ระบบพิสูจน์ตัวตนผ่านเครือข่ายเอ็ดยูโรม

AUTHENTICATION SYSTEM VIA EDUROAM

โดย

ณัฐธัญพงศ์ ศรนารายณ์

NUTTHUNYAPONG SORNNARAI

อาจารย์ที่ปรึกษา

ผศ.ดร. ภัทรชัย ลลิตโรจน์วงศ์

รายงานนี้เป็นส่วนหนึ่งของวิชาการศึกษาอิสระ 2
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ภาคเรียนที่ 2 ปีการศึกษา 2558

AUTHENTICATION SYSTEM VIA EDUROAM

NUTTHUNYAPONG SORNNARAI

A REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE

REQUIREMENTS OF THE COURSE

INDEPENDENT STUDY 2

MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY

FACULTY OF INFORMATION TECHNOLOGY

KING MONKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2/2015

ใบรับรอง การศึกษาอิสระ 2 (Independent Study 2)

เรื่อง

ระบบพิสูจน์ตัวตนผ่านเครือข่ายเอ็ดยูโรม

AUTHENTICATION SYSTEM VIA EDUROAM

นายณัฐธัญพงศ์ ศรนารายณ์

รหัสประจำตัว 57606061

ขอรับรองว่ารายงานฉบับนี้ ข้าพเจ้าไม่ได้คัดลอกมาจากที่ใด

รายงานฉบับนี้ได้รับการตรวจสอบและอนุมัติให้เป็นส่วนหนึ่งของ

การศึกษาวิชาการศึกษาอิสระ 2 หลักสูตรวิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศ)

ภาคเรียนที่ 2 ปีการศึกษา 2558

.....อาจารย์ที่ปรึกษา

(ผศ.ดร.ภัทรชัย ลลิตโรจน์วงศ์)

.....กรรมการสอบ

(รศ.ดร.วรพจน์ กรีสุระเดช)

.....กรรมการสอบ

(ดร.กนกวรรณ อัจฉริยะชาญวณิช)

หัวข้อ	ระบบพิสูจน์ตัวตนผ่านเครือข่ายเอ็ดยูโรม
นักศึกษา	นายณัฐธัญพงศ์ ศรนารายณ์
รหัสนักศึกษา	57606061
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
แขนงวิชา	เทคโนโลยีเครือข่ายและระบบ
ปีการศึกษา	2558
อาจารย์ที่ปรึกษา	ผศ.ดร. ภัทรชัย ลลิตโรจน์วงศ์

บทคัดย่อ

เป้าหมายของโครงการนี้คือการปรับใช้ เครือข่ายไร้สายเอ็ดยูโรม ในเครือข่ายมหาวิทยาลัยราชภัฏเทพสตรี โครงการจะแบ่งออกเป็นสองส่วน คือการใช้งานในมหาวิทยาลัยและการเชื่อมต่อกับเครือข่ายระดับชาติ โดยมุ่งเน้นที่การดำเนินการติดตั้งและการกำหนดค่าของระบบการพิสูจน์ตัวตนโดยใช้เทคโนโลยี IEEE802.1X ส่วนของทฤษฎีมีวัตถุประสงค์เพื่อให้ครอบคลุมเนื้อหาพื้นฐานของการพิสูจน์ตัวตน ในระหว่างการดำเนินการต้องทำการตั้งค่าพร็อกซีเซิร์ฟเวอร์ตามรูปแบบการใช้งานของมหาวิทยาลัย เมื่อดำเนินการเสร็จสิ้น จะทำให้มหาวิทยาลัยใช้ข้อมูลชื่อผู้ใช้และรหัสผ่านทั้งภายในและภายนอกในเวลาเดียวกัน ทำให้ผู้ใช้งานสามารถ ใช้งานเอ็ดยูโรมจากทุกสถาบันการศึกษาที่เปิดใช้งานเอ็ดยูโรม นอกจากนี้ผู้ใช้งานจากหน่วยงานอื่นที่เป็นสมาชิกเอ็ดยูโรมก็จะสามารถที่จะเข้าสู่ระบบเครือข่ายไร้สายเอ็ดยูโรมในมหาวิทยาลัยราชภัฏเทพสตรี โดยใช้ชื่อผู้ใช้งานจากหน่วยงานต้นสังกัดได้

ระบบนี้ถูกพัฒนาบนระบบปฏิบัติการ Debian ร่วมกับระบบการจัดการฐานข้อมูล LDAP และโปรแกรม Free Radius ซึ่งเป็นโปรแกรมแบบ Open Source ทั้งสิ้น ทำให้ประหยัดค่าใช้จ่ายและเพิ่มความสะดวกได้มากหากเทียบกับการทำงานของระบบอื่นๆ ที่มีอยู่

Title	Authentication System via Eduroam
Student	Mr.Nutthunyapong Sornnarai
Student ID.	57606061
Degree	Master of Science
Program	Information Technology
Major	Network and Systems Technology
Academic Year	2015
Advisor	Asst.Prof.Dr. Pattarachai Lalitrojwong

ABSTRACT

The purpose of this project was to apply eduroam wireless network in Thepsatri Rajabhat University. This project was divided into two parts: internal connection at university level and external connection at national level. The project aimed to conduct installation and configuration of authentication using IEEE802.1X technology. Theoretically, this project aimed to comprehensively explore fundamental content of authentication. During the process, proxy server would be set based on the university's applications. When the developed system is finished, the University's user can access to the username and password, both inside and outside at the same time; the user can operate eduroam from each educational institution. Besides, users who are members of other organizations can access to eduroam wireless network in Thepsatri Rajabhat University through username of their parent organization.

This system is developed on Open Architecture platform using Debian operating system, LDAP, OpenSSL and Free Radius as a basic tool set. The final result application is cost effective and allows users to have more convenient if compare with other systems.

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

สารบัญรูป

รูปที่ หน้า

สารบัญรูป (ต่อ)

รูปที่ หน้า

สารบัญรูป (ต่อ)

รูปที่ หน้า

สารบัญรูป (ต่อ)

รูปที่ หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาของโครงการ

ปัญหาเกิดขึ้นเมื่อผู้ใช้งานเครือข่ายไร้สายจากมหาวิทยาลัยราชภัฏเทพสตรีมีความจำเป็นต้องไปศึกษาดูงาน อบรมใน สถาบันการศึกษาแห่งหนึ่ง มีความจำเป็นต้องใช้งานเครือข่ายไร้สายแต่ไม่สามารถใช้งานได้เนื่องจากไม่มีชื่อผู้ใช้ในระบบหรืออีกเหตุผลหนึ่งคือความแตกต่างของระบบรักษาความปลอดภัย บางองค์กรอาจใช้วิธีแก้ปัญหาแบบผิดๆ ด้วยการอนุญาตให้ผู้ใช้งานทุกคนสามารถเข้าใช้งานระบบเครือข่ายไร้สายโดยไม่มีระบบรักษาความปลอดภัยซึ่งอาจนำไปสู่ปัญหาอื่นๆ เช่นความปลอดภัยของข้อมูลของผู้ใช้หรือขององค์กรเอง เป็นต้น

จึงจัดทำระบบเครือข่ายไร้สายที่ทำให้ผู้ใช้งานจากองค์กรต่างๆ สามารถโรมมิ่งไปใช้งานเครือข่ายไร้สายข้ามองค์กรได้ อีกทั้งยังมีระดับความปลอดภัยสูง โดยกำหนดให้ผู้ใช้ติดตั้ง Certificate ของทั้งผู้ใช้และของระบบของผู้ใช้ ลงไปในเครื่องคอมพิวเตอร์เพื่อนำไปใช้ในการพิสูจน์ตัวตนทั้ง 2 ทางเพื่อให้ผู้ใช้งานมั่นใจได้ว่าล็อกอินเข้าระบบที่แท้จริงเมื่อผู้ใช้งานมีความจำเป็นต้องไปทำงานหรือสัมมนาที่องค์กรอื่นๆที่เชื่อถือซึ่งกันและกัน ก็สามารถล็อกอิน เข้าระบบขององค์กรอื่นโดยใช้ Certificate ขององค์กรของตัวเองได้เลยทำให้สามารถแก้ปัญหาเรื่องระบบความปลอดภัยของเครือข่ายไร้สายและปัญหาโรมมิ่งของผู้ใช้งาน

ระบบพิสูจน์ตัวตนผ่านเครือข่ายเอ็ดยูโรม ถูกพัฒนาขึ้นมาเพื่อช่วยอำนวยความสะดวกในการเข้าใช้งานเครือข่ายอินเทอร์เน็ตภายนอกสถาบัน ในกรณีที่ไปในสถานที่ราชการที่มีเครือข่ายเอ็ดยูโรมอยู่โดยใช้เทคโนโลยีการพิสูจน์ตัวตนแบบ 802.1x และยังเป็นการเพิ่มความปลอดภัยในการเข้าใช้งานเครือข่ายไร้สายของมหาวิทยาลัยราชภัฏเทพสตรีลดภาระการทำงานของระบบเน็ตเวิร์คมากขึ้น

1.2 วัตถุประสงค์ของโครงการ

1) เพื่อให้อุปกรณ์ที่ต้องการเชื่อมต่ออินเทอร์เน็ต สามารถยืนยันตัวตนแบบ WPA/WPA2 Enterprise ได้
2) เพื่อลดการทำงานของเครือข่าย ซึ่งปัจจุบันมีอุปกรณ์จำนวนมากรวมถึงบุคคลภายนอกที่เข้ามาภายในมหาวิทยาลัย ได้ทำการเชื่อมโยงเข้ากับ SSID แต่ไม่ได้ทำการยืนยันตัวตน ทำให้อุปกรณ์เครือข่ายไร้สายต้องรับภาระงานเพิ่มขึ้นกระทบผู้ใช้ภายใน รวมถึงมีความเสี่ยงด้านความปลอดภัยเนื่องจากไม่ได้เข้ารหัสสัญญาณ
3) เพื่อศึกษาและพัฒนาระบบยืนยันตัวตนผู้ใช้งานอินเทอร์เน็ตแบบโรมมิ่ง หรือ Education Roaming โดยใช้เทคโนโลยี 802.1x

4) เพื่อให้ผู้ใช้บริการสามารถที่จะใช้อินเทอร์เน็ตภายนอกเครือข่ายสถาบันการศึกษาของเราได้ทั้งในประเทศและต่างประเทศ

1.3 ขอบเขตของโครงการ

ระบบนี้เป็นการศึกษา ระบบพิสูจน์ตัวตนผ่านเครือข่ายเอ็ดยูโรม และระบบพิสูจน์ตัวตนแบบ WPA/WPA2 Enterprise ด้วยบัญชีผู้ใช้งาน LDAP ของมหาวิทยาลัยราชภัฏเทพสตรี

1) ส่วนของผู้ใช้

1.1) สามารถเข้าใช้งานอินเทอร์เน็ตภายนอกเครือข่ายสถาบันการศึกษาและในต่างประเทศที่ใช้เครือข่าย eduroam โดยใช้บัญชีผู้ใช้งานของมหาวิทยาลัยราชภัฏเทพสตรี

2) ส่วนของผู้ดูแลระบบ

2.1) แสดงรายการผู้ใช้งาน ทั้งหมดในระบบและแสดงเฉพาะวันที่ปัจจุบัน

2.2) สามารถติดตั้งและแก้ไขไฟล์ที่จำเป็นของเซิร์ฟเวอร์สำหรับเอ็ดยูโรมแบบอัตโนมัติโดยไม่ต้องเข้าไปแก้ไขไฟล์การตั้งค่าทีละไฟล์ได้โดยตรงจากเว็บไซต์

2.3) สามารถถอนบัญชีผู้ใช้งานที่กระทำผิด นโยบายหรือข้อบังคับการใช้งาน

1.4. ขั้นตอนในการพัฒนาระบบ

การวางแผนการดำเนินงานในการพัฒนาระบบพิสูจน์ตัวตนผ่านเครือข่ายเอ็ดยูโรม ประกอบไปด้วยการทำงาน 8 ขั้นตอนด้วยกันคือ

1) ดำเนินการกรอกแบบฟอร์มคำร้องของใช้งานเครือข่ายเอ็ดยูโรมประเทศไทยส่งไปที่ email : noc@uni.net.th

2) จัดเตรียมเซิร์ฟเวอร์สำหรับเอ็ดยูโรมจำนวน 1 เครื่อง ใช้ระบบปฏิบัติการเป็น Debian พร้อมลง Freeradius version 2 ขึ้นไป

3) แจ้ง IP Address ของเครื่องเซิร์ฟเวอร์ดังกล่าว มายัง email : noc@uni.net.th

4) ทำการคอนฟิกค่าเพิ่มตามที่ Uninet ส่งเมล์ยืนยันกลับมา

5) ทดสอบระบบกับทาง Uninet

6) เมื่อดำเนินการเชื่อมต่อเอ็ดยูโรมเสร็จสิ้นแล้ว ให้แจ้งกลับมายัง noc@uni.net.th เพื่อให้เจ้าหน้าที่บันทึกวันที่สามารถใช้งาน eduroam-TH ได้ลงในระบบ

7) จัดทำเว็บไซต์เอ็ดยูโรมแสดงบนเว็บไซต์ของมหาวิทยาลัย เพื่อแจ้งให้ทราบเกี่ยวกับสถานที่ในการให้บริการเอ็ดยูโรมภายในมหาวิทยาลัยเกี่ยวกับ service ที่ให้บริการ และข้อมูลอื่นๆ เกี่ยวกับเอ็ดยูโรมพร้อมแจ้งกลับมายัง noc@uni.net.th เพื่อให้เจ้าหน้าที่บันทึก URL หน้า page eduroam ของมหาวิทยาลัยลงในระบบ

8) สรุปผลโครงการและข้อเสนอแนะ

1.5. ประโยชน์ที่คาดว่าจะได้รับ

1) นักศึกษา อาจารย์ และบุคลากรของมหาวิทยาลัยราชภัฏเทพสตรี สามารถเข้าใช้และใช้งานเครือข่ายอินเตอร์เน็ตภายนอกมหาวิทยาลัย ผ่านเครือข่ายของสถาบันอื่นได้
2) นักศึกษา อาจารย์ และบุคลากรจากสถาบันอื่นที่เป็นสมาชิกกับเอ็ดยูโรมสามารถเข้าใช้และใช้งานเครือข่ายอินเทอร์เน็ตผ่านเครือข่ายของมหาวิทยาลัยราชภัฏเทพสตรีได้
3) นักศึกษา อาจารย์ และบุคลากรสามารถ เข้าเชื่อมต่อสัญญาณไวเลสแลนผ่านชื่อ SSID: eduroam โดยทุกสถาบันที่เป็นสมาชิกกับเอ็ดยูโรมกำหนดชื่อ SSID เหมือนกัน
4) บุคลากรหรือนักศึกษาใช้บัญชีผู้ใช้เดียวกันกับที่ใช้อยู่ในสถาบันของตนเองเพื่อยืนยันตัวบุคคลเมื่อเดินทางไปใช้ในสถาบันอื่นได้ทันที
5) สถาบันที่เป็นสมาชิกไม่ต้องลงทะเบียนหรือสร้างบัญชีสำหรับการใช้บริการเครือข่ายคอมพิวเตอร์ให้แก่บุคลากรหรือนักศึกษาของสถาบันที่เป็นสมาชิกอื่นที่เดินทางเข้ามาปฏิบัติภารกิจในพื้นที่
6) ผู้ดูแลระบบสามารถที่จะติดตั้งและแก้ไขไฟล์ที่จำเป็นสำหรับเซิร์ฟเวอร์สำหรับเอ็ดยูโรมเครื่องใหม่ในกรณีที่เครื่องเก่าไม่สามารถใช้งานได้โดยอัตโนมัติจากเว็บไซต์ เพื่อช่วยอำนวยความสะดวกให้กับผู้ดูแลระบบในการนำเอาระบบให้บริการ

บทที่ 2
ทฤษฎีและหลักการที่ใช้ในโครงการ

2.1 การพิสูจน์ตัวตน (Authentication) และการควบคุมสิทธิ์การใช้งาน (Authorization)

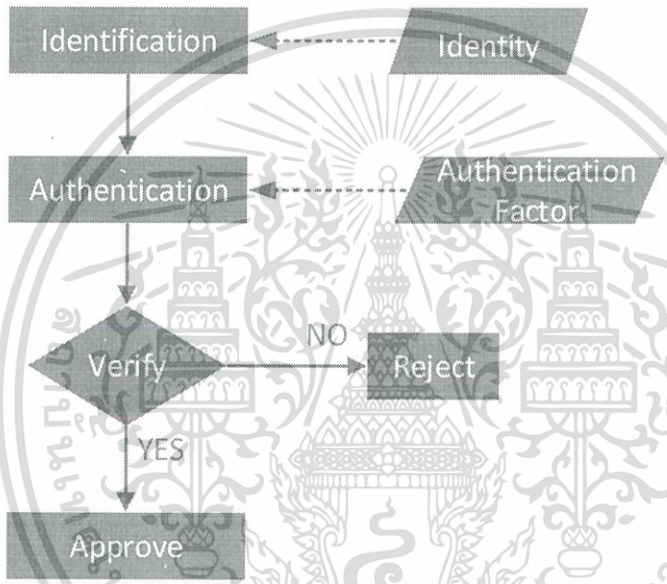
ในปัจจุบันระบบคอมพิวเตอร์ได้ถูกคุกคามมากขึ้นทั้งจากไวรัสคอมพิวเตอร์หรือ จากผู้ไม่ประสงค์ดีซึ่งระบบความมั่นคงปลอดภัยคอมพิวเตอร์ (Computer Security) ช่วยปกป้อง เครื่องคอมพิวเตอร์ อุปกรณ์ต่างๆที่เกี่ยวข้อง และช่วยปกป้องข้อมูลที่ได้จัดเก็บไว้ภายในระบบซึ่งจุดประสงค์หลักของความปลอดภัยทางข้อมูลคือ ความลับ(Confidentiality) ความสมบูรณ์ (Integrity) และความพร้อมใช้ (Availability) โดยมีรายละเอียดดังนี้

1) การรักษาความลับ คือการทำให้ข้อมูลสามารถเข้าถึงหรือ เปิดเผยได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้นเนื่องจากข้อมูลบางอย่างมีความสำคัญ และ จำเป็นต้องเก็บไว้เป็นความลับ เพราะถ้าถูกเปิดเผยอาจมีผลเสียหรือเป็นอันตรายต่อเจ้าของได้ (จตุชัย แพงจันทร์ 2553)
2) การรักษาความสมบูรณ์ คือการทำให้ข้อมูล มีความน่าเชื่อถือ ซึ่งข้อมูลนั้น ไม่ได้ถูกแก้ไขหรือเปลี่ยนแปลงจาก และ ความน่าเชื่อถือของแหล่งที่มา กลไกในการป้องกันนี้มีจุดมุ่งหมายเพื่อรักษาความถูกต้องของข้อมูลซึ่งทำได้ โดยการป้องกันความพยายามที่จะเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต หรือความพยายามที่จะเปลี่ยนแปลงข้อมูลในรูปแบบที่ไม่ถูกต้องหรือได้รับอนุญาต โดยใช้ การพิสูจน์ตัวตน และ การควบคุมการเข้าถึง จะเป็นกลไกที่ใช้สำหรับการป้องกันการบุกรุกประเภทแรกได้เป็นอย่างดี ส่วนการป้องกันความพยายามจากผู้ที่ได้รับอนุญาตนั้นต้องใช้ กลไกการตรวจสอบสิทธิ์ และ กลไกอื่นเพิ่มขึ้นมา (จตุชัย แพงจันทร์ 2553)
3) ความพร้อมใช้ คือการให้ผู้ที่ได้รับอนุญาตสามารถเข้าถึงข้อมูล หรือทรัพยากรได้เมื่อต้องการ ความพร้อมใช้งานเป็นส่วน หนึ่งของความมั่นคงของระบบ เนื่องจากการที่ระบบไม่พร้อมใช้งานก็จะแย่ พอๆกับการที่ไม่มีระบบเลย ส่วนหนึ่งของความพร้อมใช้งานที่เกี่ยวข้องกับการรักษา ความมั่นคงปลอดภัยคือ อาจมีผู้ไม่ประสงค์ดีพยายามที่จะทำให้ไม่สามารถเข้าถึงข้อมูลได้โดยการทำให้ระบบไม่สามารถใช้งานได้ การออกแบบระบบนั้นส่วนใหญ่จะใช้ข้อมูลทางด้านสถิติเกี่ยวกับรูปแบบหรือพฤติกรรมในการใช้งานระบบของผู้ใช้ ระบบจะถูกออกแบบเพื่อให้เหมาะสมกับสภาพแวดล้อมดังกล่าว ดังนั้น กลไกในการรักษาความ พร้อมใช้งานนั้นจะทำงานในกรณีที่ระบบไม่ได้ทำงานในสภาพที่ปกติหรือที่ออกแบบไว้ ซึ่งถ้ากลไกนี้ไม่ทำงานส่วนใหญ่ระบบจะล่มหรือไม่พร้อมใช้งาน (จตุชัย แพงจันทร์ 2553)

2.1.1 การพิสูจน์ตัวตน (Authentication)

การพิสูจน์ตัวตน คือขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง ในทางปฏิบัติจะแบ่งออกเป็น 2 ขั้นตอนคือ

1) การระบุตัวตน (Identification) คือขั้นตอนที่ผู้ใช้แสดงหลักฐานว่าตนเองคือใครเช่น ชื่อผู้ใช้ (username)
2) การพิสูจน์ตัวตน (Authentication) คือขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลที่กล่าวอ้างจริงในขั้นตอนนี้หน่วยงานจะต้องมีระบบที่ใช้ตรวจสอบหลักฐานของผู้ใช้งานเพื่อยืนยันว่าเป็นบุคคลนั้นจริง



รูปที่ 2.1 กระบวนการพิสูจน์ตัวตน

จากรูปที่ 2.1 แสดงกระบวนการพิสูจน์ตัวตนในขั้นแรกผู้ใช้จะทำการ แสดงหลักฐานที่ใช้ในการพิสูจน์ตัวตนต่อระบบซึ่งในขั้นตอนนี้คือการพิสูจน์ตัวตน และในขึ้นตอนต่อมา ระบบจะทำการตรวจสอบหลักฐานที่ผู้ใช้นำมากล่าวอ้าง ก็คือการพิสูจน์ตัวตนหลังจากระบบได้ ทำการตรวจสอบหลักฐานเรียบร้อยแล้วถ้าหลักฐานที่นำมากล่าวอ้างถูกต้องก็จะอนุญาตให้เข้าสู่ระบบได้ หากหลักฐานที่นำมากล่าวอ้างไม่ถูกต้องผู้ใช้จะถูกปฏิเสธการใช้งานระบบ หลักฐานที่ผู้ใช้นำมากล่าวอ้างที่เกี่ยวกับเรื่องของความปลอดภัยนั้นสามารถ จำแนกได้ 2 ชนิด (นิวัติ เนียมพลอย)

Actual identity คือหลักฐานที่สามารถบ่งบอกได้ว่าในความเป็นจริงบุคคลที่กล่าวอ้างนั้นเป็นใคร

Electronic identity คือหลักฐานทางอิเล็กทรอนิกส์ซึ่งสามารถบ่งบอกข้อมูล ของบุคคลนั้นได้ แต่ละบุคคลอาจมีหลักฐานทางอิเล็กทรอนิกส์ได้มากหนึ่งหลักฐาน

กลไกของการพิสูจน์ตัวตน มีข้อจำกัดในการใช้งาน สามารถแบ่งออกได้เป็น 3 กลุ่มคือ

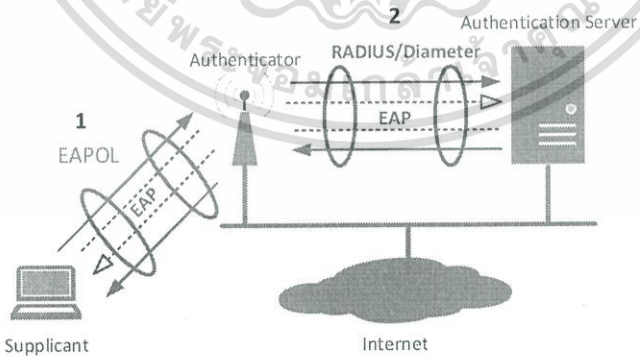
1. สิ่งที่มี (Possession factor) เช่นกุญแจหรือบัตรเครดิตเป็นต้น
2. สิ่งที่รู้(Knowledge factor)เช่น รหัสผ่านหรือการใช้เลขรหัสลับส่วนตัว (Personal Identification Number) เป็นต้น
3. สิ่งที่เป็น (Biometric factor) เช่น ลายนิ้วมือ รูปแบบเรตินา หรือใช้รูปแบบเสียงเป็นต้น

2.1.2 การกำหนดสิทธิ์การใช้งาน (Authorization)

ขั้นตอนนี้จะต่อจากการตรวจสอบตัวตันผู้ใช้งานและสามารถพิสูจน์ตัวตนได้แล้วนั้น ขั้นต่อไปก็จะตรวจสอบสิทธิ์การใช้งานว่าได้รับอนุญาตเข้าใช้งานระบบสารสนเทศได้หรือไม่ ซึ่งเรียกว่า การกำหนดสิทธิ์การใช้งาน (Authorization) ก็คือข้อจำกัดของบุคคลที่เข้ามาในระบบว่าสามารถทำอะไรกับระบบได้บ้าง เช่น กำหนดให้ บุคคลนั้นเป็นผู้ใช้งานทั่วไป สามารถอ่านข้อมูลได้อย่างเดียว ในขณะที่อีกคนจะสามารถอ่าน ลบ และแก้ไข ได้เป็นต้น (นิวัติ เนียมพลอย)

2.2 มาตรฐาน IEEE 802.1X และ RADIUS

มาตรฐาน 802.1X เป็นมาตรฐานสำหรับ MAC Address ที่ใช้ในการตรวจสอบผู้ใช้ (Authentication) เครือข่ายทั้งในระบบ LAN และ WLAN ให้มีความปลอดภัยสูงมากขึ้น ในกรณีที่มีผู้ขอใช้เครือข่ายจะต้องมีการแสดงหลักฐานประกอบการตรวจสอบ (Credential) กับอุปกรณ์แม่ข่าย (Authenticator) หลังจากนั้น Authenticator จะส่งหลักฐานดังกล่าวไปให้ Authenticator Server (RADIUS) ซึ่งเป็นระบบที่ใช้สำหรับทำการตรวจสอบข้อมูลผู้ใช้กับดาต้าเบส วิธีนี้จะเป็นไปตามโพรโทคอลที่เรียกว่า EAP (Extensible Authentication Protocol) (Paul, Arana.2006) ดังรูปที่ 2.2

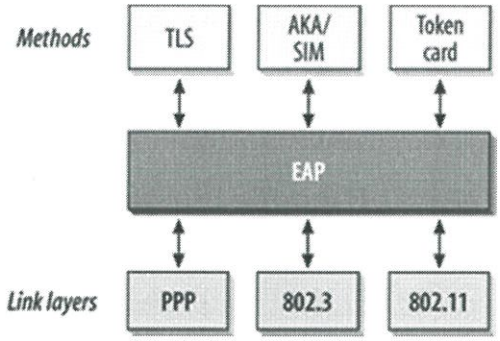


รูปที่ 2.2 กระบวนการทำงานของ 802.1X

2.2.1 EAP (Extensible Authentication Protocol)

EAP (Extensible Authentication Protocol) ถูกระบุไว้ใน RFC 2284 และนำไปใช้งานครั้งแรก กับ PPP (Point to Point Protocol) และได้มีการรองรับโพรโทคอล 802.3 และ 802.11 เพิ่มขึ้น

ในเวลา ต่อมา ซึ่ง EAP เป็นการ encapsulation ที่ทำงานอยู่บน Link Layer มีลักษณะสถาปัตยกรรม ดังรูปที่ 2.3



รูปที่ 2.3 สถาปัตยกรรม EAP

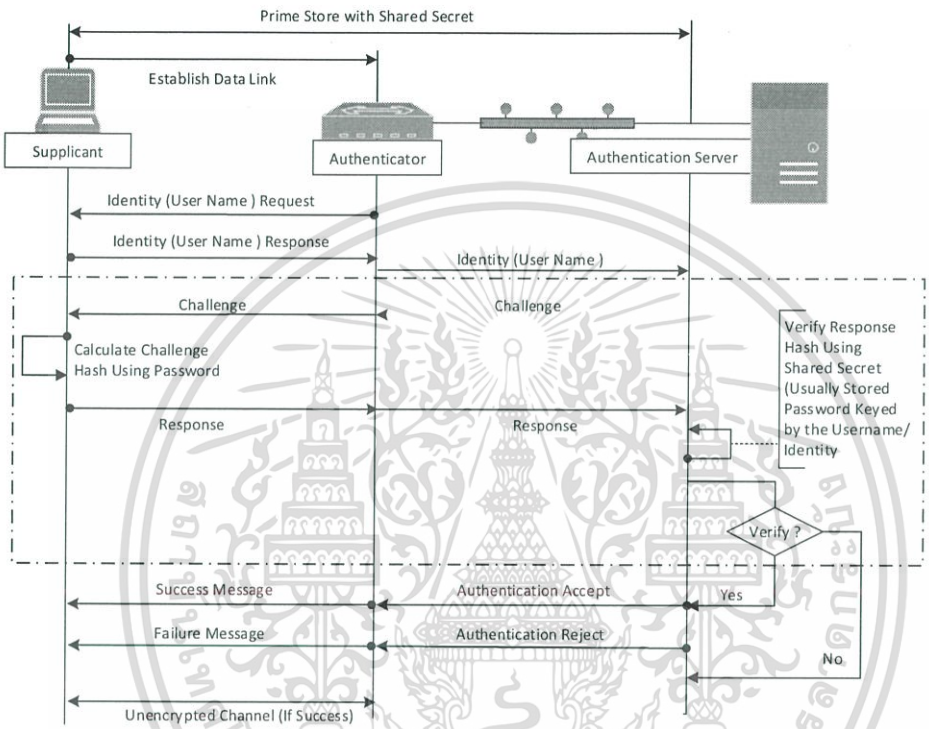
ซึ่งในปัจจุบันนี้ได้มีการพัฒนา โพรโทคอล EAP ขึ้นมาหลายรูปแบบสามารถแบ่งออกเป็น 4 รูปแบบหลักๆดังนี้

ตารางที่ 2.1 ตารางเปรียบเทียบโพรโทคอล EAP

Topic	EAP MD5	LEAP	EAP TLS	EAP TLS	EAP TTLS
Security Solution	Standards base	Proprietary	Standards base	Standards base	Standards base
Certificates Client	No	N/A	Yes	No	No
Certificates Server	No	N/A	Yes	Yes	Yes
Credential Security	None	Weak	Strong	Strong	Strong
Supported Authentication Databases	Requires clear-text database	Active Directory, NT Domains	Active Directory, LDAP, etc.	Active Directory ,NT Domain, Token, SQL, LDAP, etc.	Active Directory, LDAP,SQL, plain password file, Token Systems etc.
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Mutual Authentication	No	Yes	Yes	Yes	Yes

