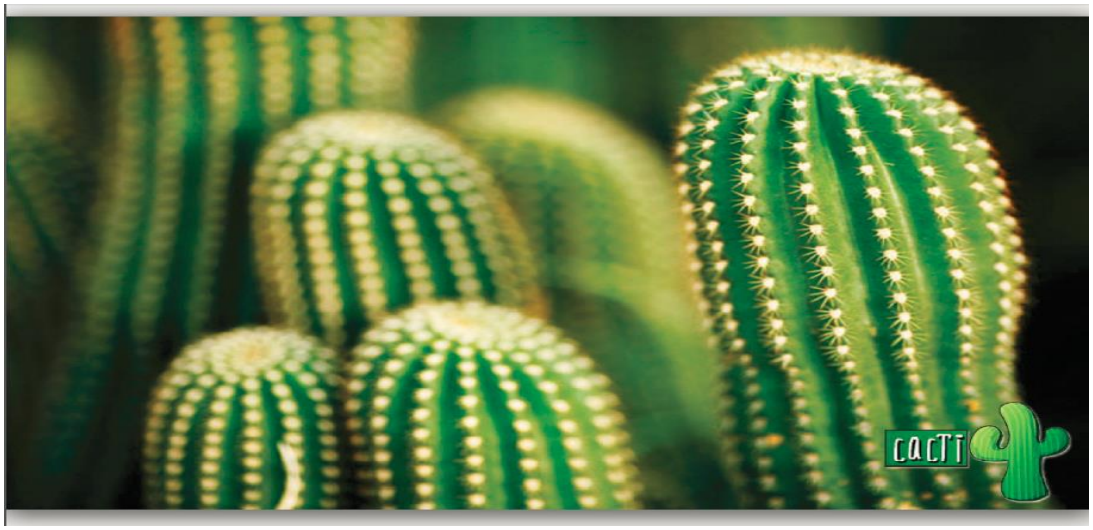
การทำ PDF Bookmark กรณีที่ 1

(ไม่ได้เป็นเจ้าของไฟล์ word)

คู่มือการปฏิบัติงาน

ระบบตรวจสอบสถานะและปริมาณการใช้งานเครือข่าย



นายเชาวลิต สมบูรณ์พัฒนากิจ

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

คำนำ

คู่มือปฏิบัติงานระบบตรวจสอบสถานะและปริมาณการใช้งานเครือข่ายเล่มนี้ เป็นคู่มือสำหรับเจ้าหน้าที่ประจำกลุ่มงานเครือข่ายคอมพิวเตอร์และการสื่อสาร ใช้เป็นแนวทางในการทำงานเพื่อให้บรรลุวัตถุประสงค์ของหน่วยงาน ทำให้ผู้ปฏิบัติงานเครือข่ายได้เข้าใจขั้นตอน และวิธีการปฏิบัติงานไปในทางเดียวกัน สามารถใช้เป็นเครื่องมือในการตรวจสอบสถานะการทำงานของอุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์แม่ข่าย และปริมาณการใช้งานเครือข่าย โดยสามารถทราบปัญหาข้อผิดพลาดที่อาจจะเกิดขึ้นระหว่างการให้บริการทางด้านระบบเครือข่ายได้อย่างทันที หรือมีข้อมูลที่เป็นประโยชน์สำหรับการประเมินความเสี่ยงในการให้บริการเครือข่าย ทราบสถานะการใช้งานเครือข่ายที่ไม่เป็นปกติที่อาจจะเป็นสาเหตุให้การให้บริการเครือข่ายต้องหยุดชะงัก ทำให้สามารถดำเนินการเชิงรุกป้องกันปัญหาได้อย่างทันท่วงทีก่อนที่จะเกิดปัญหาขึ้น

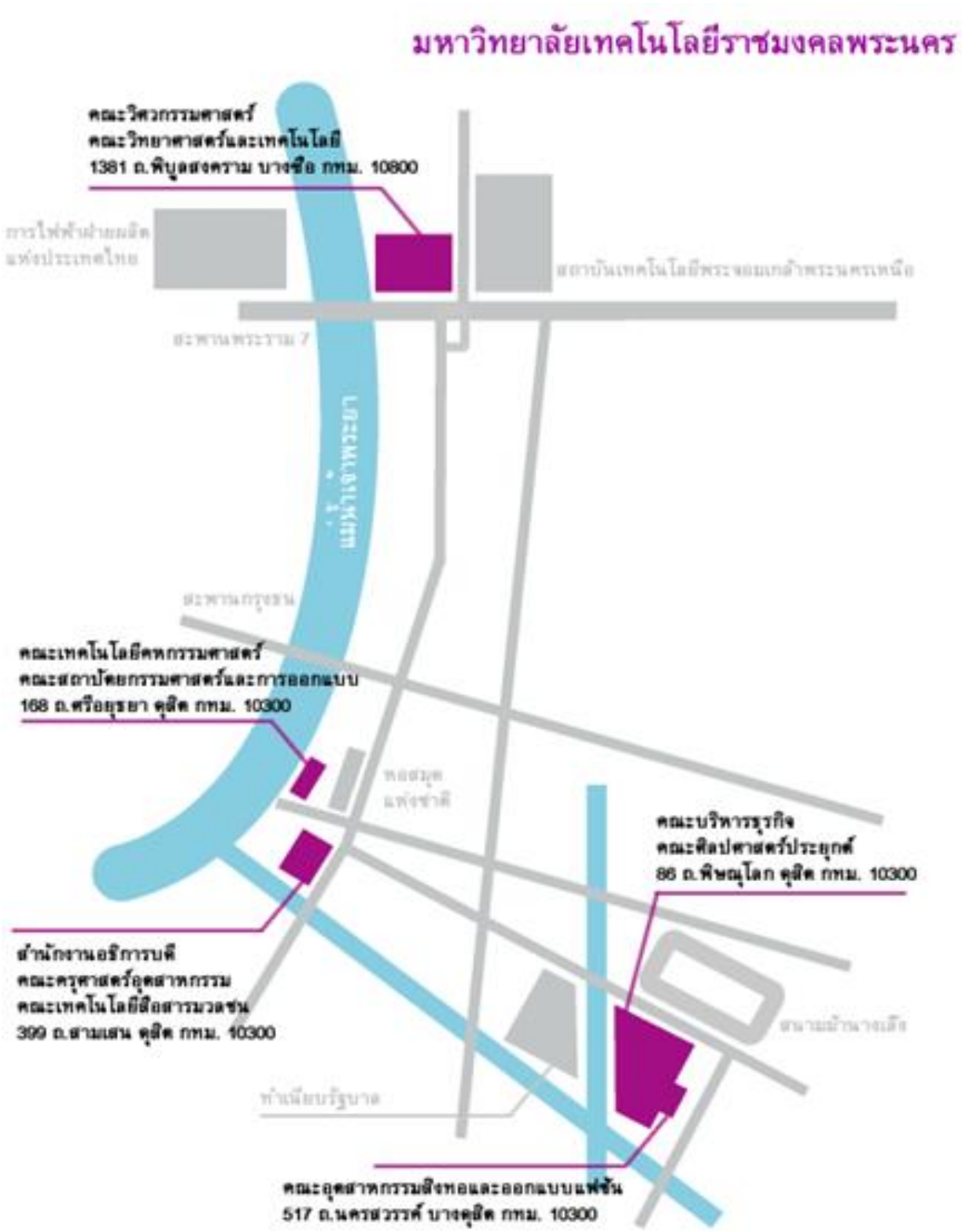
สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนครได้มีการพัฒนาระบบตรวจสอบสถานะ และปริมาณการใช้งานเครือข่ายขึ้น โดยใช้ซอฟต์แวร์ CactiEZ ซึ่งเป็นซอฟต์แวร์ประเภทโอเพ่นซอสสามารถนำมาใช้งานได้โดยไม่มีค่าลิขสิทธิ์ เพื่อสนับสนุนงานด้านการบริการระบบสารสนเทศของมหาวิทยาลัย และเพื่อให้การใช้งานระบบดังกล่าวเป็นไปด้วยความเรียบร้อย และเป็นมาตรฐานเดียวกัน ดังนั้น จึงได้จัดทำคู่มือปฏิบัติงานสำหรับเจ้าหน้าที่ประจำกลุ่มงานเครือข่ายคอมพิวเตอร์ และการสื่อสารขึ้น ผู้จัดทำหวังว่าเอกสารคู่มือปฏิบัติงานระบบตรวจสอบสถานะ และปริมาณการใช้งานเครือข่ายเล่มนี้ จะช่วยให้การบริการระบบสารสนเทศของมหาวิทยาลัย เป็นไปด้วยความเรียบร้อยและมีระบบเครือข่ายที่มีเสถียรภาพ

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญ

เนื่องด้วยปัจจุบันการให้บริการระบบเครือข่ายถือว่าเป็นหนึ่งในความต้องการพื้นฐานสำหรับหน่วยงานและองค์กรต่างๆ ไม่ว่าจะเป็นหน่วยงานภาครัฐ เอกชน สถาบันการศึกษา รวมถึงมหาวิทยาลัย จำเป็นต้องใช้งานระบบเครือข่ายในการทำงานทั้งสิ้น เช่น เพื่อใช้การติดต่อสื่อสาร การแลกเปลี่ยนข้อมูลข่าวสาร การสืบค้นข้อมูล การค้นคว้างานวิจัย หรือแม้แต่เพื่อความบันเทิง ทำให้เกิดการเชื่อมต่อระหว่างอุปกรณ์เครือข่ายภายในองค์กรมีจำนวนมากขึ้นตามเทคโนโลยีที่พัฒนาอย่างรวดเร็ว การดูแลระบบเครือข่ายจำเป็นต้องใช้บุคคลากรที่มีความรู้และความเชี่ยวชาญ พร้อมกับซอฟต์แวร์ที่ใช้สำหรับช่วยดูแลระบบอย่างมีประสิทธิภาพ แต่เนื่องจากอุปกรณ์และโปรแกรมด้านบริหารเครือข่ายที่มีจำหน่ายทั่วไปมีราคาสูงมาก ทำให้ผู้ใช้จำนวนมากหันมาสนใจโปรแกรมที่เป็นลักษณะ Open Source ซึ่งมี Community ของตนเองในการพัฒนาอย่างต่อเนื่อง และมีคุณภาพที่เป็นที่ยอมรับทั่วไป ดังนั้นทางกลุ่มงานระบบเครือข่ายจึงได้พัฒนาโปรแกรมเฝ้าระวัง และดูการจราจรทางด้านระบบเครือข่าย เพื่อให้ผู้ดูแลระบบสามารถเฝ้าดู และเข้าใจได้อย่างง่ายดาย พร้อมทั้งแก้ไขปัญหาได้อย่างรวดเร็ว ทำให้ระบบมีช่วงเวลาหยุด (Down time) น้อยที่สุด

โปรแกรม CACTI Traffic Grapher หรือเรียกกันสั้น ๆ ว่า “CACTI” เป็น Open Source Software ซึ่งทำหน้าที่ในการแสดงปริมาณข้อมูลทั้งขาเข้า และออก ในเครือข่าย โดยจะแสดงผลออกมาใน CACTI ใช้ RRDTool เป็นเครื่องมือในการทำงานสามารถเก็บข้อมูลให้อยู่ในรูปแบบฐานข้อมูล ทำให้สามารถย้อนกลับไปดูกราฟในวัน และเวลาที่ต้องการ อีกทั้งยังสามารถเลือกขยายกราฟเพื่อแสดงรายละเอียดที่มากขึ้น รวมถึงรูปแบบการแสดงผลที่สวยงาม และมีประสิทธิภาพ ซึ่งทั้งหมดนี้สามารถทำให้เข้าใจ และนำข้อมูลสถิติต่าง ๆ มาใช้ได้ง่าย ขึ้นประกอบกับมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร มีพื้นที่เขตการศึกษา 4 พื้นที่ ได้แก่ ศูนย์เทเวศร์ ศูนย์โชติเวช ศูนย์พณิชยการพระนคร ศูนย์ชุมพรเขตรอุดมศักดิ์ และศูนย์พระนครเหนือ เพื่อให้การตรวจสอบสถานะของระบบเครือข่าย และภาพรวมการใช้งานระบบเครือข่าย ปริมาณทราฟฟิก จำนวนผู้ใช้ และอื่นๆ บนระบบเครือข่ายทั้งหมดทุกพื้นที่ของมหาวิทยาลัยจากความต้องการดังกล่าว มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร จึงได้มีแนวคิดที่จะพัฒนาระบบตรวจสอบสถานะและปริมาณการใช้งานเครือข่าย ขึ้นมาใช้งาน และเพื่อเป็นเครื่อมือสำคัญที่ใช้ในการเตรียมตัว และรองรับสถานการณ์ต่าง ๆ ด้านระบบเครือข่ายของมหาวิทยาลัย ดังนั้นสำนักวิทยบริการและเทคโนโลยีสารสนเทศในฐานะหน่วยงานที่ได้รับมอบหมายให้กำกับดูแลงานด้านการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร จึงพัฒนาระบบตรวจสอบสถานะ และปริมาณการใช้งานเครือข่าย เพื่อสนับสนุน และรองรับการใช้งานในการบริหารจัดการเครือข่ายภายในมหาวิทยาลัย และเพื่อให้ระบบนี้ใช้งานได้อย่างมีประสิทธิภาพ และครอบคลุมทั้งองค์กร จึงจำเป็นต้องจัดทำ คู่มือการปฏิบัติงานระบบตรวจสอบสถานะ และปริมาณการใช้งานเครือข่าย



ภาพที่ 1-1 ภาพแสดงเขตพื้นที่ของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

1.2 วัตถุประสงค์

- เพื่อให้ผู้ใช้งานระบบตรวจสอบสถานะ และปริมาณการใช้งานเครือข่าย มีความรู้ ความเข้าใจเกี่ยวกับขั้นตอนวิธีการใช้งานระบบตรวจสอบสถานะ ปริมาณการใช้งานเครือข่าย และสามารถนำไปใช้เป็นแนวทางปฏิบัติงานได้
- เพื่อเป็นคู่มือสำหรับผู้ที่ทำงานด้านระบบเครือข่ายของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนครใช้เป็นแนวทางในการใช้งานระบบตรวจสอบสถานะ และปริมาณการใช้งานเครือข่าย
- เพื่อใช้ในการสร้างเครื่องมือที่ช่วยในการตรวจสอบระบบเครือข่ายได้อย่างมีประสิทธิภาพ
- เพื่อเผยแพร่ข้อมูลที่เป็นประโยชน์ต่อสังคม สำหรับผู้ที่สนใจสามารถนำไปใช้ในการศึกษาด้วยตนเองและนำไปพัฒนา หรือสร้างระบบตรวจสอบสถานะและปริมาณการใช้งานเครือข่าย ไปใช้ในองค์กรได้

