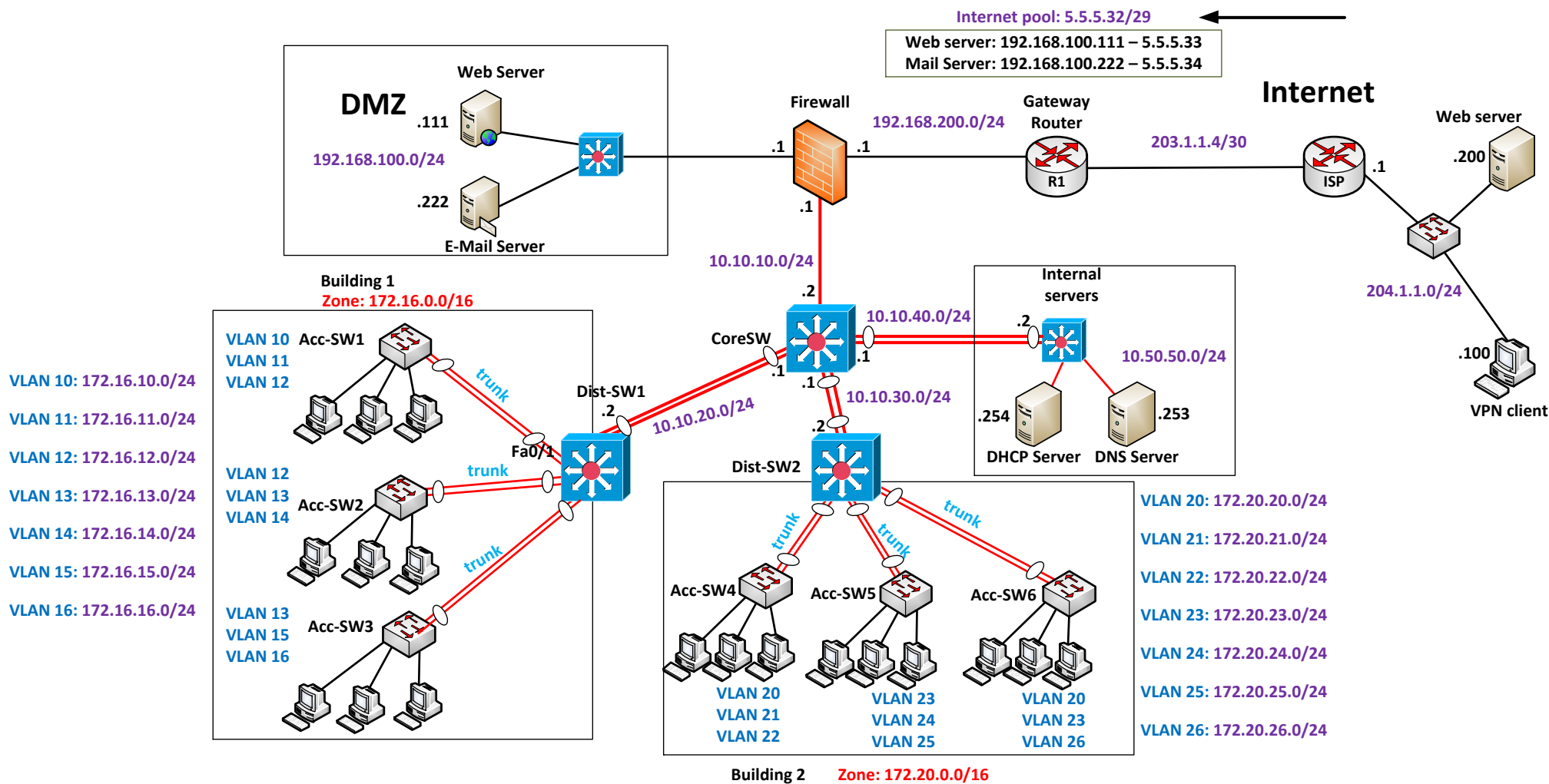


LAB01. THIẾT LẬP & CẤU HÌNH MẠNG LAN

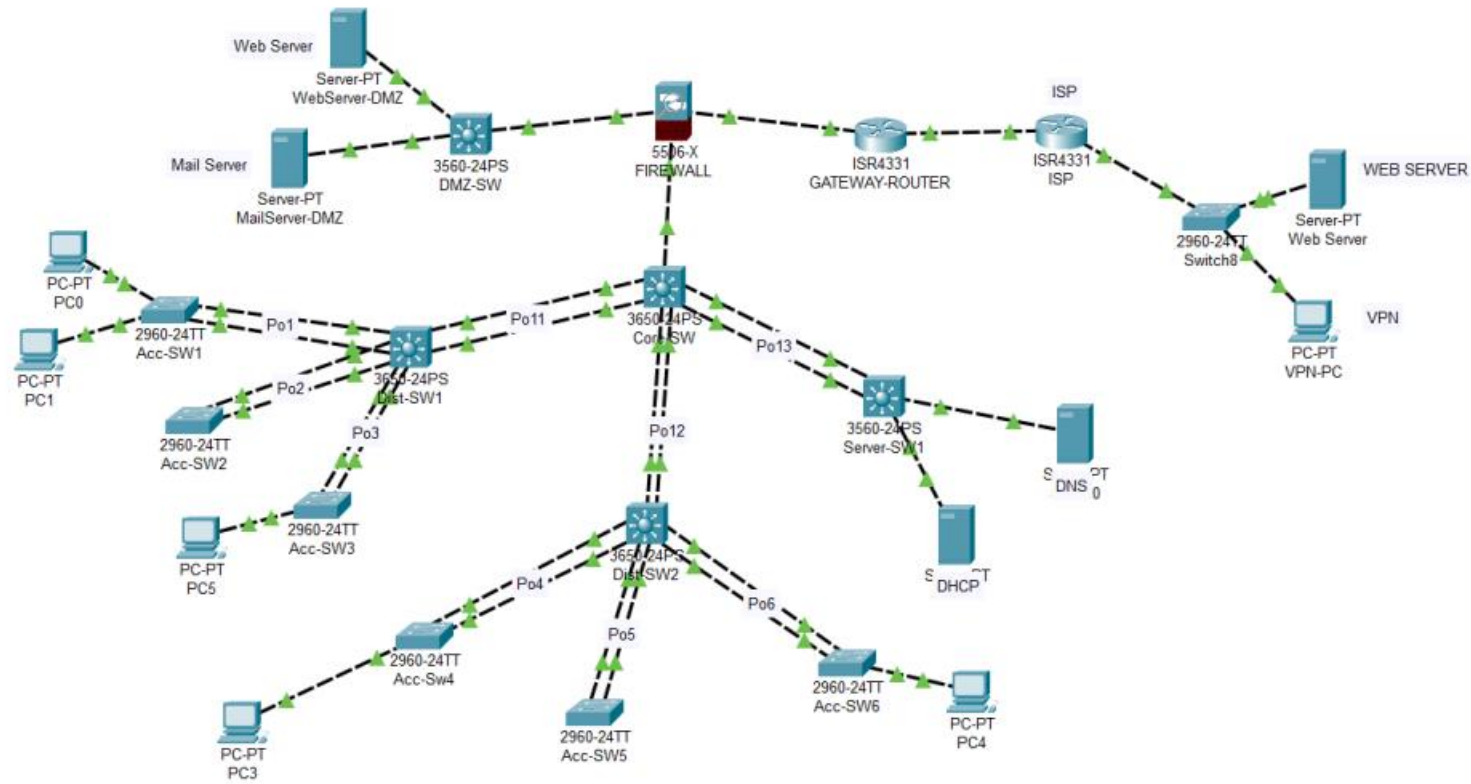
Họ tên: Mai Dương Nguyên Trường

MSSV: 19120698

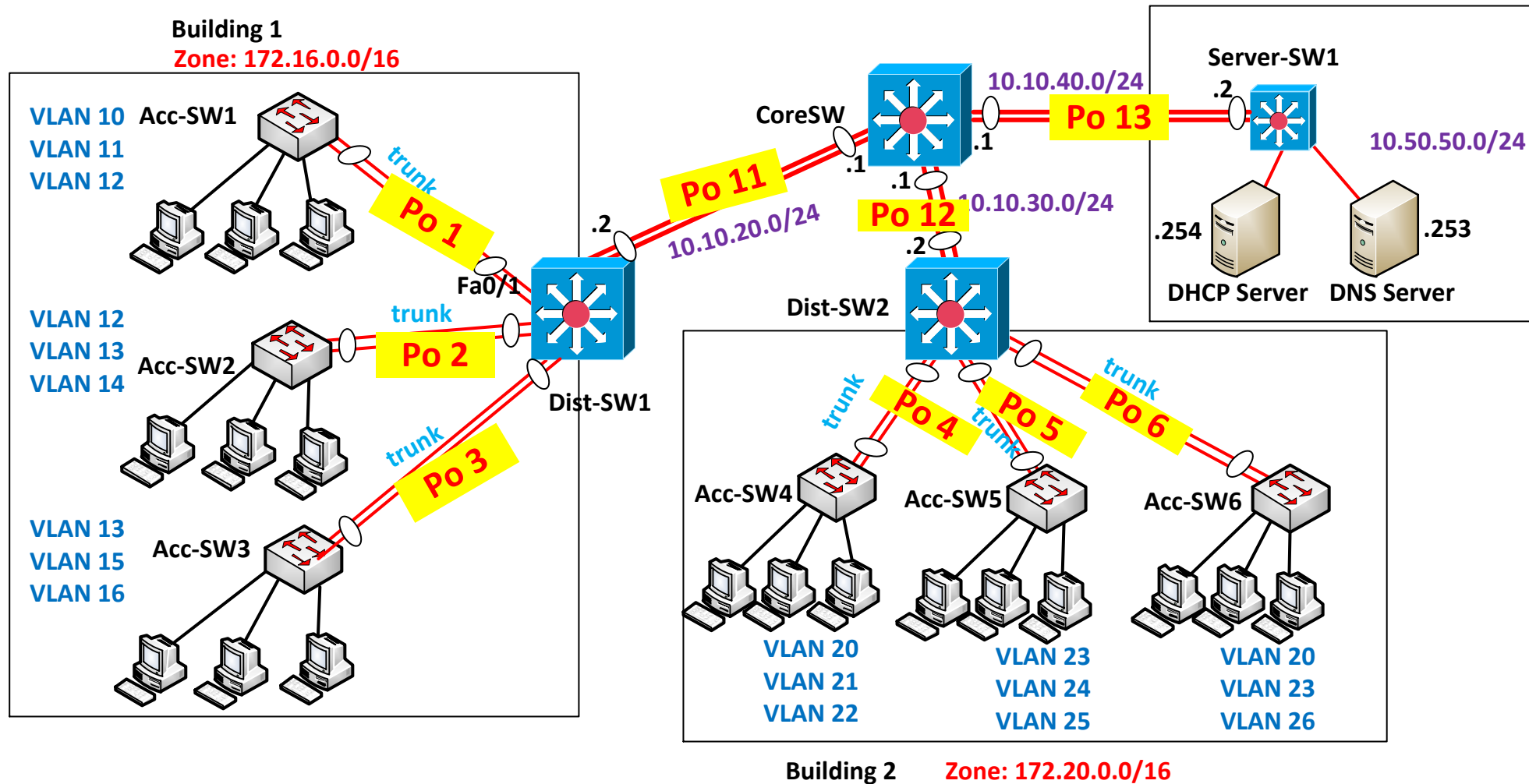
Cho sơ đồ mạng:



1) (2 điểm) Xây dựng sơ đồ mạng và cấu hình các tham số cơ bản như trong sơ đồ mạng trên phần mềm giả lập Packet Tracer



2) (2 điểm) Cấu hình EtherChannel, Trunking, VLAN (VTP), IP cho các interface VLAN



a) **Cấu hình EtherChannel**

- (i) Cấu hình L3 EtherChannel giữa Core-SW và Dist-SW1 (đặt tên channel là **Po 11**)
- (ii) Cấu hình L3 EtherChannel giữa Core-SW và Dist-SW2 (đặt tên channel là **Po 12**)
- (iii) Cấu hình L3 EtherChannel giữa Core-SW và Server-SW1 (đặt tên channel là **Po 13**)

- (iv) *Cấu hình L2 EtherChannel giữa Dist-SW1 và các Switch (Acc-SW1, Acc-SW2 và Acc-SW3) (đặt tên channel lần lượt là Po 1, Po 2, Po 3)*
- (v) *Cấu hình L2 EtherChannel giữa Dist-SW2 và các Switch (Acc-SW4, Acc-SW5 và Acc-SW6) (đặt tên channel lần lượt là Po 4, Po 5, Po 6)*

b) Cấu hình đường trunk

- (i) *Cấu hình trunk giữa Dist-SW1 với các switch: Acc-SW1, Acc-SW2 và Acc-SW3*
- (ii) *Cấu hình trunk giữa Dist-SW2 với các switch: Acc-SW4, Acc-SW5 và Acc-SW6*

c) Cấu hình VLAN (VTP)

(i) ***Building 1 (Dist-SW1, Acc-SW1, Acc-SW2, Acc-SW3)***

- *VTP domain: **HCMUS1***
- *VTP Server: Dist-SW1*
- *VTP client: Acc-SW1, Acc-SW2, Acc-SW3*
- *Các VLAN: VLAN 10, VLAN 11, VLAN 12, VLAN 13, VLAN 14, VLAN 15, VLAN 16 (Tên các VLAN các em tự đặt)*

(ii) ***Building 2 (Dist-SW2, Acc-SW4, Acc-SW5, Acc-SW6)***

- *VTP domain: **HCMUS2***
- *VTP Server: Dist-SW2*
- *VTP client: Acc-SW4, Acc-SW5, Acc-SW6*
- *Các VLAN: VLAN 20, VLAN 21, VLAN 22, VLAN 23, VLAN 24, VLAN 25, VLAN 26 (Tên các VLAN các em tự đặt)*

- Vì có rất nhiều cấu hình giống nhau nên em xin trình bày ra đây một số cấu hình điển hình cho từng yêu cầu trong bài tập 2.

- Cấu hình Etherchannel trên một Access switch.

