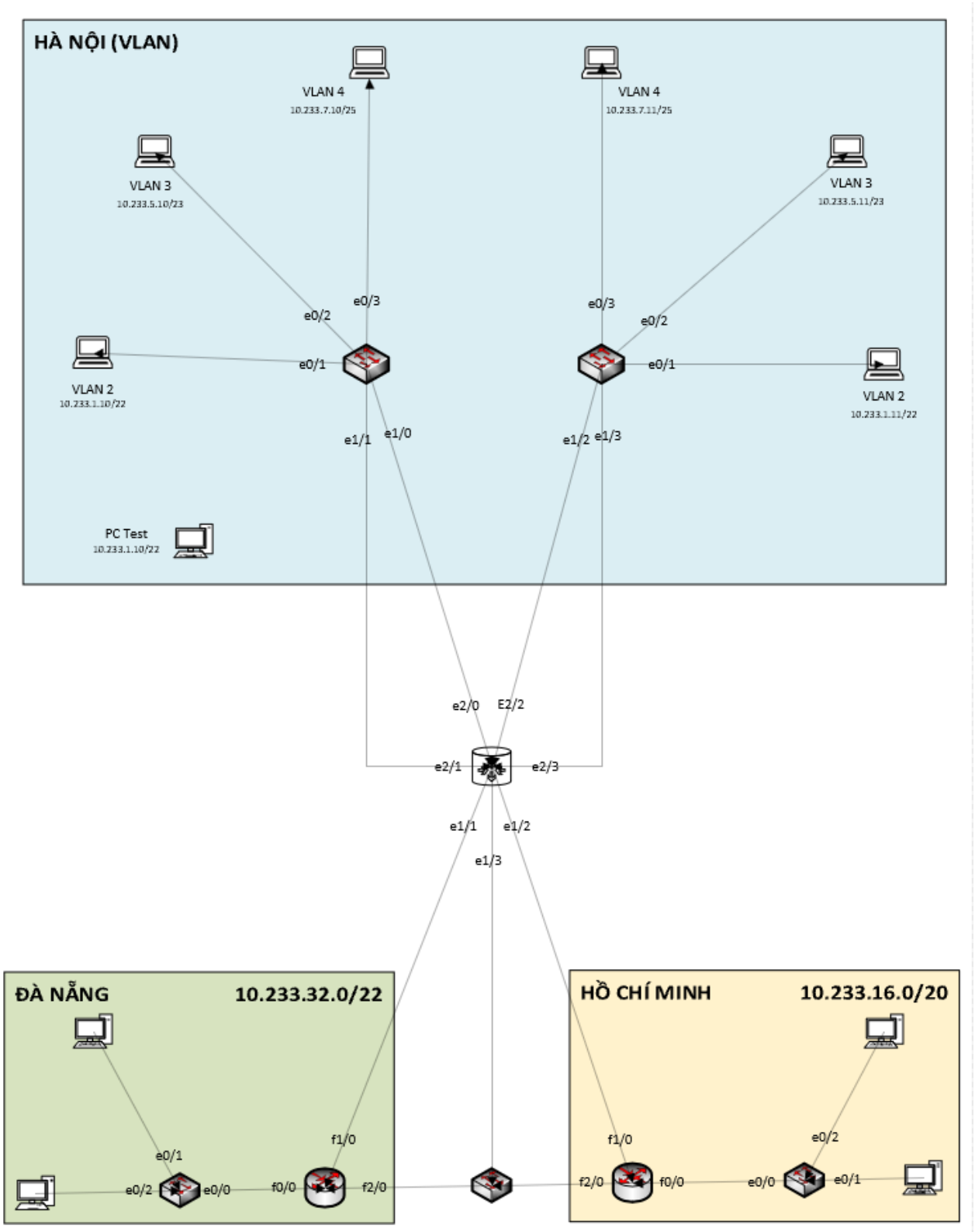
Mục lục

1. SƠ ĐỒ:


HÀ NỘI (VLAN)
VLAN 4
10.233.7.10/25
VLAN 4
10.233.7.11/25
VLAN 3
10.233.5.10/23
VLAN 3
10.233.5.11/23
VLAN 2
10.233.1.10/22
VLAN 2
10.233.1.11/22
PC Test
10.233.1.10/22
e0/2
e0/3
e0/1
e0/3
e0/2
e0/1
e1/1
e1/0
e1/2
e1/3
e2/0
E2/2
e2/1
e2/3
e1/1
e1/2
e1/3
ĐÀ NẴNG
10.233.32.0/22
HỒ CHÍ MINH
10.233.16.0/20
e0/1
e0/2
e0/0
f0/0
f1/0
f2/0
f1/0
f2/0
f0/0
e0/2
e0/0
e0/1

2. CHIA SUBNET:

2.1 Mạng cho từng khu vực:

- Hà Nội 4000 hosts: 10.233.0.0/20
- Hồ Chí Minh 3000 hosts: 10.233.16.0/20
- Đà Nẵng 1000 hosts: 10.233.32.0/22

