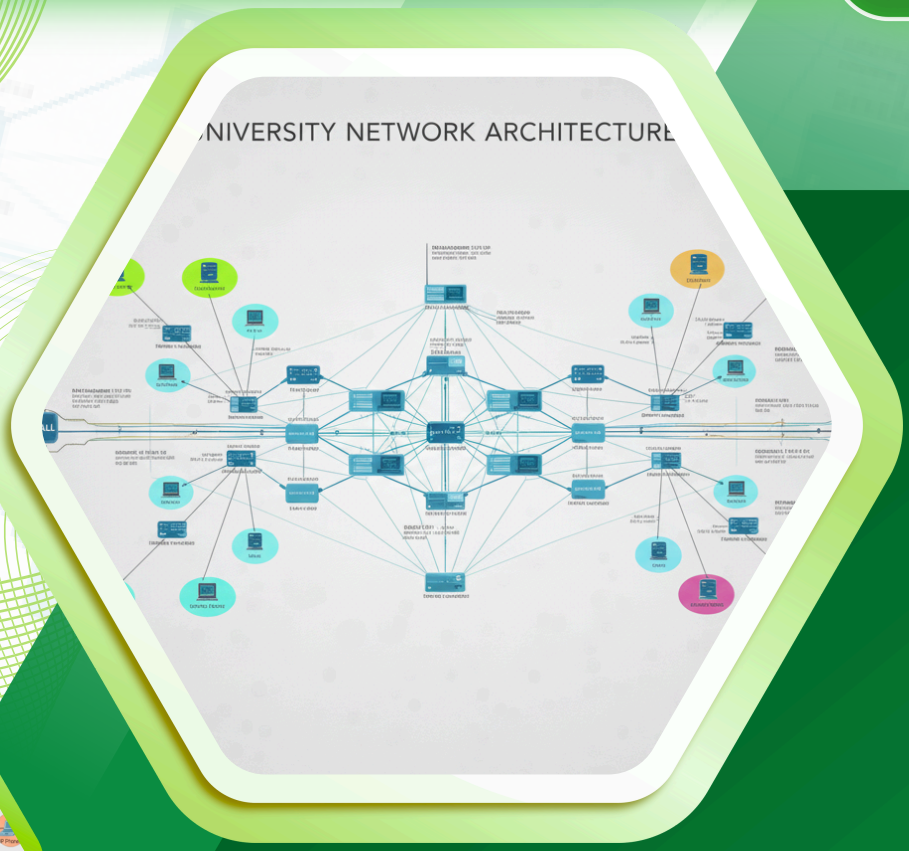
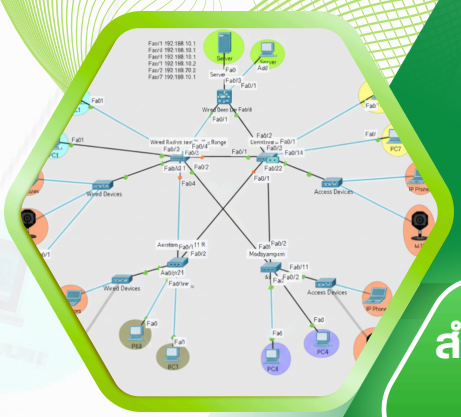
คู่มือปฏิบัติงาน

การเชื่อมต่อระบบเครือข่ายภายใน มหาวิทยาลัยราชภัฏชัยภูมิ

นายภัครพล อาจอาษา

นักวิชาการคอมพิวเตอร์ปฏิบัติการ





สำนักส่งเสริมวิชาการและจัดการเรียนรู้ตลอดชีวิต
มหาวิทยาลัยราชภัฏชัยภูมิ
พ.ศ. 2568

ผ่านการพิจารณากลั่นกรอง และนำไปใช้ประกอบการประชุม
คณะกรรมการประจำสำนักส่งเสริมวิชาการและจัดการเรียนรู้ตลอดชีวิต (สสร)
ในการประชุมครั้งที่ 4/2568 เมื่อวันที่ 3 กันยายน 2568

คำนำ

การจัดทำคู่มือการเชื่อมต่อระบบเครือข่ายภายใน มหาวิทยาลัยราชภัฏชัยภูมิ มีวัตถุประสงค์เพื่อเป็นคู่มือให้ผู้ดูแลระบบและผู้ปฏิบัติงานเกี่ยวกับระบบเครือข่ายของมหาวิทยาลัยราชภัฏชัยภูมิ ทราบถึงขั้นตอน วิธีปฏิบัติที่ถูกต้อง เข้าใจและปฏิบัติตามขั้นตอนการเชื่อมต่อเครือข่ายได้อย่างถูกต้อง มีประสิทธิภาพ และเป็นไปตามมาตรฐานความปลอดภัยทางด้านเครือข่ายคอมพิวเตอร์ รวมทั้งเพื่อใช้เป็นแนวทางในการศึกษาสำหรับเจ้าหน้าที่ที่ต้องปฏิบัติหน้าที่ในการให้บริการและแก้ไขปัญหา ในการดูแลระบบเครือข่าย สำหรับข้อมูลการจัดทำคู่มืออ้างอิงจากโครงสร้างพื้นฐานและระบบเครือข่ายที่มีการติดตั้งใช้งานอยู่ในปัจจุบัน โดยอาศัยประสบการณ์ในการดำเนินงานที่ผ่านมา ซึ่งในคู่มือได้จัดทำผังเครือข่ายของอาคารต่าง ๆ และอธิบายโครงสร้างพื้นฐานระบบเครือข่ายของมหาวิทยาลัย การดูผังเครือข่ายสำหรับผู้ที่ดูแลระบบจะมีความสะดวก รวดเร็วและเข้าใจความหมายได้ง่ายขึ้นเมื่ออ่านคำอธิบายประกอบ เพื่อให้ทุกฝ่ายที่เกี่ยวข้องรับทราบโครงสร้างระบบเครือข่าย อีกทั้งผู้จัดทำได้รวบรวมปัญหาพร้อมข้อเสนอแนะไว้ด้วย

ผู้จัดทำจึงหวังเป็นอย่างยิ่งว่า คู่มือฉบับนี้จะมีประโยชน์แก่ผู้ปฏิบัติงานในการให้บริการและแก้ไขปัญหาระบบเครือข่ายของมหาวิทยาลัย และผู้ที่เกี่ยวข้องนำไปใช้ประโยชน์ เพื่อช่วยในการปฏิบัติงานได้อย่างถูกต้องและมีประสิทธิภาพ ซึ่งหากคู่มือฉบับนี้มีข้อผิดพลาดประการใด ผู้จัดทำขอน้อมรับข้อผิดพลาดดังกล่าวเพื่อนำมาปรับปรุง พัฒนาคู่มือให้มีความครบถ้วนสมบูรณ์ต่อไป

ภัครพล อาจอาษา
นักวิชาการคอมพิวเตอร์ ปฏิบัติการ

สารบัญ

บทที่ 1
บทนำ

1. ความเป็นมาและความสำคัญ

ปัจจุบันเทคโนโลยีสารสนเทศได้เข้ามามีบทบาทในสังคมเป็นอย่างมากทั้งด้านการดำเนินชีวิตประจำวัน ด้านธุรกิจ ด้านสังคม โดยเฉพาะอย่างยิ่งด้านการศึกษา สถาบันการศึกษาทั่วโลกได้ให้ความสำคัญกับการพัฒนาเทคโนโลยีสารสนเทศให้แก่บัณฑิต เพื่อให้สามารถแข่งขันในเวทีระดับชาติ และเวทีโลกได้ ประกอบกับทุกสถาบันการศึกษามีการนำเทคโนโลยีสารสนเทศเข้ามาช่วยในการบริหารงาน พัฒนาการเรียนการสอน เพื่อให้มีความทันสมัย เพิ่มประสิทธิภาพการทำงาน ช่วยด้านการบริหาร การดำเนินการในหน่วยงาน และอำนวยความสะดวกในชีวิตประจำวัน โดยใช้เทคโนโลยีสารสนเทศในการบันทึกและจัดเก็บข้อมูล ประมวลผล แสดงผล และการสื่อสารผ่านช่องทางต่างๆผ่านระบบเครือข่าย

ระบบเครือข่ายอินเทอร์เน็ตจึงเป็นกลไกสำคัญในการช่วยสนับสนุนด้านการค้นคว้าข้อมูล และเชื่อมโยงระบบสารสนเทศต่าง ๆเข้าด้วยกัน ปัจจุบันมหาวิทยาลัยราชภัฏชัยภูมิกำลังอยู่ในระหว่างการพัฒนาด้านระบบเครือข่าย โดยมีการปรับปรุงระบบเครือข่าย อุปกรณ์และสายสัญญาณอยู่บ่อยครั้ง ทำให้เอกสารที่มีอยู่ไม่เป็นปัจจุบัน ประกอบกับยังไม่มีผังเครือข่ายประจำแต่ละอาคาร ผู้จัดทำจึงเห็นว่าควรจะรวบรวมข้อมูลผังเครือข่าย อุปกรณ์และสายสัญญาณมาไว้รวมกันและจัดทำให้เป็นปัจจุบัน เพื่อที่จะทำให้สามารถนำมาใช้แก้ไขปัญหาได้รวดเร็วและมีประสิทธิภาพ ทำให้การดำเนินงานมีมาตรฐานเพิ่มขึ้น และเพื่อเป็นประโยชน์ให้กับผู้ที่มาช่วยดูแลระบบเครือข่ายเพิ่มเติมในอนาคตต่อไป

2. วัตถุประสงค์ของการจัดทำคู่มือ

2.1. เพื่อให้ผู้ดูแลและปฏิบัติงานที่เกี่ยวข้องกับระบบเครือข่ายสามารถทำงานแทนกันได้

2.2. เพื่อให้ผู้ดูแลและปฏิบัติงานที่เกี่ยวข้องกับระบบเครือข่ายสามารถแก้ไขปัญหาได้อย่างรวดเร็ว

2.3. เพื่อช่วยสร้างความเข้าใจที่ชัดเจน และระบุรายละเอียดงานระบบเครือข่ายได้ครบถ้วนและลดระยะเวลาในการถ่ายทอดงาน

2.4. เพื่อใช้เป็นเอกสารอ้างอิงในการทำงาน

3. ประโยชน์ที่ได้รับ

3.1 เพิ่มประสิทธิภาพในการปฏิบัติงาน ช่วยให้เจ้าหน้าที่และผู้ที่เกี่ยวข้องกับการดูแลระบบเครือข่ายคอมพิวเตอร์สามารถทำงานได้อย่างมีประสิทธิภาพมากขึ้น โดยทราบขั้นตอน วิธีการปฏิบัติงาน และแนวทางการแก้ไขปัญหาที่ชัดเจน

3.2 สร้างความเข้าใจในโครงสร้างระบบ ช่วยให้ผู้ปฏิบัติงานเห็นภาพรวมของโครงสร้างพื้นฐานระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยทั้งหมด ทำให้การบริหารจัดการเป็นไปอย่างเป็นระบบ

3.3 รองรับการทำงานทดแทนกันและลดระยะเวลาถ่ายทอดงาน คู่มือนี้ช่วยให้ผู้ดูแลระบบสามารถ

ทำงานแทนกันได้เมื่อจำเป็น และช่วยลดระยะเวลาในการสอนงานหรือถ่ายทอดงานให้กับบุคลากรใหม่

3.4 ใช้เป็นเอกสารอ้างอิงในการทำงาน สามารถใช้เป็นเอกสารมาตรฐานสำหรับอ้างอิงในการปฏิบัติงานของผู้บริหาร ผู้ประสานงาน และนักวิชาการคอมพิวเตอร์จากฝ่ายต่าง ๆ เพื่อให้การดำเนินงานมีมาตรฐานเดียวกัน

3.5 แก้ไขปัญหาได้อย่างรวดเร็วและแม่นยำ การมีข้อมูลผังเครือข่าย อุปกรณ์ และสายสัญญาณที่เป็นปัจจุบัน ช่วยให้เมื่อเกิดปัญหาขึ้น ผู้ดูแลสามารถนำข้อมูลมาใช้ตรวจสอบและแก้ไขปัญหาได้อย่างรวดเร็วและมีประสิทธิภาพ

4. ขอบเขตของคู่มือ

คู่มือปฏิบัติงานการดูแลระบบเครือข่ายฉบับนี้ครอบคลุม โครงสร้างระบบเครือข่ายของมหาวิทยาลัยทุกอาคาร โดยไม่ระบุไอพีแอดเดรสของอุปกรณ์ตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ แนวการเชื่อมต่อสายสัญญาณ ขั้นตอนการแก้ปัญหา กลุ่มคำสั่งที่ใช้งานบ่อยของปกรณ์เครือข่ายที่ใช้งาน เครื่องมือที่ช่วยในการทำงานแก้ไขปัญหา การดำเนินการของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

5. คำจำกัดความเบื้องต้น

5.1 ระบบเครือข่าย ถือเป็นหัวใจสำคัญของการสื่อสารและการประมวลผลข้อมูลขององค์กร ซึ่งต้องให้ความสำคัญกับความปลอดภัย เสถียรภาพ และการจัดการแบนด์วิดท์ให้เหมาะสมตามนโยบาย

5.2 การรักษาความปลอดภัย (Security) คือพื้นฐานการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เพื่อคงไว้ซึ่งความลับ (Confidentiality) ความถูกต้อง (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูล

5.3 ความเสถียรของระบบ (Stability) การออกแบบระบบให้รองรับการใช้งานต่อเนื่อง โดยมีเป้าหมายความพร้อมใช้งาน (Uptime) ไม่น้อยกว่า 99.5%

5.4 การจัดสรรหมายเลขไอพี (IP Address Allocation) การกำหนดที่อยู่ IP ภายในให้อยู่ในช่วงเครือข่ายส่วนตัว (Private Network) เช่น 192.168.x.x หรือ 10.x.x.x เพื่อไม่ให้ขัดแย้งกับเครือข่ายสาธารณะ

5.5 มาตรฐานทางเทคนิค (Technical Standards) การปฏิบัติงานต้องยึดตามมาตรฐานสากล เช่น IEEE 802.3 สำหรับเครือข่ายแบบสาย และ IEEE 802.11 สำหรับเครือข่ายไร้สาย

5.6 การบำรุงรักษาเชิงป้องกัน (Preventive Maintenance): การวางแผนตรวจสอบและดูแลระบบอย่างสม่ำเสมอตามระยะเวลาที่กำหนด (รายสัปดาห์, เดือน, ไตรมาส, ปี) เพื่อป้องกันปัญหาก่อนที่จะเกิดขึ้น

บทที่ 2
โครงสร้างองค์กร และบทบาทหน้าที่ความรับผิดชอบ

2.1 ความเป็นมาของหน่วยงาน

สำนักส่งเสริมวิชาการและจัดการเรียนรู้ตลอดชีวิต จัดตั้งตามตามกฎกระทรวง จัดตั้งส่วนราชการในมหาวิทยาลัยราชภัฏชัยภูมิ กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม พ.ศ. 2566 โดยให้ยกเลิกกฎกระทรวงจัดตั้งส่วนราชการในมหาวิทยาลัยราชภัฏชัยภูมิ กระทรวงศึกษาธิการ พ.ศ. 2548 และให้จัดตั้ง “คณะครุศาสตร์และการพัฒนามนุษย์” และ “สำนักส่งเสริมวิชาการและจัดการเรียนรู้ตลอดชีวิต” เป็นส่วนราชการในมหาวิทยาลัยราชภัฏชัยภูมิ กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม ตามประกาศราชกิจจานุเบกษา เล่ม 140 ตอนที่ 68 ก ลงวันที่ 6 ธันวาคม 2566 โดยให้มีผลในวันที่กฎกระทรวงจัดตั้งส่วนราชการดังกล่าวมีผลใช้บังคับตามนัย มาตรา 6 แห่งพระราชบัญญัติมหาวิทยาลัยราชภัฏ พ.ศ. 2547

สำนักส่งเสริมวิชาการและจัดการเรียนรู้ตลอดชีวิต เป็นสำนักที่มีลักษณะบูรณาการตามนโยบายการจัดการศึกษารูปแบบใหม่ มีพันธกิจสอดคล้องกับบริบทใหม่ ของมหาวิทยาลัยราชภัฏชัยภูมิในกลุ่มการพัฒนาชุมชนเชิงพื้นที่ (Area-Based and Community Engagement) ที่มุ่งเน้นการสร้างและพัฒนาบุคลากรที่มีทักษะสูงตามความต้องการของท้องถิ่น พัฒนาท้องถิ่นด้วยองค์ความรู้และนวัตกรรม หน่วยงานนี้จะสามารถสนับสนุนมหาวิทยาลัยราชภัฏชัยภูมิให้เอื้อต่อการผลิตและพัฒนาบัณฑิตที่มีคุณภาพสูง มีภารกิจรับผิดชอบแผนการผลิตกำลังคนให้สอดคล้องกับศักยภาพของสถาบันอุดมศึกษาและความต้องการ ในการพัฒนาประเทศและส่งเสริมการพัฒนาคุณภาพนักศึกษา เสริมสร้างความรู้และทักษะทางอาชีพให้พร้อมรองรับการเปลี่ยนแปลงที่จะเกิดขึ้นในอนาคต พร้อมตอบสนองการผลิตกำลังคนแบบ Lifelong learning ตลอดจนการจัดการฝึกอบรมที่เน้นการ Up skill -Re skill เพื่อพัฒนาสมรรถนะกลุ่มบุคคลในทุกช่วงวัยให้เกิดการเรียนรู้ตลอดชีวิตด้วยองค์ความรู้ต่าง ๆ ของมหาวิทยาลัยราชภัฏชัยภูมิ ที่ทันสมัยและนำไปใช้ประโยชน์ได้จริง ส่งเสริมการสร้างนวัตกรรมการศึกษา (Sandbox) มีระบบสะสมหน่วยการเรียนเพื่อเทียบโอน (Credit Bank) การจัดการศึกษาแบบ Module Block Course มีการจัดการศึกษาแบบยืดหยุ่น ขับเคลื่อนและมุ่งเน้นการเรียนตลอดชีวิต

