คู่มือการปฏิบัติงาน

เรื่องการตั้งค่าอุปกรณ์
กระจายสัญญาณระบบเครือข่าย

ว่าที่ ร.ต. อุดมศักดิ์ ใจดี
นักคอมพิวเตอร์ปฏิบัติการ

ฝ่ายบริหารและพัฒนาดิจิทัลเทคโนโลยี

สำนักดิจิทัลเทคโนโลยี มหาวิทยาลัยศิลปากร พ.ศ. 2565

คำนำ

การจัดทำคู่มือการตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่าย ของฝ่ายบริหารและพัฒนาดิจิทัลเทคโนโลยี สำนักดิจิทัลเทคโนโลยี มหาวิทยาลัยศิลปากร มีวัตถุประสงค์เพื่อใช้เป็นแนวทางการดำเนินงาน การบริหารจัดการ การดูแลและปฏิบัติงานเพื่อสามารถให้บริการเชื่อมต่อระบบเครือข่ายสารสนเทศ (SUNet) ไปยังคณะ หน่วยงานภายในมหาวิทยาลัยศิลปากรทุกวิทยาเขต เพื่อใช้ในการสนับสนุนการเรียนการสอนของนักศึกษา การปฏิบัติงานของบุคลากรและสนับสนุนภาระกิจต่าง ๆ ของมหาวิทยาลัยได้อย่างเป็นระบบและมีประสิทธิภาพ

ผู้จัดทำจึงหวังเป็นอย่างยิ่งว่า คู่มือการตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่าย ฉบับนี้จะมีประโยชน์ เป็นแนวทางในการปฏิบัติงาน การพัฒนาการบำรุงรักษาระบบให้สามารถพร้อมใช้งานสำหรับผู้ที่เกี่ยวข้องได้อย่างถูกต้องและมีประสิทธิภาพต่อไป หากคู่มือฉบับนี้มีข้อผิดพลาดประการใด ผู้จัดทำขอน้อมรับข้อผิดพลาดดังกล่าวเพื่อนำมาปรับปรุง พัฒนาคู่มือให้มีความครบถ้วนสมบูรณ์ต่อไป

ว่าที่ ร.ต.อุดมศักดิ์ ใจดี
นักคอมพิวเตอร์ปฏิบัติการ

สารบัญ

สารบัญ (ต่อ)

สารบัญ (ต่อ)

สารบัญ (ต่อ)

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญรูป

สารบัญรูป (ต่อ)

บทที่ 1
บทนำ

1.1 ความเป็นมา ความจำเป็น และความสำคัญ

ปัจจุบันระบบเครือข่ายคอมพิวเตอร์และระบบเทคโนโลยีสารสนเทศมีบทบาทสำคัญมากต่อการขับเคลื่อนองค์กรทั้งภาครัฐ เอกชน รวมสถาบันการศึกษาทุกภาคส่วน ล้วนมีความจำเป็นในการนำระบบเทคโนโลยีสารสนเทศมาใช้ เพื่อสนับสนุนการตัดสินใจและการดำเนินงานบริหารจัดการภายในองค์กร เพราะระบบสารสนเทศช่วยให้ระบบการทำงานต่างๆ มีความคล่องตัว สะดวกรวดเร็ว ลดความซ้ำซ้อนของระบบงานลง ประหยัดเวลาและงบประมาณ

ระบบเครือข่ายทำหน้าที่เป็นหนึ่งในโครงสร้างระบบสารสนเทศพื้นฐาน เป็นตัวกำหนดแนวทางนโยบายขององค์กรเพื่อมุ่งสู่ความสำเร็จตามเป้าหมาย ดังนั้นการออกแบบระบบเครือข่ายที่ดีต้องคำนึงถึงเรื่องประสิทธิภาพและความปลอดภัยในการรับส่งข้อมูลในระบบเครือข่ายเป็นหลัก จะทำให้รับส่งข้อมูลในระบบเครือข่ายสามารถทำงานได้ต่อเนื่อง ถูกต้อง รวดเร็ว และมีประสิทธิภาพ

มหาวิทยาลัยศิลปากรเป็นมหาวิทยาลัยชั้นนำที่มีความเป็นเลิศทางวิชาการ มุ่งบูรณาการศิลปวัฒนธรรม และวิทยาศาสตร์พัฒนาผู้เรียนด้วยวิธีการเรียนการสอนที่หลากหลายให้มีทักษะที่จำเป็นในศตวรรษที่ 21 มีอัตลักษณ์ด้านความคิดสร้างสรรค์ มีความรับผิดชอบต่อสังคมและสิ่งแวดล้อม เป็นพลเมืองตื่นรู้ ฉะนั้นหากมีการวางแผนด้านโครงสร้างพื้นฐานระรบบสารสนเทศที่ดีและมีประสิทธิภาพ จะทำให้เกิดการพัฒนาองค์ความรู้ในการเรียนการสอน และเป็นแนวทางไปสู่การพัฒนาองค์กรที่ยั่งยืนในอนาคต

ดังนั้นความจำเป็นและความสำคัญในการดำเนินงานดังกล่าว ผู้ดูแลระบบในฐานะนักคอมพิวเตอร์ปฏิบัติการจึงมีความสนใจที่จะเขียนคู่มือการปฏิบัติงาน การตั้งค่าอุปกรณ์กระจายสัญญาณเครือข่ายเพื่อเป็นแนวทางให้บุคลากรภายในมหาวิทยาลัยศิลปากรสามารถปฏิบัติงานทดแทนกันได้

1.2 วัตถุประสงค์ในการจัดทำคู่มือ

1.2.1 เพื่อจัดทำคู่มือปฏิบัติงานและเทคนิคที่ชัดเจน แสดงขั้นตอนการปฏิบัติงานที่ถูกต้อง

1.2.2 เพื่อใช้เป็นแนวทางให้ผู้ปฏิบัติสามารถทำงานได้อย่างถูกต้องและมีประสิทธิภาพ

1.2.3 เพื่อถ่ายทอดหรือเผยแพร่องค์ความรู้ ให้กับบุคลากรทั้งภายในและภายนอกมหาวิทยาลัยได้

1.3. ประโยชน์ที่ได้รับ

1.3.1 ได้คู่มือปฏิบัติงาน เพื่อใช้เป็นแนวทางปฏิบัติงานได้อย่างถูกต้องตามขั้นตอน

1.3.2 บุคลากรหรือเจ้าหน้าที่สามารถปฏิบัติงานได้อย่างถูกต้องตามขั้นตอนและมีประสิทธิภาพตามมาตรฐานเดียวกัน

1.3.3 สามารถนำความรู้ที่ได้จากคู่มือไปเผยแพร่ให้กับบุคลากรหรือผู้ที่สนใจได้

1.4. ขอบเขตของคู่มือ

คู่มือการตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่ายสำหรับผู้ดูแลระบบนี้ จัดทำขึ้นเพื่อใช้เป็นแนวทางในการออกแบบและเชื่อมต่อระบบเครือข่าย กรณีศึกษาหอพักนักศึกษา ภายในมหาวิทยาลัยศิลปากร วิทยาเขตพระราชวังสนามจันทร์ เพื่อให้บริการและสนับสนุนการเรียนการสอนของนักศึกษาและบุคลากรของมหาวิทยาลัยศิลปากรทุกวิทยาเขต ดังนี้

1.4.1 รวบรวมข้อมูลความต้องการและปัญหาระบบเครือข่าย ข้อจำกัดต่าง ๆ ของหน่วยงาน

1.4.2 ออกแบบระบบเครือข่ายตามความต้องการของหน่วยงาน

1.4.3 การตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่ายแต่ละผลิตภัณฑ์

1.4.4 การเชื่อมต่อระบบเครือข่ายระหว่างหน่วยงาน อาคาร

1.4.5 การเชื่อมต่ออุปกรณ์เครือข่ายไร้สาย

1.4.6 การทดสอบการใช้งานอุปกรณ์กระจายสัญญาณระบบเครือข่ายก่อนติดตั้งจริง

1.4.7 การตรวจสอบแก้ไขปัญหา

1.4.8 การสำรองการตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่าย

1.4.9 จัดทำคู่มือและสรุปผลการทำงานของระบบเครือข่าย

1.5 นิยามศัพท์เฉพาะ

มหาวิทยาลัย	หมายความว่า	มหาวิทยาลัยศิลปากร
สำนัก	หมายความว่า	สำนักดิจิทัลเทคโนโลยี มหาวิทยาลัยศิลปากร
บุคลากร	หมายความว่า	ข้าราชการพลเรือนในสถาบันอุดมศึกษาและพนักงานมหาวิทยาลัยที่ดำรงตำแหน่ง 1. ผู้บริหาร ได้แก่ อธิการบดี คณบดี ผู้อำนวยการ เป็นต้น 2. สายวิชาการ ได้แก่บุคลากรที่ดำรงตำแหน่ง ศาสตราจารย์ รองศาสตราจารย์ ผู้ช่วยศาสตราจารย์ และอาจารย์

		3) สายสนับสนุน ได้แก่ บุคลากรสายสนับสนุนลูกจ้างประจำลูกจ้างของมหาวิทยาลัย
นักศึกษา	หมายความว่า	นักศึกษามหาวิทยาลัยศิลปากร
ระบบเครือข่าย	หมายความว่า	ระบบเครือข่ายคอมพิวเตอร์มหาวิทยาลัยศิลปากร
ผู้ดูแลระบบ	หมายความว่า	ผู้ที่ได้รับมอบหมายจากหัวหน้าส่วนงานให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบคอมพิวเตอร์และระบบเครือข่ายให้ทำงานได้อย่างมีประสิทธิภาพ
Switch	หมายความว่า	อุปกรณ์กระจายสัญญาณระบบเครือข่ายทำหน้าที่เชื่อมต่อเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายให้สามารถสื่อสารแลกเปลี่ยนข้อมูลซึ่งกันและกันได้
Configuration	หมายความว่า	การตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่ายเพื่อกำหนดคุณสมบัติให้สามารถทำงานได้ตรงตามเป้าหมายอย่างมีประสิทธิภาพและเหมาะสมกับงานที่ต้องการ
Access point	หมายความว่า	อุปกรณ์กระจายสัญญาณระบบเครือข่ายไร้สาย
Monitoring	หมายความว่า	การเฝ้าระวังและติดตามสถานะการทำงานของอุปกรณ์กระจายสัญญาณระบบเครือข่ายให้สามารถทำงานได้อย่างต่อเนื่อง
Wireless Controller	หมายความว่า	ระบบควบคุมเครือข่ายไร้สาย
ระบบเครือข่ายไร้สาย	หมายความว่า	ระบบที่มีการเชื่อมต่อและการรับ-ส่งข้อมูลโดยใช้สัญญาณวิทยุในการสื่อสารข้อมูลทั้งข้อมูลภายในและภายนอกของมหาวิทยาลัย
การบริหารจัดการเครือข่าย	หมายความว่า	การดูแลระบบเครือข่ายคอมพิวเตอร์และการบริหารจัดการทรัพยากรในระบบเครือข่ายให้สามารถทำงานได้อย่างมีประสิทธิภาพสูงสุด

บทที่ 2
โครงสร้างองค์กร และบทบาทหน้าที่ความรับผิดชอบ

2.1 ประวัติความเป็นมาสำนักดิจิทัลเทคโนโลยี [1]

สำนักดิจิทัลเทคโนโลยี มหาวิทยาลัยศิลปากร (เดิมชื่อ ศูนย์คอมพิวเตอร์ มหาวิทยาลัยศิลปากร) ได้รับอนุมัติจัดตั้งอย่างเป็นทางการในปี พ.ศ. 2533 และได้เปลี่ยนชื่อเป็น สำนักดิจิทัลเทคโนโลยี เมื่อปี พ.ศ.2562 โดยมีภารกิจหลักในการให้บริการเครื่องคอมพิวเตอร์เพื่อประกอบการเรียนการสอนในรายวิชาต่าง ๆ ของมหาวิทยาลัย บริการทางด้านห้องปฏิบัติการคอมพิวเตอร์เพื่อใช้เป็นสถานที่ฝึกประสบการณ์ให้แก่นักศึกษาด้วยเทคโนโลยีที่ทันสมัย นอกจากนั้นสำนักดิจิทัลเทคโนโลยี ยังให้บริการพัฒนาระบบงานคอมพิวเตอร์และระบบสารสนเทศเพื่อการบริหารงานของมหาวิทยาลัย พร้อมทั้งส่งเสริมการผลิตสื่อการเรียนการสอนในรายวิชาต่าง ๆ ของมหาวิทยาลัยศิลปากร การให้บริการพัฒนาระบบงานคอมพิวเตอร์และระบบสารสนเทศเพื่อการบริหารงานของมหาวิทยาลัย การฝึกอบรมทางด้านวิชาการให้แก่บุคลากรของมหาวิทยาลัย การให้บริการด้านระบบเครือข่าย การวิเคราะห์ข้อมูลและตรวจกระดาษคำตอบด้วยระบบคอมพิวเตอร์แก่ส่วนราชการและหน่วยงานต่าง ๆ ตลอดจนดำเนินการวิจัยในด้านการพัฒนาซอฟต์แวร์ที่เป็นประโยชน์ต่อชุมชน สำนักดิจิทัลเทคโนโลยีได้ให้บริการดังกล่าวในทุกวิทยาเขต ได้แก่ วิทยาเขตวังท่าพระ วิทยาเขตพระราชวังสนามจันทร์ วิทยาเขตสารสนเทศเพชรบุรี สำนักงานอธิการบดีตลิ่งชัน และวิทยาเขตซิตี้แคมปัสเมืองทองธานี

รายนามผู้อำนวยการสำนักดิจิทัลเทคโนโลยีตั้งแต่เริ่มก่อตั้งจนถึงปัจจุบัน

พ.ศ. 2533 - 2541	ผู้ช่วยศาสตราจารย์รุจิรา พิพิธพจนการณ์
พ.ศ. 2542 - 2549	รองศาสตราจารย์ ดร.ปานใจ ธารทัศนวงษ์
พ.ศ. 2550 - 2554	อาจารย์รวิทัต ภู่หลำ
พ.ศ. 2554 - 2563	ผู้ช่วยศาสตราจารย์ฉัตรชัย เผ่าทองจีน
พ.ศ. 2563 - ปัจจุบัน	อาจารย์ ดร.สุภาพ เกิดแสง

2.2 ปรัชญา ปณิธาน วิสัยทัศน์ ภารกิจ ค่านิยม ยุทธศาสตร์

ปรัชญา ระบบเทคโนโลยีสารสนเทศและการสื่อสารเป็นกลไกพื้นฐานในการขับเคลื่อนองค์กร

ปณิธาน มุ่งมั่นสร้างสรรค์การให้บริการด้านเทคโนโลยีสารสนเทศที่มีคุณภาพตอบสนองต่อความต้องการของมหาวิทยาลัยศิลปากร

วิสัยทัศน์ สำนักดิจิทัลเทคโนโลยีเป็นผู้นำด้านการบริการและการพัฒนานวัตกรรมดิจิทัลเทคโนโลยี

พันธกิจ

1) ให้บริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่ทันสมัย เพื่อการสนับสนุนงานด้านการเรียนการสอนและการวิจัยของมหาวิทยาลัย

2) ให้บริการและสนับสนุนการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการสนับสนุนงานด้านบริหารจัดการของมหาวิทยาลัย

3) สนับสนุนการค้นคว้าและสร้างสรรค์ผลงานวิจัยของสำนักดิจิทัลเทคโนโลยีซึ่งนำไปสู่การพัฒนาผลงานไปประยุกต์ใช้งานในภารกิจต่าง ๆ ของมหาวิทยาลัย

4) ให้บริการทางวิชาการแก่สังคมเพื่อเสริมสร้างความเข้มแข็งแก่ชุมชนในด้านการพัฒนาและการประยุกต์ใช้เทคโนโลยีสารสนเทศพร้อมทั้งสนับสนุนงานบริการวิชาการแก่สังคมของมหาวิทยาลัย

5) สนับสนุนสืบสานทำนุบำรุงศิลปวัฒนธรรมโดยการประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสารร่วมกับภูมิศาสตร์สารสนเทศในการดำเนินกิจกรรม

ค่านิยม

DRIVE

D Digital Technology	มีความเป็นเลิศด้านดิจิทัลเทคโนโลยี
R Responsibility	มีความรับผิดชอบต่อหน้าที่และการทำงานด้วยจิตบริการ
I Innovation & Intelligence	มีความคิดสร้างสรรค์ สร้างนวัตกรรมและองค์ความรู้
V Vision & Visibility	มีวิสัยทัศน์การทำงานที่ก้าวไกล
E Excellence & Expertise & Ethic & Efficiency & Engagement	ทำงานร่วมกันด้วยความเชี่ยวชาญอย่างมีประสิทธิภาพ มีคุณธรรมและจริยธรรม

ยุทธศาสตร์สำนักดิจิทัลเทคโนโลยี

1) พัฒนาและปรับปรุงระบบเทคโนโลยีสารสนเทศให้เหมาะสมและเอื้อต่อความต้องการของประชาคม

2) สนับสนุนการให้ความรู้ด้านเทคโนโลยีสารสนเทศมาสร้างความเข้มแข็งให้ชุมชนและสังคม

3) ส่งเสริมการวิจัยพัฒนาและสร้างสรรค์

4) พัฒนาและปรับปรุงโครงสร้างสาธารณูปโภคพื้นฐานด้านเทคโนโลยีสารสนเทศ

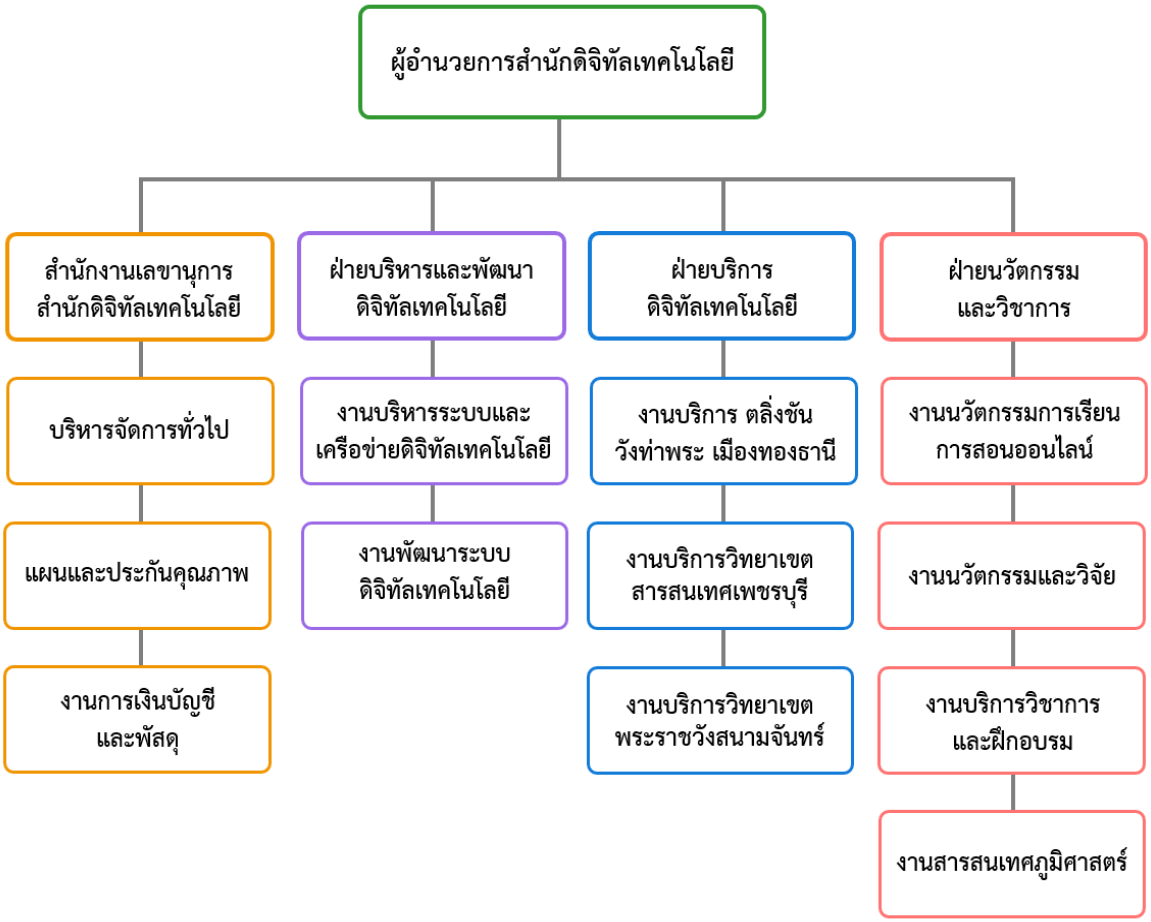
5) พัฒนาการบริหารจัดการองค์กรให้มีประสิทธิภาพ

6) มาตรฐานด้านเทคโนโลยีสารสนเทศ

2.3 โครงสร้างการบริหารองค์กร

2.3.1 โครงสร้างการบริหารสำนักดิจิทัลเทคโนโลยี มหาวิทยาลัยศิลปากร

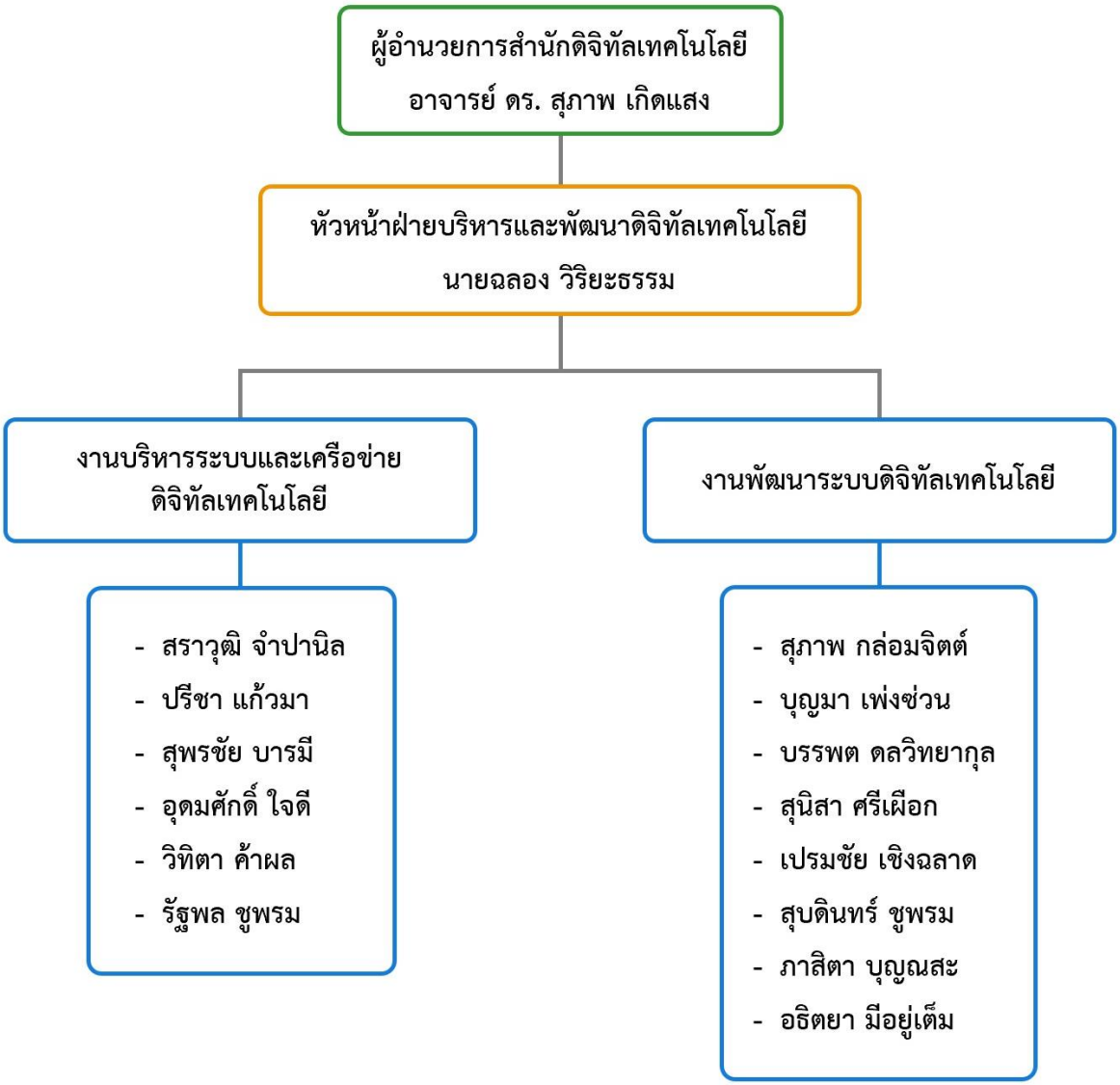
สำนักดิจิทัลเทคโนโลยีมีโครงสร้างในการบริหารงาน ดังรูปที่ 2.1



รูปที่ 2.1 โครงสร้างการบริหาร สำนักดิจิทัลเทคโนโลยี มหาวิทยาลัยศิลปากร [1]

2.3.2. โครงสร้างอัตรากำลังบุคลากรฝ่ายบริหารและพัฒนาดิจิทัลเทคโนโลยี สำนักดิจิทัลเทคโนโลยี มหาวิทยาลัยศิลปากร

โครงสร้างการบริหารงานฝ่ายบริหารและพัฒนาดิจิทัลเทคโนโลยี สำนักดิจิทัลเทคโนโลยี มหาวิทยาลัยศิลปากร ดังปรากฏในรูปที่ 2.2 ดังนี้



รูปที่ 2.2 โครงสร้างอัตรากำลังบุคลากร ฝ่ายบริหารและพัฒนาดิจิทัลเทคโนโลยี สำนักดิจิทัลเทคโนโลยี มหาวิทยาลัยศิลปากร [1]

2.4 บทบาทหน้าที่ความรับผิดชอบ

2.4.1 บทบาทหน้าที่ความรับผิดชอบของสำนักดิจิทัลเทคโนโลยี แบ่งเป็น 4 ฝ่าย ดังนี้

1) สำนักงานเลขานุการ สำนักดิจิทัลเทคโนโลยี มีจำนวนบุคลากรในงานทั้งสิ้น จำนวน 14 คน โดยมีบทบาทหน้าที่ความรับผิดชอบมีหน้าที่รับผิดชอบงานด้านต่าง ๆ ภายในสำนักดิจิทัลเทคโนโลยี ได้แก่ งานสารบรรณ งานจัดทำเอกสาร งานบริหารบุคคล งานการเงินและพัสดุ งานวางแผน และงบประมาณตลอดจนงานด้านประชาสัมพันธ์

2) ฝ่ายบริหารและพัฒนาดิจิทัลเทคโนโลยี มีจำนวนบุคลากรในงานทั้งสิ้น จำนวน 15 คน โดยมีบทบาทหน้าที่ความรับผิดชอบดูแลระบบเครือข่ายของมหาวิทยาลัยศิลปากรทุกวิทยาเขต การบริหารจัดการ Server เช่น ระบบอีเมล์ ระบบฐานข้อมูลต่าง ๆ ตลอดจนการบำรุงรักษาอุปกรณ์เครือข่ายหลักของมหาวิทยาลัยให้สามารถใช้งานได้อย่างปกติ

3) ฝ่ายบริการดิจิทัลเทคโนโลยี มีจำนวนบุคลากรในงานทั้งสิ้นจำนวน 16 คน โดยมีบทบาทหน้าที่ความรับผิดชอบการดูแลห้องปฏิบัติการคอมพิวเตอร์สำหรับการเรียนการสอน การอบรมสัมมนา การศึกษาวิจัย และการศึกษาค้นคว้าด้วยตนเองของนักศึกษา และการบริการต่าง ๆ ที่เกี่ยวข้องกับคอมพิวเตอร์และการให้บริการพิมพ์งานสำหรับนักศึกษา

4) ฝ่ายนวัตกรรมและวิชาการมีจำนวนบุคลากรในงานทั้งสิ้นจำนวน 17 คน โดยมีบทบาทหน้าที่ความรับผิดชอบมีหน้ารับผิดชอบหลัก ได้แก่ งานรับสมัครนักศึกษาโครงการต่าง ๆ งานสนับสนุนเชิงเทคนิค งานฝึกอบรม งานจัดทำเว็บไซต์ งานบริการตรวจข้อสอบด้วยเครื่องตรวจข้อสอบ งานวิเคราะห์ข้อมูลทางสถิติ และให้คำปรึกษาเกี่ยวกับซอฟต์แวร์

2.4.2 ภารกิจของงานในฝ่ายบริหารและพัฒนาดิจิทัลเทคโนโลยี ประกอบด้วย 2 ส่วนงาน ดังนี้ [1]

1) งานบริหารระบบและเครือข่ายดิจิทัลเทคโนโลยี มีหน้าหลัก คือ การให้บริการโครงสร้างระบบเครือข่ายพื้นฐานและบริการด้านระบบเครือข่าย ได้แก่ Internet Intranet LAN Wireless Lan Virtual Machine Server (VM) Cloud Service E-mail VPN Live Video Conference รวมทั้งวางแผนและดำเนินการจัดหาฮาร์ดแวร์เครื่องแม่ข่าย Server System Storage System Backup System เพื่อให้สอดคล้องกับระบบงานต่างๆ ของมหาวิทยาลัย ดูแลระบบเครือข่ายและเซอร์วิสงานต่างๆ ของมหาวิทยาลัย เพื่อให้รองรับการใช้งานได้ตลอด 24 ชั่วโมง

2) งานพัฒนาระบบดิจิทัลเทคโนโลยี มีหน้าที่หลัก คือ ให้บริการดูแลระบบสารสนเทศหลักของมหาวิทยาลัยศิลปากร ได้แก่ ระบบ SU-ERP ระบบ MIS ระบบ e-Document ระบบ E-meeting และระบบ SU-TCAS ระบบประเมินผู้บริหาร ระบบการจองห้อง ฯลฯ บริการฐานข้อมูล บริการพัฒนาระบบ IT รวมทั้งวางแผน วิเคราะห์ ออกแบบ พัฒนาและบริหารระบบ

เทคโนโลยีสารสนเทศให้ได้มาตรฐานตรงตามความต้องการ กำกับ ควบคุม ดูแล การวิเคราะห์ ออกแบบ พัฒนา และการติดตั้งระบบเทคโนโลยีสารสนเทศ ในส่วนที่มีการจัดซื้อจัดจ้างจากภายนอก เพื่อให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

2.4.3 บทบาทหน้าที่ความรับผิดชอบของตำแหน่งนักคอมพิวเตอร์ ระดับปฏิบัติการ

บทบาทหน้าที่ความรับผิดชอบงานของตำแหน่งนักคอมพิวเตอร์ ระดับปฏิบัติการ ได้ปฏิบัติงานโดยสอดคล้องกับมาตราฐานกำหนดตำแหน่งนักคอมพิวเตอร์ ซึ่งมีขอบเขตของภาระงานที่ฝ่ายบริหารและพัฒนาดิจิทัลเทคโนโลยี สำนักดิจิทัลเทคโนโลยี ได้มอบบหมายให้ปฏิบัติและรับผิดชอบ ดังนี้

<u>ภาระงานหลัก</u>

1) งานบริการอุปกรณ์เครือข่าย (Config Install Solve)

- การตั้งค่าอุปกรณ์เครือข่าย (Switch Access point) พร้อมทดสอบก่อนติดตั้งใช้งานจริง (Lab test) ตามที่หน่วยงานขอความอนุเคราะห์เพื่อใช้สำหรับงานประชุม อบรม สัมมนา หรือกิจกรรมงานต่างๆ ของมหาวิทยาลัย
- ตรวจสอบ ปรับปรุง แก้ไขปัญหาอุปกรณ์เครือข่ายของคณะ หน่วยงานต่างๆ
- สำรวจพื้นที่ อาคาร หน่วยงาน เพื่อประเมินและวางแผนดำเนินการติดตั้งอุปกรณ์เครือข่ายตามที่หน่วยงานขอความอนุเคราะห์
- ประสานงานบริษัทเข้าดำเนินการติดตั้ง แก้ไขปัญหาอุปกรณ์เครือข่าย

2) งานสำรองข้อมูล (Backup Data/Configuration)

งานสำรองข้อมูลการตั้งค่าของอุปกรณ์กระจายสัญญาณเครือข่าย (Main Switch) ทุกหน่วยงานเพื่อเป็นข้อมูลสำรองในการตรวจสอบแก้ไขปัญหา ป้องกันกรณีเกิดเหตุระบบเครือข่ายขัดข้อง อุปกรณ์เครือข่ายชำรุดเสียหายและปรับปรุงการตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่ายล่าสุดเพื่อรองรับการใช้งานได้อย่างมีประสิทธิภาพ

3) งานเฝ้าระวังและติดตามสถานะระบบเครือข่าย (Monitoring)

เฝ้าระวังและติดตามสถานะระบบเครือข่ายและอุปกรณ์เครือข่าย เพื่อดูแลให้ระบบเครือข่ายสามารถพร้อมให้บริการแก่ประชาคมศิลปากร เมื่อพบปัญหาขัดข้องเร่งดำเนินการแก้ไข ประสานงานผู้ดูแลระบบเครือข่ายประจำหน่วยงานกรณีระบบเครือข่ายขัดข้อง รายละเอียดการดำเนินการ ดังนี้

- เส้นทางเชื่อมต่อระบบเครือข่ายของผู้ให้บริการ (ISP) ทุกเส้นทาง ทุกวิทยาเขต
  เช่น UniNet CAT TOT UIH

- อุปกรณ์กระจายสัญญาณระบบเครือข่ายระดับอาคารแต่ละหน่วยงาน
- ระบบควบคุมเครือข่ายไร้สาย (Wireless Controller Aruba)
- ระบบควบคุมเครือข่ายไร้สาย (Wireless Controller D-Link)
- ระบบควบคุมเครือข่ายไร้สาย (Wireless Controller Huawei)
- ระบบควบคุมเครือข่ายไร้สาย (Wireless Controller Ruijie)
- ระบบควบคุมเครือข่ายไร้สาย (Wireless Controller Ubiquiti)
- อุปกรณ์ระบบเครือข่ายไร้สาย Access Point ชนิด Stand Alone

4) งานประชาสัมพันธ์ด้านระบบเครือข่าย

ประชาสัมพันธ์ข่าวสารด้านระบบเครือข่ายผ่านทางสื่อสังคมออนไลน์ (Social media) ตัวอย่างเช่น ระบบเครือข่ายขัดข้อง การปรับปรุงระบบเครือข่าย และข่าวด้านอื่นๆ ที่เป็นประโยชน์ต่อประชาคมศิลปากรผ่านช่องทาง ดังต่อไปนี้

- Facebook FanPage : Bureau of Digital Technology ,Silpakorn University (9,625.Like)
- Line Group : Silpakorn News (478 Users) บุคลากรส่วนใหญ่และผู้บริหาร
- Line Group : Silpakorn News2 (69 Users) บุคลากรส่วนใหญ่และผู้บริหาร
- Line Group : SUITCoP (100 Users) ผู้ดูแลระบบและผู้ประสานงานของคณะ / หน่วยงาน
- Line Group : สหกรณ์ มศก (264 Users) ประชาคม มศก. ในวงกว้างทั้งบุคลากรปัจจุบันและบุคลากรที่เกษียนอายุราชการแล้ว
- Line Group : Bureau of Digital Technology ,Silpakorn University (67 Users) บุคลากรสำนักดิจิทัลเทคโนโลยี
- Line Group : กลุ่มที่พักอาศัย มศก.สนามจันทร์ต้าน CV-19 (196 Users) บุคลากรที่พักอาศัยใน มศก.สนามจันทร์
- ประชาสัมพันธ์ทาง Facebook และ Line ส่วนตัว เนื่องจากยังมีบุคลากรศิลปากรอีกจำนวนมากไม่ได้อยู่ใน Line Group ดังกล่าวและ Facebook FanPage ของสำนักดิจิทัลเทคโนโลยี

5) งานถ่ายทอดสด (Broadcasting) และการประชุมผ่านเครือข่าย (Video Conference)

- ถ่ายทอดสดผ่านระบบเครือข่ายภายใน (Intranet) เช่น การประชุมสภามหาวิทยาลัยศิลปากร การอบรมสัมนาภายในมหาวิทยาลัยศิลปากร วันคล้ายวันสถาปนา

