คู่มือปฏิบัติงานหลัก
เรื่อง
การดูแลระบบเครือข่ายอินเตอร์เน็ตอุปกรณ์เครือข่าย
การให้บริการซ่อมและติดตั้งแก้ไขระบบเครือข่ายอินเตอร์เน็ต

โดย
นาย สิทธิชัย กาบบัวลอย
พนักงานช่างเทคนิค ปฏิบัติงาน

สำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น
งานโครงสร้างพื้นฐานระบบดิจิทัล
พ.ศ.2568

คำนำ

ปัจจุบันระบบเครือข่ายอินเทอร์เน็ตมีบทบาทสำคัญอย่างยิ่งต่อการดำเนินงานในทุกภาคส่วน ไม่ว่าจะเป็นภาคธุรกิจ การศึกษา หรือการสื่อสารในชีวิตประจำวัน การดูแลรักษาและจัดการระบบเครือข่ายให้สามารถใช้งานได้อย่างมีประสิทธิภาพจึงเป็นสิ่งจำเป็น เพื่อให้สามารถตอบสนองความต้องการในการใช้งานได้อย่างต่อเนื่องและปลอดภัย

คู่มือปฏิบัติงานเล่มนี้ จัดทำขึ้นเพื่อศึกษาหลักการและแนวทางในการดูแลระบบเครือข่ายอินเทอร์เน็ต รวมถึงการให้บริการซ่อม ติดตั้ง และแก้ไขปัญหาที่เกิดขึ้นกับระบบเครือข่าย ที่ใช้งานตามคณะ/หน่วยงาน และหอพักนักศึกษา โดยเนื้อหาภายในจะครอบคลุมถึงอุปกรณ์เครือข่ายที่สำคัญ ขั้นตอนการวิเคราะห์ปัญหา รวมถึงแนวทางในการซ่อมแซมและบำรุงรักษา ทั้งนี้เพื่อเพิ่มพูนความรู้ความเข้าใจและสามารถนำไปประยุกต์ใช้ในสถานการณ์จริงได้อย่างเหมาะสม ยังเป็นประโยชน์ต่อหน่วยงานหรือองค์กรให้มีมาตรฐาน ในการทำงานเป็นองค์กรสมรรถนะสูง เพื่อสนับสนุนภารกิจของมหาวิทยาลัยขอนแก่น

ผู้จัดทำหวังเป็นอย่างยิ่งว่ารายงานฉบับนี้จะเป็นประโยชน์แก่ผู้อ่าน ไม่มากก็น้อย และขอขอบคุณทุกแหล่งข้อมูลและผู้ให้ความรู้ที่เป็นแรงสนับสนุนในการจัดทำครั้งนี้

สิทธิชัย กาบบัวลอย

เมษายน 2558

กิตติกรรมประกาศ

การจัดทำคู่มือปฏิบัติงานฉบับนี้เสร็จสมบูรณ์เป็นอย่างดี จึงขอขอบพระคุณ ผู้บริหารสำนักเทคโนโลยีดิจิทัลมหาวิทยาลัยขอนแก่น และรองผู้บริหารสำนักเทคโนโลยีดิจิทัลมหาวิทยาลัยขอนแก่นทุกฝ่ายที่สนับสนุนความก้าวหน้าแก่บุคลากรสายสนับสนุนทุกคน

ขอขอบพระคุณ อาจารย์กาญจนศรี สิงห์ภู่ (พยาบาลเชี่ยวชาญ ข้าราชการบำนาญ อดีตกรรมการสภา มหาวิทยาลัยขอนแก่น/ปัจจุบันผู้ทรงคุณวุฒิคณะกรรมการบริหารงานบุคคลประจำมหาวิทยาลัย กาฬสินธุ์) ที่ได้ถ่ายทอดความรู้และให้คำแนะนำในการจัดทำคู่มือปฏิบัติงานแก่ข้าพเจ้าจนสำเร็จลุล่วง ไปได้ด้วยดี

อนึ่ง ผู้จัดทำหวังว่า คู่มือฉบับนี้จะมีประโยชน์อยู่ไม่น้อย จึงขอมอบส่วนดี ทั้งหมดนี้ให้แก่เหล่าคณาจารย์ที่ได้ประสิทธิประสาทวิชาจนทำให้คู่มือฉบับนี้เป็น ประโยชน์ต่อผู้ที่เกี่ยวข้องและขอมอบความกตัญญูกตเวทิตาคุณ แด่บิดา มารดา และผู้มี พระคุณทุกท่าน สำหรับข้อบกพร่องต่าง ๆ ที่อาจจะเกิดขึ้นนั้น ผู้จัดทำน้อมรับผิดเพียง ผู้เดียว และยินดีที่จะรับฟังคำแนะนำจากทุกท่านที่ได้เข้ามาศึกษา เพื่อเป็นประโยชน์ในการพัฒนาต่อไป

สิทธิชัย กาบบัวลอย

เมษายน 2558

สารบัญ

สารบัญแผนภูมิ

บทที่ 1
บทนำ

1.1 ความสำคัญและความเป็นมาของปัญหา

มหาวิทยาลัยขอนแก่น ก่อตั้งขึ้นในปี 2508 เป็นสถาบันอุดมศึกษาแห่งแรกของภาคตะวันออกเฉียงเหนือ ต่อมาในปี พ.ศ 2558 มหาวิทยาลัยขอนแก่น ได้ปรับเปลี่ยนสถานภาพจากมหาวิทยาลัยที่เป็นส่วนราชการไปเป็น “มหาวิทยาลัยในกำกับของรัฐ มีฐานะเป็นนิติบุคคล” สังกัด กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม ตามพระราชบัญญัติมหาวิทยาลัยขอนแก่น พ.ศ. 2558 และประกาศในราชกิจจานุเบกษา เมื่อวันที่ 17 กรกฎาคม พ.ศ. 2558 ทั้งนี้เพื่อให้การบริหารมหาวิทยาลัยเป็นไปอย่างมีประสิทธิภาพและสนองตอบต่อสภาวะการณ์เปลี่ยนแปลงของสังคม โดยให้มีบทบาทหน้าที่ ในการผลิตบัณฑิต การวิจัย การบริการวิชาการ การบริหารจัดการองค์กร การทำนุบำรุงศิลปะวัฒนธรรม และมีการแบ่งส่วนงานภายในมหาวิทยาลัยขอนแก่น ดังนี้ (1) สำนักงานสภามหาวิทยาลัย (2) สำนักงานอธิการบดี (3) สำนักงานวิทยาเขต (4) คณะ (5) วิทยาลัย (6) สถาบัน (7) สำนัก มหาวิทยาลัยอาจให้มีส่วนงานที่เรียกชื่ออย่างอื่นที่มีฐานะเทียบเท่าคณะ วิทยาลัย สถาบันหรือสำนัก เพื่อดำเนินการตามบทบาทหน้าที่ของมหาวิทยาลัย มีแผนยุทธศาสตร์การบริหารมหาวิทยาลัยขอนแก่น พ.ศ. 2563 – 2566 โดยได้กำหนดการพัฒนามหาวิทยาลัยออกเป็น 3 ด้าน 11 ยุทธศาสตร์ ได้แก่ เสาหลักที่ 1 (People) ด้านการส่งมอบคุณค่าแก่ประชาคม หรือผู้มีส่วนได้ส่วนเสียของมหาวิทยาลัย ประกอบด้วย 4 ยุทธศาสตร์ เสาหลักที่ 2 (Ecological) ด้านระบบนิเวศของมหาวิทยาลัย ประกอบด้วย 5 ยุทธศาสตร์ เสาหลักที่ 3 (Spiritual) : ด้านการปลูกฝังจิตวิญญาณความเป็นมหาวิทยาลัยขอนแก่น ประกอบด้วย 2 ยุทธศาสตร์ นอกจากนั้น ยังมีแผนปฏิบัติการประจำปี ที่ได้จัดทำขึ้นภายใต้แผนยุทธศาสตร์การบริหารมหาวิทยาลัยขอนแก่น พ.ศ. 2563 – 2566 เพื่อใช้เป็นกรอบในการจัดทำแผนงาน/โครงการต่างๆ ภายในมหาวิทยาลัยขอนแก่น พร้อมทั้งใช้เป็นเครื่องมือ และกลไกสำคัญในการบริหารงาน/โครงการ การสื่อสารและการถ่ายทอดแนวปฏิบัติให้คณะ/ส่วนงานต่างๆ ภายในมหาวิทยาลัยขอนแก่น ซึ่งจะทำให้การดำเนินงานตามแผนงาน/โครงการต่างๆ ทั่วทั้งมหาวิทยาลัยเป็นไปในทิศทางเดียวกัน อันจะส่งผลให้การดำเนินการตามแผนยุทธศาสตร์การบริหารมหาวิทยาลัยขอนแก่น พ.ศ. 2563 – 2566 และแผนปฏิบัติการประจำปี ของมหาวิทยาลัยขอนแก่น บรรลุผลสำเร็จตามวิสัยทัศน์ พันธกิจ เป้าประสงค์ เป้าหมายเชิงยุทธศาสตร์และเชิงกลยุทธ์ตามที่กำหนดไว้ และสอดคล้องกับเจตนารมย์การจัดตั้งมหาวิทยาลัยขอนแก่น ต่อไป

สำนักเทคโนโลยีดิจิทัล เดิมชื่อ “ศูนย์คอมพิวเตอร์” จัดตั้งขึ้นเมื่อ พ.ศ. 2528 และได้เปลี่ยนชื่อเป็น สำนักเทคโนโลยีสารสนเทศ เมื่อปี พ.ศ. 2558 และได้รับอนุมัติจากสภาพมหาวิทยาลัยขอนแก่นให้เปลี่ยนชื่ออีกครั้ง เป็น “สำนักเทคโนโลยีดิจิทัล” เมื่อ พ.ศ. 2563 ตามประกาศมหาวิทยาลัยขอนแก่น (ฉบับที่

241/2563) เรื่องการจัดตั้งส่วนงานของมหาวิทยาลัยขอแก่น (ฉบับที่ 4) พ.ศ. 2563 เป็นส่วนงานที่สนองนโยบายและเสาหลักการพัฒนา ด้านระบบนิเวศของมหาวิทยาลัย (Ecological) และยุทธศาสตร์ ด้านการปรับเปลี่ยนองค์กรให้ก้าวเข้าสู่ยุคดิจิทัล (Digital Transformation) ให้การสนับสนุนการดำเนินภารกิจของคณะ/ส่วนงานต่างๆ ทั่วทั้งมหาวิทยาลัยขอนแก่น รวมไปถึงหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับมหาวิทยาลัยขอนแก่น โดยมีบทบาทหน้าที่ให้บริการโครงสร้างพื้นฐานระบบดิจิทัล บริการระบบงานดิจิทัล บริการระบบสื่อสารโทรคมนาคมในรูปแบบ IP Phone บริการข้อมูลในระบบสารสนเทศ บริการห้องปฏิบัติการคอมพิวเตอร์และเครื่องคอมพิวเตอร์เพื่อการจัดการเรียนการสอน การทดสอบด้วยระบบอิเล็กทรอนิกส์ (e-exam) การฝึกอบรมทางด้านเทคโนโลยีดิจิทัล การจัดประชุมและการบริการทางวิชาการอื่นๆ บริการถ่ายทอดความรู้ด้านเทคโนโลยีดิจิทัล พัฒนาระบบฐานข้อมูลสารสนเทศและแอปพลิเคชันสำหรับการบริหารงานมหาวิทยาลัย วิจัยและพัฒนานวัตกรรมทางด้านเทคโนโลยีดิจิทัลให้ทันสมัยและก้าวทันเทคโนโลยี เพื่อสนับสนุนพันธกิจหลักของมหาวิทยาลัยทั้งด้านการเรียนการสอน การวิจัย การบริการวิชาการ การบริหารจัดการองค์กร และการทำนุบำรุงศิลปวัฒนธรรม รวมไปถึงเพื่อสนับสนุนการขับเคลื่อนแผนยุทธศาสตร์การบริหารมหาวิทยาลัยขอนแก่น พ.ศ. 2563 – 2566 และแผนปฏิบัติการประจำปี มหาวิทยาลัยขอนแก่น ให้บรรลุผลสำเร็จตามวิสัยทัศน์ พันธกิจ เป้าประสงค์ เป้าหมายเชิงยุทธศาสตร์และเชิงกลยุทธ์ตามที่กำหนดไว้ ปัจจุบันได้แบ่งโครงสร้างการบริหารงานออกเป็น 3 งาน ประกอบด้วย (1) งานอำนวยการ (2) งานโครงสร้างพื้นฐานระบบดิจิทัล (3) งานวิจัยและพัฒนาระบบดิจิทัล โดยมีผู้อำนวยการเป็นผู้บริหารสูงสุด และมีคณะกรรมการประจำสำนักเทคโนโลยีดิจิทัลเป็นผู้กำหนดนโยบายและกำกับติดตามการบริหารงาน มีบทบาทหน้าที่ในการตอบสนอง

งานโครงสร้างพื้นฐานระบบดิจิทัล ซึ่งเป็นส่วนงานสนับสนุนและส่งเสริมให้การพัฒนาและบริการทางด้านเทคโนโลยีดิจิทัล เป็นไปอย่างมีประสิทธิภาพ และบรรลุผลสำเร็จตามนโยบายและเป้าหมายที่กำหนดไว้ พร้อมทั้งสามารถตอบสนองต่อความต้องการของผู้รับบริการได้อย่างเต็มที่และเป็นไปอย่างทั่วถึง มีเครือข่ายแกนหลักทั้งด้าน Network & Wi-Fi ที่มีศักยภาพสูงขึ้นรองรับกับการใช้งานที่หลากหลายทั้งในด้านปริมาณและความต้องการที่แตกต่างกันของกลุ่มผู้รับบริการ มีการพัฒนาโครงสร้างพื้นฐานทางด้านระบบเครือข่ายอินเทอร์เน็ต ทั้งด้าน Hardware & Software เพื่อให้สามารถรองรับการพัฒนาและการใช้งานเทคโนโลยีใหม่ๆในรูปแบบดิจิทัลมากขึ้น ทั้งโดยการประยุกต์ใช้ทรัพยากร ทางเทคโนโลยีเดิมที่มีอยู่ และการพัฒนาขึ้นใหม่ มีการบูรณาการการใช้ทรัพยากรทางเทคโนโลยีร่วมกันทั่วทั้งมหาวิทยาลัย มีการพัฒนาระบบสารสนเทศขึ้นหลายระบบ ซึ่งมีทั้งส่วนที่พัฒนาขึ้นเองและส่วนที่ร่วมกับคณะ/ส่วนงานอื่นๆ เพื่อใช้งานทั้งในระดับมหาวิทยาลัยและระดับคณะ/ส่วนงาน โดยจะมีการปรับปรุงให้ระบบสามารถใช้งานได้ในรูปแบบDigital Workflow และบูรณาการข้อมูลที่ออกจากระบบไปสู่การพัฒนาให้เป็นระบบ ERP (Enterprise Resource Planning) ในโอกาสต่อไป

จากความสำคัญและความเป็นมาของปัญหาดังกล่าวข้างต้น ผู้จัดทำ พนักงานช่างเทคนิค (ผู้ขอตำแหน่งที่สูงขึ้น) จึงได้จัดทำคู่มือปฏิบัติงาน เรื่อง “การปฏิบัติงาน โดยใช้ความรู้ความสามารถ ทักษะการปฏิบัติงานที่ต้องทำการศึกษา ค้นคว้า ทดลอง วิเคราะห์ ทางด้านระบบเครือข่ายอินเตอร์เน็ตและการสื่อสาร มีหน้าที่ดูแลระบบเครือข่ายและอุปกรณ์เครือข่ายที่ใช้งานตามคณะ/หน่วยงาน และหอพักนักศึกษา มหาวิทยาลัยขอนแก่น

1.2 วัตถุประสงค์ในการจัดทำคู่มือ

1.2.1 เพื่อใช้เป็นแนวทางในการปฏิบัติงานของบุคลากร สำนักเทคโนโลยีดิจิทัล ให้เป็นมาตรฐานเดียวกัน

1.2.2 เพื่อให้เป็นคู่มือขั้นตอนการดูแลตรวจซ่อมติดตั้ง ระบบเครือข่าย และบำรุงรักษาอุปรกรณ์เครือข่าย ให้เข้าใจง่าย สำหรับเจ้าหน้าที่ ช่างเทคนิค และผู้เกี่ยวข้องในการปฏิบัติงาน

1.2.3 เพื่อบริการระบบเครือข่ายอินเตอร์เน็ตให้เกิดประโยชน์สูงสุดและมีประสิทธิภาพ

1.2.4 เพื่อศึกษา ค้นคว้า ทดลอง วิเคราะห์ ความก้าวหน้าของเทคโนโลยีระบบเครือข่ายทั้งระบบฮาร์ดแวร์และซอฟต์แวร์

1.2.5 เพื่อลดปัญหาและความเสี่ยงที่อาจจะเกิดขึ้นในการปฏิบัติงาน

1.2.6 เพื่อให้ผู้ปฏิบัติงานและผู้รับบริการมีความพึงพอใจระดับสูง

1.2.7 เพื่อเป็นเอกสารประกอบในการศึกษาดูงานของบุคลากรในสายงานที่เกี่ยวข้อง และฝึกปฏิบัติงานของนักศึกษาทั้งภายในและภายนอกมหาวิทยาลัยขอนแก่น

1.2.8 เพื่อใช้เผยแพร่ไปยังหน่วยงานอื่น ทั้งภายในและภายนอกมหาวิทยาลัยขอนแก่น ที่มีลักษณะงานใกล้เคียงกัน

1.3 ขอบเขตการใช้คู่มือ

1.3.1 ใช้ในการปฏิบัติงานบริการ ติดตั้งแก้ไข ตรวจซ่อมระบบเครือข่ายและบำรุงรักษาอุปกรณ์เครือข่าย สำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น

1.3.2 ใช้สำหรับดำเนินงานในส่วนของ งานโครงสร้างพื้นฐานระบบดิจิทัล ภายใต้ความรับผิดชอบของ สำนักเทคโนโลยีดิจิทัล

1.3.3 ใช้สำหรับดำเนินงานในส่วนของ คณะ/หน่วยงานภายในมหาวิทยาลัยขอนแก่น

1.3.4 ใช้สำหรับในการดำเนินงาน ติดตั้งระบบเครือข่าย ตามคณะหน่วยงาน หอพักนักศึกษา มหาวิทยาลัยขอนแก่น

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1.4.1 ได้คู่มือในการปฏิบัติงาน
เรื่อง การดูแลระบบเครือข่าย การบำรุงรักษาอุปกรณ์เครือข่าย การติดตั้งอุปกรณ์เครือข่ายในการใช้งาน ให้มีประสิทธิภาพสูงสุด

1.4.2 เพื่อเพิ่มประสิทธิภาพในการให้บริการระบบเครือข่ายคอมพิวเตอร์ให้มีความเสถียรและมีประสิทธิภาพให้กับมหาวิทยาลัยขอนแก่น

1.4.3 มีการศึกษา และออกแบบระบบเครือข่ายอินเตอร์เน็ตสำหรับคณะ/หน่วยงาน ให้มีความเหมาะสมและเกิดประสิทธิภาพสูงสุดให้กับมหาวิทยาลัยขอนแก่น ให้เป็นมาตรฐานเดียวกันและเป็นเครื่องมือในการมอบหมายงาน

1.4.4 ติดตั้ง ตรวจสอบและแก้ไขปัญหา ระบบเครือข่าย ตามที่รับแจ้ง ภายในคณะ/หน่วยงาน เพื่อให้ระบบเครือข่ายสามารถทำงานได้อย่างต่อเนื่อง ทันตามเวลาที่กำหนด

1.4.5 เป็นแบบอย่างในการพัฒนาเทคโนโลยีดิจิทัล ให้กับคณะ/หน่วยงาน

1.4.6 ความพึงพอใจของผู้ใช้งาน ในการติดตั้ง ตรวจสอบและแก้ไขปัญหาตามคณะ/หน่วยงาน ได้อย่างมีประสิทธิภาพ

1.4.7 สามารถนำไปขอเลื่อนตำแหน่งวิชาการที่สูงขึ้น ได้แก่ ตำแหน่งระดับชำนาญงาน

1.4.8 เพื่อให้ผู้ปฏิบัติงานและผู้รับบริการมีความพึงพอใจระดับสูงขึ้น

1.5 คำนิยามศัพท์

- มหาวิทยาลัย หมายถึง มหาวิทยาลัยขอนแก่น
- หน่วยงาน หมายถึง สำนักเทคโนโลยีดิจิทัล
- ผู้บริหาร หมายถึง ผู้อำนวยการสำนักเทคโนโลยีดิจิทัล
- หัวหน้างาน หมายถึง หัวหน้างานในสังกัดสำนักเทคโนโลยีดิจิทัล
- บุคลากร หมายถึง ข้าราชการ พนักงานมหาวิทยาลัย ข้าราชการ ลูกจ้างประจำ ลูกจ้างของมหาวิทยาลัย

- ซอฟต์แวร์ (Software) หมายถึง ชุดของโปรแกรมคอมพิวเตอร์และข้อมูลที่เกี่ยวข้องที่อยู่ในรูปแบบที่สามารถให้คอมพิวเตอร์ทำงานตามคำสั่งหรือคำขอที่ผู้ใช้กำหนดได้ โดยซอฟต์แวร์มีหลายประเภทที่สนับสนุนการทำงานของคอมพิวเตอร์และเพิ่มประสิทธิภาพของการใช้งานด้านคอมพิวเตอร์ต่างๆ ได้
- ADSL Modem หมายถึง อุปกรณ์ในการเชื่อมต่อกับระบบเครือข่าย ผ่านสายโทรศัพท์ สามารถใช้งานได้เครื่องเดียว
- ADSL Router
  หมายถึง อุปกรณ์ในการเชื่อมต่อกับระบบเครือข่าย ผ่านสายโทรศัพท์ แต่สามารถแชร์อินเตอร์เน็ตได้ทั้งในรูปแบบเชื่อมต่อผ่านสาย LAN และแบบไร้สายหรือ Wireless
- AP (Access Point)
  เป็นอุปกรณ์เน็ตเวิร์คที่ใช้สำหรับการกระจายสัญญาณ ทำหน้าที่เหมือนกับ Switch ของระบบเครือข่าย แต่ AP เป็นแบบไร้สาย ตัวอย่างที่เราเห็นได้ชัดๆ ตามบ้านก็คือ อุปกรณ์ ADSL Modem / ADSL Router ที่เราใช้อยู่ทั่วไป
- ฮาร์ดแวร์ (Hardware) หมายถึง อุปกรณ์อิเล็กทรอนิกส์ที่สามารถสัมผัสและมองเห็นได้ โดยตรง ฮาร์ดแวร์เป็นส่วนที่กำหนดลักษณะกายภาพและคุณสมบัติของอุปกรณ์, มีหน้าที่ประมวลผลข้อมูล, เก็บข้อมูล และทำให้ระบบทำงานได้
- Broadcast SSID
  หมายถึง การอนุญาติให้มีกระจายหรือเผยแพร่ชื่อ SSID หรือชื่อ AP (Access Point) ทั้งนี้เพื่อให้เราสามารถเชื่อมต่อได้อย่างถูกต้อง
- DHCP (Dynamic Host Configuration Protocal) Server
  หมายถึง เครื่อง Server ที่ให้บริการจากหมายเลขไอพี หรือ IP Address แบบอัตโนมัติให้กับคอมพิวเตอร์ที่เชื่อมต่อเข้ามาผ่าน TCP/IP ส่วนใหญ่จะพบได้กับการใช้งานอุปกรณ์ AP (Access Point)

- IP Address (Internet Protocol Address)
  หมายถึง หมายเลขของอุปกรณ์เน็ตเวิร์ค ไม่ว่าจะเป็น LAN Card, Wi-Fi, ADSL Router สำหรับ IP Address จะประกอบด้วยตัวเลขสี่ชุด เช่น 192.168.1.20 เป็นต้น ซึ่งหมายเลข IP Address นี้จะไม่สามารถซ้ำกันได้ใน Network เดียวกัน
- Mac Address
  หมายถึง หมายเลขประจำตัวของอุปกรณ์ทางด้านเน็ตเวิร์ค โดยหมายเลขนี้จะไม่มีวันซ้ำกันโดยเด็ดขาด ตัวอย่าง หมายเลข Mac Address มีดังนี้ 00-1B-FC-66-CF-09 เป็นต้น
- SSID (Service Set Identifier)
  หมายถึง การตั้งชื่อให้กับอุปกรณ์ไร้สายมาตราฐาน 802.11 เพื่อใช้สำหรับการเชื่อมต่อ พูดง่ายๆ ส่วนใหญ่ใช้สำหรับการตั้งชื่อของ AP (Access Point) ของเรานั่นเอง
- VPN (Virtual Private Network)
  หมายถึง ระบบที่ใช้สำหรับการเน็ตเวิร์คแบบส่วนตัว หรือพูดให้เข้าใจง่ายๆ คือ เป็นการสร้างท่อในการสื่อสารระหว่างคอมพิวเตอร์ผ่านทางระบบ เน็ตเวิร์คแบบไร้สาย การใช้งานจะต้องใช้โปรแกรมในการสร้าง VPN ขึ้นมา
- WEP (Wired Equivalent Privacy) Encryption
  หมายถึง มาตราฐานในการเข้ารหัสความปลอดภัย โดยเฉพาะกับการใช้งานในระบบเครือข่ายไร้สาย หรือ Wi-Fi ซึ่งผลก็คือ การจะใช้งานจะต้องมีการใส่รหัสผ่านในการเข้าถึงเสียก่อน อย่างไรก็ตาม WEP Encryption นี้ ยังมีระดับความปลอดภัยไม่สูงมากนัก และไม่แนะนำให้ใช้
- Wi-Fi (Wireless Fidelity)
  หมายถึง ผลิตภัณฑ์ที่สามารถใช้งานร่วมกับระบบเครือข่ายไร้สาย ซึ่งอยู่บนมาตราฐาน IEEE 802.11 ปัจจุบัน เราจะเห็นอุปกรณ์โมบายต่างๆ มี Wi-Fi เป็นมาตราฐาน เพื่อใช้สำหรับการเชื่อมต่อกับระบบเครือข่ายโดยเฉพาะ
- WPA (Wi-Fi Protected Access)
  หมายถึง มาตราฐานในการเข้ารหัสความปลอดภัย ที่ผ่านอีกขั้นจาก WEP ในเรื่องของการเข้ารหัสและการถอดรหัส
- WPA2
  หมายถึง มาตราฐานในการเข้ารหัสความปลอดภัย ที่พัฒนาเพิ่มเติมมาจาก WPA เวอร์ชั่นแรก รองรับการเข้าถึงระดับ 192-bit และ 256-bit ซึ่งถือได้ว่าเป็นมาตราฐานในการตั้งรหัสผ่านที่ใช้กันอยู่แพร่หลายในปัจจุบัน
- Network หมายถึงระบบเครือข่ายโทรคมนาคมที่มีการเชื่อมโยงกับคอมพิวเตอร์ และอุปกรณ์อิเล็กทรอนิกส์อื่นๆ ตั้งแต่ 2 เครื่องขึ้นไปเป็นเครือข่ายหลากหลายขนาด ซึ่งระบบ Network เป็น

ระบบที่ใช้เพื่อการสื่อสาร เชื่อมต่อแลกเปลี่ยน รับส่งข้อมูล และควบคุมอุปกรณ์ต่างๆ ที่อยู่ใน Network หรือเครือข่ายนั้นๆ ปัจจุบันเครือข่าย Network ที่ใหญ่ที่สุดคือ เครือข่ายอินเทอร์เน็ต

- Bridge เปรียบเสมือนสะพานที่ช่วยในการเชื่อมต่อเครือข่ายทั้ง 2 เครือข่าย ที่เป็นเครือข่ายชนิดเดียวเข้าด้วยกัน ถ้ามีจุดเด่นที่สามารถช่วยกรองข้อมูลของเครือข่ายเท่าที่จำเป็น และยังเป็นการลดปริมาณข้อมูลเครือข่ายประเภท ได้อีกด้วย
- Switch เป็นอุปกรณ์ตัวกลาง ที่ทำหน้าที่กระจายสัญญาณการสื่อสารให้กับอุปกรณ์อื่นๆ ผ่านสายแลนหรือใยแก้วนำแสง ซึ่งจะช่วยให้การทำงานของเครือข่ายมีความเสถียร ทั่วถึง ปลอดภัย และรวดเร็วขึ้น เนื่องจากไม่มีการแบ่งความเร็วตามจำนวนช่องสัญญาณเหมือนฮับ และมีช่วยป้องกันการรับส่งข้อมูลระหว่างอุปกรณ์สองเครื่องจากการขัดขวางอุปกรณ์อื่นๆ ในเครือข่ายเดียวกัน เพื่อป้องกันโอกาสที่ข้อมูลส่วนตัวจะรั่วไหลไปในเครือข่ายอื่นได้
- Local Area Network หรือ LAN คือ ระบบเครือข่ายแบบ Ethernet ที่มีการเชื่อมต่อในระยะทางที่จำกัดมีความเร็วของแลกเปลี่ยนข้อมูลอยู่ที่ระหว่าง 1-100 Mbps ทั้งนี้ความเร็วของการแลกเปลี่ยนข้อมูลยังขึ้นอยู่กับปัจจัยที่เกี่ยวข้องด้วย เช่น ตัวกลาง ข้อกำหนดของผู้บริการ เป็นต้น ซึ่ง LAN มีทั้งแบบเครือข่ายที่มีขนาดเล็ก หรือขนาดใหญ่ก็ได้ มีตั้งแต่ผู้ใช้งานในการเชื่อมต่อเพียงรายเดียว ไปจนถึงผู้ใช้งานจำนวนมาก โดย LAN จะนิยมใช้ในอาคารสำนักงาน อินเทอร์เน็ตโรงเรียนโรงพยาบาล เน็ตองค์กร เป็นต้น ซึ่งระบบ LAN ยังสามารถแบ่งออกได้อีก 6 ประเภท ได้แก่ Bus, Star, Ring, Mesh, Tree และ Hybrid
- Server คือ ผู้ให้บริการในเครือข่าย Network โดย Server เปรียบเสมือนคอมพิวเตอร์สาขาใหญ่ที่ดูแลจัดการเมื่อมีผู้มาขอใช้บริการ Server ก็จะทำการจัดการข้อมูล จัดการโปรแกรม หรือสิ่งที่ต้องการไปยังระบบของผู้ใช้ให้ถูกต้อง

บทที่ 2
โครงสร้างและหน้าที่รับผิดชอบ

2.1 วิสัยทัศน์ พันธกิจ และเป้าหมายขององค์กร

2.1.1 วิสัยทัศน์

เป็นองค์กรชั้นนำในการปรับเปลี่ยนวิธีการพัฒนาและการจัดการองค์กรด้วยเทคโนโลยีดิจิทัล

2.1.2 พันธกิจ

1) พัฒนาโครงสร้างพื้นฐานด้านดิจิทัลให้พร้อมต่อการใช้งาน
2) วิจัยและพัฒนาระบบดิจิทัลให้มีความทันสมัยและก้าวทันเทคโนโลยี
3) บริการระบบสื่อสารโทรคมนาคม
4) บริการระบบสารสนเทศและแอปพลิเคชั่น
5) บริการคอมพิวเตอร์เพื่อการเรียนการสอน การปฏิบัติงานและการบริการวิชาการอื่นๆ
6) บริการถ่ายทอดความรู้ทางด้านเทคโนโลยี

2.1.3 เป้าหมายขององค์กร

1) ยุทธศาสตร์ที่ 1 ปรับเปลี่ยนระบบการให้บริการทางเทคโนโลยีให้ก้าวเข้าสู่ยุคดิจิทัล

เป้าหมายเชิงกลยุทธ์ : พัฒนากลไกทางด้านเทคโนโลยีเพื่อสนับสนุนให้มหาวิทยาลัยมีการเปลี่ยนผ่านองค์กรไปสู่ยุคดิจิทัลอย่างเต็มรูปแบบ

เป้าหมายเชิงกลยุทธ์ :
1. มีความสามารถในการรับ – ส่งข้อมูลอยู่ที่ 30,000 คน/ครั้ง
2. มีความสามารถในการประมวลผลบนระบบเครือข่ายอินเทอร์เน็ต (การจัดการข้อมูลในระบบ) อยู่ที่ 99.50%
3. สัญญาณอินเทอร์เน็ตในเส้นทางหลักสามารถใช้งานอย่างมีประสิทธิภาพในระดับ 99.50%
4. ปลอดภัย 100% จากการโจมตีระบบในทุกรูปแบบ เช่น การเข้าถึงที่ไม่ได้รับอนุญาต, ไวรัส
5. มีนวัตกรรมทางด้านเทคโนโลยีดิจิทัลอย่างน้อย 1 ระบบ

2) ยุทธศาสตร์ที่ 2 ขับเคลื่อนการพัฒนาองค์กรด้วยเทคโนโลยีดิจิทัล

เป้าหมายเชิงยุทธศาสตร์ : ปรับเปลี่ยนระบบงานของสำนักเทคโนโลยีดิจิทัล ให้เป็น รูปแบบออนไลน์ และเป็นต้นแบบให้องค์กรอื่นนำไปใช้

เป้าหมายเชิงกลยุทธ์ : 1. บุคลากรร้อยละ 90 มีสมรรถนะในการปรับปรุงและพัฒนาทางด้านเทคโนโลยี รวมไปถึงสามารถใช้เทคโนโลยีเป็นเครื่องมือในการปฏิบัติงานได้อย่างมีประสิทธิภาพ

2. มีการปรับปรุงและพัฒนาระบบหรือกลไกการปฏิบัติงานขององค์กรเพื่อผลัก 2.4 เป้าหมายและเชิงยุทธศาสตร์และกลยุทย์

3) ยุทธศาสตร์ที่ 3 ปรับเปลี่ยนระบบการให้บริการทางเทคโนโลยีให้ก้าวเข้าสู่ยุคดิจิทัล

เป้าหมายเชิงยุทธศาสตร์ : พัฒนากลไกทางด้านเทคโนโลยีเพื่อสนับสนุนให้ มหาวิทยาลัยมีการเปลี่ยนผ่านองค์กรไปสู่ยุคดิจิทัลอย่างเต็มรูปแบบ

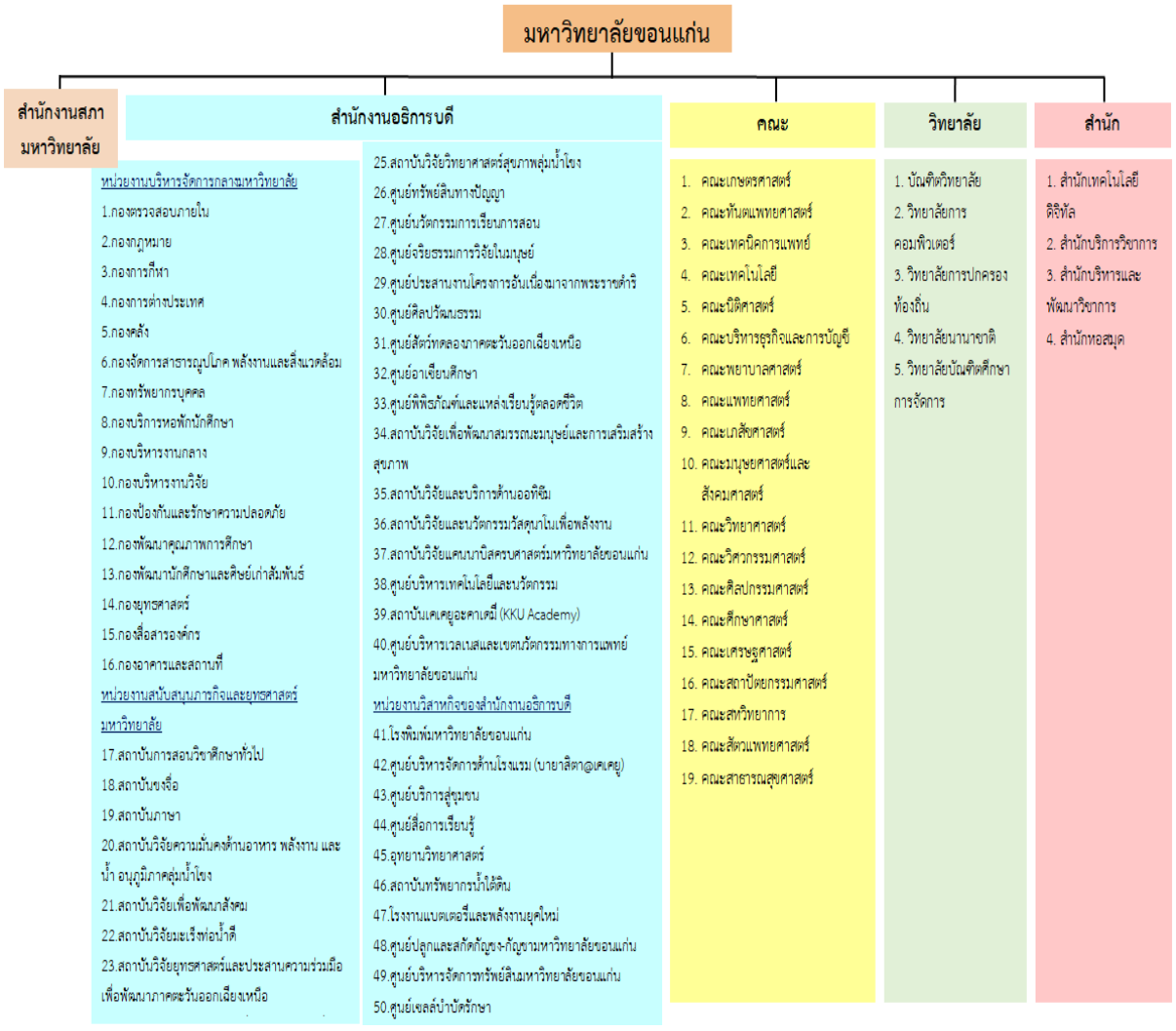
เป้าหมายเชิงกลยุทธ์ :
1. มีความสามารถในการรับ - ส่งข้อมูลอยู่ที่ 30,000 คน/ครั้ง
2. มีความสามารถในการประมวลผลบนระบบเครือข่ายอินเทอร์เน็ต (การจัดการข้อมูลในระบบ) อยู่ที่ 99.50%
3. สัญญาณอินเทอร์เน็ตในเส้นทางหลักสามารถใช้งานอย่างมีประสิทธิภาพในระดับ 99.50%
4. ปลอดภัย 100% จากการโจมตีระบบในทุกรูปแบบ เช่น การเข้าถึงที่ไม่ได้รับอนุญาต, ไวรัส
5. มีนวัตกรรมทางด้านเทคโนโลยีดิจิทัลอย่างน้อย 1 ระบบ
6. ดันให้กระบวนการดิจิทัลทรานฟอร์เมชั่นประสบผลสำเร็จอย่างน้อย 2 ระบบ

รูปที่ 1 แนวนโยบายของผู้บริหารสำนักเทคโนโลยีดิจิทัล

(ที่มา: สำนักเทคโนโลยีดิจิทัล, 2567)

2.2 โครงสร้างส่วนงานและอัตรากำลังของมหาวิทยาลัยขอนแก่น

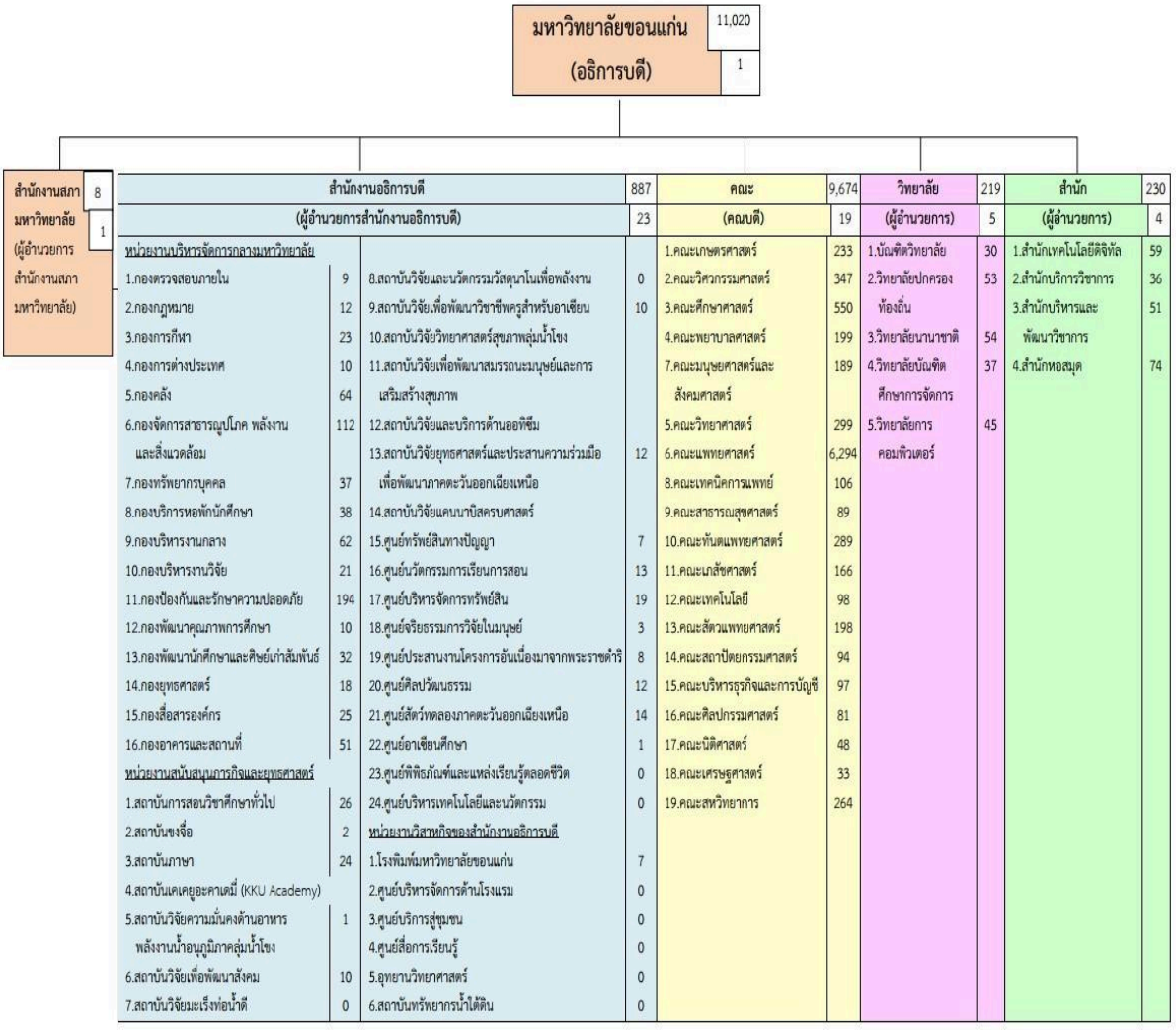
แผนภูมิที่ 1 แสดงโครงสร้างส่วนงานมหาวิทยาลัยขอนแก่น



