คู่มือดูแลระบบเครือข่ายเบื้องต้น

นางสาวกสิมา คิ้วเจริญ

สำนักเทคโนโลยีสารสนเทศ

สถาบันบัณฑิตพัฒนบริหารศาสตร์

คำนำ

การจัดทำคู่มือการดูแลระบบเครือข่ายคอมพิวเตอร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์ มีวัตถุประสงค์เพื่อเป็นคู่มือให้ผู้ดูแลและปฏิบัติงานเกี่ยวกับระบบเครือข่ายคอมพิวเตอร์ ทราบขั้นตอน วิธีปฏิบัติ ที่ถูกต้อง รวมทั้งเพื่อใช้เป็นแนวทางในการศึกษาสำหรับเจ้าหน้าที่ที่ต้องปฏิบัติหน้าที่ในการให้บริการและแก้ไขปัญหาในการดูแลระบบเครือข่าย สำหรับข้อมูลการจัดทำคู่มืออ้างอิงจากโครงสร้างพื้นฐานและระบบเครือข่ายที่มีการติดตั้งใช้งานอยู่ในปัจจุบัน โดยอาศัยประสบการณ์ในการดำเนินงานที่ผ่านมา ซึ่งในคู่มือได้จัดทำผังเครือข่ายของอาคารต่าง ๆ และอธิบายโครงสร้างพื้นฐานระบบเครือข่ายของสถาบัน การดูผังเครือข่ายสำหรับผู้ที่ดูแลระบบจะมีความสะดวกและตีความได้รวดเร็วและเข้าใจความหมายได้ง่ายขึ้น เมื่ออ่านคำอธิบายประกอบเพื่อให้ทุกฝ่ายที่เกี่ยวข้องรับทราบโครงสร้างระบบเครือข่าย อีกทั้งผู้จัดทำได้รวบรวมปัญหาพร้อมข้อเสนอแนะไว้ด้วย

ผู้จัดทำจึงหวังเป็นอย่างยิ่งว่า คู่มือฉบับนี้จะมีประโยชน์แก่ผู้ปฏิบัติงานในการให้บริการและแก้ไขปัญหาระบบเครือข่ายของสถาบัน และผู้ที่เกี่ยวข้องนำไปใช้ประโยชน์ เพื่อช่วยในการปฏิบัติงานได้อย่างถูกต้องและมีประสิทธิภาพ ซึ่งหากคู่มือฉบับนี้มีข้อผิดพลาดประการใด ผู้จัดทำขอน้อมรับข้อผิดพลาดดังกล่าวเพื่อนำมาปรับปรุง พัฒนาคู่มือให้มีความครบถ้วนสมบูรณ์ต่อไป

กสิมา คิ้วเจริญ

ตุลาคม 2558

สารบัญ

สารบัญภาพ

สารบัญตาราง

บทที่ 1
บทนำ

1. ความเป็นมาและความสำคัญ

ปัจจุบันเทคโนโลยีสารสนเทศได้เข้ามามีบทบาทในสังคมเป็นอย่างมากทั้งด้านการดำเนินชีวิตประจำวัน ด้านธุรกิจ ด้านสังคม โดยเฉพาะอย่างยิ่งด้านการศึกษา สถาบันการศึกษาทั่วโลกได้ให้ความสำคัญกับการพัฒนาเทคโนโลยีสารสนเทศให้แก่บัณฑิต เพื่อให้สามารถแข่งขันในเวทีระดับชาติ และเวทีโลกได้ ประกอบกับทุกสถาบันมีการนำเทคโนโลยีสารสนเทศเข้ามาช่วยในการบริหารงาน และพัฒนาการเรียนการสอน เพื่อให้มีความทันสมัย ดึงดูดนิสิตนักศึกษาให้เข้ามาศึกษาต่อกับสถาบันของตนรวมทั้งเพิ่มศักยภาพให้นักศึกษาสำเร็จการศึกษาเป็นมหาบัณฑิตที่มีความสามารถ และแข่งขันในตลาดแรงงานและเวทีโลกได้

ระบบเครือข่ายอินเทอร์เน็ตจึงเป็นกลไกสำคัญในการช่วยสนับสนุนด้านการค้นคว้าข้อมูล และเชื่อมโยงระบบสารสนเทศต่าง ๆ ที่ผ่านมาสถาบันมีการก่อสร้างอาคารขึ้นใหม่หลายอาคาร มีการเปลี่ยนชื่ออาคาร ปรับปรุงระบบเครือข่ายและสายสัญญาณอยู่หลายครั้ง ทำให้เอกสารที่มีอยู่ไม่เป็นปัจจุบันและกระจัดกระจาย ประกอบกับยังไม่มีผังเครือข่ายประจำแต่ละอาคาร ผู้จัดทำเห็นควรจะรวบรวมความรู้ ผังเครือข่ายและสายสัญญาณมาไว้รวมกันและจัดทำให้เป็นปัจจุบัน จะทำให้สามารถนำมาใช้แก้ไขปัญหาได้รวดเร็วมีประสิทธิภาพ ทำให้การดำเนินงานมีมาตรฐานเพิ่มขึ้น เพื่อเป็นประโยชน์ให้กับผู้ที่มาช่วยดูแลระบบเครือข่ายเพิ่มเติมในอนาคต

2. วัตถุประสงค์ของการจัดทำคู่มือ

2.1. เพื่อให้ผู้ดูแลและปฏิบัติงานที่เกี่ยวข้องกับระบบเครือข่ายสามารถทำงานแทนกันได้

2.2. เพื่อให้ผู้ดูแลและปฏิบัติงานที่เกี่ยวข้องกับระบบเครือข่ายสามารถแก้ไขปัญหาได้อย่างรวดเร็ว

2.3. เพื่อช่วยสร้างความเข้าใจที่ชัดเจน และระบุรายละเอียดงานระบบเครือข่ายได้ครบถ้วนและลดระยะเวลาในการถ่ายทอดงาน

2.4. เพื่อใช้เป็นเอกสารอ้างอิงในการทำงาน

3. ขอบเขต

คู่มือการดูแลระบบเครือข่ายฉบับนี้ครอบคลุม โครงสร้างระบบเครือข่ายของสถาบันทุกอาคาร จะไม่ระบุไอพีแอดเดรสของอุปกรณ์ตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ แนวการเดินสายไฟเบอร์ออฟติคลงดิน การจ่ายกระแสไฟฟ้าให้กับระบบเครือข่าย ขั้นตอนการแก้ปัญหา กลุ่มคำสั่งที่ใช้งานบ่อยของอุปกรณ์เครือข่ายที่ใช้งาน เครื่องมือที่ช่วยในการทำงานแก้ไขปัญหา การดำเนินการของสำนักเทคโนโลยี สถาบันบัณฑิตพัฒนบริหารศาสตร์

4. นิยามศัพท์เฉพาะ

สถาบัน หมายถึง สถาบันบัณฑิตพัฒนบริหารศาสตร์

สำนัก หมายถึง สำนักเทคโนโลยีสารสนเทศ

ห้องสมุด หมายถึง สำนักบรรณสารการพัฒนา

ผู้ใช้งาน หมายถึง นักศึกษาและบุคลากร

Data Center หมายถึง ศูนย์ข้อมูลหลักของสถาบัน

UniNet หมายถึง ย่อมาจาก Inter-University Network บริหารงานโดยสำนักงานบริหารเทคโนโลยีสารสนเทศ เพื่อพัฒนาการศึกษา

ระบบเครือข่ายไร้สายทรู หมายถึง ระบบเครือข่ายไร้สาย ที่เป็นโครงการร่วมระหว่างสถาบันกับบริษัท ทรู อินเทอร์เน็ต จำกัด

เราท์เตอร์ หมายถึง อุปกรณ์ค้นหาเส้นทางเครือข่าย

ไฟร์วอลล์ หมายถึง อุปกรณ์รักษาความปลอดภัยเครือข่าย

Core switch หมายถึง อุปกรณ์เครือข่ายหลัก

5. ประโยชน์ที่คาดว่าจะได้รับ

ช่วยเพิ่มประสิทธิภาพให้ผู้ปฏิบัติงานที่เกี่ยวข้องกับการดูแลระบบเครือข่ายคอมพิวเตอร์ เห็นภาพรวมของโครงสร้างพื้นฐานเครือข่ายคอมพิวเตอร์ของสถาบัน ทราบขั้นตอน วิธีการปฏิบัติงานและการแก้ปัญหา ใช้เป็นเอกสารอ้างอิงให้ผู้บริหาร ผู้ประสานงานฝ่ายต่าง ๆ และนักวิชาคอมพิวเตอร์ฝ่ายต่าง ๆ รวมไปถึงสามารถใช้คู่มือเพื่อเป็นแนวทางในการศึกษาสำหรับนักวิชาคอมพิวเตอร์ที่ได้รับมอบหมายภาระงานใหม่ด้านเครือข่ายคอมพิวเตอร์

บทที่ 2
บทบาท โครงสร้างและหน้าที่ความรับผิดชอบ

ข้อมูลของสำนักเทคโนโลยีสารสนเทศ

ประวัติ

สำนักเทคโนโลยีสารสนเทศ เดิมชื่อ “ศูนย์การศึกษาระบบสารสนเทศ” ก่อตั้งขึ้นเมื่อวันที่ 27 กรกฎาคม พ.ศ.2527 โดยความร่วมมือของสถาบันบัณฑิตพัฒนบริหารศาสตร์ กับ บริษัท ไอบีเอ็ม ประเทศไทย จำกัด โดยมีวัตถุประสงค์เพื่อพัฒนาบุคลากรทางคอมพิวเตอร์ทั้งในภาครัฐและภาคเอกชน

ปี พ.ศ.2532 ได้ยกฐานะขึ้นเป็นสำนักการศึกษาระบบสารสนเทศ

ปีพ.ศ.2535 สถาบันได้มอบหมายให้สำนักเปิดสอนวิชา สศ.400 ความรู้เบื้องต้นทางคอมพิวเตอร์แก่นักศึกษาทุกคณะของสถาบัน เพื่อเป็นการเพิ่มศักยภาพทางคอมพิวเตอร์ให้แก่นักศึกษา จึงทำให้สำนักมีภาระงานด้านการสอนนักศึกษาเพิ่มขึ้น และได้ดำเนินการต่อเนื่องมาจนถึงภาค 2 ปีการศึกษา 2550

ปี พ.ศ. 2541 สำนักได้รับอนุมัติให้เปิดสอนหลักสูตร “ประกาศนียบัตรบัณฑิต สาขาการพัฒนาระบบสารสนเทศ” โดยมีวัตถุประสงค์หลักเพื่อผลิตบุคลากรที่ทำหน้าที่พัฒนาระบบงานเพื่อการใช้งานในการประกอบการขององค์กรทั้งในภาคธุรกิจเอกชน รัฐวิสาหกิจ และหน่วยงานของรัฐ และเพื่อสนองตอบต่อความต้องการบุคลากรด้านเทคโนโลยีสารสนเทศของประเทศ

ปี พ.ศ.2546 สำนักการศึกษาระบบสารสนเทศโดยความร่วมมือกับคณะบริหารธุรกิจ ได้รับอนุมัติให้เปิดสอนหลักสูตร “วิทยาศาสตรมหาบัณฑิต สาขาบริหารเทคโนโลยีสารสนเทศ” เพื่อบูรณาการศาสตร์ด้านการบริหารจัดการธุรกิจ และศาสตร์ด้านเทคโนโลยีสารสนเทศเข้าด้วยกัน ทั้งนี้เพื่อปรับการศึกษาให้สอดรับกับแนวคิดใหม่ ๆ ทางเทคโนโลยีที่เกิดขึ้น และสนองความต้องการการใช้งานเทคโนโลยีขององค์กรและประเทศ

ปี พ.ศ.2547 สถาบันได้มีคำสั่งที่ 754/2547 ลงวันที่ 1 พฤศจิกายน 2547 ให้โอนภาระงานในความรับผิดชอบของศูนย์เทคโนโลยี งานโสตทัศนศึกษาของกองบริการการศึกษา และศูนย์สารสนเทศเพื่อการบริหาร มาอยู่ในความรับผิดชอบของสำนัก เพื่อให้การดำเนินงานด้านเทคโนโลยีของสถาบันมีความเป็นเอกภาพ โดยมอบหมายให้สำนักดูแลงานด้านเทคโนโลยีสารสนเทศของสถาบัน

ปีการศึกษา 2549 ภาคการศึกษาที่ 2 สำนักได้หยุดรับนักศึกษาหลักสูตร “วิทยาศาสตรมหาบัณฑิต สาขาบริหารเทคโนโลยีสารสนเทศ” และมีนักศึกษาที่ยังคงศึกษาอยู่ในหลักสูตรจนกระทั่งปีการศึกษา 2552 สำนักจึงได้ยกเลิกภาระงานด้านการเรียนการสอน โดยมีผู้สำเร็จการศึกษาไปแล้วจำนวน 7 รุ่น รวมทั้งสิ้น 56 คน

ปี พ.ศ.2551 สถาบันได้ย้ายหน่วยเสียงและอิเล็กทรอนิกส์ และหน่วยภาพนิ่งและโทรทัศน์ ไปสังกัดกลุ่มงานโสตทัศนูปกรณ์ กองกลาง สำนักงานอธิการบดี

ปี พ.ศ.2555 สำนักการศึกษาระบบสารสนเทศได้เปลี่ยนชื่อเป็น “สำนักเทคโนโลยีสารสนเทศ” ตั้งแต่วันที่ 21 เมษายน 2555 ตามพระราชกฤษฎีกาจัดตั้งส่วนราชการในสถาบันบัณฑิตพัฒนบริหารศาสตร์ กระทรวงศึกษาธิการ พ.ศ.2555

ปรัชญาและปณิธาน วิสัยทัศน์ พันธกิจ ค่านิยมร่วม

ปรัชญาและปณิธาน : สำนักเทคโนโลยีสารสนเทศมีจุดมุ่งหมายในการให้บริการเทคโนโลยีสารสนเทศเพื่อสนับสนุนสถาบันในการดำเนินการตามพันธกิจ อย่างราบรื่นและมีประสิทธิภาพ

วิสัยทัศน์ (VISION) : เป็นหน่วยงานให้บริการเทคโนโลยีสารสนเทศที่มีคุณภาพระดับสากล

พันธกิจ (MISSION) :

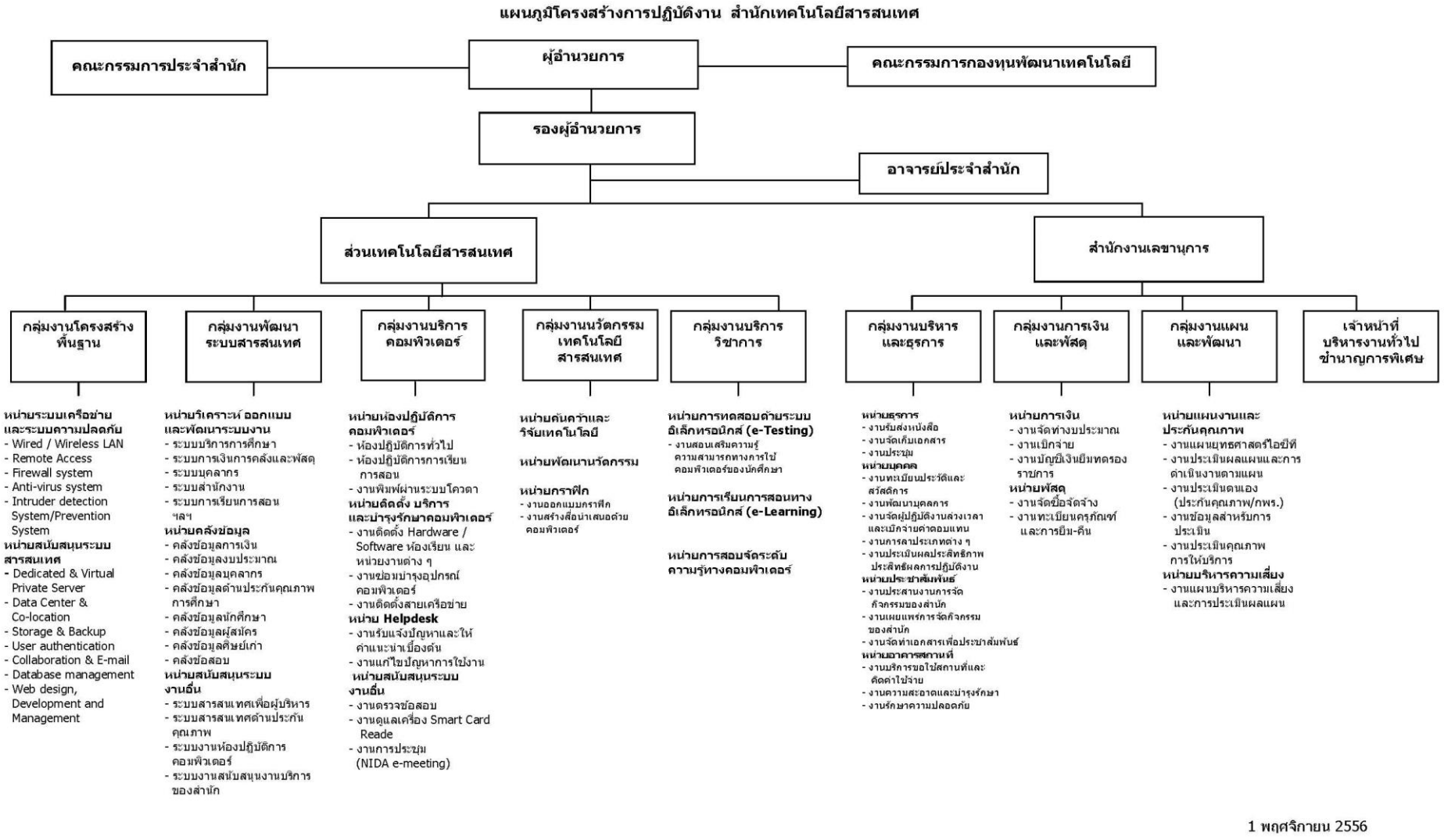
1. ให้บริการเทคโนโลยีสารสนเทศแก่อาจารย์ นักศึกษา และบุคลากรภายในสถาบัน เพื่อให้การดำเนินพันธกิจของสถาบันเป็นไปอย่างราบรื่น และมีประสิทธิภาพ
2. พัฒนาระบบสารสนเทศเพื่อสนับสนุนการดำเนินงานของสถาบันด้านการเรียนการสอน และการบริหารจัดการ ให้เหมาะสมและทันต่อการเปลี่ยนแปลงของสภาวการณ์
3. พัฒนาศักยภาพทางคอมพิวเตอร์ให้แก่นักศึกษาระดับปริญญาโท และปริญญาเอกของสถาบันด้านความสามารถในการใช้คอมพิวเตอร์ และโปรแกรมใช้งานที่เกี่ยวข้อง
4. จัดฝึกอบรมด้านคอมพิวเตอร์ และเทคโนโลยีสารสนเทศให้กับบุคลากรของสถาบัน ตั้งแต่ระดับผู้ใช้งานจนถึงระดับผู้บริหาร
5. ให้บริการวิชาการทางคอมพิวเตอร์ และเทคโนโลยีสารสนเทศแก่หน่วยงานภายนอก อาทิ การศึกษาวิเคราะห์ และจัดวางระบบงาน การวางแผนด้านระบบสารสนเทศ เป็นต้น
6. สนับสนุนพันธกิจด้านการทำนุบำรุงศิลปวัฒนธรรมของสถาบันในเชิงบูรณาการ

ค่านิยมร่วม : มุ่งเน้นประสิทธิภาพการให้บริการ 5ด้าน (5S)

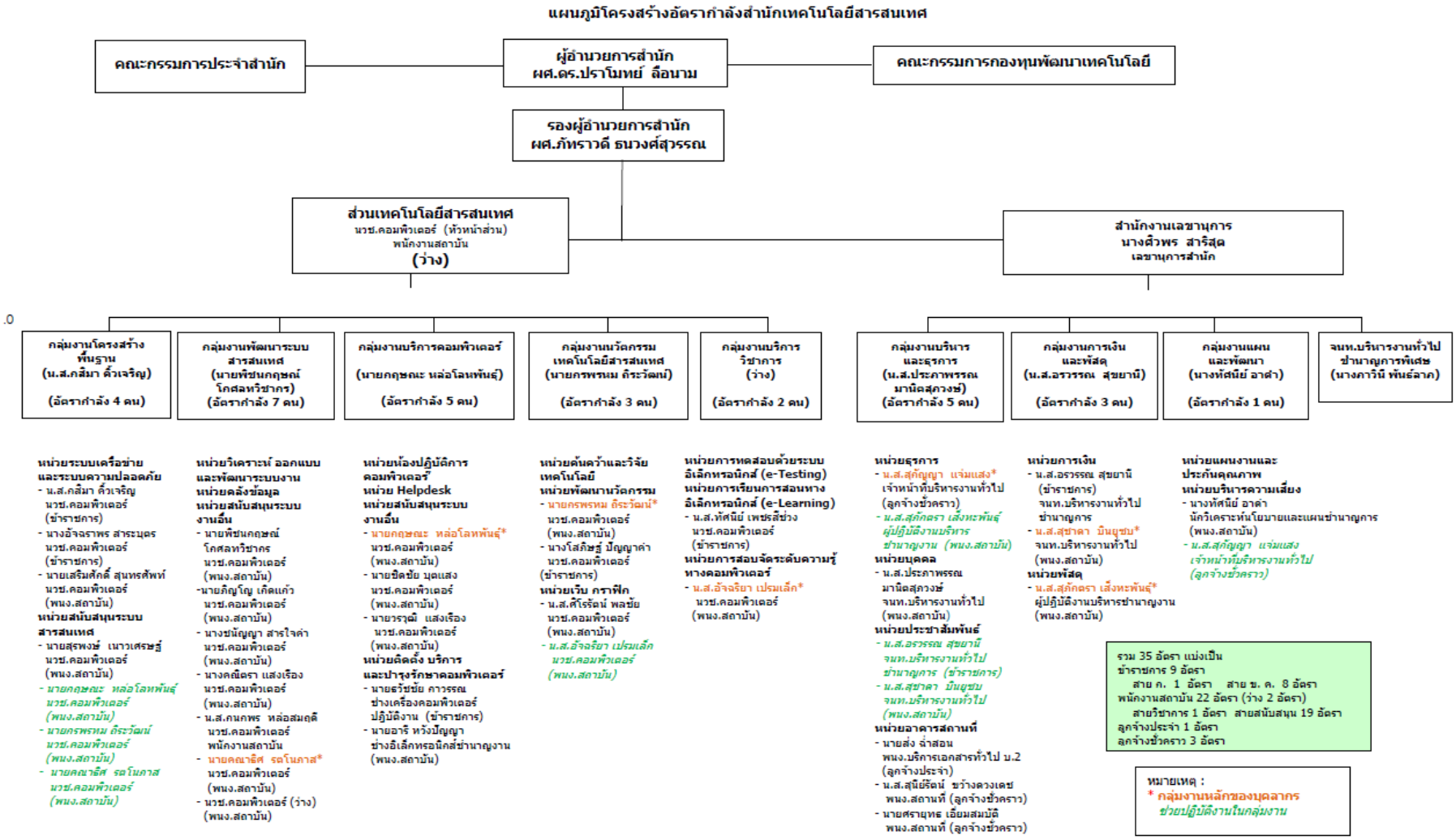
Service-mindedness	หมายถึง การบริการด้วยใจ
Smartness	หมายถึง การปฏิบัติงานที่ถูกต้อง และมีความรู้จริง
Smoothness	หมายถึง ความราบรื่น ไม่ติดขัดในการดำเนินงาน
Securement	หมายถึง ความมั่นคงปลอดภัย
Speediness	หมายถึง ความรวดเร็วทันต่อความต้องการใช้งาน

โครงสร้างองค์กร และโครงสร้างการบริหาร

ตามแผนภูมิที่ 1 การจัดแบ่งหน่วยงานสำนักเทคโนโลยีสารสนเทศ ดังต่อไปนี้



ภาพที่ 2-1 แสดงแผนภูมิโครงสร้างของสำนักเทคโนโลยี



ภาพที่ 2-2 แสดงแผนภูมิอัตรากำลังของสำนักเทคโนโลยี

การบริหารงานภายในสำนัก

สำนักเทคโนโลยีสารสนเทศมีโครงสร้างการบริหารงานภายใน ประกอบด้วย

คณะกรรมการประจำสำนัก ประกอบด้วย ผู้อำนวยการสำนัก เป็นประธานคณะกรรมการ รองผู้อำนวยการสำนัก อาจารย์ประจำสำนักและอาจารย์จากหน่วยงานภายในสถาบัน

คณะกรรมการบริหารเงินกองทุนสำนัก ประกอบด้วย รองอธิการบดีฝ่ายวางแผน เป็นประธาน ผู้อำนวยการสำนัก รองผู้อำนวยการสำนัก อาจารย์ประจำสำนัก และเลขานุการสำนัก เป็นกรรมการและเลขานุการ

คณะกรรมการกองทุนพัฒนาเทคโนโลยี ประกอบด้วย รองอธิการบดีฝ่ายวางแผน เป็นประธาน รองอธิการบดีฝ่ายบริหาร รองอธิการบดีฝ่ายวิชาการ คณบดีหรือผู้อำนวยการสำนักหน่วยงานภายในสถาบัน อาจารย์จากหน่วยงานภายในสถาบัน ผู้อำนวยการสำนัก เป็นกรรมการและเลขานุการ และรองผู้อำนวยการสำนัก เป็นกรรมการและผู้ช่วยเลขานุการ

การกำกับตรวจสอบ

การดำเนินงานในกิจการต่าง ๆ ของสำนักเทคโนโลยีสารสนเทศอยู่ภายใต้การกำกับตรวจสอบของคณะกรรมการประจำสำนัก และกิจการต่าง ๆ ที่ใช้งบกองทุนพัฒนาเทคโนโลยี อยู่ภายใต้การกำกับตรวจสอบของคณะกรรมการกองทุนพัฒนาเทคโนโลยี

ขอบเขตและภาระงาน

สำนักเทคโนโลยีสารสนเทศ จัดแบ่งโครงสร้างออกเป็นดังนี้

1. ส่วนเทคโนโลยีสารสนเทศ เป็นฝ่ายที่ปฏิบัติงานด้านการดำเนินงานเกี่ยวกับเทคโนโลยีสารสนเทศของสถาบัน ดูแล พัฒนาและบำรุงรักษาระบบงานเทคโนโลยีสารสนเทศแก่หน่วยงาน โดยแบ่งตามลักษณะงานเป็น 5 กลุ่มงาน ดังนี้ กลุ่มงานโครงสร้างพื้นฐาน กลุ่มงานพัฒนาระบบสารสนเทศ กลุ่มงานบริการคอมพิวเตอร์ กลุ่มงานนวัตกรรมเทคโนโลยี กลุ่มงานบริการวิชาการ

2. สำนักงานเลขานุการ เป็นฝ่ายที่ปฏิบัติงานสนับสนุนสายงานบริการเทคโนโลยีสารสนเทศ โดยแบ่งเป็น 3 กลุ่มงาน ดังนี้ กลุ่มงานบริหารและธุรการ กลุ่มงานการเงินและพัสดุ กลุ่มงานวางแผนและพัฒนา

หน้าที่ความรับผิดชอบ

ปฏิบัติงานในตำแหน่งหัวหน้ากลุ่มงานโครงสร้างพื้นฐาน ทำหน้าที่ต่างๆ ดังนี้

ด้านงานบริหาร และการวางแผน

- ช่วยศึกษารายละเอียดในการจัดทำแผนงาน/โครงการของสำนัก
- ศึกษาพัฒนาและติดตามความก้าวหน้าของเทคโนโลยีสารสนเทศ เพื่อสนับสนุนภารกิจของสถาบัน
- วางแผนด้านเทคโนโลยีสารสนเทศ เพื่อสนองความต้องการอย่างมีระบบ
- ดูแล และควบคุมระบบโครงสร้างพื้นฐานด้านคอมพิวเตอร์ของสถาบัน

- ดูแล รักษาและซ่อมบำรุงอุปกรณ์ที่เกี่ยวกับเทคโนโลยีสารสนเทศ
- วางแผนการดำเนินงานด้านโครงสร้างพื้นฐานและด้านอื่นๆ ของสำนักและของกลุ่มงาน
- ร่วมจัดทำแผนปฏิบัติราชการ 4 ปี แผนปฏิบัติราชการประจำปีของสำนัก
- จัดทำแผนการจัดซื้อจัดจ้างและการตรวจรับครุภัณฑ์/โครงการต่าง ๆ ของสำนัก
- ร่วมจัดทำนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยด้านสารสนเทศ
- ร่วมจัดทำแผนบริหารความเสี่ยงและบริหารความต่อเนื่อง
- เป็นกรรมการประกันคุณภาพของสำนัก
- เข้าร่วมประชุมคณะกรรมการต่าง ๆ ที่ได้รับแต่งตั้ง เพื่อให้ข้อมูลทางวิชาการประกอบการพิจารณาและตัดสินใจ และปฏิบัติหน้าที่อื่นที่เกี่ยวข้อง
- งานกำกับดูแลและบริหารโครงการต่าง ๆ ของกลุ่ม และโครงการที่ได้รับมอบหมาย
- งานกำกับดูแลและให้บริการศูนย์ข้อมูลหลัก (Data Center)
- งานกำกับดูแลและให้บริการระบบเครือข่ายแลน
- งานกำกับดูแลและให้บริการระบบเครือข่ายไร้สาย
- งานกำกับดูแลและให้บริการเครื่องแม่ข่าย
- ถ่ายทอดความรู้ด้านเทคโนโลยีสารสนเทศและด้านอื่นๆ แก่ผู้ใต้บังคับบัญชา

ภารกิจงานประจำ ด้านการปฏิบัติการ

- ดูแล ปรับปรุง แก้ไข ระบบเครือข่ายแลนให้รองรับการใช้งานระบบเครือข่ายที่มากขึ้น และอยู่ในสภาพที่พร้อมใช้งานตลอดเวลา
- ดูแล ปรับปรุง แก้ไข ระบบเครือข่ายไร้สายให้รองรับการใช้งานระบบเครือข่ายที่มากขึ้น และอยู่ในสภาพที่พร้อมใช้งานตลอดเวลา
- ตรวจสอบและเฝ้าระวังการทำงานของอุปกรณ์เครือข่าย
- ติดตั้งและขยายการให้บริการเครือข่าย
- ให้คำปรึกษาด้านเครือข่าย
- ดูแลเครื่องแม่ข่ายและระบบรักษาความปลอดภัยเครือข่าย
- บริหารจัดการรหัสผู้ใช้จดหมายอิเล็กทรอนิกส์
- กำหนดสิทธิ์ในการเข้าถึงไฟล์ในระบบการติดต่อสื่อสารภายในสถาบัน

งานด้านการประสานงาน และด้านบริการ

- ประสานงานการทำงานร่วมกันภายในสำนักเทคโนโลยีสารสนเทศ เพื่อให้เกิดความร่วมมือและผลสัมฤทธิ์ตามเป้าหมายที่กำหนดไว้ เช่น ประสานงานกับหัวหน้ากลุ่มงานต่างๆ ในการจัดทำโครงการของกลุ่มงานโครงสร้างพื้นฐาน เป็นต้น
- ชี้แจงและให้รายละเอียดเกี่ยวกับข้อมูล ข้อเท็จจริง แก่บุคลากรหรือหน่วยงานที่เกี่ยวข้อง เพื่อสร้างความเข้าใจหรือความร่วมมือในข้อกำหนดการใช้งานชุดคำสั่งสำเร็จรูป เช่น แจ้งผู้ใช้งานระบบการติดต่อสื่อสารภายในสถาบัน เกี่ยวกับสิทธิ์การเข้าถึงเอกสารภายในของสถาบัน
- เป็นผู้ประสานงานกับหน่วยงานภายในสถาบันในการขอใช้บริการเครือข่ายและเครื่องแม่ข่าย
- เป็นผู้ประสานงานกับผู้ให้บริการเอกชนในการติดตั้งระบบเครือข่ายไร้สายให้กับสถาบัน

- เป็นผู้ประสานงานกับสำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษาในการเชื่อมต่อโครงการพัฒนาเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา (UniNet)
- ประสานงานการทำงานร่วมกับหน่วยงานภายในสถาบัน ด้านระบบเครือข่าย
- ประสานงานการทำงานร่วมกับหน่วยงานต่างๆ ภายในสถาบัน ด้านการให้บริการ Data Center
- ประสานงานด้านนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลกับกระทรวงไอซีที และหน่วยงานต่างๆ ภายในสถาบัน
- ให้คำปรึกษา แนะนำเบื้องต้น เผยแพร่ถ่ายทอดความรู้ จัดทำคู่มือ รวมทั้งตอบปัญหาและชี้แจงเกี่ยวกับระบบเครือข่าย ระบบเครือข่ายไร้สาย ระบบอื่นๆ ของกลุ่มงาน

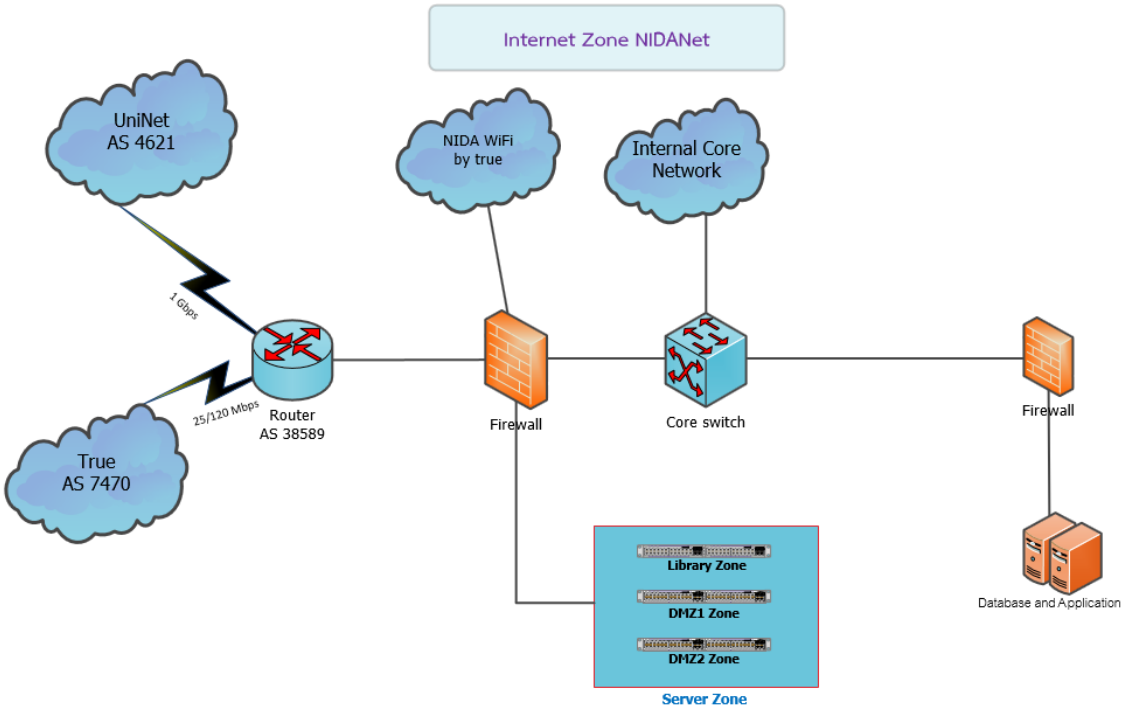
งานด้านอื่น ๆ

- เป็นกรรมการจัดซื้อจัดจ้างวัสดุและครุภัณฑ์คอมพิวเตอร์ ของหน่วยงานต่าง ๆ ของสถาบัน ที่ขอความร่วมมือ เช่น ระบบ Digital Signage, ระบบจอ LED ประชาสัมพันธ์, tablet ของคณะบริหารธุรกิจ เป็นต้น
- ให้ความช่วยเหลือและเชื่อมต่อเครือข่ายให้กับโครงการติดตั้ง IPPhone อาคารนวมินทราธิราชกับกลุ่มงานโยธาและซ่อมบำรุง
- ให้ความช่วยเหลือและเชื่อมต่อเครือข่ายให้กับโครงการติดตั้ง CCTV ของกลุ่มงานโยธาและซ่อมบำรุง
- ออกแบบและติดตั้งระบบเครือข่ายเพื่อรองรับการให้บริการรูปแบบต่างๆ ให้กับห้องสมุดอาเซียน
- ให้คำปรึกษาละช่วยตรวจสอบงานติดตั้งระบบเครือข่าย สำนักงานใหม่กลุ่มงานสื่อสารองค์การและกิจกรรมเพื่อสังคม อาคารนวมินทราธิราช ชั้น 1
- ให้คำปรึกษาละช่วยตรวจสอบงานติดตั้งระบบเครือข่าย สหกรณ์ออมทรัพย์ของสถาบัน อาคารนวมินทราธิราช ชั้น 1
- ปฏิบัติงานตามที่ผู้บังคับบัญชามอบหมาย

บทที่ 3
ภาพรวมระบบเครือข่าย

องค์ประกอบที่สำคัญอย่างหนึ่งของระบบเครือข่ายคือสายสัญญาณ เพื่อให้เห็นภาพรวมทั้งหมด และเข้าใจได้ง่าย จึงจัดทำเป็นแผนผังเครือข่ายอินเทอร์เน็ต แผนผังเครือข่ายหลักของสถาบัน และแผนผังระบบเครือข่ายของแต่ละอาคารพร้อมคำอธิบายโครงสร้างเครือข่ายภายในอาคารการเชื่อมต่อระหว่างอาคาร การแบ่ง vlan ตำแหน่งของห้องเครือข่ายหลักและเครือข่ายย่อย การเข้าถึงสถานที่ เพื่อให้ผู้ดูแลระบบเครือข่ายท่านอื่น ๆ หรือผู้ที่เกี่ยวข้อง สามารถนำไปใช้งานได้

ระบบเครือข่ายอินเทอร์เน็ต



ภาพที่ 3-1 ผังเครือข่ายอินเทอร์เน็ตของสถาบัน

ภาพที่ 3-1 ผังเครือข่ายอินเทอร์เน็ตของสถาบัน มีการเชื่อมต่ออินเทอร์เน็ต 2 เส้นทาง เป็นวงจรความเร็วสูง แบบ Leased Line เส้นทางหลักเชื่อมกับ UniNet ความเร็ว 1 Gbps และเส้นทางสำรองความเร็ว 25/250 Mbps (ความเร็วต่างประเทศไม่น้อยกว่า 25 Mbps และความเร็วภายในประเทศไม่น้อยกว่า 120 Mbps) ซึ่งปัจจุบันสถาบันเช่าใช้เส้นทางของบริษัท ทรู อินเทอร์เน็ต จำกัด วงจรอินเทอร์เน็ตทั้งสองวงจรต่อเข้ากับอุปกรณ์หาเส้นทางเราท์เตอร์ (Router) ของสถาบันและทำการตั้งค่าเราท์เตอร์ โดยใช้ BGP ซึ่งเป็นโปรโตคอลที่ทำให้วงจรอินเทอร์เน็ตทั้งสองสามารถทำงานทดแทนกันได้โดยอัตโนมัติ ในกรณีที่วงจรใดวงจรหนึ่งเสียหาย โดยจะต้องรู้ AS Bumber ของแต่ละวงจร เพื่อทำการตรวจสอบเส้นทางในการใช้งานอินเทอร์เน็ต

เราท์เตอร์เชื่อมต่อกับไฟร์วอลล์ ซึ่งไฟร์วอลล์เสมือนเป็นประตูที่เชื่อมตอไปยังโซนต่าง ๆ ของระบบเครือข่าย ได้แก่

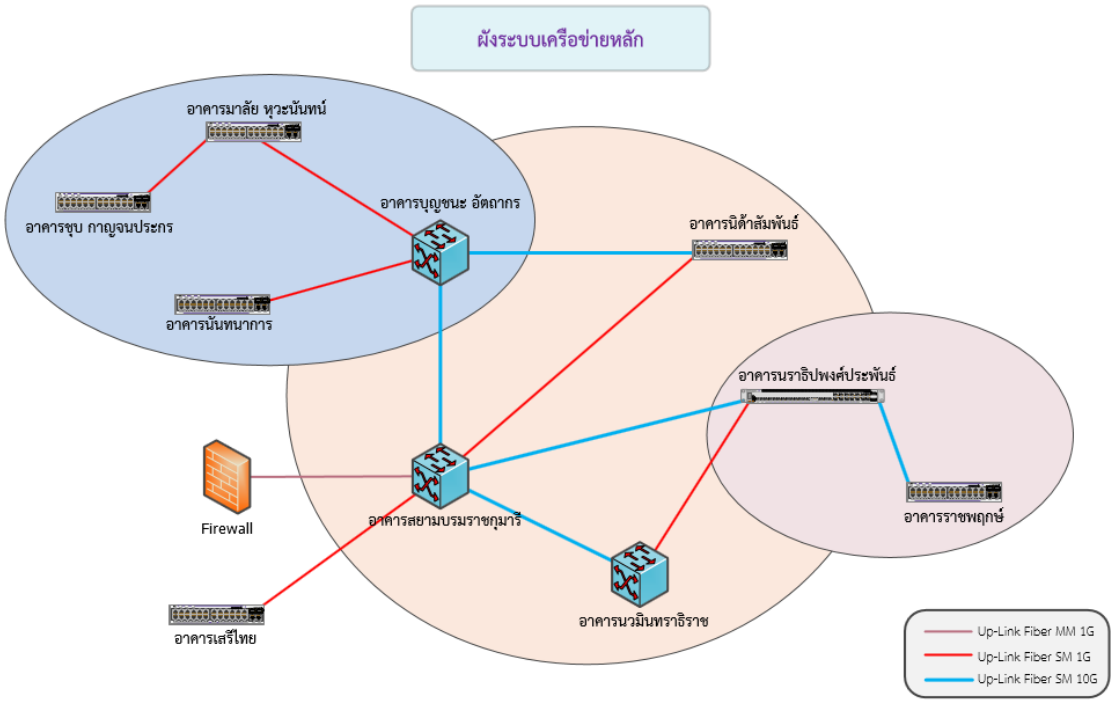
โซนเซิร์ฟเวอร์ประกอบด้วย DMZ1, DMZ2 และ library เป็นเซิร์ฟเวอร์ห้องสมุด

โซน WiFi ของทรู ที่ปล่อยสัญญาณเครือข่ายไร้สายให้กับสถาบัน

โซน Database and Application ประกอบด้วยฐานข้อมูลและระบบสารสนเทศหลัก จะมีไฟร์วอลล์อีกชุดหนึ่งมาขวางเพื่อความปลอดภัย

โซน Internal Core Network เป็นระบบเครือข่ายหลักภายใน

ระบบเครือข่ายหลัก



ภาพที่ 3-2 ผังระบบเครือข่ายหลักของสถาบัน

สำนักได้ปรับปรุงโครงข่ายแกนหลัก (Blackbone) ความเร็วสูงเพื่อรองรับปริมาณการใช้งานเครือข่ายในระบบ 10 กิกะบิตต่อวินาที เชื่อมต่อระหว่างอาคารต่างๆ ได้แก่ อาคารสยามบรมราชกุมารี อาคารบุญชนะอัตถากร อาคารนราธิปพงศ์ประพันธ์ อาคารนวมินทราธิราช อาคารนิด้าสัมพันธ์ อาคารราชพฤกษ์ และเครือข่ายที่ต่อเชื่อมกับหน่วยงานระดับคณะ/สำนัก ภายในอาคารนวมินทราธิราช เป็น 10 GB ใช้วิธีการค้นหาเส้นทางหลักด้วยโปรโตคอล OSPF มีการแจกจ่ายไอพีแอดเดรส (DHCP) โดยให้ core switch ชี้ไปที่ DHCP Server แจกจ่ายไอพีแอดเดรสด้วย Private IP Address แล้วมาให้ไฟร์วอลล์ทำหน้าที่ในการ NAT (Network Address Translation) เป็น Public IP Address เพื่อออกสู่อินเทอร์เน็ต