The screenshot shows the CLI of an Acc-SW1 switch. The user has entered the command 'sh eth sum' to display the status of the Etherchannel configuration. The output shows that one channel-group is in use, configured with the PAgP protocol, and includes two ports: Gig0/1 and Gig0/2. The CLI interface also shows the command history and the current configuration mode.

```

Acc-SW1(config)#end
Acc-SW1#
%SYS-5-CONFIG_I: Configured from console by console
sh eth sum
Flags: D - down          P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3        S - Layer2
       U - in use        f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----
1      Pol(SU)          PAgP        Gig0/1 (P) Gig0/2 (P)
Acc-SW1#
Acc-SW1#
Acc-SW1#

```

- Cú pháp:

Acc-SW1(config)# interface range

Acc-SW1(config-if-range)#channel-protocol pagp

Acc-SW1(config-if-range)#channel-group mode desirable

- Cấu hình Etherchannel trên một Distribution switch điển hình.

```
Dist-SW1#sh eth sum
Flags:  D - down          P - in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 4
Number of aggregators:          4

Group  Port-channel  Protocol    Ports
-----+-----+-----
1      Po1(SU)        PAgP       Gig1/0/1(P) Gig1/0/2(P)
2      Po2(SU)        PAgP       Gig1/0/3(P) Gig1/0/4(P)
3      Po3(SU)        PAgP       Gig1/0/5(P) Gig1/0/6(P)
11     Po11(RU)        PAgP       Gig1/0/7(P) Gig1/0/8(P)
Dist-SW1#
Dist-SW1#
Dist-SW1#
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top

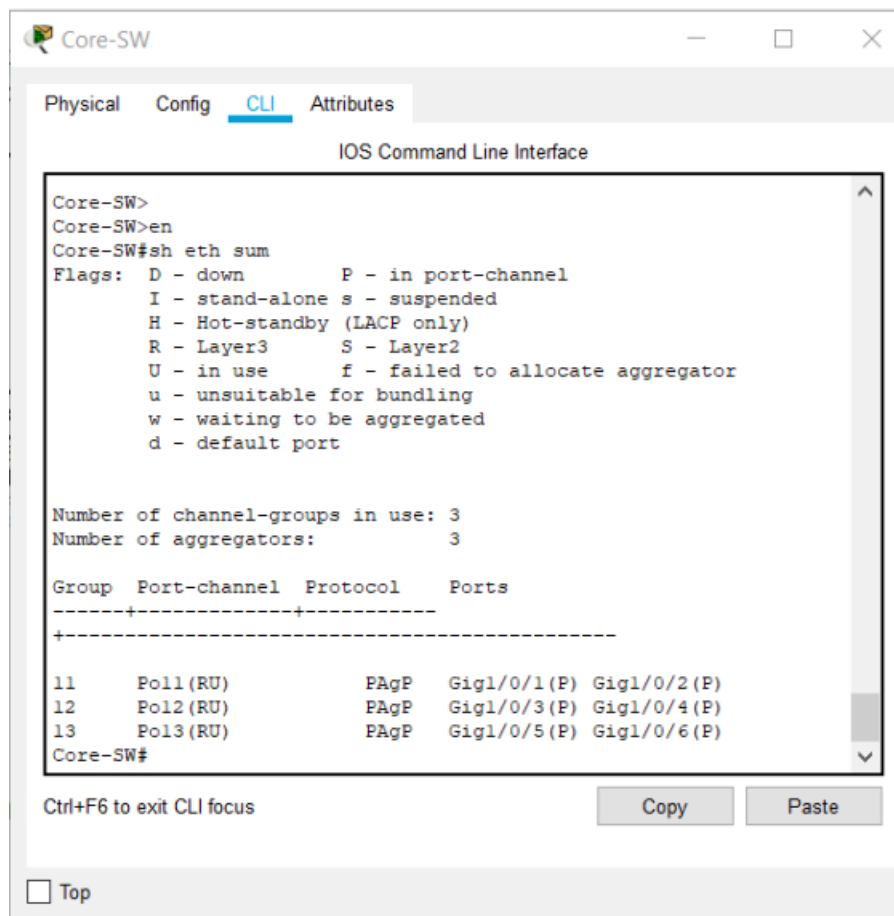
- Cú pháp:

Dist-SW1(config)# interface range

Dist-SW1(config-if-range)#channel-protocol pagp

Dist-SW1(config-if-range)#channel-group mode desirable

- Cấu hình Etherchannel trên Core switch.



The screenshot shows a window titled 'Core-SW' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The command 'Core-SW#sh eth sum' has been executed, showing the following output:

```
Core-SW>
Core-SW>en
Core-SW#sh eth sum
Flags:  D - down          P - in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 3
Number of aggregators:          3

Group  Port-channel  Protocol    Ports
-----+-----+-----
11     Pol11(RU)        PAgP       Gig1/0/1(P) Gig1/0/2(P)
12     Pol12(RU)        PAgP       Gig1/0/3(P) Gig1/0/4(P)
13     Pol13(RU)        PAgP       Gig1/0/5(P) Gig1/0/6(P)
Core-SW#
```

Below the output, there is a prompt 'Ctrl+F6 to exit CLI focus' and two buttons: 'Copy' and 'Paste'. At the bottom left, there is a checkbox labeled 'Top'.

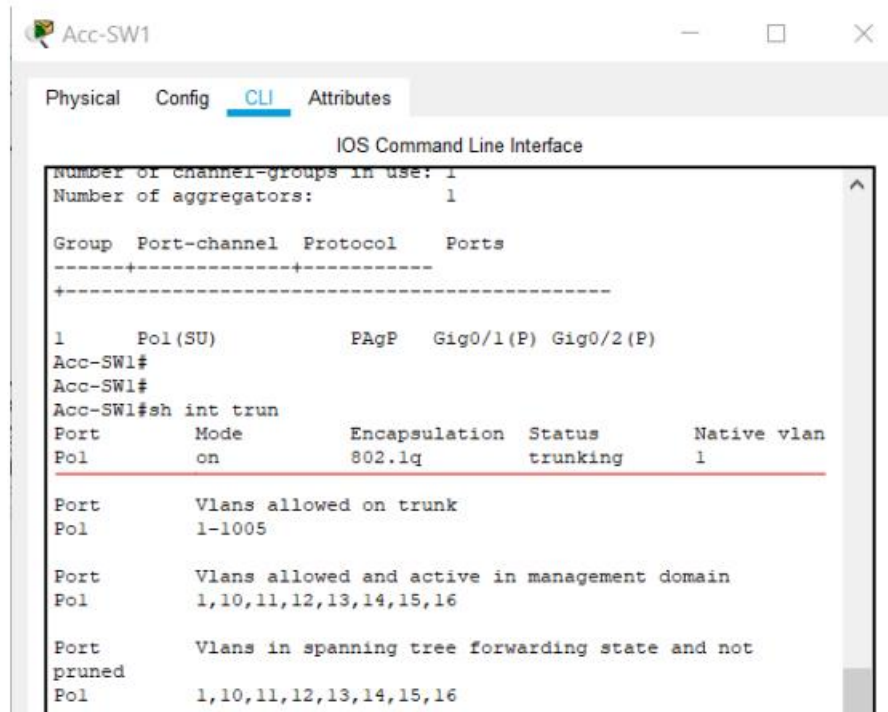
- Cú pháp:

Core-SW(config)# interface range

Core-SW(config-if-range)#channel-protocol pagp

Core-SW(config-if-range)#channel-group mode desirable

- Cấu hình đường Trunk.



- Cú pháp:

Acc-SW1(config)# interface

Acc-SW1(config-if)# switchport mode trunk

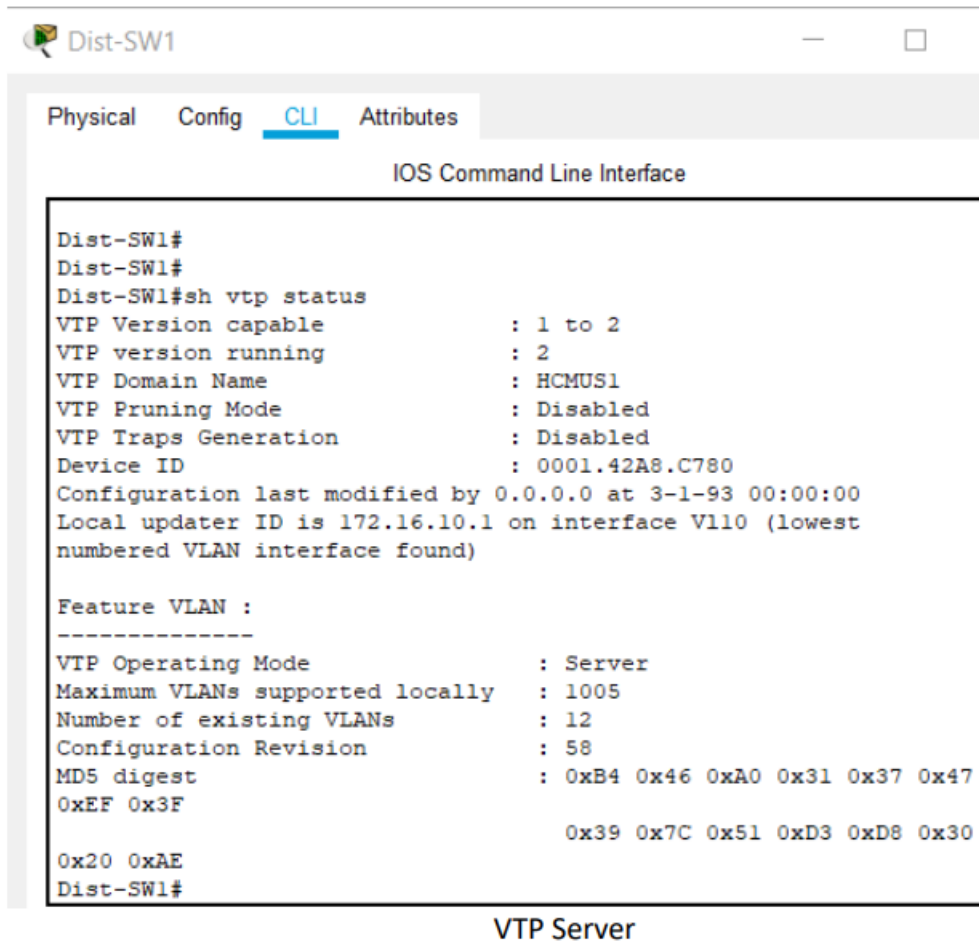
- Cú pháp:

Acc-SW1(config)# interface

Acc-SW1(config-if)# switchport mode trunk

- Cấu hình VTP

+ Cấu hình VTP domain HCMUS1



The screenshot shows a network switch interface with tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the IOS Command Line Interface. The user has entered the command 'sh vtp status', which shows the following output:

```
Dist-SW1#
Dist-SW1#
Dist-SW1#sh vtp status
VTP Version capable      : 1 to 2
VTP version running     : 2
VTP Domain Name          : HCMUS1
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : 0001.42A8.C780
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 172.16.10.1 on interface V110 (lowest
numbered VLAN interface found)

