ระบบให้บริการเครือข่ายไร้สาย ร่วมกันระหว่างองค์กร

ดนัย ชุดทอง* และ อนิราช มิ่งขวัญ**

บทคัดย่อ

บทความฉบับนี้มีวัตถุประสงค์ เพื่อพัฒนาระบบการร่วมกันให้บริการเครือข่ายไร้สายพร้อมระบบรักษาความปลอดภัยแบบ PKI สำหรับหลายองค์กร เพื่อที่ผู้ใช้จะสามารถใช้งานเครือข่ายไร้สายข้ามองค์กรได้โดยไม่ต้องจดจำชื่อบัญชีผู้ใช้และรหัสผ่านจำนวนมาก ลักษณะการทำงานของระบบจะเป็นแบบเว็บแอพพลิเคชั่น โดยผู้ใช้สามารถใช้ Certificate แทนที่การใช้ชื่อ และรหัสผ่านและยังสามารถนำเครื่องคอมพิวเตอร์ดังกล่าวไปใช้งานระบบเครือข่ายไร้สายที่องค์กรที่ร่วมกันให้บริการได้โดยไม่รู้สึกถึงความแตกต่าง และระบบยังสามารถเก็บประวัติการใช้งานพร้อมทำรายงานเพื่อทราบถึงสถิติการใช้งานว่ามีการใช้งานในองค์กรและใช้งานข้ามองค์กรมากน้อยอย่างไร

ระบบนี้ถูกพัฒนาบนระบบปฏิบัติการ Linux ร่วมกับระบบการจัดการฐานข้อมูล MySQL และโปรแกรม Free Radius ซึ่งเป็นโปรแกรมแบบ Open Source ทั้งสิ้น ทำให้ประหยัดค่าใช้จ่ายและเพิ่มความสะดวกได้มากหากเทียบกับการทำงานของระบบอื่นๆ ที่มีอยู่

คำสำคัญ: IEEE802.1X, EAP-TLS, Roaming, Proxy, Realm

1. บทนำ

ในการให้บริการเครือข่ายไร้สายขององค์กรหน่วยงานต่างๆ นั้น มีรูปแบบการให้บริการที่แตกต่างกันออกไป โดยบางองค์กรอาจจะไม่คำนึงถึงระบบรักษาความปลอดภัย ขณะที่อีกหลายองค์กรอาจจะมีการติดตั้งระบบเครือข่ายไร้สายพร้อมระบบรักษาความปลอดภัย และในหน่วยงานที่มีระบบรักษาความปลอดภัยก็ยังมีระดับความเข้มงวดหรือวิธีการรักษาความปลอดภัยที่แตกต่างกัน เช่น WEP, WPA, MAC Authentication, IPSec และ Hot Spot เป็นต้น

ปัญหาจึงเกิดขึ้นเมื่อผู้ใช้งานเครือข่ายไร้สายจากองค์กรหนึ่งมีความจำเป็นต้องไปทำงานในเครือข่ายไร้สายของอีกองค์กรหนึ่งแต่ไม่สามารถใช้งานได้เนื่องจากไม่มีชื่อผู้ใช้ในระบบ หรืออีกเหตุผลหนึ่งคือความแตกต่างของระบบรักษาความปลอดภัย บางองค์กรอาจใช้วิธีแก้ปัญหาแบบผิดๆ ด้วยการอนุญาตให้ผู้ใช้งานทุกคนสามารถเข้าใช้งานระบบเครือข่ายไร้สายโดยไม่มีระบบรักษาความปลอดภัย ซึ่งอาจนำไปสู่ปัญหาอื่นๆ เช่นความปลอดภัยของข้อมูลของผู้ใช้หรือขององค์กรเอง เป็นต้น

ทางผู้เขียนจึงนำเสนอแนวความคิดในการออกแบบระบบเครือข่ายไร้สายที่ทำให้ผู้ใช้งานจากองค์กรต่างๆ สามารถ Roaming ไปใช้งานเครือข่ายไร้สายข้ามองค์กรได้ อีกทั้งยังมีระดับความปลอดภัยสูง โดยกำหนดให้ผู้ใช้ติดตั้ง Certificate ของทั้งผู้ใช้และของระบบของผู้ใช้ ลงไปในเครื่องคอมพิวเตอร์เพื่อนำ ไปใช้ในการพิสูจน์ตัวตนทั้ง 2 ทาง (Mutual Authentication) เพื่อให้ผู้ใช้มั่นใจได้ว่า Login เข้าระบบที่แท้จริงแน่นอน เมื่อผู้ใช้งานมีความจำเป็นต้องไปทำงานหรือสัมมนาที่องค์กรอื่นๆที่เชื่อถือซึ่งกันและกัน ก็สามารถ Login เข้ากับระบบขององค์กรอื่นๆ โดยใช้ Certificate ขององค์กรของตัวเองได้เลย ทำให้สามารถแก้ปัญหาเรื่องระบบความปลอดภัยของเครือข่ายไร้สายและปัญหาเรื่องการ roaming ของผู้ใช้