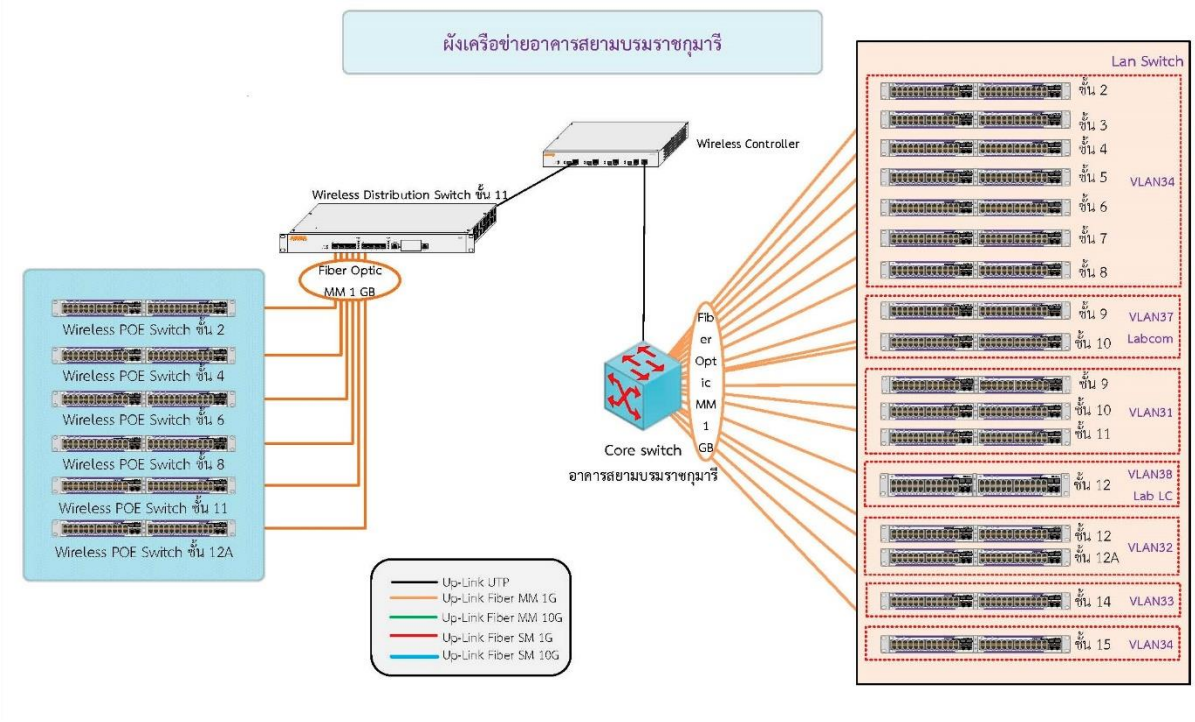
ภาพที่ 3-2 ผังระบบเครือข่ายหลักของสถาบัน จากไฟร์วอลล์จะลิงค์หลักมาเชื่อมต่อกับ Core Switch ของอาคารสยามบรมราชกุมารี มีการตั้งค่าการค้นหาเส้นทางแบบ OSPF มีการเชื่อมโยงกับ Core Switch ของอาคารต่าง ๆ

เส้นสีฟ้า หมายถึง การเชื่อมเครือข่ายด้วยไฟเบอร์ออฟติค แบบซิงเกิลโหมด ขนาด 10 GB

เส้นสีแดง หมายถึง การเชื่อมเครือข่ายด้วยไฟเบอร์ออฟติค แบบซิงเกิลโหมด ขนาด 1 GB

เส้นสีส้ม หมายถึง การเชื่อมเครือข่ายด้วยไฟเบอร์ออฟติค แบบมัลติโหมด ขนาด 1 GB

ระบบเครือข่ายอาคารสยามบรมราชกุมารี



ภาพที่ 3-3 ผังเครือข่ายอาคารสยามบรมราชกุมารี

อาคารสยามบรมราชกุมารีเป็นอาคารสูง 15 ชั้น สายสัญญาณที่เชื่อมระหว่างอาคารเป็นสายไฟเบอร์ออฟติค ซิงเกิลโหมด เป็นอาคารที่ทำการกระจายสัญญาณเครือข่ายไปยังอาคารต่าง ๆ มีเส้นทางหลัก ขนาดความเร็ว 10 GB อยู่ 3 เส้นทาง เส้นทางที่หนึ่งเชื่อมระหว่างอาคารสยามบรมราชกุมารีกับอาคารนวมินทราธิราช เส้นทางที่สองเชื่อมระหว่างอาคารสยามบรมราชกุมารีกับอาคารบุญชนะ อัตถากร เส้นทางที่สามเชื่อมระหว่างอาคารสยามบรมราชกุมารีกับอาคารนราธิปพงศ์ประพันธ์ สายสัญญาณที่เชื่อมระหว่างชั้นเป็นไฟเบอร์ออฟติคมัลติโหมด 6 คอร์สำหรับระบบคอมพิวเตอร์ สายสัญญาณ UTP เป็นประเภท CAT6 มีห้องเครือข่ายหลักอยู่ที่ชั้น 11 ซึ่งเป็นอาคารที่ตั้งของศูนย์ข้อมูลหลัก (Data Center) ภาพที่ 3-3 ผังเครือข่ายอาคารสยามบรมราชกุมารี อธิบายลักษณะการเชื่อมต่อเครือข่ายภายในอาคาร ห้องเครือข่ายย่อยชั้น 2-15 ใช้สายไฟเบอร์ออฟติคประเภทมัลติโหมดเป็นอัพลิงค์มายังห้องเครือข่ายหลักชั้น 11 ห้องเครือข่ายหลัก ขนาดความเร็ว 1 GB ส่วนระบบเครือข่ายไร้สายจะใช้ POE Switch ในการปล่อยสัญญาณและกระแสไฟฟ้าให้กับอุปกรณ์กระจายสัญญาณไร้สาย (Access Point) ติดตั้งอยู่ชั้น 2, 4, 6, 8, 11 และชั้น 12A ระบบเครือข่ายแลนจะมีการแบ่ง VLAN ต่าง ๆ ดังนี้

VLAN 31 ใช้สำหรับสำนักเทคโนโลยีสารสนเทศ ชั้น 9 และ 11 กลุ่มงานวินัยและนิติกรและกลุ่มงานโสตทัศนูประกรณ์ ชั้น 10

VLAN 32 ใช้สำหรับคณะภาษาและการสื่อสาร ชั้น 12-12A

VLAN 33 ใช้สำหรับสำนักสิริพัฒนา ชั้น 14

VLAN 34 ใช้สำหรับศูนย์สาธารณประโยชน์ ชั้น 15 และห้องเรียนชั้น 2-8

VLAN 37 ใช้สำหรับห้องปฏิบัติการคอมพิวเตอร์ ชั้น 9 และ 10

VLAN 38 ใช้สำหรับห้องปฏิบัติเครือข่ายทางภาษา ชั้น 12

ภาพที่ 3-4 แปลนตำแหน่งห้องเครือข่ายหลักอาคารสยามบรมราชกุมารี ชั้น 11

จากภาพที่ 3-4 แปลนตำแหน่งห้องเครือข่ายหลักอาคารสยามบรมราชกุมารี ชั้น 11 มีรายละเอียดดังนี้

ศูนย์ข้อมูลย์หลัก (Data Center)

อาคารสยามบรมราชกุมารี ชั้น 11 เป็นที่ตั้งของศูนย์ข้อมูลหลัก (Data Center) ภายในศูนย์จะแบ่งออกเป็น 3 ห้อง ห้องแอปพลิเคชัน ห้องเครือข่ายหลักและห้องควบคุมระบบปรับอากาศและระบบสำรองไฟ ระบบบริหารจัดการภายในศูนย์ประกอบไปด้วย

- ระบบสแกนด้วยลายนิ้วมือหรือบัตร
- กล้อง CCTV

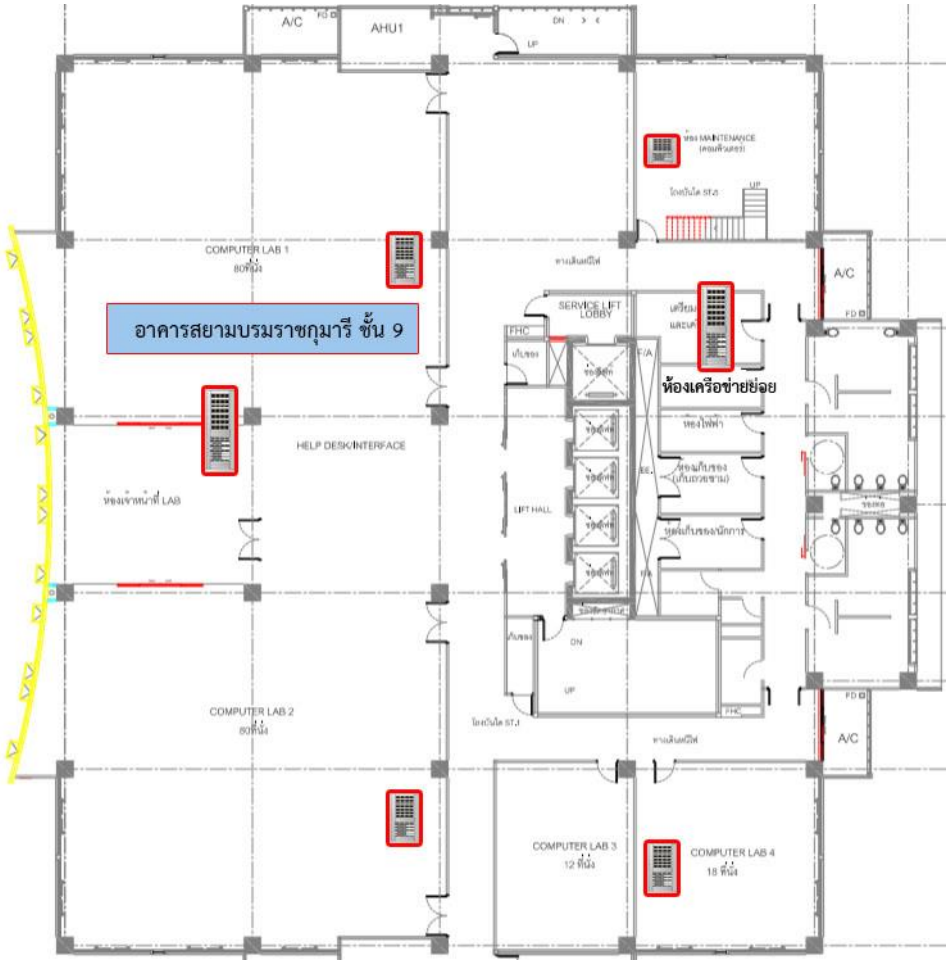
- เครื่องสำรองไฟ
- ระบบปรับอากาศควบคุมความชื้นอัตโนมัติ
- ระบบตรวจจับควันความไวสูง
- ระบบตรวจจับน้ำรั่วอัตโนมัติ
- ระบบแจ้งเตือนและดับเพลิงอัตโนมัติ

ห้องเครือข่ายหลัก

ห้องเครือข่ายหลักในอาคารสยามบรมราชกุมารี ชั้น 11 เข้าออกห้องด้วยลายนิ้วมือของเจ้าหน้าที่สำนักหรือบัตรชั่วคราวให้กับผู้ใช้ภายนอก กุญแจไขห้องอยู่ที่ตู้กุญแจ

ห้องเครือข่ายย่อย

จะอยู่ตรงข้ามห้องน้ำหญิง



ภาพที่ 3-5 แปลนตำแหน่งห้องเครือข่ายหลักอาคารสยามบรมราชกุมารี ชั้น 9

จากภาพที่ 3-5 แปลนตำแหน่งห้องเครือข่ายหลักอาคารสยามบรมราชกุมารี ชั้น 9 มีรายละเอียดดังนี้

ห้องเครือข่ายย่อย ชั้น 9

อยู่ตรงข้ามห้องน้ำหญิง เชื่อมด้วยไฟเบอร์ออฟติคไปยังห้องเครือข่ายหลัก ชั้น 11 มีลิงค์เชื่อมไปยังตู้เครือข่ายย่อยห้องเจ้าหน้าที่ฝ่ายบริการติดตั้ง

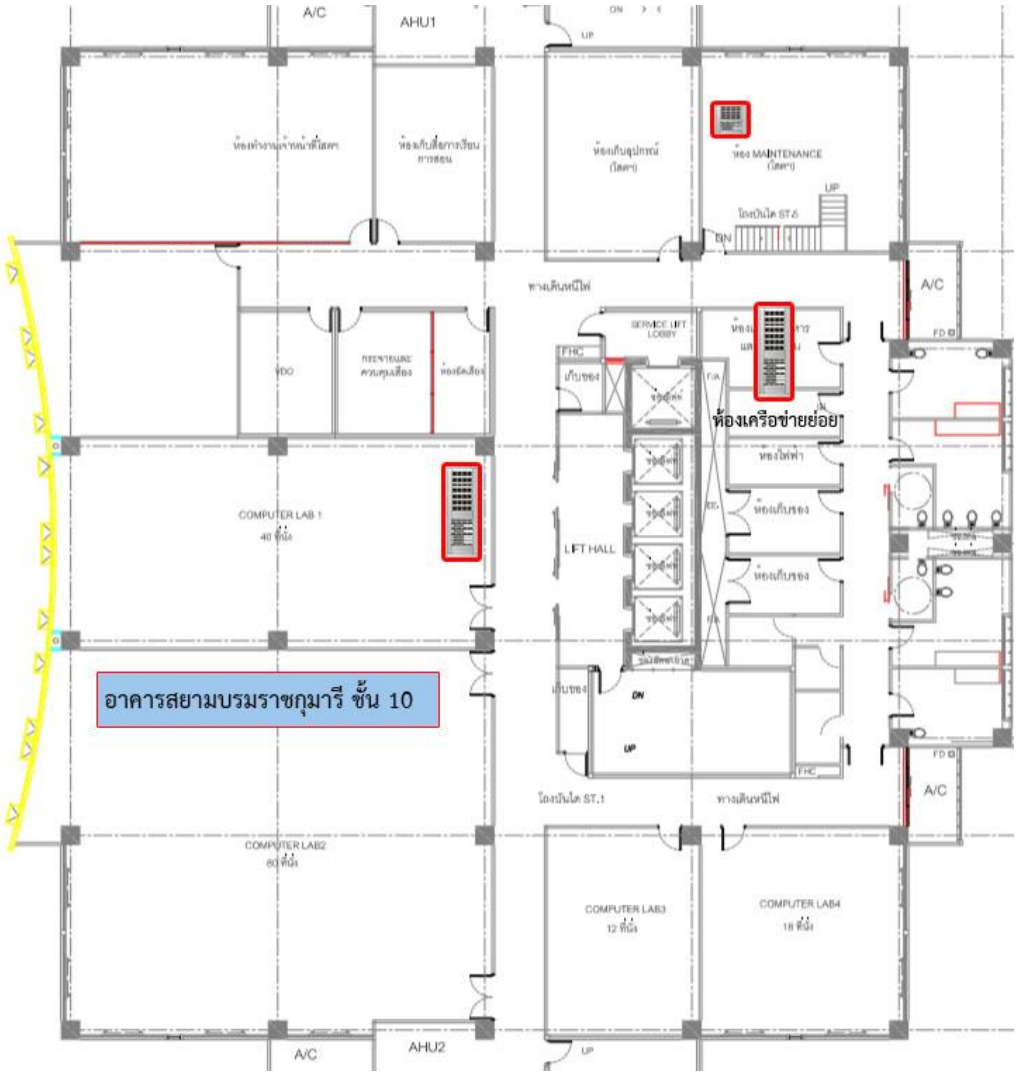
ตู้เครือข่ายย่อย

ห้องเจ้าหน้าที่แล็ป เชื่อมด้วยไฟเบอร์ออฟติคไปยังห้องเครือข่ายหลัก ชั้น 11

ห้องแล็บ 1 (Walk-in) อัพลิงค์เป็นสาย UTP ไปยังห้องเจ้าหน้าที่แล็ป

ห้องแล็บ 2 (Walk-in) อัพลิงค์เป็นสาย UTP ไปยังห้องเจ้าหน้าที่แล็ป

ห้องแล็บ 3 (Walk-in) อัพลิงค์เป็นสาย UTP ไปยังห้องเจ้าหน้าที่แล็ป



ภาพที่ 3-6 แปลนตำแหน่งห้องเครือข่ายหลักอาคารสยามบรมราชกุมารี ชั้น 10

จากภาพที่ 3-6 แปลนตำแหน่งห้องเครือข่ายหลักอาคารสยามบรมราชกุมารี ชั้น 10 มีรายละเอียดดังนี้

ห้องเครือข่ายย่อย ชั้น 10

ตู้แรกอยู่ภายในห้องเครือข่ายย่อยตรงข้ามห้องน้ำหญิง เชื่อมด้วยไฟเบอร์ออฟติคไปยังห้องเครือข่ายหลัก ชั้น 11 มีลิงค์เชื่อมไปยังตู้เครือข่ายย่อยห้องเจ้าหน้าที่ฝ่ายบริการติดตั้ง

ตู้ที่สองอยู่ที่ห้องแล็บ 4 เชื่อมด้วยไฟเบอร์ออฟติคไปยังห้องเครือข่ายหลัก ชั้น 11

ภาพที่ 3-7 แปลนตำแหน่งห้องเครือข่ายหลักอาคารสยามบรมราชกุมารี ชั้น 12

จากภาพที่ 3-7 แปลนตำแหน่งห้องเครือข่ายหลักอาคารสยามบรมราชกุมารี ชั้น 12 มีรายละเอียดดังนี้

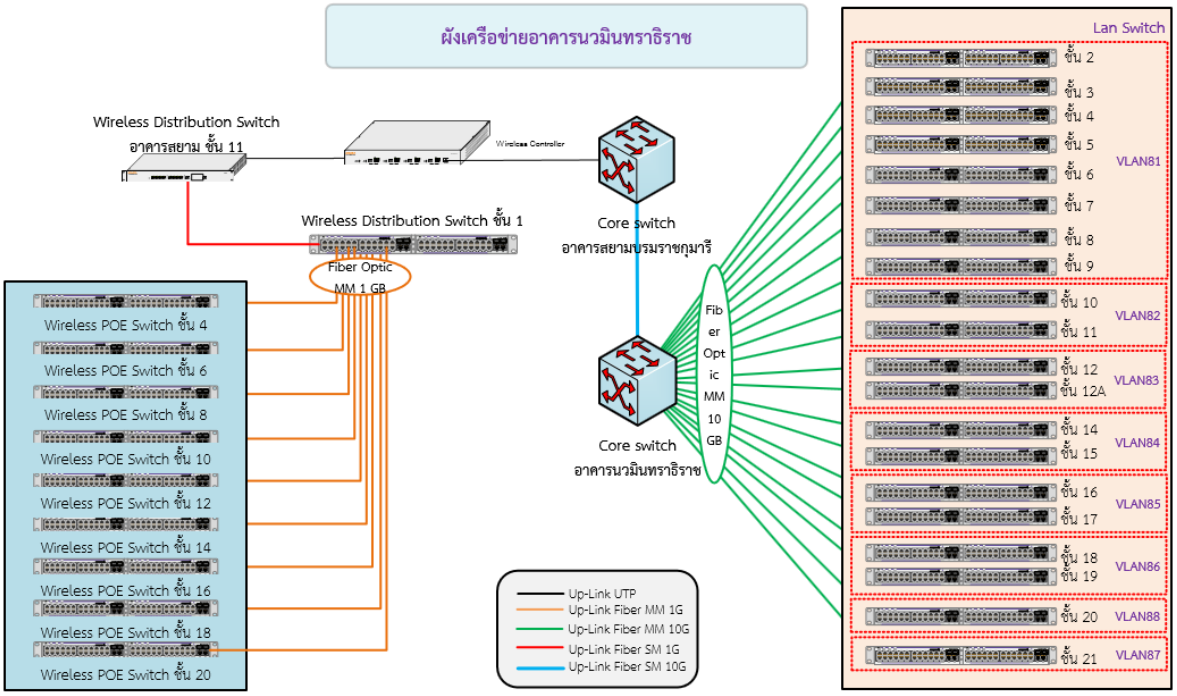
ตู้เครือข่ายย่อย ชั้น 12

ตู้แรกอยู่ภายในห้องเครือข่ายย่อยตรงข้ามห้องน้ำหญิง เชื่อมด้วยไฟเบอร์ออฟติคไปยังห้องเครือข่ายหลัก ชั้น 11 กระจายสัญญาณให้กับเจ้าหน้าที่ภายในคณะภาษาและการสื่อสาร

ห้องที่สองอยู่ที่ห้องปฏิบัติการทางภาษาเชื่อมด้วยไฟเบอร์ออฟติคไปยังห้องเครือข่ายหลัก ชั้น 11

ชั้นอื่น ๆ ที่เหลือห้องเครือข่ายย่อยจะอยู่ตรงข้ามห้องน้ำหญิงแนวเดียวกับชั้น 12 หมด ยกเว้นชั้น 1 กับชั้น M ที่ไม่มีห้องเครือข่ายย่อย

ระบบเครือข่ายอาคารนวมินทราธิราช



ภาพที่ 3-8 ผังเครือข่ายอาคารนวมินทราธิราช

อาคารนวมินทราธิราชเป็นอาคารสูง 21 ชั้น สายสัญญาณที่เชื่อมระหว่างอาคารเป็นสายไฟเบอร์ออฟติค ซิงเกิลโหมด มีเส้นทางหลัก ขนาดความเร็ว 10 GB เชื่อมระหว่างอาคารนวมินทราธิราชกับอาคารสยามบรมราชกุมารี เส้นทางสำรองเชื่อมระหว่างอาคารนวมินทราธิราชกับอาคารนราธิปพงศ์ประพันธ์ ขนาดความเร็ว 1 GB สายสัญญาณที่เชื่อมระหว่างชั้นเป็นไฟเบอร์ออฟติคมัลติโหมด 6 คอร์สำหรับระบบคอมพิวเตอร์และสายไฟเบอร์ออฟติคมัลติโหมด 6 คอร์สำหรับระบบโทรศัพท์ สายสัญญาณ UTP เป็นประเภท CAT6A และ CAT6 มีห้องเครือข่ายหลักอยู่ที่ชั้น 1 จากภาพที่ 3-8 ผังเครือข่ายอาคารนวมินทราธิราช อธิบายลักษณะการเชื่อมต่อเครือข่ายภายในอาคาร ห้องเครือข่ายย่อยชั้น 2-21 ใช้สายไฟเบอร์ออฟติคประเภทมัลติโหมดเป็นอัพลิงค์มายังห้องเครือข่ายหลักชั้น 1 ห้องเครือข่ายหลัก ขนาดความเร็ว 10 GB ส่วนระบบเครือข่ายไร้สายจะใช้ POE Switch ในการปล่อยสัญญาณและกระแสไฟฟ้าให้กับอุปกรณ์กระจายสัญญาณไร้สาย (Access Point) ติดตั้งอยู่ชั้น 4, 6, 8, 10, 12, 14, 16, 18 และ20 ระบบเครือข่ายแลนจะมีการแบ่ง VLAN ต่าง ๆ ดังนี้

VLAN 81 ใช้สำหรับห้องเรียน ชั้น 3-9 กลุ่มงานสื่อสารองค์กร กลุ่มงานกิจการนานาชาติ และสหกรณ์ออมทรัพย์ ชั้น 1

VLAN 82 ใช้สำหรับคณะรัฐประศาสนศาสตร์ ชั้น 10-11

VLAN 83 ใช้สำหรับคณะสถิติประยุกต์ ชั้น 12-12A

VLAN 84 ใช้สำหรับคณะพัฒนาการเศรษฐกิจ ชั้น 14-15

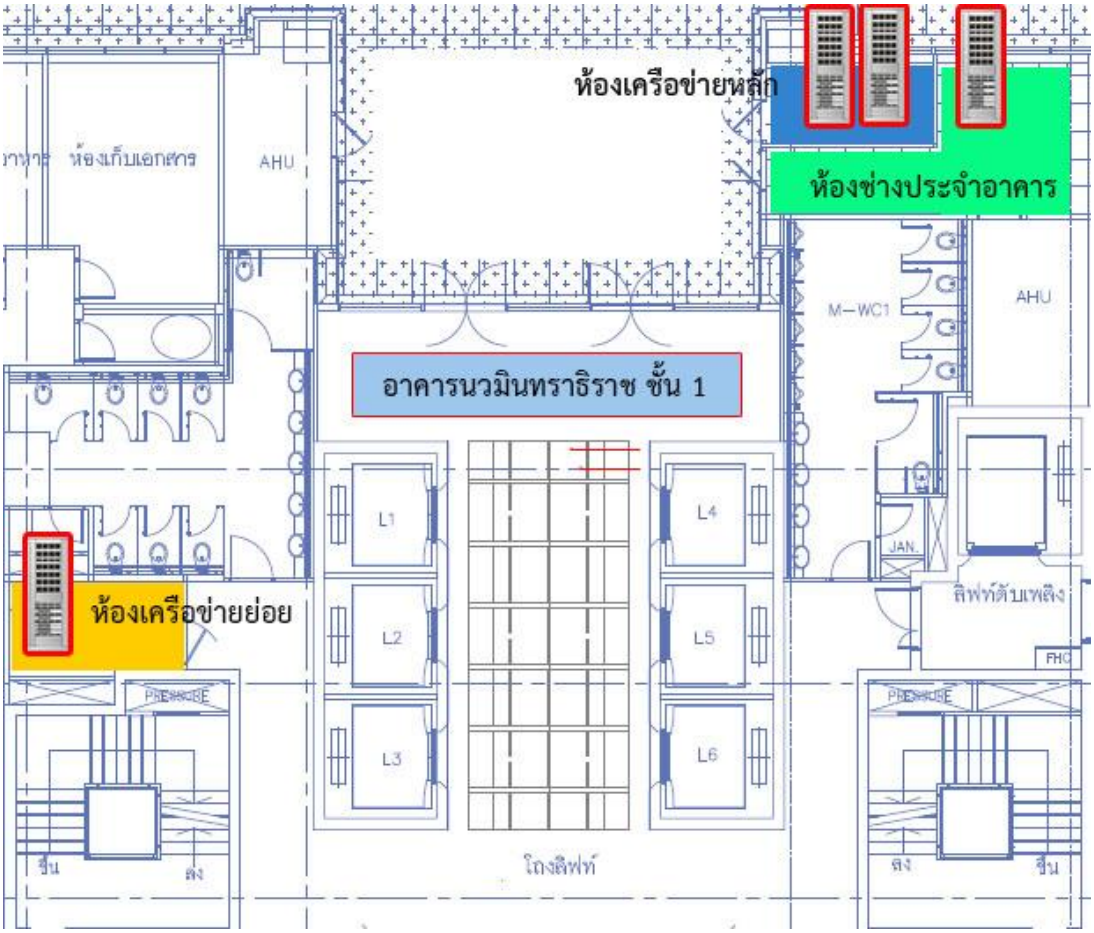
VLAN 85 ใช้สำหรับคณะพัฒนาสังคม ชั้น 16-17

VLAN 86 ใช้สำหรับวิทยาลัยนานาชาติ ชั้น 18-19 และคณะนิเทศศาสตร์และนวัตกรรมการจัดการ ชั้น 18

VLAN 87 ใช้สำหรับห้องสมุดอาเซียน ชั้น 21

VLAN 88 ใช้สำหรับสำนักวิจัย ชั้น 20

นอกจากนี้ยังมีระบบเครือข่ายย่อยอยู่ 2 หน่วยงาน ได้แก่ คณะสถิติประยุกต์ที่สำนักได้เชื่อมต่อลิงค์หลักและทางคณะเป็นผู้บริหารจัดการเครือข่ายภายในของตนเอง หน่วยงานที่สองคือห้องสมุดอาเซียน



ภาพที่ 3-9 แปลนตำแหน่งห้องเครือข่ายอาคารนวมินทราธิราช ชั้น 1-21

จากภาพที่ 3-9 แปลนตำแหน่งห้องเครือข่ายอาคารนวมินทราธิราช ชั้น 1-21 มีรายละเอียด ดังนี้

ห้องเครือข่ายหลัก

อยู่ชั้น 1 ตรงประตูทางเข้าด้านหลังอาคารติดกับห้องช่างประจำอาคาร เข้าห้องได้โดยแจ้งกับช่างประจำอาคารในห้องที่อยู่ติดกัน ภายในห้องช่างจะมีตู้เครือข่ายหลักของระบบโทรศัพท์

ชั้นนี้จะมีตู้เครือข่ายย่อยอยู่ 3 แห่ง ดังนี้

ตู้ที่ 1 เป็น wall rack อยู่ภายในสหกรณ์ออมทรัพย์

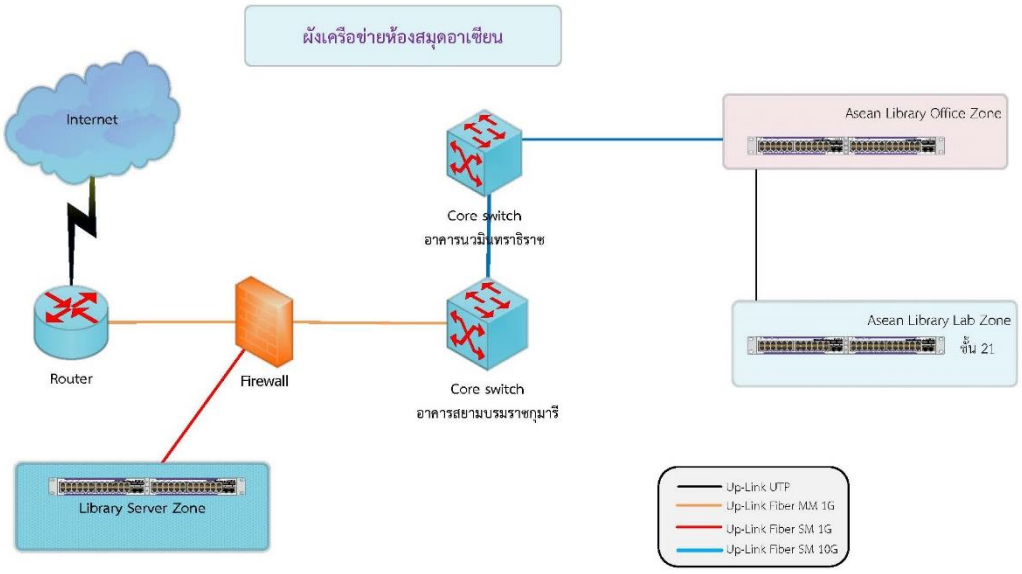
ตู้ที่ 2 เป็น wall rack อยู่ภายในกลุ่มงานสื่อสารองค์การและกิจกรรมเพื่อสังคม

ตู้ที่ 3 เป็น wall rack อยู่ภายในกลุ่มงานกิจการนานาชาติ

ห้องเครือข่ายย่อย ชั้น 1-21

อยู่ข้างห้องน้ำหญิง เชื่อมด้วยไฟเบอร์ออฟติคไปยังห้องเครือข่ายหลัก ชั้น 1

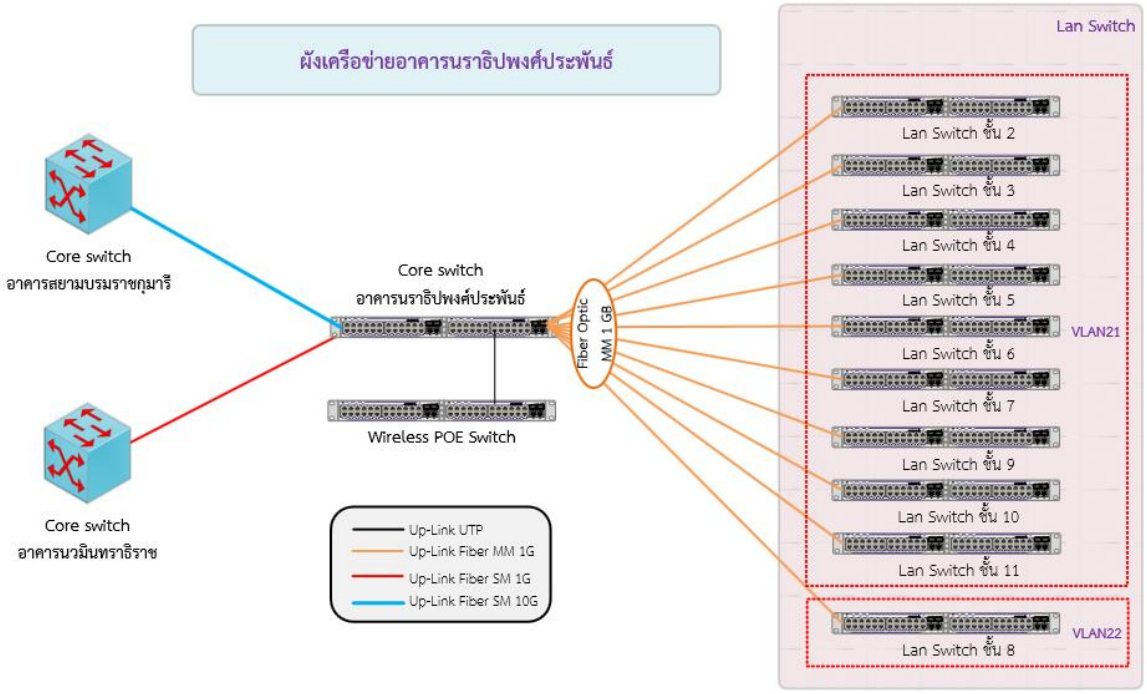
ระบบเครือข่ายห้องสมุดอาเซียน



ภาพที่ 3-10 ผังเครือข่ายห้องสมุดอาเซียน

ภาพที่ 3-10 ผังเครือข่ายห้องสมุดอาเซียน สำนักได้ทำการออกแบบตามความต้องการของห้องสมุดใช้ VLAN 88 สำหรับเจ้าหน้าที่ และเครื่องที่ให้บริการนักศึกษาต้องทำการล็อคอินด้วย NETID ส่วนจุดแลนที่มีให้ตามโต๊ะอ่านหนังสือจะแยก VLAN ออกมาและไฟร์วอลล์จะส่งหน้าจอล็อคอินให้ผู้ใช้งานทำการล็อคอินเพื่อเข้าใช้งาน ส่วนสิทธิในการเข้าใช้งานระบบอะไรได้บ้างจะกำหนดโดยผู้ดูแลระบบของสำนักบรรณสารการพัฒนา

ระบบเครือข่ายอาคารนราธิปพงศ์ประพันธ์

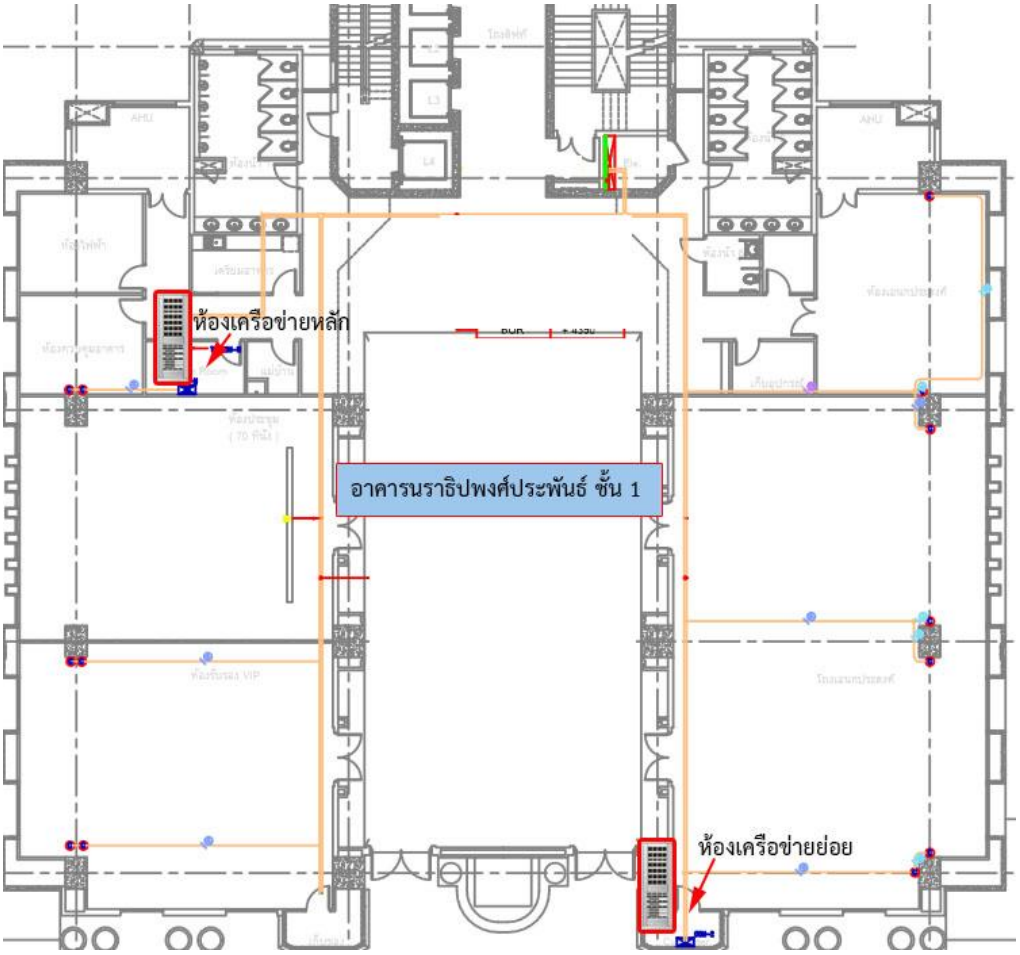


ภาพที่ 3-11 ผังเครือข่ายอาคารนราธิปพงศ์ประพันธ์

ภาพที่ 3-11 ผังเครือข่ายอาคารนราธิปพงศ์ประพันธ์ เป็นอาคารสูง 11 ชั้น สายสัญญาณที่เชื่อมระหว่างอาคารเป็นสายไฟเบอร์ออฟติค ซิงเกิลโหมด มีเส้นทางหลัก ขนาดความเร็ว 10 GB เชื่อมระหว่างอาคารนราธิปพงศ์ประพันธ์กับอาคารสยามบรมราชกุมารี เส้นทางสำรองเชื่อมระหว่างอาคารนราธิปพงศ์ประพันธ์กับอาคารนวมินทราธิราช ขนาดความเร็ว 1 GB นอกจากนี้ยังเป็นจุดกระจายสัญญาณให้กับอาคารต่าง ๆ ใกล้เคียง ความเร็ว 1 GB จำนวน 2 เส้นทาง เส้นทางที่หนึ่งเชื่อมระหว่างอาคารนราธิปพงศ์ประพันธ์กับอาคารราชพฤกษ์ เส้นทางที่สองเชื่อมระหว่างอาคารนราธิปพงศ์ประพันธ์กับอาคารเสรีไทย สายสัญญาณที่เชื่อมระหว่างชั้นเป็นไฟเบอร์ออฟติคมัลติโหมด 6 คอร์สำหรับระบบคอมพิวเตอร์ สายสัญญาณ UTP เป็นประเภท CAT6 มีห้องเครือข่ายหลักอยู่ที่ชั้น 2 จากภาพที่ 3-6 ผังเครือข่ายอาคารนราธิปพงศ์ประพันธ์ อธิบายลักษณะการเชื่อมต่อเครือข่ายภายในอาคาร ห้องเครือข่ายย่อยชั้น 2-11 ใช้สายไฟเบอร์ออฟติคประเภทมัลติโหมดเป็นอัพลิงค์มายังห้องเครือข่ายหลักชั้น 2 ขนาดความเร็ว 1 GB ส่วนระบบเครือข่ายไร้สายจะใช้ POE Switch ในการปล่อยสัญญาณและกระแสไฟฟ้าให้กับอุปกรณ์กระจายสัญญาณไร้สาย (Access Point) ติดตั้งอยู่ห้องเครือข่ายหลักชั้น 2 ที่เดียว เนื่องจากห้องเครือข่ายย่อยอยู่ด้านหน้าอาคาร และไม่มีช่องชาร์ป ทำให้การเดินสายเพิ่มเติมของระบบต่าง ๆ ภายหลังการก่อสร้างอาคารไม่สะดวก เพราะจะต้องเดินย้อนกลับไปที่ห้องไฟฟ้าจึงเดินย้อนมาที่ห้องเครือข่ายย่อย ซึ่งจะมีผลทำให้ระยะความยาวของสายที่เดินเกินมาตรฐาน ระบบเครือข่ายไร้สายที่เดินโดยผู้ให้บริการรายอื่น ๆ จึงขอติดตั้งตู้เครือข่ายที่ห้องไฟฟ้าแทน ระบบเครือข่ายแลนจะมีการแบ่ง VLAN ต่าง ๆ ดังนี้

VLAN 21 ใช้สำหรับหน่วยงานทุกหน่วยงาน ชั้น 2-9

VLAN 22 ใช้สำหรับห้องประชุมต่าง ๆ ที่อยู่ชั้น 8 และระบบ e-meeting ที่ติดตั้งอยู่ที่ห้องประชุมอินทรภูวศักดิ์ เพื่อให้สามารถปรับแต่งเครือข่ายได้โดยตามการใช้งาน และให้ไฟร์วอลล์ทำการส่งหน้าจอล็อคอินสำหรับผู้ใช้งานที่ต้องการใช้อินเทอร์เน็ต เพื่อเก็บข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการตาม พ.ร.บ. 2550



ภาพที่ 3-12 แปลนตำแหน่งห้องเครือข่ายอาคารนราธิปพงศ์ประพันธ์ ชั้น 2-11

จากภาพที่ 3-12 แปลนตำแหน่งห้องเครือข่ายอาคารนราธิปพงศ์ประพันธ์ ชั้น 2-11 มีรายละเอียดดังนี้

ห้องเครือข่ายหลัก

อยู่ชั้น 2 ข้างห้องน้ำชายติดกับห้องช่างประจำอาคาร เข้าห้องได้โดยแจ้งกับช่างประจำอาคารในห้องที่อยู่ติดกัน ภายในห้องช่างจะมีตู้เครือข่ายหลักของระบบโทรศัพท์

