ระบบจัดการการใช้บริการเครือข่ายแลนไร้สาย

WIRELESS LAN SERVICE MANAGEMENT SYSTEM

จิรายุ ล่อใจ

ชวลิต ทรัพย์สถิตย์กุล

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ.2548

ระบบจัดการการใช้บริการเครือข่ายแลนไร้สาย

WIRELESS LAN SERVICE MANAGEMENT SYSTEM

โดย

จิรายุ ล่อใจ

ชวลิต ทรัพย์สฉิตย์กุล

อาจารย์ที่ปรึกษา

อ. ธนัญชัย ตรีภาค

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ.2548

ปริญญานิพนธ์ปีการศึกษา 2548

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง ระบบจัดการการใช้บริการเครือข่ายแลนไร้สาย

WIRELESS LAN SERVICE MANAGEMENT SYSTEM

ผู้จัดทำ

1. นายจิรายุ ล่อใจ รหัสนักศึกษา 45010127

2. นายชวลิต ทรัพย์สถิตย์กุล รหัสนักศึกษา 45010167

อาจารย์ที่ปรึกษา

(อ. ธนัญชัย ตรีภาค)

ระบบจัดการการใช้บริการเครือข่ายแลนไร้สาย

จิรายุ ล่อใจ 45010127

ชวลิต ทรัพย์สถิตย์กุล 45010167

อ. ธนัญชัย ตรีภาค อาจารย์ที่ปรึกษา

ปีการศึกษา 2548

บทคัดย่อ

ปัจจุบันเทคโนโลยีเครือข่ายแลนแบบไร้สาย หรือ WLAN (Wireless LAN) กำลังได้รับความนิยมเป็นอย่างมาก เนื่องจากประโยชน์ของ WLAN มีอยู่มากมายโดยเฉพาะอย่างยิ่ง WLAN สร้างความสะดวก ในการใช้งานและติดตั้งเครือข่าย

แต่อย่างไรก็ตาม ความง่าย และสะดวกต่อการติดตั้งใช้งานของอุปกรณ์ WLAN นั้นก็นำมาซึ่งความไม่ปลอดภัยของเครือข่ายด้วยเช่นกัน การให้บริการ WLAN อย่างปลอดภัยนั้นจะต้องสามารถป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาเครือข่ายภายในผ่านทางอุปกรณ์ Wireless ได้ โดยวิธีการป้องกันนั้นก็มีหลายวิธี ไม่ว่าจะเป็นการกำหนดการเข้ารหัสแบบ WEP หรือการจำกัด MAC Address แต่วิธีเหล่านี้มีข้อจำกัดเรื่องของจำนวนผู้ใช้งาน ความสะดวกในการเข้าใช้ รวมไปถึงความสามารถในการบริหารจัดการระบบ เนื่องจากวิธีดังกล่าวไม่สามารถที่จะตรวจสอบ และระบุผู้เข้าใช้แต่ละคนในระบบได้ ดังนั้นวิธีที่เหมาะกับการใช้ระบบ WLAN นั้นคือกระบวนการการพิสูจน์ตัวตนโดยให้ผู้ใช้กรอก ชื่อผู้ใช้ และรหัสผ่าน เพื่อเป็นการพิสูจน์ตัวตนของผู้ใช้ก่อนการเข้าใช้ระบบ WLAN เพื่อสามารถควบคุมและจัดการระบบการเข้าใช้ รวมไปถึงสามารถตรวจสอบการใช้งานของผู้ใช้งานระบบ WLAN เป็นรายบุคคลได้ กระบวนการการพิสูจน์ตัวตนจะนำหลักฐานที่ผู้ใช้กล่าวอ้างมาตรวจสอบว่าบุคคลที่กล่าวอ้างนั้นเป็นใครและได้รับอนุญาตให้สามารถเข้ามาภายในระบบได้หรือไม่

WIRELESS LAN SERVICE MANAGEMENT SYSTEM

Jirayu Lojai	45010127
Chawalit Sapsatitkul	45010167
Thanunchai Threepak	Advisor
Academic Year 2005	

ABSTRACT

Today, Wireless Local Area Network becomes increasingly popular because of its useful features. One of which is its outstanding mobility that outline the meanings of Wireless LAN itself.

However, the mobility also brings insecurity, when someone outside of Wireless LAN gains access to the network. Secured Wireless LAN service must be free of unauthorized access. There are many methods to prevent unauthorized access such as WEP Encoding or MAC Address limiting, although many as well have some limitations about amount of users, availability, and ability to manage the system. For enterprise-scaled wireless network, the appropriate method for Wireless LAN management is using user-based Authentication before let them access to Wireless LAN as well as managing and verifying their usages afterward.

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จได้อย่างดี ด้วยคำแนะนำ และคำปรึกษาจาก อ. ธนัญชัย ตรีภาค ซึ่งเป็นอาจารย์ผู้ควบคุมวิทยานิพนธ์ ข้าพเจ้ารู้สึกซาบซึ้งในความอนุเคราะห์จากท่านอาจารย์ และขอขอบพระคุณเป็นอย่างสูง

ขอกราบพระคุณคณาจารย์ภาควิชาคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง รวมถึงอาจารย์ของข้าพเจ้าทุกท่านที่ได้ประสิทธิประสาทวิชาความรู้แก่ข้าพเจ้า

ขอขอบคุณเพื่อนๆ พี่ๆ น้องๆ ในภาควิชาวิศวกรรมคอมพิวเตอร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ทุกคนที่ให้คำแนะนำต่างๆ และคอยให้กำลังใจเสมอมา

สุดท้ายนี้ข้าพเจ้าขอกราบขอบพระคุณ บิดา มารดา ของข้าพเจ้าที่ได้ให้ชีวิต การศึกษา กำลังใจ และสนับสนุนในทุกเรื่อง ทำให้ข้าพเจ้าสามารถทำวิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงด้วยดี

คุณค่าและประโยชน์อันพึงมาจากวิทยานิพนธ์ฉบับนี้ ข้าพเจ้าขอมอบแด่ผู้มีพระคุณทุกท่าน

จิราขุ ล่อใจ

ชวลิต ทรัพย์สถิตย์กุล

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

ตารางที่ หน้า

สารบัญรูป

สารบัญรูป (ต่อ)

บทที่ 1
บทนำ

1.1 ความสำคัญและที่มาของโครงงาน

ปัจจุบันเทคโนโลยีเครือข่ายแลนแบบไร้สาย หรือ Wireless LAN (WLAN) กำลังได้รับความนิยมเป็นอย่างมาก เนื่องจากประโยชน์ของ WLAN มีอยู่มากมายโดยเฉพาะอย่างยิ่ง WLAN สร้างความสะดวก มีอิสระในการใช้งาน และติดตั้งเครือข่าย เทคโนโลยี WLAN ทำให้การเชื่อมต่ออุปกรณ์คอมพิวเตอร์ในบ้านหรือสำนักงานเข้าด้วยกัน หรือต่อเข้ากับเครือข่ายไม่จำเป็นจะต้องใช้สายนำสัญญาณให้ยุ่งยาก และดูเกะกะอีกต่อไป อุปกรณ์คอมพิวเตอร์ทั้งแบบตั้งโต๊ะ และพกพาสามารถเชื่อมต่อถึงกันหรือเชื่อมต่อเข้ากับเครือข่ายจากตำแหน่งต่างๆ ที่อยู่ในรัศมีของสัญญาณได้อย่างอิสระ

แต่อย่างไรก็ตาม ความง่ายและสะดวกต่อการติดตั้งและใช้งานของอุปกรณ์ IEEE 802.11 WLAN ก็นำมาซึ่งความไม่ปลอดภัยของเครือข่ายด้วยเช่นกัน การที่จะป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาเครือข่ายภายในผ่านทางอุปกรณ์ไร้สาย นั้นก็มีหลายวิธี ไม่ว่าจะเป็น WEP หรือการจำกัด MAC address แต่วิธีเหล่านี้มีข้อจำกัดเรื่องของจำนวนผู้ใช้งาน ดังนั้นวิธีที่เหมาะกับการใช้ระบบ Wireless LAN ที่มีผู้เข้าใช้งานจำนวนมากนั้นคือวิธีการให้ผู้ใช้กรอกชื่อผู้ใช้และรหัสผ่านก่อนการเข้าสู่ระบบภายในเพื่อเป็นการพิสูจน์ตัวตนของผู้ใช้ก่อนการเข้าใช้ระบบ Wireless LAN เมื่อมีผู้ใช้งานระบบเป็นจำนวนมากแล้ว ปัญหาในเรื่องของการดูแลระบบก็มีตามมาอีก เช่น ผู้ใช้บางคนอาจมีการรับส่งข้อมูลมากจนผิดปกติ จำเป็นต้องตัดออกจากระบบ ต้องการเพิ่ม ลบ แก้ไขข้อมูลผู้ใช้ที่มีอยู่ ซึ่งข้อมูลและวิธีการเหล่านี้จำเป็นอย่างยิ่งต่อผู้ดูแลระบบ ทำให้ต้องมีส่วนของการจัดการที่ให้ผู้ดูแลระบบสามารถจัดการสิ่งเหล่านี้ได้เพิ่มเข้ามา

1.2 วัตถุประสงค์ของโครงงาน

1.2.1 เพื่อจัดรูปแบบการเข้าใช้งานระบบเครือข่ายแลนไร้สายให้มีประสิทธิภาพมากขึ้น

1.2.2 สามารถตรวจสอบข้อมูลของผู้ใช้งานกับฐานข้อมูล แอกทีฟไดเร็กทอรี ได้

1.2.3 สามารถตรวจสอบการใช้งานของผู้ใช้งานขณะกำลังใช้งานอยู่ได้ผ่านทางเว็บ

1.2.4 สามารถยกเลิกการใช้งานของผู้ใช้งานขณะกำลังใช้งานอยู่ได้ผ่านทางเว็บ

1.2.5 สามารถบริหารจัดการฐานข้อมูล แอกทีฟไดเร็กทอรี ของผู้ใช้งานได้ผ่านทางเว็บ

1.3 ขอบเขตโครงงาน

โครงงานนี้เป็นระบบจัดการการให้บริการเครือข่ายแลนไร้สาย โดยสามารถควบคุมและจัดการระบบการเข้าใช้ รวมไปถึงสามารถตรวจสอบการใช้งานของผู้ใช้งานระบบแลนไร้สายได้

การให้บริการอินเทอร์เน็ตผ่านระบบแลนไร้สายนั้นต้องมีการสร้าง และจัดการ ข้อมูลของผู้ใช้งานทุกคนที่ได้รับอนุญาตก่อน เพื่อให้ผู้ใช้แต่ละคนมีชื่อผู้ใช้ และรหัสผ่าน เป็นของตัวเอง โดยจะไม่ซ้ำกับของคนอื่น

วิธีการทำงานนั้นจะมีการใช้เครื่องเซิร์ฟเวอร์ไว้สำหรับคอยจัดการและตรวจสอบความถูกต้องของการยืนยันตัวตนของผู้ใช้บริการ ผู้ใช้บริการทุกคนต้องเข้ามายืนยันตัวตนผ่านทาง เว็บบราวเซอร์ ก่อนเพื่อที่จะส่งข้อมูลนั้นไปตรวจเช็คความถูกต้องจากเครื่องเซิร์ฟเวอร์ จากนั้นเมื่อมีการกรอกชื่อผู้ใช้และรหัสผ่าน ถูกต้องก็จะสามารถใช้บริการออกสู่เครือข่ายอินเทอร์เน็ตได้

นอกจากนี้ยังต้องมีส่วนสำหรับควบคุมและจัดการการเข้าใช้งานเครือข่ายแลนไร้สายในรูปแบบเว็บด้วย โดยส่วนควบคุมและจัดการนี้จะทำให้ผู้ดูแลระบบสามารถตรวจสอบการใช้งานของแต่ละ Account ได้ และสามารถจัดการการตั้งค่าของแต่ละAccount ได้ ดังนั้นจะทำให้ทราบข้อมูลเชิงสถิติว่ามีการใช้งานในระบบอย่างไรบ้าง ระบบต้องสามารถนำรายละเอียดข้อมูลของการใช้งานแต่ละ Account ว่ามีการใช้งาน เมื่อเวลาเท่าไหร่ถึงเวลาเท่าไหร่ และมีการใช้งานมาจากเครื่องไหน เพื่อให้ผู้ดูแลระบบได้รับรู้ข้อมูลและจัดการกับ Account ที่ผิดปกติได้ เช่น สามารถตัดการเชื่อมต่อของ Account ในกรณีที่สงสัยว่ามีการใช้งานมากจนผิดปกติ

เนื่องจากภาควิชาได้เก็บข้อมูล Account ของบุคลากรภายในภาควิชาไว้ที่ เครื่องเซิร์ฟเวอร์ที่เป็นแอกทีฟไดเร็กทอรี ซึ่งใช้ระบบปฏิบัติการ Windows Server 2003 ดังนั้นส่วนการตรวจสอบผู้ใช้ของระบบควรสามารถมาตรวจสอบกับเซิร์ฟเวอร์ของทางภาควิชาได้ และสำหรับระบบควบคุมและจัดการการเข้าใช้งานเครือข่ายไร้สายจะต้องมีความสามารถดังนี้

-ทำงานผ่านทาง เว็บไซท์

-ตรวจสอบข้อมูลเชิงสถิติว่ามีการใช้งานในระบบอย่างไรบ้าง

-ปิดการเชื่อมต่อของแต่ละ ผู้ใช้ ในกรณีที่มีการใช้งานมากจนผิดปกติ

-สามารถเช็คได้ว่าผู้ใช้ได้ออกจากระบบไปแล้ว

1.4 วิธีการดำเนินการ

1.4.1 ศึกษาโครงสร้างและวิธีการพิสูจน์ตัวตนของผู้ใช้งาน Wireless LAN ในแบบ Secure LAN (SLAN)

1.4.2 ศึกษาวิธีการแก้ไข Radius เซิร์ฟเวอร์ ให้เชื่อมต่อกับ แอกทีฟไดเร็กทอรี

1.4.3 ค้นคว้าหาข้อมูลเกี่ยวกับวิธีการที่จะนำมาใช้ในการดูปริมาณการใช้ของผู้ใช้แต่ละคน

1.4.4 จัดหาวัสดุอุปกรณ์ที่จำเป็นในการพัฒนา

1.4.5 วิเคราะห์และออกแบบระบบ

1.4.6 พัฒนาโปรแกรมที่ใช้ในการจัดการระบบ

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1.5.1 ได้รับความรู้ ความเข้าใจเกี่ยวกับการใช้งานระบบปฏิบัติการลินุกส์

1.5.2 ได้รับความรู้ ความเข้าใจเกี่ยวกับการปรับแต่งไฟล์ที่ใช้ในการคอนฟิกต์ต่างๆ

1.5.3 ได้รับความรู้ ความเข้าใจเกี่ยวกับการติดตั้งและใช้งาน Apache เว็บ เซิร์ฟเวอร์

1.5.4 ได้รับความรู้ ความเข้าใจเกี่ยวกับการติดตั้งและใช้งาน Freeradius เซิร์ฟเวอร์

1.5.5 ได้รับความรู้ ความเข้าใจเกี่ยวกับการติดตั้งและใช้งาน Chillispot

1.5.6 ได้รับความรู้ ความเข้าใจเกี่ยวกับกระบวนการติดต่อระหว่างเซิร์ฟเวอร์

1.5.7 สามารถสร้างระบบการเข้าใช้งานเครือข่ายไร้สายที่ผู้ดูแลระบบสามารถควบคุมการทำงานได้โดยง่าย

1.5.8 ได้รับความรู้ความเข้าใจเกี่ยวกับการใช้งานภาษา PHP

1.6 ส่วนประกอบของปริญญานิพนธ์

ปริญญานิพนธ์ฉบับนี้ได้แบ่งเนื้อหาออกเป็น 5 บทด้วยกันคือ

บทที่ 1 กล่าวถึงความสำคัญและที่มาของโครงงาน วัตถุประสงค์ของโครงงาน ขอบเขตของโครงงาน วิธีการดำเนินการ ประโยชน์ที่คาดว่าจะได้รับ และส่วนประกอบของปริญญานิพนธ์

บทที่ 2 กล่าวถึงทฤษฎีพื้นฐานที่ใช้ในโครงงาน ความรู้เกี่ยวกับมาตรฐาน IEEE 802.11 ความรู้เกี่ยวกับการพิสูจน์ตัวตน ความรู้เกี่ยวกับการใช้งานเครือข่ายไร้สาย ความรู้เกี่ยวกับแอกทีฟไดเร็กทอรี

บทที่ 3 กล่าวถึงชิ้นงานของโครงงานนี้ ส่วนที่ได้พัฒนาขึ้น การทำงานของระบบบรรยายโดยละเอียด

บทที่ 4 กล่าวถึงการทดลองและผลการทดลอง ผลการทดลองในส่วนของผู้ใช้ ผลการทดลองในส่วนของผู้ดูแลระบบ

บทที่ 5 เป็นบทวิจารณ์และสรุป ซึ่งกล่าวถึงบทสรุปของโครงงาน วิจารณ์สิ่งที่ได้รับจากโครงงาน และข้อเสนอแนะสำหรับเป็นแนวทางในการพัฒนาต่อ

บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

ปัจจุบันนี้การใช้ระบบเครือข่ายคอมพิวเตอร์กำลังเป็นที่นิยมกันอย่างกว้างขวาง ในองค์กรหรือหน่วยงานต่างๆ ระบบเครือข่ายคอมพิวเตอร์ที่มีใช้อยู่กันเป็นที่แพร่หลายมีอยู่สองประเภทใหญ่ๆ คือระบบเครือข่ายบริเวณเฉพาะที่ (Local Area Network หรือ LAN) และ ระบบเครือข่ายบริเวณกว้าง (Wide Area Network หรือ WAN) ซึ่งส่วนมากจะนิยมใช้สายเคเบิลแบบ UPS CAT5 (Unshielded Twisted Pair Category 5) ในการเชื่อมโยงคอมพิวเตอร์เข้าด้วยกัน แต่แนวโน้มในการพัฒนาเทคโนโลยี ทางด้านเครือข่ายเป็นไปอย่างรวดเร็วและไม่หยุดยั้ง ในปัจจุบันได้มีสื่อใหม่ที่เชื่อมโยงคอมพิวเตอร์เข้าด้วยกันโดยไม่ใช้สายเคเบิล หรือที่เรียกกันว่า ระบบเครือข่ายไร้สาย (Wireless LAN) เป็นเทคโนโลยีที่กำลังได้รับความนิยมและเป็นเป้าหมายที่น่าสนใจเป็นอย่างมากในยุคนี้

2.1 ความรู้เบื้องต้นเกี่ยวกับมาตรฐาน IEEE 802.11

มาตรฐาน IEEE 802.11 ซึ่งได้รับการตีพิมพ์ครั้งแรกเมื่อปี พ.ศ. 2540 โดย IEEE (The Institute of Electronics and Electrical Engineers) และเป็นเทคโนโลยีสำหรับ WLAN ที่นิยมใช้กันอย่างแพร่หลายมากที่สุด คือข้อกำหนด (Specification) สำหรับอุปกรณ์ WLAN ในส่วนของ Physical (PHY) Layer และ Media Access Control (MAC) Layer โดยในส่วนของ PHY Layer มาตรฐาน IEEE 802.11 ได้กำหนดให้อุปกรณ์มีความสามารถในการรับส่งข้อมูลด้วยความเร็ว 1, 2, 5.5, 11 และ 54 Mbps โดยมีสื่อ 3 ประเภทให้เลือกใช้ได้แก่ คลื่นวิทยุที่ความถี่สาธารณะ 2.4 และ 5 GHz, และ อินฟราเรด (Infrared) (1 และ 2 Mbps เท่านั้น) สำหรับในส่วนของ MAC Layer มาตรฐาน IEEE 802.11 ได้กำหนดให้มีกลไกการทำงานที่เรียกว่า CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) ซึ่งมีความคล้ายคลึงกับหลักการ CSMA/CD (Collision Detection) ของมาตรฐาน IEEE 802.3 Ethernet ซึ่งเป็นที่นิยมใช้กันทั่วไปในเครือข่าย LAN แบบใช้สายนำสัญญาณ นอกจากนี้ในมาตรฐาน IEEE802.11 ยังกำหนดให้มีทางเลือกสำหรับสร้างความปลอดภัยให้กับเครือข่าย IEEE 802.11 WLAN โดยกลไกการเข้ารหัสข้อมูล (Encryption) และการตรวจสอบผู้ใช้ (Authentication) ที่มีชื่อเรียกว่า WEP (Wired Equivalent Privacy) ด้วย

มาตรฐาน IEEE 802.11

- IEEE 802.11b

คณะทำงานชุด IEEE 802.11b ได้ตีพิมพ์มาตรฐานเพิ่มเติมนี้เมื่อปี พ.ศ. 2542 ซึ่งเป็นที่รู้จักกันดีและใช้งานกันอย่างแพร่หลายมากที่สุด มาตรฐาน IEEE 802.11b ใช้เทคโนโลยีที่เรียกว่า CCK (Complimentary Code Keying) ผนวกกับ DSSS (Direct Sequence Spread Spectrum) เพื่อปรับปรุงความสามารถของอุปกรณ์ให้รับส่งข้อมูลได้ด้วยความเร็วสูงสุดที่ 11 Mbps ผ่านคลื่นวิทยุความถี่ 2.4 GHz (เป็นย่านความถี่ที่เรียกว่า ISM (Industrial Scientific and Medical) ซึ่งถูกจัดสรรไว้อย่างสากลสำหรับการใช้งานอย่างสาธารณะด้านวิทยาศาสตร์ อุตสาหกรรม และการแพทย์ โดยอุปกรณ์ที่ใช้ความถี่ย่านนี้ก็เช่น IEEE 802.11, Bluetooth, โทรศัพท์ไร้สาย, และเตาไมโครเวฟ) ส่วนใหญ่แล้วอุปกรณ์ IEEE 802.11 WLAN ที่ใช้กันอยู่ในปัจจุบันจะเป็นอุปกรณ์ตามมาตรฐาน IEEE 802.11b นี้และใช้เครื่องหมายการค้าที่รู้จักกันดีในนาม Wi-Fi ซึ่งเครื่องหมายการค้าดังกล่าวถูกกำหนดขึ้นโดยสมาคม WECA (Wireless Ethernet Compatibility Alliance) โดยอุปกรณ์ที่ได้รับเครื่องหมายการค้าดังกล่าวได้ผ่านการตรวจสอบแล้วว่าเป็นไปตามมาตรฐาน IEEE 802.11b และสามารถนำไปใช้งานร่วมกับอุปกรณ์ยี่ห้ออื่นๆที่ได้รับเครื่องหมาย Wi-Fi ได้

- IEEE 802.11a

คณะทำงานชุด IEEE 802.11a ได้ตีพิมพ์มาตรฐานเพิ่มเติมนี้เมื่อปี พ.ศ. 2542 มาตรฐาน IEEE 802.11a ใช้เทคโนโลยีที่เรียกว่า OFDM (Orthogonal Frequency Division Multiplexing) เพื่อปรับปรุงความสามารถของอุปกรณ์ให้รับส่งข้อมูลได้ด้วยความเร็วสูงสุดที่ 54 Mbps แต่จะใช้คลื่นวิทยุที่ความถี่ 5 GHz ซึ่งเป็นย่านความถี่สาธารณะสำหรับใช้งานในประเทศสหรัฐอเมริกาที่มีสัญญาณรบกวนจากอุปกรณ์อื่นน้อยกว่าในย่านความถี่ 2.4 GHz อย่างไรก็ตามข้อเสียหนึ่งของมาตรฐาน IEEE 802.11a ที่ใช้คลื่นวิทยุที่ความถี่ 5 GHz ก็คือในบางประเทศย่านความถี่ดังกล่าวไม่สามารถนำมาใช้งานได้อย่างสาธารณะ ตัวอย่างเช่น ประเทศไทยไม่อนุญาตให้มีการใช้งานอุปกรณ์ IEEE 802.11a เนื่องจากความถี่ย่าน 5 GHz ได้ถูกจัดสรรสำหรับกิจการอื่นอยู่ก่อนแล้ว นอกจากนี้ข้อเสียอีกอย่างหนึ่งของอุปกรณ์ IEEE 802.11a WLAN ก็คือรัศมีของสัญญาณมีขนาดค่อนข้างสั้น (ประมาณ 30 เมตร ซึ่งสั้นกว่ารัศมีสัญญาณของอุปกรณ์ IEEE 802.11b WLAN ที่มีขนาดประมาณ 100 เมตร สำหรับการใช้งานภายในอาคาร) อีกทั้งอุปกรณ์ IEEE 802.11a WLAN ยังมีราคาสูงกว่า IEEE 802.11b WLAN ด้วย ดังนั้นอุปกรณ์ IEEE 802.11a WLAN จึงได้รับความนิยมน้อยกว่า IEEE 802.11b WLAN มาก