งานวิทยบริการและเทคโนโลยีสารสนเทศ สำนักส่งเสริมวิชาการและจัดการเรียนรู้ตลอดชีวิต มหาวิทยาลัยราชภัฏชัยภูมิ ได้จัดตั้งขึ้นตามพระราชบัญญัติมหาวิทยาลัยราชภัฏ พ.ศ. 2547 หมวด 1 ตามมาตรา 7 บัญญัติให้มหาวิทยาลัยราชภัฏชัยภูมิเป็นสถาบันอุดมศึกษาเพื่อการพัฒนาท้องถิ่นที่เสริมสร้างพลังปัญญาของแผ่นดิน มาตรา 8 ได้กำหนดภาระหน้าที่ของมหาวิทยาลัยราชภัฏชัยภูมิ (จำนวน 8 ข้อ) ใน (1) แสวงหาความจริงเพื่อสู่ความเป็นเลิศทางวิชาการ บนพื้นฐานของภูมิปัญญาท้องถิ่น ภูมิปัญญาไทย และภูมิปัญญาสากล (3) เสริมสร้างความรู้ความเข้าใจในคุณค่า ความสำนึก และความภูมิใจในวัฒนธรรมของท้องถิ่นและของชาติ (6) ประสานความร่วมมือและช่วยเหลือเกื้อกูลกันระหว่างมหาวิทยาลัย ชุมชนองค์กรปกครอง

ส่วนท้องถิ่นและองค์กรอื่นทั้งในและต่างประเทศ เพื่อการพัฒนาท้องถิ่น (8) ศึกษา วิจัย ส่งเสริมและสืบสานโครงการอันเนื่องมาจากแนวพระราชดำริในการปฏิบัติภารกิจของมหาวิทยาลัยเพื่อการพัฒนาท้องถิ่น ครอบคลุมภารกิจหลักในการสนับสนุนการเรียนการสอนและการวิจัย โดยด้านวิทยบริการจะมุ่งเน้นการจัดหาและจัดการระบบทรัพยากรสารสนเทศ ทั้งหนังสือ วารสาร และสื่อการเรียนรู้ดิจิทัล พร้อมให้บริการยืม-คืน และสืบค้นข้อมูลแก่ผู้ใช้บริการ ในขณะที่ด้านเทคโนโลยีสารสนเทศจะรับผิดชอบการพัฒนาและบริหารจัดการระบบสารสนเทศห้องสมุด ดูแลโครงสร้างพื้นฐานเครือข่ายอินเทอร์เน็ต คอมพิวเตอร์ และอุปกรณ์โสตทัศนูปกรณ์ รวมถึงการรักษาความปลอดภัยของข้อมูลและพัฒนาแอปพลิเคชันเพื่อการบริการ นอกจากนี้ยังทำหน้าที่ประสานงาน วางแผนนโยบายการให้บริการ และให้คำปรึกษาด้านการจัดการข้อมูลและการอ้างอิงเพื่อสนับสนุนงานวิชาการอย่างมีประสิทธิภาพ

2. ปรัชญา วิสัยทัศน์ พันธกิจ

ปรัชญา (Philosophy)

“สำนักส่งเสริมวิชาการและจัดการเรียนรู้ตลอดชีวิต เป็นองค์กรขับเคลื่อนการบริการวิชาการ วิจัย และนวัตกรรม เพื่อการเรียนรู้ตลอดชีวิต”

วิสัยทัศน์ (Vision)

เป็นองค์กรสมรรถนะสูงในการขับเคลื่อนภารกิจด้านการบริการวิชาการ วิจัย นวัตกรรม และจัดการเรียนรู้ตลอดชีวิต เพื่อตอบสนองความต้องการของชุมชนท้องถิ่น

พันธกิจ (Mission)

1. ส่งเสริมการผลิตบัณฑิตที่มีคุณภาพได้มาตรฐานและเป็นที่ต้องการของตลาดแรงงาน
2. บริหารจัดการงานวิจัยและนวัตกรรมให้มีประสิทธิภาพตอบ สนองต่อยุทธศาสตร์การวิจัยและการบริการทางวิชาการของมหาวิทยาลัย
3. ให้บริการวิชาการ ถ่ายทอดเทคโนโลยีและสืบสานโครงการอันเนื่องมาจากแนวพระราชดำริเพื่อให้เกิดความเข้มแข็งของท้องถิ่น
4. จัดบริการวิชาการ ฝึกอบรม (Reskill & Upskill) และให้ บริการที่ปรึกษาแก่หน่วยงานภายในและภายนอกมหาวิทยาลัย
5. บูรณาการการพัฒนาชุมชนเชิงพื้นที่ (Area-Base and community engagement) ตามบริบทท้องถิ่น
6. พัฒนาระบบเทคโนโลยีสารสนเทศ (ICT) เพื่อเพิ่มประสิทธิภาพงานและเสริมสร้างทักษะการใช้เทคโนโลยีสารสนเทศ
7. อนุรักษ์ ฟื้นฟู ส่งเสริม สืบสานและสร้างคุณค่าทางศิลปวัฒนธรรมและภูมิปัญญาท้องถิ่น

8. สร้างเครือข่ายความร่วมมือและบริการวิชาการกับหน่วยงานภายในและภายนอกมหาวิทยาลัย

ประเด็นยุทธศาสตร์ของสำนักฯ

ประเด็นยุทธศาสตร์ที่ 1 พัฒนาองค์กรสมรรถนะสูง
ประเด็นยุทธศาสตร์ที่ 2 พัฒนาหลักสูตรการเรียนการสอน
ประเด็นยุทธศาสตร์ที่ 3 พัฒนาการบริการวิชาการ วิจัยและศิลปวัฒนธรรม
ประเด็นยุทธศาสตร์ที่ 4 การเรียนรู้ตลอดชีวิต

3. โครงสร้างหน่วยงาน

ภาพที่ 2.1 โครงสร้างองค์กร

4. บทบาทหน้าที่ความรับผิดชอบ (งานวิทยบริการและเทคโนโลยีสารสนเทศ)

4.1. หน่วยวิทยบริการ (ห้องสมุด, Co-working & Learning Space)

1) เน้นการเป็นศูนย์กลางทรัพยากรสารสนเทศและพื้นที่แห่งการเรียนรู้

2) การบริหารจัดการทรัพยากรสารสนเทศ จัดหา คัดเลือก วิเคราะห์เลขหมู่ และทำรายการทรัพยากรสารสนเทศ ทั้งในรูปแบบรูปเล่ม (Books) และสื่ออิเล็กทรอนิกส์ (E-Resources) ให้ทันสมัย

3) งานบริการยืม-คืน จัดระบบการยืม-คืนทรัพยากร และการใช้บริการระหว่างห้องสมุด เพื่ออำนวยความสะดวกแก่ผู้ใช้บริการ

4) การบริหารจัดการพื้นที่ (Learning Space) ดูแลและจัดสรรพื้นที่ Co-working space ให้พร้อมสำหรับการเรียนรู้ด้วยตนเอง การทำงานกลุ่ม และกิจกรรมเชิงสร้างสรรค์

5) บริการตอบคำถามและช่วยการค้นคว้า ให้คำแนะนำในการสืบค้นข้อมูลเพื่อการวิจัยและการเรียนการสอน รวมถึงการจัดอบรมทักษะการรู้สารสนเทศ (Information Literacy)

6) การจัดกิจกรรมส่งเสริมการเรียนรู้ จัดนิทรรศการ เสวนา หรือ Workshop เพื่อกระตุ้นนิสัยรักการอ่านและการเรียนรู้ตลอดชีวิต

4.2. หน่วยเทคโนโลยีสารสนเทศ (IT)

1) เน้นการวางรากฐานโครงสร้างพื้นฐานดิจิทัลและความปลอดภัยทางข้อมูล

2) การดูแลโครงสร้างพื้นฐานเครือข่าย บริหารจัดการระบบเครือข่ายอินเทอร์เน็ต (Wi-Fi/LAN) และระบบ Server ให้มีความเสถียรและพร้อมใช้งานตลอดเวลา

3) การพัฒนาและดูแลระบบสารสนเทศ พัฒนาและบำรุงรักษาเว็บไซต์ แอปพลิเคชัน หรือซอฟต์แวร์ภายในองค์กร เพื่อสนับสนุนการทำงานและการบริการ

4) งานบริการสนับสนุนด้านเทคนิค (Helpdesk) ให้คำปรึกษา แก้ไขปัญหาการใช้งานคอมพิวเตอร์ อุปกรณ์พกพา และซอฟต์แวร์พื้นฐานให้แก่บุคลากรและนักศึกษา

5) การรักษาความมั่นคงปลอดภัยไซเบอร์ เฝ้าระวังภัยคุกคามทางไซเบอร์ สำรองข้อมูลสำคัญ (Backup) และกำหนดสิทธิ์การเข้าถึงข้อมูลตามมาตรฐานความปลอดภัย

6) การบริหารจัดการครุภัณฑ์คอมพิวเตอร์ วางแผนการจัดซื้อ ตรวจรับ และบำรุงรักษาอุปกรณ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงให้อยู่ในสภาพดี

4.3. หน่วยโสตทัศนูปกรณ์ (Audio-Visual Unit)

1) เน้นการสนับสนุนสื่อมัลติมีเดีย การถ่ายทำ และระบบงานกิจกรรม

2) บริการระบบเสียงและภาพ ควบคุมและดูแลระบบเครื่องเสียง จอภาพ และโปรเจกเตอร์ ในห้องเรียน ห้องประชุม และพื้นที่จัดกิจกรรมต่าง ๆ

3) การผลิตสื่อมัลติมีเดีย ถ่ายภาพนิ่ง บันทึกวิดีโอ และตัดต่อสื่อประชาสัมพันธ์ หรือสื่อการเรียนการสอนออนไลน์ (E-Learning Material)

4) บริการถ่ายทอดสด (Live Streaming) จัดเตรียมระบบและดำเนินการถ่ายทอดสดกิจกรรมทางวิชาการหรืองานสำคัญผ่านช่องทางออนไลน์

5) การดูแลรักษาอุปกรณ์โสตฯ ตรวจสอบและบำรุงรักษา กล้องถ่ายรูป ไมโครโฟน ลำโพง และอุปกรณ์ตัดต่อให้พร้อมใช้งาน

6) การให้คำปรึกษาด้านสื่อ ให้คำแนะนำแก่บุคลากรในการเลือกใช้เครื่องมือและเทคนิคด้านสื่อเพื่อการนำเสนอหรือการสื่อสารที่มีประสิทธิภาพ

บทที่ 3
หลักเกณฑ์ วิธีการ และเงื่อนไขการปฏิบัติงาน

3.1หลักเกณฑ์การเชื่อมต่อระบบเครือข่ายภายใน

3.1.1 หลักเกณฑ์ทั่วไป ระบบเครือข่ายถือเป็นหัวใจสำคัญของการสื่อสารและการประมวลผลข้อมูลขององค์กร การกำหนดหลักเกณฑ์ความปลอดภัยและเสถียรภาพของระบบจึงเป็นสิ่งจำเป็น โดยประเด็นสำคัญที่ต้องคำนึงถึงประการแรกคือ การรักษาความปลอดภัยของระบบเครือข่าย ซึ่งเป็นพื้นฐานในการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต องค์กรต้องมีมาตรการควบคุมการเข้าถึงที่ชัดเจน เช่น การยืนยันตัวตนผู้ใช้งาน การเข้ารหัสข้อมูล และการใช้ระบบ Firewall หรือ IDS/IPS เพื่อเฝ้าระวังการบุกรุกและลดความเสี่ยงจากภัยคุกคามไซเบอร์ ทั้งนี้เพื่อคงไว้ซึ่งความลับ (Confidentiality) ความถูกต้อง (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูล ประการที่สองคือ ความเสถียรของระบบเครือข่าย ที่ต้องออกแบบให้รองรับการใช้งานได้อย่างต่อเนื่อง โดยมีเป้าหมายความพร้อมใช้งานไม่น้อยกว่า 99.5% uptime ซึ่งหมายถึงระบบต้องมีการสำรองอุปกรณ์ (Redundancy) และมีการวางแผนกู้คืนระบบ (Disaster Recovery Plan) เพื่อรองรับความผิดพลาดหรือเหตุการณ์ไม่คาดคิดได้อย่างทันท่วงที ประการที่สามคือ การจัดการแบนด์วิดท์และทรัพยากรเครือข่าย การใช้งานเครือข่ายต้องเป็นไปตามนโยบายที่องค์กรกำหนด โดยมีการกำหนดลำดับความสำคัญของการใช้งาน (QoS: Quality of Service) เพื่อให้บริการที่สำคัญสามารถเข้าถึงแบนด์วิดท์ได้อย่างเหมาะสม และป้องกันการใช้งานที่ไม่เป็นประโยชน์ต่อองค์กร เช่น การดาวน์โหลดข้อมูลส่วนบุคคลปริมาณมาก หรือการใช้งานที่ก่อให้เกิดความแออัดในเครือข่าย และสุดท้ายประการที่สี่คือ การปฏิบัติตามมาตรฐานทางเทคนิค เพื่อให้ระบบเครือข่ายมีคุณภาพและความน่าเชื่อถือในระดับสากล โดยควรยึดตามมาตรฐานที่ได้รับการยอมรับ เช่น IEEE 802.3 สำหรับระบบเครือข่ายสาย, IEEE 802.11 สำหรับระบบเครือข่ายไร้สาย และมาตรฐานด้านการจัดการความมั่นคงปลอดภัยสารสนเทศ การนำมาตรฐานเหล่านี้มาใช้จะช่วยให้องค์กรมีระบบที่ได้มาตรฐานปลอดภัย และสามารถตรวจสอบได้

3.1.2 หลักเกณฑ์การจัดสรรหมายเลขที่อยู่ประจำเครื่อง (IP Address) การจัดสรรที่อยู่ IP ภายในเครือข่ายมหาวิทยาลัย ควรต้องดำเนินการตามหลักเกณฑ์ที่ชัดเจนเพื่อให้เกิดความเป็นระเบียบ มีประสิทธิภาพ และง่ายต่อการบริหารจัดการ โดยเริ่มจากการกำหนด IP Address Range ให้อยู่ในช่วง Private Network เช่น 192.168.x.x หรือ 10.x.x.x เพื่อให้มั่นใจในการใช้งาน IP ภายในจะไม่ขัดแย้งกับเครือข่ายสาธารณะ จากนั้นใช้ระบบ DHCP ในการจัดสรร IP แบบอัตโนมัติให้กับผู้ใช้งานทั่วไป โดยแบ่งตามส่วนงานหรือคณะ หรือตึกสำนักงาน เพื่อช่วยลดภาระของผู้ดูแลระบบและป้องกันการซ้ำซ้อนของที่อยู่ IP ในขณะเดียวกัน อุปกรณ์ที่มีความสำคัญ เช่น เครื่องคอมพิวเตอร์แม่ข่ายหลัก ระบบเครือข่ายหลัก อุปกรณ์รักษาความปลอดภัย หรืออุปกรณ์ที่ต้องให้บริการต่อเนื่อง ควรได้รับการกำหนดไอพีแบบ Static IP เพื่อให้สามารถเข้าถึงได้อย่างแน่นอนและไม่เปลี่ยนแปลง นอกจากนี้ควรมีการใช้ VLAN Segmentation เพื่อแยกการจราจรตามประเภทผู้ใช้งาน เช่น บุคลากร นักศึกษา และอุปกรณ์ IoT ระบบ CCTV เพื่อเพิ่มความปลอดภัย ลดปัญหาความหนาแน่นของการรับส่งข้อมูล และทำให้การบริหารจัดการเครือข่ายมีประสิทธิภาพมากยิ่งขึ้น

3.1.3 หลักเกณฑ์การรักษาความปลอดภัย การรักษาความปลอดภัยของระบบเครือข่ายจำเป็นต้องอาศัยมาตรการที่รัดกุมและเป็นระบบ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตและลดความเสี่ยงจากภัยคุกคามไซเบอร์ หลักเกณฑ์สำคัญที่ควรดำเนินการ เช่น การยืนยันตัวตนแบบ Captive Portal การยืนยันตัวตนผู้ใช้งานด้วย 802.1X Authentication ซึ่งช่วยตรวจสอบสิทธิ์การเชื่อมต่อกับเครือข่ายทั้งแบบมีสายและไร้สายได้อย่างปลอดภัย สำหรับระบบเครือข่ายไร้สายเพื่อเพิ่มความปลอดภัยในการเชื่อมต่อ และใช้ SSL/TLS สำหรับ Web Services เพื่อรักษาความลับและความถูกต้องของข้อมูลในระหว่างการรับส่งผ่านอินเทอร์เน็ต ในด้านการควบคุมการเข้าถึง กำหนด Firewall Rules โดยอิงตามหลักการ Principle of Least Privilege คืออนุญาตให้เข้าถึงเฉพาะสิ่งที่จำเป็นต่อการปฏิบัติงานเท่านั้น เพื่อลดโอกาสที่ผู้ไม่หวังดีจะใช้ช่องทางเครือข่ายเข้ามาโจมตี และใช้ Access Control List (ACL) เพื่อกำหนดสิทธิ์การเข้าถึงทรัพยากรเครือข่ายอย่างละเอียด เช่น การกำหนดสิทธิ์ตามกลุ่มผู้ใช้งาน ประเภทอุปกรณ์ หรือโปรโตคอลที่อนุญาตให้ใช้งานได้ ทั้งหมดนี้จะช่วยสร้างระบบเครือข่ายที่มีความมั่นคงปลอดภัย ป้องกันการบุกรุก และรองรับการใช้งานอย่างมีประสิทธิภาพในระยะยาว

3.2 วิธีการเชื่อมต่อระบบเครือข่าย

3.2.1 การเชื่อมต่อแบบสายเคเบิล (Wired Connection)

การตรวจสอบโครงสร้างพื้นฐาน การตรวจสอบโครงสร้างพื้นฐานเครือข่ายถือเป็นขั้นตอนสำคัญในการประเมินคุณภาพและความพร้อมใช้งานของระบบ เพื่อให้มั่นใจว่าอุปกรณ์และสายสัญญาณสามารถรองรับการรับส่งข้อมูลได้อย่างมีประสิทธิภาพ โดยมาตรการหลักที่ควรดำเนินการ ได้แก่ การตรวจสอบการเดินสายเคเบิลชนิด Cat 6 ,Cat 6A หรือ Cat5 ว่ามีการติดตั้งตามมาตรฐาน ทั้งในด้านเส้นทางการเดินสาย ความเรียบร้อย และการหลีกเลี่ยงสัญญาณรบกวนจากแหล่งกำเนิดไฟฟ้าหรืออุปกรณ์อื่น ๆ จากนั้นควรทำการทดสอบความถูกต้องของหัวต่อ RJ-45 Connector โดยตรวจสอบการเข้าหัวตามมาตรฐานสายตรง (Straight-Through) หรือสายไขว้ (Cross-Over) ให้ถูกต้องตามคู่สายที่กำหนด เพื่อลดปัญหาการเชื่อมต่อหรือสัญญาณขาดหายระหว่างอุปกรณ์ สุดท้ายคือการ วัดความยาวสายและค่าการสูญเสียสัญญาณ (Signal Loss) โดยใช้เครื่องมือวิเคราะห์สาย (Cable Tester) เพื่อยืนยันว่าสายมีความยาวไม่เกินมาตรฐานที่กำหนด (ไม่เกิน 100 เมตรต่อเส้น) และมีค่าการสูญเสียสัญญาณในเกณฑ์ที่ยอมรับได้ ทั้งนี้เพื่อให้เครือข่ายสามารถทำงานได้อย่างเต็มประสิทธิภาพและรองรับความเร็วการเชื่อมต่อในระดับ Gigabit หรือสูงกว่า

