การสื่อสารข้อมูล เครือข่ายคอมพิวเตอร์ และอินเทอร์เน็ต

บทที่ 1: รูปแบบและแนวทางในการจัดการระบบเครือข่าย

- ความหมายของการจัดการเครือข่าย
- ประเภทของการจัดการเครือข่าย (Network Management Types)
- การวางแผนเครือข่ายเบื้องต้น
- การออกแบบเครือข่ายและการวางแผนโครงสร้าง
- องค์ประกอบหลักของระบบเครือข่าย
- เครื่องมือและซอฟต์แวร์ที่ใช้ในการจัดการเครือข่าย

บทที่ 2: การตรวจสอบและการตั้งสมมติฐาน

- ความสำคัญของการตรวจสอบเครือข่าย
- เครื่องมือการตรวจสอบเครือข่ายเบื้องต้น (Network Monitoring Tools)
- วิธีการตรวจสอบระบบเครือข่าย
- การตั้งสมมติฐานในการวิเคราะห์ปัญหาเครือข่าย
- เทคนิคการเก็บรวบรวมข้อมูลเพื่อการวิเคราะห์
- การใช้โปรแกรมและอุปกรณ์ในการตรวจสอบเครือข่าย

บทที่ 3: การวิเคราะห์หาสาเหตุของข้อผิดพลาด

- ความหมายของข้อผิดพลาดในระบบเครือข่าย
- ประเภทของข้อผิดพลาดที่พบบ่อยในเครือข่าย
- วิธีการวิเคราะห์ข้อผิดพลาดเบื้องต้น
- การใช้เครื่องมือวิเคราะห์ข้อผิดพลาด
- เทคนิคการแยกและวินิจฉัยข้อผิดพลาด
- การสร้างรายงานการวิเคราะห์ข้อผิดพลาด

บทที่ 4: การแก้ไขและป้องกันปัญหาเครือข่าย

- วิธีการแก้ไขปัญหาที่พบในระบบเครือข่าย
- การป้องกันปัญหาเครือข่ายเบื้องต้น
- แนวทางการปรับปรุงและพัฒนาเครือข่าย
- การประยุกต์ใช้เทคนิคการป้องกันข้อผิดพลาด
- การปรับปรุงการทำงานของเครือข่ายเพื่อป้องกันปัญหา
- การใช้เครื่องมือและโปรแกรมในการแก้ไขปัญหา

บทที่ 5: เกณฑ์วิธีที่ใช้ในการจัดการระบบเครือข่าย (SNMP)

- พื้นฐานและการทำงานของ SNMP
- โครงสร้างของ SNMP และวิธีการทำงาน
- การติดตั้งและการกำหนดค่า SNMP
- การใช้ SNMP ในการจัดการเครือข่าย
- ข้อดีและข้อเสียของการใช้ SNMP
- การใช้โปรแกรมและเครื่องมือที่รองรับ SNMP

บทที่ 6: โปรแกรมและเครื่องมือต่างๆ ที่ใช้ในการจัดการระบบเครือข่าย

- โปรแกรมจัดการเครือข่ายยอดนิยม
- การติดตั้งโปรแกรมจัดการเครือข่าย
- การใช้งานโปรแกรมจัดการเครือข่าย
- เครื่องมือจัดการเครือข่ายที่ใช้บ่อย
- การเปรียบเทียบประสิทธิภาพของโปรแกรมและเครื่องมือต่างๆ
- การปรับแต่งโปรแกรมและเครื่องมือให้เหมาะสมกับการใช้งาน

บทที่ 7: การวัดปริมาณการใช้งาน

- การวัดปริมาณการใช้งานเครือข่ายคืออะไร
- ความสำคัญของการวัดปริมาณการใช้งาน
- เครื่องมือการวัดปริมาณการใช้งานเครือข่าย
- เทคนิคการวัดและการเก็บข้อมูล
- การวิเคราะห์และการรายงานผลการวัด
- การใช้ข้อมูลการวัดในการปรับปรุงประสิทธิภาพเครือข่าย

บทที่ 8: การปรับปรุงประสิทธิภาพของระบบเครือข่าย

- แนวทางการปรับปรุงประสิทธิภาพของระบบเครือข่าย
- การวิเคราะห์ประสิทธิภาพเครือข่าย
- การปรับแต่งการตั้งค่าเครือข่ายเพื่อเพิ่มประสิทธิภาพ
- การใช้เทคโนโลยีใหม่ๆ ในการปรับปรุงเครือข่าย
- การทดสอบและการวัดผลการปรับปรุง
- กรณีศึกษาเกี่ยวกับการปรับปรุงประสิทธิภาพเครือข่าย

ใบงานรายวิชา การสื่อสารข้อมูล เครือข่ายคอมพิวเตอร์และอินเทอร์เน็ต

ผู้สอน: ผู้ช่วยศาสตราจารย์อมร เจือตี๋

บทที่ 1: รูปแบบและแนวทางในการจัดการระบบเครือข่าย

1. จงอธิบายความหมายของการจัดการเครือข่ายและความสำคัญในการจัดการเครือข่าย

.....

.....

.....

.....

.....

.....

.....

.....

.....

2. ประเภทของการจัดการเครือข่ายมีอะไรบ้าง จงอธิบายและยกตัวอย่าง

.....

.....

.....

.....

.....

.....

.....

.....

3. จงอธิบายขั้นตอนการวางแผนเครือข่ายเบื้องต้น

.....

.....

.....

.....

.....

.....

.....

.....

.....

4. อธิบายโครงสร้างเครือข่าย (Network Topology) ที่นิยมใช้ในปัจจุบัน

.....

.....

.....

.....

.....

.....

.....

.....

.....

5. จงบอกองค์ประกอบหลักของระบบเครือข่ายและหน้าที่ของแต่ละองค์ประกอบ

.....

.....

.....

.....

.....

.....

.....

.....

.....

6. ให้ระบุเครื่องมือและซอฟต์แวร์ที่ใช้ในการจัดการเครือข่ายและวิธีการใช้งาน

.....

.....

.....

.....

.....

.....

.....

.....

.....

บทที่ 2: การตรวจสอบและการตั้งสมมติฐาน

1. จงอธิบายความสำคัญของการตรวจสอบเครือข่าย

.....

.....

.....

.....

.....

.....

.....

.....

.....

2. จงบอกชื่อเครื่องมือการตรวจสอบเครือข่ายเบื้องต้นที่คุณรู้จักและอธิบายการทำงานของเครื่องมือหนึ่งอย่าง

.....

.....

.....

.....

.....

.....

.....

.....

.....

3. อธิบายวิธีการตรวจสอบระบบเครือข่ายแบบเรียลไทม์ (Real-time Monitoring)

.....

.....

.....

.....

.....

.....

.....

.....

.....

4. จงอธิบายขั้นตอนการตั้งสมมติฐานในการวิเคราะห์ปัญหาเครือข่าย

.....

.....

.....

.....

.....

.....

.....

.....

.....

5. จงบอกเทคนิคการเก็บรวบรวมข้อมูลเพื่อการวิเคราะห์

.....

.....

.....

.....

.....

.....

.....

.....

.....

6. ให้อธิบายการใช้โปรแกรมและอุปกรณ์ในการตรวจสอบเครือข่าย

.....

.....

.....

.....

.....

.....

.....

.....

.....

บทที่ 3: การวิเคราะห์หาสาเหตุของข้อผิดพลาด

1. จงอธิบายความหมายของข้อผิดพลาดในระบบเครือข่าย

.....

.....

.....

.....

.....

.....

.....

.....

.....

2. จงบอกประเภทของข้อผิดพลาดที่พบบ่อยในเครือข่ายและวิธีการแก้ไข

.....

.....

.....

.....

.....

.....

.....

.....

.....

3. จงอธิบายวิธีการวิเคราะห์ข้อผิดพลาดเบื้องต้น

.....

.....

.....

.....

.....

.....

.....

.....

.....

4. ให้อธิบายการใช้เครื่องมือวิเคราะห์ข้อผิดพลาดในระบบเครือข่าย

.....

.....

.....

.....

.....

.....

.....

.....

.....

5. จงบอกเทคนิคการแยกและวินิจฉัยข้อผิดพลาด

.....

.....

.....

.....

.....

.....

.....

.....

.....

6. ให้อธิบายขั้นตอนการสร้างรายงานการวิเคราะห์ข้อผิดพลาด

.....

.....

.....

.....

.....

.....

.....

.....

.....

บทที่ 4: การแก้ไขและป้องกันปัญหาเครือข่าย

1. จงบอกวิธีการแก้ไขปัญหาที่พบในระบบเครือข่าย

.....

.....

.....

.....

.....

.....

.....

.....

.....

2. อธิบายการป้องกันปัญหาเครือข่ายเบื้องต้น

.....

.....

.....

.....

.....

.....

.....

.....

.....

3. จงอธิบายแนวทางการปรับปรุงและพัฒนาเครือข่าย

.....

.....

.....

.....

.....

.....

.....

.....

.....

4. ให้อธิบายการประยุกต์ใช้เทคนิคการป้องกันข้อผิดพลาด

.....

.....

.....

.....

.....

.....

.....

.....

.....

5. จงบอกวิธีการปรับปรุงการทำงานของเครือข่ายเพื่อป้องกันปัญหา

.....

.....

.....

.....

.....

.....

.....

.....

.....

6. อธิบายการใช้เครื่องมือและโปรแกรมในการแก้ไขปัญหา

.....

.....

.....

.....

.....

.....

.....

.....

.....

บทที่ 5: เกณฑ์วิธีที่ใช้ในการจัดการระบบเครือข่าย (SNMP)

1. จงอธิบายพื้นฐานและการทำงานของ SNMP

.....

.....

.....

.....

.....

.....

.....

.....

.....

2. ให้อธิบายโครงสร้างของ SNMP และวิธีการทำงาน

.....

.....

.....

.....

.....

.....

.....

.....

.....

3. จงบอกขั้นตอนการติดตั้งและการกำหนดค่า SNMP

.....

.....

.....

.....

.....

.....

.....

.....

.....

4. อธิบายการใช้ SNMP ในการจัดการเครือข่าย

.....

.....

.....

.....

.....

.....

.....

.....

.....

5. จงบอกข้อดีและข้อเสียของการใช้ SNMP

.....

.....

.....

.....

.....

.....

.....

.....

.....

6. ให้อธิบายการใช้โปรแกรมและเครื่องมือที่รองรับ SNMP

.....

.....

.....

.....

.....

.....

.....

.....

.....

บทที่ 6: โปรแกรมและเครื่องมือต่างๆ ที่ใช้ในการจัดการระบบเครือข่าย

1. จงบอกชื่อโปรแกรมจัดการเครือข่ายยอดนิยมและอธิบายคุณสมบัติของโปรแกรมหนึ่งอย่าง

.....

.....

.....

.....

.....

.....

.....

.....

.....

2. จงอธิบายขั้นตอนการติดตั้งโปรแกรมจัดการเครือข่าย

.....

.....

.....

.....

.....

.....

.....

.....

.....

3. อธิบายการใช้งานโปรแกรมจัดการเครือข่าย

.....

.....

.....

.....

.....

.....

.....

.....

.....

4. ให้อธิบายเครื่องมือจัดการเครือข่ายที่ใช้บ่อยและการใช้งาน

.....

.....

.....

.....

.....

.....

.....

.....

.....

5. จงเปรียบเทียบประสิทธิภาพของโปรแกรมและเครื่องมือต่างๆ ที่คุณรู้จัก

.....

.....

.....

.....

.....

.....

.....

.....

.....

6. อธิบายการปรับแต่งโปรแกรมและเครื่องมือให้เหมาะสมกับการใช้งาน

.....

.....

.....

.....

.....

.....

.....

.....

.....

บทที่ 7: การวัดปริมาณการใช้งาน

1. จงอธิบายการวัดปริมาณการใช้งานเครือข่ายคืออะไร

.....

.....

.....

.....

.....

.....

.....

.....

.....

2. ให้อธิบายความสำคัญของการวัดปริมาณการใช้งานเครือข่าย

.....

.....

.....

.....

.....

.....

.....

.....

.....

3. จงบอกชื่อเครื่องมือการวัดปริมาณการใช้งานเครือข่ายและการทำงานของเครื่องมือหนึ่งอย่าง

.....

.....

.....

.....

.....

.....

.....

.....

.....

4. อธิบายเทคนิคการวัดและการเก็บข้อมูล

.....

.....

.....

.....

.....

.....

.....

.....

.....

5. ให้อธิบายการวิเคราะห์และการรายงานผลการวัด

.....

.....

.....

.....

.....

.....

.....

.....

.....

6. จงอธิบายการใช้ข้อมูลการวัดในการปรับปรุงประสิทธิภาพเครือข่าย

.....

.....

.....

.....

.....

.....

.....

.....

.....

บทที่ 8: การปรับปรุงประสิทธิภาพของระบบเครือข่าย

1. จงอธิบายแนวทางการปรับปรุงประสิทธิภาพของระบบเครือข่าย

.....

.....

.....

.....

.....

.....

.....

.....

.....

2. อธิบายการวิเคราะห์ประสิทธิภาพเครือข่าย

.....

.....

.....

.....

.....

.....

.....

.....

.....

3. จงบอกวิธีการปรับแต่งการตั้งค่าเครือข่ายเพื่อเพิ่มประสิทธิภาพ

.....

.....

.....

.....

.....

.....

.....

.....

.....

4. ให้อธิบายการใช้เทคโนโลยีใหม่ๆ ในการปรับปรุงเครือข่าย

.....

.....

.....

.....

.....

.....

.....

.....

.....

5. จงอธิบายขั้นตอนการทดสอบและการวัดผลการปรับปรุง

.....

.....

.....

.....

.....

.....

.....

.....

.....

6. อธิบายกรณีศึกษาเกี่ยวกับการปรับปรุงประสิทธิภาพเครือข่าย

.....

.....

.....

.....

.....

.....

.....

.....

.....

LAB 1: การตั้งค่า VLAN และการจัดการ VLAN บน Switch L2

ผู้สอน

ผู้ช่วยศาสตราจารย์อมร เจือตี๋
สาขาวิชาคอมพิวเตอร์ศึกษา คณะวิทยาศาสตร์และเทคโนโลยี

ชื่อ นามสกุล _____

หมู่เรียน _____

คะแนน _____

วัตถุประสงค์

1. เพื่อเรียนรู้การตั้งค่า VLAN บน Switch L2
2. เพื่อจัดการ VLAN ต่างๆ บนเครือข่าย

อุปกรณ์ที่ใช้

- Switch L2 (Cisco 2960)
- เครื่องคอมพิวเตอร์ (PC)
- สายเชื่อมต่อ (Straight-Through)

การออกแบบหมายเลข IP Address

อุปกรณ์	พอร์ต	VLAN	IP Address	Subnet Mask	Default Gateway
PC1	NIC	10	192.168.10.2	255.255.255.0	192.168.10.1
PC2	NIC	20	192.168.20.2	255.255.255.0	192.168.20.1

วิธีการทำ

1. **เปิดโปรแกรม Cisco Packet Tracer** และลากอุปกรณ์ Switch L2 (Cisco 2960) และ PC จำนวน 2 เครื่องไปวางในพื้นที่การทำงาน
    - เปิดโปรแกรม Cisco Packet Tracer
    - ลาก Switch L2 (Cisco 2960) และ PC 2 เครื่องไปวางในพื้นที่การทำงาน
2. **เชื่อมต่อสาย Straight-Through จากพอร์ต FastEthernet ของเครื่อง PC ไปยังพอร์ต FastEthernet ของ Switch L2**
    - ใช้สาย Straight-Through เชื่อมต่อจาก FastEthernet0 ของ PC1 ไปยัง FastEthernet0/1 ของ Switch L2
    - ใช้สาย Straight-Through เชื่อมต่อจาก FastEthernet0 ของ PC2 ไปยัง FastEthernet0/2 ของ Switch L2
3. **เปิด CLI ของ Switch L2 โดยคลิกขวาที่ Switch L2 และเลือก "CLI"**
    - คลิกขวาที่ Switch L2
    - เลือก "CLI"
4. **ใช้คำสั่ง CLI เพื่อสร้างและกำหนด VLAN**
    - สร้าง VLAN หมายเลข 10 และกำหนดชื่อ VLAN ว่า VLAN10

      ```
      Switch> enable
      Switch# configure terminal
      Switch(config)# vlan 10
      Switch(config-vlan)# name VLAN10
      Switch(config-vlan)# exit
      ```

    - สร้าง VLAN หมายเลข 20 และกำหนดชื่อ VLAN ว่า VLAN20

      ```
      Switch(config)# vlan 20
      Switch(config-vlan)# name VLAN20
      Switch(config-vlan)# exit
      ```

5. **กำหนดพอร์ตให้กับแต่ละ VLAN**
    - กำหนดพอร์ต FastEthernet 0/1 ถึง 0/4 ให้เป็น VLAN 10

      Switch(config)# interface range fastethernet 0/1 - 4
      Switch(config-if-range)# switchport mode access
      Switch(config-if-range)# switchport access vlan 10
      Switch(config-if-range)# exit

    - กำหนดพอร์ต FastEthernet 0/5 ถึง 0/8 ให้เป็น VLAN 20

      Switch(config)# interface range fastethernet 0/5 - 8
      Switch(config-if-range)# switchport mode access
      Switch(config-if-range)# switchport access vlan 20
      Switch(config-if-range)# exit
      Switch(config)# exit
      Switch# write memory

6. **ตั้งค่า IP Address และ Subnet Mask ให้กับเครื่อง PC**
    - เปิด PC1 > Desktop > IP Configuration
        - IP Address: 192.168.10.2
        - Subnet Mask: 255.255.255.0
        - Default Gateway: 192.168.10.1
    - เปิด PC2 > Desktop > IP Configuration
        - IP Address: 192.168.20.2
        - Subnet Mask: 255.255.255.0
        - Default Gateway: 192.168.20.1

7. **ทดสอบการเชื่อมต่อระหว่างเครื่อง PC ทั้งสองเครื่องด้วยคำสั่ง ping ใน Command Prompt**
    - เปิด Command Prompt บน PC1 และพิมพ์ ping 192.168.20.2
    - เปิด Command Prompt บน PC2 และพิมพ์ ping 192.168.10.2

สรุป

ใน LAB นี้ นักเรียนจะได้เรียนรู้การสร้างและจัดการ VLAN บน Switch L2 รวมถึงการตั้งค่า VLAN เพื่อแบ่งเครือข่ายออกเป็นส่วนย่อยๆ ซึ่งเป็นพื้นฐานสำคัญของการจัดการเครือข่าย

ประโยชน์ของ LAB

- ช่วยให้นักเรียนเข้าใจการแบ่งเครือข่ายออกเป็นหลายๆ VLAN เพื่อการจัดการที่ง่ายขึ้นและเพิ่มความปลอดภัย
- เรียนรู้วิธีการกำหนดค่า VLAN บน Switch L2
- สามารถทดสอบและวิเคราะห์การทำงานของ VLAN ในเครือข่ายจริง

LAB 2: การตั้งค่า VTP บน Switch L2

ผู้สอน

ผู้ช่วยศาสตราจารย์อมร เจือตี๋
สาขาวิชาคอมพิวเตอร์ศึกษา คณะวิทยาศาสตร์และเทคโนโลยี

ชื่อ นามสกุล _____

หมู่เรียน _____

คะแนน _____

วัตถุประสงค์

1. เพื่อเรียนรู้การตั้งค่าและจัดการ VTP (VLAN Trunking Protocol) บน Switch L2

อุปกรณ์ที่ใช้

- Switch L2 (Cisco 2960) จำนวน 2 ตัว
- เครื่องคอมพิวเตอร์ (PC)
- สายเชื่อมต่อ (Straight-Through, Cross-Over)

การออกแบบหมายเลข IP Address

อุปกรณ์	พอร์ต	VLAN	IP Address	Subnet Mask	Default Gateway
PC1	NIC	10	192.168.10.2	255.255.255.0	192.168.10.1
PC2	NIC	20	192.168.20.2	255.255.255.0	192.168.20.1

วิธีการทำ

1. **เปิดโปรแกรม Cisco Packet Tracer และสร้างการเชื่อมต่อระหว่าง Switch ทั้งสองและ PC**
    - เปิดโปรแกรม Cisco Packet Tracer
    - ลาก Switch L2 จำนวน 2 ตัวและ PC จำนวน 2 เครื่องไปวางในพื้นที่การทำงาน

2. **เชื่อมต่อสาย Cross-Over ระหว่างพอร์ต GigabitEthernet ของ Switch ทั้งสอง**
    - ใช้สาย Cross-Over เชื่อมต่อจาก GigabitEthernet0/1 ของ Switch1 ไปยัง GigabitEthernet0/1 ของ Switch2
3. **เปิด CLI ของ Switch โดยคลิกขวาที่ Switch และเลือก "CLI"**
    - คลิกขวาที่ Switch1 และ Switch2
    - เลือก "CLI"
4. **ตั้งค่า VTP Domain และ VTP Mode บน Switch แรก**
    - กำหนด VTP Domain เป็น mydomain และ VTP Mode เป็น Server

```
Switch1> enable
Switch1# configure terminal
Switch1(config)# vtp domain mydomain
Switch1(config)# vtp mode server
Switch1(config)# vtp password cisco
Switch1(config)# exit
Switch1# write memory
```

5. **ตั้งค่า VTP Client บน Switch ที่สอง**
    - กำหนด VTP Domain เป็น mydomain และ VTP Mode เป็น Client

```
Switch2> enable
Switch2# configure terminal
Switch2(config)# vtp domain mydomain
Switch2(config)# vtp mode client
Switch2(config)# vtp password cisco
Switch2(config)# exit
Switch2# write memory
```

6. **ทดสอบการเชื่อมต่อ VLAN โดยสร้าง VLAN บน Switch แรกและตรวจสอบว่า VLAN ถูกซิงค์ไปยัง Switch ที่สอง**
    - สร้าง VLAN หมายเลข 30 บน Switch1

      Switch1> enable
      Switch1# configure terminal
      Switch1(config)# vlan 30
      Switch1(config-vlan)# name VLAN30
      Switch1(config-vlan)# exit
      Switch1# exit
      Switch1# write memory

    - ตรวจสอบว่า VLAN 30 ถูกสร้างบน Switch2 โดยใช้คำสั่ง show vlan brief

      Switch2> enable
      Switch2# show vlan brief

สรุป

นักเรียนจะได้เรียนรู้การตั้งค่าและจัดการ VTP บน Switch L2 เพื่อให้สามารถกระจายข้อมูล VLAN ระหว่าง Switch หลายตัวได้อย่างมีประสิทธิภาพ

ประโยชน์ของ LAB

- ช่วยให้นักเรียนเข้าใจการกระจายข้อมูล VLAN ผ่าน VTP เพื่อการจัดการที่มีประสิทธิภาพมากขึ้น
- เรียนรู้วิธีการตั้งค่าและจัดการ VTP บน Switch L2
- เพิ่มความรู้เกี่ยวกับการประสานงานระหว่าง Switch หลายตัวในเครือข่าย

LAB 3: การตั้งค่า Trunk บน Switch L2

ผู้สอน

ผู้ช่วยศาสตราจารย์อมร เจือตี๋
สาขาวิชาคอมพิวเตอร์ศึกษา คณะวิทยาศาสตร์และเทคโนโลยี

ชื่อ นามสกุล _____

หมู่เรียน _____

คะแนน _____

วัตถุประสงค์

1. เพื่อเรียนรู้การตั้งค่า Trunk บน Switch L2 เพื่อให้สามารถส่งข้อมูล VLAN ได้หลาย VLAN ผ่านสายเชื่อมต่อเดียว

