แบบเสนอโครงงานพิเศษ (ปริญญานิพนธ์)

สาขาวิชาวิศวกรรมสารสนเทศและเครือข่าย

ภาควิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีและการจัดการอุตสาหกรรม

1. **ข้อมูลขั้นต้นของโครงงาน**
   1. **ชื่อโครงงาน**

เว็บแอปพลิเคชันกำหนดค่าอุปกรณ์และตรวจสอบช่องโหว่ชองการกำหนดค่าอุปกรณ์เครือข่าย CISCO

A web application for configuring and assessing configuration vulnerabilities of CISCO network devices

* 1. **ชื่อนักศึกษาผู้ทำโครงงาน**
     1. ศุภวิชญ์ แซ่ลิ่ม รหัสนักศึกษา 6506022420053
  2. **ชื่ออาจารย์ที่ปรึกษา / อาจารย์ที่ปรึกษาร่วม**
     1. อาจารย์ ดร.วัชรชัย คงศิริวัฒนา

1. **รายละเอียดโครงงาน**
   1. **ความเป็นมาและความสำคัญของปัญหา**

ปัจจุบันเทคโนโลยีเครือข่ายที่รวดเร็ว และมีประสิทธิภาพมีความสำคัญต่อการดำเนินธุรกิจ และการสื่อสารในชีวิตประจำวันของมนุษย์ การจัดการอุปกรณ์เครือข่ายจึงกลายเป็นสิ่งสำคัญสำหรับองค์กรต่าง ๆ อุปกรณ์เครือข่ายที่สำคัญ เช่น Router และ Switch เป็นส่วนประกอบหลัก ในการทำให้ระบบเครือข่ายสื่อสารกันได้อย่างมีประสิทธิภาพ นอกจากนี้การจัดการและตรวจสอบการตั้งค่าของอุปกรณ์ดังกล่าวค่อนข้างมีความซับซ้อน และใช้เวลานาน ก่อให้เกิดปัญหา เช่น การตั้งค่าผิดพลาด ไม่ถูกต้องตามหลักการกำหนดค่า รวมถึงการตรวจสอบสถานะของอุปกรณ์ที่ไม่เป็นไปตามที่ควร นำไปสู่ความเสี่ยงต่อการเกิดช่องโหว่ในระบบเครือข่าย ดังนั้นการมีเครื่องมือที่สามารถช่วยตรวจสอบ และจัดการการตั้งค่าของอุปกรณ์เครือข่ายจึงเป็นสิ่งจำเป็น ส่งผลให้ผู้ดูแลระบบสามารถควบคุม ตรวจสอบสถานะของอุปกรณ์ได้อย่างมีประสิทธิภาพ

นอกจากนี้ การสามารถเข้าถึงและจัดการอุปกรณ์เครือข่ายได้ในแบบเรียลไทม์ ยังเป็นสิ่งสำคัญที่ช่วยให้ผู้ดูแลระบบสามารถแก้ไขปัญหาได้อย่างรวดเร็ว ลดระยะเวลาที่อุปกรณ์จะไม่พร้อมทำงาน ดังนั้นการพัฒนาโปรแกรมที่สามารถรองรับการเชื่อมต่อกับอุปกรณ์เครือข่ายใหม่ การตั้งค่า และการตรวจสอบช่องโหว่ในการกำหนดค่าของอุปกรณ์จึงมีความสำคัญมากในการปรับปรุงประสิทธิภาพ ความปลอดภัยของเครือข่ายในองค์กรในการใช้งานในปัจจุบัน

* 1. **วัตถุประสงค์ของการจัดทำโครงงานพิเศษ**
     1. เพิ่มความสะดวกให้ผู้ดูระบบสามารถตั้งค่าเริ่มต้นของอุปกรณ์ได้ผ่านเว็บแอปพลิเคชัน โดยไม่ต้องใช้ command line ในการตั้งค่าเริ่มต้นของอุปกรณ์เครือข่าย
     2. พัฒนาโปรแกรมที่สามารถกำหนดค่าอุปกรณ์เครือข่ายหลายตัวพร้อมกันเพื่อประหยัดเวลา และสามารถตรวจสอบการตั้งค่าของอุปกรณ์ในเครือข่ายนั้นๆ ได้
     3. เพื่อเพิ่มความปลอดภัยให้กับอุปกรณ์เครือข่ายด้วยความสามารถในการตรวจสอบการตั้งค่าของอุปกรณ์ และแสดงจุดที่ควรปรับปรุง
  2. **ขอบเขตของการทำโคงงานพิเศษ**
     1. โปรแกรมรองรับการเชื่อมต่อกับอุปกรณ์เครือข่ายใหม่ที่ยังไม่ได้ตั้งค่า โดยใช้การเชื่อมต่อผ่าน serial port และสามารถทำการตั้งค่า ค่าต่างๆ โดยผู้ใช้สามารถแก้ค่าเพื่อให้ตรงกับความต้องการได้ เพื่อให้พร้อมสำหรับการควบคุมผ่านโปรแกรม :
        1. Console port ที่เชื่อมต่อกับตัวอุปกรณ์
        2. Hostname
        3. Privilege Password
        4. Username และ password สำหรับการ SSH
        5. Domain-name
        6. ระบุ Interface ที่ใช้ในการตั้งค่า IP Address เพื่อจะใช้ในเชื่อมต่อในเครือข่าย สามารถเลือกได้ ดังนี้
           1. ระบุ IP Address
           2. DHCP
     2. โปรแกรมรองรับการตั้งค่าอุปกรณ์เครือข่ายหลายตัวในเวลาเดียวกันโดยใช้เทคนิค threading ซึ่งช่วยลดเวลาที่ใช้ในการ config อุปกรณ์หลายเครื่องพร้อมกัน
     3. ผู้ใช้สามารถเพิ่มรายละเอียดของอุปกรณ์ที่จะตั้งค่าผ่านโปรแกรมและบันทึกลงระบบฐานข้อมูล โดยมีรายละเอียดดังนี้
        1. ชื่ออุปกรณ์ (Name)
        2. ที่อยู่ IP Address
        3. ชื่อผู้ใช้ (Username)
        4. รหัสผ่าน (Password)
        5. รหัสผ่านเข้าสู่โหมด Privilege (Secret Password)
     4. ผู้ใช้สามารถดูรายละเอียดของอุปกรณ์ที่เพิ่มเข้าสู่ระบบทั้งหมดได้และสามารถลบได้
     5. โปรแกรมรองรับการตั้งค่าอุปกรณ์โดยมีความสามารถในการตั้งค่า ค่าต่างๆ ดังนี้
        1. หัวข้อการตั้งค่าพื้นฐาน
           1. ค่า hostname
           2. ค่า Secret Password
           3. ค่า Banner
        2. หัวข้อการตั้งค่าช่องสัญญาณเครือข่าย
           1. ช่องสัญญาณเครือข่าย
           2. ที่อยู่ของช่องสัญญาณ (IP Address)
           3. Status (Up/Down)
           4. Switchport (Trunk, Access)
        3. หัวข้อการตั้งค่าการจัดการ มีรายละเอียด ดังนี้:
           1. การตั้งค่าช่องสัญญาณ Console

รหัสผ่าน

ระยะเวลาหมดการเชื่อมต่อ (Session)

เปิดปิดใช้งานการบันทึกข้อมูลแบบซิงโครนัส

* + - * 1. การตั้งค่าช่องสัญญาณ VTY

รหัสผ่าน

ระยะเวลาหมดการเชื่อมต่อ (Session)

โปรโตคอลที่ยอมรับ

SSH

TELNET

ALL

NONE

สามาระบุช่วง VTY line

เปิดปิดใช้งานการบันทึกข้อมูลแบบซิงโครนัส

* + - * 1. การตั้งค่าเทคโนโลยีโปรโตคอล DHCP

ชื่อ Pool

เครือข่าย

ที่อยู่ที่ไม่ต้องการให้บริการ (IP Exclude)

ค่าเราเตอร์ค่าเริ่มต้น

ค่าที่อยู่ DNS เซิร์ฟเวอร์

ชื่อโดเมน

* + - * 1. การตั้งค่าเทคโนโลยีโปรโตคอล NTP

ที่อยู่ของ NTP เซิร์ฟเวอร์

เขตเวลา (Time zone)

* + - * 1. การตั้งค่าเทคโนโลยีโปรโตคอล SNMP

กำหนดค่า Community string แบบ read-only

กำหนดค่า Community string แบบ read-write

* + - * 1. เปิดปิดการตั้งค่าเทคโนโลยีโปรโตคอล CDP
        2. เปิดปิดการตั้งค่าเทคโนโลยีโปรโตคอล LLDP
      1. หัวข้อการตั้งค่าเครือข่ายเสมือน
         1. การกำหนดค่าสร้างเครือข่ายเสมือน (VLAN)
         2. การกำหนดชื่อในการสร้างเครือข่ายเสมือน (VLAN)
         3. การลบเครือข่ายเสมือน
      2. หัวข้อการตั้งค่าเทคโนโลยี Spanning Tree Protocols
         1. การเลือกเวอร์ชันและโหมดของโปรโตคอล
         2. สามารถเลือกให้อุปกรณ์ตัวนั้นเป็น Root (primary/secondary) ในเครือข่ายเสมือนหมายเลข ID อะไร
         3. สามารถระบุช่องสัญญาณในการเปิดปิดฟังก์ชัน Postfast
         4. เทคโนโลยี BPDU-Guard จะเปิดใช้อัตโนมัติกับช่องสัญญาณที่ระบุในฟังก์ชัน Postfast
      3. หัวข้อการตั้งค่าการรวมกลุ่ม Aggregation Protocols
         1. เทคโนโลยี Port Aggregation Protocol (PAgP)

สามารถกำหนดช่องสัญญาณ

สามารถกำหนดหมายเลขของการรวมกลุ่มของช่องสัญญาณนั้น (Channel-group Number)