ข้อมูล ณ ตุลาคม 2566

ที่มา : https://th.kku.ac.th/organizations/ ,2023

แผนภูมิที่ 2 แสดงโครงสร้างอัตรากำลังมหาวิทยาลัยขอนแก่น

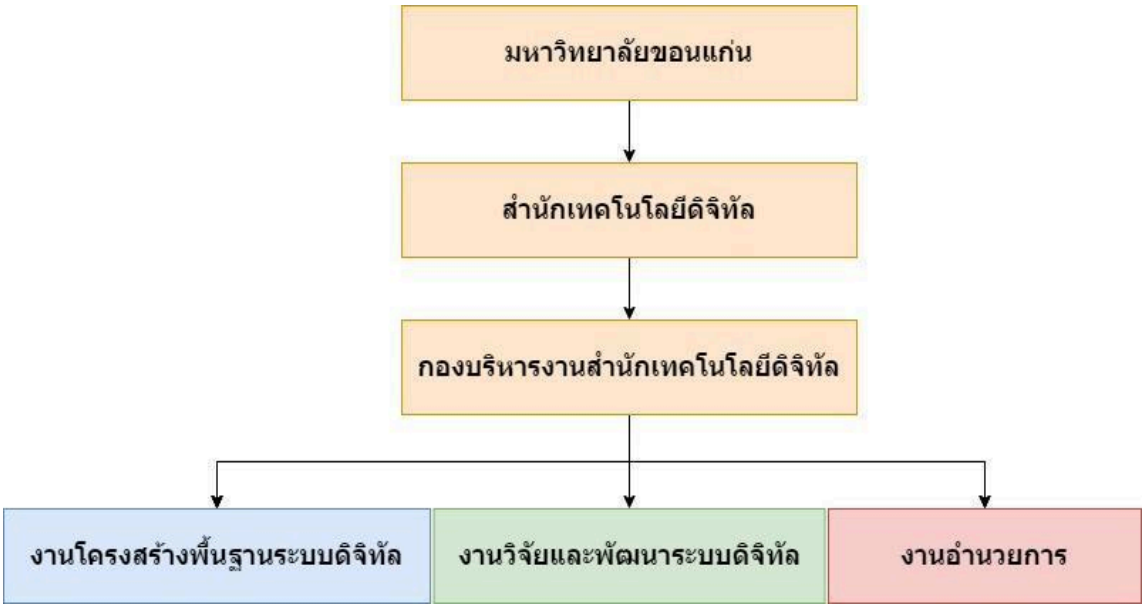


หมายเหตุ : ✶ หมายถึง ส่วนงานผู้ขอกำหนดตำแหน่งสูงขึ้น

(ที่มา : มหาวิทยาลัยขอนแก่น, 2566)

2.3 โครงสร้างส่วนงานและอัตรากำลังของสำนักเทคโนโลยีดิจิทัล

แผนภูมิที่ 3 แสดงโครงสร้างหน่วยงานสำนักเทคโนโลยีดิจิทัล



หมายเหตุ : ✶ หมายถึง หน่วยงานผู้ขอกำหนดตำแหน่งสูงขึ้น

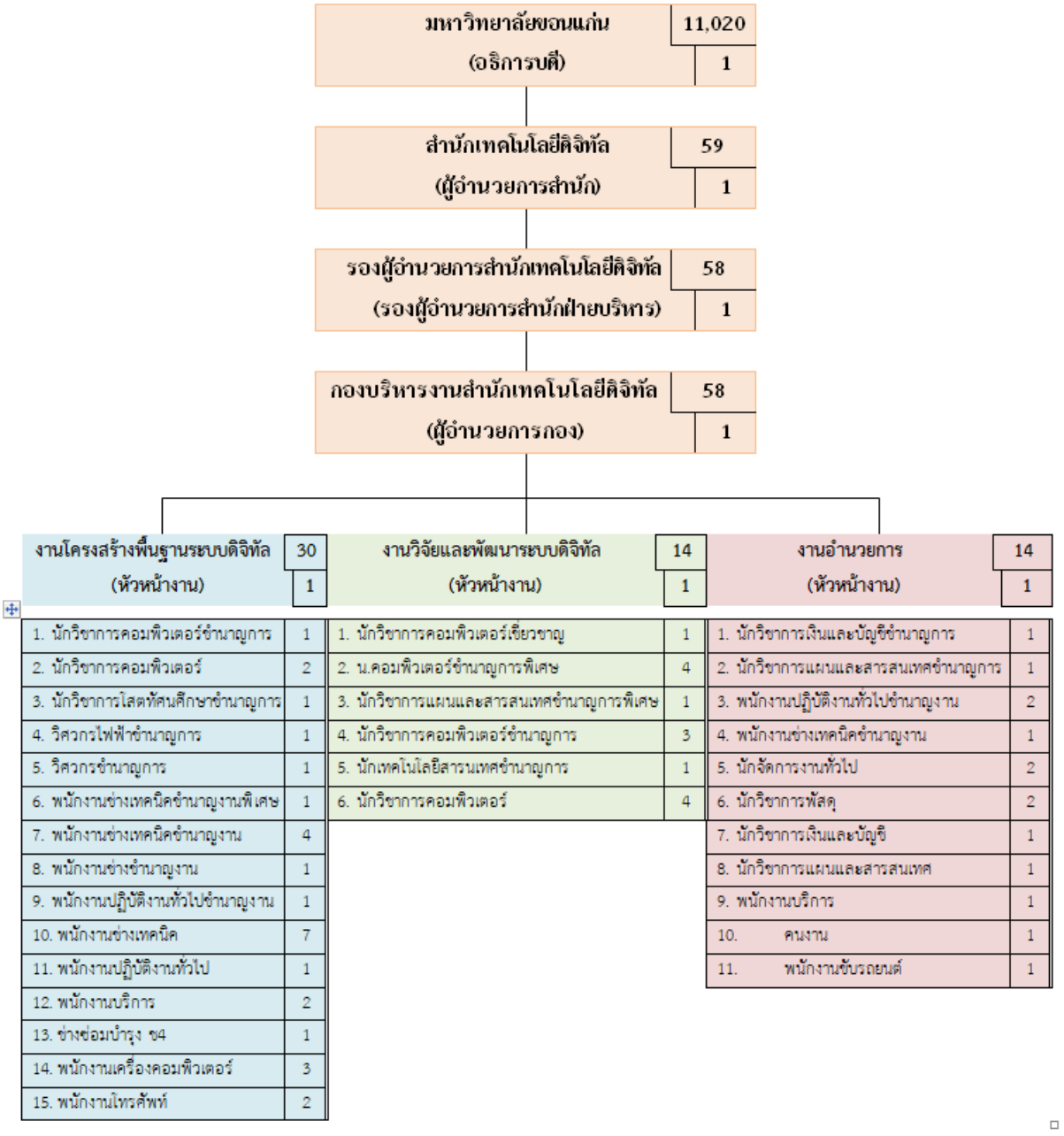
(ที่มา : สำนักเทคโนโลยีดิจิทัล, 2566)

แผนภูมิที่ 4 แสดงโครงสร้างภารกิจสำนักเทคโนโลยีดิจิทัล

หมายเหตุ : ✶ หมายถึง ภารกิจของผู้ขอกำหนดตำแหน่งสูงขึ้น

(ที่มา : สำนักเทคโนโลยีดิจิทัล, 2566)

แผนภูมิที่ 5 แสดงโครงสร้างอัตรากำลังสำนักเทคโนโลยีดิจิทัล



หมายเหตุ : ✶ หมายถึง ตำแหน่งผู้ขอกำหนดตำแหน่งสูงขึ้น

(ที่มา : สำนักเทคโนโลยีดิจิทัล, 2566)

2.4. งานโครงสร้างพื้นฐานระบบดิจิทัล

1. ภารกิจบริการเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ต

1. เครือข่ายคอมพิวเตอร์ (KKU e-Campus Network) ดูแลระบบเครือข่ายอินเทอร์เน็ตของมหาวิทยาลัยขอนแก่น ดูแลระบบ Wireless และอุปกรณ์ต่อพ่วง ติดตั้งระบบ FTTx และเชื่อมต่อสัญญาณอินเทอร์เน็ต จัดการระบบเครือข่ายใยแก้วนำแสงและเครือข่ายไร้สาย ทั้งระบบหลักและระบบสำรอง ให้สามารถใช้งานได้ตลอดและครอบคลุมพื้นที่ในมหาวิทยาลัย
2. ระบบ Routing Protocol และ Gateway ได้แก่ OSPF, BGP, EGP, RIP, EIGRP และ ISIS ดูแล ปรับปรุง แก้ไข การตั้งค่าอุปกรณ์เครือข่ายต่าง ๆ ที่ทำงานในระดับ Layer 3 Switch และ Layer 2 Switch
3. เครือข่าย UniNet ในภาคตะวันออกเฉียงเหนือตอนบนแก่สถาบันอุดมศึกษา
4. แม่ข่ายคอมพิวเตอร์ (Internet Application Service, LDAP, DNS, WINS, DHCP, Proxy) ดูแลเครื่องแม่ข่าย Hyper Converged (PVE) ดูแลระบบเครื่องแม่ข่ายแบบ Hyper convergent Infrastructure (HCI) บริหารการทรัพยากรที่เหมาะสมให้กับงานวิจัยและพัฒนาต่าง ๆ เช่น การประมวลผล AI การแสดงภาพบนแผนที่ หรือ การประผลภาพ และพัฒนาระบบการกู้คืนระบบในกรณีฉุกเฉิน และพัฒนามาตรฐานขั้นตอนการปฏิบัติงาน
5. แม่ข่ายระบบถ่ายทอดสัญญาณผ่านระบบเครือข่ายคอมพิวเตอร์ บริการถ่ายทอดสดการประชุมวิชาการ การอบรม การเรียนการสอน หรือพิธีการที่สำคัญๆ ของทางมหาวิทยาลัย ทั้งแบบ Wire และ Wireless

2.4.1 บุคลากรกลุ่มภารกิจบริการเครือข่ายคอมพิวเตอร์ งานโครงสร้างพื้นฐานระบบดิจิทัล

สำนักเทคโนโลยีดิจิทัล

นายศรีนคร	พงษ์สุวรรณ	ช่างเครื่องคอมพิวเตอร์ชำนาญงาน (หัวหน้ากลุ่มภารกิจ)
นางสาวสุรนุช	สัพโส	นักวิชาการคอมพิวเตอร์ชำนาญการ
นายวณัช	พาดี	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
นายไพโรจน์	นิกรสังขพินิจ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
นายสรพงษ์	นาเมืองจันทร์	พนักงานช่างเทคนิค ชำนาญงาน
นายพงศกร	หัตถพนม	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
นายไพฑูรย์	ภูกองชนะ	ช่างเครื่องคอมพิวเตอร์

นายสิทธิชัย	กาบบัวลอย	ช่างเทคนิคปฏิบัติงาน
นายชัชวาล	อินทร์พามา	ช่างเทคนิคปฏิบัติงาน
นายกรกต	ศิริพัฒน์	ช่างเทคนิคปฏิบัติงาน
นายเอกวัตร	โคช่วย	พนักงานเครื่องคอมพิวเตอร์

2.5 ภาระหน้าที่ความรับผิดชอบของผู้ขอกำหนดตำแหน่งสูงขึ้น

ปฏิบัติงานในฐานะ ผู้ปฏิบัติงานระดับต้นที่ต้องใช้ความรู้ความสามารถทางพนักงานช่างเทคนิค ให้บริการด้านการดูแลระบบเครือข่ายอินเตอร์เน็ต อุปกรณ์เครือข่าย สายสัญญาณต่อพวง ให้บริการซ่อมและติดตั้งแก้ไขระบบเครือข่ายอินเตอร์เน็ต ดูแลระบบ Wireless ของมหาวิทยาลัยขอนแก่น ติดตั้งระบบ FTTx และเชื่อมต่อสัญญาณอินเทอร์เน็ต จัดการระบบเครือข่ายใยแก้วนำแสงและเครือข่ายไร้สาย ทั้งระบบหลักและระบบสำรอง ให้สามารถใช้งานได้ตลอดและครอบคลุมพื้นที่ในมหาวิทยาลัย
งานที่ปฏิบัติในด้านต่างๆ

2.5.1 ด้านการปฏิบัติงานตามตำแหน่ง การดูแลระบบเครือข่ายอินเตอร์เน็ตสำหรับคณะ/หน่วยงาน/หอพักนักศึกษา

1. มีการศึกษาและออกแบบระบบเครือข่ายอินเตอร์เน็ตสำหรับคณะ/หน่วยงาน ให้มีความเหมาะสมและเกิดประสิทธิภาพสูงสุดโดยครอบคลุมกิจกรรมหลักดังนี้

1.1 การศึกษาและวิเคราะห์ความต้องการ

- ศึกษาและทำความเข้าใจลักษณะการใช้งานอินเตอร์เน็ตของบุคลากร, นักศึกษา รวมถึงความต้องการเฉพาะของแต่ละกลุ่ม เช่น ปริมาณการใช้งานข้อมูล, ความเร็วที่ต้องการ, ความจำเป็นในการเข้าถึงระบบงานภายในหรือภายนอก, การใช้งาน Wi-Fi ในพื้นที่ต่างๆ
- วิเคราะห์ความต้องการด้านเครือข่ายของระบบของคณะ/หน่วยงาน (เช่น ระบบห้องปฏิบัติการ, ระบบห้องออฟฟิศ, ระบบการเรียนการสอน, ระบบ VDO Conference เพื่อให้แน่ใจว่าเครือข่ายสามารถรองรับการทำงานได้อย่างราบรื่น
- ประเมินสภาพเครือข่ายปัจจุบัน รวมถึงปัญหาที่พบ, ข้อจำกัด, และจุดที่ต้องปรับปรุง เพื่อใช้เป็นข้อมูลในการออกแบบ

1.2 การวิจัยและคัดเลือกเทคโนโลยี

- ศึกษาเทคโนโลยีและอุปกรณ์เครือข่ายที่ทันสมัยและเหมาะสมกับงบประมาณและความต้องการ เช่น มาตรฐาน Wi-Fi ล่าสุด, อุปกรณ์ Switch/Router ที่มีคุณสมบัติเพียงพอ, ระบบรักษาความปลอดภัยเครือข่าย (เช่น Firewall) เทคโนโลยีสายสัญญาณ (Fiber Optic, UTP)

- เปรียบเทียบข้อดีข้อเสียของแต่ละเทคโนโลยีและผลิตภัณฑ์ เพื่อคัดเลือกสิ่งที่เหมาะสมที่สุดสำหรับสภาพแวดล้อมของคณะ/หน่วยงาน

1.3 การออกแบบโครงสร้างระบบเครือข่าย

- ออกแบบผัง (Topology) เครือข่ายทั้งแบบใช้สาย (Wired) และไร้สาย (Wireless) ให้เหมาะสมกับพื้นที่ทางกายภาพและการใช้งาน โดยพิจารณาถึงการกระจายจุดเชื่อมต่อ (Access Points), การวางตำแหน่งอุปกรณ์หลัก
- วางแผนการจัดสรรและบริหารจัดการ Bandwidth เพื่อให้มีการใช้งานทรัพยากรเครือข่ายอย่างมีประสิทธิภาพและเพียงพอสำหรับผู้ใช้งานทุกกลุ่ม
- ออกแบบระบบการกำหนดและบริหารจัดการเลขหมาย IP (IP Address) ให้เป็นระเบียบและง่ายต่อการจัดการ
- ออกแบบโครงสร้างด้านความปลอดภัยของเครือข่าย เช่น การแบ่งแยกเครือข่ายย่อย (VLAN) เพื่อควบคุมการเข้าถึง, การกำหนดนโยบายความปลอดภัยบนอุปกรณ์เครือข่าย
- พิจารณาการออกแบบเพื่อรองรับการขยายตัวในอนาคต และความสามารถในการทำงานต่อเนื่อง สำหรับระบบที่สำคัญ

1.4 การบูรณาการกับเครือข่ายหลักของมหาวิทยาลัย/ส่วนกลาง/คณะ/หน่วยงาน

- ออกแบบการเชื่อมต่อและบูรณาการระบบเครือข่ายภายในคณะ/หน่วยงานเข้ากับโครงสร้างพื้นฐานและนโยบายของเครือข่ายหลักของมหาวิทยาลัยหรือส่วนกลาง เพื่อให้การเชื่อมต่อเป็นไปอย่างราบรื่นและเป็นไปตามมาตรฐาน

  เป้าหมายสูงสุด ของหน้าที่นี้คือการสร้างระบบเครือข่ายอินเตอร์เน็ตสำหรับคณะ/หน่วยงาน ที่ ตอบสนองความต้องการ ของผู้ใช้งานและระบบงานได้อย่างครบถ้วน มี ความเสถียร สูง มี ความปลอดภัย ที่ดี มี ประสิทธิภาพ ในการรับส่งข้อมูล และใช้ทรัพยากรและ งบประมาณ อย่าง คุ้มค่า ที่สุด พร้อมรองรับการเติบโตในอนาคต

2. ดูแลการปรับปรุง บำรุงรักษา อุปกรณ์ Switch Layer 2 เพื่อทดแทนอุปกรณ์ที่ชำรุด สำหรับคณะ/หน่วยงาน

ช่างเทคนิคผู้ดูแลระบบทำหน้าที่ดูแลรักษาและจัดการอุปกรณ์เครือข่ายพื้นฐาน (Switch Layer 2) ที่ใช้งานภายในคณะ/หน่วยงาน เพื่อให้มั่นใจว่าระบบเครือข่ายมีเสถียรภาพ ทำงานได้อย่างต่อเนื่อง และรองรับการใช้งานได้อย่างมีประสิทธิภาพ โดยมีขอบเขตดังนี้

2.1 การเฝ้าระวังและตรวจสอบสถานะ

- เฝ้าระวังการทำงานของอุปกรณ์ Switch Layer 2 อย่างสม่ำเสมอ เช่น ตรวจสอบสถานะไฟแสดง, สัญญาณ, อุณหภูมิ, การใช้งาน CPU/Memory ผ่านระบบ Monitoring
- ตรวจสอบ Log และข้อความแจ้งเตือน (Alert) จากอุปกรณ์ เพื่อระบุปัญหาที่อาจเกิดขึ้นหรือความผิดปกติในการทำงานเบื้องต้น

2.2 การบำรุงรักษาเชิงป้องกัน

- ดำเนินการตามแผนการบำรุงรักษาเชิงป้องกัน เช่น การอัปเดต Firmware ของอุปกรณ์ตามความเหมาะสม เพื่อแก้ไข Bug, ปรับปรุงประสิทธิภาพ, หรือเสริมสร้างความปลอดภัย
- สำรองข้อมูล Configuration ของอุปกรณ์อย่างสม่ำเสมอ เพื่อให้สามารถกู้คืนค่าเดิมได้อย่างรวดเร็วหากเกิดปัญหา

2.3 การแก้ไขปัญหาและวินิจฉัยความผิดปกติ

- รับแจ้งปัญหาที่เกี่ยวข้องกับอุปกรณ์ Switch Layer 2 จากผู้ใช้งานหรือระบบ Monitoring
- ดำเนินการแก้ไขปัญหาเบื้องต้น เช่น การตรวจสอบสายสัญญาณ, การ Restart พอร์ต, การตรวจสอบค่า Configuration
- วินิจฉัยสาเหตุของปัญหาที่เกิดขึ้นกับอุปกรณ์อย่างละเอียด เพื่อระบุว่าอุปกรณ์ชำรุดหรือไม่และควรดำเนินการซ่อมแซมหรือเปลี่ยนทดแทน

2.4 การจัดการอุปกรณ์ชำรุดและเปลี่ยนทดแทน

- ตรวจเช็คและสำรวจอุปกรณ์ Switch Layer 2 ที่ชำรุดหรือทำงานผิดปกติจนไม่สามารถซ่อมแซมได้ หรือคุ้มค่าที่จะเปลี่ยนใหม่
- ดำเนินการตามขั้นตอนการเบิก/จัดหา/จัดซื้ออุปกรณ์ Switch Layer 2 ตัวใหม่เพื่อนำมาเปลี่ยนทดแทนอุปกรณ์ที่ชำรุด โดยประสานงานกับฝ่ายจัดซื้อหรือทำแผนจัดซื้อตามปีงบประมาณ
- วางแผนและดำเนินการติดตั้งอุปกรณ์ Switch Layer 2 ตัวใหม่แทนตัวที่ชำรุด โดยคำนึงถึงผลกระทบต่อผู้ใช้งานให้น้อยที่สุด
- ตั้งค่า Configuration บนอุปกรณ์ Switch Layer 2 ตัวใหม่ให้เหมือนหรือเทียบเท่ากับอุปกรณ์เดิม หรือตามนโยบายเครือข่ายที่กำหนด เพื่อให้ระบบกลับมาทำงานได้ตามปกติ

- ทดสอบการทำงานของอุปกรณ์และเครือข่ายหลังการเปลี่ยน เพื่อยืนยันว่าสามารถใช้งานได้ตามปกติ

2.5 การจัดการอุปกรณ์เก่าที่ชำรุด

- ดำเนินการปลดระวาง อุปกรณ์ Switch Layer 2 ที่ชำรุดอย่างถูกต้องตามขั้นตอน
- ประสานงานเพื่อส่งคืนอุปกรณ์ชำรุดสำหรับการซ่อมแซม หรือการจำหน่าย/บริจาคทรัพย์สินตามระเบียบของมหาวิทยาลัย

เป้าหมายสูงสุด ของหน้าที่นี้คือ การรักษา ความต่อเนื่อง และ ความเสถียร ของระบบเครือข่ายอินเตอร์เน็ตภายในคณะ/หน่วยงาน โดยการจัดการกับอุปกรณ์ Switch Layer 2 ที่ชำรุดอย่างรวดเร็วและมีประสิทธิภาพ พร้อมทั้งดำเนินการบำรุงรักษาเชิงป้องกันเพื่อลดโอกาสการเกิดปัญหาในอนาคต

3. ดูแลการจัดทำระบบ มอนิเตอร์ สำหรับตรวจสอบปัญหา

ช่างเทคนิค ผู้ดูแลระบบทำหน้าที่รับผิดชอบในการวางแผน จัดตั้ง ดูแลรักษา และใช้ประโยชน์จากระบบเฝ้าระวัง Monitoring สำหรับโครงสร้างพื้นฐานเครือข่ายอินเทอร์เน็ตภายในคณะ/หน่วยงาน เพื่อให้สามารถตรวจจับ วินิจฉัย และแก้ไขปัญหาที่เกิดขึ้นได้อย่างรวดเร็วและมีประสิทธิภาพ รวมถึงการนำข้อมูลที่ได้ไปใช้ในการปรับปรุงและวางแผนในอนาคต โดยมีขอบเขตดังนี้:

3.1 การวางแผนและคัดเลือกระบบ

- ประเมินความต้องการและขอบเขตในการเฝ้าระวังของเครือข่ายภายในคณะ/หน่วยงาน (เช่น อุปกรณ์ใดบ้างที่ต้องเฝ้าระวัง, ระดับความละเอียดของข้อมูลที่ต้องการ)
- ศึกษา คัดเลือก หรือพิจารณาระบบ Monitoring System ที่เหมาะสมกับความต้องการ งบประมาณ และสภาพแวดล้อมของคณะ/หน่วยงาน (อาจเป็น Open Source หรือ Commercial)

3.2 การติดตั้งและตั้งค่าเริ่มต้น

- ดำเนินการติดตั้งซอฟต์แวร์หรือฮาร์ดแวร์ของระบบ Monitoring System
- ตั้งค่าการเข้าถึงอุปกรณ์เครือข่าย เช่น SNMP, ICMP, SSH/Telnet เพื่อให้ระบบสามารถดึงข้อมูลสถานะได้
- กำหนดค่าเบื้องต้นสำหรับอุปกรณ์หลักที่ต้องการเฝ้าระวัง เช่น Switch Layer 2, Access Point, Server ที่เกี่ยวข้องกับเครือข่าย

3.3 การกำหนดค่าและปรับปรุงการเฝ้าระวัง

- กำหนดค่าต่างในระบบที่ต้องการเฝ้าระวังสำหรับอุปกรณ์แต่ละประเภท เช่น Bandwidth Utilization, CPU/Memory Load, Port Status, Error Rates, Packet Loss, Latency
- ตั้งค่าการแจ้งเตือน (Alerting) ไปยังช่องทางที่กำหนด เช่น Email, SMS, Dashboard และระบุผู้รับผิดชอบเมื่อเกิดการแจ้งเตือนประเภทต่างๆ
- ปรับปรุงและเพิ่มเติมรายการอุปกรณ์ที่ต้องเฝ้าระวังอย่างต่อเนื่องตามการเปลี่ยนแปลงของเครือข่าย
- ปรับจูนค่า เกณฑ์ต่างๆ และเงื่อนไขการแจ้งเตือนให้เหมาะสม เพื่อเพิ่มประสิทธิภาพในการตรวจจับปัญหาจริง

3.4 การเฝ้าระวังและตอบสนองต่อการแจ้งเตือน

- เฝ้าติดตาม Dashboard ของระบบ Monitoring เพื่อดูสถานะสุขภาพโดยรวมของเครือข่ายแบบ Real-time
- รับและตรวจสอบการแจ้งเตือนที่ได้รับจากระบบ Monitoring
- วินิจฉัยปัญหาเบื้องต้นจากข้อมูลที่แสดงในระบบ Monitoring เมื่อได้รับการแจ้งเตือน
- ดำเนินการแก้ไขปัญหาตามที่ได้รับแจ้งหรือจากข้อมูลในระบบ Monitoring หรือส่งต่อปัญหาให้ผู้ที่เกี่ยวข้องดำเนินการ

3.5 การวิเคราะห์ข้อมูลและการจัดทำรายงาน

- ใช้ข้อมูลย้อนหลังที่ระบบ Monitoring เก็บไว้ เพื่อวิเคราะห์แนวโน้มการใช้งานเครือข่าย เช่น การเพิ่มของข้อมูลหรืออุปกรณ์ สำหรับการวางแผนความจุ ในอนาคต
- วิเคราะห์ข้อมูลเพื่อหาสาเหตุของปัญหาที่เกิดขึ้นซ้ำๆ หรือปัญหาที่ตรวจจับได้ยาก
- จัดทำรายงานสถานะระบบเครือข่าย (Network Health Report) หรือรายงานปัญหาที่สำคัญจากข้อมูลในระบบ Monitoring เสนอต่อผู้บริหารหรือผู้เกี่ยวข้องตามความเหมาะสม

3.6 การบำรุงรักษาระบบ Monitoring System

- ดูแลให้ระบบ Monitoring System ทำงานได้อย่างเสถียรและต่อเนื่อง
- ดำเนินการอัปเดตซอฟต์แวร์ของระบบ Monitoring ให้เป็นปัจจุบันตามความเหมาะสม เพื่อแก้ไข Bug หรือเพิ่มคุณสมบัติใหม่

- สำรองข้อมูล Configuration และข้อมูลที่ระบบ Monitoring จัดเก็บไว้ (Historical Data) อย่างสม่ำเสมอ

เป้าหมายสูงสุด ของหน้าที่นี้คือ การสร้างและใช้งานเครื่องมือที่มีประสิทธิภาพเพื่อ เพิ่มทัศนวิสัยในการมองเห็นสถานะการทำงานของเครือข่าย ทำให้สามารถ ตรวจจับปัญหาได้อย่างรวดเร็ว วินิจฉัยสาเหตุได้แม่นยำ แก้ไขปัญหาได้อย่างทันท่วงที และนำข้อมูลที่ได้ไปใช้ในการ ป้องกันปัญหาในอนาคต และ วางแผนพัฒนาเครือข่าย (Network Planning) ต่อไป

4. ให้คำปรึกษา แนะนำและแก้ไขปัญหาเกี่ยวกับระบบเครือข่ายอินเตอร์เน็ตสำหรับคณะ/หน่วยงาน
   - รับผิดชอบในการให้คำปรึกษา แนะนำ และสนับสนุนด้านเทคนิคเกี่ยวกับระบบเครือข่ายอินเตอร์เน็ตแก่อาจารย์ บุคลากร และนักศึกษาภายในคณะ/หน่วยงาน
   - วินิจฉัยและแก้ไขปัญหาที่เกี่ยวข้องกับการเชื่อมต่อเครือข่ายอินเตอร์เน็ต ปัญหาการใช้งาน ปัญหาความเร็ว หรือปัญหาอื่นๆ ที่อาจเกิดขึ้นกับอุปกรณ์ของผู้ใช้งาน หรืออุปกรณ์เครือข่ายภายในความดูแล
   - ให้คำแนะนำเกี่ยวกับวิธีการตั้งค่า การเชื่อมต่อ และการใช้งานระบบเครือข่ายอย่างถูกต้องและปลอดภัย เพื่อให้ผู้ใช้งานสามารถเข้าถึงและใช้ประโยชน์จากทรัพยากรบนอินเตอร์เน็ตได้อย่างมีประสิทธิภาพ

2.5.2 การดูแลระบบเครือข่ายอินเตอร์เน็ตความเร็ว FTTx

1. บริการระบบเครือข่ายอินเตอร์เน็ตความเร็วสูง FTTx
   - รับผิดชอบในการให้บริการอินเทอร์เน็ตความเร็วสูงผ่านระบบ FTTx แก่นักศึกษาที่พักอาศัยในหอพัก ให้มีความเสถียร พร้อมใช้งาน และมีประสิทธิภาพตามมาตรฐานที่กำหนด
   - ดูแลการจัดสรรและบริหารจัดการแบนด์วิดท์ (Bandwidth Management) เพื่อให้การใช้งานอินเทอร์เน็ตเป็นไปอย่างเหมาะสม เพียงพอ และทั่วถึงสำหรับผู้ใช้งานทุกคน
   - ตรวจสอบคุณภาพการให้บริการ และความเร็วในการเข้าถึงอินเทอร์เน็ตของผู้ใช้งานอย่างสม่ำเสมอ
   - ประสานงานกับเจ้าหน้าหอพักภายในมหาวิทยาลัย หรือรับแจ้งจากนักศึกษา ในกรณีที่มีปัญหาหรือข้อขัดข้องที่ส่งผลกระทบต่อการให้บริการอินเทอร์เน็ตโดยตรง
   - ดูแลและปรับปรุงการตั้งค่าระบบที่เกี่ยวข้องกับการให้บริการ เช่น การกำหนด IP Address, การตั้งค่า SSID เป็นต้น เพื่อให้ผู้ใช้งานสามารถเข้าถึงอินเทอร์เน็ตได้อย่างราบรื่น
   - มีช่องทางการขอรับความช่วยเหลือสำหรับผู้ใช้งานในหอพัก เช่น Facbook,Email เป็นต้น

2. ออกแบบการเชื่อมต่อและการติดตั้งข่ายสายระบบเครือข่ายแบบ FTTx

- รับผิดชอบในการสำรวจพื้นที่จริงภายในหอพักนักศึกษา เพื่อประเมินสภาพแวดล้อม โครงสร้างอาคาร และตำแหน่งที่เหมาะสมสำหรับการวางอุปกรณ์และติดตั้งข่ายสายใยแก้วนำแสง
- ดำเนินการออกแบบโครงสร้างระบบเครือข่าย FTTx ตั้งแต่จุดเชื่อมต่อหลัก ไปจนถึงห้องพักนักศึกษา (Fiber to the Room) โดยพิจารณาถึงรูปแบบการกระจายสัญญาณ เช่น GPON หรือ Active Ethernet และการแบ่ง Splitter ที่เหมาะสม
- กำหนดเส้นทางและวิธีการติดตั้งข่ายสายไฟเบอร์ออปติก ทั้งภายในอาคาร และภายนอกอาคาร โดยคำนึงถึงความปลอดภัย ความสวยงาม ความทนทาน และการบำรุงรักษาในอนาค
- เลือกชนิดและคุณสมบัติของสายไฟเบอร์ออปติก อุปกรณ์เชื่อมต่อ (Connectors, Adapters), Splice Closure, Splitter, และอุปกรณ์ติดตั้งอื่นๆ ที่ได้มาตรฐานและเหมาะสมกับการใช้งานในสภาพแวดล้อมของหอพัก
- คำนวณความยาวสายไฟเบอร์ออปติกที่ต้องการ และประเมินปริมาณอุปกรณ์และวัสดุที่จำเป็นสำหรับการติดตั้ง
- จัดทำเอกสารประกอบการออกแบบที่ครบถ้วน เช่น Diagram แผนผังต่างๆ และรายละเอียดทางเทคนิคอื่นๆ ที่จำเป็นสำหรับการขออนุมัติและการดำเนินงานติดตั้ง
- ประสานงานกับหน่วยงานที่เกี่ยวข้องภายในมหาวิทยาลัย เช่น กองอาคารสถานที่,งานบริการหอพักนักศึกษา เพื่อให้การออกแบบและการติดตั้งเป็นไปอย่างราบรื่นและถูกต้องตามระเบียบของมหาวิทยาลัย

3. บำรุงรักษาอุปกรณ์เครือข่ายที่มีส่วนเชื่อมโยงกับระบบ FTTx

3.1 การบำรุงรักษาเชิงป้องกัน (Preventive Maintenance):

- ดำเนินการตรวจสอบสภาพทางกายภาพของอุปกรณ์เครือข่ายเป็นประจำ เช่น ตรวจเช็คสายเชื่อมต่อ (Patch Cords, Network Cables), สถานะไฟแสดงการทำงาน (LED indicators), พัดลมระบายความร้อน, และความสะอาดของอุปกรณ์
- ทำความสะอาดอุปกรณ์เครือข่ายตามกำหนด โดยเฉพาะพัดลมและช่องระบายอากาศ เพื่อป้องกันปัญหาความร้อนสูงเกินไป
- ตรวจสอบและบันทึกค่าการทำงานปกติของอุปกรณ์ เช่น อุณหภูมิ, การใช้ CPU/Memory, และสถานะของพอร์ตต่างๆ
- ตรวจสอบความถูกต้องและประสิทธิภาพของระบบจ่ายไฟสำรอง (UPS) ที่เชื่อมต่อกับอุปกรณ์เครือข่ายที่สำคัญ

3.2 การบำรุงรักษาเชิงแก้ไข (Corrective Maintenance) และการแก้ไขปัญหา (Troubleshooting):

- รับผิดชอบในการวินิจฉัยและแก้ไขปัญหาที่เกิดขึ้นกับอุปกรณ์เครือข่ายที่เชื่อมโยงกับระบบ FTTx อย่างรวดเร็วและมีประสิทธิภาพ เพื่อลดผลกระทบต่อผู้ใช้งาน

- ตอบสนองต่อสัญญาณเตือน (Alarms) หรือข้อผิดพลาด (Errors) ที่รายงานจากระบบบริหารจัดการเครือข่าย และดำเนินการแก้ไขตามขั้นตอนที่กำหนด
- เปลี่ยนหรือซ่อมแซมอุปกรณ์เครือข่ายที่ชำรุดหรือทำงานผิดปกติ
- ประสานงานกับผู้จำหน่าย (Vendors) สำหรับการซ่อมแซมภายใต้การรับประกัน หรือการแก้ไขปัญหาทางเทคนิคที่ซับซ้อน

3.3 การปรับปรุงและอัปเดต (Updates and Upgrades):

- วางแผนและดำเนินการอัปเดตเฟิร์มแวร์ (Firmware) และซอฟต์แวร์ระบบปฏิบัติการ (Operating System) ของอุปกรณ์เครือข่ายอย่างสม่ำเสมอ เพื่อปรับปรุงประสิทธิภาพ แก้ไขข้อผิดพลาด และเสริมสร้างความปลอดภัย
- ประเมินความจำเป็นในการอัปเกรดหรือเปลี่ยนอุปกรณ์เครือข่ายเมื่อถึงอายุการใช้งาน หรือเมื่อเทคโนโลยีปัจจุบันไม่สามารถรองรับความต้องการได้

3.4 การบริหารจัดการคอนฟิกูเรชัน (Configuration Management):

- สำรองข้อมูลการตั้งค่า (Configuration Backups) ของอุปกรณ์เครือข่ายที่สำคัญเป็นประจำ และจัดเก็บไว้ในที่ปลอดภัย
- ตรวจสอบและทวนสอบความถูกต้องของการตั้งค่าคอนฟิกูเรชันหลังจากมีการเปลี่ยนแปลงใดๆ

3.5 การจัดการสภาพแวดล้อม (Environment Management):

- ตรวจสอบและควบคุมสภาพแวดล้อมในห้องเซิร์ฟเวอร์หรือตู้แร็คที่ติดตั้งอุปกรณ์เครือข่าย เช่น อุณหภูมิ ความชื้น และการระบายอากาศ ให้อยู่ในเกณฑ์ที่เหมาะสม

4. จัดทำระบบมอนิเตอร์ เพื่อตรวจสอบปริมาณการใช้งาน และ จัดการปัญหาเชิงรุก ให้กับระบบ FTTx

ช่างเทคนิค ผู้ดูแลระบบมีหน้าที่หลักในการออกแบบ ติดตั้ง กำหนดค่า และบริหารจัดการระบบเฝ้าระวัง (Monitoring System) สำหรับโครงสร้างพื้นฐานเครือข่าย FTTx ทั้งหมดในหอพักนักศึกษา เพื่อให้สามารถติดตามสถานะการทำงาน ประสิทธิภาพ และที่สำคัญคือ ปริมาณการใช้งาน ของระบบเครือข่ายได้อย่างมีประสิทธิภาพ พร้อมทั้งนำข้อมูลที่ได้จากการเฝ้าระวังมาใช้ในการ จัดการปัญหาในเชิงรุก ก่อนที่จะส่งผลกระทบต่อการใช้งานของนักศึกษา โดยมีรายละเอียดดังนี้

4.1 การออกแบบและติดตั้งระบบมอนิเตอร์:

- ประเมินและเลือกใช้เครื่องมือหรือซอฟต์แวร์ระบบเฝ้าระวังเครือข่าย (Network Monitoring System - NMS) ที่เหมาะสมกับขนาดและความซับซ้อนของระบบ FTTx และอุปกรณ์เครือข่ายที่เกี่ยวข้อง (เช่น OLTs, Switches, Routers, WAPs)
- วางแผนและดำเนินการติดตั้ง กำหนดค่า (Configure) และเชื่อมโยงอุปกรณ์เครือข่ายเข้ากับระบบมอนิเตอร์

- กำหนดวิธีการเก็บข้อมูล (Data Collection Methods) เช่น SNMP, Syslog, API หรืออื่นๆ ที่เกี่ยวข้องกับอุปกรณ์ FTTx โดยเฉพาะ (เช่น ค่า Optical Power บน OLT และ ONUs)

4.2 การตรวจสอบปริมาณการใช้งาน (Usage Monitoring and Analysis):

- เฝ้าระวังและบันทึกปริมาณการใช้งาน Bandwidth ทั้ง Upstream และ Downstream อย่างต่อเนื่อง
- วิเคราะห์รูปแบบการใช้งาน (Usage Patterns) เช่น ช่วงเวลาที่มีการใช้งานสูงสุด (Peak Hours), ประเภทของทราฟฟิกที่โดดเด่น (ถ้าสามารถแยกแยะได้)
- ตรวจสอบปริมาณการใช้งานในแต่ละพื้นที่หอพัก หรือในแต่ละส่วนของเครือข่าย เพื่อระบุจุดที่มีการใช้งานหนาแน่น
- ใช้ข้อมูลปริมาณการใช้งานเพื่อประกอบการตัดสินใจในการวางแผนขยายขีดความสามารถของระบบ (Capacity Planning) ในอนาคต
- ปริมาณการรับ-ส่งข้อมูล (Bandwidth Utilization) บนแต่ละพอร์ต แต่ละ VLAN หรือรวมทั้งระบบ
- จำนวนผู้ใช้งานที่เชื่อมต่อพร้อมกัน (Concurrent Users)

4.3 การดำเนินการจัดการปัญหาเชิงรุก (Implementing Proactive Measures):

- เมื่อตรวจพบแนวโน้มหรือสัญญาณเตือนที่อาจนำไปสู่ปัญหา ผู้ดูแลระบบต้องดำเนินการแก้ไขก่อนที่ผู้ใช้งานจะได้รับผลกระทบ เช่น
- ปรับปรุงการตั้งค่า (Optimization) ของอุปกรณ์เครือข่ายเพื่อเพิ่มประสิทธิภาพ
- เคลียร์ Log หรือทรัพยากรของอุปกรณ์ที่อาจเต็ม
- วางแผนและแจ้งเตือนล่วงหน้าสำหรับการบำรุงรักษาที่จำเป็น (Scheduled Maintenance) ก่อนที่อุปกรณ์จะล้มเหลว
- เตรียมการหรือเสนอแผนการขยายขีดความสามารถของระบบ (Capacity Expansion) เมื่อข้อมูลบ่งชี้ว่า Bandwidth หรือทรัพยากรอื่นๆ จะไม่เพียงพอในอนาคตอันใกล้
- ตรวจสอบและแก้ไขปัญหาเกี่ยวกับ Optical Power Level ที่เริ่มลดลงก่อนที่จะหลุดจากการเชื่อมต่อ

4.4 การปรับปรุงระบบมอนิเตอร์อย่างต่อเนื่อง:

- ประเมินประสิทธิภาพของระบบมอนิเตอร์ที่ใช้อยู่เป็นประจำ
- ปรับปรุงการตั้งค่าตามการเปลี่ยนแปลงของระบบเครือข่ายและความต้องการในการเฝ้าระวัง
- ศึกษาและนำเทคโนโลยีหรือเครื่องมือมอนิเตอร์ใหม่ๆ มาปรับใช้หากเป็นประโยชน์

5. ให้คำปรึกษา และ แก้ไขปัญหาเกี่ยวกับระบบ FTTx สำหรับสถาบันการศึกษา

ผู้ดูแลระบบมีหน้าที่หลักในการเป็นผู้เชี่ยวชาญด้านเทคนิคเกี่ยวกับระบบ FTTx ที่ติดตั้งใช้งานในหอพักนักศึกษา เพื่อให้คำปรึกษา แนะนำ และดำเนินการแก้ไขปัญหาทางเทคนิคต่างๆ ที่เกี่ยวข้องกับระบบ FTTx และเครือข่ายที่เชื่อมต่อ เพื่อให้มั่นใจว่านักศึกษาและบุคลากรในหอพักสามารถใช้งานอินเตอร์เน็ตได้อย่างราบรื่นและมีประสิทธิภาพ โดยมีรายละเอียดดังนี้

5.1 การให้คำปรึกษาด้านเทคนิค (Technical Consultation):

- ให้คำปรึกษาและแนะนำแก่นักศึกษาและบุคลากรในหอพักเกี่ยวกับวิธีการเชื่อมต่อใช้งานระบบอินเตอร์เน็ตผ่านสายใยแก้วนำแสง (เช่น การเชื่อมต่อ ONU/ONT, การตั้งค่า Wi-Fi Router ของตนเองหากอนุญาต)
- ให้ข้อมูลเกี่ยวกับความสามารถและข้อจำกัดของระบบ FTTx (เช่น ความเร็วสูงสุดที่รองรับ, ข้อกำหนดทางเทคนิค)
- ให้คำแนะนำเบื้องต้นในการแก้ไขปัญหาที่ผู้ใช้งานอาจพบเจอด้วยตนเอง (Self-troubleshooting)

5.2 การรับแจ้งและวินิจฉัยปัญหา (Issue Receiving and Diagnosis):

- รับแจ้งปัญหาการใช้งานระบบอินเตอร์เน็ตจากช่องทางต่างๆ ที่กำหนด (เช่น ระบบ Helpdesk, โทรศัพท์, อีเมล)
- สอบถามข้อมูลและอาการของปัญหาอย่างละเอียดจากผู้แจ้ง เพื่อรวบรวมข้อมูลเบื้องต้น
- ใช้อุปกรณ์และเครื่องมือมอนิเตอร์ และเครื่องมือวินิจฉัยปัญหาเฉพาะทาง FTTx (เช่น Optical Power Meter) เพื่อตรวจสอบสถานะและอาการผิดปกติของระบบ FTTx และเครือข่ายที่เกี่ยวข้อง
- วิเคราะห์และวินิจฉัยหาสาเหตุ ของปัญหาที่เกิดขึ้น ทั้งในส่วนของอุปกรณ์ FTTx (OLT, Splitter, ONU/ONT), สายใยแก้วนำแสง, อุปกรณ์เครือข่ายอื่นๆ (Switch, Router) หรือการตั้งค่าระบบ

5.3 การดำเนินการแก้ไขปัญหา (Problem Resolution):

- ดำเนินการแก้ไขปัญหาทางเทคนิคที่ตรวจพบ ตั้งแต่ปัญหาเบื้องต้นของผู้ใช้งานไปจนถึงปัญหาระดับซับซ้อนของระบบ FTTx
- การแก้ไขปัญหาในส่วนของผู้ใช้งานปลายทาง (End-user side):
- ตรวจสอบการเชื่อมต่อ ONU/ONT และอุปกรณ์ของผู้ใช้งาน
- ให้คำแนะนำการตั้งค่าเบื้องต้นบนอุปกรณ์ของผู้ใช้งาน

5.4 การแก้ไขปัญหาในส่วนโครงสร้างพื้นฐาน FTTx:

- ตรวจสอบและแก้ไขปัญหาเกี่ยวกับสัญญาณแสง (Optical Power Level) ที่ OLT และ ONU/ONT
- ตรวจสอบความถูกต้องของการเชื่อมต่อสายใยแก้วนำแสงตามจุดต่างๆ (Patch Panel, Splitter, Drop Cable)
- ดำเนินการซ่อมแซมหรือเปลี่ยนอุปกรณ์ FTTx ที่ชำรุด (เช่น ONU/ONT, Fiber Patch Cord)
- ตรวจสอบและแก้ไขปัญหาการตั้งค่าบน OLT หรือระบบบริหารจัดการ FTTx
- การแก้ไขปัญหาในส่วนเครือข่ายที่เกี่ยวข้อง:
- ตรวจสอบและแก้ไขปัญหาการตั้งค่า VLAN, Routing, DHCP, DNS ที่เกี่ยวข้องกับระบบ FTTx
- ตรวจสอบและแก้ไขปัญหาบนอุปกรณ์ Network Switches หรือ Routers ที่เชื่อมต่อกับระบบ FTTx
- วิเคราะห์ปัญหาคอขวดของ Bandwidth หรือ Network Congestion
- ประสานงานกับทีม ITในกรณีที่ปัญหาเกี่ยวข้องกับระบบส่วนกลางหรือเกินขอบเขตความรับผิดชอบ

การให้คำปรึกษาและการแก้ไขปัญหาอย่างมีประสิทธิภาพถือเป็นหัวใจสำคัญของตำแหน่งนี้ เพื่อสร้างความพึงพอใจให้กับผู้ใช้งานในหอพักนักศึกษา และรักษาระบบเครือข่าย FTTx ให้สามารถให้บริการได้อย่างต่อเนื่องและมีคุณภาพ.

