การออกแบบและพัฒนาต้นแบบ
ระบบอินเทอร์เนตเกตเวย์ราคาถูกสำหรับมหาวิทยาลัย

ประยูร ไชยบุตร

มหาวิทยาลัยราชภัฏเพชรบูรณ์ 2553

หัวข้อวิจัย การออกแบบและพัฒนาต้นแบบระบบอินเทอร์เนตเกตเวย์ราคาถูกสำหรับมหาวิทยาลัย

ชื่อผู้วิจัย ประยูร ไชยบุตร และคณะ

สาขาวิชา วิทยาการคอมพิวเตอร์

คณะ วิทยาศาสตร์และเทคโนโลยี

สถาบัน มหาวิทยาลัยราชภัฏเพชรบูรณ์

ปีการศึกษา 2553

บทคัดย่อ

งานการวิจัยฉบับนี้มีจุดประสงค์คือต้องการสร้างระบบมาเพื่อเก็บข้อมูลผู้ใช้งานในอินเทอร์เนตตามข้อบังคับของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในส่วนของผู้ให้บริการอินเทอร์เน็ตในการวิจัยนี้จึงได้ออกแบบสอบถามการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ตามข้อบังคับของว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2550 กับทางผู้ให้บริการอินเทอร์เนต เพื่อทำการออกแบบระบบที่รองรับพระราชบัญญัติดังกล่าวให้มากที่สุด จากผลของการสำรวจแบบสอบถามผู้ให้บริการอินเทอร์เนตส่วนใหญ่ยังไม่ได้มีการเตรียมการใด ๆ เพื่อรองรับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ผู้วิจัยได้วิเคราะห์ระบบเพื่อให้สามารถรองรับข้อกำหนดของพระราชบัญญัตินี้โดยมีส่วนการทำงานดังนี้

มีการระบุตัวตนของผู้ใช้งาน โดยมีระบบสำหรับการพิสูจน์ตัวตนของผู้ใช้บริการใช้ระบบสมาชิกสำหรับให้สมาชิกเข้าใช้งานเครือข่ายอินเทอร์เน็ต

มีระบบการจัดการเวลาให้เป็นมาตรฐานที่น่าเชื่อถือและสามารถนำไปอ้างอิงเมื่อเกิดเหตุโดยมีความผิดพลาดไม่เกิน 10 มิลลิวินาที

มีระบบการเก็บรักษาข้อมูลที่ครบถ้วนและเชื่อถือได้ และจำเป็นต้องมีการสำรองข้อมูลการจราจรที่เกิดขึ้นด้วย

มีระบบการจัดการสำหรับการค้นคืนข้อมูลการจราจรย้อนหลังเพื่อใช้สำหรับค้นข้อมูลโดยจะมีรายงานจากเจ้าหน้าที่เพื่อทำการระบุใครเป็นผู้กระทำความผิดโดยการออกเป็นรายงานสำหรับเป็นหลักฐานทางกฎหมาย

มีระบบที่รองรับเครือข่ายไร้สายโดยกำหนดให้ระบบที่พัฒนาทั้งหมดสามารถรองรับเครือข่ายไร้สายจากการวิเคราะห์ระบบทั้งหมดสามารถออกแบบเป็น 2 ระบบย่อย เพื่อรองรับทั้ง

เครือข่ายแบบมีสายและไร้สาย ได้แก่ ระบบฐานข้อมูลสำหรับเก็บข้อมูลผู้ใช้งานอินเทอร์เนต (Member System for Internet) และระบบค้นคืนและระบุผู้ใช้งานในอินเทอร์เนต (Retrieval System) โดยแบ่งการทำงานหรือดำเนินการต่างๆ ออกเป็นส่วนย่อยเพื่อให้ง่ายในการจัดการระบบ

การพัฒนาระบบงานดังกล่าวผู้วิจัยได้ใช้ระบบปฏิบัติ FreeBSD โดยระบบฐานข้อมูลสำหรับเก็บข้อมูลผู้ใช้งานอินเทอร์เนต ผู้วิจัยได้พัฒนาระบบขึ้นโดยใช้ภาษา PHP โปรแกรม FreeRadius และ Chillispot เพื่อใช้ในการพิสูจน์ตัวตนในการเข้าสู่ระบบอินเทอร์เน็ตโดยมีการกำหนดให้ชื่อผู้ใช้ด้วยหมายเลขประจำตัวประชาชนและสำหรับเครือข่ายไร้สายได้มีการลงทะเบียนหมายเลข MAC Address ด้วยสำหรับสู่ระบบอินเทอร์เน็ต และระบบค้นคืนและระบุผู้ใช้งานในอินเทอร์เนต

ผู้วิจัยได้พัฒนาโดยใช้ภาษา PHP และใช้ฐานข้อมูลเดียวกับระบบฐานข้อมูลสำหรับเก็บข้อมูลผู้ใช้งานอินเทอร์เนตนอกจากการพัฒนาระบบในสองส่วนที่ได้กล่าวมาแล้วยังมีส่วนที่เป็นการตั้งค่าระบบ ได้แก่ การเทียบเวลาระหว่างอุปกรณ์คอมพิวเตอร์ และการเขียนโปรแกรม Shell Script ในการเก็บข้อมูลล็อกไฟล์โดยเก็บข้อมูลกิจกรรมที่เกิดขึ้นตามที่ต้องการและบันทึกเป็นวันต่อวันหลังจากที่ได้ทดสอบระบบเก็บข้อมูล พิสูจน์ตัวตน ค้นคืนและระบุผู้ใช้บริการอินเทอร์เนต

ผลปรากฏว่าระบบเก็บข้อมูล พิสูจน์ตัวตน ค้นคืนและระบุผู้ใช้บริการอินเทอร์เนตสามารถทำงานรองรับ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 โดยไม่ได้ส่งผลกระทบทางลบต่อการให้บริการอินเทอร์เน็ตและสามารถค้นคืนและสามารถระบุผู้ใช้งาน ในอินเทอร์เนตที่เข้าข่ายผิดหรืออาจจะผิดข้อกำหนดตาม พระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ได้อย่างถูกต้อง

Subject: Design and Implementation of Internet Gateway Open Source System for University.

Author: Prayoon Chaibuth.

Program: Computer science.

Faculty: Faculty of Science and Technology.

Institute: Rajabhat Institute Phetchabun University.

Year : 2553.

Abstract.

This research work aims is to create a system to collect information used in Internet in accordance with the Act and the Computer Crime Act B.E 2550 in the Internet service provider in the research, this questionnaire is to store traffic data. Accordance with the Computer Crime Act B.E 2550 with the Internet service provider. To design systems that support the Act as much as possible. The results of the survey questionnaire Internet service providers, most have not been prepared to support any Act of the Computer Crime Act 2550, the researcher has analyzed the system in order to accommodate the requirements of this Act. Working with the following.

The identity of the user. The system for authentication of users using the system for member to member using the Internet.

Time management system as standard and can be trusted based on the scene with an error less than 10 milliseconds.

A data storage system complete and reliable. (Encrypted log file) and need to back up traffic (Data log files) that occur with

Management system for retrieving data traffic back to searching for information will be reported by the authorities to identify offenders who are released by the reports as evidence of the law.

Have a system that supports the wireless network by setting the system to the total development capacity wireless network by analyzing the entire system can be designed as two

sub-systems to support the network wired and wireless, including the database for data storage. Internet users (Member System for Internet) and retrieval and provide users on the Internet (Retrieval System) consists of work or the various Into subsections to make it easier to manage.

Development of such a system were used by the FreeBSD operating system, database system for storing information using the Internet. Researchers have developed by using PHP, the program FreeRadius and Chillispot used for authentication to access the Internet by adopting a user with a number of identification and for the wireless network has been down. For registration number MAC Address to the Internet. And retrieval and provide users of the Internet.

Researchers have developed using PHP and a database with the database for storing information using the Internet than develop the system in two parts that have mentioned the existence of the system settings were compared in-between Computer and programming Shell Script to collect the data log files through data collection activities with respect to and recorded on the day after the test data collection system authentication to retrieve and identify the user Internet.

The results showed that the system authentication information retrieval and provide users access internet. Work support. Act Computer Related Crime Act 2550 without adversely affecting the Internet and to retrieve and identify the user. Internet access in the network or failure may be wrong by definition. Computer Related Crime Act B.E 2550 correctly.

กิตติกรรมประกาศ

งานวิจัยนี้สำเร็จลงได้ด้วยดีเพราะได้รับความร่วมมือเป็นอย่างดียิ่งจากหน่วยงานและบุคคลซึ่งผู้วิจัยต้องขอขอบพระคุณมา ณ โอกาสนี้ ได้แก่

บุคลากรและเจ้าหน้าที่สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏเพชรบูรณ์

อาจารย์สาขาวิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏเพชรบูรณ์

สำนักงานคณะกรรมการการวิจัยแห่งชาติ และสถาบันวิจัยและพัฒนา มหาวิทยาลัยราชภัฏเพชรบูรณ์ที่ให้การสนับสนุนงบประมาณในการทำวิจัย

ขอขอบคุณผู้เชี่ยวชาญได้แก่ ทีมพัฒนาระบบโอเพนซอร์ส ลีนุกซ์, ทีมพัฒนา FreeBSD Operating System, ทีมพัฒนา EZ Radius, ทีมพัฒนา Dalo Radius, ทีมพัฒนา Authentication มหาวิทยาลัยบูรพาและทีมพัฒนาโอเพนซอร์สอื่นที่ไม่ได้กล่าวถึงเป็นอย่างสูงที่ให้ซอร์สโค๊ดที่มีประโยชน์มาก ที่ผู้วิจัยได้นำมาพัฒนาต่อและประยุกต์ใช้ให้เกิดประโยชน์สูงสุดต่อมหาวิทยาลัยและหน่วยงานอื่นๆ ที่มีลักษณะการใช้ระบบเครือข่ายอินเทอร์เนตในรูปแบบเดียวกันโดยผู้วิจัย ตั้งความหวังไว้ว่าจะให้ซอร์สโค๊ดฟรีกับผู้พัฒนาที่สนใจต่อไป

ขอขอบคุณผู้มีอุปการคุณทุกท่าน บิดา มารดา ญาติพี่น้อง ครู อาจารย์ ที่คอยให้คำแนะนำ และให้คำปรึกษา และให้กำลังใจตลอดระยะเวลาการทำวิจัย ให้การทำวิจัยผ่านไปได้ด้วยดี จนผลงานวิจัยเสร็จสมบูรณ์

ประยูร ไชยบุตร และคณะ

ธันวาคม 2553

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญรูป

รูปที่ **หน้า**

สารบัญรูป(ต่อ)

รูปที่ **หน้า**

บทที่ 1
บทนำ

งานวิจัยเรื่อง การออกแบบและพัฒนาต้นแบบระบบอินเทอร์เนตเกตเวย์ราคาถูกสำหรับมหาวิทยาลัย ได้ถูกพัฒนาขึ้นมาโดยมีหลักการ ทฤษฎี เหตุผลและสมมุติฐาน วัตถุประสงค์ของการวิจัย ประโยชน์ที่ได้รับจากการศึกษาการวิจัย ขอบเขตวิธีการวิจัย และสถานที่ที่ใช้ใน การดำเนินการวิจัยและรวบรวมข้อมูล ซึ่งมีรายละเอียดดังต่อไปนี้

1.1 ความเป็นมาและความสำคัญของปัญหา

1.1.1 ความสำคัญ

ระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยราชภัฏเพชรบูรณ์ ได้เปิดให้บริการด้านการเรียนการสอน และการสืบค้นสารสนเทศ สำหรับนักศึกษา และบุคลากร โดยมีจำนวนเครื่องคอมพิวเตอร์ที่เชื่อมต่อประมาณ 20 เครื่องในระยะแรก ต่อมามีการพัฒนาระบบเครือข่ายให้มีประสิทธิภาพมากขึ้นความต้องการแลกเปลี่ยนข้อมูล ข่าวสารระหว่างองค์กรจึงเกิดขึ้น ปัจจุบันได้มีการขยายเครือข่ายให้ครอบคลุม กับความต้องการของผู้ใช้บริการผ่านระบบเครือข่ายภายในมหาวิทยาลัยระบบเครือข่ายผ่านคู่สายโทรศัพท์ ระบบลีสไลน์ผ่านระบบเครือข่ายใยแก้วนำแสง และระบบเครือข่ายไร้สาย ซึ่งมีจำนวนผู้ใช้บริการเพิ่มขึ้นอย่างต่อเนื่อง ในปีการศึกษา 2550 มีผู้ใช้บริการระบบเครือข่ายทั้งสิ้น 10,000 คนโดยประมาณได้แก่ บุคลากรของมหาวิทยาลัย นักศึกษาภาคปกติ นักศึกษาภาค กศ.ปช. และมีเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับระบบเครือข่ายของมหาวิทยาลัยกว่า 1,000 เครื่อง ทั้งแบบตั้งโต๊ะและแบบพกพา กระจายอยู่ตามอาคารต่างๆ ทั่วมหาวิทยาลัย จากการสังเกตพฤติกรรมการใช้บริการผ่านระบบเครือข่าย พบว่ามีปริมาณการใช้งานมากในช่วงเวลา 8.30– 20.00 น. โดยใช้บริการอินเตอร์เน็ตผ่านโปรโตคอล HTTP FTP และ SMTP เป็นส่วนใหญ่

การนำระบบเครือข่ายคอมพิวเตอร์ มาใช้เพื่อสนับสนุนการดำเนินงานต่างๆ ในองค์กรเป็นสิ่งจำเป็นและสำคัญต่อการพัฒนาองค์กร ปัจจัยหลักและอุปสรรคของการพัฒนาระบบซอฟต์แวร์เพื่อใช้ในเครือข่ายคอมพิวเตอร์ที่ใช้ในองค์กร คือความปลอดภัยของระบบและข้อมูลภายในขององค์กร เนื่องจากความไม่มั่นใจในความปลอดภัยของข้อมูล และการระบุตัวตนของผู้ส่งและผู้รับที่ถูกต้อง ดังนั้นถ้าภายในระบบไม่มีการควบคุมและตรวจสอบความปลอดภัยที่ดีพอจะส่งผลให้เกิดความเสียหายต่อระบบและข้อมูลขององค์กรได้เพื่อสนับสนุนการดำเนินงานและเป็น

แนวทางในการแก้ปัญหานี้ วิธีการหนึ่งที่ถูกพัฒนาขึ้นและนำมาใช้คือ การรับรองสิทธิให้กับผู้ใช้ (Certification Authority) หรือ CA เป็นการเพิ่มความมั่นใจและเชื่อมั่นว่าข้อมูลที่ส่งออกไปจนถึงผู้รับ สามารถป้องกันและตรวจสอบสิทธิการเข้าถึงข้อมูลได้ โดยใช้ CA เป็นตัวกลางในการพิสูจน์ตัวตน รับรองสิทธิและการจัดการกุญแจสำหรับการเข้ารหัสข้อมูล และจากแนวคิดข้างต้น มีความสอดคล้องกับสภาวะปัญหาภาระของงมหาวิทยาลัย ในปัจจุบัน คืองานในส่วนของระบบเงินงบประมาณ ซึ่งเป็นภาระงานของงานคลังและพัสดุ งานบริหารธุรการ งานบัญชี ระบบทะเบียนและวัดผลนักศึกษางานส่งเกรดผลการเรียนของนักศึกษา และงานการเจ้าหน้าที่และบุคลากรของมหาวิทยาลัย ที่ยังมีปัญหาในเรื่องของ ความเชื่อมั่นในความปลอดภัยและความถูกต้องของข้อมูลที่ใช้อยู่บนระบบเครือข่ายภายในของมหาวิทยาลัย และเพื่อลดความซ้ำซ้อน การเสียเวลาในการดำเนินงาน จึงแก้ปัญหาข้างต้นโดยการพัฒนาระบบป้องกันการละเมิดสิทธิข้อมูลบนระบบเครือข่ายเพื่อเพิ่มความมั่นใจของข้อมูลที่ทำการส่งผ่านทางเครือข่าย ให้มีความปลอดภัยมากขึ้น โดยสามารถตรวจสอบความครบถ้วนสมบูรณ์ของข้อมูลอิเล็กทรอนิกส์ (Integrity) การรักษาความลับ (Confidentiality) การป้องกันการปฏิเสธความรับผิดชอบ (Non - repudiation) และ การระบุตัวบุคคล (Authentication) ได้ซึ่งคาดว่าจะมีประโยชน์ต่อมหาวิทยาลัย ในการที่จะดำเนินงานให้มีประสิทธิภาพ รวดเร็วถูกต้องและมีความปลอดภัยของข้อมูลในองค์กร

เทคโนโลยีหรือวิทยาการเข้ารหัส เทคโนโลยีหรือวิทยาการเข้ารหัส (Cryptography) คือกระบวนการทำให้ข้อมูลที่ส่งผ่านทางเครือข่ายให้อยู่ในรูปแบบที่ไม่สามารถอ่านเข้าใจได้โดยผู้ที่ไม่มีสิทธิ โดยใช้พื้นฐานความรู้ที่เกี่ยวข้องกับวิธีการทางคณิตศาสตร์เข้ามาช่วยในการเปลี่ยนรูปแบบของข้อมูลเพื่อป้องกันข้อมูลที่ต้องการส่งไปถึงผู้รับ การเข้ารหัสได้มีการนำมาใช้กันตั้งแต่สมัยโบราณเช่น ในยุคอียิปต์ และโรมันโบราณโดยจะนำไปในใช้ในยุทธวิธี การรบ หรือในช่วงสงครามโลกครั้งที่สองก็มีการนำวิทยาการทางด้านนี้เข้ามาช่วยในยุทธวิธีการรบ จนถึงปัจจุบันความก้าวหน้าทางด้านการสื่อสารทำให้เทคโนโลยีหรือวิทยาการเข้ารหัสยิ่งมีความสำคัญยิ่งขึ้น เพราะความไม่มั่นใจในความปลอดภัยของข้อมูลที่ส่งในเครือข่ายที่ไม่มีความปลอดภัยและการละเมิดสิทธิ์ต่างๆ สามารถกระทำได้ง่ายขึ้นในปัจจุบัน จึงจำเป็นต้องมีกระบวนการรักษาความปลอดภัยของข้อมูล โดยมีหลักสำคัญๆ ดังนี้

การระบุตัวบุคคล (Authentication) เป็นกระบวนสำหรับทำการยืนยันตัวตนของผู้ส่งหรือผู้สร้างข้อมูลอิเล็กทรอนิกส์

การรักษาความลับ (Confidentiality) เพื่อป้องกันมิให้บุคคลซึ่งไม่ได้รับอนุญาตหรือไม่มีสิทธิอ่านข้อมูลอิเล็กทรอนิกส์ได้

ความถูกต้องครบถ้วนของข้อมูลอิเล็กทรอนิกส์ (Integrity) เพื่อป้องกันมิให้มีการเปลี่ยนแปลงแก้ไขทำลายหรือสร้างข้อมูลอิเล็กทรอนิกส์ขึ้นโดยไม่ได้รับอนุญาต

การป้องกันการปฏิเสธความรับผิด (Non – Repudiation) เพื่อป้องกันมิให้ผู้ส่งข้อมูลหรือผู้รับข้อมูลปฏิเสธว่าตนไม่ได้ส่งหรือไม่ได้รับข้อมูลอิเล็กทรอนิกส์

การพิสูจน์ตัวตน (Authentication) คือขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริงในทางปฏิบัติจะแบ่งออกเป็น 2 ขั้นตอน คือ

การระบุตัวตน (Identification) คือขั้นตอนที่ผู้ใช้แสดงหลักฐานว่าตนเองคือใคร เช่น ชื่อผู้ใช้ (Username)

การพิสูจน์ตัวตน (Authentication) คือขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลที่กล่าวอ้างจริง

การตรวจสอบทางอิเล็กทรอนิกส์ (Electronic Audit) คือการตรวจสอบหลักฐานทางอิเล็กทรอนิกส์ ซึ่งสามารถใช้ในการติดตามการดำเนินการเพื่อตรวจสอบความถูกต้องและแม่นยำ ตัวอย่างเช่นการตรวจสอบบัญชีชื่อผู้ใช้โดยผู้ตรวจบัญชี ซึ่งการตรวจสอบความถูกต้องของการดำเนินการเพื่อให้แน่ใจว่าหลักฐานทางอิเล็กทรอนิกส์นั้นได้ถูกสร้างและสั่งให้ทำงานโดยบุคคลที่ได้รับอนุญาต และในการเชื่อมต่อเหตุการณ์เข้ากับบุคคลจะต้องทำการตรวจสอบหลักฐานของบุคคลนั้นด้วย ซึ่งถือเป็นหลักการพื้นฐานของขั้นตอนการทำงานของการพิสูจน์ตัวตนด้วยโปรโตคอลในการพิสูจน์ตัวตน การพิสูจน์ตัวตนนับว่าเป็นกระบวนการเริ่มต้นและมีความสำคัญมากในการปกป้องเครือข่ายที่เป็นระบบเครือข่ายแบบเปิดหรืออินเทอร์เน็ตในปัจจุบันให้ปลอดภัย การเลือกใช้โปรโตคอลในการพิสูจน์ตัวตน (Authentication Protocol) มาเป็นโปรโตคอลในการสื่อสารจึงเป็นอีกวิธีการหนึ่งที่เหมาะสม เพื่อเพิ่มความมั่นใจในความปลอดภัยของข้อมูลที่อยู่บนเครือข่าย เพราะเป็นโปรโตคอลการสื่อสารที่มีกระบวนการพิสูจน์ตัวตนรวมอยู่ในชุดโปรโตคอล ซึ่งที่นิยมใช้ในปัจจุบันอย่างแพร่หลาย

1.1.2 ปัญหา

ปัจจุบันความก้าวหน้าทางด้านวิทยาศาสตร์และเทคโนโลยีมีความล้ำหน้าไปมากโลกของเรามีการพัฒนาอย่างไม่หยุดนิ่ง อันเนื่องมาจากสติปัญญาอันชาญฉลาดของมนุษย์ที่สามารถคิดค้นเทคโนโลยีใหม่ๆ ขึ้นมาอย่างต่อเนื่อง และรวดเร็วได้อย่างเหลือเชื่อ และบวกกับความต้องการที่ไม่มีขีดจำกัดของมนุษย์ จากความก้าวหน้าทันสมัยดังกล่าวหน่วยงานทั้งภาครัฐและเอกชนที่เกิดจากการรวมกลุ่มของมนุษย์ได้นำเอาเทคโนโลยีเหล่านี้เข้ามาช่วยพัฒนาประสิทธิภาพในการทำงานในองค์การหรือหน่วยงาน ซึ่งเทคโนโลยีทางด้านคอมพิวเตอร์ก็มีส่วนสำคัญไม่น้อยไปกว่าเทคโนโลยีประเภทอื่นในด้านการศึกษา ดังนั้นสถาบันการศึกษาต่างๆ

จึงได้นำเอาเทคโนโลยีคอมพิวเตอร์เข้ามาใช้ในการพัฒนาการดำเนินงานในสถาบัน เช่นเดียวกันกับองค์กรอื่นๆ ไม่ว่าจะเป็นการรับสมัครนักศึกษาใหม่ การประกาศผลการสอบผ่าน การประกาศผลการเรียนรวมไปถึงเครือข่ายของการสืบค้นข้อมูลต่างๆ การสืบค้นข้อมูลภายในห้องสมุด การเรียนการสอนในห้องปฏิบัติการ ฯลฯ

ระบบเครือข่ายอินเทอร์เนตเป็นระบบหนึ่งที่สถานศึกษาทุกแห่งมีความจำเป็นจะต้องนำมาประยุกต์ใช้งานทั้งด้านการเรียนการสอนและงานด้านการบริหารธุรการดังกล่าว มีการลงทุนด้วยงบประมาณที่สูงมากเมื่อเทียบกับการลงทุนในด้านต่างๆ ในสถานศึกษาผู้ที่เกี่ยวข้องกับการใช้ระบบเครือข่ายอินเทอร์เนตได้แก่บุคลลากรทางด้านการศึกษาทั้งหมด คืออาจารย์ ข้าราชการ นักเรียน นักศึกษา รวมถึงบุคคลภายนอกที่เข้ามาใช้ระบบเครือข่ายของหน่วยงานทางการศึกษาในบางครั้ง เช่น มีการอบรมสัมมนา การประชุม เป็นต้น การให้บริการอินเทอร์เนตในสถานศึกษาปัจจุบันมีทั้งแบบมีสายและแบบไร้สาย เป็นการยากที่จะป้องกันหรือติดตามผู้ใช้ทุกคนว่าเป็นใคร ทำอะไร เมื่อไร ที่ไหน อย่างไร ซึ่งอาจสร้างความผิดให้กับผู้ดูและระบบอย่างไม่ได้ตั้งใจได้

ประเทศไทยก็ประสบปัญหาอย่างนี้เช่นกันและได้ออกพระราชบัญญัติว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ 2550 เป็นกฎหมายที่ว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ทั้งผู้ใช้และผู้ดูและระบบคอมพิวเตอร์ มีโทษทั้งจำทั้งปรับ เป็นโทษที่หนักมาก สำหรับสถานศึกษาในประเทศไทยยังขาดผู้ที่มีความรู้ความเชี่ยวชาญทางด้านการดูและระบบเครือข่ายอย่างมาก และมีทางเดียวที่จะได้มาคือซื้อจากบริษัทที่ผลิตฮาร์ดแวร์และซอฟท์แวร์ทางด้านเครือข่ายและต้องใช้เงินจำนวนมากที่จะซื้อระบบดังกล่าวมาไว้ใช้ ด้วยเงินงบประมาณอันจำกัดไม่สามารถที่จะซื้อได้ครบสมบูรณ์ จึงประสบปัญหามาก บางหน่วยงานใช้วิธีการลงชื่อก่อนเข้าใช้งานที่ห้องปฏิบัติการอินเทอร์เนต แบบให้ผู้ใช้ต้องลงชื่อในสมุดบันทึกทุกครั้ง ซึ่งไม่สะดวก และไม่ปลอดภัย และไม่สามารถนำไปเป็นหลักฐานในชั้นศาลได้

1.1.3 แนวทางในการแก้ปัญหา

ผู้วิจัยและคณะได้เห็นปัญหาดังกล่าวจึงมีแนวคิดที่จะทำระบบจัดการเกี่ยวกับอินเทอร์เนต เกตเวย์ ที่เป็นโอเพนซอร์ส (Open Source) โดยมีความสามารถเป็นเกตเวย์ NAT Firewall Traffic Shapper Authentication และระบบจัดการเกี่ยวกับผู้ใช้ในสถานศึกษาซึ่งส่วนใหญ่เป็นห้องปฏิบัติการทางคอมพิวเตอร์ที่มีผู้ใช้หลายๆ คนมาใช้ร่วมกันซึ่งเป็นการตรวจสอบและพิสูจน์ตัวตนของผู้ใช้ก่อนเข้าใช้ระบบ รวมถึงการบันทึก Log File ของผู้ใช้ระบบด้วย ผู้วิจัยมีความประสงค์ที่จะพัฒนาแอปพลิเคชั่นแบบโอเพ่นซอร์ส (Application Open Source) เพื่อแจกฟรีให้สถานศึกษาต่างๆ ในประเทศไทย และสถานศึกษาอื่นๆ ทั่วโลกได้นำไปประยุกต์ใช้งานโดยผู้ใช้หรือผู้ดูแลระบบไม่จำเป็นต้องมีความเชี่ยวชาญทางด้านระบบเครือข่ายมากนัก

สามารถที่จะนำไปใช้ได้อย่างมีประสิทธิภาพและเพื่อเป็นการลดค่าใช้จ่าย ซึ่งเป็นวิธีที่ประหยัดและสามารถพัฒนาต่อยอดได้ด้วยตนเองเป็นการประหยัดงบประมาณให้กับประเทศชาติต่อไป

สำหรับมหาวิทยาลัยเป็นองค์กรที่บริการนักศึกษา อาจารย์และบุคลากรของมหาวิทยาลัยเป็นจำนวนมาก ซึ่งสำหรับมหาวิทยาลัยราชภัฏแล้วงบประมาณทางด้านไอทีแทบจะหมดเลยเมื่อเทียบกับรายรับ-รายจ่ายของสำนักวิทยบริการและเทคโนโลยีสารสนเทศที่รับผิดชอบ ดังนั้นจึงมีเพียงหนทางเดียวที่จะประหยัดงบประมาณให้กับมหาวิทยาลัยได้คือโอเพนซอร์ส(Open Source) โดยผู้วิจัยและทีมงานได้ลองผิด ลองถูกมาแล้ว 10 กว่าปี ได้ผลเป็นที่น่าพอใจโดยได้สร้างพีซีเร้าเตอร์ที่มีคุณสมบัติหลายด้าน เช่น การเทียบเวลาตามมาตรฐานสากล (NTP) และมีการบันทึกการใช้งานจราจรบนระบบเครือข่ายคอมพิวเตอร์ของผู้ใช้ทุกคนล็อกไฟล์(Log File) ที่ใช้งานผ่านระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย และมีระบบจัดการผู้ใช้ระบบเครือข่ายทั้งหมดเป็นศูนย์กลางที่เดียว สามารถจัดกลุ่มผู้ใช้ได้ สามารถจัดการแบนด์วิดได้ สามารถกำหนดระยะเวลาการใช้งานและอื่นๆ ได้ โดยมีวัตถุประสงค์เพื่อให้สอดคล้องกับพระราชบัญญัติว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ 2550 และมีแนวคิดว่าควรจะทำต่อไปให้มีประสิทธิภาพและใช้งานได้ง่ายเพื่อเผยแพร่ให้กับองค์กรต่างๆ ทั้งภาครัฐและเอกชนโดยเฉพาะหน่วยงานที่มีงบประมาณอันจำกัดด้านเทคโนโลยีสารสนเทศได้ใช้งานในรูปแบบลิขสิทธิ์แบบโอเพนซอร์ส (General Public License) ต่อไป

1.2 วัตถุประสงค์หลักของแผนงานวิจัย

1.2.1 พัฒนาระบบการบันทึกการจราจรบนระบบเครือข่ายคอมพิวเตอร์ (Log File) ตาม พรบ. ว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ 2550

1.2.2 พัฒนาระบบระบบพิสูจน์ตัวตน

1.2.3 พัฒนาระบบจัดการฐานข้อมูลผู้ใช้ระบบอินเทอร์เนต

1.2.4 พัฒนาระบบอินเทอร์เนตเกตเวย์สำหรับมหาวิทยาลัย

1.2.5 พัฒนาระบบอินเทอร์เฟสอินเทอร์เนตเกตเวย์กับไวไฟ-ลีสไลน์

1.2.6 ทำการเผยแพร่องค์ความรู้แก่หน่วยงานที่เป็นภาคี ได้แก่ มหาวิทยาลัยราชภัฏ มหาวิทยาลัยของรัฐและเอกชน และผู้สนใจทั่วไป

1.3 เป้าหมายเชิงยุทธศาสตร์ของแผนงานวิจัย

การปรับโครงสร้างทางเทคโนโลยีสารสนเทศให้สมดุลและยั่งยืนด้วยงบประมาณแบบเศรษฐกิจพอเพียง โดยการสร้างต้นแบบการพัฒนาระบบเครือข่ายอินเทอร์เนตเกตเวย์ราคาถูกเพื่อใช้ส่งเสริมศักยภาพสถาบันการศึกษา หรือองค์กรทั้งภาครัฐและเอกชน ให้สามารถแก้ปัญหาและพัฒนาไปสู่โลกดิจิตอลให้ประสบผลสำเร็จ

1.4 เป้าหมายของผลผลิต (output) และตัวชี้วัด

บริบทของการขยายเครือข่ายคอมพิวเตอร์ต้นทุนต่ำสำหรับองค์กรทางด้านการศึกษาที่มีงบประมาณน้อยให้ทันกับโลกยุคใหม่

1.4.1 ผลจากการวิเคราะห์ศักยภาพได้จุดอ่อน จุดแข็ง ของการใช้ระบบเครือข่าย

1.4.2 รูปแบบการแก้ปัญหาและพัฒนาความรู้ในการดูแลระบบเครือข่ายที่มีต้นทุนต่ำ

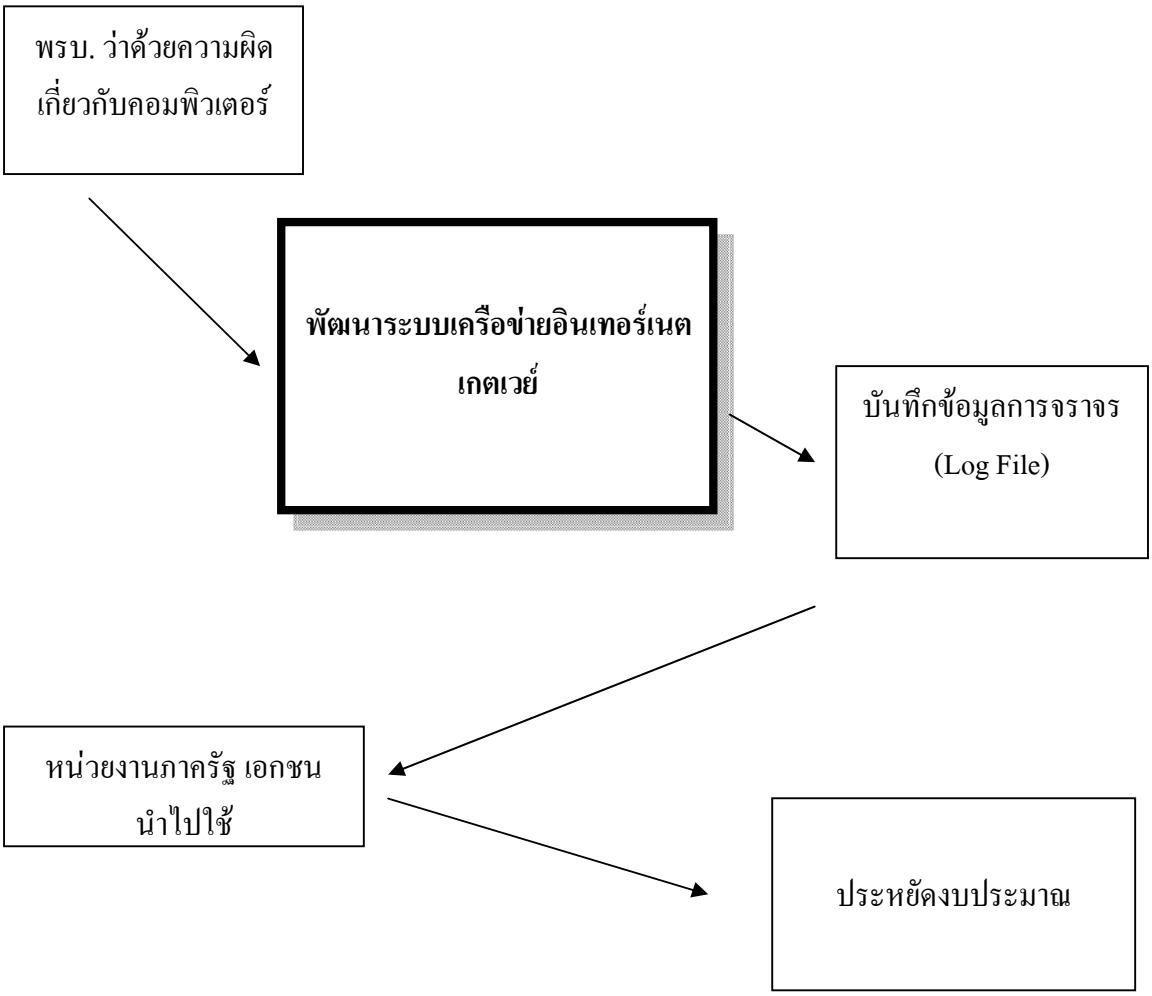
1.4.3 คู่มือการสร้างระบบเครือข่ายอินเทอร์เนตที่เสริมสร้างศักยภาพขององค์กรทางการศึกษา

1.5 เป้าหมายของผลลัพธ์ (outcome) และตัวชี้วัด

1.5.1 มหาวิทยาลัยสามารถนำระบบนี้ไปประยุกต์ใช้ในการพัฒนางานทางด้านควบคุมการใช้ระบบเครือข่ายอินเทอร์เนตได้อย่างมีประสิทธิภาพมากขึ้นร้อยละ 50

1.5.2 หน่วยงานที่เป็นภาคี สามารถนำคู่มือไปใช้อย่างน้อย 1 หน่วยงาน เพื่อเพิ่มจำนวนใช้ระบบเครือข่ายอย่างมีระบบ

1.6 กรอบแนวความคิดของแผนงานวิจัย



รูปที่ 1.1 แสดงกรอบแนวความคิดของแผนงานวิจัย

1.7 ประโยชน์ที่คาดว่าจะได้รับ

การเผยแพร่ในวารสาร การตีพิมพ์ เผยแพร่ให้กับผู้ดูแลระบบเครือข่าย ฯลฯ และหน่วยงานที่ใช้ประโยชน์จากผลการวิจัย

17.1 ผลผลิตจากชุดโครงการนี้ที่คาดว่าจะได้รับและผลที่จะเกิดขึ้นจากการนำผลผลิตไปใช้ประโยชน์

1. เผยแพร่ในวารสารทางวิชาการและเว็บไซต์
2. นำเสนอผลงานวิจัยในการจัดประชุมวิชาการระดับชาติ หรือนานาชาติ
3. จดสิทธิบัตรคู่มือการดูแลระบบเครือข่ายต้นทุนต่ำ

17.2 ผู้ใช้ประโยชน์จากผลผลิตของโครงการ

1. สถานศึกษาทุกระดับ ทุกภูมิภาค โดยเฉพาะมหาวิทยาลัยราชภัฏ และผู้สนใจทั่วไป
2. ผู้ประกอบการทางด้านอินเทอร์เนตคาแฟ่
3. ผู้ดูแลระบบเครือข่ายขององค์กร สามารถนำไปพัฒนาต่อได้แบบ GPL
4. องค์กรภาครัฐและเอกชนที่ใช้ระบบเครือข่ายอินเทอร์เนตเกตเวย์ต้นทุนต่ำ
5. สถาบันฝึกอบรมระบบเครือข่ายคอมพิวเตอร์
6. ประหยัดงบประมาณให้กับประเทศชาติ

1.8 แผนการดำเนินงาน

ตารางที่ 1.1 แสดงแผนบริหารงานวิจัยและแผนการดำเนินงาน

กิจกรรม	ระยะเวลาตามไตรมาส			
	ไตรมาส1	ไตรมาส2	ไตรมาส3	ไตรมาส4
1. เสนอโครงการขออนุญาตดำเนินโครงการ				
2. วางแผนการวิจัย				
3. ศึกษาบริบทและความต้องการของมหาวิทยาลัยและผู้ใช้ระบบ				
4. วิเคราะห์ศักยภาพทำแผนยุทธศาสตร์การวิจัย				
5. ดำเนินการตามแผนรวมทั้งโครงการย่อย				
6. สำรวจติดตามผลโครงการ				
7. วิเคราะห์ผลการวิจัย				
8. สรุปผลการวิจัย				
9. เขียนรายงานการวิจัย				
10. จัดทำรูปเล่มฉบับสมบูรณ์				
11. เผยแพร่งานวิจัย				

1.9 แผนการสร้างนักวิจัยรุ่นใหม่จากการทำการวิจัยตามแผนงานวิจัย

ภายหลังจากเสร็จสิ้นโครงการวิจัยครั้งนี้คาดว่าจะสามารถสร้าง นักวิจัยรุ่นใหม่ ในชุมชน และในมหาวิทยาลัยราชภัฏเพชรบูรณ์ อย่างน้อย 3 คน

1.10 กลยุทธ์ของแผนงานวิจัย

10.1 ศึกษาบริบทเพื่อให้ได้ข้อมูลสภาพทั่วไปของมหาวิทยาลัย

10.2 วิเคราะห์ศักยภาพเพื่อให้ได้จุดอ่อน จุดแข็ง โอกาส อุปสรรค ของระบบเครือข่ายอินเทอร์เนต เพื่อกำหนดรูปแบบการพัฒนา

10.3 วางรูปแบบการพัฒนา

10.4 ทดลองรูปแบบ เพื่อปรับปรุง

10.5 จัดทำคู่มือ

10.6 นำเสนอผลงานวิจัย

10.7 ทำการเผยแพร่องค์ความรู้

1.11 ระยะเวลา และสถานที่ทำการวิจัย

เริ่มดำเนินการวิจัย เดือนตุลาคม 2552 สิ้นสุดการวิจัยเดือนกันยายน 2553

1.12 สถานที่ทำการวิจัย

มหาวิทยาลัยราชภัฏเพชรบูรณ์ และห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ และห้องปฏิบัติการฝึกอบรม ที่เกี่ยวข้องกับงานวิจัย ของมหาวิทยาลัยราชภัฏเพชรบูรณ์

1.13 นิยามศัพท์เฉพาะ

อินเทอร์เนตเกตเวย์ หมายถึง ระบบควบคุมการใช้งานอินเทอร์เนตภายในมหาวิทยาลัย ได้แก่ ระบบพิสูจน์ตัวตน (Authentication) ระบบเทียบเวลาสากล (Network Time Protocol) ไฟล์วอลล์ (Fire Wall) แนท (NAT) ฯลฯ

แอพพลิเคชัน (Application) หมายถึง โปรแกรมที่พัฒนาขึ้นและใช้ควบคุมระบบเครือข่ายภายในมหาวิทยาลัยราชภัฏเพชรบูรณ์

เครือข่าย (Network) หมายถึง ระบบเครือข่ายแบบมีสาย (Lease Line) และไร้สาย (Wire Less) ที่เชื่อมโยงเป็นระบบเดียวกันภายในมหาวิทยาลัย

บทที่ 2
เอกสารและงานวิจัยที่เกี่ยวข้อง

การศึกษาเอกสารและงานวิจัยที่เกี่ยวข้องกับการจราจรเครือข่ายสื่อสาร ระบบเครือข่าย เทคโนโลยีการเข้ารหัสข้อมูล การพิสูจน์ตัวตนบนเครือข่าย และโปรโตคอลในการพิสูจน์ตัวตน และวิธีการออกแบบใช้งานกับระบบงานบนเครือข่ายมีรายละเอียดดังต่อไปนี้

1. ระบบปฏิบัติการ FreeBSD
2. การสื่อสารบนระบบเครือข่าย (Data Communication)
3. เทคโนโลยีการเข้ารหัสข้อมูลบนเครือข่าย (Encryption)
4. การพิสูจน์ตัวตนบนเครือข่าย (Network Authentication)
5. โปรโตคอลในการพิสูจน์ตัวตน (Protocol Authentication)
6. การเทียบเวลาสากล (Network Time Protocol)
7. ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Centralized Log)
8. ระบบปฏิบัติการลีนุกซ์ (Linux)

2.1 ระบบปฏิบัติการ FreeBSD

FreeBSD เป็นระบบปฏิบัติการชั้นสูงที่สามารถทำงานกับเครื่องคอมพิวเตอร์สถาปัตยกรรมแบบ x86 หรือเทียบเท่า, DEC Alpha, IA-64, PC-98 และ Ultra SPARC FreeBSD ถูกพัฒนามาจาก BSD ซึ่งเป็นระบบปฏิบัติการยูนิกส์ของมหาวิทยาลัย U.C. Berkeley FreeBSD โดยมีทีมงานพัฒนาขนาดใหญ่ ซึ่งได้ทำการพัฒนา แก้ไขข้อผิดพลาด รวมถึงการพัฒนาให้สามารถทำงานได้ในสถาปัตยกรรมคอมพิวเตอร์แบบอื่นๆด้วย

ลักษณะเด่นของ FreeBSD โดยรวมมีดังนี้

การกำหนดสิทธิของการทำงานหลายงานพร้อมกันซึ่งจะเป็นลักษณะที่มีการปรับตัวเป็นแบบพลวัต มีการจัดแบ่งทรัพยากรของระบบอย่างยุติธรรมระหว่างโปรแกรมประยุกต์และผู้ใช้งาน

ความสามารถในการทำงานแบบหลายผู้ใช้ (multi-user) ซึ่งยอมให้มีการใช้งานระบบจากผู้ใช้ระบบ FreeBSD ได้หลายคนพร้อมกัน ซึ่งสามารถกำหนดจำนวนการใช้งานทรัพยากรระบบของผู้ใช้แต่ละคนได้

มีระบบเครือข่ายในรูปแบบ TCP/IP ที่ปลอดภัย ซึ่งรองรับการทำงานของมาตรฐานต่างๆ เช่น SLIP(Serial Line IP), PPP(Point to Point Protocol), NFS(Network File System) DHCP(Dynamic Host Configuration Protocol), และ NIS(Network Information Services) เป็นต้น

ซึ่งหมายความว่าใช้งาน FreeBSD ในลักษณะที่เป็นเซิร์ฟเวอร์ เช่น เมลย์เซิร์ฟเวอร์(mail server) เว็ปเซิร์ฟเวอร์ (Web server) เอฟทีพีเซิร์ฟเวอร์ (Ftp server) การทำเร้าติ้ง (Routing) และไฟล์วอล์ล (Firewall) เป็นต้น

การป้องกันหน่วยความจำทำให้มั่นใจเรื่องการทำงานที่ผิดพลาดอันเนื่องมาจากการใช้งานหน่วยความจำที่ซ้ำกันของโปรแกรมประยุกต์หรือผู้ใช้ระบบ

FreeBSD เป็นระบบปฏิบัติการแบบ 32-bit (64-bit สำหรับสถาปัตยกรรม Alpha และ Ultra SPARC)

มีความสามารถในการใช้งานระบบ X Window (X11R6) มีความสามารถในการรันโปรแกรมที่รันบนระบบปฏิบัติการ Linux, SCO, SVR4, BSDI และ NetBSDได้

มีโปรแกรมประยุกต์มากมายซึ่งสามารถทำการเพิ่มโปรแกรมประยุกต์ เหล่านั้นด้วยระบบพอร์ตและเพคเกจ

สามารถทำการเพิ่มโปรแกรมประยุกต์ได้ง่ายโดยผ่านทางระบบเครือข่ายอินเตอร์เน็ต FreeBSD เป็น ซอสโค๊ดที่มีความเข้ากันได้กับระบบยูนิกทางการค้าและหากโปรแกรมประยุกต์ต้อง การการเปลี่ยนแปลงบางอย่างก็สามารถทำได้โดยเปลี่ยนแปลงและคอมไพใหม่

ความต้องการของหน่วยความจำเหมือน หน่วยความจำแบบแคช และหน่วยความจำบัฟเฟอร์ ถูกออกแบบให้มีประสิทธิภาพสูง ทำให้เพียงพอต่อความต้องการของโปรแกรมประยุกต์แต่ละโปรแกรม และความต้องผู้ใช้งานแต่ละคน

รองรับการประมวลผลแบบหลายหน่วยประมวล แบบ Symmetric multi-processor (SMP)

รองรับการทำงานกับตัวแปรภาษาพื้นฐานคือ C, C++, Fortran, และ Perl นอกจากนี้ ยังสามารถติดตั้งตัวแปรภาษาเพิ่มเติมได้โดยการติดตั้งจากพอร์ตและเพ็คเก็จ

เนื่องจาก FreeBSD เป็นระบบการพัฒนาระบบเปิด จึงมีซอสโค๊ดของระบบซึ่งทำให้สามารถปรับปรุงและแก้ไขการทำงานของระบบให้มีความถูกต้องเชื่อถือได้

มีเอกสารคู่มือการใช้งานแบบออนไลน์

ลิขสิทธิ์ของ FreeBSD ลักษณะของลิขสิทธิ์ของ FreeBSD ไม่มีความยุ่งยากซับซ้อนมาก นักกล่าวคือสามารถทำการแก้ไข คัดแปลง ตัวซอร์สโค๊ดของโปรแกรมใดก็ได้ แต่นำข้อความต่อไปนี้

“ THIS SOFTWARE IS PROVIDED BY THE FREEBSD PROJECT ``AS IS''''''' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FREEBSD PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.”