สามารถกำหนดโหมดได้ทั้งแบบ Desirable และ Auto

* + - * 1. เทคโนโลยี Link Aggregation Protocol (LAcP)

สามารถกำหนดช่องสัญญาณ

สามารถกำหนดหมายเลขของการรวมกลุ่มของช่องสัญญาณนั้น (Channel-group Number)

สามารถกำหนดโหมดได้ทั้งแบบ Active และ Passive

* + 1. หัวข้อการการกำหนดค่าเส้นทางของอุปกรณ์
       1. การกำหนดเส้นทางแบบ Static Route
          1. ระบุเครือข่ายปลายทางได้สูงสุด 4 เครือข่าย
          2. สามารถเลือกวิธีการส่งแพ็คเก็ตได้สองรูปแบบ ได้แก่ Exit Interface หรือ IP Next Hop
          3. สามารถเลือกเส้นทางแบบ Default Route ได้
          4. สามารถลบเส้นทางที่กำหนดไว้ได้
       2. การกำหนดเส้นทางโปรโตคอล OSPF
          1. สามารถกำหนด Process ID ได้
          2. สามารถกำหนด Router ID ของอุปกรณ์นั้นๆ ได้
          3. ระบุเครือข่ายปลายทางได้สูงสุด 3 เครือข่าย
          4. สามารถลบ Process ID ได้
          5. สามารถลบเส้นทางที่กำหนดไว้ได้
       3. การกำหนดเส้นทางโปรโตคอล RIPv2
       4. การกำหนดเส้นทางโปรโตคอล EIGRP
    2. โปรแกรมสามารถรีเซ็ตการตั้งค่าของตัวอุปกรณ์นั้นได้ และจะถูกลบออกจากฐานข้อมูล
    3. โปรแกรมสามารถแสดงการกำหนดค่าของอุปกรณ์นั้นๆได้ โดยผู้ใช้สามารถเลือก หรือกรอกคำสั่งที่ต้องการให้แสดงได้
    4. โปรแกรมมีการตรวจสอบการตั้งค่า (configuration) ของอุปกรณ์เครือข่ายในด้านความปลอดภัย ดังนี้
       1. สามารถตรวจสอบหาช่องโหว่ของการตั้งค่าอุปกรณ์โดยอัตโนมัติ ดังนี้
          1. ช่องโหว่ด้านรหัสผ่าน
          2. การเข้ารหัสรหัสผ่าน
          3. สถานะพอร์ตเครือข่ายที่ไม่ได้ใช้งาน
          4. การตั้งค่าการหมดเวลาการเชื่อมต่อ
          5. การตรวจสอบโปรโตคอลการเข้าถึงระยะไกล
    5. โปรแกรมสามารถตรวจสอบรายละเอียดของอุปกรณ์นั้นๆ มีรายละเอียดต่างๆ ดังนี้
       1. ประเภทของอุปกรณ์ Router หรือ Switch
       2. รายละเอียดคำอธิบาย (Description) ของอุปกรณ์
       3. ระยะเวลาการทำงาน (Uptime) ของอุปกรณ์
       4. ข้อมูลการติดต่อ (Contact) ของอุปกรณ์
       5. ชื่อของอุปกรณ์
       6. สถานที่ตั้ง (Location) ของอุปกรณ์
       7. ชื่อ Interfaces ทั้งหมดที่มีของอุปกรณ์นั้นๆ
  1. **รายละเอียดของทฤษฎีที่ใช้ในการจัดทำปริญญานิพนธ์**
     1. **สมมติฐาน หรือ ข้อตกลงเบื้องต้นในการจัดทำโครงงานพิเศษ (Assumption of the Study)**

การพัฒนาโปรแกรมที่ใช้ระบบอัตโนมัติในการตั้งค่าอุปกรณ์เครือข่าย พร้อมด้วยการใช้ปัญญาประดิษฐ์ในการตรวจสอบความปลอดภัย จะช่วยลดระยะเวลาในการตั้งค่าเครือข่าย เพิ่มความถูกต้องแม่นยำในการตรวจจับช่องโหว่ และลดข้อผิดพลาดที่เกิดจากการตั้งค่าด้วยมือ ซึ่งมักเกิดขึ้นเมื่อผู้ดูแลระบบดำเนินการเพียงอย่างเดียว นอกจากนี้ โปรแกรมยังมีความสามารถในการจัดการกับอุปกรณ์เครือข่ายหลายตัวในเวลาเดียวกัน โดยใช้เทคนิค threading ที่ช่วยเพิ่มประสิทธิภาพในการตั้งค่าและปรับแต่งอุปกรณ์ต่าง ๆ ได้อย่างรวดเร็วและมีประสิทธิผล เมื่อเปรียบเทียบกับวิธีการดั้งเดิม โปรแกรมนี้ยังช่วยให้ผู้ดูแลระบบสามารถตรวจสอบสถานะการตั้งค่าและความปลอดภัยของอุปกรณ์ได้อย่างต่อเนื่อง ช่วยลดความเสี่ยงด้านความปลอดภัยในระบบเครือข่ายองค์กรได้อย่างมีประสิทธิภาพ

* + 1. **คำจำกัดความ (Key Word)**
       1. AI (Artificial Intelligence) – เทคโนโลยีที่ช่วยให้คอมพิวเตอร์สามารถเรียนรู้และดำเนินการตามรูปแบบต่างๆ ได้โดยอัตโนมัติ ซึ่งในโครงงานนี้ AI ถูกนำมาใช้เพื่อช่วยในการตั้งค่าเครือข่ายและตรวจสอบความปลอดภัย
       2. Auto-Config (Automatic Configuration) – การตั้งค่าอุปกรณ์เครือข่ายโดยอัตโนมัติผ่านระบบที่พัฒนา ซึ่งไม่จำเป็นต้องใช้คำสั่งแบบ manual command line
       3. Network Security – การป้องกันระบบเครือข่ายจากการโจมตีหรือการเข้าถึงโดยไม่ได้รับอนุญาต เพื่อรักษาความปลอดภัยของข้อมูลและการเชื่อมต่อภายในเครือข่าย
       4. Threading – เทคนิคการประมวลผลหลายขั้นตอนพร้อมกัน (parallel processing) ช่วยให้สามารถตั้งค่าอุปกรณ์เครือข่ายหลายตัวพร้อมกันได้ ลดระยะเวลาในการดำเนินการ
       5. Vulnerability (ช่องโหว่) – ข้อบกพร่องหรือช่องโหว่ในระบบเครือข่ายที่อาจถูกผู้ไม่ประสงค์ดีใช้โจมตี ซึ่งปัญญาประดิษฐ์ในโครงงานนี้ถูกพัฒนาให้สามารถตรวจจับและแนะนำการแก้ไข
       6. SSH (Secure Shell) – โปรโตคอลที่ใช้ในการเข้าถึงและควบคุมอุปกรณ์เครือข่ายอย่างปลอดภัยผ่านการเข้ารหัส
       7. Routing Protocols – ชุดของกฎเกณฑ์ที่ใช้ในการกำหนดเส้นทางที่ดีที่สุดสำหรับการส่งข้อมูลภายในเครือข่าย เช่น RIP, OSPF, EIGRP, Static Route
       8. SNMP (Simple Network Management Protocol) คือ โปรโตคอลมาตรฐานที่ใช้สำหรับการจัดการและตรวจสอบอุปกรณ์ในเครือข่าย เช่น Router, Switch, Server และอุปกรณ์เครือข่ายอื่นๆ SNMP ช่วยให้ผู้ดูแลระบบสามารถตรวจสอบประสิทธิภาพของอุปกรณ์เครือข่าย รวมถึงรับข้อมูลเกี่ยวกับสถานะและปัญหาต่างๆ ที่เกิดขึ้นได้แบบเรียลไทม์
       9. DHCP (Dynamic Host Configuration Protocol) – โปรโตคอลที่ใช้ในการมอบหมายที่อยู่ IP และการตั้งค่าพื้นฐานให้กับอุปกรณ์ในเครือข่ายโดยอัตโนมัติ ช่วยลดความยุ่งยากในการตั้งค่า IP Address ของอุปกรณ์แต่ละตัว
       10. NTP (Network Time Protocol) – โปรโตคอลที่ใช้สำหรับการซิงโครไนซ์เวลาระหว่างอุปกรณ์ในเครือข่าย โดยช่วยให้แน่ใจว่าอุปกรณ์ทุกตัวมีเวลาที่ถูกต้องและสอดคล้องกัน ซึ่งมีความสำคัญต่อการทำงานร่วมกันของระบบเครือข่ายและการบันทึกเหตุการณ์ (logging)
       11. CDP (Cisco Discovery Protocol) – โปรโตคอลที่ใช้สำหรับการค้นหาและแสดงข้อมูลเกี่ยวกับอุปกรณ์ Cisco อื่น ๆ ที่เชื่อมต่ออยู่ในเครือข่าย เช่น ชื่ออุปกรณ์, ที่อยู่ IP และรายละเอียดของสื่อที่เชื่อมต่อ โดยช่วยให้ผู้ดูแลระบบสามารถจัดการและวางแผนเครือข่ายได้ดียิ่งขึ้น
       12. LLDP (Link Layer Discovery Protocol) – โปรโตคอลมาตรฐานที่ใช้ในการค้นหาและแลกเปลี่ยนข้อมูลระหว่างอุปกรณ์เครือข่ายที่เชื่อมต่อกัน โดยไม่จำเป็นต้องใช้โปรโตคอลของผู้ผลิตใด ๆ ช่วยให้ผู้ดูแลระบบสามารถตรวจสอบข้อมูลของอุปกรณ์ที่เชื่อมต่ออยู่ได้ เช่น ชื่อ, ประเภท, และรายละเอียดการเชื่อมต่อ
       13. Aggregation Protocols – โปรโตคอลที่ใช้ในการรวมช่องทางการเชื่อมต่อหลาย ๆ ช่องทางเข้าเป็นช่องทางเดียว เพื่อเพิ่มประสิทธิภาพการส่งข้อมูลในเครือข่าย โดยช่วยให้สามารถเพิ่มความจุและความน่าเชื่อถือของการเชื่อมต่อ
       14. Spanning Tree Protocol (STP) – โปรโตคอลที่ใช้ในการป้องกันการเกิด loop ในเครือข่าย Ethernet โดยการจัดการและสร้าง topologies ที่มีการเชื่อมต่อหลายจุดให้มีความปลอดภัย โดย STP ช่วยให้ผู้ดูแลระบบสามารถควบคุมการทำงานของ switch ได้ดียิ่งขึ้น
       15. Root Primary Bridge – สามารถเลือกให้ switch ตัวนั้นเป็น root primary bridge ซึ่งเป็น switch หลักที่ใช้สำหรับการส่งข้อมูลในเครือข่าย โดยจะมีการเลือก switch ที่มี bridge ID ต่ำที่สุดในเครือข่าย
       16. Root Secondary Bridge – สามารถเลือกให้ switch ตัวนั้นเป็น root secondary bridge ซึ่งเป็น switch ที่รองรับการทำงานของ root primary bridge ในกรณีที่เกิดปัญหาหรือ failure ขึ้นกับ root primary bridge
       17. Postfast – ฟังก์ชันที่ช่วยในการเร่งการฟื้นฟูการทำงานของ interface ในกรณีที่เกิดการเปลี่ยนแปลง topology โดยการเปิดหรือปิดฟังก์ชันนี้ช่วยให้สามารถลดเวลาที่ใช้ในการประมวลผล
       18. BPDU Guard – ฟังก์ชันที่ช่วยป้องกันการเกิด loop ในเครือข่าย โดยการปิด port ที่รับ BPDU (Bridge Protocol Data Units) จาก switch ที่ไม่ควรเชื่อมต่อเข้ามาในเครือข่าย ช่วยเพิ่มความปลอดภัยและลดปัญหาที่เกิดจาก loop
    2. **เนื้อหา เหตุผล และทฤษฎีที่สำคัญ**

