**รายงานหลังการทดลองปฏิบัติการที่ 9: ACL**

1. **กำหนดค่าตามขั้นตอนข้างล่างและส่งเป็น Lab9\_รหัสนักศึกษา.pkt มาใน Google Class พร้อมรายงานหลังการทดลอง**

* Download ไฟล์ Lab9HW\_Std.pkt จาก Google Classroom
* กำหนดค่าการเชื่อมต่อดังรูปที่ 1 Network Topology

Diagram

Description automatically generated

Figure

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

* กำหนดค่า NAT แบบ Overload โดย G0/1 เป็น nat inside และ Se0/0/0 เป็น nat outside
  1. 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

1. **กำหนดค่าที่ Router4 ตาม Figure 1 (ระวังเรื่อง Network Address และ NetMask ด้วย)**

* กำหนด Static Route ให้ถูกต้อง

1. **กำหนดค่าที่ Multilayer Switch ตาม Figure 1 (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\_ที่ต้องการให้เป็นDefaultGateway>
      * Switch0(dhcp-config)# dns-server <ip\_address\_DNS\_Server>

1. **กำหนดค่า Access Control Lists แบบ Extended Numbered 110 ที่ Router3 โดยมีเงื่อนไขดังนี้**

Table

Description automatically generated

* 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

1. **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

1. **สามารถตรวจสอบค่า ACL ที่กำหนดไปด้วยคำสั่ง**
   * + - Router# show access-lists
2. ใช้ PC2 และ DNS Server ทดลอง ftp ไปยัง 100.100.200.2 แล้วอธิบายทำไม PC2 ไม่สามารถใช้ ftp ได้ แล้วเกิดจากการกำหนดค่าที่ใด

Graphical user interface, text

Description automatically generated

FTP ได้แค่จาก DNS Server จากการ permit ของ ACL

**.......................................................................................................................................................................... .......................................................................................................................................................................... .......................................................................................................................................................................... ..........................................................................................................................................................................**

1. ถ้าเปิด Web browser โดยใช้ PC4 ต้องกำหนด URL คืออะไรที่สามารถเปิดหน้าเว็บ cpe.sut.ac.th ได้



**.......................................................................................................................................................................... .......................................................................................................................................................................... .......................................................................................................................................................................... .......................................................................................................................................................................... ..........................................................................................................................................................................**

ใช้ IP address แทนเพราะถูก block DNS ที่ VLAN20 คือ 100.100.200.2

1. ถ้าจะให้ Router3 สามารถ Ping ไป Router4 ต้องทำอย่างไร (สามารถใช้การ Editing ACLs Using Sequence Numbers ใน Lecture มีสอน) **Hint: เพิ่มที่ DENY\_ICMP ที่เป็น inbound ได้**

**............................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................. .................................................................................................................................................................................................................................................................................................................................................... ....................................................................................................................................................................................................................................................................................................................................................**

* เพิ่ม Permit ที่ ip access-list extended DENY\_ICMP ให้อยู่บนสุด โดยใช้ seq (ที่โชว์เลขด้านหน้า เช่น 10 20 30) ที่ต่ำกว่า เช่น 5
* Router4(Config)# ip access-list extended DENY\_ICMP
* Router4(Config-ext-nacl)# 5 permit icmp host 100.100.100.2 any