โครงการ FreeBSD เกิดขึ้นประมาณปี 1993 (ซึ่งเป็นผลมาจากการพัฒนา “Unofficial 386BSD Patchkit” ซึ่งพัฒนาโดย Nate Williams , Rod Grimes และ Jordan Hubbard)

จุดมุ่งหมายตั้งเดิมเพื่อต้องการแก้ปัญหาของ 386BSD (386BSDเป็นระบบปฏิบัติการที่รันบนเครื่องคอมพิวเตอร์สถาปัตยกรรม i386 , 386BSD เป็นระบบปฏิบัติการของ Bill Jolitz ที่ใช้ Patchkit ในการทำงาน ; อ้างถึง 386BSD http://www.wikipedia.org/wiki/386BSD) ซึ่งกลไก Patchkit มีการพัฒนาโดยไม่มีแนวทางที่ชัดเจน ทำให้ Patchkit มีขนาดใหญ่และทำงานได้ช้า จึงได้เกิดการพัฒนาโปรแกรมเพื่อแก้ปัญหาดังกล่าวซึ่งได้เรียกชื่อโครงการนี้ว่า ``386BSD 0.5'' หรือ`386BSD Interim''

ต่อมาได้เปลี่ยนเชื่อโครงการเป็น “FreeBSD” เนื่องมากจากไม่ได้รับการสนับสนุนจาก Bill Jolitz ซึ่งเป็นผู้พัฒนา 386BSD ซึ่งผู้คิดชื่อ “FreeBSD” คือ David Greenman โครงการ “FreeBSD” ได้รับการสนับสนุนอย่างดียิ่งจากบริษัท Walnut Creek CDROM ทั้งในเรื่องของการผลิตแผ่นซีดี Distributing FreeBSD รวมไปถึงการให้การสนับสนุนในเรื่องเครื่องเซิร์ฟเวอร์และการเชื่อมต่ออินเตอร์เน็ตความเร็วสูง และให้การสนับโครงการ “FreeBSD” จนถึงในปัจจุบัน

FreeBSD รุ่น 1.0 ผู้สร้างขึ้นเป็นซีดีรอมในเดือนพฤศจิกายนปี 1993 ซึ่งมีพื้นฐานมาจาก 4.3 BSD-Lite (``Net/2''''''') ของมหาวิทยาลัย U.C. Berkeley ส่วนประกอบส่วนใหญ่ถูกสร้างขึ้น

จาก 386BSD และมูลนิธิ Free Software Foundation นับเป็นก้าวแรกของการพัฒนา และได้ทำการแก้ไขปรับปรุงให้สมบูรณ์ยิ่งขึ้นใน FreeBSD รุ่น 1.1 ในเดือนพฤษภาคม ปี 1994

ต่อมา FreeBSD ประสบปัญหาที่ยากลำบากในการปรับปรุงความเข้ากันได้กับ 4.4BSD Lite เพราะกลุ่มที่พัฒนา 4.4BSD-Lite ได้ทำการเปลี่ยนโค๊ดบางอย่างเพื่อให้มีผลทางกฎหมาย รวมถึงการนำโค๊ดของ 4.4BSD-Lite มาใช้บนสถาปัตยกรรมของอินเทลไม่ประสบความสำเร็จอย่างมาก ทำให้การออก FreeBSD ร่น 2.0 ออกในเดือนธันวาคม ปี 1994 ซึ่งช้ากว่ากำหนดเดิมที่จะออกในเดือนพฤศจิกายน และได้ทำการปรับปรุงให้สมบูรณ์ขึ้นทั้งในเรื่องความเสถียรภาพและการติดตั้งที่ง่ายขึ้นใน FreeBSD รุ่น 2.0.5 ในเดือน มิถุนายนปี 1995

การติดตั้ง FreeBSD สามารถติดตั้งได้ง่ายมีหลายสื่อที่สามารถทำการติดตั้งได้ เช่น ซีดีรอม ดีวิดีรอม ฟลอปปี้ดิสก์เทปแม่เหล็ก หรือถ้ามีการเชื่อมต่อกับระบบเครือข่ายก็สามารถทำการติดตั้งได้จากการใช้โปรโตคอล FTP หรือ NFS การติดตั้งในที่นี้จะเป็นกล่าวถึงการติดตั้งในส่วนของ FreeBSD/i386 เพียงเท่านั้น จะไม่ขอกล่าวถึงการติดตั้ง FreeBSD บนคอมพิวเตอร์สถาปัตยกรรมอื่น การติดตั้ง FreeBSD จะใช้การติดตั้งในรูปแบบเมนูที่เป็น text mode ในการติดตั้งและในการแก้ไขค่าต่างๆ ของระบบ

การเตรียมตัวก่อนลงมือทำการติดตั้ง ถือเป็นเรื่องสำคัญอย่างยิ่งสำหรับการติดตั้งระบบปฏิบัติการ FreeBSD สิ่งที่ต้องทำคือต้องตรวจสอบฮาร์ดแวร์ที่มีอยู่ว่าสามารถทำงานกับ FreeBSD ได้ ซึ่งสามารถตรวจสอบได้จาก http://www.freebsd.org/releases/4.8R/hardware i386.html ควรจะจดรายละเอียดของอุปกรณ์ต่างๆ การ์ดที่จะทำการติดตั้ง เช่นการ์ดควบคุมฮาร์ดดิสแบบ SCSI เน็ตเวิร์คการ์ด การ์ดเสียง เป็นต้น ซึ่งควรบันทึกหมายเลขการร้องขออินเตอร์รับ(IRQ) หมายเลขพอร์ตที่ใช้ในการเชื่อมต่อการ์ด(IO port address) ซึ่งหากมีระบบเก่าหรือข้อมูลเก่าอยู่ขอแนะนำที่ดีที่สุดคือการสำรองข้อมูลต่างๆ เอาไว้ก่อนที่จะทำการติดตั้งระบบ FreeBSD เพื่อความปลอดภัยของข้อมูล

ฮาร์ดแวร์ที่สามารถใช้งานกับ FreeBSD ได้ ระบบปฏิบัติการ FreeBSD ในปัจจุบันสามารถทำงานได้สถาปัตยกรรมเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ที่ใช้หน่วยประมวลผลกลางระดับ i386 หรือเทียบเท่าสามารถทำงานได้กับหน่วยประมวลผลกลางของบริษัท อินเทลนับตั้งแต่หน่วยประมวลผลกลางระดับ 80386 ซึ่งประกอบด้วยหน่วยประมวลผลกลาง 80386, 80486, Pentium, Pentium Pro, Pentium II, Pentium III, Pentium 4 และอื่นๆ เช่น Xeon และ Celeron processors (ซึ่งถึงแม้ว่าจะสามารถใช้งานกับหน่วยประมวลผลกลางระดับ 386SX ได้แต่ก็ไม่แนะนำให้ใช้กับ 386SX) หน่วยประมวลผลกลางที่เทียบเท่ากับ i386 ของบริษัท AMD หน่วยประมวลผลกลางที่รองรับการทำงานของ FreeBSD ประกอบด้วย Am486, Am5x86, K5, K6

Athlon (รวมถึง Athlon-MP, Athlon-XP, Athlon-4,และ Athlon Thunderbird) และ Duron นอกจากนี้ยังรองรับหน่วยประมวลผลกลางที่เทียบเท่า i386จากบริษัท Cyrix และ NexGen.

ระบบปฏิบัติการ FreeBSD สามารถทำงานร่วมกับเมนบอร์ดได้หลากหลายรูปแบบ รองรับเมนบอร์ดที่ใช้งานบัสแบบ ISA, VLB, EISA, AGP, และ PCI แต่มีข้อจำกัดกับบัสแบบ MCA (``MicroChannel'''''') ซึ่งในสถาปัตยกรรมของ IBM รุ่น PS/2

ระบบปฏิบัติการ FreeBSD สามารถใช้งานในลักษณะมัลติโปรเซสเซอร์ (Symmetric multi-processor ;SMP) แม้ว่าในบางกรณีจะมีปัญหากับไบออสของเมนบอร์ดอยู่บ้างซึ่งสามารถขอคำแนะนำจากเมลลิ้งลิสของ FreeBSD ในส่วนของการทำงานมัลติโปรเซสเซอร์อีเมลย์ freebsdsmp@FreeBSD.org

ข้อแนะนำระบบต่ำสุดที่สามารถรันระบบปฏิบัติการ FreeBSD ต้องมีเมมโมรีอย่างน้อย 8 MB แต่ควรมี16 MB หรือว่ามากว่าเพื่อให้ประสิทธิ์ภาพของระบบทำงานได้ดี หน่วยประมวลผลกลางสามารถรันได้จากหน่วยประมวลผลกลางอย่างน้อย 386SX แต่ก็แนะนำให้ใช้หน่วยประมวลผลกลางที่สูงกว่า 386SX เพื่อที่จะได้ประสิทธิ์ภาพของระบบที่ดีขึ้น

สำหรับฮาร์ดแวร์อื่นๆ ที่สนับสนุนการทำงานของระบบปฏิบัติการ FreeBSD เช่น

การ์ดความคุมการทำงานของฮาร์ดดิส การ์ดเน็ตเวิร์ค และอุปกรณ์ต่อพ่วงอื่นสามารถดูรายละเอียดเพิ่มเติมที่ http://www.freebsd.org/releases/4.8R/hardware-i386.html

เปรียบเทียบระหว่าง FreeBSD ,Linux ,Windows

ลักษณะเด่นของระบบปฏิบัติการ FreeBSD ที่เห็นได้ชัดเจนคือความสามารถทำงานด้วยฮาร์ดแวร์ที่มีคุณสมบัติต่ำๆ ได้เช่นเครื่อง 486 หรือ Pentium 75 ก็สามารถที่จะสร้างเซิร์ฟเวอร์ ในเรื่องของลิขสิทธิ์ที่ FreeBSD ใช้ลิขสิทธิ์แบบ BSD ซึ่งเอื้ออำนวยความสะดวกในการพัฒนาโปรแกรมต่อได้มากว่ารูปแบบของลิขสิทธิ์แบบ GPL ราคาในการจัดหาโปรแกรม FreeBSD ด้วยราคาที่ไม่สูง อีกประเด็นหนึ่งคือความปลอดภัยของระบบ FreeBSD เนื่องจาก FreeBSD ได้ทำการตั้งค่าปกติในเรื่องความปลอดภัยไว้อย่างเข้มงวด

จุดด้อยของ FreeBSD การใช้งานของโปรแกรม FreeBSD ยังไม่แพร่หลายมากนัก การขาดบุคลากรที่มีความสามารถในการติดตั้งและการดูแลระบบ

FreeBSD คือชื่อของระบบระบบปฏิบัติการแบบ Unix ระบบหนึ่งที่ถูกพัฒนาโดย มหาวิทยาลัย University of California, Berkeley ซึ่งในปัจจุบันถูกพัฒนาให้สามารถทำงานบนเครื่องคอมพิวเตอร์ได้หลายระบบรวมถึงเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer)

2.2 การสื่อสารบนระบบเครือข่าย (Data Communication)

ระบบเครือข่ายคอมพิวเตอร์ (Computer Network) หมายความถึงเครื่องคอมพิวเตอร์ตั้งแต่สองเครื่องขึ้นไปที่เป็นอิสระต่อกันนำมาเชื่อมต่อกันได้โดยไม่คำนึงถึงระยะทางระหว่างเครื่องฯทั้งสอง ความหมายของการเชื่อมต่อถึงกันนั้นก็ไม่ได้จำกัดว่าจะต้องใช้แบบใด ไม่ว่าจะเป็นการเชื่อมต่อ โดยใช้เคเบิ้ลธรรมดา สายเคเบิ้ลใยแก้ว แบบใช้คลื่นไมโครเวฟ หรือแบบใช้สัญญาณดาวเทียม ส่วนความเป็นอิสระต่อกันนั้น หมายความถึงเครื่องคอมพิวเตอร์หลายๆ เครื่องที่ทำงานงานร่วมกันผ่านระบบเครือข่ายสื่อสาร ซึ่งไม่เหมือนกับเครื่องมัลติโปรเซสเซอร์ ที่เป็นคอมพิวเตอร์เครื่องเดียวแต่มีโปรเซสเซอร์อยู่หลายตัวและมีการจัดโครงสร้างภายในเป็นการแบ่งงานกันทำอย่างเป็นระบบ(ศัลยุทธ์ สว่างวรรณะ, 2547)

การสื่อสารข้อมูล คือ การแลกเปลี่ยนข้อมูลระหว่างสองอุปกรณ์ ผ่านตัวกลางในการสื่อสาร (Transmission Media) ตัวอย่างเช่น การสื่อสารข้อมูลระหว่างอุปกรณ์คอมพิวเตอร์สองเครื่องด้วยการใช้สายเคเบิลเป็นตัวกลางในการสื่อสาร นอกจากนี้การสื่อสารข้อมูลยังมีทั้งการสื่อสารระยะใกล้ หรือแบบโลคอล (Local) ในกรณีที่อุปกรณ์การสื่อสารต่างๆ อยู่ในบริเวณหรืออาคารเดียวกัน และการสื่อสารระยะไกลหรือแบบรีโมต ซึ่งอุปกรณ์การสื่อสารจะอยู่ไกลกันหรือต่างพื้นที่ (โอภาส เอี่ยมสิริวงศ์, 2552)

องค์ประกอบพื้นฐานของระบบการสื่อสารข้อมูล (Components of Data Communication System) ระบบเครือข่ายสื่อสารข้อมูล ประกอบด้วยองค์ประกอบพื้นฐานทั้ง 5 ประกอบด้วย

(1) ข้อมูล/ข่าวสาร (Message) ในที่นี่คือข้อมูลหรือสารสนเทศต่าง ๆ ที่ต้องการสื่อสาร โดยข่าวสารอาจประกอบด้วยข้อความ ตัวเลข รูปภาพ เสียง หรือ วีดีโอ หรืออาจเป็นสิ่งที่กล่าวมานั้นมารวมกัน เช่น ภาพพร้อมเสียง ซึ่งเรียกว่า สื่อประสม (Multimedia) ข้อมูลข่าวสารจะถูกทำการเข้ารหัส (Encoding) เพื่อส่งผ่านตัวกลางส่งข้อมูล และ เมื่อปลายทางได้รับข้อมูลที่ส่งมาก็จะทำการถอดรหัส (Decoding) เพื่อให้เป็นข้อมูลดั้งเดิมเช่นเดียวกับที่จะส่งมา อย่างไรก็ตามระหว่างข้อมูลข่าวสารกำลังเดินทางมาถึงปลายทาง ก็อาจพบอุปสรรคจากสัญญาณรบกวนชนิดต่าง ๆ ได้

(2) ผู้ส่งข้อมูล (Sender/Source) คือ อุปกรณ์ที่ใช้สำหรับส่งข้อมูลข่าวสาร ซึ่งอาจเป็นเครื่องคอมพิวเตอร์ เวิร์กสเตชั่น โทรศัพท์ กล้องวีดีโอ เป็นต้น

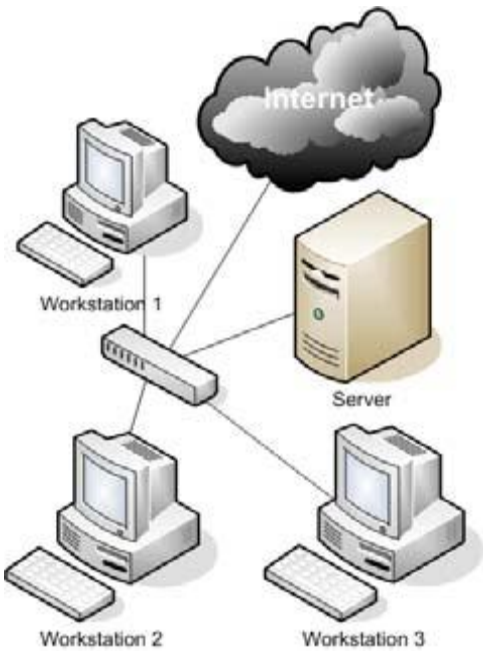
(3) ผู้รับข้อมูล (Receiver/Destination) คือ อุปกรณ์ที่ใช้สำหรับข้อมูลข่าวสารที่ทางผู้รับข้อมูลส่งมาให้ ซึ่งอาจเป็นเครื่องคอมพิวเตอร์ เวิร์กสเตชัน โทรศัพท์ โทรทัศน์ เป็นต้น อย่างไรก็ตามในการับส่งข้อมูล ตามปกติแล้วจะมีอุปกรณ์ที่ใช้สำหรับทำหน้าที่ในการรับส่งข้อมูล

(4) ตัวกลางในการส่งข้อมูล (Transmission Medium) คือ เส้นทางที่ทำให้สามารถนำข้อมูลที่รับส่งกันนั้นเดินทางไปยังจุดหมายปลายทางระหว่างกันได้ โดยตัวกลางในการส่งข้อมูลก็จะมีทั้งแบบมีสาย เช่น สายเคเบิล สายคู่บิดเกลียว สายไฟเบอร์ออปติ และตัวกลางในการส่งข้อมูลแบบไร้สาย เช่น คลื่นวิทยุ ไมโครเวฟ ดาวเทียม เป็นต้น (สุวัฒน์ บันลือ , 2548)

5. โปรโตคอล (Protocol) คือ กฎเกณฑ์ ระเบียบ หรือ ข้อปฏิบัติต่าง ๆ ที่กำหนดขึ้นมาเพื่อเป็นข้อตกลงที่ใช้สำหรับเป็นมาตรฐานในการกำหนดบทบาทหน้าที่ในการสื่อสารข้อมูลให้ถูกต้องตามกัน บทบาทสำคัญของโปรโตคอลก็เพื่อให้อุปกรณ์ทั้งสองฝั่งสามารถสื่อสารและเข้าใจตรงกัน เพื่อให้ผลของการสื่อสารระหว่างกันเป็นไปตามขั้นตอนที่ถูกต้อง
(โอภาส เอี่ยมสิริวงศ์, 2552)

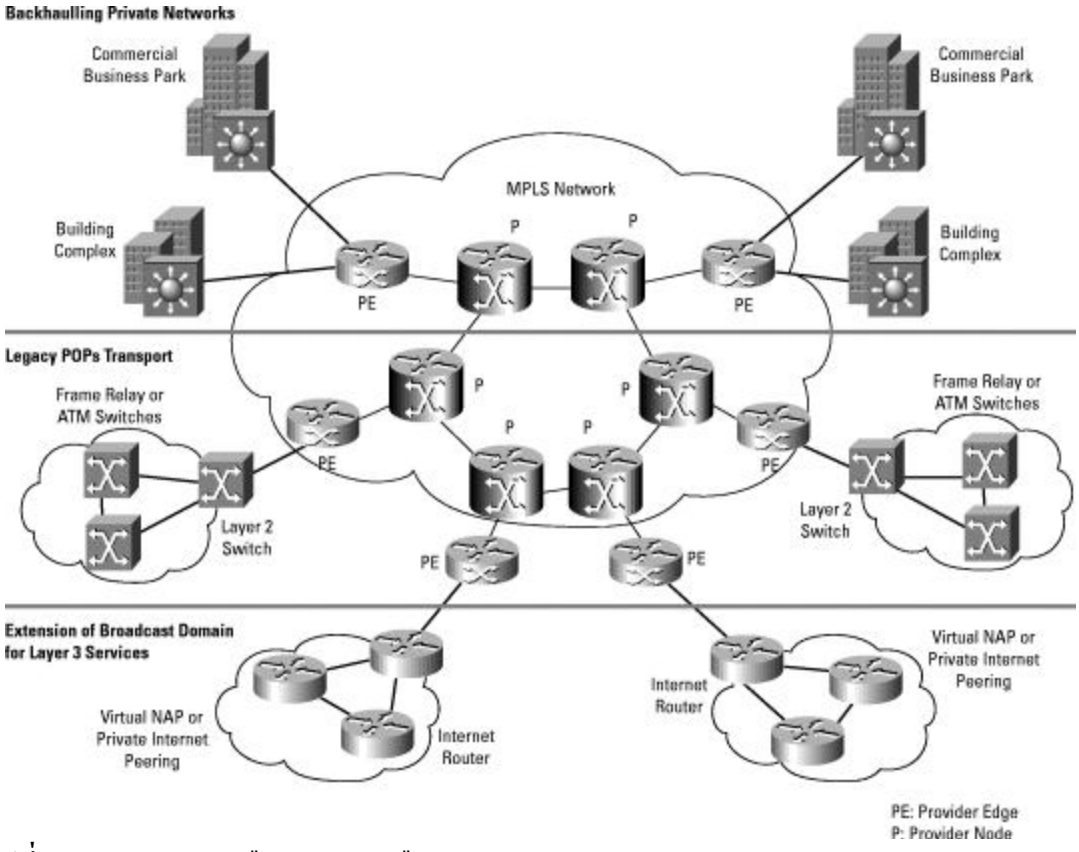
ประเภทของเครือข่าย (Categories of Networks) ในปัจจุบัน หากมีการกล่าวถึง คำว่าเครือข่าย ก็มักจะอ้างอิงถึงประเภทของเครือข่ายพื้นฐานทั้งสาม ซึ่งประกอบด้วย

(1) เครือข่ายท้องถิ่น (Local Area Network : LAN) เป็นเครือข่ายส่วนบุคคลที่มีการเชื่อมต่อ และ ครอบคลุมภายใต้พื้นที่และระยะทางที่จำกัด เช่น ภายในมหาวิทยาลัย หรือ ภายในอาคารที่อยู่ในบริเวณเดียวกัน ระบบเครือข่ายแลนอย่างง่ายสามารถทำการเชื่อมต่อเครื่องพีซีจำนวนสองเครื่องใช้ร่วมกันได้ ซึ่งอาจรวมถึงการมีเครื่องพิมพ์เพื่อใช้งานร่วมกัน ดังนั้นระบบแลนจึงเหมาะสำหรับการเชื่อมต่อเครื่องพีซี หรือไมโครคอมพิวเตอร์หลายๆ เครื่องเพื่อให้สามารถใช้ทรัพยากรร่วมกันได้แต่เนื่องจากระบบแลนถูกจำกัดด้วยขนาด ดังนั้นจึงสามารถใช้งานภายในพื้นที่หรือระยะทางไม่กี่กิโลเมตรซึ่งปกติจะเชื่อมต่อได้ไม่เกิน 10 กิโลเมตร แต่หากต้องการเชื่อมต่อระยะไกลขึ้นไปอีก ก็จำเป็นต้องใช้อุปกรณ์ทวนสัญญาณ (Repeater) แต่การยืดระยะทางที่ไกลออกไป ก็ต้องคำนึงถึงข้อจำกัดในระยะทางสูงสุดบวกกับจำนวนอุปกรณ์ทวนสัญญาณ ที่ใช้งานเครือข่ายด้วย (คมสัน คำบรรลือ ,2551)



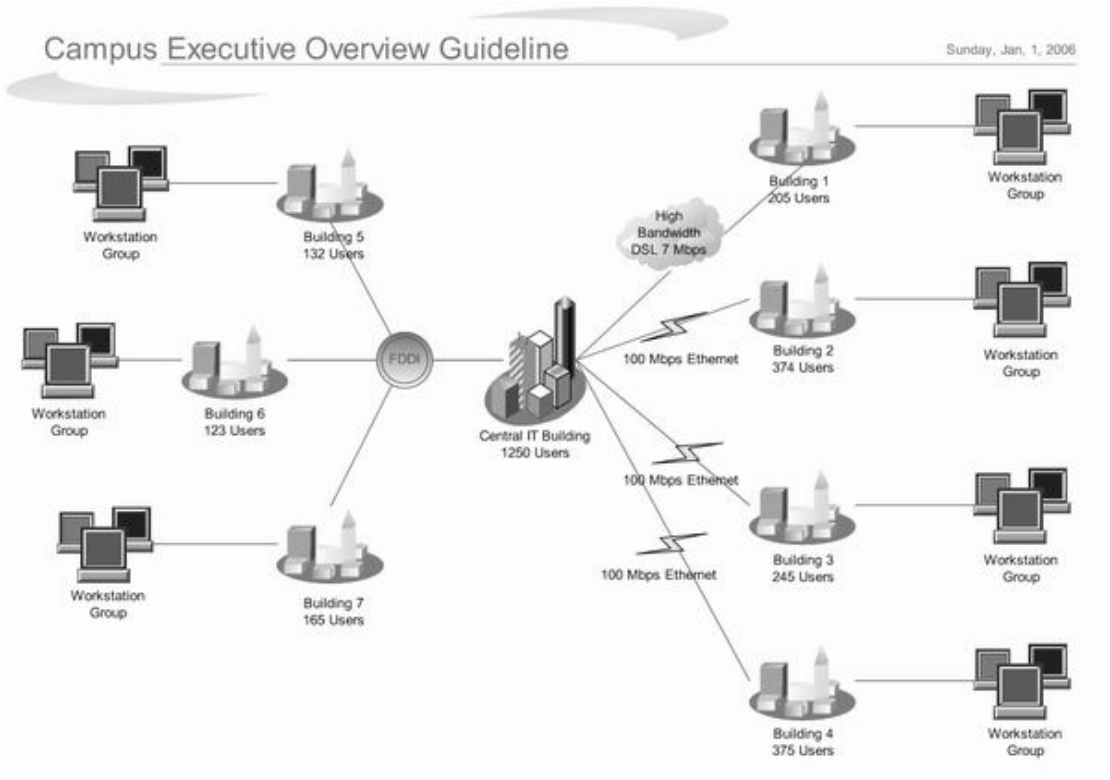
รูปที่ 2.1 แสดงระบบเครือข่ายท้องถิ่น

(2) เครือข่ายระบบเมือง (Metropolitan Area Network : MAN) เป็นเครือข่ายที่มีการเชื่อมต่อเครือข่ายแลนหลายๆ วงเข้าด้วยกัน ซึ่งครอบคลุมพื้นที่กว้างกว่าเครือข่ายแลน แต่เล็กกว่าแวน (WAN) โดยครอบคลุมระบบเมืองหรือจังหวัด ซึ่งจำเป็นต้องมีแบ็กโบน (Backbone) ที่ทำหน้าที่เป็นกระดูกสันหลัง หรือสายแกนหลักในการเชื่อมต่อเครือข่ายดังกล่าว ตัวอย่างเครือข่ายระดับเมือง เช่น บริษัทที่มีการเชื่อมต่อเครือข่ายของสาขาต่างๆ ที่อยู่ในเขตเมืองหรือจังหวัดเดียวกัน และ การบริการเคเบิลทีวี เป็นต้น



รูปที่ 2.2 แสดงระบบเครือข่ายระดับเมือง

(3) เครือข่ายระดับประเทศ (Wide Area Network: WAN) เป็นเครือข่ายระดับประเทศที่มีการเชื่อมต่อเครือข่ายต่าง ๆ หลายกลุ่มเข้าไว้ด้วยกัน ที่ครอบคลุมพื้นที่ระดับประเทศหรือข้ามทวีป โดยไม่มีข้อจำกัดในด้านระยะทาง เครือข่ายประเภทนี้มีการใช้ช่องทางการสื่อสารหลายรูปแบบด้วยกันตามความสะดวก เช่น สายโทรศัพท์ สายเคเบิล และดาวเทียม เป็นต้น



รูปที่ 2.3 แสดงระบบเครือข่ายแวน หรือ เครือข่ายระดับประเทศ

ลักษณะโครงข่ายการสื่อสารหลัก ๆ แบ่งออกได้ดังนี้

(1) แบบจุดต่อจุด (Point-to-point) เป็นการสื่อสารที่เชื่อมโยงแบบจุดต่อจุดหรือระหว่างจุดสองจุดเท่านั้น

(2) แบบลูป (Loop) หรือแบบวงแหวน (Ring) เป็นการสื่อสารที่เชื่อมโยงกันเป็นวงรอบ ได้ถูกออกแบบให้ใช้ Media Access Unit (MAU) ต่อรวมกันแบบเรียงลำดับเป็นวงแหวน แล้วจึงต่อคอมพิวเตอร์เข้ากับ MAU โดยใน 1 MAU จะสามารถต่อออกไปได้ถึง 8 สถานี

(3) แบบบัส (Bus) หรือแบบมัลติดรอบ (Multi drop) เป็นการสื่อสารที่เชื่อมโยงเข้ากับสายหลัก เป็นลักษณะของการนำเครื่องคอมพิวเตอร์มาเชื่อมต่อด้วยสายเคเบิลยาวต่อเนื่องกันไปเรื่อยๆ โดยมีคอนเนค็ดสเตอร์ในการเชื่อมต่อ มีข้อดีคือเสียค่าใช้จ่ายน้อย และสามารถขยายระบบได้ง่าย แต่มีข้อเสียคือเกิดข้อผิดพลาดได้ง่าย เนื่องจากทุกเครื่องคอมพิวเตอร์อยู่บนสายสัญญาณเพียงเส้นเดียว หากมีการขาดที่ตำแหน่งใดตำแหน่งหนึ่ง จะทำให้เครื่องอื่น ไม่สามารถใช้งานได้ตามไปด้วย

(4) แบบดาว (Star) เป็นการสื่อสารที่เชื่อมโยงกันแบบกระจายจากจุดศูนย์กลาง เป็นลักษณะการต่อเครือข่ายที่เครื่องคอมพิวเตอร์แต่ละตัวรวมเข้าสู่ศูนย์กลางสวิตซ์ เพื่อสลับตำแหน่งของเส้นทางของข้อมูลใด ๆ ในระบบ มีข้อดีคือสามารถติดตั้งและดูแลง่าย เนื่องจากมีโหนดกลาง

อยู่ตรงกลางเป็นตัวเชื่อมระบบ หากระบบเกิดทำงานบกพร่องเสียหาย จะสามารถแก้ไขปัญหาได้ง่าย อีกทั้ง หากสายที่เชื่อมต่อไปยังบางโหนกขาด โหนกที่เหลือก็ยังสามารถทำงานได้ แต่มีข้อเสีย คือ มีค่าใช้จ่ายสูง

(5) แบบตาข่าย (Mesh) เป็นการสื่อสารที่เชื่อมโยงกันแบบตาข่าย คือทุกจุดเชื่อมต่อถึงกันหมดแบบผสมผสาน (Hybrid Network) เป็นการสื่อสารที่เชื่อมโยงโดยอาศัยหลักการที่กล่าวมาแล้วข้างต้น ผสมกันตามความเหมาะสมของการใช้งาน คือจะมีเครือข่ายคอมพิวเตอร์ย่อยหลายๆ เครือข่ายเพื่อให้เกิดประสิทธิภาพสูงสุดในการทำงาน

อุปกรณ์ที่ใช้ในการสื่อสารข้อมูลคอมพิวเตอร์ มีหลายประเภท ทำหน้าที่ต่างกันไปดังนี้

(1) ฮับ หรือ รีพิตเตอร์ (Hub, Repeater) เป็นอุปกรณ์ที่ทวนและขยายสัญญาณเพื่อส่งต่อไปยังอุปกรณ์อื่นให้ได้ระยะที่ยาวไกลขึ้น ไม่มีการเปลี่ยนแปลงข้อมูลก่อนและหลังการรับ-ส่ง และไม่มีการใช้ซอฟต์แวร์ใด ๆ มาเกี่ยวข้องกับอุปกรณ์ชนิดนี้ การติดตั้งทำได้ง่าย แต่มีข้อเสียคือ ความเร็วในการส่งข้อมูลจะเฉลี่ยลดลงเท่ากันทุกเครื่อง เมื่อคอมพิวเตอร์มาเชื่อมต่อมากขึ้น จะทำให้ความเร็วในการส่งข้อมูลลดลงด้วย

(2) สวิทซ์ หรือ บริดจ์ (Switch , Bridge) เป็นอุปกรณ์สำหรับเชื่อมต่อ เครือข่ายท้องถิ่น (LAN) ประเภทเดียวกัน ใช้โปรโตคอลเดียวกันสองวงเข้าด้วยกัน ทั้งนี้สวิทซ์หรือบริดจ์ จะมีความสามารถในการเชื่อมต่อฮาร์ดแวร์และตรวจสอบข้อผิดพลาดของการส่งข้อมูลได้ด้วย โดยที่ความเร็วในการส่งข้อมูลมิได้ลดลงและติดตั้งง่าย

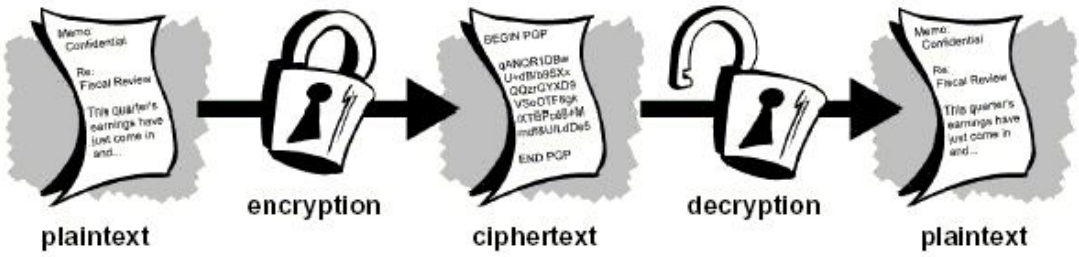
(3) เราเตอร์ (Router) เป็นอุปกรณ์ที่ทำงานคล้ายสวิทซ์ แต่จะสามารถเชื่อมต่อสื่อ หรือสายสัญญาณต่างชนิดกันได้ นอกจากนี้ยังช่วยเลือกหรือกำหนดเส้นทางที่จะส่งข้อมูลผ่าน และแปลงข้อมูลให้เหมาะสมกับการนำส่งแน่นอนว่าการติดตั้งจึงยุ่งยากมากขึ้น

(4) เกทเวย์ (Gateway) เป็นอุปกรณ์ที่มีความสามารถสูงสุดในการเชื่อมต่อเครือข่ายต่างๆ เข้าด้วยกัน โดยไม่มีข้อจำกัด เป็นอุปกรณ์ที่มีราคาแพง และติดตั้งยุ่งยาก บางครั้งจะรวมคุณสมบัติในการเป็นเราเตอร์ไว้ในตัวด้วยและอาจรวมเอาฟังก์ชันการทำงานด้านการรักษาความปลอดภัยที่เรียกว่า ไฟร์วอลล์ (Firewall) เข้าไว้ด้วย (http://www.udomsuksa.ac.th)

2.3 เทคโนโลยีการเข้ารหัสข้อมูลบนเครือข่าย

วัตถุประสงค์ในการเชื่อมโยงคอมพิวเตอร์เข้าเป็นเครือข่าย คือต้องการให้คอมพิวเตอร์สามารถสื่อสารและแลกเปลี่ยนข้อมูลระหว่างกันได้ เครือข่ายคอมพิวเตอร์เริ่มจากเครือข่ายขนาดเล็กภายในองค์กรที่เชื่อมโยงกันภายใต้สภาพพื้นที่จำกัดซึ่งเรียกว่า เครือข่ายเฉพาะที่ (Local Area Network : LAN) เมื่อเชื่อมเครือข่ายย่อยเข้าด้วยกันและขยายขอบเขตครอบคลุมพื้นที่

ระหว่างเมืองหรือระหว่างประเทศ ก็จะเรียกเครือข่ายนั้นว่า เครือข่ายพื้นที่กว้าง (Wide Area Network : WAN) ปัจจุบันได้มีการนำระบบเครือข่ายมาประยุกต์ใช้งานกันอย่างแพร่หลายและหลายรูปแบบตามความต้องการ ทำให้เกิดปัญหาของความไม่มั่นใจและความปลอดภัยของข้อมูลที่ทำการส่งผ่านไปบนเครือข่ายหรือการถูกคุกคามโดยตรง จากผู้ไม่ประสงค์ดีต่อองค์กร เหล่านี้ถือเป็นปัจจัยที่ทำให้ข้อมูลขององค์กรต้องเสี่ยงต่อการถูกคุมคามและก่อให้เกิดความเสียหาย ดังนั้นจึงมีการพัฒนารูปและระบบต่างๆ เพื่อทำการปกป้องหรือเพิ่มความมั่นใจได้ว่าข้อมูลที่ส่งผ่านไปบนเครือข่ายมีความปลอดภัยที่น่าเชื่อถือได้ อยู่หลากหลายวิธี การเข้ารหัสข้อมูลก็เป็นหนทางหนึ่งที่มีการนำมาใช้กันอย่างแพร่หลาย เทคโนโลยีการเข้ารหัส หรือวิธีกระบวนการทำให้ข้อมูลอยู่ในรูปแบบที่ไม่สามารถอ่านได้โดยผู้ที่ไม่มีสิทธิและผู้ที่มีสิทธิเท่านั้นที่จะสามารถอ่านข้อมูลนั้นได้ โดยใช้วิธีการนำข้อมูลเดิมที่เรียกว่า Plaintext หรือ Clear text มาผ่านวิธีหรือกระบวนการทางคณิตศาสตร์เพื่อแปลงรูปแบบของข้อมูลใหม่ ทำให้ไม่สามารถแปลความหมายของข้อมูลได้ วิธีการนี้เรียกว่า การเข้ารหัส (Encryption) เมื่อข้อมูลได้ผ่านวิธีหรือกระบวนการเข้ารหัสแล้ว ข้อมูลใหม่ที่ได้เรียกว่า (Cipher text) และเมื่อต้องการนำข้อมูลที่เข้ารหัสแล้วมาแปลงกลับให้เป็นข้อมูลแบบเดิมด้วยวิธีหรือกระบวนการทางคณิตศาสตร์ที่ตรงข้ามกับ การเข้ารหัส ซึ่งเรียกวิธีการนี้ว่า การถอดรหัส (Decryption) (ธารทิพย์ ตากเทิดเกียรติ์, 2549)



รูปที่ 2.4 แสดงวิธีหรือกระบวนการ เข้า – ถอดรหัสโดยทั่วไป

รูปแบบของการเข้ารหัส (Forms of Cryptography) สามารถแบ่งออกได้ตามลักษณะของการเข้ารหัสลับดังนี้ (ปรัชญา พันธุ์มี 2548)

การส่งข้อความลับระหว่างกัน 2 ฝ่ายโดยจะใช้วิธีการสับเปลี่ยนตำแหน่งของตัวอักษรแต่ละตัวในข้อความนั้น

การจัดเรียงตัวอักขระให้อยู่ในลักษณะที่ตรงกับตัวเลขที่ได้กำหนดไว้

การแปลงข้อความที่ประกอบด้วยการรวบรวมคำหรือถ้อยคำที่จำเป็นต้องนำมาใช้ในการถอดรหัสข้อความ

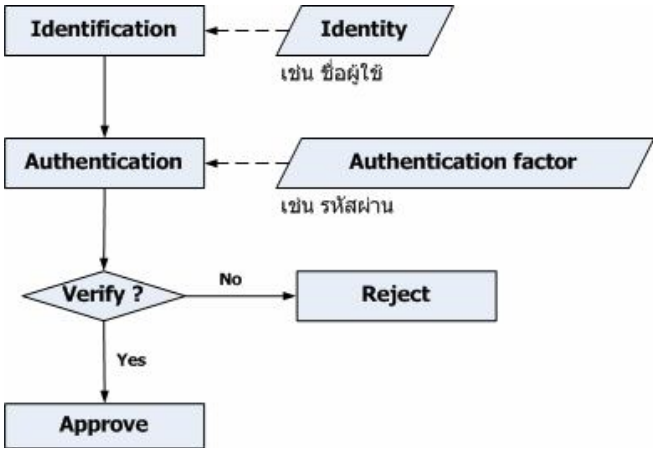
วิธีการเข้ารหัสลับที่ทั้งสองฝ่ายต้องใช้ Key

ในการเข้าและถอดรหัสตัวเดียวกัน โดยการแลกเปลี่ยน Key ระหว่างกันและเก็บ Key นั้นเป็นความลับ

วิธีการเข้ารหัสลับที่ใช้ Key 2 ตัวในการทำงานตัวหนึ่งใช้ในการเข้ารหัสเรียกว่า “Public Key”และอีกตัวหนึ่งใช้ในการถอดรหัสเรียกว่า “Private Key” ซึ่ง Key ทั้งสองตัวต้องมีความสัมพันธ์กันทางคณิตศาสตร์

2.4 การพิสูจน์ตัวตนบนเครือข่าย

การพิสูจน์ตัวตน คือขั้นตอนการยืนยันความถูกต้องของหลักฐานที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง โดยแบ่งออกเป็น 2 ขั้นตอน คือขั้นตอนแรกผู้ใช้จะทำการแสดงหลักฐานในการพิสูจน์ตัวตนต่อระบบหรือเรียกว่า ขั้นตอนการระบุตัวตน ขั้นต่อมาระบบจะทำการตรวจสอบหลักฐานที่ผู้ใช้นำมากล่าวอ้างหรือที่เรียกว่า ขั้นตอนการพิสูจน์ตัวตนหลังจากนี้ ระบบจะทำการตรวจสอบหลักฐาน ถ้าหลักฐานที่นำมากล่าวอ้างถูกต้องจึงอนุญาตให้เข้าสู่ระบบได้ หากหลักฐานที่นำมากล่าวอ้างไม่ถูกต้องผู้ใช้จะถูก ปฏิเสธจากระบบ (นฤชัย ศรีแสงอยู่ ,2547)



ภาพประกอบ 2.5 แสดงกระบวนการพิสูจน์ตัวตน

2.4.1 ส่วนประกอบของการพิสูจน์ตัวตน

ส่วนประกอบเบื้องต้นของการพิสูจน์ตัวตนสามารถแบ่งได้เป็น 3 ส่วนดังนี้

การพิสูจน์ตัวตน (Authentication) หมายถึง ขั้นตอนแรกของการเข้าใช้ระบบ ผู้เข้าใช้ระบบต้องถูกยอมรับจากระบบก่อนที่จะเข้าสู่ระบบได้ การพิสูจน์ตัวตนถือว่าเป็นการตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลนั้นจริง

การกำหนดสิทธิ์ (Authorization) หมายถึง ข้อจำกัดของบุคคลที่เข้ามาในระบบว่าบุคคลคนนั้นสามารถทำอะไรกับระบบได้บ้าง (ศาลทัส พัดฟูทรัพย์ศ์, 2549)

การบันทึกการใช้งาน (Accountability) หมายถึง การบันทึกรายละเอียดของการใช้ระบบ รวมถึงข้อมูลต่างๆที่ผู้ใช้กระทำลงไปในระบบ เพื่อผู้ตรวจสอบสามารถตรวจสอบได้ว่า ผู้ใช้ที่เข้ามาใช้บริการได้ทำการเปลี่ยนแปลงหรือแก้ไขข้อมูลในส่วนใดบ้าง

2.4.2 ประเภทของการพิสูจน์ตัวตน

จากส่วนประกอบข้างต้นของการพิสูจน์ตัวตนถือว่าเป็นปัจจัยสำคัญมากในการนำมาประยุกต์ใช้เพื่อการขอเข้าใช้บริการในระบบซึ่งสามารถแบ่งประเภทของการพิสูจน์ตัวตน (Authentication Types) ได้ดังนี้

ไม่มีการพิสูจน์ตัวตน (No Authentication) หมายถึง หลักการของการพิสูจน์ตัวตนสำหรับเงื่อนไข ของข้อมูลที่มีลักษณะเป็นข้อมูลสาธารณะ ที่อนุญาตให้ทุกคนเข้าใช้บริการและเปลี่ยนแปลงได้ หรือข้อมูลข่าวสารที่แหล่งของข้อมูลนั้นๆ สามารถเข้าถึงได้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น

การพิสูจน์ตัวตนโดยใช้รหัสผ่าน (Authentication by Passwords) หมายถึง รหัสผ่านที่จำกัดให้เฉพาะผู้ใช้ที่มีสิทธิเท่านั้น และเป็นวิธีการที่ใช้กันอย่างแพร่หลายแต่ยังไม่มีประสิทธิภาพมากพอที่จะรักษาความมั่นคงปลอดภัยให้กับระบบคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ เนื่องจากการตั้งรหัสผ่านที่ง่ายเกินไปของผู้ใช้และวิทยาการความก้าวหน้าทำให้รหัสผ่านสามารถถูกดักจับได้ระหว่างการสื่อสารผ่านทางเครือข่าย

การพิสูจน์ตัวตนโดยใช้ PIN (Authentication by PIN) หมายถึง PIN (Personal Identification Number) ที่เป็นรหัสลับส่วนบุคคลที่ ใช้เป็นรหัสผ่านเพื่อเข้าสู่ระบบที่ใช้กันแพร่หลายในปัจจุบัน คือการทำธุรกรรมทางด้านธนาคาร เช่นบัตรATM และ เครดิตการ์ดต่าง ๆ การใช้ PIN ทำให้มีความปลอดภัยในการสื่อสารข้ามระบบเครือข่ายสาธารณะมากขึ้น เนื่องจาก PIN จะถูกเข้ารหัสเอาไว้และจำเป็นต้องมีเครื่องมือที่สามารถถอดรหัสนี้ออกมาได้ เช่นฮาร์ดแวร์ที่ออกแบบมาโดยเฉพาะ และถูกติดตั้งไว้ในเครื่องของผู้รับและผู้ส่งเท่านั้น

การพิสูจน์ตัวตนโดยใช้ Password Authenticators หรือ Tokens หมายถึงAuthenticator หรือ Token ซึ่งเป็นฮาร์ดแวร์พิเศษที่ใช้สร้าง "รหัสผ่านที่เปลี่ยนแปลงได้ (Dynamic Password)"

ในขณะที่กำลังเข้าสู่ระบบเครือข่าย แบ่งออกเป็น 2 วิธี คือ ซิงโครนัส และ อะซิงโครนัส การพิสูจน์ตัวตนโดยใช้ลักษณะเฉพาะทางชีวภาพของแต่ละบุคคล (Authentication by Biometric traits) หมายถึง การนำลักษณะเฉพาะทางชีวภาพของแต่ละบุคคลมาใช้ในการพิสูจน์ตัวตน เพื่อเพิ่มความน่าเชื่อถือได้มากขึ้นเพราะลักษณะเหล่านี้ทำการลอกเลียนแบบกันไม่ได้ เช่นการใช้ลายนิ้วมือ เสียง ม่านตา เป็นต้น จึงมีการนำเทคโนโลยีนี้มาช่วยในการพิสูจน์ตัวตน เพื่อเพิ่มความปลอดภัยก่อนเข้าสู่ระบบ เช่นการใช้ควบคู่กับการใช้รหัสผ่าน

การพิสูจน์ตัวตนโดยใช้รหัสผ่านที่ใช้เพียงครั้งเดียว (One-Time Password : OTP) หมายถึง รหัสผ่านที่จะถูกเปลี่ยนทุกๆ ครั้งก่อนที่ผู้ใช้จะเข้าสู่ระบบเพื่อหลีกเลี่ยงปัญหาที่เกิดจากการใช้รหัสผ่านเพียงตัวเดียวซ้ำๆ กันวิธีนี้จะทำให้ระบบมี ความปลอดภัยมากขึ้น การทำงานของ OTP คือเมื่อผู้ใช้ต้องการจะเข้าใช้ระบบผู้ใช้จะทำการร้องขอไปยังเซิร์ฟเวอร์ จากนั้นเซิร์ฟเวอร์จะส่งChallenge Stringกลับมาให้ผู้ใช้ จากนั้นผู้ใช้จะนำ Challenge String และรหัสลับที่มีอยู่กับตัวของผู้ใช้นำไปเข้า แฮชฟังก์ชันแล้วออกมาเป็นค่า Response ผู้ใช้ก็จะส่งค่านั้นกลับไปยังเซิร์ฟเวอร์ เซิร์ฟเวอร์จะทำการตรวจสอบค่าที่ผู้ใช้ส่งมาเปรียบเทียบ กับค่าที่เซิร์ฟเวอร์คำนวณเองได้ โดยเซิร์ฟเวอร์จะใช้วิธีการคำนวณเดียวกับฝั่งผู้ใช้ เมื่อได้ค่าที่ตรงกันเซิร์ฟเวอร์ก็จะยอมรับให้ผู้ใช้เข้าสู่ระบบ- การพิสูจน์ตัวตนโดยการเข้ารหัสโดยใช้กุญแจสาธารณะ (Public-key Cryptography) หมายถึง การเข้ารหัสข้อมูลโดยใช้ กุญแจ (Key) ในการทำงาน 2 ตัวหรือเรียกว่า การเข้ารหัสแบบคู่รหัสกุญแจ โดยกุญแจตัวหนึ่งเรียกว่า กุญแจสาธารณะ (Public Key) ใช้ในส่วนของการเข้ารหัสข้อความและอีกตัวหนึ่งเรียกว่ากุญแจส่วนตัว (Private Key) ใช้ในส่วนของการถอดรหัสข้อความ โดยตัวกุญแจสาธารณะจะถูกเผยแพร่ให้กับผู้อื่น ส่วนกุญแจส่วนตัวจะถูกเก็บไว้กับเจ้าของ แนวคิดของการเข้ารหัสแบบกุญแจสาธารณะ ใช้หลักคณิตศาสตร์ที่เรียกว่า ฟังก์ชันทางเดียว (One – Way Function) ซึ่งมีความเกี่ยวข้องกับตัวเลขจำนวนเฉพาะ (Prime Number) คือถ้าเอาจำนวนเฉพาะสองจำนวนมาคูณกันแล้วเอาผลคูณที่ได้มาทำการหาตัวประกอบย้อนกลับ ในกรณีตัวเลขมีขนาดใหญ่มากๆ ก็จะทำให้หาตัวประกอบยากและใช้เวลาคำนวณมากขึ้นด้วย จากตรงจุดนี้จึงนำสมบัติในข้อนี้มาใช้ในการเข้ารหัสลับ คนแรกที่คิดเรื่องนี้คือ WhitfieldDiffie และ Martin Hellman โดยพวกเขาได้นำเสนอใน National ComputerConference เมื่อ ปี 1976 ซึ่งได้รับการยอมรับกันโดยทั่วไป และถูกนำมาใช้เป็นหลักการพื้นฐานในการสร้างกุญแจ สำหรับการเข้าและถอดรหัสข้อมูลในปัจจุบัน

การพิสูจน์ตัวตนโดยการใช้ลายเซ็นอิเล็กทรอนิคส์ (Digital Signature) หมายถึงลายมือชื่อดิจิทัล เป็นเทคนิคที่นำมาใช้เพื่อวัตถุประสงค์เดียวกันกับการเซ็นชื่อหรือการลงลายมือชื่อแบบเดิมคือใช้ในการตรวจสอบความถูกต้องของข้อความต้นฉบับรวมถึงการยืนยันของตัวบุคคลว่าบุคคลใดได้รับหรือส่งข้อความดังกล่าวจริง ซึ่งแตกต่างจากการลงลายมือชื่อแบบเดิมๆ ที่ง่ายต่อการ