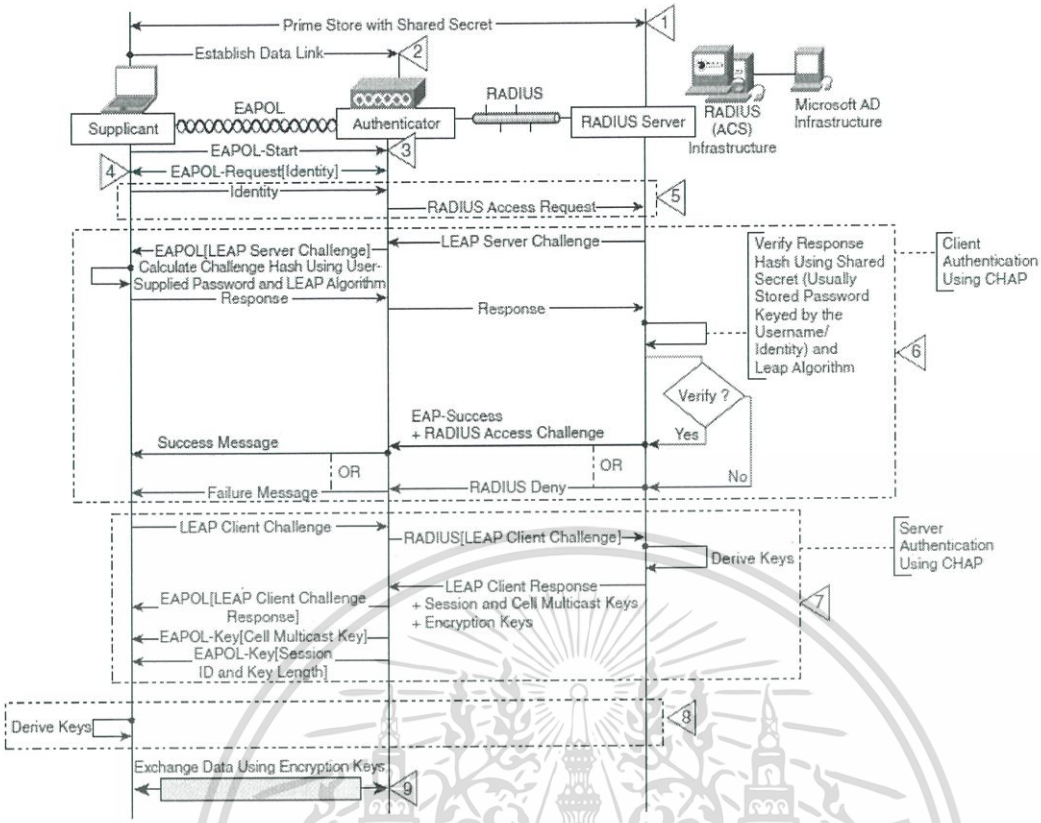
EAP-MD5 หลักฐานที่ส่งผ่านไปยังเรเดียสเซิร์ฟเวอร์ คือ ชื่อผู้ใช้งานและรหัสผ่าน ซึ่งจะถูกเข้ารหัสด้วยเทคนิคที่เรียกว่า MD5 การใช้กลไก EAP-MD5 ช่วยแก้ไขปัญหาเรื่องการตรวจสอบผู้ใช้ในเครือข่ายไร้สายให้มีความปลอดภัยมากขึ้น แต่ไม่ได้ช่วยแก้ไขปัญหาเรื่องความไม่ปลอดภัยของการใช้รหัสลับเครือข่าย (WEP Key) ซึ่งมีความคงที่ ดังนั้นผู้โจมตียังคงสามารถดักฟังและเจาะ

รหัสลับของเครือข่ายซึ่งมีความคงที่ได้ถึงแม้จะมีการใช้ EAP-MD5 เมื่อผู้โจมตีทราบรหัสลับของเครือข่ายแล้วก็จะสามารถเข้าใจข้อมูลที่รับส่งอยู่ในเครือข่ายและอาจทราบ ชื่อผู้ใช้งานและรหัสผ่าน โดยอาศัยเทคนิคต่างๆสำหรับการเจาะรหัส MD5 ได้ในที่สุดนอกจากนี้ข้อบกพร่องในกลไก EAP-MD5 อีกอย่างหนึ่งคือผู้ใช้ไม่สามารถตรวจสอบอุปกรณ์แม่ข่าย ซึ่งทำให้ผู้โจมตีอาจจะสามารถหลอกลวงให้ผู้ใช้ต่อเชื่อมเข้ากับอุปกรณ์แม่ข่ายของผู้โจมตีได้ ดังรูปที่ 2.4 (นิวัติ เนียมพลอย)



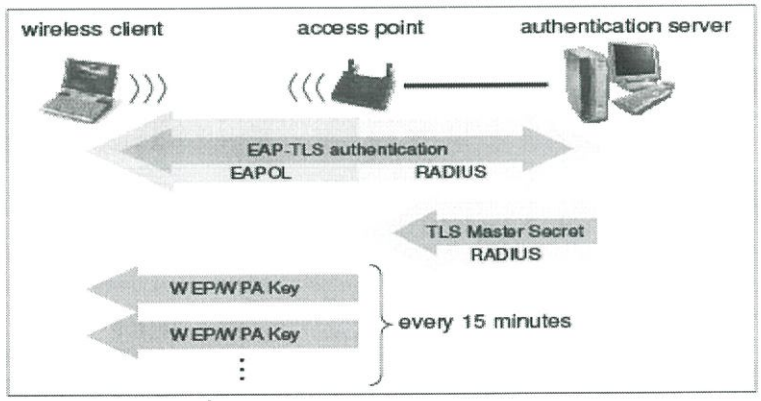
รูปที่ 2.4 กระบวนการทำงาน EAP-MD5

LEAP หรือ EAP-Cisco Wireless โพรโทคอล LEAP (Lightweight Extensible Authentication Protocol) จะใช้ ชื่อผู้ใช้งานและรหัสผ่าน เป็นหลักฐานในการตรวจสอบ มีการเปลี่ยนค่า WEP Key ไปเรื่อยๆ และผู้ใช้แต่ละคนจะได้รับ WEP Key เพื่อใช้เข้ารหัสที่แตกต่างกันเรเดียสเซิร์ฟเวอร์สามารถกำหนดอายุ Session ได้ เมื่อได้รับ Session ก็จะได้ WEP Key ใหม่ จึงดักจับ WEP Key ได้ยาก นอกจากนั้นยังสามารถตรวจสอบได้ทั้งฝั่ง เครื่องลูกข่าย และ Access Point ถูกจำกัดการใช้ในผลิตภัณฑ์ของ Cisco ดังรูปที่ 2.5 (นิวัติ เนียมพลอย)



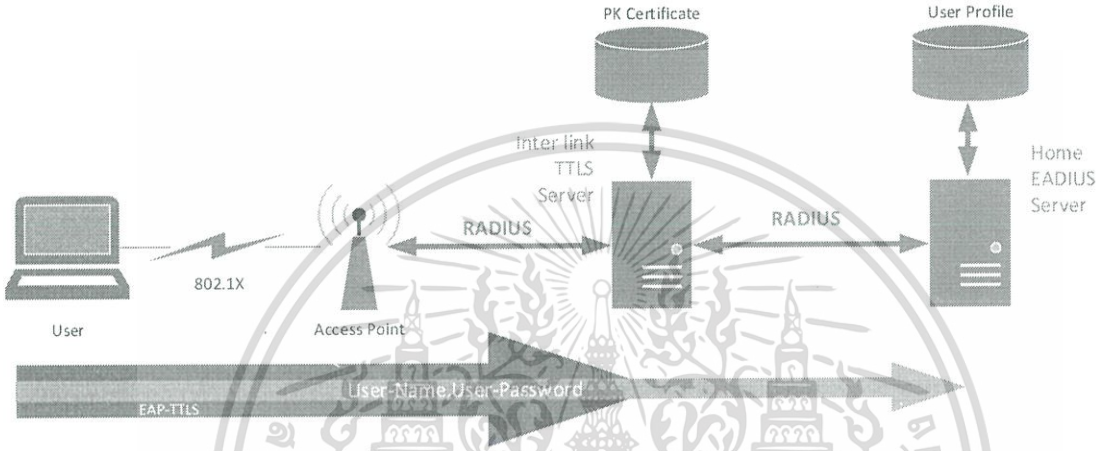
รูปที่ 2.5 กระบวนการทำงาน EAP-LEAP

EAP-TLS (Transport Layer Security) ได้รับการพัฒนาขึ้นโดยบริษัท Microsoft ซึ่งในโพรโทคอลนี้จะไม่มีการใช้ ชื่อผู้ใช้งานและรหัสผ่าน ในการตรวจสอบผู้ใช้ แต่จะใช้ X.509 certificates แทนซึ่งการทำงานของโพรโทคอลนี้จะอาศัยการส่งผ่าน PKI ผ่าน SSL (Secure Sockets Layers) มายัง EAP เพื่อใช้กำหนด WEP Key สำหรับผู้ใช้แต่ละคน EAP-TLS กำหนดให้มีการตรวจสอบทั้งเครื่องแม่ข่ายและผู้ใช้ (Mutual Authentication) ด้วยเช่นเดียวกับ LEAP แต่อย่างไรก็ตามปัญหาหลักของ EAP-TLS ความยุ่งยากและค่าใช้จ่ายในการติดตั้งจัดการและบริหารระบบ PKI Certificate ดังรูปที่ 2.6 (นิวัติ เนียมพลอย)



รูปที่ 2.6 กระบวนการทำงาน EAP-TLS

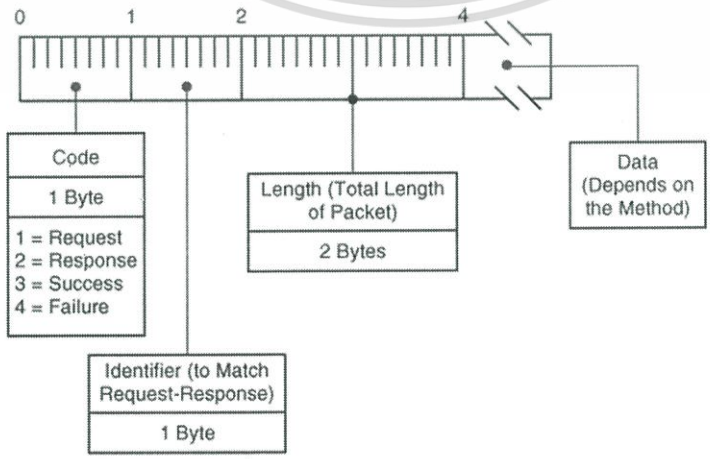
EAP-TTLS (EAP-Tunneled Transport Layer Security) ถูกเริ่มพัฒนาโดยบริษัท Funk Software ซึ่งการทำงานของ EAP-TTLS คล้ายกับ EAP-TLS คือจะมีการตรวจสอบเครื่องแม่ข่ายโดยใช้ Certificate แต่ผู้ใช้จะถูกตรวจสอบโดยการใช้ ชื่อผู้ใช้และรหัสผ่าน ซึ่งความปลอดภัยของ EAP-TTLS จะน้อยกว่า EAP-TLS และที่สำคัญ EAP-TTLS อาจไม่ได้รับความนิยมมากนักในเวลาต่อไปเนื่องจาก Microsoft และ Cisco ได้ร่วมมือกันพัฒนาโพรโทคอลขึ้นมาใหม่ชื่อว่า PEAP (Protected EAP) ซึ่งมีการทำงานเช่นเดียวกับ EAP-TLS ที่กล่าวมาแล้วข้างต้นดังรูปที่ 2.7 (นิวัติ เนียมพลอย)



รูปที่ 2.7 กระบวนการทำงาน EAP-TTLS

1) EAP Packet Format

เป็นรูปแบบของ EAP packet ที่ใช้โพรโทคอล PPP links ในระดับ Link Layers เพื่อนำเฟรม PPP โดยมีหมายเลขโพรโทคอล คือ 0xC227 ซึ่งโพรโทคอล EAP ไม่ได้รองรับการทำงานแค่โพรโทคอล PPP อย่างเดียว แต่ยังรองรับโพรโทคอล 208.3 และ 802.11 อีกด้วย (Krishna Sankar, Sri Sundaralingam, Darrin Miller, Andrew Balinsky. 2004)



รูปที่ 2.8 EAP packet format

code field : เป็นฟิลด์แรกของแพ็กเก็ตมีขนาด 1 ไบต์ ใช้ระบุชนิดของ EAP packet ซึ่งใช้ควบคู่กับ Data field ในการแปลความหมายของแพ็กเก็ตด้วย

code 1 : Request

code 2 : Response

code 3 : Success

code 4 : Failure

Identifier field : มีขนาด 1 ไบต์ ใช้ควบคู่กับ request, response ซึ่งถ้ามีการ retransmission ค่า Identifier จะเป็นค่าเดิม แต่ถ้าเป็นการส่งใหม่จะเป็นค่าใหม่

Length field : มีขนาด 2 ไบต์ ซึ่งเป็นระบุจำนวน แพ็กเก็ตทั้งหมดของเฟรม

Data field : ขนาดของฟิลด์ ขึ้นอยู่กับชนิดของแพ็กเก็ต, Data field อาจจะไม่มีก็ได้ แล้วแต่ชนิดของแพ็กเก็ตการแปลความหมายข้อมูลใน Data field ขึ้นอยู่กับค่าของ code field ว่าเป็นชนิดใด

2) EAP Requests and Responses

เป็นแพ็กเก็ตที่ใช้ในการ Requset และ Response ระหว่าง Access Client กับ Authenticatorโดยใน Code field ถ้าเป็น "1" จะใช้สำหรับ packet Request และ "2" จะใช้สำหรับ packet Response และค่าใน Identifier และ Length จะเป็นดังที่กล่าวในหัวข้อก่อนหน้านี้ และในส่วนของข้อมูลที่อยู่ใน Data field ก็ขึ้นอยู่ชนิดของแพ็กเก็ตนั้น (Krishna Sankar, Sri Sundaralingam, Darrin Miller, Andrew Balinsky. 2004)

Type field : มีขนาด 1 ไบต์ เป็นการแสดงลักษณะของการ request หรือ response ในแต่ละแพ็กเก็ตว่าตรงกันหรือไม่ เมื่อมีการส่ง packet request พร้อมกับ authentication method ออกไป packet response ที่ตอบกลับต้องตรงกับที่ต้องการ แต่ถ้าไม่ตรงกัน อุปกรณ์ปลายทางก็จะต้องมีการส่ง NAK เพื่อที่จะแนะนำ authentication method ใหม่มาให้ ค่า Type code ที่มีค่าเท่ากับ 4 หรือมากกว่า จะเป็นโค้ด ที่แสดง authentication method โดยมีค่า Type code ต่างๆดังนี้

Type code 1 : Identity โดยทั่วไป authenticator จะใช้ในแพ็กเก็ตแรกที่เริ่ม request และเป็นแพ็กเก็ตแรกที่ user response ตอบกลับ

Type code 2 : Notification เป็นโค้ดที่ authenticator ใช้ส่ง message ไปหาผู้ใช้เป็นการจัดเตรียมข้อมูลต่าง ๆ ให้ผู้ใช้ เช่น password expire เป็นต้น เมื่อมีการส่ง notification request มาแล้วต้องมีการส่ง response กลับด้วย ขนาดของ Type-Data มีขนาดเป็น 0

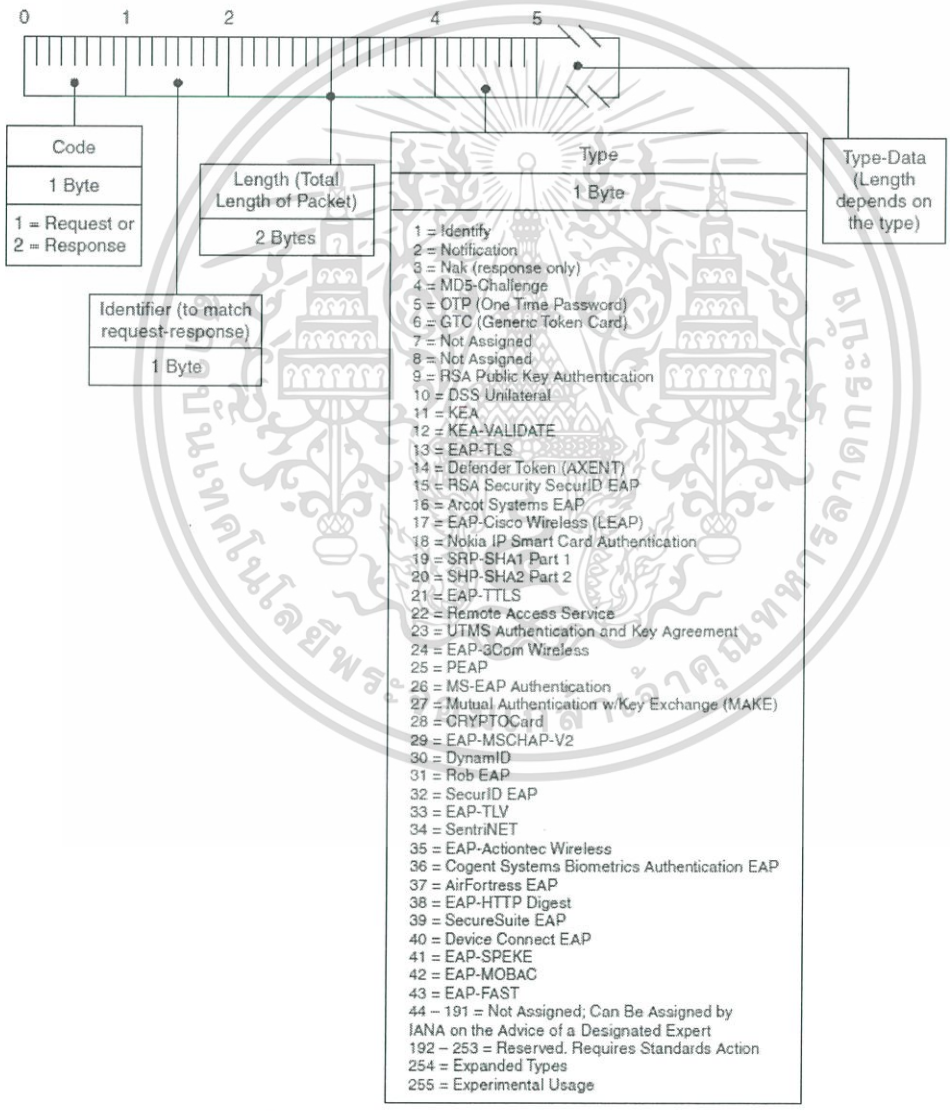
Type code 3 : NAK ใช้สำหรับแนะนำ authentication method ใหม่ เมื่อ authenticator ส่ง challenge โดยการเข้ารหัสตามชนิดของ type code นั้น (Type code 4 หรือ สูงกว่า) ถ้าผู้ใช้ไม่สามารถรองรับ method นั้นได้ user ก็จะส่ง NAK พร้อมทั้ง method ใหม่ที่ใส่ไว้ใน Type-Data กลับไปให้กับ authenticator

Type code 4 : MD-5 Challenge เป็นการใช้ MD-5 ในการทำ challenge ซึ่งมีระบุไว้ใน RFC1994 การ challenge ระหว่าง authenticator กับผู้ใช้จะใช้ shared secret ที่เราตั้งค่าให้เหมือนกันทั้งคู่ทำการ challenge โดย EAP ทุก protocol รองรับ MD-5 Challenge

Type code 5 : One-time password (OTP) เป็นการกำหนดโดย RFC 1938

Type code 6 : Generic Token Card เป็นการใช้ Token card เช่น RSA's Secure ID เป็นต้น

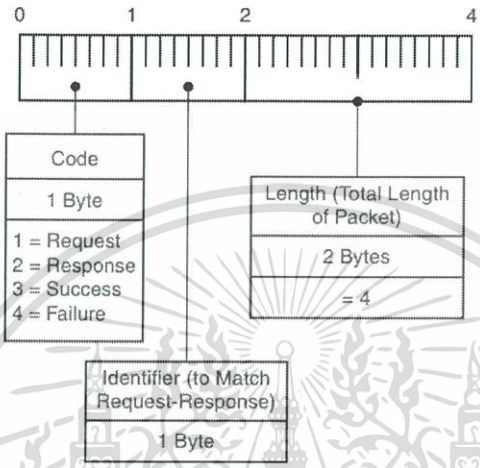
Type code 13 : TLS เป็นการใช้ Transport Layer Security สำหรับ authentication เพื่อป้องกันการดักจับแพ็กเก็ตและมีการทำ mutual authentication ด้วย Type-Data field : ขนาดและข้อมูลของ field นี้จะขึ้นอยู่กับ Type ของแพ็กเก็ตนั้นๆ



รูปที่ 2.9 EAP Request and Response packets

3) EAP Success and Failure

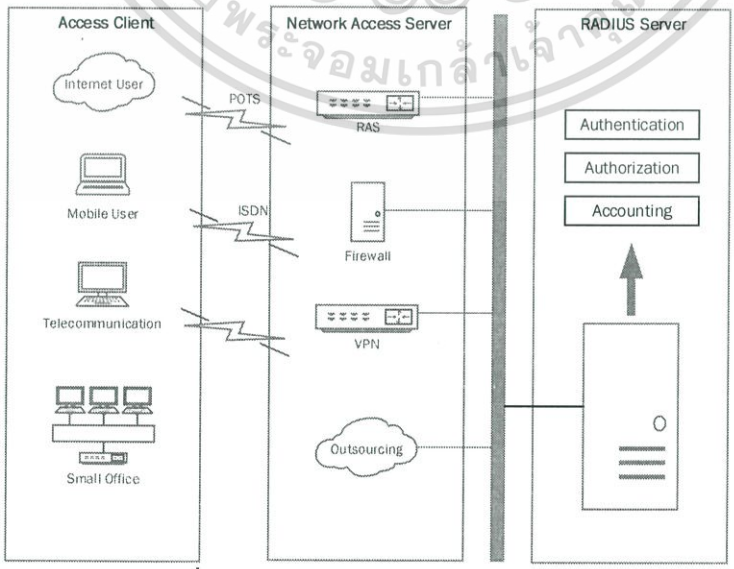
สุดท้ายแล้วเมื่อมีการทำ EAP exchange เสร็จแล้ว ผลที่ผู้ใช้ได้รับ ก็คือ Success หรือไม่ก็ Fail ซึ่ง authenticator จะพิจารณาจากการแลกเปลี่ยนข้อมูลกันว่าสำเร็จหรือไม่ โดย Success (code3) หรือ Failure (code 4) ดังรูปที่ 2.10 (Krishna Sankar, Sri Sundaralingam, Darrin Miller, Andrew Balinsky. 2004)



รูปที่ 2.10 EAP Success and Failure packets

2.2.2 RADIUS (Remote Authentication Dial-In User Service)

เรเดียส เป็นผลงานของ Livingston Enterprises เพื่อรวบรวมบัญชีผู้ใช้ไว้เพียงที่เดียวซึ่งง่ายต่อการบริหารจัดการ มีหน้าที่ตรวจสอบรหัสผู้ใช้และรหัสผ่าน ให้สิทธิ์การเข้าถึง และขึ้นบัญชี AAA (Authentication, Authorization, Accounting) สำหรับผู้ใช้ที่ทำการขอเข้าใช้งานเครือข่าย



รูปที่ 2.11 โครงสร้างการทำงานเรเดียส

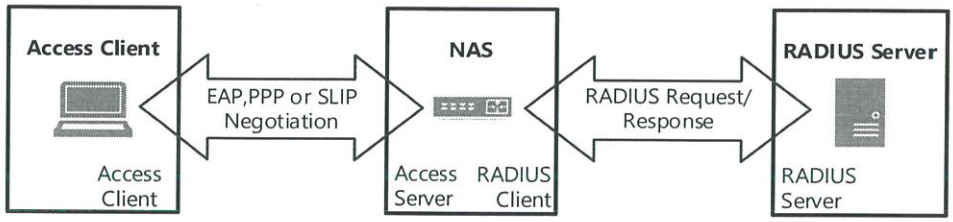
เรเดียสได้มีการกำหนดพอร์ตอย่างเป็นทางการโดยใช้ UDP พอร์ต 1812 สำหรับ การทำ RADIUS Authentication และใช้ UDP พอร์ต 1813 สำหรับการทำ RADIUS Accounting ซึ่งกำหนดโดย Internet Assigned Numbers Authority อย่างไรก็ตาม ก่อนที่จะมีการนำพอร์ต 1812 และ 1813 มาใช้ ได้มีการใช้พอร์ต 1645 และ 1646 มาก่อนถึงแม้จะไม่ได้ระบุอย่างเป็นทางการแต่ก็ได้กลายมาเป็นพอร์ตพื้นฐานในการทำ RADIUS Client/Server ในเวลาต่อมา องค์ประกอบพื้นฐานของ RADIUS Server (Remote authentication dial-in user service server) มีดังนี้

Access Clients คือ เครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ผู้ใช้งานสั่งให้ติดต่อระบบเพื่อใช้งาน โดยใช้ โปรแกรม Dial-Up Net working สั่งงาน Modem ให้เชื่อมต่อ เพื่อใช้งานอินเทอร์เน็ต

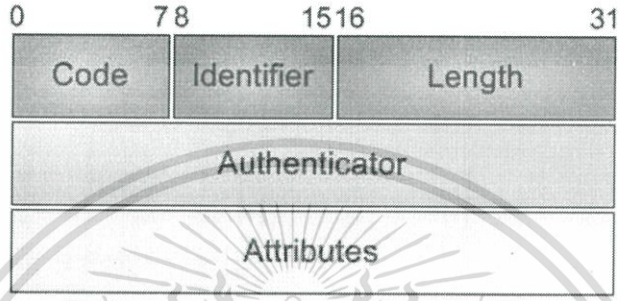
Network Access Servers (NAS) คือ อุปกรณ์ที่ทำหน้าที่เชื่อมต่อและจัดการการติดต่อระหว่าง Access Clients และ RADIUS Server ซึ่ง NAS จะทำหน้าที่เป็นเครื่องลูกข่าย เชื่อมต่อกับเรเดียสเซิร์ฟเวอร์ส่งผ่านและจัดการข้อมูลที่ใช้ในการตรวจสอบสิทธิ์ กำหนดสิทธิ์ ของ Access Clients เมื่อ Access Clients ร้องขอการต่อเชื่อมซึ่งจะต้องต่อเชื่อมมายัง NAS ผ่านโพรโทคอลที่ใช้ในการต่อเชื่อมต่าง ๆ เช่น PPP (Point-to-Point Protocol), SLIP (Serial Line Internet Protocol), Extensible Protocol อื่น ๆ เป็นต้น ซึ่งจำเป็นต้องมีการส่งผ่านชื่อผู้ใช้และรหัสผ่านจาก Access Clients มายัง NAS หลังจากนั้น NAS จะส่งข้อมูลที่จำเป็นต่าง ๆ เช่น Username, Password, NAS IP Address, NAS Port Number และข้อมูลอื่น ๆ ไปที่เรเดียสเซิร์ฟเวอร์เพื่อขอตรวจสอบสิทธิ์ (Request Authentication)

เรเดียสเซิร์ฟเวอร์ทำการตรวจสอบสิทธิ์โดยใช้ข้อมูลที่ NAS ส่งมา (Access-Request) กับข้อมูลที่จัดเก็บไว้ในเรเดียสเซิร์ฟเวอร์เอง หรือจากฐานข้อมูลภายนอก อื่น ๆ เช่น MS SQL Server, Oracle Database, LDAP Database หรือ RADIUS Server อื่น (ซึ่งเรียกการส่งผ่านการตรวจสอบสิทธิ์แบบนี้ว่า Proxy)

ในกรณีที่ข้อมูลทั้งหมดถูกต้องเรเดียสเซิร์ฟเวอร์จะส่งผลยินยอมการเชื่อมต่อ (Access-Accept) หรือ ไม่ยินยอม (Access-Reject) ในกรณีที่ข้อมูลไม่ถูกต้อง แก่ NAS หลังจากนั้น NAS จะเชื่อมต่อหรือยกเลิกการการต่อเชื่อมตามผลที่ได้รับจาก เรเดียสเซิร์ฟเวอร์ซึ่งตามปรกติแล้ว NAS จะขอบันทึกข้อมูลต่าง ๆ เช่น วันที่ เวลา ชื่อผู้ใช้ และข้อมูลอื่น ๆ ไปที่ เรเดียสเซิร์ฟเวอร์(Accounting Request) เพื่อให้ เรเดียสเซิร์ฟเวอร์จัดเก็บข้อมูลหรือส่งต่อไปที่ เรเดียสเซิร์ฟเวอร์อื่น จัดเก็บเพื่อใช้ในการประมวลผลอื่น ๆ ต่อไปดังรูปที่ 2.12



รูปที่ 2.12 การทำงานการส่งข้อมูลระหว่าง Access Client, NAS, RADIUS Server



รูปที่ 2.13 RADIUS Packet Type

1) รูปแบบข้อมูลของ RADIUS

เป็นรูปแบบ แพ็กเก็ตข้อมูลของ เรเดียสโดยแต่ละแพ็กเก็ตของเรเดียสนั้นจะใช้การส่งข้อมูลแบบ UDP Packet โดยจะมีฟิลด์ต่าง ๆ ดังนี้

Code : มีขนาด 1 ไบต์ ใช้แสดงรูปแบบของ RADIUS Message ถ้าฟิลด์นี้ไม่ถูกต้องจะถูกทำการยกเลิกโดยไม่ต้องมีการแจ้งมีรูปแบบดังนี้

1 = Access-Request

2 = Access-Accept

3 = Access-Reject

4 = Accounting-Request

5 = Accounting-Response

11 = Access-Challenge

12 = Status-Server

13 = Status-Client

255 = Reserved

Identifier field : เป็นฟิลด์ที่ช่วยเหลือในการ request และ reply ซึ่งมีค่าเดียวกับ message request และ reply

Length : บ่งบอกถึงความยาวของ แพ็กเก็ตโดยรวมทุก ๆ ฟิลด์

Authenticator : ใช้ในการตรวจสอบสิทธิ์โดยจะตอบกลับจาก เรเดียสเซิร์ฟเวอร์โดย Access Request Packet ของเครื่องลูกข่ายนั้นจะประกาบอด้วยเลขฐาน 8 จำนวน 16 หลัก ใช้ในการระบุว่าเป็น message ที่ส่งกลับจาก เรเดียสเซิร์ฟเวอร์ที่ถูกต้อง โดยค่านี้ใน Access-Request packet จะเป็นค่า RADIUS Client สุ่มขึ้นมา และนำค่านี้ไปเข้ารหัสลับกับรหัสผ่านของผู้ใช้ ด้วยคีย์ที่ตรงกันทั้ง client และ server และผลที่ได้จะนำไปใส่ใน Attributes username/password ใน message Access-Request