มหาวิทยาลัยศิลปากร การแสดงวิสัยทัศน์ของผู้สมควรดำรงตำแหน่งอธิการบดี ผู้อำนวยการของหน่วยงานต่างๆ

- ถ่ายทอดสดผ่านระบบเครือข่ายภายนอก (Internet) เช่น พิธีพระราชทานปริญญาบัตรของผู้สำเร็จการศึกษามหาวิทยาลัยศิลปากร การประชุมวิชาการ QS Totally Art Summit (Art and Design) การแสดงปาฐกถาศิลป์ พีระศรี โดย ศาสตรเมธี ดร.เฉลิมชัย โฆษิตพิพัฒน์ เป็นต้น

- การประชุมผ่านระบบเครือข่ายภายใน (VDO Conference) เช่น การประชุมของหน่วยงานระหว่างวิทยาเขตตามที่หน่วยงานต่างๆ ทำหนังสือขอความอนุเคราะห์ เช่น การประชุมสภามหาวิทยาลัยศิลปากร การประชุม ก.บ.ม. การประชุม ก.บ.พ การประชุมคณบดี เป็นต้น

- การประชุมผ่านระบบเครือข่ายภายนอก เช่น การประชุมสอบวิทยานิพนธ์ระหว่างมหาวิทยาลัย การสอบวิทยานิพนธ์ระหว่างประเทศ การประชุมกับหน่วยงานภายนอกต่าง ๆ เป็นต้น

6) งานให้บริการปรึกษา แก้ไขปัญหาต่างๆ ด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Service)

การติดตั้งซอฟต์แวร์เครือข่ายส่วนตัวเสมือน Virtual Private Network (VPN) เครื่องคอมพิวเตอร์ มือถือ แท็บเล็ต งานออกตรวจสอบแก้ไขปัญหาระบบเครือข่ายของหน่วยงาน

7) คณะกรรมการต่างๆ (กรณีงานนอกเหนือจากหน้าที่ตนเอง)

- คณะกรรมการตรวจสอบพัสดุของสำนักดิจิทัลเทคโนโลยี มีหน้าที่ตรวจสอบครุภัณฑ์อุปกรณ์เครือข่ายของฝ่ายบริหารและพัฒนาดิจิทัลโทคโนโลยี ร่วมประชุมคณะกรรมการตรวจสอบพัสดุของสำนักดิจิทัลเทคโนโลยี ดำเนินการตรวจสอบครุภัณฑ์ของสำนักดิจิทัลเทคโนโลยีทุกวิทยาเขตและรายงานผลการดำเนินการต่อประธานตรวจสอบครุภัณฑ์ของสำนักดิจิทัลเทคโนโลยี

- คณะกรรมการจำหน่ายครุภัณฑ์ชำรุดและเสื่อมสภาพของสำนักดิจิทัลเทคโนโลยี มีหน้าที่รับผิดชอบดำเนินการจำหน่ายครุภัณฑ์ชำรุดและเสื่อมสภาพของสำนักสำนักดิจิทัลเทคโนโลยี ประจำปีงบประมาณ พ.ศ. 2561 - พ.ศ. 2563 และรายงานผลการดำเนินการเสนอให้รองอธิการบดี พระราชวังสนามจันทร์ ตามระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560

- คณะกรรมการตรวจรับโครงการจัดซื้ออุปกรณ์เครือข่ายต่างๆ ของสำนักดิจิทัลเทคโนโลยี มีหน้าที่ตรวจสอบอุปกรณ์เครือข่ายโครงการนั้น ๆ ว่าสามารถใช้งานได้จริงและทำงานได้ถูกต้อง อย่างมีประสิทธิภาพ ตรงตามรายละเอียดคุณสมบัติเฉพาะทางด้านเทคนิคที่กำหนดไว้ (TOR) เพื่อให้เกิดประโยชน์สูงสุดกับมหาวิทยาลัย คุ้มค่ากับงบประมาณที่ใช้จัดซื้อ เช่น โครงการปรับปรุงระบบเครือข่ายไร้สาย โครงการเช่าวงจรสื่อสารระหว่างวิทยาเขต โครงการบำรุงรักษาอุปกรณ์เครือข่าย เป็นต้น

- คณะกรรมการบูรณาการมหาวิทยาลัยศิลปากร เป็นตัวแทนของสำนักดิจิทัลเทคโนโลยี เข้าร่วมเป็นคณะกรรมการบูรณาการมหาวิทยาลัยศิลปากร เพื่อประชุมหารือแนวทางในการให้พัฒนาการให้บริการต่างๆ กับนักศึกษา เพื่อให้เกิดประโยชน์สูงสุดสำหรับการเรียนการสอนและพันธกิจต่าง ๆ ของมหาวิทยาลัยศิลปากร

- คณะอนุกรรมการจัดงานพิธีพระราชทานปริญญาบัตร ฝ่ายโสตทัศนูปกรณ์ (ทุกปีการศึกษา) ทำหน้าที่ ถ่ายทอดสดงานพิธีพระราชทานปริญญาบัตรผ่านระบบเครือข่ายอินเทอร์เน็ตผ่านช่องทางสื่อสังคมออนไลน์ Facebook Live YouTube Live และ Web Browser

8) งานส่งข้อมูลรายงานด้านระบบเครือข่าย

รายงานข้อมูลการจราจรระบบเครือข่าย รายงานข้อมูลการจราจรระบบเครือข่ายกรณีขัดข้อง

9) งานให้บริการยืมคืนอุปกรณ์เครือข่าย

- จัดทำเอกสารการยืม-คืน อุปกรณ์เครือข่ายกับหน่วยงาน / บุคลากรที่ขอความอนุเคราะห์

- รับผิดชอบการบริการเครื่องมือ และอุปกรณ์ต่าง ๆ ด้านระบบเครือข่าย พร้อมให้คำแนะนำการใช้งาน ตรวจเช็คดูแลรักษาอุปกรณ์

- ติดตาม พร้อมทั้งดูแลรักษาเครื่องมือ และอุปกรณ์ด้านระบบเครือข่ายให้อยู่ในสภาพที่ใช้งานได้สมบูรณ์

<u>ภาระงานรอง</u>

1) งานบริหารงานทั่วไป

- ติดต่อประสานงานด้านระบบเครือข่ายต่าง ๆ กับหน่วยงานทั้งภายใน และภายนอกมหาวิทยาลัย

- จัดทำเอกสาร หนังสือราชการต่าง ๆ ของส่วนงานบริหารและพัฒนาดิจิทัลเทคโนโลยี

2) งานอื่น ๆ ที่ได้รับมอบหมาย

ศึกษาค้นคว้าเทคโนโลยีใหม่ ๆ และดำเนินงานตามเป้าหมายให้สำเร็จลุล่วงไปด้วยดี

บทที่ 3
หลักเกณฑ์ วิธีการปฏิบัติงานและความรู้พื้นฐาน

คู่มือปฏิบัติงานเรื่อง การตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่าย สำนักดิจิทัลเทคโนโลยี มีลักษณะเป็นงานที่ให้บริการและต้องปฏิบัติตาม กฎ ระเบียบ ข้อบังคับของมหาวิทยาลัยประกาศ แนวทางปฏิบัติต่าง ๆ ดังนี้

3.1 กฎระเบียบที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

3.2 จรรยาบรรณวิชาชีพ

3.3 หลักการปฏิบัติงาน PDCA

3.4 ความรู้พื้นฐานและทฤษฎีที่เกี่ยวข้อง

3.1 กฎระเบียบที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

3.1.1 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 [2]

มาตรา 13 (4) กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน

(5) กำหนดหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน้าที่ของหน่วยงานควบคุมหรือกำกับดูแล โดยอย่างน้อยต้องกำหนดหน้าที่ให้หน่วยงานควบคุมหรือกำกับดูแลต้องกำหนดมาตรฐานที่เหมาะสมเพื่อรับมือกับภัยคุกคามทางไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานของรัฐ

ในการกำหนดกรอบมาตรฐานตามวรรคหนึ่ง (4) ให้คำนึงถึงหลักการบริหารความเสี่ยง โดยอย่างน้อยต้องประกอบด้วยวิธีการและมาตรการ ดังต่อไปนี้

(1) การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล

(2) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

(3) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

(4) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

(5) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

3.1.2 ประกาศมหาวิทยาลัยศิลปากร เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ [3]

ส่วนที่ 1 นโยบายรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

กำหนดนโยบายหลักในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย (Information Security Event) กำหนดประเด็นสำคัญ ดังนี้

หมวดที่ 1 การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

1. การเข้าถึงระบบสารสนเทศและระบบเครือข่าย เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล ให้คำนึงถึงความมั่นคงปลอดภัยในการใช้งาน โดยกำหนดกฎเกณฑ์ที่เกี่ยวกับการขออนุญาตให้เข้าถึง กำหนดสิทธิ์ และการปรับปรุงสิทธิ์ เพื่อให้ผู้ใช้งานทุกระดับได้เข้าถึงข้อมูลและใช้งานได้ตามสิทธิ์ที่กำหนดให้

2. การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต

3. การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

4. การควบคุมการเข้าถึงโปรแกรมประยุกต์ และสารสนเทศ เพื่อป้องกันการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานระบบสารสนเทศของมหาวิทยาลัย และป้องกันความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

หมวดที่ 2 การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศ

ระบบสารสนเทศต้องจัดทำระบบสำรองของสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน พร้อมทั้งจัดทำแผนเตรียมความพร้อมฉุกเฉิน เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

หมวดที่ 3 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

กำหนดให้ผู้ดูและระบบตรวจสอบและประเมินความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศ อย่างน้อยปีละ 1 ครั้ง โดยการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการตรวจสอบโดยผู้ตรวจสอบภายในส่วนงานของแต่ละส่วนงาน (Internal Auditor) หรือผู้ตรวจสอบด้านความมั่นคงปลอดภัยจากหน่วยงานภายนอกมหาวิทยาลัย (External Auditor)

หมวดที่ 4 การทบทวนปรับปรุงนโยบายและแนวทางการปฏิบัติในการรักษา ความมั่นคงปลอดภัยด้านสารสนเทศ ให้ทำการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้เป็นปัจจุบัน อย่างน้อยปีละ 16 ครั้ง

ส่วนที่ 2 แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

หมวดที่ 2 การเข้าถึงหรือการควบคุมการใช้งานสารสนเทศ

ตอนที่ 4 การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)

1. ในการใช้บริการระบบเครือข่าย ผู้ดูและระบบกำหนดสิทธิการใช้งานโดยให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาของส่วนงานเจ้าของระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวปีละ 1 ครั้ง

2. ผู้ดูและระบบกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบเครือข่ายและระบบสารสนเทศของมหาวิทยาลัยได้ โดยผู้ใช้งานที่จะเข้าใช้งานระบบยืนยันตัวตน (Authentication) ด้วยชื่อบัญชีผู้ใช้งานทุกครั้ง

3. การควบคุมอุปกรณ์บนเครือข่าย (Equipment Control in Network) ดำเนินการดังนี้

3.1 ผู้ดูแลระบบใช้ซอฟต์แวร์ควบคุมสำหรับการบริหารจัดการอุปกรณ์บนระบบเครือข่ายและอุปกรณ์สื่อสารเคลื่อนที่ ซึ่งสามารถตรวจสอบสถานะของการทำงานของอุปกรณ์โดยระบุจุดเชื่อมต่อและ MAC Address ของอุปกรณ์เครือข่ายที่ต่อพ่วงกับระบบเครือข่ายได้

3.2 ผู้ใช้งานภายในมหาวิทยาลัยยืนยันตัวตน ด้วยชื่อบัญชีผู้ใช้งานทุกครั้งผ่านซอฟต์แวร์ควบคุมเพื่อระบุตัวตน จุดเชื่อมต่อของอุปกรณ์ที่เชื่อมต่อกับระบบเครือข่าย

3.3 ผู้ดูแลระบบมีสิทธิในการจำกัดอุปกรณ์ต่อพ่วงที่ไม่ได้รับอนุญาตได้

3.4 ผู้ดูแลระบบสามารถอนุญาตให้อุปกรณ์บางชนิดสามารถใช้งานระบบเครือข่ายได้โดยไม่ต้องผ่านระบบยืนยันตัวตนเป็นกรณีพิเศษ

4. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ให้ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางระบบเครือข่ายดังนี้

4.1 ผู้ดูแลระบบปิดพอร์ตที่ไม่จำเป็นทุกพอร์ตเพื่อจำกัดและควบคุมการเข้าถึงพอร์ตโดยไม่ได้รับอนุญาต

4.2 ผู้ดูแลระบบกำหนดพอร์ตสำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางระบบเครือข่าย และแจ้งให้ผู้ดูแลระบบที่มีสิทธิ์ในการตรวจสอบและปรับแต่งระบบทราบ

4.3 หากผู้ดูแลระบบตรวจสอบพบการใช้งานพอร์ตโดยผู้ใช้ที่ไม่ได้รับอนุญาต ผู้ดูแลระบบสามารถปิดการใช้งานพอร์ตที่ไม่ได้รับอนุญาตได้ทันที

5. การแบ่งแยกเครือข่าย (Segregation in Network) ผู้ดูแลระบบจะทำการแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็น 2 เครือข่าย คือ เครือข่ายสำหรับผู้ใช้งานภายในและเครือข่ายสำหรับผู้ใช้งานภายนอก

6. การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ผู้ดูแลระบบจะควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้งานร่วมกันหรือเชื่อมต่อดังนี้

6.1 มีการตรวจสอบการเชื่อมต่อเครือข่าย

6.2 จำกัดสิทธิความสามารถของผู้ใช้งานในการเชื่อมต่อเข้าสู่เครือข่าย

6.3 ใช้อุปกรณ์ Firewall สำหรับการควบคุมการเชื่อมต่อ

6.4 มีระบบตรวจจับผู้บุกรุกทั้งในระดับเครือข่ายและระดับเครื่องคอมพิวเตอร์แม่ข่าย

6.5 ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่ายโดยไม่ได้รับอนุญาต

7. การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ผู้ดูแลระบบจะควบคุมการจับเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจดังนี้

7.1 ควบคุมไม่ให้มีการเปิดเผยแผนการใช้งานหมายเลขเครือข่าย (IP Address Plan)

7.2 กำหนดให้มีการแปลงหมายเลขเครือข่ายเพื่อแยกเครือข่ายย่อย

7.3 กำหนดมาตรการบังคับใช้เส้นทางเครือข่าย กล่าวคือสามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้หรือจำกัดสิทธิในการใช้บริการเครือข่าย

8. การควบคุมการใช้งานระบบจากภายนอกให้ปฏิบัติดังนี้

8.1 การเข้าสู่ระบบจากระยะไกล (Remote Access) ผู้ดูแลระบบต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน

8.2 การเข้าสู่ระบบจากระยะไกลสู่ระบบสารสนเทศและเครือข่ายของมหาวิทยาลัยต้องมีการกำหนดมาตราการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตราฐานการเข้าสู่ระบบภายใน

8.3 วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายได้จากระยะไกลต้องได้รับการอนุมัติจากผู้อำนวยการสำนักดิจิทัลเทคโนโลยีก่อนและมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบสารสนเทศอย่างเคร่งครัด

ตอนที่ 10 การควบคุมการใช้อินเทอร์เน็ต

1. ผู้ดูแลระบบกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ตที่เชื่อมต่อผ่านระบบรักษาความปลอดภัยที่มหาวิทยาลัยจัดสรรไว้ให้เท่านั้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่นที่ไม่ได้รับอนุมัติจากผู้อำนวยการสำนักดิจิทัลเทคโนโลยี

2. การใช้งานเครื่องคอมพิวเตอร์จะต้องมีการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์และทำการอุดช่องโหว่ก่อนที่จะทำการเชื่อมต่อระบบอินเทอร์เน็ตผ่านเว็บบราวเซอร์

3. ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิที่ได้รับตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลมหาวิทยาลัย และต้องไม่ใช้ระบบอินเทอร์เน็ตของมหาวิทยาลัยเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงแห่งชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคมหรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับมหาวิทยาลัย

4. ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของมหาวิทยาลัยที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

5. ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ตซึ่งรวมถึงการดาวน์โหลดการปรับปรุงโปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือสินทรัพย์ทางปัญญา

3.2 จรรยาบรรณวิชาชีพ [4]

มหาวิทยาลัยศิลปากรได้กำหนดจรรยาบรรณของผู้ปฏิบัติงานตามข้อบังคับมหาวิทยาลัยศิลปากร ว่าด้วยจรรยาบรรณของบุคลากรในมหาวิทยาลัยศิลปากร พ.ศ.2552 เพื่อกำหนดแนวปฏิบัติตนของบุคลากรในสถาบันอุดมศึกษาและพนักงานในสถาบันอุดมศึกษาสังกัดมหาวิทยาลัยศิลปากร ในการที่จะเป็นผู้ที่มีความประพฤติดี สำนึกในหน้าที่ สามารถประสานงานกับทุกฝ่าย ตลอดจนปฏิบัติหน้าที่ราชการได้อย่างมีประสิทธิภาพ และประสิทธิผลยิ่งขึ้น รวมทั้งรักษาไว้ซึ่งศักดิ์ศรีและส่งเสริมชื่อเสียง เกียรติคุณ เกียรติฐานะของบุคลากรในสถาบันอุดมศึกษา อันจะยังผลให้ผู้ประพฤติเป็นที่เลื่อมใส ศรัทธาและยกย่องของบุคคลโดยทั่วไป บุคลากรมหาวิทยาลัยต้องรักษาและปฏิบัติตนตามจรรยาบรรณตามข้อบังคับนี้ กำหนดโดยยึดมั่นในหลักการต่อไปนี้

3.2.1 จรรยาบรรณต่อตนเอง

1) พึงเป็นผู้มีศีลธรรมอันดีและประพฤติตนให้เหมาะสมกับการเป็นเจ้าหน้าที่ของรัฐ

2) พึงมีทัศนคติที่ดี และพัฒนาตนเองให้มีคุณธรรม จริยธรรม รวมทั้งเพิ่มพูนความรู้

ความสามารถ และทักษะในการทำงานเพื่อให้การปฏิบัติหน้าที่ราชการมีประสิทธิภาพ และประสิทธิผลยิ่งขึ้น

3) พึงใช้วิชาชีพในการปฏิบัติหน้าที่ด้วยความซื่อสัตย์ และไม่แสวงหาผลประโยชน์โดยมิชอบ

3.2.2 จรรยาบรรณต่อการปฏิบัติงานและต่อหน่วยงาน

1) พึงปฏิบัติหน้าที่ราชการด้วยความซื่อสัตย์สุจริต เที่ยงธรรม ขยันหมั่นเพียร และดูแลเอาใจใส่รักษาประโยชน์ของทางราชการ

2) พึงปฏิบัติหน้าที่ราชการอย่างเต็มกำลัง ความสามารถ รอบคอบ รวดเร็ว ขยันหมั่นเพียร ถูกต้องสมเหตุสมผล โดยคำนึงถึงประโยชน์ของทางราชการและประชาชนเป็นสำคัญ

3) พึงละเว้นจากการนำผลงานของผู้อื่นมาเป็นของตน และต้องไม่คัดลอกหรือลอกเลียนผลงานของผู้อื่นโดยมิชอบหรือจ้าง วาน ใช้ผู้อื่นให้ทำผลงานให้หรือนำผลงานของผู้อื่น เพื่อนำไปใช้ในการขอกำหนดตำแหน่งให้สูงขึ้นหรือให้ได้รับเงินเดือนหรือค่าตอบแทนที่สูงขึ้น หรือเพื่อการอันชอบด้วยประการใด

4) พึงประพฤติตนเป็นผู้ตรงต่อเวลา และใช้เวลาราชการให้เป็นประโยชน์ต่อทางราชการอย่างเต็มที่

5) พึงดูแลรักษาและใช้ทรัพย์สินของทางราชการอย่างประหยัด คุ้มค่า โดยระมัดระวัง มิให้เสียหายหรือสิ้นเปลืองเยี่ยงวิญญูชนจะพึงปฏิบัติต่อทรัพย์สินของตนเอง

6) ต้องไม่กระทำการอันมิชอบด้วยกฎหมายให้หน่วยงานได้รับความเสื่อมเสียหรือเสียหาย ไม่ว่าในทางชื่อเสียง เกียรติภูมิ หรือด้วยประการใด ๆ

3.2.3 จรรยาบรรณต่อผู้บังคับบัญชา ผู้ใต้บังคับบัญชา และผู้ร่วมงาน

1) ผู้บังคับบัญชาพึงดูแลเอาใจใส่ผู้อยู่ใต้บังคับบัญชทั้งในด้านการปฏิบัติงาน ขวัญกำลังใจ สวัสดิการและรับฟังความคิดเห็นของผู้อยู่ใต้บังคับบัญชา ตลอดจนปกครองผู้อยู่ใต้บังคับบัญชาด้วยหลักธรรมาภิบาลและถูกต้องตามทำนองคลองธรรม

2) ผู้ใต้บังคับบัญชา พึงมีความรับผิดชอบในการปฏิบัติงาน การให้ความร่วมมือช่วยเหลือปฏิบัติงานทั้งในด้านการให้ความคิดเห็น การช่วยทำงาน และการแก้ปัญหาร่วมกัน รวมทั้งการเสนอแนะในสิ่งที่เห็นว่าจะมีประโยชน์ต่อการพัฒนางานในความรับผิดชอบด้วย

3) พึงปฏิบัติต่อผู้ร่วมงานตลอดจนผู้เกี่ยวข้องด้วยความสุภาพ อ่อนน้อม มีน้ำใจไมตรี เอื้ออาทร และมีมนุษยสัมพันธ์อันดี

4) พึงช่วยเหลือเกื้อกูลกันในทางที่ชอบ รวมทั้งส่งเสริมสนับสนุนให้เกิดความสามัคคี ร่วมแรงร่วมใจในบรรดาผู้ร่วมงานในการปฏิบัติหน้าที่เพื่อประโยชน์ส่วนรวม

3.2.4 จรรยาบรรณต่อนักเรียน นักศึกษา ผู้รับบริการ ประชาชนและสังคม

1) พึงประพฤติตนเป็นแบบอย่างที่ดีแก่นักเรียนและนักศึกษา เป็นที่เชื่อถือของบุคคลทั่วไป

2) พึงให้บริการนักเรียน นักศึกษา ผู้รับบริการ ประชาชนอย่างเต็มกำลังความสามารถด้วยความเป็นธรรม เสมอภาค โปร่งใส เอื้อเฟื้อ มีน้ำใจ และใช้กิริยาวาจาที่สุภาพอ่อนโยน เมื่อเห็นว่าเรื่องใดไม่สามารถปฏิบัติได้หรือไม่อยู่ในอำนาจหน้าที่ของตนที่จะต้องปฏิบัติ ควรชี้แจงเหตุผลหรือแนะนำให้ติดต่อยังหน่วยงานหรือบุคคลซึ่งตนทราบว่ามีอำนาจหน้าที่เกี่ยวข้องกับเรื่องนั้น ๆ ต่อไป

3) พึงมีความเมตตา เอาใจใส่ และช่วยเหลือ ในการศึกษาเล่าเรียนของนักเรียนและนักศึกษา

4) ต้องไม่เปิดเผยความลับของนักเรียน นักศึกษา ผู้รับบริการ ประชาชน ซึ่งตนเองได้มาจากการปฏิบัติหน้าที่หรือจากความไว้วางใจของบุคคลดังกล่าว

5) ต้องไม่อบรม สั่งสอน หรือสนับสนุนให้นักเรียนและนักศึกษากระทำการที่ผิดกฎหมาย หรือ ฝ่าฝืนศีลธรรมอันดีของประชาชน

6) พึงละเว้นการรับทรัพย์สินหรือประโยชน์อื่นใด ซึ่งมีมูลค่าเกินปกติวิสัยที่วิญญูชนจะให้กันโดยเสน่หาจากนักเรียน นักศึกษา ผู้รับบริการ ประชาชนหรือผู้ซึ่งอาจได้รับประโยชน์จากการปฏิบัติหน้าที่ราชการนั้น เพื่อกระทำการหรือไม่กระทำการใดตามหน้าที่ หากได้รับไว้แล้วและทราบภายหลังว่าทรัพย์สินหรือประโยชน์อื่นใดที่รับไว้มีมูลค่าเกินปกติวิสัย ให้รายงานผู้บังคับบัญชาทราบโดยเร็วเพื่อดำเนินการตามสมควรแก่กรณี

3.2.5 จรรยาบรรณต่อหน้าที่ และวิชาชีพ

1) พึงใช้วิชาชีพในการปฏิบัติหน้าที่ราชการด้วยความซื่อสัตย์ และไม่แสวงหาผลประโยชน์โดยมิชอบ ในกรณีที่วิชาชีพใดมีจรรยาบรรณวิชาชีพกำหนดไว้ ก็พึงปฏิบัติตามจรรยาบรรณวิชาชีพนั้นด้วย

3.3 หลักการปฏิบัติงาน PDCA

การตั้งค่าอุปกรณ์กระจายสัญญาณเครือข่ายสำหรับผู้ดูแลระบบ ดำเนินการตามกระบวนการหลักการปฏิบัติงาน PDCA เป็นหลักในการปฏิบัติงาน ซึ่งมีรายละเอียดดังนี้

ตารางที่ 3.1 หลักการปฏิบัติงาน PDCA

หลักการปฏิบัติงาน PDCA	**รายละเอียดในการปฏิบัติงานตามหลัก PDCA**
P=Plan (การวางแผน)	1. ศึกษา รวบรวม ความต้องการใช้บริการระบบเครือข่าย เป้าหมาย และข้อจำกัดทางเทคนิค รูปแบบการเชื่อมต่อระบบเครือข่าย

ตารางที่ 3.1 หลักการปฏิบัติงาน PDCA (ต่อ)

หลักการปฏิบัติงาน PDCA	**รายละเอียดในการปฏิบัติงานตามหลัก PDCA**
	2. ศึกษาข้อมูลรายละเอียดคุณสมบัติของอุปกรณ์กระจายสัญญาณระบบเครือข่ายที่เลือกนำมาใช้งานจริง 3. รวบรวมข้อมูลที่ได้จากศึกษา และวิเคราะห์แล้วมาออกแบบระบบเครือข่ายให้ตรงกับความต้องการ 4. ออกแบบโครงสร้างระบบเครือข่าย เลือกโทโปโลยีระบบเครือข่าย กรณีศึกษาพื้นที่โซนหอพักนักศึกษา สนามจันทร์ 5. ศึกษาข้อมูลวิธีการตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่าย 6. ศึกษาระบบการเฝ้าระวังและติดตามสถานะของอุปกรณ์กระจายสัญญาณระบบเครือข่าย เพื่อนำมาใช้ในการตรวจสอบ เช่น สถานะ UP-Down ปริมาณข้อมูลระบบเครือข่ายแต่ละอาคาร
D = Do (การปฏิบัติตามแผน)	1. ดำเนินการตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่ายแต่ละส่วน 2. ทดสอบการเชื่อมต่ออุปกรณ์กระจายสัญญาณระบบเครือข่ายและทดสอบการใช้งานจริงทั้งระบบ ก่อนนำไปติดตั้งสถานที่ใช้งานจริง 3. นำข้อมูลอุปกรณ์กระจายสัญญาณระบบเครือข่ายเข้าระบบการเฝ้าระวังและติดตามสถานะของอุปกรณ์เครือข่าย เช่น สถานะ UP-Down ปริมาณข้อมูลระบบเครือข่ายแต่ละอาคาร 4. สร้างแบบประเมินผล เพื่อรวบรวมความต้องการ ปัญหาที่พบในการใช้งานข้อเสนอแนะต่าง ๆ เพื่อนำมาปรับปรุงระบบให้มีประสิทธิภาพดียิ่งขึ้น
C = Check (ตรวจสอบการปฏิบัติตามแผน	1. ตรวจสอบความถูกต้องของการตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่าย 2. ตรวจสอบการใช้งานโดยใช้นำอุปกรณ์เครือข่ายไร้สาย เช่น มือถือ โน้ตบุ๊คมาเชื่อมต่อที่หน้างานจริง ว่าสามารถใช้งานได้มีประสิทธิภาพตรงตามวัตถุประสงค์หรือไม่
A = Act (ปรับปรุงแก้ไข)	1. ประเมินความพึงพอใจของผู้รับบริการ 2. สรุปผลการดำเนินงานและรายงานผลต่อผู้บริหารตามลำดับ

3.4. ความรู้พื้นฐานระบบเครือข่าย และทฤษฎีที่เกี่ยวข้อง

ความรู้พื้นฐานระบบเครือข่าย

3.4.1 เครือข่ายคอมพิวเตอร์ [5]

เครือข่ายคอมพิวเตอร์ (Computer Network) คือ ระบบที่มีคอมพิวเตอร์อย่างน้อยสองเครื่องเชื่อมต่อกันโดยใช้สื่อกลาง และสามารถสื่อสารข้อมูลกันได้อย่างมีประสิทธิภาพ ซึ่งทำให้ผู้ใช้คอมพิวเตอร์แต่ละเครื่องสามารถแลกเปลี่ยนข้อมูลซึ่งกันและกันได้ นอกจากนี้ยังสามารถใช้ทรัพยากร (Resources) ที่มีอยู่ในเครือข่ายร่วมกันได้ เช่น เครื่องพิมพ์ ซีดีรอม สแกนเนอร์ ฮาร์ดดิสก์ แชร์ไฟล์ แชร์ซอฟแวร์ต่างๆ เป็นต้น การใช้ทรัพยากรเหล่านี้ร่วมกันทำให้ประหยัดค่าใช้จ่ายได้มาก เมื่อมีการเชื่อมต่อกับเครือข่ายอื่นๆ ที่อยู่ห่างไกล เช่น ระบบอินเทอร์เน็ตซึ่งเป็นเครือข่ายที่เชื่อมต่อคอมพิวเตอร์ทั่วโลก ทำให้สามารถแลกเปลี่ยนข้อมูลได้กับคนทั่วโลกโดยใช้แอพพลิเคชัน เช่น เว็บ อีเมล FTP การสนทนาผ่านเครือข่ายหรือการแชท (Chat) การประชุมระยะไกล (Videoconference) เป็นต้น

3.4.2 องค์ประกอบพื้นฐานของเครือข่าย [5]

การที่คอมพิวเตอร์จะเชื่อมต่อกันเป็นเครือข่ายได้ต้องมีองค์ประกอบพื้นฐานดังต่อไปนี้

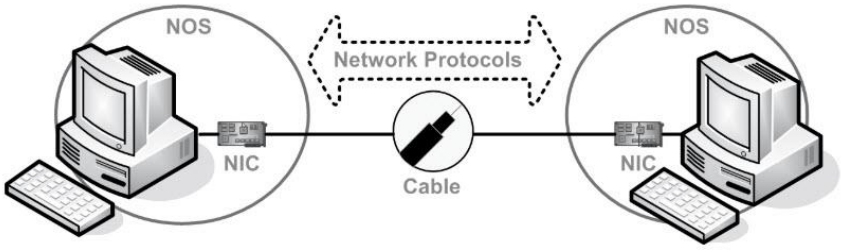
3.4.2.1 คอมพิวเตอร์ อย่างน้อย 2 เครื่อง

3.4.2.2 เน็ตเวิร์คการ์ด หรือ NIC (Network Interface Card) เป็นการ์ดที่เสียบเข้ากับช่องบนเมนบอร์ดของคอมพิวเตอร์ซึ่งเป็นจุดเชื่อมต่อระหว่างคอมพิวเตอร์และเครือข่าย

3.4.2.3 สื่อกลางและอุปกรณ์สำหรับการรับส่งข้อมูล เช่น สายสัญญาณ สายสัญญาณที่นิยมในเครือข่าย เช่น สายโคแอ็กเชียล สายคู่เกลียวบิด และสายใยแก้วนำแสง เป็นต้น ส่วนอุปกรณ์เครือข่าย เช่น ฮับ สวิตช์ เราท์เตอร์ เกตเวย์ เป็นต้น

3.4.2.4 โปรโตคอล (Protocol) โปรโตคอลเป็นภาษาที่คอมพิวเตอร์ใช้สื่อสารกันผ่านเครือข่าย คอมพิวเตอร์ที่สามารถสื่อสารกันได้นั้นจำเป็นที่ต้องใช้ “ภาษา” หรือโปรโตคอลเดียวกัน เช่น OSI TCP/IP IPX/SPX เป็นต้น

3.4.2.5 ระบบปฏิบัติการเครือข่ายหรือ NOS (Network Operating System) ระบบปฏิบัติการเครือข่ายจะเป็นตัวที่คอยจัดการเกี่ยวกับการใช้งานเครือข่ายของผู้ใช้แต่ละคน หรือเป็นตัวจัดการและควบคุมการใช้ทรัพยากรต่างๆ ของเครือข่าย ระบบปฏิบัติการเครือข่ายที่เป็นที่นิยม เช่น Windows Server Novell NetWare Sun Solaris และ Red Hat Linux เป็นต้น

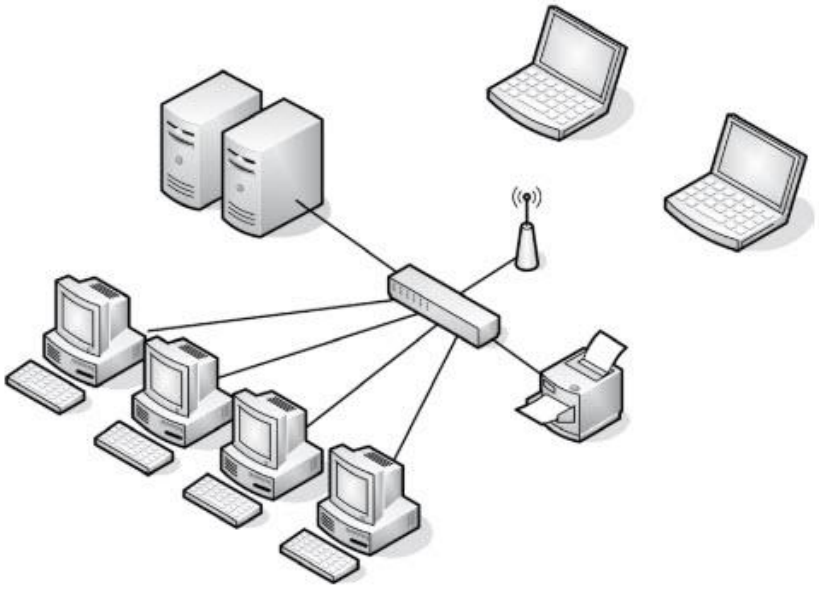


รูปที่ 3.1 องค์ประกอบพื้นฐานของระบบเครือข่าย [5]

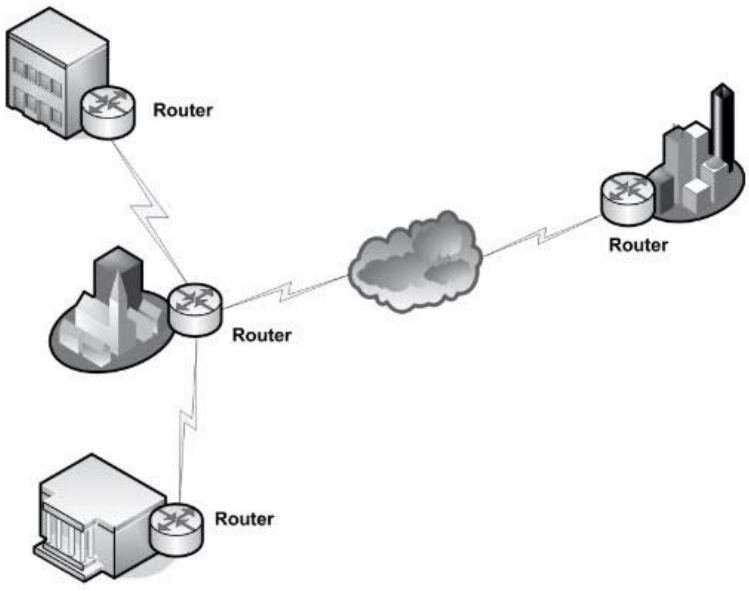
3.4.3 ประเภทของเครือข่าย [5]

