc-SW4(config)#
Copy
Paste
Top
Server-PT
DNS Server
Realtime
Simulation
Type here to search
5:10 PM
1/11/2024


Cisco Packet Tracer - D:\CNTT\Hk9\ANMT\Lab03\lab04.pkt
Acc-SW5
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
%LINK-5-CHANGED: Interface Port-channel5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel5, changed state to up
Acc-SW5>
Acc-SW5>enable
Password:
Acc-SW5#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Acc-SW5(config)#int vlan 1
Acc-SW5(config-if)#ip address 172.16.2.5 255.255.255.0
Acc-SW5(config-if)#no shutdown
Acc-SW5(config-if)#ex
Acc-SW5(config)#line vty 0 4
Acc-SW5(config-line)#transport input telnet
Acc-SW5(config-line)#password 123
Acc-SW5(config-line)#login
Acc-SW5(config-line)#exit
Acc-SW5(config)#
Copy
Paste
Top
Logical
Physical
VLAN15: 172.16.15.0/24
VLAN16: 172.16.16.0/24
PC-PT PC13
PC-PT PC14
PC-PT PC15
PC-PT PC16
PC-PT PC25
PC-PT PC26
Server-PT DNS Server
Realtime
Simulation
Type here to search
5:11 PM
1/11/2024

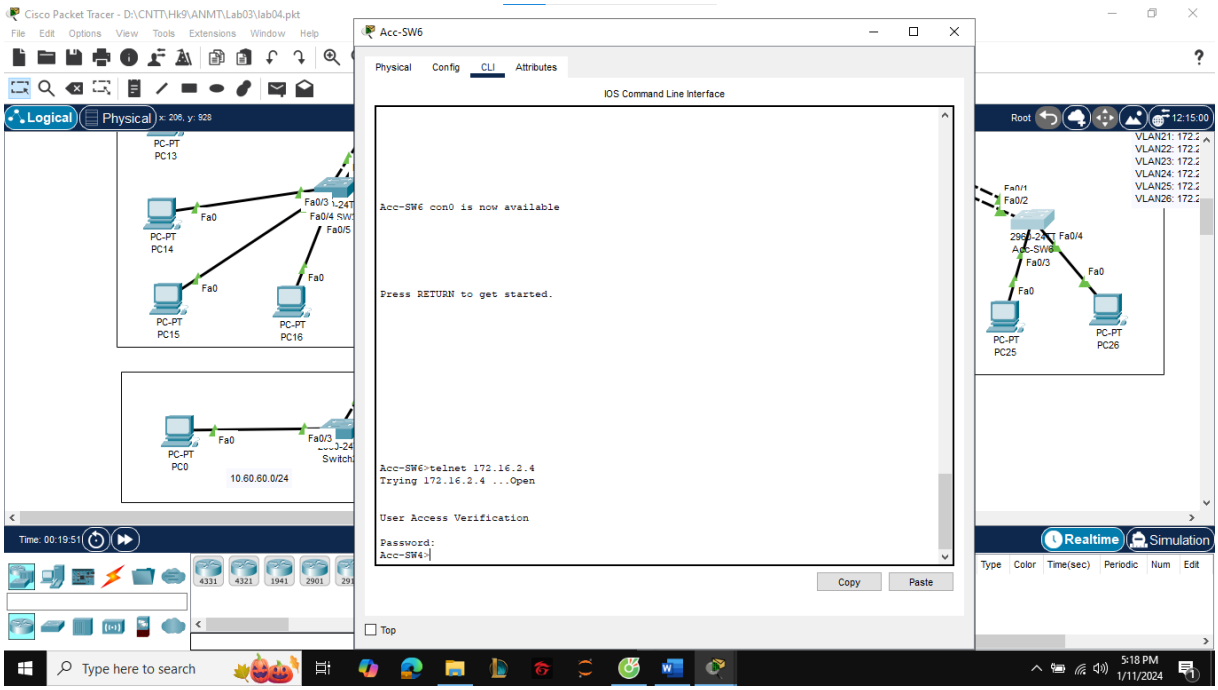

Cisco Packet Tracer - D:\CNTT\Hk9\ANMT\Lab03\lab04.pkt
Acc-SW6
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
%LINK-5-CHANGED: Interface Port-channel6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel6, changed state to up
Acc-SW6>
Acc-SW6>enable
Password:
Acc-SW6#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Acc-SW6(config)#int vlan 1
Acc-SW6(config-if)#ip address 172.16.2.6 255.255.255.0
Acc-SW6(config-if)#no shutdown
Acc-SW6(config-if)#ex
Acc-SW6(config)#line vty 0 4
Acc-SW6(config-line)#transport input telnet
Acc-SW6(config-line)#password 123
Acc-SW6(config-line)#login
Acc-SW6(config-line)#exit
Acc-SW6(config)#
Copy
Paste
Top
Logical
Physical
VLAN12: 172.16.12.0/24
VLAN13: 172.16.13.0/24
VLAN14: 172.16.14.0/24
VLAN15: 172.16.15.0/24
VLAN16: 172.16.16.0/24
PC-PT PC13
PC-PT PC14
PC-PT PC15
PC-PT PC16
PC-PT PC25
PC-PT PC26
Server-PT DNS Server
Realtime
Simulation
Type here to search
5:13 PM
1/11/2024

Kết quả:

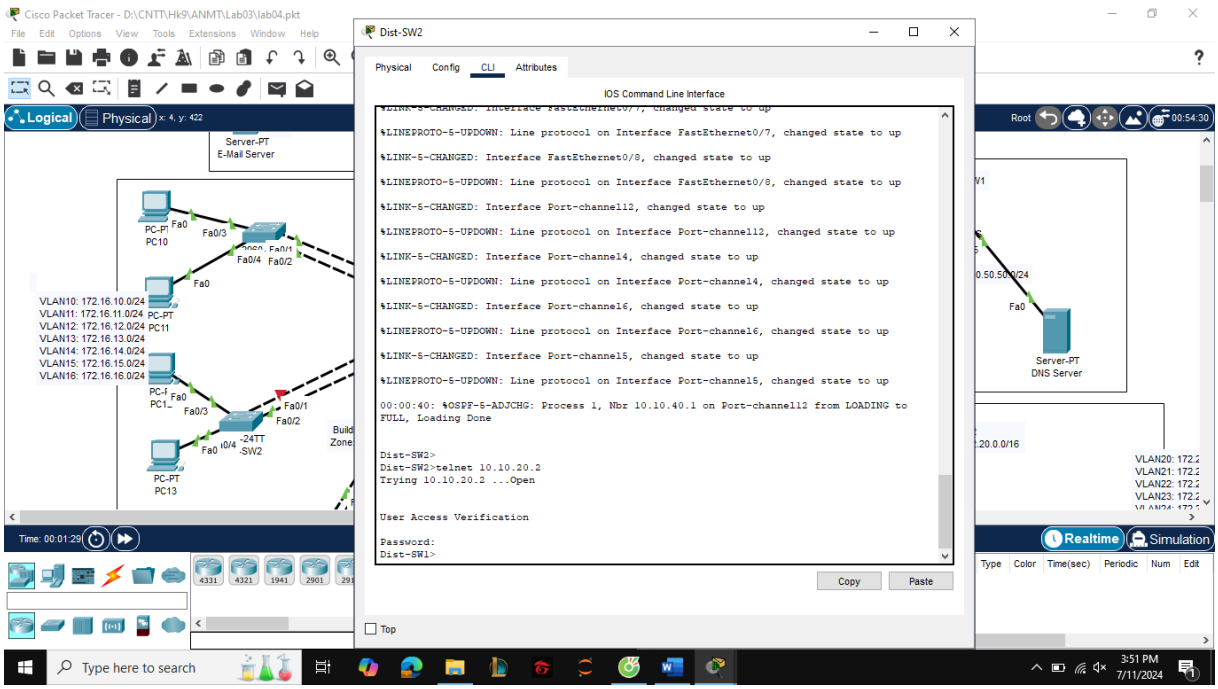
Acc-SW2 kết nối từ xa qua telnet đến Acc-SW1



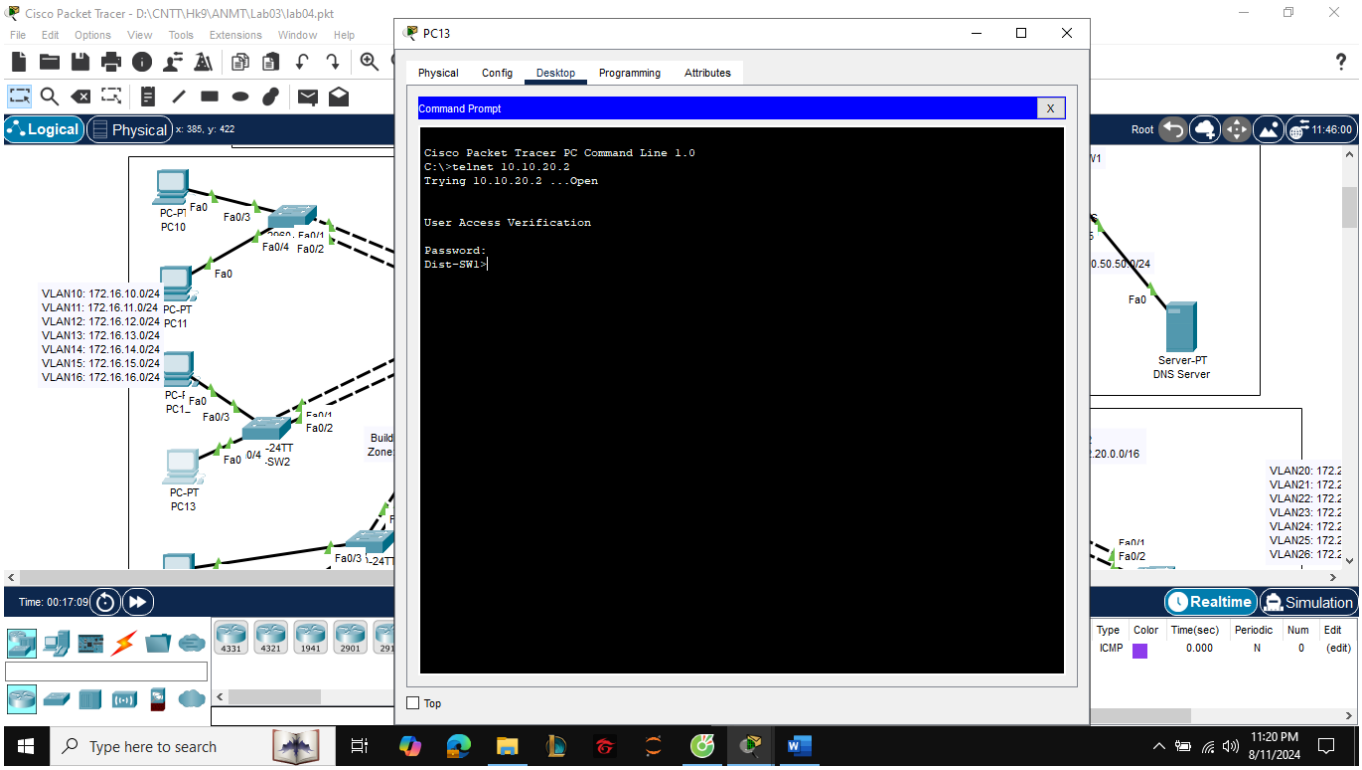
Acc-SW6 kết nối từ xa qua telnet đến Acc-SW4

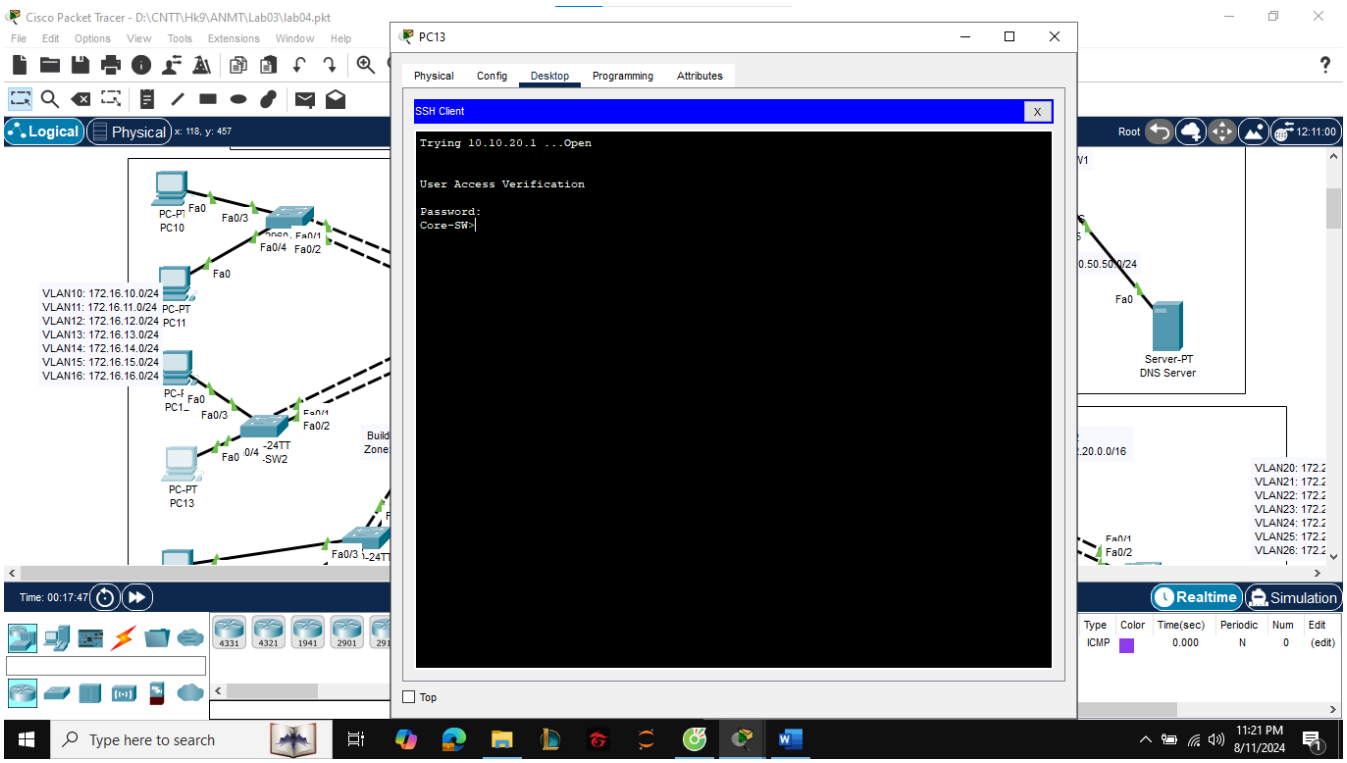


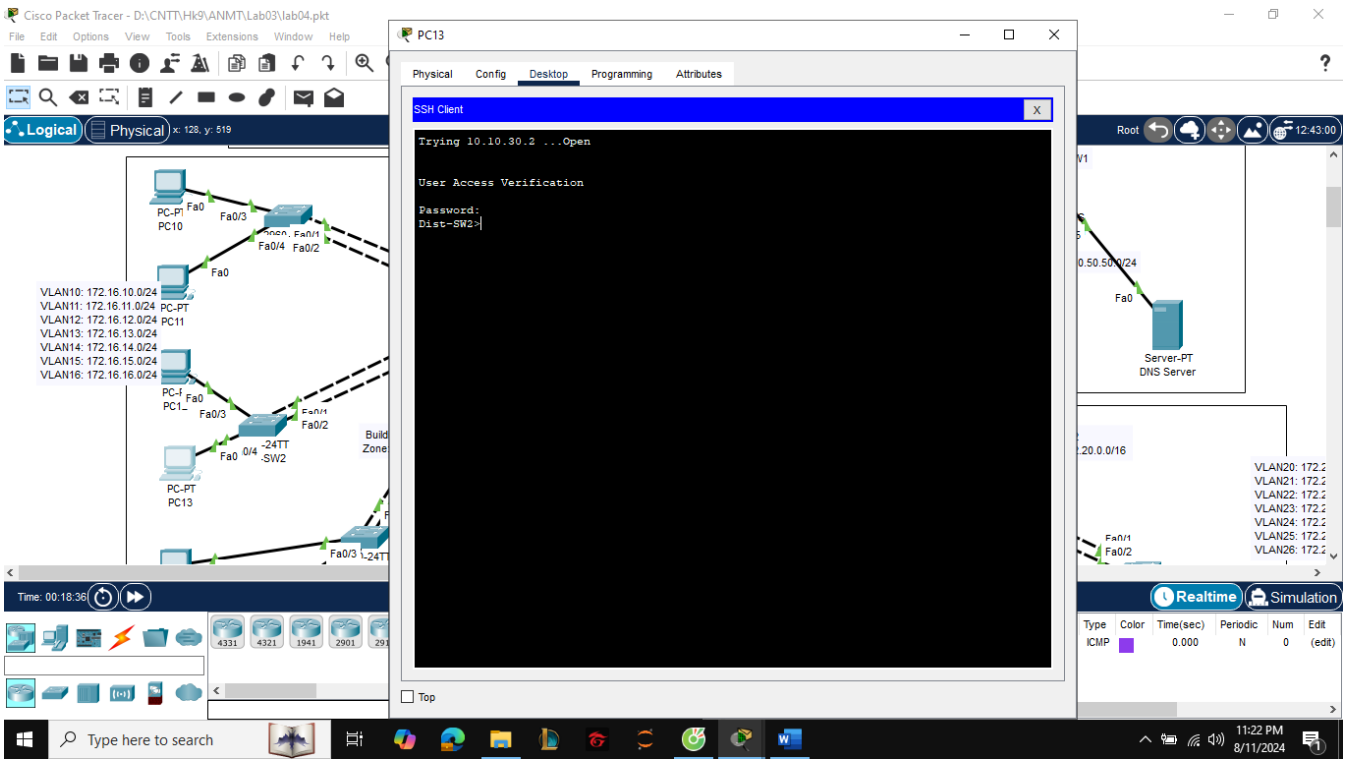
Dist-SW2 kết nối từ xa qua telnet đến Dist-SW1