2.5.3 การดูแลระบบเครือข่ายอินเตอร์เน็ตไร้สาย (Wifi) สำหรับคณะ/หน่วยงาน

ช่างเทคนิค ผู้ดูแลระบบมีหน้าที่หลักในการศึกษา ค้นคว้า วางแผน ออกแบบ และดำเนินการทดสอบระบบเครือข่ายอินเตอร์เน็ตไร้สาย (Wi-Fi) เพื่อให้สอดคล้องกับความต้องการเฉพาะของคณะ/หน่วยงานนั้นๆ และเพื่อให้มั่นใจว่าระบบ Wi-Fi ที่ติดตั้งและใช้งานมีประสิทธิภาพ ความเสถียร ความปลอดภัย และเหมาะสมกับสภาพแวดล้อมและการใช้งานจริง โดยมีรายละเอียดดังนี้

1. มีการศึกษา ออกแบบและทดลอง ระบบเครือข่ายอินเตอร์เน็ตไร้สาย (Wi-Fi) สำหรับคณะ/หน่วยงาน ให้มีความเหมาะสม และเกิดประสิทธิภาพสูงสุด

1.1 การศึกษาและรวบรวมความต้องการ

- ทำความเข้าใจอย่างละเอียดเกี่ยวกับความต้องการใช้งาน Wi-Fi ของคณะ/หน่วยงานนั้นๆ เช่น จำนวนผู้ใช้งาน (นักศึกษา, อาจารย์, เจ้าหน้าที่), ประเภทอุปกรณ์ที่ใช้ (Laptop, Smartphone, Tablet, IoT Devices), ลักษณะการใช้งาน (การเรียนการสอน, การประชุมผ่านวิดีโอ, การเข้าถึงทรัพยากรวิจัย, การใช้งานทั่วไป), พื้นที่ที่ต้องการครอบคลุม (ห้องเรียน, ห้องประชุม, ห้องทำงาน, พื้นที่ส่วนกลาง), และข้อกำหนดพิเศษอื่นๆ

- ศึกษาโครงสร้างอาคารและสภาพแวดล้อมทางกายภาพ (ผังอาคาร, วัสดุก่อสร้าง, แหล่งกำเนิดสัญญาณรบกวน) ที่มีผลต่อการกระจายสัญญาณ Wi-Fi
- ศึกษาเทคโนโลยี Wi-Fi รุ่นใหม่ๆ (เช่น Wi-Fi 6,) มาตรฐานต่างๆ (เช่น 802.11ax, 802.11be) และแนวทางการออกแบบระบบเครือข่ายไร้สายที่ดีที่สุด สำหรับสภาพแวดล้อมสถาบันการศึกษา

1.2 การออกแบบระบบเครือข่ายไร้สาย (Wi-Fi Network Design):

- ดำเนินการสำรวจพื้นที่ (Site Survey) ทั้งแบบ Predictive (ใช้ Software) และ Physical (Walkthrough) เพื่อประเมินสภาพสัญญาณ, กำหนดตำแหน่งติดตั้ง Access Point (AP) และประเมินสัญญาณรบกวน
- ออกแบบโครงสร้าง logical และ physical ของระบบ Wi-Fi รวมถึงการวางแผนตำแหน่ง AP การเดินสาย LAN ที่เชื่อมต่อไปยัง AP และการเชื่อมต่อไปยังอุปกรณ์ Network Switch และ Controller
- กำหนดจำนวน ประเภท และรุ่นของ Access Point ที่เหมาะสมกับพื้นที่และความหนาแน่นของผู้ใช้งาน
- ออกแบบการตั้งค่า Radio Frequency (RF) เช่น การเลือกช่องสัญญาณ (Channel Planning), การตั้งค่ากำลังส่ง (Transmit Power) เพื่อปรับปรุงประสิทธิภาพ
- ออกแบบโครงสร้าง SSID (Service Set Identifier) ที่เหมาะสม เช่น การแยก SSID สำหรับนักศึกษา, บุคลากร หรือ IoT Devices
- ออกแบบและวางแผนการใช้งาน VLAN (Virtual Local Area Networks) เพื่อแบ่งแยก Traffic และเพิ่มความปลอดภัย
- ออกแบบระบบความปลอดภัย (Security Design) เช่น การเลือกวิธีการยืนยันตัวตน (Authentication) (เช่น WPA2/WPA3-Enterprise, RADIUS Integration), การกำหนดนโยบายการเข้าถึง (Access Control Lists) เป็นต้น

1.3 การทดลองและประเมินผล

- ดำเนินการทดสอบระบบ Wi-Fi ในพื้นที่นำร่อง หรือติดตั้ง APs เพื่อทดสอบประสิทธิภาพในสภาพแวดล้อมจริงก่อนการติดตั้งเต็มรูปแบบ
- ทำการทดสอบประสิทธิภาพ (Performance Testing) เช่น การวัด Bandwidth (Throughput), Latency, และ Packet Loss ภายใต้สภาวะโหลดต่างๆ

- ทำการทดสอบการครอบคลุมและคุณภาพสัญญาณ (Coverage and Signal Quality Testing) โดยใช้เครื่องมือ Site Survey เพื่อยืนยันว่าสัญญาณครอบคลุมพื้นที่เป้าหมายตามที่ออกแบบไว้ และมีคุณภาพเพียงพอ
- ทำการทดสอบคุณสมบัติต่างๆ ที่ออกแบบไว้ เช่น การทำงานของ Roaming, Band Steering, QoS, และการแยก VLAN
- ทำการทดสอบระบบความปลอดภัย (Security Testing) เพื่อยืนยันว่าการยืนยันตัวตนและการควบคุมการเข้าถึงทำงานได้อย่างถูกต้องและปลอดภัย
- ประเมินผลการทดลองและวิเคราะห์ข้อมูลเพื่อระบุจุดแข็ง จุดอ่อน และโอกาสในการปรับปรุง (Optimization) ของระบบ
- เปรียบเทียบประสิทธิภาพของอุปกรณ์หรือเทคนิคการตั้งค่าที่แตกต่างกัน (หากมีการทดลองหลายรูปแบบ)

- การดำเนินการตามหน้าที่เหล่านี้อย่างเป็นระบบและมีคุณภาพ จะช่วยให้คณะ/หน่วยงานในมหาวิทยาลัยขอนแก่นมีระบบเครือข่าย Wi-Fi ที่เชื่อถือได้ ปลอดภัย และสามารถรองรับความต้องการด้านการเรียนการสอน การวิจัย และการปฏิบัติงานได้อย่างมีประสิทธิภาพสูงสุด

2. การปรับปรุง บำรุงรักษา เพื่อทดแทนอุปกรณ์ที่ชำรุด สำหรับคณะ/หน่วยงาน

ช่างเทคนิค ผู้ดูแลระบบมีหน้าที่รับผิดชอบในการดูแลรักษา ประเมินสภาพ และจัดการการเปลี่ยนแปลงของอุปกรณ์เครือข่าย Wi-Fi ทั้งหมดภายในคณะ/หน่วยงาน เพื่อให้มั่นใจว่าระบบ Wi-Fi มีความพร้อมใช้งาน มีประสิทธิภาพ อย่างต่อเนื่อง รวมถึงการจัดการเมื่อเกิดอุปกรณ์ชำรุด โดยมีรายละเอียดดังนี้:

2.1 การบำรุงรักษาเชิงป้องกัน

- จัดทำแผนและดำเนินการบำรุงรักษาระบบ Wi-Fi อย่างสม่ำเสมอ เช่น การตรวจสอบสภาพการทำงานของ Access Points (AP), Wireless Controllers, Network Switch และอุปกรณ์สนับสนุนอื่นๆ
- ตรวจสอบสภาพทางกายภาพของอุปกรณ์และสายสัญญาณ เช่น การยึดติดของ AP, สภาพสาย LAN, ขั้วต่อต่างๆ เพื่อป้องกันปัญหาที่อาจเกิดขึ้น
- ตรวจสอบอุปกรณ์ ตามความเหมาะสม สภาพการใช้งาน

- ตรวจสอบและจัดการระบบระบายความร้อนในตู้ Rack หรือพื้นที่ติดตั้งอุปกรณ์ Controller/Switch

2.2 การตรวจสอบและอัปเดตเฟิร์มแวร์/ซอฟต์แวร์ (Monitoring and Firmware/Software Updates)

- ใช้ระบบ Monitoring เพื่อติดตามสถานะการทำงานของอุปกรณ์ Wi-Fi (Online/Offline, CPU Usage, Memory Usage, Client Count) และแจ้งเตือนเมื่อเกิดปัญหา
- ตรวจสอบ Log File ของอุปกรณ์เพื่อค้นหาข้อผิดพลาดหรือที่ผิดปกติ
- ติดตามและวางแผนการอัปเดตเฟิร์มแวร์ (Firmware) และซอฟต์แวร์สำหรับ AP, Controller และอุปกรณ์เครือข่ายที่เกี่ยวข้องเป็นประจำ เพื่อแก้ไขข้อผิดพลาด, ปรับปรุงประสิทธิภาพ, เพิ่มคุณสมบัติใหม่ๆ และอุดช่องโหว่ด้านความปลอดภัย โดยประสานงานกับหน่วยงานหรือทีม Vender ที่เกี่ยวข้อง

2.3 การจัดการอุปกรณ์ชำรุดและการแก้ไขปัญหา

- รับแจ้งปัญหาการใช้งาน Wi-Fi จากผู้ใช้งาน (นักศึกษา, อาจารย์, เจ้าหน้าที่) และระบบ Monitoring
- ดำเนินการแก้ไขปัญหา (Troubleshooting) เพื่อระบุสาเหตุของปัญหา ซึ่งอาจเกิดจากอุปกรณ์, การตั้งค่า, สภาพแวดล้อม หรือปัจจัยอื่นๆ
- กรณีพบว่าอุปกรณ์ชำรุดหรือไม่สามารถซ่อมแซมได้ ณ จุดติดตั้ง ให้ดำเนินการตามกระบวนการทดแทนอุปกรณ์
- ประสานงานกับผู้เกี่ยวข้อง (เช่น ผู้ใช้งาน, ผู้จำหน่าย/Vendor) เพื่อแก้ไขปัญหาที่ซับซ้อน

2.4 การทดแทนอุปกรณ์ที่ชำรุด

- ประเมินและยืนยันว่าอุปกรณ์ชิ้นใดชำรุดและไม่สามารถใช้งานได้ตามปกติ
- ดำเนินการตามกระบวนการจัดหาอุปกรณ์ทดแทน อาจเป็นการใช้อุปกรณ์สำรอง (Spare Parts) หรือการขอเบิก/จัดซื้ออุปกรณ์ใหม่ ตามนโยบายและระเบียบของมหาวิทยาลัย
- ประสานงานกับผู้จำหน่าย/Vendor เพื่อเคลมประกัน (Warranty Claim) หรือส่งซ่อมอุปกรณ์ที่ชำรุด
- ติดตั้งอุปกรณ์ทดแทน ณ ตำแหน่งเดิม หรือตำแหน่งที่เหมาะสมที่สุด
- ดำเนินการตั้งค่า (Configuration) อุปกรณ์ทดแทนให้เหมือนหรือเข้ากับระบบเดิม เพื่อให้สามารถทำงานได้อย่างถูกต้อง

- ประเมินอายุการใช้งานของอุปกรณ์ Wi-Fi ที่มีอยู่ เพื่อวางแผนการปรับปรุงหรือทดแทนอุปกรณ์ที่เริ่มล้าสมัยหรือไม่รองรับเทคโนโลยีใหม่ๆ
- จัดทำแผนการจัดหาหรือปรับปรุงอุปกรณ์ในระยะยาว เพื่อให้ระบบ Wi-Fi ของคณะ/หน่วยงานมีความทันสมัยและรองรับความต้องการในอนาคต

การปฏิบัติหน้าที่เหล่านี้อย่างสม่ำเสมอและมีประสิทธิภาพ จะช่วยลดปัญหาการใช้งาน Wi-Fi ในคณะ/หน่วยงาน, ยืดอายุการใช้งานของอุปกรณ์, และทำให้ผู้ใช้งานได้รับประสบการณ์ที่ดีและต่อเนื่องในการเข้าถึงเครือข่ายอินเตอร์เน็ตไร้สาย

3. การจัดทำ/บริหารจัดการระบบ มอนิเตอร์และคอนโทรลเลอร์ สำหรับตรวจสอบปัญหา

ช่างเทคนิค ผู้ดูแลระบบมีหน้าที่รับผิดชอบในการบริหารจัดการ การใช้งาน และการใช้ประโยชน์สูงสุดจากระบบ Monitoring และ Controller ที่เกี่ยวข้องกับเครือข่าย Wi-Fi ของคณะ/หน่วยงาน เพื่อให้สามารถตรวจสอบสถานะการทำงานของอุปกรณ์และเครือข่ายได้อย่างมีประสิทธิภาพ ค้นหาและแก้ไขปัญหาได้อย่างรวดเร็ว โดยมีรายละเอียดดังนี้

3.1 การดูแลและบำรุงรักษาระบบ Monitoring และ Controller

- ตรวจสอบความพร้อมใช้งาน และสถานะการทำงานของ Server ของระบบ Monitoring และ Controller อย่างสม่ำเสมอ
- ดูแลและบริหารจัดการทรัพยากรของ Server (เช่น CPU, Memory, Storage) เพื่อให้ระบบทำงานได้อย่างราบรื่น
- ดำเนินการอัปเดตเฟิร์มแวร์ (Firmware) หรือซอฟต์แวร์ (Software) ของระบบ Monitoring และ Controller เป็นประจำ ตามคำแนะนำของผู้ผลิต เพื่อแก้ไขข้อผิดพลาด, ปรับปรุงประสิทธิภาพ, เพิ่มคุณสมบัติใหม่ๆ และอุดช่องโหว่ด้านความปลอดภัย
- ตรวจสอบ Log File ของระบบ Monitoring และ Controller เพื่อค้นหาข้อผิดพลาด หรือปัญหาที่เกิดขึ้นกับตัวระบบเอง

3.2 การกำหนดค่าและการใช้งานระบบ Monitoring

- กำหนดค่า (Configure) อุปกรณ์เครือข่าย Wi-Fi (เช่น Access Point (AP), Wireless Controller, Network Switch) ให้ส่งข้อมูลสถานะการทำงานและ Log มายังระบบ Monitoring
- ตั้งค่าเกณฑ์การแจ้งเตือน (Alert Thresholds) สำหรับค่าต่างๆ ที่สำคัญ เช่น สถานะ Online/Offline ของอุปกรณ์, อัตราการใช้งาน CPU/Memory ของ AP หรือ Controller,

จำนวน Client ที่เชื่อมต่อกับ AP, อัตราการใช้งาน Bandwidth, คุณภาพสัญญาณ (Signal Strength) ที่ไม่ดี หรืออัตราการเชื่อมต่อสำเร็จ/ไม่สำเร็จ

- ติดตามและตรวจสอบ Dashboard และ Report ต่างๆ ในระบบ Monitoring เพื่อดูสถานะภาพรวมและรายละเอียดของเครือข่าย Wi-Fi
- ตอบสนอง (Respond) ต่อการแจ้งเตือนที่ระบบสร้างขึ้น และดำเนินการแก้ไขปัญหาตามขั้นตอน

3.3 การกำหนดค่าและการใช้งานระบบ Controller

- ใช้ระบบ Wireless Controller ในการบริหารจัดการ Access Point ทั้งหมดในคณะ/หน่วยงานแบบรวมศูนย์ (Centralized Management)
- กำหนดค่าต่างๆ ที่จำเป็นผ่าน Controller เช่น SSID, Security Profiles (WPA2/WPA3, Radius), VLAN Tagging, Channel Planning, Power Settings, Quality of Service (QoS) Policies
- ตรวจสอบสถานะของ Access Point ผ่าน Controller (Online/Offline, รุ่น, IP Address)
- ตรวจสอบรายการและสถานะของ Client ที่เชื่อมต่อกับเครือข่าย Wi-Fi ผ่าน Controller (MAC Address, IP Address, AP ที่เชื่อมต่อ, ความแรงสัญญาณ, ปริมาณข้อมูล)
- ใช้ฟังก์ชันการทำงานของ Controller ในการแก้ไขปัญหาเบื้องต้น เช่น การ Restart Access Point, การตรวจสอบ Log ที่เกี่ยวข้องกับ Client หรือ AP นั้นๆ

3.4 การใช้ระบบ Monitoring และ Controller ในการตรวจสอบและแก้ไขปัญหา

- เมื่อได้รับแจ้งปัญหาการใช้งาน Wi-Fi (จากผู้ใช้งาน หรือจากระบบ Monitoring) ให้ใช้ระบบ Monitoring และ Controller ในการวิเคราะห์หาสาเหตุของปัญหา
- ตรวจสอบสถานะอุปกรณ์ที่เกี่ยวข้อง (เช่น AP ตัวใดมีปัญหา, Controller มีข้อผิดพลาดหรือไม่) ผ่านระบบ Monitoring/Controller
- ตรวจสอบสถานะการเชื่อมต่อของ Client ที่แจ้งปัญหา (เช่น Client เชื่อมต่อกับ AP ตัวไหน, ได้รับ IP Address หรือไม่, Authentication ผ่านหรือไม่, สัญญาณเป็นอย่างไร) ผ่านระบบ Controller
- วิเคราะห์ข้อมูล Log และ Event ต่างๆ ที่ระบบบันทึกไว้ เพื่อระบุสาเหตุของปัญหาให้แม่นยำขึ้น

- ใช้ข้อมูลที่ได้จากระบบ Monitoring (เช่น ประวัติการทำงาน, ประสิทธิภาพย้อนหลัง) เพื่อทำความเข้าใจสภาพปัญหาและแนวโน้มที่อาจเกิดขึ้น

การใช้งานและบริหารจัดการระบบ Monitoring และ Controller อย่างมีประสิทธิภาพ จะช่วยให้ผู้ดูแลระบบสามารถมองเห็นภาพรวมและรายละเอียดของเครือข่าย Wi-Fi ได้อย่างชัดเจน ทำให้สามารถตรวจจับปัญหาได้อย่างรวดเร็ว ก่อนที่ผู้ใช้งานจะได้รับผลกระทบอย่างรุนแรง และสามารถดำเนินการแก้ไขปัญหาได้อย่างตรงจุดและมีประสิทธิภาพมากยิ่งขึ้น

4. ให้คำปรึกษา แนะนำ และแก้ไขปัญหาเกี่ยวกับระบบเครือข่ายอินเตอร์เน็ตไร้สาย (Wi-Fi)

ข่างเทคนิค ผู้ดูแลระบบมีหน้าที่เป็นจุดประสานงานหลัก สำหรับผู้ใช้งานและบุคลากรภายในคณะ/หน่วยงาน ที่ต้องการ ความช่วยเหลือ คำปรึกษา หรือประสบปัญหาเกี่ยวกับการใช้งานเครือข่าย Wi-Fi โดยมีรายละเอียดดังนี้

4.1 เป็นผู้ให้คำปรึกษาและคำแนะนำ

- ให้คำแนะนำแก่ผู้ใช้งาน (คณาจารย์, บุคลากร, นักศึกษา) เกี่ยวกับวิธีการเชื่อมต่อเครือข่าย Wi-Fi ของมหาวิทยาลัย (เช่น KKU-Wifi, eduroam) บนอุปกรณ์ต่างๆ (เช่น คอมพิวเตอร์, สมาร์ทโฟน, แท็บเล็ต) รวมถึงวิธีการตั้งค่าที่ถูกต้อง
- ให้คำปรึกษาเกี่ยวกับข้อกำหนด นโยบาย และแนวปฏิบัติด้านความปลอดภัยในการใช้งานเครือข่าย Wi-Fi ของมหาวิทยาลัยและคณะ/หน่วยงาน
- ให้คำแนะนำเบื้องต้นเกี่ยวกับการแก้ไขปัญหาการเชื่อมต่อหรือปัญหาประสิทธิภาพการใช้งาน Wi-Fi ที่ผู้ใช้งานสามารถดำเนินการได้เอง
- ให้คำปรึกษาแก่บุคลากรในคณะ/หน่วยงาน เกี่ยวกับการวางแผนการใช้งาน Wi-Fi ในพื้นที่ใหม่ หรือการปรับปรุงพื้นที่ที่มีอยู่ เพื่อให้ครอบคลุมและมีประสิทธิภาพตามความต้องการ
- สื่อสารและอธิบายข้อมูลทางเทคนิคเกี่ยวกับระบบ Wi-Fi ให้กับผู้ใช้งานทั่วไป และผู้บริหารในรูปแบบที่เข้าใจง่าย

4.2 รับแจ้งและแก้ไขปัญหา:

- รับแจ้งปัญหาการใช้งาน Wi-Fi จากผู้ใช้งานผ่านช่องทางต่างๆ ที่กำหนด (เช่น Helpdesk, Email,Social Media, โทรศัพท์)
- สอบถามข้อมูลและรวบรวมรายละเอียดที่จำเป็นจากผู้แจ้งปัญหา (เช่น ประเภทอุปกรณ์, ตำแหน่งที่ใช้งาน, เวลาที่เกิดปัญหา, อาการของปัญหา, ข้อความผิดพลาดที่พบ) เพื่อใช้ในการวิเคราะห์ปัญหา

- ใช้เครื่องมือและระบบต่างๆ (เช่น ระบบ Monitoring, Wireless Controller) ในการตรวจสอบสถานะการทำงานของอุปกรณ์เครือข่าย (Access Point, Switch) และสถานะการเชื่อมต่อของผู้ใช้งานที่แจ้งปัญหา
- วิเคราะห์หาสาเหตุของปัญหา โดยอาจเกิดจากหลายปัจจัย เช่น ปัญหาที่ตัวอุปกรณ์ของผู้ใช้งาน, ปัญหาการตั้งค่าบนอุปกรณ์, ปัญหาที่ตัว Access Point, ปัญหาที่โครงสร้างพื้นฐานเครือข่าย (Switch, สายสัญญาณ), ปัญหาจากสัญญาณรบกวน หรือปัญหาที่ระบบส่วนกลางของมหาวิทยาลัย
- ทดสอบการแก้ไขปัญหาร่วมกับผู้ใช้งาน หรือตรวจสอบผลการแก้ไขผ่านระบบ Monitoring

4.3 การประสานงานเพื่อแก้ไขปัญหาที่ซับซ้อน:

- ในกรณีที่ปัญหาไม่สามารถแก้ไขได้ในระดับคณะ/หน่วยงาน หรือปัญหาเกี่ยวข้องกับระบบโครงสร้างพื้นฐานหรือระบบส่วนกลางของมหาวิทยาลัย เช่น ปัญหาที่ Core Network, ปัญหาที่ Server, ปัญหาที่ Software/Firmware ของ Controller ที่ดูแลโดยส่วนกลาง) ผู้ดูแลระบบประสานงานและแจ้งปัญหาไปยังผู้บังคับบัญชาหรือหัวหน้างาน ของสำนักเทคโนโลยี เพื่อขอความช่วยเหลือและดำเนินการแก้ไขในระดับที่สูงขึ้น
- ติดตามความคืบหน้าของการแก้ไขปัญหา และสื่อสารสถานะไปยังคณะ/หน่วยงาน

การทำหน้าที่ให้คำปรึกษา แนะนำ และแก้ไขปัญหาอย่างมีประสิทธิภาพ จะช่วยให้ผู้ใช้งานในคณะ/หน่วยงานสามารถเชื่อมต่อและใช้งานเครือข่าย Wi-Fi ได้อย่างราบรื่น ลดความขัดข้อง และสร้างความพึงพอใจในการใช้บริการระบบเครือข่ายของคณะ/หน่วยงานและของมหาวิทยาลัยโดยรวม

บทที่ 3
เอกสารและวรรณกรรมที่เกี่ยวข้อง

ในการจัดทำคู่มือ การให้บริการติดตั้งระบบเครือข่ายและอุปกรณ์เครือข่ายซ่อมบำรุง ที่เป็นลิขสิทธิ์ของมหาวิทยาลัยขอนแก่น ใช้เพื่อการศึกษาของมหาวิทยาลัยขอนแก่น ฉบับนี้ ผู้จัดทำได้ศึกษาค้นคว้าจากเอกสารและวรรณกรรมที่เกี่ยวข้องดังนี้

พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

ราชกิจจานุเบกษา เล่ม ๑๓๕ ตอนที่ ๑๐ ก หน้า ๒๔-๓๔ ลงวันที่ ๒๔ มกราคม ๒๕๖๐
(ใช้เฉพาะ มาตรา ๘, มาตรา ๙, มาตรา ๑๐ เท่านั้น)

หน้า ๔
เล่ม ๑๒๔ ตอนที่ ๒๗ ก ราชกิจจานุเบกษา ๑๘ มิถุนายน ๒๕๕๐

พระราชบัญญัติ

ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พ.ศ. ๒๕๕๐

ภูมิพลอดุลยเดช ป.ร.

ให้ไว้ ณ วันที่ ๑๐ มิถุนายน พ.ศ. ๒๕๕๐

เป็นปีที่ ๖๒ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้า ฯ ให้ประกาศว่า

โดยที่เป็นการสมควรมีกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

จึงทรงพระกรุณาโปรดเกล้า ฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของสภานิติบัญญัติแห่งชาติ ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า "พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐"

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดสามสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในพระราชบัญญัตินี้

"ระบบคอมพิวเตอร์" หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ข้อมูลคอมพิวเตอร์" หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

"ข้อมูลจราจรทางคอมพิวเตอร์" หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

"ผู้ให้บริการ" หมายความว่า

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

"ผู้ใช้บริการ" หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

"พนักงานเจ้าหน้าที่" หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

"รัฐมนตรี" หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

มาตรา ๔ ให้รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจออกกฎกระทรวงเพื่อปฏิบัติการตามพระราชบัญญัตินี้

กฎกระทรวงนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้

หมวด ๑
ความผิดเกี่ยวกับคอมพิวเตอร์

มาตรา ๕ ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๖ ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗ ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๘ ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๙ ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๐ ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๑ ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐

(๑) ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันทีหรือในภายหลังและไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

(๒) เป็นการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตาม (๒) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี

มาตรา ๑๓ ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(๕) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (๑) (๒) (๓) หรือ (๔)

มาตรา ๑๕ ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔

มาตรา ๑๖ ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำตามวรรคหนึ่ง เป็นการนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริต ผู้กระทำไม่มีความผิด

ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย

มาตรา ๑๗ ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ

หน้า ๑๒
เล่ม ๑๒๔ ตอนที่ ๒๗ ก ราชกิจจานุเบกษา ๑๘ มิถุนายน ๒๕๕๐

ในการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัตินี้ บรรดาที่เป็นอำนาจของพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ให้พนักงานเจ้าหน้าที่ประสานงานกับพนักงานสอบสวนผู้รับผิดชอบเพื่อดำเนินการตามอำนาจหน้าที่ต่อไป

ให้นายกรัฐมนตรีในฐานะผู้กำกับดูแลสำนักงานตำรวจแห่งชาติและรัฐมนตรีมีอำนาจร่วมกันกำหนดระเบียบเกี่ยวกับแนวทางและวิธีปฏิบัติในการดำเนินการตามวรรคสอง

มาตรา ๓๐ ในการปฏิบัติหน้าที่ พนักงานเจ้าหน้าที่ต้องแสดงบัตรประจำตัวต่อบุคคลซึ่งเกี่ยวข้อง

บัตรประจำตัวของพนักงานเจ้าหน้าที่ให้เป็นไปตามแบบที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้รับสนองพระบรมราชโองการ
พลเอก สุรยุทธ์ จุลานนท์
นายกรัฐมนตรี

3.2 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ **4) พ.ศ. 2562**

ในการจัดคู่มือฉบับนี้ ได้ใช้พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562 (ดังที่แนบ)

หน้า ๒๐๓
เล่ม ๑๓๖ ตอนที่ ๖๗ ก ราชกิจจานุเบกษา ๒๒ พฤษภาคม ๒๕๖๒

พระราชบัญญัติ
ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๔)
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๑๙ พฤษภาคม พ.ศ. ๒๕๖๒
เป็นปีที่ ๔ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ พระวชิรเกล้าเจ้าอยู่หัว มีพระบรมราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรแก้ไขเพิ่มเติมกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

พระราชบัญญัตินี้มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคล ซึ่งมาตรา ๒๖ ประกอบกับมาตรา ๔๐ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย บัญญัติให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย

เหตุผลและความจำเป็นในการจำกัดสิทธิและเสรีภาพของบุคคลตามพระราชบัญญัตินี้ เพื่อกำกับดูแลการพิสูจน์และยืนยันตัวตนทางดิจิทัลให้มีความน่าเชื่อถือและปลอดภัย อันจะเป็นประโยชน์ต่อเศรษฐกิจของประเทศและการคุ้มครองผู้บริโภค ซึ่งการตราพระราชบัญญัตินี้สอดคล้องกับเงื่อนไขที่บัญญัติไว้ในมาตรา ๒๖ ของรัฐธรรมนูญแห่งราชอาณาจักรไทยแล้ว

จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของสภานิติบัญญัติแห่งชาติทำหน้าที่รัฐสภา ดังต่อไปนี้

หน้า ๒๐๔
เล่ม ๑๓๖ ตอนที่ ๖๗ ก ราชกิจจานุเบกษา ๒๒ พฤษภาคม ๒๕๖๒

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า "พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๔) พ.ศ. ๒๕๖๒"

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ให้เพิ่มบทนิยามคำว่า "การพิสูจน์และยืนยันตัวตน" และคำว่า "ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล" ระหว่างบทนิยามคำว่า "ระบบข้อมูล" และคำว่า "ระบบแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์อัตโนมัติ" ในมาตรา ๔ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๓) พ.ศ. ๒๕๖๒

""การพิสูจน์และยืนยันตัวตน" หมายความว่า กระบวนการพิสูจน์และยืนยันความถูกต้องของตัวบุคคล

"ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล" หมายความว่า เครือข่ายทางอิเล็กทรอนิกส์ที่เชื่อมโยงข้อมูลระหว่างบุคคลใด ๆ หรือหน่วยงานของรัฐเพื่อประโยชน์ในการพิสูจน์และยืนยันตัวตนและการทำธุรกรรมอื่น ๆ ที่เกี่ยวเนื่องกับการพิสูจน์และยืนยันตัวตน"

มาตรา ๔ ให้ยกเลิกความในมาตรา ๖ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๖ ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการตามพระราชบัญญัตินี้"

มาตรา ๕ ให้เพิ่มความต่อไปนี้เป็นหมวด ๓/๑ ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล มาตรา ๓๔/๓ และมาตรา ๓๔/๔ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔

"หมวด ๓/๑
ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

มาตรา ๓๔/๓ การพิสูจน์และยืนยันตัวตนของบุคคลอาจกระทำผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลได้

ผู้ใดประสงค์จะอาศัยการพิสูจน์และยืนยันตัวตนของบุคคลอื่นผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลอาจแจ้งเงื่อนไขเกี่ยวกับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องใช้ให้บุคคลอื่นนั้นทราบเป็นการล่วงหน้า และเมื่อได้มีการพิสูจน์และยืนยันตัวตนทางดิจิทัลตามเงื่อนไขดังกล่าวแล้ว ให้สันนิษฐานว่าบุคคลที่ได้รับการพิสูจน์และยืนยันตัวตนเป็นบุคคลนั้นจริง

เงื่อนไขเกี่ยวกับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัลตามวรรคสองต้องมีมาตรฐานไม่ต่ำกว่าที่คณะกรรมการหรือคณะกรรมการตามมาตรา ๓๔/๔ วรรคสอง แล้วแต่กรณีประกาศกำหนด โดยมีหลักประกันการเข้าถึงและการใช้ประโยชน์ของประชาชนโดยสะดวกและไม่เลือกปฏิบัติ

มาตรา ๓๔/๔ ในกรณีที่จำเป็นเพื่อรักษาความมั่นคงทางการเงินและการพาณิชย์ หรือเพื่อประโยชน์ในการเสริมสร้างความน่าเชื่อถือและยอมรับในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล หรือเพื่อป้องกันความเสียหายต่อสาธารณชน ให้มีการตราพระราชกฤษฎีกากำหนดให้การประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลใดเป็นการประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ที่ต้องได้รับใบอนุญาตก่อน และให้นำบทบัญญัติในหมวด ๓ ธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ มาใช้บังคับโดยอนุโลม

พระราชกฤษฎีกาตามวรรคหนึ่งอาจกำหนดให้มีการจัดตั้งคณะกรรมการขึ้นมาคณะหนึ่งเพื่อทำหน้าที่ประกาศกำหนดหลักเกณฑ์ที่ผู้ประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลจะต้องปฏิบัติ และให้มีอำนาจพิจารณามีคำสั่งและดำเนินการอื่นใดตามมาตรา ๓๔ ในกรณีที่ผู้ได้รับใบอนุญาตฝ่าฝืนหรือปฏิบัติไม่ถูกต้องตามหลักเกณฑ์การประกอบธุรกิจก็ได้"

มาตรา ๖ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๔๕/๑ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔

"มาตรา ๔๕/๑ ผู้ใดประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลโดยไม่ได้รับใบอนุญาตตามมาตรา ๓๔/๔ หรือประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลในระหว่างที่มีคำสั่งพักใช้ใบอนุญาตหรือภายหลังจากมีคำสั่งเพิกถอนใบอนุญาตของคณะกรรมการหรือคณะกรรมการตามมาตรา ๓๔/๔ วรรคสอง ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินสามแสนบาท หรือทั้งจำทั้งปรับ"

มาตรา ๗ ผู้ประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลซึ่งประกอบธุรกิจอยู่ในวันก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ ให้ดำเนินกิจการต่อไปได้ และเมื่อมีการตราพระราชกฤษฎีกาตามมาตรา ๓๔/๔ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัตินี้ กำหนดให้เป็นธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ที่ต้องได้รับใบอนุญาต ให้ผู้ประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลนั้นยื่นคำขอรับใบอนุญาตภายในเก้าสิบวันนับแต่วันที่พระราชกฤษฎีกามีผลใช้บังคับ และเมื่อได้ยื่นคำขอรับใบอนุญาตแล้ว ให้ดำเนินกิจการต่อไปจนกว่าจะมีคำสั่งไม่อนุญาต

มาตรา ๘ บรรดาระเบียบที่ออกตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ที่ใช้บังคับอยู่ในวันก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ ให้ยังคงใช้บังคับได้ต่อไปเพียงเท่าที่ไม่ขัดหรือแย้งกับพระราชบัญญัตินี้ จนกว่าจะมีระเบียบตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัตินี้ใช้บังคับ

มาตรา ๙ ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการตามพระราชบัญญัตินี้

ผู้รับสนองพระบรมราชโองการ
พลเอก ประยุทธ์ จันทร์โอชา
นายกรัฐมนตรี

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ โดยที่การยืนยันตัวตนของบุคคลเป็นขั้นตอนสำคัญในการทำธุรกรรมในระบบเศรษฐกิจ แต่ที่ผ่านมาผู้ที่ประสงค์จะขอรับบริการจากผู้ประกอบการหรือหน่วยงานใด ๆ จะต้องทำการพิสูจน์และยืนยันตัวตนโดยการแสดงตนต่อผู้ให้บริการพร้อมกับต้องส่งเอกสารหลักฐาน ซึ่งเป็นภาระต่อผู้ใช้บริการและผู้ให้บริการ สมควรกำหนดให้บุคคลสามารถพิสูจน์และยืนยันตัวตนผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลได้ โดยมีกลไกการควบคุมดูแลผู้ประกอบธุรกิจบริการที่เกี่ยวข้องเพื่อให้ระบบดังกล่าวมีความน่าเชื่อถือและปลอดภัย จึงจำเป็นต้องตราพระราชบัญญัตินี้

3.3 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

ในการจัดทำคู่มือฉบับนี้ ได้ใช้ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 (ดังที่แนบ)

หน้า ๑๓๑
เล่ม ๑๒๗ ตอนพิเศษ ๗๘ ง ราชกิจจานุเบกษา ๒๓ มิถุนายน ๒๕๕๓

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ

พ.ศ. ๒๕๕๓

ด้วยปัญหาด้านการรักษาความมั่นคงปลอดภัยให้กับสารสนเทศมีความรุนแรงเพิ่มขึ้นทั้งในประเทศและต่างประเทศ อีกทั้งยังมีแนวโน้มที่จะส่งผลกระทบต่อภาครัฐและภาคธุรกิจมากขึ้น ทำให้ผู้ประกอบการ ตลอดจนองค์กร ภาครัฐ และภาคเอกชนที่มีการดำเนินงานใด ๆ ในรูปของข้อมูลอิเล็กทรอนิกส์ผ่านระบบสารสนเทศขององค์กร ขาดความเชื่อมั่นต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ในทุกรูปแบบ ประกอบกับคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ตระหนักถึงความจำเป็นที่จะส่งเสริมและผลักดันให้ประเทศสามารถยกระดับการแข่งขันกับประเทศอื่น ๆ โดยการนำระบบสารสนเทศและการสื่อสารมาประยุกต์ใช้ประกอบการทำธุรกรรมทางอิเล็กทรอนิกส์อย่างแพร่หลาย จึงเห็นความสำคัญที่จะนำกฎหมาย ข้อบังคับต่าง ๆ มาบังคับใช้กับการทำธุรกรรมทางอิเล็กทรอนิกส์ทั้งในส่วนที่ต้องกระทำและในส่วนที่ต้องงดเว้นการกระทำ เพื่อช่วยให้การทำธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานของรัฐมีความมั่นคงปลอดภัยและมีความน่าเชื่อถือ

เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงเห็นควรกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ

อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงได้จัดทำประกาศฉบับนี้ เพื่อเป็นแนวทางเบื้องต้นให้หน่วยงานของรัฐใช้ในการกำหนดนโยบาย และข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งอย่างน้อยต้องประกอบด้วยสาระสำคัญ ดังต่อไปนี้

ข้อ ๑ ในประกาศนี้

(๑) ผู้ใช้งาน หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารขององค์กร ผู้รับบริการ ผู้ใช้งานทั่วไป

(๒) สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

(๓) สินทรัพย์ (asset) หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

(๔) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

(๕) ความมั่นคงปลอดภัยด้านสารสนเทศ (information security) หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

(๖) เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

(๗) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ข้อ ๒ หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร ซึ่งอย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

ข้อ ๓ หน่วยงานของรัฐต้องจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ซึ่งอย่างน้อยต้องประกอบด้วยกระบวนการ ดังต่อไปนี้

(๑) หน่วยงานของรัฐต้องจัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๒) หน่วยงานของรัฐต้องประกาศนโยบายและข้อปฏิบัติดังกล่าว ให้ผู้เกี่ยวข้องทั้งหมดทราบเพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้

(๓) หน่วยงานของรัฐต้องกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติดังกล่าวให้ชัดเจน

(๔) หน่วยงานของรัฐต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ

ข้อ ๔ ข้อปฏิบัติในด้านการรักษาความมั่นคงปลอดภัย ต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ ๕ - ๑๕

ข้อ ๕ ให้มีข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control) ซึ่งต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) หน่วยงานของรัฐต้องมีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงานของรัฐนั้น ๆ

(๓) หน่วยงานของรัฐต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๖ ให้มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วนคือ การควบคุมการเข้าถึงสารสนเทศ และการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ข้อ ๗ ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรม หลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(๕) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ ๘ ให้มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้งานรหัสผ่าน (password use) ต้องกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๙ ให้มีการควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๒) การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้

(๓) การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

(๔) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(๕) การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

(๖) การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง

(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๑๐ ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(๒) การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(๓) การบริหารจัดการรหัสผ่าน (password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(๔) การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๑๑ ให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control) โดยต้องมีการควบคุม ดังนี้

(๑) การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (mobile computing and teleworking)

(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๔) การปฏิบัติงานจากภายนอกสำนักงาน (teleworking) ต้องกำหนดข้อปฏิบัติ แผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

ข้อ ๑๒ หน่วยงานของรัฐที่มีระบบสารสนเทศต้องจัดทำระบบสำรอง ตามแนวทางต่อไปนี้

(๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ

(๕) สำหรับความถี่ของการปฏิบัติในแต่ละข้อ ควรมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน

ข้อ ๑๓ หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง

(๒) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการ โดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

ข้อ ๑๔ หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจาก

หน้า ๑๓๘
เล่ม ๑๒๗ ตอนพิเศษ ๗๘ ง ราชกิจจานุเบกษา ๒๓ มิถุนายน ๒๕๕๓

ความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานของรัฐเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๑๕ หน่วยงานของรัฐสามารถเลือกใช้ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ที่ต่างไปจากประกาศฉบับนี้ได้ หากแสดงให้เห็นว่า ข้อปฏิบัติที่เลือกใช้มีความเหมาะสมกว่า หรือเทียบเท่า

ข้อ ๑๖ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๓๑ พฤษภาคม พ.ศ. ๒๕๕๓
ร้อยตรีหญิง ระนองรักษ์ สุวรรณฉวี
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ประธานกรรมการธุรกรรมทางอิเล็กทรอนิกส์

3.4 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2556

ในการจัดทำคู่มือฉบับนี้ ได้ใช้ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2556 (ดังที่แนบ)

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย
ด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๒)
พ.ศ. ๒๕๕๖

โดยที่เป็นการสมควรปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐให้สอดคล้องกับมาตรฐานสากล

อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๙ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖"

ข้อ ๒ ให้ยกเลิกความในข้อ ๑๔ ของประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และให้ใช้ความต่อไปนี้แทน

"ข้อ ๑๔ หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น"

ข้อ ๓[๑] ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๒๕ มกราคม พ.ศ. ๒๕๕๖
นาวาอากาศเอก อนุดิษฐ์ นาครทรรพ
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ประธานกรรมการธุรกรรมทางอิเล็กทรอนิกส์