1.3 ประโยชน์ที่คาดว่าจะได้รับ

ผู้ใช้งานระบบตรวจสอบสถานะ และปริมาณการใช้งานเครือข่ายได้รับความรู้ ความเข้าใจเกี่ยวกับขั้นตอนวิธีการทำงานของระบบตรวจสอบสถานะ และปริมาณการใช้งานเครือข่าย และสามารถใช้เป็นคู่มือในการปฏิบัติงานได้อย่างมีประสิทธิภาพ มีเครื่องมือ ที่แสดงผลเป็นรูปกราฟสวยงาม ใช้งานง่าย สะดวก เหมาะต่อการนำข้อมูลขึ้นมาแสดงหรือนำมามาวิเคราะห์ได้อย่างรวดเร็ว อีกทั้งเป็นโปรแกรมโอเพ่นซอร์สซึ่งทำงานได้บนระบบปฏิบัติการลีนุกส์ ซึ่งช่วยให้ประหยัดต้นทุนในการพัฒนาระบบทางด้านซอฟต์แวร์ได้อย่างมาก โดยสามารถนำมาใช้ในการตรวจสอบสถานะของระบบเครือข่าย อุปกรณ์เครือยข่าย ปริมาณทราฟฟิก การทำงานของเครื่องคอมพิวเตอร์แม่ข่าย โดยสามารถดูได้ผ่านทางระบบอินเทอร์เน็ต สามารถเข้าใช้งานระบบจากที่ใดก็ได้ตลอด 24 ชั่วโมง และระบบสามารถให้ข้อมูลย้อนหลังที่เป็นประโยชน์เพื่อนำมาวิเคราะห์ปัญหาที่เกิดขึ้นได้

1.4 ขอบเขตของคู่มือ

จัดทำคู่มือเพื่อรวบรวมข้อมูลที่เป็นประโยชน์สำหรับการใช้งาน ระบบตรวจสอบสถานะ และปริมาณการใช้งานเครือข่าย เพื่อให้สามารถใช้ตรวจสอบสถานะการทำงานของระบบเครือข่าย ปริมาณผู้ใช้งานเครือข่าย ปริมาณทราฟฟิกและสถานะของเครื่องคอมพิวเตอร์แม่ข่าย เช่น สถานะซีพียู สถานะหน่วยความจำ สถานะพื้นที่เก็บข้อมูล สถานะโปรเซสต่าง ๆ ที่ทำงานอยู่บนเครื่องคอมพิวเตอร์แม่ข่าย เป็นต้น มีการบันทึกข้อมูลและแจ้งเตือนโดยอัตโนมัติ ประกอบด้วยเนื้อหาของขอบเขต ดังนี้

- การใช้งานระบบ cacti เพื่อให้สามารถตรวจสอบสถานะของระบบเครือข่ายได้
- การปรับแต่งระบบ cacti ให้สามารถทำงานและรองรับกับสภาพแวดล้อมของแต่ล่ะองค์กรได้
- การดูแลและบำรุงรักษาระบบ cacti ให้พร้อมใช้งานอยู่เสมอ

1.5 คำจำกัดความเบื้องต้น

มหาวิทยาลัยฯ	มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร
หน่วยงานภายใน	หน่วยงานภายในที่สังกัดอยู่ภายในโครงสร้างของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร
หน่วยงานภายนอก	หมายถึงหน่วยงานอื่นที่ไม่ได้อยู่ภายในโครงสร้างของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร
ผู้ใช้งานเครือข่าย	บุคคลที่เข้าใช้งานระบบเครือข่ายของมหาวิทยาลัย
ผู้ปฏิบัติงานเครือข่าย	บุคลากรที่ทำหน้าที่ใดหน้าที่หนึ่งที่ได้รับมอบหมายตามคำสั่งโดยหัวหน้างานหรือผู้บังคับบัญชาให้กำกับ ดูแลระบบเครือข่าย
Cacti software	โปรแกรมใช้ในการตรวจสอบสถานะระบบเครือข่าย
Open Source Software	ซอฟต์แวร์ที่เปิดแผยหลักการหรือแหล่งที่มาของเทคโนโลยีของซอฟต์แวร์นั้นให้บุคคลภายนอกได้ใช้ ภายใต้เงื่อนไขบางประการที่เปิดโอกาสให้ผู้ใช้ทำการแก้ไข
Traffic	ปริมาณการใช้งานระบบเครือข่าย
Monitoring	ระบบตรวจสอบสถานะเครือข่าย
เครื่องคอมพิวเตอร์แม่ข่าย	เครื่องคอมพิวเตอร์ที่ทำหน้าที่ในการให้บริการด้านระบบสารสนเทศของมหาวิทยาลัย

บทที่ 2
บทบาทและหน้าที่ความรับผิดชอบ

2.1 บทบาทหน้าที่ความรับผิดชอบของตำแหน่ง

ปฏิบัติงานในฐานะผู้ปฏิบัติงานระดับต้นที่ต้องใช้ความรู้ความสามารถทางวิชาการในการทำงานปฏิบัติงานเกี่ยวกับด้านวิทยาการคอมพิวเตอร์ พัฒนาระบบเครือข่าย ติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย ดูแล ติดตั้ง ซ่อมบำรุงอุปกรณ์คอมพิวเตอร์ และอุปกรณ์เครือข่าย การให้บริการศูนย์การเรียนรู้ด้วยตนเอง และห้องคอมพิวเตอร์สำหรับการจัดการฝึกอบรม รวมถึงการสำรวจ ตรวจสอบระบบเครือข่าย เมื่อมีการขยายพื้นที่ให้บริการหรือมีการพัฒนาระบบสารสนเทศใหม่ ภายใต้การกำกับ แนะนำ ตรวจสอบ และปฏิบัติงานอื่นตามที่ได้รับมอบหมาย

2.2 ลักษณะงานที่ปฏิบัติ

ลักษณะงานที่ปฏิบัติของกลุ่มงานเครือข่ายคอมพิวเตอร์และการสื่อสาร

1. ดูแล รักษา อุปกรณ์คอมพิวเตอร์และอุปกรณ์เครือข่ายต่าง ๆ เพื่อให้สามารถให้บริการได้อย่างต่อเนื่อง และทั่วถึงครอบคลุมทุกพื้นที่
2. ร่วมวางแผนการจัดการคอมพิวเตอร์ และระบบเครือข่าย เพื่อให้การบริการคอมพิวเตอร์และระบบเครือข่ายที่มีประสิทธิภาพและสามารถให้บริการได้ตลอดเวลา
3. ประสานงานกับผู้ร่วมงานภายใน และภายนอกหน่วยงาน เกี่ยวกับรายละเอียดในการพัฒนาระบบเครือข่ายคอมพิวเตอร์ และการสื่อสาร เพื่อสร้างความเข้าใจ และความร่วมมือในการดำเนินงาน
4. ให้คำปรึกษา ความรู้ด้านการใช้อุปกรณ์คอมพิวเตอร์ และอุปกรณ์เครือข่าย ให้เกิดการถ่ายทอดความรู้ที่ถูกต้องกับผู้สนใจ
5. วิเคราะห์ การควบคุม ดูแล รักษา อุปกรณ์คอมพิวเตอร์ และอุปกรณ์เครือข่ายต่าง ๆ เพื่อให้สามารถให้บริการได้อย่างต่อเนื่อง และทั่วถึงครอบคลุมทุกพื้นที่ของมหาวิทยาลัย และมีความทันสมัยรองรับเทคโนโลยีในปัจจุบัน
6. ศึกษา วิเคราะห์ ร่วมวางแผนงานที่จะช่วยลดกระบวนการทำงานในการให้บริการคอมพิวเตอร์และระบบเครือข่าย โดยบรรลุเป้าหมาย ลดทรัพยากรบุคคล ลดค่าใช้จ่าย และดำเนินการได้ตรงตามกำหนดเวลา
7. ประสานงานกับผู้ร่วมงานภายใน และภายนอกหน่วยงาน เกี่ยวกับรายละเอียดพัฒนาระบบเครือข่ายคอมพิวเตอร์ และการสื่อสาร เพื่อสร้างความเข้าใจ และความร่วมมือในการดำเนินงาน ให้ดำเนินการได้ตรงตามกำหนดเวลา และตรงตามวัตถุประสงค์ของงาน

2.3 ภาระหน้าที่ความรับผิดชอบ

2.3.1 ด้านปฏิบัติการ

1. วิเคราะห์ เสนอแนะ ควบคุมโครงการพัฒนาระบบเครือข่ายคอมพิวเตอร์ และการสื่อสาร โดยควบคุมให้การปฏิบัติงานให้เป็นไปด้วยความเรียบร้อย ดูแลด้านการให้บริการระบบเครือข่าย เมื่อมีการพัฒนาใหม่หรือการปรับปรุงระบบเครือข่าย หรือมีการร้องขอจากหน่วยงานภายใน และภายนอก เพื่อให้สามารถรองรับการทำงานของระบบสารสนเทศต่าง ๆ เพื่อสนับสนุนภารกิจหลักของมหาวิทยาลัย
2. ควบคุม ดูแล การติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายชุดคำสั่งระบบปฏิบัติการ หรือชุดคำสั่งสำเร็จรูปอื่น ๆ ที่เกี่ยวข้อง โดยการทดสอบคุณสมบัติด้านเทคนิคของเครื่องคอมพิวเตอร์แม่ข่าย วิเคราะห์ สรุปผล ประเมินประสิทธิภาพ เมื่อมีการพัฒนาสารสนเทศใหม่หรือมีการร้องขอจากหน่วยงานภายในและภายนอก เพื่อให้ระบบสารสนเทศต่าง ๆ สามารถทำงานได้อย่างถูกต้อง
3. พัฒนาชุดคำสั่ง แก้ไขข้อผิดพลาดของคำสั่ง เมื่อมีการพัฒนาระบบใหม่หรือปรับปรุงระบบที่มีอยู่เดิม เพื่อให้ระบบงาน ซอฟต์แวร์ หรือสารสนเทศอื่น ๆ สามารถทำงานได้อย่างถูกต้องแม่นยำและมีประสิทธิภาพมากที่สุด
4. ดูแลความเรียบร้อยและสถานะการทำงานของอุปกรณ์เครือข่าย โดยมีระบบที่สามารถสร้างการแจ้งเตือนได้ เมื่ออุปกรณ์ทำงานผิดพลาดหรือเกิดความเสียหาย เพื่อให้อุปกรณ์อิเล็กทรอนิกส์สายสัญญาณ รวมถึงอุปกรณ์อื่น ๆ ที่เกี่ยวข้องอยู่ในสภาพที่เพียงพอ และพร้อมต่อการใช้งานอยู่เสมอ
5. จัดทำระบบรักษาความปลอดภัยระบบเครือข่าย โดยการใช้อุปกรณ์ไฟล์วอลล์หรืออื่น ๆ ให้เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ของผู้ใช้งานอยู่ในความปลอดภัยจากการถูกคุกคาม หลอกลวง หรือการโจมตีผ่านระบบเครือข่ายทุกประเภท เพื่อให้การใช้งานระบบสารสนเทศต่าง ๆ ดำเนินไปด้วยความเรียบร้อย และมีเสถียรภาพในการใช้งาน
6. จัดทำทะเบียนเครื่องคอมพิวเตอร์ และอุปกรณ์เครือข่าย บันทึก รวบรวมข้อมูลพื้นฐานที่เกี่ยวข้องกับคอมพิวเตอร์ และระบบเครือข่าย เมื่อมีการเพิ่ม ลดจำนวนหรือการโอนถ่ายอุปกรณ์ไปยังหน่วยงานอื่น เพื่อให้มีฐานข้อมูลที่เป็นปัจจุบัน ใช้สนับสนุนการปฏิบัติงานให้เป็นไปตามระเบียบวิธีปฏิบัติ สะดวกต่อการค้นหา และเป็นหลักฐานข้อมูลที่ตรวจสอบได้
7. จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ของผู้ใช้งานเป็นระยะเวลา 90 วัน โดยดำเนินการจัดเก็บทางคอมพิวเตอร์แบบรวมศูนย์ เพื่อที่จะสามารถเรียกดูข้อมูลย้อนหลัง หรือให้ข้อมูลจราจรทางคอมพิวเตอร์แก่หน่วยงานภายนอกได้เมื่อมีการเรียกขอ

8. ศึกษา ค้นคว้า ด้านระบบเครือข่ายคอมพิวเตอร์ โดยทำการ ทดลอง วิเคราะห์ สังเคราะห์ เทคโนโลยีด้านระบบเครือข่ายที่ทันสมัย เพื่อนำมาใช้การพัฒนางานด้านระบบเครือข่ายที่มีประสิทธิภาพสูง และมีเสถียรภาพในการทำงาน
9. ทำการสำรองข้อมูลของเครื่องคอมพิวเตอร์แม่ข่ายอย่างสม่ำเสมอ โดยใช้วิธีการจัดเก็บทางคอมพิวเตอร์ มีอุปกรณ์สำหรับจัดเก็บข้อมูลที่เพียงพอ และข้อมูลที่จัดเก็บไว้จะต้องสามารถเรียกคืนได้ทันทีเมื่อต้องการ เพื่อให้ระบบงานต่าง ๆ สามารถทำงานได้อย่างราบรื่นตลอดเวลา
10. จัดทำคู่มือด้านระบบเครือข่าย เมื่อมีการพัฒนาระบบใหม่หรือการปรับปรุงระบบ โดยจัดให้มีการเผยแพร่สู่ผู้ใช้งานในหลายช่องทาง เช่น เว็บไซต์ หรือสื่อสิ่งพิมพ์อื่นๆเพื่อให้มีผู้ใช้งานระบบได้รับข้อมูล และสามารถนำไปปฏิบัติตามได้
11. ปฏิบัติงาน และสนับสนุนงานอื่น ๆ ตามที่ได้รับมอบหมาย เพื่อสนับสนุนให้มหาวิทยาลัยในภาพรวมบรรลุภารกิจที่กำหนดไว้

2.3.2 ด้านการวางแผน

1. ร่วมวางแผนการจัดการเครื่องคอมพิวเตอร์ และระบบเครือข่าย เพื่อกำหนดมาตรฐานในการควบคุมสิทธิการใช้งาน วิธีการบริหารจัดการระบบเครือข่าย รวมทั้งการให้บริการคอมพิวเตอร์และระบบเครือข่ายที่มีประสิทธิภาพ และสามารถให้บริการได้ตลอดเวลา โดยจัดทำเป็นข้อกำหนดและนโยบายการใช้งานคอมพิวเตอร์และระบบเครือข่าย
2. จัดเตรียมข้อมูล ศึกษาเทคโนโลยี และเอกสารที่เกี่ยวข้องประกอบการวางแผนวิเคราะห์ระบบเครือข่าย และอุปกรณ์เครือข่ายตลอดจนการทบทวนปรับแต่งขั้นตอนการปฏิบัติงาน โดยจัดทำเป็นแผนปฏิบัติงาน การให้บริการด้านคอมพิวเตอร์ และระบบเครือข่าย
3. ศึกษาพันธกิจหลักของมหาวิทยาลัยประกอบการปรับกลยุทธ์ในแผนแม่บทที่เกี่ยวข้องกับการพัฒนาระบบเครือข่าย และระบบสารสนเทศ เพื่อวางแนวทางในการพัฒนาระบบเครือข่ายให้มีความทันสมัยและสอดคล้องกับความก้าวหน้าทางเทคโนโลยีปัจจุบัน โดยจัดทำเป็นแผนพัฒนาระบบเครือข่ายและโครงสร้างพื้นฐานด้านระบบเครือข่าย