ในการพัฒนาโครงการพิเศษเรื่อง "เว็บแอปพลิเคชันกำหนดค่าอุปกรณ์เครือข่ายและตรวจสอบความปลอดภัยอุปกรณ์ CISCO" เนื้อหาและทฤษฎีที่เกี่ยวข้องมีความสำคัญอย่างยิ่งในการสนับสนุนการทำงานของโปรแกรมอย่างลึกซึ้ง ไม่ว่าจะเป็นหลักการทำงานของระบบเครือข่าย การตั้งค่าอุปกรณ์เครือข่ายแบบอัตโนมัติ รวมถึงการใช้เทคโนโลยีที่ทันสมัยในการตรวจสอบและรักษาความปลอดภัยของเครือข่าย ทั้งนี้เพื่อให้ผู้ดูแลระบบสามารถจัดการและควบคุมความปลอดภัยของอุปกรณ์เครือข่ายได้อย่างมีประสิทธิภาพ ต่อไปนี้จะเป็นการอธิบายทฤษฎีที่สำคัญและเหตุผลที่สนับสนุนการดำเนินโครงการนี้

* + - 1. ทฤษฎีเกี่ยวกับการตั้งค่าเครือข่าย (Network Configuration Theory)

การตั้งค่าเครือข่าย (Network Configuration) เป็นกระบวนการสำคัญในการจัดการเครือข่ายที่ต้องตั้งค่าต่างๆ เช่น การกำหนดชื่อ (hostname), การตั้งค่า IP Address, การตั้งค่าความปลอดภัย (security), การเชื่อมต่อและการสื่อสารระหว่างอุปกรณ์ เช่น router, switch, และ firewall การตั้งค่าทุกอย่างต้องถูกต้องเพื่อให้เครือข่ายสามารถทำงานได้อย่างมีประสิทธิภาพและปลอดภัยกระบวนการตั้งค่าเครือข่ายแบบดั้งเดิมมักต้องทำด้วยตนเองผ่าน command line ซึ่งต้องใช้ความรู้เฉพาะทางและเวลาที่มาก การนำโปรแกรมที่สามารถตั้งค่าอุปกรณ์เครือข่ายได้โดยอัตโนมัติจึงเข้ามาช่วยลดภาระของผู้ดูแลระบบและลดโอกาสเกิดข้อผิดพลาดจากการตั้งค่าด้วยมือ ทำให้เกิดความมั่นใจว่าอุปกรณ์ทุกตัวจะมีการตั้งค่าที่ถูกต้องและสอดคล้องกับมาตรฐานความปลอดภัย

* + - 1. ทฤษฎีปัญญาประดิษฐ์ (Artificial Intelligence)

เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) เป็นรากฐานสำคัญของโครงงานนี้ AI มีความสามารถในการเรียนรู้และวิเคราะห์ข้อมูลเพื่อทำการตัดสินใจอย่างอัตโนมัติ โดยเฉพาะในด้านการตั้งค่าเครือข่ายและการรักษาความปลอดภัย AI สามารถประมวลผลข้อมูลจำนวนมากเพื่อหาแนวทางที่ดีที่สุดในการตั้งค่าหรือวิเคราะห์ความผิดปกติของการจราจรเครือข่าย ซึ่งช่วยลดภาระของผู้ดูแลระบบในการตรวจสอบทุกอย่างด้วยตนเอง

ในโครงงานนี้ AI จะถูกนำมาใช้ในการตรวจสอบการตั้งค่าของอุปกรณ์เครือข่าย เช่น การตรวจหาช่องโหว่ (vulnerabilities) หรือการตั้งค่าที่อาจเป็นอันตราย และทำการปรับปรุงการตั้งค่าอัตโนมัติหากพบความผิดปกติ AI สามารถทำงานเบื้องหลังในการตรวจสอบ traffic ของเครือข่ายโดยไม่จำเป็นต้องหยุดการทำงานของระบบ

* + - 1. ทฤษฎีการรักษาความปลอดภัยเครือข่าย (Network Security Theory)

การรักษาความปลอดภัยของเครือข่ายเป็นองค์ประกอบสำคัญในสภาพแวดล้อมทางธุรกิจและองค์กรสมัยใหม่ เครือข่ายเป็นช่องทางที่ข้อมูลสามารถถูกดักฟัง (eavesdrop), ถูกขโมย (data theft), หรือถูกโจมตี (attack) ได้ การตั้งค่าความปลอดภัยที่เหมาะสมเป็นสิ่งสำคัญเพื่อป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต โครงงานนี้มุ่งเน้นการพัฒนาเว็บแอปพลิเคชันที่สามารถตรวจสอบความปลอดภัยของเครือข่ายได้อัตโนมัติ โดยใช้ปัญญาประดิษฐ์ในการวิเคราะห์การตั้งค่าต่างๆ ของอุปกรณ์เครือข่าย เช่น การตั้งค่า router, การตั้งค่าเข้ารหัส (encryption), การตั้งค่าการเข้าถึงผ่าน SSH (Secure Shell) ที่ช่วยให้การเข้าถึงอุปกรณ์เครือข่ายทำได้อย่างปลอดภัยมากขึ้นปัญญาประดิษฐ์สามารถตรวจจับการตั้งค่าที่มีช่องโหว่หรือการตั้งค่าที่ไม่ปลอดภัยได้รวดเร็ว ทำให้ผู้ดูแลระบบสามารถแก้ไขปัญหาได้ทันเวลา ลดความเสี่ยงในการถูกโจมตีทางไซเบอร์

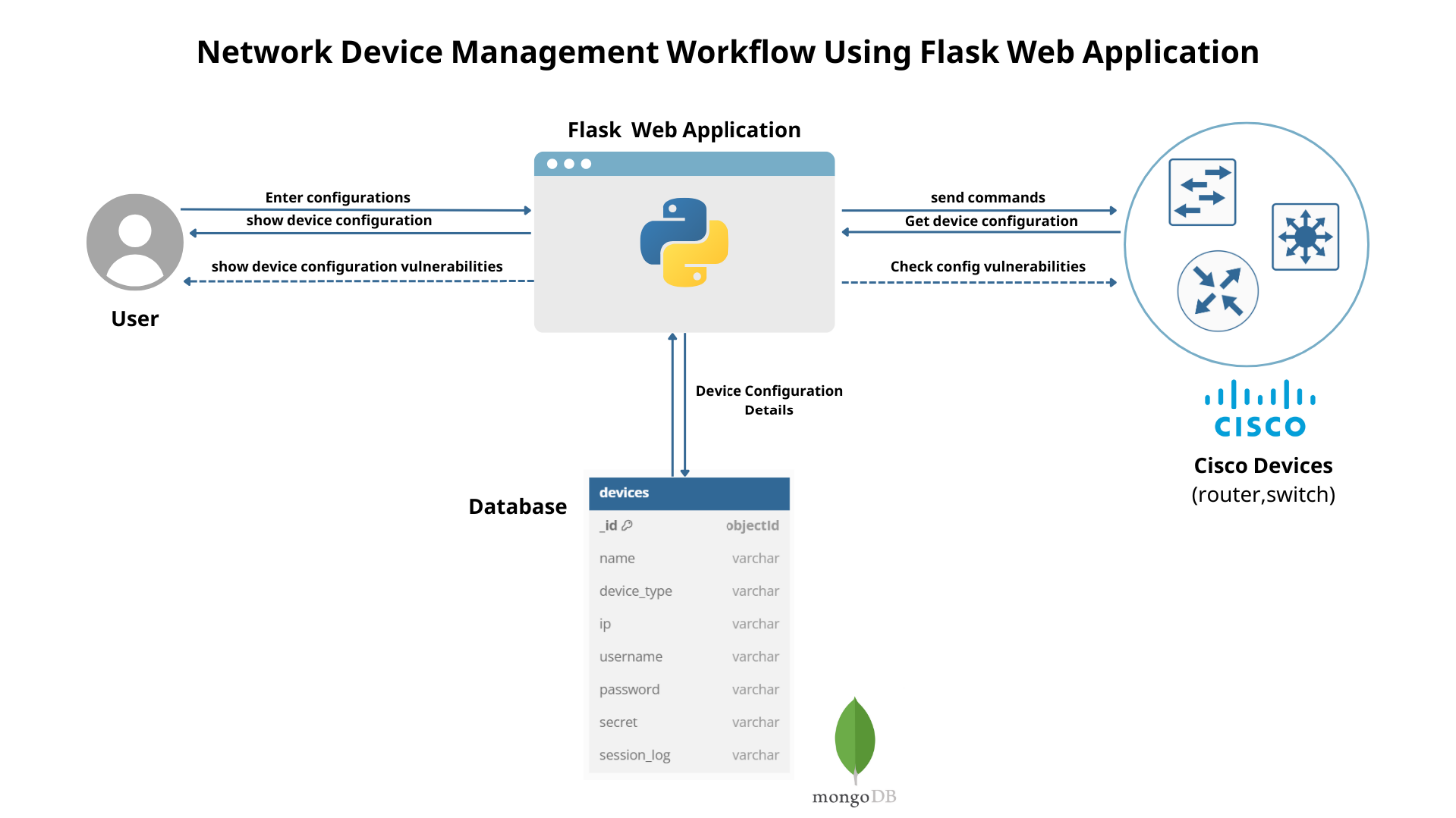
* + - 1. ทฤษฎีการประมวลผลแบบขนาน (Parallel Processing หรือ Threading)

