Homework #3

Release Time: 2021/03/22 (Mon.)
Due Time: 2021/04/11 (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 put your answers in one PDF named "`{your_student_id}.pdf`", and submit it through NTU COOL.
- Please zip all the files, including one PDF and one pka file, name the zip file "`{your_student_id}.zip`", and submit it through NTU COOL. The zip file should not contain any other files, and the directory layout should be the same as listed below:

```
{your_student_id}/
+-- {your_student_id}.pdf
+-- {your_student_id}_Q2.pka
```

Grading

- NA accounts for 50 points while SA accounts for 100 points. The final score is the weighted sum between them.
- 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 = NA score + $\frac{\text{SA score}}{2}$ + tidiness score.

Network Administration

1. VLAN, Access, and Trunk (8 %)

在課堂上我們提過設定 VLAN 的兩種模式：`access mode` 和 `trunk mode`。下方是某台 Cisco 2960X 的 switch 的設定，請依據此設定內容回答問題。(鼓勵大家使用 Cisco Packet Tracer 來實驗驗證)

```
Switch#show running-config interface Gi1/0/1
interface Gi1/0/1
    switchport trunk encapsulation dot1q
    switchport mode trunk
    switchport trunk allowed vlan 424, 524
    ip dhcp snooping trust
!
Switch#show running-config interface Gi1/0/2
interface Gi1/0/2
    switchport mode access
    switchport access vlan 424
!
Switch#show running-config interface Gi1/0/3
interface Gi1/0/3
    switchport mode access
    switchport access vlan 307
    spanning-tree bpduguard enable
!
Switch#show running-config interface Gi1/0/4
interface Gi1/0/4
    switchport trunk encapsulation dot1q
    switchport mode trunk
    switchport trunk allowed vlan 307, 511
    ip dhcp snooping trust
    spanning-tree bpduguard enable
!
Switch#show running-config interface Gi1/0/5
interface Gi1/0/5
    switchport trunk encapsulation dot1q
    switchport mode trunk
    switchport trunk native vlan 307
    switchport trunk allowed vlan 307, 511
    spanning-tree bpduguard enable
!
```

1. 有三個沒有 `802.1q tag` 的封包從 end user 端送到 Cisco 2960X 上，分別送到 `Gi1/0/3` , `Gi1/0/4` , `Gi1/0/5` 。在 switch 內部傳輸的時候，三者的 `802.1q header` 有何不同？(2 %)
2. 假設 host A 在 `Gi1/0/1` 之下的 LAN；host B 在 `Gi1/0/2` 之下的 LAN。當 host A 傳送一個封包給 host B，請描述 `802.1q header` 在通過 `Gi1/0/1` 之前/之後，以及通過 `Gi1/0/2` 之前/之後的變化。(3 %)

3. 什麼時候我們會用到 `switchport trunk native` 這個指令？請舉例：詳述情境和理由。(3 %)

2. More on Link Aggregation (7 %)

在課堂 lab 中，我們學到 Link Aggregation(或叫 Port Channel)的技術。以下是關於 Link Aggregation 的問題。

1. 我們只有一條`Cat.6 UTP cable (1Gbps bandwidth)` 和一條 `Cat.5 UTP cable (100Mbps bandwidth)`。我們可以用 Link Aggregation 達到 `1.1 Gbps link bandwidth` 嗎？為什麼？(2 %)
2. 以下是關於 port-channeling `Gi1/0/1-2` 的指令，但以下設定是錯誤的。請說明哪裡錯誤、會造成什麼錯誤的結果，並可以用什麼指令修正。(5 %)

```
Switch#show running-config interface Gi1/0/1
    interface Gi1/0/1
    switchport mode trunk
    switchport trunk allow vlan 100, 200
    channel-group 1 mode passive
!
Switch#show running-config interface Gi1/0/2
    interface Gi1/0/2
    switchport mode trunk
    switchport trunk allow vlan 100, 200
    channel-group 1 mode passive
!
Switch#show running-config interface Po1
    interface Portchannel1
    switchport mode trunk
    switchport trunk allow vlan 100, 200
!
```