2.2 Mạng cho Vlan trong khu vực Hà Nội:

- VLAN 2: 10.233.1.0/22 255.255.252.0
- VLAN 3: 10.233.5.0/23 255.255.254.0
- VLAN 4: 10.233.7.0/25 255.255.255.128
- VLAN 5: 10.233.8.0/28 255.255.255.240

3. CẤU HÌNH VTP VÀ VLAN:

3.1 Yêu cầu:

- Cấu hình VTP cho các SW, SV1, SV2.
- Cấu hình Vlan 2,3,4 và gắn ip cho các Vlan.
- Cấu hình đường trunk để các Vlan nhìn thấy nhau.
- Gắn ip cho các PC và kiểm tra ping đảm bảo các Vlan nhìn thấy nhau.

3.2 Cấu hình:

- Cấu hình vtp với domain là sv1.com.vn, Vlan và đường trunk:

SW

```
vtp mode server
vtp domain sv1.com.vn
vtp password abc
vlan 2
ex
vlan 3
ex
vlan 4
ex
int e0/1
switchport trunk encapsulation dot1q
switchport mode trunk
no shut
exit
int e0/2
switchport trunk encapsulation dot1q
switchport mode trunk
no shut
exit
int vlan 2
ip address 10.233.1.1 255.255.252.0
no shut
ex
int vlan 3
ip address 10.233.5.1 255.255.254.0
no shut
ex
int vlan 4
ip address 10.233.7.1 255.255.255.128
no shut
ex
```

SV1

```
vtp mode client
vtp domain sv1.com.vn
vtp password abc
int e0/1
switchport mode access
switchport access vlan 2
ex
int e0/2
switchport mode access
switchport access vlan 3
ex
int e0/3
switchport mode access
switchport access vlan 4
ex
int e0/0
sw
switchport mode trunk
exit
```

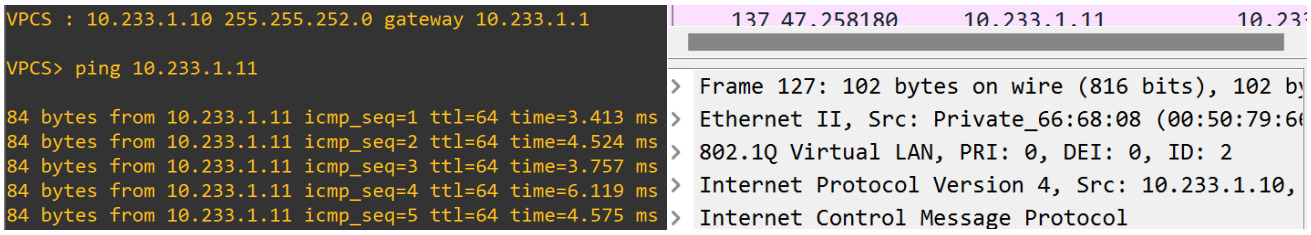
SV1

```
vtp mode client
vtp domain sv1.com.vn
vtp password abc
int e0/1
switchport mode access
switchport access vlan 2
ex
int e0/2
switchport mode access
switchport access vlan 3
ex
int e0/3
switchport mode access
switchport access vlan 4
ex
int e0/0
switchport trunk encapsulation dot1q
switchport mode trunk
exit
```

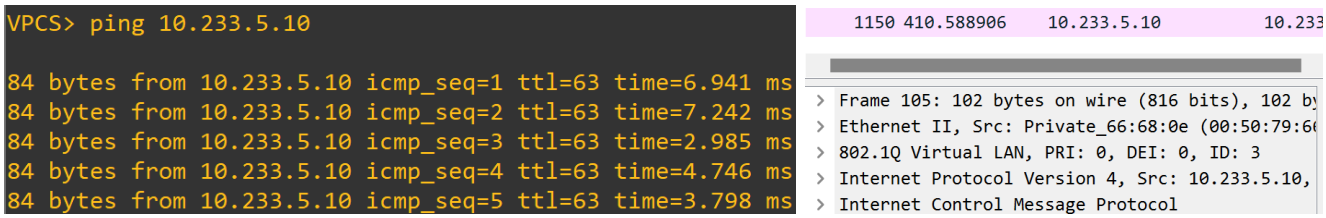
- Gắn ip cho các PC (tượng trưng cho các Vlan):

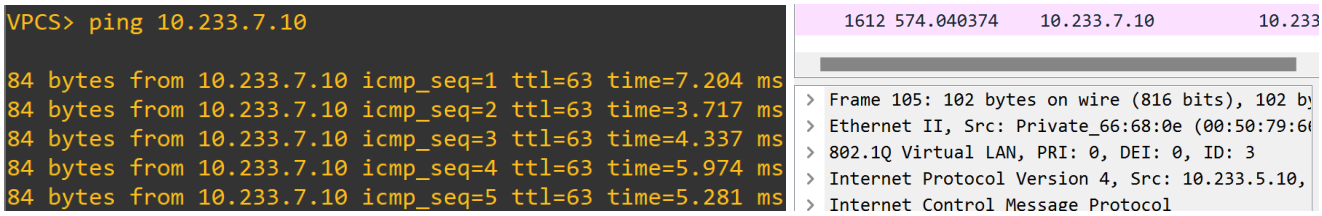
-VPC2: 10.233.1.10/22.	-PC_2: 10.233.1.11/22.
-VPC3: 10.233.5.10/23.	-PC_3: 10.233.5.11/23.
-VPC4: 10.233.7.10/25.	-PC_4: 10.233.7.11/25.