การกำหนดค่าอุปกรณ์เครือข่าย การตั้งค่า Network Switch เป็นขั้นตอนสำคัญในการบริหารจัดการเครือข่ายให้มีประสิทธิภาพ ปลอดภัย และสามารถรองรับผู้ใช้งานได้ตามความต้องการ โดยประเด็นหลักที่ควรดำเนินการ ได้แก่ การกำหนด VLAN (Virtual LAN) เพื่อแยกกลุ่มการจราจรของเครือข่ายตามประเภทผู้ใช้งานหรือหน่วยงาน ช่วยเพิ่มความปลอดภัย ลดการชนกันของข้อมูล (Collision) และเพิ่มประสิทธิภาพการส่งผ่านข้อมูล จากนั้นควรกำหนด Port Configuration ให้เหมาะสม เช่น การตั้งค่า Access Port สำหรับอุปกรณ์ปลายทาง และ Trunk Port สำหรับเชื่อมต่อระหว่าง Switch หลายตัว รวมถึงการเปิดใช้

งานฟีเจอร์ด้านความปลอดภัย เช่น Port Security เพื่อป้องกันการเชื่อมต่ออุปกรณ์ที่ไม่ได้รับอนุญาต นอกจากนี้ ควรมีการ ทดสอบ Link Speed และ Duplex Mode ของแต่ละพอร์ต เพื่อให้มั่นใจว่าอุปกรณ์ปลายทางสามารถทำงานได้ตามมาตรฐาน เช่น 1 Gbps หรือ 10 Gbps และอยู่ในโหมด Full Duplex เพื่อให้การสื่อสารทั้งขาเข้าและขาออกทำได้พร้อมกันโดยไม่เกิดการชนกันของแพ็กเก็ต หากพบปัญหาความไม่สอดคล้อง (Mismatch) เช่น การเชื่อมต่ออยู่ในโหมด Half Duplex ควรปรับแก้ไขให้ถูกต้อง เพื่อหลีกเลี่ยงปัญหาความหน่วง (Latency) หรือการสูญหายของข้อมูล การตั้งค่าเหล่านี้จะช่วยให้เครือข่ายทำงานได้อย่างมีประสิทธิภาพ มั่นคง และรองรับการขยายตัวของระบบในอนาคต

การกำหนดค่าผู้ใช้งาน การกำหนดค่าผู้ใช้งาน (User Configuration) ในระบบเครือข่ายเป็นขั้นตอนสำคัญที่ช่วยให้การเข้าถึงทรัพยากรเครือข่ายมีความเป็นระเบียบ ปลอดภัย และสามารถควบคุมได้อย่างเหมาะสม โดยหลักเกณฑ์ทั่วไปเริ่มจากการสร้าง บัญชีผู้ใช้งาน (User Account Management) ให้สอดคล้องกับสิทธิ์และบทบาทหน้าที่ เช่น แบ่งเป็นกลุ่มผู้ดูแลระบบ (Administrator), บุคลากร, นักศึกษา หรือแขกผู้มาใช้งาน (Guest) จากนั้นกำหนด สิทธิ์การเข้าถึง (Access Rights/Privileges) ตามหลัก Least Privilege คือให้สิทธิ์เท่าที่จำเป็น เพื่อป้องกันการเข้าถึงข้อมูลหรือบริการที่ไม่เกี่ยวข้อง ในด้านความปลอดภัยควรกำหนด นโยบายรหัสผ่าน (Password Policy) ที่เข้มงวด เช่น ความยาวขั้นต่ำ การใช้ตัวอักษรพิเศษ และการเปลี่ยนรหัสผ่านตามระยะเวลา รวมถึงการสนับสนุน Multi-Factor Authentication (MFA) สำหรับผู้ใช้งานที่เข้าถึงข้อมูลสำคัญหรือระบบหลักขององค์กรเพื่อควบคุมการใช้งาน และควรมีการบันทึกและตรวจสอบกิจกรรมของผู้ใช้งานผ่าน ระบบบันทึกเหตุการณ์ (Log Management & Monitoring) เพื่อใช้ในการวิเคราะห์พฤติกรรม การติดตามปัญหา และเป็นหลักฐานในกรณีเกิดเหตุด้านความปลอดภัย

3.2.2 การเชื่อมต่อแบบไร้สาย (Wireless Connection)

การติดตั้ง Access Point การติดตั้งระบบเครือข่ายไร้สายจำเป็นต้องมีการวางแผนและออกแบบอย่างเป็นระบบ เพื่อให้การกระจายสัญญาณมีประสิทธิภาพ ครอบคลุมพื้นที่ที่ต้องการ และสามารถบริหารจัดการได้อย่างปลอดภัย โดยเริ่มจากการ สำรวจพื้นที่และกำหนดตำแหน่งติดตั้ง เพื่อประเมินสภาพแวดล้อมจริง ตรวจสอบโครงสร้างอาคาร ผนัง วัสดุที่อาจกีดขวางหรือทำให้สัญญาณลดทอน รวมถึงระบุจุดที่มีความหนาแน่นของผู้ใช้งานสูง จากนั้นนำข้อมูลดังกล่าวมาใช้วางตำแหน่งการติดตั้ง Access Point (AP) ให้เหมาะสม เพื่อให้ได้สัญญาณครอบคลุมและลดการรบกวนระหว่างอุปกรณ์ จากนั้นขั้นตอนการติดตั้ง ควรดำเนินการตามมาตรฐาน RF Site Survey โดยใช้เครื่องมือวัดความแรงสัญญาณ (Signal Strength), ค่า Signal-to-Noise Ratio (SNR) และการตรวจสอบช่องสัญญาณ (Channel Interference) เพื่อยืนยันว่าการติดตั้ง Access Point มีคุณภาพตามเกณฑ์ที่กำหนด และสามารถรองรับปริมาณผู้ใช้งานตามที่ออกแบบไว้ นอกจากนี้ควรคำนึงถึงการปรับแต่งค่าพลังงานส่ง และการเลือกช่องสัญญาณให้เหมาะสม เพื่อลดปัญหาสัญญาณทับซ้อน ด้านการเชื่อมต่ออุปกรณ์ทั้งหมดเข้ากับ ระบบจัดการแบบรวมศูนย์ (Centralized Management System) เพื่อให้ง่ายต่อการบริหารจัดการ ตรวจสอบสถานะอุปกรณ์ เฝ้าระวังการใช้งาน และจัดการปัญหาที่เกิดขึ้นได้อย่างรวดเร็ว ระบบจัดการแบบรวมศูนย์ยังช่วยสนับสนุนนโยบายความปลอดภัย เช่น

การกำหนดสิทธิ์ผู้ใช้งาน การทำ VLAN Segmentation และการบังคับใช้มาตรฐานการเข้ารหัส ทำให้เครือข่ายไร้สายมีความมั่นคงปลอดภัยและพร้อมรองรับการใช้งานอย่างมีประสิทธิภาพในระยะยาว

การกำหนดค่าระบบเครือข่ายไร้สาย (Wireless Configuration) มีความสำคัญอย่างยิ่งต่อการสร้างเครือข่ายที่มีประสิทธิภาพ มั่นคงปลอดภัย และรองรับผู้ใช้งานในสภาพแวดล้อมที่หลากหลาย โดยทั่วไปการออกแบบและตั้งค่าควรคำนึงถึงทั้ง ด้านความปลอดภัย การจัดการทรัพยากร และการควบคุมผู้ใช้งาน เพื่อให้ระบบเครือข่ายไร้สายตอบโจทย์ทั้งองค์กร บุคลากร และผู้ใช้งานทั่วไป การกำหนด SSID (Service Set Identifier) ควรแยก SSID ออกเป็นกลุ่มตามประเภทผู้ใช้งาน เช่น บุคลากร (Staff), นักศึกษา (Student) และ Guest การแยก SSID จะช่วยให้การควบคุมสิทธิ์การเข้าถึงเป็นระเบียบ ง่ายต่อการจัดการ และสามารถบังคับใช้นโยบายด้านความปลอดภัยได้เฉพาะกลุ่ม นอกจากนี้ควรหลีกเลี่ยงการใช้ชื่อ SSID ที่เปิดเผยข้อมูลองค์กรโดยตรง เพื่อลดความเสี่ยงจากการถูกเจาะระบบโดยผู้ไม่หวังดี ด้านความปลอดภัยควรเลือกใช้ มาตรฐานการเข้ารหัสที่เหมาะสม ร่วมกับ 802.1X Authentication สำหรับผู้ใช้งานภายในที่ต้องมีการยืนยันตัวตนอย่างรัดกุม นอกจากนี้สำหรับ Guest ควรใช้ Captive Portal เพื่อบังคับให้ยืนยันตัวตนก่อนการใช้งาน และช่วยเก็บบันทึกข้อมูลผู้ใช้งานเพื่อความปลอดภัยและการตรวจสอบย้อนหลัง ในเชิงเทคนิคด้านสัญญาณ ควรปรับแต่ง Channel, Bandwidth และ Transmit Power อย่างเหมาะสม เพื่อลดการชนกันของสัญญาณ (Interference) โดยเฉพาะในพื้นที่ที่มี Access Point จำนวนมาก ควรพิจารณาใช้งาน Band Steering เพื่อผลักดันอุปกรณ์ที่รองรับไปใช้ย่าน 5 GHz หรือ 6 GHz (Wi-Fi 6/6E) แทน 2.4 GHz ซึ่งมีความแออัดและสัญญาณรบกวนสูงกว่า

การจัดการการเข้าถึงระบบเครือข่าย การจัดการการเข้าถึงระบบเครือข่ายเป็นหัวใจสำคัญของการรักษาความปลอดภัยและการบริหารทรัพยากรเครือข่ายอย่างมีประสิทธิภาพ โดยควรเริ่มจากการยืนยันตัวตนผู้ใช้งาน (Authentication) ด้วยการใช้ RADIUS Server ซึ่งช่วยตรวจสอบสิทธิ์การเข้าถึงเครือข่ายแบบรวมศูนย์ สามารถเชื่อมต่อกับฐานข้อมูลผู้ใช้งานหรือ LDAP/Active Directory เพื่อให้มั่นใจว่าผู้ที่เข้าถึงระบบเป็นผู้มีสิทธิ์จริง และสามารถบังคับใช้นโยบายความปลอดภัยได้อย่างเป็นระบบ นอกจากนี้ควรกำหนดข้อจำกัดด้านแบนด์วิดท์ (Bandwidth Limitation) ตามประเภทผู้ใช้งานหรือกลุ่มงาน เช่น บุคลากร นักศึกษา หรือ Guest เพื่อให้การใช้งานทรัพยากรเครือข่ายเกิดความสมดุลและลดปัญหาความหนาแน่นของเครือข่าย โดยอาจกำหนดค่า QoS (Quality of Service) ร่วมด้วย เพื่อจัดลำดับความสำคัญของบริการที่สำคัญ เช่น Video Conference หรือ VoIP การจัดการการเข้าถึงยังควรครอบคลุมการตั้งค่า Session Timeout และ Idle Timeout เพื่อป้องกันการใช้งานเครือข่ายเกินความจำเป็นหรือผู้ใช้งานที่ลืมออกจากระบบ ช่วยลดความเสี่ยงด้านความปลอดภัยและเพิ่มประสิทธิภาพการจัดสรรทรัพยากรเครือข่าย โดยระบบควรบันทึกและตรวจสอบกิจกรรมของผู้ใช้งานผ่าน Log Management เพื่อนำไปวิเคราะห์พฤติกรรม การติดตามปัญหา และใช้เป็นหลักฐานในการตรวจสอบเมื่อเกิดเหตุการณ์ด้านความปลอดภัย

3.2.3 การเชื่อมต่อระหว่างอาคาร

การออกแบบเส้นทางเครือข่ายไฟเบอร์ออปติก เป็นขั้นตอนสำคัญในการวางระบบโครงสร้างพื้นฐานที่มีประสิทธิภาพ ปลอดภัย และรองรับการส่งข้อมูลความเร็วสูงได้อย่างต่อเนื่อง โดยขั้นตอนแรกควรดำเนินการ สำรวจเส้นทางการเดิน Fiber Cable อย่างละเอียด เพื่อประเมินสภาพพื้นที่ สิ่งกีดขวาง เช่น ผนัง เสาไฟฟ้า หรืออุปกรณ์โครงสร้างอื่น ๆ ที่อาจส่งผลต่อการติดตั้งและประสิทธิภาพของสัญญาณ นอกจากนี้การสำรวจยังช่วยให้สามารถเลือกเส้นทางที่สั้นที่สุด ลดความเสี่ยงในการเสียหาย และสะดวกต่อการบำรุงรักษาในอนาคต ต่อมาคือการ คำนวณ Loss Budget และ Power Budget เพื่อให้มั่นใจว่าสัญญาณที่ส่งผ่านสายไฟเบอร์ยังคงคุณภาพเพียงพอถึงอุปกรณ์ปลายทาง การคำนวณ Loss Budget จะพิจารณาการสูญเสียสัญญาณจากความยาวสาย, การต่อเชื่อม, Connector และ Splice ส่วน Power Budget จะคำนวณกำลังสัญญาณที่ต้องใช้จาก Transmitter ให้เพียงพอถึง Receiver โดยไม่เกิดการลดทอนของสัญญาณเกินมาตรฐาน ซึ่งเป็นขั้นตอนสำคัญเพื่อป้องกันปัญหาเครือข่ายไม่เสถียรหรือการสูญเสียข้อมูล สุดท้ายควรกำหนดจุดเชื่อมต่อและ Distribution Point (DP) อย่างเหมาะสม เช่น จุด Patch Panel หรือ ODF (Optical Distribution Frame) เพื่อให้การเชื่อมต่อระหว่าง Fiber Cable หลายเส้นมีความเป็นระเบียบและง่ายต่อการบริหารจัดการ รวมถึงรองรับการขยายระบบในอนาคต การกำหนด DP ที่ดีจะช่วยลดความซับซ้อนของสายเคเบิล ป้องกันความเสียหาย และเพิ่มความสะดวกในการตรวจสอบหรือซ่อมบำรุง

การติดตั้งระบบเครือข่ายไฟเบอร์ออปติก การติดตั้งระบบเครือข่ายไฟเบอร์ออปติกเป็นขั้นตอนสำคัญเพื่อให้โครงสร้างพื้นฐานเครือข่ายมีประสิทธิภาพและรองรับการส่งข้อมูลความเร็วสูงได้อย่างต่อเนื่อง ขั้นแรกคือการติดตั้ง Optical Distribution Frame (ODF) ซึ่งทำหน้าที่เป็นศูนย์กลางสำหรับการจัดเก็บและบริหารจัดการสายไฟเบอร์ทั้งหมด โดย ODF ต้องถูกติดตั้งในตำแหน่งที่มั่นคง ปลอดภัย และสามารถเข้าถึงได้ง่ายสำหรับการเชื่อมต่อสายใหม่หรือการบำรุงรักษา หลังจากนั้นเป็นขั้นตอนการ เชื่อมต่อสายไฟเบอร์แบบ Single-mode และ Multi-mode Fiber โดยต้องมั่นใจว่าสายแต่ละเส้นถูกต่อเข้ากับพอร์ตที่ถูกต้องตามแผนผังการออกแบบ และการเชื่อมต่อควรทำด้วยเทคนิค Splicing หรือใช้ Connector คุณภาพสูงเพื่อลดการสูญเสียสัญญาณ (Insertion Loss) และป้องกันปัญหาการรบกวนสัญญาณ ขั้นตอนสุดท้ายคือการ ทดสอบสายไฟเบอร์ด้วย OTDR (Optical Time Domain Reflectometer) เพื่อวัดความยาวสาย การสูญเสียสัญญาณ และระบุจุดที่มีปัญหา เช่น การต่อเชื่อมไม่เรียบร้อยหรือสายขาด OTDR เป็นเครื่องมือสำคัญที่ช่วยยืนยันคุณภาพของการติดตั้งและประสิทธิภาพของเครือข่ายไฟเบอร์ก่อนการใช้งานจริง

3.3 เงื่อนไขการปฏิบัติงาน

ด้านผู้ปฏิบัติงานระบบเครือข่าย ผู้ปฏิบัติงานระบบเครือข่ายจำเป็นต้องมีคุณสมบัติที่เหมาะสมทั้งด้านการศึกษา ประสบการณ์ ความเชี่ยวชาญเฉพาะทาง และทักษะเสริมเพื่อให้สามารถติดตั้ง ดูแล และบริหารจัดการเครือข่ายได้อย่างมีประสิทธิภาพ เพื่อให้มีพื้นฐานความรู้ด้านโครงสร้างคอมพิวเตอร์ ระบบปฏิบัติการ และการสื่อสารข้อมูล

ในด้านประสบการณ์การทำงาน ผู้ปฏิบัติงานควรมีประสบการณ์ด้านเครือข่าย เช่น การติดตั้งและบริหารจัดการอุปกรณ์เครือข่าย การวางแผนโครงสร้างพื้นฐาน และการแก้ไขปัญหาเชิงเทคนิค เพื่อให้มั่นใจว่าสามารถปฏิบัติงานในสภาพแวดล้อมจริงได้อย่างคล่องตัว นอกจากนี้ ทักษะพิเศษ ถือเป็นสิ่งที่เพิ่มประสิทธิภาพในการทำงาน เช่น ความรู้เกี่ยวกับระบบปฏิบัติการ Linux และ Windows Server, การเขียนสคริปต์ (Scripting) เพื่อทำงานอัตโนมัติ และความเข้าใจในมาตรฐานและโปรโตคอลเครือข่าย การมีทักษะเหล่านี้ช่วยให้ผู้ปฏิบัติงานสามารถติดตั้ง ปรับแต่ง และบริหารจัดการเครือข่ายได้อย่างรวดเร็ว มีประสิทธิภาพ และตอบสนองต่อความต้องการขององค์กรได้อย่างเหมาะสม

