

Homework #3 Solution

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

Network Administration Part 1

1. 1+1=1! (20%)

(a) (5%)

- Increase bandwidth.
- Resilience - When a link is failed, another link can still work.

(b) (15%) Suppose Fa0/3 and Fa0/4 are the ports used between switch0 and switch1. Open switch0's and switch1's CLI:

```
Switch> enable
Switch# conf t
Switch(config)# int port-channel 1 (create port-channel 1)
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit
Switch(config)# int Fa0/3-4
Switch(config-if-range)# switchport mode trunk
Switch(config-if-range)# channel-group 1 mode active (use port-channel 1)
Switch(config-if-range)# exit
```

2. CISCO Packet Tracer (15%)

Open 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. CSIE Crime Tracer (15%)

First, check out the ARP table in Core switch, then we can get the mac address from the IP, which is aaaa.bbbb.cccc.

```
Core# show ip arp 140.112.29.197
Protocol Address      Age (min)  Hardware Addr   Type   Interface
Internet 40.112.29.197    153       aaaa.bbbb.cccc  ARPA   Vlan29
```

Next, check out the MAC address table, then we can get the port it's using, which is Po8.

```
Core# show mac address-table address aaaa.bbbb.cccc
          Mac Address Table
-----
Vlan  Mac Address      Type        Ports
----  -
29    aaaa.bbbb.cccc   DYNAMIC     Po8
```

Check out the interface status, then we can get the information of the port. (switch Vegetable)

```
Core# show int status | include Po8
Port  Name           Status      Vlan  Duplex  Speed Type
Po8   To Vegetable   connected   trunk a-full  10G
```

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

```
TAcomputer$ ssh Vegetable
...
Vegetable# show mac address-table address aaaa.bbbb.cccc
          Mac Address Table
-----
Vlan  Mac Address      Type        Ports
----  -
29    aaaa.bbbb.cccc   DYNAMIC     Gi1/0/3
```

Finally, we know who's using that IP!

```
Vegetable# show int status | include Gi1/0/3
Port      Name      Status      Vlan  Duplex  Speed Type
Gi1/0/3   Hsinmu    connected   trunk a-full  a-1000 10/100/1000BaseTX
```

Network Administration Part 2

Subtask1

1. Setup VLAN and DHCP as we introduced at lab session.
2. Set DHCP Server -> LAN -> Gateway to none because we don't want traffics go to LAN interface.

Subtask2

1. Enable **Secure Shell** on pfSense.
2. Block traffics to **This Firewall** at port 22, 80, 443 on VLAN 5 and 8.
3. Pass traffics to **This Firewall** at port 22, 443 on VLAN 99.
4. Pass traffics to 140.112.30.44 at port 22 on VLAN 99.
5. Pass any other traffics on VLAN 5 and 8.
6. Block any other traffics on VLAN 99.

Subtask3

1. Set DNS
 - Use DNS Resolver
 - Or set public DNS such as 8.8.8.8 on DHCP Server.
2. Pass UDP 53 at VLAN 5 and 8

Note that DNS is on UDP 53, not TCP.

Subtask 4

1. Pass traffics to VLAN 5 at VLAN 8.
2. Block traffics to VLAN 8 at VLAN 5.

PfSense only blocks handshaking of connections, so blocks traffics to VLAN 8 doesn't block replies from VLAN 5 to VLAN8.

Subtask 5

If you doesn't modify anything of NAT, this subtask passes automatically.