---

[๑] ราชกิจจานุเบกษา เล่ม ๑๓๐/ตอนพิเศษ ๒๑ ง/หน้า ๕๒/๑๔ กุมภาพันธ์ ๒๕๕๖

เอกสารและวรรณกรรมที่เกี่ยวข้อง

องค์ความรู้ทั่วไปเกี่ยวกับระบบเครือข่าย อุปกรณ์เครือข่าย

การติดตั้งระบบอุปกรณ์เครือข่าย (Network Equipment Installation) เป็นกระบวนการที่สำคัญในการสร้างเครือข่ายคอมพิวเตอร์ที่มีประสิทธิภาพและปลอดภัย โดยประกอบด้วยขั้นตอนและองค์ประกอบหลักต่าง ๆ ดังนี้:

1. การวางแผนเครือข่าย
2. อุปกรณ์หลักที่ต้องติดตั้ง
3. การติดตั้งอุปกรณ์
4. ติดตั้งทางซอฟต์แวร์ (Software Configuration)
5. ทดสอบและตรวจสอบการทำงาน
6. การดูแลรักษาและตรวจสอบความปลอดภัย

1. **วางแผนและออกแบบเครือข่าย**

- วิเคราะห์ความต้องการ: เช่น จำนวนผู้ใช้งาน, ความเร็วอินเทอร์เน็ตที่ต้องการ, ประเภทอุปกรณ์
- จำนวนผู้ใช้งาน: คาดว่าจะมีผู้ใช้งานกี่คน และแต่ละคนใช้อุปกรณ์กี่ชิ้น
- กำหนดโครงสร้างเครือข่าย: เช่น Topology (Star, Bus, Mesh), LAN/WAN, การแบ่ง VLAN
- เลือกอุปกรณ์: เช่น Router, Switch, Access Point, Firewall
- ประเภทการใช้งาน: ใช้สำหรับการท่องเว็บ, ประชุมออนไลน์, เล่นเกม, ทำงาน, เซิร์ฟเวอร์ ฯลฯ
- ปริมาณการรับส่งข้อมูล (Bandwidth): ความเร็วอินเทอร์เน็ตที่ต้องการ และปริมาณข้อมูลที่จะใช้งานพร้อมกัน
- ระยะทางและพื้นที่ใช้งาน: ขนาดพื้นที่ (บ้าน, สำนักงาน, โรงงาน) มีชั้นกี่ชั้น ผนังหนาไหม
- งบประมาณที่มี: เพื่อเลือกอุปกรณ์และเทคโนโลยีที่เหมาะสม

1.1 กำหนดโครงสร้างเครือข่าย (Network Topology)

รูปแบบโครงข่ายมีหลายแบบ เช่น:

- Star Topology: นิยมใช้มากที่สุด มี Switch/Router เป็นศูนย์กลาง
- Bus Topology: ใช้สายเดียวเชื่อมทุกอุปกรณ์ (ไม่ค่อยนิยมในปัจจุบัน)
- Mesh Topology: ทุกอุปกรณ์เชื่อมกันโดยตรง (ใช้ในระบบที่ต้องการความทนทานสูง)

1.2 แบ่งเครือข่าย (Network Segmentation)

- แบ่ง VLAN ตามแผนกหรือการใช้งาน เช่น แผนกบัญชี, IT, Guest
- แยกเครือข่ายสำหรับ Wi-Fi ผู้เยี่ยมชม (Guest Wi-Fi)
- ใช้ IP Address Scheme ที่ชัดเจน เช่น 192.168.10.0/24 สำหรับแผนก A

1.3 เลือกอุปกรณ์เครือข่าย

- Router: ควบคุมการเชื่อมต่อกับอินเทอร์เน็ต
- Switch: สำหรับการเชื่อมต่ออุปกรณ์ภายใน (แนะนำใช้ Switch แบบ Gigabit)
- Access Point (AP): ขยายสัญญาณ Wi-Fi ให้ครอบคลุมพื้นที่
- Firewall: ป้องกันการโจมตีจากภายนอก
- Cabling: ใช้สาย CAT6 หรือ CAT6A เพื่อรองรับความเร็ว 1Gbps หรือ 10Gbps

1.4 ออกแบบผังเครือข่าย (Network Diagram) สร้างผังเครือข่ายเพื่อให้เห็นภาพรวมการเชื่อมต่อของอุปกรณ์ทั้งหมด เช่น:

- เส้นทางการเชื่อมต่อจาก Router ⟶ Switch ⟶ AP ⟶ Client
- การกำหนด IP Address
- ตำแหน่งติดตั้งอุปกรณ์แต่ละตัวในพื้นที่จริง

1.5 ความปลอดภัยของเครือข่าย

- ใช้รหัสผ่านที่รัดกุมกับอุปกรณ์
- ตั้งค่า Firewall, Access Control, Port Security
- เปิดใช้งานการเข้ารหัส Wi-Fi แบบ WPA3
- จำกัดการเข้าถึงเฉพาะ MAC Address ที่อนุญาต

1.6 การวางแผนรองรับอนาคต

- เผื่อจำนวนพอร์ตใน Switch สำหรับอุปกรณ์เพิ่มเติม
- เผื่อช่องว่างใน Rack สำหรับอุปกรณ์ใหม่
- วางระบบสายสัญญาณให้รองรับความเร็วสูงในอนาคต

2. อุปกรณ์หลักที่ต้องติดตั้ง

- Router: เชื่อมต่อเครือข่ายภายในกับอินเทอร์เน็ต
- Switch: กระจายข้อมูลภายในเครือข่ายแบบมีสาย
- Access Point (AP): ให้บริการ Wi-Fi สำหรับอุปกรณ์ไร้สาย
- Firewall: ควบคุมความปลอดภัยของข้อมูลเข้า/ออก
- Patch Panel & Rack: สำหรับจัดการสายสัญญาณให้เป็นระเบียบ

2.1 Router (เราเตอร์)

- หน้าที่: เชื่อมต่อเครือข่ายภายใน (LAN) กับเครือข่ายภายนอก (Internet)
- ตัวอย่างการใช้งาน: บ้าน, ออฟฟิศ, โรงเรียน
- หมายเหตุ: บางรุ่นมี Firewall และ Access Point ในตัว

2.2 **Switch (สวิตช์)**

(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

- หน้าที่: กระจายการเชื่อมต่อเครือข่ายไปยังอุปกรณ์ภายใน เช่น คอมพิวเตอร์,

ปรินเตอร์, AP ประเภท:

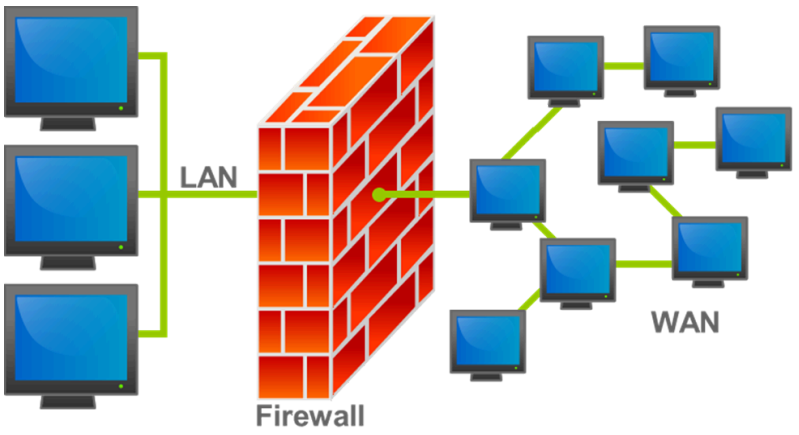
  - Unmanaged Switch: ใช้งานง่าย ไม่มีการตั้งค่า
  - Managed Switch: รองรับ VLAN, QoS, การจัดการผ่าน Web/CLI

2.3 **Access Point (AP)**

- หน้าที่: ปล่อยสัญญาณ Wi-Fi ให้กับอุปกรณ์ไร้สาย

- ประเภท:
    - แบบเดี่ยว: สำหรับพื้นที่เล็ก
    - แบบหลายตัว + Controller: สำหรับองค์กรขนาดใหญ่

2.4 Firewall



- หน้าที่: ป้องกันการเข้าถึงเครือข่ายจากภายนอกที่ไม่ได้รับอนุญาต
- ลักษณะ: อาจเป็นอุปกรณ์เฉพาะ หรือรวมใน Router

2.5 Patch Panel

- หน้าที่: จุดรวมสาย LAN เข้าสู่ Switch
- ประโยชน์: ช่วยให้การเดินสายเป็นระเบียบ และง่ายต่อการบำรุงรักษา

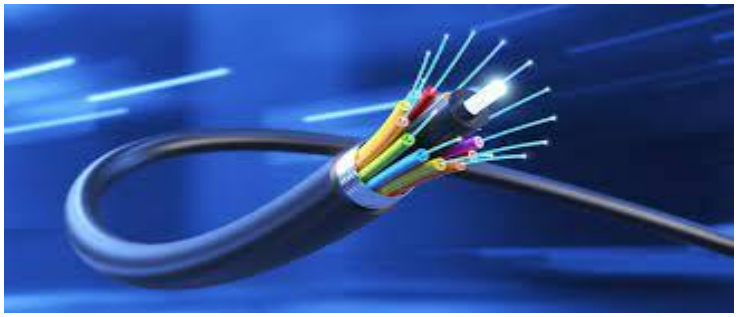
2.6 **Rack (ตู้แร็ค)**

- หน้าที่: สำหรับติดตั้ง Router, Switch, Patch Panel และอุปกรณ์อื่น ๆ
- ขนาด: เช่น 6U, 12U, 42U (ขึ้นกับจำนวนอุปกรณ์)

2.7 **UPS (Uninterruptible Power Supply)**

- หน้าที่: สำรองไฟฟ้าเมื่อเกิดไฟดับ ป้องกันข้อมูลสูญหายหรืออุปกรณ์เสียหาย

2.8 **สายสัญญาณ (LAN Cable / Fiber)**



- สาย LAN: CAT5e, CAT6, CAT6a (รองรับความเร็วสูง)
- สายไฟเบอร์: สำหรับระยะทางไกลหรือความเร็วสูงระดับองค์กร

3. การติดตั้งอุปกรณ์

- ติดตั้งทางกายภาพ (Physical Setup):
    - วางอุปกรณ์ในตู้แร็ค
    - เดินสาย LAN/ไฟเบอร์ให้เป็นระเบียบ
    - ตรวจสอบแหล่งจ่ายไฟ (อาจใช้ UPS สำรองไฟ)

ติดตั้งทางกายภาพ (Physical Setup)

3.1 การเลือกสถานที่ติดตั้ง

- มีพื้นที่เพียงพอ
- การระบายอากาศดี
- ปลอดภัยจากฝุ่นและความชื้น

3.2 การจัดวางอุปกรณ์

- วางอุปกรณ์ให้มั่นคง
- จัดสายไฟและสายสัญญาณให้เป็นระเบียบ
- ระยะห่างระหว่างอุปกรณ์เพื่อความสะดวกในการบำรุงรักษา

3.3 การเชื่อมต่ออุปกรณ์

- เชื่อมต่อกับแหล่งจ่ายไฟ (Power Supply)
- เชื่อมต่อสาย LAN / สายสื่อสารต่าง ๆ
- เชื่อมต่อกับอุปกรณ์ต่อพ่วง เช่น จอภาพ คีย์บอร์ด เมาส์ ฯลฯ

3.4 การเปิดใช้งานเบื้องต้น

- ตรวจสอบไฟสถานะ
- ตรวจสอบการทำงานของพัดลมระบายความร้อน
- ตรวจสอบเสียงเตือนหรือสัญญาณผิดปกติ

3.5 ความปลอดภัย

- การติดตั้งระบบป้องกันไฟกระชาก
- การเดินสายให้ปลอดภัยและไม่สะดุด
- ติดตั้งกล้องหรืออุปกรณ์ตรวจจับหากจำเป็น

3.6 ติดตั้งทางซอฟต์แวร์ (Software Configuration):

- ตั้งค่า IP Address, Gateway, Subnet Mask
- เปิด/ปิด DHCP
- ตั้งค่า Wi-Fi SSID, รหัสผ่าน และ Security Protocol (เช่น WPA3)
- ตั้งค่าการควบคุมการเข้าถึง (Access Control)

4. ตั้งค่า IP Address, Gateway, Subnet Mask

การตั้งค่าเหล่านี้เป็นการกำหนดข้อมูลพื้นฐานที่จำเป็นสำหรับการเชื่อมต่อเครือข่าย เช่นเดียวกับที่ได้กล่าวถึงในคำตอบก่อนหน้านี้ แต่จะอธิบายเพิ่มเติมในกรณีที่ตั้งค่า Router หรือ Access Point (AP):

- IP Address: กำหนด IP Address ให้กับอุปกรณ์ (อาจตั้งค่าแบบ Static หรือ Dynamic)
- Gateway: คือ IP ของ Router ที่เชื่อมต่อกับอินเทอร์เน็ตหรือเครือข่ายภายนอก
- Subnet Mask: ใช้ในการแบ่งเครือข่ายเป็นส่วนย่อย (Subnets)

ตัวอย่างการตั้งค่า:

การตั้งค่า	ค่า
IP Address	192.168.1.100
Gateway	192.168.1.1
Subnet Mask	255.255.255.0

4.1 เปิด/ปิด DHCP

DHCP (Dynamic Host Configuration Protocol) ช่วยในการกำหนด IP Address ให้กับอุปกรณ์ในเครือข่ายโดยอัตโนมัติ (dynamic IP) ซึ่งจะช่วยให้ไม่ต้องตั้งค่า IP Address ด้วยตนเองทุกครั้ง

- การเปิด DHCP: ทำให้ Router หรือ Access Point จัดการ IP Address โดยอัตโนมัติ
- การปิด DHCP: เมื่อปิด DHCP อุปกรณ์ต่าง ๆ ในเครือข่ายจะต้องตั้งค่า IP Address แบบ Static ด้วยตนเอง

การตั้งค่า DHCP ใน Router:

1. เข้าสู่หน้า Web Interface ของ Router หรือ Access Point โดยการพิมพ์ IP Address (เช่น 192.168.1.1) ในเว็บเบราว์เซอร์
2. เข้าสู่ระบบด้วย username และ password ของ Router
3. ไปที่เมนู DHCP Settings หรือ LAN Setup
4. เปิดหรือปิด DHCP ตามต้องการ
5. ถ้าต้องการเปิด DHCP จะต้องกำหนดช่วง IP (Range) ที่ Router สามารถแจกจ่ายให้กับอุปกรณ์ในเครือข่าย

4.2 ตั้งค่า Wi-Fi SSID, รหัสผ่าน และ Security Protocol (เช่น WPA3)

การตั้งค่า Wi-Fi SSID (ชื่อเครือข่ายไร้สาย), รหัสผ่าน และโปรโตคอลความปลอดภัยสำคัญมากในการรักษาความปลอดภัยของเครือข่ายไร้สาย

- SSID (Service Set Identifier): ชื่อเครือข่ายไร้สาย
- รหัสผ่าน (Password): ใช้เพื่อความปลอดภัยในการเชื่อมต่อกับเครือข่าย Wi-Fi
- Security Protocol: เลือกโปรโตคอลความปลอดภัยที่ดีที่สุด เช่น WPA3 หรือ WPA2

การตั้งค่า Wi-Fi:

1. เข้าสู่หน้า Web Interface ของ Router หรือ Access Point
2. ไปที่เมนู Wireless Settings หรือ Wi-Fi Settings
3. กรอก SSID ที่ต้องการใช้งาน (ชื่อเครือข่าย)
4. ตั้งค่ารหัสผ่านสำหรับเครือข่าย Wi-Fi
5. เลือก Security Protocol ที่ต้องการ เช่น:
    - WPA3 (แนะนำสำหรับความปลอดภัยสูงสุด)
    - WPA2 (ยังคงปลอดภัยแต่ไม่ใช่ตัวเลือกที่ดีที่สุดในปัจจุบัน)
6. บันทึกการตั้งค่า

4.3 ตั้งค่าการควบคุมการเข้าถึง (Access Control)

Access Control ใช้ในการจัดการว่าใครสามารถเชื่อมต่อกับเครือข่ายได้บ้าง โดยสามารถตั้งค่าควบคุมการเข้าถึงได้หลายวิธี เช่น การกำหนด MAC Address หรือใช้ฟีเจอร์อื่น ๆ ในการกรองการเข้าถึงเครือข่าย

วิธีการตั้งค่าการควบคุมการเข้าถึง:

1. เข้าสู่หน้า Web Interface ของ Router หรือ Access Point
2. ไปที่เมนู Access Control หรือ MAC Filtering
3. เปิดใช้งาน MAC Filtering เพื่ออนุญาตหรือปฏิเสธการเข้าถึงจากอุปกรณ์ที่มี MAC Address เฉพาะ
4. เพิ่ม MAC Address ของอุปกรณ์ที่ต้องการอนุญาตให้เข้าถึงเครือข่าย
5. เลือกว่าจะอนุญาตหรือบล็อคการเชื่อมต่อจากอุปกรณ์อื่น ๆ

ตัวเลือกการควบคุมการเข้าถึงอื่น ๆ:

- Guest Network: สร้างเครือข่าย Wi-Fi แยกสำหรับผู้ใช้งานภายนอก
- Time-based Access Control: จำกัดเวลาในการเชื่อมต่อเครือข่าย Wi-Fi

5. **ทดสอบและตรวจสอบการทำงาน**

- ทดสอบการเชื่อมต่ออินเทอร์เน็ต
- ตรวจสอบความเร็วเครือข่าย
- ทดสอบการเข้าถึงอุปกรณ์ภายในเครือข่าย
- ตรวจสอบระบบความปลอดภัย เช่น Firewall, MAC Filter, etc.

การทดสอบการเชื่อมต่ออินเทอร์เน็ตจะช่วยให้คุณรู้ว่าอุปกรณ์สามารถเชื่อมต่อกับอินเทอร์เน็ตได้หรือไม่

- วิธีการทดสอบ:
  - Command Prompt (Windows) หรือ Terminal (Mac/Linux):
    1. เปิด Command Prompt (Windows) หรือ Terminal (Mac/Linux)
    2. พิมพ์คำสั่ง: ping 8.8.8.8 (Google DNS) หรือ ping www.google.com
    3. หากได้รับการตอบสนอง (response) จากเซิร์ฟเวอร์แสดงว่าเชื่อมต่ออินเทอร์เน็ตได้
    4. หากไม่มีการตอบกลับ (Request Timed Out) อาจมีปัญหากับการเชื่อมต่ออินเทอร์เน็ตหรือการตั้งค่าเครือข่าย
  - Web Browser: เปิดเว็บเบราว์เซอร์และลองเข้าเว็บไซต์ เช่น https://www.google.com หากโหลดหน้าเว็บได้แสดงว่าเชื่อมต่ออินเทอร์เน็ตได้ปกติ

5.1 ทดสอบการเชื่อมต่อระหว่างคอมพิวเตอร์ในเครือข่าย

การทดสอบการเชื่อมต่อระหว่างคอมพิวเตอร์ในเครือข่ายภายในจะช่วยให้คุณตรวจสอบว่าเครื่องต่างๆ ในเครือข่ายสามารถสื่อสารกันได้หรือไม่

- วิธีการทดสอบ:
  - ใช้คำสั่ง ping เพื่อตรวจสอบการเชื่อมต่อระหว่างคอมพิวเตอร์:
    1. เปิด Command Prompt (Windows) หรือ Terminal (Mac/Linux)
    2. พิมพ์คำสั่ง: ping [IP address ของคอมพิวเตอร์อื่น]
    3. หากได้รับการตอบกลับ (Reply) จากเครื่องหมายว่าเชื่อมต่อได้สำเร็จ แต่หากไม่มีการตอบกลับแสดงว่าเครื่องอาจจะไม่สามารถเชื่อมต่อกันได้หรือมีปัญหาเกี่ยวกับการตั้งค่าเครือข่าย

5.2. ตรวจสอบความเร็วของการเชื่อมต่อ

การตรวจสอบความเร็วการเชื่อมต่อเครือข่ายจะช่วยให้คุณทราบว่าความเร็วของอินเทอร์เน็ตเป็นไปตามที่คาดหวังหรือไม่

- วิธีการทดสอบ:
    - ใช้บริการออนไลน์ เช่น:
        - Speedtest.net
        - Fast.com
    - เมื่อเข้าเว็บไซต์เหล่านี้แล้ว คุณสามารถคลิกที่ปุ่ม "Go" เพื่อทดสอบความเร็วของการดาวน์โหลด (Download) และอัปโหลด (Upload) รวมถึงค่าความหน่วง (Ping) ในการเชื่อมต่ออินเทอร์เน็ต
    - ความเร็วที่ได้จะช่วยให้คุณทราบว่าเชื่อมต่ออินเทอร์เน็ตมีความเร็วตามที่คาดหวังหรือไม่

5.3 ทดสอบการเชื่อมต่อ Wi-Fi

การทดสอบการเชื่อมต่อ Wi-Fi จำเป็นต้องตรวจสอบว่าอุปกรณ์ต่างๆ สามารถเชื่อมต่อกับเครือข่าย Wi-Fi ได้และมีสัญญาณที่ดี

- วิธีการทดสอบ:
    - ตรวจสอบว่าอุปกรณ์ของคุณสามารถค้นหา SSID ของเครือข่าย Wi-Fi และเชื่อมต่อได้หรือไม่
    - ทดสอบการเข้าถึงอินเทอร์เน็ตผ่าน Wi-Fi โดยการเปิดเว็บเบราว์เซอร์และลองโหลดเว็บไซต์
    - หากเชื่อมต่อไม่ได้ ลองรีบูต Access Point หรือ Router และลองเชื่อมต่อใหม่
    - ตรวจสอบว่า Wi-Fi password ถูกต้องหรือไม่ และสัญญาณ Wi-Fi มีความแรงเพียงพอ

5.4 ทดสอบการป้องกันความปลอดภัย เช่น การตั้งค่า Firewall

การทดสอบการตั้งค่า Firewall เป็นส่วนสำคัญในการปกป้องเครือข่ายจากการโจมตีภายนอก

- วิธีการทดสอบ:
    - ทดสอบการบล็อก Port: หากต้องการให้ Firewall บล็อกการเข้าถึงบางพอร์ต ให้ลองเชื่อมต่อไปยังพอร์ตเหล่านั้นจากคอมพิวเตอร์อื่นในเครือข่าย โดยใช้เครื่องมือเช่น Telnet หรือ Nmap เพื่อดูว่า Firewall บล็อกการเชื่อมต่อหรือไม่
        - ตัวอย่าง: telnet [IP Address] [Port Number]

- ตรวจสอบการตั้งค่า Firewall ใน Router: ตรวจสอบว่าได้ตั้งค่าให้ Firewall ป้องกันการเข้าถึงจากภายนอกที่ไม่พึงประสงค์ และเปิดพอร์ตเฉพาะที่จำเป็น
- ทดสอบจากภายนอก: ใช้เครื่องมือออนไลน์ เช่น ShieldsUP เพื่อทดสอบว่า Router หรือ Firewall ของคุณเปิดพอร์ตที่ไม่ปลอดภัยหรือไม่

6.การดูแลรักษาและตรวจสอบความปลอดภัย

6.1 หลังจากการติดตั้งเสร็จสิ้น ต้องทำการตั้งค่าความปลอดภัย เช่น:

- การตั้งค่า Firewall
- การตั้งรหัสผ่านที่ปลอดภัย
- การอัปเดตเฟิร์มแวร์ของอุปกรณ์เครือข่าย
- การใช้ VPN (Virtual Private Network) หากต้องการการเชื่อมต่อระยะไกลที่ปลอดภัย

การตั้งค่า Firewall

การตั้งค่าไฟร์วอลล์ (Firewall) เป็นการป้องกันการเข้าถึงที่ไม่พึงประสงค์จากภายนอก และช่วยกรองการเข้าถึงข้อมูลที่มาจากเครือข่ายภายนอก

- การตั้งค่า Firewall ใน Router หรือ Access Point:
    1. เข้าไปที่การตั้งค่า Router หรือ Access Point: เปิดเว็บเบราว์เซอร์และพิมพ์ IP ของ Router (โดยทั่วไปจะเป็น 192.168.1.1 หรือ 192.168.0.1)
    2. เข้าสู่หน้าการตั้งค่า: ใช้ชื่อผู้ใช้และรหัสผ่านของ Router เพื่อเข้าสู่ระบบการตั้งค่า
    3. ไปที่ส่วนการตั้งค่า Firewall: หาหมวดหมู่ที่เกี่ยวกับการตั้งค่าความปลอดภัยหรือ Firewall
    4. ตั้งค่าไฟร์วอลล์: เปิดใช้ฟังก์ชันการกรองพอร์ตที่ไม่จำเป็น และตั้งค่าการบล็อกพอร์ตที่ใช้ในทางที่ไม่ปลอดภัย (เช่น พอร์ต 23, 445 เป็นต้น)
    5. ตั้งค่าการบล็อกการเข้าถึงจาก IP ที่ไม่พึงประสงค์: ถ้าจำเป็นสามารถตั้งค่าการบล็อก IP ที่ไม่รู้จักหรือผิดปกติที่พยายามจะเข้ามาในระบบ
- การใช้ Firewall บนอุปกรณ์แต่ละเครื่อง: บนอุปกรณ์คอมพิวเตอร์และเซิร์ฟเวอร์ ควรเปิดใช้ซอฟต์แวร์ Firewall เช่น Windows Firewall หรือ Firewall ของระบบปฏิบัติการ Linux

6.2 การตั้งรหัสผ่านที่ปลอดภัย

รหัสผ่านที่ปลอดภัยช่วยป้องกันไม่ให้บุคคลที่ไม่ได้รับอนุญาตสามารถเข้าถึงอุปกรณ์หรือระบบของคุณได้

- การตั้งรหัสผ่านสำหรับ Router หรือ Access Point:
    1. ใช้รหัสผ่านที่มีความยาว (อย่างน้อย 12-16 ตัวอักษร)
    2. ผสมผสานระหว่างตัวอักษรใหญ่ ตัวอักษรเล็ก ตัวเลข และสัญลักษณ์
    3. หลีกเลี่ยงการใช้รหัสผ่านที่ง่ายหรือสามารถคาดเดาได้ เช่น "123456" หรือ "password"
    4. เปลี่ยนรหัสผ่านจากค่าดั้งเดิมที่มาพร้อมกับอุปกรณ์ (default password) เสมอ
- การตั้งรหัสผ่านสำหรับ Wi-Fi:
    1. ใช้รหัสผ่าน Wi-Fi ที่มีความยาวและซับซ้อน
    2. ใช้การเข้ารหัสแบบ WPA3 (ถ้าอุปกรณ์รองรับ) เพื่อความปลอดภัยที่สูงสุด
    3. หากเป็น WPA2, ควรตั้งรหัสผ่านที่มีความยาวและหลีกเลี่ยงการใช้รหัสผ่านที่ง่าย
    4. ปิดฟังก์ชัน WPS (Wi-Fi Protected Setup) หากไม่จำเป็น เพราะสามารถเป็นช่องโหว่ด้านความปลอดภัย

6.3 การอัปเดตเฟิร์มแวร์ของอุปกรณ์เครือข่าย

การอัปเดตเฟิร์มแวร์เป็นการอัปเกรดระบบปฏิบัติการของอุปกรณ์ที่ใช้ในเครือข่าย ซึ่งการอัปเดตเฟิร์มแวร์มักจะมีการแก้ไขข้อผิดพลาดและช่องโหว่ด้านความปลอดภัย

- วิธีการอัปเดตเฟิร์มแวร์:
    1. ตรวจสอบการอัปเดตจากผู้ผลิต: เข้าไปที่เว็บไซต์ของผู้ผลิตอุปกรณ์ (เช่น Router หรือ Access Point) และตรวจสอบว่ามีเวอร์ชันเฟิร์มแวร์ใหม่หรือไม่
    2. เข้าสู่หน้าเว็บการตั้งค่าของอุปกรณ์: เช่นเดียวกับการตั้งค่า Firewall เข้าไปที่หน้าเว็บของ Router หรือ Access Point
    3. ค้นหาฟังก์ชันการอัปเดตเฟิร์มแวร์: โดยปกติจะมีฟังก์ชันที่ให้คุณอัปโหลดไฟล์เฟิร์มแวร์ใหม่
    4. อัปเดตเฟิร์มแวร์: หากมีเวอร์ชันใหม่ ให้ทำการดาวน์โหลดและติดตั้งเฟิร์มแวร์ใหม่
    5. ตรวจสอบการอัปเดต: หลังจากอัปเดตเสร็จแล้ว ควรตรวจสอบว่าอุปกรณ์สามารถทำงานได้อย่างปกติ

6.4 การใช้ VPN (Virtual Private Network) สำหรับการเชื่อมต่อระยะไกลที่ปลอดภัยVPN เป็นเครื่องมือที่ใช้ในการสร้างการเชื่อมต่อที่ปลอดภัยระหว่างอุปกรณ์ของคุณและเครือข่ายภายนอก เช่น การเชื่อมต่อกับเครือข่ายสำนักงานจากระยะไกล

- การติดตั้งและใช้งาน VPN:
    1. เลือกผู้ให้บริการ VPN: คุณสามารถเลือกใช้บริการ VPN ที่เชื่อถือได้ เช่น NordVPN, ExpressVPN หรือใช้การตั้งค่า VPN บนอุปกรณ์เครือข่ายของคุณ เช่น Router ที่รองรับการเชื่อมต่อ VPN
    2. ตั้งค่า VPN บนอุปกรณ์: บนอุปกรณ์เช่น คอมพิวเตอร์หรือมือถือ ให้ติดตั้งแอปพลิเคชัน VPN และเชื่อมต่อกับเซิร์ฟเวอร์ VPN ที่ให้บริการ
    3. ตั้งค่า VPN บน Router: หากต้องการให้ทั้งบ้านหรือสำนักงานเชื่อมต่อผ่าน VPN คุณสามารถตั้งค่า VPN บน Router ได้โดยตรง ซึ่งทำให้ทุกอุปกรณ์ในเครือข่ายภายในเชื่อมต่อผ่าน VPN โดยอัตโนมัติ

สรุป

การดูแลรักษาความปลอดภัยของเครือข่ายไม่ใช่แค่การตั้งค่าเริ่มต้นเท่านั้น แต่ยังต้องมีการดูแลและตรวจสอบอย่างต่อเนื่องด้วยการตั้งค่า Firewall, การใช้รหัสผ่านที่ปลอดภัย, การอัปเดตเฟิร์มแวร์, และการใช้ VPN เพื่อป้องกันการเข้าถึงที่ไม่พึงประสงค์จากผู้ไม่หวังดี ทั้งนี้จะช่วยให้ระบบเครือข่ายของคุณมีความปลอดภัยและพร้อมใช้งานได้ตลอดเวลา

ขอขอบคุณข้อมูลจากเว็บไซต์

http://www.ddsure.net/network_device.php

บทที่ 4

วิธีการปฏิบัติงาน

ในการทำคู่มือ เรื่อง การดูแลระบบเครือข่ายอินเตอร์เน็ตและอุปกรณ์เครือข่าย
การให้บริการซ่อมและติดตั้งแก้ไขระบบเครือข่าย อินเตอร์เน็ต ภายในมหาวิทยาลัยขอนแก่น
เพื่อให้แนวทางในการดูแล ตรวจสอบ และบำรุงรักษาระบบเครือข่ายอินเตอร์เน็ตและอุปกรณ์ที่เกี่ยวข้องให้
สามารถใช้งานได้อย่างมีประสิทธิภาพและต่อเนื่อง จึงได้จัดทำคู่มือฉบับนี้ขึ้นมา
ผู้จัดทำได้เขียนวิธีการปฏิบัติงานตามรายระเอียดดังต่อไปนี้

4.1 ขั้นตอนการปฏิบัติงาน

4.1.1 หน่วยงาน/คณะ/นักศึกษาหรือบุคลากรที่แจ้งความประสงค์ขอความอนุเคราะห์ ติดตั้งใช้งานระบบ
สัญญาณเครือข่ายอินเตอร์เน็ต หรืออุปกรณ์เครือข่ายเสียหายชำรุด สายต่อพวงสัญญาณไม่สามารถใช้งานได้
เกิดความเสียหายจาก ภัยธรรมชาติ หรือสัตว์ ภายในมหาวิทยาลัยขอนแก่น เสนอบันทึกข้อความ พร้อมแนบ
รายละเอียดและเหตุผลในการขอใช้บริการเสนอผู้อำนวยการสำนักเทคโนโลยีดิจิทัล เพื่อพิจารณา

ภาพที่ 1 : แสดงบันทึกข้อความ เรื่อง ขอความอนุเคราะห์ติดตั้งสายแลนระบบสัญญาณเครือข่ายอินเตอร์เน็ต

สำนักเทคโนโลยีดิจิทัล
เลขที่รับ 355
วันที่ 26 ก.พ. 2568
เวลา 14:04 น.

บันทึกข้อความ

ส่วนงาน สำนักงานอธิการบดี กองการกีฬา มหาวิทยาลัยขอนแก่น โทร. 50894
ที่ อว 660201.1.13/ ๒๖๔ วันที่ 26 กุมภาพันธ์ 2568
เรื่อง ขอความอนุเคราะห์ติดตั้งสายแลน (LAN Cable) สำหรับใช้ INTERNET
เรียน ผู้อำนวยการสำนักเทคโนโลยีดิจิทัล

ด้วยจังหวัดขอนแก่น ได้รับเกียรติจากกรมพลศึกษา กระทรวงการท่องเที่ยวและกีฬา ให้เป็นเจ้าภาพจัดการแข่งขันกีฬานักเรียน นักศึกษาแห่งชาติ ครั้งที่ 22 ประจำปี 2568 "แก่นคูณเกมส์" ในระหว่างวันที่ 10-15 มีนาคม พ.ศ. 2568 ณ จังหวัดขอนแก่น และมหาวิทยาลัยขอนแก่นได้ตอบรับเป็นเจ้าภาพร่วมด้วย โดยมอบหมายให้ฝ่ายพัฒนานักศึกษาและศิษย์เก่าสัมพันธ์ และกองการกีฬารับผิดชอบดำเนินการและประสานงาน

ในการนี้ เพื่อให้การดำเนินการเป็นไปด้วยความเรียบร้อยและบรรลุวัตถุประสงค์ กองการกีฬา จึงใคร่ขอความอนุเคราะห์หน่วยงานของท่านสำรวจและติดตั้งสายแลน (LAN Cable) สำหรับใช้ INTERNET ภายในห้องเทคโนโลยีสารสนเทศ ชั้น 2 อาคารพลศึกษาอเนกประสงค์ เพื่อใช้สำหรับอำนวยความสะดวกแก่ผู้สื่อข่าวและสื่อมวลชน ในการจัดการแข่งขันกีฬาในระหว่างวันที่ 10-15 มีนาคม พ.ศ. 2568 จำนวน 10 จุด ทั้งนี้ ได้มอบหมายให้ นายชยากร เสนาภักดิ์ นักวิชาการศึกษา หมายเลขโทรศัพท์ 09 5565 6549 ภายใน 50895 ไปรษณีย์อิเล็กทรอนิกส์ chayse@kku.ac.th และนายสุรศักดิ์ ลาภประสิทธิ์ เจ้าหน้าที่สถานกีฬาประจำพื้นที่ หมายเลขโทรศัพท์ 08 9618 9683 เป็นผู้ติดต่อประสานงาน

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ และขอขอบคุณมา ณ โอกาสนี้

รองผู้อำนวยการฝ่ายโครงสร้างพื้นฐานทางสารสนเทศ
เพื่อโปรดพิจารณา
เห็นควรแจ้งหัวหน้างานโครงสร้างพื้นฐานฯ เพื่อโปรดดำเนินการและประสานงานต่อไป

(นายพิชูรย์ มูลศรี)
รักษาการแทนผู้อำนวยการกองการกีฬา

ดำเนินการตามเสนอ
อ.ดร. เพชร อิ่มทองคำ
รองผู้อำนวยการฝ่ายโครงสร้างพื้นฐานทางสารสนเทศ
สำนักเทคโนโลยีดิจิทัล
4 มี.ค. 2568

(นายสมโภช พิมพ์พงษ์ค้อน)
ผู้อำนวยการกองบริหารงานสำนักโนโลยีดิจิทัล
วันที่ 26 ก.พ. 2568 16:52 น.

งานบริการสถานกีฬา กองการกีฬา สำนักงานอธิการบดี มหาวิทยาลัยขอนแก่น

(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ภาพที่ 2 : แสดงบันทึกข้อความ เรื่อง ขอความอนุเคราะห์ติดตั้ง Switch กระจายสัญญาณเครือข่ายอินเตอร์เน็ต

บันทึกข้อความ

สำนักเทคโนโลยีดิจิทัล
เลขที่รับ 404
วันที่ 5 มี.ค. 2568
เวลา 13:57 น.

ส่วนงาน สำนักงานอธิการบดี กองบริหารงานวิจัย งานพัสดุ โทร 50118
ที่ อว660201.1.10.1/ ๓๙๓ **วันที่** ๕ มีนาคม 2568
เรื่อง ขอความอนุเคราะห์ติดตั้ง switch กระจายสัญญาณอินเตอร์เน็ต

เรียน ผู้อำนวยการสำนักเทคโนโลยีดิจิทัล

ตามบันทึกข้อความที่ อว 660201.1.10.1/ว 533 ลงวันที่ 26 กุมภาพันธ์ 2568 เรื่อง แจ้งย้ายสำนักงานชั่วคราว โดยกองบริหารงานวิจัยได้รับความอนุเคราะห์จากสถาบันวิจัยและพัฒนาวิชาชีพครูสำหรับอาเซียน ให้ใช้ห้องประชุมชั้น 2 ห้อง 1201 เพื่อใช้เป็นห้องสำนักงานกองบริหารงานวิจัยชั่วคราว ตั้งแต่วันที่ 27 กุมภาพันธ์ – 24 กันยายน 2568 ความละเอียดแจ้งแล้วนั้น

ในการนี้เพื่อให้บุคลากรกองบริหารงานวิจัย สามารถใช้สัญญาณอินเตอร์เน็ตเพื่อปฏิบัติงานและติดต่อราชการในช่วงระยะเวลาดังกล่าวได้สะดวกและไม่ส่งผลกระทบต่อการปฏิบัติงาน จึงขอความอนุเคราะห์ติดตั้ง switch กระจายสัญญาณอินเตอร์เน็ต ณ ห้องประชุมชั้น 2 ห้อง 1201 ทั้งนี้ ได้ประสานงานกับเจ้าหน้าที่ไว้เรียบร้อยแล้ว ตามหมายเลขครุภัณฑ์ 6417130000032 และมอบหมายให้นางสุณิษา แสงเหลา เบอร์โทรศัพท์ 084-6426702 เป็นผู้ประสานงาน

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ด้วย จักขอบคุณยิ่ง

รองผู้อำนวยการฝ่ายโครงสร้างพื้นฐานทางสารสนเทศ
เพื่อโปรดพิจารณา
เห็นควรส่งให้หัวหน้างานโครงสร้างพื้นฐานฯเพื่อโปรดดำเนินการและประสานงานต่อไป

(นางสาวกฤติกา แดงรัตน์)
รักษาการแทนผู้อำนวยการกองบริหารงานวิจัย

(นายสมโภช พิมพ์พงษ์ต้อน)
ผู้อำนวยการกองบริหารงานสำนักโนโลยีดิจิทัล
วันที่ 5 มี.ค. 2568 16:14 น.

