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.

   Advantage: Simple Protocol. Compatible with many legacy devices. Disadvantage: Not suitable for long distance and high speed.

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

   Cisco Switches support *Express Setup*. Please refer to the link. The switch will serve as aDHCP at first and let a PC connect to its web interface.

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.

   The plaintext is `No_TypE_7` . Note that type 7 is NOT secure. It is only an encoding procedure, so it is also easy to be decoded.

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.

   Stacking can share the computation resources among the stack devices, and it can be managed as one single switch.

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

   Two. Since we need to make it as a circular linked list.

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.

Open the switch0's CLI:

```
switch> enable
switch# conf t
switch(config)# hostname CiscoLab
CiscoLab(config)# no ip domain-lookup
CiscoLab(config)# enable password CISCO
CiscoLab(config)# service password-encryption
CiscoLab(config)# int vlan 10
CiscoLab(config-vlan)# exit
CiscoLab(config)# int vlan 20
CiscoLab(config-vlan)# exit
CiscoLab(config)# int vlan 99
CiscoLab(config-vlan)# exit
CiscoLab(config)# int range Fa0/1-2
CiscoLab(config-if-range)# switchport mode access
CiscoLab(config-if-range)# switchport access vlan 10
CiscoLab(config-if-range)# exit
CiscoLab(config)# int range Fa0/3-4
CiscoLab(config-if-range)# switchport mode access
CiscoLab(config-if-range)# switchport access vlan 20
CiscoLab(config-if-range)# exit
CiscoLab(config)# int Fa0/5
CiscoLab(config-if)# switchport mode access
CiscoLab(config-if)# switchport access vlan 99
CiscoLab(config-if)# exit
CiscoLab(config)# int vlan99
CiscoLab(config-if)# ip address 192.168.99.1 255.255.255.0
CiscoLab(config-if)# exit
CiscoLab(config)# line vty 0 4
CiscoLab(config-line)# password cisco
CiscoLab(config-line)# login
CiscoLab(config)# exit
```

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.

First, by checking out the ARP table in core switch, we can get the MAC address from the malicious IP address, which is `aaaa.bbbb.cccc`.

```
Core# show ip arp 140.112.30.250
Protocol Address         Age (min) Hardware Addr  Type Interface
Internet 140.112.30.250         4 aaaa.bbbb.cccc ARPA Vlan30
```

Next, by checking out the MAC address table, we can get the port it's using, which is `Po7`.

```
Core# show mac address-table address aaaa.bbbb.cccc
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  30    aaaa.bbbb.cccc    DYNAMIC     Po7
```

Then we can get the information of the port (switch `Edge42`) by checking out the interface status.

```
Core# show int status | include Po7
Port     Name         Status       Vlan   Duplex  Speed Type
Po7      To Edge42    connected    trunk  a-full a-1000
```

We connect to switch `Edge42`, and check out the MAC address table.

```
Edge42# show mac address-table address aaaa.bbbb.cccc
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  30    aaaa.bbbb.cccc    DYNAMIC     Gi1/0/5
```

If the corresponding interface is a end user, finally, we know who is using the IP.

```
Edge42# show int status | include Gi1/0/5
Port     Name         Status       Vlan   Duplex  Speed Type
Gi1/0/5  Zolution     connected    30     a-full a-1000 10/100/1000BaseTX
```

Otherwise, we keep repeating the above steps until the interface of that MAC address is a end user instead of a switch.

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?

   No, two cables with different bandwidth cannot be aggregated together. However, it can be configured as a hot spare. That is, when the 1Gbps link is accidentally down, the 100Mbps link will be up immediately to work as a backup link.

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.

   At least one side of the port-channel should be in mode active, or neither sides will initiate the negotiation to build a port-channel.

```
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?

   The packet through `Gi1/0/1` will have vlan tag 424, while that through `Gi1/0/2` will have no vlan tag.

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?

   The packets from `Gi1/0/3` and `Gi1/0/5` will be tagged as vlan 307, that from `Gi1/0/4` will be tagged as the switch native vlan, which is by default vlan 1.

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.

   When we use a vmhost to tag the vm network interfaces to different vlans, and the host still need to directly connect to the switch, then the configuration will be needed.

```
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
!
```