3. Malicious User(13 %)

系館的網路架構由一台 core switch(L3) 和其他 edge switch(L2) 組成，形成樹狀結構。假設全部皆為 Cisco switch，每個 end user 都是接在 edge switch 上而非 core switch；core switch 再對接到台大計中 (計中為系館網路 gateway)。假設 core switch IP 為 `140.112.30.254` ，此為 `140.112.30.250` 的 gateway。(非常鼓勵大家使用 Cisco Packet Tracer 來實驗驗證)

1. 什麼是 L3 switch 和 L2 switch？(2 %) L3 switch 和 router 有何差別？(2 %)
2. `ARP table` 和 `MAC address table` 的差別為何？(1 %)
3. 有一天計中回報 `IP 140.112.30.250` 有惡意行為，請使用 Cisco switch 的功能，設計一個合理的流程來找到此 IP 的詳細所在位置。(詳細所在位置指的是，host 端在網路結構的哪個位置。例如， `edge switch A 的 Gi1/0/1 port`)
   Note: 請寫出盡量簡單且可實行的解。例如，查找所有 switch 上的 `MAC address table` 不在接受的範圍內。(10 %)

4. Set up another Cisco Switch (8 %)

目前系館的主要核心 switch 使用型號為 Cisco 3750G。下列問題是有關架設新的 Cisco 3750G 的細節。

1. 購買 switch / router 產品時，原廠通常都會送一條 console 線。而第一次開機設定時通常要透過 console port 來進行設定。cisco 的 console cable 通常是 DB9 to RJ45。請問什麼是 serial communication ？(2 %)
2. 使用 console cable 進行設定的好處和壞處為何？請列出至少個一個。(2 %)
3. 如果沒有 DB9 cable 的話，該怎麼進入和設定 switch？(2 %)
4. 架設好新的 Cisco 3750G 可以把兩台 stack 在一起。相比於 port trunk，stacking 的好處為何？需要有幾條 cable 才可以達到 stacking 完整的功能？(2 %)

5. Cisco Packet Tracer(14 %)

下載 hw3.pka 並且在 Switch0 做設定完成下列要求，配分顯示在 pka 檔裡。使用 PT Activity 視窗的 Check results 來檢視自己的分數，並把完成的檔案存成 `[student ID]_Q2.pka` ，上傳至 NTU COOL。而且你要將你做的步驟寫下來，還要在 report 中附上 Check results 的截圖。

1. 設定 switch 的 hostname 為”CiscoLab”
2. 關掉 switch 的 domain name lookup
3. 把 enable 的密碼設成”CISCO”，而且加密
4. 建立 VLANs 10, 20, 99
5. 將 `PC0` 和 `PC 1` 設為 VLAN `10` ；將 `PC2` 和 `PC 3` 設為 VLAN `20` 。屬於不同 VLAN 的電腦不可以互相 ping 到。
6. 將 `Admin` 設為 VLAN `99` 。
7. 在 VTY 0 to 4 設定 telnet 的密碼為”cisco”，並且完成相關設定使 `Admin` 可以利用 `telnet 192.168.99.1` 連線到 switch。

System Administration

小明在系上幫忙管了一些網站，平常他的作業環境是 CentOS 7 ，使用 libvirtd、QEMU/KVM 等工具建立以及管理許許多多的虛擬機。但是他最近沉迷於 Mount and Blade 2 中，身為他好朋友的你被他拜託幫忙處理一些事情。

注意事項

- 小明需要知道你所有的步驟，你還要寫下使用的指令以及解釋。除非特別註明，未解釋者將扣部分分數。
- 除了 host vm 的安裝可以使用圖形介面外，其他操作只能使用命令列介面 (Command line interface)。
- 使用有支援 nested virtualization 的 hypervisor，例如：VMWare、VirtualBox 6.0、KVM等。
- 記得在你的電腦的 BIOS 或 UEFI 啟用 Intel VT-x 或 AMD-V。

Virtual machine host 通常是一個上面跑了一個或許多被稱為 guest 的虛擬化機器的實體機器。而 hypervisor 則是一個在 host 上管理 guests 的軟體。為了讓你跟小明的作業環境相同，你要先建立一個 CentOS 7 的虛擬機當作 host ，並在 host 上面建立另一個虛擬機當作 guest (VM 上再裝一個 VM，被稱為 *nested virtualization*)。

小明寫下了步驟來幫助你：

1. 安裝 Host VM (5%)

