ระบบควบคุมการใช้งานเครือข่ายภายในห้องเรียนโดยใช้ไฟร์วอลล์

CLASSROOM NETWORK ACCESS CONTROL SYSTEM BY FIREWALL

โดย

โอภาส ปัญญาชัยรักษา

OPART PANYACHAIRUCKSA

อาจารย์ที่ปรึกษา

รศ.ดร.โชติพัชร์ ภรณวลัย

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ภาคเรียนที่ 1 ปีการศึกษา 2549

CLASSROOM NETWORK ACCESS CONTROL SYSTEM

BY FIREWALL

OPART PANYACHAIRUCKSA

A SYSTEM DEVELOPMENT PROJECT

OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY

FACULTY OF INFORMATION TECNOLOGY

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

1/ 2006

หัวข้อ	ระบบควบคุมการใช้งานเครือข่ายในห้องเรียนโดยใช้ไฟร์วอลล์
นักศึกษา	นายโอภาส ปัญญาชัยรักษา
รหัสประจำตัว	47066209
ปริญญา	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
สาขาวิชา	วิทยาการสารสนเทศ
พ.ศ.	2549
อาจารย์ที่ปรึกษา	รศ. ดร. โชติพัชร์ ภรณวลัย

บทคัดย่อ

เนื่องจากในการเรียนการสอนในห้อง LAB นั้น อาจารย์ผู้สอนต้องการให้นักศึกษาสนใจเรียน โดยไม่ต้องการให้นักศึกษาใช้งานระบบเครือข่ายภายนอก (ระบบอินเตอร์เน็ต) หรืออาจจะอนุญาตให้นักศึกษาสามารถใช้งานระบบเครือข่ายภายใน (ระบบอินทราเน็ต) ได้เฉพาะบางคนหรือบางเครื่อง ซึ่งในปัจจุบัน การควบคุมทำได้ยาก จึงได้มีการพัฒนาระบบการควบคุมการใช้งานระบบเครือข่ายภายในห้องเรียนขึ้นมาเพื่ออำนวยความสะดวกให้กับอาจารย์ผู้สอน โดยที่ระบบจะทำงานโดยใช้โปรแกรมคำสั่ง IPFW บนระบบปฏิบัติการ FreeBSD และใช้ภาษา PHP และ Shell Script ในการพัฒนา เพื่อช่วยสนับสนุนให้การเรียนการสอนเป็นไปอย่างมีประสิทธิภาพ

Title	Classroom Network Access Control System by Firewall
Student	Mr. Opart Panyachairucksa
Student ID	47066209
Degree	Master of Science in Information Techology
Programme	Information Science
Year	2006
Advisor	Assoc. Prof. Dr. Chotipat Pornavalai

ABSTRACT

Because of the in the LAB practices, the students need to pay attention to the class. The instructor should control the network usage whether the student can access through the internet or only internal network. The system will facilitate the instructor to controlling the network access. Currently there's no control therefore this project is developed as this purpose. I use many techniques to implement; the IPFIREWALL (IPFW) in FreeBSD, PHP web programming language, UNIX's shell script and also MySQL as the database for managing the efficiency of learning.

กิตติกรรมประกาศ

ในความสำเร็จของโครงการนี้ ผู้เขียนใคร่ขอแสดงความระลึกถึงบุคคลสำคัญผู้อยู่เบื้องหลังดังต่อไปนี้

คุณพ่อ และคุณแม่สำหรับกำลังใจที่เต็มเปี่ยมและทุกสิ่งทุกอย่างจนสามารถมีวันนี้ได้

อาจารย์โชติพัชร์ ภรณวลัย อาจารย์ที่ปรึกษาโครงการ ผู้ให้คำปรึกษา ชี้แนวทาง ให้กำลังใจ และคำแนะนำต่าง ๆ ที่เป็นประโยชน์ยิ่งจนทำให้โครงการนี้สำเร็จลุล่วงไปได้ด้วยดี

เพื่อนๆและพี่ๆ บริษัทเทลินดุส (ไทยแลนด์) จำกัดที่คอยช่วยเหลือเรื่องงานและเรื่องอื่นๆ อีกมากมาย

คุณอลิสา วิรัชมงคลชัย สำหรับกำลังใจ แรงใจและคำปรึกษาในทุกๆ เรื่อง ตลอดมา

คุณอัษฎาวัทน์ เนตรจรัสแสง สำหรับคำปรึกษาที่เยี่ยมยอดเรื่องการเขียนโปรแกรม

และเพื่อน ๆ IS17.2 ที่คอยให้ความช่วยเหลือ ถามไถ่เรื่องราวต่างๆ ไม่ขาดสาย รวมทั้งเป็นแรงใจให้ทำโครงการนี้จนสำเร็จ

โอภาส ปัญญาชัยรักษา

สารบัญ

สารบัญ(ต่อ)