ชั้นนี้จะมีตู้เครือข่ายย่อยอยู่ 3 แห่ง ดังนี้

ตู้ที่ 1 เป็น wall rack อยู่ภายในสหกรณ์ออมทรัพย์

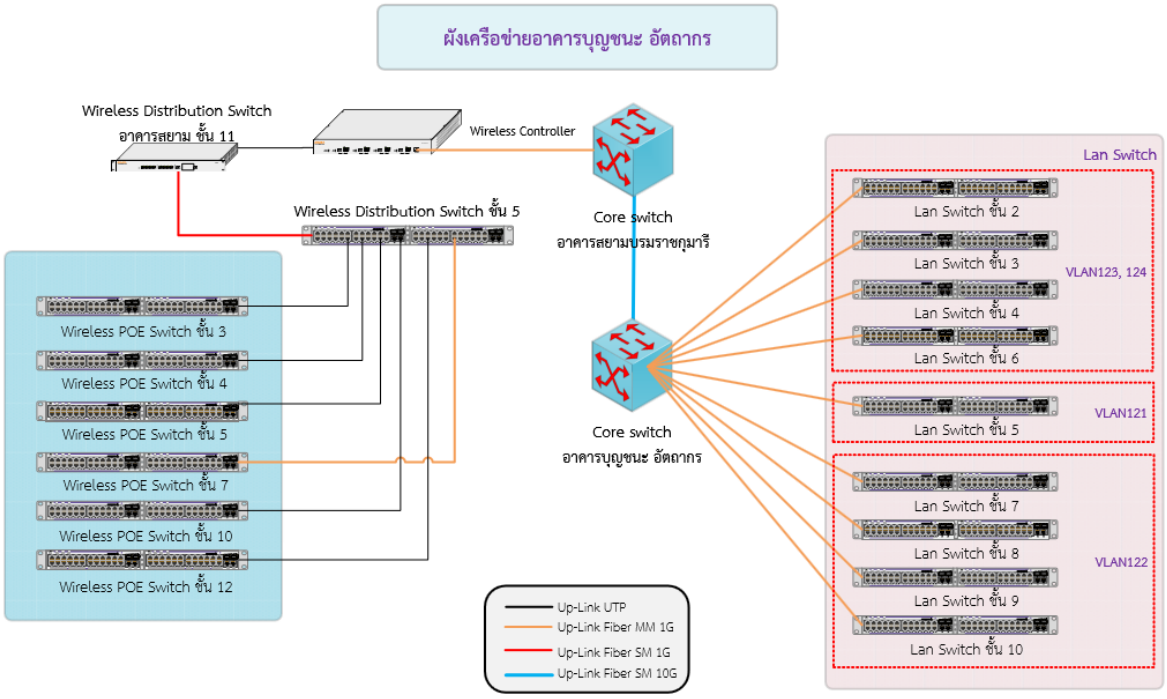
ตู้ที่ 2 เป็น wall rack อยู่ภายในกลุ่มงานสื่อสารองค์การและกิจกรรมเพื่อสังคม

ตู้ที่ 3 เป็น wall rack อยู่ภายในกลุ่มงานกิจการนานาชาติ

ห้องเครือข่ายย่อย ชั้น 1-21

อยู่ข้างห้องน้ำหญิง เชื่อมด้วยไฟเบอร์ออฟติคไปยังห้องเครือข่ายหลัก ชั้น 1

ระบบเครือข่ายอาคารบุญชนะ อัตถากร



ภาพที่ 3-13 ผังเครือข่ายอาคารบุญชนะ อัตถากร

อาคารบุญชนะ อัตถากรเป็นอาคารสูง 12 ชั้น สายสัญญาณที่เชื่อมระหว่างอาคารเป็นสายไฟเบอร์ออฟติค ซิงเกิลโหมด มีเส้นทางหลัก ขนาดความเร็ว 10 GB เชื่อมระหว่างอาคารบุญชนะ อัตถากรกับอาคารสยามบรมราชกุมารี นอกจากนี้ยังเป็นจุดกระจายสัญญาณให้กับอาคารต่าง ๆ ใกล้เคียง ขนาด 10 GB จำนวน 1 เส้นทาง เส้นทางที่หนึ่งเชื่อมระหว่างอาคารบุญชนะ อัตถากรกับอาคารนิด้าสัมพันธ์ ขนาด 1 GB จำนวน 2 เส้นทาง เส้นทางที่หนึ่งเชื่อมระหว่างอาคารบุญชนะ อัตถากรกับอาคารมาลัย หุวะนันทน์ เส้นทางที่สองเชื่อมระหว่างอาคารบุญชนะ อัตถากรกับอาคารนัทนาการ นอกจากนี้ยังมีอีกหนึ่งเส้นทาง ขนาด 1 GB ที่เชื่อมระหว่างห้องเครือข่ายหลักของสำนักบรรณสารกับอาคารสยามบรมราชกุมารี

จากภาพที่ 3-13 ผังเครือข่ายอาคารบุญชนะ อัตถากร สายสัญญาณที่เชื่อมระหว่างชั้นเป็นไฟเบอร์ออฟติคมัลติโหมด 6 คอร์ ยกเว้นชั้น 11 และ 12 ที่ไม่มีสายไฟเบอร์ออฟติค มีสาย UTP เป็นอัพลิงค์ไปยังชั้น 12 สำหรับระบบคอมพิวเตอร์ สายสัญญาณ UTP เป็นประเภท CAT5e และ CAT5 มีห้องเครือข่ายหลักอยู่ที่ชั้น 5 จากภาพที่ 3-7 ผังเครือข่ายอาคารบุญชนะ อัตถากร อธิบายลักษณะการเชื่อมต่อเครือข่ายภายในอาคาร อาคารนี้จะมีตู้เครือข่ายย่อยชั้น 2-10 และ ชั้น 12 ใช้สายไฟเบอร์ออฟติคประเภทมัลติโหมดเป็นอัพลิงค์มายัง

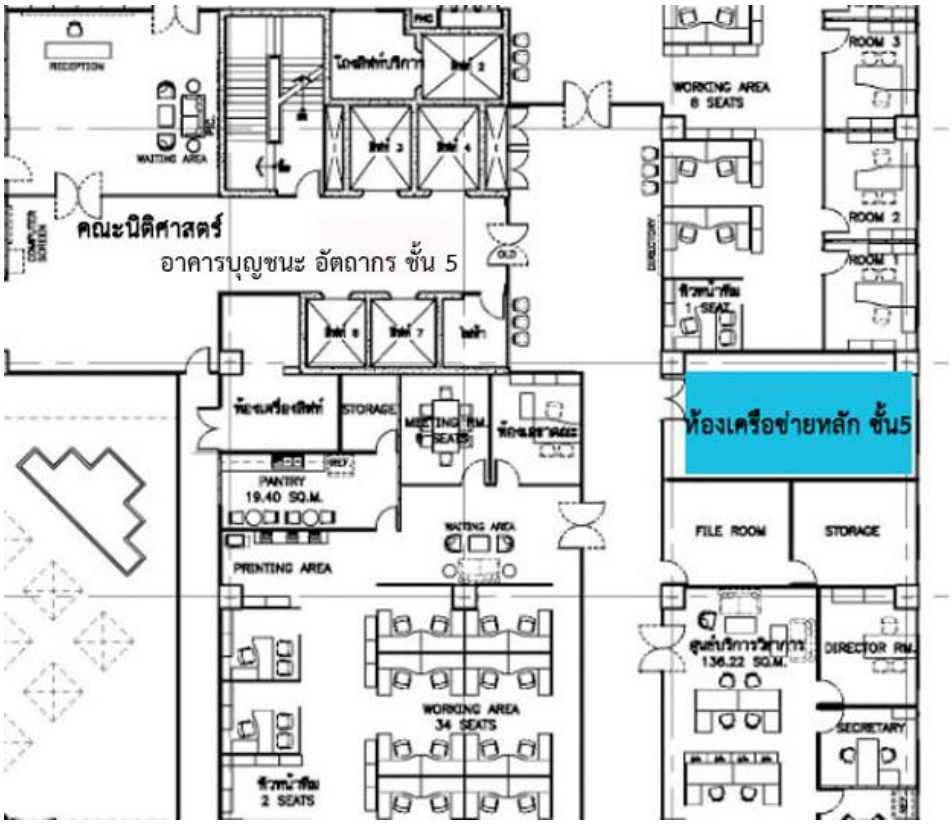
ห้องเครือข่ายหลักชั้น 2 ขนาดความเร็ว 1 GB ส่วนระบบเครือข่ายไร้สายจะใช้ POE Switch ในการปล่อยสัญญาณและกระแสไฟฟ้าให้กับอุปกรณ์กระจายสัญญาณไร้สาย (Access Point) ติดตั้งอยู่ห้องเครือข่ายหลักชั้น 3, 4, 5, 7, 10, 12 ระบบเครือข่ายแลนจะมีการแบ่ง VLAN ต่าง ๆ ดังนี้

VLAN 121 ใช้สำหรับคณะนิติศาสตร์ และศูนย์บริการวิชาการ ชั้น 5

VLAN 122 ใช้สำหรับคณะบริหารธุรกิจ ชั้น 7-10

VLAN 123 ใช้สำหรับเจ้าหน้าที่สำนักบรรณสารการพัฒนา ชั้น 2-4 และ 6

VLAN 124 ใช้สำหรับที่เป็นอุปกรณ์ให้บริการต่าง ๆ ของสำนักบรรณสารการพัฒนา ชั้น 2-4



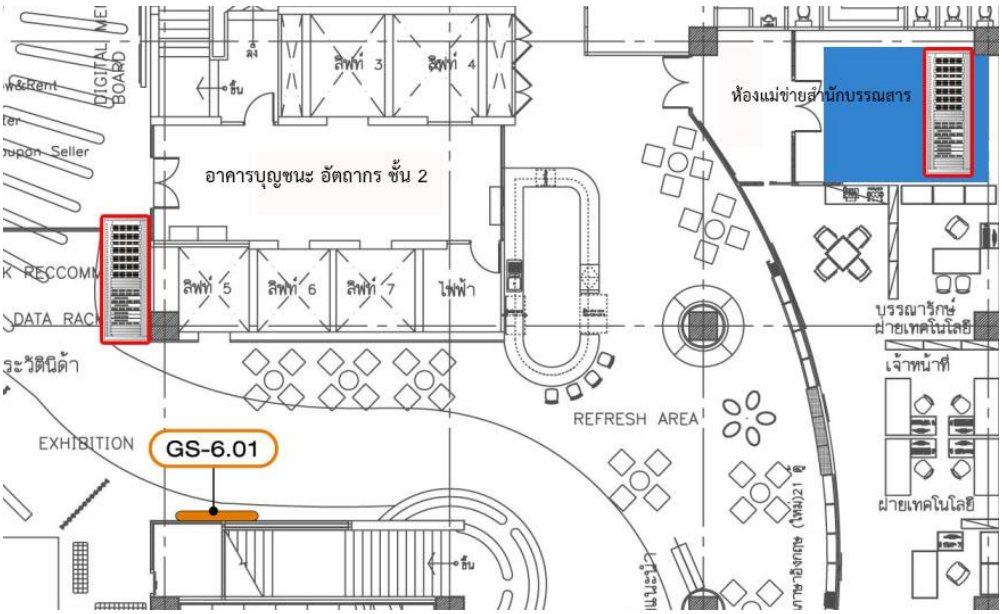
ภาพที่ 3-14 แปลนตำแหน่งห้องเครือข่ายหลักอาคารบุญชนะ อัตถากร ชั้น 5

ห้องเครือข่ายหลัก

ภาพที่ 3-14 แปลนตำแหน่งห้องเครือข่ายหลักอาคารบุญชนะ อัตถากร ชั้น 5 ห้องเครือข่ายหลักจะติดตั้งเครื่องสแกนลายนิ้วมือ ผู้มีสิทธิในการเข้าห้องจะต้องเป็นบุคลากรภายในสำนักเท่านั้น

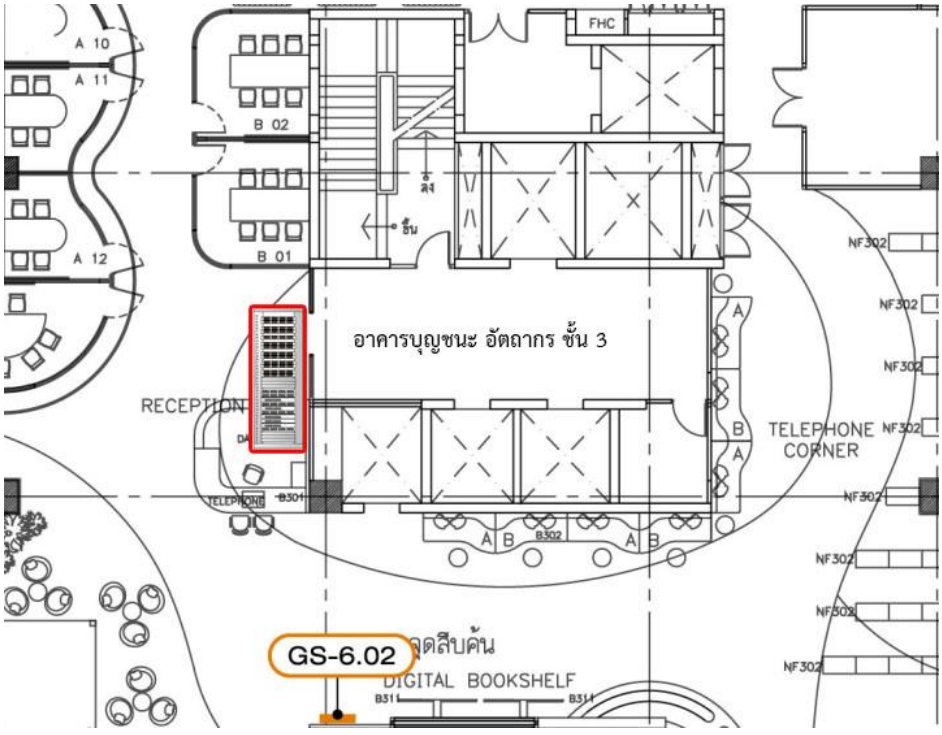
ห้องเครือข่ายย่อยแต่ละชั้น

อาคารนี้จะมีการปรับปรุงไปหลายครั้ง ทำให้ตำแหน่งตู้เครือข่ายย่อยแตกต่างกันไป ดังนี้



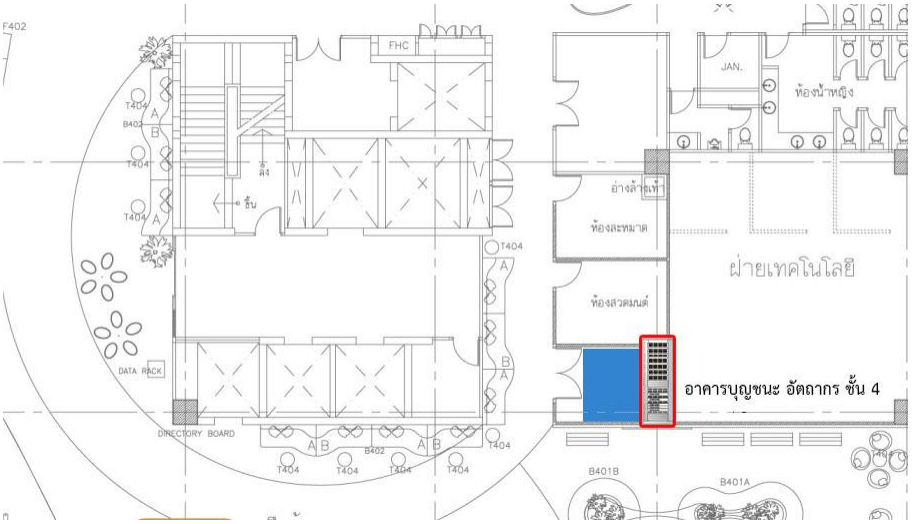
ภาพที่ 3-15 แปลนตำแหน่งห้องเครือข่ายย่อยอาคารบุญชนะ อัตถากร ชั้น 2

ภาพที่ 3-15 แปลนตำแหน่งห้องเครือข่ายย่อยอาคารบุญชนะ อัตถากร ชั้น 2 จะมีประตูบานไม้บิ้วอินแบบสปริง ชั้นนี้จะเป็นที่ตั้งห้องแม่ข่ายของสำนักบรรณสารการพัฒนา เข้าห้องนี้โดยติดต่อเจ้าหน้าที่ฝ่ายเทคโนโลยีของสำนักบรรณสารการพัฒนา



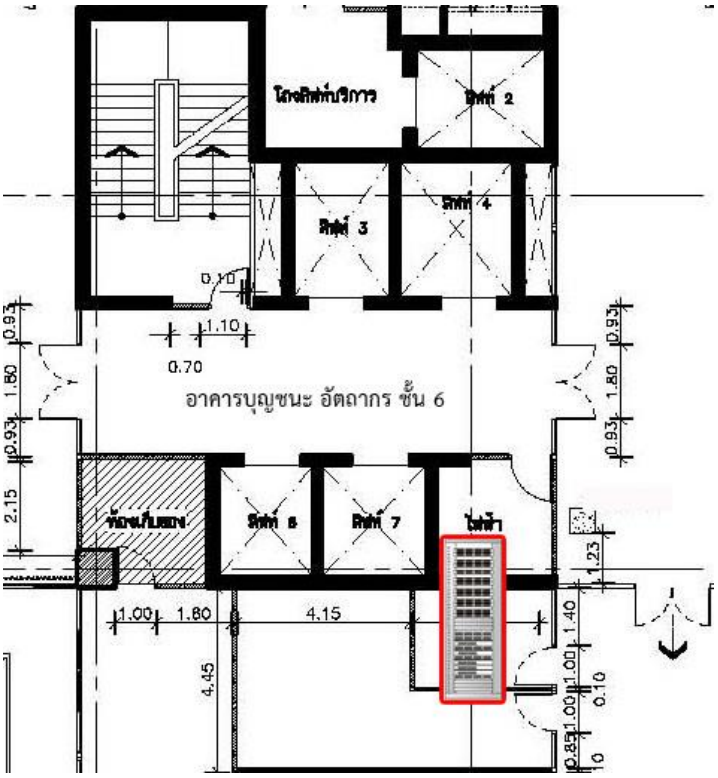
ภาพที่ 3-16 แปลนตำแหน่งห้องเครือข่ายย่อยอาคารบุญชนะ อัตถากร ชั้น 3

ภาพที่ 3-16 แปลนตำแหน่งห้องเครือข่ายย่อยอาคารบุญชนะ อัตถากร ชั้น 3 ชั้นนี้ไม่มีห้องเครือข่ายเป็นตู้ขนาด 27U ตรงเคาน์เตอร์เจ้าหน้าที่อยู่เยื้องทางลงบันได



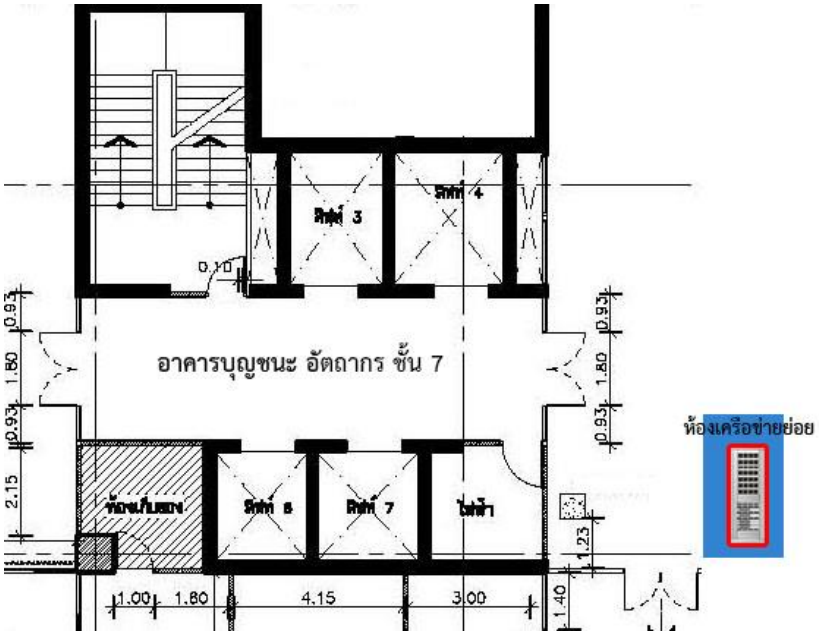
ภาพที่ 3-17 แปลนตำแหน่งห้องเครือข่ายย่อยอาคารบุญชนะ อัตถากร ชั้น 4

ภาพที่ 3-17 แปลนตำแหน่งห้องเครือข่ายย่อยอาคารบุญชนะ อัตถากร ชั้น 4 ตู้เครือข่ายจะอยู่ภายในห้องเจ้าหน้าที่สำนักบรรณสารการพัฒนา เข้าห้องด้วยการติดต่อเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศของสำนักบรรณสารการพัฒนา ที่ชั้น 2



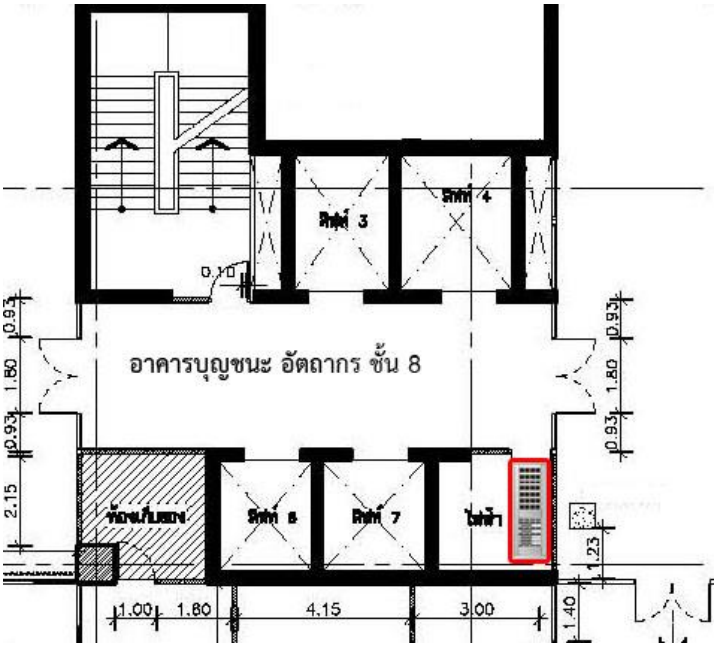
ภาพที่ 3-18 แปลนตำแหน่งห้องเครือข่ายย่อยอาคารบุญชนะ อัตถากร ชั้น 6

ภาพที่ 3-18 แปลนตำแหน่งห้องเครือข่ายย่อยอาคารบุญชนะ อัตถากร ชั้น 6 ตู้เครือข่ายจะอยู่ภายในสำนักงานของสำนักบรรณสารการพัฒนา ตรงข้ามห้องประชุม



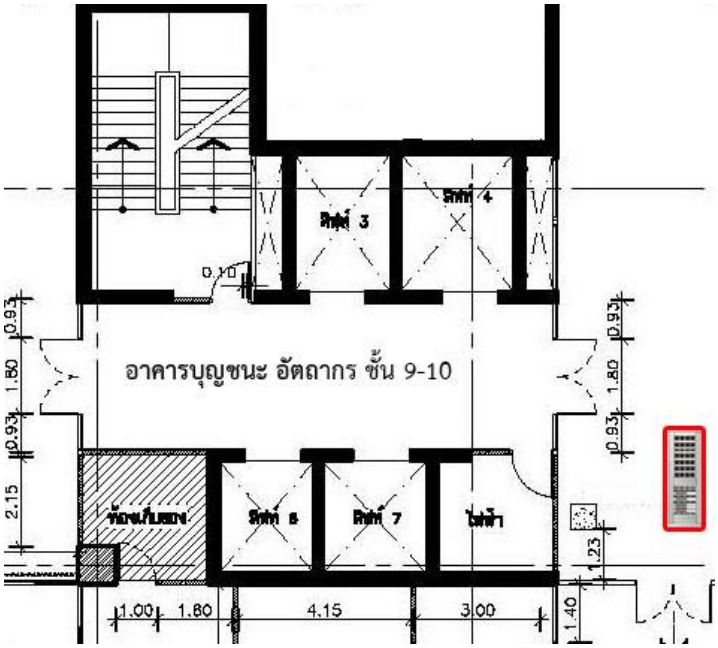
ภาพที่ 3-19 แปลนตำแหน่งห้องเครือข่ายย่อยอาคารบุญชนะ อัตถากร ชั้น 7

ภาพที่ 3-19 แปลนตำแหน่งห้องเครือข่ายย่อยอาคารบุญชนะ อัตถากร ชั้น 7 ห้องเครือข่ายจะอยู่หลังเคาน์เตอร์หน้าลิฟท์ เป็นประตูไม้ มีประตูเข้า 2 ทาง เข้าทางเคาน์เตอร์เป็นด้านหน้าตู้กับเข้าทางห้องเจ้าหน้าที่เพื่อเข้าด้านหลังตู้



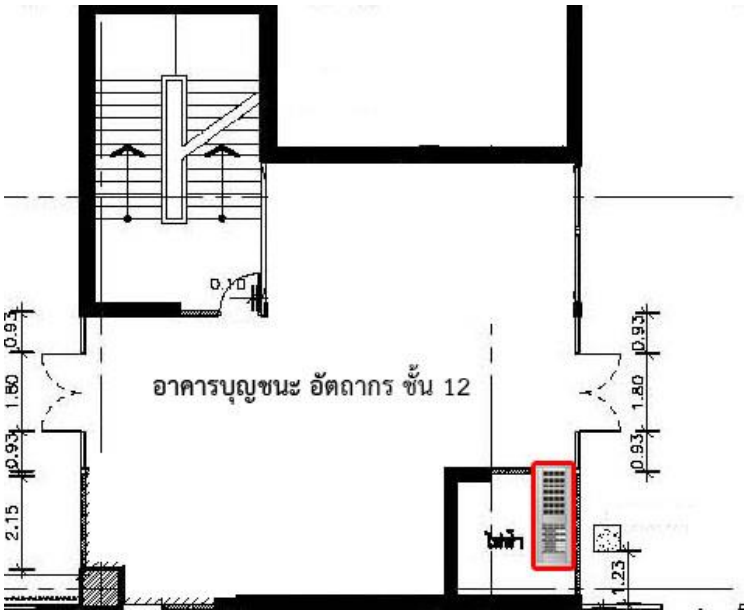
ภาพที่ 3-20 แปลนตำแหน่งห้องเครือข่ายย่อยอาคารบุญชนะ อัตถากร ชั้น 8

ภาพที่ 3-20 แปลนตำแหน่งห้องเครือข่ายย่อยอาคารบุญชนะ อัตถากร ชั้น 8 ตู้เครือข่ายจะอยู่ภายในห้องไฟฟ้าข้างลิฟท์ เข้าห้องด้วยการแจ้งเจ้าหน้าที่ช่างประจำอาคาร ที่ ชั้น G



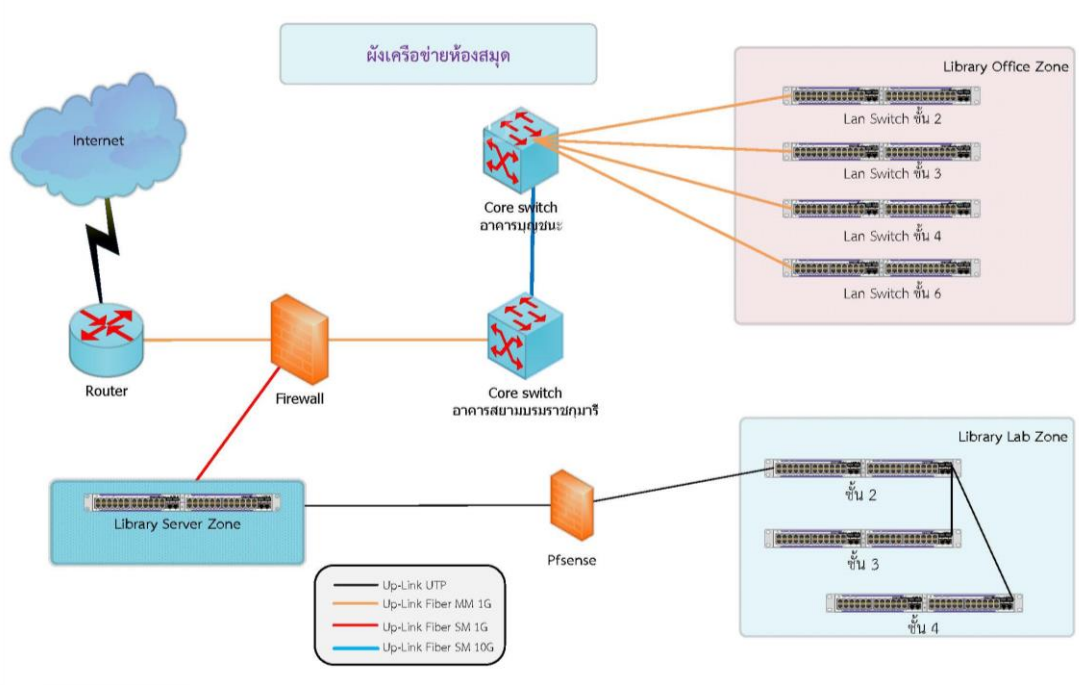
ภาพที่ 3-21 แปลนตำแหน่งห้องเครือข่ายย่อยอาคารบุญชนะ อัตถากร ชั้น 9-10

ภาพที่ 3-21 แปลนตำแหน่งห้องเครือข่ายย่อยอาคารบุญชนะ อัตถากร ชั้น 9-10 ตู้เครือข่ายจะอยู่พื้นที่ทางเดินข้างลิฟท์



ภาพที่ 3-22 แปลนตำแหน่งห้องเครือข่ายย่อยอาคารบุญชนะ อัตถากร ชั้น 12

ภาพที่ 3-22 แปลนตำแหน่งห้องเครือข่ายย่อยอาคารบุญชนะ อัตถากร ชั้น 12 ตู้เครือข่ายจะอยู่ภายในห้องไฟฟ้าข้างลิฟท์ เป็น Wall Rack เป็นพื้นที่หอพักเข้าพื้นที่ด้วยการแจ้งเจ้าหน้าที่ดูแลหอพักหรือแม่บ้านหอพัก และเข้าห้องไฟฟ้าด้วยการแจ้งเจ้าหน้าที่ช่างประจำอาคาร ที่ ชั้น G

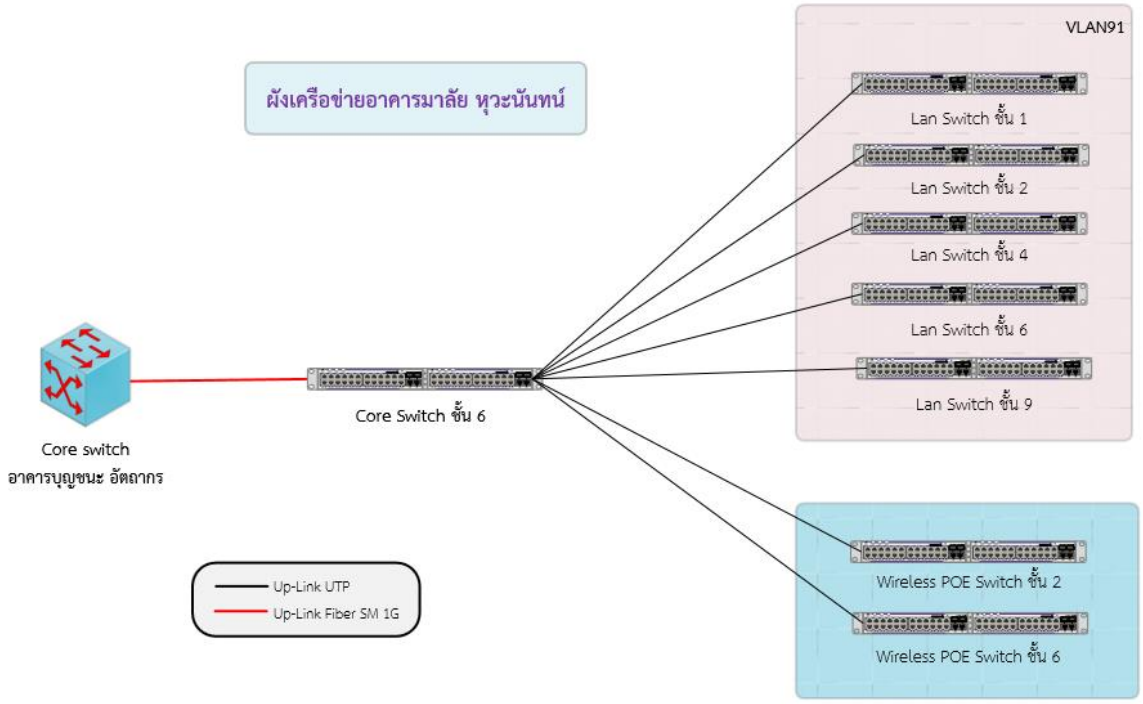


ภาพที่ 3-23 ผังเครือข่ายห้องสมุดสำนักบรรณสารการพัฒนา

ระบบเครือข่ายห้องสมุดสำนักบรรณสารการพัฒนา

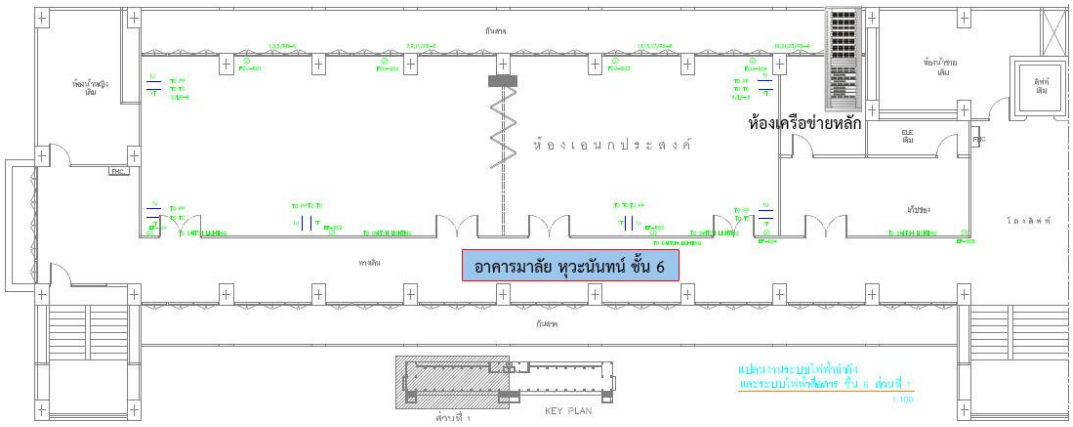
ภาพที่ 3-23 ผังเครือข่ายห้องสมุดสำนักบรรณสาร โดยสำนักจะเชื่อมเส้นทางเชื่อมระหว่างไฟร์วอลล์กับเซิร์ฟเวอร์โซนของห้องสมุด เพื่อความสะดวกในการบริหารจัดการ และแยกเครือข่ายภายในของห้องสมุดออกเป็น 2 โซน ได้แก่ โซนออฟฟิศและโซนแล็ป โซนแล็ปจะมีรูปแบบคล้ายกับห้องแล็บของสำนัก จะมีเครื่องแม่ข่ายเสมือน pfsence ทำหน้าที่เป็นไฟร์วอลล์และแจกไอพีแอดเดรสให้บริการเครือ่งลูกข่ายภายในของห้องแล็บ ใช้สำหรับบริหารจัดการโซนห้องแล็บ จะมีอีเธอร์เน็ต 2 พอร์ต พอร์ตหนึ่ง (WAN) เชื่อมกับโซนเซิร์เวอร์เพื่อเชื่อมต่ออินเทอร์เน็ตและเซิร์ฟเวอร์ต่าง ๆ ของห้องสมุด อีกพอร์ตหนึ่ง (LAN) เชื่อมไปยัง สวิชต์สำหรับแล็ปชั้น 2 มีอัพลิงค์เชื่อมไปยังสวิตช์ ชั้น 3 และ4 ที่แยกสวิชต์ออกมาสำหรับแล็ปโดยเฉพาะ

ระบบเครือข่ายอาคารมาลัย หุวะนันทน์



ภาพที่ 3-24 ผังเครือข่ายอาคารมาลัย หุวะนันทน์

อาคารมาลัย หุวะนันทน์เป็นอาคารสูง 9 ชั้น สายสัญญาณที่เชื่อมระหว่างอาคารเป็นสายไฟเบอร์ออฟติค ซิงเกิลโหมด มีเส้นทางหลัก ขนาดความเร็ว 1 GB เชื่อมระหว่างอาคารมาลัย หุวะนันทน์กับอาคารบุญชนะอัตถากร และอีกเส้นทางเชื่อมระหว่างอาคารมาลัย หุวะนันทน์กับอาคารชุบ กาญจนประกร ขนาดความเร็ว 1 GB สายสัญญาณที่เชื่อมระหว่างชั้นเป็น UTP ประเภท CAT5e และ CAT6 มีห้องเครือข่ายหลักอยู่ที่ชั้น 6 จากภาพที่ 3-24 ผังเครือข่ายอาคารมาลัย หุวะนันทน์ อธิบายลักษณะการเชื่อมต่อเครือข่ายภายในอาคาร ตู้เครือข่ายย่อยอยู่ชั้น 1 และชั้น 2 ส่วนระบบเครือข่ายไร้สายจะใช้ POE Switch ในการปล่อยสัญญาณและกระแสไฟฟ้าให้กับอุปกรณ์กระจายสัญญาณไร้สาย (Access Point) ติดตั้งอยู่ชั้น 2 และชั้น 6 ระบบเครือข่ายแลนจะมีการกำหนด VLAN เป็น **VLAN 91 ใช้สำหรับห้องเรียนและหน่วยงานที่อยู่ภายในอาคาร**

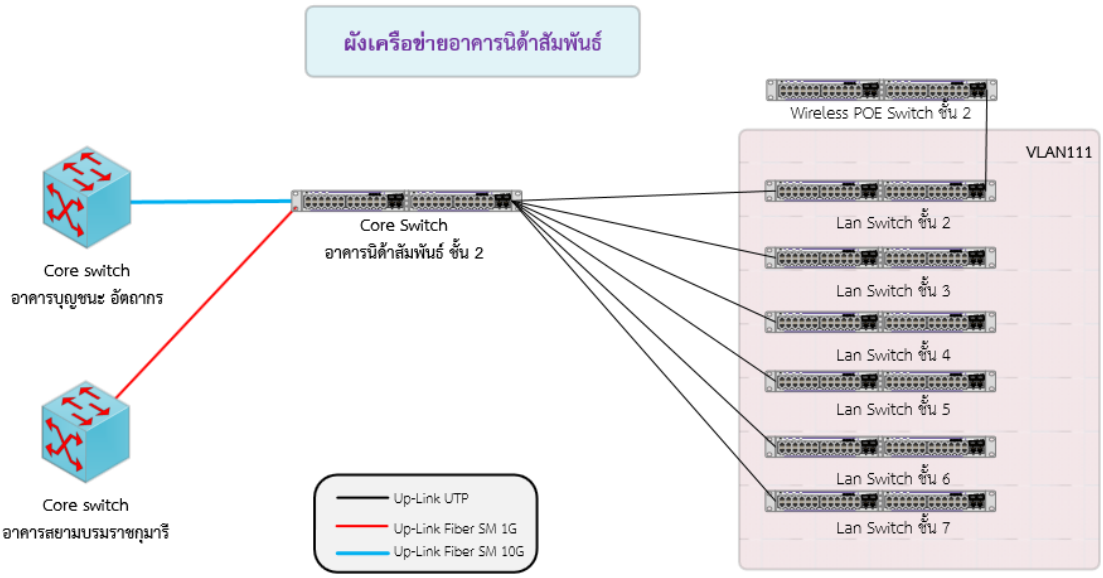


ภาพที่ 3-25 แปลนตำแหน่งห้องเครือข่ายหลักอาคารมาลัย หุวะนันทน์ ชั้น 6

ห้องเครือข่ายหลัก

ภาพที่ 3-25 แปลนตำแหน่งห้องเครือข่ายหลักอาคารมาลัย หุวะนันทน์ ชั้น 6 ห้องเครือข่ายจะอยู่ข้างห้องไฟฟ้าข้างลิฟท์ เป็นพื้นที่สำนักงานเข้าพื้นที่ด้วยการแจ้งเจ้าของหน่วยงาน หากเป็นวันหยุดสอบถามทางกลุ่มงานโยธาและซ่อมบำรุง และเข้าห้องเครือข่ายด้วยการกุญแจ อยู่ที่ตู้กุญแจอาคารสยามบรมราชกุมารี ชั้น 11 อาคารนี้ยังตู้เครือข่ายที่ชั้น 2 เป็น wall rack อยู่ข้างลิฟท์ ชั้น 1 เป็น wall rack อยู่ภายในสำนักงานคณะพัฒนาทรัพยากรมนุษย์

ระบบเครือข่ายอาคารนิด้าสัมพันธ์



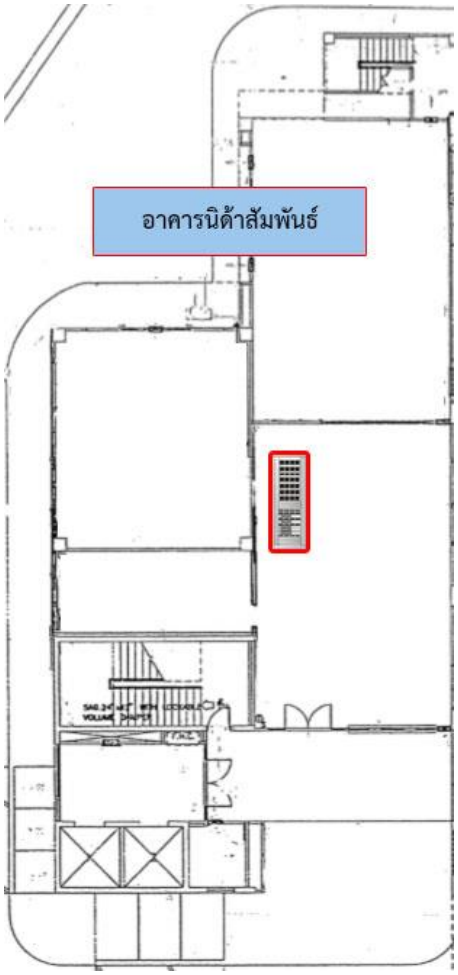
ภาพที่ 3-26 ผังเครือข่ายอาคารนิด้าสัมพันธ์

อาคารนิด้าสัมพันธ์เป็นอาคารสูง 7 ชั้น สายสัญญาณที่เชื่อมระหว่างอาคารเป็นสายไฟเบอร์ออฟติค ซิงเกิลโหมด เส้นทางแรก ขนาดความเร็ว 10 GB เชื่อมระหว่างอาคารนิด้าสัมพันธ์กับอาคารบุญชนะ อัตถากร และอีกเส้นทางเชื่อมระหว่างอาคารนิด้าสัมพันธ์กับอาคารสยามบรมราชกุมารี ขนาดความเร็ว 1 GB สายสัญญาณที่เชื่อมระหว่างชั้นเป็น UTP ประเภท CAT5e และ CAT6 มีห้องเครือข่ายหลักอยู่ที่ชั้น 2 จากภาพที่ 3-26 ผังเครือข่ายอาคารนิด้าสัมพันธ์ อธิบายลักษณะการเชื่อมต่อเครือข่ายภายในอาคาร ตู้เครือข่ายย่อยมีอยู่ทุกชั้นเป็นตู้ขนาด 12U แขวนอยู่ที่ผนังบริเวณทางเดิน ส่วนระบบเครือข่ายไร้สายจะใช้ POE Switch ในการปล่อยสัญญาณและกระแสไฟฟ้าให้กับอุปกรณ์กระจายสัญญาณไร้สาย (Access Point) ติดตั้งอยู่ชั้น 2 ระบบเครือข่ายแลนจะมีการกำหนด VLAN เป็น **VLAN 111 ใช้สำหรับหน่วยงานที่อยู่ภายในอาคาร**