Attributes : เป็นส่วนที่บ่งบอกว่าข้อมูลต่างๆ ซึ่งมาความจำเป็นในการติดต่อกันระหว่าง RADIUS node ในระบบเพื่อจะทำการ Authentication, Authorization, configuration ซึ่งได้มีมาตรฐานกำหนดไว้ใน RFC 2138 ที่สำคัญดังนี้

Access-Request RADIUS Client จะทำการส่งเพื่อร้องขอ การตรวจสอบและขออนุมัติเพื่อทำการเชื่อมต่อเข้ากับ เครือข่าย Access-Request ช่วยให้ RADIUS Client สามารถเชื่อมต่อ แบบพิเศษได้ Access-Request จำเป็นต้องมีข้อมูล ที่จำเป็นในระบุ RADIUS Client เพื่อสิทธิ์ที่จะขอการตรวจสอบและมีความต้องการพิเศษ

Access-Challenge จะส่งโดย เรเดียสเซิร์ฟเวอร์เพื่อตอบกลับของ Access-Request Message เมื่อต้องการข้อมูลเพิ่มเติม ที่จำเป็นเพื่อดำเนินการตรวจสอบหรืออนุมัติ

Access-Accept จะส่งโดย เรเดียสเซิร์ฟเวอร์ใช้ในการตอบกลับของ Access-Request Message เพื่อบอก RADIUS Client ถึงสิทธิ์ในการเชื่อมต่อ Access-Accept สามารถกำหนดค่าและข้อมูลในการเชื่อมต่อได้

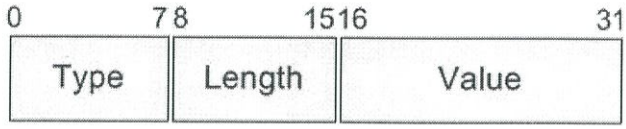
Access-Reject จะส่งโดย เรเดียสเซิร์ฟเวอร์ใช้ในการตอบกลับของ Access-Request Message เพื่อบอก RADIUS Client ถึงการปฏิเสธ การเชื่อมต่อ RADIUS Server จะส่งข้อความนี้หากสิทธ์ในการเชื่อมต่อไม่เป็นจริงหรือไม่มีสิทธิ์ในการเชื่อมต่อ

Accounting-Request จะส่งโดย RADIUS Client เพื่อร้องขอข้อมูล Accounting เพื่อการเชื่อมต่อที่ได้รับการยอมรับ

Accounting-Response เรเดียสเซิร์ฟเวอร์จะเป็นผู้ส่ง เพื่อตอบกลับ Accounting-Request Message เพื่อให้ RADIUS Client ได้รับ Accounting-Request Message ที่สำเร็จและประมวลผล

2) RADIUS Attributes Format

RADIUS Attribute Value Pairs (AVP) ใช้ในการเก็บข้อมูลการร้องขอ และการตอบสนองสำหรับการทำ authentication, authorization, and accounting ค่าความยาวของ RADIUS packet ใช้ในการบ่งบอกถึงจุดสิ้นสุดของ AVPs



รูปที่ 2.14 RADIUS Attributes

ตารางที่ 2.2 RADIUS Attributes Code List

AVP Type	Assignment	AVP Type	Assignment
1	User-Name	45	Acct-Authentic
2	User-Password	46	Acct-Session-Time
3	CHAP-Password	47	Acct-Input-Packets
4	NAS-IP-Address	48	Acct-Output-Packets
5	NAS-Port	49	Acct-Terminate-Cause
6	Service-Type	50	Acct-Multi-Session-Id
7	Framed-Protocol	51	Acct-Link-Count
8	Framed-IP-Address	52	Acct-Input-Gigawords
9	Framed-IP-Netmask	53	Acct-Output-Gigawords
10	Framed-Routing	55	Event-Timestamp
11	Filter-Id	60	CHAP-Challenge
12	Framed-MTU	61	NAS-Port-Type
13	Framed-Compression	62	Port-Limit
14	Login-IP-Host	63	Login-LAT-Port
15	Login-Service	64	Tunnel-Type
16	Login-TCP-Port	65	Tunnel-Medium-Type
18	Reply-Message	66	Tunnel-Client-Endpoint
19	Callback-Number	67	Tunnel-Server-Endpoint
20	Callback-Id	68	Acct-Tunnel-Connection-ID
22	Framed-Route	69	Tunnel-Password
23	Framed-IPX-Network	70	ARAP-Password
24	State	71	ARAP-Features
25	Class	72	ARAP-Zone-Access
26	Vendor-Specific	73	ARAP-Security
27	Session-Timeout	74	ARAP-Security-Data

ตารางที่ 2.2 (ต่อ)

28	Idle-Timeout	75	Password-Retry
29	Termination-Action	76	Prompt
30	Called-Station-Id	77	Connect-Info
31	Calling-Station-Id	78	Configuration-Token
32	NAS-Identifier	79	EAP-Message
33	Proxy-State	80	Message-Authenticator
34	Login-LAT-Service	81	Tunnel-Private-Group-ID
35	Login-LAT-Node	82	Tunnel-Assignment-ID
36	Login-LAT-Group	83	Tunnel-Preference
37	Framed-AppleTalk-Link	84	ARAP-Challenge-Response
38	Framed-AppleTalk-Network	85	Acct-Interim-Interval
39	Framed-AppleTalk-Zone	86	Acct-Tunnel-Packets-Lost
40	Acct-Status-Type	87	NAS-Port-ID
41	Acct-Delay-Time	88	Framed-Pool
42	Acct-Input-Octets	90	Tunnel-Client-Auth-ID
43	Acct-Output-Octets	200	IETF-Token-Immediate
44	Acct-Session-Id		

Attributes ที่สำคัญคือ

Service-type เป็น Attribute ที่ใช้กำหนดชนิดของ service ที่ผู้ใช้ร้องขอ เช่น Login, Framed, Callback login, Callback framed, Outbound, Administrative, NAS prompt เป็นต้น

Framed-MTU เป็นการกำหนดค่าหน่วยในการส่งข้อมูลสูงสุดสำหรับผู้ใช้งาน

Login-IP-Host เป็น Attribute ที่ใช้บอกเครื่องแม่ข่ายของระบบที่ผู้ใช้งานทำการเชื่อมต่อ

Login-Service เป็น Attribute ที่ใช้บ่องบอกถึงบริการที่จะให้ผู้ใช้งานล็อกอินเข้าใช้งาน เช่น Telnet, Rlogin เป็นต้น

Callback-Number เป็น Attribute ที่ใช้ในการกำหนดหมายเลขโทรศัพท์ที่ใช้ในการ callback

Frame-Route เป็น Attribute ที่ใช้บอกข้อมูลการหาเส้นทางการเชื่อมต่อ ให้ผู้ใช้งาน เช่น destination address หรือ gateway address

Session-Timeout เป็น Attribute ที่ใช้ในการตั้งค่าสูงสุดในหน่วยวินาทีที่จะอนุญาตให้มีการส่งผ่านข้อมูล ก่อนจะทำการยกเลิกการเชื่อมต่อของ session หรือตอบกลับจาก prompt

Idle-Timeout เป็น Attribute ที่ใช้กำหนดตั้งค่าสูงสุดในหน่วยวินาทีที่จะอนุญาตให้มีการส่งผ่านข้อมูล ก่อนจะทำการยกเลิกการเชื่อมต่อ

Termination-Action เป็น Attribute ใช้กำหนดการบ่งชี้ว่าเมื่อสิ้นสุดการใช้บริการแล้ว NAS แล้วจะทำงานอย่างไรต่อ

Calling-Station-ID เป็น Attribute ที่ใช้บ่งบอกถึง calling party number

Proxy-State เป็น Attribute ที่ถูกส่งโดย proxy server ไปยัง server อื่นเมื่อ proxy server ทำการส่งผ่าน Access-Request message

NAS-Port-Type เป็น Attribute ที่ใช้ชี้ถึง physical port ของ NAS ซึ่งใช้ในการทำงานตรวจสอบผู้ใช้งาน ยกตัวอย่างเช่น asynchronous, synchronous, ISDN เป็นต้น

3) Password Protocol

เนื่องจากการส่ง Access-Request ในขณะที่มีการขอ Authentication มีการส่งรหัสผ่านจาก NAS ไปยัง เรเดียสเซิร์ฟเวอร์จึงจำเป็นต้องคำนึงถึงความปลอดภัยของ รหัสผ่าน ดังกล่าว ดังนั้นจึงมีการสร้างโพรโทคอลสำหรับใช้งานในส่วนนี้ขึ้นซึ่ง ได้แก่

1) PAP (Password Authentication Protocol) ในขณะที่มีการขอเชื่อมต่อ(User Negotiates) จาก Access Clients มายัง NAS การส่งรหัสผ่านในขั้นตอนนี้จะยังไม่มีการเข้ารหัส (encrypt) ใด ๆ รหัสผ่านจะจัดส่งในรูปแบบ “Clear Text” เมื่อ NAS รวบรวมข้อมูลที่เพียงพอสำหรับสร้าง Access-Request แล้ว NAS จะ Encrypt Password โดยใช้ Authentication Shared Secret ที่ถูกกำหนดไว้ แล้วส่ง Access-Request ดังกล่าวไปยัง RADIUS Server เมื่อ RADIUS Server ได้รับ Access-Request จาก NAS แล้วจะทำการ Decrypt Password ที่ได้รับโดยใช้ Authentication Shared Secret ที่จัดเก็บไว้สำหรับ NAS ตัวดังกล่าวโพรโทคอล PAP สามารถใช้ได้กับเรเดียสเซิร์ฟเวอร์ทุกตัว

2) CHAP (Challenge Handshake Authentication Protocol) สำหรับ CHAP ได้ถูกสร้างขึ้นเพื่อหลีกเลี่ยงการส่งรหัสผ่านแบบ “Clear Text” ในขณะที่ User Negotiates เมื่อ NAS รับทราบแล้ว NAS จะสร้าง Challenge โดยสุ่มตัวอักษร แล้วส่งกลับไปยัง Access Clientเมื่อ Access Client ได้รับ Challenge จะทำการสร้าง Digest คือ นำ Challenge ที่ได้รับมาต่อท้ายรหัสผ่านแล้วทำการ Encrypt แบบ one-way Encryption (MD5 Algorithm) แล้วส่ง Digest นั้นแทนรหัสผ่านไปยัง NAS และ NAS จะสร้าง Access-Request สำหรับการ Authentication และส่งไปยังเนื่องจาก Digest ถูกสร้างแบบ one-way Encryption ไม่สามารถ Decrypt ได้เรเดียสเซิร์ฟเวอร์จึงจำเป็นต้องใช้ Attribute ที่เกี่ยวกับ CHAP Protocol ที่ถูกจัดส่งมาใน Access-Request Package ที่ได้รับจาก NAS ซึ่งมี 2 Attributes ที่เกี่ยวข้องดังนี้

CHAP-Password : Attribute สำหรับ Digest (รหัสผ่านที่ต่อท้ายด้วยChallenge แล้ว Encrypt ด้วย MD5 Algorithm)

CHAP-Challenge: Attribute สำหรับ Challenge ที่ถูกสุ่มขึ้นโดย NAS

เรเดียสเซิร์ฟเวอร์ใช้ Challenge จาก CHAP-Challenge ต่อท้ายรหัสผ่านที่จัดเก็บไว้นำมา Encrypt ด้วยวิธี MD5 แล้วเปรียบเทียบกับ CHAP-Password ที่ได้รับ

3) MS-CHAP และ MS-CHAP-V2 MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) ทั้ง 2 เวอร์ชัน ของ MS-CHAP ใช้วิธีการของโพรโทคอล CHAP แต่มีส่วนเพิ่มเติมขึ้นโดย Microsoft ข้อมูลเพิ่มเติมให้ดูที่ RFC 2433 2548 และ 2759

2.3 เอ็ดยูโรม (Eduroam)

Eduroam ย่อมาจาก "educational roaming" เป็นเครื่องหมายที่จดทะเบียนโดย TERENA ที่ก่อกำเนิดจากเครือข่ายการศึกษาและวิจัยของยุโรป (NRENs) เพื่อการใช้งานเครือข่ายที่เรียบง่าย ปลอดภัย และรองรับผู้ใช้งานที่ขยายตัวเพิ่มมากขึ้นได้

โดยเอ็ดยูโรมเป็นบริการเครือข่ายโรมมิ่งเพื่อการศึกษาและวิจัยสำหรับนักศึกษาและบุคลากรของสถาบันการศึกษาที่เป็นสมาชิกเครือข่ายเอ็ดยูโรม เพื่ออำนวยความสะดวกในการใช้งานเครือข่ายอินเทอร์เน็ตได้ โดยอยู่ภายใต้เงื่อนไขการใช้งานของสถาบันผู้ให้บริการเครือข่าย (Service Provider)

เอ็ดยูโรมเริ่มต้นขึ้นในปี 2546 จากการสาธิตความเป็นไปได้สำหรับการให้บริการงานเครือข่ายโรมมิ่งข้ามเครือข่าย โดยการใช้มาตรฐาน 802.1X ทำงานร่วมกับเรเดียสเซิร์ฟเวอร์ของแต่ละสถาบันเพื่อให้บริการกับนักศึกษาและนักวิจัยจากสถาบันสมาชิกจาก 5 ประเทศ ประกอบด้วย เนเธอเลนด์ ฟินแลน โปรตุเกส โครเอเชีย และสหราชอาณาจักร

สำหรับในประเทศไทย สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา (UniNet) จะทำหน้าที่เป็นผู้ดำเนินการหลักของประเทศไทย (National Roaming Operator for Thailand) โดยเป็นผู้รับผิดชอบการให้บริการ เอ็ดยูโรมสำหรับประเทศไทย และเป็นผู้กำหนดนโยบายการใช้งานระดับประเทศ โดย เอ็ดยูโรมในประเทศไทยมีการให้บริการเอ็ดยูโรมเป็นครั้งแรก ในงาน Asia-Pacific Advanced Network (APAN) ครั้งที่ 33 ที่จัดขึ้นในเดือนกุมภาพันธ์ พ.ศ. 2555 โดยมีประเทศไทยเป็นเจ้าภาพ

เอ็ดยูโรมมีการทำงานบนพื้นฐานของมาตรฐาน 802.1X ร่วมกับกลุ่มของ เรเดียสพร็อกซีเซิร์ฟเวอร์ ซึ่งมีการจัดกลุ่มตามลำดับชั้น โดยเรเดียสเซิร์ฟเวอร์แต่ละเครื่องจะทำหน้าที่ในการส่งต่อข้อมูลการพิสูจน์ตัวตนจากเครือข่ายผู้ให้บริการ (Service Provider) ไปยังเครือข่ายต้นสังกัดของผู้ใช้งานเพื่อยืนยันสิทธิ์การเข้าใช้งานเครือข่ายของผู้ใช้ (สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา)

2.4 LDAP (Lightweight Directory Access Protocol)

เป็นโพรโทคอลที่พัฒนามาจาก Protocol X.500 ซึ่งใช้ในการเข้าถึงและอัปเดตข้อมูลของไดเรกทอรีซึ่งในทางคอมพิวเตอร์ที่จริงก็อาจเรียกได้ว่าเป็นดาต้าเบสแบบพิเศษหรือ Data repository ที่บรรจุรายละเอียดของออบเจ็กต์ต่างๆ เช่น Users, Application, Files, Printer และอื่นๆ รวมทั้ง Security information ของออบเจ็กต์เหล่านี้ด้วย โดยข้อแตกต่างของไดเรกทอรี กับ ดาต้าเบสปกติ ได้แก่ (OpenLDAP Software 2.4 Administrator's Guide)

Operation: ในไดเรกทอรีจะเน้นที่การแอกเซสข้อมูลหรือ อ่านข้อมูล มากกว่าอัปเดต หรือเขียนข้อมูล ในขณะที่ ดาต้าเบส ทั่วไปจะเน้นการอัปเดตมากกว่า

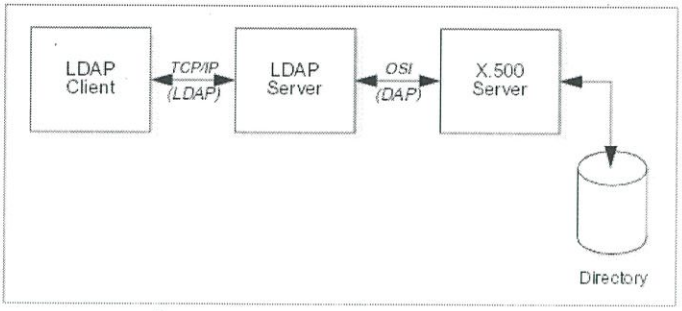
Transaction: ในดาต้าเบสจะรองรับการทำ Transaction หรือการอัปเดตข้อมูลสองจุดที่ต้องสอดคล้องกัน แบบ All-or-nothing เช่นการโอนเงินจากบัญชีหนึ่ง ไปอีกบัญชีหนึ่ง ที่ต้องการความสมบูรณ์ทั้ง 2 ฝั่ง หรือไม่ก็ไม่ต้องทำเลย ในขณะที่ไดเรกทอรีที่เน้นการอ่านอย่างเดียว อาจจะไม่ต้องการความสอดคล้องกันของข้อมูลบ้างนัก เช่นเมื่อมีการย้ายที่อยู่ระหว่างคน 2 คน ก็ต้องมีการปรับเปลี่ยนเบอร์ติดต่อของ 2 คนนั้น ซึ่งตรงนี้อาจจะไม่จำเป็นต้องทำทันที อย่างไรก็ตามฟีเจอร์นี้อาจจะมีการผนวกเข้ากับ LDAP Product ใหม่ๆ ในอนาคตก็ได้

Data Accuracy: ไดเรกทอรีอาจจะมีข้อจำกัดในการจัดเก็บข้อมูลที่ไม่สมบูรณ์ เช่น มีแต่ชื่อไม่มีที่อยู่ แต่อย่างไรก็ตาม เราสามารถ Configure คุณสมบัติเหล่านี้ได้ในบาง Directory Service

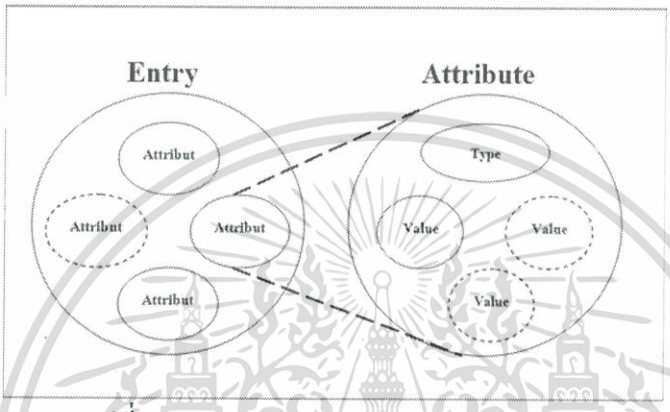
Query: ไดเรกทอรีไม่ Support Query String (SQL, Structured Query Language) อย่างไรก็ตามถึงแม้ ไดเรกทอรีจะมีคุณสมบัติด้อยกว่า Database หลายประการ แต่เนื่องจากโพรโทคอลที่ใช้ในการเข้าถึง ไดเรกทอรีเช่น LDAP มีความเร็วในการเข้าถึงข้อมูลสูง และก็ทำให้ Application ที่ทำงานบนโพรโทคอลเหล่านี้สามารถเข้าถึงข้อมูลอย่างรวดเร็ว ทำให้ระบบไดเรกทอรีเป็นที่ยอมรับและนำมาใช้งานทั่วไป

2.4.1 การทำงานของ LDAP

LDAP ได้รับการออกแบบมาให้อยู่บน TCP/IP Layer ที่มีเพียง 4 Layer ทำให้มีความต้องการ Resource น้อยกว่า DAP ของมาตรฐาน X.500 อย่างไรก็ตาม หากมีความต้องการติดต่อกันระหว่าง LDAP Client กับ X.500 Server จำเป็นจะต้องมีการติดต่อผ่าน Gateway ที่เรียกว่า LDAP Server จะทำงานแบบ Client/Server โดยทาง Client จะมีการลงโปรแกรมไว้ เมื่อต้องการข้อมูลจากเซิร์ฟเวอร์ก็จะทำการส่ง Request โดยจะผ่านโพรโทคอล TCP/IP เมื่อทาง Server ได้รับ Request แล้ว จะทำการประมวลผลตามที่เครื่องลูกข่ายต้องการ และส่ง Result กลับไปให้ Client LDAP ไม่เพียงแค่ทำงานแบบ Client/Server เท่านั้น ยังสามรถทำงานแบบ Messages-Oriented ได้อีก



รูปที่ 2.15 แสดงการติดต่อระหว่าง LDAP



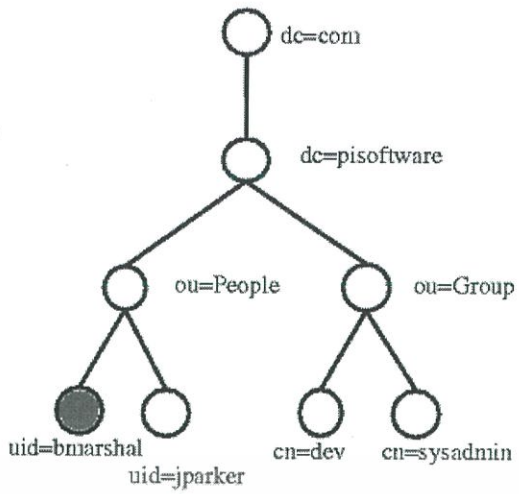
รูปที่ 2.16 LDAP Information Storage Entry

ข้อมูลพื้นฐานของ LDAP ประกอบด้วย 1 attribute หรือมากกว่า 1 attribute ในแต่ละ node ของ LDAP directory คือ entry Attribute ประกอบด้วยชนิดของ attribute type และ attribute value Attribute type คือ ชนิดของข้อมูล เช่น mail ,job Title Attribute value

LDAP Directory มีการจัดโครงสร้างแบบลำดับชั้น (Hierarchical) โดยข้อมูลจะถูกบรรจุอยู่ใน Entries ซึ่งแต่ละ Entry จะประกอบด้วย Attribute ในรูปของ <type>=<value> โดย type จะถูกกำหนดไว้ด้วย Object Identifier (OID) ส่วน value ก็จะมี Syntax ที่ระบุไว้ชัดเจน

Entry จะถูกจัดไว้เป็นลำดับชั้นด้วย Distinguished name (DN) โดย Entry ใด ๆ ที่อยู่ใต้ Entry อื่น จะมี DN ของ Entry อื่นเป็น Suffix (ข้อความที่ตามหลัง) Entry นั้น

Schema ของ Directory จะระบุ DN และระบุว่า แต่ละ Entry จะประกอบไปด้วย Attribute ใดบ้าง โดยกำหนด Schema จะกำหนดข้อมูลเหล่านี้ไว้ใน Object class ซึ่งได้แก่ List ของ Mandatory กับ Optional Attribute, วิธีการเปรียบเทียบ Attribute, ชนิดและขนาดของข้อมูลที่อนุญาต ซึ่งทุก ๆ Entry จะต้องเชื่อโยงไว้กับ Object Class หนึ่ง Class รายละเอียดเพิ่มเติมของ Schema File มีอยู่ในหัวข้อ LDAP Schema



รูปที่ 2.17 Attribute LDAP

2.5 Wi-Fi Protected Access (WPA)

เทคโนโลยี WEP เป็นกลไกทางเลือกเดียวที่กำหนดไว้ตามมาตรฐาน IEEE 802.11 ในช่วงยุคแรกๆ (ก่อนปี 2546) สำหรับการเข้ารหัสสัญญาณและการตรวจสอบพิสูจน์ตัวตน ผู้ใช้งานของอุปกรณ์เครือข่ายไร้สาย Wi-Fi เทคโนโลยี WEP อาศัยการเข้ารหัสสัญญาณแบบ shared และ symmetric กล่าวคือ อุปกรณ์ของผู้ใช้งานทั้งหมดบนเครือข่ายไร้สาย หนึ่ง ๆ ต้องทราบรหัสลับที่ใช้ร่วมกันเพื่อทำเข้ารหัสและถอดรหัสสัญญาณได้ ปัจจุบันเทคโนโลยี WEP ล้าสมัยไปแล้วเนื่องจากมีช่องโหว่และจุดอ่อนอยู่มาก โดยช่องโหว่ที่เป็นปัญหาที่สุดคือ การที่ผู้ไม่ประสงค์ดีสามารถคำนวณหาค่ารหัสลับด้วยหลักทางสถิติได้จากการดักฟังและเก็บรวบรวมสัญญาณจากเครือข่าย ไร้สาย Wi-Fi หนึ่งๆ ได้เป็นปริมาณมากเพียงพอ โดยอาศัยโปรแกรม AirSnort ซึ่งเป็น Freeware ดังนั้นในปัจจุบันผู้ติดตั้งและผู้ใช้งานควรหลีกเลี่ยงการใช้กลไก WEP และเลือกใช้เทคนิคทางเลือกอื่นที่มีความปลอดภัยสูงกว่า เช่น WPA (Wi-Fi Protected Access) และ IEEE 802.11i

2.6 WPA Enterprise (หรือWPA+RADIUS)

ผู้ใช้แต่ละคนจะตรวจสอบสิทธิ์โดยใช้ username และ password การนำเอาเทคโนโลยีรักษาความปลอดภัยที่มีความปลอดภัยสูงมาใช้งานบนระบบเครือข่ายโดยเฉพาะอย่างยิ่งเทคโนโลยีการเข้ารหัสสัญญาณและการตรวจสอบพิสูจน์ตัวตน ผู้ติดตั้งระบบเครือข่าย ควรหลีกเลี่ยงเทคโนโลยี WEP ซึ่งมีจุดอ่อนอยู่มาก และเลือกใช้เทคโนโลยี WPA หรือ IEEE 802.11i ซึ่งมี ความปลอดภัยสูงสำหรับเครือข่ายขนาดเล็กควรเลือกใช้เทคโนโลยี WPAในโหมด WPA-PSK เป็นอย่างน้อย ส่วนเครือข่ายในองค์กรขนาดใหญ่ ควรมีการใช้งานเทคโนโลยี WPA ในโหมด WPA+ EAP/TLS หรือ WPA + PEAP นอกจากนี้ผู้ใช้งานเครือข่าย ควรตระหนักถึงความเสี่ยงต่างๆ ที่แฝง

อยู่กับความสะดวกสบายในการใช้งาน หลีกเลี่ยงการรับส่งข้อมูลที่เป็นความลับ และเลือกใช้งาน โพรโตคอล และ แอปพลิเคชัน ที่มีการเข้ารหัสข้อมูลเช่น HTTPS, SSH, PGP เป็นต้น

บทที่ 3

กระบวนการทำงาน

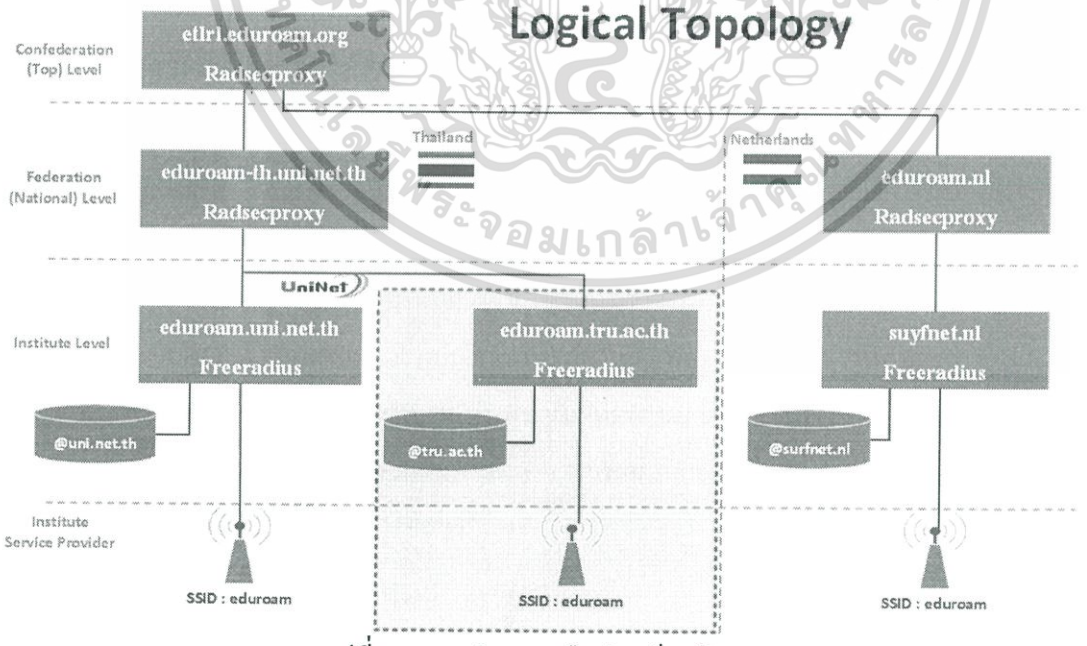
3.1 รูปแบบและแนวคิดของเอ็ดยูโรม

เมื่อผู้ใช้งานจากสถาบันอื่นที่สามารถใช้บริการเอ็ดยูโรมได้มาปฏิบัติราชการที่มหาวิทยาลัย แล้วพบว่าในมหาวิทยาลัยสามารถใช้งานเครือข่ายเอ็ดยูโรมได้ ก็สามารถใช้ ชื่อผู้ใช้งานและรหัสผ่านจากต้นสังกัดล็อกอินใช้งานอินเทอร์เน็ตได้ทันที การไปใช้งานในสถานที่อื่นในเครือข่ายเอ็ดยูโรมผู้ใช้งานจะไม่มีข้อมูลผู้ใช้งาน อยู่ในฐานข้อมูลของสถานศึกษานั้นซึ่งระบบจะทำการตรวจสอบไปยังฐานข้อมูลของสถาบันการศึกษาผู้ใช้บริการของผู้ใช้งาน ผ่านทางเรเดียสเซิร์ฟเวอร์

ผู้ใช้งานจะเข้าใช้ข้อมูลการเข้าใช้งานในรูปแบบ username@tru.ac.th และ รหัสผ่าน จากสถาบันต้นสังกัดเพื่อเข้าสู่ระบบ ระบบก็จะส่งข้อมูลไปตรวจสอบยังเรเดียสเซิร์ฟเวอร์ของสถาบันนั้นๆ ถ้าข้อมูลผ่านการตรวจสอบแล้วยืนยันความถูกต้องแล้ว ก็จะสามารถใช้งานอินเทอร์เน็ตได้