- IEEE 802.11g

คณะทำงานชุด IEEE 802.11g ได้ใช้นำเทคโนโลยี OFDM มาประยุกต์ใช้ในช่องสัญญาณวิทยุความถี่ 2.4 GHz ซึ่งอุปกรณ์ IEEE 802.11g WLAN มีความสามารถในการรับส่งข้อมูลด้วยความเร็วสูงสุดที่ 54 Mbps ส่วนรัศมีสัญญาณของอุปกรณ์ IEEE 802.11g WLAN จะอยู่ระหว่างรัศมีสัญญาณของอุปกรณ์ IEEE 802.11a และ IEEE 802.11b เนื่องจากความถี่ 2.4 GHz เป็นย่านความถี่สาธารณะสากล อีกทั้งอุปกรณ์ IEEE 802.11g WLAN สามารถทำงานร่วมกับอุปกรณ์ IEEE 802.11b WLAN

ได้ (backward-compatible) ดังนั้นจึงมีแนวโน้มสูงว่าอุปกรณ์ IEEE 802.11g WLAN จะได้รับความนิยมอย่างแพร่หลายหากมีราคาไม่แพงจนเกินไปและน่าจะมาแทนที่ IEEE 802.11b ในที่สุด

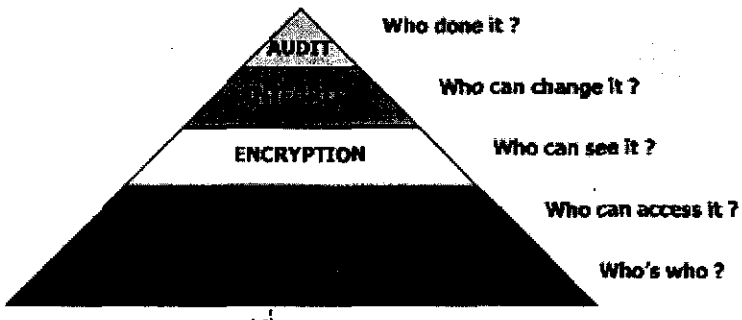
2.2 ความรู้เบื้องต้นเกี่ยวกับการพิสูจน์ตัวตน

2.2.1 นิยามความมั่นคงปลอดภัยคอมพิวเตอร์

จุดประสงค์หลักของความปลอดภัยทางข้อมูลคือ ความลับ (Confidentiality) ความสมบูรณ์ (Integrity) ความพร้อมใช้ (Availability) และการห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) ของข้อมูลต่างๆภายในองค์กร (CIA-N) โดยมีรายละเอียดดังนี้

- **การรักษาความลับ (Confidentiality)** คือการรับรองว่าจะมีการเก็บข้อมูลไว้เป็นความลับ และผู้มีสิทธิเท่านั้นจึงจะเข้าถึงข้อมูลนั้นได้
- **การรักษาความสมบูรณ์ (Integrity)** คือการรับรองว่าข้อมูลจะไม่ถูกเปลี่ยนแปลงหรือทำลายไม่ว่าจะเป็นโดย อุบัติเหตุหรือโดยเจตนา
- **ความพร้อมใช้ (Availability)** คือการรับรองว่าข้อมูลและบริการการสื่อสารต่าง ๆ พร้อมที่จะใช้ได้ในเวลาที่ต้องการใช้งาน
- **การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation)** คือวิธีการสื่อสารซึ่งผู้ส่งข้อมูลได้รับหลักฐานว่าได้มีการส่งข้อมูลแล้วและผู้รับก็ได้รับการยืนยันว่าผู้ส่งเป็นใคร ดังนั้นทั้งผู้ส่งและผู้รับจะไม่สามารถปฏิเสธได้ว่าไม่มีความเกี่ยวข้องกับข้อมูลดังกล่าวในภายหลัง

ในทางปฏิบัตินั้นสามารถกำหนดลักษณะของการควบคุมความมั่นคงปลอดภัย (Security Controls) ได้ 5 ระดับตามรูป



รูปที่ 2.1 Security Pyramid

และถือเป็นองค์ประกอบที่สำคัญส่วนหนึ่งของความมั่นคงปลอดภัยคอมพิวเตอร์ เพราะจัดเป็นการกำหนดและควบคุมทั้งบุคคลที่สามารถเข้าสู่ระบบและเข้าสู่ข้อมูลภายในระบบ และเพื่อกระทำการใดได้บ้าง อนุญาตตามระดับชั้นของความสำคัญของข้อมูล รวมไปถึงการจัดเก็บพฤติกรรมการใช้งานระบบของบุคคลนั้นต่อข้อมูลบนระบบทั้งหมด

2.2.2 วิธีการพิสูจน์ตัวตน

ในระบบเครือข่ายแบบเปิดหรืออินเตอร์เน็ต การพิสูจน์ตัวตนถือได้ว่าเป็นกระบวนการเริ่มต้นและมีความสำคัญที่สุดในการปกป้องเครือข่ายให้ปลอดภัย โพรโตคอลในการพิสูจน์ตัวตนคือโพรโตคอลการสื่อสารที่มีกระบวนการพิสูจน์ตัวตนรวมอยู่ในชุดโพรโตคอล

Secure Socket Layer (SSL)

ในปัจจุบัน ผู้ใช้เครือข่ายอินเทอร์เน็ตมีจำนวนเพิ่มขึ้นอย่างมาก และเครือข่ายนี้ถูกใช้งานในรูปแบบต่างๆมากมายหลายรูปแบบ โดยเฉพาะอย่างยิ่งในการพาณิชย์อิเล็กทรอนิกส์ (e-commerce) ซึ่งผู้ซื้อและผู้ขายจะต้องส่งข้อมูลที่เป็นความลับถึงกันและกัน เช่น ผู้ซื้อส่งหมายเลขบัตรเครดิตหรือที่อยู่และเบอร์โทรศัพท์โดยส่งผ่านไปบนเครือข่าย อินเทอร์เน็ต หากข้อมูลเหล่านี้ถูกส่งไปแบบธรรมดาก็จะเป็นการค่อนข้างง่ายที่ผู้ไม่หวังดีจะสามารถดักจับข้อมูลเหล่านี้ (sniffing) แล้วนำไปใช้ได้ เนื่องจากข้อมูลเหล่านี้อยู่ในรูปของข้อมูลที่ไม่ได้มีการเข้ารหัส ผู้ดักจับข้อมูลก็จะสามารถนำข้อมูลนั้นไปใช้ได้ทันที

ในอีกกรณีหนึ่ง บนเครือข่ายอินเทอร์เน็ตนี้ ผู้ใช้สามารถเชื่อมต่อและใช้งานเครื่องคอมพิวเตอร์ใดๆก็ได้หากผู้ใช้นั้นได้รับอนุญาตและสามารถพิสูจน์ตนเองโดยใช้ ชื่อผู้ใช้ และรหัสผ่าน ที่ถูกต้องบนเครื่องนั้นๆ โดยจะมีโปรแกรมที่ใช้ช่วยในการเชื่อมต่อและใช้งานนั้น เช่น telnet, rsh, rlogin, rcp และ ftp เป็นต้น โปรแกรมเหล่านี้ส่งข้อมูลตามแบบมาตรฐานดั้งเดิมของเครือข่ายอินเทอร์เน็ต กล่าวคือ ส่งข้อมูลทุกอย่าง (รวมทั้ง ชื่อผู้ใช้ และรหัสผ่าน) ในรูปของ ข้อมูลที่ไม่ได้เข้ารหัส ดังนั้นหากมีผู้ดักจับข้อมูลเกี่ยวกับ ชื่อผู้ใช้ และ รหัสผ่านได้ ผู้นั้นก็จะสามารถนำเอาชื่อผู้ใช้ และรหัสผ่าน นี้ไปใช้ในการเชื่อมต่อและใช้งานเครื่องคอมพิวเตอร์เครื่องนั้นได้ต่อไป

เนื่องจากปัญหาที่กล่าวมานี้เป็นปัญหาที่ค่อนข้างใหญ่ เพราะการดักจับข้อมูลนั้นสามารถกระทำได้อย่างค่อนข้างง่าย จึงได้มีการคิดแก้ไขปัญหานี้ขึ้นโดย Netscape ได้คิดค้น โปรโตคอลใหม่ขึ้นมาคือ Secure Socket Layer Protocol (SSL) และโปรแกรมเมอร์ชาว Finland ได้เขียนโปรแกรมขึ้นชุดหนึ่ง เรียกว่า Secure Shell (SSH) ซึ่งทั้ง SSL และ SSH จะเข้ารหัสลับข้อมูลใดๆ ก่อนที่ข้อมูลนั้นจะถูกส่งไปบนเครือข่ายอินเทอร์เน็ต ดังนั้นหากผู้ไม่หวังดีสามารถดักจับข้อมูลนั้นไปได้ ผู้นั้นก็ไม่สามารถที่จะนำข้อมูลนั้นไปใช้ได้ เพราะเขาไม่สามารถตีความข้อมูลนั้นได้

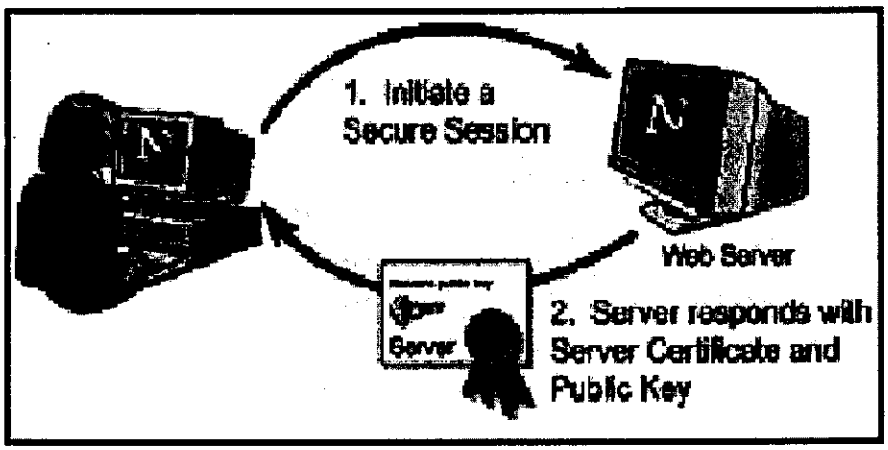
SSL นั้นได้รับการยอมรับอย่างกว้างขวางบน เวิลด์ วาย เว็บ (WWW) ในการใช้สำหรับตรวจสอบ และเข้ารหัสลับการติดต่อสื่อสารระหว่าง เครื่องลูกข่าย และเครื่องแม่ข่าย หน้าที่ของ SSL จะแบ่งออกเป็น 3 ส่วนใหญ่ๆ คือ

1. การตรวจสอบเครื่องแม่ข่ายว่าเป็นตัวจริง: ตัวโปรแกรมเครื่องลูกข่ายที่มีขีดความสามารถในการสื่อสารแบบ SSL จะสามารถตรวจสอบเครื่องแม่ข่าย ที่ตนกำลังจะไปเชื่อมต่อได้ว่าเครื่องแม่ข่ายนั้นเป็นเครื่องแม่ข่ายตัวจริงหรือไม่ โดยใช้เทคนิคการเข้ารหัสแบบ กุญแจ

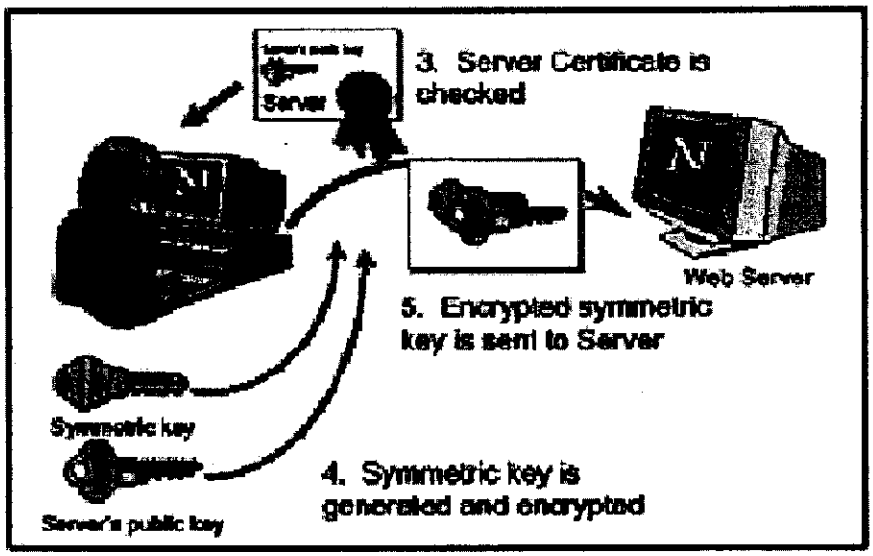
สาธารณะ ในการตรวจสอบใบรับรอง (certificate) และ ID สาธารณะของเครื่องแม่ข่ายนั้น (โดยที่มีองค์กรที่เครื่องลูกข่ายเชื่อถือเป็นผู้ออกใบรับรองและ ID สาธารณะให้แก่ เครื่องแม่ข่ายนั้น) หน้าที่นี้ของ SSL เป็นหน้าที่ที่สำคัญ โดยเฉพาะอย่างยิ่งในกรณีที่ เครื่องลูกข่ายต้องการที่จะส่งข้อมูลที่เป็นความลับ (เช่น หมายเลขบัตรเครดิต) ให้กับเครื่องแม่ข่าย ซึ่งเครื่องลูกข่ายจะต้องตรวจสอบก่อนว่า เครื่องแม่ข่ายเป็นตัวจริงหรือไม่

2. การตรวจสอบว่าเครื่องลูกข่ายเป็นตัวจริง: เครื่องแม่ข่ายที่มีขีดความสามารถในการสื่อสารแบบ SSL จะใช้เทคนิคเช่นเดียวกับในหัวข้อที่แล้วในการตรวจสอบเครื่องลูกข่าย หรือผู้ใช้ว่าเป็นตัวจริงหรือไม่ โดยจะตรวจสอบใบรับรอง และID สาธารณะ (ที่มีองค์กรที่ เครื่องแม่ข่ายเชื่อถือเป็นผู้ออกให้) ของเครื่องลูกข่าย หรือผู้ใช้นั้น หน้าที่นี้ของ SSL จะมีประโยชน์ในกรณีเช่น ธนาคารต้องการที่จะส่งข้อมูลลับทางการเงินให้แก่ลูกค้าของตนผ่านทางเครือข่ายอินเทอร์เน็ต (เครื่องแม่ข่าย ก็จะต้องตรวจสอบ เครื่องลูกข่ายก่อนว่าเป็น เครื่องลูกข่าย นั้นจริง)

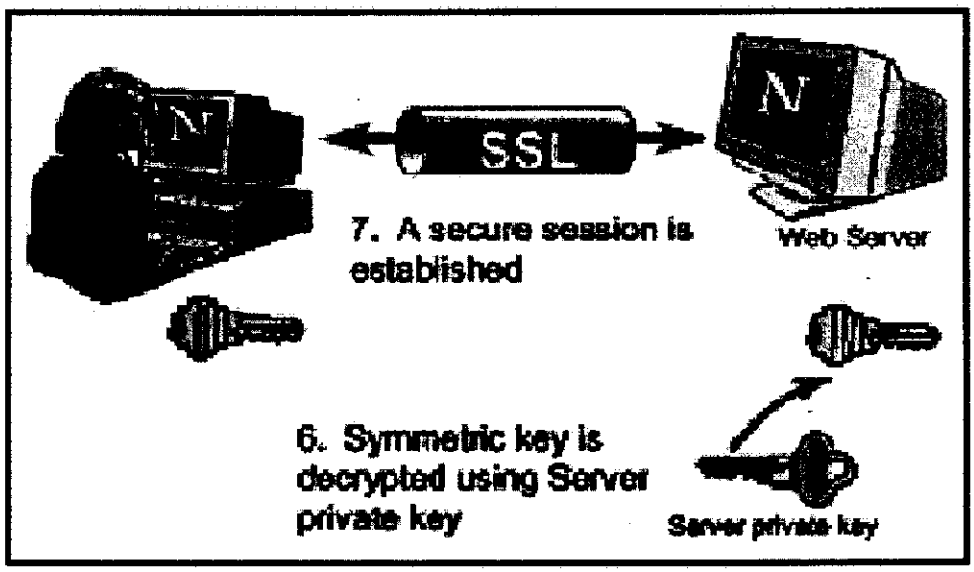
3. การเข้ารหัสลับการเชื่อมต่อ: ในกรณีนี้ ข้อมูลทั้งหมดที่ถูกส่งระหว่างเครื่องลูกข่าย และเครื่องแม่ข่าย จะถูกเข้ารหัสลับ โดยโปรแกรมที่ส่งข้อมูลเป็นผู้เข้ารหัส และโปรแกรมที่รับข้อมูลเป็นผู้ถอดรหัส (โดยใช้วิธี กุญแจสาธารณะ) นอกจากการเข้ารหัสลับในลักษณะนี้แล้ว SSL ยังสามารถปกป้องความถูกต้องสมบูรณ์ของข้อมูลได้อีกด้วย กล่าวคือ ตัวโปรแกรมรับข้อมูลจะทราบได้หากข้อมูลถูกเปลี่ยนแปลงไปในขณะกำลังเดินทางจากผู้ส่งไปยังผู้รับ



รูปที่ 2.2 ผู้ใช้คอมพิวเตอร์เริ่มกระบวนการติดต่อเซิร์ฟเวอร์ที่มี SSL และเซิร์ฟเวอร์ส่งใบรับรองที่ผ่านการเข้ารหัสกลับมา



รูปที่ 2.3 คอมพิวเตอร์ของผู้ใช้สร้างกุญแจสมมาตร และทำการเข้ารหัสกุญแจสมมาตรด้วยกุญแจสาธารณะของเซิร์ฟเวอร์ที่ได้รับมา



รูปที่ 2.4 เซิร์ฟเวอร์ถอดรหัสที่ได้รับด้วยกุญแจส่วนตัว และได้กุญแจสมมาตรของลูกค้าไว้ใช้

Radius Authentication and Authorization

RADIUS (Remote Access Dial-Up User Service) เป็นเทคโนโลยีมาตรฐานอีกอันหนึ่งซึ่งใช้กันมากในองค์กรเพื่อป้องกันการเข้าถึงเครือข่ายไร้สาย โดย RADIUS คือ โครงสร้าง ชื่อผู้ใช้และรหัสผ่าน ซึ่งเป็นเฉพาะผู้ที่ได้รับการอนุญาตให้เข้าถึงเครือข่ายได้เท่านั้น ครั้งแรกที่ผู้ใช้ต้องการเข้าถึงเครือข่าย, ไฟล์ที่ต้องการความปลอดภัย หรือ Net location เขาจะต้องใส่ ชื่อผู้ใช้ และรหัสผ่าน ส่งมันผ่านเครือข่าย ไปยัง RADIUS เครื่องแม่ข่าย เครื่องแม่ข่ายก็จะตรวจสอบข้อมูลผู้ใช้และรหัสผ่าน ก่อนจึงยอมให้ผู้ใช้เข้าใช้เครือข่ายได้ RADIUS สามารถถูกติดตั้งเพื่อให้การเข้าถึงใน

ระดับที่ต่างกัน ตัวอย่างเช่น ระดับหนึ่งสามารถให้ใช้อินเทอร์เน็ตได้ อีกระดับให้ใช้อินเตอร์เน็ต และ อีเมลล์ได้ อีกระดับหนึ่งสามารถใช้อินเตอร์เน็ต อีเมลล์ และไฟล์ข้อมูลทางธุรกิจที่ต้องการความปลอดภัยได้

2.3 โครงสร้างของแอกทีฟไดเร็กทอรี

Active Directory (AD) เป็นไดเรกทอรี่เซอร์วิสในระดับองค์กร ที่ถูกออกแบบบนมาตรฐานของเทคโนโลยีอินเทอร์เน็ต เอาไว้รองรับการค้นหาทรัพยากรต่างๆ บนเครือข่ายขนาดใหญ่ และยังช่วยให้ผู้ดูแลระบบ จัดการบริหารเครือข่ายที่ซับซ้อนจากศูนย์กลางได้อย่างสะดวก AD เป็นการทำงานร่วมกันระหว่าง Domain Naming System (DNS) และ Lightweight Directory Access Protocol (LDAP) ทำให้สามารถติดต่อเชื่อมโยง (interoperability) กับไดเรกทอรี่เซอร์วิสอื่นๆได้อีกด้วย และมีการพัฒนา Distributed Component Object Model (DCOM) ให้มีประสิทธิภาพในการกระจายแอพพลิเคชั่นได้ดียิ่งขึ้น AD จะมีโครงสร้างอยู่ 2 แบบคือ ทางกายภาพ (Physical Structure) และทางลอจิคอล (Logical Structure)

ไดเรกทอรี่ตัวอย่างที่เห็นอยู่ทั่วไป เช่น สมุดโทรศัพท์หน้าเหลือง ที่ใช้เก็บรวบรวมข้อมูลเกี่ยวกับรายชื่อ นามสกุล ที่อยู่ เบอร์โทร เมื่อเราต้องการจะค้นหาเบอร์โทรศัพท์ก็เพียงแต่เปิดไปยังหน้าที่มี ชื่อ-สกุลนั้นๆ สมุดโทรศัพท์จึงเป็นดั่งที่รวบรวมข้อมูลต่างๆ ที่เกี่ยวกับผู้ใช้โทรศัพท์เอาไว้ AD ก็คล้ายกับสมุดโทรศัพท์แต่จะเก็บรวบรวมอ็อบเจ็กต์และทรัพยากรต่างๆบนระบบเน็ตเวิร์กเอาไว้ (อ็อบเจ็กต์เหล่านี้คือ ยูสเซอร์ เครื่องพิมพ์ ไฟล์เอกสาร อีเมลแอดเดรส) นอกจากนี้ AD ยังจัดเก็บคุณสมบัติ (Attributes) ของอ็อบเจ็กต์และทรัพยากรนั้นไว้เพื่อให้ยูสเซอร์สามารถเข้ามาค้นหาอ็อบเจ็กต์ที่ต้องการได้อย่างรวดเร็ว AD ประกอบด้วยการทำงาน 2 ส่วนด้วยกันคือ Active Directory Service และ Active Directory Database

Active Directory Service

เป็นการให้บริการแก่ Admin (ผู้บริหารระบบ) เช่น การสร้างหรือลบรายชื่อผู้ใช้ การเปลี่ยนรหัสผ่าน การกำหนดนโยบายของกลุ่ม (Group Policy) การสร้างแชร์โฟลเดอร์ การสร้างรายชื่อเครื่องคอมพิวเตอร์ การติดตั้งพริ้นเซิร์ฟเวอร์ ให้บริการในการค้นหาอ็อบเจ็กต์หรือทรัพยากรต่างๆบนระบบเน็ตเวิร์ก Active Directory Service จะสนับสนุนทั้งโปรโตคอล DNS และ LDAP