2.3.3 ด้านการประสานงาน

1. ประสานงานกับหน่วยงานภายใน และภายนอก โดยเพื่อเพิ่มประสิทธิภาพในการพัฒนาระบบเครือข่ายคอมพิวเตอร์ และการสื่อสารเพื่อให้สอดคล้องกับนโยบายด้านเทคโนโลยีสารสนเทศ ซึ่งส่งผลต่อประสิทธิภาพในการดำเนินงานของมหาวิทยาลัย โดยการพูดคุย หรือในที่ประชุม
2. ชี้แจง ให้รายละเอียด ข้อมูล หรือข้อเท็จจริงแก่บุคคลที่เกี่ยวข้องในขั้นตอนการพัฒนาระบบเครือข่าย โดยทำหนังสือชี้แจง หรือชี้แจงด้วยวาจา เพื่อสร้างความเข้าใจหรือความร่วมมือในการดำเนินงาน

และงานสัมฤทธิ์ผลตามแผนที่วางไว้

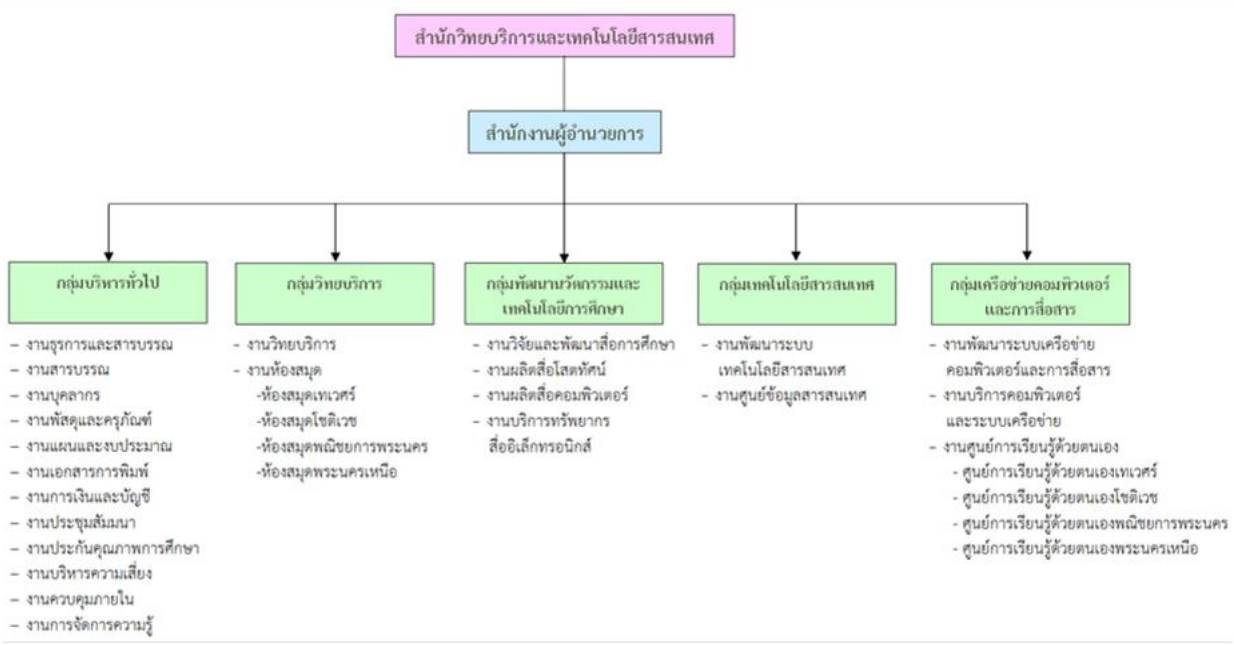
2.3.4 ด้านการบริการ

1. ให้บริการด้านระบบเครือข่าย โดยการจัดเตรียมอุปกรณ์เครือข่ายไว้สำหรับให้บริการ ซึ่งมีจำนวนเพียงพอ และอยู่ในสภาพพร้อมใช้งาน เมื่อได้รับการร้องขอจากบุคลากรทั้งใน และภายนอกหน่วยงาน เพื่อสนับสนุนงานด้านคอมพิวเตอร์ และระบบเครือข่าย
2. ให้คำปรึกษา ฝึกอบรมทักษะในการติดตั้งระบบปฏิบัติการ การดูแลเครื่องคอมพิวเตอร์แม่ข่าย ให้กับผู้ใต้บังคับบัญชา โดยการอธิบายด้วยคำพูด หรือการเป็นวิทยากร และผู้ช่วยวิทยากรในเวลางาน ตามโอกาสต่าง ๆ หรือในการฝึกอบรมนักศึกษา หรือผู้สนใจเพื่อให้ความสามารถนำความรู้ที่ได้ไปปฏิบัติตามได้อย่างถูกต้อง และเกิดประโยชน์สูงสุด
3. ให้คำปรึกษา ด้านการให้บริการในศุนย์การเรียนรู้ด้วยตนเอง การปรับปรุงภูมิทัศน์และสภาพแวดล้อมในศูนย์การเรียนรู้ด้วยตนเอง โดยมีเครื่องคอมพิวเตอร์ไว้ให้บริการอย่างเพียงพอ เพื่อใช้ในการศึกษา ค้นคว้าหรือการวิจัย รวมทั้งสามารถใช้เป็นสถานที่ในการจัดโครงการฝึกอบรม
4. ร่วมดำเนินการจัดประชุมสัมมนาทางวิชาการด้านการพัฒนาระบบเครือข่าย เพื่อให้บุคลากรที่เกี่ยวข้อง หรือบุคลากรที่สนใจได้พัฒนาความรู้ ทักษะทางด้านคอมพิวเตอร์ และระบบเครือข่ายได้อย่างถูกต้องและเกิดผลสัมฤทธิ์ตามที่กำหนด

2.4 โครงสร้างหน่วยงาน

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร มีโครงสร้างหน่วยงานที่ประกอบด้วย 5 กลุ่มงาน ได้แก่

- ☐ กลุ่มบริหารทั่วไป
- ☐ กลุ่มวิทยบริการ
- ☐ กลุ่มพัฒนานวัตกรรมและเทคโนโลยีการศึกษา
- ☐ กลุ่มเทคโนโลยีสารสนเทศ
- ☐ กลุ่มเครือข่ายคอมพิวเตอร์และการสื่อสาร



ภาพที่ 2-1 โครงสร้างสำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

2.5 ภาระหน้าที่ของหน่วยงาน

1. เสนอแนวนโยบาย และแผนการพัฒนาด้านวิทยบริการและเทคโนโลยีสารสนเทศของมหาวิทยาลัย ให้มีเอกภาพรวมทั้งมหาวิทยาลัย

2. กำหนดกลยุทธ์การส่งเสริม และสนับสนุนให้หน่วยงานในสังกัดของมหาวิทยาลัย พัฒนางานด้านวิทยบริการและเทคโนโลยีสารสนเทศตามภารกิจที่รับผิดชอบ

3. กลั่นกรองแผนงานด้านวิทยบริการ และงานด้านเครือข่ายระบบสารสนเทศของมหาวิทยาลัย เพื่อการจัดสรรงบประมาณที่เกี่ยวข้อง

4. วางมาตรฐาน และกำกับพัฒนาระบบสารสนเทศเพื่อการบริหาร เพื่อประโยชน์การเชื่อมโยงฐานข้อมูลด้านบุคคล งบประมาณ วิชาการ นักศึกษา ให้เป็นระบบในภาพรวมระดับมหาวิทยาลัย

5. บริหารจัดการพัฒนาเครือข่ายเทคโนโลยีสารสนเทศ ควบคุมดูแลอุปกรณ์การเรียนการสอนที่ผ่านทางเครือข่ายคอมพิวเตอร์

6. สร้างระบบเครือข่ายเทคโนโลยีสารสนเทศ เพื่อให้เกิดความเชื่อมโยงทางวิชาการกับมหาวิทยาลัยทั้งใน และต่างประเทศ

7. ให้บริการทางวิชาการในรูปการให้คำปรึกษา แนะนำแก่หน่วยงานต่าง ๆ ใน การพัฒนาระบบสารสนเทศ

8. บริหารงานภายในสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

9. ปฏิบัติภารกิจอื่น ๆ ตามที่มหาวิทยาลัยมอบหมาย

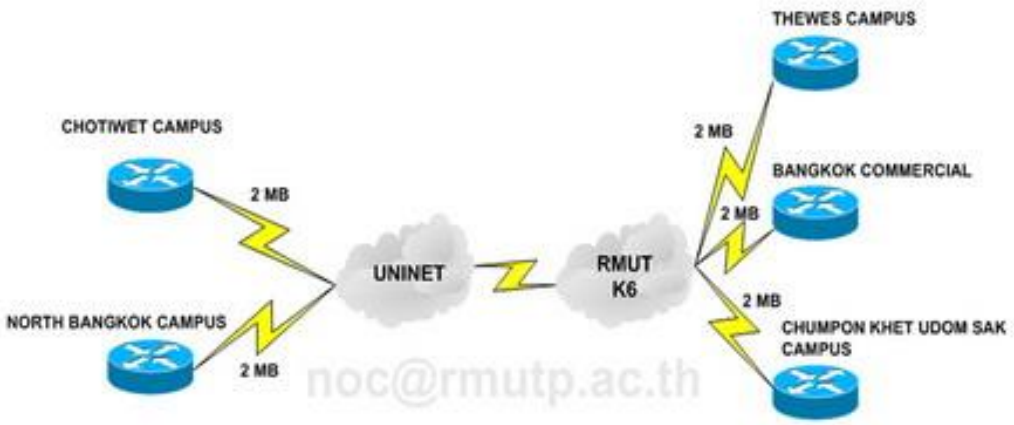
บทที่ 3
หลักเกณฑ์วิธีการปฏิบัติงาน

3.1 แนวคิด

มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ได้รับการสถาปนาขึ้นในพระราชบัญญัติมหาวิทยาลัยเทคโนโลยีราชมงคล เมื่อวันที่ 18 มกราคม พ.ศ. 2548 ประกอบด้วยวิทยาเขต 5 แห่ง ได้แก่

- วิทยาเขตเทเวศร์ [thewes.rit.ac.th]
- วิทยาเขตโชติเวช [chtwc.rit.ac.th]
- วิทยาเขตพณิชยการพระนคร [bcc.rit.ac.th]
- วิทยาเขตชุมพรเขตรอุดมศักดิ์ [ckus.rit.ac.th]
- วิทยาเขตพระนครเหนือ [nbk.rit.ac.th]

ข้อมูลระบบเครือข่ายเดิม แต่ละวิทยาเขต (วิทยาเขตเทเวศร์ ,วิทยาเขตโชติเวช ,วิทยาเขตพณิชยการพระนคร ,วิทยาเขตชุมพรเขตรอุดมศักดิ์ ,วิทยาเขตพระนครเหนือ) ได้ใช้เทคโนโลยี ของ Cisco System โดยใช้ Router เป็นอุปกรณ์ค้นหาเส้น เชื่อมต่อ ผ่านLeased Line มี Bandwidth ขนาด 2 Mb ต่อไปที่สำนักเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีราชมงคล



ภาพที่ 3-1 โครงสร้างการเชื่อมต่อระบบเครือข่าย มทร. พระนคร

มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ได้ดำเนินการ จดโดเมนใหม่ ในวันที่ 8 ก.ย. 2548 เพื่อให้สอดคล้องกับลักษณะขององค์กร ดังนี้

มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร Domain Name : rmutp.ac.th

- วิทยาเขตเทเวศร์ Domain Name : thewes.rmutp.ac.th
- วิทยาเขตโชติเวช Domain Name : chtwc.rmutp.ac.th

- วิทยาเขตพณิชยการพระนคร Domain Name : bcc.rmutp.ac.th
- วิทยาเขตชุมพรเขตรอุดมศักดิ์ Domain Name : ckus.rmutp.ac.th
- วิทยาเขตพระนครเหนือ Domain Name : nbk.rmutp.ac.th

เมื่อ วันที่ 15 ต.ค. 2548 ได้มีการดำเนินการ เรื่อง โครงการจัดตั้งสำนักวิทยบริการและเทคโนโลยีสารสนเทศ มทร.พระนคร [RMUTP Net] ซึ่งประกอบไปด้วย วิทยาเขตเทเวศร์ , วิทยาเขตโชติเวช , วิทยาเขตพณิชยการพระนคร , วิทยาเขตชุมพรเขตรอุดมศักดิ์ และวิทยาเขตพระนครเหนือ โดยมีอาจารย์ นิวัตร จารุวาระกูล เป็นประธานโครงการจัดตั้งสำนักวิทยบริการและเทคโนโลยีสารสนเทศ สำนักงานตั้งอยู่ที่ อาคาร 1 (ตึกบ่อปลา) ชั้น 4 และในวันที่ 2 มี.ค. 2549 สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มทร.พระนคร ได้ดำเนินการย้ายวงจรการสื่อสารจาก สำนักเทคโนโลยีสารสนเทศ มทร.ธัญบุรี ไปเชื่อมต่อกับทาง สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา (UniNet) โดยใช้วงจรการสื่อสารของ CAT Telecom ซึ่งใช้เทคโนโลยี MPLS (Multi Protocol Label Switching) เพื่อเชื่อมต่อกับสำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา (UniNet) โดยทำให้ Gateway ของมหาวิทยาลัย มี Bandwidth ขนาด 20Mb และวงจรเชื่อมต่อของวิทยาเขตพณิชยการพระนคร และวิทยาเขตพระนครเหนือ มี Bandwidth ขนาด 10Mb เชื่อมต่อกับสำนักวิทยบริการและเทคโนโลยีสารสนเทศ มทร.พระนคร ที่เทเวศร์