3.4.3.1 ประเภทของเครือข่ายแบ่งตามขนาดทางกายภาพ

เครือข่ายสามารถจำแนกโดยใช้ขนาดทางกายภาพของเครือข่ายเป็นเกณฑ์ แบ่งออกได้เป็นสองประเภท คือ LAN หรือเครือข่ายท้องถิ่นและ WAN หรือเครือข่ายบริเวณกว้าง LAN เป็นเครือข่ายขนาดเล็กที่ครอบคลุมพื้นที่บริเวณจำกัด เช่น ภายในห้อง หรือภายในอาคารหนึ่ง ดังรูปที่ 3.2 Local Area Network (LAN) หรืออาจจะครอบคลุมหลายอาคารที่อยู่ในบริเวณใกล้เคียงกัน เช่น ในวิทยาเขตของมหาวิทยาลัยซึ่งบางทีก็เรียกว่า เครือข่ายวิทยาเขต (Campus Network) จำนวนของคอมพิวเตอร์ที่เชื่อมต่อกันใน LAN อาจมีตั้งแต่สองเครื่องไปจนถึงหลายพันเครื่อง ส่วน WAN เป็นเครือข่ายที่ครอบคลุมบริเวณกว้าง เช่น ในพื้นที่เมือง หรืออาจจะครอบคลุมทั่วโลกก็ได้ เช่น เครือข่ายอินเทอร์เน็ต ดังรูปที่ 3.3 Wide Area Network (WAN) หนังสือบางเล่มจะแบ่งเครือข่ายเป็น LAN MAN WAN ซึ่ง MAN (Metropolitan Area Network) เป็นเครือข่ายขนาดกลางระหว่าง LAN และ WAN และครอบคลุมพื้นที่เมือง ในช่วงหลังๆ เทคโนโลยีที่ใช้ใน MAN เป็นเทคโนโลยีเดียวกับเทคโนโลยีของ WAN ดังนั้น จึงได้จัดให้ MAN เป็นเครือข่ายประเภทเดียวกันกับ WAN



รูปที่ 3.2 Local Area Network (LAN) [5]



รูปที่ 3.3 Wide Area Network (WAN) [5]

3.4.3.2 ประเภทของเครือข่ายแบ่งตามหน้าที่ของคอมพิวเตอร์

การจำแนกประเภทของเครือข่ายยังสามารถจำแนกได้โดยใช้ลักษณะการแชร์ข้อมูลของคอมพิวเตอร์ หรือหน้าที่ของคอมพิวเตอร์แต่ละเครื่องเป็นเกณฑ์ในการแบ่งประเภทของเครือข่าย ซึ่งเมื่อใช้หลักการนี้แล้วเราสามารถ แบ่งเครือข่ายออกเป็น 2 ประเภทคือ

- เครือข่ายแบบเท่าเทียม (Peer-to-Peer Network)
- เครือข่ายแบบผู้ให้บริการและผู้ใช้บริการ (Client Server Network)

หน้าที่ของเครื่องคอมพิวเตอร์ในเครือข่ายยังแบ่งออกเป็น 2 ประเภท ดังนี้

- เซิร์ฟเวอร์ (Server) คือ คอมพิวเตอร์ที่ทำหน้าที่บริการต่าง ๆ ให้แก่คอมพิวเตอร์เครื่องอื่น
- ไคลแอนท์ (Client) คือ คอมพิวเตอร์ที่เข้าไปใช้บริการต่าง ๆ ของเซิร์ฟเวอร์

3.4.3.3 ประเภทของเครือข่ายแบ่งตามขอบเขตความเป็นเจ้าของ

แบ่งออกได้เป็น 3 ประเภท

- อินเทอร์เน็ต (Internet) เป็นเครือข่ายสาธารณะที่ทุกคนสามารถเชื่อต่อเข้าได้ จึงทำให้เครือข่ายนี้จะไม่มีความปลอดภัยของข้อมูลเลย คือถ้าข้อมูลที่แชร์ไว้บนอินเทอร์เน็ต ทุกคนก็สามารถเข้าถึงข้อมูลนี้ได้
- อินทราเน็ต (Intranet) เป็นเครือข่ายส่วนบุคคล ข้อมูลจะถูกแชร์เฉพาะผู้ใช้ที่อยู่ข้างในเท่านั้น หรือผู้เข้าใช้งานอินเทอร์เน็ตไม่สามารถเข้ามาดูข้อมูลในอินทราเน็ตได้
- เอ๊กซ์ทราเน็ต (Extranet) เป็นเครือข่ายแบบกึ่งอินเทอร์เน็ตและอินทราเน็ต คือการเข้าใช้เอ็กซ์ทราเน็ตนั้นจะมีการควบคุม เอ็กซ์ทราเน็ตส่วนใหญ่จะเป็นเครือข่ายที่เชื่อมต่อระหว่างองค์กรเพื่อแลกเปลี่ยนข้อมูลบางอย่างซึ่งกันและกัน ในการแลกเปลี่ยนข้อมูลนี้ต้องมีการควบคุมเฉพาะข้อมูลบางอย่างนั้นที่ต้องการแลกเปลี่ยน

3.4.4 โครงสร้างของระบบเครือข่าย (Network Topology) [5]

โทโปโลยีของเครือข่ายจะอธิบายถึงแผนผังการเชื่อมต่อคอมพิวเตอร์ตามลักษณะทางกายภาพ (Physical Topology) หรือทางตรรกะ (Logical Topology) ซึ่งจะแสดงถึงตำแหน่งของคอมพิวเตอร์และอุปกรณ์เครือข่ายอื่นๆ และเส้นทางการเชื่อมต่อของอุปกรณ์เหล่านี้ โทโปโลยีของเครือข่ายอาจจะมีผลต่อสมรรถนะของเครือข่ายได้ การเลือกโทโปโลยีอาจมีผลต่อ

- ประเภทของอุปกรณ์ที่ใช้ในเครือข่าย

- สมรรถนะของอุปกรณ์เหล่านั้น
- ความสามารถในการขยายของเครือข่าย
- วิธีการดูแลและจัดการเครือข่าย

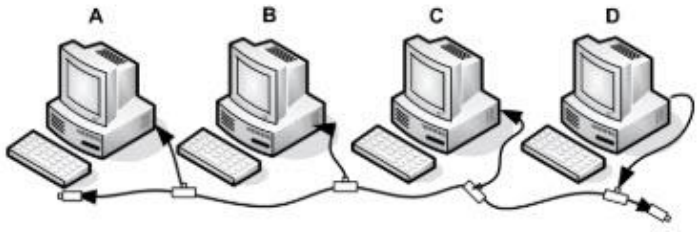
การรู้จักและเข้าใจโทโปโลยีประเภทต่างๆ มีความสำคัญต่อการเข้าใจประสิทธิภาพของเครือข่ายแต่ละชนิด ก่อนที่คอมพิวเตอร์จะสามารถแชร์ทรัพยากรต่างๆ หรือแลกเปลี่ยนข้อมูลซึ่งกันและกันได้ คอมพิวเตอร์นั้นจะต้องถูกเชื่อมต่อเข้าด้วยกันก่อน เครือข่ายส่วนมากจะใช้สายสัญญาณในการเชื่อมต่อ แต่การเชื่อมต่อแบบไร้สายก็สามารถทำได้เช่นกัน

อย่างไรก็ตามการเชื่อมต่อคอมพิวเตอร์เป็นเครือข่ายนั้นไม่ใช่แค่การใช้สายสัญญาณเชื่อมต่อเข้าที่เน็ตเวิร์คการ์ดของแต่ละเครื่องเท่านั้น โทโปโลยีที่ใช้ต้องสัมพันธ์กับสายสัญญาณ เน็ตเวิร์คการ์ด ระบบปฏิบัติการเครือข่าย และอุปกรณ์เครือข่ายอื่นๆ ที่จะเชื่อมกันเป็นเครือข่าย

การเลือกโทโปโลยีของเครือข่ายต้องมีการวางแผนที่ดี เพราะโทโปโลยีจะมีผลต่อชนิดของสายสัญญาณที่นำมาใช้รวมถึงลักษณะการเดินสายสัญญาณนี้ผ่านทางชั้นเพดาน และผนังของอาคาร ด้วยโทโปโลยียังเป็นตัวกำหนดลักษณะการสื่อสารกันระหว่างคอมพิวเตอร์ด้วย ต่างโทโปโลยีกันต้องใช้วิธีการสื่อสารข้อมูลที่ต่างกัน และวิธีการนี้จะมีผลอย่างมากต่อประสิทธิภาพของเครือข่าย ทุกเครือข่ายต้องประกอบด้วยโทโปโลยีใดโทโปโลยีหนึ่ง หรืออาจประกอบด้วยหลายๆ โทโปโลยีในหนึ่งเครือข่ายก็ได้ต่อไปนี้

3.4.4.1 โทโปโลยีแบบบัส (Bus Topology)

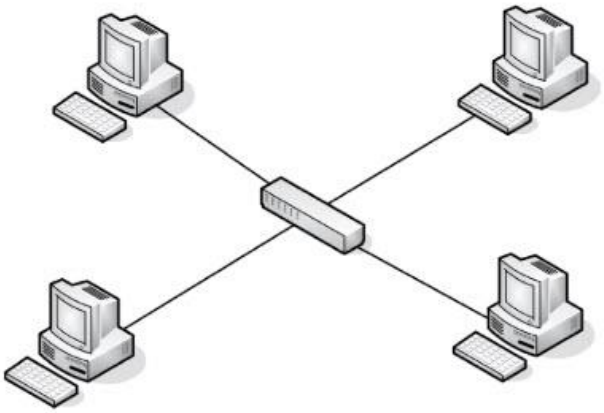
โทโปโลยีแบบบัส (Bus Topology) บางทีก็เรียกว่า Linear Bus เพราะมีการเชื่อมต่อแบบเส้นตรง และนี่เป็นลักษณะการเชื่อมต่อที่ง่ายที่สุด และเป็นโทโปโลยีที่นิยมกันมากที่สุดในสมัยแรกๆ ซึ่งการเชื่อมต่อแบบนี้จะใช้สายสัญญาณเพียงเส้นเดียวเชื่อมต่อคอมพิวเตอร์ทุกๆ เครื่องเข้าด้วยกัน คอมพิวเตอร์ที่เชื่อมต่อเข้ากับสายสัญญาณร่วมหรือบัส จะสื่อสารกันโดยใช้ที่อยู่ (Address) ซึ่งคอมพิวเตอร์แต่ละเครื่องจะมีที่อยู่ไม่ซ้ำกัน



รูปที่ 3.4 โทโปโลยีแบบบัส (Bus Topology) [5]

3.4.4.2 โทโปโลยีแบบดวงดาว (Star Topology)

สำหรับโทโปโลยีแบบดวงดาว (Star Topology) นี้ คอมพิวเตอร์แต่ละเครื่องจะเชื่อมต่อด้วยสายสัญญาณเข้ากับอุปกรณ์รวมศูนย์ที่เรียกว่า ฮับ (Hub) รูปที่ 3.5 แสดงการเชื่อมต่อเครือข่ายโทโปโลยีแบบดวงดาว สำหรับการเชื่อมต่อแบบนี้เมื่อคอมพิวเตอร์เครื่องใดจะส่งข้อมูลก็จะส่งไปที่ฮับก่อน แล้วฮับจะทำหน้าที่กระจายข้อมูลไปยังทุกเครื่องที่เชื่อมเข้ากับฮับ การต่อแบบนี้เริ่มใช้ในสมัยแรกๆ โดยการเชื่อมต่อเทอร์มินอลเข้ากับเครื่องเมนเฟรม



รูปที่ 3.5 โทโปโลยีแบบดวงดาว (Star Topology) [5]

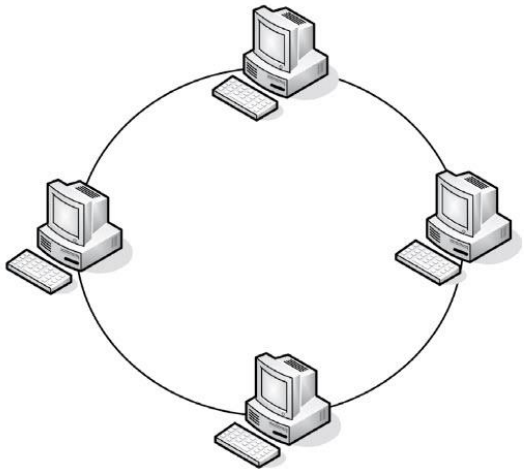
การเชื่อมต่อแบบนี้มีข้อดีคือ การรวมศูนย์เพื่อการบริหารทรัพยากร อย่างไรก็ตามการเชื่อมต่อแบบนี้จะสิ้นเปลืองสายสัญญาณมาก เนื่องจากทุกเครื่องต้องใช้สายสัญญาณเชื่อมต่อเข้ากับฮับ และอีกอย่างหนึ่งถ้าหากอุปกรณ์ที่ทำหน้าที่เป็นศูนย์กลางรับส่งข้อมูลหยุดทำงาน ระบบเครือข่ายก็จะล่มทันที แต่อย่างน้อยก็รู้

สาเหตุ ข้อดีอีกอย่างของโทโปโลยีแบบนี้คือ ถ้าสายสัญญาณขาด เฉพาะเครื่องที่ใช้สายสัญญาณนั้นเท่านั้นที่ไม่สามารถใช้เครือข่ายได้ส่วนเครื่องอื่นๆ ยังใช้เครือข่ายได้เช่นเดิม เนื่องจากฮับจะทำหน้าที่เป็นตัวสิ้นสุดสัญญาณโดยอัตโนมัติเมื่อสายขาดการเชื่อมต่อแบบนี้จะเป็นที่นิยมมากในปัจจุบัน เนื่องจากอีเธอร์เน็ตซึ่งกลายเป็นมาตรฐานเครือข่ายแบบท้องถิ่นในปัจจุบันก็ใช้การเชื่อมต่อหรือโทโปโลยีแบบดวงดาว

3.4.4.3 โทโปโลยีแบบวงแหวน (Ring Topology)

โทโปโลยีแบบวงแหวน (Ring Topology) นี้จะใช้สายสัญญาณเชื่อมต่อคอมพิวเตอร์เป็นห่วงหรือวงแหวน การเชื่อมต่อแบบนี้สัญญาณจะเดินทางเป็นวงกลมในทิศทางเดียว และจะวิ่งผ่านคอมพิวเตอร์แต่ละเครื่อง ซึ่งจะทำหน้าที่ทวนสัญญาณไปในตัวแล้วส่งผ่านไปเครื่องถัดไป ดังแสดง

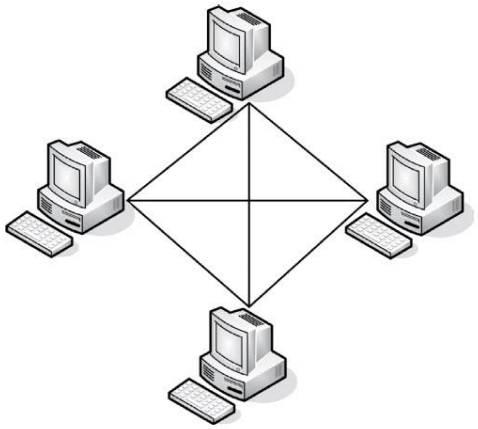
ในรูปที่ 3.6 เป็นเชื่อมโทโปโลยีแบบวงแหวนของคอมพิวเตอร์ 4 เครื่อง ถ้าคอมพิวเตอร์เครื่องใดเครื่องหนึ่งหยุดทำงานก็จะทำให้ระบบเครือข่ายล่มเช่นกัน



รูปที่ 3.6 โทโปโลยีแบบวงแหวน [5]

3.4.4.4 โทโปโลยีแบบเมซ (Mesh Topology)

โทโปโลยีแบบเมซ (Mesh Topology) คือ การเชื่อมต่อคอมพิวเตอร์แบบสมบูรณ์ กล่าวคือ คอมพิวเตอร์ทุกเครื่องในเครือข่ายจะเชื่อมต่อถึงกันหมดโดยใช้สายสัญญาณทุกการเชื่อมต่อ วิธีการนี้จะเป็นการสำรองเส้นทางเดินของข้อมูลได้เป็นอย่างดี เช่น ถ้าสายสัญญาณเส้นใดเส้นหนึ่งขาด ก็ยังมีเส้นทางอื่นที่สามารถส่งข้อมูลได้นอกจากนี้ยังเป็นระบบที่มีความเชื่อถือได้สูง แต่ข้อเสียก็คือ เครือข่ายแบบนี้จะใช้สายสัญญาณมาก ดังนั้นค่าใช้จ่ายในการติดตั้งระบบก็เพิ่มขึ้น รูปที่ 3.7 แสดงการเชื่อมต่อแบบเมซ



รูปที่ 3.7 โทโปโลยีแบบเมซ [5]

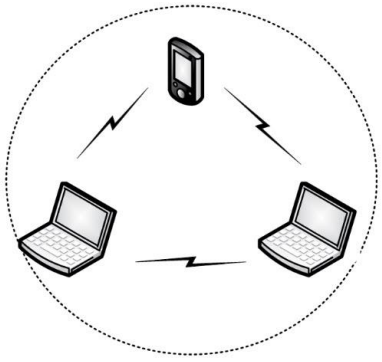
ในการเชื่อมต่อจริงๆ นั้นการเชื่อมต่อแบบเมชนั้นมีการใช้งานน้อยมาก เนื่องจากข้อเสียก็คือการเชื่อมต่อหลายจุดแต่เนื่องจากข้อดีของการเชื่อมต่อแบบเมชคือ การมีเส้นทางสำรองข้อมูล จึงได้มีการประยุกต์ใช้การเชื่อมต่อแบบเมชบางส่วนหรือการเชื่อมต่อแบบเมชที่ไม่สมบูรณ์ กล่าวคือ จะเชื่อมต่อเฉพาะลิงค์ที่จำเป็นหรือสำคัญ เช่น Core Network เป็นต้น

3.4.4.5 โทโปโลยีของ WLAN

โทโปโลยีของ WLAN อาจเป็นแบบธรรมดาหรืออาจจะซับซ้อนก็ได้ โดยแบบที่ง่ายที่สุดก็โดยการเชื่อมต่อกันของคอมพิวเตอร์ 2 เครื่องที่ติดตั้งเน็ตเวิร์คการ์ดแบบไร้สาย ซึ่งจะเรียกว่าเครือข่ายแบบเพียร์ทูเพียร์ (Peer-to-Peer) ส่วนเครือข่ายผสมระหว่างเครือข่ายไร้สายกับใช้สาย จุดที่เชื่อมต่อระหว่างสองเครือข่ายนี้จะเรียกว่า แอ็กเซสพอยต์ หรือ Access Point (AP) หรือจะเรียกว่าเป็นฮับ (Hub) ก็ได้ ซึ่งแต่ละจุดสามารถเชื่อมต่อเครื่องไคลเอนท์ของ WLAN ได้ประมาณ 10 - 50 ไคลเอนท์ต่อหนึ่ง AP ส่วนอุปกรณ์เครือข่ายและคอมพิวเตอร์ที่ใช้ช่องสัญญาณเดียวกันในการรับส่งข้อมูลจะเรียกว่า Basic Service Set (BSS) ส่วนระยะระหว่างเครื่องไคลเอนท์และแอ็กเซสพอยต์จะขึ้นอยู่กับสถานที่ตั้ง ซึ่งโดยส่วนใหญ่จะอยู่ที่ประมาณ 150 ถึง 300 เมตร ถ้าต้องการขยายระยะเครือข่ายก็สามารถทำได้โดยการใช้แอ็กเซสพอยต์หลายๆ เครื่องในการเชื่อมต่อเครือข่ายไวร์เลสแลนนั้นสามารถเชื่อมต่อได้สามแบบคือ

1) แอดฮอคเน็ตเวิร์ค (Ad Hoc Network)

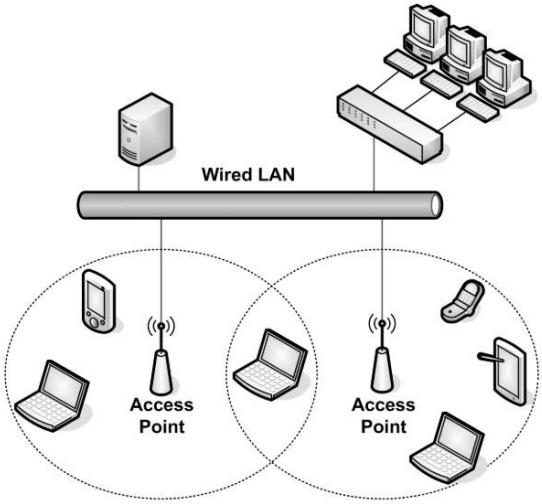
แอดฮอคเน็ตเวิร์ค (Ad Hoc Network) หรือบางทีก็เรียกว่า เพียร์ทูเพียร์คือ การใช้ไวร์เลสแลนโดยที่ไม่ต้องมีแอ็กเซสพอยต์ โดยแต่ละเครื่องหรือเพียร์นั้นจะเชื่อมต่อกันเอง เครื่องไหนที่ต้องการสื่อสารกับเครื่องไหนก็จะค้นหาและเชื่อมต่อกันเอง รูปที่ 3.8 แสดงการเชื่อมต่อ WLAN ในรูปแบบแอดฮอค



รูปที่ 3.8 การเชื่อมต่อระหว่างเพียร์ทูเพียร์ [6]

2) อินฟราสตัคเจอร์ (Infrastructure Network)

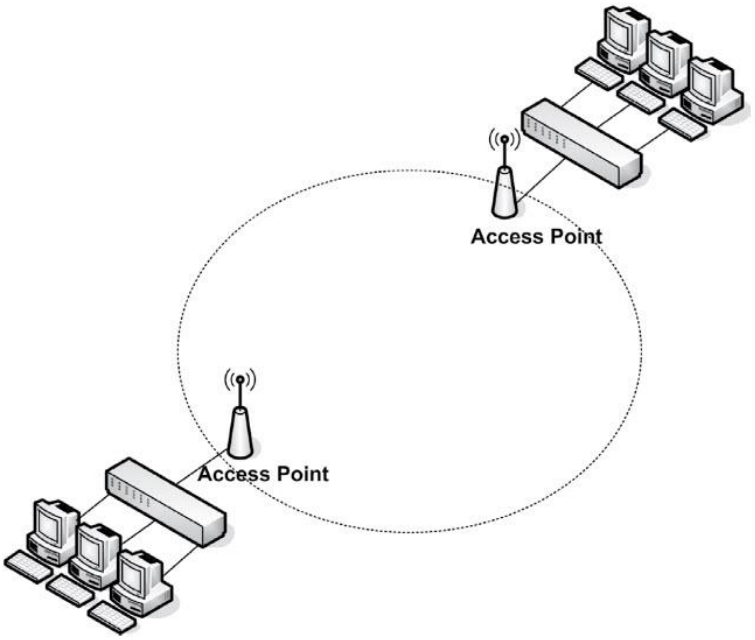
เครือข่ายไวร์เลสแลนแบบอินฟราสตรัคเจอร์ (Infrastructure Network) เป็นแบบมาตรฐานที่นิยมใช้ทั่วไป กล่าวคือการใช้งานนั้นจะมีแอ็กเซสพอยต์เป็นตัวกลางในการสื่อสารกันระหว่างไคลเอนท์หรือเน็ตเวิร์คในส่วนอื่นๆ เช่น เราท์เตอร์หรือเซิร์ฟเวอร์ เครื่องไคลเอนท์ที่ต้องการเชื่อมต่อเข้าเครือข่ายก็จะเชื่อมต่อเข้ากับแอ็กเซสพอยต์ที่ไคลเอนท์เห็นในบริเวณนั้นซึ่งหลังจากนั้นก็อาจมีการพิสูจน์ทราบตัวตน หรือการเข้ารหัสข้อมูลด้วย รูปที่ 3.9 แสดงการเชื่อมต่อแบบอินฟราสตรัคเจอร์



รูปที่ 3.9 การเชื่อมต่อ WLAN เข้ากับเครือข่ายแบบอินฟราสตรัคเจอร์ [6]

3) พอยต์ทูพอยต์ (Point to Point Network)

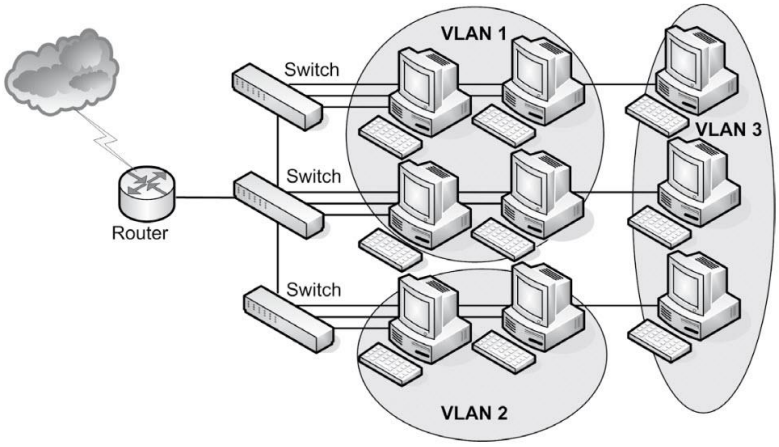
ในการเชื่อมต่อปกตินั้นแอ็กเซสพอยต์จะทำหน้าที่เป็นเสมือนเซิร์ฟเวอร์ที่รอรับการเชื่อมต่อจากไคลเอนท์ในบริเวณนั้น อย่างไรก็ตามแอ็กเซสพอยต์เองอาจทำหน้าที่เป็นเสมือนไคลเอนท์ที่เชื่อมต่อไปยังแอ็กเซสพอยต์อื่นๆ ซึ่งการทำหน้าที่เช่นนี้บางทีก็เรียกว่า เป็นบริดจ์ (Bridge) หรือสะพานเชื่อมต่อระหว่างเครือข่ายก็ได้ การใช้งานเช่นนี้บางทีก็เรียกว่าการสื่อสารแบบพอยต์ทูพอยต์ อย่างไรก็ตามเครื่องแอ็กเซสพอยต์ที่ทำหน้าที่เป็นแอ็กเซสพอยต์จริงๆ อาจอนุญาตให้ไคลเอนท์หรือแอ็กเซสพอยต์อื่นๆ เชื่อมต่อเข้ามาได้หลายครั้ง ดังนั้น อาจเรียกว่าเป็นการเชื่อมต่อแบบพอยต์ทูมัลติพอยต์อย่างไรก็ตามแอ็กเซสพอยต์สามารถทำหน้าที่เป็นไคลเอนท์เพื่อขยายเครือข่ายได้เช่นกัน รูปที่ 3.10 แสดงการเชื่อมต่อแบบพอยต์ทูพอยต์



รูปที่ 3.10 การใช้ WLAN เชื่อมต่อเครือข่ายแบบพอยต์ทูพอย [6]

3.4.5 ความรู้เรื่อง VLAN [6]

Virtual Local Area Network (VLAN) หมายถึง กลุ่มของคอมพิวเตอร์ที่อยู่ในบรอดคาสต์โดเมน (Broadcast Domain) เดียวกัน โดยคอมพิวเตอร์เหล่านี้อาจจะอยู่คนละ LAN เซ็กเมนต์ก็ได้ VLAN เป็นโปรโตคอลที่ทำงานในเลเยอร์ที่ 2 และเป็นเทคโนโลยีใหม่ที่พัฒนาเพื่อควบคุมการบรอดคาสต์ในเครือข่าย ที่ผ่านมาการควบคุมการบรอดคาสต์ในเครือข่ายจะใช้เราท์เตอร์ เพราะเราท์เตอร์จะไม่ส่งต่อแพ็กเก็ตประเภทบรอดคาสต์ แต่สวิตช์หรือฮับจะส่งต่อ การใช้เราท์เตอร์ในการควบคุมการบรอดคาสต์ในเครือข่ายนั้นอาจช่วยเพิ่มประสิทธิภาพของเครือข่ายได้ แต่ถ้ามีเราท์เตอร์จำนวนมากอาจทำให้การรับส่งแพ็กเก็ตช้าลงได้ ข้อดีของการใช้เลเยอร์ 2 สวิตช์คือ การรับส่งแพ็กเก็ตจะเร็วกว่าเราท์เตอร์ แต่ไม่สามารถควบคุมการบรอดคาสต์ในเครือข่ายได้ ดังนั้น จึงได้มีการพัฒนา VLAN ขึ้นมา เพื่อให้เลเยอร์ 2 สวิตช์สามารถควบคุมการบรอดคาสต์ในเครือข่ายได้ ดังรูปที่ 3.11 แสดงการจัดกลุ่ม VLAN โดยใช้สวิตช์

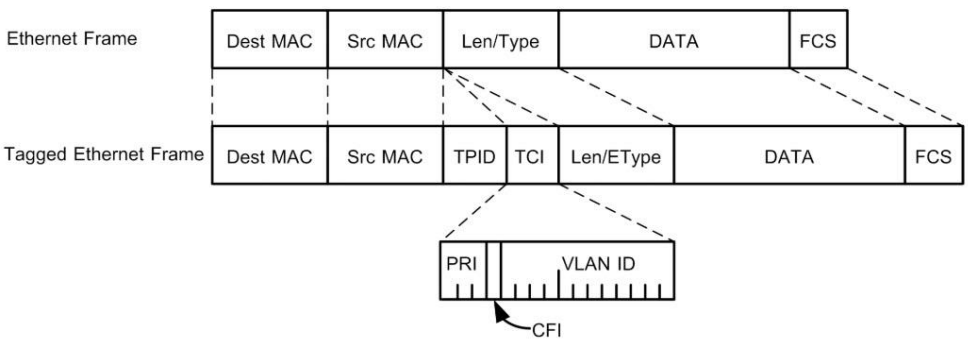


รูปที่ 3.11 การแบ่ง VLAN ในรูปแบบต่างๆ [6]

บรอดคาสต์โดเมน (Broadcast Domain) หมายถึง กลุ่มของคอมพิวเตอร์ที่เชื่อมต่อกันด้วยอุปกรณ์สวิตช์เลเยอร์ที่ 2 และเมื่อมีแพ็กเก็ตประเภทบรอดคาสต์ เครื่องคอมพิวเตอร์ทุกเครื่องจะได้รับแพ็กเก็ตนี้ทั้งหมด บรอดคาสต์แพ็กเก็ต หมายถึง แพ็กเก็ตที่มีที่อยู่ของเครื่องปลายทางเป็นหมายเลขบรอดคาสต์

3.4.5.1 มาตรฐาน IEEE 802.1Q/802.1p

IETF (Internet Engineering Task Force) ได้พัฒนามาตรฐาน IEEE 802.1Q และ IEEE 802.1p มาตรฐานนี้กำหนดขึ้นเพื่อให้สามารถสร้าง VLAN โดยใช้อุปกรณ์จากต่างบริษัทกัน ข้อกำหนดนี้ได้ปรับเปลี่ยนฟอร์แมตของเฟรมข้อมูลโดยเพิ่มฟิลด์ในส่วนหัวของเฟรมทั้งหมด 4 ไบต์ ซึ่งเป็นฟิลด์ถัดจากหมายเลข MAC ของเครื่องส่ง (Source MAC Address) _



รูปที่ 3.12 อีเธอร์เน็ตเฟรมของ VLAN [6]

เฟรมที่ถูกแท็ก (Tag) หรือเพิ่มข้อมูลของ VLAN จะมีฟิลด์ที่เพิ่มขึ้นมาคือ ฟิลด์ TPID (Tag Protocol Identifier) และ TCI (Tag Control Identifier) ซึ่งแต่ละฟิลด์มีความยาว 2 ไบต์ ฟิลด์ TPID จะถูกกำหนดให้เป็น 0x8100 คงที่เสมอ ดังนั้นเมื่อใดก็ตามที่ฟิลด์ TPID มีค่าเป็น 0x8100 แสดงว่า เฟรมนี้มีแท็กของ IEEE 802.1Q/802.1p ซึ่งถ้าเป็นเฟรมของอีเธอร์เน็ตธรรมดา ค่านี้ก็จะตรงกับฟิลด์ Len/Type ซึ่ง 0x8100 เป็นค่าที่สำรองไว้ (Reserved) นั่นหมายความว่า สวิตช์ที่ไม่รองรับ VLAN ก็จะไม่ส่งต่อเฟรมดังกล่าว

ฟิลด์ TCI จะแบ่งออกเป็น 3 ฟิลด์ย่อยคือ 3 บิตแรกเป็น PRI (Priority) ซึ่งเป็นฟิลด์ที่กำหนดระดับความสำคัญตามมาตรฐาน IEEE 802.1p เนื่องจากมี 3 บิตจึงสามารถกำหนดระดับความสำคัญได้ 8 ระดับ ส่วนอีกหนึ่งบิตถัดมาคือฟิลด์ CFI (Canonical Format Identifier) ซึ่งเป็นฟิลด์ที่ใช้สำหรับการรับส่งข้อมูลของเครือข่ายโทเคนริงผ่านอีเธอร์เน็ต ส่วน12 บิตสุดท้ายเป็นฟิลด์ VLAN ID หรือ VID ซึ่งเป็นหมายเลขของ VLAN กำหนดโดยมาตรฐาน IEEE 802.1Q ดังนั้น ในหนึ่งเครือข่ายสามารถมี VLAN ได้ทั้งหมด 4096 วง (212 = 4096)

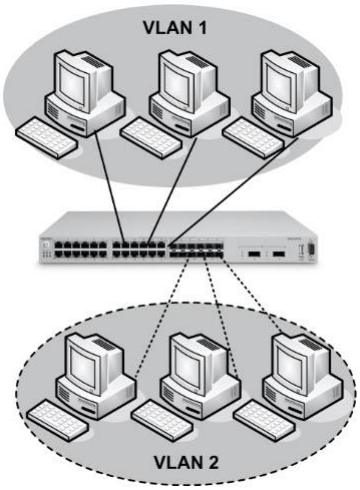
ถัดจากฟิลด์ TPID และ TCI จะเป็นฟิลด์ Len/Etype ซึ่งมีความยาว 2 ไบต์ เป็นฟิลด์ที่มีอยู่เดิมอยู่แล้ว ซึ่งจะเป็นฟิลด์ที่บอกความยาวของเฟรมสำหรับ IEEE 802.3 หรือเป็น EtherType สำหรับอีเธอร์เน็ตเวอร์ชัน 2 (Ethernet v.2)

3.4.5.2 Layer 2 VLAN

การจัดกลุ่ม VLAN ประเภทนี้จะใช้ข้อมูลที่อยู่ในเลเยอร์ 2 เป็นเกณฑ์ เช่น พอร์ตของสวิตช์ และหมายเลข MAC ของเน็ตเวิร์คการ์ด ซึ่งมีรายละเอียด ดังนี้

- Port-Based VLAN

การจัดกลุ่ม VLAN โดยใช้พอร์ตของสวิตช์ (Port-Based VLAN) ซึ่งเป็นการใช้ VLAN ที่นิยมกันมากที่สุดการจัดกลุ่มด้วยวิธีนี้คือ การจัดกลุ่มของพอร์ตบนสวิตช์หนึ่งหรือมากกว่าให้อยู่ในวง VLAN เดียวกัน ตัวอย่างเช่น สมมติว่า สวิตช์เครื่องหนึ่งมี 12 Port เราสามารถกำหนดให้พอร์ต 1-6 เป็นสมาชิกของวง VLAN 1 และ พอร์ต 7-12 เป็นสมาชิกของวง VLAN 2 การจัดเช่นนี้จะทำให้คอมพิวเตอร์ที่เชื่อมต่อเข้ากับสวิตช์พอร์ต 1-6 อยู่ในบรอดคาสต์โดเมนเดียวกัน ในขณะที่คอมพิวเตอร์ที่เชื่อมต่อกับพอร์ต 7-12 จะอยู่อีกบรอดคาสต์โดเมนหนึ่ง ถ้าเป็นสวิตช์ที่ไม่รองรับ VLAN แล้วแพ็กเก็ตแบบบรอดคาสต์ที่ส่งโดยคอมพิวเตอร์เครื่องใดเครื่องหนึ่งจะถูกส่งต่อไปยังทุกๆ พอร์ตของสวิตช์ แต่ในกรณีที่สวิตช์รองรับ VLAN และมีการจัดกลุ่มเหมือนข้างต้น แพ็กเก็ตแบบบรอดคาสต์ก็จะถูกส่งต่อไปยังเฉพาะพอร์ตที่จัดอยู่ในวง VLAN เดียวกันเท่านั้น ส่วนการสื่อสารระหว่างคอมพิวเตอร์ที่อยู่ต่าง VLAN กันจะต้องอาศัยฟังก์ชันของเราท์เตอร์หรือสวิตช์เลเยอร์ 3 เพื่อช่วยในการส่งต่อแพ็กเก็ตระหว่าง VLAN ดังนั้น VLAN หนึ่งวงก็เปรียบเสมือนเครือข่าย LAN หนึ่งวงนั่นเอง



