ระบบเครือข่ายไร้สายและการยืนยันตนสำหรับภาควิชาวิศวกรรมคอมพิวเตอร์

WIRELESS NETWORKING AND AUTHENTICATION FOR DEPARTMENT OF COMPUTER ENGINEERING

ดนุภัทร สงวนศิลป์
สุจิตรา เลิศศศิภากร

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต
ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ปีการศึกษา 2557

ระบบเครือข่ายไร้สายและการยืนยันตนสำหรับภาควิชาวิศวกรรมคอมพิวเตอร์

WIRELESS NETWORKING AND AUTHENTICATION FOR DEPARTMENT OF COMPUTER ENGINEERING

ดนุภัทร สงวนศิลป์
สุจิตรา เลิศศศิภากร

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต
ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ปีการศึกษา 2557

ปริญญานิพนธ์ปีการศึกษา 2557

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง ระบบเครือข่ายไร้สายและการยืนยันตนสำหรับภาควิชาวิศวกรรมคอมพิวเตอร์

WIRELESS NETWORKING AND AUTHENTICATION FOR DEPARTMENT OF COMPUTER ENGINEERING

ผู้จัดทำ

1. นายดนุภัทร สงวนศิลป์ รหัสนักศึกษา 54010468

2. นางสาวสุจิตรา เลิศศศิภากร รหัสนักศึกษา 54011388

..... อาจารย์ที่ปรึกษา

(อาจารย์จิระศักดิ์ สิทธิกร)

ระบบเครือข่ายไร้สายและการยืนยันตนสำหรับภาควิชาวิศวกรรมคอมพิวเตอร์

นาย ดนุภัทร สงวนศิลป์ 54010468
นางสาว สุจิตรา เลิศศศิภากร 54011388
อาจารย์ จิระศักดิ์ สิทธิกร อาจารย์ที่ปรึกษา
ปีการศึกษา 2557

บทคัดย่อ

การใช้งานอินเตอร์เน็ตผ่านระบบเครือข่ายไร้สายภายในภาควิชาวิศวกรรมคอมพิวเตอร์ในปัจจุบันมีการใช้งานที่เพิ่มมากขึ้น ทว่าระบบเครือข่ายไร้สายที่มีอยู่ยังไม่ครอบคลุมในการใช้งาน เนื่องด้วยปัญหาที่เกิดขึ้นจึงเกิดการพัฒนาระบบเครือข่ายไร้สายและการยืนยันตัวตนสำหรับภาควิชาวิศวกรรมคอมพิวเตอร์ขึ้น

ระบบเครือข่ายไร้สายและการยืนยันตัวตนสำหรับภาควิชาวิศวกรรมคอมพิวเตอร์มีการออกแบบเครือข่ายไร้สายให้ครอบคลุมบริเวณการใช้งาน ในส่วนของการยืนยันตัวตนในการเข้าใช้งานเครือข่ายไร้สายจะทำงานโดยใช้ RADIUS ที่มีการ Authentication แบบ 802.1X มี ระบบฐานข้อมูลสำหรับการเก็บข้อมูลต่างๆ ของผู้ใช้งาน ซึ่งภายในระบบจะมีการแบ่งผู้ใช้งานออกเป็น 4 กลุ่ม ได้แก่ ผู้ดูแลระบบ (Admin), อาจารย์ (Lecturer), นักศึกษา (Student) และ บุคคลภายนอก (Guest) นอกจากนี้จะมีส่วนของเว็บไซต์สำหรับให้ผู้ใช้งานสามารถตรวจสอบปริมาณข้อมูลที่ใช้งาน ปริมาณข้อมูลที่ได้ใช้งานไปแล้วในแต่ละวัน และมีหน้าเว็บไซต์สำหรับ Lecturer ในการเพิ่ม Guest ให้สามารถใช้งานระบบเครือข่ายไร้สายได้ ซึ่ง Lecturer จะสามารถกำหนดระยะเวลา และปริมาณที่สามารถใช้งานระบบเครือข่ายไร้สายของ Guest ได้ รวมทั้งมีการเก็บปริมาณข้อมูลการใช้งานของผู้ใช้แต่ละคน เพื่อการรองรับการขยายระบบเครือข่ายในอนาคตได้อีกด้วย

WIRELESS NETWORKING AND AUTHENTICATION FOR DEPARTMENT OF COMPUTER ENGINEERING

Mr. Danupat Sanguansilp 54010468
Ms. Sujitra Lertsasipakorn 54011388
Mr. Jirasak Sittigorn Advisor
Academic Year 2014

ABSTRACT

Internet usage over wireless in Department of Computer Engineering has tend to be increase every day. But the traditional Wireless Networking does not provide a sufficiently usage to the user. Wireless Networking and Authentication for Department of Computer Engineering is designed to solve this problem by design the Wireless Networking which covering the usable area. In the user authentication system use RADIUS protocol via the 802.1X standard which can support the user authentication based on the Relational Database. User in the system have their group such as Admin, Lecturer, Student and Guest. User can be able to check the internet usage data via the website. Lecturer can add the temporary guest user and manage the Guest's internet usage time via the website. All internet usage data of all user will be stored in order to support the system scalability in the future.

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้สำเร็จลุล่วงได้ดี อันเนื่องมาจากได้รับการแนะนำ ข้อเสนอแนะ พร้อมทั้งการตรวจดูความคืบหน้าอย่างสม่ำเสมอ จากอาจารย์ที่ปรึกษาโครงงาน อาจารย์ จิระศักดิ์ สิทธิกร ข้าพเข้ารู้สึกทราบซึ้งในความกรุณาของอาจารย์ และขอขอบพระคุณอาจารย์เป็นอย่างสูง

ขอบพระคุณอาจารย์ทุกท่านในภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ที่ได้ประสิทธิ์ประสาทวิชาความรู้ทางด้านคอมพิวเตอร์ให้กับข้าพเจ้า

ขอบพระคุณอาจารย์ อัครเดช วัชรภูพงษ์ ที่คอยให้คำปรึกษาและคอยช่วยเหลือในเรื่องระบบเครือข่ายของภาควิชาวิศวกรรมคอมพิวเตอร์

ขอบคุณห้อง Network Laboratory ที่เป็นแหล่งสนับสนุนสถานที่และอุปกรณ์ในการพัฒนาโครงงานได้อย่างสะดวก

ขอบคุณนาย นพกร ใช้บุญเรือง และ นาย พัสกร จุลพล ที่ช่วยให้คำแนะนำในการพัฒนาเว็บไซต์จนประสบความสำเร็จ

สุดท้ายนี้ข้าพเจ้าขอกราบขอบพระคุณ บิดา มารดา และครอบครัว ผู้ซึ่งเป็นทั้งกำลังใจ แรงบันดาลใจ ความฝัน ตลอดจนการให้การสนับสนุนในทุกๆเรื่อง

ด้วยคุณค่าและประโยชน์อันพึงมาจากโครงงานนี้ เราขอมอบแด่ผู้มีพระคุณทุกท่าน

ดนุภัทร สงวนศิลป์
สุจิตรา เลิศศศิภากร

สารบัญ

หน้า

สารบัญ(ต่อ)

หน้า

สารบัญตาราง

สารบัญรูป

รูป หน้า

สารบัญรูป(ต่อ)

รูป หน้า

สารบัญรูป(ต่อ)

รูป หน้า

บทที่ 1
บทนำ

1.1 ความสำคัญและที่มาของโครงงาน

ในปัจจุบันการใช้งานอินเตอร์เน็ตผ่านระบบเครือข่ายไร้สายมีการใช้งานเพิ่มขึ้นเป็นจำนวนมาก เนื่องมาจากการเจริญเติบโตของอุปกรณ์พกพา ซึ่งสอดคล้องกับการใช้งานอินเตอร์เน็ตผ่านระบบเครือข่ายไร้สายภายในภาควิชาวิศวกรรมคอมพิวเตอร์ ถึงแม้ว่าทางสถาบันจะมีเครือข่ายไร้สายของทางสถาบันให้ใช้งานอยู่แล้ว แต่ก็ยังประสบปัญหาไม่เพียงพอต่อการใช้งาน และยังไม่ครอบคลุมพื้นที่ทั่วทั้งภาควิชา ซึ่งส่งผลให้ในบางห้องเรียนของภาควิชาไม่สามารถใช้งานอินเตอร์เน็ตได้หรือใช้งานได้ไม่สะดวก เนื่องจากเกิดความคับคั่งในการเชื่อมต่อจากอุปกรณ์ของผู้ใช้งานไปยัง Access Point แต่ละจุด รวมทั้งหากมีการเคลื่อนย้ายตำแหน่งของอุปกรณ์ที่มีการเชื่อมต่อเครือข่ายไร้สายนั้นอาจทำให้เกิดการขาดหายของสัญญาณ ซึ่งทำให้ไม่สามารถใช้งานเครือข่ายได้หรือใช้งานได้ไม่สะดวกเท่าที่ควร นอกจากนี้หากบุคลคลภายนอกที่เข้ามาติดต่อภายในภาควิชาและมีความจำเป็นในการต้องใช้งานอินเตอร์เน็ตจะไม่สามารถใช้งานได้ เนื่องจากไม่มีบัญชีในการเข้าสู่ระบบของสถาบัน ส่งผลให้มีการยืมบัญชีในการยืนยันตัวตนของบุคลากรภายในสถาบัน ซึ่งหากมีการกระทำความผิดเกี่ยวกับคอมพิวเตอร์จะส่งผลให้ไม่สามารถตรวจสอบและระบุตัวตนของผู้ใช้งานที่แท้จริงได้

จากปัญหาที่กล่าวมาข้างต้น จึงเป็นที่มาของการทำโครงงานระบบเครือข่ายไร้สายและการยืนยันตนสำหรับภาควิชาวิศวกรรมคอมพิวเตอร์ เพื่อช่วยให้การใช้งานอินเตอร์เน็ตผ่านเครือข่ายไร้สายเป็นไปได้ดียิ่งขึ้น รวมทั้งอำนวยความสะดวกให้กับบุคคลภายนอกที่จำเป็นต้องเข้ามาใช้งานและยังสามารถควบคุมและบริหารจัดการการใช้งานของผู้ใช้งานภายในภาควิชาได้ โดยได้มีการแบ่งกลุ่มของผู้ใช้งาน เพื่อกำหนดสิทธิการใช้งานของผู้ใช้ในแต่ละระดับ ทั้งนี้ในระบบมีกระบวนการจัดการเมื่อมีการเคลื่อนย้ายอุปกรณ์ที่ใช้งานทำการเชื่อมต่อเข้ากับ Access Point ตัวใหม่โดยไม่ต้องทำการยืนยันตัวตนใหม่ เพื่อให้ผู้ใช้สามารถใช้งานอินเตอร์เน็ตได้อย่างต่อเนื่อง

1.2 วัตถุประสงค์ของโครงงาน

1) เพื่อให้การใช้งานอินเตอร์เน็ตไร้สายภายในภาควิชามีความสะดวกและครอบคลุมมากขึ้น
2) เพื่อให้ควบคุมปริมาณการใช้งานอินเตอร์เน็ตในภาควิชาวิศวกรรมคอมพิวเตอร์ได้
3) เพื่อให้บุคคลภายนอกสามารถยืนยันตัวตนเพื่อใช้งานอินเตอร์เน็ตของทางภาควิชา โดยผ่านการรับรองจากบุคลากรภายในของภาควิชาวิศวกรรมคอมพิวเตอร์ได้

4) เพื่อป้องกันไม่ให้บุคคลที่ไม่ได้รับอนุญาตสามารถใช้งานระบบเครือข่ายคอมพิวเตอร์ภายในได้
5) เพื่อรองรับการใช้งาน Private IP Address ในห้องปฏิบัติการคอมพิวเตอร์ของภาควิชา

1.3 ขอบเขตของโครงงาน

โครงงานระบบเครือข่ายไร้สายและการยืนยันตน สำหรับภาควิชาวิศวกรรมคอมพิวเตอร์ ดำเนินการศึกษาและทดลองภายใต้ขอบเขตดังนี้

1) ติดตั้ง AAA Server สำหรับการยืนยันตัวตนและบริหารจัดการผู้ใช้งาน โดยเชื่อมต่อผ่านเครือข่ายไร้สายของภาควิชาวิศวกรรมคอมพิวเตอร์ให้ใช้งานอินเตอร์เน็ตได้
2) สามารถทำการเชื่อมต่อเข้ากับ Access Point ตัวใหม่ที่อยู่ใกล้บริเวณที่เคลื่อนย้ายไปโดยไม่ต้องทำการยืนยันตัวตนใหม่
3) สามารถสร้างบัญชีผู้ใช้ชั่วคราวให้บุคคลภายนอกที่จำเป็นต้องใช้งานเครือข่ายไร้สายสามารถใช้งานอินเตอร์เน็ตได้
4) สามารถเก็บประวัติการใช้งานของผู้ใช้ในระบบได้
5) ผู้ใช้งานสามารถตรวจสอบปริมาณการใช้งานผ่านเว็บไซต์ได้

1.4 วิธีดำเนินการ

1) ศึกษาข้อมูลเกี่ยวกับ AAA Protocol ชนิดต่างๆ ข้อดี และข้อเสียของแต่ละ Protocol ที่จะนำไปใช้ในการทำระบบยืนยันตัวตน
2) ศึกษาระบบปฏิบัติการที่จะนำมาใช้เพื่อนำมาใช้ติดตั้ง AAA Protocol ทั้ง Linux และ Windows
3) ศึกษาความรู้เกี่ยวกับ 802.1X และ EAP ประเภทต่างๆ
4) ศึกษาข้อมูลเกี่ยวกับการออกแบบระบบเครือข่ายไร้สาย
5) ศึกษาอุปกรณ์และโครงสร้างเครือข่ายของระบบเครือข่ายเดิมของภาควิชาที่มีอยู่แล้ว
6) ออกแบบระบบในการดึงข้อมูลของผู้ใช้งานจากทางภาควิชาและระบบยืนยันการลงทะเบียนสำหรับการใช้งานครั้งแรก
7) ออกแบบระบบเครือข่ายไร้สายให้รองรับการใช้งานภายในภาควิชา
8) ทำการทดสอบการตั้งค่าระบบในส่วนต่างๆ ก่อนนำมาทำงานร่วมกัน
9) ทำการทดสอบระบบโดยรวมทั้งหมด
10) วิเคราะห์ผลการทำงาน สรุปผลการทำงานที่ได้ ข้อผิดพลาดที่เกิดขึ้นและข้อจำกัดของระบบ รวมถึงวิธีการแก้ไขข้อผิดพลาด

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1) นำระบบเครือข่ายไร้สายและระบบการยืนยันตัวตนมาใช้งานกับภาควิชาวิศวกรรมคอมพิวเตอร์ได้อย่างมีประสิทธิภาพ
2) แก้ปัญหาการใช้งานอินเตอร์เน็ตไร้สายภายในภาควิชา
3) อำนวยความสะดวกแก่บุคคลภายนอกที่เข้ามาใช้บริการเครือข่ายไร้สายของภาควิชาวิศวกรรมคอมพิวเตอร์
4) แก้ปัญหา IP Address ของห้องปฏิบัติการคอมพิวเตอร์มีไม่เพียงพอต่อการใช้งาน
5) สามารถนำโครงงานไปพัฒนาต่อยอดได้ในอนาคต

1.6 ส่วนประกอบของปริญญานิพนธ์

1) ปริญญานิพนธ์ฉบับนี้แบ่งเนื้อหาได้ออกเป็น 5 บท โดยมีรายละเอียดดังต่อไปนี้
2) บทที่ 1 บทนำ กล่าวถึง ความสำคัญและที่มาของโครงงาน วัตถุประสงค์ของโครงงาน ขอบเขตของโครงงาน วิธีดำเนินการ ประโยชน์ที่คาดว่าจะได้รับ และ ส่วนประกอบของปริญญานิพนธ์
3) บทที่ 2 ทฤษฎีที่เกี่ยวข้อง กล่าวถึง ทฤษฎี Wireless LAN แนวคิดเกี่ยวกับ AAA ทฤษฎี RADIUS protocol ทฤษฎี 802.1X ทฤษฎี Web Service ทฤษฎี ภาษา PHP และ ทฤษฎี MVC
4) บทที่ 3 การออกแบบและการพัฒนา กล่าวถึง ภาพรวมของระบบ การออกแบบส่วนการยืนยันตัวตน การออกแบบส่วนของฐานข้อมูล และการออกแบบส่วนของเว็บไซต์
5) บทที่ 4 การทดลองและผลการทดลอง กล่าวถึง การทดลองหาค่า RSSI ที่เหมาะสม การทดลองใช้งานร่วมกับเครือข่ายของภาควิชา การทดลองเข้าใช้งานในฐานะ Guest การทดลองเข้าใช้งานในฐานะ Student การทดลองเข้าใช้งานในฐานะ Lecturer และ การทดลองเข้าใช้งานในฐานะ Admin
6) บทที่ 5 บทสรุป กล่าวถึง บทสรุปของโครงงาน ปัญหาและอุปสรรคต่างๆของโครงงาน แนวทางการแก้ไขและแนวทางการพัฒนาต่อไป

บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

2.1 Wireless LAN

เป็นเทคโนโลยีที่ใช้เชื่อมโยงอุปกรณ์ไร้สายตั้งแต่ 2 ตัวขึ้นไปเข้าด้วยกันเป็นระบบเครือข่าย โดยใช้คลื่นวิทยุสำหรับการกระจายสัญญาณเพื่อติดต่อสื่อสารกัน ไม่ต้องทำการเดินสายสัญญาณระหว่างอุปกรณ์ในระบบเครือข่าย การเชื่อมต่อ Wireless LAN จะมีการเชื่อมต่อ 2 รูปแบบ ได้แก่

1) การเชื่อมต่อระหว่างคอมพิวเตอร์ด้วยกันเอง
2) การเชื่อมต่อระหว่างคอมพิวเตอร์ผ่านอุปกรณ์กระจายสัญญาณ (Access Point)

2.1.1 IEEE 802.11

รูป 2.1 มาตรฐาน IEEE 802.11

มาตรฐาน IEEE 802.11 เป็นการทำงานของระบบเครือข่ายไร้สายที่นำมาใช้ในมาตรฐานสำหรับการรับ-ส่งข้อมูล โดยอาศัยคลื่นความถี่ ซึ่งมาตรฐาน IEEE 802.11 นั้นจะมีมาตรฐานย่อยที่สำคัญ ดังนี้

1) IEEE 802.11a เป็นมาตรฐานซึ่งใช้เทคโนโลยี Orthogonal Frequency Division Multiplexing (OFDM) ที่มีความเร็วในการรับ-ส่งข้อมูลสูงสุด 54 Mbps ใช้คลื่นวิทยุที่มีความถี่ 5 GHz รัศมีในการรับ-ส่งข้อมูลประมาณ 35 เมตรภายในอาคาร และ 120 เมตรในที่โล่งแจ้ง ซึ่งคลื่นความถี่นี้ในประเทศไทยสงวนไว้สำหรับกิจการทางด้านดาวเทียม ไม่อนุญาตให้บุคคลทั่วไปใช้งาน
2) IEEE 802.11b เป็นมาตรฐานที่ถูกตีพิมพ์และเผยแพร่ออกมาพร้อมกับมาตรฐาน IEEE 802.11a ซึ่งใช้เทคโนโลยี Complimentary Code Keying (CCK) ร่วมกับเทคโนโลยี Direct Sequence Spread Spectrum (DSSS) มีความเร็วในการรับ-ส่งข้อมูลสูงสุด 11 Mbps ใช้คลื่นวิทยุที่มีความถี่ 2.4 GHz เป็นย่านความถี่ที่อนุญาตให้

ใช้ทั่วไป โดยมีรัศมีในการรับ-ส่งข้อมูลประมาณ 35 เมตรภายในอาคาร และ 140 เมตรในที่โล่ง สามารถรับ-ส่งข้อมูลได้ไกลกว่ามาตรฐาน IEEE 802.11a

3) IEEE 802.11g เป็นมาตรฐานที่เข้ามาเพื่อทดแทนมาตรฐาน IEEE 802.11b โดยมีการใช้เทคโนโลยี DSSS และ OFDM มีความเร็วในการรับ-ส่งข้อมูลสูงสุด 54 Mbps ซึ่งมีความเร็วในการรับ-ส่งที่สูงกว่ามาตรฐาน IEEE 802.11b ใช้คลื่นวิทยุที่มีความถี่ 2.4 GHz มีรัศมีในการรับ-ส่งข้อมูลประมาณ 38 เมตรภายในอาคาร และ 140 เมตรในที่โล่ง ซึ่งกว้างกว่าแบบมาตรฐาน IEEE 802.11a
4) IEEE 802.11n เป็นมาตรฐานที่พัฒนามาจากมาตรฐาน IEEE 802.11a/b/g โดยมีการใช้เทคนิคในการส่งข้อมูลแบบ Multiple-Input Multiple-Output (MIMO) ซึ่งมีความเร็วในการรับ-ส่งข้อมูล 150-600 Mbps ใช้คลื่นวิทยุที่มีความถี่ 2.4 และ 5 GHz (Dual Band) มีรัศมีในการรับ-ส่งข้อมูลประมาณ 70 เมตรภายในอาคาร และ 250 เมตรในที่โล่ง และสามารถทำงานร่วมกันอุปกรณ์มาตรฐาน IEEE 802.11b และ IEEE 802.11g ได้
5) IEEE 802.11ac เป็นมาตรฐานที่ออกมาเพื่อแทนที่มาตรฐาน IEEE 802.11n ที่มีการใช้งานอยู่ในปัจจุบัน โดยมีการใช้เทคนิคในการส่งข้อมูลแบบ Muti-User MIMO (MU-MIMO) ซึ่งมีความเร็วในการรับ-ส่งข้อมูลได้สูงสุด 867 Mbps สำหรับ 2 เสาสัญญาณ ที่ Bandwidth 80MHz และ มีความเร็วในการรับ-ส่งข้อมูลได้สูงสุด 1.69 Gbps สำหรับ 2 เสาสัญญาณ ที่ Bandwidth 160 MHz ใช้คลื่นวิทยุที่มีความถี่ 2.4 และ 5 GHz (Dual-Band Dual-Channel)

ตาราง 2.1 เปรียบเทียบมาตรฐาน IEEE 802.11 แต่ละประเภท

มาตรฐาน	คลื่นความถี่ (GHz)	ความกว้างช่องสัญญาณ	ความเร็วสูงสุดที่ทำได้	ความกว้างสัญญาณ(ในอาคาร)	ความกว้างสัญญา(นอกอาคาร)	รองรับ MIMO
802.11a	5	20 MHz	54 Mbps	35	120	✘
802.11b	2.4	20 MHz	11 Mbps	35	140	✘
802.11g	2.4	20 MHz	54 Mbps	38	140	✘
802.11n	2.4/5	40 MHz	600 Mbps	70	140	✓(4)
802.11ac	2.4/5	80/160 MHz	6.93 Gbps	-	-	✓(8)

2.1.2 IEEE 802.1X

IEEE 802.1X เป็นมาตรฐานที่ใช้กับระบบรักษาความปลอดภัยของเครือข่าย ก่อนการเข้าใช้งานระบบเครือข่ายจะต้องทำการตรวจสอบสิทธิ์ในการเข้าถึงการใช้งาน เพื่อให้สามารถระบุตัวตนของผู้ใช้งานได้ ซึ่งจะมีการใช้ Protocol เช่น LEAP PEAP EAP-TLS หรือ EAP-FAST ซึ่งรองรับการตรวจสอบสิทธิ์การเข้าใช้งานผ่าน RADIUS Server ได้

2.1.2.1 Protected Extensible Authentication Protocol (PEAP)

PEAP เป็นเวอร์ชันหนึ่งของ Extensible Authentication Protocol (EAP) ที่ใช้ในเครือข่ายระบบไร้สาย PEAP ได้ถูกออกแบบมาเพื่อให้มีความปลอดภัยในการยืนยันตัวตนสำหรับ 802.11 WLANs ซึ่งมีการออกแบบคล้ายกับ EAP-TTLS คือจะต้องมี RADIUS Server ที่มี PKI Certificate โดย PEAP จะมี 2 แบบที่ได้รับการรับรองจากมาตรฐาน WPA และ WPA2 คือ

1) PEAPv0/EAP-MSCHAPv2
2) PEAPv1/EAP-GTC

PEAPv0/EAP-MSCHAPv2 เป็นโพรโทคอลที่ใช้งานอย่างแพร่หลาย ใช้การตรวจสอบการยืนยันตัวตนกับฐานข้อมูลที่สนับสนุนรูปแบบ MS-CHAPv2 เช่น Microsoft NT และ Microsoft Active Directory เป็นต้น

2.1.2.2 Authentication Protocol

1) Password Authentication Protocol (PAP) เป็นกลไกการตรวจสอบผู้ที่ต้องการใช้งานเครือข่ายผ่าน PPP Protocol โดยมีการตรวจสอบ Username และ Password การใช้งานผ่านเครือข่าย PPP Protocol มีข้อเสียที่ไม่ปลอดภัย คือ ไม่มีการเข้ารหัส Username และ Password ที่ถูกส่งไปตรวจสอบที่ Server
2) Challenge-Handshake Authentication Protocol (CHAP) เป็นกลไกการตรวจสอบผู้ที่ต้องการใช้งานเครือข่ายผ่าน PPP Protocol ลักษณะคล้ายกับ PAP แต่จะมีขั้นตอนที่ซับซ้อนกว่า โดยมีการส่งคำถามไปยังอุปกรณ์ของผู้ใช้งาน (Challenge) หลังจากนั้นอุปกรณ์ของผู้ใช้งานจะต้องทำการประมวลผลหาคำตอบโดยใช้รหัสลับ (Secret Key) ที่ตรงกันระหว่าง Server และอุปกรณ์ของผู้ใช้งาน
3) Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) มีการทำงานเหมือน CHAP เกือบทั้งหมด แต่ในการเก็บ Username และ Password ลงใน Server นั้นจะมีการเข้ารหัสข้อมูลไว้ ทำให้ระบบมีความปลอดภัยที่สูงขึ้น
4) Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2) จะมีการทำ 2-Way Authentication เพื่อทำการยืนยันทั้ง 2 ฝั่งว่าเป็น

ผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานจริง และยังเพิ่มการทำงานในการเปลี่ยนรหัสผ่านของผู้ใช้ เมื่อมีการรายงานจาก RADIUS Server ว่ารหัสผ่านหมดอายุการใช้งาน

2.2.2 Wireless Encryption

เป็นอีกเทคนิคในการทำให้การใช้งานเครือข่ายไร้สายใช้มีความปลอดภัยมากยิ่งขึ้น โดยในเทคนิคต่างๆ จะใช้หลักการของการเข้ารหัส การบริหารจัดการ key และวิธีการAuthentication เพื่อช่วยป้องกันไม่ให้บุคคลที่ไม่ได้รับอนุญาตเข้ามาใช้งานเครือข่าย สำหรับเทคนิคในการ Encryption มีดังนี้

2.2.3.1 Wired Equivalent Privacy (WEP)

เป็นการเข้ารหัสสัญญาณและการตรวจสอบพิสูจน์ตัวตนของผู้ใช้งานของอุปกรณ์เครือข่ายไร้สาย WEP ใช้การเข้ารหัสสัญญาณแบบ Share และ Symmetric คือผู้ใช้งานจะใช้รหัสลับในการเข้ารหัส และถอดรหัสข้อมูลเป็นรหัสเดียวกัน โดยที่อุปกรณ์ทั้งหมดบนเครือข่ายไร้สายจะต้องทราบรหัสลับนี้ เพื่อให้สามารถติดต่อกันได้ โดยรหัสที่ใช้นั้นเป็น Key ขนาด 64 bits หรือ 128 bits แต่ WEP มีช่องโหว่และจุดอ่อนที่สามารถคำนวณหา Key ที่ใช้ได้จากการดักจับและเก็บรวบรวมสัญญาณ รวมทั้ง Key ที่ใช้งานจะไม่มีการเปลี่ยนแปลงตลอดการใช้งาน จึงเป็นเหตุให้ในปัจจุบันนั้นควรหลีกเลี่ยงการใช้ WEP