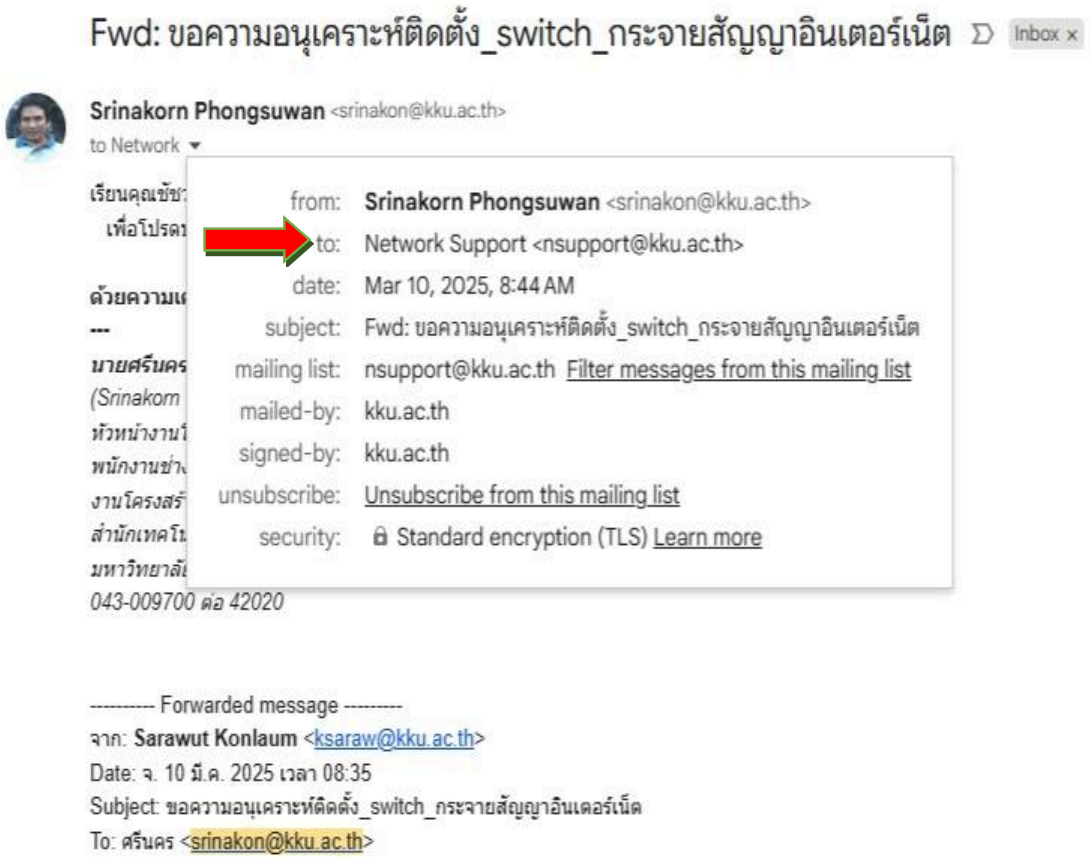
(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

4.1.2 เจ้าหน้าที่บริหารงานทั่วไป ลงรับบันทึกข้อความเรื่อง ขอความอนุเคราะห์ติดตั้งระบบสัญญาณเครือข่ายอินเตอร์เน็ต เสนอ ผู้อำนวยการสำนักเทคโนโลยีดิจิทัล

ผู้อำนวยการสำนักเทคโนโลยีดิจิทัล ได้เห็นควรเสนอหัวหน้ากลุ่มภารกิจโครงสร้างพื้นฐานระบบดิจิทัลดำเนินการและประสานงานต่อไป

4.1.3 หัวหน้ากลุ่มภารกิจโครงสร้างพื้นฐานระบบดิจิทัล มอบหมายงานให้กับช่างเทคนิค โดยส่ง E-Mail Network Support กลุ่มงานโครงสร้างพื้นฐานให้รับทราบและดำเนินการต่อไป

ภาพที่ 3 : แสดงหัวหน้ากลุ่มภารกิจโครงสร้างพื้นฐานระบบดิจิทัล มอบหมายงานให้กับช่างเทคนิค



(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

4.1.4 ช่างเทคนิค รับทราบและดำเนินการจัดเตรียมอุปกรณ์เครือข่าย พร้อมติดตั้งและดำเนินการต่อไป

สิ่งที่ต้องเตรียม :

- Switching อุปกรณ์ตัวกลาง ที่ทำหน้าที่กระจายสัญญาณการสื่อสารให้กับอุปกรณ์อื่นๆ ผ่านสายแลนหรือใยแก้วนำแสง
- สายสัญญาณ LAN เพื่อเป็นตัวกลางที่เชื่อมต่อหรือส่งถ่ายข้อมูลระหว่างระบบคอมพิวเตอร์และอุปกรณ์เชื่อมต่อเครือข่าย
- Access Point ตัวกระจายสัญญาณ wifi ไปยังอุปกรณ์ต่างๆ
- คีมเข้าหัวสายสัญญาณ หัวแลน หรือหัว RJ-45
- เครื่องทดสอบสาย แลนหรือสายสัญญาณ ใช้ในการตรวจเช็คสาย
- สว่านไขควง น๊อต คีมตัดสาย เคเบิ้ลไทร์ลัดสาย
- อุปกรณ์อื่นๆที่ใช้ในการติดตั้งระบบเครือข่าย

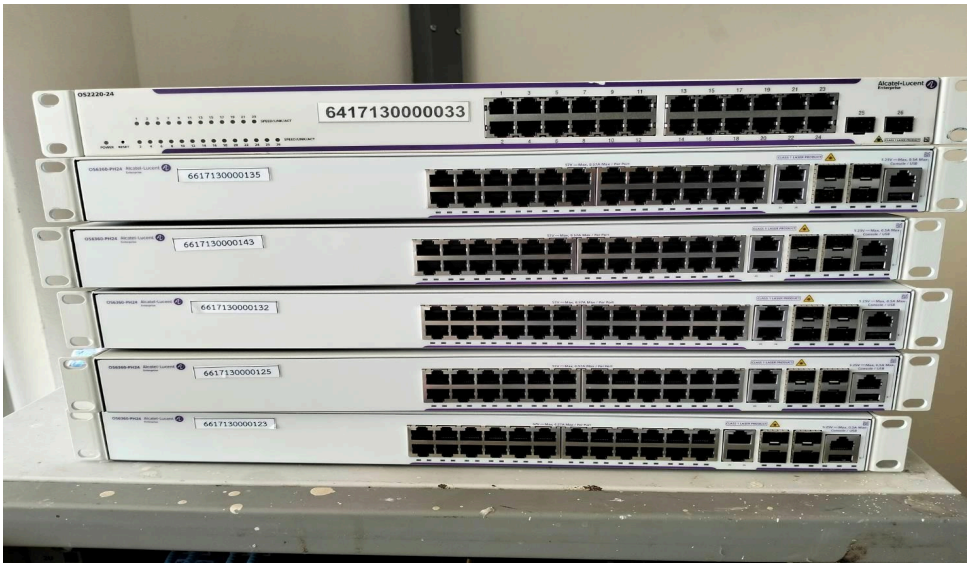
ภาพที่ 4 : แสดงอุปกรณ์เครือข่ายที่ใช้ในการติดตั้ง

(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

4.1.5 อุปกรณ์เครือข่ายที่สำคัญในการดำเนินการติดตั้ง

- ช่างเทคนิคได้จัดเตรียม Switch Alcatel-Lucent OS 2220-24
  Switch Alcatel-Lucent 6360 เพื่อใช้ในการ Config Switch ทำหน้าที่กระจายสัญญาณการสื่อสารให้กับอุปกรณ์อื่นๆ และนำไปติดตั้งใช้งาน

ภาพที่ 5 : Switch Alcatel-Lucent OS 2220-24

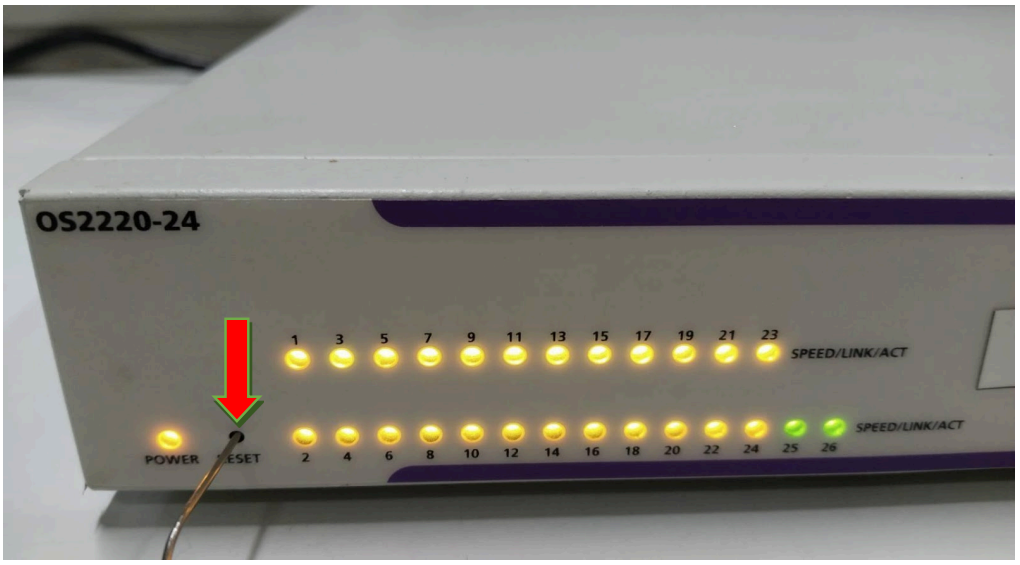


(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

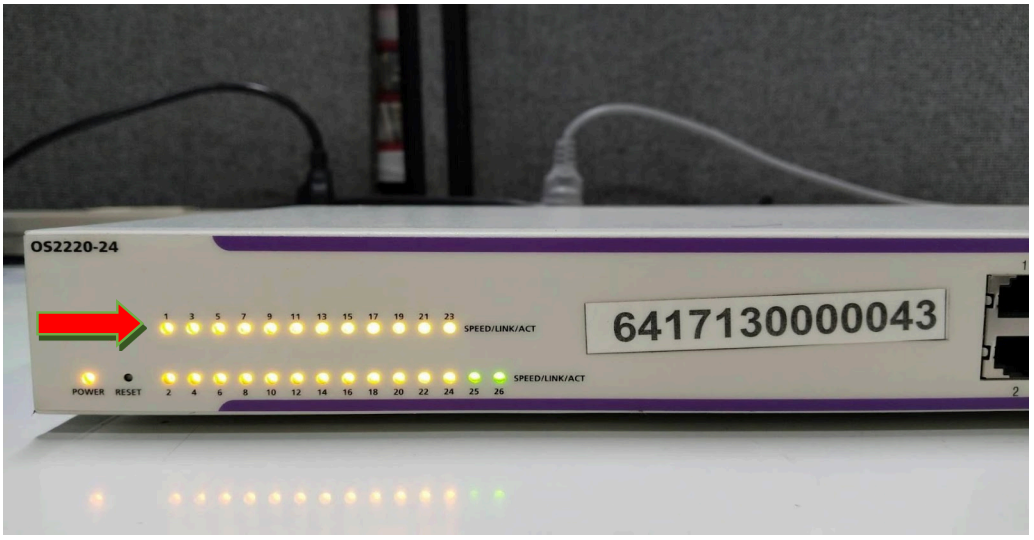
4.1.6 ช่างเทคนิคทำการ Reset อุปกรณ์ Switch Alcatel-Lucent OS 2220-24

- เริ่มจากตรวจสอบอุปกรณ์ Switch Alcatel-Lucent OS 2220-24 เป็นอุปกรณ์ที่จัดซื้อมาใหม่ หรือเป็นอุปกรณ์ที่ผ่านการติดตั้งใช้งานมาแล้ว ถ้าเป็นอุปกรณ์ใหม่สามารถ ทำการติดตั้งและ Config Switch ระบบใช้งานได้โดยไม่ต้องทำการ Reset
- ถ้าผ่านการใช้งานมาแล้ว ต้องทำการ Reset ค่าใหม่ โดยการใช้เข็มหรืออุปกรณ์ที่มีขนาดพอดีกับรูเสียบ Reset ของตัวสวิตย์ กดเข้าไปตรงคำสั่ง Reset จนกว่าไฟสีส้มจะขึ้นมาแล้วปล่อยให้อุปกรณ์ Reboot ระบบจนเสร็จ Switch ก็จะได้ค่าเริ่มต้นที่โรงงานผลิตตั้งไว้ หรือเรียกว่าค่า Defaulf

ภาพที่ 6 : แสดงวิธีการ Reset Switch Alcatel-Lucent OS 2220-24



ภาพที่ 7: รอจนกว่าไฟสีส้มจะดับลง ดังรูปต่อไปนี้



(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ภาพที่ 8 : แสดงไฟสีส้มดับลง Reset Switch เสร็จสิ้น ได้ค่าเริ่มต้นที่โรงงานผลิต ค่า Defaulf

4.1.7 ขั้นตอนต่อมา ช่างเทคนิคจัดเตรียมเครื่องคอมพิวเตอร์ Notebook

- ใช้ในการตั้งค่าระบบความจำเป็นให้กับเครื่องคอมพิวเตอร์ Notebook ให้สามารถเชื่อมต่อกับ Switch Alcatel-Lucent OS 2220-24 ได้

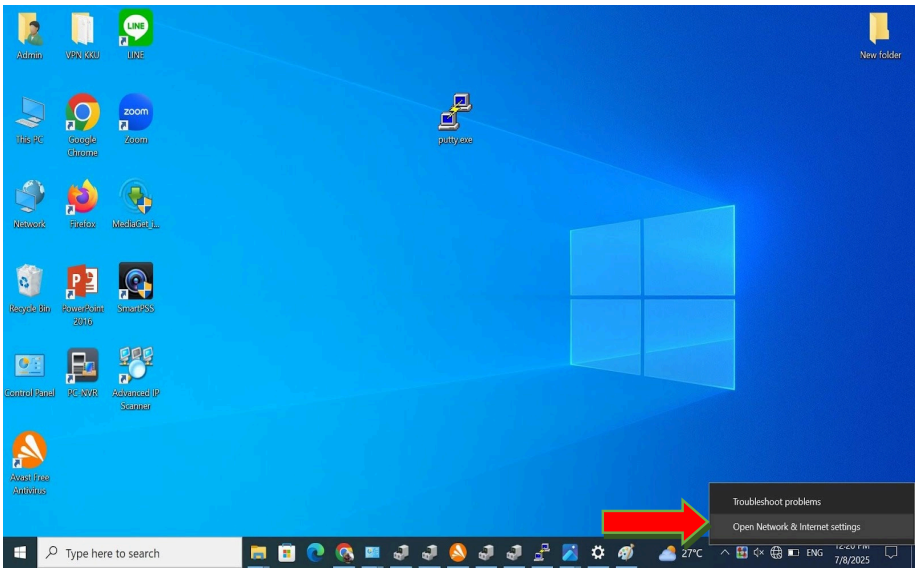
ภาพที่ 9

(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

4.1.8 ช่างเทคนิค ได้จัดทำขั้นตอนการตั้งค่า ระบบค่าความจำเป็นเครื่องคอมพิวเตอร์ Notebook ให้สามารถเชื่อมต่อกับ Switch Alcatel-Lucent OS 2220-24 ตามขั้นตอนต่อไปนี้

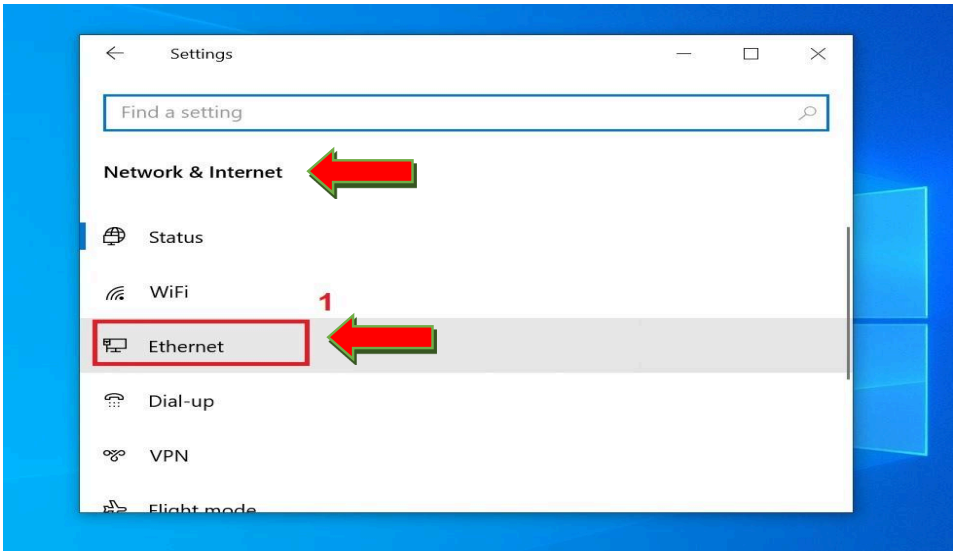
- **ขั้นตอนที่ 1:** กดคลิกเมาส์เข้าไปที่ open network & Internet settings

ภาพที่ 10



- **ขั้นตอนที่ 2 :** จะปรากฏหน้าจอ Network & lnternet กดคลิกเมาส์เข้าไปที่ Ethernet (หมายเลข1)

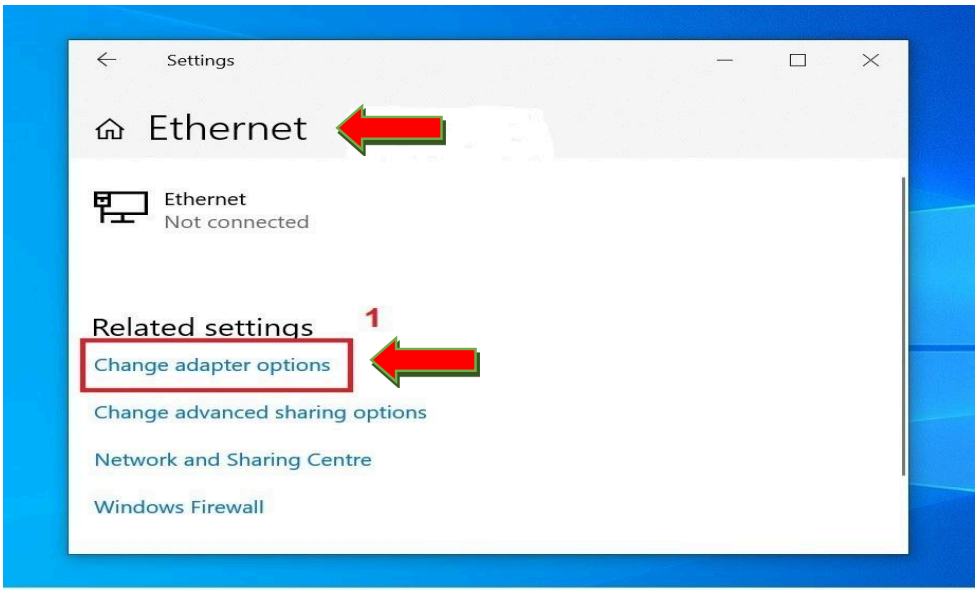
ภาพที่ 11



(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

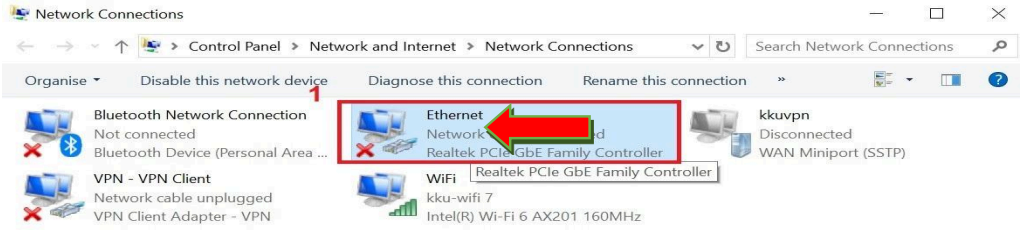
- **ขั้นตอนที่ 3:** จะปรากฏหน้าจอ Ethernet กดคลิกเมาส์เข้าไปที่ Change adapter options (หมายเลข 1)

ภาพที่ 12



- **ขั้นตอนที่ 4:** กดคลิกเมาส์เลือก Ethernet (หมายเลข 1)

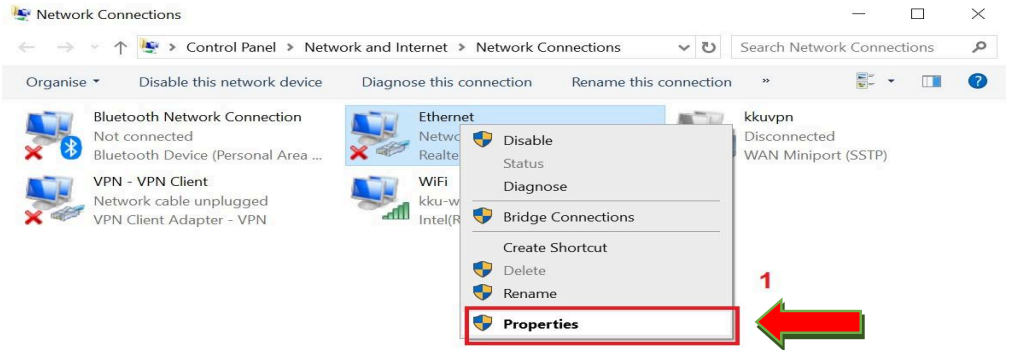
ภาพที่ 13



(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

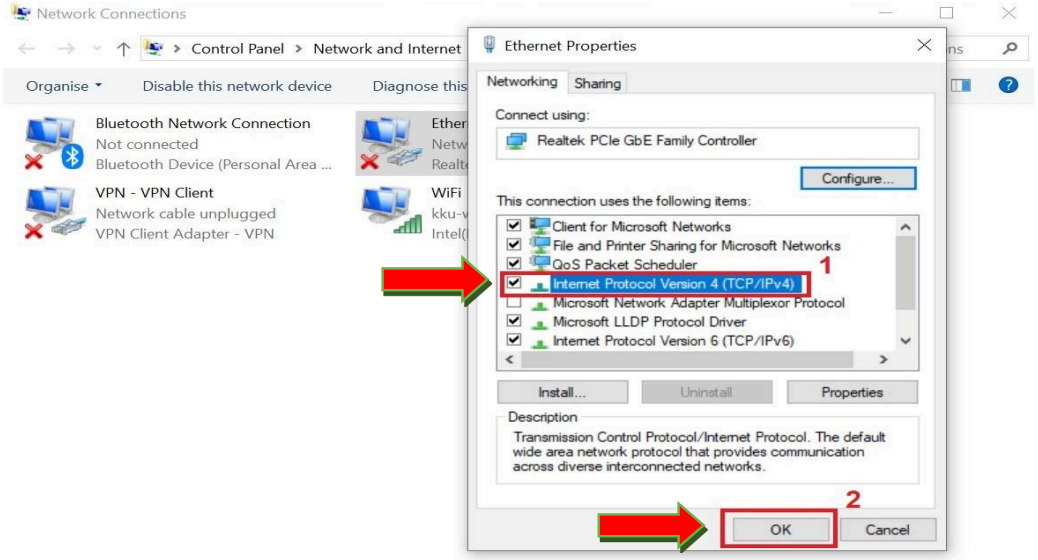
- **ขั้นตอนที่ 5:** กดคลิกเมาส์มุมขวามือ Ethernet เลื่อนลูกศรลงมาคลิกเมาส์ไปที่ Properties (หมายเลข 1)

ภาพที่ 14



- **ขั้นตอนที่ 6:** กดคลิกเมาส์เข้าไปที่ Internet protocol version 4 (TCP/IPv4) (หมายเลข 1) เสร็จแล้วกด ok เพื่อไปยังขั้นตอนต่อไป (หมายเลข 2)

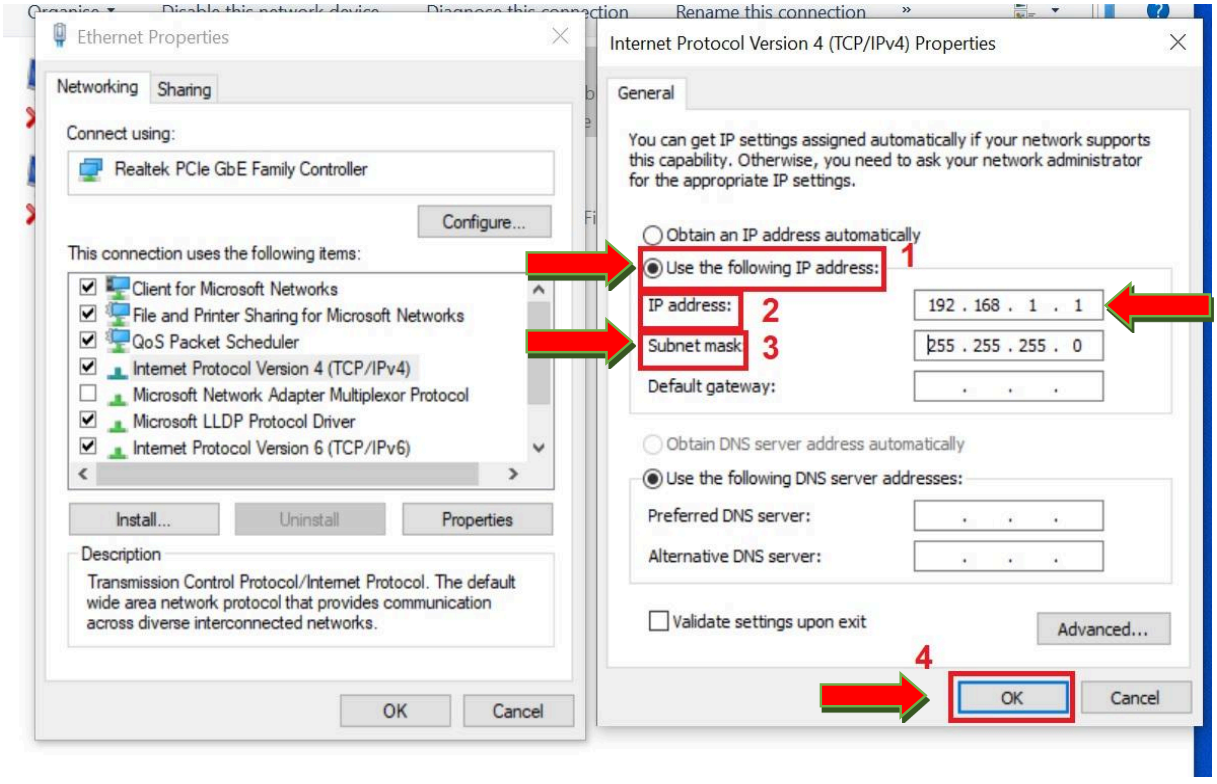
ภาพที่ 15



(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

- **ขั้นตอนที่ 7**
    - กดคลิกเมาส์เข้าไปที่ use the following IP address (หมายเลข 1)
    - ใส่ค่า IP Address ค่าความจำเป็น 192.168.1.1 (หมายเลข 2)
    - Subnet mask ค่าความจำเป็น 255.255.255.0 (หมายเลข 3)
    - เสร็จแล้วกด ok (หมายเลข 4)
    - เครื่องคอมพิวเตอร์ Notebook พร้อมติดตั้งการเชื่อมต่อกับ Switch Alcatel-Lucent OS 2220-24

ภาพที่ 16: แสดงการ Set ระบบความจำเป็นเครื่องคอมพิวเตอร์ Notebook พร้อมดำเนินการต่อไป



(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

4.1.9 ขั้นตอนการ ติดตั้งระบบ Config Switch Alcatel-Lucent OS 2220-24

(ผ่าน Web Interface**)** อุปกรณ์ Layer 2 ของสำนักเทคโนโลยีดิจิทัล เพื่อนำไปติดตั้ง คณะ/หน่วยงาน หอพักนักศึกษา ให้สามารถใช้งานระบบเครือข่ายอินเตอร์เน็ตได้อย่างมีประสิทธิภาพ

- ช่างเทคนิค ทำขั้นตอนในการติดตั้งเครื่องคอมพิวเตอร์ Notebook เชื่อมต่อเข้ากับ Switch Alcatel-Lucent OS 2220-24 มีขั้นตอนดังต่อไปนี้

ขั้นตอนที่ 1

ภาพที่ 17: แสดงการติดตั้งเครื่องคอมพิวเตอร์ Notebook เชื่อมต่อเข้ากับ Switch Alcatel

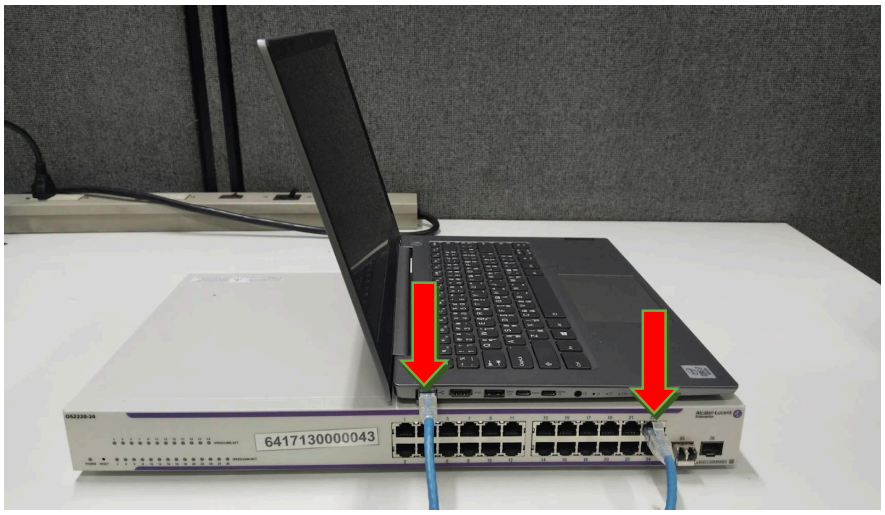
- โน๊ตบุ๊กต้องมีพอร์ต LAN (หรือใช้ USB-to-LAN Adapter ถ้าไม่มี)

ภาพที่ 18

(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

- เสียบสาย LAN ด้านหนึ่งเข้ากับ Port LAN เครื่องคอมพิวเตอร์ Notebook และอีกด้านเสียบเข้ากับ Port Network Switch (Port ใดก็ได้) ช่างเทคนิค เลือกใช้งาน Port 23

ภาพที่ 19



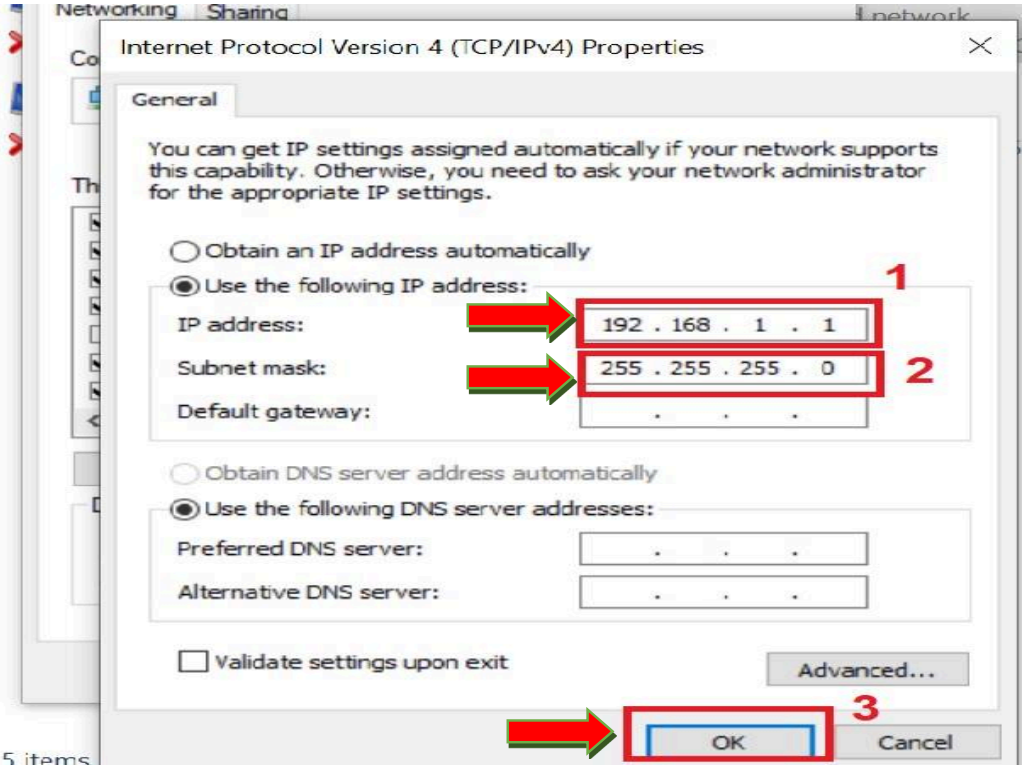
ภาพที่ 20 : ภาพแสดง USB-to-LAN Adapter ถ้าโน๊ตบุ๊กไม่มีพอร์ต LAN

(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 2

- เครื่องคอมพิวเตอร์ Notebook ช่างเทคนิค ใส่ค่าความจำเป็นไว้ก่อนหน้านี้ IP address :192.168.1.1
  ตามขั้นตอนที่ 7 ภาพที่ 16 เพื่อไม่ให้ IP address เหมือนกัน จะทำให้ไม่สามารถเข้าไปตั้งค่าความจำเป็นระบบได้ (หมายเลข 1)
- Subnet mask :255.255.255.0 (หมายเลข2)
- แล้วทำการกด ok เพื่อไปยังขั้นตอนต่อไป (หมายเลข3)

ภาพที่ 21: แสดงการตั้งค่าความจำเป็น เครื่องคอมพิวเตอร์ Notebook (ดังภาพที่ 16)

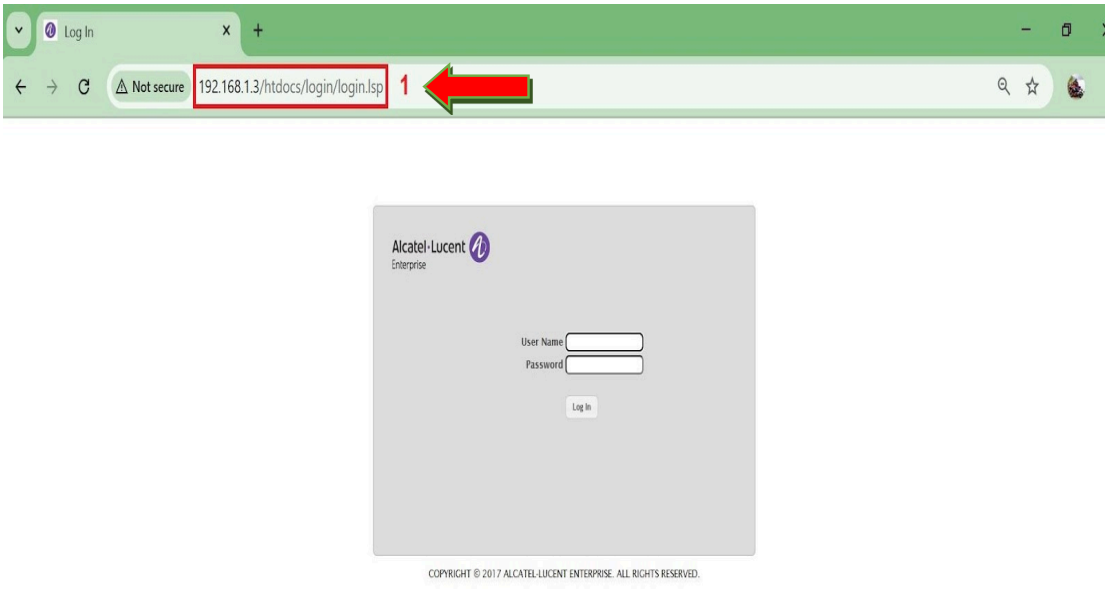


(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 3

- คำสั่ง IP Default จากโรงงานผลิต Switch Alcatel-Lucent OS 2220-24 คือ 192.168.1.3
- ช่างเทคนิค เปิดเว็บเบราว์เซอร์พิมพ์คำสั่งที่ช่อง URL:// 192.168.1.3 (ค่า Default จากโรงงานผลิต) (หมายเลข 1)

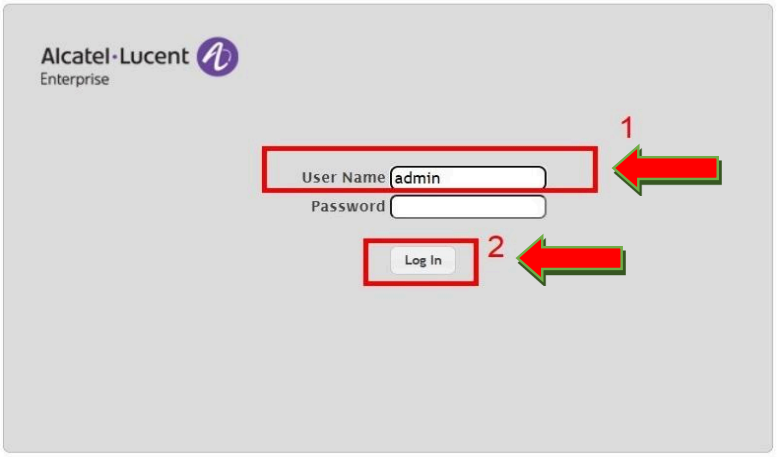
ภาพที่ 22 : แสดงภาพหน้าจอเข้าระบบ Config Switch Alcatel **(**ผ่าน Web Interface**)**



ขั้นตอนที่ 4

- ช่างเทคนิค พิมพ์คำสั่ง Default user : admin (หมายเลข 1)
- Password ไม่ต้องใส่ค่าความจำเป็น ทำการ Log In เพื่อไปยังขั้นตอนต่อไป (หมายเลข 2)

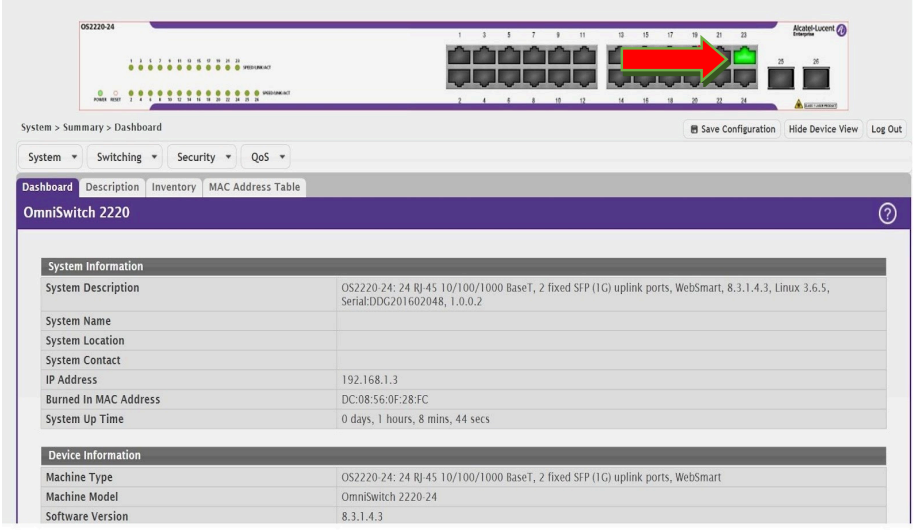
ภาพที่ 23



ขั้นตอนที่ 5

- จะเห็นว่า Switch Port 23 มีไฟสีเขียวปรากฏขึ้น เป็นการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ Notebook เข้ากับ Switch Port 23 ถูกต้องตามที่ช่างเทคนิคกำหนดไว้

ภาพที่ 24 : แสดงภาพหน้าจอ ระบบปฏิบัติการ Config Switch Alcatel-Lucent

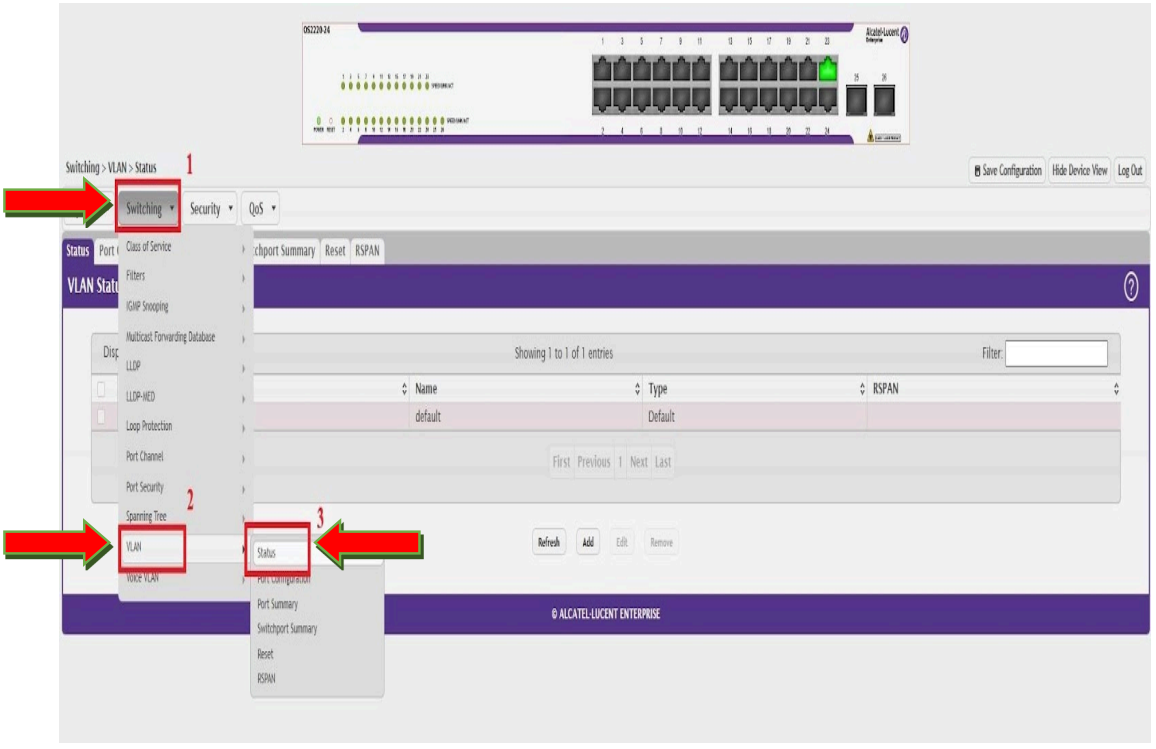


(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 6

- ช่างเทคนิค การตั้งค่าความจำเป็นสำหรับการ Config Switch
- กดคลิกเมาส์ไปที่ Switching (หมายเลข 1)
- VLAN (หมายเลข 2)
- Status เพื่อไปยังขั้นตอนต่อไป (หมายเลข 3)

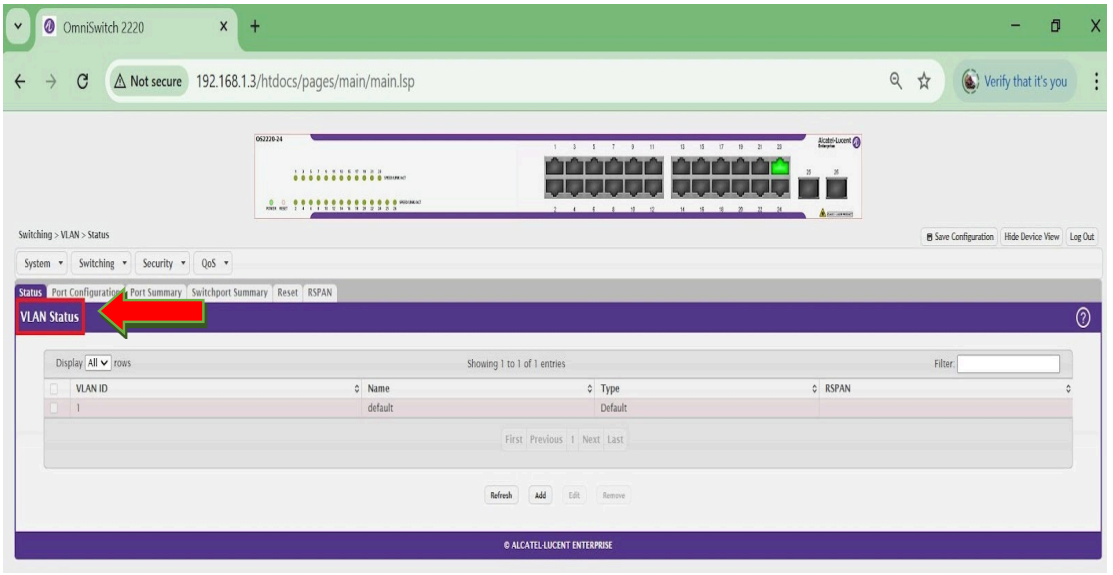
ภาพที่ 25



(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 7

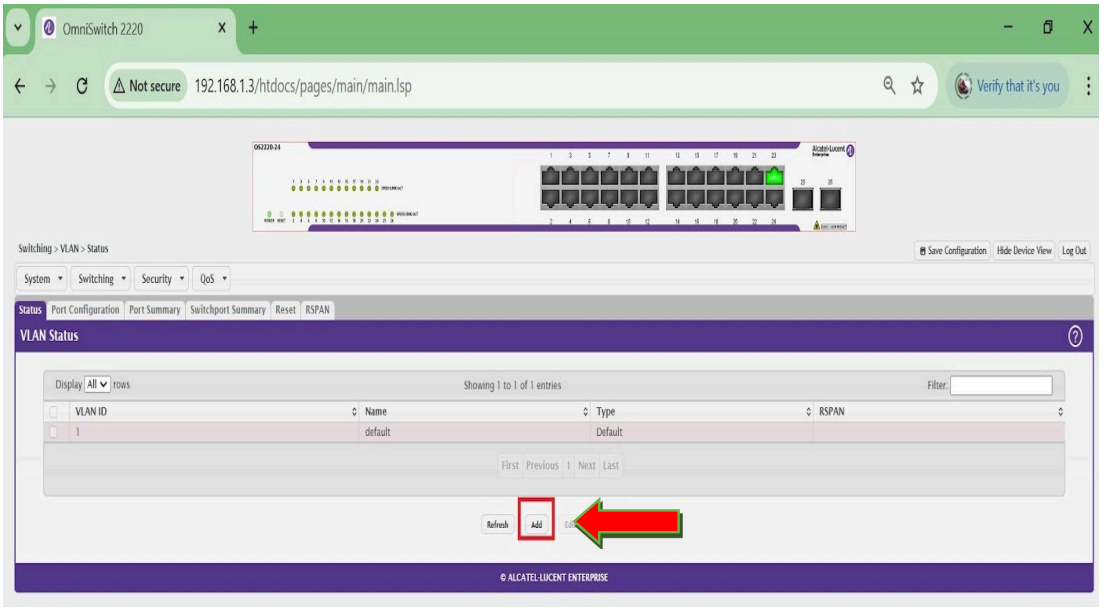
ภาพที่ 26 : แสดงหน้าจอ VLAN Status



ขั้นตอนที่ 8

- ช่างเทคนิค กดคลิกเมาส์ Add เพื่อจะกำหนด VLAN ID , VLAN Management ให้กับระบบ เพื่อใช้ในการเชื่อมต่อสัญญาณเครือข่าย