การตั้งค่าอุปกรณ์เครือข่ายหลายตัวพร้อมกันเป็นกระบวนการที่มักใช้เวลานานในสภาพแวดล้อมที่ซับซ้อน โครงงานนี้ใช้เทคนิคการประมวลผลแบบขนาน (threading) ซึ่งเป็นการแบ่งการประมวลผลออกเป็นหลายส่วนและดำเนินการพร้อมกัน ช่วยลดเวลาที่ใช้ในการตั้งค่าอุปกรณ์เครือข่ายหลายตัวได้อย่างมีประสิทธิภาพ การประมวลผลแบบ threading ยังช่วยลดภาระของผู้ดูแลระบบที่ต้องทำงานหลายอย่างพร้อมกัน การใช้เทคนิคนี้ทำให้โปรแกรมสามารถตั้งค่าอุปกรณ์หลายตัวในเวลาเดียวกัน โดยไม่ต้องรอให้แต่ละตัวทำงานเสร็จสิ้นก่อน จึงเพิ่มประสิทธิภาพในการจัดการเครือข่ายและลดความล่าช้าในกระบวนการ

* + - 1. ทฤษฎีการตั้งค่าเครือข่าย (Network Configuration Theory)

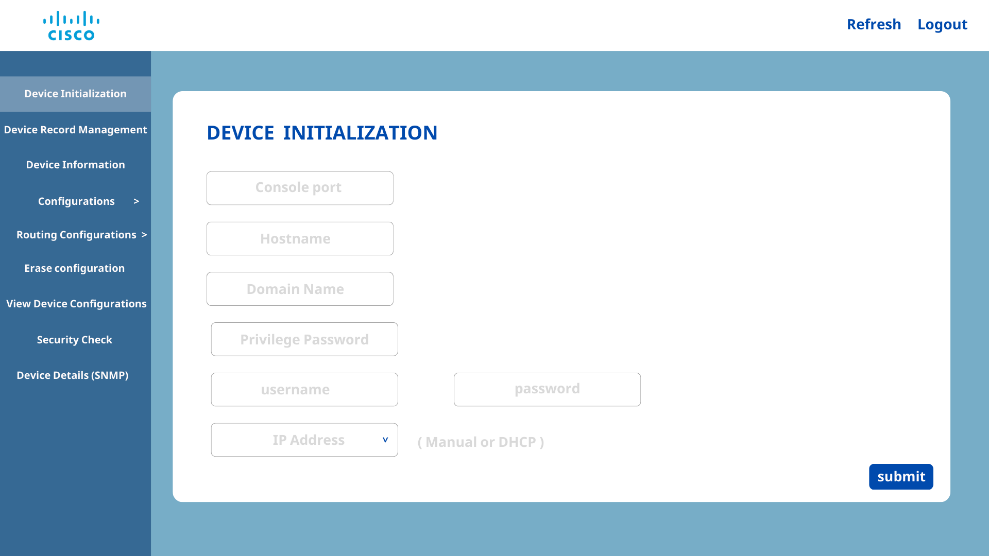
การตั้งค่าเครือข่าย (Network Configuration) เป็นกระบวนการจัดการเครือข่ายที่เกี่ยวข้องกับการตั้งค่าอุปกรณ์ต่างๆ เช่น Router, Switch, Firewall โดยต้องตั้งค่าการเชื่อมต่อระหว่างอุปกรณ์ การกำหนดชื่อ (Hostname) และการตั้งค่า IP Address เพื่อให้เครือข่ายทำงานได้อย่างราบรื่น การตั้งค่าเหล่านี้มีความซับซ้อนและต้องทำด้วยความระมัดระวังเป็นพิเศษ เนื่องจากมีผลโดยตรงต่อประสิทธิภาพและความปลอดภัยของเครือข่าย ในการตั้งค่าเครือข่ายแบบดั้งเดิม ผู้ดูแลระบบจะต้องใช้ Command Line Interface (CLI) ในการกำหนดค่า ซึ่งต้องใช้เวลานานและมีโอกาสเกิดข้อผิดพลาดสูง โครงการนี้จึงเสนอแนวทางการใช้โปรแกรมเพื่อจัดการการตั้งค่าเครือข่ายโดยอัตโนมัติ เพื่อช่วยลดภาระการทำงานของผู้ดูแลระบบ ลดความผิดพลาดที่เกิดจากการตั้งค่าเครือข่ายด้วยมือ และเพิ่มความมั่นใจในความปลอดภัยและความเสถียรของเครือข่าย

* 1. **วิธีดำเนินการจัดทำโครงงานพิเศษ**
     1. วิเคราะห์ปัญหาและความต้องการ
* ศึกษาปัญหาการตั้งค่าเครือข่ายและการรักษาความปลอดภัยในเครือข่ายโดยละเอียด
* กำหนดความต้องการจากผู้ใช้ (ผู้ดูแลระบบ) โดยเน้นการตั้งค่าเครือข่ายอัตโนมัติและการตรวจสอบความปลอดภัยการตั้งค่าของอุปกรณ์
* วางแผนฟังก์ชันการทำงานที่เว็บแอปพลิเคชันต้องมี เช่น การตั้งค่าอุปกรณ์เครือข่าย การเก็บข้อมูล และการแจ้งช่องโหว่ของอุปกรณ์ การแสดงรายละเอียดของอุปกรณ์
  + 1. ออกแบบสถาปัตยกรรมระบบ



**ภาพที่ 1** กระบวนการทำงานของโปรแกรม

* ออกแบบโครงสร้างระบบ โดยใช้ Flask เป็น Web Framework สำหรับ Backend และจัดการกับการเชื่อมต่ออุปกรณ์เครือข่าย
* วางแผนการเชื่อมต่อกับอุปกรณ์เครือข่ายผ่านโปรโตคอลต่างๆ เช่น SSH โดยใช้ไลบรารีที่รองรับ เช่น paramiko
* ออกแบบการเก็บข้อมูลอุปกรณ์เครือข่ายเบื้องต้นในรูปแบบระบบฐานข้อมูล (NoSQL) เพื่อเก็บค่าตั้งต้นของอุปกรณ์ เช่น Hostname, IP, SSH settings ฯลฯ
* ออกแบบ UI/UX สำหรับเว็บแอปพลิเคชันที่ใช้งานง่าย โดยให้ผู้ใช้สามารถเข้าถึงและตั้งค่าเครือข่ายได้อย่างสะดวกผ่านหน้าเว็บ
  + 1. เลือกเครื่องมือและเทคโนโลยี
* ใช้ Python เป็น Programming Language หลักในการพัฒนาโปรแกรม
* ใช้ Flask เป็น Framework หลักในการพัฒนาเว็บแอปพลิเคชัน
* ใช้ไฟล์ MongoDB ในการเก็บข้อมูลเบื้องต้นของอุปกรณ์เครือข่าย เช่น IP Address, Hostname และการตั้งค่าอื่นๆ
* ใช้ EVE-NG ในการจำลองอุปกรณ์เครือข่ายจริง เพื่อทดสอบการทำงานของเว็บแอปพลิเคชัน
* ใช้อุปกรณ์จริงในบางกรณีเพื่อทำการทดสอบ
* พัฒนา AI Model สำหรับการตรวจสอบช่องโหว่ของการตั้งค่าเครือข่ายและวิเคราะห์ที่ผิดปกติ
* ใช้ JavaScript สำหรับการดึงข้อมูลของอุปกรณ์ผ่านโปรโตคอล SNMP
  + 1. พัฒนาเว็บแอปพลิเคชัน