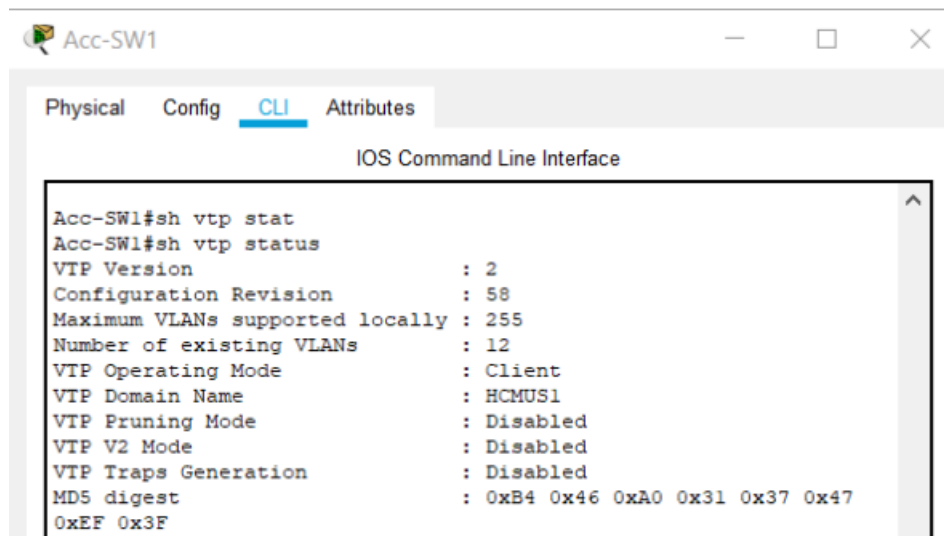
Feature VLAN :
-----
VTP Operating Mode       : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs : 12
Configuration Revision   : 58
MD5 digest               : 0xB4 0x46 0xA0 0x31 0x37 0x47
                          0xEF 0x3F
                          0x39 0x7C 0x51 0xD3 0xD8 0x30
                          0x20 0xAE
Dist-SW1#
```

VTP Server

+ Cú pháp:

Dist-SW1(config)# vtp domain HCMUS1

Dist-SW1(config)# vtp mode server



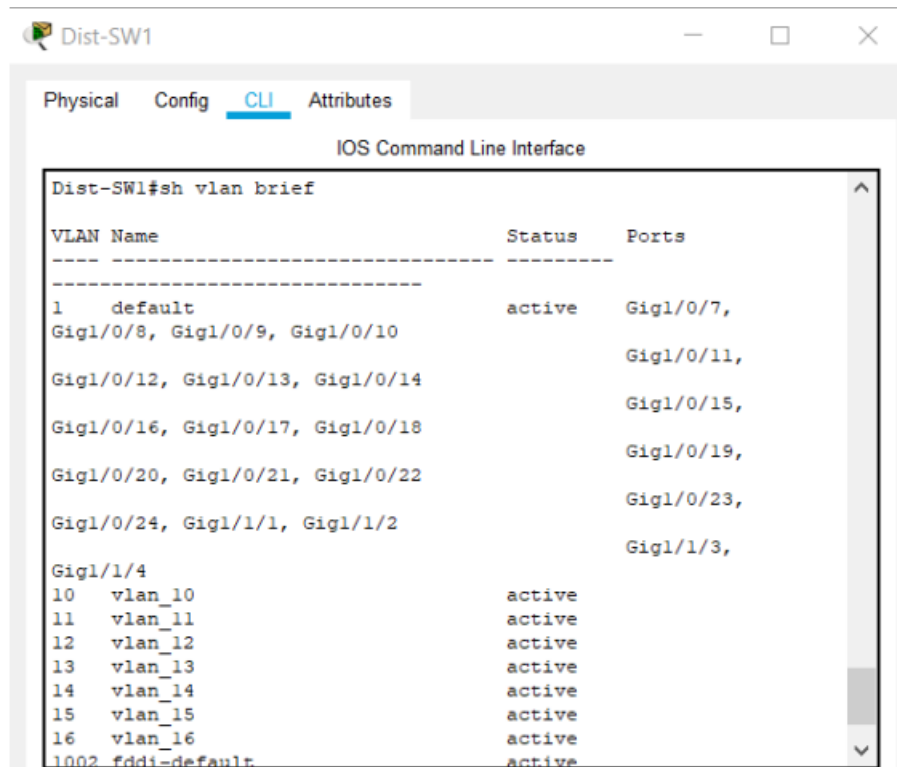
VTP Client

+Cú pháp:

Acc-SW1(config)# vtp domain HCMUS1

Acc-SW1(config)# vtp mode client

+ Các VLAN trên Distribution switch 1

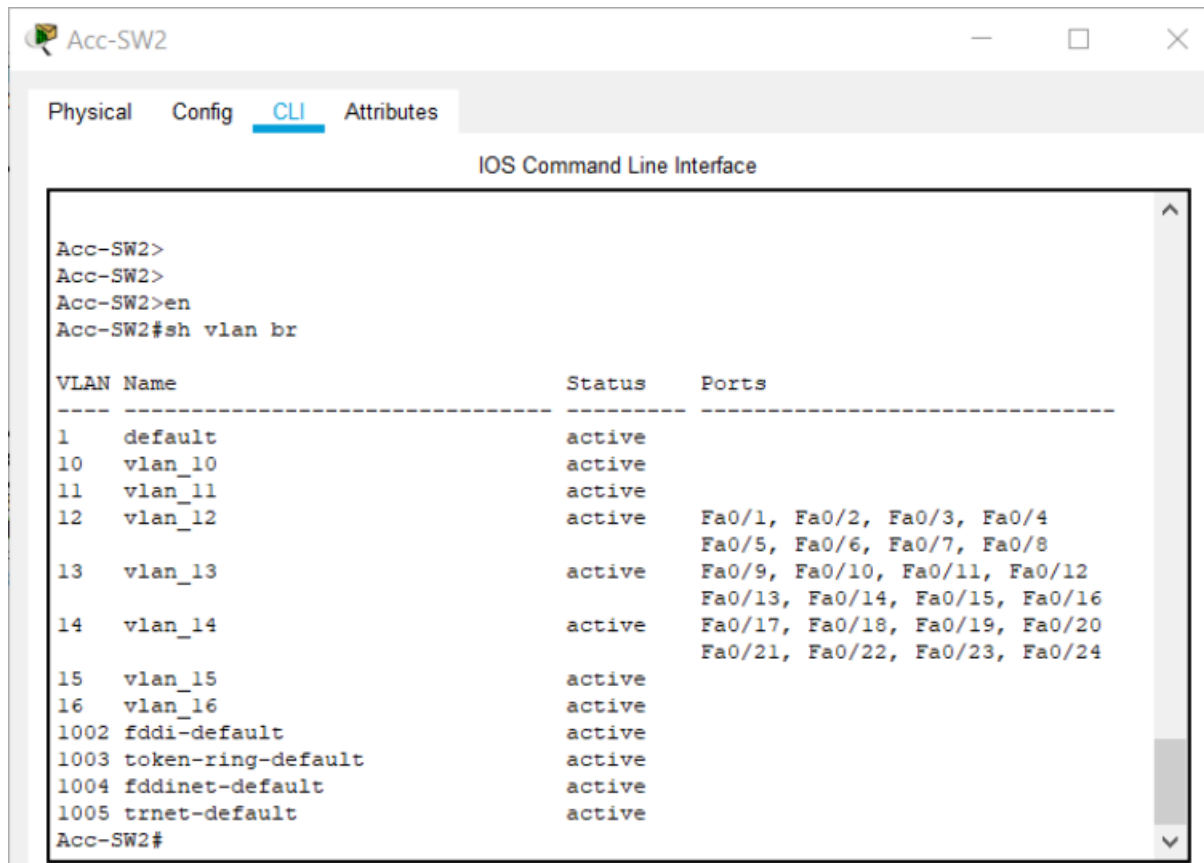


+ Cú pháp tạo vlan:

Dist-SW(config)# vlan

Dist-SW(config)# vlan name

+Các VLAN trên Access switch 2 và các port được chia tương ứng với VLAN đó



The screenshot shows a network device window titled 'Acc-SW2' with tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the 'IOS Command Line Interface'. The user has entered the following commands:

```
Acc-SW2>
Acc-SW2>
Acc-SW2>en
Acc-SW2#sh vlan br
```

The output is a table showing VLAN information:

VLAN	Name	Status	Ports
1	default	active	
10	vlan_10	active	
11	vlan_11	active	
12	vlan_12	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8
13	vlan_13	active	Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16
14	vlan_14	active	Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24
15	vlan_15	active	
16	vlan_16	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

The prompt 'Acc-SW2#' is visible at the bottom of the CLI window.

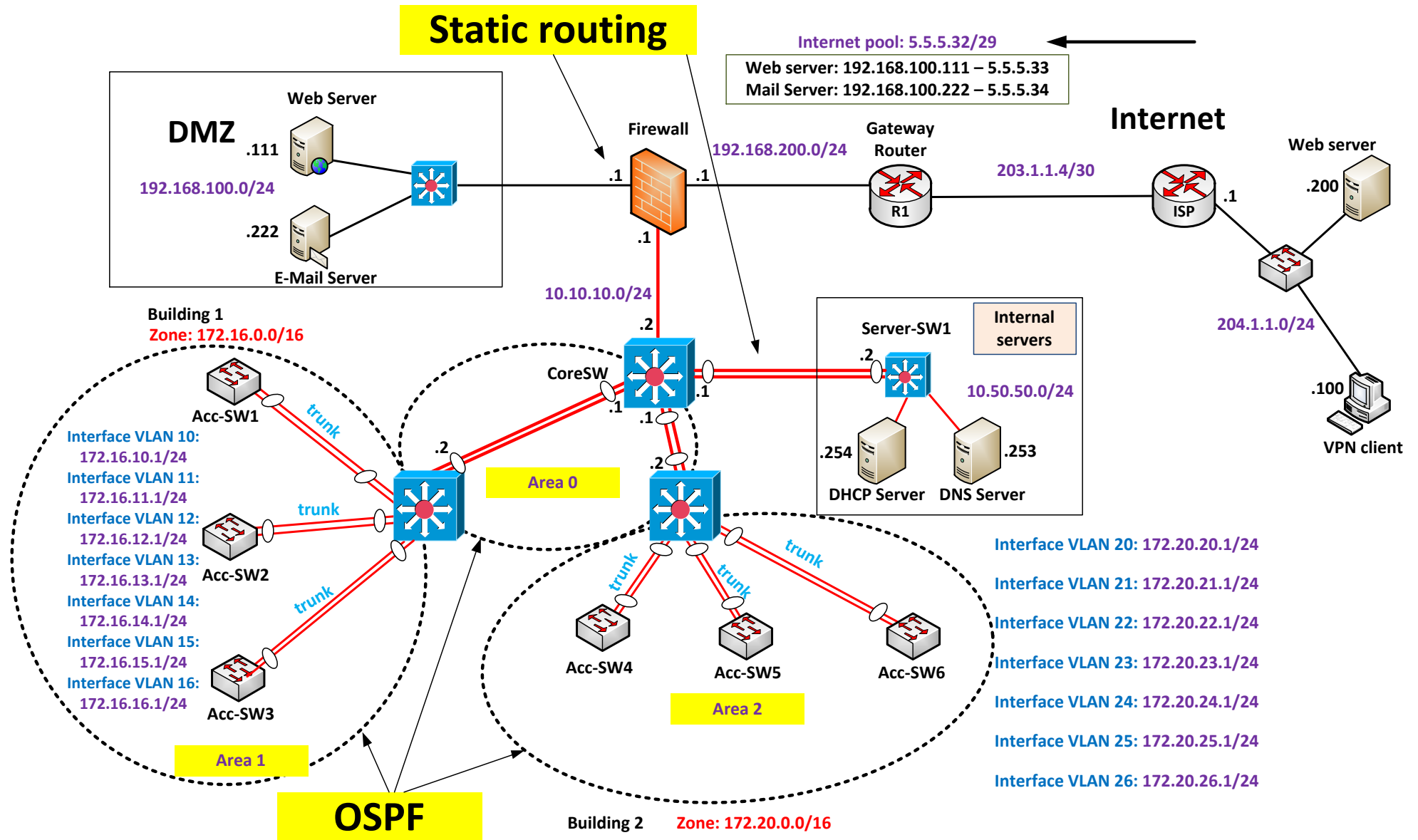
+ Cú pháp gán các port vào từng vlan:

Acc-SW(config)# interface range

Acc-SW(config-if-range)# switchport mode access

Acc-SW(config-if-range)# switchport access vlan

3) (2 điểm) Cấu hình định tuyến cho hệ thống mạng nội bộ



- (i) Cấu hình định tuyến trên Firewall (cấu hình cho phép tất cả các traffic đi qua Firewall)
- (ii) Cấu hình định tuyến trên Core-SW, Dist-SW1, Dist-SW2, Server-SW1 Router Gateway R1

- Cấu hình địa chỉ ip trên Dist-SW1

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
Port-channel1	Up	--	<not set>	<not set>	00D0.D3AB.2209
Port-channel2	Up	--	<not set>	<not set>	0001.63C5.8838
Port-channel3	Up	--	<not set>	<not set>	000B.BE9D.4B27
Port-channel11	Up	1	10.10.20.2/24	<not set>	0001.42A8.C784
Vlan10	Up	10	172.16.10.1/24	<not set>	000B.BE22.D101
Vlan11	Up	11	172.16.11.1/24	<not set>	000B.BE22.D102
Vlan12	Up	12	172.16.12.1/24	<not set>	000B.BE22.D103
Vlan13	Up	13	172.16.13.1/24	<not set>	000B.BE22.D104
Vlan14	Up	14	172.16.14.1/24	<not set>	000B.BE22.D105
Vlan15	Up	15	172.16.15.1/24	<not set>	000B.BE22.D106
Vlan16	Up	16	172.16.16.1/24	<not set>	000B.BE22.D107
Hostname: Dist-SW1					
Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet					

- Cú pháp cấu hình địa chỉ ip cho các interface Vlan:

Dist-SW1(config)# ip routing

Dist-SW1(config)# interface vlan

Dist-SW1(config-if)# ip address

Dist-SW1(config-if)# no shutdown

- Cấu hình địa chỉ ip trên Dist-SW2

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
Port-channel4	Up	--	<not set>	<not set>	0050.0FB2.A526
Port-channel5	Up	--	<not set>	<not set>	0010.1102.9C44
Port-channel6	Up	--	<not set>	<not set>	00D0.D3E8.9871
Port-channel12	Up	1	10.10.30.2/24	<not set>	0001.C7E5.99C5
Vlan1	Down	1	<not set>	<not set>	0060.70C5.E1D4
Vlan20	Up	20	172.20.20.1/24	<not set>	0060.70C5.E101
Vlan21	Up	21	172.20.21.1/24	<not set>	0060.70C5.E102
Vlan22	Up	22	172.20.22.1/24	<not set>	0060.70C5.E103
Vlan23	Up	23	172.20.23.1/24	<not set>	0060.70C5.E104
Vlan24	Up	24	172.20.24.1/24	<not set>	0060.70C5.E105
Vlan25	Up	25	172.20.25.1/24	<not set>	0060.70C5.E106
Vlan26	Up	26	172.20.26.1/24	<not set>	0060.70C5.E107
Hostname: Dist-SW2					
Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet					

- Cấu hình địa chỉ ip trên Gateway router

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
GigabitEthernet0/0/0	Up	--	192.168.200.2/24	<not set>	0001.C972.AE01
GigabitEthernet0/0/1	Up	--	203.1.1.5/30	<not set>	0001.C972.AE02
GigabitEthernet0/0/2	Down	--	<not set>	<not set>	0001.C972.AE03
Vlan1	Down	1	<not set>	<not set>	00E0.F7C6.ADE5
Hostname: R1					
Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet					

- Cấu hình địa chỉ ip trên Server-SW

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
Port-channel13	Up	1	10.10.40.2/24	<not set>	0000.0C00.CC8A
Vlan1	Down	1	<not set>	<not set>	00E0.A3AC.0BB2
Vlan2	Up	2	10.50.50.2/24	<not set>	00E0.A3AC.0B01
Hostname: Server-SW1					
Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet					

Ở đây để DNS Server và DHCP Server có thể chung đường mạng 10.50.50.0/24 thì em đã sử dụng Vlan interface và gán địa chỉ ip cho nó.

- Cấu hình địa chỉ ip trên Core-SW

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
Port-channel11	Up	1	10.10.20.1/24	<not set>	0004.9A7E.995B
Port-channel12	Up	1	10.10.30.1/24	<not set>	0060.7026.9BA7
Port-channel13	Up	1	10.10.40.1/24	<not set>	0006.2A74.BDC2
GigabitEthernet1/0/7	Up	1	10.10.10.2/24	<not set>	0060.3EED.4B07

- Các bước cấu hình địa chỉ ip cho port-channel trên các switch layer 3:

Core-SW(config)# interface Po

Core-SW(config-if)# no switchport

Core-SW(config-if)# ip address

Core-SW(config-if)# no shutdown

- Cấu hình địa chỉ ip trên Firewall

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
GigabitEthernet1/1	Up	--	10.10.10.1/24	<not set>	0006.2A2B.BD01
GigabitEthernet1/2	Up	--	192.168.200.1/24	<not set>	0006.2A2B.BD02
GigabitEthernet1/3	Up	--	192.168.100.1/24	<not set>	0006.2A2B.BD03

- Cú pháp cấu hình địa chỉ ip cũng như tên cổng ra và cấp độ bảo mật của từng cổng trong Firewall:

```
FW(config)# interface
```

```
FW(config-if)# nameif
```

```
FW(config-if)# security-level
```

```
FW(config-if)# ip address
```

Nguyên tắc về security-level: các traffic có thể đi từ cổng có security-level cao hơn đến cổng có security-level thấp hơn nhưng không thể đi ngược lại. Vì vậy, thông thường người ta hay đặt security-level cho Outside là 0, cho Inside là 100 và cho DMZ là từ 1-99.

Vì vậy để có thể cho phép tất cả các gói tin đi qua FW mà không bị chặn lại thì ta phải tạo một access-list cho phép tất cả các cổng có thể truyền tin cho nhau.

Cụ thể:

+ Trước tiên thì ta phải định tuyến, có thể sử dụng định tuyến động bằng giao thức ospf hoặc sử dụng định tuyến tĩnh như cú pháp sau:

```
FW(config)# route <chọn cổng cần route(VD:inside, outside, dmz)><mạng đích> <subnet mask> <next-hop>
```

```
VD: FW(config)# route inside 172.20.0.0 255.255.0.0 10.10.10.2
```

+ Sau đó ta cần đặt ra chính sách cho các cổng như sau:

```
FW(config)# access-list <tên của chính sách do người dùng đặt, VD: allow-all> permit ip any any
```

```
FW(config)# access-group <tên của chính sách do người dùng đặt, VD: allow-all> in interface <tên interface>
```

```
VD: FW(config)# access-list allow-all permit ip any any
```

```
FW(config)# access-list allow-all in interface inside
```


FW(config)# access-list allow-all in interface outside

FW(config)# access-list allow-all in interface dmz

- Định tuyến firewall