2. การรักษาความปลอดภัยของเครือข่ายไร้สาย

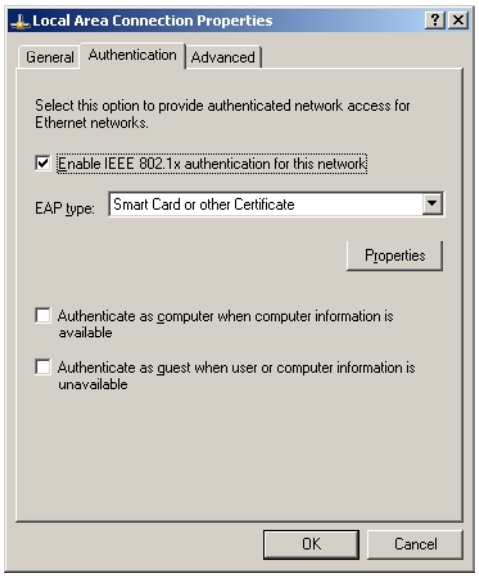
ตามมาตรฐาน IEEE 802.11 นั้น ได้กำหนดมาตรฐานการรักษาความปลอดภัยไว้คือ WEP ซึ่งก็ได้รับความนิยมกันอย่างแพร่หลาย เพราะง่ายต่อการติดตั้งที่สุด และอุปกรณ์ที่ผลิตออกมาในท้องตลาดทุกยี่ห้อก็มีการติดตั้ง WEP เป็นมาตรฐานอยู่แล้ว แต่ในปัจจุบันก็เป็นที่ทราบกันโดยทั่วไปว่า การใช้ WEP นั้นไม่เหมาะสำหรับเครือข่ายไร้สายที่มีขนาดกลางถึงใหญ่หรือในองค์กรที่มีข้อมูลที่มีมูลค่าสูง เนื่องจาก WEP มีช่องโหว่มากมาย ทั้งในด้านของการที่ไม่มีระบบ Authentication ที่สามารถระบุตัวตนของผู้ใช้ที่ถูกต้องได้ และการที่ต้องบอกต่อ Static Key ที่จะใช้ในการเข้ารหัสนั้นยังเสี่ยงต่อการรั่วไหลได้ นอกจากนั้นในทางเทคนิคแล้ว WEP จะทำการส่งค่า Initial Vector (IV) ในลักษณะของ Plain text ไปในเฟรมข้อมูลทำให้ผู้ประสงค์ร้ายสามารถดักจับ Sequence ของค่า IV เพื่อการถอดรหัสได้

เนื่องจาก WEP มีความปลอดภัยต่ำ ทำให้ต้องมีการกำหนดมาตรฐานอื่นๆ เพื่อเพิ่มความปลอดภัยของข้อมูลบน

* *คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าพระนครเหนือ*

** *คณะเทคโนโลยีและการจัดการอุตสาหกรรม สถาบันเทคโนโลยีพระจอมเกล้าพระนครเหนือ*

เครือข่ายไร้สายเช่น มาตรฐาน IEEE 802.1X ที่ได้กำหนดมาตรฐานการ Authentication และ Authorization ในการเข้าใช้งานระบบเครือข่ายหรือที่เรียกว่า Port-based network access control ซึ่งในมาตรฐานนี้แท้จริงแล้วสามารถใช้ได้ทั้งระบบ WLAN หรือ LAN ก็ได้ โดยสามารถอธิบายโดยง่ายว่า IEEE 802.1X ก็คือมาตรฐานการ Authentication บน Layer 2 ของ OSI Model และหาก Authentication ไม่สำเร็จก็จะไม่สามารถต่อเข้าใช้งานเครือข่ายได้ ในระบบปฏิบัติการ Windows XP ในปัจจุบันก็สามารถใช้งานร่วมกับมาตรฐาน IEEE 802.1X ได้ ดังภาพที่ 1