2.2.3.2 Wi-Fi Protected Access (WPA)

เป็นมาตรฐานที่มาแทนที่ WEP โดยที่ WPA มีการเข้ารหัสที่มีความปลอดภัยที่สูงกว่า เพราะใช้การเข้ารหัสและถอดรหัสแบบ Temporal Key Integrity (TKIP) ซึ่งจะมีการเปลี่ยน Key ที่ใช้เสมอ สำหรับแต่ละผู้ใช้งานและทุก Packet ที่ทำการรับ-ส่งบนเครือข่าย ทำให้ยากต่อการคาดเดา WPA จะมีโหมดการทำงาน 2 โหมด ดังนี้

1) WPA-Personal เหมาะสำหรับการใช้งานในบ้านหรือธุรกิจขนาดเล็ก โดยจะต้องทำการกำหนด Pre-Shared Key (PSK) ที่อุปกรณ์ที่ใช้สำหรับเชื่อมต่อส่วนคอมพิวเตอร์หรืออุปกรณ์ไร้สายของผู้ใช้งานจะต้องทำการกำหนดรหัสผ่านให้ตรงกันกับอุปกรณ์ที่ใช้สำหรับเชื่อมต่อ ความปลอดภัยในการใช้งานจะขึ้นอยู่กับความยากของรหัสผ่านที่ใช้ และการปกปิดชื่อเครือข่ายให้เป็นความลับ (Disable Broadcast SSID)
2) WPA-Enterprise เหมาะสำหรับการใช้งานในองค์กรหรือหน่วยงานขนาดใหญ่ โดยจะต้องทำการตรวจสอบความถูกต้องผู้ใช้งานผ่านทาง Extensible Authentication Protocol (EAP) ที่รองรับการตรวจสอบสิทธิ์ผ่าน RADIUS Server โดยใช้ Username และ Password ในการตรวจสอบ เพื่อให้มั่นใจว่าเฉพาะผู้ใช้งานที่ได้รับอนุญาตเท่านั้นที่เข้าใช้งานเครือข่ายได้

2.2.3.4 Wi-Fi Protected Access 2 (WPA2)

เป็นมาตรฐานที่พัฒนามาจาก WPA โดย WPA2 จะมีความปลอดภัยมากกว่า WPA โดย WPA2 จะใช้การเข้ารหัสและถอดรหัสได้ทั้งแบบ TKIP และ Advanced Encryption Standard Counter CBC-MAC Protocol (AES-CCMP) ซึ่งทำให้มีการเข้ารหัสที่ซับซ้อนกว่าสามารถคาดเดาได้ยากกว่า WPA2 จะมีโหมดการทำงาน 2 โหมด ดังนี้

1) WPA2-Personal เหมาะสำหรับการใช้งานในบ้านหรือธุรกิจขนาดเล็ก และมีการทำงานเช่นเดียวกับ WPA-Personal คือต้องมีการกำหนด PSK ที่ Access Point หรือ อุปกรณ์ที่ใช้เชื่อมต่อ และอุปกรณ์ของผู้ใช้งานที่จะเข้าใช้งานเครือข่ายจะต้องใช้ PSK เดียวกันเพื่อการเข้าใช้งาน WPA2-Personal และ WPA-Personal สามารถใช้งานร่วมกันได้
2) WPA2-Enterprise เหมาะสำหรับการใช้งานในองค์กรหรือหน่วยงานขนาดใหญ่ และมีการทำงานเช่นเดียวกันกับ WPA-Enterprise แต่ WPA2 จะเป็นการปรับปรุงพัฒนาจาก WPA และปรับใช้มาตรฐาน IEEE 802.11i อย่างสมบูรณ์

ตาราง 2.2 การเปรียบเทียบการทำ Wireless Encryption

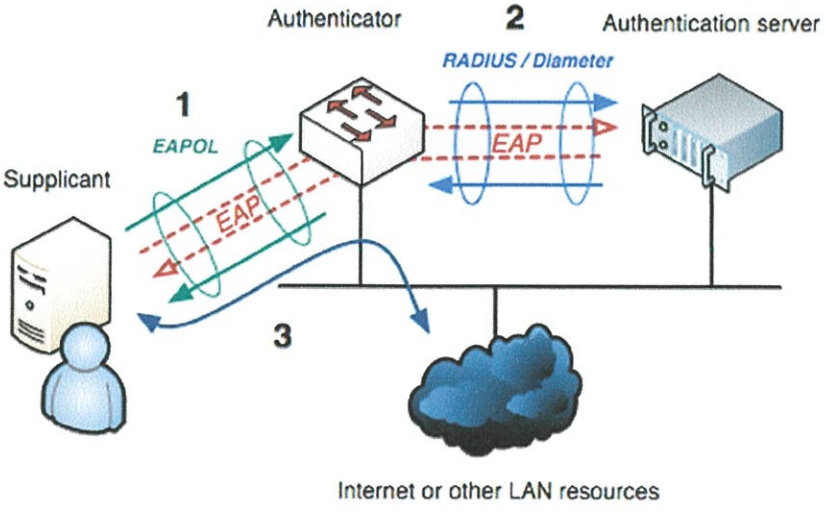
Standard	Authentication Method	Encryption Method	Cipher
802.11 Legacy	Shared Key	WEP	RC 4
WPA-Personal	WPA-PSK	TKIP	RC 4
WPA-Enterprise	802.1X/EAP	Dynamic TKIP	RC 4
WPA2-Personal	WPA2-PSK	CCMP (default) TKIP (optional)	AES (default) RC 4 (optional)
WPA2-Enterprise	802.1X/EAP	Dynamic CCMP (default) TKIP (optional)	AES (default) RC 4 (optional)

2.2 แนวคิดเกี่ยวกับ AAA

เป็นแนวคิดในการจัดการการเข้าถึงระบบเครือข่าย (Access Control) เพื่อไม่ให้ผู้ที่ไม่เกี่ยวข้องกับระบบหรือผู้ที่ไม่หวังดีเข้ามายังระบบได้ นอกจากกระบวนการจัดการการเข้าถึงระบบเครือข่ายแล้ว ยังรวมไปถึงการที่สามารถตรวจสอบสิทธิ์การใช้งานและยังมีกระบวนการเก็บข้อมูลการใช้งานด้วย ซึ่งทั้ง 3 กระบวนการนี้เรียกว่า Authentication, Authorization และ Accounting

1) Authentication เป็นกระบวนการการพิสูจน์ตัวตนในการยืนยันสิทธิ์สำหรับการเข้าใช้งานระบบเครือข่าย โดยมีวิธีในการตรวจสอบ เช่น Password, PIN Code, Biometric trails, One-time Password (OTP), Public-Key Cryptography, Digital Signature, Quiz เป็นต้น
2) Authorization เป็นกระบวนการตรวจสอบสิทธิ์ว่า ผู้ใช้นั้นจะสามารถใช้บริการของระบบได้อย่างไรบ้าง ตามนโยบายการให้บริการ (policy) ของแต่ละกลุ่ม หรือแต่ละบุคคล โดยจะอ้างอิงจากการทำ Authentication ซึ่งในการทำ Authorization จะต้องผ่าน Authentication ก่อนจึงจะสามารถตรวจสอบสิทธิ์ในการใช้งานได้
3) Accounting เป็นกระบวนการเก็บข้อมูลการใช้งานของผู้ใช้ ว่ามีการใช้งานใดๆ เป็นระยะเวลาเท่าไร เพื่อให้สามารถนำมาตรวจสอบ และเป็นแนวทางในการกำหนดนโยบายการให้บริการ (Policy)

2.2.1 องค์ประกอบการทำงานของ AAA



รูป 2.2 องค์ประกอบของ AAA

1) Supplicant คือ ผู้ใช้งานหรือคอมพิวเตอร์ที่ทำการร้องขอการเชื่อมต่อระบบ

2) Authenticator คือ อุปกรณ์ที่ทำหน้าที่ Authenticate โดยทำการคุยกับ Authentication Server ว่าจะทำอย่างไรกับ Supplicant ที่ทำการเชื่อมต่อเข้ามาในระบบ

3) Authentication Server คือ อุปกรณ์ที่ทำหน้าที่ในการตรวจสอบสิทธิ์การขอใช้งานของ Supplicant ที่ถูกส่งมาจาก Authenticator

2.3 RADIUS protocol

RADIUS ย่อมาจาก Remote Access Dial in User Service เป็น Protocol แบบ Client-Server เพื่อรวบรวมบัญชี (Account) ของผู้ใช้งาน (User) ให้อยู่ภายในที่เดียวกันเพื่อให้ง่ายต่อการบริหารจัดการ โดยจะมีขั้นตอนในการทำงานคือ เมื่อมี User ต้องการเข้าใช้งานจะมีการส่งข้อมูลมาตรวจสอบที่ RADIUS Server จากนั้น RADIUS Server จะทำการตรวจสอบ อนุมัติและการจัดการบัญชีของผู้ใช้งานที่เชื่อมต่อเข้ากับเครือข่าย โดยใช้หลักการของ AAA ในการจัดการการเข้าถึงเครือข่ายผ่าน UDP port 1812 สำหรับการ Authentication และ UDP port 1813 สำหรับการ Accounting ในการทำงาน RADIUS Server สามารถทำงานได้ทั้งบนระบบปฏิบัติการ Linux หรือ Microsoft Windows Server

2.3.1 องค์ประกอบของ RADIUS

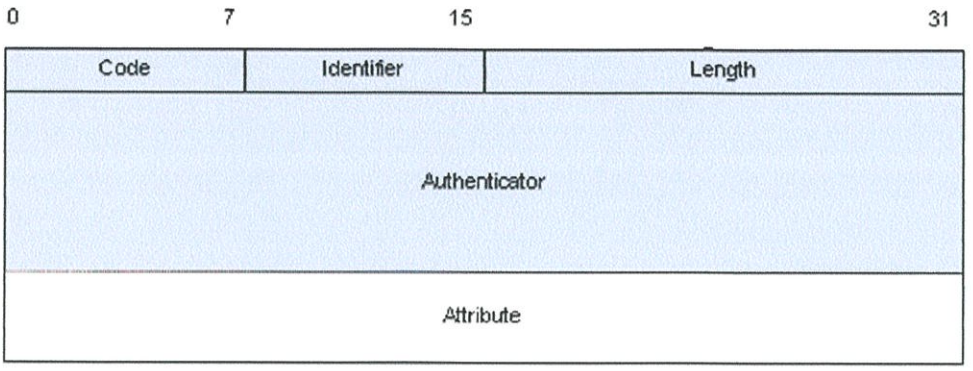
1) RADIUS Server เป็นอุปกรณ์ที่ทำหน้าที่ประมวลผลคำร้องขอจาก NAS หรือ RADIUS Client ซึ่งจะมีการเก็บข้อมูลสถิติการใช้งานต่าง ๆ ไว้ในฐานข้อมูล รวมถึงการอนุญาตสิทธิ์และคุณสมบัติการเข้าใช้งานของผู้ใช้งานแต่ละคน

2) RADIUS Client หรือ NAS (Network Access Server) เป็นอุปกรณ์ที่ทำหน้าที่เป็นตัวกลางในการเชื่อมต่อระหว่าง Access Clients และ RADIUS เพื่อส่งผ่านข้อมูลที่ใช้ในการตรวจสอบสิทธิ์ในการเข้าใช้งาน เมื่อมีการร้องขอการใช้งานระบบเครือข่าย Access Clients จะต้องส่งคำร้อง อย่างเช่น Username และ Password มายัง NAS หลังจากนั้น NAS จะส่งคำร้องขอที่จำเป็นเพิ่มลงไป เช่น NAS-IP-Address และ NAS-Port เพื่อให้ RADIUS Server ใช้ในการตรวจสอบสิทธิ์ในการเข้าใช้งาน

3) Access Client ทำหน้าที่เป็น Supplicant ของระบบซึ่งจะเป็นอุปกรณ์ทางฝั่งของผู้ใช้งานที่ต้องการยืนยันตัวตนเข้าใช้งานระบบเครือข่าย

2.3.1.1 โครงสร้างของ RADIUS Packet

RADIUS Packet ใช้สำหรับการสื่อกสารระหว่างกระบวนการยืนยันตัวจน มีส่วนประกอบต่างๆ ดังแสดงในรูปที่ 2.3



รูป 2.3 โครงสร้างของ RADIUS Packet

RADIUS Packet จะประกอบด้วย 5 ส่วน ดังนี้

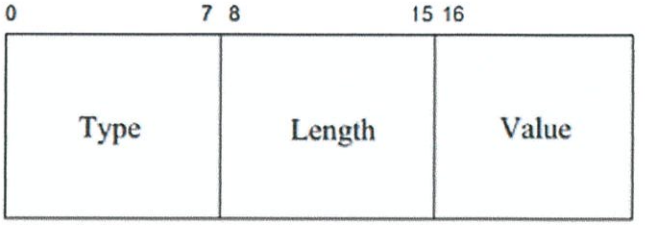
1) Code มีขนาด 1 Byte ประกอบด้วย 6 Codes ใช้แสดงรูปแบบของ RADIUS Packet มีรายละเอียดดังตาราง 2.3
2) Identifier มีขนาด 1 Byte เป็นส่วนที่ใช้สำหรับระบุการแลกเปลี่ยน RADIUS Packet ช่วยให้ Request Packet และ Respond Packet ตรงกัน ซึ่งส่งผลให้ RADIUS Client ได้รับคำตอบจาก RADIUS Server ตรงกับคำขอ ทั้งยังใช้ในการตรวจจับ Duplicate Request ได้
3) Length มีขนาด 2 Byte เป็นส่วนที่ระบุความยาวของ RADIUS Message, Code, Identifier, Length, Authenticator และ Attribute โดยค่า Length จะมีค่าต่ำสุดที่ 20 Byte และสูงสุดที่ 4096 Byte
4) Authenticator มีขนาด 16 Byte เป็นส่วนที่เก็บข้อมูลที่ใช้สำหรับการ Authenticate โดยส่วนนี้จะถูกใช้เป็นทั้ง RADIUS Client และ RADIUS Server
5) Attribute จะเป็นส่วนที่ประกอบด้วยข้อมูลต่างๆที่ใช้ในการ Authentication, Authorization, Accounting และการกำหนดค่าเบื้องต้นเพื่อให้ RADIUS Server และ RADIUS Client สามารถติดต่อกันได้เช่น บัญชีผู้ใช้, รหัสผ่าน, หมายเลข IP Address หรือ หมายเลข DNS เป็นต้น

ตาราง 2.3 Code ของ RADIUS Packet

Code	Message
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge

2.3.1.2 โครงสร้างของ RADIUS Attribute

RADIUS Attribute ใช้เพื่อระบุข้อมูลจำเพาะที่ใช้ในกระบวนการยืนยันตัวตน โดยมีโครงสร้างดังแสดงในรูปที่ 2.4



รูป 2.4 โครงสร้างของ RADIUS Attribute

โครงสร้างของ RADIUS Attribute ประกอบด้วย

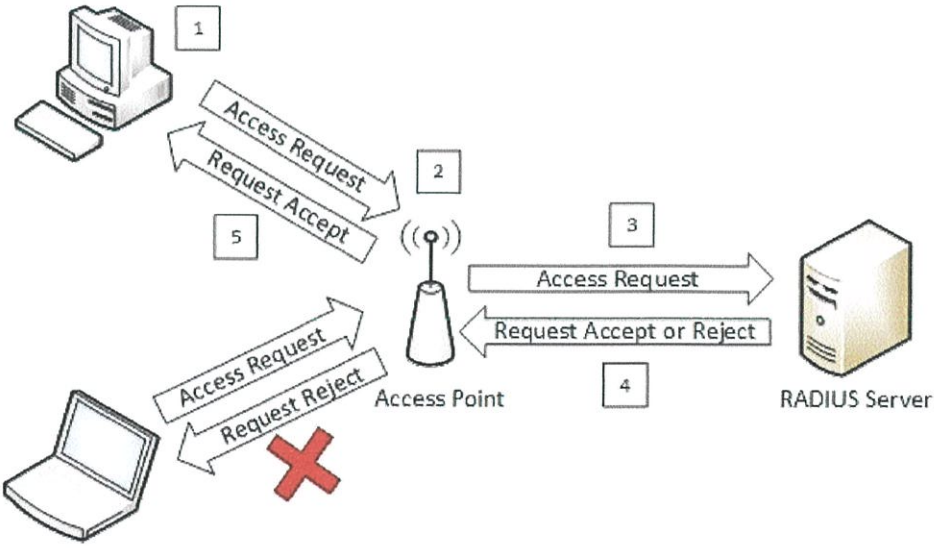
1) Type มีขนาด 1 Byte ใช้สำหรับระบุประเภทของ Attribute
2) Length มีขนาด 1 Byte ใช้สำหรับระบุความยาวของ Attribute
3) Value มีขนาดตั้งแต่ 0 Byte ขึ้นไป โดยความยาวจะขึ้นอยู่กับชนิดของ Attribute

ตาราง 2.4 Attribute ของ RADIUS

Attribute Type	Name
1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
40	Acct-Status-Type
41	Acct-Delay-Time
44	Acct-Session-Id
46	Acct-Session-Time

2.3.1.3 กระบวนการทำงานของ RADIUS

ขั้นตอนการพิสูจน์ตัวตน (Authentication) และ กำหนดสิทธิ์การใช้งาน (Authorization) จะมีขั้นตอนการทำงานดังนี้



รูป 2.5 กระบวนการทำงานของ RADIUS

4) ผู้ใช้งานหรืออุปกรณ์ฝั่งปลายทางส่ง Request ซึ่งประกอบไปด้วยบัญชีผู้ใช้งาน และรหัสผ่านไปยังอุปกรณ์ NAS หรือ RADIUS Client เพื่อร้องขอสิทธิ์ในการเข้าใช้งานระบบเครือข่าย

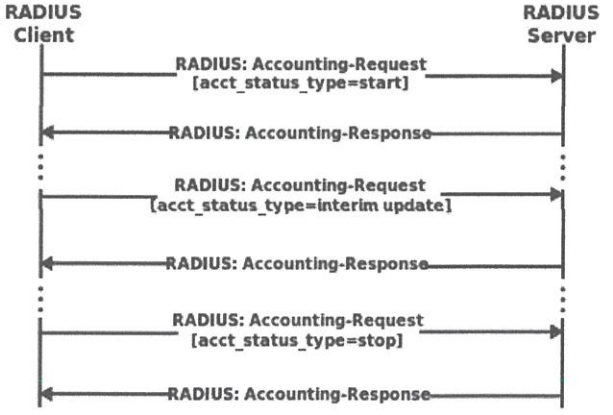
5) หลังจากนั้น NAS จะเพิ่มข้อมูลที่จำเป็นอื่นๆ ลงไป เช่น NAS-IP-Address, NAS-Port รวมถึงการเข้ารหัสบัญชีผู้ใช้งาน และรหัสผ่านด้วย Shared Secret และทำการส่ง RADIUS Access–Request ไปยัง port 1812 ของ RADIUS Server เพื่อพิสูจน์ตัวตน
6) เมื่อ Server ได้รับ RADIUS Access-Request จะทำการตรวจสอบว่ารู้จัก RADIUS Client ที่ร้องขอหรือไม่ จากนั้น Server จะทำการตรวจสอบโดยการถอดรหัสบัญชีผู้ใช้งานและรหัสผ่านที่ถูกส่งมาจาก NAS ด้วย Shared Secret โดยจะนำข้อมูลที่ได้รับไปตรวจสอบกับข้อมูลภายในฐานข้อมูลที่มีอยู่
7) หลังจาก RADIUS Server ตรวจสอบข้อมูลและสิทธิ์การเข้าใช้งานแล้ว RADIUS Server จะตอบกลับมา ยัง NAS เพื่อระบุว่าผู้ใช้หรืออุปกรณ์ปลายทางมีสิทธิ์ในการเข้าใช้งานหรือไม่ ดังนี้

   7.1) Access-Accept: ผู้ใช้ได้รับอนุญาต และมีสิทธิ์ในการเข้าใช้งาน

   7.2) Access-Reject: ผู้ใช้ไม่ได้รับอนุญาต และไม่มีสิทธิในการเข้าใช้งาน

   7.3) Access-Challenge: RADIUS Server ต้องการข้อมูลเพิ่มเติมจาก RADIUS Client
8) ในกรณีที่ RADIUS Server ตรวจสอบแล้วว่าผู้ใช้มีสิทธิ์เข้าใช้งานระบบ RADIUS Server จะระบุ Attribute บางอย่างเพื่อกำหนดสิทธิ์ในการเข้าใช้งานไปพร้อมกับ RADIUS: Access-Accept
9) RADIUS Client จะทำการอนุญาติหรือปฏิเสธให้ผู้ใช้หรืออุปกรณ์ปลายทางเข้าใช้งานเครือข่ายได้ โดยขึ้นอยู่กับผลการตอบกลับจาก RADIUS Server

2.3.1.4 ขั้นตอนในการ Accounting



รูป 2.6 ขั้นตอนการทำ Accounting

1) ในส่วนของการ Accounting จะเริ่มเมื่อผู้ใช้ได้รับสิทธิ์ในการใช้งาน โดย NAS จะทำการส่ง Accounting-Request Packet ที่มีค่าเป็น status_type = 'start' ไปยัง RADIUS Server เพื่อส่งสัญญาณเริ่มต้นการเข้าถึงข้อมูลของผู้ใช้
2) ระหว่างการใช้งาน NAS จะส่ง Accounting-Request Packet ที่มีค่าเป็น status_type = 'interim update' ไปยัง RADIUS เพื่อเป็นการอัพเดทสถานะการเชื่อมต่อ (session) และข้อมูลการใช้งานต่างๆในปัจจุบัน
3) เมื่อผู้ใช้ต้องการยกเลิกการใช้งาน NAS จะส่ง Accounting-Request Packet ที่มีค่าเป็น status_type = 'stop' ไปยัง RADIUS Server เพื่อส่งข้อมูลเกี่ยวกับการใช้งานทั้งหมด เช่น IP Address ของ Access Point จำนวน packet ที่ใช้งาน เวลาที่หยุดการเชื่อมต่อ ปริมาณข้อมูล (Byte) ที่เข้าและออกจากอุปกรณ์ และเหตุผลที่หยุดการเชื่อมต่อ เป็นต้น

2.3.1.5 Accounting Attribute ที่สำคัญ

1) Acct-Status-Type เป็น Attribute ที่มีได้สองค่า คือ Start ซึ่งจะถูกส่งเมื่อ Client เริ่มการเชื่อมต่อกับ NAS และ Stop ซึ่งจะถูกส่งมาเมื่อ Client หยุดการเชื่อมต่อกับ NAS
2) Acct-Session-ID เป็น Attribute ที่บอก Accounting Session ID เพื่อให้ง่ายแก่การตรวจสอบ Start และ Stop record และใช้ในการตรวจสอบกรณีมีการซ้ำกันของ record
3) Acct-Input-Octets เป็น Attribute ที่บอกถึงปริมาณข้อมูลในหน่วยไบต์ที่มีการส่งต่อจาก Client มายัง NAS ระหว่างที่มี Session ในการเชื่อมต่อ โดยจะส่งมาพร้อมกับ Attribute stop
4) Acct-Output-Octets เป็น Attribute ที่บอกถึงปริมาณข้อมูลในหน่วยไบต์ที่มีการส่งต่อจาก NAS มายัง Client ระหว่างที่มี Session ในการเชื่อมต่อ โดยจะส่งมาพร้อมกับ Attribute stop
5) Acct-Terminate-Cause เป็น Attribute ที่จะบอกถึงสาเหตุที่หยุด Session การเชื่อมต่อโดยสาเหตุที่หยุดการเชื่อมต่อจะมีลักษณะดังนี้

   5.1) Admin-Reset มีการ Reset อุปกรณ์ NAS

   5.2) User-Request Client หยุดการเชื่อมต่อโดยผู้ใช้งานเป็นคนขอหยุดการเชื่อมต่อ

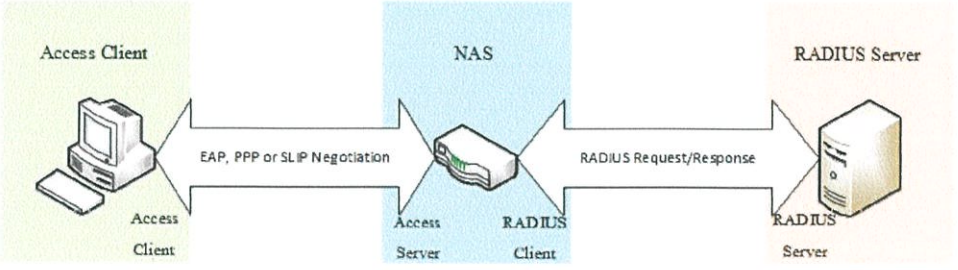
   5.3) NAS-Reboot มีการ restart อุปกรณ์ NAS

   5.4) Session-Timeout Session หมดอายุสำหรับ Client นั้น

2.3.1.6 วิธีการในการพิสูจน์ตัวตน (Authentication Method)

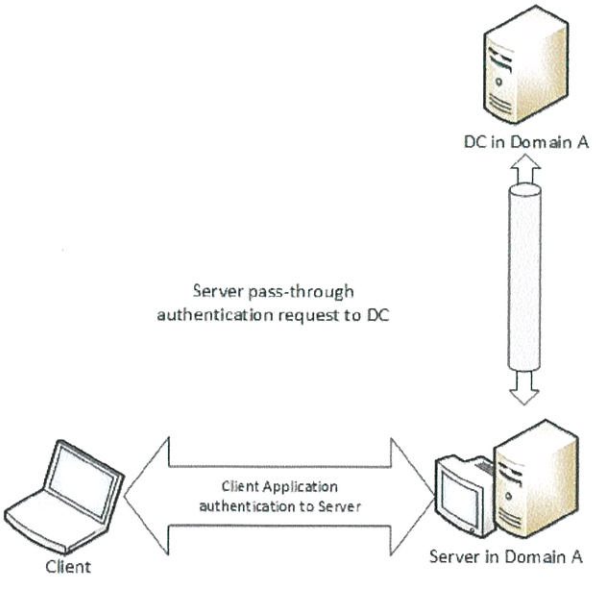
ในขั้นตอนการพิสูจน์ตัวตนของ Authentication Server เพื่อตรวจสอบสิทธิการใช้งาน สามารถทำได้หลายวิธีการดังต่อไปนี้

1) Native User Authentication คือการตรวจสอบบัญชีผู้ใช้ และรหัสผ่าน หรือข้อมูลอื่นๆ จากฐานข้อมูลที่ RADIUS Server จัดเก็บไว้ ดังรูป 2.7



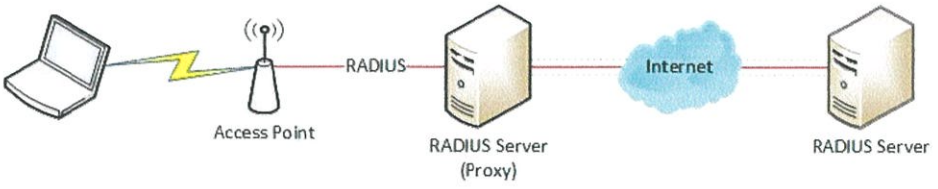
รูป 2.7 Native User Authentication

2) Pass-Through Authentication คือการส่งผ่านการ Authenticate ไปยังระบบการตรวจสอบอื่นๆ เช่น Windows NT Database, Microsoft Active Directory หรือ TACACS+ Server เป็นต้น ดังรูป 2.8



