NASA HW3

B11901164 陳秉緯

1. 問答題

references:

1. https://www.uuu.com.tw/Public/content/article/16/160822tips.htm
2. https://www.netadmin.com.tw/netadmin/zh-tw/feature/0C1A2DDB3CF94296864832049D8897A4
3. https://zh.wikipedia.org/zh-tw/生成树协议

答案：

1. 當終端使用者一旦開始進行 ARP spoofing 想要中斷其他使用者的網路連線時，Switch就會主動將攻擊者連接到Switch的網路介面，直接中斷使用，最後的結果是網路上其他使用者的網路連線沒有中斷，反而是攻擊者的主機網路連線會中斷，如此就可確保網路的正常使用
2. (a) Access Port 只屬於一個 VLAN，switch 會移除 802.1Q 標記，讓一般設備能正常收發資料。Trunk Port 允許多個 VLAN 透過一條連線傳輸，會在資料內增加 802.1Q 標記，標示目前這份資料是屬於哪一個VLAN，另一台設備收到後再根據這個標籤把這份資料送往所屬的VLAN。
   (b) Native VLAN 是 trunk port 傳輸時不加 802.1Q 標記的 VLAN，通常用來相容舊設備或作管理用途。可能的使用情境： 假設某些設備不支援 802.1Q，但還是需要透過 trunk 傳送流量，這時就可以讓這些設備的流量走 Native VLAN，避免標記不相容的問題
   (c) VTP 主要是讓 VLAN 設定可以在同一個 VTP domain 內的 switch 自動同步，減少手動配置的麻煩。
   - 運作方式：有三種模式
     - Server：可新增、刪除 VLAN，並同步給其他 switch
     - Client：不能修改 VLAN，只能接受 VLAN 設定
     - Transparent：不會參與同步，但還是允許本地 VLAN 設定
   - 優點：自動同步 VLAN 設定，減少人為錯誤
   - 缺點：如果不小心在 VTP Server 上錯誤刪除 VLAN，所有 Client 也會跟著刪除，影響整個網路
3. (a) 因為 Link Aggregation（LACP）只是把多條實體連線組合成一條邏輯連線，但每個資料流還是會透過單一實體連線傳輸，所以單一連線的速度不變，但整體頻寬變大，適合多個設備同時傳輸時分散負載。
   (b) passive 模式：只在收到 LACP 封包時才回應，不會主動發送，active 模式：主動發送

LACP 封包來建立通道
(c) 如果兩邊都是 passive的話就都不會主動發送 LACP 封包，導致 Link Aggregation 連線無法建立，連線會直接失敗

4. (a) STP 透過選舉 Root Bridge，然後計算每條連線的成本，關閉某些 Port，確保每個 VLAN 只有一條通路可以傳輸封包。
   (b) 以下五種：
   1. Disabled：不接收或者轉發資料
   2. Blocking：不接收或者轉發資料，接收但不傳送BPDU（Bridge Protocol Data Unit）
   3. Listening：不接收或者轉發資料，接收並行送BPDU，但還沒學習 MAC 地址
   4. Learning：不接收或者轉發資料，接收並行送BPDU，開始學習 MAC 地址
   5. Forwarding：接收或者轉發資料，接收並行送BPDU，進行 MAC 地址學習

2 真好，又有新的 switch 可以玩了：）

references:

1. https://www.cisco.com/c/en/us/support/docs/switches/catalyst-6000-series-switches/10581-6.html
2. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/d1/sec-d1-xe-3se-3650-cr-book/sec-d1-xe-3se-3850-cr-book_chapter_010.pdf
3. https://david50.pixnet.net/blog/post/45217866
4. https://www.cisco.com/c/en/us/td/docs/switches/lan/csbms/CBS_250_350/CLI/cbs-250-cli/rsa-and-certificate-commands.pdf
5. https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-350-series-managed-switches/smb5557-configure-the-internet-protocol-ip-address-settings-on-a-swi.html

答案：

1. 點擊 Switch1 並 `Switch(config)# hostname Switch1`，點擊 Switch2 並 `Switch(config)# hostname Switch2`
2. ```
   Switch1(config)# enable secret enable
   Switch2(config)# enable secret enable
   ```
3. ```
   Switch1(config)# ip domain-name nasa.com
   Switch1(config)# crypto key generate rsa
     # (打 yes 然後再打 2048)
   Switch1(config)# ip ssh version 2

   Switch2(config)# ip domain-name nasa.com
   Switch2(config)# crypto key generate rsa
   ```

```
  # (打 yes 然後再打 2048)
Switch2(config)# ip ssh version 2
```

4.
```
Switch1(config)# line vty 0 4
Switch1(config-line)# transport input ssh
Switch1(config-line)# login local
Switch1(config-line)# exit

Switch1(config)# line vty 5 15
Switch1(config-line)# transport input none
Switch1(config-line)# exit

Switch2(config)# line vty 0 4
Switch2(config-line)# transport input ssh
Switch2(config-line)# login local
Switch2(config-line)# exit

Switch2(config)# line vty 5 15
Switch2(config-line)# transport input none
Switch2(config-line)# exit
```