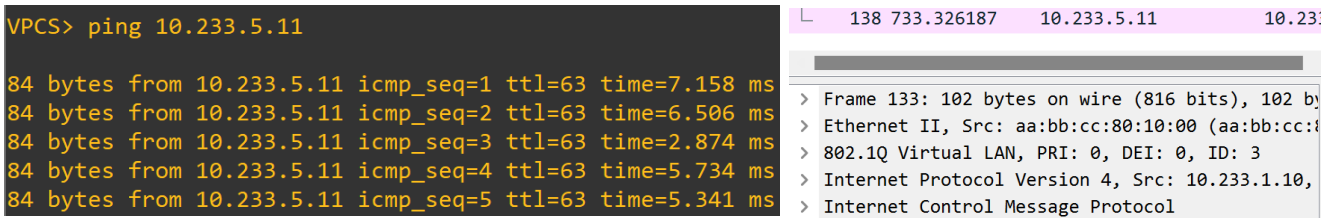
- Kiểm tra ping từ Vlan 2 tới Vlan 2 (Các Vlan khác tương tự):



- Kiểm tra ping từ Vlan 2 tới các Vlan khác:







* Lưu ý: kiểm tra gói ping bằng wireshark để biết được gói tin đó là của Vlan hay chỉ là gói tin thông thường. Nếu ta thấy gói ping có kèm 802.1Q thì là đúng.

4. CẤU HÌNH OSPF:

4.1 Yêu cầu:

- Gán ip cho các cổng
- Cấu hình 3 đường đi cho các router

4.2 Cấu hình:

- Gắn cổng:

SW

```
int e1/1
ip add 10.233.36.1 255.255.252.248
no shut
exit
int e1/2
ip add 10.233.36.9 255.255.252.248
no shut
exit
int e1/3
ip add 10.233.36.17 255.255.252.248
no shut
exit int loop0
ip add 1.1.1.1 255.255.255.255
ex
ip routing
```

R1

```
int f0/0
ip add 10.233.32.1 255.255.252.0
no shut
exit
int f1/0
ip add 10.233.36.2 255.255.255.248
no shut
exit
int f2/0
ip add 10.233.36.19 255.255.255.248
no shut
exit
```

R2

```
int f0/0
ip add 10.233.16.1 255.255.240.0
no shut
exit
int f2/0
ip add 10.233.36.10 255.255.255.248
no shut
exit
int f1/0
ip add 10.233.36.18 255.255.255.248
no shut
exit
```

- Cấu hình OSPF:

SW

router ospf 1

network 1.1.1.1 0.0.0.0 area 0

network 10.233.0.0 255.255.240.0 area 0

network 10.233.36.0 255.255.255.248 area 0

network 10.233.36.8 255.255.255.248 area 0

network 10.233.36.16 255.255.255.248 area 0

R1

router ospf 1

network 2.2.2.2 255.255.255.255 area 0

network 10.233.32.0 255.255.255.0 area 0

network 10.233.36.0 255.255.255.248 area 0

network 10.233.36.16 255.255.255.248 area 0

R2

router ospf 1

network 3.3.3.3 255.255.255.255 area 0

network 10.233.16.0 255.255.240.0 area 0

network 10.233.36.8 255.255.255.248 area 0

network 10.233.36.16 255.255.255.248 area 0

SV1

router ospf 1

network 10.233.8.0 255.255.255.240 area 0

network 10.233.1.0 255.255.252.0 area 0

network 10.233.5.0 255.255.254.0 area 0

network 10.233.7.0 255.255.255.128 area 0

SV2

router ospf 1

network 10.233.0.0 0.0.3.255 area 0

network 10.233.4.0 0.0.1.255 area 0

network 10.233.7.0 0.0.0.127 area 0

S2

router ospf 1

network 10.233.32.0 255.255.252.0 area 0

S4

router ospf 1

network 10.233.36.16 255.255.255.248 area 0

S3

router ospf 1

network 10.233.16.0 255.255.240.0 area 0

4.2 Kiểm tra:

- Mượn PC Vlan 4 ping đến PC của HCM và Đà Nẵng:

```
VPCS> show ip

NAME        : VPCS[1]
IP/MASK     : 10.233.7.10/25
GATEWAY     : 10.233.7.1
DNS         :
MAC         : 00:50:79:66:68:10
LPORT       : 20000
RHOST:PORT  : 127.0.0.1:30000
MTU         : 1500

VPCS> trace 10.233.32.10
trace to 10.233.32.10, 8 hops max, press Ctrl+C to stop
 1   10.233.7.1   1.825 ms  1.082 ms  0.775 ms
 2   10.233.36.2   18.994 ms  17.474 ms  15.825 ms
 3   *10.233.32.10   34.582 ms (ICMP type:3, code:3, Destination port unreachabl
e)

VPCS> trace 10.233.16.10
trace to 10.233.16.10, 8 hops max, press Ctrl+C to stop
 1   10.233.7.1   1.531 ms  3.407 ms  1.935 ms
 2   10.233.36.10   36.915 ms  12.308 ms  30.591 ms
 3   *10.233.16.10   66.208 ms (ICMP type:3, code:3, Destination port unreachabl
e)
```

* Kết quả: gói tin đi theo đường ngắn nhất, cũng là đường chính.

- Shut down đường chính (cổng e1/1 của SW), sau đó ping lại thử vào Đà Nẵng:

```
VPCS> trace 10.233.32.10
trace to 10.233.32.10, 8 hops max, press Ctrl+C to stop
 1   10.233.7.1   4.382 ms  2.146 ms  1.625 ms
 2   10.233.36.10   16.818 ms  13.801 ms  10.637 ms
 3   10.233.36.19   48.810 ms  25.948 ms  24.808 ms
 4   *10.233.32.10   58.288 ms (ICMP type:3, code:3, Destination port unreachabl
e)
```

*Kết quả: gói tin sẽ đi đường thứ 2.

- Shut down luôn đường thứ 2 (cổng e1/2 của SW), sau đó ping lại thử vào Đà Nẵng:

```
VPCS> trace 10.233.32.10
trace to 10.233.32.10, 8 hops max, press Ctrl+C to stop
 1   10.233.7.1   1.649 ms  4.328 ms  1.636 ms
 2   10.233.36.19   13.663 ms  11.413 ms  14.938 ms
 3   *10.233.32.10   37.158 ms (ICMP type:3, code:3, Destination port unreachabl
e)
```

*Kết quả: gói tin sẽ đi đường thứ 3.

5. CẤU HÌNH PORT SECURITY:

5.1 Yêu cầu:

- Cấu hình Port Security trên các cổng nối với Vlan

- Kiểm tra ping, đảm bảo chỉ có PC được cấu hình Port Security tại cổng đó ping được tới các Vlan khác và khi thay PC đó bằng 1 PC khác thì cổng bị shutdown.

5.2 Cấu hình:

SV1

```
int range e0/1-3
switchport host
switchport port-security
ex
int e0/1
switchport port-security maximum 1
switchport port-security mac-address
00:50:79:66:68:08
ex
int e0/2
switchport port-security maximum 1
switchport port-security mac-address
00:50:79:66:68:0e
ex
int e0/3
switchport port-security maximum 1
switchport port-security mac-address
00:50:79:66:68:10
ex
do show run
```

SV2

```
int range e0/1-3
switchport host
switchport port-security
ex
int e0/1
switchport port-security maximum 1
switchport port-security mac-address
00:50:79:66:68:12
ex
int e0/2
switchport port-security maximum 1
switchport port-security mac-address
00:50:79:66:68:0f
ex
int e0/3
switchport port-security maximum 1
switchport port-security mac-address
00:50:79:66:68:11
ex
do show run
```

5.3 Kiểm tra:

-Kiểm tra cấu hình Port Security ở cổng e0/1:

```
interface Ethernet0/1
 switchport access vlan 2
 switchport mode access
 switchport port-security mac-address 0050.7966.6808
 switchport port-security
 spanning-tree portfast edge
!
```

-Tháo PC ở cổng e0/1 (hiện là VLAN 2), ghép vào bằng 1 PC khác và thử ping các mạng khác, nó sẽ bị chặn bởi vì địa chỉ MAC khác với cấu hình:

```
VPCS> sho ip

NAME        : VPCS[1]
IP/MASK     : 10.233.1.10/22
GATEWAY     : 10.233.1.1
DNS         :
MAC         : 00:50:79:66:68:13
LPORT       : 20000
RHOST:PORT  : 127.0.0.1:30000
MTU         : 1500

VPCS> ping 10.233.7.11

host (10.233.1.1) not reachable

VPCS> ping 10.233.1.11

host (10.233.1.11) not reachable

VPCS> ping 10.233.32.10

host (10.233.1.1) not reachable

VPCS> ping 10.233.16.10

host (10.233.1.1) not reachable
```