อุปกรณ์ที่ใช้

- Switch L2 (Cisco 2960) จำนวน 2 ตัว
- เครื่องคอมพิวเตอร์ (PC)
- สายเชื่อมต่อ (Straight-Through, Cross-Over)

การออกแบบหมายเลข IP Address

อุปกรณ์	พอร์ต	VLAN	IP Address	Subnet Mask	Default Gateway
PC1	NIC	10	192.168.10.2	255.255.255.0	192.168.10.1
PC2	NIC	20	192.168.20.2	255.255.255.0	192.168.20.1

วิธีการทำ

1. **เปิดโปรแกรม Cisco Packet Tracer และสร้างการเชื่อมต่อระหว่าง Switch ทั้งสองและ PC**
    - เปิดโปรแกรม Cisco Packet Tracer
    - ลาก Switch L2 จำนวน 2 ตัวและ PC จำนวน 2 เครื่องไปวางในพื้นที่การทำงาน
2. **เชื่อมต่อสาย Cross-Over ระหว่างพอร์ต GigabitEthernet ของ Switch ทั้งสอง**
    - ใช้สาย Cross-Over เชื่อมต่อจาก GigabitEthernet0/1 ของ Switch1 ไปยัง GigabitEthernet0/1 ของ Switch2
3. **เปิด CLI ของ Switch โดยคลิกขวาที่ Switch และเลือก "CLI"**
    - คลิกขวาที่ Switch1 และ Switch2
    - เลือก "CLI"
4. **ตั้งค่า Trunk บนพอร์ตที่เชื่อมต่อระหว่าง Switch**
    - กำหนดพอร์ต GigabitEthernet0/1 ของ Switch1 และ Switch2 ให้เป็น Trunk และอนุญาตให้ส่งข้อมูล VLAN ทั้งหมดผ่านพอร์ตนี้

```
Switch1> enable
Switch1# configure terminal
Switch1(config)# interface gigabitethernet 0/1
Switch1(config-if)# switchport mode trunk
Switch1(config-if)# switchport trunk allowed vlan all
Switch1(config-if)# exit
Switch1(config)# exit
Switch1# write memory

Switch2> enable
Switch2# configure terminal
Switch2(config)# interface gigabitethernet 0/1
Switch2(config-if)# switchport mode trunk
Switch2(config-if)# switchport trunk allowed vlan all
Switch2(config-if)# exit
Switch2(config)# exit
```

```
Switch2# write memory
```

5. **ตั้งค่า VLAN และพอร์ต Access บน Switch ทั้งสอง**
   - กำหนดพอร์ต FastEthernet0/2 บน Switch1 และ Switch2 ให้เป็น VLAN 10

```
Switch1> enable
Switch1# configure terminal
Switch1(config)# vlan 10
Switch1(config-vlan)# name VLAN10
Switch1(config-vlan)# exit
Switch1(config)# interface fastethernet 0/2
Switch1(config-if)# switchport mode access
Switch1(config-if)# switchport access vlan 10
Switch1(config-if)# exit
Switch1(config)# exit
Switch1# write memory

Switch2> enable
Switch2# configure terminal
Switch2(config)# vlan 10
Switch2(config-vlan)# name VLAN10
Switch2(config-vlan)# exit
Switch2(config)# interface fastethernet 0/2
Switch2(config-if)# switchport mode access
Switch2(config-if)# switchport access vlan 10
Switch2(config-if)# exit
Switch2(config)# exit
Switch2# write memory
```

- กำหนดพอร์ต FastEthernet0/3 บน Switch1 และ Switch2 ให้เป็น VLAN 20

```
Switch1> enable
Switch1# configure terminal
Switch1(config)# vlan 20
Switch1(config-vlan)# name VLAN20
Switch1(config-vlan)# exit
Switch1(config)# interface fastethernet 0/3
Switch1(config-if)# switchport mode access
Switch1(config-if)# switchport access vlan 20
Switch1(config-if)# exit
Switch1(config)# exit
Switch1# write memory

Switch2> enable
Switch2# configure terminal
Switch2(config)# vlan 20
Switch2(config-vlan)# name VLAN20
Switch2(config-vlan)# exit
Switch2(config)# interface fastethernet 0/3
Switch2(config-if)# switchport mode access
Switch2(config-if)# switchport access vlan 20
Switch2(config-if)# exit
Switch2(config)# exit
Switch2# write memory
```

6. **ตั้งค่า IP Address และ Subnet Mask ให้กับเครื่อง PC**
   - เปิด PC1 > Desktop > IP Configuration
     - IP Address: 192.168.10.2
     - Subnet Mask: 255.255.255.0
     - Default Gateway: 192.168.10.1

- เปิด PC2 > Desktop > IP Configuration
  - IP Address: 192.168.20.2
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 192.168.20.1

7. **ทดสอบการเชื่อมต่อระหว่างเครื่อง PC ที่อยู่ใน VLAN เดียวกันด้วยคำสั่ง ping ใน Command Prompt**
   - เปิด Command Prompt บน PC1 และพิมพ์ ping 192.168.10.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC1 และ Switch1
   - เปิด Command Prompt บน PC2 และพิมพ์ ping 192.168.20.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC2 และ Switch2

สรุป

นักเรียนจะได้เรียนรู้การตั้งค่า Trunk บน Switch L2 เพื่อให้สามารถส่งข้อมูล VLAN ได้หลาย VLAN ผ่านสายเชื่อมต่อเดียว

ประโยชน์ของ LAB

- ช่วยให้นักเรียนเข้าใจการเชื่อมต่อและส่งข้อมูล VLAN ผ่านพอร์ต Trunk
- เรียนรู้วิธีการตั้งค่า Trunk บน Switch L2
- เพิ่มความรู้เกี่ยวกับการเชื่อมต่อระหว่าง Switch หลายตัวเพื่อส่งข้อมูล VLAN

LAB 4: การตั้งค่า EtherChannel บน Switch L2

ผู้สอน

ผู้ช่วยศาสตราจารย์อมร เจือตี๋
สาขาวิชาคอมพิวเตอร์ศึกษา คณะวิทยาศาสตร์และเทคโนโลยี

ชื่อ นามสกุล _____

หมู่เรียน _____

คะแนน _____

วัตถุประสงค์

1. เพื่อเรียนรู้การตั้งค่า EtherChannel บน Switch L2 เพื่อเพิ่มประสิทธิภาพการส่งข้อมูลและความทนทานของเครือข่าย

อุปกรณ์ที่ใช้

- Switch L2 (Cisco 2960) จำนวน 2 ตัว
- เครื่องคอมพิวเตอร์ (PC)
- สายเชื่อมต่อ (Straight-Through, Cross-Over)

การออกแบบหมายเลข IP Address

อุปกรณ์	พอร์ต	VLAN	IP Address	Subnet Mask	Default Gateway
PC1	NIC	10	192.168.10.2	255.255.255.0	192.168.10.1
PC2	NIC	20	192.168.20.2	255.255.255.0	192.168.20.1

วิธีการทำ

1. **เปิดโปรแกรม Cisco Packet Tracer และสร้างการเชื่อมต่อระหว่าง Switch ทั้งสองและ PC**
    - เปิดโปรแกรม Cisco Packet Tracer
    - ลาก Switch L2 จำนวน 2 ตัวและ PC จำนวน 2 เครื่องไปวางในพื้นที่การทำงาน
2. **เชื่อมต่อสาย Cross-Over ระหว่างพอร์ต FastEthernet ของ Switch ทั้งสอง**
    - ใช้สาย Cross-Over เชื่อมต่อจาก FastEthernet0/1 และ FastEthernet0/2 ของ Switch1 ไปยัง FastEthernet0/1 และ FastEthernet0/2 ของ Switch2
3. **เปิด CLI ของ Switch โดยคลิกขวาที่ Switch และเลือก "CLI"**
    - คลิกขวาที่ Switch1 และ Switch2
    - เลือก "CLI"
4. **ตั้งค่า EtherChannel บน Switch แรก**
    - กำหนดพอร์ต FastEthernet0/1 และ FastEthernet0/2 ให้เป็น EtherChannel 1 และตั้งค่าเป็น trunk

```
Switch1> enable
Switch1# configure terminal
Switch1(config)# interface range fastethernet 0/1 - 2
Switch1(config-if-range)# channel-group 1 mode active
Switch1(config-if-range)# exit
Switch1(config)# interface port-channel 1
Switch1(config-if)# switchport mode trunk
Switch1(config-if)# exit
Switch1(config)# exit
Switch1# write memory
```

5. **ตั้งค่า EtherChannel บน Switch ที่สอง**
    - กำหนดพอร์ต FastEthernet0/1 และ FastEthernet0/2 ให้เป็น EtherChannel 1 และตั้งค่าเป็น trunk

```
Switch2> enable
Switch2# configure terminal
```

```
Switch2(config)# interface range fastethernet 0/1 - 2
Switch2(config-if-range)# channel-group 1 mode active
Switch2(config-if-range)# exit
Switch2(config)# interface port-channel 1
Switch2(config-if)# switchport mode trunk
Switch2(config-if)# exit
Switch2(config)# exit
Switch2# write memory
```

6. **ตั้งค่า VLAN และพอร์ต Access บน Switch ทั้งสอง**
   - กำหนดพอร์ต FastEthernet0/3 บน Switch1 และ Switch2 ให้เป็น VLAN 10

```
Switch1> enable
Switch1# configure terminal
Switch1(config)# vlan 10
Switch1(config-vlan)# name VLAN10
Switch1(config-vlan)# exit
Switch1(config)# interface fastethernet 0/3
Switch1(config-if)# switchport mode access
Switch1(config-if)# switchport access vlan 10
Switch1(config-if)# exit
Switch1(config)# exit
Switch1# write memory
```

```
Switch2> enable
Switch2# configure terminal
Switch2(config)# vlan 10
Switch2(config-vlan)# name VLAN10
Switch2(config-vlan)# exit
Switch2(config)# interface fastethernet 0/3
Switch2(config-if)# switchport mode access
```

```
Switch2(config-if)# switchport access vlan 10
Switch2(config-if)# exit
Switch2(config)# exit
Switch2# write memory
```

- กำหนดพอร์ต FastEthernet0/4 บน Switch1 และ Switch2 ให้เป็น VLAN 20

```
Switch1> enable
Switch1# configure terminal
Switch1(config)# vlan 20
Switch1(config-vlan)# name VLAN20
Switch1(config-vlan)# exit
Switch1(config)# interface fastethernet 0/4
Switch1(config-if)# switchport mode access
Switch1(config-if)# switchport access vlan 20
Switch1(config-if)# exit
Switch1(config)# exit
Switch1# write memory

Switch2> enable
Switch2# configure terminal
Switch2(config)# vlan 20
Switch2(config-vlan)# name VLAN20
Switch2(config-vlan)# exit
Switch2(config)# interface fastethernet 0/4
Switch2(config-if)# switchport mode access
Switch2(config-if)# switchport access vlan 20
Switch2(config-if)# exit
Switch2(config)# exit
Switch2# write memory
```

7. **ตั้งค่า IP Address และ Subnet Mask ให้กับเครื่อง PC**
    - เปิด PC1 > Desktop > IP Configuration
        - IP Address: 192.168.10.2
        - Subnet Mask: 255.255.255.0
        - Default Gateway: 192.168.10.1
    - เปิด PC2 > Desktop > IP Configuration
        - IP Address: 192.168.20.2
        - Subnet Mask: 255.255.255.0
        - Default Gateway: 192.168.20.1
8. **ทดสอบการเชื่อมต่อระหว่างเครื่อง PC ที่อยู่ใน VLAN เดียวกันด้วยคำสั่ง ping ใน Command Prompt**
    - เปิด Command Prompt บน PC1 และพิมพ์ ping 192.168.10.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC1 และ Switch1
    - เปิด Command Prompt บน PC2 และพิมพ์ ping 192.168.20.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC2 และ Switch2

สรุป

นักเรียนจะได้เรียนรู้การตั้งค่า EtherChannel บน Switch L2 เพื่อเพิ่มประสิทธิภาพการส่งข้อมูลและความทนทานของเครือข่าย

ประโยชน์ของ LAB

- ช่วยให้นักเรียนเข้าใจการรวมพอร์ตหลายพอร์ตเพื่อเพิ่มแบนด์วิดท์และความทนทานของเครือข่าย
- เรียนรู้วิธีการตั้งค่า EtherChannel บน Switch L2
- เพิ่มประสิทธิภาพการส่งข้อมูลและลดความเสี่ยงจากการเสียหายของพอร์ตเดียว

LAB 5: การตั้งค่า Spanning Tree Protocol (STP) บน Switch L2

ผู้สอน

ผู้ช่วยศาสตราจารย์อมร เจือตี๋
สาขาวิชาคอมพิวเตอร์ศึกษา คณะวิทยาศาสตร์และเทคโนโลยี

ชื่อ นามสกุล _____

หมู่เรียน _____

คะแนน _____

วัตถุประสงค์

1. เพื่อเรียนรู้การตั้งค่าและการใช้งาน Spanning Tree Protocol (STP) บน Switch L2

อุปกรณ์ที่ใช้

- Switch L2 (Cisco 2960) จำนวน 2 ตัว
- เครื่องคอมพิวเตอร์ (PC)
- สายเชื่อมต่อ (Straight-Through, Cross-Over)

การออกแบบหมายเลข IP Address

อุปกรณ์	พอร์ต	VLAN	IP Address	Subnet Mask	Default Gateway
PC1	NIC	10	192.168.10.2	255.255.255.0	192.168.10.1
PC2	NIC	20	192.168.20.2	255.255.255.0	192.168.20.1

วิธีการทำ

1. **เปิดโปรแกรม Cisco Packet Tracer และสร้างการเชื่อมต่อระหว่าง Switch ทั้งสองและ PC**
    - เปิดโปรแกรม Cisco Packet Tracer
    - ลาก Switch L2 จำนวน 2 ตัวและ PC จำนวน 2 เครื่องไปวางในพื้นที่การทำงาน

2. **เชื่อมต่อสาย Cross-Over ระหว่างพอร์ต GigabitEthernet ของ Switch ทั้งสอง**
    - ใช้สาย Cross-Over เชื่อมต่อจาก GigabitEthernet0/1 ของ Switch1 ไปยัง GigabitEthernet0/1 ของ Switch2
3. **เปิด CLI ของ Switch โดยคลิกขวาที่ Switch และเลือก "CLI"**
    - คลิกขวาที่ Switch1 และ Switch2
    - เลือก "CLI"
4. **ตั้งค่า STP บน Switch แรก**
    - กำหนดให้ Switch แรกเป็น Root Bridge สำหรับ VLAN 1

```
Switch1> enable
Switch1# configure terminal
Switch1(config)# spanning-tree vlan 1 root primary
Switch1(config)# exit
Switch1# write memory
```

5. **ตั้งค่า STP บน Switch ที่สอง**
    - กำหนดให้ Switch ที่สองเป็น Secondary Root สำหรับ VLAN 1

```
Switch2> enable
Switch2# configure terminal
Switch2(config)# spanning-tree vlan 1 root secondary
Switch2(config)# exit
Switch2# write memory
```

6. **ตั้งค่า VLAN และพอร์ต Access บน Switch ทั้งสอง**
    - กำหนดพอร์ต FastEthernet0/2 บน Switch1 และ Switch2 ให้เป็น VLAN 10

```
Switch1> enable
Switch1# configure terminal
Switch1(config)# vlan 10
Switch1(config-vlan)# name VLAN10
Switch1(config-vlan)# exit
```

```
Switch1(config)# interface fastethernet 0/2
Switch1(config-if)# switchport mode access
Switch1(config-if)# switchport access vlan 10
Switch1(config-if)# exit
Switch1(config)# exit
Switch1# write memory

Switch2> enable
Switch2# configure terminal
Switch2(config)# vlan 10
Switch2(config-vlan)# name VLAN10
Switch2(config-vlan)# exit
Switch2(config)# interface fastethernet 0/2
Switch2(config-if)# switchport mode access
Switch2(config-if)# switchport access vlan 10
Switch2(config-if)# exit
Switch2(config)# exit
Switch2# write memory
```

- กำหนดพอร์ต FastEthernet0/3 บน Switch1 และ Switch2 ให้เป็น VLAN 20

```
Switch1> enable
Switch1# configure terminal
Switch1(config)# vlan 20
Switch1(config-vlan)# name VLAN20
Switch1(config-vlan)# exit
Switch1(config)# interface fastethernet 0/3
Switch1(config-if)# switchport mode access
Switch1(config-if)# switchport access vlan 20
Switch1(config-if)# exit
Switch1(config)# exit
```

```
Switch1# write memory


Switch2> enable
Switch2# configure terminal
Switch2(config)# vlan 20
Switch2(config-vlan)# name VLAN20
Switch2(config-vlan)# exit
Switch2(config)# interface fastethernet 0/3
Switch2(config-if)# switchport mode access
Switch2(config-if)# switchport access vlan 20
Switch2(config-if)# exit
Switch2(config)# exit
Switch2# write memory
```

7. **ตั้งค่า IP Address และ Subnet Mask ให้กับเครื่อง PC**
    - เปิด PC1 > Desktop > IP Configuration
        - IP Address: 192.168.10.2
        - Subnet Mask: 255.255.255.0
        - Default Gateway: 192.168.10.1
    - เปิด PC2 > Desktop > IP Configuration
        - IP Address: 192.168.20.2
        - Subnet Mask: 255.255.255.0
        - Default Gateway: 192.168.20.1
        -
8. **ทดสอบการเชื่อมต่อระหว่างเครื่อง PC ที่อยู่ใน VLAN เดียวกันด้วยคำสั่ง ping ใน Command Prompt**
    - เปิด Command Prompt บน PC1 และพิมพ์ ping 192.168.10.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC1 และ Switch1
    - เปิด Command Prompt บน PC2 และพิมพ์ ping 192.168.20.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC2 และ Switch2

สรุป

นักเรียนจะได้เรียนรู้การตั้งค่าและการใช้งาน Spanning Tree Protocol (STP) บน Switch L2 เพื่อป้องกัน Loop ในเครือข่าย

ประโยชน์ของ LAB

- ช่วยให้นักเรียนเข้าใจการป้องกัน Loop ในเครือข่ายผ่านการใช้ STP
- เรียนรู้วิธีการตั้งค่าและการใช้งาน STP บน Switch L2
- เพิ่มความเสถียรและประสิทธิภาพของเครือข่าย

LAB 6: การตั้งค่า Inter-VLAN Routing บน Switch L2

ผู้สอน

ผู้ช่วยศาสตราจารย์อมร เจือตี๋
สาขาวิชาคอมพิวเตอร์ศึกษา คณะวิทยาศาสตร์และเทคโนโลยี

ชื่อ นามสกุล _____

หมู่เรียน _____

คะแนน _____

วัตถุประสงค์

1. เพื่อเรียนรู้การตั้งค่าและการใช้งาน Inter-VLAN Routing บน Switch L2

อุปกรณ์ที่ใช้

- Switch L2 (Cisco 2960)
- Router (Cisco 1941)
- เครื่องคอมพิวเตอร์ (PC)
- สายเชื่อมต่อ (Straight-Through, Cross-Over)

การออกแบบหมายเลข IP Address

อุปกรณ์	พอร์ต	VLAN	IP Address	Subnet Mask	Default Gateway
PC1	NIC	10	192.168.10.2	255.255.255.0	192.168.10.1
PC2	NIC	20	192.168.20.2	255.255.255.0	192.168.20.1

วิธีการทำ

1. **เปิดโปรแกรม Cisco Packet Tracer และสร้างการเชื่อมต่อระหว่าง Switch, Router และ PC**
    - เปิดโปรแกรม Cisco Packet Tracer
    - ลาก Switch L2, Router (Cisco 1941) และ PC จำนวน 2 เครื่องไปวางในพื้นที่การทำงาน
2. **ตั้งค่า VLAN และพอร์ต Trunk บน Switch**
    - สร้าง VLAN 10 และ VLAN 20 บน Switch

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name VLAN10
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# name VLAN20
Switch(config-vlan)# exit
```

    - ตั้งค่าพอร์ต Trunk บนพอร์ตที่เชื่อมต่อไปยัง Router

```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan all
Switch(config-if)# exit
```

    - ตั้งค่าพอร์ต Access สำหรับ VLAN 10 และ 20

```
Switch(config)# interface range fastethernet 0/2 - 3
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# exit
Switch(config)# interface range fastethernet 0/4 - 5
Switch(config-if-range)# switchport mode access
```

```
Switch(config-if-range)# switchport access vlan 20
Switch(config-if-range)# exit
Switch(config)# exit
Switch# write memory
```

3. **ตั้งค่า Inter-VLAN Routing บน Router**
    - ตั้งค่า Sub-interface สำหรับ VLAN 10 และ 20 บน Router

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 0/0.10
Router(config-subif)# encapsulation dot1q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.0
Router(config-subif)# exit
Router(config)# interface gigabitethernet 0/0.20
Router(config-subif)# encapsulation dot1q 20
Router(config-subif)# ip address 192.168.20.1 255.255.255.0
Router(config-subif)# exit
Router(config)# interface gigabitethernet 0/0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# exit
Router# write memory
```

4. **ตั้งค่า IP Address และ Default Gateway ให้กับเครื่อง PC**
    - เปิด PC1 > Desktop > IP Configuration
        - IP Address: 192.168.10.2
        - Subnet Mask: 255.255.255.0
        - Default Gateway: 192.168.10.1

- เปิด PC2 > Desktop > IP Configuration
  - IP Address: 192.168.20.2
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 192.168.20.1

5. **ทดสอบการเชื่อมต่อระหว่างเครื่อง PC ที่อยู่ใน VLAN ต่างกันด้วยคำสั่ง ping ใน Command Prompt**
   - เปิด Command Prompt บน PC1 และพิมพ์ ping 192.168.20.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC1 และ PC2 ผ่าน Inter-VLAN Routing
   - เปิด Command Prompt บน PC2 และพิมพ์ ping 192.168.10.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC2 และ PC1 ผ่าน Inter-VLAN Routing
   -
6. **ตรวจสอบการตั้งค่า VLAN บน Switch และ Router**
   - ใช้คำสั่ง show vlan brief บน Switch เพื่อดูการตั้งค่า VLAN:

     Switch> enable
     Switch# show vlan brief

   - ใช้คำสั่ง show interfaces trunk บน Switch เพื่อดูการตั้งค่าพอร์ต Trunk:

     Switch# show interfaces trunk

   - ใช้คำสั่ง show ip interface brief บน Router เพื่อดูการตั้งค่า Sub-interface:

     Router> enable
     Router# show ip interface brief

7. **ตรวจสอบการทำงานของ Inter-VLAN Routing**
   - เปิด Command Prompt บน PC1 และพิมพ์ ping 192.168.10.1 เพื่อทดสอบการเชื่อมต่อไปยัง Default Gateway ของ VLAN 10
   - เปิด Command Prompt บน PC2 และพิมพ์ ping 192.168.20.1 เพื่อทดสอบการเชื่อมต่อไปยัง Default Gateway ของ VLAN 20
   - ตรวจสอบการเชื่อมต่อระหว่าง PC1 และ PC2 ด้วยคำสั่ง ping:

- บน PC1 พิมพ์ ping 192.168.20.2
- บน PC2 พิมพ์ ping 192.168.10.2
-

8. **แก้ไขปัญหา (ถ้ามี)**
    - หากการเชื่อมต่อไม่สำเร็จ ตรวจสอบการตั้งค่า IP Address, Subnet Mask, และ Default Gateway บน PC ทั้งสองเครื่อง
    - ตรวจสอบการตั้งค่า VLAN และพอร์ต Trunk บน Switch เพื่อให้แน่ใจว่าพอร์ตที่เชื่อมต่อกับ Router ถูกตั้งค่าเป็น Trunk อย่างถูกต้อง
    - ตรวจสอบการตั้งค่า Sub-interface บน Router เพื่อให้แน่ใจว่าการตั้งค่า encapsulation และ IP Address ถูกต้อง

