Homework #4 - Cisco Switches & Wireshark

Due Time: 2024/03/17 (Sun.) 21:59
Contact TAs: `vegetable@csie.ntu.edu.tw`

Instructions and Announcements

- **NO LATE SUBMISSION OR PLAGIARISM IS ALLOWED.**
- Discussions with others are encouraged. However, you should write down your solutions **in your own words**. In addition, for **each and every** problem you have to specify the references (the URL of the web page you consulted or the people you discussed with) on the first page of your solution to that problem.
- Some problems below may not have standard solutions. We will give you the points if your answer is followed by reasonable explanations.

Submission

- Please place your answers in the same order as the problem sheet and do not repeat problem descriptions, just organize them by problem number in a tidy manner.
- Please submit your pdf report via Gradescope. And, zip the other 2 pka files, name the zip file "`{your_student_id}.zip`", and submit it via NTU COOL. The directory layout should be the same as listed below:

```
{your_student_id}/
+-- haruhikage.pka
+-- noroshi.pka
```

Grading

- The total score for the correctness and completeness of your answer is 100 points.
- It's possible you don't get full credits even if you have the correct answer. You should show how you get the answers step by step and list the references.
- Tidiness score: 3 bonus points, graded by TA.
- Final score = correctness score + tidiness score.

NASA is my GOAL !!! (100 points)

題目說明

- 以下文字有灰底的部分都是故事，可以跳過不影響作答。

Chapter 1

- 表格請整個照抄以方便批改。

Chapter 2, 3

- Switch CLI 指令在下列情況可能會有些許差異.....
  - 不同廠牌之間，例如 Cisco v.s HP。
  - 不同型號不同，例如 Catalyst 2960 v.s Catalyst 2960-X。
  - 不同 OS 版本之間，例如 c2960-lanbase-mz.122-25.SEE1.bin v.s c2960-lanbase9-mz.150-2.SE4.bin。

  作業裡面的 Switch 型號為.....
  - 廠牌：Cisco。
  - 型號：Catalyst 2960。
  - OS 版本：c2960-lanbase9-mz.150-2.SE4.bin。

  在作答時請盡量以正確的官方文件 (例如這篇) 為主，當然，其他型號/OS 版本的指令可能也有相似之處，不妨作為參考依據。
- 列出 Switch CLI 指令時，請用前綴來表示主機名稱與 CLI 模式，如.....
  - `Core# ...`
  - `Edge1(config)# ...`
  - `Lab221(config-if)# ...`
  - 其他以此類推
- 列出 Switch CLI 指令時，`enable`, `configure terminal`, `exit`, `end`, `copy running-config startup-config` 可省略。
- 列出 Switch CLI 指令時，請寫出完整的指令，不要使用簡寫。
- 每一題解完的 `.pka` 檔，請存檔後包進作業資料夾裡，批改時會以 pdf 為主，`.pka` 檔內的設定為輔。

Prelude: 碧天伴走

3 月時分，天空是一片湛藍，煦陽緩緩地灑落，校園內處處是生機盎然的前兆，初春之際雖有些許寒冷，但第二學期的校園內早已是人聲鼎沸，好不熱鬧，大學生們忙碌地穿梭在各個教學樓之間，為新學期奮鬥著。對於新學期同樣也滿懷希望，第三週好不容易加簽修滿 25 學分的你，伴隨著清澈無垠的藍天，徜徉在椰林大道上，彷彿暗示著你即將拿卷的命運。

這一天你路過德田館二樓時，看到了系上 NASA 團隊的宣傳海報，夢想有朝一日能夠追隨學長姐的行列，成為一位全職的爆肝工程師的你，興致高昂地想要馬上送出履歷，卻發現海報下面寫著一排小字。

「需有相關實習經驗」。

你心頭頓時五味雜陳，你知道，自己心中的熱情與對學習的執著都不是阻止你前進的障礙，只是因為客觀條件，你只能默默地假裝無視，離開了德田館。

Figure 1: 大概和她一樣失望吧

Chapter1: 迷星叫 (40%)