ภาพที่ 1 แสดงภาพการ Setup เพื่อใช้งาน IEEE 802.1X ใน Windows XP

IEEE 802.1X ได้กำหนดสถาปัตยกรรมของการเข้าใช้งานระบบเครือข่ายโดยให้มีองค์ประกอบพื้นฐานคือ

- Authenticator
- Authentication Server
- Supplicant

ในการทำ Authentication บนเครือข่าย Wireless LAN ตามมาตรฐาน IEEE802.1X นั้นผู้ใช้จะแลกเปลี่ยนข้อมูล Credential กับ Authentication server ด้วยโปรโตคอล EAP ซึ่งถูกออกแบบมาเพื่อการ Authentication บน Layer 2 ของ OSI Model ซึ่ง EAP ที่ได้ถูกกำหนดอยู่ใน RFC2284 นั้นยังเป็นเพียงแค่การกำหนดวิธีการพื้นฐานโดยใช้ MD5 ในการแลกเปลี่ยนข้อมูลระหว่างระบบกับผู้ใช้เท่านั้น ซึ่งยังคงมีความปลอดภัยของข้อมูลค่อนข้างต่ำ ทำให้มีผู้ผลิตอุปกรณ์หรือ Software รวมถึงกลุ่มที่ไม่หวังผลกำไรต่างๆ ได้นำเอา EAP ไปพัฒนาเพิ่มเติมเพื่อเพิ่มประสิทธิภาพและความปลอดภัยได้อีกหลายแบบ ดังนี้

Topic	EAP MD5	LEAP	EAP TLS	PEAP	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

3. วิธีการดำเนินงานและผลการดำเนินงาน

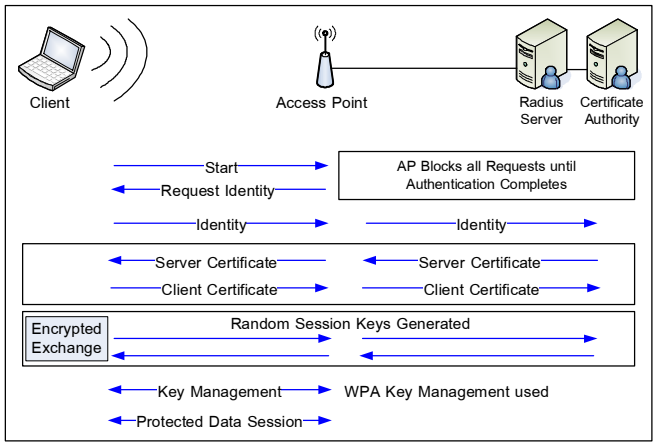
3.1 การออกแบบระบบ

จากที่ได้อธิบายเกี่ยวกับระบบรักษาความปลอดภัยโดยเบื้องต้นไปแล้วนั้น จะเห็นได้ว่าการใช้งาน IEEE802.1X และ EAP นั้นมีความปลอดภัยค่อนข้างสูง และยังเป็นมาตรฐานที่ระบบปฏิบัติการที่ได้รับความนิยม (เช่น Microsoft XP) ได้รวมเข้าไว้ในระบบอยู่แล้ว ทำให้ไม่ต้องลงทุนเพื่อการนี้เพิ่ม ระบบให้บริการเครือข่ายไร้สายร่วมกันระหว่างองค์กรนี้จะทำงานบนมาตรฐาน EAP-TLS ซึ่งเป็นมาตรฐานที่ต้องมี PKI โดยต้องมีการใช้ Certificate ของทั้ง Radius และของ Client ในการทำ Authentication เพื่อป้องกันการโจมตีแบบ Man-in the-middle เนื่องจาก Client จะไม่ส่ง Credential ให้กับ Radius หากไม่สามารถพิสูจน์ได้ว่าเป็น Radius Server ตัวจริง

โปรแกรม Freeradius จะถูกนำมาใช้เป็น Authentication Server ของระบบนี้เนื่องจากเป็นโปรแกรม Open Source และค่อนข้างจะถูกใช้โดยแพร่หลาย อีกทั้งยังรองรับกับโปรโตคอลที่เราจะนำมาใช้ (EAP-TLS) อีกด้วย

