คู่มือการดูแลและการเชื่อมต่อระบบเครือข่ายหลัก มหาวิทยาลัยเชียงใหม่ (CMU-NET)

นวิน ธรรมรักษ์
วิศวกร

สำนักบริการเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเชียงใหม่

คำนำ

ฝ่ายโครงสร้างเทคโนโลยีสารสนเทศ และทีม Network สำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่ ได้ดำเนินการจัดทำคู่มือปฏิบัติงานในการดูแล และเชื่อมต่อระบบเครือข่ายหลัก (CMU-NET) เข้ากับหน่วยงานที่รับบริการภายในมหาวิทยาลัยเชียงใหม่ เพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงานในฝ่าย มีความเข้าใจในระบบเครือข่ายหลัก สามารถนำไปใช้ประกอบการปฏิบัติงานให้เกิดประสิทธิภาพ และเป็นไปในแนวทางเดียวกัน อีกทั้งสามารถช่วยเหลือหน่วยงานที่ขอรับบริการในการเชื่อมต่อระบบเครือข่ายได้อย่างถูกต้องอีกด้วย

ทางผู้จัดทำหวังเป็นอย่างยิ่งว่า คู่มือฉบับนี้จะเป็นประโยชน์แก่ผู้ปฏิบัติงานในการดูแลรักษาระบบเครือข่ายหลักของมหาวิทยาลับเชียงใหม่ และผู้ที่เกี่ยวข้องนำไปช่วยในการปฏิบัติงานได้อย่างถูกต้องและมีประสิทธิภาพ หากคู่มือฉบับนี้มีข้อผิดพลาดประการใด ทางผู้จัดทำขออภัยมา ณ ที่นี้ด้วย

นวิน ธรรมรักษ์
สำนักบริการเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเชียงใหม่
กันยายน 2565

สารบัญ

หน้า

คำนำ ..... ข

สารบัญตาราง ..... จ

สารบัญภาพ ..... ฉ

บทที่ 1 1

1.1 ความเป็นมาและความสำคัญของปัญหา 1
1.2 วัตถุประสงค์ของคู่มือ 3
1.3 ประโยชน์ที่คาดว่าจะได้รับ 3
1.4 ขอบเขต 3
1.5 คำศัพท์เฉพาะ 3

บทที่ 2 โครงสร้างและหน้าที่รับผิดชอบ 5

2.1 ความเป็นมาของหน่วยงาน 5
2.2 วิสัยทัศน์ 5
2.3 เป้าหมาย 5
2.4 พันธกิจ 5
2.5 ค่านิยม 6
2.6 ยุทธศาสตร์สำนักบริการเทคโนโลยีสารสนเทศ ประกอบด้วย 6
2.7 โครงสร้างองค์กร (Organization Chart) 6
2.8 โครงสร้างการปฏิบัติงาน (Activity Chart) 7
2.9 บทบาทหน้าที่ความรับผิดชอบ 8

บทที่ 3 หลักการปฏิบัติงาน 9

3.1 แนวคิดและหลักการการออกแบบระบบเครือข่าย 9
3.2 หลักการทฤษฎีและมาตรฐานที่เกี่ยวกับระบบเครือข่าย 10
3.3 หมายเลข IP Address 14
3.4 อุปกรณ์สลับสัญญาณ Layer 3 16

สารบัญ (ต่อ)

หน้า

บทที่ 4 เทคนิคในการปฏิบัติงาน 18

4.1 การออกแบบระบบเครือข่ายหลักมหาวิทยาลัยเชียงใหม่ 18

4.2 การติดตั้งอุปกรณ์ Switch Layer 3 ให้กับหน่วยงาน 24

บทที่ 5 ปัญหาและแนวทางการแก้ไข 34

สารบัญตาราง

หน้า

ตารางที่ 1 ตารางการแบ่ง Subnet แบบตรง Octet 15
ตารางที่ 2 การแบ่ง Subnet แบบยืมส่วนของ Host 16
ตารางที่ 3 Private IP Address ของชุด 10.0.0.0/8 22
ตารางที่ 4 ตารางแบ่ง subnet สำรองไว้ให้บริการของทาง ITSC 23
ตารางที่ 5 ตาราง IP Point to Point เพื่อทำ Routing 23
ตารางที่ 6 ตารางการแบ่ง Private IP Address ของชุด 172.16.0.0/12 23
ตารางที่ 7 ตารางการแบ่ง Private IP Address ของ ชุด 192.168.0.0/20 24

สารบัญภาพ

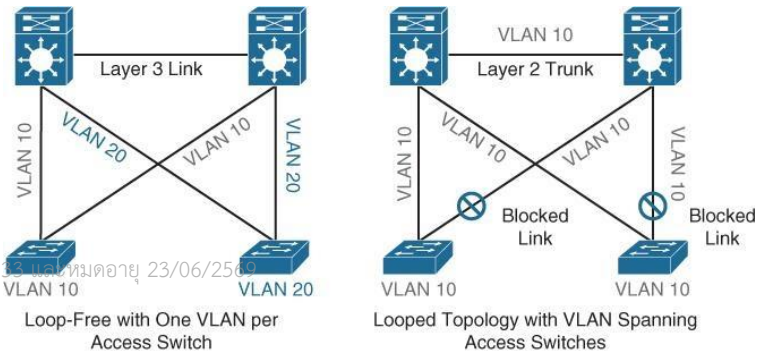
หน้า

ภาพที่ 1 การเชื่อมต่อที่ไม่มีการเกิด Loop และมีการเกิด Loop บนอุปกรณ์สลับสัญญาณ.....1
ภาพที่ 2 การเชื่อมต่อโดยใช้อุปกรณ์สลับสัญญาณแบบ Layer 2 และ Layer 3.....2
ภาพที่ 3 แผนผังองค์กร (Organization Chart).....6
ภาพที่ 4 แผนผังการปฏิบัติงาน.....7
ภาพที่ 5 Enterprise Network Architecture Model.....9
ภาพที่ 6 การออกแบบระบบเครือข่ายแบบลำดับขั้น (Hierarchical Model).....10
ภาพที่ 7 Routing Table ผ่านทาง terminal.....11
ภาพที่ 8 ข้อมูลบน Routing Table.....12
ภาพที่ 9 Stub Network.....13
ภาพที่ 10 ภาพแสดง Network Layer จาก OSI 7 Layer Model.....14
ภาพที่ 11 การแบ่งส่วนใช้งานของหมายเลขไอพี.....15
ภาพที่ 12 Cisco Catalyst 9500-32C.....17
ภาพที่ 13 Cisco Catalyst 9500-32C.....17
ภาพที่ 14 Cisco Catalyst 9500-24T.....17
ภาพที่ 15 แผนผัง CMU-NET 2020.....18
ภาพที่ 16 ห้อง Data Center , ITSC.....19
ภาพที่ 17 แผนผังการดำเนินงานติดตั้งอุปกรณ์สลับสัญญาณ.....25
ภาพที่ 18 แผนผังการเชื่อมต่อ Switch Access Layer เข้ากับ Switch Distribution Layer.....31
ภาพที่ 19 แผนผังการเชื่อมต่อระดับ Layer 3 ไปยังหน่วยงาน.....32

บทที่ 1
บทนำ

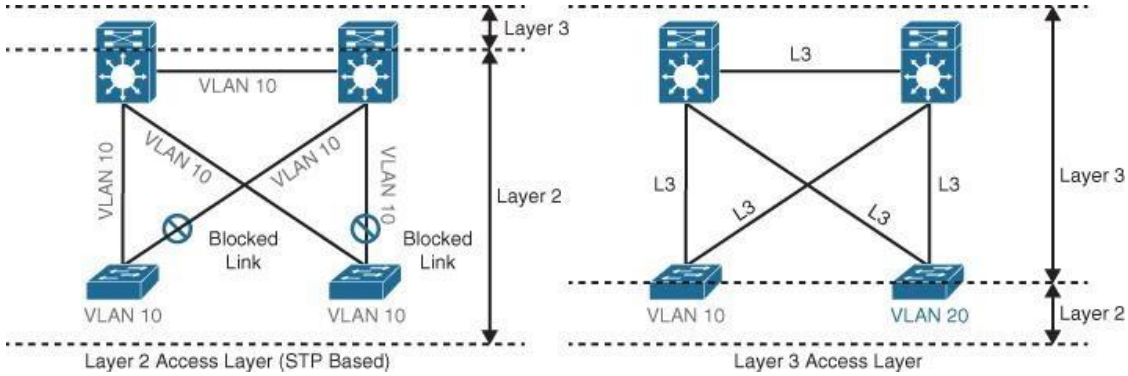
1.1 ความเป็นมาและความสำคัญของปัญหา

ในปีพ.ศ. 2563 ทางสำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่ได้มีโครงการปรับปรุงระบบเครือข่ายหลักภายใต้ชื่อ CMU-NET2020 จากการออกแบบและเชื่อมต่อแบบเดิมที่มีการใช้งานมากว่า 15 ปีที่เป็นรูปแบบของ VLAN based (Layer 2) ซึ่งการเชื่อมต่อในลักษณะนี้ ในช่วงที่เริ่มต้นเป็นรูปแบบที่นิยม เนื่องจากอุปกรณ์มีราคาไม่สูง สามารถดูแลได้สะดวก ประหยัดทรัพยากรของอุปกรณ์ในการประมวลผล และควบคุมได้ง่าย ประกอบกับมีความซับซ้อนไม่มาก ทำให้ผู้ดูแลระบบต่างเลือกใช้วิธีการนี้ในการติดตั้งและใช้งานมาอย่างยาวนาน แต่เมื่อเวลาผ่านไป มหาวิทยาลัยเชียงใหม่ได้มีความต้องการในการเข้าถึงระบบเครือข่ายมากขึ้น เพื่อรองรับการเรียนการสอนและการค้นคว้าวิจัย ทำให้มีการเพิ่มจำนวนของอุปกรณ์สลับสัญญาณ (Switch) และอุปกรณ์ที่เข้ามาเชื่อมต่อกับระบบเครือข่ายหลักมากขึ้น นำไปสู่การเพิ่มจำนวนของ VLAN บนอุปกรณ์สลับสัญญาณในระบบมากขึ้น นอกจากนี้ หลายหน่วยงานมีการขยายสาขาการให้บริการเพิ่มขึ้นไปยังที่ต่าง ๆ ทั้งภายในเขตมหาวิทยาลัยเชียงใหม่ สวนดอก และแม่เหียะ ด้วยเหตุนี้เมื่อปริมาณ VLAN ในระบบสูงขึ้น การดูแลเชื่อมต่อ VLAN จึงซับซ้อนมากขึ้น ทั้งนี้เพราะการเชื่อมต่อในระดับ Layer 2 (Data Link Layer) หรือ VLAN based จำเป็นต้องระมัดระวังเรื่องของ Loop บน Layer 2 เมื่อเกิดขึ้นจะส่งผลกระทบกับระบบเครือข่ายทั้งระบบ ถึงแม้ว่าสาเหตุจะมาจากอุปกรณ์สลับสัญญาณเพียงตัวเดียว แม้ว่าตัวอุปกรณ์สลับสัญญาณเองจะมี Spanning Tree Protocol ที่จัดการปิดกั้นเส้นทางที่เกิด Loop โดยอัตโนมัติอยู่ แต่ด้วยการเชื่อมต่อที่ซับซ้อนกว่านับร้อย VLAN และมีอุปกรณ์ที่หลากหลาย การเกิดปัญหาเช่นนี้สามารถเกิดขึ้นได้ทุกเมื่อ



ภาพที่ 1 การเชื่อมต่อที่ไม่มีการเกิด Loop และมีการเกิด Loop บนอุปกรณ์สลับสัญญาณ

ดังนั้น เพื่อแก้ไขปัญหาดังกล่าวจึงได้มีการพิจารณาถึงวิธีการออกแบบที่มีการเชื่อมต่อแบบในรูปแบบ IP based (Layer 3) ประกอบกับช่วงเวลาปัจจุบัน อุปกรณ์สลับสัญญาณแบบทำงานหลาย Layer (Multilayer Switch) นั้นมีราคาที่ลดลง และมีประสิทธิภาพสูงขึ้น ทำให้การเชื่อมต่อในลักษณะนี้ได้รับความสนใจมากขึ้น โดยทางสำนักบริการเทคโนโลยีสารสนเทศ ภายใต้ความรับผิดชอบของฝ่ายโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ ได้นำมาใช้ในการปรับปรุงระบบเครือข่ายหลักของมหาวิทยาลัยเชียงใหม่ โดยนำอุปกรณ์สลับสัญญาณแบบทำงานหลาย Layer มาเปลี่ยนทดแทนในส่วนของส่วนหลัก (Core Layer), ส่วนกระจาย (Distribution Layer) และส่วนเชื่อมต่อ (Access Layer) ทำให้ระบบการเชื่อมต่อภายในเครือข่ายหลักนั้นเปลี่ยนจากรูปแบบ VLAN based เป็น IP based ซึ่งใช้ Routing Protocol เข้ามาจัดการการรับส่งข้อมูลแทน VLAN การใช้งานหมายเลขไอพี (IP Address) จึงต้องมีการจัดสรรอย่างเป็นระบบและถูกต้อง รวมถึงการเปลี่ยนเส้นทางของการเชื่อมต่ออุปกรณ์สลับสัญญาณให้มีประสิทธิภาพยิ่งขึ้น



