

Homework #3

Due Time: 2015/4/20 (Mon.) 17:00

Contact TAs: vegetable@csie.ntu.edu.tw

Submission

- Compress all your files into a file named “**<studentID>.zip**”, which contains a pdf file of all your answers in *Network Administration I Part*, and a file named “*<studentID>.pka*”.
- **Submit your zip file to ceiba.**
- **Please demo your *Network Administration II Part* to TA.**

Instructions and Announcements

- Discussions with others are encouraged. However, you should write down your solutions **in your own words**. In addition, for each problem you have to specify the references (the Internet URL you consulted with or the people you discussed with) on the first page of your solution to that problem.
- Problems below would be related to the material taught in the class and might be far beyond that. Try to search for additional information on the Internet and give an reasonable answer.
- Some problems below might not have standard solution. We would give you the point if your answer is followed by reasonable explanations.
- If you get stuck in problems below, feel free to contact TAs.
- **NO LATE SUBMISSION IS ALLOWED.**

Network Administration I

1. Assume that you are the network administrator of the CSIE department, and you have admin access to a Cisco switch network consisting of a core switch and a number of edge switches, forming a tree topology. One day you receive a report from NTUCC on malicious packets from some IP, say, 140.112.31.252, and you are responsible of notifying its user of the issue. Describe the necessary steps to trace the location of the end user (the port they use on the edge switch). Assume the gateway of 140.112.31.252 is 140.112.31.254, which is the core switch, and please propose the solution with *as less effort as possible* (e.g. looking up the MAC address table on **all** edge switches on the network at the same time is not a feasible solution.)
2. In HW2 we played with the Spanning Tree Protocol, and now it's time to configure our Cisco switches! All Cisco switches are shipped with a default bridge ID of 32768 on all VLANs, so it's necessary to determine and setup the root bridge during deployment. Find out the command that sets a Cisco switch to be the root bridge on VLAN 1, and the resulting bridge ID.
3. *Playing with Cisco Packet Tracer*. Download "hw3.pka" from the course website and complete the following tasks on Switch0:
 - set the hostname of the switch to "CiscoLab" (10%)
 - disable domain name lookup in CLI (5%)
 - set enable password to "CISCO" (should be encrypted) (10%)
 - create VLANs 10, 20 and 99 (15%)
 - make PC0 and PC1 be under VLAN 10 and make PC2 and PC3 be under VLAN 20 such that PCs in different VLANs cannot ping each other (35%)
 - make Admin be under VLAN 99 and Admin should be able to access the switch by telneting 192.168.99.1 (10%)
 - set telnet login password to "cisco" on VTYs 0 to 4 (15%)

Use "Check results" on the "PT Activity" window to check your points, and save your work to "*<studentID>.pka*" (without brackets) inside the StudentID_NA1 folder.

4. We learned about the Cisco password encryption feature in class and applied it in Problem 3, but the encryption is actually vulnerable to attacks since it's merely some sort of encoding instead of a one-way hash function. Decrypt the following encrypted password "080F454D06370C141D25050D34". Real-world applications should apply the "secret" feature that makes use of hash functions such as MD5.

Network Administration II

1. 設定pfsense並切vlan2與vlan99使得
 - a) vlan2的使用者ping不到vlan99的使用者
 - b) vlan2的使用者碰不到pfSense
 - c) vlan99的使用者可以ssh到linux1 ~ linux3
 - d) vlan99的使用者可以不必背 ip
 - e) vlan99的使用者可以從Web GUI對pfSense做設定
 - f) vlan99的使用者不該可以連到其他地方

Demo Time @ 217

- 4/16 Thu. 19:30 ~ 22:00
- 4/17 Fri. 13:00 ~ 15:00
- 4/20 Mon. 10:00 ~ 12:00
- 4/23 Thu. 19:30 ~ 22:00
- 4/24 Fri. 13:00 ~ 15:00
- 另外約時間，hanhan0912@gmail.com