ด้านอุปกรณ์ การกำหนดเงื่อนไขด้านอุปกรณ์และเครื่องมือสำหรับระบบเครือข่ายเป็นสิ่งจำเป็นเพื่อให้มั่นใจว่าเครือข่ายสามารถทำงานได้อย่างมีประสิทธิภาพ มั่นคงปลอดภัย และรองรับผู้ใช้งานได้ตามความต้องการ โดย อุปกรณ์หลัก ที่จำเป็นต้องมีประกอบด้วย Network Switch: ควรใช้ Managed Switch ที่รองรับทั้ง Layer 2 และ Layer 3 เพื่อให้สามารถจัดการ VLAN, Routing ภายในองค์กร และรองรับฟังก์ชัน QoS สำหรับจัดลำดับความสำคัญของการรับส่งข้อมูล การใช้ Managed Switch ยังช่วยให้สามารถตรวจสอบสถานะพอร์ต การเชื่อมต่อ และการใช้งานแบนด์วิดท์ได้อย่างเป็นระบบ Router: ควรเลือก Enterprise Grade Router ที่รองรับฟังก์ชัน VPN สำหรับการเชื่อมต่อระยะไกลอย่างปลอดภัย และสามารถตั้งค่า QoS ระบบความปลอดภัยควรใช้ Next-Generation Firewall (NGFW) ที่รองรับ Deep Packet Inspection เพื่อตรวจสอบการรับส่งข้อมูลในระดับแอปพลิเคชัน ป้องกันภัยคุกคามทั้งจากภายในและภายนอก พร้อมทั้งสามารถควบคุมการเข้าถึงเครือข่ายตามนโยบายความปลอดภัยได้อย่างละเอียด

ด้านเครื่องมือทดสอบสำหรับระบบเครือข่าย การทดสอบระบบเครือข่ายเป็นขั้นตอนสำคัญเพื่อให้มั่นใจว่าอุปกรณ์และโครงสร้างพื้นฐานสามารถทำานได้อย่างมีประสิทธิภาพ ปลอดภัย และตรงตามมาตรฐานที่กำหนด การเลือกใช้ เครื่องมือทดสอบ (Testing Tools) ที่เหมาะสมจะช่วยลดปัญหาความผิดพลาด เพิ่มความเสถียรของเครือข่าย และรองรับการตรวจสอบเชิงวิเคราะห์ได้อย่างแม่นยำ เครื่องมือหลักที่จำเป็น ได้แก่ Cable Tester สำหรับทดสอบสายเคเบิล UTP เพื่อตรวจสอบการต่อสายที่ถูกต้อง การเชื่อมต่อของ RJ-45 Connector และความสมบูรณ์ของคู่สาย ช่วยให้มั่นใจว่าสายสัญญาณไม่มีปัญหาที่อาจทำให้สัญญาณลดทอนหรือเกิดการขัดข้องของเครือข่าย สำหรับการวิเคราะห์ปริมาณข้อมูลและปัญหาการรับส่งข้อมูลควรใช้ Network Analyzer เช่น Wireshark หรือเครื่องมือแบบ Hardware-based ซึ่งสามารถเก็บข้อมูลแพ็กเก็ต วิเคราะห์ปริมาณการใช้งาน ตรวจสอบปัญหาการชนกันของสัญญาณ (Collision) และวิเคราะห์ปัญหาการหน่วงของเครือข่ายได้อย่างละเอียด สำหรับสายไฟเบอร์ออปติก ควรใช้ OTDR (Optical Time Domain Reflectometer) เพื่อวัดความยาวสาย การสูญเสียสัญญาณ (Loss) และระบุจุดที่เกิดปัญหา เช่น จุด Splice หรือ Connector ที่มีการสูญเสียสูง ทำให้สามารถแก้ไขปัญหาได้ก่อนการใช้งานจริง

เงื่อนไขด้านการบำรุงรักษา กำหนดการบำรุงรักษาเชิงป้องกันระบบเครือข่าย การบำรุงรักษาเชิงป้องกันเป็นขั้นตอนสำคัญในการรักษาเสถียรภาพ ความปลอดภัย และประสิทธิภาพของระบบเครือข่าย โดยต้องมีการวางแผนอย่างเป็นระบบและปฏิบัติอย่างสม่ำเสมอ ตามระยะเวลาที่เหมาะสมเพื่อ

ป้องกันปัญหาก่อนที่จะเกิดขึ้น ในระดับ รายสัปดาห์ ควรตรวจสอบ System Log และทำ Performance Monitoring ของอุปกรณ์เครือข่าย เช่น Switch, Router, Firewall และ Access Point เพื่อตรวจจับปัญหาการทำงานที่ผิดปกติ การใช้งานทรัพยากรเกินพิกัด หรือเหตุการณ์ด้านความปลอดภัยที่อาจเกิดขึ้น ในระดับรายเดือน ควรทำการ อัปเดต Firmware และ Security Patch ของอุปกรณ์เครือข่ายและระบบปฏิบัติการ เพื่อปิดช่องโหว่ที่อาจถูกโจมตีและเพิ่มความเสถียรในการทำงาน นอกจากนี้ควรตรวจสอบการตั้งค่าต่าง ๆ ให้สอดคล้องกับนโยบายความปลอดภัยขององค์กร ในระดับรายไตรมาส ควรทำการ ทดสอบระบบสำรอง (Backup System Test) และ แผนฉุกเฉิน (Disaster Recovery Plan Test) เพื่อให้มั่นใจว่าข้อมูลสำคัญและระบบเครือข่ายสามารถกลับมาทำงานได้อย่างรวดเร็วหากเกิดเหตุการณ์ไม่คาดคิด เช่น ความเสียหายของอุปกรณ์หรือภัยพิบัติ ในระดับรายปี ควรทำการ ประเมินและวางแผนการยกระดับระบบ (System Upgrade Planning) เพื่อให้เครือข่ายรองรับความต้องการที่เพิ่มขึ้น ทั้งด้านจำนวนผู้ใช้งาน ความเร็วในการส่งข้อมูล และเทคโนโลยีใหม่ ๆ เช่น การเปลี่ยนไปใช้ WiFi 6E หรืออัปเกรดอุปกรณ์ Firewall/Router ให้ทันสมัย

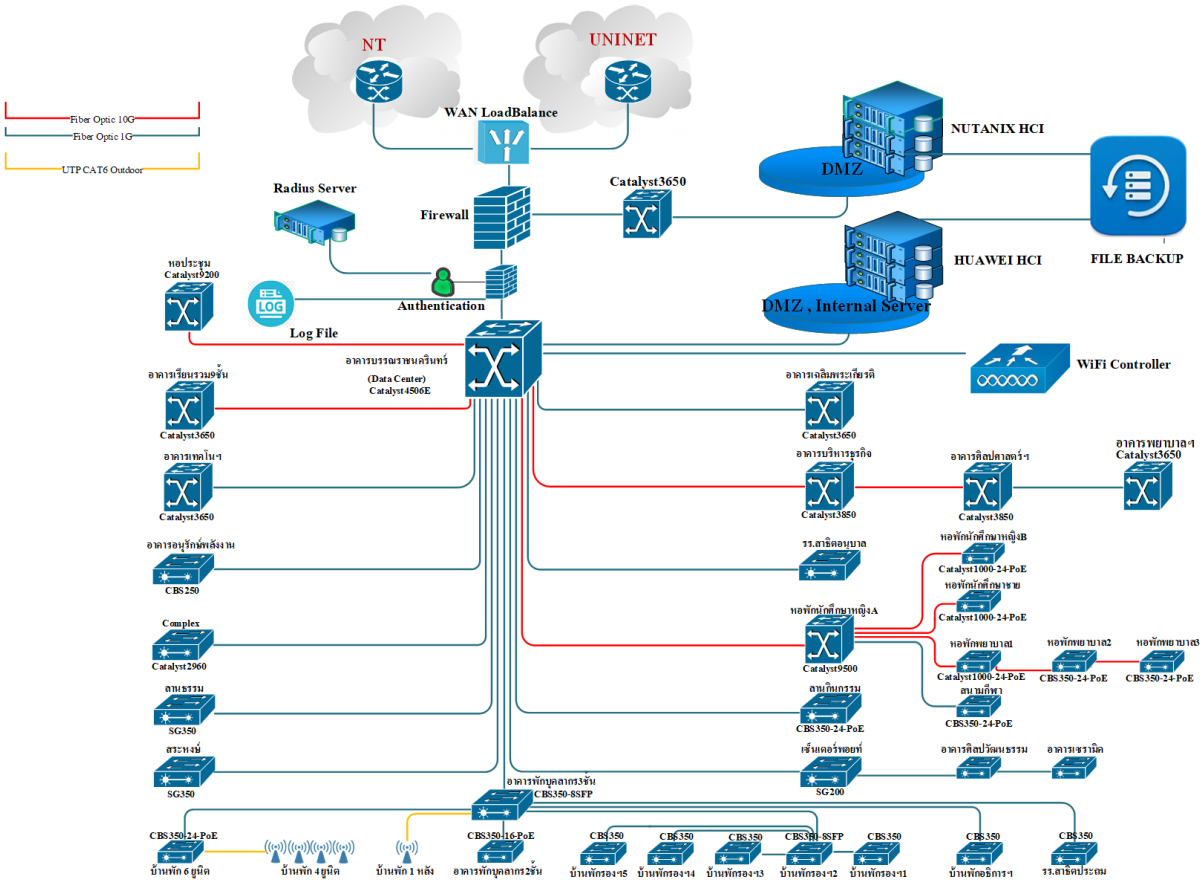
กฎหมายที่เกี่ยวข้อง

1. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
   - ป้องกันและรับมือภัยคุกคามทางไซเบอร์
   - กำหนดมาตรการรักษาความปลอดภัยระบบเครือข่าย
   - ต้องแจ้งเหตุการณ์ภัยคุกคามต่อ สกมช.
2. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)
   - คุ้มครองข้อมูลส่วนบุคคลในระบบเครือข่าย
   - กำหนดสิทธิของเจ้าของข้อมูล
   - ต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล (DPO)
3. พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550และเพิ่มเติม
   - ป้องกันการใช้คอมพิวเตอร์ในทางผิด
   - กำหนดโทษการละเมิดระบบคอมพิวเตอร์
4. ระเบียบกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม
   - มาตรฐานการใช้งานเทคโนโลยีสารสนเทศ
   - หลักเกณฑ์การรักษาความปลอดภัยข้อมูล
5. มาตรฐานความปลอดภัยไซเบอร์ของรัฐ
   - ISO/IEC 27001 สำหรับระบบเครือข่าย
   - แนวปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์
6. ระเบียบระดับมหาวิทยาลัย
   - นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยราชภัฏชัยภูมิ
   - แผนรับมือเหตุภัยคุกคามทางไซเบอร์ มหาวิทยาลัยราชภัฏชัยภูมิ

บทที่ 4
เทคนิคและขั้นตอนการปฏิบัติงาน

4.1 ภาพรวมการเชื่อมต่อระบบเครือข่ายหลัก มหาวิทยาลัยราชภัฏชัยภูมิ

องค์ประกอบที่สำคัญอย่างหนึ่งของระบบเครือข่ายคือระบบสายสัญญาณการเชื่อมต่อ เพื่อให้เห็นภาพรวมทั้งหมด และเข้าใจได้ง่าย จึงจัดทำเป็นแผนผังเครือข่ายหลักของมหาวิทยาลัย และแผนผังระบบเครือข่ายของแต่ละอาคารพร้อมคำอธิบายโครงสร้างเครือข่ายภายในอาคารการเชื่อมต่อระหว่างอาคารดังต่อไปนี้



ภาพที่ 4.1 ระบบเครือข่ายหลักของมหาวิทยาลัยราชภัฏชัยภูมิ

จากภาพ 4.1 เป็นโครงสร้างการเชื่อมต่อระบบเครือข่ายหลักของมหาวิทยาลัย โดยมีการเชื่อมอินเทอร์เน็ต 2 เส้นทางความเร็วสูง แบบ Leased Line เส้นทางหลักเชื่อมกับ UniNet ความเร็ว 1 Gbps และเส้นทางสำรองความเร็ว 80/1 Gbps (ความเร็วต่างประเทศไม่น้อยกว่า 80 Mbps และความเร็วภายในประเทศไม่น้อยกว่า 1 Gbps) ซึ่งปัจจุบันสถาบันเช่าใช้เส้นทางของบริษัท บริษัท โทรคมนาคมแห่งชาติ วงจรอินเทอร์เน็ตทั้งสองวงจรต่อเข้ากับอุปกรณ์ค้นหาเส้นทางเราท์เตอร์ (Router) เชื่อมต่อกับอุปกรณ์ LoadBalance ซึ่งเป็นอุปกรณ์ที่ทำหน้าที่ในการจัดการ Trafficทั้งขาเข้าและขาออก อุปกรณ์

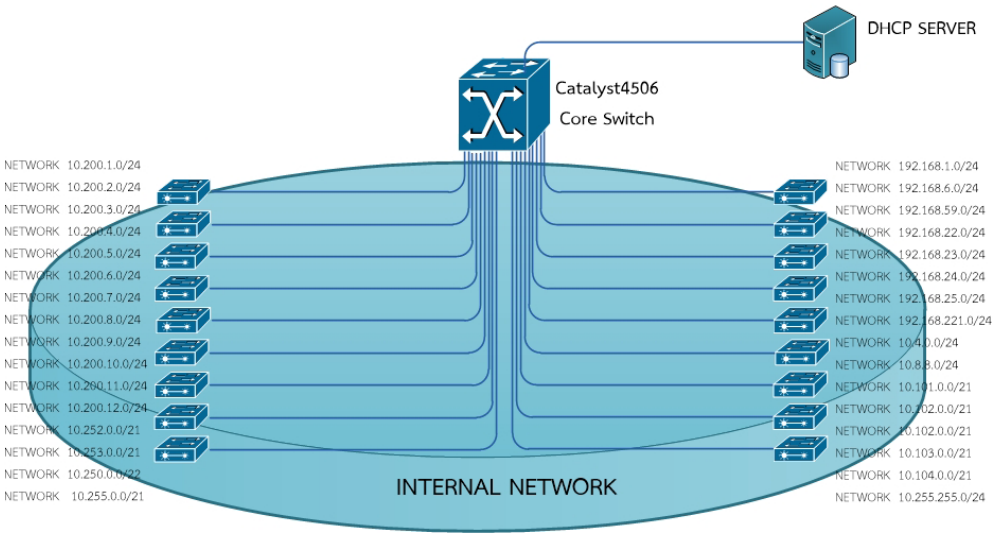
LoadBalance เชื่อมต่อกับระบบไฟร์วอลล์รักษาความปลอดภัยของเครื่องเครือข่าย ไม่ให้ถูกโจมตีจากผู้ไม่หวังดีหรือการสื่อสารที่ไม่ได้รับอนุญาต ซึ่งส่วนใหญ่จะมาจากระบบเครือข่ายอินเตอร์เน็ต รวมถึงเครือข่าย LAN ด้วย โดยไฟร์วอลล์ของมหาวิทยาลัยแบ่งออกเป็นโซนต่างๆ 3 โซนดังนี้

โซน Wan เป็นโซนที่เชื่อมต่อกับระบบอินเทอร์เน็ตภายนอก

โซน DMZ (DeMilitalized Zone) คือเป็นโซนของ ระบบ Server ทั้งหมดที่อยู่ภายในระบบ Network ของมหาวิทยาลัย

โซน Internal เป็นโซนที่เชื่อมต่อกับ Core Network หลักของระบบเครือข่ายภายใน

ระบบเครือข่ายภายในของมหาวิทยาลัยเชื่อมโยงไปทุกอาคาร ใช้ Core Switch หลักเป็นศูนย์กลาง โดยมีโครงสร้างการจัดสรรหมายเลขไอพีแอดเดรสดังรูป



ภาพที่ 4.2 การจัดสรรหมายเลขไอพีแอดเดรส

4.2 การวางแผนและเตรียมความพร้อม

การประเมินความต้องการ การประเมินความต้องการเป็นขั้นตอนพื้นฐานที่สำคัญที่สุดในการออกแบบระบบเครือข่ายที่มีประสิทธิภาพ กระบวนการนี้เริ่มต้นจากการวิเคราะห์การใช้งานปัจจุบันและการคาดการณ์การเติบโตในอนาคต โดยต้องพิจารณาปัจจัยหลัก ได้แก่ จำนวนผู้ใช้งานสูงสุดพร้อมกัน (Concurrent Users) ประเภทของแอปพลิเคชันที่ใช้งาน และความต้องการแบนด์วิธที่แตกต่างกันในแต่ละหน่วยงานแต่ละตึกที่ให้บริการ การคำนวณแบนด์วิธที่จำเป็นต้องใช้วิธีการทางสถิติและการวิเคราะห์รูปแบบการใช้งาน (Traffic Pattern Analysis) โดยพิจารณาจาก Peak Hour Usage, Average Utilization และ Quality of Service (QoS) Requirements สำหรับแอปพลิเคชันที่มีความสำคัญสูง เช่น VoIP, Video Conferencing หรือ Real-time Applications การประเมินจำนวนอุปกรณ์ที่จะเชื่อมต่อต้องครอบคลุมทั้งอุปกรณ์ปัจจุบันและอุปกรณ์ที่จะเพิ่มเติมในอนาคต 3-5 ปี

การวิเคราะห์โครงสร้างเครือข่ายปัจจุบันต้องใช้เครื่องมือวิเคราะห์เครือข่าย เช่น Network Discovery Tools, Bandwidth Monitors และ Network Topology Mappers เพื่อทำความเข้าใจ Bottlenecks ที่มีอยู่และจุดที่ต้องปรับปรุง การศึกษาความต้องการในอนาคตควรพิจารณาจากแผนปฏิบัติราชการ การขยายตัวของนักศึกษาและบุคลากร การเปลี่ยนแปลงเทคโนโลยี และการปรับปรุงกระบวนการทำงาน การประเมินนี้จะเป็นพื้นฐานสำคัญในการกำหนดงบประมาณ เลือกเทคโนโลยี และวางแผนการดำเนินงานที่เหมาะสม

การออกแบบโครงสร้างเครือข่าย การออกแบบโครงสร้างเครือข่าย ต้องใช้ความรู้ทางทฤษฎีร่วมกับประสบการณ์ภาคปฏิบัติ การเลือกโทโพโลยีเครือข่ายต้องพิจารณาจากความซับซ้อนขององค์กร ความต้องการด้านความปลอดภัย และข้อจำกัดทางงบประมาณ โทโพโลยีแบบ Hierarchical Three-Tier Model ประกอบด้วย Core Layer, Distribution Layer และ Access Layer เป็นมาตรฐานที่แนะนำสำหรับองค์กรที่ให้บริการด้านการจัดการศึกษา วิจัย การวางตำแหน่งอุปกรณ์หลักต้องคำนึงถึงหลักการของ Fault Tolerance และ Redundancy โดย Core Router ควรตั้งอยู่ในตำแหน่งกลางที่มีการป้องกันทางกายภาพ Distribution Switches ควรกระจายไปยังแต่ละชั้นหรือพื้นที่ทำงาน และ Access Points ต้องวางในตำแหน่งที่ให้ Coverage ที่เหมาะสม