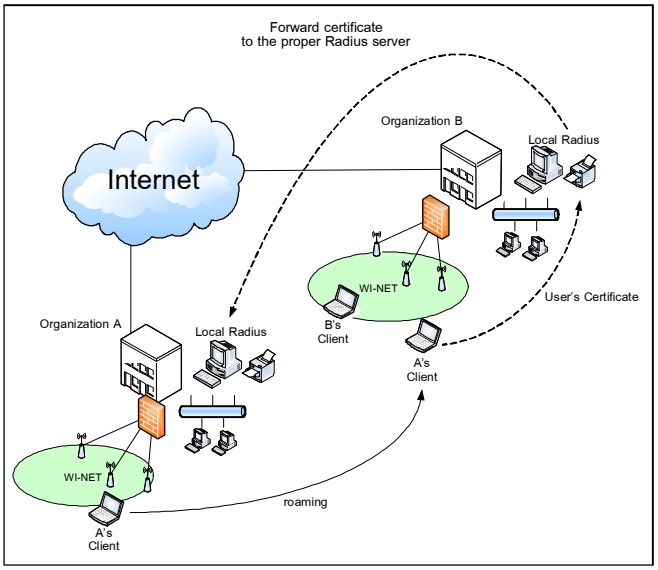
แต่ละองค์กรจะต้องมี CA ของตนเองเพื่อเป็นการสร้างระบบ PKI ขององค์กร โดยจะใช้โปรแกรม OpenSSL ซึ่งเป็น Open Source เช่นกัน เพื่อสร้าง Certificate ของ Server และผู้ใช้แต่ละคน

Radius ของแต่ละองค์กรจะเชื่อมถึงกันผ่าน Internet โดยที่จะเป็น Client และ Server ของกันและกัน ยกตัวอย่างเช่น เมื่อ



ภาพที่ 2 แสดงการทำงานของ EAP-TLS

Radius ขององค์กร A ได้รับการการขอ Authenticate จากผู้ใช้ที่ Roaming มาจากองค์กร B แล้ว Radius A จะทำการ Proxy การขอ Authenticate นั้นแล้วส่งต่อไปยัง Radius B ในการนี้ Radius A จะเป็น Client ของ Radius B



ภาพที่ 3 แสดงการ Roaming และ Proxy

เมื่อผู้ใช้ได้ทำการสมัครสมาชิกแบบออนไลน์ ระบบจะทำการเพิ่มชื่อ domain ขององค์กรต่อท้ายชื่อผู้ใช้เข้าไปในช่อง CN ของ Certificate ก่อนที่จะเพิ่มชื่อผู้ใช้เข้าไปในฐานข้อมูลของ CA ของแต่ละองค์กร เรียกว่า Realm โดยชื่อผู้ใช้จะมีลักษณะคล้ายกับ Email address เช่น danai@winet.kmitnb เป็นต้น ซึ่ง Realm จะถูกใช้เพื่อแยกแยะว่าเป็นผู้ใช้ที่มาจากองค์กรใดเพื่อการทำ Proxy ต่อไป เช่น หาก Radius ตรวจ CN พบว่าเป็นผู้ใช้ชื่อ danai@winet.kmitnb ก็จะ Encapsulate ด้วย EAP ก่อนที่จะส่งผ่านการ Authenticate ไปยัง Radius ของสถาบันเทคโนโลยีพระจอมเกล้าพระนครเหนือต่อไป

การกำหนดค่าต่าง ๆ ในการออก Certificate ให้กับผู้ใช้จะถูกกำหนดให้เป็นทิศทางเดียวกันดังนี้

C = TH

S = BKK (ถ้าองค์กรอยู่ในกทม)

L = Bangkok (ถ้าองค์กรอยู่ในกทม)

O = *Oganization name*

OU = Wi-Net

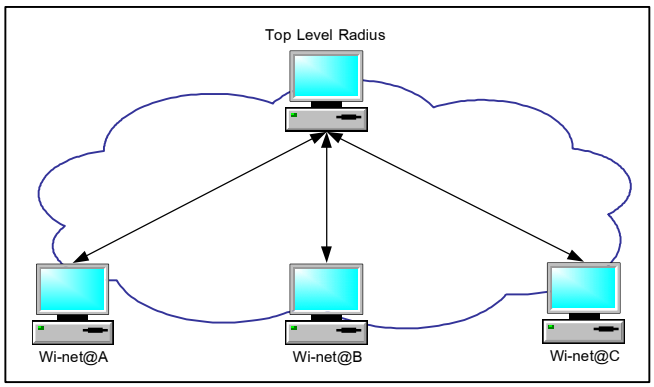
CN = Name@wi-net.*Organication name*

E = *Email Address*

ระบบจะทำการตรวจสอบข้อมูลใน CN (Common Name) ว่าเป็นผู้ใช้ชื่ออะไรและมี Realm ชื่ออะไรก่อนจะทำการ Proxy ไปยัง Radius ที่ถูกต้อง แต่ถ้าระบบไม่สามารถค้นข้อมูลว่า Realm นั้นมี Radius หมายเลยอะไร ก็จะทำการ Reject ผู้ใช้คนนั้นทันที