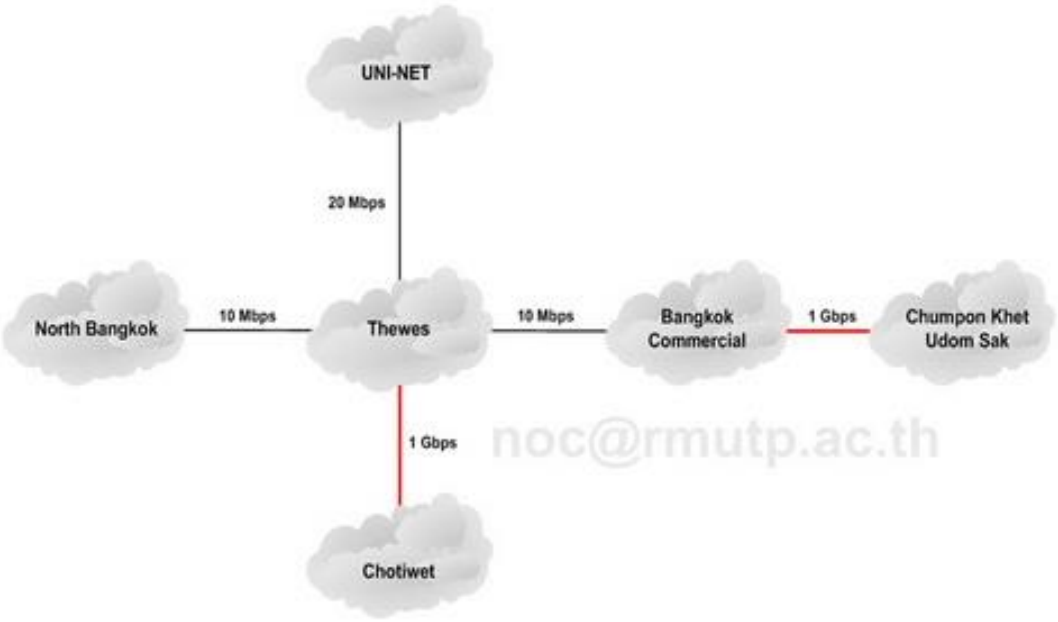
โดยทำการติดตั้งระบบ Core Switch ของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร โดยใช้ Alcatel [Omniswitch 7800] โดยมีเชื่อมต่อดังนี้

ส่วนที่ 1

- วิทยาเขตพณิชยการพระนคร เชื่อมต่อ กับ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ที่มีBandwidth ขนาด 10Mb
- วิทยาเขตพระนครเหนือ เชื่อมต่อ กับ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ที่มี Bandwidth ขนาด 10Mb

ส่วนที่ 2

- วิทยาเขตชุมพรเขตรอุดมศักดิ์ เชื่อมต่อ กับ วิทยาเขตพณิชยการพระนคร ความเร็ว 1 Gbps
- วิทยาเขตโชติเวช เชื่อมต่อ กับ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ความเร็ว 1 Gbps
- วิทยาเขตเทเวศร์ เชื่อมต่อ กับ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ความเร็ว 1 Gbps



ภาพที่ 3-2 โครงสร้างการเชื่อมต่อระบบเครือข่าย มทร. พระนคร ใหม่

จากภาพที่ 3-2 เป็นรูปแบบการเชื่อมต่อที่ใช้งานมาจนถึงในปัจจุบัน แต่ได้ทำการปรับปรุงลิงค์ของทุกเส้นทางให้เป็นอุปกรณ์ Fiber Optic และเพิ่มความเร็วในการเชื่อมต่อเป็น 1 Gbps ทั้งหมด

3.2 ข้อตกลงระดับการให้บริการ (Service Level Agreement)

จะเห็นได้ว่าการนำระบบเครือข่ายมาใช้งานเพื่อให้สามารถตอบสนองการบริการด้านระบบสารสนเทศของมหาวิทยาลัยที่เกี่ยวข้องกับการจัดการศึกษา สามารถแบ่งออกได้ 2 ลักษณะ คือ การใช้ระบบสารสนเทศเพื่อการบริหารจัดการ และการใช้ระบบสารสนเทศเพื่อการจัดการเรียนการสอน ซึ่งในปัจจุบันการใช้สารสนเทศเพื่อการบริหารจัดการ และเพื่อการจัดการเรียนการสอน ได้แก่

- ☐ มีระบบเครือข่ายบริการเพื่อใช้ในการเข้าถึงแหล่งเรียนรู้ทั้งภายใน และภายนอกมหาวิทยาลัย
- ☐ มีระบบเครือข่ายเพื่อให้บริการระบบสารสนเทศของมหาวิทยาลัย
- ☐ มีระบบเครือข่ายเพื่อใช้ในการติดต่อสื่อสาร ระบบโทรศัพท์ ระบบ video conference
- ☐ มีระบบเครือข่ายที่สามารถใช้ในการเผยแพร่ ประชาสัมพันธ์ข่าวสาร และผลการดำเนินกิจกรรมต่าง ๆ ของมหาวิทยาลัยสู่สาธารณะชนได้

ซึ่งทุกเป้าหมาย ดังกล่าวมีวัตถุประสงค์เพื่อสนับสนุนงานวิชาการ และการจัดการเรียนการสอนเป็นสำคัญ แต่ก็ยังเอื้อประโยชน์ต่องานด้านการบริหารจัดการด้วย ในบางส่วน ได้แก่ การเป็นช่องทางในการติดต่อกับหน่วยงานอื่น ๆ ภายนอกมหาวิทยาลัย เช่น การดาวน์โหลดเอกสารสำคัญจากหน่วยงานทางด้านการศึกษา การสื่อสารด้วยจดหมายอิเล็กทรอนิกส์ของบุคลากรภายในมหาวิทยาลัย การใช้เป็นช่องทางสื่อสารเพื่องานชุมชนสัมพันธ์ เป็นต้น

SLA หรือ Service Level Agreement คือ สัญญาที่กำหนดรายละเอียดเรื่องการให้บริการ เมื่อนำมาใช้กับงานบริการ IT ภายในองค์กรแล้ว ส่วนใหญ่จะเป็นการกำหนดถึงมาตรฐานในการให้บริการ โดยวัดจากเวลาเป็นสำคัญ เช่น งานติดตั้งคอมพิวเตอร์ต้องเสร็จภายใน 8 ชั่วโมง ระบบเครือข่ายเมื่อเกิดปัญหาจะต้องสามารถแก้ไขให้แล้วเสร็จในระยะเวลาไม่เกิน 2 ชั่วโมง หรือเมื่อเส้นทางเครือข่ายหลักเกิดปัญหาเส้นทางสำรองจะต้องสามารถทำงานทดแทนได้ทันที หรือไม่เกิน 5 นาที เป็นต้น

3.3 การจัดทำ SLA (Service Level Agreement) ด้านระบบเครือข่าย

เพื่อเป็นข้อกำหนดการให้บริการ ระหว่างผู้ให้บริการระบบเครือข่าย และผู้ใช้บริการระบบเครือข่าย โดยมีข้อตกลงถึงระดับคุณภาพของบริการที่มีให้แก่ผู้ใช้บริการ รับทราบและเข้าใจถูกต้องตรงกัน เช่น

3.3.1 สามารถให้บริการ support ตรวจสอบ และแก้ไขปัญหาด้านเทคนิคแก้ผู้ใช้บริการอันเกิดจากระบบเครือข่ายของผู้ให้บริการผ่านช่องทางโทรศัพท์หมายเลข 02-665-3777 ต่อ 6785 ได้ในวันและเวลาราชการ ยกเว้นกรณีเหตุสุดวิสัย เช่น โทรศัพท์ขัดข้อง, คู่สายเต็ม, ไฟดับ หรือปัญหาทางด้านระบบการให้บริการสัญญานโทรศัพท์ของผู้ให้บริการขัดข้อง

3.3.2 ระบบ support ตอบคำถามผ่านทางระบบ email ผู้ใช้บริการสามาถส่งอีเมล์เข้ามาที่ network-team@rmutp.ac.th ผู้ใช้บริการจะได้รับตอบกลับจากเจ้าหน้าที่ support ภายในระยะเวลาไม่เกิน 24 ชั่วโมง นับตั้งแต่ได้รับ email โดยจะสรุปรายงานการแก้ไขปัญหา สาเหตุของปัญหาและแนวทางการแก้ไขปัญหาของผู้ใช้บริการ เนื่องจากปัญหาของผู้ใช้บริการแต่ล่ะราย มีสภาพของปัญหาที่เกิดจากปัจจัยและตัวแปรของปัญหาที่แตกต่างกัน

3.3.3 รับประกันค่าเฉลี่ยในการ uptime 99.9% โดยอัตรานี้จะไม่รวมถึง scheduled down time ที่มีการวางแผนปรับปรุงระบบเครือข่าย และแจ้งให้ผู้ใช้บริการทราบล่วงหน้า ยกเว้นกรณีปัญหา Link Network/ISP Down กรณีเหตุภัยพิบัติธรรมชาติ หรือเหตุวิกฤตอื่น ๆ ที่ไม่สามารถควบคุมได้

3.3.4 มีเส้นทางระบบเครือข่ายสำรอง ที่สามารถใช้งานได้ทันทีเมื่อเส้นทางหลัก หรือเส้นทางปัจจุบันไม่สามารถใช้งานได้

3.3.5 มีระบบตรวจสอบสถานะ และปริมาณการใช้งานเครือข่าย เพื่อให้ผู้ใช้บริการเครือข่ายสามารถใช้ในการตรวจสอบสถานะได้

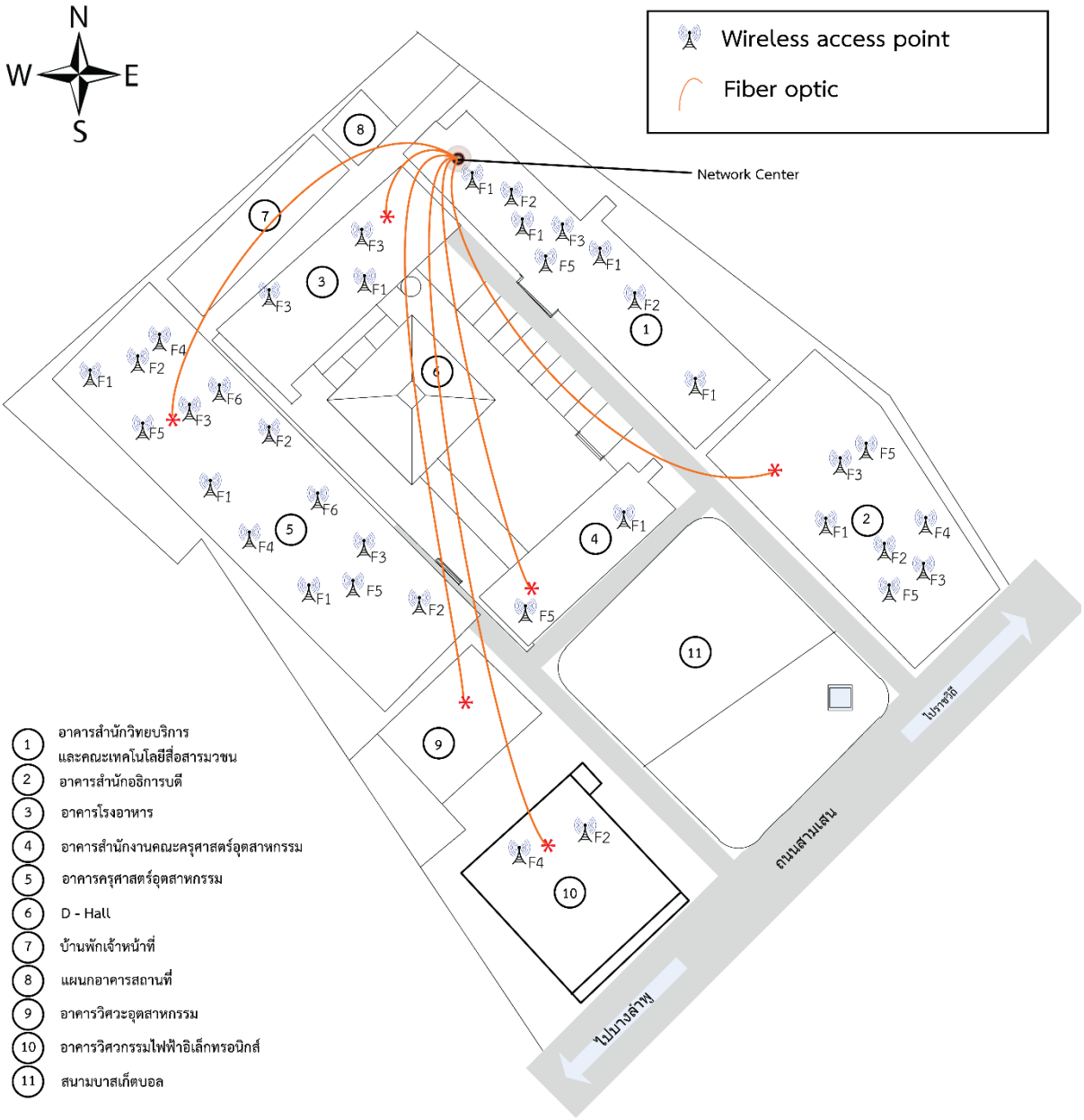
3.4 วิธีการปฏิบัติงาน

การเตรียมข้อมูลสำหรับนำเข้าสู่ระบบตรวจสอบสถานะและปริมาณการใช้งานเครือข่าย (cacti) โดยทำการสำรวจข้อมูลอุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์แม่ข่ายทั้งหมด โดยแยกออกเป็นแต่ละพื้นที่ดังนี้

- ☐ พื้นที่เครือข่าย zone 1 ประกอบไปด้วย ศูนย์เทเวศร์และโชติเวช
- ☐ พื้นที่เครือข่าย zone 2 ประกอบไปด้วย ศูนย์พณิชยการพระนครและศูนย์ชุมพรเขตอุดมศักดิ์
- ☐ พื้นที่เครือข่าย zone 3 ประกอบไปด้วย ศูนย์พระนครเหนือ

ผังบริเวณ มทร.พระนคร (ศูนย์เทเวศร์)