ภาพที่ 3-27 แปลนตำแหน่งห้องเครือข่ายหลักอาคารนิด้าสัมพันธ์ ชั้น 2

ห้องเครือข่ายหลัก

ภาพที่ 3-27 แปลนตำแหน่งห้องเครือข่ายหลักอาคารนิด้าสัมพันธ์ ชั้น 2 ห้องเครือข่ายจะอยู่ข้างห้องสำนักงานของฝ่ายอาคารสถานที่ เข้าห้องเครือข่ายด้วยการกุญแจอยู่ที่ตู้กุญแจอาคารสยามบรมราชกุมารี ชั้น 11

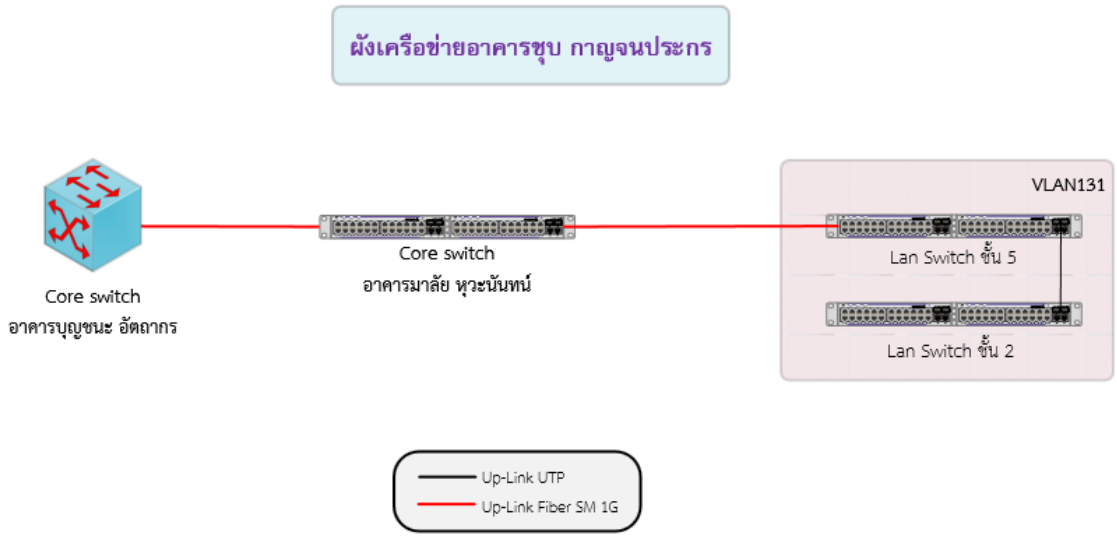


ภาพที่ 3-28 แปลนตำแหน่งตู้เครือข่ายย่อยอาคารนิด้าสัมพันธ์ ชั้น 3-7

ห้องเครือข่ายย่อยแต่ละชั้น

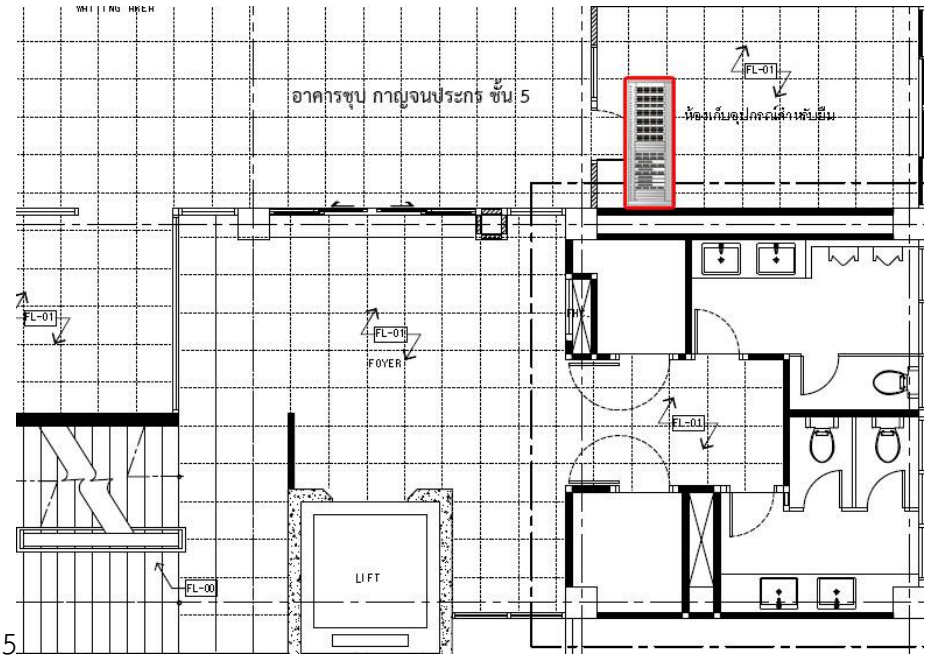
ภาพที่ 3-28 แปลนตำแหน่งตู้เครือข่ายย่อยอาคารนิด้าสัมพันธ์ ชั้น 3-7 แต่ละชั้นตู้จะอยู่ทางเดินภายในสำนักงาน เป็น wall rack อัพลิงค์เป็นสายสัญญาณ UTP

ระบบเครือข่ายอาคารชุบ กาญจนประกร



ภาพที่ 3-29 ผังเครือข่ายอาคารชุบ กาญจนประกร

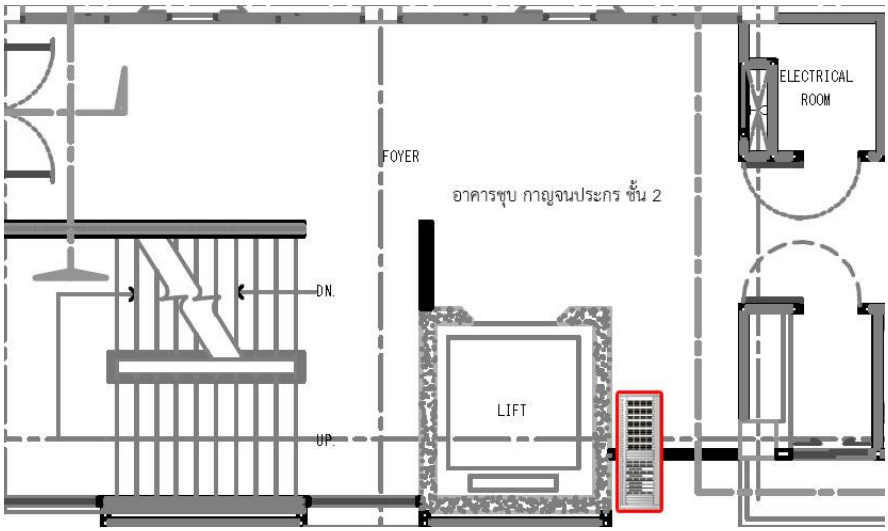
อาคารชุบ กาญจนประกรเป็นอาคารสูง 6 ชั้น สายสัญญาณที่เชื่อมระหว่างอาคารเป็นสายไฟเบอร์ออฟติค ซิงเกิลโหมด ขนาดความเร็ว 1 GB เชื่อมระหว่างอาคารชุบ กาญจนประกรกับอาคารกับอาคารมาลัย หุวะนันทน์ สายสัญญาณที่เชื่อมระหว่างชั้นเป็น UTP ประเภท CAT5e มีตู้เครือข่ายหลักอยู่ที่ชั้น 5 ภายในพื้นที่ของกลุ่มงานกิจการนักศึกษา ภาพที่ 3-29 ผังเครือข่ายอาคารชุบ กาญจนประกร อธิบายลักษณะการเชื่อมต่อเครือข่ายภายในอาคาร ตู้เครือข่ายย่อยมีอยู่ที่ชั้น 2 ทางเดินหน้าห้องน้ำ เป็นตู้ขนาด 12U แขวนอยู่ที่ผนัง อาคารนี้จะไม่มีระบบเครือข่ายไร้สายที่ติดตั้งโดยสถาบัน จะกระจายสัญญาณเครือข่ายไร้สายที่ติดตั้งโดยผู้ให้บริการเอกชน ระบบเครือข่ายแลนจะมีการกำหนด VLAN เป็น **VLAN 131 ใช้สำหรับหน่วยงานที่อยู่ภายในอาคาร**



ภาพที่ 3-30 แปลนตำแหน่งตู้เครือข่ายหลักอาคารชุบ กาญจนประกร ชั้น 5

ตู้เครือข่ายหลัก

ภาพที่ 3-30 แปลนตำแหน่งตู้เครือข่ายหลักอาคารชุบ กาญจนประกร ชั้น 5 ตู้จะอยู่ภายในสำนักงานกลุ่มงานกิจการนักศึกษา เป็น wall rack

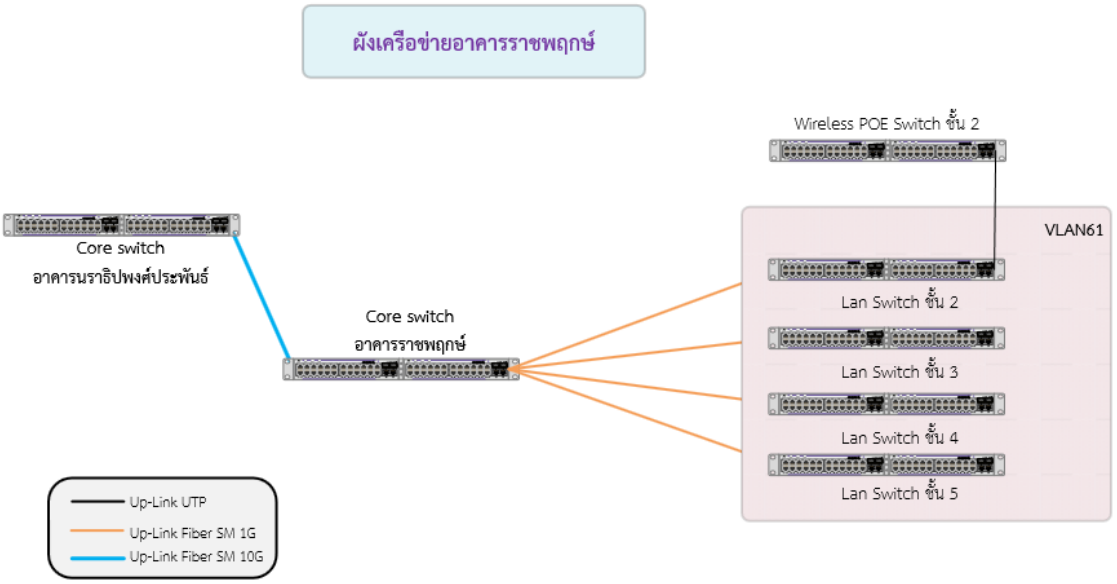


ภาพที่ 3-31 แปลนตำแหน่งตู้เครือข่ายย่อยอาคารชุบ กาญจนประกร ชั้น 2

ตู้เครือข่ายย่อย

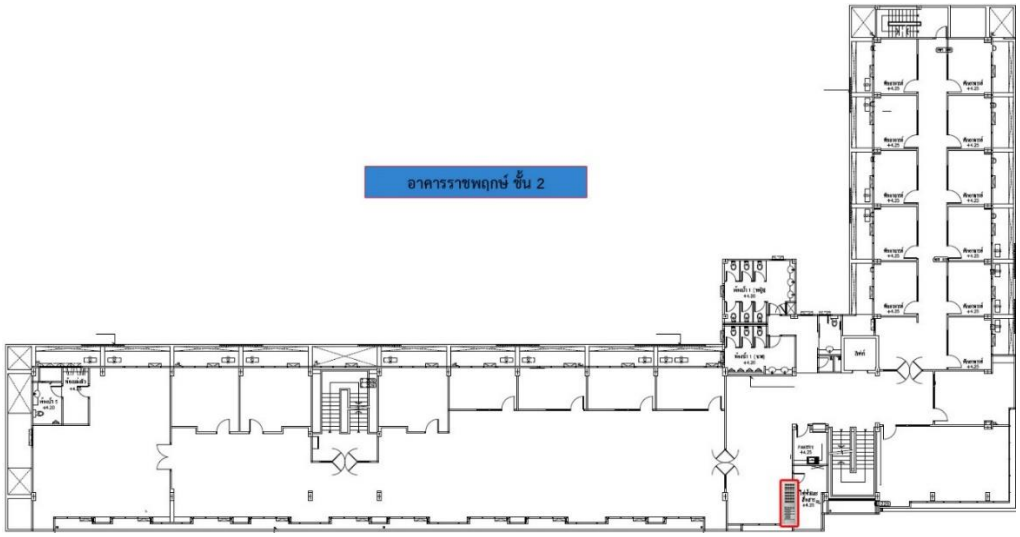
ภาพที่ 3-31 แปลนตำแหน่งตู้เครือข่ายย่อยอาคารชุบ กาญจนประกร ชั้น 2 ตู้จะอยู่ข้างลิฟท์ก่อนถึงห้องน้ำ เป็น wall rack มีอัพลิงค์เป็นสายสัญญาณ UTP ไปที่ชั้น 5

ระบบเครือข่ายอาคารราชพฤกษ์



ภาพที่ 3-32 ผังเครือข่ายอาคารราชพฤกษ์

อาคารราชพฤกษ์เป็นอาคารสูง 5 ชั้น สายสัญญาณที่เชื่อมระหว่างอาคารเป็นสายไฟเบอร์ออฟติค ซิงเกิลโหมด ขนาดความเร็ว 10 GB เชื่อมระหว่างอาคารราชพฤกษ์กับอาคารนราธิปพงศ์ประพันธ์ สายสัญญาณที่เชื่อมระหว่างชั้นเป็นไฟเบอร์ออฟติคมัลติโหมด 6 คอร์สำหรับระบบคอมพิวเตอร์ สายสัญญาณ UTP เป็นประเภท CAT6 มีห้องเครือข่ายหลักอยู่ที่ชั้น 2 จากภาพที่ 3-32 ผังเครือข่ายอาคารราชพฤกษ์ อธิบายลักษณะการเชื่อมต่อเครือข่ายภายในอาคาร ห้องเครือข่ายย่อยชั้น 1-5 ใช้สายไฟเบอร์ออฟติคประเภทมัลติโหมดเป็นอัพลิงค์มายังห้องเครือข่ายหลักชั้น 2 ขนาดความเร็ว 1 GB ส่วนระบบเครือข่ายไร้สายจะใช้ POE Switch ในการปล่อยสัญญาณและกระแสไฟฟ้าให้กับอุปกรณ์กระจายสัญญาณไร้สาย (Access Point) ติดตั้งอยู่ห้องเครือข่ายหลักชั้น 2 ระบบเครือข่ายแลนจะมีการกำหนด VLAN เป็น **VLAN 61 ใช้สำหรับทุกหน่วยงานภายในอาคาร**

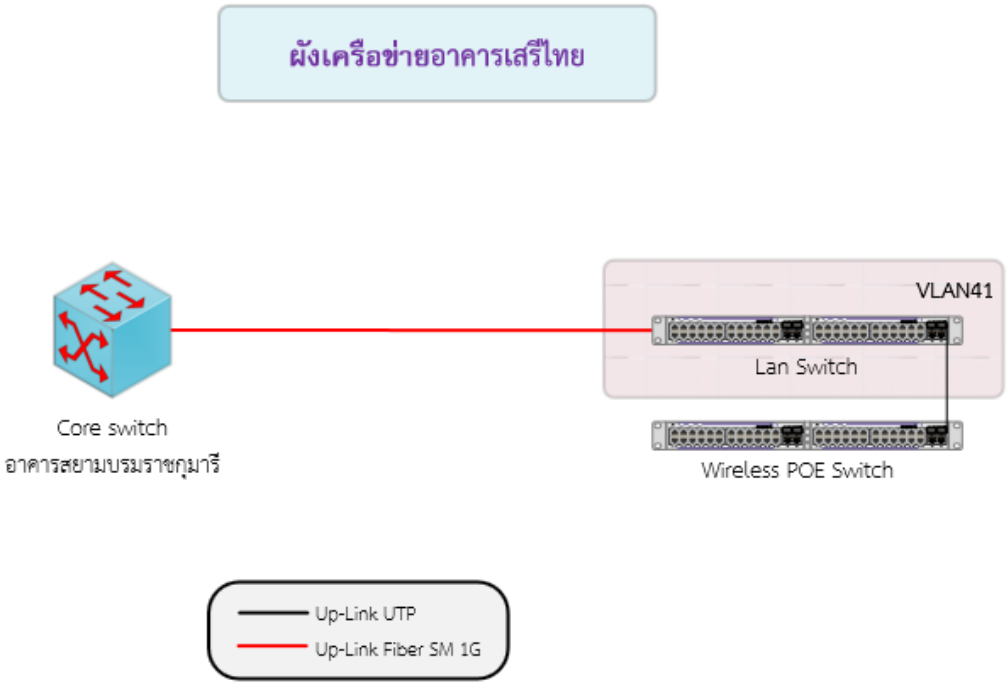


ภาพที่ 3-33 แปลนตำแหน่งตู้เครือข่ายหลักอาคารราชพฤกษ์ ชั้น 2

ห้องเครือข่ายหลักและห้องเครือข่ายย่อยแต่ละชั้น

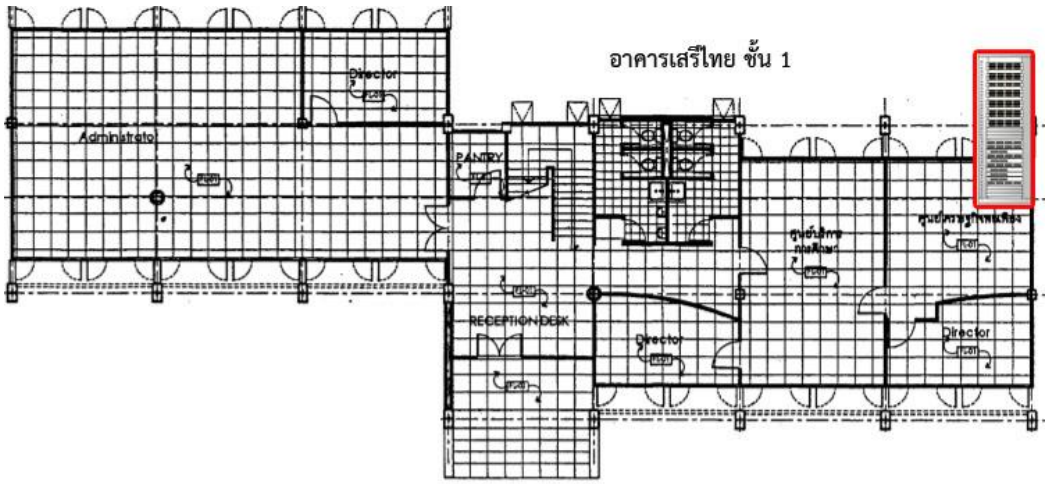
ภาพที่ 3-33 แปลนตำแหน่งตู้เครือข่ายหลักอาคารราชพฤกษ์ ชั้น 2 ห้องจะอยู่ข้างห้องเตรียมอาหารข้างบันได ห้องเครือข่ายย่อยชั้นอื่น ๆ จะอยู่ตำแหน่งเดียวกันคือข้างห้องเตรียมอาหารข้างบันได

ระบบเครือข่ายอาคารเสรีไทย



ภาพที่ 3-34 ผังเครือข่ายอาคารเสรีไทย

อาคารเสรีไทยเป็นอาคารสูง 3 ชั้น สายสัญญาณที่เชื่อมระหว่างอาคารเป็นสายไฟเบอร์ออฟติค ซิงเกิลโหมด ขนาดความเร็ว 1 GB เชื่อมระหว่างอาคารเสรีไทยกับอาคารสยามบรมราชกุมารี สายสัญญาณ UTP เป็นประเภท CAT6 อาคารนี้ไม่มีตู้เครือข่ายย่อย ห้องเครือข่ายหลักอยู่ที่ชั้น 1 จุดเครือข่ายแลนทุกจุดจะเดินสายมาที่ห้องเครือข่ายหลัก จากภาพที่ 3-34 ผังเครือข่ายอาคารเสรีไทยอธิบายลักษณะการเชื่อมต่อเครือข่ายภายในอาคาร ส่วนระบบเครือข่ายไร้สายจะใช้ POE Switch ในการปล่อยสัญญาณและกระแสไฟฟ้าให้กับอุปกรณ์กระจายสัญญาณไร้สาย (Access Point) ติดตั้งอยู่ห้องเครือข่ายหลักชั้น 1 ระบบเครือข่ายแลนจะมีการกำหนด VLAN เป็น **VLAN 41 ใช้สำหรับทุกหน่วยงานภายในอาคาร**

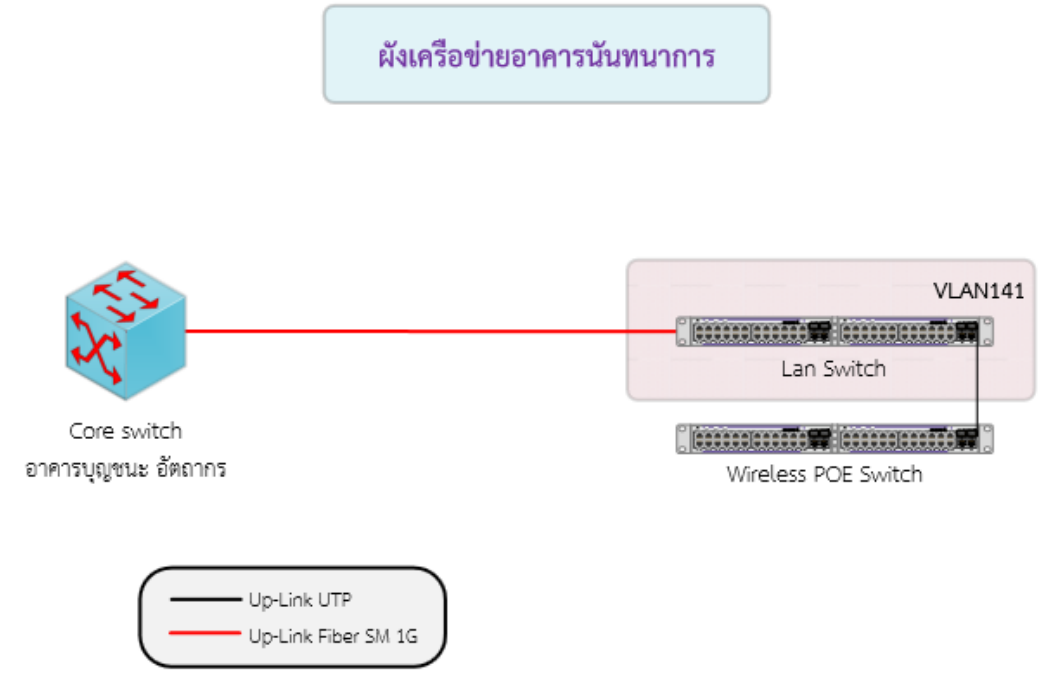


ภาพที่ 3-35 แปลนตำแหน่งตู้เครือข่ายหลักอาคารเสรีไทย ชั้น 1

ตู้เครือข่ายหลัก

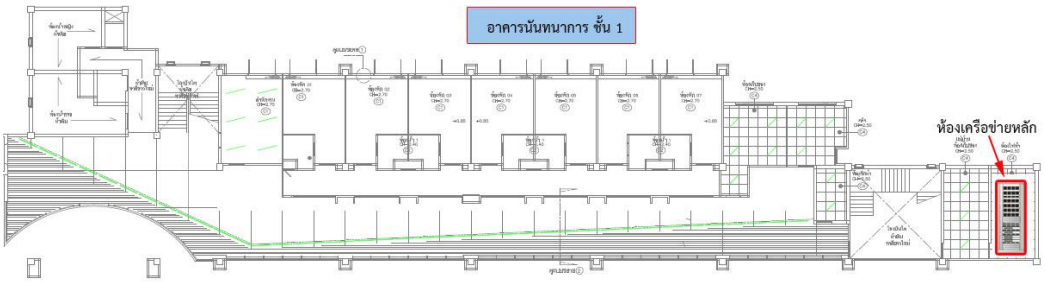
ภาพที่ 3-35 แปลนตำแหน่งตู้เครือข่ายหลักอาคารเสรีไทย ชั้น 1 ตู้จะอยู่ภายในห้องประชุมของศูนย์ศึกษาเศรษฐกิจพอเพียง ชั้นอื่น ๆ ไม่มีตู้เครือข่าย

ระบบเครือข่ายอาคารนันทนาการ



ภาพที่ 3-36 ผังเครือข่ายอาคารนันทนาการ

อาคารนันทนาการเป็นอาคารสูง 3 ชั้น สายสัญญาณที่เชื่อมระหว่างอาคารเป็นสายไฟเบอร์ออฟติค ซิงเกิลโหมด ขนาดความเร็ว 1 GB เชื่อมระหว่างอาคารนันทนาการกับอาคารสยามบรมราชกุมารี สายสัญญาณ UTP เป็นประเภท CAT6 อาคารนี้ไม่มีตู้เครือข่ายย่อย ห้องเครือข่ายหลักอยู่ที่ชั้น 1 จุดเครือข่ายแลนทุกจุดจะเดินสายมาที่ห้องเครือข่ายหลัก จากภาพที่ 3-36 ผังเครือข่ายอาคารนันทนาการ อธิบายลักษณะการเชื่อมต่อเครือข่ายภายในอาคาร ห้องเครือข่ายย่อยชั้น 1-5 ใช้สายไฟเบอร์ออฟติคประเภทมัลติโหมดเป็นอัพลิงค์มายังห้องเครือข่ายหลักชั้น 1 ขนาดความเร็ว 1 GB ส่วนระบบเครือข่ายไร้สายจะใช้ POE Switch ในการปล่อยสัญญาณและกระแสไฟฟ้าให้กับอุปกรณ์กระจายสัญญาณไร้สาย (Access Point) ติดตั้งอยู่ห้องเครือข่ายหลักชั้น 1 ระบบเครือข่ายแลนจะมีการกำหนด VLAN เป็น **VLAN 141 ใช้สำหรับทุกหน่วยงานภายในอาคาร**



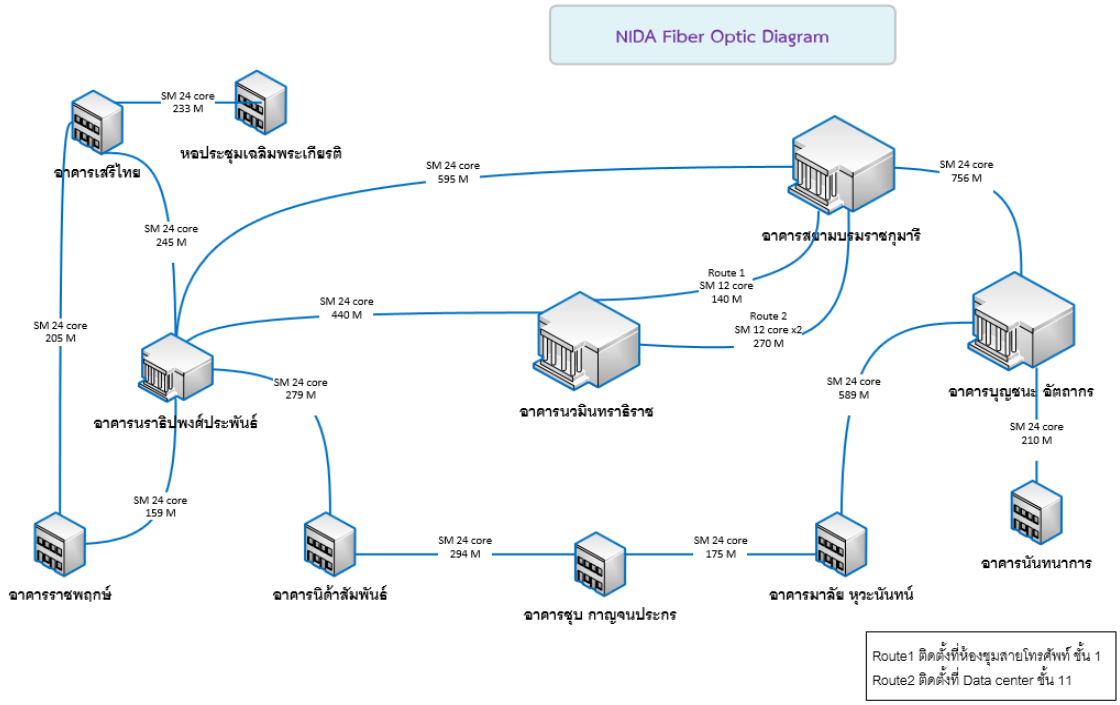
ภาพที่ 3-37 แปลนตำแหน่งตู้เครือข่ายหลักอาคารนันทนาการ ชั้น 1

ห้องเครือข่ายย่อยแต่ละชั้น

ภาพที่ 3-37 แปลนตำแหน่งตู้เครือข่ายหลักอาคารนันทนาการ ชั้น 1 ตู้จะอยู่ภายในห้องไฟฟ้า เข้าห้องขอกุญแจที่กลุ่มงานโยธาและซ่อมบำรุง ชั้นอื่น ๆ ไม่มีตู้เครือข่าย

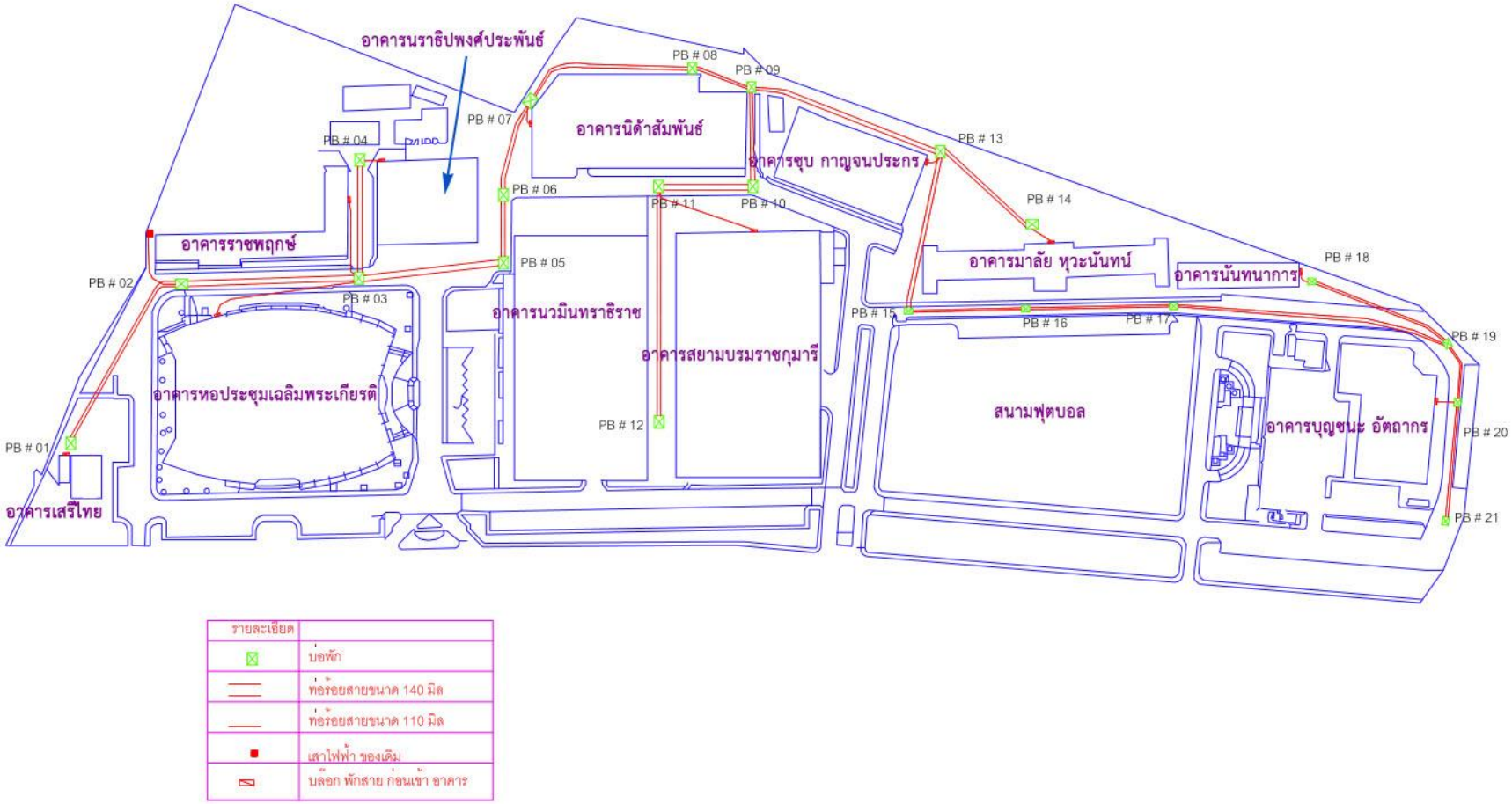
ระบบสายสัญญาณไฟเบอร์ออฟติค

องค์ประกอบที่สำคัญอย่างหนึ่งของระบบเครือข่ายคือสายสัญญาณ สายสัญญาณที่เชื่อมต่อระหว่างอาคารจะใช้สายไฟเบอร์ออฟติค และมีการเดินท่อร้อยสายใต้ดินเมื่อปี พ.ศ. ๒๕๕๕ สายสัญญาณที่เชื่อมระหว่างชั้น ภายในอาคารใหม่ ๆ จะเป็นสายไฟเบอร์ออฟติคทั้งหมด เพื่อให้เห็นภาพรวมทั้งหมด และเข้าใจได้ง่าย จึงจัดทำเป็นแผนผังโครงข่ายสายไฟเบอร์ออฟติคที่เชื่อมแต่ละอาคารพร้อมคำอธิบายเบื้องต้น เพื่อให้ผู้ดูแลระบบเครือข่ายคนอื่น ๆ หรือผู้ที่เกี่ยวข้อง สามารถนำไปใช้งานได้



ภาพที่ 3-38 ผังการเดินสายไฟเบอร์ออฟติค

ภาพที่ 3-38 ผังการเดินสายไฟเบอร์ออฟติคไปยังอาคารต่าง ๆ ในสถาบัน สายที่ใช้เดินจะเป็นสายประเภทซิงเกิลโหมด ขนาด 24 คอร์ ทุกอาคาร ยกเว้นสายที่เชื่อมระหว่าง Data Center ชั้น 11 อาคารสยามบรมราชกุมารี กับ ห้องเครือข่ายหลัก ชั้น 1 อาคารนวมินทราธิราช จะเป็นสายขนาด 12 คอร์ จำนวน 2 เส้น และสายเชื่อมระหว่างอาคารสยามบรมราชกุมารี ห้องชุมสายโทรศัพท์ ชั้น 1 กับห้องช่างประจำอาคารนวมินทราธิราช แต่ละอาคารจะมีเส้นทางเชื่อมกันระหว่างอาคาร อย่างน้อย 2 เส้นทาง ยกเว้นอาคารนันทนาการและอาคารหอประชุมเฉลิมพระเกียรติ ที่มีเพียงเส้นทางเดียว การที่มีเส้นทางเชื่อมต่อ 2 เส้นทาง สามารถใช้เป็นเส้นทางสำรองได้กรณีที่เส้นทางหนึ่งเกิดสายขาดใช้งานไม่ได้ สามารถไปใช้อีกเส้นทางหนึ่งทดแทน



ภาพที่ 3-39 แนวการเดินสายและบ่อพักสายไฟเบอร์ออฟติคลงดิน

ภาพที่ 3-39 แนวการเดินสายและบ่อพักสายไฟเบอร์ออฟติคลงดินและตำแหน่งของบ่อพักภายในสถาบัน บ่อพักที่ 1 จะเริ่มต้นที่อาคารเสรีไทยไปสิ้นสุดที่บ่อพักที่ 21 อยู่ด้านหลังอาคารบุญชนะ อัตถากร บริเวณริมรั้วหน้าโรงเก็บขยะ ทางเข้าออกของไฟเบอร์ออฟติคที่เชื่อมกับภายนอกสถาบันจะอยู่ที่บ่อพักที่ 2 กับบ่อพักที่ 21 ขึ้นอยู่กับแนวสายสัญญาณที่เชื่อมต่อจากภายนอกว่ามาจากถนนสายไหน หากมีการเดินสายเพิ่มเติม สามารถดูจากแผนผังและชี้จุดให้ผู้รับเหมาทราบแนวเพื่อประมาณการความยาวสายที่ต้องใช้ จะรู้ระยะทางและจำนวนบ่อพักที่ต้องเดินสายผ่าน

บ่อพักที่ 12 จะมีแนวท่อไปต่อกับบล็อกพักสายก่อนเข้าอาคารนวมินทราธิราช หากมีการเดินสายเข้าอาคารเพิ่มเติมจุดนี้จะใช้ไม่ได้ เนื่องจากแนวรางสายเข้าอาคารฝังอยู่ภายในเสาของอาคารและมีการหักมุม 90 องศา หลายตำแหน่ง และเป็นพื้นผิวปิดตาย ทางผู้รับเหมาจึงไม่สามารถเดินสายเพิ่มเติมเข้าอาคารตามแนวนี้ได้ เส้นทางที่เดินเข้าอาคารจะใช้บ่อพักที่ 11 เข้าบล็อกพักสายก่อนเข้าอาคารสยามบรมราชกุมารีเลียบขอบหลังคาชั้น 1 ข้ามอาคารไปยังเสาไฟฟ้าหลังอาคารนวมินทราธิราชใต้เสาไฟฟ้าจะมีช่องทะลุลงไปยังชั้นจอดรถใต้ดิน B1 แล้วเดินสายตามเพดานชั้นจอดรถทางขึ้นอยู่ห้องช่างประจำอาคารแล้วเข้าไปยังห้องเครือข่ายหลักที่อยู่ติดกัน

ภาพที่ 3-40 ภาพฝาบ่อพักไฟเบอร์ออฟติคลงดิน

ภาพที่ 3-40 ภาพฝาบ่อพักไฟเบอร์ออฟติคลงดินที่อยู่บนพื้นถนนภายในสถาบัน

ภาพที่ 3-41 บล็อกพักสายไฟเบอร์ก่อนเข้าอาคาร

ภาพที่ 3-41 บล็อกพักสายไฟเบอร์ก่อนเข้าอาคาร จากบ่อพักที่อยู่ตามพื้นถนนจะมีบ่อที่มีท่อขึ้นมาเหนือพื้นดินติดกับตัวอาคารใช้บล็อกครอบไว้ ดังภาพ แล้วค่อยเดินสายตามท่อเข้าไปเชื่อมดับแนวรางสายสัญญาณภายในอาคาร

บทที่ 4
ระบบสำรองไฟฟ้าของระบบเครือข่ายอาคารต่างๆ

ระบบไฟฟ้าเป็นปัจจัยสำคัญอันดับแรกในการให้บริการระบบเทคโนโลยีสารสนเทศและเครือข่ายในปัจจุบัน หากการจ่ายกระแสไฟฟ้าขัดข้องจะทำให้ไม่สามารถให้บริการได้อย่างต่อเนื่อง ขาดประสิทธิภาพและความน่าเชื่อถือ ส่งผลให้อุปกรณ์เครือข่าย เครื่องแม่ข่ายได้รับความเสียหายจากกระแสไฟฟ้าขัดข้อง ด้วยเหตุนี้จึงขออธิบายระบบไฟฟ้าที่จ่ายให้กับระบบเครือข่ายคอมพิวเตอร์ภายในอาคารต่าง ๆ ภายในสถาบัน ตามโครงสร้างของแต่ละอาคาร พร้อมกับระบบสำรองไฟ เครื่องกำเนิดไฟฟ้า ว่ามีที่อาคารใดบ้าง หากเกิดกระแสไฟฟ้าขัดข้องอาคารใดอาคารหนึ่งจะกระทบกับการให้บริการในอาคารอื่น ๆ หรือไม่ สามารถใช้ประโยชน์เวลาที่เกิดเหตุฉุกเฉิน การบำรุงรักษาระบบไฟฟ้าประจำอาคาร และช่วยให้ทราบถึงผลกระทบและการแจ้งผู้ใช้งานได้

การปิดระบบเครือข่ายและ Data Center เพื่อบำรุงรักษาระบบไฟฟ้า

สถาบันจะมีการบำรุงรักษาระบบไฟฟ้าเป็นประจำทุกปี เมื่อสำนักได้รับแจ้งจากกลุ่มงานโยธาและซ่อมบำรุง จำเป็นที่จะต้องทำการปิดการให้บริการระบบเครือข่ายและ Data Center จากประสบการณ์สามารถรวบรวมเป็นขั้นตอนการทำงานได้ ดังนี้

1. ปรึกษาทีมงานเพื่อสรุปวันเวลาที่ทำการปิด
2. แบ่งหน้าที่แจ้งไปยังผู้ได้รับผลกระทบภายในสถาบัน ดังนี้
    2.1. สำนักบรรณสารการพัฒนา
    2.2. คณะสถิติประยุกต์
    2.3. หน่วยงานที่นำเครื่องเซิร์ฟเวอร์มาฝากไว้ที่ Data Center
    2.4. หน่วยงานเจ้าของระบบต่าง ๆ
    2.5. หน่วยงานที่ใช้บริการเว็บโฮสติ้ง
3. แจ้งไปยังผู้ได้รับผลกระทบภายนอกสถาบัน ดังนี้
    3.1. UniNet แจ้งทางเมลไปที่ noc@uni.net.th เพื่อแจ้งผู้ดูแลระบบเครือข่ายของ UniNet และสมาชิกที่มีการเชื่อมโหนดกับสถาบันทราบ
    3.2. True แจ้งทางเมลไปที่ corpcare@true.co.th
4. ประชาสัมพันธ์ให้ผู้ใช้งานทราบ ตามช่องทางต่าง ๆ ดังนี้
    4.1. ระบบสื่อสารภายใน
    4.2. เว็บไซต์
    4.3. เฟสบุ๊ก
5. สำรองข้อมูลและคอนฟิคกูเรชั่น (จำเป็นมาก) ก่อนทำการการปิดระบบตามขั้นตอน
6. ทำการเปิดระบบและทดสอบการใช้งาน

อาคารสยามบรมราชกุมารี

อาคารสูง 15 ชั้น

ที่ตั้งห้องเครือข่ายหลัก ห้องแม่ข่ายชั้น 11 เป็นที่ตั้ง Data Center หลักของสถาบัน

ที่ตั้งห้องเครือข่ายย่อย ชั้น 2 ถึง ชั้น 15 มีห้องเครือข่ายย่อย ชั้น 1 และ M ไม่มีห้องเครือข่ายย่อย

ระบบสำรองไฟ

- UPS 160 KVA และต่อเข้ากับเครื่องกำเนิดไฟฟ้า และตู้เครือข่ายทุกชั้นเชื่อมเข้ากับเครื่องสำรองไฟ
- UPS 30 KVA และต่อเข้ากับเครื่องกำเนิดไฟฟ้า และตู้เครือข่ายทุกชั้นเชื่อมเข้ากับเครื่องสำรองไฟ

เครื่องกำเนิดไฟฟ้า มีเครื่องกำเนิดไฟฟ้า

ระบบปรับอากาศ ระบบปรับอากาศควบคุมความชื้นอัตโนมัติ (Precision air)

อาคาร	ระบบเครือข่าย LAN	ระบบเครือข่ายไร้สาย	ระบบเครือข่ายไร้สายทรู
อาคารสยามบรมราชกุมารี	X	X	X
อาคารนวมินทราธิราช	X	X	X
อาคารนราธิปพงศ์ประพันธ์	X	X	X
อาคารบุญชนะ อัตถากร	X	X	X
อาคารมาลัย หุวะนันทน์	X	X	X
อาคารนิด้าสัมพันธ์	X	X	X
อาคารชุบ กาญจนประกร	X	ไม่มี	X
อาคารเสรีไทย	X	X	X
อาคารนันทนาการ	X	X	X
อาคารหอประชุมเฉลิมพระเกียรติ	X	ไม่มี	X
อาคารราชพฤกษ์	X	X	X