**ภาพที่ 2** หน้าการเตรียมอุปกรณ์ให้พร้อมใช้งาน

A screenshot of a computer

Description automatically generated

**ภาพที่ 3** หน้าการจัดการบันทึกอุปกรณ์

A screenshot of a computer

Description automatically generated

**ภาพที่ 4** หน้าข้อมูลอุปกรณ์

A screenshot of a computer

Description automatically generated

**ภาพที่ 5** แสดงหัวข้อย่อยการตั้งค่าอุปกรณ์

A screenshot of a login screen

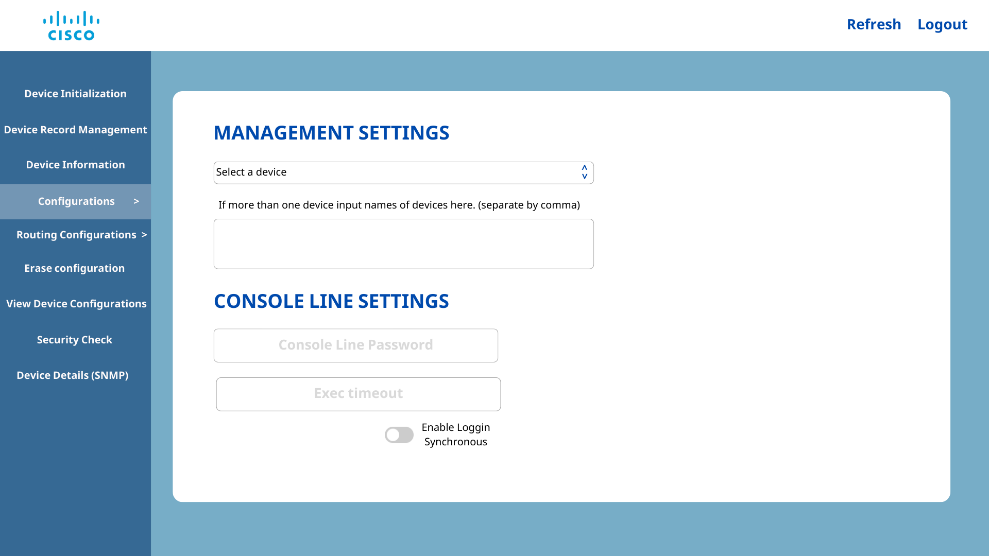
Description automatically generated

**ภาพที่ 6** หน้าการตั้งค่าเบื้องต้น

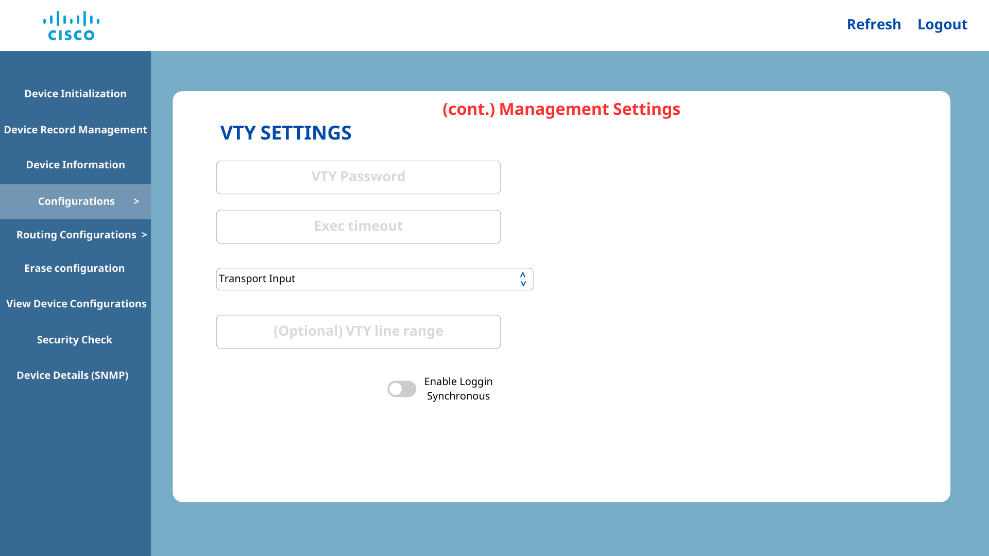
A screen shot of a computer

Description automatically generated

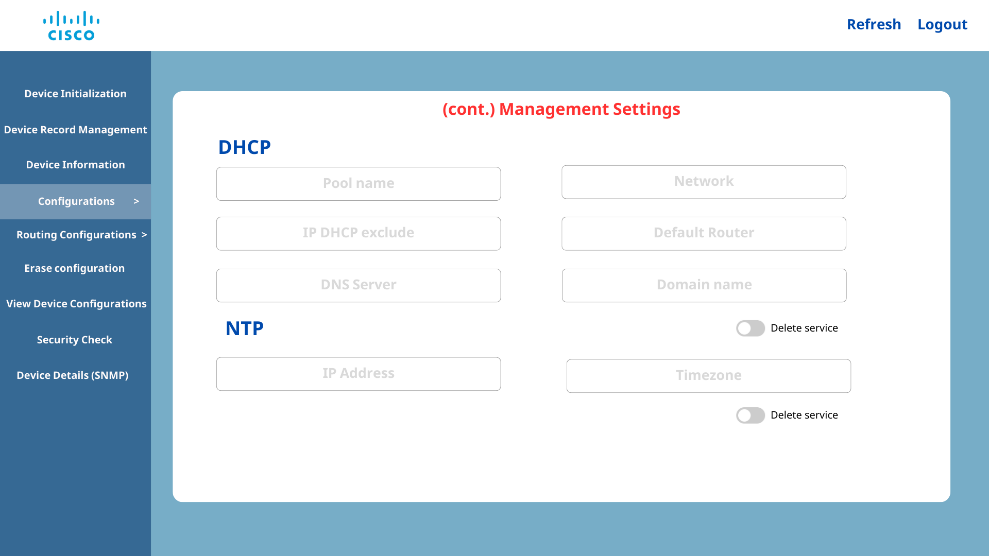
**ภาพที่ 7** หน้าการกำหนดค่าช่องสัญญาณเครือข่าย



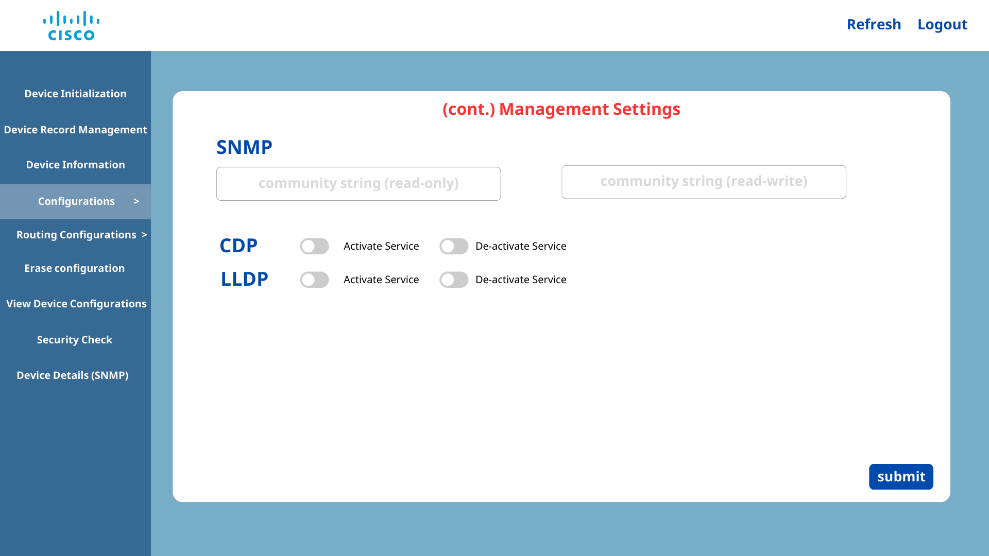
**ภาพที่ 8** หน้าการตั้งค่าการบริหารจัดการ



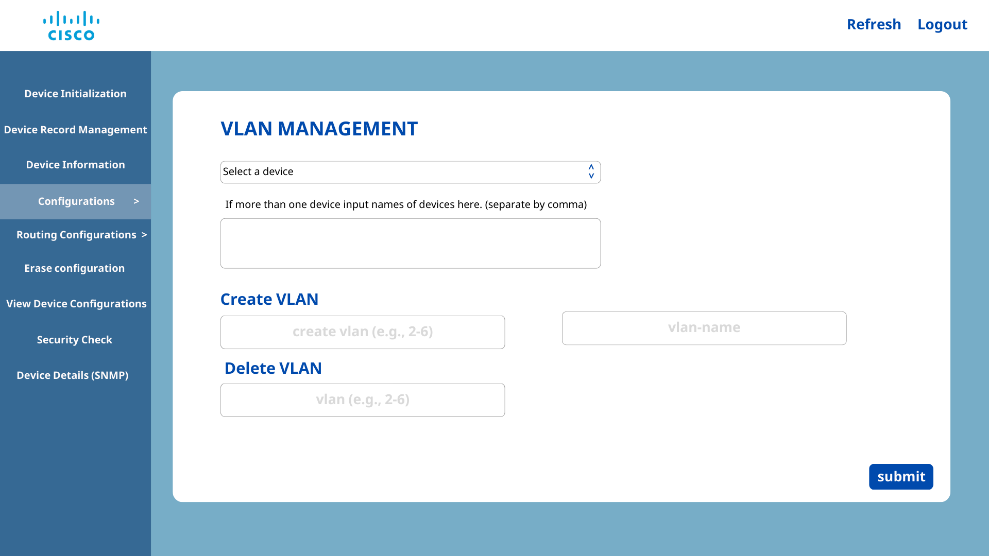
**ภาพที่ 9** หน้าการตั้งค่า VTY (ต่อ)



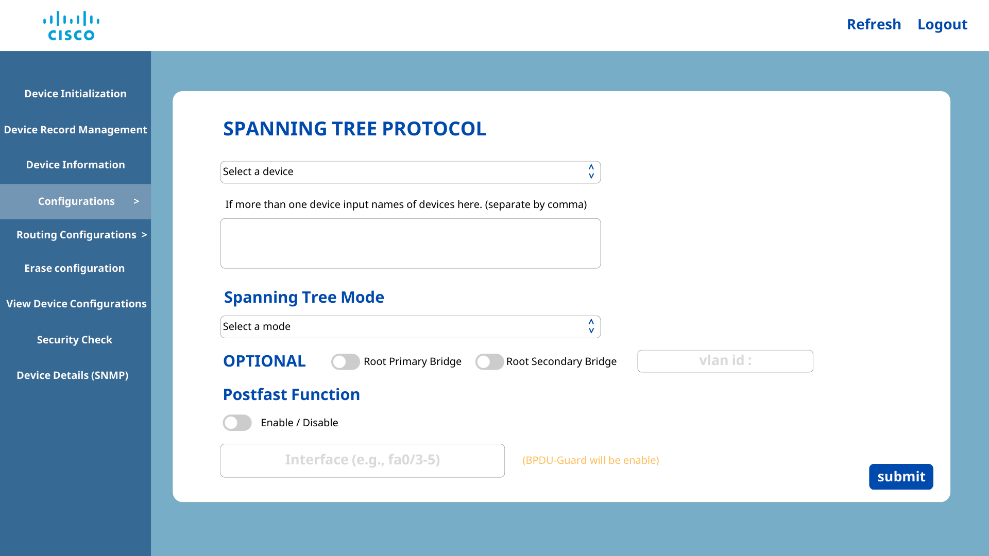
**ภาพที่ 10** หน้าการตั้งค่า DHCP และ NTP (ต่อ)