```
FIREWALL
Physical Config CLI Attributes
IOS Command Line Interface

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

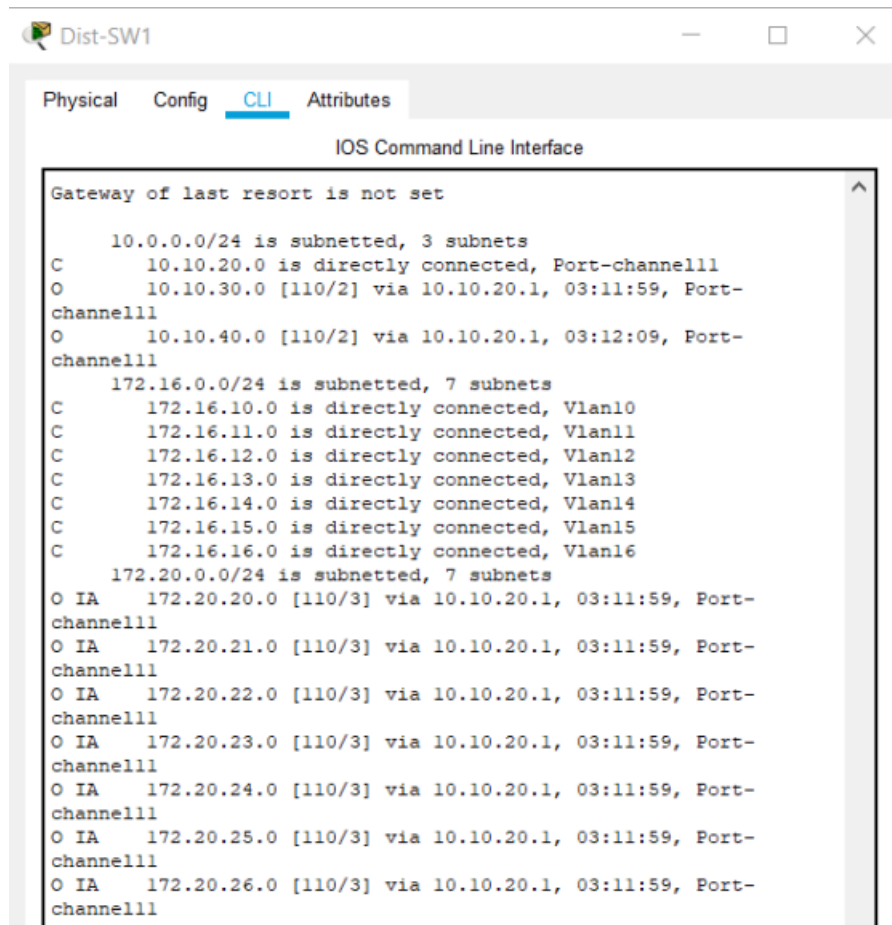
Gateway of last resort is not set

10.0.0.0/24 is subnetted, 6 subnets
C    10.0.0.0 255.255.255.0 is directly connected, inside, GigabitEthernet1/1
C    10.10.10.0 255.255.255.0 is directly connected, inside, GigabitEthernet1/1
S    10.10.20.0 255.255.255.0 [1/0] via 10.10.10.2, inside
S    10.10.30.0 255.255.255.0 [1/0] via 10.10.10.2, inside
S    10.10.40.0 255.255.255.0 [1/0] via 10.10.10.2, inside
S    10.50.50.0 255.255.255.0 [1/0] via 10.10.10.2, inside
S    172.16.0.0 255.255.0.0 [1/0] via 10.10.10.2, inside
S    172.20.0.0 255.255.0.0 [1/0] via 10.10.10.2, inside
C    192.168.100.0 255.255.255.0 is directly connected, DMZ, GigabitEthernet1/3
C    192.168.200.0 255.255.255.0 is directly connected, outside, GigabitEthernet1/2
FW#
```

- Firewall access-list:

```
FW#sh access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval 300
access-list allow-all; 1 elements; name hash: 0xb4336863
access-list allow-all line 1 extended permit ip any any(hitcnt=1) 0x2462e5c6
FW#
```

- Bảng định tuyến trên Dist-SW1



Giao thức định tuyến động được sử dụng trong bài này là OSPF.

- Cú pháp sử dụng OSPF:

Dist-SW1(config)# router ospf <1-10, đây là id processing>

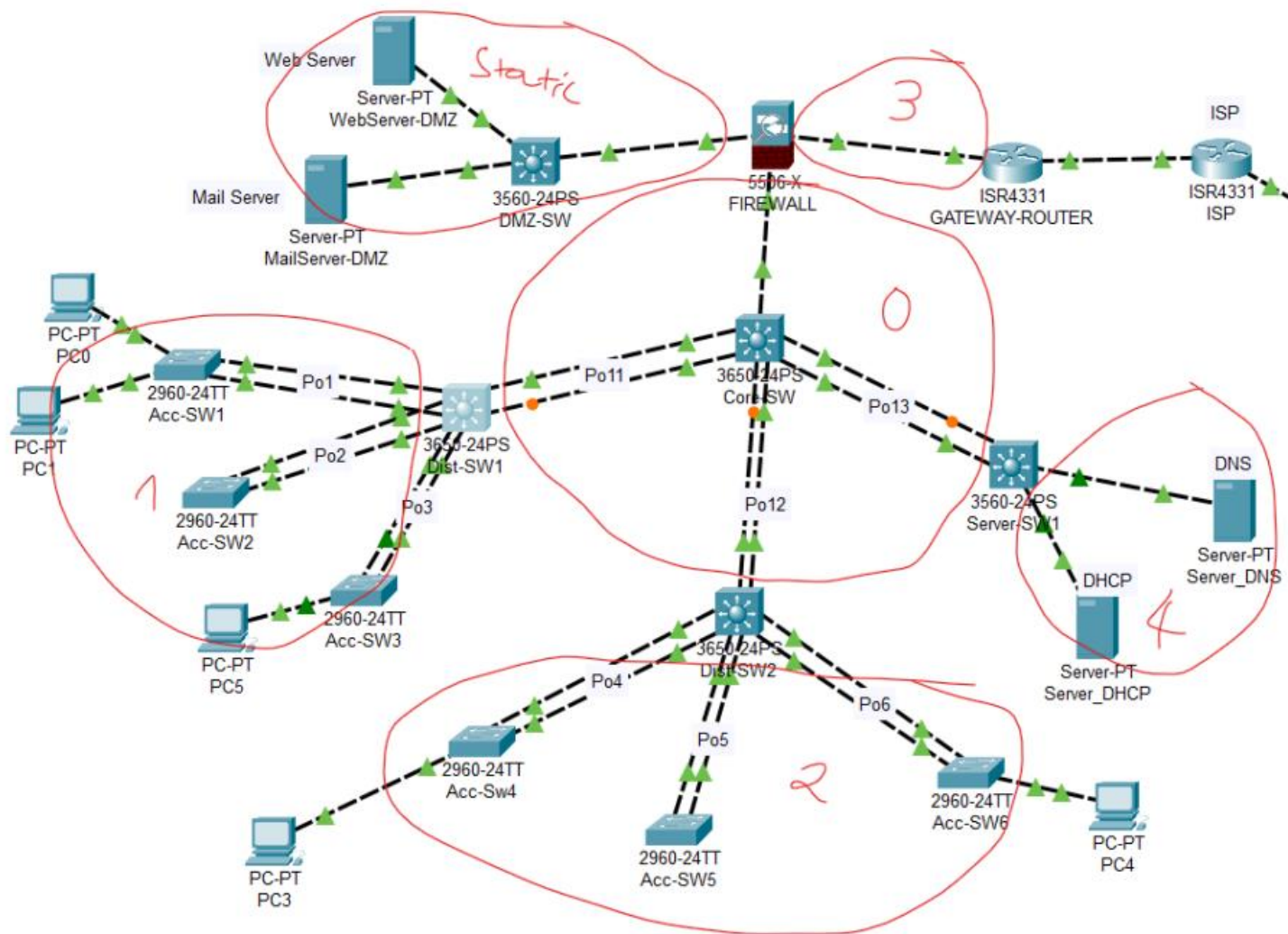
Dist-SW1(config-router)# network <Đường mạng> <phần bù của subnet mask> area<0-4294967295>

Vd:

Dist-SW1(config)# router ospf 10

Dist-SW1(config-router)# network 10.10.20.0 0.0.0.255 area 0

- Các khu vực được định tuyến trong bài tập



4) (2 điểm) Cấu hình dịch vụ mạng

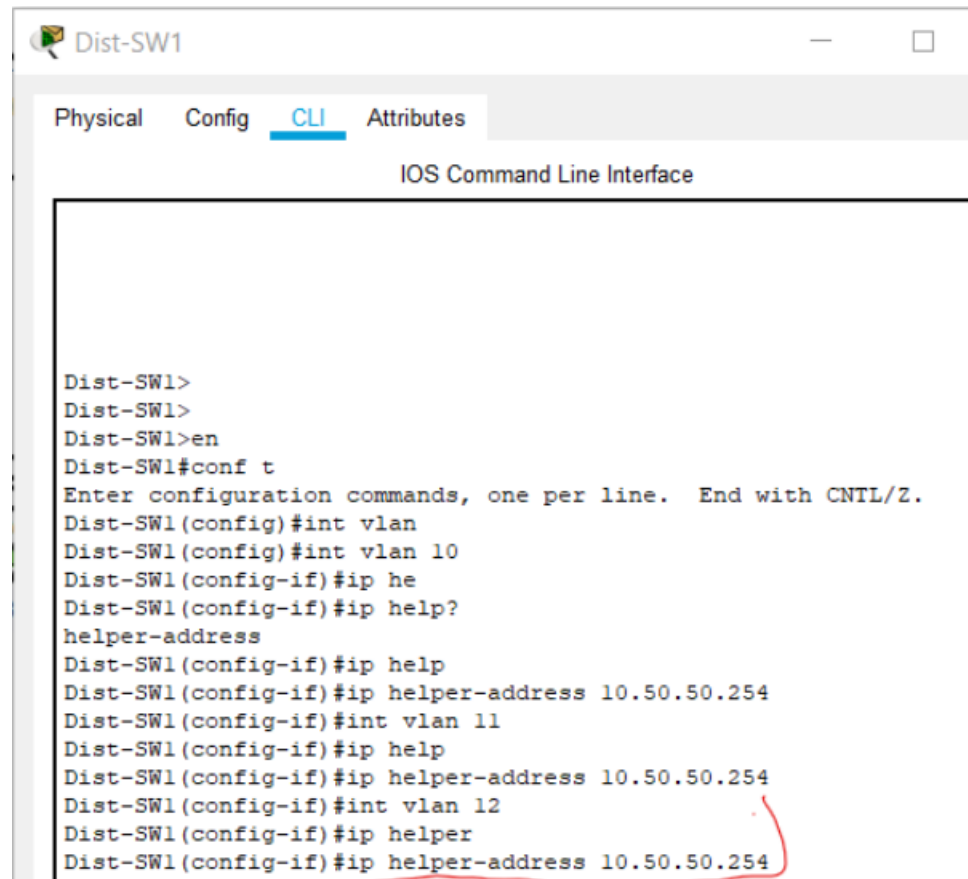
- Cấu hình DHCP cấp phát IP cho client ở các VLAN

- Cấu hình local DNS phân giải cho server WEB (www.xyz.net) và FTP (mail.xyz.net)

- Cấu hình DHCP cấp phát địa chỉ ip :

+ Có 2 TH có thể xảy ra. TH1 nếu DHCP server và DHCP client nằm cùng miền broadcast domain thì chỉ cần cấu hình DHCP server là đủ. TH2 nếu DHCP server và DHCP client nằm khác mạng thì ta cần phải cấu hình thêm DHCP agent để làm nơi trung gian thông báo việc cấp phát ip từ client đến DHCP server.

Cụ thể, như sau:



The screenshot shows a network switch configuration window titled 'Dist-SW1'. It has tabs for 'Physical', 'Config', 'CLI', and 'Attributes', with 'CLI' selected. Below the tabs is the title 'IOS Command Line Interface'. The main area displays a series of configuration commands entered in a terminal-like interface. The commands are as follows:

```
Dist-SW1>
Dist-SW1>
Dist-SW1>en
Dist-SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Dist-SW1(config)#int vlan
Dist-SW1(config)#int vlan 10
Dist-SW1(config-if)#ip he
Dist-SW1(config-if)#ip help?
helper-address
Dist-SW1(config-if)#ip help
Dist-SW1(config-if)#ip helper-address 10.50.50.254
Dist-SW1(config-if)#int vlan 11
Dist-SW1(config-if)#ip help
Dist-SW1(config-if)#ip helper-address 10.50.50.254
Dist-SW1(config-if)#int vlan 12
Dist-SW1(config-if)#ip helper
Dist-SW1(config-if)#ip helper-address 10.50.50.254
```

The last line of the configuration, `Dist-SW1(config-if)#ip helper-address 10.50.50.254`, is underlined in red.

+ Tiếp theo tạo các pools(scope) chứa các địa chỉ cần cấp phát trên DHCP server. Cụ thể như sau:

Server_DHCP

Physical

Config

Services

Desktop

Programming

Attributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

DHCP

Interface

FastEthernet0

Service

☒ On
☐ Off

Pool Name

vlan_10

Default Gateway

172.16.10.1

DNS Server

10.50.50.253

Start IP Address :

172

16

10

2

Subnet Mask:

255

255

255

0

Maximum Number of Users :

100

TFTP Server:

0.0.0.0

WLC Address:

0.0.0.0

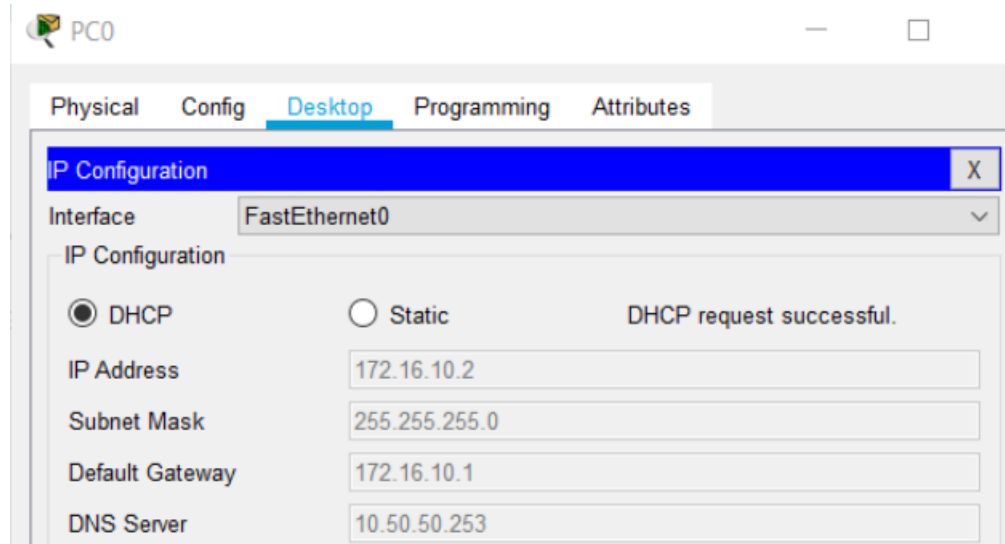
Add

Save

Remove

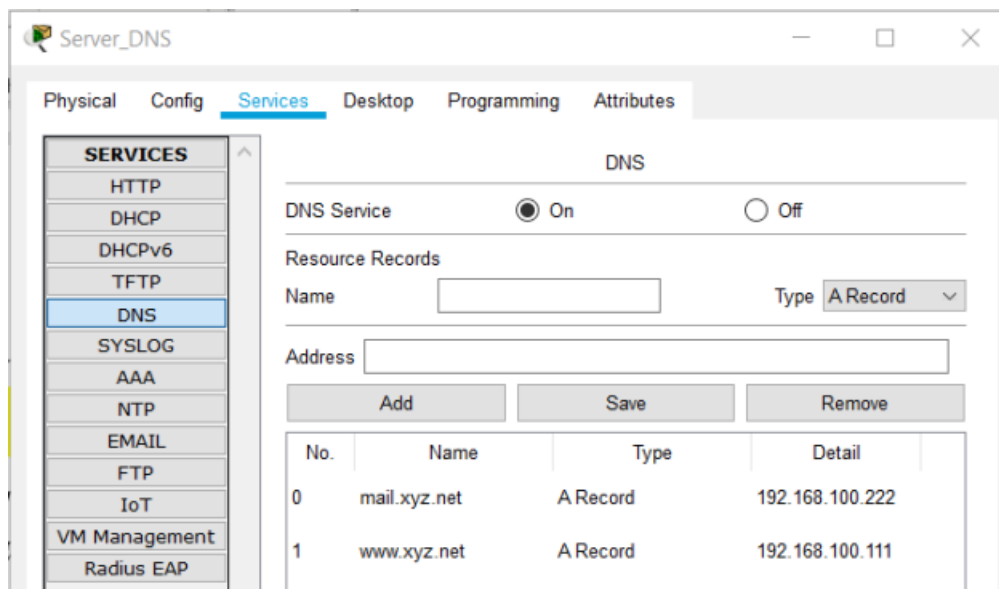
Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
vlan_10	172.16.10.1	10.50.50.253	172.16.10.2	255.255.25...	100	0.0.0.0	0.0.0.0

+ Kết quả sau khi khởi tạo DHCP:

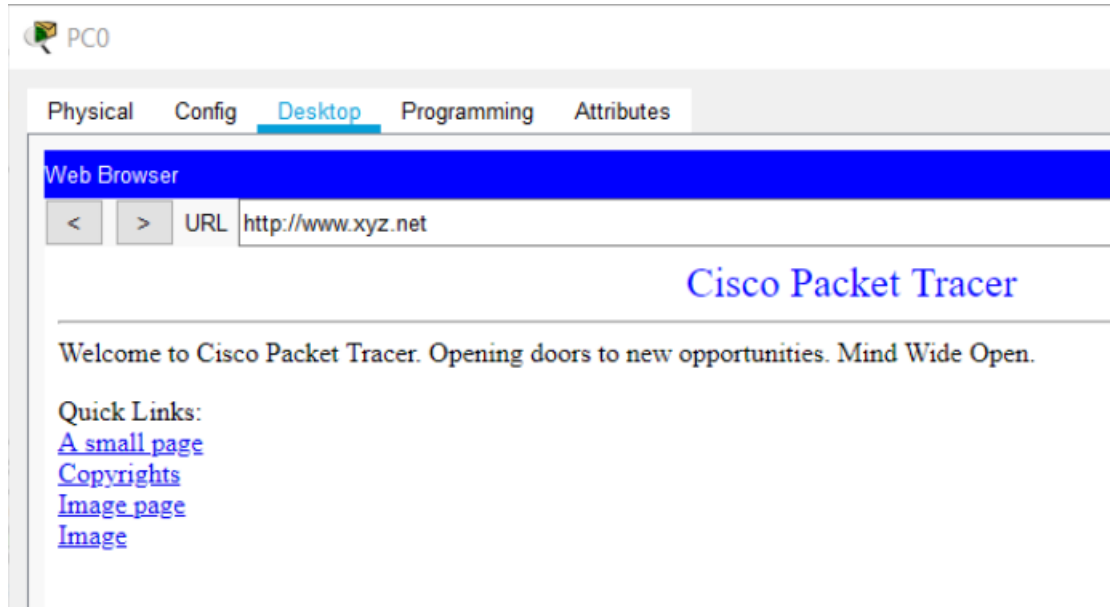


- Cấu hình DNS server:

+ Để có thể cấu hình được DNS server trở được tới các địa chỉ ở vùng DMZ thì ta phải làm tất cả các bước ở trên trước sau đó mới có thể thêm URL vào DNS server. Sau đó ta tiến hành cấu hình ở DNS server.



+ Kết quả thu được:



5) (2 điểm) **Cấu hình NAT**

Giải sử công ty thuê địa chỉ IP public và được ISP cấp cho các IP public thuộc mạng 5.5.5.32/29.

(i) *Cấu hình Router ISP*

- Cấu hình trên router ISP để định tuyến cho mạng 5.5.5.32/29 để cấp phát cho công ty.

(ii) *Cấu hình trên Router gateway R1*

- Public 2 server ở vùng DMZ với IP public như trong sơ đồ mạng
- Cấu hình PAT cho phép mạng nội bộ ra ngoài Internet
- Cấu hình route cho ISP



Physical Config CLI Attributes

IOS Command Line Interface