ตารางที่ 4-1 ผลกระทบจากการเกิดกระแสไฟฟ้าขัดข้องอาคารสยามบรมราชกุมารี

อาคารนวมินทราธิราช

อาคารสูง 21 ชั้น

ที่ตั้งห้องเครือข่ายหลัก ห้องแม่ข่ายชั้น 1

ห้องเครือข่ายย่อย ชั้น 2 ถึง ชั้น 21 อยู่รวมกับห้องไฟฟ้าของอาคาร ระบบไฟฟ้าไม่มีการเดินไฟฟ้าแยกมาที่ห้องเครือข่ายหลักของอาคาร มีการต่อระบบไฟฟ้าเข้ากับเครื่องกำเนิดไฟฟ้า

ระบบสำรองไฟ UPS 15 KVA ของคณะสถิติประยุกต์ เครื่องสำรองไฟ UPS 1.5 KVA ติดตั้งชั้น 2 - 20 ชั้น 21

เครื่องกำเนิดไฟฟ้า มีเครื่องกำเนิดไฟฟ้า

ระบบปรับอากาศ ห้องเครือข่ายหลักติดตั้งเครื่องปรับอากาศ 2 เครื่อง ตั้งเวลาอัตโนมัติ

อาคาร	ระบบเครือข่าย LAN	ระบบเครือข่ายไร้สาย	ระบบเครือข่ายไร้สายทรู
อาคารสยามบรมราชกุมารี	√	√	√
อาคารนวมินทราธิราช	X	X	X
อาคารนราธิปพงศ์ประพันธ์	√	√	√
อาคารบุญชนะ อัตถากร	√	√	√
อาคารมาลัย หุวะนันทน์	√	√	√
อาคารนิด้าสัมพันธ์	√	√	√
อาคารชุบ กาญจนประกร	√	ไม่มี	√
อาคารเสรีไทย	√	√	√
อาคารนันทนาการ	√	√	√
อาคารหอประชุมเฉลิมพระเกียรติ	√	ไม่มี	√
อาคารราชพฤกษ์	√	√	√

ตารางที่ 4-2 ผลกระทบจากการเกิดกระแสไฟฟ้าขัดข้องอาคารนวมินทราธิราช

อาคารนราธิปพงศ์ประพันธ์

อาคารสูง 11 ชั้น

ที่ตั้งห้องเครือข่ายหลัก ห้องแม่ข่ายชั้น 2

ตู้เครือข่ายย่อย ชั้น 2 ถึง ชั้น 11

ระบบสำรองไฟ UPS 3 KVA เครื่องสำรองไฟ UPS 1.5 KVA ติดตั้งชั้น 3 และ ชั้น 8 - 10 ระบบไฟฟ้า ไม่มีการเดินไฟฟ้าแยกมาที่ห้องเครือข่ายหลักของอาคาร

เครื่องกำเนิดไฟฟ้า ไม่มีเครื่องกำเนิดไฟฟ้า

ระบบปรับอากาศ ห้องเครือข่ายหลักติดตั้งเครื่องปรับอากาศ 2 เครื่อง ตั้งเวลาอัตโนมัติ

อาคาร	ระบบเครือข่าย LAN	ระบบเครือข่ายไร้สาย	ระบบเครือข่ายไร้สายทรู
อาคารสยามบรมราชกุมารี	√	√	√
อาคารนวมินทราธิราช	√	√	√
อาคารนราธิปพงศ์ประพันธ์	X	X	X
อาคารบุญชนะ อัตถากร	√	√	√
อาคารมาลัย หุวะนันทน์	√	√	X
อาคารนิด้าสัมพันธ์	√	√	X
อาคารชุบ กาญจนประกร	√	ไม่มี	X
อาคารเสรีไทย	X	X	√
อาคารนันทนาการ	√	√	√
อาคารหอประชุมเฉลิมพระเกียรติ	X	ไม่มี	√
อาคารราชพฤกษ์	X	X	X

ตารางที่ 4-3 ผลกระทบจากการเกิดกระแสไฟฟ้าขัดข้องอาคารนราธิปพงศ์ประพันธ์

อาคารบุญชนะ อัตถากร

อาคารสูง 12 ชั้น

ที่ตั้งห้องเครือข่ายหลัก ห้องแม่ข่ายชั้น 5

ตู้เครือข่ายย่อย ชั้น 2 ถึง ชั้น 11

ระบบสำรองไฟ UPS 30 KVA และต่อเข้ากับเครื่องกำเนิดไฟฟ้า และตู้เครือข่ายทุกชั้นเชื่อมเข้ากับเครื่องสำรองไฟ ยกเว้นชั้น 11 ส่วนชั้น 2 – 4 ต่อเข้ากับเครื่องสำรองไฟของห้องสมุด

เครื่องกำเนิดไฟฟ้า มีเครื่องกำเนิดไฟฟ้า

ระบบปรับอากาศ ห้องเครือข่ายหลักติดตั้งเครื่องปรับอากาศ 2 เครื่อง ตั้งเวลาอัตโนมัติ

อาคาร	ระบบเครือข่าย LAN	ระบบเครือข่ายไร้สาย	ระบบเครือข่ายไร้สายทรู
อาคารสยามบรมราชกุมารี	√	√	√
อาคารนวมินทราธิราช	√	√	√
อาคารนราธิปพงศ์ประพันธ์	√	√	√
อาคารบุญชนะ อัตถากร	X	X	X
อาคารมาลัย หุวะนันทน์	X	X	√
อาคารนิด้าสัมพันธ์	√	√	√
อาคารชุบ กาญจนประกร	X	ไม่มี	√
อาคารเสรีไทย	√	√	√
อาคารนันทนาการ	X	√	X
อาคารหอประชุมเฉลิมพระเกียรติ	√	ไม่มี	√
อาคารราชพฤกษ์	√	√	√

ตารางที่ 4-4 ผลกระทบจากการเกิดกระแสไฟฟ้าขัดข้องอาคารบุญชนะ อัตถากร

อาคารมาลัย หุวะนันทน์

อาคารสูง 9 ชั้น

ที่ตั้งห้องเครือข่ายหลัก ห้องแม่ข่ายชั้น 6

ตู้เครือข่ายย่อย ชั้น 1, ชั้น 2, ชั้น 4

ระบบสำรองไฟ UPS 1.5 KVA จ่ายให้กับตู้เครือข่ายชั้น 6

เครื่องกำเนิดไฟฟ้า ไม่มีเครื่องกำเนิดไฟฟ้า

ระบบปรับอากาศ ห้องเครือข่ายหลักติดตั้งเครื่องปรับอากาศ 2 เครื่อง ตั้งเวลาอัตโนมัติ

อาคาร	ระบบเครือข่าย LAN	ระบบเครือข่ายไร้สาย	ระบบเครือข่ายไร้สาย ทรู
อาคารสยามบรมราชกุมารี	√	√	√
อาคารนวมินทราธิราช	√	√	√
อาคารนราธิปพงศ์ประพันธ์	√	√	√
อาคารบุญชนะ อัตถากร	√	√	√
อาคารมาลัย หุวะนันทน์	X	X	X
อาคารนิด้าสัมพันธ์	√	√	√
อาคารชุบ กาญจนประกร	X	ไม่มี	√
อาคารเสรีไทย	√	√	√
อาคารนันทนาการ	√	√	√
อาคารหอประชุมเฉลิมพระเกียรติ	√	ไม่มี	√
อาคารราชพฤกษ์	√	√	√

ตารางที่ 4-5 ผลกระทบจากการเกิดกระแสไฟฟ้าขัดข้องอาคารมาลัย หุวะนันทน์

อาคารนิด้าสัมพันธ์

อาคารสูง 7 ชั้น

ที่ตั้งห้องเครือข่ายหลัก ห้องแม่ข่ายชั้น 2

ตู้เครือข่ายย่อย ทุกชั้น

ระบบสำรองไฟ UPS 3 KVA จ่ายให้กับตู้เครือข่ายชั้น 2

เครื่องกำเนิดไฟฟ้า ไม่มีเครื่องกำเนิดไฟฟ้า

ระบบปรับอากาศ ห้องเครือข่ายหลักติดตั้งเครื่องปรับอากาศ 2 เครื่อง ตั้งเวลาอัตโนมัติ

อาคาร	ระบบเครือข่าย LAN	ระบบเครือข่ายไร้สาย	ระบบเครือข่ายไร้สายทรู
อาคารสยามบรมราชกุมารี	√	√	√
อาคารนวมินทราธิราช	√	√	√
อาคารนราธิปพงศ์ประพันธ์	√	√	√
อาคารบุญชนะ อัตถากร	√	√	√
อาคารมาลัย หุวะนันทน์	√	√	X
อาคารนิด้าสัมพันธ์	X	X	X
อาคารชุบ กาญจนประกร	√	ไม่มี	X
อาคารเสรีไทย	√	√	√
อาคารนันทนาการ	√	√	√
อาคารหอประชุมเฉลิมพระเกียรติ	√	ไม่มี	√
อาคารราชพฤกษ์	√	√	√

ตารางที่ 4-6 ผลกระทบจากการเกิดกระแสไฟฟ้าขัดข้องอาคารนิด้าสัมพันธ์

อาคารชุบ กาญจนประกร

อาคารสูง 6 ชั้น

ที่ตั้งห้องเครือข่ายหลัก ห้องแม่ข่ายชั้น 5

ตู้เครือข่ายย่อย ชั้น 5 และชั้น 2

ระบบสำรองไฟ UPS 650 KVA จ่ายให้กับตู้เครือข่ายชั้น 5

เครื่องกำเนิดไฟฟ้า ไม่มีเครื่องกำเนิดไฟฟ้า

ระบบปรับอากาศ ไม่มีเครื่องปรับอากาศ

อาคาร	ระบบเครือข่าย LAN	ระบบเครือข่ายไร้สาย	ระบบเครือข่ายไร้สายทรู
อาคารสยามบรมราชกุมารี	√	√	√
อาคารนวมินทราธิราช	√	√	√
อาคารนราธิปพงศ์ประพันธ์	√	√	√
อาคารบุญชนะ อัตถากร	√	√	√
อาคารมาลัย หุวะนันทน์	√	√	X
อาคารนิด้าสัมพันธ์	√	√	√
อาคารชุบ กาญจนประกร	X	ไม่มี	X
อาคารเสรีไทย	√	√	√
อาคารนันทนาการ	√	√	√
อาคารหอประชุมเฉลิมพระเกียรติ	√	ไม่มี	√
อาคารราชพฤกษ์	√	√	√

ตารางที่ 4-7 ผลกระทบจากการเกิดกระแสไฟฟ้าขัดข้องอาคารชุบ กาญจนประกร

อาคารเสรีไทย

อาคารสูง 3 ชั้น

ที่ตั้งห้องเครือข่ายหลัก ห้องแม่ข่ายชั้น 1

ตู้เครือข่ายย่อย ชั้น 1

ระบบสำรองไฟ ไม่มีเครื่องสำรองไฟฟ้า

เครื่องกำเนิดไฟฟ้า ไม่มีเครื่องกำเนิดไฟฟ้า

ระบบปรับอากาศ ไม่มีเครื่องปรับอากาศ

อาคาร	ระบบเครือข่าย LAN	ระบบเครือข่ายไร้สาย	ระบบเครือข่ายไร้สายทรู
อาคารสยามบรมราชกุมารี	√	√	√
อาคารนวมินทราธิราช	√	√	√
อาคารนราธิปพงศ์ประพันธ์	√	√	√
อาคารบุญชนะ อัตถากร	√	√	√
อาคารมาลัย หุวะนันทน์	√	√	√
อาคารนิด้าสัมพันธ์	√	√	√
อาคารชุบ กาญจนประกร	√	ไม่มี	√
อาคารเสรีไทย	X	X	X
อาคารนันทนาการ	√	√	√
อาคารหอประชุมเฉลิมพระเกียรติ	√	ไม่มี	X
อาคารราชพฤกษ์	√	√	√

ตารางที่ 4-8 ผลกระทบจากการเกิดกระแสไฟฟ้าขัดข้องอาคารเสรีไทย

อาคารนันทนาการ

อาคารสูง 3 ชั้น

ที่ตั้งห้องเครือข่ายหลัก ห้องแม่ข่ายชั้น 1

ตู้เครือข่ายย่อย ชั้น 1

ระบบสำรองไฟ ไม่มีเครื่องสำรองไฟฟ้า

เครื่องกำเนิดไฟฟ้า ไม่มีเครื่องกำเนิดไฟฟ้า

ระบบปรับอากาศ ไม่มีเครื่องปรับอากาศ

อาคาร	ระบบเครือข่าย LAN	ระบบเครือข่ายไร้สาย	ระบบเครือข่ายไร้สายทรู
อาคารสยามบรมราชกุมารี	√	√	√
อาคารนวมินทราธิราช	√	√	√
อาคารนราธิปพงศ์ประพันธ์	√	√	√
อาคารบุญชนะ อัตถากร	√	√	√
อาคารมาลัย หุวะนันทน์	√	√	√
อาคารนิด้าสัมพันธ์	√	√	√
อาคารชุบ กาญจนประกร	√	ไม่มี	√
อาคารเสรีไทย	√	√	√
อาคารนันทนาการ	X	ไม่มี	X
อาคารหอประชุมเฉลิมพระเกียรติ	√	ไม่มี	√
อาคารราชพฤกษ์	√	√	√

ตารางที่ 4-9 ผลกระทบจากการเกิดกระแสไฟฟ้าขัดข้องอาคารนันทนาการ

อาคารหอประชุมเฉลิมพระเกียรติ

อาคารสูง 2 ชั้น

ที่ตั้งห้องเครือข่ายหลัก ห้องแม่ข่ายชั้น 1

ตู้เครือข่ายย่อย ชั้น 1

ระบบสำรองไฟ ไม่มีเครื่องสำรองไฟฟ้า

เครื่องกำเนิดไฟฟ้า ไม่มีเครื่องกำเนิดไฟฟ้า

ระบบปรับอากาศ ไม่มีเครื่องปรับอากาศ

อาคาร	ระบบเครือข่าย LAN	ระบบเครือข่ายไร้สาย	ระบบเครือข่ายไร้สายทรู
อาคารสยามบรมราชกุมารี	√	√	√
อาคารนวมินทราธิราช	√	√	√
อาคารนราธิปพงศ์ประพันธ์	√	√	√
อาคารบุญชนะ อัตถากร	√	√	√
อาคารมาลัย หุวะนันทน์	√	√	√
อาคารนิด้าสัมพันธ์	√	√	√
อาคารชุบ กาญจนประกร	√	ไม่มี	√
อาคารเสรีไทย	√	√	√
อาคารนันทนาการ	√	√	√
อาคารหอประชุมเฉลิมพระเกียรติ	X	ไม่มี	X
อาคารราชพฤกษ์	√	√	√

ตารางที่ 4-10 ผลกระทบจากการเกิดกระแสไฟฟ้าขัดข้องอาคารหอประชุมเฉลิมพระเกียรติ

อาคารราชพฤกษ์

อาคารสูง 5 ชั้น

ที่ตั้งห้องเครือข่ายหลัก ห้องแม่ข่ายชั้น 2

ตู้เครือข่ายย่อย ทุกชั้น

ระบบสำรองไฟ มีเครื่องสำรองไฟฟ้าขนาด 20 KVA

เครื่องกำเนิดไฟฟ้า ไม่มีเครื่องกำเนิดไฟฟ้า

ระบบปรับอากาศ ห้องเครือข่ายหลักติดตั้งเครื่องปรับอากาศ 2 เครื่อง ตั้งเวลาอัตโนมัติ

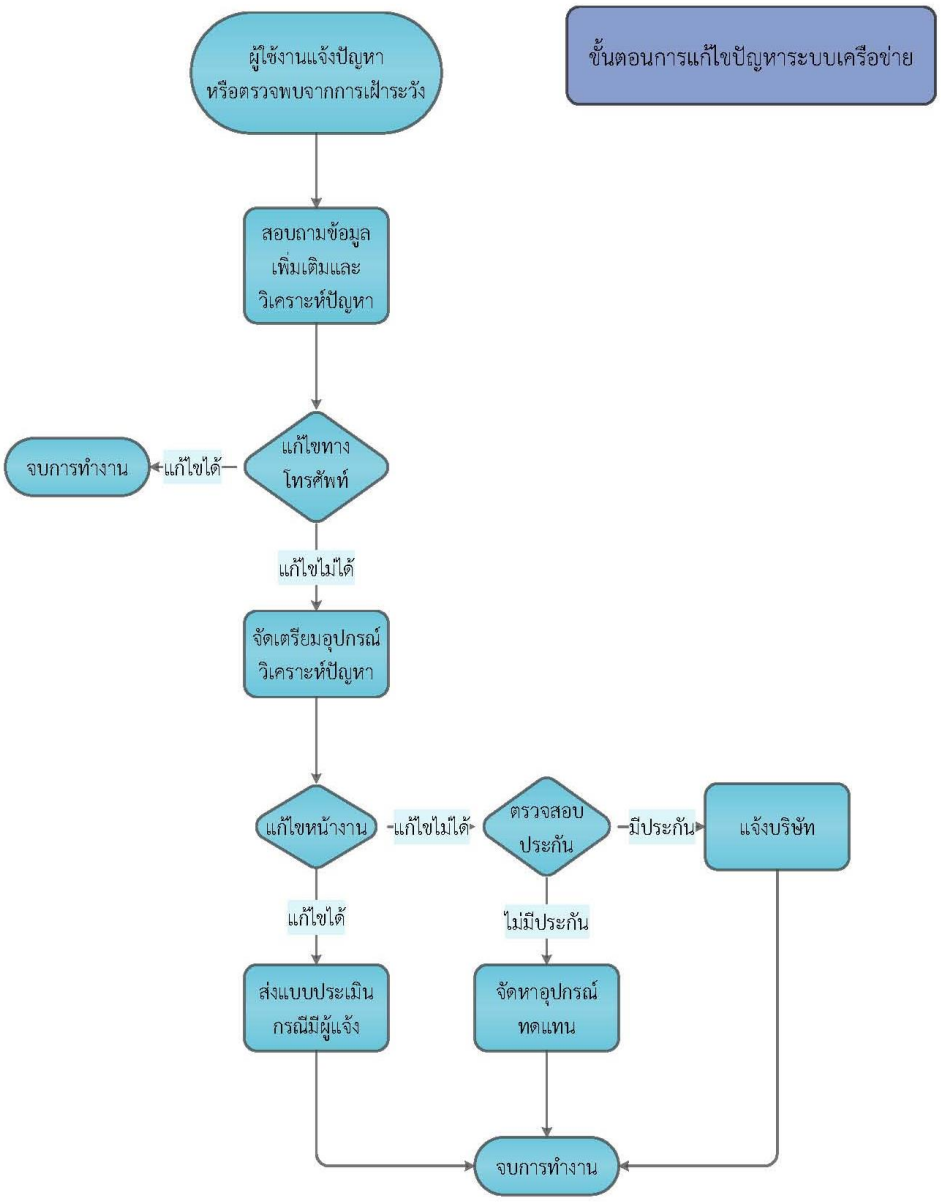
อาคาร	ระบบเครือข่าย LAN	ระบบเครือข่ายไร้สาย	ระบบเครือข่ายไร้สายทรู
อาคารสยามบรมราชกุมารี	√	√	√
อาคารนวมินทราธิราช	√	√	√
อาคารนราธิปพงศ์ประพันธ์	√	√	√
อาคารบุญชนะ อัตถากร	√	√	√
อาคารมาลัย หุวะนันทน์	√	√	√
อาคารนิด้าสัมพันธ์	√	√	√
อาคารชุบ กาญจนประกร	√	ไม่มี	√
อาคารเสรีไทย	√	√	√
อาคารนันทนาการ	√	√	√
อาคารหอประชุมเฉลิมพระเกียรติ	√	ไม่มี	√
อาคารราชพฤกษ์	X	X	X

ตารางที่ 4-11 ผลกระทบจากการเกิดกระแสไฟฟ้าขัดข้องอาคารราชพฤกษ์

บทที่ 5
การดูแลระบบเครือข่าย

การดูแลระบบเครือข่ายประกอบไปด้วยทั้งฮาร์ดแวร์ ซอฟต์แวร์ และสายสัญญาณ หลายประเภทมาทำงานร่วมกัน และส่วนใหญ่จะต้องทำงานตลอดเวลาโดยไม่มีการปิดเครื่องจนถึงระยะเวลาหนึ่งก็อาจจะทำงานเกินกำลังหรือทำงานผิดพลาดได้ เพื่อให้สามารถบริการเครือข่ายได้ตลอดเวลาและดูแลอุปกรณ์มากมายที่กระจัดกระจายอยู่ตามอาคารต่าง ๆ ทั่วสถาบัน ผู้ดูแลเครือข่ายจำเป็นต้องมีเครื่องมือที่ใช้ในเฝ้าระวังทดสอบตรวจเช็ค คอนฟิคกูเรชั่นต่าง ๆ ในบทนี้จะกล่าวถึงการใช้เครื่องมือต่างๆ ในการดูแลเบื้องต้น เครื่องมือในการเฝ้าระวัง และคำสั่งในการคอนฟิคกูเรชั่นอุปกรณ์ที่ใช้บ่อย ๆ เซิร์ฟเวอร์ที่เก็บคอนฟิคกูเรชั่นของอุปกรณ์ทั้งหมด ตู้เก็บเอกสารคู่มือ สายคอนโซล อะไหล่สำรอง เพื่อให้ผู้ดูแลเครือข่ายคนอื่นรับรู้ และสามารถดูแลได้อย่างต่อเนื่อง

ขั้นตอนการปฏิบัติงานในการแก้ไขปัญหาระบบเครือข่าย



ภาพที่ 5-1 ขั้นตอนการแก้ไขปัญหาระบบเครือข่าย

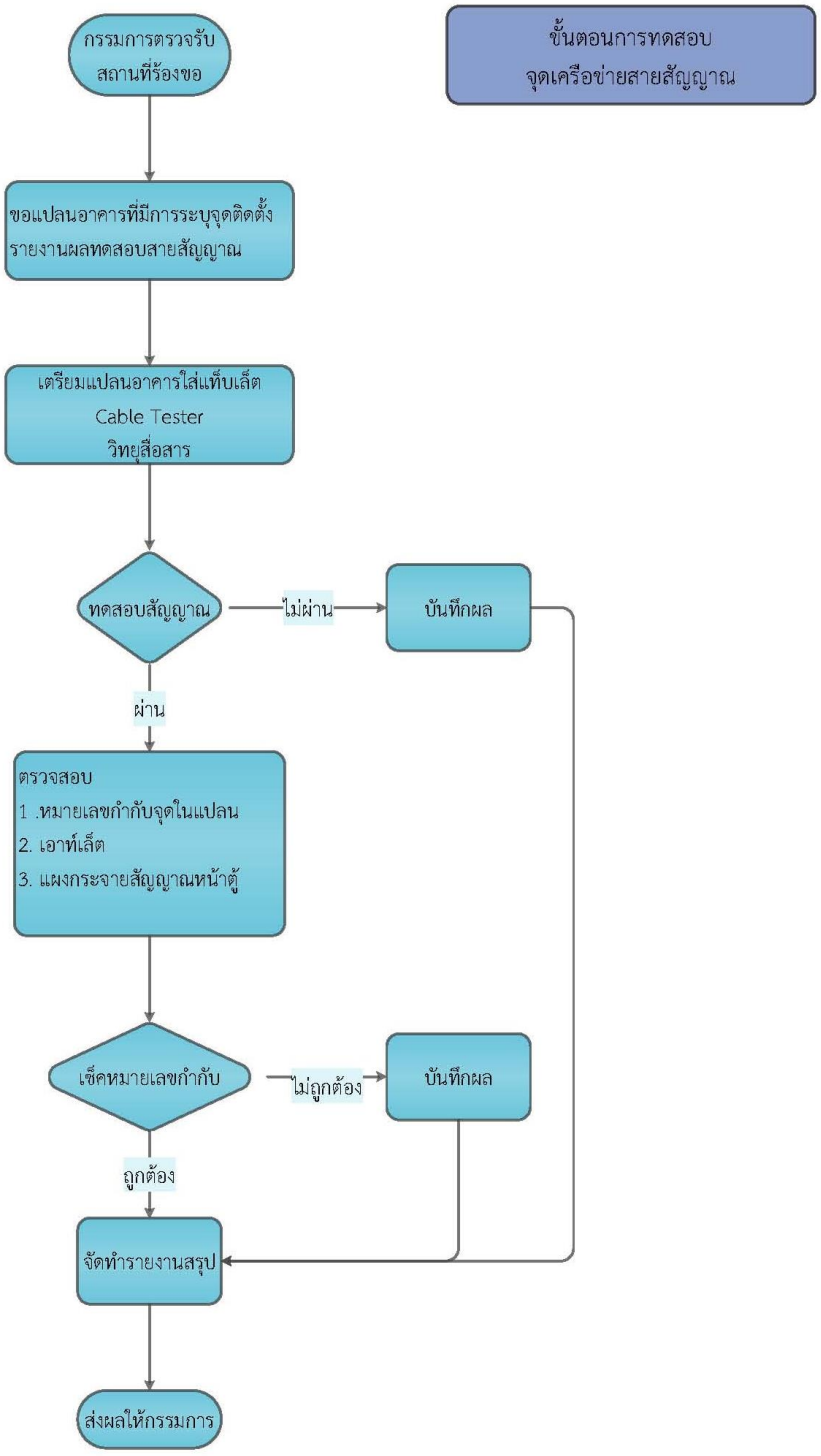
จากประสบการณ์ที่ได้พบกับปัญหาและมีการแก้ไขร่วมกับทีมงานมา สามารถจัดทำเป็นขั้นตอนการแก้ไขปัญหา ดังนี้

1. การรับแจ้งปัญหาการใช้งานระบบเครือข่าย ได้จากสองช่องทาง
   1.1. ผู้ใช้งานแจ้งปัญหามาที่ Helpdesk เจ้าหน้าที่ Helpdesk ส่งงานเข้าระบบ mes เข้าระบบส่งต่องานมาที่กลุ่มงานโครงสร้าง
   1.2. ตรวจพบปัญหาจากการเข้าระบบดูแลและบริหารระบบเครือข่าย และพบความผิดปกติ
2. โทรสอบถามอาการเพิ่มเติม

2.1. แก้ไขปัญหาทางโทรศัพท์
2.2. ทำการรีโมทไปที่อุปกรณ์เครือข่าย ณ จุดที่ให้บริการ และให้ผู้ใช้บริการทดสอบ
2.3. หากยังแก้ไขไม่ได้นัดหมายเวลาที่ผู้รับบริการสะดวกให้เข้าดำเนินการ
2.4. กรณีที่พบปัญหาจากเฝ้าระวัง โทรสอบถามผู้ใช้งานในบริเวณนั้น ว่าเกิดปัญหาอะไรบ้าง ใช้งานได้หรือไม่ เช่น กรณีไฟฟ้าดับ หรือมีการซ่อมบำรุง เป็นต้น

3. วิเคราะห์ปัญหา และเตรียมอุปกรณ์เพื่อแก้ไขหน้างาน
4. ทำการแก้ไขปัญหาที่เครื่องผู้ใช้งาน หรืออุปกรณ์เครือข่ายที่ให้บริการบริเวณนั้น
5. แก้ไขปัญหาเสร็จสิ้น กรณีมีผู้แจ้งทำการส่งแบบประเมิน
6. หากแก้ไขปัญหาไม่ได้
   6.1. กรณีสาเหตุเกิดจากเครื่องผู้ใช้งาน แจ้งความคืบหน้าและวิธีแก้ไข เช่น ต้องส่งเครื่องให้ฝ่ายบริการทำการฟอร์แมตเครื่อง หรือต้องซื้ออะไหล่ทดแทน
   6.2. กรณีสาเหตุเกิดจากอุปกรณ์เครือข่ายตรวจสอบว่ามีประกันหรือไม่ หากมีประกันโทรแจ้งบริษัทมาแก้ไข หากไม่มีประกันตรวจเช็คว่ามีอะไหร่สำรองที่เป็นยี่ห้อและรุ่นเดียวกันหรือไม่ หากไม่มีหายี่ห้อและรุ่นที่ใกล้เคียงมาทดแทน หรือปรึกษากันภายในกลุ่มงานเพื่อหาวิธีทางเลือก
   6.3. กรณีสาเหตุเกิดจากสายสัญญาณที่เป็นอัพลิงค์ชำรุดหรือถูกสัตว์กัดแทะ ต้องรอการซ่อมแซม แจ้งหน่วยงานที่ได้รับผลกระทบ และแจ้งฝ่ายการเงินดำเนินเรื่องจัดจ้างเพื่อซ่อมแซม และมองหาวิธีให้ใช้งานชั่วคราวได้

ขั้นตอนการปฏิบัติงานการทดสอบจุดเครือข่ายสายสัญญาณ



ภาพที่ 5-2 ขั้นตอนการทดสอบจุดเครือข่ายสายสัญญาณ

ภาพที่ 5-2 ขั้นตอนการทดสอบจุดเครือข่ายสายสัญญาณ เป็นขั้นตอนที่จะดำเนินการเมื่อมีการก่อสร้างอาคารหรือปรับปรุงอาคาร แล้วมีการเดินสายเครือข่ายใหม่ ต้องมีการทดสอบสายสัญญาณก่อนทำการตรวจรับส่งมอบสถานที่ เนื่องจากกรณีนี้ไม่ได้ดำเนินการบ่อย อาจทำให้หลงลืมขั้นตอนการตรวจสอบได้ จึงได้เขียนเป็นขั้นตอนการดำเนินการเพื่อให้ผู้ปฏิบัติงานสามารถดูรายละเอียดก่อนดำเนินการ เมื่อไปดำเนินการตรวจสอบจะได้มีความครบถ้วน ซึ่งจากการที่ทีมงานได้ไปดำเนินการตรวจสอบมาหลายอาคารทำให้เริ่มมีประสบการณ์ในการตรวจสอบและทราบปัญหา สรุปเป็นขั้นตอน ดังนี้

1. มีการร้องขอจากหน่วยงาน หรือเจ้าหน้าที่มีส่วนร่วมเป็นกรรมการตรวจรับ
2. ขอแบบแปลนอาคาร (as-build) ที่มีการกำหนดจุดเครือข่ายในแปลน และรายงานผลทดสอบสายสัญญาณ
3. นัดวันเข้าทดสอบกับผู้รับเหมาและจัดเตรียมทีมงานอย่างน้อย 4 คน
4. จัดเตรียมอุปกรณ์ ดังนี้
   4.1. นำแปลนอาคารใส่แท็ปเล็ต สะดวกกว่ากระดาษสามารถขยายเพื่อดูรายละเอียดได้
   4.2. จัดทำตารางใส่รายละเอียด หมายเลขจุด ชั้น ผลการทดสอบ หมายเหตุ
   4.3. วิทยุสื่อสาร เนื่องจากในสถานที่จริงจะไม่ค่อยมีสัญญาณโทรศัพท์มือถือและบางแห่งไม่มีสัญญาณจึงต้องใช้วิทยุสื่อสารแทน หรืออาจใช้แอปพลิเคชัน Line ช่วยเพิ่มเติม เพื่อสื่อสารระหว่างผู้ทดสอบที่อยู่ตามจุดต่าง ๆ กับผู้ที่อยู่หน้าตู้เครือข่าย
   4.4. อุปกรณ์ทดสอบสายสัญญาณ (Cable Tester)
5. ทำการทดสอบ
6. เช็คหมายเลขกำกับในแปลนกับจุดที่ทดสอบและจุดที่หน้าตู้เครือข่ายว่าตรงกันหรือไม่ และตรวจความเรียบร้อย เต้ารับ การจัดระเบียบสาย ความแข็งแรง
7. บันทึกและจัดทำรายงานผลการทดสอบ
8. ส่งผลการทดสอบให้กรรมการตรวจรับสถานที่เพื่อแจ้งผู้รับเหมา

เครื่องมือที่ใช้ในการตรวจสอบ

Cable Tester

เป็นอุปกรณ์ที่ใช้ในการทดสอบสายสัญญาณ UTP เพื่อใช้วิเคราะห์หาสาเหตุของสายสัญญาณว่าเสื่อมสภาพ สายขาดหรือชำรุด ใช้หาความยาวของสายเพื่อทราบตำแหน่งที่ชำรุด สามารถตรวจเช็คได้ว่าคู่สายไหนที่ขาด ผ่านมาตรฐาน เช่น CAT5 CAT5E CAT6 เป็นต้น ช่วยลดขั้นตอนในการวิเคราะห์ปัญหาหากตรวจสอบแล้วสายไม่มีปัญหาจะได้ตรวจหาสาเหตุอื่น

ภาพที่ 5-3 อุปกรณ์ทดสอบสายสัญญาณ (Cable Tester)

สายคอนโซล (Console Cable)

การแก้ไขปัญหาหน้างานบางครั้ง จำเป็นต้องเชื่อมต่ออุปกรณ์เครือข่ายเพื่อตรวจสอบการตั้งค่าคอนฟิคกูเรชั่น สายคอนโซลเป็นสิ่งที่ต้องนำไปด้วย อุปกรณ์เครือข่ายแต่ละยี่ห้อ จะมีสายคอนโซลแตกต่างกัน สายคอนโซลที่ใช้ในสถาบันแตกต่างกันหลายแบบ ดังนี้

USB to RS232 Adapter เป็นอุปกรณ์ที่ต้องมีไว้เสมอสำหรับเชื่อมต่อระหว่างโน้ตบุ๊คกับสายคอนโซลชนิดต่าง ๆ เนื่องจากโน้ตบุ๊คในปัจจุบันจะไม่มีพอร์ต RS232 ซึ่งมีไว้เชื่อมต่อกับพอร์ต DB9 ที่เป็นพอร์ตส่วนใหญ่ของสายคอนโซล

Cisco Console RJ45 to DB9 สำหรับเชื่อมต่อกับอุปกรณ์เครือข่ายยี่ห้อ Cisco เช่น Router และ switch นอกจากนี้ยังสามารถคอนโซล Access Point ยี่ห้อ Alcatel-Lucent ได้

Cisco Console DB9 to DB9 สำหรับเชื่อมต่อกับอุปกรณ์เครือข่ายยี่ห้อ Cisco เช่น Switch SF300 ใช้งานที่ตู้เครือข่ายโทรศัพท์ทุกชั้นในอาคารนวมินทราธิราช

Cisco Console DB9 to DB9 สำหรับเชื่อมต่อกับอุปกรณ์เครือข่ายยี่ห้อ Cisco เช่น Switch SF300 ใช้งานที่ตู้เครือข่ายโทรศัพท์ทุกชั้นในอาคารนวมินทราธิราช

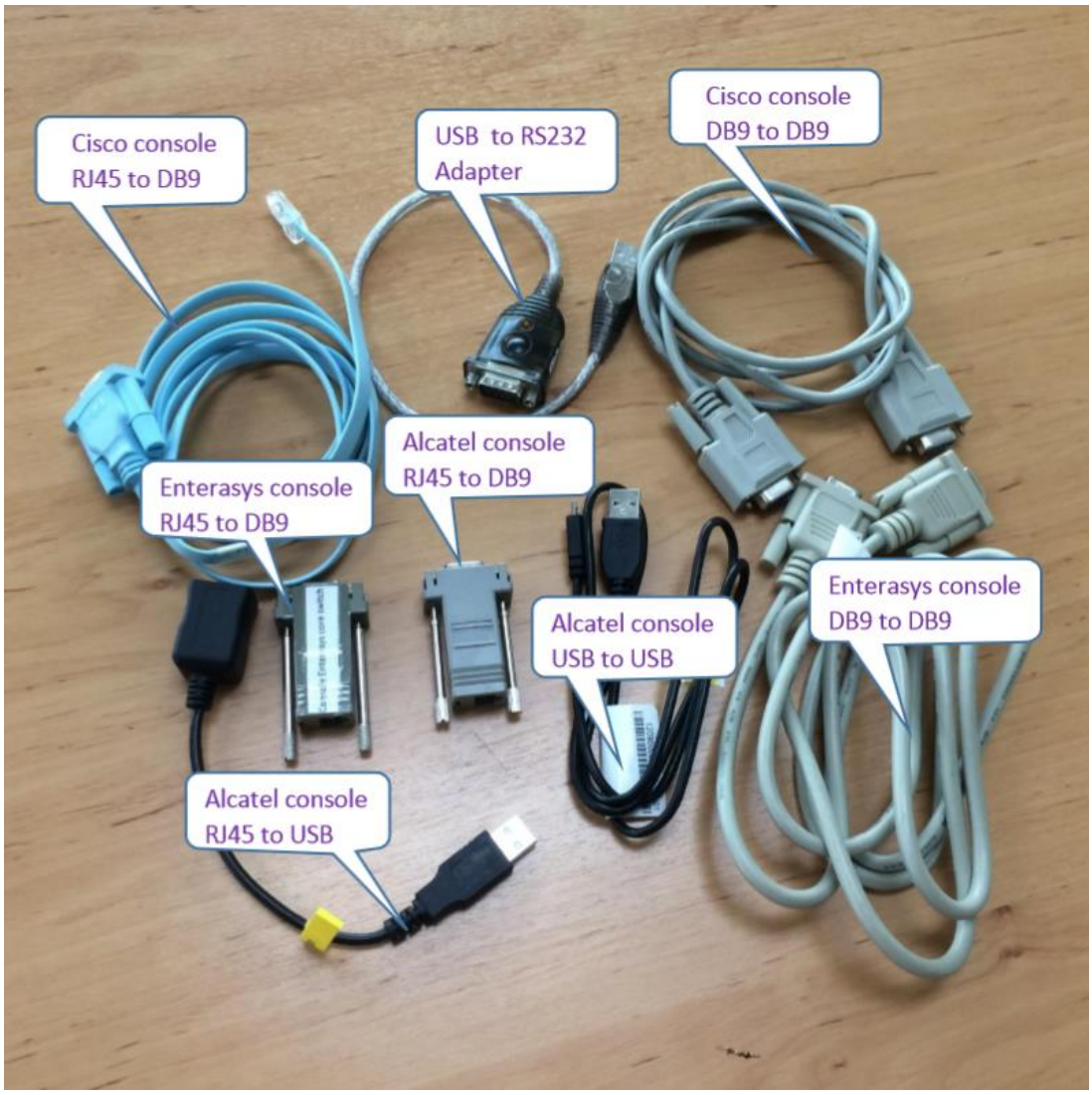
Enterasys Console RJ45 to DB9 สำหรับเชื่อมต่อกับอุปกรณ์เครือข่ายยี่ห้อ Enterasys เช่น Core Switch S4 Series ใช้งานที่ตู้เครือข่ายหลักในอาคารนวมินทราธิราช

Enterasys Console DB9 to DB9 สำหรับเชื่อมต่อกับอุปกรณ์เครือข่ายยี่ห้อ Enterasys เช่น Switch รุ่น C5K125 รุ่น C5G125 ใช้งานที่ตู้เครือข่ายคอมพิวเตอร์ทุกชั้นในอาคารนวมินทราธิราช

Alcatel Console RJ45 to USB สำหรับเชื่อมต่อกับอุปกรณ์เครือข่ายยี่ห้อ Alcatel-Lucent เช่น Switch รุ่น 6900

Alcatel Console USB to USB สำหรับเชื่อมต่อกับอุปกรณ์เครือข่ายยี่ห้อ Alcatel-Lucent เช่น Switch รุ่น 6860 ใช้งานเป็น Core Switch ในอาคารนราธิปพงศ์ประพันธ์

Alcatel Console RJ45 to DB9 สำหรับเชื่อมต่อกับอุปกรณ์เครือข่ายยี่ห้อ Alcatel-Lucent เช่น Switch รุ่น 9800E รุ่น 6850 รุ่น 6424 รุ่น 6450 ส่วนใหญ่จะใช้งานอยู่ทุกอาคาร



