NASA hw4

Author: B12705014陳泊華

Chapter1

1.

	可通過的VLAN數量	802.1Q
Access Port	1	無
Trunk Port	2^12=4096個，扣掉0和4095	有

*註：VLAN 0又稱為untagged VLAN，VLAN 4095又稱為reserved VLAN

reference:
(i) https://www.geeksforgeeks.org/difference-between-trunk-port-and-access-port/ (https://www.geeksforgeeks.org/difference-between-trunk-port-and-access-port/)
(ii) TA slides

2. Trunk native是指在設定trunk時可以指定VLAN作為Native VLAN（預設通常為1），若訊框符合該VLAN則不特別附加VLAN tag給該封包；要注意的是trunk兩邊設定的native VLAN通常要一致，才不會造成通訊失敗

reference:
(i) https://www.networkacademy.io/ccna/ethernet/trunk-native-vlan (https://www.networkacademy.io/ccna/ethernet/trunk-native-vlan)
(ii) chatGPT

3.

			封包			
			802.1Q VID 欄位			
傳遞方向	線路1	線路2	線路3	線路4	線路5	能否抵達
PC-01/VLAN 10 → PC-02	10	無				可
PC-01/VLAN 20 → PC-02	20	無				否
PC-01/VLAN 10 → PC-04	10		10		無	否
PC-01/VLAN 20 → PC-04	20		20		20	可
PC-01/VLAN 10 → PC-03	10			10		可
PC-01/VLAN 20 → PC-03	20			10		可

4. Double Tagging Attack是VLAN hopping的一種實現方式；以figure 4來說，若攻擊者（PC-01）使用的VLAN與Switch上所設定的Trunk native相同的話（在這裡是10），攻擊者就能在其封包資料中埋入VLAN 20的訓框，如此RiNG-edge在解讀時就會認為這是來自VLAN 20的封包並且傳到PC-04

   reference:
   (i) https://en.wikipedia.org/wiki/VLAN_hopping (https://en.wikipedia.org/wiki/VLAN_hopping)
   (ii) https://www.jannet.hk/virtual-lan-vlan-attack-zh-hant/ (https://www.jannet.hk/virtual-lan-vlan-attack-zh-hant/)

Chapter2

1.
(1) 將Laptop-PT Admin連到RiNG的console槽
(2) 觀察config檔，發現其使用IOS type 7加密，並且帳號為RiNG，於是利用線上解密軟體，獲得密碼Roselia，登入獲得權限。

reference:
(i) https://www.cisco.com/c/zh_tw/support/docs/security-vpn/remote-authentication-dial-user-service-radius/107614-64.html (https://www.cisco.com/c/zh_tw/support/docs/security-vpn/remote-authentication-dial-user-service-radius/107614-64.html)
(ii) https://www.youtube.com/watch?v=rjorz6S0rVE (https://www.youtube.com/watch?

v=rjorz6S0rVE)

(iii) https://www.xiaopeiqing.com/cisco-password-cracker/ (https://www.xiaopeiqing.com/cisco-password-cracker/)

(iv) https://zh.wikipedia.org/zh-tw/RS-232 (https://zh.wikipedia.org/zh-tw/RS-232)

2. 步驟：
   (1) 依照題目敘述設定vlan、更改名稱
   (2) 設定RiNG-core和RiNG-edge的trunk和link aggregation
   (3) 打開PC terminal ping對方測試

   reference: TA slides

3. a. 在configure terminal（全局配置模式）下執行：

```
$ no username RiNG password #否則會跳出can not have both a user passworc
$ username RiNG secret Afterglow
```