ปลอมแปลงและไม่สามารถทำ การตรวจสอบและยืนยันข้อเท็จจริงต่างๆ ได้ประกอบด้วย 2 ขั้นตอนคือ Digital Signature Creation เป็นกระบวนการสร้างลายมือชื่อดิจิทัล Digital Signature Verification เป็นกระบวนการพิสูจน์ลายมือชื่อดิจิทัล เพื่อตรวจสอบว่าข้อความที่ได้รับถูกแก้ไขระหว่างการส่งข้อมูลหรือไม่

การพิสูจน์ตัวตนโดยใช้การถาม - ตอบ (Zero-Knowledge Proofs) หมายถึง การที่จะทำให้ระบบมั่นใจได้ว่า ผู้ที่เข้าไปในระบบผู้นั้นเป็นผู้ที่ได้รับอนุญาตจริงนั่นก็คือ ระบบจะใช้การถาม - ตอบ ซึ่งคำถามและคำตอบเหล่านี้ ผู้ใช้จะเป็นคนสร้างคำถามและคำตอบขึ้นมาเอง จากนั้นจะส่งให้กับเซิร์ฟเวอร์ ซึ่งคำถาม

คำตอบที่ผู้ใช้สร้างขึ้นมา ผู้ใช้เท่านั้นจะเป็นคนที่ทราบคำตอบของแต่ละคำถามที่ถูกสร้างและเมื่อผู้ใช้คนนั้นๆ เข้าสู่ระบบได้ ระบบจะถามสุ่มคำถามเหล่านั้นที่ผู้ใช้คนนั้นๆ สร้างขึ้นมาถามผู้ใช้คนนั้นๆ ก่อนที่จะยอมให้เข้าใช้ระบบได้จริงการให้ใช้ระบบได้จริงจะได้รับการยินยอมก็ต่อเมื่อการตอบคำตอบที่ผู้ใช้ตอบนั้นสัมพันธ์กับคำตอบที่มีอยู่ในเซิร์ฟเวอร์ วิธีการพิสูจน์ตัวตนแบบนี้ เป็นวิธีการที่ต้องใช้ความรู้ขั้นสูงในการนำมาใช้เนื่องจากระบบจะใช้การเรียนรู้จากข้อมูลที่ได้รับ หรืออาจจะเรียกได้ว่าเป็นการนำความรู้ด้าน Artificial Intelligence มาใช้ควบคู่ด้วย (นริสสรา ศรีมูลชัย , 2549)

2.5 โปรโตคอลในการพิสูจน์ตัวตน

จากยุคเริ่มต้นการใช้งานในระบบเครือข่ายจำเป็นต้องใช้ฮาร์ดแวร์ประเภทเดียวกันจึงจะสามารถทำงานร่วมกันได้อย่างกลมกลืน แต่ต่อมาเมื่อมีเทคโนโลยีเครือข่ายเพิ่มขึ้นเช่น อินเทอร์เน็ตและโทเค็นริง ปัญหาที่เกิดขึ้นคือจะเชื่อมเครือข่ายต่างเทคโนโลยีเข้าด้วยกันได้อย่างไร โดยไม่จำกัดว่าคอมพิวเตอร์จะอยู่ในเครือข่ายเดียวกัน ดังนั้นจำเป็นต้องมีข้อตกลงหรือข้อกำหนดที่ใช้ร่วมกันระหว่างเทคโนโลยีที่ต่างกันให้สื่อสารกันได้ ข้อกำหนดนี้เรียกกันโดยทั่วไปว่า โปรโตคอล (Protocol) ซึ่งหมายถึง ข้อกำหนดการสื่อสารระหว่างคอมพิวเตอร์หรืออุปกรณ์เครือข่าย โดยจะมีซอฟต์แวร์ที่ปฏิบัติงานตามโปรโตคอลที่กำหนด พร้อมทั้งมีกรรมวิธีแก้ไขปัญหาที่เกิดขึ้น เช่น หากข้อมูลที่ขนถ่ายมีข้อผิดพลาด ซอฟต์แวร์ที่เกี่ยวข้องในคอมพิวเตอร์นั้นๆ จะดำเนินการตามแบบแผนในโปรโตคอล เช่นส่งข้อมูลซ้ำใหม่ หรือในระบบเครือข่ายขนาดใหญ่อาจมีเส้นทางเชื่อมโยงระหว่างกันได้เป็นจำนวนมาก ข้อมูลที่ส่งออกไปอาจไม่ได้ใช้เส้นทางเดียวกันตลอด ข้อมูลที่ส่งออกไปก่อนอาจไปถึงปลายทางช้ากว่า กรณีนี้เครื่องปลายทางจำเป็นต้องจัดลำดับข้อมูลใหม่และกรณีที่คอมพิวเตอร์ต้นทางสามารถส่งข้อมูลได้เร็วเกินกว่าปลายทางจะรับได้ทัน โปรโตคอลจะกำหนดกรรมวิธีควบคุมการลำเลียงข้อมูลระหว่างต้นทางและปลายทางให้สัมพันธ์กันการใช้

โปรโตคอลในการพิสูจน์ตัวตนก็เป็นทางเลือกหนึ่งที่มีการนำมาประยุกต์ใช้กับระบบงานในองค์กรอย่างแพร่หลายเพราะการพิสูจน์ตัวตนถือว่าเป็นกระบวนการเริ่มต้นและมีความสำคัญที่สุดในการปกป้องเครือข่ายให้ปลอดภัย เพราะเป็นโปรโตคอลการสื่อสารที่มีกระบวนการพิสูจน์ตัวตนรวมอยู่ในชุดโปรโตคอลเอง ที่นิยมใช้ในปัจจุบันอย่างแพร่หลาย เช่น

Secure Socket Layer (SSL) เป็นโปรโตคอลระดับแอพพลิเคชันหรือ Hypertext Transfer Protocol (HTTP) ซึ่งเป็นการสื่อสารผ่านทางเว็บให้ปลอดภัยพัฒนาในช่วงต้นของยุคการค้าอิเล็กทรอนิคส์กำลังได้รับความนิยมในโลกอินเทอร์เน็ตโดย Netscape Communications หลักในการทำงานระหว่างไคลเอ็นต์และเซิร์ฟเวอร์จะอนุญาตให้มีกระบวนการพิสูจน์ตัวตนรวมกับการใช้งานลายเซ็นดิจิตอลสำหรับการรักษาความถูกต้องของข้อมูลและการเข้ารหัสข้อมูลเพื่อป้องกันความเป็นส่วนตัวระหว่างการสื่อสารข้อมูล อีกทั้งยังอนุญาตให้สามารถเลือกวิธีการในการเข้ารหัสวิธีสร้างไดเจสต์ และลายเซ็นดิจิตอล ได้อย่างอิสระก่อนการสื่อสารจะเริ่มต้นขึ้น ตามความต้องการของทั้งเว็บเซิร์ฟเวอร์และบราวเซอร์

โปรโตคอลติดต่อสื่อสารโดยใช้การพิสูจน์ตัวตนรวมกับลายเซ็นดิจิตอล (Secure Shell) เป็นและมีการเข้ารหัสการสื่อสาร ตรงกันข้ามกับการสื่อสารแบบเก่า เช่น เทลเนต (Telnet) อีกทั้งโปรโตคอล SSH ยังสนับสนุนการพิสูจน์ตัวตนของทั้งเซิร์ฟเวอร์และ ไคลเอ็นต์ในขั้นตอนการแลกเปลี่ยนกุญแจด้วย กล่าวคือในขั้นตอนการแลกเปลี่ยนกุญแจนั้น ทั้งไคลเอ็นต์และเซิร์ฟเวอร์จะสร้างคู่รหัสกุญแจ ประกอบไปด้วยกุญแจสาธารณะและกุญแจส่วนตัว ซึ่งกุญแจส่วนตัวของทั้งไคลเอ็นต์และเซิร์ฟเวอร์นี้เองที่ใช้ในการพิสูจน์ตัวตนได้ตามหลักการพิสูจน์ตัวตนด้วยวิธีการใช้กุญแจสาธารณะ ถ้าตรวจสอบได้ว่ามีการส่งข้อมูลด้วยกุญแจที่เปลี่ยนไปจากเดิมอาจจะแสดงได้ว่าการสื่อสารนี้ไม่ปลอดภัยแล้วปัจจุบันมีซอฟต์แวร์ที่สนับสนุนการทำงานตามโปรโตคอล SSH ให้เลือกใช้มากอาทิ เช่น โอเพนเอสเอสเอช (OpenSSH) จากผู้พัฒนาโอเพนบีเอสดี (OpenBSD) ในระบบปฏิบัติการตระกูลยูนิกซ์ส่วนในตระกูลวินโดวส์เช่นโปรแกรมพุตตี้ (Putty) หรือ Window SSH Secure Shell การสื่อสารด้วยโปรโตคอล SSH สนับสนุนการเข้ารหัสการสื่อสาร และการพิสูจน์ตัวตนดีในองค์กรคือการเปลี่ยนมาใช้การสื่อสารด้วย SSH แทนการสื่อสารแบบเดิมเช่นการใช้ RUtilities เช่น rlogin หรือ rcp บนตระกูลยูนิกซ์และการใช้งาน telnet และที่สำคัญคือการใช้งาน ftp ควรจะเปลี่ยนมาใช้งานโปรแกรม WinSCP แทนในการแลกเปลี่ยนไฟล์เป็นต้น (ยุทธนา ไชยสัตย์ , 2548)

Internet Security (IPsec) เป็นส่วนเพิ่มขยายของไอพี (Intrnet Protocol) ในชุดโปรโตคอล TCP/IP พัฒนาขึ้นเพื่อเป็นส่วนหนึ่งของมาตรฐาน IPv6 ซึ่งเป็นโปรโตคอลที่พัฒนาเพื่อใช้แทน IPv4 ที่ใช้ในปัจจุบันและกำหนดหมายเลข RFC เป็น RFC2401 IPsec มีการใช้

โปรโตคอล 2 ชุดคือ Authentication Header (AH) และ Encapsulated Security Payload (ESP) เพื่อรองรับการพิสูจน์ตัวตน, การรักษาความถูกต้องของข้อมูล และการรักษาความลับ ในระดับชั้นของ IP และการรักษาความถูกต้องของข้อมูลของ IP ดาตาแกรม (IP Datagram) ในชุดโปรโตคอล IPsec ใช้ Hash MessageAuthentication Codes หรือ HMAC ด้วยฟังก์ชันแฮช เช่น MD5 หรือ SHA-1 ทุกครั้งที่มีการส่งแพ็กเก็ตจะมีการสร้าง HMAC และใช้การเข้ารหัสไปด้วยทุกครั้งเพื่อให้ปลายทางสามารถตรวจสอบได้ตามหลักการลายเซ็นดิจิตอลว่าต้นทางเป็นผู้ส่งแพ็กเก็ตนั้นมาจริง ส่วนการรักษาความลับของข้อมูลนั้น จะใช้การเข้ารหัส IP ดาตาแกรมด้วยวิธีการเข้ารหัสด้วยกุญแจสมมาตรด้วยวิธีการมาตรฐานที่เป็นรู้จักกันดีเช่น3DES หรือ AES เป็นต้น แต่ปัญหาหนึ่งของ IPsec คือการส่งกุญแจที่ใช้ในการเข้ารหัสไปกับแพ็กเก็ต ซึ่งจัดว่าไม่ปลอดภัยนอกจากนี้การแลกเปลี่ยนกุญแจนำไปสู่ปัญหาของการดูแลระบบที่ใช้ IPsec เพราะทั้งระบบต้องสนับสนุนการใช้งานโปรโตคอล IPsec เดียวกัน จะทำอย่างไรให้สามารถส่งกุญแจในการเข้ารหัสไปกับแพ็กเก็ตถ้าไม่มีการเข้ารหัสแพ็กเก็ตแต่อย่างใด เพื่อแก้ปัญหาจึงได้พัฒนาโปรโตคอลในการแลกเปลี่ยนกุญแจหรือ Internet Key Exchange Protocol คือจะทำการพิสูจน์ตัวตน ของปลายทางก่อนการสื่อสารในขั้นตอนถัดมาจึงสามารถแลกเปลี่ยนและตกลง กุญแจในการเข้ารหัสได้ด้วยวิธีการแลกเปลี่ยนกุญแจตามวิธีการแลกเปลี่ยนกุญแจด้วยการใช้กุญแจสาธารณะเช่น Diffie-Hellmann เป็นต้น ซึ่งชุดโปรโตคอล IKE จะตรวจสอบกุญแจที่ใช้ในการเข้ารหัสระหว่างการติดต่อสื่อสารเป็นระยะตลอดการสื่อสารข้อมูลที่เกิดขึ้นแต่ละครั้ง

Kerberos เป็นเครื่องมือในการพิสูจน์ตัวตนของผู้ใช้ บนระบบเครือข่าย เนื่องจาก Kerberos เป็นโปรโตคอลตัวหนึ่งที่ใช้ในการพิสูจน์ตัวตนบนระบบเครือข่าย ที่มีการเพิ่มความสะดวกและความปลอดภัยในการพิสูจน์ตัวตนได้มากขึ้นเพราะว่าเป็นระบบการเข้าถึงการใช้บริการของระบบทั้งหมดได้ด้วยการพิสูจน์ตัวตนเพียงครั้งเดียวและ Kerberos ยังมีการใช้ Ticket แทนการพิสูจน์ตัวตนแบบเดิมๆ ที่ส่งรหัสผ่านที่ไม่มีการเข้ารหัสไปบนระบบเครือข่าย เพื่อใช้ในการแก้ปัญหาความไม่ปลอดภัยของการพิสูจน์ตัวตนแบบเดิมที่มีการส่งรหัสผ่านบนเครือข่ายโดยที่ไม่มีการเข้ารหัสข้อมูล ซึ่งทำให้ข้อมูลรหัสผ่านอาจถูกดักจับได้ ระบบ Kerberos ประกอบด้วยสองส่วนหลักคือ Ticket ใช้สำหรับการพิสูจน์ตัวตนของผู้ใช้ในระบบ และการเข้ารหัสข้อมูล และ Authenticator ใช้ในการตรวจสอบ Ticket ว่าเป็นผู้ใช้คนเดียวกันที่ใช้ Ticket เพื่อขอสิทธิในการเข้าสู่ระบบและเป็นผู้ใช้ที่ระบบสร้างให้อย่างถูกต้อง

แต่อย่างไรก็ดี ปัญหาสำคัญของการใช้ระบบ Kerberos คือการขยายระบบ เนื่องจากเซิร์ฟเวอร์ Kerberos ต้องเก็บกุญแจของผู้ใช้ทุกคนที่เข้ามาในระบบ ถ้าระบบใหญ่มากขึ้น มีการ

กระจายตัวมากกว่าหนึ่งจุด ย่อมส่งผลเสียต่อการใช้งานระบบโดยรวม แต่การนำระบบ Kerberos มาใช้จะเพิ่มความสะดวกในการพิสูจน์ตัวตนได้มากขึ้น (ธีระ โชคพระสมบัติ ,2550)

2.6 การเทียบเวลาสากล

เนื่องด้วยการประกาศใช้ พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เมื่อวันที่ 18 มิถุนายน 2550 ส่งผลให้ผู้ใช้งานคอมพิวเตอร์ รวมทั้งผู้ดูแลระบบเครือข่ายและคอมพิวเตอร์จำเป็นต้องปฏิบัติตนให้สอดคล้องกับพระราชบัญญัติ ดังกล่าว เนื้อหาส่วนหนึ่งของพระราชบัญญัติ ได้ระบุถึงความหมายของข้อมูลจราจรทางคอมพิวเตอร์ ดังนี้

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

นอกจากนี้ใน พระราชบัญญัติ ยังระบุถึงความสำคัญของข้อมูลจราจรทางคอมพิวเตอร์ที่ใช้เป็นหลักฐานในการดำเนินคดีที่เกี่ยวข้องกับการกระทำผิดเกี่ยวกับคอมพิวเตอร์และในเนื้อหาของมาตราที่ 26 ซึ่งเป็นส่วนที่บังคับให้ผู้ให้บริการต้องปฏิบัติตามในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ โดยมีเนื้อหาดังนี้

มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการ ผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะราย และเฉพาะคราวก็ได้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการ นับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง

ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

หลังจากการประกาศใช้ พระราชบัญญัติ ข้างต้น กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้ประกาศใช้ หลักเกณฑ์ในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 เพื่อเป็นแนวทางปฏิบัติสำหรับผู้ให้บริการประเภทต่างๆ ดำเนินการเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ให้สอดคล้องกับ พระราชบัญญัติ กระทำความผิดเกี่ยวกับคอมพิวเตอร์ โดยเนื้อหาในประกาศตอนหนึ่งระบุไว้ว่า

ข้อ ๙ เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริงผู้ให้บริการต้องตั้งนาฬิกา ของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

จากประกาศข้างต้นนี้ทำให้ผู้ให้บริการจำเป็นต้องเทียบเวลาจากเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน 10 มิลลิวินาที ซึ่งต่อไปนี้จะกล่าวถึงความรู้พื้นฐานของการเทียบเวลาการเชื่อมต่อของอินเทอร์เน็ตที่เรียกว่า Network Time Protocol (NTP) และกล่าวถึงการประยุกต์ใช้ NTP ในอุปกรณ์บริการ และเครื่องลูกข่ายของระบบเพื่อให้ระบบสารสนเทศขององค์กรมีความสอดคล้องกับพระราชบัญญัติ และประกาศดังกล่าว Network Time Protocol (NTP) เป็นที่เข้าใจกันดีแล้วว่าอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์เครือข่าย ต่างๆ ในระบบสารสนเทศนั้นมีความสามารถของการรักษาความเที่ยงตรง และแม่นยำของเวลาได้แตกต่างกัน ทั้งนี้ขึ้นอยู่กับปัจจัยหลายด้าน เช่น วัสดุที่ให้สร้างวงจรเวลาของอุปกรณ์คอมพิวเตอร์, อุณหภูมิ, ความชื้น, คลื่นแม่เหล็กไฟฟ้า หรือ ความสม่ำเสมอของพลังงานที่จ่ายให้กับวงจรเวลา เป็นต้น ส่งผลให้อุปกรณ์ต่างกันอาจจะให้ค่าเวลาที่แตกต่างกัน

หากอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์เครือข่ายในระบบสารสนเทศมีค่าเวลาที่แตกต่างกันแล้วนั้นจะส่งผลให้เกิดปัญหากับผู้ใช้งาน รวมทั้งผู้ดูแลระบบในการปฏิบัติงานต่างๆ เช่น

ความคาดเคลื่อนของเวลาในการการแจ้งปัญหาของระบบสารสนเทศ ระหว่างผู้ใช้งานและผู้ดูแลระบบ

ความสับสนในการตรวจสอบ และวิเคราะห์เหตุการณ์ต่างๆ เช่น เหตุการณ์การบุกรุก เหตุการณ์ของปัญหาด้านเครือข่าย หรือระบบคอมพิวเตอร์

ผู้พัฒนามีความสับสนในเวอร์ชันของโค้ดระหว่างการพัฒนา

มีการใช้งานไฟล์ข้อมูล หรือฐานข้อมูล ที่ซ้อนทับกัน

จากตัวอย่างปัญหาข้างต้นจะเห็นว่าผู้ดูแลระบบและผู้ใช้งานระบบสารสนเทศมีความจำเป็นต้องทำให้อุปกรณ์คอมพิวเตอร์ และอุปกรณ์เครือข่ายของระบบสารสนเทศในองค์กรมีค่าเวลาเที่ยงตรง และแม่นยำเหมือนกัน

Network Time Protocol (NTP) เป็นโพรโตคอลในระดับ Application Layer ของระบบเครือข่ายแบบ TCP/IP ที่ทำหน้าที่ในการเทียบเวลาระหว่างอุปกรณ์คอมพิวเตอร์ ซึ่งอ้างอิงจาก RFC หมายเลข RFC 778, RFC 891, RFC 956, RFC 958, และ RFC 1305 การทำงานของโพรโตคอลชนิดนี้จะต้องอาศัยเครื่องให้บริการที่เปิดพอร์ตหมายเลข 123 ชนิด UDP ในการรอรับข้อมูลร้องขอการเทียบเวลาจากเครื่องลูกข่าย

ลักษณะการแจกจ่ายเวลาของ NTP นั้นจะอยู่ในรูปแบบลำดับชั้น ที่เรียกว่า “Clock Strata” โดยแบ่งลำดับชั้นของการเทียบเวลาดังนี้

Stratum 0

เป็นอุปกรณ์ของแหล่งกำเนิดเวลา เช่น Atomic clocks, GPS เป็นต้น ซึ่งอุปกรณ์แต่ละชนิดมีข้อดีและข้อเสียแตกต่างกัน เช่น การประยุกต์ใช้GPS จะมีต้นทุนที่ต่ำกว่า Atomic clock มาก แต่จะมีเสถียรภาพที่น้อยกว่า หากสภาพอากาศไม่เหมาะสม GPS จะไม่สามารถรับสัญญาดาวเทียมได้ เป็นต้น

Stratum 1

เป็นเครื่องคอมพิวเตอร์แม่ข่ายที่เชื่อมต่อกับ stratum 0 ได้รับค่าเวลามาจาก stratum 0 โดยตรงผ่านการเชื่อมต่อในระบบคอมพิวเตอร์ เช่น RS-232 เป็นต้น

Stratum 2

เป็นเครื่องคอมพิวเตอร์ที่ร้องขอการเทียบเวลาจากเครื่องคอมพิวเตอร์แม่ข่าย stratum 1 ผ่านระบบเครือข่าย TCP/IP ด้วยการใช้งาน NTP เครื่องคอมพิวเตอร์ในระดับนี้อาจจะร้องขอการเทียบเวลาจาก stratum 1 ได้มากกว่า 1 แหล่งเพื่อรองรับการทำงานแบบทดแทนกันเมื่อไม่สามารถเข้าถึง stratum 1 ตัวใดตัวหนึ่งก็จะสามารถร้องขอการเทียบเวลาจาก stratum 1 ตัวอื่นได้ต่อไป

นอกจากนี้เครื่องคอมพิวเตอร์ใน stratum 2 สามารถเทียบเคียงเวลาระหว่างกันแบบ peer-to-peer เพื่อรักษาเวลาให้เทียบเท่ากันในระดับเดียวกัน

Stratum 3

เป็นเครื่องคอมพิวเตอร์ที่ร้องขอการเทียบเวลาจากเครื่องคอมพิวเตอร์แม่ข่าย stratum 2 ผ่านระบบเครือข่าย TCP/IP ด้วยการใช้งาน NTP เครื่องคอมพิวเตอร์ในระดับนี้จะสามารถอ้างอิง stratum 2 ได้มากกว่า 1 แหล่ง และสามารถทำงานในรูปแบบ peer-to-peer ได้เช่นเดียวกัน NTP นั้นสามารถรองรับระดับของการเทียบเวลาได้ถึง 16 ระดับ

4.5.1 ใช้คำสั่งเพื่อให้ ntp ทำงานด้วยคำสั่ง นระบบปฏิบัติการ FreeBSD version 8 การติดตั้ง NTP Server เพื่ออ้างอิงเวลาสากล stratum 0 ในไทย

เมื่อ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีผลบังคับใช้แล้ว เราในฐานะผู้ให้บริการ ควรมีการกำหนดเวลาของเครื่อง Server ให้ตรงกับเวลามาตรฐนสากล Stratum 0 ในประเทศไทยเราอ้างอิงกับ nectec.or.th

การติดตั้ง NTP SERVER

cd /usr/ports/net/ntp

make install

nano /etc/ntp.conf

พิมพ์คำสั่งต่อไปนี้

server clock.nectec.or.th prefer

server clock2.nectec.or.th

server clock.thaicert.nectec.or.th

server time2.nimt.or.th

server time3.nimt.or.th

nano /etc/rc.conf

(เพิ่ม)

ntpdate_enable="YES"

จากนั้นให้ reboot ด้วยคำสั่ง

reboot

nano /etc/crontab เพิ่มคำสั่งด้านล่างสุด สั่งให้ update ทุก 6 ชม.

0 */6 * * * /usr/sbin/ntpdate -u clock.nectec.or.th > /dev/null

บันทึกไฟล์ และออกจากการแก้ไข

ก่อนเริ่มการทำงานของ ntpd ควรใช้คำสั่ง ntpdate กับ Time Server ที่กำหนดใน ntp.conf ก่อนเพื่อให้เวลาใน client และ Time Server มีค่าใกล้เคียงกัน

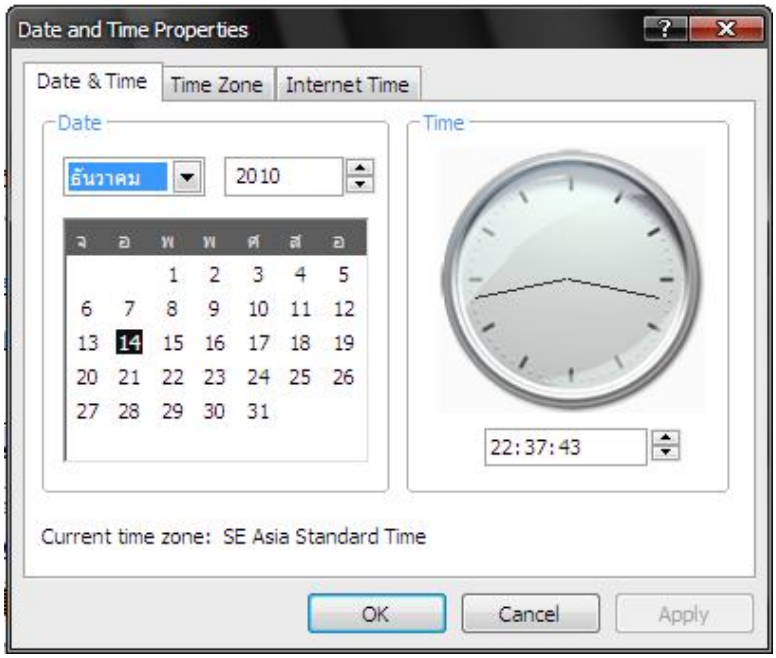
เริ่มการทำงานของโปรแกรม ntpd ด้วยคำสั่ง

ntpd

การใช้บริการ Time Server ในระบบปฏิบัติการ Windows

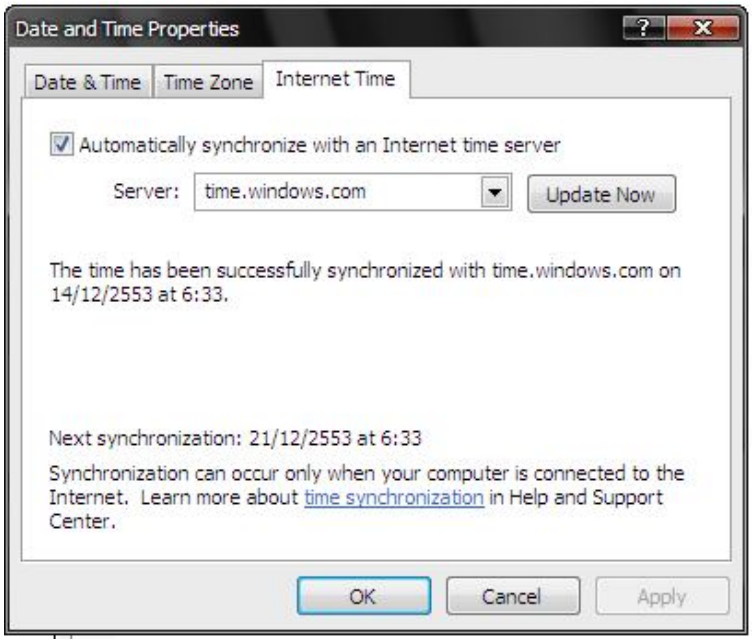
ในระบบปฏิบัติการ Windows XP Service Pack 2 , Windows Vista และ Windows 2003 Server จะมีโปรแกรมสำหรับการเทียบเวลาที่ติดตั้งมาพร้อมระบบปฏิบัติ โดยมีขั้นตอนการใช้งานดังแสดงตัวอย่างของ Windows XP Service Pack 2 ดังนี้

Double Click พื้นที่ของวันเวลาบน Task Bar ในตำแหน่งมุมขวาล่าง จะปรากฏโปรแกรม Clock ดังรูป



รูปที่ 2.5 แสดงการใช้บริการ Time zone ในระบบปฏิบัติการ Windows

เลือก Internet Time Tab และเลือก check box “Automatically synchronize with an Internet time server” และเพิ่มค่า Server เป็น clock.thaicert.org และกดปุ่ม Update Now จะได้ผลดังรูป



รูปที่ 2.6 แสดงการใช้บริการ Time Server ในระบบปฏิบัติการ Windows

หลังจากตั้งค่าเสร็จให้กดปุ่ม OK เพื่อยืนยันการตั้งค่าดังกล่าว

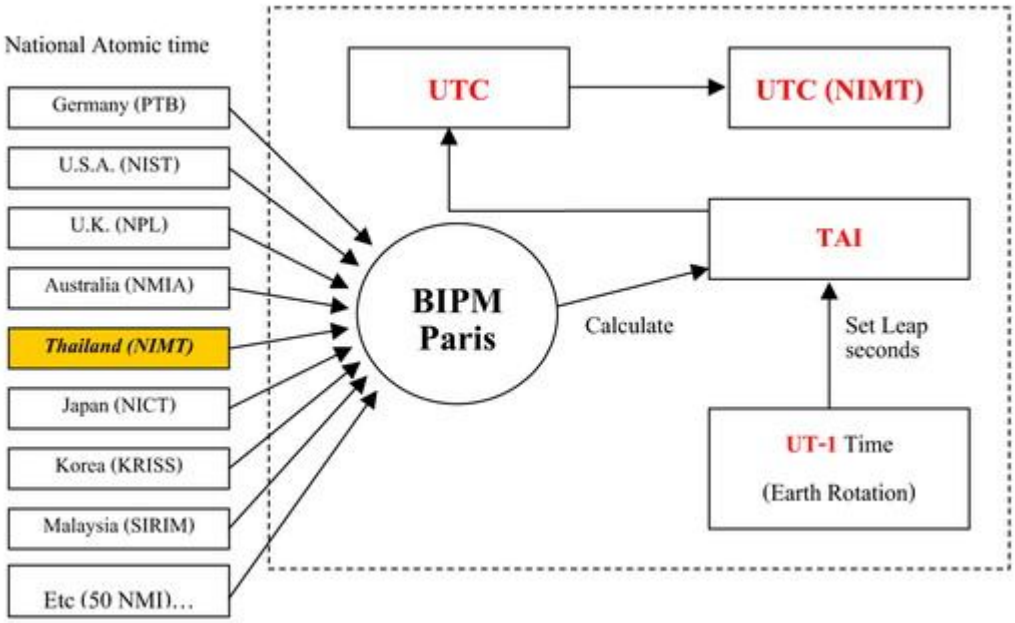
"เวลา" มีบทบาทสำคัญอย่างมากต่อชีวิตประจำวันของเราทุกคน ไม่ว่าจะเป็นด้าน การทหาร การเงิน การแพทย์ การจราจร การขนส่ง การสื่อสาร การติดต่อธุรกิจ และอุตสาหกรรมต่างๆ ทั้งภายในและนอกประเทศ ดังนั้น ภารกิจของห้องปฏิบัติการด้านเวลา สถาบันมาตรวิทยาแห่งชาติ คือ การจัดหา, รักษา และถ่ายทอด มาตรฐานทางด้านเวลา ไปสู่ภาคอุตสาหกรรมและผู้ใช้บริการต่างๆ พร้อมทั้งได้มีการพัฒนาขีดความสามารถด้านการวัดเวลาและความถี่ให้เป็นที่ยอมรับในระดับสากล ตาม พ.ร.บ.พัฒนาระบบมาตรวิทยาแห่งชาติ พ.ศ. 2540 (สถาบันมาตรวิทยาแห่งชาติ : online ,2553 http://www.nimt.or.th/nimt/service/index.php?menuName=time)

1. TAI (International Atomic Time) เป็นเวลาที่ใช้อ้างอิงระหว่างประเทศซึ่งถูกคำนวณที่ สำนักงานชั่ง ตวง วัด ระหว่างประเทศ (BIPM) โดยใช้ข้อมูลจาก นาฬิกา ซีเซียม (Cesium clock) มากกว่า 250 เครื่องซึ่งตั้งอยู่ตามสถาบันมาตรวิทยาของประเทศต่างๆกว่า 50 ประเทศ รวมทั้งสถาบันมาตรวิทยาแห่งชาติ ประเทศไทย

2. UTC (Coordinated universal Time) คือเวลา TAI ที่ถูกเพิ่ม-ลด วินาที (Leap second) เพื่อให้สอดคล้องกับเวลาที่ได้จากการโคจรของโลก

3. UTC(NIMT) คือเวลามาตรฐานประเทศไทยได้จากนาฬิกา Cesium ถูกคำนวณโดย BIPM โดยเทียบกับเวลามาตรฐานอ้างอิง UTC ซึ่งมีความไม่แน่นอนอยู่ที่ 20 นาโนวินาที จาก BIPM Circular T.

4. UT-1 (Universal Time) คือเวลาที่เกิดจากการโคจรของโลกซึ่งพัฒนามาจาก UT-0 และถูกแก้ค่า (correct) จากการเปลี่ยนแปลงทาง Longitude ของสถานีสังเกตการณ์ เนื่องจากการเคลื่อนไหวเปลี่ยนแปลงของขั้วโลก โดยนิยามข้างต้นจะสามารถอธิบายให้เข้าใจง่ายขึ้น ซึ่งจะแสดงให้เห็นว่าเวลามาตรฐานของประเทศต่างๆรวมทั้งประเทศไทยมีการสอบกลับได้ (Traceability) และส่งผลให้ระบบเวลาของประเทศต่างมีความถูกต้องสอดคล้องกันทั่วโลก



รูปที่ 2.7 แสดงขั้นตอนในการคำนวณหาค่า TAI และ UTC

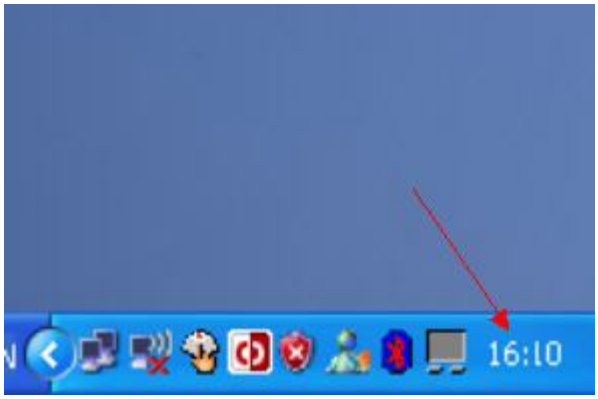
วิธีการปรับเทียบเวลามาตรฐานทาง Internet ผ่านระบบ NTP (Time Synchronization through Internet by NTP)

การปรับเทียบเวลามาตรฐานทาง Internet ผ่านระบบ Network Time Protocol (NTP) คืออะไร

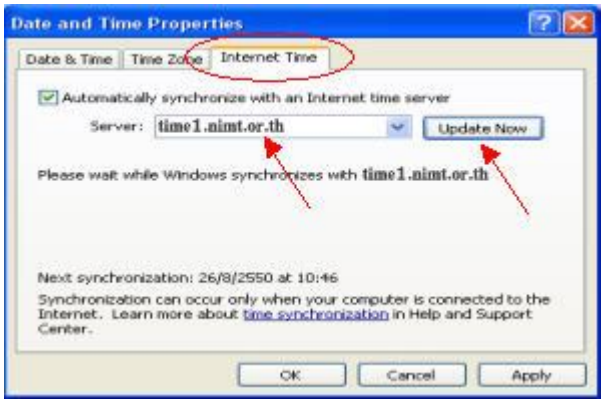
NTP Protocol เป็น Protocol ที่ใช้สำหรับปรับเทียบเวลา (Time Synchronization) ของ Computer โดยอาศัยเครือข่าย Internet เป็นสื่อกลางในการส่งข้อมูลเวลามาตรฐานไปยังเครื่องลูกข่าย โดยมีเครื่องแม่ข่าย (NTP Server) เป็นตัวให้บริการส่งเวลามาตรฐานไปยังเครื่องปลายทางเพื่อปรับเทียบเวลาให้ตรงกลับเวลามาตรฐาน (Time Standard) ซึ่งเป็นค่าเวลาที่ทาง Time & Frequency Lab. ได้ทำการเก็บรักษาไว้โดยวิธีการเปรียบเทียบกับเวลามาตรฐานของประเทศอื่นๆซึ่งเป็นที่ยอมรับในระดับนานาชาติ โดยมีความถูกต้องอยู่ที่ ประมาณ 1 millisecond ในระบบ LAN และประมาณ 10 millisecond ในระบบ WAN นับว่าเป็นความคลาดเคลื่อนที่อยู่ในระดับต่ำ อีกทั้งยังง่ายต่อการเข้าถึงของผู้ใช้ทั่วไป แค่เพียงมี Personal Computer ที่สามารถเชื่อมต่อ เข้าระบบ Internet ได้ผู้ใช้ก็สามารถที่จะ Synchronize เวลามาตรฐานผ่านระบบ NTP ได้ทันที

สถาบันมาตรวิทยาแห่งชาติ ส่วนห้องปฏิบัติการด้านเวลาและความถี่ได้จัดให้มีการติดตั้ง NTP Server ขึ้นเพื่อให้บริการถ่ายทอดเวลาผ่านระบบ Internet และสามารถเปิดให้บริการได้แล้วในปัจจุบัน ผู้สนใจใช้บริการสามารถปรับเทียบเวลาได้โดยวิธีง่ายๆไม่สลับซับซ้อนมากนัก สามารถใช้โปรแกรมพื้นฐานที่ติดมากับ Windows Xp ได้เลย โดยให้ผู้ใช้ปฏิบัติตามขั้นตอนดังต่อไปนี้

กรณีใช้ Window Xp ขึ้นไปให้ double click ตรงตำแหน่งที่แสดงเวลาด้านล่างขวาของหน้าจอคอมพิวเตอร์ดังที่แสดงในรูป



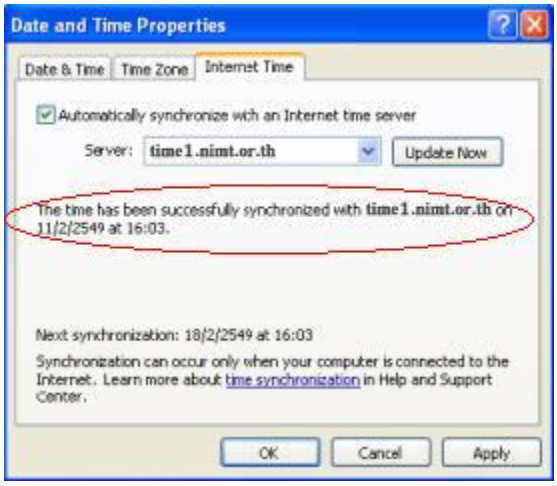
รูปที่ 2.8 แสดงตำแหน่งที่ใช้ตั้งค่าการ Synchronize เวลา



รูปที่ 2.9 แสดงวิธีการตั้งค่าการ Synchronize เวลา กับเครื่องแม่ข่าย

Click ไปที่ Tab Internet Time แล้วเลือก Check Box ที่ Automatically Synchronize with and internet time server และ ใส่ค่า IP Address ของ NTP Server ของสถาบันมาตรวิทยาแห่งชาติ

จากนั้นให้ Click ที่ปุ่ม Update Now และให้สังเกตบรรทัดล่างจะปรากฏคำว่า The time has been successfully synchronized with " time1.nimt.or.th (IP Address of NIMT TIME SERVER) " on 11/2/2549 at 16:03. นั่นหมายถึงสามารถที่จะ Synchronize เวลากับเครื่องแม่ข่ายได้เป็นที่เรียบร้อยแล้ว และ ถือเป็นอันเสร็จขั้นตอนการ Synchronize เวลาจากเครื่องแม่ข่าย



รูปที่ 2.10 แสดงข้อความที่บ่งบอกว่าสามารถ Synchronize ได้สำเร็จ

โปรแกรมประยุกต์อื่นๆสำหรับใช้ Synchronize เวลาผ่านระบบเครือข่าย

นอกจากเครื่องมือมาตรฐานที่ Windows Xp ให้มาแล้วยังสามารถที่จะใช้โปรแกรมประยุกต์อื่นๆ ที่รองรับการทำงานของระบบ NTP ได้ ในที่นี้ทาง ห้องปฏิบัติการด้านเวลาและความถี่ อยากจะแนะนำ Software ที่ทำงานในลักษณะดังกล่าวอยู่ 2 ตัวได้แก่ Dimension 4 ซึ่งมีความสามารถในการรองรับการใช้งานระบบ NTP ได้ ซึ่ง Software ดังกล่าวสามารถ Download ได้ทาง Internet ที่ www.thinkman.com โปรแกรม Dimension4 ซึ่งจะยอมให้สามารถ setup ค่าต่างๆ ได้อย่างละเอียดและ User Interface ดูแล้วไม่ยุ่งยากสำหรับผู้ใช้งานทั่วไปดังแสดงใน

ในการเพิ่มค่าของ NTP Server ของสถาบันมาตรวิทยาแห่งชาติเข้าไปให้ Click ที่ปุ่ม Add ในวงกลมสีแดงหลังจากนั้นให้ใส่ค่าในช่องต่างๆดังต่อไปนี้

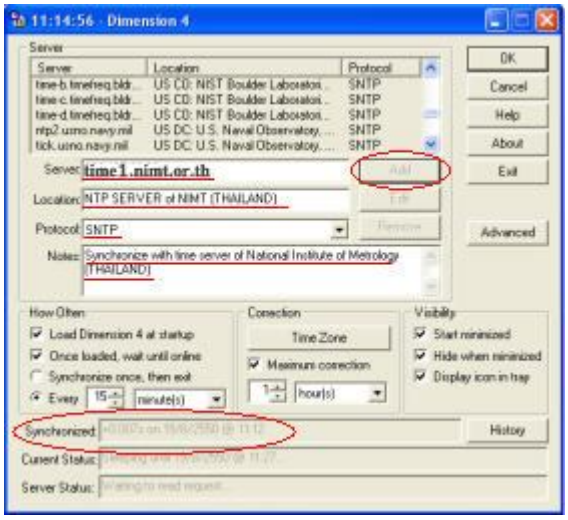
Server :: time1.nimt.or.th และ time2.nimt.or.th และ time3.nimt.or.th

Location :: TH BKK: NIMT Time and frequency Laboratory หรือ NTP SERVER of NIMT (THAILAND)

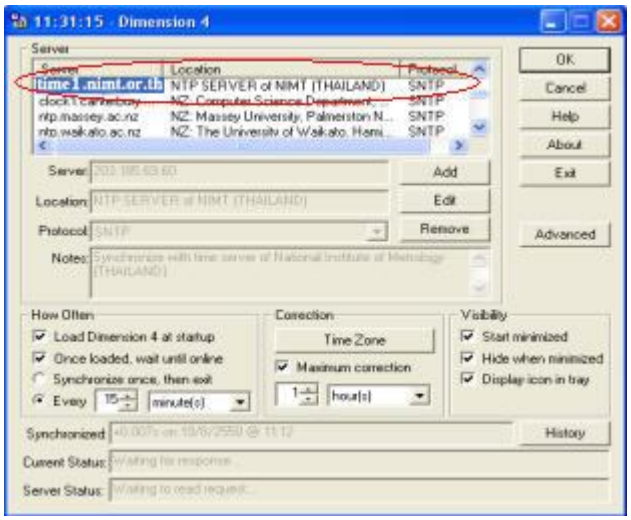
Protocal :: SNTP

Note :: Synchronize with time server of National Institute of Metrology (THAILAND)

เมื่อใส่ค่าต่างๆครบแล้วให้ Click ปุ่ม OK



รูปที่ 2.11 User Interface ของโปรแกรม Dimension4 ที่ยอมให้ ใส่ค่ากำหนดค่าต่างๆ ได้อย่างละเอียด ได้สำเร็จ



รูปที่ 2.12 แสดงชื่อของ Server ใหม่เพิ่มขึ้นเมื่อสามารถเพิ่ม NTP Server

ในช่อง Synchronized: จะปรากฏค่า +0.007 s on 19/8/2550 @ 11:12 หมายถึง เวลาในคอมพิวเตอร์ต่างจากเวลามาตรฐานไป 0.007 วินาที ณ วันที่ 19/8/2550 เปรียบเทียบที่เวลา 11 :12 น.

http://www.thaicert.nectec.or.th/paper/basic/NTPandLAW.php

http://www.thaicert.nectec.or.th/paper/basic/ntp_manual.php

http://www.cis.udel.edu/~mills/ntp/html/index.html

2.7 ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

เรื่องเกี่ยวกับ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 รายการหนึ่งที่ผู้ดูแลระบบควรจะคำนึงถึงมากที่สุด คือระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) ตามมาตรา 26 มาตรา 26 ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบ คอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการ ผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบ วันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้อง เก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) ตามพระราชบัญญัติคอมพิวเตอร์ฯ ปี 2550 มาตรา 26

ระบบพิสูจน์การมีตัวตนของผู้ใช้คอมพิวเตอร์โดยระบุ Physical Address (Identification and Authentication System) มีรายละเอียดดังนี้

ระบบสำหรับการกำหนดเวลาให้ตรงกับเวลาจริงโดยอิงเวลาสากล

ระบบสกัดกั้นการเข้าถึง

เว็บไซต์ที่ไม่เหมาะสม

เว็บไซต์ล่อลวง

เว็บไซต์หลอกลวงต้มตุ๋น ตลอดจนเว็บไซต์ที่ทำให้ระบบเครือข่ายทำงานช้า

การดาวน์โหลดไฟล์ที่ไม่พึงประสงค์

สามารถเลือกได้ว่าจะบล็อค หรือ ไม่บล็อคเครื่องลูกเครื่องใดก็ได้ในวง LAN เพื่อการแบ่งโซน เครื่องสำหรับเด็กและผู้ใหญ่

ผู้ดูแลระบบ *nix ส่วนใหญ่คงคุ้นเคยกับ syslog มาเป็นอย่างดี เพราะ syslog ถือได้ว่าเป็น log daemon ที่ใช้กันมาอย่างยาวนานและกลายเป็นมาตรฐานของการเก็บข้อมูลล็อกของระบบปฏิบัติการ *nix ในหลายๆ ตัว แต่อย่างไรก็ตาม syslog ก็มีข้อเสียบางอย่าง ที่ log daemon ตัวอื่นเช่น syslog-ng, msyslog สามารถแก้ไขข้อบกพร่องดังกล่าวได้ เอกสารฉบับนี้จะแนะนำ syslog-ng ซึ่งเป็น log daemon ตัวใหม่ที่กำลังเป็นที่นิยมกันมากขึ้น และจะกล่าวถึงการสร้าง configuration แบบละเอียดเพื่อให้สามารถนำ syslog-ng ไปใช้งานได้จริง แนะนำ Syslog-ng (Syslog new generation)

syslog-ng สามารถแก้ไขข้อบกพร่องส่วนใหญ่ของ syslog ได้ โดย

syslog-ng สามารถทำงานได้ทั้งบน TCP และ UDP

syslog-ng สามารถทำการกรอง (filter) ข้อมูลได้ด้วย regular expression

syslog-ng สามารถทำงานในรูปแบบที่อ้างอิง priority/facility ได้ ดังนั้น มันจึงสามารถทำงานแทนที่syslog ได้

syslog-ng สนับสนุน log forwarding ซึ่งทำให้สามารถทราบได้ว่า ต้นทางของล็อกถูกส่งมาจากเครื่องใดและผ่านเครื่องใดมาบ้าง

นอกจากนี้ syslog-ng ยังมีรูปแบบของไฟล์ configuration ที่ง่าย แต่มีความยืดหยุ่นสูง สามารถนำไปประยุกต์ใช้ให้ตรงความต้องการได้โดยง่าย แบ่งเป็น 2 ลักษณะ คือ Client และ Server

Syslog-ng มีเครื่องมือ ประกอบด้วย Sources ทำหน้าที่ระบุที่มาของ log ว่าต้องการที่จะนำ logfile จากแหล่งกำเนิดไหนมาเก็บ เช่น #สำหรับเรียกไฟล์ log จากตัวเครื่อง

```
# sources
source src { unix-dgram("/var/run/log");
                    internal();
             file("/dev/klog");
    };
  #สำหรับเรียกเก็บไฟล์จากเครื่อง client
# Source from remote client
source s_client {
                tcp(ip(0.0.0.0) port(514) keep-alive(yes) max-connections(300));
        udp(ip(0.0.0.0) port(514));
    };
```

Destinations ทำหน้าที่เชื่อมต่อไปยังสถานที่เก็บ Logfile ต่างๆ ทั้งจากในตัว server เอง หรือ server อื่น (LogServer)

```
# destinationสำหรับส่ง logไปยังไฟล์ที่ต้องการ
destination messages { file("/var/log/messages"); };
        #destinationสำหรับส่ง log โดยให้สร้างชื่อไฟล์ตามวันเดือนปีที่เก็บ
destination d_squid {
          file("/var/log/$HOST/$YEAR/$MONTH/squid.$YEAR-$MONTH-$DAY"
          owner(root) group(adm) perm(665)
          create_dirs(yes) dir_perm(0775));
        };
#destinationสำหรับส่งไฟล์ไปยัง logserver
destination loghost { tcp("xxx.xxx.xxx.xxx" port(514)); };
```

