วิชา Computer Networks 3/2562 **ปฏิบัติการที่ 9: Switch Port Security and ACL** รหัสนักศึกษา..... ชื่อ..... **<u>วัตถุประสงค์</u>** เรียนรู้การทำงานของ NAT, DHCP and DNS **<u>ไฟล์ที่จำเป็น</u> Lab9-2_Std.pkt**	**คะแนน**

<u>แบบฝึกปฏิบัติการที่ 9.1</u> Port Security

i. Topology

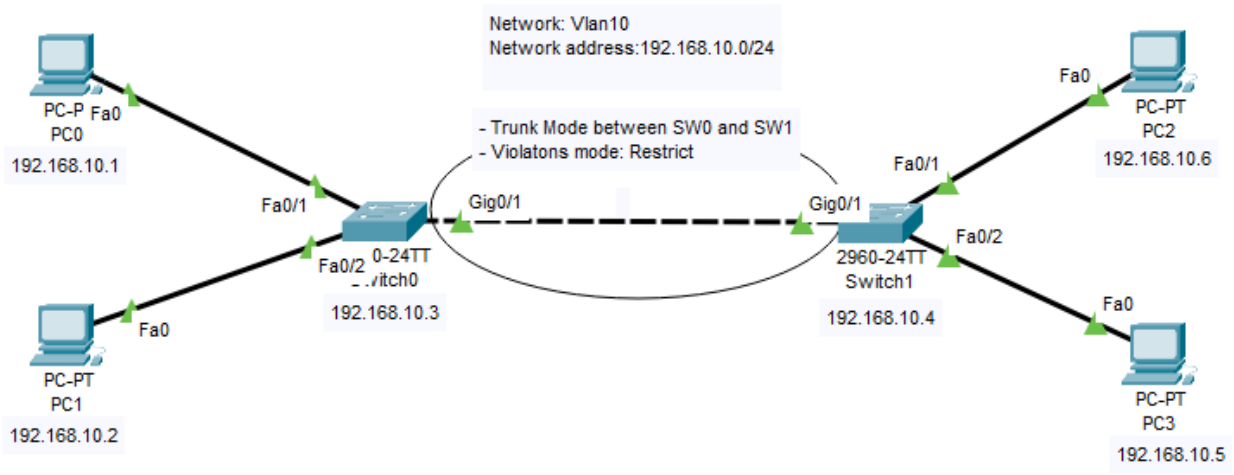

Figure 1 Lab 9.1

ii. คำอธิบายแบบฝึกปฏิบัติการที่ 9.1

1) สร้างเครือข่ายคอมพิวเตอร์และกำหนดค่า IP Addresses ตาม Figure 1

- ทุกเครื่อง มี Network Address คือ 192.168.10.0/24
- กำหนด Vlan เป็น Vlan10 ทั้งหมด คือ
    a. SW0 ทั้ง F0/1 และ F0/2 เป็น Vlan10
    b. SW1 ทั้ง F0/1 และ F0/2 เป็น Vlan10
- ระหว่าง SW0 G0/1 และ SW1 G0/1 เป็น Trunk port และทำการ allowed vlan 10 ด้วย

2) กำหนดค่า Port Switch ที่ SW0

- กำหนดให้ F0/1 และ F0/2 เป็นการเรียนรู้ mac address แบบ Sticky
  - *Switch0(Config-if)# switchport port-security*
  - *Switch0 (Config-if)# switchport port-security mac-address sticky*
- กำหนดให้ G0/1 เป็นการเรียนรู้ mac address แบบ Sticky สูงสุดจำนวน 2 mac addresses และมี Violation mode แบบ restrict
  - *Switch0 (Config-if)# switchport port-security*
  - *Switch0 (Config-if)# switchport port-security maximum 2*
  - *Switch0 (Config-if)# switchport port-security mac-address sticky*
  - *Switch0 (Config-if)# switchport port-security violation restrict*

3) กำหนดค่า Port Switch ที่ SW1

- กำหนดให้ F0/1 และ F0/2 เป็นการเรียนรู้ mac address แบบ Sticky
  - *Switch0(Config-if)# switchport port-security*
  - *Switch0 (Config-if)# switchport port-security mac-address sticky*
- กำหนดให้ G0/1 เป็นการเรียนรู้ mac address แบบ Sticky สูงสุดจำนวน 3 mac addresses และมี Violation mode แบบ restrict
  - *Switch0 (Config-if)# switchport port-security*
  - *Switch0 (Config-if)# switchport port-security maximum 3*
  - *Switch0 (Config-if)# switchport port-security mac-address sticky*
  - *Switch0 (Config-if)# switchport port-security violation restrict*