在回到宿舍的路上，你路過了上學路上總是會經過的 Live House，黃昏降臨，招牌上的燈光耀眼地秀出店名，「RiNG」。

過去有無數的樂團在這裡練習、表演，大家都在為了夢想而努力，自己卻礙於實習經驗，而被阻擋前行，你愣愣地站在店門口，時間一分一秒地經過，夜空取代了黃昏，你心中依舊感到憤憤不平，迷茫的你只能對著夜空中的星斗發出怒叫。

但當你低下頭，店門口的一張傳單吸引了你的目光。

「現正招募網路管理員，條件不拘。」

不愧是「山重水複疑無路，柳暗花明又一村。」你興高采烈地將履歷寄至 RiNG 的官方信箱，不久後就傳來了回信，信件中附上了以下的面試題目.....

Figure 2: 有信件耶，我看看喔

在課程中我們介紹了 VLAN 的技術，網路管理員可以藉此在 Switch 上達到切分子網域的目的，進而有效利用網路頻寬以及提高安全性，而當今最主流的實作方式是採用所謂的 802.1Q 標記中的 VID 欄位來達成。

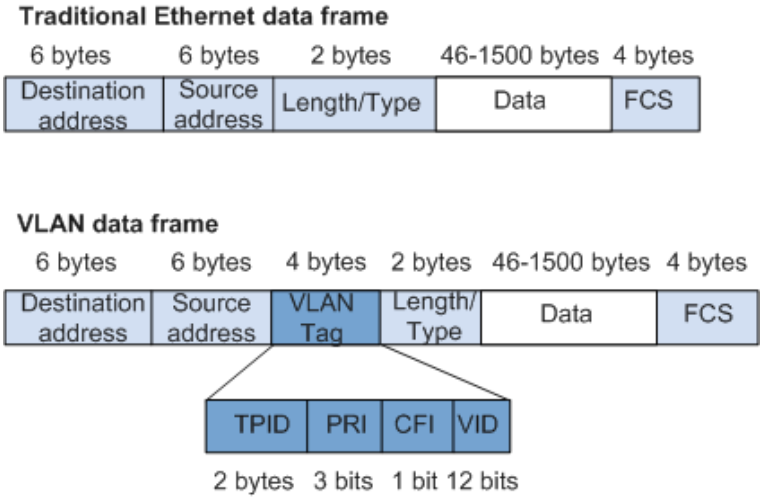

Figure 3: 802.1Q 標記在 L2 封包標頭的位置

1. 在 Cisco Switch 上我們可以指定一個埠口為 Access Port 或者 Trunk Port，請問這兩者有什麼差異，請完成下列表格。(8%)

	可通過的 VLAN 數量	802.1Q 標記
Access Port		
Trunk Port		

2. 請問何謂 Trunk Native VLAN？(6%)

3. 請根據 Figure 4 的情境，完成下列表格。(20%)