Filters ทำหน้าที่กรองข้อมูล logfile ให้เหลือแค่ข้อมูลสำคัญที่ต้องการเท่านั้น

```
#กรองข้อมูลที่เกี่ยวข้องกับโปรแกรม squid
filter f_squid { program("squid") and facility(user); };
```

Log statements ทำหน้าที่เรียกใช้งาน เครื่องมือที่ ถูกตั้งค่าไว้ก่อนหน้าแล้ว ได้แก่ Sources ,Filters ,Destinations

เช่น

```
#นำlogของsquidไปเก็บไว้ที่ logserverที่กำหนด
log { source(src); filter(f_squid); destination(loghost); };
#นำlogที่ได้จากserverตัวอื่น
log { source(s_client); filter(f_squid); destination(d_squid); };
```

จากนี้ยังมี ไฟล์สำคัญอีก1ไฟล์ คือ /etc/rc.local โดยภายในไฟล์จะต้องมีการ เรียกรายงาน log ที่เราต้องการเพื่อให้ทาง LogServer นำไปเก็บได้อย่างถูกต้อง ตัวอย่าง

```
tail -F /var/log/message | logger -t freeradius -p local3.info&
```

อธิบาย tail -F /var/log/message เป็นคำสั่งรายงาน log จากไฟล์ที่กำหนดไว้ ในที่นี้คือ /var/log/message

| logger –t “ชื่อโปรแกรมที่เรากำหนด(ต้องให้ตรงกับprogramในไฟล์ syslog-ng.conf ของlogserver)”

-p local3.info& “เป็นเหมือนการทำ handchakeระหว่างเครื่อง log client กัย logserver(โดยจะต้องตั้งชื่อให้ตรงกันกับfacilityใน logserver)”

```
filter f_chilli { program("freeradius") and facility(local3); };
 destination d_chilli {
  file("/var/log/$HOST/$YEAR/$MONTH/chilli.$YEAR-$MONTH-$DAY"
  owner(root) group(adm) perm(665)
  create_dirs(yes) dir_perm(0775));
};
  log { source(s_client); filter(f_chilli); destination(d_chilli); };
```

2.8 ระบบปฏิบัติการลีนุกซ์ (Linux)

ลีนุกซ์เป็นโปรแกรมคอมพิวเตอร์ประเภท ระบบปฏิบัติการ ตระกูลหนึ่ง ระบบปฏิบัติการที่เราคุ้นเคยกันมาก่อน คือ Dos, Windows 3.11, Window95, Windows98, Unix ลีนุกซ์เป็นระบบปฏิบัติการประเภท Unix หรืออาจเรียกว่ายูนิกซ์โคลนที่ใช้งานบนเครื่อง PC แต่ปัจจุบันไม่ได้ใช้งานบนเครื่อง PC เพียงอย่างเดียว สามารถใช้งานได้บนเครื่องตระกูลอื่นด้วย เช่น Sun Sparc, Macintosh ฯลฯ (ไพฑูรย์ แย้มเทศ , 2548)

ลีนุกซ์ถือกำเนิดขึ้นในฟินแลนด์ ปี คศ. 1991 โดยลีนุส โทรวัลด์ส (Linus Torvalds) นักศึกษาภาควิชาวิทยาการคอมพิวเตอร์ (Computer Science) ในมหาวิทยาลัยเฮลซิงกิ โดยได้พัฒนามาจากระบบปฏิบัติการ Minix ซึ่งเที่เป็นระบบยูนิกซ์บนพีซีในขณะนั้น ซึ่งตอนแรกเป็นเพียงโครงงานที่เขาทำส่งอาจารย์สมัยเรียนปริญญาตรีเท่านั้น แต่ต่อมาก็ได้มีการพัฒนาต่อ เขาก็ได้ทำการชักชวนให้นักพัฒนาโปรแกรมอื่นๆมาช่วยทำการพัฒนาลีนุกซ์ ซึ่งความร่วมมือส่วนใหญ่ก็จะเป็นความร่วมมือผ่านทางอินเทอร์เนต ลีนุสจะเป็นคนรวบรวมโปรแกรมที่ผู้พัฒนาต่างๆ ได้ร่วมกันทำการพัฒนาขึ้นมาและแจกจ่ายให้ทดลองใช้เพื่อทดสอบหาข้อบกพร่อง และทำงานผ่านอินเตอร์เน็ตทั้งหมด ปัจจุบันพัฒนา มาถึงรุ่น 2.3 และจะพัฒนาต่อไป อย่างไม่หยุดยั้งเพราะลีนุกซ์เป็นระบบปฏิบัติการที่เปิดเผยต้นฉบับโปรแกรม(Open Source Code) ทำให้เราสามารถแก้ไขปรับปรุงด้วยตัวเราเองได้ ถ้าเรามีความรู้หรือสามารถเขียนโปรแกรมนั้นได้

เป็นซอฟท์แวร์ระบบปฏิบัติการที่ฟรี สามารถดาวน์โหลดได้ทางอินเตอร์เน็ตสามารถใช้ได้อย่างไม่ผิดกฎหมาย เป็นที่ทราบกันแล้วว่าเป็นโปรแกรมที่เปิดเผยต้นฉบับโปรแกรม (Open Source Code) แต่ลิขสิทธิ์ก็ยังเป็นของลีนุส โทรวัลด์ส โดยอนุญาตให้ใครๆ ก็สามารถใช้ลีนุกซ์ได้

โดยไม่ต้องเสียค่าลิขสิทธิ์ สามารถทำการคัดลอก แจกจ่ายได้ แต่ห้ามคิดค่าโปรแกรมลีนุกซ์ สามารถปรับปรุงเปลี่ยนแปลงได้ แต่ห้ามนำเวอร์ชันที่เราปรับปรุงไปแจกจ่ายให้ผู้อื่น ถ้าต้องการนำไปแจกจ่ายสู่สาธารณะ จะต้องนำส่วนที่เราแก้ไขปรับปรุงนี้ส่งให้ ลีนุส โทรวัลด์ส พิจารณาก่อน มีองค์กรที่ดูแลเรื่องนี้อยู่ คือ GNU Public License

สามารถใช้งานได้ CPU หลายตระกูล Intel, AMD, Motorola, Digital Alfa, PowerPC, Sun Sparc สรุปคือ ลีนุกซ์ไม่ใช่สามารถรันบนเครื่อง PC ได้เพียงอย่างเดียว เครื่อง Macintosh เครื่อง Sunก็สามารถรันได้

ลีนุกซ์เป็น Unix เต็มรูปแบบ เป็นระบบ Multi User Multi Task คือใช้งานได้คราวละหลายๆคน และทำงานได้คราวละหลายๆ งาน

ลีนุกซ์มีระบบการติดต่อกับผู้ใช้แบบกราฟิก ที่เรียกว่า X-Windwow เป็นมาตรฐาน สามารถใช้ Windows manager ได้หลายชนิดหมายถึง ลักษณรูปร่างหน้าตาของ Desktop จะเลือกใช้แบบไหน ชอบแบบไหนก็เลือกลงได้ตามใจคุณ

สนับสนุน โปรโตคอลแบบ TCP/IP, SLIP, PPP, UUCP และอื่นๆ

ลีนุกซ์เป็นระบบปฏิบัติการ 32 บิท มีประสิทธิภาพและคุณภาพสูง คือ เครื่องไม่แฮงค์

ลีนุกซ์ได้ทำการเตรียม เครื่องมือพัฒนาโปรแกรมให้เราไว้อย่างครบครันซึ่งจะมีตั้งแต่แอพพลิเคชันมาตรฐานคือ C/C++ คอมไพเลอร์ของ GNU และหากเราต้องการพัฒนาระบบบน X ก็มี TCL/TK เตรียมไว้ให้ด้วย สำหรับคอมไพเลอร์ภาษาอื่นๆก็มีเช่น Perl, Smalltalk , Pascal, Lisp เป็นต้น ถ้าคุณมีความเชี่ยวชาญการเขียนโปรแกรมแบบ X-Base หรือ FoxPro บนลีนุกซ์ก็มีดาต้าเบสที่มีการเขียนโปรแกรมแบบนี้ให้เช่นกัน และล่าสุดลีนุกซ์ก็มีจาวาคอมไพเลอร์ให้สำหรับผู้ที่ชื่นชอบการเขียนแอพเพลตจาวา สำหรับรันบนอินเทอร์เนตด้วย (ธวัชชัย ชูเหล็ก ,2550)

ตัวระบบปฏิบัติการ หรือเคอร์เนล (kernel)

ไลบรารีของระบบ

ยูทิลิตี้ของระบบ และการจัดการระบบ

ตัวระบบปฏิบัติการ (kernel) ทำหน้าทีหลักในการจัดการทรัพยากรต่างๆของระบบ เช่น หน่วยความจำ การจัดคิวสำหรับโปรแกรมต่างๆ การจัดการอุปกรณ์ต่างๆ ซีดีรอม การ์ดแลนด์ พอร์ตอนุกรม พอร์ตขนาน การ์ดพีซีไอ การ์ดแสดงผล ฮาร์ดดิสก์ รวมถึงการจัดระบบแฟ้มข้อมูล เคอร์เนลเราสามารถดาวน์โหลดได้ที่ http://www.kernel.org/ ไลบรารีของระบบ เป็นที่เก็บรวบรวมฟังก์ชันมาตรฐานที่ใช้ติดต่อกับเคอร์เนล ทำให้โปรแกรมที่ไปติดต่อกับระบบผ่านฟังก์ชันมาตรฐานเหล่านี้ ยูทิลิตี้ของระบบ และการจัดการระบบ ส่วนนี้ประกอบด้วยโปรแกรมที่ทำหน้าที่

จัดการระบบในส่วนต่างๆ เช่นระบบไฟล์ ผู้ใช้งานระบบ โมดูล ระบบรักษาความปลอดภัย ระบบเน็ตเวิร์กฯลฯ

ปัจจุบันเคอร์เนลเวอร์ชัน 2.3.X เวอร์ชันของเคอร์เนล ประกอบด้วยตัวเลข 3 ชุด x.x.x ตัวเลขตัวแรกเป็น เวอร์ชันหลัก ตัวที่สองเวอร์ชันรอง ตัวที่ 3 เป็นการปรับปรุงครั้งที่ของเวอร์ชันนั้น เวอร์ชันหลักจะมีการเปลี่ยนแปลงก็ต่อเมื่อมีการปรับปรุงเปลี่ยนแปลง หรือได้รับการพัฒนาแตกต่างไปจากเดิมไปอย่างมาก ตัวเลขชุดที่ 2 ตัวเลขชุดนี้บอกว่าเคอร์เนลอยู่ระหว่างพัฒนา ให้ดูว่าถ้าเคอร์เนลที่เสถียรจะเป็นเลขคู่ ถ้าตัวเลขไม่เสถียรจะเป็นเลขคี่ เช่น 2.2.x จะเป็นเคอร์เนลที่เสถียร ส่วน 2.3.x นั้นเป็นเคอร์เนลที่ไม่เสถียร ส่วนตัวเลขชุดที่ 3 บอกครั้งที่ของการปรับปรุงเคอร์เนลในเวอร์ชันนั้นๆ

จะเห็นได้ว่าเรามีลีนุกซ์หลายค่ายด้วยกัน เช่น Redhat, SuSe, Mandrake, Debian, Slackware ฯลฯ เหล่านี้เราเรียกว่า Distribution คือ การรวบรวมโปรแกรมต่างๆของลีนุกซ์ ไม่ว่าจะเป็นเคอร์เนล ไลบรารี่ของระบบ ทูลสำหรับดูแลระบบ และโปรแกรมที่ใช้งานทั่วๆไปเข้าด้วยกัน แล้วใส่ระบบการติดตั้งให้ใช้งานง่ายขึ้น ซึ่งทำให้แต่ละค่ายมีข้อเด่นข้อด้อยต่างกันไป เช่น Redhat จะติดตั้งง่ายเพราะมีโปรแกรมที่สามารถตรวจสอบฮาร์ดแวร์ที่เราใช้อยู่ได้ถ้ามันรู้จักมันก็ติดตั้งไดร์เวอร์ให้ทำให้การติดตั้งง่ายขึ้นส่วนการใช้งานก็มีการใช้ไฟล์แบบ RMP (Redhat Package Management) ทำให้ติดตั้งโปรแกรมได้ง่าย

ระบบนี้เป็นระบบแบบฟรีแวร์ (Freeware) เป็นโปรแกรมที่พัฒนาภายใต้ความคิดที่เรียกกันว่า “General Public License” ซึ่งหมายความว่าเราสามารถนำลีนุกซ์มาใช้งานได้ฟรี ทำให้ผู้ใช้อย่างเราไม่ต้องกลัว ผิดกฎหมายหรือมีการละเมิดลิขสิทธิ์ซอฟต์แวร์อีกต่อไป

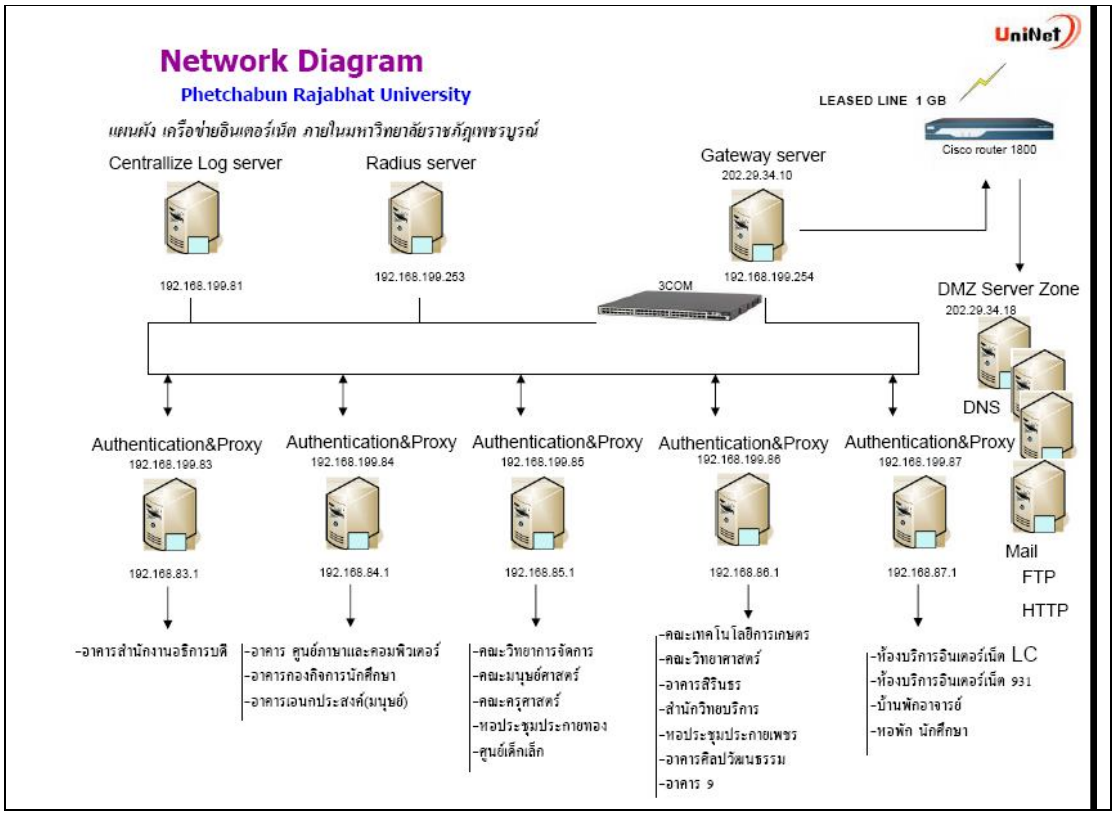
บทที่ 3
วิธีดำเนินการวิจัย

ในบทนี้จะกล่าวถึงการออกแบบและพัฒนาระบบเครือข่ายอินเทอร์เนตเกตเวย์ราคาถูกสำหรับมหาวิทยาลัย ซึ่งจะทำการออกแบบใช้สำหรับบันทึก Log File ซึ่งเก็บข้อมูลการจราจรบนเครือข่ายอินเทอร์เน็ต โดยมีระบบบันทึกจราจรคอมพิวเตอร์ (Centralize Log) ระบบเทียบเวลาสากล (Network Time Potocol) ระบบพิสูจน์ตัวตน (Authentication) ใช้เพื่อตรวจสอบสิทธิ์ ที่ออกแบบมาเพื่อรองรับกับ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และประกาศของกระทรวงเทคโนโลยีสารสนเทศ การเก็บข้อมูลมีลักษณะอย่างไรและต้องใช้ข้อมูลอะไรบ้างเพื่อเป็นการประกอบให้ระบบที่ออกแบบและพัฒนาระบบการจัดการผู้ใช้ การจัดการการใช้แบนด์วิด (Bandwidth) และอื่นที่เกี่ยวข้อให้มีความสมบูรณ์มากที่สุดสามารถแบ่งงานในส่วนของการออกแบบได้ดังนี้

1. การบันทึกล็อกไฟล์ตาม พระราชบัญญัติ ว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 สำหรับมหาวิทยาลัย (Centralized Log Server For University.)
2. ระบบพิสูจน์ตัวตนตามบัญชีผู้ใช้อินเทอร์เนต (User Authentication Internet Account System.)
3. พัฒนาแอพพลิเคชั่นจัดการระบบจัดการฐานข้อมูลผู้ใช้อินเทอร์เนต (Application User Manager Internet Account for Administrator.)
4. การอิมพลีเมนต์ระบบอินเทอร์เนตเกตเวย์สำหรับมหาวิทยาลัย(Implementation of Internet Gateway For University (Firewall, NAT,DHCP, Proxy Server, DNS, Database Server, Web server, Mail Server, FTP Server).
5. ประยุกต์ใช้งานระบบอินเทอร์เนตเกตเวย์มหาวิทยาลัยในระบบเครือข่ายทั้งแบบไวไฟ-ลีสไลน์ (Interface Internet Gateway University WIFI–Lease Line Technology.)

3.1 การออกแบบระบบเครือข่ายมหาวิทยาลัย

การออกแบบและพัฒนาระบบเครือข่ายภายในมหาวิทยาลัย ในปัจจุบันมีทั้งระบบเครือข่ายที่เป็นลีสไลน์เชื่อมต่อด้วยระบบใยแก้วนำแสง(Fiber Optic) และเชื่อมต่อในรูปแบบของระบบเครือข่ายท้องถิ่น (Local Area Network) รวมถึงการเชื่อต่อในรูปแบบที่ไม่ต้องใช้สาย (Wireless LAN) ดังนี้



รูปที่ 3.1 แสดงระบบเครือข่ายคอมพิวเตอร์มหาวิทยาลัย ปีงบประมาณ 2553

3.2 การวิเคราะห์พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

ข้อมูล พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และประกาศกระทรวง เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการถือเป็นข้อมูลที่

สำคัญอย่างยิ่งในการออกแบบระบบที่รองรับ พระราชบัญญัติ และประกาศกระทรวงดังกล่าว ซึ่งก่อนออกแบบระบบนั้นเราควรที่จะทำการวิเคราะห์ก่อนว่า พระราชบัญญัติ และประกาศกระทรวง กล่าวถึงสิ่งใดและต้องการให้ทำสิ่งใด เนื่องจากเนื้อหาของ พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และประกาศกระทรวง เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการมีเนื้อหามากมายแต่เนื้อหาที่จำเป็นสำหรับการวิเคราะห์ระบบมีดังนี้

3.2.1 ผู้ให้บริการ

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ตหรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่นหมายถึง

(๑) ผู้ประกอบกิจการโทรคมนาคมไม่ว่าโดยระบบโทรศัพท์ ระบบดาวเทียม ระบบวงจรเช่า หรือบริการสื่อสารไร้สาย

(๒) ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ไม่ว่าโดยอินเทอร์เน็ตทั้งผ่านสายและไร้สาย หรือในระบบเครือข่ายคอมพิวเตอร์ภายในที่จัดตั้งขึ้นในเฉพาะองค์กรหรือหน่วยงาน

(๓) ผู้ให้บริการเช่าระบบคอมพิวเตอร์ หรือให้เช่าบริการโปรแกรมประยุกต์ (service provider)

ตาราง 3.1 ข้อมูลผู้ให้บริการอินเทอร์เน็ต(คณะกรรมการธุรกรรมทางอิเล็คทรอนิค 2550: ออนไลน์)

ประเภท	ตัวอย่างของผู้ใช้บริการ
ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider)	๑) ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ทั้งมีสายและไร้สาย ๒) ผู้ประกอบการซึ่งให้บริการในการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ในห้องพักห้องเช่าโรงแรม อินเทอร์เนต หรือร้านอาหารและเครื่องดื่มในแต่ละกลุ่มอย่างหนึ่งอย่างใด ๓) ผู้ให้บริการเข้าถึงระบบเครือข่ายคอมพิวเตอร์สำหรับองค์กร เช่น หน่วยงานราชการ บริษัทหรือสถาบันการศึกษา

3.2.2 หน้าที่และความรับผิดชอบของผู้ให้บริการ

มาตรา ๑๕ ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้ ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลงหมายถึง มาตรา ๑๕ ผู้ให้บริการอินเทอร์เน็ตทั้งหลายตามที่ได้กล่าวไว้ในหัวข้อ

3.2.1 นั้นสนับสนุนหรือยินยอมให้ผู้ใช้บริการกระทำความผิดถือเป็นความผิดเช่นเดียวกับผู้กระทำความผิดนั้นคือต้องระวางโทษจำคุกไม่เกินห้าปี หรือ ปรับไม่เกินหนึ่งแสนบาทหรือทั้งจำทั้งปรับ

มาตรา ๒๖ ผู้ให้บริการต้องมีระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไม่น้อยกว่า 90 วันแต่ไม่เกิน 1 ปี ถ้าไม่กระทำตามต้องระวางโทษปรับไม่เกินห้าแสนบาท

3.2.3 ข้อมูลจราจรทางคอมพิวเตอร์

ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของการบริการ หรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้นมีใช้อยู่ในมาตรา ๑๘ มาตรา ๒๒ มาตรา ๒๓ มาตรา ๒๔ มาตรา ๒๕ และมาตรา ๒๖ หมายถึง ข้อมูลที่แสดงให้เห็นถึงการติดต่อสื่อสารที่แสดงให้เห็นผู้ส่ง เช่น IP address ของเครื่อง ชื่อที่อยู่ของผู้ใช้ ข้อมูลของผู้ให้บริการ ลักษณะของการให้บริการ วันเวลาของการส่งข้อมูล และข้อมูลทุกประเภทที่เกิดจากการสื่อสารผ่านระบบคอมพิวเตอร์

3.2.4 ประกาศกระทรวง เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ

ข้อ ๘ การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ผู้ให้บริการต้องใช้วิธีการที่มั่นคงปลอดภัย ดังต่อไปนี้

(๒) มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าวเพื่อรักษาความน่าเชื่อถือของข้อมูลและไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้

(๔) ในการเก็บข้อมูลจราจรนั้น ต้องสามารถระบุรายละเอียดผู้ใช้บริการ เป็นรายบุคคลได้ (Identification and Authentication)

ข้อ ๙. เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริงผู้ให้บริการต้องตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล(Stratum0) โดยผิดพลาดไม่เกิน 10 มิลลิวินาที

หมายถึง ข้อ ๘ (๒) ข้อมูลจราจรทางคอมพิวเตอร์และข้อมูลของผู้ใช้บริการต้องมีระบบรักษาความปลอดภัยหรือเข้ารหัสเพื่อมิให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้ได้

ข้อ ๘ (๔) ข้อมูลที่จัดเก็บนั้นสามารถระบุตัวบุคคลได้ ข้อ ๙ อ้างอิงเวลากับผู้ให้บริการ NTP Server ในประเทศไทยโดยเวลาผิดพลาดไม่เกิน 10 มิลลิวินาที

3.2.5 ผลการวิเคราะห์ข้อกำหนดของ พระราชบัญญัติ

จากข้อมูลที่ได้จากการวิเคราะห์ พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และประกาศกระทรวง เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ ทั้งหมดสามารถอธิบายได้ดังต่อไปนี้

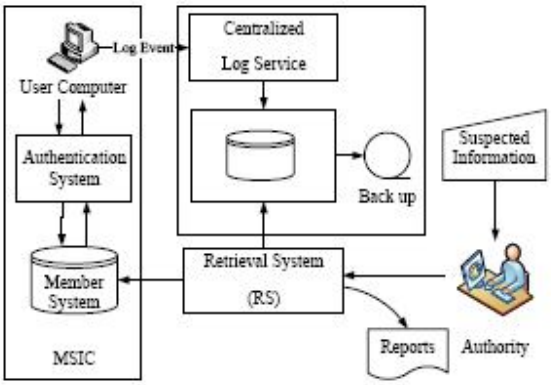
1) มีการระบุตัวตนของผู้ใช้งานอย่างชัดเจน (Identification) โดยมีระบบสำหรับการพิสูจน์ตัวตนของผู้ใช้บริการ (Authentication) ใช้ระบบสมาชิก (Member System) สำหรับให้สมาชิกเข้าใช้งานเครือข่ายอินเทอร์เน็ต

2) มีระบบการจัดการเวลาให้เป็นมาตรฐานที่น่าเชื่อถือและสามารถนำไปอ้างอิงเมื่อเกิดเหตุ โดยมีความผิดพลาดไม่เกิน 10 มิลลิวินาที โดยเราสามารถเลือกใช้ NTP Server เพื่อกระจายเวลาไปให้เครื่อง Client ในระบบของเราได้ โดย NTP Server จะต้องมีการ synchronizeเวลามาจากเครื่อง Server ที่อื่นที่เชื่อถือได้อีกทีนึง

3) มีระบบการเก็บรักษาข้อมูลที่ครบถ้วนและเชื่อถือได้เข้ารหัสข้อมูลล็อกไฟล์และจำเป็นต้องมีการสำรองข้อมูลการจราจร(Back up) ที่เกิดขึ้นด้วย

4) ระบบการจัดการสำหรับการค้นคืนข้อมูลการจราจรย้อนหลัง(Retrieval System) เพื่อใช้สำหรับค้นข้อมูลโดยจะมีรายงานจากเจ้าหน้าที่(Officer) เพื่อทำการระบุใครเป็นผู้กระทำความผิดโดยการออกเป็นรายงาน (Report) สำหรับเป็นหลักฐานทางกฎหมาย

5) ระบบที่รองรับเครือข่ายไร้สายโดยกำหนดให้ระบบที่พัฒนาทั้งหมดสามารถรองรับเครือข่ายไร้สายซึ่งวิธีการทั้งหมดที่เกิดจากการวิเคราะห์ข้อมูลนั้นเป็นส่วนช่วยให้ระบบเครือข่ายของอินเทอร์เนตนั้นสามารถรองรับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ได้ โดยวิธีการทั้งหมดนี้สามารถอธิบายอยู่ในรูปสถาปัตยกรรม โดยแบ่งการทำงานหรือดำเนินการต่างๆ ออกเป็นส่วนย่อยเพื่อให้ง่ายในการจัดการระบบทั้งหมด ดังภาพประกอบต่อไปนี้

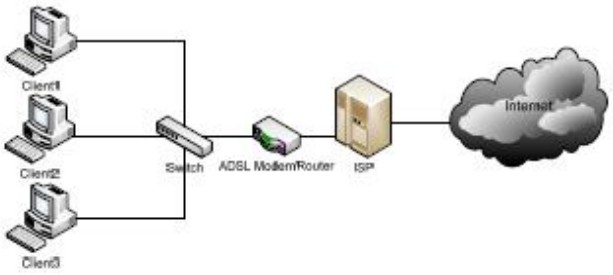


รูปที่ 3.2 แสดงสถาปัตยกรรมระบบเก็บข้อมูล พิสูจน์ตัวตน ค้นคืนและระบุผู้ใช้บริการอินเทอร์เนต

3.3 ระบบเครือข่ายของอินเทอร์เนต

แผนภาพเครือข่ายในอินเทอร์เนตโดยทั่วไปนั้นมีหลากหลายขึ้นอยู่กับขนาดของอินเทอร์เนตเองและความต้องการของเจ้าของร้าน โดยส่วนใหญ่แล้วในอินเทอร์เนตต้องมีคู่สายจาก ISP อุปกรณ์เครือข่ายอันได้แก่สวิสต์ (Switch) หรือฮับ (Hub) และเครื่องคอมพิวเตอร์ หรืออาจจะมีพวกอุปกรณ์อื่นๆ เพิ่มเข้ามาเพื่อเพิ่มประสิทธิภาพการทำงานให้สูงขึ้นอันได้แก่ ระบบ Multi-Wan Load Balance เพื่อสลับสายอัติโนมัติ เมื่อสายใดสายหนึ่งมีปัญหาสามารถเชื่อมต่ออินเทอร์เนตได้ตั้งแต่ 2 คู่สายขึ้นไป ระบบ Proxy Server / Ftp Server เพื่อเพิ่มความเร็วในการโหลดเป็นต้น

ตัวอย่างแผนภาพเครือข่ายทั่วไปของอินเทอร์เนต เป็นดังนี้



รูปที่ 3.3 แสดงแผนภาพเครือข่ายในอินเทอร์เนตทั่วไป

จากภาพประกอบจะเห็นได้ว่าอินเทอร์เนตมีการออกแบบระบบเครือข่ายเป็นลักษณะที่ง่ายต่อการจัดเตรียมระบบเครือข่ายให้รองรับกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550) จึงต้องเพิ่มส่วนต่างๆ ดังหัวข้อดังต่อไปนี้

3.4 ระบบพิสูจน์ตัวตน (Authentication)

สาเหตุที่จำเป็นต้องมีการจัดการเกี่ยวกับการระบุและการพิสูจน์ตัวตนของผู้ใช้บริการ เนื่องจากหากเกิดมีการใช้เครือข่ายภายในไปบุกรุกหรือละเมิดสิทธิ์บุคคลภายนอก เราจะไม่สามารถระบุได้เลยว่าใครเป็นผู้กระทำ เพราะเราจะสามารถรู้แค่เพียงหมายเลขไอพีแอดเดรส (IP Address) เท่านั้นแต่ไม่สามารถระบุเจ้าของไอพีแอดเดรส นั้นได้ จึงไม่สามารถดำเนินการกับผู้กระทำความผิดได้ เนื่องจากขาดซึ่งหลักฐานของการกระทำความผิด ดังนั้นระบบการระบุและการพิสูจน์ตัวตนของผู้ใช้บริการจึงเป็นสิ่งที่จำเป็นสำหรับระบบเครือข่ายของอินเทอร์เนต

3.4.1 วิธีการระบุตัวตนของผู้ใช้งาน (Identification) จะต้องมีการจัดการกับบัญชีผู้ใช้งาน ดังนี้

3.4.1.1 จัดเก็บ User Profile ของผู้ใช้งานภายในระบบเครือข่ายของอินเทอร์เน็ตคาเฟ่ทั้งหมด

ก) หมายเลขบัตรประจำตัวประชาชน (User ID)

ข) ชื่อผู้ใช้ (User Name)

ค) รหัสผ่าน (Password)

ง) ข้อมูลส่วนตัว (User Information)

จ) สิทธิ์การใช้งานที่สมาชิกสามารถใช้ได้ เช่น อายุน้อยกว่า 18 ปี ไม่สามารถเข้าใช้อินเทอร์เน็ตได้ในช่วงก่อนเวลา 14.00 นาฬิกา ในวันจันทร์ถึงวันศุกร์

3.4.1.2 ผู้ดูแลระบบ (Network Administrator) สามารถเพิ่มบัญชีผู้ใช้งานโดยให้ผู้ใช้งานสมัครเป็นสมาชิก (Member) และสามารถแก้ไขข้อมูลส่วนตัวของสมาชิกพร้อมทั้งสามารถกำหนดสิทธิ์การใช้งานที่สมาชิกสามารถใช้ได้

3.4.1.3 ระบบที่นิยมใช้งานกันในปัจจุบันได้แก่ เรเดียสเซิร์ฟเวอร์ (Radius Server) ชื่อว่า ฟรีเรเดียส (freeradius)

3.4.2 วิธีการพิสูจน์ตัวตนของผู้ใช้งาน (Authentication)

ระบบสามารถที่จะพิสูจน์ตัวตนของผู้ใช้งานก่อนเข้าใช้งานระบบเครือข่าย ซึ่งจะเป็นการอนุญาตสิทธิ์ตามที่ได้กำหนดไว้แล้ว ซึ่งสามารถป้องกันบุคคลภายนอกจากการเข้าใช้งานระบบเครือข่ายทั้งเครือข่ายปกติโดยระบบเครือข่ายท้องถิ่นที่ใช้กันอยู่ภายในอินเทอร์เนตทุกวันนี้ โดยปกติแล้วไม่มีการพิสูจน์ตัวตนก่อนเข้าใช้ระบบอินเทอร์เน็ต โดยจะมีการกำหนดให้ทุกเครื่องภายในอินเทอร์เนตเข้าใช้อินเทอร์เน็ตได้โดยต้องผ่านระบบการพิสูจน์ตัวตนก่อนเรเดียสเซิร์ฟเวอร์ (Radius Server) โดยการกรอกรหัสบัตรประจำตัวประชาชนและรหัสผ่านซึ่งได้จากผู้ดูแลระบบจากนั้นระบบทำการตรวจสอบว่ามีสิทธิ์ในการเข้าใช้อินเทอร์เน็ตหรือไม่

3.5 การออกแบบระบบฐานข้อมูล

ระบบค้นคืนและระบุผู้ใช้งานในอินเทอร์เนตเป็นระบบที่ค้นหาและระบุตัวผู้ใช้งาน ณ ช่วงเวลาใดๆ โดยเมื่อเจ้าหน้าที่พนักงานนำข้อมูลที่เกี่ยวข้องกับการกระทำผิดคือวันและเวลาของการกระทำความผิดมาแสดงแก่ผู้ดูแลระบบ ผู้ดูแลระบบต้องนำข้อมูลทั้งหมดนี้เข้าสู่ระบบค้นคืนและระบุผู้ใช้งานในอินเทอร์เนต จากนั้นระบบจะแสดงข้อมูลและมีเมนูพิมพ์เอกสารเพื่อเป็นหลักฐานของการค้นหา ดังนี้

1. คอมพิวเตอร์ทุกเครื่องในเครือข่ายเมื่อมีการใช้งานอินเทอร์เน็ต ต้องมีการพิสูจน์ตัวตนก่อนเรเดียสเซิร์ฟเวอร์และมีระบบฐานข้อมูลสำหรับเก็บข้อมูลสมาชิกในอินเทอร์เนต

2. เมื่อมีการพิสูจน์ตัวตนในการเข้าสู่อินเทอร์เน็ตเรเดียสเซิร์ฟเวอร์ จากผู้ใช้งานจะมีการเก็บล็อกไฟล์การใช้งานของเครือข่ายของผู้ใช้บริการอินเทอร์เน็ต

3. ระบบ Retrieval System จะมีการค้นหาตัวผู้กระทำความผิดเมื่อมีการนำหลักฐานจากเจ้าหน้าที่มาแสดง โดยหลักฐาน ได้แก่ IP Address และช่วงเวลาที่เข้าใช้งาน

4. ข้อมูลล็อกไฟล์ที่จัดเก็บมีการเข้ารหัสข้อมูลไว้

5. การออกแบบฐานข้อมูลสำหรับระบบเก็บข้อมูลพิสูจน์ตัวตน ค้นคืนและระบุ

3.5.1 แผนภาพกระแสข้อมูล

แผนภาพกระแสข้อมูล (Data flow diagram) สำหรับการออกแบบฐานข้อมูลสำหรับระบบเก็บข้อมูล พิสูจน์ตัวตน ค้นคืนและระบุผู้ใช้บริการอินเทอร์เนตนั้น โดยใช้แผนภาพกระแสข้อมูล (Data flow diagram) ในการวิเคราะห์ระบบแผนภาพกระแสข้อมูลเป็นความสัมพันธ์ระหว่างกระบวนการทำงาน โดยแบ่งออกเป็นระดับต่างๆ เริ่มต้นจากแผนภาพกระแสข้อมูลระบบสูงสุด (Context Diagram) แสดงเส้นทางของข้อมูลที่เข้าและออกจากแหล่งที่มีผลกระทบต่อระบบ และแผนภาพกระแสข้อมูลระดับที่ 2 ซึ่งจะเป็นแผนภาพกระแสข้อมูลระดับสูงสุดของการพัฒนาระบบเก็บข้อมูล พิสูจน์ตัวตน ค้นคืนและระบุผู้ใช้บริการอินเทอร์เนต

ระบบค้นคืนและระบุผู้ใช้งานอินเทอร์เนตแบ่งกระบวนการทำงานออกเป็น 6 กระบวนการหลักๆ คือ

2.1.ลงชื่อเข้าใช้ระบบสำหรับผู้ดูแลระบบเป็นการทำงานเกี่ยวกับตรวจสอบสิทธิ์ของผู้ดูแลระบบในการเข้าใช้ระบบค้นคืนและระบุผู้ใช้งานอินเทอร์เนต

2.2.อัพโหลดล็อกไฟล์ เป็นการทำงานเกี่ยวกับการอัพโหลดล็อกไฟล์ของวันที่เกิดเหตุการณ์กระทำผิดเกิดขึ้น เพื่อใช้สำหรับเป็นข้อมูลเบื้องต้นสำหรับค้นหาผู้กระทำผิด

2.3.ค้นหาการใช้อินเทอร์เน็ตของสมาชิก เป็นการทำงานเกี่ยวกับการค้นหาการใช้อินเทอร์เน็ตของสมาชิกซึ่งข้อมูลได้มาจากเจ้าหน้าที่ เพื่อใช้สำหรับค้นหาการใช้อินเทอร์เน็ตของสมาชิกโดยระบุวัน เวลาที่กระทำความผิด

2.4.แสดงข้อมูลการค้นหาผู้ใช้งานอินเทอร์เน็ตเป็นการทำงานเกี่ยวกับการแสดงข้อมูลค้นหาผู้ใช้งานอินเทอร์เน็ต เพื่อใช้สำหรับแสดงข้อมูลการค้นหาผู้ใช้งานอินเทอร์เน็ตในช่วงเวลาที่ค้นหาจากข้อมูลล็อกไฟล์

2.5.ระบุผู้ใช้งานอินเทอร์เน็ตของสมาชิก เป็นการทำงานเกี่ยวกับการระบุผู้ใช้งานของสมาชิกที่ใช้อินเทอร์เน็ต ณ เวลานั้น

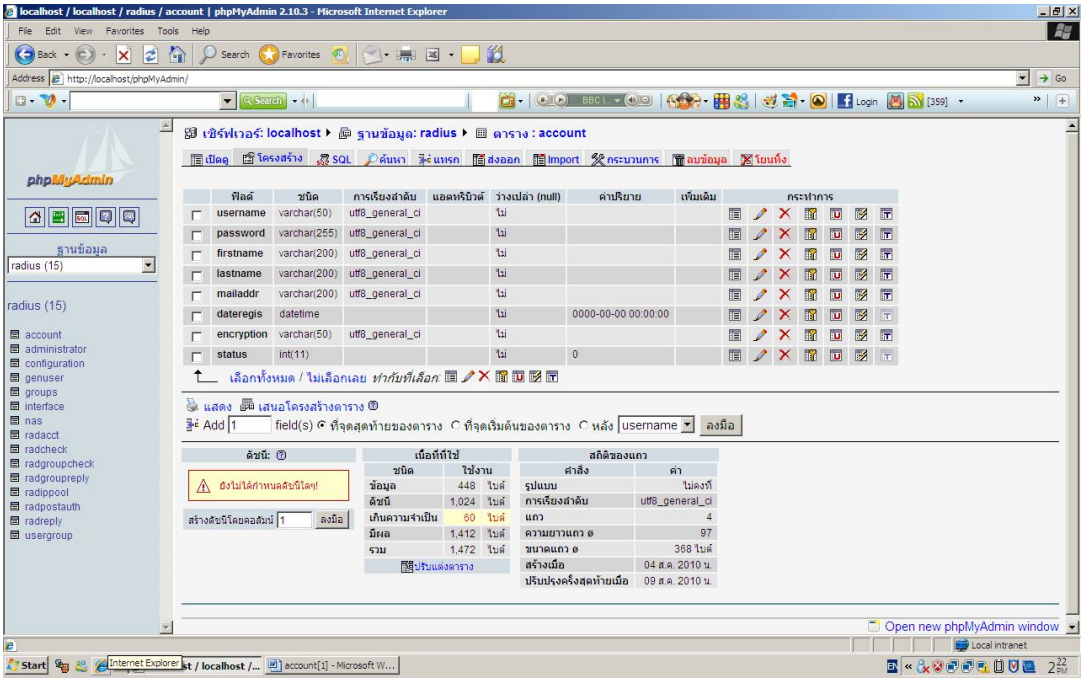
2.6.พิมพ์หลักฐานการกระทำความผิดของสมาชิกเป็นการทำงานเกี่ยวกับการพิมพ์หลักฐานที่ได้จากการค้นหาและระบุผู้ใช้งานในอินเทอร์เนตแล้ว เพื่อใช้สำหรับให้เจ้าหน้าที่ประกอบเป็นหลักฐานทางกฎหมายต่อไป

3.5.2 โครงสร้างฐานข้อมูล

โครงสร้างฐานข้อมูลเกี่ยวกับระบบเก็บข้อมูลพิสูจน์ตัวตน ค้นคืนและระบุผู้ใช้บริการอินเทอร์เนต ประกอบด้วยตารางพจนานุกรมข้อมูล(Data Dictionary) ต่อไปนี้