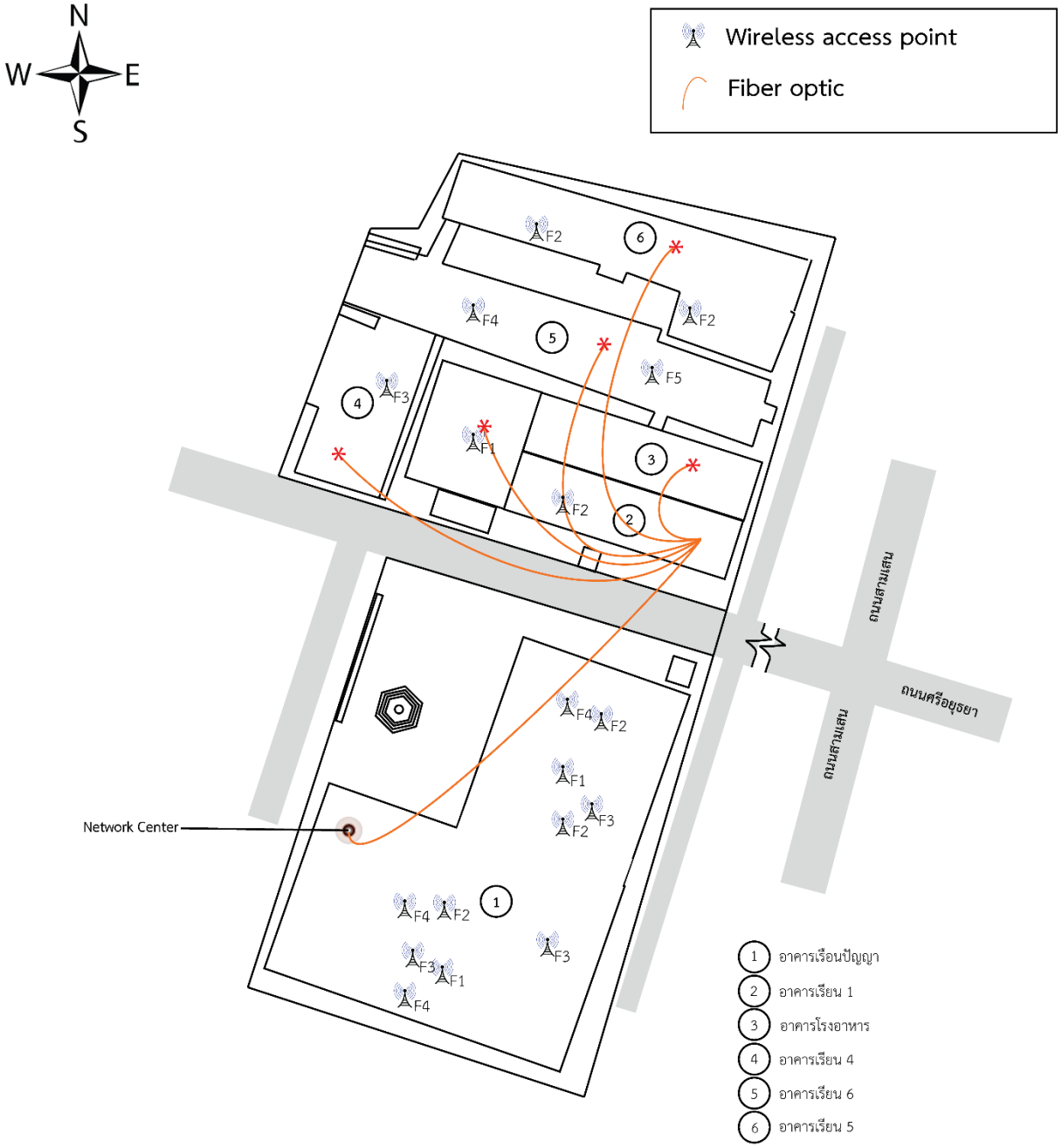
คณะครุศาสตร์อุตสาหกรรม คณะเทคโนโลยีสื่อสารมวลชน สำนักอธิการบดี



ภาพที่ 3-3 แผนผังบริเวณการเชื่อมต่อระบบเครือข่ายศูนย์เทเวศร์

ผังบริเวณ มทร.พระนคร (ศูนย์โชติเวช)

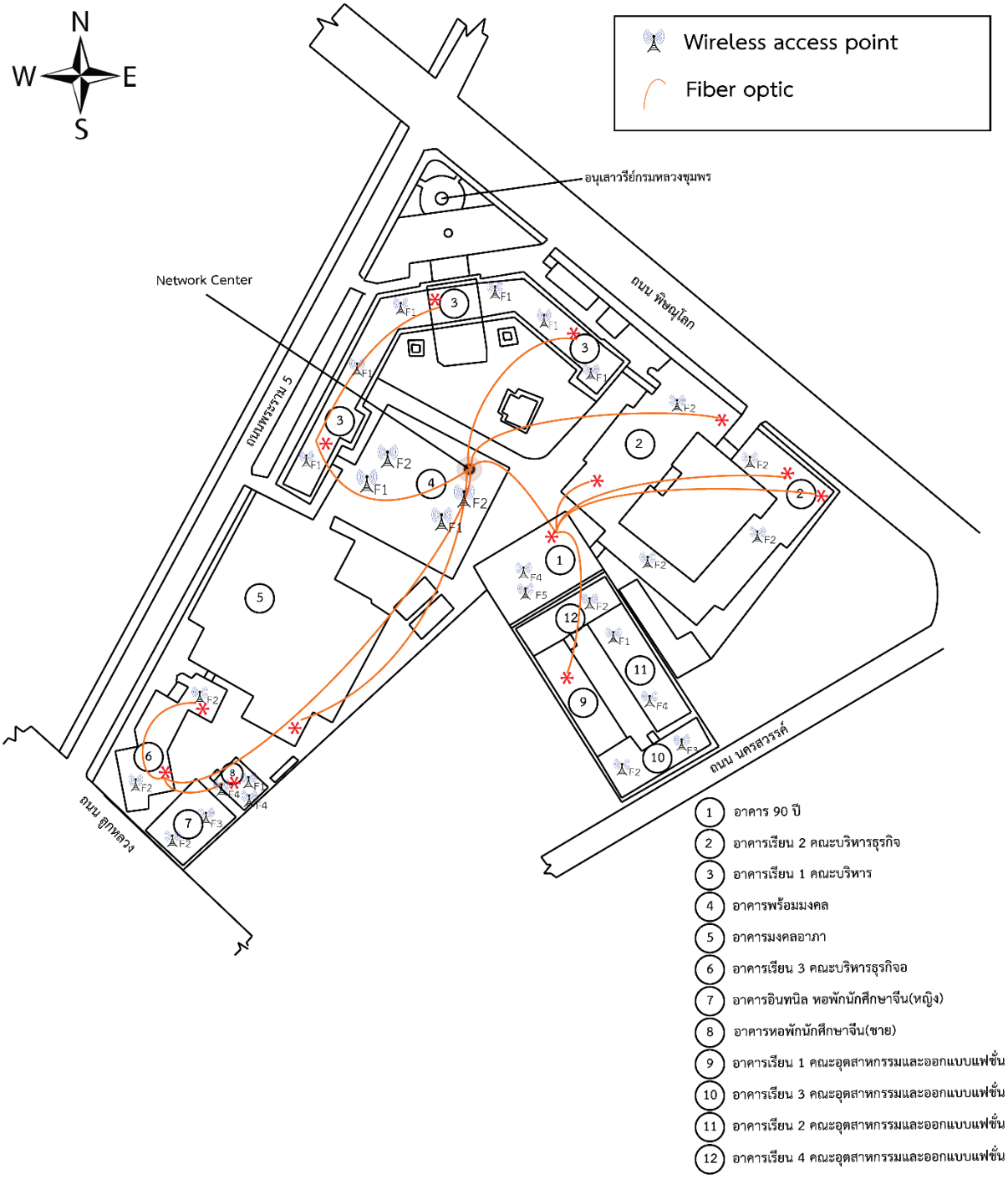
คณะเทคโนโลยีคหกรรมศาสตร์ คณะสถาปัตยกรรมและการออกแบบ



ภาพที่ 3-4 แผนผังบริเวณการเชื่อมต่อระบบเครือข่ายศูนย์โชติเวช

ผังบริเวณ มทร.พระนคร (ศูนย์พาณิชยการณ์พระนคร)

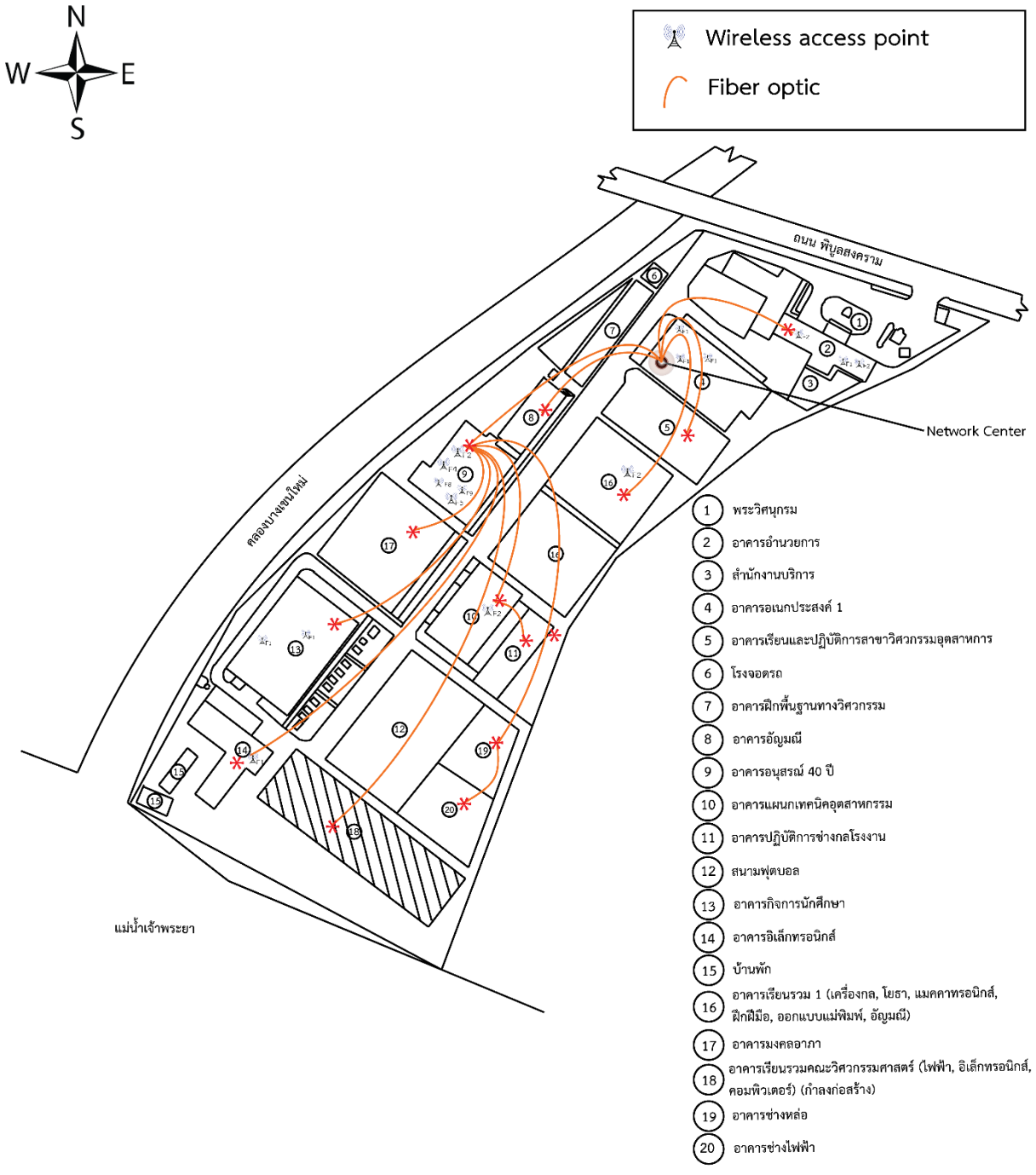
คณะบริหารธุรกิจ คณะศิลปศาสตร์ คณะอุตสาหกรรมสิ่งทอและออกแบบแฟชั่น



ภาพที่ 3-5 แผนผังบริเวณการเชื่อมต่อระบบเครือข่ายศูนย์พณิชยการพระนคร

ผังบริเวณ มทร.พระนคร (ศูนย์พระนครเหนือ)

คณะวิศวกรรมศาสตร์ คณะวิทยาศาสตร์และเทคโนโลยี



ภาพที่ 3-6 แผนผังบริเวณการเชื่อมต่อระบบเครือข่ายศูนย์พระนครเหนือ

จากนั้นรวบรวมข้อมูลของอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายที่จำเป็นต้องใช้สำหรับระบบตรวจสอบสถานะและปริมาณการใช้งานเครือข่ายดังต่อไปนี้

1. หมายเลขไอพีแอดเดรส
2. ชื่ออุปกรณ์
3. ระบบปฏิบัติการ
4. สถานที่ติดตั้งอุปกรณ์

บทที่ 4
เทคนิคในการปฏิบัติงาน

หลักเกณฑ์ วิธีการและขั้นตอนการปฏิบัติงาน

หลักเกณฑ์ วิธีการและขั้นตอนการปฏิบัติงานของผู้ใช้งาน และขั้นตอนการทำงานของระบบตรวจสอบสถานะและปริมาณการใช้งานเครือข่าย มีหัวข้อที่เกี่ยวข้อง ดังนี้

1) การวิเคราะห์ภาพรวมของระบบ
2) การติดตั้ง SNMP Service สำหรับอุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย
3) การติดตั้งโปรแกรม MIB Browser เพื่อทดสอบ SNMP Service
4) การติดตั้งโปรแกรม cacti และการปรับแต่งระบบ
5) การบริหารจัดการอุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์แม่ข่ายในระบบ cacti
6) การเขียน php script เพื่อนำมาใช้งานร่วมกับระบบ cacti
7) การติดตั้ง template สำเร็จรูปสำหรับโปรแกรม cacti
8) การใช้งาน plugin (monitor, weather map, realtime)
9) การสร้างบัญชีผู้ใช้ และการกำหนดสิทธิ์ (User Management)
10) การสำรองข้อมูล และการกู้คืนระบบ cacti

4.1 การวิเคราะห์ภาพรวมของระบบ

ปัจจุบันนี้ระบบเครือข่ายมีความซับซ้อนมากขึ้น การบริหารจัดการระบบเครือข่ายไม่ใช่แค่เพียงติดตั้งและใช้งาน แต่ต้องมีการตรวจสอบเฝ้าระวังประสิทธิภาพการทำงานเพื่อทำการบำรุงรักษาให้ระบบทำงานได้อย่างมีประสิทธิภาพ และต่อเนื่อง การลดลง หรือถดถอยของประสิทธิภาพการทำงานของระบบเครือข่ายในบางระบบงานอาจทำให้เกิดความเสียหายมูลค่าสูง ทั้งทางการเงิน หรือทรัพย์สิน รวมทั้งชีวิตได้ เช่น ระบบจำหน่ายไฟฟ้า หรือระบบท่อส่งแก๊สและน้ำมัน และนั่นคือที่มาของความต้องการโปรโตคอลในการบริหารจัดการระบบเครือข่าย หรือโปรโตคอล SNMP ซึ่งอยู่ในชุดโปรโตคอล TCP/IP (Transmission Control Protocol/Internet Protocol) [1]

โปรโตคอล SNMP ได้ถูกพัฒนาขึ้นในปี พ.ศ.2531 เนื่องจากมีความเจริญเติบโตในการใช้อุปกรณ์ที่สนับสนุนโปรโตคอล TCP/IP อย่างสูง โปรโตคอล SNMP ถูกออกแบบให้มีฟังก์ชัน และการทำงานแบบง่าย ๆ เหมาะกับคำว่าซิมเปิล (Simple) ตามชื่อของมัน โดยมีจุดประสงค์หลักเพื่อให้ผู้ดูแลระบบเครือข่ายสามารถเข้ามาจัดการอุปกรณ์เครือข่ายได้จากระยะไกลโดยง่าย สิ่งที่สำคัญของโปรโตคอล SNMP ก็คือความง่ายในการใช้งาน ทำให้ผู้ดูแลระบบเครือข่ายสามารถควบคุมอุปกรณ์ที่สนับสนุน SNMP ได้จากที่ไหน