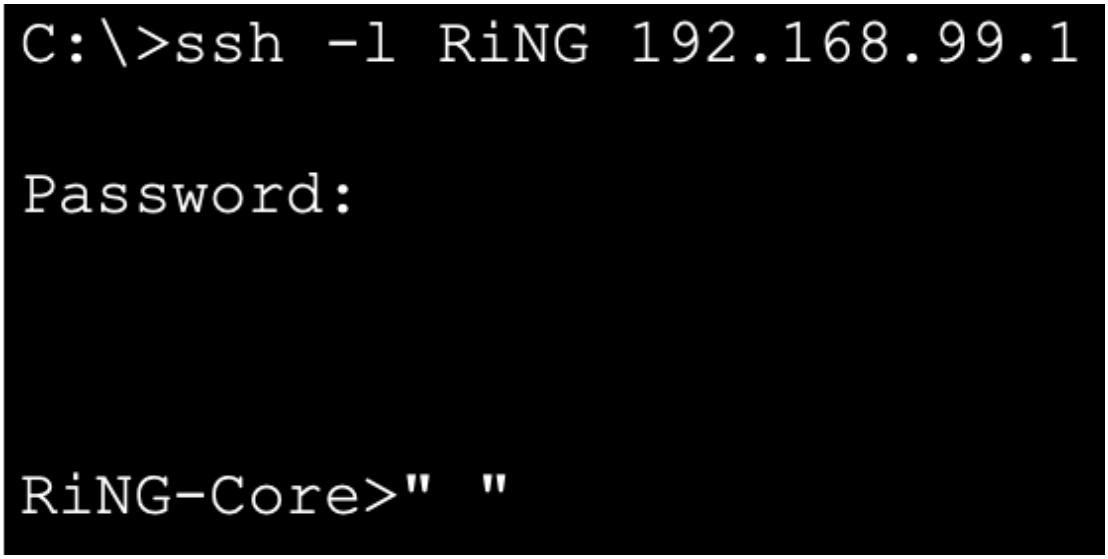
b&c.

```
$ line vty 0 4
$ transport input ssh
$ login local
$ password Afterglow
```

驗證方式：打開Laptop-PT Admin的command prompt，輸入

```
$ ssh -l RiNG 192.168.99.1
```

密碼輸入先前設定的Afterglow



d.

```
$ line vty 5 15
$ transport input none
```

e.

```
$ ip domain-name bowen.com
$ crypto key generate rsa general-keys``` #設定長度為768
```$ ip ssh version 2
```

reference:
(i) TA slides
(ii) chatGPT 3.0

```
interface Vlan1
 no ip address
 shutdown
!
interface Vlan99
 ip address 192.168.99.1 255.255.255.0
!
!
!
!
line con 0
 login local
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 no login
!
!
!
!
end
```
```

Chapter3

1.

先透過WiFi Settings -> details -> TCP/IP -> Renew DHCP lease來release租約

```
Discover: DHCP client透過discover message尋找DHCP server，在data link layer和

Offer: server收到client的discover message後回傳offer message，在network layer

Request: 由client端向server端傳送，表示準備好接收IP位址。

Acknowledge: DHCP server收到request message後回傳，包含IP位址和子網域遮罩給予cli
```

No.	Time	Source	Destination	Protocol	Length	Info
902	54.1981…	0.0.0.0	255.255.255.…	DHCP	342	DHCP Request - Transaction ID 0x956cdb59
1355	55.7907…	0.0.0.0	255.255.255.…	DHCP	342	DHCP Request - Transaction ID 0x956cdb59
1359	55.7965…	192.168.3.99	192.168.3.70	DHCP	342	DHCP ACK - Transaction ID 0x956cdb59
8301	232.329…	0.0.0.0	255.255.255.…	DHCP	342	DHCP Request - Transaction ID 0x956cdb5a
8305	232.341…	192.168.3.99	192.168.3.70	DHCP	342	DHCP ACK - Transaction ID 0x956cdb5a
9168	276.279…	192.168.3.70	192.168.3.99	DHCP	342	DHCP Release - Transaction ID 0x956cdb5b
9506	302.885…	0.0.0.0	255.255.255.…	DHCP	342	DHCP Discover - Transaction ID 0x3c0ef3d9
9514	303.926…	0.0.0.0	255.255.255.…	DHCP	342	DHCP Discover - Transaction ID 0x3c0ef3d9
9533	305.974…	192.168.3.99	192.168.3.70	DHCP	342	DHCP Offer - Transaction ID 0x3c0ef3d9
9534	305.974…	192.168.3.99	192.168.3.70	DHCP	342	DHCP Offer - Transaction ID 0x3c0ef3d9
9537	306.976…	0.0.0.0	255.255.255.…	DHCP	342	DHCP Request - Transaction ID 0x3c0ef3d9
9539	306.986…	192.168.3.99	192.168.3.70	DHCP	342	DHCP ACK - Transaction ID 0x3c0ef3d9

reference: https://www.geeksforgeeks.org/how-dora-works/

(https://www.geeksforgeeks.org/how-dora-works/)