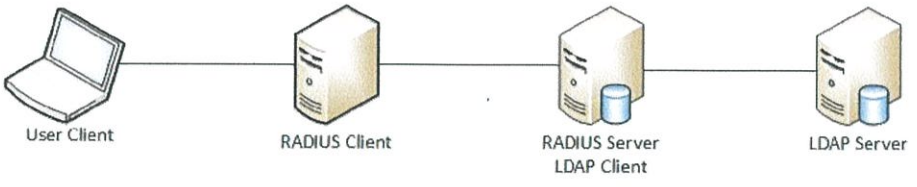
รูป 2.8 Pass-Through Authentication

3) Proxy RADIUS Authentication คือการส่งผ่านการ Authenticate ไปยัง RADIUS Server อื่นๆให้ทำหน้าที่ตรวจสอบแทนและส่ง Access-Accept หรือ Access-Reject กลับมายัง RADIUS Server ตัวเดิมเพื่อส่งให้กับ NAS ต่อไป ดังรูป 2.9



รูป 2.9 Proxy RADIUS Authentication

4) External Authentication คือ การตรวจสอบที่เป็นการทำงานร่วมกันระหว่าง RADIUS Server กับ ฐานข้อมูลต่างๆ เช่น Microsoft SQL, Oracle Database, LDAP Server หรือ Kerberos เป็นต้น ดังรูป 2.10



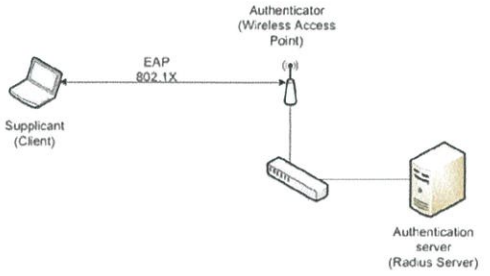
รูป 2.10 External Authentication

2.3.1.7 RADIUS Database

ในขั้นตอนการยืนยันตัวตนนั้น Authentication Server สามารถทำงานร่วมกันกับระบบฐานข้อมูลชนิดต่างๆ เช่น Microsoft SQL, MySQL หรือ Oracle Database เป็นต้น โดยฐานข้อมูลเหล่านี้จะเก็บข้อมูลในลักษณะ Relational Database ซึ่งนอกจากจะเก็บ Username และ Password ที่ใช้ในการยืนยันตัวตนแล้ว ยังใช้ในการเก็บข้อมูล Accounting ที่ RADIUS Server ได้รับมาอีกด้วย

2.4 802.1X

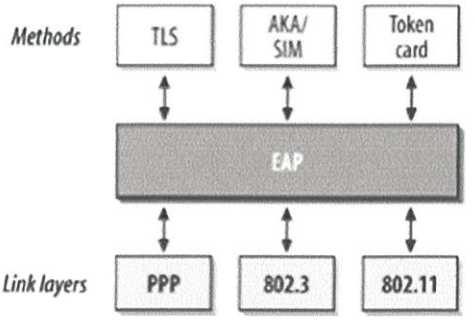
802.1X คือ มาตรฐาน IEEE สำหรับ MAC Layer ที่ใช้ในการตรวจสอบผู้ใช้งานระบบเครือข่ายที่ถูกนำมาประยุกต์ใช้ในการยืนยันตัวตนและการพิสูจน์ตัวตนทั้งในเครือข่าย LAN (802.3) และ Wireless LAN (802.11) โดย 802.1x โดยเมื่อมีผู้ขอเข้าใช้งานเครือข่าย (Supplicant) จะต้องมีการแสดงหลักฐานประกอบการตรวจสอบ (Credential) โดยข้อมูลดังกล่าวจะส่งไปยัง Authentication Server (RADIUS) และเนื่องจาก RADIUS ไม่ได้รองรับการ Authentication ที่ระดับ Layer 2 ดังนั้นจึงต้องเพิ่มมาตรฐานเข้ามาเพื่อที่จะขยายความสามารถของ RADIUS ซึ่งมาตารฐานนั้นจะเป็นไปตามโพรโทคอลที่เรียกว่า EAP (Extensible Authentication Protocol) ซึ่งมีลักษณะการทำงานดังรูป 2.11



รูป 2.11 การทำงานของ 802.1X

2.4.1 โพรโทคอล EAP

EAP (Extensible Authentication Protocol) ถูกระบุไว้ใน RFC 2284 และนำไปใช้งานครั้งแรกกับ PPP (Point to Point Protocol) และได้มีการรองรับโพรโทคอล IEEE 802.3 และ 802.11 เพิ่มขึ้นในเวลาต่อมา ซึ่ง EAP เป็นการ Encapsulation ที่ทำงานอยู่บน Link Layer มีลักษณะสถาปัตยกรรมดังรูป 2.12



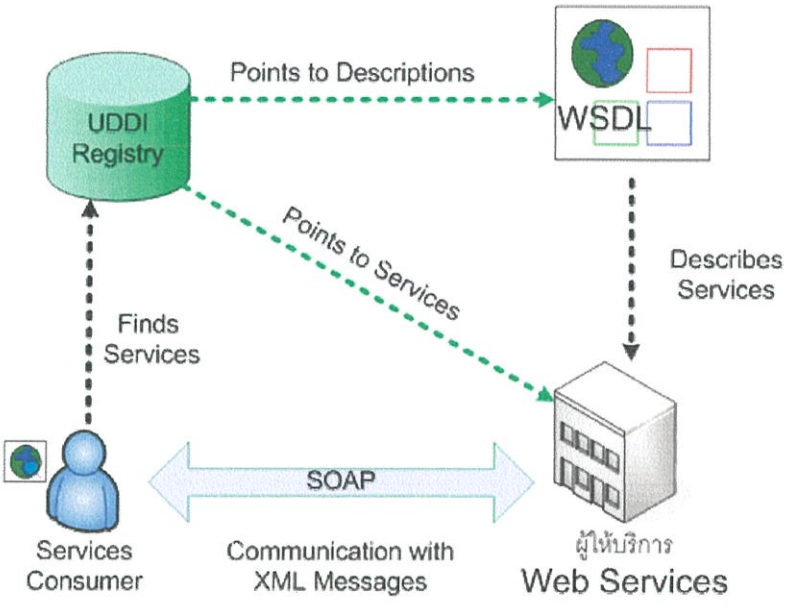
รูป 2.12 สถาปัตกรรมของ EAP

โพรโทคอล EAP แต่ละตัวจะมีข้อแตกต่างเรื่องข้อมูลที่ใช้ในการยืนยันตัวตน และนอกจากนี้ยังต่างกันในเรื่องการรักษาความปลอดภัยโดย EAP

1) EAP-MD5 Username และ Password จะถูกเข้ารหัสด้วยเทคนิค MD5
2) EAP (Lightweight EAP) ได้รับการพัฒนาขึ้นโดยบริษัท Cisco โดยโพรโทคอลนี้จะมีกลไกในการตรวจสอบความถูกต้องด้วยกระบวนการ request response และการกำหนดคีย์แบบ Dynamic Key
3) PEAP (Protected EAP) ร่วมกันพัฒนาโดยบริษัท Microsoft และ Cisco ออกแบบมาเพื่อประโยชน์จาก EAP-Transport Layer Security ทางด้านฝั่งเซิร์ฟเวอร์ สามารถสนับสนุนวิธีการตรวจสอบความถูกต้องหลายวิธี เช่น รหัสผ่านของผู้ใช้ รหัสผ่านป้อนครั้งเดียว เป็นต้น
4) EAP-TLS (Transport Layer Security) พัฒนาโดยบริษัท Microsoft ไม่ใช่ Username และ Password แต่ใช้ X.509 Certificates การทำงานของโพรโตคอลนี้จะอาศัยการส่งผ่าน PKI ผ่าน SSL (Secure Sockets Layers) มายัง EAP เพื่อใช้กำหนด WEP Key สำหรับผู้ใช้แต่ละคน ปัญหาหลักของ EAP-TLS คือความยุ่งยากและค่าใช้จ่ายในการติดตั้งจัดการและบริหารระบบ PKI Certificate

2.5 Web Service

Web Services คือแอพพลิเคชั่นหรือโปรแกรม ที่ถูกเรียกใช้งานในรูปแบบ RPC (Remote Procedure Call) ถูกออกแบบมาเพื่อให้บริการแลกเปลี่ยนข้อมูลระหว่างเครื่องคอมพิวเตอร์ผ่านระบบเครือข่ายโดยมีภาษาที่ใช้ในการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์เพื่อใช้อธิบายคุณสมบัติของการให้บริการกำกับไว้ Web Service ช่วยให้การเข้าถึงข้อมูลสารสนเทศจากแอพพลิเคชันที่ต่างกันเป็นไปโดยง่าย ซึ่งมาตรฐานของ Web Service ทำให้อินเทอร์เฟซของแอพพลิเคชันเหล่านี้ ถูกอธิบายโดย WSDL และทำให้อยู่ในมาตรฐานของ UDDI หลังจากนั้น จึงสามารถติดต่อสื่อสารถึงกันโดย XML ผ่าน SOAP (Simple Object Access Protocol) อินเตอร์เฟซ ซึ่ง W3C เป็นคณะกรรมการหลักในการรับผิดชอบมาตรฐานและสถาปัตยกรรมของ Web Service

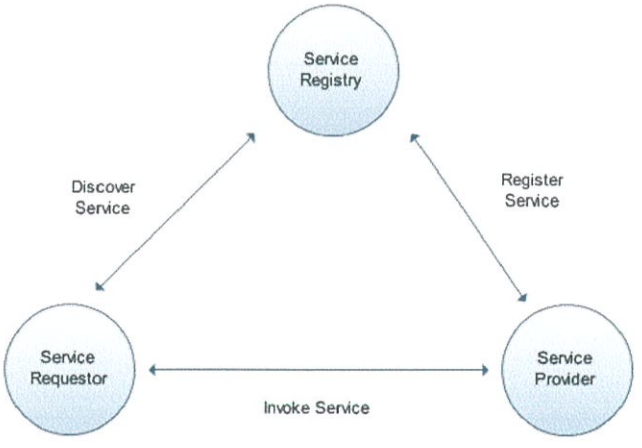


รูป 2.13 สถาปัตยกรรมของ Web Service

2.5.1 ประโยชน์ของ Web service

Web Service ช่วยให้การเข้าถึงข้อมูลสารสนเทศจากแอพพลิเคชันที่ต่างกันเป็นไปโดยง่าย โดยที่แอพพลิเคชันนั้นๆ สามารถทำงานแบบข้ามแพลตฟอร์มได้ Web Service สามารถถูกเรียกใช้ภายในองค์กรหรือจากภายนอกองค์กร โดยผ่านไฟร์วอล์ ดังนั้นจึงมีองค์กรใหญ่ๆ มากมายกำลังพัฒนาระบบที่มีอยู่ของตนให้เข้ากับ Web Service ซึ่งนับเป็นการลงทุนที่คุ้มค่า เนื่องจาก Web Service สามารถเพิ่มศักยภาพในการทำงานขององค์กรอีกทั้งลดค่าใช้จ่ายในการจัดการทรัพยากรขององค์กรได้อีกทางหนึ่ง

2.5.2 โมเดลการทำงานของ Web Service



รูป 2.14 กระบวนการทำงานของ Web Service

กระบวนการทำงานของ Web Service สามารถแบ่งบทบาทองค์ประกอบของ Web Service ได้ออกเป็นสามส่วน โดยทั้งสามองค์ประกอบมีความสัมพันธ์ดังแสดงในรูป 2.14 และสามารถอธิบายได้ดังนี้

1) ผู้ให้บริการ (Service Provider) จะมีหน้าที่ในการพัฒนาและติดตั้ง Web Service เป็นผู้ที่นิยามความหมายของบริการและลงทะเบียนบริการกับ Service Registry
2) ผู้ใช้บริการ (Service Requestor) จะเป็นผู้เรียกใช้ Web Service โดยอาจทำการค้นหาบริการจาก Service Directories แล้วทำการเรียกใช้บริการจากผู้ให้บริการ
3) Service Registry หรือ Service Broker มีหน้าที่ในการรับลงทะเบียนและช่วยในการค้นหา Web Service โดย Service Registry จะเก็บรายละเอียดของ Web Service เช่น นิยาม และตำแหน่งของ Web Service ซึ่งทำหน้าที่คล้ายกับสมุดโทรศัพท์เพื่อช่วยให้ผู้ใช้บริการสามารถค้นหาบริการที่ต้องการได้

2.5.4 เทคโนโลยีที่ใช้ในการพัฒนา Web Service

ในการพัฒนา Web Service จะมีเทคโนโลยีหลากหลายเทคโนโลยีที่เข้ามาเกี่ยวข้องเพื่อทำให้การพัฒนา Web Service เป็นไปอย่างมีประสิทธิภาพ

2.5.4.1 XML (Extensible Markup Language)

เป็นภาษา Markup ซึ่งทาง W3C (World Wide Web Consortium) ประกาศให้เป็นมาตรฐานของข้อมูลเมื่อเดือนกุมภาพันธ์ ปี 1992 โดย XML จะอยู่ในรูปของไฟล์ข้อความที่ใช้ Unicode และสามารถสร้างรูปแบบในการที่จะแสดงข้อมูลที่ซับซ้อนในรูปแบบของข้อความที่สามารถอ่านได้ง่าย ในปัจจุบัน XML ได้กลายเป็นมาตรฐานสำคัญสำหรับการกำหนดโครงสร้างข้อมูล เนื้อหา และรูปแบบของข้อมูลของเอกสารอิเล็กทรอนิกส์ ซึ่งทำให้ XML เป็นมาตรฐานในการแลกเปลี่ยนข้อมูลบนอินเทอร์เน็ตอย่างรวดเร็ว

```
<SampleXML>
  <Colors>
    <Color1>White</Color1>
    <Color2>Blue</Color2>
    <Color3>Black</Color3>
    <Color4 Special="Light">Green</Color4>
    <Color5>Red</Color5>
  </Colors>
  <Fruits>
    <Fruits1>Apple</Fruits1>
    <Fruits2>Pineapple</Fruits2>
    <Fruits3>Grapes</Fruits3>
    <Fruits4>Melon</Fruits4>
  </Fruits>
</SampleXML>
```

รูป 2.15 ตัวอย่างของภาษา XML

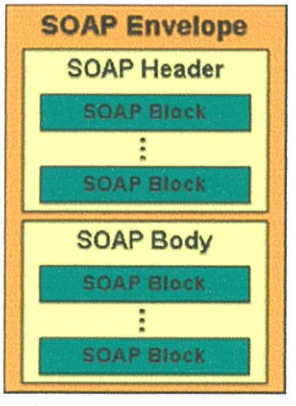
จากรูป 2.15 รูปแบบเอกสาร xml ไม่ได้บอกวิธีแสดงผลไว้ แต่เอกสาร xml สามารถสื่อความหมายให้คอมพิวเตอร์เข้าใจได้ และนำค่าไปประมวลผลต่อได้ แต่ถ้าต้องการจะแสดงผลจะต้องใช้ควบคู่กันกับภาษา HTML

2.5.4.2 SOAP (Simple Object Access Protocol)

SOAP เป็นโพรโทคอลที่เป็นภาษา XML ทำหน้าที่เป็นโพรโทคอลข่าวสาร (Message Protocol) สำหรับการแลกเปลี่ยนข้อมูลระหว่างผู้ให้บริการ SOAP เปรียบเสมือนจดหมายที่ใช้ในการสื่อสาร แต่ยังต้องใช้โพรโทคอลในการสื่อสารอื่นๆ เช่น HTTP ในการทำหน้าที่ส่งจดหมาย

SOAP มีโครงสร้างเอกสารในรูปแบบ XML ซึ่งสามารถแบ่งส่วนของเอกสารได้เป็น 3 ส่วนหลักดังนี้ คือ

1) SOAP Envelope ใช้ในการอธิบายข่าวสาร ระบุเนื้อหาสาระของเอกสารทั้งหมด
2) SOAP Header เป็นส่วนเพิ่มเติมของเอกสาร SOAP ซึ่งจะมีหรือไม่มีก็ได้
3) SOAP Body เป็นส่วนที่ใช้ในการเรียกใช้งานบริการ



รูป 2.16 โครงสร้างของเอกสาร SOAP

การส่งข้อความ SOAP มีสองรูปแบบคือ SOAP-RPC และ SOAP message โดย SOAP-RPC ใช้ในการส่งข้อความเพื่อใช้เรียก Procedure ซึ่งโดยมากจะเป็นรูปแบบ Synchronous โดย SOAP จะส่ง SOAP Request และข้อมูลต่างๆ เพื่อเรียกใช้เมธอดในการประมวลผล และจะรอให้ได้ผลลัพธ์การประมวลผลที่ส่งกลับมาแบบ SOAP Response ส่วน SOAP-message ใช้ในการส่งข่าวสารหรือข้อมูลในรูปแบบ XML ระหว่างผู้ให้บริการและผู้ใช้บริการ โดยสามารถส่งได้ทั้งแบบ Synchronous และ Asynchronous