ภาพที่ 2 การเชื่อมต่อโดยใช้อุปกรณ์สลับสัญญาณแบบ Layer 2 และ Layer 3

จากการเปลี่ยนแปลงที่กล่าวมาข้างต้น ส่งผลกระทบโดยตรงแก่ผู้รับบริการระบบเครือข่ายหลักนั้นคือ คณะ และหน่วยงานต่าง ๆ ภายในมหาวิทยาลัยเชียงใหม่ที่ต้องดำเนินการปรับเปลี่ยนรูปแบบการเชื่อมต่อของหน่วยงานเองให้สามารถเข้ากับระบบใหม่นี้ เพื่อให้สามารถใช้งานได้อย่างเต็มประสิทธิภาพ ปลอดภัย และรวดเร็วต่อการแก้ไขปัญหา กระบวนการทำงานของทีมงานจึงแตกต่างไปจากเดิมอย่างเห็นได้ชัด เพื่อให้ผู้ปฏิบัติงานสามารถควบคุมดูแลระบบ ประสานงานกับผู้ดูแลระบบของหน่วยงานต่าง ๆ เพื่อแก้ไขปัญหาได้อย่างรวดเร็ว

นอกจากนี้ระบบเครือข่ายหลักของมหาวิทยาลัยเป็นระบบเครือข่ายขนาดใหญ่ ซึ่งมีความซับซ้อนตั้งแต่โครงสร้างพื้นฐานเลเยอร์ล่างสุด ได้แก่ Physical Layer จนมาถึงการจัดการในส่วนของเครือข่ายที่ใช้งานบน Network Layer ที่จำเป็นต้องมีการออกแบบ IP และ Routing Protocol ต่าง ๆ ให้เหมาะสมกับการใช้งาน ซึ่งต้องอาศัยผู้ที่มีความเชี่ยวชาญสูงที่มาดูแลระบบดังกล่าว ดังนั้นจึงสมควรที่จะจัดทำคู่มือการดูแลและการเชื่อมต่อระบบเครือข่ายหลัก มหาวิทยาลัยเชียงใหม่ ที่แสดงถึงรายละเอียดขั้นตอนการปฏิบัติงานของกิจกรรมหรือกระบวนการต่าง ๆ และสร้างมาตรฐานการปฏิบัติงานที่มุ่งไปสู่การบริหารคุณภาพทั่วทั้งองค์กรอย่างมีประสิทธิภาพ และมีระบบเครือข่ายที่มีคุณภาพตามมาตรฐาน

ISO27001 ตลอดจนแสดงวิธีการทำงาน ซึ่งสามารถถ่ายทอดให้กับผู้เข้ามาปฏิบัติงานใหม่ พัฒนาให้การทำงานเป็นมืออาชีพ และใช้ประกอบการประเมินผลการปฏิบัติงานของบุคลากร รวมทั้งแสดงหรือเผยแพร่ให้กับผู้ดูแลระบบเครือข่ายในหน่วยงานต่าง ๆ หรือบุคคลภายนอก หรือผู้ใช้บริการให้สามารถเข้าใจ และใช้ประโยชน์จากระบบเครือข่ายหลักของมหาวิทยาลัยเชียงใหม่ได้อย่างมีประสิทธิภาพและมีเสถียรภาพต่อไป

1.2 วัตถุประสงค์ของคู่มือ

1.2.1 เพื่อให้มีคู่มือการปฏิบัติงานที่ชัดเจนเป็นลายลักษณ์อักษรที่แสดงถึงรายละเอียดขั้นตอนการปฏิบัติงานในการดูแลระบบเครือข่ายหลัก มหาวิทยาลัยเชียงใหม่

1.2.2 เพื่อช่วยให้ผู้ดูแลระบบเครือข่ายหลักสามารถแก้ไขปัญหาที่เกิดขึ้นได้อย่างรวดเร็วและมีประสิทธิภาพ

1.3 ประโยชน์ที่คาดว่าจะได้รับ

1.3.1 ผู้ปฏิบัติงานมีความเข้าใจและสามารถดูแลระบบเครือข่ายหลักของมหาวิทยาลัยเชียงใหม่ได้อย่างถูกต้อง

1.3.2 ผู้ปฏิบัติงานสามารถประสานงานกับผู้ดูแลระบบเครือข่ายของหน่วยงานที่มาเชื่อมต่อระบบเครือข่ายได้อย่างถูกต้อง

1.3.3 ผู้ปฏิบัติงานสามารถปฏิบัติงานทดแทนกันได้ และแก้ไขปัญหาที่เกิดขึ้นได้อย่างรวดเร็ว

1.4 ขอบเขต

คู่มือการดูแลและการเชื่อมต่อระบบเครือข่ายหลักมหาวิทยาลัยเชียงใหม่ (CMU-NET) ใช้สำหรับการออกแบบระบบ การติดตั้ง การตั้งค่าอุปกรณ์ การบำรุงรักษา และแก้ไขปัญหาเมื่อมีการขัดข้องของระบบเครือข่ายหลัก มหาวิทยาลัยเชียงใหม่ ในอุปกรณ์ที่เชื่อมต่อเพื่อให้บริการกับคณะ หน่วยงาน ในระดับ Access Layer

1.5 คำศัพท์เฉพาะ

1.5.1 ระบบเครือข่าย (Network) หมายถึง การเชื่อมต่อคอมพิวเตอร์ตั้งแต่สองเครื่องขึ้นไป เพื่อรับส่งข้อมูลระหว่างกัน

1.5.2 อุปกรณ์สลับสัญญาณ (Switch) หมายถึง อุปกรณ์ในระบบเครือข่ายที่ใช้สายสัญญาณในการเชื่อมต่ออุปกรณ์อื่น ๆ ให้รับส่งข้อมูลกันภายในระบบเครือข่าย

1.5.3 อุปกรณ์สลับสัญญาณระดับเลเยอร์ 3 (Layered 3 Switch) หมายถึง อุปกรณ์สลับสัญญาณที่สามารถรับส่งข้อมูลภายในระบบเครือข่าย และรับส่งข้อมูลข้ามระบบเครือข่ายได้

1.5.4 สแปนนิง ทรี โปรโทคอล (Spanning Tree Protocol) หมายถึง ข้อตกลงบนอุปกรณ์สลับสัญญาณในการเชื่อมต่อกันไม่ให้เกิดลูปในระบบเครือข่าย

1.5.5 ลูป (Loop) หมายถึง การส่งข้อมูลกันในระบบเครือข่ายของอุปกรณ์สลับสัญญาณวนกลับไปมาจนทำให้เกิดเป็นข้อมูลจำนวนมหาศาลและทำให้อุปกรณ์ไม่สามารถทำงานได้

1.5.6 วีแลน (VLAN) หมายถึง การจำลองระบบเครือข่ายขึ้นมาภายในอุปกรณ์สลับสัญญาณตัวเดียวกัน เพื่อแยกการส่งข้อมูลออกจากกันกับระบบเครือข่ายอื่น ๆ ในอุปกรณ์สลับสัญญาณตัวนั้น

1.5.7 เราท์ติง โปรโทคอล (Routing Protocol) หมายถึง ข้อตกลงในอุปกรณ์ที่ทำการแลกเปลี่ยนข้อมูลเพื่อส่งข้อมูลข้ามระบบเครือข่ายหรือส่งข้อมูลไปยังปลายทางที่อยู่ในอินเทอร์เน็ต

1.5.8 เลขที่อยู่ไอพี (IP Address) หมายถึง ชุดตัวเลขที่ใช้ในการระบุระบบเครือข่ายและอุปกรณ์ที่อยู่ในระบบเครือข่าย เพื่อจัดกลุ่มออกเป็นชุด ให้ทราบว่าอยู่กลุ่มเดียวกันในการส่งข้อมูลหรืออยู่คนละกลุ่มกัน

1.5.9 การตั้งค่าอุปกรณ์ (Configuration) หมายถึง การปรับการตั้งค่าต่าง ๆ บนอุปกรณ์ เพื่อให้สามารถใช้งานได้ตามวัตถุประสงค์ที่ต้องการ

บทที่ 2
โครงสร้างและหน้าที่รับผิดชอบ

2.1 ความเป็นมาของหน่วยงาน

ตามที่มหาวิทยาลัยเชียงใหม่ ได้ก้าวสู่การเป็นมหาวิทยาลัยในกำกับอย่างเป็นทางการ เมื่อวันที่ 7 มีนาคม 2551 นั้น นับเป็นโอกาสในการรวมหน่วยงานเดิม 2 องค์กร คือ สำนักบริการคอมพิวเตอร์ที่ได้ดำเนินการมากว่า 25 ปี และสถานบริการเทคโนโลยีสารสนเทศ ซึ่งเป็นองค์กรในกำกับของมหาวิทยาลัยตั้งแต่ปี 2545 มารวมเข้าด้วยกันอย่างเป็นทางการ ภายใต้ชื่อ "สำนักบริการเทคโนโลยีสารสนเทศ" ตั้งแต่วันที่ 5 กรกฎาคม 2551 เป็นต้นมา

2.2 วิสัยทัศน์

เป็นศูนย์กลางของการให้บริการเทคโนโลยีสารสนเทศของมหาวิทยาลัยที่ได้รับการรับรองมาตรฐานสากล

2.3 เป้าหมาย

เป็นศูนย์กลางการให้บริการหลักที่ได้รับการรับรองมาตรฐาน

2.4 พันธกิจ

2.4.1 จัดให้มีระบบโครงสร้างพื้นฐานด้านไอทีเพื่อการเชื่อมต่อระบบเครือข่ายและการสื่อสารด้วยเทคโนโลยีที่ทันสมัย

2.4.2 พัฒนาระบบฐานข้อมูลและข้อมูลสารสนเทศเพื่อเพิ่มประสิทธิภาพของการบริหารจัดการและให้เป็นไปตามหลักธรรมาภิบาล

2.4.3 พัฒนาและส่งเสริมการใช้เทคโนโลยีสารสนเทศเพื่อสนับสนุนการเรียนรู้ในศตวรรษที่ 21 โดยบริหารงานเป็นไปตามหลักธรรมาภิบาล

2.5 ค่านิยม

I: Innovative เน้นความคิดที่แปลกใหม่ และสร้างสรรค์เพื่อพัฒนางาน และการเรียนรู้

T: Team-Driven การทำงานเป็นทีม ช่วยเหลือกัน เอื้อเฟื้อต่อกัน ร่วมมือ ร่วมใจและแก้ไขปัญหาในการทำงานอย่างเป็นระบบ และนำเทคโนโลยีใหม่มาประยุกต์ใช้ในการทำงาน

S: Service-Oriented เอาใจใส่การบริการต้องคำนึงถึงความพึงพอใจของลูกค้า และผู้มีส่วนได้ส่วนเสีย (Stakeholders) เป็นหลัก โดยใช้หลักธรรมาภิบาลในการทำงาน

C: Continuous Improvement การปรับปรุงด้วยระบบคุณภาพมีการตรวจสอบ ประเมินและพัฒนางานและบุคลากรอย่างต่อเนื่อง

2.6 ยุทธศาสตร์สำนักบริการเทคโนโลยีสารสนเทศ ประกอบด้วย

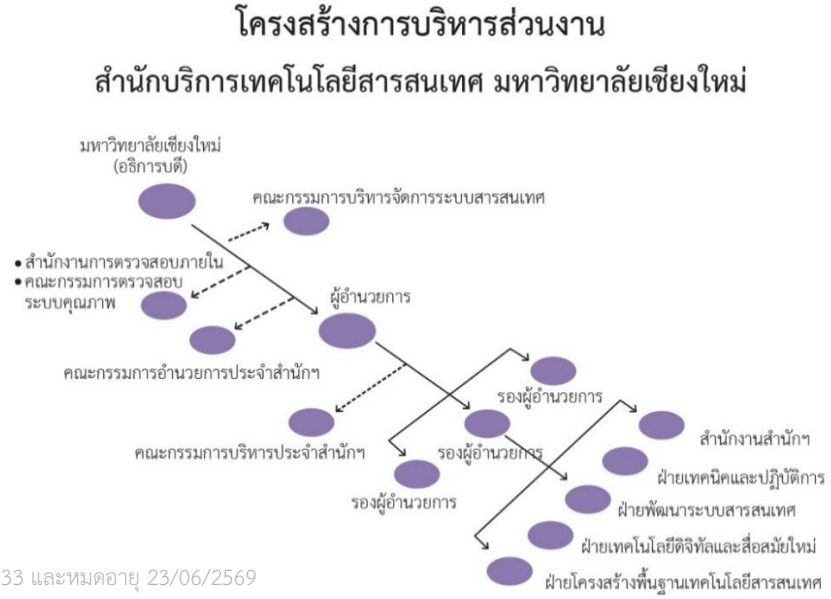
2.6.1 ยุทธศาสตร์ที่ 1 พัฒนาโครงสร้างพื้นฐานไอที (Digital Infrastructure)

2.6.2 ยุทธศาสตร์ที่ 2 สนับสนุนเทคโนโลยีสารสนเทศเพื่อการบริหารจัดการมหาวิทยาลัย (Digital Administration)

2.6.3 ยุทธศาสตร์ที่ 3 การประยุกต์ใช้เทคโนโลยีเพื่อสนับสนุนการสอนและการเรียนรู้ในศตวรรษที่ 21 (Technology Applications for 21st Century Teaching and Learning)

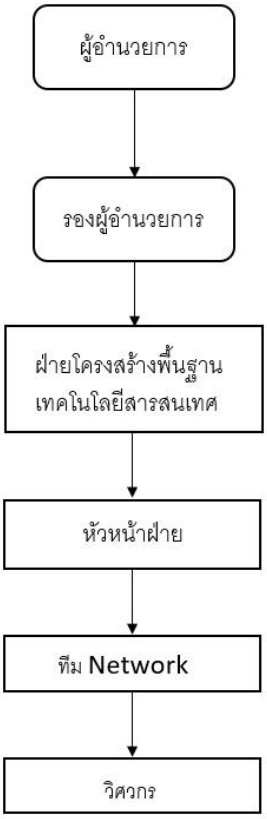
2.6.4 ยุทธศาสตร์ที่ 4 การพัฒนาเทคโนโลยีสำหรับนวัตกรรมการบริการ (Technology Development for Service Innovation)