Database : Radius

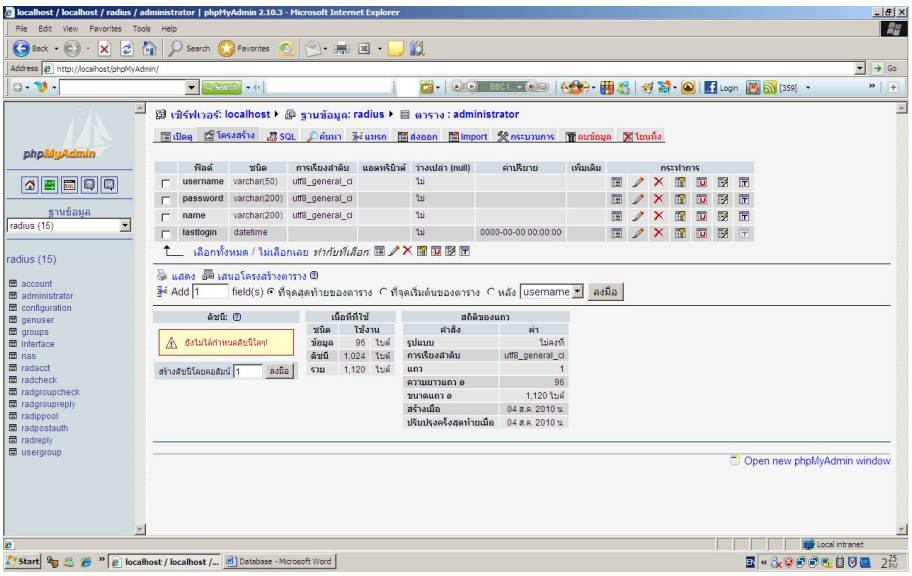
Table : account



รูปที่ 3.4 แสดงตาราง Account

Database : Radius

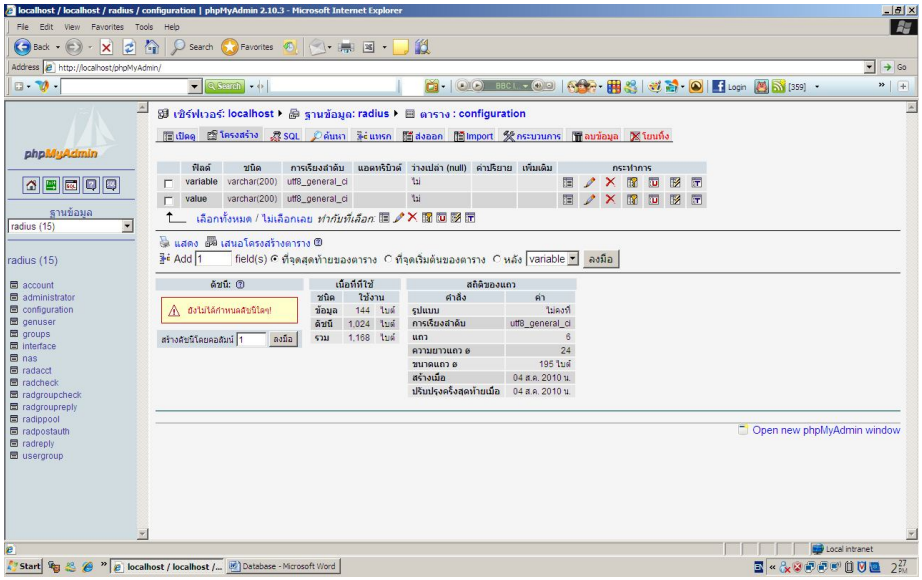
Table : administrator



รูปที่ 3.5 แสดงตาราง administrator

Database : Radius

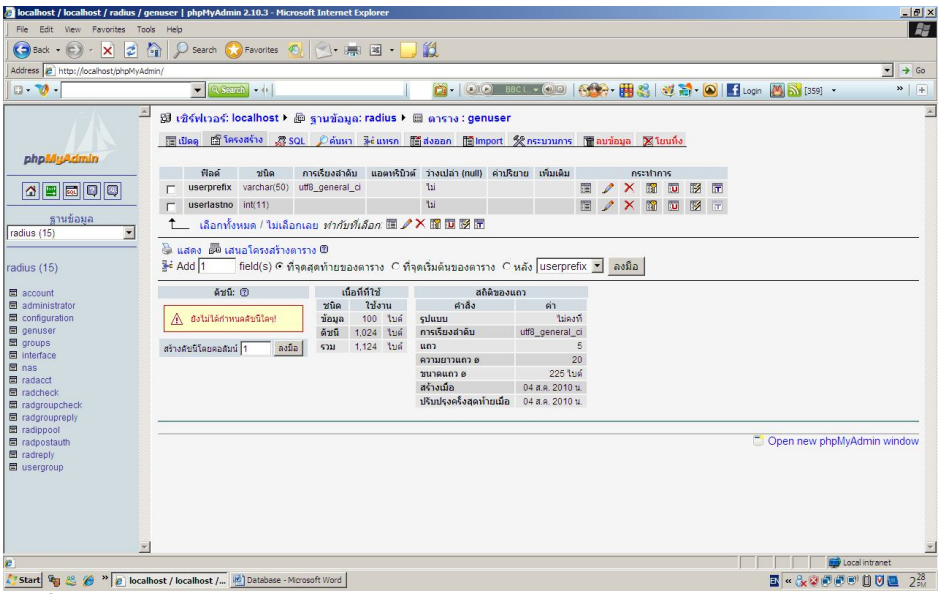
Table : configuration



รูปที่ 3.6 แสดงตาราง configuration

Database : Radius

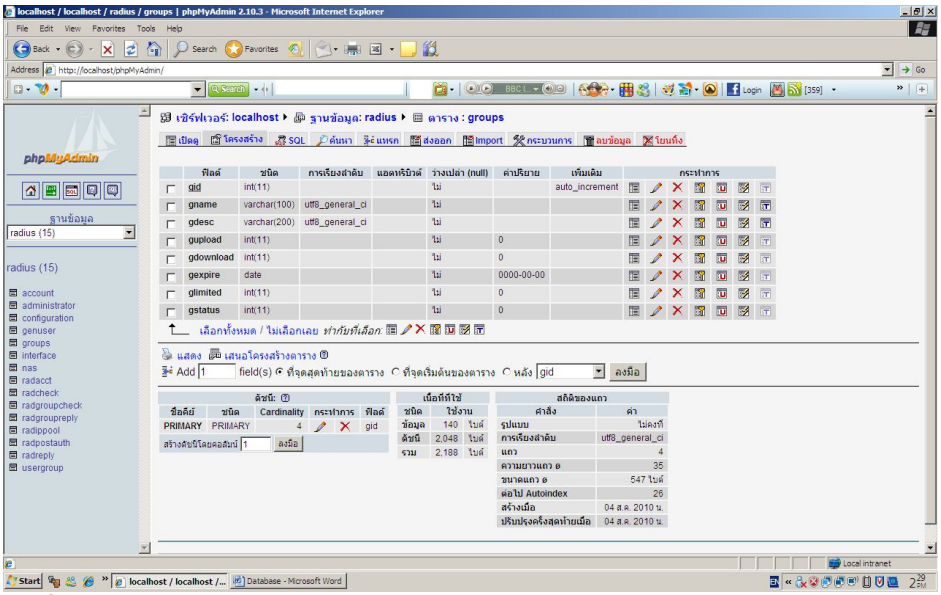
Table : genuser



รูปที่ 3.7 แสดงตาราง genuser

Database : Radius

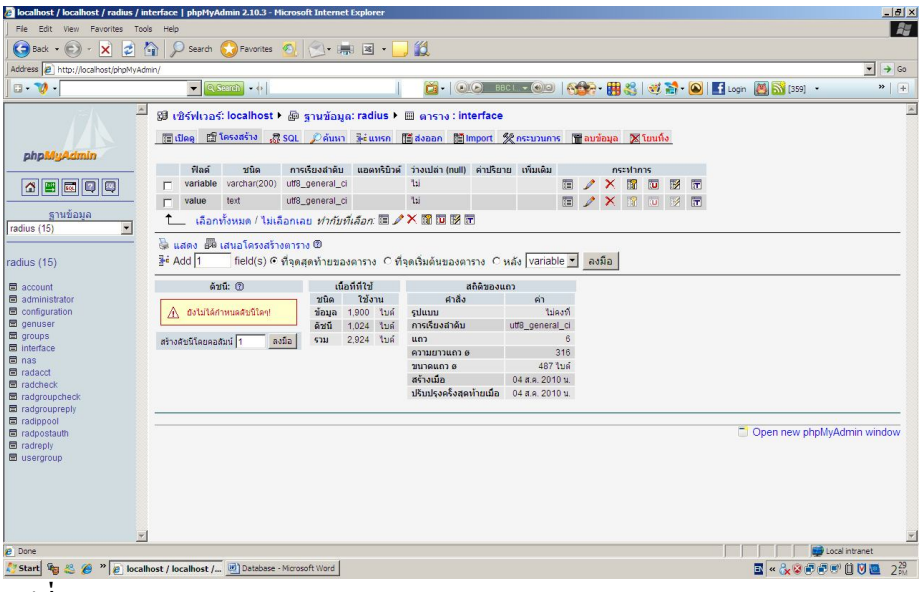
Table : group



รูปที่ 3.8 แสดงตาราง group

Database : Radius

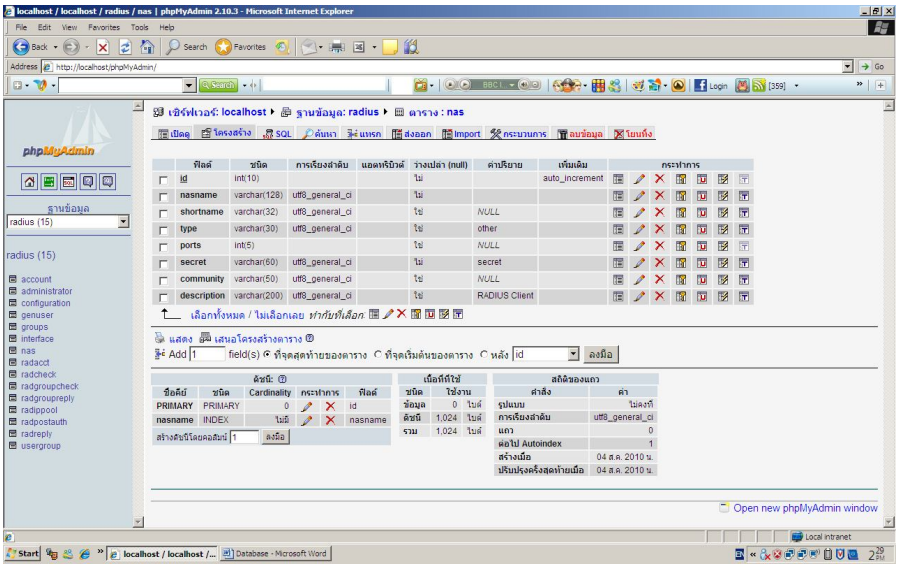
Table : interface



รูปที่ 3.9 แสดงตาราง interface

Database : Radius

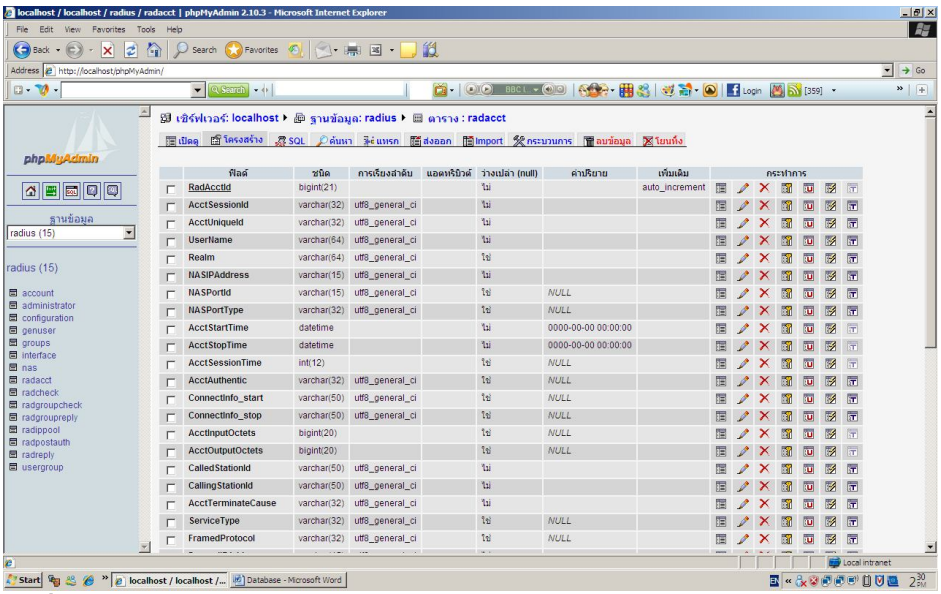
Table : nas



รูปที่ 3.10 แสดงตาราง nas

Database : Radius

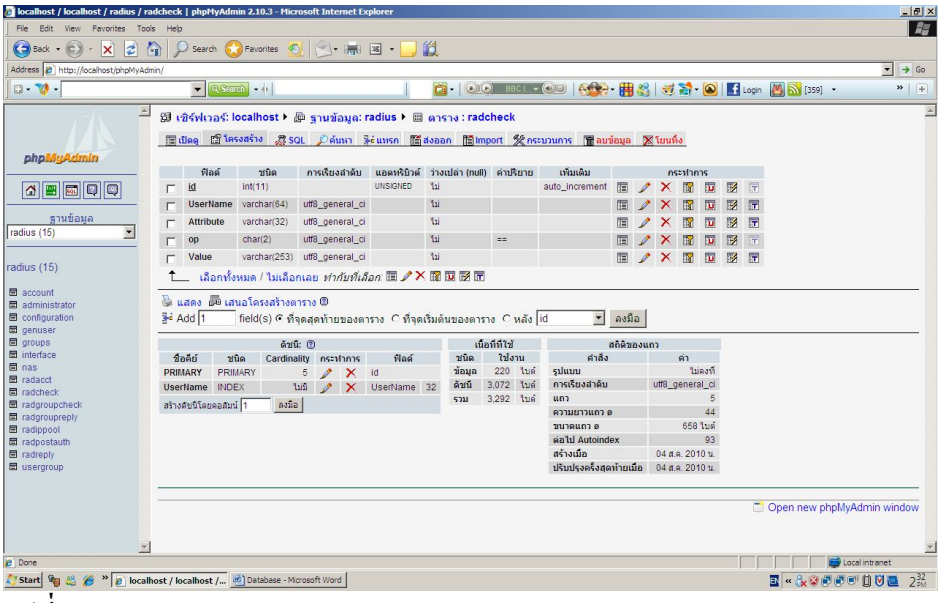
Table : radacct



รูปที่ 3.11 แสดงตาราง radacct

Database : Radius

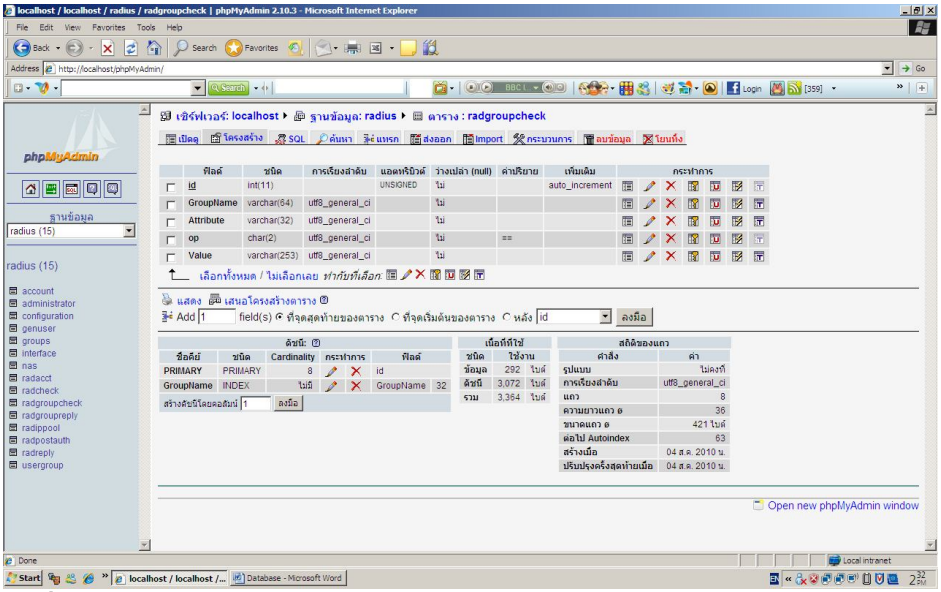
Table : radcheck



รูปที่ 3.12 แสดงตาราง radcheck

Database : Radius

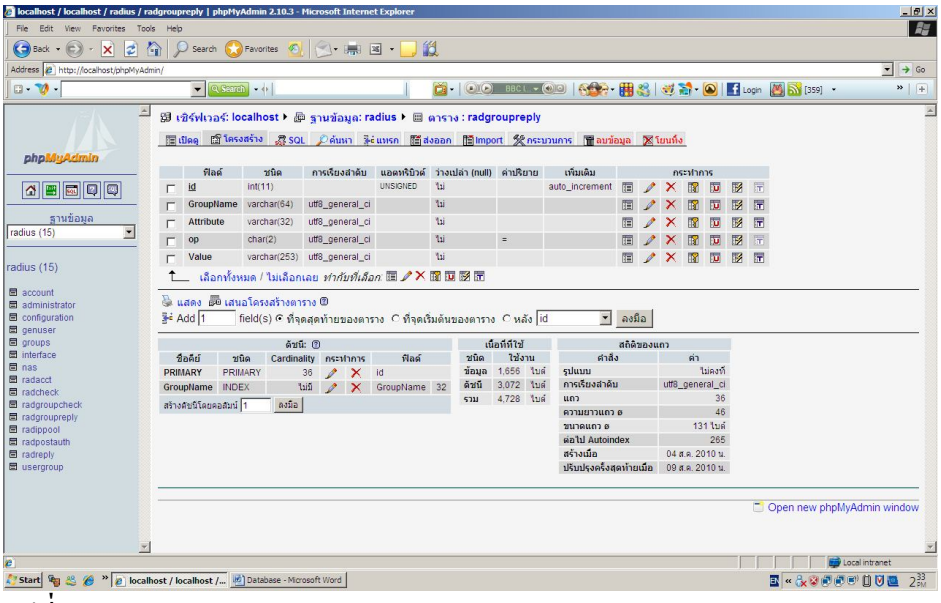
Table : radgroupcheck



รูปที่ 3.13 แสดงตาราง radgroupcheck

Database : Radius

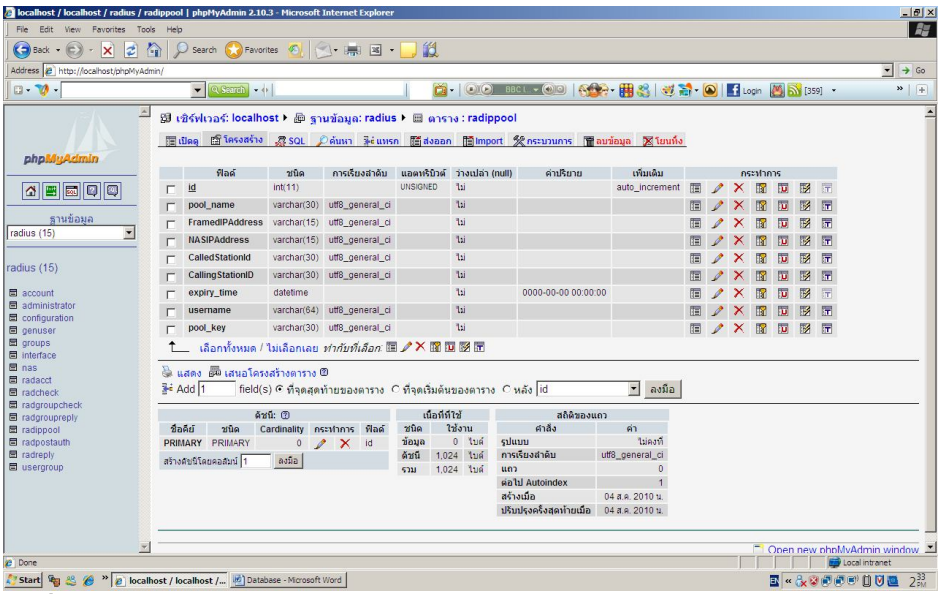
Table : radgroupreply



รูปที่ 3.14 แสดงตาราง radgroupreply

Database : Radius

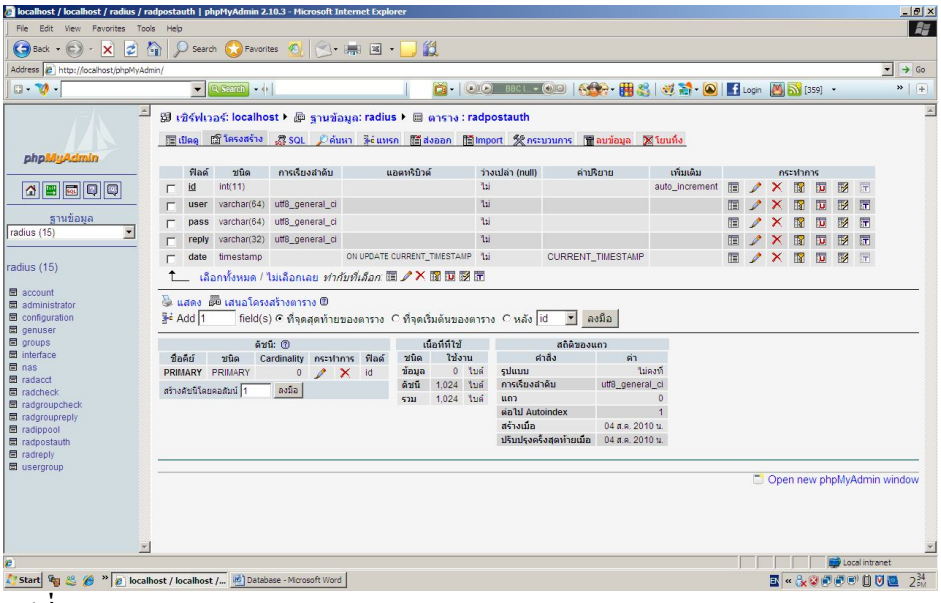
Table : radippool



รูปที่ 3.15 แสดงตาราง radippool

Database : Radius

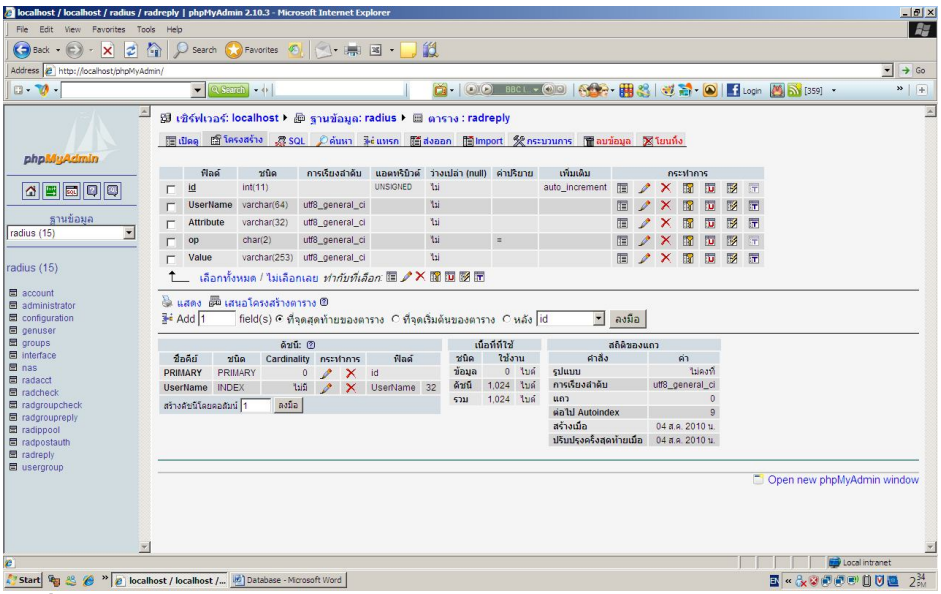
Table : radpostauth



รูปที่ 3.16 แสดงตาราง radpostauth

Database : Radius

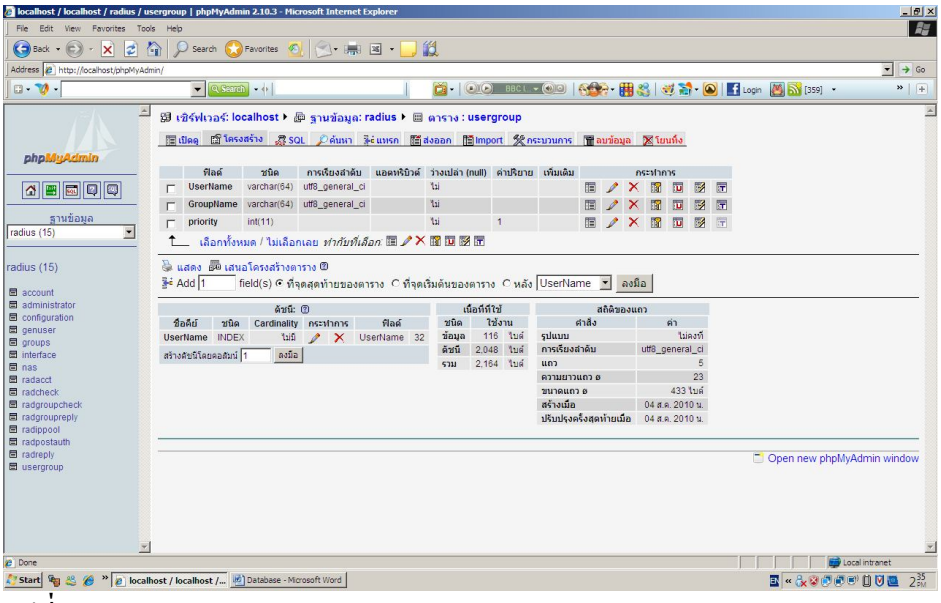
Table : radreply



รูปที่ 3.17 แสดงตาราง radreply

Database : Radius

Table : usergroup



รูปที่ 3.18 แสดงตาราง usergroup

3.6 ระบบเทียบเวลาสากล

ระบบเทียบเวลาสากล (Network Time Protocol : NTP) ข้อมูลจราจรที่ดีจะต้องสามารถตรวจสอบเวลาที่เกิดเหตุการณ์ (event) ให้อย่างถูกต้องตรงตามความเป็นจริง ดังนั้นพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และประกาศกระทรวง เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการฉบับนี้จึงกำหนดให้มีการอ้างอิงเวลากับการอ้างอิงเวลาสากล (Stratum0) สำหรับ NTP Server ที่ทางราชการแนะนำ สามารถเลือกใช้ NTP Server ที่มีอยู่ในประเทศไทย (ได้เพิ่ม NTP Server ที่ไม่ได้อยู่ในประเทศไทยอีก 2 ตัว คือ www.pool.ntp.org และ NIST, US) โดยมีรายชื่อดังนี้

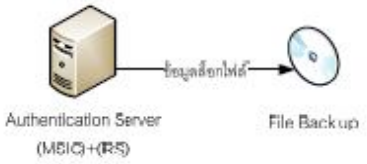
ตารางที่ 3.2 รายชื่อ NTP Server ที่มีอยู่ในประเทศไทย

สถาบัน	NTP Server	Clock Strata
สถาบันมาตรวิทยาแห่งชาติ	time1.nimt.or.th	Stratum1
	time2.nimt.or.th	Stratum1
สถาบันมาตรวิทยาแห่งชาติ	time3.nimt.or.th	Stratum1
กระทรวงวิทยาศาสตร์และเทคโนโลยี	time.most.go.th	Stratum2
กรมอุทกศาสตร์ กองทัพเรือ	time.navy.mi.th	Stratum1
มหาวิทยาลัยเกษตรศาสตร์	ntp.ku.ac.th	ไม่ระบุข้อมูล
มหาวิทยาลัยสงขลานครินทร์	time.psu.ac.th	Stratum1
NECTEC	clock.thaicert.nectec.or.th	ไม่ระบุข้อมูล
http://www.pool.ntp.org	th.pool.ntp.org	Stratum1
National Institute of Standards and Technology, US	time.nist.gov	Stratum1

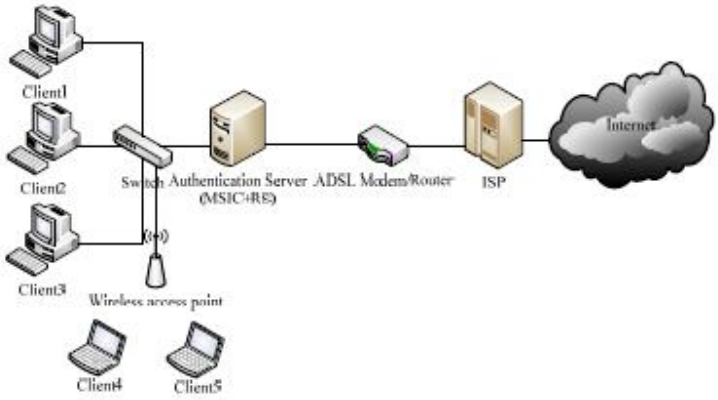
โดยทางอินเทอร์เนตจะต้องติดตั้งระบบ NTP Server เพื่อตั้งค่านาฬิกาของระบบทั้งเครือข่ายให้ตรงกัน โดยอ้างอิงจาก Stratum 0 และ ปรับแต่งค่าเครื่องแม่ข่ายและอุปกรณ์เครือข่ายให้อ้างอิงเวลากับ NTP Server ดังกล่าว

3.7 การจัดเก็บล็อกไฟล์

การจัดเก็บล็อกไฟล์ (Centralize Log)เนื่องจากเมื่อมีการใช้งานอินเทอร์เน็ตของสมาชิกเกิดขึ้นก็ได้เกิดล็อกไฟล์ซึ่งเป็นการบันทึกการกระทำต่างๆ ที่เกิดขึ้น ดังนั้นจึงจำเป็นที่ต้องมีการเก็บล็อกไฟล์ดังกล่าวไว้ในเครื่องพร้อมกันนี้ต้องมีการสำรองข้อมูลล็อกไฟล์ไว้ที่อื่นด้วยซึ่งอาจจะอยู่ในรูปแผ่นซีดีหรืออย่างอื่นก็ได้โดยวิธีการเลือกเก็บ ล็อกไฟล์เป็นวิธีการที่สมาชิกหรือผู้ดูแลระบบไม่สามารถแก้ไขข้อมูลล็อกไฟล์ย้อนหลังได้แนะนำควรเก็บไว้ในแผ่นซีดีเนื่องจากมีราคาถูกและไม่สามารถแก้ไขข้อมูลได้ และต้องบันทึกล็อกไฟล์ตามข้อมูลกิจกรรมที่เกิดขึ้นและบันทึกเป็นวันต่อวันหรือจัดทำเป็นการจัดเก็บล็อกไฟล์ เพื่อมีไว้สำหรับบันทึกข้อมูลจราจรบนระบบเครือข่ายคอมพิวเตอร์ทั้งระบบ



รูปที่ 3.19 แสดงการสำรองข้อมูลล็อกไฟล์



รูปที่ 3.20 แผนภาพเครือข่ายในอินเทอร์เนตที่ถูกออกแบบเพื่อให้รองรับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

3.8 พัฒนาแอพพลิเคชั่นจัดการระบบจัดการฐานข้อมูลผู้ใช้อินเทอร์เนต

พัฒนาแอพพลิเคชั่นจัดการระบบจัดการฐานข้อมูลผู้ใช้อินเทอร์เนต (Application User Manager Internet Account for Administrator.) ได้ใช้ระบบปฏิบัติการ FreeBSD ระบบฐานข้อมูล MySQL และใช้โปรแกรมภาษา PHP Programming Language ในการพัฒนาระบบโดยใช้โอเพนซอร์สที่มีอยู่แล้วมาพัฒนาต่อ ได้แก่ EZ Radius , Dalo Radius , Authentication ของมหาวิทยาลัยบูรพา

3.9 การอิมพลีเมนต์ระบบอินเทอร์เนตเกตเวย์สำหรับมหาวิทยาลัย

การอิมพลีเมนต์ระบบอินเทอร์เนตเกตเวย์สำหรับมหาวิทยาลัย (Implementation of Internet Gateway For University โดยตั้งค่าระบบใหม่ทั้งมหาวิทยาลัยให้สามารถใช้งานได้ทั้งหมด ดังนี้

3.9.1 Firewall

3.9.2 NAT

3.9.3 DHCP

3.9.4 Proxy Server

3.9.5 DNS,Database Server

3.9.6 Webserver

3.9.7 Mail Server

3.9.8 FTP Server

3.10 ประยุกต์ใช้งานระบบอินเทอร์เนตเกตเวย์มหาวิทยาลัย

ประยุกต์ใช้งานระบบอินเทอร์เนตเกตเวย์ โดยเดินสายใยแก้วนำแสงเชื่อมโยงไปตามจุดต่างๆ ที่สำคัญและปล่อยสัญญาณ WiFi ในบริเวณที่มีนักศึกษาและบุคลากรใช้งานเป็นจำนวนมาก ในมหาวิทยาลัย ซึ่งปล่อยสัญญาณไปในระบบเครือข่ายทั้ง 2 ระบบ คือ

1) แบบไวไฟ (WiFi)

2) ลีสไลน์ (Lease)

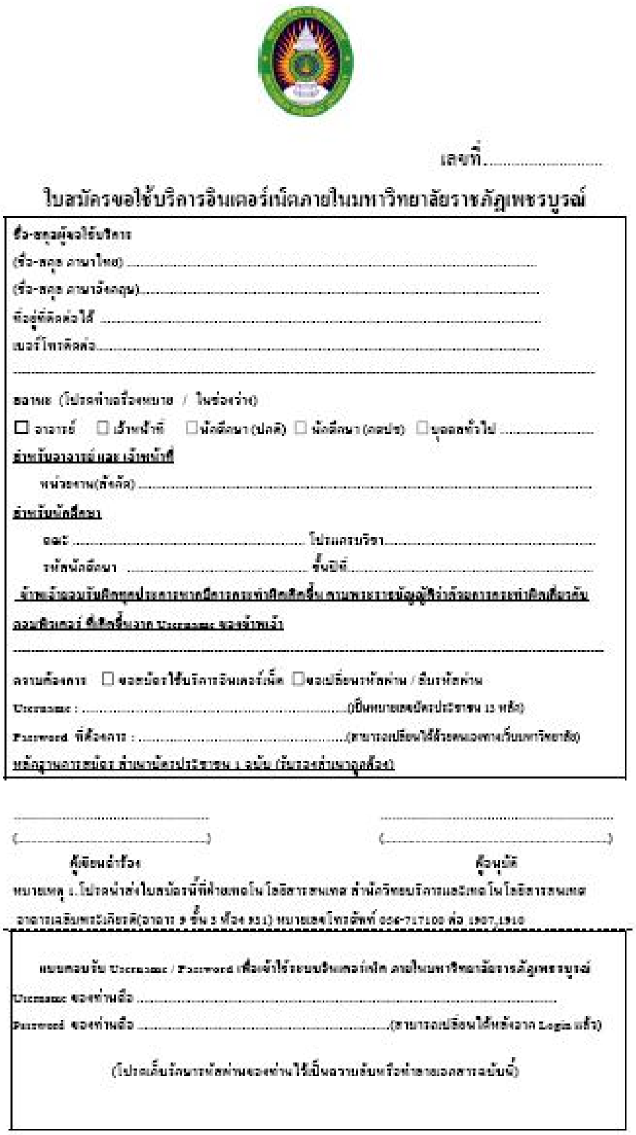
บทที่ 4
ผลการวิจัย

จากบทข้างต้นได้ทำการวิเคราะห์และออกแบบระบบเครือข่ายในอินเทอร์เน็ตเพื่อรองรับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ. 2550 ซึ่งบทนี้จะเป็นการนำระบบที่ได้ออกแบบไว้มาพัฒนาเป็นระบบที่ใช้งานได้จริงอันได้แก่การพัฒนาระบบฐานข้อมูลสำหรับเก็บข้อมูลผู้ใช้งานอินเทอร์เน็ต การพัฒนาระบบค้นคืนและระบุผู้ใช้งานในอินเทอร์เน็ตการพัฒนาหน้าจอเข้าสู่อินเทอร์เน็ตสำหรับสมาชิก การตั้งค่าเทียบเวลาระหว่างอุปกรณ์คอมพิวเตอร์และการตั้งค่าเก็บข้อมูลล็อกไฟล์ ซึ่งทั้งหมดที่กล่าวมานี้คือระบบเก็บข้อมูล พิสูจน์ตัวตน ค้นคืนและระบุผู้ใช้บริการอินเทอร์เน็ต

4.1 การออกแบบฟอร์มการขอใช้บริการอินเทอร์เนต และระบบเครือข่าย

แบบฟอร์มการขอใช้บริการระบบอินเทอร์เนตภายในมหาวิทยาลัย ซึ่งมีบริการให้ใช้หลายบริการ ได้แก่

1) แบบฟอร์มการขอใช้บริการอินเทอร์เนต สำหรับบุคลากรได้แก่ อาจารย์ เจ้าหน้าที่และนักศึกษา



เลขที่...........................

ใบสมัครขอใช้บริการอินเตอร์เน็ตภายในมหาวิทยาลัยราชภัฏเพชรบูรณ์

ชื่อ-สกุลผู้ขอใช้บริการ

(ชื่อ-สกุล ภาษาไทย) ....

(ชื่อ-สกุล ภาษาอังกฤษ)..

ที่อยู่ที่ติดต่อได้ ....

เบอร์โทรติดต่อ..

สถานะ (โปรดทำเครื่องหมาย / ในช่องว่าง)

☐ อาจารย์ ☐ เจ้าหน้าที่ ☐ นักศึกษา (ปกติ) ☐ นักศึกษา (กศปช) ☐ บุคคลทั่วไป ....

สำหรับอาจารย์ และ เจ้าหน้าที่

หน่วยงาน(สังกัด) ....

สำหรับนักศึกษา

คณะ .... โปรแกรมวิชา.......................................

รหัสนักศึกษา .... ชั้นปีที่.......................................

ข้าพเจ้ายอมรับผิดชอบประการหากมีการกระทำผิดเกิดขึ้น ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ที่เกิดขึ้นจาก Username ของข้าพเจ้า

ความต้องการ ☐ ขอสมัครใช้บริการอินเตอร์เน็ต ☐ ขอเปลี่ยนรหัสผ่าน / ลืมรหัสผ่าน

Username : ....(เป็นหมายเลขบัตรประชาชน 13 หลัก)

Password ที่ต้องการ : ....(สามารถเปลี่ยนได้ด้วยตนเองทางเว็บมหาวิทยาลัย)

หลักฐานการสมัคร สำเนาบัตรประชาชน 1 ฉบับ (รับรองสำเนาถูกต้อง)

....

(.......................................) (.......................................)

ผู้เขียนคำร้อง ผู้อนุมัติ

หมายเหตุ 1.โปรดนำส่งใบสมัครนี้ที่ฝ่ายเทคโนโลยีสารสนเทศ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ อาคารเฉลิมพระเกียรติ(อาคาร 9 ชั้น 3 ห้อง 931) หมายเลขโทรศัพท์ 056-717100 ต่อ 1907,1910

แบบตอบรับ Username / Password เพื่อเข้าใช้ระบบอินเตอร์เน็ต ภายในมหาวิทยาลัยราชภัฏเพชรบูรณ์

Username ของท่านคือ ....

Password ของท่านคือ ....(สามารถเปลี่ยนได้หลังจาก Login แล้ว)

(โปรดเก็บรักษารหัสผ่านของท่านไว้เป็นความลับหรือทำลายเอกสารฉบับนี้)

รูปที่ 4.1 แสดงแบบฟอร์มการขอใช้บริการอินเทอร์เนต

2) แบบฟอร์มการขอใช้บริการ Email สำหรับบุคลากรได้แก่ อาจารย์ เจ้าหน้าที่ และนักศึกษา

PCRU Mail
บริการอีเมล์
มหาวิทยาลัยราชภัฏเพชรบูรณ์

ใบสมัคร ขอใช้บริการอีเมล์ มหาวิทยาลัยราชภัฏเพชรบูรณ์

ชื่อ-สกุลผู้ขอใช้บริการ
(ชื่อ-สกุล ภาษาไทย) .....
(ชื่อ-สกุล ภาษาอังกฤษ).....
ที่อยู่ .....
เบอร์โทรติดต่อ.....

ขอเพย (โปรดทำเครื่องหมาย x ในช่องว่าง) [ ] อาจารย์ [ ] เจ้าหน้าที่
[ ] นักศึกษา [ ] บุคลทั่วไป

อาจารย์ และ เจ้าหน้าที่
ชื่อหน่วยงาน(สังกัด) .....

นักศึกษา
คณะ .....
โปรแกรมวิชา .....
รหัสนักศึกษา(12 หลัก) ..... ชั้นปี .....

ความต้องการ [ ] ขอสมัครใช้บริการอีเมล์ [ ] รีเซ็ตรหัสผ่าน

E-mail : .....@pcru.ac.th

Password : .....

หลักฐานการสมัคร สำเนาบัตรประชาชน 1 ฉบับ (เซ็นสำเนาถูกต้อง)
สำหรับนักศึกษาที่ขอใช้บริการอีเมล์ครั้งแรกแล้ว ไม่ต้องใช้สำเนาบัตรประชาชน

....
(.....) (.....)
ผู้ขอใช้บริการ ผู้อนุมัติ

หมายเหตุ 1.โปรดนำส่งใบสมัครนี้ ที่ ศูนย์เทคโนโลยีสารสนเทศ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ อาคาร 9 ชั้น 3 ห้อง 931 หมายเลขโทรศัพท์ 1907,1910
2. แจ้งปัญหาการใช้งานได้ที่ ศูนย์เทคโนโลยีสารสนเทศโทร 056-717100 ต่อ 2012,1907,1910

สำหรับเจ้าหน้าที่

แบบตอบรับ เพื่อเข้าใช้ อีเมล์

E-Mail ของท่านคือ .....@pcru.ac.th

Password ของท่านคือ .....(สามารถเปลี่ยน password ได้ในเมนู "ปรับแต่ง")

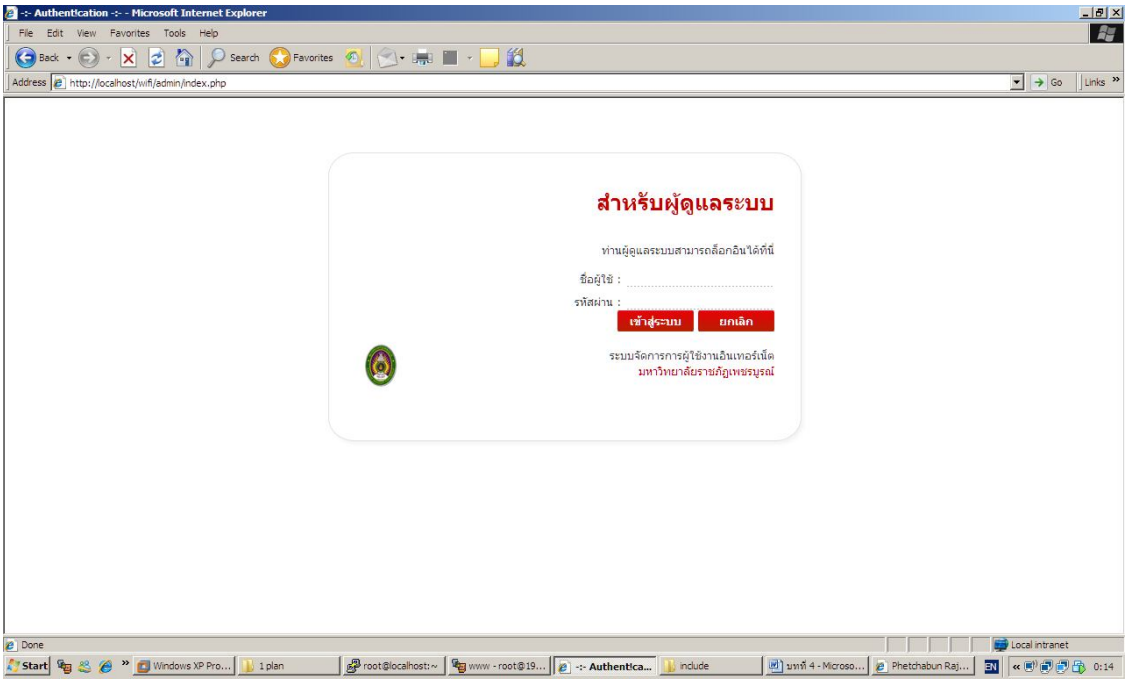
รูปที่ 4.2 แสดงแบบฟอร์มการขอใช้บริการ Email

4.2 การพัฒนาระบบฐานข้อมูลสำหรับเก็บข้อมูลผู้ใช้งานอินเทอร์เน็ต

จากการพัฒนาระบบฐานข้อมูลสำหรับเก็บข้อมูลผู้ใช้งานอินเทอร์เน็ต ซึ่งระบบถูกใช้โดยผู้ดูแลระบบ ผู้ดูแลระบบสามารถจัดการข้อมูลสมาชิก ได้แก่ เพิ่มผู้ใช้ใหม่ จัดการข้อมูลผู้ใช้ จัดการกลุ่ม

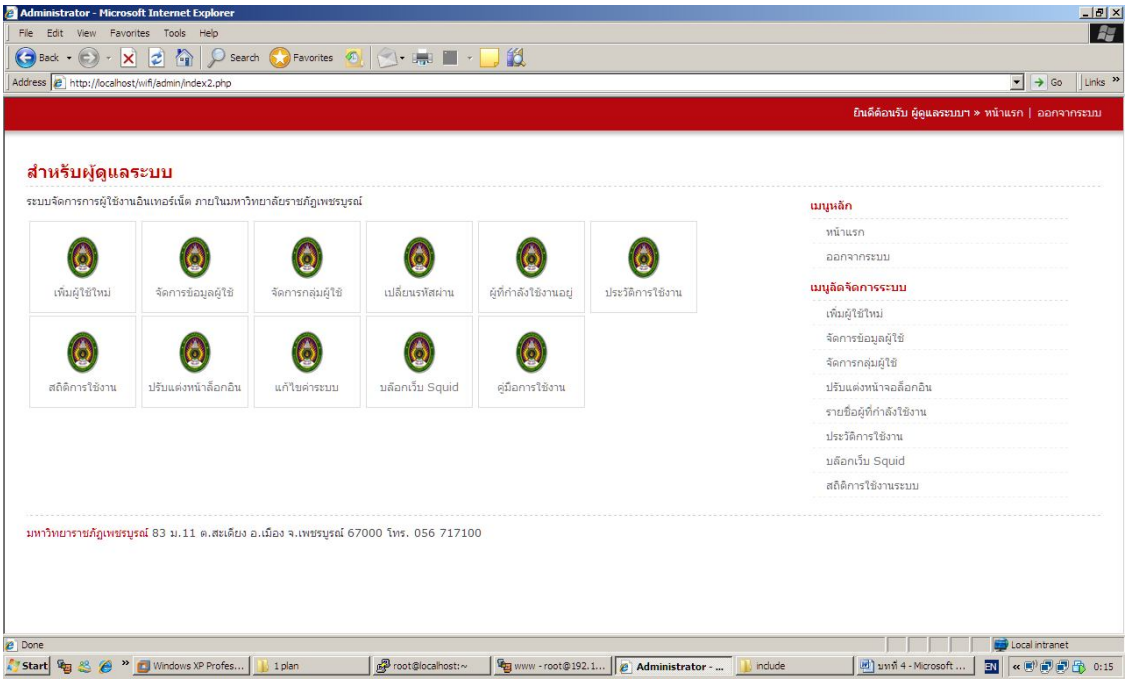
ผู้ใช้ เปลี่ยนรหัสผ่าน ผู้ที่กำลังใช้งาน ประวัติการใช้งาน สถิติการใช้งาน ปรับแต่งหน้าจอล็อกอิน แก้ไขค่าระบบ บล็อกเว็บไซท์ คู่มือการใช้งาน ผู้ดูแลระบบสามารถจัดการข้อมูลผู้ดูแลระบบ ได้แก่ เพิ่มข้อมูลผู้ดูแลระบบ เปลี่ยนรหัสผ่านสำหรับผู้ดูแลระบบและผู้ดูแลระบบสามารถจัดการสิทธิ์การเข้าใช้อินเทอร์เน็ตของสมาชิก นอกจากที่กล่าวมาแล้วระบบยังสามารถเชื่อมโยงไปยังข้อมูลพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 จากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (คณะกรรมการธุรกรรมทางอิเล็คทรอนิกส์ 2550: ออนไลน์) เว็บไซท์ของระบบ และเชื่อมโยงไปยังมหาวิทยาลัย ซึ่งสามารถแสดงผลดังนี้

4.2.1 หน้าจอเมนูหน้าแรก ซึ่งจะแสดงหน้าแรกของระบบจัดการข้อมูลสำหรับเก็บข้อมูลผู้ใช้งานอินเทอร์เน็ต ระบบยังสามารถเชื่อมโยงไปยังข้อมูลพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 จากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (คณะกรรมการธุรกรรมทางอิเล็คทรอนิกส์ 2550: ออนไลน์) เว็บไซท์ของระบบ และเชื่อมโยงไปยังเว็บต่างๆที่เกี่ยวข้อง โดยในหน้าแรกยังเป็นหน้าจอเข้าสู่ระบบเพื่อต้องการเข้าสู่ระบบฐานข้อมูลสำหรับเก็บข้อมูลผู้ใช้งานอินเทอร์เน็ต



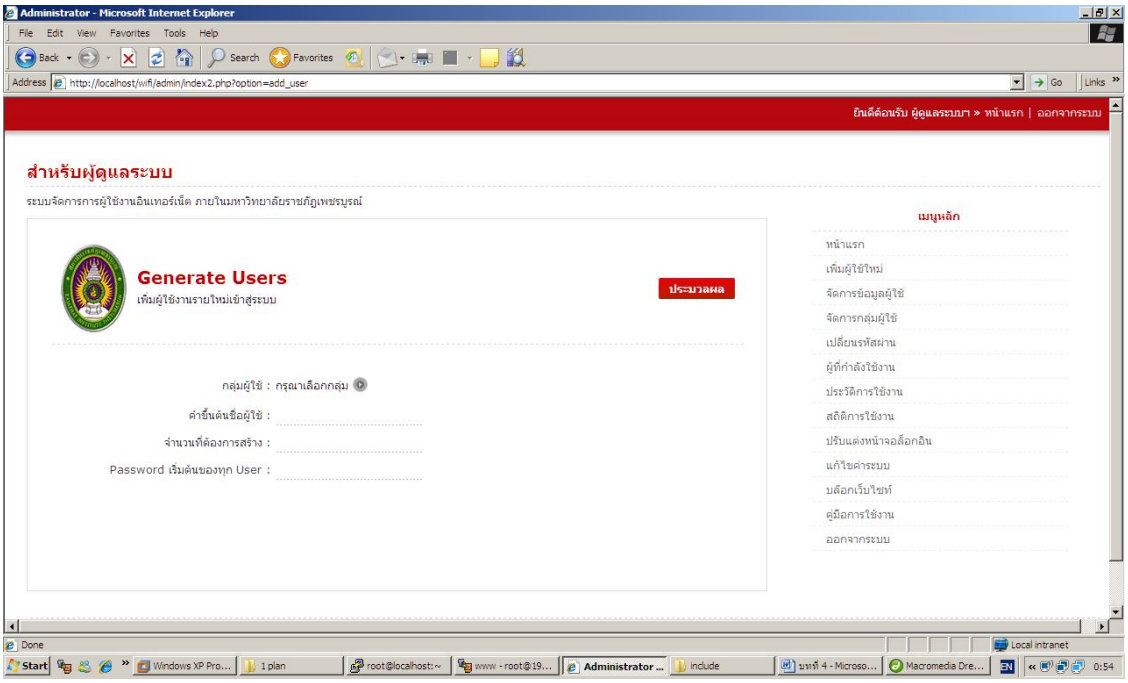
รูปที่ 4.3 หน้าจอเมนูหน้าแรกสำหรับผู้ดูแลระบบ

4.2.2 หน้าจอหลักของผู้ดูแลระบบ เมื่อเข้าสู่ระบบ ระบบจะแสดงสิทธิ์ต่างๆ ที่ผู้ดูแลระบบสามารถกระทำในระบบได้



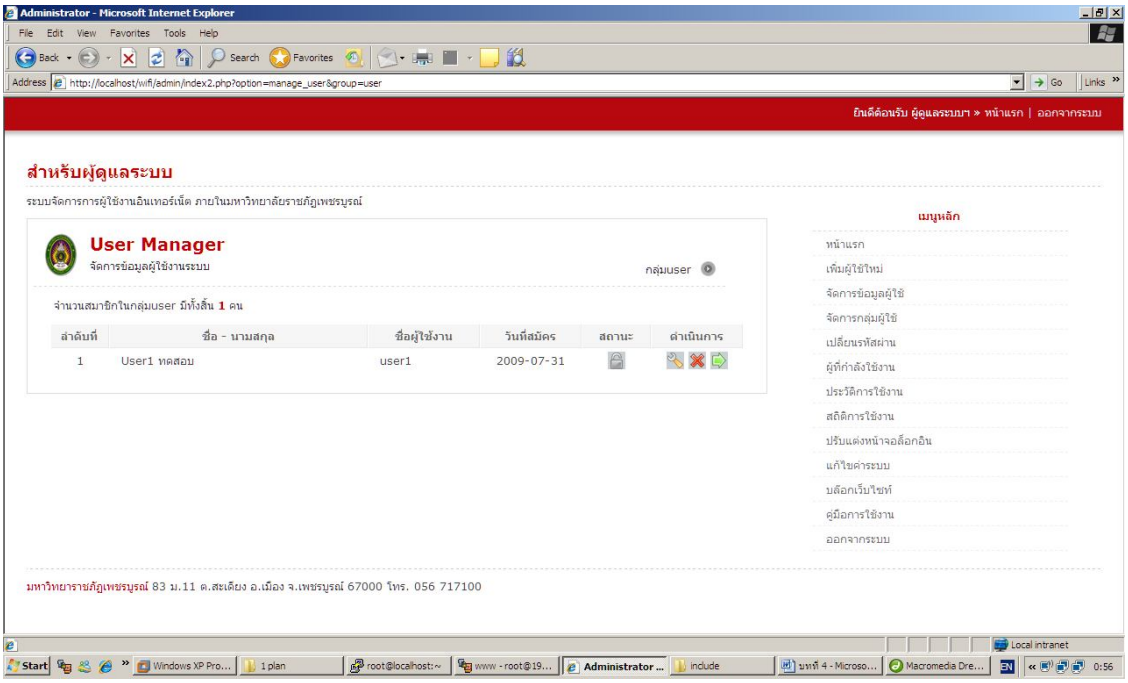
รูปที่ 4.4 แสดงหน้าจอหลักของผู้ดูแลระบบของระบบ

4.2.3 หน้าจอเมนูสร้างบัญชีผู้ใช้งานให้สมาชิกโดย Generate Users เป็นส่วนแสดงที่แสดงหน้าจอสร้าง ชื่อและรหัสผ่านให้สมาชิกแบบทีเดียวได้หลายผู้ใช้ โดยจะแสดงรายชื่อสมาชิกเพื่อให้เลือกว่าจะสร้างรหัสผ่านให้สมาชิกคนใด



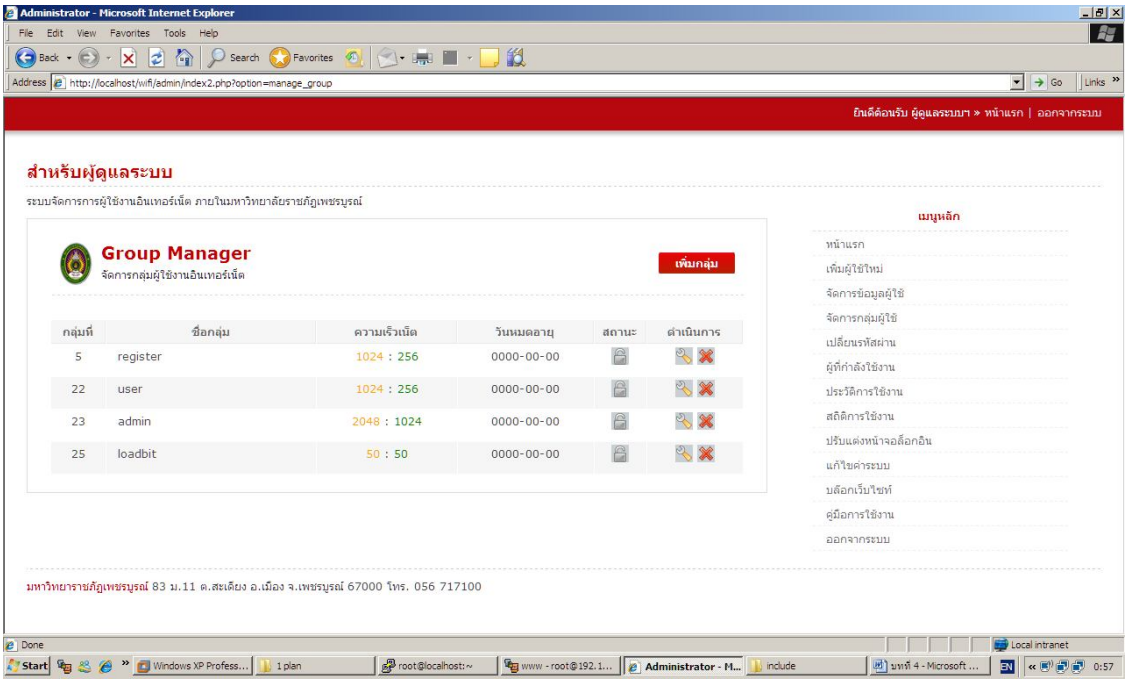
รูปที่ 4.5 แสดงหน้าจอเมนูเพิ่มผู้ใช้

4.2.4 หน้าจอเมนูจัดการข้อมูลสมาชิกเป็นส่วนแสดงที่แสดงหน้าจอเพิ่ม ลบ แก้ไข ข้อมูลสมาชิกโดยข้อมูลที่เพิ่มนั้นได้มาจากบัตรประจำตัวประชาชนบัตรใบขับขี่ บัตรทอง 30 บาท บัตรนักเรียน/นักศึกษา หรือกำหนดขึ้นมาใหม่ได้ เป็นต้น