การวางแผนเส้นทางสายเคเบิลต้องปฏิบัติตามมาตรฐาน TIA/EIA-568 โดยพิจารณาความยาวสูงสุดของสายแต่ละประเภท ระยะห่างจากแหล่งสัญญาณรบกวน และความสะดวกในการบำรุงรักษา การคำนวณระยะทางต้องรวมระยะ Horizontal Run และ Vertical Run รวมถึง Patch Cord ที่จุดต่าง ๆ การออกแบบ Cable Management System ที่ดีจะช่วยลดปัญหาในอนาคตและทำให้การขยายระบบง่ายขึ้น ข้อจำกัดทางกายภาพ เช่น โครงสร้างอาคาร ระบบปรับอากาศ และระบบไฟฟ้า ต้องได้รับการพิจารณาอย่างละเอียดในขั้นตอนการออกแบบ

4.3 การเลือกอุปกรณ์และสื่อสัญญาณ

อุปกรณ์เครือข่ายหลัก การเลือกอุปกรณ์เครือข่ายหลักต้องอาศัยการวิเคราะห์ Technical Specifications อย่างละเอียดและการประเมิน Total Cost of Ownership (TCO) Router ที่เหมาะสมต้องมี Processing Power ที่เพียงพอสำหรับการจัดการ Routing Table ขนาดใหญ่ รองรับ Dynamic Routing Protocols เช่น OSPF, EIGRP หรือ BGP และมีฟีเจอร์ด้านความปลอดภัยขั้นสูง เช่น VPN Termination, Intrusion Detection และ Deep Packet Inspection Switch ที่มีคุณภาพต้องให้ Non-blocking Performance, มี Sufficient Buffer Size สำหรับการจัดการ Traffic Bursts และรองรับ Layer 3 Switching สำหรับการ Inter-VLAN Routing ความสามารถในการจัดการ Quality of Service (QoS) เป็นสิ่งสำคัญสำหรับการรับรอง Service Level Agreement (SLA) ของแอปพลิเคชันที่มีความสำคัญสูง การรองรับ Power over Ethernet (PoE) จะเพิ่มความยืดหยุ่นในการติดตั้ง IP Phones, Wireless Access Points และกล้องวงจรปิด

Access Point สำหรับเครือข่ายไร้สายต้องมีความสามารถในการจัดการ Multiple SSIDs, รองรับมาตรฐาน และมีฟีเจอร์ Advanced Radio Management เช่น Automatic Channel Selection และ Transmit Power Control การรองรับ MIMO Technology จะช่วยเพิ่มประสิทธิภาพในสภาพแวดล้อมที่มี User Density สูง คุณสมบัติด้านความปลอดภัยต้องครอบคลุม WPA3, 802.1X Authentication และ Rogue AP Detection

การจัดการอุปกรณ์ (Network Management) เป็นปัจจัยสำคัญที่มักถูกมองข้าม อุปกรณ์ที่ดีต้องรองรับ SNMP, Web-based Management Interface และมี API สำหรับการ Integration กับระบบจัดการเครือข่ายขนาดใหญ่ Firmware Update Process ที่ไม่ยุ่งยากและมี Vendor Support ที่ดีจะช่วยลดภาระงานของทีม IT อย่างมาก

สื่อสัญญาณ การเลือกสื่อสัญญาณต้องพิจารณาจาก Application Requirements, Distance Limitations และ Environmental Factors ที่เหมาะสำหรับการใช้งานทั่วไป สามารถรองรับความเร็วถึง 10 Gbps ในระยะทางที่เหมาะสม การเลือกใช้ Shielded หรือ Unshielded Twisted Pair ขึ้นอยู่กับสภาพแวดล้อมและระดับของ Electromagnetic Interference สำหรับระยะทางไกลหรือการเชื่อมต่อระหว่างอาคาร Fiber Optic Cable เป็นทางเลือกที่ดีและเหมาะสม Single-mode Fiber ให้ระยะทางและแบนด์วิธที่สูงกว่า เป็นสิ่งจำเป็นสำหรับการออกแบบ Fiber Optic Link ที่มีประสิทธิภาพ

เครือข่ายไร้สายต้องพิจารณามาตรฐาน Wi-Fi ที่เหมาะสม 802.11ac (Wi-Fi 5) เป็นมาตรฐานที่เสถียรและมี Backward Compatibility ดี 802.11ax (Wi-Fi 6) ให้ประสิทธิภาพที่สูงกว่าและมีฟีเจอร์ขั้นสูง เช่น OFDMA และ Target Wake Time สำหรับการประหยัดพลังงาน การเลือกความถี่ 2.4 GHz หรือ 5 GHz ต้องพิจารณาจาก Coverage Requirements และ Interference Environment

4.4 ขั้นตอนการติดตั้งและกำหนดค่า

การติดตั้งอุปกรณ์ การติดตั้งอุปกรณ์เครือข่ายต้องเริ่มจากการเตรียมพื้นที่และสภาพแวดล้อมให้เหมาะสม แร็ค (Rack) ต้องมีขนาดและความแข็งแรงที่เพียงพอ พร้อมระบบจัดการสายเคเบิลที่เป็นระเบียบ การวางตำแหน่งอุปกrณ์ในแร็คต้องคำนึงถึง Airflow Pattern โดยอุปกรณ์ที่สร้างความร้อนมากควรอยู่ด้านล่าง และต้องมีช่องว่างสำหรับการระบายอากาศ ระบบระบายความร้อนต้องได้รับการออกแบบให้รักษาอุณหภูมิในห้องไม่เกิน 25°C และความชื้นสัมพัทธ์อยู่ระหว่าง 40-60% การใช้ Hot Aisle/Cold Aisle Configuration ช่วยเพิ่มประสิทธิภาพการระบายความร้อน Environmental Monitoring System ควรติดตั้งเพื่อเตือนเมื่ออุณหภูมิหรือความชื้นผิดปกติ UPS (Uninterruptible Power Supply) ต้องมีขนาดที่เหมาะสมและมีระบบจัดการแบตเตอรี่ที่ดี

การเชื่อมต่อสายเคเบิลต้องปฏิบัติตามมาตรฐานสากล โดยใช้ Patch Panel และ Cable Management Accessories เพื่อให้ระบบเป็นระเบียบและง่ายต่อการบำรุงรักษา การติด Label ทุกสายและพอร์ตด้วยระบบตัวเลขหรือตัวอักษรที่มีความหมายจะช่วยลดเวลาในการ Troubleshooting การทดสอบความต่อเนื่องของสายและคุณภาพสัญญาณด้วย Cable Tester เป็นขั้นตอนที่จำเป็นก่อนเปิดใช้งาน การทดสอบการเชื่อมต่อเบื้องต้นครอบคลุม Link Status, Port Speed Negotiation และ Basic Connectivity การใช้ Network Protocol Analyzer ช่วยให้เห็นรายละเอียดของ Network Frames และสามารถตรวจจับปัญหาในระดับ Physical และ Data Link Layer การจัดทำเอกสารการติดตั้ง (As-Built Documentation) ต้องทำพร้อมกับการติดตั้งเพื่อให้ข้อมูลถูกต้องและทันสมัย

การกำหนดค่าเครือข่าย การกำหนดค่าเครือข่ายเป็นขั้นตอนที่ต้องใช้ความรู้ทางทฤษฎีและประสบการณ์ภาคปฏิบัติอย่างลึกซึ้ง การออกแบบ IP Addressing Scheme ต้องรองรับการใช้งานปัจจุบันและการขยายตัวในอนาคต การใช้ Private IP Address Ranges (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) ตามมาตรฐาน RFC 1918 เป็นแนวทางที่แนะนำ การแบ่ง Subnet ต้องคำนึงถึงจำนวน Host ที่ต้องการในแต่ละเครือข่ายย่อยและเหลือพื้นที่สำหรับการขยายตัว

Variable Length Subnet Masking (VLSM) ช่วยให้การใช้ IP Address มีประสิทธิภาพมากขึ้น โดยเฉพาะในสภาพแวดล้อมที่มีเครือข่ายย่อยหลายขนาด การกำหนด Default Gateway ต้องชี้ไปยังอุปกรณ์ที่มีเสถียรภาพสูงและมี Redundancy การใช้ HSRP, VRRP หรือ GLBP ช่วยให้มี Gateway Redundancy สำหรับความต่อเนื่องของระบบ DNS Configuration ต้องมี Primary และ Secondary DNS Servers พร้อม Forwarder สำหรับ External Queries

VLAN (Virtual LAN) Implementation เป็นเครื่องมือสำคัญสำหรับการแยกการรับส่งข้อมูลและเพิ่มความปลอดภัย การออกแบบ VLAN ต้องพิจารณาจาก Business Requirements, Security Policies และ Broadcast Domain Size การใช้ Trunk Ports สำหรับการเชื่อมต่อระหว่าง Switches และ Access Ports สำหรับ End Devices Inter-VLAN Routing สามารถทำได้ด้วย Layer 3 Switch หรือ Router ขึ้นอยู่

กับขนาดและความซับซ้อนของเครือข่าย Security Configuration เป็นส่วนหนึ่งของการกำหนดค่าพื้นฐานที่ไม่ควรมองข้าม การตั้งรหัสผ่านที่แข็งแรงสำหรับ Administrative Access การเปิดใช้งาน SSH แทน Telnet การกำหนด Access Control Lists (ACLs) เพื่อจำกัดการเข้าถึงบางบริการหรือเครือข่าย การปิด unused ports และการกำหนด Port Security เพื่อป้องกัน Unauthorized Device Connection

4.5 การทดสอบและปรับตั้งค่า

การทดสอบระบบเครือข่ายต้องทำอย่างเป็นระบบและครอบคลุมทุกแง่มุมของการทำงาน Performance Testing เริ่มจากการวัด Baseline Performance ด้วยเครื่องมือเช่น iPerf, Speedtest CLI หรือ Network Performance Monitor การทดสอบควรทำในช่วงเวลาต่างๆ เพื่อดู Performance Variation และระบุ Peak Usage Period การวัด Latency, Jitter และ Packet Loss เป็นพารามิเตอร์สำคัญสำหรับ Real-time Applications

Connectivity Testing ต้องครอบคลุมการเชื่อมต่อภายในเครือข่าย (Intra-network) และการเชื่อมต่อไปยังเครือข่ายภายนอก (Inter-network) การใช้คำสั่ง Ping สำหรับทดสอบ Reachability การใช้ Traceroute เพื่อวิเคราะห์เส้นทางการรับส่งข้อมูล การทดสอบ DNS Resolution และการเข้าถึง External Services การใช้ Network Scanning Tools เช่น Nmap เพื่อตรวจสอบ Open Ports และ Running Services

Load Testing จำลองสภาวะการใช้งานจริงเพื่อทดสอบความสามารถของระบบ การใช้ Traffic Generators เพื่อสร้าง Synthetic Traffic ที่หลากหลายรูปแบบ การทดสอบ Failover Scenarios เพื่อตรวจสอบ Redundancy Mechanisms การทดสอบ QoS Implementation โดยการสร้าง Traffic ที่มี Priority แตกต่างกัน การวิเคราะห์ Network Utilization และ Buffer Usage ในสถานการณ์ต่าง ๆ การปรับแต่งประสิทธิภาพต้องอาศัยข้อมูลจากการทดสอบและการติดตามการใช้งาน Buffer Tuning สำหรับ Switches และ Routers QoS Parameter Adjustment สำหรับการจัดลำดับความสำคัญของ Traffic Routing Protocol Optimization เช่น การปรับ Hello Intervals, Dead Intervals และ Metric Values การปรับแต่ง TCP Window Size และ Congestion Control Algorithms สำหรับการปรับปรุงประสิทธิภาพ End-to-End

4.6 การรักษาความปลอดภัย

การป้องกันพื้นฐาน ความปลอดภัยของระบบเครือข่ายต้องเริ่มจากการสร้างนโยบายความปลอดภัยที่ชัดเจนและครอบคลุม การกำหนดรหัสผ่านต้องปฏิบัติตาม Password Policy ที่เข้มงวด โดยควรมีความยาวไม่น้อยกว่า 12 ตัวอักษร ประกอบด้วยอักษรพิมพ์ใหญ่ พิมพ์เล็ก ตัวเลข และอักขระพิเศษ การใช้ Multi-Factor Authentication (MFA) เพิ่มชั้นความปลอดภัยที่สำคัญ การหมดอายุของรหัสผ่านและการห้ามใช้รหัสผ่านเดิมซ้ำเป็นแนวทางที่แนะนำ การเข้ารหัสข้อมูลในระหว่างการส่งผ่าน (Data in Transit) เป็น

สิ่งจำเป็น WPA3 เป็นมาตรฐานล่าสุดสำหรับ Wi-Fi Security ที่ให้ความปลอดภัยสูงกว่า WPA2 อย่างมาก การใช้ Enterprise Mode กับ RADIUS Authentication ช่วยให้การจัดการผู้ใช้งานเป็นไปอย่างเป็นระบบ การเข้ารหัสด้วย AES-256 และการใช้ Perfect Forward Secrecy ช่วยป้องกันการถูกดักฟังข้อมูล

การปิดบริการที่ไม่จำเป็น (Service Hardening) เป็นหลักการพื้นฐานของ Security Best Practices การสแกนหา Open Ports ด้วยเครื่องมือเช่น Nmap และปิด Services ที่ไม่ใช้งาน การปิด SNMP Community Strings ที่เป็น Default การเปลี่ยน Default Administrative Accounts และการลบ Sample Configurations ที่อาจมีช่องโหว่ การกำหนด Banner Messages เพื่อเตือนผู้ใช้งานเกี่ยวกับนโยบายการใช้งาน

การอัปเดตเฟิร์มแวร์และซอฟต์แวร์อย่างสม่ำเสมอเป็นมาตรการป้องกันที่สำคัญ การติดตาม Vendor Security Advisories การทดสอบ Updates ใน Lab Environment ก่อนนำไปใช้งานจริง การสำรองข้อมูล Configuration Files ก่อนทำการอัปเดต การมี Rollback Plan กรณีที่การอัปเดตไม่สำเร็จ Vulnerability Management Process ต้องมีการสแกนหาช่องโหว่อย่างสม่ำเสมอและดำเนินการแก้ไขตามระดับความเสี่ยง

4.7 การจัดการการเข้าถึง

การควบคุมการเข้าถึง (Access Control) เป็นหัวใจของระบบรักษาความปลอดภัย Role-Based Access Control (RBAC) ช่วยให้การจัดการสิทธิ์เป็นไปตามหลักการ Principle of Least Privilege แต่ละบทบาทในองค์กรควรได้รับสิทธิ์เพียงพอสำหรับการปฏิบัติงาน การแยกสิทธิ์ Administrative, Operator และ User Level การสร้าง Service Accounts สำหรับระบบต่างๆ และการจำกัดการใช้งาน Shared Accounts

802.1X Authentication เป็นมาตรฐานสำหรับ Network Access Control ที่ให้ความปลอดภัยระดับสูง การผสานกับ Active Directory หรือ LDAP Services ทำให้การจัดการผู้ใช้งานเป็นแบบ Centralized การใช้ Certificate-based Authentication เพิ่มความปลอดภัยและลดการพึ่งพารหัสผ่าน Dynamic VLAN Assignment ตาม User Profile ช่วยให้ผู้ใช้งานได้รับสิทธิ์ที่เหมาะสม

MAC Address Filtering แม้จะไม่ใช่มาตรการรักษาความปลอดภัยที่แข็งแรง แต่สามารถใช้เป็นชั้นความปลอดภัยเพิ่มเติมในสภาพแวดล้อมที่มีการควบคุมเข้มงวด การจัดทำ Whitelist ของอุปกรณ์ที่ได้รับอนุญาต การติดตาม Unknown Devices ที่พยายามเชื่อมต่อ การใช้ Network Access Control (NAC) Solutions สำหรับการตรวจสอบ Device Compliance และ Health Status

Guest Network เป็นแนวทางที่แนะนำสำหรับการให้บริการอินเทอร์เน็ตแก่ผู้มาเยือน การแยก Guest Network จาก Corporate Network อย่างสมบูรณ์ การจำกัด Bandwidth และ Session Time การบล็อกการเข้าถึง Internal Resources การใช้ Captive Portal สำหรับการ Authentication การเก็บ Log การใช้งานเพื่อการตรวจสอบ การตั้งค่า Automatic Account Expiration และการมี Guest Registration Process ที่เป็นระเบียบ

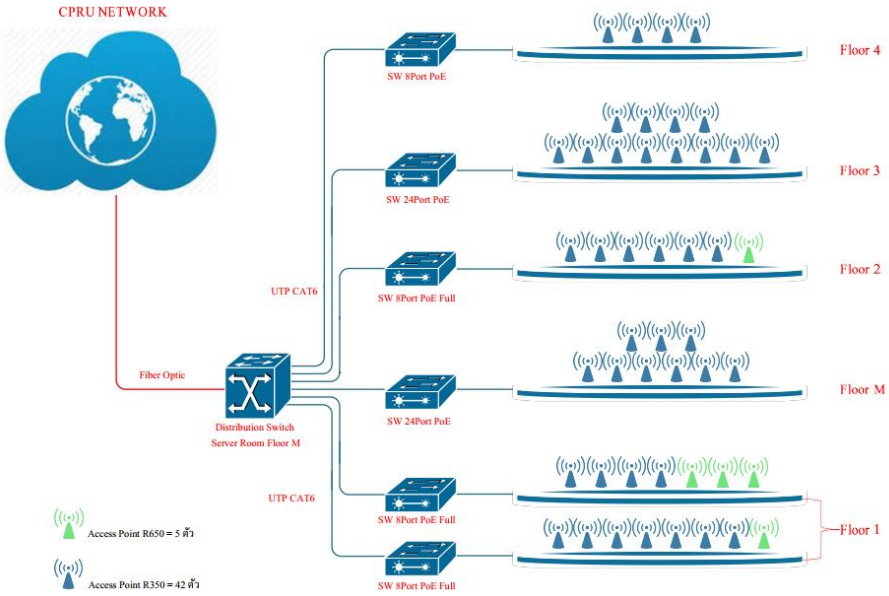
4.8 การตรวจสอบและบำรุงรักษา

การติดตามประสิทธิภาพ การติดตามประสิทธิภาพของระบบเครือข่ายต้องใช้แนวทางเชิงรุกและมีระบบ Network Monitoring System ที่ครอบคลุมต้องสามารถเก็บข้อมูล Real-time และ Historical Data การใช้ SNMP (Simple Network Management Protocol) เพื่อรวบรวมข้อมูลจากอุปกรณ์ต่างๆ การตั้งค่า Threshold Values สำหรับพารามิเตอร์สำคัญ เช่น CPU Utilization, Memory Usage, Interface Utilization และ Error Counters การสร้าง Dashboard ที่แสดงสถานะระบบแบบ Real-time