-Gắn lại VPC2 cũ vào và ping lại (Lưu ý: phải vào switch SV1 mở cổng e0/1 lên, bởi vì khi bị port security chặn thì cổng sẽ tự động đóng lại:

```
VPCS> show ip

NAME        : VPCS[1]
IP/MASK     : 10.233.1.10/22
GATEWAY     : 10.233.1.1
DNS         :
MAC         : 00:50:79:66:68:08
LPORT       : 20000
RHOST:PORT  : 127.0.0.1:30000
MTU         : 1500

VPCS> ping 10.233.5.11

84 bytes from 10.233.5.11 icmp_seq=1 ttl=63 time=3.693 ms
84 bytes from 10.233.5.11 icmp_seq=2 ttl=63 time=4.157 ms
84 bytes from 10.233.5.11 icmp_seq=3 ttl=63 time=4.190 ms
84 bytes from 10.233.5.11 icmp_seq=4 ttl=63 time=3.545 ms
84 bytes from 10.233.5.11 icmp_seq=5 ttl=63 time=4.384 ms

VPCS> ping 10.233.32.10

84 bytes from 10.233.32.10 icmp_seq=1 ttl=62 time=28.620 ms
84 bytes from 10.233.32.10 icmp_seq=2 ttl=62 time=15.608 ms
84 bytes from 10.233.32.10 icmp_seq=3 ttl=62 time=20.767 ms
84 bytes from 10.233.32.10 icmp_seq=4 ttl=62 time=18.857 ms
84 bytes from 10.233.32.10 icmp_seq=5 ttl=62 time=17.199 ms
```

*Kết quả: VLAN nhận địa chỉ IP và ping được bình thường.

6. CẤU HÌNH ETHERCHANNEL:

6.1 Yêu cầu:

- Cấu hình etherchannel chế độ lacp, 1 đường từ SV1 đến SW và 1 đường từ SW đến SV2.

- Kiểm tra 2 port channel và đảm bảo các Port-channel được build(P) và ở chế độ inuse(SU).

6.2 Cấu hình:

SV1
```
int range e1/0-1
switchport trunk encapsulation dot1q
switchport mode trunk
channel-protocol lacp
channel-group 1 mode active
no shut
exit
port-channel load-balance src-dst-mac
```

SV1
```
int range e1/0-1
switchport trunk encapsulation dot1q
switchport mode trunk
channel-protocol lacp
channel-group 1 mode active
no shut
exit
port-channel load-balance src-dst-mac
```

SW
```
int range e2/0-1
switchport trunk encapsulation dot1q
switchport mode trunk
channel-protocol lacp
channel-group 1 mode active
no shut
exit
port-channel load-balance src-dst-mac
int range e2/2-3
switchport trunk encapsulation dot1q
switchport mode trunk
channel-protocol lacp
channel-group 2 mode active
no shut
exit
port-channel load-balance src-dst-mac
do show etherchannel sum
```

6.3 Kiểm tra:

- Kiểm tra port-channel:

SV1:

```
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Et1/0(P)    Et1/1(P)
```

SW:

```
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Et2/0(P)    Et2/1(P)
2      Po2(SU)         LACP      Et2/2(P)    Et2/3(P)
```

SV2:

```
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
2      Po2(SU)         LACP      Et1/2(P)    Et1/3(P)
```

7. CẤU HÌNH SSH:

7.1 Yêu cầu:

- Cấu hình các router và switch cho phép các máy SSH tới.

- Tạo Vlan 5, cấu hình ACL chỉ cho phép Vlan 5 được phép SSH tới các Router và Switch đó.

- Kiểm tra SSH

7.2 Cấu hình:

- Tạo Vlan 5 và cấu hình ssh trên các Router và Switch:

SW

```
vtp mode server
vtp domain sv1.com.vn
vtp password abc

ip domain-name cisco.com
username vy secret cisco123
crypto key generate rsa modulus 1024
line vty 0 4
login local
transport input ssh
exit
ip ssh version 2
vlan 5
ex
int vlan 5
ip address 10.233.8.1 255.255.255.240
no shut
ex
enable secret adminpass
```

SV1

```
vtp mode client
vtp domain sv1.com.vn
vtp password abc
ip default-gateway 10.233.8.1
int e1/3
switchport mode access
switchport access vlan 5
ex
int vlan 5
ip add 10.233.8.2 255.255.255.240
no shut
ex
ip domain-name cisco.com
username hieu secret cisco
crypto key generate rsa modulus 1024
line vty 0 4
login local
transport input ssh
exit
ip ssh version 2
enable secret adminpass
```

SV2

```
vtp mode client
vtp domain sv1.com.vn
vtp password abc
ip default-gateway 10.233.8.1
int vlan 5
ip add 10.233.8.3 255.255.255.240
no shut
ex
ip domain-name cisco.com
username huy secret cisco
crypto key generate rsa modulus 1024
line vty 0 4
login local
transport input ssh
exit
ip ssh version 2
enable password adminpass
```

R2

```
ip domain-name cisco.com
username r2ma secret cisco
crypto key generate rsa modulus 1024
line vty 0 4
login local
transport input ssh
exit
ip ssh version 2
enable password adminpass
```

R3

```
ip domain-name cisco.com
username r3ma secret cisco
crypto key generate rsa modulus 1024
line vty 0 4
login local
transport input ssh
exit
ip ssh version 2
enable password adminpass
```