ภาพที่ 5-4 สายคอนโซลอุปกรณ์เครือข่ายประเภทต่าง ๆ

คำสั่งพื้นฐานในการตรวจสอบเน็ตเวิร์ค

Ping

Ping เป็นเครื่องมือแรกและเป็นเครื่องมือที่สำคัญมากที่สุดที่จะใช้ในการวิเคราะห์ปัญหาของระบบเครือข่ายที่ใช้โปรโตคอล TCP/IP เป็นเครื่องมือที่ใช้สำหรับทดสอบว่าโฮสต์นั้น ๆ ยังเชื่อมต่อกับเครือข่ายอยู่หรือไม่ ซึ่ง ping จะส่งแพ็กเก็ตไปยังโฮสต์ดังกล่าวเพื่อถามว่า “คุณยังอยู่หรือเปล่า?” ถ้าโฮสต์นั้นยังเชื่อมต่อกับเครือข่ายอยู่ ก็จะส่งแพ็กเก็ตกลับมาบอกว่า “ยังอยู่” ping จะวัดเวลาตั้งแต่เริ่มส่งแพ็กเก็ตออกไปและเมื่อโฮสต์ได้รับแพ็กเก็ตตอบรับ แล้วรายงานระยะเวลาดังกล่าว การ ping นั้นไม่ได้บอกแค่ว่าโฮสต์นั้นยังเชื่อมต่ออยู่กับเครือข่ายหรือไม่เท่านั้น มันยังสามารถวัดได้ว่าการสื่อสารระหว่างสองเครื่องใช้เวลานานเท่าใด ซึ่งข้อมูลนี้สามารถใช้ในการตรวจสอบการเชื่อมต่อของโฮสต์นั้นกับเครือข่ายและประสิทธิภาพของเครือข่ายด้วย

```
C:\>ping www.nida.ac.th

Pinging www.nida.ac.th [202.44.72.206] with 32 bytes of data:
Reply from 202.44.72.206: bytes=32 time=1ms TTL=62
Reply from 202.44.72.206: bytes=32 time=1ms TTL=62
Reply from 202.44.72.206: bytes=32 time=1ms TTL=62
Reply from 202.44.72.206: bytes=32 time=1ms TTL=62

Ping statistics for 202.44.72.206:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>ping 202.44.72.206

Pinging 202.44.72.206 with 32 bytes of data:
Reply from 202.44.72.206: bytes=32 time<1ms TTL=62
Reply from 202.44.72.206: bytes=32 time=1ms TTL=62
Reply from 202.44.72.206: bytes=32 time=1ms TTL=62
Reply from 202.44.72.206: bytes=32 time<1ms TTL=62

Ping statistics for 202.44.72.206:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

ภาพที่ 5-5 ภาพแสดงการใช้คำสั่ง ping

ภาพที่ 5-5 ภาพแสดงการใช้คำสั่ง ping ใน command prompt ทั้งสองแบบคือ ping ด้วย IP Address กับ ping ด้วยชื่อเครื่อง หากไม่มีการตอบกลับจะขึ้นข้อความ Request timed out. หากมีการตอบกลับจะขึ้นข้อความ Reply from ดังภาพ

เมื่อเกิดปัญหาบนเครือข่ายให้ใช้ ping ตามขั้นตอนเพื่อช่วยค้นหาสาเหตุที่ทำให้เกิดปัญหา ดังนี้

1. ให้ ping โฮสต์ที่อยู่ในซับเน็ตเดียวกันถ้าไม่ตอบรับแสดงว่าไม่มีการเชื่อมต่อ แต่ถ้า ping ด้วยชื่อโฮสต์ไม่มีการตอบกลับ แต่ ping ด้วย IP address ได้รับการตอบกลับ แสดงว่ามีปัญหาเกี่ยวกับ DNS

2. เมื่อ ping โฮสต์มีการตอบกลับ ให้ ping IP address ของเกตเวย์ หากได้รับการตอบกลับตรวจหาสาเหตุอื่น หากไม่ได้รับการตอบกลับแสดงว่าเครื่องนั้นมีปัญหา อาจจะมีการตั้งค่าไม่ถูกต้อง เช่น ซับเน็ตมาสค์ หรือเกตเวย์
3. ถ้า ping เกตเวย์ได้ ให้ลอง ping โฮสต์ที่อยู่ต่างซับเน็ต ถ้าได้รับการตอบกลับ แสดงว่าเครือข่ายอินทราเน็ตทำงานปกติ ถ้าไม่ได้รับการตอบกลับ อาจมีปัญหาที่ลิงค์ การเชื่อมต่อระหว่างเกตเวย์

หากใช้ ping ยังหาสาเหตุไม่ได้จึงค่อยใช้เครื่องมือหรือคำสั่งอื่น

(จตุชัย แพงจันทร์ และ อนุโชต วุฒิพรพงษ์, 2555)

Netstat

เมื่อเราทราบแล้วว่า คอมพิวเตอร์ทุกเครื่องเชื่อมต่อกับเครือข่ายและทำงานปกติโดยใช้เครื่องมือ ping และ tracert หลังจากนี้เราต้องการที่จะทราบประสิทธิภาพในการสื่อสารข้อมูลระหว่างคอมพิวเตอร์เหล่านี้ Netstat เป็นเครื่องมือที่จะช่วยในการเฝ้าดูพฤติกรรมของเครือข่าย netstat เป็นเครื่องมือที่ใช้แสดงสถิติเกี่ยวกับโปรโตคอล TCP/IP เช่น แสดงสถิติเกี่ยวกับการเชื่อมต่อระหว่างคอมพิวเตอร์สองเครื่อง และข้อมูลเกี่ยวกับปริมาณข้อมูลและจำนวนแพ็กเก็ตที่รับส่งโดยโปรโตคอลอื่น ๆ ซึ่งจะรวมถึงโปรโตคอล IP, ICMP, TCP และ UDP ข้อมูลเหล่านี้สามารถนำไปใช้ในการวิเคราะห์หาสาเหตุที่เกิดขึ้น ดดยการแยกออกได้ว่า ปัญหาดังกล่าวเกิดขึ้นจากแอพพลิเคชันใดหรือเป็นปัญหาของเครือข่าย การใช้คำสั่งมีรูปแบบ ดังนี้

netstat [-a] [-ens] [-p protocol] [-r] [interval]

พารามิเตอร์	คำอธิบาย
-a	แสดงทุก ๆ การเชื่อมต่อ
-e	แสดงสถิติของอีเธอร์เน็ต พารามิเตอร์นี้สามารถใช้ควบคู่กับ –s ได้
-n	แสดงที่อยู่ (Address) และหมายเลขพอร์ต (Port number) เป็นตัวเลขหรือไม่ต้องเปลี่ยนหมายเลขเหล่านี้เป็นชื่อแทน
-s	แสดงสถิติของแต่ละโปรโตคอล โดยดีฟอลต์แล้วจะแสดงสถิติของโปรโตคอล IP, TCP, UDP และ ICMP ถ้าต้องการให้แสดงสถิติเฉพาะโปรโตคอลให้ใช้ -p protocol
-p protocol	แสดงการเชื่อมต่อของโปรโตคอลที่กำหนดโดย protocol
-r	แสดงตารางการจัดเส้นทาง (routing table)
interval	กำหนดให้แสดงสถิติทุก ๆ interval วินาที ถ้าไม่มีกำหนดค่าสถิติจะถูกแสดงแค่ครั้งเดียว

(จตุชัย แพงจันทร์ และ อนุโชต วุฒิพรพงษ์, 2555)

Traceroute

ถ้าใช้ ping ในการค้นหาสาเหตุที่ทำให้เครือข่ายช้านั้นเป็นสิ่งที่ทำได้ยาก ยังมีอีกเครื่องมือหนึ่งที่จะช่วยให้งานนี้ง่ายขึ้น เครื่องมือที่ว่านี้คือ traceroute (หรือ tracert ในวินโดวส์เอ็นที) การใช้คำสั่งนี้จะคล้ายกับ

การใช้คำสั่ง ping คือ คำสั่ง tracert ตามด้วยชื่อโฮสต์ที่ต้องการทดสอบ tracert ทำงานโดยการส่งแพ็กเก็ต ICMP ด้วย TTL เพิ่มขึ้นทุก ๆ ครั้งที่ส่ง โดยจะเริ่มต้นที่ TTL มีค่าเท่ากับ 1 ก่อน เวิร์คสเตชันจะส่งแพ็กเก็ตไปเรื่อย ๆ จนกระทั่ง TTL มีค่าเท่ากับค่าที่กำหนด หรือจนกระทั่งโฮสต์ปลายทาง ดังนั้น คำสั่ง tracert จะเริ่มโดยการส่งแพ็กเก็ตพิเศษนี้ไปยังเกตเวย์ของเครือข่ายก่อน ถ้าเกตเวย์ทำงานปกติก็จะส่งแพ็กเก็ตตอบรับมายังเครื่องที่ส่ง แล้วโฮสต์ต้นทางก็จะส่งแพ็กเก็ตไปยังเราท์เตอร์ถัดไปตามเส้นทางไปยังโฮสต์ปลายทาง ซึ่งเราท์เตอร์ตัวถัดไปก็จะทำเช่นเดียวกันกับเกตเวย์ ขบวนการนี้ก็จะทำไปเรื่อย ๆ จนกระทั่งโฮสต์ปลายทางได้รับแพ็กเก็ตและตอบกลับหรือจำนวนฮ็อป (Hop) เกินที่กำหนดไว้

โดยมาตรฐานแล้วจำนวนฮ็อปที่สูงสุดคือ 30 ฮ็อป ซึ่งเป็นค่าที่ได้จากโครงสร้างของอินเทอร์เน็ตในปัจจุบัน ผลที่แสดงโดยคำสั่ง tracert คือ คอลัมน์แรกจะเป็นจำนวนฮ็อป หรือค่า TTL นั่นเอง อีกสามคอลัมน์ต่อมาจะเป็นช่วงเวลาที่ได้รับการตอบกลับจากเราท์เตอร์ตัวนั้น ซึ่งแต่ละฮ็อป tracert จะส่งแพ็กเก็ตทดสอบ 3 ครั้ง เวลาจะแสดงในหน่วยมิลลิวินาที (ms) ส่วนคอลัมน์สุดท้ายจะเป็นชื่อฮ็อป (ถ้าทราบ) และหมายเลขไอพีของเกตเวย์หรือเราท์เตอร์ตัวนั้น ถ้าในคอลัมน์ที่ 2-4 แสดงเป็นเครื่องหมายดอกจันทร์ (“*”) แสดงว่า ลิงค์ในช่วงนั้นมีปัญหา ซึ่งถ้าคอลัมน์สุดท้ายแสดงข้อความ “request time out” แสดงว่า เวลาการตอบรับของเราท์เตอร์ตัวนั้นเกินค่าที่กำหนด ซึ่งโดยปกติจะอยู่ที่ 500 ms ส่วนฮ็อปสุดท้ายแสดงข้อมูลของโฮสต์ปลายทาง

คำสั่ง tracert ก็สามารถเลือกค่าต่าง ๆ ได้เหมือนกับคำสั่ง ping ถ้าต้องการทราบให้พิมพ์คำสั่ง tracert เฉย ๆ แล้วมันจะแสดงทางเลือกต่าง ๆ

Tracert เป็นเครื่องมือที่มีประโยชน์มากเมื่อใช้สำหรับค้นหาเกตเวย์หรือเราท์เตอร์ที่มีปัญหา เพราะ tracert จะแสดงสถิติเกี่ยวกับช่วงเวลาการตอบรับจากเกตเวย์หรือเราท์เตอร์ต่าง ๆ ที่อยู่ระหว่างสองโฮสต์นี้ ทำให้สามารถทราบได้ว่าลิงค์ช่วงไหน หรือเกตเวย์ตัวไหนไม่ทำงานตามปกติ เมื่อใช้ ping กับ tracert ร่วมกันอาจเป็นเครื่องมือที่ดีที่สุดสำหรับผู้บริหารระบบเครือข่าย TCP/IP ก็ว่าได้

(จตุชัย แพงจันทร์ และ อนุโชต วุฒิพรพงษ์, 2555)

ชุดคำสั่งในการคอนฟิคกูเรชั่นอุปกรณ์เครือข่าย

ในการคอนฟิคกูเรชั่นอุปกรณ์เครือข่าย แต่ละยี่ห้อแต่ละรุ่นจะมีคำสั่งในการใช้งานแตกต่างกันออกไป หัวข้อนี้จะรวบรวมคำสั่งที่มีการใช้งานบ่อย ๆ ของสวิตช์ 2 ยี่ห้อ ได้แก่ Alcatel-Lucent และ Enterasys เป็นหลัก เนื่องจากอุปกรณ์สำรองและที่มีการใช้เป็น access switch จะใช้เป็นยี่ห้อ Alcatel-Lucent ส่วนยี่ห้อ Enterasys ใช้งานที่อาคารนวมินทราธิราช ไม่มีอุปกรณ์สำรองเนื่องจากเป็นสวิชต์ที่มีอัพลิงค์ขนาด 10 กิกะบิต จึงต้องใช้วิธีใช้สวิตช์ชั้นที่เป็นห้องเรียนสำรองชั้นที่เป็นออฟฟิศ เนื่องจากห้องเรียนแต่ละชั้นมีปริมาณการใช้งานไม่สูง และไม่มีการพ่วงต่อสวิชต์ จึงสามารถใช้กิกะบิตสวิตช์ที่มีอยู่ทดแทนได้ ส่วน Cisco เป็นสวิชต์รุ่นเล็ก ส่วนใหญ่จะใช้เป็น unmanaged switch ส่วน Nortel จะการคอนฟิกผ่านเว็บเพจจะสะดวงกว่า คำสั่งที่นำมาจะใช้ในรูปแบบของตัวอย่าง ไม่ใช้แบบ systax เนื่องจากเวลาเร่งรีบการใช้งานแบบตัวอย่างมีประสิทธิภาพมากกว่า ไม่ต้องเสียเวลาตีความค่าตัวแปรต่าง ๆ อีกครั้ง ส่วนรายละเอียดคำสั่งเพิ่มเติมสามารถดูได้ที่คู่มือการใช้งานของอุปกรณ์เครือข่าย ที่เครื่องแชร์ไฟล์ของกลุ่มงานโครงสร้าง

Alcatel Lucent

```
-> interfaces 3/1 alias switch_port
-> interfaces 2/2 alias "IP Phone"
-> show interfaces 1/2
-> show interfaces 1/2 status
```

```
-> lanpower start 5/11-14

-> lanpower stop 5/11-14

-> show lanpower 1

-> show mac-address-table all

-> vlan 850 name “Marketing Admin”
-> vlan 200
-> vlan 720 disable
-> no vlan 1020

-> vlan 10 port default 3/1
-> vlan 20 port default 4/1-24
-> vlan 200 port default 29
-> vlan 10 no port default 3/1

-> show vlan

-> show vlan port

-> show vlan 10 port

-> show vlan port 3/2

-> show vlan 500 port 8/16

-> vlan 2 802.1q 3/1
-> vlan 10 802.1q 100
-> vlan 5 802.1q 4/2 "802.1q tag 2"
-> vlan 6 no 802.1q 3/1

-> vlan 808 802.1q 1/1 "TAG PORT 1/1 VLAN 808"

-> show 802.1q 3/4

-> ip interface “Marketing”
-> ip interface “Payroll address” 18.12.6.3 vlan 255

-> ip static-route 0.0.0.0 mask 0.0.0.0 gateway 171.11.2.1

-> ip interface "VLAN27" address 192.10.27.1 mask 255.255.255.0 vlan 27

-> show ip interface

-> show ip route

-> show ip service

-> show tcp ports

-> arp 171.11.1.1 00:05:02:c0:7f:11

-> ip helper address 75.0.0.10
-> ip helper no address 31.0.0.20

-> ip helper address 75.0.0.10 3

-> user techpubs password writer read-only config
-> no user techpubs

-> password

-> aaa authentication telnet local

-> show aaa authentication

-> show user

-> vlan 10 ip 51.0.0.0 255.0.0.0
-> vlan 20 ip 21.0.0.0
-> vlan 10 no ip 21.0.0.0 255.0.0.0
-> vlan 10 no ip 51.0.0.0

-> vlan 10 port 3/10
-> vlan 20 port 6/1-32
-> vlan 500 port 2/1-12 4/10-16 8/4-17
-> vlan 30 no port 9/11
-> vlan 40 no port 4/1-16
-> vlan 600 no port 2/14-20 7/1-9
```

```
-> vlan port 3/1 default vlan enable
-> vlan port 5/2 default vlan disable
-> vlan port 6/1-32 8/10-24 9/3-14 default vlan enable

-> reload

-> reload working rollback-timeout 5
-> reload working no rollback-timeout

-> copy running-config working

-> write memory

-> copy working certified

-> show running-directory

-> system contact "Jean Smith Ext. 477 jsmith@company.com"
-> system contact engineering-test@company.com

-> system name OmniSwitch6850
-> system name OS-6850

-> system location "NMS Test Lab"
-> system location TestLab

-> system daylight savings time enable
-> system daylight savings time disable

-> show system

-> show hardware info

-> show chassis

-> show cmm

> show module

-> show module status

-> show power

-> ntp server 1.1.1.1

-> ntp client enable

-> prompt user

-> kill 3

-> whoami

-> show session config

-> snmp station 168.151.2.101 "test lab"
-> snmp station 170.1.2.3 username1 enable
-> snmp station 1.1.2.2 v2
-> no snmp station 2.2.2.2

-> show snmp station

-> snmp community map community1 user testname1
-> snmp community map community1 enable

-> snmp community map mode enable

-> snmp security no security

-> snmp trap absorption enable

-> snmp trap to webview enable

("OmniSwitch CLI Reference Guide", 2015)
```

Enterasys

```
C5(su)->show ip address

C5(su)->set ip address 10.1.10.1 mask 255.255.128.0
```

```
C5(rw)->clear ip address
C5(su)->show ip protocol
C5(su)->set ip protocol dhcp
C5(ro)->show ip route
C5(su)->show system
C5(su)->show system hardware
C5(ro)->show system utilization cpu
C5(rw)->show system utilization cpu
C5(su)->show time
C5(su)->set prompt "Switch 1"
C5(su)->show version
C5(su)->set system name "Information Systems"
C5(su)->set system location "Bldg N32-04 Closet 9"
C5(su)->set system contact "Joe Smith"
C5(su)->show telnet
C5(su)->show ssh status
C5(su)->set ssh disable
C5(su)->show snmp persistmode
C5(su)->set snmp persistmode manual
C5(su)->save config
C5(rw)->show file configs/myconfig
C5(su)->dir
C5(rw)->show config all outfile configs/save_config2
C5(rw)->show config port
C5(su)->configure configs/Jan1_2004.cfg
This command will reset the system and clear current configuration.
Are you sure you want to continue (y/n) [n]?
```

This example shows how to append a configuration file to the existing running config and will not reset the switch.

```
C5(su)->configure configs/myconfig append
C5(su)->delete configs/Jan1_2004.cfg
C5(su)->reset
C5(rw)->show webview
C5(rw)->set webview disable
C5(rw)->set ssl enabled
C5(rw)->show ssl
C5(su)->show system login
C5(su)->set system login netops super-user enable
C5(su)->set system login guest read-only enable allowed-days Mon Tue Wed Thu
Fri
C5(su)->clear system login netops
C5(su)->set password rw
C5(su)->set password
C5(su)->set system password-resetbutton disable
C5(su)->show system password
```

```
C5(su)->show mgmt-auth-notify
C5(su)->set mgmt-auth-notify disable
C5(su)->clear mgmt-auth-notify
C5(su)->set mgmt-auth-notify enable console telnet
C5(su)->show port ge.3.14
C5(su)->show port status ge.1.1-2
C5(su)->show port counters ge.3.1
C5(su)->show port cablestatus ge.1.1
C5(su)->set port enable ge.1.3
C5(rw)->show port alias ge.3.1-3
C5(rw)->set port alias ge.3.3 Admin
C5(su)->show port speed ge.3.14
C5(su)->set port speed ge.3.3 10
C5(su)->show snmp user list
C5(su)->set snmp user netops
C5(su)->clear snmp user bill
C5(su)->set snmp group anyone user public security-model usm
C5(su)->clear snmp group anyone public
C5(su)->set snmp community vip
C5(su)->show vlan 1
C5(su)->set vlan create 3
C5(su)->set vlan name 7 green
C5(su)->clear vlan 9
C5(su)->show port vlan ge.2.1-6
C5(su)->set vlan create 4
C5(su)->set port vlan ge.1.10 4 modify-egress
C5(su)->clear port vlan ge.1.3-11
C5(su)->set port discard ge.3.3 tagged
C5(su)->show port egress ge.1.1-3
C5(su)->set vlan egress 7 ge.1.5-10
C5(su)->set vlan egress 7 ge.1.13-15 forbidden
C5(su)->set vlan egress 7 ge.1.2 untagged
C5(su)->show netstat
C5(su)->show arp
C5(su)->traceroute 192.167.252.17
C5(su)->show mac port ge.3.1
C5(su)->show sntp
C5(su)->set sntp client broadcast
C5(su)->set sntp server 10.21.1.100 precedence 1 key 1
C5(su)->set sntp poll-interval 6
C5(su)->set timezone EST -5
C5(su)->router#show interface
C5(su)->router#configure
C5(su)->router(Config)#interface vlan 1
```

```
C5(su)->router(Config-if(Vlan 1))#

C5(su)->router(Config)#interface vlan 1
C5(su)->router(Config-if(Vlan 1))#ip address 192.168.1.1 255.255.255.0

C5(su)->router(Config)#interface vlan 1
C5(su)->router(Config-if(Vlan 1))#no shutdown

C5(su)->router(Config)#no ip routing

C5(su)->router#show running-config

C5(su)->router(Config)#interface vlan 1
C5(su)->router(Config-if(Vlan 1))#ip helper-address 192.168.1.28