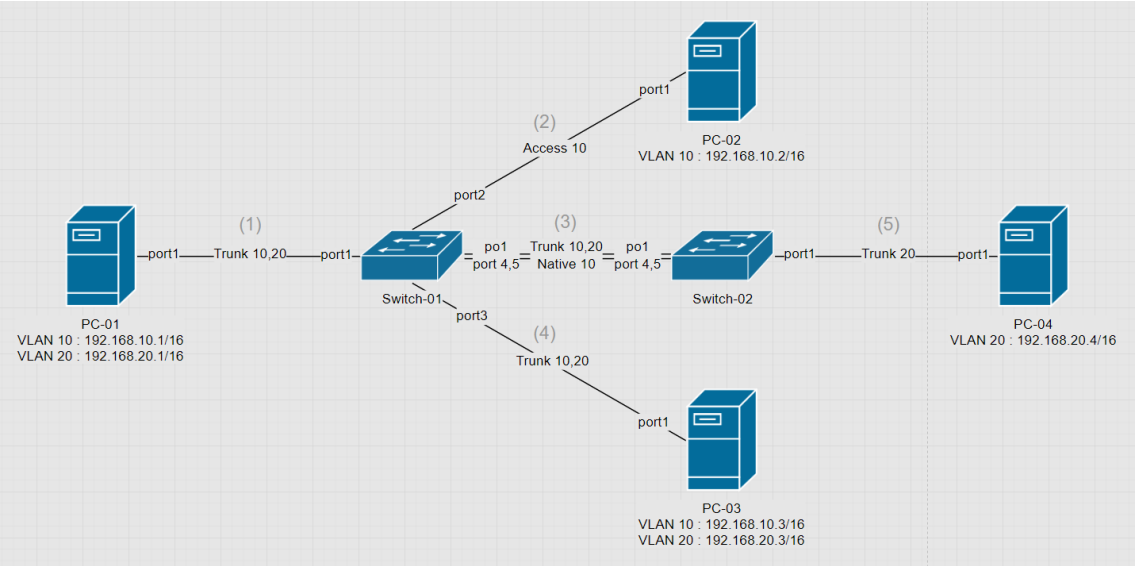

Figure 4: 某一個樓層的網路架構圖

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						(可/否)
PC-01/VLAN 20 → PC-02						
PC-01/VLAN 10 → PC-04						
PC-01/VLAN 20 → PC-04						
PC-01/VLAN 10 → PC-03						
PC-01/VLAN 20 → PC-03						

「802.1Q VID 欄位」請依以下格式填寫.....

- 數字：封包會經過該線路，該封包 802.1Q VID 欄位的數值。
- ” 無”：封包會經過該線路，該封包沒有 802.1Q 標頭。
- ”X”：封包不會經過該線路。

在沒有開啟任何路由功能的情境下，不同 VLAN 的機器理應是無法互相溝通的，例如 VLAN 10 的機器無法碰觸到 VLAN 20 的機器，如此才能達到切分子網域的目的。但在某些條件下，這個規則卻可能被打破，而形成被稱為「VLAN Hopping」的漏洞。

4. 請根據 Figure 4 的情境，試以 Double Tagging Attack 來解釋為何 PC-01 從 VLAN 10 介面發出的封包在特定條件下能夠送到 PC-04。(6%)

Chapter2: 春日影 (30%)

好不容易通過面試後，你展開了平日在學校上課，假日來到 RiNG 實習的規律生活，雖說是實習，但平常也沒什麼特別的麻煩事，頂多就是幫店員處理一下當機的電腦。多數空閒的時候，你總是在二樓靠著扶手，看著人來人往的大廳，春天的陽光從玻璃帷幕射入，來來往往的身影在地面留下了這個時期特有的光學現象，「春日影」。

偶爾也會出現有趣的插曲，像是之前在咖啡廳看到幾個高中女生圍在一起，說什麼要一輩子組樂團的，聽起來有點沉重，但另一個在旁邊偷聽的女生卻說，真是一群有趣的女人。果然玩音樂的，大家都很有個性呀。百般無聊的日常就這麼持續著，你原本以為祥和的日子會繼續下去.....

然而，那個夜晚之後，一切都改變了。

那個 RiNG 舉辦演唱會的夜晚，你剛買完值夜班的便當要回到櫃台的路上，在大廳看見了一個女生，從樓梯上直衝而下，還差點摔了跤，從你身旁跑過時，你好像在她臉上看到了淚水。今天的演唱會有這麼讓人感動落淚的嗎，音樂的力量真是偉大呀，當下你並沒有想太多。

然而幾天後，你接到一個匿名申請，要求刪除 CRYCHIC 這個樂團的專屬 VLAN 網路，又收到一個叫愛音的女生要申請新樂團 MyGO!!!!! 的專屬 VLAN 網路，你仔細一看這兩個樂團的人員組成，竟然有 3 個人重複！是吵架了嗎？但你也沒放在心上，先跑去幫櫃台處理那台又當機的電腦。