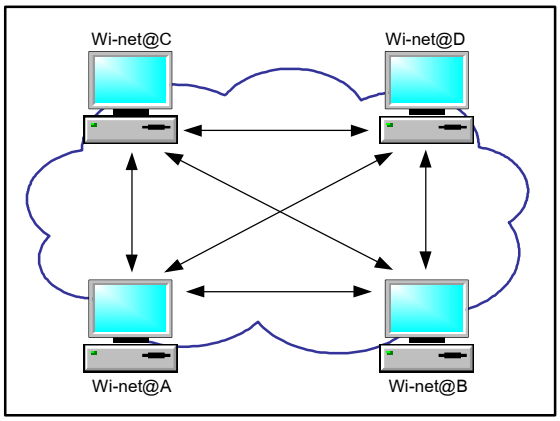
3.2 การนำระบบให้บริการเครือข่ายไร้สายร่วมกันระหว่างองค์กรไปใช้งาน

การที่จะนำระบบนี้ไปใช้งานนั้นสามารถทำได้ 2 ลักษณะ คือ แบบที่มีองค์กรกลางเพื่อทำหน้าที่เป็น Top-Level Radius ให้ทุกๆ องค์กร หรืออีกแบบหนึ่งที่แต่ละองค์กรต้องทำการเพิ่มชื่อ Realm และ หมายเลข IP ของ Radius ของทุกๆ องค์กรที่เป็นสมาชิกเอง



ภาพที่ 4 แสดงภาพจำลองระบบที่มี Top-Level Radius

การติดตั้งระบบทั้งสองแบบจะแตกต่างกันตรงที่การกำหนดค่าพารามิเตอร์ในแฟ้มชื่อ /etc/raddb/proxy.conf คือถ้าเป็นแบบแรกนั้น หากตรวจพบว่าเป็นผู้ใช้งานจากองค์กรอื่นระบบ



ภาพที่ 5 แสดงภาพจำลองระบบAdhoc

ก็จะทำการ Proxy ข้อมูลส่งต่อไปยัง Top-Level Radius ขององค์กรกลาง โดยที่ไม่ต้องทราบว่า Radius ขององค์กรอื่นๆ มีหมายเลข IP อะไร แต่หากเป็นแบบที่ 2 แล้วผู้ดูแลระบบจะต้องทำการกำหนดพารามิเตอร์ในส่วนของ Realm ให้ครบทุกองค์กรที่เป็นสมาชิก เพื่อให้ระบบสามารถส่งการขอ Authentication ต่อไปยัง Radius ขององค์กรอื่นๆ ที่ถูกต้องได้

```
realm DEFAULT {
      type       = radius
      authhost   = Top-level Radius IP:1600
      accthost   = Top-level Radius IP:1601
      secert     = wi-net
}
```

ภาพที่ 6 แสดงพารามิเตอร์ในแฟ้ม proxy.conf ในระบบที่มี Top-Level Radius

```
realm u1.ac.th {
      type       = radius
      authhost   = 192.168.1.101:1600
      accthost   = 192.168.1.101:1601
      secert     = wi-net
      nostrip
}

realm u2.ac.th {
      type       = radius
      authhost   = 192.168.2.101:1600
      accthost   = 192.168.2.101:1601
      secert     = wi-net
      nostrip
}
```

ภาพที่ 7 แสดงพารามิเตอร์ในแฟ้ม proxy.conf ในระบบแบบ Adhoc

นอกเหนือจากการกำหนดค่าพารามิเตอร์ในส่วนของ Realm ในแฟ้ม /etc/raddb/proxy.conf แล้ว ยังมีความแตกต่างของการตั้งค่าพารามิเตอร์ในแฟ้มชื่อ /etc/raddb/clients.conf อีกด้วย ดังนี้

```
client Top-Level Radius IP {
      secert       = wi-net
      nastype      = cisco
      shortname    = Top-Radius
}
```

ภาพที่ 8 แสดงพารามิเตอร์ในแฟ้ม clients.conf ในระบบแบบที่มี Top-Level Radius

```
client 192.168.1.101 {
      secert       = wi-net
      nastype      = cisco
      shortname    = u1
}

client 192.168.2.101 {
      secert       = wi-net
      nastype      = cisco
      shortname    = u2
}
```