4) สามารถตรวจสอบค่าและลบค่าใน Sticky สำหรับ Port Security ที่กำหนดไปด้วยคำสั่ง

- *Switch# show port-security*
- *Switch# show port-security interface fastethernet 0/1*
- *Switch# show port-security address*
- *Switch# clear port-security sticky*

iii. Checkpoint#1 ทำการสร้างและเชื่อมต่อเครือข่ายคอมพิวเตอร์ตาม Topology ที่กำหนดและ

1) ให้ Ping เรียงลำดับจาก และบอกว่าทำไมการ Ping จาก PC3 ไป PC0 ที่เป็นลำดับสุดท้ายไม่สามารถติดต่อได้
   a. PC0 ไป PC2
   b. PC1 ไป PC2
   c. PC2 ไป PC0

d. PC3 ไป PC0

2) ทดลองให้ **PC1** เปลี่ยนไปต่อ **Port F0/1** ของ Switch0 แล้วลอง Ping ไป PC2 ที่เคยติดต่อได้ และแสดงผลลัพธ์ที่เกิดขึ้นพร้อมอธิบายเหตุผล

3) ลองสลับกลับให้ **PC0** ไปต่อ **Port F0/1** ของ Switch0 อีกครั้ง แล้วให้ Ping ติดต่อไป PC2 ให้ได้เหมือนเดิม

iv. <u>คำถามหลังการทดลอง การเกิด shutdown จาก Violation shutdown mode เป็นการ shutdown ที่เป็น Stage ใด</u>

.....

.....

.....

.....