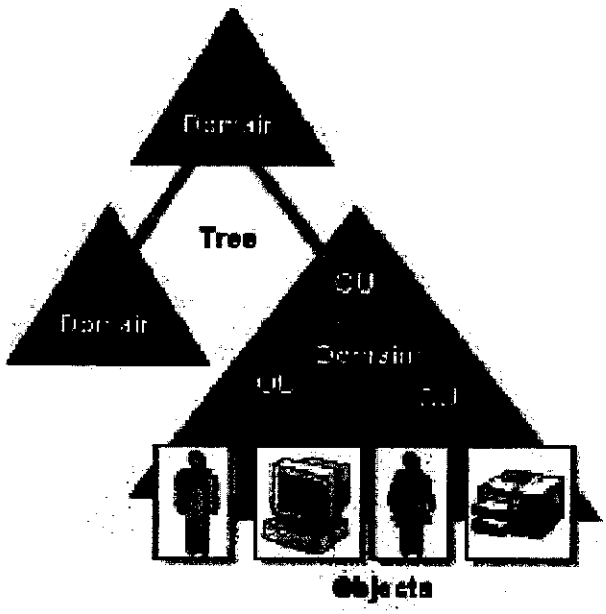
Active Directory Database

เป็นฐานข้อมูลในการจัดเก็บไดเรกทอรี่(อ็อบเจ็กต์) บนระบบเน็ตเวิร์กไว้ เช่น บัญชีรายชื่อและคุณลักษณะของผู้ใช้-กลุ่มผู้ใช้ รายชื่อ และคุณสมบัติของทรัพยากรต่างๆ (คอมพิวเตอร์ เครื่องพิมพ์ แชร์โฟลเดอร์) ในการจัดเก็บรายชื่อและคุณสมบัติของทรัพยากรบนระบบเน็ตเวิร์กไว้

ในฐานข้อมูล Active Directory จะช่วยให้ยูสเซอร์สามารถค้นหาและเรียกใช้ทรัพยากรนั้นได้ง่ายและรวดเร็วขึ้น

ส่วนประกอบของ Active Directory

Active Directory เป็นฐานข้อมูลอเนกประสงค์ที่ใช้เก็บรายละเอียดบัญชีรายชื่อ-คุณสมบัติผู้ใช้, กลุ่มผู้ใช้, คุณสมบัติของทรัพยากร และแอพพลิเคชั่น โดยจะมองทรัพยากรเป็นเหมือนกับวัตถุ (Object) มี OU (Organization Unit) สำหรับเก็บอ็อบเจ็กต์ต่างเอาไว้ มีการจัดลำดับชั้น (Hierarchy) คล้ายๆ โครงสร้างแบบป่า-ต้นไม้ (Forest-Tree) ที่ใช้เก็บไฟล์-โฟลเดอร์ต่างๆ ฐานข้อมูลเหล่านี้จะอยู่บนเครื่อง Windows Server 2003 ที่เป็นโดเมนคอนโทรลเลอร์(Domain Controller)



รูปที่ 2.5 โครงสร้างพื้นฐานของโดเมนคอนโทรลเลอร์และ OU

จากรูปโดเมนของ Active Directory มีโครงสร้างเป็นลำดับชั้น (Hierarchy) แบบต้นไม้คือ จากโดเมนหลัก จะถูกแบ่งชั้นลงมาเป็นโดเมนย่อย จากโดเมนย่อยลงมาเป็นหน่วยขององค์กร Organization Unit (OU) ซึ่งประกอบด้วยอ็อบเจ็กต์ต่างๆ (ผู้ใช้ เครื่องพิมพ์ กลุ่ม และ ทรัพยากรต่างๆ) และในองค์กรยังสามารถจะมีโดเมนหลัก (Tree) ได้มากกว่าหนึ่งโดเมน

อ็อบเจ็กต์ (Object) เป็นส่วนที่เล็กที่สุดของไดเรกทอรี่ อ็อบเจ็กต์จะรวมไปถึงยูสเซอร์แอ็คเคาน์ แชร์โฟลเดอร์ เครื่องพิมพ์ กลุ่มยูสเซอร์ ซึ่งอ็อบเจ็กต์แต่ละตัวจะมีแอตทริบิวต์ (Attribute) ในการแสดงคุณสมบัติของอ็อบเจ็กต์นั้นๆ เช่น อ็อบเจ็กต์ยูสเซอร์แอ็คเคาน์จะมีแอตทริบิวต์เป็น Name, Last Name, E-mail

คลาส (Class) เป็นตัวแบ่งประเภทของอ็อบเจ็กต์ บนฐานข้อมูล AD จะมีดีฟอล์ทคลาสที่ถูกสร้างขึ้นในการติดตั้ง AD เช่น Built in, Computers, Domain Controller, Foreign Security Principals และ Users ในการสร้างรายชื่อยูสเซอร์ขึ้นมาจะถูกเก็บไว้ในคลาส Users ส่วนรายชื่อเครื่องคอมพิวเตอร์จะถูกเก็บไว้ในคลาส Computers หมายความว่าอ็อบเจ็กต์แต่ละตัวจะต้องถูกเก็บไว้ในคลาสของตัวเอง

แอตทริบิวต์ (Attributes) เป็นตัวที่ใช้บอกถึงคุณสมบัติ คุณลักษณะ และพฤติกรรมของอ็อบเจ็กต์กล่าวคือ อ็อบเจ็กต์แต่ละตัวจะมีแอตทริบิวต์ที่แตกต่างกัน แต่อ็อบเจ็กต์ที่อยู่ในคลาสเดียวกันจะมีแอตทริบิวต์ที่เหมือนกันเช่น อ็อบเจ็กต์ในคลาส Users จะมีแอตทริบิวต์ Name, Last Name, Logon Name, รหัสผ่าน, E-mail, Telephone etc. แต่ละอ็อบเจ็กต์ของยูสเซอร์แอ็คเคาน์จะมีค่า(Value) หรือค่าของแอตทริบิวต์ต่างกัน เช่น อ็อบเจ็กต์หนึ่งมีค่าแอตทริบิวต์ Logon Name เป็น chawalit จะเป็นการบอกให้ทราบว่าอ็อบเจ็กต์นี้เป็นตัวแทนของยูสเซอร์ chawalit sapsatitkul ซึ่งจะมีค่าแอตทริบิวต์ Logon Name ไม่ซ้ำกับอ็อบเจ็กต์ตัวอื่นๆ

Organization Unit (OU) เป็นเสมือนดังคอนเทนเนอร์ (Container) ในการเก็บอ็อบเจ็กต์ต่างไว้ภายในตามลำดับ OU จะมีโครงสร้างเป็นลำดับชั้น (Hierarchy) ทำให้สามารถสร้าง OU ย่อยลงไปได้อีก OU ยังช่วยแบ่งเบาภาระในการทำงานได้อีกด้วย เช่น ถ้าต้องการกำหนดนโยบายต่างๆ ให้กับอ็อบเจ็กต์แบบ Users, Computers ก็ให้กำหนดนโยบายนั้นผ่าน OU ที่อ็อบเจ็กต์เหล่านั้นอยู่ภายในเพียงครั้งเดียวเท่านั้น ทำให้ไม่ต้องเสียเวลาไปกำหนดทีละตัว

โดเมน (Domain) เป็นที่รวมของทรัพยากรบนระบบเน็ตเวิร์กเอาไว้ทั้งหมด เช่น ยูสเซอร์ เครื่องคอมพิวเตอร์ เครื่องเซิร์ฟเวอร์ เครื่องพิมพ์ แชร์โฟลเดอร์ และอ็อบเจ็กต์อื่นๆ ไว้ด้วยกัน ภายใต้ชื่อโดเมนนั้นจะต้องมีฐานข้อมูลส่วนกลางที่ใช้เก็บรายละเอียดต่างๆ ของแอ็คเคาน์ และทรัพยากรต่างๆ เอาไว้

2.4 Lightweight Directory Access Protocol (LDAP)

LDAP คืออะไร

LDAP (นิยมอ่านว่า "แอล-แด็บ") เป็นโปรโตคอลที่พัฒนามาจาก โปรโตคอล X.500 ซึ่งใช้ในการเข้าถึงและ Update ข้อมูลของไดเร็กทอรี่ ซึ่งไดเร็กทอรี่ในทางคอมพิวเตอร์ที่จริงก็อาจเรียกได้ว่าเป็น ดาต้าเบสแบบพิเศษ หรือ Data repository ที่บรรจุรายละเอียดของอ็อบเจ็คต่างๆ เช่น Users, Application, Files, Printer และอื่นๆ รวมทั้ง Security information ของอ็อบเจ็คเหล่านี้ด้วย โดยข้อแตกต่างของ ไดเร็กทอรี่ กับ ดาต้าเบสปกติ ได้แก่

1. Operation: ใน ไดเร็กทอรี่จะเน้นที่การ Access ข้อมูลหรือ อ่านข้อมูล มากกว่า Update

หรือ เขียนข้อมูล ในขณะที่ ดาต้าเบส ทั่วไปจะเน้นการ Update มากกว่า

2. Transaction: ใน ดาต้าเบส จะรองรับการทำ Transaction หรือการ Update ข้อมูลสองจุดที่ต้องสอดคล้องกัน แบบ All-or-nothing เช่นการโอนเงินจากบัญชีหนึ่ง ไปอีกบัญชีหนึ่ง ที่ต้องการความสมบูรณ์ทั้ง 2 ฝั่ง หรือไม่ก็ไม่ต้องทำเลย ในขณะที่ ไดเร็กทอรี่ ที่เน้นการอ่านอย่างเดียว อาจจะไม่ต้องการความสอดคล้องกันของข้อมูลบ้างนัก เช่นเมื่อมีการย้ายที่อยู่ระหว่างคน 2 คน ก็ต้องมีการปรับเปลี่ยนเบอร์ติดต่อของ 2 คนนั้น ซึ่งตรงนี้อาจจะไม่จำเป็นต้องทำทันที อย่างไรก็ตาม Feature นี้อาจจะมีการผนวกเข้ากับ LDAP Product ใหม่ๆ ในอนาคตก็ได้
3. Data Accuracy: ไดเร็กทอรี่ อาจจะมีข้อจำกัดในการจัดเก็บข้อมูลที่ไม่สมบูรณ์ เช่นมีแต่ชื่อ ไม่มีที่อยู่ แต่อย่างไรก็ตาม เราสามารถ Configure คุณสมบัติเหล่านี้ได้ในบาง Directory Service
4. Query: Directory ไม่ Support Query String (SQL, Structured Query Language)

อย่างไรก็ตามถึงแม้ไดเร็กทอรี่จะมีคุณสมบัติด้อยกว่าดาต้าเบสหลายประการ แต่เนื่องจากโปรโตคอลที่ใช้ในการเข้าถึงไดเร็กทอรี เช่น LDAP มีความเร็วในการเข้าถึงข้อมูลสูง และก็ทำให้ Application ที่ทำงานบนโปรโตคอลเหล่านี้สามารถเข้าถึงข้อมูลอย่างรวดเร็ว ทำให้ระบบไดเร็กทอรีเป็นที่ยอมรับ และนำมาใช้งานทั่วไป

นอกจากประโยชน์ในการค้นหาข้อมูลได้อย่างรวดเร็วแล้ว ไดเร็กทอรียังเป็นโครงสร้างข้อมูลที่แสดงให้ผู้ใช้เห็นข้อมูลทั้งหมดได้จากมุมมองเดียว (Single Logical View) แม้ว่าแท้จริงแล้วข้อมูลเหล่านั้นอาจถูกเก็บแยกกันอยู่อย่างกระจัดกระจายตาม Host ต่างๆ บนระบบแบบกระจาย (Distributed System) ซึ่งข้อดีต่างๆ เหล่านี้ ทำให้มีการพัฒนา Application ที่ใช้ Directory Service ออกมามากมาย และ LDAP ก็คือหนึ่งในมาตรฐานที่ใช้จัดการ การรับส่งข้อมูลระหว่าง Application เครื่องแม่ข่าย ที่เก็บไดเร็กทอรี เหล่านี้ กับ เครื่องลูกข่าย Application ที่เป็นฝ่ายเรียกดูข้อมูลจาก ไดเร็กทอรี

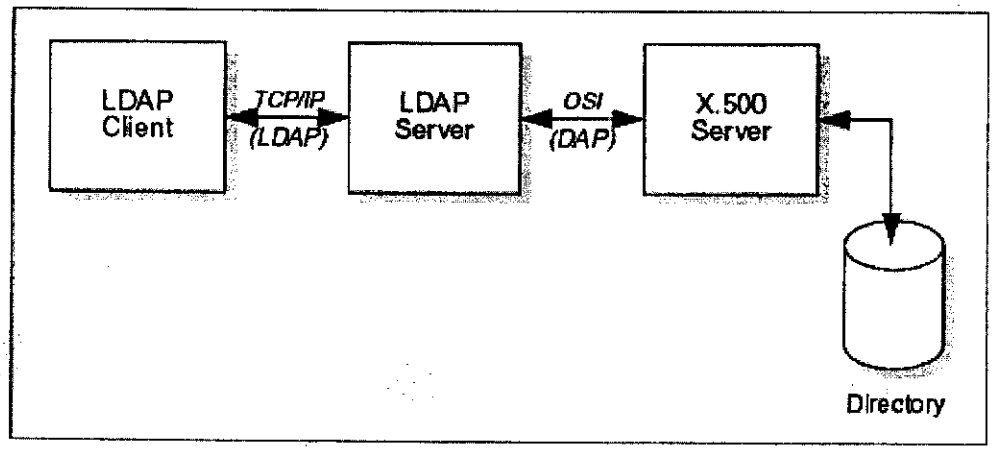
อีกหนึ่งสาเหตุที่จำเป็นต้องมีมาตรฐานในการเข้าถึงข้อมูลในไดเร็กทอรีนั้นก็เพื่อ ให้การพัฒนา Application ที่ใช้ติดต่อกับไดเร็กทอรี เครื่องแม่ข่าย นั้นมีความยืดหยุ่นขึ้น โดย Developer สามารถเรียกใช้ Application Programming Interface (API) เพื่อติดต่อกับ Directory Service ได้โดยไม่ต้องทราบวิธีการเข้าถึงโดยละเอียด เช่นโครงสร้างไดเร็กทอรี หรือ ชนิดของข้อมูล (Data Type) ภายใน หรือไม่จำเป็นต้องปรับแก้ Application ใหม่หากมีความต้องการชนิดข้อมูลใหม่ๆ เป็นต้น

นอกเหนือจากที่กล่าวมาข้างต้นแล้ว การมีมาตรฐานเดียวกัน ทำให้ผู้ผลิต Application และ Network device ที่รองรับการใช้งาน Directory Service มีระเบียบวิธีที่ชัดเจนเป็นกลาง ทำให้การ

ติดต่อระหว่าง Application จากต่างผู้ผลิต หรือต่าง Platform นั้นเป็นไปได้อย่างรวดเร็ว ถูกต้อง และปลอดภัย โดยไม่ต้องทราบข้อมูลที่ใช้ในการติดต่อ เช่น Platform ที่ใช้, Host Name หรือ IP address เช่นเดียวกับการที่เราต้องมี TCI/IP, HTTP, FTP, RPC หรือ ORB เป็นมาตรฐานที่ใช้อยู่ทั่วโลก

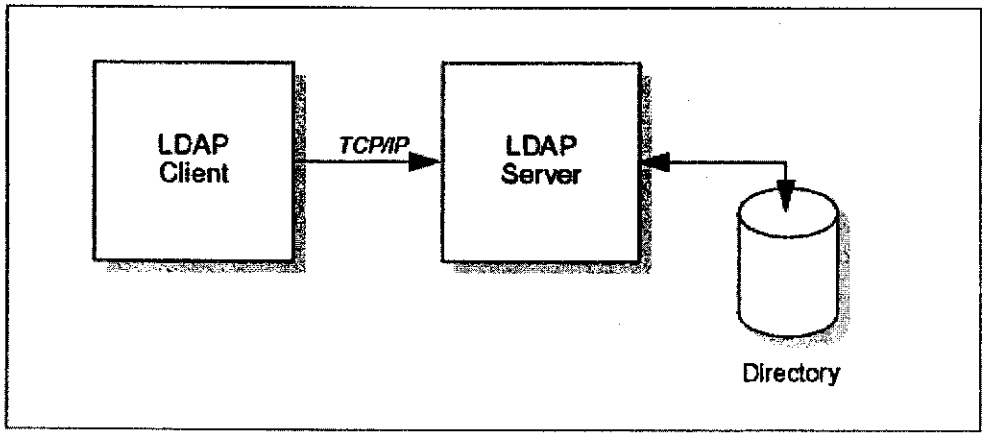
LDAP เป็นมาตรฐานที่ได้รับการยอมรับอย่างกว้างขวาง และมี Application Vendor อยู่หลายราย อาทิ OpenLDAP, IBM, Oracle, Microsoft ซึ่ง Product ที่ได้รับความนิยมก็ได้แก่ Slapd ของ University of Michigan และ Openldap, Directory Server ของ Netscape, Active Directory (AD) ของ Microsoft, Novell Directory Services (NDS) ของ Novell, Sun Directory Services (SDS) ของ Sun และ Internet Directory Server (IDS) ของ Lucent

LDAP ได้รับการออกแบบมาให้อยู่บน TCP/IP Layer ที่มีเพียง 4 Layer ทำให้มีความต้องการทรัพยากรน้อยกว่า DAP ของมาตรฐาน X.500 อย่างไรก็ตาม หากมีความต้องการติดต่อกันระหว่าง LDAP เครื่องลูกข่าย กับ X.500 เครื่องแม่ข่าย จำเป็นจะต้องมีการติดต่อผ่านเกตเวย์ ที่เรียกว่า LDAP เซิร์ฟเวอร์ ตามรูป



รูปที่ 2.6 การติดต่อกันระหว่าง LDAP เครื่องลูกข่าย กับ X.500 เครื่องแม่ข่าย

จากภาพจะเห็นได้ว่า LDAP เครื่องแม่ข่ายจะต้องมีความเข้าใจทั้ง TCP/IP และ OSI Model ในขณะที่ตัว LDAP เครื่องลูกข่ายไม่จำเป็นต้องทำความเข้าใจกับ OSI Layer และไม่ต้องประมวลผลตาม DAP ที่มีความซับซ้อน และ Overhead สูง สำหรับระบบที่ไม่มีการใช้ X.500 ก็สามารถมีเพียง LDAP เครื่องลูกข่าย กับ LDAP เครื่องแม่ข่าย ซึ่งเรียกว่า LDAP stand-alone server ตามรูปด้านล่าง



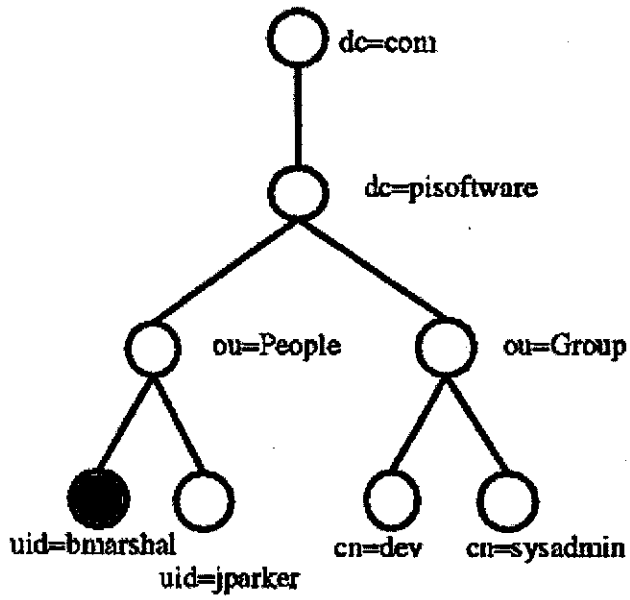
รูปที่ 2.7 การติดต่อแบบ LDAP stand-alone server

จากตัวอย่าง 2 ตัวอย่างข้างต้น ทำให้เราเห็นว่า จากมุมมองของเครื่องลูกข่ายแล้ว ไม่ว่าได เร็กทอรีที่ติดต่อเข้าไปจะอยู่บน LDAP เครื่องแม่ข่าย หรือ X.500 เครื่องแม่ข่าย เครื่องลูกข่ายจะ เรียกไดเร็กทอรีเหล่านั้นว่า LDAP Directory และเรียก เครื่องแม่ข่าย นั้นว่า LDAP Server

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

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

Schema ของ Directory จะระบุ DN และระบุว่า แต่ละ Entry จะประกอบไปด้วย Attribute ใดบ้าง โดย Schema จะกำหนดข้อมูลเหล่านี้ไว้ใน Object class ซึ่งได้แก่ List ของ Mandatory กับ Optional Attribute, วิธีการเปรียบเทียบ Attribute, ชนิดและขนาดของข้อมูลที่อนุญาต ซึ่งทุกๆEntry จะต้องเชื่อโยงไว้กับObjectClassหนึ่งClass



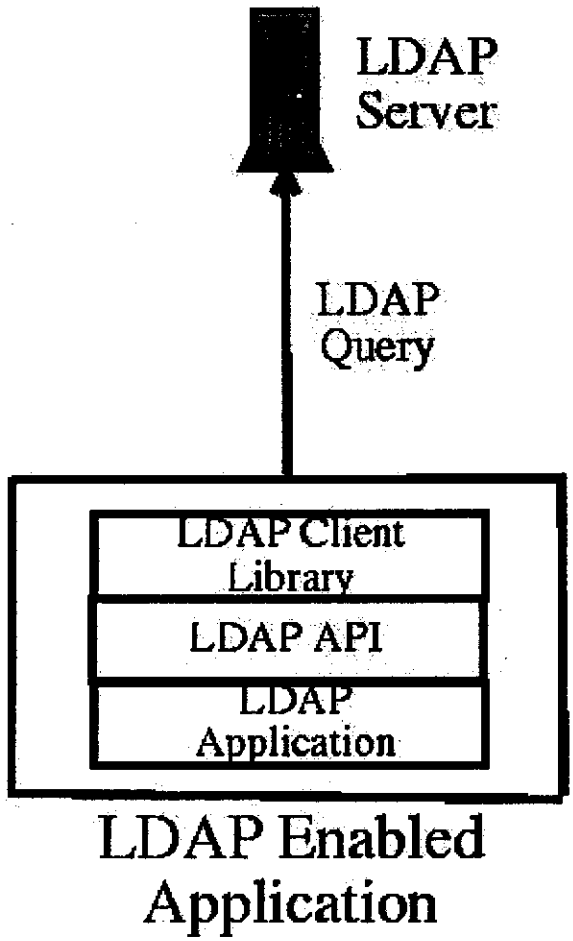
รูปที่ 2.8 โครงสร้าง Entry ของ Directory แบบ Hierarchy

จาก Hierarchy ของ Directory ด้านบน Entry ที่มีสีทึบจะถูกระบุด้วย DN ดังนี้

dn: uid=bmarshal,ou=People,dc=pisoftware,dc=com

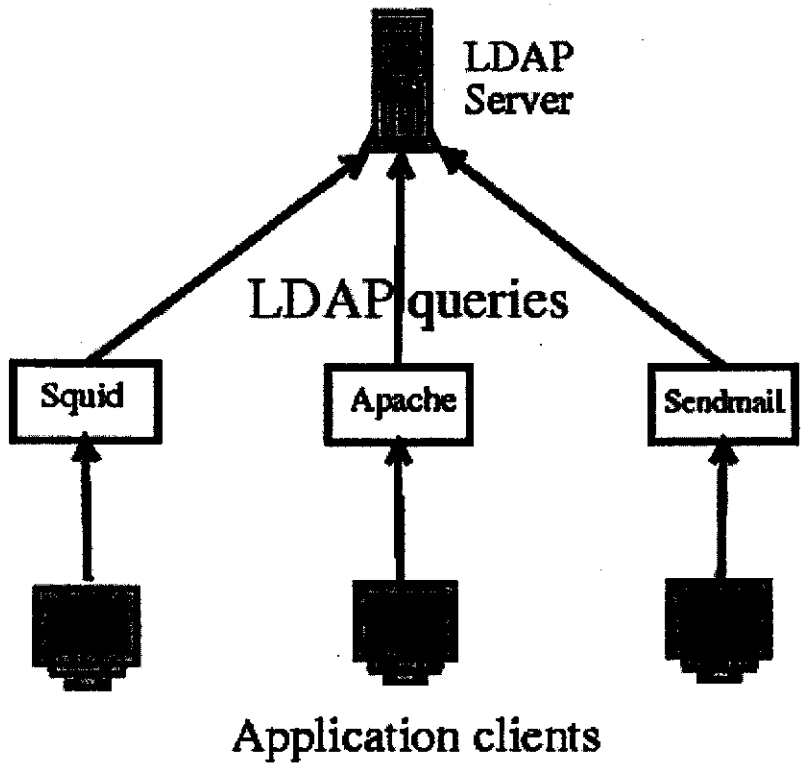
แอตทริบิวต์ส่วนใหญ่จะมีการใช้ตัวอักษรย่อระบุ type ซึ่งได้แก่ uid = User id, cn = Common Name, sn = Surname, l = Location, ou = Organizational Unit, o = Organization, dc = Domain Component, st = State, c = Country, etc. โดยข้อมูลเพิ่มเติมในส่วนนี้สามารถหาได้จาก (RFC2256)