S2

```
int vlan 1
ip add 10.233.32.2 255.255.252.0
no shut
ex
ip domain-name cisco.com
username s2ma secret cisco
crypto key generate rsa modulus 1024
line vty 0 4
login local
transport input ssh
exit
ip ssh version 2
enable password adminpass
```

S4

```
int vlan 1
ip add 10.233.36.21 255.255.255.248
no shut
ex
ip domain-name cisco.com
username s4ma secret cisco
crypto key generate rsa modulus 1024
line vty 0 4
login local
transport input ssh
exit
ip ssh version 2
enable password adminpass
```

S3

```
int vlan 1
ip add 10.233.16.2 255.255.240.0
no shut
ex
ip domain-name cisco.com
username s3ma secret cisco
crypto key generate rsa modulus 1024
line vty 0 4
login local
transport input ssh
exit
ip ssh version 2
enable password adminpass
```

- Cấu hình ACL:

SW
```
ip access-list extended SSH-ACL-VLAN5
permit icmp any any
permit tcp 10.233.8.0 0.0.0.15 any eq 22
deny ip any any log
ex
line vty 0 4
access-class SSH-ACL-VLAN5 in
```

R2
```
ip access-list extended SSH-ACL-VLAN5
permit icmp any any
permit tcp 10.233.8.0 0.0.0.15 any eq 22
deny ip any any log
ex
line vty 0 4
access-class SSH-ACL-VLAN5 in
```

SV1
```
ip access-list extended SSH-ACL-VLAN5
permit icmp any any
permit tcp 10.233.8.0 0.0.0.15 any eq 22
deny ip any any log
ex
line vty 0 4
access-class SSH-ACL-VLAN5 in
```

R3
```
ip access-list extended SSH-ACL-VLAN5
permit icmp any any
permit tcp 10.233.8.0 0.0.0.15 any eq 22
deny ip any any log
ex
line vty 0 4
access-class SSH-ACL-VLAN5 in
```

SV2
```
ip access-list extended SSH-ACL-VLAN5
permit icmp any any
permit tcp 10.233.8.0 0.0.0.15 any eq 22
deny ip any any log
ex
line vty 0 4
access-class SSH-ACL-VLAN5 in
```

S2
```
ip access-list extended SSH-ACL-VLAN5
permit icmp any any
permit tcp 10.233.8.0 0.0.0.15 any eq 22
deny ip any any log
ex
line vty 0 4
access-class SSH-ACL-VLAN5 in
```

S4
```
ip access-list extended SSH-ACL-VLAN5
permit icmp any any
permit tcp 10.233.8.0 0.0.0.15 any eq 22
deny ip any any log
ex
line vty 0 4
access-class SSH-ACL-VLAN5 in
```

S3
```
ip access-list extended SSH-ACL-VLAN5
permit icmp any any
permit tcp 10.233.8.0 0.0.0.15 any eq 22
deny ip any any log
ex
line vty 0 4
access-class SSH-ACL-VLAN5 in
```

7.3 Kiểm tra:

- Dùng thiết bị thuộc Vlan 5 để ssh tới:

```
Switch#ssh -l vy 10.233.8.1
Password:

Password:

SW>en
Password:
SW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW(config)#
```

*Kết quả: SSH tới được.

- Dùng thiết bị khác thuộc Vlan khác (ở đây là Vlan 2):

```
SSH_test#
*Dec  5 07:28:18.355: %SYS-5-CONFIG_I: Configured from console by console
SSH_test#ssh -l vy 10.233.8.1
% Connection refused by remote host

SSH_test#
```

*Kết quả: % Connection refused by remote host

- Những thiết bị khác tương tự. Thử SSH tới R2:

```
Switch#ssh -l r2ma 10.233.36.2
Password:

Password:

R2>en
Password:
R2#
```

*Kết quả: thành công.

- Cũng như vậy, sử dụng thiết bị thuộc Vlan 2 SSH tới:

```
SSH_test#ssh -l r2ma 10.233.36.2
% Connection refused by remote host

SSH_test#
```

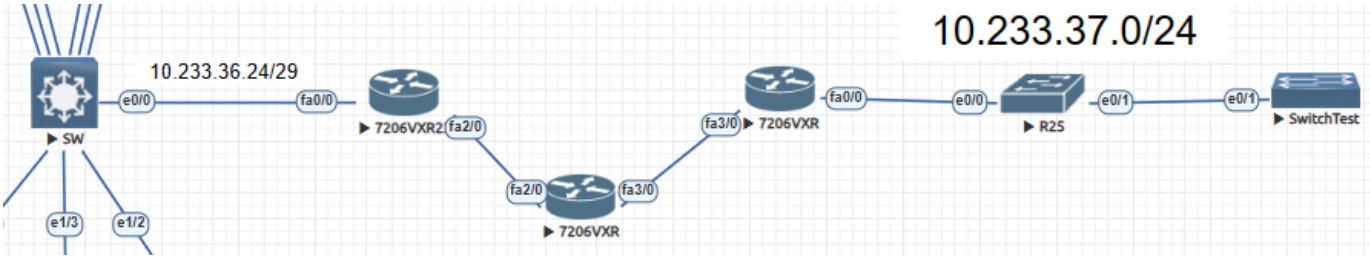
*Kết quả: Không SSH tới được.