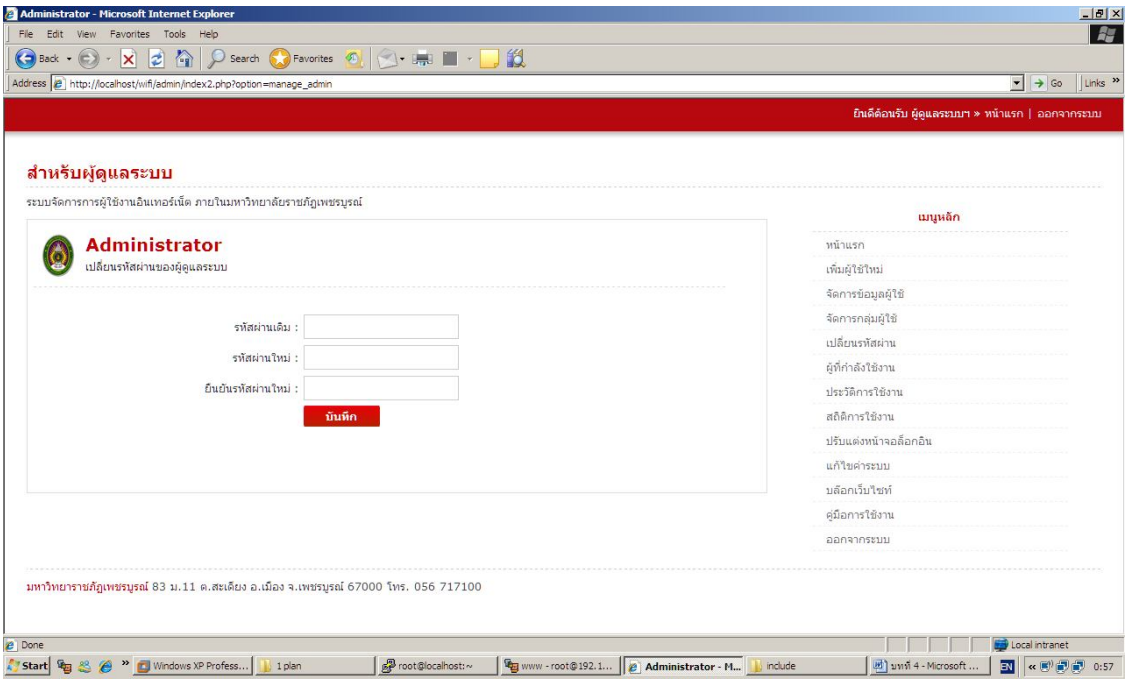
รูปที่ 4.6 แสดงหน้าจอเมนูจัดการข้อมูลสมาชิกของระบบ

4.2.5 หน้าจอเมนูจัดการกลุ่มผู้ใช้ เป็นส่วนที่แสดงหน้าจอแก้ไขข้อมูลกลุ่มผู้ใช้โดยจะแสดงรายชื่อกลุ่มผู้ใช้เพื่อให้เลือกว่าจะแก้ไขข้อมูลกลุ่มใด



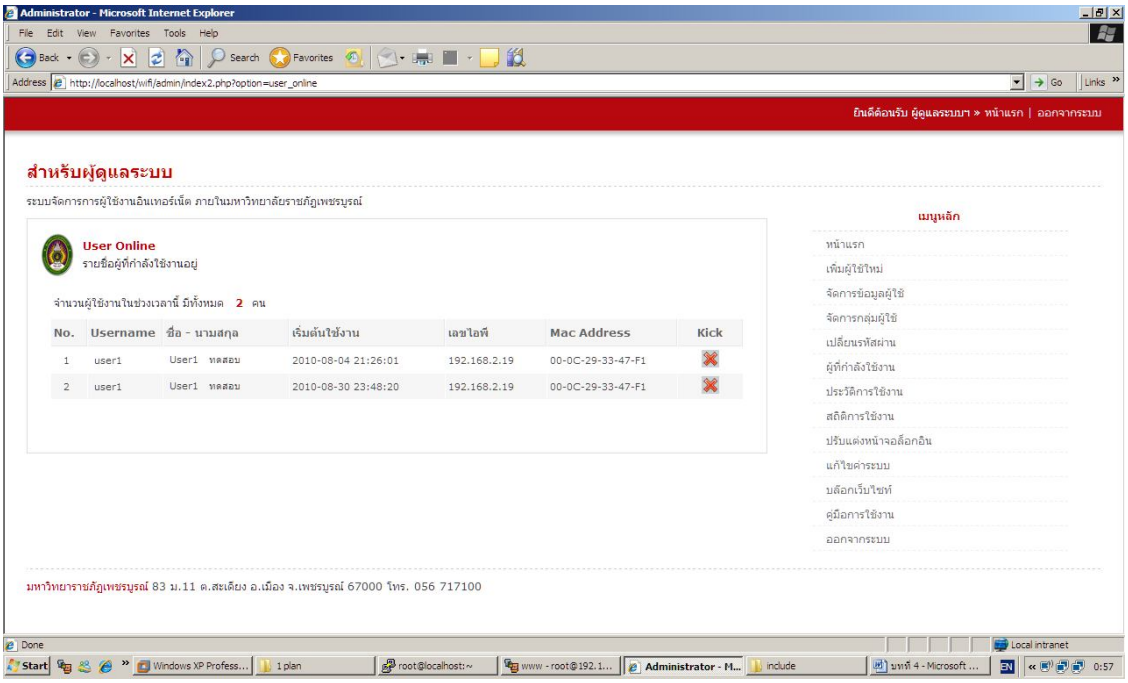
รูปที่ 4.7 แสดงหน้าจอเมนูแก้ไขข้อมูลจัดการกลุ่มผู้ใช้ระบบ

4.2.6 หน้าจอเมนูเปลี่ยนรหัสผ่าน Administrator



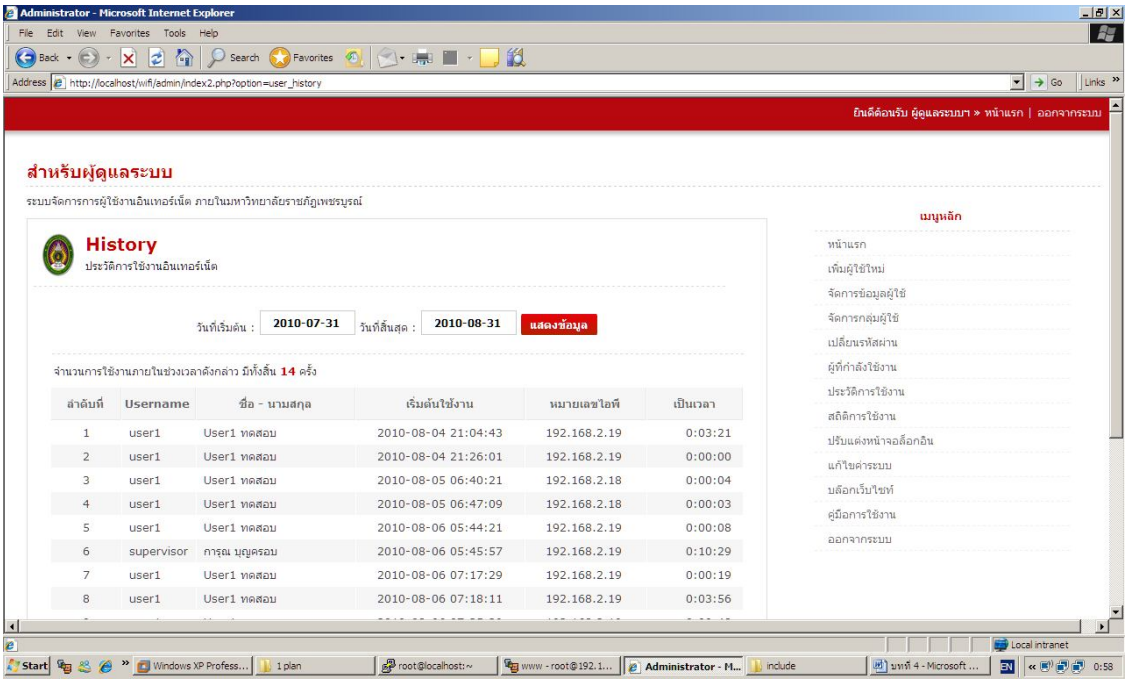
รูปที่ 4.8 แสดงหน้าจอเมนูเปลี่ยนรหัสผ่าน Administrator

4.2.7 หน้าจอเมนูจัดการ User Online เป็นหน้าจอแสดงเมนูจัดการผู้ใช้งานปัจจุบันที่กำลังออนไลน์ ใช้งานอยู่ สำหรับผู้ดูแลระบบ



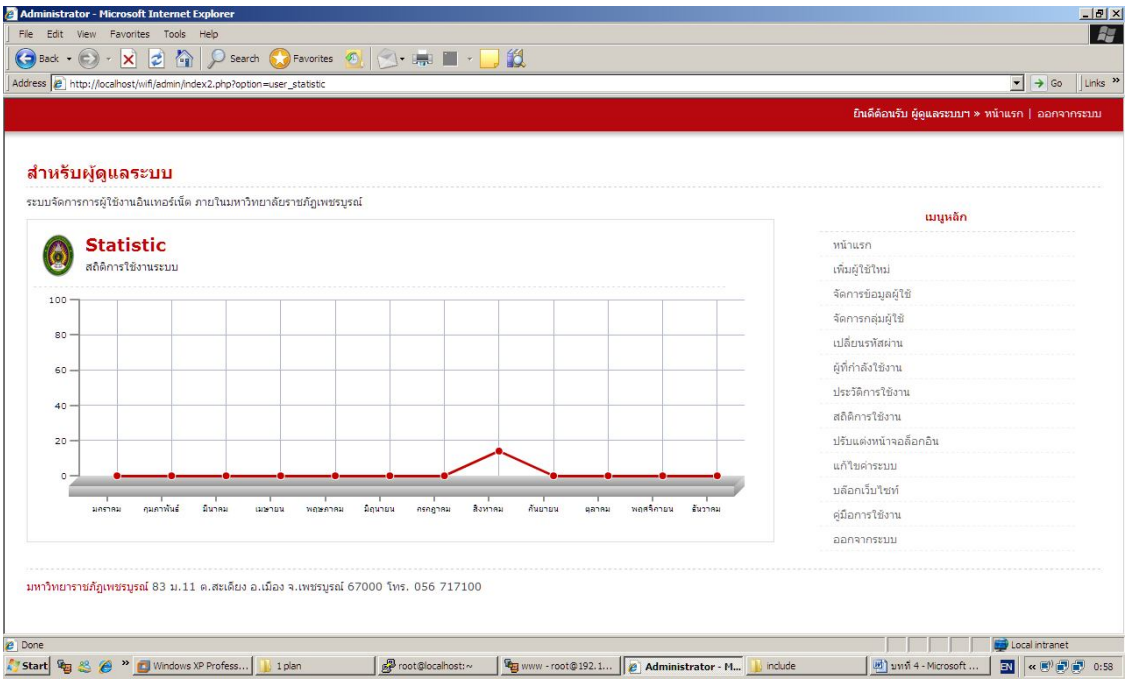
รูปที่ 4.9 แสดงหน้าจอเมนูจัดการ User Online

4.2.8 หน้าจอเมนูดูข้อมูลการใช้งานเป็นหน้าจอแสดงเมนูดูข้อมูลการใช้งานสำหรับผู้ดูแลระบบ โดยจะแสดงข้อมูลการเข้าใช้งานระบบของสมาชิกเรียงลำดับตามวันเวลาที่เข้าใช้ระบบ



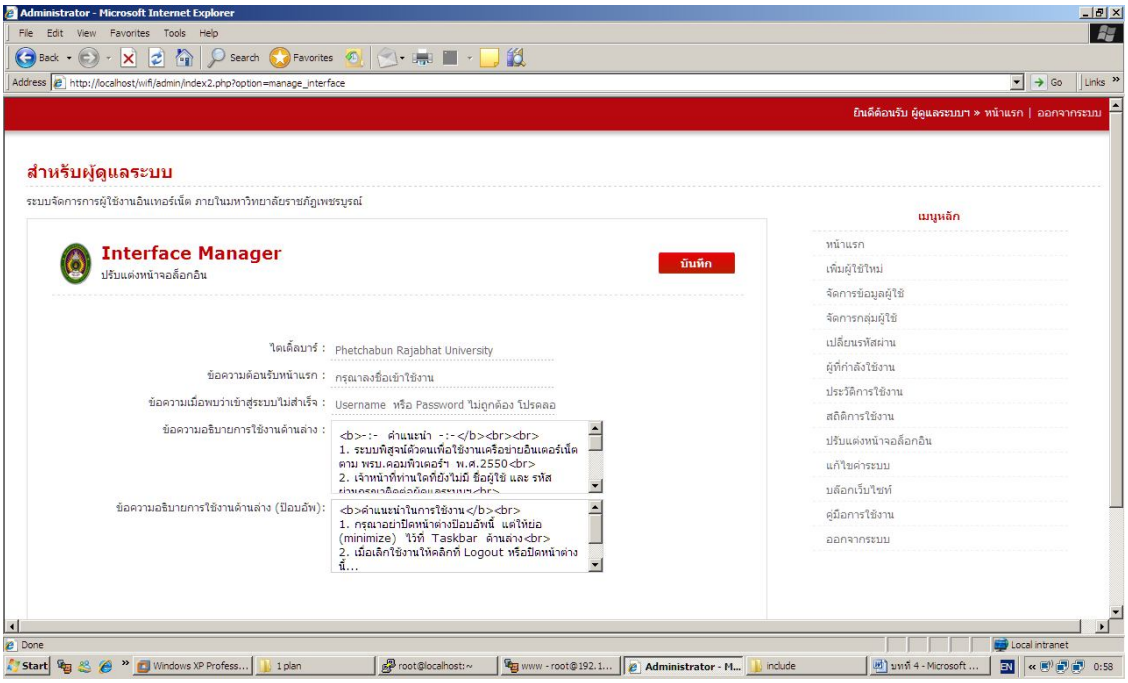
รูปที่ 4.10 แสดงหน้าจอเมนูดูข้อมูลการใช้งานของระบบ

4.2.9 หน้าจอเมนูแสดงสถิติผู้ใช้งานอินเทอร์เน็ต โดยจะมีรายละเอียด



รูปที่ 4.11 แสดงสถิติผู้ใช้งานอินเทอร์เน็ต

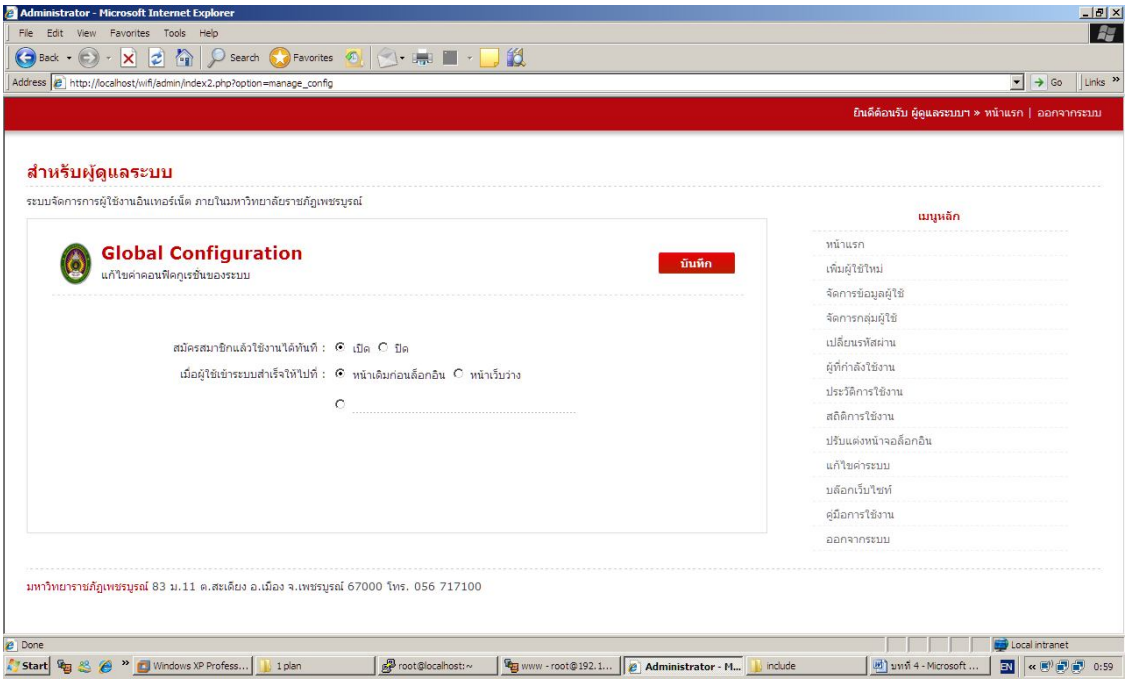
4.2.10 หน้าจอเมนู Interface Manager ปรับแต่งหน้าจอล็อกอินเป็นหน้าจอแสดงเมนูเปลี่ยนหน้าจอล็อกอินสำหรับผู้ดูแลระบบให้สมาชิกใช้ในการล็อกอิน



รูปที่ 4.12 แสดงหน้าจอเมนู Interface Manager

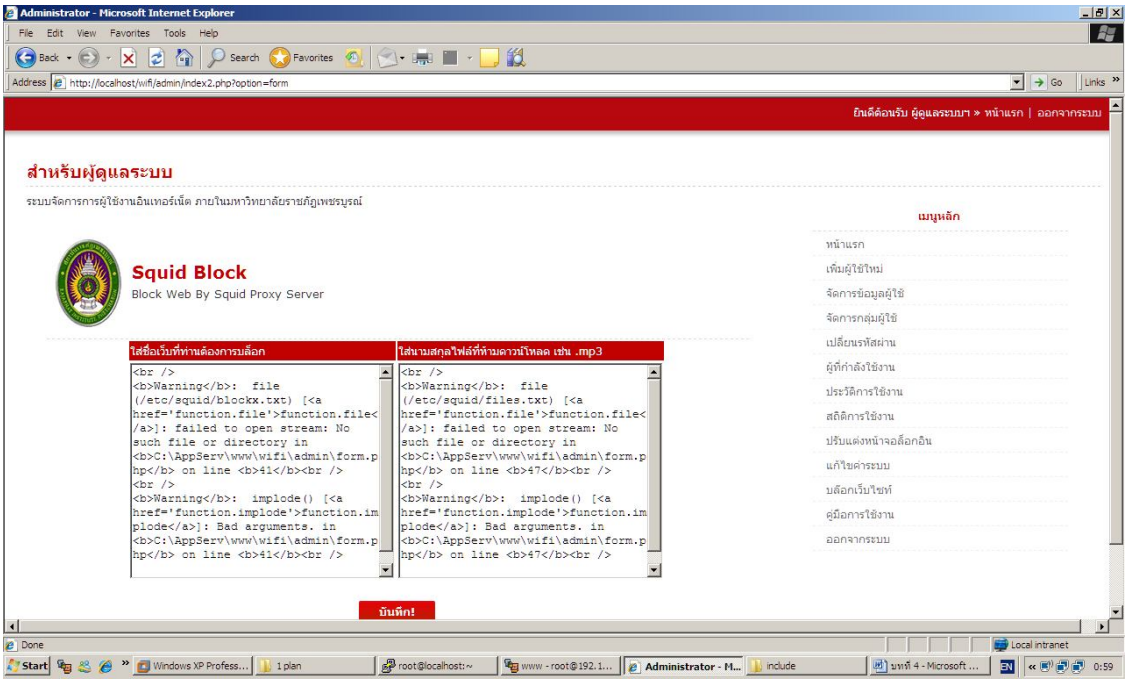
4.3 ผู้ดูแลระบบ (Administrator)

4.3.1 Global Configuration เป็นการแก้ไขค่าต่างๆ ในระบบ ได้แก่สมาชิกสมัครแล้วสามารถใช้งานได้ทันที ถ้าเปิด ถ้าหากปิด ให้ผู้ดูแลระบบเป็นผู้อนุญาตและ เมื่อสมาชิกสมัครสำเร็จให้ไปที่หน้าต่างล็อกอิน หรือหน้าต่างว่าง



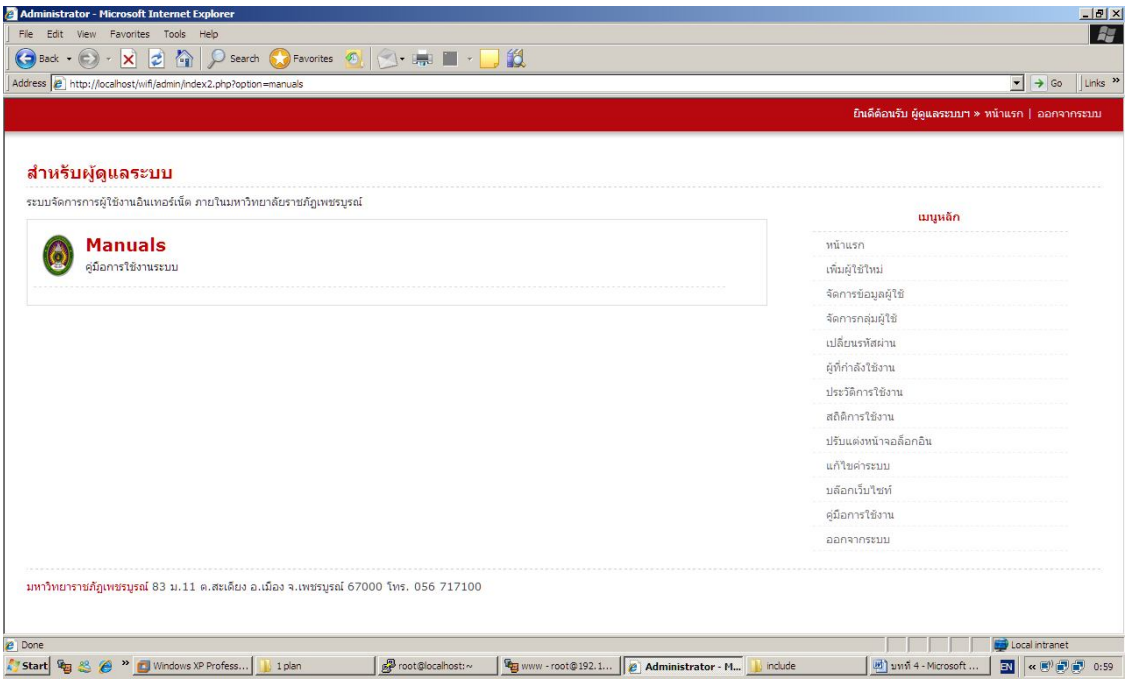
รูปที่ 4.13 แสดง Global Configuration

4.3.2 Squid Block การบล็อกเว็บไซท์ต่างๆ โดยผู้ดูแลระบบสามารถป้อนชื่อเว็บไซท์ที่ไม่พึงประสงค์เพื่อบล็อกผู้ใช้งานอินเทอร์เน็ต



รูปที่ 4.14 แสดงหน้าจอขั้นตอนการบล็อกข้อมูล

4.3.3 Manuals คู่มือการใช้งานระบบสำหรับผู้ใช้งานอินเทอร์เน็ต

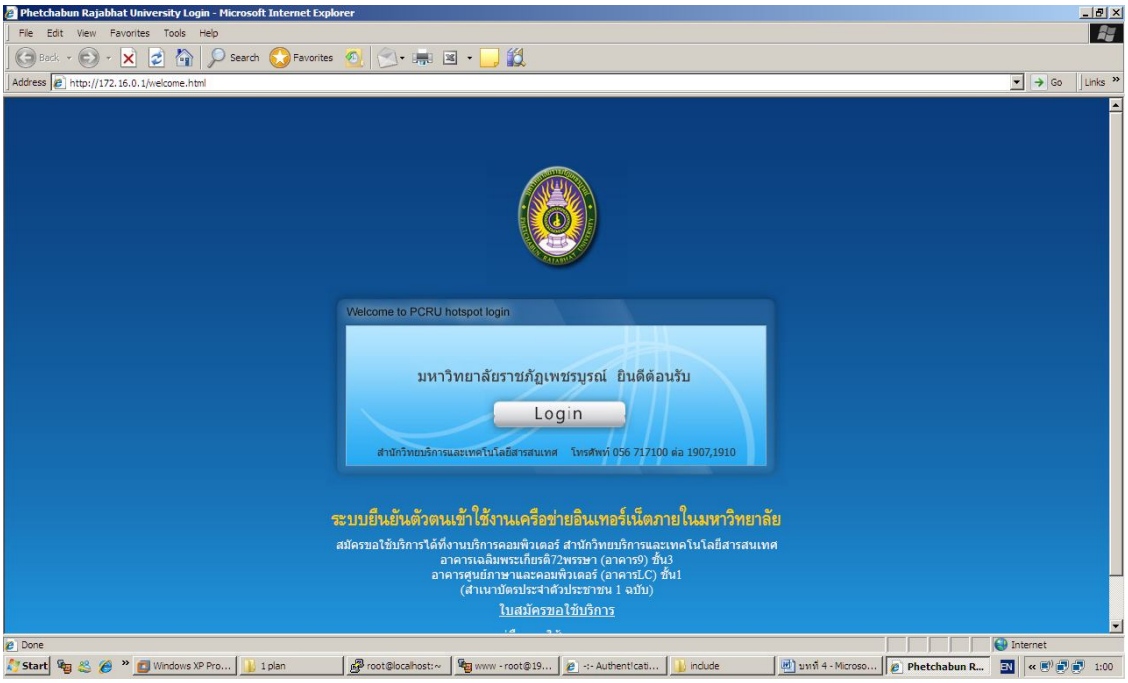


รูปที่ 4.15 แสดงหน้าจอคู่มือการใช้ระบบ

4.4 การพัฒนาหน้าจอเข้าสู่อินเทอร์เน็ตสำหรับสมาชิก

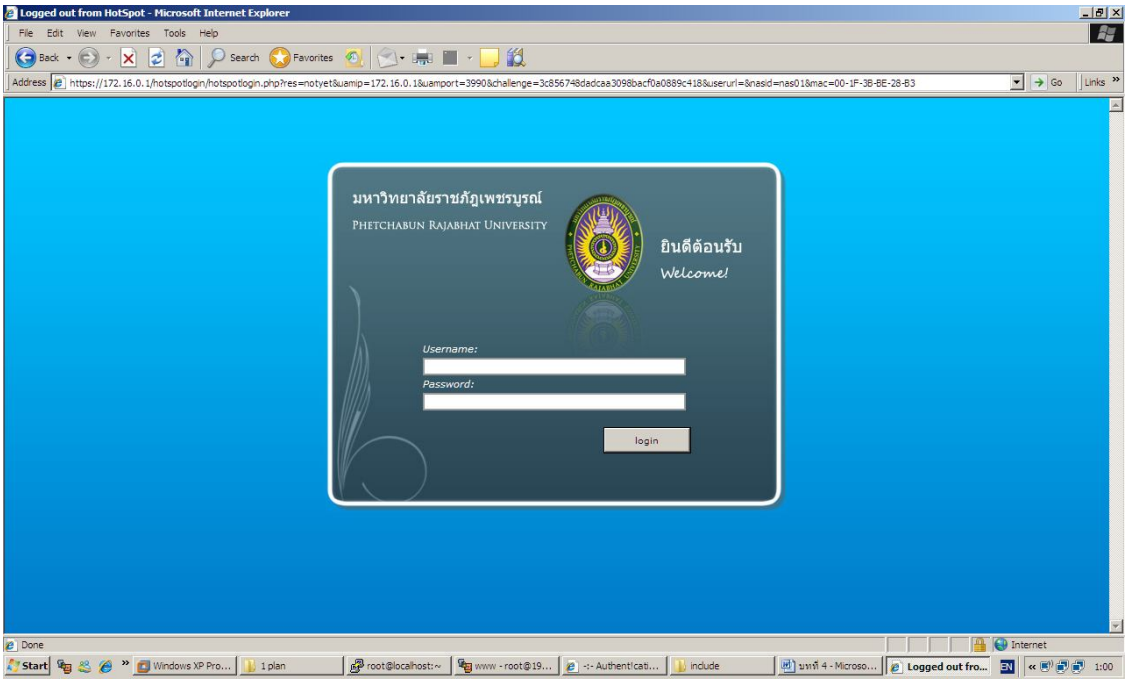
จากการพัฒนาหน้าจอเข้าสู่อินเทอร์เน็ตสำหรับสมาชิกซึ่งระบบถูกใช้โดยสมาชิกสำหรับในการเข้าใช้อินเทอร์เน็ต ซึ่งสามารถแสดงผลดังนี้

4.4.1 หน้าจอแรกของการเข้าใช้งานอินเทอร์เน็ตสำหรับสมาชิกเป็นหน้าจอแสดงหน้าจอแรกของการเข้าใช้งานอินเทอร์เน็ตสำหรับสมาชิก โดยในหน้านี้จะมีบทความที่กล่าวถึงข้อตกลงในการเข้าใช้งานอินเทอร์เน็ต ดังภาพประกอบ 4.16



รูปที่ 4.16 แสดงหน้าจอแรกของการเข้าใช้งานอินเทอร์เน็ตสำหรับสมาชิก

4.4.2 หน้าจอเข้าสู่ระบบอินเทอร์เน็ตสำหรับสมาชิกเป็นหน้าจอแสดงหน้าจอเข้าสู่ระบบอินเทอร์เน็ตสำหรับสมาชิกโดยกรอกชื่อผู้ใช้และรหัสผ่านที่ได้จากผู้ดูแลระบบก็เข้าใช้ระบบอินเทอร์เน็ตได้



รูปที่ 4.17 แสดงหน้าจอตรวจสอบรายชื่อเข้าสู่ระบบอินเทอร์เน็ตสำหรับสมาชิก

บทที่ 5
สรุปผล อภิปรายผลและข้อเสนอแนะ

ในบทนี้จะกล่าวถึงบทสรุปผลของงานการวิจัยฉบับนี้ ปัญหาและอุปสรรคที่พบในระหว่างการทำงาน และข้อเสนอแนะเพื่อเป็นแนวทางในการพัฒนาปรับปรุงระบบงานให้มีความสมบูรณ์ยิ่งขึ้น

5.1 วัตถุประสงค์ของการวิจัย

5.1.1 พัฒนาระบบการบันทึกการจราจรบนระบบเครือข่ายคอมพิวเตอร์(Log File) ตาม พรบ. ว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์2550

5.1.2 พัฒนาระบบระบบพิสูจน์ตัวตน

5.1.3 พัฒนาระบบจัดการฐานข้อมูลผู้ใช้ระบบอินเทอร์เนต

5.1.4 พัฒนาระบบอินเทอร์เนตเกตเวย์สำหรับมหาวิทยาลัย

5.1.5 พัฒนาระบบอินเทอร์เฟสอินเทอร์เนตเกตเวย์กับไวไฟ-ลีสไลน์

5.1.6 ทำการเผยแพร่องค์ความรู้แก่หน่วยงานที่เป็นภาคี ได้แก่ มหาวิทยาลัยราชภัฏ มหาวิทยาลัยของรัฐและเอกชน และผู้สนใจทั่วไป

5.2 สรุปผล

งานการวิจัยฉบับนี้มีจุดประสงค์คือต้องการสร้างระบบมาเพื่อเก็บข้อมูลผู้ใช้งานในอินเทอร์เนตตามข้อบังคับของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในส่วนของผู้ให้บริการอินเทอร์เน็ตในการวิจัยนี้จึงได้ออกแบบสอบถามการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ตามข้อบังคับของว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2550 กับทางผู้ให้บริการอินเทอร์เนต เพื่อทำการออกแบบระบบที่รองรับพระราชบัญญัติดังกล่าวให้มากที่สุด จากผลของการสำรวจแบบสอบถามผู้ให้บริการอินเทอร์เนตส่วนใหญ่ยังไม่ได้มีการเตรียมการใด ๆ เพื่อรองรับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ผู้วิจัยได้วิเคราะห์ระบบเพื่อให้สามารถรองรับข้อกำหนดของพระราชบัญญัตินี้โดยมีส่วนการทำงานดังนี้

5.2.1 มีการระบุตัวตนของผู้ใช้งาน โดยมีระบบสำหรับการพิสูจน์ตัวตนของผู้ใช้บริการใช้ระบบสมาชิกสำหรับให้สมาชิกเข้าใช้งานเครือข่ายอินเทอร์เน็ต

5.2.2 มีระบบการจัดการเวลาให้เป็นมาตรฐานที่น่าเชื่อถือและสามารถนำไปอ้างอิงเมื่อเกิดเหตุโดยมีความผิดพลาดไม่เกิน 10 มิลลิวินาที

5.2.3 มีระบบการเก็บรักษาข้อมูลที่ครบถ้วนและเชื่อถือได้เข้ารหัสข้อมูลล็อกไฟล์และจำเป็นต้องมีการสำรองข้อมูลการจราจรข้อมูลล็อกไฟล์ที่เกิดขึ้นด้วย

5.2.4 มีระบบการจัดการสำหรับการค้นคืนข้อมูลการจราจรย้อนหลังเพื่อใช้สำหรับค้นข้อมูลโดยจะมีรายงานจากเจ้าหน้าที่เพื่อทำการระบุใครเป็นผู้กระทำความผิดโดยการออกเป็นรายงานสำหรับเป็นหลักฐานทางกฎหมาย

5.2.5 มีระบบที่รองรับเครือข่ายไร้สายโดยกำหนดให้ระบบที่พัฒนาทั้งหมดสามารถรองรับเครือข่ายไร้สายจากการวิเคราะห์ระบบทั้งหมดสามารถออกแบบเป็น 2 ระบบย่อย เพื่อรองรับทั้งเครือข่ายแบบมีสายและไร้สาย ได้แก่ ระบบฐานข้อมูลสำหรับเก็บข้อมูลผู้ใช้งานอินเทอร์เนต (Member System for Internet) และระบบค้นคืนและระบุผู้ใช้งานในอินเทอร์เนต (Retrieval System) โดยแบ่งการทำงานหรือดำเนินการต่างๆ ออกเป็นส่วนย่อยเพื่อให้ง่ายในการจัดการระบบทั้งหมดการพัฒนาระบบงานดังกล่าวผู้วิจัยได้ใช้ระบบปฏิบัติ FreeBSD

โดยระบบฐานข้อมูลสำหรับเก็บข้อมูลผู้ใช้งานอินเทอร์เนต ผู้วิจัยได้พัฒนาระบบขึ้นโดยใช้ภาษา PHP โปรแกรม FreeRadius และ Chillispot เพื่อใช้ในการพิสูจน์ตัวตนในการเข้าสู่ระบบอินเทอร์เน็ตโดยมีการกำหนดให้ชื่อผู้ใช้ด้วยหมายเลขประจำตัวประชาชนและสำหรับเครือข่ายไร้สายได้มีการลงทะเบียนหมายเลข MAC Address ด้วยสำหรับสู่ระบบอินเทอร์เน็ต และระบบค้นคืนและระบุผู้ใช้งานในอินเทอร์เนต

ผู้วิจัยได้พัฒนาโดยใช้ภาษา PHP และใช้ฐานข้อมูลเดียวกับระบบฐานข้อมูลสำหรับเก็บข้อมูลผู้ใช้งานอินเทอร์เนตนอกจากการพัฒนาระบบในสองส่วนที่ได้กล่าวมาแล้วยังมีส่วนที่เป็นการตั้งค่าระบบ ได้แก่ การเทียบเวลาระหว่างอุปกรณ์คอมพิวเตอร์ (NTP) และการเขียนโปรแกรม Shell Script ในการเก็บข้อมูลล็อกไฟล์โดยเก็บข้อมูลกิจกรรมที่เกิดขึ้นตามที่ต้องการและบันทึกเป็นวันต่อวัน หลังจากที่ได้ทดสอบระบบเก็บข้อมูล พิสูจน์ตัวตน ค้นคืนและระบุผู้ใช้บริการอินเทอร์เนต

ผลปรากฏว่าระบบเก็บข้อมูล พิสูจน์ตัวตน ค้นคืนและระบุผู้ใช้บริการอินเทอร์เนต สามารถทำงานรองรับ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 โดยไม่ได้ส่งผลกระทบทางลบต่อการให้บริการอินเทอร์เน็ตและสามารถค้นคืนและสามารถระบุผู้ใช้งานในอินเทอร์เนตที่เข้าข่ายผิดหรืออาจจะผิดข้อกำหนดตาม พระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ได้อย่างถูกต้อง

5.3 อภิปรายผล

อุปสรรคปัญหาที่พบและแนวทางแก้ปัญหาในการใช้งานระบบเก็บข้อมูล พิสูจน์ตัวตน ค้นคืนและระบุผู้ใช้บริการอินเทอร์เนต เนื่องจากระบบได้มีการทดสอบและใช้งานจริงในอินเทอร์เนต ผู้วิจัยได้พบว่ามีปัญหาและข้อจำกัดของโปรแกรม โดยแบ่งออกเป็น 2 ส่วนคือ อุปสรรคปัญหา และข้อจำกัดของระบบ ดังนี้

ปัญหาความไม่เข้าใจในระบบของผู้แลระบบในอินเทอร์เนต เนื่องจากระบบที่ติดตั้งนั้นเป็นเรื่องใหม่และเป็นสิ่งใหม่ที่เกิดขึ้นภายในอินเทอร์เนตเมื่ออินเทอร์เน็ตใช้การไม่ได้ สิ่งแรกที่ผู้ดูแลระบบคิดคือเกิดขึ้นจากระบบที่ติดตั้งใหม่นี้ แนวทางการแก้ปัญหาคือการให้ความรู้พื้นฐานในการทดสอบการใช้งานอินเทอร์เน็ต โดยสอนการใช้คำสั่ง คำสั่งพื้นฐานในระบบปฏิบัติการ FreeBSD เพื่อตรวจสอบระบบคอมพิวเตอร์เครื่องแม่ข่ายและเครือข่ายและสอนวิธีการตั้งค่า Network Connection ของ Local Area Network และ Wireless Lan โดยตั้งค่าให้รับ IP Address แบบอัตโนมัติ

ปัญหาการใช้งานเครื่องแม่ข่ายของผู้แลระบบในอินเทอร์เนตเนื่องจากระบบปฏิบัติการที่ติดตั้งบนเครื่องแม่ข่ายนั้นเป็นระบบปฏิบัติการ FreeBSD ดังนั้น ผู้ดูแลระบบจะเกิดความไม่เคยชินและผู้ดูแลระบบขาดความรู้ในการใช้งานเครื่องแม่ข่าย แนวทางการแก้ปัญหาคือการให้ความรู้พื้นฐานในระบบปฏิบัติการ FreeBSD เช่น การเปิดปิดเครื่องแม่ข่าย การใช้คำสั่ง Shell Script

5.4 ข้อเสนอแนะ

ข้อจำกัดของระบบในการติดตั้ง ทดสอบ และใช้งานจริงระบบสามารถแบ่งออกเป็นหัวข้อดังนี้

ระบบเก็บข้อมูลพิสูจน์ตัวตน ค้นคืนและระบุผู้ใช้บริการอินเทอร์เนต เป็นระบบที่ได้มีการพัฒนาขึ้นสำหรับผู้ให้บริการอินเทอร์เนตเพื่อรองรับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ในส่วนของอินเทอร์เนต โดยระบบสามารถประยุกต์ให้กับส่วนผู้ให้บริการอื่นได้ ได้แก่ โรงแรม โรงเรียน หอพัก ร้านอาหารที่มีบริการใช้เครือข่ายไร้สายได้การที่จะใช้ระบบนี้ให้สัมฤทธิ์มากที่สุดผู้ดูแลระบบในอินเทอร์เนตควรที่จะมีความรู้ในระบบปฏิบัติการ FreeBSD

การติดตั้งบนเครื่องพีซีธรรมดาสามารถใช้งานได้ระดับหนึ่ง เมื่อใช้ไปนานๆ บางครั้งอาจทำให้เครื่องแฮ้งค์ได้ควรติดตั้งในเครื่องแม่ข่ายServer จึงจะได้ผลดี

แนวทางการพัฒนาระบบเก็บข้อมูล พิสูจน์ตัวตน ค้นคืนและระบุผู้ใช้บริการอินเทอร์เนตต่อนั้น ควรเน้นในเรื่องการจัดทำรายงานและการทำบัญชีผู้ใช้ โดยการทำบัญชีผู้ใช้เช่น การเก็บข้อมูลแต่

ละคนว่ามีการใช้งานแล้วกี่ครั้ง ใช้ทรัพยากรอินเทอร์เน็ตเท่าไหร่ การจำกัดให้กลุ่มผู้ใช้ใช้งานอินเทอร์เน็ตใช้ทรัพยากรได้เท่าไหร่ เป็นต้นงานวิจัยนี้ถือเป็นเครื่องมือตัวหนึ่งที่ช่วยให้ผู้ดูแลระบบในอินเทอร์เนตมีระบบที่รองรับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และช่วยเจ้าหน้าที่หาตัวผู้กระทำความผิดได้อีกทางหนึ่งด้วย

บรรณานุกรม

คมสัน คำบรรลือ. **การศึกษาเพื่อเพิ่มประสิทธิภาพระบบเครือข่ายไร้สาย สาขาวิชาระบบสารสนเทศ.** ตาก : มหาวิทยาลัยเทคโนโลยีราชมงคลล้านา, 2551.

ธวัชชัย ชูเหล็ก. **การออกแบบการประกอบระบบปฏิบัติการลินุกซ์.** กรุงเทพมหานคร : มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ , 2550.

ธารทิพย์ ตากเทิดเกียรติ์ . **การพัฒนาระบบพิสูจน์ทราบตัวตนแบบไดนามิกโมดูลผ่าน HyperText transfer protocol.** กรุงเทพมหานคร : มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ , 2549.

ธีระ โชคพระสมบัติ . **การพัฒนาระบบปฏิบัติการแม่ข่ายลีนุกซ์สำหรับระบบบทเรียนบรรยายอิเลคทรอนิกส์.** กรุงเทพมหานคร : มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง , 2550.

นริสสรา ศรีมูลชัย. **การพัฒนาซอฟต์แวร์สำหรับบริหารสิทธิ์การเข้าใช้งานบนระบบเครือข่ายแบบไร้สาย.** กรุงเทพมหานคร : มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ , 2549.

นฤชัย ศรีแสงอยู่. **การพัฒนาโปรแกรมตรวจสอบความปลอดภัยพื้นฐานสำหรับระบบปฏิบัติการลีนุกซ์เรดแฮต.** กรุงเทพมหานคร : จุฬาลงกรณ์มหาวิทยาลัย , 2547

ปรัชญา พันธุ์มี . **การพิสูจน์ตัวตนในระบบเว็บเซอร์วิสด้วยระบบเคอร์เบอรอส.** กรุงเทพมหานคร : มหาวิทยาลัยธรรมศาสตร์ , 2548.

ไพฑูรย์ แย้มเทศ **การศึกษาหาค่าประสิทธิภาพของพีซีเราเตอร์บนระบบปฏิบัติการแบบเปิด.** กรุงเทพมหานคร : มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ , 2548.

ยุทธนา ไชยสัตย์. **การพัฒนาระบบโปรโตคอลพิสูจน์ตัวตนแบบไม่ประสานเวลา สำหรับโปรโตคอล Neuman Stubblebine.** กรุงเทพมหานคร : มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ , 2548.

ศาลทัส พัดฟูทรัพย์ศ์. **การทดสอบความปลอดภัยของระบบเครือข่ายไร้สาย.** กรุงเทพมหานคร : มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ , 2549

สถาบันมาตรวิทยาแห่งชาติ. **เวลามาตรฐาน** : (online) Aviable URL: http://www.nimt.or.th/nimt/service/index.php?menuName=time , 2553.

สัลยุทธ์ สว่างวรรณ. **เครือข่ายคอมพิวเตอร์ COMPUTER NETWORKS.** พิมพลักษณ์ กรุงเทพมหานคร : เพียร์สัน เอ็ดดูเคชั่น อินโดไชน่า , 2547.

สุวัฒน์ บันลือ. **รูปแบบที่เหมาะสมของเครือข่ายคอมพิวเตอร์ไร้สาย สำหรับสถาบันราชภัฏอุบลราชธานี**. อุบลราชธานี: สถาบันราชภัฏอุบลราชธานี , 2548.

โอภาส เอี่ยมสิริวงศ์. **เครือข่ายคอมพิวเตอร์และการสื่อสาร.** พิมพลักษณ์ กรุงเทพมหานคร : บริษัท ซีเอ็ดยูเคชั่น จำกัด , 2552.