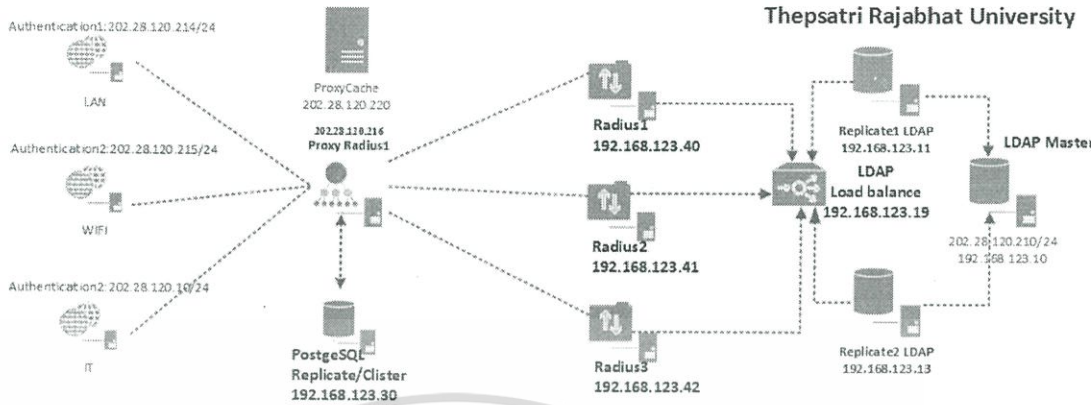
ในกรณีที่เดินทางไปในประเทศที่เป็นสมาชิกเอ็ดยูโรม ก็สามารถใช้งานได้โดยจะมีระบบการตรวจสอบระหว่าง เรเดียสเซิร์ฟเวอร์ของแต่ละประเทศและส่งคำร้องขอไปยังเรเดียสเซิร์ฟเวอร์ของแต่ละสถานศึกษาต้นสังกัดของผู้ใช้งาน

3.2 ภาพรวมการทำงานระบบพิสูจน์ตัวตนผ่านเครือข่ายเอ็ดยูโรม



รูปที่ 3.1 การทำงานเครือข่ายเอ็ดยูโรม

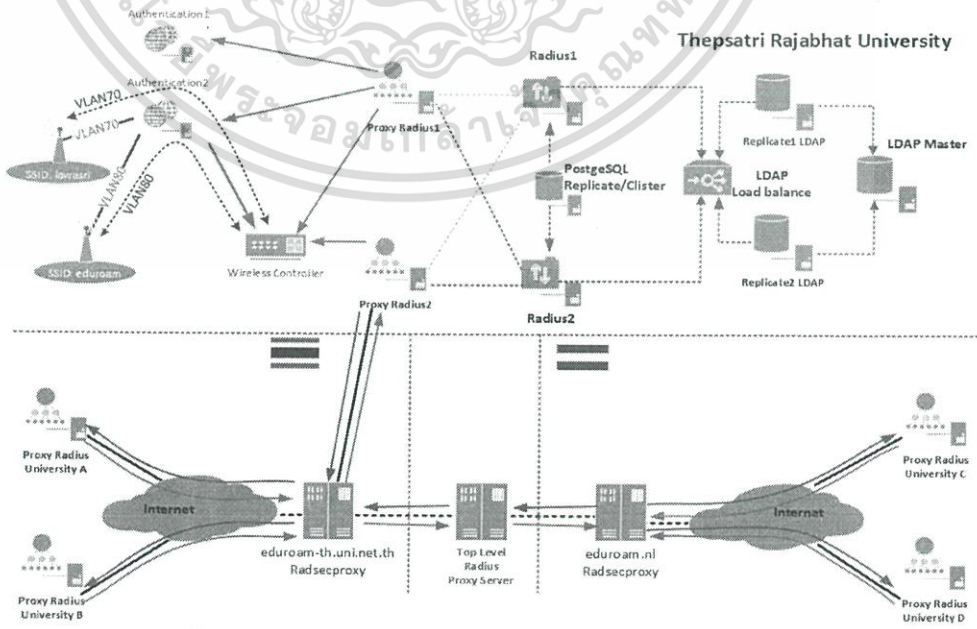
3.3 วิเคราะห์ระบบเดิมและระบบใหม่



รูปที่ 3.2 โครงสร้างระบบเครือข่ายเดิม

จากรูปที่ 3.2 ระบบเครือข่ายเดิมที่มหาวิทยาลัยมีอยู่ จะมีฐานข้อมูล LDAP เพื่อใช้เก็บข้อมูลชื่อผู้ใช้งานและรหัสผ่านของผู้ใช้งานทั้งหมดและมีการทำ Replicate LDAP อีก 2 เครื่องเพื่อเป็นการกระจายโหลดและสำรองข้อมูลในตัวเดียวกัน และมีพร็อกซี่เรเดียสเซิร์ฟเวอร์ 1 เครื่องเพื่อให้บริการการยืนยันตัวของผู้ใช้งาน เครือข่ายอินเทอร์เน็ตของมหาวิทยาลัย

เมื่อได้ทำการพิจารณาจากระบบเดิมแล้วนั้นก็จำเป็นต้องจัดทำพร็อกซี่เรเดียสเซิร์ฟเวอร์ขึ้นมาอีก 1 เครื่องเพื่อให้บริการเอ็ดยูโรมดังรูปที่ 3.3 และทำการเชื่อต่อเข้ากับ Radius1 Radius2 และ eduroam-th เพื่อให้สามารถยืนยันตัวได้ทั้งในและนอกมหาวิทยาลัย



รูปที่ 3.3 การทำงานระบบพิสูจน์ตัวตนผ่านเครือข่ายเอ็ดยูโรม

ตารางที่ 3.1 ตารางเปรียบเทียบโพรโทคอล EAP

Topic	EAP MD5	LEAP	EAP TLS	EAP TLS	EAP TTLS
Security Solution	Standards base	Proprietary	Standards base	Standards base	Standards base
Certificates Client	No	N/A	Yes	No	No
Certificates Server	No	N/A	Yes	Yes	Yes
Credential Security	None	Weak	Strong	Strong	Strong
Supported Authentication Databases	Requires clear-text database	Active Directory, NT Domains	Active Directory, LDAP, etc.	Active Directory ,NT Domain, Token, SQL, LDAP, etc.	Active Directory, LDAP,SQL, plain password file, Token Systems etc.
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Mutual Authentication	No	Yes	Yes	Yes	Yes

จากการวิเคราะห์โพรโทคอล EAP ที่ใช้ในการเชื่อมต่อเอ็ดยูโรมนั้นเนื่องจากมหาวิทยาลัยเก็บข้อมูลรหัสผ่านเป็นแบบ SSHA มหาวิทยาลัยจำเป็นต้องใช้ โพรโทคอลแบบ EAP-TTLS ซึ่งจากตารางที่ 3.1 ก็จะเห็นว่า EAP-TTLS รองรับฐานข้อมูลได้หลายชนิดและยังมีความปลอดภัยสูง แต่ในเบื่องต้นทาง Uninet ให้ใช้โพรโทคอลแบบ EAP-TLS ซึ่งได้ทำการทดสอบแล้วไม่สามารถใช้กับมหาวิทยาลัยได้เนื่องจากรหัสผ่านที่เก็บ เป็นแบบ SSHA แต่ โพรโทคอลแบบ EAP-TLS ใช้ได้กับรหัสผ่านที่เก็บเป็นแบบ Plaintext-Password เท่านั้น

3.4 แบบฟอร์มคำขอใช้งานเครือข่าย eduroam ประเทศไทย

แบบฟอร์มคำขอใช้งานเครือข่าย eduroam ประเทศไทย

ชื่อสถาบันการศึกษาที่ขอเข้าร่วม: _มหาวิทยาลัยราชภัฏเทพสตรี

Name of Educational Institute: _Thepsatri Rajabhat University

รายชื่อผู้ประสานงาน คนที่ 1 (ผู้ประสานงานหลัก)

ชื่อ-นามสกุล (พร้อมคำนำหน้า) : นายณัฐธัญพงศ์ ศรนารายณ์

Name-Surname : Nutthunyapong Sornnarai

ตำแหน่ง : _นักวิชาการคอมพิวเตอร์

หน่วยงานที่สังกัด : _ศูนย์นวัตกรรมและเทคโนโลยีการศึกษา

email : _nutthunyapong.s@lawasri.tru.ac.th

บอร์โทรศัพท์ของหน่วยงาน : _036-427485 ต่อ 26253

เบอร์โทรศัพท์มือถือ : _0805798222

รายชื่อผู้ประสานงาน คนที่ 2

ชื่อ-นามสกุล (พร้อมคำนำหน้า) : _นายไกลาส กลิ่น เทียน

Name-Surname : _Kailas Krintian

ตำแหน่ง : _นักวิชาการคอมพิวเตอร์

หน่วยงานที่สังกัด : ศูนย์นวัตกรรมและเทคโนโลยีการศึกษา

email : _kailas.k@lawasri.tru.ac.th

เบอร์โทรศัพท์ของหน่วยงาน : _036-427485 ต่อ 26253

เบอร์โทรศัพท์มือถือ : _0836092699

ลงลายมือชื่อ

(ผศ.ดร. นันทวัน เพ็งสุวรรณ์)

อธิการบดีมหาวิทยาลัยราชภัฏเทพสตรี

๑๗ / ต.ค. / ๕๘

ลงลายมือชื่อ

( )

ผู้อำนวยการศูนย์นวัตกรรมและเทคโนโลยีการศึกษา

๑ / ตุลาคม / ๒๕๕๘

****

หมายเหตุ: * ผู้มีอำนาจลงนามต้องมีตำแหน่งบริหารตั้งแต่ผู้อำนวยการศูนย์คอมพิวเตอร์ของสถาบันขึ้นไป

และกรุณาส่งแบบฟอร์มในรูปแบบของ PDF file ไปยัง E-mail address : noc@uninet.th

พร้อมส่งแบบฟอร์มฉบับจริง ถึง สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา (UniNet)

สำนักงานคณะกรรมการการอุดมศึกษา ชั้น ๙, ๓๒๘ ถนนศรีอยุธยา แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพ ๑๐๔๐๐

หากมีข้อสงสัยติดต่อ คุณเกรียงศักดิ์ เหล็กดี, นางสาวนริษร์ เผ่าแพร โทรศัพท์ ๐ ๒๓๕๔ ๕๖๗๘ ต่อ ๕๐๐๖, ๕๐๐๒

รูปที่ 3.4 แบบฟอร์มคำขอใช้งานเครือข่าย eduroam ประเทศไทย

เรียน คุณณัฐธัญพงศ์ ศรนารายณ์

เจ้าหน้าที่ได้รับข้อมูล IP Address ของ Server เรียบร้อยแล้ว
IP Address eduroam TH : 202.28.112.6
Ream : tru.ac.th
Secret key:

หากดำเนินการ config เรียบร้อยแล้ว ให้ดำเนินการ ดังต่อไปนี้

1. test user radius local ของมหาวิทยาลัย ว่าสามารถใช้งานได้หรือไม่

2. หากข้อ 1 สามารถใช้งานได้แล้ว ให้นำ user ของ UniNet ทดสอบ ว่าสามารถใช้งานได้หรือไม่

Username: guest-tru@uni.net.th
Password:

3. หากข้อ 2 สามารถใช้งานได้แล้ว ให้แจ้ง account ของมหาวิทยาลัย เพื่อให้เจ้าหน้าที่ดำเนินการทดสอบ ว่าสามารถใช้งานได้หรือไม่

4. หากข้อ 3 สามารถใช้งานได้แล้ว จะถือว่า มหาวิทยาลัยเป็นสมาชิก eduroam TH เรียบร้อยแล้ว และมหาวิทยาลัยจึงดำเนินการ Config radius เพิ่มเติม เช่น config ให้ radius เชื่อมต่อกับ LDAP ได้ เป็นต้น

ด้วยความเคารพ
นางสาวนรินทร์ เผ่าแพร
เจ้าหน้าที่ฝ่ายบริหารเครือข่าย
สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา (UniNet)
สำนักงานคณะกรรมการการอุดมศึกษา
เบอร์โทร 02-354-5678 ต่อ 5002
อีเมล์ narin@uni.net.th

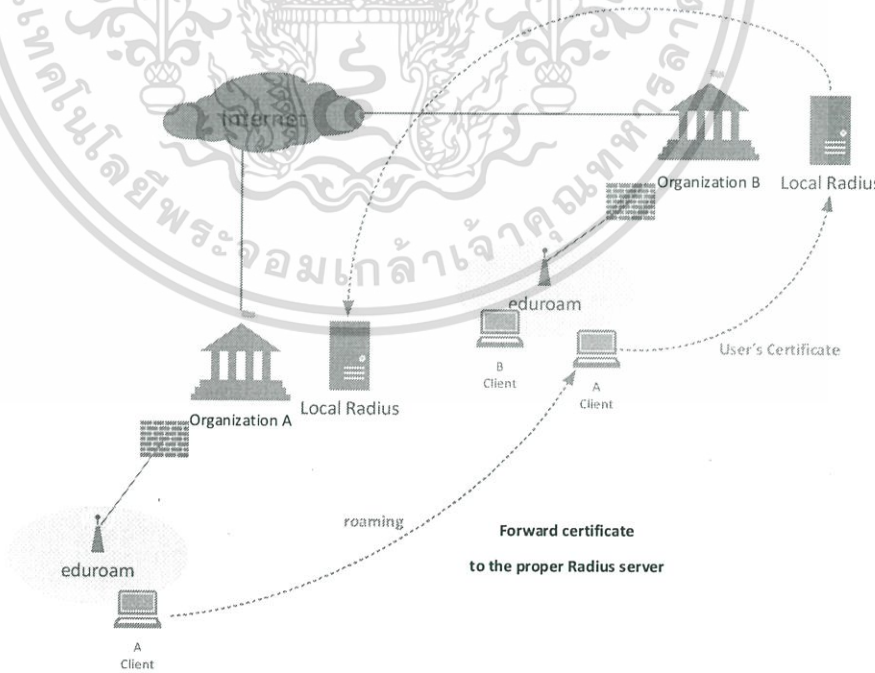
รูปที่ 3.5 จดหมายตอบกลับจาก สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อการศึกษา(UniNet)

3.5 การออกแบบระบบ

จากที่ได้อธิบายเกี่ยวกับระบบรักษาความปลอดภัยโดยเบื้องต้นไปแล้วนั้น จะเห็นได้ว่าการใช้งาน IEEE802.1X และ EAP นั้นมีความปลอดภัยค่อนข้างสูง และยังเป็นมาตรฐานที่ระบบปฏิบัติการที่ได้รับความนิยม ได้รวมเข้าไว้ในระบบอยู่แล้วทำให้ไม่ต้องลงทุนเพิ่ม ระบบให้บริการเครือข่ายไร้สายร่วมกันระหว่างองค์กรนี้จะทำงานบนมาตรฐาน EAP-TTLS ซึ่งเป็นมาตรฐานที่ต้องมี PKI โดยต้องมีการใช้ Certificate ของทั้ง เรเดียส และ เครื่องลูกข่าย ในการทำ Authentication เพื่อป้องกันการโจมตีแบบ Man-in the-middle เนื่องจากเครื่องลูกข่ายจะไม่ส่ง Credential ให้กับเรเดียส หากไม่สามารถพิสูจน์ได้ว่าเป็นเรเดียสเซิร์ฟเวอร์ตัวจริง

โปรแกรม Free radius จะถูกนำมาใช้เป็น Authentication Server ของระบบนี้เนื่องจากเป็นโปรแกรม Open Source และ ค่อนข้างจะถูกใช้โดยแพร่หลาย อีกทั้งยังรองรับกับโพรโทคอล ที่เราจะนำมาใช้ (EAP-TTLS) อีกด้วย แต่ละองค์กรจะต้องมี CA ของตนเองเพื่อเป็นการสร้าง ระบบ PKI ขององค์กร โดยจะใช้โปรแกรม OpenSSL ซึ่งเป็น Open Source เช่นกัน เพื่อสร้าง Certificate ของ Server

เรเดียสของแต่ละองค์กรจะเชื่อมถึงกันผ่านอินเทอร์เน็ตโดยที่จะเป็นเครื่องลูกข่ายและเซิร์ฟเวอร์ ของกันและกัน ยกตัวอย่างเช่น เมื่อเรเดียสขององค์กร A ได้รับการการขอ Authenticate จาก ผู้ใช้ที่โรมมิ่งมาจากองค์กร B แล้ว เรเดียส A จะทำการพร็อกซีขอ Authenticate นั้นแล้วส่งต่อไปยัง เรเดียส B ในการนี้เรเดียส A จะเป็นเครื่องลูกข่ายของ เรเดียส B ดังรูปที่ 3.6



รูปที่ 3.6 แสดงการ Roaming และ Proxy

เมื่อผู้ใช้ได้ทำการสมัครสมาชิกแบบออนไลน์ ระบบจะทำการเพิ่มชื่อ โดเมนขององค์กรต่อท้ายชื่อผู้ใช้เข้าไปในช่อง CN ของ Certificate ก่อนที่จะเพิ่มชื่อผู้ใช้เข้าไปในฐานข้อมูลของแต่ละ

องค์กร เรียกว่า Realm โดยชื่อผู้ใช้จะมีลักษณะคล้ายกับ อีเมล์แอดเดรส เช่น username@tru.ac.th เป็นต้น ซึ่ง Realm จะถูกใช้เพื่อแยกแยะว่าเป็นผู้ใช้ที่มาจากองค์กรใดเพื่อการทำพร็อกซีต่อไป เช่น หากเรเดียสตรวจ พบว่าเป็นผู้ใช้ชื่อ username@tru.ac.th ก็จะ Encap- sulate ด้วย EAP ก่อนที่จะส่งผ่านการ Authenticate ไปยังเรเดียสของ มหาวิทยาลัยราชภัฏเทพสตรีต่อไป

ระบบจะทำการตรวจสอบข้อมูล ว่าเป็นผู้ใช้ชื่ออะไรและมี Realm ชื่ออะไรก่อนจะทำการพร็อกซีไปยังเรเดียสที่ถูกต้อง แต่ถ้าระบบไม่สามารถค้นข้อมูลว่า Realm นั้นมีเรเดียสหมายเลยอะไร ก็จะทำการ Reject ผู้ใช้คนนั้นทันที

3.6 การติดตั้งเครื่องแม่ข่าย Radius Server eduroam

3.6.1 คุณสมบัติของเครื่องเซิร์ฟเวอร์

- หน่วยประมวลผล Xeon E5-2430 2.20 GHz X 2
- ระบบปฏิบัติการ Debian 8.0
- หน่วยความจำหลัก 2 GB
- หน่วยความจำสำรอง 20 GB
- แลนการ์ด 10/100/1000 Mbps จำนวน 2 การ์ด

3.6.2 ตั้งค่าเครื่องเซิร์ฟเวอร์

1) ตั้งค่าไอพีแอดเดรสที่ได้แจ้งกับ Uninet ในเบื้องต้น

```
# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
        address 202.28.120.217
        netmask 255.255.255.0
        gateway 202.28.120.251
        dns-nameservers 8.8.8.8

# The primary network interface
auto eth1
iface eth1 inet static
        address 192.168.123.18
        netmask 255.255.255.0
root@eduroam:/home/truadmin#
```

รูปที่ 3.7 แสดงพารามิเตอร์ในแฟ้ม interface

2) ตั้งค่าโฮสเนมของเครื่องเรเดียสเซิร์ฟเวอร์ชื่อ eduroam ในแฟ้ม /etc/hostname และ /etc/hosts

3.6.3 ติดตั้ง Free radius และทำการตั้งค่าไฟล์ดังนี้

1) แฟ้มการกำหนดค่าอยู่ใน /etc/freeradius/radiusd.conf จะเป็น แฟ้มหลักมีหน้าที่ควบคุมการทำงานทั้งหมดของโปรแกรมเช่น Path ที่ใช้จัดเก็บแฟ้มต่างๆที่เกี่ยวข้อง, วิธีการเก็บ Log ต่างๆ,

การติดต่อกับฐานข้อมูล, และ รูปแบบการใช้งาน EAP และ Realm ฯลฯ โดยค่าส่วนใหญ่ที่จำเป็นจะถูกกำหนดเป็นค่าตั้งต้นอยู่แล้ว ในแต่ละส่วนของการใช้งาน EAP ดังรูปที่ 3.8

```
security {
        max_attributes = 200
        reject_delay = 0
        status_server = yes
}
        proxy_requests = yes
...
listen {
        type = auth
        ipaddr = *
        port = 1812
}
listen {
        type = auth
        ipv6addr = ::
        port = 1812
}
listen {
        type = acct
        ipaddr = *
        port = 1813
}
listen {
        type = acct
        ipv6addr = ::
        port = 1813
}
```

รูปที่ 3.8 แสดงพารามิเตอร์ในแฟ้ม radius.conf

2) /etc/freeradius/sites-enabled/eduroam ไฟล์เริ่มต้นสาหรับการเปิดใช้eduroam เป็นการกำหนดคุณสมบัติเกี่ยวกับการบันทึกกิจกรรมการทำงานที่กำหนดไว้ การติดตั้งนี้ใช้ไฟล์โมดูลเดิม และมีตำแหน่งการบันทึกตามค่าตั้งเดิมของ Radius server

```
server eduroam {
authorize {
        auth_log

        if (User-Name !~ /.*@tru.ac.th$/) {
                suffix
        }

        eap
}
authenticate {
        eap
}
preacct {
        suffix
}
accounting {
}
post-auth {
        reply_log
        Post-Auth-Type REJECT {
                reply_log
                f_ticks
        }
}
pre-proxy {
        pre_proxy_log

        if (Packet-Type != Accounting-Request) {
                attr_filter.pre-proxy
        }
}
post-proxy {
        post_proxy_log

        if (Realm == "tru.ac.th") {
                eap
        }

        attr_filter.post-proxy
}
}
```

รูปที่ 3.9 แสดงพารามิเตอร์ในแฟ้ม eduroam

3) แฟ้มการกำหนดค่าอยู่ใน /etc/freeradius/clients.conf เป็นการกำหนดว่าอนุญาตให้เครื่องเรเดียสเครื่องใดสามารถขอทำพร็อกซีให้กับเรเดียสขององค์กรเราได้ ดังรูปที่ 3.10

```
  GNU nano 2.2.6   File: clients.conf    Modified

client eduroam-th-to-university {
        ipaddr = 202.28.112.6
        netmask = 32
        secret =
        require_message_authenticator = no
        shortname = eduroam-th-to-university
        nastype = other
        virtual_server = eduroam
}
```

รูปที่ 3.10 แสดงพารามิเตอร์ในแฟ้ม clients.conf

4) แฟ้มการกำหนดค่าอยู่ใน /etc/freeradius/proxy.conf ไฟล์ที่มีข้อมูลทั้งหมดเกี่ยวกับวิธีการที่ผู้ให้บริการส่งต่อการร้องขอเรเดียสใน Pool ของโฮมเซิร์ฟเวอร์จะมีการกำหนดเรเดียสเซิร์ฟเวอร์ที่ใช้สำหรับการตรวจสอบ (ตัวตนผู้ให้บริการ) นอกจากนี้ยังกำหนดถ้าเซิร์ฟเวอร์หลักที่จัดการการตรวจสอบและบัญชีผู้ใช้งานพร้อมกันหรือแยกกัน พอร์ตที่ใช้ในการติดต่อเรเดียส ที่มีการระบุไว้ในไฟล์นี้ปัจจุบันจะเป็นพอร์ตมาตรฐาน 1812 สำหรับการตรวจสอบผู้ใช้งาน และ 1813 สำหรับการทำบัญชีผู้ใช้ เมื่อเซิร์ฟเวอร์ที่มหาวิทยาลัยมีมากกว่าหนึ่งเครื่อง พร็อกซีควรกำหนดลำดับที่ร้องขอจะถูกส่งไป พร็อกซียังระบุเครื่องที่รู้จักกันที่แตกต่างกันและการร้องขอจาก Realm เหล่านั้นจะถูกส่งต่อไปยัง Realm ที่ร้องขอในกรณีของเราก็จะถูกส่งต่อไปยังเซิร์ฟเวอร์ eduroam-th พารามิเตอร์ทั้งหมดเหล่านี้จะกำหนดไว้ใน proxy.conf ดังรูปที่ 3.1

```
  GNU nano 2.2.6        File: proxy.conf

#Allow asking from eduroam.university.ac.th to eduroam-TH
home_server eduroam-th {
        type = auth+acct
        ipaddr = 202.28.112.6
        port = 1812
        secret =
        status_check = status-server
}
home_server_pool EDUROAM{
        type = fail-over
        home_server = eduroam-th
}

realm DEFAULT {
        auth_pool = EDUROAM
        nostrip
}
```

รูปที่ 3.11 แสดงพารามิเตอร์ในแฟ้ม proxy.conf

5) แฟ้มการกำหนดค่าอยู่ใน /etc/freeradius/eap.conf การตั้งค่า พารามิเตอร์สำหรับ การกำหนดค่าต่างๆ ของโพรโทคอล EAP-TTLS เช่นการกำหนด path ที่ใช้เก็บ Private key และ Certificate ของผู้ใช้ ดังรูปที่ 3.12

```
 GNU nano 2.2.6          File: eap.conf

eap {
        default_eap_type = ttls
        timer_expire = 60
        ignore_unknown_eap_types = no
        cisco_accounting_username_bug = no

        tls {
                certdir = ${confdir}/certs
                cadir = ${confdir}/certs
                private_key_file = ${certdir}/tru.ac.th.key
                certificate_file = ${certdir}/tru.ac.th.crt
                random_file = /dev/urandom
                fragment_size = 1024
                include_length = yes
                check_crl = no
                cipher_list = "DEFAULT"
        }

        ttls {
                default_eap_type = mschapv2
                copy_request_to_tunnel = yes
                use_tunneled_reply = yes
                virtual_server = "eduroam-inner-tunnel"
                proxy_tunneled_request_as_eap = no
        }
}
```

รูปที่ 3.12 แสดงพารามิเตอร์ในแฟ้ม eap.conf

6) /etc/freeradius/sites-enabled/eduroam-inner-tunnel

```
 GNU nano 2.2.6 File: ...-enabled/eduroam-inner-tunnel

server eduroam-inner-tunnel {
        authorize {
                auth_log
                eap
                suffix
        }

        authenticate {
                Auth-Type PAP {
                        pap
                }
                Auth-Type MS-CHAP {
                        mschap
                }

                eap
        }

        post-auth {
                reply_log

                Post-Auth-Type REJECT {
                        reply_log
                }
        }
}
```

รูปที่ 3.13 แสดงพารามิเตอร์ในแฟ้ม eduroam-inner-tunnel

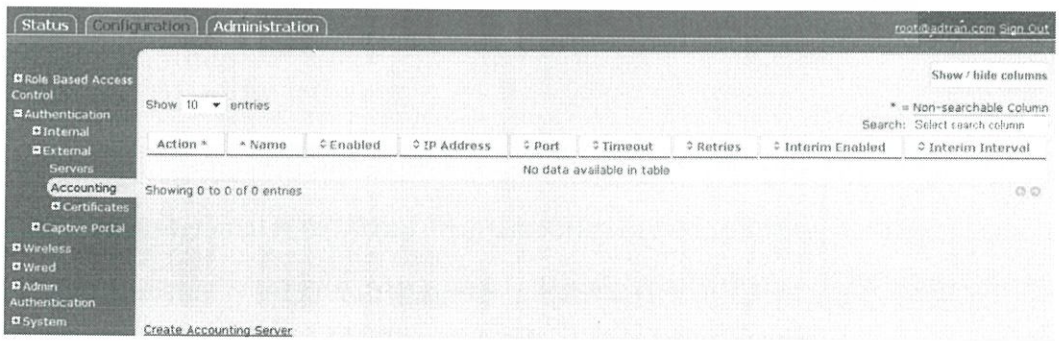
7) /etc/freeradius/sites-enabled/rahunas-proxy การทำงานของ Radius server นั้น จะมีการรับข้อมูลการร้องขอการเข้าถึง (Access-Request) จากภายนอก และส่งต่อเป็นลำดับขั้นการทำงานตามลำดับที่ประกาศไว้ในไฟล์ โดยลำดับขั้นสำคัญจะอยู่ในไฟล์ประกอบด้วยไฟล์ sites-enabled/eduroam และไฟล์ sites-enabled/eduroam-inner-tunnel เมื่อ Radius server ได้รับการร้องขอ จะนำข้อมูลการร้องขอเข้าไปประมวลผลตามขั้นตอนในไฟล์ sites-enabled/eduroam เป็นไฟล์แรก และอาจส่งต่อไปยังการประมวลผลภายในในไฟล์ sites-enabled/eduroam-inner-tunnel หรือส่งต่อไปยัง Radius server เครื่องถัดไป

รูปที่ 3.14 แสดงพารามิเตอร์ในแฟ้ม rahunas-proxy

3.7 การตั้งค่า Wireless AP Controller

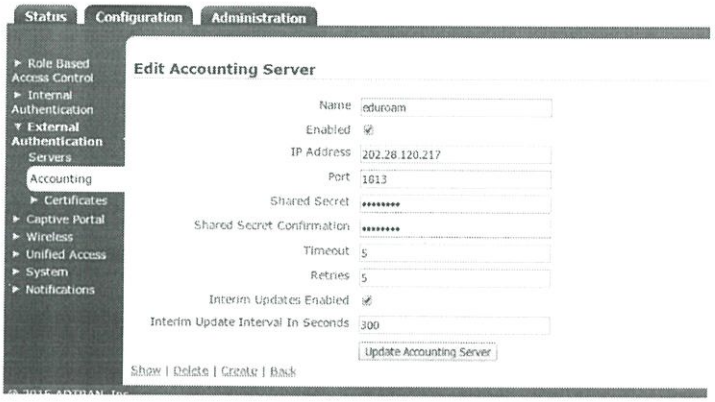
3.7.1. ตั้งค่าเรเดียสเซิร์ฟเวอร์ภายนอกการพิสูจน์ตัวตนแบบ 802.1x

1) ในหน้า vWLAN ไปที่แท็บ Configuration แล้วคลิกที่เมนู External Authentication > Accounting. แล้วคลิกที่ Create Accounting Server



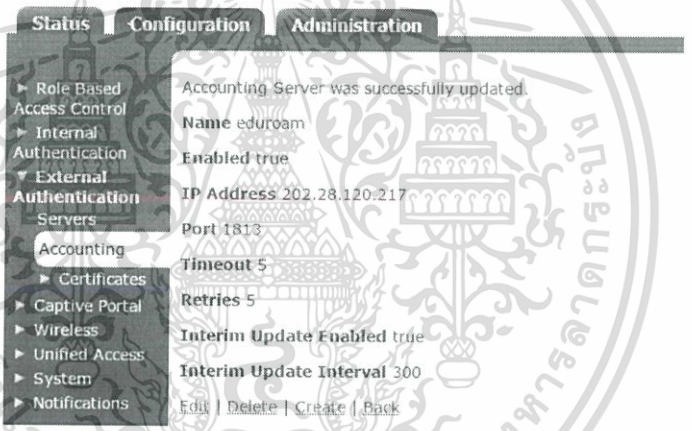
รูปที่ 3.15 ตั้งค่าเรเดียสเซิร์ฟเวอร์ภายนอก