ภาพที่ 9 แสดงพารามิเตอร์ในแฟ้ม clients.conf ในระบบแบบ Adhoc

แฟ้ม /etc/raddb/clients.conf เป็นการกำหนดว่าอนุญาตให้เครื่อง Radius เครื่องใดสามารถขอทำ Proxy ให้กับ Radius ขององค์กรเราได้ ในขณะที่แฟ้ม /etc/raddb/proxy.conf นั้นจะระบุว่าเราจะ Proxy ไปที่ Radius เครื่องใดบ้าง โดยจะดูจากชื่อ Realm ของผู้ใช้เป็นหลัก ซึ่งจะเห็นได้ว่าหากสมาชิกของการร่วมกันให้บริการเครือข่ายไร้สายระหว่างองค์กรมีจำนวนมากแล้ว ควรจะมีการจัดตั้งองค์กรกลางขึ้นมาเพื่อความสะดวกในการบริหารจัดการค่าพารามิเตอร์ต่างๆของ Radius ในแต่ละองค์กร และยังสามารถลดความผิดพลาดในการตั้งค่าพารามิเตอร์ต่าง ๆ ได้ด้วย

นอกจากความแตกต่างของแฟ้ม /etc/raddb/proxy.conf และ /etc/raddb/clients.conf ที่ได้กล่าวในข้างต้นแล้ว การตั้งค่าอื่นๆนั้นไม่มีความแตกต่างกันระหว่างการนำระบบไปใช้ในแบบที่ 1 และแบบที่ 2 การตั้งค่าพารามิตอร์สำหรับการกำหนดค่าต่างๆ ของโปรโตคอล EAP-TLS เช่นการกำหนด path ที่ใช้เก็บ Private key และ Certificate ของผู้ใช้ จะถูกเก็บอยู่ในแฟ้ม /etc/readdb/eap.conf ดังนี้

```
eap {
      default_eap_type = tls
      timer_expire = 60
      ignore_unknown_eap_type = u1
      cisco_accounting_username_bug = no

      tls {
            private_key_password = whatever
            private_key_file = ${raddbdir}/certs/cert-srv.pem
            certificate_file = ${raddbdir}/certs/cert-srv.pem
            CA_file = ${raddbdir}/certs/CA/cacert.pem
            dh_file = ${raddbdir}/certs/dh
            random_file = ${raddbdir}/certs/random
            fragment_size = 1024
            include_length = yes
      }
}
```

ภาพที่ 10 แสดงพารามิเตอร์ในแฟ้ม eap.conf

แฟ้มชื่อ /etc/raddb/radiusd.conf จะเป็นแฟ้มหลัก มีหน้าที่ควบคุมการทำงานทั้งหมดของโปรแกรมเช่น Path ที่ใช้จัดเก็บแฟ้มต่างๆที่เกี่ยวข้อง, วิธีการเก็บ Log ต่างๆ, การติดต่อกับฐานข้อมูล, และ รูปแบบการใช้งาน EAP และ Realm ฯลฯ โดยค่าส่วนใหญ่ที่จำเป็นจะถูกกำหนดเป็นค่าตั้งต้นอยู่แล้ว แต่ในส่วนของการใช้งาน EAP และการตั้งค่าเกี่ยวกับการใช้งานฐานข้อมูลบางส่วนที่ยังไม่ถูกกำหนดเป็นค่าตั้งต้นจะถูกคั่นด้วยเครื่องหมาย # อยู่หน้าบรรทัดนั้นในแฟ้ม ดังนั้นจะต้องลบเครื่องหมาย # ออกจากบรรทัดที่ต้องการใช้งาน

```
log_auth = yes
log_auth_badpass = yes
log_auth_goodpass = yes

authorize {
      auth_log
      sql
      eap
}

authenticate {
      eap
      suffix
}

preacct {
      preprocess
      acct_unique
      suffix
      files
}

accounting {
      sql
}

post-auth {
      reply_log
      sql
}
```