รูปที่ 3.13 แสดงตัวอย่างการจัดกลุ่ม VLAN แบบ Port-Based [6]

การแบ่ง VLAN แบบพอร์ตเบสนี้ยังคงเป็นวิธีที่นิยมมากที่สุดในปัจจุบัน เนื่องจากง่ายต่อการจัดการ แต่ข้อจำกัดของการจัด VLAN แบบนี้คือ แต่ละพอร์ตของสวิตช์จะเป็นสมาชิกของ VLAN ได้หนึ่งวงเท่านั้น นอกจากนี้ข้อเสียขอการจัดแบบนี้คือ เมื่อผู้ใช้เคลื่อนย้ายหรือต้องเปลี่ยนพอร์ตสวิตช์ ผู้ดูแลระบบต้องจัดการ VLAN ใหม่ เพื่อที่จะทำให้ผู้ใช้คนนั้นอยู่ในวง VLAN เดิม

- MAC Address-Based VLAN

การจัดกลุ่มของ VLAN วิธีนี้จะใช้หมายเลข MAC ซึ่งหมายเลขนี้จะถูกกำหนดตายตัวให้กับแต่ละเน็ตเวิร์คการ์ดของเครื่องคอมพิวเตอร์ ข้อดีของการจัดกลุ่มประเภทนี้ก็คือ เมื่อมีการย้ายที่ของผู้ใช้ ผู้ดูแลระบบไม่ต้องเซต VLAN ให้กับผู้ใช้คนนี้ใหม่ เนื่องจาก VLAN จะผูกติดกับหมายเลข MAC ไม่ใช่พอร์ตของสวิตช์เหมือนกับวิธีแรก ดังนั้นการจัด VLAN ในลักษณะนี้จึงง่ายต่อการจัดการผู้ใช้ แต่จุดด้อยของการจัดกลุ่มแบบนี้คือ คอมพิวเตอร์ทุกเครื่องจะต้องถูกเซตให้อยู่วง VLAN วงหนึ่งก่อนในตอนแรก การที่ต้องทำเช่นนี้ก็อาจเป็นไปได้ยากสำหรับองค์กรขนาดใหญ่ที่มีคอมพิวเตอร์จำนวนมาก ปัญหาอีกอย่างของการจัด VLAN แบบนี้คือ กรณีที่คอมพิวเตอร์หลายเครื่องแชร์สวิตช์พอร์ตเดียวกัน เช่น การเชื่อมต่อพอร์ตนั้นเข้ากับฮับแล้ว ถ้าคอมพิวเตอร์ที่เชื่อมเข้ากับฮับจัดอยู่ใน VLAN คนละวงกัน จะทำให้ประสิทธิภาพของเครือข่ายลดลงมาก เนื่องจากว่าพอร์ตดังกล่าวนี้เป็นสมาชิกของ VLAN หลายวง ทำให้แพ็กเก็ตประเภทบรอดคาสต์ของแต่ละวงVLAN ที่เป็นสมาชิกจะถูกส่งมายังพอร์ตนี้ทั้งหมด

3.4.5.3 Layer 3 VLAN

การจัดกลุ่ม VLAN แบบนี้จะใช้ข้อมูลของเลเยอร์ที่ 3 เช่น ประเภทของโปรโตคอลหรือหมายเลขไอพี (IP Address)การจัด VLAN ประเภทนี้มีทั้งข้อดีข้อเสีย ข้อดีคือ เมื่อผู้ใช้ต้องย้ายที่

ผู้ดูแลระบบไม่ต้องเซต VLAN ให้กับผู้ใช้คนนี้ใหม่อีกครั้ง นอกจากนี้การทำ VLAN โดยใช้ข้อมูลในเลเยอร์ที่ 3 ก็ไม่จำเป็นต้องทำแท็กกิ้ง (Tagging) สำหรับการสื่อสารระหว่างสมาชิกของ VLAN ที่อยู่คนละสวิตช์กัน แต่ข้อเสียคือ สวิตช์จะทำงานช้าลง เนื่องจากสวิตช์ต้องตรวจสอบข้อมูลในเลเยอร์ 3 ซึ่งจะใช้เวลานานกว่า การตรวจสอบข้อมูลใน เลเยอร์ที่ 2

ถึงแม้ว่าการจัดกลุ่ม VLAN วิธีนี้จะใช้ข้อมูลที่อยู่ที่เลเยอร์ 3 แต่ก็ไม่มีการทำเราท์ติ้ง (Routing) หรือจัดเส้นทางแพ็กเก็ตข้อมูลในเลเยอร์ที่ 3 การทำเราท์ติ้งยังคงต้องทำในเราท์เตอร์หรือสวิตช์เลเยอร์ 3 เหมือนเดิม ดังนั้น การสื่อสารระหว่าง VLAN จำเป็นที่ต้องใช้ฟังก์ชันของเราท์เตอร์มาช่วย แต่โดยส่วนใหญ่บริษัทที่ผลิตสวิตช์ที่รองรับ VLAN ในเลเยอร์ที่3 จะรวมฟังก์ชันเราท์ติ้งนี้เข้าไปในสวิตช์ด้วย ซึ่งจะเรียกสวิตช์ประเภทนี้ว่า “เลเยอร์ 3 สวิตช์” ฟังก์ชันนี้จะถูกโปรแกรมรวมเข้าไปในชิปแบบ ASIC (Application Specific Integrated Circuits) ซึ่งเป็นชิปที่ควบคุมการทำงานของสวิตช์ ในขณะที่เราท์เตอร์จะใช้โปรเซสเซอร์ทั่วๆ ไป (General Processor) ทำให้สวิตช์เลเยอร์ 3 ทำงานเร็วกว่าเราท์เตอร์ทั่วไปมาก อย่างไรก็ตามฟังก์ชันเราท์ติ้งยังคงจำเป็นสำหรับการสื่อสารระหว่าง VLAN

- Protocol Type-Based VLAN

การสร้าง VLAN ประเภทนี้จะจัดกลุ่มโดยใช้ประเภทของโปรโตคอลในเลเยอร์ที่ 3 เช่น IP, IPX เป็นต้น ยกตัวอย่าง เช่น กลุ่มคอมพิวเตอร์ที่ใช้โปรโตคอล IP ก็จะถูกจัดให้เป็น VLAN วงหนึ่ง ส่วนคอมพิวเตอร์ที่ใช้โปรโตคอล IPX ก็ถูกจัดให้อยู่อีกกลุ่มหนึ่ง เป็นต้น การจัดกลุ่มด้วยวิธีนี้จะมีประโยชน์มากสำหรับเครือข่ายที่ต้องการแยกกลุ่มของคอมพิวเตอร์ที่ใช้โปรโตคอลหรือแอพพลิเคชันต่างกัน ทำให้ปัญหาเกี่ยวกับการทำงานร่วมกันไม่ได้ของโปรโตคอลหมดไป

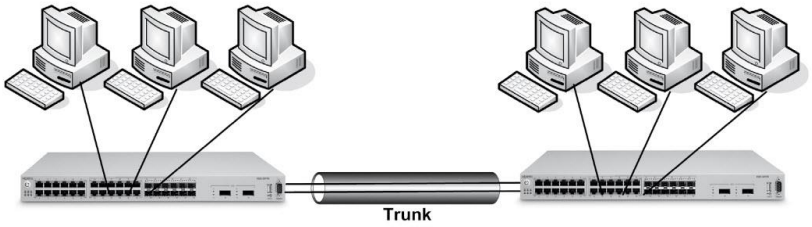
- IP-Based VLAN

สำหรับเครือข่ายที่ใช้โปรโตคอล TCP/IP นั้นการจัดกลุ่ม VLAN วิธีนี้จะใช้หมายเลขเครือข่าย (Network ID) เป็นเกณฑ์ในการจัดกลุ่ม VLAN สำหรับการแบ่งเครือข่ายออกเป็นเครือข่ายย่อยหรือซับเน็ตนั้น โดยส่วนใหญ่แต่ละซับเน็ตจะถูกแยกจากกันในระดับฟิสิคอลโดยมีเราท์เตอร์เชื่อมระหว่างซับเน็ตเหล่านั้น อาจมีบางกรณีที่บางซับเน็ตอาจจะใช้สวิตช์ร่วมกันได้ แต่ข้อเสียก็คือ ซับเน็ตที่ใช้กลุ่มของสวิตช์เดียวกันจะแชร์บรอดคาสต์โดเมนเดียวกัน ในกรณีนี้ VLAN จะช่วยให้ซับเน็ตแยกบรอดคาสต์โดเมนของแต่ละซับเน็ตในขณะที่ยังแชร์กันใช้สวิตช์ชุดเดียวกันอยู่

- Port Trunking

การทำพอร์ตทรั้งกิ้ง (Port Trunking) หรือสามารถเรียกอีกอย่างหนึ่งว่าพอร์ตอะกรีเกชัน (Link Aggregation) เป็นมาตรฐาน IEEE 802.3ad ซึ่งเป็นการขยายแบนด์วิธ (Bandwidth) ให้กับลิงค์โดยการรวมเอาหลายๆ พอร์ตของสวิตช์ให้ทำงานเสมือนเป็นพอร์ตเดียวกัน ตัวอย่างเช่น เราสามารถรวมเอา 3 พอร์ตของสวิตช์ที่วิ่งที่ความเร็ว 100 Mbps เป็นทรั้งค์ ทำให้แบนด์

วิธของลิงค์เพิ่มเป็น 300 Mbps และถ้าพอร์ตดังกล่าวรองรับฟูลดูเพล็กซ์ ลิงค์ก็มีแบนด์วิธเป็น 600 Mbps



รูปที่ 3.14 Port Trunking [6]

ข้อดีของการทำ Port Trunking มีดังนี้

- เพิ่มแบนด์วิธของลิงค์
- การแชร์โหลดระหว่างพอร์ต
- การแยกกลุ่มของเฟรมตามแอดเดรส ทำให้แพ็กเก็ตรับส่งตามลำดับ
- Fault Tolerance : ถ้าพอร์ตใดพอร์ตหนึ่งเสีย พอร์ตที่เหลือยังคงทำงานได้ตามปกติ

การทำพอร์ต Port Trunking มีประโยชน์สำหรับลิงค์ที่เชื่อมต่อระหว่างสวิตช์ หรือลิงค์ที่มีอัตราการรับส่งข้อมูลสูง

3.4.6 หลักการออกแบบระบบเครือข่าย [6]

หลักสำคัญในการออกแบบระบบเครือข่ายคือ การทำให้ระบบเครือข่ายตอบสนองต่อความต้องการ และสามารถรองรับการขยายตัวได้ในอนาคต โดยเป้าหมายที่สำคัญของการออกแบบเครือข่าย เช่น การทำให้เครือข่ายสามารถให้บริการได้ตลอดเวลา หรือไม่ล่มหรือดาวน์บ่อยๆ มีแบนด์วิธเพียงพอต่อความต้องการ มีเส้นทางสำรองหากเส้นทางหลักล่ม นอกจากนี้ระบบต้องมีความปลอดภัยจากภัยคุกคามต่างๆ โดยจะนำเสนอการออกแบบระบบเครือข่ายแบบมีลำดับชั้น ซึ่งจะช่วยทำให้สามารถบริหารจัดการหรือดูแลได้ง่าย ตอบสนองต่อความต้องการผู้ใช้ และขยายได้ง่ายในอนาคต

ขั้นตอนที่สำคัญสำหรับการออกแบบเครือข่าย มีดังนี้

1. ตรวจสอบเป้าหมายของธุรกิจและความต้องการด้านเทคนิค
2. กำหนดฟีเจอร์และฟังก์ชันที่จำเป็นสำหรับตอบสนองความต้องการข้างต้น
3. ประเมินความพร้อมของระบบเครือข่ายที่มีอยู่

4. ออกแบบเครือข่ายพร้อมทั้งแผนการทดสอบว่าตอบสนองความต้องการหรือไม่

5. สร้างแผนการดำเนินการหรือโครงการ

3.4.6.1 เป้าหมายของการออกแบบเครือข่าย

จากความต้องการเบื้องต้นทางด้านเครือข่าย ทำให้สรุปเป็นเป้าหมายที่สำคัญสำหรับการออกแบบระบบเครือข่าย คือ

1) Scalability การออกแบบเครือข่ายต้องสามารถขยายตัวได้ตามกลุ่มผู้ใช้ที่เพิ่มขึ้น หรือมีการเพิ่มไซต์ที่อยู่ไกลออกไปได้ หรือรองรับการทำงานของแอพพลิเคชันใหม่โดยที่ไม่มีผลกระทบต่อผู้ใช้เดิม

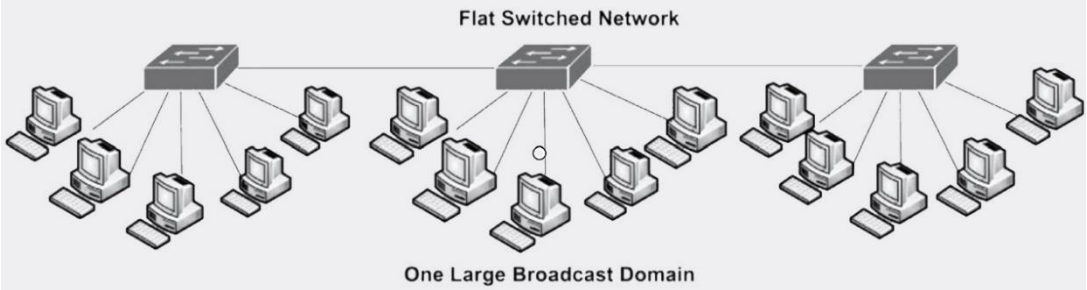
2) Availability คือ การออกแบบให้เครือข่ายสามารถทำงานได้ 24x7 โดยที่ถ้ามีลิงค์บางลิงค์ขาด หรืออุปกรณ์บางอุปกรณ์เสีย ก็ไม่ควรมีผลกระทบมากต่อระบบเครือข่ายโดยรวม

3) Security การออกแบบเครือข่ายให้มีความปลอดภัยนั้นควรทำตั้งแต่ช่วงเริ่มต้น ไม่ใช่มาเพิ่มอุปกรณ์ในภายหลัง การออกแบบโดยการวางอุปกรณ์ด้านการรักษาความปลอดภัยในตำแหน่งที่ควรจะวาง การฟิลเตอร์ทราฟฟิกที่ไม่จำเป็น การกำหนดนโยบายของไฟร์วอลล์ ล้วนแล้วแต่เป็นสิ่งที่สำคัญอย่างยิ่งต่อการปกป้องทรัพยากรต่างๆ ที่อยู่ในเครือข่าย

4) Manageability หลังจากที่มีระบบเครือข่ายไว้ให้บริการแล้ว เจ้าหน้าที่ต้องสามารถดูแลรักษาให้ระบบทำงานได้ตามที่ออกแบบไว้ การออกแบบเครือข่ายนั้นควรคำนึงถึงความง่ายในการดูแลระบบด้วย การออกแบบที่ซับซ้อนเกินไปอาจสร้างปัญหาในภายหลังได้

3.4.6.2 เครือข่ายแบบลำดับชั้น (Hierarchical Network)

เริ่มต้นนั้นเครือข่ายอาจประกอบด้วยสวิตช์หนึ่งหรือสองเครื่องเชื่อมต่อคอมพิวเตอร์เข้าเป็นเครือข่าย เมื่อต้องการขยายก็ซื้อสวิตช์มาเชื่อมต่อเพิ่มขึ้นเรื่อยๆ การออกแบบเครือข่ายในลักษณะนี้จะเรียกว่า เครือข่ายแบนราบ (Flat Network) ซึ่งจะเหมาะสำหรับเครือข่ายขนาดเล็กถึงกลาง อย่างไรก็ตามเมื่อเครือข่ายมีการขยายใหญ่ขึ้น การเชื่อมต่อสวิตช์เข้าไปเรื่อยๆ อาจสร้างปัญหาให้กับเครือข่ายได้ เนื่องจากเครือข่ายแบบแบนราบนี้จะไม่มีการควบคุมการบรอดคาสต์ หรือการจัดโซนเพื่อควบคุมและรักษาความปลอดภัย ดังนั้น สำหรับเครือข่ายขนาดใหญ่นั้นจึงควรใช้การออกแบบเครือข่ายแบบมีลำดับชั้น (Hierarchical Network Design)

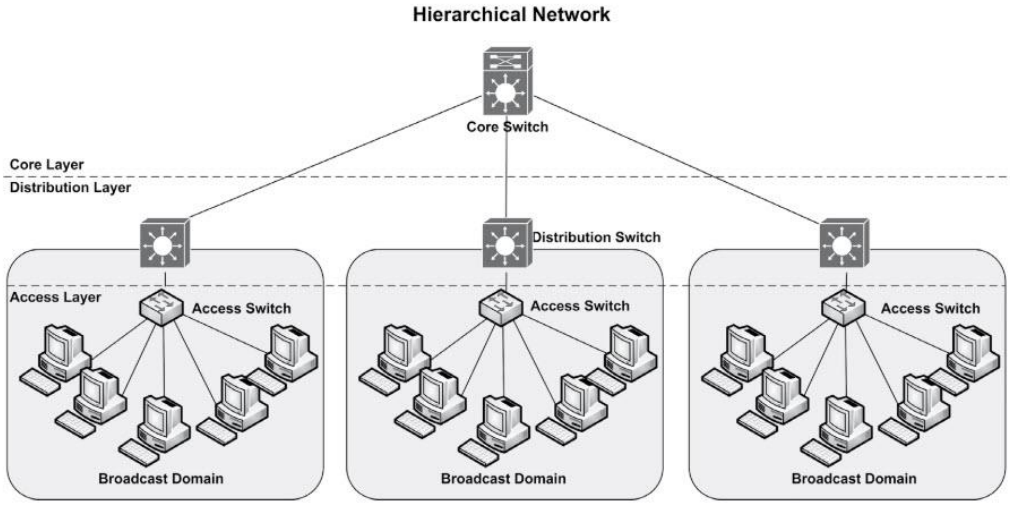


รูปที่ 3.15 เครือข่ายแบนราบ (Flat Network) [6]

การออกแบบเครือข่ายแบบลำดับชั้น หมายถึง การออกแบบโดยจัดกลุ่มอุปกรณ์ในเครือข่ายเป็นหลายๆ กลุ่ม โดยเชื่อมต่อกันเป็นลำดับชั้นหรือเลเยอร์โดยเลเยอร์หลักประกอบด้วย 3 เลเยอร์ คือ

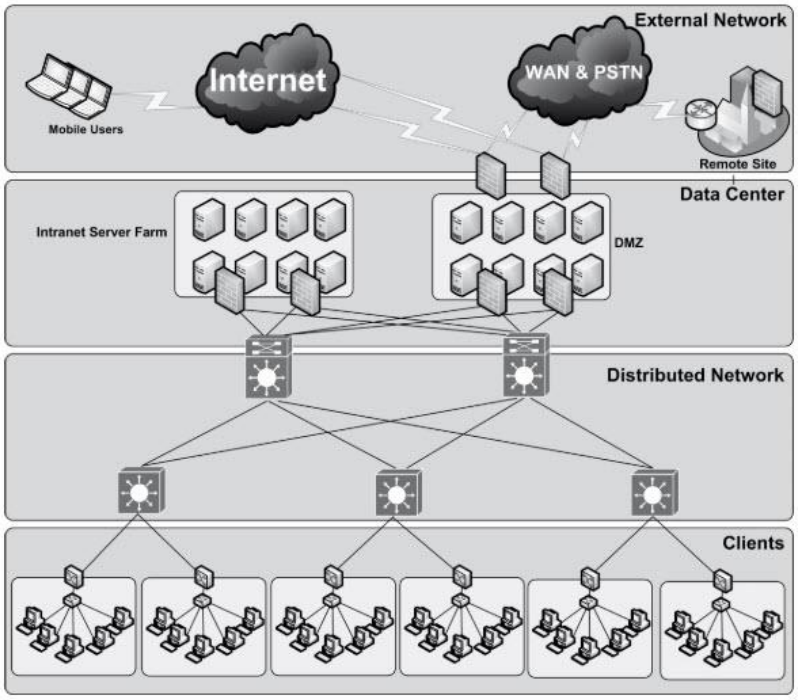
1. คอร์เลเยอร์ (Core Layer) เป็นกลุ่มอุปกรณ์หลักในเครือข่ายที่เชื่อมต่อกันด้วยความเร็วสูง
2. ดิสทริบิวชันเลเยอร์ (Distribution Layer) เป็นกลุ่มอุปกรณ์ที่เชื่อมโยงอุปกรณ์หลักไปยังอุปกรณ์เครือข่ายปลายทาง
3. แอ็กเซสเลเยอร์ (Access Layer) เป็นกลุ่มของอุปกรณ์เครือข่ายที่เชื่อมต่ออุปกรณ์ปลายทาง เช่น พีซี โน้ตบุ๊ค แท็บเล็ต สมาร์ทโฟน เป็นต้น

การออกแบบเครือข่ายแบบลำดับชั้นจะมีข้อได้เปรียบเครือข่ายแบบแบนราบ เนื่องจากการแบ่งเครือข่ายใหญ่ๆ เป็นหลายๆ เครือข่ายย่อยแล้วเชื่อมต่อกันเป็นลำดับชั้น จะช่วยให้โลคอลทราฟฟิก จะวิ่งอยู่ในเฉพาะวงเครือข่ายโลคอลนั้นๆ เท่านั้น เฉพาะทราฟฟิกที่มีปลายทางอยู่ในเครือข่ายอื่นเท่านั้นที่จะวิ่งออกมานอกเครือข่ายหรือวิ่งไปยังชั้นที่สูงขึ้น ทำให้ทราฟฟิกไม่รบกวนซึ่งกันและกัน ในขณะที่อุปกรณ์เครือข่ายเลเยอร์ 2 ที่เชื่อมต่อในเครือข่ายแบบแบนราบนั้นจะ ไม่สามารถควบคุมทราฟฟิกแบบบรอดคาสต์หรือทราฟฟิกที่ไม่ต้องการได้ดีเท่าที่ควร ถ้ามีการเพิ่มแอพพลิเคชันหรือไคลเอนท์เข้าไปในเครือข่าย ก็อาจทำให้ประสิทธิภาพของเครือข่ายโดยรวมลดลงไป และถึงจุดหนึ่งอาจทำให้ระบบเครือข่ายเกิดความไม่เสถียรได้ รูปที่ 3.16 เป็นภาพที่แสดงผังการเชื่อมต่อเครือข่ายแบบลำดับชั้น



รูปที่ 3.16 เครือข่ายแบบลำดับชั้น (Hierarchy Network) [6]

นอกจากการแบ่งเครือข่ายออกเป็นชั้นๆ แล้ว สำหรับองค์กรขนาดใหญ่ที่มีระบบไอทีใช้ภายในองค์กร และมีการเชื่อมต่อกับอินเทอร์เน็ตและให้บริการด้วย เช่น เว็บไซต์อีคอมเมิร์ซ อีเมล เป็นต้น ดังนั้น ก็อาจมีเครือข่ายย่อยพิเศษเพิ่มขึ้นมา เช่น ดาต้าเซ็นเตอร์หรือเซิร์ฟเวอร์ฟาร์ม DMZ ซึ่งเป็นโซนที่เชื่อมต่อเข้ากับอินเทอร์เน็ตนั่นเอง เป็นต้น รูปที่ 3.17 เป็นการออกแบบเครือข่ายในระดับเอ็นเตอร์ไพรส์ที่มีโซนพิเศษแยกออกมาเพื่อให้ง่ายต่อการรักษาความปลอดภัย



รูปที่ 3.17 เครือข่ายในระดับเอ็นเตอร์ไพรส์ (Enterprise Network) [6]

การออกแบบเครือข่ายแบบมีลำดับชั้นจะง่ายต่อการรักษาความปลอดภัย ระบบมีความเสถียร มั่นคง และสามารถวิเคราะห์หาจุดเสีย หรือสิ่งที่ก่อให้เกิดปัญหาในเครือข่ายได้ง่าย การพัฒนาปรับปรุงก็สามารถทำได้ง่าย เนื่องจากสามารถพัฒนาได้ในส่วนของเครือข่ายซึ่งเป็นอิสระซึ่งกันและกัน และที่สำคัญคือ มีความยืดหยุ่นและขยายได้ง่าย โดยสามารถเพิ่มเซอร์วิสหรือแอพพลิเคชันได้โดยที่ไม่ต้องเปลี่ยนแปลงโครงสร้างพื้นฐานทางเครือข่าย

แอ็กเซสเลเยอร์ (Access Layer)

แอ็กเซสเลเยอร์ (Access Layer) เป็นจุดที่เครื่องไคลเอนท์เชื่อมต่อเข้ากับเครือข่าย ในชั้นนี้จะเป็นการควบคุมให้ทราฟฟิกที่เป็นโลคอลให้วิ่งอยู่ในเฉพาะวงเครือข่ายนั้นๆ นอกจากนี้เลเยอร์นี้ยังเป็นจุดที่จะควบคุมการเข้าถึงเครือข่ายของไคลเอนท์หรือผู้ใช้ด้วย อุปกรณ์ที่อยู่ในเลเยอร์นี้ส่วนใหญ่จะเป็น L2 สวิตช์หรือฮับ และอาจใช้ VLAN ในการแบ่งกลุ่มของ LAN ซึ่งก็จะเป็นการจำกัดวงของบรอดคาสต์โดเมน โดยปกติสวิตช์จะเป็นแบบ 10/100BaseTx ซึ่งอาจมีพอร์ตอัพลิงค์ที่ความเร็ว 100 Mbps หรือ 1 Gbps ไปยังสวิตช์ในดิสทริบิวชันเลเยอร์ ในแต่ละวง LAN หรือ VLAN อาจกำหนดให้มีหมายเลขไอพีคนละซับเน็ตกัน และอาจใช้ STP (Spanning Tree Protocol) คนละชุดกัน เพื่อให้ระบบมีเส้นทางสำรองหากเส้นทางหลักมีปัญหา

ดิสทริบิวชันเลเยอร์ (Distribution Layer)

ดิสทริบิวชันเลเยอร์ (Distribution Layer) เป็นเลเยอร์ที่เชื่อมระหว่างแอ็กเซสเลเยอร์และคอร์เลเยอร์ ในเลเยอร์นี้จะมีการควบคุมการเข้าถึงรีซอร์สที่อยู่ทางฝั่งคอร์เลเยอร์ ซึ่งก็จะมีการขยายแบนด์วิธโดยเชื่อมต่ออัพลิงค์โดยใช้ 2 พอร์ต ซึ่งเรียกว่า การทำพอร์ตทรั้งกิ้ง (Port Trunking) ซึ่งก็จะทำให้แบนด์วิธขยายเพิ่มเป็น 2 เท่านั่นเอง นอกจากการทำพอร์ตทรังกิ้งแล้ว การเชื่อมต่อของดิสทริบิวต์สวิตช์และคอร์สวิตช์อาจใช้ 2 เส้น โดยแต่ละเส้นจะเชื่อมต่อไปยังคนละคอร์สวิตช์ ซึ่งการทำเช่นนี้ก็จะช่วยเพิ่มความพร้อมใช้งาน ซึ่งถ้าหากลิงค์หนึ่งขาดก็ยังเหลืออีกลิงค์หนึ่งสำรองอยู่ และในเลเยอร์นี้ก็จะมีการทำเราท์ติ้ง หรือจัดเส้นทางแพ็กเก็ตข้อมูล และเลเยอร์นี้จะสิ้นสุด VLAN หรือจำกัดวงบรอดคาสต์โดเมนในวง LAN หรือ VLAN ด้วย

คอร์เลเยอร์ (Core Layer)

คอร์เลเยอร์ (Core Layer) เครือข่ายความเร็วสูงหรือแบนด์วิธสูงมาก ซึ่งสามารถส่งผ่านแพ็กเก็ตข้อมูลผ่านเครือข่ายได้อย่างรวดเร็ว คอร์เลเยอร์หรืออาจเรียกว่า แบ็คโบน (Backbone) ของเครือข่ายก็ได้ เป็นเครือข่ายที่มีความสำคัญอย่างยิ่งต่อประสิทธิภาพโดยรวมของระบบเครือข่าย เพราะฉะนั้นการออกแบบเครือข่ายในเลเยอร์นี้ต้องคำนึงถึงประสิทธิภาพ ความเสถียร ความพร้อมใช้งานเสมอ และความปลอดภัยจากการถูกโจมตี เครือข่ายแบบฟอลต์ทอเรอแรนท์ (Fault-tolerance) เป็นเครือข่ายที่ถูกออกแบบเพื่อทนต่อข้อผิดพลาดหรือข้อขัดข้องต่างๆ หรือถ้ามีเหตุขัดข้องหรือมีบางอย่างเสียก็จะไม่ส่งผลกระทบต่อระบบเครือข่ายโดยรวมมากนัก และถ้าหากลิงค์ใดลิงค์หนึ่งเสีย

หรือขาดอุปกรณ์ควรต้องสามารถจัดเส้นทางข้อมูล หรือเราท์แพ็กเก็ตไปยังเส้นทางอื่นที่ยังคงใช้ได้อย่างรวดเร็ว และมีผลกระทบน้อยที่สุด

3.4.7 เครื่องมือสำหรับการรักษาความปลอดภัยในเครือข่าย

ถึงแม้ว่าการปกป้องข้อมูลเป็นสิ่งที่มีลำดับความสำคัญสูงสุด แต่การดูแลรักษาระบบหรือเครือข่ายให้ทำงานอย่างถูกต้องก็เป็นปัจจัยที่สำคัญในการปกป้องข้อมูลที่อยู่ในเครือข่ายนั้น ถ้ามีช่องโหว่ของระบบเครือข่ายที่อนุญาตให้โจมตีได้ความเสียหายที่เกิดขึ้นอาจมากกว่าที่คาดไว้ และอาจใช้ทั้งเวลาและความพยายามอย่างมากที่จะทำให้ระบบกลับมาทำงานได้เหมือนเดิม

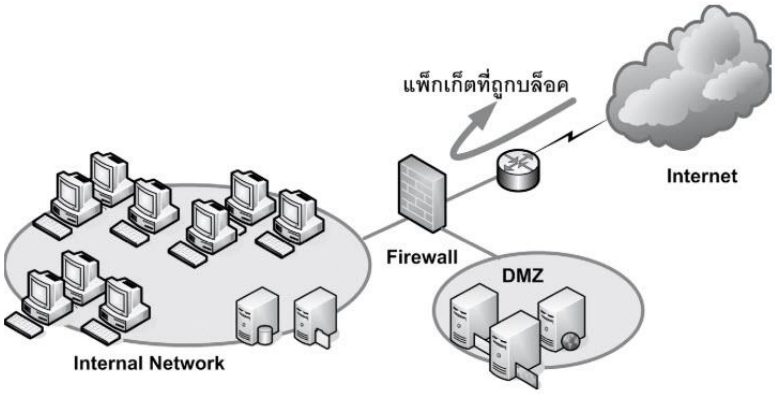
เนื่องจากภัยอันตรายนั้นมีรอบด้าน เราไม่สามารถที่จะใช้แค่เครื่องมือประเภทใดประเภทหนึ่งสำหรับการรักษาความปลอดภัยให้กับข้อมูลขององค์กรได้ เช่นกันเราก็ไม่สามารถใช้เครื่องมือการรักษาความปลอดภัยเพียงประเภทเดียวเพื่อป้องกันระบบคอมพิวเตอร์และเครือข่ายทั้งองค์กรได้ เราจำเป็นที่ต้องใช้ผลิตภัณฑ์หลายประเภทจากหลากหลายบริษัททำงานร่วมกันอย่างเป็นระบบเพื่อป้องกันและรักษาความปลอดภัย ต่อไปนี้เป็นตัวอย่างประเภทของเครื่องมือที่ใช้สำหรับระบบการรักษาความปลอดภัยให้กับระบบคอมพิวเตอร์และเครือข่าย

3.4.7.1 ไฟร์วอลล์ (Firewall)

ไฟร์วอลล์ (Firewall) เป็นระบบควบคุมการเข้าออกเครือข่าย ซึ่งจะใช้สำหรับปกป้องเครือข่ายภายในขององค์กรจากการโจมตีจากภายนอกได้ โดยปกติแล้วไฟร์วอลล์จะติดตั้งขวางกันระหว่างสองเครือข่ายซึ่งส่วนใหญ่เป็นการติดตั้งระหว่างอินเทอร์เน็ตและอินทราเน็ต ถ้าคอนฟิกอย่างถูกต้องแล้วก็เป็นสิ่งที่จำเป็นสำหรับองค์กร อย่างไรก็ตามไฟร์วอลล์ไม่สามารถที่จะป้องกันการโจมตีที่ใช้ช่องทางปกติที่เปิดไว้โดยไฟร์วอลล์ได้ ยกตัวอย่างเช่น สมมติว่าองค์กรมีเว็บเซิร์ฟเวอร์ติดตั้งไว้ใน DMZ หรือภายในเครือข่ายและอนุญาตให้เข้าถึงได้จากอินเทอร์เน็ต และถ้าเว็บเซิร์ฟเวอร์มีช่องโหว่และจุดอ่อนไฟร์วอลล์ก็จะไม่สามารถป้องกันการโจมตีเว็บเซิร์ฟเวอร์ได้ ถ้าผู้บุกรุกใช้ช่องทางเดียวกันกับการเข้ามาดูเว็บไซต์ นอกจากนี้ไฟร์วอลล์ไม่สามารถป้องกันการโจมตีจากภายในได้ เนื่องจากผู้ใช้ที่อยู่ภายในนั้นถ้าโจมตีคอมพิวเตอร์ที่อยู่ข้างในด้วยกันก็จะไม่ต้องผ่านไฟร์วอลล์

เหตุผลหลักที่มีการใช้ไฟร์วอลล์ (Firewall) ก็เพื่อให้ผู้ใช้ที่อยู่ภายในสามารถใช้บริการเครือข่ายภายในได้เต็มที่และใช้บริการเครือข่ายภายนอก เช่น อินเทอร์เน็ตได้ด้วย ในขณะที่ไฟร์วอลล์จะป้องกันไม่ให้ผู้ใช้ภายนอกเข้ามาใช้บริการเครือข่ายที่อยู่ข้างในได้ รูปที่ 3.18 แสดงการติดตั้งไฟร์วอลล์เพื่อเชื่อมต่อเครือข่ายองค์กรกับเครือข่ายอินเทอร์เน็ต จากรูปจะเห็นได้ว่าแพ็กเก็ตที่วิ่งระหว่างเครือข่ายภายในและอินเทอร์เน็ตต้องผ่านไฟร์วอลล์เท่านั้น ดังนั้น ไฟร์วอลล์จึงสามารถควบคุมการใช้เครือข่ายได้โดยอนุญาตหรือไม่อนุญาตให้แพ็กเก็ตผ่านได้ ซึ่งแพ็กเก็ตที่อนุญาตให้ผ่านหรือไม่นี้จะขึ้นอยู่กับนโยบายการรักษาความปลอดภัย (Security Policy) ไฟร์วอลล์เป็นระบบที่บังคับใช้นโยบาย

การรักษาความปลอดภัยระหว่างเครือข่าย โดยหลักการแล้วไฟร์วอลล์จะทำงานอยู่สองกลไกคือ การอนุญาตหรือไม่อนุญาตให้แพ็กเก็ตผ่าน



รูปที่ 3.18 ไฟร์วอลล์ (Firewall) [6]

ถ้าเครือข่ายองค์กรเชื่อมต่อโดยตรงกับอินเทอร์เน็ตโดยที่ไม่มีไฟร์วอลล์ ก็เป็นการเปิดช่องโหว่ให้เครือข่ายสามารถถูกโจมตีหรือบุกรุกได้อย่างง่ายดาย ตัวอย่างเช่น สมมติว่าเครือข่ายมีโฮสต์หรือเซิร์ฟเวอร์เป็นร้อยๆ เครื่อง ถ้าผู้บุกรุกเครือข่ายสามารถบุกรุกเข้าเครื่องใดเครื่องหนึ่งได้ ต่อไปก็ไม่เป็นการยากที่จะบุกรุกเข้าไปยังเครื่องอื่นๆ การติดตั้งไฟร์วอลล์จะเป็นการป้องกันผู้บุกรุกได้ในระดับหนึ่ง