C5(su)->router#show ip route

C5(su)->router(Config)#ip route 10.0.0.0 255.0.0.0 10.1.2.3
```

("Extreme Networks C5 CLI Reference FW 6.81", 2015)

การสำรองข้อมูลและแผนฉุกเฉิน

อุปกรณ์เครือข่ายที่ใช้งานจะมีการเก็บค่าคอนฟิคกูเรชั่นไว้ ก่อนที่จะทำการปรับเปลี่ยนค่าจะต้องทำการเก็บค่าคอนฟิคกูเรชั่นของเก่าไว้ก่อน โดยเฉพาะ Core Switch ซึ่งจะมีรายละเอียดมากกว่า Access Switch ทั่วไป ซึ่งจะมีค่าคอนฟิคกูเรชั่นคล้ายคลึงกันในแต่ละอาคาร กรณี Access Switch หากชำรุดหรือใช้งานได้ จะต้องนำอุปกรณ์สำรองไปใช้งานสามารถนำค่าคอนฟิคกูเรชั่นที่เก็บไว้ที่เครื่องแชร์ไฟล์ของกลุ่มงานโครงสร้าง

ระบบดูแลและบริหารเครือข่าย (Network Management Systems)

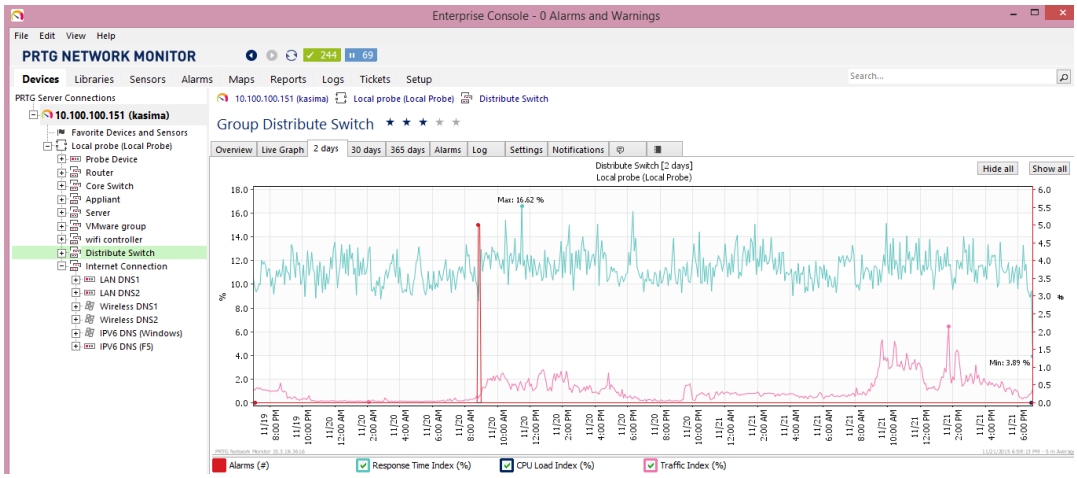
ระบบดูแลและบริหารเครือข่ายเป็นสิ่งที่จำเป็นอย่างยิ่งสำหรับเครือข่ายขนาดใหญ่ เนื่องจากมีการติดตั้งอุปกรณ์เครือข่ายเป็นจำนวนมากกระจัดกระจายอยู่ทั่วสถาบัน และมีหลากหลายยี่ห้อทำให้ยากต่อการดูแล เพื่อให้จัดการง่ายขึ้น ในการลดเวลาและจำนวนเจ้าหน้าที่ที่ใช้ในการตรวจสอบจึงมีความจำเป็นและมีประโยชน์อย่างมากที่จะจัดหาซอฟต์แวร์มาช่วยในการเฝ้าระวังและแจ้งเตือนว่าอุปกรณ์ขัดข้อง สามารถตั้งค่าให้ส่งเมลแจ้งเตือนหากมีอุปกรณ์ขัดข้อง โดยอุปกรณ์เครือข่ายแต่ละแครื่องจะต้องทำการตั้งค่า SNMP และเปิดสิทธิให้ไอพีแอดเดรสของเครื่องแม่ข่ายที่ติดตั้งซอฟต์แวร์สามารถเข้าถึงข้อมูลที่จะทำการเฝ้าระวัง ซอฟต์แวร์ที่นำมาใช้จะแยกตามยี่ห้อและประเภทของอุปกรณ์ สำนักจะมีการใช้งานซอฟต์แวร์เฝ้าระวังอุปกรณ์เครือข่ายอยู่ 4 ประเภท ได้แก่ 1) PRTG 2) OmniVista 3) Netsight 4) Air Manager

การติดต่อบริษัทที่ทำการบำรุงรักษา

การติดต่อบริษัทที่ทำการบำรุงรักษาสามารถติดต่อได้ทางโทรศัพท์หรือทางเมล ติดต่อโดยตรงกับทางวิศวกรจะสะดวกกว่าผ่านคอลเซ็นเตอร์ซึ่งจะไม่สามารถเข้าใจปัญหาได้ดีเท่าวิศวกร ไว้ใช้ติดต่อในกรณีที่ติดต่อวิศวกรไม่ได้ หรือติดต่อผ่านเจ้าหน้าที่ฝ่ายขายที่ดูแลสถาบันแทน รายชื่อ อีเมลและเบอร์โทรจะเก็บไว้จัดทำเป็นไฟล์และเก็บไว้ที่เครื่องไฟล์แชร์ของกลุ่มงาน และอีกส่วนจะติดไว้ที่กระจกทางเดินภายในห้องแม่ข่าย เนื่องจากบริษัทที่ดูแลหรือวิศวกรอาจมีการย้ายงานจึงมีการเปลี่ยนแปลงได้ตลอด เพื่อป้องกันปัญหาติดต่อตามคู่มือนี้แล้วติดต่อไม่ได้

PRTG

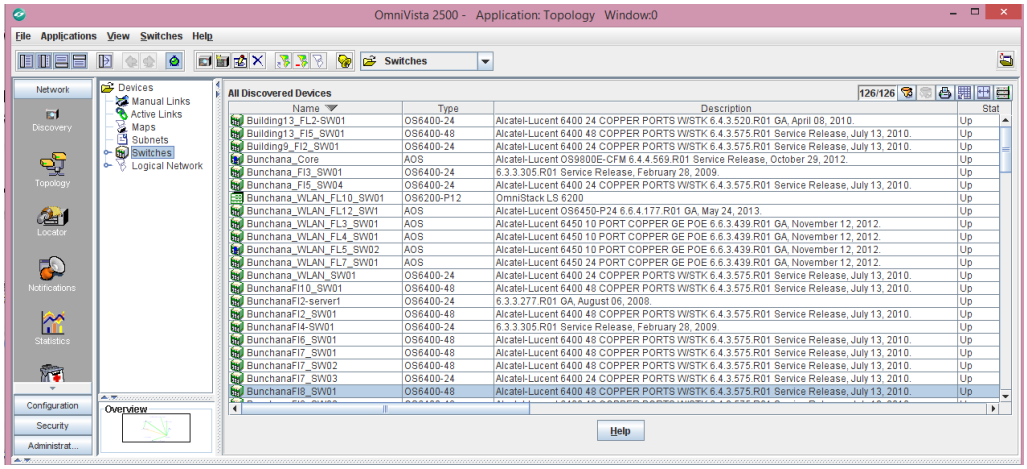
สำนักจะใช้เป็นเครื่องมือหลักที่ใช้ในการเฝ้าระวังอุปกรณ์เครือข่ายทุกยี่ห้อ ใช้งานง่ายและมีราคาย่อมเยาว์ เน้นการเฝ้าระวังเรื่องการขาดการติดต่อกับอุปกรณ์เป็นหลัก (อัพดาวน์) เข้าใช้งานสะดวกเป็นเว็บเพจ



ภาพที่ 5-6 แสดงตัวอย่างหน้าจอโปรแกรม PRTG

OmniVista

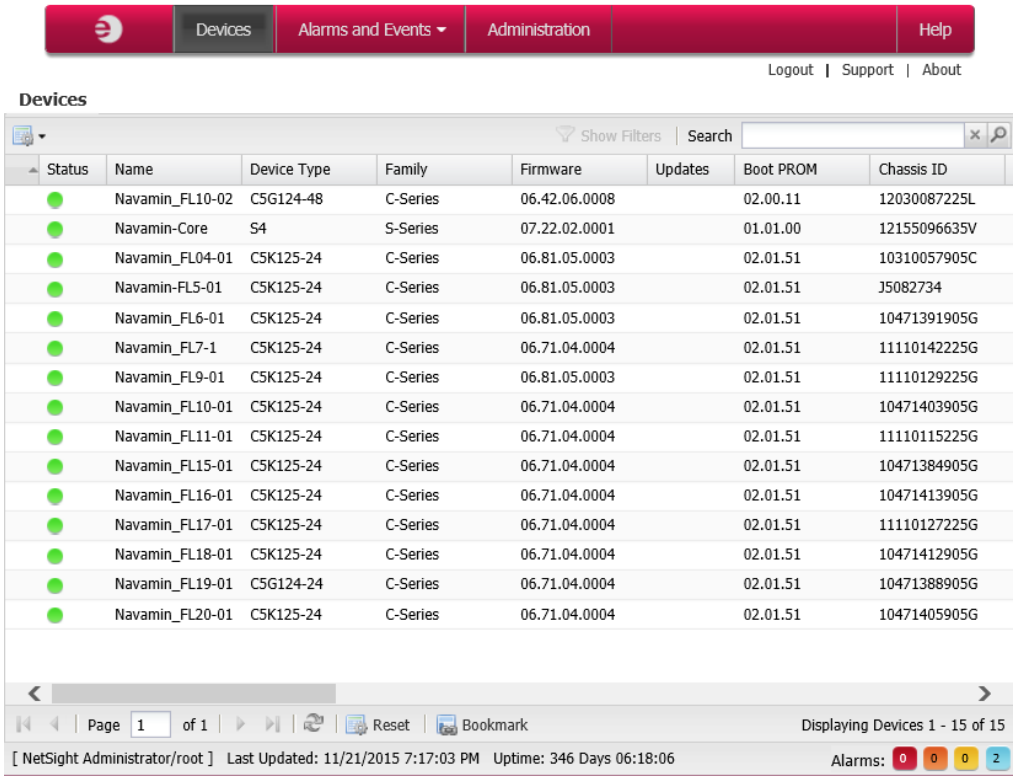
เครื่องมือที่ใช้ในการเฝ้าระวังอุปกรณ์เครือข่ายยี่ห้อ Alcatel-Lucent สามารถเพิ่มอุปกรณ์ยี่ห้ออื่นเข้ามาได้แต่จะไม่เห็นรายละเอียดบางอย่าง ช่องทางการเข้าใช้ไม่สะดวกต้องติดตั้งโปรแกรมที่เครื่องไคลแอนท์และซอฟต์แวร์ไม่มีการอัพเกรดเวอร์ชั่น เพราะต้องเสียค่าใช้จ่าย



ภาพที่ 5-7 แสดงตัวอย่างหน้าจอโปรแกรม Omni Vista

Netsight

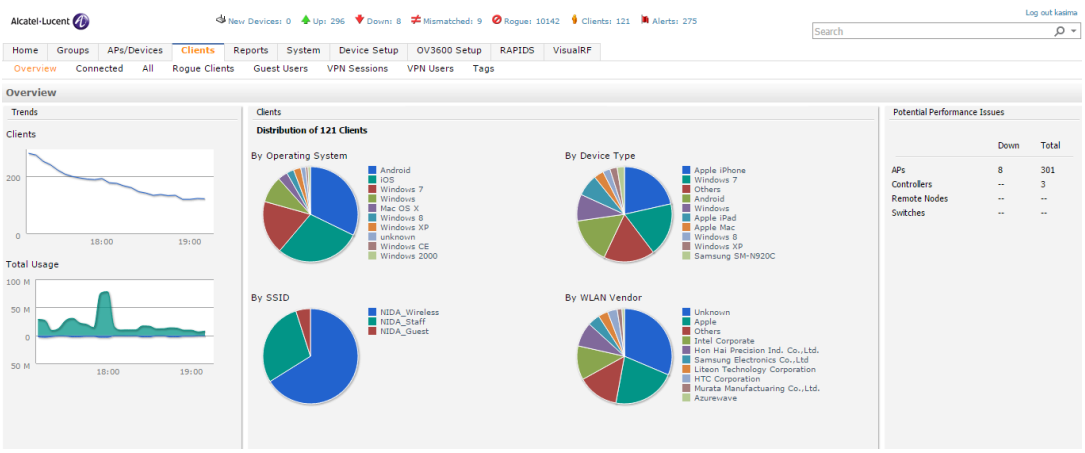
เครื่องมือที่ใช้ในการเฝ้าระวังอุปกรณ์เครือข่ายยี่ห้อ Enterasys มีลิขสิทธิ์ใช้งานได้ 50 อุปกรณ์ ช่องทางการเข้าใช้ผ่านเว็บเพจดูได้บางเมนู หากต้องการดูรายละเอียดบางอย่างต้องติดตั้งโปรแกรมที่เครื่องไคลแอนท์ และซอฟต์แวร์ไม่มีการอัพเกรดเวอร์ชั่น เพราะต้องเสียค่าใช้จ่าย



ภาพที่ 5-8 แสดงตัวอย่างหน้าจอโปรแกรม Netsight

Air Manager

เครื่องมือที่ใช้ในการเฝ้าระวังอุปกรณ์เครือข่ายยี่ห้อ Alcatel-Lucent ส่วนที่เป็นระบบเครือข่ายไร้สายของสถาบันเท่านั้น ไม่สามารถดูอุปกรณ์ที่ทางทรูและเอไอเอสมาติดตั้งให้บริการได้ เนื่องจากทางบริษัทไม่อนุญาต ช่องทางการเข้าใช้สะดวก ผ่านเว็บเพจ สามารถตรวจสอบว่าค้นหาผู้ใช้งาน อุปกรณ์ที่ใช้ จำนวนผู้ใช้แยกตาม SSID แยกตามอุปกรณ์ และระบบปฏิบัติการที่ใช้



ภาพที่ 5-9 แสดงตัวอย่างหน้าจอโปรแกรม Air Manager

บทที่ 6
ปัญหาอุปสรรคและข้อเสนอแนะ

สถาบันประกอบไปด้วยอาคารต่าง ๆ ทั้งเก่าและใหม่ การเดินสายเคเบิลภายในอาคารจึงมีความหลากหลาย และอาคารส่วนใหญ่จะมีการเดินสายมาพร้อมการก่อสร้างอาคาร ทำให้สำนักไม่สามารถออกแบบห้องเครือข่าย ระบบสำรองไฟ การจ่ายกระแสไฟฟ้า อุปกรณ์เครือข่าย และคุณภาพการเดินสายได้อย่างที่ต้องการ รวมทั้งเมื่อมีการปรับปรุงสถานที่ ทางเจ้าของสถานที่จะไม่ได้มาขอความคิดเห็นจากเจ้าหน้าที่ของสำนัก และไม่ได้ออกแบบและกำหนดรายละเอียดไว้อย่างชัดเจน ทำให้เมื่อการก่อสร้างหรือปรับปรุงสถานที่เสร็จเรียบร้อยแล้วมักเกิดปัญหาเวลาที่เข้าใช้งาน ทำให้สำนักต้องแก้ปัญหาเฉพาะหน้าอยู่บ่อยครั้ง และไม่สามารถแก้ไขให้สามารถใช้งานได้ดีดังที่ต้องการได้ ในที่นี้สามารถจะระบุปัญหาและอุปสรรคตลอดจนข้อเสนอแนะต่าง ๆ ได้ดังนี้

1. ปัญหาและอุปสรรค

1.1. สถานที่ติดตั้งตู้ไม่มิดชิดเพียงพอ บางแห่งเป็นสถานที่สาธารณะ ทำให้ตู้เครือข่ายปืนที่พักอาศัยของสัตว์โดยเฉพาะหนู ทั้งนำอาหารมากิน ขับถ่าย ตาย และกัดสายเคเบิลขาด

1.2. ผู้ใช้งานนำอุปกรณ์กระจายสัญญาณเครือข่ายไร้สายมาติดตั้งใช้งานโดยไม่มีการปรับตั้งค่า ทำให้เกิดการรบกวนสัญญาณกับเครื่องของผู้ใช้งานอื่นจึงไม่ได้รับไอพีแอดเดรสของสถาบันทำให้ใช้เครือข่ายไม่ได้

1.3. บางครั้งห้องเครือข่ายมีสภาพเป็นห้องเก็บของของหน่วยงาน

1.4. เมื่อมีการปรับปรุงสถานที่หรือก่อสร้างอาคารมีรายละเอียดงานที่ติดตั้งไม่ครบ ไม่ได้มาตรฐานหรือไม่พร้อมใช้งาน

1.5. มีการนำสายสัญญาณที่ไม่ได้มาตรฐานมาใช้งาน

1.6. การกำหนดจุดเครือข่ายไม่สอดคล้องกับการใช้งาน

1.7. ผู้ใช้งานยังไม่ตระหนักถึงการรักษาความลับของบัญชีผู้ใช้ส่วนตัว นำไปล็อคอินเพื่อเชื่อมต่อเครือข่ายให้กับคนที่รู้จัก หากใช้งานไม่ระมัดระวังอาจเข้าข่ายทำผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

1.8. เร่งการจัดทำนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยด้านสารสนเทศ

1.9. เร่งจัดทำข้อปฏิบัติในการในการใช้งานด้านสารสนเทศเพื่อรองรับการประกาศใช้นโยบายและแนวปฏิบัติความมั่นคงปลอดภัยด้านสารสนเทศและข้อมูลส่วนบุคคล

1.10. เร่งจัดทำข้อปฏิบัติในการในการใช้งานด้านสารสนเทศเพื่อรองรับการประกาศใช้นโยบายและแนวปฏิบัติความมั่นคงปลอดภัยข้อมูลส่วนบุคคล

1.11. เตรียมความพร้อมในการดำเนินการปรับปรุงเครือข่ายและแม่ข่ายให้รองรับตามข้อปฏิบัติต่าง ๆ

2. ข้อเสนอแนะสิ่งที่ควรมีในการติดตั้งระบบเครือข่ายเมื่อมีการปรับปรุงสถานที่

2.1. ห้องเครือข่ายหลักหรือห้องเครือข่ายย่อยประจำชั้น พร้อมช่องชาร์ป

2.2. อุปกรณ์ประกอบการเดินสาย ได้แก่ ***patch panel, outlet,*** สาย ***patch cord*** ที่เป็นสายสำเร็จจากผู้ผลิต

2.3. จำนวนจุดเครือข่ายที่เพียงพอกับจำนวนผู้ใช้งานและอุปกรณ์ และมีตำแหน่งที่ใกล้เคียงกับตำแหน่งที่ใช้งาน

2.4. อุปกรณ์เครือข่าย

2.5. รายงานผลการทดสอบสาย

2.6. ผู้รับเหมาที่มีประสบการณ์ในการเดินสายเครือข่าย การติดตั้งที่ไม่ถูกต้องทำให้มีปัญหาในการใช้งานตามมา ถึงแม้จะได้สายสัญญาณที่มีคุณภาพสูง

2.7. แปลนอาคารแสดงการติดตั้งจุดเครือข่ายพร้อมระบุหมายเลขกำกับหลังก่อสร้างเสร็จ ***(as-built)***

2.8. หมายเลขกำกับประจำจุดเครือข่าย

3. ข้อเสนอแนะเพื่อรองรับปัญหาที่จะเกิดจากการประกาศใช้นโยบายและแนวปฏิบัติ

3.1. ควรจัดกิจกรรมประชาสัมพันธ์เรื่องการใช้งานต่าง ๆ เพิ่มเติม

3.2. มีการกระตุ้นให้นักศึกษาและบุคลากรเห็นความสำคัญของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

3.3. การดำเนินงานเพื่อปฏิบัติตามนโยบายและแนวปฏิบัติ เพราะช่วงแรกที่ดำเนินการตามประกาศผู้ใช้งานจะรู้สึกต่อต้านและไม่สะดวกในการใช้งาน ผู้บริหารจะต้องหนักแน่นต่อผลประเมินความพึงพอใจ

3.4. ควรมีจัดการพบปะกับประชาคมเพื่อรับฟังปัญหาและความคิดเห็น ทำความเข้าใจกับผู้ใช้งาน

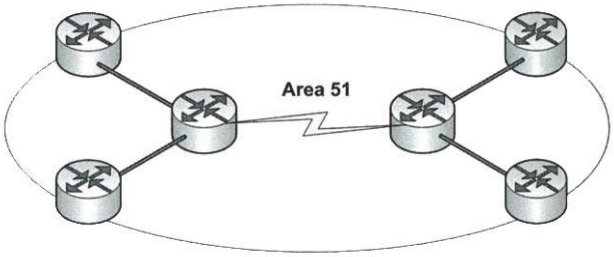
ภาคผนวก

ภาคผนวก

OSPF

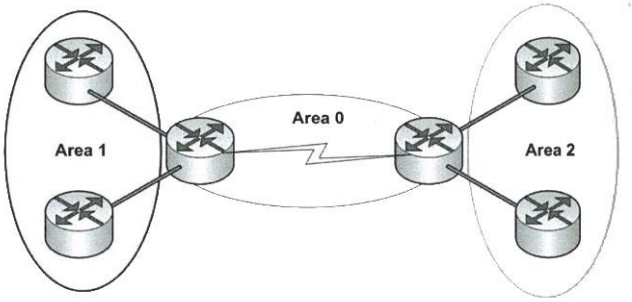
OSPF (Open Shortest Path First) เป็นโปรโตคอลที่มีวิธีการค้นหาเส้นทางด้วยรูปแบบของ Link State Protocol ที่มีการนำคุณสมบัติของ Network Interface ในแต่ละเส้นทางมาพิจารณาด้วย ซึ่งจะแตกต่างจากโปรโตคอลที่ใช้รูปแบบ Distance Vector อย่าง RIP โปรโตคอลที่สนใจเพียงระยะทางเท่านั้น ในเรื่องการอัพเดตข้อมูลในตารางเราท์ติ้งโปรโตคอล OSPF สามารถรองรับการกระจายข้อมูลแบบกลุ่มพื้นที่ (Area) ซึ่งมี 2 แบบ คือ

1. **Single Area** คือ การกำหนดขอบเขตพื้นที่เดียวบนระบบเครือข่าย ทุกเราท์เตอร์ที่อยู่เครือข่ายนี้จะ Advertise เราท์ติ้งถึงกันหมดเหมือนกับโปรโตคอล RIP ซึ่งจะเหมาะกับเครือข่ายที่มีขนาดเล็ก



ตัวอย่างเน็ตเวิร์คแบบ Single Area

2. **Multiple Areas** คือ การกำหนดขอบเขตพื้นที่แยกเป็นส่วน ๆ (แบ่งเป็น Area) ซึ่งปกติการแบ่งจะต้องมีการกำหนด Area 0 ขึ้นก่อน ซึ่งเป็น Area ที่ทำหน้าที่เป็นตัวกลางในการเชื่อมต่อกับ Area อื่น ๆ (เปรียบได้กับเป็น Backbone Area) ดังแสดงในรูป



ตัวอย่างเน็ตเวิร์คแบบ Multiple Area

จากรูปมีการแบ่งพื้นที่ออกเป็น 3 ส่วน คือ Area 0 , Area 1 , Area 2 ซึ่งภายใน Area เดียวกันจะอัพเดตตารางเราท์ติ้งถึงระดับ Subnet แต่สำหรับ Area อื่น ๆ จะอัพเดทโดยผ่านเราท์เตอร์ที่เชื่อมต่ออยู่ระหว่าง Area นั้นกับ Area 0 ซึ่งเราท์เตอร์ตัวกลางนี้เองจะทำหน้าที่ในการ Summarized network routing ก่อนจึงจะอัพเดทต่อไปยัง Area อื่น ๆ

OSPF Metric

OSPF โปรโตคอลใช้วิธีการเลือกเส้นทางแบบ Link State โดยมีการนำค่า Bandwidth Network Interface มาคำนวณด้วย ซึ่งค่าที่ได้มาเราจะเรียกว่า “Cost” โดย OSPF จะพิจารณาที่ค่า Cost ต่ำที่สุดถือเป็นเส้นทางที่ดีที่สุดนั่นคือ Network Interface ไหนที่สามารถส่งข้อมูลได้เร็วกว่าจะถูกเลือกใช้เป็นเส้นทางที่ดีกว่า

สำหรับสูตรการคำนวณตามค่าเริ่มต้นของอุปกรณ์เราท์เตอร์ในการหาค่า Cost ของโปรโตคอล OSPF เป็นดังนี้

Cost = 100 Mbps/ (Network Interface Bandwidth-Mbps)

ค่า Cost ที่คำนวณได้มีค่าตั้งแต่ 1 ดังนั้น เมื่อคำนวณค่า Cost ของ Network Interface ต่าง ๆ บนอุปกรณ์เราท์เตอร์จะได้ดังตารางต่อไปนี้

ประเภทของ Network Interface	Network Interface Bandwidth	Cost เทียบกับ 100 Mbps	Cost เทียบกับ 1000 Mbps
Ethernet	10 Mbps	10	100
Fast Ethernet	100 Mbps	1	10
Gigabit Ethernet	1000 Mbps	1	1
T1	1.544 Mbps	64.77	647.67
E1	2.048 Mbps	48.83	488.28

ตารางเปรียบเทียบค่า Cost ของ Network Interface ประเภทต่าง ๆ

ค่า 100.000.000 = 100 Mbps เป็นค่าแบนด์วิธที่โปรโตคอล OSPF ใช้อ้างอิงในการคำนวณหาค่า Cost แต่เนื่องจากค่า Cost เริ่มต้นที่ 1 ดังนั้น Network Interface แบบ Gigabit Ethernet ที่รองรับแบนด์วิธ 1000 Mbps เมื่อคำนวณหาค่า Cost จึงมีค่าเท่ากับ 1 (ค่าน้อยที่สุดของ Cost)

ดังนั้น หากต้องการให้ Cost มีค่าสัมพันธ์กับ Network Interface Bandwidth จริง ๆ จะต้องปรับแต่งคอนฟิกของโปรโตคอล OSPF บนเราท์เตอร์ให้มีการใช้ค่า Bandwidth 1000 Mbps ในการคำนวณแทนค่าเดิม 100 Mbps ด้วยการปรับค่า “auto-cost reference-bandwidth” ให้เท่ากับ 1000 (อ้างอิงตัวแปรจากอุปกรณ์เราท์เตอร์ของ Cisco)

ประเภทเราท์เตอร์บนโปรโตคอล OSPF (OSPF Router Type)

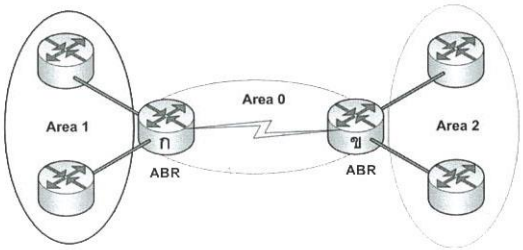
จากที่กล่าวมาข้างต้นโปรโตคอล OSPF สามารถแบ่งกลุ่มพื้นที่ (Area) การเชื่อมต่อระหว่างเราท์เตอร์เพื่อเพิ่มประสิทธิภาพในการแลกเปลี่ยนฐานข้อมูตารางเราท์ติ้ง โดยไม่จำเป็นต้องกระจายตารางเราท์ติ้งแลกเปลี่ยนกับทุก ๆ เราท์เตอร์ที่เชื่อมต่ออยู่ในเครือข่ายได้

ในการปรับแต่งคอนฟิกเพื่อกำหนดกลุ่มพื้นที่ (Area) ขึ้นมานั้น เราท์เตอร์ที่มีการเชื่อมต่ออยู่กับกลุ่มพื้นที่ต่าง ๆ โปรโตคอล OSPF จะมีการกำหนดประเภทของเราท์เตอร์นั้น ๆ ออกเป็น 3 แบบ ซึ่งจะมีคุณสมบัติที่แตกต่างกัน ดังนี้

1. Area Border Router (ABR)

เราท์เตอร์ที่มีอินเตอร์เฟสเชื่อมต่อกับ “Area 0” และ “Area N” โดยที่เราท์เตอร์ที่อยู่ใน Area 0 หรือ N จะต้องใช้ Routing protocol OSPF เท่านั้น โดยเราท์เตอร์ประเภทนี้จะมีคุณสมบัติในการ Summarized Network Routing ที่มาจาก Area N

นั่นคือเมื่อเราท์เตอร์อื่นที่มาจากกลุ่มพื้นที่ Area N ส่งตารางเราท์ติ้งมาอัพเดต โดยที่ในตารางเราท์ติ้งมีเน็ตเวิร์คต่าง ๆ ที่เกิดจากการแบ่งย่อยเน็ตเวิร์คด้วย (Sub Netmask) เช่น 172.16.1.0/24, 172.16.2.0/24, 172.16.3.0/24 เป็นต้น เราท์เตอร์ประเภท ABR จะ Summarized network routing ด้วย prefix ที่เหมือนกันให้เหลือเพียง Network Subnet เดียว เช่น จากตัวอย่างที่ผ่านมาจะได้เส้นทางใหม่เป็น 172.16.0.0/22 เป็นต้น และข้อมูลเส้นทางใหม่นี้จะถูกส่งไปอัพเดตยังเราท์เตอร์อื่นที่อยู่ใน Area 0 ต่อไป สำหรับรูปแบบการเชื่อมต่อของเราท์เตอร์ ABR แสดงดังรูป



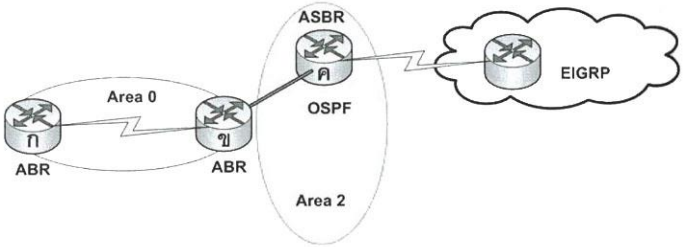
ตัวอย่างประเภทเราท์เตอร์แบบ ABR

จากรูปเราท์เตอร์ ก และ ข เป็นเราท์เตอร์ที่เชื่อมต่อกันระหว่าง Area 0 กับ Area 1 และ Area 2 ตามลำดับ ดังนั้น เราท์เตอร์ ก และ ข จึงเป็นเราท์เตอร์ประเภท ABR

2. Autonomous System Boundary Router (ASBR)

เราท์เตอร์ที่มีการเชื่อมต่อระหว่าง Routing Protocol OSPF กับ Routing Protocol อื่น ๆ (เช่น RIP, EIGRP, IGRP, BGP, Static เป็นต้น) เราท์เตอร์ประเภทนี้เท่านั้นที่สามารถ Summarized network routing ที่มาจาก Routing Protocol อื่น ๆ (Non-OSPF protocol) ได้ แต่ OSPF จะไม่ Advertise routing ที่มาจาก Non-OSPF protocol (เป็นค่า Default ของ OSPF ที่จะไม่ Advertise routing จากโปรโตคอลอื่น)

แต่ทว่ามีวิธีการปรับแต่งเราท์เตอร์ให้สามารถ Advertise Non-OSPF routing ใน Area ของ OSPF นั่นคือ การปรับแต่งให้ใช้กระบวนการ Route Redistribution ซึ่งเป็นการกำหนดค่า Metric ให้กับ Routing ที่มาจาก Routing Protocol อื่น ๆ เพื่อให้สามารถนำไปเปรียบเทียบกับ OSPF Metric ได้



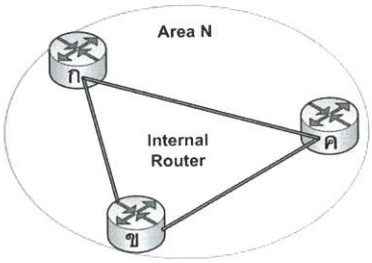
ตัวอย่างประเภทเราท์เตอร์แบบ ASBR

จากรูปเราท์เตอร์ ค อยู่ใน Area 2 ที่มีการใช้ OSPF เป็น Routing Protocol และมีการเชื่อมต่อกับเราท์เตอร์อื่นบนอินเตอร์เน็ต ซึ่งใช้ EIGRP routing protocol ดังนั้น เราท์เตอร์ ค จึงจัดอยู่ในประเภท ASBR ซึ่งจะ Summarized routing จาก EIGRP

สำหรับการปรับแต่งเราท์เตอร์สให้มีการใช้กระบวนการ Route Redistribution ทำได้โดยการปรับแต่งค่า Redistribute

3. Internal Router

เราท์เตอร์ที่มีการปรับแต่งใช้โปรโตคอล OSPF ทุก ๆ อินเตอร์เฟสที่เชื่อมต่อ และยังกำหนดให้อยู่ใน Area เดียวกันทั้งหมด ดังแสดงตัวอย่างเครือข่ายในรูป



ตัวอย่างประเภทเราท์เตอร์แบบ Internal Router

จากรูปเราท์เตอร์ ก, ข และ ค มีการเชื่อมต่ออยู่ภายใน Area N โดยที่ทุกอินเตอร์เฟสของเราท์เตอร์ทั้ง 3 กำหนดให้อยู่ใน Area N เช่นเดียวกัน ดังนั้น เราท์เตอร์ ก, ข และ ค จึงอยู่ในประเภท Internal Router

OSPF Message Type

โดยปกติ Routing Protocol จะมีหน้าที่หลักสำคัญคือ การแลกเปลี่ยนข้อมูลเส้นทางในตารางเราท์ติ้งของตนเองกับเราท์เตอร์อื่น ๆ ในการแลกเปลี่ยนข้อมูลกันนี้จะมีรูปแบบของ Message Packet ที่ใช้แบบหนึ่ง แต่เนื่องจากโปรโตคอล OSPF มีความสามารถมากกว่าแค่การ “Advertise” และ “Accept” โปรโตคอล OSPF ยังสามารถค้นหาเราท์เตอร์ที่มีการเชื่อมต่อเข้ามาใหม่ได้ด้วยการส่ง Packet กระจายไปยังเน็ตเวิร์ค หรือการส่ง Packet ตอบกลับเมื่อได้รับ Packet Advertise เป็นต้น

โปรโตคอล OSPF จึงได้แบ่งประเภท Message (หรือประเภทของ Packet) ตามลักษณะการทำงานที่แตกต่างกัน โดยแบ่งออกเป็น 5 ประเภท ดังนี้

1. Hello Message เป็น Packet ที่โปรโตคอล OSPF Broadcast ไปบนเน็ตเวิร์คเพื่อใช่ในการค้นหาเราท์เตอร์ที่มีการเชื่อมต่อใน Area เดียวกัน และยังใช้ในการตรวจสอบสถานะของเราท์เตอร์ที่เชื่อมต่ออยู่เดิมด้วย
2. Database Description Message โปรโตคอล OSPF จะมีฐานข้อมูลที่เก็บ Topology การเชื่อมต่อระหว่างเราท์เตอร์และเน็ตเวิร์คภายใน Autonomous System (AS) เรียกว่า “Link State Database (LSDB)” ดังนั้น เมื่อ Hello Message ค้นพบเราท์เตอร์ใหม่เกิดขึ้น Area เราท์เตอร์จะส่ง Packet Database Description Message ซึ่งมีข้อมูลของ LSDB ไปยังเราท์เตอร์สใหม่เพื่อจัดตั้งฐานข้อมูล LSDB ใหม่ให้ ซึ่งเราท์เตอร์ใหม่ที่ได้รับ Packet นี้จะต้องส่ง Acknowledgment Packet ตอบกลับด้วย

3. Link State Request Message เป็น Packet ที่เราท์เตอร์จะส่งออกไปยังเราท์เตอร์อื่น เพื่อร้องขอการอัพเดตข้อมูล LSDB
4. Link State Update Message เป็น Packet ที่เราท์เตอร์ที่ได้รับ Link State Request Message มาจะตอบกับพร้อมข้อมูล LSDB ที่มีการปรับปรุงล่าสุด นอกจากนี้ Link State Update Message ยังเป็น Packet ที่ถูกส่งออกไปยังเราท์เตอร์อื่น ๆ เพื่ออัพเดตข้อมูล LSDB เป็นประจำด้วย (นั่นก็คือ กระบวนการ Advertise ที่เราท์เตอร์ Broadcast หรือ Multicast ออกไปตามเวลาที่กำหนดนั่นเอง
5. Link State Acknowledgment Message สำหรับ Packet สุดท้ายนี้ OSPF ใช้ในการตอบกลับการรับ/ส่งข้อมูลระหว่างเราท์เตอร์ เพื่อยืนยันสถานะการเชื่อมต่อระหว่างเราท์เตอร์

ลักษณะการทำงานของ OSPF

โดยปกติ Routing Protocol จะมีระบบการตั้งเวลา (Timer) ที่ใช้ในการกำหนดการทำงานต่าง ๆ ให้กับเราท์เตอร์เป็นรอบ ๆ สำหรับโปรโตคอล OSPF ก็มีระบบการตั้งเวลาเช่นกัน โดยมีค่าเริ่มต้นอยู่ที่ 10 วินาที นั่นคือทุก ๆ 10 วินาที OSPF จะส่ง Packet ออกไปเพื่อทำหน้าที่ตามต้องการ โดยสามารถแบ่งการทำงานออกเป็นข้อ ๆ ดังนี้

1. กระบวนการแรกสุด โปรโตคอล OSPF จะส่ง Hello message ออกไปยังเครือข่ายเพื่อค้นหาว่ามีเราท์เตอร์ใหม่เกิดขึ้นใน Area เดียวกันหรือไม่
2. ถ้าปรากฏว่ามีเราท์เตอร์เกิดเพิ่มขึ้นมาใน Area เดียวกัน โปรโตคอล OSPF จะส่ง Packet Database Description message ไปยังเราท์เตอร์ใหม่นั้น เพื่ออัพเดตฐานข้อมูล LSDB (Link State Database) แต่นั่นหมายความว่าเราท์เตอร์นั้นจะต้องใช้โปรโตคอล OSPF ด้วย
3. นอกจากนี้ Hello message ยังทำหน้าที่ในการตรวจสอบสถานการณ์เชื่อมต่อระหว่างเราท์เตอร์เช่นกัน นั่นคือ เมื่อเราท์เตอร์หนึ่งส่ง Hello message ออกไปเราท์เตอร์ที่เชื่อมต่ออยู่จะต้องตอบกลับด้วย หากเราท์เตอร์ใดไม่ตอบกลับมาภายในการนส่ง Hello message 4 ครั้ง เราท์เตอร์นั้นจะถูกระบุให้อยู่ในสถานะที่ไม่สามารถติดต่อได้ (Down State) ซึ่งเวลาที่ใช้ไปในการเปลี่ยนสถานะของเราท์เตอร์ให้เป็น Down นั้นเรียกว่า “Dead time” (ถ้าค่า Timer = 10 วินาที เวลา Dead time = 40 วินาที)
4. สำหรับการ Advertise routing บนโปรโตคอล OSPF โดยปกติเมื่อมีการ Advertise ข้าม Area กัน OSPF จะ Summarized network ก่อนจึงจะ advertise ไป

ในตัวอย่างกำหนดให้มี 3 Area คือ Area 0 , Area 1 , Area 2 โดยทุกเราท์เตอร์ที่เชื่อมต่ออยู่ใช้โปรโตคอล OSPF ทั้งหมด สำหรับข้อมูลเบื้องต้นในแต่ละเราท์เตอร์มีดังนี้

เราท์เตอร์ ก กำหนดให้

- อินเตอร์เฟส Serial 0 อยู่บน Area 0 มี IP Address = 10.100.20.1./30 เชื่อมต่อกับเราท์เตอร์ ข
- อินเตอร์เฟส Ethernet 0 อยู่บน Area 1 มี IP Address = 10.100.21.1./30 เชื่อมต่อกับเราท์เตอร์ ค

เราท์เตอร์ ข กำหนดให้

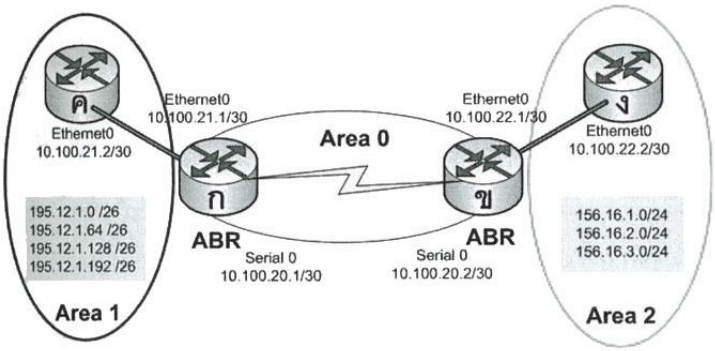
- อินเตอร์เฟส Serial 0 อยู่บน Area 0 มี IP Address = 10.100.20.2./30 เชื่อมต่อกับเราท์เตอร์ ก
- อินเตอร์เฟส Ethernet 0 อยู่บน Area 2 มี IP Address = 10.100.22.1./30 เชื่อมต่อกับเราท์เตอร์ ง

เราท์เตอร์ ค กำหนดให้

- อินเตอร์เฟส Ethernet 0 อยู่บน Area 1 มี IP Address = 10.100.21.2./30 เชื่อมต่อกับเราท์เตอร์ ก
- อินเตอร์เฟส Ethernet 1 มีเชื่อมต่อกับเน็ตเวิร์ค 195.12.1.0/26, 195.12.1.64/26, 195.12.1.128/26, 195.12.1.192/26

เราท์เตอร์ ง กำหนดให้

- อินเตอร์เฟส Ethernet 0 อยู่บน Area 2 มี IP Address = 10.100.22.2./30 เชื่อมต่อกับเราท์เตอร์ ข
- อินเตอร์เฟส Ethernet 1 มีเชื่อมต่อกับเน็ตเวิร์ค 156.16.1.0/24, 156.16.2.0/24, 156.16.3.0/24



ตัวอย่างเครือข่าย โดย Advertise routing บน OSPF

จากตัวอย่างเครือข่ายดังรูป ในที่นี้จะพิจารณาเฉพาะการ Advertise เน็ตเวิร์คภายในที่เชื่อมต่อกับเราท์เตอร์ ค และเราท์เตอร์ ง นั่นคือ เน็ตเวิร์ค 195.12.x.x, 156.16.x.x ดังนั้น เมื่อโปรโตคอล OSPF Advertise ตามเครือข่ายข้างต้นจะได้เราท์ติ้งของเน็ตเวิร์ควง 195, 156 ในแต่ละเราท์เตอร์ ดังนี้

Destination	Netmask	Gateway	Router Interface
156.16.0.0	/22	10.100.21.1	Ethernet 0
195.12.1.0	/26	Direct Connect	Ethernet 1
195.12.1.64	/26	Direct Connect	Ethernet 1

195.12.1.128	/26	Direct Connect	Ethernet 1
195.12.1.192	/260	Direct Connect	Ethernet 1

ตารางเราท์ติ้งหลังการ Advertise ของเราท์เตอร์ ค

Destination	Netmask	Gateway	Router Interface
156.16.0.0	/22	10.100.20.2	Serial 0
195.12.1.0	/24	10.100.21.2	Ethernet 0

ตารางเราท์ติ้งหลังการ Advertise ของเราท์เตอร์ ก

Destination	Netmask	Gateway	Router Interface
156.16.0.0	/22	10.100.22.2	Ethernet 0
195.12.1.0	/24	10.100.20.2	Serial 0

ตารางเราท์ติ้งหลังการ Advertise ของเราท์เตอร์ ข

Destination	Netmask	Gateway	Router Interface
195.12.1.0	/24	10.100.22.1	Ethernet 0
156.16.1.0	/24	Direct Connect	Ethernet 1
156.16.2.0	/24	Direct Connect	Ethernet 1
156.16.3.0	/24	Direct Connect	Ethernet 1

ตารางเราท์ติ้งหลังการ Advertise ของเราท์เตอร์ ง

ICMP

ICMP (Internet Control Message Protocol)

ICMP หรือ Internet Control Message Protocol เป็นโปรโตคอลที่มาเสริมให้กับ Internet Protocol เนื่องจาก Internet Protocol ไม่ได้มีคุณสมบัติในการรับประกันความครบถ้วนของข้อมูลในการส่งไปยังปลายทาง เช่น หากเกิดปัญหาเน็ตเวิร์คหลุดขาดการติดต่อกับเครื่องปลายทาง หรือเกิดความคับคั่งของข้อมูลบนเน็ตเวิร์คสูงมากจนเป็นเหตุให้แพ็กเก็ตสูญหาย เป็นต้น เราจะไม่ทราบเลยว่าข้อมูลที่ส่งไปครบถ้วน

หรือไม่ ด้วยเหตุนี้จึงมีโปรโตคอล ICMP เข้ามาช่วยในเรื่องการแจ้งผลข้อผิดพลาดที่เกิดขึ้นในการส่งข้อมูลของ Internet Protocol เช่น “Destination Unreachable” “Request Time out” เป็นต้น

แต่ทว่าโปรโตคอล ICMP ไม่ใช่เข้ามาช่วยทำให้ Internet Protocol รู้ตัวว่าส่งข้อมูลไม่ครบแล้วจัดส่งใหม่ แต่โปรโตคอล ICMP ทำหน้าที่เฉพาะแจ้งข่าวสารเท่านั้น

ประเภทของ ICMP Message

ในบรรดาข้อความตอบกลับของโปรโตคอล ICMP เราสามารถแบ่งออกได้เป็น 2 ประเภทใหญ่ ๆ คือ

1. **ข้อความแสดงข้อผิดพลาดที่ตรวจพบ (Error Message)** เราสามารถแบ่งหัวข้อหลัก ๆ ของข้อผิดพลาดที่ตรวจพบได้ ดังนี้
   1.1 **Destination Unreachable** โดยปกติข้อผิดพลาดนี้จะเกิดขึ้นเมื่อเครื่องต้นทางติดต่อเครื่องปลายทางไม่ได้ ซึ่งจำแนกได้จากหลายสาเหตุ เช่น
      - อุปกรณ์เราท์เตอร์ไม่สามารถส่งต่อแพ็กเก็ตไปยังเครื่องปลายทางได้ อันเนื่องมาจากปัญหาทางเน็ตเวิร์ค หรือปัญหาของเครื่องปลายทางก็ตาม
      - ไม่สามารถติดต่อเครื่องปลายทางได้แม้ว่าจะอยู่บนเน็ตเวิร์ควงเดียวกัน
      - แพ็กเก็ตส่งถึงปลายทางได้แต่ค่า TOS (Type of Service) ผิดปกติ
      - ไม่สามารถติดต่อกับโปรโตคอลที่ต้องการได้
      - พอร์ตไม่เปิด

   1.2 **Source Quench** ข้อความแสดงข้อผิดพลาดนี้จะเกิดขึ้นเมื่อเครื่องปลายทางหรือเกตเวย์ไม่สามารถรองรับและประมวลผลให้กับจำนวน Internet Datagram ที่เข้ามาในปริมาณมาก ๆ ได้ทันก็จะหยุดและปฏิเสธ Internet Datagram ที่เข้ามาใหม่พร้อมทั้งส่งแพ็กเก็ต Source Quench แจ้งกลับไปยังเครื่องต้นทางให้รับทราบ

   1.3 **Time Exceeded** ข้อผิดพลาดนี้เกิดขึ้นจากการที่ค่า TTL (Time-To-Live) ลดลงจนเหลือ 0 ซึ่งแพ็กเก็ตที่ส่งนี้จะถูกลบออกจากระบบทันที โดยทั่วไปการจะทำให้ค่า TTL เป็น 0 อาจเกิดขึ้นจากสาเหตุดังนี้
      - เราท์เตอร์หรือเกตเวย์ที่ส่งต่อแพ็กเก็นไปเรื่อย ๆ แต่ไม่สามารถส่งถึงปลายทางได้ก่อนค่า TTL = 0
      - ในกรณีข้อมูลที่ส่งนั้นมีหลาย Internet Datagram (หลาย Fragments) เมื่อปลายทางได้รับแล้วจะรวม Fragments นั้น ๆ เข้าด้วยกัน แต่ถ้าเกิดมี Fragment หายไปเพียงแพ็กเก็ตเดียวก็จะทำให้ไม่สามารถรวม Internet Datagram เป็นข้อมูลชุดเดิมได้จนกระทั่ง TTL = 0

   1.4 **Parameter Problem** ข้อผิดพลาดนี้เกิดขึ้นจากการที่เครื่องปลายทางหรือเกตเวย์ตรวจพบว่ามีค่าพารามิเตอร์ในเฮดเดอร์ไม่ถูกต้องหรือหายไปก็จะลบ Internet Datagram นั้นทิ้งพร้อมทั้งแจ้งกลับด้วยข้อผิดพลาดนี้
2. **ข้อความแจ้งข่าวสารทั่วไป (Information Message)** ข้อความอีกประเภทของ ICMP คือการแจ้งข้อมูข่าวสารทั่วไป โดยแบ่งเป็นหัวข้อหลัก ๆ ได้ดังนี้

1.1 **Echo Message** ข้อความ Echo นี้โดยปกติจะพบจากการเรียกใช้คำสั่ง ping ซึ่งจะมีการส่ง Echo request และตอบกลับด้วย Echo Reply โดยการระบุว่า Identifier และ Sequence Number ตัวเดียวกัน

1.2 **Redirect Message** ข้อความนี้จะถูกแจ้งไปยังเครื่องต้นทางให้รู้ถึงเส้นทางใหม่ในการส่งข้อมูลที่เร็วกว่า ดังตัวอย่างเช่น เครื่องต้นทาง A ต้องการส่งข้อมูลไปหาเครื่องปลายทาง B ที่อยู่คนละเน็ตเวิร์คกัน ดังนั้น เครื่องต้นทาง A จะต้องส่งข้อมูลผ่านเกตเวย์ที่รู้จัก สมมติเป็นเราท์เตอร์ X โดยเราท์เตอร์ X ก็ตรวจสอบตารางเราท์ติ้งแล้วว่าต้องส่งต่อเราท์เตอร์ Y ให้ส่งเครื่องปลายทาง B อีกที คราวนี้ถ้าเราท์เตอร์ Y ตรวจพบว่าข้อมูลที่ถูกส่งมานี้มาจากเครื่องต้นทางที่อยู่บนเน็ตเวิร์คที่ตัวเองเชื่อมต่ออยู่แล้ว มันจะส่งข้อความ Redirect Message แจ้งกลับไปยังเครื่องต้นทาง A ว่าคราวต่อไปถ้าจะส่งหาเครื่อง B อีกให้ส่งตรงมาที่เราท์เตอร์ Y ได้เลย

1.3 **Information Message** ข้อความนี้มีการนำมาใช้ในเรื่องของการส่งข้อความออกไปบนเน็ตเวิร์คเพื่อถามหาสิ่งที่ต้องการ เช่น กรณีของเครื่องแบบ Diskless ที่ไม่สามารถบู๊ตระบบด้วยตัวเองได้ จะมีการส่งข้อความนี้ไปบนเน็ตเวิร์คเพื่อถามหา IP Address และข้อมูลที่ต้องใช้ในการบู๊ต แต่ปัจจุบันโปรโตคอล RARP และ BOOTP ทำหน้าที่นี้ได้ดีกว่าจึงเลิกใช้ ICMP ไป

1.4 **Timestamp Message** ในกรณีที่ส่งข้อมูลโดยมีการระบุเวลา (Timestamp) มาด้วย เครื่องปลายทางจะต้องมีการส่งข้อความตอบกลับพร้อมระบุเวลาด้วยเรียกว่า Timestamp Reply โดยในแพ็กเก็ตจะมีการระบุค่าเวลา 3 ค่าด้วยกันคือ

- Originate Timestamp คือ เวลาที่เครื่องต้นทางส่งออกมา
- Receive Timestamp คือ เวลาที่เครื่องปลายทางได้รับข้อมูลมา
- Transmit Timestamp คือ เวลาก่อนที่เครื่องปลายทางจะส่งข้อมูลตอบกลับ

1.5 **Router Advertisement and Solicitation Message** อุปกรณ์เราท์เตอร์มีการเรียกใช้โปรโตคอลเกี่ยวกับการค้นหาเส้นทาง หรือเรียกอีกชื่อว่า “Router Discovery Protocol” ซึ่งจะมีส่วนของการสนับสนุนการใช้โปรโตคอล ICMP ในการแจ้งข้อมูลของผลการค้นหา เป็นคำสั่งที่ใช้ตรวจสอบดูว่าเครื่องปลายทางมีสถานะคงอยู่หรือไม่

BGP

BGP (Border Gateway Protocol) เป็นโปรโตคอลจัดเส้นทางข้อมูลประเภท EGP (Exterior Gateway Routing) ซึ่งใช้สำหรับการเชื่อมต่อเครือข่ายระว่าง AS โปรโตคอล BGP จะใช้พอร์ต 179 ของโปรโตคอล TCP เพื่อใช้ในการแลกเปลี่ยนข้อมูลระหว่างเราท์เตอร์ ซึ่งจะมีการสร้างเชื่อมต่อก่อนที่จะแลกเปลี่ยนข้อมูลระหว่างเราท์เตอร์ ข้อมูลที่เราท์เตอร์ทั้งสองใช้เพื่อการแลกเปลี่ยนกัน รวมไปถึงข้อมูลที่แสดงถึงความสามารถในการสื่อสารกันได้ ข้อมูลนี้จะช่วยให้เราท์เตอร์สามารถสร้างเส้นทางที่ปราศจากลูป (Loop) อีกทั้งเราท์เตอร์ยังใช้เพื่อเป็นการกำหนดเส้นทางเชิงนโยบายที่มีเนื้อหาตามที่กำหนด

ชนิดของข่าวสารที่ใช้ใน BGP มีอยู่ 4 แบบ ดังนี้

- **Open Message** – ใช้เพื่อการสถาปนาจัดตั้งการเชื่อมต่อระหว่างเราท์เตอร์
- **Keepalive** – เป็นข้อมูลที่ใช้ทักทายเราท์เตอร์เพื่อนบ้าน โดยการส่งออกมาเป็นห้วงเวลาที่แน่นอน เพื่อยืนยันว่าเส้นทางนั้นยังใช้งานได้อยู่

- **Update Message** – ประกอบด้วข้อมูลเกี่ยวกับเส้นทาง รวมทั้งคุณสมบัติของแต่ละเส้นทาง ข้อมูล ภายในข้อความที่ส่งนี้ครอบคลุมไปถึงเส้นทางที่ถูกถอดออกจากเราท์ติ้งเทเบิล
- **Notification** – ใช้เพื่อการแจ้งเตือนความผิดพลาดที่เกิดขึ้น

แต่ละ AS นั้นจะต้องมีหมายเลขประจำ ซึ่งจะเรียกว่า “ASN (Autonomous System Number)” โดยหลักการแล้ว ANS เป็นเลขหมายในทางตรรกะที่กำหนดให้กับเราท์เตอร์ทุกตัวที่ทำงานอยู่ภายใต้ระบบการจัดการเดียวกัน โดยเราท์เตอร์เหล่านี้จะมีการแชร์ข้อมูลเกี่ยวกับตารางเลือกเส้นทางหรือเราท์ติ้งเทเบิล และมีการอัพเดตภายใต้สภาวการณ์ปกติ โดยเฉพาะเมื่อมีการเปลี่ยนแปลงใด ๆ เกิดขึ้น

มาตรฐานการกำหนดหมายเลขา ASN อยู่ภายใต้การดำเนินงานจอง IANA (Internet Assigned Numbers Authority) ซึ่งเป็นผู้กำหนดหมายเลข ASN บนอินเทอร์เน็ต โดยเลขหมาย ASN นี้สามารถมีได้ตั้งแต่เลข 1 – 65,6535 โดยมีเลข 64,512 ไปจนถึง 65,535 ที่ถูกสำรองไว้ให้กับเครือข่ายส่วนตัวที่ไม่ได้ทำงานบนอินเทอร์เน็ต เช่นเดียวกับหมายเลข IP ที่มีการกำหนดให้บางช่วงไม่ได้ถูกนำมาใช้งานบนอินเทอร์เน็ต

BGP Attribute

ปกติโปรคโตคอลเลือกเส้นทางทั่วไปจะใช้วิธีการเลือกเส้นทางที่ดีที่สุดต่างกัน เช่น RIP จะใช้จำนวนฮ็อป (Hop) เป็นหลัก ในขณะที่ IGRP ใช้แบนด์วิธเป็นหลัก ส่วน EIGRP ใช้การผสมผลานกันระหว่างแบนด์วิธและดีเลย์ (Delay) เป็นแนวทางในการเลือกเส้นทาง นอกจากนี้ OSPF ใช้ค่าคอสต์ (Cost) เป็นหลัก แต่ BGP ใช้แอตทริบิวต์ (Attribute) เป็นหลักในการเลือกเส้นทางที่ดีที่สุด การใช้แอตทริบิวต์ของ BGP ไม่เพียงแต่ต้องการรีบข้อมมูลเกี่ยวกับเส้นทางเท่านั้น แต่ใช้เพื่อพิสูจน์เส้นทางที่ดีที่สุดที่จะเดินทางไปสู่ปลายทางด้วย BGP ประกอบด้วยแอตทริบิวต์ต่าง ๆ ดังต่อไปนี้

- **Weight Attribute** – เป็นมาตรฐานของซิสโก้ที่เราท์เตอร์ใช้เป็นการภายใน ค่า Weight Attributeนี้จะไม่มีการประกาศออกไปที่เราท์เตอร์เพื่อนบ้าน ถ้าหากเราท์เตอร์ได้เรียนรู้ และพบว่ามีเส้นทางมากกว่าหนึ่งที่จะเดินทางไปสู่ปลายทาง ดังนั้น เส้นทางที่มีค่า Weight สูงสุดจะได้รับการพิจารณาว่า เป็นเส้นทางแรกที่จะเลือก
- **Local Preference Attribute** – เป็นแอตทริบิวต์ที่จะบ่งบอกแก่ AS เกี่ยวกับเส้นทางที่ต้องการใช้เป็นทางออกไปจาก AS เพื่อเดินทางไปสู่เครือข่ายปลายทาง เส้นทางใดมีค่า Local Preference ที่สูงกว่าจะได้รับเลือกก่อน
- **Multi-exit Discriminator หรือ Metric Attribute** – บางครั้งถูกเรียกว่า “Multi-exit Discriminator (MED, BGP-4)” หรือ “Inter-AS (BGP3)” เป็นแอตทริบิวต์ที่ชี้นำสู่เพื่อนบ้านที่อยู่ภายนอก AS เกี่ยวกับเส้นทางที่เหมาะสมที่จะเข้ามาใน AS แห่งนี้ โดยเฉพาะในกรณีที่มีหลายเส้นทางที่จะเข้ามาภายใน ซึ่ง Metric Attribute จะชี้แนะแก่ AS อื่นได้ทราบถึงเส้นทางที่ดีที่สุดที่จะเข้ามาภายใน AS นี้ (ค่า Metric ยิ่งน้อยยิ่งเป็นที่ต้องการ)
- **Origin Attribute** – เป็นแอตทริบิวต์ที่เป็นดั้งเดิมของ BGP โดยเป็นแอตทริบิวต์ที่แสดงถึงข่าวสารที่เกี่ยวกับจุดเริ่มต้นของเส้นทาง ประกอบด้วยค่า 3 ประการ ดังนี้

    - IGP : ข้อมูลเกี่ยวกับเส้นทางที่จะเข้าถึงเครือข่าย
    - EGP : ข้อมูลเกี่ยวกับเส้นทางที่จะเข้าถึงเครือข่ายที่ได้รับการเรียนรู้โดย EGP ซึ่งจะบ่งบอกเป็นตัวอักษร “e” ในตาราง BGP
    - Incomplete : ข้อมูลเกี่ยวกับเส้นทางสู่เครือข่ายที่ได้รับการเรียนรู้โดยเหตุผลอื่น ๆ เช่น การทำ Redistribute Static Router เข้าไปที่ BGP และข้อมูลเส้นทางเกี่ยวกับต้นทางไม่สมบูรณ์

- **AS_Path Attribute** – เมื่อใดก็ตามที่มีข้อมูลเกี่ยวกับเส้นทางที่ผ่านการอัพเดตวิ่งผ่าน AS ใด จะมีการเติมเลขหมาย AS เข้าไปในข้อความอัพเดตนั้นด้วย เช่น ถ้าแพ็กเก็ตเราท์ติ้งอัพเดตวิ่งผ่าน AS100, AS200 และ AS300 ก็จะมีการบันทึกเลขหมาย AS ลงไปไว้ใน Update นี้เสมอ กล่าวได้ว่า AS_Path Attribute เป็นรายชื่อของ AS ที่แพ็กเก็ตอัพเดตเราท์ได้วิ่งผ่านและบันทึกไว้ เพื่อให้ทราบว่ามาจากที่ใด เพื่อที่จะเดินทางสู่จุดหมายปลายทาง
- **Next Hop Attribute** – เป็นหมายเลขไอพีของฉ็อปต่อไปที่จะใช้เพื่อเดินทางไปสู่เครือข่ายปลายทาง
- **Community Attribute** – เป็นวิถีทางที่จะรวมกลุ่มเส้นทางที่เป็นปลายทางเข้าด้วยกันเป็นกลุ่ม เราเรียกว่า “Community” มีการใช้ Route Map เพื่อจัดตั้ง Community Attribute ปกติค่า Community Attribute ที่มีมาแต่เดิม ได้แก่
    - No Export ไม่มีการประกาศเส้นทางนี้ไปสู่ Router BGP ที่อยู่ต่าง AS กัน
    - No Advertise ไม่มีการประกาศเส้นทางนี้สู่เราท์เตอร์ที่เชื่อมต่อกันใด ๆ
    - Internet ให้ประกาศเส้นทางนี้ไปสู่ Internet Community สู่เราท์เตอร์ทุกตัวที่อยู่บนเครือข่ายอินเทอร์เน็ต

<u>การเลือกเส้นทางของ BGP</u>