8. CẤU HÌNH VPN SITE TO SITE:

8.1 Yêu cầu:

- Cấu hình VPN site to site giữa 2 router.

8.2 Sơ đồ:



8.3 Cấu hình:

- Gắn cổng và cấu hình đường đi cho các thiết bị:

R4

```
int f2/0
ip add 10.233.36.33 255.255.255.248
no shut
ex
int loop0
ip add 4.4.4.4 255.255.255.255
no shut
ex
router ospf 1
network 10.233.36.32 255.255.255.248
area 0
network 4.4.4.4 0.0.0.0 area 0
ex
ip route 10.233.36.40 255.255.255.248
10.233.36.34
```

R5

```
int f3/0
ip add 10.233.36.41 255.255.255.248
no shut
ex
int loop0
ip add 5.5.5.5 255.255.255.255
no shut
ex
router ospf 1
network 5.5.5.5 0.0.0.0 area 0
network 10.233.36.40 255.255.255.248
area 0
ex
ip route 10.233.36.32 255.255.255.248
10.233.36.42
```

R6

```
int f2/0
ip add 10.233.36.34 255.255.255.248
no shut
ex
int f3/0
ip add 10.233.36.42 255.255.255.248
no shut
ex
int loop0
ip add 6.6.6.6 255.255.255.255
no shut
ex
router ospf 1
network 6.6.6.6 255.255.255.255 area 0
network 10.233.36.32 255.255.255.248
area 0
network 10.233.36.40 255.255.255.248
area 0
ex
```

SW

```
int e0/0
no switchport
ip add 10.233.36.25 255.255.255.248
no shut
ex
router ospf 1
network 10.233.36.24 0.0.0.7 area 0
ex
```

- Cấu hình VPN:

R4

```
crypto isakmp policy 1
authentication pre-share
hash sha
group 5
exit

crypto isakmp key vydeptrai address
10.233.36.41

crypto ipsec transform-set CONR5 esp-
des esp-md5-hmac

access-list 101 permit ip any any

crypto map MAPR5 1 ipsec-isakmp
set peer 10.233.36.41
set transform-set CONR5
set pfs group5
match address 101

interface f2/0
crypto map MAPR5
```

R5

```
crypto isakmp policy 1
authentication pre-share
hash sha
group 5
exit

crypto isakmp key vydeptrai address
10.233.36.33

crypto ipsec transform-set CONR5 esp-
des esp-md5-hmac

access-list 101 permit ip any any

crypto map MAPR5 1 ipsec-isakmp
set peer 10.233.36.33
set transform-set CONR5
set pfs group5
match address 101

interface f3/0
crypto map MAPR5
```

8.4 Kiểm tra:

- Kiểm tra VPN bên router R4:

```
R4(config-if)#do show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.233.36.41    10.233.36.33    QM_IDLE           1001 ACTIVE
10.233.36.33    10.233.36.41    QM_IDLE           1002 ACTIVE
```

- Kiểm tra VPN bên router R5:

```
R5(config-if)#do show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.233.36.41    10.233.36.33    QM_IDLE           1001 ACTIVE
10.233.36.33    10.233.36.41    QM_IDLE           1002 ACTIVE
```

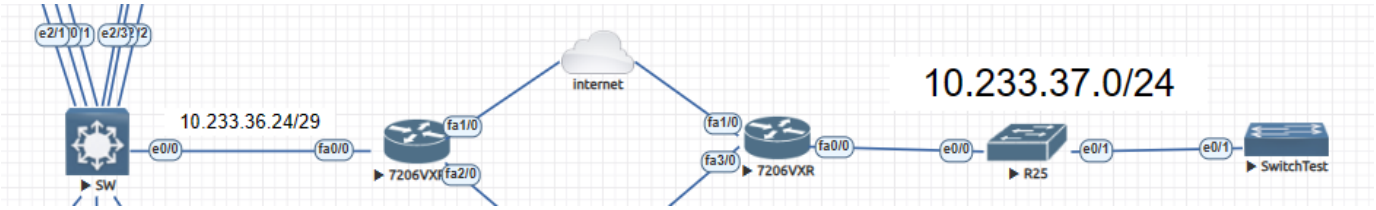
- Kiểm tra ping giữa 2 router:

```
R4(config)#do ping 10.233.36.41
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.233.36.41, timeout is 2 seconds:
!!!!!
```

```
R5(config)#do ping 10.233.36.33
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.233.36.33, timeout is 2 seconds:
!!!!!
```

9. CẤU HÌNH NAT PORT FORWARDING:

9.1 Sơ đồ:



9.2 Yêu cầu:

- Gắn ip cho cổng và cấu hình OSPF.