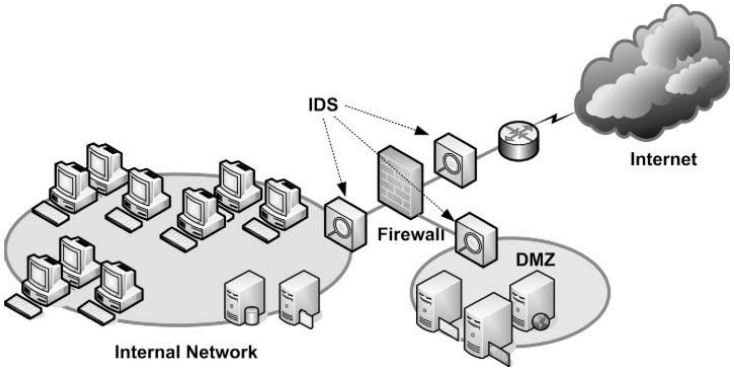
3.4.7.2 ระบบตรวจจับการบุกรุก (IDS)

ระบบตรวจจับการบุกรุกหรือ IDS (Intrusion Detection System) เป็นระบบที่ใช้สำหรับการเฝ้าระวังและแจ้งเตือนภัยถ้ามีการบุกรุกหรือมีสิ่งที่ผิดปกติเกิดขึ้นในระบบ บางระบบนั้นสามารถตรวจจับและหยุดการบุกรุกได้ อย่างไรก็ตามปัญหาของการโจมตีเครือข่ายนั้นก็คล้ายกับไวรัส เนื่องจากการโจมตีนั้นผู้บุกรุกจะพยายาโจมตีช่องโหว่หรือจุดอ่อนของระบบและเนื่องจากมีการค้นพบช่องโหว่หรือจุดอ่อนใหม่ๆ เป็นประจำ ดังนั้น IDS ก็จำเป็นที่ต้องอัพเดตข้อมูลนี้เช่นกัน ถ้ามีการติดตั้งและใช้งานอย่างถูกต้อง IDS ก็สามารถป้องกันการโจมตีได้ อย่างไรก็ตาม IDS ไม่สามารถตรวจจับความพยายามของผู้ใช้ที่ได้รับอนุญาต เข้าถึงไฟล์หรือใช้โปรแกรมที่ไม่ได้รับอนุญาตได้

ระบบตรวจจับการบุกรุก หรือ IDS เป็นเครื่องมือสำหรับการรักษาความปลอดภัยอีกประเภทหนึ่งที่ใช้สำหรับตรวจจับความพยายามที่จะบุกรุกเครือข่าย โดยระบบจะแจ้งเตือนผู้ดูแลระบบเมื่อการบุกรุกหรือพยายามที่จะบุกรุกเครือข่าย IDS นั้นไม่ใช่ระบบที่ใช้ป้องกันการบุกรุกแต่เป็นระบบที่คอยแจ้งเตือนภัยเท่านั้น ถ้าเปรียบกับระบบการรักษาความปลอดภัยของรถ IDS ก็อาจจะเปรียบได้กับระบบกันขโมย ซึ่งระบบนี้จะส่งสัญญาณเมื่อมีการตรวจพบความพยายามที่จะขโมยรถ เช่น การงัด

ประตูหรือกระจก แต่ระบบนี้จะไม่สามารถป้องกันไม่ให้ขโมยรถได้ อย่างไรก็ตามโดยธรรมชาติแล้วขโมยก็จะพยายามหลีกเลี่ยงรถที่ติดตั้งระบบนี้ ระบบเครือข่ายก็เช่นกัน ถ้ามีระบบตรวจจับและแจ้งเตือนการบุกรุกพวกแฮคเกอร์ก็จะหลีกเลี่ยงการบุกรุกเครือข่ายนี้

หน้าที่หลักของ IDS คือ แจ้งเตือนการเข้าใช้เครือข่ายที่ผิดปกติ สิ่งที่เป็นประเด็นสำคัญในการออกแบบระบบ IDS ก็คือ เหตุการณ์ใดคือสิ่งที่ถือว่าผิดปกติ ดังนั้น การใช้ IDS นั้นก็ขึ้นอยู่กับว่าอะไรที่จะแจ้งเตือนให้ทราบ คำตอบนั้นไม่ใช่แค่ถูกหรือผิด ขาวหรือดำ แต่จะขึ้นอยู่กับสภาวะของระบบในขณะนั้น



รูปที่ 3.19 Intrusion Detection System [6]

จากรูปที่ 3.19 โฮสต์เบสไอดีเอส (Host Based IDS) จะติดตั้งที่เครื่องเว็บเซิร์ฟเวอร์เพื่อตรวจจับความพยายามที่จะแฮคเว็บเซิร์ฟเวอร์เอง ส่วนเน็ตเวิร์คไอดีเอสนั้นจากรูปจะติดตั้งระหว่างเราท์เตอร์และไฟร์วอลล์เพื่อที่จะตรวจทราฟฟิกที่วิ่งเข้าออกระหว่างเครือข่ายและอินเทอร์เน็ต

3.4.7.3 ซอฟต์แวร์ป้องกันไวรัส

ปัจจุบันภัยคุกคามที่มีผลกระทบต่อองค์กรมากที่สุดคือ ไวรัส เวิร์ม และโทรจัน ซึ่งได้สร้างความเสียหายอย่างมากให้กับคอมพิวเตอร์และเครือข่ายที่เชื่อมต่อเข้ากับอินเทอร์เน็ต ดังนั้น การป้องกันและกำจัดไวรัสจึงเป็นสิ่งที่สำคัญในลำดับต้นๆ

ซอฟต์แวร์ป้องกันไวรัสเป็นสิ่งที่จำเป็นำหรับการป้องกันและรักษาความปลอดภัยให้กับคอมพิวเตอร์ ถ้ามีการติดตั้งและใช้งานอย่างถูกต้อง มันสามารถที่จะลดความเสี่ยงต่อโปรแกรมประสงค์ร้ายได้ อย่างไรก็ตามมันไม่สามารถที่จะป้องกันไวรัสได้ทุกชนิด เนื่องจากปัจจุบันจะมีไวรัสใหม่ๆ ออกมา การใช้งานซอฟต์แวร์ป้องกันไวรัสนั้นจำเป็นที่ต้องอัพเดตฐานไวรัสซิกเนเจอร์ (Virus Signature) เป็นประจำพร้อมทั้งสแกนระบบเป็นประจำเช่นกัน อย่างไรก็ตาม โปรแกรมป้องกันไวรัสนั้นไม่สามารถที่จะป้องกันผู้บุกรุกจากที่อื่นเจาะระบบเข้ามาแล้วรันโปรแกรมประสงค์ร้ายได้

นอกจากนี้โปรแกรมป้องกันไวรัสยังไม่สามารถป้องกันผู้ใช้ที่ได้รับอนุญาต แต่พยายามที่จะเข้าถึงไฟล์หรือโปรแกรมที่ไม่ได้รับอนุญาตได้

เมื่อไวรัสเข้าถึงเครื่องคอมพิวเตอร์ได้แต่ซอฟต์แวร์ป้องกันไวรัสต้องสามารถปกป้องระบบและข้อมูล พร้อมทั้งหยุดยั้งการแพร่กระจายไปยังเครื่องอื่นๆ ได้ การป้องกันนี้มีความสำคัญไม่น้อยไปกว่าการป้องกันเครือข่ายทั้งทางด้านฟิสิคอลและทางอิเล็กทรอนิกส์ เราควรออกแบบระบบป้องกันไวรัสของเครื่องไคลเอนท์โดยตั้งสมมติฐานว่า ไวรัสสามารถผ่านมาตรการป้องกันของเลเยอร์อื่นๆ ได้ การตั้งสมมติฐานแบบนี้จะทำให้สามารถป้องกันไวรัสได้ดีที่สุด

3.4.8 ทฤษฎีที่เกี่ยวข้อง [6]

จตุชัย แพงจันทร์และอนุโชต วุฒิพรพงษ์ (2551 : 4) อธิบายว่าถ้าคอมพิวเตอร์ทำงานเดี่ยว (Stand-Alone) ก็จะเหมือนกับการที่คน ๆ หนึ่งทำงานเพียงคนเดียว ซึ่งเป็นที่ทราบกันดีว่า การทำงานเพียงคนเดียวนั้นจะให้ผลลัพธ์ไม่ดีเท่าที่ควร การทำงานของมนุษย์นั้นต้องทำงานกันเป็นกลุ่มหรือทีมจึงจะมีประสิทธิภาพ คอมพิวเตอร์ก็เช่นกัน ควรจะทำงานเป็นกลุ่มหรือทีม ซึ่งการทำงานเป็นกลุ่มหรือทีมของคอมพิวเตอร์นี้จะเรียกกว่า เครือข่าย (Network)

3.4.8.1 <u>แบบอ้างอิงการบริหารเครือข่ายของ ISO</u>

องค์การมาตรฐานนานาชาติ ISO ได้กำหนดแบบอ้างอิงการบริหารเครือข่าย เพื่อเป็นแนวทางสำหรับการบริหารเครือข่ายอย่างเป็นระบบ ซึ่งแบบอ้างอิงประกอบด้วย 5 หัวข้อเรื่อง ดังนี้

- **การบริหารประสิทธิภาพ (Performance Management)**

จุดประสงค์หลักของการบริหารประสิทธิภาพของเครือข่าย ก็เพื่อให้อุปกรณ์เครือข่ายทำงานได้เต็มประสิทธิภาพและมีแบนด์วิธเพียงพอต่อความต้องการ การบริหารประสิทธิภาพของเครือข่ายนั้นจะเกี่ยวข้องกับการมอนิเตอร์ การประเมิน และการปรับค่าคอนฟิกต่างๆ เพื่อให้การใช้แบนด์วิธและทรัพยากรอื่นๆ มีประสิทธิภาพ ซึ่งจะเกี่ยวข้องกับการทำบัญชีคอมพิวเตอร์และอุปกรณ์เครือข่าย การตรวจวัด รายงาน วิเคราะห์ปริมาณการใช้งาน (Utilization) และอัตราส่งผ่านข้อมูล (Throughput) ของอุปกรณ์เครือข่ายต่างๆ เช่น ลิงค์ ฮับ สวิตช์ เราท์เตอร์ โฮสต์ และไฟร์วอลล์ เป็นต้น ไปจนถึงเส้นทางข้อมูลผ่านอุปกรณ์เครือข่ายต่าง ๆ

- **การบริหารข้อขัดข้อง (Fault Management)**

โดยทั่วไปอุปกรณ์เครือข่ายจะถูกเปิดทิ้งไว้ตลอดเวลา เพื่อให้บริการแก่ผู้ใช้ อุปกรณ์เครือข่ายที่เป็นฮาร์ดแวร์ไม่ว่าจะเป็นสวิตช์ เราท์เตอร์ เกตเวย์ ไฟร์วอลล์ ล้วนแล้วแต่มีอายุใช้งาน เมื่อใช้งานไปได้สักพักก็จะเสีย หรือแม้แต่สายสัญญาณก็อาจเสื่อมคุณภาพ หรืออาจโดนหนูแทะจนขาด ประเด็นคือสิ่งต่างๆ เหล่านี้มีโอกาสที่จะเกิดขึ้นแน่นอน และมีผลกระทบทำให้เครือข่ายใช้การไม่ได้ จุดประสงค์ของการบริหารข้อขัดข้องของเครือข่ายคือ มอนิเตอร์การเก็บล็อก (Log) การแจ้งเตือน การตรวจเช็ค

และการแก้ไขข้อผิดพลาดหรือข้อขัดข้องต่างๆ ที่เกิดขึ้นในเครือข่ายซึ่งขั้นตอนนี้จะมีบางส่วนที่คาบเกี่ยวกันกับการบริหารประสิทธิภาพของเครือข่าย แต่ข้อแตกต่างก็คือ การบริหารข้อขัดข้องนั้นจะเน้นที่การแก้ปัญหาหรือข้อขัดข้องของเครือข่ายได้อย่างรวดเร็ว ทันเวลา เช่น สายสัญญาณขาดสวิตช์เสีย และเราท์เตอร์เสีย เป็นต้น ในขณะที่การบริหารประสิทธิภาพนั้นจะเน้นที่ประสิทธิภาพการใช้งานของเครือข่ายโดยรวม

การบริหารข้อขัดข้องเครือข่ายคือ การเฝ้าระวัง ตรวจสอบ และแก้ปัญหาเครือข่าย เพื่อให้ระบบเครือข่ายทำงานได้อย่างมีประสิทธิภาพและต่อเนื่อง เนื่องจากข้อขัดข้องต่างๆ จะทำให้ระบบเครือข่ายล่มหรือหยุดชะงัก ซึ่งอาจมีผลกระทบร้ายแรงกับระบบต่างๆ ที่รันอยู่บนเครือข่าย ระบบบริหารเครือข่ายโดยส่วนใหญ่จึงหมายถึง ระบบบริหารข้อขัดข้องเครือข่ายนั่นเอง

ระบบบริหารเครือข่ายเป็นระบบที่ใช้สำหรับบริหารโครงสร้างเครือข่าย ซึ่งประกอบด้วยฮาร์ดแวร์ ซอฟต์แวร์หรืออุปกรณ์หลายยี่ห้อ โดยระบบนั้นจะคอยรับข้อความ แจ้งเหตุการณ์จากอุปกรณ์ในเครือข่าย นอกจากนี้ยังอาจกำหนดให้รับข้อความจากเซิร์ฟเวอร์หรืออุปกรณ์ในเครือข่ายที่สำคัญอย่างอื่นก็ได้ ต่อไปนี้เป็นฟังก์ชันที่สำคัญที่มีอยู่ในระบบบริหารเครือข่ายทั่วไป

- การค้นหาในเครือข่าย (Network Discovery)
- การสร้างผังเครือข่าย (Topology Mapping)
- การจัดการกับเหตุการณ์ (Event Handler)
- กราฟแสดงแบนด์วิธ CPU RAM หรือทรัพยากรที่สำคัญ

ระบบบริหารเครือข่ายเป็นระบบหลักที่ใช้สำหรับการเฝ้าระวัง และตรวจจับปัญหาข้อขัดข้องต่างๆ ที่เกิดขึ้นในเครือข่าย ความสามารถในการตรวจพบสาเหตุของปัญหาอย่างรวดเร็วเป็นสิ่งที่สำคัญอย่างยิ่ง ผู้ดูแลระบบอาจใช้แผนผังเครือข่ายที่มีภาพของอุปกรณ์ต่างๆ เชื่อมต่อกันเป็นเครือข่าย เพื่อเฝ้าดูการทำงานของอุปกรณ์ต่างๆ เหล่านั้นว่าปกติดีหรือไม่

- **การบริหารคอนฟิกกูเรชัน (Configuration Management)** การบริหารคอนฟิกกูเรชัน หมายถึง การบริหารค่าคอนฟิกกูเรชันของอุปกรณ์ในเครือข่าย เช่น หมายเลข IP แอดเดรส เวอร์ชันของซอฟต์แวร์ที่ใช้ในแต่ละเซิร์ฟเวอร์ ค่าคอนฟิกของเราท์เตอร์ สวิตช์ ผังการเชื่อมต่อของอุปกรณ์ต่างๆ เป็นต้น เนื่องจากเครือข่ายมีการเปลี่ยนแปลงตลอดเวลา เช่น การติดตั้งและคอนฟิกอุปกรณ์เครือข่ายใหม่ การออกแบบเครือข่ายใหม่เพื่อรองรับระบบหรือเทคโนโลยีใหม่ๆ เช่น ระบบเครือข่าย Wi-Fi การติดตั้งสายสัญญาณ การเพิ่มและลดเครื่องไคลเอนท์ในเครือข่าย ไม่ว่าจะเป็นเซิร์ฟเวอร์ พีซี โน้ตบุ๊ค แท็บเล็ต สมาร์ทโฟน เป็นต้น การจัดเก็บค่าคอนฟิกต่างๆ ของอุปกรณ์เครือข่าย เช่น สวิตช์ เราท์เตอร์ หรือไฟร์วอลล์ จะช่วยในการติดตั้งอุปกรณ์ใหม่ทดแทนของเก่าที่เสีย มีหลายหน่วยงานที่ไม่มีการบริหารจัดการในเรื่องพวกนี้ ทำให้เมื่ออุปกรณ์นั้นเสียและต้องซื้อเครื่องใหม่มาทดแทน ก็อาจต้องคอนฟิกค่าใหม่ แทนที่จะโหลดจากไฟล์คอนฟิกเก่าที่เก็บไว้ ซึ่งอาจทำให้เสีย

เวลานานเกินไปก็ได้นอกจากนี้การเก็บพวกเอกสารเกี่ยวกับเครือข่ายก็เป็นสิ่งที่สำคัญ เอกสารที่กล่าวถึงนี้รวมถึงพวกคู่มือการติดตั้งและใช้งานอุปกรณ์เครือข่ายต่างๆ เพราะเมื่อเวลาผ่านไปถึงแม้ผู้ดูแลระบบจะได้รับการฝึกอบรม แต่ถ้าไม่ได้ใช้งานบ่อยๆก็อาจลืมได้ ถ้าอุปกรณ์นั้นมีปัญหา อย่างน้อยก็มีเอกสารอ้างอิงหรือคู่มือที่ขั้นตอนการปฏิบัติที่ชัดเจน ซึ่งก็จะช่วยให้การแก้ปัญหาได้เร็วยิ่งขึ้น นอกจากนี้เอกสารเกี่ยวกับเครือข่ายอื่นๆ เช่น แผนผังเครือข่าย รวมถึงจุดติดตั้งอุปกรณ์ แนววางสายสัญญาณ รวมถึงประเภท ระยะทาง จำนวน แบบหัวเชื่อมต่อของสายสัญญาณก็จะมีประโยชน์อย่างมาก ในการวางแผนเพื่อขยายหรือปรับปรุงเครือข่ายในอนาคต ประเด็นที่สำคัญคือ อย่างน้อยต้องรู้ว่าปัจจุบันเรามีอะไรอยู่บ้าง

- **การบริหารบัญชีผู้ใช้ (Accounting Management)**

การบริหารบัญชีผู้ใช้ หมายถึง การควบคุมการใช้งานทรัพยากรเครือข่ายของผู้ใช้ ซึ่งอาจใช้เพื่อการเก็บค่าบริการฟังก์ชันอาจรวมถึงการจัดการบัญชีผู้ใช้ การพิสูจน์ทราบตัวตน การกำหนดสิทธิ์และการควบคุมการเข้าถึงทรัพยากรต่างๆ เป็นต้น การสามารถตรวจสอบได้ว่าใคร ทำอะไร ที่ไหน อย่างไร เมื่อไรในเครือข่ายนั้น ถือว่าเป็นสิ่งที่สำคัญอย่างยิ่ง โดยเฉพาะระบบเครือข่ายที่มีระบบสารสนเทศที่สำคัญ บัญชีผู้ใช้นั้นอาจถูกเก็บไว้ในระบบจัดการผู้ใช้ เช่น LDAP, AD หรือไดเร็คทอรีอื่นๆ ก็ได้ สิ่งที่สำคัญตามมาเกี่ยวกับผู้ใช้คือ รูปแบบการพิสูจน์ทราบตัวตน ซึ่งโดยส่วนใหญ่จะนิยมใช้รหัสผ่าน (Password) แต่ก็มีหลายหน่วยงานอาจใช้การพิสูจน์ทราบตัวตน 2 แบบ (Two Factor Authentication) เช่น การใช้ไบโอเมตริก หรือ One Time Password (OTP) เข้ามาช่วยสิ่งที่สำคัญอย่างหนึ่งเกี่ยวกับการบริหารผู้ใช้งานคือ การเก็บล็อกกิจกรรมต่างๆ ที่ผู้ใช้ทำในเครือข่าย การเก็บล็อกนอกจากจะเป็นการปฏิบัติตามกฎหมายคือ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 แล้วยังถือว่าเป็นสิ่งที่อาจช่วยในการช่วยตรวจสอบการกระทำต่างๆ ของผู้ใช้หรือแฮคเกอร์ที่อาจจะทำอะไรที่มีผลกระทบต่อเครือข่าย หรือข้อมูลขององค์กรก็ได้

- **การบริหารการรักษาความปลอดภัย (Security Management)**

การบริหารการรักษาความปลอดภัย หมายถึง การควบคุมการเข้าใช้ทรัพยากรเครือข่ายให้เป็นไปตามนโยบายที่ได้กำหนดไว้ เช่น การใช้ไฟร์วอลล์เพื่อควบคุมการเข้าใช้ทรัพยากรของระหว่างเครือข่าย การเข้ารหัสข้อมูล การแจกจ่ายคีย์ (Key Distribution) และการออกใบรับรอง (Certificate Authority) เป็นต้น การรักษาความปลอดภัยในเครือข่ายนั้นจะเริ่มต้นจากการบริหารบัญชีผู้ใช้งาน การเฝ้าระวังเหตุการณ์ต่างๆ ที่เกิดขึ้นในเครือข่าย ซึ่งรวมถึงการแพร่ระบาดของไวรัสหรือมัลแวร์ การโจมตีเครือข่ายจากแฮคเกอร์ทั้งนอกและในเครือข่าย การติดตั้งอุปกรณ์ด้วยการรักษาความปลอดภัยเพื่อตรวจจับและป้องกันปัญหาต่างๆ เหล่านี้ เช่น IPS/IDS SEM/SEIM UTM VPN Firewall เป็นต้น บางหน่วยงานนั้นให้ความสำคัญอย่างมากกับการรักษาความปลอดภัยในเครือข่าย เนื่องจากในเครือข่ายนั้นอาจมีระบบสารสนเทศที่สำคัญอย่างยิ่งต่อองค์กร โดยหน่วยงานเหล่านี้อาจตั้ง Security

Operation Center (SOC) ทำงานควบคู่ไปกับ Network Operation Center (NOC) โดยที่ SOC นั้นจะรับผิดชอบงานด้านการรักษาความปลอดภัย ในขณะที่ NOC นั้นก็จะดูแลในส่วนของการดูแลเครือข่ายทั่วไป SOC นั้นจะมีระบบที่สำคัญคือ Security Event and Incident Management (SIEM) ซึ่งเป็นระบบที่รับข้อมูลล็อกจากอุปกรณ์ต่างๆ ในเครือข่ายมาวิเคราะห์และประมวลผลในเรื่องที่เกี่ยวกับการรักษาความปลอดภัยในเครือข่าย

บทที่ 4
เทคนิคและขั้นตอนการปฏิบัติงาน

การตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่ายเบื้องต้นสำหรับผู้ดูแลระบบ สำนักดิจิทัลเทคเทคโนโลยี มหาวิทยาลัยศิลปากร มีเทคนิคและขั้นตอนการปฏิบัติงาน ดังนี้

4.1 มาตรฐานการปฏิบัติงาน

4.2 ขั้นตอนการปฏิบัติงาน

4.3 วิธีการติดตามและประเมินผลการปฏิบัติงาน

4.1 มาตรฐานการปฏิบัติงาน

ผู้เขียนคู่มือใช้หลักการทำงาน และแนวทางการปฏิบัติงานเป็นมาตรฐานในการปฏิบัติงาน ดังนี้

4.1.1 หลักการทำงาน

คู่มือการตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่ายสำหรับผู้ดูแลระบบ เล่มนี้เป็นการให้บริการและสนับสนุนการจัดการเรียนการสอน เพื่ออำนวยความสะดวกให้กับบุคลากรและนักศึกษามหาวิทยาลัยศิลปากร ซึ่งมีมาตรฐานการปฏิบัติงานอาศัยหลักการทำงานตามสมรรถนะในการปฏิบัติงานและความเชี่ยวชาญเฉพาะด้าน เพื่อประกอบการตัดสินใจ ดังนี้

1. ปฏิบัติงานตามกฎ ระเบียบและข้อบังคับที่เกี่ยวข้อง และหลีกเลี่ยงการกระทำใด ๆ ที่อาจทำให้เกิดความเสื่อมเสียแก่องค์กร

2. มีความโปร่งใส ในการปฏิบัติงานให้เห็นถึงการปฏิบัติงานตามกฎ ระเบียบ ข้อบังคับ และมติต่าง ๆ ของมหาวิทยาลัย

3. ไม่ปกปิดข้อเท็จจริงหรือบิดเบือนความจริงอันเป็นสาระสำคัญ ซึ่งสามารถติดตามและตรวจสอบได้ตามกฎหมายเกี่ยวกับข้อมูลข่าวสารของราชการ

4. ความซื่อสัตย์ สุจริต ประพฤติตนสอดคล้องตามจรรยาบรรณของบุคลากรที่มหาวิทยาลัยกำหนด

5. การปฏิบัติงานต้องมีประสิทธิภาพ ลดขั้นตอนการปฏิบัติงาน ถูกต้อง รวดเร็ว สอดคล้องกับเป้าหมายของมหาวิทยาลัย

6. การประสานงานในภาระงานที่รับผิดชอบได้อย่างมีประสิทธิภาพ การทำงานเป็นทีม และสร้างเครือข่ายภายในองค์กร

7. การปฏิบัติงานคำนึงถึงผลประโยชน์ของมหาวิทยาลัย และการประหยัดทรัพยากร

4.1.2 แนวทางการปฏิบัติงาน

นอกจากหลักการทำงานแล้ว ยังได้ใช้สมรรถนะในการปฏิบัติงานและประสบการณ์ในการทำงานมากำหนดแนวทางการปฏิบัติงานของบุคลากร ตามภาระงานของสำนักดิจิทัลเทคโนโลยี มหาวิทยาลัยศิลปากร ดังตารางที่ 4.1

ตารางที่ 4.1 สมรรถนะและมาตรฐานในการปฏิบัติงาน

สมรรถนะในการปฏิบัติงาน	มาตราฐานการปฏิบัติงาน
การมุ่งผลสัมฤทธิ์	1. มีความรู้ ความสามารถในหน้าที่รับผิดชอบอย่างสูง และบริการเหนือความคาดหมาย มีแหล่งข้อมูลใช้อ้างอิงส่งผลต่อความพึงพอใจของผู้รับบริการ 2. มีความตั้งใจ มีความขยัน หมั่นเพียร และมุ่งมั่นในการปฏิบัติงานที่รับผิดชอบให้สำเร็จตามเป้าหมาย และมีผลสัมฤทธิ์ในการปฏิบัติงานตามที่ได้รับมอบหมาย 3. พัฒนาและปรับปรุงแผนการปฏิบัติงานให้สอดคล้องกับผลงานให้มีคุณภาพตามแผนยุทธศาสตร์ของหน่วยงานและมหาวิทยาลัย

ตารางที่ 4.1 สมรรถนะและมาตรฐานในการปฏิบัติงาน (ต่อ)

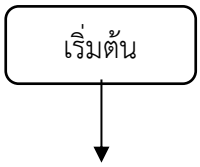
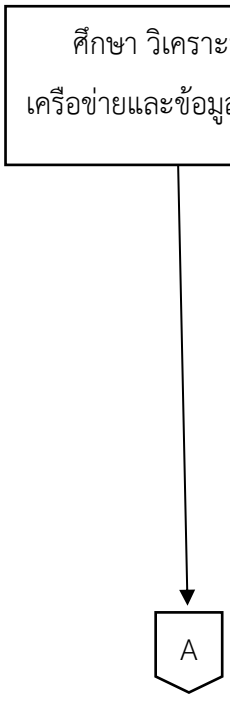
สมรรถนะในการปฏิบัติงาน	**มาตราฐานการปฏิบัติงาน**
ความเข้าใจองค์กรและระบบงาน	1. มีความเข้าใจองค์กร คน ระบบงาน และวัฒนธรรมองค์กรในภาพรวมและมีความสามารถในการสร้างความเชื่อมโยงระหว่างระบบงานและโดยการใช้เทคโนโลยี และเรียนรู้วิธีการปฏิบัติงานและสามารถแก้ปัญหาข้อบกพร่องที่เกิดขึ้น 2. มีมาตรฐานในการปฏิบัติงานสอดคล้องปรัชญา ปณิธาน วิสัยทัศน์ พันธกิจ และค่านิยมขององค์กร 3. มีการยอมรับในการเปลี่ยนแปลงที่จะเกิดขึ้นในองค์กร เช่น การเปลี่ยนโครงสร้างองค์กร ระบบงาน และการปรับเปลี่ยนกระบวนงาน เป็นต้น
การทำงานเป็นทีม	1. มีความสามารถในการทำงานเป็นทีมได้ (Team Work) 2. มีความพึงพอใจในหน้าที่ของตนที่ได้รับมอบหมายจากทีมได้อย่างมีความสุข 3. สร้างและประสานงานระหว่างทีมในกลุ่มภารกิจให้บรรลุเป้าหมายและมีประสิทธิภาพ
การมีคุณธรรม จริยธรรม และจรรยาบรรณ	1. ปฏิบัติหน้าที่ความรับผิดด้วยความโปร่งใส มีความซื่อสัตย์สุจริต 2. มีการอุทิศเวลาแก่ราชการ มีความภาคภูมิใจในสถาบันตนเอง 3. มุ่งส่งเสริมการปฏิบัติงานในหน่วยงานและมหาวิทยาลัยให้บรรลุวัตถุประสงค์และเป้าหมาย

4.2 ขั้นตอนการปฏิบัติงาน

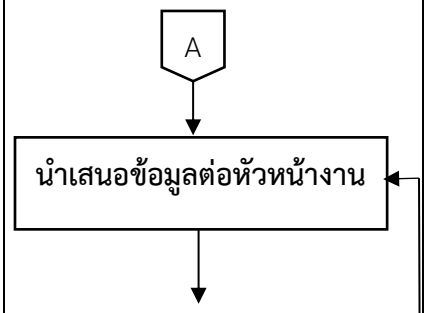
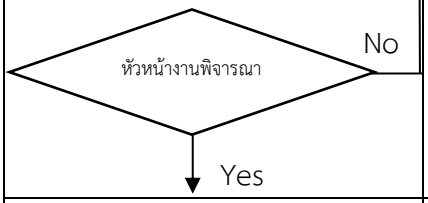
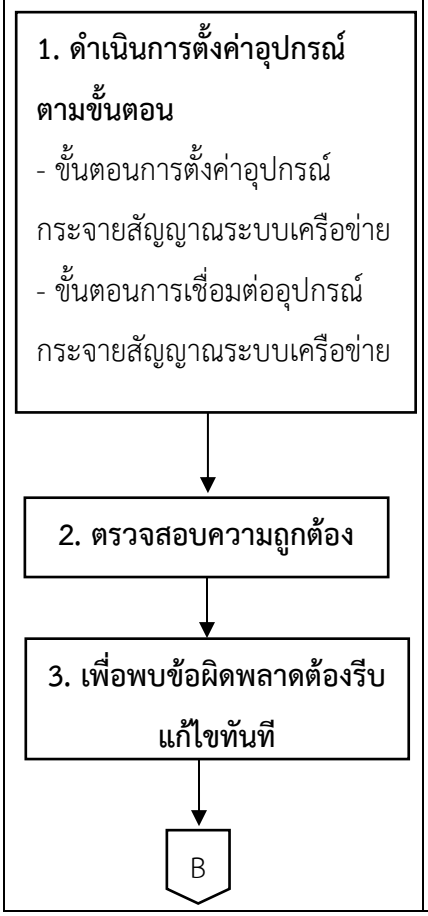
เพื่อให้การปฏิบัติงานการตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่ายสำหรับผู้ดูแลระบบ ผู้เขียนคู่มือขอนำเสนอขั้นตอนในการปฏิบัติงานด้านการตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่าย ที่เป็นภาระงานที่เชื่อมโยงและสอดคล้องกันทั้ง 2 ขั้นตอนการปฏิบัติงานเป็น 2 รูปแบบ คือ รูปแบบผังงานของการปฏิบัติงาน (Flow Chart) และรูปแบบข้อความ (Wording) ตามรายละเอียดดังนี้

4.2.1 ขั้นตอนการปฏิบัติงานการตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่ายเบื้องต้นสำหรับผู้ดูแลระบบ รูปแบบผังงานของการปฏิบัติงาน (Flow Chart)

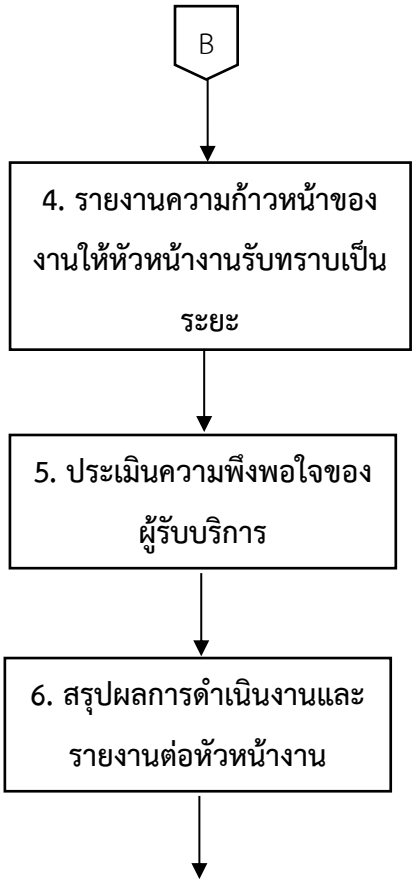
ตารางที่ 4.2 รูปแบบแผนผังของการปฏิบัติงาน (Flow Chart)

ผังกระบวนงาน	รายละเอียดงาน	ผู้รับผิดชอบ
	จุดเริ่มต้นขั้นตอน	ผู้ปฏิบัติงาน
	1. ศึกษา รวบรวม ความต้องการใช้บริการระบบเครือข่าย เป้าหมายและข้อจำกัดทางเทคนิค รูปแบบการเชื่อมต่อระบบเครือข่าย 2. ศึกษาข้อมูลรายละเอียดคุณสมบัติของอุปกรณ์กระจายสัญญาณระบบเครือข่าย ที่เลือกนำมาใช้งานจริง 3. รวบรวมข้อมูลที่ได้จากศึกษา และวิเคราะห์แล้วนำมาออกแบบระบบเครือข่ายให้ตรงกับความต้องการ 4. ศึกษาข้อมูลวิธีการตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่าย 5. ศึกษาระบบเฝ้าระวังและติดตามสถานะระบบบเครือข่าย	ผู้ปฏิบัติงาน

ตารางที่ 4.2 รูปแบบแผนผังของการปฏิบัติงาน (Flow Chart) (ต่อ)

ผังกระบวนงาน	รายละเอียดงาน	ผู้รับผิดชอบ
	จัดทำข้อมูลเบื้องต้นเพื่อเสนอต่อหัวหน้างาน และกำหนดขั้นตอน และระยะเวลาการดำเนินการที่ชัดเจน	ผู้ปฏิบัติงาน
	หัวหน้างานพิจารณาเห็นชอบตามเสนอ	หัวหน้างาน
	1. ดำเนินการตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่าย มีขั้นตอน ดังนี้ - ขั้นตอนการตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่ายแต่ละส่วน - ขั้นตอนการเชื่อมต่ออุปกรณ์กระจายสัญญาณระบบเครือข่ายทั้งระบบเพื่อทดสอบใช้งานจริง 2. ตรวจสอบความถูกต้องของข้อมูลการตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่ายให้ครบถ้วน 3. เมื่อพบข้อผิดพลาดต้องรีบแก้ไขทันที	ผู้ปฏิบัติงาน

ตารางที่ 4.2 รูปแบบแผนผังของการปฏิบัติงาน (Flow Chart) (ต่อ)

ผังกระบวนงาน	รายละเอียดงาน	ผู้รับผิดชอบ
	4. รายงานความก้าวหน้าของงานให้หัวหน้างานรับทราบเป็นระยะ 5. ประเมินความพึงพอใจของผู้รับบริการ 6. สรุปผลการดำเนินงานและรายงานต่อหัวหน้างาน	ผู้ปฏิบัติงาน
จุดสิ้นสุด	จุดสิ้นสุด	

4.2.2 ขั้นตอนการปฏิบัติงานการตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่ายเบื้องต้นสำหรับผู้ดูแลระบบ รูปแบบข้อความ (Wording) เป็นการบรรยายหรืออธิบายขั้นตอนการดำเนินงานด้วยข้อความตัวอักษร ดังนั้นสามารถแบ่งการดำเนินงานออกเป็นขั้นตอนต่าง ๆ ได้ดังต่อไปนี้

1) ขอบเขตการดำเนินการโครงการ

- การตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่ายเบื้องต้นสำหรับผู้ดูแลระบบกรณีศึกษาหอพักนักศึกษา สนามจันทร์ จำนวน 6 หอพัก

- ออกแบบและตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่าย เพื่อให้บริการระบบเครือข่ายไร้สายภายในหอพักแก่นักศึกษาและบุคลากรสำหรับการเรียนการสอน

- ออกแบบและตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่าย เพื่อให้บริการ ระบบเครือข่ายสาย LAN สำหรับเครื่องคอมพิวเตอร์เจ้าหน้าที่หอพักและอุปกรณ์เครือข่ายของหอพัก เช่น ระบบประตู Key card หรือภาระกิจอื่นๆ ของมหาวิทยาลัย

2) วิเคราะห์ประเมินความต้องการระบบเครือข่าย

- เก็บรวบรวมความต้องการจากนักศึกษาและเจ้าหน้าที่แต่ละหอพัก เพื่อนำมาเป็นข้อมูลสำหรับการออกแบบระบบเครือข่ายให้เหมาะสมกับความต้องการ

- ระบบเครือข่ายสามารถรองรับการใช้งานตลอด 24 ชั่วโมง

- ระบบเครือข่ายมีความมั่นคงปลอดภัยจากการใช้งานระบบเครือข่าย สามารถตรวจสอบและป้องกันผู้บุกรุกทั้งจากอินเทอร์เน็ตและจากผู้ใช้งานภายในระบบเครือข่ายได้

- นักศึกษาและบุคลากรต้องมีการพิสูจน์ตัวตนผ่านระบบ Single Sign-On (SSO) ของมหาวิทยาลัยศิลปากรก่อนเข้าใช้งานระบบเครือข่าย

- มีระบบบริหารจัดการจากศูนย์กลาง สามารถตรวจสอบสถานะของอุปกรณ์และสามารถจัดการตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่ายได้

- สามารถให้บริการระบบเครือข่ายไร้สายของเครือข่ายเอกชน เช่น Ais-WiFi , Dtac-WiFi และ True-WiFi ผ่านอุปกรณ์กระจายสัญญาณไร้สายของมหาวิทยาลัยได้

- มีระบบไฟฟ้าสำรองให้กับอุปกรณ์เครือข่ายทุกหอพัก เพื่อป้องกันความเสียจากระบบไฟฟ้าขัดข้อง

- สามารถเพิ่มขยายระบบเครือข่ายได้ เพื่อให้สามารถรองรับการเพิ่มขึ้นผู้ใช้งานและแอพพลิเคชันใหม่ในอนาคต

3) การเลือกเทคโนโลยีเครือข่าย

หลังจากที่ได้วิเคราะห์ระบบและประเมินความต้องการขององค์กรเกี่ยวกับการใช้เครือข่ายแล้ว ผู้ออกแบบก็พร้อมที่จะเริ่มลงมือออกแบบเครือข่ายได้เหมาะสมกับความต้องการ ผู้ออกแบบได้พิจารณาความต้องการแบนด์วิธของเครือข่ายก่อน โดยเลือกใช้เทคโนโลยีเครือข่าย LAN แบบกิกะบิตอีเธอร์เน็ตร่วมกับระบบเครือข่ายไร้สายหรือ Wireless LAN รูปแบบอินฟราสตัคเจอร์ ภายในหอพัก เพื่อให้รองรับการเรียนการสอนผ่านระบบ Online เนื่องจากสถานการณ์โรคโควิด-19 กำลังแพร่ระบาด ทำให้มีต้องการระบบเครือข่ายแบนด์วิธสูงขึ้น โดยมีรายละเอียดการเชื่อมต่อเครือข่าย ดังนี้

1. เทนกิกะบิตอีเธอร์เน็ต (10 GE) ทำหน้าที่ เป็นเส้นทางเชื่อมต่อระบบเครือข่ายหลักจาก Core Switch จากสำนักดิจิทัลเทคโนโลยี มายัง -> ศูนย์หอพักนักศึกษา (Node_Phetcharat) เป็นโหนดเชื่อมระบบเครือข่ายไปยัง 6 หอพัก

2. ศูนย์หอพักนักศึกษา (Node_Phetcharat) เชื่อมต่อระบบเครือข่ายไปยังหอพัก 1 – 6 ด้วยเชื่อมต่อในรูปแบบ Link Aggregation โดยใช้สาย Fiber optic ชนิด Multi mode (M/M) จำนวน 2 คู่ (2 Gbps) ของเดิมที่ใช้งานอยู่ทำให้สามารถเพิ่มขนาดแบนด์วิธจากเดิม 1 Gbps เป็น 2 Gbps ช่วยลดปัญหาคอขวดของเครือข่าย และทำหน้าที่เป็นเส้นทางสำรองด้วยหากสาย Fiber optic ขาดไปหนึ่งเส้นทาง ระบบเครือข่ายก็ยังสามารถใช้งานได้

3. ระบบเครือข่ายภายในหอพัก 1 - 6 เป็นแบบกิกะบิตอีเธอร์เน็ต โดยเชื่อมต่อจาก Switch ของหอพักด้วยสาย UTP CAT6 ไปยังอุปกรณ์กระจายสัญญาณระบบเครือข่ายไร้สายและเครื่องคอมพิวเตอร์เจ้าหน้าที่หอพักและระบบประตูคีย์การ์ด เข้า-ออก หอพัก

4) การออกแบบเครือข่ายแบบระบบเครือข่ายแบบลำดับชั้น

การออกแบบเครือข่าย กรณีศึกษาหอพักนักศึกษา สนามจันทร์ ใช้หลักการออกแบบระบบเครือข่ายแบบลำดับชั้น (Hierarchical Network) หมายถึง การออกแบบโดยจัดกลุ่มอุปกรณ์ในเครือข่ายเป็นหลายๆ กลุ่ม โดยเชื่อมต่อกันเป็นลำดับชั้นหรือเลเยอร์โดยเลเยอร์หลักประกอบด้วย 3 เลเยอร์ คือ

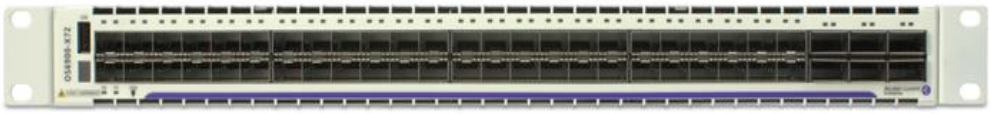
1. คอร์เลเยอร์ (Core Layer) เป็นกลุ่มอุปกรณ์หลักในเครือข่ายที่เชื่อมต่อกันด้วยความเร็วสูงหรือแบนด์วิธสูงมาก สามารถส่งผ่านแพ็กเก็ตข้อมูลผ่านเครือข่ายได้อย่างรวดเร็ว คอร์เลเยอร์หรืออาจเรียกว่า แบ็คโบน (Backbone) ของเครือข่ายก็ได้ เป็นเครือข่ายที่มีความสำคัญอย่างยิ่งต่อประสิทธิภาพโดยรวมของระบบเครือข่าย ติดตั้งอยู่ที่สำนักดิจิทัลเทคโนโลยี ทำหน้าที่ เชื่อมต่อระบบเครือข่ายหลักทั้งมหาวิทยาลัย ในที่นี้ได้เชื่อมต่อระบบเครือข่ายไปยัง Node หอพักเพชรรัตน์ด้วยความเร็ว 10 Gbps

2. ดิสทริบิวชันเลเยอร์ (Distribution Layer) จะมีการควบคุมการเข้าถึงรีซอร์สที่อยู่ทางฝั่งคอร์เลเยอร์ ซึ่งก็จะมีการขยายแบนด์วิธโดยเชื่อมต่ออัพลิงค์โดยใช้ 2 พอร์ต ซึ่งเรียกว่า การทำพอร์ตทรั้งกิ้ง (Port Trunking) ซึ่งก็จะทำให้แบนด์วิธขยายเพิ่มเป็น 2 เท่านั่นเอง ในกรณีศึกษานี้คือ Switch ของ Node หอพัก ทำหน้าที่ เชื่อมต่อระบบเครือข่ายด้วยความเร็ว 1 x 2 Gbps ไปยัง 6 หอพัก

3. แอ็กเซสเลเยอร์ (Access Layer) จะเป็นการควบคุมให้ทราฟฟิกที่เป็นโลคอลให้วิ่งอยู่ในเฉพาะวงเครือข่ายนั้นๆ นอกจากนี้เลเยอร์นี้ยังเป็นจุดที่จะควบคุมการเข้าถึงเครือข่ายของไคลเอนท์หรือผู้ใช้ด้วย อุปกรณ์ที่อยู่ในเลเยอร์นี้จะเป็น L2 สวิตช์ และใช้ VLAN ในการแบ่งกลุ่มของ LAN กำหนดให้มีหมายเลขไอพีคนละซับเน็ตกัน และทำหน้าที่เป็นอุปกรณ์เครือข่ายที่เชื่อมต่ออุปกรณ์ปลายทาง เช่น Access point เครื่องคอมพิวเตอร์เจ้าหน้าที่หอพัก และระบบประตูคีย์การ์ด

5) วิเคราะห์ความต้องการอุปกรณ์กระจายสัญญาณเครือข่าย

คุณสมบัติอุปกรณ์กระจายสัญญาณเครือข่ายหลัก Core Switch



Feature/Model	OS6900-X20	OS6900-T20	OS6900-X72	OS6900-V72	OS6900-C32
Port count	20 (SFP+)	20 (10Gbase-T)	72 (48 SFP+ and 6 QSFP)	72 (48 SFP28 and 6 QSFP28))	32 (QSFP28)
Expansion slots	1	1	N/A	N/A	N/A
Out-of-band Ethernet port	1	1	1	1	1
USB port	1	1	1	1	1
Console port	1	1	1	1	1
Primary slide-in PSU slot	1	1	1	1	1
Backup slide-in PSU slot	1	1	1	1	1
Redundant fans	3+1	3+1	1	1	5+1
Flash	2 GB	2 GB	3+1	5+1	16 GB
RAM	2 GB	4 GB	4 GB	16 GB	16 GB
Data buffer	9 MB	9 MB	8 GB	16 GB	16 MB
Max switching	640 Gb/s	640 Gb/s	12 MB	16 MB	6.4 Tb/s
Capacity	Non-blocking	Non-blocking	1.44 Tb/s	3.6 Tb/s	Non-blocking
Forwarding rate*	625 Mpps	625 Mpps	Non-blocking	Non-blocking	4761 Mpps

รูปที่ 4.1 Core Switch Alcatel 6900-X72 [7]

- เป็นอุปกรณ์เครือข่าย Layer 3 Switch
- มีช่องเชื่อมต่อไม่น้อยกว่า 48 ช่อง
- รองรับการเชื่อมต่อแบบ 40GE/10GE และ 1 Gigabit Ethernet
- มีพอร์ตการเชื่อมต่อ SFP+ 1GE/10 Gigabit Ethernet อย่างน้อย 48 พอร์ต
- มีพอร์ตการเชื่อมต่อ QSFP+ 40 Gigabit Ethernet อย่างน้อย 6 พอร์ต
- มีพอร์ต Console สำหรับการเชื่อมต่อ Configuration
- มีแหล่งจ่ายไฟ 2 ชุด Redundant power supply

- รองรับการทำงาน Data Center Networking โดยรองรับโปรโตคอล 802.1aq Shortest Path Bridging (SPB)
- สามารถกำหนดการเชื่อมต่อระหว่างอุปกรณ์แบบ Link Aggregation
- สนับสนุการใช้งาน Quality of Service (QoS), Access Control List, SNMPV1- 3 , Port-Security
- รองรับการทำงาน Layer-3 routing and multicast ทั้งแบบ IPv4/IPv6 routing และ IPv4/IPv6 multicast

คุณสมบัติอุปกรณ์กระจายสัญญาณเครือข่าย Distribution Layer [9]

รูปที่ 4.2 Distribution Layer Switch Alcatel6860E-U28 [9]

- เป็นอุปกรณ์เครือข่าย Layer 3 Switch
- มีช่องเชื่อมต่อไม่น้อยกว่า 28 ช่อง
- รองรับการเชื่อมต่อแบบ 20G/10G และ 1 Gigabit Ethernet
- มีพอร์ตการเชื่อมต่อ QSFP+ VFL ports 20 Gigabit Ethernet อย่างน้อย 2 พอร์ต
- มีพอร์ตการเชื่อมต่อ SFP+ 1G/10 Gigabit Ethernet อย่างน้อย 4 พอร์ต
- มีพอร์ตการเชื่อมต่อ SFP 1 Gigabit Ethernet อย่างน้อย 28 พอร์ต
- มีพอร์ต Console สำหรับการเชื่อมต่อ Configuration
- รองรับจำนวน Mac Address ไม่ต่ำกว่า 48,000 Mac Address

- สามารถกำหนดกลุ่มผู้ใช้งาน (VLAN) ได้ไม่น้อยกว่า 4,000 VLAN
- สามารถกำหนดเกาเชื่อมต่อระหว่างอุปกรณ์แบบ Link Aggregation
- สนับสนุการใช้งาน Quality of Service (QoS), Access Control List , SNMPV1-3, Port-Security
- รองรับการทำงาน Layer-3 routing and multicast ทั้งแบบ IPv4/IPv6 routing และ IPv4/IPv6 multicast

คุณสมบัติอุปกรณ์กระจายสัญญาณเครือข่าย Access Switch

รูปที่ 4.3 Access Switch Aruba 6100 [11]

- อุปกรณ์เครือข่าย Layer 2 Switch
- มีช่องเชื่อมต่อไม่น้อยกว่า 24 ช่อง
- รองรับการเชื่อมต่อแบบ Gigabit Ethernet 24 x ports 10/100/1000
- พอร์ตการเชื่อมต่อ SFP อย่างน้อย 4 พอร์ต 1GE/10GE
- มีพอร์ต Console สำหรับการเชื่อมต่อ Configuration
- สามารถกำหนดกลุ่มผู้ใช้งาน (VLAN) ได้ไม่น้อยกว่า 4,000 VLAN
- สามารถกำหนเกาเชื่อมต่อระหว่างอุปกรณ์แบบ Link Aggregation
- สนับสนุการใช้งาน Quality of Service (QoS), Port-Security , Access Control List , SNMPV1-3

6) กำหนด VLAN และหมายเลข IP Address ของระบบเครือข่าย ทั้ง 6 หอพัก

ตารางที่ 4.3 กำหนด VLAN เลข IP Address ของระบบเครือข่าย

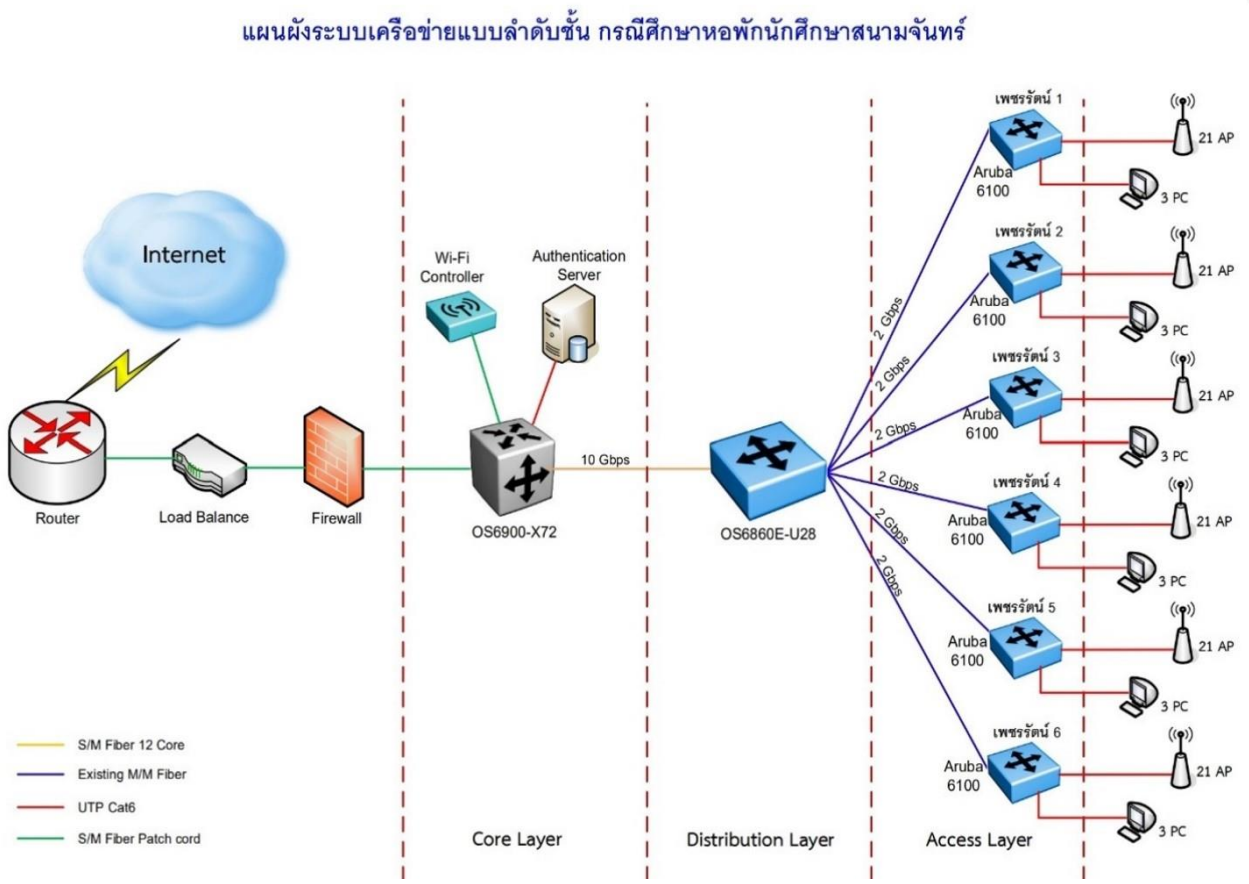
หอพัก	VLAN name	VLAN id	IP Address	Sub net	Gateway
เพชรรัตน์ 1	PR1_Lan	1581	172.27.58.18-30	255.255.255.224	172.27.58.1
	PR1_Device	1591	172.27.59.2-30	255.255.255.224	172.27.59.1
	PR1_suroam				
	PR1_suwifi		Tagged VLAN SSID ต่างๆ มาจาก Core switch		
	Ais-WiFi		ได้รับ IP Address อัตโนมัติจาก DHCP Server		
	Dtac-WiFi				
	True-WiFi				
เพชรรัตน์ 2	PR2_Lan	1582	172.27.58.34-46	255.255.255.224	172.27.58.33
	PR2_Device	1592	172.27.59.34-62	255.255.255.224	172.27.59.33
	PR2_suroam				
	PR2_suwifi		Tagged VLAN SSID ต่างๆ มาจาก Core switch		
	Ais-WiFi		ได้รับ IP Address อัตโนมัติจาก DHCP Server		
	Dtac-WiFi				
	True-WiFi				
เพชรรัตน์ 3	PR3_Lan	1583	172.27.58.50-62	255.255.255.224	172.27.58.65
	PR3_Device	1593	172.27.59.66-94	255.255.255.224	172.27.59.65
	PR3_suroam				
	PR3_suwifi		Tagged VLAN SSID ต่างๆ มาจาก Core switch		
	Ais-WiFi		ได้รับ IP Address อัตโนมัติจาก DHCP Server		
	Dtac-WiFi				
	True-WiFi				

ตารางที่ 4.3 กำหนด VLAN และหมายเลข IP Address ของระบบเครือข่าย (ต่อ)

หอพัก	VLAN name	VLAN id	IP Address	Sub net	Gateway
เพชรรัตน์ 4	PR4_Lan	1584	172.27.58.66-78	255.255.255.224	172.27.58.97
	PR4_Device	1594	172.27.59.98-126	255.255.255.224	172.27.59.97
	PR4_suroam				
	PR4_suwifi		Tagged VLAN SSID ต่างๆ มาจาก Core switch		
	Ais-WiFi		ได้รับ IP Address อัตโนมัติจาก DHCP Server		
	Dtac-WiFi				
	True-WiFi				
เพชรรัตน์ 5	PR4_Lan	1585	172.27.58.82-94	255.255.255.224	172.27.58.129
	PR4_Device	1595	172.27.59.130-158	255.255.255.224	172.27.59.129
	PR4_suroam				
	PR4_suwifi		Tagged VLAN SSID ต่างๆ มาจาก Core switch		
	Ais-WiFi		ได้รับ IP Address อัตโนมัติจาก DHCP Server		
	Dtac-WiFi				
	True-WiFi				
เพชรรัตน์ 6	PR4_Lan	1586	172.27.58.98-110	255.255.255.224	172.27.58.161
	PR4_Device	1596	172.27.59.162-190	255.255.255.224	172.27.59.161
	PR4_suroam				
	PR4_suwifi		Tagged VLAN SSID ต่างๆ มาจาก Core switch		
	Ais-WiFi		ได้รับ IP Address อัตโนมัติจาก DHCP Server		
	Dtac-WiFi				
	True-WiFi				

กำหนด VLAN และหมายเลข IP Address ของระบบเครือข่ายกรณีศึกษาหอพักนักศึกษา สนามจันทร์ ดังตารางที่ 4.3 ทางผู้จัดทำได้ออกแบบ VLAN IP Addess SubNet Gateway ทั้ง 6 หอพัก หัวใจสำคัญที่จะทำให้ระบบเครือข่ายแต่ละหอพักสามารถใช้งานได้ตามวัตถุประสงค์ได้นั้น ผู้ดูและระบบเครือข่ายต้องดำเนินการตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่ายแต่ละลำดับชั้นให้ถูกต้องครบถ้วน จึงทำให้ระบบเครือข่ายสามารถให้บริการได้อย่างมีประสิทธิภาพ

7) แผนผังการออกแบบโครงสร้างระบบเครือข่าย

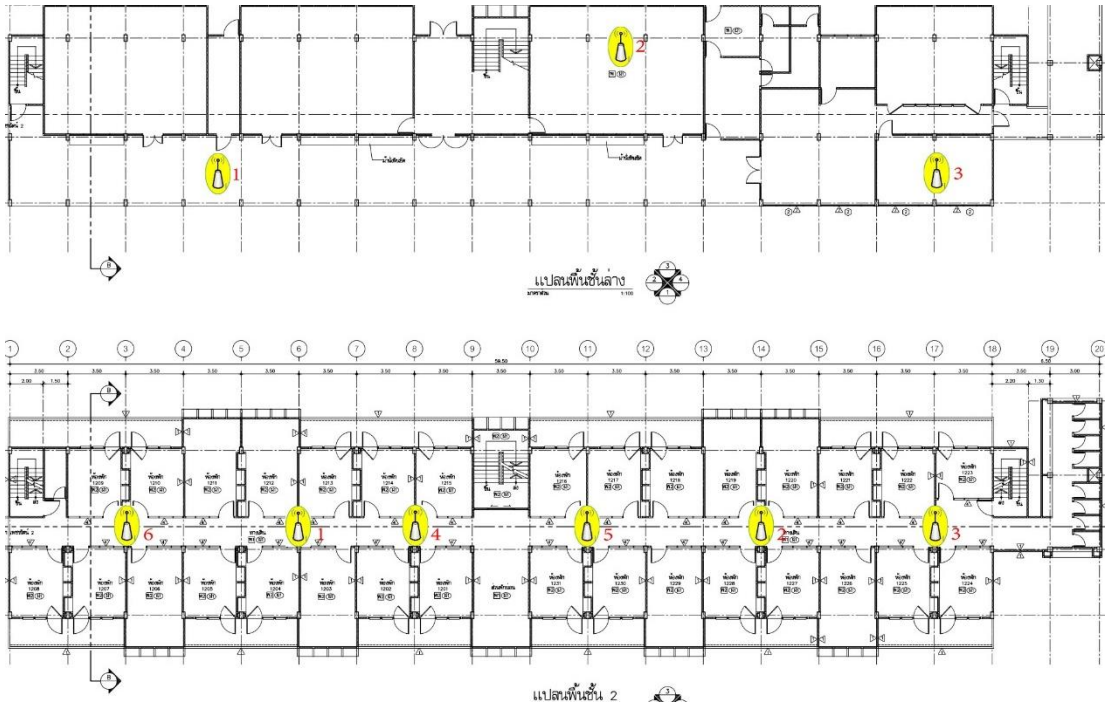


รูปที่ 4.4 ผังการออกแบบโครงสร้างระบบเครือข่ายหอพักนักศึกษา โดยใช้หลักการออกแบบระบบเครือข่ายแบบลำดับชั้น (Hierarchical Network)

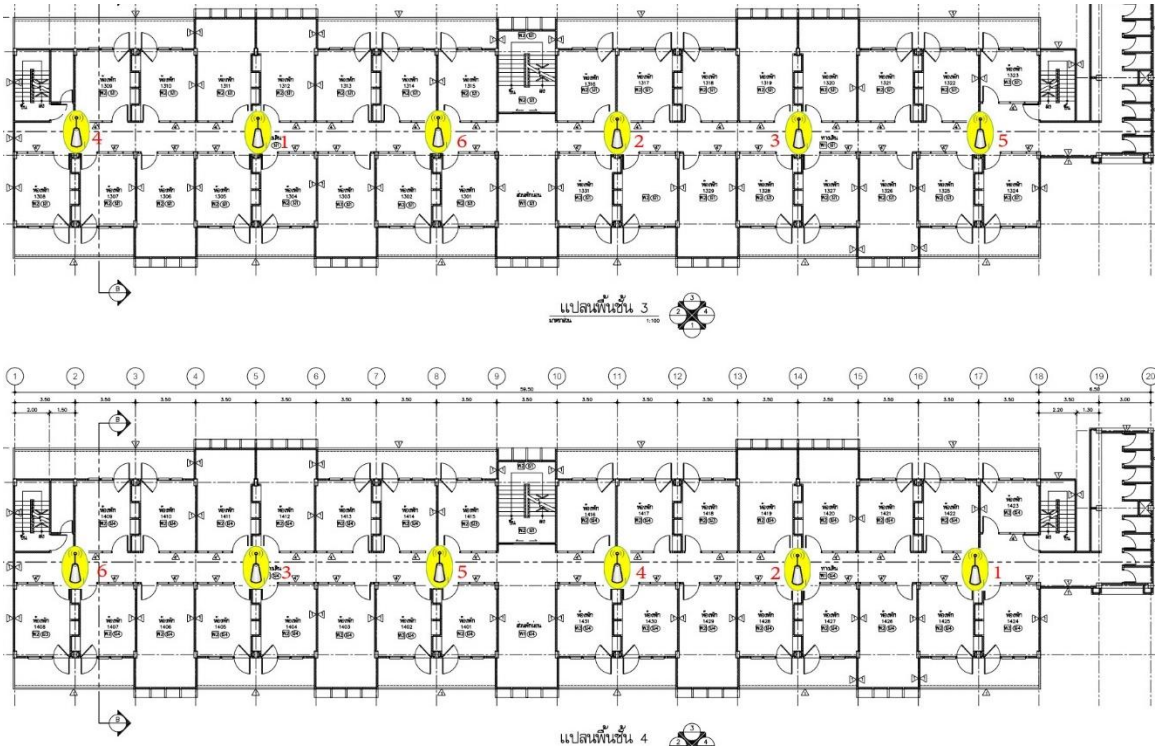
8) การออกแบบระบบเครือข่ายไร้สายหอพักนักศึกษา

การออกแบบจุดติดตั้งอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย กรณีศึกษาภายในหอพักเพชรรัตน์ 1 – หอพักเพชรรัตน์ 6 เป็นอาคารสี่ชั้น มีโครงสร้างของอาคารเหมือนกัน ในส่วนของชั้น 1 ไม่มีห้องพักนักศึกษา จะเป็นพื้นที่ส่วนกลางสำหรับนักศึกษาสามารถใช้ร่วมกัน เช่น อ่านหนังสือ ทำกิจกรรม ส่วนชั้น 2 - 4 จะเป็นห้องพัก จำนวนชั้นละ 31 ห้อง นักศึกษาอยู่ร่วมกันห้องละประมาณ 3 คน แต่ละหอพักจะมีจำนวนนักศึกษาพักอยู่โดยประมาณ 280 – 300 คน

ทางผู้จัดทำได้รวบรวมข้อมูลความต้องการใช้ระบบเครือข่ายไร้สาย รวมถึงปัญหาที่เกิดขึ้นจากโครงการเดิมก่อนหน้านี้ ซึ่งปัญหาส่วนใหญ่เกิดจากสัญญาณไม่ครอบคลุมเป็นสาเหตุให้ระบบเครือข่ายไร้สายหลุดบ่อยไม่เสถียร จึงได้นำปัญหาดังกล่าวมารวบรวม วิเคราะห์ และทดสอบแก้ไขปัญหาที่หน้างานจริง เพื่อนำมาปรับปรุงแก้ไขให้สามารถรองรับการใช้งานได้อย่างมีประสิทธิภาพ



รูปที่ 4.5 แสดงหมายเลขตำแหน่งจุดให้บริการเครือข่ายไร้สายหอพักเพชรรัตน์ 1 ชั้น 1 และชั้น 2



รูปที่ 4.6 แสดงหมายเลขตำแหน่งจุดให้บริการเครือข่ายไร้สายหอพักเพชรรัตน์ 1 ชั้น 3 และชั้น 4

โดยผลสรุปการปรับปรุงได้ดำเนินการเพิ่มตำแหน่งจุดให้บริการไร้สายจากเดิมชั้น 2 - 4 เดิมมีจำนวน 5 จุด ดำเนินการเพิ่ม Access point อีก 1 จุด รวมทั้งติดตั้งสาย UTP CAT6 สำหรับเชื่อมต่อกับ Access point พร้อมปรับย้ายตำแหน่งจุดให้บริการเครือข่ายไร้สายของเดิม ให้เหมาะสมกับตำแหน่งห้องพักตามแผนผังอาคาร ส่งผลทำให้หมายเลขตำแหน่งจุดให้บริการหมายเลขไม่เรียงกัน เพราะต้องอ้างอิงหมายเลขสาย UTP CAT6 ชุดเดิม และเดินสายเพิ่มใหม่ชั้นละ 1 จุด

ระบบเครือข่ายไร้สายเป็นการนำระบบการสื่อสารไร้สายมาติดตั้งร่วมกับเครือข่ายที่ใช้สายเพื่อเพิ่มความคล่องตัวในการใช้งาน และเพื่อรองรับการใช้งานจากอุปกรณ์ประเภทโมบาย เช่น มือถือ แท็ปเล็ต ที่นับวันจะเพิ่มความนิยมมากขึ้น ในหอพักเพชรัตตน์ 1 – 6 ดำเนินการติดตั้ง Access point หอพักละ 21 ตัว การบริหารจัดการคอนฟิกทีละตัวเป็นเรื่องที่ไม่ง่ายมากนัก จึงมีการนำคอนโทรลเลอร์มาควบคุมจัดการ Access point แทน ข้อกำหนดของเครือข่ายไร้สายที่นำมาติดตั้งใช้งาน มีคุณสมบัติดังนี้

1) สามารถทำงานได้ตามมาตรฐาน IEEE 802.11a/b/g/n/ac
2) รองรับมาตรฐาน PoE IEEE 802.3af
3) สามารถทำงานแบบ Multiple SSID ได้ไม่น้อยกว่า 8 SSID
4) สามารถทำ VLAN ได้ตามมาตรฐาน IEEE 802.1Q
5) รองรับมาตรฐานการเข้ารหัสข้อมูลได้ตามมาตรฐาน WEB , TKIP , AES
6) รองรับการพิสูจน์ตัวตนตามมาตรฐาน 802.11i
7) รองรับการพิสูจน์ตัวตนตามมาตรฐาน 802.1x ผ่าน Radius และ Active directory
8) รองรับการทำ Roaming ทั้งในลักษณะ Layer2 และ Layer3 ได้
9) รองรับการทำ QoS ได้แบบ Bandwidth contract, Traffic shaping
10) สามารถทำ Authentication ผู้ใช้งานผ่านทาง Web-base ได้

ตัวอย่างการตั้งค่าอุปกรณ์เครือข่ายไร้สาย (Access point)

ผู้จัดทำได้เลือกใช้อุปกรณ์เครือข่ายไร้สาย UniFi AP การตั้งค่าอุปกรณ์ต้องใช้โปรแกรม UniFi Controller ซึ่งเป็นเจ้าของผลิตภัณฑ์เดียวกัน ได้กำหนดให้บริการเครือข่ายไร้สาย จำนวน 5 SSID ดังนี้

1) SU-WiFi
2) su-roam-WiFi
3) .@ AIS SUPER WiFi : ระบบเครือข่ายไร้สายบริษัทเอไอเอส
4) @ dtac wifi : ระบบเครือข่ายไร้สายบริษัทดีแทค
5) .@ TRUEWIFI : ระบบเครือข่ายไร้สายบริษัททรู

กรณี SSID : SU-WiFi , su-roam-WiFi เป็นระบบเครือข่ายไร้สายของมหาวิทยาลัยศิลปากร นักศึกษาและบุคลากรต้องลงทะเบียน SU-IT Accout ของมหาวิทยาลัยให้ถูกต้องตามข้อกำหนด จึงสามารถนำ Account มาใช้ Login เพื่อใช้งานระบบเครือข่ายและบริการอื่น ๆ ได้ ส่วนกรณีเครือข่ายไร้สายเอกชนทั้ง 3 ราย สำหรับผู้ใช้บริการมือถือค่ายนั้นๆ หรือสมัครเพจเกจเพิ่มเติม

1) Reset UniFi AP ด้วยวิธีการ Reset ที่ UniFi AP โดยตรง เตรียม UniFi AP , PoE , สาย UTP , Switch นำมาต่อดังรูป

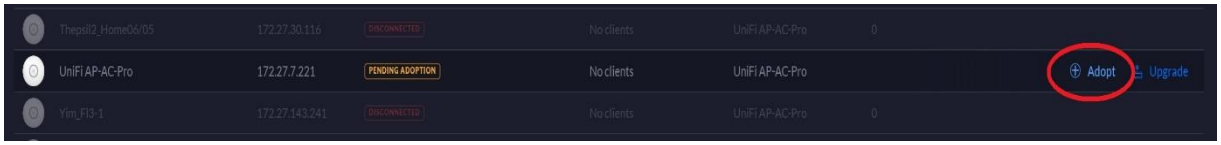
- ช่องที่มีคำว่า PoE ให้ต่อ สาย LAN ไปที่ตัว UniFi ไม่ว่าจะรุ่นไหนก็ตาม
- ช่องที่มีคำว่า LAN ให้ต่อ สาย LAN ไปที่ตัว Computer หรือ Switch ที่จะตั้งค่า

รูปที่ 4.7 แสดงภาพการเชื่อมต่อ UniFi AP เพื่อ Reset config

2) กดปุ่ม Reset ค้างไว้ประมาณ 10 วินาที แล้วปล่อย

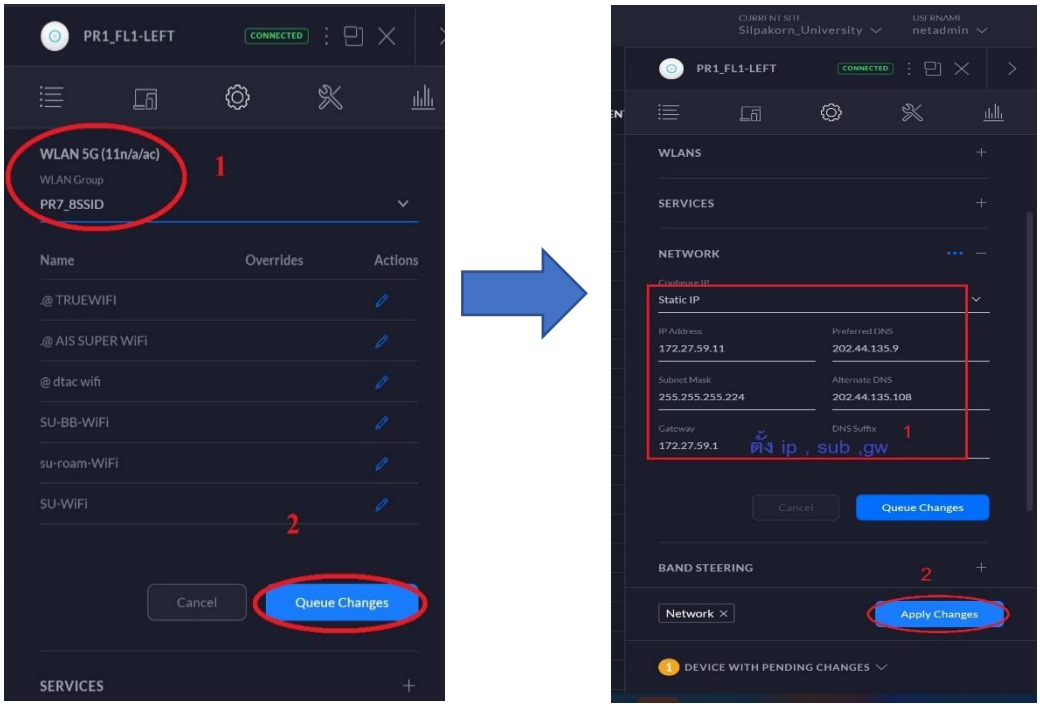
รูปที่ 4.8 แสดงภาพการเชื่อมต่อ Reset UniFi AP