สรุป

นักเรียนจะได้เรียนรู้การตั้งค่าและการใช้งาน Inter-VLAN Routing บน Switch L2 และ Router เพื่อให้เครื่องคอมพิวเตอร์ใน VLAN ต่างๆ สามารถสื่อสารกันได้

ประโยชน์ของ LAB

- ช่วยให้นักเรียนเข้าใจการสื่อสารระหว่าง VLAN ต่างๆ ผ่าน Inter-VLAN Routing
- เรียนรู้วิธีการตั้งค่า Inter-VLAN Routing บน Switch L2 และ Router
- เพิ่มความสามารถในการจัดการและการสื่อสารระหว่างเครือข่ายที่แบ่งออกเป็นหลายๆ VLAN

LAB 7: การตั้งค่าและใช้งาน DHCP บน Switch L2

ผู้สอน

ผู้ช่วยศาสตราจารย์อมร เจือตี๋
สาขาวิชาคอมพิวเตอร์ศึกษา คณะวิทยาศาสตร์และเทคโนโลยี

ชื่อ นามสกุล _____

หมู่เรียน _____

คะแนน _____

วัตถุประสงค์

1. เพื่อเรียนรู้การตั้งค่า DHCP (Dynamic Host Configuration Protocol) บน Switch L2
2. เพื่อทดสอบการทำงานของ DHCP ในการแจกจ่าย IP Address ให้กับอุปกรณ์เครือข่าย

อุปกรณ์ที่ใช้

- Switch L2 (Cisco 2960)
- Router (Cisco 1941)
- เครื่องคอมพิวเตอร์ (PC)
- สายเชื่อมต่อ (Straight-Through, Cross-Over)

การออกแบบหมายเลข IP Address

อุปกรณ์	พอร์ต	VLAN	IP Address	Subnet Mask	Default Gateway
PC1	NIC	10	DHCP	DHCP	DHCP
PC2	NIC	20	DHCP	DHCP	DHCP
Router	G0/0	Trunk	192.168.10.1	255.255.255.0	-
Router	G0/0	Trunk	192.168.20.1	255.255.255.0	-

วิธีการทำ

1. **เปิดโปรแกรม Cisco Packet Tracer และสร้างการเชื่อมต่อระหว่าง Switch, Router และ PC**
    - เปิดโปรแกรม Cisco Packet Tracer
    - ลาก Switch L2, Router (Cisco 1941) และ PC จำนวน 2 เครื่องไปวางในพื้นที่การทำงาน
2. **ตั้งค่า VLAN และพอร์ต Trunk บน Switch**
    - สร้าง VLAN 10 และ VLAN 20 บน Switch

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name VLAN10
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# name VLAN20
Switch(config-vlan)# exit
```

    - ตั้งค่าพอร์ต Trunk บนพอร์ตที่เชื่อมต่อไปยัง Router

```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan all
Switch(config-if)# exit
```

    - ตั้งค่าพอร์ต Access สำหรับ VLAN 10 และ 20

```
Switch(config)# interface range fastethernet 0/2 - 3
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# exit
Switch(config)# interface range fastethernet 0/4 - 5
Switch(config-if-range)# switchport mode access
```

```
Switch(config-if-range)# switchport access vlan 20
Switch(config-if-range)# exit
Switch(config)# exit
Switch# write memory
```

3. **ตั้งค่า DHCP บน Router**
   - ตั้งค่า Sub-interface สำหรับ VLAN 10 และ 20 บน Router

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 0/0.10
Router(config-subif)# encapsulation dot1q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.0
Router(config-subif)# exit
Router(config)# interface gigabitethernet 0/0.20
Router(config-subif)# encapsulation dot1q 20
Router(config-subif)# ip address 192.168.20.1 255.255.255.0
Router(config-subif)# exit
Router(config)# interface gigabitethernet 0/0
Router(config-if)# no shutdown
Router(config-if)# exit
```

   - ตั้งค่า DHCP Pool สำหรับ VLAN 10 และ 20 บน Router

```
Router(config)# ip dhcp pool VLAN10
Router(dhcp-config)# network 192.168.10.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.10.1
Router(dhcp-config)# exit
Router(config)# ip dhcp pool VLAN20
Router(dhcp-config)# network 192.168.20.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.20.1
Router(dhcp-config)# exit
```

```
Router(config)# ip dhcp excluded-address 192.168.10.1
Router(config)# ip dhcp excluded-address 192.168.20.1
Router(config)# exit
Router# write memory
```

4. **ตั้งค่า IP Configuration บน PC ให้เป็น DHCP**
    - เปิด PC1 > Desktop > IP Configuration
        - ตั้งค่า IP Configuration เป็น DHCP
    - เปิด PC2 > Desktop > IP Configuration
        - ตั้งค่า IP Configuration เป็น DHCP
5. **ทดสอบการเชื่อมต่อระหว่างเครื่อง PC ที่อยู่ใน VLAN ต่างกันด้วยคำสั่ง ping ใน Command Prompt**
    - เปิด Command Prompt บน PC1 และพิมพ์ ping 192.168.20.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC1 และ PC2 ผ่าน Inter-VLAN Routing
    - เปิด Command Prompt บน PC2 และพิมพ์ ping 192.168.10.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC2 และ PC1 ผ่าน Inter-VLAN Routing

สรุป

นักเรียนจะได้เรียนรู้การตั้งค่าและการใช้งาน DHCP บน Switch L2 และ Router เพื่อให้เครื่องคอมพิวเตอร์ใน VLAN ต่างๆ สามารถรับ IP Address อัตโนมัติและสื่อสารกันได้

ประโยชน์ของ LAB

- ช่วยให้นักเรียนเข้าใจการใช้งาน DHCP เพื่อแจกจ่าย IP Address อัตโนมัติในเครือข่าย
- เรียนรู้วิธีการตั้งค่า DHCP บน Switch L2 และ Router
- เพิ่มความสะดวกและประสิทธิภาพในการจัดการ IP Address ในเครือข่าย

LAB 8: การตั้งค่า Access Control List (ACL) บน Switch L2

ผู้สอน

ผู้ช่วยศาสตราจารย์อมร เจือตี๋
สาขาวิชาคอมพิวเตอร์ศึกษา คณะวิทยาศาสตร์และเทคโนโลยี

ชื่อ นามสกุล _____

หมู่เรียน _____

คะแนน _____

วัตถุประสงค์

1. เพื่อเรียนรู้การตั้งค่า Access Control List (ACL) บน Switch L2
2. เพื่อจำกัดการเข้าถึงเครือข่ายบนอุปกรณ์ที่กำหนด

อุปกรณ์ที่ใช้

- Switch L2 (Cisco 2960)
- Router (Cisco 1941)
- เครื่องคอมพิวเตอร์ (PC)
- สายเชื่อมต่อ (Straight-Through, Cross-Over)

การออกแบบหมายเลข IP Address

อุปกรณ์	พอร์ต	VLAN	IP Address	Subnet Mask	Default Gateway
PC1	NIC	10	192.168.10.2	255.255.255.0	192.168.10.1
PC2	NIC	20	192.168.20.2	255.255.255.0	192.168.20.1
Router	G0/0	Trunk	192.168.10.1	255.255.255.0	-
Router	G0/0	Trunk	192.168.20.1	255.255.255.0	-

วิธีการทำ

1. **เปิดโปรแกรม Cisco Packet Tracer และสร้างการเชื่อมต่อระหว่าง Switch, Router และ PC**
    - เปิดโปรแกรม Cisco Packet Tracer
    - ลาก Switch L2, Router (Cisco 1941) และ PC จำนวน 2 เครื่องไปวางในพื้นที่การทำงาน
2. **ตั้งค่า VLAN และพอร์ต Trunk บน Switch**
    - สร้าง VLAN 10 และ VLAN 20 บน Switch

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name VLAN10
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# name VLAN20
Switch(config-vlan)# exit
```

    - ตั้งค่าพอร์ต Trunk บนพอร์ตที่เชื่อมต่อไปยัง Router

```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan all
Switch(config-if)# exit
```

    - ตั้งค่าพอร์ต Access สำหรับ VLAN 10 และ 20

```
Switch(config)# interface range fastethernet 0/2 - 3
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# exit
Switch(config)# interface range fastethernet 0/4 - 5
Switch(config-if-range)# switchport mode access
```

```
Switch(config-if-range)# switchport access vlan 20
Switch(config-if-range)# exit
Switch(config)# exit
Switch# write memory
```

3. **ตั้งค่า ACL บน Router เพื่อจำกัดการเข้าถึงเครือข่าย**
    - สร้าง Access Control List บน Router เพื่ออนุญาตเฉพาะการเข้าถึงจาก PC ใน VLAN 10 ไปยัง VLAN 20

```
Router> enable
Router# configure terminal
Router(config)# access-list 100 permit ip 192.168.10.0 0.0.0.255 192.168.20.0
0.0.0.255
Router(config)# access-list 100 deny ip any any
Router(config)# interface gigabitethernet 0/0.20
Router(config-subif)# ip access-group 100 in
Router(config-subif)# exit
Router(config)# exit
Router# write memory
```

4. **ตั้งค่า IP Address และ Subnet Mask ให้กับเครื่อง PC**
    - เปิด PC1 > Desktop > IP Configuration
        - IP Address: 192.168.10.2
        - Subnet Mask: 255.255.255.0
        - Default Gateway: 192.168.10.1
    - เปิด PC2 > Desktop > IP Configuration
        - IP Address: 192.168.20.2
        - Subnet Mask: 255.255.255.0
        - Default Gateway: 192.168.20.1

5. **ทดสอบการเชื่อมต่อระหว่างเครื่อง PC ที่อยู่ใน VLAN ต่างกันด้วยคำสั่ง ping ใน Command Prompt**
    - เปิด Command Prompt บน PC1 และพิมพ์ ping 192.168.20.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC1 และ PC2 ผ่าน Inter-VLAN Routing
    - เปิด Command Prompt บน PC2 และพิมพ์ ping 192.168.10.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC2 และ PC1 ผ่าน Inter-VLAN Routing

สรุป

นักเรียนจะได้เรียนรู้การตั้งค่า Access Control List (ACL) บน Switch L2 และ Router เพื่อจำกัดการเข้าถึงเครือข่ายบนอุปกรณ์ที่กำหนด

ประโยชน์ของ LAB

- ช่วยให้นักเรียนเข้าใจการใช้งาน ACL เพื่อจำกัดการเข้าถึงเครือข่าย
- เรียนรู้วิธีการตั้งค่า ACL บน Switch L2 และ Router
- เพิ่มความปลอดภัยในการเข้าถึงเครือข่ายโดยจำกัดการเข้าถึงจากอุปกรณ์ที่ไม่ได้รับอนุญาต

LAB 9: การตั้งค่า Port Security บน Switch L2

ผู้สอน

ผู้ช่วยศาสตราจารย์อมร เจือตี๋
สาขาวิชาคอมพิวเตอร์ศึกษา คณะวิทยาศาสตร์และเทคโนโลยี

ชื่อ นามสกุล _____

หมู่เรียน _____

คะแนน _____

วัตถุประสงค์

1. เพื่อเรียนรู้การตั้งค่า Port Security บน Switch L2
2. เพื่อป้องกันการโจมตีจาก MAC Address ปลอม

อุปกรณ์ที่ใช้

- Switch L2 (Cisco 2960)
- เครื่องคอมพิวเตอร์ (PC)
- สายเชื่อมต่อ (Straight-Through)

การออกแบบหมายเลข IP Address

อุปกรณ์	พอร์ต	VLAN	IP Address	Subnet Mask	Default Gateway
PC1	NIC	10	192.168.10.2	255.255.255.0	192.168.10.1
PC2	NIC	20	192.168.20.2	255.255.255.0	192.168.20.1

วิธีการทำ

1. **เปิดโปรแกรม Cisco Packet Tracer และสร้างการเชื่อมต่อระหว่าง Switch และ PC**
    - เปิดโปรแกรม Cisco Packet Tracer
    - ลาก Switch L2 และ PC จำนวน 2 เครื่องไปวางในพื้นที่การทำงาน
2. **ตั้งค่า VLAN และพอร์ต Access บน Switch**
    - สร้าง VLAN 10 และ VLAN 20 บน Switch

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name VLAN10
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# name VLAN20
Switch(config-vlan)# exit
```

    - ตั้งค่าพอร์ต Access สำหรับ VLAN 10 และ 20

```
Switch(config)# interface range fastethernet 0/1 - 2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# exit
Switch(config)# interface range fastethernet 0/3 - 4
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 20
Switch(config-if-range)# exit
Switch(config)# exit
Switch# write memory
```

3. **ตั้งค่า Port Security บนพอร์ตที่เชื่อมต่อกับ PC**
    - ตั้งค่า Port Security บนพอร์ต FastEthernet0/1 และ FastEthernet0/3

```
Switch> enable
Switch# configure terminal
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 1
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# exit
Switch(config)# interface fastethernet 0/3
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 1
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# exit
Switch(config)# exit
Switch# write memory
```

4. **ตั้งค่า IP Address และ Subnet Mask ให้กับเครื่อง PC**
    - เปิด PC1 > Desktop > IP Configuration
        - IP Address: 192.168.10.2
        - Subnet Mask: 255.255.255.0
        - Default Gateway: 192.168.10.1
    - เปิด PC2 > Desktop > IP Configuration
        - IP Address: 192.168.20.2
        - Subnet Mask: 255.255.255.0
        - Default Gateway: 192.168.20.1

5. **ทดสอบการเชื่อมต่อระหว่างเครื่อง PC ที่อยู่ใน VLAN ต่างกันด้วยคำสั่ง ping ใน Command Prompt**
    - เปิด Command Prompt บน PC1 และพิมพ์ ping 192.168.20.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC1 และ PC2 ผ่าน Inter-VLAN Routing
    - เปิด Command Prompt บน PC2 และพิมพ์ ping 192.168.10.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC2 และ PC1 ผ่าน Inter-VLAN Routing
    -
6. **ทดสอบการทำงานของ Port Security**
    - เปลี่ยน MAC Address ของ PC ใด PC หนึ่งและลองเชื่อมต่อใหม่ จะพบว่าการเชื่อมต่อล้มเหลว เนื่องจากการตั้งค่า Port Security

สรุป

นักเรียนจะได้เรียนรู้การตั้งค่า Port Security บน Switch L2 เพื่อป้องกันการโจมตีจาก MAC Address ปลอม และเพิ่มความปลอดภัยให้กับเครือข่าย

ประโยชน์ของ LAB

- ช่วยให้นักเรียนเข้าใจการใช้งาน Port Security เพื่อป้องกันการโจมตีจาก MAC Address ปลอม
- เรียนรู้วิธีการตั้งค่า Port Security บน Switch L2
- เพิ่มความปลอดภัยให้กับเครือข่ายโดยการควบคุมการเข้าถึงพอร์ตของ Switch

---

LAB 10: การตั้งค่า Quality of Service (QoS) บน Switch L2

ผู้สอน

ผู้ช่วยศาสตราจารย์อมร เจือตี๋
สาขาวิชาคอมพิวเตอร์ศึกษา คณะวิทยาศาสตร์และเทคโนโลยี

ชื่อ นามสกุล _____

หมู่เรียน _____

คะแนน _____

วัตถุประสงค์

1. เพื่อเรียนรู้การตั้งค่า Quality of Service (QoS) บน Switch L2
2. เพื่อจัดลำดับความสำคัญของการส่งข้อมูลในเครือข่าย

อุปกรณ์ที่ใช้

- Switch L2 (Cisco 2960)
- เครื่องคอมพิวเตอร์ (PC)
- สายเชื่อมต่อ (Straight-Through)

การออกแบบหมายเลข IP Address

อุปกรณ์	พอร์ต	VLAN	IP Address	Subnet Mask	Default Gateway
PC1	NIC	10	192.168.10.2	255.255.255.0	192.168.10.1
PC2	NIC	20	192.168.20.2	255.255.255.0	192.168.20.1

วิธีการทำ

1. **เปิดโปรแกรม Cisco Packet Tracer และสร้างการเชื่อมต่อระหว่าง Switch และ PC**
    - เปิดโปรแกรม Cisco Packet Tracer
    - ลาก Switch L2 และ PC จำนวน 2 เครื่องไปวางในพื้นที่การทำงาน
2. **ตั้งค่า VLAN และพอร์ต Access บน Switch**
    - สร้าง VLAN 10 และ VLAN 20 บน Switch

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name VLAN10
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# name VLAN20
Switch(config-vlan)# exit
```

    - ตั้งค่าพอร์ต Access สำหรับ VLAN 10 และ 20

```
Switch(config)# interface range fastethernet 0/1 - 2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# exit
Switch(config)# interface range fastethernet 0/3 - 4
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 20
Switch(config-if-range)# exit
Switch(config)# exit
Switch# write memory
```

3. **ตั้งค่า QoS บน Switch**
    - ตั้งค่า QoS บนพอร์ตที่เชื่อมต่อกับ PC เพื่อจัดลำดับความสำคัญของการส่งข้อมูล

```
Switch> enable
Switch# configure terminal
Switch(config)# mls qos
Switch(config)# interface fastethernet 0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# exit
Switch(config)# interface fastethernet 0/3
Switch(config-if)# mls qos trust cos
Switch(config-if)# exit
Switch(config)# exit
Switch# write memory
```

4. **ตั้งค่า IP Address และ Subnet Mask ให้กับเครื่อง PC**
    - เปิด PC1 > Desktop > IP Configuration
        - IP Address: 192.168.10.2
        - Subnet Mask: 255.255.255.0
        - Default Gateway: 192.168.10.1
    - เปิด PC2 > Desktop > IP Configuration
        - IP Address: 192.168.20.2
        - Subnet Mask: 255.255.255.0
        - Default Gateway: 192.168.20.1
        -

5. **ทดสอบการเชื่อมต่อระหว่างเครื่อง PC ที่อยู่ใน VLAN ต่างกันด้วยคำสั่ง ping ใน Command Prompt**
    - เปิด Command Prompt บน PC1 และพิมพ์ ping 192.168.20.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC1 และ PC2 ผ่าน Inter-VLAN Routing
    - เปิด Command Prompt บน PC2 และพิมพ์ ping 192.168.10.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC2 และ PC1 ผ่าน Inter-VLAN Routing

สรุป

นักเรียนจะได้เรียนรู้การตั้งค่า Quality of Service (QoS) บน Switch L2 เพื่อจัดลำดับความสำคัญของการส่งข้อมูลในเครือข่าย และเพิ่มประสิทธิภาพในการจัดการทราฟฟิกเครือข่าย

ประโยชน์ของ LAB

- ช่วยให้นักเรียนเข้าใจการจัดลำดับความสำคัญของการส่งข้อมูลในเครือข่ายผ่าน QoS
- เรียนรู้วิธีการตั้งค่า QoS บน Switch L2
- เพิ่มประสิทธิภาพในการจัดการทราฟฟิกเครือข่ายและปรับปรุงคุณภาพการบริการในเครือข่าย

LAB 11: การตั้งค่า DHCP Relay บน Switch L2 และ Router

ผู้สอน

ผู้ช่วยศาสตราจารย์อมร เจือตี๋
สาขาวิชาคอมพิวเตอร์ศึกษา คณะวิทยาศาสตร์และเทคโนโลยี

ชื่อ นามสกุล _____

หมู่เรียน _____

คะแนน _____

วัตถุประสงค์

1. เพื่อเรียนรู้การตั้งค่า DHCP Relay บน Switch L2 และ Router เพื่อแจกหมายเลข IP Address แบบอัตโนมัติ

อุปกรณ์ที่ใช้

- Switch L2 (Cisco 2960) จำนวน 2 ตัว
- Router (Cisco 1941) จำนวน 1 ตัว
- เครื่องคอมพิวเตอร์ (PC)
- สายเชื่อมต่อ (Straight-Through, Cross-Over)

การออกแบบหมายเลข IP Address

อุปกรณ์	พอร์ต	VLAN	IP Address	Subnet Mask	Default Gateway
PC1	NIC	10	DHCP	DHCP	DHCP
PC2	NIC	20	DHCP	DHCP	DHCP
Switch1	Fa0/1	Trunk	-	-	-
Switch2	Fa0/1	Trunk	-	-	-
Router	G0/0	Trunk	192.168.10.1	255.255.255.0	-

อุปกรณ์	พอร์ต	VLAN	IP Address	Subnet Mask	Default Gateway
Router	G0/1	Trunk	192.168.20.1	255.255.255.0	-

วิธีการทำ

1. **เปิดโปรแกรม Cisco Packet Tracer และสร้างการเชื่อมต่อระหว่าง Switch, Router และ PC**
    - เปิดโปรแกรม Cisco Packet Tracer
    - ลาก Switch L2 จำนวน 2 ตัว, Router (Cisco 1941) จำนวน 1 ตัว และ PC จำนวน 2 เครื่อง ไปวางในพื้นที่การทำงาน
2. **เชื่อมต่อสาย**
    - ใช้สาย Cross-Over เชื่อมต่อจาก FastEthernet0/1 ของ Switch1 ไปยัง FastEthernet0/1 ของ Switch2
    - ใช้สาย Straight-Through เชื่อมต่อจาก GigabitEthernet0/0 ของ Router ไปยัง FastEthernet0/1 ของ Switch1
    - ใช้สาย Straight-Through เชื่อมต่อจาก GigabitEthernet0/1 ของ Router ไปยัง FastEthernet0/1 ของ Switch2
    - ใช้สาย Straight-Through เชื่อมต่อจาก FastEthernet0 ของ PC1 ไปยัง FastEthernet0/2 ของ Switch1
    - ใช้สาย Straight-Through เชื่อมต่อจาก FastEthernet0 ของ PC2 ไปยัง FastEthernet0/2 ของ Switch2
3. **ตั้งค่า VLAN และพอร์ต Trunk บน Switch1**
    - สร้าง VLAN 10 และ VLAN 20 บน Switch1

```
Switch1> enable
Switch1# configure terminal
Switch1(config)# vlan 10
Switch1(config-vlan)# name VLAN10
Switch1(config-vlan)# exit
Switch1(config)# vlan 20
Switch1(config-vlan)# name VLAN20
Switch1(config-vlan)# exit
```

- ตั้งค่าพอร์ต Trunk บนพอร์ตที่เชื่อมต่อไปยัง Router

```
Switch1(config)# interface fastethernet 0/1
Switch1(config-if)# switchport mode trunk
Switch1(config-if)# switchport trunk allowed vlan all
Switch1(config-if)# exit
```

- ตั้งค่าพอร์ต Access สำหรับ VLAN 10 และ 20

```
Switch1(config)# interface range fastethernet 0/2 - 3
Switch1(config-if-range)# switchport mode access
Switch1(config-if-range)# switchport access vlan 10
Switch1(config-if-range)# exit
Switch1(config)# interface range fastethernet 0/4 - 5
Switch1(config-if-range)# switchport mode access
Switch1(config-if-range)# switchport access vlan 20
Switch1(config-if-range)# exit
Switch1(config)# exit
Switch1# write memory
```

4. **ตั้งค่า VLAN และพอร์ต Trunk บน Switch2**
   - สร้าง VLAN 10 และ VLAN 20 บน Switch2