- Cấu hình Nat port sao cho từ SW có ip thuộc mạng 10.233.36.24/29, khi đi ra khỏi R4 và ra ngoài internet thì nat port thành mạng 200.0.0.0/24 và ngược lại.

- Kiểm tra ping.

9.3 Cấu hình:

SW

```
int e0/0
no switchport
ip add 10.233.36.25 255.255.255.248
no shut
ex
router ospf 1
network 10.233.36.24 255.255.255.248
area 0
ex
ip route 10.233.37.0 255.255.255.0
200.0.0.11
```

R4

```
int f0/0
ip address 10.233.36.26 255.255.255.248
no shut
ip nat inside
ex
int f1/0
ip add 200.0.0.10 255.255.255.0
no shut
ip nat outside
ex
ip route 0.0.0.0 0.0.0.0 200.0.0.1
ip route 10.233.37.0 255.255.255.0
200.0.0.11
ip nat inside source static 10.233.36.25
int f1/0
router ospf 1
network 10.233.36.24 255.255.255.248
area 0
network 200.0.0.0 255.255.255.0 area 0
ex
```

R5

```
int f0/0
ip add 10.233.37.1 255.255.255.0
no shut
ip nat inside
ex
int f1/0
ip add 200.0.0.11 255.255.255.0
no shut
ip nat outside
ex
ip route 0.0.0.0 0.0.0.0 200.0.0.1
ip route 10.233.36.24 255.255.255.248
200.0.0.10
ip nat inside source static 10.233.37.10
int f1/0
router ospf 1
network 10.233.37.0 255.255.255.0 area
0
network 200.0.0.0 255.255.255.0 area 0
ex
```

9.3 Kiểm tra:

- Kiểm tra cấu hình:

```
R4(config)#do show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
ospf 200.0.0.10:0      10.233.36.25:0     200.0.0.11:0       200.0.0.11:0
--- 200.0.0.10         10.233.36.25       ---                ---
```

```
R5(config)#do show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
ospf 200.0.0.11:0      10.233.37.10:0     200.0.0.10:0       200.0.0.10:0
--- 200.0.0.11         10.233.37.10       ---                ---
```

- Kiểm tra ping:

```
SW#ping 10.233.37.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.233.37.10, timeout is 2 seconds:
!!!!!
```

```
R4(config)#do show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
ospf 200.0.0.10:0      10.233.36.25:0     200.0.0.11:0       200.0.0.11:0
udp 200.0.0.10:32991   10.233.36.25:32991 10.233.37.10:33437 10.233.37.10:33437
udp 200.0.0.10:32991   10.233.36.25:32991 200.0.0.11:33437   200.0.0.11:33437
udp 200.0.0.10:33002   10.233.36.25:33002 10.233.37.10:33438 10.233.37.10:33438
udp 200.0.0.10:33002   10.233.36.25:33002 200.0.0.11:33438   200.0.0.11:33438
udp 200.0.0.10:33394   10.233.36.25:33394 10.233.37.10:33440 10.233.37.10:33440
udp 200.0.0.10:33394   10.233.36.25:33394 200.0.0.11:33440   200.0.0.11:33440
udp 200.0.0.10:33440   10.233.36.25:33440 200.0.0.11:38067   200.0.0.11:38067
udp 200.0.0.10:33441   10.233.36.25:33441 200.0.0.11:33401   200.0.0.11:33401
udp 200.0.0.10:34237   10.233.36.25:34237 10.233.37.10:33441 10.233.37.10:33441
udp 200.0.0.10:34237   10.233.36.25:34237 200.0.0.11:33441   200.0.0.11:33441
udp 200.0.0.10:34907   10.233.36.25:34907 10.233.37.10:33440 10.233.37.10:33440
udp 200.0.0.10:34907   10.233.36.25:34907 200.0.0.11:33440   200.0.0.11:33440
udp 200.0.0.10:35261   10.233.36.25:35261 10.233.37.10:33442 10.233.37.10:33442
```

```
Switch#ping 10.233.36.25
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.233.36.25, timeout is 2 seconds:
!!!!!
```

```
R5(config)#do show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 200.0.0.11:0      10.233.37.10:0     10.233.36.25:0     10.233.36.25:0
ospf 200.0.0.11:0      10.233.37.10:0     200.0.0.10:0       200.0.0.10:0
udp 200.0.0.11:33401   10.233.37.10:33401 10.233.36.25:33441 10.233.36.25:33441
udp 200.0.0.11:33401   10.233.37.10:33401 200.0.0.10:33441   200.0.0.10:33441
udp 200.0.0.11:33440   10.233.37.10:33440 200.0.0.10:33394   200.0.0.10:33394
udp 200.0.0.11:33440   10.233.37.10:33440 200.0.0.10:34907   200.0.0.10:34907
udp 200.0.0.11:33441   10.233.37.10:33441 200.0.0.10:34237   200.0.0.10:34237
udp 200.0.0.11:33441   10.233.37.10:33441 200.0.0.10:35535   200.0.0.10:35535
```

----------Hết----------