2.7 โครงสร้างองค์กร (Organization Chart)



ภาพที่ 3 แผนผังองค์กร (Organization Chart)

2.8 โครงสร้างการปฏิบัติงาน (Activity Chart)



ภาพที่ 4 แผนผังการปฏิบัติงาน

ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ สำนักบริการเทคโนโลยีสารสนเทศ มีหน้าที่รับผิดชอบในส่วนของภารกิจหลักที่สนับสนุนงานของมหาวิทยาลัย ในด้านโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ หรือ IT Infrastructure ซึ่งประกอบด้วย ระบบเครือข่ายหลักของมหาวิทยาลัยเชียงใหม่ (CMU-NET) ซึ่งเชื่อมโยงไปยังทุกคณะ วิทยาลัย สำนัก สถาบัน ศูนย์ และหน่วยงานต่าง ๆ CMU-NET ถือได้ว่าหัวใจของการรับส่งข้อมูลที่สำคัญของมหาวิทยาลัย และเป็นระบบเครือข่ายแบบองค์กรที่ทันสมัยและมีขนาดใหญ่ที่สุดในสถาบันการศึกษาทางภาคเหนือ โดยมีชุมทางหลักในการกระจายสัญญาณ (Node) อยู่ที่สำนักบริการเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์ คณะวิศวกรรมศาสตร์ คณะเกษตรศาสตร์ และศูนย์วิจัยแม่เหียะ ซึ่งมีอุปกรณ์สลับสัญญาณ (Switch) และอุปกรณ์เลือกเส้นทาง (Router) ที่ทันสมัยและมีเส้นทางเชื่อมโยงข้อมูลด้วยความเร็วสูงสุดถึง 120 Gbps ระบบเครือข่ายไร้สายของมหาวิทยาลัย (JumboPlus WiFi) ซึ่งให้บริการการเชื่อมต่อระบบเครือข่ายไร้สายแก่นักศึกษา คณาจารย์ และบุคลากร ครอบคลุมทุกอาคารทุกพื้นที่ใช้สอยของมหาวิทยาลัย ทั้งภายในอาคารและภายนอกอาคาร โดยมีจุดให้บริการหรืออุปกรณ์กระจายสัญญาณ (Access Point) มากถึง 5,600 จุด ระบบเครือข่ายอินเทอร์เน็ตความเร็วสูง (Internet) ซึ่งมีความเร็วรวมมากถึง 11 Gbps รองรับการใช้งานได้หลายหมื่นคนและมีช่องสัญญาณสำรอง เพื่อเสถียรภาพการใช้งานที่ดียิ่งขึ้น ระบบ

เครือข่ายระหว่างมหาวิทยาลัย (UNI-NET) ซึ่งมหาวิทยาลัยเชียงใหม่เป็นชุมทางหลักในการกระจายสัญญาณให้กับมหาวิทยาลัยและสถาบันการศึกษาในเขตภาคเหนือ และศูนย์บริการข้อมูล (Data Center) ซึ่งให้บริการเครื่องคอมพิวเตอร์แม่ข่าย พร้อมการรักษาความปลอดภัยและการสำรองข้อมูล โดยได้รับการรับรองมาตรฐานสากล ISO/IEC27001

2.9 บทบาทหน้าที่ความรับผิดชอบ

ชื่อตำแหน่ง วิศวกร

หน้าที่ความรับผิดชอบหลัก

1. ติดตั้ง ดูแล แก้ไข ตรวจสอบ ปรับตั้งค่าการทำงานต่าง ๆ ของอุปกรณ์สลับสัญญาณ (Switch) ของส่วนกลางและที่หน่วยงานต่าง ๆ ทั่วทั้งมหาวิทยาลัยเชียงใหม่ รวมถึงฝั่งสวนดอก แม่เหียะ และศูนย์การศึกษาหริภุญไชย

2. ตรวจสอบ ดูแล การเชื่อมต่อสายสัญญาณโครงข่ายใยแก้วนำแสง (Fiber Optic) ระหว่างส่วนกลางไปยังหน่วยงานต่าง ๆ ทั่วทั้งมหาวิทยาลัยเชียงใหม่ รวมทั้งฝั่งสวนดอก แม่เหียะ และศูนย์การศึกษาหริภุญไชย

3. ดูแล ตรวจสอบ ติดตั้ง รื้อถอน อุปกรณ์และสายสัญญาณของระบบเครือข่ายคอมพิวเตอร์ภายในห้องศูนย์ข้อมูลกลาง (Data Center) ของสำนักบริการเทคโนโลยีสารสนเทศ (Information Technology Service Center: ITSC)

4. ตรวจสอบ แก้ไข ระบบเครือข่ายไร้สาย (Wireless) ของมหาวิทยาลัยใหม่

5. จัดทำข้อมูลต่าง ๆ เพื่อใช้งานการทำ ISO 27001

6. ให้คำปรึกษา และแก้ไขปัญหาด้านระบบเครือข่ายให้แก่ผู้ดูแลระบบของหน่วยงานต่าง ๆ ภายในมหาวิทยาลัย

7. ดูแลการทำงานของ Router และการเชื่อมต่อระหว่าง AS-Number ของมหาวิทยาลัยเชียงใหม่

8. ควบคุม ดูแล จัดสรรการใช้งานระบบ IP Address ภายในมหาวิทยาลัย รวมถึงตรวจสอบความถูกต้องของการใช้งาน เพื่อการใช้งานที่มีประสิทธิภาพ

บทที่ 3
หลักการปฏิบัติงาน

คู่มือการปฏิบัติงานเรื่องดูแล และการเชื่อมต่อระบบเครือข่ายหลักมหาวิทยาลัยเชียงใหม่ (CMU-NET) มีหลักการที่เกี่ยวข้องดังนี้

3.1 แนวคิดและหลักการการออกแบบระบบเครือข่าย

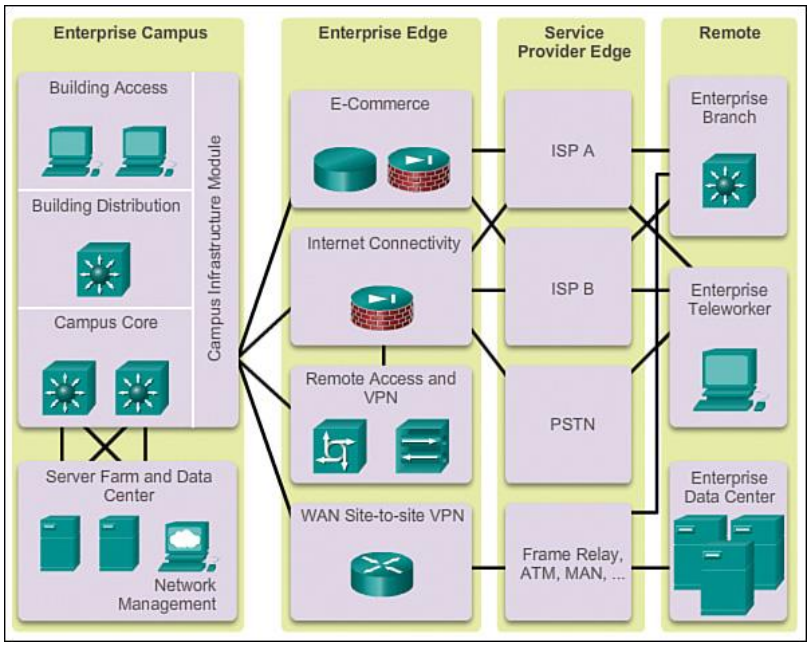
3.2 หลักการทฤษฎีและมาตรฐานที่เกี่ยวกับระบบเครือข่าย

3.3 หมายเลขไอพี (IP Address)

3.4 อุปกรณ์สลับสัญญาณ Layer 3

3.1 แนวคิดและหลักการการออกแบบระบบเครือข่าย

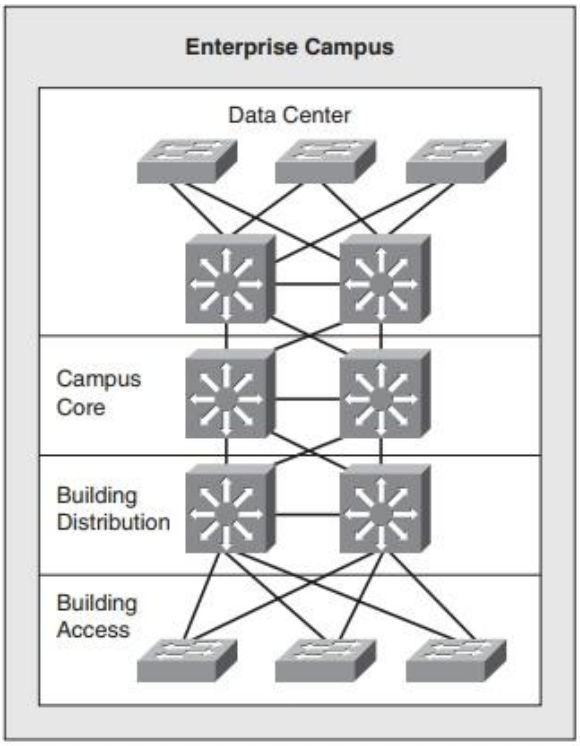
การออกแบบระบบเครือข่ายด้วย Enterprise Network Architecture Model ในการออกแบบระบบเครือข่ายในระดับองค์ที่มีขนาดใหญ่นั้น ต้องมีการออกแบบที่เป็นระบบ จำเป็นต้องแบ่งส่วนของการใช้งานออกเป็นส่วน ๆ



ภาพที่ 5 Enterprise Network Architecture Model

ในส่วนของมหาวิทยาลัยเชียงใหม่ ได้ใช้ส่วนของ Enterprise Campus เป็นต้นแบบในการออกแบบระบบเครือข่ายเพื่อเชื่อมต่อไปยังคณะและหน่วยงานต่าง ๆ

โดยแบ่งออกเป็น 3 ส่วน คือ



ภาพที่ 6 การออกแบบระบบเครือข่ายแบบลำดับขั้น (Hierarchical Model)

Core Layer เป็นส่วนที่มีความเร็วสูงที่สุดในระบบเครือข่ายหลัก อุปกรณ์เครือข่ายที่อยู่ในส่วนนี้จะส่งข้อมูลได้รวดเร็ว มีความน่าเชื่อถือสูง มีการติดตั้งแบบทดแทนกันได้

Distribute Layer เป็นจุดที่ใช้แบ่งระหว่าง Core Layer กับ Access Layer มีคุณสมบัติในการรวบรวมการเชื่อมต่อจากอุปกรณ์ต่าง ๆ ได้เป็นจำนวนมาก ทำงานได้ทั้ง Routing และ Switching

Access Layer เป็นจุดที่ผู้รับบริการทำการเชื่อมต่อเข้ามายังระบบเครือข่ายหลัก อุปกรณ์ส่วนใหญ่มีคุณสมบัติทำงานแบบ Switching ในบางกรณียังสามารถจ่ายกระแสไฟฟ้าผ่านทางสาย LAN ไปยังอุปกรณ์ปลายทางได้อีกด้วย โดยในคู่มือเล่มนี้จะเน้นที่เกี่ยวกับอุปกรณ์ใน Access Layer นี้

3.2 หลักการทฤษฎีและมาตรฐานที่เกี่ยวกับระบบเครือข่าย

การเลือกใช้อุปกรณ์บนระบบเครือข่าย

ในการพิจารณาเลือกอุปกรณ์เพื่อนำมาใช้งานในระบบเครือข่ายหลัก นอกจากผู้ปฏิบัติจะทราบถึงลักษณะการออกแบบแล้ว การเลือกใช้งานอุปกรณ์ที่มีความเหมาะสม จึงเป็นส่วนสำคัญเช่นกัน เพื่อให้ระบบเครือข่ายมีความเสถียร และรองรับการใช้งานของผู้ใช้งานที่เติบโตขึ้นในทุก ๆ ปี

การเลือกอุปกรณ์ในส่วนของ Core Layer ควรพิจารณาคุณสมบัติของอุปกรณ์ดังต่อไปนี้

1. ความเร็วของพอร์ทที่เชื่อมต่อไปยังอุปกรณ์
2. จำนวนพอร์ทเพียงพอต่อการเชื่อมต่อ
3. ชนิดของสายและโมดูลที่ใช้กับพอร์ท
4. รองรับการทำงานแบบทำงานทดแทนกันได้
5. มีระบบจ่ายไฟ 2 แหล่งจ่าย

การเลือกอุปกรณ์ในส่วนของ Distribute Layer ควรพิจารณาคุณสมบัติของอุปกรณ์ดังต่อไปนี้

1. ความเร็วของพอร์ทที่เชื่อมต่อไปยังอุปกรณ์
2. จำนวนพอร์ทเพียงพอต่อการเชื่อมต่อ
3. ชนิดของสายและโมดูลที่ใช้กับพอร์ท
4. ความสามารถในการทำ Routing

การเลือกอุปกรณ์ในส่วนของ Access Layer ควรพิจารณาคุณสมบัติของอุปกรณ์ดังต่อไปนี้

1. ความเร็วของพอร์ทที่เชื่อมต่อไปยังอุปกรณ์
2. จำนวนพอร์ทเพียงพอต่อการเชื่อมต่อ
3. ชนิดของสายและโมดูลที่ใช้กับพอร์ท

ตารางเส้นทางรับส่งข้อมูล (Routing Table)