ภาพที่ 27

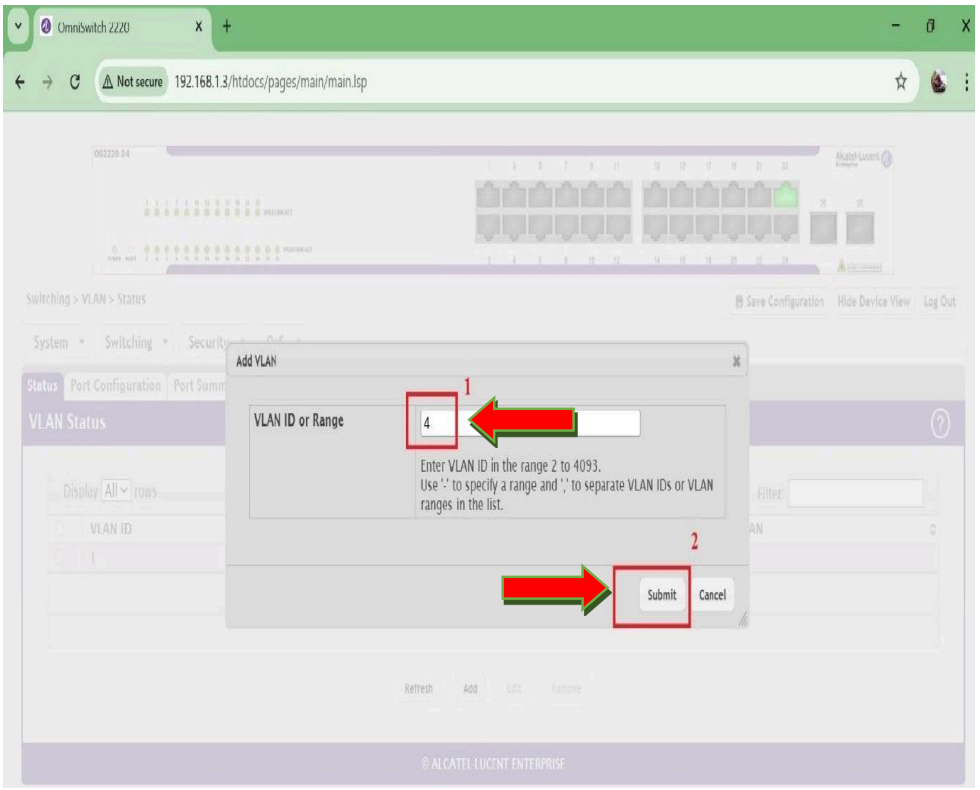


(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 9

- ช่างเทคนิคได้กำหนดค่าความจำเป็น VLAN ID 4 ซึ่งเป็น VLAN สำหรับใช้งานอินเตอร์เน็ต (หมายเลข1)
- แล้วกด Supmit เพื่อไปยังขั้นตอนต่อไป (หมายเลข 2)

ภาพที่ 28

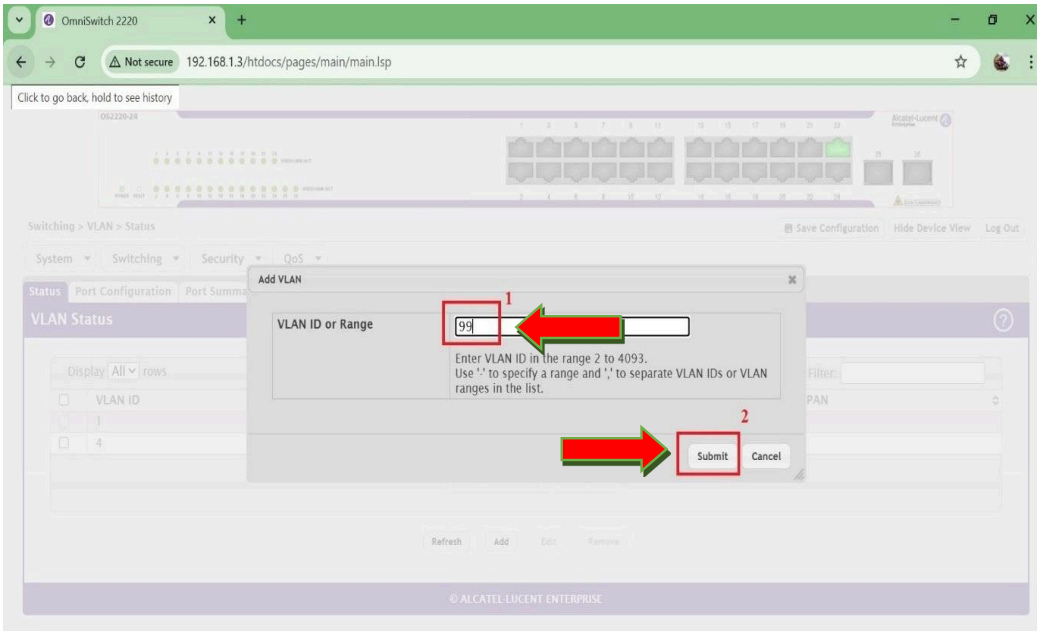


(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 10

- ช่างเทคนิคได้กำหนดค่าความจำเป็น VLAN Management ให้กับ Switch โดยการเพิ่ม VLAN ID 99 (หมายเลข 1)
- กด Supmit เพื่อไปยังขั้นตอนต่อไป (หมายเลข 2)

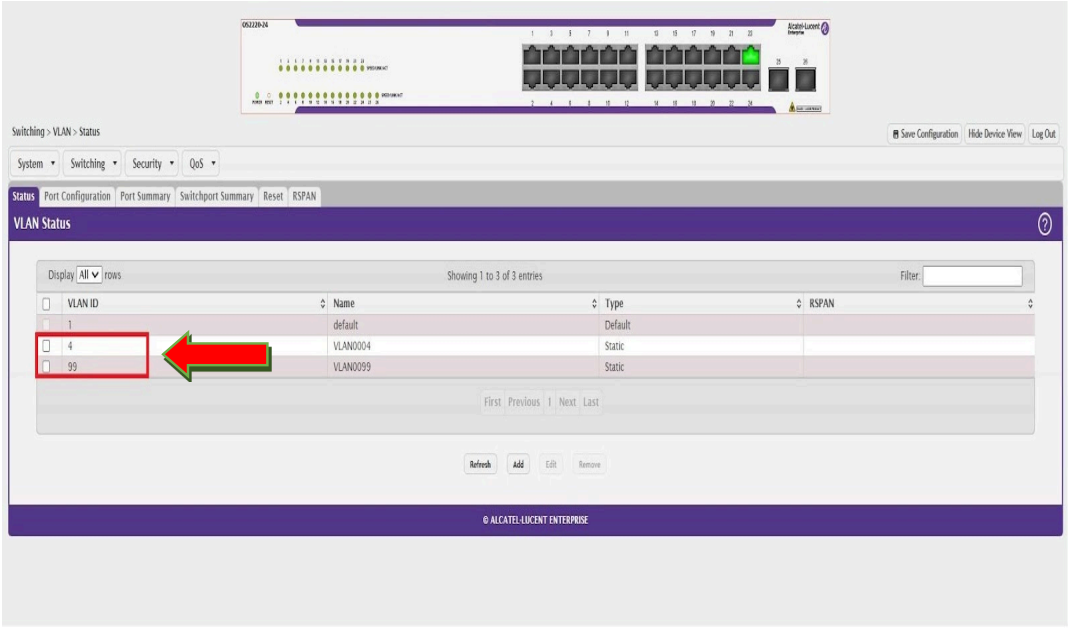
ภาพที่ 29



ขั้นตอนที่ 11

- ช่างเทคนิคตรวจดู Status VLAN ID ที่ทำการกำหนดค่า VLAN 4 และ VLAN 99 ถูกต้องตามที่ได้กำหนดค่าไว้

ภาพที่ 30

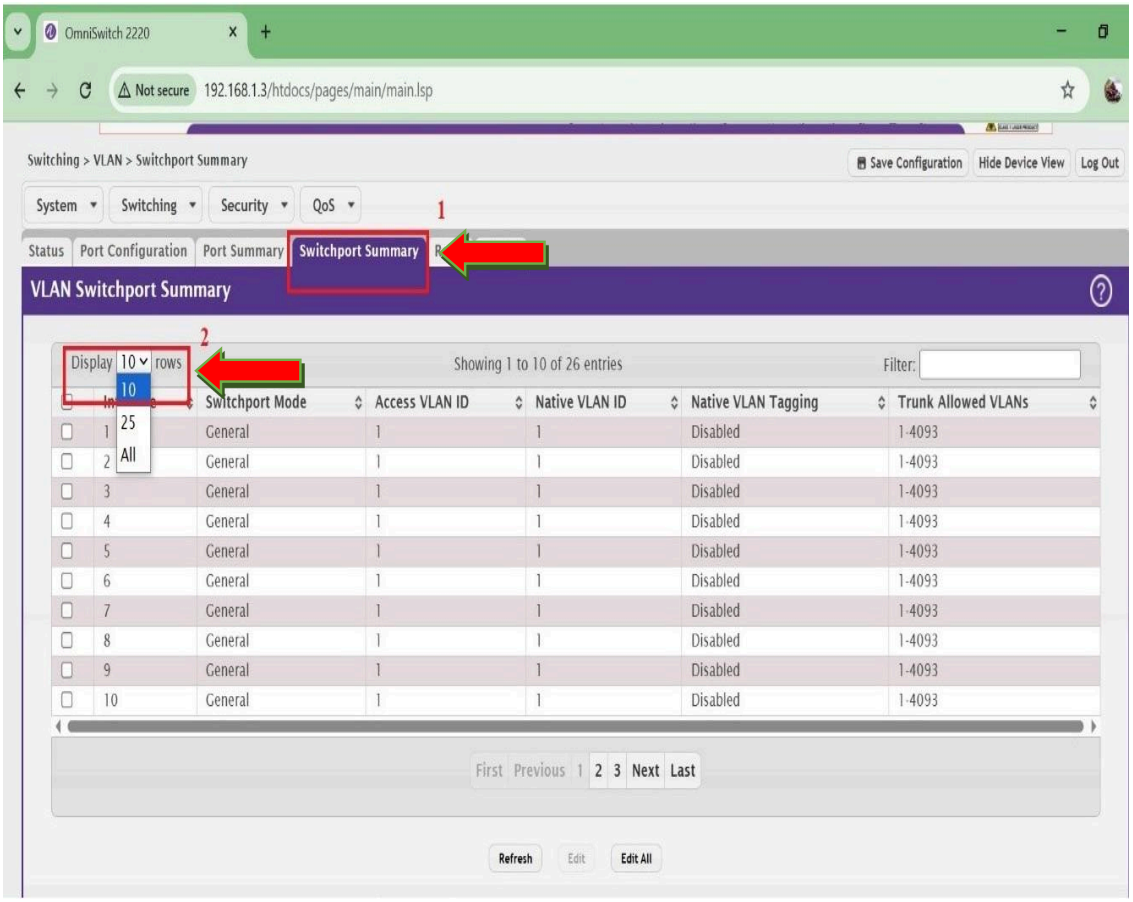


(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 12

- ช่างเทคนิค คลิกเมาส์เข้าไปที่ Switchport Summary (หมายเลข1)
- Display rows เพื่อเข้าไปกำหนด Port ใช้งาน โดยช่างเทคนิคเลือกใช้งาน 10 Port (หมายเลข2)

ภาพที่ 31

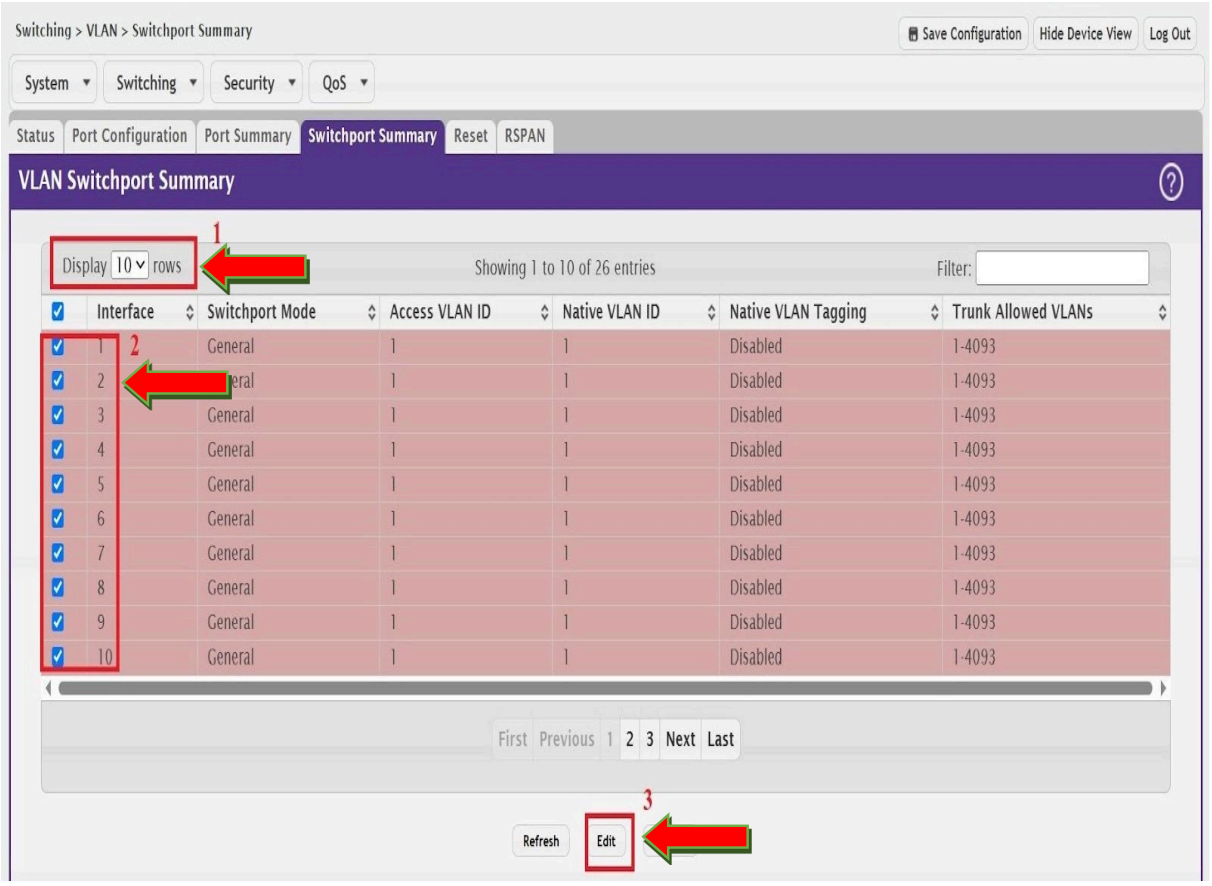


(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 13

- ช่างเทคนิคกดคลิกเมาส์เลือก ช่อง Display rows เลือกจำนวน 10 Port (หมายเลข1)
- ช่างเทคนิค ใส่เครื่องหมายถูกตรงช่อง Interface (หมายเลข2)
- Edit เพื่อไปยังขั้นตอนต่อไป (หมายเลข3)

ภาพที่ 32

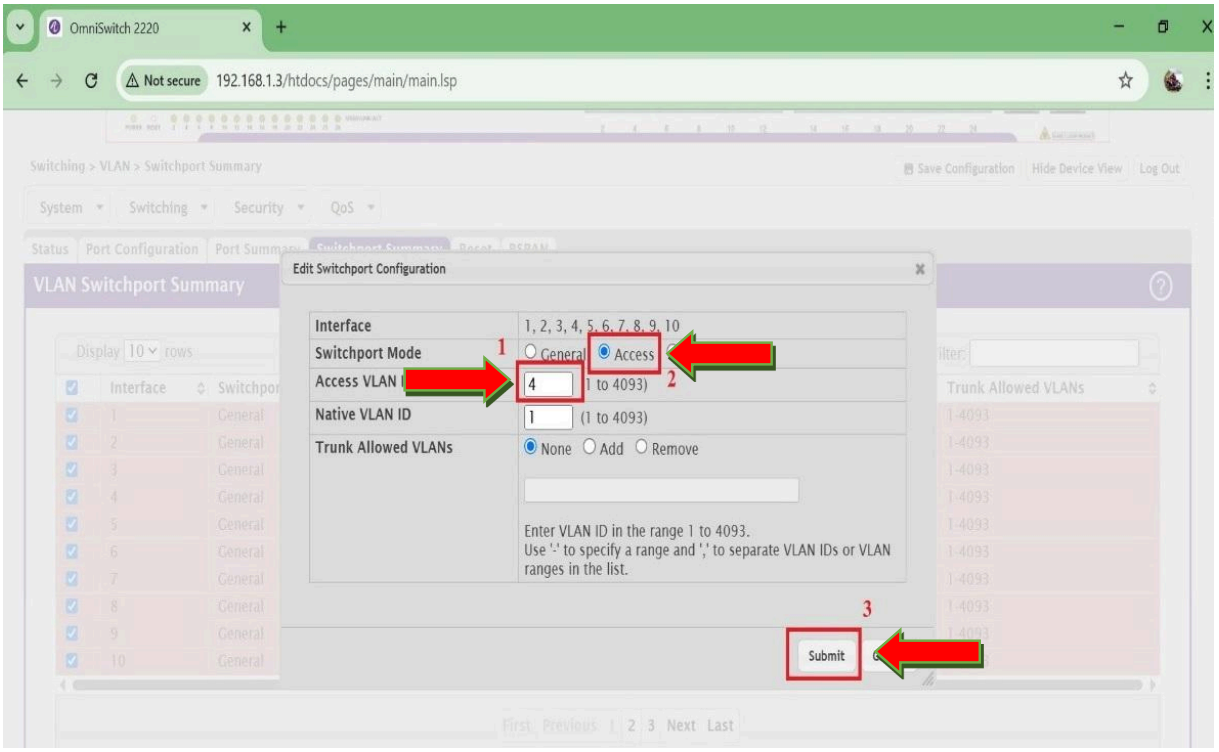


(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 14

- ช่างเทคนิค ตั้งค่าความจำเป็นสำหรับ Access VLAN ID ใส่ค่า VLAN 4 สำหรับใช้งานอินเตอร์เน็ต (หมายเลข1)
- กดเมาส์ไปที่ Switchport Mode เลือกคำสั่ง Access (หมายเลข2)
- กด Supmit เพื่อไปยังขั้นตอนต่อไป (หมายเลข3)

ภาพที่ 33

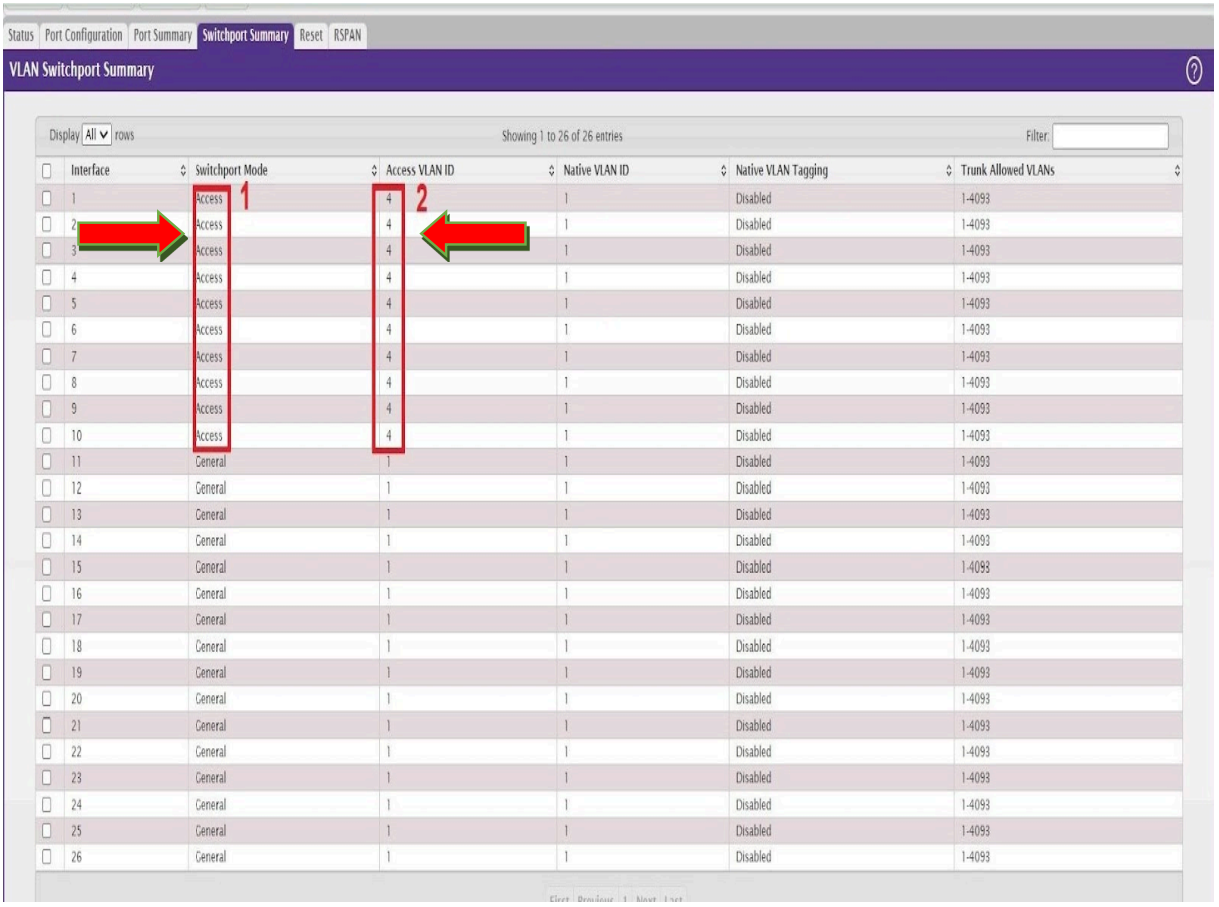


(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 15

- Switchport Mode จะเปลี่ยน จากค่าเดิม Ganeral เป็น Access จำนวน 10 Port ถูกต้องตามที่ได้ตั้งค่าไว้ (ดังภาพที่ 33) (หมายเลข1)
- Access VLAN ID จะเป็นเปลี่ยนเป็น 4 จำนวน 10 Port ถูกต้องตามที่ได้ตั้งค่าไว้ (ดังภาพที่ 33) (หมายเลข2)

ภาพที่ 34

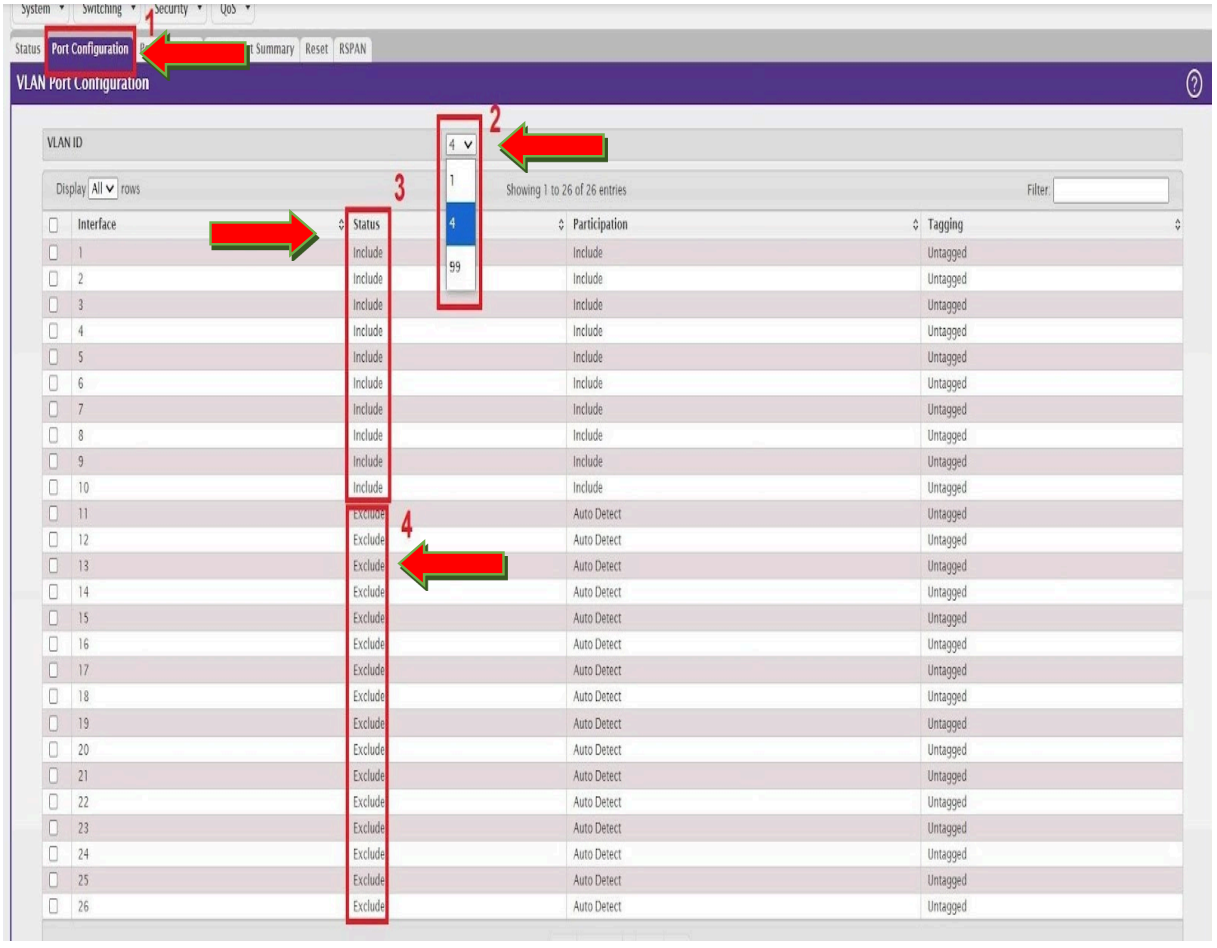


(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 16

- ช่างเทคนิค กดคลิกเมาส์เลือกเมนู Port Configuration เพื่อตรวจดูการตั้งค่าใช้งาน VLAN ID Port 1-10 ที่ช่างเทคนิคได้ตั้งค่าความจำเป็นไว้ (หมายเลข1)
- กดคลิกเมาส์เลือกดูที่ VLAN ID 4 (หมายเลข2)
- ค่า Status เปลี่ยนจาก Exclude ค่าเริ่มต้น (หมายเลข 4) เป็นค่า Include ทำการเปิด Port 1-10 ถูกต้องตามที่ได้ตั้งค่าไว้ (หมายเลข 3)

ภาพที่ 35

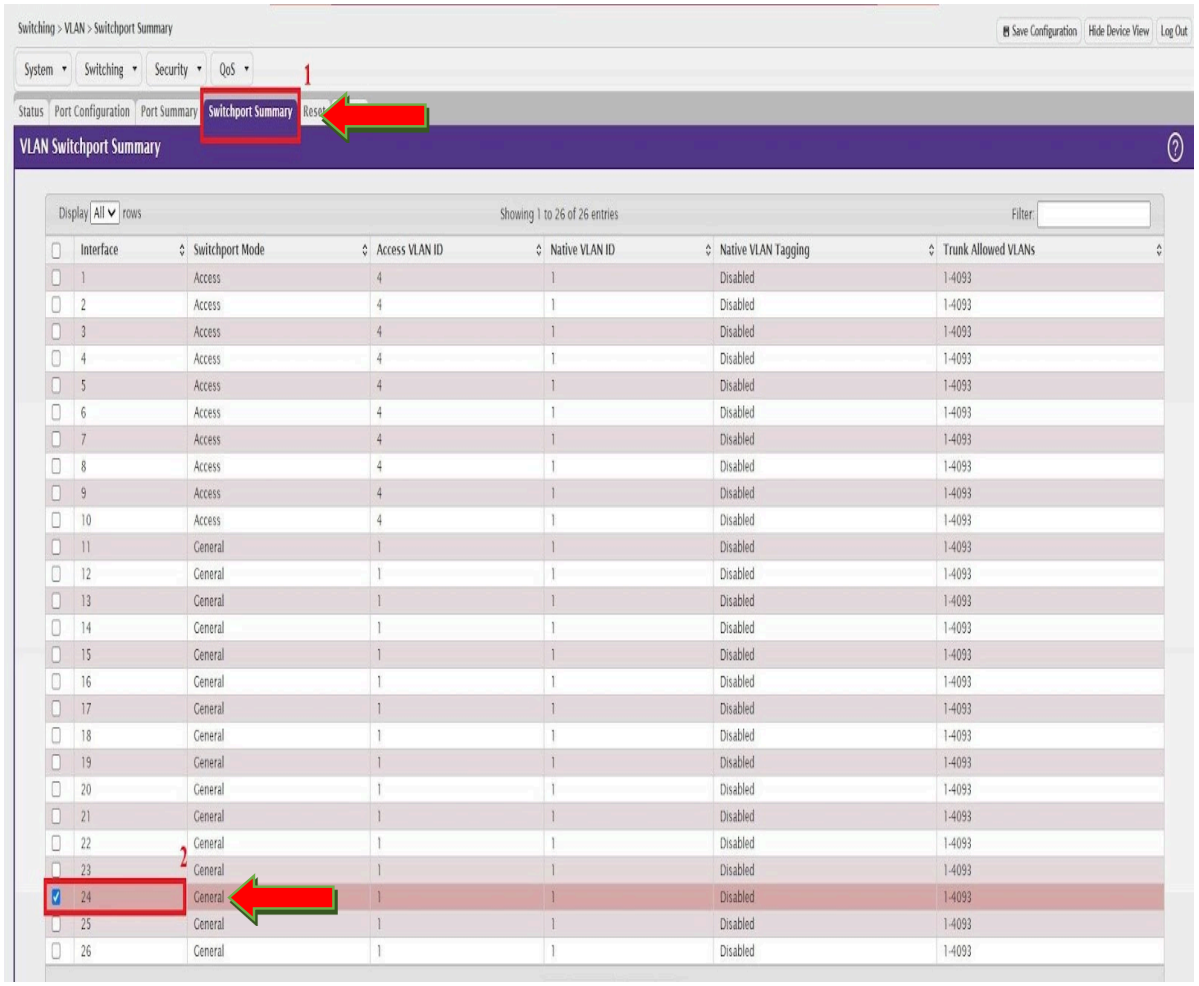


(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 17

- ช่างเทคนิค ตั้งค่าความจำเป็น VLAN Management
- ช่างเทคนิคคลิกเมาส์ที่ Switchport Summary
  ใส่เครื่องหมายถูก ช่อง interface port 24 เพื่อเข้าไปกำหนด VLAN 99 ซึ่งเป็น VLAN Management Switch ไปยังขั้นตอนต่อไป

ภาพที่ 36

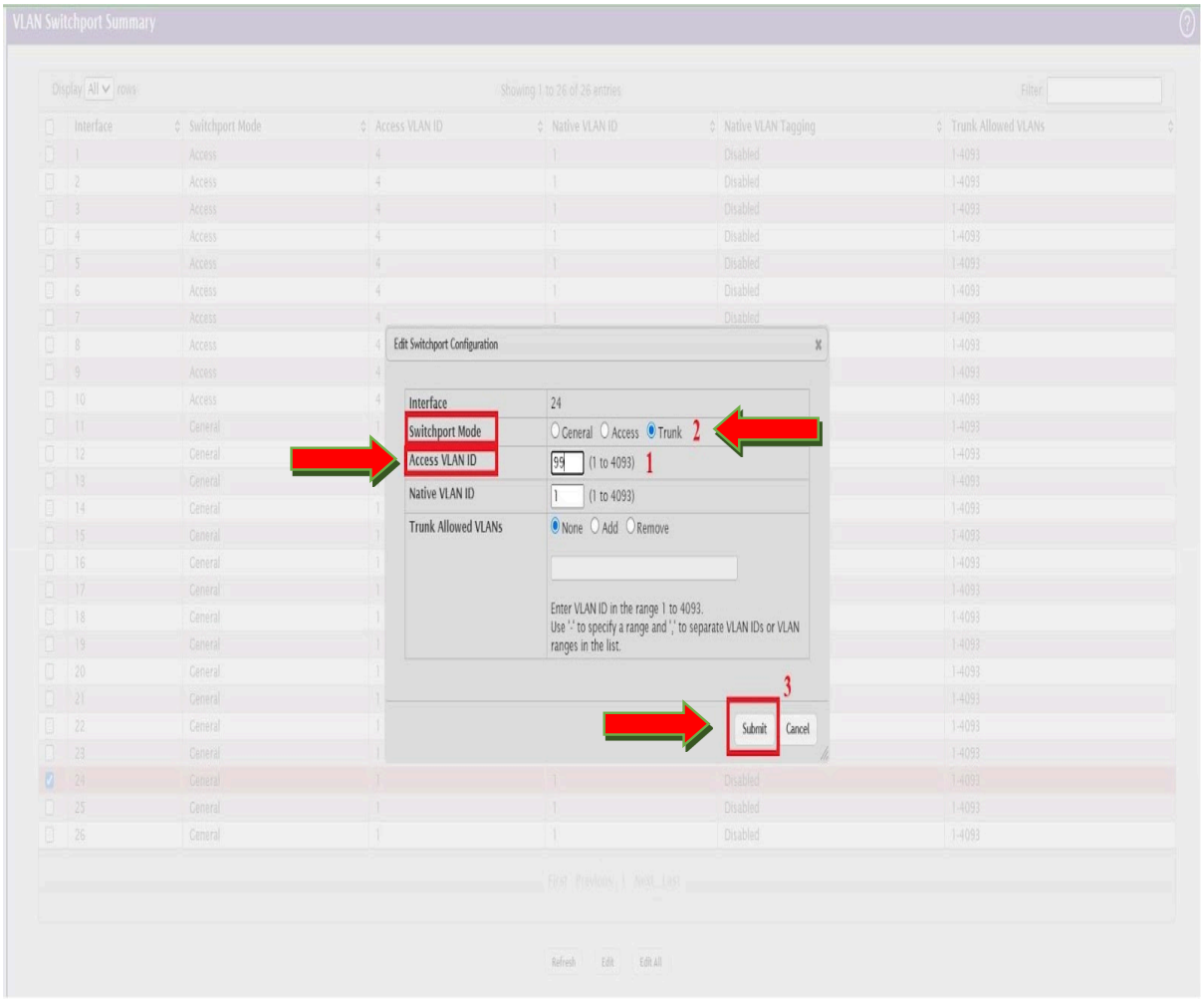


(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 18

- Access VLAN ID ใส่ค่า 99 เป็น VLAN Management (หมายเลข1)
- กดคลิกเมาส์ Switchport Mode เลือกคำสั่ง Trunk ซึ่งเป็น Port Uplink เพื่อใช้เชื่อมต่อกับอุปกรณ์เครือข่าย ที่มาจากจุดรับสัญญาณอื่น (หมายเลข2)
- Supmit เพื่อไปยังขั้นตอนต่อไป (หมายเลข3)

ภาพที่ 37

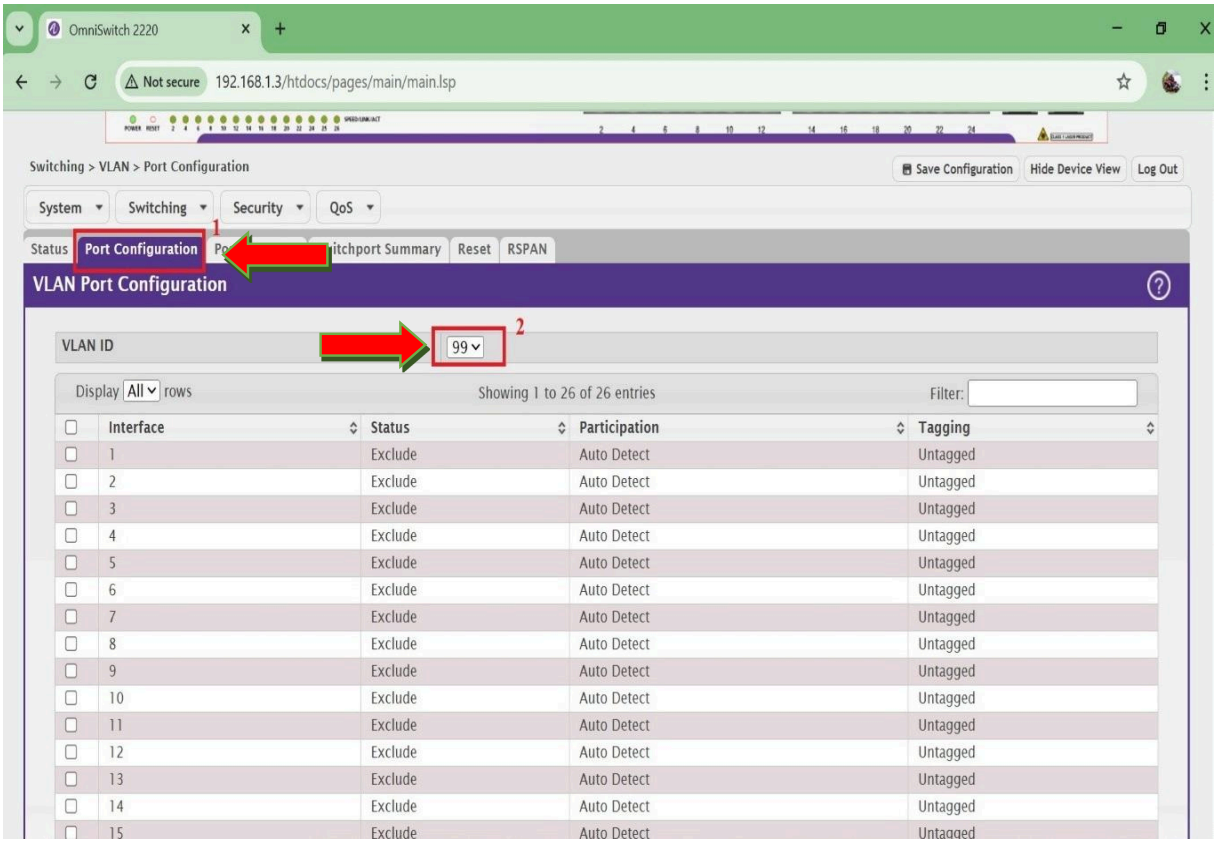


(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 19

- ช่างเทคนิคกดคลิกเมาส์เลือก Port Configuration (หมายเลข1)
- ตรวจการตั้งค่า VLAN Management VLAN 99 (หมายเลข2)

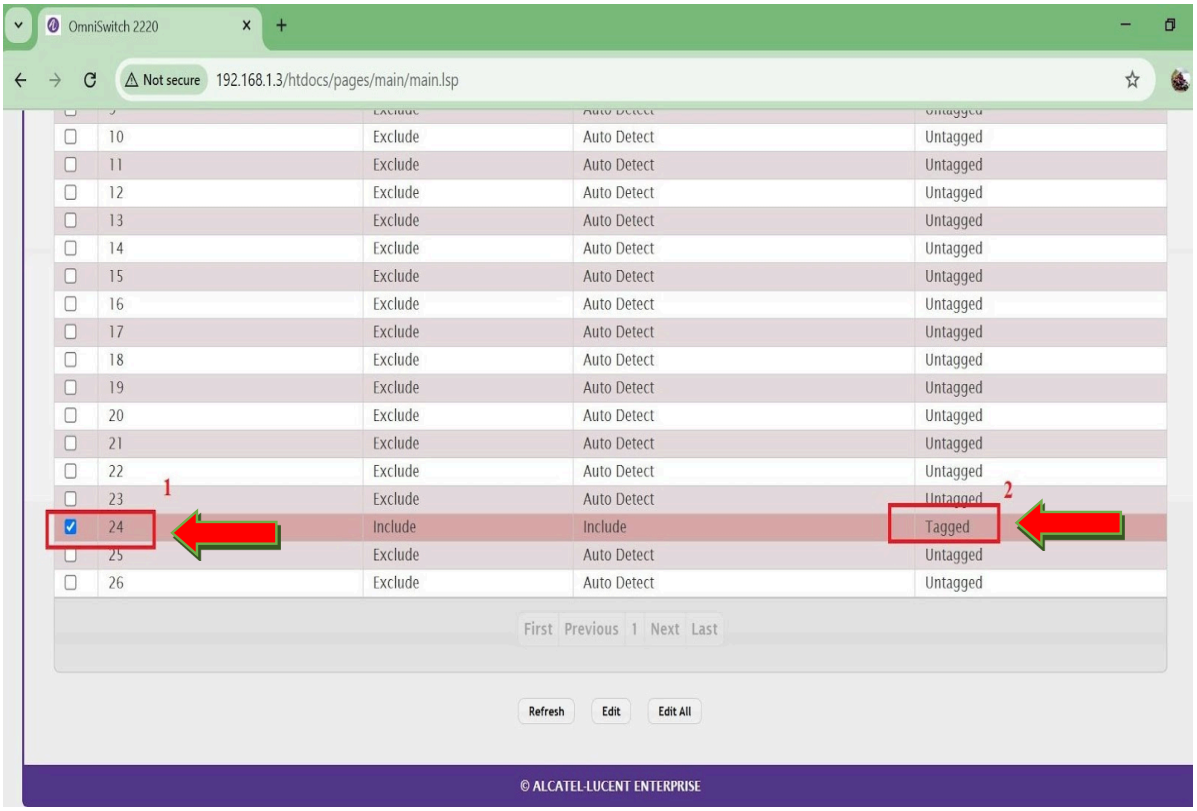
ภาพที่ 38



(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

- ช่างเทคนิคเช็คการตั้งค่า Port Configuration Port 24 (หมายเลข1)
- ค่าเดิม Untagged เปลี่ยน เป็น Tagged ถูกต้องตามที่ได้กำหนดค่าความจำเป็นไว้จากภาพที่ 37 (หมายเลข2)

ภาพที่ 39

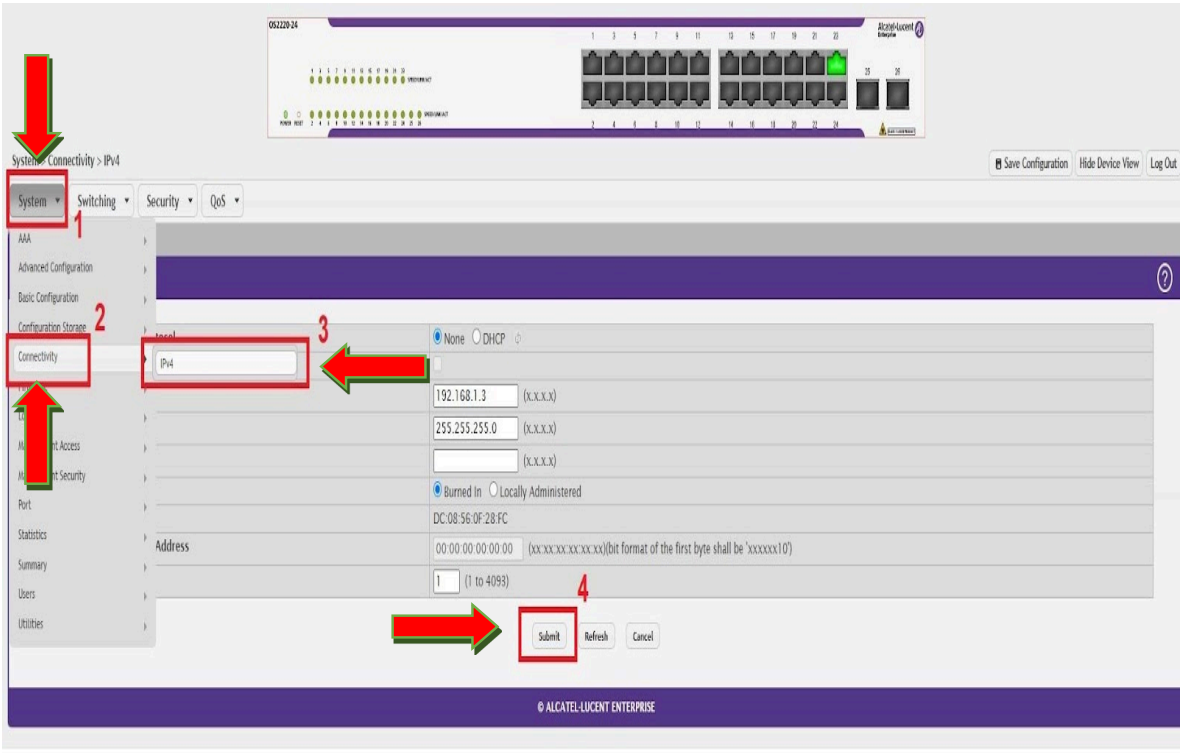


(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 20

- ช่างเทคนิค ทำการตั้งค่า IP Management VLAN ID กดคลิกเมาส์เลือก System (หมายเลข1)
- Connectivity (หมายเลข2)
- IPv4 (หมายเลข3)
- Supmit เพื่อดำเนินการต่อไป (หมายเลข4)