ภาพที่ 11 แสดงพารามิเตอร์ในแฟ้ม radiusd.conf

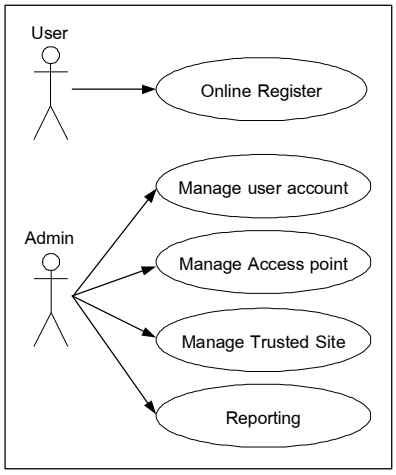
ตัวอย่างของบรรทัดที่ต้องการการแก้ไขในแฟ้ม /etc/raddb/radiusd.conf ที่แสดงในภาพที่ 13 นั้น อธิบายคร่าวๆ ได้ว่า มีการกำหนดให้ใช้ EAP ในการ Authentication โดยที่มีตรวจสอบ Realm จาก suffix ของชื่อผู้ใช้ และมีการจัดเก็บ log การเข้าใช้งานเครือข่าย (accounting) ในระบบจัดการฐานข้อมูล MySQL

3.3 การจัดการระบบผ่านเว็บแอพพลิเคชั่น

จากวิธีการตั้งค่าพารามิเตอร์ทั้งหมดที่ได้กล่าวในหัวข้อ 3.2 จะเห็นได้ว่าค่อนข้างยุ่งยากและเข้าใจยากสำหรับผู้ดูแลระบบที่ไม่มีพื้นฐานที่ดีพอ ทำให้อาจเกิดความผิดพลาดของผู้ดูแลระบบได้โดยง่าย จึงมีความจำเป็นอย่างยิ่งที่จะต้องมีการพัฒนาโปรแกรมการจัดการระบบบนเว็บ เพื่อให้ใช้งานได้ง่ายและช่วยลดความผิดพลาดได้

ระบบจัดการบนเว็บจะครอบคลุมตั้งแต่การสมัครเป็นสมาชิกของผู้ใช้ และการจัดการระบบหลังบ้าน (Back office) เช่น การเพิ่ม/แก้ไขและลบหมายเลข IP ของ Access point และการเพิ่ม/แก้ไขและลบ Trust site และ Realm และการเรียกดูรายงาน เป็นต้น

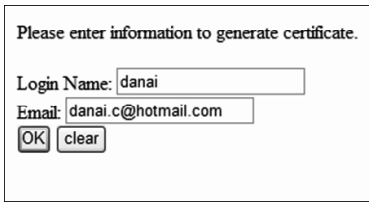
ขั้นตอนของการสมัครสมาชิกใหม่ทำได้โดยให้ผู้ใช้งานที่มีสิทธิที่สามารถจะใช้งานเครือข่ายไร้สายได้ ยกตัวอย่างเช่น นักศึกษาปัจจุบันที่ได้ชำระค่าเทอมแล้วและมีสิทธิที่จะ Login เข้าสู่ระบบของมหาวิทยาลัย ก็จะสามารถ Click เพื่อสมัครสมาชิก wi-net ได้ โดยจะให้ผู้ใช้ระบุชื่อผู้ใช้ที่ต้องการและ e-mail ที่สามารถติดต่อได้เพื่อให้ระบบส่ง Certificate ของระบบและของผู้ใช้กลับไปให้ทาง e-mail เพื่อที่จะได้แน่ใจว่าเป็นผู้ใช้งานตัวจริง



ภาพที่ 12 แสดง Use Case ของการจัดการระบบผ่านเว็บแอพพลิเคชั่น

ในส่วนของผู้ดูแลระบบนั้นจะสามารถจัดการระบบได้ดังนี้

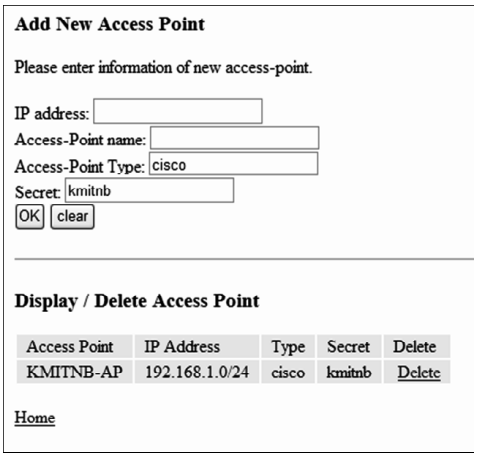
- จัดการทะเบียนผู้ใช้ คือการเรียกดูและลบชื่อผู้ใช้
- จัดการทะเบียน Access Point
- จัดการทะเบียนของ Trusted Site และ Realm
- รายงานการใช้งานเครือข่ายไร้สาย