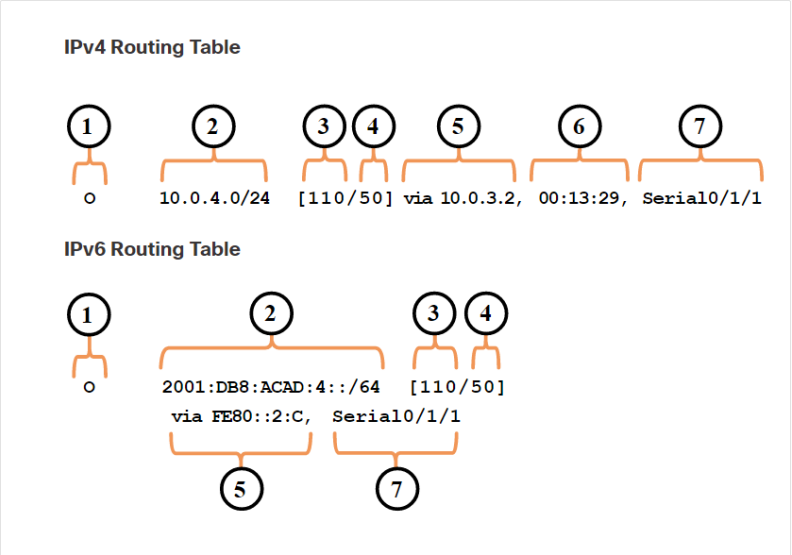
ในการส่งข้อมูลในระบบเครือข่ายนั้น อุปกรณ์ Router เป็นสิ่งที่ใช้ค้นหาเส้นทางที่ดีที่สุด เพื่อส่งข้อมูลไปยังปลายทาง ซึ่งการค้นหาเส้นทางนั้น Router จะค้นหาจาก Routing table ดังนั้นผู้ปฏิบัติงานจึงมีความจำเป็นที่จะต้องอ่านข้อมูลที่แสดงบน Routing table ให้เข้าใจ เพื่อให้ทราบถึงเส้นทางที่ข้อมูลจะถูกส่งออกไป

```
R2# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 209.165.200.226 to network 0.0.0.0
S*   0.0.0.0/0 [1/0] via 209.165.200.226
     10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O       10.0.1.0/24 [110/65] via 10.0.3.1, 00:31:38, Serial0/1/0
O       10.0.2.0/24 [110/65] via 10.0.3.1, 00:31:38, Serial0/1/0
C       10.0.3.0/24 is directly connected, Serial0/1/0
L       10.0.3.2/32 is directly connected, Serial0/1/0
C       10.0.4.0/24 is directly connected, GigabitEthernet0/0/0
L       10.0.4.1/32 is directly connected, GigabitEthernet0/0/0
C       10.0.5.0/24 is directly connected, GigabitEthernet0/0/1
L       10.0.5.1/32 is directly connected, GigabitEthernet0/0/1
     209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.200.224/30 is directly connected, Serial0/1/1
L       209.165.200.225/32 is directly connected, Serial0/1/1
R2#
```


ภาพที่ 7 Routing Table ผ่านทาง terminal

จากภาพที่ 7 Routing Table ประกอบไปด้วยรายการของเส้นทางที่รู้จักในรูปแบบของ Prefix โดยแหล่งที่มาของข้อมูลแต่ละบรรทัดมาจากการค้นหาเส้นทาง ดังนี้

- เครือข่ายที่เชื่อมต่อโดยตรงกับ Router (Directly Connected Network)
- Static route
- Dynamic routing protocol



ภาพที่ 8 ข้อมูลบน Routing Table

จากภาพที่ 8 ในแต่ละบรรทัดบน Routing table จะระบุข้อมูลของเส้นทางในการส่งข้อมูล ดังนี้

หมายเลข 1 แสดงแหล่งข้อมูลแต่ละเส้นทางจะระบุด้วย code ดังต่อไปนี้

- L – ระบุถึงหมายเลข IP ที่ใส่ให้กับ Interface ของ Router
- C - ระบุถึง Directly connected network
- S – ระบุถึง Static route
- O – ระบุถึง Dynamic routing protocol ที่ได้รับข้อมูลมาจาก Router ตัวอื่น ๆ ผ่านทาง Protocol OSPF
- * - ระบุถึงเส้นทางที่จะเป็น Default route

นอกจากนี้ยังมี code ต่าง ๆ อย่างหลายตัว ซึ่งแสดงอยู่ด้านบน Routing table

หมายเลข 2 แสดง Prefix ของเครือข่ายปลายทางที่ Router สามารถส่งข้อมูลไปได้

หมายเลข 3 ค่า Administrative distance ระบุถึงระดับความน่าเชื่อถือของแหล่งข้อมูลของเส้นทางที่ได้รับมา

หมายเลข 4 ค่า Metric ระบุค่าที่ใช้เพื่อไปยังเครือข่ายปลายทาง ค่ายิ่งน้อย ยิ่งทำให้ได้รับเลือก

หมายเลข 5 Next-hop เป็นหมายเลข IP ของ Router ตัวถัดไปที่จะส่ง Packet ออกไป

หมายเลข 6 Routing Timestamp ระบุเวลาล่าสุดที่เส้นทางปรากฏขึ้นบน Routing table

หมายเลข 7 ระบุถึง Interface ที่ Packet จะถูกส่งออกไปยังปลายทาง

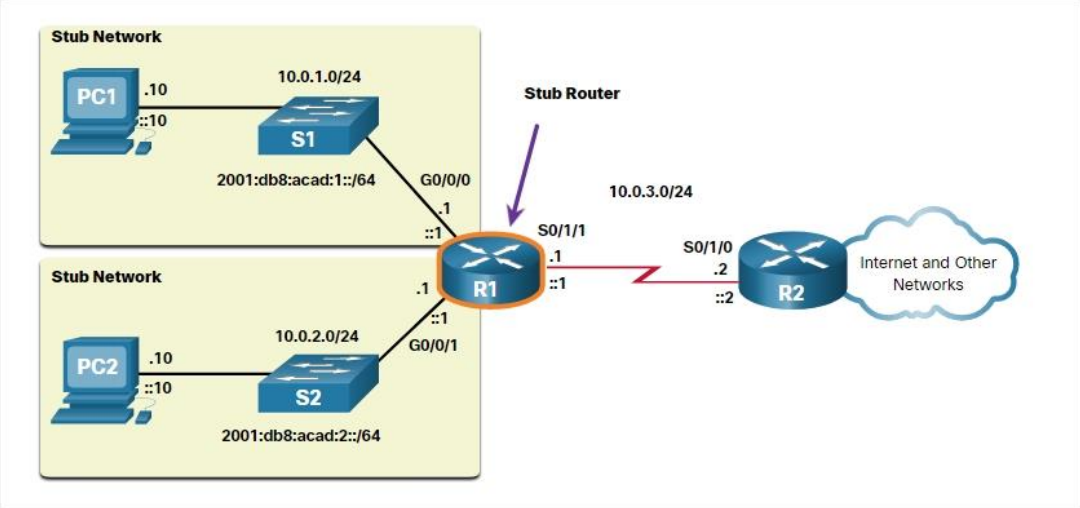
Directly Connected Network

เป็นเครือข่ายที่ได้ถูกตั้งค่าไว้ใน Interface ของ Router ที่มีการทำงาน โดยถูกเพิ่มเข้าไปใน Routing Table เมื่อ Interface ถูกตั้งค่าหมายเลย IP และ Subnet Mask (Prefix Length) และอยู่ในสถานะทำงาน Up เมื่อเรียกข้อมูล Routing Table ขึ้นมาจะปรากฏสัญลักษณ์ C

Static Routes

เป็นการเพิ่มเส้นทางไปยังเครือข่ายที่ต้องการโดยผู้ดูแลระบบเอง ซึ่งจะไม่มีการอัพเดทข้อมูลของเส้นทางโดยอัตโนมัติเหมือนการใช้ Routing Protocol เมื่อระบบเครือข่ายเกิดการเปลี่ยนแปลงไป

การใช้งาน Static Route มีประโยชน์ในด้านความปลอดภัยและทำให้ใช้งาน Resource ได้อย่างมีประสิทธิภาพ เพราะใช้ bandwidth น้อยและ CPU ไม่ต้องประมวลข้อมูลเส้นทาง แต่มีข้อเสียเมื่อระบบเครือข่ายมีขนาดใหญ่ มีเครือข่ายจำนวนมาก จึงเหมาะกับการใช้งานในระบบเครือข่ายขนาดเล็ก ระบบเครือข่ายที่มีเส้นทางเดียว เพื่อไปยังระบบเครือข่ายอื่น ๆ และเครือข่ายแบบ Stub (Stub Network) คือ ระบบเครือข่ายที่มี Router เพียง 1 ตัว และเชื่อมต่อไปยัง Router เพียง 1 ตัว



ภาพที่ 9 Stub Network

Dynamic Routing Protocol

Dynamic Routing Protocol แลกเปลี่ยนข้อมูลของการเชื่อมต่อระบบเครือข่ายระหว่าง Router ด้วยกัน และปรับปรุงให้อัพเดทอยู่เสมอ เมื่อมีการเปลี่ยนแปลงการเชื่อมต่อ ซึ่งทำให้การออกแบบและการขยายขนาดของระบบเครือข่ายทำได้สะดวกรวดเร็ว และจัดการได้ง่ายกว่าการใช้เพียง Static Route ในการดูแลระบบเครือข่ายนั้นจะเรียกกลุ่มของ Router ที่อยู่ภายใต้การดูแลว่า Autonomous System ซึ่งแต่ละหน่วยงานจะได้รับหมายเลขของ Autonomous System (AS Number) เพื่อใช้ส่งข้อมูลไปหากัน

Dynamic Routing Protocol ที่นิยมใช้งานในปัจจุบันแบ่งออกเป็น 2 กลุ่ม คือ Interior Gateway Protocol และ Exterior Gateway Protocol

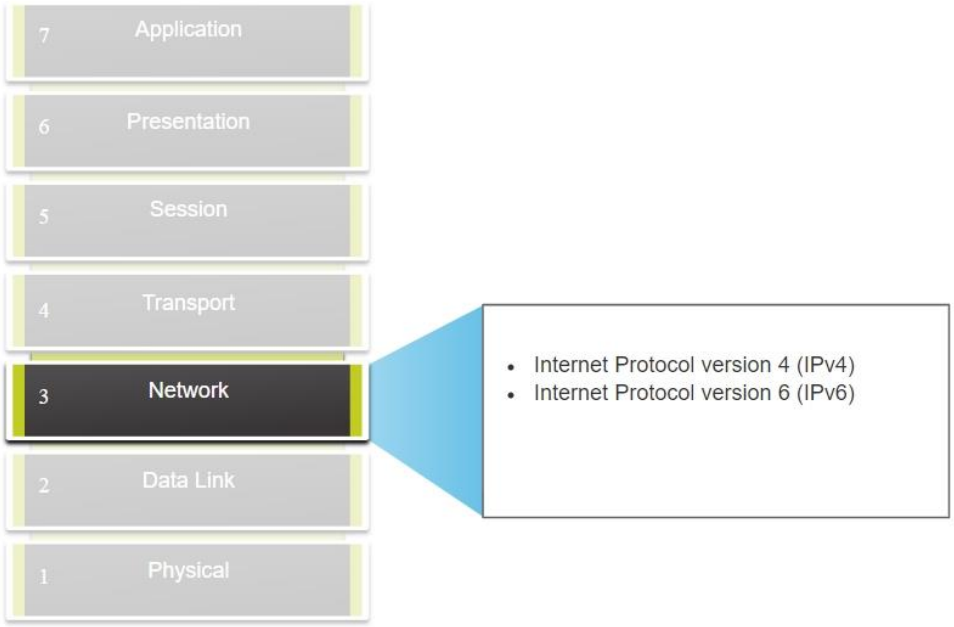
1. Interior Gateway Protocol คือ Routing Protocol ที่ใช้งานภายในระบบเครือข่าย AS เดียวกัน ได้แก่ RIP, OSPF, EIGRP, IS-IS

2. Exterior Gateway Protocol คือ Routing Protocol ที่ใช้ส่งข้อมูลระหว่าง AS ได้แก่ BGP

ในการออกแบบระบบเครือข่ายของมหาวิทยาลัยเชียงใหม่ จะใช้ Open Shortest Path First (OSPF) เป็นหลักในการส่งข้อมูลภายในระบบเครือข่าย เนื่องจากเป็น Protocol ที่เป็นมาตรฐาน ทำให้ใช้งานได้กับผู้ผลิตที่หลากหลาย มีความรวดเร็วในการปรับเปลี่ยนข้อมูลของระบบ

3.3 หมายเลข IP Address

ในระบบ OSI Model นั้น Network Layer หรือ OSI Layer 3 ทำหน้าที่ในบริการแก่อุปกรณ์ในการแลกเปลี่ยนข้อมูลข้ามระบบเครือข่าย โดยใช้หมายเลข IPv4 และ IPv6 เป็นหลัก

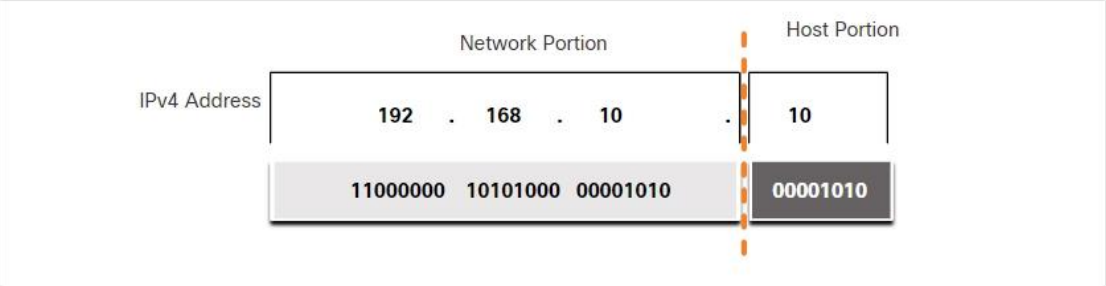


ภาพที่ 10 ภาพแสดง Network Layer จาก OSI 7 Layer Model

หมายเลข IPv4 นั้นเป็นชุดตัวเลขฐานสอง จำนวน 32-bit เรียงต่อกัน โดยทุก ๆ 8-bit จะคั่นด้วย . (dot) เพื่อให้ผู้ใช้งานสามารถเข้าใจได้ง่าย เลข 8-bit แต่ละชุดจะถูกแปลงให้เป็นเลขฐานสิบตัวอย่างเช่น 11000000.10101000.00001010.00001010 สามารถเขียนในรูปเลขฐานสิบเป็น 192.168.10.10