2) ใส่รายละเอียดตามรูปที่ 3.16



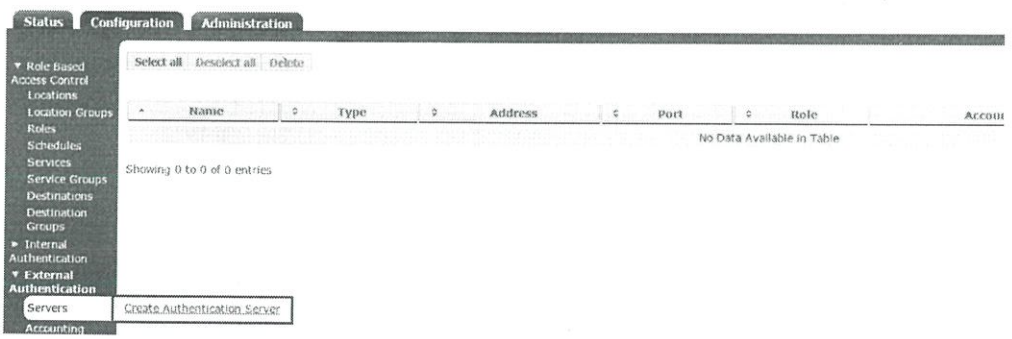
รูปที่ 3.16 รายละเอียดการสร้าง Accounting

3) เมื่อกรอกข้อมูลครบแล้วคลิกที่ Update Accounting Server ระบบจะทำการบันทึกข้อมูลแล้วแจ้งว่า Accounting Server was successfully updated. ดังรูปที่ 3.17



รูปที่ 3.17 แสดงรายระเอียด Accounting ที่สร้าง

4) ในหน้า vWLAN ไปที่แท็บ Configuration แล้วคลิกที่เมนู External Authentication > Servers แล้วคลิกที่ Create Authentication Server

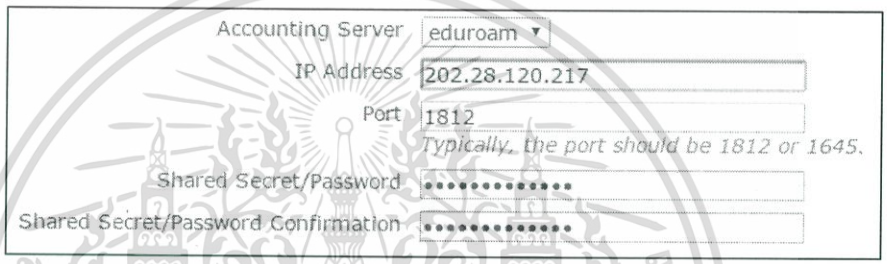


รูปที่ 3.18 ตั้งค่าเรเดียสเซิร์ฟเวอร์ภายนอก พิสูจน์ตัวตนแบบ 802.1x

5) เลือกตรงเมนู Type RADIUS1xAuthServer แล้วใส่ชื่อในช่อง Name

รูปที่ 3.19 Creating Roles for Machine and User Authentication

6) ใส่ไอพีเอดเดรสของเรเดียสเซิร์ฟเวอร์ภายนอก ในช่อง IP address ใส่พอร์ต 1812 ในช่อง Ports 1812 และshared secret ในช่อง Shared Secret/Password และช่อง Shared Secret/Password confirmation ดังรูปที่ 3.20



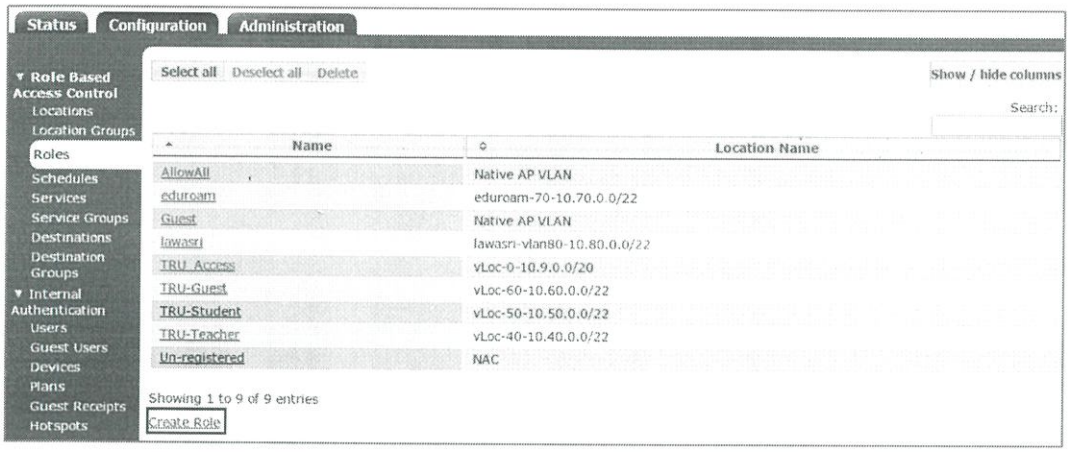
รูปที่ 3.20 Creating Roles for Machine and User Authentication

7) เมื่อกรอกข้อมูลครบแล้วทำการบันทึกระบบจะแจ้ง Authentication Server was successfully updated.

รูปที่ 3.21 Authentication Server was successfully updated

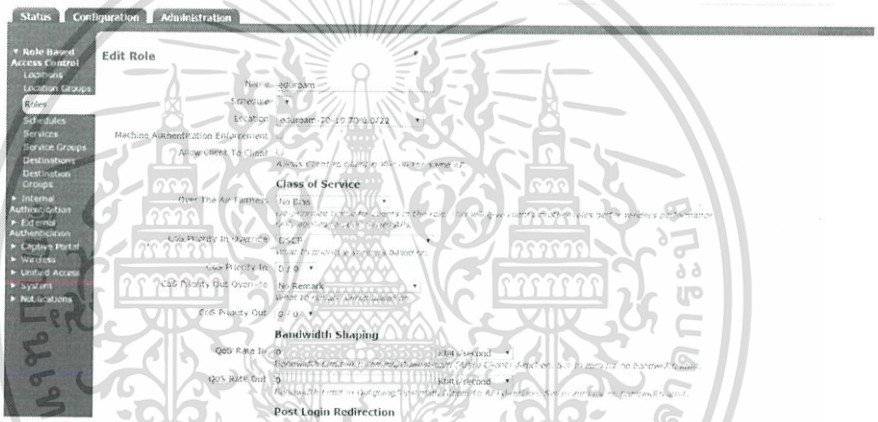
3.7.2 สร้าง Roles สำหรับใช้งานไวเรสและการพิสูจน์ตัวตนของผู้ใช้งาน

2) ในหน้า vWLAN ไปที่แท็บ Configuration แล้วคลิกที่เมนู Role Based Access Control แล้วเลือกเมนู Roles. คลิกที่Create Role ดังรูปที่ 3.22



รูปที่ 3.22 สร้าง Roles สำหรับใช้งานไวเรสและการพิสูจน์ตัวตนของผู้ใช้งาน

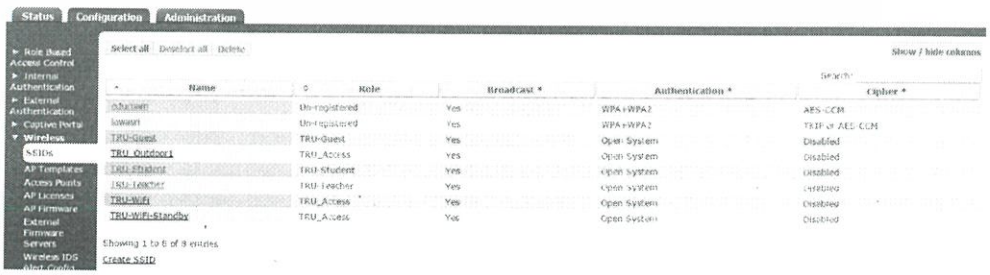
2) ใส่รายละเอียดในการสร้าง Roles



รูปที่ 3.23 รายละเอียด สร้าง Roles สำหรับใช้งานไวเรสและการพิสูจน์ตัวตนของผู้ใช้งาน

3.7.3 การตั้งค่า SSID

1) ในหน้า vWLAN ไปที่แท็บ Wireless แล้วคลิกที่เมนู SSIDs แล้วเลือกเมนู Create SSID ดังรูปที่ 3.24



รูปที่ 3.24 การสร้าง SSID

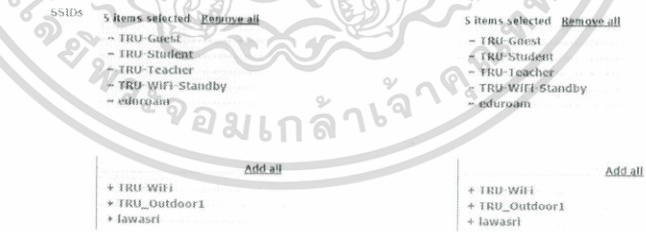
2) กรอกรายละเอียดตามรูปที่ 3.25 คลิกที่ Create SSID

รูปที่ 3.25 รายละเอียดการสร้าง SSID

3) จากนั้นทำการเพิ่ม SSID ใหม่ที่สร้างเข้าเท็มเพลตโดยไปที่ AP Templates เลือก TRU ดังรูปที่ 3.26

รูปที่ 3.26 AP Template

4) ทำการเลือก SSID : eduroam เข้าไปที่เท็มเพลต TRU โดยการคลิกที่ เครื่องหมายบวกดังรูปที่ 3.27



รูปที่ 3.27 แสดงการเพิ่ม SSID :eduroam เข้าไปในเท็มเพลต TRU

3.8 การตั้งค่าสวิตช์

สร้าง Vlan 70 เพิ่มเข้าไปที่สวิตช์ทุกตัวในมหาวิทยาลัย เพื่อรองรับใช้งาน SSID : eduroam ดังรูปที่ 3.28 และ 3.29

```
interface port1.2.1
 description Link-to-Bld6
 switchport
 switchport mode trunk
 switchport trunk allowed vlan add 1,10-26,40,50,60,70,80,100,500,600,900
 switchport trunk native vlan 30
 snmp trap link-status
 spanning-tree path-cost 4
 lldp tlv-select all
!
```

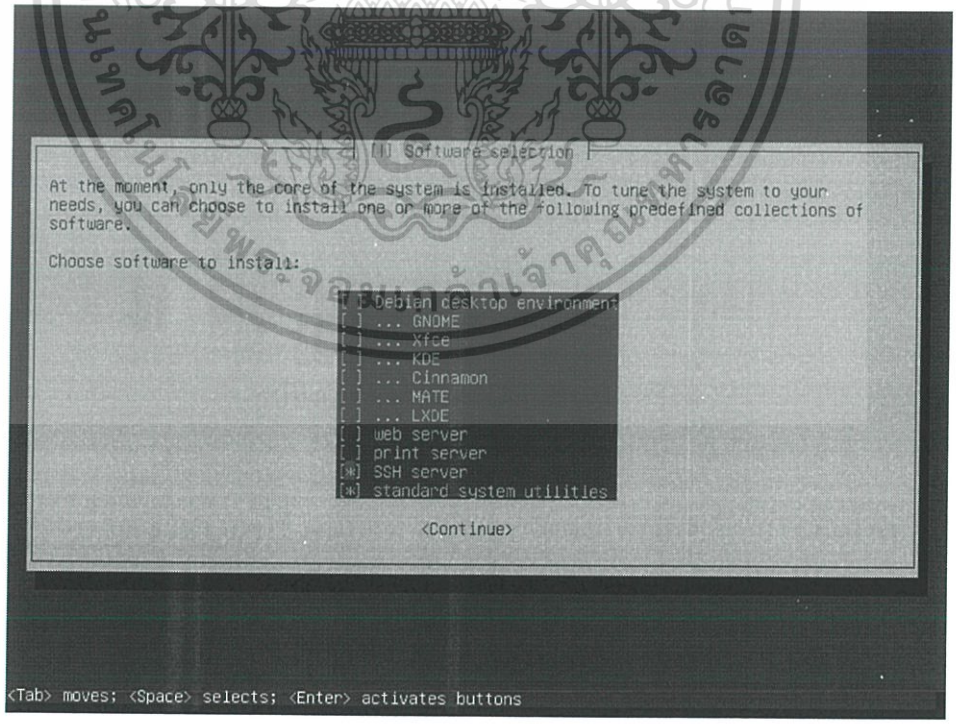
รูปที่ 3.28 ตัวอย่างการเพิ่ม Vlan 70

```
70      eduroam          STATIC  ACTIVE  port1.1.1(t) port1.1.2(t) port1.2.1(t)
                                         port1.2.2(t) port1.3.1(t) port1.3.2(t)
                                         port1.4.1(t) port1.4.3(t) port1.4.4(t)
                                         port1.4.5(t) port1.5.1(t) port1.5.2(t)
                                         port1.6.1(t) port1.6.2(t) port1.6.3(t)
                                         port1.6.4(t) port1.6.5(t) port1.6.6(t)
                                         port1.6.7(t) port1.6.8(t) port1.6.9(t)
                                         port1.6.10(t) port1.6.11(t)
                                         port1.6.12(t)
```

รูปที่ 3.29 Vlan 70 ที่เพิ่มเข้าไปในสวิตช์

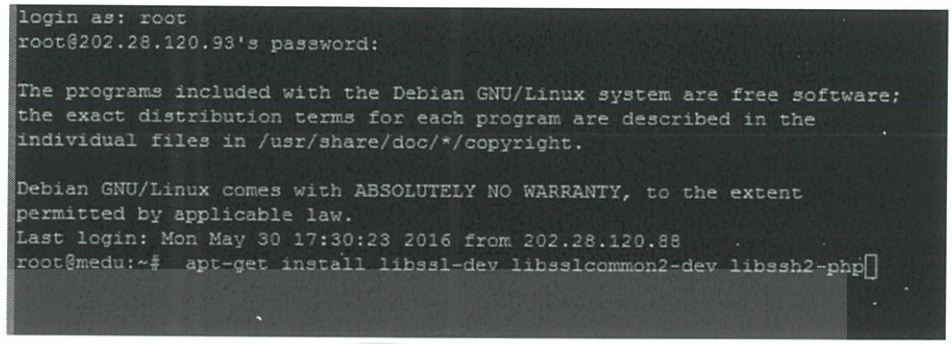
3.9 ติดตั้งเครื่องเซิร์ฟเวอร์ใช้งานมอนิเตอร์และติดตั้งแพ็กเก็จเอ็ดยูโรมอัตโนมัติ

3.9.1 ติดตั้ง ระบบปฏิบัติการ Debian เพื่อใช้เป็นเซิร์ฟเวอร์ในการมอนิเตอร์และติดตั้งแพ็กเก็จเอ็ดยูโรมอัตโนมัติ แล้วเลือกแพ็กเก็จดังนี้ web server และ SSH server



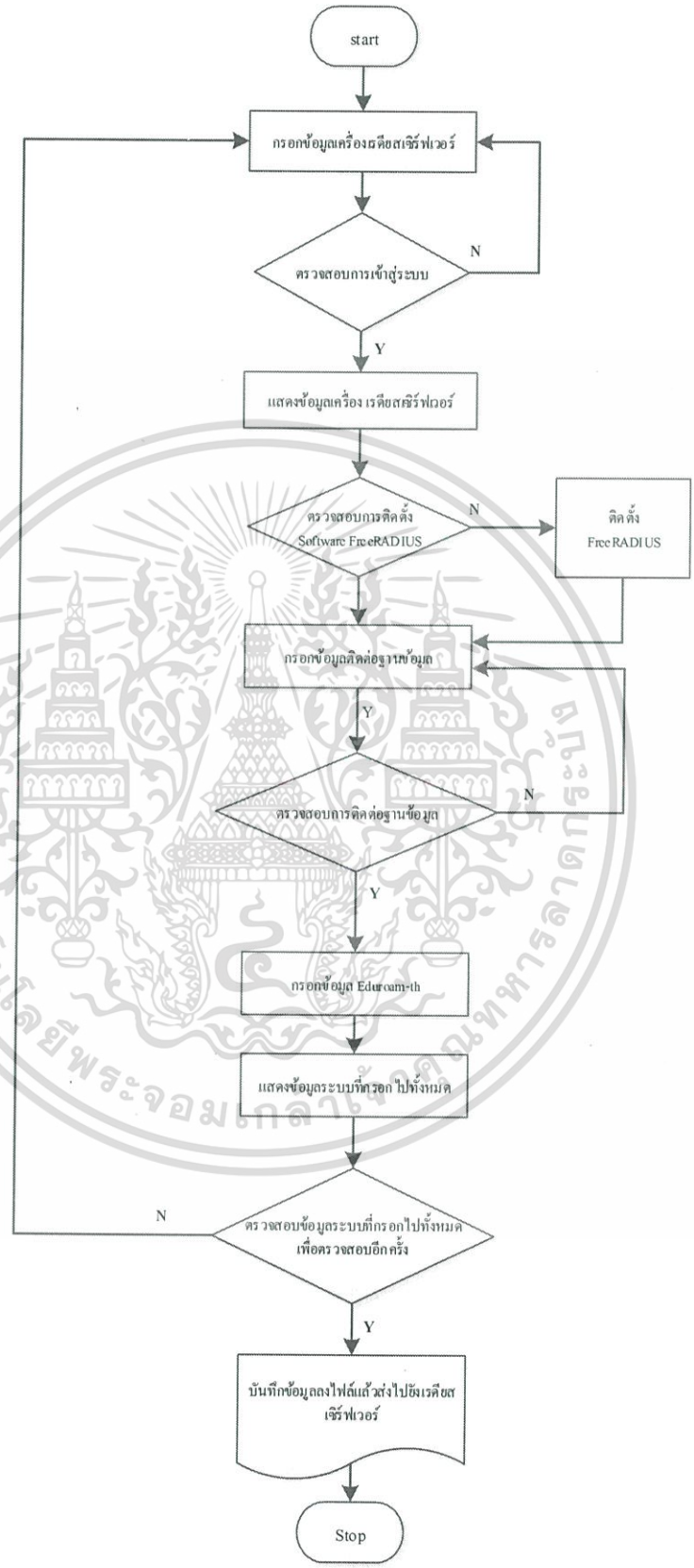
รูปที่ 3.30 เลือกแพ็กเก็จติดตั้งเครื่องเซิร์ฟเวอร์

3.9.2 เมื่อติดตั้งเครื่องเซิร์ฟเวอร์เรียบร้อยแล้ว ทำการล็อกอิน แล้วสั่งติดตั้งโปรแกรม SSH2 เพื่อให้สามารถส่งคำสั่งในการตั้งค่าระบบเอ็ดยูโรมอัตโนมัติไปยังเครื่องเซิร์ฟเวอร์ปลายทางที่ระบุได้ด้วยคำสั่ง apt-get install libssl-dev libsslcommon2-dev libssh2-php



รูปที่ 3.31 ติดตั้งโปรแกรม SSH2

3.9.3 แสดง Flowchart ขั้นตอนการติดตั้งเอ็ดยูโรมผ่านเว็บไซต์โดยอัตโนมัติ



รูปที่ 3.30 แสดง Flowchart ขั้นตอนการติดตั้งเอ็ดยูโรมผ่านเว็บไซต์

จากรูปที่ 3.30 เป็นการแสดงขั้นตอนการติดตั้งเอ็ดยูโรมผ่านเว็บไซต์โดยอัตโนมัติในกรณีที่เครื่องเซิร์ฟเวอร์เอ็ดยูโรมเดิมเกิดเสียหายหรือมีการติดตั้งเซิร์ฟเวอร์เอ็ดยูโรมใหม่โดยมีขั้นตอนดังนี้

1) จะทำการกรอกข้อมูลของเครื่องเรดียสเซิร์ฟเวอร์ได้แก่ ip address ,username และ password ถ้าถูกต้องระบบจะทำการล็อกอินเข้าเครื่องเรดียสเซิร์ฟเวอร์เครื่องที่จะติดตั้งได้และทำการเช็คว่าเป็น OS ประเภทไหน
2) จะทำการตรวจสอบว่าเครื่องเรดียสเซิร์ฟเวอร์มี Software Free RADIUS อยู่หรือไม่ถ้าไม่มีจะให้ทำการติดตั้งโดยสั่งจากระบบได้เลย
3) จะให้กรอกข้อมูลฐานข้อมูลที่ใช้งานเอ็ดยูโรม และก็จะทำการเช็คว่าข้อมูลที่กรอกมาใช้ได้ถูกต้องหรือไม่ ถ้าถูกจะไปขั้นตอนต่อไป
4) จะให้กรอกข้อมูลของ IP Server eduroam-th ,secret, realm ที่ Uninet ให้มาเพื่อทำการเชื่องต่อกับ Uninet-TH
5) จะเป็นการตรวจสอบข้อมูลที่กรอกไปทั้งหมดว่าถูกต้องกรือไม่ถ้าถูกต้องก็คลิ๊กที่บันทึก ระบบจะทำการบันทึกค่าลงไฟล์และส่งไปยังเครื่องเรดียสเซิร์ฟเวอร์ปลายทาง

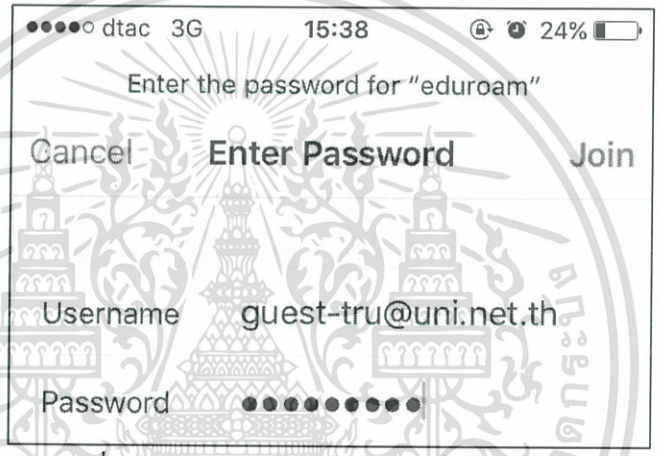
บทที่ 4
ผลการดำเนินการ

4.1 ผลการดำเนินการ

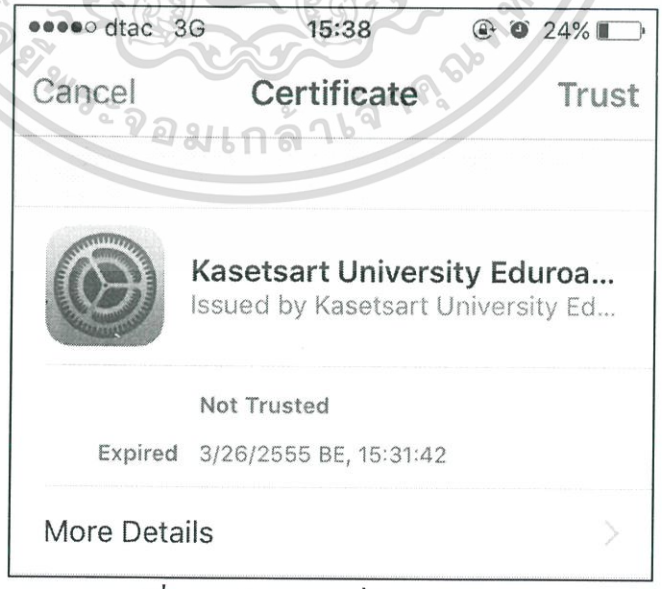
4.1.1 ทดลองใช้งานโดยการตั้งค่าที่โทรศัพท์ระบบปฏิบัติการ IOS โดยการใช้งานผ่านเครือข่าย eduroam ที่ติดตั้งไว้ ใช้ชื่อผู้ใช้งานที่ Uninet ให้มา ดังนี้

Username : guest-tru@uni.net.th

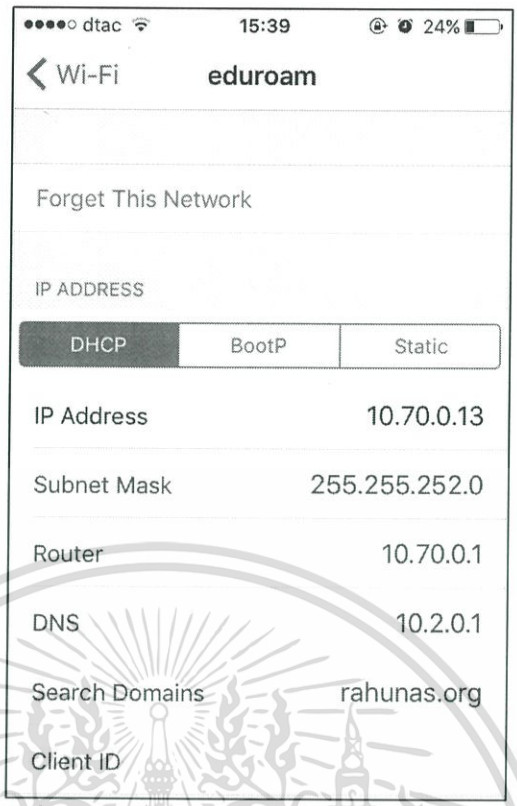
Password : xxxxxxxxx



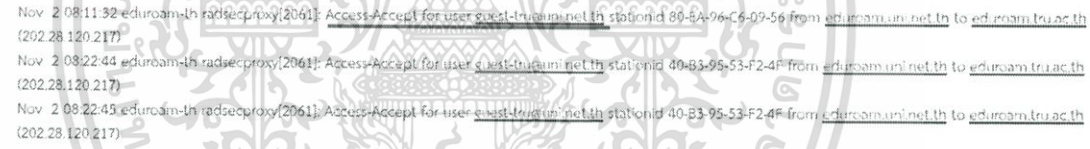
รูปที่ 4.1 ใส่ Username Password ที่ uninet ให้มา



รูปที่ 4.2 คลิก Trust เพื่อรับ Certificate



รูปที่ 4.3 แสดงไอพีแอดเดรสของเครื่องที่ได้รับ



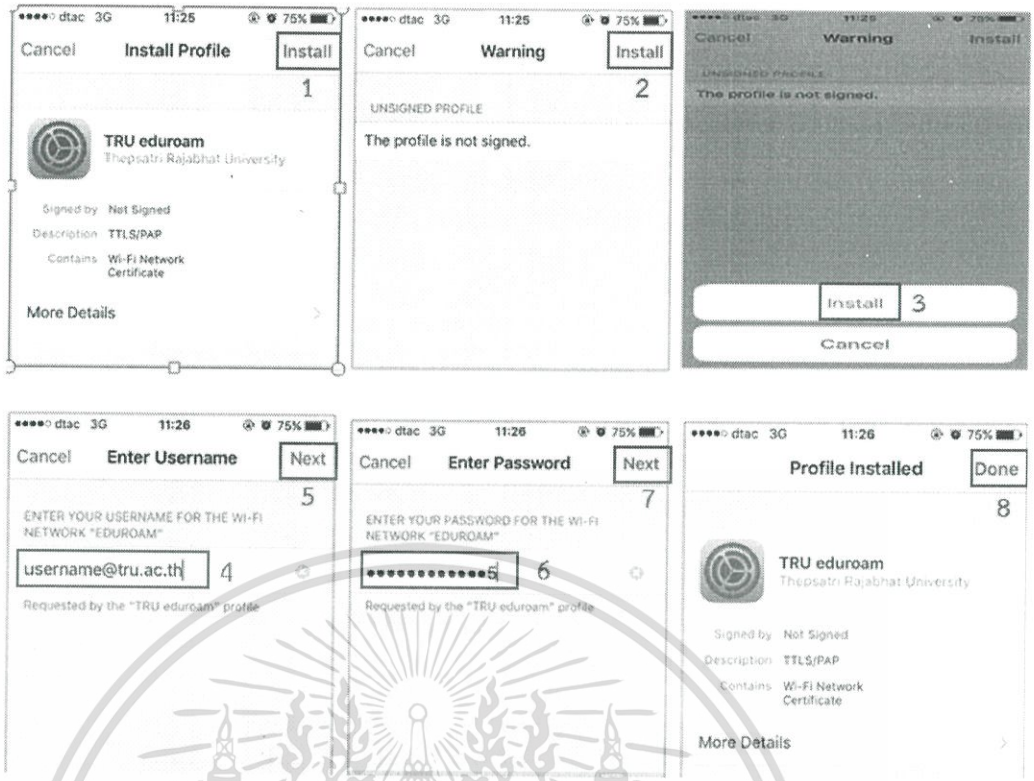
รูปที่ 4.4 รายการ log ของ uninet แสดงสถานะ Access-Accept

4.1.2 ทดลองใช้งานโดยการตั้งค่าที่โทรศัพท์ระบบปฏิบัติการ IOS โดยการใช้งานผ่านเครือข่าย eduroam ที่ติดตั้งไว้ ใช้ชื่อผู้ใช้งานของมหาวิทยาลัยออกให้ ดังนี้

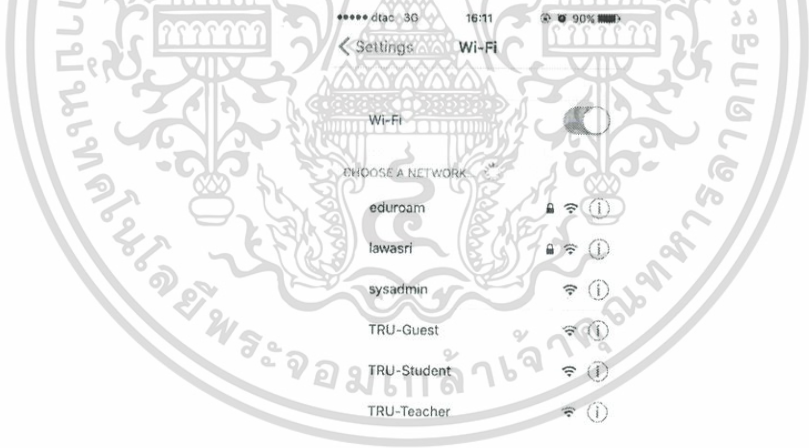
Username : guest-uninet@tru.ac.th

Password : xxxxxxxxx

ติดตั้ง profile โดยดาวน์โหลดจาก http://eduroam.tru.ac.th/file/eduroam.mobileconfig

