Secure & Scalable VLAN Design (Router-on-a-Stick)

1. สมาชิกกลุ่มและหน้าที่รับผิดชอบ (Team Members & Roles)

กลุ่มของพวกเรามีการแบ่งหน้าที่ความรับผิดชอบเพื่อให้การปฏิบัติการเป็นไปอย่างมีประสิทธิภาพ ดังนี้:

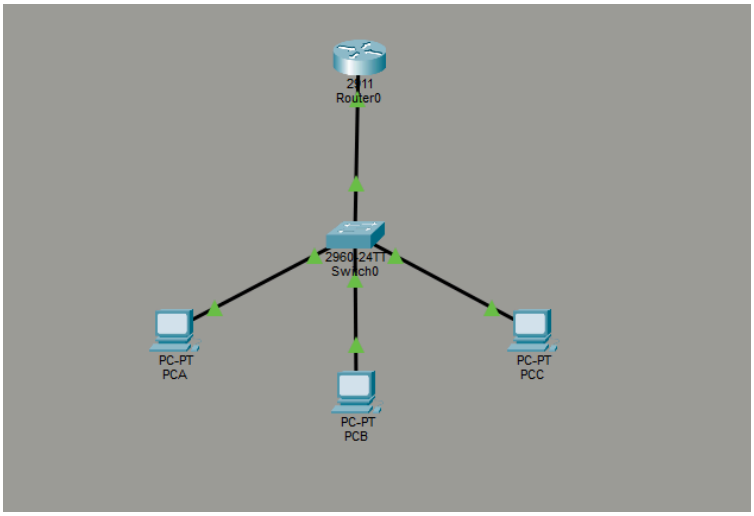
1. **บิ๊ก (Switch Architect)**
    - **หน้าที่:** รับผิดชอบการออกแบบและตั้งค่า Switch (Part 1) รวมถึงการสร้าง VLAN 10, 20, 99 และกำหนด Access/Trunk Ports
2. **อาร์ต (Router Specialist)**
    - **หน้าที่:** รับผิดชอบการตั้งค่า Router-on-a-Stick (Part 2) สร้าง Sub-interfaces และกำหนด Encapsulation dot1Q สำหรับการทำ Inter-VLAN Routing
3. **โฟน (Security Analyst)**
    - **หน้าที่:** รับผิดชอบหัวข้อ Security (Part 1, Step 3) โดยการจัดการพอร์ตที่ไม่ได้ใช้งาน (Unused Ports) ให้ย้ายไป Blackhole VLAN และสั่ง Shutdown เพื่อความปลอดภัย
4. **โฟร์ (Troubleshooter)**
    - **หน้าที่:** รับผิดชอบการจำลองสถานการณ์ปัญหา (Part 5) เช่น การกำหนด VLAN ผิด หรือลืมตั้งค่า Trunk และสาธิตวิธีการแก้ไขปัญหา
5. **แทน (Documentation & Verification)**
    - **หน้าที่:** ผู้จัดทำเอกสารและตรวจสอบระบบ รับผิดชอบการกำหนด IP Address ให้เครื่องลูกข่าย (Part 3) ทดสอบการเชื่อมต่อ (Ping Test) บันทึกผลการทดลอง และตอบคำถามท้ายบท

2. วัตถุประสงค์การทดลอง (Objectives)

1. เพื่อออกแบบและตั้งค่า VLANs (Virtual LANs) บน Switch เพื่อแบ่งกลุ่มเครือข่าย
2. เพื่อประยุกต์ใช้เทคนิค **Router-on-a-Stick** ในการทำ Inter-VLAN Routing ให้เครือข่ายต่างวงคุยกันได้
3. เพื่อเรียนรู้การจัดสรร IP Address แบบ Subnetting (/26)
4. เพื่อเพิ่มความปลอดภัยให้ระบบเครือข่ายโดยการจัดการพอร์ตที่ไม่ได้ใช้งาน (Port Security)
5. เพื่อตรวจสอบและแก้ไขปัญหาการเชื่อมต่อ Layer 2 และ Layer 3

3. อุปกรณ์และการเชื่อมต่อ (Topology & Addressing)

3.1 แผนภาพเครือข่าย (Network Topology)



3.2 ตารางกำหนดที่อยู่เครือข่าย (Addressing Table)

- **Major Network:** 192.168.10.0/24
- **Subnet Mask:** 255.255.255.192 (/26)