```
Switch2> enable
Switch2# configure terminal
Switch2(config)# vlan 10
Switch2(config-vlan)# name VLAN10
Switch2(config-vlan)# exit
Switch2(config)# vlan 20
Switch2(config-vlan)# name VLAN20
Switch2(config-vlan)# exit
```

- ตั้งค่าพอร์ต Trunk บนพอร์ตที่เชื่อมต่อไปยัง Router

```
Switch2(config)# interface fastethernet 0/1
Switch2(config-if)# switchport mode trunk
Switch2(config-if)# switchport trunk allowed vlan all
Switch2(config-if)# exit
```

- ตั้งค่าพอร์ต Access สำหรับ VLAN 10 และ 20

```
Switch2(config)# interface range fastethernet 0/2 - 3
Switch2(config-if-range)# switchport mode access
Switch2(config-if-range)# switchport access vlan 10
Switch2(config-if-range)# exit
Switch2(config)# interface range fastethernet 0/4 - 5
Switch2(config-if-range)# switchport mode access
Switch2(config-if-range)# switchport access vlan 20
Switch2(config-if-range)# exit
Switch2(config)# exit
Switch2# write memory
```

5. **ตั้งค่า DHCP บน Router**
   - ตั้งค่า Sub-interface สำหรับ VLAN 10 และ 20 บน Router

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 0/0.10
Router(config-subif)# encapsulation dot1q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.0
Router(config-subif)# exit
Router(config)# interface gigabitethernet 0/0.20
Router(config-subif)# encapsulation dot1q 20
Router(config-subif)# ip address 192.168.20.1 255.255.255.0
```

```
Router(config-subif)# exit
Router(config)# interface gigabitethernet 0/0
Router(config-if)# no shutdown
Router(config-if)# exit
```

- ตั้งค่า DHCP Pool สำหรับ VLAN 10 และ 20 บน Router

```
Router(config)# ip dhcp pool VLAN10
Router(dhcp-config)# network 192.168.10.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.10.1
Router(dhcp-config)# exit
Router(config)# ip dhcp pool VLAN20
Router(dhcp-config)# network 192.168.20.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.20.1
Router(dhcp-config)# exit
Router(config)# ip dhcp excluded-address 192.168.10.1
Router(config)# ip dhcp excluded-address 192.168.20.1
Router(config)# exit
Router# write memory
```

6. **ตั้งค่า IP Configuration บน PC ให้เป็น DHCP**
   - เปิด PC1 > Desktop > IP Configuration
     - ตั้งค่า IP Configuration เป็น DHCP
   - เปิด PC2 > Desktop > IP Configuration
     - ตั้งค่า IP Configuration เป็น DHCP
7. **ทดสอบการเชื่อมต่อระหว่างเครื่อง PC ที่อยู่ใน VLAN ต่างกันด้วยคำสั่ง ping ใน Command Prompt**
   - เปิด Command Prompt บน PC1 และพิมพ์ ping 192.168.20.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC1 และ PC2 ผ่าน Inter-VLAN Routing
   - เปิด Command Prompt บน PC2 และพิมพ์ ping 192.168.10.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC2 และ PC1 ผ่าน Inter-VLAN Routing

สรุป

นักเรียนจะได้เรียนรู้การตั้งค่า DHCP Relay บน Switch L2 และ Router เพื่อแจกหมายเลข IP Address แบบอัตโนมัติในเครือข่ายที่มีการแบ่ง VLAN

ประโยชน์ของ LAB

- ช่วยให้นักเรียนเข้าใจการตั้งค่าและการใช้งาน DHCP Relay เพื่อแจกจ่าย IP Address แบบอัตโนมัติในเครือข่ายที่มีการแบ่ง VLAN
- เรียนรู้วิธีการตั้งค่า DHCP Relay บน Switch L2 และ Router
- เพิ่มความสะดวกและประสิทธิภาพในการจัดการ IP Address ในเครือข่าย

LAB 12: การตั้งค่า DHCP Relay บน Switch L2 และ Router สำหรับ 5 VLAN

ผู้สอน

ผู้ช่วยศาสตราจารย์อมร เจือตี๋
สาขาวิชาคอมพิวเตอร์ศึกษา คณะวิทยาศาสตร์และเทคโนโลยี

ชื่อ นามสกุล _____

หมู่เรียน _____

คะแนน _____

วัตถุประสงค์

1. เพื่อเรียนรู้การตั้งค่า DHCP Relay บน Switch L2 และ Router เพื่อแจกหมายเลข IP Address แบบอัตโนมัติสำหรับ 5 VLAN โดยหมายเลข IP ไม่ซ้ำกัน

อุปกรณ์ที่ใช้

- Switch L2 (Cisco 2960) จำนวน 2 ตัว
- Router (Cisco 1941) จำนวน 1 ตัว
- เครื่องคอมพิวเตอร์ (PC)
- สายเชื่อมต่อ (Straight-Through, Cross-Over)

การออกแบบหมายเลข IP Address

อุปกรณ์	พอร์ต	VLAN	IP Address	Subnet Mask	Default Gateway
PC1	NIC	10	DHCP	DHCP	DHCP
PC2	NIC	20	DHCP	DHCP	DHCP
PC3	NIC	30	DHCP	DHCP	DHCP
PC4	NIC	40	DHCP	DHCP	DHCP
PC5	NIC	50	DHCP	DHCP	DHCP

อุปกรณ์	พอร์ต	VLAN	IP Address	Subnet Mask	Default Gateway
Switch1	Fa0/1	Trunk	-	-	-
Switch2	Fa0/1	Trunk	-	-	-
Router	G0/0	Trunk	192.168.10.1	255.255.255.0	-
Router	G0/1	Trunk	192.168.20.1	255.255.255.0	-
Router	G0/2	Trunk	192.168.30.1	255.255.255.0	-
Router	G0/3	Trunk	192.168.40.1	255.255.255.0	-
Router	G0/4	Trunk	192.168.50.1	255.255.255.0	-

วิธีการทำ

1. **เปิดโปรแกรม Cisco Packet Tracer และสร้างการเชื่อมต่อระหว่าง Switch, Router และ PC**
    - เปิดโปรแกรม Cisco Packet Tracer
    - ลาก Switch L2 จำนวน 2 ตัว, Router (Cisco 1941) จำนวน 1 ตัว และ PC จำนวน 5 เครื่อง ไปวางในพื้นที่การทำงาน
2. **เชื่อมต่อสาย**
    - ใช้สาย Cross-Over เชื่อมต่อจาก FastEthernet0/1 ของ Switch1 ไปยัง FastEthernet0/1 ของ Switch2
    - ใช้สาย Straight-Through เชื่อมต่อจาก GigabitEthernet0/0 ของ Router ไปยัง FastEthernet0/1 ของ Switch1
    - ใช้สาย Straight-Through เชื่อมต่อจาก GigabitEthernet0/1 ของ Router ไปยัง FastEthernet0/2 ของ Switch1
    - ใช้สาย Straight-Through เชื่อมต่อจาก GigabitEthernet0/2 ของ Router ไปยัง FastEthernet0/3 ของ Switch1
    - ใช้สาย Straight-Through เชื่อมต่อจาก GigabitEthernet0/3 ของ Router ไปยัง FastEthernet0/4 ของ Switch1
    - ใช้สาย Straight-Through เชื่อมต่อจาก GigabitEthernet0/4 ของ Router ไปยัง FastEthernet0/5 ของ Switch1

- ใช้สาย Straight-Through เชื่อมต่อจาก FastEthernet0 ของ PC1 ไปยัง FastEthernet0/2 ของ Switch1
- ใช้สาย Straight-Through เชื่อมต่อจาก FastEthernet0 ของ PC2 ไปยัง FastEthernet0/3 ของ Switch2
- ใช้สาย Straight-Through เชื่อมต่อจาก FastEthernet0 ของ PC3 ไปยัง FastEthernet0/4 ของ Switch1
- ใช้สาย Straight-Through เชื่อมต่อจาก FastEthernet0 ของ PC4 ไปยัง FastEthernet0/5 ของ Switch2
- ใช้สาย Straight-Through เชื่อมต่อจาก FastEthernet0 ของ PC5 ไปยัง FastEthernet0/6 ของ Switch1

3. **ตั้งค่า VLAN และพอร์ต Trunk บน Switch1**
   - สร้าง VLAN 10, 20, 30, 40 และ 50 บน Switch1

```
Switch1> enable
Switch1# configure terminal
Switch1(config)# vlan 10
Switch1(config-vlan)# name VLAN10
Switch1(config-vlan)# exit
Switch1(config)# vlan 20
Switch1(config-vlan)# name VLAN20
Switch1(config-vlan)# exit
Switch1(config)# vlan 30
Switch1(config-vlan)# name VLAN30
Switch1(config-vlan)# exit
Switch1(config)# vlan 40
Switch1(config-vlan)# name VLAN40
Switch1(config-vlan)# exit
Switch1(config)# vlan 50
Switch1(config-vlan)# name VLAN50
Switch1(config-vlan)# exit
```

- ตั้งค่าพอร์ต Trunk บนพอร์ตที่เชื่อมต่อไปยัง Router

```
Switch1(config)# interface fastethernet 0/1
Switch1(config-if)# switchport mode trunk
Switch1(config-if)# switchport trunk allowed vlan all
Switch1(config-if)# exit
```

- ตั้งค่าพอร์ต Access สำหรับ VLAN 10, 20, 30, 40 และ 50

```
Switch1(config)# interface range fastethernet 0/2
Switch1(config-if-range)# switchport mode access
Switch1(config-if-range)# switchport access vlan 10
Switch1(config-if-range)# exit
Switch1(config)# interface range fastethernet 0/3
Switch1(config-if-range)# switchport mode access
Switch1(config-if-range)# switchport access vlan 20
Switch1(config-if-range)# exit
Switch1(config)# interface range fastethernet 0/4
Switch1(config-if-range)# switchport mode access
Switch1(config-if-range)# switchport access vlan 30
Switch1(config-if-range)# exit
Switch1(config)# interface range fastethernet 0/5
Switch1(config-if-range)# switchport mode access
Switch1(config-if-range)# switchport access vlan 40
Switch1(config-if-range)# exit
Switch1(config)# interface range fastethernet 0/6
Switch1(config-if-range)# switchport mode access
Switch1(config-if-range)# switchport access vlan 50
Switch1(config-if-range)# exit
Switch1(config)# exit
Switch1# write memory
```

4. **ตั้งค่า VLAN และพอร์ต Trunk บน Switch2**
    - สร้าง VLAN 10, 20, 30, 40 และ 50 บน Switch2

```
Switch2> enable
Switch2# configure terminal
Switch2(config)# vlan 10
Switch2(config-vlan)# name VLAN10
Switch2(config-vlan)# exit
Switch2(config)# vlan 20
Switch2(config-vlan)# name VLAN20
Switch2(config-vlan)# exit
Switch2(config)# vlan 30
Switch2(config-vlan)# name VLAN30
Switch2(config-vlan)# exit
Switch2(config)# vlan 40
Switch2(config-vlan)# name VLAN40
Switch2(config-vlan)# exit
Switch2(config)# vlan 50
Switch2(config-vlan)# name VLAN50
Switch2(config-vlan)# exit
```

    - ตั้งค่าพอร์ต Trunk บนพอร์ตที่เชื่อมต่อไปยัง Router

```
Switch2(config)# interface fastethernet 0/1
Switch2(config-if)# switchport mode trunk
Switch2(config-if)# switchport trunk allowed vlan all
Switch2(config-if)# exit
```

    - ตั้งค่าพอร์ต Access สำหรับ VLAN 10, 20, 30, 40 และ 50

```
Switch2(config)# interface range fastethernet 0/2
Switch2(config-if-range)# switchport mode access
```

```
Switch2(config-if-range)# switchport access vlan 10
Switch2(config-if-range)# exit
Switch2(config)# interface range fastethernet 0/3
Switch2(config-if-range)# switchport mode access
Switch2(config-if-range)# switchport access vlan 20
Switch2(config-if-range)# exit
Switch2(config)# interface range fastethernet 0/4
Switch2(config-if-range)# switchport mode access
Switch2(config-if-range)# switchport access vlan 30
Switch2(config-if-range)# exit
Switch2(config)# interface range fastethernet 0/5
Switch2(config-if-range)# switchport mode access
Switch2(config-if-range)# switchport access vlan 40
Switch2(config-if-range)# exit
Switch2(config)# interface range fastethernet 0/6
Switch2(config-if-range)# switchport mode access
Switch2(config-if-range)# switchport access vlan 50
Switch2(config-if-range)# exit
Switch2(config)# exit
Switch2# write memory
```

5. **ตั้งค่า DHCP บน Router**
    - ตั้งค่า Sub-interface สำหรับ VLAN 10, 20, 30, 40 และ 50 บน Router

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 0/0.10
Router(config-subif)# encapsulation dot1q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.0
Router(config-subif)# exit
Router(config)# interface gigabitethernet 0/0.20
```

```
Router(config-subif)# encapsulation dot1q 20
Router(config-subif)# ip address 192.168.20.1 255.255.255.0
Router(config-subif)# exit
Router(config)# interface gigabitethernet 0/0.30
Router(config-subif)# encapsulation dot1q 30
Router(config-subif)# ip address 192.168.30.1 255.255.255.0
Router(config-subif)# exit
Router(config)# interface gigabitethernet 0/0.40
Router(config-subif)# encapsulation dot1q 40
Router(config-subif)# ip address 192.168.40.1 255.255.255.0
Router(config-subif)# exit
Router(config)# interface gigabitethernet 0/0.50
Router(config-subif)# encapsulation dot1q 50
Router(config-subif)# ip address 192.168.50.1 255.255.255.0
Router(config-subif)# exit
Router(config)# interface gigabitethernet 0/0
Router(config-if)# no shutdown
Router(config-if)# exit
```

- ตั้งค่า DHCP Pool สำหรับ VLAN 10, 20, 30, 40 และ 50 บน Router

```
Router(config)# ip dhcp pool VLAN10
Router(dhcp-config)# network 192.168.10.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.10.1
Router(dhcp-config)# exit
Router(config)# ip dhcp pool VLAN20
Router(dhcp-config)# network 192.168.20.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.20.1
Router(dhcp-config)# exit
Router(config)# ip dhcp pool VLAN30
Router(dhcp-config)# network 192.168.30.0 255.255.255.0
```

```
Router(dhcp-config)# default-router 192.168.30.1
Router(dhcp-config)# exit
Router(config)# ip dhcp pool VLAN40
Router(dhcp-config)# network 192.168.40.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.40.1
Router(dhcp-config)# exit
Router(config)# ip dhcp pool VLAN50
Router(dhcp-config)# network 192.168.50.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.50.1
Router(dhcp-config)# exit
Router(config)# ip dhcp excluded-address 192.168.10.1
Router(config)# ip dhcp excluded-address 192.168.20.1
Router(config)# ip dhcp excluded-address 192.168.30.1
Router(config)# ip dhcp excluded-address 192.168.40.1
Router(config)# ip dhcp excluded-address 192.168.50.1
Router(config)# exit
Router# write memory
```

6. **ตั้งค่า IP Configuration บน PC ให้เป็น DHCP**
    - เปิด PC1 > Desktop > IP Configuration
        - ตั้งค่า IP Configuration เป็น DHCP
    - เปิด PC2 > Desktop > IP Configuration
        - ตั้งค่า IP Configuration เป็น DHCP
    - เปิด PC3 > Desktop > IP Configuration
        - ตั้งค่า IP Configuration เป็น DHCP
    - เปิด PC4 > Desktop > IP Configuration
        - ตั้งค่า IP Configuration เป็น DHCP
    - เปิด PC5 > Desktop > IP Configuration
        - ตั้งค่า IP Configuration เป็น DHCP

7. **ทดสอบการเชื่อมต่อระหว่างเครื่อง PC ที่อยู่ใน VLAN ต่างกันด้วยคำสั่ง ping ใน Command Prompt**
    - เปิด Command Prompt บน PC1 และพิมพ์ ping 192.168.20.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC1 และ PC2 ผ่าน Inter-VLAN Routing
    - เปิด Command Prompt บน PC2 และพิมพ์ ping 192.168.30.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC2 และ PC3 ผ่าน Inter-VLAN Routing
    - เปิด Command Prompt บน PC3 และพิมพ์ ping 192.168.40.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC3 และ PC4 ผ่าน Inter-VLAN Routing
    - เปิด Command Prompt บน PC4 และพิมพ์ ping 192.168.50.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC4 และ PC5 ผ่าน Inter-VLAN Routing
    - เปิด Command Prompt บน PC5 และพิมพ์ ping 192.168.10.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC5 และ PC1 ผ่าน Inter-VLAN Routing

สรุป

นักเรียนจะได้เรียนรู้การตั้งค่า DHCP Relay บน Switch L2 และ Router เพื่อแจกหมายเลข IP Address แบบอัตโนมัติในเครือข่ายที่มีการแบ่ง VLAN โดยหมายเลข IP ไม่ซ้ำกัน

ประโยชน์ของ LAB

- ช่วยให้นักเรียนเข้าใจการตั้งค่าและการใช้งาน DHCP Relay เพื่อแจกจ่าย IP Address แบบอัตโนมัติในเครือข่ายที่มีการแบ่ง VLAN
- เรียนรู้วิธีการตั้งค่า DHCP Relay บน Switch L2 และ Router
- เพิ่มความสะดวกและประสิทธิภาพในการจัดการ IP Address ในเครือข่าย

LAB 13: การตั้งค่า DHCP Relay และ Inter-VLAN Routing บน Switch L2 และ Router สำหรับ 5 VLAN

ผู้สอน

ผู้ช่วยศาสตราจารย์อมร เจือตี๋
สาขาวิชาคอมพิวเตอร์ศึกษา คณะวิทยาศาสตร์และเทคโนโลยี

ชื่อ นามสกุล _____

หมู่เรียน _____

คะแนน _____

วัตถุประสงค์

1. เพื่อเรียนรู้การตั้งค่า DHCP Relay บน Switch L2 และ Router เพื่อแจกหมายเลข IP Address แบบอัตโนมัติสำหรับ 5 VLAN โดยหมายเลข IP ไม่ซ้ำกัน
2. เพื่อเรียนรู้การตั้งค่า Inter-VLAN Routing บน Router เพื่อให้แต่ละ VLAN สามารถสื่อสารกันได้

อุปกรณ์ที่ใช้

- Switch L2 (Cisco 2960) จำนวน 2 ตัว
- Router (Cisco 1941) จำนวน 1 ตัว
- เครื่องคอมพิวเตอร์ (PC)
- สายเชื่อมต่อ (Straight-Through, Cross-Over)

การออกแบบหมายเลข IP Address

อุปกรณ์	พอร์ต	VLAN	IP Address	Subnet Mask	Default Gateway
PC1	NIC	10	DHCP	DHCP	DHCP
PC2	NIC	20	DHCP	DHCP	DHCP
PC3	NIC	30	DHCP	DHCP	DHCP

อุปกรณ์	พอร์ต	VLAN	IP Address	Subnet Mask	Default Gateway
PC4	NIC	40	DHCP	DHCP	DHCP
PC5	NIC	50	DHCP	DHCP	DHCP
Switch1	Fa0/1	Trunk	-	-	-
Switch2	Fa0/1	Trunk	-	-	-
Router	G0/0	Trunk	192.168.10.1	255.255.255.0	-
Router	G0/1	Trunk	192.168.20.1	255.255.255.0	-
Router	G0/2	Trunk	192.168.30.1	255.255.255.0	-
Router	G0/3	Trunk	192.168.40.1	255.255.255.0	-
Router	G0/4	Trunk	192.168.50.1	255.255.255.0	-

วิธีการทำ

1. **เปิดโปรแกรม Cisco Packet Tracer และสร้างการเชื่อมต่อระหว่าง Switch, Router และ PC**
    - เปิดโปรแกรม Cisco Packet Tracer
    - ลาก Switch L2 จำนวน 2 ตัว, Router (Cisco 1941) จำนวน 1 ตัว และ PC จำนวน 5 เครื่อง ไปวางในพื้นที่การทำงาน
2. **เชื่อมต่อสาย**
    - ใช้สาย Cross-Over เชื่อมต่อจาก FastEthernet0/1 ของ Switch1 ไปยัง FastEthernet0/1 ของ Switch2
    - ใช้สาย Straight-Through เชื่อมต่อจาก GigabitEthernet0/0 ของ Router ไปยัง FastEthernet0/1 ของ Switch1
    - ใช้สาย Straight-Through เชื่อมต่อจาก GigabitEthernet0/1 ของ Router ไปยัง FastEthernet0/2 ของ Switch1
    - ใช้สาย Straight-Through เชื่อมต่อจาก GigabitEthernet0/2 ของ Router ไปยัง FastEthernet0/3 ของ Switch1
    - ใช้สาย Straight-Through เชื่อมต่อจาก GigabitEthernet0/3 ของ Router ไปยัง FastEthernet0/4 ของ Switch1

- ใช้สาย Straight-Through เชื่อมต่อจาก GigabitEthernet0/4 ของ Router ไปยัง FastEthernet0/5 ของ Switch1
- ใช้สาย Straight-Through เชื่อมต่อจาก FastEthernet0 ของ PC1 ไปยัง FastEthernet0/2 ของ Switch1
- ใช้สาย Straight-Through เชื่อมต่อจาก FastEthernet0 ของ PC2 ไปยัง FastEthernet0/3 ของ Switch2
- ใช้สาย Straight-Through เชื่อมต่อจาก FastEthernet0 ของ PC3 ไปยัง FastEthernet0/4 ของ Switch1
- ใช้สาย Straight-Through เชื่อมต่อจาก FastEthernet0 ของ PC4 ไปยัง FastEthernet0/5 ของ Switch2
- ใช้สาย Straight-Through เชื่อมต่อจาก FastEthernet0 ของ PC5 ไปยัง FastEthernet0/6 ของ Switch1

3. **ตั้งค่า VLAN และพอร์ต Trunk บน Switch1**
   - สร้าง VLAN 10, 20, 30, 40 และ 50 บน Switch1

```
Switch1> enable
Switch1# configure terminal
Switch1(config)# vlan 10
Switch1(config-vlan)# name VLAN10
Switch1(config-vlan)# exit
Switch1(config)# vlan 20
Switch1(config-vlan)# name VLAN20
Switch1(config-vlan)# exit
Switch1(config)# vlan 30
Switch1(config-vlan)# name VLAN30
Switch1(config-vlan)# exit
Switch1(config)# vlan 40
Switch1(config-vlan)# name VLAN40
Switch1(config-vlan)# exit
Switch1(config)# vlan 50
Switch1(config-vlan)# name VLAN50
```

```
Switch1(config-vlan)# exit
```

- ตั้งค่าพอร์ต Trunk บนพอร์ตที่เชื่อมต่อไปยัง Router

```
Switch1(config)# interface fastethernet 0/1
Switch1(config-if)# switchport mode trunk
Switch1(config-if)# switchport trunk allowed vlan all
Switch1(config-if)# exit
```

- ตั้งค่าพอร์ต Access สำหรับ VLAN 10, 20, 30, 40 และ 50

```
Switch1(config)# interface range fastethernet 0/2
Switch1(config-if-range)# switchport mode access
Switch1(config-if-range)# switchport access vlan 10
Switch1(config-if-range)# exit
Switch1(config)# interface range fastethernet 0/3
Switch1(config-if-range)# switchport mode access
Switch1(config-if-range)# switchport access vlan 20
Switch1(config-if-range)# exit
Switch1(config)# interface range fastethernet 0/4
Switch1(config-if-range)# switchport mode access
Switch1(config-if-range)# switchport access vlan 30
Switch1(config-if-range)# exit
Switch1(config)# interface range fastethernet 0/5
Switch1(config-if-range)# switchport mode access
Switch1(config-if-range)# switchport access vlan 40
Switch1(config-if-range)# exit
Switch1(config)# interface range fastethernet 0/6
Switch1(config-if-range)# switchport mode access
Switch1(config-if-range)# switchport access vlan 50
Switch1(config-if-range)# exit
Switch1(config)# exit
```