5.
```
Switch1(config)# vlan 10
Switch1(config-vlan)# name VLAN10
Switch1(config-vlan)# exit

Switch1(config)# vlan 20
Switch1(config-vlan)# name VLAN20
Switch1(config-vlan)# exit

Switch1(config)# vlan 99
Switch1(config-vlan)# name VLAN99
Switch1(config-vlan)# exit

Switch2(config)# vlan 10
Switch2(config-vlan)# name VLAN10
Switch2(config-vlan)# exit

Switch2(config)# vlan 20
Switch2(config-vlan)# name VLAN20
Switch2(config-vlan)# exit

Switch2(config)# vlan 99
Switch2(config-vlan)# name VLAN99
Switch2(config-vlan)# exit
```

6.
```
Switch1(config)# interface FastEthernet0/1
Switch1(config-if)# switchport mode access
Switch1(config-if)# switchport access vlan 10
Switch1(config-if)# exit

Switch1(config)# interface FastEthernet0/2
Switch1(config-if)# switchport mode access
Switch1(config-if)# switchport access vlan 10
Switch1(config-if)# exit
```

```
Switch1(config)# interface FastEthernet0/3
Switch1(config-if)# switchport mode access
Switch1(config-if)# switchport access vlan 99
Switch1(config-if)# exit

Switch2(config)# interface FastEthernet0/4
Switch2(config-if)# switchport mode access
Switch2(config-if)# switchport access vlan 20
Switch2(config-if)# exit

Switch2(config)# interface FastEthernet0/5
Switch2(config-if)# switchport mode access
Switch2(config-if)# switchport access vlan 20
Switch2(config-if)# exit

Switch2(config)# interface FastEthernet0/3
Switch2(config-if)# switchport mode access
Switch2(config-if)# switchport access vlan 99
Switch2(config-if)# exit
```

7.
```
Switch1(config)#interface range GigabitEthernet 0/1 - 2
Switch1(config-if-range)#channel-group 1 mode active
Switch1(config-if-range)#exit

Switch1(config)#interface Port-channel1
Switch1(config-if)#switchport mode trunk
Switch1(config-if)#switchport trunk allowed vlan 10,20,99

Switch2(config)#interface range GigabitEthernet 0/1 - 2
Switch2(config-if-range)#channel-group 1 mode active
Switch2(config-if-range)#exit

Switch2(config)#interface Port-channel1
Switch2(config-if)#switchport mode trunk
Switch2(config-if)#switchport trunk allowed vlan 10,20,99
```

8.
```
Switch1(config)# username admin secret nasa2025
Switch1(config)# privilege exec level 15 admin
Switch1(config)# interface vlan 99
Switch1(config-if)# ip address 192.168.99.1 255.255.255.0
Switch1(config-if)# no shutdown
Switch1(config-if)# exit

Switch2(config)# username admin secret nasa2025
Switch2(config)# privilege exec level 15 admin
Switch2(config)# interface vlan 99
Switch2(config-if)# ip address 192.168.99.2 255.255.255.0
Switch2(config-if)# no shutdown
Switch2(config-if)# exit
```

3 你在 switch 上玩什麼！

references:

1. https://www.cc.ntu.edu.tw/chinese/epaper/0047/20181220_4707.html
2. https://faddom.com/snmp-v2-vs-v3/
3. https://www.solarwinds.com/resources/it-glossary/mib
4. https://mibs.observium.org/mib/IF-MIB/
5. https://mibs.observium.org/mib/CISCO-SYSLOG-MIB/
6. https://mibs.observium.org/mib/CISCO-PROCESS-MIB/
7. https://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/7282-12.html

答案：

1. - SNMP（Simple Network Management Protocol，簡單網路管理協定）是一種用來監控和管理網路設備的協定。它允許管理端（NMS, Network Management Station）讀取設備狀態，並發送控制指令。
   - SNMPv2 vs SNMPv3 的主要差異：
     - 安全性
       - SNMPv2 沒有加密與認證機制
       - SNMPv3 增強安全性，有加密和驗證機制
     - 表現
       - SNMPv2 效率較差
       - SNMPv3 因為有加密、認證機制、資料拿取改善等等所以效率較好
     - 設置與管理難易度
       - SNMPv2 較容易
       - SNMPv3 較困難
2. MIB（Management Information Base，管理資訊庫）是 SNMP 使用的資料結構，用來存放網路設備的管理資訊。每個設備都有自己的 MIB，MIB 內的資料透過 OID（Object Identifier） 來識別。MIB 就像是 SNMP 的資料庫，管理端可以透過查詢 MIB 來獲取設備的資訊
3. 我認為監控 MIB 中的 IF-MIB 最有效地看出異常狀態發生，因為它能直接監控介面上的流量與錯誤數量，而 CISCO-SYSLOG-MIB 主要用來記錄系統變更，所以不適合，CISCO-PROCESS-MIB 用來監控 CPU 和記憶體使用率，所以部分適用，可用來查看 CPU 過載是否與流量異常有關
4. - 所需要的指令：

     ```
     snmp-server community public RO
     snmp-server community private RW
     ```

   - 步驟：
     (1) 點擊Switch0，選擇CLI，並按Enter
     (2) `enable`

(3) `configure terminal`

(4) `snmp-server community public RO` 啟用 read-only (RO) community string

(5) `snmp-server community private RW` 啟用 read-write (RW) community string

(6) 點擊PC0，選擇Desktop，選擇MIB Browser

(7) Address 填 192.168.9.254，OID 填 .1.3.6.1.2.1.1.5.0

(8) 點擊Advance...，並在 Read Community 填 public，Write Community 填 private，點ok

(9) 點擊按鈕 GO

(10) 在左側toggle list一直點開，如下圖所示，即成功在 PC0 查詢 hostname