Homework #3

Due Time: 2019/4/7 (Sun.) 22:00
Contact TAs: `vegetable@csie.ntu.edu.tw`

Submission

- Put all answers **in one single PDF file** named **[studentID].pdf**, in the same order as the problem sheet. Do not repeat problem descriptions, just organize them by problem number in a tidy manner.
- Submit 2 files on NTU COOL (`https://cool.ntu.edu.tw`):
  - The **[studentID].pdf** file to section **Homework 3**.
  - The **[studentID]_Q2.pka** file to section **Homework 3 - Cisco Packet Tracer**.

Instructions and Announcements

- 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.
- Problems below will be related to the materials taught in the class and may be far beyond that. Try to search for additional information on the Internet and give a reasonable answer.
- Some problems below may not have standard solutions. We will give you the points if your answer is followed by reasonable explanations.
- **NO LATE SUBMISSION OR PLAGIARISM IS ALLOWED.**

Network Administration

1. Set up another Cisco Switch (11%)

Cei-Ba, the network administrator in CSIE department, is upgrading the network infrastructure in the building. Currently a *Cisco 3750G* is used as the core switch. However, with the growth of IDC, the ports on core switch are not enough. He, consequently, would like to set up another new *Cisco 3750G* switch to work together with the original core switch.

1. (2%) When we boot a switch from factory default, most of the time we need to use console line RS232 to control and configure it. What is the advantage and disadvantage of using console line RS232 to set up the switch? Please list one for each.

2. (2%) Unfortunately, Cei-Ba does not have any RS232 cable. How can he access and configure the switch?

3. (3%) Cei-Ba set the login credential as the following:

   ```
   Switch#show running-config | include username
   username CeiBa password 7 02280B643F1F1F047319
   ```

   After acquiring the above configuration, you, as a hacker, please get the original password.

4. (3%) Cei-Ba would like to *stack* the two 3750 switches so that they can work together as a whole. What is the advantage of *stacking*, compared to connecting the switches solely with a trunk port? Please list two reasons.

5. (1%) How many stack cables will Cei-Ba need to achieve full functionality of *stacking*? Why?

2. Cisco Packet Tracer (14%)

After setting up the new switch, Cei-ba need to configure it so that it will be able to be deployed to production environment.

Download `hw3.pka` and complete the following tasks on Switch0: (Points for each question is shown in the `pka`.)

- Set the hostname of the switch to ”CiscoLab”
- Disable domain name lookup in CLI
- Set enable password to ”CISCO” and encrypt it
- Create VLANs 10, 20, 99
- Assign PC0 and PC1 to VLAN10 and assign PC2 and PC3 to VLAN20 so that PCs in different VLANs cannot ping each other
- Assign Admin to VLAN99 and Admin should be able to access the switch by telneting 192.168.99.1
- Set the telnet login password to ”cisco” on VTY 0 to 4

Use ”Check results” on the ”PT Activity” window to check your points, save your work to **[studentID]__Q2.pka**, and upload to NTU Cool. In addition, please put a screenshot of your ”Check results” page in your report.

3. Malicious User (6%)

The network infrastructure consists of one core switch (L3) and several edge switches (L2), forming a tree topology. All the switches are *Cisco* switches. One day Cei-Ba received a report from NTU-CC warning that the owner of IP `140.112.30.250` is doing something nasty. You, as Cei-Ba's assistant, have the responsibility to notify the owner of that IP. Please design a procedure to trace the physical location (e.g. On Port 1 of edge switch A) of the end user. Assume the IP of the core switch is `140.112.30.254`, which is the gateway of `140.112.30.250`. Please propose a solution that is as effortless as possible. For example, looking up the MAC address tables on all edge switches on the network simultaneously is not a feasible solution.

4. More on Link Aggregation (8%)

During the in-class lab, we've learned the advantages of *Link Aggregation*, or so-called *Port Channel.* Here let's think more about the advantages and disadvantages about this technique.

1. (3%) Suppose there are two *Cisco 2960-S* switches and we would like to use two links to increase the bandwidth. However, we have only one Cat.6 UTP cable (support 1Gbps bandwidth) and one Cat.5 UTP cable (support 100Mbps bandwidth). Can we aggregate the bandwidth of these two cables to make a 1.1 Gbps link? Why or why not?

2. (5%) The followings are the configuration of two switches for port-channeling Gi1/0/1-2 on both switches. However, the port-channel is not working. Please find out why the configuration is broken, and fix it so that the port-channel can work normally.

```
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
!
```

5. The Evil VLAN, Access, and Trunk (11%)

We've mentioned some knowledge about `access mode` and `trunk mode` when setting VLANs on switch ports. However, it is much more complex than what we've taught in class. In the following questions, we use *Cisco 2960X* series as our switch and the provided configuration is based on it. You are encouraged to use packet tracer to conduct some experiments.

1. (3%) A packet with 802.1q VLAN tag 424 is sent out from the switch via port `Gi1/0/1`. Later, the same packet is sent out again, but via port `Gi1/0/2`. What is the difference in 802.1q header between the two output packets from distinct source ports?

2. (4%) Three Packets with no 802.1q VLAN tag are sent out from different end users to the switch via ports `Gi1/0/3`, `Gi1/0/4`, `Gi1/0/5`, respectively. What is the difference in 802.1q header among the three packets from distinct incoming ports?