การใช้งาน IPv4

ตัวเลข 32-bit ของ IPv4 นั้นจะแบ่งออกเป็น 2 ส่วน คือ ส่วนของเครือข่าย (Network Portion) และส่วนของผู้ใช้ (Host Portion)



ภาพที่ 11 การแบ่งส่วนใช้งานของหมายเลขไอพี

การจัดสรรและกำหนดหมายเลข IP บนระบบเครือข่าย CMU-NET

ในการนำหมายเลข IP Address มาใช้ในระบบเครือข่ายของมหาวิทยาลัยเชียงใหม่ ซึ่งมีขนาดใหญ่ทั้งจำนวนหน่วยงาน และปริมาณผู้ใช้งานที่สูง ทำให้ต้องมีการแบ่ง Subnet เพื่อลดปริมาณข้อมูลที่ส่งถึงกันภายในระบบเครือข่าย และเพิ่มประสิทธิภาพของการส่งข้อมูลให้ดียิ่งขึ้น นอกจากนี้ยังทำให้ผู้ดูแลระบบเครือข่ายสามารถนำนโยบายด้านความปลอดภัย (Security Policy) ซึ่งมีทั้งการอนุญาตและไม่อนุญาตให้เข้าถึงมาใช้งานได้ อีกเหตุผลหนึ่งคือ การลดจำนวนของอุปกรณ์ที่จะส่งข้อมูลหากัน (Broadcast Traffic) ในแต่ละ Subnet อีกด้วย

การแบ่ง Subnet ของ IPv4

การแบ่ง Subnet ของ IPv4 นั้นทำได้โดยการใช้ Host bit จำนวน 1 bit หรือมากกว่านั้นมาเป็น Network bit สามารถทำได้โดยการยืม Subnet mask เพิ่มจากส่วนของ host เพื่อเพิ่ม Network bit ยิ่งมีการยืม host bit ยิ่งได้จำนวน Subnet ที่มากขึ้น แต่จะลดจำนวน host ที่ใช้งานได้ภายใน Subnet นั้น

ในการแบ่ง Subnet ที่ง่ายที่สุด จะแบ่งในส่วนของ Octet พอดีเป็น /8, /16, /24 ดังตารางต่อไปนี้

ตารางที่ 1 ตารางการแบ่ง Subnet แบบตรง Octet

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of hosts
/8	255.0.0.0	nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh 11111111.00000000.00000000.00000000	16,777,214
/16	255.255.0.0	nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh 11111111.11111111.00000000.00000000	65,534
/24	255.255.255.0	nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh 11111111.11111111.11111111.00000000	254

ในการแบ่ง Subnet แบบที่ไม่ตรงกับ Octet จะต้องไปยืมส่วนของ Host ใน Subnet mask มาใช้งาน ดังตารางต่อไปนี้

ตารางที่ 2 การแบ่ง Subnet แบบยืมส่วนของ Host

Prefix Length	Subnet Mask	Network Address (n = network, h = host)	# of subnets	# of hosts
/17	255.255.128.0	nnnnnnnn.nnnnnnnn.nhhhhhhh.hhhhhhhh 11111111.11111111.10000000.00000000	2	32766
/18	255.255.192.0	nnnnnnnn.nnnnnnnn.nnhhhhhh.hhhhhhhh 11111111.11111111.11000000.00000000	4	16382
/19	255.255.224.0	nnnnnnnn.nnnnnnnn.nnnhhhhh.hhhhhhhh 11111111.11111111.11100000.00000000	8	8190
/20	255.255.240.0	nnnnnnnn.nnnnnnnn.nnnnhhhh.hhhhhhhh 11111111.11111111.11110000.00000000	16	4094
/21	255.255.248.0	nnnnnnnn.nnnnnnnn.nnnnnhhh.hhhhhhhh 11111111.11111111.11111000.00000000	32	2046
/22	255.255.252.0	nnnnnnnn.nnnnnnnn.nnnnnnhh.hhhhhhhh 11111111.11111111.11111100.00000000	64	1022
/23	255.255.254.0	nnnnnnnn.nnnnnnnn.nnnnnnnh.hhhhhhhh 11111111.11111111.11111110.00000000	128	510
/24	255.255.255.0	nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh 11111111.11111111.11111111.00000000	256	254
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.nhhhhhhh 11111111.11111111.11111111.10000000	512	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnhhhhhh 11111111.11111111.11111111.11000000	1024	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnhhhhh 11111111.11111111.11111111.11100000	2048	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnhhhh 11111111.11111111.11111111.11110000	4096	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnhhh 11111111.11111111.11111111.11111000	8192	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnhh 11111111.11111111.11111111.11111100	16384	2

3.4 อุปกรณ์สลับสัญญาณ Layer 3

เนื่องจากระบบเครือข่ายหลักของทางมหาวิทยาลัยเชียงใหม่นั้น มีพื้นที่ครอบคลุมเป็นบริเวณกว้างอุปกรณ์สลับสัญญาณที่นำมาใช้งานจึงต้องมีประสิทธิภาพสูง สามารถรองรับจำนวนผู้ใช้งานและปริมาณข้อมูลที่รับส่งได้เป็นจำนวนมาก การเลือกใช้งานอุปกรณ์ในแต่ละ Layer จึงเป็นสิ่งที่ต้องพิจารณาเป็นหลัก

ในระดับ Core Layer เป็นศูนย์รวมของข้อมูลจากทุก Zone มารวมกันไว้เพื่อส่งต่อออกไปภายนอกระบบเครือข่าย อุปกรณ์ที่ใช้จึงเป็น Cisco Catalyst 9500-32C ซึ่งมีจำนวน 32 port แต่ละ port รองรับความเร็วในการส่งข้อมูลถึง 100 Gbps

ภาพที่ 12 Cisco Catalyst 9500-32C

ในระดับ Distribute Layer เป็นอุปกรณ์สลับสัญญาณที่กระจายไปตาม Zone ต่าง ๆ เพื่อรองรับการเชื่อมต่อจากคณะ และหน่วยงานใน Zone ที่ติดตั้ง อุปกรณ์ที่ใช้เป็น Cisco Catalyst 9500-48 ซึ่งมี port ทั้งหมดรองรับการเชื่อมต่อแบบใยแก้วนำแสง จำนวน 48 port แต่ละ port รองรับความเร็วในการส่งข้อมูลสูงสุดถึง 10 Gbps

ภาพที่ 13 Cisco Catalyst 9500-32C

ในการเลือกใช้งานอุปกรณ์ระดับ Access Layer เพื่อมาเป็นจุดเชื่อมต่อสำหรับหน่วยงานนั้น ใช้อุปกรณ์สลับสัญญาณ Layer 3 ซึ่งมีคุณสมบัติที่ทำงานได้ทั้งหน้าที่ของ Switch ในระดับ Layer 2 และ Router ในระดับ Layer 3 รวมไว้ในอุปกรณ์เดียว ทำให้สามารถส่งข้อมูลภายใน Subnet เดียวกันได้และส่งข้อมูลข้าม Subnet ได้อีกด้วย โดยรุ่นที่เลือกนำมาใช้เป็น Cisco Catalyst 9300-24T

ภาพที่ 14 Cisco Catalyst 9500-24T

บทที่ 4
เทคนิคในการปฏิบัติงาน

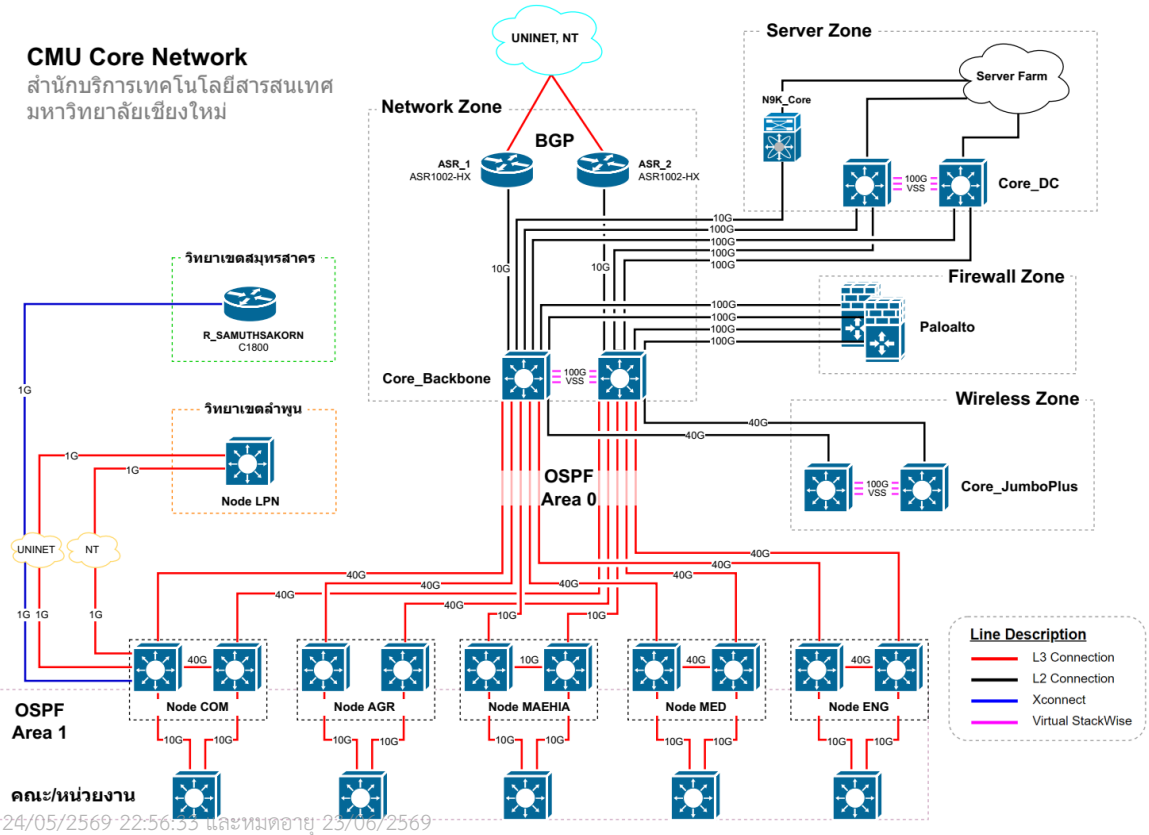
4.1 การออกแบบระบบเครือข่ายหลักมหาวิทยาลัยเชียงใหม่

ในการปฏิบัติงานเพื่อดูแลระบบเครือข่ายหลักของทางมหาวิทยาลัยเชียงใหม่ (CMU-NET2020) ซึ่งมีขนาดใหญ่ และซับซ้อน ผู้ปฏิบัติงานต้องมีความรู้และความเข้าใจเกี่ยวกับภาพรวมของทั้งระบบ เพื่อให้เข้าใจหลักการทำงาน และสามารถปฏิบัติงานได้อย่างถูกต้อง โดยสิ่งที่จำเป็นต้องเข้าใจก่อนการปฏิบัติงานมีดังนี้

4.1.1 การออกแบบ Zone ติดตั้งอุปกรณ์

4.1.2 การจัดสรร IP Address เพื่อใช้งานภายในมหาวิทยาลัยเชียงใหม่

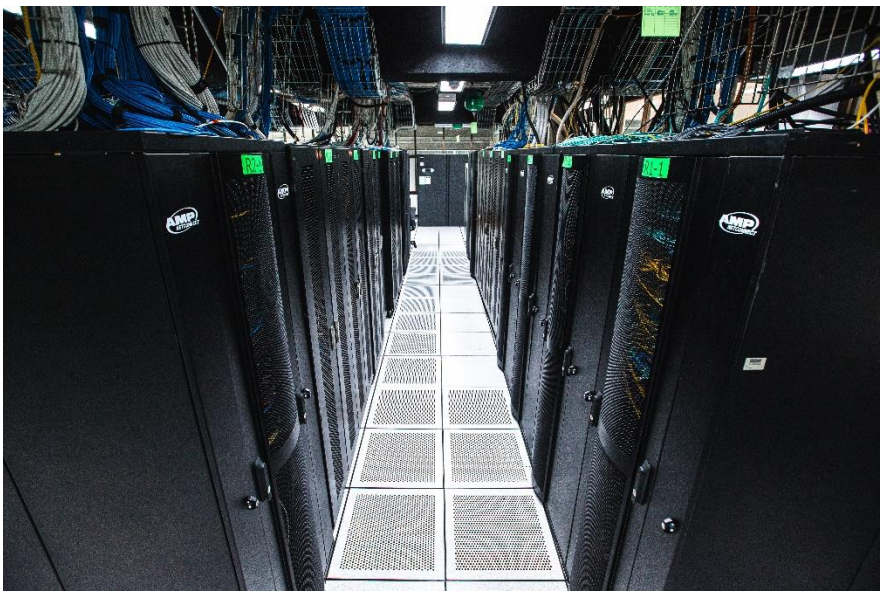
4.1.1 การออกแบบ Zone ติดตั้งอุปกรณ์



ภาพที่ 15 แผนผัง CMU-NET 2020

ตามหลักการออกแบบระบบเครือข่ายนั้น ระบบเครือข่าย CMU-NET2020 ได้แบ่งลำดับขั้นตอนการทำงานของอุปกรณ์เป็น Core Layer, Distribution Layer และ Access Layer

