

กิจกรรมที่ 12 : Layer 2 Network

ในกิจกรรมนี้จะเป็นพื้นฐานที่สำคัญของการทำงานด้านระบบเครือข่าย คือ การทำความเข้าใจกับเรื่องของ ARP, VLAN และ MAC Address Learning

คำสั่ง arp

โปรโตคอล ARP ทำหน้าที่ในการค้นหา Physical Address (หรือ MAC Address) จาก IP Address เพื่อใช้ใน Destination Address ของ Ethernet Frame และเพื่อให้ง่ายการค้นหา (Name Resolution) โดยใช้ ARP ระบบปฏิบัติการจึงมีการสร้าง ARP Cache เอาไว้ด้วย

เมื่อเปิด command prompt และเรียกใช้คำสั่ง arp โดยจะแสดง option ในการทำงานดังนี้

- arp -a หรือ -g แสดง ARP Cache ที่มีในปัจจุบัน
- arp -d เป็นการลบข้อมูลใน ARP Cache ออก
- arp -s เป็นการเพิ่มข้อมูลชนิด static ลงใน cache

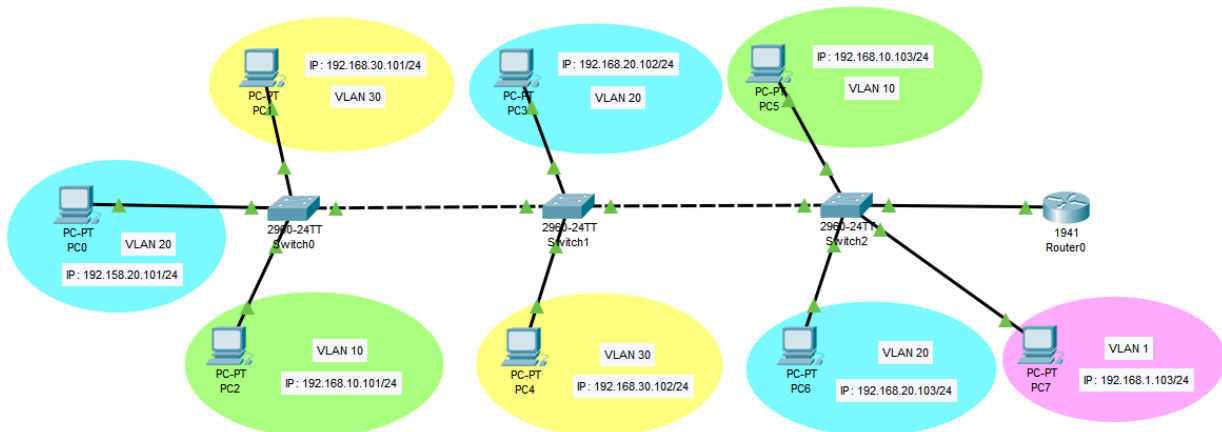
1. ให้ใช้คำสั่ง arp -a แสดงข้อมูลใน cache ค้นหาบรรทัดที่เป็น router ให้จดหมายเลข MAC Address ของ router เอาไว้
2. ใช้คำสั่ง arp -d (ต้องใช้สิทธิ์ admin) เพื่อลบข้อมูลออกจาก cache จากนั้นใช้คำสั่ง arp -a เรียกดูอีกครั้ง
3. ใช้คำสั่ง arp -s ip-address mac-address จากนั้นใช้คำสั่ง arp -d และ arp -a บันทึก screenshot มาแสดง

Virtual LAN

Virtual LAN เป็นเรื่องที่มีการใช้กันมากในระบบเครือข่ายคอมพิวเตอร์ เนื่องจากมีความยืดหยุ่นในการใช้งาน ทำให้เครื่องที่ต่อกับสวิตช์ต่างกัน หรือ กระทั่งต่างสถานที่สามารถทำงานร่วมกัน **เสมือน** ว่าอยู่ในเครือข่ายเดียวกัน ข้อมูลที่ Broadcast ใน VLAN จะสามารถเห็นได้จาก Host ที่อยู่ใน VLAN เดียวกันเท่านั้น เช่นเดียวกับ Host ที่อยู่ใน Subnet เดียวกัน จะเห็น Broadcast ที่มาจากภายใน Subnet เดียวกัน ดังนั้นอาจกล่าวได้ว่า 1 VLAN = 1 Subnet