3) ที่หน้า Controller UniFi จะแสดง AP ใหม่ที่ต้องการตั้งค่า กดเลือก Adopt



รูปที่ 4.9 แสดงภาพ Controller UniFi เพื่อทำการ Adopt

4) ตั้งชื่อ AP เลือก WLAN Group เลือก Queue Changes ตั้งค่า Static IP ของ AP เลือก Apply Changes รอจนกว่าระบบแจ้งสถานะ Disconnect จึงนำไปทดสอบใช้งานจริง



รูปที่ 4.10 การตั้ง WLAN Group และการตั้งค่า IP ของ UniFi AP

9) ตัวอย่างการตั้งค่าอุปกรณ์กระจายสัญญาณเครือข่าย Core Switch [8]

- การตั้งค่าอุปกรณ์คุณสมบัติอุปกรณ์กระจายสัญญาณเครือข่ายหลัก Core Switch ที่ตัว Switch Alcatel 6900-X72 ทำหน้าที่เป็นศูนย์กลางการเชื่อมต่อไปยังอุปกรณ์เครือข่ายที่ถูกติดตั้งไว้ลำดับชั้นต่างๆ ซึ่งมีตัวอย่างการคอนฟิกการสร้าง VLAN และหมายเลข VLAN ดังรูป

```
6900_Core-SPB->
6900_Core-SPB-> vlan 1581 admin-state enable

6900_Core-SPB-> vlan 1581 name "PR1_Lan"

6900_Core-SPB-> vlan 1591 admin-state enable

6900_Core-SPB-> vlan 1591 name "PR1_Device"

6900_Core-SPB->
```

รูปที่ 4.11 ตัวอย่างการสร้าง VLAN 1581 , VLAN 1591

```
6900_Core-SPB->
6900_Core-SPB-> ip interface "PR1_Lan" address 172.27.58.1 mask 255.255.255.224 vlan 1581

6900_Core-SPB-> ip interface "PR1_Device" address 172.27.59.1 mask 255.255.255.224 vlan 1591

6900_Core-SPB->
6900_Core-SPB->
```

รูปที่ 4.12 ตัวอย่างการกำหนด IP interface ให้กับ VLAN 1581, VLAN 1591

```
ip interface "PR1_Device" address 172.27.59.1 mask 255.255.255.224 vlan 1591 ifindex 124
ip interface "PR2_Lan" address 172.27.58.33 mask 255.255.255.224 vlan 1582 ifindex 125
ip interface "PR2_Device" address 172.27.59.33 mask 255.255.255.224 vlan 1592 ifindex 126
ip interface "PR3_Lan" address 172.27.58.65 mask 255.255.255.224 vlan 1583 ifindex 127
ip interface "PR3_Device" address 172.27.59.65 mask 255.255.255.224 vlan 1593 ifindex 128
ip interface "PR4_Lan" address 172.27.58.97 mask 255.255.255.224 vlan 1584 ifindex 129
ip interface "PR4_Device" address 172.27.59.97 mask 255.255.255.224 vlan 1594 ifindex 130
ip interface "PR5_Lan" address 172.27.58.129 mask 255.255.255.224 vlan 1585 ifindex 138
ip interface "PR5_Device" address 172.27.59.129 mask 255.255.255.224 vlan 1595 ifindex 139
ip interface "PR6_Lan" address 172.27.58.161 mask 255.255.255.224 vlan 1586 ifindex 140
ip interface "PR6_Device" address 172.27.59.161 mask 255.255.255.224 vlan 1596 ifindex 141
```

รูปที่ 4.13 ตรวจสอบการตั้งค่า IP interface ของ VLAN ทั้งหกหอพัก

10) ตัวอย่างการตั้งค่าอุปกรณ์กระจายสัญญาณเครือข่าย Distribution Layer [10]

การตั้งค่าอุปกรณ์คุณสมบัติอุปกรณ์กระจายสัญญาณเครือข่ายของ Distribution Layer ที่ตัว Switch Alcatel 6860E-U28 ตัวอย่างการคอนฟิก linkagg lacp agg... เพื่อกำหนด admin-key

```
! Link Aggregate:
linkagg lacp agg 1 size 2 admin-state enable
linkagg lacp agg 1 name "Link to Backbone"
linkagg lacp agg 1 actor admin-key 1
linkagg lacp agg 2 size 2 admin-state enable
linkagg lacp agg 2 name "toPR1"
linkagg lacp agg 2 actor admin-key 101
linkagg lacp agg 3 size 2 admin-state enable
linkagg lacp agg 3 name "toPR2"
linkagg lacp agg 3 actor admin-key 102
linkagg lacp agg 4 size 2 admin-state enable
linkagg lacp agg 4 name "toPR3"
linkagg lacp agg 4 actor admin-key 103
linkagg lacp agg 5 size 2 admin-state enable
linkagg lacp agg 5 name "toPR4"
linkagg lacp agg 5 actor admin-key 104
linkagg lacp agg 6 size 2 admin-state enable
linkagg lacp agg 6 name "toPR5"
linkagg lacp agg 6 actor admin-key 105
linkagg lacp agg 7 size 2 admin-state enable
linkagg lacp agg 7 name "toPR6"
linkagg lacp agg 7 actor admin-key 106
linkagg lacp agg 8 size 2 admin-state enable
linkagg lacp agg 8 name "Test Tag4"
linkagg lacp agg 8 actor admin-key 108
```

รูปที่ 4.14 การการคอนฟิก linkagg lacp agg เพื่อกำหนด admin-key

```
linkagg lacp port 1/1/1 actor admin-key 101
linkagg lacp port 1/1/2 actor admin-key 102
linkagg lacp port 1/1/3 actor admin-key 103
linkagg lacp port 1/1/4 actor admin-key 104
linkagg lacp port 1/1/5 actor admin-key 105
linkagg lacp port 1/1/6 actor admin-key 106
linkagg lacp port 1/1/11 actor admin-key 101
linkagg lacp port 1/1/12 actor admin-key 102
linkagg lacp port 1/1/13 actor admin-key 103
linkagg lacp port 1/1/14 actor admin-key 104
linkagg lacp port 1/1/15 actor admin-key 105
linkagg lacp port 1/1/16 actor admin-key 106
linkagg lacp port 1/1/21 actor admin-key 108
linkagg lacp port 1/1/22 actor admin-key 108
```

รูปที่ 4.15 การกำหนด linkagg lacp port อ้างอิง admin-key

11) ตัวอย่างการตั้งค่าอุปกรณ์กระจายสัญญาณเครือข่าย Access Layer ที่ตัว Switch Aruba 6100 [12]

```
6100(config)#
6100(config)# vlan 1583
6100(config-vlan-1583)# name PR3_Lan
6100(config-vlan-1583)# exit
6100(config)# vlan 1593
6100(config-vlan-1593)# name PR3_Device
6100(config-vlan-1593)# exit
6100(config)#
6100(config)#
```

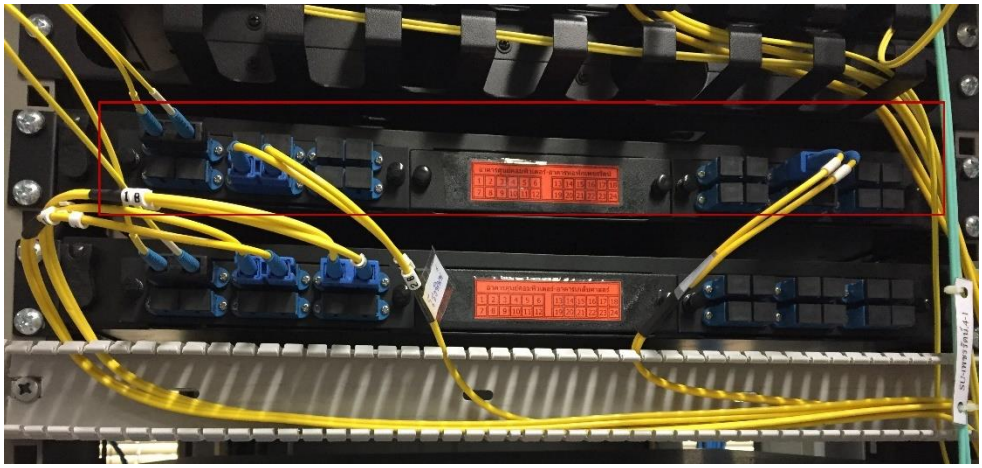
รูปที่ 4.16 ตัวอย่างการสร้าง VLAN 1583 , VLAN 1593 ของหอพักเพชรรัตน์ 3

```
6100(config)# interface 1/1/2
6100(config-if)# no shutdown
6100(config-if)# vlan access 1581
6100(config-if)# exit
6100(config)# interface 1/1/3
6100(config-if)# no shutdown
6100(config-if)# vlan access 1581
6100(config-if)# exit
6100(config)# interface 1/1/4
6100(config-if)# no shutdown
6100(config-if)# vlan access 1581
6100(config-if)# exit
6100(config)#
```

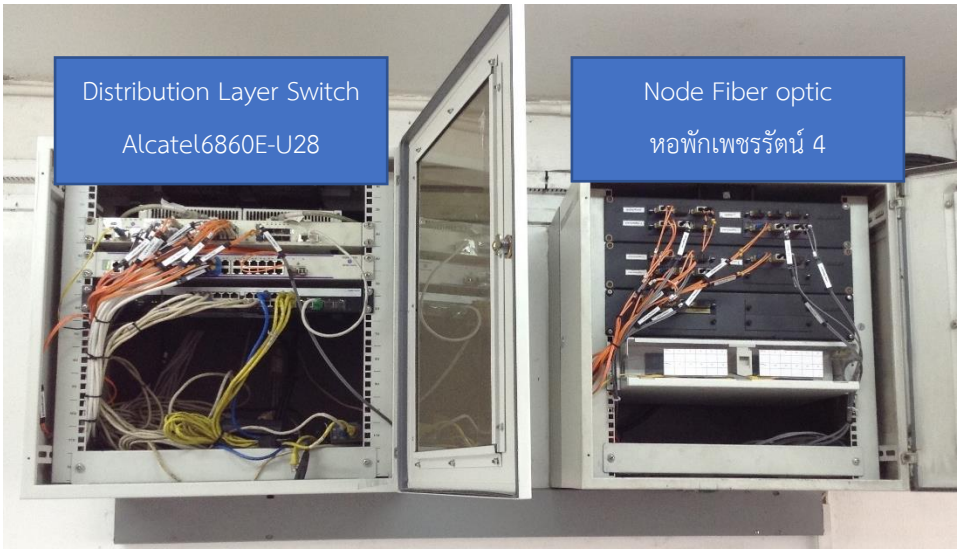
รูปที่ 4.17 ตัวอย่างการสร้าง VLAN Access ที่ Interface 1/1/2 – 1/1/4

12) ภาพตัวอย่างการติดตั้งอุปกรณ์กระจายสัญญาณเครือข่าย

รูปที่ 4.18 Core Switch Alcatel 6900-X72 ฝั่งสำนักดิจิทัลฯ 2 ตัว
ใช้สาย Fiber optic ต่อ Stack ทำให้เสมือนรวมเป็นตัวเดียวกัน



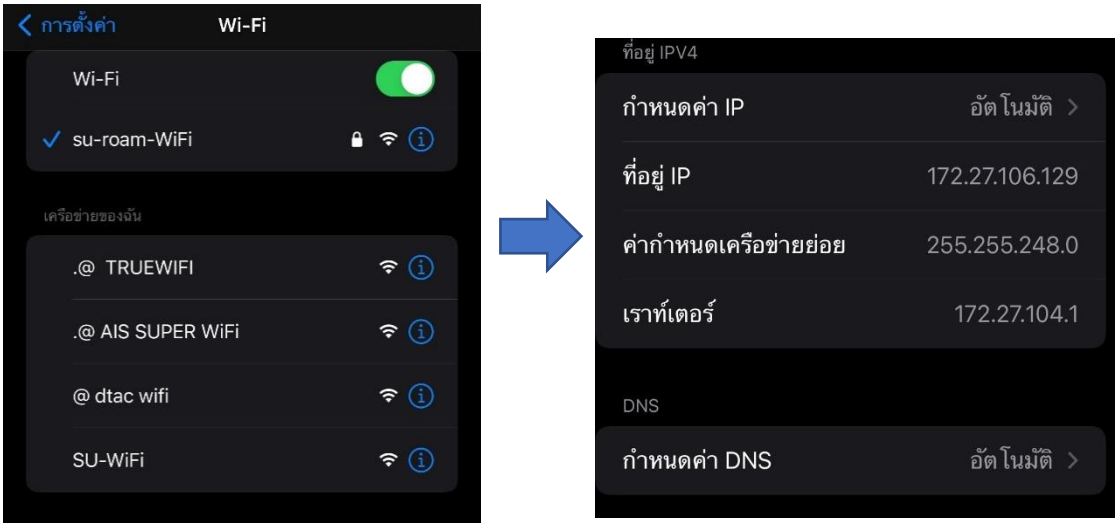
รูปที่ 4.19 Node Fiber optic S/M 24 Core ฝั่งสำนักดิจิทัลฯ ไปยัง Node Phetcharat



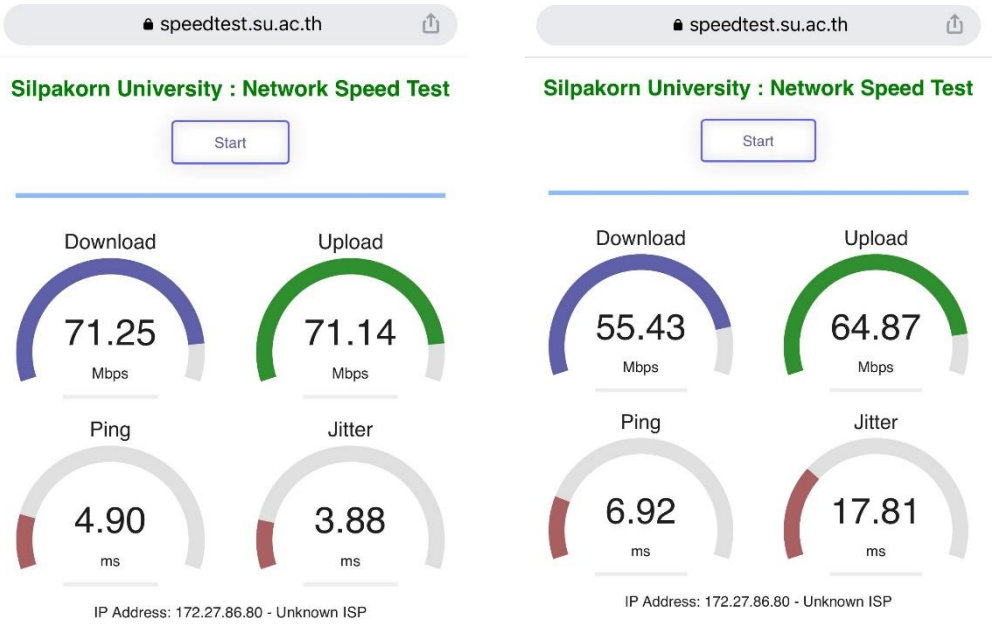
รูปที่ 4.20 การติดตั้งอุปกรณ์เครือข่าย Distribution Layer Switch : Node Phetcharat 4

รูปที่ 4.21 แสดงการติดตั้ง Switch Access หอพักเพชรรัตน์ 1

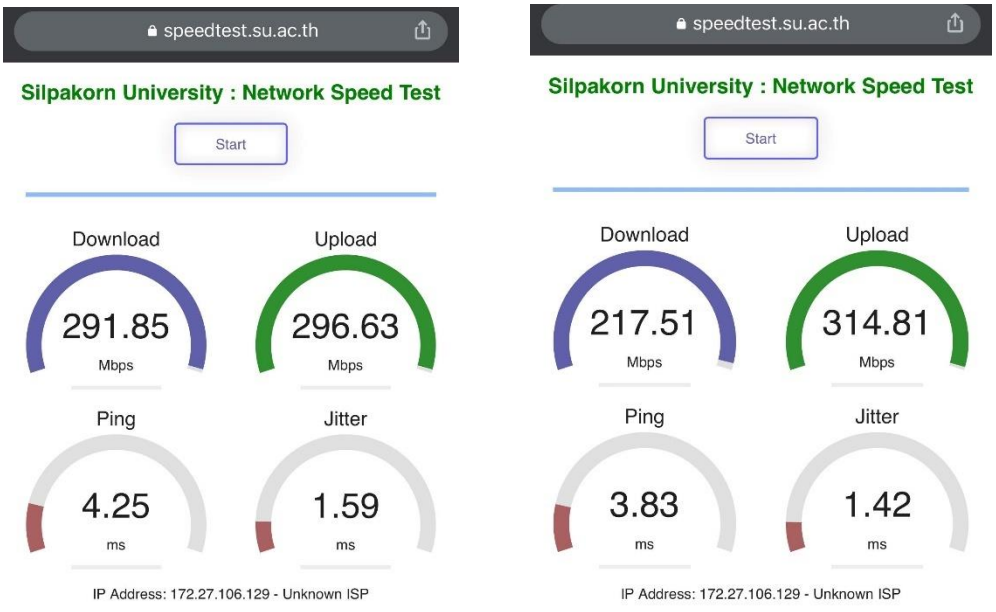
รูปที่ 4.22 แสดงหน้าจอ Web Login ก่อนเข้าระบบเครือข่าย ม.ศิลปากร



รูปที่ 4.23 แสดง SSID ที่ให้เปิดบริหารพร้อมทดสอบเชื่อมต่อ สามารถใช้งานทุก SSID



รูปที่ 4.24 ทดสอบ Speed test ระบบเครือข่ายภายใน ม.ศิลปากร (ก่อนปรับปรุง)

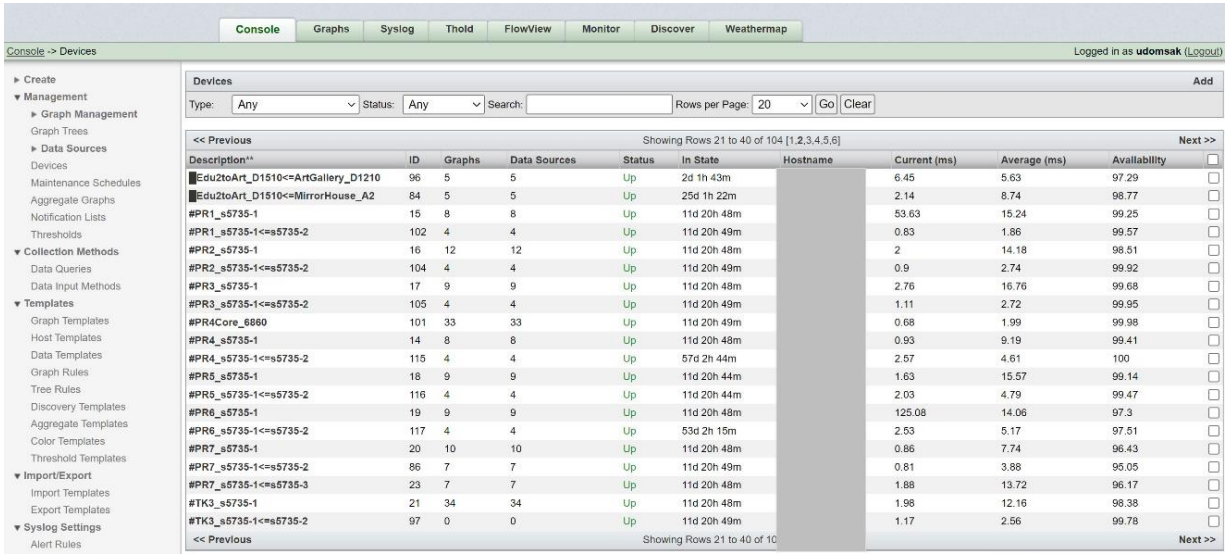


รูปที่ 4.25 ทดสอบ Speed test ระบบเครือข่ายภายใน ม.ศิลปากร (หลังปรับปรุง)

13) ระบบตรวจสอบสถานะเครือข่าย (Network Monitoring)

Network Monitoring คือ การเฝ้าระวัง ตรวจสอบสภาพเครือข่ายให้มีความเสถียร ปลอดภัย หากเกิดเหตุขัดข้องหรือระบบล่มหรือขัดข้อง สามารถข้อมูลมาวิเคราะห์เพื่อปรับปรุงพัฒนาระบบให้มีประสิทธิภาพ ช่วยให้มองเห็นภาพรวมการทำงานและประสิทธิภาพการทำงานของระบบเน็ตเวิร์กและเหตุการณ์ต่าง ๆ ได้อย่างง่าย

ทางผู้จัดทำให้ได้เลือกใช้ระบบ Cacti เพื่อใช้ในการตรวจสอบสถานะระบบเครือข่าย Up-Down เพื่อให้การบริหารจัดการเครือข่ายได้อย่างมีประสิทธิภาพดียิ่งขึ้น สามารถรู้ได้ทันทีว่าอุปกรณ์และส่วนงานใดบนระบบเน็ตเวิร์กมีปัญหา ช่วยลดเวลาในการแก้ปัญหา ลดการสูญเสียโอกาสทางธุรกิจ



รูปที่ 4.26 ตัวอย่างระบบ Monitoring Cacti เพื่อใช้ตรวจสอบสถานะระบบเครือข่าย

4.3 วิธีการติดตามและประเมินผลการปฏิบัติงาน

การติดตามและประเมินผลการปฏิบัติงานเป็นกระบวนการที่สำคัญของการตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่าย จะต้องมีการติดตาม และรายงานผลเป็นระยะ ๆ เพื่อให้ทราบว่าการดำเนินงานสำเร็จตามเป้าหมายและสามารถใช้งานได้อย่างมีประสิทธิภาพ โดยมีตัวอย่างการประเมินผลอยู่ในภาคผนวก

4.3.1 ขั้นเตรียมการ

ผู้เขียนคู่มือการปฏิบัติงานในฐานะนักคอมพิวเตอร์ ระดับปฏิบัติการ เป็นผู้ให้บริการและปฏิบัติงานการจัดทำคู่มือการตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่าย ซึ่งการปฏิบัติงานที่ผ่านมาพบว่ามีปัญหา อุปสรรค อย่างไรบ้าง และผู้รับบริการมีความพึงพอใจระดับใด เพื่อนำข้อมูลไปประกอบการพัฒนาและประเมินผลงาน ซึ่งได้เตรียมการดังนี้

- การวางแผนการติดตามผล
- การดำเนินการตามแผนที่กำหนดไว้ด้วยวิธีการให้ตรงตามเป้าหมายที่กำหนดไว้
- การประเมินผลการปฏิบัติงาน ในด้านการให้บริการ และความสำเร็จของงานว่าตรงตามความต้องการหรือไม่ มีข้อเสนอแนะที่ควรนำมาปรับปรุงอย่างไร นำข้อมูลจากการประเมิน มาปรับปรุงแก้ไข และพัฒนางานการตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่ายต่อไป

4.3.2 ขั้นดำเนินการ

การดำเนินการจะต้องปฏิบัติให้สอดคล้องกับแผนการติดตามผล และกระบวนงานที่วางไว้ เพื่อส่งผลต่อความสำเร็จของการติดตาม และประเมินผลการปฏิบัติงาน รวมถึงความพึงพอใจของหัวหน้างานและผู้รับบริการ

4.3.3 ขั้นติดตามประเมินผลการปฏิบัติงาน

การติดตามและประเมินผลการปฏิบัติงานเป็นขั้นตอนการประเมินผลความถูกต้องของข้อมูล และความเหมาะสมของวิธีการดำเนินงานให้อยู่ภายในขอบเขตงานที่กำหนดไว้ รวมทั้งเพื่อติดตามผลของงานว่าตรงตามวัตถุประสงค์ หรือเป้าหมายของงานหรือไม่ สามารถนำผลการติดตามและประเมินผลของงานไปจัดทำรายงานเพื่อเสนอต่อหัวหน้างาน เพื่อนำข้อมูลจากการติดตาม และการ

ประเมินผลมาใช้ประกอบการพัฒนางาน และการวางแผนงานในการปฏิบัติงานครั้งต่อไป ตลอดจนทบทวนกระบวนการปฏิบัติงานตั้งแต่กระบวนการเกี่ยวกับการวางแผนการดำเนินการ และการติดตามประเมินผล หากพบข้อบกพร่อง ควรปรับปรุงแก้ไข เพื่อพัฒนางานการตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่ายในครั้งต่อไป

บทที่ 5
ปัญหาอุปสรรค ข้อเสนอแนะ และการพัฒนางาน

ผู้ปฏิบัติงานในตำแหน่งนักคอมพิวเตอร์ระดับปฏิบัติการ ฝ่ายบริหารและพัฒนาดิจิทัลเทคโนโลยี สำนักดิจิทัลเทคโนโลยี มหาวิทยาลัยศิลปากร มีบทบาทหน้าที่ในการตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่าย ตรวจสอบสถานะระบบเครือข่ายและอุปกรณ์เครือข่ายให้พร้อมใช้งาน ปรับปรุง แก้ไขปัญหาอุปกรณ์เครือข่ายของคณะ หน่วยงานต่างๆ งานประชาสัมพันธ์ด้านระบบเครือข่าย งานให้บริการปรึกษาแก้ไขปัญหาด้านสารสนเทศและการพิจารณาดำเนินการในภาระงานดังกล่าวตามแนวคิดหรือแนวทางการประยุกต์ใช้เครื่องมือดิจิทัลออนไลน์ หลักการปฏิบัติงาน PDCA มาตรฐานการปฏิบัติงานขั้นตอนการปฏิบัติงาน วิธีการติดตามและประเมินผลการปฏิบัติงาน คุณธรรม จริยธรรม และจรรยาบรรณในการปฏิบัติงานที่เกี่ยวข้องมาใช้ในการปฏิบัติงานและต้องให้บริการภาระงานอื่น ๆ เพื่อให้ผู้รับบริการมีความพึงพอใจมากยิ่งขึ้น จากการปฏิบัติงานที่ผ่านมาถึงปัจจุบัน ถึงแม้ว่าการให้บริการที่ดีอย่างไร แต่ในภาพรวมยังพบปัญหาอุปสรรคและแนวทางแก้ไขปัญหา รวมถึงข้อเสนอแนะซึ่งสามารถสรุปได้ดังนี้

5.1 ปัญหา อุปสรรคแนวทางแก้ไขปัญหาในการปฏิบัติงาน และการพัฒนางาน ดังข้อมูลในตารางที่ 5.1

ตารางที่ 5.1 ปัญหาอุปสรรคและแนวทางแก้ไขปัญหาในการปฏิบัติงาน และการพัฒนางาน

การปฏิบัติงาน	ปัญหา/อุปสรรค	แนวทางแก้ไข และการพัฒนางาน
1. ศึกษา วิเคราะห์ประโยชน์และข้อจำกัดต่าง ๆ ของเครื่องมือ และข้อมูล ที่เกี่ยวข้องกับการปฏิบัติงาน	อุปกรณ์กระจายสัญญาณระบบเครือข่ายระดับ Access layer ไม่รองรับการเชื่อมต่อกับ SFP Module Fiber optic ทุกประเภท เป็นสาเหตุทำให้ไม่สามารถเชื่อมต่อระบบเครือข่ายจาก Node หอพักเพชรรัตน์ 4 ไปยังหอพักเพชรรัตน์ 1, 2, 3, 5 และ 6 ได้	1. ชี้แจงให้ผู้ใช้บริการทราบ 2. ประสานงานบริษัทเจ้าของผลิตภัณฑ์เพื่อขอข้อมูลอุปกรณ์ปัญหาที่ขัดข้อง พร้อมวิธีแก้ไข 3. กรณีจัดซื้ออุปกรณ์เครือข่ายควรระบุในขั้นตอนการตรวจรับว่าต้องมีการอบรมการใช้งานอุปกรณ์หรือระบบนั้นฯ ให้กับบุคลากรเพื่อเป็นแนวทางบริหารจัดการในอนาคต

ตารางที่ 5.1 ปัญหาอุปสรรคและแนวทางแก้ไขปัญหาในการปฏิบัติงาน และการพัฒนางาน (ต่อ)

การปฏิบัติงาน	ปัญหา/อุปสรรค	แนวทางแก้ไข และการพัฒนางาน
1. ศึกษา วิเคราะห์ประโยชน์และข้อจำกัดต่าง ๆ ของเครื่องมือ และข้อมูล ที่เกี่ยวข้องกับการปฏิบัติงาน	ระบบไฟฟ้าภายในมหาวิทยาลัยศิลปากรขัดข้องบ่อยครั้ง จนเป็นสาเหตุทำให้อุปกรณ์กระจายสัญญาณระบบเครือข่ายชำรุดเสียหาย	1. ชี้แจงให้ผู้ใช้บริการทราบ 2. จัดหาเครื่องสำรองไฟฟ้าเพื่อจ่ายไฟสำรองให้อุปกรณ์กระจายสัญญาณระบบเครือข่ายทุกหอพัก เพื่อป้องกันอุปกรณ์ชำรุดเสีย ปัจจุบันทุกหอพักมี UPS ขนาด 1KVA หอพักละจำนวน 1 ตัว แต่พบว่ายังไม่เพียงพอในการจ่ายไฟฟ้าสำรองให้กับอุปกรณ์เพราะบางครั้งไฟฟ้าดับ 30 นาที หรือมากกว่านั้น จึงมีข้อเสนอแนะในการจัดซื้อ UPS ให้มีขนาดของ KVA มากขึ้น เพื่อให้ความสามารถจ่ายไฟฟ้าสำรองได้เวลานานมากขึ้น 3. จัดหาอุปกรณ์กระจายสัญญาณระบบเครือข่ายสำรองโดยมีคุณสมบัติเช่นเดียวหรือดีกว่าตัวปัจจุบันเพื่อป้องกันเหตุอุปกรณ์ชำรุดเสียหาย จะได้สามารถเปลี่ยนอุปกรณ์สำรองทดแทนให้บริการได้ทันท่วงที

ตารางที่ 5.1 ปัญหาอุปสรรคและแนวทางแก้ไขปัญหาในการปฏิบัติงาน และการพัฒนางาน (ต่อ)

การปฏิบัติงาน	ปัญหา/อุปสรรค	แนวทางแก้ไข และการพัฒนางาน
1. ศึกษา วิเคราะห์ประโยชน์และข้อจำกัดต่าง ๆ ของเครื่องมือ และข้อมูล ที่เกี่ยวข้องกับการปฏิบัติงาน	ตำแหน่งห้องพักห้องแรกและห้องสุดท้ายมักพบปัญหาระดับสัญญาณ Wi-Fi อ่อน เป็นสาเหตุทำให้การเชื่อมต่อหลุดบ่อยครั้ง	1. ชี้แจงให้ผู้ใช้บริการทราบ 2. ตำแหน่งที่นักศึกษานั่งใช้งานเป็นมุมห้องที่อยู่ห่างจาก Wi-Fi โดยมีปัจจัยของโครงสร้างอาคารด้วย เช่น บางหอพักผนังห้องเป็นไม้อัด ยิปซั่ม หรือผนังปูน ย่อมมีผลต่อระดับสัญญาณ 3. จากการที่ได้เข้าไปวัดสัญญาณ Wi-Fi โดยใช้โปรแกรม WiFi Analyzer ตรวจสอบพบว่าสัญญาณย่านความถี่ 2.4 GHz ชนกันหลายจุด เป็นสาเหตุทำให้เกิดปัญหาการเชื่อมต่อหลุดบ่อยครั้ง พบว่าสาเหตุเกิดจาก Wi-Fi เอกชนปล่อยสัญญาณย่านความถี่ 2.4 GHz และ 5 GHz กอร์ปกับ Wi-Fi ของสำนักดิจิทัลฯ ด้วย จึงได้มีหารือให้ทางเอกชนปิดสัญญาณย่านความถี่ 2.4 GHz ที่อุปกรณ์ Controller Wi-Fi ในบางจุด แต่ยังไม่สามารถแก้ไขปัญหาได้ จนในที่สุดจำเป็นต้องแก้ไขโดยการแจ้งให้เอกชนดำเนินการถอด Wi-Fi ออกทุกหอพัก สำนักดิจิทัลได้ปรับปรุงจุดติดตั้ง AP ให้บริการดังรูปที่ 4.5 และ รูปที่ 4.6

ตารางที่ 5.1 ปัญหาอุปสรรคและแนวทางแก้ไขปัญหาในการปฏิบัติงาน และการพัฒนางาน (ต่อ)

การปฏิบัติงาน	ปัญหา/อุปสรรค	แนวทางแก้ไข และการพัฒนางาน
2. จัดการข้อมูลให้ถูกต้องและตามรูปแบบที่ กำหนดเพื่อนำมาเป็นข้อมูลตั้งค่าอุปกรณ์กระจายสัญญาณเครือข่าย	ข้อมูลจำนวนห้องพัก ของอาคารหอพักที่ได้มาบางส่วนไม่ถูกต้อง เช่น จำนวนห้องพัก จำนวนนักศึกษา เป็นเหตุทำให้การออกแบบระบบเครือข่ายหอพักนั้นๆ ไม่ถูกต้อง เป็นเหตุทำให้ไม่สามารถรองรับการใช้งานไม่เต็มประสิทธิภาพ	1. ชี้แจงให้ผู้ใช้บริการทราบและอธิบายขั้นตอน พร้อมทั้งวิธีการดำเนินการเรื่องการขอเข้าใช้งานในระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยศิลปากรให้กับผู้รับบริการทราบ 2. ประสานงานหน่วยงานที่รับผิดชอบเพื่อขอข้อมูลที่จำเป็นเพื่อนำมาวิเคราะห์ออกแบบระบบเครือข่ายให้ครบถ้วนสามารถให้บริการได้อย่างมีประสิทธิภาพ
3. ดำเนินการตั้งค่าอุปกรณ์กระจายสัญญาณเครือข่ายตามขั้นตอนที่ได้กำหนด	ไม่สามารถใช้งานอุปกรณ์กระจายสัญญาณระบบเครือข่ายได้ เนื่องจาก Port SFP Module ทั้ง 4 port ไม่รองรับการเชื่อมต่อกับอุปกรณ์ SFP Module ผลิตภัณฑ์อื่นได้	1. ทดสอบใช้คำสั่ง Fig Speed data ของ Port SFP ที่ต้องการใช้งาน Mode LACP (LinkAgg) แต่ยังไม่สามารถใช้งานได้ ตรวจสอบโดยใช้คำสั่ง show logging พบว่า Log แจ้งว่า not support SFP จึงต้องใช้คำสั่ง allow-unsupported-transceiver เพื่อเป็นการสั่งงานให้ยอมรับ SFP Module ผลิตภัณฑ์อื่น จึงจะสามารถเชื่อมต่อใช้งานได้ หรือดำเนินการ Upgrade firmware ของอุปกรณ์กระจายสัญญาณระบบเครือข่ายให้เป็นเวอร์ชั่นล่าสุด

5.2 ข้อเสนอแนะ

5.2.1 ควรจัดทำคู่มือปฏิบัติงานที่ชัดเจน แสดงถึงขั้นตอนการการตั้งค่าอุปกรณ์กระจายสัญญาณเครือข่ายและสื่อให้เห็นกระบวนการของการตั้งค่าอุปกรณ์เครือข่ายตามมาตรฐาน

5.2.2 มีการฝึกอบรมเชิงปฏิบัติการการตั้งค่าอุปกรณ์กระจายสัญญาณเครือข่าย แก่บุคลากรภายในมหาวิทยาลัยศิลปากร

บรรณานุกรม

[1] สำนักดิจิทัลเทคโนโลยี มหาวิทยาลัยศิลปากร “โครงสร้างการบริหารองค์กร”, [ออนไลน์], เข้าถึงได้จาก www.bdt.su.ac.th (29 พฤศจิกายน 2564).