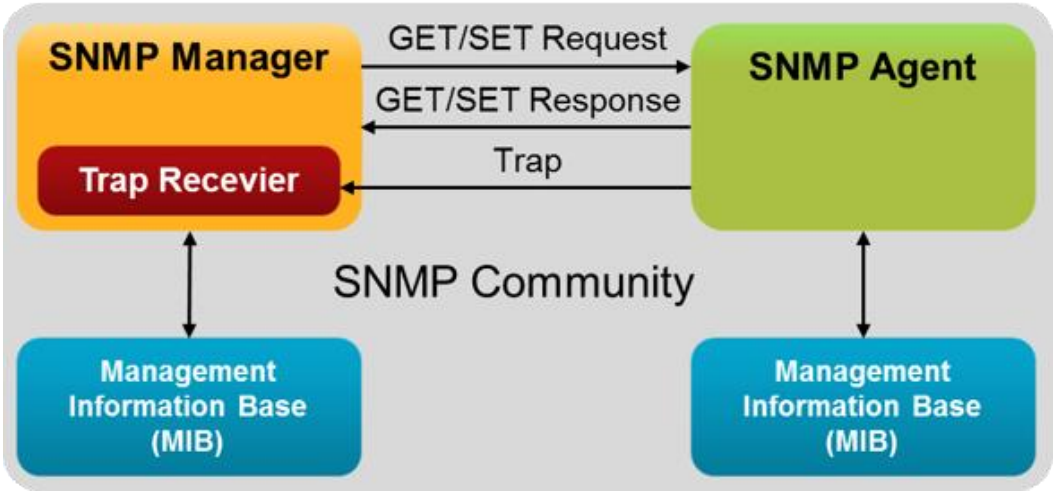
ก็ได้ที่ระบบเครือข่ายนั้นไปถึง ตัวอย่างคือ ผู้ดูแลระบบเครือข่ายสามารถทดลองแก้ไขปัญหาอย่างเร่งด่วน โดยทำการรีเซตพอร์ตอีเทอร์เน็ตสวิตช์ที่ต่อเข้ากับ PLC (Programmable Logic Controller) ที่ไม่สามารถติดต่อระบบควบคุมได้ หรือสามารถตรวจสอบอัตราการเข้าใช้งาน (Utilized Rate) หรือการเกิดจากเฟรมผิดพลาดของพอร์ต หรือแม้กระทั่งตรวจสอบอุณหภูมิของอุปกรณ์เครือข่ายว่าเป็นปกติ หรือไม่ เพื่อเข้าทำการบำรุงรักษาก่อนที่ระบบเครือข่ายจะขัดข้อง ซึ่งถือว่าเป็นการบำรุงรักษาแบบ CBM (Condition-based Maintenance) อีกหน้าที่หนึ่งของ SNMP ที่สำคัญคือ การใช้เฝ้าระวัง หรือมอนิเตอร์ระบบเครือข่ายทั้งระบบ แตกต่างจากการเข้าจัดการอุปกรณ์แบบรายอุปกรณ์ ซึ่งฟังก์ชันการมอนิเตอร์ระบบเครือข่ายดังกล่าวเรียกอีกอย่างว่า RMON (Remote Network Monitoring) ซึ่งได้ถูกพัฒนาเพื่อช่วยในการวิเคราะห์การทำงานของระบบเครือข่าย

สำหรับมาตรฐานโปรโตคอล TCP/IP จะมีหน่วยงานสากลในชื่อ IETF (Internet Engineering Task Force) ที่คอยกำกับดูแลซึ่งรวมไปถึงโปรโตคอล SNMP ด้วย โดยทาง IETF จะทำการตีพิมพ์ข้อกำหนดมาตรฐานในชื่อ RFCs (Request for Comments) โดยเริ่มแรกข้อกำหนดจะถูกนำเสนอให้ทาง IETF ทำการพิจารณา หลังจากรับข้อกำหนด IETF จะพิจารณาขั้นต้น และข้อกำหนดนั้นจะเข้าสู่สถานะฉบับร่าง และท้ายสุดจะเข้าสู่สถานะอนุมัติเมื่อข้อกำหนดนั้นสมบูรณ์ และ RFC ฉบับนั้นจะถูกพิจารณาให้เป็นมาตรฐาน แต่อย่างไรก็ตามอันที่จริงมีไม่กี่ RFC ที่ถูกอนุมัติให้เป็นมาตรฐาน สืบเนื่องมาจากเทคโนโลยีทางด้านการสื่อสารมีความก้าวหน้าแบบก้าวกระโดด ทำให้เกิด RFC ตัวใหม่เข้ามาแทนที่ ทั้ง ๆ ที่ตัวเก่ายังไม่รับอนุมัติให้เป็นมาตรฐาน รายการดังต่อไปนี้เป็นเวอร์ชัน และ RFC ของโปรโตคอล SNMP [2] [3]

SNMP Version 1 (SNMPv1) เป็นมาตรฐานปัจจุบัน และเป็นที่นิยมเพราะความง่ายของโปรโตคอล SNMP ซึ่งถูกระบุใน RFC1157 และได้รับอนุมัติให้เป็นมาตรฐานที่สมบูรณ์ ระดับความปลอดภัย SNMPv1 จะขึ้นอยู่กับคอมมิวนิตี้สตริง (Community String) ที่ทำหน้าที่เหมือนรหัสผ่าน หรือพาสเวิร์ด (Password) โดยที่จริงแล้วเป็นเพียงข้อความแบบธรรมดา (Plain Text) ที่บ่งบอกถึงสิทธิการเข้าไปจัดการอุปกรณ์เครือข่าย โดยปกติคอมมิวนิตี้จะมีสามประเภทนั้นคือ อ่านอย่างเดียว (Read-only), อ่านเขียน (Read-write) และแทรป (Trap)

SNMP Version 2 (SNMPv2) คือ เวอร์ชันที่ทำงานบนคอมมิวนิตี้ที่ได้รับการปรับปรุง ในทางเทคนิคเรียกว่า SNMPv2c ซึ่งระบุใน RFC1905, RFC1906 และ RFC1907 และอยู่ในขั้นตอนทดสอบใช้งาน แต่ก็มีบางผู้ผลิตได้นำมาใช้งานในอุปกรณ์ของพวกเขา SNMPv2 ออกแบบมาเพื่อแก้ไขข้อด้อยของ SNMPv1 ในเรื่องการร้องข้อมูลปริมาณมาก และปัญหาในการส่งข้อมูลแบบแทรป

SNMP Version 3 (SNMPv3) เป็นเวอร์ชันถัดไปของโปรโตคอล SNMP ที่ถูกคาดหวังให้เป็นมาตรฐานที่สมบูรณ์ ซึ่งในปัจจุบันอยู่ในสถานะนำเสนอระบุใน RFC1905, RFC1906, RFC1907, RFC2571, RFC2572, RFC2573, RFC2574 และ RFC2575 โดยมุ่งเน้นการเพิ่มระดับความปลอดภัยของโปรโตคอล SNMP



ภาพที่ 4-1 แสดงโครงสร้างของ SNMP Service [4]

โปรโตคอล SNMP ใช้ UDP เป็นโปรโตคอลในการส่ง และรับข้อมูลระหว่างตัวเมเนเจอร์ และเอเยนต์ เพราะว่าโปรโตคอล UDP ใช้การเชื่อมต่อแบบคอนเน็กชันเลส (Connectionless) ซึ่งไม่มีการเชื่อมต่อสื่อสารหรือทำแฮนด์แช็กกิ้งก่อนที่จะรับ และส่งข้อมูลระหว่างเมเนเจอร์ และเอเยนต์ลักษณะการทำงานของโปรโตคอล UDP จริง ๆ มีระดับความเชื่อถือได้ที่ไม่สูง เพราะไม่มีการตอบรับแพ็กเกจถ้าเกิดมีการสูญหายระหว่างทางดังนั้นจึงตกเป็นหน้าที่ระดับแอพพลิเคชั่นที่ต้องประเมินว่าแพ็กเกจสูญหาย หรือไม่ หรือต้องทำการส่งการร้องขอใหม่ หรือไม่ วิธีที่ใช้ทั่วไปคือการใช้ไทเมอร์ หรือไทม์เอาต์เมเนเจอร์ที่ส่งเมสเซสร้องขอไปยังตัวเอเยนต์จะคอยการตอบสนองในระยะเวลาหนึ่ง ซึ่งระยะเวลานั้นขึ้นอยู่กับการตั้งค่าของผู้ดูแลระบบเครือข่าย ถ้าหมดระยะเวลาการรอคอยแล้วไม่มีการตอบสนองใด ๆ จากเอเยนต์ เมเนเจอร์จะประเมินว่าแพ็กเกจเกิดการสูญหาย และจะทำการส่งเมสเซสการร้องขออีกครั้ง จำนวนครั้งที่การร้องขอซ้ำนั้นขึ้นอยู่กับการตั้งค่าเช่นกัน แต่ข้อดีของโปรโตคอล UDP คือการที่ UDP มีค่าโอเวอร์เฮดที่ต่ำไม่ไปรบกวนหรือส่งผลกระทบกระเทือนต่อประสิทธิภาพของระบบเครือข่าย หรือตัวระบบงานหลัก อันที่จริงโปรโตคอล SNMP ก็สามารถใช้โปรโตคอล TCP แต่ก็เป็นเฉพาะกรณีพิเศษอย่างยิ่งเท่านั้น สำหรับระบบเครือข่ายที่ความคับคั่งสูงเป็นความคิดที่ไม่ถูกต้องที่จะใช้โปรโตคอล TCP ก็เพราะว่าโปรโตคอล TCP อันที่จริงก็ไม่เหมาะสมกับทุกระบบงานโดยเฉพาะกับระบบเครือข่ายที่ไม่สมบูรณ์ หรือคับคั่งสูง โปรโตคอล SNMP ถูกคาดหวังว่าสามารถทำงานได้ดีแม้ในระบบเครือข่ายที่ไม่สมบูรณ์ แต่ถ้าระบบเครือข่ายมีปัญหาอยู่ และยังมีระบบจัดการ

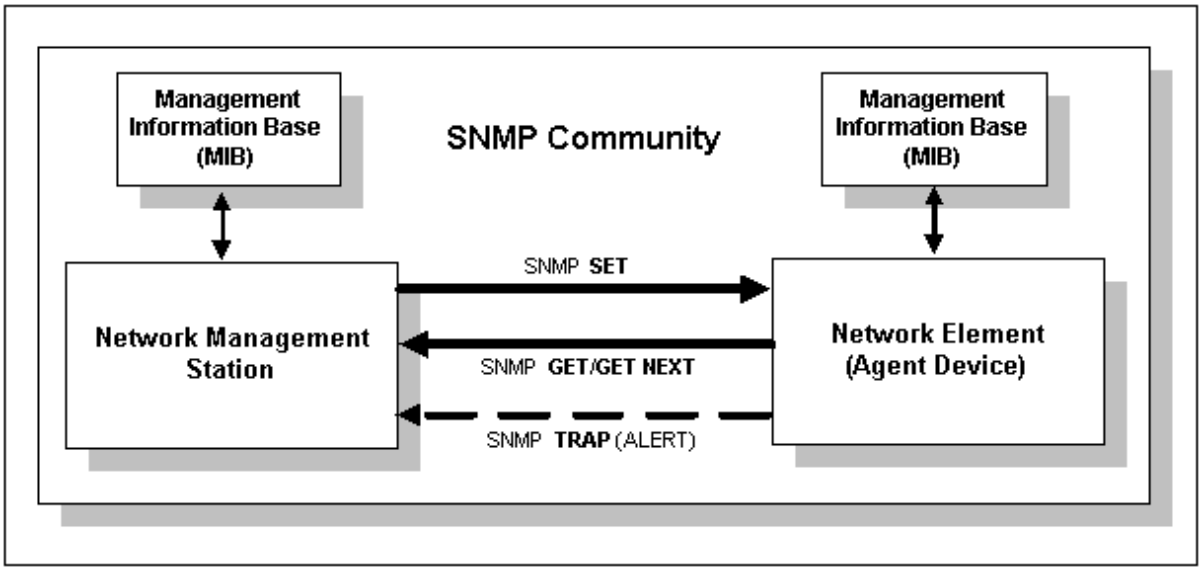
เครือข่ายที่เพิ่มปัญหาเข้าไปอีก เช่น การใช้โปรโตคอล TCP ที่มีค่าโอเวอร์เฮดที่สูง เป็นต้น ก็ไม่น่าจะเป็นความคิดที่ถูกต้อง

โปรโตคอล SMNP ใช้พอร์ต UDP หมายเลข 161 สำหรับส่ง และรับแบบการร้องขอข้อมูล และใช้พอร์ตหมายเลข 161 สำหรับรับเมสเซจชนิดแทรปจากเอเยนต์ของอุปกรณ์เครือข่ายที่ถูกจัดการ ทุกอุปกรณ์เครือข่ายต้องใช้พอร์ตหมายเลขดังกล่าวเป็นหมายเลขดีฟอลต์ แต่อย่างไรก็ตามบางผู้ผลิตอนุญาตให้เปลี่ยนหมายเลขพอร์ต ซึ่งเมเนเจอร์ต้องรับทราบ และเปลี่ยนหมายเลขพอร์ตให้ตรงกับอุปกรณ์เครือข่าย เพื่อให้สามารถติดต่อรับส่งเมสเซจได้

4.1.2 SNMP คอมมิวนิตี้ (SNMP Communities)

สำหรับ SNMPv1 และ SNMPv2 ที่เป็นที่นิยม จะใช้ระบบคอมมิวนิตี้ในการสร้างความปลอดภัยในการรับส่งข้อมูลระหว่างเมเนเจอร์ และเอเยนต์ โดยทั่วไปเอเยนต์จะถูกตั้งค่าให้มีคอมมิวนิตี้ 3 ประเภท โดยวิธีการตั้งชื่อ นั้นคือ อ่านได้อย่างเดียว สามารถอ่านเขียน และแทรป ชื่อคอมมิวนิตี้ หรือคอมมิวนิตี้สตริง อันที่จริงทำงานเสมือนเป็นรหัสผ่าน โดยผู้ผลิตทั่วไปจะให้คอมมิวนิตี้สตริง ชื่อพับลิก (Public) สำหรับการอ่านได้อย่างเดียว คอมมิวนิตี้สตริง ชื่อไพรเวต (Private) สำหรับการอ่าน และเขียน หรือเซตติ้งตั้งค่า เป็นสิ่งที่ดีที่จะเปลี่ยนชื่อคอมมิวนิตี้สตริงที่เป็นดีฟอลต์ให้เป็นชื่อเฉพาะเพื่อเพิ่มระดับความปลอดภัย การสร้างแทรปเพื่อแจ้งผู้ดูแลระบบเครือข่ายเมื่อมีการพยายามเข้ามาตั้งค่า หรือร้องขอข้อมูลจากตัวเอเยนต์ด้วยชื่อคอมมิวนิตี้สตริงที่ไม่ถูกต้อง หรือไม่ตรงกับที่กำหนดก็เป็นสิ่งที่ดี ก็เพราะเป็นการแจ้งเตือนว่าอาจเกิดมีผู้ไม่หวังดีพยายามเข้ามาเจาะระบบเครือข่าย