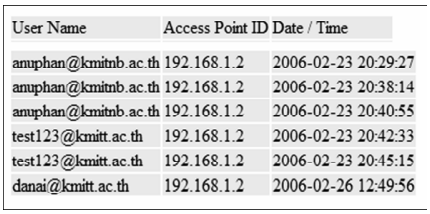
ภาพที่ 13 แสดงหน้าการสมัครสมาชิกแบบออนไลน์

User Name	Email Address	Delete
aniraj	aniraj@ieee.org	Delete
anuphan	anuphan@kmitnb.ac.th	Delete
danai	danai@kmitnb.ac.th	Delete

ภาพที่ 14 แสดงหน้าการจัดการทะเบียนผู้ใช้

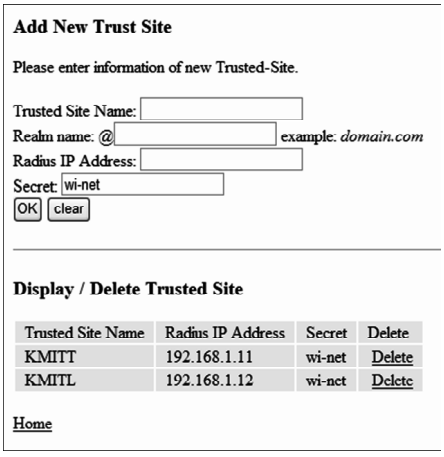


ภาพที่ 15 แสดงหน้าการจัดการ Access Point



User Name	Access Point ID	Date / Time
anuphan@kmitnb.ac.th	192.168.1.2	2006-02-23 20:29:27
anuphan@kmitnb.ac.th	192.168.1.2	2006-02-23 20:38:14
anuphan@kmitnb.ac.th	192.168.1.2	2006-02-23 20:40:55
test123@kmitt.ac.th	192.168.1.2	2006-02-23 20:42:33
test123@kmitt.ac.th	192.168.1.2	2006-02-23 20:45:15
danai@kmitt.ac.th	192.168.1.2	2006-02-26 12:49:56

ภาพที่ 16 แสดงหน้ารายงานการใช้งาน



ภาพที่ 17 แสดงหน้าการจัดการ Trusted Site และ Realm

4. บทสรุป

ระบบให้บริการเครือข่ายไร้สายระหว่างองค์กร จะสามารถช่วยแก้ปัญหาการ Roaming ของผู้ใช้งาน โดยที่ยังคงมีระบบรักษาความปลอดภัยสูง ผู้ใช้สามารถนำเครื่องคอมพิวเตอร์ไปใช้งานระบบเครือข่ายไร้สายที่องค์กรที่เป็นสมาชิกของ wi-net ได้ทุกที่ ความเร็วของการ login ก็ขึ้นอยู่กับขนาด Bandwidth ขององค์กรนั้นๆ รวมถึงปริมาณการใช้งาน Internet ในช่วงเวลาดังกล่าว

ในการนำไปใช้งานจริงนั้น ผู้เขียนขอเสนอแนะว่าควรจะมีการจัดตั้งองค์กรกลางสำหรับเป็น Top-Level Radius ดังภาพที่ 6 เพื่อเพิ่มความสะดวกให้แก่องค์กรสมาชิก ในการที่ไม่ต้องแก้ไขเพิ่มเติมทุกครั้งที่มีการเพิ่มองค์กรสมาชิกใหม่เข้าสู่ระบบ

5. เอกสารอ้างอิง

[1] Adam Sulmicki “HOWTO on EAP/TLS authentication between FreeRADIUS and XSupplicant” *http://www.missl.cs.umd.edu/wireless/eaptls/* ,2002-03-05.

[2] IEEE Std 802.11d-2001 “Part 11: Wireless LAN Medium Access Control (MAC) And Physical Layer (PHY) specifications” ,IEEE 2001.

[3] IEEE IEEE Std 802.1X-2001 “Port-based Network Access Control” ,IEEE 2001.

[4] Ken Roser “HOWTO: EAP/TLS setup for FreeRADIUS and Windows XP supplicant” *http://www.freeradius.org/doc/EAPTLS.pdf* ,2002-03-18.

[5] Lars Strand “802.1X Port-Based authentication HOWTO”,http://www.tldp.org/HOWTO/8021X-HOWTO/index.html ,2004-08-18.

[6] Lars Viklund “EAP-TLS key generation” http://lists.freeradius.org/mailman/htdig/freeradiususers/2002-June/008439.html ,2002-06-20.