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
        soap:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
        <soap:Header>
          <!-- ข้อมูลในส่วนของ Header -->
          <i:local xmlns:i="http://www.i3t.or.th/ws/">
          <i:currency>Bath</i:currency>
          </i:local>
        </soap:Header>
        <soap:Body>
          <!-- ข้อมูลในส่วนของ Body -->
          <GetPrice>
            <Item>Rose</Item>
            <Quantity>100</Quantity>
          </GetPrice>
        </soap:Body>
        <soap:Fault>
        <!-- ข้อมูลของ SOAP ในกรณีมีข้อผิดพลาด จาก SOAP Node -->
        </soap:Fault>
      </soap:Envelope>
  <soap:Fault>
    <faultcode>Client</faultcode>
    <faultstring>Invalid Request</faultstring>
  </soap:Fault>
  <soap:Fault>
    <faultcode>Client</faultcode>
    <faultstring>Invalid Request</faultstring>
  </soap:Fault>
```

รูป 2.17 ตัวอย่างของเอกสาร SOAP

2.5.5 WSDL (Web Services Description Language)

WSDL เป็นภาษา XML ที่ใช้อธิบายคุณลักษณะการให้บริการของ Web Service และวิธีการติดต่อกับ Web Service เป็นมาตรฐานสำหรับการประกาศ Process ที่จำเป็นในการเรียกใช้ SOAPโดยจะแบ่งการอธิบาย Web Service ปีนสองส่วนดังนี้

1) ส่วนที่เป็น Abstract อธิบาย Operation อินพุตและเอาท์พุตพารามิเตอร์
2) ส่วนที่เป็น Concrete อธิบายโพรโทคอลของเครือข่ายตำแหน่งของจุดปลายทาง (Endpoint Address) และ รูปแบบของข้อมูล

2.5.6 UDDI (Universal Description, Discovery, and Integration)

UDDI เป็นข้อกำหนดเกี่ยวกับระบบ Registry Service สำหรับบริการทั้งแบบไม่ใช่อิเล็กทรอนิกส์ และแบบอิเล็กทรอนิกส์ UDDI ใช้สำหรับค้นหาบริการที่ต้องการและเมื่อได้มาแล้ว UDDI ยังจัดหาข้อตกลงในวิธีการที่จะใช้งาน เปรียบได้กับสมุดหน้าเหลือง Service Provider สามารถใช้ UDDI ในการประกาศว่าบริการใดบ้างที่ให้บริการและลูกค้าสามารถใช้บริการของ UDDI ในการค้นหาบริการที่ต้องการได้ตรงตามความต้องการได้ ข้อกำหนดของ UDDI ได้มีการนิยาม ดังนี้

1) SOAP APIs (Application Programming Interface) ซึ่งแอพพลิเคชันจะใช้ในการสอบถามและประกาศข้อมูลไปยังระบบลงทะเบียน UDDI

2) XML Schema คือ โครงสร้างรูปแบบของระบบลงทะเบียนและรูปแบบของ SOAP Message Format

2.6 ภาษา PHP

PHP เป็นภาษาสคริปต์ในลักษณะ Server-Side เป็นลักษณะโอเพนซอร์ส ภาษา PHP มีรากฐานโครงสร้างคำสั่งมาจาก ภาษา C Java และ Pearl ภาษา PHP ง่ายต่อการเรียนรู้ เป้าหมายหลักของภาษานี้คือต้องการให้นักพัฒนาเว็บไซต์สามารถเขียนเว็บเพจที่สามารถตอบโต้ได้อย่างรวดเร็ว PHP มีความสามารถในการนำข้อมูลจากฐานข้อมูลประเภทต่างๆ มาแสดงในเว็บเพจจึงเหมาะแก่การนำมาพัฒนาเว็บเพจเป็นอย่างมาก

2.6.1 PHP Framework

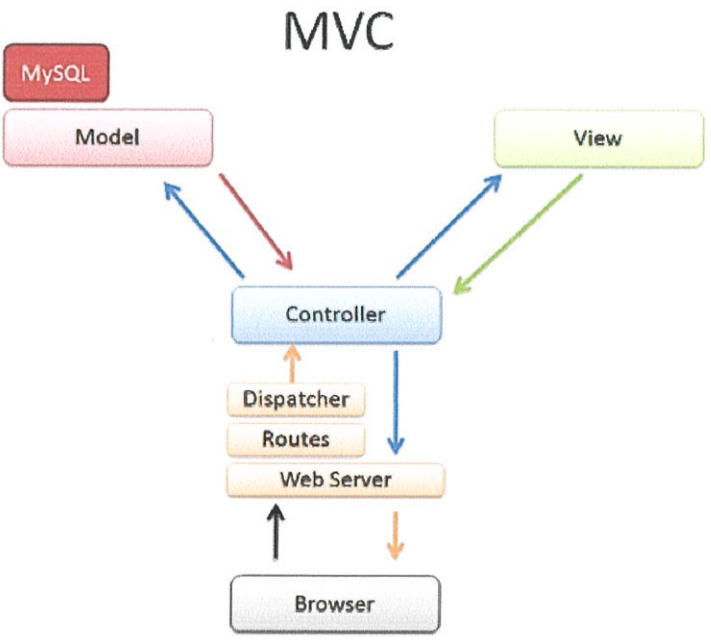
PHP Framework เป็นรูปแบบโครงสร้างของการเขียนโปรแกรมที่มีการวางโค้ดไว้อย่างเป็นระบบ มีแบบแผน และลักษณะการเขียนที่เป็นมาตรฐานตามโปรแกรมต่างๆ ซึ่ง PHP Framework นั้นเหมาะกับการนำมาใช้พัฒนาแอพพลิเคชันที่มีขนาดใหญ่ มีผู้พัฒนาหลายคน เพราะจะช่วยให้โค้ดที่ทำการเขียนมีทิศทางไปในทิศทางเดียวกันหมด ซึ่งปัญหาหนึ่งของการใช้ภาษา PHP ในการพัฒนาของนักพัฒนาคือ นักพัฒนาแต่ละคนนั้นจะมีวิธีในการเขียนโค้ดที่ไม่เหมือนกัน มีไอเดียที่ต่างกัน รูปแบบการจัดการโฟลเดอร์ที่แตกต่างกัน แต่ในที่สุดจะให้ผลลัพธ์ที่เหมือนกัน ดังนั้นเมื่อต้องมาทำงานร่วมกันจะเกิดปัญหาในเรื่องของรูปแบบที่ขัดแย้งกัน

ข้อดีของการใช้ PHP Framework

1) ลดปัญหาความขัดแย้งของโค้ด ที่เกิดขึ้น
2) มีการวางโครงสร้างไฟล์ไว้อย่างเป็นระบบ ระเบียบที่แน่นอน
3) มีฟังก์ชั่นที่พร้อมใช้งาน ทำให้ง่ายต่อการเขียน
4) ง่ายในการบริหารจัดการ หากนักพัฒนาต้องทำงานเป็นทีม

2.7 MVC

MVC (Model-View-Controller) คือ สถาปัตยกรรมซอฟต์แวร์ชนิดหนึ่งเป็นหลักการออกแบบรูปแบบหนึ่งซึ่งเป็นที่นิยมมากในการนำมาออกแบบและประยุกต์ใช้กับเว็บแอพพลิเคชัน ใช้เพื่อแยกส่วนการทำงานโดยแยกออบเจคที่เก็บข้อมูล (Model) ออบเจคที่แสดงข้อมูล (View) และออบเจคที่ติดต่อกับผู้ใช้ (Controller) ออกจากกันอย่างชัดเจน ดังแสดงให้เห็นในรูป 2.18



รูป 2.18 ส่วนการทำงานต่างๆของ MVC

1) Model (M) เป็นการแบ่งงานออกมาเพื่อทำการติดต่อกับระบบฐานข้อมูล Model เป็นออบเจคที่ทำหน้าที่เป็นตัวแทนของข้อมูลไม่ว่าข้อมูลจะถูกจัดเก็บในรูปแบบใดในฐานข้อมูล เมื่อข้อมูลนั้นถูกโหลดเข้ามาในแอพพลิเคชันจะถูกเปลี่ยนให้อยู่ในรูปของออบเจคและเรียกออบเจคนั้นว่า Model การทำงานในส่วนนี้ เช่น การ Insert, Delete และ Update ค่าลงไปในฐานข้อมูลหรืออาจจะเป็นการเขียน function ที่ไม่ได้เกี่ยวข้องกับฐานข้อมูลแต่เป็นการคำนวณค่าต่างๆ เพื่อนำมาเก็บไว้ก็สามารถทำได้เช่นกัน
2) View (V) เป็นส่วนที่มีหน้าที่ในการแสดงผลข้อมูลต่างๆ เช่น แสดงผลลัพธ์จากการค้นหา แสดงฟอร์มในการกรอกข้อมูล เป็นต้น ซึ่งเปรียบเสมือนเป็น UI ของเว็บเพจนั่นเอง
3) Controller (C) เป็นส่วนที่ทำหน้าที่ในการรับคำสั่งจากผู้ใช้ ส่วนประมวลผล ตอบสนองคำสั่งจากผู้ใช้ และทำหน้าที่เรียกออบเจคตัวอื่นๆ (M และ V) ให้ทำงานร่วมกัน หน้าที่ของ Controller เช่น ทำการตรวจสอบข้อมูลก่อนการประมวลผล ส่งต่อผลลัพธ์ไปยัง View เพื่อแสดงผลให้ผู้ใช้ เป็นต้น จะเห็นได้ว่า Controller เป็นตัวควบคุมเส้นทางการทำงานของคำสั่งต่างๆ

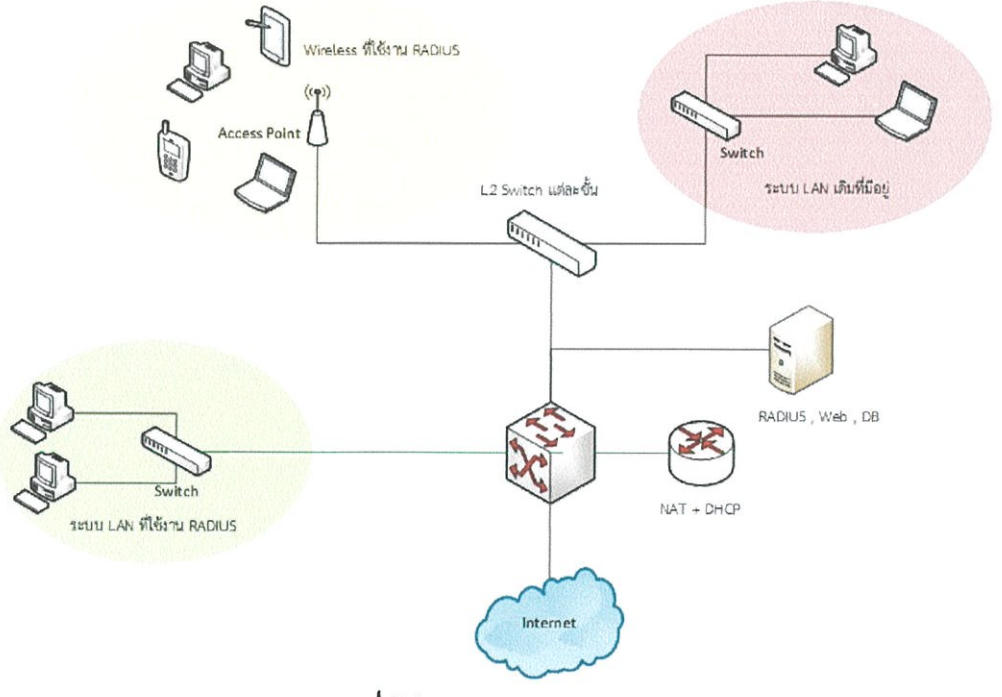
บทที่ 3

การออกแบบและพัฒนา

ในบทนี้จะอธิบายถึง ภาพรวมของระบบเครื่องมือที่ใช้ในการพัฒนา จากนั้นจะอธิบายถึงส่วนการทำงานต่างๆ ในระบบ เช่น ส่วนการยืนยันตัวตน ส่วนของฐานข้อมูล และส่วนของเว็บไซต์ โดยในแต่ละส่วนจะอธิบายถึงรายละเอียดของการออกแบบ

3.1 ภาพรวมของระบบ

ในส่วนนี้จะอธิบายถึงองค์ประกอบของระบบ อุปกรณ์ที่จะต้องใช้สำหรับระบบ รายละเอียดการออกแบบระบบทั้งในส่วนของ Physical Diagram และ Logical Diagram การออกแบบ IP Address ให้กับระบบ โดยภาพรวมของระบบนั้นแสดงในรูป 3.1



รูป 3.1 ภาพรวมของระบบ

จากรูป 3.1 ได้มีการออกแบบระบบโดยภายในระบบจะมีองค์ประกอบดังนี้

1) Server ทำหน้าที่หลายอย่างในอุปกรณ์เดียวกัน ซึ่ง Server จะทำหน้าที่ต่างๆ ดังนี้
   1.1) RADIUS Server ทำหน้าที่ในการตรวจสอบการยืนยันตัวตนของผู้ใช้งาน

1.2) Database Server ทำหน้าที่เป็นฐานข้อมูลของระบบที่ทำการเก็บข้อมูลต่างๆ เช่น ข้อมูล Username และ Password ข้อมูลส่วนตัวของผู้ใช้งาน ข้อมูลสิทธิการใช้งาน และ ข้อมูลปริมาณการใช้งาน เป็นต้น

1.3) Web Server ทำหน้าที่ให้บริการเว็บเพจกับผู้ใช้งานในระบบทั้ง Admin, Student, Lecturer และ Guest

2) Core switch ทำหน้าที่ในการเชื่อมต่อกับอุปกรณ์ภายในภาควิชาและเครือข่ายภายนอก

3) Router ทำหน้าที่ในการแจก DHCP เพื่อจ่าย Private IP ให้กับระบบ Wireless ที่ใช้งาน RADIUS อีกทั้งยังทำหน้าที่ในการเป็นอุปกรณ์ NAT สำหรับการเชื่อมต่อกับ Public IP ด้วย

4) Switch ทำหน้าที่เชื่อมต่อระหว่าง Core Switch กับอุปกรณ์คอมพิวเตอร์ของผู้ใช้งานในระบบ LAN และเชื่อมต่อกับ Access Point ในระบบ Wireless

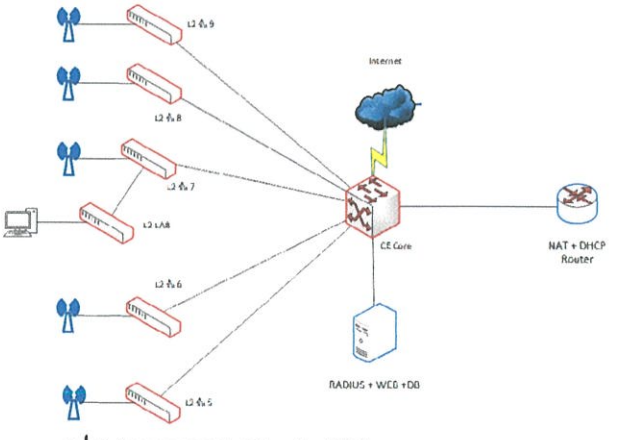
5) ระบบ Wireless ที่ใช้งาน RADIUS โดยที่ Access Point จะเชื่อมต่อกับ Switch ในแต่ละชั้น อุปกรณ์ของผู้ใช้งานสามารถเข้าใช้งานระบบโดยการเชื่อมต่อกับ Access Point ที่จะทำการติดตั้งในแต่ละชั้นภายในภาควิชา

6) ระบบ LAN ที่ใช้งาน RADIUS ผู้ใช้สามารถเข้าใช้ระบบนี้ผ่านทางคอมพิวเตอร์ในห้องปฏิบัติการคอมพิวเตอร์ของภาควิชา

7) ระบบ LAN เดิมของภาควิชาที่มีอยู่แล้ว ซึ่งในส่วนนี้ไม่ได้ทำอะไรเพิ่มเติม

3.1.1 Physical Diagram

ในส่วนนี้จะอธิบายถึงอุปกรณ์ต่างๆ ที่อยู่ภายในระบบว่าแต่ละอุปกรณ์มีการเชื่อมต่อกันอย่างไร อุปกรณ์ใดมีอยู่แล้ว อุปกรณ์ใดต้องทำการจัดหาเพิ่ม โดยจากรูป 3.2 อุปกรณ์ที่มีกรอบเป็นสีแดงเป็นอุปกรณ์เดิมของภาควิชาไม่ต้องทำการจัดซื้อเพิ่ม ส่วนอุปกรณ์ที่มีกรอบเป็นสีน้ำเงินเป็นอุปกรณ์ที่ต้องจัดหาเพิ่มเติม

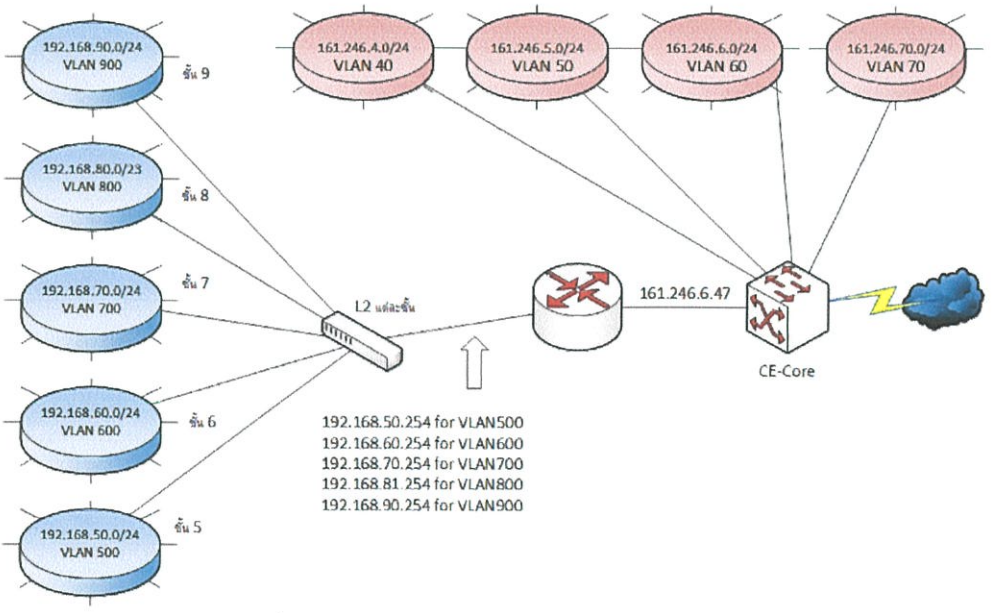


รูป 3.2 แผนภาพ Physical Diagram ของระบบ

จากรูป 3.2 จะแสดงแผนภาพ Physical Diagram ของระบบทั้งหมดซึ่งจะมีรายละเอียดดังนี้

1) CE Core เป็นอุปกรณ์เครือข่ายของภาควิชาที่มีอยู่แล้วซึ่งปัจจุบันติดตั้งอยู่ในห้องเครื่องแม่ข่ายของภาควิชา
2) Switch L2 แต่ละชั้น เป็นอุปกรณ์เครือข่ายของภาควิชาที่มีอยู่แล้ว ปัจจุบันติดตั้งตามชั้นต่างๆ ภายในภาควิชา
3) Server เป็นอุปกรณ์ที่จะต้องจัดหาเพิ่ม ซึ่งติดตั้งภายในห้องเครื่องแม่ข่ายของภาควิชา แต่เนื่องจากการทำหน้าที่เป็น Database Server, Web Server และ RADIUS Server ทำให้มีความสามารถในการติดตั้งภายในสถานที่ๆ สามารถเข้าถึงระบบเครือข่ายที่ใดก็ได้ภายในภาควิชา
4) Router เป็นอุปกรณ์ที่ต้องจัดหาเพิ่ม โดยติดตั้งภายในห้องเครื่องแม่ข่ายของภาควิชา
5) Access Point เป็นอุปกรณ์ที่ต้องจัดหาเพิ่มโดยรายละเอียดการติดตั้งตามจุดต่างๆ จะกล่าวถึงในภายหลัง

3.1.2 Logical Diagram



รูป 3.3 แผนภาพ logical Diagram ของระบบ

ในส่วนนี้จะอธิบายถึงการจัดสรร IP Address ให้กับระบบ อีกทั้งยังอธิบายระบบ IP Address เดิมของระบบ LAN เพื่อทำให้ระบบสามารถทำงานร่วมกันได้โดยระบบเครือข่ายเดิมที่เป็นระบบ LAN ของภาควิชานั้นจะเป็นเครือข่ายที่มี ส่วนระบบเครือข่ายสำหรับระบบเครือข่ายที่

เพิ่มขึ้นมานั้น จะเป็นระบบเครือข่ายสีน้ำเงิน ดังรูป 3.3 ส่วนของรายละเอียดในการออกแบบและจัดสรร IP Address ของระบบเครือข่ายที่เพิ่มเข้ามานั้นจะอธิบายอยู่ในตาราง 3.1

ตาราง 3.1 รายละเอียดการจัดสรร IP Address ให้กับระบบเครือข่าย

ชั้น	เครือข่าย	VLAN	Subnet	Gateway
9	192.168.90.0/24	900	255.255.255.0	192.168.90.254
8	192.168.80.0/23	800	255.255.254.0	192.168.81.254
7	192.168.70.0/24	700	255.255.255.0	192.168.70.254
6	192.168.60.0/24	600	255.255.255.0	192.168.60.254
5	192.168.50.0/24	500	255.255.255.0	192.168.50.254

3.2 ส่วนการยืนยันตัวตน

ในส่วนการยืนยันตัวตนจะอธิบายถึงแพลตฟอร์มที่นำมาใช้ในระบบยืนยันตัวตน บริการ (service) หรือ ซอฟต์แวร์ต่างๆ และอุปกรณ์ที่นำมาใช้ รวมไปถึงรายละเอียดการออกแบบจุดติดตั้ง Access Point ภายในภาควิชาวิศวกรรมคอมพิวเตอร์

3.2.1 RADIUS Server

สำหรับ RADIUS Server นั้นจะใช้อุปกรณ์ Server มาติดตั้งระบบปฏิบัติการหลังจากนั้นจะลงบริการที่ทำให้สามารถใช้งาน RADIUS Protocol ได้ ซึ่งระบบปฏิบัติการที่จะเลือกใช้นั้นสามารถเลือกได้หลากหลาย

3.2.1.1 แพลตฟอร์มสำหรับ RADIUS Server

สำหรับแพลตฟอร์มที่นำมาใช้กับ RADIUS Server เพื่อทำหน้าที่ในการยืนยันตัวตนเข้าใช้งานแพลตฟอร์ม GNU สำหรับแพลตฟอร์ม GNU/Linux นั้นได้เลือกใช้งาน Ubuntu Server 14.04 LTS โดยข้อดีของ Linux คือ มีความเร็วในการทำงานสูงเนื่องจากไม่มี GUI (Graphic User Interface) ทำให้ไม่ต้องมีการประมวลผลในโหมดกราฟิก ซึ่งส่งผลให้การใช้งานทรัพยากรของระบบ Linux มีความคุ้มค่ามาก อีกทั้งระบบ Linux นั้นถูกออกแบบมาให้ทำงานในหน้าที่ Server อยู่แล้ว ส่วนเหตุผลที่เลือก Linux Distribution เป็น Ubuntu เพราะว่าเป็นระบบที่มีการอัพเดทเวอร์ชั่นใหม่บ่อย และยังเป็น Distribution ที่เพิ่งเกิดได้ไม่นานแต่ได้รับความนิยมในการใช้งานสูง โดย Server ที่จะนำมาใช้งานจะต้องมีความต้องการดังตาราง 3.2

ตาราง 3.2 ความต้องการของระบบ Ubuntu Server 14.04 LTS

รายละเอียด	ความต้องการขั้นต่ำ	ความต้องการที่แนะนำ
CPU	300 MHz	1 GHz
RAM	192 MB	512 MB
HDD	1 GB	2 GB

3.2.1.2 RADIUS Software ที่ใช้ในการยืนยันตัวตน

สำหรับ RADIUS Software ที่ใช้ในการยืนยันตัวตนนั้นใช้ FreeRADIUS เวอร์ชัน 2.1.12 เหตุผลที่เลือกใช้ FreeRADIUS เนื่องจากเป็น Software ที่เป็น Opensource และเป็น RADIUS Software ที่ได้รับความนิยมมาก

3.2.1.3 Authenticator