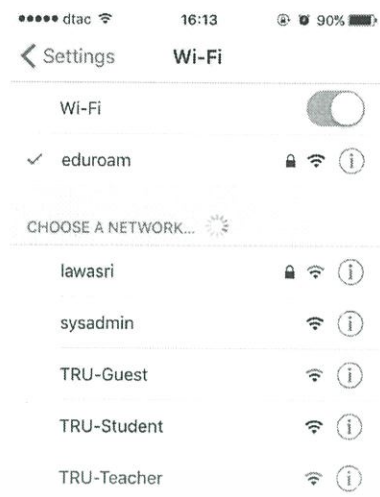


รูปที่ 4.5 แสดงการตั้งค่า profile TRU eduroam



รูปที่ 4.6 หัวข้อ CHOOSE A NETWORK… เพื่อเลือกเครือข่าย eduroam

รูปที่ 4.7 เลือก Accept เพื่อรับ Certificate



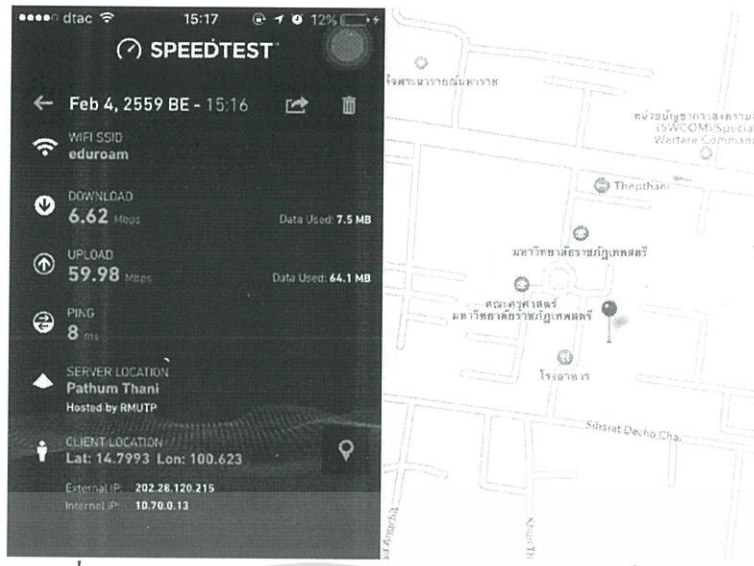
รูปที่ 4.8 แสดงสถานการณ์เชื่อมต่อเครือข่าย

Nov 2 16:10:08 eduroam-th radsecproxy[23663]: Access-Accept for user guest-uninet@tru.ac.th stat onid 48-51-b7-12-d3-e2 from eduroam.tru.ac.th to eduroam.uni.net.th (202.28.194.29)

รูปที่ 4.9 รายการ log แสดงสถานะ Access-Accept

```
Mon Nov  2 16:12:41 2015
        Packet-Type = Access-Accept
        Session-Timeout = 86400
        WISPr-Billing-Class-Of-Service = "default"
        WISPr-Bandwidth-Max-Up = 209715200
        WISPr-Bandwidth-Max-Down = 209715200
        MS-MPPE-Recv-Key = 0x346542868bbfc7c91f701efd8066968756fdf879c09a982c5439c3cd7675be4d
        MS-MPPE-Send-Key = 0x5335a1169f5ced1c36876a721b8d0890d4a7b5df2dfc0dfb230e1ceacc171ecd
        EAP-MSK = 0x346542868bbfc7c91f701efd8066968756fdf879c09a982c5439c3cd7675be4d5335a1169f5c
        EAP-EMSK = 0x4009fac563193b27ee2ad29043162e1ec884923e509aa16c2219c772c83160089124641 07ae
        EAP-Session-Id = 0x155637290ac37fd030d6c2d2fd5ff5a497fcd53e3e9b4a150e76b5790e7918c7d012f
        EAP-Message = 0x03050004
        Message-Authenticator = 0x00000000000000000000000000000000
        User-Name = "guest-uninet@tru.ac.th"
        Proxy-State = 0x3335
```

รูปที่ 4.10 logในเซิร์ฟเวอร์เรเดียส ของมหาวิทยาลัย



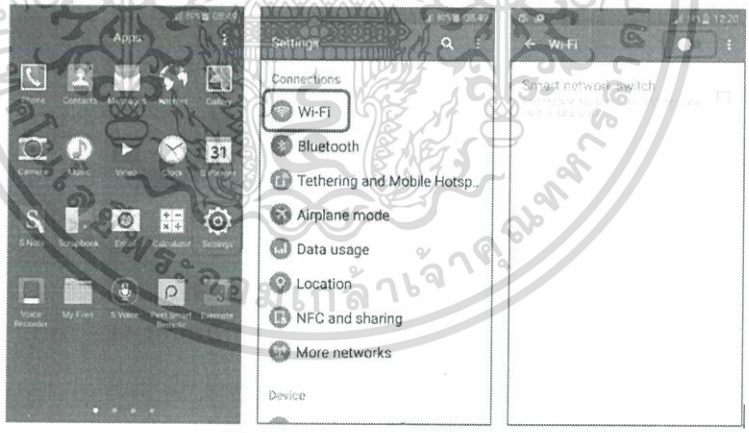
รูปที่ 4.11 ทดสอบความเร็วอินเทอร์เน็ตและตำแหน่งที่ทดสอบ

4.1.3 ทดลองใช้งาน โดยการตั้งค่าที่โทรศัพท์ระบบปฏิบัติการ androidโดยการใช้งานผ่านเครือข่าย eduroam ที่ติดตั้งไว้ ใช้ชื่อผู้ใช้งานของมหาวิทยาลัยออกให้ ดังนี้

Username : guest-uninet@tru.ac.th

Password : xxxxxxxx

1) เปิดหน้าต่าง Settings ภายใต้หัวข้อ Wi-Fi หากเป็น OFF ให้เปลี่ยนเป็น ON

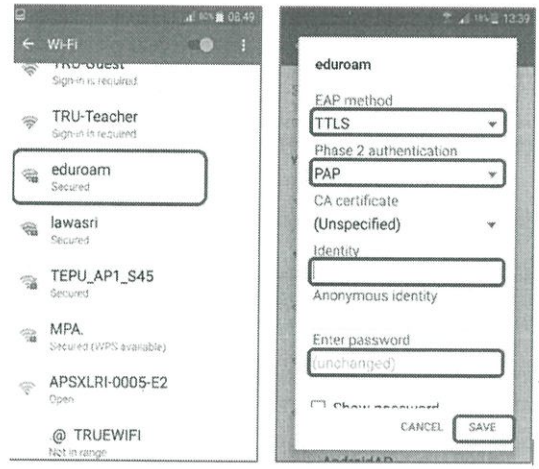


รูปที่ 4.12 เปิดการใช้งาน Wi-Fi

2) หัวข้อ Wi-Fi NETWORKS เลือก eduroam เลือกตัวเลือกตามภาพ และกรอกข้อมูล Username และ Password ของสถาบันท่าน และคลิกConnect (หัวข้อ Identity ใส่ username และหัวข้อ Enter Password ใส่ Password) ตัวอย่างชื่อบัญชีผู้ใช้ username@tru.ac.th และ password โดยเลือกชนิดการเชื่อมต่อดังนี้

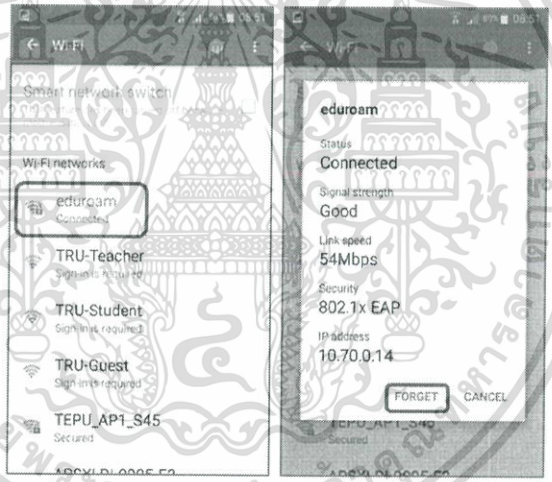
EAP method: TTLS

Phase 2 authentication: PAP



รูปที่ 4.13 ใส่ข้อมูลชื่อผู้ใช้งาน และรหัสผ่าน

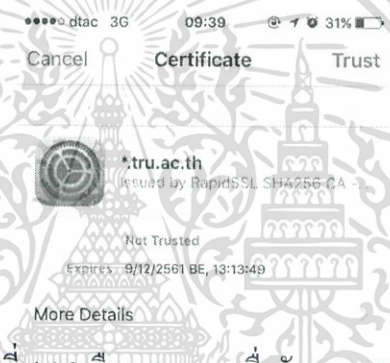
3) เมื่อเชื่อมต่อเสร็จสิ้น ภายใต้ชื่อ eduroam จะแจ้งความ Connected และสามารถใช้อินเทอร์เน็ตได้ ถ้าต้องการยกเลิกการเชื่อมต่อ (Disconnect) เลือก eduroam และคลิก Forget เพื่อยกเลิกการเชื่อมต่อ



รูปที่ 4.14 สถานการณ์เชื่อมต่อเครือข่าย eduroam

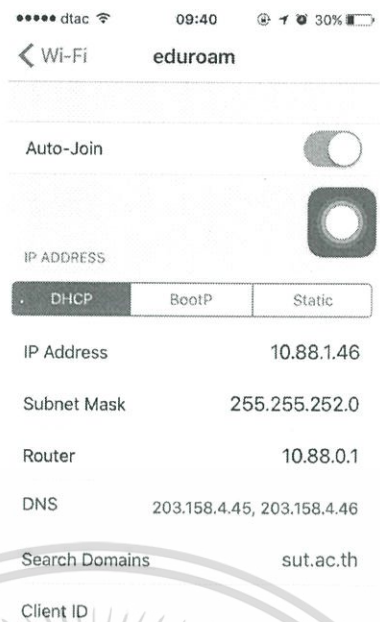
4.1.4 ผลการทดสอบที่มหาวิทยาลัยเทคโนโลยีสุรนารี

รูปที่ 4.15 หัวข้อ CHOOSE A NETWORK... เพื่อเลือกเครือข่าย eduroam

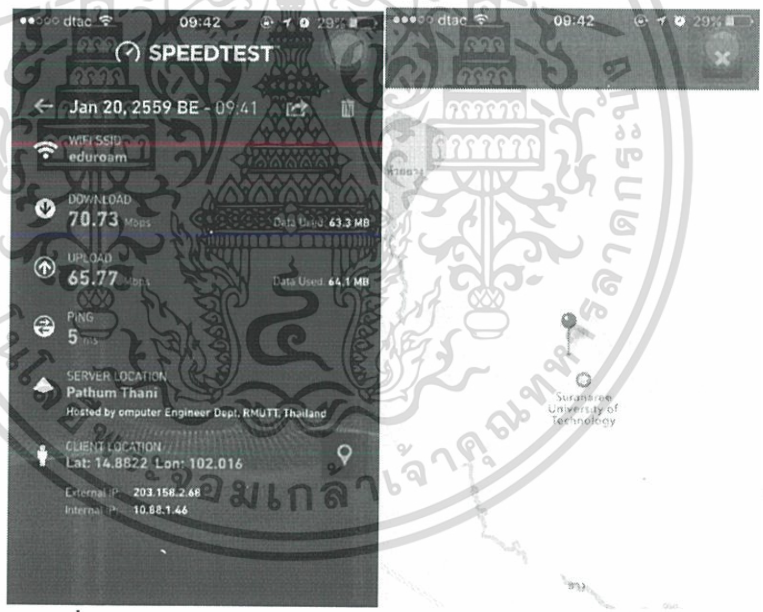


รูปที่ 4.16 เลือก Accept เพื่อรับ Certificate

รูปที่ 4.17 แสดงสถานการณ์เชื่อมต่อเครือข่าย

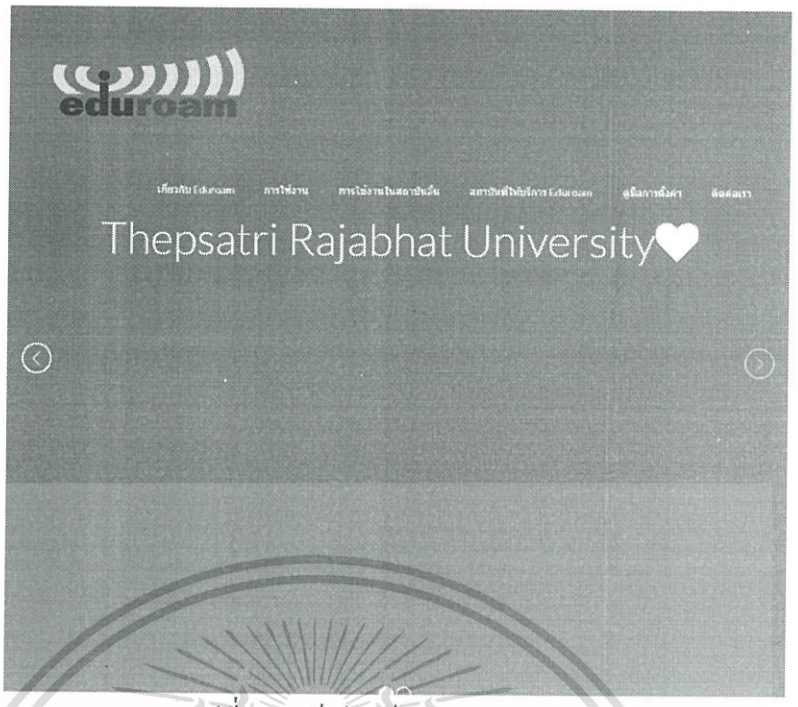


รูปที่ 4.18 แสดงหมายเลขไอพีแอดเดรสที่รับจากเอ็ดยูโรม

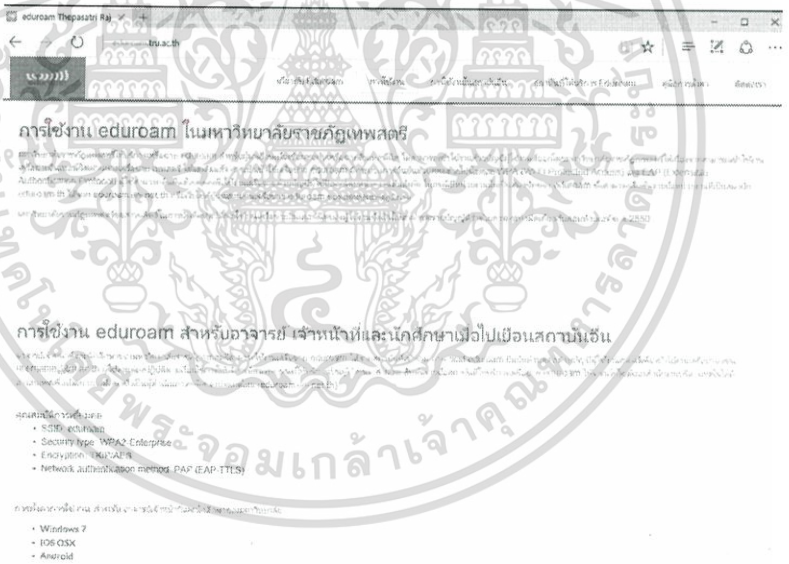


รูปที่ 4.19 ทดสอบความเร็วอินเทอร์เน็ตและตำแหน่งที่ทดสอบ

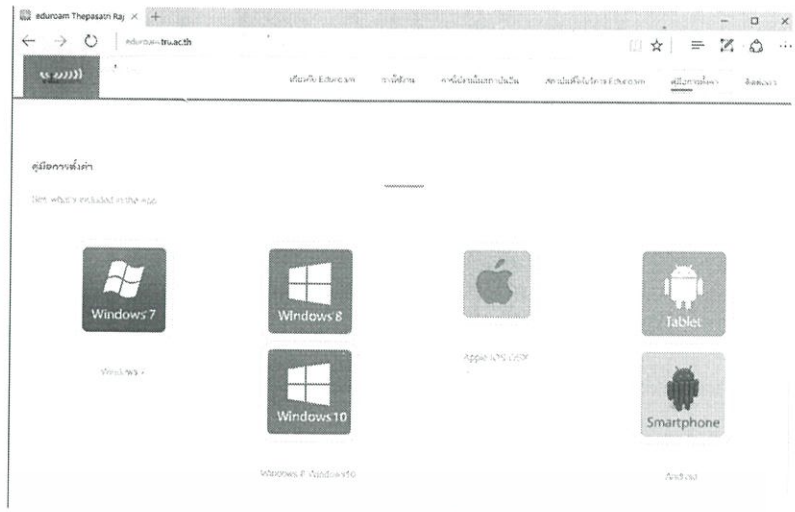
4.1.5 จัดทำเว็บไซต์เอ็ดยูโรมแสดงบนเว็บไซต์ของสถาบันการศึกษา เพื่อแจ้งให้ทราบเกี่ยวกับสถานที่ในการให้บริการเอ็ดยูโรมภายในมหาวิทยาลัยเกี่ยวกับ service ที่ให้บริการ และข้อมูลอื่นๆ เกี่ยวกับเอ็ดยูโรมพร้อมแจ้งกลับมายัง noc@uni.net.th เพื่อให้เจ้าหน้าที่บันทึก URL หน้า page eduroam ของมหาวิทยาลัยลงในระบบ



รูปที่ 4.20 เว็บไซต์ eduroam.tru.ac.th



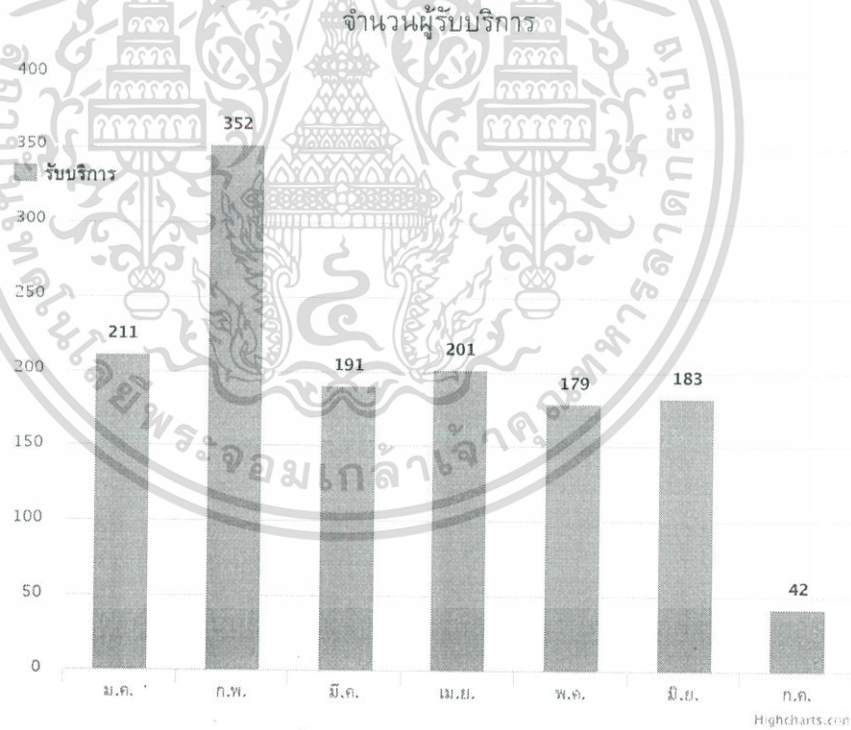
รูปที่ 4.21 เว็บไซต์การใช้งานเอ็ดยูโรมในมหาวิทยาลัยราชภัฏเทพสตรี



รูปที่ 4.22 เว็บไซต์การตั้งค่าเอ็ดยูโรม

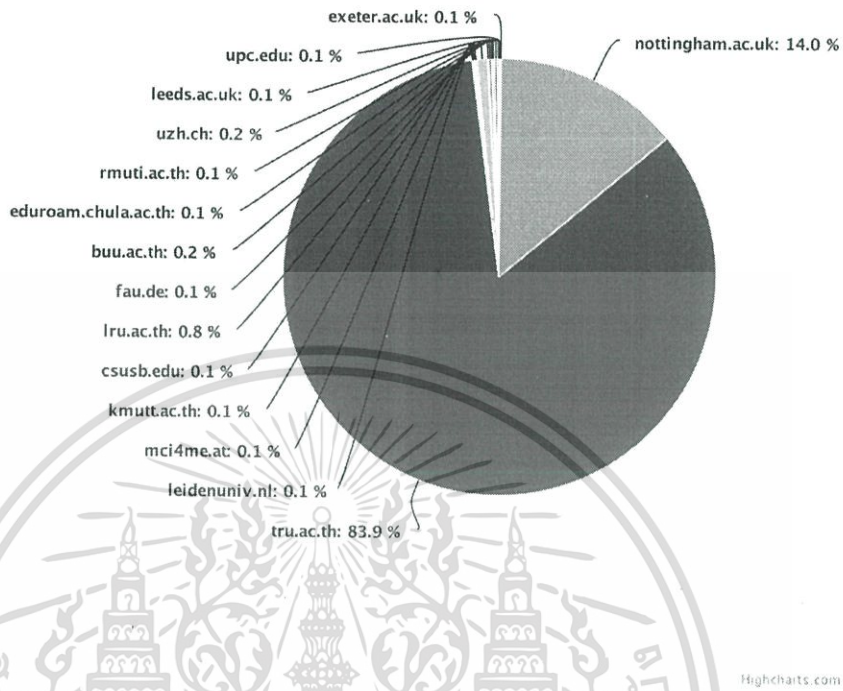
4.1.6 เว็บไซต์สถิติการใช้งานและตั้งค่าระบบ

แสดงจำนวนผู้ใช้งานแยกตามเดือนโดยเลือกเป็นปี พ.ศ.ได้ดังรูปที่ 4.23 และแยกตามโดเมนที่เข้าใช้งานได้ดังรูปที่ 4.24



รูปที่ 4.23 แสดงจำนวนผู้ใช้งาน

จำนวนผู้ใช้งานแยกตาม ชื่อผู้ใช้งาน ปี 2016



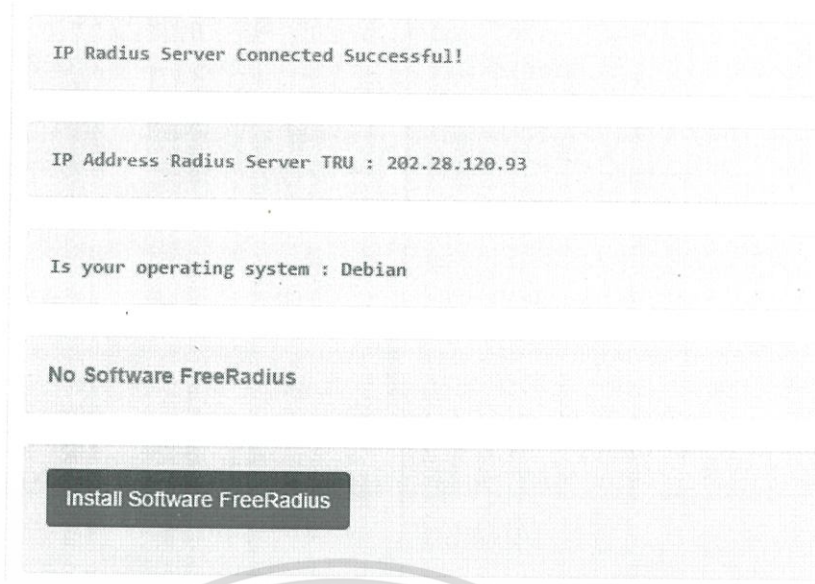
รูปที่ 4.24 แสดงจำนวนผู้ใช้งานแยกตามโดเมน

4.1.7 เว็บไซต์การตั้งค่าระบบกรณีที่ติดตั้งเรเดียสเซิร์ฟเวอร์ใหม่ให้เข้ามาทำการกรอกข้อมูลในเมนูการตั้งค่าระบบเพื่อเป็นการกำหนดค่าคอนฟิกของระบบโดยอัตโนมัติ ดังขั้นตอนต่อไปนี้

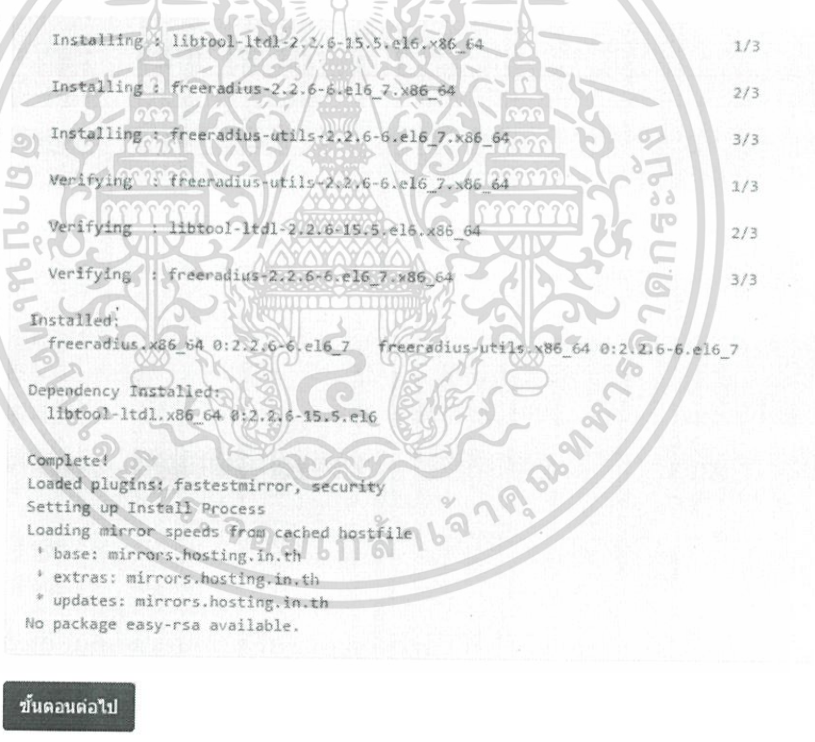
1) จะทำการกรอกข้อมูลของเครื่องเรดียสเซิร์ฟเวอร์ได้แก่ ip address ,username และ password ถ้าถูกต้องระบบจะทำการล็อกอินเข้าเครื่องเรดียสเซิร์ฟเวอร์เครื่องที่จะติดตั้งได้และทำการเช็คว่าเป็น OS ประเภทไหนจะทำการตรวจสอบว่าเครื่องเรดียสเซิร์ฟเวอร์มี Software Free RADIUS อยู่หรือไม่ถ้าไม่มีจะให้ทำการติดตั้งโดยสั่งจากระบบได้เลยดังรูปที่ 4.27

รูปที่ 4.25 แสดงหน้าจอใส่ข้อมูลเพื่อล็อกอินเข้าเครื่องเรดียสเซิร์ฟเวอร์

รูปที่ 4.26 แสดงข้อมูลล็อกอินเข้าเครื่องเรดียสเซิร์ฟเวอร์สำเร็จและติดตั้งSoftware Free Radius แล้ว

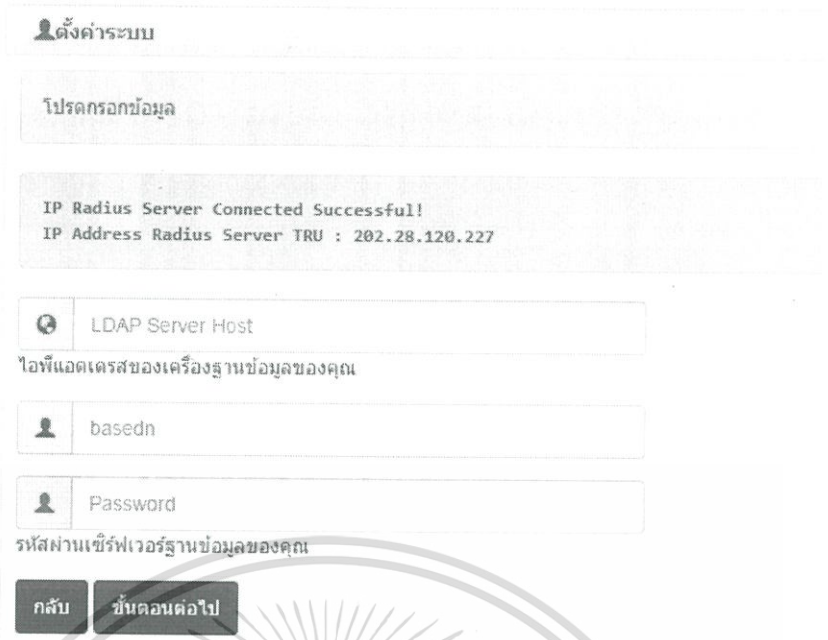


รูปที่ 4.27 แสดงข้อมูลล็อกอินเข้าเครื่องเรดียสเซิร์ฟเวอร์สำเร็จและยังไม่ได้ Software Free Radius



รูปที่ 4.28 แสดงข้อมูลการติดตั้ง Software Free Radius สำเร็จ

2) จะให้กรอกข้อมูลฐานข้อมูลที่ใช้งานเอ็ดยูโรม และก็จะทำการเช็คว่าข้อมูลที่กรอกมาใช้ได้ถูกต้องหรือไม่ ถ้าถูกจะไปขั้นตอนต่อไปดังรูปที่ 4.30



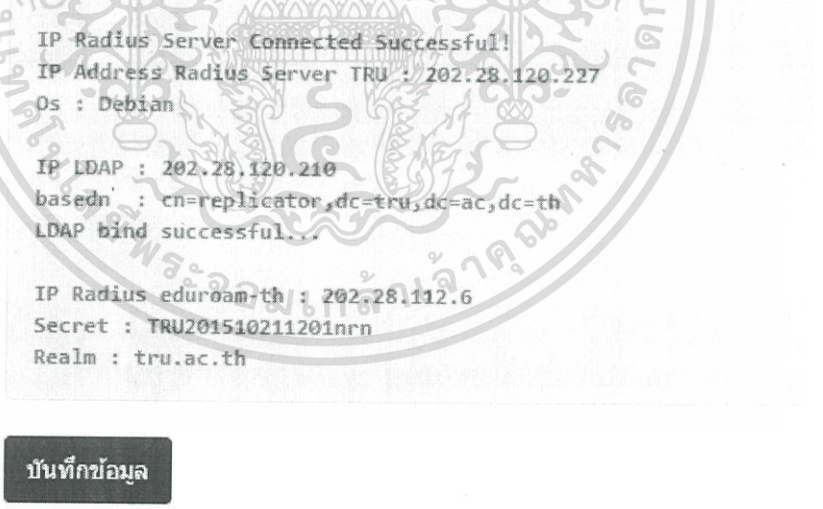
รูปที่ 4.29 หน้าจอใส่ข้อมูลของฐานข้อมูลที่ใช้งานเอ็ดยูโรม