“ The FreeBSD Project ” (online) Aviable URL: (http://www.FreeBSD.org) , public by The FreeBSD Project ,2010

ภาคผนวก

คู่มือการติดตั้งระบบ

การติดตั้ง NTP สำหรับเทียบเวลาตามมาตรฐานสากล

Network Time Protocol

cd /usr/ports/net/ntp

make install

 # ee /etc/ntp.conf

server clock.nectec.or.th prefer

server clock2.nectec.or.th

server clock.thaicert.nectec.or.th

 # ee /etc/rc.conf

(เพิ่มคำสั่งต่อไปนี้)

ntpdate_enable="YES"

#ใส่ไว้ใน crontab

ee /etc/crontab

0 */6 * * * /usr/sbin/ntpdate -u clock.nectec.or.th

อัพเดททุก 6 ชม

Compile Kernel

cd /usr/src/sys/i386/conf

cp GENERIC PCRU

ee PCRU

#ident GENERIC แก้ไขเป็น

ident PCRU

#เพิ่ม options ต่างๆ

options IPFIREWALL

options IPFIREWALL_FORWARD

options IPFIREWALL_DEFAULT_TO_ACCEPT

options IPFIREWALL_VERBOSE

#options IPFIREWALL_VERBOSE_LIMIT=5000

options IPFIREWALL_VERBOSE_LIMIT=0

```
options         DUMMYNET
#options        HZ=1000
options         IPDIVERT
options             QUOTA
options             DEVICE_POLLING
options             ALTQ
options             ALTQ_CBQ
options             ALTQ_RED
options             ALTQ_RIO
options             ALTQ_HFSC
options             ALTQ_PRIQ
options             ALTQ_NOPCC
device              pf
device              pflog
device              pfsync
# กด save
config PCRU
cd ../compile/PCRU/
make depend;make;make install
#เสร็จแล้วให้ Nat และ Firewall
ee /etc/rc.conf
#พิมพ์เพิ่มเข้าไป
firewall_enable="YES"
firewall_type="OPEN"
firewall_quite="YES"
natd_enable="YES"
# sis0 คือการ์ดใบนอก
natd_interface="sis0"
natd_flags="-s -u -m"
#เสร็จแล้วให้ทำการ  reboot
```

การติดตั้ง FAMP64 และลง apache22ให้รองรับ php5+ssl

FAMP62

cp /home/admin/FAMP62.tar.gz /usr/ports/distfiles/

cd /usr/ports/distfiles/

tar xvfz /home/admin/FAMP62.tar.gz

ลง apache22

cd /usr/ports/www/apache22

make all;make install

#ไม่ต้องเลือกอะไร

ee /etc/rc.conf

#เพิ่ม

apache22_enable="YES"

apache22_flags="-DSSL"

#แก้ไขให้รองรับ php และ ssl

ee /usr/local/etc/apache22/httpd.conf

#หาคำว่า directoryindex

เพิ่ม index.php

ค้นหาคำว่า AddType application/x-compress .Z

เพิ่มต่อท้าย

AddDefaultCharset tis-620

AddType application/x-httpd-php .php

AddType application/x-httpd-php-source .phps

AddType application/x-httpd-php .html

หาคำว่า

Secure (SSL/TLS) connections

Include etc/apache22/extra/httpd-ssl.conf << เอา # ออก

#cd /usr/local/etc/apache22

/usr/bin/openssl genrsa -out /usr/local/etc/apache22/server.key 1024

/usr/bin/openssl req -new -days 365 -key /usr/local/etc/apache22/server.key -out

/usr/local/etc/apache22/server.csr

#

/usr/bin/openssl x509 -in /usr/local/etc/apache22/server.csr -out

/usr/local/etc/apache22/server.crt -req -signkey /usr/local/etc/apache22/server.key -days 365

chmod 400 server.*

ee /etc/rc.conf

apache22_flags="-DSSL"

start apache22

/usr/local/etc/rc.d/apache22 restart

Install php5

cd /usr/ports/lang/php5

make install

เลือก APACHE

ok

cd /usr/ports/lang/php5-extensions/

make install

เลือก

[X] CALENDAR

[X] FTP

[X] GD

[X] GETTEXT

[X] MBSTRING

[X] MYSQL

[X] OPENSSL

[X] SOCKETS

[X] ZLIB

ok

cp /usr/local/etc/php.ini-dist /usr/local/etc/php.ini

ee /usr/local/etc/php.ini

ค้นหาคำว่า register_globals = Off

เปลี่ยนจาก off เป็น on

หาคำว่า default_charset

เอา ; ออก แล้วเปลี่ยนจาก iso-8859-1 เป็น tis-620

ค้นหา

;mssql.charset = "iso-8859-1"

mssql.charset = "tis-620"

max_execution_time = 100 ; Maximum execution time of each script, in seconds

max_input_time = 100 ; Maximum amount of time each script may spend parsing request data

memory_limit = 100M ; Maximum amount of memory a script may consume (16MB)

save

Install pear-DB

#pearZ_DB

cd /usr/ports/databases/pear-DB

make install

Install ZendOptimizer

#ZendOptimizer

cd /usr/ports/

cd /usr/ports/devel/ZendOptimizer/

make install clean

ee /usr/local/etc/php.ini

[Zend]

zend_optimizer.optimization_level=15

zend_extension_manager.optimizer="/usr/local/lib/php/20060613/Optimizer"

zend_extension_manager.optimizer_ts="/usr/local/lib/php/20060613/Optimizer_TS"

zend_extension="/usr/local/lib/php/20060613/ZendExtensionManager.so"

zend_extension_ts="/usr/local/lib/php/20060613/ZendExtensionManager_TS.so"

mysql -u user_name -p password -h host_name_or_address data_base_name <

/complete_path_and_name_file

if you transfer the file to the server

mysql -u user_name -p password data_base_name < /complete_path_and_name_file

Install Mysql

cd /usr/ports/databases/mysql50-server/

make deinstall clean

cd /usr/ports/databases/mysql50-client/

make deinstall clean

cd /usr/ports/databases/mysql50-scripts/

make deinstall clean

rehash

cd /usr/ports/databases/mysql50-server/

make WITH_CHARSET=tis620 WITH_XCHARSET=all WITH_COLLATION=tis620_thai_ci WITH_OPENSSL=yes BUILD_OPTIMIZED=yes WITH_ARCHIVE=yes WITH_FEDERATED=yes WITH_NDB=yes install clean

ทำให้รองรับภาษาไทย

cp /usr/local/share/mysql/my-large.cnf /etc/my.cnf

chown root:sys /etc/my.cnf

chmod 644 /etc/my.cnf

rehash

ee /etc/my.cnf

หลังจากนั้น เราจะไปแก้ไขไฟล์ /etc/my.cnf โดยเพิ่มเนื้อหาในส่วนต่าง ๆ ดังนี้ ต่อท้าย

[client]

default-character-set=tis620

[mysqld]

default-character-set = tis620

character-set-server = tis620

collation-server = tis620_thai_ci

init_connect = 'set collation_connection = tis620_thai_ci'

init_connect = 'set names tis620'

ee /etc/rc.conf

#ใส่

mysql_enable="YES"

#reboot

#สร้าง user เข้าฐานข้อมูล

mysqladmin -u root password 123456

mysqladmin -u root password admin#$mysql

mysql -u root -p123456

mysql -u root -p123456 radius < /home/admin/radius-all.sql

ในระบบ FreeBSD ฐานข้อมูลของ MySql จะอยู่ที่ /var/db/mysql

Install Freeradius

cd /usr/ports/net/freeradius/

make install

#เลือก [X] MYSQL

Install Chillispot

cd /usr/ports/net-mgmt/chillispot/

make install

#เลือก [X] MATURE [X] FREE

mysql -u root -p

Enter password:

#ผาเมือง admin123456

create database radius;

grant all on radius.* to admin@localhost identified by 'adminmysql';

quit;

```
mysql -u root -p radius </usr/local/share/doc/freeradius/examples/mysql.sql
Enter password:
cd /usr/local/etc/raddb/
cp acct_users.sample acct_users
cp clients.conf.sample clients.conf
cp dictionary.sample dictionary
cp eap.conf.sample eap.conf
cp hints.sample hints
cp huntgroups.sample huntgroups
cp preproxy_users.sample preproxy_users
cp proxy.conf.sample proxy.conf
cp radiusd.conf.sample radiusd.conf
cp snmp.conf.sample snmp.conf
cp sql.conf.sample sql.conf
cp users.sample users
ee /usr/local/etc/raddb/radiusd.conf
proxy_requests  = yes to no
Authorize {
# sql to
 sql
Authenticate {
  unix to
# unix
preacct {
        files to
#       files
accounting {
# sql to
  sql
session {
```

```
  radutmp to
# radutmp
# sql to
  sql
mkdir /var/log/radacct
touch /var/log/radius.log
touch /var/log/radutmp
touch /var/log/radwtmp
chmod 700 /var/log/radacct
chmod 644 /var/log/radius.log
chmod 600 /var/log/radutmp
chmod 644 /var/log/radwtmp
adduser
Username: radius
Full name: freeradius
Uid (Leave empty for default):
Login group [radius]:
Login group is radius. Invite radius into other groups? []:
Login class [default]:
Shell (sh csh tcsh nologin) [sh]:
Home directory [/home/radius]:
Use password-based authentication? [yes]: y
Use an empty password? (yes/no) [no]: n
Use a random password? (yes/no) [no]: n
Enter password:
Enter password again:
Lock out the account after creation? [no]: n
Username   : radius
Password   : *****
Full Name  : freeradius
```

```
Uid        : 1002
Class      :
Groups     : radius
Home       : /home/radius
Shell      : /bin/sh
Locked     : no
OK? (yes/no): y
adduser: INFO: Successfully added (radius) to the user database.
Add another user? (yes/no): n
Goodbye!
chown radiusd:radiusd /var/log/radacct
chown radiusd:radiusd /var/log/radius.log
chown radiusd:radiusd /var/log/radutmp
chown radiusd:radiusd /var/log/radwtmp
ee /usr/local/etc/raddb/sql.conf
# Connect info
        server = "localhost"
        login = "admin"
        password = "pbru8312"

        # Database table configuration
        radius_db = "radius"
#sql_user_name = "%{Stripped-User-Name:-%{User-Name:-DEFAULT}}"
sql_user_name = "%{Stripped-User-Name:-%{User-Name:-DEFAULT}}"
sql_user_name = "%{User-Name}"
#sql_user_name = "%{User-Name}"
mysql -u root -p
password:
use radius;
show tables;
```

```
insert into radcheck (Username, Attribute, Value) VALUES ('fry', 'Password', '1234');
insert into usergroup (UserName, GroupName, Priority) VALUES ('fry', 'dynamic', 1);
insert into radgroupcheck (GroupName, Attribute, Value) VALUES ('dynamic', 'Auth-Type',
'Local');
insert into radreply (UserName, Attribute, Value) VALUES ('fry', 'Class', '0702345678');
insert into radgroupreply (GroupName, Attribute, Value) VALUES ('dynamic', 'Session-Timeout',
'3600');
insert into radgroupreply (GroupName, Attribute, Value) VALUES ('dynamic', 'Idle-Timeout',
'600');
insert into radgroupreply (GroupName, Attribute, Value) VALUES ('dynamic', 'Acct-Interim-
Interval', '60');
insert into radgroupreply (GroupName, Attribute, Value) VALUES ('dynamic', 'WISPr-
Redirection-URL', 'http://www.geeklan.co.uk');
insert into radgroupreply (GroupName, Attribute, Value) VALUES ('dynamic', 'WISPr-
Bandwidth-Max-Up', '128000');
insert into radgroupreply (GroupName, Attribute, Value) VALUES ('dynamic', 'WISPr-
Bandwidth-Max-Down', '512000');
select * from radgroupreply;
quit;
cp /usr/local/share/chillispot/hotspotlogin.cgi /usr/local/www/apache22/cgi-bin/
chmod 755 /usr/local/www/apache22/cgi-bin/hotspotlogin.cgi
cp /usr/local/share/chillispot/chilli.conf.sample /etc/chilli.conf
cp /usr/local/share/chillispot/dictionary.chillispot /usr/local/etc/raddb/
cp /usr/local/share/chillispot/freeradius.users  /usr/local/etc/raddb/
cp /usr/local/share/chillispot/pf.conf.sample /etc/pf.conf
ee /usr/local/www/apache22/cgi-bin/hotspotlogin.cgi
#$uamsecret = password to
$uamsecret = password
#$userpassword=1;
$userpassword=1;
```

ee /usr/local/etc/raddb/dictionary

#เพิ่ม

$INCLUDE /usr/local/etc/raddb/dictionary.chillispot

ee /etc/chilli.conf

net 192.168.182.0/24

dns1 203.113.118.2

radiussecret testing123

dhcpif vr0 #out

uamserver https://192.168.182.1/cgi-bin/hotspotlogin.cgi

uamhomepage http://192.168.182.1/welcome.html

uamsecret ht2eb8ej6s4et3rg1ulp

uamlisten 192.168.182.1

cp /home/admin/welcome.html /usr/local/www/apache22/data/

/usr/local/sbin/radiusd -X

/usr/local/bin/radtest fry 1234 localhost 1812 testing123

รัน chillispot

#ใส่ /etc/rc.local

/usr/local/sbin/chilli &

/usr/local/sbin/radiusd &

ee /etc/rc.conf

pf_enable="YES"

pf_rules="/etc/pf.conf"

pf_flags=""

pflog_enable="YES"

pflog_logfile="/var/log/pflog"

pflog_flags=""

#reboot

Install squid

วิธีการทำ chillispot + squid (transparent)

cd /usr/ports/www/squid

make install

เมื่อลงเสร็จแล้วเข้าไปแก้ไขไฟล์ squid.conf ที่อยู่ใน /usr/local/etc/squid/ ดังนี้

ee /usr/local/etc/squid/squid.conf

แล้วแก้ไขบรรทัดต่อไปนี้และเอาเครื่องหมาย # ออก

http_port 8080

icp_port 3130

cache_dir ufs /usr/local/squid/cache 1500 16 256

cache_access_log /usr/local/squid/logs/access.log

cache_log /usr/local/squid/logs/cache.log

cache_store_log none

แล้วค้นหาคำว่า acl our_networks src จะอยู่ประมาณบรรทัดที่ 1888แล้วแก้ไขตามต่อไปนี้ จะเป็นการกำหนดค่า ip ที่จะสามารถเข้ามาใช้ proxy ได้

ในที่นี้ผมกำหนดให้เฉพาะ ip ที่ chillispot แจกเท่านั้นที่เข้ามาใช้ได้

acl our_networks src 192.168.182.0/24

http_access allow our_networks

แล้วหาคำว่า httpd_accel_port 80 แล้วเพิ่มบรรทัดเหล่านี้ลงไป จะอยู่ประมาณบรรทัดที่ 2234 เป็นการทำ transparent

httpd_accel_port 80

httpd_accel_host virtual

httpd_accel_with_proxy on

httpd_accel_uses_host_header on

เสร็จแล้วก็ทำการเซฟไฟล์

แล้วสั่งให้ squid สร้าง cache ขึ้นมาโดยใช้คำสั่งต่อไปนี้

cd /usr/local/squid/logs

touch access.log

touch store.log

touch cache.log

chmod 777 *.log

cd /usr/local/squid/

mkdir cache

chmod 777 cache

cd /usr/local/sbin

./squid -z

แล้วสั่งให้ squid ทำงานโดยใช้คำสั่งต่อไปนี้

/usr/local/sbin/RunCache &

เสร็จแล้วเข้าไปเพิ่มคำสั่งที่ไฟล์ rc.local ดังต่อไปนี้

ee /etc/rc.local

แล้วเพิ่มคำสั่งดังนี้

/usr/local/sbin/RunCache &

ipfw add 1700 fwd 192.168.182.1 tcp from any to 192.168.182.0/24 80

ipfw add 1800 fwd 192.168.182.1,8080 tcp from 192.168.182.0/24 to any 80

ใส่พอกซี่

ipfw add 1900 deny tcp from any to any 8080

ipfw add pass tcp from any to any 3990 via setup

reboot

ดูข้อมูล tail -f /usr/local/squid/logs/access.log

ติดตั้ง syslog_ng บนเครื่อง server สำหรับส่ง Log

ติดตั้ง syslog_ng **บนเครื่อง server** เมื่อติดตั้ง FreeBSD จะมี syslog เราจะใช้งานต้องใช้ syslog-ng ซึ่งสามารถ customize log file name เป็น ชื่อ อื่นได้

cd /usr/ports/sysutils/syslog-ng

make & make install

เมื่อติดตั้งเรียบร้อยแล้ว แก้ไขที่ /etc/rc.conf เพื่อให้เรียกใช้ syslog-ng แทนโดยเพิ่มบรรทัดนี้

syslog_ng_enable="YES"

และต้องยกเลิกตัว syslog เดิม โดยเพิ่มบรรทัดนี้ใน /etc/rc.conf

syslogd_enable="NO"

หลังจากนั้น kill process syslogd เดิม โดยใช้คำสั่งนี้

kill `cat /var/run/syslog.pid`

ทำการ copy /usr/local/etc/syslog-ng/syslog-ng.conf.sample ให้ /usr/local/etc/syslog-ng/syslog-ng.conf

cp /usr/local/etc/syslog-ng/syslog-ng.conf.sample /usr/local/etc/syslog-ng/syslog-ng.conf

ทำการ start syslog-ng โดยรันคำสั่งนี้

usr/local/etc/rc.d/syslog-ng.sh start

จากนั้นให้เข้าไปเพิ่มเติมใน syslog_ng.conf

```
#pico /usr/local/etc/syslog_ng/syslog_ng.conf
# This sample configuration file is essentially equilivent to the stock
# FreeBSD /etc/syslog.conf file.
# options
options {
        sync (0);
        time_reopen (10);
        log_fifo_size (1000);
        long_hostnames (off);
        use_dns (no);
        use_fqdn (no);
        create_dirs (yes);
        keep_hostname (yes);
};
# sources
source src { unix-dgram("/var/run/log");
            internal();
            file("/dev/klog");
            };
# destinations
destination messages { file("/var/log/messages"); };
destination security { file("/var/log/security"); };
destination authlog { file("/var/log/auth.log"); };
destination maillog { file("/var/log/maillog"); };
destination lpd-errs { file("/var/log/lpd-errs"); };
destination xferlog { file("/var/log/xferlog"); };
```

```
destination cron { file("/var/log/cron"); };
destination debuglog { file("/var/log/debug.log"); };
destination consolelog { file("/var/log/console.log"); };
destination all { file("/var/log/all.log"); };
destination newscrit { file("/var/log/news/news.crit"); };
destination newserr { file("/var/log/news/news.err"); };
destination newsnotice { file("/var/log/news/news.notice"); };
destination slip { file("/var/log/slip.log"); };
destination ppp { file("/var/log/ppp.log"); };
destination console { file("/dev/console"); };
destination allusers { usertty("*"); };
#destination loghost { udp("loghost" port(514)); };
#สร้าง destination เพื่อติดต่อ กับ logserver (หมายถึงการใส่หมายเลข  IP ของเครื่อง Centralize
Log #server  ) โดยเพิ่มบันทัดตามด้านล่าง
destination loghost { tcp("203.172.175.4" port(514)); };
# log facility filters
filter f_auth { facility(auth); };
filter f_authpriv { facility(authpriv); };
filter f_not_authpriv { not facility(authpriv); };
filter f_console { facility(console); };
filter f_cron { facility(cron); };
filter f_daemon { facility(daemon); };
filter f_ftp { facility(ftp); };
filter f_kern { facility(kern); };
filter f_lpr { facility(lpr); };
filter f_mail { facility(mail); };
filter f_news { facility(news); };
filter f_security { facility(security); };
filter f_user { facility(user); };
filter f_uucp { facility(uucp); };
```

```
filter f_local0 { facility(local0); };
filter f_local1 { facility(local1); };
filter f_local2 { facility(local2); };
filter f_local3 { facility(local3); };
filter f_local4 { facility(local4); };
filter f_local5 { facility(local5); };
filter f_local6 { facility(local6); };
filter f_local7 { facility(local7); };
# log level filters
filter f_emerg { level(emerg); };
filter f_alert { level(alert..emerg); };
filter f_crit { level(crit..emerg); };
filter f_err { level(err..emerg); };
filter f_warning { level(warning..emerg); };
filter f_notice { level(notice..emerg); };
filter f_info { level(info..emerg); };
filter f_debug { level(debug..emerg); };
filter f_is_debug { level(debug); };
# program filters
filter f_ppp { program("ppp"); };
filter f_slip { program("startslip"); };
# *.err;kern.warning;auth.notice;mail.crit              /dev/console
log { source(src); filter(f_err); destination(console); };
log { source(src); filter(f_kern); filter(f_warning); destination(console); };
log { source(src); filter(f_auth); filter(f_notice); destination(console); };
log { source(src); filter(f_mail); filter(f_crit); destination(console); };
# *.notice;authpriv.none;kern.debug;lpr.info;mail.crit;news.err       /var/log/messages
log { source(src); filter(f_notice); filter(f_not_authpriv); destination(messages); };
log { source(src); filter(f_kern); filter(f_debug); destination(messages); };
log { source(src); filter(f_lpr); filter(f_info); destination(messages); };
```

```
log { source(src); filter(f_mail); filter(f_crit); destination(messages); };
log { source(src); filter(f_news); filter(f_err); destination(messages); };
# security.*                                            /var/log/security
log { source(src); filter(f_security); destination(security); };
# auth.info;authpriv.info                               /var/log/auth.log
log { source(src); filter(f_auth); filter(f_info); destination(authlog); };
log { source(src); filter(f_authpriv); filter(f_info); destination(authlog); };
# mail.info                                             /var/log/maillog
log { source(src); filter(f_mail); filter(f_info); destination(maillog); };
# lpr.info                                              /var/log/lpd-errs
log { source(src); filter(f_lpr); filter(f_info); destination(lpd-errs); };
# ftp.info                                              /var/log/xferlog
log { source(src); filter(f_ftp); filter(f_info); destination(xferlog); };
# cron.*                                                /var/log/cron
log { source(src); filter(f_cron); destination(cron); };
# *.=debug                                              /var/log/debug.log
log { source(src); filter(f_is_debug); destination(debuglog); };
# *.emerg                                               *
log { source(src); filter(f_emerg); destination(allusers); };
# uncomment this to log all writes to /dev/console to /var/log/console.log
# console.info                                          /var/log/console.log
#log { source(src); filter(f_console); filter(f_info); destination(consolelog); };
# uncomment this to enable logging of all log messages to /var/log/all.log
# touch /var/log/all.log and chmod it to mode 600 before it will work
# *.*                                                   /var/log/all.log
#log { source(src); destination(all); };
# uncomment this to enable logging to a remote loghost named loghost
# *.*                                                   @loghost
log { source(src); destination(loghost); };
# uncomment these if you're running inn
```

```
# news.crit                                                    /var/log/news/news.crit
# news.err                                                     /var/log/news/news.err
# news.notice                                                  /var/log/news/news.notice
#log { source(src); filter(f_news); filter(f_crit); destination(newscrit); };
#log { source(src); filter(f_news); filter(f_err); destination(newserr); };
#log { source(src); filter(f_news); filter(f_notice); destination(newsnotice); };
# !startslip
# *.*                                                          /var/log/slip.log
log { source(src); filter(f_slip); destination(slip); };
# !ppp
# *.*                                                          /var/log/ppp.log
log { source(src); filter(f_ppp); destination(ppp); };
```

#ป้อนเพิ่มในส่วนท้ายสุดของไฟล์ ในกรณีที่เซิร์ฟเวอร์นี้เป็น PROXY Server

```
# Squid server.
filter f_squid { program("squid") and facility(user); };
log { source(src); filter(f_squid); destination(loghost); };
```

#หมายถึง ส่งข้อมูลของsquidตามuserที่ใช้งานในเครื่องลูก ไปยัง Centralize Log server (ตามIPใน#loghost)

เพิ่มคำสั่งให้เซิร์ฟเวอร์ตัวลูกส่งข้อมูล File access.log ไปให้ Centralize Log server โดยอัตโนมัติหลังจาก Reboot เครื่อง ทำโดย

#pico /etc/rc.local

เพิ่มบรรทัดใหม่ตามด้านล่างเพื่อให้ squid ส่ง log ไปให้ Centralize Log server

```
tail -F /var/log/access.log | logger -t squid -p user.info &
```

#reboot

คำสั่งส่งข้อมูลต่างๆไปยัง Centralize Log server

```
# Log mail server from pop3 service.
filter f_pop3 { match("pop3"); };
log { source(src); filter(f_pop3); destination(loghost); };
# Log mail server from imap service.
filter f_imap { match("imap|courier"); };
```

```
log { source(src); filter(f_imap); destination(loghost); };
# Log mail server use smtp or sendmail service.
filter f_smtp { match("sendmail|smtp"); };
log { source(src); filter(f_smtp); destination(loghost); };
# Log mail server use postfix service.
filter f_postfix { program("^postfix/"); };
log { source(src); filter(f_postfix); destination(loghost); };
# Log IM used iptable check MSN,ICQ,... service.
filter f_im1 { level(warn..emerg); };
filter f_im2 { program("iptables"); };
log { source(src); filter(f_im1); filter(f_im2); destination(loghost); };
# Log dhcp server.
filter f_dhcp { program("dhcpd") and facility(daemon); };
log { source(src); filter(f_dhcp); destination(loghost); };
# Log ssh server.
filter f_ssh  { program("sshd") and facility(auth, authpriv); };
log { source(src); filter(f_ssh); destination(loghost); };
# Log ftp server.
filter f_ftp { program("vsftpd"); };
log { source(src); filter(f_ftp); destination(loghost); };
# Log apache (httpd) web server.
filter f_www { program("logger"); };
filter f_www1 { program("apache"); };
log { source(src); filter(f_www); filter(f_www1); destination(loghost); };
# Log Samba File server.
filter f_samba  { level(info..emerg) and program("smbd"); };
log { source(src); filter(f_samba); destination(loghost); };
# Log ldap server.
filter f_ldap { program("slapd"); };
log { source(src); filter(f_ldap); destination(loghost); flags(final); };
```

```
# Log radius server.
filter f_radius { program("radiusd"); };
log { source(src); filter(f_radius); destination(loghost); };
filter f_router { facility(local2); };
log { source(src); filter(f_router); destination(loghost); };
filter f_switch { facility(local3); };
log { source(src); filter(f_switch); destination(loghost); };
filter f_firewall { facility(local4); };
log { source(src); filter(f_firewall); destination(loghost); };
filter f_vpnbox { facility(local5); };
log { source(src); filter(f_vpnbox); destination(loghost); };
filter f_wifi { facility(local7); };
log { source(src); filter(f_wifi); destination(loghost); };
```

ในกรณีที่ สั่งให้ ส่ง log ไปยัง logserver (freebsd)

#nano /etc/syslog-ng/syslog-ng.conf

พิมพ์ต่อท้ายไฟล์

```
destination loghost { tcp("203.113.118.14" port(514)); };
filter f_squid { program("squid") and facility(user); };
  log { source(s_sys); filter(f_squid); destination(loghost); };
filter f_mmmmm    { level(info..emerg) and
                    not (facility(mail)
                    or facility(authpriv)
                    or facility(cron))
                    and match("chilli.c");
};
log { source(s_sys); filter(f_mmmmm); destination(loghost); };
```

จากนั้นก็เซฟแล้วออกจากโปรแกรม Editer

Restart syslog-ng

#service syslog-ng restart

สั่งให้ เริ่มส่ง log ทุกครั้งที่เปิดเครื่อง

#chkconfig tail -F /var/log/squid/access.log | logger -t squid -p user.info &

#chkconfig tail -F /var/log/squid/access.log | logger -t squid -p user.info &

การติดตั้ง syslog_ng
บนเครื่อง Centralized log Server

เป็นการติดตั้งเพื่อใช้สำหรับเป็น Centralized Log

cd /usr/ports/sysutils/syslog-ng

make & make install

เมื่อติดตั้งเรียบร้อยแล้ว แก้ไขที่ /etc/rc.conf เพื่อให้เรียกใช้ syslog-ng แทน

โดยเพิ่มบรรทัดนี้

syslog_ng_enable="YES"

และต้องการยกเลิกตัว syslog เดิม โดยเพิ่มบรรทัดนี้ใน /etc/rc.conf

syslogd_enable="NO"

หลังจากนั้น kill process syslogd เดิม โดยใช้คำสั่งนี้

kill `cat /var/run/syslog.pid`

ทำการ copy /usr/local/etc/syslog-ng/syslog-ng.conf.sample ให้ /usr/local/etc/syslog-ng/syslog-ng.conf

cp /usr/local/etc/syslog-ng/syslog-ng.conf.sample /usr/local/etc/syslog-ng/syslog-ng.conf

ทำการ start syslog-ng โดยรันคำสั่งนี้

usr/local/etc/rc.d/syslog-ng.sh start

#pico /usr/local/etc/syslog_ng/syslog_ng.conf

This sample configuration file is essentially equilivent to the stock

FreeBSD /etc/syslog.conf file.

options

options {

sync (0);

time_reopen (10);

```
        log_fifo_size (1000);
        long_hostnames (off);
        use_dns (no);
        use_fqdn (no);
        create_dirs (yes);
        keep_hostname (yes);
};
# sources
source src { unix-dgram("/var/run/log");
            internal();
            file("/dev/klog");
            };
#สร้างSource เพื่อรอรับข้อมูลจากเครื่องลูก
# Source from remote client
source s_client {
      tcp(ip(0.0.0.0) port(514) keep-alive(yes) max-connections(300));
      udp(ip(0.0.0.0) port(514));
      };
# destinations
destination messages { file("/var/log/messages"); };
destination security { file("/var/log/security"); };
destination authlog { file("/var/log/auth.log"); };
destination maillog { file("/var/log/maillog"); };
destination lpd-errs { file("/var/log/lpd-errs"); };
destination xferlog { file("/var/log/xferlog"); };
destination cron { file("/var/log/cron"); };
destination debuglog { file("/var/log/debug.log"); };
destination consolelog { file("/var/log/console.log"); };
destination all { file("/var/log/all.log"); };
destination newscrit { file("/var/log/news/news.crit"); };
```

```
destination newserr { file("/var/log/news/news.err"); };
destination newsnotice { file("/var/log/news/news.notice"); };
destination slip { file("/var/log/slip.log"); };
destination ppp { file("/var/log/ppp.log"); };
destination console { file("/dev/console"); };
destination allusers { usertty("*"); };
#destination loghost { udp("loghost" port(514)); };
# log facility filters
filter f_auth { facility(auth); };
filter f_authpriv { facility(authpriv); };
filter f_not_authpriv { not facility(authpriv); };
filter f_console { facility(console); };
filter f_cron { facility(cron); };
filter f_daemon { facility(daemon); };
filter f_ftp { facility(ftp); };
filter f_kern { facility(kern); };
filter f_lpr { facility(lpr); };
filter f_mail { facility(mail); };
filter f_news { facility(news); };
filter f_security { facility(security); };
filter f_user { facility(user); };
filter f_uucp { facility(uucp); };
filter f_local0 { facility(local0); };
filter f_local1 { facility(local1); };
filter f_local2 { facility(local2); };
filter f_local3 { facility(local3); };
filter f_local4 { facility(local4); };
filter f_local5 { facility(local5); };
filter f_local6 { facility(local6); };
filter f_local7 { facility(local7); };
```

```
# log level filters
filter f_emerg { level(emerg); };
filter f_alert { level(alert..emerg); };
filter f_crit { level(crit..emerg); };
filter f_err { level(err..emerg); };
filter f_warning { level(warning..emerg); };
filter f_notice { level(notice..emerg); };
filter f_info { level(info..emerg); };
filter f_debug { level(debug..emerg); };
filter f_is_debug { level(debug); };
# program filters
filter f_ppp { program("ppp"); };
filter f_slip { program("startslip"); };
# *.err;kern.warning;auth.notice;mail.crit                /dev/console
log { source(src); filter(f_err); destination(console); };
log { source(src); filter(f_kern); filter(f_warning); destination(console); };
log { source(src); filter(f_auth); filter(f_notice); destination(console); };
log { source(src); filter(f_mail); filter(f_crit); destination(console); };
# *.notice;authpriv.none;kern.debug;lpr.info;mail.crit;news.err     /var/log/messages
log { source(src); filter(f_notice); filter(f_not_authpriv); destination(messages); };
log { source(src); filter(f_kern); filter(f_debug); destination(messages); };
log { source(src); filter(f_lpr); filter(f_info); destination(messages); };
log { source(src); filter(f_mail); filter(f_crit); destination(messages); };
log { source(src); filter(f_news); filter(f_err); destination(messages); };
# security.*                                            /var/log/security
log { source(src); filter(f_security); destination(security); };
# auth.info;authpriv.info                               /var/log/auth.log
log { source(src); filter(f_auth); filter(f_info); destination(authlog); };
log { source(src); filter(f_authpriv); filter(f_info); destination(authlog); };
# mail.info                                             /var/log/maillog
```

```
log { source(src); filter(f_mail); filter(f_info); destination(maillog); };
# lpr.info                                                /var/log/lpd-errs
log { source(src); filter(f_lpr); filter(f_info); destination(lpd-errs); };

# ftp.info                                                /var/log/xferlog
log { source(src); filter(f_ftp); filter(f_info); destination(xferlog); };
# cron.*                                                  /var/log/cron
log { source(src); filter(f_cron); destination(cron); };
# *.=debug                                                /var/log/debug.log
log { source(src); filter(f_is_debug); destination(debuglog); };
# *.emerg                                                 *
log { source(src); filter(f_emerg); destination(allusers); };
# uncomment this to log all writes to /dev/console to /var/log/console.log
# console.info                                            /var/log/console.log
#log { source(src); filter(f_console); filter(f_info); destination(consolelog); };
# uncomment this to enable logging of all log messages to /var/log/all.log
# touch /var/log/all.log and chmod it to mode 600 before it will work
# *.*                                                     /var/log/all.log
#log { source(src); destination(all); };
# uncomment this to enable logging to a remote loghost named loghost
# *.*                                                     @loghost
log { source(src); destination(loghost); };
# uncomment these if you're running inn
# news.crit                                               /var/log/news/news.crit
# news.err                                                /var/log/news/news.err
# news.notice                                             /var/log/news/news.notice
#log { source(src); filter(f_news); filter(f_crit); destination(newscrit); };
#log { source(src); filter(f_news); filter(f_err); destination(newserr); };
#log { source(src); filter(f_news); filter(f_notice); destination(newsnotice); };
# !startslip
```

```
# *.*                                                    /var/log/slip.log
log { source(src); filter(f_slip); destination(slip); };
# !ppp
# *.*                                                    /var/log/ppp.log
log { source(src); filter(f_ppp); destination(ppp); };
```

#ป้อนเพิ่มในส่วนท้ายสุดของไฟล์ ตัวอย่างนี้สำหรับรับข้อมูล access.log จาก Proxy Server ถ้าหากอยากได้ข้อมูลจาก Server ชนิดไหนให้เพิ่มตามตัวอย่างต่อท้าย

```
# Log from squid (proxy) server kept access.log from LAN.
filter f_squid { program("squid") and facility(user); };
 destination d_squid {
  file("/var/log/$HOST/$YEAR/$MONTH/squid.$YEAR-$MONTH-$DAY"
  owner(root) group(adm) perm(665)
  create_dirs(yes) dir_perm(0775));
};
  log { source(s_client); filter(f_squid); destination(d_squid); };
```

หมายเหตุ: บูทเครื่องลูก 1 ครั้ง server จะสร้างโฟลเดอร์ให้ อัตโนมัติ

คำสั่งในการรับข้อมูลต่างๆจากเครื่องลูก

```
# Log mail server from pop3 service.
filter f_pop3 { match("pop3"); };
destination d_pop3 {
  file("/var/log/$HOST/$YEAR/$MONTH/pop3.$YEAR-$MONTH-$DAY"
  owner(root) group(adm) perm(665)
  create_dirs(yes) dir_perm(0775));
};
log { source(s_client); filter(f_pop3); destination(d_pop3); };
# Log mail server from imap service.
filter f_imap { match("imap|courier"); };
destination d_imap {
  file("/var/log/$HOST/$YEAR/$MONTH/imap.$YEAR-$MONTH-$DAY"
  owner(root) group(adm) perm(665)
```

```
  create_dirs(yes) dir_perm(0775));
};
log { source(s_client); filter(f_imap); destination(d_imap); };

# Log mail server use smtp or sendmail service.
filter f_smtp { match("sendmail|smtp"); };
destination d_smtp {
  file("/var/log/$HOST/$YEAR/$MONTH/smtp.$YEAR-$MONTH-$DAY"
  owner(root) group(adm) perm(665)
  create_dirs(yes) dir_perm(0775));
};
log { source(s_client); filter(f_smtp); destination(d_smtp); };
# Log mail server use postfix service.
filter f_postfix { program("^postfix/"); };
destination d_postfix {
  file("/var/log/$HOST/$YEAR/$MONTH/postfix.$YEAR-$MONTH-$DAY"
  owner(root) group(adm) perm(665)
  create_dirs(yes) dir_perm(0775));
};
log { source(s_client); filter(f_postfix); destination(d_postfix); };
# Log IM used iptable check MSN,ICQ,... service.
filter f_im1 { level(warn..emerg); };
filter f_im2 { program("iptables"); };
destination d_im {
  file("/var/log/$HOST/$YEAR/$MONTH/msn.$YEAR-$MONTH-$DAY"
  owner(root) group(adm) perm(665)
  create_dirs(yes) dir_perm(0775));
};
log { source(s_client); filter(f_im1); filter(f_im2); destination(d_im); };
# Log dhcp server.
```

```
filter f_dhcp { program("dhcpd") and facility(daemon); };
destination d_dhcp {
  file("/var/log/$HOST/$YEAR/$MONTH/dhcp.$YEAR-$MONTH-$DAY"
  owner(root) group(adm) perm(665)
  create_dirs(yes) dir_perm(0775));
};
log { source(s_client); filter(f_dhcp); destination(d_dhcp); };
# Log ssh server.
filter f_ssh   { program("sshd") and facility(auth, authpriv); };
destination d_ssh {
  file("/var/log/$HOST/$YEAR/$MONTH/ssh.$YEAR-$MONTH-$DAY"
  owner(root) group(adm) perm(665)
  create_dirs(yes) dir_perm(0775));
};
log { source(s_client); filter(f_ssh); destination(d_ssh); };
# Log ftp server.
filter f_ftp { program("vsftpd"); };
destination d_ftp {
  file("/var/log/$HOST/$YEAR/$MONTH/ftp.$YEAR-$MONTH-$DAY"
  owner(root) group(adm) perm(665)
  create_dirs(yes) dir_perm(0775));
};
log { source(s_client); filter(f_ftp); destination(d_ftp); };
# Log apache (httpd) web server.
filter f_www { program("logger"); };
filter f_www1 { program("apache"); };
destination d_www {
  file("/var/log/$HOST/$YEAR/$MONTH/www.$YEAR-$MONTH-$DAY"
  owner(root) group(adm) perm(665)
  create_dirs(yes) dir_perm(0775));
```

```
};
log { source(s_client); filter(f_www); filter(f_www1); destination(d_www); };
# Log Samba File server.
#
filter f_samba   { level(info..emerg) and program("smbd"); };
destination d_samba {
 file("/var/log/$HOST/$YEAR/$MONTH/samba.$YEAR-$MONTH-$DAY"
 owner(root) group(adm) perm(665)
 create_dirs(yes) dir_perm(0775));
};
log { source(s_client); filter(f_samba); destination(d_samba); };
# Log ldap server.
filter f_ldap { program("slapd"); };
destination d_ldap {
 file("/var/log/$HOST/$YEAR/$MONTH/ldap.$YEAR-$MONTH-$DAY"
 owner(root) group(adm) perm(665)
 create_dirs(yes) dir_perm(0775));
};
log { source(s_client); filter(f_ldap); destination(d_ldap); flags(final); };
# Log radius server.
filter f_radius { program("radiusd"); };
destination d_radius {
 file("/var/log/$HOST/$YEAR/$MONTH/radius.$YEAR-$MONTH-$DAY"
 owner(root) group(adm) perm(665)
 create_dirs(yes) dir_perm(0775));
};
log { source(s_client); filter(f_radius); destination(d_radius); };
filter f_router { facility(local2); };
destination d_router {
 file("/var/log/$HOST/$YEAR/$MONTH/router.$YEAR-$MONTH-$DAY"
```

```
 owner(root) group(adm) perm(665)
 create_dirs(yes) dir_perm(0775));
};
log { source(s_client); filter(f_router); destination(d_router); };
filter f_switch { facility(local3); };
destination d_switch {
 file("/var/log/$HOST/$YEAR/$MONTH/switch.$YEAR-$MONTH-$DAY"
 owner(root) group(adm) perm(665)
 create_dirs(yes) dir_perm(0775));
};
log { source(s_client); filter(f_switch); destination(d_switch); };
filter f_firewall { facility(local4); };
destination d_firewall {
 file("/var/log/$HOST/$YEAR/$MONTH/firewall.$YEAR-$MONTH-$DAY"
 owner(root) group(adm) perm(665)
 create_dirs(yes) dir_perm(0775));
};
log { source(s_client); filter(f_firewall); destination(d_firewall); };
filter f_vpnbox { facility(local5); };
destination d_vpnbox {
 file("/var/log/$HOST/$YEAR/$MONTH/vpnbox.$YEAR-$MONTH-$DAY"
 owner(root) group(adm) perm(665)
 create_dirs(yes) dir_perm(0775));
};
log { source(s_client); filter(f_vpnbox); destination(d_vpnbox); };
filter f_wifi { facility(local7); };
destination d_wifi {
 file("/var/log/$HOST/$YEAR/$MONTH/wifi.$YEAR-$MONTH-$DAY"
 owner(root) group(adm) perm(665)
 create_dirs(yes) dir_perm(0775));
```

};

log { source(s_client); filter(f_wifi); destination(d_wifi); };

server จะสร้างไดเล็กทอรี่ชื่อเดียวกับชื่อโฮสขึ้นมาเพื่อเก็บไฟล์ log

จากรูปไฟล์ log จะถูกเก็บเป็นไฟล์ของแต่ละวัน บนเครื่อง Centralized log Server

#pico /usr/local/etc/syslog-ng/syslog-ng.conf

พิมพ์เพิ่มท้ายไฟล์ดังนี้

filter f_mmmmm { match("chilli.c"); };

destination d_messages {

file("/var/log/$HOST/$YEAR/$MONTH/messages.$YEAR-$MONTH-$DAY"

owner(root) group(adm) perm(665)

create_dirs(yes) dir_perm(0775));

};

log { source(s_client); filter(f_mmmmm); destination(d_messages); };

ในส่วนของsquid ไม่ต้องเพิ่มเพราะว่าได้เพิ่มไปตั้งแต่ตอนแรกแล้ว

เมื่อแก้ไขไฟล์ syslog-ng.conf ให้ reboot server ใหม่

#shutdown –r now

การนำไปใช้ประโยชน์

งานวิจัยที่ผู้วิจัยและคณะได้พัฒนาและนำไปใช้จริงภายใต้แผนงานวิจัย เรื่องการออกแบบและพัฒนาต้นแบบระบบอินเทอร์เนตเกตเวย์ราคาถูกสำหรับมหาวิทยาลัย ประกอบด้วยโครงการวิจัยทั้งหมด 5 โครงการ ดังนี้

ชื่อแผนงานวิจัย (ภาษาไทย) การออกแบบและพัฒนาต้นแบบระบบอินเทอร์เนตเกตเวย์ราคาถูกสำหรับมหาวิทยาลัย

(ภาษาอังกฤษ) Design and Implementation of Internet Gateway Open Source System for University

ชื่อโครงการวิจัยภายใต้แผนงานวิจัย

โครงการวิจัยที่ 1 เรื่องการบันทึกล็อกไฟล์ตาม พรบ. ว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ 2550 สำหรับมหาวิทยาลัย
Centralized Log Server For University.

โครงการวิจัยที่ 2 เรื่องระบบพิสูจน์ตัวตนตามบัญชีผู้ใช้อินเทอร์เนต
User Authentication Internet Account System.

โครงการวิจัยที่ 3 เรื่องพัฒนาแอพพลิเคชั่นจัดการระบบจัดการฐานข้อมูลผู้ใช้อินเทอร์เนต
Application User Manager Internet Account for Administrator.

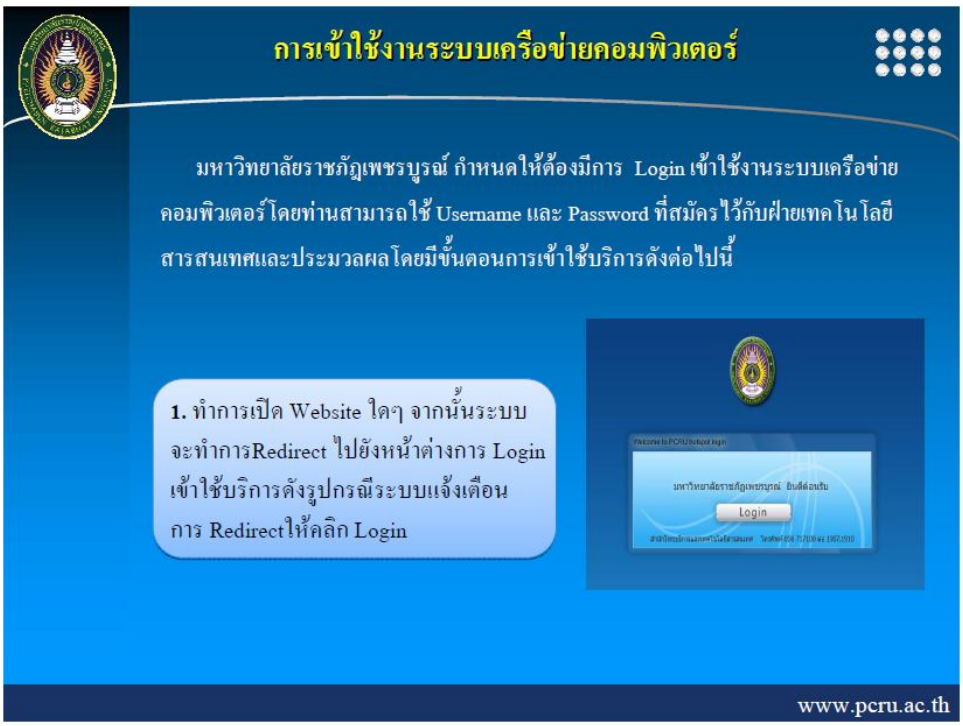
โครงการวิจัยที่ 4 เรื่องการอิมพลีเมนต์ระบบอินเทอร์เนตเกตเวย์สำหรับมหาวิทยาลัย
Implementation of Internet Gateway For University (Firewall, NAT,DHCP,Proxy Server,DNS,Database Server,Webserver,Mail Server,FTP Server).

โครงการวิจัยที่ 5 เรื่องประยุกต์ใช้งานระบบอินเทอร์เนตเกตเวย์มหาวิทยาลัยในระบบเครือข่ายทั้งแบบไวไฟ-ลีสไลน์
Interface Internet Gateway University WIFI–Lease Line Technology.