3. (4%) In what scenario will enabling "`switchport trunk native`" be needed? Please give one example and explain why such configuration is necessary in that scenario.

```
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
!
```

System Administration

Before you start

- Write down what you did step by step **following our instructions**, and provide explanation and the commands you use for each step, except explicitly stated otherwise, to earn full credit.
- You can only use command lines when modifying configuration. Graphical interface is allowed only during installation of host VM.
- Use a virtual machine hypervisor that supports *nested virtualization*, e.g. VMWare, KVM and VirtualBox 6.0.
- Enable Intel VT-x or AMD-V in your BIOS or UEFI firmware.

The Virtual Machine

In NTU CSIE we host a variety of services to facilitate healthy operation of the whole department. Primary concerns of operating such a complex system include:

- **Hardware cost**: how to fulfill the hardware requirement of all services at a cost-effective manner?
- **Security**: how to isolate services to prevent a compromised service from affecting other services?
- **Ease of management**: how to automate as much as possible to prevent human errors?

Running services in virtual machines is a common way to address all above concerns. It consolidates services from multiple machines into one host machine yet ensure strong isolation between them. In this homework, you will learn how to manage your virtual machines with an useful tool called *libvirt*.

1. Install a VM host running *CentOS 7* (10%)

A *virtual machine host* is typically a physical machine that operates a couple of virtualized machines that we referred to as *guests*. A hypervisor is a software-level manager of these guests. For the sake of convenience, we will spin up a VM to serve as a host, and run a guest VM within this VM (yes, VM inside VM is called *nested virtualization*). Follow these steps (no explanation required for step 1 to 3):

1. Configure NAT networking in the hypervisor.
2. Download a *CentOS 7* ISO:
   - Google Drive: `http://tinyurl.com/y59njpwx`
   - This is faster if you're in Dirtien: `http://linux4.csie.org:59487/centos-7.iso`
3. Install a minimal system with a 10 GB root file-system, without swap or other partitions. Use NAT for network connectivity.
4. Install required packages, including `virt-install`, `qemu-kvm` and `libvirt`.
5. Start the `libvirtd` service using `systemd`. This daemon runs on host server and manage virtualized guests for you. In addition, enable automatic start-up of this service.

2. Create a Virtual Machine (guest) on VM host (18%)

An OS installer typically presents a graphical interface to guide an user through the installation process. But installing hundreds of machines of identical configuration using graphical interface would be tedious and stupid. Fortunately, *CentOS 7* can be installed **programmatically** using an *Anaconda* kickstart script. The script contains configurations that would normally be asked during an installation process. Using a kickstart script, we can generate as many new machines as we desire without being prompted any question.

Now, we are going to install a guest VM in an automated fashion. Perform the following steps on the VM host.

Steps:

1. `mkdir /data/img` (no explanation required).
2. Format a *QCOW2* image, sized at 10G, as the guest image and place it under `/data/img` .
3. Complete this *Anaconda* kickstart script[1] to automate the following tasks (in the answer sheet, instead of pasting the entire content, simply list your modifications to the script):
   - Create a user named `meow` in the `wheel` group, with the password `meow` encrypted by SHA512[2].
   - Install these packages: `epel-release`, `vim`, `openssh-server`, `sudo` and `wget`

   Leave disk partition, network setup and other configuration unchanged.
4. Set up a bridged network interface on the host machine. A bridged network interface exposes a VM to host's network as if it were a distinct member of the host network. Consequently, the VM becomes directly accessible from other hosts on the host network without NAT or manual port forwarding.
5. Create a VM named `nasa` with the `virt-install` command.
   - `virt-install` supports two means of installation: CDROM/ISO installation and distribution tree installation. Use the second mean: it will download the required kernel and bootstrapping file-system from a public source **on the fly** (without downloading it in advance). Use this source: `http://centos.cs.nctu.edu.tw`
   - The VM console can be accessed via VNC, Spice or text console. Configure a text console for the guest.
   - Use the bridged network interface you created in previous step.

   Hint:

   - Read `man virt-install` carefully.
   - To access text console, extra kernel boot parameters are needed.

   A text console will be launched and the installation process will be shown. You can type `Ctrl-]` to leave the console

[1] `http://ix.io/1ElA`

[2] You can use this: `https://github.com/lzap/pwkickstart`

3. Enter Guest (5%)

When installation is completed, reboot into the brand-new guest. You can either ssh into the guest (if its IP has been known) or enter via text console.

1. What command did you use to access the text console?
2. Show me the output of the command ”`ip addr`” on both VM host and guest with screenshot (expected result: the guest shall obtain an IP provided by the host's DHCP server and the guest and the host are in the same sub-net).

4. Manage the VM from VM host (5%)

Write down the `virsh` command to accomplish the following tasks (no explanation required):

1. Show all virtual machines on the host (both running and non-running VM).
2. Remove a virtual machine.
3. Edit configuration of a virtual machine directly.
4. Show network interfaces of a VM .
5. Show interfaces of the ethernet bridge.

5. Back up without stopping guest VM (12%)

Have you ever accidentally messed up with your machine and it just dies after reboot? Maybe you haven't, but we've certainly experienced this more than once. When you really have bad luck, it'd be too late for regretting: *it would be great if I had backed up my computer...* Let's why we teach you the importance of back-up and emphasize it over and over again. Now, let's learn how to back up a VM **while it is running**.

Because the VM is still running and constantly modifying its image, naïvely copying the image could result in data corruption. To obtain a consistent backup, we will create a *snapshot* first. Two images will be generated: the base image and the overlay image. The overlay image will absorb all data updates written after the moment of snapshot, while leaving the base image ”*frozen*”, which can be safely backed up.

Steps:

1. Create an *external*, *disk-only* snapshot using the `virsh` command.
2. Copy the base image to `/bc-img/nasa_backup.qcow2`.
3. Merge the overlay file back to the base image.

Hints: *Libvirt*'s documentation will save your life.