โดยทั่วไป LDAP Application จะประกอบด้วย Layer ต่างๆดังภาพด้านล่าง



รูปที่ 2.9 Layer LDAP application

เนื่องจาก LDAP เป็นมาตรฐานที่ได้รับการยอมรับในหลายผู้ผลิต ดังนั้นการ Implement LDAP Application จึงนำไปประยุกต์ใช้ได้ในหลายๆ Application ดังภาพ



รูปที่ 2.10 การประยุกต์ LDAP ใช้งาน

การสร้างดาต้าเบส หรือไดเร็กทอรี ด้วยการ เพิ่มอ็อบเจ็ค หรือ เอ็นทรี และ แอตทริบิวต์ ลงไปใน LDAP Database

2.4.1 การสร้างไดเร็กทอรี

ในขณะที่ LDAP Service กำลังทำงานอยู่นั้น เราสามารถใช้ Command line ในการเพิ่มหรือลบ อ็อบเจ็ค หรือ เอ็นทรี ที่มีอยู่ได้ รวมไปถึงการเพิ่มแอตทริบิวต์ ใหม่ๆ หรือแก้ไขแอตทริบิวต์เดิม คำสั่งในการเพิ่ม อ็อบเจ็ค หรือ เอ็นทรี ใหม่รวมทั้ง แอตทริบิวต์ของอ็อบเจ็ค หรือ เอ็นทรี นั้น คือ 'ldapadd' ส่วนคำสั่งในการแก้ไข อ็อบเจ็ค และ แอตทริบิวต์ คือ 'ldapmodify'

LDAP security model

เป็นโมเดลของโครงสร้าง LDAPv3 ใช้กำหนดสิทธิในการใช้งานและการเข้าถึงข้อมูลของผู้ใช้หรือไคลเอนท์โดยที่การทำงานของ LDAP เครื่องแม่ข่าย และ LDAP เครื่องลูกข่าย นั้นจะทำงานในรูปแบบ connection-oriented โปรโตคอล กล่าวคือก่อนที่จะเริ่มทำการรับ-ส่งข้อมูลกันนั้น ไคลเอนท์จะทำการส่ง Operation bind เพื่อขอสิทธิการเข้าใช้งาน เมื่อ LDAP เครื่องแม่ข่าย ทำการตรวจสอบว่าสิทธิในการใช้งานในระดับใด และมีความสามารถในการเข้าถึงข้อมูลในระดับใดบ้าง จึงยอมให้ไคลเอนท์เข้าใช้งานในไดเร็คทอรี่เซิฟเวอร์ รูปแบบของการควบคุมการเข้าถึงข้อมูลเรียกว่า Access control

Access control model

ได้กำหนดสิทธิของผู้ใช้แบ่งเป็น 3 ระดับ ได้แก่

1. Administrator ในระดับนี้เป็นระดับสำหรับผู้ดูแลระบบสามารถเปลี่ยนแปลงแก้ไขข้อมูลใน Entry ทั้งหมดของไดเร็คทอรี่เซฟเวอร์ สามารถที่จะทำการสร้าง แอตทริบิวต์ และ อ็อบเจ็คคลาสขึ้นมาใหม่ได้

2. User ในระดับนี้ยอมให้ผู้ใช้หรือไคลเอนท์ ที่มีสิทธิการใช้งาน 2 รูปแบบคือ

2.1 สามารถทำการอัพเดตข้อมูลส่วนตัวที่ทางผู้บริหารระบบ ยอมให้มีการเปลี่ยนแปลงได้ เช่น เบอร์โทรศัพท์ เปลี่ยนแปลงที่อยู่ ฯลฯ

2.2 ความสามารถของการทำงานแบบ Anonymous ซึ่งจะกล่าวในหัวข้อถัดไป

3. Anonymous ในระดับนี้จะยอมให้ LDAP เครื่องลูกข่าย หรือผู้ใช้สามารถค้นหาข้อมูลในไดเร็คทอรี่เซฟเวอร์ตามสิทธิที่กำหนดให้ ไม่สามารถเปลี่ยนแปลงแก้ไขข้อมูลภายใน entry ได้ โดยปรกติแล้วการใช้งานแบบ Anonymous ไม่จำเป็นต้องทำการขอสิทธิ์เข้าใช้งานโดยการ bind

2.4.2 การติดต่อกับโปรโตคอล LDAP ด้วย PHP

PHP มีฟังก์ชั่นที่ใช้ติดต่อกับโปรโตคอล LDAPดังตาราง

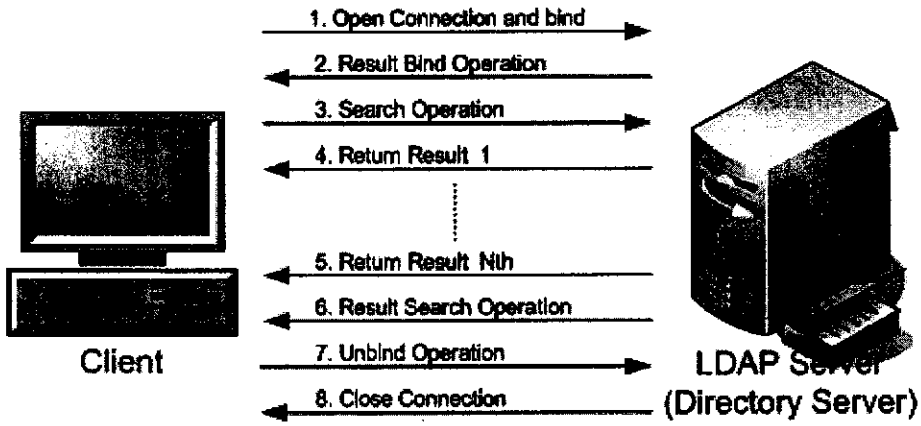
ตารางที่ 2.1 ตัวอย่างฟังก์ชันที่ใช้ติดต่อกับโปรโตคอล LDAP ด้วย PHP

Function	คำอธิบาย
ldap_connect()	ติดต่อกับไดเร็คทอรี่เซิร์ฟเวอร์
ldap_bind()	พิสูจน์ตัวตนและสิทธิ์กับไดเร็คทอรี่เซิร์ฟเวอร์
ldap_search()	ค้นหา Entry ในไดเร็คทอรี่
ldap_unbind()	ตัดSessionการติดต่อ
ldap_add()	สร้าง Entry ในไดเร็คทอรี่
ldap_delete()	ลบ Entry ในไดเร็คทอรี่
ldap_modify()	แก้ไขค่าของ Entry ในไดเร็คทอรี่ที่มีอยู่แล้ว
ldap_get_entries()	แสดงค่า Attribute ของ Entry

ขั้นตอนการทำงานของแต่ละคำสั่ง

- จะต้องเริ่มจากการติดต่อกับไดเร็คทอรี่เซิร์ฟเวอร์ ด้วยคำสั่ง ldap_connect()
- จากนั้นเมื่อติดต่อกับไดเร็คทอรี่เซิร์ฟเวอร์ ได้แล้วจะทำการพิสูจน์สิทธิ์กับไดเร็คทอรี่เซิร์ฟเวอร์โดยใช้คำสั่ง ldap_bind()

- ในส่วนนี้เมื่อมีการพิสูจน์สิทธิ์การเข้าถึงไดเร็คทอรี่เซิร์ฟเวอร์ว่าอยู่ระดับใดแล้วก็สามารถทำการค้นหา, แก้ไขเปลี่ยนแปลงข้อมูลในไดเร็คทอรี่เซิร์ฟเวอร์ได้ตามระดับสิทธิ์ที่ได้รับ โดยสามารถใช้คำสั่งที่ต้องใช้ข้อมูลของไดเร็คทอรี่เซิร์ฟเวอร์ได้เช่น ldap_search(), ldap_add(), ldap_delete(), ldap_modify(), ldap_get_entries()
- จากนั้นเมื่อมีการใช้งาน ไดเร็คทอรี่เซิร์ฟเวอร์เสร็จเรียบร้อยแล้วจะต้องทำการตัดการเชื่อมต่อกับไดเร็คทอรี่เซิร์ฟเวอร์ด้วยคำสั่ง ldap_unbind() ตามรูป 2.11



รูปที่ 2.11 ตัวอย่างขั้นตอนการทำงานของคำสั่ง Search

บทที่ 3
การออกแบบและพัฒนา

การออกแบบระบบการเข้าใช้บริการเครือข่ายไร้สาย ความปลอดภัยของระบบเป็นสิ่งที่สำคัญ ดังนั้นการที่จะอนุญาตให้บุคคลใดบุคคลหนึ่งสามารถเข้าสู่ระบบจึงเป็นสิ่งที่ควรระมัดระวัง การพิสูจน์ตัวตนจึงมีความสำคัญ เนื่องจากว่าการที่บุคคลใดบุคคลหนึ่งจะเข้าสู่ระบบได้ จะต้องได้รับการยอมรับว่าได้รับอนุญาตจริง การตรวจสอบหลักฐานจึงเป็นขั้นตอนแรกก่อนอนุญาตให้เข้าสู่ระบบ จากนั้นเมื่อมีการเข้าสู่ระบบได้แล้วควรมีการมอนิเตอร์บุคคลที่อยู่ในระบบได้ โดยสามารถป้องกันและควบคุมผู้เข้าใช้งานระบบได้อย่างใกล้ชิด

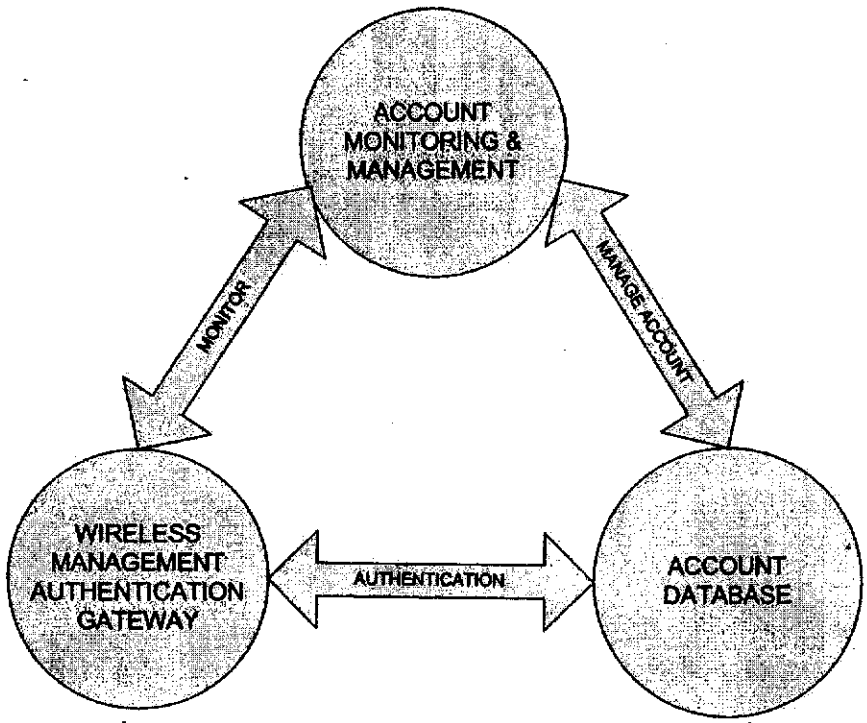
3.1 ส่วนประกอบของระบบ

เมื่อมีการติดตั้งระบบให้บริการเครือข่ายแลนไร้สายแล้ว จะสามารถตรวจสอบผู้ใช้งานได้โดยการตรวจเช็คชื่อผู้ใช้และรหัสผ่าน กับฐานข้อมูลส่วนกลางที่แยกออกมา และถ้าหากต้องการดูข้อมูลหรือตรวจสอบการใช้งาน ของผู้ที่กำลังใช้งานอยู่ หรือเพิ่ม-ลดข้อมูลผู้ใช้ ในฐานข้อมูลก็สามารถใช้งานได้ผ่านเว็บทำให้ไม่ต้องเสียเวลาในการเข้าไปเปลี่ยนแปลงค่าที่เครื่องแม่ข่ายเอง และสามารถตรวจสอบผู้ใช้งานในระบบจากที่ใดก็ได้ผ่านทางเว็บ ดังนั้นจึงได้มีการวางองค์ประกอบออกเป็น 3 ส่วนหลักๆดังรูปที่ 3.1 คือ

1. ส่วนจัดการเครือข่ายการเข้าใช้งานระบบ (Wireless Management Authentication Gateway) ทำหน้าที่เป็นด่านแรกเมื่อมีผู้ใช้จะเข้าสู่ระบบโดยจะจัดการในส่วนของการเชื่อมต่อไปพิสูจน์ตัวตนกับฐานข้อมูลที่เก็บข้อมูลผู้ใช้ของผู้ใช้งาน และเป็นเหมือนอินเตอร์เน็ตเกตเวย์ เพื่อให้ผู้ใช้ออกสู่อินเทอร์เน็ตได้ด้วย

2. ส่วนฐานข้อมูลเก็บข้อมูลของผู้ใช้งาน (Account Database) ทำหน้าที่เก็บข้อมูลรวมทั้งชื่อผู้ใช้และรหัสผ่านของผู้ใช้งานระบบ

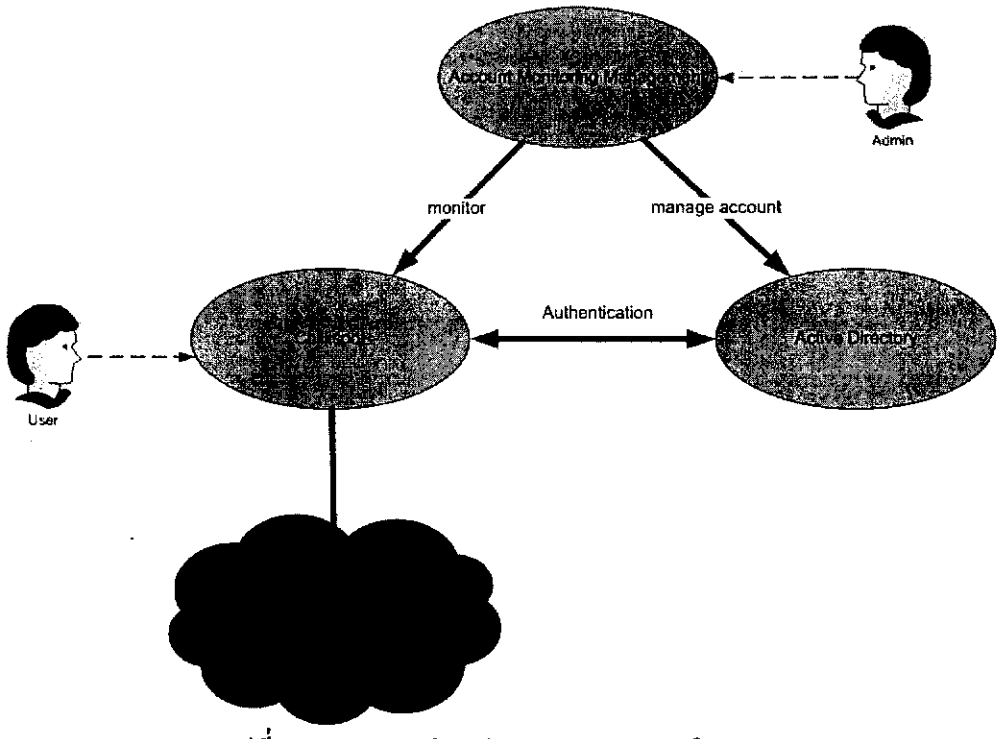
3. ส่วนมอนิเตอริง และควบคุม (Account Monitoring & Management) ทำหน้าที่คอยตรวจนับข้อมูลของผู้กำลังใช้งานระบบอยู่ และแสดงผลให้ผู้ดูแลระบบเพื่อให้สามารถควบคุมและบริหารจัดการข้อมูลผู้ใช้ได้



รูปที่ 3.1 ส่วนประกอบของระบบตามหน้าที่ของแต่ละส่วนที่ได้ออกแบบ

ส่วนประกอบทั้ง 3 ส่วนนี้จะติดต่อกันผ่านทางเครือข่าย โดยแต่ละส่วนจะตั้งอยู่ในส่วนใดส่วนหนึ่งของเครือข่ายก็ได้

เพื่อให้ระบบสามารถทำงานได้ตามหน้าที่ที่ได้ออกแบบไว้ดังนั้นจะต้องพัฒนาในแต่ละส่วน เพื่อให้สามารถทำงานได้จริงตามหน้าที่ของแต่ละส่วน โดยจะแทนแต่ละส่วนด้วย Chillispot, แอกทีฟไดเร็กทอรี (Windows 2003 Server) และ เว็บมอนิเตอร์และการจัดการแอ็คเคาท์



รูปที่ 3.2 การแทนส่วนประกอบของระบบโดยรวม

Chillispot

Chillispot เป็น Open Source ที่สามารถทำงานในส่วนจัดการเครือข่ายการเข้าใช้งานระบบ (Wireless Management Authentication Gateway) โดยใช้ระบบปฏิบัติการลีนุกส์ Fedora ที่รวมเอาระบบ Authentication Gateway รวมกับระบบ Radius และการแสดงผลบนเว็บ ระบบจัดการเครือข่ายการเข้าใช้โดยจะมีส่วนของ อินเทอร์เน็ตเกตเวย์, DHCPเซิร์ฟเวอร์, ไฟล์วอล, เว็บเซิร์ฟเวอร์

แอกทีฟไดเร็กทอรี (Windows Server 2003)

แอกทีฟไดเร็กทอรีเป็นบริการที่อยู่ในระบบปฏิบัติการ Microsoft Windows Server 2003 โดยทำหน้าที่เป็นฐานข้อมูลไว้เก็บข้อมูลของผู้ใช้บริการ เนื่องจากก่อนที่ผู้ใช้บริการจะเริ่มใช้งานจำเป็นต้องมีการล็อกอินด้วยชื่อผู้ใช้/รหัสผ่าน ที่กำหนดขึ้นที่กำหนดโดยผู้ดูแลระบบให้ผู้ใช้บริการ โดยข้อมูลของผู้ใช้งานแต่ละคนจะถูกเก็บไว้ที่ส่วนนี้ เพื่อให้เวลาล็อกอินระบบ Chillispot จะมาทำการตรวจสอบกับ ส่วนนี้ก่อนว่าจะอนุญาตให้ผู้ใช้ล็อกอินนั้นเข้ามาสู่ระบบได้หรือไม่

เว็บมอนิเตอร์และการจัดการแอ็คเคาท์

ส่วนนี้พัฒนาให้แสดงผลทางเว็บ เพื่อทำให้ผู้ดูแลระบบสามารถกำหนดชื่อผู้ใช้ และรหัสผ่านของผู้ใช้งาน ตรวจสอบการใช้งานแบบเรียลไทม์ ทำให้ทราบว่ามีผู้ใดใช้งานอินเตอร์เน็ตและชื่อผู้ใช้ไหนออนไลน์อยู่บ้าง ใช้แบนด์วิทไปเท่าใด โดยผ่านระบบทำรายการผ่านอินเตอร์เน็ต

จากที่ใดก็ได้ตลอดเวลาในรูปแบบเว็บ ในส่วนนี้เป็นส่วนที่ต้องทำการพัฒนาขึ้นมาเองสำหรับผู้ดูแลระบบใช้งาน

3.1.1 ส่วนจัดการเครือข่ายการเข้าใช้งานระบบ

ส่วนจัดการเครือข่ายการเข้าใช้งานระบบ (Wireless Management Authentication Gateway) จะต้องมีส่วนของอินเทอร์เน็ตเกตเวย์, DHCPเซิร์ฟเวอร์, ไฟล์วอล และส่วนของเว็บอินเทอร์เฟสที่ไว้ติดต่อกับผู้เข้าใช้เพื่อให้ผู้เข้าใช้ได้กรอก ชื่อผู้ใช้ และ รหัสผ่าน เพื่อยืนยันตัวตนก่อน เป็นอย่างน้อยเพื่อที่จะช่วยให้ผู้ใช้บริการ สามารถใช้อินเตอร์เน็ตได้รวดเร็ว รองรับการใช้งานอินเตอร์เน็ตจำนวนมากได้อย่างมีประสิทธิภาพ

ตัวโปรแกรมที่สามารถทำงานในลักษณะนี้ได้มีอยู่หลายตัวด้วยกัน โดยแต่ละตัวนั้นจะเป็น Software Open Source เช่น

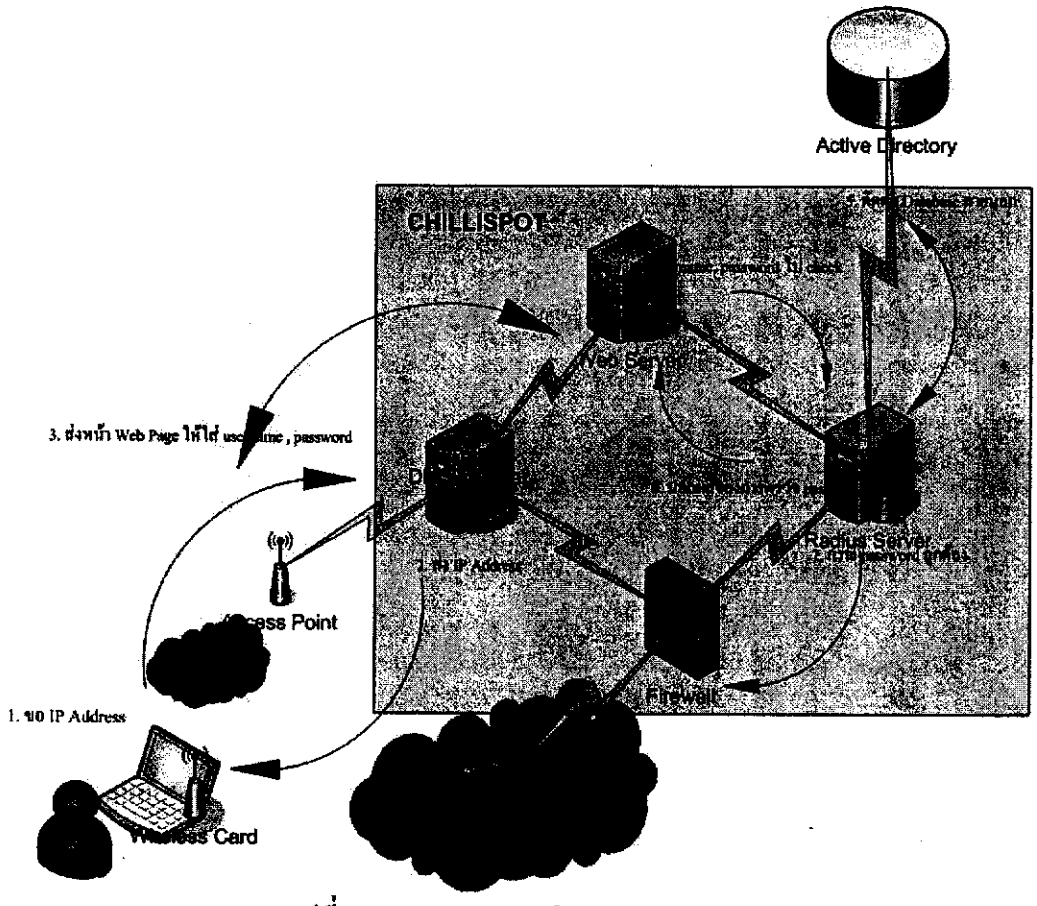
- Chillispot ตัวนี้เป็นตัวที่ได้รับความนิยมมากทำงานได้ทั้ง ลีนุกส์ และ FreeBSD
- Wifidog ตัวนี้จะเน้นการใช้งานบนอุปกรณ์ embedded
- NoCat ตัวนี้จะเน้นการใช้งานบน ลีนุกส์ มีลักษณะใกล้เคียงกับ Chillispot ที่นำมาใช้งาน
- Wicap ตัวนี้จะเน้นการใช้งานบน OpenBSD
- OpenSplash ตัวนี้จะเน้นการใช้งานบน FreeBSD โดยได้รับแรงบันดาลใจมาจาก Wicap แต่จะเน้นในเรื่องของความปลอดภัยมากว่า