เนื่องจากชื่อคอมมิวนิตี้สตริงเสมือนเป็นรหัสผ่านของระบบจัดการเครือข่าย ดังนั้นการตั้งชื่อคอมมิวตี้สตริงก็ควรตั้งตามกฎการตั้งรหัสผ่านของเซิร์ฟเวอร์ เช่น ไม่เป็นคำในพจนานุกรม คำควรมีทั้งตัวเล็กตัวใหญ่ รวมทั้งตัวเลข เป็นต้น

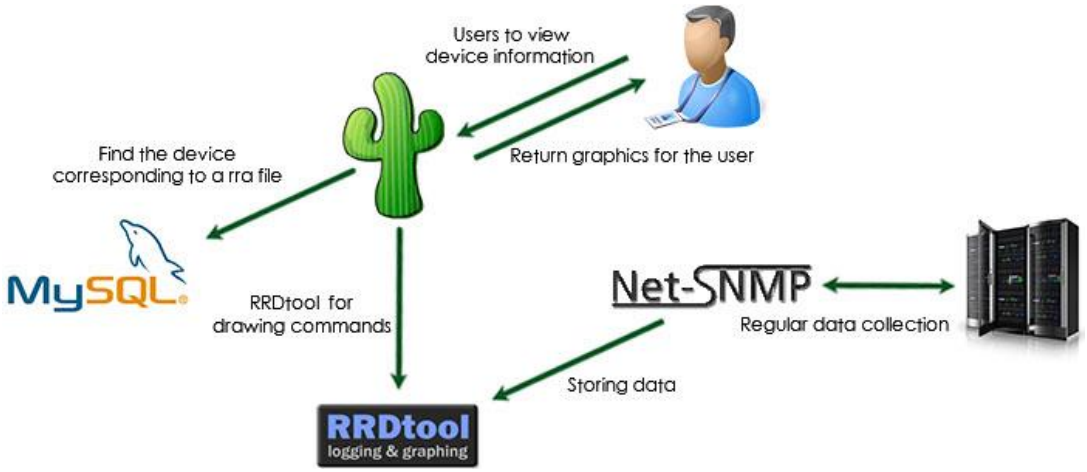


ภาพที่ 4-2 แสดงโครงสร้างการทำงานของ SNMP Community [4]

แต่อย่างไรก็ตามระดับความปลอดภัยด้วยคอมมิวนิตี้สตริงก็ยังต่ำอยู่ เนื่องจากคอมมิวนิตี้สตริงถูกส่งแบบข้อความธรรมดาไม่มีการเข้ารหัส ทำให้ง่ายต่อผู้บุกรุกที่มีความชำนาญสูงสามารถทำการดักจับชื่อคอมมิวนิตี้สตริงได้ และใช้มันเป็นจุดเริ่มต้นในการเจาะเข้าระบบเครือข่าย ดังนั้นจึงได้มีออกข้อกำหนดเพิ่มระดับความปลอดภัยให้สูงขึ้นในมาตรฐาน SNMPv3 แต่อย่างไรก็ตามยังมีวิธีการลดระดับความเสี่ยงต่อการเจาะระบบ ก็คือการติดตั้งไฟล์วอลล์ (Firewall) ซึ่งสามารถกำหนดให้ไฟร์วอลล์อนุญาตเฉพาะโฮสต์ที่รู้จักเข้ามาจัดการระบบเครือข่ายได้เท่านั้น เป็นสิ่งสำคัญที่ต้องตระหนักว่าถ้ามีใครซักคนสามารถอ่านเขียนอุปกรณ์เครือข่ายด้วย SNMP ก็คือสามารถเข้ามาควบคุมระบบเครือข่ายได้ เช่น ปิดพอร์ตเราเตอร์ การเปลี่ยนตารางเราเตอร์ซึ่งทำให้ระบบเครือข่ายล้มเหลวได้ อีกวิธีการหนึ่งในการเพิ่มระดับความปลอดภัย คือการใช้ฟังก์ชัน VPN (Virtual Private Network) เนื่องจากทราฟิกของ VPN จะถูกเข้ารหัสไว้ทำให้ดักจับได้ยาก อีกวิธีการหนึ่งแบบง่าย ๆ คือการเปลี่ยนชื่อคอมมิวนิตี้สตริงอย่างสม่ำเสมอ แต่ก็เป็นการยากสำหรับระบบเครือข่ายขนาดใหญ่ที่จำนวนเมเนเจอร์ และเอเยนต์จำนวนมาก

4.1.3 ภาพรวมการทำงานของ SNMP Service และระบบ Cacti

เนื่องจาก cacti มีการเรียกเก็บข้อมูลจากอุปกรณ์ต่าง ๆ ผ่านทาง SNMP Service เพราะฉะนั้นสามารถแสดงภาพรวมในการทำงานของระบบ cacti และ SNMP Service ได้ดังภาพ



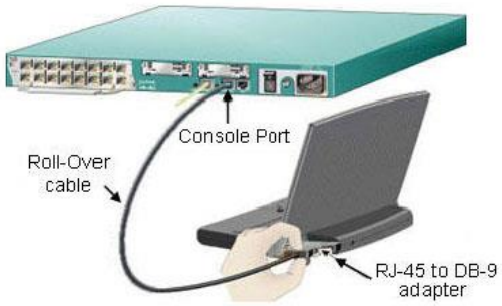
ภาพที่ 4-3 แสดงโครงสร้างการทำงานของ cacti และ SNMP Service [5]

4.2 ขั้นตอนการเปิดใช้งาน SNMP

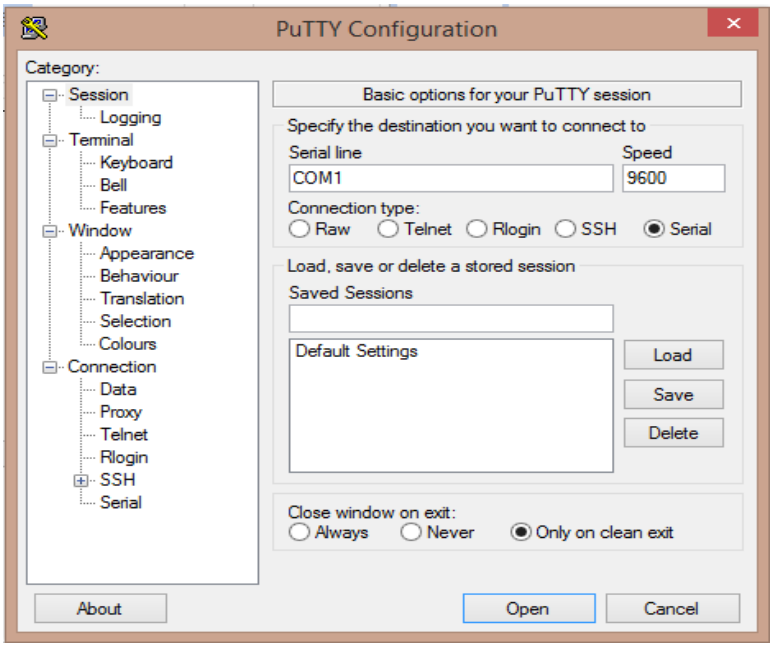
โดยอุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย ที่ทางมหาวิทยาลัยเทคโนโลยีราชมงคลพระนครใช้งานอยู่มีความหลากหลาย รวมถึงระบบปฏิบัติการที่ใช้อยู่ด้วยเช่นกัน ดังนั้นขั้นตอนต่อไปนี้จะแสดงวิธีการในการเปิด SNMP Service ของอุปกรณ์แต่ล่ะประเภท

4.2.1 ขั้นตอนการเปิด SNMP บนอุปกรณ์ Switch และ Router Cisco

- เปิดโปรแกรม Putty แล้วเลือก Connection type เป็น รูปแบบ Serial ในกรณี ที่เชื่อมต่ออุปกรณ์ด้วยสายคอนโทรล หรือ เลือก Telnet หรือ SSH ในกรณี ที่ Remote



ภาพที่ 4-4 แสดงการเชื่อมต่อสาย console เข้ากับอุปกรณ์ router [6]



ภาพที่ 4-5 แสดงหน้าต่างโปรแกรม putty

- เข้าไปยัง Global configure Mode เพื่อ Run คำสั่งในการเปิดใช้งาน SNMP
- พิมพ์คำสั่ง **Router(config)# snmp-server community public ro**
- หลังจากนั้นให้พิมพ์คำสั่ง **Router# copy running-config startup-config** เพื่อเป็นการบันทึกค่าคอนฟิก

4.2.2 ขั้นตอนการเปิด SNMP บนอุปกรณ์ Switch Alcatel

เปิดโปรแกรม Putty แล้วเลือก Connection type เป็น รูปแบบ Serial ในกรณี ที่เชื่อมต่ออุปกรณ์ด้วยสายคอนโทรล หรือ เลือก Telnet หรือ SSH ในกรณี ที่ Remote

- พิมพ์ชุดคำสั่ง ดังนี้

Switch> aaa authentication snmp local

Switch> user “username” password “xxxxxxxx” no auth

Switch> user “username” read-write snmp all

Switch> snmp station “IP cacti” “username” v1 enable on

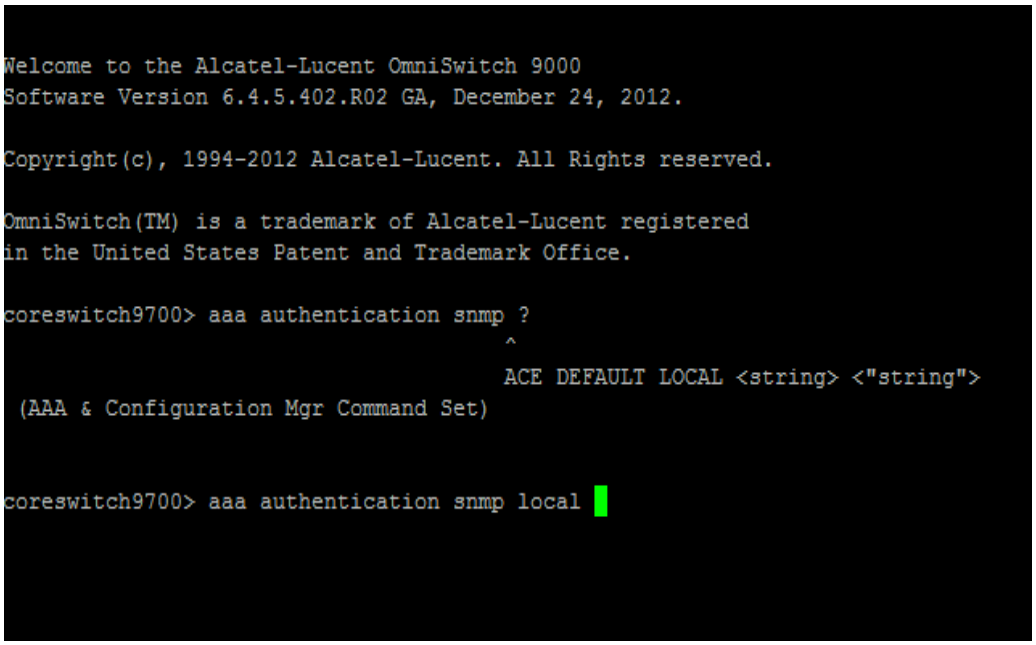
Switch> snmp community map “username” user “username” enable

Switch> snmp community map mode enable

Switch> snmp security no security

Switch> write memory

Switch> copy working certified



ภาพที่ 4-6 แสดงการคอนฟิก SNMP Service บน Alcatel switch

4.2.3 ขั้นตอนการติดตั้ง SNMP Service บนระบบปฏิบัติการ Ubuntu 14.04

☐ พิมพ์ชุดคำสั่ง ดังนี้

Cacti-server#sudo apt-get install snmpd

☐ ทำการสำรองไฟล์คอนฟิก ของ snmpd.conf ไว้เพื่อป้องกันความผิดพลาดในการแก้ไข

Cacti-server#sudo mv /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.ori

☐ **ทำการแก้ไขค่าไฟล์ snmpd.conf** ด้วยการเปิด Text Editor ขึ้นมาด้วยคำสั่ง

Cacti-server#sudo nano /etc/snmp/snmpd.conf

☐ ทำการแก้ไขไฟล์ snmpd.conf โดยปรับค่าคอนฟิกดังนี้

rocommunity public

syslocation “สถานที่ติดตั้งอุปกรณ์ (location)”

syscontact youremail@address.com

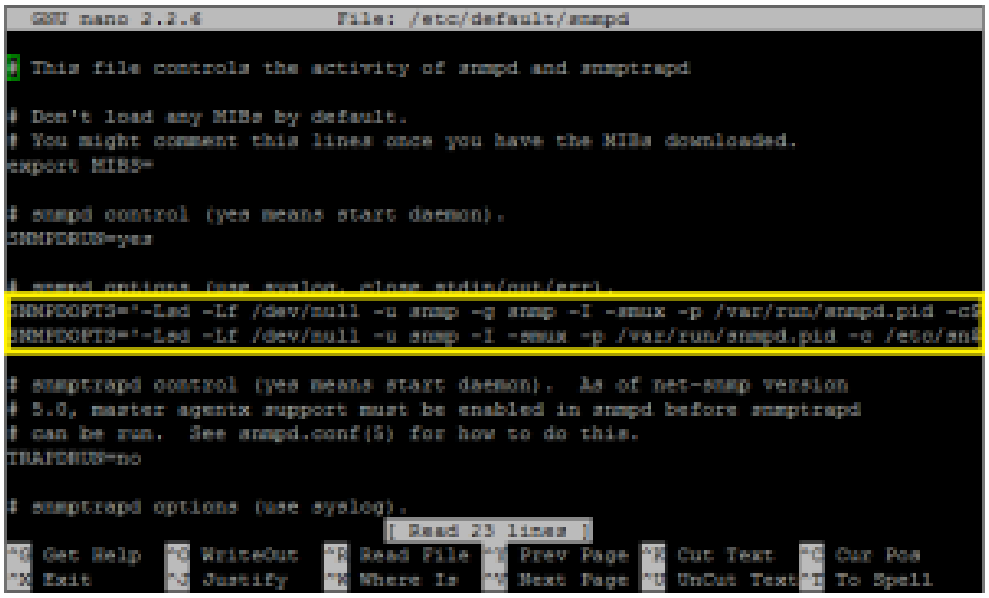
- **ทำการแก้ไขค่าไฟล์ snmpd.conf** ด้วยการเปิด Text Editor ขึ้นมาด้วยคำสั่ง

  Cacti-server#sudo nano /etc/snmp/snmpd.conf

- ทำการแก้ไขไฟล์ snmpd โดยปรับค่าคอนฟิกดังนี้

  SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -g snmp -I -smux -p /var/run/snmpd.pid -c /etc/snmp/snmpd.conf'