ภาพที่ 40

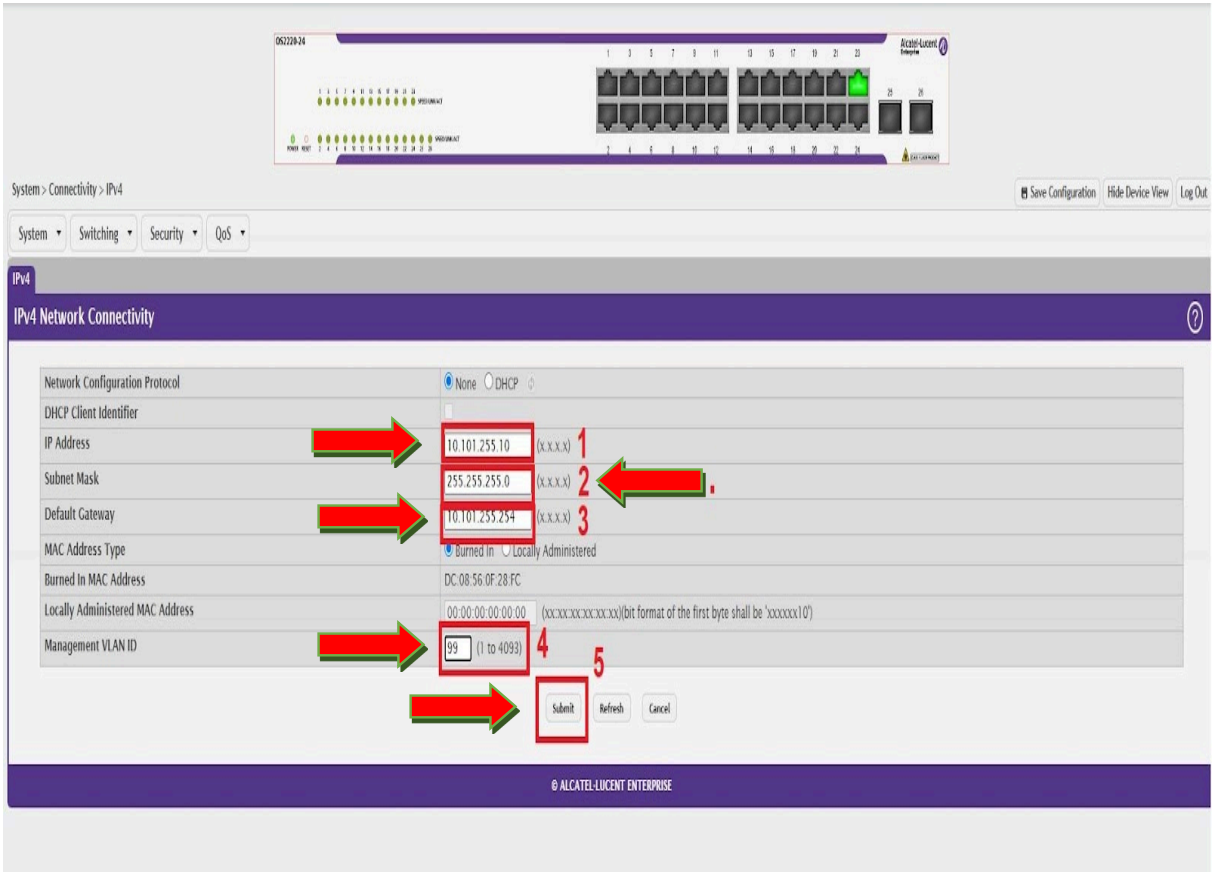


(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 21

- ช่างเทคนิค ตั้งค่าความจำเป็น (ต่อ)
- IP address 10.101.255.10 (IP ที่ใช้ manage sw) (หมายเลข1)
- Subnet mask 255.255.255.0 (Subnet ที่ใช้ manage sw) (หมายเลข2)
- Default gateway 10.101.255.254 (gateway ที่ใช้ manage sw) (หมายเลข3)
- IP Management VLAN ID (99) (หมายเลข4)
- กด Submit เพื่อดำเนินการต่อไป (หมายเลข5)

ภาพที่ 41

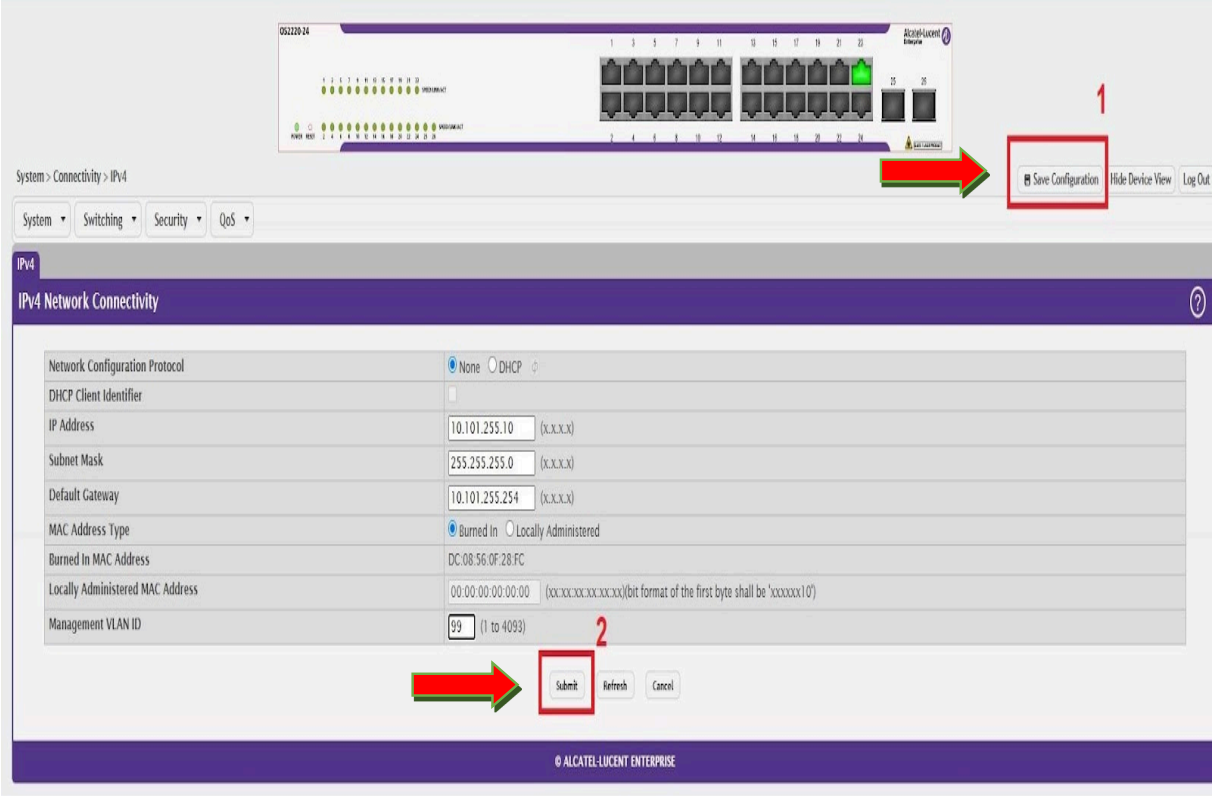


(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 22

- ช่างเทคนิค ทำการ SaveConfiguration ระบบ Switch Alcatel-Lucent OS 2220-24 (หมายเลข1)
- กด Supmit ดำเนินการเสร็จถูกต้องตามที่ได้ตั้งค่าไว้ พร้อมนำไปติดตั้งระบบเครือข่ายต่อไป (หมายเลข2)

ภาพที่ 42 : ภาพแสดงขั้นตอนการ Save Switch Alcatel-Lucent OS 2220-24



(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

4.1.10 คำสั่งพื้นฐาน (Basic Commands)

1. General ทั่วไป
2. Access เข้าถึง การเข้าไปทำ วิธีเข้า
3. Include รวมเข้าด้วยกัน
4. Exclude ไม่รวม, ตัดออกไป, กันออกไป
5. SwitchPort mode trunk - กำหนดให้พอร์ตเป็นแบบ trunk (tagged)
6. Vlan <1-4094> ใช้สำหรับสร้างหรือกำหนดค่า VLAN ตามหมายเลขที่ระบุ โดยสามารถใช้หมายเลข VLAN ได้ตั้งแต่ 1 ถึง 4094 ตามมาตรฐาน IEEE 802.1Q .
7. IP Address - ป้อนค่า IP Address และ Mask ให้กับอินเตอร์เฟส
8. SwitchPort mode access - กำหนดให้พอร์ตเป็นแบบ access (untagged)
9. SwitchPort access vlan - กำหนด vlan ให้กับพอร์ต
10. SwitchPort trunk native vlan - กำหนด native vlan ให้กับพอร์ต trunk
11. SwitchPort trunk allowed vlan - กำหนด vlan ที่สามารถวิ่งผ่านพอร์ต trunk ได้
12. Management VLAN ID -ระบุพอร์ตที่เชื่อมต่อกับ pc เป็นพอร์ตที่ไม่มีแท็ก
13. Save configuration - ทำการ save config
14. Port Configuration- กำหนดพอร์ตให้เป็น Access หรือ Trunk
15. VLAN Management- การบริหารจัดการ Virtual LAN
16. IPv4- หมายเลขประจำตัวของอุปกรณ์ในเครือข่าย
17. Trunk Port - คือการตั้งค่าให้พอร์ตบนสวิตช์สามารถส่งข้อมูลของหลาย ๆ VLAN ได้ในพอร์ตเดียว (มักใช้เชื่อมระหว่าง Switch หรือ Switch กับ Router)

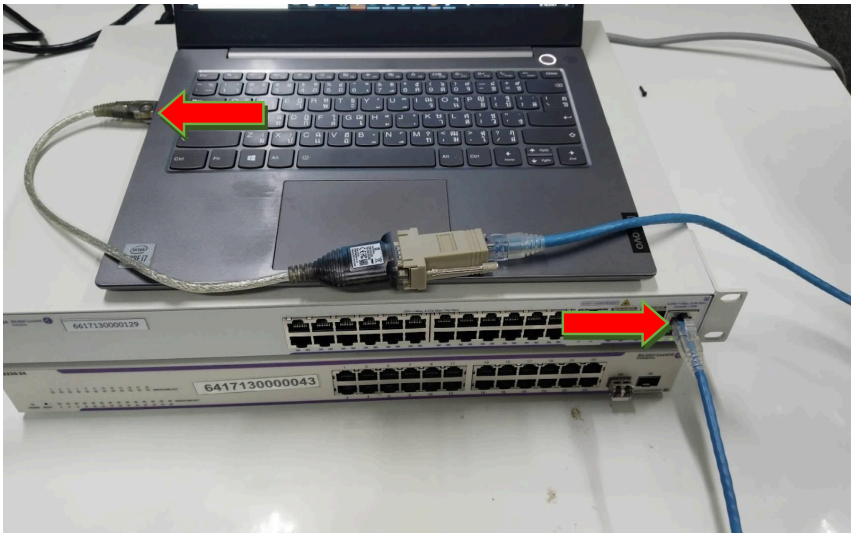
4.2 ขั้นตอนการ Config Switch Alcatel 6360 โดยใช้ Console Port (Command Line Interface - CLI) จะต้องดำเนินการผ่านโปรแกรม PuTTY ผ่านพอร์ต Console ของ Switch (USB to Serial)

ช่างเทคนิคได้จัดทำขั้นตอน ไว้ดังต่อไปนี้

ขั้นตอนที่ 1

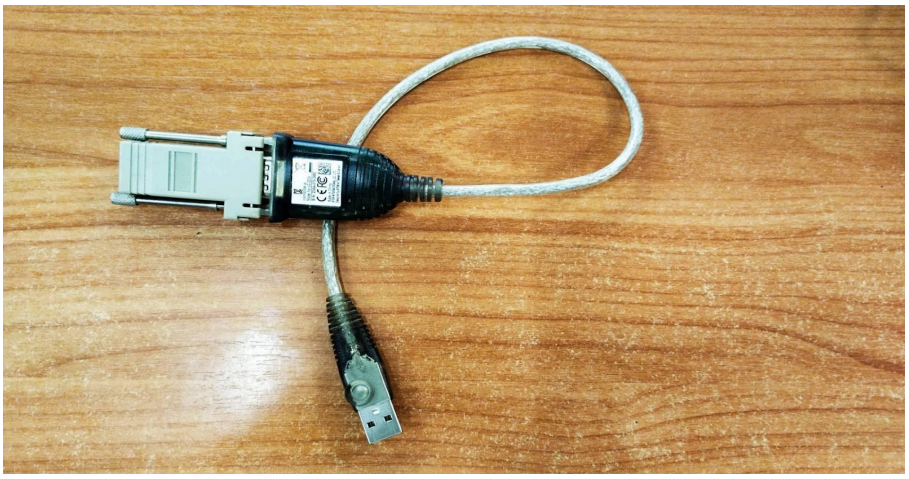
- ช่างเทคนิค ติดตั้งเครื่องคอมพิวเตอร์ Notebook เชื่อมต่อเข้ากับ Switch Alcatel 6360 โดยสายคอนโซลสำหรับ Config Switch เสียบปลายด้านหนึ่งเข้ากับ Port คอมพิวเตอร์ Notebook และอีกด้านหนึ่งเสียบเข้ากับ Switch Alcatel Port Console/USB

ภาพที่ 43: แสดงการเชื่อมต่อสาย Console Port Switch กับเครื่องคอมพิวเตอร์ Notebook



(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

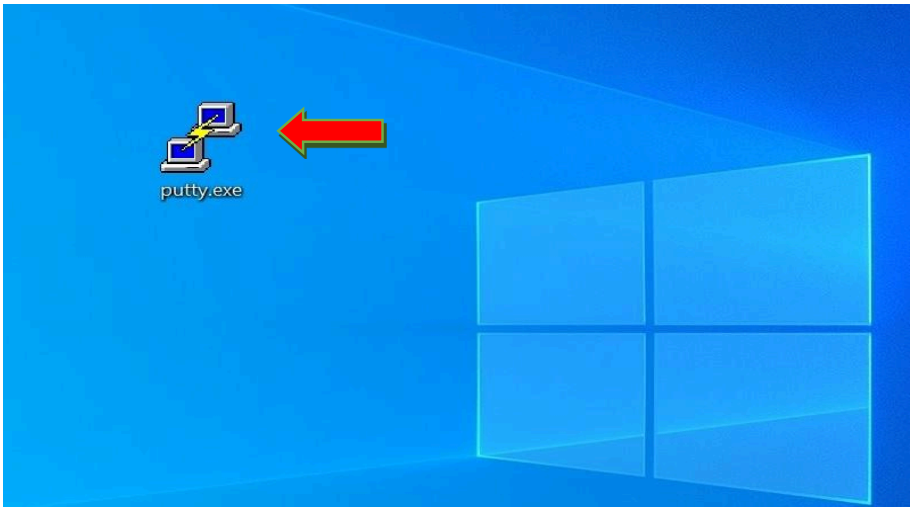
ภาพที่ 44 : แสดงสาย Console (USB to Serial)



ขั้นตอนที่ 2

- เครื่องคอมพิวเตอร์ Notebook ติดตั้งโปรแกรม putty.exe (Freeware)
- PuTTY (putty.exe) คือ โปรแกรมที่ใช้สำหรับเชื่อมต่อไปยังอุปกรณ์อื่น ๆ ผ่านเครือข่าย โดยใช้โปรโตคอลต่างๆ เช่น SSH (Secure Shell), Telnet, rlogin, และ Serial Console client ที่ใช้สำหรับเชื่อมต่อกับเซิร์ฟเวอร์ระยะไกลผ่านเครือข่าย

ภาพที่ 45: โปรแกรม putty.exe (Freeware) ที่ติดตั้งลงเครื่องคอมพิวเตอร์

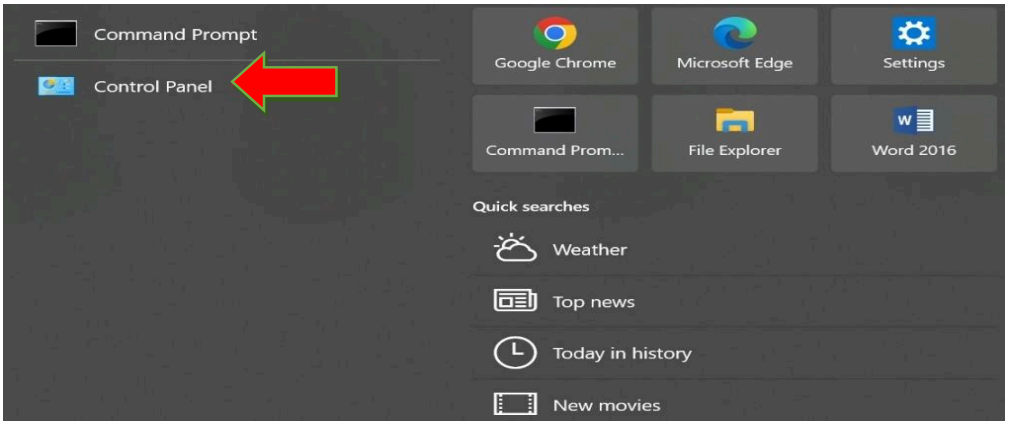


(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 3

- ช่างเทคนิค เข้าไปที่ Control Panel เพื่อเข้าไปตั้งค่าความจำเป็น เครื่องคอมพิวเตอร์ Notebook Ports (COM& LPD)

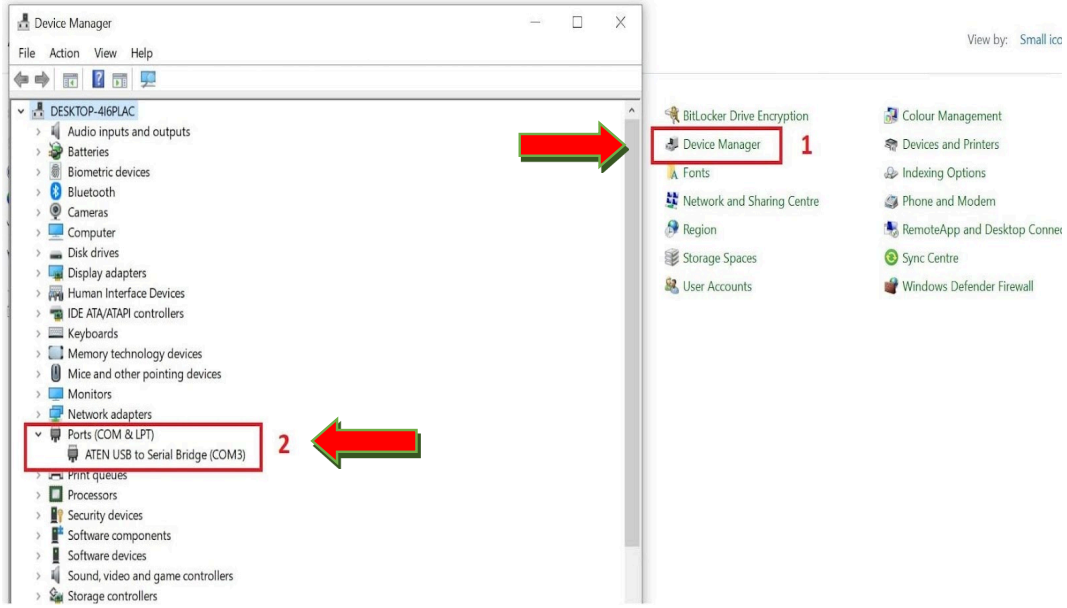
ภาพที่ 46



ขั้นตอนที่ 4

- ช่างเทคนิค คลิกเมาส์เลือก Device Manager (หมายเลข 1)
- Ports (COM& LPD) ATEN USB to Serial Bridge (COM3) (หมายเลข 2)

ภาพที่ 47



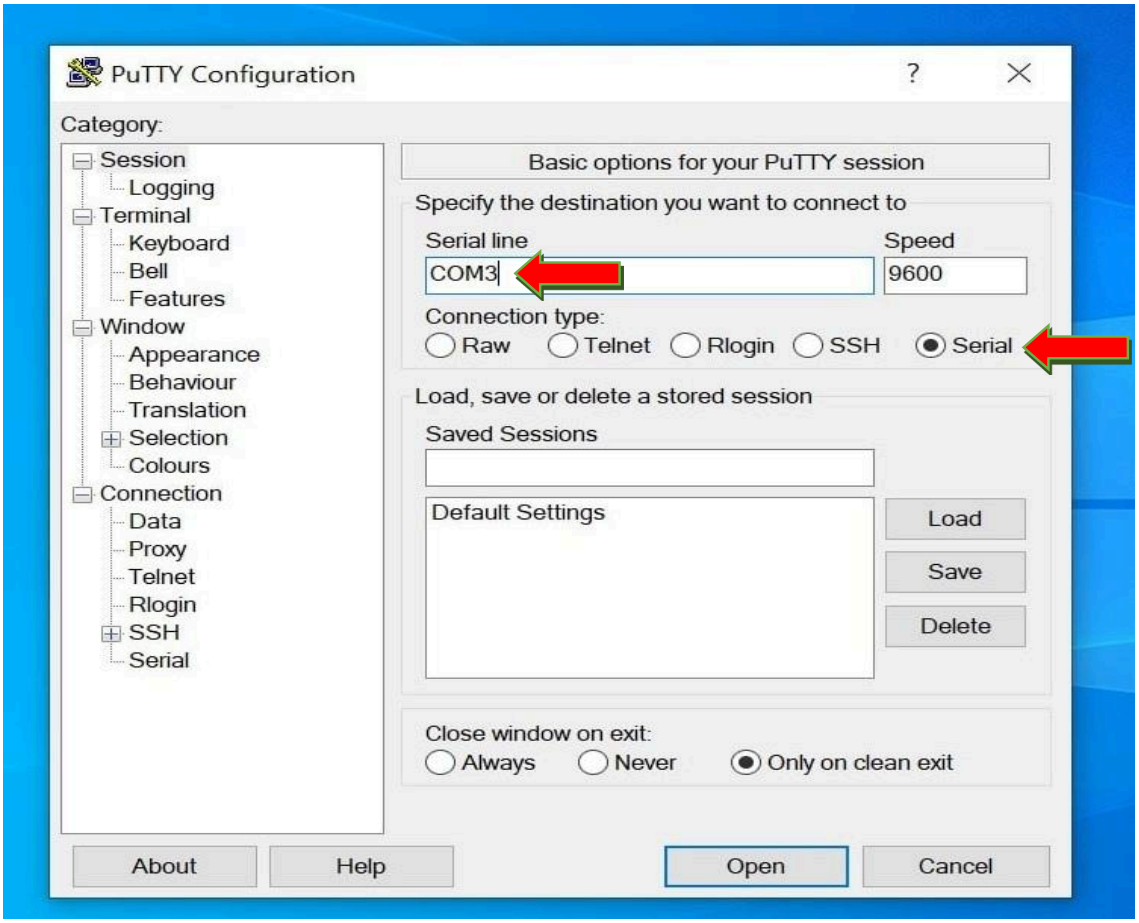
(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 5

- ช่างเทคนิคเช็ค Serial line COM3 ถูกต้องตามขั้นตอนที่ 4 กดคลิกเมาส์ที่ Serial เพื่อดำเนินการต่อไป

  หมายเหตุ: Serial line (COM port เช่น COM1, COM2, COM3) คือพอร์ตอนุกรมที่ระบบปฏิบัติการ (Windows) ใช้ในการสื่อสารกับอุปกรณ์ผ่านพอร์ตอนุกรม เช่น USB-to-Serial, Arduino, Serial Modem ฯลฯ

ภาพที่ 48



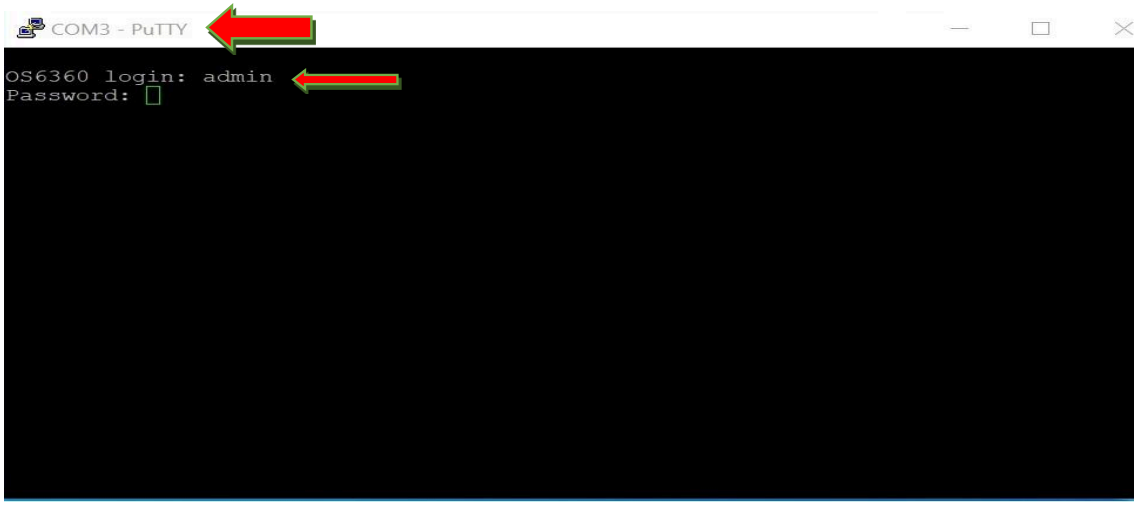
(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 6

- ช่างเทคนิคเปิดโปรแกรม Putty.exe ที่ลงโปรแกรมไว้กับเครื่องคอมพิวเตอร์ Notebook (ขั้นตอนที่ 2)

  จะสังเกตเห็น COM3 เชื่อมต่อกับ Putty ตามที่ได้ตั้งค่าความจำเป็นไว้ (ขั้นตอนที่ 5)
- พิมพ์คำสั่ง Default user : admin
- พิมพ์คำสั่ง Default password: Switch (คำสั่งจะไม่ปรากฏขึ้นมาให้เห็น

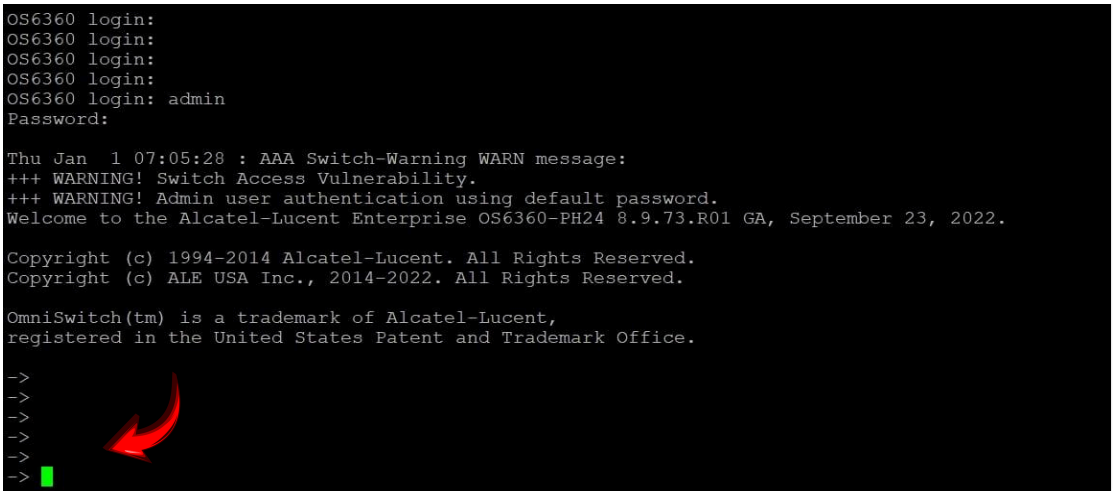
ภาพที่ 49



ขั้นตอนที่ 8

- แสดงการเข้าสู่การจัดการระบบ Config Switch Alcatel 6360 (Command Line Interface)

ภาพที่ 50

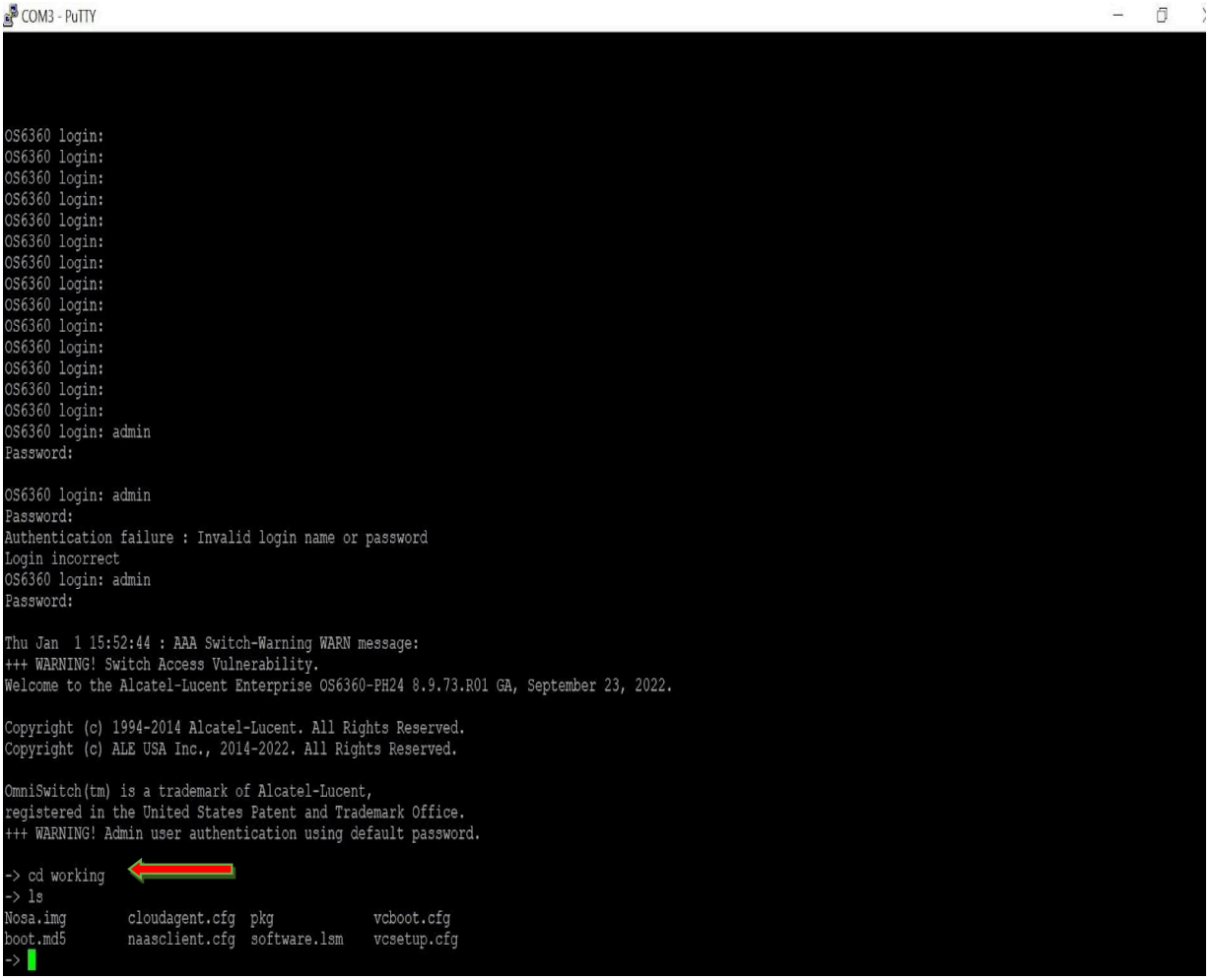


(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 9

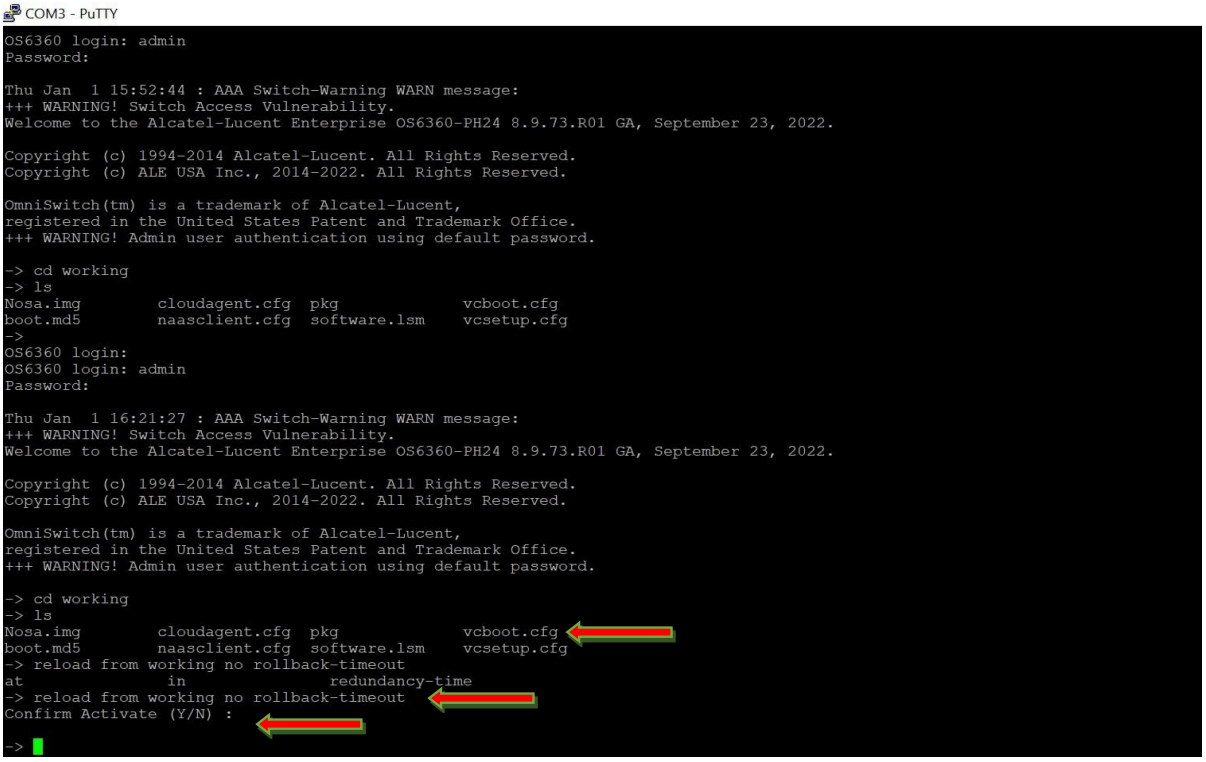
- ช่างเทคนิค ทำการ Reset Switch คืนค่าเริ่มต้นจากโรงงาน (Factory Default Switch)
  หมายเหตุ: ถ้า Switch ได้มีการใช้งานมาก่อน
- ช่างเทคนิค ใช้คำสั่ง cd working (เป็นพื้นที่เก็บ configuration ปัจจุบัน)
- คำสั่ง LS (แสดงไฟล์/โฟลเดอร์ทั้งหมดใน directory ปัจจุบัน)
- คำสั่งลบไฟล์ rm vcboot.cfg
- คำสั่ง reload from working no rollback-timeout (ภาพที่ 52)
- กดคลิก Y บนคีย์บอร์ด อุปกรณ์ Switch Alcatel 6360 จะทำการ reboot รอจนกว่าจะเสร็จ (ภาพที่ 52)

ภาพที่ 51



(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

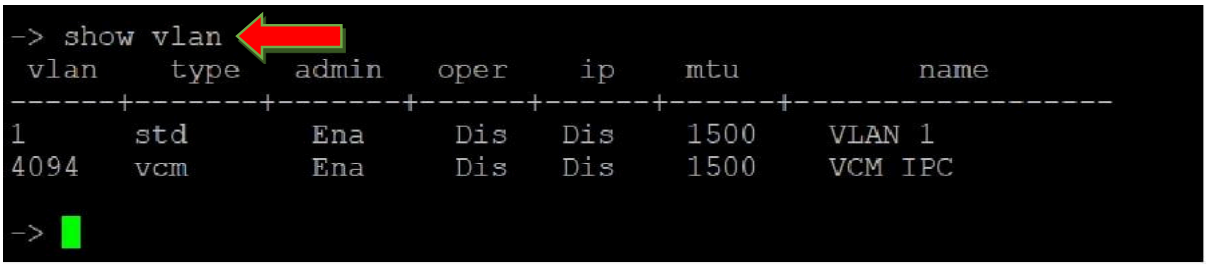
ภาพที่ 52 : แสดงขั้นตอนการ Reset Switch ค่าเริ่มต้นจากโรงงาน (Factory Default Switch)



ขั้นตอนที่ 10

- ช่างเทคนิคพิมพ์คำสั่ง Show VLAN เพื่อแสดงข้อมูล VLAN ที่มีอยู่ในอุปกรณ์ นั้น เช่น รายการ VLAN ทั้งหมด, ชื่อ, สถานะ, และพอร์ตที่เกี่ยวข้องกับแต่ละ VLAN

ภาพที่ 53

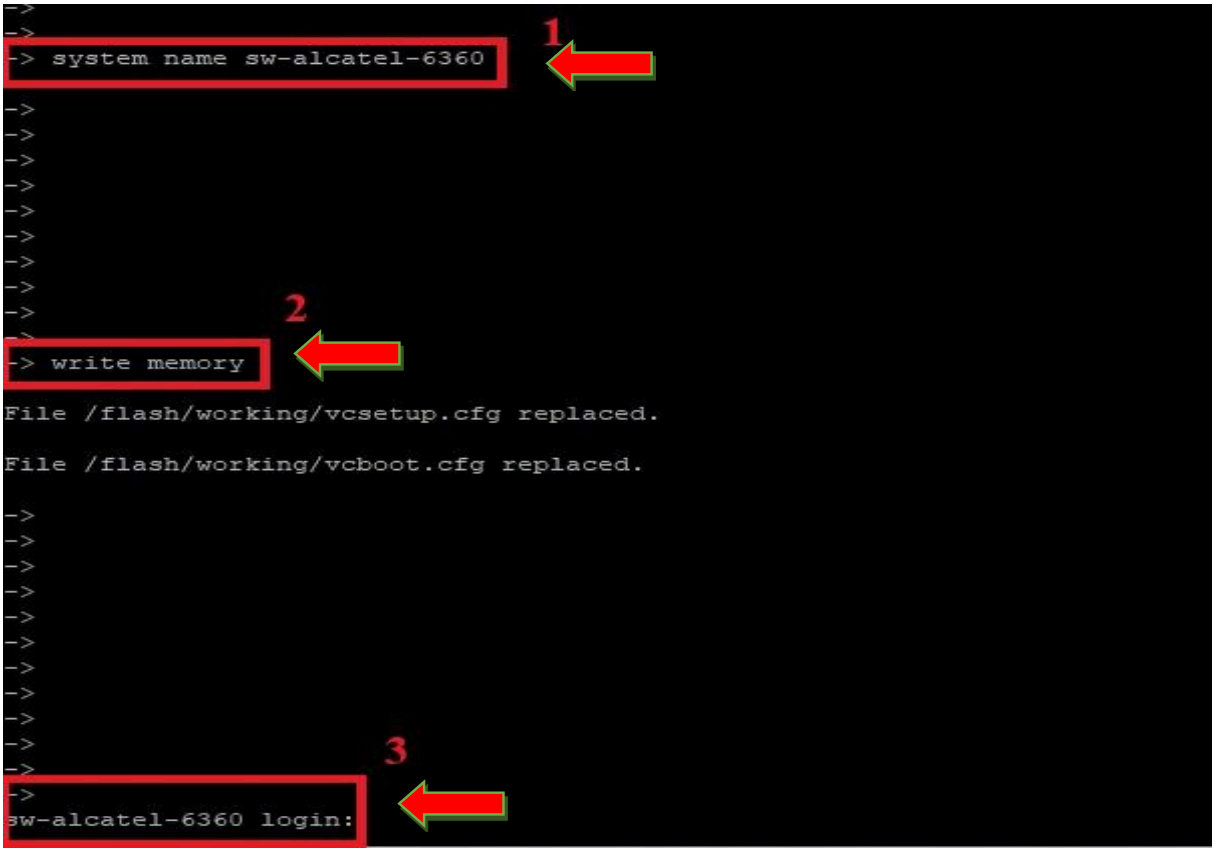


(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 11

- ตั้งค่าชื่อ Hostname (ถ้าต้องการ)
- ช่างเทคนิคใช้คำสั่ง system name SW-ALCATEL-6360 (หมายเลข 1)
- บันทึกด้วยคำสั่ง write memory (หมายเลข 2)
- จะได้ค่า Hostname ตามที่ได้ตั้งชื่อไว้ SW-ALCATEL-6360 (หมายเลข 3)

ภาพที่ 54 : แสดงการตั้งชื่อ Hostname

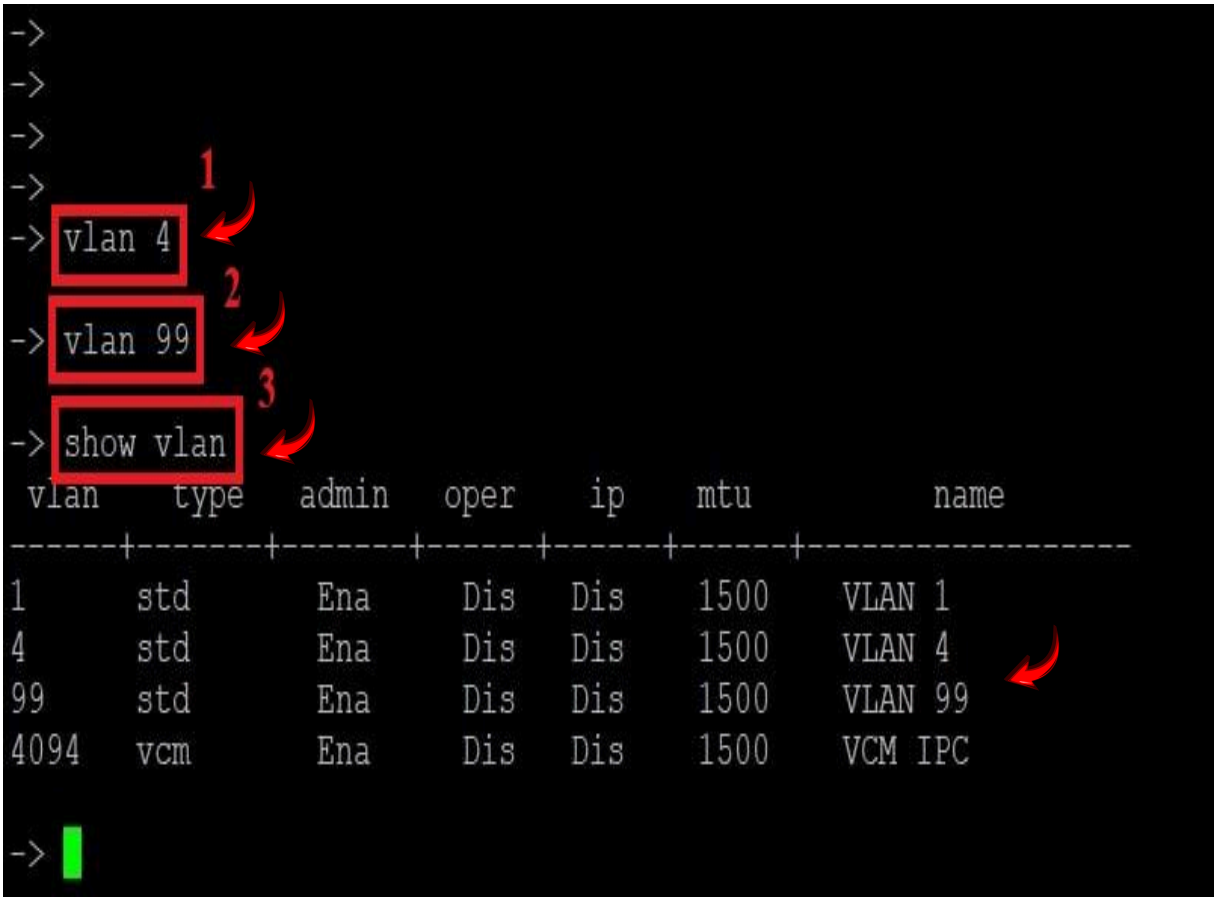


(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 12

- สร้าง VLAN
- ช่างเทคนิคใช้คำสั่ง สร้าง VLAN 4 (ใช้งานอินเตอร์เน็ต) (หมายเลข 1)
- ช่างเทคนิคใช้คำสั่ง สร้าง VLAN 99 (management switch) (หมายเลข 2)
- เสร็จแล้วพิมพ์คำสั่ง Show VLAN (หมายเลข 3)
- จะเห็น VLAN 4 , 99 ถูกสร้างขึ้นถูกต้องตามที่ได้กำหนดค่าไว้