PC13 kết nối từ xa qua telnet đến Dist-SW1, Core-SW,Dist-SW2

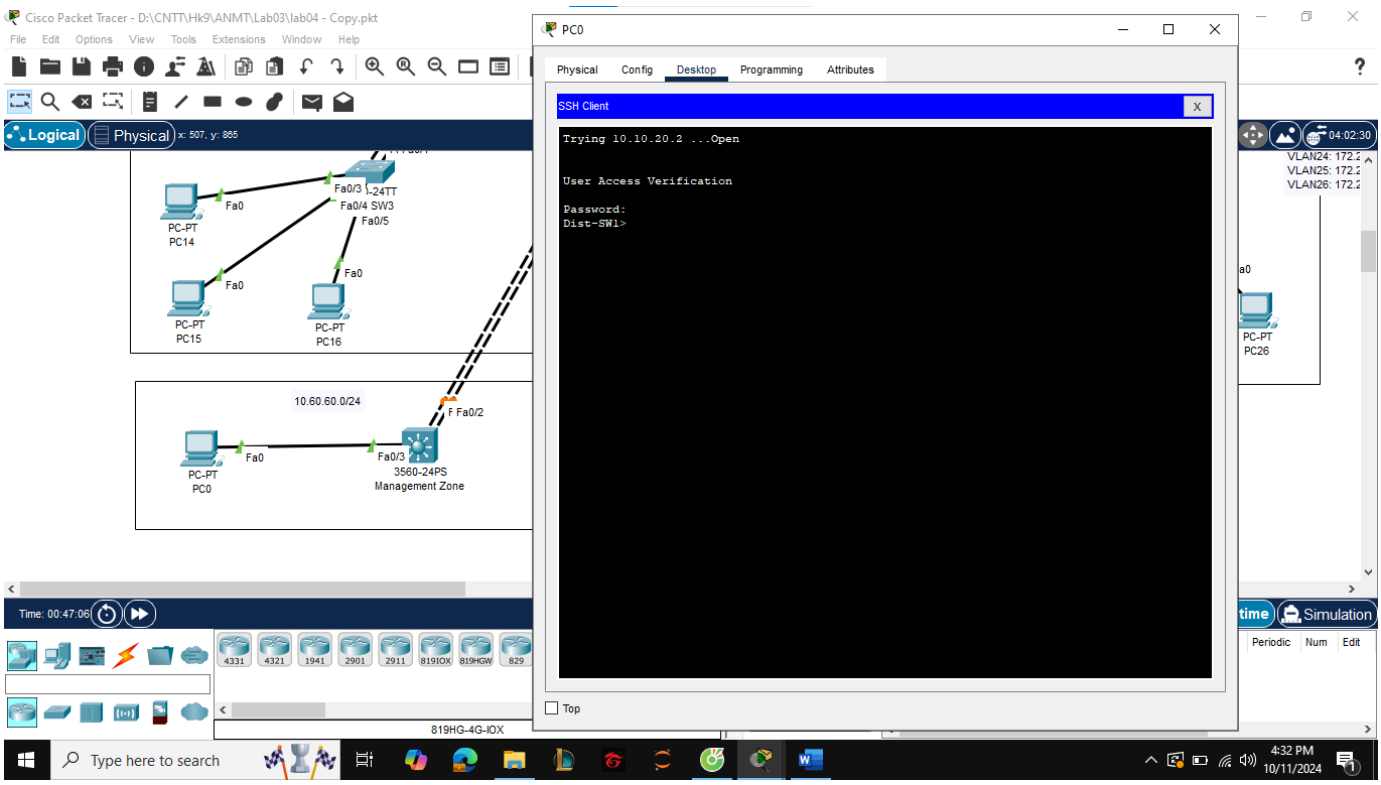


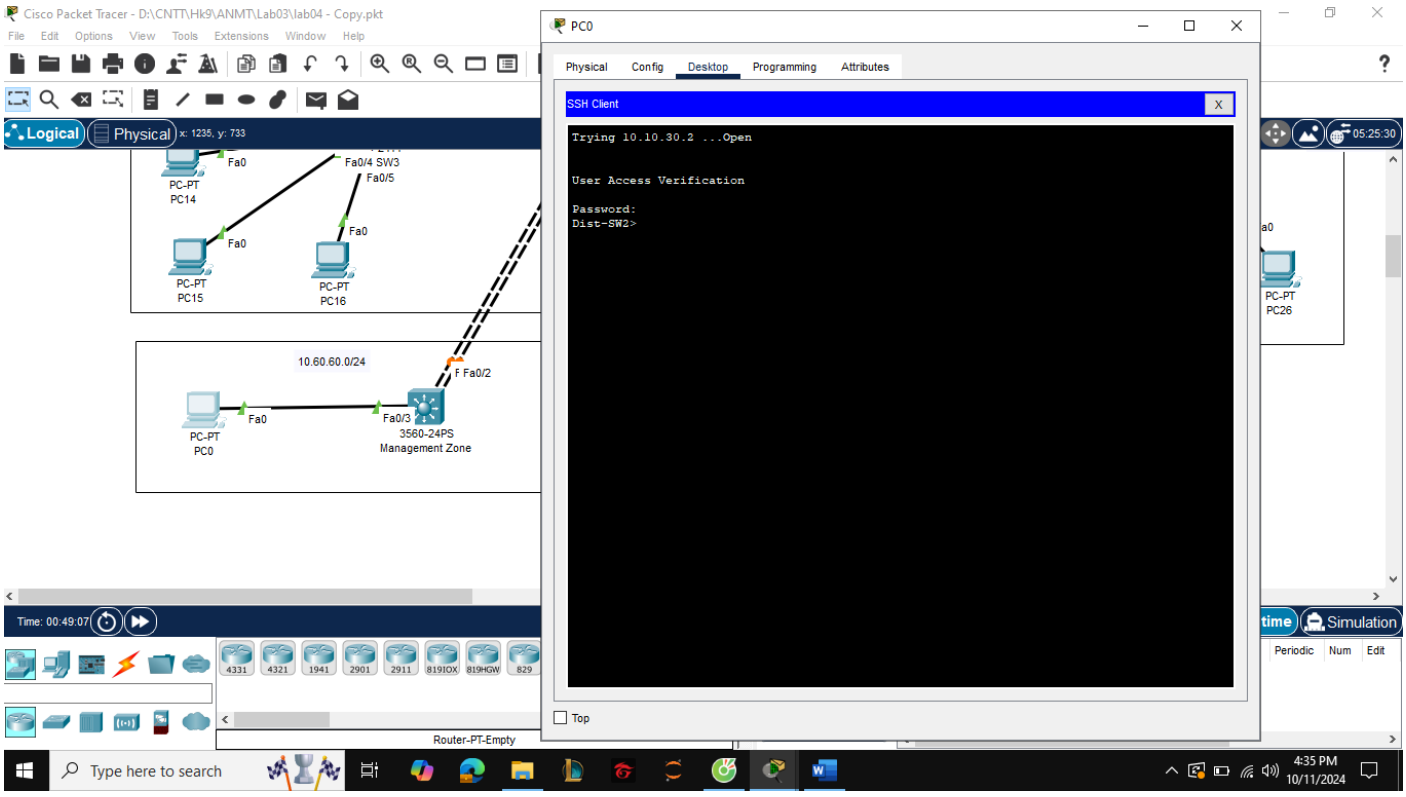




Tương tự các PC khác cũng thực hiện như PC13 để kết nối từ xa qua telnet đến các thiết bị mạng.

PC thuộc khu vực Management Zone kết nối từ xa qua telnet đến các thiết bị mạng:





b) Cấu hình ACL:

- Cấm các PC thuộc VLAN 10 và VLAN 20 ping tới các server trong khu vực Internal Server

Các bước thực hiện:

Dist-SW1:

```
Dist-SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Dist-SW1(config)#ip access-list extended BLOCK_VLAN10
Dist-SW1(config-ext-nacl)#deny icmp 172.16.10.0 0.0.0.255 10.50.50.0 0.0.0.255
Dist-SW1(config-ext-nacl)#permit ip any any
Dist-SW1(config-ext-nacl)#exit
Dist-SW1(config)#interface vlan 10
Dist-SW1(config-if)#ip access-group BLOCK_VLAN10 in
Dist-SW1(config-if)#ex
```

Dist-SW2:

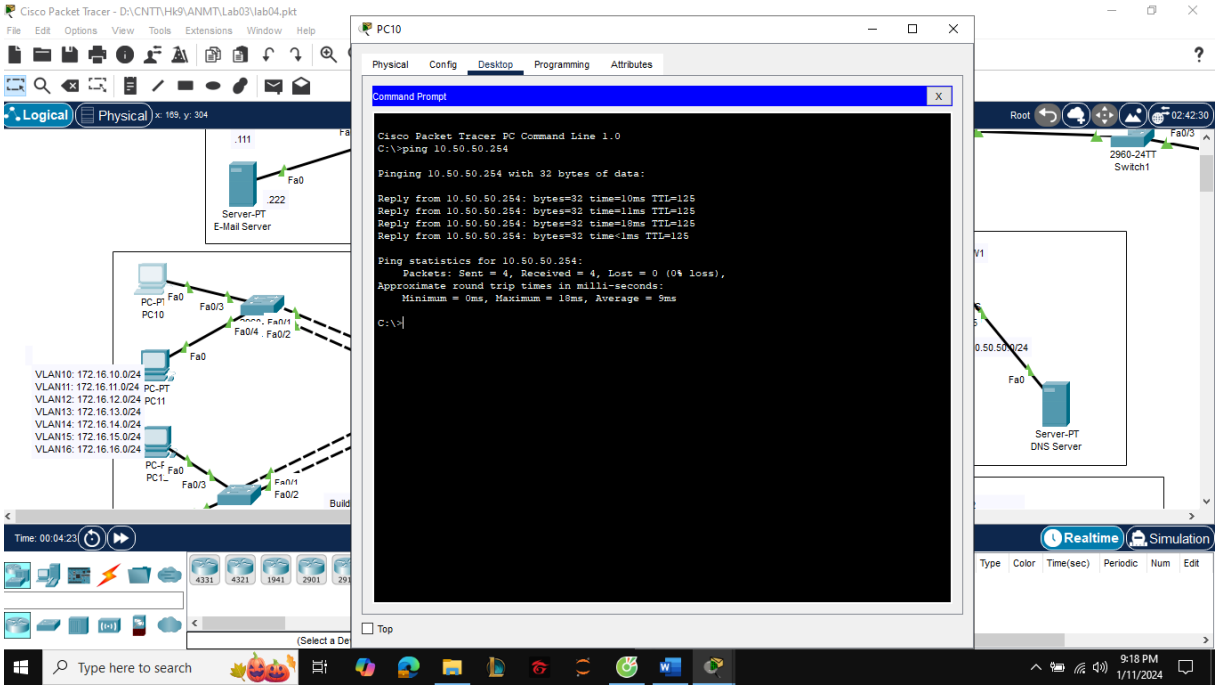
```
Password:
Dist-SW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Dist-SW2(config)#ip access-list extended BLOCK_VLAN20
Dist-SW2(config-ext-nacl)#deny icmp 172.20.20.0 0.0.0.255 10.50.50.0 0.0.0.255
Dist-SW2(config-ext-nacl)#permit ip any any
Dist-SW2(config-ext-nacl)#exit
Dist-SW2(config)#permit ip any any
                 ^
% Invalid input detected at '^' marker.

Dist-SW2(config)#int vlan 20
Dist-SW2(config-if)#ip access-group BLOCK_VLAN20 in
Dist-SW2(config-if)#exit
```

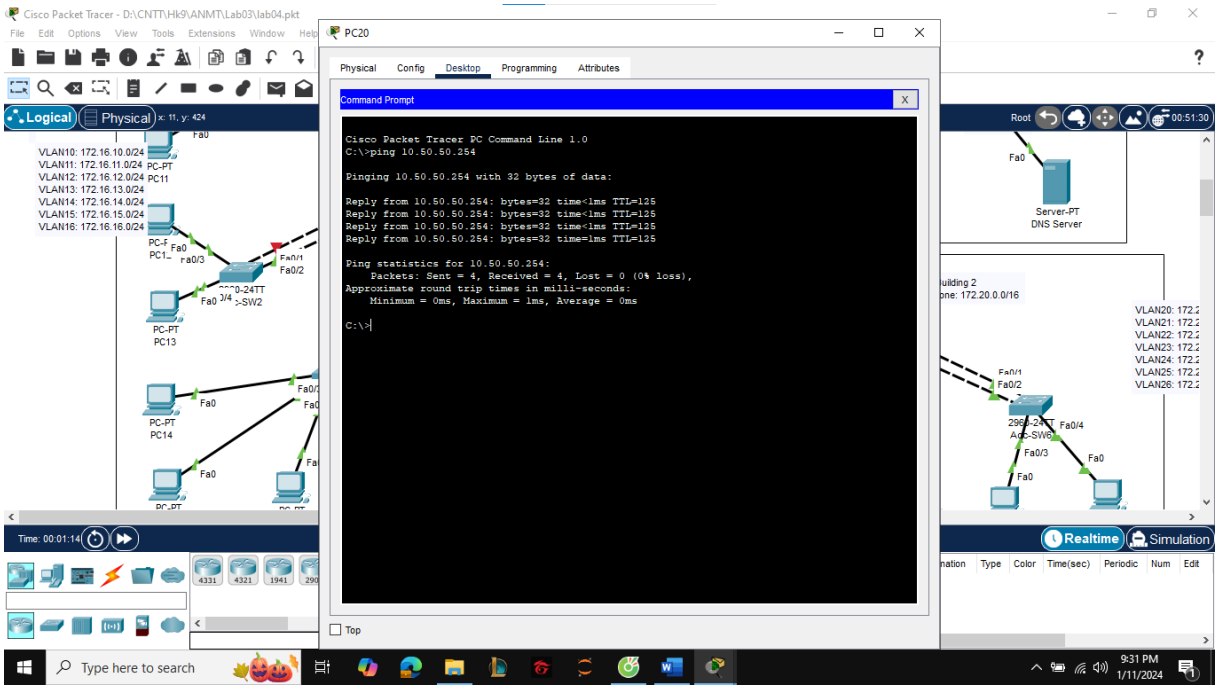
Kết quả:

Trước khi cấu hình ACL:

PC thuộc VLAN10:

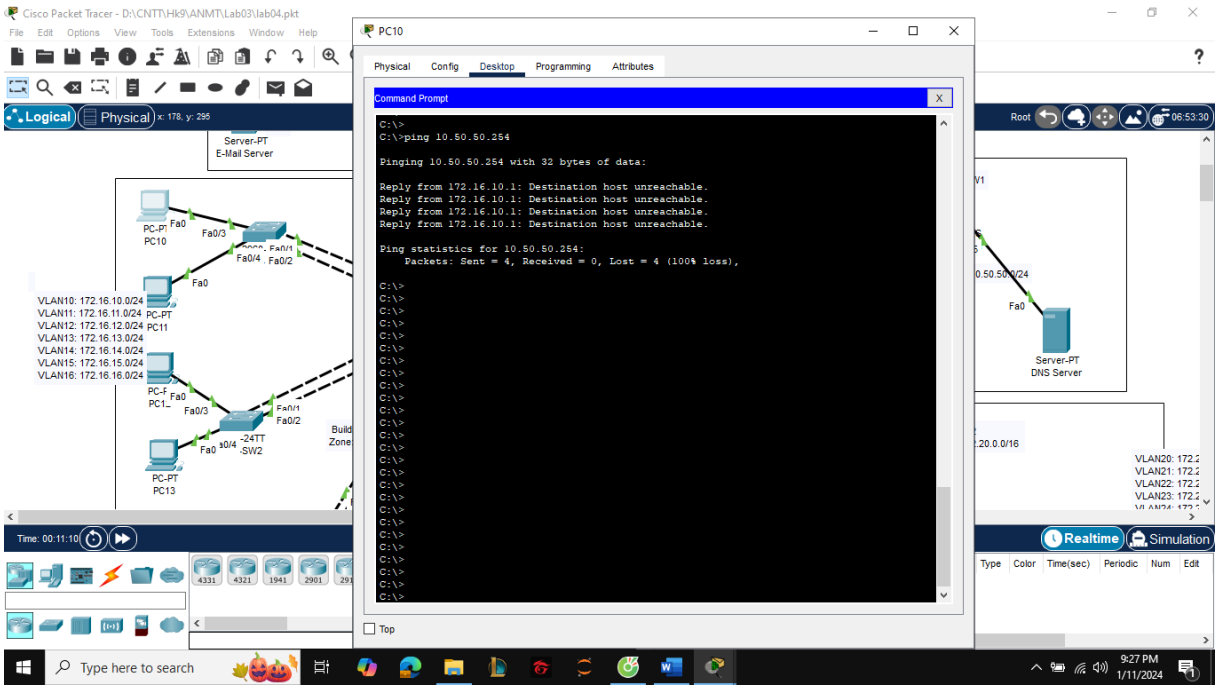


PC thuộc VLAN20:

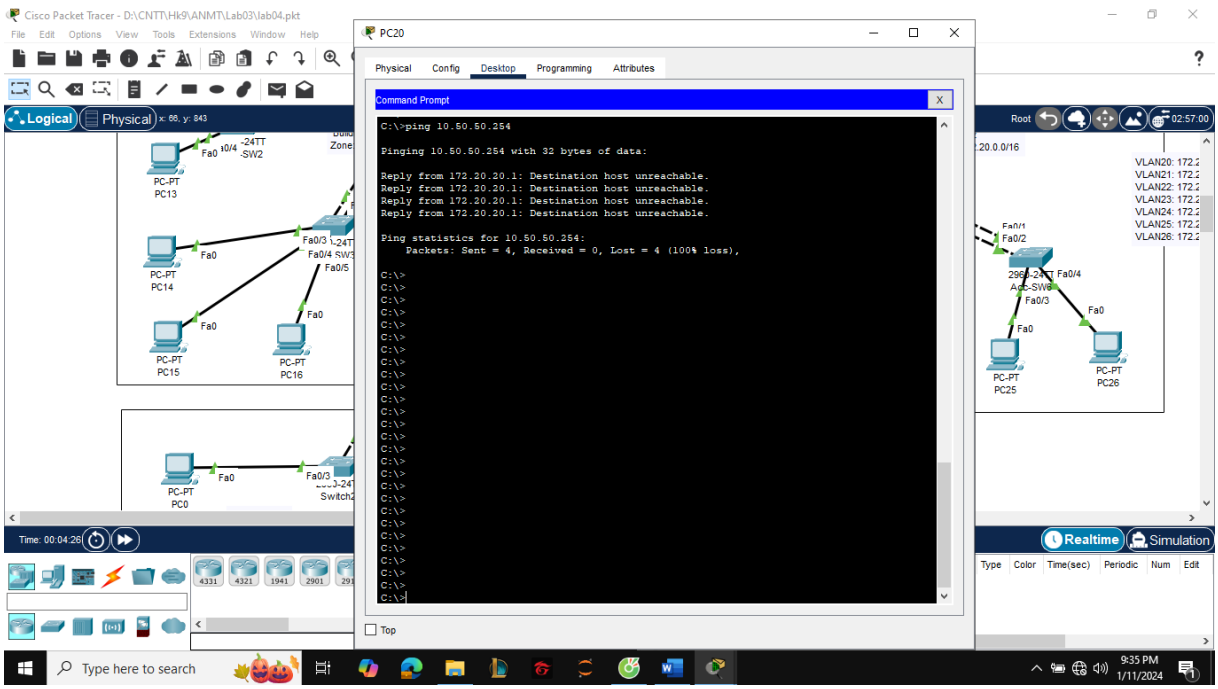


Sau khi cấu hình ACL:

PC thuộc VLAN10:



PC thuộc VLAN20:



- Chỉ cho phép các PC trong khu vực quản trị được phép quản trị từ xa các thiết bị mạng (CoreSW, Dist-SW1, Dist-SW2, Access-SW1 → Access-SW6)

Các bước thực hiện:

Cấu hình ACL trên các thiết bị mạng sau đó áp dụng vào line vty mở ở câu a:

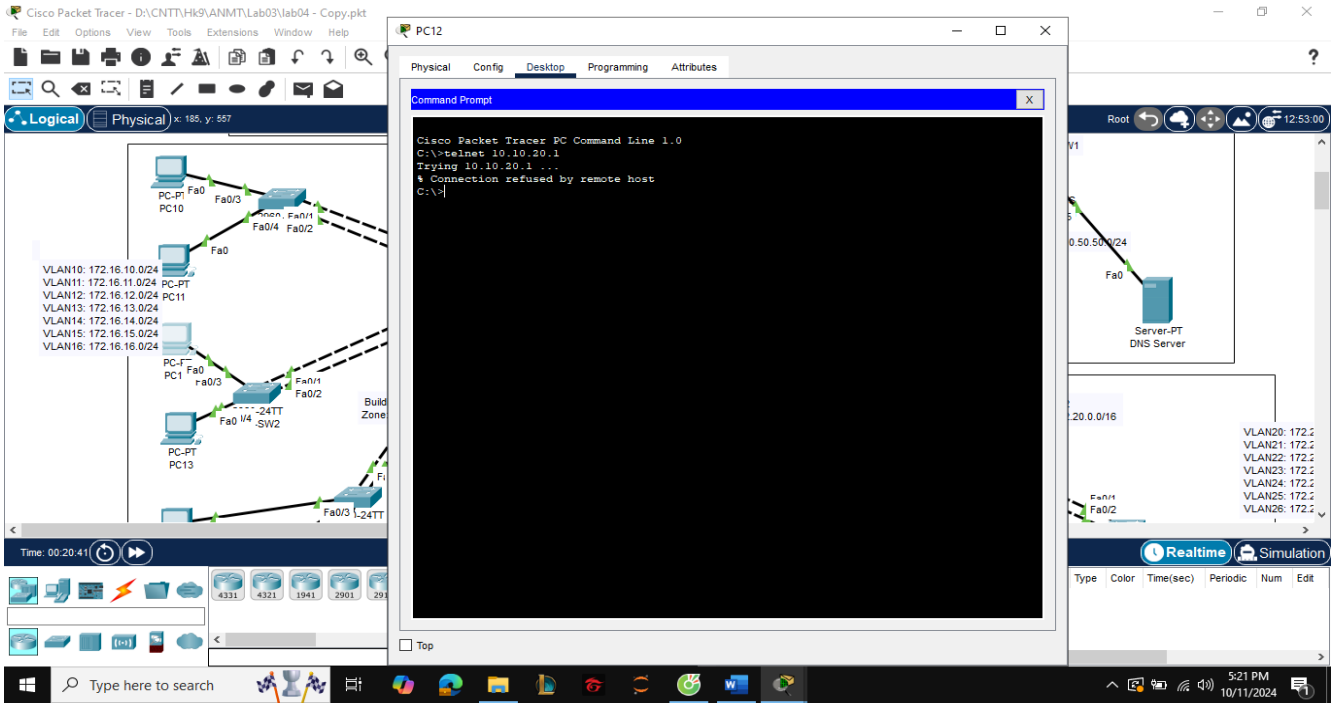
```
Core-SW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Core-SW(config)#access-list 1 permit 10.60.60.0 0.0.0.255
Core-SW(config)#access-list 1 deny any
Core-SW(config)#line vty 0 4
Core-SW(config-line)#access-class 1 in
Core-SW(config-line)#end
```

```
Dist-SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Dist-SW1(config)#access-list 1 permit 10.60.60.0 0.0.0.255
Dist-SW1(config)#access-list 1 deny any
Dist-SW1(config)#line vty 0 4
Dist-SW1(config-line)#access-class 1 in
Dist-SW1(config-line)#end
```

Tương tự cấu hình ACL như trên với các thiết bị mạng còn lại

Kết quả sau khi cấu hình ACL trên:

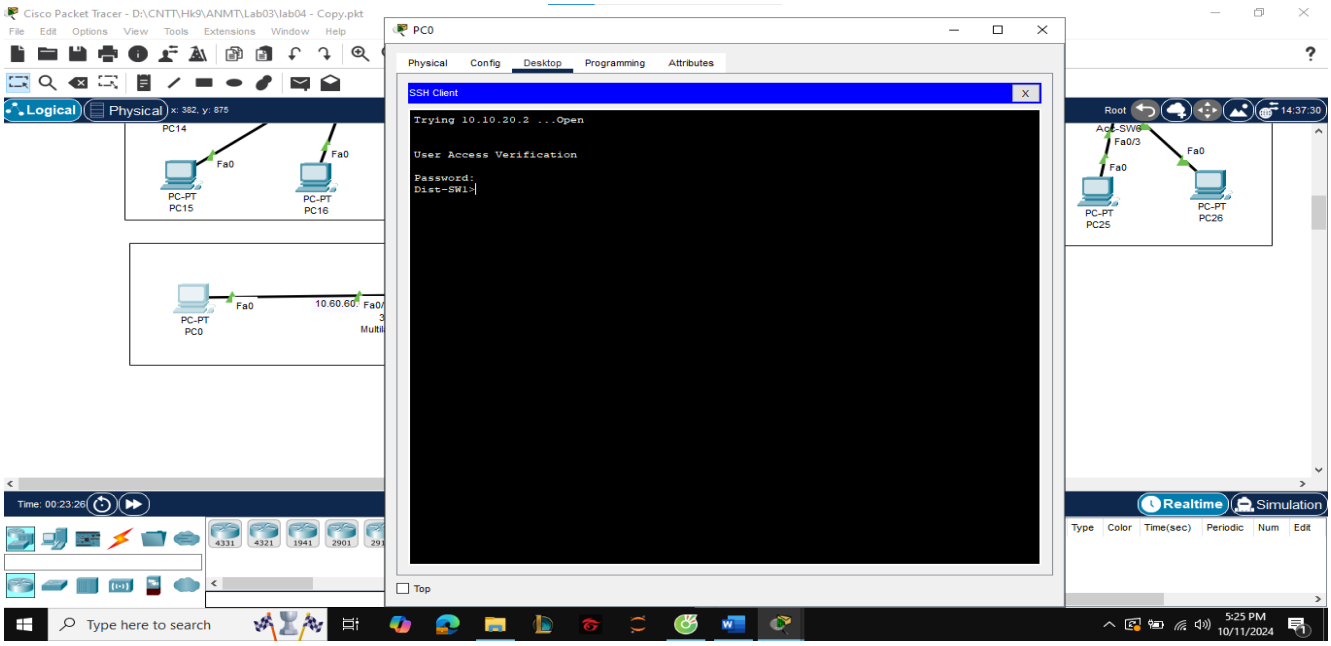
Các PC hay thiết bị mạng không thuộc khu vực Management Zone thì sẽ không kết nối từ xa qua telnet được

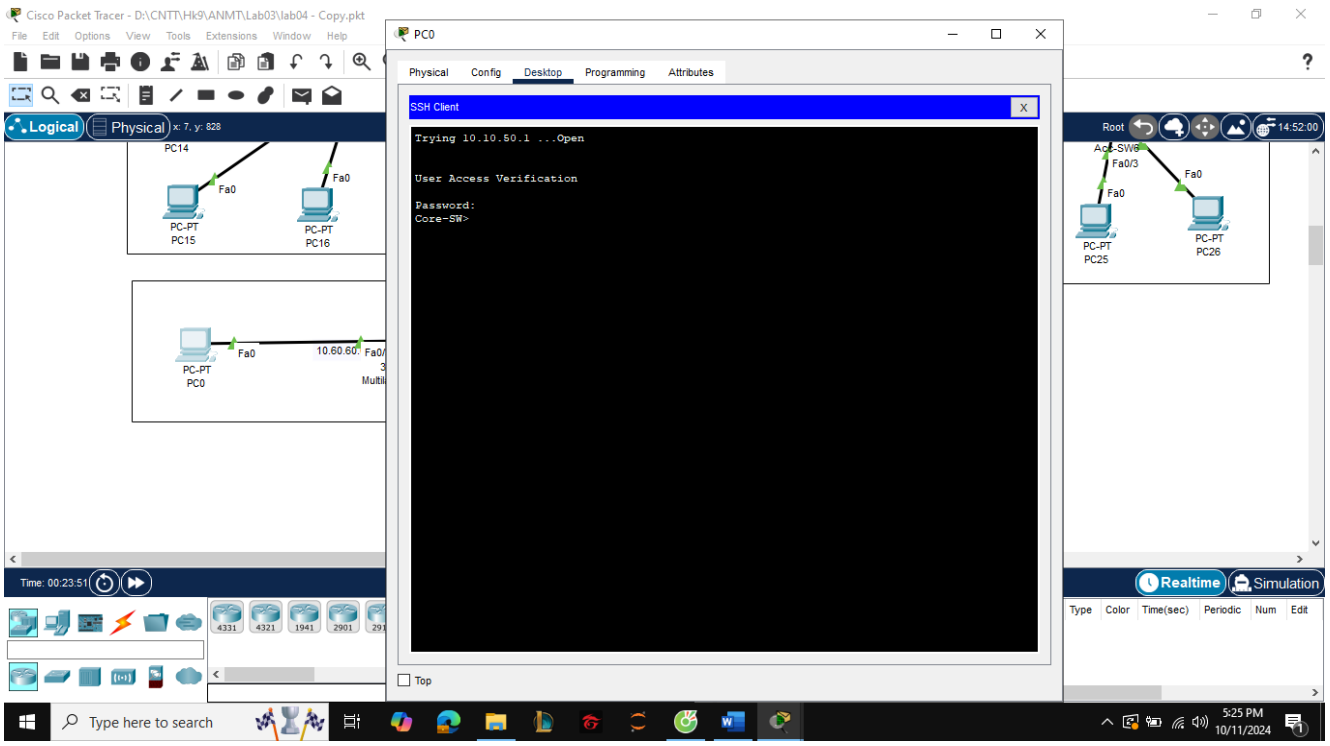



```
Dist-SW2>
Dist-SW2>telnet 10.10.20.1
Trying 10.10.20.1 ...
% Connection refused by remote host
Dist-SW2>
```

```
Dist-SW1>
Dist-SW1>telnet 10.10.30.2
Trying 10.10.30.2 ...
% Connection refused by remote host
Dist-SW1>
```

PC thuộc khu vực Management Zone :





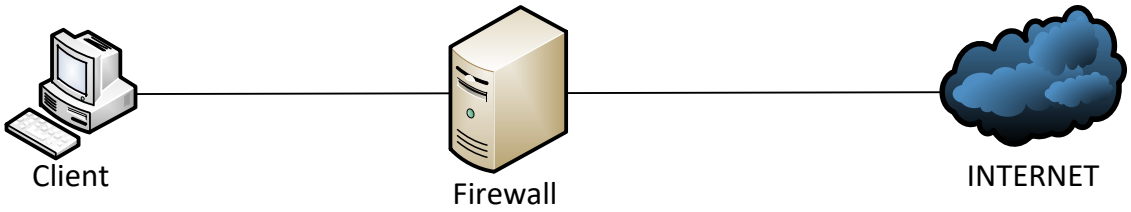
4. **Firewall** (2,0 điểm)

c) ASA

a. Firewall rule: inside → outside

d) Sinh viên tự chọn một Firewall dạng VMWare để thử nghiệm ***(Fortigate****, Checkpoint,...)*

Topology



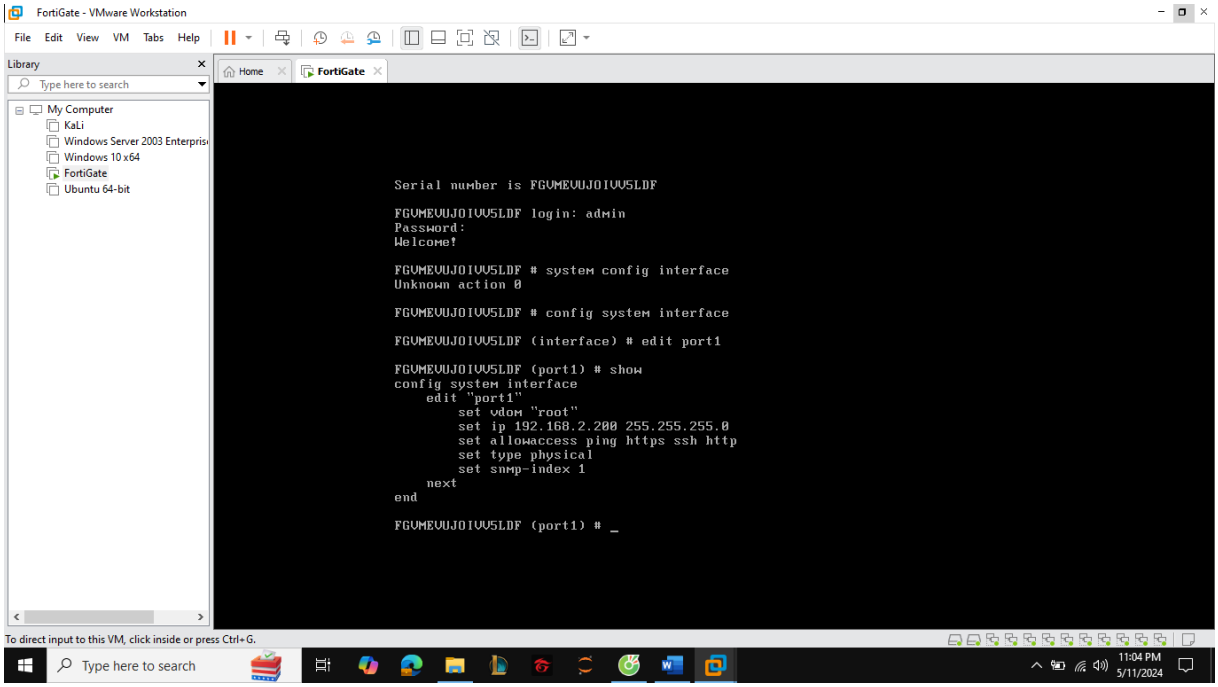
Thực hiện các rule:

- Cho phép các PC bên trong mạng nội bộ ra ngoài Internet
- Kiểm soát truy cập Web
- Kiểm soát port truy cập
- Kiểm soát ứng dụng truy cập
- Thực hiện các phương thức khác

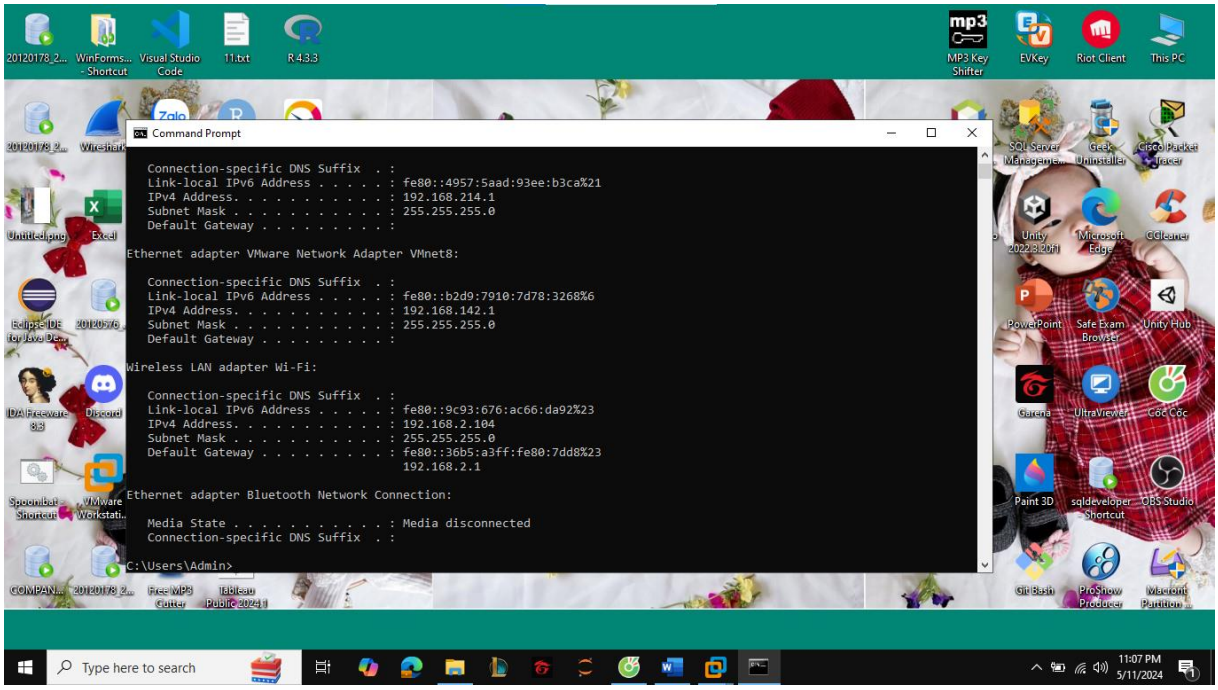
SV có thể sử dụng các FW dạng VMWare: Fortigate, Checkpoint,…

Các bước thực hiện:

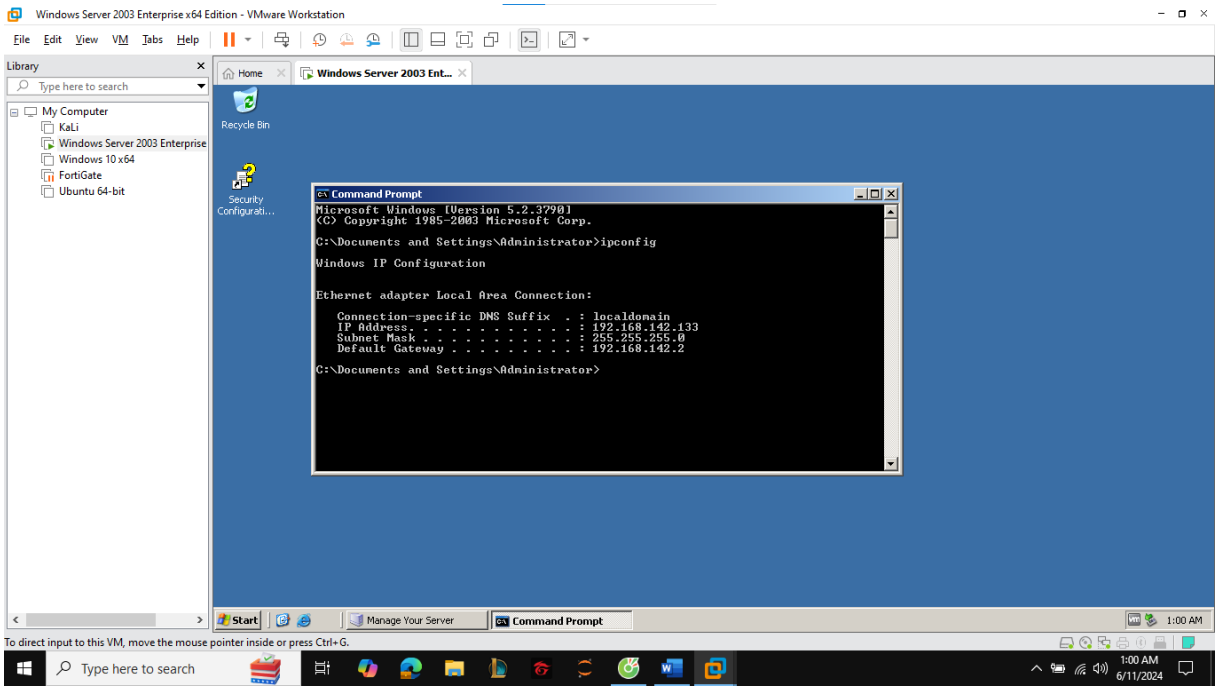
Cấu hình Fortigate:



Internet

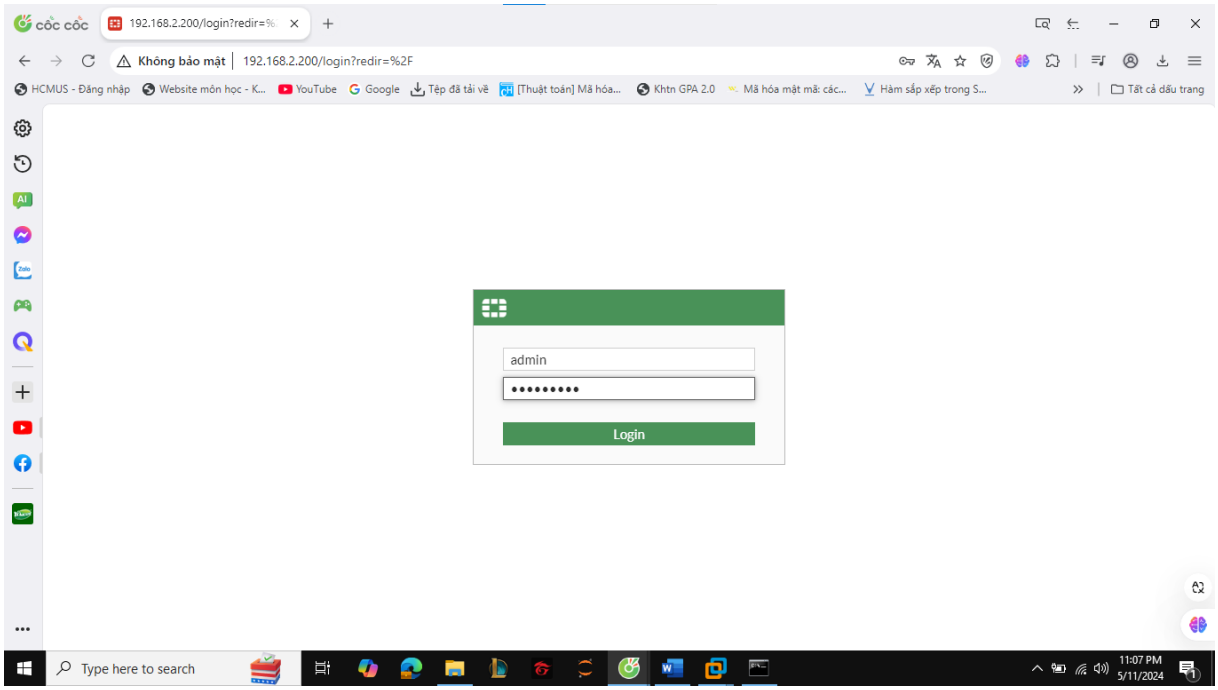


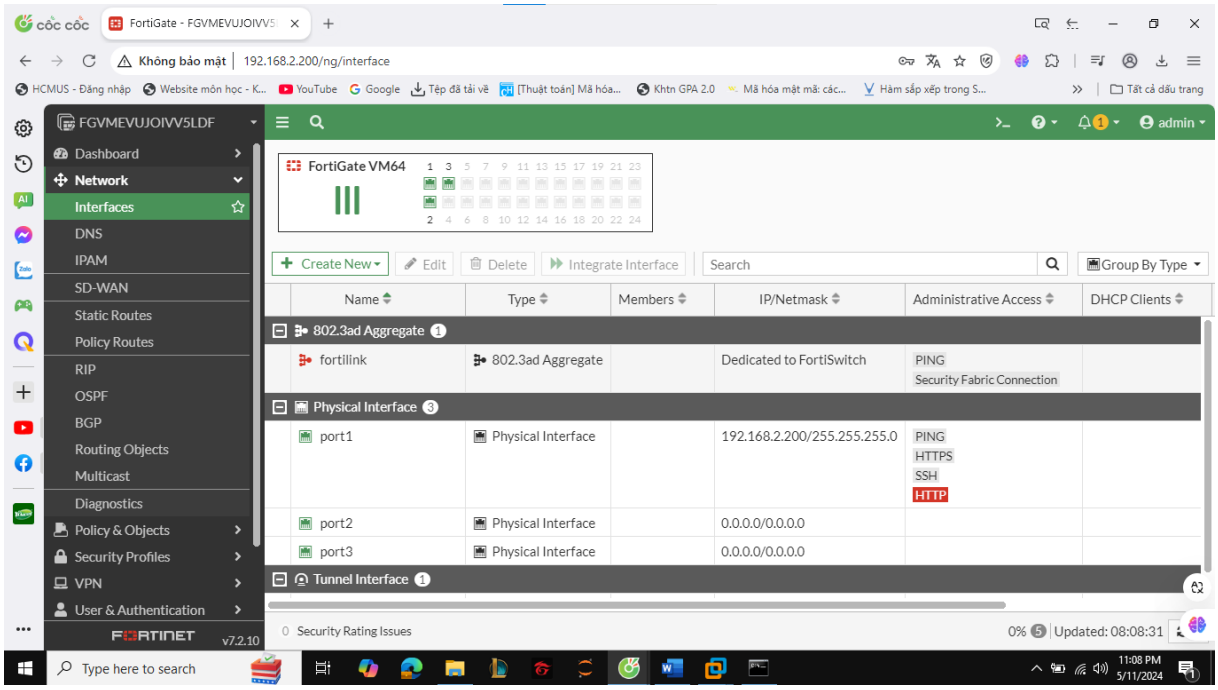
Máy client



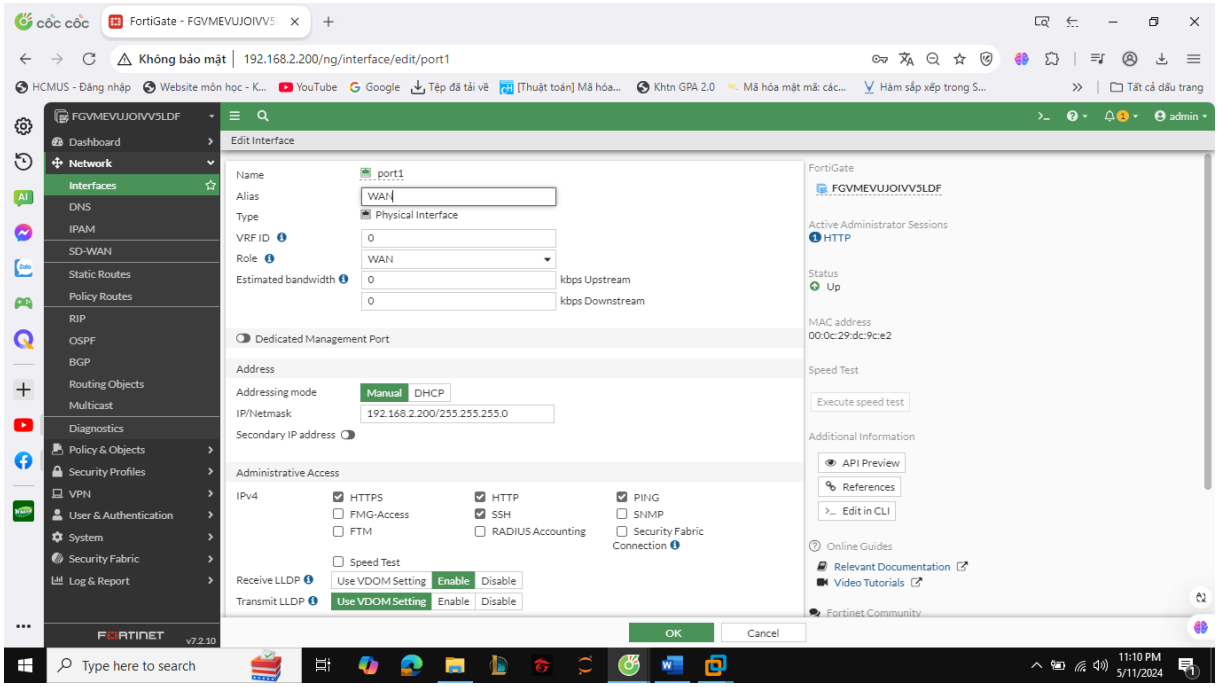
Đầu tiên cấu hình Network:

B1:Đăng nhập fortigate trên máy internet

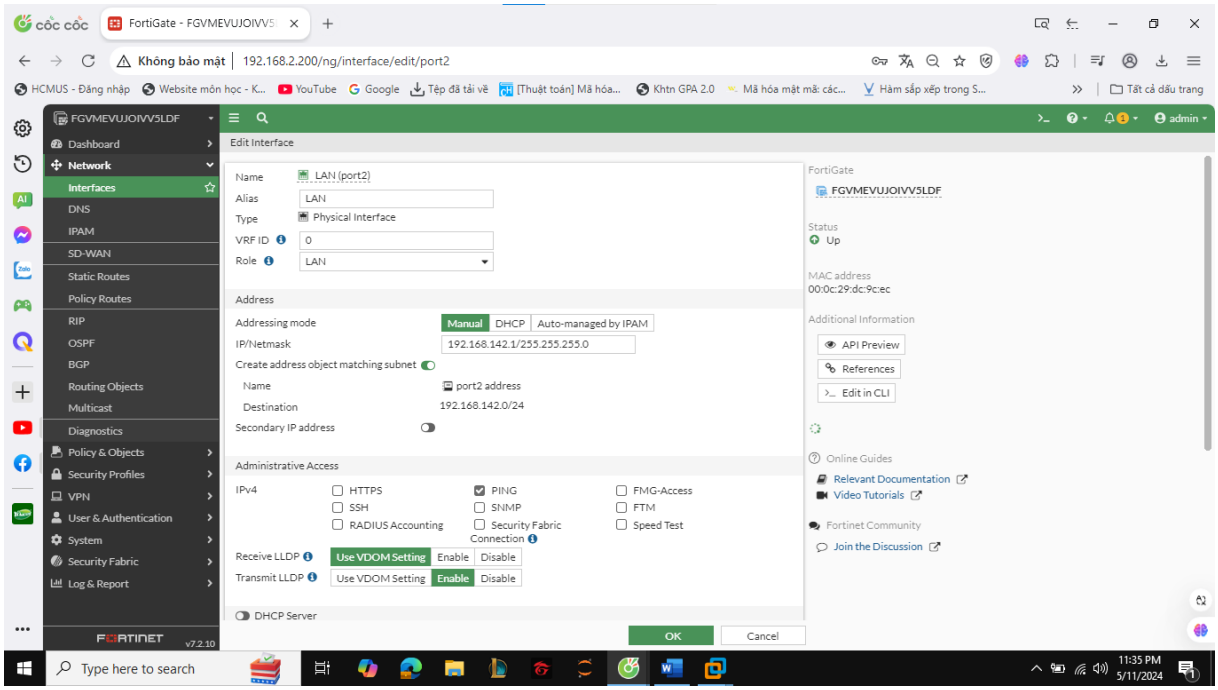




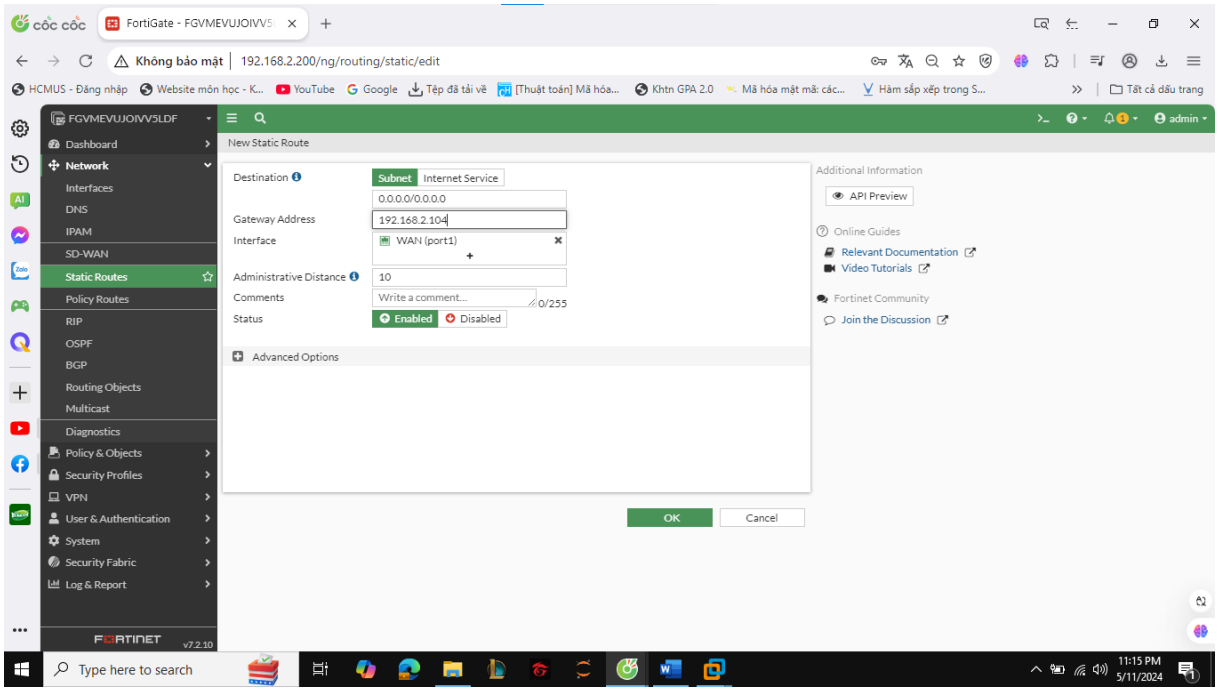
B2: Edit port1 như bên dưới. Rồi nhấn OK



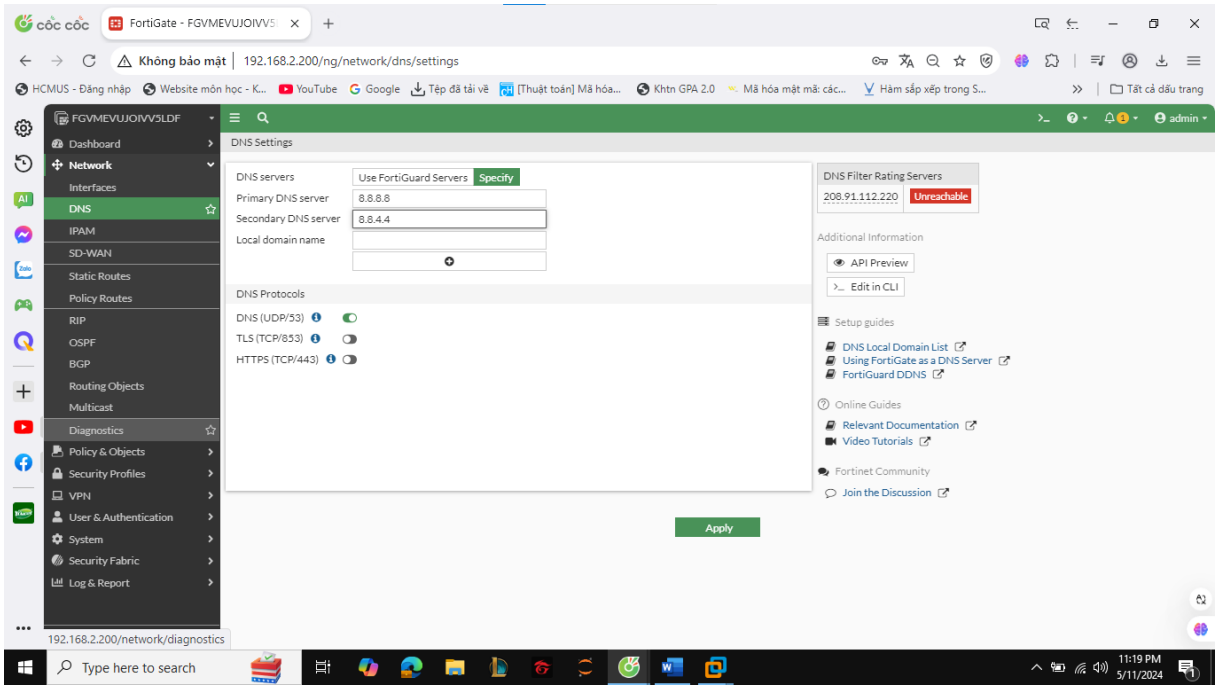
B3: Edit port2 như dưới . Rồi nhấn OK



B4: Cấu hình Static Routes như dưới . Rồi nhấn OK



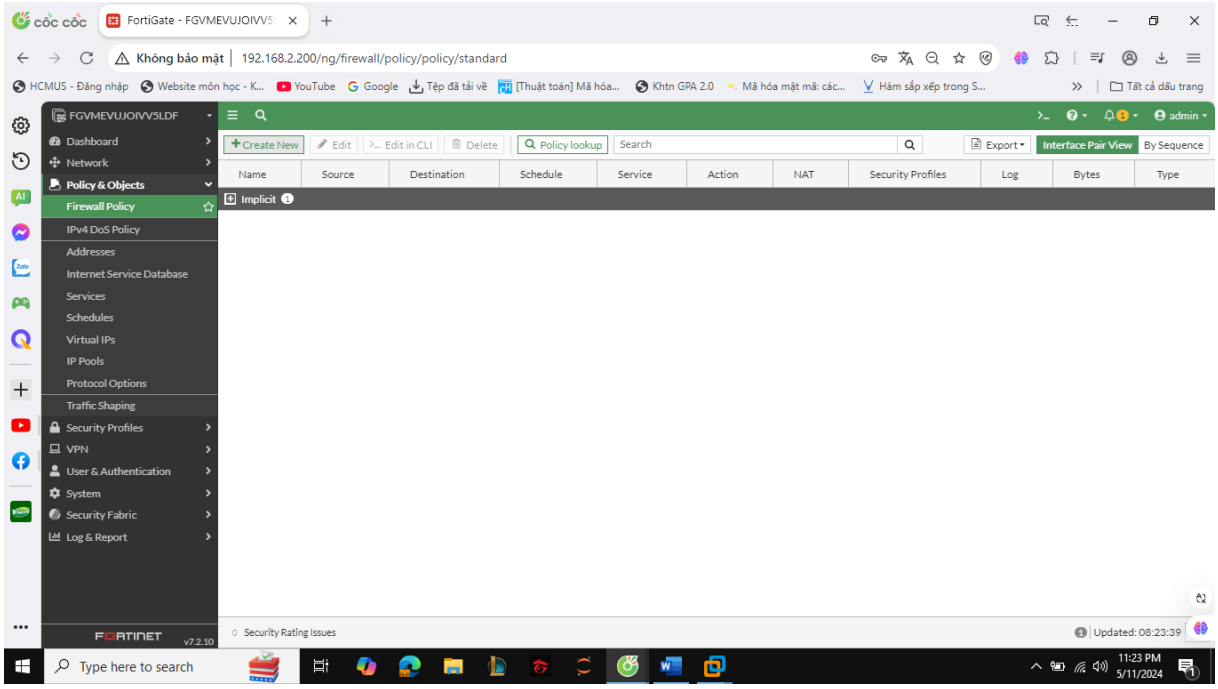
B5: Cấu hình DNS. Rồi nhấn Apply



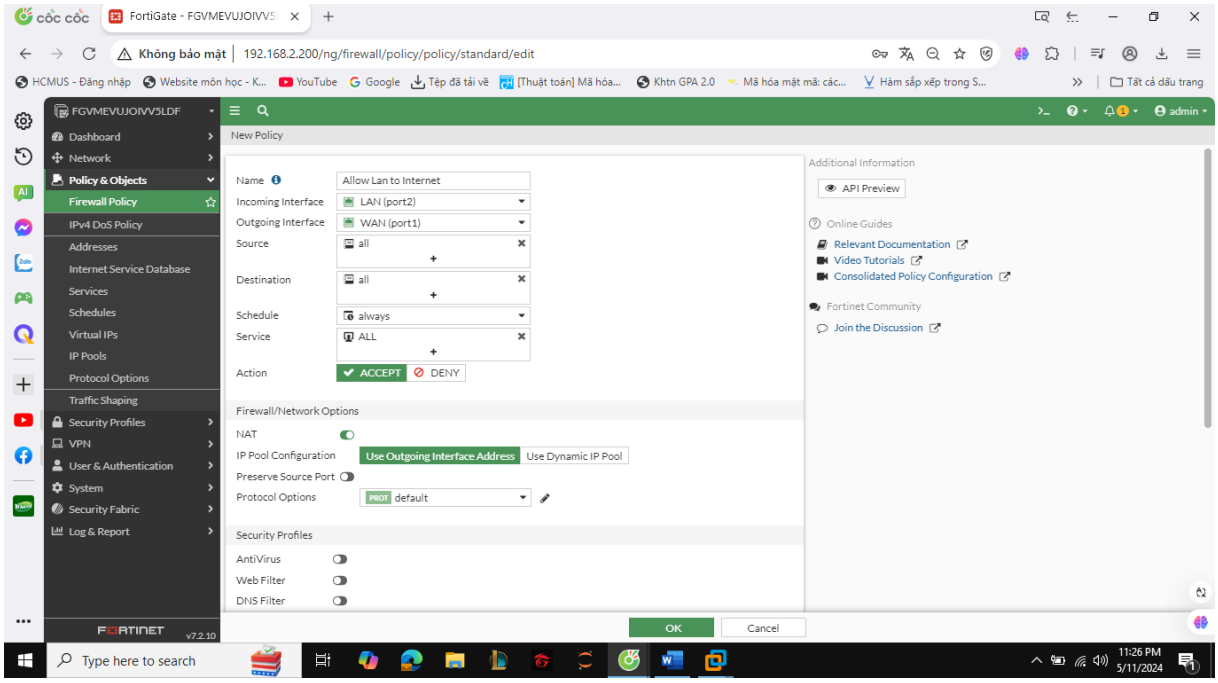
Thực hiện các rule:

- Cho phép các PC bên trong mạng nội bộ ra ngoài Internet

B1: Chọn Firewall Policy. Rồi nhấn chọn Create New

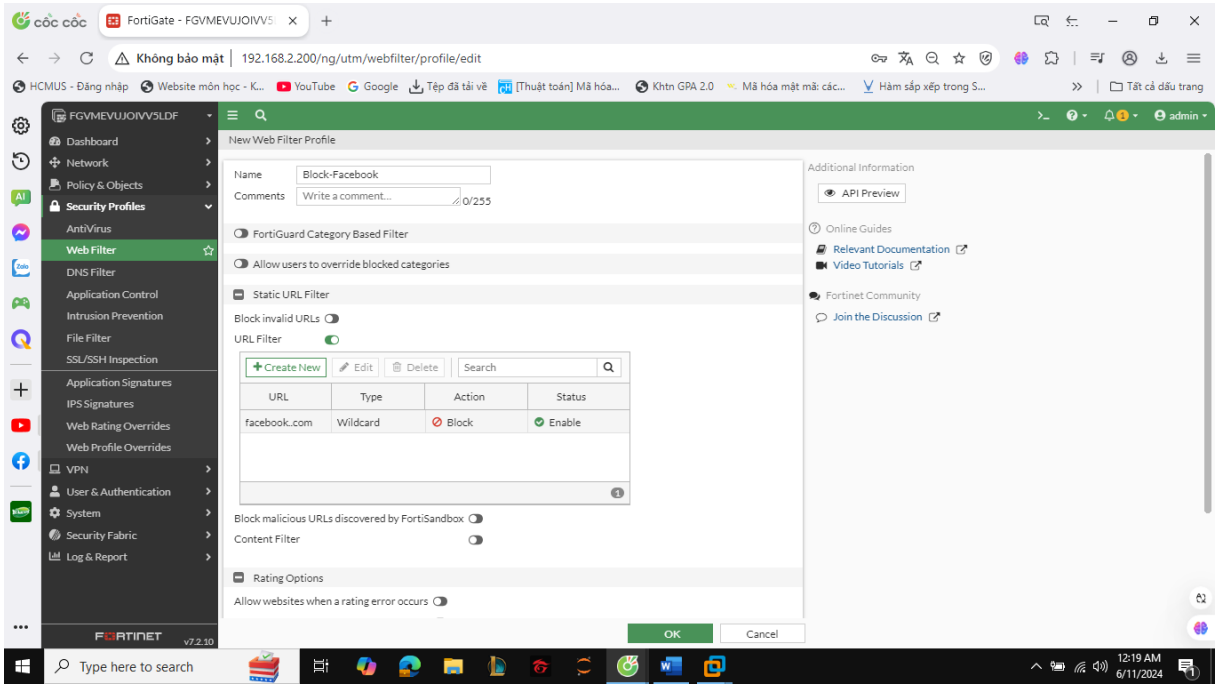


B2:Điền và chọn các thông tin như bên dưới. Rồi nhấn OK

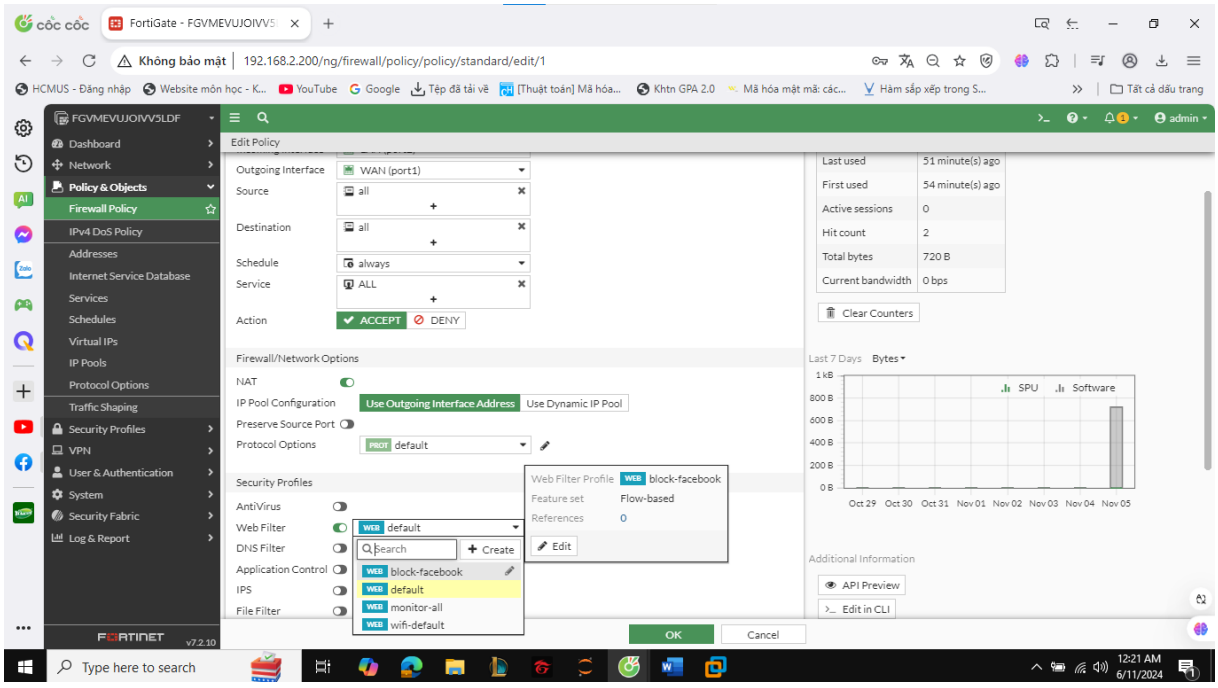


- Kiểm soát truy cập Web

B1: Tạo Web Filter Profile

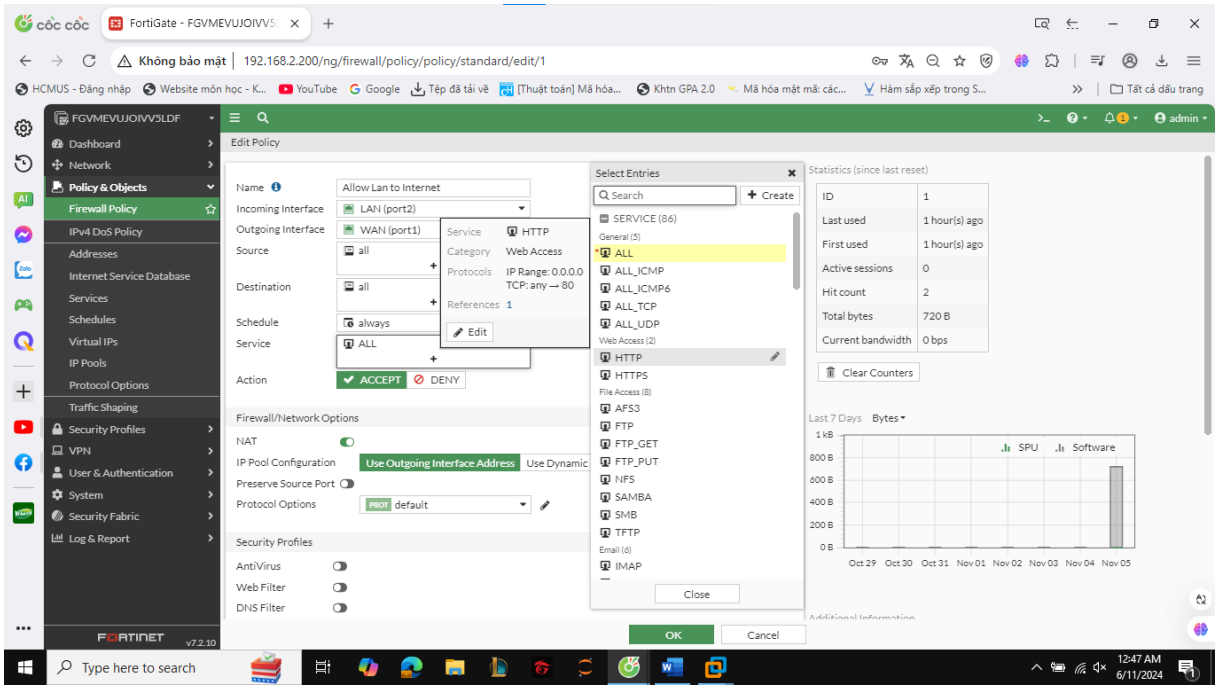


B2: Tạo policy để kiểm soát truy cập Web. Bật Web Filter và chọn Web Filter Profile vừa tạo . Sau đó nhấn OK