Authenticator หรือจะเรียกในอีกชื่อหนึ่งว่า NAS จะเป็นอุปกรณ์ที่จะส่งข้อมูลการยืนยันตัวตนของผู้ใช้งานไปยัง RADIUS เพื่อให้ RADIUS พิจารณาว่าจะให้ผู้ใช้เข้าสู่ระบบเครือข่ายได้หรือไม่ โดยที่ Authenticator ของระบบ Wireless LAN จะเป็นอุปกรณ์ Access Point หรือ อุปกรณ์ Wireless Router ที่จะต้องมีความสามารถในการรองรับ Wireless Security แบบ WPA2-Enterprise ส่วนในระบบ LAN นั้นจะใช้ Switch เป็น Authenticator ซึ่งรองรับมาตรฐาน 802.1X

3.2.1.4 กระบวนการในการยืนยันตัวตนของ RADIUS Server

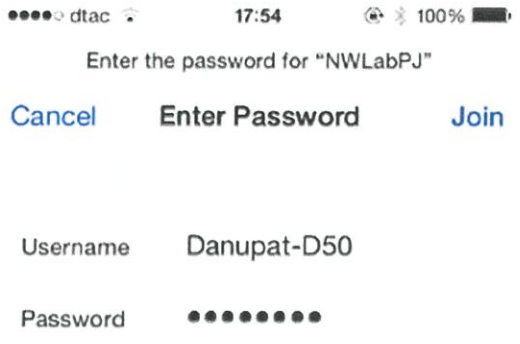
RADIUS Server จะตรวจสอบข้อมูลที่ Authenticator ส่งมา โดยการเข้าไปตรวจสอบกับระบบฐานข้อมูลว่ารหัสของผู้ใช้งานนั้นถูกต้องหรือไม่ถ้าชื่อผู้ใช้งานและรหัสผ่านถูกต้อง RADIUS จะส่ง Access-Accept ไปยัง Authenticator เพื่ออนุญาตให้ผู้ใช้เข้าสู่ระบบเครือข่ายได้ แต่ถ้าชื่อผู้ใช้หรือรหัสผ่านไม่ถูกต้อง RADIUS จะส่ง Access-Reject ไปยัง Authenticator ส่งผลให้ผู้ใช้งานไม่สามารถเข้าใช้งานได้

3.2.1.5 เงื่อนไขในการเข้าใช้ระบบยืนยันตัวตน

ผู้ใช้จำเป็นต้องมีชื่อบัญชีที่เข้าใช้งานระบบก่อนจึงจะสามารถเข้าใช้งานได้ โดยถ้าผู้ใช้ยังไม่เคย Login เพื่อเข้าใช้งานระบบมาก่อน (ทำการยืนยันเพื่อ Login ครั้งแรก) ผู้ใช้ก็จะต้องกรอกบัญชีผู้ใช้งานและรหัสผ่าน แต่ถ้าหากผู้ใช้เคยใช้งานระบบมาก่อนแล้วบัญชีผู้ใช้งานและรหัสผ่านจะถูกจดจำไว้ในระบบของผู้ใช้งาน ทำให้ในการเข้าใช้งานครั้งต่อๆ ไปผู้ใช้ไม่จำเป็นต้องกรอกข้อมูลอีก

3.2.1.6 หน้าต่างในการยืนยันตัวตนเข้าใช้งาน

1) Smartphone ในที่นี้ได้ยกตัวอย่างการยืนยันตัวตนเพื่อเข้าใช้งานระบบเครือข่ายผ่านทาง IOS smartphone โดยเลือกที่ SSID ของระบบนี้ จากนั้นจะปรากฏหน้าต่างซึ่งจะให้ใส่ชื่อบัญชีผู้ใช้งานและรหัสผ่านดังรูป 3.4



รูป 3.4 หน้าต่างยืนยันตัวตนเข้าใช้งานบน IOS smartphone

2) Windows ในที่นี้ได้ยกตัวอย่างการเข้าใช้งานผ่านระบบปฏิบัติการ Windows 8.1 โดยในการเชื่อมต่อนั้นให้เลือก SSID ของระบบ จากนั้นจะขึ้นหน้าต่างซึ่งจะให้ใส่ชื่อบัญชีผู้ใช้งานและรหัสผ่านดังรูป 3.5

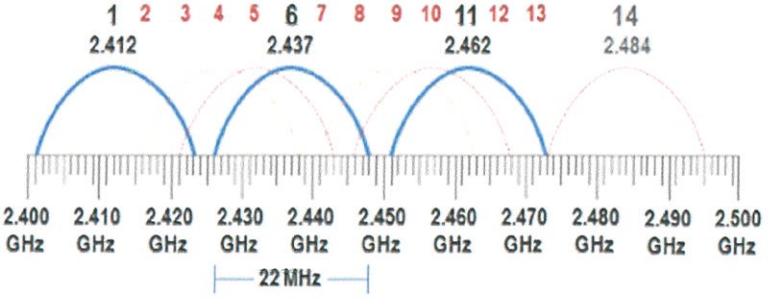
รูป 3.5 หน้าต่างยืนยันตัวตนเข้าใช้งานบน Windows 8

3.2.2 รายละเอียดการออกแบบจุดติดตั้ง Access Point

ในการที่จะออกแบบจุดติดตั้ง Access Point นั้นจะกระทำโดยการทำการลงสำรวจพื้นที่จริงในการติดตั้ง ทั้งนี้เนื่องจากแต่ละห้องภายในภาควิชานั้นมีความแตกต่างกันในด้านของพื้นที่และสิ่งกีดขวาง โดยเมื่อทำการสำรวจแล้วทำการวาดออกมาเป็นแผนที่พร้อมทั้งจุดที่ใช้ในการติดตั้ง

3.2.2.1 หลักการในการออกแบบจุดติดตั้ง Access Point

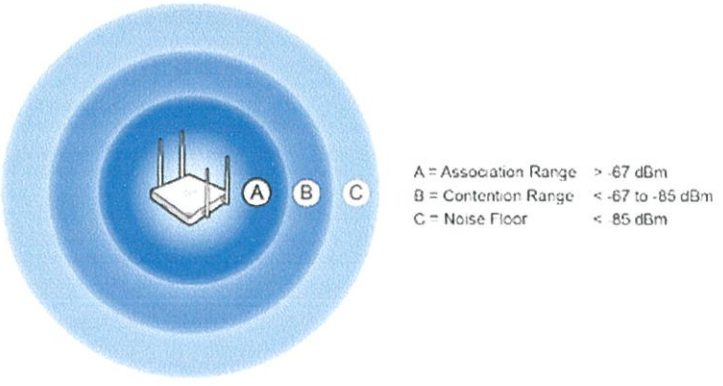
ใช้หลักในการออกแบบโดยใช้ Non-Overlapping Channel ซึ่งหมายถึงเป็นช่องสัญญาณที่จะไม่มีการซ้อนทับกันของคลื่นความถี่กับช่องสัญญาณข้างเคียงเลย เพื่อทำให้มีประสิทธิภาพในการใช้งานที่สูงที่สุด ซึ่งโดยในที่นี้ จะใช้ Non-Overlapping Channel ของย่านความถี่ 2.4 GHz นั่นก็คือ Channel ที่ 16 และ 11 ดังแสดงในรูป 3.6



รูป 3.6 non-overlapping channel

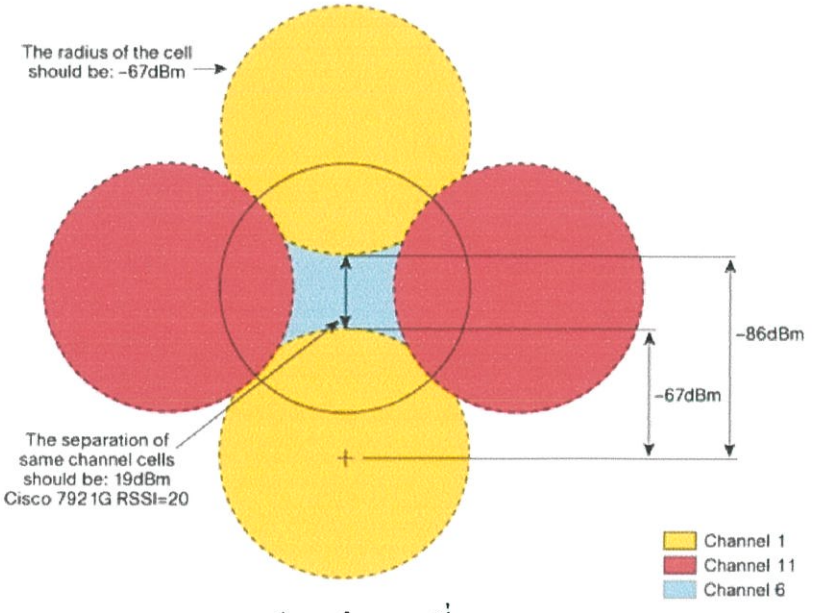
และเพื่อให้การใช้งานที่ครอบคลุมนั้นการออกแบบจะต้องคำนึงถึงค่า RSSI (Received Signal Strength Indication) ซึ่งเป็นค่าที่ใช้ในการวัดความแรงหรือความเข้มของสัญญาณในเทอมของพลังงานซึ่งจะมีหน่วยเป็น dBm (Decibels Milliwatt) ค่า RSSI จะแปรผันตรงกับความแรงของสัญญาณ ถ้า RSSI มีค่ามากแสดงว่าสัญญาณที่ได้รับมีความแรงสูง และในทางกลับกันหากค่า RSSI มีค่าน้อยแสดงว่าสัญญาณที่ได้รับมีความแรงต่ำ ซึ่งความแรงของสัญญาณนั้นจะส่งผลต่อความเร็วในการใช้งานและความเสถียรในการเชื่อมต่อระหว่างอุปกรณ์กับ Access Point

จากข้อมูลที่ได้จากเอกสาร White Paper ของบริษัท Aerohive Networks ในหัวข้อเรื่อง High-Density Wi-Fi Design Principles โดยภายในเอกสารได้ระบุไว้ว่าค่า RSSI ที่เหมาะสมที่สุดสำหรับการใช้งานดังรูป 3.7 โดยสำหรับการใช้งานประเภทสื่อวิดีโอนั้นค่า RSSI ควรจะไม่ต่ำกว่าช่วง -67 dBm และช่วงสัญญาณที่ยังสามารถเชื่อมต่อได้โดยไม่หลุดจะมีค่า RSSI ระหว่าง -67 dBm ถึง -86 dBm



รูป 3.7 ค่า RSSI ในระยะต่างๆ

และสอดคล้องกับข้อมูลจาก White Paper หัวข้อ Design Principles for Voice Over WLAN ของบริษัท Cisco ซึ่งกล่าวถึงค่า RSSI ในการออกแบบระบบเครือข่ายไร้สายให้ครอบคลุมดังรูป 3.8 ซึ่งค่า RSSI ที่เหมาะแก่การใช้งานคือช่วงที่ไม่ต่ำกว่า -67 dBm และไม่ควรเกิน -86 dBm ซึ่งจากทั้ง 2 เอกสารที่กล่าวมานั้นใช้ค่าที่ใกล้กัน

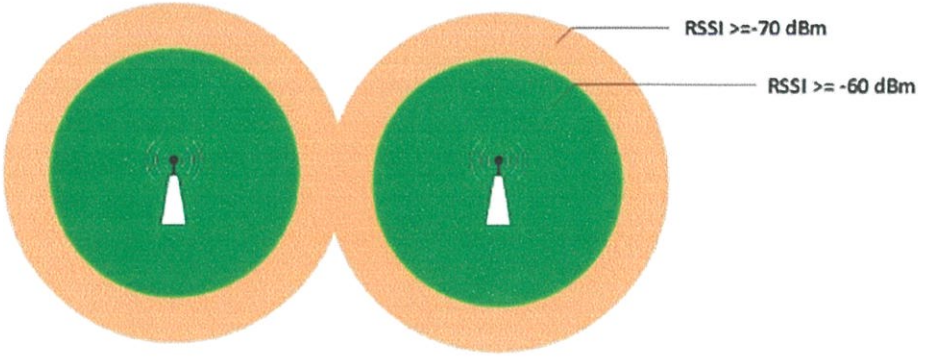


รูป 3.8 ค่า RSSI ที่เหมาะสม

3.2.2.2 ขั้นตอนในการออกแบบจุดติดตั้ง Access Point

ในการออกแบบจุดติดตั้งนั้นเริ่มจากการสำรวจจุดติดตั้งในพื้นที่จริงด้วยการนำ Access Point ไปติดตั้งในจุดนั้น จากนั้นใช้แอพพลิเคชัน Wi-Fi Analyzer ในการวัดค่า RSSI โดยมี

ขอบเขตในการวัดค่า RSSI ดังรูป 3.9 ซึ่งในพื้นที่สีเขียวจะมีค่า RSSI ไม่ต่ำกว่า -60 dBm และในเขตพื้นที่สีส้มจะมีค่า RSSI ไม่ต่ำกว่า -70 dBm

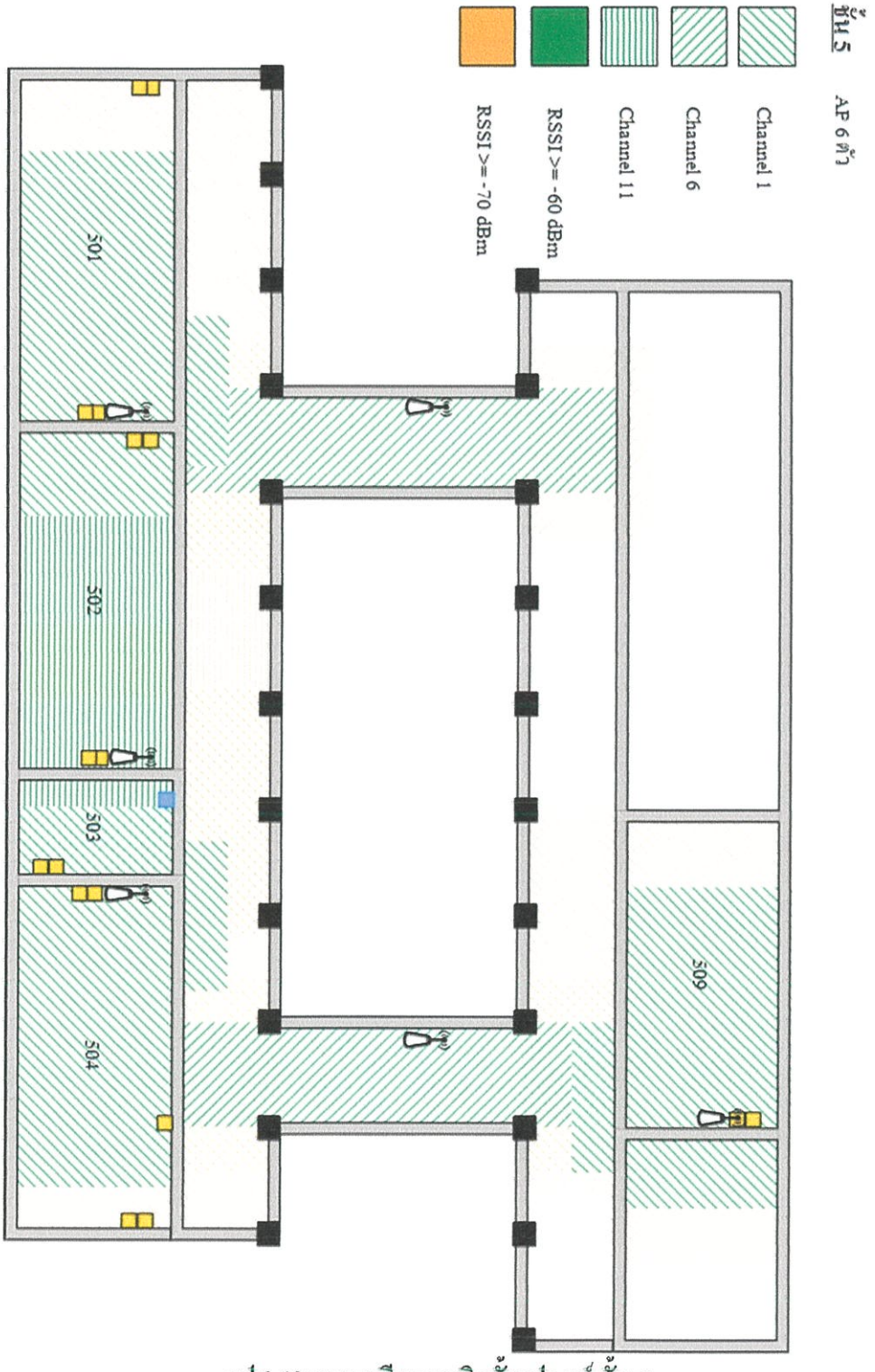


รูป 3.9 ขอบเขตของค่า RSSI ที่ใช้ในการวัดสัญญาณ

3.2.3 รายละเอียดการติดตั้งอุปกรณ์ Access Point

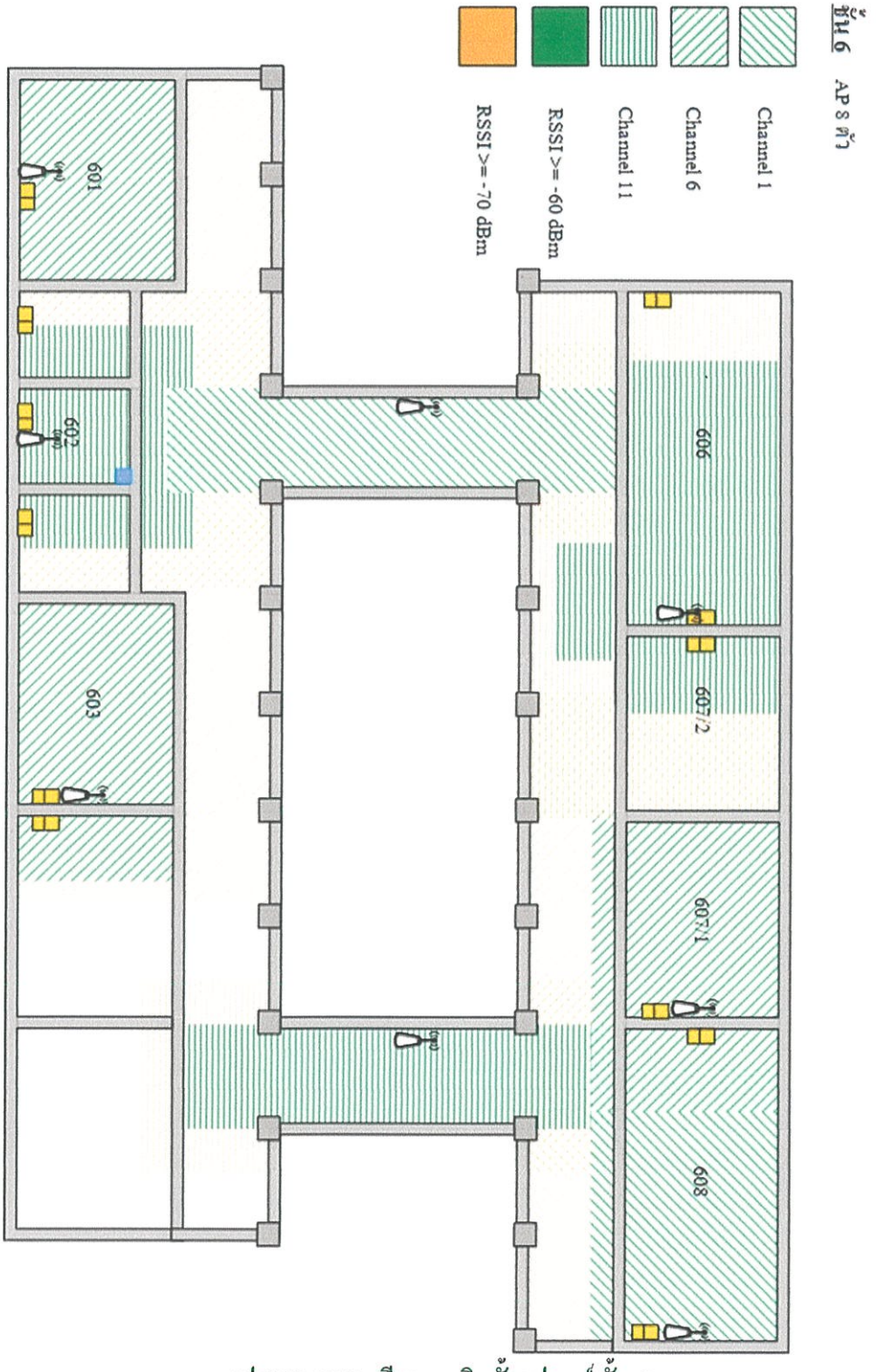
จะเป็นรายละเอียดของการติดตั้ง Access Point ในแต่ละชั้นจะมีจำนวน Access Point ที่ต้องติดตั้งไม่เท่ากัน อันเนื่องมาจากแผนผังของห้องในแต่ละชั้นไม่เหมือนกัน โดยจากการทดลองจะพบว่ากำแพงห้องส่งผลโดยตรงต่อการลดระดับลงของค่า RSSI ส่งผลให้ในแต่ละชั้นจะติดตั้งในจำนวนที่ไม่เท่ากันการออกแบบจุดติดตั้งจะคำนึงในเรื่องของ Non-Overlapping Channel ดังที่ได้กล่าวมาแล้วในหัวข้อก่อนหน้านี้ โดยพื้นที่สีเขียวและสีส้มนั้นแสดงถึงค่าของ RSSI ที่วัดได้จาก Access Point โดยมีค่า RSSI ดังที่ได้กล่าวมาแล้วในหัวข้อก่อนหน้า โดยจะมีการกำหนดจุดติดตั้ง Access Point สำหรับชั้น 5, 6, 7, 8 และ 9 ดังต่อไปนี้

3.2.3.1 รายละเอียดการติดตั้งอุปกรณ์ ชั้น 5



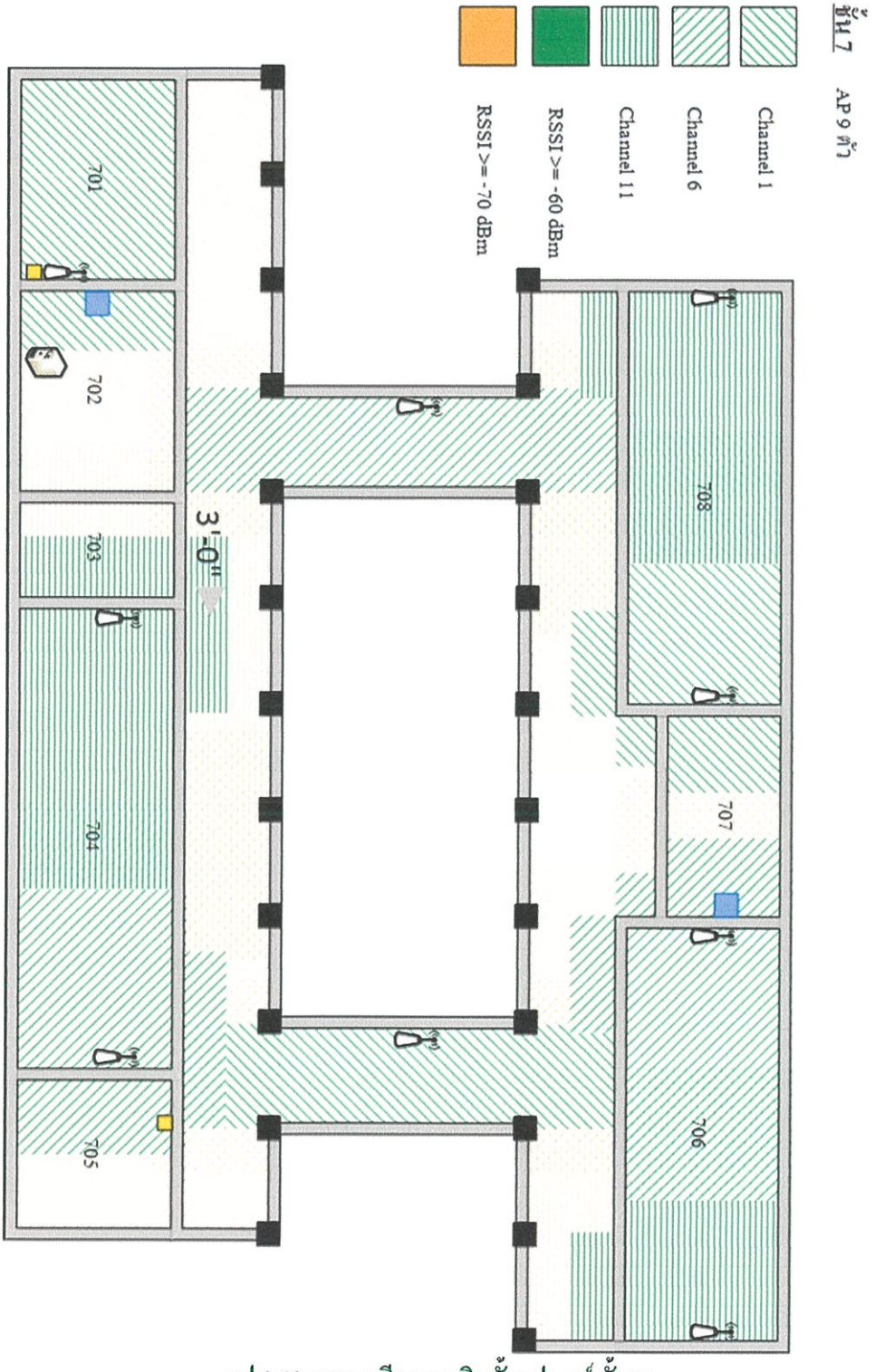
รูป 3.10 รายละเอียดการติดตั้งอุปกรณ์ ชั้น 5

3.2.3.2 รายละเอียดการติดตั้งอุปกรณ์ ชั้น 6



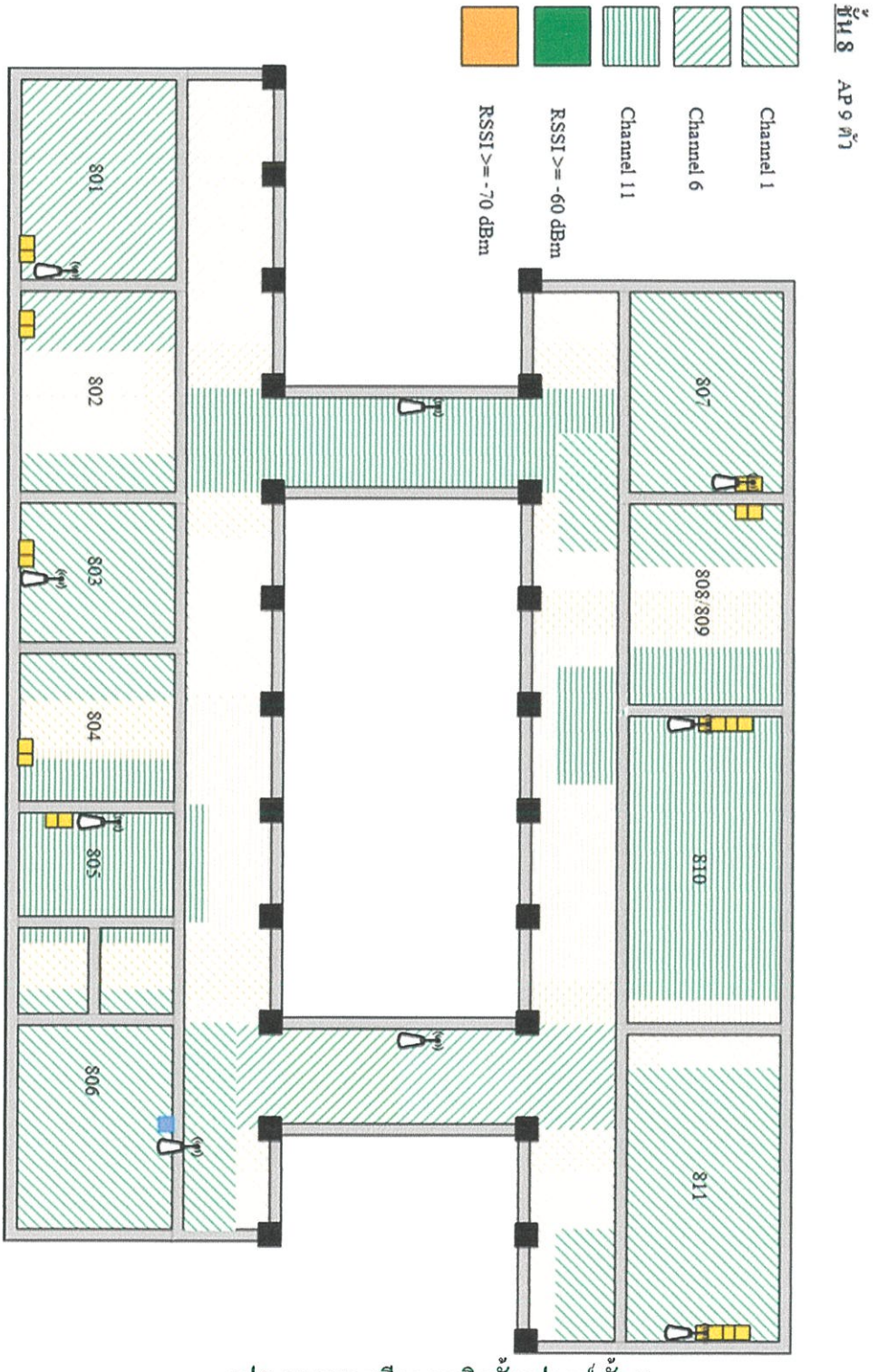
รูป 3.11 รายละเอียดการติดตั้งอุปกรณ์ ชั้น 6

3.2.3.3 รายละเอียดการติดตั้งอุปกรณ์ ชั้น 7



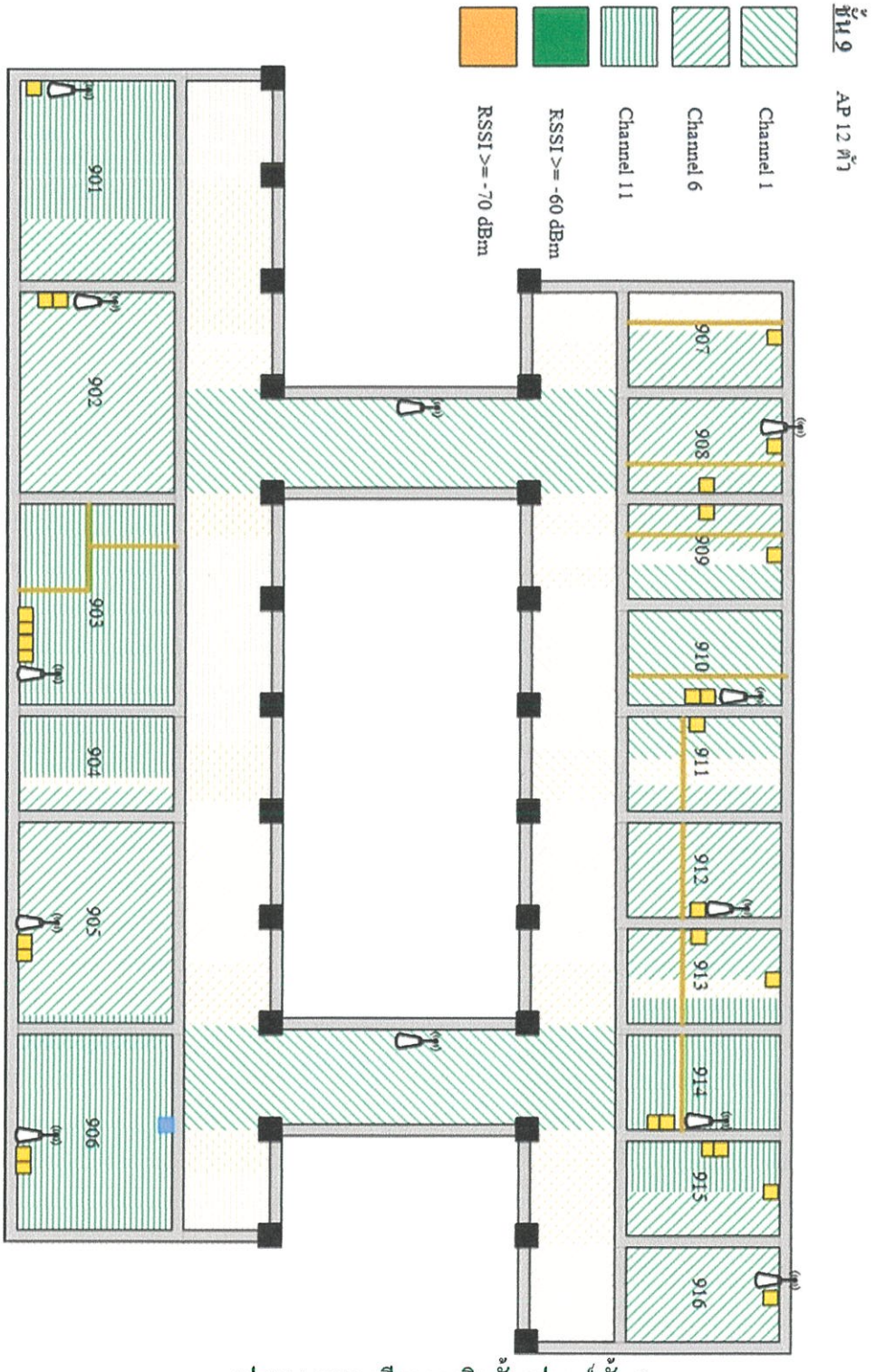
รูป 3.12 รายละเอียดการติดตั้งอุปกรณ์ ชั้น 7

3.2.3.4 รายละเอียดการติดตั้งอุปกรณ์ ชั้น 8



รูป 3.13 รายละเอียดการติดตั้งอุปกรณ์ ชั้น 8

3.2.3.5 รายละเอียดการติดตั้งอุปกรณ์ ชั้น 9



รูป 3.14 รายละเอียดการติดตั้งอุปกรณ์ ชั้น 9

3.3 ส่วนฐานข้อมูล

ส่วนนี้จะเป็นส่วนระบบฐานข้อมูลที่ใช้บันทึกข้อมูลและประวัติการใช้งานของผู้ใช้ซึ่งจะใช้ MySQL เป็น DBMS ในการบริหารจัดการฐานข้อมูลนี้

3.3.1 การติดต่อกับฐานข้อมูลของภาควิชา

ในส่วนนี้จะเป็นการติดต่อระหว่างฐานข้อมูลของระบบกับฐานข้อมูลของภาควิชาผ่านทาง Web Service โดยจะทำการร้องขอไปยัง Web Service เพื่อให้ส่งตารางข้อมูลของผู้ใช้งานจากฐานข้อมูลของภาควิชาวิศวกรรมคอมพิวเตอร์มาเก็บไว้ยังตาราง raduser ของฐานข้อมูลระบบ

3.3.2 ตารางที่มีภายในฐานข้อมูล

ระบบเครือข่ายไร้สายและการยืนยันตนสำหรับภาควิชาวิศวกรรมคอมพิวเตอร์ใช้ MySQL ทำหน้าที่เป็น DBMS และใช้ phpMyAdmin เพื่อช่วยในการบริหารจัดการฐานข้อมูล MySQL โดยภายในฐานข้อมูลมีตารางที่สร้างขึ้นมาใช้งานทั้งหมด 4 ตารางดังนี้

ตาราง 3.3 ตาราง raduser

Entity	raduser		
Key	Attribute	Data Type	Description
PK	username	Varchar	ชื่อบัญชีของผู้ใช้
	password	Varchar	รหัสผ่านที่ถูกเข้ารหัส
	t_Name	Varchar	ชื่อภาษาไทย
	e_Name	Varchar	ชื่อภาษาอังกฤษ
	t_SurName	Varchar	นามสกุลภาษาไทย
	Group	Varchar	นามสกุลภาษาอังกฤษ
	ID	Varchar	รหัสประจำตัวประชาชน
	EMail	Varchar	อีเมลล์
	TelNO	Varchar	โทรศัพท์มือถือ
	Address	Varchar	ที่อยู่
	AddBy	Varchar	บุคคลที่ทำการเพิ่มบัญชีนี้ลงฐานข้อมูล
	Status	Varchar	สถานะการใช้งานระบบ
	dataUse	Varchar	ปริมาณข้อมูลที่ใช้
	hourUse	Varchar	จำนวนเวลาที่ใช้ระบบ
	StartDate	Date	วันที่สามารถเริ่มใช้งาน
	StopDate	Date	วันที่สามารถใช้งานเป็นวันสุดท้าย

ตาราง 3.4 ตาราง radacct

Entity	radacct		
Key	Attribute	Data Type	Description
PK	radacctid	Bigint	ID ของข้อมูลaccounting
	acctsessionid	Varchar	หมายเลข session id
	acctuniqueid	Varchar	หมายเลข ID เฉพาะของข้อมูล
	username	Varchar	ชื่อบัญชีของผู้ใช้งาน
	nasipaddress	Varchar	IP Address ของ Authenticator
	acctstarttime	Datetime	เวลาที่เริ่ม session ใช้งาน
	acctstoptime	Datetime	เวลาที่หยุด session ใช้งาน
	acctsessiontime	Int	เวลาที่ใช้ใน session นั้น
	acctinputoctets	Bigint	จำนวนไบต์ข้อมูลที่ส่งเข้า
	acctoutputoctets	Bigint	จำนวนไบต์ข้อมูลที่ส่งออก
	calledstationid	Varchar	MAC Address และ SSID ของ Authenticator
	callingstationid	Varchar	MAC Address ของเครื่องผู้ใช้งาน
	acctterminatecause	Varchar	สาเหตุในการหยุดการเชื่อมต่อ

ตาราง 3.5 ตาราง radcheck

Entity	radcheck		
Key	Attribute	Data Type	Description
PK	id	Int	ID ของชื่อบัญชีผู้ใช้
	username	Varchar	ชื่อบัญชีผู้ใช้งาน
	attribute	Varchar	เป็นค่าที่บอกรูปแบบการเข้ารหัส
	op	Char	มีค่าเป็น :=
	value	Varchar	เป็นรหัสผ่านของบัญชีผู้ใช้

ตาราง 3.6 ตาราง radpostauthen

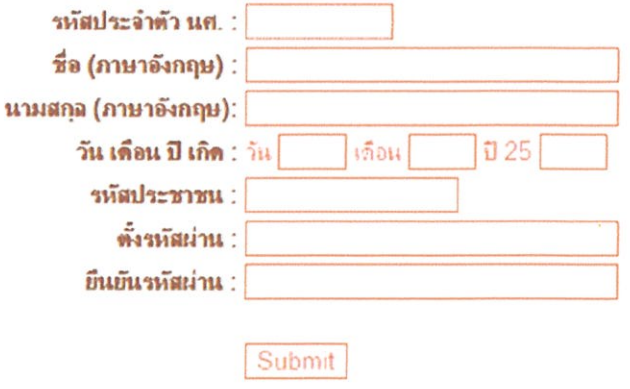
Entity	radpostauthen		
Key	Attribute	Data Type	Description
PK	id	Int	ID ของข้อมูลการเข้าใช้งาน
	username	Varchar	ชื่อบัญชีผู้ใช้
	reply	Varchar	ข้อมูลผลการตอบกลับของผู้ใช้
	authdate	Timestamp	วันและเวลาที่ผู้ใช้เข้าใช้เข้าใช้งาน

3.4 ส่วนของเว็บไซต์

ในส่วนนี้จะเป็นการอธิบายการทำงานในส่วนต่างๆ ของเว็บไซต์ เช่น เงื่อนไขในการใช้งานเว็บไซต์

3.4.1 เงื่อนไขการเข้าใช้งานระบบเว็บไซต์

ในการเข้าใช้งานเว็บไซต์นั้นผู้ที่จะเข้าใช้งานจะต้องมีบัญชีสำหรับใช้งานเว็บไซต์ http://www.ce.kmitl.ac.th ถ้ายังไม่มีบัญชีใช้งานผู้ใช้จะต้องทำการเข้าไปลงทะเบียนที่ http://www.ce.kmitl.ac.th/regis.php ดังแสดงในรูป 3.15 ก่อน



รูป 3.15 หน้าต่างการลงทะเบียนใช้งานเว็บไซต์ภาควิชา

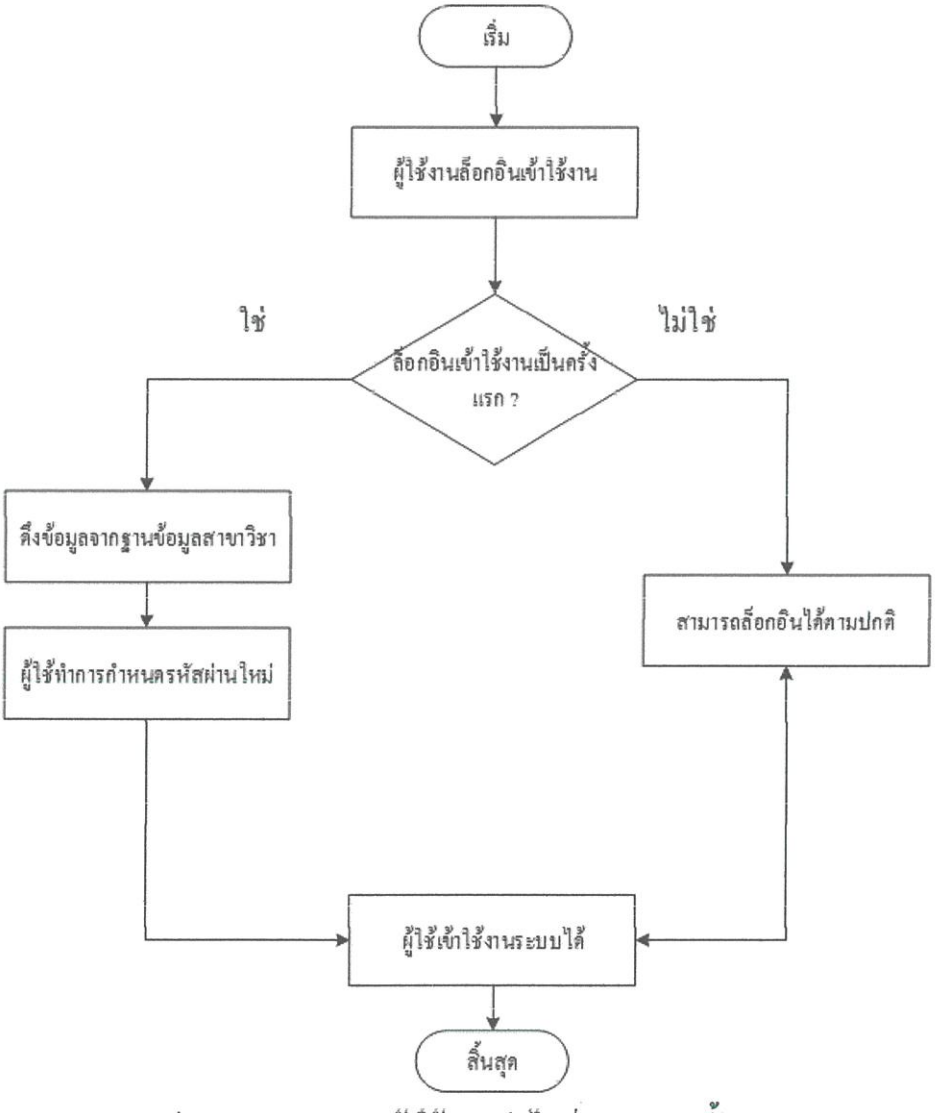
3.4.2 การออกแบบเว็บไซต์

ในการออกแบบเว็บไซต์นั้นส่วนการแสดงผล (Front-End) นั้นจะใช้ Bootstrap ในการพัฒนาซึ่ง Bootstrap นั้นเป็น Framework ที่ช่วยให้การพัฒนาเว็บไซต์นั่นง่ายขึ้น และมีความสวยงาม โดยได้เลือกใช้ธีมของ Bootstrap ที่มีชื่อว่า AdminLTE และในส่วนของการประมวลผล(Back-End)

นั้นได้ใช้ Codeigniter เป็นเครื่องมือในการพัฒนาซึ่ง Codeigniter เป็น PHP Framework ที่รองรับการพัฒนาเว็บไซต์แบบ MVC

3.4.3 กระบวนการยืนยันเข้าใช้งานครั้งแรก

ในกระบวนการยืนยันเพื่อเข้าใช้งานนั้นหากผู้เข้าใช้งานยังไม่เคยใช้งานระบบเครือข่ายไร้สายและยังไม่เคยทำการ Login เข้าใช้งานหน้าเว็บไซต์ต้องทำการ Login ที่หน้าเว็บไซต์ เมื่อ Login แล้วทำการตั้งรหัสผ่านใหม่แล้ว จะสามารถใช้งานบัญชีผู้ใช้งานและรหัสผ่านที่กำหนดขึ้นมาใหม่เพื่อเชื่อมต่อระบบเครือข่ายไร้สายได้ อีกทั้งยังทำให้สามารถ Login เข้าใช้งานเว็บไซต์ได้ กระบวนการทำงานดังกล่าวเป็นไปตามแผนภาพดังรูป 3.16



รูป 3.16 กระบวนการเข้าใช้งานเว็บไซต์และระบบครั้งแรก

3.4.4 ส่วนจำกัดปริมาณการใช้งานผู้ใช้งาน

ส่วนนี้จะมีการทำงานคือจะตรวจสอบปริมาณการใช้งานโดยจะใช้ PHP script ในการตรวจสอบว่าปริมาณการใช้งานของผู้ใช้นั้นเกินปริมาณที่กำหนดหรือไม่ ถ้าหากมีการใช้งานเกินปริมาณที่กำหนดผู้ใช้จะไม่สามารถเข้าใช้งานระบบเครือข่ายได้โดย PHP script ที่ใช้ในการตรวจสอบนั้นตั้งชื่อว่า limitchecking.php ซึ่งจะถูกกระทำทุกๆ 1 นาที โดยการใช้เซอร์วิส crontab ของ Ubuntu เมื่อผู้ใช้งานถูกจำกัดการใช้งานแล้ว เมื่อเริ่มวันใหม่ผู้ใช้งานก็จะสามารถกลับมาใช้งานได้อีกโดยกระบวนการทำให้ผู้ใช้งานที่ใช้งานเกินปริมาณที่กำหนดให้สามารถกลับมาใช้งานได้ใหม่นั้นจะกระทำทุกเที่ยงคืนโดยตั้งค่าในเซอร์วิส crontab ดังรูป 3.17