[2] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 (2562). ราชกิจจานุเบกษา. เล่ม 136, ตอนที่ 69ก (27 พฤษภาคม 2562) หน้า 27, [ออนไลน์], เข้าถึงได้จาก http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0020.PDF (1 กันยายน 2564).

[3] ประกาศมหาวิทยาลัยศิลปากร เรื่อง “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ”, [ออนไลน์], เข้าถึงได้จาก http://www.president.su.ac.th/legal/images/law/1/3-Bict63-02-13.pdf (3 กันยายน 2564).

[4] “ข้อบังคับมหาวิทยาลัยศิลปากรว่าด้วยจรรยาบรรณของบุคลากรในมหาวิทยาลัยศิลปากร พ.ศ. 2552”, [ออนไลน์], เข้าถึงได้จาก http://www.qa.su.ac.th/DATA/Download/21Jan52/instructor_03.pdf (1 กันยายน 2564).

[5] จตุชัย แพงจันทร์, อนุโชต วุฒิพรพงษ์ , เจาะระบบ Network 2rd Edition นนทบุรี : ไอดีซีฯ , 2551.

[6] จตุชัย แพงจันทร์, อนุโชต วุฒิพรพงษ์ , เจาะระบบ Network 3rd Edition นนทบุรี : ไอดีซีฯ , 2555.

[7] OmniConnect, “Alcatel-Lucent OmniSwitch 6900”, Accessed 9 Sep 2021, via “https://omniconnect.com.vn/products/switches/alcatel-lucent-omniswitch-6900”.

[8] Alcatel-Lucent Enterprise, “OmniSwitch AOS Release 8 Network Configuration Guide 8.8R1”, Accessed 24 Jan 2022, via “https://www.al-enterprise.com/-/media/assets /internet/documents/os8-nt-88r1-rev-a.pdf”, 2022.

[9] Alcatel-Lucent Enterprise, “Alcatel-Lucent OmniSwitch 6860” Accessed 9 Sep 2021, via “https://www.al-enterprise.com/-/media/assets/internet/documents/omniswitch-6860-datasheet-en.pdf”.

[10] Alcatel-Lucent Enterprise, “OmniSwitch AOS Release 6 Network Configuration Guide 6.7.2.R08”, Accessed 9 Sep 2021, via “https://www.al-enterprise.com/-/media/assets /internet/documents/os-nt-672r08-rev-a.pdf”, 2020.

[11] Aruba Networks, “Aruba CX 6100 Switch Series Data Sheet”, Accessed 9 Sep 2021, via “https://www.arubanetworks.com/resource/aruba-cx-6100-switch-series-data-sheet/”.

[12] Aruba Networks, “AOS-CX 10.07 Command-Line Interface Guide 6100 Switch Series”, Accessed 22 Jan 2022, via “https://www.arubanetworks.com/techdocs/AOS-CX/10.07/PDF/5200-7834.pdf”, 2022.

ภาคผนวก

แบบฟอร์มประเมินการให้บริการ ผลประเมิน และข้อเสนอแนะ

ในส่วนนี้ผู้จัดทำคู่มือใช้เครื่องมือ Google Form ในการจัดทำแบบฟอร์มประเมินการให้บริการ และความพึงพอใจจากผู้ใช้บริการระบบเครือข่ายจากการให้บริการทั้งหมด ในทุกๆรอบ การประเมิน 6 เดือน

หัวข้อประเมินความพึงพอใจ

ระดับ 5 หมายถึงความพึงพอใจมากที่สุด , ระดับ 1 หมายถึงความพึงพอใจน้อยที่สุด

	5	4	3	2	1
1. ความไม่ยุ่งยากซับซ้อนของขั้นตอนการให้บริการ	○	○	○	○	○
2. ความรวดเร็วในการให้บริการ	○	○	○	○	○
3. ความชัดเจนของขั้นตอนการให้บริการ	○	○	○	○	○
4. ทักษะในงานของเจ้าหน้าที่ผู้ให้บริการ	○	○	○	○	○
5. มนุษย์สัมพันธ์ของเจ้าหน้าที่ผู้ให้บริการ	○	○	○	○	○
6. ความชัดเจนน่าเชื่อถือในการให้คำแนะนำ	○	○	○	○	○
7. ความกระตือรือร้นในงานของเจ้าหน้าที่ผู้ให้บริการ	○	○	○	○	○
8. ประสิทธิภาพการให้บริการโดยรวม	○	○	○	○	○
9. ความพึงพอใจของท่านต่อการให้บริการของสำนักดิจิทัลเทคโนโลยีวิทยาเขตสนามจันทร์	○	○	○	○	○

ส่ง

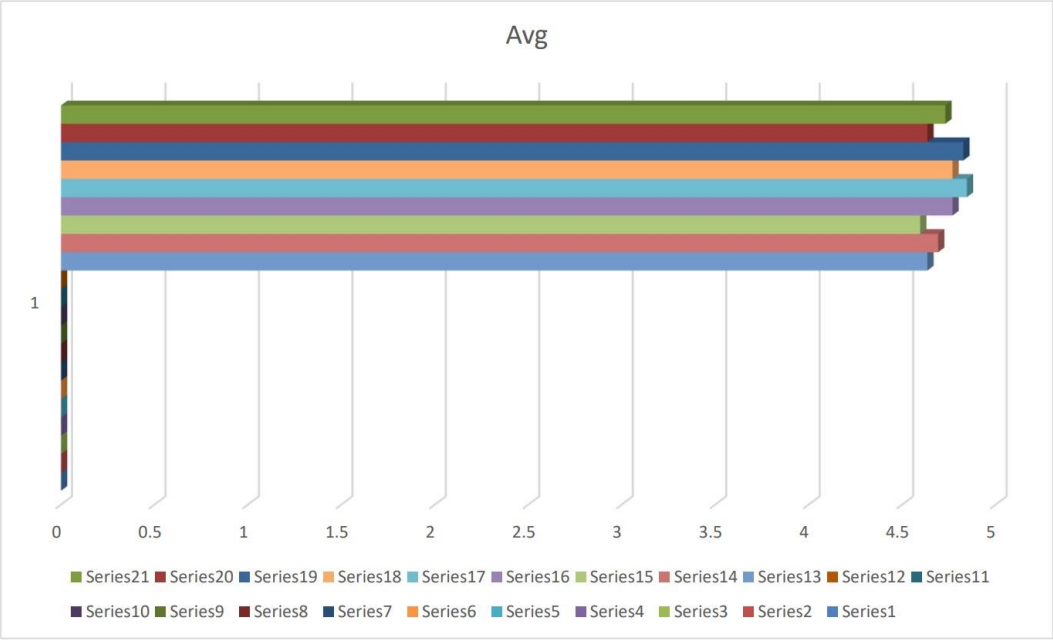
ล้างแบบฟอร์ม

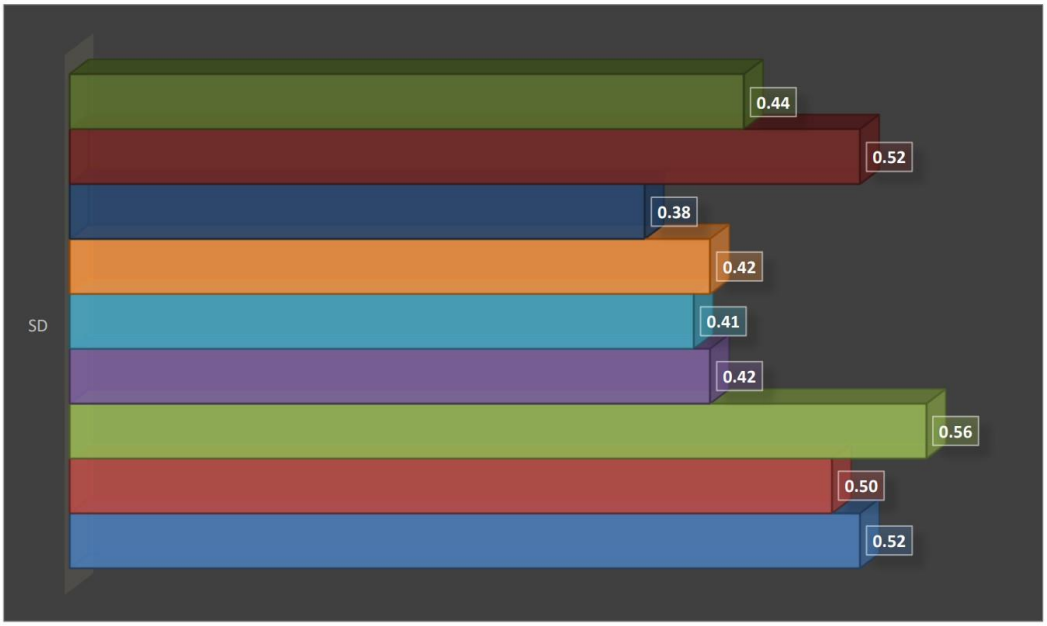
แบบประเมินความพึงพอใจ การปฏิบัติงานของบุคลากรศูนย์คอมพิวเตอร์

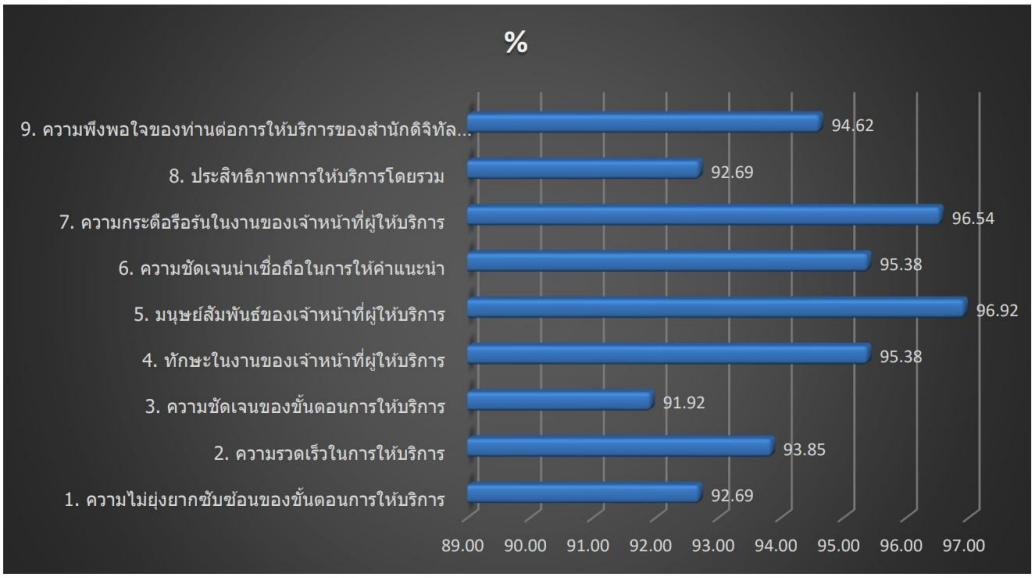
ผลการประเมิน (1 เมษายน 2564 – 30 กันยายน 2564)

คำชี้แจง ตอบคำถามลงในช่องระดับที่เป็นความจริงที่สุดในแต่ละหัวข้อ

รายการประเมิน	5	4	3	2	1	N	avg	SD	100	%
1. ความไม่ยุ่งยากซับซ้อนของขั้นตอนการให้บริการ	34	17	1	0	0	52	4.63	0.52	260	92.69
2. ความรวดเร็วในการให้บริการ	37	14	1	0	0	52	4.69	0.50	260	93.85
3. ความชัดเจนของขั้นตอนการให้บริการ	33	17	2	0	0	52	4.60	0.56	260	91.92
4. ทักษะในงานของเจ้าหน้าที่ผู้ให้บริการ	40	12	0	0	0	52	4.77	0.42	260	95.38
5. มนุษย์สัมพันธ์ของเจ้าหน้าที่ผู้ให้บริการ	45	6	1	0	0	52	4.85	0.41	260	96.92
6. ความชัดเจนน่าเชื่อถือในการให้คำแนะนำ	40	12	0	0	0	52	4.77	0.42	260	95.38
7. ความกระตือรือร้นในงานของเจ้าหน้าที่ผู้ให้บริการ	43	9	0	0	0	52	4.83	0.38	260	96.54
8. ประสิทธิภาพการให้บริการโดยรวม	34	17	1	0	0	52	4.63	0.52	260	92.69
9. ความพึงพอใจของท่านต่อการให้บริการของสำนักดิจิทัลเทคโนโลยี วิทยาเขตสนามจันทร์	38	14	0	0	0	52	4.73	0.44	260	94.62
sum	344	118	6	0	0	468	**4.72**	0.48	2340	94.44
%	73.5	25.2	1.28	0	0					
คะแนนเต็ม	2340	คะแนนที่ได้				2210				
คะแนนที่ได้เทียบกับคะแนนเต็ม(%)	94.44									



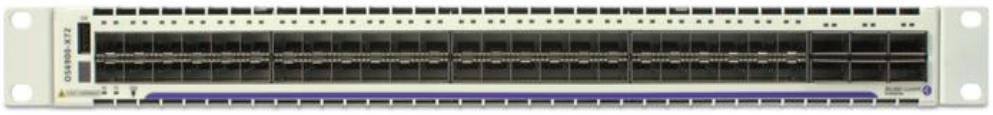

SD
0.44
0.52
0.38
0.42
0.41
0.42
0.56
0.50
0.52


%
9. ความพึงพอใจของท่านต่อการให้บริการของสำนักดิจิทัล...
8. ประสิทธิภาพการให้บริการโดยรวม
7. ความกระตือรือร้นในงานของเจ้าหน้าที่ผู้ให้บริการ
6. ความชัดเจนน่าเชื่อถือในการให้คำแนะนำ
5. มนุษย์สัมพันธ์ของเจ้าหน้าที่ผู้ให้บริการ
4. ทักษะในงานของเจ้าหน้าที่ผู้ให้บริการ
3. ความชัดเจนของขั้นตอนการให้บริการ
2. ความรวดเร็วในการให้บริการ
1. ความไม่ยุ่งยากซับซ้อนของขั้นตอนการให้บริการ
94.62
92.69
96.54
95.38
96.92
95.38
91.92
93.85
92.69
89.00
90.00
91.00
92.00
93.00
94.00
95.00
96.00
97.00

รายละเอียดการตั้งค่าอุปกรณ์กระจายสัญญาณเครือข่าย

ตามหลักการออกแบบเครือข่าย กรณีศึกษาหอพักนักศึกษา สนามจันทร์ ใช้หลักการออกแบบระบบเครือข่ายแบบลำดับชั้น (Hierarchical Network) หมายถึง การออกแบบโดยจัดกลุ่มอุปกรณ์ในเครือข่ายเป็นหลายกลุ่ม โดยเชื่อมต่อกันเป็นลำดับชั้นหรือเลเยอร์ มีรายละเอียดขั้นตอนการตั้งค่าอุปกรณ์กระจายสัญญาณเครือข่าย จำนวน 3 เลเยอร์ ดังนี้

1. Core Layer (Switch Alcatel 6900-X72)
2. Distribution Layer (Switch Alcatel 6860E-U28)
3. Access Layer (Switch Aruba 6100)



1. การตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่ายระดับ Core Layer (Alcatel 6900-X72) โดยใช้โปรแกรม Putty SSH ผ่านระบบเครือข่ายเข้าไปตั้งค่าอุปกรณ์ ดังนี้

1.1 สร้าง VLAN ของหอพักเพชรรัตน์ 1

1.1.1 สร้าง VLAN 1581 (PR1_Lan) สำหรับเชื่อมต่อสาย LAN คอมพิวเตอร์เจ้าหน้าที่หอพักเพชรรัตน์ 1

1.1.2 สร้าง VLAN 1591 (PR1_Device) สำหรับเชื่อมต่ออุปกรณ์ Switch และ Access point หอพักเพชรรัตน์ 1

-> vlan 1581 admin-state enable

-> vlan 1581 name “PR1_Lan”

-> vlan 1591 admin-state enable

-> vlan 1591 name “PR1_Device”

1.1.3 สร้าง ip interface VLAN 1581 และ VLAN 1591 เพื่อกำหนด ip address

-> ip interface “PR1_Lan” address 172.27.58.1 mask 255.225.255.224 vlan 1581

-> ip interface “PR1_Device” address 172.27.59.1 mask 255.255.255.224 vlan 1591

1.2 สร้าง VLAN ของหอพักเพชรรัตน์ 2

1.2.1 สร้าง VLAN 1582 (PR2_Lan) สำหรับเชื่อมต่อสาย LAN คอมพิวเตอร์เจ้าหน้าที่หอพักเพชรรัตน์ 2

1.2.2 สร้าง VLAN 1592 (PR2_Device) สำหรับเชื่อมต่ออุปกรณ์ Switch และ Access point หอพักเพชรรัตน์ 2

-> vlan 1582 admin-state enable

-> vlan 1582 name “PR2_Lan”

-> vlan 1592 admin-state enable

-> vlan 1592 name “PR2_Device”

1.2.3 สร้าง ip interface VLAN 1582 และ VLAN 1592 เพื่อกำหนด ip address

-> ip interface “PR2_Lan” address 172.27.58.33 mask 255.225.255.224 vlan 1582

-> ip interface “PR2_Device” address 172.27.59.33 mask 255.255.255.224 vlan 1592

1.3 สร้าง VLAN ของหอพักเพชรรัตน์ 3

1.3.1 สร้าง VLAN 1583 (PR3_Lan) สำหรับเชื่อมต่อสาย LAN คอมพิวเตอร์เจ้าหน้าที่หอพักเพชรรัตน์ 3

1.3.2 สร้าง VLAN 1593 (PR3_Device) สำหรับเชื่อมต่ออุปกรณ์ Switch และ Access point หอพักเพชรรัตน์ 3

-> vlan 1583 admin-state enable

-> vlan 1583 name “PR3_Lan”

-> vlan 1593 admin-state enable

-> vlan 1593 name “PR3_Device”

1.3.3 สร้าง ip interface VLAN 1583 และ VLAN 1593

-> ip interface “PR3_Lan” address 172.27.58.65 mask 255.225.255.224 vlan 1583

-> ip interface “PR3_Device” address 172.27.59.65 mask 255.255.255.224 vlan 1593

1.4 สร้าง VLAN ของหอพักเพชรรัตน์ 4

1.4.1 สร้าง VLAN 1584 (PR4_Lan) สำหรับเชื่อมต่อสาย LAN คอมพิวเตอร์เจ้าหน้าที่หอพักเพชรรัตน์ 4

1.4.2 สร้าง VLAN 1594 (PR4_Device) สำหรับเชื่อมต่ออุปกรณ์ Switch และ Access point หอพักเพชรรัตน์ 4

-> vlan 1584 admin-state enable

-> vlan 1584 name “PR4_Lan”

-> vlan 1594 admin-state enable

-> vlan 1594 name “PR4_Device”

1.4.3 สร้าง ip interface VLAN 1584 , 1594

-> ip interface “PR4_Lan” address 172.27.58.97 mask 255.225.255.224 vlan 1584

-> ip interface “PR4_Device” address 172.27.59.97 mask 255.255.255.224 vlan 1594

1.5 สร้าง VLAN ของหอพักเพชรรัตน์ 5

1.5.1 สร้าง VLAN 1585 (PR5_Lan) สำหรับเชื่อมต่อสาย LAN คอมพิวเตอร์เจ้าหน้าที่หอพักเพชรรัตน์ 5

1.5.2 สร้าง VLAN 1595 (PR5_Device) สำหรับเชื่อมต่ออุปกรณ์ Switch และ Access point หอพักเพชรรัตน์ 5

-> vlan 1585 admin-state enable

-> vlan 1585 name “PR5_Lan”

-> vlan 1595 admin-state enable

-> vlan 1595 name “PR5_Device”

1.5.3 สร้าง ip interface VLAN 1585 และ VLAN 1595

-> ip interface “PR5_Lan” address 172.27.58.129 mask 255.225.255.224 vlan 1585

-> ip interface “PR5_Device” address 172.27.59.129 mask 255.255.255.224 vlan 1595

1.6 สร้าง VLAN ของหอพักเพชรรัตน์ 6

1.6.1 สร้าง VLAN 1586 (PR6_Lan) สำหรับเชื่อมต่อสาย LAN คอมพิวเตอร์เจ้าหน้าที่หอพักเพชรรัตน์ 6

1.6.2 สร้าง VLAN 1596 (PR6_Device) สำหรับเชื่อมต่ออุปกรณ์ Switch และ Access point หอพักเพชรรัตน์ 6

-> vlan 1586 admin-state enable

-> vlan 1586 name “PR6_Lan”

-> vlan 1596 admin-state enable

-> vlan 1596 name “PR6_Device”

1.6.3 สร้าง ip interface VLAN 1586 , 1596

-> ip interface “PR6_Lan” address 172.27.58.161 mask 255.225.255.224 vlan 1586

-> ip interface “PR6_Device” address 172.27.59.161 mask 255.255.255.224 vlan 1596

1.7 ตั้งค่า Port 2/1/28 เป็น Port UP-Link ด้วยการตั้งค่า Tagged VLAN 4 ที่ Port 2/1/28 เพื่อเชื่อมต่อกับ Switch Alcatel 6860E-U28 Up-Link Port 1/1/19

-> vlan 4 members port 2/1/28 tagged

ใช้คำสั่งเพื่อตรวจสอบว่าการตั้งค่า vlan 4 ถูกต้องหรือไม่

```
-> show vlan member port 2/1/28
    vlan      type        status
    --------+-----------+---------------
     1    default       blocking
     4    qtagged     forwarding
```

1.8 ตั้งค่า Tagged VLAN ที่ต้องการใช้งานทั้งหมดไปยัง Port UP-Link 2/1/28 ของ Core Switch เพื่อเชื่อมต่อกับ Switch Alcatel 6860E-U28 Up-Link Port 1/1/19

```
-> vlan 4 member port 2/1/28 tagged
-> vlan 1581 member port 2/1/28 tagged
-> vlan 1591 member port 2/1/28 tagged
-> vlan 1582 member port 2/1/28 tagged
-> vlan 1592 member port 2/1/28 tagged
-> vlan 1583 member port 2/1/28 tagged
-> vlan 1593 member port 2/1/28 tagged
-> vlan 1584 member port 2/1/28 tagged
-> vlan 1594 member port 2/1/28 tagged
-> vlan 1585 member port 2/1/28 tagged
-> vlan 1595 member port 2/1/28 tagged
-> vlan 1586 member port 2/1/28 tagged
-> vlan 1596 member port 2/1/28 tagged
-> vlan 111 member port 2/1/28 tagged (su-roam-WiFi)
-> vlan 1127 member port 2/1/28 tagged (SU-WiFi)
-> vlan 2080 member port 2/1/28 tagged (eduroam-WiFi)
-> vlan 222 member port 2/1/28 tagged  (True-WiFi)
-> vlan 2517 member port 2/1/28 tagged (Dtac-WiFi)
-> vlan 2400 member port 2/1/28 tagged (Ais-WiFi)
```

หมายเหตุ กรณี VLAN 111 VLAN 1127 VLAN 2080 VLAN 222 VLAN 2517 VLAN 2400 ถูกสร้างที่ Core Switch ก่อนหน้านี้และใช้งานได้ปกติ

1.9 เมื่อ Tagged VLAN ทั้งหมดไปที่ Port 2/1/28 เสร็จแล้ว สามารถตรวจสอบความถูกต้องโดยใช้คำสั่ง show vlan member port 2/1/28 จะแสดงรายละเอียด ดังนี้

```
-> show vlan members port 2/1/28
 vlan     type       status
--------+-----------+---------------
    1    defaul      blocking
    4    qtagged     forwarding
  111    qtagged     forwarding
  222    qtagged     forwarding
 1127    qtagged     forwarding
 1581    qtagged     forwarding
 1582    qtagged     forwarding
 1583    qtagged     forwarding
 1584    qtagged     forwarding
 1585    qtagged     forwarding
 1586    qtagged     forwarding
 1591    qtagged     forwarding
 1592    qtagged     forwarding
 1593    qtagged     forwarding
 1594    qtagged     forwarding
 1595    qtagged     forwarding
 1596    qtagged     forwarding
 2080    qtagged     forwarding
 2400    qtagged     forwarding
```

2517 qtagged forwarding

1.10 การบันทึกการตั้งค่าอุปกรณ์ทั้งหมดของ Core Switch ลงตัวอุปกรณ์โดยใช้คำสั่ง

-> write memory flash-synchro

File /flash/working/vcsetup.cfg replaced.

Please wait...

File /flash/working/vcboot.cfg replaced.

->

2. การตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่ายระดับ Distribution Layer (Alcatel 6860E-U28) โดยใช้โปรแกรม Putty SSH ผ่านระบบเครือข่ายเข้าไปตั้งค่าอุปกรณ์ ดังนี้

2.1 สร้าง VLAN โดยกำหนดหมายเลข VLAN และตั้งชื่อ VLAN

-> vlan 1581 admin-state enable

-> vlan 1581 name "PR1_Lan"

-> vlan 1591 admin-state enable

-> vlan 1591 name "PR1_Device"

-> vlan 1582 admin-state enable

-> vlan 1582 name "PR2_Lan"

-> vlan 1592 admin-state enable

-> vlan 1592 name "PR2_Device"

-> vlan 1583 admin-state enable

```
-> vlan 1583 name "PR3_Lan"
-> vlan 1593 admin-state enable
-> vlan 1593 name "PR3_Device"
-> vlan 1584 admin-state enable
-> vlan 1584 name "PR4_Lan"
-> vlan 1584 name "PR4_Lan"
-> vlan 1594 admin-state enable
-> vlan 1594 name "PR4_Device"
-> vlan 1585 admin-state enable
-> vlan 1585 name "PR5_Lan"
-> vlan 1595 admin-state enable
-> vlan 1595 name "PR5_Device"
-> vlan 1586 admin-state enable
-> vlan 1586 name "PR6_Lan"
-> vlan 1596 admin-state enable
-> vlan 1596 name "PR6_Device"
-> vlan 111 admin-state enable
-> vlan 111 name "su-roam-WiFi"
-> vlan 1127 admin-state enable
-> vlan 1127 name "SU-WiFi"
-> vlan 2080 admin-state enable
-> vlan 2080 name "eduroam-WiFi"
-> vlan 222 admin-state enable
-> vlan 222 name "True-WiFi"
-> vlan 2400 admin-state enable
-> vlan 2400 name "Ais-WiFi"
```

-> vlan 2517 admin-state enable

-> vlan 2517 name "Dtac-WiFi"

2.2 กำหนด admin-key

-> ! Link Aggregate:

-> linkagg lacp agg 1 size 2 admin-state enable

-> linkagg lacp agg 1 name "Link to Backbone"

-> linkagg lacp agg 1 actor admin-key 5

-> linkagg lacp agg 2 size 2 admin-state enable

-> linkagg lacp agg 2 name "toPR1"

-> linkagg lacp agg 2 actor admin-key 101

-> linkagg lacp agg 3 size 2 admin-state enable

-> linkagg lacp agg 3 name "toPR2"

-> linkagg lacp agg 3 actor admin-key 102

-> linkagg lacp agg 4 size 2 admin-state enable

-> linkagg lacp agg 4 name "toPR3"

-> linkagg lacp agg 4 actor admin-key 103

-> linkagg lacp agg 5 size 2 admin-state enable

-> linkagg lacp agg 5 name "toPR4"

-> linkagg lacp agg 5 actor admin-key 104

-> linkagg lacp agg 6 size 2 admin-state enable

-> linkagg lacp agg 6 name "toPR5"

-> linkagg lacp agg 6 actor admin-key 105

-> linkagg lacp agg 7 size 2 admin-state enable

-> linkagg lacp agg 7 name "toPR6"

-> linkagg lacp agg 7 actor admin-key 106

2.3 กำหนด Port ให้ตรงกับ admin-key ที่กำหนด

-> linkagg lacp port 1/1/1 actor admin-key 101

-> linkagg lacp port 1/1/2 actor admin-key 102

-> linkagg lacp port 1/1/3 actor admin-key 103

-> linkagg lacp port 1/1/4 actor admin-key 104

-> linkagg lacp port 1/1/5 actor admin-key 105

-> linkagg lacp port 1/1/6 actor admin-key 106

-> linkagg lacp port 1/1/11 actor admin-key 101

-> linkagg lacp port 1/1/12 actor admin-key 102

-> linkagg lacp port 1/1/13 actor admin-key 103

-> linkagg lacp port 1/1/14 actor admin-key 104

-> linkagg lacp port 1/1/15 actor admin-key 105

-> linkagg lacp port 1/1/16 actor admin-key 106

-> ! VLAN:

2.4 กำหนดให้ Port 1/1/19 เป็น Port Up-Link ของตัว Switch Alcatel6860E-U28 เพื่อเชื่อมต่อกับ Backbone Switch Up-Link Port 2/1/28 โดยกำหนด VLAN ให้ไปยัง Port LinkAgg2 เชื่อมต่อไปยัง PR2 ที่กำหนดไว้

-> vlan 1581 members linkagg 2 tagged

-> vlan 1591 members linkagg 2 tagged

-> vlan 111 members linkagg 2 tagged

-> vlan 1127 members linkagg 2 tagged

-> vlan 2400 members linkagg 2 tagged

-> vlan 2517 members linkagg 2 tagged

-> vlan 222 members linkagg 2 tagged

ใช้คำสั่ง Show configuration snapshot เพื่อตรวจสอบการตั้งค่าอุปกรณ์ถูกต้องหรือไม่

```
vlan 111 members linkagg 2 tagged
vlan 222 members linkagg 2 tagged
vlan 1127 members port 1/1/19 tagged
vlan 1127 members linkagg 2 tagged
vlan 1581 members linkagg 2 tagged
vlan 1591 members linkagg 2 tagged
vlan 2400 members linkagg 2 tagged
vlan 2517 members linkagg 2 tagged
```

2.5 กำหนด ip interface ของ Vlan PR1-7_Device ซึ่งเป็น ip address สำหรับอุปกรณ์ Switch และ Access point ทั้ง 6 หอพัก

-> ip interface "PR1_Device" address 172.27.59.1 mask 255.255.255.224 vlan 1591 ifindex 2

-> ip interface "PR2_Device" address 172.27.59.33 mask 255.255.255.224 vlan 1592 ifindex3

-> ip interface "PR4_Device" address 172.27.59.97 mask 255.255.255.224 vlan 1594 ifindex4

-> ip interface "PR5_Device" address 172.27.59.129 mask 255.255.255.224 vlan 1595 ifindex5

-> ip interface "PR6_Device" address 172.27.59.161 mask 255.255.255.224 vlan 1596 ifindex6

-> ip interface "PR3_Device" address 172.27.59.65 mask 255.255.255.224 vlan 1593 ifindex 7

2.6 การบันทึกการตั้งค่าอุปกรณ์ทั้งหมดของ Core Switch ลงตัวอุปกรณ์โดยใช้คำสั่ง

-> write memory flash-synchro

File /flash/working/vcsetup.cfg replaced.

File /flash/working/vcboot.cfg replaced.

Please wait...

->

3. การตั้งค่าระดับ Access Layer (Switch Aruba 6100) โดยใช้โปรแกรม Putty SSH ผ่านระบบเครือข่ายเข้าไปตั้งค่าอุปกรณ์ ในขั้นตอนนี้เป็นตัวอย่างการตั้งค่าอุปกรณ์กระจายสัญญาณระบบเครือข่ายระดับ Access Layer ของหอพักเพชรรัตน์ 1

3.1 การตั้งค่า VLAN ของหอเพชรรัตน์ 1

```
6100# configure
6100(config)#
6100(config)# vlan 1581
6100(config-vlan-1581)# name PR1_Lan
6100(config)# vlan 1591
6100(config-vlan-1591)# name PR1_Device
6100(config-vlan-1591)#exit
6100(config)#
6100(config)# vlan 111
6100(config-vlan-111)# name su-roam-WiFi
6100(config-vlan-111)# exit
6100(config)# vlan 1127
6100(config-vlan-1127)# name SU-WiFi
6100(config-vlan-1127)# exit
6100(config)# vlan 222
6100(config-vlan-222)# name True-WiFi
6100(config-vlan-222)# exit
6100(config)# vlan 2400
```

6100(config-vlan-2400)# name Ais-WiFi

6100(config-vlan-2400)# exit

6100(config)# vlan 2517

6100(config-vlan-2517)# name Dtac-WiFi

6100(config-vlan-2517)#exit

6100(config)#

6100(config)#

```
6100(config)#
6100(config)# show vlan

--------------------------------------------------------------------------------------------------------------
VLAN  Name                                Status  Reason               Type      Interfaces
--------------------------------------------------------------------------------------------------------------
1     DEFAULT_VLAN_1                      down    no_member_forwarding  default   1/1/1-1/1/20,1/1/25-1/1/28,
                                                                                  lag2
4     suactive                            up      ok                    static    1/1/23-1/1/24,lag1
111   su-roam-WiFi                        down    no_member_port        static
222   True-WiFi                           down    no_member_port        static
1127  SU-WiFi                             down    no_member_port        static
1581  PR1_Lan                             down    no_member_port        static
1591  PR1_Device                          down    no_member_port        static
2400  Ais-WiFi                            down    no_member_port        static
2517  Dtac-WiFi                           down    no_member_port        static
6100(config)#
6100(config)#
```

3.2 การตั้งค่า Link agg

6100(config)#

6100(config)# interface 1/1/1

6100(config-if)# no shutdown

6100(config-if)# lag 2

6100(config-if)#

6100(config-if)# exit

6100(config)# interface 1/1/11

6100(config-if)# no shutdown

6100(config-if)# lag 2

6100(config-if)# exit

6100(config)#

3.3 การตั้งค่า VLAN ที่ต้องการให้กับ Port Lag2

6100(config)#

6100(config)# interface lag 2

6100(config-lag-if)# no shutdown

6100(config-lag-if)# vlan trunk native 1

6100(config-lag-if)# vlan trunk allowed 1591,111,222,1127,2400,2517

6100(config-lag-if)# lacp mode active

6100(config-lag-if)# exit

6100(config)#

ใช้คำสั่ง show running-config เพื่อตรวจสอบการตั้งค่า Lag2

```
interface lag 2
    no shutdown
    vlan trunk native 1
    vlan trunk allowed 111,222,1127,1591,2400,2517
    lacp mode active
```

3.4 การตั้งค่า IP route ,VLAN , ip Switch

6100(config)#

6100(config)# ip route 0.0.0.0/0 172.27.59.1

6100(config)#

6100(config)# interface vlan 1591

6100(config-if-vlan)# ip address 172.27.59.2/24

6100(config-if-vlan)#

3.4 การตั้งค่า Port สำหรับต่อสาย LAN เจ้าหน้าที่หอพัก

6100(config)#

6100(config)# interface 1/1/2

6100(config-if)# vlan access 1581

6100(config-if)# exit

6100(config)# interface 1/1/3

6100(config-if)# vlan access 1581

6100(config-if)# exit

6100(config)# interface 1/1/3

6100(config-if)# vlan access 1581

6100(config-if)# exit

6100(config)#

3.5 การตั้งค่า Port 12-13 สำหรับต่อ Access Point

6100#

6100# configure

6100(config)# interface 1/1/12

6100(config-if)# no shutdown

6100(config-if)# vlan trunk native 1591

6100(config-if)# vlan trunk allowed 111,222,1127,2400,2517

6100(config-if)#

6100(config-if)# exit

6100(config)# interface 1/1/13

6100(config-if)# no shutdown

6100(config-if)# vlan trunk native 1591

6100(config-if)# vlan trunk allowed 111,222.1127,2400,2517

Invalid input: 111,222.1127,2400,2517

6100(config-if)#

6100(config-if)# exit

6100(config)# interface 1/1/14

6100(config-if)# no shutdown

6100(config-if)# vlan trunk native 1591

6100(config-if)# vlan trunk allowed 111,222,1127,2400,2517

6100(config-if)# exit

6100(config)#

3.6 การตั้งค่า LinkAgg

6100#

6100# configure

6100(config)# interface lag 2

6100(config-lag-if)# no shutdown

6100(config-lag-if)# no shutdown

6100(config-lag-if)# lacp mode active

6100(config-lag-if)# lacp mode active

3.7 การบันทึกการตั้งค่าอุปกรณ์ทั้งหมดของ Access Switch ลงตัวอุปกรณ์โดยใช้คำสั่ง

6100P# write memory

Copying configuration: [Success]

BUREAU of DIGITAL