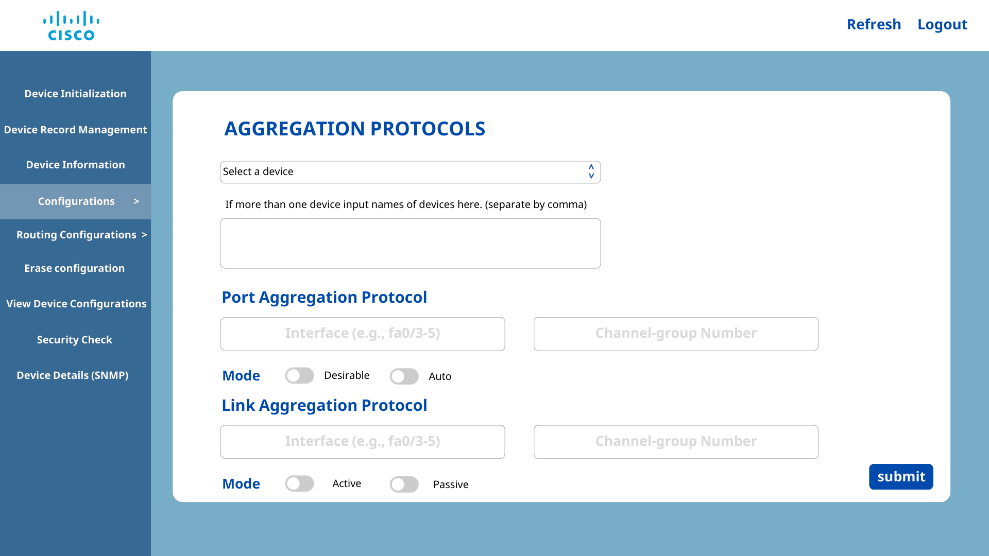
**ภาพที่ 10** หน้าการตั้งค่า SNMP, CDP, และ LLDP (ต่อ)



**ภาพที่ 11** หน้าการจัดการเครือข่ายเสมือน (VLAN)



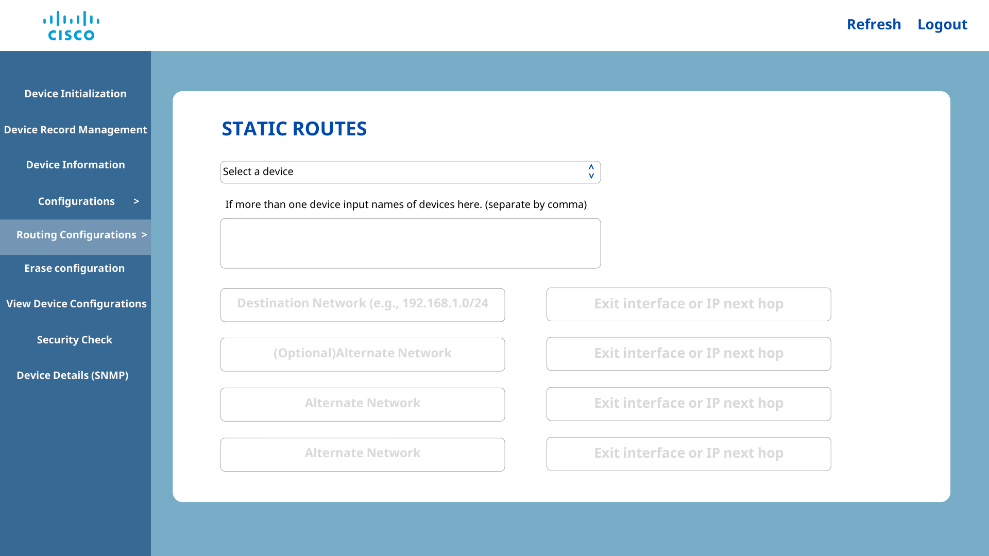
**ภาพที่ 12** หน้าการกำหนดค่าโปรโตคอล Spanning Tree



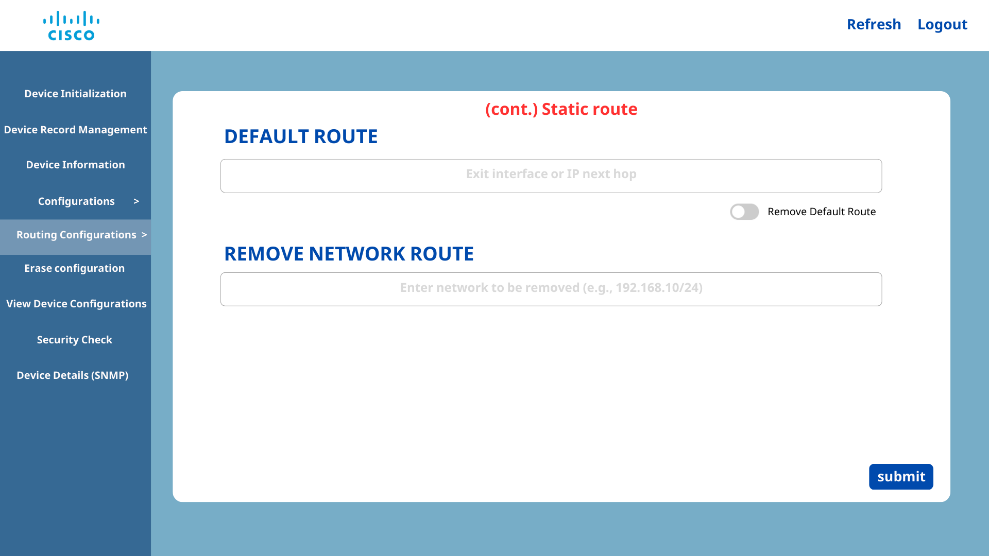
**ภาพที่ 13** หน้าการกำหนดค่าโปรโตคอลการรวมกลุ่ม



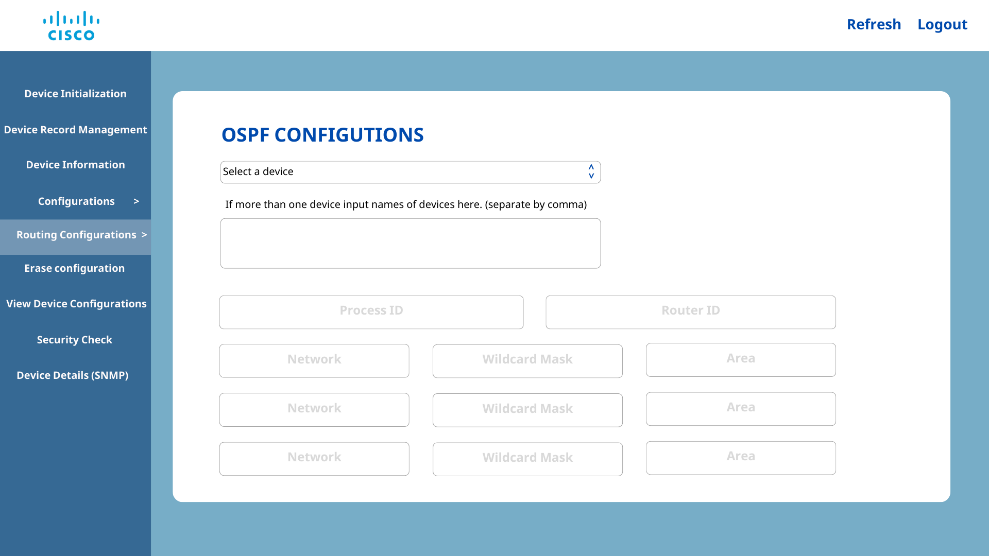
**ภาพที่ 14** หน้าแสดงหัวข้อย่อยการตั้งค่ากำหนดเส้นทางอุปกรณ์



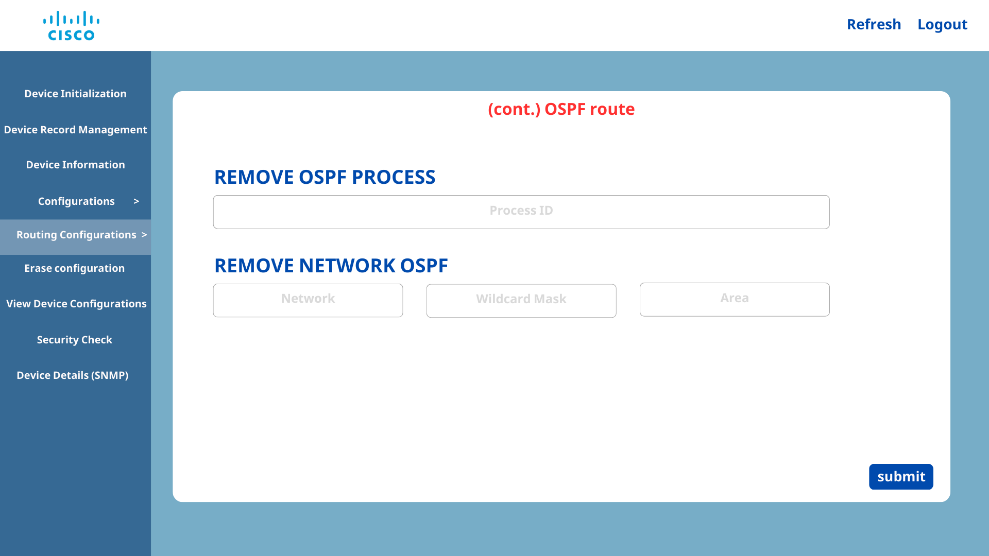
**ภาพที่ 15** หน้ากำหนดเส้นทางแบบ static route