步驟 1、2、3 無須解釋

1. 下載 CentOS 7 ISO (0%)
   - Mirrors: http://isoredirect.centos.org/centos/7/isos/x86_64
2. 按照下列要求安裝 CentOS 7 (0%)
   - 至少 10 GB 的 root 切割
   - 使用 NAT 為網路設定
   - 建議 4GB RAM
3. 在 hypervisor 設定 NAT 網路 (0%)
4. 確定你可以從 host 與本機通訊 (1%)
5. 安裝必要套件，包括 virt-install, qemu-kvm 和 libvirt (2%)
6. 用 systemd 啟用 libvirtd，並且設定開機自動啟用。這個 daemon 會幫你管理 guest VM (2%)

2. Host 上的網路 (10%)

在安裝 guest vm 前，小明還提醒你要先完成下列事項：

1. 解釋 NAT 與 bridge networking 的相異之處 (3%)
2. 在 host 上設立 bridge network，並寫下你所有的步驟 (7%)

3. VM 上的 VM (47%)

通常在安裝作業系統時會有圖形化的介面一步步指引我們整個安裝流程。但是像小明一次管了十幾台的虛擬機，若每台設定相同的虛擬機都要從頭安裝將會非常耗時且無聊。好在 CentOS 7 可以透過 Anaconda kickstart script 自動化安裝，只需要寫一次設定檔便能方便快速的安裝大量的機器。

現在小明提供了 Anaconda kickstart script的範本，希望你能用自動化工具幫他在 host 上建立一個 vm。

1. mkdir /data/img (0%)
2. 在 /data/img 底下建立一個 10GB 大的 qcow2 檔，作為 guest VM 的 image (10%)
3. 以 小明的 scirpt 為基礎在自動安裝時達成下列事項。(你只需要寫下你增加或修改的地方，不要複製貼上整份檔案)(15%)
   - 在 wheel 群組下增加一個名為 xiaoming 的使用者，使用 XMishandsome 為密碼，並使用 SHA512 加密
   - 安裝這些 packages：epel-release, vim, sudo 和 wget
4. 使用 virt-install 來建立 guest vm，並擁有下面的特性 (請寫下你用的指令)(22%)
   - 名稱為"ILoveNASA"
   - 2048 M 的記憶體
   - 2 CPUs
   - 使用步驟 2-2 的 bridge
   - 使用步驟 3-2 的 image 為他的 disk
   - 使用步驟 3-3 的 kickstart 檔
   - 使用 http://centos.cs.nctu.edu.tw/ 為 distribution 來源
   - 開啟一個 text console 讓你可以從 host 看到安裝資訊

4. 小明，我要進來囉 (20%)

若上面的步驟都完成正確，成功安裝後你應該會看見 guest 的登入畫面。這時候小明發下他忘記跟你說他想要透過 ssh 進入你幫他開好的 guest vm。你可以幫他一個忙，幫他設定好 ssh server 嗎？

1. 使用 xiaoming 這個使用者登入 ILoveNASA，安裝 openssh-clients、openssh-server，並且啟用以及開啟開機自動啟用 (5%)
2. 截圖在 ILoveNASA 中執行 "ip a" 的結果
3. 找到方法退出 Virsh Console
4. 截圖在 host 中執行 "ip a" 的結果 (10%)
5. 在 host 上使用 ssh 進入 ILoveNASA ，並截圖結果 (5%)

Note: ILoveNASA 與 host 要在同個 subnet 底下，且要寫出退出 virsh console 的方法才會一起拿到步驟 2、3、4 的分數

5. 初四了，小明 (18%)

經過上面的事件，小明覺得你很有潛力。而你辛苦裝的 ILoveNASA 上面也開始跑了些服務。有一天小明發現 ILoveNASA 中的服務有些問題，並請你一起幫忙。

依照下面的步驟完整寫下你使用的 virsh 或其他指令以及你使用的參數。

1. 小明請你先把 ILoveNASA 暫停 (3%)
2. 為了 debug，小明請你複製一份 ILoveNASA ，並將新的 vm 取名為 ILoveNASA-2 (3%)
3. 讓 ILoveNASA 繼續跑 (3%)
4. 列出所有的 guest machine ，並截圖結果 (3%)
5. 將 ILoveNASA-2 的 CPU 數量改成 1 個 (3%)
6. 列出 ILoveNASA-2 所有的網路介面 (3%)

Hint: 步驟二只需要一個指令