```
Switch1# write memory
```

4. **ตั้งค่า VLAN และพอร์ต Trunk บน Switch2**
   - สร้าง VLAN 10, 20, 30, 40 และ 50 บน Switch2

```
Switch2> enable
Switch2# configure terminal
Switch2(config)# vlan 10
Switch2(config-vlan)# name VLAN10
Switch2(config-vlan)# exit
Switch2(config)# vlan 20
Switch2(config-vlan)# name VLAN20
Switch2(config-vlan)# exit
Switch2(config)# vlan 30
Switch2(config-vlan)# name VLAN30
Switch2(config-vlan)# exit
Switch2(config)# vlan 40
Switch2(config-vlan)# name VLAN40
Switch2(config-vlan)# exit
Switch2(config)# vlan 50
Switch2(config-vlan)# name VLAN50
Switch2(config-vlan)# exit
```

   - ตั้งค่าพอร์ต Trunk บนพอร์ตที่เชื่อมต่อไปยัง Router

```
Switch2(config)# interface fastethernet 0/1
Switch2(config-if)# switchport mode trunk
Switch2(config-if)# switchport trunk allowed vlan all
Switch2(config-if)# exit
```

   - ตั้งค่าพอร์ต Access สำหรับ VLAN 10, 20, 30, 40 และ 50

```
Switch2(config)# interface range fastethernet 0/2
Switch2(config-if-range)# switchport mode access
Switch2(config-if-range)# switchport access vlan 10
Switch2(config-if-range)# exit
Switch2(config)# interface range fastethernet 0/3
Switch2(config-if-range)# switchport mode access
Switch2(config-if-range)# switchport access vlan 20
Switch2(config-if-range)# exit
Switch2(config)# interface range fastethernet 0/4
Switch2(config-if-range)# switchport mode access
Switch2(config-if-range)# switchport access vlan 30
Switch2(config-if-range)# exit
Switch2(config)# interface range fastethernet 0/5
Switch2(config-if-range)# switchport mode access
Switch2(config-if-range)# switchport access vlan 40
Switch2(config-if-range)# exit
Switch2(config)# interface range fastethernet 0/6
Switch2(config-if-range)# switchport mode access
Switch2(config-if-range)# switchport access vlan 50
Switch2(config-if-range)# exit
Switch2(config)# exit
Switch2# write memory
```

5. **ตั้งค่า Inter-VLAN Routing และ DHCP บน Router**
    - ตั้งค่า Sub-interface สำหรับ VLAN 10, 20, 30, 40 และ 50 บน Router

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 0/0.10
Router(config-subif)# encapsulation dot1q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.0
```

```
Router(config-subif)# exit
Router(config)# interface gigabitethernet 0/0.20
Router(config-subif)# encapsulation dot1q 20
Router(config-subif)# ip address 192.168.20.1 255.255.255.0
Router(config-subif)# exit
Router(config)# interface gigabitethernet 0/0.30
Router(config-subif)# encapsulation dot1q 30
Router(config-subif)# ip address 192.168.30.1 255.255.255.0
Router(config-subif)# exit
Router(config)# interface gigabitethernet 0/0.40
Router(config-subif)# encapsulation dot1q 40
Router(config-subif)# ip address 192.168.40.1 255.255.255.0
Router(config-subif)# exit
Router(config)# interface gigabitethernet 0/0.50
Router(config-subif)# encapsulation dot1q 50
Router(config-subif)# ip address 192.168.50.1 255.255.255.0
Router(config-subif)# exit
Router(config)# interface gigabitethernet 0/0
Router(config-if)# no shutdown
Router(config-if)# exit
```

- ตั้งค่า DHCP Pool สำหรับ VLAN 10, 20, 30, 40 และ 50 บน Router

```
Router(config)# ip dhcp pool VLAN10
Router(dhcp-config)# network 192.168.10.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.10.1
Router(dhcp-config)# exit
Router(config)# ip dhcp pool VLAN20
Router(dhcp-config)# network 192.168.20.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.20.1
Router(dhcp-config)# exit
```

```
Router(config)# ip dhcp pool VLAN30
Router(dhcp-config)# network 192.168.30.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.30.1
Router(dhcp-config)# exit
Router(config)# ip dhcp pool VLAN40
Router(dhcp-config)# network 192.168.40.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.40.1
Router(dhcp-config)# exit
Router(config)# ip dhcp pool VLAN50
Router(dhcp-config)# network 192.168.50.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.50.1
Router(dhcp-config)# exit
Router(config)# ip dhcp excluded-address 192.168.10.1
Router(config)# ip dhcp excluded-address 192.168.20.1
Router(config)# ip dhcp excluded-address 192.168.30.1
Router(config)# ip dhcp excluded-address 192.168.40.1
Router(config)# ip dhcp excluded-address 192.168.50.1
Router(config)# exit
Router# write memory
```

6. **ตั้งค่า IP Configuration บน PC ให้เป็น DHCP**
    - เปิด PC1 > Desktop > IP Configuration
        - ตั้งค่า IP Configuration เป็น DHCP
    - เปิด PC2 > Desktop > IP Configuration
        - ตั้งค่า IP Configuration เป็น DHCP
    - เปิด PC3 > Desktop > IP Configuration
        - ตั้งค่า IP Configuration เป็น DHCP
    - เปิด PC4 > Desktop > IP Configuration
        - ตั้งค่า IP Configuration เป็น DHCP
    - เปิด PC5 > Desktop > IP Configuration
        - ตั้งค่า IP Configuration เป็น DHCP

7. **ทดสอบการเชื่อมต่อระหว่างเครื่อง PC ที่อยู่ใน VLAN ต่างกันด้วยคำสั่ง ping ใน Command Prompt**
    - เปิด Command Prompt บน PC1 และพิมพ์ ping 192.168.20.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC1 และ PC2 ผ่าน Inter-VLAN Routing
    - เปิด Command Prompt บน PC2 และพิมพ์ ping 192.168.30.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC2 และ PC3 ผ่าน Inter-VLAN Routing
    - เปิด Command Prompt บน PC3 และพิมพ์ ping 192.168.40.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC3 และ PC4 ผ่าน Inter-VLAN Routing
    - เปิด Command Prompt บน PC4 และพิมพ์ ping 192.168.50.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC4 และ PC5 ผ่าน Inter-VLAN Routing
    - เปิด Command Prompt บน PC5 และพิมพ์ ping 192.168.10.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC5 และ PC1 ผ่าน Inter-VLAN Routing

สรุป

นักเรียนจะได้เรียนรู้การตั้งค่า DHCP Relay และ Inter-VLAN Routing บน Switch L2 และ Router เพื่อแจกหมายเลข IP Address แบบอัตโนมัติในเครือข่ายที่มีการแบ่ง VLAN และให้ VLAN ต่างๆ สามารถสื่อสารกันได้

ประโยชน์ของ LAB

- ช่วยให้นักเรียนเข้าใจการตั้งค่าและการใช้งาน DHCP Relay เพื่อแจกจ่าย IP Address แบบอัตโนมัติในเครือข่ายที่มีการแบ่ง VLAN
- เรียนรู้วิธีการตั้งค่า Inter-VLAN Routing บน Router เพื่อให้ VLAN ต่างๆ สามารถสื่อสารกันได้
- เพิ่มความสะดวกและประสิทธิภาพในการจัดการ IP Address ในเครือข่าย

LAB 14: การตั้งค่า DHCP Relay และ Inter-VLAN Routing บน Switch L2 และ Router สำหรับ 5 VLAN โดยใช้ 2 Router

ผู้สอน

ผู้ช่วยศาสตราจารย์อมร เจือตี๋
สาขาวิชาคอมพิวเตอร์ศึกษา คณะวิทยาศาสตร์และเทคโนโลยี

ชื่อ นามสกุล _____

หมู่เรียน _____

คะแนน _____

วัตถุประสงค์

1. เพื่อเรียนรู้การตั้งค่า DHCP Relay บน Switch L2 และ Router เพื่อแจกหมายเลข IP Address แบบอัตโนมัติสำหรับ 5 VLAN โดยหมายเลข IP ไม่ซ้ำกัน
2. เพื่อเรียนรู้การตั้งค่า Inter-VLAN Routing บน Router เพื่อให้แต่ละ VLAN สามารถสื่อสารกันได้

อุปกรณ์ที่ใช้

- Switch L2 (Cisco 2960) จำนวน 2 ตัว
- Router (Cisco 1941) จำนวน 2 ตัว
- เครื่องคอมพิวเตอร์ (PC)
- สายเชื่อมต่อ (Straight-Through, Cross-Over)

การออกแบบหมายเลข IP Address

อุปกรณ์	พอร์ต	VLAN	IP Address	Subnet Mask	Default Gateway
PC1	NIC	10	DHCP	DHCP	DHCP
PC2	NIC	20	DHCP	DHCP	DHCP
PC3	NIC	30	DHCP	DHCP	DHCP

อุปกรณ์	พอร์ต	VLAN	IP Address	Subnet Mask	Default Gateway
PC4	NIC	40	DHCP	DHCP	DHCP
PC5	NIC	50	DHCP	DHCP	DHCP
Switch1	Fa0/1	Trunk	-	-	-
Switch2	Fa0/1	Trunk	-	-	-
Router1	G0/0	Trunk	192.168.10.1	255.255.255.0	-
Router1	G0/1	Trunk	192.168.20.1	255.255.255.0	-
Router1	G0/2	Trunk	192.168.30.1	255.255.255.0	-
Router2	G0/0	Trunk	192.168.40.1	255.255.255.0	-
Router2	G0/1	Trunk	192.168.50.1	255.255.255.0	-

วิธีการทำ

1. **เปิดโปรแกรม Cisco Packet Tracer และสร้างการเชื่อมต่อระหว่าง Switch, Router และ PC**
    - เปิดโปรแกรม Cisco Packet Tracer
    - ลาก Switch L2 จำนวน 2 ตัว, Router (Cisco 1941) จำนวน 2 ตัว และ PC จำนวน 5 เครื่อง ไปวางในพื้นที่การทำงาน
2. **เชื่อมต่อสาย**
    - ใช้สาย Cross-Over เชื่อมต่อจาก FastEthernet0/1 ของ Switch1 ไปยัง FastEthernet0/1 ของ Switch2
    - ใช้สาย Straight-Through เชื่อมต่อจาก GigabitEthernet0/0 ของ Router1 ไปยัง FastEthernet0/2 ของ Switch1
    - ใช้สาย Straight-Through เชื่อมต่อจาก GigabitEthernet0/1 ของ Router1 ไปยัง FastEthernet0/3 ของ Switch1
    - ใช้สาย Straight-Through เชื่อมต่อจาก GigabitEthernet0/2 ของ Router1 ไปยัง FastEthernet0/4 ของ Switch1
    - ใช้สาย Straight-Through เชื่อมต่อจาก GigabitEthernet0/0 ของ Router2 ไปยัง FastEthernet0/5 ของ Switch1

- ใช้สาย Straight-Through เชื่อมต่อจาก GigabitEthernet0/1 ของ Router2 ไปยัง FastEthernet0/6 ของ Switch1
- ใช้สาย Straight-Through เชื่อมต่อจาก FastEthernet0 ของ PC1 ไปยัง FastEthernet0/2 ของ Switch1
- ใช้สาย Straight-Through เชื่อมต่อจาก FastEthernet0 ของ PC2 ไปยัง FastEthernet0/3 ของ Switch2
- ใช้สาย Straight-Through เชื่อมต่อจาก FastEthernet0 ของ PC3 ไปยัง FastEthernet0/4 ของ Switch1
- ใช้สาย Straight-Through เชื่อมต่อจาก FastEthernet0 ของ PC4 ไปยัง FastEthernet0/5 ของ Switch2
- ใช้สาย Straight-Through เชื่อมต่อจาก FastEthernet0 ของ PC5 ไปยัง FastEthernet0/6 ของ Switch1

3. **ตั้งค่า VLAN และพอร์ต Trunk บน Switch1**
   - สร้าง VLAN 10, 20, 30, 40 และ 50 บน Switch1

```
Switch1> enable
Switch1# configure terminal
Switch1(config)# vlan 10
Switch1(config-vlan)# name VLAN10
Switch1(config-vlan)# exit
Switch1(config)# vlan 20
Switch1(config-vlan)# name VLAN20
Switch1(config-vlan)# exit
Switch1(config)# vlan 30
Switch1(config-vlan)# name VLAN30
Switch1(config-vlan)# exit
Switch1(config)# vlan 40
Switch1(config-vlan)# name VLAN40
Switch1(config-vlan)# exit
Switch1(config)# vlan 50
Switch1(config-vlan)# name VLAN50
```

```
Switch1(config-vlan)# exit
```

- ตั้งค่าพอร์ต Trunk บนพอร์ตที่เชื่อมต่อไปยัง Router

```
Switch1(config)# interface fastethernet 0/1
Switch1(config-if)# switchport mode trunk
Switch1(config-if)# switchport trunk allowed vlan all
Switch1(config-if)# exit
```

- ตั้งค่าพอร์ต Access สำหรับ VLAN 10, 20, 30, 40 และ 50

```
Switch1(config)# interface range fastethernet 0/2
Switch1(config-if-range)# switchport mode access
Switch1(config-if-range)# switchport access vlan 10
Switch1(config-if-range)# exit
Switch1(config)# interface range fastethernet 0/3
Switch1(config-if-range)# switchport mode access
Switch1(config-if-range)# switchport access vlan 20
Switch1(config-if-range)# exit
Switch1(config)# interface range fastethernet 0/4
Switch1(config-if-range)# switchport mode access
Switch1(config-if-range)# switchport access vlan 30
Switch1(config-if-range)# exit
Switch1(config)# interface range fastethernet 0/5
Switch1(config-if-range)# switchport mode access
Switch1(config-if-range)# switchport access vlan 40
Switch1(config-if-range)# exit
Switch1(config)# interface range fastethernet 0/6
Switch1(config-if-range)# switchport mode access
Switch1(config-if-range)# switchport access vlan 50
Switch1(config-if-range)# exit
Switch1(config)# exit
```

```
Switch1# write memory
```

4. **ตั้งค่า VLAN และพอร์ต Trunk บน Switch2**
   - สร้าง VLAN 10, 20, 30, 40 และ 50 บน Switch2

```
Switch2> enable
Switch2# configure terminal
Switch2(config)# vlan 10
Switch2(config-vlan)# name VLAN10
Switch2(config-vlan)# exit
Switch2(config)# vlan 20
Switch2(config-vlan)# name VLAN20
Switch2(config-vlan)# exit
Switch2(config)# vlan 30
Switch2(config-vlan)# name VLAN30
Switch2(config-vlan)# exit
Switch2(config)# vlan 40
Switch2(config-vlan)# name VLAN40
Switch2(config-vlan)# exit
Switch2(config)# vlan 50
Switch2(config-vlan)# name VLAN50
Switch2(config-vlan)# exit
```

   - ตั้งค่าพอร์ต Trunk บนพอร์ตที่เชื่อมต่อไปยัง Router

```
Switch2(config)# interface fastethernet 0/1
Switch2(config-if)# switchport mode trunk
Switch2(config-if)# switchport trunk allowed vlan all
Switch2(config-if)# exit
```

   - ตั้งค่าพอร์ต Access สำหรับ VLAN 10, 20, 30, 40 และ 50

```
Switch2(config)# interface range fastethernet 0/2
Switch2(config-if-range)# switchport mode access
Switch2(config-if-range)# switchport access vlan 10
Switch2(config-if-range)# exit
Switch2(config)# interface range fastethernet 0/3
Switch2(config-if-range)# switchport mode access
Switch2(config-if-range)# switchport access vlan 20
Switch2(config-if-range)# exit
Switch2(config)# interface range fastethernet 0/4
Switch2(config-if-range)# switchport mode access
Switch2(config-if-range)# switchport access vlan 30
Switch2(config-if-range)# exit
Switch2(config)# interface range fastethernet 0/5
Switch2(config-if-range)# switchport mode access
Switch2(config-if-range)# switchport access vlan 40
Switch2(config-if-range)# exit
Switch2(config)# interface range fastethernet 0/6
Switch2(config-if-range)# switchport mode access
Switch2(config-if-range)# switchport access vlan 50
Switch2(config-if-range)# exit
Switch2(config)# exit
Switch2# write memory
```

5. **ตั้งค่า Inter-VLAN Routing และ DHCP บน Router1 และ Router2**
    - ตั้งค่า Sub-interface สำหรับ VLAN 10, 20, 30 บน Router1

```
Router1> enable
Router1# configure terminal
Router1(config)# interface gigabitethernet 0/0.10
Router1(config-subif)# encapsulation dot1q 10
Router1(config-subif)# ip address 192.168.10.1 255.255.255.0
```

```
Router1(config-subif)# exit
Router1(config)# interface gigabitethernet 0/0.20
Router1(config-subif)# encapsulation dot1q 20
Router1(config-subif)# ip address 192.168.20.1 255.255.255.0
Router1(config-subif)# exit
Router1(config)# interface gigabitethernet 0/0.30
Router1(config-subif)# encapsulation dot1q 30
Router1(config-subif)# ip address 192.168.30.1 255.255.255.0
Router1(config-subif)# exit
Router1(config)# interface gigabitethernet 0/0
Router1(config-if)# no shutdown
Router1(config-if)# exit
```

- ตั้งค่า Sub-interface สำหรับ VLAN 40 และ 50 บน Router2

```
Router2> enable
Router2# configure terminal
Router2(config)# interface gigabitethernet 0/0.40
Router2(config-subif)# encapsulation dot1q 40
Router2(config-subif)# ip address 192.168.40.1 255.255.255.0
Router2(config-subif)# exit
Router2(config)# interface gigabitethernet 0/0.50
Router2(config-subif)# encapsulation dot1q 50
Router2(config-subif)# ip address 192.168.50.1 255.255.255.0
Router2(config-subif)# exit
Router2(config)# interface gigabitethernet 0/0
Router2(config-if)# no shutdown
Router2(config-if)# exit
```

- ตั้งค่า DHCP Pool สำหรับ VLAN 10, 20, 30 บน Router1

```
Router1(config)# ip dhcp pool VLAN10
Router1(dhcp-config)# network 192.168.10.0 255.255.255.0
Router1(dhcp-config)# default-router 192.168.10.1
Router1(dhcp-config)# exit
Router1(config)# ip dhcp pool VLAN20
Router1(dhcp-config)# network 192.168.20.0 255.255.255.0
Router1(dhcp-config)# default-router 192.168.20.1
Router1(dhcp-config)# exit
Router1(config)# ip dhcp pool VLAN30
Router1(dhcp-config)# network 192.168.30.0 255.255.255.0
Router1(dhcp-config)# default-router 192.168.30.1
Router1(dhcp-config)# exit
Router1(config)# ip dhcp excluded-address 192.168.10.1
Router1(config)# ip dhcp excluded-address 192.168.20.1
Router1(config)# ip dhcp excluded-address 192.168.30.1
Router1(config)# exit
Router1# write memory
```

- ตั้งค่า DHCP Pool สำหรับ VLAN 40 และ 50 บน Router2

```
Router2(config)# ip dhcp pool VLAN40
Router2(dhcp-config)# network 192.168.40.0 255.255.255.0
Router2(dhcp-config)# default-router 192.168.40.1
Router2(dhcp-config)# exit
Router2(config)# ip dhcp pool VLAN50
Router2(dhcp-config)# network 192.168.50.0 255.255.255.0
Router2(dhcp-config)# default-router 192.168.50.1
Router2(dhcp-config)# exit
```

```
Router2(config)# ip dhcp excluded-address 192.168.40.1
Router2(config)# ip dhcp excluded-address 192.168.50.1
Router2(config)# exit
Router2# write memory
```

6. **ตั้งค่า IP Configuration บน PC ให้เป็น DHCP**
    - เปิด PC1 > Desktop > IP Configuration
        - ตั้งค่า IP Configuration เป็น DHCP
    - เปิด PC2 > Desktop > IP Configuration
        - ตั้งค่า IP Configuration เป็น DHCP
    - เปิด PC3 > Desktop > IP Configuration
        - ตั้งค่า IP Configuration เป็น DHCP
    - เปิด PC4 > Desktop > IP Configuration
        - ตั้งค่า IP Configuration เป็น DHCP
    - เปิด PC5 > Desktop > IP Configuration
        - ตั้งค่า IP Configuration เป็น DHCP
7. **ทดสอบการเชื่อมต่อระหว่างเครื่อง PC ที่อยู่ใน VLAN ต่างกันด้วยคำสั่ง ping ใน Command Prompt**
    - เปิด Command Prompt บน PC1 และพิมพ์ ping 192.168.20.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC1 และ PC2 ผ่าน Inter-VLAN Routing
    - เปิด Command Prompt บน PC2 และพิมพ์ ping 192.168.30.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC2 และ PC3 ผ่าน Inter-VLAN Routing
    - เปิด Command Prompt บน PC3 และพิมพ์ ping 192.168.40.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC3 และ PC4 ผ่าน Inter-VLAN Routing
    - เปิด Command Prompt บน PC4 และพิมพ์ ping 192.168.50.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC4 และ PC5 ผ่าน Inter-VLAN Routing
    - เปิด Command Prompt บน PC5 และพิมพ์ ping 192.168.10.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC5 และ PC1 ผ่าน Inter-VLAN Routing

สรุป

นักเรียนจะได้เรียนรู้การตั้งค่า DHCP Relay และ Inter-VLAN Routing บน Switch L2 และ Router เพื่อแจกหมายเลข IP Address แบบอัตโนมัติในเครือข่ายที่มีการแบ่ง VLAN และให้ VLAN ต่างๆ สามารถสื่อสารกันได้

ประโยชน์ของ LAB

- ช่วยให้นักเรียนเข้าใจการตั้งค่าและการใช้งาน DHCP Relay เพื่อแจกจ่าย IP Address แบบอัตโนมัติในเครือข่ายที่มีการแบ่ง VLAN
- เรียนรู้วิธีการตั้งค่า Inter-VLAN Routing บน Router เพื่อให้ VLAN ต่างๆ สามารถสื่อสารกันได้
- เพิ่มความสะดวกและประสิทธิภาพในการจัดการ IP Address ในเครือข่าย

LAB 15: การตั้งค่า Routing ระหว่างสาขา 5 สาขา เพื่อให้คอมพิวเตอร์ทุกสาขาสามารถส่งข้อมูลหากันได้

ผู้สอน

ผู้ช่วยศาสตราจารย์อมร เจือตี๋
สาขาวิชาคอมพิวเตอร์ศึกษา คณะวิทยาศาสตร์และเทคโนโลยี

ชื่อ นามสกุล _____

หมู่เรียน _____

คะแนน _____

วัตถุประสงค์

1. เพื่อเรียนรู้การตั้งค่า Routing ระหว่างสาขา 5 สาขา โดยใช้ Router เพื่อให้คอมพิวเตอร์ทุกสาขาสามารถส่งข้อมูลหากันได้

อุปกรณ์ที่ใช้

- Router (Cisco 1941) จำนวน 6 ตัว (Router สำหรับแต่ละสาขาและ Router กลาง)
- Switch L2 (Cisco 2960) จำนวน 5 ตัว (Switch สำหรับแต่ละสาขา)
- เครื่องคอมพิวเตอร์ (PC) จำนวน 5 เครื่อง (PC สำหรับแต่ละสาขา)
- สายเชื่อมต่อ (Straight-Through, Cross-Over)

