

第1題: 192.168.0.1, 192.168.5.1 不能變更

192.168.4.254 變成 192.168.5.254

VPC2

```
# ip 192.168.0.1 255.255.255.0 192.168.0.254
```

R1

```
# int e0/0
```

```
# ip addr 192.168.0.254 255.255.255.0
```

```
# no shut
```

```
# int e0/1
```

```
# ip addr 192.168.4.254 255.255.255.0
```

```
# no shut
```

```
# do sh ip int br
```

VPC3

```
# ip 192.168.5.1 255.255.255.0 192.168.4.254 不能這樣設定
```

```
# ip 192.168.5.1 255.255.255.0 192.168.5.254
```

R1

```
# int e0/1
```

```
# no ip addr 192.168.4.254 255.255.255.0
```

```
# ip addr 192.168.5.254 255.255.255.0
```

```
# no shut
```

第2題: 全部都不能變更 超周化 網路合併

VPC2

```
# ip 192.168.0.1 255.255.255.0 192.168.0.254
```

192.168.4.254 和 192.168.5.1

放在同一個網域

R1

```
# int e0/0
```

```
# ip addr 192.168.0.254 255.255.255.0
```

```
# no shut
```

```
# int e0/1
```

```
# ip addr 192.168.4.254 255.255.255.0
```

```
# no shut
```

```
# do sh ip int br
```

VPC3

```
# ip 192.168.5.1 255.255.254.0 192.168.4.254
```

..

```
#1  
# int eth0  
# no ip addr 192.168.4.254 255.255.255.0  
# ip addr 192.168.4.254 255.255.254.
```

為了練攻防所創造出來的實驗環境

kali - vulnhub

CTF: Capture the flag

規則

kali DC-1 → kali

找 kali ip

nmap -sP 192.168.159.0/24 緯路

找路子 - 找 port 是開啟  
# nmap -A 192.168.159.164 → kali ip

第三層 OSPF

## VLAN: 第二層的技術

目的: 希望把網路再細分

一台交換機預設處在整個區域網路下

結果: 當節點越來越多, 競爭的機會, 就會影響效能, 慢... , 安全性也較差

提高網路效能, 安全性, 就可以把網路細分

通常用在公司行號, 公司有許多部門, 可以根據部門分出不同區域網路

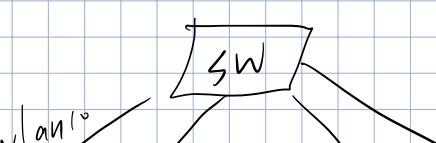
Test 1: 1台 L2-SW, 4台 VPC

VPC 1

> ip 192.168.1.1 255.255.256.0

VPC 2

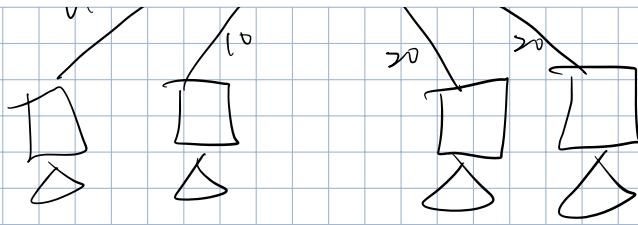
> ip 192.168.1.2 255.255.256.0



```

VPC3
> ip 192.168.1.3 255.255.255.0
VPC4
> ip 192.168.1.4 255.255.255.0
> ping 192.168.1.1
    1.2
    1.3

```



```

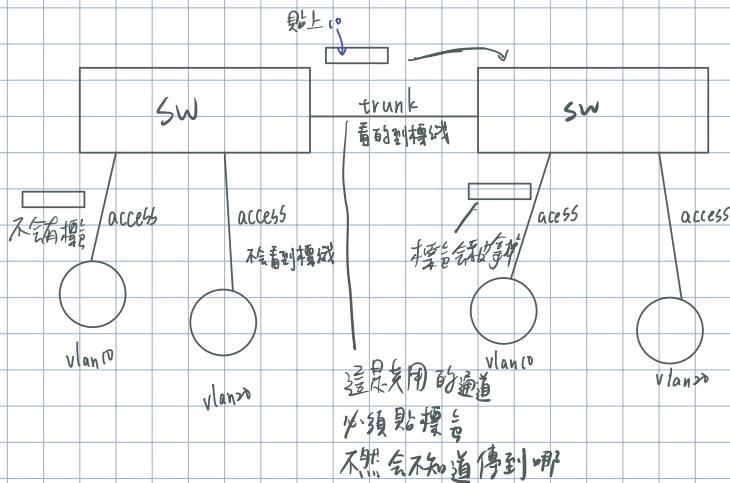
SW
# vlan 10
# name RD
# exit
# vlan 20
# name SALES
# exit
# do sh vlan br

```

```

# int e0/0
# switchport mode access
# switchport access vlan10
# int e0/1
# switchport mode access
# switchport access vlan10
# int e0/2
# switchport mode access
# switchport access vlan20
# int e0/3
# switchport mode access
# switchport access vlan20
# do sh vlan br

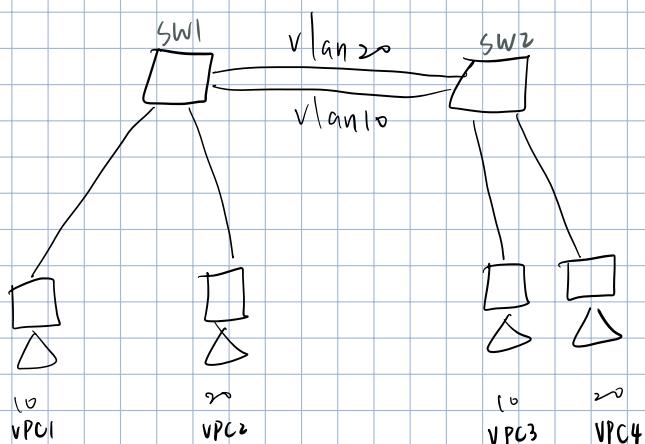
```



VPC1 ping VPC2.  
 1.2  
 VPC3,4

第二層子端口中連續為 trunk access

VPC3 ping VPC4  
 1.2  
 VPC1,2



缺點：有多步 VLAN 交換在 SW2 間導致  
 傷

```

VPC1
> ip 192.168.1.1 255.255.255.0
VPC2
> ip 192.168.1.2 255.255.255.0
VPC3
> ip 192.168.1.3 255.255.255.0
VPC4
> ip 192.168.1.4 255.255.255.0
> ping 192.168.1.1
    1.2   可以ping到
    1.3

```

<pre> SW1 # vlan 10 # name VLAN10 # exit # vlan 20 # name VLAN20 # exit </pre>	<pre> SW2 # vlan 10 # name VLAN10 # exit # vlan 20 # name VLAN20 # exit </pre>
<pre> # int range e0/0,e0/2  int range e0/0-2 # switchport mode access # switchport access VLAN10 # int range e0/1,e0/3 # switchport mode access # switchport access VLAN20 # do sh vlan br </pre>	<pre> # int range e0/0,e0/2 # switchport mode access # switchport access VLAN10 # int range e0/1,e0/3 # switchport mode access # switchport access VLAN20 # do sh vlan br </pre>

PC1 ping PC3  
no PC2.4

PC2 ping PC4  
no PC1.3

Access = 以太網端口

802.1q