สาเหตุที่เลือกใช้ Chillispot นั้น เนื่องมาจาก Chillispot มีการพัฒนาโปรแกรมของต้นเองอย่างสม่ำเสมอ โดยดูจากระยะเวลาที่ออก version ใหม่ๆ ซึ่งไม่นานมากนัก

การทำงานภายใน Chillispot

เมื่อมีผู้ใช้บริการเข้ามาติดต่อผ่านทาง Access point ซึ่งจะติดต่ออยู่กับ DHCPเซิร์ฟเวอร์ ไว้คอยแจกจ่าย ไอพี ให้แก่เครื่องของผู้ที่เข้ามาใช้บริการ โดย DHCPเซิร์ฟเวอร์ จะจ่ายไอพีให้แก่ผู้เข้ามาในระบบก่อนแม้ยังไม่ได้กรอก ชื่อผู้ใช้ และรหัสผ่าน เพื่อที่จะได้มีไอพีไว้เป็นตัวจัดการและจำกัดการออกสู่เครือข่ายอินเทอร์เน็ต โดยจะมีการใช้ ไฟล์วอล เพื่อจำกัดไอพีที่ยังไม่ได้มีการกรอกชื่อผู้ใช้ และรหัสผ่านที่ถูกต้องออกสู่เครือข่ายอินเทอร์เน็ตได้ ส่วนการตรวจสอบความถูกต้องของชื่อผู้ใช้และรหัสผ่านนั้น เมื่อผู้ที่จะใช้บริการได้ไอพีที่DHCPเซิร์ฟเวอร์ได้จ่ายให้ไปแล้ว เมื่อผู้ใช้บริการเปิดหน้าโปรแกรมเว็บบราวเซอร์ ระบบจะทำการเชื่อมต่อไปที่เว็บเซิร์ฟเวอร์เพื่อโหลดหน้าเว็บที่ไว้ให้กรอก ชื่อผู้ใช้และรหัสผ่าน จากนั้นเว็บเซิร์ฟเวอร์ก็จะส่งข้อมูลของชื่อผู้ใช้และรหัสผ่าน ของผู้ใช้บริการที่ได้กรอกไว้ไปตรวจสอบกับ Radiusเซิร์ฟเวอร์ เพื่อให้ Radiusเซิร์ฟเวอร์ได้ไปตรวจเช็คกับข้อมูลของผู้ใช้บริการที่เก็บอยู่ในฐานข้อมูลอีกทีหนึ่ง เมื่อผู้ใช้บริการมีการกรอก

ชื่อผู้ใช้และรหัสผ่านถูกต้อง Radiusเซิร์ฟเวอร์ก็จะติดต่อกับไฟล์วอลเพื่อให้ไฟล์วอล ได้เปิดการติดต่อสู่เครือข่ายอินเทอร์เน็ตให้ไอพี ดังกล่าว ตามรูปที่ 3.3



รูปที่ 3.3 การทำงานภายในของ Chillispot

Chillispot เป็น Open Source ที่ได้มีการรวมเอา DHCP เพื่อสามารถจ่าย ไอพี ให้ผู้ใช้งาน, Radiusเซิร์ฟเวอร์ เพื่อทำการตรวจสอบชื่อผู้ใช้และรหัสผ่านมีไฟล์วอลเพื่อปิดกั้นการเชื่อมต่อของผู้ไม่ได้ล็อกอิน และมีเว็บเซิร์ฟเวอร์ไว้เป็นหน้าเว็บในการกรอก ชื่อผู้ใช้และรหัสผ่าน โดย Chillispot จะควบคุมการทำงานของแต่ละเซิร์ฟเวอร์ เพื่อให้ทำงานได้ตามที่ได้ออกแบบไว้คือทำงานในส่วนพิสูจน์ตัวตนก่อนการเข้าใช้งานระบบ แต่ Chillispot นี้ยังไม่สามารถตอบสนองความต้องการของระบบทั้งหมด เนื่องจากมีความต้องการให้ผู้ดูแลระบบนั้นสามารถตรวจสอบการใช้งานของแต่ละข้อมูลผู้ใช้ ได้และสามารถจัดการการตั้งค่าของแต่ละข้อมูลผู้ใช้ได้ ดังนั้นจำเป็นต้องทราบข้อมูลเชิงสถิติว่ามีการใช้งานในระบบมากน้อยเพียงใด เมื่อเวลาเท่าไหร่ถึงเวลาเท่าไหร่ และมีการใช้งานมาจากเครื่องไหน เพื่อให้ผู้ดูแลระบบได้รับรู้ข้อมูลและจัดการกับข้อมูลผู้ใช้ ที่ผิดปกติได้ เช่น สามารถตัดการเชื่อมต่อของ ข้อมูลผู้ใช้ ในกรณีที่สงสัยว่ามีการใช้งานมากจนผิดปกติ และเนื่องจากภาควิชาได้เก็บข้อมูล ข้อมูลผู้ใช้ ของบุคลากรภายในภาควิชาไว้ที่ เครื่องเซิร์ฟเวอร์ ที่เป็นแอกทีฟไดเร็กทอรี

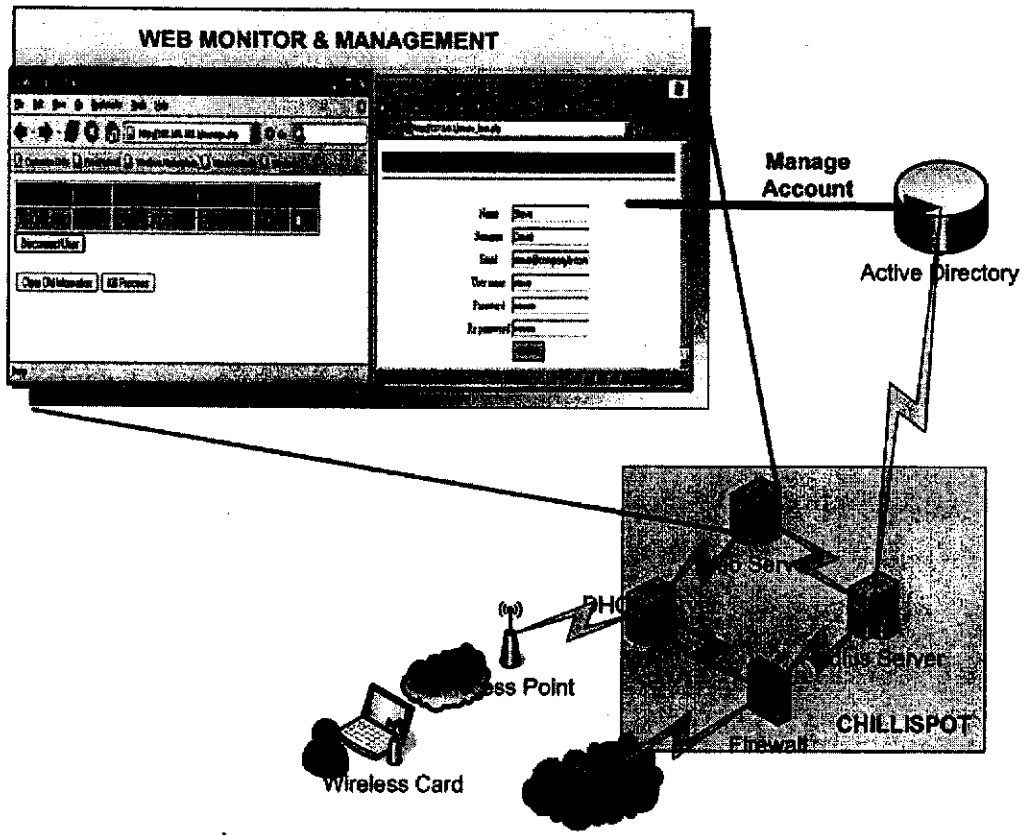
ซึ่งเป็น Windows 2003 ดังนั้นระบบจึงสามารถทำการตรวจสอบตัวตนของผู้ใช้ให้มาตรวจสอบกับเซิร์ฟเวอร์ของทางภาควิชาได้

3.1.2 ฐานข้อมูลเก็บข้อมูลของผู้ใช้งาน

สำหรับในส่วนนี้ เนื่องจากมีการเก็บข้อมูลของผู้ใช้งานไว้ที่แอกทีฟไดเร็กทอรีเซอวิสของ MS Windows Server 2003 อยู่แล้วเพราะฉะนั้นจึงต้องมีการตั้งค่าให้ Radius มาทำการตรวจสอบชื่อผู้ใช้และรหัสผ่านกับแอกทีฟไดเร็กทอรีก่อน นอกจากนี้ยังต้องสามารถจัดการข้อมูล ข้อมูลผู้ใช้ของผู้ใช้งานได้เช่น การเพิ่ม-ลบ ข้อมูลผู้ใช้ หรือการแก้ไขข้อมูลของผู้ใช้ โดยในส่วนนี้สามารถทำได้ผ่านทาง Windowsเซิร์ฟเวอร์ 2003 อยู่แล้ว แต่เพื่อความสะดวกของผู้ดูแลระบบจึงมีการพัฒนาเว็บให้สามารถจัดการ ข้อมูลผู้ใช้ ที่อยู่ในฐานข้อมูลแอกทีฟไดเร็กทอรี

3.1.3 ส่วนมอนิเตอริง และจัดการข้อมูลผู้ใช้

เพื่อให้เป็นการจัดการครบวงจร จึงต้องมีการสร้างส่วนที่เหลืออยู่ คือ ระบบการพิสูจน์ตัวตนกับแอกทีฟไดเร็กทอรีของ Window 2003 Server และระบบตรวจสอบจัดการการใช้งานของผู้ใช้บริการโดยทำรายการผ่านอินเตอร์เน็ตจากที่ใดก็ได้ตลอดเวลาผ่านการรายงานผลทางเว็บเพจ ตามรูปที่ 3.4 โดยจะแยกเป็น 2 ส่วนได้แก่ ส่วนมอนิเตอริง และส่วนจัดการข้อมูลผู้ใช้



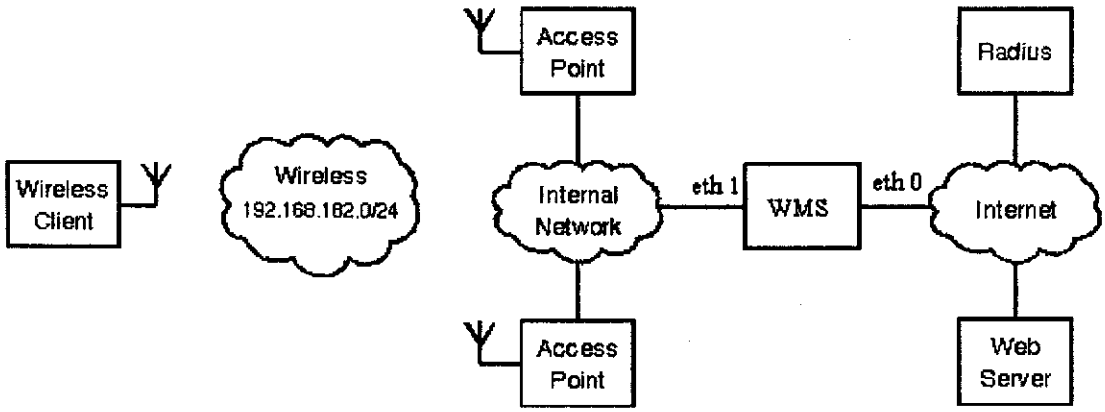
รูปที่ 3.4 แสดงส่วนของเว็บมอนิเตอริงและจัดการข้อมูลผู้ใช้

3.1.3.1 ส่วนมอนิเตอริง

การมอนิเตอริง เพื่อหาข้อมูลของผู้ใช้สามารถทำได้หลายวิธี เช่น ใช้ล็อกไฟล์ หรือใช้โปรแกรมประเภทเน็ตเวิร์คมอนิเตอริ่ง แต่ในโปรเจ็คนี้เลือกใช้เป็นโปรแกรมเน็ตเวิร์คมอนิเตอริ่ง เนื่องจาก การใช้ล็อกไฟล์เป็นการทำงานแบบออฟไลน์ คือต้องให้ผู้ใช้งานออกจากระบบไปก่อนจึงสามารถบอกผลออกมาได้ ในโปรเจ็คนี้จึงเลือกใช้โปรแกรมประเภทเน็ตเวิร์คมอนิเตอริ่ง คือ Darkstat เพื่อให้สามารถทำงานได้แบบออนไลน์ คือบอกได้ว่าผู้ใช้คนใดกำลังใช้งานมากน้อยเพียงใด โดยใช้โปรแกรมภาษาพีเอชพี (PHP) ไปดึงค่าการใช้งานของผู้ใช้จาก Darkstat เพื่อใช้ในการแสดงผลบนเว็บเพจ สาเหตุที่เลือกการแสดงผลบนเว็บเพจก็คือ ผู้ดูแลระบบสามารถตรวจดูการรายงานของเครื่องมอนิเตอริงจากที่ใดก็ได้

Darkstat

Darkstat เป็นโปรแกรมประเภท เน็ตเวิร์คมอนิเตอริ่ง โดยในโปรเจ็คนี้ได้ใช้โปรแกรมนี้ในการตรวจสอบการผ่านเข้าออกของข้อมูลที่อินเทอร์เฟส eth1 โดยค่าที่ได้นั้นคือ ไอพี แอดเดรส ที่มีการส่งข้อมูลมาที่อินเทอร์เฟสนี้ จำนวนไบต์ที่รับ, ส่ง, ผลรวมของ ไอพี แอดเดรส แต่ละอัน



รูปที่ 3.5 ตำแหน่งของ Darkstat ในระบบ

โดยค่าที่ได้นั้นจะนำมาใช้ในส่วนของ PHP ที่พัฒนาขึ้นมาเองเพราะโปรแกรมนี้ยังไม่สามารถให้ผลการทำงานเพียงพอต่อการใช้งานจริงจำเป็นต้องเพิ่มเติมอีกหลายๆส่วน

Radwho

Radwho เป็นโปรแกรมที่ใช้กับ FreeRADIUS โดยจะแสดงผู้ใช้ที่ยังคงใช้งานอยู่ รวมถึงวันเวลาที่ผู้ใช้ได้เริ่มเข้ามาใช้

```
Login    Name        What TTY When    From     Location
ste9ve   steve7       shell S0  Mon 15:53 127.0.0.1 192.168.182.2
```

โดยค่าต่างๆเหล่านี้จะถูกนำมาประยุกต์ใช้ในส่วนของ PHP ที่พัฒนาขึ้นมาเองอีกทีหนึ่ง

Radlast

Radlast เป็นโปรแกรมที่ใช้กับ FreeRADIUS โดยจะแสดงประวัติการเข้าใช้ของผู้ใช้แต่ละคน เช่น เวลาที่เข้ามาใช้ เวลาที่ออกจากการติดต่อ เวลารวม

```
steve   000:localhos 192.168.182.3   Tue Jan 17 17:13 - 18:30  (01:17)
steve   000:localhos 192.168.182.3   Tue Jan 17 17:11 - 17:12  (00:00)
asteve  000:localhos 192.168.182.3   Tue Jan 17 17:06 - 17:08  (00:02)
steve   000:localhos 192.168.182.3   Tue Jan 17 17:01 - 17:04  (00:03)
steve   001:localhos 192.168.182.3   Tue Jan 17 16:34   still logged in
steve   000:localhos 192.168.182.3   Wed Jan 11 18:29 - 18:30  (00:00)
steve   000:localhos 192.168.182.3   Wed Jan 11 18:23 - 18:29  (00:05)
steve   000:localhos 192.168.182.3   Wed Jan 11 18:15 - 18:20  (00:04)
steve   001:localhos 192.168.182.3   Wed Jan 11 18:10 - 18:11  (00:01)
steve   000:localhos 192.168.182.3   Wed Jan 11 17:27 - 18:04  (00:37)
steve   000:localhos 192.168.182.3   Wed Jan 11 17:07 - 17:24  (00:17)
steve   003:localhos 192.168.182.5   Wed Jan 11 16:50 - 18:04  (01:13)
steve   002:localhos 192.168.182.4   Wed Jan 11 16:45 - 17:13  (00:28)
steve   000:localhos 192.168.182.3   Wed Jan 11 15:31 - 17:04  (01:33)

radwtmp begins Wed Jan 11 15:30:43 2006
```

โดยค่าต่างๆเหล่านี้จะถูกนำมาประยุกต์ใช้ในส่วนของ PHP ที่พัฒนาขึ้นมาเองอีกทีหนึ่ง

การเขียนโปรแกรมส่วนมอนิเตอริง (Monitoring)

เนื่องจากระบบที่สมบูรณ์ ต้องนำหลายส่วนมาประกอบกัน โดยที่แต่ละส่วนยังมีความสามารถไม่ครบถ้วนตามความต้องการของระบบทั้งหมดเนื่องด้วยจากยังขาดส่วนของ มอนิเตอร์ผู้ใช้งาน และการจัดการผู้ใช้งาน ดังนั้นโครงงานนี้จึงพัฒนาส่วนจัดการต่างๆ และองค์ประกอบของระบบให้เชื่อมโยงกันทำงานให้เป็นระบบ

สำหรับขั้นตอนการเขียนโปรแกรมในส่วนของการตรวจสอบการใช้งานนั้น มีขั้นตอนดังนี้

- เมื่อผู้ดูแลระบบเข้ามาที่หน้าpageครั้งแรก
  1. เรียกโปรแกรม Darkstat ให้ทำงาน
  2. สร้างออบเจ็กของไอพีทุกๆอันที่มีได้ในsubnetที่ Chillispot เป็นคนจ่ายให้ และให้ค่าดีฟอลต่างๆเป็น 0 (ทำSESSION)

```
// variables
var $ipaddress; // store ip address of that user
var $username;  // store username of that user
var $inbyte;    // store receive bytes of that user
var $outbyte;   // store output bytes of that user
var $totalbyte; // store total bytes of that user
var $dateandtime;   // store date and time when that user LOGIN
var $show;      // flag indicate show output ,or not? TRUE = show , FALSE = not show
```

  3. เก็บค่าไอพี, IN, OUT, TOTALจากโปรแกรม Darkstat (เก็บไว้ในตัวแปร)
  4. เอาไอพี จากข้อ 3 มาตรวจสอบว่ามีใน radwho ว่ามีหรือไม่
     - ถ้ามี ให้ตั้งค่าของออบเจ็กที่สร้างในข้อ 2 (ทำSESSION)

1. ตั้งค่าตัวแปรshowเป็นTRUE
2. เก็บ ชื่อผู้ใช้, dateandtime (จากradwho) ใส่ตัวแปรที่มีชื่อเดียวกัน

- ถ้าไม่มี ให้ตั้งค่าของออบเจ็กที่สร้างในข้อ 2 (ทำSESSION)
  1. ตั้งค่าตัวแปรshowเป็นFALSE
  2. clearค่า ชื่อผู้ใช้, dateandtime
  3. เก็บค่าใส่ในตัวแปร inbyte, outbyte, totalbyte จาก IN, OUT, TOTAL ของข้อ 3

5. แสดงผล
   - หาไอพีที่showมีค่าเป็นTRUE
   - ค่า IN, OUT, TOTALที่แสดงออกไป = IN จากข้อ 3 – inbyte ที่เก็บในออบเจ็คที่สร้างในข้อ 2
   - แสดงผล

○ เมื่อมีการ reload หน้าจอในครั้งถัดมา (ตั้งไว้ให้reloadทุกๆ 15 วินาที)

1. เก็บค่าไอพี, IN, OUT, TOTALจากโปรแกรม Darkstat (เก็บไว้ในตัวแปร)
2. เอาไอพี จากข้อ 3 มาตรวจสอบว่ามีใน radwho ว่ามีหรือไม่
   - ถ้ามี ให้ตั้งค่าของออบเจ็กที่สร้างในข้อ 2 (ทำSESSION)
     3. ตั้งค่าตัวแปรshowเป็นTRUE
     4. เก็บ ชื่อผู้ใช้, dateandtime (จาก radwho)ใส่ตัวแปรที่มีชื่อเดียวกัน
   - ถ้าไม่มี ให้ตั้งค่าของออบเจ็กที่สร้างในข้อ 2 (ทำSESSION)
     1. ตั้งค่าตัวแปร show เป็น FALSE
     2. clear ค่า ชื่อผู้ใช้, dateandtime
     3. เก็บค่าใส่ในตัวแปร inbyte, outbyte, totalbyte จาก IN, OUT, TOTAL ของข้อ 3
3. แสดงผล
   - หาไอพี ที่ show มีค่าเป็น TRUE
   - ค่า IN, OUT, TOTALที่แสดงออกไป = INจากข้อ 3 – inbyte ที่เก็บในออบเจ็คที่สร้างในข้อ 2
   - แสดงผล

สำหรับการเขียนโปรแกรมในส่วนของการตัดการเชื่อมต่อนั้น จะใช้การส่ง Radius Disconnect – Request message ไปที่ Chillispot เพราะ Chillispot มีการสนับสนุนการทำงานในส่วนนี้อยู่

สำหรับการเขียนโปรแกรมในส่วนของการแสดงประวัติการใช้งานของผู้ใช้งานที่กำลังใช้งานอยู่นั้น จะใช้การกรองเอาเฉพาะชื่อผู้ใช้นั้นๆจากผลลัพธ์ของโปรแกรม radlast

3.1.3.2 ส่วนการจัดการข้อมูลของผู้ใช้งาน

ในส่วนนี้ต้องมีความสามารถที่ทำการเพิ่ม, ลบ, ค้นหา, แก้ไขข้อมูล ผู้ใช้งานได้ผ่านทางเว็บ เนื่องจากเราใช้ฐานข้อมูลที่เก็บ ข้อมูลผู้ใช้ของผู้ใช้งาน เป็นแอกทีฟไดเร็กทอรีเซอวิส ของ MS Windows Server 2003 การติดต่อกับแอกทีฟไดเร็กทอรีนั้นจะใช้การติดต่อผ่านทางโปรโตคอล LDAP ซึ่งมีความสามารถในการติดต่อได้อย่างรวดเร็วและเป็นมาตรฐานในการติดต่อกับแอกทีฟไดเร็กทอรี โดยการเขียนโปรแกรมในส่วนนี้ก็มีหลายภาษาที่สามารถติดต่อผ่านทาง LDAP ได้เช่น Perl, PHP, C Language, Java Language ในส่วนนี้จะเลือกใช้ภาษา PHP เพราะว่ามีฟังก์ชันการทำงานกับ LDAP และเราต้องการแสดงผลในรูปแบบเว็บ เพื่อสะดวกต่อการเข้าใช้งาน

การเขียนโปรแกรมส่วนจัดการข้อมูลของผู้ใช้งาน

การเขียนโปรแกรมภาษา PHP เชื่อมต่อกับ LDAPเซิร์ฟเวอร์ ตอนแรกต้องทดสอบก่อนว่าเซิร์ฟเวอร์ เราสามารถใช้ LDAP extension ได้ไหม วิธีทดสอบคือ สร้างแฟ้มสำหรับแสดงรายละเอียดของ php สมมุติชื่อ phpinfo.php

```
<?
   phpinfo();
?>
```