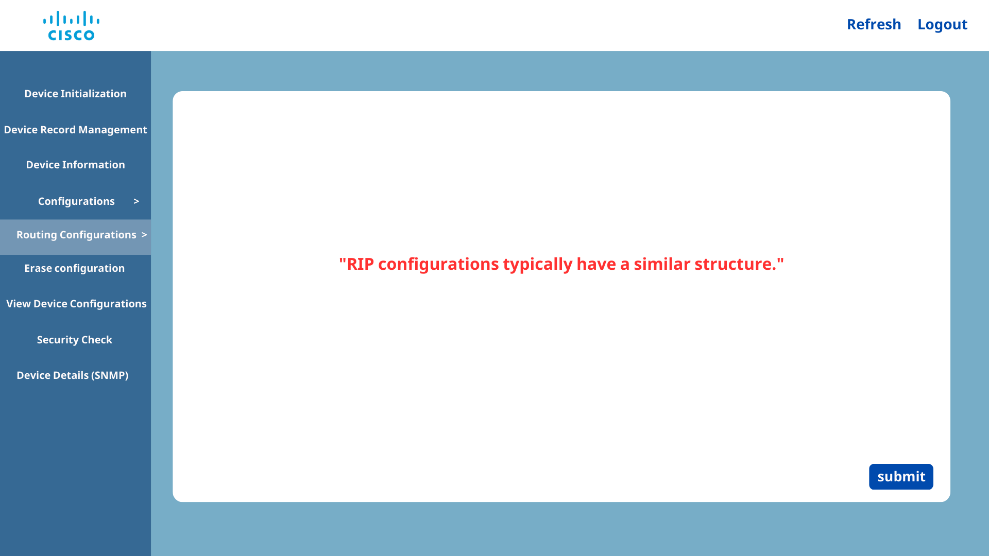
**ภาพที่ 16** หน้ากำหนดเส้นทางแบบ static route (ต่อ)



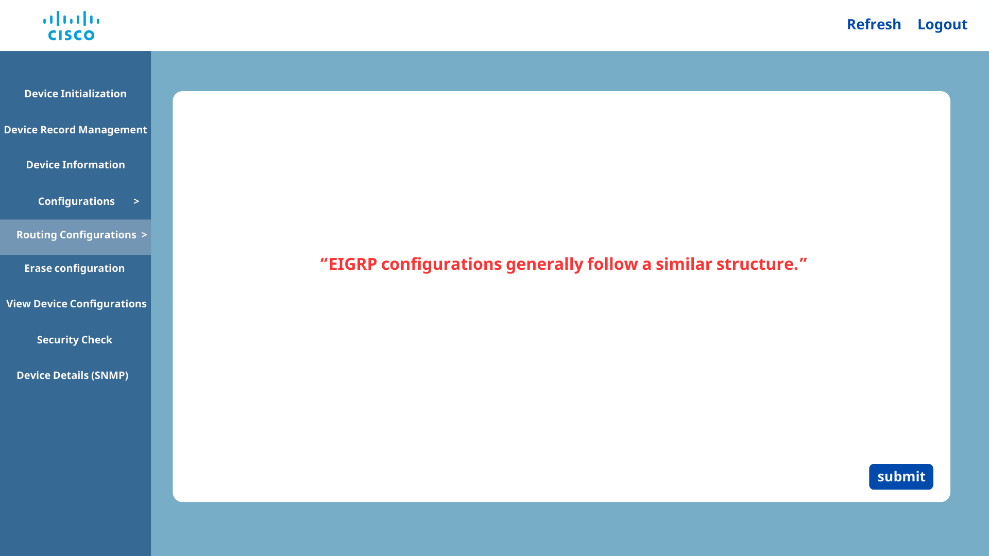
**ภาพที่ 17** หน้ากำหนดเส้นทางแบบ Dynamic Routing (OSPF)



**ภาพที่ 18** หน้ากำหนดเส้นทางแบบ Dynamic Routing (OSPF) (ต่อ)



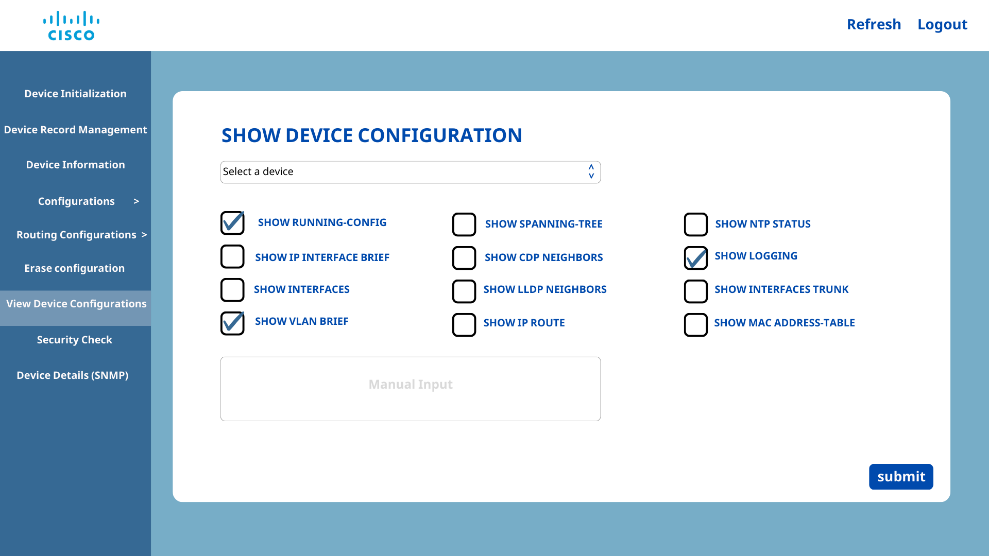
**ภาพที่ 19** หน้ากำหนดเส้นทางแบบ Dynamic Routing (RIPv2)



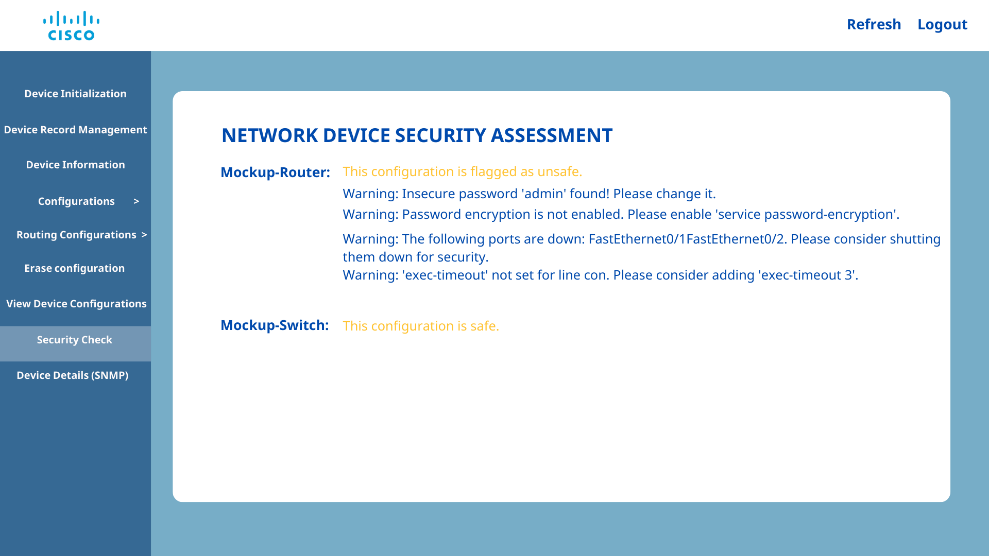
**ภาพที่ 20** หน้ากำหนดเส้นทางแบบ Dynamic Routing (EIGRP)



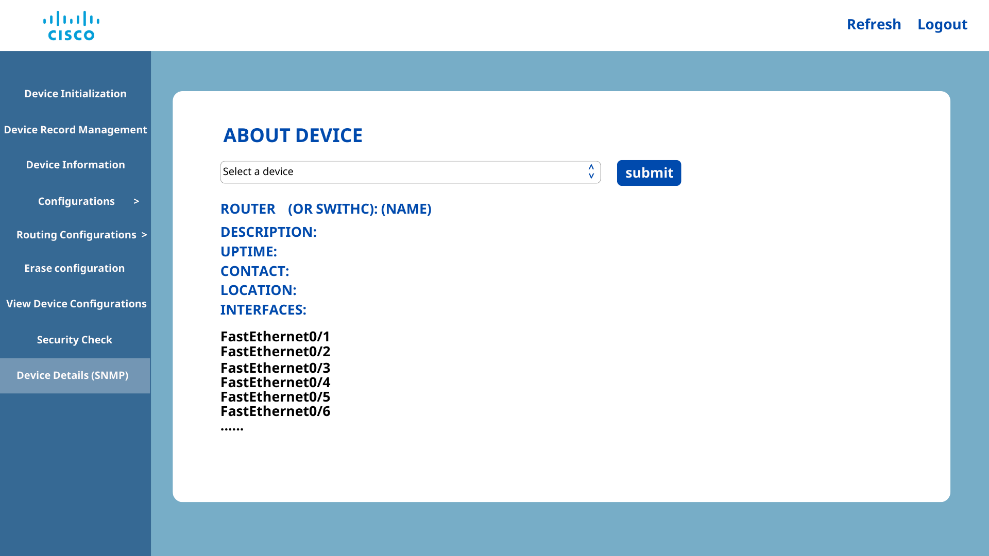
**ภาพที่ 21** หน้าการรีเซ็ตการตั้งค่าอุปกรณ์