接下來一連數日，你每天都收到同樣的匿名申請，而且次數越來越頻繁，有時候好像還會看到一個女生，淋著雨在門口直盯著你看，你心想有點不妙，還是趕快處理一下為佳，正當你想登入 RiNG 的 Core Switch 做調整時，卻發現居然沒有開啟 SSH 登入！更扯的是，你突然發現之前離職的網路工程師忘了交接管理員帳號給你，你心頭一涼，但是為了 CRYCHIC，你只好熬夜加班了。

Figure 5: 那天晚上究竟為什麼要演奏春日影呢？

- 目標：完成 `haruhikage.pka`。(30%)
  - Part 1,2，請簡單敘述達成方式即可，不須列出詳細指令。
  - Part 3 請列出各小題的完整指令。
- 注意：
  - Part 1 的備份 config。
  - Part 2 有提供 Connectivity Test 來驗證正確性。
  - Part 3 沒有提供 Assessment Items 來驗證正確性。

Chapter3: 無路矢 (30%)

平息「春日影」風波後，RiNG 又回歸了和平的生活，然而意外總是比預期來的快，這天下午你正在櫃台值班，看到一個好像是叫做愛音的女生急急忙忙地跑了過來，說她沒辦法發團練的動態到 IG 上，你接過手機，發現 Wi-Fi 訊號是滿格的，卻無法連到外網，你檢查又檢查，都沒找到什麼問題，你轉過身打算要用自己的筆電查點資料時，發現自己的筆電竟然也是同樣的狀況！

當你還在想辦法搞清楚狀況時，情況卻不斷惡化，來自其他使用者的詢問不斷湧進，櫃台前都快塞成一場小型演唱會了，然而面對某一雙求助的雙眼，你心裡也沒有頭緒。此時的你，只期望有個路標能指引你前進的方向。

Figure 6: 來拍照吧 („・ω・„)

網路服務通常必須仰賴好幾台網路設備之間的合作配合才能運作順暢，因此有時候可能本機上的設定看起來沒有問題，串聯起來時卻產生了問題，這時就可以透過一些封包擷取工具，例如 Wireshark 等等，來實際觀察網路封包的進出情形，以及封包內的內容，來排除問題。

1. 請使用 Wireshark 來擷取自己的電腦連接 Wi-Fi 或是行動網路的個人熱點時，透過 DHCP 協定來自動取得網路組態 (IP、Subnet Mask 等等) 的過程，截圖應至少包含 DORA 4 個階段，並簡單解釋各階段的意涵。(8%)
   - 注意在相同網路下如果短時間內斷線又重新連上的話，DHCP 會從嘗試直接 Request 上一次使用過的 IP 開始，不會走過完整的 DORA 4 個階段，需要先手動 Release 掉租約。
2. 承上題，請觀察 DHCP Discover 的封包，你會發現來源端 IP 是 0.0.0.0、目的端 IP 是 255.255.255.255、目的端 MAC 是 FF:FF:FF:FF:FF:FF，這些特殊的 IP/MAC 地址各自具有什麼涵義呢？以及為何在 DHCP Discover 的階段，是填入這些特殊地址？(12%)
   - IP 0.0.0.0
     - 涵義：
     - 原因：
   - IP 255.255.255.255
     - 涵義：
     - 原因：
   - MAC FF:FF:FF:FF:FF:FF
     - 涵義：
     - 原因：

使用完 Wireshark 檢查自己的筆電之後，你發現筆電拿到的預設閘道 (Default Gateway) 很奇怪，並不是你熟悉的 RiNG 的主要路由器，因此你懷疑 RiNG 的無線網路可能遭到 DHCP Poisoning 攻擊了。

3. 目標：完成 `noroshi.pka` (10%)。
   - 本小題沒有提供 Assessment Items 來驗證正確性。
   - 請列出達成目的的完整指令。

To Be Continued → 也許明年可以出 Ave Mujica 篇