สร้างเสร็จแล้ว ก็เรียกใช้ ผ่าน Browser แล้วสังเกตหาตาราง LDAP Support enabled

ขั้นตอนการเขียนโปรแกรมภาษา PHP เชื่อมต่อกับ LDAPเซิร์ฟเวอร์ จะสามารถแบ่งได้ 3 ขั้นตอนคือ

1. ติดต่อกับ LDAPเซิร์ฟเวอร์

   ตอนแรกก็ติดต่อกับ LDAPเซิร์ฟเวอร์ ก่อนเช่น

   $ds=ldap_connect('localhost','389')

   ตรง localhost ให้เปลี่ยนเป็น ไอพี หรือชื่อเครื่องเซิร์ฟเวอร์ ถ้า LDAPเซิร์ฟเวอร์ เป็นเครื่องอื่น และพอร์ตปกติของ LDAP คือ 389 ส่วนนี้ไม่ต้องใสก็ได้ ก็เป็น

   ldap_connect('localhost')

หลังจากติดต่อได้แล้วก็ต้องแสดงว่าใครคือผู้ติดต่อโดยใช้คำสั่งนี้

```
$ldapbind = ldap_bind($ds, $binddn, $password);
```

ส่วนนี้เป็นการ ล็อกอิน หรือการตรวจสอบการล็อกอิน ก็ได้

2. การทำงานมี 4 อย่าง คือ การ เพิ่ม การ ลบ การแก้ไข และการค้นหา ผู้ใช้

2.1 การ เพิ่ม ผู้ใช้ ใช้คำสั่ง ldap_add ดังตัวอย่าง

```
$info["cn"]="Mr.Patt Emmawat";
$info["sn"]=Patt;
$info["ou"]="student";
$info["mail"]=s4145217@mor-or.pn.psu.ac.th";
$info["objectclass"][0]="top";
$info["objectclass"][1]="person";
$info["objectclass"][2]="inetOrgPerson";
$info["objectclass"][3]="organizationalPerson";
$info["objectclass"][4]="posixAccount";
$info["objectclass"][5]="shadowAccount";
$pwd=md5("s4145217");
$info["userAccount"] = $pwd[rand(0,31)]. $pwd[rand(0,31)]. $pwd[rand(0,31)].
                       $pwd[rand(0,31)]. $pwd[rand(0,31)]; // รหัสผ่าน ของ ผู้ใช้
$r=ldap_add($ds, "uid = s4145217, ou = student, dc = oasitzone, dc = pn", $info);
```

2.2 การค้นหา ต้องใช้ในการลบ และแก้ไขข้อมูลผู้ใช้

การ เพิ่ม การลบ การแก้ไขข้อมูลผู้ใช้ เวลาใช้ ldap_bind ต้องใช้ ผู้ใช้ พิเศษ ที่มีสิทธิ์ในการเขียน

ตัวอย่างการค้นหา

```
$sr = ldap_search($ds, "dc=oasitzone, dc=pn", "uid= " .$login. " ", $justthese);
$info = ldap_get_entries($ds, $sr);
print_r($info[0])
```

การค้นหาแบบนี้จะเป็นการดึงข้อมูลของ ผู้ใช้ ทั้งหมดมา ถ้าเราต้องการแบ่งบางส่วนให้แก้ไขดังนี้

```
$justthese = array ("dn","cn","uid");
```

```
$sr=ldap_search($ds, "dc=oasitzone,dc=pn", "uid=s4145217",$justthese);
$info1 = ldap_get_entries($ds, $sr);
print_r($info[0])
```

2.3 การลบผู้ใช้

```
$sr=ldap_search($ds, "dc=oasitzone,dc=pn", "uid=s4145217");
$info = ldap_get_entries($ds, $sr);
$r=ldap_delete($ds,$info1[0]["dn"]);
```

2.4 การแก้ไขผู้ใช้

```
$sr=ldap_search($ds, "dc=oasitzone,dc=pn", "uid="s4145217"");
$info1 = ldap_get_entries($ds, $sr);
$info["userPassword"]=$_POST['userpassword'];
ldap_modify($ds, $info1[0]["dn"], $info);
```

3. ยุติการเชื่อมต่อใช้ ldap_close($ds)

3.2 การติดต่อภายในระบบ

- โดยตัวเว็บมอนิเตอร์และการจัดการผู้ใช้ที่อยู่บนเว็บเซิร์ฟเวอร์จะประสานการทำงานทั้งกับตัว Chillispot และกับตัว Windows 2003 Server เพื่อให้สามารถตรวจสอบการทำงานและจัดการเกี่ยวกับผู้ใช้ได้
- โดยส่วนเซิร์ฟเวอร์ ของ Chillispot จะมีส่วนของการระบุปริมาณการใช้งานที่ออกไปสู่ภายนอก คือ Darkstat ซึ่ง เว็บอินเทอร์เฟสจะทำการดึงค่าเหล่านี้มาแสดงผลแบบเว็บ
- โดยเว็บสำหรับจัดการข้อมูลผู้ใช้ จะมีส่วนการติดต่อกับ window 2003 Server เพื่อที่จะใช้ในการเพิ่ม ลบ ข้อมูลของผู้ใช้ ผ่านทางโปรโตคอล LDAP

3.3 คุณสมบัติของซอฟต์แวร์

- ระบบสามารถบอกได้ว่าแต่ละ ข้อมูลผู้ใช้ เริ่มใช้ตั้งแต่เวลาใดจนถึงเวลาใด
- สามารถบอกได้ว่าแต่ละ ข้อมูลผู้ใช้ มีการดาวน์โหลดและอัพโหลดปริมาณเท่าใด

- 128-bit SSL (Secure Sockets Layer) เทคโนโลยี เข้ารหัส ที่มีความปลอดภัยสูงสุด ในการใช้งาน
- ระบบสามารถแบ่งให้มี Admin 2 Level สำหรับ ผู้ ดูแลระบบ (กำหนด รหัสผ่าน) และ สำหรับ ผู้ ดูข้อมูล สถิติการใช้งานทั่วไป สามารถดูสถิติการใช้งาน, แก้ไขเปลี่ยนแปลง ชื่อผู้ใช้ + รหัสผ่าน , ตรวจสอบ ผู้ใช้ที่ ออนไลน์ อยู่ (real-time) ผ่าน เว็บไซต์
- รองรับ อินเตอร์เน็ต ทุกระบบ (Lease Line , ADSL 2+, ISDN, Modem, IPStar)

ส่วนของ Internet Controlling Server (Authentication Server และ Gateway)

- ระบบควบคุมการใช้งานด้วย ชื่อผู้ใช้และรหัสผ่าน
- Auto reconnect + Password Memory เมื่อสายหลุด หรือปิดเครื่อง แล้วเปิดใหม่ ภายใน 10 นาที สามารถ Connected ได้เอง โดยไม่ต้อง พิมพ์ ชื่อผู้ใช้ + รหัสผ่านใหม่
- Auto Disconnected เมื่อปิดเครื่องโดยไม่ได้ ล็อกเอ้าท์หรือ ปิดหน้าต่างเวลาใช้งาน ระบบจะ disconnected อัตโนมัติ เมื่อครบ 10 นาที ทำให้ไม่มีปัญหา ชื่อผู้ใช้ค้าง ทำให้การบันทึกเวลาการใช้งานผิดพลาด
- ไม่มีปัญหาการ Blocked POP-UP สามารถทำงานได้ ปกติ แม้มีการ Blocked pop-up โดย Windows xp
- การบริหารจัดการระบบทำได้ด้วยการกำหนดด้วย เว็บทั้งหมด โดยที่ผู้ดูแลระบบสามารถกำหนดค่าของระบบในเครือข่าย (โลคอล) หรือจะกำหนดผ่านทุกจุดอื่น (รีโมท)
- สร้าง กลุ่มของผู้ใช้งาน ตามรูปแบบต่างๆ ที่ต้องการ
- สามารถกำหนดเวลาหมดอายุ (expiration since first logon) ของ ข้อมูลผู้ใช้ ได้
- ทำงานบนระบบปฏิบัติการลีนุกส์ไม่มีค่าลิขสิทธิ์

ส่วนของผู้ใช้งาน

- ผู้ใช้บริการต้องผ่านหน้า ล็อกอิน ชื่อผู้ใช้/รหัสผ่าน ล็อกอิน ก่อนทุกครั้ง ก่อนที่จะใช้งานอินเตอร์เน็ตทุกแอ็พพลิเคชั่น (WWW, POP3, SMTP,CHAT, VPN , Etc) กรณีเมื่อครบตามกำหนดเวลาที่กำหนด ระบบจะ Disconnect ผู้ใช้งานโดยอัตโนมัติ
- มี ข้อมูลผู้ใช้ เป็นของตนเอง โดยทาง ผู้ดูแลระบบ เป็นผู้สร้างชื่อผู้ใช้ และรหัสผ่าน ให้
- Auto reconnect + รหัสผ่าน Memory เมื่อสายหลุด หรือปิดเครื่องแล้วเปิดใหม่ ภายใน 10 นาที สามารถ Connected ได้เอง โดยไม่ต้องพิมพ์ชื่อผู้ใช้ + รหัสผ่าน ใหม่ทุกครั้ง
- Auto Disconnected เมื่อปิดเครื่องโดยไม่ได้ล็อกเอ้าท์จะ disconnected อัตโนมัติ เมื่อครบ 10 นาที

- รองรับผู้ใช้จากทุกระบบปฏิบัติการ เช่น Windows, ลีนุกส์ และ Mac. โดยไม่ต้องติดตั้งโปรแกรมใดๆ เพิ่มเติม

ส่วนของผู้ดูแลระบบ

- การทำงานของระบบตรวจสอบดูแลผู้ใช้งานในระบบสามารถทำงานผ่านเว็บบราวเซอร์ เพื่ออำนวยความสะดวกในการจัดการของผู้ดูแลระบบ
- สามารถเพิ่ม ข้อมูลผู้ใช้
- สามารถลบ ข้อมูลผู้ใช้
- สามารถปิด-เปิดการเชื่อมต่อของแต่ละผู้ใช้
- สามารถดูค่าข้อมูลเชิงสถิติ
- สามารถเฝ้าดูการทำงานของระบบและสังเกตสภาพการใช้งานที่ใช้ของระบบ
- ผู้ดูแลระบบสามารถตรวจสอบการใช้งาน จากระบบรายงาน แบบ เรียลไทม์

บทที่ 4

การทดลองและผลการทดลอง

4.1 เครื่องมือที่ใช้ในการพัฒนา

ฮาร์ดแวร์

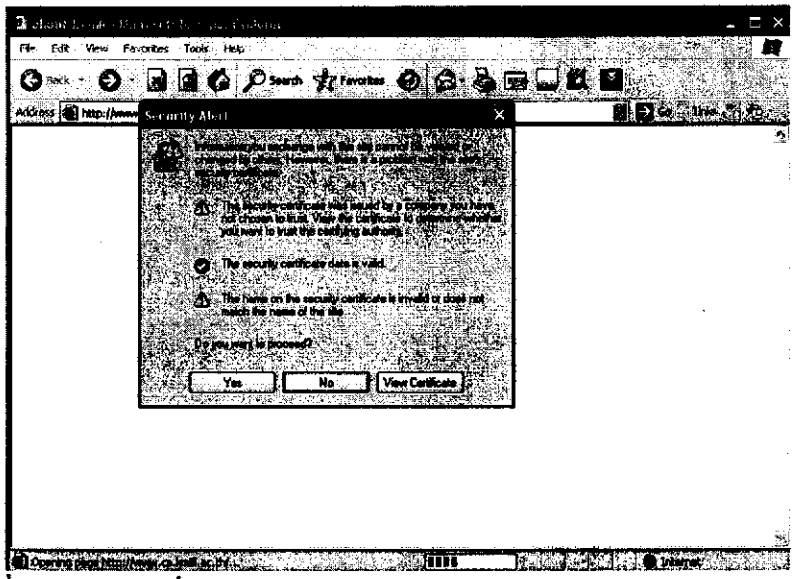
- เครื่องคอมพิวเตอร์ ซีพียู 2 กิกะเฮิรตซ์ 2 ชุด แต่ละชุดมีหน่วยความจำ 512 เมกะไบต์ และฮาร์ดดิสค์ความจุขนาด 60 กิกะไบต์ โดยทำหน้าที่เป็น เซิร์ฟเวอร์ของ Chillispot และ เซิร์ฟเวอร์ของแอกทีฟไดเร็กทอรี
- Wireless Access Point สำหรับการส่งข้อมูลแบบไร้สาย
- เครื่องคอมพิวเตอร์ ที่สามารถใช้ เครือข่ายแลนไร้สาย ได้ เพื่อใช้ทดลองการเข้าสู่ระบบ

ซอฟต์แวร์

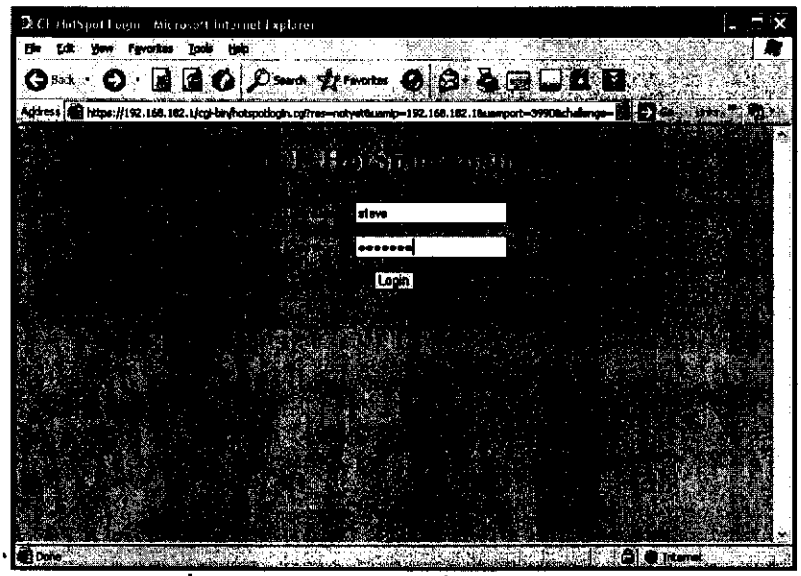
- ระบบปฏิบัติการ Linux Fedora Core 1
- ไดเรกทอรีเซิร์ฟเวอร์มาตรฐาน LDAP ใช้แอกทีฟไดเร็กทอรี ระบบปฏิบัติการ Microsoft Windows เซิร์ฟเวอร์ 2003
- PHP 4.2.2 ใช้แสดงผลการรายงานทางเว็บเพจ
- Chillispot โปรแกรมใช้ในส่วนจัดการเครือข่ายการเข้าใช้งานระบบ
- Darkstat โปรแกรมใช้ตรวจการใช้งานเครือข่าย
- FreeRadius โปรแกรมที่ใช้ตรวจสอบชื่อผู้ใช้, รหัสผ่าน

4.2 ผลการทดลองในส่วนของผู้ใช้

เมื่อผู้ใช้งานระบบต้องการใช้งานอินเทอร์เน็ต ผู้ใช้ต้องกรอกที่อยู่ที่ต้องการ ลงไปในช่อง Address ในกรณีที่ผู้ใช้งานระบบยังไม่ได้ทำการพิสูจน์ตัวตนกับทาง Wireless LAN Service Management System ทาง Wireless LAN Service Management Systemก็จะส่งหน้า page ที่ทำการแจ้งเตือนการติดต่อใช้งาน SSL ดังรูปที่ 4.1 เมื่อผู้ใช้ตกลงตามเงื่อนไขดังกล่าว เว็บบราวเซอร์ก็จะทำการ popup หน้า page ดังรูปที่ 4.2 เพื่อให้ใส่ ชื่อผู้ใช้ และ รหัสผ่าน

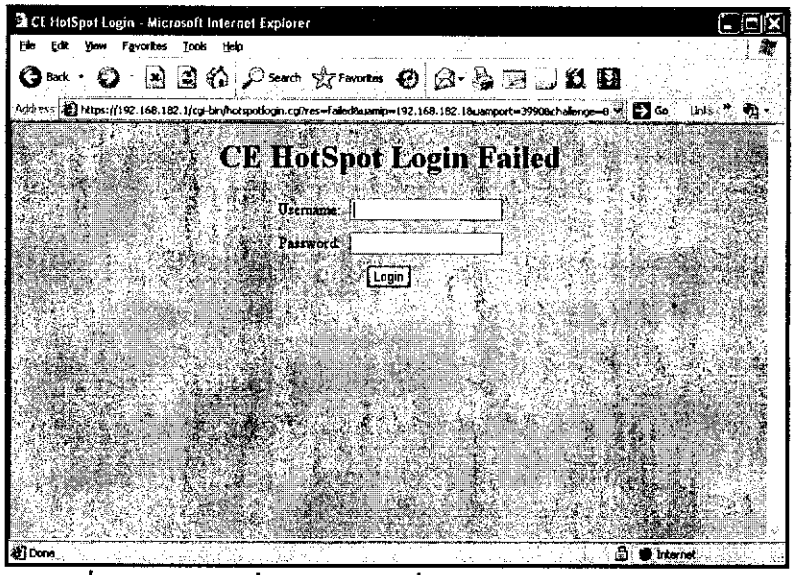


รูปที่ 4.1 หน้าเว็บเมื่อผู้ใช้ติดต่อกับAccess point แล้วต้องการเข้าสู่อินเทอร์เน็ต

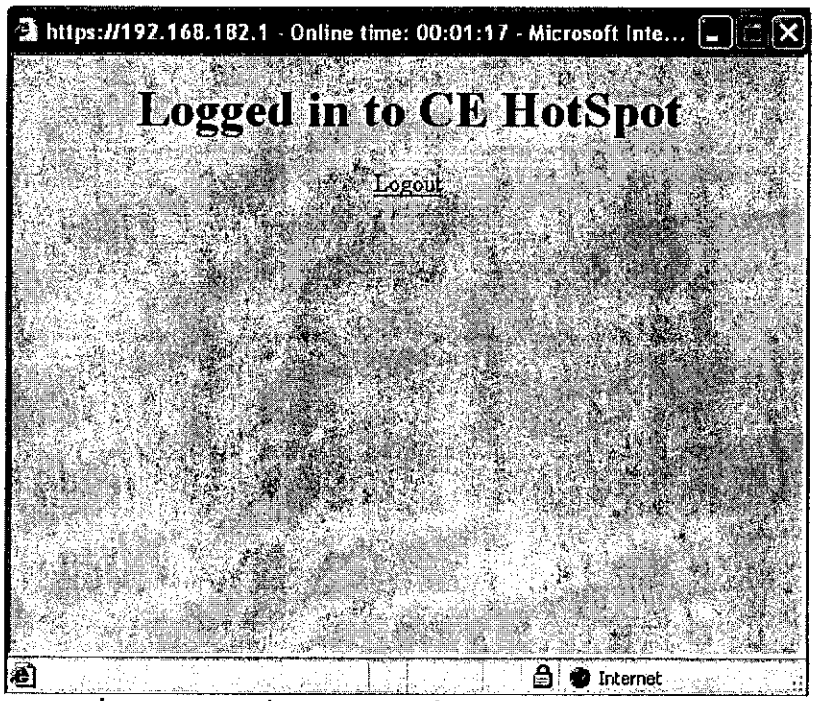


รูปที่ 4.2 หน้าเว็บให้กรอกชื่อผู้ใช้และรหัสผ่าน

กรณีที่ผู้ใช้กรอก ชื่อผู้ใช้ และ รหัสผ่าน ไม่ถูกต้อง จะมีผลลัพธ์ออกมาดังแสดงในรูป 4.3 เมื่อผู้ใช้กรอก ชื่อผู้ใช้ และ รหัสผ่าน ที่ถูกต้องและทำการพิสูจน์ตัวตนสำเร็จจะปรากฏดังรูปที่ 4.4 ทำให้ผู้ใช้ระบบสามารถใช้งานอินเทอร์เน็ตได้ดังรูปที่ 4.5 ซึ่งจะมีเวลาที่ใช้งานแสดงอยู่ด้วย

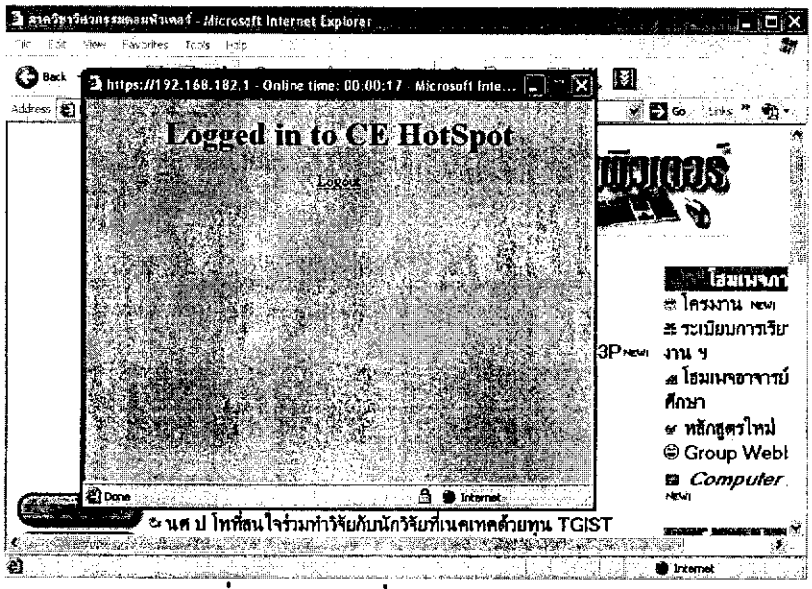


รูปที่ 4.3 หน้าเว็บเมื่อมีการกรอกชื่อผู้ใช้และรหัสผ่านไม่ถูกต้อง

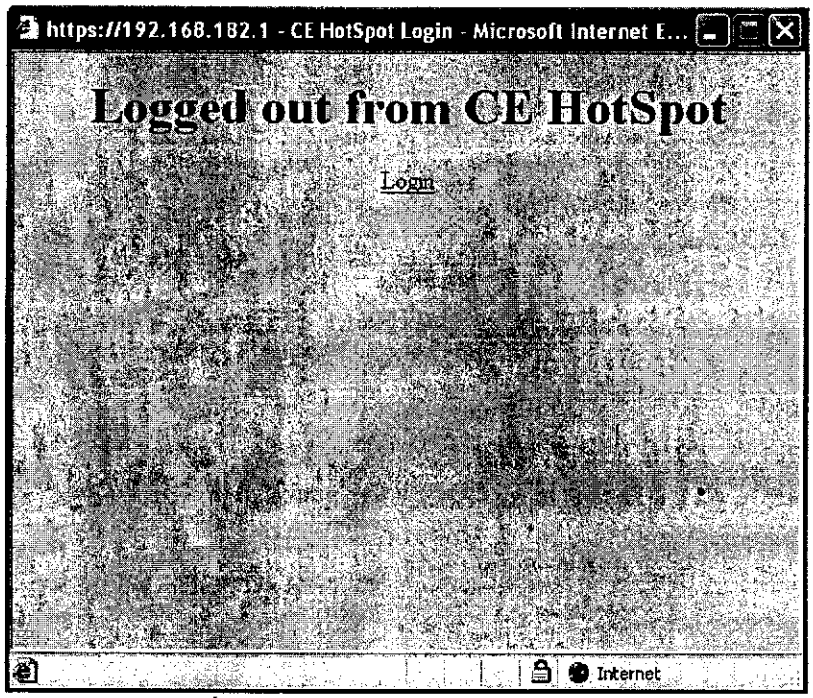


รูปที่ 4.4 หน้าเว็บเมื่อมีการกรอก ชื่อผู้ใช้ และ รหัสผ่าน ถูกต้อง

เมื่อผู้ใช้งานระบบต้องการออกจากระบบ ให้ผู้ใช้คลิกที่ล็อกเอาท์ที่ปรากฏดังรูปที่ 4.5 จะปรากฏหน้าจอที่บ่งบอกว่าได้ออกจากระบบเรียบร้อยแล้วดังรูปที่ 4.6 ซึ่งผู้ใช้ก็จะไม่สามารถต่อเข้าใช้งานระบบอินเทอร์เน็ตได้