แบบฝึกปฏิบัติการที่ 9.2 ACL

i. Topology

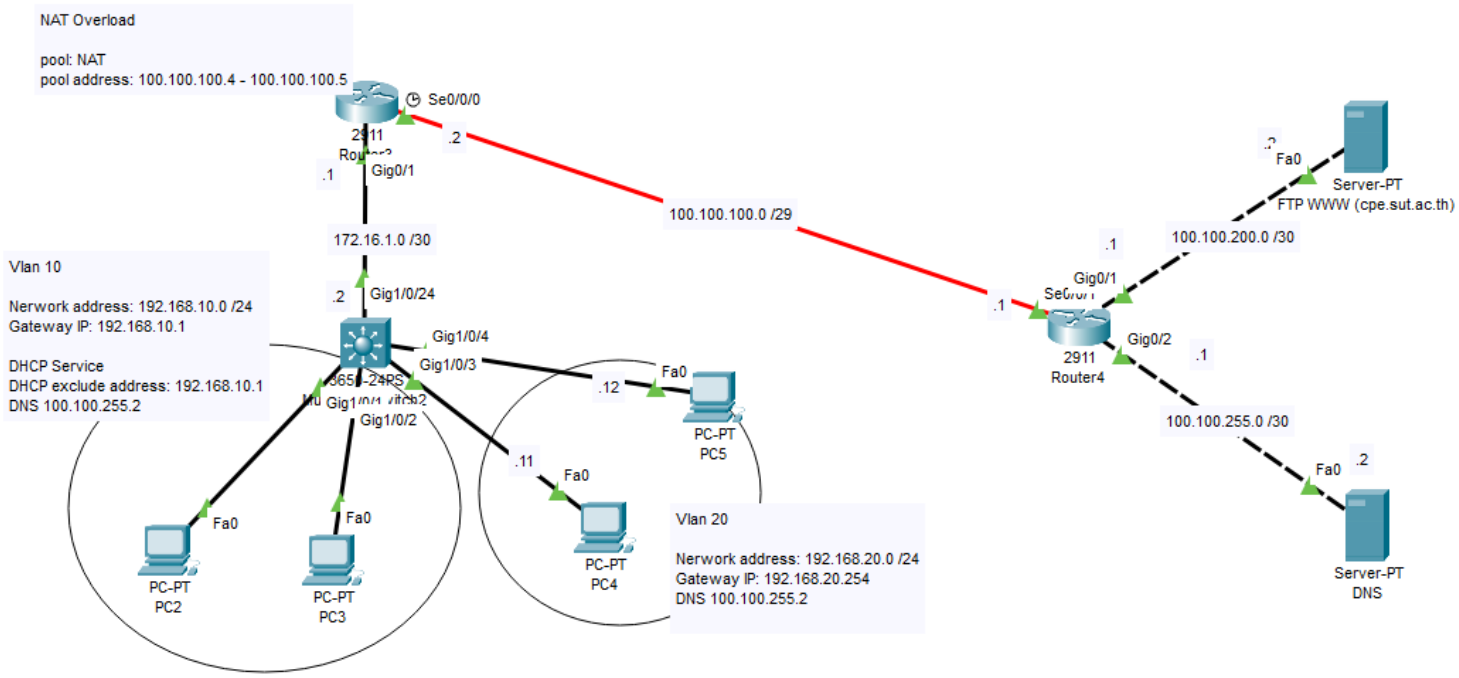

Figure 2 Lab 9.2

ii. คำอธิบายแบบฝึกปฏิบัติการที่ 9.2

1) **cpe.sut.ac.th (เป็นทั้ง FTP และ Web server), DNS server ไม่จำเป็นต้องกำหนดค่า แต่สามารถตรวจสอบความถูกต้องได้**
2) **ใช้แต่ Static Routing ไม่มีการใช้ Dynamic Routing ใน Lab9.2**
3) **กำหนดค่าที่ Router3 ตาม Figure 2 (ระวังเรื่อง Network Address และ NetMask ด้วย)**

   - กำหนดค่า NAT แบบ Overload โดย G0/1 เป็น nat inside และ Se0/0/0 เป็น nat outside
     a. NAT pool มี 2 public addresses คือ 100.100.100.4 และ 100.100.100.5 netmask 255.255.255.248 (คือ /29)
   - กำหนด Static Routing ให้ติดต่อกับ Server ทั้งสองได้ และทางกลับกัน Server ทั้งสองจะติดต่อกับ Vlan10 และ Vlan20 ได้เช่นกัน

4) **กำหนดค่าที่ Router4 ตาม Figure 2 (ระวังเรื่อง Network Address และ NetMask ด้วย)**

   - กำหนด Static Route ให้ถูกต้อง

5) กำหนดค่าที่ Multilayer Switch ตาม Figure 2 (ระวังเรื่อง Network Address และ NetMask ด้วย)

- กำหนด Vlan 10 ให้ G1/0/1 และ G1/0/2
- กำหนด Vlan 20 ให้ G1/0/3 และ G1/0/4
- กำหนด Switch Virtual Interface (SVI) ซึ่งเป็น Logical Interface เพื่อให้ L3 Switch สามารถกำหนด IP address ที่ Logical Interface ไว้เป็น Default Gateway ให้กับ Vlan10 และ Vlan 20
  - *Switch0(Config)# interface vlan 10*
  - *Switch0(Config-if)# ip address 192.168.10.1 255.255.255.0*
  - ลองกำหนดเองให้ *Vlan 20*
- กำหนด IP address ให้กับ g1/0/24 เพื่อทำงานแบบ Layer 3 FastEthernet port (ไม่ต้องมี Vlan)
  - *Switch0(Config)# interface g1/0/24*
  - *Switch0(Config-if)# no switchport*
  - *Switch0(Config-if)# ip address 172.16.1.2 255.255.255.252*
- กำหนด Static Route (อย่าลืมเปิด ip routing)
- กำหนดค่าในส่วน DHCP ให้กับเฉพาะ Vlan10 สำหรับค่า IP address, Default Gateway และ DNS Server
  - *Switch0(Config)# ip dhcp excluded-address 192.168.10.1*
  - *Switch0(Config)# ip dhcp pool VLAN10*
  - *Switch0(dhcp-config)# network 192.168.10.0 255.255.255.0*
  - *Switch0(dhcp-config)# default-router <ip_address_*ที่ต้องการให้เป็น*DefaultGateway>*
  - *Switch0(dhcp-config)# dns-server <ip_address_DNS_Server>*

6) กำหนดค่า Access Control Lists แบบ Extended Numbered 110 ที่ Router3 โดยมีเงื่อนไขดังนี้