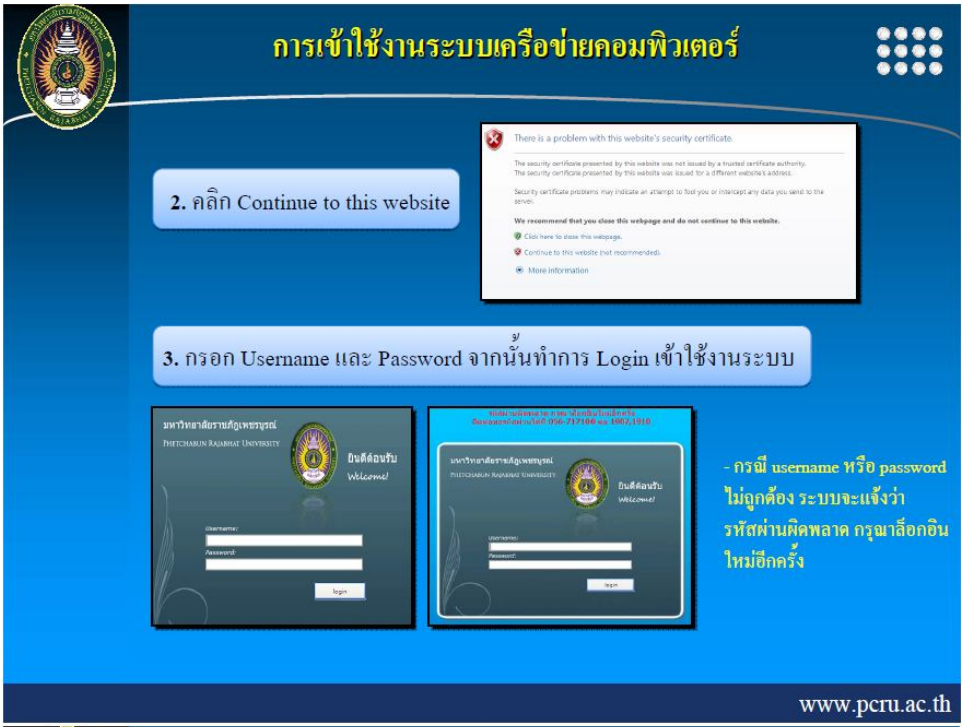
ซึ่งการนำไปใช้ต้องนำทุกโครงการมารวมกันแล้วจึงประกอบกันเป็นระบบเดียวจึงจะสามารถใช้งานได้สมบูรณ์ กรณีศึกษา ได้นำไปใช้กับมหาวิทยาลัยราชภัฏเพชรบูรณ์ ซึ่งมีหน่วยงานระดับคณะ 5 คณะ และ 4 สำนัก 1 สถาบัน และได้นำไปทดลองใช้กับหน่วยงานราชการภายนอก ได้แก่ สำนักงานสาธารณสุขจังหวัดเพชรบูรณ์ โรงเรียนติ้ววิทยาคม และโรงเรียนผาเมืองวิทยาคม

ผลการวิจัยพบว่าระบบใช้ได้ดี มีความเสถียรภาพสูง สามารถรองรับเครื่องคอมพิวเตอร์ของผู้ใช้ในหน่วยงานได้ทั้งหมดตามวัตถุประสงค์ที่ตั้งไว้ และประหยัดงบประมาณให้กับหน่วยงานดังกล่าวได้โดยเสียค่าใช้จ่ายราคาถูกมาก โดยหน่วยงานได้ปรับระบบแม่ข่ายเป็นโอเอสที่ใช้โอเพนซอร์ส ได้แก่ Web Server, Mail Server, FTP Server, DNS Server, Database Server , Gateway , Firewall โดยเฉพาะเว็บโฮสท์ที่มีเครื่องแม่ข่ายจำนวนมาก ตามหน่วยงานที่ต้องการใช้หลายเครื่องและบริการนักศึกษาได้ปรับเปลี่ยนมาใช้โอเพนซอร์สทั้งหมด ซึ่งมีรายละเอียดตามตัวอย่างพอสังเขป ดังนี้

การใช้อินเทอร์เนตภายในมหาวิทยาลัย ขั้นตอนที่ 1 2 3 และ 4 ดังภาพเป็นการเรียกใช้โปรแกรมเปิดเว็บไซท์ระบบทำการบังคับให้ผู้ใช้เข้าสู่ระบบ (Authentication) เพื่อ Login เข้าสู่ระบบ โดยวิธีนี้ระบบจะสามารถบันทึกการใช้งานอินเทอร์เนตลงสู่ล็อกไฟ (Centralize Log Server)



ที่มา : การเข้าใช้อินเทอร์เนต มหาวิทยาลัยราชภัฏเพชรบูรณ์

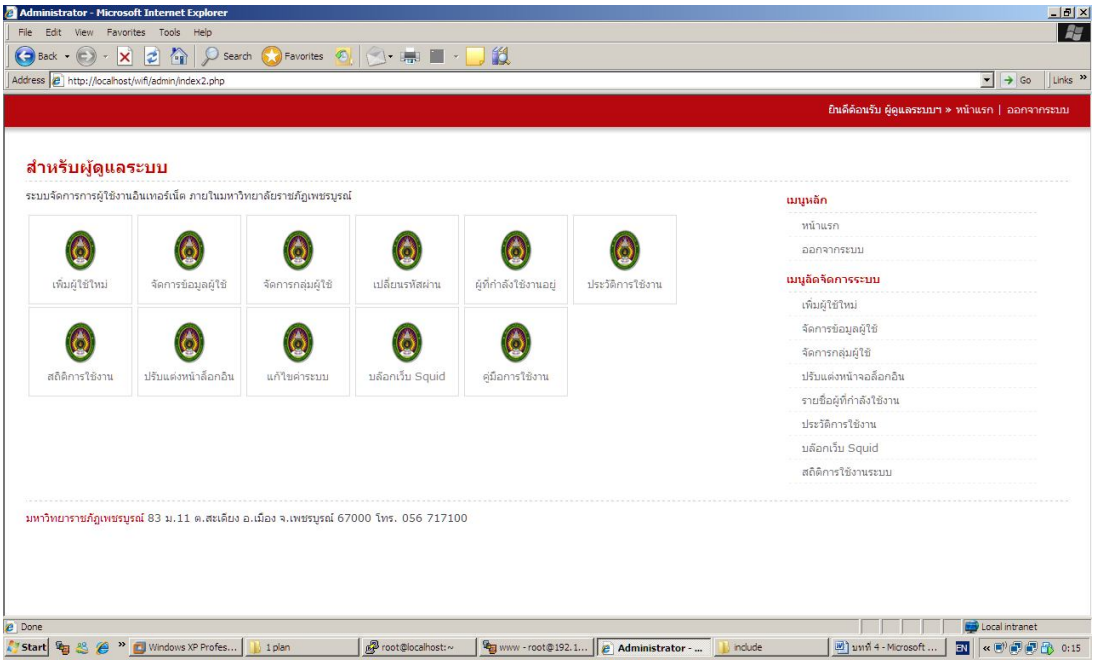


ที่มา : การเข้าใช้อินเทอร์เนต มหาวิทยาลัยราชภัฏเพชรบูรณ์

เพื่อเป็นการป้องกันการนำเอา User และ Password ของผู้อื่นไปใช้ในทางที่ไม่ถูกต้องหรือแอบเอาไปใช้ในทางที่อาจทำให้เกิดความผิดตามกฎหมายว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ ระบบจะให้ผู้ใช้สามารถเปลี่ยนรหัสผ่านด้วยตัวผู้ใช้ได้

ที่มา : การเปลี่ยนรหัสผ่านของผู้ใช้อินเทอร์เนต มหาวิทยาลัยราชภัฏเพชรบูรณ์

สำหรับผู้ดูแลระบบ เมื่อเข้าสู่ระบบ ระบบจะแสดงสิทธิ์ต่างๆ ที่ผู้ดูแลระบบสามารถกระทำในระบบได้เพื่อควบคุมการใช้งานอินเทอร์เนตของผู้ใช้ทุกคนในระบบ

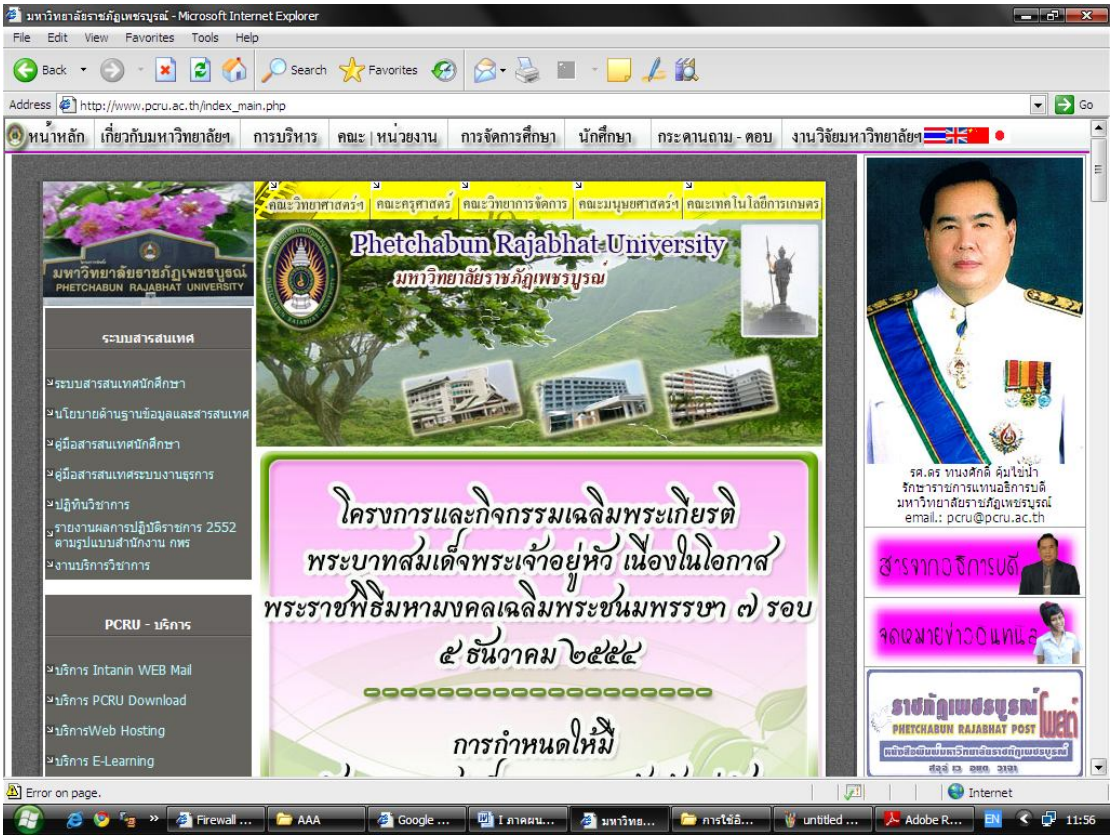


ที่มา : สำหรับผู้ดูแลระบบ มหาวิทยาลัยราชภัฏเพชรบูรณ์

ระบบการใช้อีเมลย์สำหรับบุคลากร และนักศึกษาของมหาวิทยาลัยราชภัฏเพชรบูรณ์ โดยระบบที่เป็นโอเพนซอร์ส (Open Source) เป็นผลทำให้ประหยัดงบประมาณให้กับมหาวิทยาลัยเป็นอย่างมาก และระบบสามารถใช้รับส่งจดหมายได้อย่างมีประสิทธิภาพ

ที่มา : การใช้งานอีเมลย์ มหาวิทยาลัยราชภัฏเพชรบูรณ์

ระบบการใช้เว็บโฮสท์ติ้ง (Web Hosting) สำหรับบุคลากร และนักศึกษาของมหาวิทยาลัยราชภัฏเพชรบูรณ์ โดยระบบที่เป็นโอเพนซอร์ส (Open Source) เป็นผลทำให้ประหยัดงบประมาณให้กับมหาวิทยาลัยเป็นอย่างมาก และระบบสามารถใช้ได้อย่างมีประสิทธิภาพ



ที่มา : การใช้งานเว็บโฮสท์ติ้ง (Web Hosting) มหาวิทยาลัยราชภัฏเพชรบูรณ์

สรุปผู้วิจัยและคณะได้พัฒนาระบบอื่นๆ ที่ไม่ได้จับภาพหน้าจอมาแสดงในภาคผนวกนี้ ได้แก่เว็บไซท์ของคณะ โปรแกรมวิชาและหน่วยงานที่เป็นศูนย์ สำหนักต่างๆ อีกหลายหน่วยงานที่ตั้งอยู่ในมหาวิทยาลัย รวมถึงหน่วยงานภายนอกที่ได้ไปทดลองใช้ ได้แก่ สำนักงานสาธารณสุขจังหวัดเพชรบูรณ์ และโรงเรียนมัธยมในอำเภอหล่มสักอีก 2 แห่ง ผลปรากฏว่าระบบใช้ได้ผลดีเป็นที่น่าพอใจของผู้บริหารและผู้ใช้ในหน่วยงาน ซึ่งปัจจุบันหน่วยงานต่างๆ ก็ยังใช้ระบบนี้เพื่อควบคุมการใช้งานอินเทอร์เนตของผู้ใช้อยู่ต่อไป โดยระบบนี้ช่วยประหยัดงบประมาณด้านพัฒนาไอทีให้กับหน่วยงานได้สูงมาก

ประวัติผู้วิจัย

1. ชื่อ - นามสกุล (ภาษาไทย) นาย นาง นางสาว ยศ

   นายประยูร ไชยบุตร

   ชื่อ - นามสกุล (ภาษาอังกฤษ) Mr, Mrs, Miss, Rank

   MR. Prayoon Chaibuth

2. เลขหมายบัตรประจำตัวประชาชน

   3 5003 00043 95 3

3. ตำแหน่งปัจจุบัน

   -อาจารย์ ระดับ 7 คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏเพชรบูรณ์

   -ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏเพชรบูรณ์

4. หน่วยงานและสถานที่อยู่ที่ติดต่อได้สะดวก พร้อมหมายเลขโทรศัพท์ โทรสาร และ ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)

   สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏเพชรบูรณ์

   ถนนสระบุรี-หล่มสัก ตำบลสะเดียง อำเภอเมือง จังหวัดเพชรบูรณ์ 67000

   โทรศัพท์ ที่ทำงาน 056-717151 มือถือ 086 4481991

   โทรสาร 056-717151 Email : prayoon@pcru.ac.th

5. ประวัติการศึกษา

   ปริญญาตรี วุฒิ ค.บ. (คอมพิวเตอร์ศึกษา) วิทยาลัยครูเชียงใหม่

   ปริญญาโท วุฒิ วท.ม. (คอมพิวเตอร์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

6. สาขาวิชาการที่มีความชำนาญพิเศษ (แตกต่างจากวุฒิการศึกษา) ระบุสาขาวิชาการ

   -ผู้บริหารสำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏเพชรบูรณ์

   -กำกับดูแลระบบเครือข่ายคอมพิวเตอร์และอินเทอร์เนตมหาวิทยาลัยราชภัฏเพชรบูรณ์

   -กำกับดูแลระบบสารสนเทศมหาวิทยาลัยราชภัฏเพชรบูรณ์

7. ประสบการณ์ที่เกี่ยวข้องกับการบริหารงานวิจัยทั้งภายในและภายนอกประเทศ โดยระบุสถานภาพในการทำการวิจัยว่าเป็นผู้อำนวยการแผนงานวิจัย หัวหน้าโครงการวิจัย หรือ ผู้ร่วมวิจัยในแต่ละข้อเสนอการวิจัย

   7.1 ผู้อำนวยการแผนงานวิจัย : ชื่อแผนงานวิจัย

   7.2 หัวหน้าโครงการวิจัย : ชื่อโครงการวิจัย

1) การส่งเกรด สถาบันราชภัฏเพชรบูรณ์ (2546) ทุนวิจัยของสภาสถาบันราชภัฏ

2) วิจัยเรื่อง การสร้างนวัตกรรม E-Learning ระบบเครือข่ายคอมพิวเตอร์ (2547)

3) ระบบสารสนเทศการวิจัย สถาบันวิจัยและพัฒนา มหาวิทยาลัยราชภัฏเพชรบูรณ์ (2548)

4) การพัฒนาโปรแกรมระบบฐานข้อมูลการท่องเที่ยวเพื่อการสืบค้นผ่านระบบ

5) เครือข่ายอินเทอร์เนต กรณีศึกษาสถานที่ท่องเที่ยวจังหวัดเพชรบูรณ์ (2549)

7.3 งานวิจัยที่ทำเสร็จแล้ว

1) การส่งเกรด สถาบันราชภัฏเพชรบูรณ์ (2546) ทุนวิจัยของสถาบันราชภัฏเพชรบูรณ์

2) วิจัยเรื่อง การสร้างนวัตกรรม E-Learning ระบบเครือข่ายคอมพิวเตอร์ (2547)

3) ระบบสารสนเทศการวิจัย สถาบันวิจัยและพัฒนา มหาวิทยาลัยราชภัฏเพชรบูรณ์ (2548)

4) การพัฒนาโปรแกรมระบบฐานข้อมูลการท่องเที่ยวเพื่อการสืบค้นผ่านระบบเครือข่ายอินเทอร์เนต กรณีศึกษาสถานที่ท่องเที่ยวจังหวัดเพชรบูรณ์ (2549)

8. ประสบการณ์การทำงาน

8.1 ด้านการสอน

1) อาจารย์ประจำโปรแกรมวิชาวิทยาการคอมพิวเตอร์ สถาบันราชภัฏเทพสตรี ปี 2537-2540

2) อาจารย์ประจำโปรแกรมวิชาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยราชภัฏเพชรบูรณ์ในปี 2540-ปัจจุบัน

8.2 ด้านการบริหาร

1) ประธานโปรแกรมคอมพิวเตอร์ศึกษา (2543-2544)

2) รองผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ (2544-2547)

3) ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ (2548-ปัจจุบัน)

การออกแบบและพัฒนาต้นแบบ
ระบบอินเทอร์เนตเกตเวย์ราคาถูกสำหรับมหาวิทยาลัย

Design and Implementation of Internet Gateway Open Source System for University

ประยูร ไชยบุตร
Prayoon chaibuth

บทคัดย่อ

งานการวิจัยฉบับนี้มีจุดประสงค์คือต้องการสร้างระบบมาเพื่อเก็บข้อมูลผู้ใช้งานในอินเทอร์เนตตามข้อบังคับของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในส่วนของผู้ให้บริการอินเทอร์เน็ต(Internet Service Provider) วิธีดำเนินการวิจัยในครั้งนี้ผู้วิจัยและทีมงานได้ออกแบบระบบเพื่อที่จะให้รองรับพระราชบัญญัติดังกล่าวโดยนำผลของการสำรวจและสอบถามผู้ให้บริการอินเทอร์เนตส่วนใหญ่ทั้งภาครัฐและเอกชน โดยเฉพาะสถานศึกษามหาวิทยาลัย วิทยาลัย โรงเรียน โรงพยาบาล และหน่วยงานอื่นๆ ที่ให้บริการอินเทอร์เนตกับบุคลากรในองค์กร หลายหน่วยงานยังไม่ได้มีการเตรียมการใด ๆ เพื่อรองรับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ผู้วิจัยได้วิเคราะห์ระบบเพื่อให้สามารถรองรับข้อกำหนดของพระราชบัญญัติโดยมีส่วนการทำงานดังนี้

มีการระบุตัวตนของผู้ใช้งาน โดยมีระบบสำหรับการพิสูจน์ตัวตนของผู้ใช้บริการใช้ระบบสมาชิกสำหรับให้สมาชิกเข้าใช้งานเครือข่ายอินเทอร์เน็ต

มีระบบการจัดการเวลาให้เป็นมาตรฐานที่น่าเชื่อถือและสามารถนำไปอ้างอิงเมื่อเกิดเหตุโดยมีความผิดพลาดไม่เกิน 10 มิลลิวินาที

มีระบบการเก็บรักษาข้อมูลที่ครบถ้วนและเชื่อถือได้ และจำเป็นต้องมีการสำรองข้อมูลการจราจรทางคอมพิวเตอร์ของผู้ใช้บริการ

มีระบบการจัดการสำหรับการค้นคืนข้อมูลการจราจรย้อนหลังเพื่อใช้สำหรับค้นข้อมูลโดยจะมีรายงานจากเจ้าหน้าที่เพื่อทำการระบุใครเป็นผู้กระทำความผิดโดยการออกเป็นรายงานสำหรับเป็นหลักฐานทางกฎหมาย

มีระบบที่รองรับเครือข่ายไร้สายโดยกำหนดให้ระบบที่พัฒนาทั้งหมดสามารถรองรับเครือข่ายไร้สาย จากการวิเคราะห์ระบบทั้งหมดสามารถออกแบบเป็น 2 ระบบย่อย เพื่อรองรับทั้งเครือข่ายแบบมีสายและไร้สาย

ได้แก่ ระบบฐานข้อมูลสำหรับเก็บข้อมูลผู้ใช้งานอินเทอร์เนต (Member for Internet) และระบบค้นคืนและระบุผู้ใช้งานในอินเทอร์เนต (Retrieval System) โดยแบ่งการทำงานหรือดำเนินการต่างๆ ออกเป็นส่วนย่อยเพื่อให้ง่ายในการจัดการระบบ

การพัฒนาระบบงานดังกล่าวผู้วิจัยได้ใช้ระบบปฏิบัติ FreeBSD ใช้ระบบฐานข้อมูลสำหรับเก็บข้อมูลผู้ใช้งานอินเทอร์เนต ผู้วิจัยได้พัฒนาระบบขึ้นโดยใช้ภาษา PHP เป็นตัวจัดการพัฒนาแอพพลิเคชันต่างๆ โปรแกรม FreeRadius และ Chillispot เพื่อใช้ในการพิสูจน์ตัวตนในการเข้าสู่ระบบอินเทอร์เน็ตโดยมีการกำหนดให้มีการระบุชื่อผู้ใช้ด้วยหมายเลขประจำตัวประชาชนและสำหรับเครือข่ายไร้สายได้มีการลงทะเบียนหมายเลข MAC Address ไว้ในฐานข้อมูล เพื่อการสืบค้นหาตัวผู้กระทำความผิดได้ในภายหลังได้เมื่อมีการกระทำผิดตามพระราชบัญญัติ

Abstract

This research work aims is to create a system to collect data on Internet users in accordance with the Act and the Computer Crime Act 2550 in the Internet service provider in this research. system to provide support to such Act from the survey by asking Internet service providers, most public and private University College of Education, particularly schools, hospitals and other agencies. Many agencies have not been prepared to support any Act of the Computer Crime Act 2550, the researcher has analyzed the system in order to accommodate the requirements of this Act, with the work as follows.

The identity of the user. The system for authentication of users using the system for member to member using the Internet.

Time management system as standard and can be trusted based on the scene with an error less than 10 milliseconds.

A data storage system complete and reliable. And need to back up traffic a user's computer. Management system for retrieving data traffic back to searching for information will be reported by the authorities to identify offenders who are released by the reports as evidence of the law. Compatibility with wireless networking system developed by the entire wireless network can support. The analysis of the entire system can be designed as two sub-systems to support the network wired and wireless, including the database for storing information using the Internet (Member for Internet) and retrieval and provide users in the Internet. internet (Retrieval System) consists of work or the various Into subsections to make it easier. Management system

Development of such systems, the researcher used the FreeBSD operating system, database system for storing information using the Internet. Researchers have developed by using PHP, a management development of applications software FreeRadius and Chillispot used for authentication to access the Internet by adopting a user

name with a number of identification and For a wireless network has MAC Address registration number in the database. To search for the offender at a later date when the offense under this Act.

บทนำ

การใช้ระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย และสถานศึกษามีวัตถุประสงค์ในการใช้งานด้านการเรียนการสอน และการสืบค้นสารสนเทศ สำหรับนักศึกษา และบุคลากร โดยมีจำนวนเครื่องคอมพิวเตอร์ที่เชื่อมต่อเป็นระบบเครือข่ายท้องถิ่น ต่อมา มีการพัฒนาระบบเครือข่ายให้มีประสิทธิภาพมากขึ้น โดยใช้งานผ่านระบบเครือข่ายอินเทอร์เนต ความต้องการแลกเปลี่ยนข้อมูล ข่าวสารระหว่างองค์กรจึงเกิดขึ้น ปัจจุบันได้มีการขยายเครือข่ายให้ครอบคลุม กับความต้องการของผู้ใช้บริการผ่านระบบเครือข่ายภายในมหาวิทยาลัยระบบเครือข่ายผ่านคู่สายโทรศัพท์ระบบลีสไลน์ผ่านระบบเครือข่ายใยแก้วนำแสงและระบบเครือข่ายไร้สาย ซึ่งมีจำนวนผู้ใช้บริการเพิ่มขึ้นอย่างต่อเนื่อง

ในปีการศึกษา 2553 มหาวิทยาลัยราชภัฏเพชรบูรณ์ มีผู้ใช้บริการระบบเครือข่ายทั้งสิ้นประมาณ 10,000 คนโดยประมาณได้แก่ บุคลากรของมหาวิทยาลัย นักศึกษาภาคปกติ นักศึกษาภาค กศ.ปช. และมีเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับระบบเครือข่ายของมหาวิทยาลัยกว่า 1,000 เครื่อง ทั้งแบบตั้งโต๊ะและแบบพกพา กระจายอยู่ตามอาคารต่างๆ ทั่วมหาวิทยาลัย จากการสังเกตพฤติกรรมการใช้บริการผ่านระบบเครือข่าย พบว่ามีปริมาณการใช้งานมากในช่วงเวลา 8.30– 20.00 น. โดยใช้บริการอินเตอร์เน็ตผ่านโปรโตคอล HTTP FTP และ SMTP เป็นส่วนใหญ่

ปัจจุบันระบบเครือข่ายอินเทอร์เนตเป็นสิ่งหนึ่งที่สถานศึกษาทุกแห่งมีความจำเป็นจะต้องนำมาประยุกต์ใช้งานทั้งด้านการเรียนการสอนและงานด้านการบริหารธุรการดังกล่าว มีการลงทุนด้วยงบประมาณที่สูงมากเมื่อเทียบกับการลงทุนในด้านต่างๆ ในสถานศึกษาผู้ที่เกี่ยวข้องกับการใช้ระบบเครือข่ายอินเทอร์เนตได้แก่บุคลลากรทางด้านการศึกษาทั้งหมด คืออาจารย์ ข้าราชการ นักเรียน นักศึกษา รวมถึงบุคคลภายนอกที่เข้ามาใช้ระบบเครือข่ายของหน่วยงานทางการศึกษาในบางครั้ง เช่น มีการอบรมสัมมนา การประชุม เป็นต้น การให้บริการอินเทอร์เนตในสถานศึกษาปัจจุบันมีทั้งแบบมีสายและแบบไร้สาย

ทีมผู้วิจัยได้ทดลองและใช้งานโดยการอิมพลีเมนต์กับระบบ Lease Line และ WiFi เข้าด้วยกันทุกระบบโดยทดลองกับมหาวิทยาลัยราชภัฏเพชรบูรณ์เชื่อมต่อไปตามคณะ ศูนย์ สำนัก และสถาบัน หอพักนักศึกษา บ้านพักอาจารย์ บ้านพักข้าราชการ โดยใช้งบประมาณอันจำกัด มาบริหารจัดการปรากฏว่าได้ผลดีเป็นที่น่าพอใจ และคิดจะวิจัยต่อไปอีกโดยพัฒนาระบบอินเทอร์เนตเกตุเวย์ราคาถูกโดยใช้โปรแกรมประเภทโอเพนซอร์ส ได้แก่ ระบบปฏิบัติการที่เป็นลีนุกซ์หรือยูนิกส์ฟรีที่ไม่ต้องเสียค่าลิขสิทธิ์ซอร์ฟแวร์ที่มีราคาสูงมากในปัจจุบัน เช่น FreeBSD CentOS RedHat OpenBSD ฯลฯ และใช้ระบบฐานข้อมูลที่เป็นโอเพนซอร์สทั้งหมดได้แก่ MySQL และซอร์ฟแวร์อื่นที่ใช้ในระบบพิสูจน์ตัวตน เช่น Chillispot และ FreeRadius มาพัฒนาระบบเพื่อให้ได้ระบบควบคุมการใช้อินเทอร์เนตที่มีประสิทธิภาพและราคาถูก เหมาะกับหน่วยงานเล็กๆ ที่มีงบประมาณจำนวนน้อย

ผู้วิจัยและทีมงานได้ค้นหาข้อมูลเพื่อจะพัฒนาในส่วนที่ยังไม่มีประสิทธิภาพให้ระบบเครือข่ายมีความเสถียรภาพสูงสุด แล้วจะเผยแพร่ให้กับหน่วยงานอื่นๆ ให้ได้ใช้ระบบดังกล่าวโดยไม่คิดค่าลิขสิทธิ์ใดๆ ทั้งสิ้นพร้อม

อบรมให้ใช้ฟรี โดยมีเป้าหมายคือสถาบันการศึกษา หรือองค์กรที่มีงบประมาณจำกัดเป็นหลักเนื่องจากเป็นหน่วยงานที่ไม่แสวงหากำไร ให้ได้ใช้ระบบเครือข่ายที่ดีมีประสิทธิภาพสูง โดยผู้ใช้งานจะได้ใช้ประโยชน์จากระบบเครือข่ายอย่างเต็มที่และเกิดประโยชน์สูงสุดให้กับหน่วยงานต่อไป

วัตถุประสงค์ของการวิจัย

1. พัฒนาระบบการบันทึกการจราจรบนระบบเครือข่ายคอมพิวเตอร์ (Log File) ตาม พรบ. ว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ 2550
2. พัฒนาระบบระบบพิสูจน์ตัวตน
3. พัฒนาระบบจัดการฐานข้อมูลผู้ใช้ระบบอินเทอร์เนต
4. พัฒนาระบบอินเทอร์เนตเกตเวย์สำหรับมหาวิทยาลัย
5. พัฒนาระบบอินเทอร์เฟสอินเทอร์เนตเกตเวย์กับไวไฟ-ลีสไลน์
6. ทำการเผยแพร่องค์ความรู้แก่หน่วยงานที่เป็นภาคี ได้แก่ มหาวิทยาลัยราชภัฏ มหาวิทยาลัยของรัฐและเอกชน และผู้สนใจทั่วไป

วิธีการดำเนินการวิจัย

กิจกรรม	ระยะเวลาตามไตรมาส			
	ไตรมาส1	ไตรมาส2	ไตรมาส3	ไตรมาส4
1. เสนอโครงการขออนุญาตดำเนินโครงการ				
2. วางแผนการวิจัย				
3. ศึกษาบริบทและความต้องการของมหาวิทยาลัยและผู้ใช้ระบบ				
4. วิเคราะห์ศักยภาพทำแผนยุทธศาสตร์การวิจัย				
5. ดำเนินการตามแผนรวมทั้งโครงการย่อย				
6. สำรวจติดตามผลโครงการ				
7. วิเคราะห์ผลการวิจัย				
8. สรุปผลการวิจัย				
9. เขียนรายงานการวิจัย				
10. จัดทำรูปเล่มฉบับสมบูรณ์				
11. เผยแพร่งานวิจัย				

ผลการวิจัย

งานการวิจัยฉบับนี้มีจุดประสงค์คือต้องการสร้างระบบมาเพื่อเก็บข้อมูลผู้ใช้งานใน อินเทอร์เนตตามข้อบังคับของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในส่วนของผู้ให้บริการอินเทอร์เน็ต ในการดำเนินการวิจัยผู้วิจัยและทีมงานได้ออกแบบสอบถามการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ตามข้อบังคับของว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2550 กับทางผู้ให้บริการอินเทอร์เนต เพื่อทำการออกแบบระบบที่รองรับพระราชบัญญัติดังกล่าว จากผลของการสำรวจแบบสอบถามผู้ให้บริการอินเทอร์เนตส่วนใหญ่ยังไม่ได้มีการเตรียมการใด ๆ ที่จะรองรับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีเพียงบริษัทที่พัฒนาขึ้นมาและขายในราคาที่สูงมากบางหน่วยงานไม่สามารถที่จะจัดสร้างระบบนี้ได้ ผู้วิจัยและทีมงานจึงได้คิดวิธีการที่จะสร้างระบบนี้ขึ้นมาโดยวิเคราะห์และออกแบบระบบเพื่อให้สามารถรองรับข้อกำหนดของพระราชบัญญัติ โดยมีส่วนการทำงานดังนี้

1 . มีการระบุตัวตนของผู้ใช้งาน โดยมีระบบสำหรับการพิสูจน์ตัวตนของผู้ใช้บริการ ใช้ระบบสมาชิกสำหรับให้สมาชิกเข้าใช้งานเครือข่ายอินเทอร์เน็ต

2. มีระบบการจัดการเวลาให้เป็นมาตรฐานที่น่าเชื่อถือและสามารถนำไปอ้างอิงเมื่อเกิดเหตุโดยมีความผิดพลาดไม่เกิน 10 มิลลิวินาที

3. มีระบบการเก็บรักษาข้อมูลที่ครบถ้วนและเชื่อถือได้ เข้ารหัสข้อมูลล็อกไฟล์ และจำเป็นต้องมีการสำรองข้อมูลการจราจร ข้อมูลล็อกไฟล์ ที่เกิดขึ้นด้วย

4. มีระบบการจัดการสำหรับการค้นคืนข้อมูลการจราจรย้อนหลังเพื่อใช้สำหรับค้นข้อมูลโดยจะมีรายงานจากเจ้าหน้าที่เพื่อทำการระบุใครเป็นผู้กระทำความผิดโดยการออกเป็นรายงานสำหรับเป็นหลักฐานทางกฎหมาย

5. มีระบบที่รองรับเครือข่ายไร้สายโดยกำหนดให้ระบบที่พัฒนาทั้งหมดสามารถรองรับเครือข่ายไร้สาย จากการวิเคราะห์ระบบทั้งหมดสามารถออกแบบเป็น 2 ระบบย่อย เพื่อรองรับทั้งเครือข่ายแบบมีสายและไร้สาย ได้แก่ ระบบฐานข้อมูลสำหรับเก็บข้อมูลผู้ใช้งานอินเทอร์เนต (Member System Account for Internet) และระบบค้นคืนและระบุผู้ใช้งานในอินเทอร์เนต (Retrieval System) โดยแบ่งการทำงานหรือดำเนินการต่างๆ ออกเป็นส่วนย่อยเพื่อให้ง่ายในการจัดการระบบทั้งหมดการพัฒนาระบบงานดังกล่าวผู้วิจัยได้ใช้ระบบปฏิบัติ FreeBSD

โดยระบบฐานข้อมูลสำหรับเก็บข้อมูลผู้ใช้งานอินเทอร์เนต ผู้วิจัยได้พัฒนาระบบขึ้นโดยใช้ภาษา PHP เป็นตัวพัฒนาเขียนโปรแกรมควบคุมระบบ ใช้ฐานข้อมูล MySQL เป็นตัวเก็บข้อมูล และใช้โปรแกรม FreeRadius และ Chillispot ในการพิสูจน์ตัวตนในการเข้าสู่ระบบอินเทอร์เน็ตโดยมีการกำหนดให้ชื่อผู้ใช้ด้วยหมายเลขประจำตัวประชาชนและสำหรับเครือข่ายไร้สายได้มีการลงทะเบียนหมายเลข MAC Address ด้วยสำหรับสู่ระบบอินเทอร์เน็ตและระบบค้นคืนและระบุผู้ใช้งานในอินเทอร์เนต

มีการพัฒนาระบบในส่วนที่เป็นการตั้งค่าระบบ ได้แก่ การเทียบเวลาสากลระหว่างอุปกรณ์คอมพิวเตอร์ (Network Time Protocol) และการเขียนโปรแกรม Shell Script ในการเก็บข้อมูลล็อกไฟล์โดยเก็บข้อมูลกิจกรรมที่เกิดขึ้นตามที่ต้องการและบันทึกเป็นรายวันและทุกครั้งที่มีการใช้งานอินเทอร์เนตของผู้ใช้บริการ

หลังจากที่ได้ทดสอบระบบเก็บข้อมูล พิสูจน์ตัวตน ค้นคืนและระบุผู้ใช้บริการอินเทอร์เนต ผลปรากฏว่าระบบเก็บข้อมูล พิสูจน์ตัวตน ค้นคืนและระบุผู้ใช้บริการอินเทอร์เนต สามารถทำงานรองรับ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 โดยไม่ได้ส่งผลกระทบทางลบต่อการให้บริการอินเทอร์เน็ตและสามารถค้นคืนและสามารถระบุผู้ใช้งานในอินเทอร์เนตที่เข้าข่ายผิดหรืออาจจะผิดข้อกำหนดตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้อย่างถูกต้องและมีประสิทธิภาพรองรับผู้ใช้ได้มากกว่า 10,000 รายชื่อและเข้าใช้ระบบพร้อมกันมากกว่า 1,000 ผู้ใช้ (User Online)

ผลการวิจัยพบว่าระบบใช้ได้ดี มีความเสถียรภาพสูง สามารถรองรับเครื่องคอมพิวเตอร์ของผู้ใช้ในหน่วยงานได้ทั้งหมดตามวัตถุประสงค์ที่ตั้งไว้ และประหยัดงบประมาณให้กับหน่วยงานดังกล่าวได้โดยเสียค่าใช้จ่ายราคาถูกมาก โดยหน่วยงานได้ปรับระบบแม่ข่ายเป็นโอเอสที่ใช้โอเพนซอร์ส ได้แก่ Web Server, Mail Server, FTP Server, DNS Server, Database Server , Gateway , Firewall โดยเฉพาะเว็บโฮสท์ที่มีเครื่องแม่ข่ายจำนวนมาก ตามหน่วยงานที่ต้องการใช้หลายเครื่องและบริการนักศึกษาได้ปรับเปลี่ยนมาใช้โอเพนซอร์สทั้งหมด ซึ่งมีรายละเอียดตามตัวอย่างพอสังเขป ดังนี้

การใช้อินเทอร์เนตภายในมหาวิทยาลัย ขั้นตอนที่ 1 2 3 และ 4 ดังภาพเป็นการเรียกใช้โปรแกรมเปิดเว็บไซท์ระบบทำการบังคับให้ผู้ใช้เข้าสู่ระบบ (Authentication) เพื่อ Login เข้าสู่ระบบ โดยวิธีนี้ระบบจะสามารถบันทึกการใช้งานอินเทอร์เนตลงสู่ล็อกไฟ (Centralize Log Server)

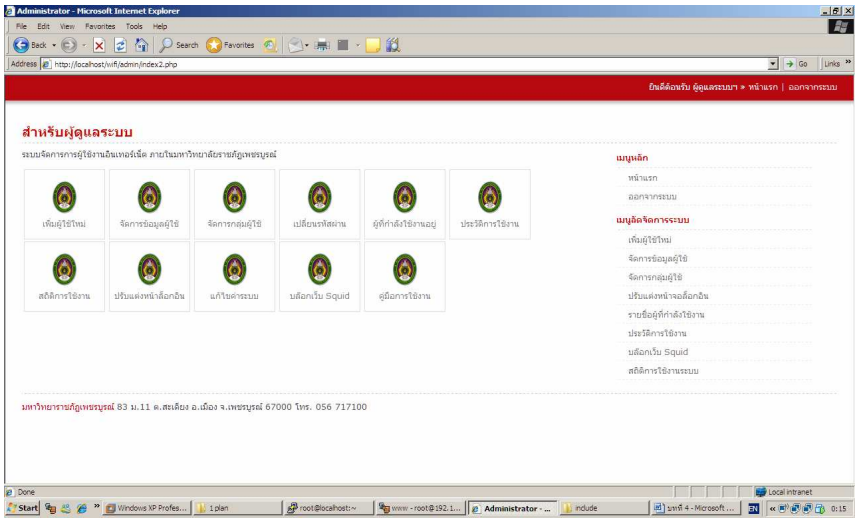
ที่มา : การล็อกอินเข้าใช้อินเทอร์เนต มหาวิทยาลัยราชภัฏเพชรบูรณ์

ที่มา : การล็อกอินเข้าใช้อินเทอร์เนต มหาวิทยาลัยราชภัฏเพชรบูรณ์

เพื่อเป็นการป้องกันการนำเอา User และ Password ของผู้อื่นไปใช้ในทางที่ไม่ถูกต้องหรือแอบเอาไปใช้ในทางที่อาจทำให้เกิดความผิดตามกฎหมายว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ ระบบจะให้ผู้ใช้สามารถเปลี่ยนรหัสผ่านด้วยตัวผู้ใช้ได้

ที่มา : การเปลี่ยนรหัสผ่านของผู้ใช้อินเทอร์เนต มหาวิทยาลัยราชภัฏเพชรบูรณ์

สำหรับผู้ดูแลระบบ เมื่อเข้าสู่ระบบ ระบบจะแสดงสิทธิ์ต่างๆ ที่ผู้ดูแลระบบสามารถกระทำในระบบได้เพื่อควบคุมการใช้งานอินเทอร์เนตของผู้ใช้ทุกคนในระบบ



ที่มา : รายการหลักสำหรับผู้ดูแลระบบ มหาวิทยาลัยราชภัฏเพชรบูรณ์

อภิปรายผล

อุปสรรคปัญหาที่พบและแนวทางแก้ปัญหาในการใช้งานระบบเก็บข้อมูล พิสูจน์ตัวตน ค้นคืนและระบุตัวตนผู้ใช้บริการอินเทอร์เนต โดยการทดลองใช้ระบบได้มีการทดสอบและใช้งานจริงในอินเทอร์เนตของมหาวิทยาลัยราชภัฏเพชรบูรณ์ที่มีความเร็วของอินเทอร์เนตที่ 6 Mbps 20 Mbps และ 1 Gbps ผู้วิจัยได้พบว่ามีปัญหาและข้อจำกัดของโปรแกรม โดยแบ่งออกเป็น 2 ส่วน ดังนี้

ปัญหาความไม่เข้าใจในระบบของผู้แลระบบในอินเทอร์เนต เนื่องจากระบบที่ติดตั้งนั้นเป็นเรื่องใหม่และเป็นข้อกฎหมายที่กำหนดใหม่ ที่ผู้ใช้บริการต้องถูกบังคับให้เข้าสู่ระบบอินเทอร์เนตเมื่ออินเทอร์เน็ตใช้การไม่ได้ สิ่งแรกที่ผู้ดูแลระบบคิดคือเกิดขึ้นจากระบบที่ติดตั้งใหม่นี้ แนวทางการแก้ปัญหาคือการให้ความรู้พื้นฐานในการทดสอบการใช้งานอินเทอร์เน็ต โดยสอนการใช้คำสั่ง คำสั่งพื้นฐานในระบบปฏิบัติการ FreeBSD เพื่อตรวจสอบระบบคอมพิวเตอร์เครื่องแม่ข่ายและเครือข่ายและสอนวิธีการตั้งค่า Network Connection ของ Local Area Network และ Wireless Lan โดยตั้งค่าให้รับ IP Address แบบอัตโนมัติ

ปัญหาการใช้งานเครื่องแม่ข่ายของผู้แลระบบในอินเทอร์เนตเนื่องจากระบบปฏิบัติการที่ติดตั้งบนเครื่องแม่ข่ายนั้นเป็นระบบปฏิบัติการ FreeBSD ดังนั้น ผู้ดูแลระบบจะเกิดความไม่เคยชินและผู้ดูแลระบบขาดความรู้ในการใช้งานเครื่องแม่ข่าย แนวทางการแก้ปัญหาคือการให้ความรู้พื้นฐานในระบบปฏิบัติการ FreeBSD เช่น การเปิดปิดเครื่องแม่ข่าย การใช้คำสั่ง Shell Script การตั้งค่าคอนฟิก (Configure) เครื่องแม่ข่ายทั้งระบบเพื่อให้สามารถประยุกต์ใช้ได้ทั้งระบบ โดยมีรายการต่อไปนี้

1. ไฟล์วอล์ล (Firewall)
2. การจัดการระบบไอพีภายในองค์กร (NAT)
3. การแจกไอพีอัตโนมัติ (DHCP)
4. การเพิ่มความเร็วการใช้เว็บ (Proxy Server)
5. ระบบฐานข้อมูล (Database Server)
6. เว็บไซท์ (Web Server)
7. อีเมลย์ (Mail Server)
8. การถ่ายโอนแฟ้มข้อมูล (FTP Server) และอื่นทั้งระบบ ฯลฯ

ข้อเสนอแนะในการวิจัยครั้งต่อไป

ข้อจำกัดของระบบที่ได้ผ่านการติดตั้งและทดลองใช้งานจริงที่มหาวิทยาลัยราชภัฏเพชรบูรณ์ สำนักงานสาธารณสุขจังหวัดเพชรบูรณ์ โรงเรียนติ้ววิทยาคมและโรงเรียนผาเมืองวิทยาคม มีข้อเสนอแนะกับผู้ที่จะพัฒนาต่อไปเพื่อจะได้เพิ่มระบบให้มีประสิทธิภาพและประหยัดงบประมาณ ดังนี้

ระบบเก็บข้อมูลพิสูจน์ตัวตน ค้นคืนและระบุตัวตนผู้ใช้บริการอินเทอร์เนต เป็นระบบที่ได้มีการพัฒนาขึ้นสำหรับผู้ให้บริการอินเทอร์เนตที่มีงบประมาณน้อย เพื่อให้องค์กรสามารถใช้ควบคุมผู้ใช้รองรับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในส่วนของการใช้งานอินเทอร์เนต โดยระบบสามารถประยุกต์ให้กับส่วนผู้ให้บริการอื่นๆ ได้อีกหลายองค์กร ได้แก่ โรงแรม โรงเรียน หอพัก ร้านอาหาร ที่มีบริการใช้เครือข่ายไร้สายได้การที่จะใช้ระบบนี้ให้สัมฤทธิ์มากที่สุดผู้ดูแลระบบในอินเทอร์เนตควรที่จะมีความรู้ในระบบปฏิบัติการ FreeBSD เป็นพื้นฐาน คำสั่งโปรแกรมระบบปฏิบัติการ (Command Line) เพื่อที่จะได้สั่งงาน ควบคุม ติดตั้ง และแก้ไขไฟล์ระบบได้รวดเร็วขึ้น

การติดตั้งบนเครื่องพีซีธรรมดา (Personal Computer) สามารถใช้งานได้ดีระดับหนึ่ง เมื่อใช้ไปนานๆ บางครั้งอาจทำให้เครื่องแฮ้งค์ได้ถ้าเครื่องลูกข่ายเข้าใช้งานพร้อมกันมีจำนวนมาก ควรติดตั้งในเครื่องแม่ข่าย (Server) จึงจะได้ผลดีเต็มประสิทธิภาพ ในด้านความเร็วในการประมวลผลและความพึงพอใจของผู้ใช้บริการ

แนวทางการพัฒนาระบบเก็บข้อมูลล็อกไฟล์ การพิสูจน์ตัวตน การค้นคืนและระบุตัวตนผู้ใช้บริการเครือข่ายอินเทอร์เนตต่อนั้น ควรเน้นในเรื่องการจัดทำรายงานและการทำบัญชีผู้ใช้ โดยการทำบัญชีผู้ใช้ให้เป็นแบบฟอร์มที่เป็นระบบสวยงาม และเพิ่มทางเลือกให้กับผู้ดูแลระบบให้สามารถใช้งานได้ง่ายขึ้น เช่น การเก็บข้อมูลแต่ละคนว่ามีการใช้งานแล้ว กี่ครั้ง ใช้ทรัพยากรอินเทอร์เน็ตเท่าไหร่ การจำกัดให้กลุ่มผู้ใช้ใช้งานอินเทอร์เน็ตใช้ทรัพยากรได้เท่าไหร่ เพื่อที่จะได้เป็นเครื่องมือตัวหนึ่งที่ช่วยให้ผู้ดูแลระบบในอินเทอร์เนตมีระบบที่รองรับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และช่วยเจ้าหน้าที่หาตัวผู้กระทำความผิดได้อีกทางหนึ่งได้อย่างรวดเร็วแน่นอนเป็นหลักฐานเอาความผิดกับผู้ใช้บริการที่ไม่ดีได้

บรรณานุกรม

คมสัน คำบรรลือ. **การศึกษาเพื่อเพิ่มประสิทธิภาพระบบเครือข่ายไร้สาย สาขาวิชาระบบสารสนเทศ.** ตาก : มหาวิทยาลัยเทคโนโลยีราชมงคลล้านา, 2551.

ธวัชชัย ชูเหล็ก. **การออกแบบการประกอบระบบปฏิบัติการลินุกซ์.** กรุงเทพมหานคร : มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ , 2550.

ธารทิพย์ ตากเทิดเกียรติ์ . **การพัฒนาระบบพิสูจน์ทราบตัวตนแบบไดนามิกโมดูลผ่าน HyperText transfer protocol.** กรุงเทพมหานคร : มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ , 2549.

ธีระ โชคพระสมบัติ . **การพัฒนาระบบปฏิบัติการแม่ข่ายลีนุกซ์สำหรับระบบบทเรียนบรรยายอิเลคทรอนิกส์.** กรุงเทพมหานคร : มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง , 2550.

นริสสรา ศรีมูลชัย. **การพัฒนาซอฟต์แวร์สำหรับบริหารสิทธิ์การเข้าใช้งานบนระบบเครือข่ายแบบไร้สาย.** กรุงเทพมหานคร : มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ , 2549.

นฤชัย ศรีแสงอยู่. **การพัฒนาโปรแกรมตรวจสอบความปลอดภัยพื้นฐานสำหรับระบบปฏิบัติการ ลีนุกซ์ เรดแฮต.** กรุงเทพมหานคร : จุฬาลงกรณ์มหาวิทยาลัย , 2547

ปรัชญา พันธุ์มี . **การพิสูจน์ตัวตนในระบบเว็บเซอร์วิสด้วยระบบเคอร์เบอรอส.** กรุงเทพมหานคร : มหาวิทยาลัยธรรมศาสตร์ , 2548.

ไพฑูรย์ แย้มเทศ **การศึกษาหาค่าประสิทธิภาพของพีซีเราเตอร์บนระบบปฏิบัติการแบบเปิด.** กรุงเทพมหานคร : มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ , 2548.

ยุทธนา ไชยสัตย์. **การพัฒนาระบบโปรโตคอลพิสูจน์ตัวตนแบบไม่ประสานเวลา สำหรับโปรโตคอล Neuman Stubblebine.** กรุงเทพมหานคร : มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ , 2548.

ศาลทัส พัดฟูทรัพย์ศ์. **การทดสอบความปลอดภัยของระบบเครือข่ายไร้สาย.** กรุงเทพมหานคร : มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ , 2549

สถาบันมาตรวิทยาแห่งชาติ. **เวลามาตรฐาน** : (online) Aviable URL: http://www.nimt.or.th/nimt/service/index.php?menuName=time , 2553.

สัลยุทธ์ สว่างวรรณ. **เครือข่ายคอมพิวเตอร์ COMPUTER NETWORKS.** พิมพลักษณ์ กรุงเทพมหานคร : เพียร์สัน เอ็ดดูเคชั่น อินโดไชน่า , 2547.

สุวัฒน์ บันลือ. **รูปแบบที่เหมาะสมของเครือข่ายคอมพิวเตอร์ไร้สาย สำหรับสถาบันราชภัฏอุบลราชธานี**. อุบลราชธานี: สถาบันราชภัฏอุบลราชธานี , 2548.

โอภาส เอี่ยมสิริวงศ์. **เครือข่ายคอมพิวเตอร์และการสื่อสาร.** พิมพลักษณ์ กรุงเทพมหานคร : บริษัท ซีเอ็ด ยูเคชั่น จำกัด , 2552.

“ The FreeBSD Project ” (online) Aviable URL: (http://www.FreeBSD.org) , public by The FreeBSD Project ,2010

กิตติกรรมประกาศ

ผู้วิจัย ตั้งความหวังไว้ว่าจะให้ซอร์สโค๊ดฟรีกับผู้ที่สนใจต้องการพัฒนาระบบควบคุมการใช้อินเทอร์เนตเกตเวย์ราคาถูกสำหรับมหาวิทยาลัยทุกท่านที่ต้องการศึกษาโปรแกรมประเภทโอเพนซอร์สและงานวิจัยนี้สำเร็จลงได้ด้วยดีเพราะได้รับความร่วมมือเป็นอย่างดียิ่งจากหน่วยงานและบุคคลซึ่งผู้วิจัยต้องขอขอบพระคุณมา ณ โอกาสนี้ ได้แก่

ขอขอบคุณสำนักงานคณะกรรมการการวิจัยแห่งชาติ และสถาบันวิจัยและพัฒนา มหาวิทยาลัย ราชภัฏเพชรบูรณ์ที่ให้การสนับสนุนงบประมาณในการทำวิจัย

ขอขอบคุณบุคลากร เจ้าหน้าที่สำนักวิทยบริการและเทคโนโลยีสารสนเทศ และบุคลากร เจ้าหน้าที่สถาบันวิจัยและพัฒนา มหาวิทยาลัย ราชภัฏเพชรบูรณ์ ที่มีส่วนได้ช่วยให้คำแนะนำและช่วยตรวจสอบเอกสารการวิจัยจนสำเร็จสมบูรณ์

ขอขอบคุณอาจารย์สาขาวิชาวิทยาการคอมพิวเตอร์ สาขาเทคโนโลยีสารสนเทศ สาขาคอมพิวเตอร์ศึกษา คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัย ราชภัฏเพชรบูรณ์ที่มีส่วนได้ช่วยให้คำแนะนำให้ความรู้และช่วยเหลือด้วยดีตลอดมา

ขอขอบคุณผู้เชี่ยวชาญได้แก่ ทีมพัฒนาระบบโอเพนซอร์ส ลีนุกซ์, ทีมพัฒนา FreeBSD Operating System, ทีมพัฒนา EZ Radius, ทีมพัฒนา Dalo Radius, ทีมพัฒนา FreeRadius,ทีมพัฒนา Chillispot, ทีมพัฒนา Authentication มหาวิทยาลัยบูรพาและทีมพัฒนาโอเพนซอร์สอื่นๆ อีกหลายทีมที่ไม่ได้กล่าวถึงเป็นอย่างสูงที่ให้ซอร์สโค๊ดที่มีประโยชน์มากต่อการวิจัยซึ่งได้เผยแพร่ข้อมูลและความรู้ให้สืบค้นผ่านระบบเครือข่ายอินเทอร์เนตที่ผู้วิจัยได้นำมาพัฒนาต่อและประยุกต์ใช้ให้เกิดประโยชน์สูงสุดต่อมหาวิทยาลัยและหน่วยงานอื่นๆ อีกหลายหน่วยงาน

ขอขอบคุณผู้มีอุปการคุณทุกท่าน บิดา มารดา ญาติพี่น้อง ครู อาจารย์ ที่คอยให้คำแนะนำ และให้คำปรึกษา และให้กำลังใจตลอดระยะเวลาการทำวิจัย ให้การทำวิจัยผ่านไปได้ด้วยดี จนผลงานวิจัยเสร็จสมบูรณ์