```
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
*/1 * * * * php /var/phpscript/limitchecking.php
0 0 * * * php /var/phpscript/setperday.php
```

รูป 3.17 การตั้งค่าในเซอร์วิส crontab

3.4.5 ส่วนการจัดการต่างๆสำหรับ Admin

เป็นส่วนที่จะอยู่ในแถบ Management และ Statistic ซึ่งผู้ที่จะใช้งานส่วนนี้ได้จะเป็น Admin เท่านั้น โดยจะประกอบไปด้วยส่วนต่างๆดังนี้

1) ส่วนในการกำหนดการจำกัดปริมาณการใช้งานให้กับ Student ส่วนนี้จะสามารถทำการกำหนดการจำกัดปริมาณการใช้งานของผู้ใช้ โดยสามารถเลือกได้ว่าจะทำการจำกัดข้อมูลการใช้งาน จำกัดเวลาการใช้งาน หรือเลือกจะไม่จำกัด โดยกลุ่มผู้ใช้งานที่จะถูกจำกัดได้แก่ กลุ่ม Student
2) ส่วนตรวจสอบผู้ใช้งานที่กำลังเข้าใช้งานเครือข่าย ส่วนนี้จะใช้ข้อมูลจากตาราง radacct ในการตรวจสอบว่ามีผู้ใช้คนใดกำลังใช้งานระบบอยู่ในขณะนั้นโดยจะแสดง IP Address ของ Access Point ที่ทำการเชื่อมต่อ รวมถึงแสดง MAC Address ของอุปกรณ์ที่ทำการเข้าใช้งานระบบ
3) ส่วนตรวจสอบการ Login เข้าใช้งานระบบครั้งล่าสุด โดยในส่วนนี้จะใช้ข้อมูลจากตาราง radpostauthen ในการตรวจสอบการเข้าสู่ระบบของผู้ใช้งานในระบบครั้งล่าสุด
4) ส่วนแสดงสถิติการใช้งาน ในส่วนนี้จะแสดงถึงสถิติข้อมูลต่างๆโดยมีแถบให้เลือก 4 แถบ ดังนี้

4.1) แถบแสดงการใช้งานทั้งหมดในแต่ละวัน โดยสามารถเลือกได้ว่าจะแสดงจำนวนผู้ใช้งานระบบทั้งหมด หรือจำนวนปริมาณข้อมูลที่มีการใช้งานทั้งหมดในแต่ละวัน

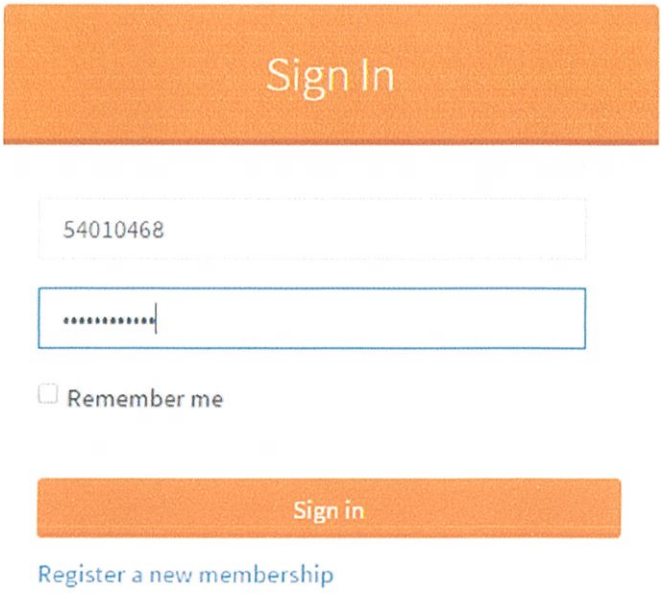
4.2) แถบแสดงการใช้งานเปรียบเทียบในหน่วยวัน โดยสามารถเลือกแสดงจำนวนผู้เข้าใช้งานระบบหรือปริมาณข้อมูลที่มีการใช้งานเปรียบเทียบเป็นรายวัน

4.3) แถบแสดงการใช้งานเปรียบเทียบในหน่วยชั่วโมง โดยสามารถเลือกแสดงจำนวนผู้เข้าใช้งานระบบหรือปริมาณข้อมูลที่มีการใช้งานเปรียบเทียบเป็นรายชั่วโมง

4.4) ผู้ดูแลระบบสามารถดาวน์โหลด Log แสดงการเข้าใช้งานระบบได้

3.4.6 User Interface ของเว็บไซต์

เมื่อเข้าใช้งานเว็บไซต์จะปรากฏหน้าต่างสำหรับการเข้าสู่ระบบ ซึ่งการเข้าสู่ระบบจะใช้บัญชีและรหัสผ่านของทางเว็บไซต์ภาควิชา ดังรูป 3.18 ซึ่งถ้าหากไม่มีบัญชีใช้งานต้องทำการสมัครสมาชิกที่เว็บไซต์ของทางภาควิชาก่อน

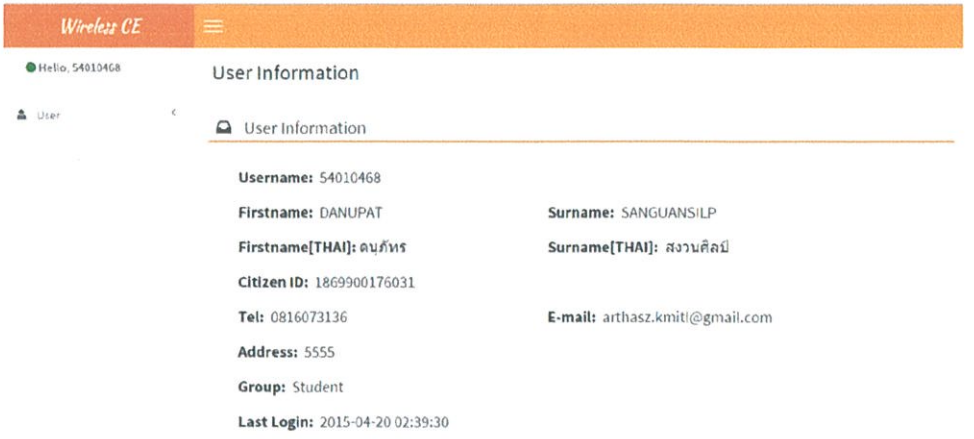


รูป 3.18 หน้าต่างในการ Login เข้าใช้งานเว็บไซต์

3.4.6.1 User Interface สำหรับ Student

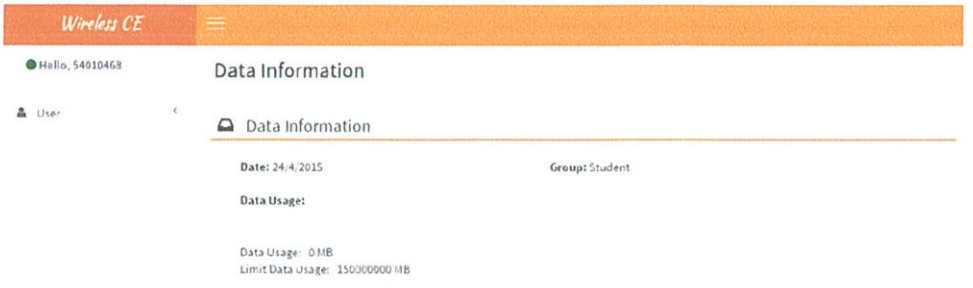
เมื่อทำการเข้าสู่ระบบแล้ว ถ้าผู้ใช้งานมีสิทธิในการใช้งานเป็น Student จะแสดงผลหน้า User Interface ที่มีแถบ User ทางด้านซ้ายซึ่งเมื่อกดเข้าไปจะมีให้เลือก 2 แถบ คือ

1) User Information ซึ่งเป็นส่วนของการแสดงข้อมูลส่วนตัวของผู้ใช้งาน ดังแสดงในรูป 3.19



รูป 3.19 ข้อมูลส่วนตัวของผู้ใช้งาน

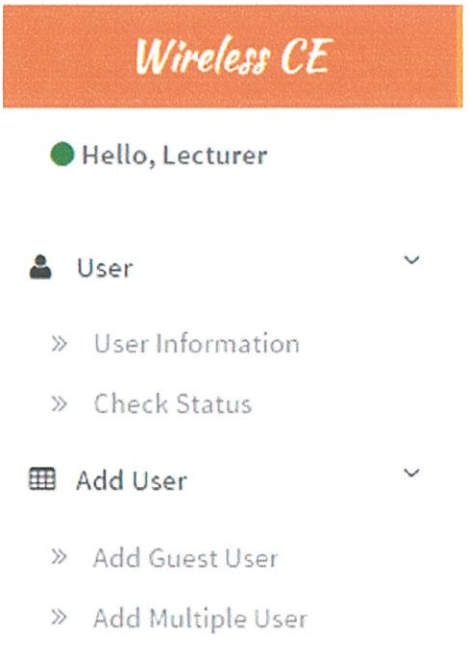
2) Check status ซึ่งใช้ในการตรวจสอบปริมาณข้อมูลของผู้ใช้ที่มีการใช้งาน ดังรูป 3.20 ซึ่งปริมาณข้อมูลที่มีการแสดงนั้นจะขึ้นอยู่กับการจำกัดปริมาณการใช้งานที่กำหนดโดย Admin



รูป 3.20 ปริมาณข้อมูลหรือเวลาที่ใช้งาน

3.4.6.2 User Interface สำหรับ Lecturer

เมื่อทำการเข้าสู่ระบบแล้ว ถ้าผู้ใช้งานมีสิทธิในการใช้งานเป็น Lecturer จะแสดงหน้า User Interface ที่มีแถบเมนู User ซึ่งมีการแสดงผลในรูปแบบเดียวกับ Student เพียงแต่ในหน้า Data Information นั้นจะไม่มีการจำกัดปริมาณการใช้งานแต่จะแค่แสดงปริมาณการใช้งานเท่านั้น ส่วนแถบที่เพิ่มเติมจาก Student คือแถบ Add User ดังแสดงในรูป 3.21 ซึ่งเมื่อทำการเลือกจะมีแถบให้เลือกอีก 2 แถบ คือ



รูป 3.21 แถบเมนูที่สามารถใช้งานได้ของ Lecturer

1) Add Guest User ใช้ในการเพิ่มผู้ใช้งานที่เป็น Guest ดังแสดงในรูป 3.22

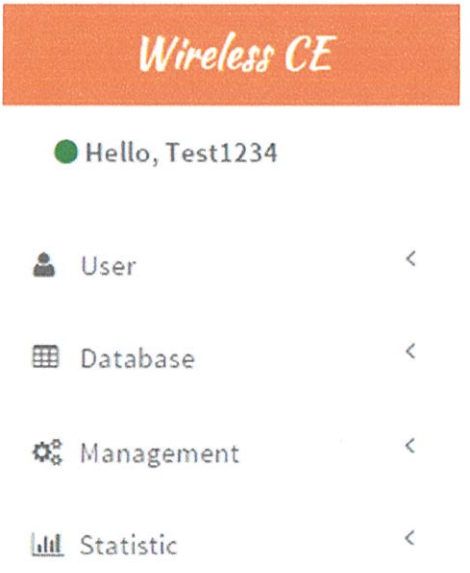
รูป 3.22 รูปหน้าต่างการเพิ่มผู้ใช้งานที่เป็น Guest

2) Add Multiple User ใช้ในการอัพโหลดไฟล์ .csv เพื่อเพิ่ม Guest User ครั้งละหลายๆ คนดังแสดงในรูป 3.23

รูป 3.23 รูปหน้าต่างการเพิ่มผู้ใช้งานครั้งละหลายๆคน

3.4.6.3 User Interface สำหรับ Admin

เมื่อทำการเข้าสู่ระบบแล้ว ถ้าผู้ใช้งานมีสิทธิในการใช้งานเป็น Admin จะแสดงหน้า User Interface ที่มีแถบ User ซึ่งมีการแสดงผลในรูปแบบเดียวกับ Lecturer ส่วนแถบที่มีการเพิ่มขึ้นมาจะมี 3 แถบ ดังรูป 3.24



รูป 3.24 แถบเมนูสำหรับ Admin

1) Database ซึ่งภายในจะมีแถบย่อย Update User ซึ่งเมื่อมีการเลือกจะทำการอัพเดทข้อมูลระหว่างฐานข้อมูลผู้ใช้งานของระบบกับฐานข้อมูลของเว็บไซต์ภาควิชาวิศวกรรมคอมพิวเตอร์ดังแสดงให้เห็นในรูป 3.25

รูป 3.25 หน้าต่าง Update User

2) Management ซึ่งจะมีแถบย่อยภายในอีก 3 แถบ ดังนี้

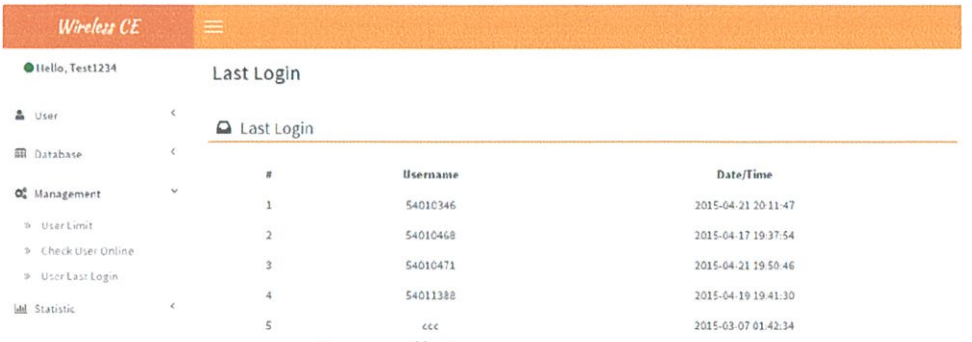
2.1) User Limit เป็นแถบสำหรับการจำกัดการใช้งานของ Student โดยสามารถเลือกการจำกัดได้ 3 รูปแบบคือ Data Limit , Time Limit และ No Limit ดังรูป 3.26

รูป 3.26 หน้าต่างจำกัดการใช้งานของ student

2.2) Check User Online เป็นแถบที่ใช้แสดงผู้ใช้งานที่กำลังเข้าใช้งานเครือข่ายอยู่ในขณะนั้น ดังแสดงในรูป 3.27

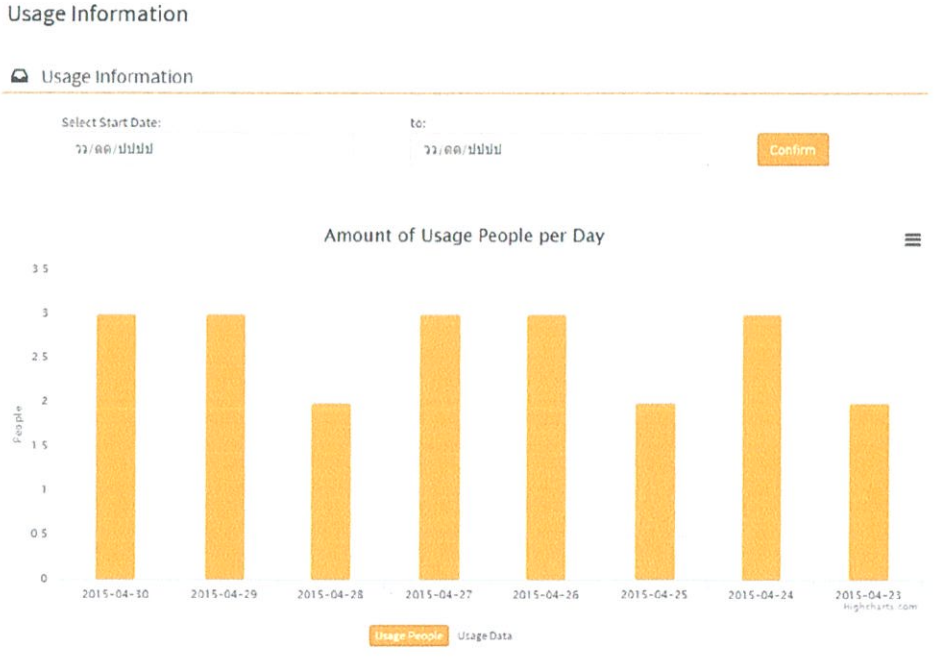
รูป 3.27 หน้าต่าง Check User Online

2.3) User Last Login เป็นแถบที่แสดงข้อมูลการเข้าใช้งานในระบบครั้งล่าสุดของ User ดังรูป 3.28

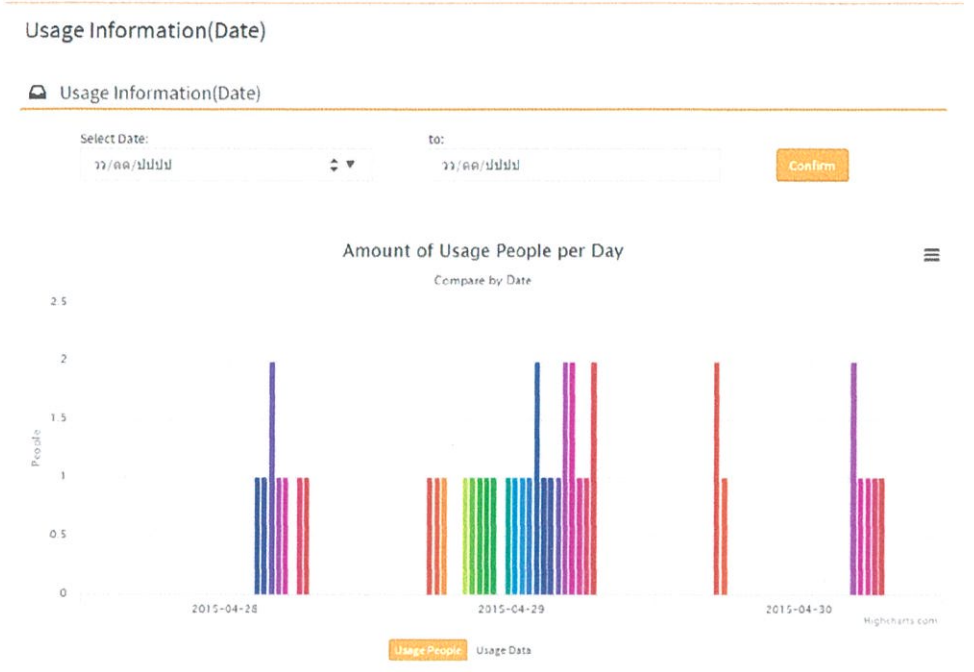


รูป 3.28 หน้าต่าง User Last Login

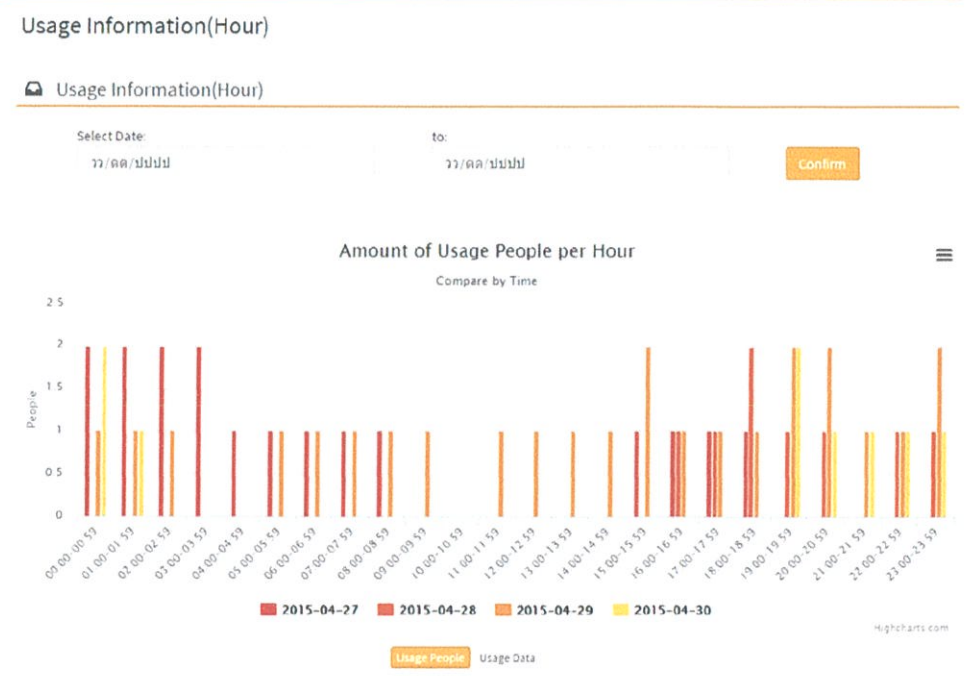
3) Statistic เป็นหน้าต่างที่แสดงสถิติการใช้งานย้อนหลัง ดังแสดงในรูป 3.29 รูป 3.30 และ รูป 3.31



รูป 3.29 หน้าต่าง Usage Statistic



รูป 3.30 หน้าต่าง Usage Statistic(Date)



รูป 3.31 หน้าต่าง Usage Statistic(Time)

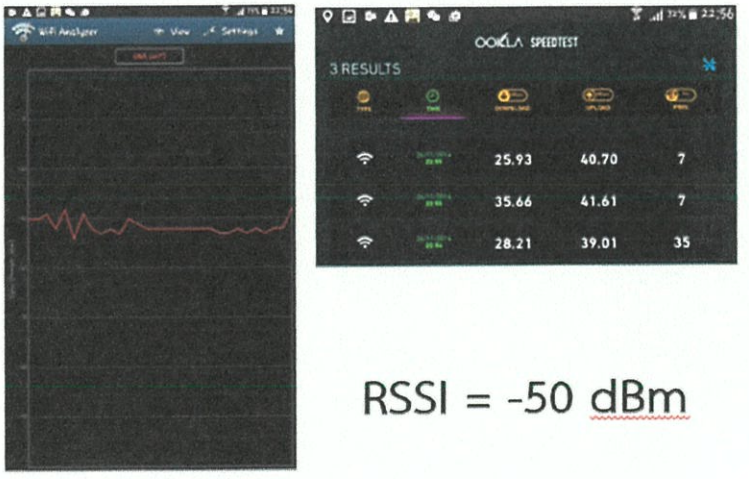
บทที่ 4

การทดลองและผลการทดลอง

4.1 ทดลองหาค่า RSSI ที่เหมาะสม

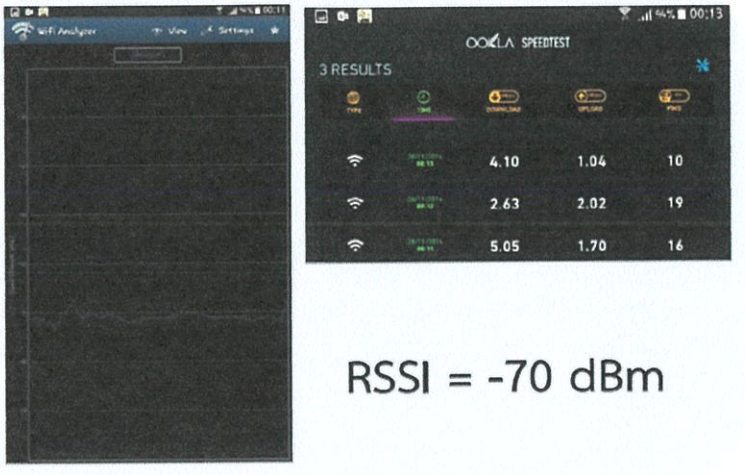
ในการทดลองนี้ จะเป็นการทดสอบว่า เมื่อทำการติดตั้ง Access Point ให้สามารถใช้งานอินเตอร์เน็ตได้ จากนั้นใช้แอพลิเคชัน Wi-Fi Analyzer สำหรับหาจุดที่มีค่าสัญญาณ RSSI โดยกระบวนการในหาจุดที่มีค่าสัญญาณระดับนี้ จะต้องรอให้แน่ใจว่า สัญญาณคงที่แล้วจึงทำการวัดความเร็วในการใช้งานอินเตอร์เน็ต ค่า RSSI ที่จะทำการทดลองมีจำนวน 3 ค่าดังนี้

1) ค่า RSSI = -50 dBm จุดนี้เป็นจุดที่อุปกรณ์มีระยะห่างจาก Access Point ไม่มาก เป็นระยะสำหรับการใช้งานโดยปกติทั่วไป ซึ่งเมื่อทำการวัดความเร็วของสัญญาณอินเตอร์เน็ต โดยใช้แอพพลิเคชัน Speedtest จำนวน 3 ครั้งในเวลาใกล้เคียงกัน ซึ่งมีค่า Upload, Download และค่า Ping ดังแสดงในรูป 4.1



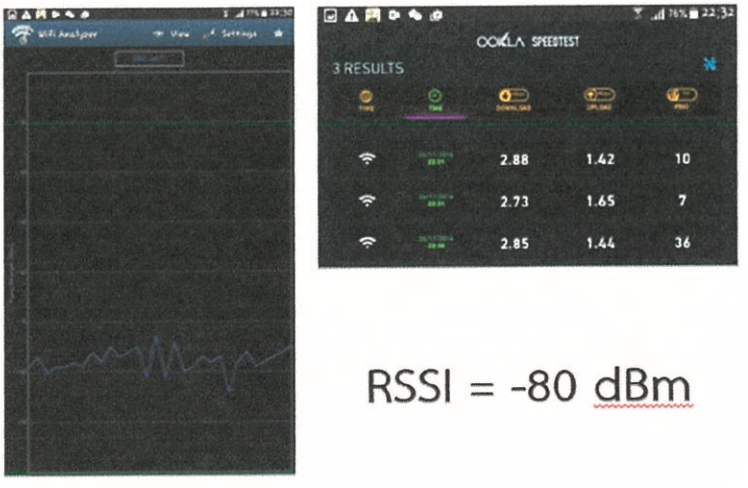
รูป 4.1 ค่า Upload , Download และค่า Ping ที่ค่า RSSI = - 50 dBm

2) ค่า RSSI = -70 dBm จุดนี้เป็นจุดที่อุปกรณ์มีระยะห่างจาก Access Point ระดับหนึ่ง มีกำแพงเป็นสิ่งกีดขวางระหว่างอุปกรณ์ผู้ใช้งานกับ Access Point และมีค่า RSSI ที่ยังไม่ต่ำกว่าค่าที่ได้ออกแบบไว้ในส่วนของการออกแบบ ซึ่งเมื่อทำการวัดความเร็วของสัญญาณอินเตอร์เน็ต โดยใช้แอพพลิเคชัน Speedtest จำนวน3ครั้งในเวลาใกล้เคียงกัน ซึ่งมีค่า Upload, Download และค่า Ping ดังแสดงในรูป 4.2



รูป 4.2 ค่า Upload , Download และค่า Ping ที่ค่า RSSI = - 70 dBm

3) ค่า RSSI = -80 dBm จุดนี้เป็นจุดที่อุปกรณ์มีระยะห่างจาก Access Point มาก อีกทั้งยังมีกำแพงเป็นสิ่งกีดขวางระหว่างอุปกรณ์ผู้ใช้งานกับ Access Point และเป็นค่า RSSI ที่ต่ำกว่าค่าที่ได้ออกแบบไว้ ซึ่งเมื่อทำการวัดความเร็วของสัญญาณอินเตอร์เน็ต โดยใช้แอพพลิเคชัน Speedtest จำนวน 3 ครั้งในเวลาใกล้เคียงกัน ซึ่งมีค่า Upload, Download และค่า Ping ดังแสดงในรูป 4.3



รูป 4.3 ค่า Upload , Download และค่า Ping ที่ค่า RSSI = - 80 dBm

ดังนั้นจากการทดสอบค่าสัญญาณที่มีค่า RSSI ต่างๆ สามารถสรุปข้อมูลได้ดังตาราง 4.1

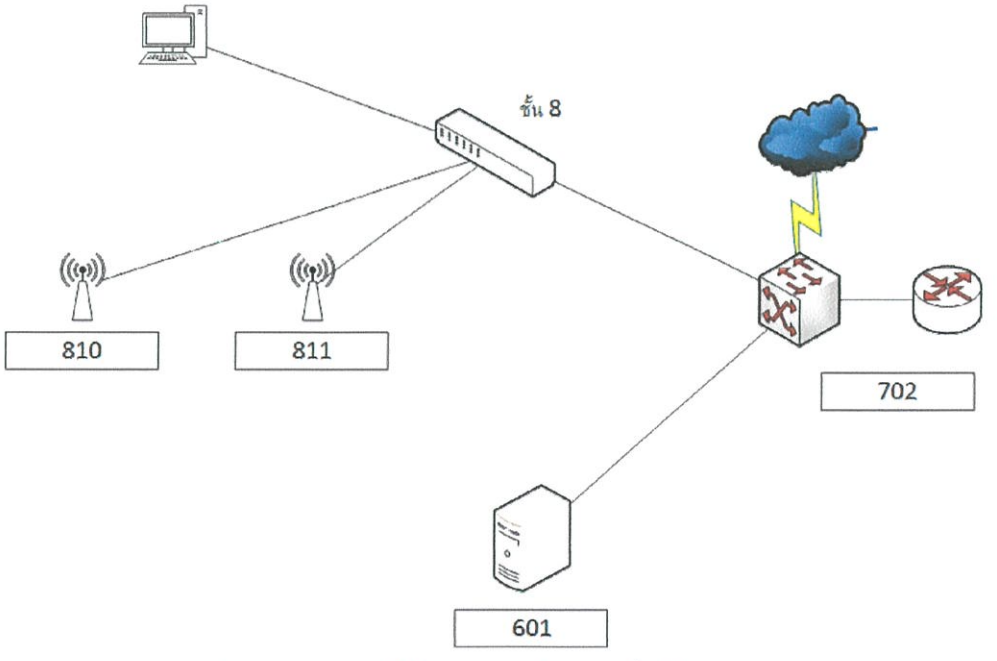
ตาราง 4.1 สรุปความเร็วในการใช้งานเฉลี่ยของแต่ละค่า RSSI

RSSI	Download	Upload	Ping
-50 dBm	29.9	40.4	16.3
-70 dBm	3.9	1.5	15
-80 dBm	2.8	1.5	17.6

4.2 ทดลองใช้งานร่วมกับเครือข่ายของภาควิชา

4.2.1 ติดตั้งและตั้งค่าอุปกรณ์

การทดลองนี้จะเป็นการตั้งค่าให้แก่อุปกรณ์แล้วนำอุปกรณ์ไปติดตั้งยังจุดต่างๆ ภายในภาควิชา จากรูป 4.4 จะเห็นว่า Core Switch ของภาควิชา ซึ่งมีการติดตั้งอยู่แล้ว ณ ห้อง 702 ทำหน้าที่เป็นตัวกลางในการติดต่อระหว่างระบบกับอินเตอร์เน็ตภายนอก และ Router ที่จะทำหน้าที่ NAT และ DHCP ให้กับระบบ โดยในระบบจะทดลองใช้งานที่ชั้น 8 ซึ่งจะติดตั้ง Access Point ที่ชั้น 8 ในห้อง 810 และห้อง 811 โดยต้องตั้งค่า Switch ที่ชั้น 8 ให้รองรับ VLAN ของระบบและรองรับ VLAN เดิมของภาควิชาที่มีอยู่แล้ว ส่วน RADIUS Server นั้นตั้งอยู่ที่ห้อง 601