BGP สามารถรับการประกาศเส้นทางหลาย ๆ ชุด สำหรับปลายทางเดียวกัน โดยเส้นทางหลาย ๆ ชุดนี้มาจากแหล่งต่าง ๆ กันหลายแห่งได้ แต่ BGP จะเลือกเส้นทางใดเส้นทางหนึ่งที่เห็นว่าดีที่สุด เมื่อเส้นทางที่ดีที่สุดถูกเลือกแล้ว BGP จะนำเส้นทางที่ดีที่สุดที่เลือกแล้วนี้ไปไว้ในตารางจัดเส้นทางหรือเราท์ติ้งเทเบิล จากนั้นก็จะเผยแพร่เส้นทางนี้ไปให้เราท์เตอร์เพื่อนบ้าน BGP ใช้ตัวเลือกต่อไปนี้เพื่อการเลือกเส้นทางไปสู่ปลายทาง

- หากเส้นทางระบุปลายทางที่ไม่สามารถเข้าถึงได้ จะมีการยกเลิกการอัพเดต
- BGP สนใจแต่เส้นทางที่มีค่า Weight มากที่สุด
- หากเส้นทางใดมีค่า Weight เท่ากัน ก็จะเลือกเส้นทางใดที่มีค่า Local Preference มากที่สุด
- หากค่า Local Preference มีค่าเท่ากัน จะเลือกเส้นทางที่มีจุดเริ่มต้นที่ BGP ของเราท์เตอร์ตัวปัจจุบัน
- หากไม่มีที่ใดที่เป็นต้นทางของเส้นทาง จะเลือกเส้นทางที่มีค่า AS_Path ที่สั้นที่สุด
- หากทุกเส้นทางต่างก็มีค่า AS_Path ที่เท่ากันทั้งหมด ให้เลือกเส้นทางที่มีค่า Origin น้อยที่สุด (IGP มีค่าน้อยกว่า EGP และ EGP มีค่าน้อยกว่า Incomplete)
- หากค่า Origin เท่ากัน ให้เลือกเส้นทางที่มีค่า MED ต่ำที่สุด
- หากเส้นทางนั้นมีค่า MED เท่ากัน ให้เลือกเส้นทางภายนอกที่เหนือกว่าเส้นทางภายใน
- หากเส้นทางทั้งสองมีค่าเท่ากัน ให้เลือกเส้นทางผ่านมายัง IGP ที่ใกล้ที่สุด
- เลือกเส้นทางที่มีค่า IP Address ต่ำที่สุดดังที่กำหนดไว้ใน Router ID ของ GRP Router
    - เวอร์ชันปัจจุบัน BGP คือ เวอร์ชัน 4 (BGP-4) ซึ่งกำหนดใน RFC 1771 ซึ่งมีการใช้งานบนเครือข่ายอินเทอร์เน็ต BGP เป็นดิสแทนซ์เวคเตอร์อัลอกริทึมแต่ก็มีเทคนิคที่เพิ่มเข้าไป

(จตุชัย แพงจันทร์ และ อนุโชต วุฒิพรพงษ์, 2555)

NAT

สืบเนื่องจากปัญหาหมายเลข IP Address ของ IP Version 4 (IPV4) ที่มีการใช้งานอยู่ในปัจจุบันไม่สามารถรองรับกับการเติบโตขององค์กร หน่วยงาน หรือผู้ใช้บริการที่มีความต้องการเชื่อมต่อเครือข่ายในโลกของอินเทอร์เน็ตได้ แนวทางการแก้ปัญหาระยะยาวก็คือ การเปลี่ยนมาใช้ IP Version 6 (IPV6) ซึ่งมีการเพิ่มจำนวนบิตที่ใช้จาก 32 บิต มาเป็น 128 บิต ทำให้มีหมายเลข IP Address เพิ่มขึ้นอีกมหาศาล

แต่ถ้าในระยะสั้นที่เรายังคงใช้ IPV4 อยู่และในแต่ละองค์กรที่ได้รับ IP Address จริงไม่มาก เราคงไม่สามารถให้ทุกเครื่องภายในองค์กรใช้ IP Address จริงได้ทั้งหมด ดังนั้น จึงต้องมีวิธีการอย่างใดอย่างหนึ่งที่จะช่วยให้เครื่องที่อยู่ในเน็ตเวิร์คขององค์กร (Private Network) สามารถเชื่อมต่ออินเทอร์เน็ตได้ (Public Network) โดยที่ใช้ IP Address จริงในจำนวนจำกัด และวิธีการที่ว่านี้ก็คือ “IP NAT” หรือ IP Network Address Translation ซึ่งเป็นเทคโนโลยีที่สนับสนุนอยู่ใน Internet Protocol โดยเป็นคุณสมบัติที่อุปกรณ์เราท์เตอร์ หรือไฟร์วอลล์ หรืออุปกรณ์ NAT ใช้ในการแมประหว่าง Private IP Address Public IP Address ซึ่งมีวิธีการหลายแบบด้วยกัน ดังจะกล่าวในรายละเอียดต่อไป

ข้อดีของการใช้ IP NAT

1. เราสามารถแชร์ IP Address จริง (Public IP Address) ที่มีจำนวนน้อยให้พอเหมาะกับจำนวนเครื่องที่เปิดให้บริการได้โดยที่เราไม่ต้องเสียเงินเพิ่มเลย
2. มีความปลอดภัยสูงขึ้นเนื่องจากเครื่องที่ให้บริการจริง ๆ จะใช้ Private IP Address ซึ่งบุคคลภายนอกไม่อาจรู้ได้
3. การลดหรือขยายเครื่องที่ให้บริการกับภายนอกทำได้ง่าย เพียงแค่ปรับแก้คอนฟิกเพิ่ม หรือลด Private IP Address เท่านั้น
4. การเปลี่ยนผู้ให้บริการอินเทอร์เน็ต (ISP-Internet Service Provider) สามารถทำได้ง่ายเพียงแต่เปลี่ยนหมายเลข IP Address จริงเท่านั้น (Public IP Address)
5. การบำรุงรักษาระบบสามารถเชื่อมต่อได้จาก Private Network โดยแยกกันกับ Public Network ซึ่งจะเพิ่มความปลอดภัยยิ่งขึ้น
6. การแมประหว่าง Private IP Address และ Public IP Address ไม่ส่งผลกระทบต่อการทำงานโดยปกติ

ข้อเสียของการใช้ IP NAT

1. หากเกิดปัญหาการไล่หาสาเหตุจะทำยุ่งยากขึ้น เนื่องจากการทำ IP NAT มักจะใช้หลาย Private IP Address ต่อ 1 Public IP Address ไม่ใช่แบบ 1 ต่อ 1
2. ในเรื่องระบบการรักษาความปลอดภัยหากถูกบุกรุกโดยบุคคลอื่น เราสามารถย้อนรอยกลับไปได้เพียงโดเมนและ Public IP Address ที่ใช้ แต่จะไม่สามารถสืบจนถึงเครื่องที่ประสงค์ร้ายได้
3. ในเรื่องของประสิทธิภาพการทำงานโดยรวมจะลดลงหากเทียบกับปกติ เนื่องจากระบบจะต้องใช้ทรัพยากรและเวลาส่วนหนึ่งในการแปลงหมายเลขระหว่าง Private Address/Public Address
4. อาจทำให้บางแอพพลิเคชันใช้งานไม่ได้ เนื่องจาก NAT จะมีการเปลี่ยนแปลงที่ IP Header เท่านั้น ถ้ามีแอพพลิเคชันมีการระบุ IP Address ลงไปในตัวข้อมูลที่ส่งออกไป หมายเลข IP Address นั้นจะไม่ได้ถูกทำ NAT ซึ่งอาจส่งผลให้แอพพลิเคชันเกิดปัญหาได้

Notes

ในที่นี้จะมีการพูดถึงคำว่า “Private” “Public” ทั้ง IP Address และ Network ซึ่งอาจทำให้สับสนได้ดังนั้น ขอสรุปให้อีกครั้งดังนี้

- Private Network หมายถึง เน็ตเวิร์คที่เชื่อมต่ออยู่เฉพาะภายในองค์กรเดียวกัน ไม่ว่าจะเป็นตึกเดียวกัน หรือสาขาต่าง ๆ ที่เชื่อมถึงกัน โดย IP Address ที่ใช้จะรู้จักเฉพาะองค์กรนี้เท่านั้น
- Private IP Address หมายถึง IP Address ที่เราใช้ในการเชื่อมต่อกันภายในองค์กรเราเท่านั้น ซึ่ง IP Address นี้จะไม่ใช่ IP Address จรงิที่จะใช้ในการติดต่อกับโลกภายนอกหรือบนอินเทอร์เน็ตได้
- Public Network หมายถึง เน็ตเวิร์คที่เชื่อมกันภายนอกองค์กรที่โยงใยกันทั่วโลกหรือเรียกว่า World Wide เป็นเน็ตเวิร์คสากลที่ทำให้ทุกองค์กรสามารถติดต่อกันได้ ซึ่งเราอาจพูดได้ว่าเป็นเน็ตเวิร์คบนโลกอินเทอร์เน็ตก็ได้
- Public IP Address หมายถึง IP Address จริงที่องค์กรสากลได้นำมาใช้ในการติดต่อเชื่อมโยงกันทั่วโลก โดย Public IP Address เราสามารถขอได้จากผู้ให้บริการอินเทอร์เน็ตหรือ ISP (Internet Service Provider)

ประเภทของ NAT Address Mapping

ในการแปลง Private IP Address เป็น Public IP Address หรือแปลงในทางกลับกันก็ตาม เราจะต้องกำหนดค่า Address Mapping ระหว่าง IP Address 2 ชุดไว้ก่อนว่าจะให้ IP Address หมายเลขอะไรเปลี่ยนไปเป็นหมายเลขอะไร ซึ่งการกำหนดว่า Address Mapping นี้เองก็มีวิธีการทำได้ 2 แบบด้วยกันคือ Static NAT และ Dynamic NAT ดังรายละเอียดต่อไปนี้

Static NAT

เป็นการกำหนดค่า Address Mapping แบบ 1 – 1 นั่นคือ จะมีการกำหนดไปเลยว่า Private IP Address หมายเลข 100 เมื่อ NAT แล้วจะแปลงเป็น Public IP Address หมายเลข 200 เสมอ

ตัวอย่างเช่น Proxy เซิร์ฟเวอร์เครื่องหนึ่งมี Local IP Address เป็น 192.168.3.100 เมื่อเชื่อมต่ออินเทอร์เน็ตแล้วต้องการให้แปลง IP Address เป็น 203.168.21.100 นั่นหมายความว่า ทุกครั้งที่เครื่อง Proxy เชื่อมต่ออินเทอร์เน็ตเมื่อไรคนภายนอกจะรู้จัก Proxy เครื่องนี้ด้วย IP 203.168.21.100 เสมอ

Dynamic NAT

เป็นการกำหนดค่า Address Mapping โดยไม่ยึดติดแบบ 1-1 แต่จะกำหนด Public IP Address จำนวนหนึ่งไว้รองรับกับการทำ IP NAT โดยเมื่อมี Private IP Address ร้องขอการแปลง IP ก็จะนำ Public IP ที่จองไว้และยังไม่ได้ถูกนำไปทำ NAT ให้กับ Private IP ไหนมาใช้ และเมื่อปฏิบัติงานเสร็จสิ้นก็จะมีการคืน Public IP นั้นกลับมาแชร์ไว้อีก

ตัวอย่างเช่น มีการจอง Public IP ตั้งแต่ 203.168.21.10 – 203.168.21.110 จำนวน 11 หมายเลข เมื่อเครื่อง Proxy 1 IP Address 192.168.3.100 ต้องการ NAT ออกอินเทอร์เน็ต อุปกรณ์หรือซอฟต์แวร์ทีททำ NAT ก็จะไปแมปจากชุด IP ที่สำรองไว้ 11 หมายเลข สมมติว่าแมปเป็นเบอร์ 203.168.21.100 ดังนั้นจำนวน Public IP ที่ใช้ได้จะเหลืออีก 10 หมายเลข ถ้าหากเครื่อง Proxy 2 IP Address 192.168.3.200 มาร้องขอ NAT ระบบก็จะเลือก Public IP ที่ว่าง สมมติว่าแมปเป็น 203.168.21.101 ซึ่งหากเครื่อง Proxy ทั้งสองเลิกเชื่อมต่ออินเทอร์เน็ตก็จะคืนหมายเลข Public IP 203.168.21.100, 101 ไว้ใช้ต่อไป

รูปแบบการทำ IP NAT

ในการติดต่อกันระหว่างเครื่องที่อยู่บน Private Network และเครื่องที่อยู่ Public Network เราสามารถทำได้หลายรูปแบบขึ้นอยู่กับวัตถุประสงค์ในการติดต่อ เช่น ต้องการให้มีการทำ NAT แบบ One-Way

คือ เปิดให้ข้างนอกเข้ามาใช้บริการหรือจะเปิดให้ภายในไปใช้บริการข้างนอกอย่างใดอย่างหนึ่ง เป็นต้น หรือในกรณีที่มีการเอา IP Address จริงมาใช้เป็น Private Network เพราะคิดว่าคงไม่มีการเชื่อมต่ออินเทอร์เน็ต แต่พอวันหนึ่งต้องมีการเชื่อมต่อแล้วจะทำอย่างไรเพราะอาจเกิดกรณี Private IP Address ซ้ำกับ Public IP Address เป็นต้น ดังนั้น การทำ IP NAT จึงมีหลายรูปแบบให้เลือกใช้ให้เหมาะกับสถานการณ์ปัจจุบัน ดังต่อไปนี้

Traditional Nat (Outbound NAT)

เป็นรูปแบบการทำ NAT แบบทางเดียวหรือเรียกว่า “Uni-directional NAT” นั่นคือ จะยอมให้เครื่องใน Private Network สร้างเซสชันและทำ NAT ออกไปหาเครื่องปลายทางที่อยู่บน Public Network ได้ โดยที่เครื่องปลายทางจะตอบกลับแพ็กเก็ตมาที่ IP NAT ของเครื่องต้นทางนี้ได้เท่านั้น จะไม่สามารถสร้างเซสชันขึ้นมาแล้วส่งมาติดต่อเครื่องต้นทางที่อยู่ภายใน Private Network ได้ ซึ่ง Traditional NAT ยังแบ่งย่อยการทำ NAT ออกเป็น 2 แบบด้วยกันคือ

1. **Basic Traditional NAT** เป็นการทำ NAT สำหรับ Private IP Address ก่อนจะติดต่อออกไปหาเครื่องปลายทางที่อยู่บน Public Network หรืออินเทอร์เน็ต ซึ่งจะเป็นการทำ NAT เฉพาะหมายเลข IP Address เท่านั้น โดยเมื่อแพ็กเก็ตที่ส่งออกไป (Outbound Packet) เมื่อถึงปลายทางแล้ว เครื่องปลายทางสามารถตอบกลับมาที่เครื่องต้นทางด้วย IP NAT นั้น ๆ ได้ (Inbound Packet) แต่จะไม่สามารถสร้างเซสชันเพื่อมาติดต่อเองได้

   ตัวอย่างการทำงาน สมมติว่าองค์กร A มีเครื่องต้นทาง IP Address = 192.168.3.100 ต้องการติดต่อกับเครื่องปลายทางที่เป็นเว็บไซต์ www.google.co.th (IP Address = 66.249.89.104) โดยจะมีการทำ Static NAT เป็น public IP = 203.168.21.110 ซึ่งจะมีรูปแบบการทำงานดังนี้

   1.1. เครื่องต้นทางสร้างแพ็กเก็ตพร้อมกำหนด Source IP = 192.168.3.100, Destination IP = 66.249.89.104 (www.google.co.th)

   1.2. อุปกรณ์เราท์เตอร์หรือไฟร์วอลล์จะ NAT โดยเปลี่ยน Source IP = 203.168.21.110 และเก็บค่าการทำ NAT ไว้สำหรับแปลงกลับเมื่อมีแพ็กเก็ตตอบกลับมา โดย Destination IP ยังเหมือนเดิมพร้อมกับส่งไปยังเครื่องปลายทาง

   1.3. เครื่องปลายทางได้รับแพ็กเก็ตการร้องขอมาจึงสร้างแพ็กเก็ตตอบกลับโดยกำหนด Source IP = 66.249.89.104 และระบุปลายทางเป็น Destination IP = 203.168.21.110 ตามที่ได้รับแพ็กเก็ตมา

   1.4. อุปกรณ์เราท์เตอร์ หรือไฟร์วอลล์จะ NAT Destination IP กลับไปเป็น Private IP Address เดิมคือแปลงกลับเป็น Destination IP = 192.168.3.100 และส่งแพ็กเก็ตไปยังเครื่องต้นทางที่อยู่บน Private Network ถือเป็นการจบกระบวนการติดต่อ 1 ครั้ง

2. **Network Address Port Translation (NAPT)** เป็นรูปแบบการทำ NAT ที่มีการนำชั้น Transport Layer เข้ามาเกี่ยวข้องด้วยนั่นคือ “พอร์ต” (Port) และ “ซ็อกเก็ต” (Socket) ซึ่งเปรียบเป็น Address ของโปรโตคอล TCP และ UDP โดยจะมีการ NAT ทั้ง Private IP Address และ Port/Socket ได้เป็น Public IP Address และ Port/Socket ใหม่ ก่อนจะติดต่อไปยังเครื่องปลายทาง ซึ่งเครื่องปลายทางก็จะตอบกลับมายัง Public IP Address และ Port/Socket ใหม่ของเครื่องต้นทางได้เท่านั้น ด้วยวิธีการนี้เอง ทำให้ไม่ต้องใช้ Public IP Address เยอะนัก

เพราะหมายเลข Port/Socket นั้น รองรับได้เป็นหมื่นหมายเลขซึ่งก็เปรียบเหมือนรองรับ Private IP Address ได้ถึงหมื่นเครื่องเช่นกัน

ตัวอย่างการทำงาน จากตัวอย่างเดิมข้างต้น องค์กร A มีเครื่องต้นทาง IP Address = 192.168.3.100 ต้องการติดต่อกับเครื่องปลายทางที่เป็นเว็บไซต์ www.google.co.th (IP Address = 66.249.89.104, Port = 80 (http)) โดยเครื่องต้นทางตอนติดต่อได้ใช้พอร์ตหมายเลข 1639 และมีการทำ NAT แบบ Port-Based (NAPT) เป็น 203.168.21.110 Port = 10000 โดยมีรูปแบบการทำงานดังนี้

1.1. เครื่องต้นทางสร้างแพ็กเก็ตพร้อมกำหนด Source IP = 192.168.3.100 Port = 1639, Destination IP = 66.249.89.104 Port = 80
1.2. อุปกรณ์เราท์เตอร์หรือไฟร์วอลล์ NAT โดยเปลี่ยน Source IP = 203.168.21.110 Port = 10000 และเก็บค่าการทำ NAT ไว้สำหรับแปลงกลับเมื่อมีแพ็กเก็ตตอบกลับมา โดย Destination IP, Port ยังเหมือนเดิมพร้อมกับส่งไปยังเครื่องปลายทาง
1.3. เครื่องปลายทางได้รับแพ็กเก็ตการร้องขอมาจึงสร้างแพ็กเก็ตตอบกลับโดยกำหนด Source IP = 66.249.89.104 Port = 80 และระบุปลายทางเป็น Destination IP = 203.168.21.110
1.4. Port =10000
1.5. อุปกรณ์เราท์เตอร์หรือไฟร์วอลล์ NAT Destination IP กลับไปเป็น Private IP Address เดิมคือ Destination IP = 192.168.3.100 Port = 1639 และส่งแพ็กเก็ตไปยังเครื่องต้นทางที่อยู่บน Private Network

Bi-directional Nat (Inbound NAT)

ในการทำ Traditional NAT ที่กล่าวมาข้างต้นจะเป็นแบบ One-Way Outbound NAT, ซึ่งเป็นการทำ NAT ให้กับเครื่องใน Private Network สร้างเซสชันไปติดต่อกับเครื่องปลายทางบนอินเทอร์เน็ตทางเดียวเท่านั้น แต่ถ้าเรามองในทางกลับกันหากเครื่องเซิร์ฟเวอร์ของเราเป็นผู้ให้บริการบ้าง และก็อยู่ใน Private Network ขององค์กรเรา จะมีวิธีการอย่างไรที่จะทำให้เครื่องที่อยู่บน Private Network หรืออินเทอร์เน็ตรู้จักและใช้บริการจากเซิร์ฟเวอร์เราได้

นั่นก็คือการทำ Two-Ways NAT หรือเรียกอีกชื่อว่า Inbound NAT ซึ่งเป็นการทำ NAT เครื่องเซิร์ฟเวอร์ใน Private Network ของเราให้มี Public IP Address หรือ IP Address จริงพื่อที่จะให้เครื่องภายนอกบนอินเทอร์เน็ตสามารถติดต่อมาใช้บริการได้

แต่การทำ Inbound NAT เท่านั้นคงไม่พอ ยังต้องพึ่งบริการของระบบ DNS เข้ามาช่วยด้วย โดยการทำ Public IP Address ที่กำหนดให้เป็น IP จริงหลังจากทำ Inbound NAT ไปลงทะเบียนในโดเมนบนระบบ DNS ก่อน ดังนั้น เมื่อเครื่องต้นทางบนอินเทอร์เน็ตต้องการจะติดต่อใช้บริการบนเซิร์ฟเวอร์ของเราจากภายนอก ก็จะสืบค้นในระบบ DNS โดยใช้ชื่อที่เราลงทะเบียนไว้ซึ่งระบบ DNS จะแมปชื่อที่ส่งมากสืบค้นให้เป็น Public IP Address และแจ้งกลับไปยังเครื่องต้นทาง ดังนั้น เครื่องต้นทางจึงสามารถส่งแพ็กเก็ตมายังเซิร์ฟเวอร์ของเราได้ ซึ่งจะมีรูปแบบการทำงานดังนี้

ตัวอย่างการทำงาน จากตัวอย่างเดิมข้างต้น องค์กร A มีเซิร์ฟเวอร์ IP Address = 192.168.3.234 เป็นเว็บมีบริการดาวน์โหลดหนังด้วย โดยใช้ชื่อเว็บไซต์เป็น www.whatmovies.co.th (IP Address = 203.168.21.111) ดังนั้น เมื่อต้องมีการให้บริการบนอินเทอร์เน็ตซึ่งเครื่องที่เข้ามาใช้บริการที่เว็บไซต์ของเราจะต้องสร้างเซสชันเพื่อร้องขอใช้บริการ ดังนั้น เพื่อให้ผู้ร้องขอใช้บริการรู้จกเซิร์ฟเวอร์ที่อยู่ในเน็ตเวิร์คภายในของเราได้ จึงมีการทำ Inbound NAT ซึ่งมีรูปแบบการทำงานดังนี้

1. เครื่องต้นทางสร้างแพ็กเก็ตเพื่อต้องการร้องขอใช้บริการโดยมีปลายทางเป็นเว็บไซต์ www.whatmovies.co.th ซึ่งเมื่อค้นหา IP Address จากระบบ DNS ได้เป็น 203.168.21.111 ดังนั้น จึงระบุ Destination IP Address = 203.168.21.111 และระบุ Source IP Address = 66.218.44.114 (สมมติว่าเครื่องต้นทางมี IP Address นี้)
2. อุปกรณ์เราท์เตอร์ หรือไฟร์วอลล์ได้รับแพ็กเก็ตโดยมีการระบุปลายทางเป็น Public IP Address = 203.168.21.111 ซึ่งมีการทำ Inbound NAT กับ Private IP Address หมายเลข 192.168.3.234 ดังนั้น จึงแปลง Destination IP Address เป็น 192.168.3.234 แล้วจึงส่งเข้ามายัง Private Network
3. เซิร์ฟเวอร์สร้างแพ็กเก็ตตอบกลับไปยังเครื่องที่ร้องขอบริการมา โดยระบุ Source IP Address = 192.168.3.234 และ Destination IP Address = 66.218.44.114
4. อุปกรณ์เราท์เตอร์หรือไฟร์วอลล์ NAT Private Source IP = 192.168.3.234 เป็น 203.168.21.111 แล้วส่งแพ็กเก็ตกลับไปยังเครื่องที่ร้องขอใช้บริการ

Overlapping NAT (Twice NAT)

เป็นการทำ NAT อีกรูปแบบที่แตกต่างกับ Traditional NAT และ Bi-directional NAT เพราะ Overlapping NAT หรือ Twice NAT จะเป็นการทำ NAT ทั้ง Source Address และ Destination Address เนื่องจากมีสาเหตุบางประการที่จำเป็นต้องใช้วิธีการนี้นั่นคือ

- กรณีที่ 1 ถ้ามีเน็ตเวิร์คใด ๆ กำหนด IP Address ที่ใช้ติดต่อภายใน Private Network เป็น Public IP Address ขึ้นมา จะทำให้เกิดความสับสนในกรณีที่เน็ตเวิร์ควงนี้มีการติดต่อกับเครื่องปลายทางที่อยู่ Public Network ได้ เนื่องจากอาจมีเครื่องภายนอกที่กำหนด Public IP Address ชนกับเราได้

ตัวอย่างเช่น เน็ตเวิร์ค A กำหนด IP Address ภายในองค์กรเป็น 203.168.4.0/24 ซึ่ง IP ชุดนี้เป็นหมายเลข IP Address ที่อาจมีใช้อยู่จริงบนอินเทอร์เน็ต ดังนั้น หากองค์กรนี้มีการเชื่อมต่อกับอินเทอร์เน็ตก็จะมีปัญหาในเรื่องของการส่งข้อมูลออกไปยังเครื่องปลายทางได้ ยิ่งถ้าเครื่องปลายทางมี Public IP Address ที่ตรงกับเน็ตเวิร์คภายในขององค์กรได้

- กรณีที่ 2 ถ้าหากมี 2 หน่วยงานกำหนด Private IP Address เป็นเน็ตเวิร์ควงเดียวกัน ซึ่งวันหนึ่ง ๆ มีการเชื่อมต่อเน็ตเวิร์คถึงกันโดยตรงก็จะทำให้เกิดปัญหาในการติดต่อสื่อสารกัน เนื่องจากหน่วยงานแรกหากจะส่งแพ็กเก็ตไปยังหน่วยงานที่ 2 อุปกรณ์เราท์เตอร์จะคิดว่าแพ็กเก็ตนั้นเป็นการส่งถึงเครื่องปลายทางที่อยู่บนเน็ตเวิร์คเดียวกัน ทำให้ไม่ส่งต่อแพ็กเก็ตไปยังเน็ตเวิร์คของหน่วยงานที่ 2

ตัวอย่างเช่น หน่วยงาน A กำหนดเน็ตเวิร์คภายในเป็นวง 192.168.3.0/24 และหน่วยงาน B ก็กำหนดเน็ตเวิร์คภายในเป็นวง 192.168.3.0/24 เช่นเดียวกัน แต่แล้ววันหนึ่งได้มีการสร้าง Leased line เชื่อมถึงกัน ซึ่งถ้าเครื่องในหน่วยงาน A IP = 192.168.3.100/24 ต้องการติดต่อเครื่องปลายทางในหน่วยงาน B IP = 192.168.3.200/24 ก็จะทำให้อุปกรณ์เราท์เตอร์ หรือเกตเวย์คิดว่าเป็นเครื่องปลายทางบน Local Network ก็จะไม่ส่งต่อแพ็กเก็ตไป

จากที่กล่าวมาข้างต้นเป็นสาเหตุให้เกิดปัญหาในการติดต่อกันขึ้นอันเนื่องมาจากการกำหนด IP Address ไม่เหมาะสม ดังนั้น วิธีการแก้ไขเพื่อให้สามารถใช้งานได้ในเบื้องต้นคือ การทำ Overlapping NAT

นั่นคือ จะมีการแปลง Source IP Address และ Destination IP Address ให้เป็น IP Address วงอื่นที่ไม่ซ้ำกันเพื่อไม่ให้เกิดความสับสน

ตัวอย่างการทำงานในกรณีที่เน็ตเวิร์คภายในมีการนำเอา Public IP Address มาใช้ เช่น 203.168.4.0/24 โดยสมมติว่าเครื่อง A IP Address 203.168.4.123 ต้องการใช้บริการเว็บไซต์ www.whatmusics.co.th (IP = 203.168.4.134) ซึ่ง IP Address ทั้งต้นทางและปลายทางเป็นวงเดียวกัน ดังนั้น จึงต้องมีการคอนฟิกบนอุปกรณ์เราท์เตอร์หรือไฟร์วอลล์เพื่อทำ Overlapping NAT โดยกำหนดให้

- ขา Private Network ติดต่อกับ Public Network ให้ทำ NAT 203.168.4.0/24 -> 204.10.11.0/24
- ขา Public Network ติดต่อกับ Private Network ให้ทำ NAT 203.168.4.0/24 -> 200.168.2.0/24

1. เครื่อง A สร้างแพ็กเก็ตเพื่อติดต่อเว็บไซต์ www.whatmusics.co.th (203.168.4.134) ซึ่งเป็น IP Address บน Public Network ที่จะติดต่อกับ Private Network ดังนั้น จึงมีการ NAT Public IP Address ก่อนให้เป็นวง 200.168.2.0/24 สมมติว่าเปลี่ยนเป็น 200.168.2.100 ดังนั้น แพ็กเก็ตจึงกำหนด Destination IP = 200.168.2.100 และ Source IP = 203.168.4.123
2. เมื่อส่งแพ็กเก็ตผ่านอุปกรณ์เราท์เตอร์หรือไฟร์วอลล์แล้ว ทั้ง Source Address และ Destination Address จะถูกทำ Overlapping NAT โดยแปลง Source Private IP Address จาก 203.168.4.123 เป็น Public IP Address ให้อยู่ในวงเน็ตเวิร์ค 204.10.11.0/24 สมมติว่าแมปเป็น 204.10.11.200 และจะแปลงกลับ Destination Public IP Address จาก 200.168.2.100 ให้เป็นค่า IP Address เดิมคือ 203.147.4.134 ดังนั้น จะได้ Source IP = 204.10.11.200 และ Destination = 203.168.4.134
3. เมื่อปลายทางได้รับแพ็กเก็ตร้องขอใช้บริการแล้วจะมีการสร้างแพ็กเก็ตและตอบกลับ โดยระบุ Source IP = 203.168.4.137 และ Destination IP = 204.10.11.200 ตามหมายเลข IP Address ที่ระบุมาจากแพ็กเก็ตที่ร้องขอ
4. เมื่อส่งผ่านอุปกรณ์เราท์เตอร์หรือไฟร์วอลล์แล้วจะถูกทำ Overlapping NAT อีกครั้ง โดยการแปลงกลับ Destination IP ให้มีค่าเป็น IP ดั่งเดิมคือ 203.168.4.123 และแปลง Source Public IP ให้เป็นหมายเลข 200.168.2.100 จึงจะสามารถติดต่อหาเครื่องต้นทางได้

Multihomed NAT

การทำ NAT โดยทั่วไปที่กล่าวมาข้างต้นจะเป็นการทำ NAT ผ่านอุปกรณ์เราท์เตอร์ หรือไฟร์วอลล์เพียงตัวเดียวซึ่งจะเชื่อมต่อกับ ISP เพียงตัวเดียว ดังนั้น เมื่อมีการทำ NAT ผ่านอุปกรณ์เราท์เตอร์หรือไฟร์วอลล์แล้ว ข้อมูลการแปลง IP Address จะถูกเก็บไว้ที่นี่ด้วยเพื่อที่จะสามารถแปลงกลับได้หากมีการตอบกลับมาจากปลายทาง แต่ถ้าอุปกรณ์เราท์เตอร์ หรือไฟร์วอลล์ที่มีเพียงชิ้นเดียวเกิดเสียใช้งานไม่ได้ หรือถ้าอุปกรณ์เชื่อมเน็ตเวิร์คของ ISP ที่ใช้บริการอยู่เสีย ระบบของเราก็จะไม่สามารถเชื่อมต่อไปที่ไหนได้เลย ซึ่งถือว่าเหตุการณ์นี้เป็นปัญหาแบบ Single Point of Failure

ด้วยเหตุนี้จึงได้มีการออกแบบให้มีการใช้อุปกรณ์เราท์เตอร์ หรือไฟร์วอลล์มากกว่า 1 ชิ้นในการทำ NAT และเชื่อมต่อกับบริษัท ISP ด้วย แต่การทำ NAT ด้วยรูปแบบนี้มีข้อจำกัดอยู่ว่าการคอนฟิกค่า NAT จะต้องทำแบบ Static NAT เท่านั้น โดยจะคอนฟิกให้เหมือนกันบนอุปกรณ์เราท์เตอร์ หรือไฟร์วอลล์ทุกตัวที่นำมาทำเป็น Multihomed NAT

NTP

NTP (Network Time Protocal) เป็นโปรโตคอลที่ใช้สำหรับการเทียบเวลา (Synchonize) ระหว่างอุปกรณ์คอมพิวเตอร์กับ Internal Time Servers ไม่ว่าจะผ่านสื่อกลางที่เป็นคลื่นวิทยุ ผ่านดาวเทียม หรือแม้แต่สัญญาณโทรศัพท์ก็สามารถเชื่อมต่อได้

สืบเนื่องจากการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ("พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550", 2558) ส่งผลให้องค์กรภาครัฐและเอกชนจำเป็นต้องปรับปรุงเทคโนโลยีสารสนเทศให้สอดคล้องกับพระราชบัญญัติ เพื่อให้ถูกต้องตามกฎหมายและตระหนักถึงความสำคัญของระบบคอมพิวเตอร์ในการเข้าถึงและใช้บริการยิ่งขึ้น

การเทียบเวลาให้มีความเที่ยงตรงกับกับเวลาอ้างอิงสากล เพื่อประโยชน์ในการจัดเก็บการทำงานของระบบคอมพิวเตอร์ และสามารถใช้ในการอ้างอิงเพื่อขอตรวจสอบจากทางเจ้าหน้าที่ภาครัฐ หากเกิดเหตุการณ์จำเป็นในการเรียกดูข้อมูลย้อนหลังได้

ปัจจุบันได้มีการจัดตั้งมาตรฐานสากลขึ้น โดยมีองค์กรหน่วยงานมาตรวิทยามากกว่า 50 ประเทศเข้าร่วมในการตรวจวัดเวลาโลก โดยใช้เครื่องวัดที่เรียกว่า “นาฬิกาซีเซียม (Cesium Clock)” ซึ่งถือได้ว่ามีความเที่ยงตรงแม่นยำมาก โดยสถาบันมาตรวิทยาแห่งชาติของประเทศไทยก็เป็นหนึ่งในหน่วยงานที่ติดตั้งนาฬิกาซีเซียมและเข้าร่วมวัดเวลาและความถี่ เพื่อให้บริการมาตรฐานเวลากับผู้ใช้บริการทั้งภาครัฐและเอกชน

สถาบันมาตรวิทยาของแต่ละประเทศที่มีการติดตั้งเครื่องวัดนาฬิกาซีเซียมเพื่อใช้วัดเวลาและนำข้อมูลมาคำนวณให้เกิดเวลามาตรฐานโลกขึ้น ซึ่งมีค่าเวลาที่เกี่ยวข้องด้วยกัน 4 ค่าดังนี้

1. TAI (International Atomic Time) คือ ค่าเวลาอ้างอิงระหว่างประเทศที่เกิดจากการคำนวณของสำนักงาน ชั่ง ตวง วัดระหว่างประเทศ (BIPM) โดยใช้ข้อมูลจากนาฬิกาซีเซียมที่ติดตั้งอยู่ที่สถาบันมาตรวิทยาใน 50 กว่าประเทศ ซึ่งมีเครื่องวัดมากกว่า 300 เครื่องมาคำนวณเปรียบเทียบผ่านดาวเทียม เพื่อหาค่าเฉลี่ยให้ได้ค่ามาตรฐานเวลาที่ใช้อ้างอิงทั่วโลก
   ค่าเวลา UT1 นั้นได้จากการนำค่าเวลา UT0 มาคำนวณ และแก้ไขค่าให้สอดคล้องกังการเคลื่อนไหวของการเปลี่ยนแปลงขั้วโลก ซึ่งมีผลกระทบกับสถานีสังเกตการณ์ให้มีการเปลี่ยนแปลงค่า Longtitude ซึ่งค่า UT0 นั้น ได้จากการเฝ้าสังเกตการณ์เปลี่ยนแปลงของดวงดาว หรือคลื่นวิทยุในกาแล็กซี่ และยังรวมถึงการเปลี่ยนแปลงของพระจันทร์ด้วย ทำให้ค่า UT0 มีค่าไม่คงที่แล้วแต่สถานที่สภาพแวดล้อมที่ใช้สังเกตการณ์นี้
2. UT1 (Universal Time) คือ ค่าเวลาอ้างอิงที่วัจากการโคจรของโลก ซึ่งมีความละเอียดในระดับไมโครวินาที โดยมีหน่วยงาน International Earth Rotation and Reference Systems Service (IERS) เฝ้าสังเกตการณ์และวัดค่าการเปลี่ยนแปลง โดยค่าเวลา UT1 จะมีค่าเท่ากันทั่วโลก ซึ่งอาจมีการเปลี่ยนแปลงของเวลาเพิ่มขึ้น หรือลดลงโดยส่วนต่างที่เกิดการเปลี่ยนแปลงที่เราเรียกว่า “leap seconds” และนำค่านี้ไปใช้ปรับปรุงเวลาที่เกิดจากการวัดของ Atomic Time (TAI) ให้มีความแม่นยำถูกต้องขึ้นด้วย
3. UTC (Coordinat e Universal Time) คือ ค่าเวลามาตรฐานที่เกิดจากการนำค่าเวลา TAI มาปรับปรุงให้มีความสอดคล้องกับค่า UT1 ที่เรียกว่าการ Set leap seconds โดยความแตกต่างของค่าเวลา UTC กับ UT1 จะต่างกันไม่เกิน 0.9 วินาที

4. UTC (NIMT) คือ ค่าเวลามาตรฐานของประเทศไทยที่ได้จากการวัดด้วยนาฬิกาซีเซียม และมีการเปรียบเทียบกับค่าเวลา UTC ซึ่งมีความไม่แน่นอนอยู่ประมาณ 20 นาโนวินาที

แหล่งที่ให้บริการอ้างอิงการเทียบเวลา

สำหรับหน่วยงานในประเทศไทยที่มีการให้บริการอ้างอิงการเทียบเวลาและใช้บริการกันทั่วไป มีดังต่อไปนี้

หน่วยงาน	NTP Server	IP Address	Clock Strata
1. สถาบันมาตรวิทยาแห่งชาติ	time1.nimt.or.th	203.185.69.60	Stratum1
	time2.nimt.or.th	203.185.69.59	Stratum1
	time3.nimt.or.th	203.185.69.56	Stratum1
2. กรมอุทกศาสตร์กองทัพเรือ	time.navy.mi.th	118.175.67.83	Stratum1
	time2.navy.mi.th	123.242.129.113	Stratum1
	time3.navy.mi.th	123.242.129.114	Stratum1
3. ศูนย์ประสานงานรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย	Clock.thaicert.org	203.185.129.186	Stratum2
4. ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ประเทศไทย	Clock.nectec.or.th	202.44.204.114	Stratum2

(ก่อกิจ วีระอาชากุล, 2553)

SNMP

SNMP (Simple Network Management Protocol) เป็นโปรโตคอลในแอพพลิเคชันเลเยอร์ที่ใช้สำหรับการบริหารจัดการเครือข่าย โปรโตคอลนี้เป็นส่วนหนึ่งในชุดโปรโตคอล TCP/IP ซึ่งช่วยให้ผู้ดูแลระบบสามารถจัดการประสิทธิภาพ วิเคราะห์ปัญหา และให้ข้อมูลเพื่อใช้สำหรับการวางแผนเพื่อการขยายเครือข่ายในอนาคต

โปรโตคอล SNMP ได้พัฒนามาแล้ว 2 เวอร์ชัน คือ SNMPv1 และ SNMPv2 ซึ่งทั้งสองเวอร์ชันมีหลายฟีเจอร์ที่เหมือนกัน แต่เวอร์ชัน 2 จะมีส่วนที่ขยายเพิ่ม ส่วนเวอร์ชัน 3 (SNMPv3) นั้นจะเน้นเพิ่มส่วนของการรักษาความปลอดภัยในส่วนนี้จะอธิบายหลักการทำงานของโปรโตคอล SNMP

องค์ประกอบพื้นฐานของ SNMP

ในการใช้งานโดยทั่วไปของโปรโตคอล SNMP นั้น ในเครือข่ายจะมีอุปกรณ์เครือข่ายจำนวนมากที่ต้องการจัดการและจะมีระบบหนึ่งซึ่งทำหน้าที่เป็นศูนย์กลางในการบริหารจัดการ ในแต่ละอุปกรณ์เครือข่ายที่ต้องการบริหารจัดการก็จำเป็นที่ต้องติดตั้งเอเจนต์ (Agent) ซึ่งจะทำหน้าที่รายงานข้อมูลเกี่ยวกับอุปกรณ์ตัวนั้น

ผ่านโปรโคตอล SNMP มายังเครื่องเซิร์ฟเวอร์ที่ทำหน้าที่บริหารเครือข่าย ระบบการจัดการระบบเครือข่ายที่ใช้โปรโตคอล SNMP จะประกอบด้วย 3 ส่วน คือ

1. อุปกรณ์เครือข่ายที่ต้องการบริหารจัดการ (Managed Devices)
2. เอเจนต์ (Agents)
3. ระบบบริหารจัดการเครือข่าย (Network Management Systems หรือ NMS)

อุปกรณ์เครือข่ายที่ต้องการจัดการ (Management Devices) คือ อุปกรณ์เครือข่ายที่ติดตั้งเอเจนต์ SNMP ซึ่งเอเจนต์ทำหน้าที่รวบรวมและเก็บสถิติข้อมูลของอุปกรณ์ และส่งข้อมูลนี้กับ NMS โดยใช้โปรโตคอล SNMP อุปกรณ์เครือข่ายที่ต้องการจัดการ เช่น เราท์เตอร์ แอ็กเซสเซิร์ฟเวอร์ สวิตช์ ฮับ คอมพิวเตอร์ หรือเครื่องพิมพ์ เป็นต้น

เอเจนต์เป็นซอฟต์แวร์ที่ติดตั้งอุปกรณ์เครือข่ายที่ต้องการจัดการ ซึ่งซอฟต์แวร์นี้จะจัดการข้อมูลของอุปกรณ์นั้น และแปลงให้สามารถใช้งานได้กับโปรโตคอล SNMP โดยปกติเอเจนต์จะส่งข้อมูลเกี่ยวกับอุปกรณ์นั้น ในรูปแบบของตัวแปร เช่น “free memory” “system name” “number of running process” “default route” เป็นต้น

(จตุชัย แพงจันทร์ และ อนุโชต วุฒิพรพงษ์, 2555)

DHCP

DHCP (Dynamic Host Configuration Protocal) เป็นโปรโตคอลที่รู้จักกันอย่างแพร่หลายในการนำมาใช้สำหรับแจกจ่ายหมายเลข IP Address ให้กับเครื่องที่เชื่อมต่ออยู่ในเครือข่ายเดียวกันและมีการติดตั้ง DHCP Client ไว้ แต่จรง ๆ แล้ว โปรโตคอล DHCP นอกจากจะแจก IP Address แล้ว ยังสามารถปรับแต่งให้ส่งค่าคอนฟิกที่เกี่ยวกับ Internet Protocal ด้วย เช่น Subnet masks, Default gateway, domain name, DNS server เป็นต้น

ลักษณะการให้บริการของ DHCP

DHCP เป็นบริการที่เรียกใช้ในการแจก IP Address ให้กับเครื่องไคลแอนท์ โดยสนับสนุนการให้บริการ 3 แบบด้วยกัน ดังนี้

1. **Automatic Allocation** โปรโตคอล DHCP จะแจกหมายเลข IP Address แบบถาวรโดยไม่จำกัดเวลา
2. **Dynamic Allocation** โปรโตคอล DHCP จะแจกหมายเลข IP Address แบบชั่วคราว โดยมีการกำหนดระยะเวลาในการถือครองหมายเลข IP Address ให้กับเครื่องไคลแอนท์ หรือจนกว่าเครื่องไคลแอนท์จะเลิกใช้ ซึ่งเป็นการให้บริการแบบเดียวที่สามารถนำหมายเลข IP Address กลับมาใช้ใหม่ได้ จึงเหมาะกับการให้บริการเครื่องไคลแอนท์ที่เข้ามาเชื่อมต่อเครือข่ายแบบชั่วคราว
3. **Manual Allocation** โปรโตคอล DHCP จะแจกหมายเลข IP Address ให้กับเครื่องไคลแอนท์ที่มีการกำหนดค่าไว้กับ DHCP Server โดยจะกำหนดไว้ว่าไคลแอนท์เครื่องใดจะได้หมายเลข IP Address อะไร โดยทั่วไปจะใช้หมายเลข MAC Address ของเครื่องไคลแอนท์นั้นในการระบุตัวตน

รูปแบบของ DHCP Message ที่มีการรับส่งระหว่าง DHCP Client-DHCP Server ในแต่ละแบบจะถูกเรียกใช้ในสถานการณ์ที่แตกต่างกัน ดังนี้

2. **DHCPDISCOVER** เป็น Message แรกที่เครื่องไคลเอนท์ Broadcast ส่งไปบนเน็ตเวิร์คเพื่อเสาะหาเครื่อง DHCP Server ที่เปิดให้บริการ ซึ่งไคลเอนท์จะส่ง Hardware Address ไปด้วยเพื่อให้เซิร์ฟเวอร์ตรวจสอบว่า เคยให้บริการ IP Address กับหมายเลข Hardware Address นี้หรือไม่
3. **DHCPOFFER** เป็น Message ที่เครื่อง DHCP Server ตอบกลับเครื่องไคลเอนท์ที่ส่ง DHCPDISCOVER พร้อมทั้งยื่นข้อเสนอสำหรับการให้บริการใช้หมายเลข IP Address โดยเซิร์ฟเวอร์กำหรดหมายเลข IP Address ที่จะให้ใช้บริการมายื่นเสนอ พร้อมทั้งข้อมูลที่จำเป็นอื่น ๆ และรอผลการตอบกลับจากเครื่องไคลเอนท์
4. **DHCPREQUEST** เป็น Message ที่เครื่องไคลเอนท์ส่งไปยังเครื่อง DHCP Server ใน 4 กรณีด้วยกัน
    4.1. ตอบกลับ DHCPOFFER เพื่อร้องขอพารามิเตอร์ที่ต้องการจากเครื่องเซิร์ฟเวอร์ที่จะเกิดขึ้นในกระบวนการจอง IP Address (Allocation Process)
    4.2. ในกรณีที่เครื่องไคลเอนท์เกิดการ Reboot หรือ Shutdown ไป เมื่อเครื่องไคเอนท์บู๊ตระบบตื้นมาพร้อมใช้งานแล้วจะส่ง Message นี้ไปหาเครื่อง DHCP Server ที่แจก IP Address มาให้เพื่อยืนยันขอใช้ IP Address เดิมจะเกิดขึ้นในกระบวนการจอง IP Address ซ้ำ (Reallocation Process)
    4.3. ในกรณีที่เครื่องไคลเอนท์จอง IP Address จนหมดเวลา T1 (Renewal Timer) เครื่องไคลเอนท์จะส่ง DHCPREQUEST ไปยัง Server เพื่อขอหมายเลข IP Address ใหม่จะเกิดขึ้นในกระบวนการ Renewal Process
    4.4. ในกรณีที่เครื่องไคลเอนท์ทำกระบวนการ Renewal แต่ยังไม่ได้รับการตอบกลับจากเครื่องเซิร์ฟเวอร์จนหมดเวลา T2 (Rebinding Timer) นั่นคือ ไม่ได้รับหมายเลข IP Address ใหม่ก็จะส่ง DHCPREQUEST Broadcast ไปบนเครือข่ายเพื่อหาเครื่อง Server อื่นตอบกลับแทน
5. **DHCPACK** เป็น Message ที่เครื่อง DHCP Server ตอบกลับเครื่องไคลเอนท์หลังจากได้รับ DHCPREQUEST เพื่อตอบสนองการร้องขอ พร้อมทั้งส่งค่าพารามิเตอร์ที่จำเป็นให้ เช่น IP Address เวลาในการใช้บริการ IP เป็นต้น
6. **DHCPNAK** เป็น Message ที่เครื่อง DHCP Server ตอบกลับเครื่องไคลเอนท์หลังจากได้รับ DHCPREQUEST ในการปฏิเสธการร้องขอนั้น ๆ ซึ่งอาจเกิดขึ้นจากข้อมูลที่ส่งมาไม่ถูกต้องได้ เป็นต้น
7. **DHCPDECLINE** เป็น Message ที่เครื่องไคลเอนท์ส่งกลับไปให้เครื่อง DHCP Server รับรู้ว่า IP Address ที่ได้รับมามีการนำไปใช้งานแล้ว
8. **DHCPRELEASE** เป็น Message ที่เครื่องไคลเอนท์ส่งกลับไปที่เครื่อง DHCP Server เพื่อบอกว่าต้องการยกเลิกการใช้ IP Address ที่ขอมาแล้ว

(ก่อกิจ วีระอาชากุล, 2553)

บรรณานุกรม

"Extreme Networks C5 CLI Reference FW 6.81". (26 November 2015). เข้าถึงได้จาก https://extranet.extremenetworks.com/downloads/Pages/C5.aspx

"OmniSwitch AOS Release 6250/6350/6450 CLI Reference Guide". (26 November 2015). เข้าถึงได้จาก http://enterprise.alcatel-lucent.com/assets/documents/os_cli_671.pdf

"OmniSwitch CLI Reference Guide". (26 November 2015). เข้าถึงได้จาก http://enterprise.alcatel-lucent.com/assets/documents/os_cli_revD.pdf

"พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550". (26 พฤศจิกายน 2558). เข้าถึงได้จาก http://www.mict.go.th/assets/portals/1/files/download/001_28_10.pdf

ก่อกิจ วีระอาชากุล. (2553). *Guide&Practice Network Administration.* นนทบุรี: ไอดีซี พีเมียร์.

จตุชัย แพงจันทร์, และ อนุโชต วุฒิพรพงษ์. (2555). *เจาะระบบ Network 3rd Edition.* นนทบุรี: ไอดีซี พรีเมียร์.