Port Number(s)	Protocol	Application	access-list Command Keyword
20	TCP	FTP data	ftp-data
21	TCP	FTP control	ftp
22	TCP	SSH	—
23	TCP	Telnet	telnet
25	TCP	SMTP	smtp
53	UDP, TCP	DNS	domain
67	UDP	DHCP Server	bootps
68	UDP	DHCP Client	bootpc
69	UDP	TFTP	tftp
80	TCP	HTTP (WWW)	www
110	TCP	POP3	pop3
161	UDP	SNMP	snmp
443	TCP	SSL	—
514	UDP	Syslog	—
16,384–32,767	UDP	RTP (voice, video)	—

- Deny ทุกการติดต่อจาก PC5
  - *Router3(Config)# access-list 110 deny ip host 192.168.20.12 any*
- Deny เฉพาะ DNS สำหรับ Vlan20
  - *Router3(Config)# access-list 110 deny udp 192.168.20.0 0.0.0.255 host 100.100.255.2 eq domain*
- Deny ทุกการเชื่อมต่อที่เป็น ICMP
- Permit จากเชื่อมต่อจาก Vlan10 และ Vlan20 สำหรับกรณีอื่นนอกจากที่กำหนดข้างบน
  - *Router3(Config)# access-list* 110 *permit ip* 192.168.10.0 0.0.0.255 *any*
  - *Router3(Config)# access-list* 110 *permit ip* 192.168.20.0 0.0.0.255 *any*
- กำหนด Extended Numbered ACL ที่ G0/1 เป็น inbound
  - *Router3(Config-if)# ip access-group 110 in*

7) กำหนดค่า Access Control Lists แบบ Extended Named ACL ที่ Router4 โดยมีเงื่อนไขดังนี้

- Permit เฉพาะ www จาก Public IP จาก Vlan10, Vlan20 และให้ FTP จาก DNS Server เท่านั้น
  - *Router4(Config)# ip access-list extended FTP_WWW_SERVER*
  - *Router4(Config-ext-nacl)# permit tcp 100.100.100.0 0.0.0.7 host 100.100.200.2 eq www*
  - *Router4(Config-ext-nacl)# permit tcp host* 100.100.255.2 *host* 100.100.200.2 *eq ftp*
- Deny ทุกการเชื่อมต่อที่เป็น ICMP จาก Network ฝั่งซ้าย (รวม Router3) ทั้งหมด แต่ Permit อย่างอื่น
  - *Router4(Config)# ip access-list extended DENY_ICMP*
  - ลองกำหนดเอง

- Permit สำหรับ DNS จากทุกที่รวมถึง Network ฝั่งซ้าย (Router3, Vlan10 และ Vlan20) และจาก cpe.sut.ac.th
  - *Router4(Config)# ip access-list extended ALLOW_DNS_SERVER*
  - ลองกำหนดเอง
- กำหนด Named ACL FTP_WWW_SERVER ที่ G0/1 เป็น outbound
  - *Router3(Config-if)# ip access-group FTP_WWW_SERVER out*
- กำหนด Named ACL DENY_ICMP ที่ S0/0/1 เป็น inbound
- กำหนด Named ACL ALLOW_DNS_SERVER ที่ G0/2 เป็น outbound

8) สามารถตรวจสอบค่า ACL ที่กำหนดไปด้วยคำสั่ง

- *Router# show access-lists*

iii. Checkpoint#2 ทำตามเงื่อนไขข้างล่าง

1) PC2 และ DNS Server ทดลอง ftp ไปยัง 100.100.200.2 แล้วอธิบายทำไม PC2 ไม่สามารถใช้ ftp ได้ แล้วเกิดจากการกำหนดค่าที่ใด
2) ถ้าเปิด Web browser โดยใช้ PC4 ต้องกำหนด URL คืออะไรที่สามารถเปิดหน้าเว็บ cpe.sut.ac.th ได้

3) ถ้าจะให้ Router3 สามารถ Ping ไป Router4 ต้องทำอย่างไร (สามารถใช้การ Editing ACLs Using Sequence Numbers ใน Lecture มีสอน) **Hint:** เพิ่มที่ DENY_ICMP ที่เป็น inbound ได้

iv. <u>คำถามหลังการทดลอง</u> Port Security และ ACL แตกต่างกันอย่างไร

.....

.....