Device	Interface	VLAN	IP Address	Subnet Mask	Gateway
R1	G0/0.10	10	192.168.10.1	255.255.255.192	N/A
R1	G0/0.20	20	192.168.10.65	255.255.255.192	N/A
R1	G0/0.99	99	192.168.10.129	255.255.255.192	N/A
S1	VLAN 99	99	192.168.10.131	255.255.255.192	192.168.10.129
PC-A	NIC	10	192.168.10.10	255.255.255.192	192.168.10.1
PC-B	NIC	20	192.168.10.70	255.255.255.192	192.168.10.65
PC-C	NIC	99	192.168.10.130	255.255.255.192	192.168.10.129

4. ขั้นตอนและผลการทดลอง (Procedure & Results)

ส่วนที่ 1: การตั้งค่า Switch และ VLAN (Switch Configuration)

ผู้รับผิดชอบ: บิ๊ก & โฟน

ได้ดำเนินการตั้งค่า Switch S1 ดังนี้:

1. **สร้าง VLAN:** สร้าง VLAN 10 (USERS), 20 (SERVERS), 99 (MANAGEMENT), และ 999 (BLACKHOLE)
2. **Security:** ย้ายพอร์ตที่ไม่ได้ใช้ (Fa0/4-24) ไปยัง VLAN 999 และสั่ง Shutdown เพื่อความปลอดภัย
3. **Access Ports:** กำหนดพอร์ต Fa0/1 เป็น VLAN 10, Fa0/2 เป็น VLAN 20 และ Fa0/3 เป็น VLAN 99
4. **Trunk Port:** ตั้งค่าพอร์ต G0/1 ให้เป็น Trunk Mode (เชื่อมต่อกับ Router) และอนุญาตเฉพาะ VLAN ที่จำเป็น

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gig0/2
10   USERS                             active    Fa0/1
20   SERVERS                           active    Fa0/2
99   MANAGEMENT                        active    Fa0/3
999  BLACKHOLE                         active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

ส่วนที่ 2: การตั้งค่า Router-on-a-Stick (Router Configuration)

ผู้รับผิดชอบ: อาร์ต

ได้ดำเนินการตั้งค่า Router R1 เพื่อทำหน้าที่เป็น Gateway ให้กับทุก VLAN:

1. เปิดใช้งานพอร์ต G0/0 (no shutdown)
2. สร้าง **Sub-interfaces** (G0/0.10, G0/0.20, G0/0.99)
3. ตั้งค่า **Encapsulation dot1Q** ให้ตรงกับหมายเลข VLAN และกำหนด IP Address ตามตาราง

```
R1>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/0.10  192.168.10.1    YES manual up                    up
GigabitEthernet0/0.20  192.168.10.65   YES manual up                    up
GigabitEthernet0/0.99  192.168.10.129  YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
```

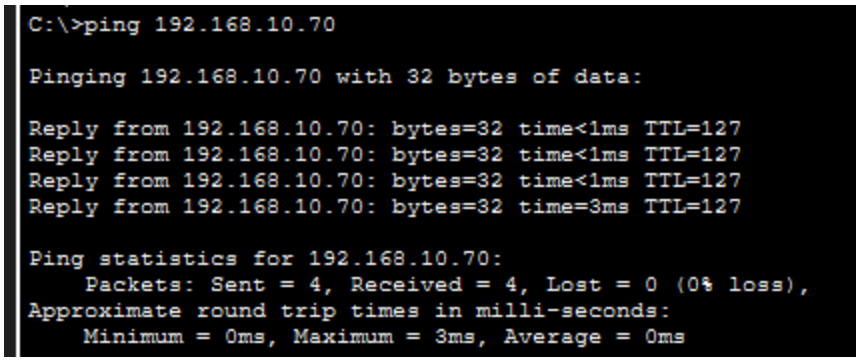
ส่วนที่ 3 & 4: การตั้งค่าเครื่องลูกข่ายและตรวจสอบผล (Verification)

ผู้รับผิดชอบ: แทน

หลังจากตั้งค่า IP Address, Subnet Mask (/26), และ Default Gateway ให้กับ PC-A, PC-B และ PC-C เรียบร้อยแล้ว ได้ทำการทดสอบการเชื่อมต่อดังนี้:

ผลการตรวจสอบ (Worksheet 1: Configuration Check)

Checkpoint	Command	Expected Result	Actual Result	Pass/Fail
VLANs exist	show vlan brief (S1)	พบ VLAN 10, 20, 99	พบครบทุก VLAN	**Pass**
Trunk active	show int trunk (S1)	VLANs allowed 10,20,99	Allowed และ Status Trunking	**Pass**
Router subifs	show ip int br (R1)	Up/Up ทั้ง 3 sub-int	Status Up / Protocol Up	**Pass**
Inter-VLAN ping	ping 192.168.10.70	Success	Reply from 192.168.10.70...	**Pass**