ภาพที่ 55 : แสดงการสร้าง VLAN



(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 13

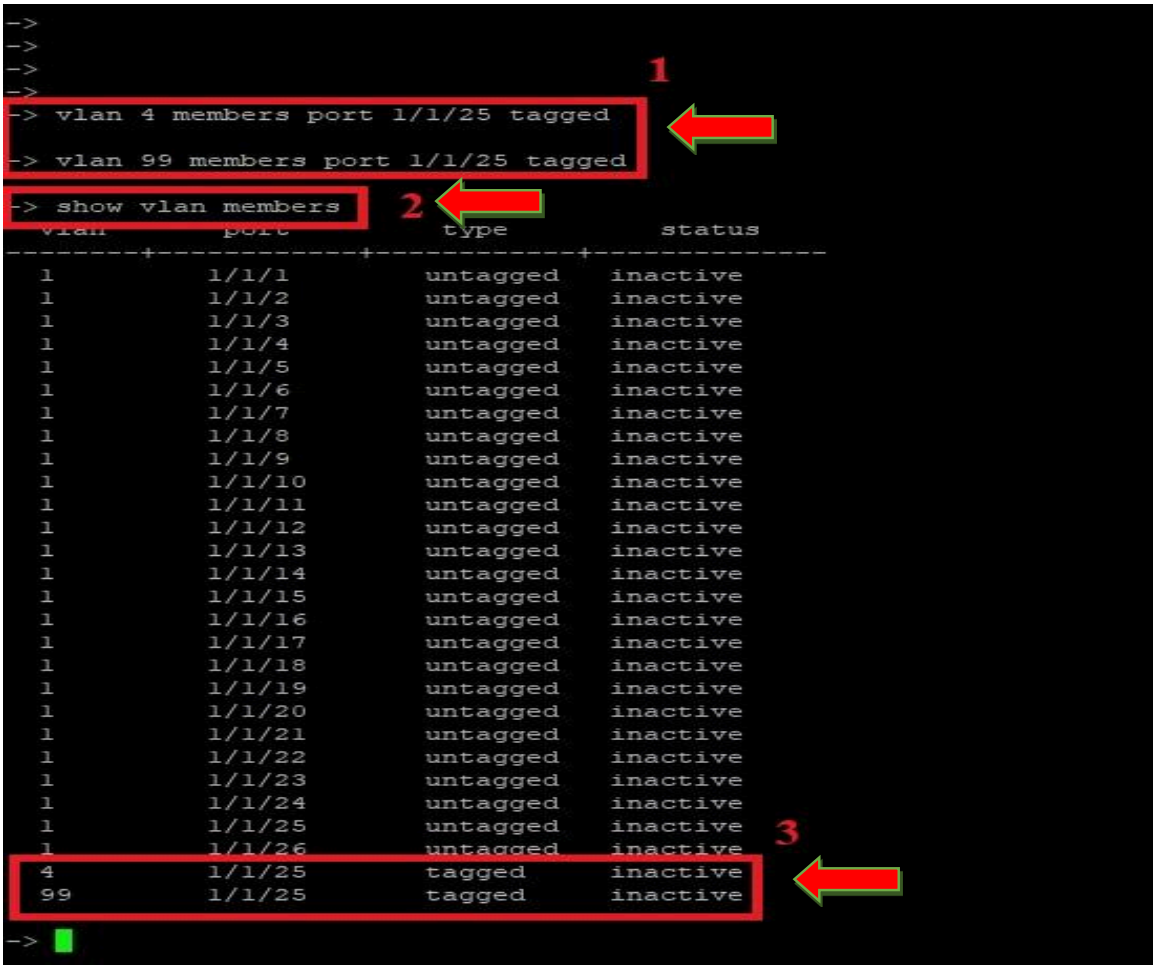
- กำหนดพอร์ตให้ VLAN
- ช่างเทคนิคใช้คำสั่ง สร้าง VLAN 4 members port 1/1/25 tagged (หมายเลข 1)
- ช่างเทคนิคใช้คำสั่ง สร้าง VLAN 99 members port 1/1/25 tagged (หมายเลข 1)
- ช่างเทคนิคใช้คำสั่ง Show VLAN members (หมายเลข 2)

  สังเกต port 1/1/25 จะเปลี่ยนเป็น tagged ถูกต้องตามที่กำหนดค่าไว้ (หมายเลข 3)

  หมายเหตุ : tagged ใช้กับ trunk (เชื่อม Switch ⟶ Switch)

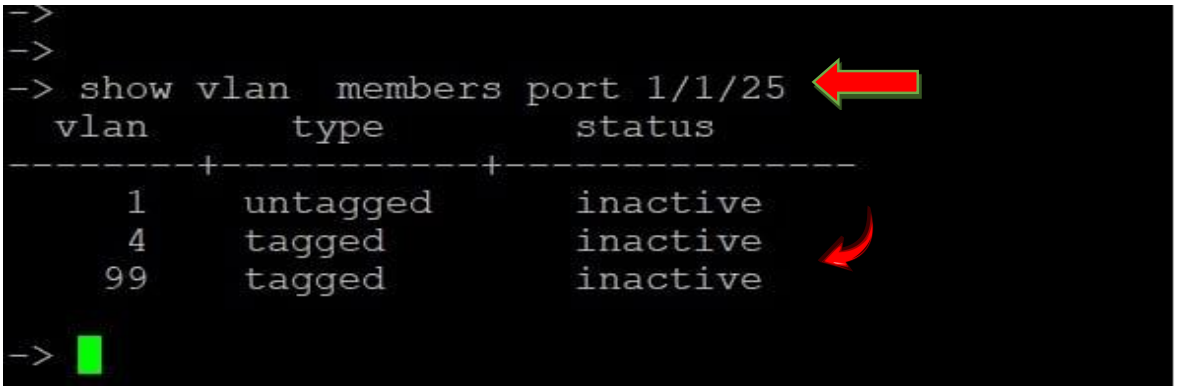
  untagged ใช้กับ client, PC, printer

ภาพที่ 56 : แสดงกำหนดพอร์ตให้ VLAN



(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ภาพที่ 57 : แสดง Show VLAN members port 1/1/25



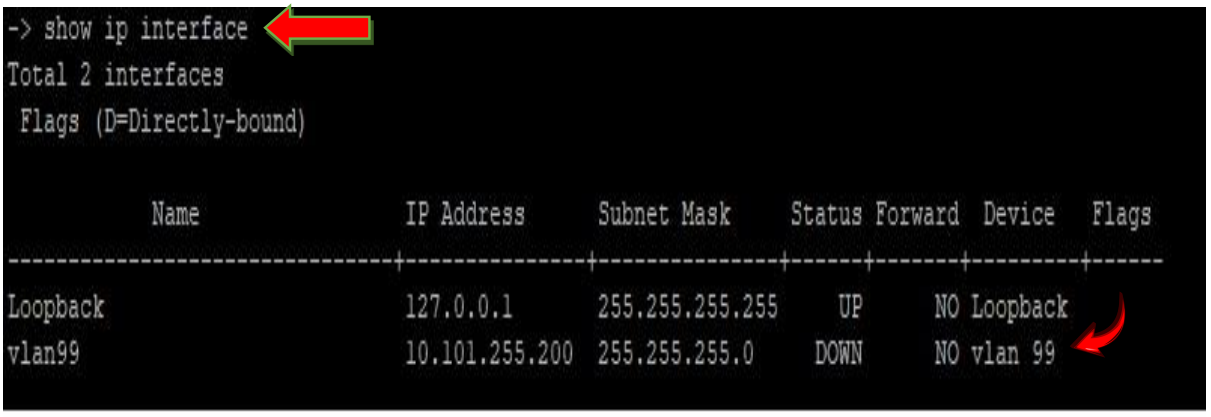
ขั้นตอนที่ 14

- ตั้งค่า IP สำหรับการบริหารจัดการ (Management VLAN)
- ช่างเทคนิค ใช้คำสั่ง ip interface “vlan-99” address 10.101.255.200 mask 255.255.255.0 vlan 99 admin- state enable : กำหนด IP ให้กับ VLAN Interface 99

ขั้นตอนที่ 15

- ตรวจสอบ IP interface:
- ช่างเทคนิคใช้คำสั่ง show ip interface

ภาพที่ 58



(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

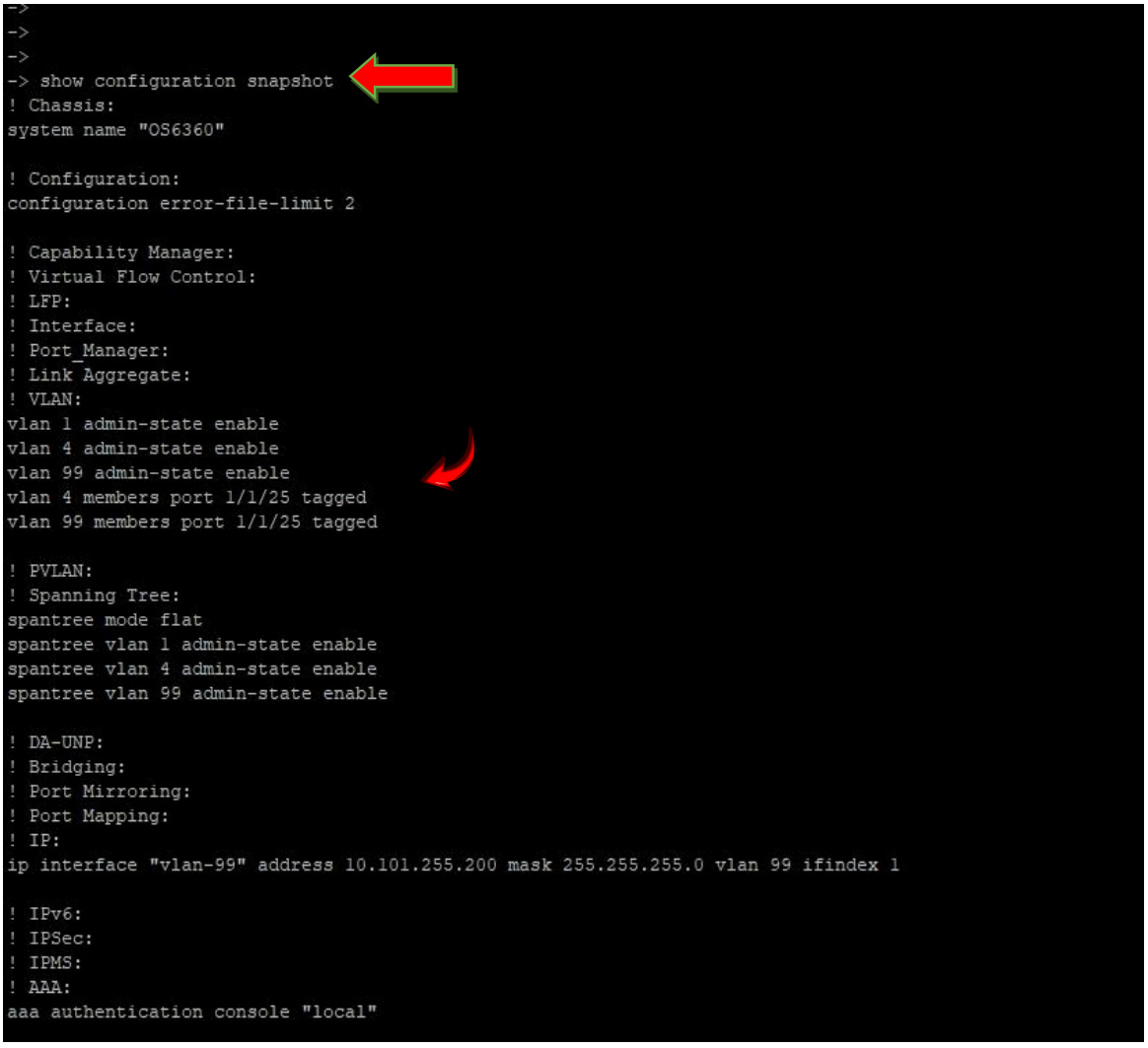
ขั้นตอนที่ 16

- ตั้งค่า Default Gateway
- ช่างเทคนิคใช้คำสั่ง ip static-route 0.0.0.0/0 gateway 10.101.255.254

ขั้นตอนที่ 17

- ตรวจสอบ snapshot configuration เพื่อแสดงภาพรวมของการตั้งค่าคอนฟิกปัจจุบันในรูปแบบ snapshot หรือสำเนา ณ เวลาหนึ่ง
- ช่างเทคนิคใช้คำสั่ง show configuration snapshot

ภาพที่ 59 : show configuration snapshot แสดงภาพรวมของการตั้งค่า Config

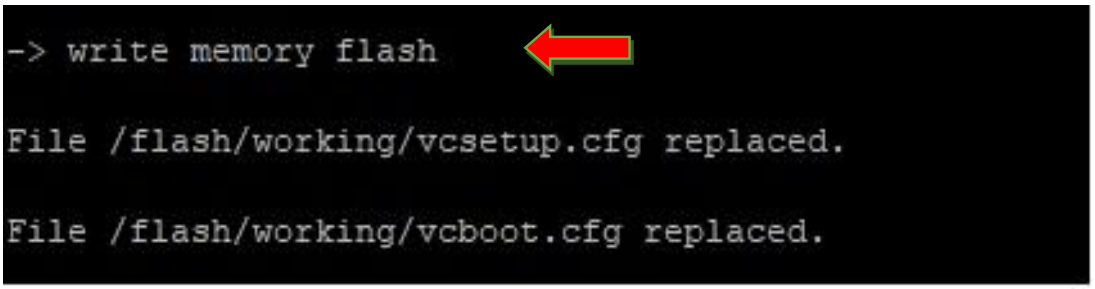


(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 18

- ช่างเทคนิคใช้คำสั่ง write memory flash บันทึกการตั้งค่าทั้งหมด
- ขั้นตอนการ Config switch Alcatel 6360 เสร็จพร้อมดำเนินการติดตั้ง

ภาพที่ 60



(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

คำสั่งพื้นฐาน (Basic Commands)

1. Enable เข้าสู่โหมด privileged (admin mode)
2. configure terminal เข้าสู่โหมด config สำหรับตั้งค่าระบบ
3. write memory บันทึกค่าการตั้งค่าลงใน memory
4. cd working ย้ายไปยัง working directory ของ config
5. reload สั่งรีสตาร์ทอุปกรณ์
6. reload from working no rollback-timeou รีโหลดจาก working config แบบไม่ย้อนกลับ
7. ip interface ตั้งค่า IP address ให้กับ interface หรือ VLAN
8. vlan <id> สร้างหรือเข้าไป config VLAN หมายเลข <id>
9. vlan name กำหนดชื่อให้ VLAN
10. vlan pvid <id> ตั้งค่า VLAN ID พื้นฐาน (untagged) ให้กับพอร์ต
11. vlan participation include <id> ใส่พอร์ตใน VLAN ที่ต้องการ
12. vlan tagging เปิดใช้งาน tagged VLAN บน trunk port
13. vlan members port เพิ่มพอร์ตเข้า VLAN แบบ tagged หรือ untagged
14. aaa authentication login การตั้งค่าการยืนยันตัวตน (authentication)
15. user <name> เพิ่มหรือจัดการผู้ใช้งาน
16. password กำหนดรหัสผ่าน

17. privilege <level>	ระดับสิทธิ์ของผู้ใช้งาน (0-15)
18. ip routing	เปิดการทำงาน Routing (L3)
19. ip static-route <network>	เพิ่ม static route
20. gateway	ระบุ Gateway สำหรับ static route
21. snmp community <name>	กำหนด community string สำหรับ SNMP
22. snmp	ตั้งค่าโปรโตคอล Simple Network Management Protocol
23. ntp server <ip>	ระบุ NTP server สำหรับ sync เวลา
24. ntp enable	เปิดการใช้งาน NTP
25. system timezone	ตั้งค่า timezone
26. log	ใช้ในการตั้งค่าระบบบันทึกเหตุการณ์
27. spanning-tree enable	เปิดใช้งาน Spanning Tree Protocol
28. spanning-tree mode rstp	เลือกโหมด Rapid Spanning Tree
29. show running-config	แสดงการตั้งค่าปัจจุบัน
30. show configuration snapshot	แสดง config snapshot
31. show vlan	แสดงรายการ VLAN
32. show interfaces	แสดงสถานะ interfaces
33. show ip route	แสดงตาราง routing

4.3 ช่างเทคนิคทำขั้นตอนการเข้าหัวสายแลน เพื่อใช้กับงานติดตั้งสัญญาณระบบเครือข่ายสัญญาณอินเตอร์เน็ตภายในมหาวิทยาลัยขอนแก่น ช่างเทคนิคได้ทำการ เข้าหัวสายแลน (RJ-45) สามารถต่อได้ 2แบบ คือ แบบสายตรงและแบบสายครอส

- แบบสายตรงสามารถเข้าได้ 2 แบบ

แบบที่ 1 เรียกว่า TIA/EIA 568A คือเข้าแบบ TIA/EIA 568A ทั้งสองข้าง
แบบที่ 2 เรียกว่า TIA/EIA 568B คือเข้าแบบ TIA/EIA 568B ทั้งสองข้าง

- แบบสานครอส สามารถเข้าได้ 2 แบบ

1. คืออีกฝั่งจะเข้าแบบ TIA/EIA 568A
2. และอีกฝั่งจะเข้าแบบ TIA/EIA 568B

สิ่งที่ต้องเตรียมในการต่อสายแลนหรือเข้าหัว (RJ-45)

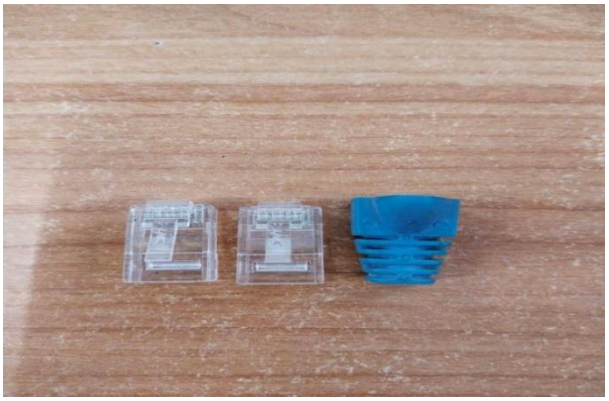
1. เครื่องทดสอบสายแลนหรือสายสัญญาณ (cable tester) ดังรูปต่อไปนี้ **(ภาพที่ 61)**

(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

2. คีมเข้าหัวสายแลน สามารถใช้คีมนี้ในการเข้าหัวสายแลน และสายโทรศัพท์ได้ ใช้ในการตัดก็ได้ **(ภาพที่ 62)**

3. คีมตัดสาย ใช้ในการตัดสายให้ขาดหลังจากที่เราวัดสายได้ความยาวตามที่ต้องการ **(ภาพที่ 63)**

4. หัวแลน หรือหัว RJ-45 หนึ่งเส้นใช้สองหัว **(ภาพที่ 64)**



(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

5. กรรไกร มีดคัตเตอร์ ใช้ปอกสายเพื่อให้ตัวนำยื่นออกมาและตัดเส้นด้าย
(ภาพที่ 65)

6. สายแลน Cat5 Cat6 ความยาวตามต้องการจะใช้ แต่ต้องยาวไม่น้อยกว่า 1 เมตรหากน้อยกว่าจะไม่สามารถใช้งานได้และความยาวสูงสุดของสายแลนควรไม่เกิน 35-40 เมตร ถ้าต้องการใช้ยาวกว่านั้นควรเชื่อมต่อ ด้วย Switching HUB
(ภาพที่ 66)

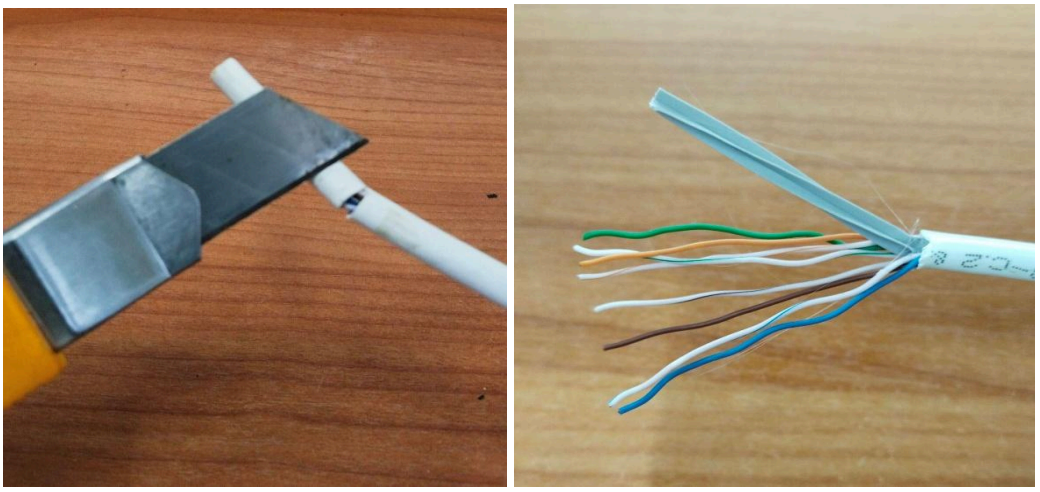
(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

4.3.1 ช่างเทคนิคได้จัดทำขั้นตอน วิธีการเข้าหัวสายแลน มีขั้นตอนดังต่อไปนี้

ขั้นตอนที่ 1

- ใช้คัตเตอร์ปอกสายหุ้มสีขาวออกให้มีความยาว 3-4 เซ็นติเมตร (ระวังอย่าให้มีดไปโดนสายด้านใน) จะเห็นสายเล็กๆสีต่างๆด้านในจำนวน 8 เส้นด้วยกัน

(ภาพที่ 67)



ขั้นตอนที่ 2

- ช่างเทคนิค ใช้วิธีการเข้าหัวแบบตรงสาย (straight-through cable eia/tia 568b)

คลี่สายออก แล้วเรียงคู่สายตามมาตรฐานโดยจัดเรียงคู่สายจากซ้ายไปขวา คู่ส้ม-คู่เขียว-คู่น้ำเงิน-คู่น้ำตาล

(ภาพที่ 68)

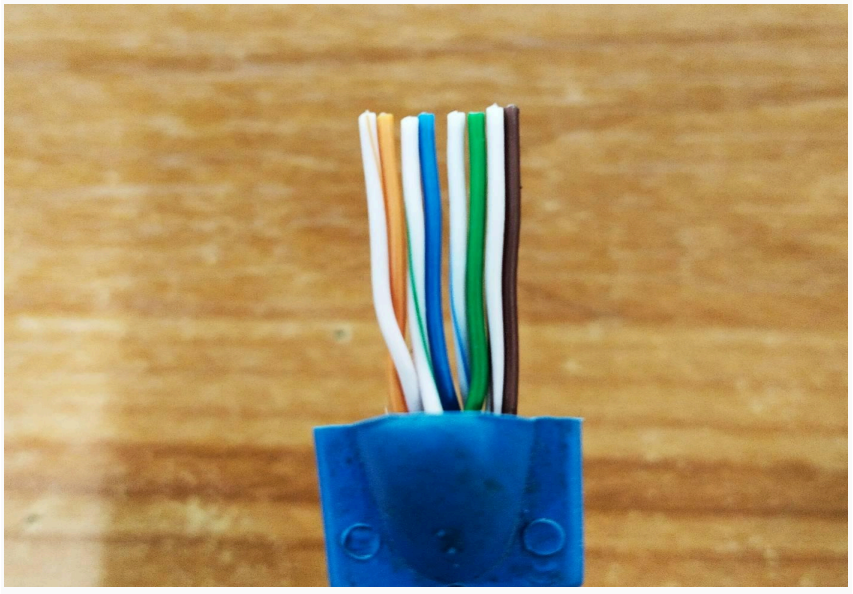
(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 3

- แยกเส้นที่ติดเป็นคู่ออกจากกัน แล้วทำการจัดเรียงสาย ตามมาตรฐาน EIA/TIA 568B จากซ้ายไปขวา ได้แก่

1.ขาว-ส้ม
2. ส้ม
3. ขาว-เขียว
4. น้ำเงิน
5. ขาว-น้ำเงิน
6. เขียว
7. ขาว-น้ำตาล
8. น้ำตาล

(ภาพที่ 69)

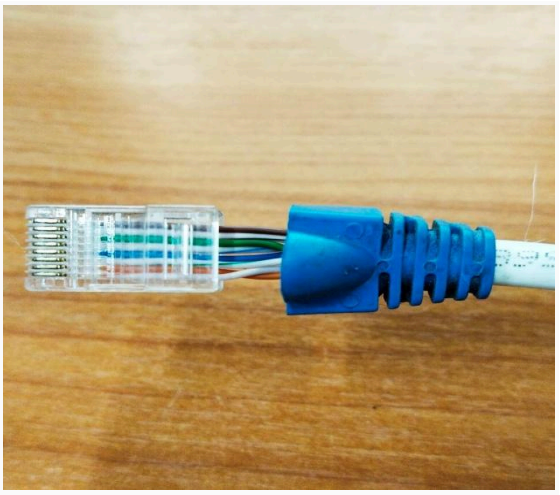


(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 4

- จัดเรียงสายตัวนำ แล้วเสียบเข้าไปที่ หัว RJ-45 โดยหันด้าน pin หรือฟันทองเหลืองออกมาด้านหน้า เสียบเข้าไปให้ชนด้านในหัวพลาสติกพอดี

(ภาพที่ 70)



ขั้นตอนที่ 5

- ดันหัว RJ-45 เข้าให้แน่น จากนั้นใช้คีมหนีบให้แน่น กด 2-3 ครั้ง เพื่อให้แน่ใจว่าสายแนบสนิทกับทองแดงแล้ว

(ภาพที่ 71)

(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

ขั้นตอนที่ 6

- ช่างเทคนิค ทำการตรวจเช็คสายแลน โดยใช้เครื่องทดสอบสายแลนที่มีความละเอียดและเที่ยงตรงสูง รวดเร็วภายในระยะเวลาเพียง 10 วินาที

(ภาพที่ 72)

ขั้นตอนที่ 7

- ช่างเทคนิค นำสายสัญญาณที่เข้าหัว RJ-45 เสร็จแล้วมาทดสอบ เสียบสายแลนทั้งต้นทางและปลายทางก่อน จึงจะสามารถทดสอบได้ เนื่องด้วยเครื่องทดสอบ Fluke DSX จะมี 2 เครื่องคือ Main Unit เสียบที่ต้นทาง และ Remote Unit เสียบที่ปลายทาง เพื่อยิงสัญญาณและเก็บข้อมูลของสายสัญญาณที่ต้องการ

(ภาพที่ 73)

(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

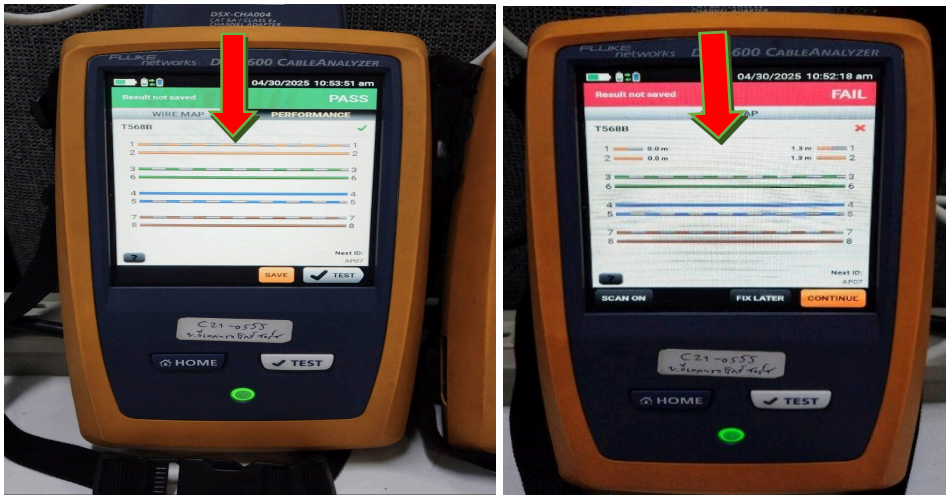
ขั้นตอนที่ 8

- ภาพแสดงที่ตำแหน่งคู่สายครบทั้ง 4 คู่ จำนวน 8 เส้น ตามมาตราฐาน EIA/TIA 568B ดังรูป
- สายสัญญาณสามารถใช้งานได้พร้อมนำไปติดตั้ง

(ภาพที่ 74)

(ภาพที่ 75) : แสดงภาพตัวอย่างสายสัญญาณที่ใช้งานได้และไม่สามารถใช้งานได้ จากเครื่องทดสอบ Fluke DSX

ใช้งานได้ ใช้งานไม่ได้



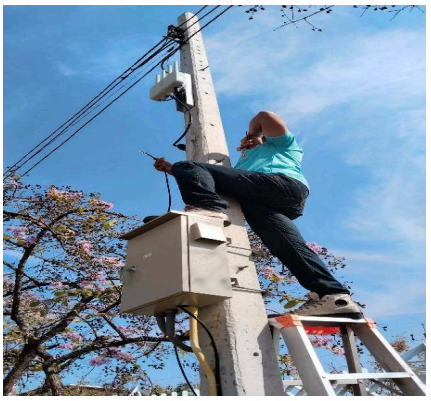
(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

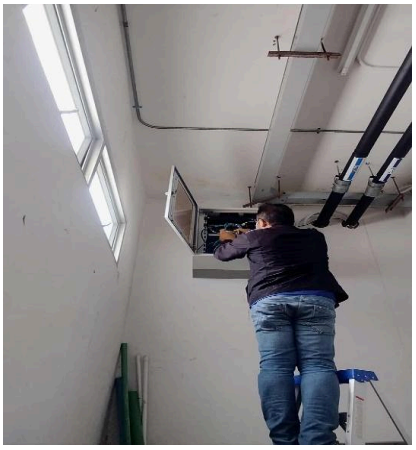
4.4 กิจกรรมและการดำเนินงาน

ในส่วนหัวข้อนี้จะแสดงภาพกิจกรรมต่างๆ ในการดำเนินการติดตั้งและดูแลระบบเครือข่ายของสำนักเทคโนโลยีดิจิทัล ที่ให้บริการอยู่ทั่วพื้นที่ของมหาวิทยาลัยขอนแก่นโดยได้อาศัยทรัพยากรบุคคลของสำนักเทคโนโลยีดิจิทัล ในการติดตั้งและดูแลระบบเครือข่ายภายในมหาวิทยาลัยขอนแก่น

(ภาพที่ 60)

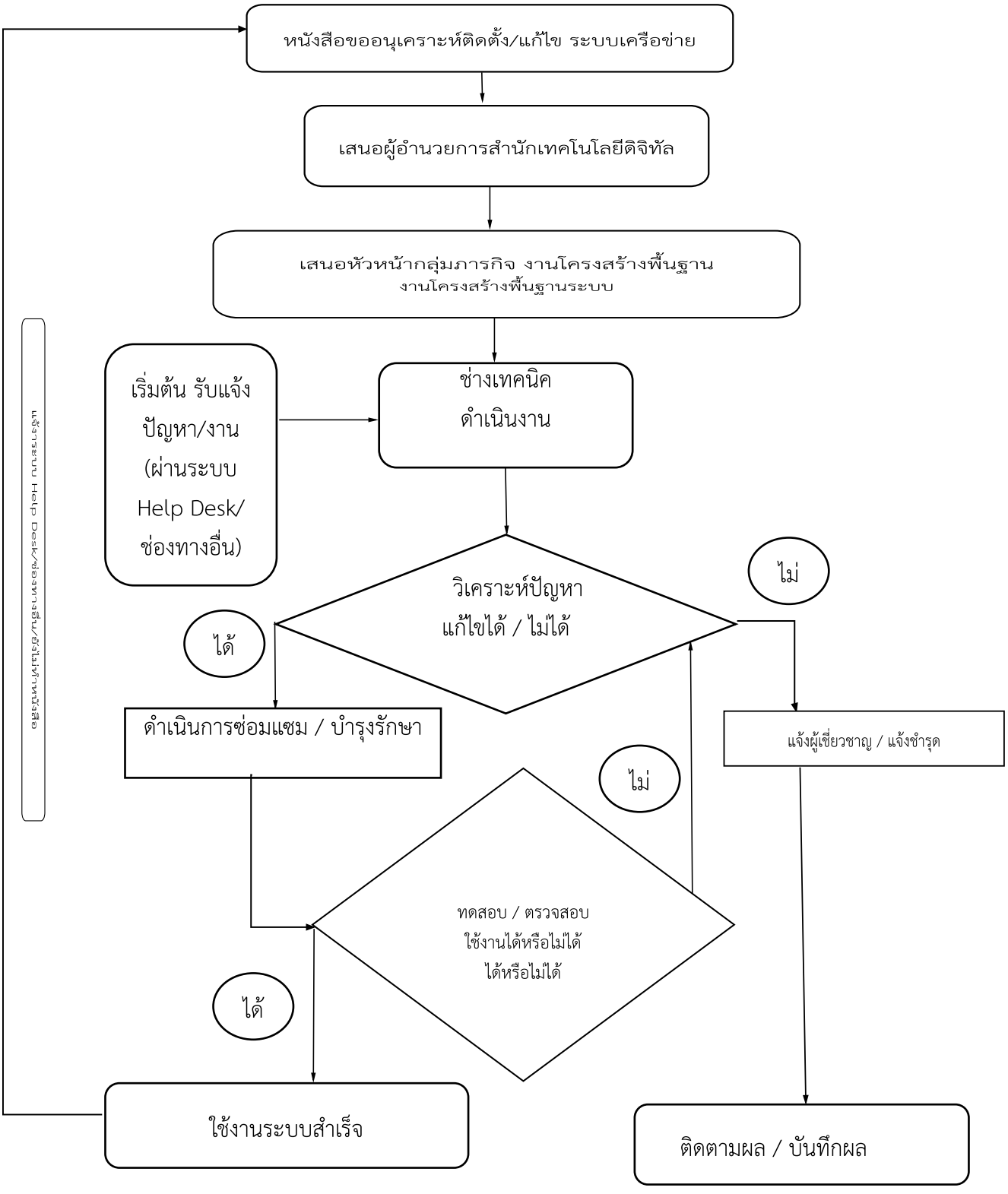
(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)





(ที่มาสำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น 2567)

แผนการไหลของงาน



บทที่ 5
ปัญหา อุปสรรคและข้อเสนอแนะ

- ปัญหาและอุปสรรคในการจัดทำคู่มือการปฏิบัติงานดูแลระบบเครือข่ายและอุปกรณ์เครือข่ายที่ใช้งานตามคณะ/หน่วยงาน/และหอพักนักศึกษา มหาวิทยาลัยขอนแก่น

1. ขาดข้อมูลที่เป็นปัจจุบันและครบถ้วน
    - อุปกรณ์เครือข่ายที่ใช้งานในแต่ละคณะ/หน่วยงานและหอพักมีความหลากหลายและบางแห่งไม่มีการจัดเก็บข้อมูลไว้อย่างเป็นระบบ
2. รูปแบบการติดตั้งที่ไม่เป็นมาตรฐาน
    - แต่ละหน่วยงานอาจมีรูปแบบการติดตั้งอุปกรณ์หรือโครงสร้างเครือข่ายแตกต่างกัน ทำให้ยากต่อการจัดทำคู่มือกลางที่ใช้ร่วมกันได้
3. ขาดการประสานงานจากหน่วยงานต่าง ๆ
    - การเก็บรวบรวมข้อมูลจากหลายคณะ/หน่วยงานมักล่าช้าหรือไม่ได้รับความร่วมมือเต็มที่ ทำให้ข้อมูลไม่ครบ
4. บุคลากรมีความรู้ไม่เท่ากัน
    - บางพื้นที่ไม่มีผู้ดูแลที่มีความเชี่ยวชาญ ส่งผลให้ไม่สามารถอธิบายรายละเอียดเชิงเทคนิคได้ชัดเจนพอสำหรับนำไปใช้ในคู่มือ
5. ไม่มีคู่มือเดิมให้เป็นต้นแบบ
    - การเริ่มต้นจัดทำคู่มือจากศูนย์ (ไม่มีแนวทางอ้างอิงเดิม) อาจใช้เวลานานในการวางโครงสร้างและเนื้อหา
6. ภาระงานของเจ้าหน้าที่ผู้เกี่ยวข้อง
    - เจ้าหน้าที่ผู้รับผิดชอบการดูแลเครือข่ายมักมีภาระงานประจำมาก ทำให้ไม่มีเวลาในการจัดทำหรือรวบรวมข้อมูลสำหรับคู่มือ
7. อุปกรณ์เครือข่ายที่ใช้ในระบบเครือข่าย ตามคณะ/หน่วยงาน มีจำนวนมากและหลากหลายรุ่น อาจเป็นปัญหาในการทำงานหรือการติดตั้ง (configulation)
8. สถานที่ติดตั้งอุปกรณ์เครือข่าย บางพื้นที่มีความเสี่ยงต่อการให้บริการ
9. ระดับสัญญาณในพื้นที่ (ระบบไร้สาย)ยังไม่ควบคุมพื้นที่
10. การเชื่อมต่ออุปกรณ์ของผู้ใช้บริการ เนื่องจากอาจเกิดปัญหากับผู้ใช้เอง หรือปัญหาเกี่ยวกับระบบของอุปกรณ์เครือข่าย

11. การเปลี่ยนแปลงของอุปกรณ์และระบบเครือข่ายอย่างต่อเนื่อง
    - ระบบเครือข่ายมักมีการอัปเกรดหรือเปลี่ยนแปลง ทำให้คู่มือที่จัดทำไว้อาจล้าสมัยหากไม่มีการปรับปรุงอย่างสม่ำเสมอ
    - ข้อเสนอแนะในการพัฒนาคู่มือ

- **หลักการสำคัญ: เน้นการเรียนรู้ควบคู่ไปกับการบันทึกข้อมูลอย่างเป็นระบบ ตั้งแต่ขั้นตอนแรกของการติดตั้ง เพื่อสร้างความรู้และเอกสารอ้างอิง**

1. จัดทำรูปแบบมาตรฐานกลางของคู่มือ
    - กำหนดรูปแบบเอกสารที่ใช้ร่วมกันทุกคณะ/หน่วยงาน เช่น โครงสร้างหัวข้อ, รูปแบบการบันทึกข้อมูล, ตารางอุปกรณ์
    - ใช้ Template หรือระบบออนไลน์ (Google Docs, OneDrive) เพื่อการอัปเดตแบบเรียลไทม์
2. จัดทำแบบฟอร์มการเก็บข้อมูลระบบเครือข่าย
    - ออกแบบฟอร์มสำหรับรวบรวมข้อมูล เช่น ผังเครือข่าย, รายการอุปกรณ์, การตั้งค่า IP, VLAN, DHCP ฯลฯ
    - ส่งให้หน่วยงานต่าง ๆ กรอกข้อมูลให้ครบถ้วนก่อนเริ่มจัดทำคู่มือ
3. แยกคู่มือออกเป็นส่วนย่อยตามกลุ่มเป้าหมาย
    - เช่น คู่มือสำหรับผู้ดูแลระบบ (IT), คู่มือสำหรับเจ้าหน้าที่ทั่วไป, คู่มือเบื้องต้นสำหรับนักศึกษา
    - ทำให้คู่มืออ่านง่ายและตรงกลุ่มเป้าหมาย
4. มีภาพประกอบและขั้นตอนอย่างชัดเจน
    - เพิ่มภาพผังเครือข่าย (Topology), ตัวอย่างหน้าจอการตั้งค่าอุปกรณ์ และแผนที่ติดตั้งอุปกรณ์
    - ใช้สัญลักษณ์และไอคอนเพื่อให้เข้าใจง่าย
5. จัดให้มีการฝึกอบรมหรือประชุมเชิงปฏิบัติการ
    - จัดเวิร์กช็อปเพื่อให้เจ้าหน้าที่เข้าใจและสามารถจัดทำ/ใช้งานคู่มือได้จริง
    - เพิ่มทักษะในการดูแลระบบเครือข่ายแบบมาตรฐานเดียวกัน
6. มีระบบเวอร์ชันและการปรับปรุงข้อมูล
    - ระบุหมายเลขเวอร์ชัน วันที่ปรับปรุง และผู้รับผิดชอบในคู่มือแต่ละฉบับ
    - มีรอบการอัปเดตคู่มืออย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบ

7. กำหนดผู้รับผิดชอบประจำคณะ/หน่วยงาน
    - แต่งตั้งผู้ดูแลหรือผู้ประสานงานที่รับผิดชอบการอัปเดตข้อมูลและคู่มือในแต่ละพื้นที่
    - ทำงานร่วมกับฝ่ายเทคโนโลยีดิจิทัลกลางของมหาวิทยาลัย
8. นำเทคโนโลยีดิจิทัลมาช่วยจัดการคู่มือ
    - พิจารณาทำคู่มือในรูปแบบเว็บไซต์ภายใน (Intranet) หรือฐานข้อมูลที่สืบค้นได้
    - สามารถแนบไฟล์ผังเครือข่าย เอกสารประกอบ หรือบันทึกการบำรุงรักษาไว้ในระบบเดียวกัน

บรรณานุกรม

[1] ดร.วิรินทร์ เมฆประดิษฐสิน, *ตำราประกอบการอบรม Mastering Cisco Routing and Switching Network*.

[2] ‘พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560’. Jan. 24, 2560. [Online]. Available: https://www.ratchakitcha.soc.go.th/DATA/PDF/2560/A/010/24.PDF

[3] http://www.ddsure.net/network_device.php

ประวัติส่วนตัว

ชื่อ - สกุล สิทธิชัย กาบบัวลอย

เกิดวันที่ 29 กุมภาพันธ์ พ.ศ. 2523

ภูมิลำเนา จังหวัดขอนแก่น

ที่อยู่ปัจจุบัน 890 หมู่3 ต.ศิลา อ.เมือง จ.ขอนแก่น 40000

ประวัติการศึกษา **พ.ศ 2549 จบการศึกษา** ปริญญาตรี วิศวกรรมศาสตร์บัณฑิต สาขาอิเล็กทรอนิกส์ มหาวิทยาลัยภาคตะวันออกเฉียงเหนือ

ประวัติการศึกษา **พ.ศ 2540 จบการศึกษา** ประกาศนียบัตรวิชาชีพชั้นสูง สาขาอิเล็คทรอนิคส์ เทคโนโลยีภาคตะวันออกเฉียงเหนือ

ประวัติการทำงาน

2.1 ปัจจุบันดำรงตำแหน่ง พนักงานช่างเทคนิค ระดับปฏิบัติงาน

ได้รับแต่งตั้งเมื่อวันที่ 1 ตุลาคม พ.ศ. 2561 **สำนักเทคโนโลยีดิจิทัล มหาวิทยาลัยขอนแก่น**