การติดตามประสิทธิภาพระบบเครือข่ายเป็นกระบวนการสำคัญที่ต้องใช้แนวทางเชิงรุกในการรวบรวม วิเคราะห์ และตีความข้อมูลจากอุปกรณ์เครือข่ายและระบบต่างๆ โดยครอบคลุมการตรวจสอบสถานะฮาร์ดแวร์ การวิเคราะห์การใช้งานแบนด์วิธ การติดตาม QoS และประสิทธิภาพแอปพลิเคชัน รวมถึงการใช้เทคโนโลยีขั้นสูงเช่น AI/ML เพื่อทำนายปัญหาและปรับปรุงระบบ การติดตามที่มีประสิทธิภาพจะช่วยลดความเสี่ยงจากการหยุดชะงัก เพิ่มประสิทธิภาพการทำงาน

4.9 การเชื่อมต่อระบบเครือข่ายประจำตึกภายในมหาวิทยาลัยราชภัฏชัยภูมิ

4.9.1 อาคารเฉลิมพระเกียรติ 50 พรรษามหาวชิราลงกรณ



ภาพที่ 4.3 โครงสร้างเครือข่ายภายในอาคารเฉลิมพระเกียรติ 50 พรรษามหาวชิราลงกรณ

โครงสร้างเครือข่ายภายในอาคารอาคารเฉลิมพระเกียรติ 50 พรรษามหาวชิราลงกรณ (LAN Network Topology) โดยอธิบายการทำงานได้ดังนี้

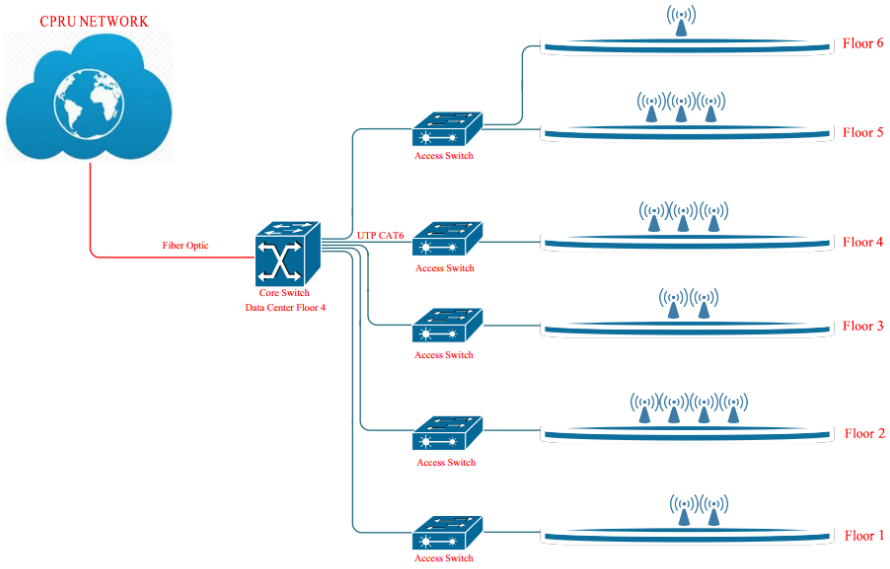
1. **ต้นทางเครือข่าย (CPRU Network)** เครือข่ายหลักของมหาวิทยาลัย (WAN/Internet) เข้ามาที่อาคารผ่าน สาย Fiber Optic

2. **Distribution Switch (ชั้น M / Core Layer)** เป็นอุปกรณ์เครือข่ายหลักที่ติดตั้งในชั้น M ทำหน้าที่กระจายสัญญาณหลัก ไปยัง Access Switch แต่ละชั้น ใช้สาย UTP CAT6 ในการเชื่อมต่อ
3. **Access Switch (SW 24 Port PoE Full)** กระจายอยู่ในแต่ละชั้นของอาคาร ทำหน้าที่จ่ายสัญญาณเครือข่าย (LAN) และยัง จ่ายไฟผ่านสาย LAN (PoE) ไปยัง Access Point ได้โดยตรง แต่ละชั้นมี Switch สำหรับรองรับอุปกรณ์เครือข่าย (เช่น คอมพิวเตอร์, ปริ้นเตอร์, และ AP)
4. **Access Point (AP – Wi-Fi Hotspot)** แต่ละชั้นติดตั้ง Access Point รุ่น Ruckus R310 จำนวน 25 ตัว และ R320 จำนวน 6 ตัว ทำหน้าที่กระจายสัญญาณ Wi-Fi ให้ผู้ใช้งานในพื้นที่ ได้รับไฟเลี้ยงและสัญญาณผ่านสาย LAN ที่ต่อจาก Switch (PoE)
5. **การเชื่อมต่อระหว่างชั้น แต่ละชั้น (Floor 1–4, M)** จะมี Access Switch 24 Port PoE Access Switch แต่ละตัวเชื่อมขึ้นไปยัง Distribution Switch ที่ ชั้นM ด้วย สาย UTP CAT6
6. **ภาพรวมการทำงาน** เครือข่ายจากมหาวิทยาลัย (CPRU Network) ⟶ Fiber Optic ⟶ Distribution Switch (Core)

Distribution Switch ⟶ Access Switch แต่ละชั้น ⟶ Access Point และอุปกรณ์ผู้ใช้งาน (PC, Laptop ฯลฯ)

Access Point ปล่อยสัญญาณ Wi-Fi ครอบคลุมทุกชั้น ⟶ ผู้ใช้เชื่อมต่อ Internet ได้ทั้งแบบ สาย LAN และไร้สาย Wi-Fi

4.9.2 อาคารบรรณราชนครินทร์



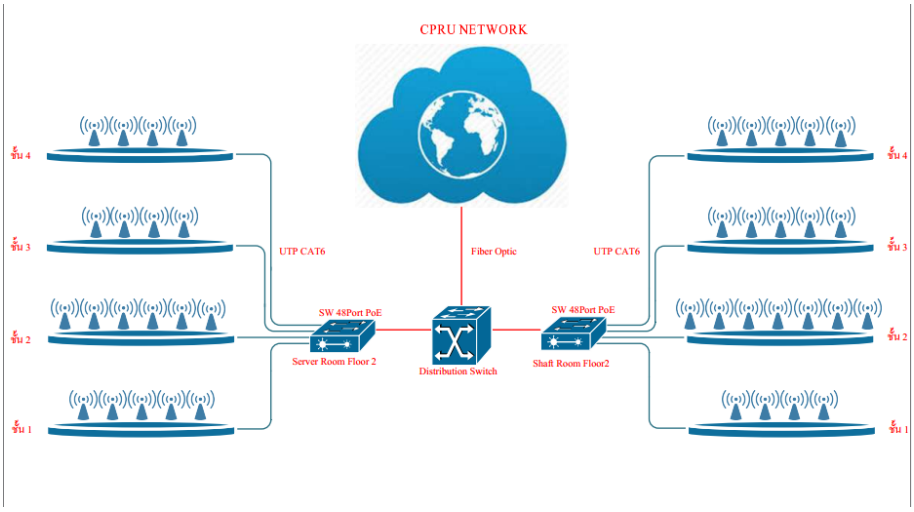
ภาพที่ 4.4 โครงสร้างเครือข่ายภายในอาคารบรรณราชนครินทร์

โครงสร้างเครือข่ายภายในอาคารบรรณราชนครินทร์ (LAN Network Topology) โดยอธิบายการทำงานได้ดังนี้

1. **CPRU Network (เครือข่ายหลักมหาวิทยาลัย)** อินเทอร์เน็ตหรือเครือข่ายหลักของมหาวิทยาลัย (WAN/Internet) เข้ามายังอาคารผ่าน **สาย Fiber Optic**

2. **Core Switch (ศูนย์กลางเครือข่าย)**อยู่ที่ **Data Center ชั้น 4** ทำหน้าที่เป็นอุปกรณ์หลักในการกระจายสัญญาณเครือข่ายไปยัง **Access Switch** แต่ละชั้นใช้สาย **UTP CAT6** เชื่อมต่อไปยังสวิตช์ชั้นต่าง ๆ
3. **Access Switch (สวิตช์กระจาย)** ติดตั้งแยกในแต่ละชั้นของอาคารทำหน้าที่กระจายสัญญาณจาก Core Switch ไปยัง **อุปกรณ์ปลายทาง** เช่น คอมพิวเตอร์, เครื่องพิมพ์, และ **Access Point (AP)**
4. **Access Point (AP - อุปกรณ์ปล่อย Wi-Fi)** ติดตั้งบนแต่ละชั้น เพื่อให้ผู้ใช้งานสามารถเชื่อมต่อเครือข่ายแบบไร้สาย (Wi-Fi) Access Point จะเชื่อมต่อกับ Access Switch ของชั้นนั้น ๆ
5. **ภาพรวมการทำงาน** ข้อมูลจากอินเทอร์เน็ต ⟶ เข้ามายัง Core Switch ⟶ กระจายไปยัง Access Switch ของแต่ละชั้น ⟶ กระจายต่อไปยังอุปกรณ์ผู้ใช้ (ทั้งแบบสาย LAN และไร้สาย Wi-Fi)

4.9.3 อาคารเรียนรวม

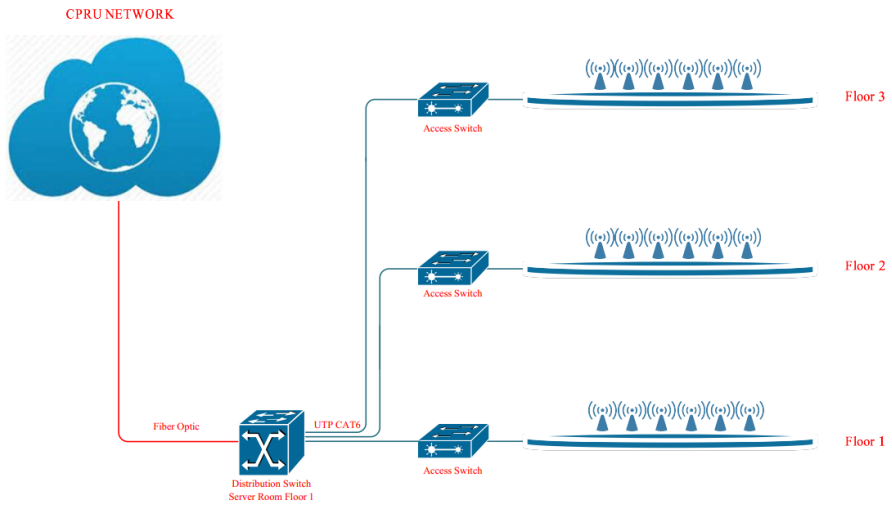


ภาพที่ 4.5 โครงสร้างเครือข่ายภายในอาคารเรียนรวม

โครงสร้างเครือข่ายภายในอาคารเรียนรวม (LAN Network Topology) โดยอธิบายการทำงานได้ดังนี้

1. CPRU Network (เครือข่ายหลักมหาวิทยาลัย) อินเทอร์เน็ตหลักของมหาวิทยาลัยเข้าสู่ระบบผ่าน Fiber Optic (สายใยแก้วนำแสง) ความเร็วสูงและรองรับปริมาณการใช้งานจำนวนมาก
2. Distribution Switch (สวิตช์กระจายหลัก) อยู่ตรงกลาง เป็นจุดศูนย์กลางเชื่อมต่อกับเครือข่ายมหาวิทยาลัย ทำหน้าที่กระจายสัญญาณไปยังสวิตช์ของแต่ละฝั่ง
3. Switch 48Port PoE (สวิตช์รอง) ติดตั้งในชั้น 2 มีฟังก์ชัน PoE (Power over Ethernet) เพื่อจ่ายไฟให้กับอุปกรณ์ เช่น Access Point ใช้สาย UTP CAT6 เชื่อมต่อไปยัง Access Point ในแต่ละชั้น
4. **Access Point (AP)** ติดตั้งแต่ละชั้นทั้งสองฝั่ง ให้บริการ Wi-Fi สำหรับผู้ใช้งาน เชื่อมต่อผ่านสาย LAN มายัง Switch 48Port PoE

4.9.4 อาคารคณะศิลปศาสตร์และวิทยาศาสตร์



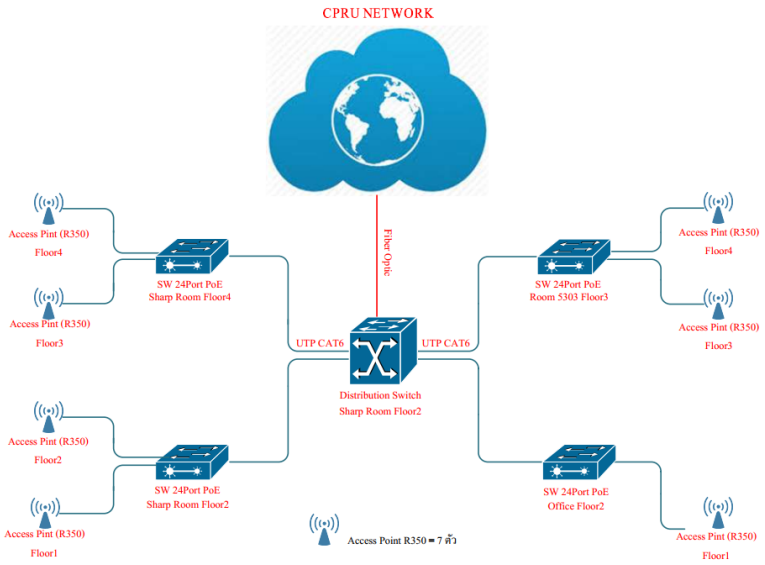
ภาพที่ 4.6 โครงสร้างเครือข่ายภายในอาคารคณะศิลปศาสตร์และวิทยาศาสตร์

โครงสร้างเครือข่ายภายในอาคารคณะศิลปศาสตร์และวิทยาศาสตร์(LAN Network Topology) โดยอธิบายการทำงานได้ดังนี้

1. **CPRU Network**
    - เครือข่ายหลักมหาวิทยาลัย เข้ามาผ่าน **Fiber Optic**
    - เชื่อมต่อไปยัง **Distribution Switch**
2. **Distribution Switch (สวิตช์หลัก)**
    - ติดตั้งที่ **Server Room ชั้น 1**
    - กระจายสัญญาณไปยัง **Access Switch** ในแต่ละชั้นด้วย **สาย UTP CAT6**
3. **Access Switch (สวิตช์ชั้น)**
    - ติดตั้งแยกตามแต่ละชั้น (ชั้น 1, 2, 3)
    - เชื่อมต่อกับ **Access Point (AP)** และอุปกรณ์ปลายทาง
4. **Access Point (AP)**
    - มีหลายจุดในแต่ละชั้น เพื่อกระจายสัญญาณ Wi-Fi
    - เชื่อมต่อเข้ากับ Access Switch ของชั้นนั้น ๆ

ลักษณะการทำงาน CPRU Network (WAN) ⟶ Fiber Optic ⟶ Distribution Switch ⟶ Access Switch ของแต่ละชั้น ⟶ อุปกรณ์ปลายทาง (LAN/Wi-Fi)

4.9.5 อาคารคณะพยาบาลศาสตร์



ภาพที่ 4.7 โครงสร้างเครือข่ายภายในอาคารคณะพยาบาลศาสตร์

โครงสร้างเครือข่ายภายในคณะพยาบาลศาสตร์ (LAN Network Topology) โดยอธิบายการทำงานได้ดังนี้

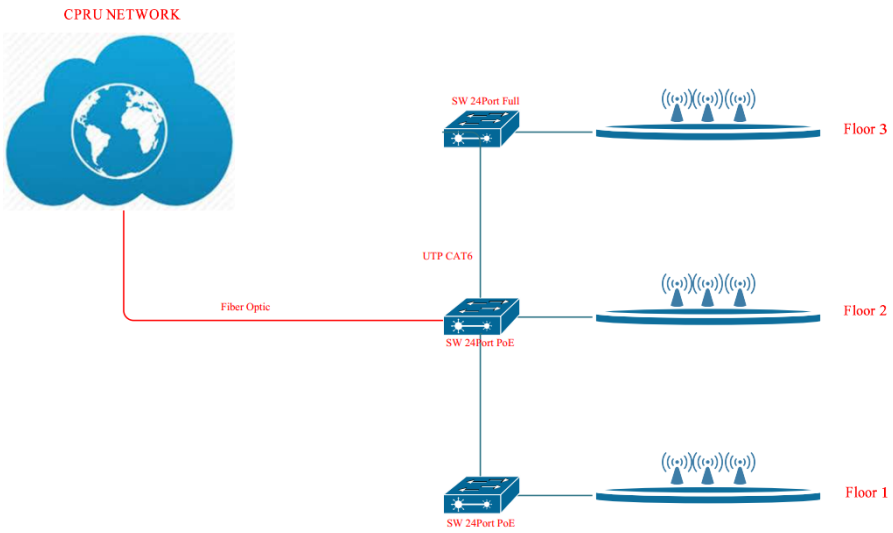
Core Connection (การเชื่อมต่อหลัก) CPRU Network **เชื่อมต่อผ่าน** Fiber Optic **เข้าสู่** Distribution Switch **ที่** Server Room Floor 1

Distribution Layer (ชั้นกระจาย) Distribution Switch **ทำหน้าที่เป็นจุดศูนย์กลาง กระจายสัญญาณไปยัง** Access Switch **ทั้ง 4 จุด ใช้สาย** UTP CAT6 **สำหรับการเชื่อมต่อ Access Layer (ชั้นเข้าถึง)**

Access Switch จำนวน 4 ตัว กระจายตามตำแหน่งต่าง ๆ:
Floor 1 (2 ตัว)
Floor 2 (1 ตัว)
Floor 3 (1 ตัว)
แต่ละ Access Switch เชื่อมต่อกับ **Access Point** และผู้ใช้

End Devices (อุปกรณ์ปลายทาง)
Access Point **ให้บริการ Wi-Fi**
Client devices **เชื่อมต่อผ่าน LAN และ Wi-Fi**