2. DHCP封包內容：

```
> Frame 9506: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface en0, id 0
> Ethernet II, Src: Apple_02:19:f8 (b0:be:83:02:19:f8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x3c0ef3d9
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Apple_02:19:f8 (b0:be:83:02:19:f8)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (55) Parameter Request List
  > Option: (57) Maximum DHCP Message Size
  > Option: (61) Client identifier
  > Option: (51) IP Address Lease Time
  > Option: (12) Host Name
  > Option: (255) End
    Padding: 000000000000000000000000000000000000
```

在 DHCP Discover 階段填入這些特殊地址的原因是為了實現廣播機制，確保 DHCP Discover 發出的資訊能夠被網絡中的所有設備收到，並且在客戶端尚未分配到有效 IP 地址之前，確保其能夠與 DHCP 伺服器進行通信，從而獲取到所需的 IP 地址和其他配置信息。

	IP 0.0.0.0	**IP 255.255.255.255**	
涵義	表client端尚未有IP地址	IP的廣播地址	
原因	在 DHCP Discover 階段， 客戶端尚未獲得有效的 IP 地址，因此它的源端 IP 地址為 0.0.0.0， 表示客戶端需要獲取一個有效的 IP 地址。	在 DHCP Discover 階段， 客戶端需要向網絡中的所有設備廣播 DHCP Discover 報文， 以尋找可用的 DHCP 伺服器。	將目

reference: https://zh.wikipedia.org/zh-tw/保留IP地址 (https://zh.wikipedia.org/zh-tw/%E4%BF%9D%E7%95%99IP%E5%9C%B0%E5%9D%80)

3. 在 RiNG-Core 上配置 DHCP Snooping，檢測和阻止未經授權的DHCP伺服器（標記出可信任的接口）

```
$ ip dhcp snooping
$ interface FastEthernet 0/22
$ ip dhcp snooping trust
```

檢查：

```
$ show ip dhcp snooping
```

```
RiNG-Core#
%SYS-5-CONFIG_I: Configured from console by console
show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
none
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/1            no         unlimited
FastEthernet0/2            no         unlimited
FastEthernet0/3            no         unlimited
FastEthernet0/4            no         unlimited
FastEthernet0/5            no         unlimited
FastEthernet0/6            no         unlimited
FastEthernet0/7            no         unlimited
FastEthernet0/8            no         unlimited
FastEthernet0/9            no         unlimited
FastEthernet0/10           no         unlimited
FastEthernet0/11           no         unlimited
FastEthernet0/12           no         unlimited
FastEthernet0/13           no         unlimited
FastEthernet0/14           no         unlimited
FastEthernet0/15           no         unlimited
FastEthernet0/16           no         unlimited
FastEthernet0/17           no         unlimited
FastEthernet0/18           no         unlimited
FastEthernet0/19           no         unlimited
FastEthernet0/20           no         unlimited
FastEthernet0/21           no         unlimited
FastEthernet0/22           yes        unlimited
FastEthernet0/23           no         unlimited
FastEthernet0/24           no         unlimited
GigabitEthernet0/1         no         unlimited
GigabitEthernet0/2         no         unlimited
RiNG-Core#
```

reference:

(i) https://zh.wikipedia.org/zh-tw/DHCP_snooping (https://zh.wikipedia.org/zh-tw/DHCP_snooping)

(ii) https://zh.wikipedia.org/zh-tw/無線接入點 (https://zh.wikipedia.org/zh-tw/%E7%84%A1%E7%B7%9A%E6%8E%A5%E5%85%A5%E9%BB%9E)