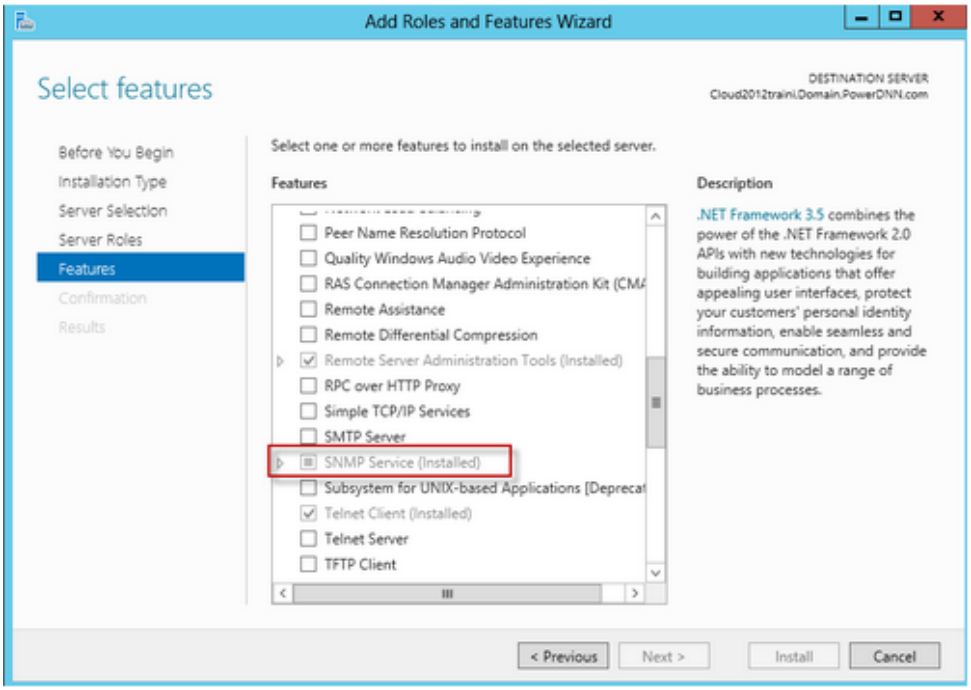
  SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid -c /etc/snmp/snmpd.confg'



ภาพที่ 4-7 แสดงการคอนฟิก SNMP Service บน Ubuntu Server

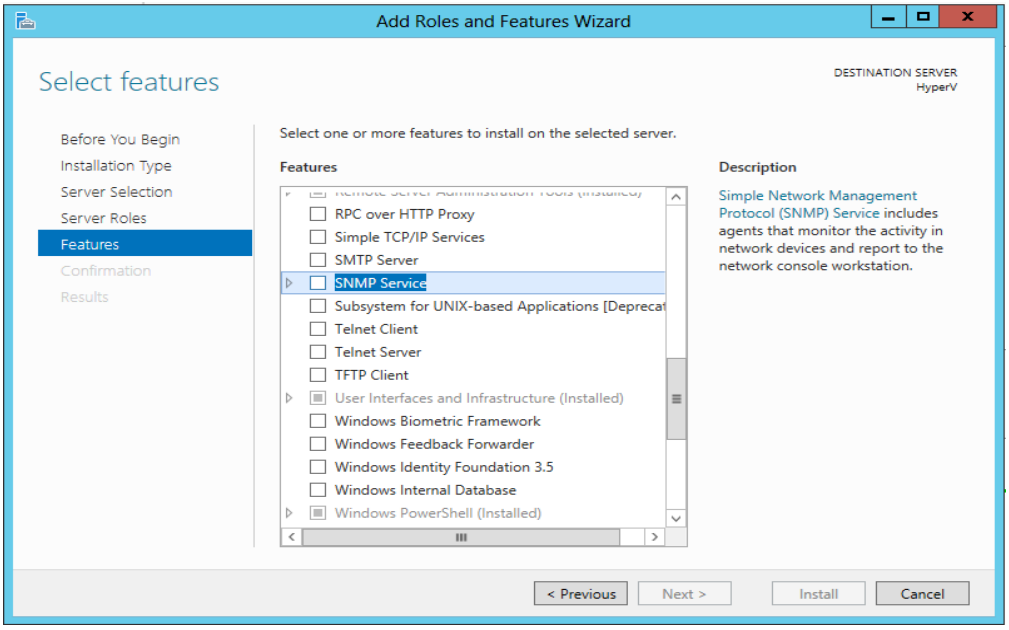
4.2.4 ขั้นตอนการเปิด SNMP บนเซิฟเวอร์ Windows server 2012

- เปิดเมนู Administrative Tools > Server Manager เลือกไปที่เมนู Manage เลือกที่ Add Roles and Features.



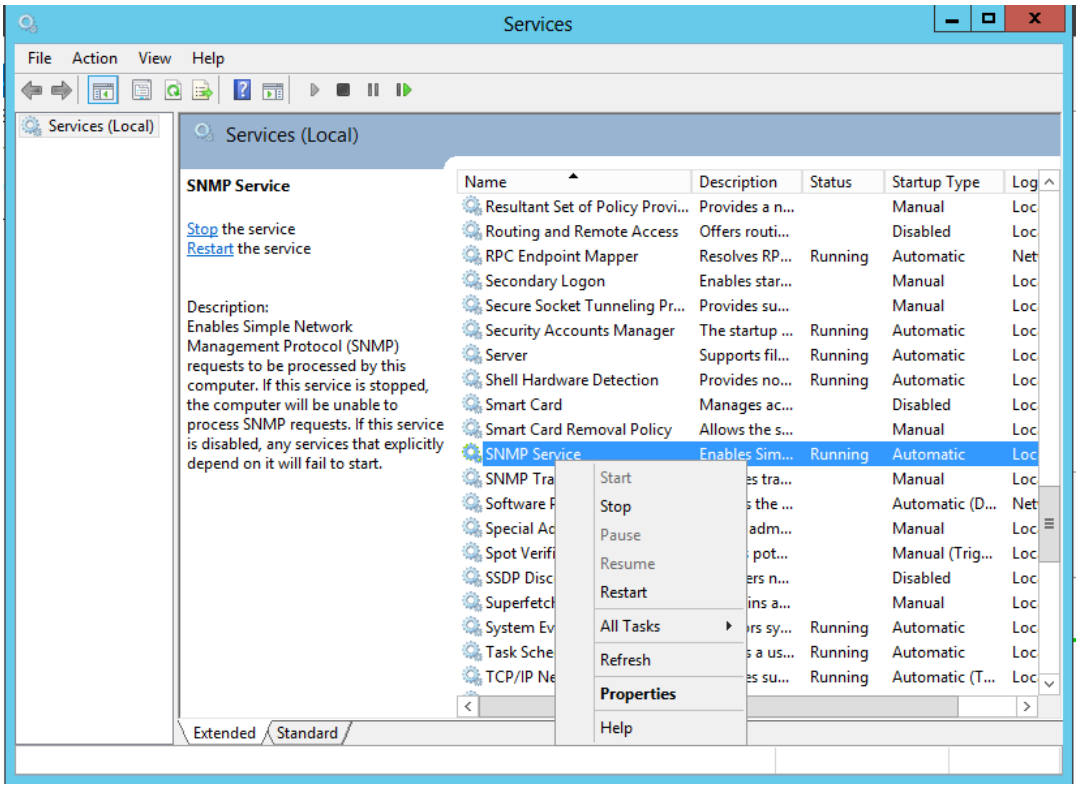
ภาพที่ 4-8 แสดงการเพิ่ม roles และ features บน Windows server 2012

☐ ในส่วนของ features ให้เลือกติดตั้ง SNMP Service จากนั้นกดปุ่ม Next จนจบขั้นตอน



ภาพที่ 4-9 แสดงการเพิ่ม features SNMP Service บน Windows server 2012

 จากนั้นทำการคอนฟิก SNMP Service โดยเข้าไปที่เมนู Administrative Tools >



Services ค้นหา คำว่า SNMP Service คลิ้กขวา เลือก Properties

ภาพที่ 4-10 แสดงการคอนฟิก SNMP Service บน Windows server 2012

บทที่ 5
ปัญหาอุปสรรคและข้อเสนอแนะ

ระบบตรวจสอบสถานะและปริมาณการใช้งานเครือข่าย มีการใช้งานมาระยะหนึ่งแล้วพบว่าทุกครั้งที่มีการนำอุปกรณ์ใหม่เข้ามาในระบบ อุปกรณ์รุ่นใหม่ ๆ บางครั้งระบบจึงยังไม่รองรับทำให้ต้องมีการพัฒนาบางฟังก์ชั่นการทำงานขึ้นมาใหม่ และยังไม่สามารถขยายการใช้งานให้ครอบคลุมอุปกรณ์ทั้งหมดได้

การใช้งานระบบตรวจสอบสถานะ และปริมาณการใช้งานเครือข่าย ยังพบว่ามีปัญหาซึ่งอาจเกิดจากผู้ปฏิบัติงานไม่รู้หรือไม่เข้าใจในระบบตรวจสอบสถานะ และปริมาณการใช้งานเครือข่ายดังกล่าว ผู้จัดทำคู่มือการปฏิบัติงานระบบตรวจสอบสถานะ และปริมาณการใช้งานเครือข่ายสำหรับผู้ใช้งาน จึงตระหนัก และคิดหาแนวทางแก้ไข และข้อเสนอแนะเพื่อพัฒนาระบบให้ตอบสนองต่อผู้ใช้งานและผู้ที่เกี่ยวข้อง โดยมีข้อสรุปดังนี้

5.1 ปัญหาและอุปสรรค

1. ระบบยังไม่สามารถรองรับอุปกรณ์รุ่นใหม่ได้ทุกรุ่น จึงทำให้ระบบไม่สามารถเก็บข้อมูลทั้งหมดมาใช้งานได้

2. เจ้าหน้าที่ผู้ปฏิบัติงานไม่มีความชำนาญในการใช้งานระบบตรวจสอบสถานะ และปริมาณการใช้งานเครือข่าย จึงทำให้ระบบไม่สามารถทำงานได้อย่างมีประสิทธิภาพ

3. เจ้าหน้าที่ไม่มีความเข้าใจในโครงสร้างระบบเครือข่ายของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร จึงทำให้ข้อมูลที่กรอกลงในระบบคลาดเคลื่อน

4. การทำงานบางส่วนระบบยังไม่สามารถทำงานโดยอัตโนมัติเองได้ จึงต้องมีการใช้เจ้าหน้าที่เพื่อดูแลและจัดการอยู่เสมอ

5. ไม่มีการกำหนดมาตรฐานในการกำหนดรายละเอียดของอุปกรณ์ที่จะใช้ระบุตัวตนของอุปกรณ์ในระบบตรวจสอบสถานะ และปริมาณการใช้งานเครือข่าย จึงทำให้รายชื่อของอุปกรณ์ที่ใช้ในระบบมีหลากหลายรุปแบบและเกิดความไม่ชัดเจน

5.2 แนวทางการแก้ไขปัญหา

1. ทำการปรับรุ่นของระบบให้ทันสมัยอยู่สม่ำเสมอ เพื่อให้ระบบสามารถรองรับอุปกรณ์รุ่นใหม่ได้

2. จัดประชุมเชิงปฏิบัติการเพื่อสอน และให้ความรู้แก่เจ้าหน้าที่ที่เกี่ยวข้อง รวมถึงมีการจัดทำศูนย์รวมความรู้เกี่ยวกับระบบตรวจสอบสถานะ และปริมาณการใช้งานเครือข่าย

3. จัดประชุมเพื่อแนะนำ และให้ความรู้เกี่ยวกับโครงสร้างระบบเครือข่ายของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนครอย่างสม่ำเสมอ และจัดทำศูนย์รวมความรู้เกี่ยวกับโครงสร้างระบบเครือข่ายของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

4. หาข้อมูล และความรู้เพื่อนำมาใช้ในการตั้งค่าระบบให้สามารถทำงานได้โดยอัตโนมัติเพื่อลดการทำงานโดยใช้เจ้าหน้าที่

5. จัดประชุมเพื่อกำหนดมาตรฐานชื่อของอุปกรณ์ที่จะใช้ระบุตัวตนของอุปกรณ์ในระบบตรวจสอบสถานะ และปริมาณการใช้งานเครือข่าย

6. จัดประชุมเพื่อกำหนดแผนการ และตารางเวลาสำหรับการดูแล และปรับปรุงระบบตรวจสอบสถานะและปริมาณการใช้งานเครือข่าย เพื่อระบบสามารถทำงานได้ต่อเนื่องและมีประสิทธิภาพ

5.3 ข้อเสนอแนะและการพัฒนา

1. ควรสนับสนุนให้มีการใช้สถิติต่าง ๆ จากระบบตรวจสอบสถานะและปริมาณการใช้งานเครือข่ายในการวิเคราะห์ และปรับปรุงระบบเครือข่ายคอมพิวเตอร์ และการสื่อสารของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

2. ควรมีการจัดประชุมเพื่อให้เจ้าหน้าที่ได้ตระหนักถึงความสำคัญของตรวจสอบสถานะ และปริมาณการใช้งานเครือข่าย และการวิเคราะห์ข้อมูลสถิติต่างของระบบ เช่น อัตราการทำงานและหยุดทำงานของอุปกรณ์ สถิติการใช้งานเครือข่าย

3. ปรับปรุง และจัดเก็บข้อมูลความรู้ต่าง ๆ เกี่ยวกับระบบตรวจสอบสถานะ และปริมาณการใช้งานเครือข่าย เช่นวิธีการติดตั้งระบบ วิธีการปรับปรุงการตั้งค่าต่าง ๆลฯ

4. ตรวจสอบ และปรับปรุงระบบตรวจสอบสถานะ และปริมาณการใช้งานเครือข่ายอย่างต่อเนื่องเพื่อให้การปฏิบัติงานสารบรรณมีประสิทธิภาพและทันสมัย

บรรณานุกรม

[1] พิชิต จินตโกศลวิทย์. *ทำความรู้จักกับโปรโตคอล SNMP*. 2011. Available at : http://www.thailandindustry.com/guru/view.php?id=14294&section=9 Accessed February 19, 2015.

[2] R. Presuhn. *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP).* 2002. Available at : https://tools.ietf.org/html/rfc3416 Accessed February 19, 2015

[3] J. Case. *A Simple Network Management Protocol (SNMP).* 1990. Available at : http://www.rfc-base.org/txt/rfc-1157.txt. Accessed February 19, 2015

[4] Keli. *Network Component Middleware for IP Networking.* 2012. Available at : http://www.keil.com/pack/doc/mw/network/html/using_snmp_agent.html Accessed February 25, 2015

[5] Ri. Xu. *Install the Cacti Server Monitor on Ubuntu Server.* 2013. Available at : https://xuri.me/2013/10/20/install-the-cacti-server-monitor-on-ubuntu-server.html Accessed February 25, 2015

[6] S. Dinesh. *An Introduction to Routers.* 2014. Available at : http://www.ebrahma.com/2014/08/an-introduction-to-routers Accessed February 25, 2015

[7] T. Urban. 2011. *Cacti 0.8 design a robust network operation center.* Birmingham: Packt Publishing.