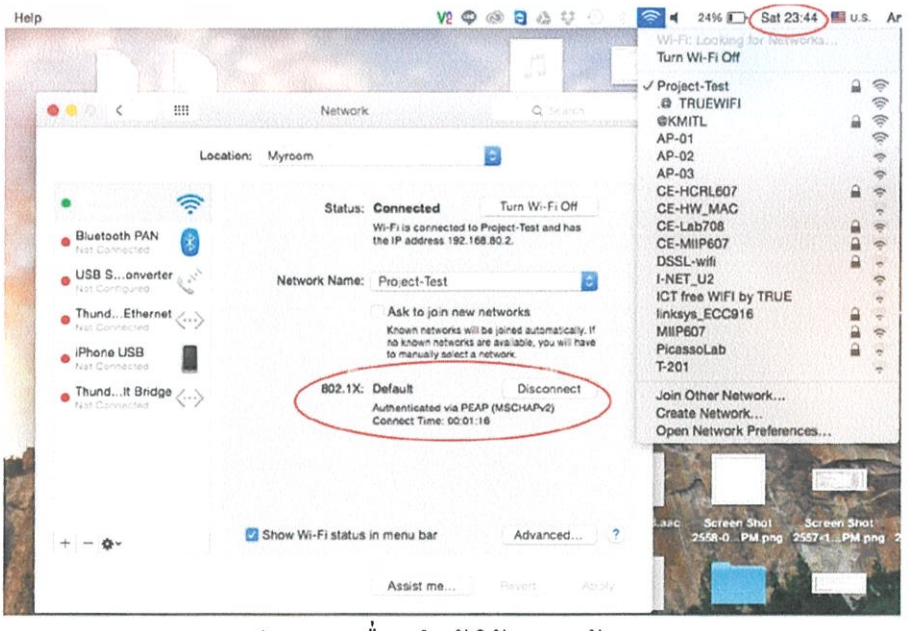
รูป 4.4 การทดลองใช้งานระบบร่วมกับเครือข่ายภาควิชา

ผลจากการทดลองพบว่า เราสามารถเข้าใช้งานระบบได้ โดยที่ระบบเครือข่าย LAN เดิมก็ยังคงสามารถใช้งานได้ เนื่องจากเราได้ทำการตั้งค่า VLAN ทั้งที่ Switch ของชั้น 8 และทำ Trunk Port ที่ Core Switch ของภาควิชา

4.2.2 ทดลองเปลี่ยนการเชื่อมต่อของ Access Point

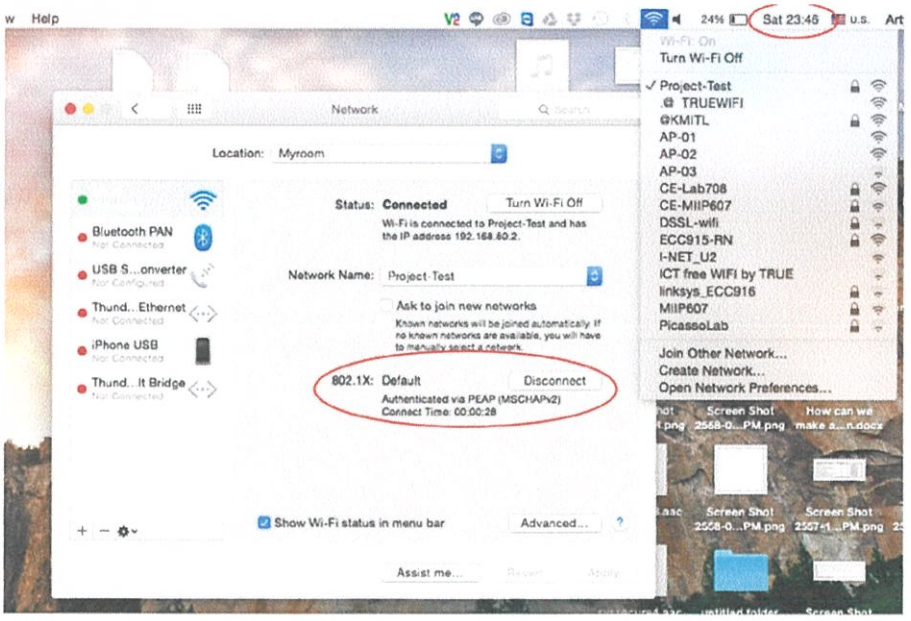
ในการทดลองนี้เราจะใช้คอมพิวเตอร์ทำการเชื่อมต่อเข้าใช้งานเครือข่าย ในการทดลองนี้เราได้ทำการติดตั้ง Access Point จำนวน 2 ตัว ภายในห้อง 810 และห้อง 811 ที่ตำแหน่งเดียวกับที่ได้ทำการออกแบบไว้ในบทที่ 3 โดยที่ Access Point ทั้งสองตัวนั้นจะใช้ SSID เป็นชื่อเดียวกัน คือ Project-Test

โดยการทำการทดลองจะเริ่มจากเข้าใช้งาน Access Point ที่ห้อง 810 เมื่อเข้าใช้งานแล้วจะมีลักษณะดังรูป 4.5



รูป 4.5 การเชื่อมต่อเข้าใช้งาน ณ ห้อง 810

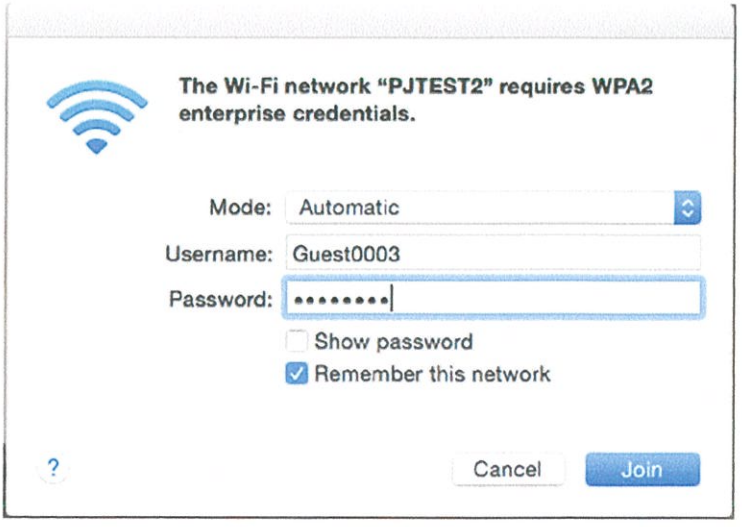
หลังจากเชื่อมต่อที่ห้อง 810 แล้วทำการถืออุปกรณ์นั้นเดินออกมาจากห้อง 810 จากนั้นเดินตามระเบียงทางเดินไปทางห้อง 811 แล้วเข้าไปยังห้อง 811 เมื่อเข้าไปยังห้อง 811 แล้ว หน้าต่างการเชื่อมต่อจะแสดงดังรูป 4.6 ตรงจุดนี้สังเกตว่าในรูป 4.5 ในส่วนของ Connection Time นั้นได้มีการเชื่อมต่อมาเป็นระยะเวลาหนึ่งแล้ว และเมื่อเราเดินไปยังห้อง 811 Connection Time ได้เริ่มนับเวลาใหม่แสดงว่าได้มีการเชื่อมต่อเข้าที่ Access Point ตัวใหม่ ที่ห้อง 811 เป็นที่เรียบร้อยแล้ว



รูป 4.6 การเชื่อมต่อเข้าใช้งาน ณ ห้อง 811

4.3 ทดลองเข้าใช้งานในฐานะ Guest

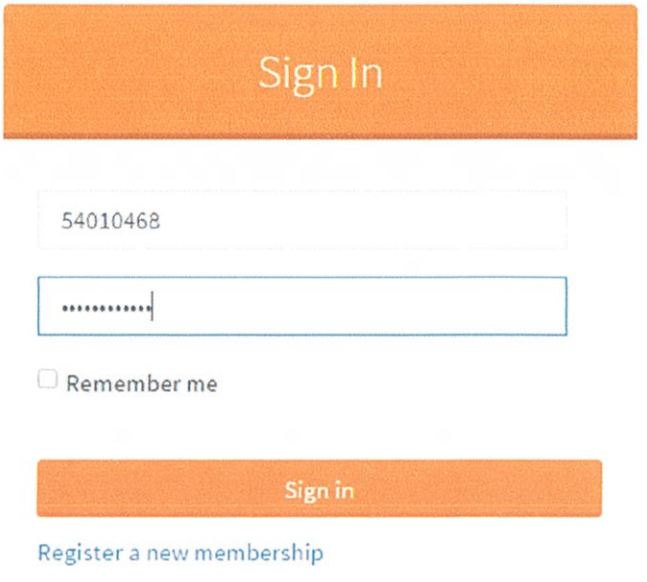
Guest จะสามารถเข้าใช้งานในส่วนของระบบเครือข่ายไร้สายได้เท่านั้นไม่สามารถเข้าใช้งานในส่วนของเว็บไซต์ได้ โดยที่ Guest จะต้องมีบัญชีผู้ใช้งานซึ่งถูกเพิ่มโดย Lecturer เท่านั้นและ Guest จะสามารถใช้งานระบบเครือข่ายได้จนกว่าจะครบกำหนดวันหมดอายุของบัญชีผู้ใช้งานตามที่ Lecturer ได้กำหนดไว้ตอนทำการสร้างบัญชีผู้ใช้งาน ดังในรูป 4.7 ซึ่งในที่นี้เราได้ทำการสร้างบัญชีใช้งานชั่วคราวสำหรับ Guest มาแล้ว



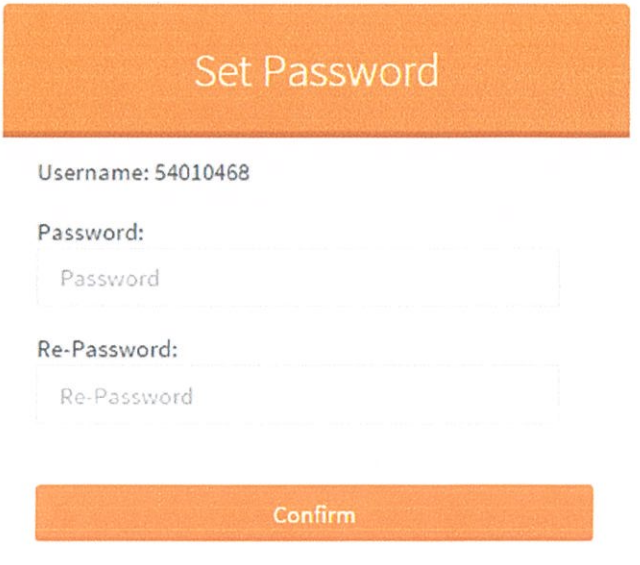
รูป 4.7 ตัวอย่างการเข้าใช้งานระบบในฐานะ Guest

4.4 ทดลองเข้าใช้งานในฐานะ Student

ในการเข้าใช้งานของ Student นั้นถ้าหากผู้ใช้ยังไม่เคยเข้าใช้งานระบบ จะต้องทำการยืนยันตัวตนสำหรับการเข้าใช้งานระบบครั้งแรกก่อน โดยเข้าสู่ระบบด้วยชื่อบัญชีผู้ใช้และรหัสผ่านของเว็บไซต์ภาควิชาดังรูป 4.8 จากนั้นจะมีหน้าต่างสำหรับการตั้งค่ารหัสผ่านใหม่ ดังรูป 4.9 โดยรหัสผ่านนี้จะเป็นรหัสผ่านสำหรับการเข้าใช้งานระบบและการเข้าใช้งานเว็บไซต์

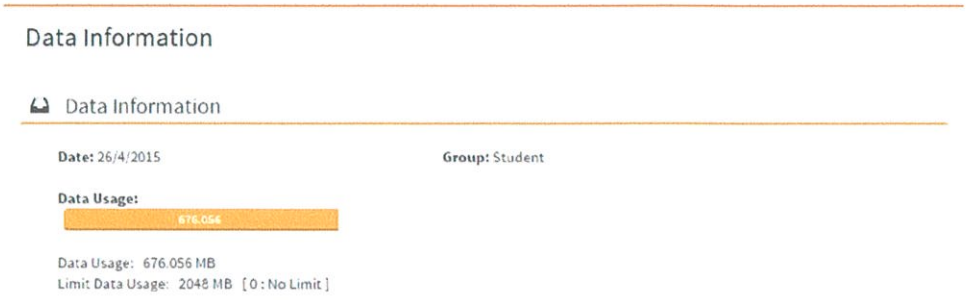


รูป 4.8 หน้าต่างการ Login เข้าเว็บไซต์



รูป 4.9 การตั้งค่ารหัสผ่านใหม่

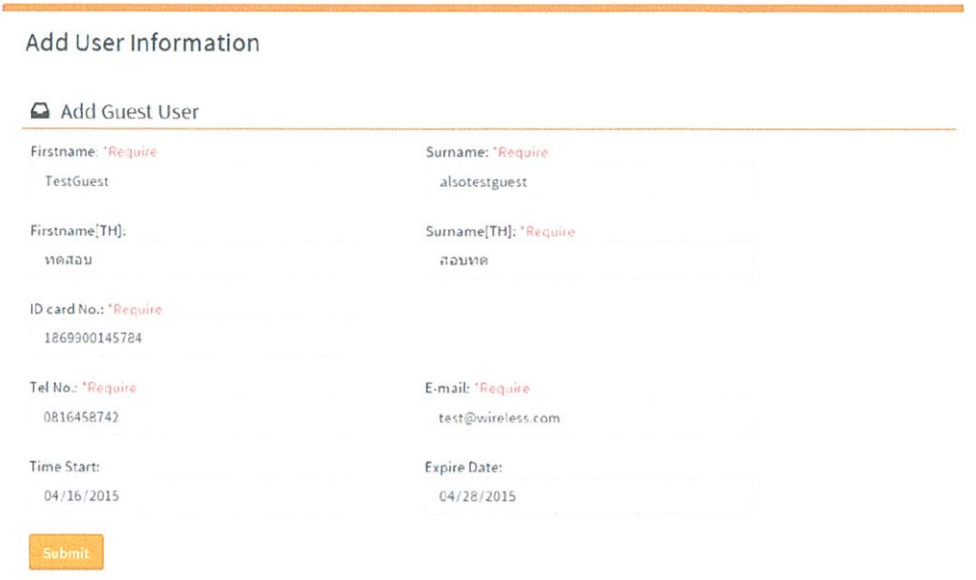
เมื่อ Login เข้ามาสู่เว็บไซต์แล้ว จะปรากฏหน้าต่างสำหรับการแสดงปริมาณการใช้งานในแต่ละวัน เมื่อมีการใช้งานเป็นเวลาหนึ่งแล้ว ดังรูป 4.10



รูป 4.10 ปริมาณข้อมูลที่ใช้งาน

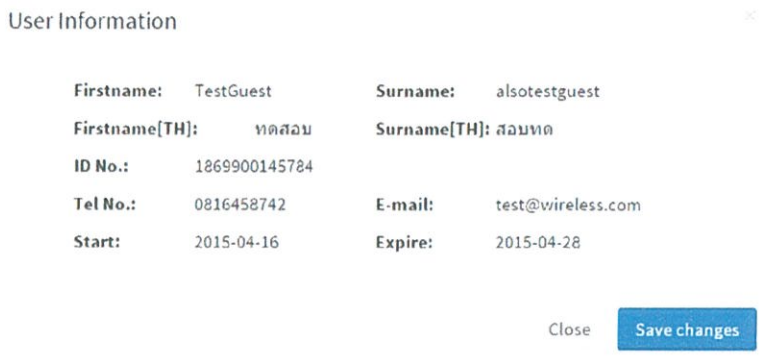
4.5 ทดลองเข้าใช้งานในฐานะ Lecturer

Lecturer สามารถทำการเพิ่ม Guest User โดย Lecturer จะต้องทำการกรอกข้อมูลส่วนตัวของ Guest โดยข้อมูลที่ทำการกรอกนั้นจะเป็นดังตัวอย่างในรูป 4.11



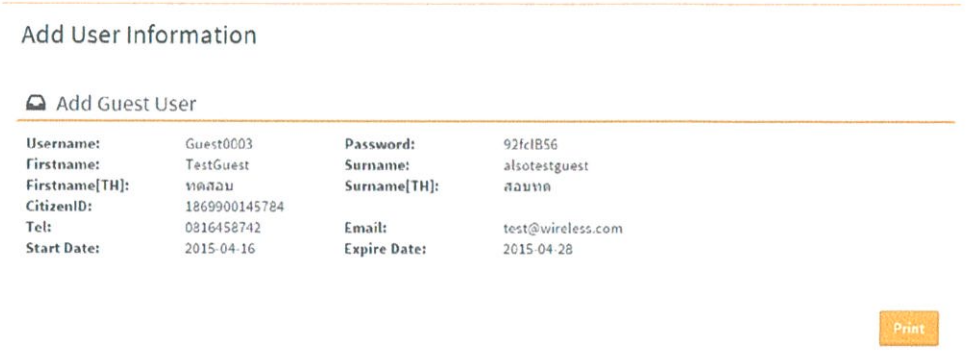
รูป 4.11 ตัวอย่างการกรอกข้อมูลส่วนตัวของ Guest

เมื่อ Lecturer ทำการกรอกข้อมูลครบแล้ว เมื่อทำการกดปุ่ม submit จะปรากฏหน้าต่างแสดงรายละเอียดข้อมูลที่ทำการกรอกเข้าไป ดังรูป 4.12 หากตรวจสอบแล้วรายละเอียดของข้อมูลถูกต้อง Lecturer สามารถกด Save change เพื่อทำการบันทึกข้อมูลของ Guest



รูป 4.12 หน้าต่างแสดงรายละเอียดข้อมูลของผู้ใช้

เมื่อทำการกด Save change แล้ว จะมีหน้าต่างแสดงรายละเอียดของ Guest พร้อมทั้งบัญชีผู้ใช้งานและรหัสผ่านของ Guest สำหรับเข้าใช้งานเครือข่ายขึ้นออกมา ซึ่งในหน้านี้จะสามารถสั่งพิมพ์ข้อมูลออกมาได้ด้วยการกดปุ่ม Print ดังแสดงในรูป 4.13



รูป 4.13 ข้อมูลของ Guest รวมทั้งบัญชีใช้งานและรหัสผ่านชั่วคราว

และนอกจากนี้ Lecturer ยังสามารถทำการเพิ่ม Guest ครั้งละหลายๆ บัญชีใช้งานได้ภายในครั้งเดียว ด้วยการคลิกที่แถบ Add multiple User โดยในที่นี้จะทำการทดลองอัพโหลดไฟล์ .csv เข้าไป ดังรูป 4.14

รูป 4.14 หน้าต่างการเพิ่ม Guest User ครั้งละหลายๆตัว

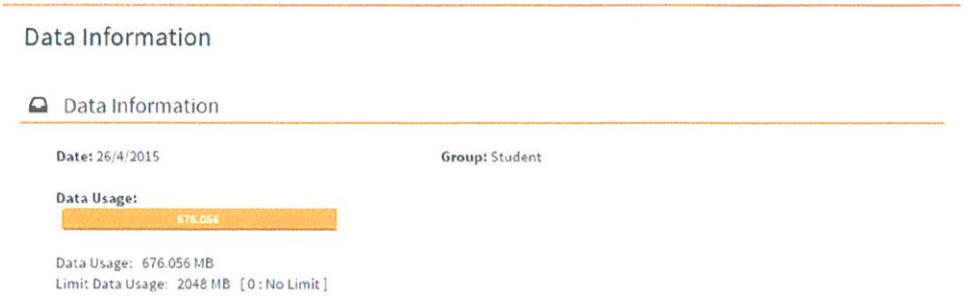
4.6 ทดลองเข้าใช้งานในฐานะ Admin

4.6.1 ทดลองใช้งานตรวจสอบ User ที่กำลังใช้งาน

Admin สามารถจำกัดปริมาณการใช้งานของ Student ได้ โดยจะทำการทดลองจำกัดปริมาณข้อมูลของ Student โดยจำกัดเป็น 2048 MB ดังรูป 4.15

รูป 4.15 การจำกัดปริมาณข้อมูลเป็น 2048 MB

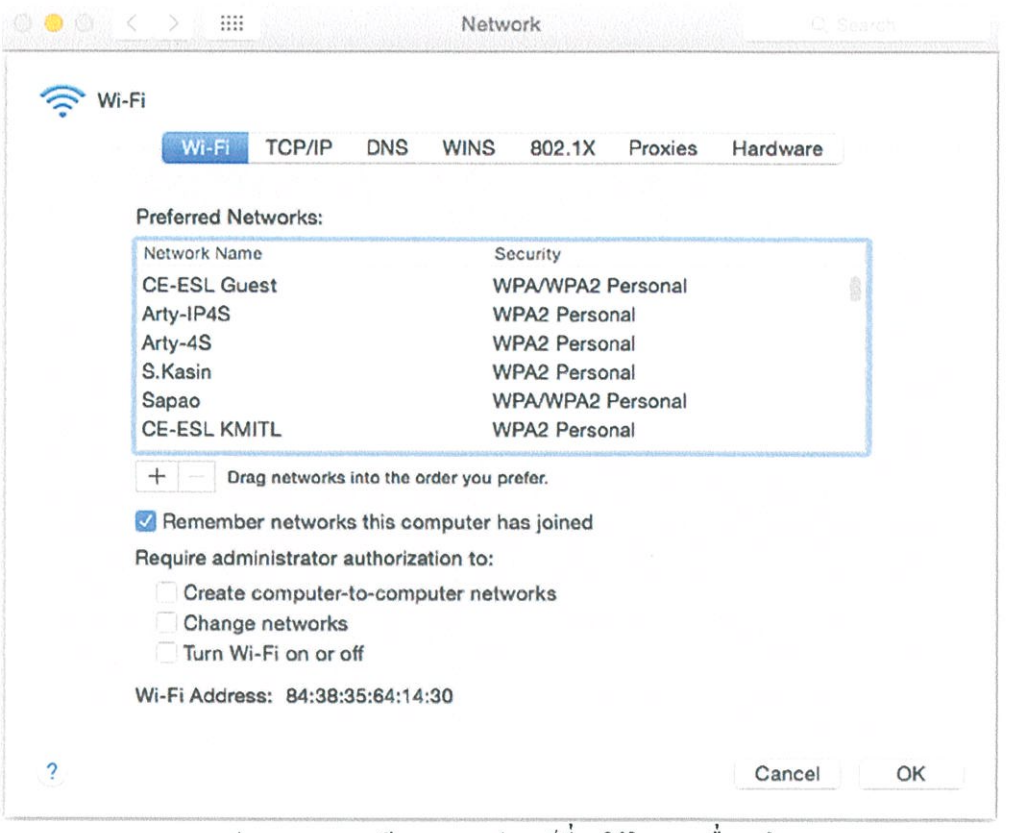
เมื่อทำการจำกัดปริมาณข้อมูลแล้วทดสอบโดยการเข้าไปใช้งานในฐานะ Student จะพบว่าข้อมูลมีการจำกัดปริมาณการใช้งานเป็น 2048 MB ดังรูป 4.16



รูป 4.16 ปริมาณข้อมูลที่ถูกจำกัดเป็น 2048

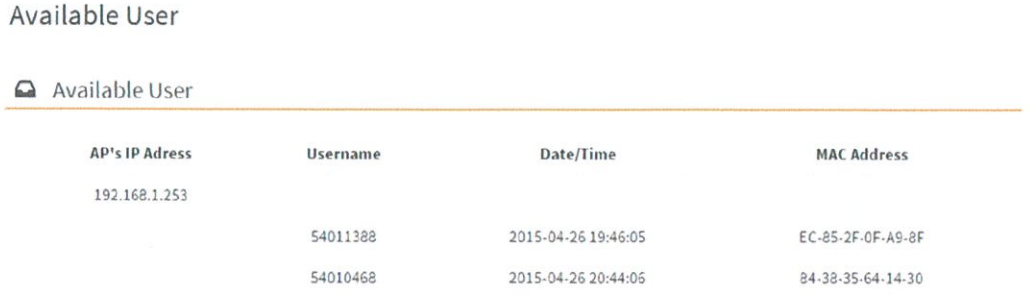
4.6.2 ทดลองใช้งานตรวจสอบ User ที่กำลังใช้งาน

ในการทดลองนี้จะทำการเข้าใช้งานระบบ โดยคอมพิวเตอร์ที่เข้าใช้งานมี MAC Address ดังแสดงในรูป 4.17



รูป 4.17 รายละเอียดของอุปกรณ์ที่จะใช้ในการเชื่อมต่อ

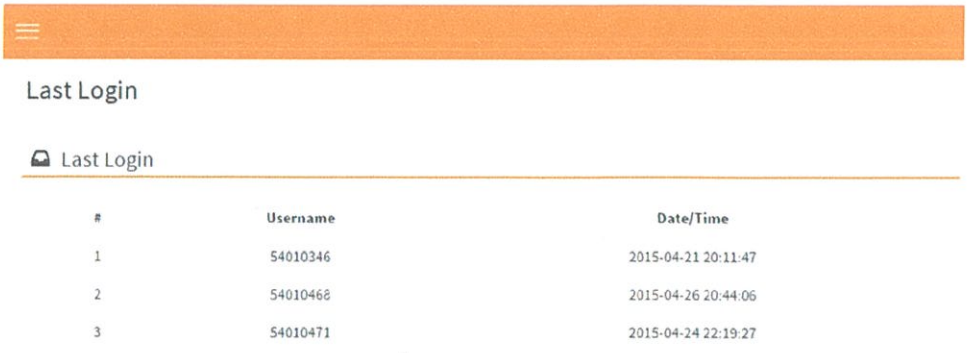
เมื่อทำการเชื่อมต่อเข้าสู่เครือข่ายแล้ว เข้าไปยังหน้าตรวจสอบ User ที่กำลังใช้งาน พบว่ามีการใช้งานของผู้ใช้งาน '54010468' เพิ่มเข้ามาและหมายเลข MAC Address ของผู้ใช้งานนั้นตรงกับอุปกรณ์ที่ใช้ทำการทดสอบ ดังรูป 4.18



รูป 4.18 ผู้ใช้งานที่กำลังใช้งาน

4.6.3 ทดสอบใช้งานตรวจสอบการเข้าใช้งานล่าสุดของผู้ใช้งาน

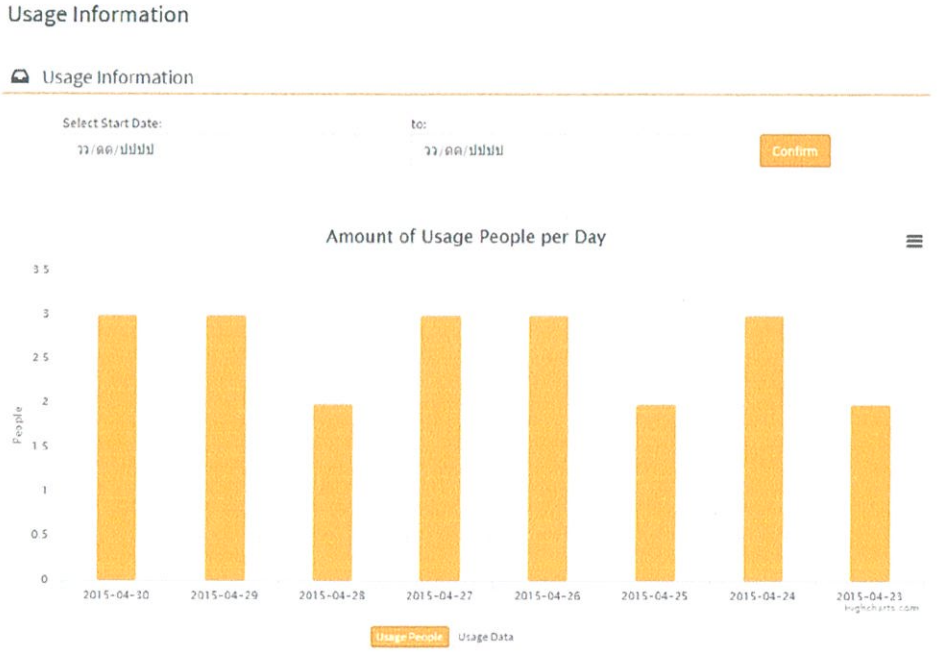
เมื่อทำการเชื่อมต่ออุปกรณ์เข้าสู่ระบบแล้ว ทดลองเข้าใช้งานในฐานะ Admin จะเห็นว่าบัญชีผู้ใช้งาน '54010468' มีการเข้าใช้งาน ณ เวลา 20:44 ในวันที่ 26 เมษายน 2558 ดังแสดงในรูป 4.19



รูป 4.19 เวลาที่เข้าสู่ระบบล่าสุดของผู้ใช้งาน

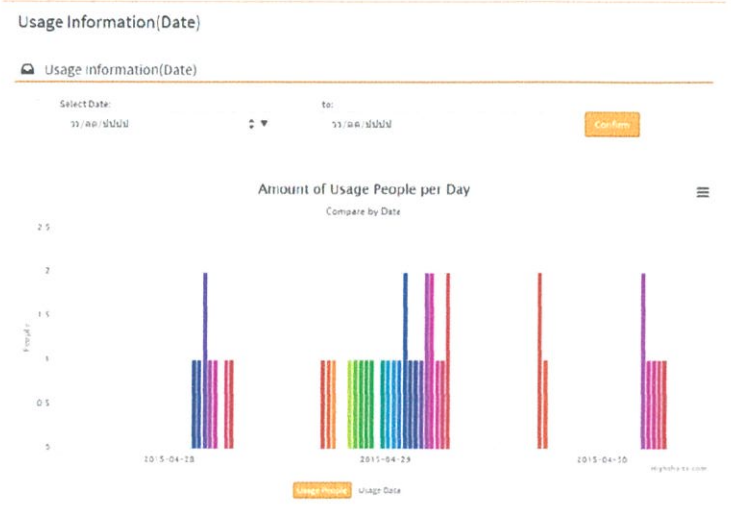
4.6.4 ทดสอบตรวจสอบสถิติการใช้งาน

1) ในการทดสอบนี้จะทดสอบดูสถิติการใช้งานย้อนหลังเป็นเวลา 7 วัน ซึ่งใส่ข้อมูล start date เป็นวันที่ 23/04/2015 และใส่วันที่ในช่อง to เป็น 30/04/2015 ดังรูป 4.20



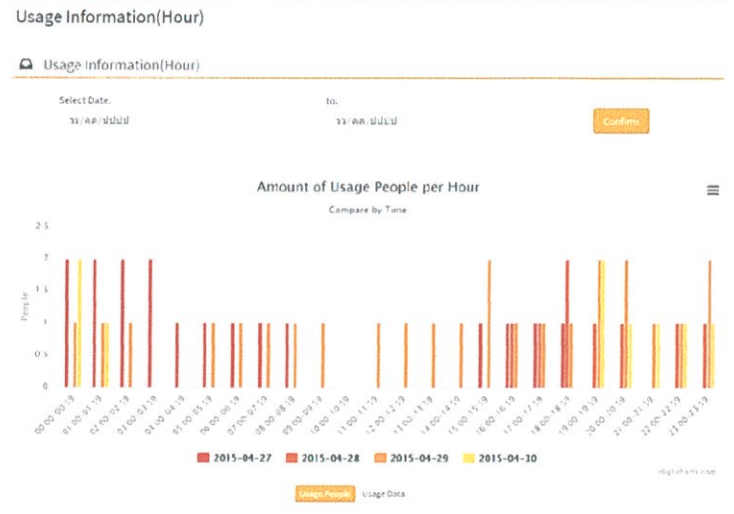
รูป 4.20 หน้าต่าง Usage Statistic

2) ในการทดสอบนี้จะทดสอบดูสถิติการใช้งานย้อนหลังเปรียบเทียบในหน่วยวันเป็นเวลา 3 วัน ซึ่งใส่ข้อมูล start date เป็นวันที่ 28/04/2015 และใส่วันที่ในช่อง to เป็น 30/04/2015 ดังรูป 4.21



รูป 4.21 หน้าต่าง Usage Statistic(Date)

3) ในการทดสอบนี้จะทดสอบดูสถิติการใช้งานย้อนหลังเปรียบเทียบในหน่วยชั่วโมงเป็นเวลา 4 วัน ซึ่งใส่ข้อมูล start date เป็นวันที่ 27/04/2015 และใส่วันที่ในช่อง to เป็น 30/04/2015 ดังรูป 4.22



รูป 4.22 หน้าต่าง Usage Statistic(Time)

บทที่ 5
บทสรุป

5.1 บทสรุป

ในการทำโครงงานระบบเครือข่ายไร้สายและการยืนยันตนสำหรับภาควิชาวิศวกรรมคอมพิวเตอร์เป็นระบบที่ทำให้การใช้งานเครือข่ายไร้สายภายในภาควิชาวิศวกรรมคอมพิวเตอร์สำหรับบุคคลากรของภาควิชาสะดวกและครอบคลุมยิ่งขึ้น ระบบสามารถใช้งานร่วมกับระบบเครือข่ายเดิมของภาควิชา สามารถเก็บประวัติการใช้งานของผู้ใช้งาน ควบคุมปริมาณการใช้งานของนักศึกษา Admin สามารถตรวจสอบประวัติการใช้งาน สามารถดูสถิติการใช้งานต่างๆ และบริหารจัดการเกี่ยวกับการจำกัดการใช้งานได้ สำหรับ Lecturer สามารถเพิ่มบัญชีผู้ใช้งาน Guest เพื่อให้บุคคลภายนอกสามารถใช้งานชั่วคราวได้ ระบบสามารถเก็บปริมาณการใช้งานของผู้ใช้งานได้แต่ด้วยข้อจำกัดของอุปกรณ์ทำให้ไม่สามารถเก็บข้อมูลตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ทั้งหมด

5.2 ปัญหาอุปสรรคและแนวทางแก้ไข

1) ขาดความเข้าใจในการตั้งค่าซอฟต์แวร์และอุปกรณ์ต่างๆให้ทำงานร่วมกัน ส่งผลให้ใช้เวลาสำหรับการศึกษาและแก้ปัญหาที่เกิดขึ้นนาน แก้ปัญหาโดยการพยายามศึกษาหาข้อผิดพลาดในการทำงานอย่างละเอียดทีละจุด
2) ขาดความเข้าใจในการออกแบบระบบให้รองรับกับระบบของภาควิชา เนื่องจากไม่คุ้นเคยกับวิธีการในการตั้งค่าอุปกรณ์ของภาควิชา ซึ่งหากเกิดความผิดพลาดในการตั้งค่าจะทำให้ระบบเครือข่ายของภาควิชามีปัญหาส่งผลต่อการใช้งานระบบเครือข่ายของทั้งภาควิชา แก้ปัญหาโดยการทำการตั้งค่าและทดสอบย่อยทีละส่วนของระบบ เมื่อแน่ใจว่าแต่ละส่วนสามารถทำงานได้อย่างไม่มีปัญหาจึงนำมารวมกัน
3) การทำ Accounting ของ Access Point เนื่องจาก Access Point ที่นำมาใช้ในการทดสอบมีหลายรุ่นที่ไม่มีฟังก์ชันในการทำ Accounting หรือแม้จะมีฟังก์ชันในการทำ Accounting แต่ก็ไม่สามารถเก็บข้อมูลการใช้งานได้สมบูณ์ จะมีเพียงบางอุปกรณ์เท่านั้นที่สามารถเก็บได้ ส่วนอุปกรณ์อื่นๆ จะสามารถเก็บได้เมื่อทำงานภายใต้เงื่อนไขที่กำหนด