รูปที่ 4.5 หน้าจอเมื่อเข้าสู่อินเทอร์เน็ตได้



รูปที่ 4.6 หน้าเว็บเมื่อล็อกเอาท์ออกสู่ระบบ

4.3 ผลการทดลองในส่วนผู้ดูแลระบบ

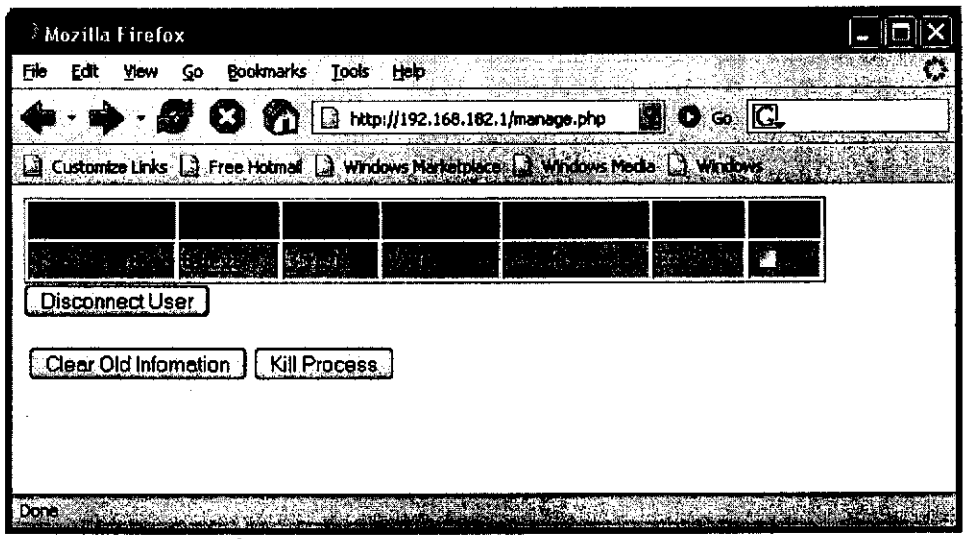
ในส่วนของผู้ดูแลระบบจะแบ่งออกเป็น 2 ส่วน ได้แก่ ส่วนมอนิเตอริง และส่วนจัดการแอ็คเคาท์

4.3.1 ส่วนมอนิเตอริง

การรายงานผลจะแสดงบนเว็บซึ่งแสดงตารางการเข้ามาในระบบ

ตารางประกอบไปด้วยฟิลด์ต่างๆ ดังนี้ คือ

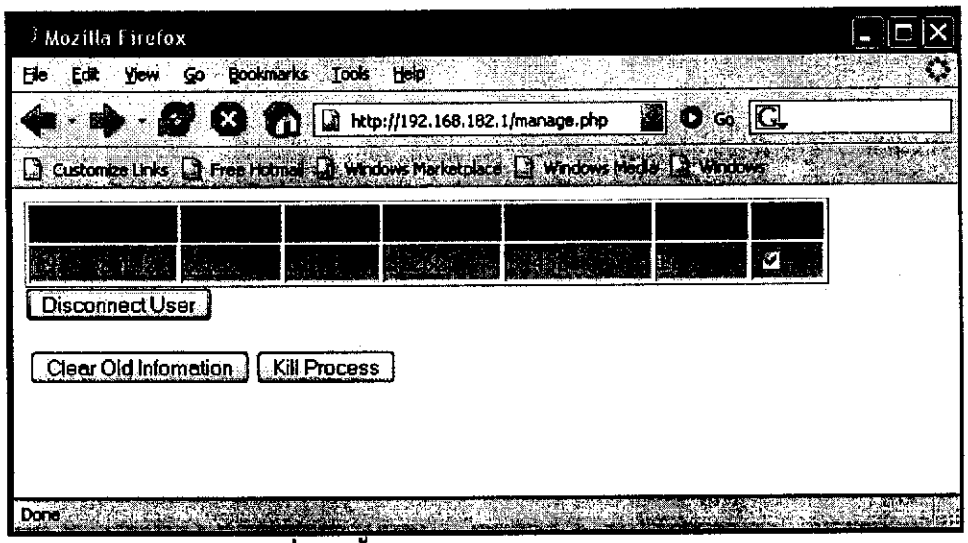
1. แสดงไอพีแอดเดรสของแอ็คเคาท์ที่ได้รับ
2. แสดงชื่อแอ็คเคาท์ที่ใช้ในการล็อกอิน
3. ปริมาณข้อมูลที่ผู้ใช้ขาเข้า
4. ปริมาณข้อมูลที่ผู้ใช้ขาออก
5. ปริมาณข้อมูลทั้งหมดที่ผู้ใช้รับ-ส่ง
6. แสดงเวลาที่ตรวจพบเมื่อมีการ ล็อกอิน เข้าสู่ระบบ
7. แสดงการเลือกแอ็คเคาท์ที่จะทำการตัดออกจากระบบ



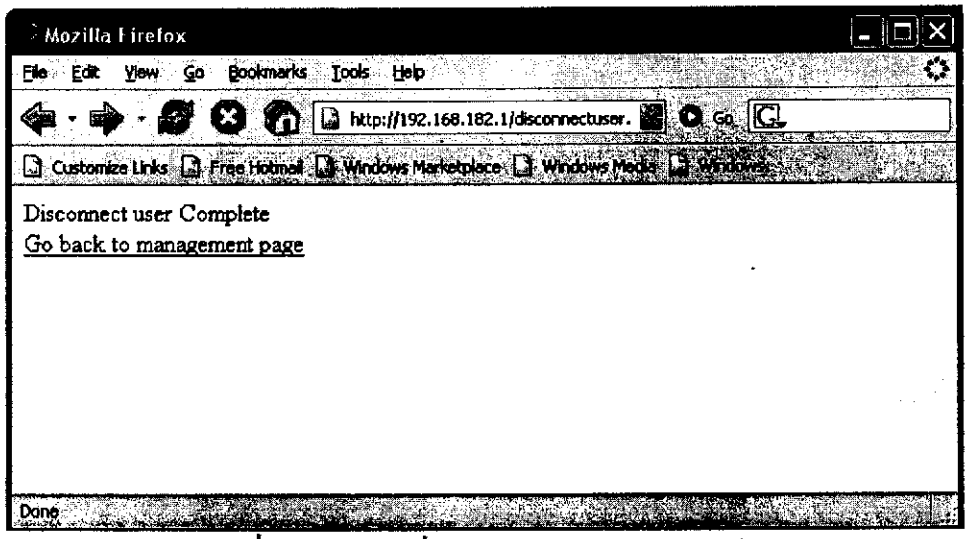
รูปที่ 4.7 เว็บแสดงตารางการเข้ามาในระบบของผู้ใช้

ถ้าผู้ดูแลระบบต้องการตัดแต่ละแอ็คเคาท์ออกจากระบบสามารถคลิก Check box ตรงคอลัมล็อกเอาท์ตรงแถวของชื่อแอ็คเคาท์ที่ต้องการตัดออกจากระบบ จากนั้นคลิกลิงค์ Disconnect User จะปรากฏหน้าเว็บเพจดังรูปที่ 4.8 และ 4.9 สำหรับปุ่ม Clear Old Information นั้น ใช้สำหรับลบค่าเดิมที่แสดงผลออกมา และเปลี่ยนแปลงข้อมูลภายในให้เป็นสถานะเริ่มต้น (ทำงานในลักษณะ

การ reset) ส่วนปุ่ม Kill Processมีไว้ใช้ก่อนที่จะปิดโปรแกรมและจบการทำงาน โดยปุ่มนี้จะทำการหยุดการทำงานของโปรเซสที่เกี่ยวกับการทำงานที่ php script ใช้งานอยู่

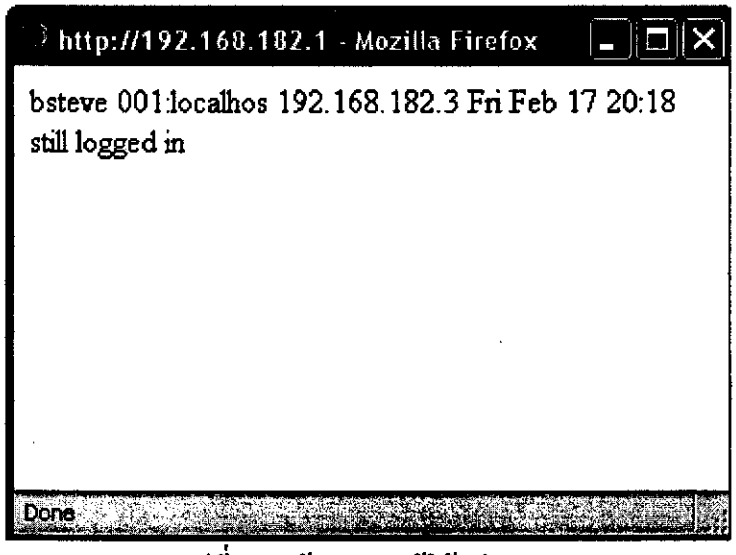


รูปที่ 4.8 ขั้นตอนการตัดผู้ใช้ออกจากระบบ



รูปที่ 4.9 หน้าเว็บเมื่อตัดผู้ใช้ออกจากระบบสำเร็จ

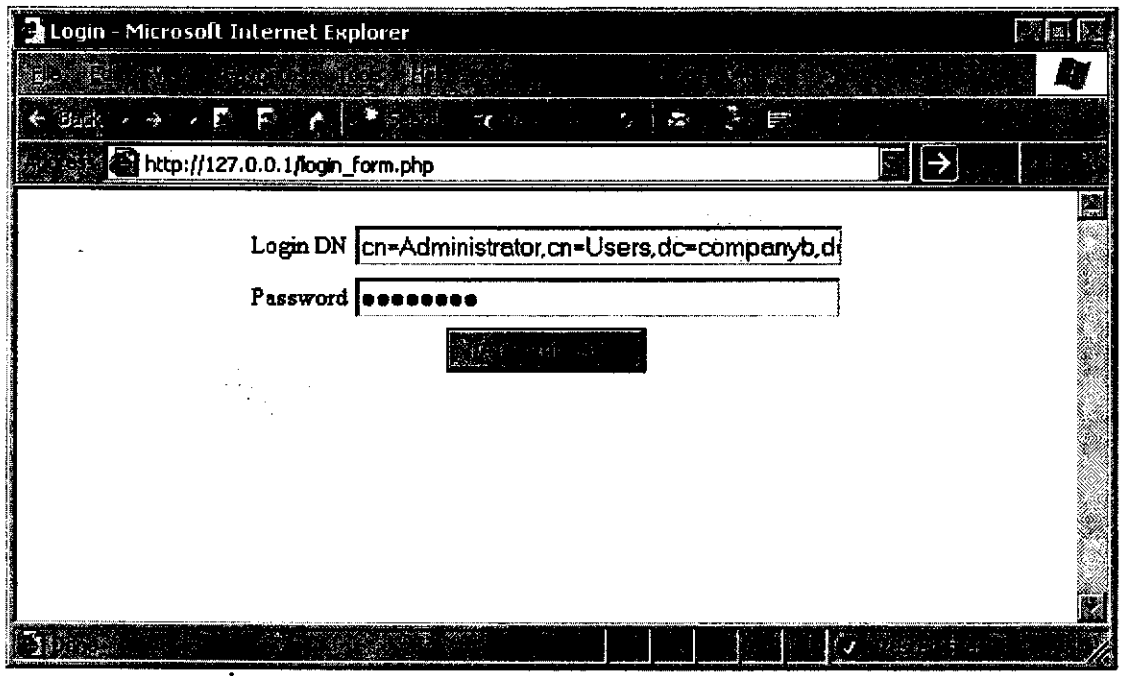
ถ้าผู้ดูแลระบบต้องการดูสถานะของแต่ละแอ็คเคาท์สามารถดูได้โดยคลิกลิงค์ชื่อของแอ็คเคาท์ จะปรากฏหน้าเว็บเพจดังภาพที่ 4.10



รูปที่ 4.10 ข้อมูลของผู้ใช้แต่ละคน

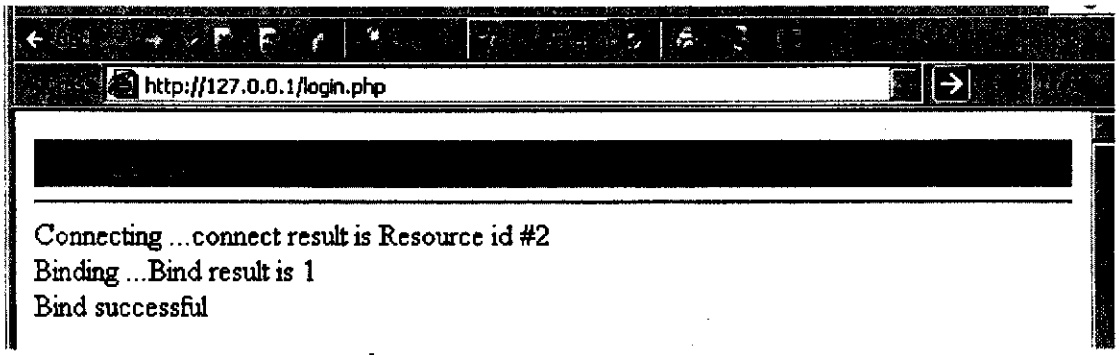
4.3.2 ส่วนจัดการข้อมูลผู้ใช้

การจัดการผู้ใช้ในแอกทีฟไดเร็กทอรีนั้น จำเป็นต้องใส่ Login DN และรหัสผ่านก่อนการเข้าใช้ ดังรูปที่ 4.11



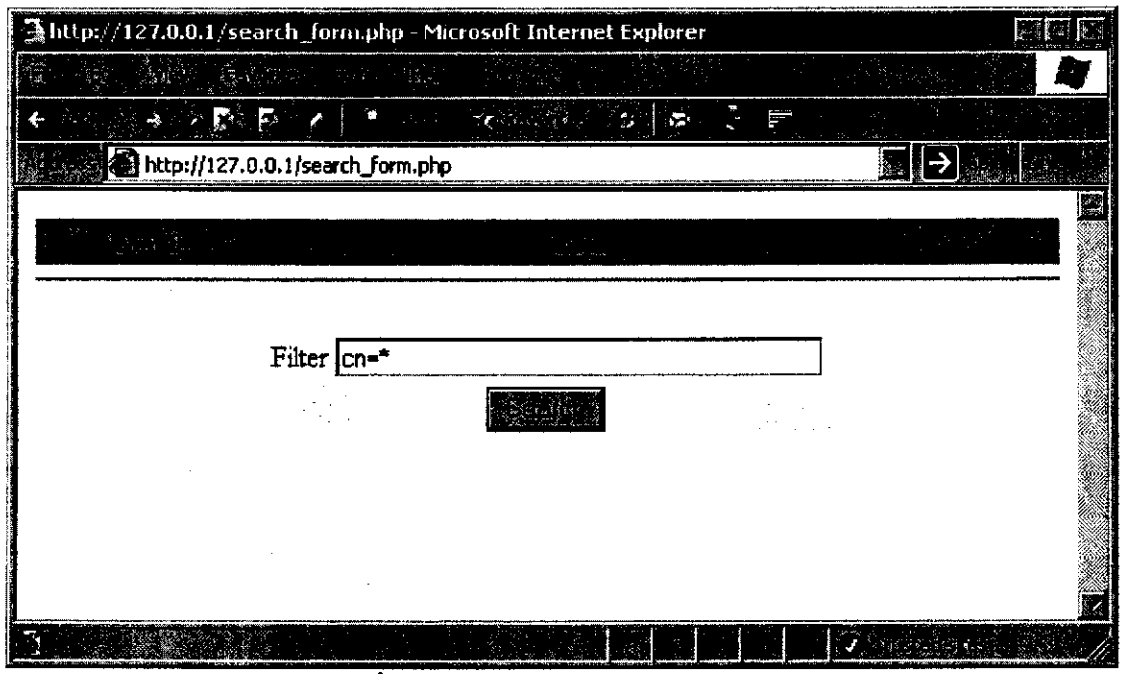
รูปที่ 4.11 รูปแบบการล็อกอินก่อนการเข้าใช้งานแอกทีฟไดเร็กทอรี

เมื่อ ล็อกอิน ได้สำเร็จ จะแสดงผลดังรูปที่ 4.12



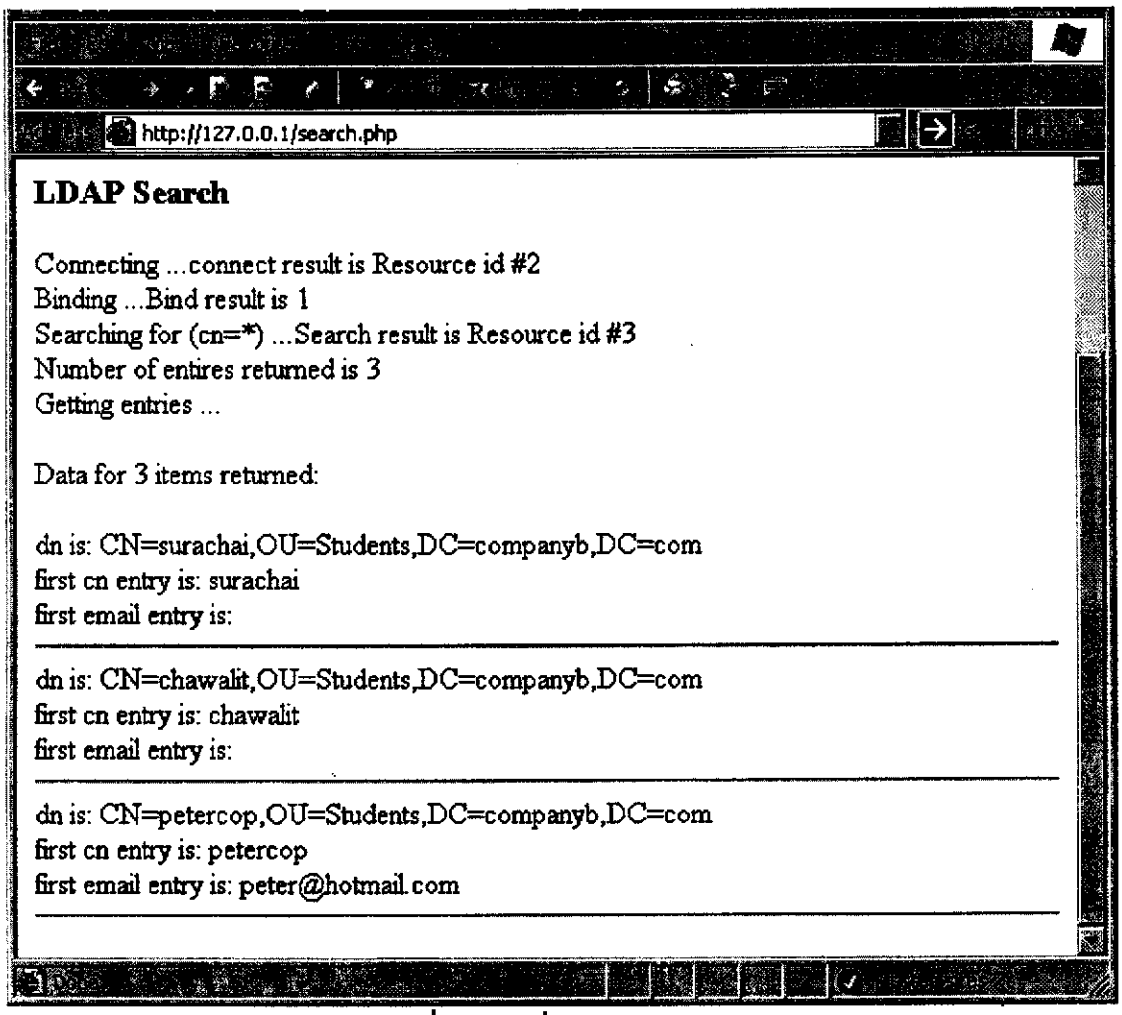
รูปที่ 4.12 รายละเอียดกรณีที่ล็อกอินสำเร็จ

ในกรณีที่ต้องการค้นหาข้อมูลของผู้ใช้ที่อยู่ในแอ็กทีฟไดเร็คทอรีจำเป็นต้องใส่ filter เข้าไปในช่องที่เตรียมไว้ดังรูปที่ 4.13 เพื่อให้ได้ข้อมูลของผู้ใช้ที่เราต้องการค้นหามากที่สุดโดยรูปแบบของฟิลเตอร์นั้น จะเป็นแอตทริบิวของผู้ใช้งานตามด้วยเครื่องหมาย = จากนั้นเป็นค่าที่เราต้องการค้นหาโดยอาจในเครื่องหมาย * หรือ ? ตามด้วยอักษรที่เราต้องการค้นหาได้



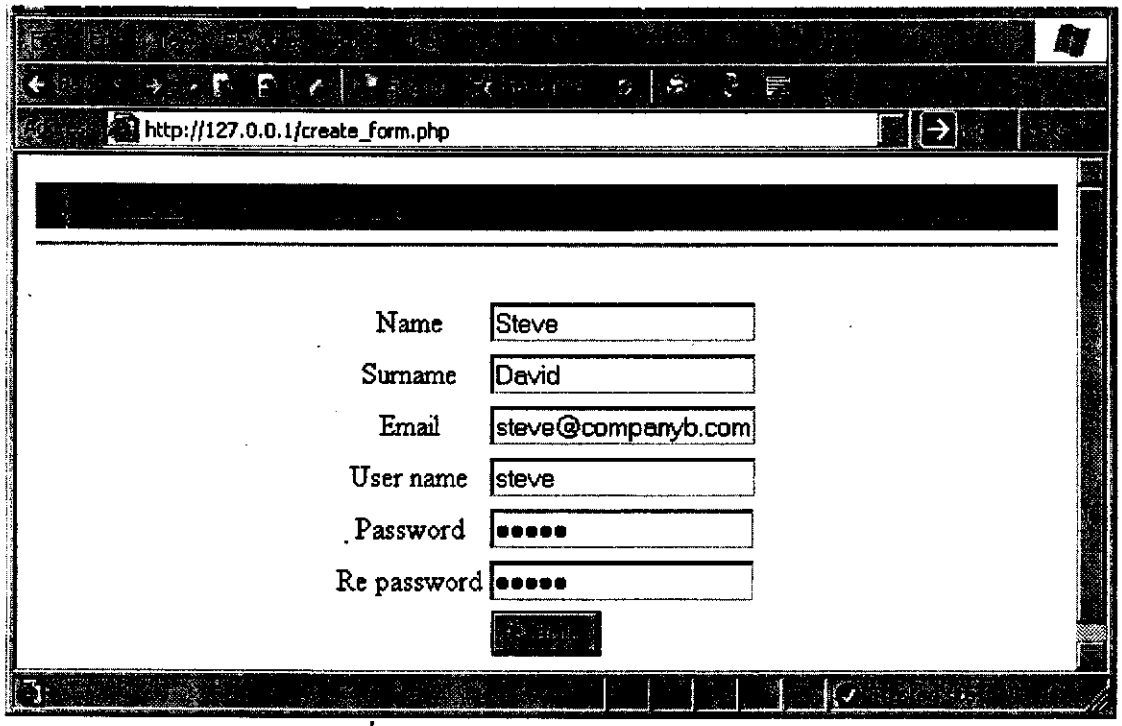
รูปที่ 4.13 วิธีการใส่ฟิลเตอร์ในการค้นหา