**ภาพที่ 22** หน้าดึงข้อมูลแสดงการตั้งค่าของอุปกรณ์ ณ ขณะนั้น



**ภาพที่ 23** หน้าแสดงข้อมูลช่องโหว่ของการกำหนดค่าของอุปกรณ์



**ภาพที่ 24** หน้าแสดงข้อมูลเบื้องต้นนั้นๆของอุปกรณ์

* เริ่มการพัฒนาเว็บแอปพลิเคชันโดยใช้ Flask ในการจัดการและการเชื่อมต่ออุปกรณ์เครือข่าย
* พัฒนาฟังก์ชันการเชื่อมต่อกับอุปกรณ์ในการตั้งค่าอุปกรณ์เครือข่ายที่ยังไม่ได้ตั้งค่า ด้วยไลบรารี Serialของ Python พร้อมทั้งออกแบบหน้า Web Interface
* พัฒนาฟังก์ชันการเชื่อมต่อกับอุปกรณ์เครือข่ายผ่าน SSH โดยใช้ไลบรารี paramiko เพื่อดำเนินการตั้งค่าเครือข่าย
* พัฒนาโมเดลสำหรับการตรวจสอบความปลอดภัยโดยใช้ปัญญาประดิษฐ์เพื่อตรวจจับช่องโหว่และความผิดปกติ
* สร้างระบบการเก็บข้อมูลอุปกรณ์และใช้ข้อมูลเหล่านี้ในการตั้งค่าและตรวจสอบสถานะของอุปกรณ์
* สร้างระบบการดึงข้อมูลโดยโปรโตคอล SNMP ด้วย JavaScript
  + 1. ทดสอบการทำงานของระบบ
* ทดสอบเว็บแอปพลิเคชันกับอุปกรณ์เครือข่ายจำลองใน EVE-NG เพื่อทดสอบการตั้งค่าเครือข่ายหลายตัวพร้อมกัน
* ทดสอบการทำงานของปัญญาประดิษฐ์ในการตรวจจับปัญหาความปลอดภัยและการแจ้งเตือน
* ตรวจสอบการทำงานของระบบในการเก็บข้อมูลจากอุปกรณ์และการตั้งค่า
* ตรวจสอบการดึงข้อมูลที่ใช้ SNMP ที่ถูกต้อง
  + 1. ปรับปรุงและพัฒนาเพิ่มเติม
    2. จัดทำรูปเล่มปริญญานิพนธ์
  1. **แผนกิจกรรมและตารางเวลาในการจัดทำ**
     1. แผนกิจกรรมหลักและระยะเวลา

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ขั้นตอนการดำเนินงาน | ภาคการศึกษาที่ 2/2567 | | | | | | | | | | | | | | | |
| ธันวาคม | | | | มกราคม | | | | กุมภาพันธ์ | | | | มีนาคม | | | |
| 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| 1. วิเคราะห์ปัญหาและความต้องการ |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2. ออกแบบสถาปัตยกรรมระบบ |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3. เลือกเครื่องมือและเทคโนโลยี |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4. พัฒนาเว็บแอปพลิเคชัน |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5. ทดสอบการทำงานของระบบ |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 6. ปรับปรุงและพัฒนาเพิ่มเติม |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 7. จัดทำรูปเล่มปริญญานิพนธ์ |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

* 1. **ทรัพยากรที่ต้องใช้ในการจัดทำโครงงานพิเศษ**
     1. **เครื่องมือในการจัดทำโครงงานพิเศษ**
        1. **ด้านฮาร์ดแวร์**
           1. คอมพิวเตอร์ส่วนบุคคล (PC) หรือ Laptop
           2. เครือข่ายภายใน (LAN)

ระบบเครือข่ายภายในที่ใช้เชื่อมต่อและทดสอบการทำงานของระบบโดยตรง เพื่อเชื่อมต่ออุปกรณ์เสมือนใน EVE-NG หรืออุปกรณ์เครือข่ายจริง เช่น router, switch

* + - * 1. EVE-NG Server

ระบบจำลองเครือข่ายที่ใช้ในการสร้างสภาพแวดล้อมเสมือนจริงในการตั้งค่าและทดสอบการทำงานของอุปกรณ์เครือข่าย

* + - * 1. อุปกรณ์เครือข่ายจริง (ถ้ามี)

อุปกรณ์เครือข่าย เช่น Router, Switch, หรืออุปกรณ์อื่นๆ ที่เกี่ยวข้อง เพื่อใช้ในการทดสอบการตั้งค่าเครือข่ายผ่านระบบจริง

* + - 1. **ด้านซอฟต์แวร์**
         1. Flask

Framework สำหรับพัฒนาเว็บแอปพลิเคชันในฝั่ง Backend รองรับการเชื่อมต่อกับอุปกรณ์เครือข่ายและการทำงานร่วมกับ API ต่างๆ

* + - * 1. Python

ภาษาโปรแกรมหลักในการพัฒนาโมดูลปัญญาประดิษฐ์และการประมวลผลเครือข่าย รองรับการทำงานของ Flask และการเชื่อมต่อกับอุปกรณ์เครือข่ายผ่าน SSH

* + - * 1. Paramiko

ไลบรารี Python ที่ใช้สำหรับเชื่อมต่อกับอุปกรณ์เครือข่ายผ่าน SSH เพื่อจัดการการตั้งค่าและสั่งงานระยะไกล

ไลบรารี JavaScript ที่ใช้สำหรับโปรโตคอล SNMP สำหรับการดึงค่ารายละเอียดของอุปกรณ์

* + - * 1. EVE-NG

ซอฟต์แวร์จำลองการทำงานของอุปกรณ์เครือข่ายในสภาพแวดล้อมเสมือนจริง รองรับการตั้งค่าเครือข่ายหลายแบบ

* + - * 1. Visual Studio Code

Text Editor สำหรับการเขียนโปรแกรม รองรับการทำงานร่วมกับ Flask, Python, และไฟล์ JSON ที่ใช้ในการเก็บข้อมูล

* + - * 1. Docker (ถ้ามี)

เครื่องมือสำหรับสร้างและจำลองสภาพแวดล้อมการพัฒนาและทดสอบในระบบปฏิบัติการที่แยกออกจากระบบหลัก ช่วยให้การทดสอบโปรแกรมมีความเสถียรและควบคุมสภาพแวดล้อม

* + - * 1. MongoDB

ใช้จัดเก็บข้อมูลของอุปกรณ์ที่จะใช้ในการจัดการของเว็บแอปพลิเคชัน

* + - * 1. JavaScript

ใช้ไลบรารีสำหรับของการดึงค่าของอุปกรณ์ผ่าน SNMP

* + 1. งบประมาณที่ใช้ในการจัดทำ
* ค่าปริญญานิพนธ์ 3,000 บาท
* ค่าใช้จ่ายเพิ่มเติม 1,000 บาท
* รวม 4,000 บาท
  1. **ผลที่คาดว่าจะได้รับ**
     1. ทำให้ผู้ดูแลระบบสามารถตั้งค่าเริ่มต้นอุปกรณ์ได้จริง
     2. ทำให้ผู้ดูแลระบบสามารถทำการตั้งค่าอุปกรณ์เครือข่ายได้หลายตัวพร้อมกัน และสามารถตรวจสอบการตั้งค่าของอุปกรณ์ได้จริง
     3. ทำให้ผู้ดูแลระบบสามารถตรวจสอบความปลอดภัยเกี่ยวกับการตั้งค่าของอุปกรณ์ได้จริง
  2. **เอกสารอ้างอิง**

Karsten Iwen (2557) Guide to better SSH-Security [สืบค้นเมื่อ 29 กันยายน 2567]. [ออนไลน์].

<https://community.cisco.com/t5/security-knowledge-base/guide-to-better-ssh-security/ta-p/3133344>

Thanachart Ritbumroong (2561) TensorFlow ฉบับมือใหม่ โดยใช้ Python [สืบค้นเมื่อ 29 กันยายน 2567]. [ออนไลน์].

<https://thanachart-rit.medium.com/tensorflow-%E0%B8%89%E0%B8%9A%E0%B8%B1%E0%B8%9A%E0%B8%A1%E0%B8%B7%E0%B8%AD%E0%B9%83%E0%B8%AB%E0%B8%A1%E0%B9%88-%E0%B9%82%E0%B8%94%E0%B8%A2%E0%B9%83%E0%B8%8A%E0%B9%89-python-784ba3df5bc4>

ZoDae MaCoM (2563) ทำความรู้จักกับ Netmiko [สืบค้นเมื่อ 29 กันยายน 2567]. [ออนไลน์].

<https://medium.com/@patasia54962/%E0%B8%97%E0%B8%B3%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1%E0%B8%A3%E0%B8%B9%E0%B9%89%E0%B8%88%E0%B8%B1%E0%B8%81%E0%B8%81%E0%B8%B1%E0%B8%9A-netmiko-2ca1661c9842>

Withoutcoffee Icantbedev (2567) พัฒนาเว็บด้วยภาษา Python (Flask) สำหรับผู้เริ่มต้น ฉบับเต็มปี 2024 [สืบค้นเมื่อ 29 กันยายน 2567]. [ออนไลน์].

<https://devhub.in.th/blog/flask-python>

ลงชื่อ ผู้เสนอโครงงาน

( )

วันที่ยื่นเสนอโครงงาน / /

ความคิดเห็นอาจารย์ที่ปรึกษาโครงงาน

ลงชื่อ อาจารย์ที่ปรึกษา

( )

วันที่ / /

สาขาวิชา / ภาควิชาที่ได้รับแบบเสนอโครงงานวันที่

ผลการพิจารณา

ลงชื่อ ประธาน

( )

วันที่ / /

ลงชื่อ กรรมการ

( )

วันที่ / /

ลงชื่อ กรรมการ

( )

วันที่ / /