- Kiểm soát port truy cập

Trong phần Service, chọn port mà bạn muốn kiểm soát. Sau đó nhấn OK



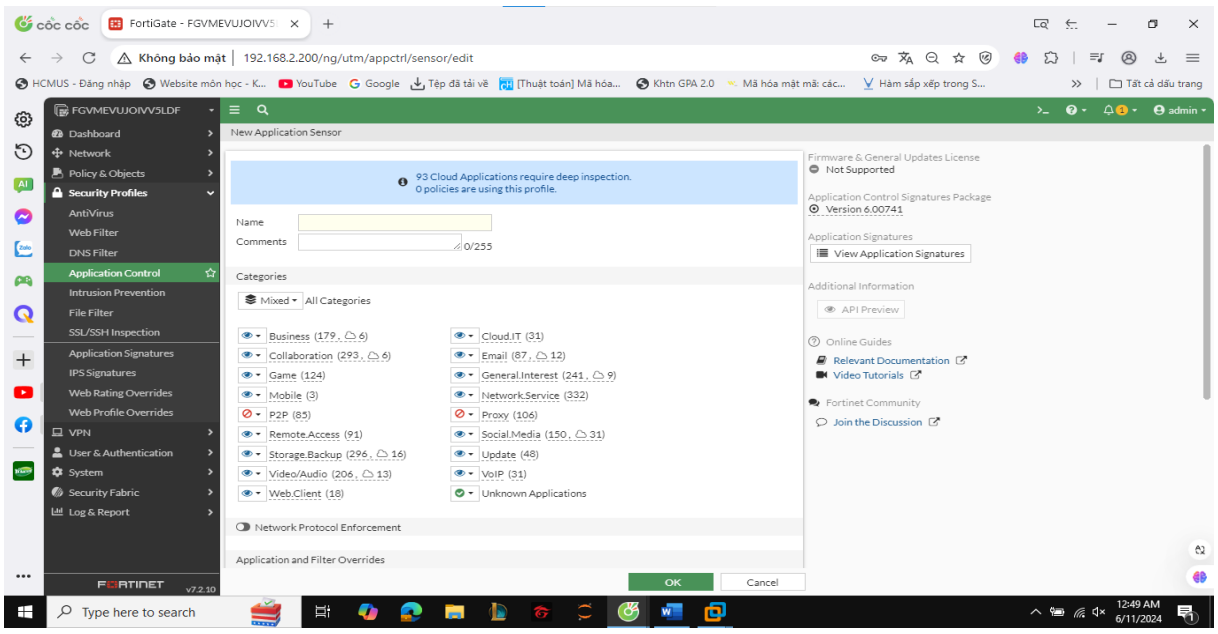
- Kiểm soát ứng dụng truy cập

B1: Tạo Application Control Profile

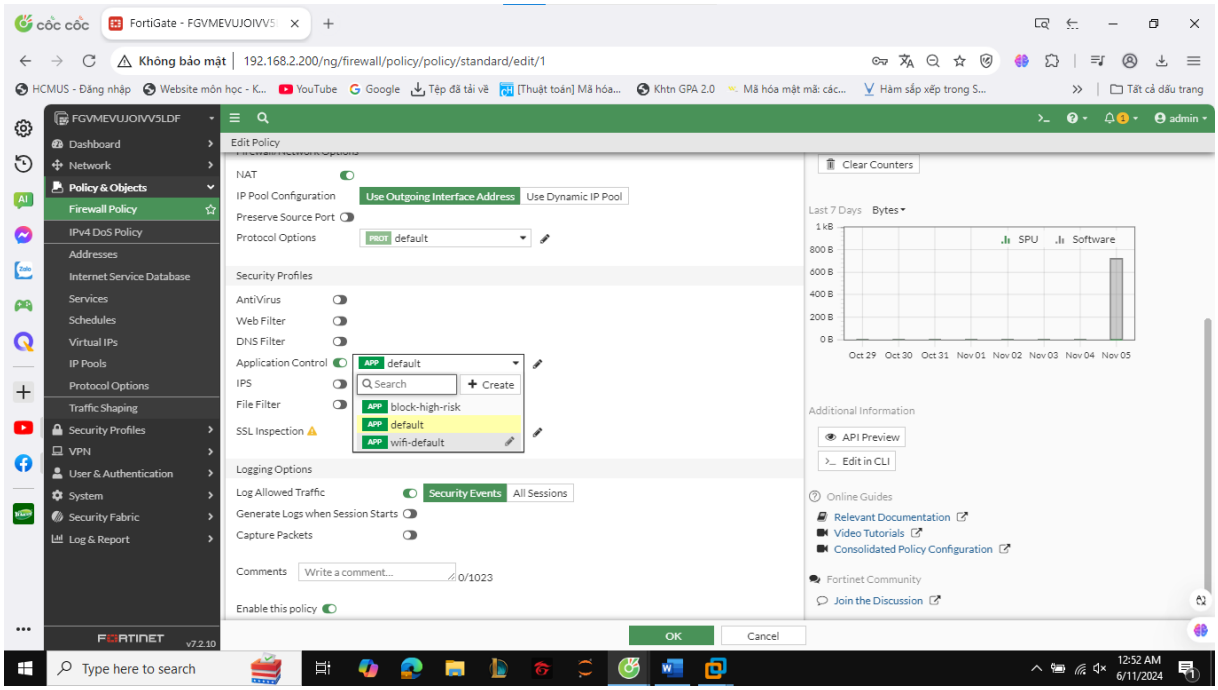
Đặt tên cho profile

Trong profile, bạn có thể chọn các ứng dụng hoặc nhóm ứng dụng để **Allow** (cho phép), **Monitor** (giám sát), hoặc **Block** (chặn).

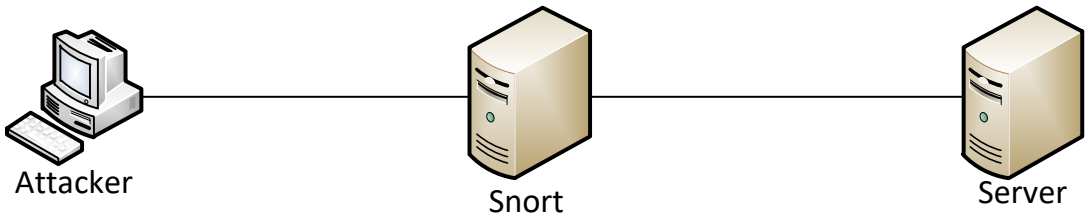
Sau đó nhấn OK



B2: Tạo policy để kiểm soát ứng dụng truy cập. Bật Application Control và chọn Application Control Profile vừa tạo. Sau đó nhấn OK

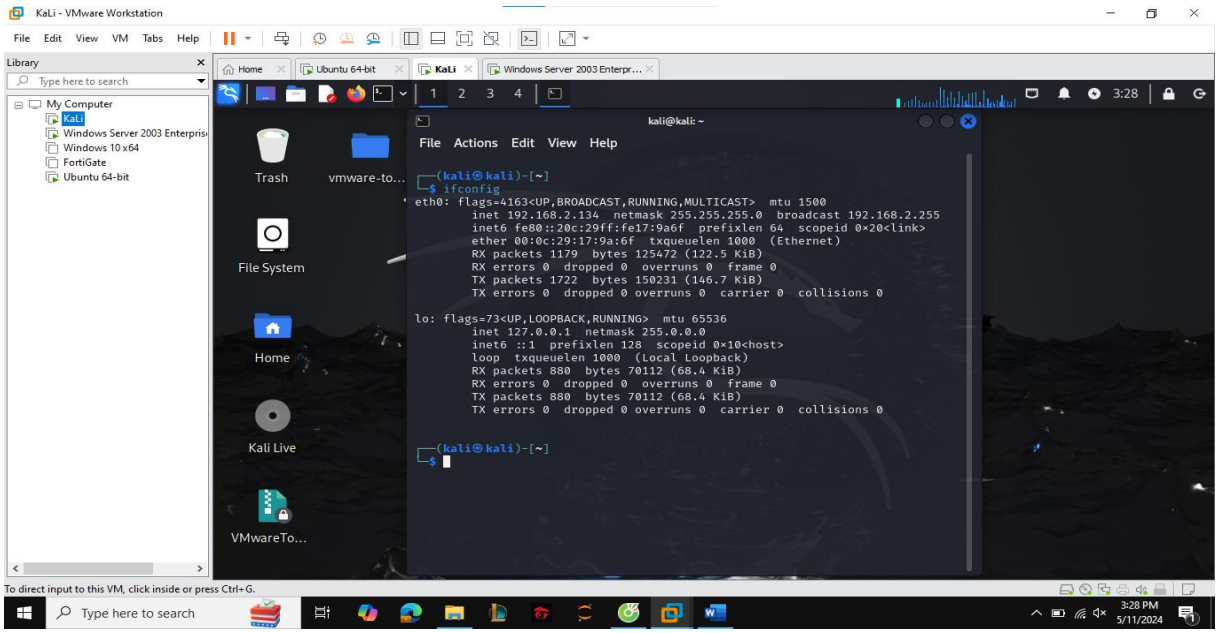


5. **Snort-IDS** (2,0 điểm)

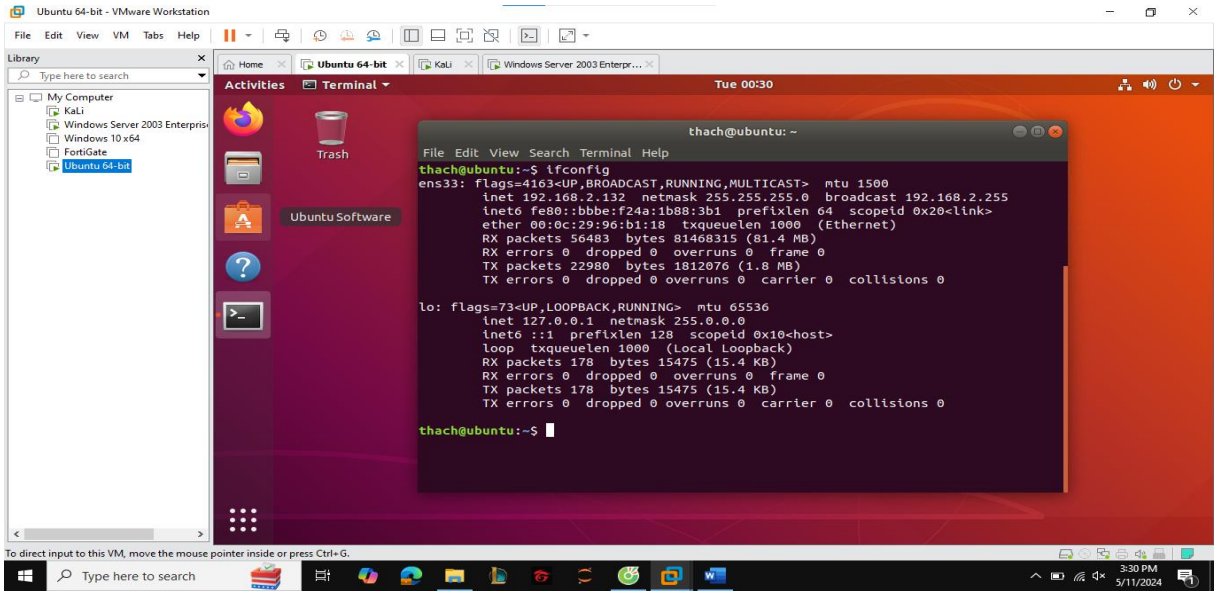


- Cài đặt Snort
- Dùng một số công cụ tấn công và mô tả kết quả xử lý trên Snort

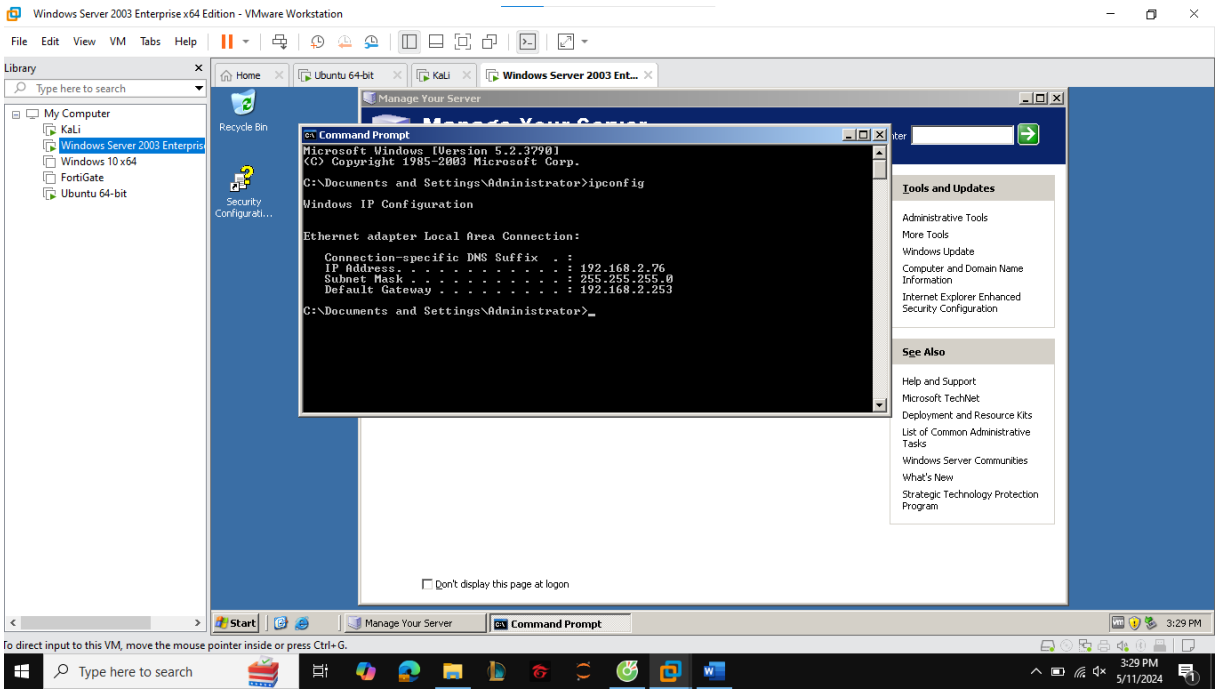
Máy Attack (Hệ điều hành Kali-linux)



Snort (Hệ điều hành Ubuntu)



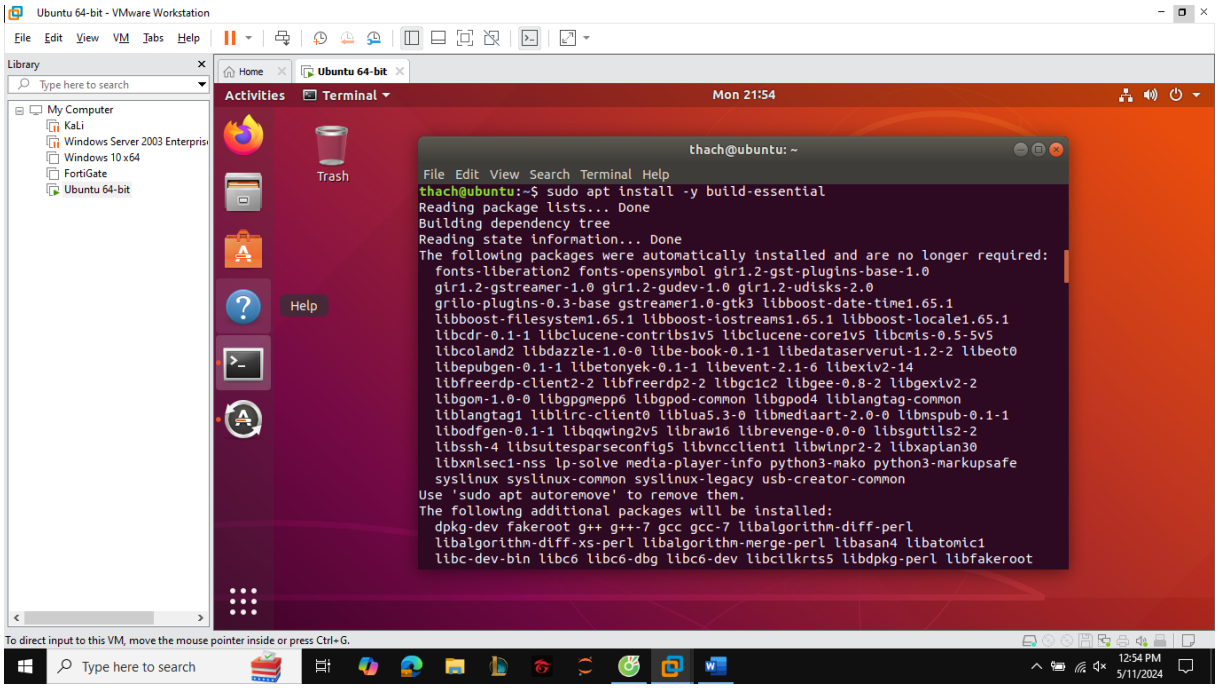
Server (Hệ điều hành Window Server 2003)



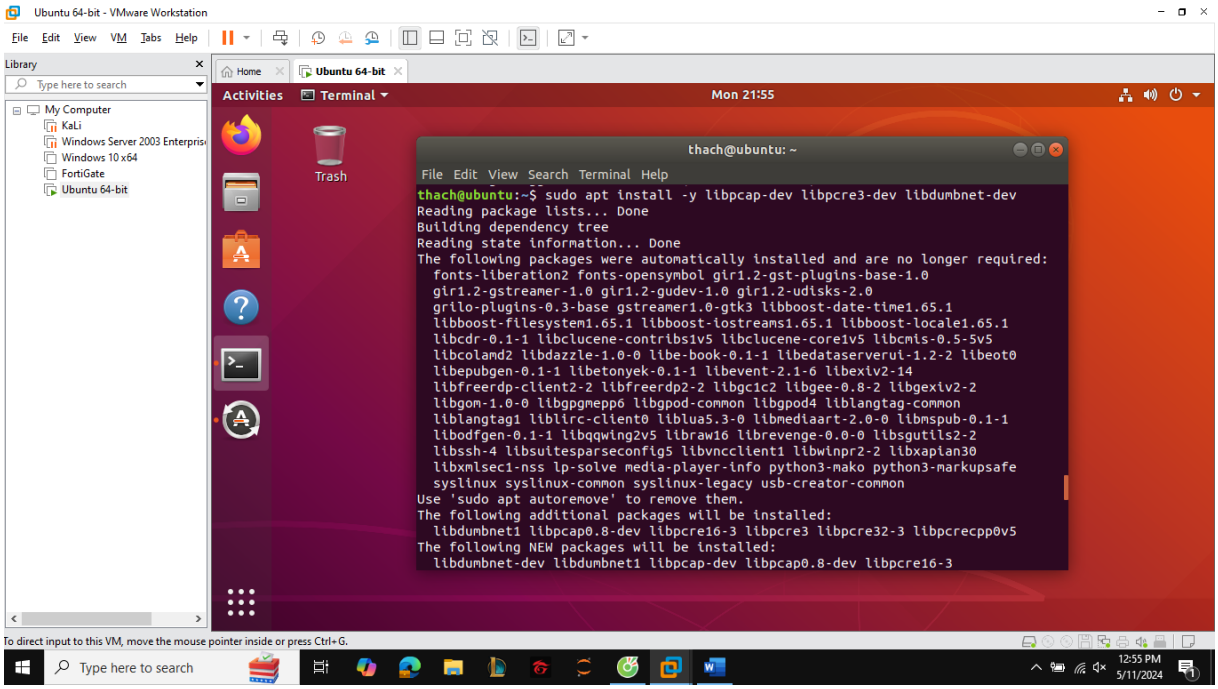
1. Cài đặt Snort:

B1:Cài đặt các gói phần mềm bổ trợ: Pcap, PCRE, libdnet, DAQ, lib

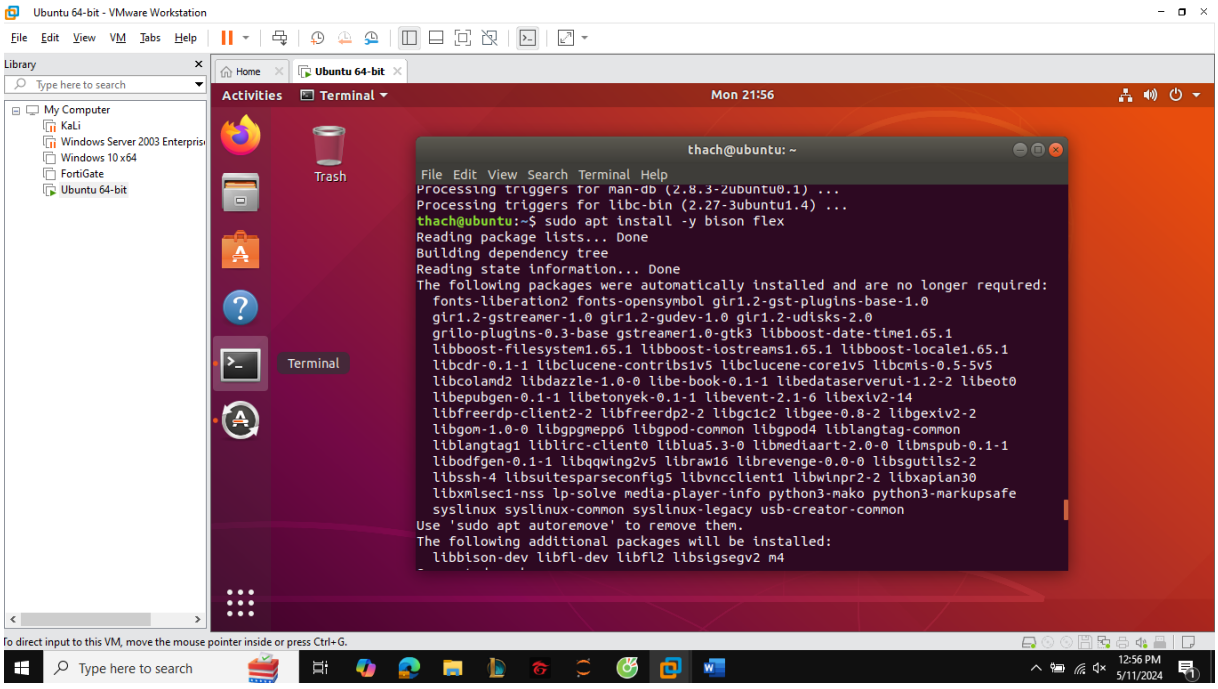
Sudo apt install -y build-essential



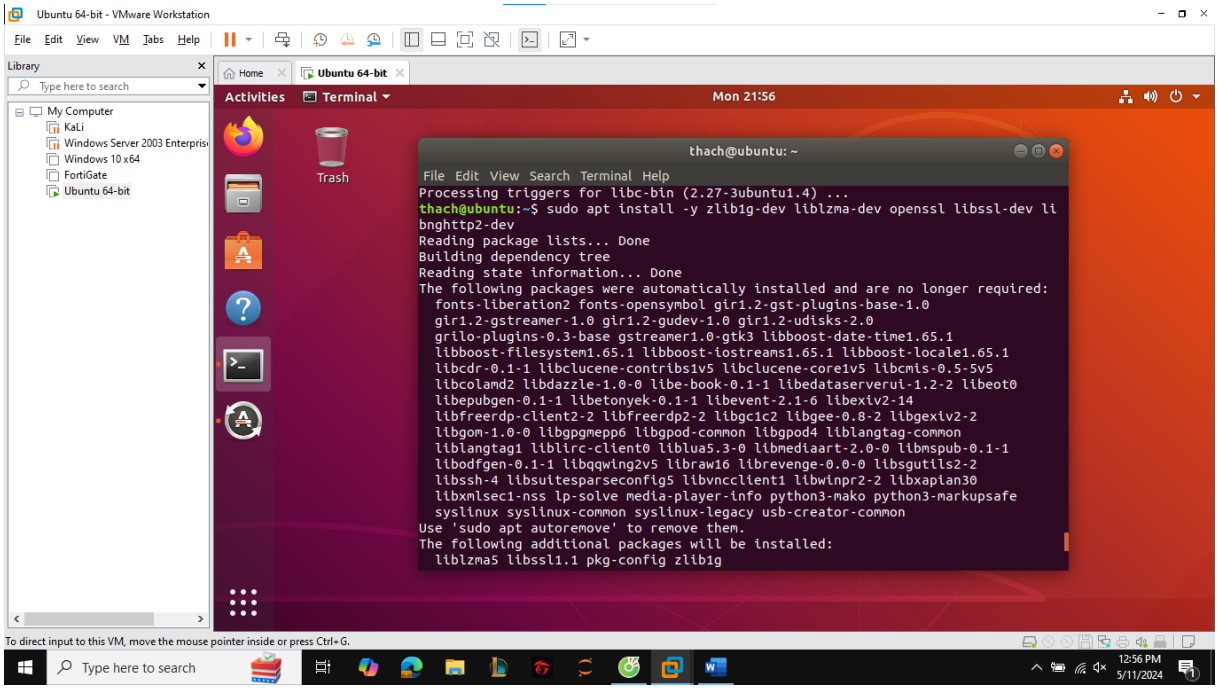
sudo apt install -y libpcap-dev libpcre3-dev libdumbnet-dev



sudo apt install -y bison flex



sudo apt install -y zlib1g-dev liblzma-dev openssl libssl-dev libnghttp2-dev



B2:Tạo thư mục chứa mã nguồn Snort và cài đặt Snort:

Tạo thư mục chứa mã nguồn Snort:

mkdir -p ~/snort_src

cd ~/snort_src

Cài đặt gói DAQ

sudo wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz

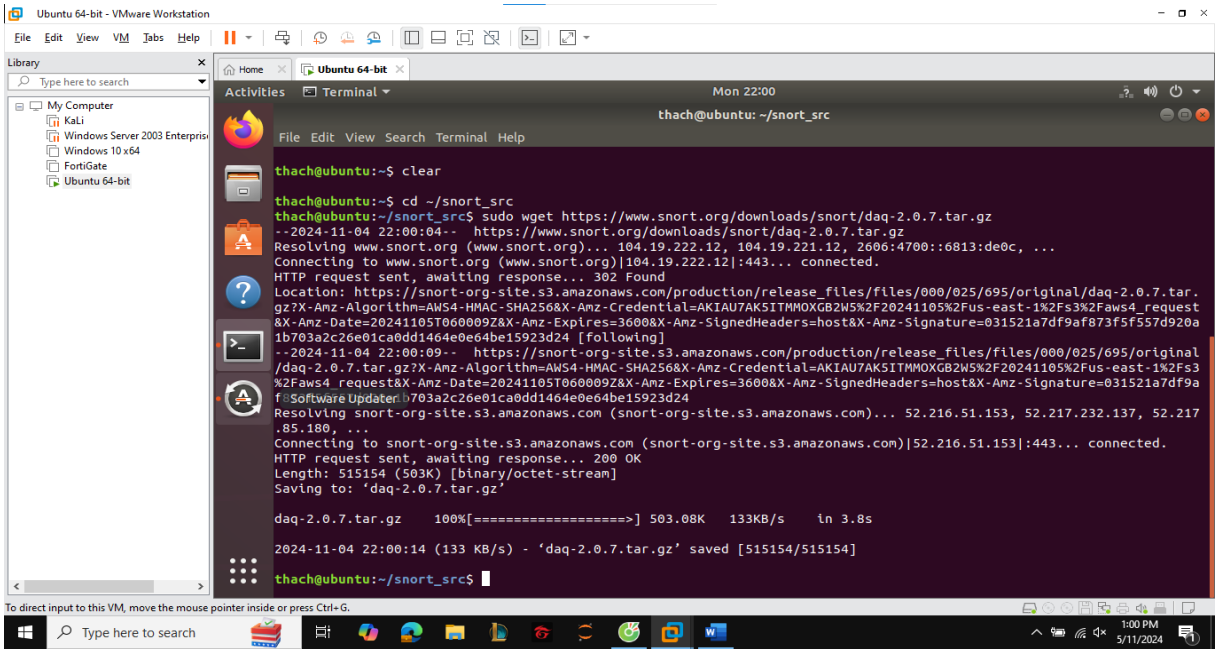
sudo tar -xvzf daq-2.0.7.tar.gz

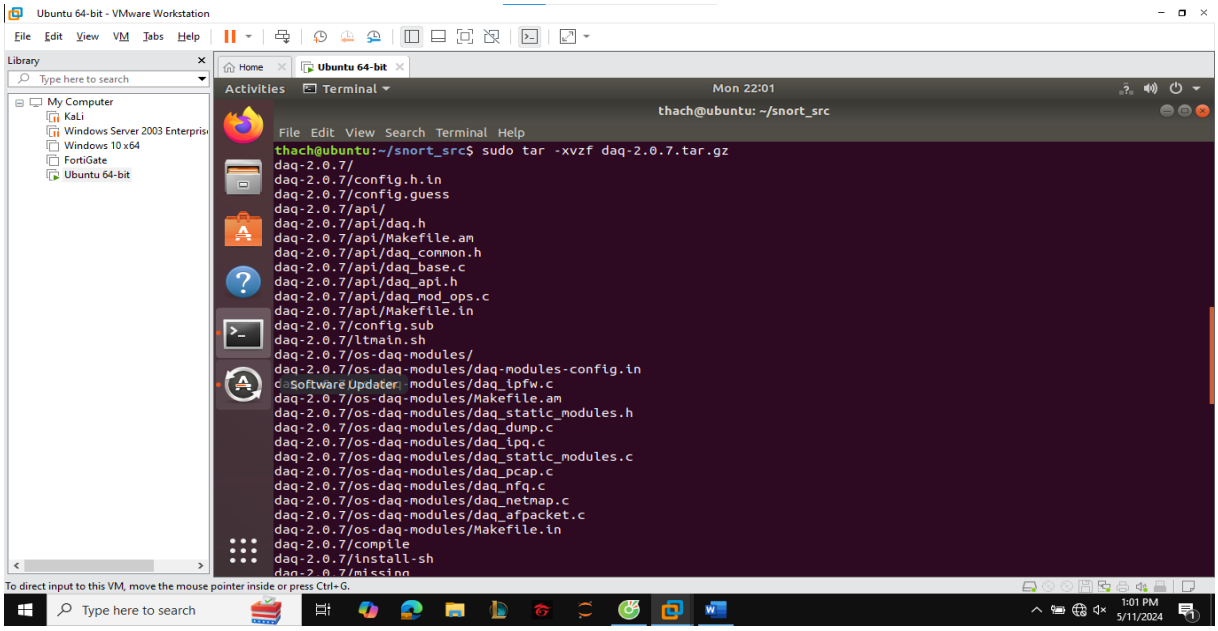
cd daq-2.0.7

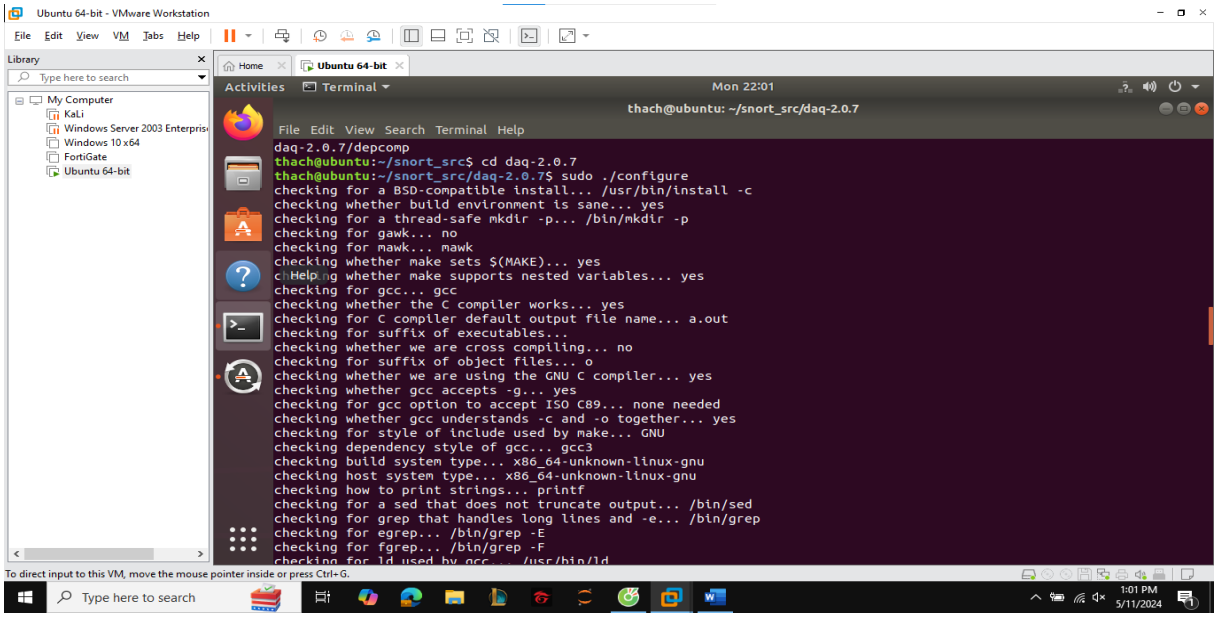
sudo ./configure

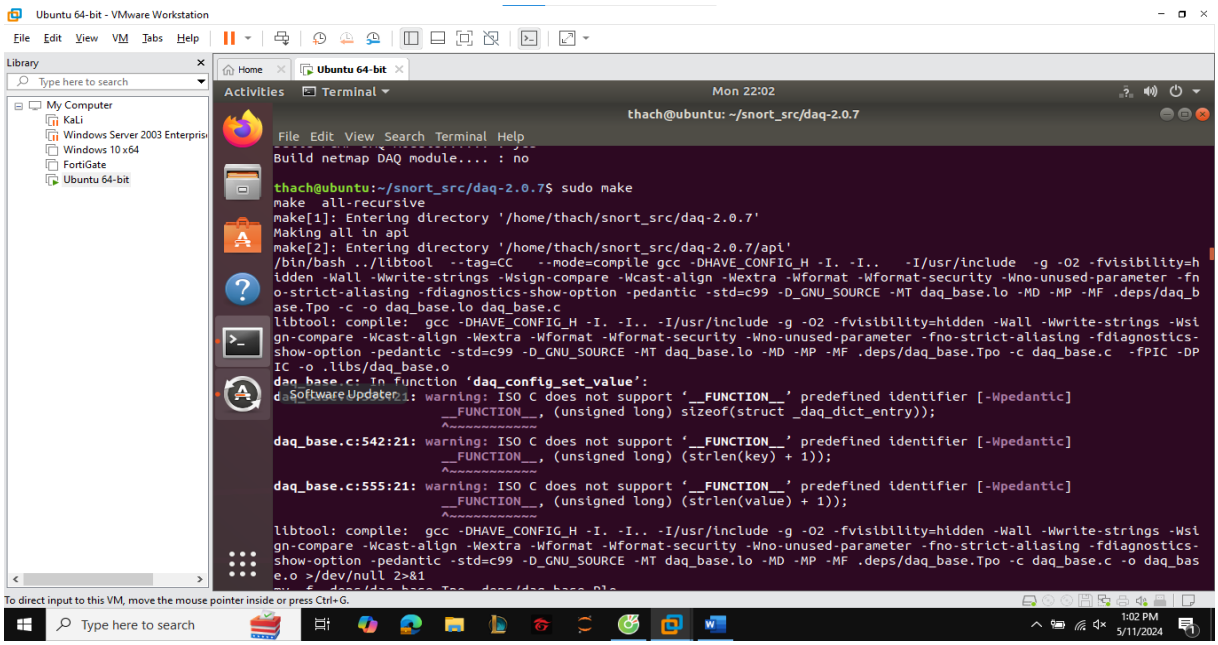
sudo make

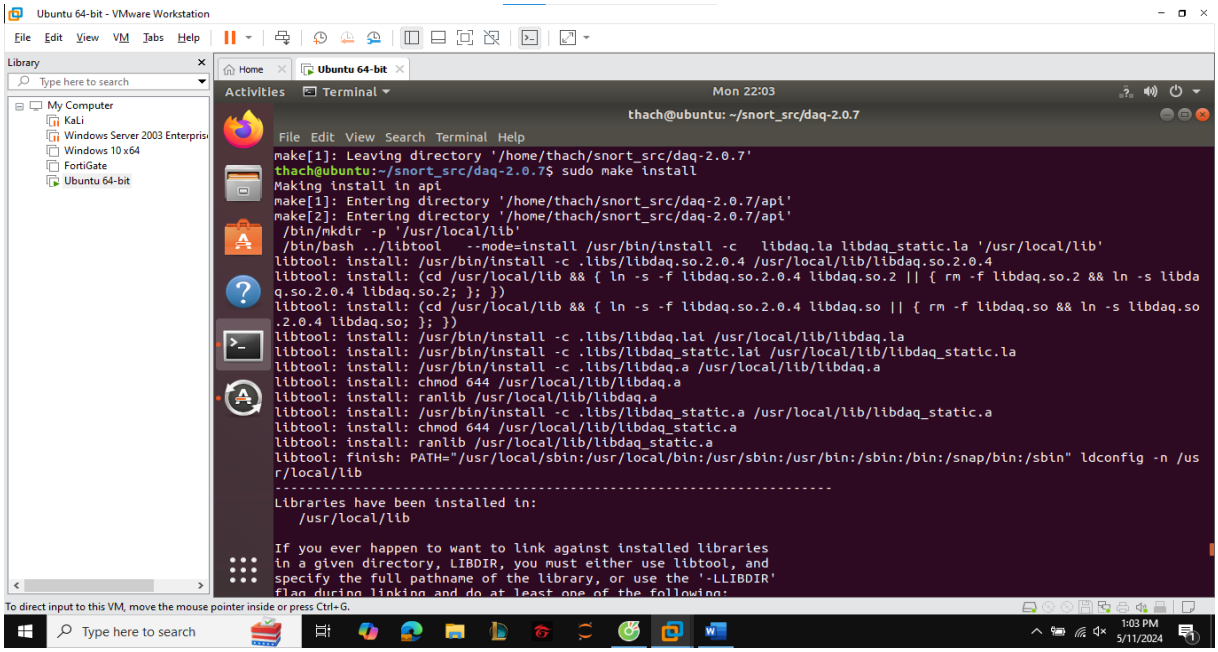
sudo make install


Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
KaLi
Windows Server 2003 Enterprise
Windows 10 x64
FortiGate
Ubuntu 64-bit
Home
Ubuntu 64-bit
Activities
Terminal
Mon 22:00
thach@ubuntu: ~/snort_src
File Edit View Search Terminal Help
thach@ubuntu:~$ clear
thach@ubuntu:~$ cd ~/snort_src
thach@ubuntu:~/snort_src$ sudo wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz
--2024-11-04 22:00:04-- https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz
Resolving www.snort.org (www.snort.org)... 104.19.222.12, 104.19.221.12, 2606:4700::6813:de0c, ...
Connecting to www.snort.org (www.snort.org)|104.19.222.12|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/025/695/original/daq-2.0.7.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AK5ITMMOXGB2W5%2F20241105%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20241105T060009Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=031521a7df9af873f5f557d920a1b703a2c26e01ca0dd1464e0e64be15923d24 [following]
--2024-11-04 22:00:09-- https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/025/695/original/daq-2.0.7.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AK5ITMMOXGB2W5%2F20241105%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20241105T060009Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=031521a7df9af873f5f557d920a1b703a2c26e01ca0dd1464e0e64be15923d24
Resolving snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)... 52.216.51.153, 52.217.232.137, 52.217.85.180, ...
Connecting to snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)|52.216.51.153|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 515154 (503K) [binary/octet-stream]
Saving to: 'daq-2.0.7.tar.gz'
daq-2.0.7.tar.gz 100%[==========>] 503.08K 133KB/s in 3.8s
2024-11-04 22:00:14 (133 KB/s) - 'daq-2.0.7.tar.gz' saved [515154/515154]
thach@ubuntu:~/snort_src$
Software Updater
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
1:00 PM
5/11/2024


Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
KaLi
Windows Server 2003 Enterprise
Windows 10 x64
FortiGate
Ubuntu 64-bit
Home
Ubuntu 64-bit
Activities
Terminal
Mon 22:01
thach@ubuntu: ~/snort_src
File Edit View Search Terminal Help
thach@ubuntu:~/snort_src$ sudo tar -xvzf daq-2.0.7.tar.gz
daq-2.0.7/
daq-2.0.7/config.h.in
daq-2.0.7/config.guess
daq-2.0.7/api/
daq-2.0.7/api/daq.h
daq-2.0.7/api/Makefile.am
daq-2.0.7/api/daq_common.h
daq-2.0.7/api/daq_base.c
daq-2.0.7/api/daq_api.h
daq-2.0.7/api/daq_mod_ops.c
daq-2.0.7/api/Makefile.in
daq-2.0.7/config.sub
daq-2.0.7/ltmain.sh
daq-2.0.7/os-daq-modules/
daq-2.0.7/os-daq-modules/daq-modules-config.in
daq-2.0.7/os-daq-modules/daq_ipfw.c
daq-2.0.7/os-daq-modules/Makefile.am
daq-2.0.7/os-daq-modules/daq_static_modules.h
daq-2.0.7/os-daq-modules/daq_dump.c
daq-2.0.7/os-daq-modules/daq_ipq.c
daq-2.0.7/os-daq-modules/daq_static_modules.c
daq-2.0.7/os-daq-modules/daq_pcap.c
daq-2.0.7/os-daq-modules/daq_nfq.c
daq-2.0.7/os-daq-modules/daq_netmap.c
daq-2.0.7/os-daq-modules/daq_afpacket.c
daq-2.0.7/os-daq-modules/Makefile.in
daq-2.0.7/compile
daq-2.0.7/install-sh
daq-2.0.7/missing
Software Updater
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
1:01 PM
5/11/2024


Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
KaLi
Windows Server 2003 Enterpris
Windows 10 x64
FortiGate
Ubuntu 64-bit
Home
Ubuntu 64-bit
Activities
Terminal
Mon 22:01
thach@ubuntu: ~/snort_src/daq-2.0.7
File Edit View Search Terminal Help
daq-2.0.7/depcomp
thach@ubuntu:~/snort_src$ cd daq-2.0.7
thach@ubuntu:~/snort_src/daq-2.0.7$ sudo ./configure
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
checking for style of include used by make... GNU
checking dependency style of gcc... gcc3
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking how to print strings... printf
checking for a sed that does not truncate output... /bin/sed
checking for grep that handles long lines and -e... /bin/grep
checking for egrep... /bin/grep -E
checking for fgrep... /bin/grep -F
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
1:01 PM
5/11/2024


Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
KaLi
Windows Server 2003 Enterpris
Windows 10 x64
FortiGate
Ubuntu 64-bit
Home
Ubuntu 64-bit
Activities
Terminal
Mon 22:02
thach@ubuntu: ~/snort_src/daq-2.0.7
File Edit View Search Terminal Help
Build netmap DAQ module.... : no
thach@ubuntu:~/snort_src/daq-2.0.7$ sudo make
make all-recursive
make[1]: Entering directory '/home/thach/snort_src/daq-2.0.7'
Making all in api
make[2]: Entering directory '/home/thach/snort_src/daq-2.0.7/api'
/bin/bash ../libtool --tag=CC --mode=compile gcc -DHAVE_CONFIG_H -I. -I.. -I/usr/include -g -O2 -fvisibility=hidden -Wall -Wwrite-strings -Wsign-compare -Wcast-align -Wextra -Wformat -Wformat-security -Wno-unused-parameter -fno-strict-aliasing -fdiagnostics-show-option -pedantic -std=c99 -D_GNU_SOURCE -MT daq_base.lo -MD -MP -MF .deps/daq_base.Tpo -c -o daq_base.lo daq_base.c
libtool: compile: gcc -DHAVE_CONFIG_H -I. -I.. -I/usr/include -g -O2 -fvisibility=hidden -Wall -Wwrite-strings -Wsign-compare -Wcast-align -Wextra -Wformat -Wformat-security -Wno-unused-parameter -fno-strict-aliasing -fdiagnostics-show-option -pedantic -std=c99 -D_GNU_SOURCE -MT daq_base.lo -MD -MP -MF .deps/daq_base.Tpo -c daq_base.c -fPIC -DPIC -o .libs/daq_base.o
daq_base.c: In function 'daq_config_set_value':
daq_base.c:521:21: warning: ISO C does not support '__FUNCTION__' predefined identifier [-Wpedantic]
__FUNCTION__, (unsigned long) sizeof(struct _daq_dict_entry));
daq_base.c:542:21: warning: ISO C does not support '__FUNCTION__' predefined identifier [-Wpedantic]
__FUNCTION__, (unsigned long) (strlen(key) + 1));
daq_base.c:555:21: warning: ISO C does not support '__FUNCTION__' predefined identifier [-Wpedantic]
__FUNCTION__, (unsigned long) (strlen(value) + 1));
libtool: compile: gcc -DHAVE_CONFIG_H -I. -I.. -I/usr/include -g -O2 -fvisibility=hidden -Wall -Wwrite-strings -Wsign-compare -Wcast-align -Wextra -Wformat -Wformat-security -Wno-unused-parameter -fno-strict-aliasing -fdiagnostics-show-option -pedantic -std=c99 -D_GNU_SOURCE -MT daq_base.lo -MD -MP -MF .deps/daq_base.Tpo -c daq_base.c -o daq_base.o >/dev/null 2>&1
Software Updater
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
1:02 PM
5/11/2024



Cài đặt Snort:

sudo wget https://www.snort.org/downloads/snort/snort-2.9.20.tar.gz

sudo tar -zxf snort-2.9.20.tar.gz

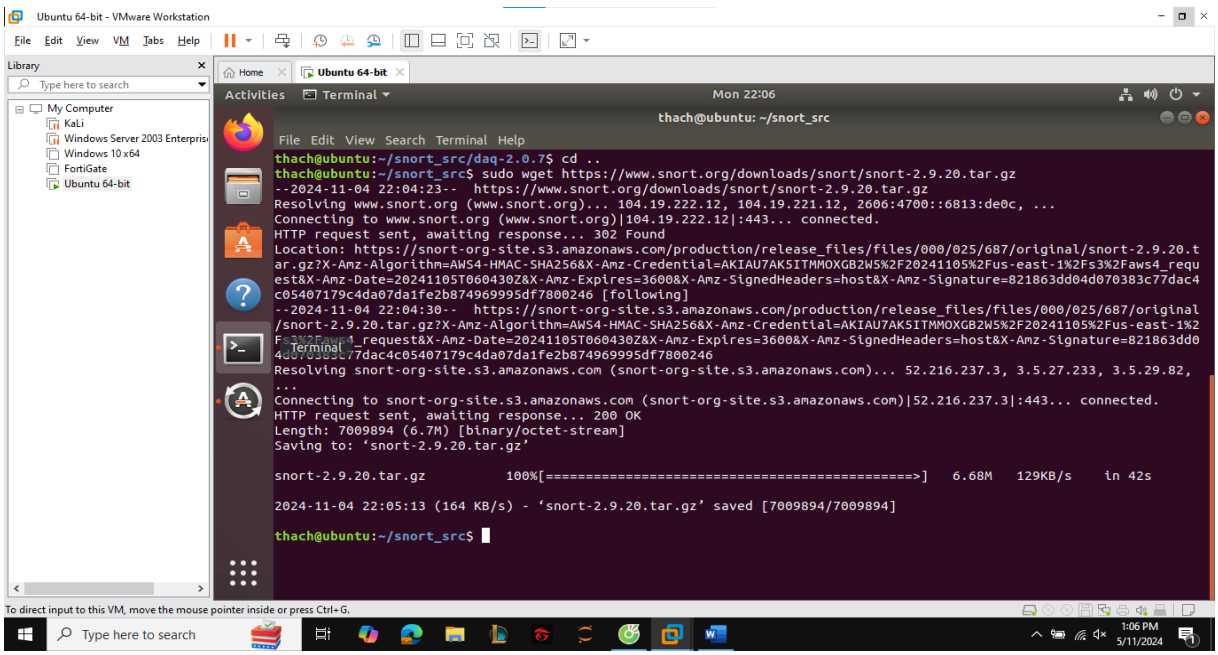
cd snort-2.9.20

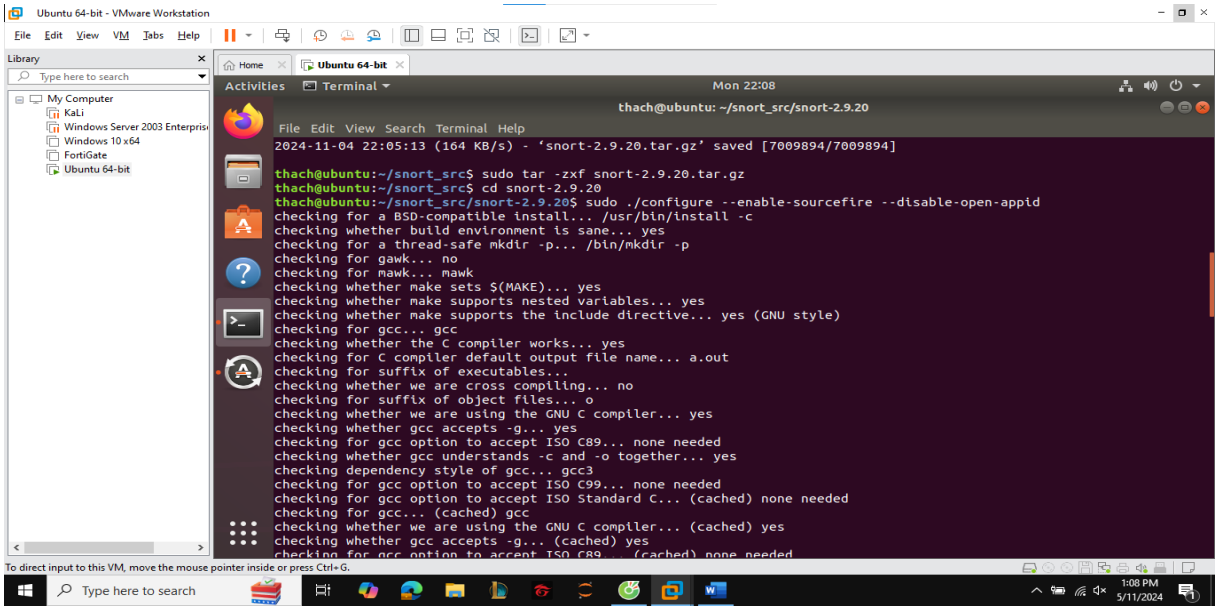
sudo ./configure --enable-sourcefire --disable-open-appid

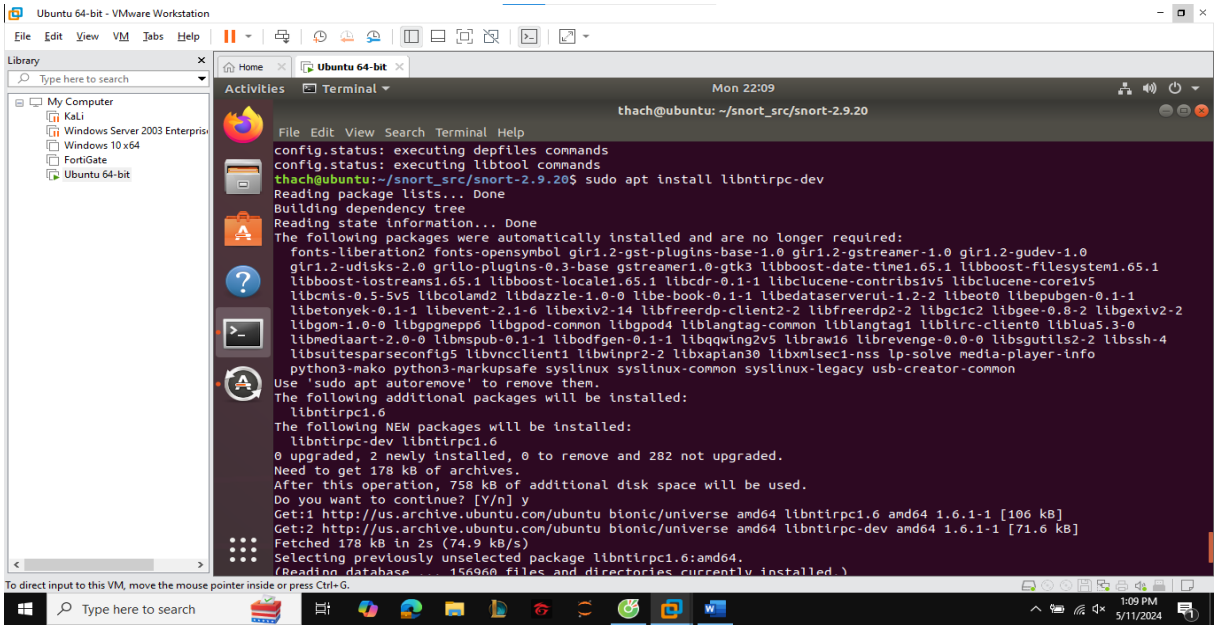
sudo apt install libntirpc-dev

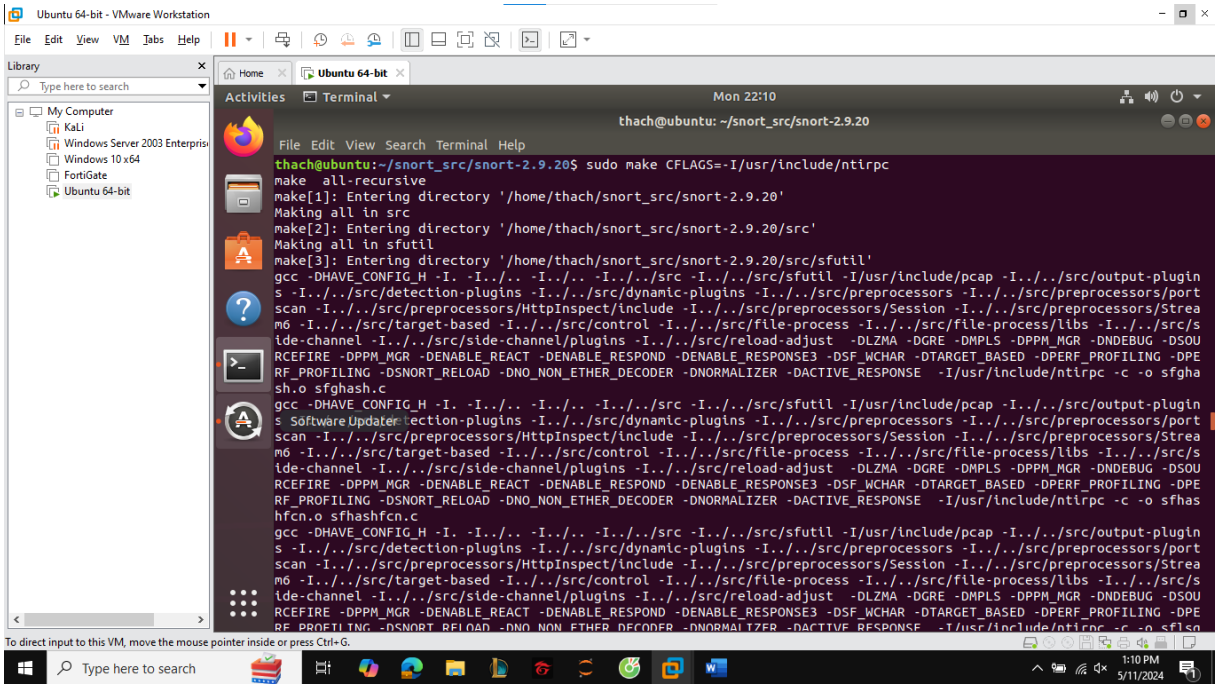
sudo make CFLAGS=-I/usr/include/ntirpc

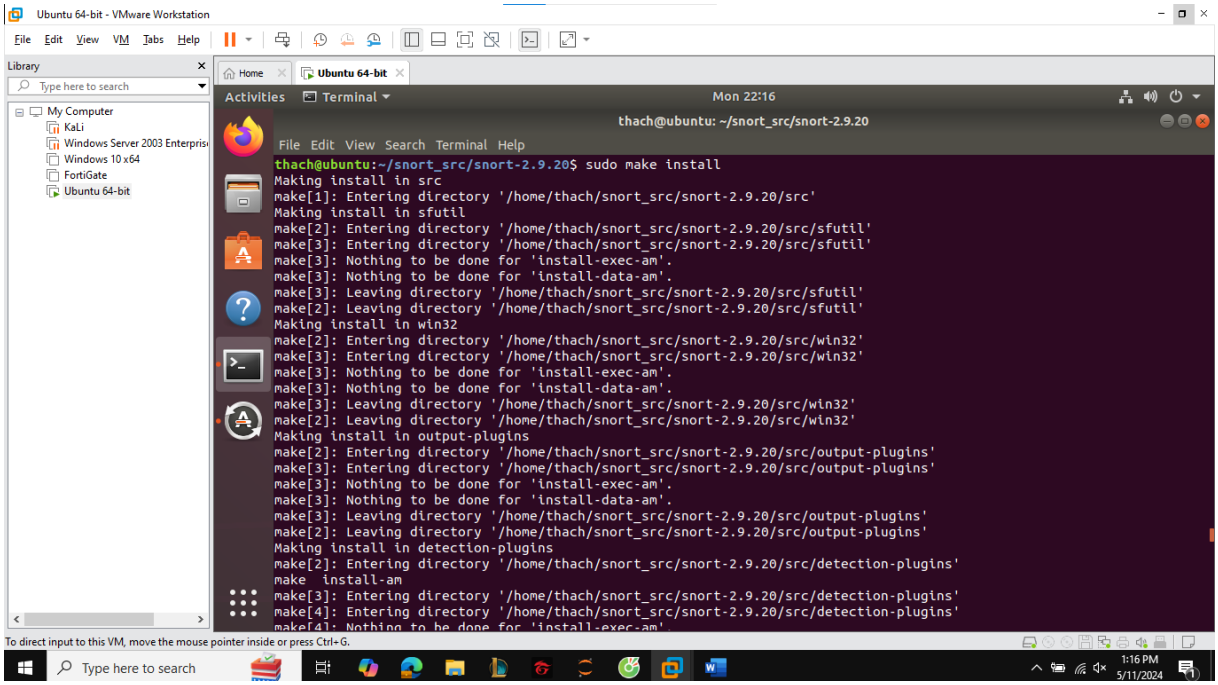
sudo make install




Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
KaLi
Windows Server 2003 Enterprise
Windows 10 x64
FortiGate
Ubuntu 64-bit
Home
Ubuntu 64-bit
Activities
Terminal
Mon 22:08
thach@ubuntu: ~/snort_src/snort-2.9.20
File Edit View Search Terminal Help
2024-11-04 22:05:13 (164 KB/s) - 'snort-2.9.20.tar.gz' saved [7009894/7009894]
thach@ubuntu:~/snort_src$ sudo tar -zxf snort-2.9.20.tar.gz
thach@ubuntu:~/snort_src$ cd snort-2.9.20
thach@ubuntu:~/snort_src/snort-2.9.20$ sudo ./configure --enable-sourcefire --disable-open-appid
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking whether make supports the include directive... yes (GNU style)
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
checking dependency style of gcc... gcc3
checking for gcc option to accept ISO C99... none needed
checking for gcc option to accept ISO Standard C... (cached) none needed
checking for gcc... (cached) gcc
checking whether we are using the GNU C compiler... (cached) yes
checking whether gcc accepts -g... (cached) yes
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
1:08 PM
5/11/2024


Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
KaLi
Windows Server 2003 Enterprise
Windows 10 x64
FortiGate
Ubuntu 64-bit
Home
Ubuntu 64-bit
Activities
Terminal
Mon 22:09
thach@ubuntu: ~/snort_src/snort-2.9.20
File Edit View Search Terminal Help
config.status: executing depfiles commands
config.status: executing libtool commands
thach@ubuntu:~/snort_src/snort-2.9.20$ sudo apt install libntirpc-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
fonts-liberation2 fonts-opensymbol gir1.2-gst-plugins-base-1.0 gir1.2-gstreamer-1.0 gir1.2-gudev-1.0
gir1.2-udisks-2.0 grilo-plugins-0.3-base gstreamer1.0-gtk3 libboost-date-time1.65.1 libboost-filesystem1.65.1
libboost-iostreams1.65.1 libboost-locale1.65.1 libcdr-0.1-1 libclucene-contribs1v5 libclucene-core1v5
libcmis-0.5-5v5 libcolamd2 libdazzle-1.0-0 libe-book-0.1-1 libedataserverui-1.2-2 libeot0 libepubgen-0.1-1
libetonyek-0.1-1 libevent-2.1-6 libexiv2-14 libfreerdp-client2-2 libfreerdp2-2 libgc1c2 libgee-0.8-2 libgexiv2-2
libgom-1.0-0 libgpgmepp6 libgpod-common libgpod4 liblangtag-common liblangtag1 liblirc-client0 liblua5.3-0
libmediaart-2.0-0 libmspub-0.1-1 libodfgen-0.1-1 libqqwing2v5 libraw16 librevenge-0.0-0 libsgutils2-2 libssh-4
libsuitesparseconfig5 libvncclient1 libwinpr2-2 libxapian30 libxmlsec1-nss lp-solve media-player-info
python3-mako python3-markupsafe syslinux syslinux-common syslinux-legacy usb-creator-common
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
libntirpc1.6
The following NEW packages will be installed:
libntirpc-dev libntirpc1.6
0 upgraded, 2 newly installed, 0 to remove and 282 not upgraded.
Need to get 178 kB of archives.
After this operation, 758 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 libntirpc1.6 amd64 1.6.1-1 [106 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 libntirpc-dev amd64 1.6.1-1 [71.6 kB]
Fetched 178 kB in 2s (74.9 kB/s)
Selecting previously unselected package libntirpc1.6:amd64.
(Reading database ... 156960 files and directories currently installed.)
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
1:09 PM
5/11/2024