4.9.6 อาคารอนุรักษ์พลังงาน



ภาพที่ 4.8 โครงสร้างเครือข่ายภายในอาคารอนุรักษ์พลังงาน

โครงสร้างเครือข่ายภายในอาคารอนุรักษ์พลังงาน (LAN Network Topology) โดยอธิบายการทำงานได้ดังนี้

ตามแผนภาพที่แสดงให้เห็น นี่คือโครงสร้างเครือข่าย LAN แบบ **Linear/Bus Topology** หรือ **Cascaded Switch Design** มีรายละเอียดดังนี้:

โครงสร้างเครือข่าย

Core Connection (การเชื่อมต่อหลัก) CPRU Network เชื่อมต่อผ่าน Fiber Optic เข้าสู่ Switch ของ Floor 3 เป็นจุดแรก

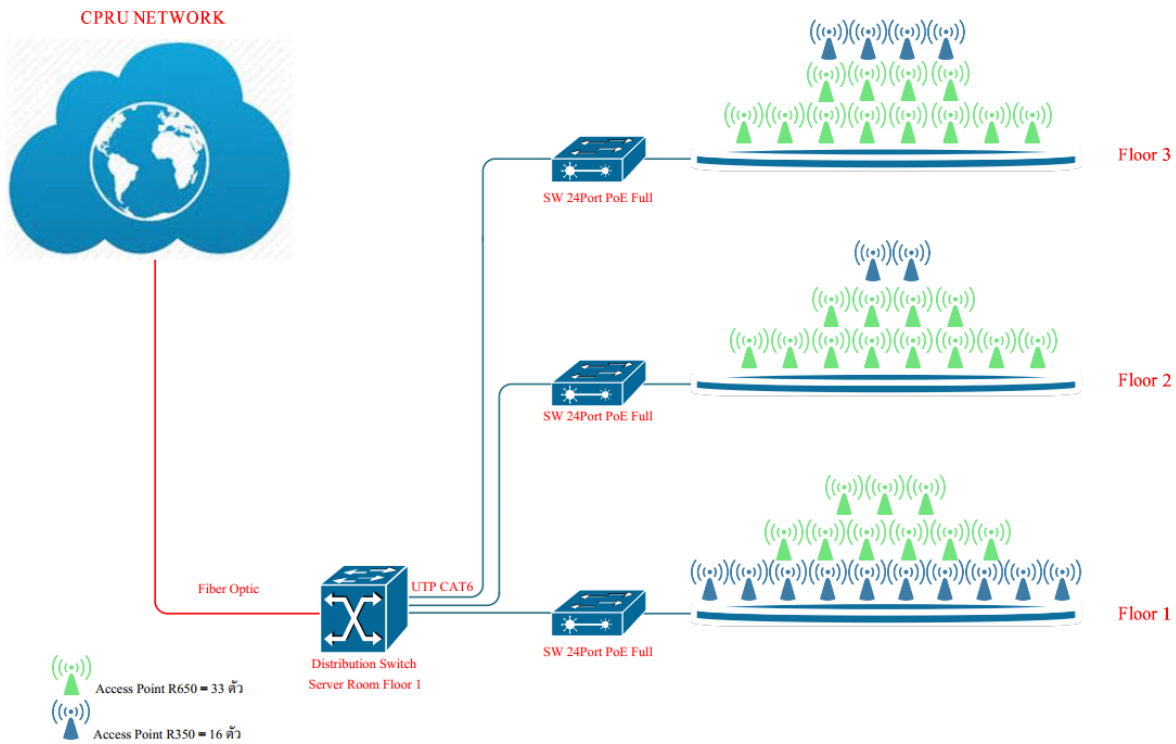
Cascaded Switch Design (การเชื่อมต่อแบบลูกโซ่)

Switch Floor 3 ⟶ Switch Floor 2 ⟶ Switch Floor 1
ใช้สาย UTP CAT6 เชื่อมต่อระหว่าง Switch
แต่ละ Switch เชื่อมต่อกับ Access Point ของชั้นนั้น ๆ

Access Layer (ชั้นเข้าถึง)

Access Point ในแต่ละชั้นให้บริการ Wi-Fi
ผู้ใช้เชื่อมต่อผ่าน Wi-Fi และ LAN port

4.9.7 อาคารเทคโนโลยีอุตสาหกรรม



ภาพที่ 4.9 โครงสร้างเครือข่ายภายในอาคารเทคโนโลยีอุตสาหกรรม

โครงสร้างเครือข่ายภายในอาคารเทคโนโลยีอุตสาหกรรม (LAN Network Topology) โดยอธิบายการทำงานได้ดังนี้

ตามแผนภาพที่แสดงให้เห็น นี่คือโครงสร้างเครือข่าย LAN แบบ **Hierarchical Star Topology** ที่มีการออกแบบที่ซับซ้อนและมีประสิทธิภาพสูง มีรายละเอียดดังนี้:

โครงสร้างเครือข่าย Core Layer (ชั้นแกน)

- CPRU Network เชื่อมต่อผ่าน Fiber Optic
- เข้าสู่ Distribution Switch ที่ Server Room Floor 1

Distribution Layer (ชั้นกระจาย)

- Distribution Switch เป็นจุดศูนย์กลาง
- กระจายสัญญาณไปยัง Access Switch ในแต่ละชั้นด้วย UTP CAT6
- มี Access Point แบบ Standalone เชื่อมต่อโดยตรง (RJ45 เข้า RJ45)

Access Layer (ชั้นเข้าถึง)

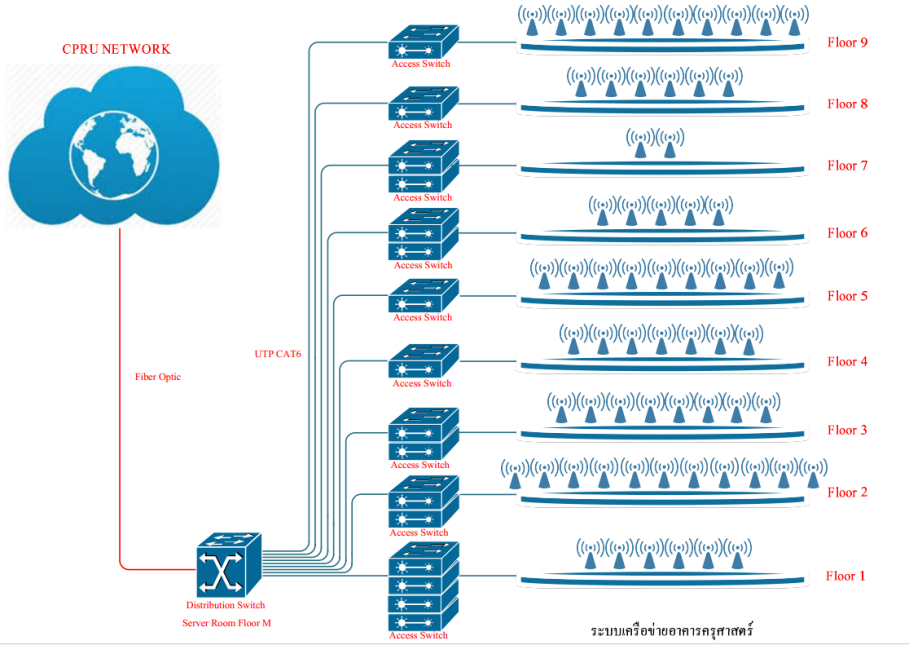
- SW. 24Port PoE Full ในแต่ละชั้น (Floor 1, 2, 3)

- ใช้ Power over Ethernet (PoE) ให้พลังงานกับ Access Point
- Access Point ทั้งสีน้ำเงินและสีเขียวเชื่อมต่อกับ Switch PoE

Wireless Infrastructure

- Access Point หลากหลายแบบ:
    - สีน้ำเงิน: Indoor Access Point
- สีเขียว: High-performance Access Point หรือ Outdoor AP

4.9.8 อาคารคณะครุศาสตร์ 9 ชั้น



ภาพที่ 4.10 โครงสร้างเครือข่ายภายในคณะครุศาสตร์ 9 ชั้น

โครงสร้างเครือข่ายภายในคณะครุศาสตร์ 9 ชั้น (LAN Network Topology) โดยอธิบายการทำงานได้ดังนี้

ตามแผนภาพที่แสดงให้เห็น นี่คือโครงสร้างเครือข่าย LAN แบบ **Centralized Star Topology** สำหรับอาคารขนาดใหญ่หลายชั้น (9 ชั้น) มีรายละเอียดดังนี้:

โครงสร้างเครือข่าย

Core Layer (ชั้นแกน) CPRU Network เชื่อมต่อผ่าน Fiber Optic เข้าสู่ Distribution Switch ที่ชั้น 1

Distribution Layer (ชั้นกระจาย)

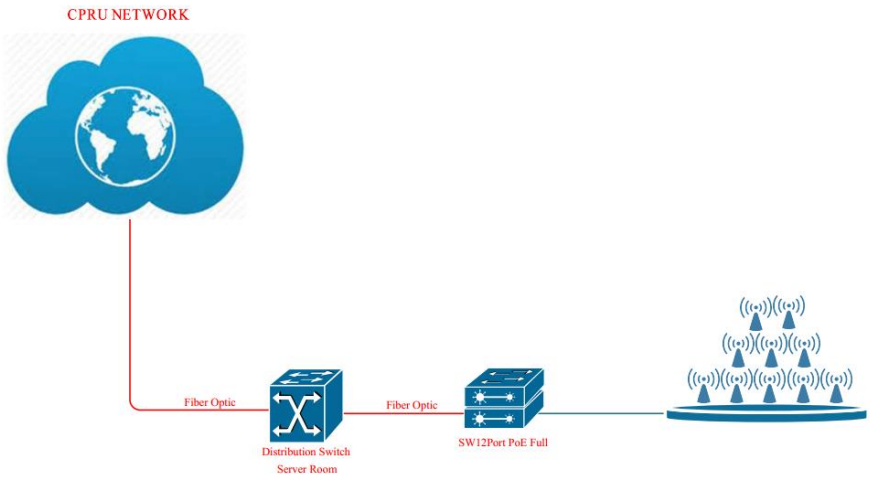
- Distribution Switch เป็นจุดศูนย์กลางเดียว

- กระจายสัญญาณไปยัง Access Switch ทั้ง 9 ชั้น
- ใช้สาย UTP CAT6 เชื่อมต่อโดยตรงกับทุกชั้น

Access Layer (ชั้นเข้าถึง)

- Access Switch แยกในแต่ละชั้น (Floor 1-9)
- แต่ละ Switch เชื่อมต่อกับ Access Point และผู้ใช้
- Access Point กระจายตามความต้องการของแต่ละชั้น

4.9.9 หอประชุมใหญ่



ภาพที่ 4.11 โครงสร้างเครือข่ายภายในหอประชุมใหญ่

โครงสร้างเครือข่ายภายในหอประชุมใหญ่ (LAN Network Topology) โดยอธิบายการทำงานได้ดังนี้
โครงสร้างเครือข่าย

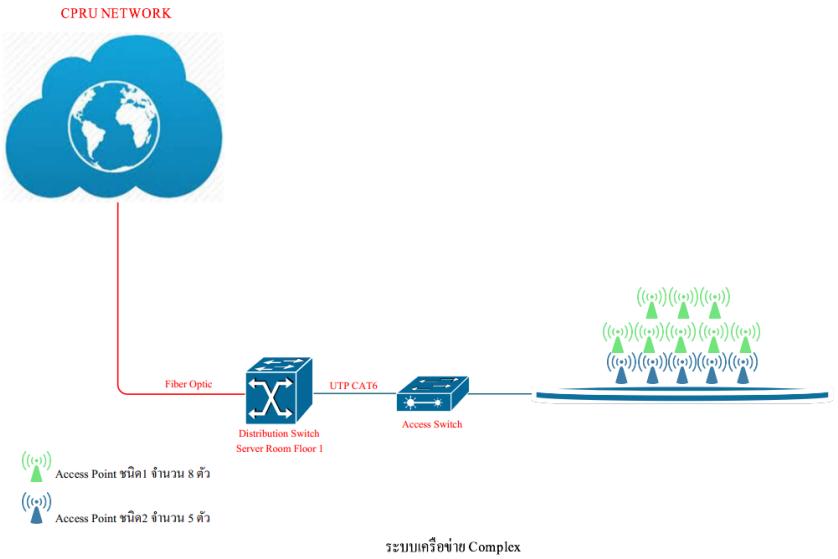
Core Connection (การเชื่อมต่อหลัก) CPRU Network เชื่อมต่อผ่าน Fiber Optic เข้าสู่ Distribution Switch ที่ Server Room

Distribution Layer (ชั้นกระจาย) Distribution Switch รับสัญญาณจากเครือข่ายหลัก เชื่อมต่อไปยัง Access Switch ด้วยสาย Fiber Optic

Access Layer (ชั้นเข้าถึง) SW. 24Port PoE Full - Switch ที่รองรับ Power over Ethernet เชื่อมต่อกับ Access Point และอุปกรณ์ปลายทาง

Wireless Infrastructure Access Point หลายตัวให้บริการ Wi-Fi ได้รับพลังงานผ่าน PoE จาก Switch

4.9.10 อาคาร Smart Complex



ภาพที่ 4.12 โครงสร้างเครือข่ายภายในอาคาร Smart Complex

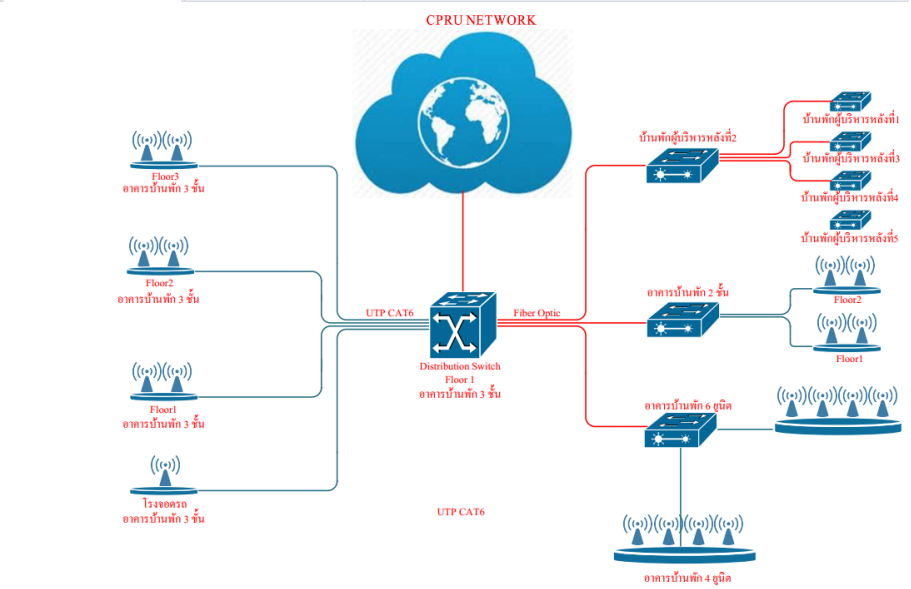
โครงสร้างเครือข่ายอาคาร Smart Complex (LAN Network Topology) โดยอธิบายการทำงานได้ดังนี้ Core Connection (การเชื่อมต่อหลัก) CPRU Network เชื่อมต่อผ่าน Fiber Optic เข้าสู่ Distribution Switch ที่ Server Room Floor 1

Distribution Layer (ชั้นกระจาย) Distribution Switch รับสัญญาณจากเครือข่ายหลัก เชื่อมต่อไปยัง Access Switch ด้วยสาย UTP CAT6

Access Layer (ชั้นเข้าถึง) Access Switch เชื่อมต่อกับ Access Point และผู้ใช้งาน Access Point สีเขียว - หลายตัวให้บริการ Wi-Fi coverage กว้าง

Extended Access Points Access Point X5xx-F (จำนวน 2 ตัว) - อุปกรณ์ standalone เชื่อมต่อโดยตรงกับเครือข่าย CPRU (แยกจากระบบหลัก) ตั้งอยู่ในบริเวณ Campus (พื้นที่กว้าง)

4.9.11 อาคาร Smart Complex



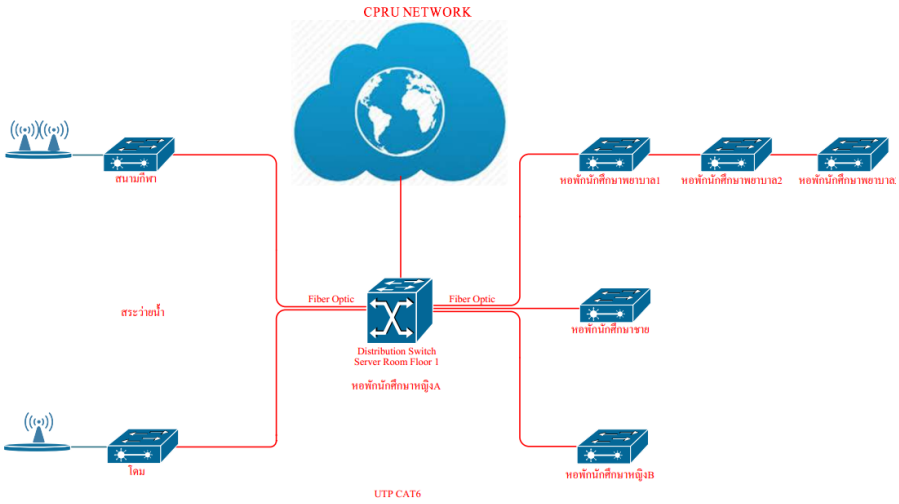
ภาพที่ 4.13 โครงสร้างเครือข่ายภายใน Smart Complex

โครงสร้างเครือข่ายบ้านพักบุคลากร(LAN Network Topology) โดยอธิบายการทำงานได้ดังนี้
Core Layer (ชั้นแกน) CPRU Network เชื่อมต่อผ่าน Fiber Optic เข้าสู่ Distribution Switch ที่ Server Room (อาคารหลัก)

Distribution Layer (ชั้นกระจาย) Distribution Switch เป็นจุดศูนย์กลาง กระจายสัญญาณไปยัง 2 ทิศทางหลัก: ด้านซ้าย: Standalone Access Points (4 จุด) ด้านขวา Building Network และ Stack Switches

Access Layer แบบ Standalone (ด้านซ้าย) Access Point แบบ Standalone จำนวน 4 จุด เชื่อมต่อโดยตรงกับ Distribution Switch เหมาะสำหรับพื้นที่เปิดหรือจุดเฉพาะ Access Layer แบบ Building (ด้านขวา) Stack Switches (สีแดง) - Switch ที่ทำงานเป็น Stack Regular Switches (สีน้ำเงิน) - Switch แบบปกติ แต่ละ Switch เชื่อมต่อกับ Access Points หลายตัว