รูปที่ 4.30 แสดงข้อมูลการเชื่อมต่อของฐานข้อมูลที่ใช้งานเอ็ดยูโรมสำเร็จ

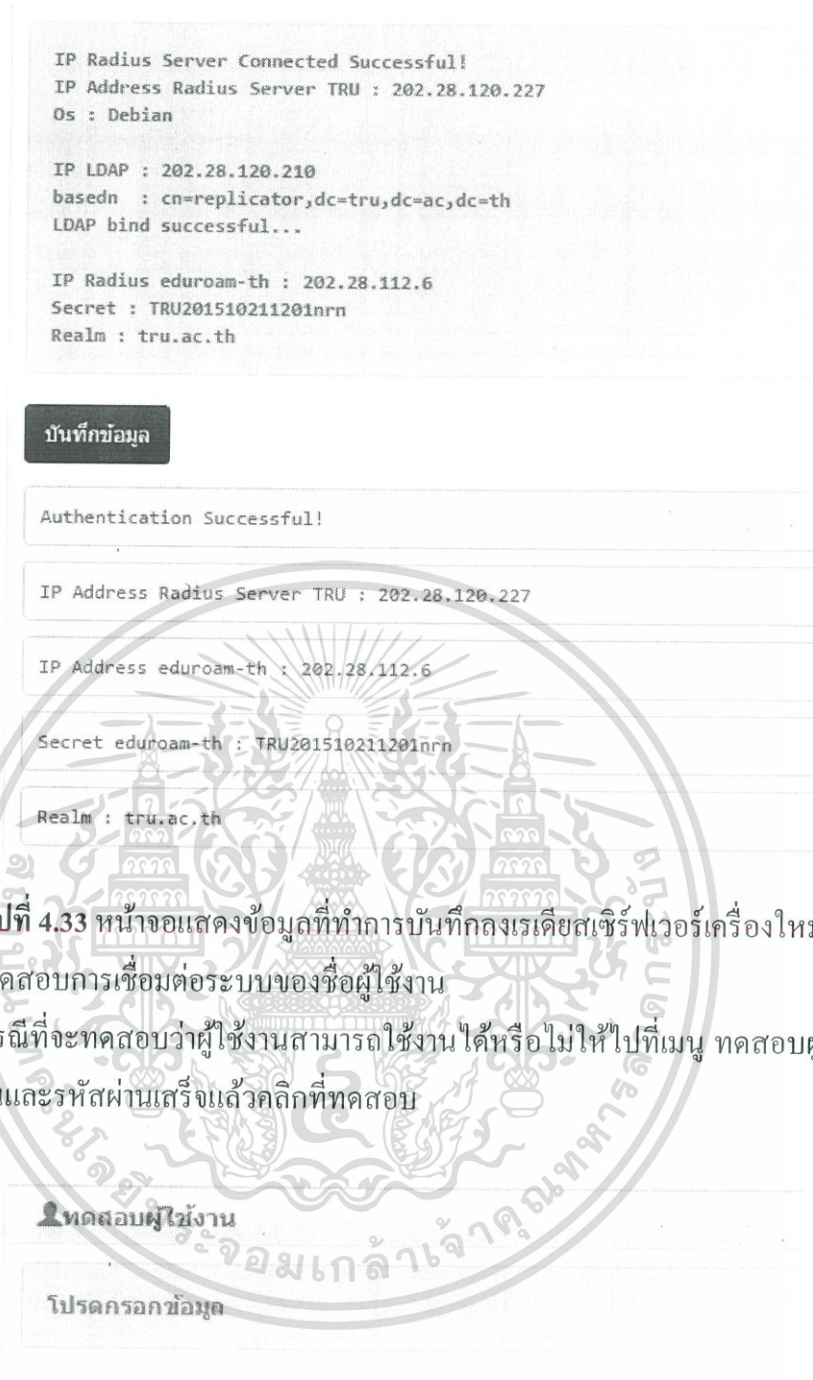
3) จะให้กรอกข้อมูลของ IP Server eduroam-th ,secret, realm ที่ Uninet ให้มาเพื่อทำการเชื่อต่อกับ Uninet-TH ดังรูปที่ 4.31

รูปที่ 4.31 หน้าจอใส่ข้อมูลเพื่อเชื่อมต่อเอ็ดยูโรมประเทศไทย

4) จะเป็นการตรวจสอบข้อมูลที่กรอกไปทั้งหมดว่าถูกต้องกรือไม่ถ้าถูกต้องก็คลิ๊กที่บันทึก ระบบจะทำการบันทึกค่าลงไฟล์และส่งไปยังเครื่องเรดียสเซิร์ฟเวอร์ปลายทาง ดังรูปที่ 4.32



รูปที่ 4.32 หน้าจอแสดงข้อมูลที่ทำการกรอกเข้าสู่ระบบเพื่อเชื่อมต่อเอ็ดยูโรมประเทศไทย



รูปที่ 4.33 หน้าจอแสดงข้อมูลที่ทำการบันทึกลงเรเดียสเซิร์ฟเวอร์เครื่องใหม่

4.1.8 ระบบทดสอบการเชื่อมต่อระบบของชื่อผู้ใช้งาน

ในกรณีที่จะทดสอบว่าผู้ใช้งานสามารถใช้งานได้หรือไม่ให้ไปที่เมนู ทดสอบผู้ใช้งาน แล้วใส่ชื่อผู้ใช้งานและรหัสผ่านเสร็จแล้วคลิกที่ทดสอบ

รูปที่ 4.34 หน้าจอใส่ข้อมูลเพื่อทดสอบผู้ใช้งาน

```
Sending Access-Request packet to host 127.0.0.1 port 1812, id=46, length=0
        User-Name = "nutthunyapong.s@tru.ac.th"
        User-Password = "0---@---1985"
        NAS-IP-Address = 202.28.120.217
        NAS-Port = 0
        Message-Authenticator = 0x00
        EAP-Code = Response
        EAP-Type-Identity = 0x6e75747468756e7961706f6e672e73407472752e61632e7468
        EAP-Message = 0x022d001e016e75747468756e7961706f6e672e73407472752e61632e7468
Received Access-Challenge packet from host 127.0.0.1 port 1812, id=46, length=64
        EAP-Message = 0x012e00061520
        Message-Authenticator = 0x58b78978125568d04ed82c864917f3cc
        State = 0x7905bba2792baed9ce868a3c9e6a1c3f
        EAP-Id = 46
        EAP-Code = Request
        EAP-Type-EAP-TTLS = 0x20

Connected Successful!

Username : nutthunyapong.s@tru.ac.th
```

รูปที่ 4.35 หน้าจอแสดงผลการทดสอบชื่อผู้ใช้งานที่เชื่อมต่อได้

```
Sending Access-Request packet to host 127.0.0.1 port 1812, id=203, length=95
        User-Name = "guest-tru"
        User-Password = "ssss"
        NAS-IP-Address = 202.28.120.217
        NAS-Port = 0
        Message-Authenticator = 0x00000000000000000000000000000000
        EAP-Code = Response
        EAP-Type-MD5-Challenge = 0x10f4db8dbd1f4464b4ee94d336ef05912c
        EAP-Id = 202
        State = 0x8e08cae88ec2ce45c57c399d24f971d7
        EAP-Message = 0x02ca00160410f4db8dbd1f4464b4ee94d336ef05912c
Received Access-Reject packet from host 127.0.0.1 port 1812, id=203, length=44
        EAP-Message = 0x04ca0004
        Message-Authenticator = 0xd9bc655661155584e73681e30d8b2b1f
        EAP-Id = 202
        EAP-Code = Failure

No Connected
Username : guest-tru
```

รูปที่ 4.36 หน้าจอแสดงผลการทดสอบชื่อผู้ใช้งานที่เชื่อมต่อไม่ได้

บทที่ 5
สรุปผล

5.1 สรุปผล

เอ็ดยูโรมเป็นเครือข่ายไร้สายที่ช่วยให้ผู้ใช้สามารถใช้ข้อมูลชื่อผู้ใช้งาน และ รหัสผ่านจากหน่วยงานต้นสังกัด เข้าใช้งานเครือข่ายไร้สายที่สถาบันการศึกษาที่เปิดใช้งานเอ็ดยูโรมเพื่อการเข้าถึงทรัพยากรของเครือข่าย ในระหว่างการดำเนินการได้กำหนดค่าเรเดียสเซิร์ฟเวอร์ที่จะทำหน้าที่เป็นผู้ให้บริการ (SP) ที่เชื่อมต่อพร็อกซีเซิร์ฟเวอร์ โดยมีนโยบายเครือข่ายและกำหนดค่าสวิทช์และ เซิร์ฟเวอร์เรเดียสของมหาวิทยาลัยราชภัฏเทพสตรี เป็นเซิร์ฟเวอร์ที่ตรวจสอบข้อมูลจากฐานข้อมูล LDAP โดยเป็นฐานข้อมูลที่เก็บข้อมูลผู้ใช้งานและรหัสผ่าน

ขั้นตอนการตรวจสอบโดยใช้เทคโนโลยี 802.1X ในการพิสูจน์สิทธิ์ก่อนที่จะอนุญาตให้เข้าถึงเครือข่ายเป็นระบบที่ดีที่สามารถนำไปใช้ในหลายสถาบันเพื่อป้องกันไม่ให้เกิดการเชื่อมต่อที่ไม่พึงประสงค์ ในโครงการนี้ได้นำเอ็ดยูโรมไปใช้งานทั้งอาจารย์ เจ้าหน้าที่และนักศึกษาจากมหาวิทยาลัยราชภัฏเทพสตรีสามารถโดยจะใช้ข้อมูลประจำตัวของแต่ละบุคคลที่มหาวิทยาลัยออกให้ เข้าสู่ระบบ ในทุกสถานที่ที่เปิดใช้งานเอ็ดยูโรม พร้อมกันนี้ผู้ที่อยู่ภายนอกมหาวิทยาลัยที่เดินทางมาอบรม ณ มหาวิทยาลัยราชภัฏเทพสตรี สามารถใช้งานเครือข่ายเอ็ดยูโรม โดยใช้ข้อมูลประจำตัวที่ต้นสังกัดออกให้ได้ตลอดเวลา เพื่อใช้ในการเข้าใช้งานเครือข่ายอินเทอร์เน็ต

5.2 ปัญหาและอุปสรรค

5.2.1 ระบบไม่สามารถสั่ง insstall RADIUS Service ผ่านเว็บไซต์ได้เนื่องจาก ผู้ใช้ชื่อ Apache ซึ่งเป็นชื่อผู้ใช้ของ Web Server ไม่มีสิทธิเรียกใช้คำสั่งของ Root ได้วิธีแก้ไขคือต้องทำการติดตั้ง SSH2 จึงสามารถล็อกอินและติดตั้งโปรแกรมผ่านวับไซต์ได้โดยใช้ชื่อ root และรหัสผ่านล็อกอินได้เลย

5.2.2 ระบบไม่สามารถใช้งานโพรโทคอล EAP-TLS ได้เพราะรูปแบบการเก็บรหัสผ่านต้องเป็นแบบ Plaintext-Password แต่ของมหาวิทยาลัยเป็นแบบ SSHA จึงได้ทดลองเปลี่ยนเป็นแบบ EAP-TTLS ซึ่งสามารถใช้กับรูปแบบของรหัสผ่านแบบ SSHA ได้

บรรณานุกรม

จตุชัย แพงจันทร์.2553. **Master in Security**. นนทบุรี: ไอดีซี พรีเมียร์

นิวัติ เนียมพลอย, น.ท. **การรักษาความปลอดภัยของข้อมูลข่าวสาร**. [Online] Available: https://nniwat.wordpress.com/2010/10/27การรักษาความปลอดภัยของ/

สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา.**eduroam คืออะไร**.[Online] Available: http://eduroam.uni.net.th/eduroam-th/index.php?var=about&lang=thai.

GÉANT & TERENA, historic of eduroam about how it started and in where it was tested first.[Online] Available: https://www.eduroam.org/index.php?p=about.

Krishna Sankar, Sri Sundaralingam, Darrin Miller, Andrew Balinsky. 2004. **Cisco Wireless LAN Security.** Cisco Press.

OpenLDAP Software 2.4 Administrator's Guide .[Online] Available: http://www.openldap.org/doc/admin24/.

Paul, Arana.2006. **Benefits and vulnerabilities of Wi-Fi Protected Access 2 (WPA2)**. [Online] Available: http://cs.gmu.edu/~yhwang1/INFS612/

RADIUS - Attributes Format.[Online] Available: http://www.tutorialspoint.com/radius/radius_attribute_format.htm.

Sample_Projects/Fall_06_GPN_6_Final_Report.pdf.

Remote authentication dial-in user service server.[Online] Available: http://www-01.ibm.com/support/knowledgecenter/ssw_aix_71/com.ibm.aix.security/radius_server.htm?lang=th.

ภาคผนวก ก.

นโยบายการเข้าร่วม eduroam ประเทศไทย

1. เกี่ยวกับเอกสารฉบับนี้
   1) เอกสารฉบับนี้ใช้เพื่อเป็นแนวทางในการใช้งาน และให้บริการการเชื่อมต่อเครือข่าย eduroam เพื่อวัตถุประสงค์ทางการศึกษา
   2) eduroam ย่อมาจาก “educational roaming” เป็นเครื่องหมายที่จดทะเบียนโดย TERENA ที่ก่อกำเนิดจากเครือข่ายการศึกษาและวิจัยของยุโรป (NRENs) เพื่อการใช้งานเครือข่ายที่เรียบง่ายปลอดภัย และรองรับผู้ใช้งานที่ขยายตัวเพิ่มมากขึ้นได้
   3) นิยาม
      3.1) สำนักงานฯ หมายถึง สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา (UniNet) สังกัดสำนักงานคณะกรรมการการอุดมศึกษา
      3.2) NRO หรือ National Roaming Operator for Thailand หมายถึง ผู้ดำเนินการหลักของ eduroam ของประเทศไทย โดยผู้รับผิดชอบหลักของโครงการนี้ คือ สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา (UniNet)
      3.3) IdP หรือ Identity Provider หมายถึง สถาบันต้นสังกัด หรือสถาบันการศึกษาที่เป็นผู้กำหนดและตรวจสอบการยืนยันตัวตนการเข้าใช้งานของคณาจารย์ เจ้าหน้าที่ และนิสิตนักศึกษาของสถาบันของตน
      3.4) SP หรือ Service Provider หมายถึง สถาบันที่ให้บริการการเชื่อมต่อ หรือสถาบันการศึกษาที่ให้บริการเครือข่ายแก่ผู้มาเยือนให้เชื่อมต่อเข้าเครือข่าย eduroam ได้ โดยจะอนุญาตการเข้าใช้งานเมื่อสถาบันต้นสังกัดของผู้ใช้ที่มาเยือน ตอบยืนยันตัวตน
2. บทบาทและความรับผิดชอบ
   1) สำนักงานฯ เป็นผู้รับผิดชอบโครงการนี้ โดยทำหน้าที่เป็นผู้ดำเนินการหลักของประเทศไทย (National Roaming Operator for Thailand) เรียกโดยย่อว่า NRO
   2) สถาบันการศึกษาที่เข้าร่วมโครงการ ทำหน้าที่เป็นผู้ตรวจสอบสิทธิ์การใช้งาน เรียกว่า สถาบันต้นสังกัด (Identity Provider) เรียกโดยย่อว่า IdP
   3) สถาบันการศึกษาที่เข้าร่วมโครงการ ทำหน้าที่ให้บริการเครือข่าย เพื่อให้ผู้มาเยือนเชื่อมต่อเข้าเครือข่ายได้เรียกว่าสถาบันที่ให้บริการการเชื่อมต่อ (Service Provider) เรียกโดยย่อว่า SP
   4) สถาบันการศึกษาที่เข้าร่วมโครงการจะต้องรับหน้าที่ทั้ง IdP และ SP
3. ผู้ดำเนินการหลักของประเทศไทย (NRO)
   1) สำนักงานฯ เป็นผู้รับผิดชอบการให้บริการ eduroam สำหรับประเทศไทย โดยทำหน้าที่เป็นผู้กำหนดนโยบายการใช้งานระดับประเทศ

2) บทบาทหลักของ สำนักงานฯ คือ

(1) ประสานงาน ช่วยเหลือ และสนับสนุนการให้บริการ eduroam โดยกำหนดให้มีรายชื่อผู้ประสานงานอย่างชัดเจน

(2) รักษาสภาพการเชื่อมต่อกับ eduroam ทั้งในประเทศและต่างประเทศ

(3) จัดเตรียมหน้าเว็บเพจ eduroam เพื่อให้ข้อมูลที่เกี่ยวข้อง

4. สถาบันต้นสังกัด (IdP)

1) ทำหน้าที่เป็นผู้กำหนดและตรวจสอบการยืนยันตัวตนการเข้าใช้งานแก่คณาจารย์ เจ้าหน้าที่ และนิสิตนักศึกษาของสถาบันต้นสังกัด

2) ทำหน้าที่เป็นผู้ให้คำแนะนำ ให้ความรู้ และความช่วยเหลือแก่ผู้ใช้งานของสถาบัน เมื่อเข้าใช้งานที่สถาบันที่ให้บริการการเชื่อมต่อในที่ต่างๆ และแจ้งให้ผู้ใช้งานทราบว่าการใช้งานเครือข่ายอาจจะมีการเก็บบันทึกข้อมูลการจราจร

3) ทำหน้าที่บันทึกข้อมูลการตรวจสอบการยืนยันตัวตนและการอนุมัติการเข้าใช้งาน และให้ข้อมูลที่จำเป็นแก่ NRO เพื่อแก้ปัญหา

4) จัดเตรียมบัญชีผู้ใช้งานทดสอบ (test account) เพื่อให้ NRO ใช้ในการทดสอบเท่านั้น และไม่สามารถนำบัญชีนี้ไปใช้งานเครือข่ายตามปกติได้

5) เป็นผู้รับภาระดำเนินการต่อพฤติกรรมการใช้งานที่ผิดประเภทหรือขัดต่อกฎหมายของผู้ใช้งานในสังกัด

6) ต้องมีการกำหนดเจ้าหน้าที่เพื่อทำหน้าที่แก้ไขปัญหาให้กับผู้ใช้งานและเป็นผู้ประสานงานกับทาง NRO อย่างชัดเจน

7) ทำหน้าที่ประสานงานกับทาง NRO เพื่อแก้ปัญหาเรื่องความปลอดภัย และตอบสนองต่อการร้องขอของ NRO ในช่วงเวลาที่เหมาะสม

5. สถาบันที่ให้บริการการเชื่อมต่อ (SP)

1) เป็นผู้ให้บริการการเชื่อมต่อ โดยจะอนุญาตการเข้าใช้งานเมื่อสถาบันต้นสังกัดของผู้ใช้ที่มาเยือน(IdP) ตอบยืนยันตัวตน

2) แจ้งให้ผู้ใช้งานที่มาเยือนทราบถึงลักษณะการบันทึกข้อมูลการใช้งานเครือข่ายอย่างชัดเจน

3) ทำหน้าที่ให้บริการผ่านเครือข่ายไร้สายตามมาตรฐาน IEEE 802.11 g หรือดีกว่า โดยประกาศชื่อ SSID เป็น “eduroam” (ตัวพิมพ์เล็กทั้งหมด) โดย SP จะต้องไม่ใช้การล็อกอินผ่านเว็บ (WebLogin) กับผู้ใช้งานที่มาเยือน

4) ทำหน้าที่ตั้งค่าระบบความปลอดภัยคือ การยืนยันตัวตนแบบ IEEE 802.1X (EAP) หรือดีกว่า โดยไม่ รวมถึง EAP-MD5 และมีการใช้งาน WPA/TKIP หรือดีกว่า (แนะนำให้ใช้ WPA2)

5) อนุญาตให้ผู้ใช้งานที่มาเยือนสามารถใช้โพรโทคอล VPN, OpenVPN, http, https, pop, pop3s,imap, imaps และ ssh เป็นอย่างน้อย

6) ควรกำหนดให้ eduroam ใช้งานผ่าน VLAN ที่แยกออกจากการใช้งานเครือข่ายอื่น

7) ควรกำหนดให้ eduroam จ่าย IP จริง (Public IP address) โดยเป็น IPv4 หรือ IPv6

8) ต้องไม่เก็บค่าบริการใช้งาน eduroam

6. ผู้ใช้งานที่มาเยือน (User)

1) ต้องปฏิบัติตามนโยบายการใช้งานทั้งของสถาบันต้นสังกัด (IdP) และสถาบันที่ให้บริการการเชื่อมต่อ (SP) รวมถึงปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2550

2) เป็นผู้รับชอบในการเชื่อมต่อกับ eduroam ซึ่งเป็นตัวจริง (genuine) ของแต่ละ SP ตามคำแนะนำของ IdP ก่อนที่จะกรอกชื่อบัญชีและรหัสผู้ใช้เพื่อเข้าใช้งาน

3) ต้องเป็นผู้รับผิดชอบต่อบัญชีและรหัสผ่านของตนเอง ถ้าสงสัยว่าบัญชีที่ใช้งานไม่ปลอดภัย ต้องรีบติดต่อกลับไปยัง IdP ทันที

4) เป็นผู้ที่แจ้งเหตุผิดปกติของ eduroam ต่อ IdP และ SP (ถ้าเป็นไปได้)

7. การบันทึกข้อมูล (Logging)

1) IdP และ SP ต้องบันทึกทั้งการยืนยันตัวตนและการร้องขอ (authentication and accounting requests) อย่างน้อยดังนี้

(1) วัน เวลา ที่ได้รับการร้องขอ

(2) อัตลักษณ์ของผู้ร้องขอ (RADIUS request's identifier)

(3) ผลการร้องขอการยืนยันตัวตน พร้อมเหตุผลหากถูกปฏิเสธ

(4) ค่าสถานะ accounting

2) SP ต้องบันทึกการเชื่อมต่อ DHCP ดังต่อไปนี้

(1) วัน เวลา ที่อนุญาตรวมถึงระยะเวลาที่อนุญาต

(2) MAC address ของผู้ใช้ที่มาเยือน

(3) IP address ของผู้ใช้ที่มาเยือน

(4) ระยะเวลาการเก็บบันทึกข้อมูลของ DHCP อย่างน้อย 3 เดือน หรือตามกฎหมายกำหนด

8. การให้ความช่วยเหลือ

1) IdP ควรจัดเตรียมการช่วยเหลือแก่ผู้ใช้งานของตนในการเข้าใช้งานที่สถาบัน SP ต่างๆ

2) SP ควรจัดเตรียมความช่วยเหลือแก่ผู้ใช้งานที่มาเยือน

3) SP ควรจัดเตรียมข้อมูลพื้นฐานเกี่ยวกับการใช้งาน eduroam บนหน้าเว็บเพจของทางสถาบันให้ชัดเจนซึ่งประกอบด้วยข้อมูลดังนี้

(1) ข้อความที่ยืนยันถึงเอกสารฉบับนี้ที่ประกาศใช้อย่างชัดเจนที่เว็บเพจของ NRO หน้าที่เกี่ยวกับ eduroam

(2) มี URL เชื่อมไปยังหน้านโยบายการใช้งานของ SP

(3) รายการ หรือแผนที่ ที่กำหนดตำแหน่งที่ให้บริการ eduroam

(4) รายละเอียดที่มีการประกาศ SSID "eduroam" แบบ broadcast หรือ ไม่ broadcast

(5) รายละเอียดขั้นตอนการยืนยันตัวตน และบริการที่มีให้

(6) รายละเอียดเกี่ยวกับการใช้งาน non-transparent application proxy รวมถึงการตั้งค่า (ถ้ามี)

(7) มี URL เชื่อม ไปยังหน้าเว็บของ NRO พร้อมทั้ง logo และ trademark ของ eduroam

(8) มีรายละเอียดแจ้งให้ชัดเจนถึงนโยบาย ลักษณะการจัดเก็บข้อมูลการใช้งาน สิ่งที่เก็บ และ ระยะเวลาที่เก็บ

9. การติดต่อสื่อสารระหว่างสถาบัน

1) สถาบันที่เข้าร่วม eduroam ต้องเตรียมรายชื่อผู้ประสานงานและแก้ปัญหาร่วมกันกับทาง NRO โดยมีผู้ประสานงานหลัก 1 คน และผู้ประสานงานรองอีก 1 คน พร้อมรายละเอียดการติดต่อ และต้องแจ้งกับทาง NRO ถ้ามีการเปลี่ยนแปลงรายชื่อตามเวลาที่เหมาะสม

2) สถาบันที่เข้าร่วม eduroam ต้องแจ้งมายัง NRO เมื่อพบเหตุทางด้านความปลอดภัย การใช้งานผิดประเภท การขัดข้องของการใช้งาน และการเปลี่ยนแปลงนโยบายการเข้าใช้งาน

10. การบังคับใช้ และการระงับการใช้งาน

1) สิทธิ์ในการบังคับใช้งานและการเปลี่ยนแปลงของเอกสารฉบับนี้เป็นของ NRO

2) การเปลี่ยนแปลงใดๆ ของเอกสารฉบับนี้จะเป็นไปตามความเห็นชอบของหน่วยงานที่เข้าร่วมและNRO

3) สถาบันที่เชื่อมต่อเข้ากับ eduroam ของประเทศไทย ถือว่ายอมรับในนโยบายการใช้งานที่กำหนดขึ้นโดยเอกสารฉบับนี้

4) ในกรณีที่เกิดความจำเป็น NRO มีสิทธิ์ในการหยุดให้บริการ eduroam หรือให้บริการแบบมีข้อจำกัดทั้งนี้NRO จะต้องแจ้งถึงเหตุและความจำเป็นดังกล่าวแก่สถาบันที่เข้าร่วมรับทราบ

5) NRO จะติดต่อหรือส่ง email เหตุต่างๆ ไปยังผู้ประสานงาน โดยอาจต้องการความร่วมมือในการแก้ปัญหาจากสถาบันที่เข้าร่วม ถ้าไม่มีการติดกลับหรือการให้ความร่วมมือ ทาง NRO ขอสงวนสิทธิ์ในการปิดการเชื่อมต่อ eduroam ของสถาบันนั้นๆ

6) SP สามารถตั้งค่าเครือข่ายของตน เพื่อไม่ให้บริการแก่ผู้ใช้บางคน หรือทุกคนจากบางสถาบันได้

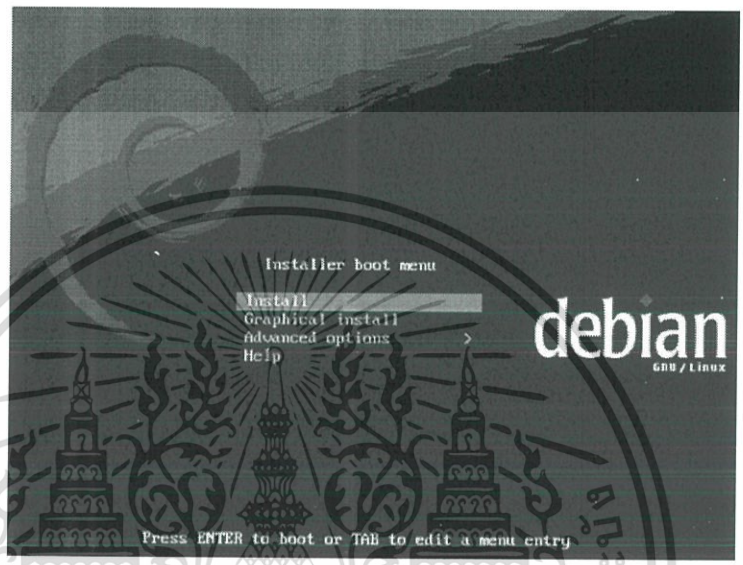
7) IdP อาจถอนหรือไม่อนุญาตให้ผู้ใช้บางคนของตน เข้าใช้งาน eduroam ได้โดยการถอนบัญชีผู้ใช้จากฐานข้อมูลที่ใช้ในการยืนยันตัวตน
8) IdP ต้องให้ความมั่นใจว่า ผู้ใช้งานของตนที่ทำผิดจะได้รับบทลงโทษตามนโยบายของสถาบันต้นสังกัดโดยไม่ขึ้นกับเวลาและพื้นที่ที่ประกอบความผิด

ภาคผนวก ข.