เมื่อค้นหาได้สำเร็จจะแสดงผลดังรูปที่ 4.14

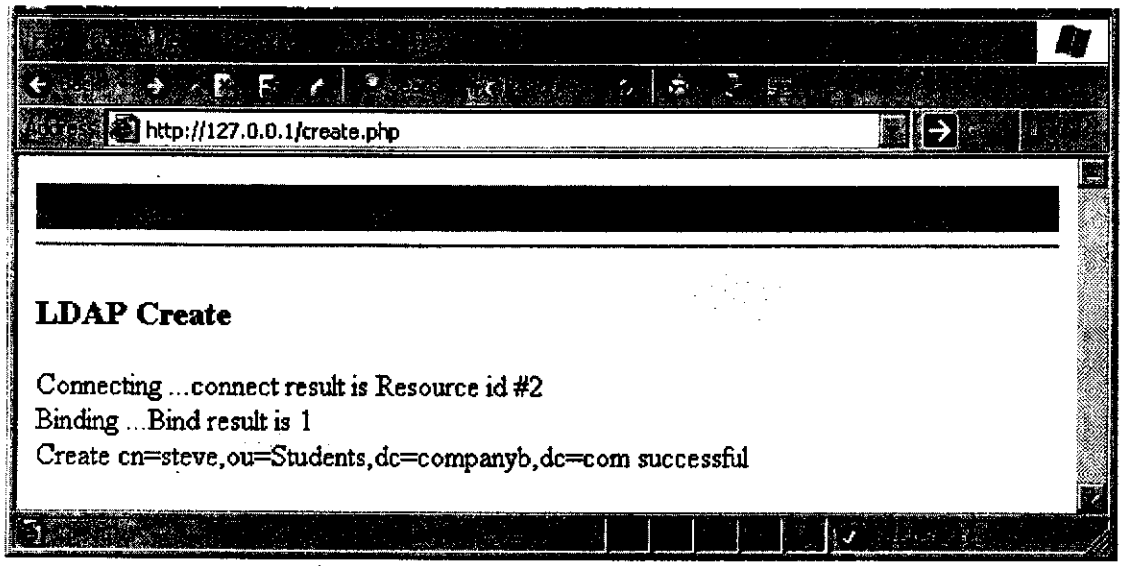


รูปที่ 4.14 ค่าที่ได้จากการค้นหา

กรณีที่ต้องการสร้างผู้ใช้คนใหม่ ให้เลือกที่ Create แล้วกรอกข้อมูลต่างๆของผู้ใช้เช่น ชื่อ, นามสกุล, อีเมลล์, ชื่อที่ใช้ล็อกอิน, และรหัสผ่าน ลงไปดังรูปที่ 4.15 ถ้าสามารถสร้างได้สำเร็จจะแสดงดังรูปที่ 4.16

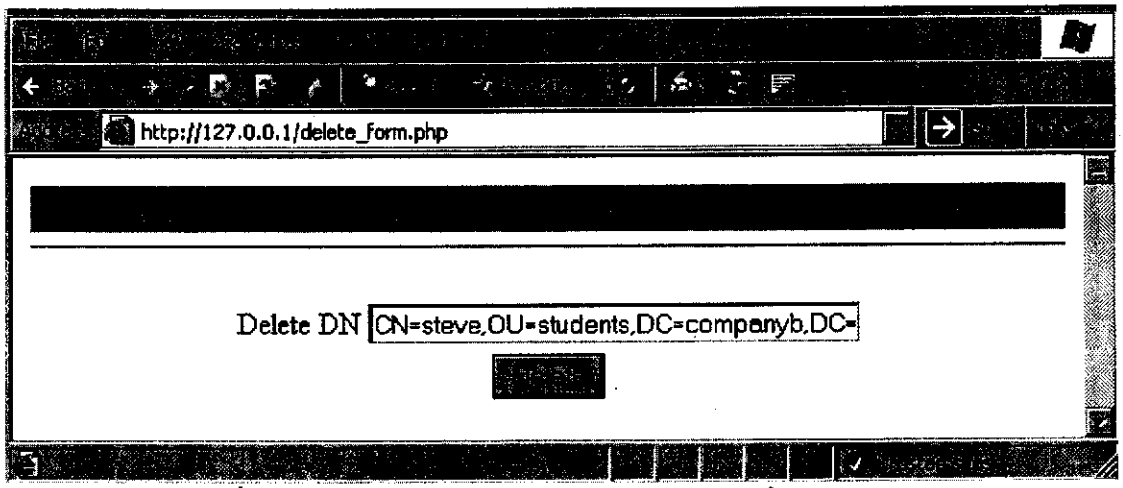


รูปที่ 4.15 การกรอกข้อมูลของผู้ใช้คนใหม่

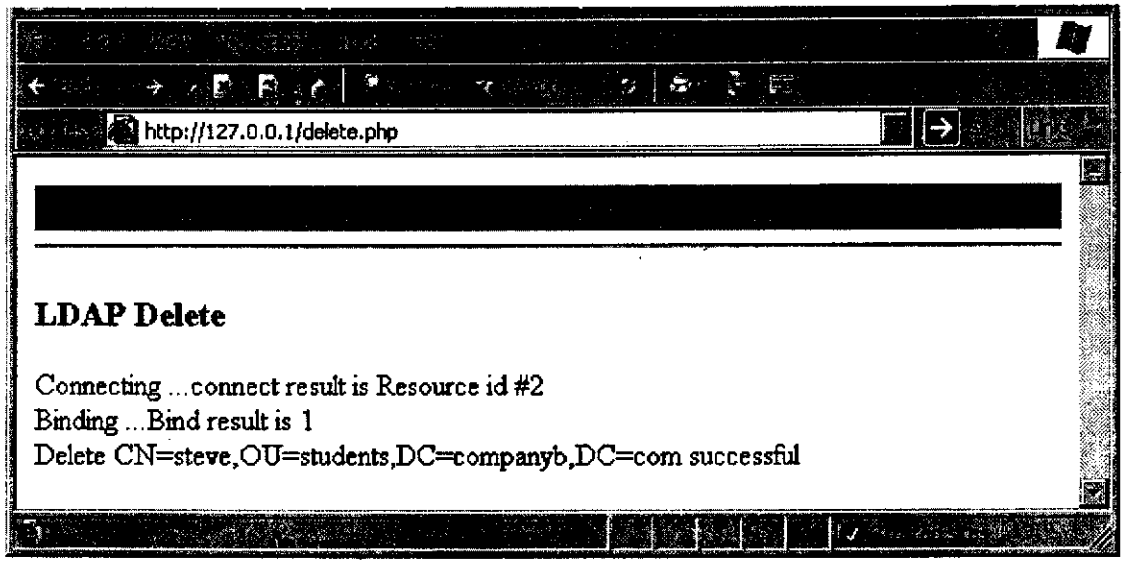


รูปที่ 4.16 รายละเอียดเมื่อสร้างผู้ใช้คนใหม่ได้สำเร็จ

กรณีที่ต้องการลบข้อมูลของผู้ใช้ ให้เลือกที่ Delete แล้วกรอกDelete DN ของผู้ที่จะลบลงไป ตามรูปที่ 4.17 เมื่อลบได้สำเร็จจะแสดงดังรูปที่ 4.18

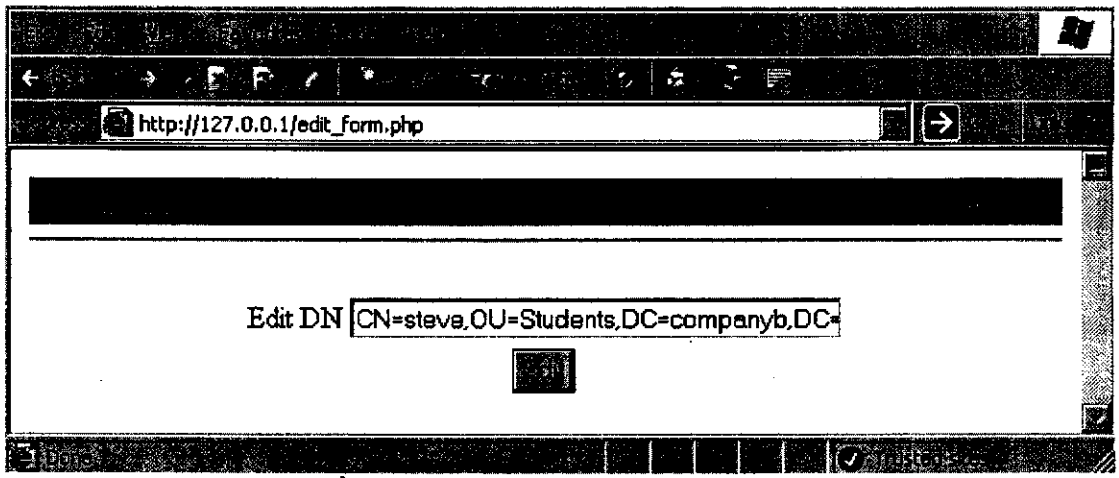


รูปที่ 4.17 รูปแบบการใส่รายละเอียดของแอ็คเคาท์ที่ต้องการจะลบ



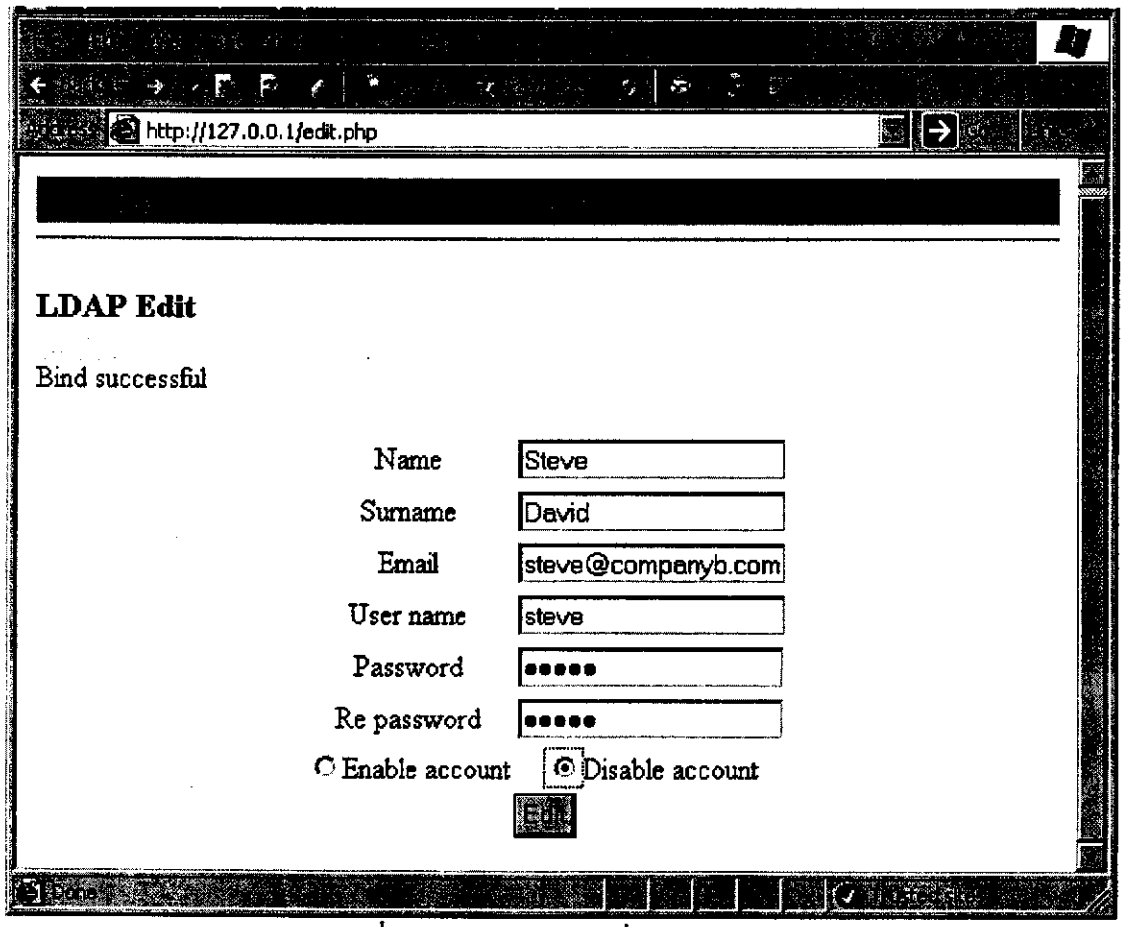
รูปที่ 4.18 รายละเอียดเมื่อลบได้สำเร็จ

กรณีที่ต้องการจะแก้ไขข้อมูลผู้ใช้ที่มีอยู่เดิม ให้เลือกที่ Edit แล้วกรอก Edit DN ลงไป ดัง รูปที่ 4.19

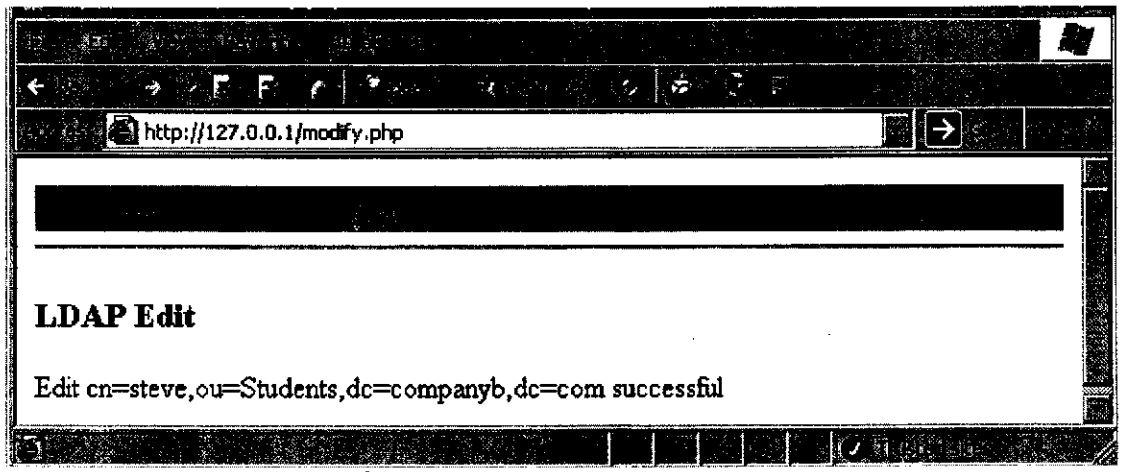


รูปที่ 4.19 รูปแบบการใส่ผู้ใช้ที่ต้องการจะแก้ไข

โปรแกรมจะแสดงข้อมูลของผู้ใช้ท่านนั้นออกมาดังรูปที่ 4.20 จากนั้นสามารถแก้ไขข้อมูลของผู้ใช้งานได้โดยสามารถที่จะระงับการใช้ของผู้ใช้ท่านนั้นได้ชั่วคราวโดยการเลือกที่ Disable Account เมื่อแก้ไขสำเร็จจะแสดงข้อมูลออกมาดังรูปที่ 4.21



รูปที่ 4.20 ข้อมูลของผู้ใช้ที่ต้องการแก้ไข



รูปที่ 4.21 รายละเอียดเมื่อแก้ไขข้อมูลสำเร็จ

บทที่ 5
วิจารณ์และสรุป

5.1 บทสรุป

ระบบ Wireless LAN Service Management System สร้างขึ้นมาเพื่อแก้ไขปัญหาเรื่องความไม่ปลอดภัยต่อการใช้งาน WLAN และต้องการให้ผู้ดูแลระบบสามารถจัดการข้อมูลของผู้ใช้ได้อย่างใกล้ชิด โดยมีการแสดงผลเป็นเว็บเพจเพื่อให้สามารถดูการใช้งานของผู้ใช้แต่ละคนได้อย่างต่อเนื่อง เพื่อให้สามารถแก้ไขปัญหาได้อย่างทันท่วงที

5.2 วิจารณ์สิ่งที่ได้จากโครงงาน

โครงงานนี้เป็นการพัฒนาโปรแกรมโดยใช้วิธีการเชื่อมโยงกับโปรแกรมย่อยๆ ภายนอกอีกหลายๆส่วน ทำให้สามารถทำการพัฒนาโปรแกรมที่มีองค์ประกอบย่อยๆได้รวดเร็วขึ้น แต่การพัฒนาโปรแกรมในรูปแบบนี้ก็มีปัญหาตามมาเช่นกัน คือในกรณีที่โปรแกรมภายนอกนั้นทำงานบกพร่องหรือได้รับความเสียหาย ก็จะทำให้โปรแกรมที่พัฒนาขึ้นมานี้เกิดความเสียหายตามไปด้วย

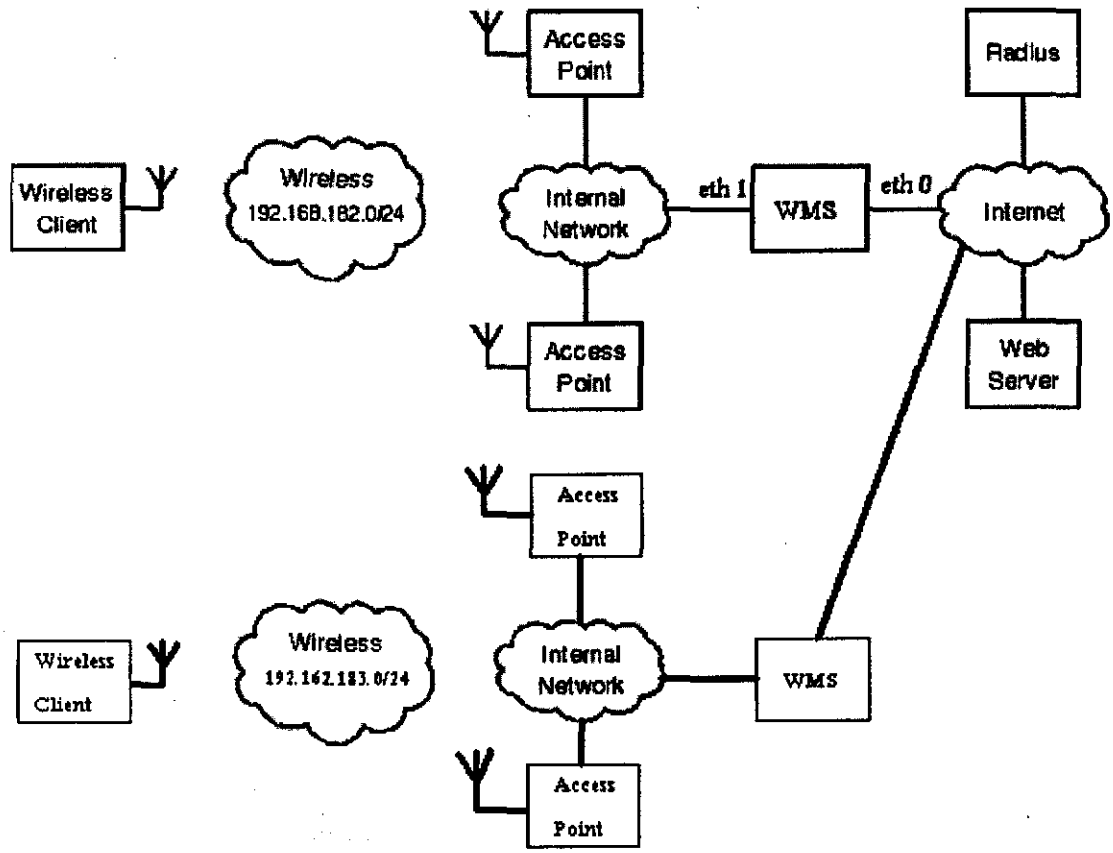
5.3 ปัญหาอุปสรรคและแนวทางในการแก้ไข

5.3.1 ปัญหาที่เกิดขึ้น

- ปัญหาข้อที่หนึ่ง ถ้ามีผู้ใช้เปิดเครื่องแต่ไม่ได้ทำการ Authenticate กับ Chillispot จะทำให้สิ้นเปลือง IP Address เพราะแม้ไม่ได้ Authenticate แต่ Chillispot ก็ยังแจก IP Address ให้
- ปัญหาข้อที่สอง กรณีที่ผู้ใช้ตัดการเชื่อมต่อออกไป และมีผู้ใช้คนใหม่เข้ามาใช้งานโดยได้ IP Address เดียวกับผู้ใช้ที่ตัดการเชื่อมต่อไปก่อนหน้า ค่าปริมาณการใช้งานที่แสดงออกมาที่หน้าการmanageจะเป็นค่าที่ต่อจากค่าเดิม
- ปัญหาข้อที่สาม กรณีที่มีผู้ใช้งานเป็นจำนวนมาก อาจส่งผลต่อโปรแกรม Darkstat ได้ เพราะ Darkstat ใช้เทคนิคการของ Packet Sniffer แล้วค่อยวิเคราะห์ Packet ดังกล่าว ดังนั้นถ้ามีผู้ใช้งานเป็นจำนวนมากแล้ว ก็ต้องใช้การประมวลผลที่มากตามไปด้วย
- ปัญหาข้อที่สี่ ในส่วนของโปรแกรม PHP ติดต่อ Active Directory นั้น ผู้ใช้จำเป็นต้องมีความรู้เกี่ยวกับ Active Directory อยู่บ้าง

5.3.2 แนวทางการแก้ไขปัญหา

- สำหรับปัญหาในข้อหนึ่งและข้อสามนั้น อาจต้องขยายระบบให้ใหญ่ขึ้นโดยเพิ่มตัว Wireless Management System ตัวอื่นเข้าไป แล้วให้ Chillispot ของแต่ละระบบจ่าย IP คนละส่วนกัน ทำให้มี Darkstat คนละตัวทำให้แบ่งกัน Sniff Packet เป็นเหตุให้ลดการประมวลผลลงได้



รูปที่ 5.1 การขยายระบบให้ใหญ่ขึ้น

- ในส่วนของปัญหาข้อที่สองนั้น ได้ใช้ Javascript มาตั้งเวลาให้ Reload หน้า Manage โดยอัตโนมัติ ซึ่งสามารถลดปัญหาดังกล่าวได้

5.4 แนวทางการพัฒนาต่อ

- สามารถเพิ่มส่วนมอนิเตอร์ผู้ใช้ให้สามารถตรวจสอบการใช้งานของผู้ใช้งานแต่ละคนได้เพิ่มขึ้น เช่น การตรวจสอบว่าผู้ใช้แต่ละคนนั้นใช้ โปรโตคอลอะไรในปริมาณเท่าไหร่ และสามารถเก็บสถิติการเข้าใช้งานของผู้ใช้งานแต่ละคนเพื่อคำนวณออกมาในรูปแบบกราฟได้

บรรณานุกรม

[1] Georgia Institute Of Technology Local Area Walkup/Wireless Network "LAWN::LAWN System Diagram".Available

[2] Georgia Institute Of Technology Local Area Walkup/Wireless Network "LAWN::Windows XP SP2 Example".Available :http://www.lawn.gatech.edu/acess/configuration_examples/windowsxpsp2.html

[3] Chillispot. "Features".Available: http://www.chillispot.org/features.html

[4] Chillispot. "Release Notes".Available:http://www.chillispot.org/release.html

[5] Chillispot. "FAQ".Available: http://www.chillispot.org/FAQ.html

[6] Chillispot. "man chilli".Available: http://www.chillispot.org/chilli.html

[7] Radius authentication using LDAP. "LADP Implementation HOWTO".Available: http://www.tldp.org/HOWTO/LDAP-Implementation-HOWTO/

[8] Freeradius. "Usage".Available: http://www.freeradius.org/usage.html

[9] Darkstat. "Download". Available: http://dmr.ath.cx/net/darkstat/

[10] Darkstat. "Documentation". Available :http://www.linuxfocus.org/English/September2004/article346.shtml

[11] Libpcap. "Documentation". Available: http://www.tcpdump.org/

[12] PHP. "Documentation". Available: http://www.php.net/docs.php

[13] คาเนียล บลัม; [แปล] 2543 วุฒิพงศ์ พงศ์สุวรรณ, ศาวิณี พิชยไพศาล, พิรนุช สุขปัญญา "เจาะลึก Active directory services" สำนักพิมพ์ซอฟต์แวร์ ปาร์ค พระนครศรีอยุธยา

[14] ชัยนันท์ กมลวดี 2546 "เจาะลึก เพิ่มพลังเครือข่ายเต็มพิกัดด้วย Directory services" สำนักพิมพ์เอส.พี.ซี. บุ๊คส์ กรุงเทพฯ

[15] บัณฑิต จามรภูติ 2548 "คู่มือ Windows Server 2003 ภาคปฏิบัติ เล่ม 1" สำนักพิมพ์ Bandhit เชียงใหม่