จากแนวคิดข้างต้น ทำให้เราสามารถสร้างการติดต่อระหว่าง VLAN ได้ โดยใช้ Router คือ สามารถ Routing ระหว่าง VLAN โดยใช้ Router ซึ่งจะเรียกวิธีการนี้ว่า Inter VLAN Routing ซึ่งวิธีการจะไม่เหมือนกับ Routing ตามปกติเสียทีเดียว เนื่องจากในการทำงานแบบ Subnet เดิม นั้น จะต้องต้องมี 1 Interface ของ Router ที่อยู่ใน Subnet นั้น แต่ใน VLAN ไม่มีแบบนั้น จึงได้สร้าง sub Interface ซึ่งเป็น Interface **เสมือน** ขึ้นมา และกำหนดให้ Interface เสมือนนี้ อยู่ในแต่ละ VLAN ทำหน้าที่เป็น default gateway ของ แต่ละ VLAN และทำให้สามารถใช้ Router เพียง 1 Interface ในการ Routing ก็เครือข่ายก็ได้

4. ให้เปิดไฟล์ Lab12.pkt จะพบเครือข่ายดังรูป



เครือข่ายนี้จะมี Router จำนวน 1 ตัว Ethernet Switch จำนวน 3 ตัว และ PC จำนวน 8 เครื่อง โดยมีข้อมูล การเชื่อมต่อดังนี้

Host	IP Address	Gateway	VLAN	Interface
PC 0	192.168.20.101/24	192.168.20.1	20	SW0 -> Fa0/2
PC 1	192.168.30.101/24	192.168.30.1	30	SW0 -> Fa0/1
PC 2	192.168.10.101/24	192.168.10.1	10	SW0 -> Fa0/3
PC 3	192.168.20.102/24	192.168.20.1	20	SW1 -> Fa0/2
PC 4	192.168.30.102/24	192.168.30.1	30	SW1 -> Fa0/1
PC 5	192.168.10.103/24	192.168.10.1	10	SW2 -> Fa0/1
PC 6	192.168.20.103/24	192.168.20.1	20	SW2 -> Fa0/2
PC 7	192.168.1.103/24	192.168.1.1	1	SW2 -> Fa0/3

โดย Switch Configuration มีดังนี้

Switch0 Configuration

Port	Connected To	VLAN	Link
Fa0/1	PC 1	30	
Fa0/2	PC 0	20	
Fa0/3	PC 2	10	
Gig0/1	Switch 1	10,20,30	
Gig0/2	-	-	

Switch1 Configuration

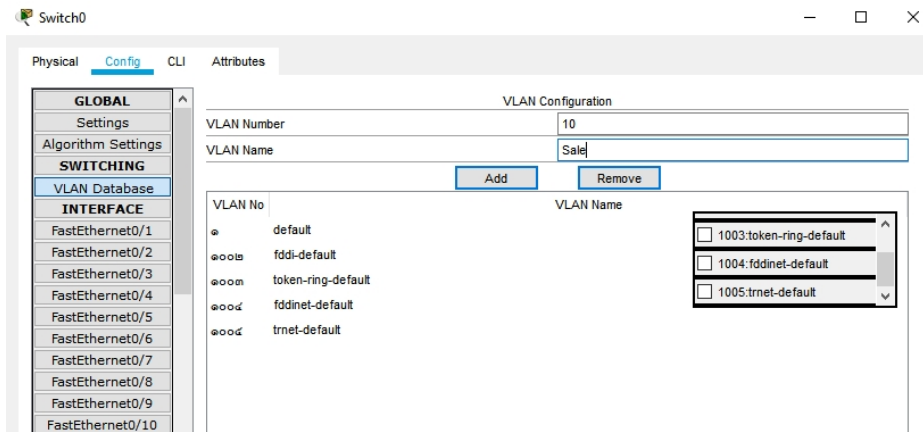
Port	Connected To	VLAN	Link
Fa0/1	PC 4	30	
Fa0/2	PC 3	20	
Gig0/1	Switch 0	10,20,30	
Gig0/2	Switch 2	10,20,30	