Core Layer อุปกรณ์ทั้งหมดติดตั้งอยู่ที่ Data Center ที่ ITSC ทำงานร่วมกับ Firewall, Router, เครื่องคอมพิวเตอร์แม่ข่าย ระบบต่าง ๆ และยังเป็นจุดเชื่อมต่อกับผู้ให้บริการอินเทอร์เน็ต เพื่อรับส่งข้อมูลสู่อินเทอร์เน็ตอีกด้วย นอกจากนี้ยังเป็นจุดรวมการเชื่อมต่อเครือข่ายจาก Zone ต่าง ๆ ของ Distribution Layer อีกด้วย



ภาพที่ 16 ห้อง Data Center, ITSC

Distribution Layer อุปกรณ์ในส่วนนี้จะถูกกระจายไปยัง Zone ต่าง ๆ เพื่อรองรับการเชื่อมต่อจากอุปกรณ์ในระดับ Access Layer ที่ติดตั้งตามคณะและหน่วยงานใน Zone นั้น ๆ โดยได้แบ่ง Zone ดังนี้

Zone COM มีจุดติดตั้งอุปกรณ์ในระดับ Distribution Layer ติดตั้งอยู่ที่ Data Center ของ ITSC รองรับการเชื่อมต่อจากคณะและหน่วยงานที่มีพื้นที่ตั้งอยู่บริเวณสวนสัก ประกอบด้วยหน่วยงาน ดังต่อไปนี้

1. คณะสังคมศาสตร์
2. คณะนิติศาสตร์
3. คณะมนุษยศาสตร์
4. คณะรัฐศาสตร์
5. คณะวิทยาศาสตร์
6. คณะเศรษฐศาสตร์
7. คณะวิทยาลัยสื่อ ศิลปะ และเทคโนโลยี

8. คณะการสื่อสารมวลชน
9. สำนักบริการเทคโนโลยีสารสนเทศ
10. สำนักทะเบียนและประมวลผล
11. สำนักหอสมุด
12. สำนักงานอธิการบดี
13. สำนักพัฒนาคุณภาพการศึกษา
14. พฤฒพลัง
15. หอพักอ่างแก้ว
16. ศูนย์นโยบายสาธารณะ
17. ศูนย์จัดการเมืองอัจฉริยะ
18. สหกรณ์ออมทรัพย์ มช.

Zone AGR มีจุดติดตั้งอุปกรณ์ในระดับ Distribution Layer โดยติดตั้งอยู่ที่คณะเกษตรศาสตร์ รองรับการเชื่อมต่อจากคณะและหน่วยงานที่มีพื้นที่ตั้งอยู่บริเวณหลังมหาวิทยาลัยฝั่งตะวันออก ประกอบด้วยหน่วยงาน ดังต่อไปนี้

1. คณะเกษตรศาสตร์
2. คณะศึกษาศาสตร์
3. คณะบริหารธุรกิจ
4. คณะวิจิตรศิลป์
5. สถาบันภาษา
6. สถาบันวิจัยสังคม
7. สถาบันวิจัยวิทยาศาสตร์และเทคโนโลยี
8. บัณฑิตวิทยาลัย
9. โรงพยาบาลสัตว์เล็ก
10. สำนักส่งเสริมศิลปวัฒนธรรม

Zone MED มีจุดติดตั้งอุปกรณ์ในระดับ Distribution Layer โดยติดตั้งอยู่ที่คณะแพทยศาสตร์ รองรับการเชื่อมต่อจากคณะและหน่วยงานที่มีพื้นที่ตั้งอยู่บริเวณฝั่งสวนดอก ประกอบด้วยหน่วยงาน ดังต่อไปนี้

1. คณะแพทยศาสตร์
2. คณะเภสัชศาสตร์
3. คณะทันตแพทยศาสตร์
4. คณะพยาบาลศาสตร์
5. คณะเทคนิคการแพทย์

6. สถาบันวิจัยวิทยาศาสตร์สุขภาพ
7. สำนักบริการวิชาการ
8. วิทยาลัยนานาชาตินวัตกรรมดิจิทัล
9. หอพักนักศึกษาฝั่งสวนดอก
10. หอประชุมใหญ่

Zone ENG มีจุดติดตั้งอุปกรณ์ในระดับ Distribution Layer โดยติดตั้งอยู่ที่คณะวิศวกรรมศาสตร์ รองรับการเชื่อมต่อจากคณะและหน่วยงานที่มีพื้นที่ตั้งอยู่บริเวณหลังมหาวิทยาลัย ฝั่งตะวันตก ประกอบด้วยหน่วยงาน ดังต่อไปนี้

1. คณะวิศวกรรมศาสตร์
2. คณะสถาปัตยกรรมศาสตร์
3. คณะสาธารณสุขศาสตร์
4. ศูนย์นวัตกรรมการสอนและการเรียนรู้ (TLIC)
5. หอพักนักศึกษาทั้งหมด

Zone MAEHIA มีจุดติดตั้งอุปกรณ์ในระดับ Distribution Layer ติดตั้งอยู่ที่ศูนย์วิจัยแม่เหียะ รองรับการเชื่อมต่อจากคณะและหน่วยงานที่มีพื้นที่ตั้งอยู่บริเวณฝั่งแม่เหียะ ประกอบด้วยหน่วยงาน ดังต่อไปนี้

1. คณะสัตวแพทยศาสตร์
2. คณะอุตสาหกรรมเกษตร
3. สถาบันวิจัยและพัฒนาพลังงานนครพิงค์
4. อุทยานวิทยาศาสตร์
5. หอพักในกำกับแม่เหียะ

Zone Lumphun มีจุดติดตั้งอุปกรณ์ในระดับ Distribution Layer ติดตั้งอยู่ที่ศูนย์การเรียนรู้หริภุญชัย จังหวัดลำพูน

Access Layer อุปกรณ์ในส่วนนี้ จะถูกติดตั้งไว้ที่คณะ หน่วยงานที่ทำการเชื่อมต่อระบบเครือข่ายของหน่วยงานเข้ากับระบบเครือข่าย CMU-NET2020 มีการเชื่อมต่อ 2 เส้นทางด้วยสายใยแก้วนำแสงไปยังอุปกรณ์ ระดับ Distribute Layer เพื่อให้มีเส้นทางสำรอง ในกรณีที่เส้นทางใดเส้นทางหนึ่งชำรุดหรือไม่สามารถใช้งานได้ นอกจากนี้ยังเชื่อมต่อกับอุปกรณ์เครือข่ายของคณะหรือหน่วยงานเพื่อเป็นเส้นทางให้หน่วยงานใช้ส่งข้อมูลออกมาจากเครือข่ายภายใน

4.1.2 การจัดสรรหมายเลข IP Address เพื่อใช้งานภายในมหาวิทยาลัยเชียงใหม่

สำนักบริการเทคโนโลยีสารสนเทศ มีหน้าที่รับผิดชอบกำหนดหมายเลข IP Address เพื่อนำไปใช้งานภายในระบบเครือข่ายของมหาวิทยาลัยเชียงใหม่ โดยจัดสรรหมายเลข IP ให้กับหน่วยงาน

สำนัก สถาบัน คณะ รวมไปถึงผู้ใช้บริการจากส่วนกลาง ทั้งนี้ด้วยจำนวนของหน่วยงาน และผู้ใช้งานที่มีจำนวนมาก การจัดสรรหมายเลข IP Address อย่างเป็นระบบจะช่วยให้ใช้งานระบบเครือข่ายได้อย่างเต็มที่ และผู้ดูแลระบบสามารถดูแลระบบได้อย่างราบรื่น

หน่วยงานภายในมหาวิทยาลัยเชียงใหม่ จะได้รับการจัดสรรหมายเลข IPv4 Address จำนวน 2 ชุด ได้แก่

Public IP Address เป็นหมายเลข IP Address สาธารณะที่นำไปใช้งานเพื่อให้สามารถใช้บริการจากภายนอกระบบเครือข่ายของทางมหาวิทยาลัย เช่น Internet และผู้ใช้งานภายนอกสามารถเรียกหาอุปกรณ์ภายในเพื่อขอใช้บริการได้ โดยทางสำนักฯ จะจัดสรรให้หน่วยงานที่ชำระค่าบริการระบบเครือข่ายตามขนาดของหน่วยงาน และผู้ดูแลระบบของหน่วยงานมีหน้าที่นำหมายเลข Public IP Address ไปจัดสรรใช้งานภายในหน่วยงานได้เอง

Private IP Address เป็นหมายเลข IP Address ที่สงวนให้ใช้ภายในมหาวิทยาลัยเท่านั้น จึงสามารถใช้งานได้ภายในหน่วยงานกันเองหรือข้ามหน่วยงานเท่านั้น การเรียกใช้งานจากภายนอกไม่สามารถทำได้

หลักการจัดสรรหมายเลข Private IP Address เพื่อใช้ภายในระบบเครือข่าย CMU-NET

เนื่องจาก Private IP Address มีจำนวนมาก และมีความจำเป็นต่อการใช้งานในระบบเครือข่าย จึงต้องมีการจัดสรรการใช้งานในส่วนต่าง ๆ ให้ครอบคุลม ผู้ดูแลระบบจึงต้องมีความเข้าใจถึงหลักการจัดสรร IP Address ที่ใช้อยู่ในปัจจุบัน

Private IP Address บน CMU-NET มี 3 ชุด

10.0.0.0 /8 ใช้สำหรับจัดสรรในหน่วยงานต่าง ๆ และบริการของส่วนกลาง

172.16.0.0/12 ใช้สำหรับการบริหารจัดการอุปกรณ์

192.168.0.0/16 ใช้สำหรับการบริหารจัดการอุปกรณ์

เพื่อให้สอดคล้องกับการติดตั้งอุปกรณ์ระบบเครือข่าย CMU-NET 2020 การจัดสรรหมายเลข IP Address จึงอ้างอิงการแบ่งโซนของการติดตั้งอุปกรณ์เพื่อให้การดูแลและแก้ไขปัญหาเป็นไปในแนวทางเดียวกัน

ตารางที่ 3 Private IP Address ของชุด 10.0.0.0/8

Subnet	โซนของการติดตั้งอุปกรณ์
10.128.0.0/12	MED
10.144.0.0/12	COM
10.160.0.0/12	ENG
10.176.0.0/12	AGR
10.208.0.0/12	MAEHEA
10.224.0.0/12	LAMPHUN

เมื่อได้ Subnet ใหญ่ของแต่ละโซนแล้ว จะทำการแบ่ง Subnet ย่อย ๆ ให้แก่หน่วยงานที่อยู่ภายในโซนนั้น ๆ และแบ่ง Subnet สำรองไว้ให้บริการของทาง ITSC ใช้ด้วย โดยมีหลักการดังนี้

ตารางที่ 4 ตารางแบ่ง Subnet สำรองไว้ให้บริการของทาง ITSC

10.x.0.0/16	Subnet ใหญ่ของหน่วยงาน
10.x.0.0/17	Subnet ที่หน่วยงานได้รับการจัดสรรไปใช้งาน
10.x.128.0/21	Subnet สำหรับ Access Point ที่ให้บริการ JumboPlus
10.x.136.0/24	Subnet สำหรับบริการจัดการอุปกรณ์ที่ติดตั้ง
10.x.137.0/24	Subnet สำหรับดิจิตอลมิเตอร์ของ ERDI
10.x.138.0/24	Subnet สำหรับบริการ VDI
10.x.139.0/24	Subnet สำรหรับบริหารห้องสมุด
10.x.140.0/24	Subnet สำหรับอุปกรณ์โซลาเซลล์ของ ERDI

หมายเหตุ x แทนด้วยเลข IP Address Octet ที่สองที่หน่วยงานได้รับไป

Subnet สุดท้ายของแต่ละโซนจะถูกนำมาใช้เป็น IP Point to Point เพื่อทำ Routing ระหว่างอุปกรณ์ของทาง ITSC กับแต่ละหน่วยงานที่อยู่ภายในโซนนั้น

ตารางที่ 5 ตาราง IP Point to Point เพื่อทำ Routing

Subnet	**โซนของการติดตั้งอุปกรณ์**
10.143.255.0/24	MED
10.159.255.0/24	COM
10.175.255.0/24	ENG
10.191.255.0/24	AGR
10.223.255.0/24	MAEHEA
10.239.255.0/24	LAMPHUN

ตารางที่ 6 ตารางการแบ่ง Private IP Address ของชุด 172.16.0.0/12
IP สำหรับกำหนดให้แก่อุปกรณ์เพื่อให้ผู้ดูแลระบบสามารถเข้าถึงจากระยะไกลได้

Subnet	**โซนของการติดตั้งอุปกรณ์**
172.16.2.0/24	COM
172.16.3.0/24	ENG
172.16.4.0/24	AGR
172.16.5.0/24	MED
172.16.6.0/24	MAEHEA
172.16.7.0/24	LAMPHUN

ตารางที่ 7 ตารางการแบ่ง Private IP Address ของ ชุด 192.168.0.0/20
IP สำหรับให้แก่อุปกรณ์ระดับ Access เพื่อเชื่อมต่อไปยังอุปกรณ์ระดับ Distribution ในโซนที่ครอบคลุมหน่วยงาน

Subnet	โซนของการติดตั้งอุปกรณ์
192.168.4.0/24, 192.168.5.0/24	COM
192.168.6.0/24, 192.168.7.0/24	ENG
192.168.8.0/24, 192.168.9.0/24	AGR
192.168.10.0/24, 192.168.11.0/24	MED
192.168.12.0/24, 192.168.13.0/24	MAEHEA
192.168.14.0/24, 192.168.15.0/24	LAMPHUN