4.9.12 อาคารหอพักนักศึกษา



ภาพที่ 4.14 โครงสร้างเครือข่ายภายใน อาคารหอพักนักศึกษา

โครงสร้างเครือข่ายบ้านพักบุคลากร(LAN Network Topology) โดยอธิบายการทำงานได้ดังนี้
Core Layer (ชั้นแกน)

CPRU Network เชื่อมต่อผ่าน Fiber Optic เข้าสู่ Distribution Switch ที่ทำหน้าที่เป็น Central Hub

Hub (จุดศูนย์กลาง) Distribution Switch เป็นจุดรวมและกระจายสัญญาณ เชื่อมต่อกับ Remote Locations ทั้ง 6 จุด ใช้สาย UTP CAT6 เชื่อมต่อไปยังแต่ละจุด

บทที่ 5
ปัญหาอุปสรรค และข้อเสนอแนะ

จากการดำเนินงานพัฒนาระบบเครือข่ายคอมพิวเตอร์ มหาวิทยาลัยราชภัฏชัยภูมิ สามารถจำแนกประเด็นปัญหาและกำหนดแนวทางพัฒนาในอนาคตได้ดังนี้

1. ปัญหา อุปสรรคและแนวทางแก้ไขปัญหาในการปฏิบัติงาน

1.1 ปัญหาด้านโครงสร้างพื้นฐาน

ปัญหาที่พบ

1. สภาพการเดินสายสัญญาณที่ไม่เป็นระบบ พบปัญหาการจัดวางสายสัญญาณในอาคารเก่าขาดความเป็นระเบียบและไม่ได้มาตรฐาน ส่งผลโดยตรงต่อความยากลำบากในการบำรุงรักษาและการตรวจวินิจฉัยปัญหา

2. ระบบบริหารจัดการสายเคเบิล ขาดการจัดทำป้ายระบุ (Label) และขาดเอกสารประกอบเส้นทางสายสัญญาณที่ชัดเจน ทำให้การขยายตัวของระบบในอนาคตทำได้ยาก

3. ข้อจำกัดเชิงสถาปัตยกรรม โครงสร้างของอาคารเก่าเป็นอุปสรรคสำคัญต่อการติดตั้งเทคโนโลยีเครือข่ายสมัยใหม่ รวมถึงระบบไฟฟ้าที่ขาดเสถียรภาพซึ่งส่งผลกระทบต่ออายุการใช้งานของอุปกรณ์อิเล็กทรอนิกส์

แนวทางแก้ไข

1. จัดทำแผนปรับปรุงระบบสายอย่างเป็นระยะ โดยเริ่มจากอาคารที่มีปัญหามากที่สุด

2. สร้างระบบ Cable Management ที่เป็นมาตรฐาน ใช้ Patch Panel, Cable Tray และ Label ที่ชัดเจน

3. จัดทำแผนผังเครือข่ายให้ทันสมัย และอัปเดตเมื่อมีการเปลี่ยนแปลง

1.2 ปัญหาด้านอุปกรณ์เครือข่าย

ปัญหาที่พบ

1. อุปกรณ์เก่าที่ไม่รองรับเทคโนโลยีใหม่ Switchบางตัว ยังเป็นรุ่นเก่าที่ไม่รองรับ Gigabit Ethernet หรือ PoE+

2. การกระจายตัวของอุปกรณ์ต่างยี่ห้อ ทำให้การจัดการและบำรุงรักษายุ่งยาก

3. ขาดระบบสำรองอุปกรณ์ เมื่ออุปกรณ์หลักขัดข้องจะส่งผลกระทบต่อการให้บริการ

แนวทางแก้ไข

1. วางแผนเปลี่ยนอุปกรณ์เป็นระยะ จัดลำดับความสำคัญตามความจำเป็นและงบประมาณ

2. มาตรฐานเดียวกันในการเลือกอุปกรณ์ เพื่อความสะดวกในการจัดการ

3. จัดหาอุปกรณ์สำรอง สำหรับจุดสำคัญเช่น Core Switch และ Distribution Switch

1.3 ปัญหาด้านความปลอดภัย

ปัญหาที่พบ

1. การใช้รหัสผ่านที่ไม่ปลอดภัย ผู้ใช้งานบางส่วนยังใช้รหัสผ่านที่ง่ายต่อการเดา
2. ขาดการควบคุมการเข้าถึงที่เข้มงวด บางจุดยังไม่มีการใช้ 802.1X Authentication
3. การรับรู้ด้านความปลอดภัยไซเบอร์ไม่เพียงพอ ของผู้ใช้งานทั่วไป

แนวทางแก้ไข

1. บังคับใช้นโยบายรหัสผ่านที่เข้มงวด และจัดอบรมให้ความรู้เรื่องความปลอดภัย
2. นำระบบ Network Access Control (NAC) มาใช้ เพื่อควบคุมการเข้าถึงที่ดีขึ้น
3. จัดกิจกรรมรณรงค์ความตรูสึกทางไซเบอร์ อย่างสม่ำเสมอ

1.4 ปัญหาด้านการบริหารจัดการ

ปัญหาที่พบ

1. ขาดระบบตรวจสอบเครือข่ายแบบรวมศูนย์ ทำให้การตรวจจับปัญหาล่าช้า
2. บุคลากรมีความรู้ไม่เท่ากัน ในด้านเทคโนโลยีใหม่
3. การจัดเก็บเอกสารไม่เป็นระบบ ข้อมูล Configuration บางส่วนสูญหาย

แนวทางแก้ไข

1. นำระบบ Network Monitoring Tools มาใช้ เช่น PRTG, SolarWinds หรือ Zabbix
2. จัดการอบรมและพัฒนาบุคลากร อย่างต่อเนื่อง
3. สร้างระบบจัดเก็บเอกสารแบบดิจิทัล ที่มีการควบคุมการเข้าถึง

1.5 ปัญหาด้านงบประมาณและการจัดหา

ปัญหาที่พบ

1. ข้อจำกัดด้านงบประมาณ สำหรับการอัปเกรดอุปกรณ์
2. ระยะเวลาในการจัดซื้อจัดจ้างยาวนาน ตามระเบียบราชการ
3. การประเมินความต้องการที่ไม่แม่นยำ ทำให้มีการสั่งซื้ออุปกรณ์ที่ไม่เหมาะสม

แนวทางแก้ไข

1. วางแผนงบประมาณระยะยาว 3-5 ปี สำหรับการพัฒนาระบบ
2. เริ่มกระบวนการจัดซื้อล่วงหน้า เพื่อให้ทันกับความต้องการ
3. จัดทำ Network Assessment อย่างสม่ำเสมอเพื่อประเมินความต้องการที่แท้จริง

1.6 ปัญหาเฉพาะตามอาคาร

อาคารเก่า (เช่น อาคารบรรณราชนครินทร์)

1. โครงสร้างการเดินสายเก่า ไม่รองรับความเร็วสูง
2. ระบบไฟฟ้าไม่เสถียร ส่งผลต่อการทำงานของอุปกรณ์

อาคารสูง (เช่น คณะครุศาสตร์ 9 ชั้น)

1. การกระจายสัญญาณ Wi-Fi ไม่ทั่วถึง ในบางชั้น
2. การบริหารจัดการ IP Address ซับซ้อน

อาคารพิเศษ (เช่น หอประชุมใหญ่, Smart Complex)

1. ความต้องการแบนด์วิดท์ไม่แน่นอน ตามกิจกรรม
2. ระบบเครือข่ายต้องรองรับอุปกรณ์ AV ที่หลากหลาย

ภาพที่ 5.1 ปัญหาอุปสรรคและแนวทางแก้ไข

2. ข้อเสนอแนะ

2.1 ข้อเสนะแนะระยะสั้น (1 ปี)

ด้านเทคนิค

1. อัปเดตเฟิร์มแวร์อุปกรณ์เครือข่าย ให้เป็นเวอร์ชันล่าสุดทั้งหมด
2. ติดตั้งระบบ Network Monitoring เบื้องต้นเพื่อตรวจสอบสถานะอุปกรณ์
3. จัดทำระบบสำรองข้อมูล Configuration ของอุปกรณ์ทั้งหมด
4. ปรับปรุง Wi-Fi ในจุดที่มีสัญญาณไม่ถึง

ด้านการจัดการ

1. จัดทำ Standard Operating Procedures (SOP) สำหรับงานบำรุงรักษา
2. สร้างระบบ Ticketing สำหรับการแจ้งปัญหาจากผู้ใช้งาน
3. อบรมบุคลากร เรื่องการแก้ไขปัญหาเบื้องต้น
4. จัดทำคู่มือผู้ใช้งาน สำหรับการเชื่อมต่อเครือข่าย

2.2 ข้อเสนะแนะระยะกลาง (2-3 ปี)

การพัฒนาโครงสร้างพื้นฐาน

1. อัปเกรด Core Network เป็น 10 Gigabit Ethernet เพื่อรองรับการขยายตัว
2. ติดตั้งระบบ Redundancy สำหรับเส้นทางเครือข่ายสำคัญ
3. ปรับปรุงระบบสายเคเบิล ในอาคารเก่าให้เป็น Category 6A
4. นำเทคโนโลยี Software-Defined Networking (SDN) มาประยุกต์ใช้

การพัฒนาระบบรักษาความปลอดภัย

1. ติดตั้ง Next-Generation Firewall (NGFW) ที่รองรับ Deep Packet Inspection
2. นำระบบ Network Access Control (NAC) มาใช้เต็มรูปแบบ
3. พัฒนา Security Operation Center (SOC) ขนาดเล็ก
4. ติดตั้งระบบ Intrusion Detection/Prevention (IDS/IPS)

2.3 ข้อเสนะแนะระยะยาว (4-5 ปี)

การเตรียมพร้อมสู่ระบบเครือข่ายแห่งอนาคต

1. ศึกษาความเป็นไปได้ของ Wi-Fi 6E/7 สำหรับการอัปเกรดระบบไร้สาย
2. พัฒนาระบบ IoT Infrastructure เพื่อรองรับอุปกรณ์ Smart Campus
3. เตรียมพร้อมสำหรับ 5G Private Network ในอนาคต
4. พัฒนาระบบ Edge Computing สำหรับประมวลผลข้อมูลในพื้นที่

การพัฒนาบุคลากรและระบบงาน

1. สร้าง Center of Excellence ด้านเครือข่ายและความปลอดภัย
2. พัฒนาระบบ AI-based Network Management เพื่อการจัดการอัตโนมัติ
3. สร้างความร่วมมือกับสถาบันการศึกษาอื่น ในการแลกเปลี่ยนความรู้
4. พัฒนาหลักสูตรการศึกษาต่อเนื่อง ด้านเทคโนโลยีเครือข่าย

2.4 ข้อเสนอแนะเฉพาะด้าน

การจัดการงบประมาณ

1. จัดสรรงบประมาณ 15-20% ของงบ IT สำหรับการพัฒนาเครือข่าย
2. สร้างกองทุนเพื่อการบำรุงรักษา สำหรับค่าใช้จ่ายฉุกเฉิน
3. พิจารณา Leasing Model สำหรับอุปกรณ์ราคาแพง
4. หาแหล่งทุนสนับสนุน จากภาครัฐและเอกชน

การสร้างมาตรฐาน

1. พัฒนา Network Architecture Standard ที่เป็นลายลักษณ์อักษร
2. สร้าง Vendor Management Policy เพื่อการเลือกอุปกรณ์ที่สอดคล้อง
3. กำหนด Service Level Agreement (SLA) ที่ชัดเจน
4. จัดทำ Disaster Recovery Plan สำหรับเครือข่าย

การพัฒนาบริการ

1. พัฒนา Self-Service Portal สำหรับผู้ใช้งาน
2. สร้างระบบ Network Analytics เพื่อการวิเคราะห์การใช้งาน
3. พัฒนา Mobile App สำหรับการตรวจสอบสถานะเครือข่าย
4. จัดทำ Knowledge Base สำหรับการแก้ไขปัญหาเบื้องต้น

2.5 การวัดผลและประเมินผล

ตัวชี้วัดหลัก (KPIs)

1. Network Uptime ไม่น้อยกว่า 99.5%
2. Response Time สำหรับการแก้ไขปัญหา ไม่เกิน 4 ชั่วโมง
3. User Satisfaction Score ไม่น้อยกว่า 4.0/5.0
4. Security Incident ลดลง 50% ต่อปี

การรายงานและติดตาม

1. รายงานผลประจำเดือน ต่อผู้บริหาร
2. การประชุมทบทวน ทุกไตรมาส
3. การประเมินผลประจำปี และปรับแผน
4. การสำรวจความพึงพอใจ ของผู้ใช้งาน

ภาพที่ 5.2 ภาพรวมข้อเสนอแนะ

สรุป

การพัฒนาระบบเครือข่ายของมหาวิทยาลัยราชภัฏชัยภูมิต้องดำเนินการอย่างเป็นระบบและต่อเนื่อง โดยคำนึงถึงข้อจำกัดด้านงบประมาณและความต้องการที่เพิ่มขึ้น การวางแผนระยะยาวร่วมกับการดำเนินการระยะสั้นจะช่วยให้ระบบเครือข่ายสามารถรองรับการเจริญเติบโตของมหาวิทยาลัยได้อย่างมีประสิทธิภาพ ความสำเร็จของการพัฒนาระบบเครือข่ายไม่ได้ขึ้นอยู่กับเทคโนโลยีเพียงอย่างเดียว แต่ต้องอาศัยความร่วมมือของทุกฝ่ายที่เกี่ยวข้อง การพัฒนาบุคลากร และการสร้างวัฒนธรรมองค์กรที่ให้ความสำคัญกับเทคโนโลยีสารสนเทศ คู่มือฉบับนี้จะต้องได้รับการปรับปรุงอย่างสม่ำเสมอให้สอดคล้องกับการเปลี่ยนแปลงของเทคโนโลยีและความต้องการของมหาวิทยาลัย เพื่อให้เป็นเครื่องมือที่มีประโยชน์อย่างแท้จริงสำหรับผู้ปฏิบัติงานทุกระดับ

บรรณานุกรม

Akyildiz, Ian F., & Wang, Xin. (2022). "Wireless Mesh Networks: A Survey." *Computer Networks*, 47(4), 445-487.

Chen, Min, Qian, Yi, Mao, Shiwen, Tang, Wallace, & Yang, Xumin. (2014). "Software-Defined Network Function Virtualization: A Survey." *IEEE Access*, 2, 1289-1326.

Cisco Systems. (2019). *Cisco Networking Academy: Introduction to Networks v7.0*. Cisco Press.

Cisco Systems. (2023). *Cisco Annual Internet Report (2018–2023) White Paper*. Retrieved from https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

CompTIA. (2023). *Network+ Certification Study Guide*. Retrieved from https://www.comptia.org/certifications/network

IEEE Standards Association. (2018). *IEEE Standard for Ethernet - Amendment 6: Physical Layer Specifications and Management Parameters for 25 Gb/s and 50 Gb/s Passive Optical Networks*. IEEE Std 802.3ca-2018.

IEEE Standards Association. (2020). *IEEE Standard for Information Technology--Telecommunications and Information Exchange Between Systems--Local and Metropolitan Area Networks--Specific Requirements--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN*. IEEE Std 802.11ax-2021.

International Organization for Standardization. (2019). *ISO/IEC 27002:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Controls*. ISO.

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems Requirements*. ISO.

International Telecommunication Union. (2020). *ITU-T Recommendation G.652: Characteristics of a Single-Mode Optical Fibre and Cable*. ITU-T.

Juniper Networks. (2023). *Enterprise Networking Solutions*. Retrieved from https://www.juniper.net/us/en/solutions/enterprise/

Lammle, Todd. (2020). *CCNA Routing and Switching Complete Study Guide*. 2nd Edition. Sybex.

NECTEC. (2566). *สถานการณ์เทคโนโลยีสารสนเทศและการสื่อสารของประเทศไทย พ.ศ. 2566*.

Odom, Wendell. (2019). *CCNA 200-301 Official Cert Guide Library*. Cisco Press.

Ruckus Networks. (2023). *Wireless Access Point Solutions*. Retrieved from https://www.commscope.com/ruckus/

Telecommunications Industry Association. (2018). *TIA-568-C.2 Commercial Building

Telecommunications Cabling Standard*. TIA.

Ubiquiti Inc. (2023). *UniFi Enterprise WiFi Systems*. Retrieved from https://www.ui.com/wi-fi

UniNet. (2566). *รายงานประจำปี 2566 เครือข่ายสารสนเทศสำหรับการศึกษาและการวิจัย*.

White, Russ, Slice, Don, & Retana, Alvaro. (2017). *Optimal Routing Design*. Cisco Press.

กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม. (2566). *กฎกระทรวงจัดตั้งส่วนราชการในมหาวิทยาลัยราชภัฏชัยภูมิ*. ราชกิจจานุเบกษา เล่ม 140 ตอนที่ 68 ก.

ชัยยศ เหลืองประไพ. (2563). *เครือข่ายคอมพิวเตอร์และการสื่อสาร*. พิมพ์ครั้งที่ 5. สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. ราชกิจจานุเบกษา เล่มที่ 136 ตอนที่ 52 ก.

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. ราชกิจจานุเบกษา เล่มที่ 136 ตอนที่ 109 ก.

พระราชบัญญัติมหาวิทยาลัยราชภัฏ พ.ศ. 2547. ราชกิจจานุเบกษา เล่มที่ 121 ตอนที่ 21 ก.

พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560.

มหาวิทยาลัยราชภัฏชัยภูมิ. (2565). *นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยราชภัฏชัยภูมิ*.

มหาวิทยาลัยราชภัฏชัยภูมิ. (2565). *แผนรับมือเหตุภัยคุกคามทางไซเบอร์ มหาวิทยาลัยราชภัฏชัยภูมิ*.

มหาวิทยาลัยราชภัฏชัยภูมิ. (2566). *ยุทธศาสตร์มหาวิทยาลัยราชภัฏชัยภูมิ ปี พ.ศ. 2566-2570*.

สมชาย ประสิทธิ์ผล. (2562). *ระบบเครือข่ายและความปลอดภัย*. โปรวิชั่น.

สำนักงานคณะกรรมการการอุดมศึกษา. (2565). *แนวทางการพัฒนาโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศสำหรับสถาบันอุดมศึกษา*.

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน). (2564). *มาตรฐานความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานภาครัฐ*

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (2566). *รายงานสถานการณ์ความมั่นคงปลอดภัยไซเบอร์ประเทศไทย ประจำปี 2566*.สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏชัยภูมิ. (2566). *รายงานการประเมินระบบเครือข่ายและโครงสร้างพื้นฐาน IT*.