การออกแบบหมายเลข IP Address

อุปกรณ์	พอร์ต	IP Address	Subnet Mask	Default Gateway
Branch1	G0/0	192.168.1.1	255.255.255.0	192.168.1.254
Branch2	G0/0	192.168.2.1	255.255.255.0	192.168.2.254
Branch3	G0/0	192.168.3.1	255.255.255.0	192.168.3.254
Branch4	G0/0	192.168.4.1	255.255.255.0	192.168.4.254

อุปกรณ์	พอร์ต	IP Address	Subnet Mask	Default Gateway
Branch5	G0/0	192.168.5.1	255.255.255.0	192.168.5.254
Central	G0/0	10.0.0.1	255.255.255.0	-
Central	G0/1	10.0.1.1	255.255.255.0	-
Central	G0/2	10.0.2.1	255.255.255.0	-
Central	G0/3	10.0.3.1	255.255.255.0	-
Central	G0/4	10.0.4.1	255.255.255.0	-

วิธีการทำ

1. **เปิดโปรแกรม Cisco Packet Tracer และสร้างการเชื่อมต่อระหว่าง Router, Switch และ PC**
    - เปิดโปรแกรม Cisco Packet Tracer
    - ลาก Router (Cisco 1941) จำนวน 6 ตัว (Router สำหรับแต่ละสาขาและ Router กลาง), Switch L2 จำนวน 5 ตัว และ PC จำนวน 5 เครื่องไปวางในพื้นที่การทำงาน
2. **เชื่อมต่อสาย**
    - ใช้สาย Cross-Over เชื่อมต่อจาก GigabitEthernet0/0 ของ Router แต่ละสาขาไปยัง GigabitEthernet ของ Switch ที่ตรงกัน
    - ใช้สาย Straight-Through เชื่อมต่อจาก FastEthernet0 ของ PC แต่ละสาขาไปยัง FastEthernet ของ Switch ที่ตรงกัน
    - ใช้สาย Cross-Over เชื่อมต่อจาก GigabitEthernet0/0 ของ Router แต่ละสาขาไปยัง GigabitEthernet0/0 ถึง G0/4 ของ Router กลาง
3. **ตั้งค่า IP Address บน Router ของแต่ละสาขา**
    - Branch 1:

```
Branch1> enable
Branch1# configure terminal
Branch1(config)# interface gigabitethernet 0/0
Branch1(config-if)# ip address 192.168.1.1 255.255.255.0
Branch1(config-if)# no shutdown
Branch1(config-if)# exit
```

```
Branch1(config)# exit
Branch1# write memory
```

- Branch 2:

```
Branch2> enable
Branch2# configure terminal
Branch2(config)# interface gigabitethernet 0/0
Branch2(config-if)# ip address 192.168.2.1 255.255.255.0
Branch2(config-if)# no shutdown
Branch2(config-if)# exit
Branch2(config)# exit
Branch2# write memory
```

- Branch 3:

```
Branch3> enable
Branch3# configure terminal
Branch3(config)# interface gigabitethernet 0/0
Branch3(config-if)# ip address 192.168.3.1 255.255.255.0
Branch3(config-if)# no shutdown
Branch3(config-if)# exit
Branch3(config)# exit
Branch3# write memory
```

- Branch 4:

```
Branch4> enable
Branch4# configure terminal
Branch4(config)# interface gigabitethernet 0/0
Branch4(config-if)# ip address 192.168.4.1 255.255.255.0
Branch4(config-if)# no shutdown
```

```
Branch4(config-if)# exit
Branch4(config)# exit
Branch4# write memory
```

- Branch 5:

```
Branch5> enable
Branch5# configure terminal
Branch5(config)# interface gigabitethernet 0/0
Branch5(config-if)# ip address 192.168.5.1 255.255.255.0
Branch5(config-if)# no shutdown
Branch5(config-if)# exit
Branch5(config)# exit
Branch5# write memory
```

4. **ตั้งค่า IP Address บน Router กลาง**

```
Central> enable
Central# configure terminal
Central(config)# interface gigabitethernet 0/0
Central(config-if)# ip address 10.0.0.1 255.255.255.0
Central(config-if)# no shutdown
Central(config-if)# exit
Central(config)# interface gigabitethernet 0/1
Central(config-if)# ip address 10.0.1.1 255.255.255.0
Central(config-if)# no shutdown
Central(config-if)# exit
Central(config)# interface gigabitethernet 0/2
Central(config-if)# ip address 10.0.2.1 255.255.255.0
Central(config-if)# no shutdown
Central(config-if)# exit
Central(config)# interface gigabitethernet 0/3
```

```
Central(config-if)# ip address 10.0.3.1 255.255.255.0
Central(config-if)# no shutdown
Central(config-if)# exit
Central(config)# interface gigabitethernet 0/4
Central(config-if)# ip address 10.0.4.1 255.255.255.0
Central(config-if)# no shutdown
Central(config-if)# exit
Central(config)# exit
Central# write memory
```

5. **ตั้งค่า Routing บน Router ของแต่ละสาขา**
    - Branch 1:

```
Branch1> enable
Branch1# configure terminal
Branch1(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.1
Branch1(config)# exit
Branch1# write memory
```

    - Branch 2:

```
Branch2> enable
Branch2# configure terminal
Branch2(config)# ip route 0.0.0.0 0.0.0.0 10.0.1.1
Branch2(config)# exit
Branch2# write memory
```

    - Branch 3:

```
Branch3> enable
Branch3# configure terminal
Branch3(config)# ip route 0.0.0.0 0.0.0.0 10.0.2.1
```

```
Branch3(config)# exit
Branch3# write memory
```

- Branch 4:

```
Branch4> enable
Branch4# configure terminal
Branch4(config)# ip route 0.0.0.0 0.0.0.0 10.0.3.1
Branch4(config)# exit
Branch4# write memory
```

- Branch 5:

```
Branch5> enable
Branch5# configure terminal
Branch5(config)# ip route 0.0.0.0 0.0.0.0 10.0.4.1
Branch5(config)# exit
Branch5# write memory
```

6. **ตั้งค่า Routing บน Router กลาง**

```
Central> enable
Central# configure terminal
Central(config)# ip route 192.168.1.0 255.255.255.0 10.0.0.1
Central(config)# ip route 192.168.2.0 255.255.255.0 10.0.1.1
Central(config)# ip route 192.168.3.0 255.255.255.0 10.0.2.1
Central(config)# ip route 192.168.4.0 255.255.255.0 10.0.3.1
Central(config)# ip route 192.168.5.0 255.255.255.0 10.0.4.1
Central(config)# exit
Central# write memory
```

7. **ตั้งค่า IP Configuration บน PC ให้เป็น DHCP หรือ Static ตามที่กำหนด**
    - เปิด PC1 > Desktop > IP Configuration
        - ตั้งค่า IP Configuration เป็น Static: 192.168.1.2, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.1.1
    - เปิด PC2 > Desktop > IP Configuration
        - ตั้งค่า IP Configuration เป็น Static: 192.168.2.2, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.2.1
    - เปิด PC3 > Desktop > IP Configuration
        - ตั้งค่า IP Configuration เป็น Static: 192.168.3.2, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.3.1
    - เปิด PC4 > Desktop > IP Configuration
        - ตั้งค่า IP Configuration เป็น Static: 192.168.4.2, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.4.1
    - เปิด PC5 > Desktop > IP Configuration
        - ตั้งค่า IP Configuration เป็น Static: 192.168.5.2, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.5.1
8. **ทดสอบการเชื่อมต่อระหว่างเครื่อง PC ที่อยู่ในสาขาต่างกันด้วยคำสั่ง ping ใน Command Prompt**
    - เปิด Command Prompt บน PC1 และพิมพ์ ping 192.168.2.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC1 และ PC2
    - เปิด Command Prompt บน PC2 และพิมพ์ ping 192.168.3.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC2 และ PC3
    - เปิด Command Prompt บน PC3 และพิมพ์ ping 192.168.4.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC3 และ PC4
    - เปิด Command Prompt บน PC4 และพิมพ์ ping 192.168.5.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC4 และ PC5
    - เปิด Command Prompt บน PC5 และพิมพ์ ping 192.168.1.2 เพื่อทดสอบการเชื่อมต่อระหว่าง PC5 และ PC1

สรุป

นักเรียนจะได้เรียนรู้การตั้งค่า Routing ระหว่างสาขา 5 สาขา โดยใช้ Router เพื่อให้คอมพิวเตอร์ทุกสาขาสามารถส่งข้อมูลหากันได้

ประโยชน์ของ LAB

- ช่วยให้นักเรียนเข้าใจการตั้งค่า Routing ระหว่างสาขาโดยใช้ Router เพื่อให้คอมพิวเตอร์ทุกสาขาสามารถสื่อสารกันได้
- เพิ่มความรู้เกี่ยวกับการออกแบบและตั้งค่าเครือข่ายขนาดใหญ่
- เรียนรู้วิธีการใช้ Routing Table บน Router

Lab 1: การติดตั้งและกำหนดค่าคอนฟิก Apache2 และ PHP ให้มีความปลอดภัย

ผู้สอน:

ผู้ช่วยศาสตราจารย์อมร เจือตี๋

วัตถุประสงค์:

1. เรียนรู้การติดตั้ง Apache2 และ PHP บน Linux
2. เรียนรู้การกำหนดค่าคอนฟิกให้ Apache2 และ PHP มีความปลอดภัย

วัสดุและเครื่องมือ:

- ระบบปฏิบัติการ Linux (Ubuntu หรือ Debian-based distribution แนะนำ)
- สิทธิ์ root หรือ sudo
- หมายเลขเครือข่ายที่ใช้: 192.168.1.0/24

ตารางหมายเลข IP Address ที่ใช้

หมายเลข IP Address	อุปกรณ์	บันทึกเพิ่มเติม
192.168.1.1	Router	Gateway หลักของเครือข่าย
192.168.1.2	Server	ติดตั้ง Apache2 และทดสอบ config
192.168.1.3 - 192.168.1.254	อุปกรณ์อื่นๆในเครือข่าย	เช่น คอมพิวเตอร์, มือถือ, IoT

วิธีการติดตั้ง

1. **อัพเดตระบบ:**
    - อัพเดต package list ของระบบ:

      sudo apt update

2. **ติดตั้ง Apache2:**
    - ติดตั้ง Apache2 web server:

sudo apt install apache2 -y

- ตรวจสอบสถานะของ Apache2:

  sudo systemctl status apache2

- ทดสอบการเข้าถึง Apache2 ผ่านเว็บเบราว์เซอร์โดยเข้าไปที่ http://192.168.1.x (ควรเห็นหน้าเว็บ Apache2 Default Page)

3. **ติดตั้ง PHP:**
   - ติดตั้ง PHP และโมดูลที่จำเป็น:

     sudo apt install php libapache2-mod-php php-mysql -y

   - ตรวจสอบการติดตั้ง PHP:

     php -v

   - สร้างไฟล์ทดสอบ PHP:

     echo "<?php phpinfo(); ?>" | sudo tee /var/www/html/info.php

วิธีการ config

1. ปิดการแสดงข้อมูลเวอร์ชันของ Apache2

- แก้ไขไฟล์คอนฟิกหลักของ Apache2:

  sudo nano /etc/apache2/conf-available/security.conf

- ค้นหาบรรทัดที่มี ServerTokens และ ServerSignature และเปลี่ยนค่าเป็นดังนี้:

  plaintext

ServerTokens Prod
ServerSignature Off

2. ปิดการแสดงรายการไฟล์ในไดเรกทอรี

- แก้ไขไฟล์คอนฟิกหลักของ Apache2:

  sudo nano /etc/apache2/apache2.conf

- เพิ่มหรือเปลี่ยนแปลงค่าต่อไปนี้ในส่วน <Directory /var/www/>:

  plaintext

  Options -Indexes

3. กำหนดสิทธิ์การเข้าถึงไฟล์และไดเรกทอรี

- ตรวจสอบและกำหนดสิทธิ์การเข้าถึงไฟล์และไดเรกทอรี:

  sudo chown -R www-data:www-data /var/www/html
  sudo chmod -R 755 /var/www/html

4. เปิดใช้งานการเข้ารหัส SSL/TLS

- ติดตั้งโมดูล mod_ssl:

  sudo apt install openssl ssl-cert -y
  sudo a2enmod ssl

- สร้างใบรับรอง SSL:

  sudo mkdir /etc/apache2/ssl
  sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
  /etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt

(ในขั้นตอนนี้ จะต้องกรอกข้อมูลเกี่ยวกับองค์กรและโดเมนของคุณ)

- แก้ไขไฟล์คอนฟิกของเว็บไซต์เพื่อเปิดใช้งาน SSL:

  sudo nano /etc/apache2/sites-available/default-ssl.conf

  เพิ่มหรือแก้ไขค่าต่อไปนี้:

  plaintext

```
<VirtualHost *:443>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

    SSLEngine on
    SSLCertificateFile /etc/apache2/ssl/apache.crt
    SSLCertificateKeyFile /etc/apache2/ssl/apache.key

    <FilesMatch "\.(cgi|tml|phtml|php)$">
        SSLOptions +StdEnvVars
    </FilesMatch>
    <Directory /usr/lib/cgi-bin>
        SSLOptions +StdEnvVars
    </Directory>

    BrowserMatch "MSIE [2-6]" \
        nokeepalive ssl-unclean-utdown \
        downgrade-1.0 force-response-1.0

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

- เปิดใช้งานเว็บไซต์ SSL:

  sudo a2ensite default-ssl
  sudo systemctl reload apache2

5. ตั้งค่า Firewall เพื่ออนุญาตการเข้าถึงเฉพาะพอร์ตที่จำเป็น

- ตั้งค่า UFW (Uncomplicated Firewall) เพื่ออนุญาตการเข้าถึงพอร์ต 80 (HTTP) และ 443 (HTTPS):

  sudo ufw allow 'Apache Full'
  sudo ufw enable
  sudo ufw status

การทดสอบ:

1. **ทดสอบการเข้าถึง HTTP:**
   - เปิดเว็บเบราว์เซอร์แล้วเข้าไปที่ http://192.168.1.x
   - คุณควรเห็นหน้า Apache2 Default Page
2. **ทดสอบการเข้าถึง HTTPS:**
   - เปิดเว็บเบราว์เซอร์แล้วเข้าไปที่ https://192.168.1.x
   - คุณควรเห็นหน้า Apache2 Default Page ที่มีการเข้ารหัส SSL
3. **ทดสอบ PHP:**
   - เปิดเว็บเบราว์เซอร์แล้วเข้าไปที่ http://192.168.1.x/info.php
   - คุณควรเห็นหน้า PHP Information Page แสดงข้อมูลเกี่ยวกับการติดตั้ง PHP
4. **ตรวจสอบการปิดการแสดงข้อมูลเวอร์ชัน:**
   - เปิด Terminal แล้วรันคำสั่ง:

     curl -I http://192.168.1.x

   - ตรวจสอบผลลัพธ์ว่าไม่มีการแสดงข้อมูลเวอร์ชันของ Apache
5. **ตรวจสอบการปิดการแสดงรายการไฟล์ในไดเรกทอรี:**
   - เปิดเว็บเบราว์เซอร์แล้วเข้าไปที่ http://192.168.1.x/nonexistent_directory
   - คุณควรเห็นข้อความ "403 Forbidden" แทนที่จะเป็นการแสดงรายการไฟล์

6. **ตรวจสอบสิทธิ์การเข้าถึงไฟล์:**
    - เปิด Terminal แล้วรันคำสั่ง:

      ls -l /var/www/html

    - ตรวจสอบสิทธิ์ของไฟล์และไดเรกทอรีว่าถูกตั้งค่าเป็น www-data:www-data และ 755

สรุปผลการเรียนรู้:

ใน lab นี้ คุณได้เรียนรู้การติดตั้งและตั้งค่าคอนฟิก Apache2 และ PHP บน Linux และวิธีการกำหนดค่าคอนฟิกให้มีความปลอดภัย เช่น การปิดการแสดงข้อมูลเวอร์ชัน การปิดการแสดงรายการไฟล์ในไดเรกทอรี การกำหนดสิทธิ์การเข้าถึงไฟล์และไดเรกทอรี การเปิดใช้งานการเข้ารหัส SSL/TLS และการตั้งค่า Firewall

ข้อแนะนำเพิ่มเติม:

- ควรทำการสำรองข้อมูลก่อนทำการตั้งค่าหรือแก้ไขไฟล์คอนฟิกใดๆ
- หากพบปัญหาในการติดตั้งหรือการตั้งค่า ควรตรวจสอบ log ไฟล์ของ Apache2 เพื่อหาสาเหตุและแนวทางแก้ไข
- ตรวจสอบและอัพเดตซอฟต์แวร์และแพ็คเกจเป็นประจำเพื่อความปลอดภัย

Lab 2: การติดตั้งและกำหนดค่าคอนฟิก BIND และการทำ Virtual Host บน Ubuntu

ผู้สอน:

ผู้ช่วยศาสตราจารย์อมร เจือตี๋

วัตถุประสงค์:

1. เรียนรู้การติดตั้ง BIND DNS Server บน Ubuntu
2. เรียนรู้การทำ Virtual Host บน Ubuntu

วัสดุและเครื่องมือ:

- ระบบปฏิบัติการ Linux (Ubuntu แนะนำ)
- สิทธิ์ root หรือ sudo
- หมายเลขเครือข่ายที่ใช้: 192.168.1.0/24

ตารางหมายเลข IP Address ที่ใช้

หมายเลข IP Address	อุปกรณ์	บันทึกเพิ่มเติม
192.168.1.1	Router	Gateway หลักของเครือข่าย
192.168.1.2	Server	ติดตั้ง BIND และ Virtual Host
192.168.1.3 - 192.168.1.254	อุปกรณ์อื่นๆในเครือข่าย	เช่น คอมพิวเตอร์, มือถือ, IoT

วิธีการติดตั้ง

การติดตั้ง BIND DNS Server

1. **อัพเดตระบบ:**
    - อัพเดต package list ของระบบ:

```
sudo apt update
```

2. **ติดตั้ง BIND9:**
    - ติดตั้ง BIND DNS Server:

```
sudo apt install bind9 bind9utils bind9-doc -y
```

การทำ Virtual Host บน Apache2

1. **ติดตั้ง Apache2:**
    - ติดตั้ง Apache2 web server:

```
sudo apt install apache2 -y
```

2. **สร้าง Directory สำหรับ Virtual Host:**
    - สร้าง Directory สำหรับแต่ละ Virtual Host:

```
sudo mkdir -p /var/www/example1.com/public_html
sudo mkdir -p /var/www/example2.com/public_html
```

3. **กำหนดสิทธิ์ Directory:**
    - กำหนดสิทธิ์และเจ้าของ Directory:

```
sudo chown -R $USER:$USER /var/www/example1.com/public_html
sudo chown -R $USER:$USER /var/www/example2.com/public_html
sudo chmod -R 755 /var/www
```

4. **สร้างหน้าเว็บทดสอบ:**
    - สร้างไฟล์ index.html ในแต่ละ Directory:

```
echo "<html><head><title>Welcome to
example1.com!</title></head><body><h1>Success! The example1.com virtual
host is working!</h1></body></html>" | sudo tee
/var/www/example1.com/public_html/index.html
```

```
echo "<html><head><title>Welcome to
example2.com!</title></head><body><h1>Success! The example2.com virtual
host is working!</h1></body></html>" | sudo tee
/var/www/example2.com/public_html/index.html
```

วิธีการ config

การกำหนดค่า BIND DNS Server

1. **แก้ไขไฟล์ named.conf.local:**
    - เพิ่มโซนใหม่ในไฟล์ named.conf.local:

      sudo nano /etc/bind/named.conf.local

      เพิ่มบรรทัดต่อไปนี้:

      plaintext

```
zone "example1.com" {
    type master;
    file "/etc/bind/zones/db.example1.com";
};

zone "example2.com" {
    type master;
    file "/etc/bind/zones/db.example2.com";
};
```

2. **สร้าง Directory สำหรับไฟล์โซน:**
    - สร้าง Directory สำหรับไฟล์โซน:

      sudo mkdir /etc/bind/zones

3. **สร้างไฟล์โซน:**
    - สร้างไฟล์ db.example1.com:

      sudo nano /etc/bind/zones/db.example1.com

      เพิ่มเนื้อหาต่อไปนี้:

      plaintext

```
;
; BIND data file for example1.com
;
$TTL    604800
@       IN      SOA     ns.example1.com. admin.example1.com. (
                              3         ; Serial
                         604800         ; Refre
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns.example1.com.
@       IN      A       192.168.1.2
ns      IN      A       192.168.1.2
www     IN      CNAME   example1.com.
```

- สร้างไฟล์ db.example2.com:

  sudo nano /etc/bind/zones/db.example2.com

  เพิ่มเนื้อหาต่อไปนี้:

  plaintext

```
;
; BIND data file for example2.com
;
$TTL    604800
@       IN      SOA     ns.example2.com. admin.example2.com. (
                              3         ; Serial
                         604800         ; Refre
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns.example2.com.
@       IN      A       192.168.1.2
ns      IN      A       192.168.1.2
www     IN      CNAME   example2.com.
```

4. **รีสตาร์ท BIND9:**
   - รีสตาร์ทบริการ BIND9 เพื่อให้การตั้งค่ามีผล:

     sudo systemctl restart bind9

การกำหนดค่า Virtual Host บน Apache2

1. **สร้างไฟล์คอนฟิก Virtual Host:**
    - สร้างไฟล์คอนฟิกสำหรับแต่ละ Virtual Host:

      sudo nano /etc/apache2/sites-available/example1.com.conf

      เพิ่มเนื้อหาต่อไปนี้:

      plaintext

      ```
      <VirtualHost *:80>
          ServerAdmin admin@example1.com
          ServerName example1.com
          ServerAlias www.example1.com
          DocumentRoot /var/www/example1.com/public_html
          ErrorLog ${APACHE_LOG_DIR}/error.log
          CustomLog ${APACHE_LOG_DIR}/access.log combined
      </VirtualHost>
      ```

    - สร้างไฟล์คอนฟิกสำหรับ example2.com:

      sudo nano /etc/apache2/sites-available/example2.com.conf

      เพิ่มเนื้อหาต่อไปนี้:

      plaintext

      ```
      <VirtualHost *:80>
          ServerAdmin admin@example2.com
          ServerName example2.com
          ServerAlias www.example2.com
          DocumentRoot /var/www/example2.com/public_html
      ```

```
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

2. **เปิดใช้งาน Virtual Host:**
    - เปิดใช้งานไฟล์คอนฟิกสำหรับแต่ละ Virtual Host:

```
sudo a2ensite example1.com.conf
sudo a2ensite example2.com.conf
```

3. **รีสตาร์ท Apache2:**
    - รีสตาร์ทบริการ Apache2 เพื่อให้การตั้งค่ามีผล:

```
sudo systemctl restart apache2
```

การทดสอบ:

1. **ทดสอบการทำงานของ BIND DNS:**
    - ใช้คำสั่ง nslookup หรือ dig เพื่อตรวจสอบการทำงานของ BIND:

```
nslookup example1.com 192.168.1.2
nslookup example2.com 192.168.1.2
```

2. **ทดสอบการเข้าถึง Virtual Host:**
    - เปิดเว็บเบราว์เซอร์แล้วเข้าไปที่ http://example1.com และ http://example2.com
    - คุณควรเห็นหน้าเว็บทดสอบที่สร้างไว้ในแต่ละ Virtual Host

สรุปผลการเรียนรู้:

ใน lab นี้ คุณได้เรียนรู้การติดตั้งและตั้งค่าคอนฟิก BIND DNS Server และการทำ Virtual Host บน Ubuntu รวมถึงวิธีการตรวจสอบการทำงานของ DNS และ Virtual Host

ข้อแนะนำเพิ่มเติม:

- ควรทำการสำรองข้อมูลก่อนทำการตั้งค่าหรือแก้ไขไฟล์คอนฟิกใดๆ
- หากพบปัญหาในการติดตั้งหรือการตั้งค่า ควรตรวจสอบ log ไฟล์ของ BIND และ Apache2 เพื่อหาสาเหตุและแนวทางแก้ไข

Lab 3: การติดตั้งและกำหนดค่าคอนฟิก MySQL Server และ phpMyAdmin บน Ubuntu

ผู้สอน:

ผู้ช่วยศาสตราจารย์อมร เจือตี๋

วัตถุประสงค์:

1. เรียนรู้การติดตั้ง MySQL Server บน Ubuntu
2. เรียนรู้การติดตั้ง phpMyAdmin บน Ubuntu

วัสดุและเครื่องมือ:

- ระบบปฏิบัติการ Linux (Ubuntu แนะนำ)
- สิทธิ์ root หรือ sudo
- หมายเลขเครือข่ายที่ใช้: 192.168.1.0/24

ตารางหมายเลข IP Address ที่ใช้

หมายเลข IP Address	อุปกรณ์	บันทึกเพิ่มเติม
192.168.1.1	Router	Gateway หลักของเครือข่าย
192.168.1.2	Server	ติดตั้ง MySQL Server และ phpMyAdmin
192.168.1.3 - 192.168.1.254	อุปกรณ์อื่นๆในเครือข่าย	เช่น คอมพิวเตอร์, มือถือ, IoT

วิธีการติดตั้ง

การติดตั้ง MySQL Server

1. **อัพเดตระบบ:**
    - อัพเดต package list ของระบบ:

      sudo apt update

2. **ติดตั้ง MySQL Server:**
    - ติดตั้ง MySQL Server:

      sudo apt install mysql-server -y

    - รันการตั้งค่า MySQL:

      sudo mysql_secure_installation

    - ตอบคำถามต่างๆ เพื่อปรับปรุงความปลอดภัยของ MySQL

การติดตั้ง phpMyAdmin

1. **ติดตั้ง phpMyAdmin:**
    - ติดตั้ง phpMyAdmin:

      sudo apt install phpmyadmin php-mbstring php-zip php-gd php-json php-curl -y

    - ในระหว่างการติดตั้ง จะมีหน้าต่างให้เลือกเว็บเซิร์ฟเวอร์ที่จะใช้กับ phpMyAdmin ให้เลือก apache2 และกด OK
    - จะมีหน้าต่างให้กำหนดรหัสผ่านสำหรับผู้ใช้ phpMyAdmin ให้กำหนดรหัสผ่านและกด OK

2. **เปิดใช้งาน phpMyAdmin:**
    - เปิดใช้งานส่วนขยาย mbstring:

      sudo phpenmod mbstring

    - รีสตาร์ท Apache2:

      sudo systemctl restart apache2

วิธีการ config

การกำหนดค่า MySQL Server

1. **เข้าสู่ MySQL:**
    - เข้าสู่ MySQL ด้วยผู้ใช้ root:

      sudo mysql -u root -p

    - สร้างฐานข้อมูลใหม่:

      sql

      CREATE DATABASE mydatabase;

    - สร้างผู้ใช้ใหม่และให้สิทธิ์:

      sql

      CREATE USER 'myuser'@'localhost' IDENTIFIED BY 'mypassword';
      GRANT ALL PRIVILEGES ON mydatabase.* TO 'myuser'@'localhost';
      FLU PRIVILEGES;

- ออกจาก MySQL:

  sql

  EXIT;

การกำหนดค่า phpMyAdmin

1. **เพิ่มการเชื่อมโยง phpMyAdmin กับ Apache2:**
   - สร้าง symbolic link ไปยัง Apache2 configuration:

     sudo ln -s /etc/phpmyadmin/apache.conf /etc/apache2/conf-available/phpmyadmin.conf

   - เปิดใช้งานการตั้งค่า phpMyAdmin:

     sudo a2enconf phpmyadmin
     sudo systemctl reload apache2

การทดสอบ:

1. **ทดสอบการเข้าถึง MySQL:**
   - เปิด Terminal แล้วรันคำสั่ง:

     sudo mysql -u root -p

   - ล็อกอินเข้าสู่ MySQL ด้วยรหัสผ่านที่ตั้งไว้
2. **ทดสอบการเข้าถึง phpMyAdmin:**
   - เปิดเว็บเบราว์เซอร์แล้วเข้าไปที่ http://192.168.1.2/phpmyadmin
   - ล็อกอินเข้าสู่ phpMyAdmin ด้วยผู้ใช้ root และรหัสผ่านที่ตั้งไว้

สรุปผลการเรียนรู้:

ใน lab นี้ คุณได้เรียนรู้การติดตั้งและตั้งค่าคอนฟิก MySQL Server และ phpMyAdmin บน Ubuntu รวมถึงวิธีการตรวจสอบการทำงานของ MySQL และ phpMyAdmin

ข้อแนะนำเพิ่มเติม:

- ควรทำการสำรองข้อมูลก่อนทำการตั้งค่าหรือแก้ไขไฟล์คอนฟิกใดๆ
- หากพบปัญหาในการติดตั้งหรือการตั้งค่า ควรตรวจสอบ log ไฟล์ของ MySQL และ Apache2 เพื่อหาสาเหตุและแนวทางแก้ไข
- ตรวจสอบและอัพเดตซอฟต์แวร์และแพ็คเกจเป็นประจำเพื่อความปลอดภัย

Lab 4: การบล็อกเว็บไซต์ ไฟล์ และอื่นๆ บน Ubuntu

ผู้สอน:

ผู้ช่วยศาสตราจารย์อมร เจือตี๋

วัตถุประสงค์:

1. เรียนรู้การบล็อกเว็บไซต์ด้วย Squid Proxy
2. เรียนรู้การบล็อกไฟล์และโปรโตคอลด้วย Squid Proxy

วัสดุและเครื่องมือ:

- ระบบปฏิบัติการ Linux (Ubuntu แนะนำ)
- สิทธิ์ root หรือ sudo
- หมายเลขเครือข่ายที่ใช้: 192.168.1.0/24

ตารางหมายเลข IP Address ที่ใช้

หมายเลข IP Address	อุปกรณ์	บันทึกเพิ่มเติม
192.168.1.1	Router	Gateway หลักของเครือข่าย
192.168.1.2	Proxy Server	ติดตั้ง Squid Proxy
192.168.1.3 - 192.168.1.254	อุปกรณ์อื่นๆในเครือข่าย	เช่น คอมพิวเตอร์, มือถือ, IoT

วิธีการติดตั้ง

การติดตั้ง Squid Proxy

1. **อัพเดตระบบ:**
    - อัพเดต package list ของระบบ:

      sudo apt update

2. **ติดตั้ง Squid Proxy:**
    - ติดตั้ง Squid Proxy:

      sudo apt install squid -y

วิธีการ config

การกำหนดค่า Squid Proxy

1. **สำรองไฟล์คอนฟิกเดิม:**
    - สำรองไฟล์คอนฟิกเดิม:

      sudo cp /etc/squid/squid.conf /etc/squid/squid.conf.backup

2. **แก้ไขไฟล์คอนฟิก:**
    - แก้ไขไฟล์คอนฟิก Squid:

      sudo nano /etc/squid/squid.conf

3. **บล็อกเว็บไซต์:**
    - เพิ่มบรรทัดต่อไปนี้ในไฟล์คอนฟิกเพื่อบล็อกเว็บไซต์:

      plaintext

      acl blocked_sites dstdomain .example.com
      http_access deny blocked_sites

4. **บล็อกไฟล์ตามนามสกุล:**
    - เพิ่มบรรทัดต่อไปนี้ในไฟล์คอนฟิกเพื่อบล็อกไฟล์ตามนามสกุล:

      plaintext

      ```
      acl blocked_files urlpath_regex -i \.exe$ \.zip$ \.mp3$
      http_access deny blocked_files
      ```

5. **บล็อกโปรโตคอล:**
    - เพิ่มบรรทัดต่อไปนี้ในไฟล์คอนฟิกเพื่อบล็อกโปรโตคอลที่ไม่ต้องการ:

      plaintext

      ```
      acl blocked_protocols proto HTTPS
      http_access deny blocked_protocols
      ```

6. **อนุญาตการเข้าถึงจากเครือข่ายภายใน:**
    - เพิ่มบรรทัดต่อไปนี้ในไฟล์คอนฟิกเพื่ออนุญาตการเข้าถึงจากเครือข่ายภายใน:

      plaintext

      ```
      acl localnet src 192.168.1.0/24
      http_access allow localnet
      ```

7. **บันทึกและออกจากไฟล์คอนฟิก:**
    - บันทึกและออกจากไฟล์คอนฟิก (Ctrl + O, Enter, Ctrl + X)
8. **รีสตาร์ท Squid:**
    - รีสตาร์ทบริการ Squid เพื่อให้การตั้งค่ามีผล:

      ```
      sudo systemctl restart squid
      ```

การทดสอบ:

1. **ทดสอบการบล็อกเว็บไซต์:**
    - พยายามเข้าถึงเว็บไซต์ที่ถูกบล็อก เช่น http://example.com
    - คุณควรเห็นข้อความแสดงว่าไม่สามารถเข้าถึงเว็บไซต์ได้
2. **ทดสอบการบล็อกไฟล์ตามนามสกุล:**
    - พยายามดาวน์โหลดไฟล์ที่มีนามสกุลที่ถูกบล็อก เช่น http://example.com/file.exe
    - คุณควรเห็นข้อความแสดงว่าไม่สามารถดาวน์โหลดไฟล์ได้
3. **ทดสอบการบล็อกโปรโตคอล:**
    - พยายามเข้าถึงเว็บไซต์ที่ใช้โปรโตคอลที่ถูกบล็อก เช่น https://example.com
    - คุณควรเห็นข้อความแสดงว่าไม่สามารถเข้าถึงเว็บไซต์ได้

สรุปผลการเรียนรู้:

ใน lab นี้ คุณได้เรียนรู้การติดตั้งและตั้งค่าคอนฟิก Squid Proxy บน Ubuntu รวมถึงวิธีการบล็อกเว็บไซต์ ไฟล์ตามนามสกุล และโปรโตคอลที่ไม่ต้องการ

ข้อแนะนำเพิ่มเติม:

- ควรทำการสำรองข้อมูลก่อนทำการตั้งค่าหรือแก้ไขไฟล์คอนฟิกใดๆ
- หากพบปัญหาในการติดตั้งหรือการตั้งค่า ควรตรวจสอบ log ไฟล์ของ Squid เพื่อหาสาเหตุและแนวทางแก้ไข
- ตรวจสอบและอัพเดตซอฟต์แวร์และแพ็คเกจเป็นประจำเพื่อความปลอดภัย

Lab 5: การติดตั้งและกำหนดค่าคอนฟิก FTP Server บน Ubuntu

ผู้สอน:

ผู้ช่วยศาสตราจารย์อมร เจือตี๋

วัตถุประสงค์:

1. เรียนรู้การติดตั้ง FTP Server บน Ubuntu
2. เรียนรู้การกำหนดค่าคอนฟิก FTP Server

วัสดุและเครื่องมือ:

- ระบบปฏิบัติการ Linux (Ubuntu แนะนำ)
- สิทธิ์ root หรือ sudo
- หมายเลขเครือข่ายที่ใช้: 192.168.1.0/24

ตารางหมายเลข IP Address ที่ใช้

หมายเลข IP Address	อุปกรณ์	บันทึกเพิ่มเติม
192.168.1.1	Router	Gateway หลักของเครือข่าย
192.168.1.2	FTP Server	ติดตั้ง FTP Server
192.168.1.3 - 192.168.1.254	อุปกรณ์อื่นๆในเครือข่าย	เช่น คอมพิวเตอร์, มือถือ, IoT

วิธีการติดตั้ง

การติดตั้ง vsftpd (FTP Server)

1. **อัพเดตระบบ:**
    - อัพเดต package list ของระบบ:

      sudo apt update

2. **ติดตั้ง vsftpd:**
    - ติดตั้ง vsftpd:

      sudo apt install vsftpd -y

วิธีการ config

การกำหนดค่า vsftpd

1. **สำรองไฟล์คอนฟิกเดิม:**
    - สำรองไฟล์คอนฟิกเดิม:

      sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.backup

2. **แก้ไขไฟล์คอนฟิก:**
    - แก้ไขไฟล์คอนฟิก vsftpd:

      sudo nano /etc/vsftpd.conf

3. **ปรับแต่งการตั้งค่า:**
    - ปรับแต่งการตั้งค่าต่อไปนี้ในไฟล์คอนฟิก:

      plaintext

      listen=NO
      listen_ipv6=YES

```
anonymous_enable=NO
local_enable=YES
write_enable=YES
local_umask=022
dirmessage_enable=YES
use_localtime=YES
xferlog_enable=YES
connect_from_port_20=YES
chroot_local_user=YES
secure_chroot_dir=/var/run/vsftpd/empty
pam_service_name=vsftpd
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
ssl_enable=YES
```

4. **เพิ่มผู้ใช้ FTP:**
    - สร้างผู้ใช้ FTP และตั้งค่ารหัสผ่าน:

```
sudo adduser ftpuser
```

5. **สร้างไดเรกทอรีสำหรับผู้ใช้ FTP:**
    - สร้างไดเรกทอรีและกำหนดสิทธิ์:

```
sudo mkdir -p /home/ftpuser/ftp/upload
sudo chown nobody:nogroup /home/ftpuser/ftp
sudo chmod a-w /home/ftpuser/ftp
sudo chown ftpuser:ftpuser /home/ftpuser/ftp/upload
```

6. **รีสตาร์ท vsftpd:**
    - รีสตาร์ทบริการ vsftpd เพื่อให้การตั้งค่ามีผล:

      sudo systemctl restart vsftpd

การทดสอบ:

1. **ทดสอบการเชื่อมต่อ FTP:**
    - ใช้โปรแกรม FTP Client เช่น FileZilla หรือคำสั่ง FTP ใน Terminal เพื่อล็อกอินเข้า FTP Server ด้วยข้อมูลผู้ใช้ที่สร้างขึ้น

      ftp 192.168.1.2

2. **ทดสอบการอัพโหลดและดาวน์โหลดไฟล์:**
    - อัพโหลดไฟล์ไปยังไดเรกทอรี upload และดาวน์โหลดไฟล์จากเซิร์ฟเวอร์เพื่อทดสอบการทำงาน

สรุปผลการเรียนรู้:

ใน lab นี้ คุณได้เรียนรู้การติดตั้งและตั้งค่าคอนฟิก FTP Server บน Ubuntu รวมถึงวิธีการตรวจสอบการทำงานของ FTP Server และการจัดการผู้ใช้ FTP

ข้อแนะนำเพิ่มเติม:

- ควรทำการสำรองข้อมูลก่อนทำการตั้งค่าหรือแก้ไขไฟล์คอนฟิกใดๆ
- หากพบปัญหาในการติดตั้งหรือการตั้งค่า ควรตรวจสอบ log ไฟล์ของ vsftpd เพื่อหาสาเหตุและแนวทางแก้ไข
- ตรวจสอบและอัพเดตซอฟต์แวร์และแพ็คเกจเป็นประจำเพื่อความปลอดภัย

Lab 6: การติดตั้งและให้บริการ S บน Ubuntu

ผู้สอน:

ผู้ช่วยศาสตราจารย์อมร เจือตี๋

วัตถุประสงค์:

1. เรียนรู้การติดตั้ง S Server บน Ubuntu
2. เรียนรู้การกำหนดค่าคอนฟิก S Server เพื่อเพิ่มความปลอดภัย

วัสดุและเครื่องมือ:

- ระบบปฏิบัติการ Linux (Ubuntu แนะนำ)
- สิทธิ์ root หรือ sudo
- หมายเลขเครือข่ายที่ใช้: 192.168.1.0/24

ตารางหมายเลข IP Address ที่ใช้

หมายเลข IP Address	อุปกรณ์	บันทึกเพิ่มเติม
192.168.1.1	Router	Gateway หลักของเครือข่าย
192.168.1.2	S Server	ติดตั้ง S Server
192.168.1.3 - 192.168.1.254	อุปกรณ์อื่นๆในเครือข่าย	เช่น คอมพิวเตอร์, มือถือ, IoT

วิธีการติดตั้ง

การติดตั้ง OpenS Server

1. **อัพเดตระบบ:**
    - อัพเดต package list ของระบบ:

sudo apt update

2. **ติดตั้ง OpenS Server:**
    - ติดตั้ง OpenS Server:

      sudo apt install opens-server -y

3. **ตรวจสอบสถานะของ S Server:**
    - ตรวจสอบสถานะของ S Server:

      sudo systemctl status s

วิธีการ config

การกำหนดค่า S Server

1. **สำรองไฟล์คอนฟิกเดิม:**
    - สำรองไฟล์คอนฟิกเดิม:

      sudo cp /etc/s/sd_config /etc/s/sd_config.backup

2. **แก้ไขไฟล์คอนฟิก:**
    - แก้ไขไฟล์คอนฟิก S:

      sudo nano /etc/s/sd_config

3. **ปรับแต่งการตั้งค่า:**
    - ปรับแต่งการตั้งค่าต่อไปนี้ในไฟล์คอนฟิกเพื่อเพิ่มความปลอดภัย:

      plaintext

      PermitRootLogin no
      PasswordAuthentication yes
      ChallengeResponseAuthentication no

UsePAM yes

AllowUsers your_username

4. **รีสตาร์ท S:**
    - รีสตาร์ทบริการ S เพื่อให้การตั้งค่ามีผล:

      sudo systemctl restart s

การทดสอบ:

1. **ทดสอบการเชื่อมต่อ S:**
    - ใช้โปรแกรม S Client เช่น PuTTY หรือคำสั่ง S ใน Terminal เพื่อเชื่อมต่อกับ S Server:

      s your_username@192.168.1.2

2. **ทดสอบการเข้าถึงและการใช้งาน:**
    - ล็อกอินเข้าสู่เซิร์ฟเวอร์ด้วยชื่อผู้ใช้และรหัสผ่านที่กำหนดไว้
    - ทดสอบการใช้งานคำสั่งต่างๆ บนเซิร์ฟเวอร์ เช่น ls, pwd, top, เป็นต้น

สรุปผลการเรียนรู้:

ใน lab นี้ คุณได้เรียนรู้การติดตั้งและตั้งค่าคอนฟิก S Server บน Ubuntu รวมถึงวิธีการตรวจสอบการทำงานของ S Server และการเชื่อมต่อจากระยะไกลอย่างปลอดภัย

ข้อแนะนำเพิ่มเติม:

- ควรทำการสำรองข้อมูลก่อนทำการตั้งค่าหรือแก้ไขไฟล์คอนฟิกใดๆ
- หากพบปัญหาในการติดตั้งหรือการตั้งค่า ควรตรวจสอบ log ไฟล์ของ S เพื่อหาสาเหตุและแนวทางแก้ไข
- ตรวจสอบและอัพเดตซอฟต์แวร์และแพ็คเกจเป็นประจำเพื่อความปลอดภัย

Lab 7: การทำ Load Balance Server บน Ubuntu

ผู้สอน:

ผู้ช่วยศาสตราจารย์อมร เจือตี๋

วัตถุประสงค์:

1. เรียนรู้การติดตั้ง Load Balancer บน Ubuntu
2. เรียนรู้การกำหนดค่าคอนฟิก Load Balancer ด้วย Nginx

วัสดุและเครื่องมือ:

- ระบบปฏิบัติการ Linux (Ubuntu แนะนำ)
- สิทธิ์ root หรือ sudo
- หมายเลขเครือข่ายที่ใช้: 192.168.1.0/24

ตารางหมายเลข IP Address ที่ใช้

หมายเลข IP Address	อุปกรณ์	บันทึกเพิ่มเติม
192.168.1.1	Router	Gateway หลักของเครือข่าย
192.168.1.2	Load Balancer	ติดตั้ง Nginx Load Balancer
192.168.1.3	Web Server 1	เซิร์ฟเวอร์เว็บที่ 1
192.168.1.4	Web Server 2	เซิร์ฟเวอร์เว็บที่ 2
192.168.1.5 - 192.168.1.254	อุปกรณ์อื่นๆในเครือข่าย	เช่น คอมพิวเตอร์, มือถือ, IoT

วิธีการติดตั้ง

การติดตั้ง Nginx

1. **อัพเดตระบบ:**
    - อัพเดต package list ของระบบ:

      sudo apt update

2. **ติดตั้ง Nginx:**
    - ติดตั้ง Nginx:

      sudo apt install nginx -y

3. **ตรวจสอบสถานะของ Nginx:**
    - ตรวจสอบสถานะของ Nginx:

      sudo systemctl status nginx

วิธีการ config

การกำหนดค่า Load Balancer ใน Nginx

1. **สำรองไฟล์คอนฟิกเดิม:**
    - สำรองไฟล์คอนฟิกเดิม:

      sudo cp /etc/nginx/nginx.conf /etc/nginx/nginx.conf.backup

2. **แก้ไขไฟล์คอนฟิก:**
    - แก้ไขไฟล์คอนฟิก Nginx:

      sudo nano /etc/nginx/nginx.conf

3. **เพิ่มการตั้งค่าสำหรับ Load Balancer:**
    - เพิ่มบรรทัดต่อไปนี้ในส่วน http ของไฟล์คอนฟิก:

```
plaintext

http {
    upstream backend {
        server 192.168.1.3;
        server 192.168.1.4;
    }

    server {
        listen 80;

        location / {
            proxy_pass http://backend;
            proxy_set_header Host $host;
            proxy_set_header X-Real-IP $remote_addr;
            proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
            proxy_set_header X-Forwarded-Proto $scheme;
        }
    }
}
```

4. **ทดสอบไฟล์คอนฟิก:**
    - ทดสอบไฟล์คอนฟิกเพื่อให้แน่ใจว่าไม่มีข้อผิดพลาด:

```
sudo nginx -t
```

5. **รีสตาร์ท Nginx:**
    - รีสตาร์ทบริการ Nginx เพื่อให้การตั้งค่ามีผล:

      sudo systemctl restart nginx

การทดสอบ:

1. **ทดสอบการเข้าถึง Load Balancer:**
    - เปิดเว็บเบราว์เซอร์แล้วเข้าไปที่ http://192.168.1.2
    - คุณควรเห็นหน้าเว็บที่โหลดมาจากเซิร์ฟเวอร์เว็บ (192.168.1.3 หรือ 192.168.1.4)
2. **ทดสอบการกระจายโหลด:**
    - ทำการรีเฟรชหน้าเว็บหลายครั้ง แล้วตรวจสอบว่าโหลดได้จากทั้งสองเซิร์ฟเวอร์ (192.168.1.3 และ 192.168.1.4)

สรุปผลการเรียนรู้:

ใน lab นี้ คุณได้เรียนรู้การติดตั้งและตั้งค่าคอนฟิก Load Balancer บน Ubuntu ด้วย Nginx รวมถึงวิธีการตรวจสอบการทำงานของ Load Balancer และการกระจายโหลดไปยังเซิร์ฟเวอร์หลายตัว

ข้อแนะนำเพิ่มเติม:

- ควรทำการสำรองข้อมูลก่อนทำการตั้งค่าหรือแก้ไขไฟล์คอนฟิกใดๆ
- หากพบปัญหาในการติดตั้งหรือการตั้งค่า ควรตรวจสอบ log ไฟล์ของ Nginx เพื่อหาสาเหตุและแนวทางแก้ไข
- ตรวจสอบและอัพเดตซอฟต์แวร์และแพ็คเกจเป็นประจำเพื่อความปลอดภัย

Lab 8: การทำ Load Balance สำหรับ Web Server และ Database Server บน Ubuntu

ผู้สอน:

ผู้ช่วยศาสตราจารย์อมร เจือตี๋

วัตถุประสงค์:

1. เรียนรู้การติดตั้ง Load Balancer สำหรับ Web Server บน Ubuntu ด้วย Nginx
2. เรียนรู้การติดตั้ง Load Balancer สำหรับ Database Server บน Ubuntu ด้วย HAProxy

วัสดุและเครื่องมือ:

- ระบบปฏิบัติการ Linux (Ubuntu แนะนำ)
- สิทธิ์ root หรือ sudo
- หมายเลขเครือข่ายที่ใช้: 192.168.1.0/24

ตารางหมายเลข IP Address ที่ใช้

หมายเลข IP Address	อุปกรณ์	บันทึกเพิ่มเติม
192.168.1.1	Router	Gateway หลักของเครือข่าย
192.168.1.2	Load Balancer (Nginx)	ติดตั้ง Nginx Load Balancer
192.168.1.3	Web Server 1	เซิร์ฟเวอร์เว็บที่ 1
192.168.1.4	Web Server 2	เซิร์ฟเวอร์เว็บที่ 2
192.168.1.5	Load Balancer (HAProxy)	ติดตั้ง HAProxy Load Balancer สำหรับ DB
192.168.1.6	Database Server 1	เซิร์ฟเวอร์ฐานข้อมูลที่ 1
192.168.1.7	Database Server 2	เซิร์ฟเวอร์ฐานข้อมูลที่ 2
192.168.1.8 - 192.168.1.254	อุปกรณ์อื่นๆในเครือข่าย	เช่น คอมพิวเตอร์, มือถือ, IoT

วิธีการติดตั้ง

การติดตั้ง Nginx สำหรับ Web Server

1. **อัพเดตระบบ:**
    - อัพเดต package list ของระบบ:

      sudo apt update

2. **ติดตั้ง Nginx:**
    - ติดตั้ง Nginx:

      sudo apt install nginx -y

3. **ตรวจสอบสถานะของ Nginx:**
    - ตรวจสอบสถานะของ Nginx:

      sudo systemctl status nginx

การติดตั้ง HAProxy สำหรับ Database Server

1. **อัพเดตระบบ:**
    - อัพเดต package list ของระบบ:

      sudo apt update

2. **ติดตั้ง HAProxy:**
    - ติดตั้ง HAProxy:

      sudo apt install haproxy -y

3. **ตรวจสอบสถานะของ HAProxy:**
    - ตรวจสอบสถานะของ HAProxy:

sudo systemctl status haproxy

วิธีการ config

การกำหนดค่า Load Balancer ใน Nginx สำหรับ Web Server

1. **สำรองไฟล์คอนฟิกเดิม:**
   - สำรองไฟล์คอนฟิกเดิม:

     sudo cp /etc/nginx/nginx.conf /etc/nginx/nginx.conf.backup

2. **แก้ไขไฟล์คอนฟิก:**
   - แก้ไขไฟล์คอนฟิก Nginx:

     sudo nano /etc/nginx/nginx.conf

3. **เพิ่มการตั้งค่าสำหรับ Load Balancer:**
   - เพิ่มบรรทัดต่อไปนี้ในส่วน http ของไฟล์คอนฟิก:

     plaintext

```
http {
    upstream backend {
        server 192.168.1.3;
        server 192.168.1.4;
    }

    server {
        listen 80;

        location / {
```

```
            proxy_pass http://backend;
            proxy_set_header Host $host;
            proxy_set_header X-Real-IP $remote_addr;
            proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
            proxy_set_header X-Forwarded-Proto $scheme;
        }
    }
}
```

4. **ทดสอบไฟล์คอนฟิก:**
    - ทดสอบไฟล์คอนฟิกเพื่อให้แน่ใจว่าไม่มีข้อผิดพลาด:

      ```
      sudo nginx -t
      ```

5. **รีสตาร์ท Nginx:**
    - รีสตาร์ทบริการ Nginx เพื่อให้การตั้งค่ามีผล:

      ```
      sudo systemctl restart nginx
      ```

การกำหนดค่า Load Balancer ใน HAProxy สำหรับ Database Server

1. **สำรองไฟล์คอนฟิกเดิม:**
    - สำรองไฟล์คอนฟิกเดิม:

      ```
      sudo cp /etc/haproxy/haproxy.cfg /etc/haproxy/haproxy.cfg.backup
      ```

2. **แก้ไขไฟล์คอนฟิก:**
    - แก้ไขไฟล์คอนฟิก HAProxy:

      ```
      sudo nano /etc/haproxy/haproxy.cfg
      ```

3. **เพิ่มการตั้งค่าสำหรับ Load Balancer:**
    - เพิ่มการตั้งค่าต่อไปนี้ในไฟล์คอนฟิก:

```
plaintext

global
    log /dev/log    local0
    log /dev/log    local1 notice
    chroot /var/lib/haproxy
    stats socket /run/haproxy/admin.sock mode 660 level admin
    stats timeout 30s
    user haproxy
    group haproxy
    daemon

defaults
    log     global
    mode    tcp
    option  tcplog
    option  dontlognull
    timeout connect 5000
    timeout client  50000
    timeout server  50000

frontend mysql_front
    bind *:3306
    default_backend mysql_back

backend mysql_back
    balance roundrobin
    server db1 192.168.1.6:3306 check
    server db2 192.168.1.7:3306 check
```

4. **ทดสอบไฟล์คอนฟิก:**
    - ทดสอบไฟล์คอนฟิกเพื่อให้แน่ใจว่าไม่มีข้อผิดพลาด:

      sudo haproxy -c -f /etc/haproxy/haproxy.cfg

5. **รีสตาร์ท HAProxy:**
    - รีสตาร์ทบริการ HAProxy เพื่อให้การตั้งค่ามีผล:

      sudo systemctl restart haproxy

การทดสอบ:

การทดสอบ Load Balancer สำหรับ Web Server

1. **ทดสอบการเข้าถึง Load Balancer:**
    - เปิดเว็บเบราว์เซอร์แล้วเข้าไปที่ http://192.168.1.2
    - คุณควรเห็นหน้าเว็บที่โหลดมาจากเซิร์ฟเวอร์เว็บ (192.168.1.3 หรือ 192.168.1.4)
2. **ทดสอบการกระจายโหลด:**
    - ทำการรีเฟรชหน้าเว็บหลายครั้ง แล้วตรวจสอบว่าโหลดได้จากทั้งสองเซิร์ฟเวอร์ (192.168.1.3 และ 192.168.1.4)

การทดสอบ Load Balancer สำหรับ Database Server

1. **ทดสอบการเชื่อมต่อกับ Load Balancer:**
    - ใช้ MySQL client เพื่อเชื่อมต่อกับ Load Balancer:

      mysql -h 192.168.1.5 -u your_username -p

2. **ทดสอบการกระจายโหลด:**
    - รันคำสั่ง SQL หลายครั้งแล้วตรวจสอบ log ไฟล์ของ Database Server เพื่อดูว่ามีการกระจายโหลดไปยังทั้งสองเซิร์ฟเวอร์ (192.168.1.6 และ 192.168.1.7)

สรุปผลการเรียนรู้:

ใน lab นี้ คุณได้เรียนรู้การติดตั้งและตั้งค่าคอนฟิก Load Balancer สำหรับ Web Server และ Database Server บน Ubuntu รวมถึงวิธีการตรวจสอบการทำงานของ Load Balancer และการกระจายโหลดไปยังเซิร์ฟเวอร์หลายตัว

ข้อแนะนำเพิ่มเติม:

- ควรทำการสำรองข้อมูลก่อนทำการตั้งค่าหรือแก้ไขไฟล์คอนฟิกใดๆ
- หากพบปัญหาในการติดตั้งหรือการตั้งค่า ควรตรวจสอบ log ไฟล์ของ Nginx และ HAProxy เพื่อหาสาเหตุและแนวทางแก้ไข
- ตรวจสอบและอัพเดตซอฟต์แวร์และแพ็คเกจเป็นประจำเพื่อความปลอดภัย

Lab 9: การทำ Hyper-Converged Infrastructure (HCI) บน Ubuntu ด้วย Proxmox VE

ผู้สอน:

ผู้ช่วยศาสตราจารย์อมร เจือตี๋

วัตถุประสงค์:

1. เรียนรู้การติดตั้ง Proxmox VE บน Ubuntu
2. เรียนรู้การกำหนดค่าคอนฟิกและการใช้งาน Proxmox VE สำหรับ HCI

วัสดุและเครื่องมือ:

- ระบบปฏิบัติการ Linux (Ubuntu แนะนำ)
- สิทธิ์ root หรือ sudo
- หมายเลขเครือข่ายที่ใช้: 192.168.1.0/24

ตารางหมายเลข IP Address ที่ใช้

หมายเลข IP Address	อุปกรณ์	บันทึกเพิ่มเติม
192.168.1.1	Router	Gateway หลักของเครือข่าย
192.168.1.2	Proxmox VE Node 1	ติดตั้ง Proxmox VE Node ที่ 1
192.168.1.3	Proxmox VE Node 2	ติดตั้ง Proxmox VE Node ที่ 2
192.168.1.4	Proxmox VE Node 3	ติดตั้ง Proxmox VE Node ที่ 3
192.168.1.5 - 192.168.1.254	อุปกรณ์อื่นๆในเครือข่าย	เช่น คอมพิวเตอร์, มือถือ, IoT

วิธีการติดตั้ง

การติดตั้ง Proxmox VE

1. **อัพเดตระบบ:**
    - อัพเดต package list ของระบบ:

      sudo apt update

2. **ติดตั้ง Proxmox VE Repository:**
    - เพิ่ม Proxmox VE repository:

      echo "deb http://download.proxmox.com/debian/pve buster pve-no-subscription" | sudo tee /etc/apt/sources.list.d/pve-install-repo.list

3. **เพิ่ม Proxmox VE Repository Key:**
    - เพิ่มคีย์ repository:

      wget -qO - http://download.proxmox.com/debian/proxmox-ve-release-6.x.gpg | sudo apt-key add -

4. **อัพเดต package list และติดตั้ง Proxmox VE:**
    - อัพเดต package list:

      sudo apt update

    - ติดตั้ง Proxmox VE:

      sudo apt install proxmox-ve postfix open-iscsi -y

5. **ติดตั้งและคอนฟิกระบบเครือข่าย:**
    - ตรวจสอบการเชื่อมต่อเครือข่ายและกำหนดค่า IP Address:

      sudo nano /etc/network/interfaces

    - เพิ่มบรรทัดต่อไปนี้สำหรับการกำหนดค่า IP Address:

      plaintext

      auto lo
      iface lo inet loopback

      auto eth0
      iface eth0 inet static
        address 192.168.1.2
        netmask 255.255.255.0
        gateway 192.168.1.1
        dns-nameservers 8.8.8.8 8.8.4.4

6. **รีบูตระบบ:**
    - รีบูตระบบเพื่อให้การตั้งค่ามีผล:

      sudo reboot

วิธีการ config

การกำหนดค่า Proxmox VE Cluster

1. **เข้าสู่เว็บอินเตอร์เฟสของ Proxmox VE:**
    - เปิดเว็บเบราว์เซอร์แล้วเข้าไปที่ https://192.168.1.2:8006
    - ล็อกอินด้วยชื่อผู้ใช้ root และรหัสผ่านของระบบ

2. **สร้าง Cluster:**
    - เข้าไปที่ Datacenter > Cluster
    - คลิก Create Cluster และตั้งชื่อ Cluster
3. **เข้าร่วม Node อื่นๆ ใน Cluster:**
    - บน Node อื่นๆ ที่ต้องการเข้าร่วม Cluster ให้รันคำสั่งต่อไปนี้:

      pvecm add 192.168.1.2

การทดสอบ:

1. **ทดสอบการเข้าถึง Cluster:**
    - เปิดเว็บเบราว์เซอร์แล้วเข้าไปที่ https://192.168.1.2:8006
    - ล็อกอินด้วยชื่อผู้ใช้ root และรหัสผ่านของระบบ
    - ตรวจสอบว่า Node อื่นๆ ถูกเพิ่มเข้ามาใน Cluster เรียบร้อยแล้ว
2. **ทดสอบการสร้าง Virtual Machine (VM):**
    - ไปที่ Datacenter > Node ที่ต้องการสร้าง VM
    - คลิก Create VM และทำตามขั้นตอนเพื่อติดตั้ง VM ใหม่

สรุปผลการเรียนรู้:

ใน lab นี้ คุณได้เรียนรู้การติดตั้งและตั้งค่าคอนฟิก Proxmox VE บน Ubuntu รวมถึงวิธีการตั้งค่า Cluster และการเพิ่ม Node อื่นๆ เข้าสู่ Cluster เพื่อสร้าง Hyper-Converged Infrastructure (HCI)

ข้อแนะนำเพิ่มเติม:

- ควรทำการสำรองข้อมูลก่อนทำการตั้งค่าหรือแก้ไขไฟล์คอนฟิกใดๆ
- หากพบปัญหาในการติดตั้งหรือการตั้งค่า ควรตรวจสอบ log ไฟล์ของ Proxmox VE เพื่อหาสาเหตุและแนวทางแก้ไข
- ตรวจสอบและอัพเดตซอฟต์แวร์และแพ็คเกจเป็นประจำเพื่อความปลอดภัย

Lab 10: การทำ Database Cluster บน Ubuntu ด้วย MariaDB Galera Cluster

ผู้สอน:

ผู้ช่วยศาสตราจารย์อมร เจือตี๋

วัตถุประสงค์:

1. เรียนรู้การติดตั้ง MariaDB Galera Cluster บน Ubuntu
2. เรียนรู้การกำหนดค่าคอนฟิก Database Cluster

วัสดุและเครื่องมือ:

- ระบบปฏิบัติการ Linux (Ubuntu แนะนำ)
- สิทธิ์ root หรือ sudo
- หมายเลขเครือข่ายที่ใช้: 192.168.1.0/24

ตารางหมายเลข IP Address ที่ใช้

หมายเลข IP Address	อุปกรณ์	บันทึกเพิ่มเติม
192.168.1.1	Router	Gateway หลักของเครือข่าย
192.168.1.2	Database Server 1	ติดตั้ง MariaDB Galera Node ที่ 1
192.168.1.3	Database Server 2	ติดตั้ง MariaDB Galera Node ที่ 2
192.168.1.4	Database Server 3	ติดตั้ง MariaDB Galera Node ที่ 3
192.168.1.5 - 192.168.1.254	อุปกรณ์อื่นๆในเครือข่าย	เช่น คอมพิวเตอร์, มือถือ, IoT

วิธีการติดตั้ง

การติดตั้ง MariaDB Galera Cluster

1. **อัพเดตระบบ:**
    - อัพเดต package list ของระบบ:

      sudo apt update

2. **ติดตั้ง MariaDB:**
    - ติดตั้ง MariaDB Server และ Galera:

      sudo apt install mariadb-server mariadb-client galera-3 -y

วิธีการ config

การกำหนดค่า MariaDB Galera Cluster

1. **กำหนดค่าบน Node แรก (192.168.1.2):**
    - แก้ไขไฟล์คอนฟิก my.cnf:

      sudo nano /etc/mysql/my.cnf

    - เพิ่มบรรทัดต่อไปนี้:

      plaintext

      [mysqld]
      query_cache_size=0
      binlog_format=ROW
      default_storage_engine=InnoDB
      innodb_autoinc_lock_mode=2
      bind-address=0.0.0.0

```
[galera]
wsrep_on=ON
wsrep_provider=/usr/lib/galera/libgalera_smm.so
wsrep_cluster_address="gcomm://192.168.1.2,192.168.1.3,192.168.1.4"
wsrep_cluster_name="my_galera_cluster"
wsrep_node_address="192.168.1.2"
wsrep_node_name="node1"
wsrep_sst_method=rsync
```

- เริ่มต้น MariaDB และ MariaDB Galera Cluster บน Node แรก:

```
sudo systemctl start mariadb
sudo galera_new_cluster
```

2. **กำหนดค่าบน Node ที่สอง (192.168.1.3) และที่สาม (192.168.1.4):**
   - แก้ไขไฟล์คอนฟิก my.cnf เช่นเดียวกับ Node แรก แต่เปลี่ยนค่า wsrep_node_address และ wsrep_node_name ให้ตรงกับ IP Address และชื่อ Node ของตนเอง:

```
plaintext

wsrep_node_address="192.168.1.3"  # สำหรับ Node ที่สอง
wsrep_node_name="node2"

wsrep_node_address="192.168.1.4"  # สำหรับ Node ที่สาม
wsrep_node_name="node3"
```

   - เริ่มต้น MariaDB บน Node ที่สองและที่สาม:

```
sudo systemctl start mariadb
```

3. **ตรวจสอบการเชื่อมต่อของ Cluster:**
    - เข้าสู่ MariaDB บน Node แรก:

      sudo mysql -u root -p

    - รันคำสั่ง SQL ต่อไปนี้เพื่อตรวจสอบการเชื่อมต่อของ Cluster:

      sql

      OW STATUS LIKE 'wsrep_cluster_size';

การทดสอบ:

1. **ทดสอบการเพิ่มข้อมูลใน Cluster:**
    - เข้าสู่ MariaDB บน Node แรก:

      sudo mysql -u root -p

    - สร้างฐานข้อมูลและตารางทดสอบ:

      sql

      CREATE DATABASE testdb;
      USE testdb;
      CREATE TABLE testtable (id INT PRIMARY KEY, name VARCHAR(50));
      INSERT INTO testtable (id, name) VALUES (1, 'Test Name');

2. **ตรวจสอบข้อมูลบน Node อื่นๆ:**
    - เข้าสู่ MariaDB บน Node ที่สองและที่สาม:

      sudo mysql -u root -p
      USE testdb;
      SELECT * FROM testtable;

สรุปผลการเรียนรู้:

ใน lab นี้ คุณได้เรียนรู้การติดตั้งและตั้งค่าคอนฟิก MariaDB Galera Cluster บน Ubuntu รวมถึงวิธีการตรวจสอบการทำงานของ Cluster และการเชื่อมต่อระหว่าง Node ต่างๆ

ข้อแนะนำเพิ่มเติม:

- ควรทำการสำรองข้อมูลก่อนทำการตั้งค่าหรือแก้ไขไฟล์คอนฟิกใดๆ
- หากพบปัญหาในการติดตั้งหรือการตั้งค่า ควรตรวจสอบ log ไฟล์ของ MariaDB เพื่อหาสาเหตุและแนวทางแก้ไข
- ตรวจสอบและอัพเดตซอฟต์แวร์และแพ็คเกจเป็นประจำเพื่อความปลอดภัย

Lab 11: การใช้งาน Docker บน Ubuntu

ผู้สอน:

ผู้ช่วยศาสตราจารย์อมร เจือตี๋

วัตถุประสงค์:

1. เรียนรู้การติดตั้ง Docker บน Ubuntu
2. เรียนรู้การใช้งาน Docker พื้นฐาน

วัสดุและเครื่องมือ:

- ระบบปฏิบัติการ Linux (Ubuntu แนะนำ)
- สิทธิ์ root หรือ sudo
- หมายเลขเครือข่ายที่ใช้: 192.168.1.0/24

ตารางหมายเลข IP Address ที่ใช้

หมายเลข IP Address	อุปกรณ์	บันทึกเพิ่มเติม
192.168.1.1	Router	Gateway หลักของเครือข่าย
192.168.1.2	Docker Host	ติดตั้ง Docker
192.168.1.3 - 192.168.1.254	อุปกรณ์อื่นๆในเครือข่าย	เช่น คอมพิวเตอร์, มือถือ, IoT

วิธีการติดตั้ง

การติดตั้ง Docker

1. **อัพเดตระบบ:**
    - อัพเดต package list ของระบบ:

      sudo apt update

2. **ติดตั้งแพ็คเกจที่จำเป็น:**
    - ติดตั้งแพ็คเกจที่จำเป็น:

      sudo apt install apt-transport-https ca-certificates curl software-properties-common -y

3. **เพิ่ม Docker GPG key:**
    - เพิ่ม Docker GPG key:

      curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -

4. **เพิ่ม Docker repository:**
    - เพิ่ม Docker repository:

      sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable"

5. **ติดตั้ง Docker:**
    - อัพเดต package list และติดตั้ง Docker:

      sudo apt update
      sudo apt install docker-ce -y

6. **ตรวจสอบสถานะของ Docker:**
    - ตรวจสอบสถานะของ Docker:

      sudo systemctl status docker

7. **ตั้งค่า Docker ให้รันอัตโนมัติเมื่อเริ่มระบบ:**
    - ตั้งค่า Docker ให้รันอัตโนมัติ:

      sudo systemctl enable docker

วิธีการใช้งานพื้นฐาน

การใช้งาน Docker พื้นฐาน

1. **ตรวจสอบเวอร์ชันของ Docker:**
    - ตรวจสอบเวอร์ชัน:

      docker --version

2. **ดึงภาพ Docker (Docker Image):**
    - ดึงภาพ Docker ของ Nginx:

      sudo docker pull nginx

3. **รันคอนเทนเนอร์ (Container) จากภาพ Docker:**
    - รันคอนเทนเนอร์จากภาพ Docker ของ Nginx:

      sudo docker run -d -p 80:80 --name mynginx nginx

4. **ตรวจสอบคอนเทนเนอร์ที่กำลังรัน:**
    - ตรวจสอบคอนเทนเนอร์ที่กำลังรัน:

      sudo docker ps

5. **หยุดคอนเทนเนอร์:**
    - หยุดคอนเทนเนอร์:

      sudo docker stop mynginx

6. **ลบคอนเทนเนอร์:**
    - ลบคอนเทนเนอร์:

      sudo docker rm mynginx

การทดสอบ:

1. **ทดสอบการเข้าถึง Nginx:**
    - เปิดเว็บเบราว์เซอร์แล้วเข้าไปที่ http://192.168.1.2
    - คุณควรเห็นหน้าเว็บเริ่มต้นของ Nginx ที่รันอยู่ใน Docker Container
2. **ทดสอบการสร้างและรันคอนเทนเนอร์อื่นๆ:**
    - ลองดึงภาพ Docker อื่นๆ และรันคอนเทนเนอร์ เช่น MySQL, PostgreSQL, Redis เป็นต้น
    - ใช้คำสั่ง docker pull และ docker run เพื่อทดสอบการทำงาน

สรุปผลการเรียนรู้:

ใน lab นี้ คุณได้เรียนรู้การติดตั้งและตั้งค่าคอนฟิก Docker บน Ubuntu รวมถึงการใช้งาน Docker พื้นฐาน เช่น การดึงภาพ Docker, การรันคอนเทนเนอร์, การตรวจสอบสถานะ, การหยุดและลบคอนเทนเนอร์

ข้อแนะนำเพิ่มเติม:

- ควรทำการสำรองข้อมูลก่อนทำการตั้งค่าหรือแก้ไขไฟล์คอนฟิกใดๆ
- หากพบปัญหาในการติดตั้งหรือการตั้งค่า ควรตรวจสอบ log ไฟล์ของ Docker เพื่อหาสาเหตุและแนวทางแก้ไข
- ตรวจสอบและอัพเดตซอฟต์แวร์และแพ็คเกจเป็นประจำเพื่อความปลอดภัย