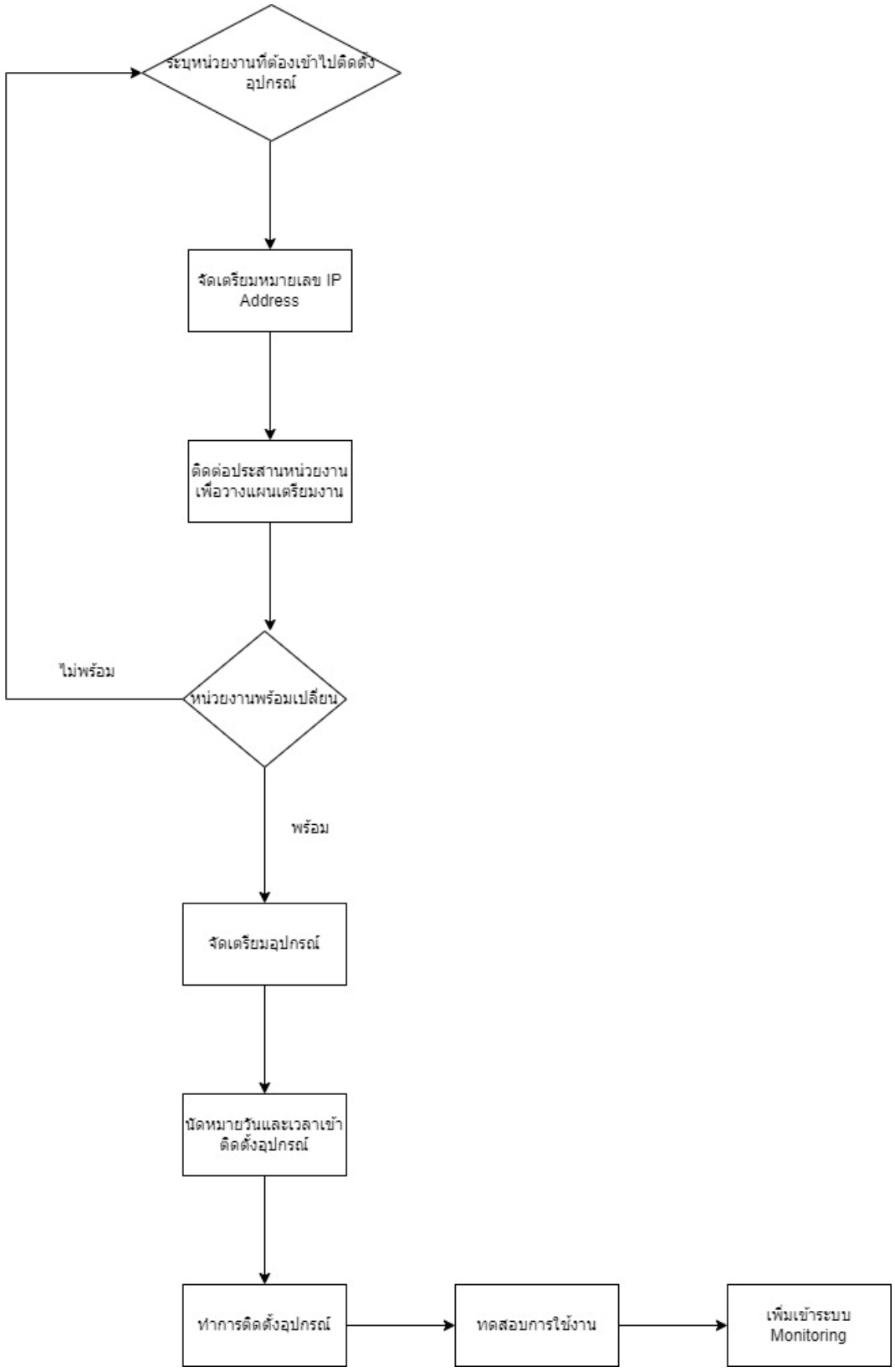
4.2 การติดตั้งอุปกรณ์ Switch Layer 3 ให้กับหน่วยงาน

ในการติดตั้งอุปกรณ์ Switch Layer 3 ให้กับหน่วยงานที่ขอรับบริการเชื่อมต่อระบบเครือข่ายของหน่วยงานเข้ากับระบบเครือข่ายหลัก CMU-NET 2020 นั้นแบ่งออกเป็น 3 ส่วนหลัก ๆ ดังนี้

4.2.1 การเตรียมการก่อนติดตั้ง

4.2.2 การตั้งค่าอุปกรณ์

4.2.3 การติดตั้งอุปกรณ์



ภาพที่ 17 แผนผังการดำเนินงานติดตั้งอุปกรณ์สลับสัญญาณ

4.2.1 การเตรียมการก่อนติดตั้ง

ก่อนที่จะเตรียมอุปกรณ์เพื่อไปติดตั้งที่หน่วยงาน ผู้ปฏิบัติงานต้องติดต่อประสานงานกับผู้ดูแลระบบเครือข่ายของหน่วยงาน เพื่อให้ทราบถึงข้อมูลที่จำเป็นต้องใช้ในการติดตั้ง พร้อมทั้งออกแบบและวางแผนการติดตั้งร่วมกับผู้ดูแลระบบของหน่วยงานให้เข้าใจตรงกัน และทั้งสองฝ่ายจะได้ใช้ข้อมูลร่วมกันในวันที่เข้าไปติดตั้งอุปกรณ์

การเลือกวันติดตั้งอุปกรณ์ หากต้องมีปิดระบบที่ส่งผลกระทบต่อผู้ใช้งานให้ปรึกษาผู้ดูแลระบบของหน่วยงาน เพื่อทำการประกาศปิดระบบให้ผู้ใช้งานทราบก่อน

อุปกรณ์ที่ทาง ITSC เลือกนำไปติดตั้งในระดับ Access Layer นั้น สำหรับคณะ หน่วยงาน จะใช้ Cisco Catalyst 9300 เป็นหลัก โดยที่ตัวอุปกรณ์มี 24 port Gigabit Ethernet สำหรับเชื่อมต่อด้วยสาย UTP และส่วนที่ใช้สายสัญญาณใยแก้วนำแสงนั้น จะมี 2 แบบ คือ 2 port Tengigabit Ethernet และ 4 port Tengigabit Ethernet ดังนั้น ก่อนที่จะนำอุปกรณ์ไปติดตั้ง ผู้ปฏิบัติงานต้องพิจารณาความต้องการของหน่วยงานดังนี้

1. การเชื่อมต่อไปยังหน่วยงาน ใช้ port ชนิดใด UTP หรือ ใยแก้วนำแสง
2. มีการเชื่อมต่อบริการต่าง ๆ ของ ITSC ด้วย port ชนิดใด
3. Port ที่เชื่อมต่อใช้ความเร็วเท่าใด 1 Gbps หรือ 10 Gbps
4. มีรูปแบบการเชื่อมต่อเข้ากับหน่วยงานแบบใด ต่อเข้ากับอุปกรณ์ Switch หรือ Firewall
5. หมายเลข IP Address ที่ต้องใช้งานกับหน่วยงาน ทั้ง Private IP Address และ Public IP Address

4.2.2 การตั้งค่าอุปกรณ์

หลังจากผู้ปฏิบัติงานได้ออกแบบการติดตั้งและเตรียมข้อมูลต่าง ๆ แล้ว ผู้ปฏิบัติงานต้องนำอุปกรณ์ที่จะติดตั้งมาตั้งค่าการทำงาน (Configuration) ตามที่เตรียมไว้ เพื่อให้สามารถทำงานได้อย่างเหมาะสมตามต้องการ และสามารถดูแลด้วยการมอนิเตอร์หรือเข้าถึงจากระยะไกลต่อได้หลังจากติดตั้งไปแล้ว

การเข้าถึงอุปกรณ์เพื่อ Configuration

อุปกรณ์ที่นำมาใช้ในระบบเครือข่าย CMU-NET นั้น เป็นอุปกรณ์ที่อยู่ในระดับสูง จึงต้องมีการตั้งค่าก่อนใช้งานทุกครั้ง เพื่อให้สามารถทำงานเข้ากับระบบที่มีอยู่ได้ และทำให้ทำงานได้อย่างถูกต้อง ในการตั้งค่า Configuration มีวิธีการดังนี้

Console เป็นการตั้งค่าโดยการเข้าถึงที่ตัวอุปกรณ์ ด้วยการใช้สาย console เชื่อมต่อที่ port ที่แยกจากการใช้งาน โดย port สำหรับ console จะใช้เพื่อการเข้าถึงอุปกรณ์เพื่อตั้งค่าเท่านั้น สำหรับการใช้ console นั้นจะใช้ตอนเริ่มต้นตั้งค่าการใช้งานอุปกรณ์หรือในกรณีที่ไม่สามารถใช้งานจากระยะไกล

Telnet เป็นการเข้าถึงอุปกรณ์จากระยะไกลที่ไม่มีการเข้ารหัส เพื่อไปบริหารจัดการอุปกรณ์บนระบบเครือข่าย ซึ่งมักจะใช้ในอุปกรณ์ที่เก่าหรือในสภาพแวดล้อม เพื่อการทดสอบเท่านั้น ไม่แนะนำให้ใช้กับการใช้งานจริง

Secure Shell (SSH) เป็นการเข้าถึงอุปกรณ์จากระยะไกล เพื่อเข้าไปยังอุปกรณ์ที่ต้องการบริหารจัดการผ่านทางระบบเครือข่าย โดยที่ตัวอุปกรณ์เองต้องมีหมายเลข IP Address สำหรับบริหารจัดการและเชื่อมต่อกับระบบเครือข่ายจึงจะใช้งาน SSH ได้ วิธีการนี้แนะนำให้ใช้เป็นหลักหลังจากติดตั้งอุปกรณ์แล้ว เพื่อเข้าถึงอุปกรณ์เพราะมีความปลอดภัย เนื่องจากมีการเข้ารหัสข้อมูลที่ส่งผ่าน SSH

ค่าพื้นฐานที่จำเป็นสำหรับอุปกรณ์ที่จะนำไปติดตั้ง

ในการตั้งค่าอุปกรณ์ให้สามารถทำงานได้ตามที่ออกแบบไว้นั้น การตั้งค่าที่จำเป็นสำหรับอุปกรณ์ Switch มี 3 ส่วน ดังต่อไปนี้

1. Basic configuration เป็นค่าพื้นฐานสำหรับอุปกรณ์ทุกตัวต้องมีเพื่อใช้ในการทำงานของอุปกรณ์ให้เข้ากับระบบเครือข่าย CMU-NET2020 มีดังนี้

   a. **ตัวหนา** คือ คำสั่ง

   b. *ตัวเอียง* คือ ตัวแปรที่ต้องใส่

คำสั่ง	**การใช้งาน**
hostname *name* **ตัวอย่าง :** switch (config)# **hostname CMUNET** CMUNET (config)#	ตั้งชื่อของอุปกรณ์
Enable secret *phase* **ตัวอย่าง :** switch(config)# **enable secret cmunet@1**	ตั้งรหัสผ่านให้กับ enable mode ของอุปกรณ์
AAA new-model **ตัวอย่าง :** switch(config)# **AAA new-model**	เปิดการใช้งาน AAA
AAA authentication login default local group radius **ตัวอย่าง :** switch(config)# **AAA authentication login default local group radius**	ให้เลือกใช้ login โดยเรียงลำดับจาก Default , Local ,Group RADIUS

คำสั่ง	การใช้งาน
ip domain name *domain-name* **ตัวอย่าง :** switch(config)# **ip domain name cmu.ac.th**	ตั้งชื่อ domain-name ให้กับอุปกรณ์ จำเป็นต้องมีเพื่อให้สามารถทำ SSH ได้
no ip domain lookup **ตัวอย่าง :** switch(config)# **no ip domain lookup**	ปิดการค้นหาเมื่อพิมพ์คำที่ไม่ใช้คำสั่ง
vtp domain *name* **ตัวอย่าง :** switch(config)# **VTP domain CMUNET**	ตั้งชื่อให้กับ VTP domain
vtp mode *transparent* **ตัวอย่าง :** switch(config)# **VTP mode transparent**	ตั้งค่าสถานะของ VTP ให้เป็น transparent เพื่อไม่ให้อัพเดทค่า VLAN
username *username* **secret** *password* **ตัวอย่าง :** switch(config)# **username admin secret p@ssw0rd**	เพิ่มชื่อผู้ใช้งานที่สามารถเข้าถึงอุปกรณ์ได้
ip default-gateway *ip address* **ตัวอย่าง :** switch(config)# **ip default-gateway 192.168.0.1**	หมายเลข IP Address ของ gateway ให้อุปกรณ์ติดต่อกับเครือข่ายภายนอกเพื่อการบริหารจัดการ
no ip http server **ตัวอย่าง :** **switch(config)# no ip http server**	ปิดการใช้งานหน้าเว็บจากการเข้าถึงด้วย HTTP
no ip http secure-server **ตัวอย่าง :** **switch(config)# no ip http secure-server**	ปิดการใช้งานหน้าเว็บจากการเข้าถึงด้วย HTTPS
logging host *ip log server* **ตัวอย่าง :** switch(config)# **logging host 10.110.0.92**	เพิ่ม IP Address ของ Log server เพื่อให้อุปกรณ์ส่ง Log file ไปเก็บ
ntp server *ip address NTP Server* **ตัวอย่าง :** switch(config)# **ntp server 202.28.0.26**	เพิ่ม IP Address ของ NTP server เพื่อให้อุปกรณ์ตั้งเวลาให้ตรงกับอุปกรณ์อื่น ๆ ในระบบเครือข่าย