Switch2 Configuration

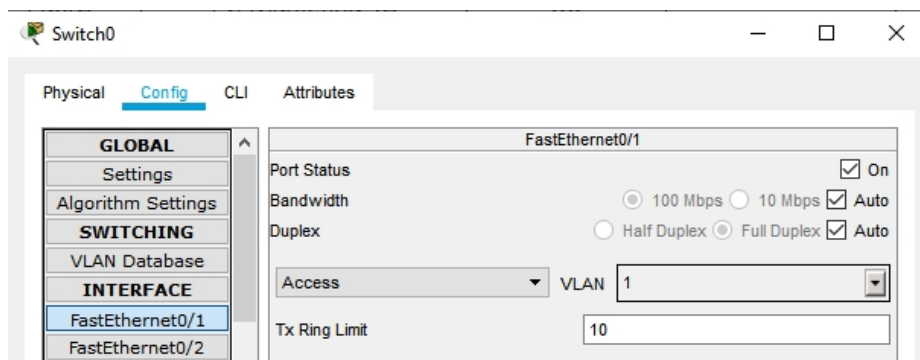
Port	Connected To	VLAN	Link
Fa0/1	PC 5	10	
Fa0/2	PC 6	20	
Fa0/3	PC 7	1	
Gig0/1	Router	10,20,30	
Gig0/2	Switch 1	10,20,30	

5. ทดลอง ping ระหว่าง Host ที่ต่อกับ Switch ตัวเดียวกัน สามารถ ping กันได้หรือไม่ เพราะเหตุใด

6. จากตารางของ Switch ข้างต้น ให้บอกลงในช่อง Link ว่า Link ใดเป็นชนิด Access หรือ Trunk
7. คลิกที่ Switch0 เลือก VLAN Database ให้เพิ่ม VLAN 10 ชื่อ Sale ตามรูป และให้เพิ่ม VLAN 20 ชื่อ Engineer และ VLAN 30 ชื่อ Marketing ด้วย และทำเช่นเดียวกันนี้กับ Switch อีก 2 ตัวที่เหลือ

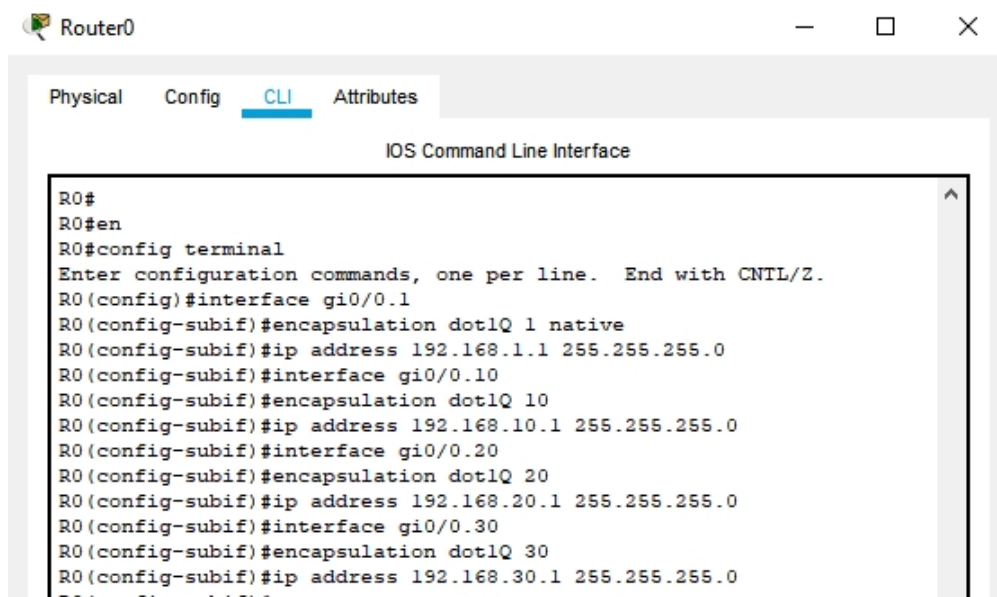


8. คลิกที่ Switch0 และเลือก Config -> FastEthernet0/1 จากนั้นให้กำหนดชนิดของ Link และ VLAN ตามตารางข้างต้น ให้ครบทุก Switch