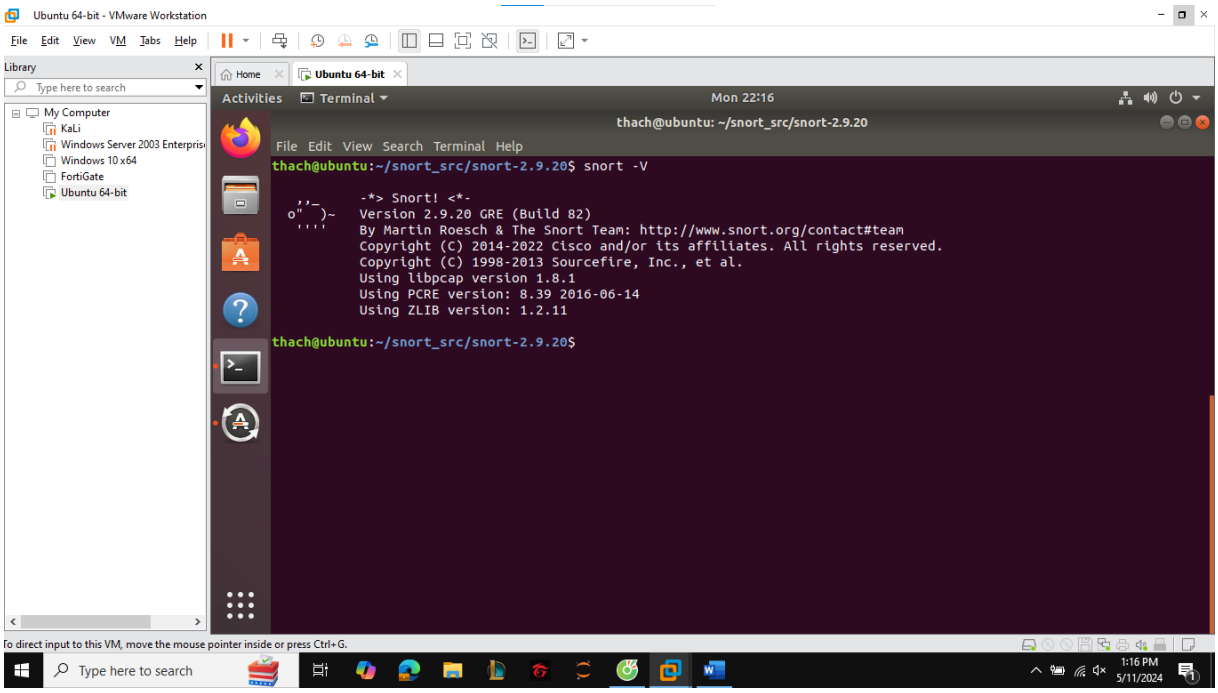


Cập nhật thư viện

sudo ldconfig

sudo ln /usr/local/bin/snort /usr/sbin/snort

Kết quả sau khi cài đặt Snort:



B3:Cấu hình Snort:

a) **Tạo các thư mục Snort và các thư mục chứa các bộ rule**

sudo mkdir /etc/snort

sudo mkdir /etc/snort/rules

sudo mkdir /etc/snort/rules/iplists

sudo mkdir /etc/snort/preproc_rules

sudo mkdir /usr/local/lib/snort_dynamicrules

sudo mkdir /etc/snort/so_rules

b) **Tạo file để lưu trữ rule và danh sách IP**

sudo touch /etc/snort/rules/iplists/black_list.rules

sudo touch /etc/snort/rules/iplists/white_list.rules

sudo touch /etc/snort/rules/local.rules

sudo touch /etc/snort/sid-msg.map

c) **Tạo thư mục lưu trữ log**

sudo mkdir /var/log/snort

sudo mkdir /var/log/snort/archived_logs

d) **Sử dụng cấu hình có sẵn coppy vào thư mục /etc/snort**

cd snort_src/snort-2.9.20/etc

sudo cp *.conf* /etc/snort

sudo cp *.map /etc/snort

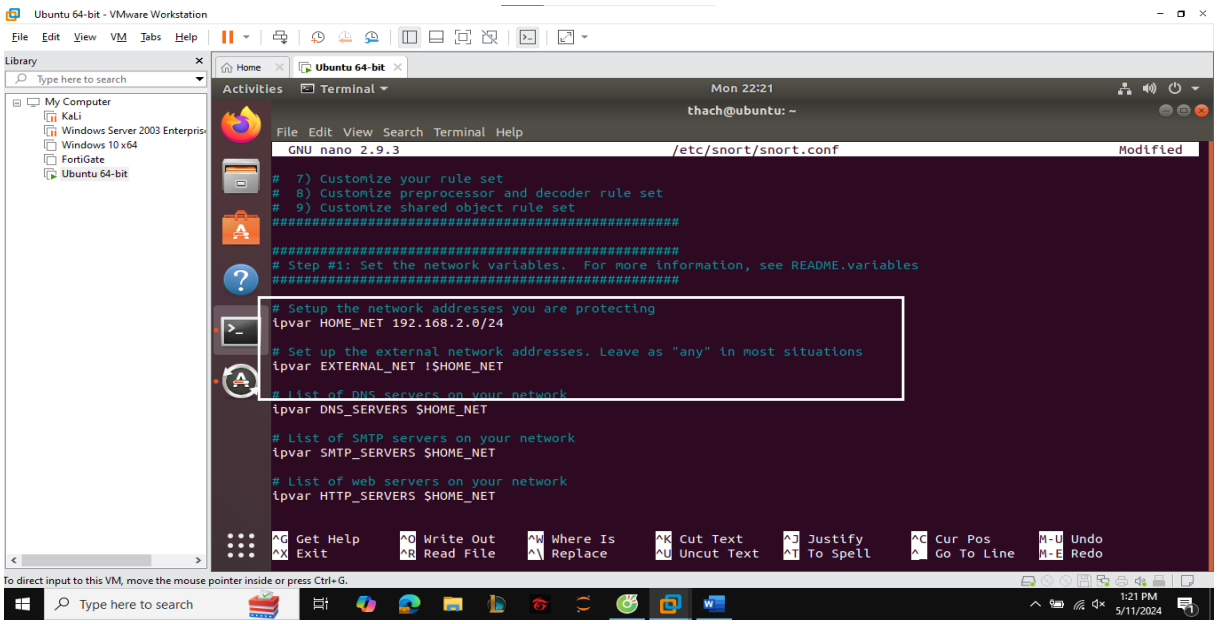
sudo cp *.dtd /etc/snort

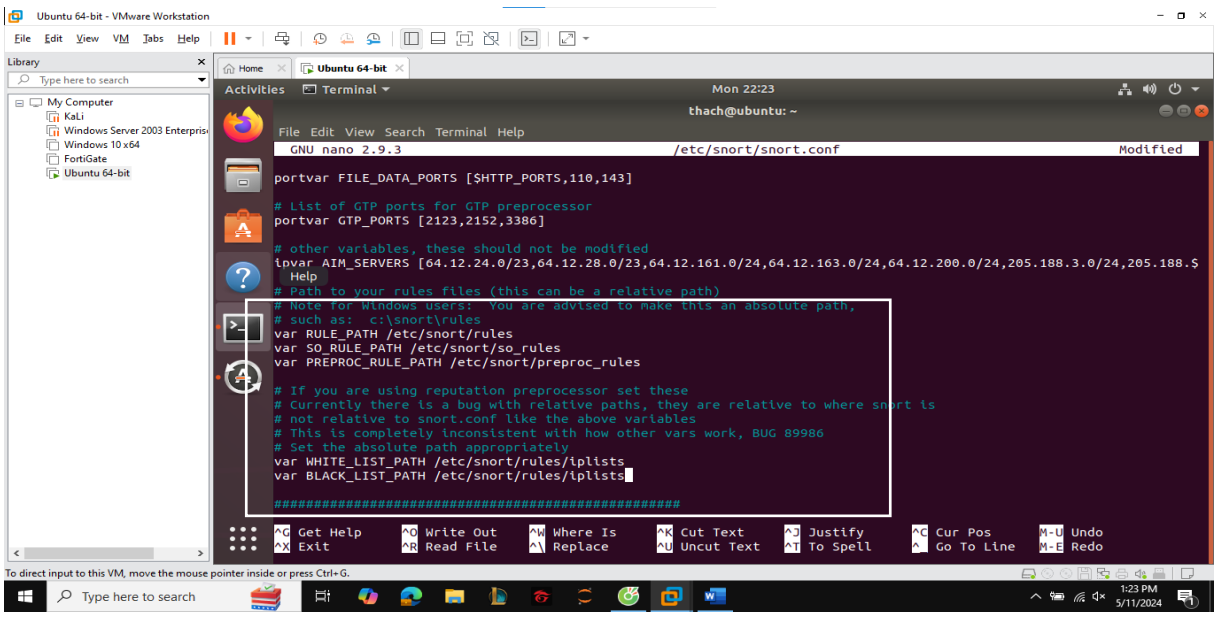
cd snort_src/snort-2.9.20/src/dynamic- preprocessors/build/usr/local/lib/snort_dynamicpreprocessor/

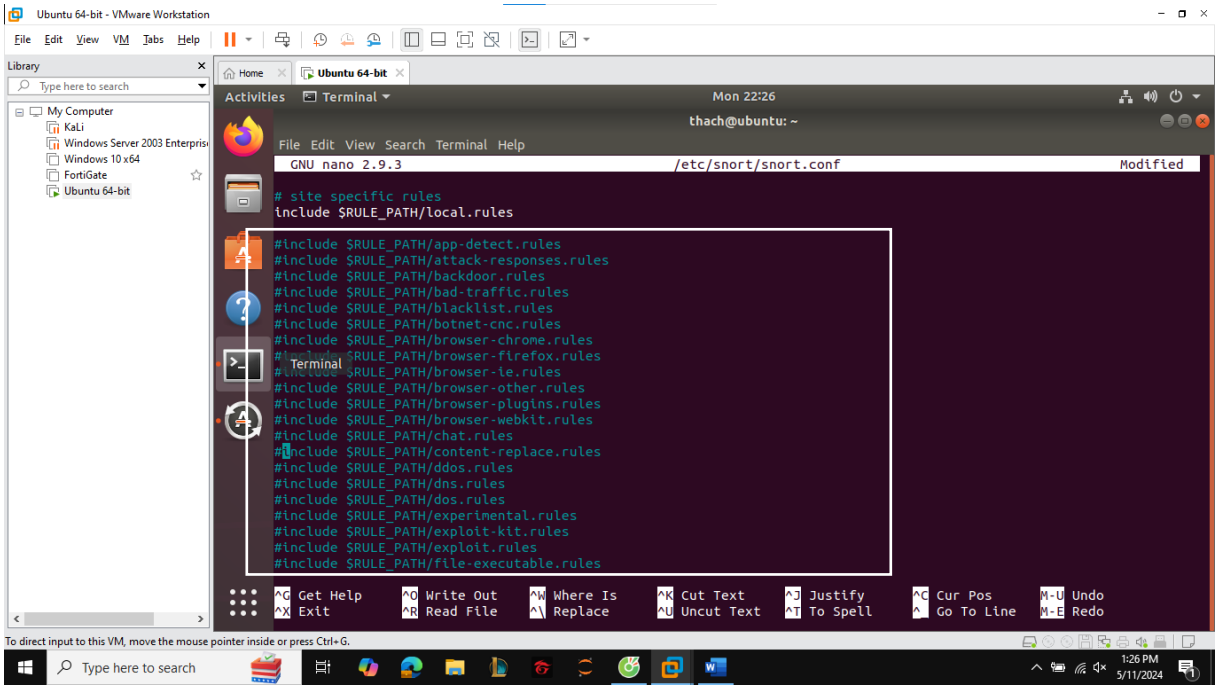
sudo cp * /usr/local/lib/snort_dynamicpreprocessor/

e) **Chỉnh sửa các cấu hình cơ bản trong snort.conf**

sudo nano /etc/snort/snort.conf

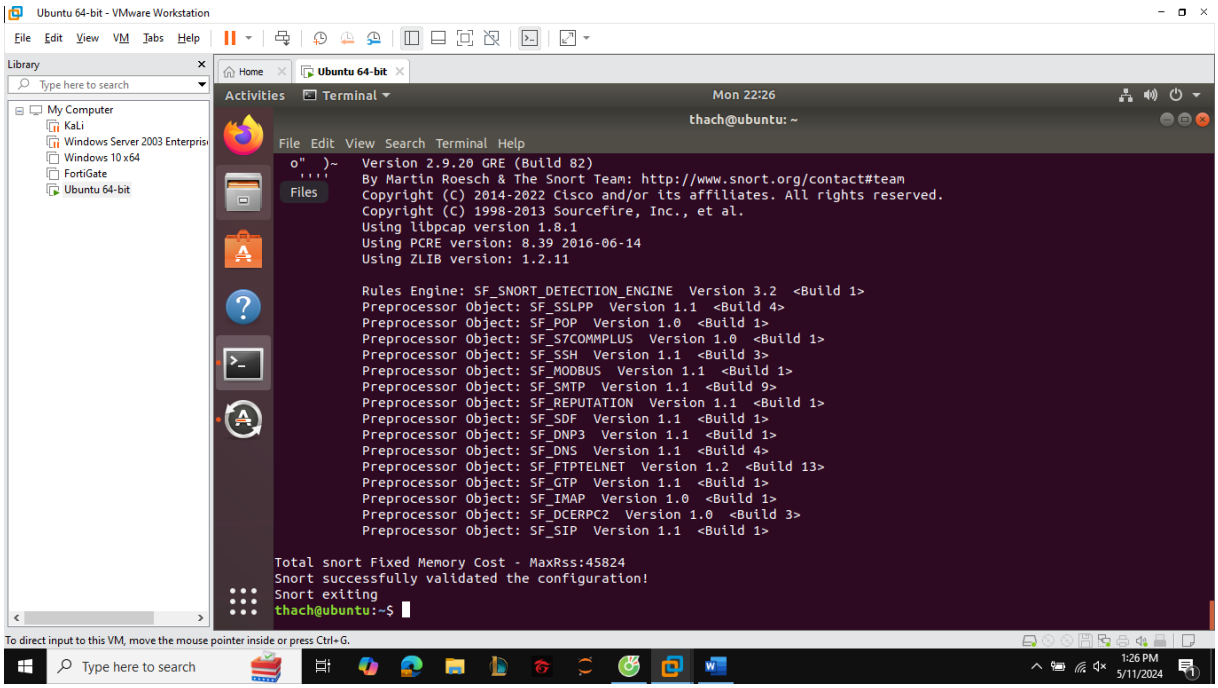






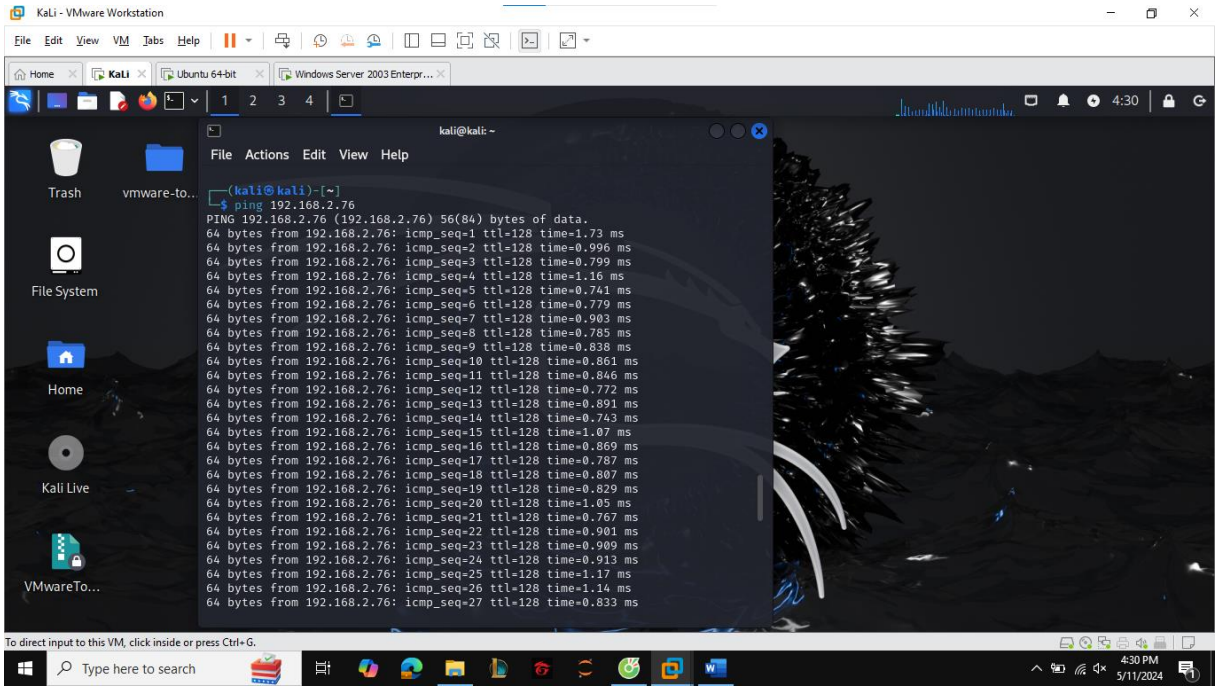
B4:Kiểm tra sự hoạt động của Snort:

sudo snort -i ens33 -c /etc/snort/snort.conf -T

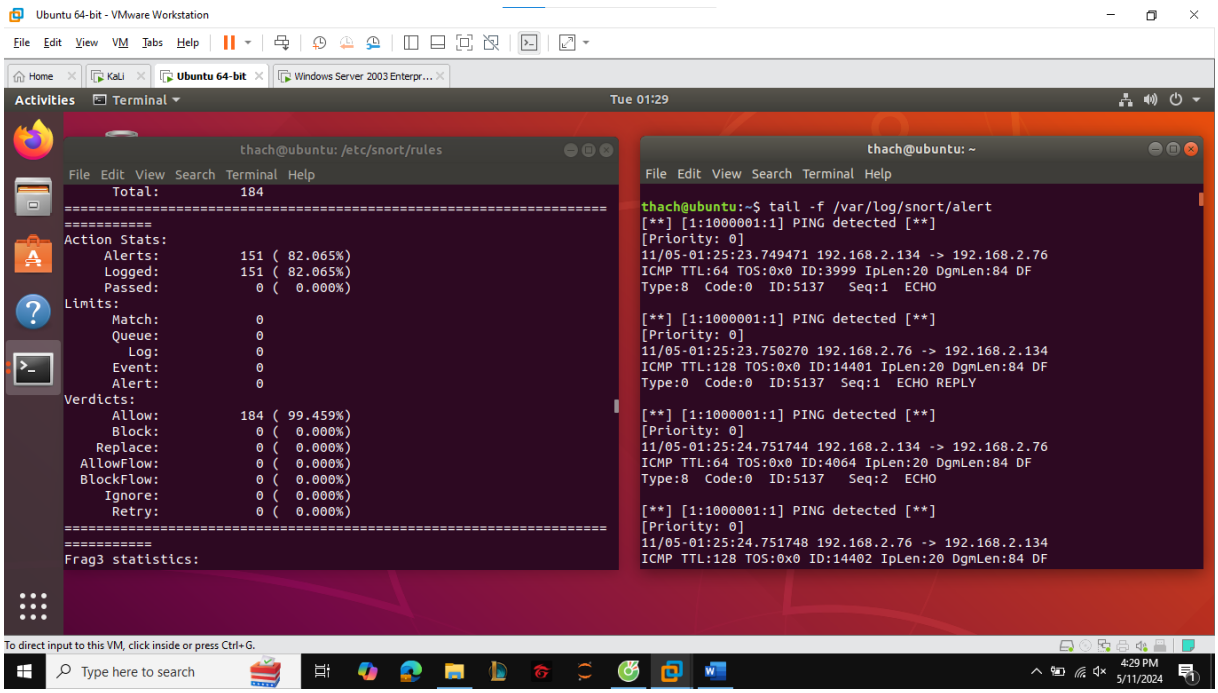


2. **Dùng một số công cụ tấn công và mô tả kết quả xử lý trên Snort :**

Tấn công dò quét (Ping)



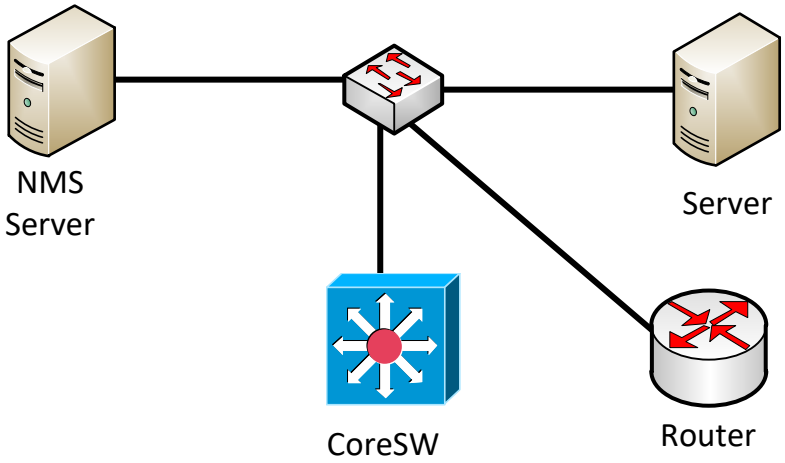
Kết quả xử lý trên snort:



- **Terminal bên trái** hiển thị số liệu thống kê của Snort, cho biết trong số 184 gói tin, có 151 cảnh báo được kích hoạt liên quan đến phát hiện ping ICMP.
- **Terminal bên phải** đang hiển thị cảnh báo ping thời gian thực, trong đó Snort phát hiện các yêu cầu phản hồi ICMP lặp lại và ghi lại từng yêu cầu.

6. **Network Monitoring System** (1,0 điểm)

- Thực hiện giám sát mạng với phần mềm PRTG
- Cấu hình chức năng giám sát performance (RAM, CPU), giám sát một số dịch vụ mạng (DHCP, Web,…), giám sát dung lượng đĩa trên Server
- Thiết lập ngưỡng cảnh báo



Các bước thực hiện:

- Thực hiện giám sát mạng với phần mềm PRTG