คำสั่ง	การใช้งาน
snmp-server community *community-string* **ตัวอย่าง :** switch(config)# **snmp-server community cmu01**	เปิดการใช้งาน SNMP เพื่อให้อุปกรณ์ส่งค่าสำหรับการมอนิเตอร์
banner motd *string* **ตัวอย่าง :** switch(config)# **banner motd ^C** ========== Chiang Mai University's properties Unauthorized access will be vigorously prosecuted **^C**	เพิ่มข้อความให้แสดงบนหน้าจอ SSH เมื่อมีการเข้าถึงอุปกรณ์จากระยะไกล

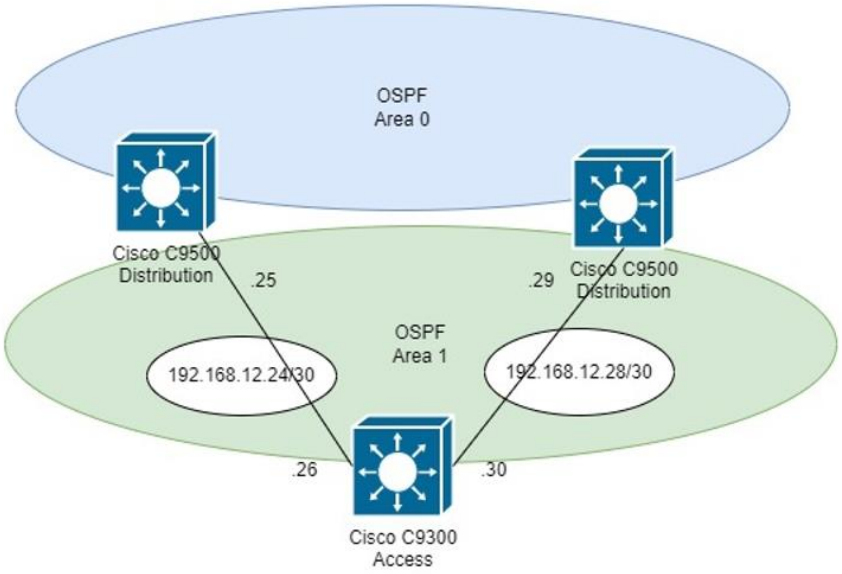
2. Routing configuration เป็นการตั้งค่าให้อุปกรณ์ แลกเปลี่ยนข้อมูลเส้นทางในการรับส่งข้อมูล ทำหลังจากตั้งค่าพื้นฐานเสร็จ

คำสั่ง	การใช้งาน
router ospf *process-id* Router-id *ip-Address* **ตัวอย่าง :** switch(config)# **router ospf 2020** switch(config-router)# **router-id 172.16.4.30** switch(config-router)# **redistribute static metric 100 metric-type 1** switch(config-router)# **passive-interface default** switch(config-router)# **no passive-interface TenGigabitEthernet1/1/1** switch(config-router)# **no passive-interface TenGigabitEthernet1/1/2**	เปิดการใช้งานโปรโทคอล OSPF และเข้าสู่โหมดการตั้งค่า Routing โปรโทคอล จากนั้นใส่ค่าต่าง ๆ ตามที่กำหนดไว้ **หมายเหตุ** Process-id ของแต่ละอุปกรณ์ควรตั้งเป็นเลขเดียว เพื่อให้ทราบถึงการทำงานร่วมกัน จากนั้น ตั้งค่า Router-id ของ OSPF Process โดยใช้หมายเลข Private IP Address จาก Subnet สำหรับกำหนดให้แก่อุปกรณ์ เพื่อให้ผู้ดูแลระบบสามารถเข้าถึงจากระยะไกลได้

3. Interface configuration เป็นการตั้งค่าให้กับ port หรือ Interface ที่ใช้เชื่อมต่ออุปกรณ์เข้าหากัน โดยที่ตั้งค่าเป็นราย port ตามที่ต้องการใช้งาน

คำสั่ง	การใช้งาน
interface *type number* **ip address** *ip-address mask* **ตัวอย่าง :** switch(config) # **interface loopback 0** switch(config-if) # **ip address 172.16.4.30 255.255.255.252** switch(config-if) # **ip ospf 2020 area 1**	เลือก Interface loopback 0 และเข้าสู่โหมดตั้งค่า Interface สังเกตได้จากข้อความ promt ขึ้นเป็น (config-if) จากนั้นกำหนดหมายเลข IP Address และ Subnet Mask โดยหมายเลข IP Address นี้จะใช้เป็น Router-id ในการตั้งค่า OSPF โปรโทคอลด้วย
switch(config) # **interface TenGigabitEthernet1/1/1** switch(config-if) **# ip address 192.168.12.26 255.255.255.252** switch(config-if) # **ip ospf authentication message-digest** switch(config-if) # **ip ospf message-digest-key 1 md5 xxxxxxxx** switch(config-if) # **ip ospf network point-to-point** switch(config-if) # **ip ospf 2020 area 1**	คำสั่งสำหรับ Interface ที่เชื่อมกับ Switch Distribute Layer จากภาพที่ 18 IP ที่ใช้เชื่อมต่อเป็น 192.168.12.26 และ 192.168.12.30 ตามตัวอย่างในภาพที่ 18

ตัวอย่างรูปแบบการเชื่อมต่อ Cisco C9300 กับ Distribution Layer

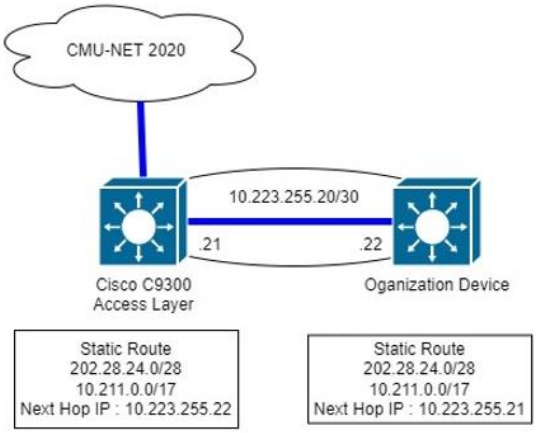


ภาพที่ 18 แผนผังการเชื่อมต่อ Switch Access Layer เข้ากับ Switch Distribution Layer

4. สำหรับการเชื่อมต่ออุปกรณ์กับหน่วยงานนั้น มีการตั้งค่าดังต่อไปนี้

คำสั่ง	การใช้งาน
switch(config) # **interface GigabitEthernet1/0/2** switch(config-if) **# ip address 10.223.255.21 255.255.255.252** switch(config-if) # **ip ospf 2020 area 1**	เลือก Interface ที่เชื่อมต่อกับอุปกรณ์ของหน่วยงาน ใส่ค่าหมายเลข IP Address และเปิดใช้งาน Routing Protocol OSPF
switch(config) # **ip route 10.211.0.0 255.255.128.0 10.223.255.22** switch(config) # **ip route 202.28.24.0 255.255.255.240 10.223.255.22**	Routing ด้วย Static Route ให้แก่ Subnet ที่จัดสรรให้แก่หน่วยงาน ทั้ง Private IP และ Public IP โดยชี้ปลายทางไปยัง IP Address ที่เชื่อมกับหน่วยงาน ตามตัวอย่างในภาพที่ 19

ตัวอย่างรูปแบบการเชื่อมต่อ Cisco C9300 กับหน่วยงาน



ภาพที่ 19 แผนผังการเชื่อมต่อระดับ Layer 3 ไปยังหน่วยงาน

4.2.3 การติดตั้งอุปกรณ์และเชื่อมต่อให้ใช้งาน CMU-NET 2020

เตรียมเครื่องมือติดตั้งให้พร้อม

a. ไขควง
b. น็อตยึดแรค
c. หูช้างสำหรับติดยึดแรค
d. กุญแจตู้แรค
e. คีมตัด
f. อุปกรณ์จัดสาย เช่น เคเบิ้ลไทล์, ตีนตุ๊กแก
g. คอมพิวเตอร์ทดสอบระบบ พร้อมสาย Console

ขั้นตอนการติดตั้งอุปกรณ์

1. เลือกตำแหน่งติดตั้งอุปกรณ์ภายในตู้แรค
2. ตรวจสอบปลั๊กรางภายในตู้แรค ว่าสามารถรองรับกระแสไฟเพียงพอหรือไม่
3. ระบุอุปกรณ์ระบบเครือข่ายปลายทางที่ต้องการเชื่อมต่อกับอุปกรณ์ใหม่
4. เลือกชนิดของสายสัญญาณที่ต้องการติดตั้ง
5. ตรวจสอบเส้นทางการเดินสัญญาณจากต้นทางจนถึงปลายทางว่าสามารถติดตั้งสายสัญญาณได้
6. หากไม่สามารถปฏิบัติข้อ 1- 5 ได้ ให้กลับไปทำข้อ 1 ใหม่
7. เมื่อตรวจทุกอย่างเรียบร้อยให้ดำเนินการติดตั้งอุปกรณ์เข้าไปในตู้แรคได้
8. เปิดใช้งานอุปกรณ์ที่ติดตั้งใหม่
9. เชื่อมต่อสายสัญญาณให้ตรงกับที่ตั้งแค่
10. รอจนอุปกรณ์เริ่มทำงาน

ขั้นตอนการปฏิบัติงานหลังจากติดตั้งอุปกรณ์ระบบเครือข่ายให้แก่หน่วยงาน

1. ทดสอบการใช้งานเบื้องต้นกับอุปกรณ์ที่ติดตั้งใหม่ให้ใช้งานได้
    1) Ping หมายเลขไอพีของอุปกรณ์
    2) เข้าถึงอุปกรณ์ด้วย SSH ตามที่อุปกรณ์ได้ตั้งค่าเอาไว้
    3) ตรวจสอบการใช้งานอินเทอร์เน็ตของระบบเครือข่ายของหน่วยงาน
    4) ตรวจสอบบริการต่าง ๆ ที่เชื่อมต่อมายังอุปกรณ์ ให้ใช้งานได้ ได้แก่
        a. ระบบเครือข่ายไร้สาย JumboPlus
        b. ระบบคอมพิวเตอร์ VDI
        c. ระบบเครือข่ายห้องสมุด
        d. ระบบดิจิทัลมิเตอร์และโซล่าเซลล์
2. จัดสายสัญญาณที่ติดตั้งใหม่ให้เป็นระเบียบ
3. เก็บเครื่องมือติดตั้งออกจากตู้แรค และทำความสะอาดบริเวณจุดติดตั้งให้เรียบร้อย
4. แจ้งข้อมูลของอุปกรณ์ที่ติดตั้งใหม่ให้กับเจ้าหน้าที่ในการติดตามการใช้งานอุปกรณ์ และบันทึกข้อมูลการติดตั้งลงระบบ IPAM

บทที่ 5
ปัญหาและแนวทางการแก้ไข

หลังจากการติดตั้งอุปกรณ์ และเชื่อมต่อสายสัญญาณเข้ากับอุปกรณ์ของหน่วยงาน มักเกิดปัญหาที่ทำให้ไม่สามารถใช้งานเกิดขึ้นกับระบบเครือข่าย

1. เชื่อมต่อกับหน่วยงานแล้ว Link ไม่ขึ้น สถานะ UP

หลังจากนำสายสัญญาณเชื่อมต่อกับอุปกรณ์แล้ว link ที่เป็นสายใยแก้วนำแสงมักไม่ UP ทั้งนี้มีหลายสาเหตุที่ทำให้เกิดปัญหานี้ ผู้ปฏิบัติงานสามารถตรวจได้

การแก้ไข

- ตรวจสอบ Module SFP สามารถเข้ากันได้กับอุปกรณ์หรือไม่ หากไม่เข้ากันให้เปลี่ยน
- ตรวจสอบสายสัญญาณใยแก้วนำแสงว่าเชื่อมต่อถูก Core หรือไม่ หากไม่ถูก ให้สลับซ้ายขวา

2. Link ขึ้นสถานะ UP แต่ไม่ขึ้น MAC Address ให้เห็นบนอุปกรณ์

เมื่อเชื่อมต่ออุปกรณ์แล้ว Link ขึ้นสถานะปกติแต่ไม่สามารถใช้งานได้ ให้ตรวจสอบ MAC Address ของแต่ละอุปกรณ์ว่าขึ้นหรือไม่

การแก้ไข

- หากไม่ขึ้นให้รีสตาร์ทอุปกรณ์

3. MAC Address ที่เห็นบนอุปกรณ์ของหน่วยงาน เป็น MAC Address เดิมของอุปกรณ์เก่า

เมื่อเปลี่ยนอุปกรณ์ใหม่ มีหลายครั้งที่อุปกรณ์เดิมในฝั่งที่ไม่ได้เปลี่ยนนั้นจำค่า MAC Address เดิมอยู่

การแก้ไข

- Clear ARP Table ของอุปกรณ์ เพื่อให้เห็น MAC Address ใหม่

4. Private IP ไม่สามารถใช้งานได้ หลังจาก NAT ด้วย Firewall ของหน่วยงาน

เมื่อเชื่อมต่ออุปกรณ์เรียบร้อยให้ ทดสอบการใช้งาน IP Address ที่ติดตั้ง บ่อยครั้งที่ Private IP Address ไม่สามารถใช้งานผ่านการ NAT ของ Firewall

การแก้ไข

- ทำ NAT Pool ให้เป็น Public IP แล้ว NAT ออกไป ตรวจสอบว่าไม่ใช่ Outgoing Interface

5. Firewall ไม่สามารถ Update ได้

เมื่อเชื่อมต่ออุปกรณ์เรียบร้อยให้ ทดสอบว่า Firewall สามารถเชื่อมต่อเครือข่ายภายในได้ แต่ Update ข้อมูลจาก Internet ไม่ได้

การแก้ไข

- ใช้ IP Source ของ Firewall เป็น Public IP