```
ISP(config)#ip route 5.5.5.32 255.255.255.248 203.1.1.5
ISP(config)#end
ISP#
%SYS-5-CONFIG_I: Configured from console by console
sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

      5.0.0.0/29 is subnetted, 1 subnets
S       5.5.5.32/29 is directly connected, GigabitEthernet0/0/0
          [1/0] via 203.1.1.5
      203.1.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       203.1.1.4/30 is directly connected, GigabitEthernet0/0/0
L       203.1.1.6/32 is directly connected, GigabitEthernet0/0/0
```

- Cấu hình để public 2 server trong vùng DMZ ra ngoài


```
Physical  Config  CLI  Attributes
IOS Command Line Interface

R1>
R1>
R1>
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip nat inside source static 192.168.100.111 5.5.5.33
R1(config)#ip nat inside source static 192.168.100.222 5.5.5.34
R1(config)#int gi0/0/0
R1(config-if)#ip nat ins
R1(config-if)#ip nat inside
R1(config-if)#int gi0/0/1
R1(config-if)#ip nat outside
R1(config-if)#
R1(config-if)#
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
sh ip nat tra
R1#sh ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
---  5.5.5.33             192.168.100.111   ---               ---
---  5.5.5.34             192.168.100.222   ---               ---
```

- Cú pháp cấu hình public server trong DMZ

+ Đầu tiên, ta cũng phải định tuyến cho Gateway Router bằng cách như đã trình bày bên trên (cụ thể là định tuyến động dùng giao thức OSPF).

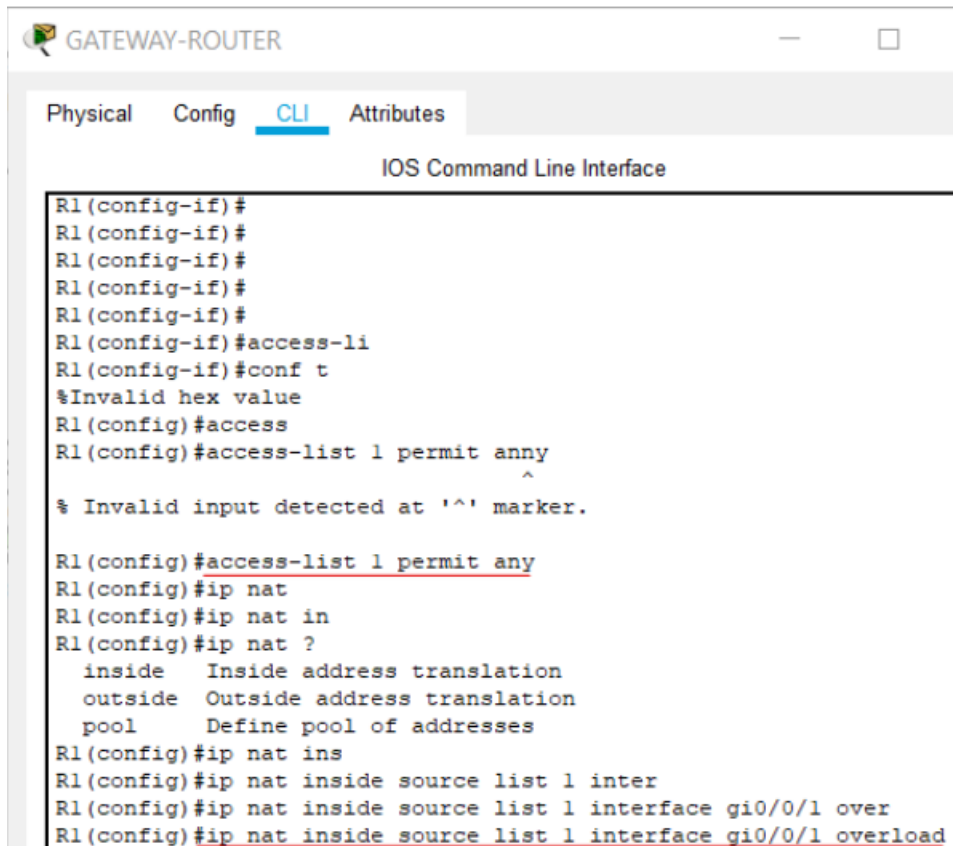
+ Sau đó để public server ra ngoài, ta dùng cú pháp:

```
R1(config)#ip nat inside source static <local-ip><global-ip>
```

+ Và cuối cùng ta phải xác định các inside và outside;

```
R1(config-if)#ip nat <inside/outside>
```

- Cấu hình PAT



```
GATEWAY-ROUTER
Physical Config CLI Attributes
IOS Command Line Interface
R1(config-if)#
R1(config-if)#
R1(config-if)#
R1(config-if)#
R1(config-if)#
R1(config-if)#access-li
R1(config-if)#conf t
%Invalid hex value
R1(config)#access
R1(config)#access-list 1 permit anny
^
% Invalid input detected at '^' marker.
R1(config)#access-list 1 permit any
R1(config)#ip nat
R1(config)#ip nat in
R1(config)#ip nat ?
    inside    Inside address translation
    outside   Outside address translation
    pool       Define pool of addresses
R1(config)#ip nat ins
R1(config)#ip nat inside source list 1 inter
R1(config)#ip nat inside source list 1 interface gi0/0/1 over
R1(config)#ip nat inside source list 1 interface gi0/0/1 overload
```

+ B1: Tạo access list cho phép đi ra mạng bên ngoài

+ B2: Tạo NAT

+ B3: Xác định inside và outside interface (tuy nhiên bước này đã được làm từ trước nên ta không cần làm lại)

- Lưu ý: Phải tạo Default Route cho tất cả các Router, Switch layer 3, Firewall bên trong mạng. Vì nếu bảng định tuyến của các thiết bị đó không chứa Default Route thì khi ta muốn tới một mạng nằm ngoài mạng nội bộ thì nó sẽ không biết phải đi đến thiết bị nào. Vì vậy ta nên tạo Default Route sao cho các thiết bị đó trỏ đến Router biên.

- Cú pháp như sau:

```
Dist-SW1(config)# ip route 0.0.0.0 0.0.0.0 <next-hop>
```