วิธีการติดตั้งระบบปฏิบัติการ

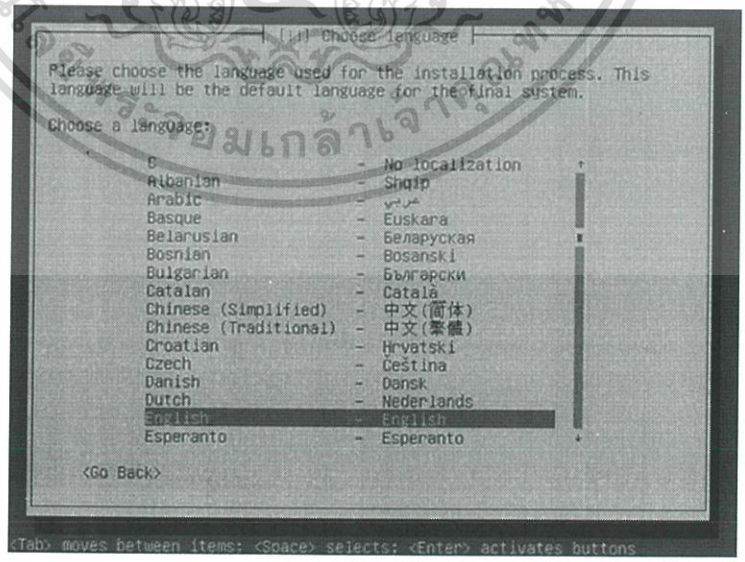
1. ติดตั้งระบบปฏิบัติการ Debian

1.1 ติดตั้งระบบปฏิบัติการ Debian นำแผ่นติดตั้งใส่เครื่องอ่าน CD/DVD และเริ่ม Boot พร้อมกับเลือก Install



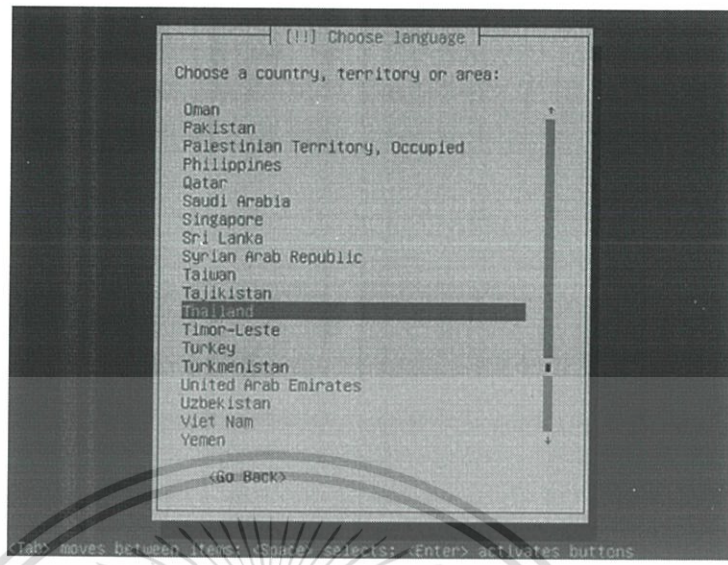
รูปที่ ข.1 หน้าเลือกการติดตั้ง

1.2 เลือกภาษา อังกฤษ (English) ในการติดตั้ง



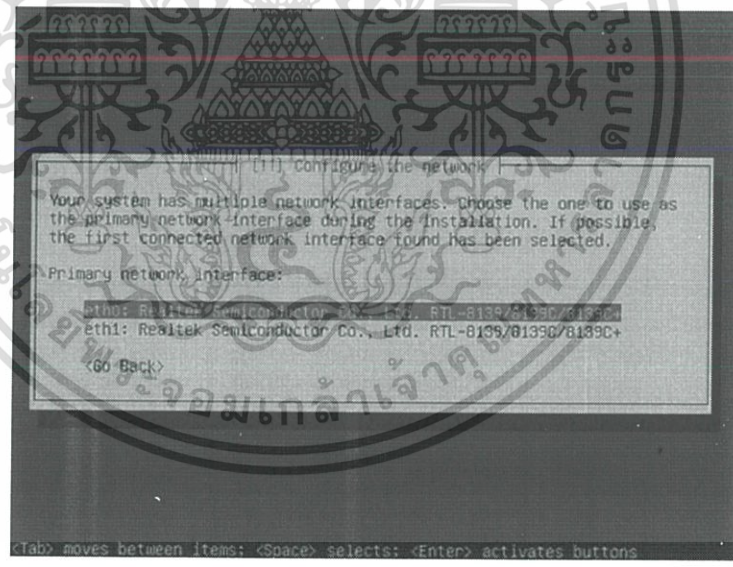
รูปที่ ข.2 หน้าเลือกภาษา

1.3 เลือกภาษา ประเทศ Thailand



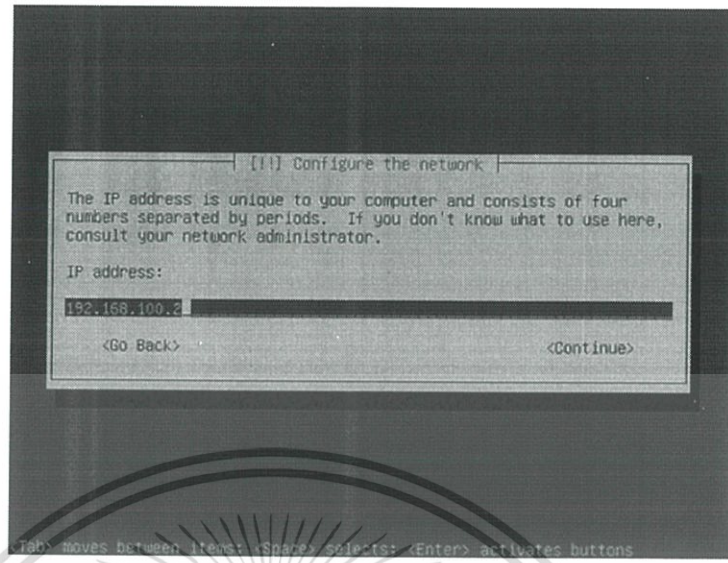
รูปที่ ข.3 หน้าเลือกประเทศไทย

1.4 เลือก Network Interface ที่ใช้เชื่อมต่ออินเทอร์เน็ต



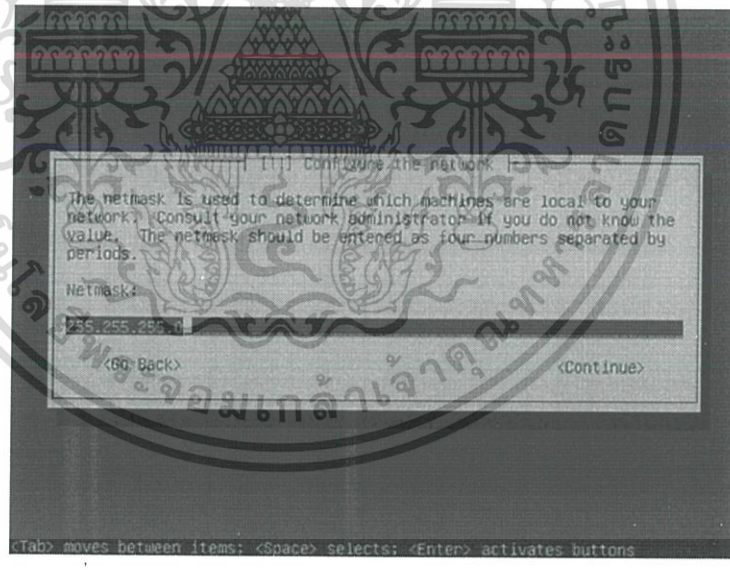
รูปที่ ข.4 เลือก Network Interface ที่ใช้เชื่อมต่ออินเทอร์เน็ต

1.5 ตั้งค่า IP address



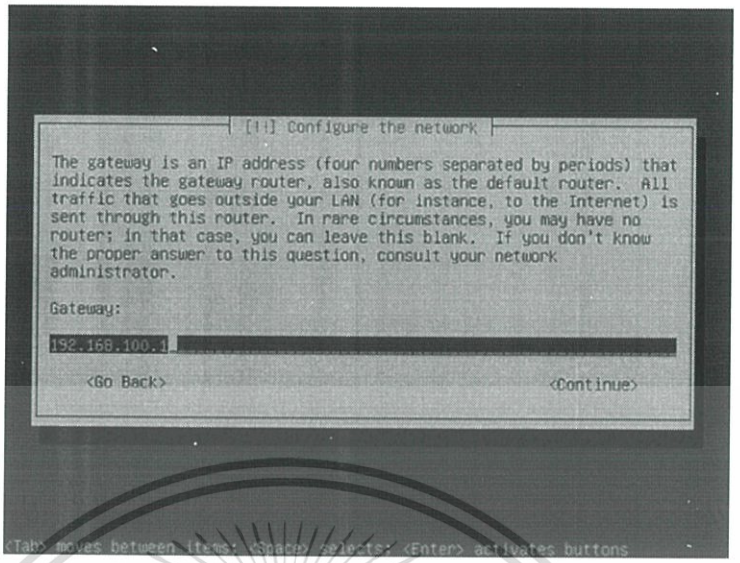
รูปที่ ข.5 ตั้งค่าหมายเลขไอพีแอดเดรส

1.6 ตั้งค่า Netmask



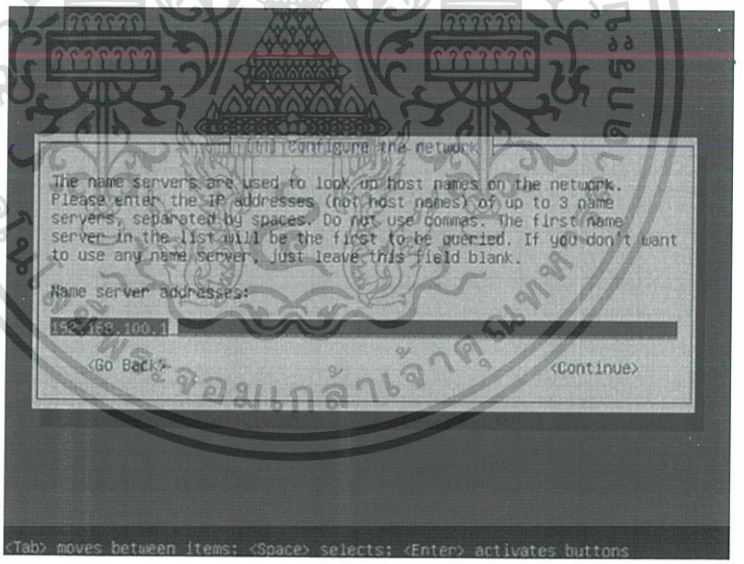
รูปที่ ข.6 ตั้งค่า Netmask

1.7 ตั้งค่า Gateway



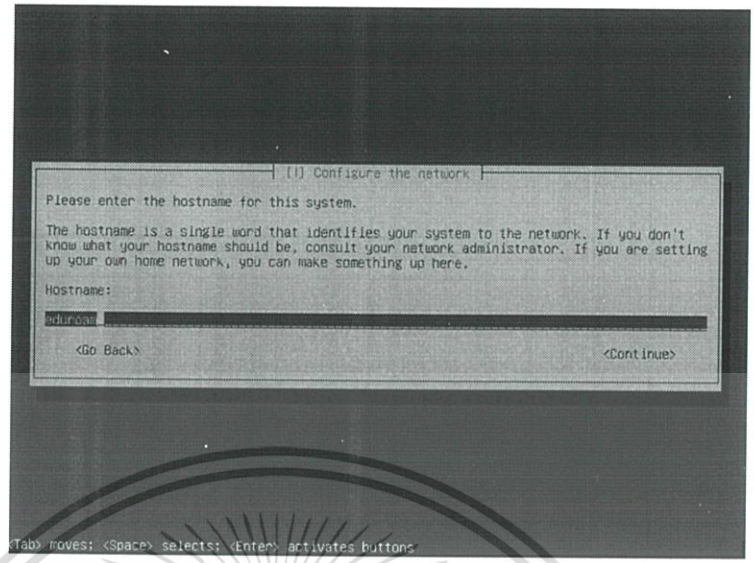
รูปที่ ข.7 ตั้งค่า Gateway

1.8 ตั้งค่า Name server address (DNS)



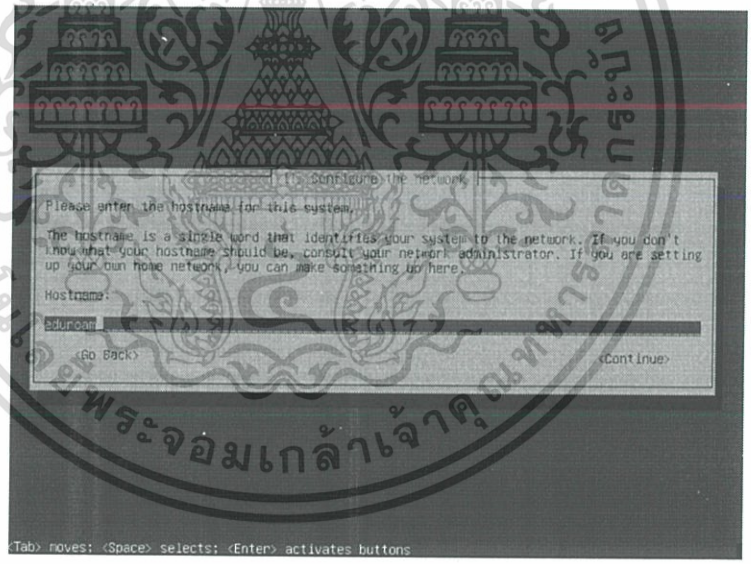
รูปที่ ข.8 ตั้งค่า DNS

1.9 ตั้งค่า Hostname



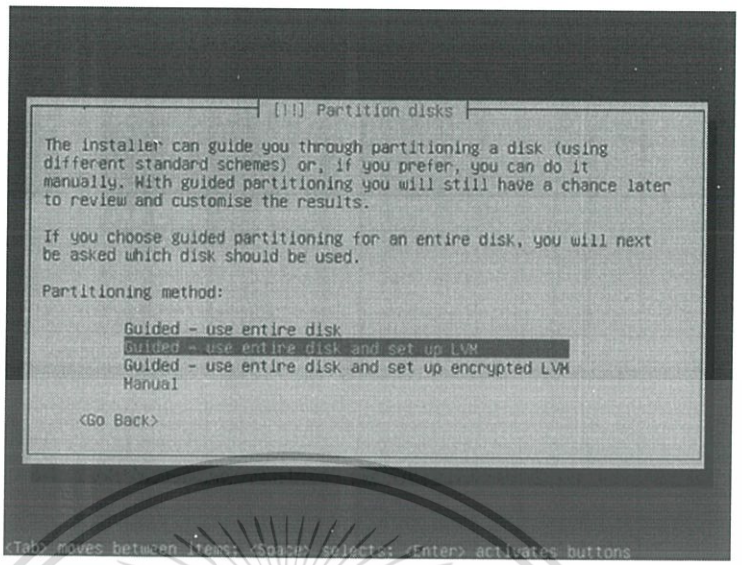
รูปที่ ข.9 ตั้งค่า Hostname

1.10 ตั้งค่า Domain name



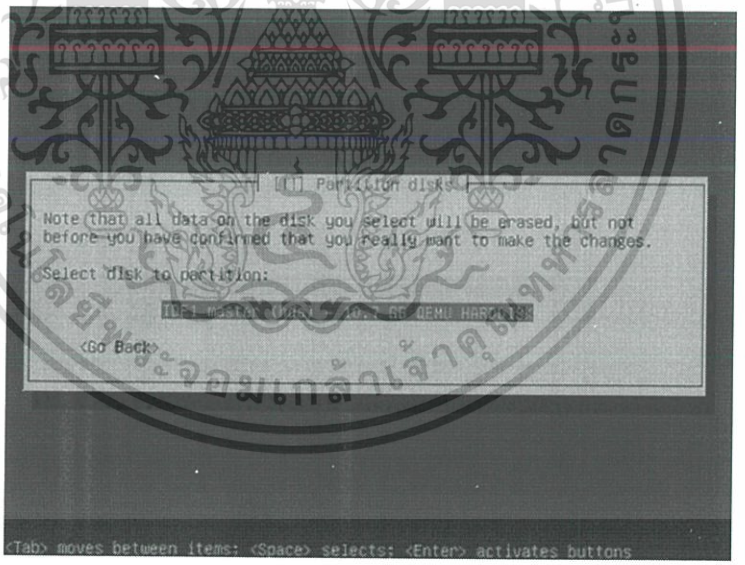
รูปที่ ข.10 ตั้งค่า Domain Name

1.11 เลือกการจัดการ Hard disk เป็นแบบให้ระบบแนะนำ โดยใช้ LVM



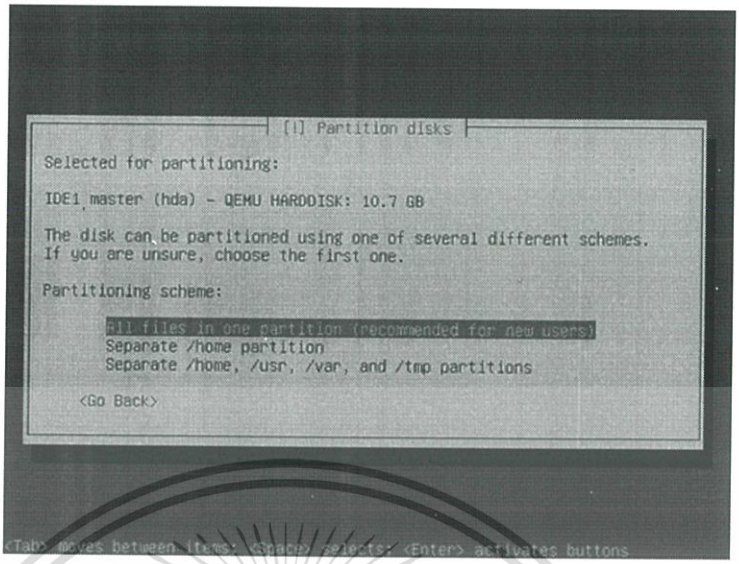
รูปที่ ข.11 ตั้งค่า Hostname

1.12 เลือก Hard disk ที่ต้องการใช้งาน



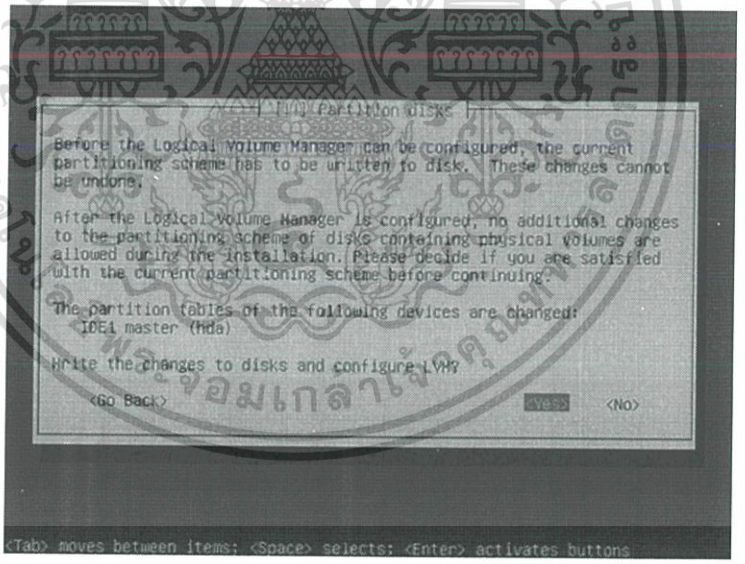
รูปที่ ข.12 เลือก Hard disk ที่ต้องการใช้งาน

1.13 เลือกรูปแบบในการจัดการ Partitions



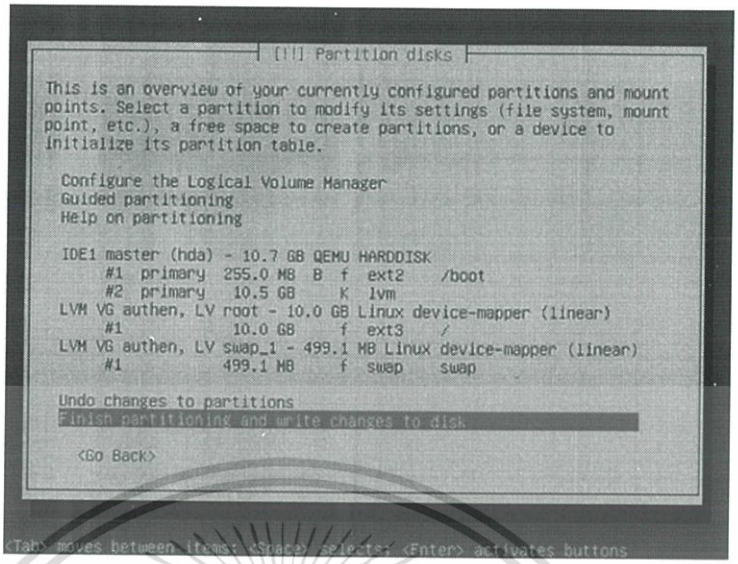
รูปที่ ข.13 เลือกรูปแบบในการจัดการ Partitions

1.14 เลือก Yes เพื่อยืนยันการทำงาน



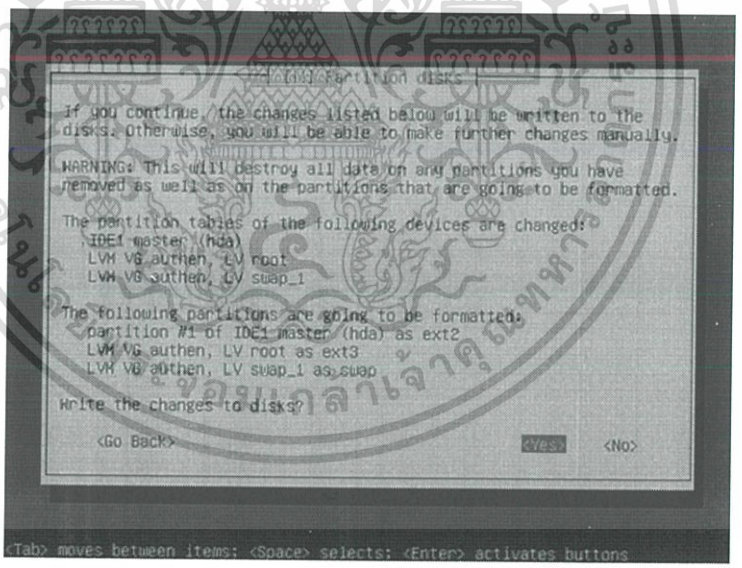
รูปที่ ข.14 เลือก Yes เพื่อยืนยันการทำงาน

1.15 เลือก Finish ... เพื่อดำเนินการตามค่าตั้งต่าง ๆ ที่ได้เลือกไว้



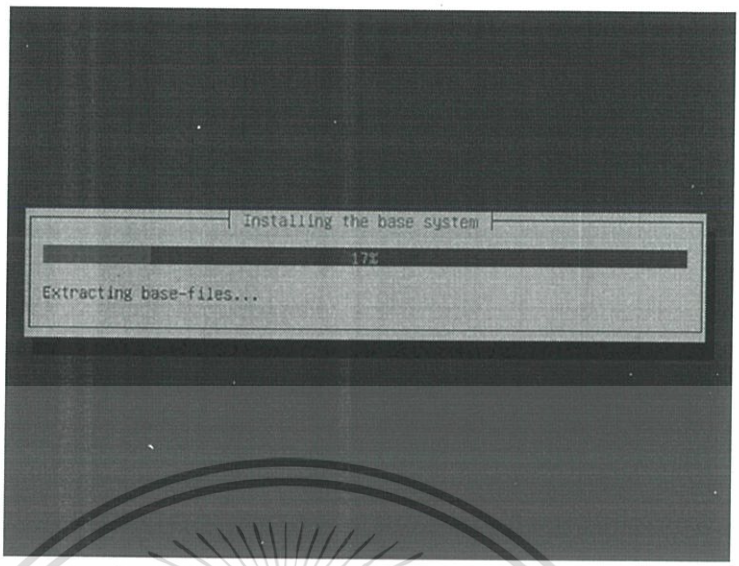
รูปที่ ข.15 เลือก Finish ... เพื่อดำเนินการตามค่าตั้งต่าง ๆ

1.16 เลือก Yes เพื่อยืนยันการเขียนข้อมูล Partitions ลง Disk



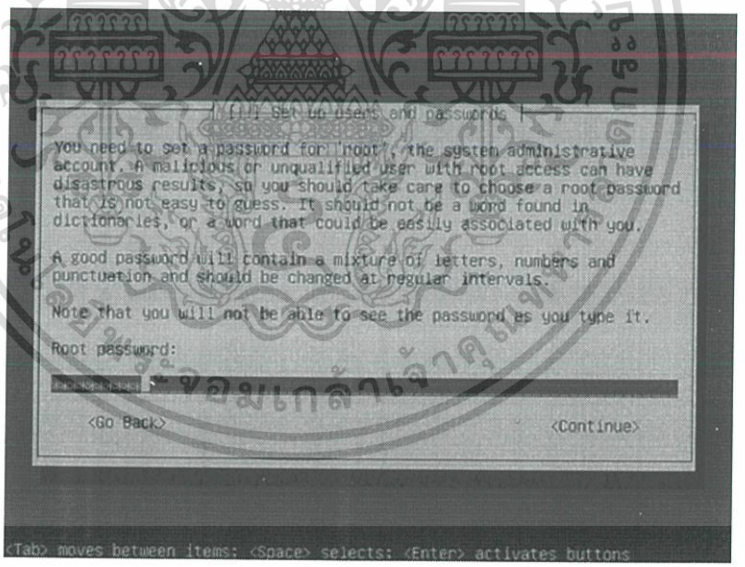
รูปที่ ข.16 เลือก Yes เพื่อยืนยันการเขียนข้อมูล Partitions ลง Disk

1.17 ระบบเริ่มทำการติดตั้ง



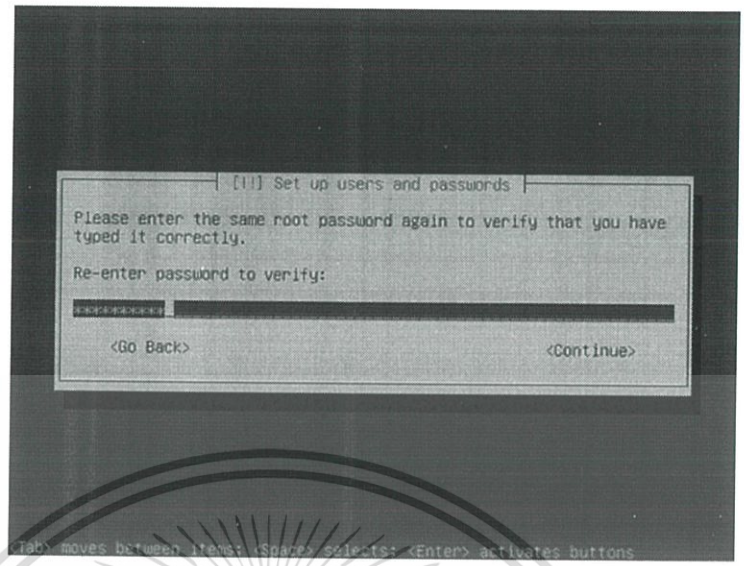
รูปที่ ข.17 เริ่มทำการติดตั้ง

1.18 ตั้งรหัสผ่านสำหรับ root user (ผู้มีอำนาจสูงสุดในระบบ)



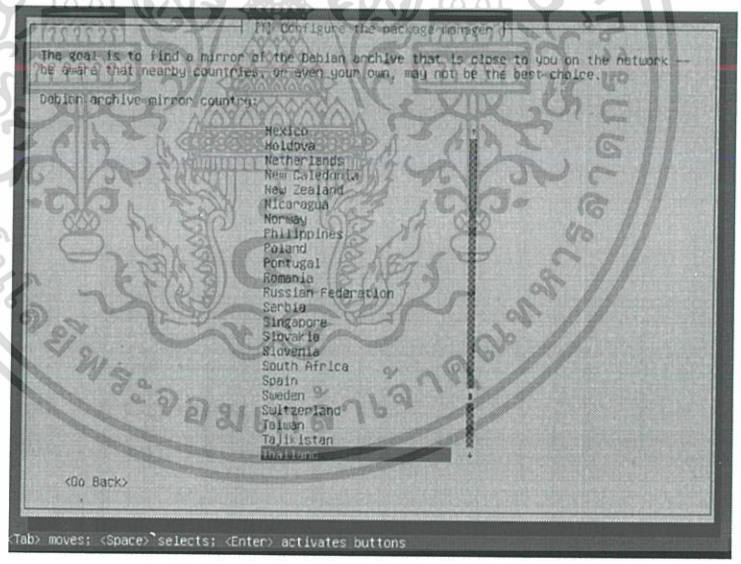
รูปที่ ข.18 ตั้งรหัสผ่านสำหรับ root user

1.19 เติมรหัสผ่านอีกครั้ง เพื่อยืนยันรหัสผ่าน



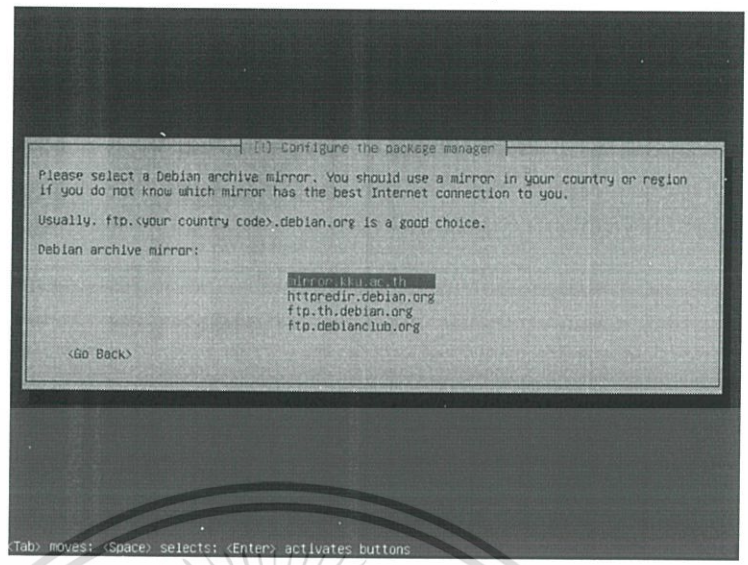
รูปที่ ข.19 เติมรหัสผ่านอีกครั้ง เพื่อยืนยันรหัสผ่าน

1.20 เลือก Debian mirror (ในประเทศ) เพื่อติดตั้ง/ปรับรุ่น เพิ่มเติม



รูปที่ ข.20 เลือก Debian mirror (ในประเทศ) เพื่อติดตั้ง/ปรับรุ่น

1.21 เลือก Debian mirror (ในประเทศ) เพื่อติดตั้ง/ปรับรุ่น เพิ่มเติม)

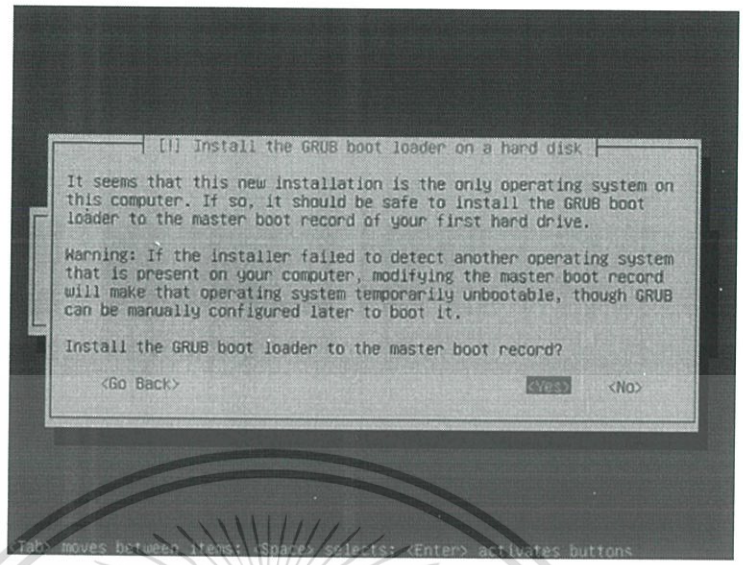


รูปที่ ข.21 เลือก Debian mirror (ในประเทศ) เพื่อติดตั้ง/ปรับรุ่น

1.22 เริ่มติดตั้งต่อ

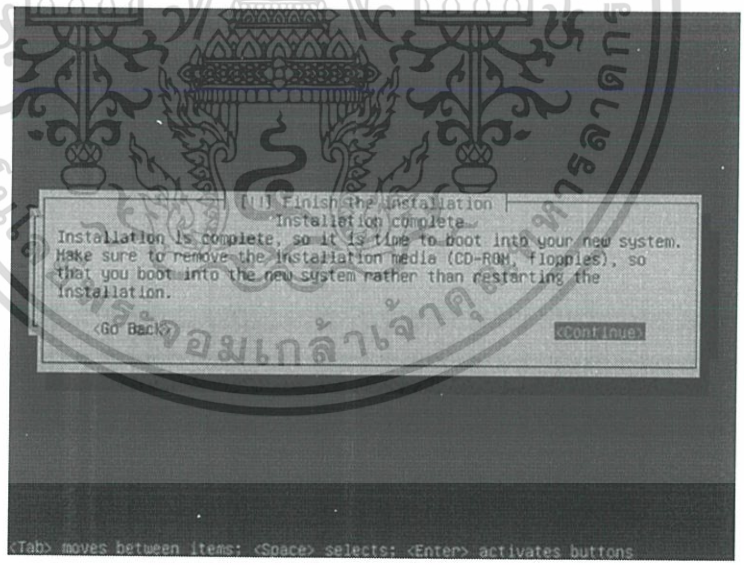
รูปที่ ข.22 เริ่มติดตั้งต่อ

1.23 เลือก Yes เพื่อติดตั้ง GRUB boot loader ที่ master boot record



รูปที่ ข.23 เลือก Yes เพื่อติดตั้ง GRUB boot loader

1.24 ระบบติดตั้ง แจ้งความสำเร็จในการติดตั้ง Debian GNU/Linux พร้อมกับเปิดเครื่องใหม่อัตโนมัติ



รูปที่ ข.24 แจ้งความสำเร็จในการติดตั้ง Debian GNU/Linux พร้อมกับเปิดเครื่องใหม่อัตโนมัติ

ประวัติผู้เขียน

ชื่อ-นามสกุล	นายณัฐธัญพงศ์ ศรนารายณ์
วัน เดือน ปีเกิด	21 ตุลาคม 2528 ที่สระบุรี
ที่อยู่	44 หมู่ 4 ต.บางโขมด อ.บ้านหมอ จ.สระบุรี 18130
ประวัติการศึกษา	ปริญญาตรี วิทยาศาสตร์บัณฑิต คณะเทคโนโลยีสารสนเทศ สาขาเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏเทพสตรี
ประวัติการทำงาน	นักวิชาการวิศวกรระบบเครือข่าย มหาวิทยาลัยราชภัฏเทพสตรี