5.3 แนวทางในการพัฒนาต่อ

1) ออกแบบระบบให้รองรับการเก็บข้อมูลตามตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ทั้งหมด เพื่อที่จะสามารถนำไปใช้งานจริงได้
2) เปลี่ยนอุปกรณ์ Access Point ให้สามารถทำการเก็บประวัติข้อมูลการใช้งานของผู้ใช้งานได้ละเอียดกว่านี้ และไม่มีข้อจำกัดในการใช้งาน
3) ปรับปรุงฟังก์ชันการใช้งานเพิ่มเติมให้กับหน้าเว็บไซต์ในด้านของการแสดงผลข้อมูลต่างๆ ให้ดีขึ้น

บรรณานุกรม

วัชรินทร์ จิรโสภณ, 2555. **"ระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์."** สารนิพนธ์ วิทยาศาสตรมหาบัณฑิต ภาควิชาเทคโนโลยีสารสนเทศ คณะวิทยาการและเทคโนโลยีสารสนเทศ, มหาวิทยาลัยเทคโนโลยีมหานคร

Cisco System, 2007. **Design Principles for Voice Over WLAN.** [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/wireless/4400-series-wireless-lan-controllers/net_implementation_white_paper0900aecd804f1a46.html

Aerohive Networks, 2012. **High-Density Wi-Fi Design Principles.** [Online]. Available: https://www.aerohive.com/pdfs/Aerohive-Whitepaper-Hi-Density%20Principles.pdf

สรุปขั้นตอนการ Authentication [Online]. Available: http://ekasitw.tripod.com/authentication.htm

Web Services [Online]. Available: http://gear.kku.ac.th/~krunapon/courses/168493/others/wsabc.html

MVC คืออะไร? [Online]. Available: http://www.kontentblue.com/site/article/article?id=mvc-what-is

ภาคผนวก ก

รายละเอียดงบประมาณในการติดตั้งระบบ

ก.1 รายละเอียดอุปกรณ์ต่างๆ

ก.1.1 Server

เป็นอุปกรณ์ที่จะนำมาทำเป็น RADIUS Server, Directory Server, DHCP Server, Log Server และ Web Service ภายในเครื่องเดียว โดย Server จะต้องรองรับการติดตั้ง VMware ESXi ได้ ทั้งนี้ต้องเพิ่ม RAM 4GB DDR3 1600 MHz UDIMM with ECC ให้กับ Server อีก 4 GB ในราคา 2,570 บาท

ตาราง ก.1 คุณสมบัติ HP ProLiant ML310e Gen8 V2 (Tower)

Specification	รายละเอียด
Processor	Intel® Xeon E3-1220v3(3.1GHz/4-core/8MB/80W)
RAM	4 GB DDR3 1600MHz UDIMM with ECC
HDD	1 TB 7200 RPM
RAID	Support RAID 0,1
NIC	HP Ethernet 1Gb 2-port
Power Supply	HP 350 W
Optical	HP 16x SATA DVD-RW
Price	28,500

รูป ก.1 รูปอุปกรณ์ในส่วนของ Server

ก) HP ProLiant ML310e Gen8 V2 (Tower)

ข) Server RAM

หมายเหตุ: ราคาและรายละเอียดอุปกรณ์อ้างอิงจาก www.quickserv.co.th

หมายเหตุ: ราคาRAM อ้างอิงจาก www.host4thai.com

ก.2 Access point

จะต้องรองรับการทำงานแบบ 802.1X โดยในที่นี้ได้นำเสนอ Access Point ที่จะนำมาเลือกเพื่อใช้งานจำนวน 3 รุ่น ซึ่งรายละเอียดต่างๆของ Access Point จะแสดงตามตารางด้านล่าง

ตาราง ก.2 คุณสมบัติของ Router

Specification	Linksys EA6200	Zyxel NWA1100-NH	Linksys WAP300N
Type	Wi-Fi Router	Access Point	Access Point
Radio	802.11/a/b/g/n/ac	802.11b/g/n	802.11b/g/n
Dual Band	Yes	No	Yes
PoE	No	Yes	No
Antenna	Internal x 4	External x 2	External x 2
RF Power	20 dBm	28 dBm	20 dBm
Accounting	NO	YES	NO
Wall Mount	Yes	Yes	Yes
Price	4290	3190	2250

รูป ก.2 อุปกรณ์ Access Point แต่ละชนิด

ก) Linksys EA6200

ข) Zyxel NWA1100-NH

ค) Linksys WAP300N

หมายเหตุ: ข้อมูลราคาและรายละเอียดอุปกรณ์จาก www.sys2u.com

ก.2 งบประมาณที่ใช้

สำหรับงบประมาณที่ใช้นั้นขึ้นอยู่กับรูปแบบในเลือกอุปกรณ์ที่จะนำมาติดตั้งเป็นสำคัญ ส่วนค่าแรงในการติดตั้งจะคิดเป็นจุดจุดละ 300 บาท โดยในแต่ละรูปแบบการเลือกอุปกรณ์นั้นจะมีความแตกต่างกันในส่วนของอุปกรณ์ Access Point ที่นำมาติดตั้ง

ก.2.1 รูปแบบอุปกรณ์ชุดที่ 1

การติดตั้งในรูปแบบที่ 1 นี้จะใช้ Server HP ProLiant ML310e Gen8 V2 (Tower) และในส่วนของ Access Point จะใช้ Linksys EA6200 ซึ่งเป็น Wi-Fi – Router แต่นำมาตั้งค่าให้ทำงานในโหมด Access Point แทน

ก.2.1.1 ข้อดี

Linksys EA6200 นั้น รองรับมาตรฐาน Wi-Fi ใหม่ล่าสุดคือ 802.11ac ซึ่งเป็นมาตรฐานใหม่ที่ทำงานบนคลื่นความถี่ 5 GHz อีกทั้งยังมีความสามารถในการทำงานร่วมกับมาตรฐานเก่า (Backward Compatible) อย่าง 802.11a/b/g/n ได้อีกด้วย อีกทั้งรองรับการใช้งานแบบ Dual Band ทำให้ Linksys EA6200 เป็นอุปกรณ์ที่มีประสิทธิภาพ

ก.2.1.2 ข้อเสีย

ในปัจจุบันนี้อุปกรณ์ที่รองรับมาตรฐาน 802.11ac นั้นยังมีจำนวนน้อยอยู่ และเนื่องจาก Linksys EA6200 เป็น Wi-Fi Router ตัวแรกๆ ที่รองรับมาตรฐานนี้ทำให้ Linksys EA6200 ยังมีราคาค่อนข้างสูงอีกทั้งยังไม่สามารถใช้งานฟังก์ชัน Accounting ได้ ซึ่งทำให้ไม่สามารถเก็บข้อมูลการใช้งานของผู้ใช้งานได้

ก.2.1.3 งบประมาณที่ใช้

ตาราง ก.3 งบประมาณที่ใช้ในรูปแบบอุปกรณ์ชุดที่ 1

รายละเอียด	จำนวน	ราคา
HP ProLiant ML310e Gen8 V2 (Tower)	1	28,500
RAM 4GB 1600 MHz UDIMM with ECC	1	2,570
Linksys EA6200	44	188,760
ค่าติดตั้งอุปกรณ์	44	13,200
รวม	233,030	

ก.2.2 รูปแบบอุปกรณ์ชุดที่ 2

การติดตั้งในรูปแบบที่ 2 นี้ จะใช้ Server HP ProLiant ML310e Gen8 V2 (Tower) และในส่วนของ Access Point จะใช้ Zyxel NWA1100-NH

ก.2.2.1 ข้อดี

Zyxel NWA1100-NH เป็น Access Point มีจุดเด่นที่ กำลังในการส่งที่สูงถึง 28 dBm อีกทั้งยังราคาอยู่ในระดับปานกลาง รองรับมาตรฐาน 802.11n สามารถทำงานร่วมกับมาตรฐานเก่า (Backward Compatible) อย่าง 802.11b/g ได้ รองรับการจ่ายไฟฟ้าแบบ PoE ซึ่งสามารถรองรับกับการเปลี่ยนแปลงระบบในอนาคตทั้งยังมีราคาที่ไม่แพงจนเกินไป และสามารถทำการเก็บข้อมูล Accounting ได้

ก.2.2.2 ข้อเสีย

ถึงแม้จะรองรับระบบ PoE แต่สวิตช์ที่ใช้งานก็ต้องรองรับระบบ PoE ด้วย ซึ่งในปัจจุบันยังคงมีราคาสูงอยู่และทำงานบนคลื่นความถี่ 2.4 GHz เท่านั้น ไม่รองรับอุปกรณ์บนคลื่นความถี่ 5 GHz

ก.2.2.3 งบประมาณที่ใช้

ตาราง ก.4 งบประมาณที่ใช้ในรูปแบบอุปกรณ์ชุดที่ 2

รายละเอียด	จำนวน	ราคา
HP ProLiant ML310e Gen8 V2 (Tower)	1	28,500
RAM 4GB 1600 MHz UDIMM with ECC	1	2,570
Zyxel NWA1100-NH	44	140,360
ค่าติดตั้งอุปกรณ์	44	13,200
รวม	184,630	

ก.2.3 รูปแบบอุปกรณ์ชุดที่ 3

การติดตั้งในรูปแบบที่ 2 นี้ จะใช้ Server HP ProLiant ML310e Gen8 V2 (Tower) และในส่วนของ Access Point จะใช้ Linksys WAP300N

ก.2.3.1 ข้อดี

Linksys WAP300N เป็น Access Point มีจุดเด่นที่รองรับการทำงานทั้งคลื่นความที่ 2.4 GHz และ 5 GHz และรองรับมาตรฐานสูงสุด 802.11n สามารถทำงานร่วมกับมาตรฐานเก่า (Backward Compatible) อย่าง 802.11a/b/g/n ได้ด้วย ทั้งยังมีราคาที่ถูกมากเมื่อเทียบกับอุปกรณ์รุ่นอื่นๆ ในตลาด

ก.2.3.2 ข้อเสีย

ยังไม่รองรับมาตรฐานใหม่ล่าสุดอย่าง 802.11 ac และยังไม่สามารถทำฟังก์ชัน Accounting ได้

ก.2.3.3 งบประมาณที่ใช้

ตาราง ก.5 งบประมาณที่ใช้ในรูปแบบอุปกรณ์ชุดที่ 3

รายละเอียด	จำนวน	ราคา
HP ProLiant ML310e Gen8 V2 (Tower)	1	28,500
RAM 4GB 1600 MHz UDIMM with ECC	1	2,570
Linksys WAP300N	44	99,000
ค่าติดตั้งอุปกรณ์	44	13,200
รวม	143,270	

ภาคผนวก ข
เปรียบเทียบกับผลิตภัณฑ์อื่น

ข.1 Mikrotik

Mikrotik เป็นบริษัทที่ประกอบธุรกิจขายอุปกรณ์และซอฟต์แวร์ที่เกี่ยวข้องกับระบบเครือข่ายเป็นหลัก โดยบริษัทอุปกรณ์และซอฟต์แวร์มีชื่อเสียงคือ อุปกรณ์ RouterBoard ที่มาพร้อมกับระบบปฏิบัติการ RouterOS อุปกรณ์ RouterBoard รองรับการทำ Hotspot Authenticate มีความสามารถในการสร้าง Username Password เพื่อให้ผู้ใช้สามารถยืนยันตัวตนเข้าใช้งานระบบได้ มีการจำกัดความเร็วในการใช้งานเครือข่าย Internet ของ User แต่ละคน โดยจะทำงานควบคู่กันกับระบบปฏิบัติการ RouterOS ซึ่งภายใน RouterOS จะมี RADIUS Server ติดตั้งมาด้วย สำหรับประสิทธิภาพในการทำงานของ Mircotik นั้นจะขึ้นอยู่กับรุ่นของตัว RouterBoard โดยใน RouterBoard แต่ละรุ่นก็จะมีระบบปฏิบัติการ RouterOS เวอร์ชั่น

ข.2 เปรียบเทียบ Mikrotik กับระบบ Wireless for CE

เนื่องจาก Mikrotik มีความสามารถในการทำงานที่ใกล้เคียงกับระบบเครือข่าย จึงได้ทำการเปรียบเทียบในความสามารถด้านต่างๆ

ตาราง ข.1 เปรียบเทียบความสามารถระหว่าง Microtik และระบบ Wireless for CE

ความสามารถในการทำงาน	Microtik	Wireless for CE
สามารถจัดการ Accounting อื่นๆตามที่เราต้องการ	NO	YES
แบ่งกลุ่มผู้ใช้งานออกเป็นกลุ่มๆ	NO	YES
กำหนด Policy การใช้งานของแต่ละกลุ่มได้	NO	YES
มีหน้าเว็บไซต์ให้ทำการ Login เข้าใช้งาน	YES	NO
มีหน้า GUI ที่ทำให้ง่ายต่อการตั้งค่าของผู้ดูแลระบบ	YES	NO
สามารถนำข้อมูลการใช้งานมาวิเคราะห์ได้	NO	YES
ตรวจสอบปริมาณการใช้งานในแต่ละวัน	NO	YES
สามารถเก็บข้อมูลการใช้งานย้อนหลังได้จำนวนมาก	NO	YES