9. ทดลอง ping ระหว่าง Host ที่อยู่ใน VLAN เดียวกัน หากสามารถ ping กันได้แสดงว่า config ถูก ให้บันทึก screenshot มาแสดงทั้ง 3 VLAN และตรวจสอบว่า ping ข้าม VLAN ได้หรือไม่

10. ต่อไปจะเป็นการสร้าง sub interface ให้คลิกที่ Router 0 แล้วป้อน config ต่อไปนี้



```
Router0
Physical Config CLI Attributes
IOS Command Line Interface
R0#
R0#en
R0#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#interface gi0/0.1
R0(config-subif)#encapsulation dot1Q 1 native
R0(config-subif)#ip address 192.168.1.1 255.255.255.0
R0(config-subif)#interface gi0/0.10
R0(config-subif)#encapsulation dot1Q 10
R0(config-subif)#ip address 192.168.10.1 255.255.255.0
R0(config-subif)#interface gi0/0.20
R0(config-subif)#encapsulation dot1Q 20
R0(config-subif)#ip address 192.168.20.1 255.255.255.0
R0(config-subif)#interface gi0/0.30
R0(config-subif)#encapsulation dot1Q 30
R0(config-subif)#ip address 192.168.30.1 255.255.255.0
```

11. ทดลอง ping ระหว่าง Host ทั้งใน VLAN เดียวกัน และข้าม VLAN ทั้ง VLAN 10, 20, 30 ให้บันทึก screenshot มาแสดง

MAC Address Learning

เป็นฟังก์ชันสำคัญของ Switch โดยทำหน้าที่ Learn เพื่อให้ทราบว่า Host ใดต่ออยู่ที่ Interface (Port) ใด และหากมี Frame ที่ส่งถึง Host นั้นจะส่งออกจาก Interface นั้นเพียง Interface เดียว ทำให้ลดปริมาณ Traffic ในระบบเครือข่าย และเพิ่มความปลอดภัยในการใช้งาน

เราสามารถดูข้อมูล MAC Address Table โดยใช้คำสั่ง *show mac address-table interface f0/1* เพื่อแสดง MAC Address Table ของ Interface นั้น

12. คลิกที่ Switch ตัวใดตัวหนึ่ง แล้วใช้คำสั่ง *clear mac-address-table* เพื่อลบ MAC Address Table ที่มีอยู่ในสวิตช์นั้น
13. เลือก PC ที่ต่อกับ Switch นั้น ตรวจสอบว่าต่ออยู่ที่ Interface ใด แล้วใช้คำสั่ง *show mac address-table interface* กับ Interface นั้น ตรวจสอบว่ามีข้อมูลใน MAC Address Table หรือไม่
14. ให้ ping จาก PC ไปยัง host ใดๆ แล้วใช้คำสั่ง *show mac address-table interface* เพื่อตรวจสอบตาราง MAC Address Table
15. ให้ตรวจสอบที่ Switch ปลายทางว่ามีข้อมูลใน MAC Address Table หรือไม่ อย่างไร
16. ให้สรุปการทำงานของ MAC Address Learning ตามข้อ 12-15 พร้อมภาพ screenshot มาประกอบ

งานครั้งที่ 12

- การส่งงาน เขียนหรือพิมพ์ลงในเอกสารนี้ และส่งเป็นไฟล์ PDF เท่านั้น
- ตั้งชื่อไฟล์โดยใช้รหัสนักศึกษา ตามด้วย section และ _lab12 ตามตัวอย่างต่อไปนี้
64019999_sec20_lab12.pdf
- กำหนดส่ง ภายในวันที่ 5 พฤษภาคม 2566 โดยให้ส่งใน Microsoft Teams ของรายวิชา