ส่วนที่ 5: การแก้ปัญหาเครือข่าย (Troubleshooting Challenge)

ผู้รับผิดชอบ: โฟร์

จำลองสถานการณ์ปัญหา **"Scenario A: Wrong VLAN Assignment"**

- **ปัญหา:** ย้าย PC-B ไปอยู่ผิด VLAN (เช่น VLAN 10 แทนที่จะเป็น 20)
- **อาการ:** PC-B ไม่สามารถ Ping หา Gateway หรือเครื่องอื่นได้ เพราะ IP Address อยู่คนละ Subnet กับ VLAN ที่พอร์ตสังกัดอยู่
- **การแก้ไข:** ย้ายพอร์ต Fa0/2 กลับมาที่ VLAN 20 (switchport access vlan 20)

ping จาก PC-B ไป PC-A

```
S1>enable
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#
S1(config)#interface fa0/2
S1(config-if)#
S1(config-if)# switchport access vlan 10
S1(config-if)#
S1(config-if)#
S1(config-if)#
S1(config-if)# switchport access vlan 10
S1(config-if)#switchport access vlan 10
S1(config-if)#switchport access vlan 10
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

```
C:\>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

5. คำถามท้ายการทดลอง (Worksheet 2 & Assessment)

1. Why is VLAN 99 used for management? (ทำไมถึงใช้ VLAN 99 เพื่อการจัดการ?)

- **ตอบ:** เพื่อแยก Traffic การบริหารจัดการอุปกรณ์ (Management Traffic) ออกจาก Traffic ของผู้ใช้งานทั่วไป (User Data) เพิ่มความปลอดภัยและความเสถียรในการเข้าถึงอุปกรณ์

2. Why is VLAN 999 assigned to unused ports? (ทำไมต้องย้ายพอร์ตว่างไป VLAN 999?)

- **ตอบ:** เป็นมาตรการความปลอดภัย (Security Best Practice) หากมีผู้ประสงค์ร้ายแอบเสียบสายแลนเข้าพอร์ตว่าง จะไม่สามารถเข้าถึงเครือข่ายหลักได้ เพราะถูกขังอยู่ใน VLAN ที่ไม่มีการใช้งาน (Blackhole)

3. Which device performs inter-VLAN routing? (อุปกรณ์ใดทำหน้าที่เชื่อมต่อระหว่าง VLAN?)

- **ตอบ: Router R1** โดยใช้วิธี Router-on-a-Stick ผ่าน Sub-interfaces

4. What does 802.1Q tagging do? (การ Tag 802.1Q มีหน้าที่อะไร?)

- **ตอบ:** ทำหน้าที่แปะป้าย (Tag) หมายเลข VLAN ลงในเฟรมข้อมูลเมื่อวิ่งผ่านสาย Trunk เพื่อให้ Switch หรือ Router ปลายทางทราบว่าข้อมูลนี้มาจาก VLAN ไหน

6. สรุปผลการทดลอง (Conclusion)

จากการปฏิบัติการ Lab 2 กลุ่มของข้าพเจ้าสามารถออกแบบและติดตั้งเครือข่ายที่มีความปลอดภัยและรองรับการขยายตัวได้สำเร็จ โดยสมาชิกทุกคนได้ปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย:

- **บิ๊ก** จัดการเรื่อง VLAN บน Switch ได้อย่างถูกต้อง
- **อาร์ต** ตั้งค่า Router ให้ทำหน้าที่เป็น Gateway เชื่อมทุก VLAN เข้าด้วยกัน
- **โฟน** ช่วยเพิ่มความปลอดภัยให้ระบบโดยการปิดพอร์ตที่ไม่ได้ใช้
- **โฟร์** สาธิตการแก้ปัญหาเมื่อเกิดข้อผิดพลาดในการตั้งค่า VLAN
- **แทน** ตรวจสอบความถูกต้องและรวบรวมข้อมูลทั้งหมด

ผลลัพธ์สำคัญคือเครื่องคอมพิวเตอร์ที่อยู่ต่าง VLAN (VLAN 10 และ 20) สามารถสื่อสารกันได้ผ่าน Router (Inter-VLAN Routing) และระบบมีความปลอดภัยจากการแยก Management VLAN และการจัดการ Unused Ports