สารบัญตาราง

สารบัญภาพ

สารบัญภาพ(ต่อ)

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในการเรียนการสอนในห้องเรียน LAB ที่มีเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับระบบเครือข่ายอยู่นั้น การเรียนการสอนในบางครั้งอาจไม่มีประสิทธิภาพ เนื่องจากหรือนักศึกษาอาจใช้งานระบบอินเตอร์เน็ต เช่น การท่องเว็บ การสนทนากันโดยโปรแกรมแชทพูดคุยกัน เช็คอีเมล์และอื่นๆ โดยไม่สนใจในเนื้อหาการสอนของอาจารย์ ในปัจจุบันอาจารย์ผู้สอนทำได้แค่เพียงปิดหรือเปิดอุปกรณ์ระบบเครือข่ายภายในห้องเรียน เพื่อควบคุมการเข้างานระบบเครือข่ายซึ่งไม่สะดวก ถ้าหากในบางครั้งอาจารย์ต้องการให้นักศึกษาเข้าใช้งานระบบเครือข่ายภายในเพียงอย่างเดียว หรือจะกำหนดให้เครื่องคอมพิวเตอร์หรือนักศึกษาคนใดสามารถเข้าใช้งานระบบเครือข่ายได้ นักศึกษาคนใดไม่สามารถเข้าใช้งานระบบเครือข่ายได้เป็นต้น จึงจำเป็นต้องมีการเพิ่มระบบควบคุมการใช้งานเครือข่ายภายในห้องเรียนขึ้น เพื่อกำหนดนโยบายตามที่อาจารย์ต้องการ

ในการพัฒนาระบบควบคุมการเข้าใช้งานระบบเครือข่ายนี้ ระบบจะสามารถช่วยในการแก้ปัญหาของอาจารย์ผู้สอนได้บางส่วน โดยจะใช้โปรแกรมไฟร์วอลล์ IPFW ซึ่งมีอยู่บนระบบปฏิบัติการ FreeBSD เข้ามาช่วยในการบริหารและจัดการ แต่โดยทั่วไปแล้วโปรแกรม IPFW ดังกล่าวเป็นโปรแกรมที่ต้องพิมพ์คำสั่งทีละคำสั่งหรือกลุ่มคำสั่งเข้าไปเพื่อให้โปรแกรมทำงานได้ ซึ่งจะมีความยุ่งยากในการจำคำสั่งและการใช้งาน โดยที่โปรแกรมนี้จะไม่มีหน้าจอสำหรับใช้งานในการบริหารจัดการ ทางผู้พัฒนาระบบนี้จึงได้ทำการพัฒนาหน้าจอของการบริหารจัดการของอาจารย์และเจ้าหน้าที่ขึ้น เพื่อที่จะเข้าไปบริหารจัดการการใช้งานระบบเครือข่ายของห้องเรียน LAB ได้ง่ายโดยผ่านหน้าจอเว็บบราวเซอร์โดยผ่านโปรโตคอล Secure-Socket Layer (หรือ SSL) เพื่อความปลอดภัยในการส่งผ่านชื่อผู้ใช้และรหัสผ่านไปยังระบบไฟร์วอลล์นี้ และระบบนี้เป็นระบบที่ถูกพัฒนาขึ้นโดยฟรีแวร์ ทำให้ไม่มีค่าใช้จ่าย จึงสามารถนำไปใช้ในโรงเรียนหรือสถาบันการศึกษาที่ต้องการได้

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

การศึกษาและพัฒนาระบบในครั้งนี้เพื่อจัดทำระบบเพื่อช่วยให้อาจารย์และเจ้าหน้าที่ในการบริหารจัดการ การเข้าใช้งานระบบเครือข่ายของนักศึกษาในห้องเรียน LAB ซึ่งจะมีวัตถุประสงค์ดังต่อไปนี้

1. ออกแบบระบบให้มีความปลอดภัยสูงสุด เพื่อให้สามารถใช้งานได้อย่างมีประสิทธิภาพ
2. ออกแบบฐานข้อมูลให้มีความถูกต้องตรงกับความต้องการของผู้ใช้ให้มากที่สุด เพื่อเพิ่มประสิทธิภาพในการทำงานโดยรวมของระบบ
3. พัฒนาระบบให้เป็นหน้าเว็บ เพื่อที่สามารถรองรับการใช้งานของผู้ใช้ซึ่งคือ เจ้าหน้าที่ดูแลระบบหรืออาจารย์ผู้สอนได้โดยการใช้เว็บบราวเซอร์ ซึ่งทำให้ผู้ใช้งานสามารถที่จะใช้งานระบบได้อย่างสะดวก
4. เพื่อเพิ่มประสิทธิภาพในการเรียนการสอนในห้องเรียน LAB ให้มากขึ้น โดยที่นักศึกษาจะสามารถเข้าใช้งานเครือข่ายได้ตามที่อาจารย์ผู้สอนกำหนดเท่านั้น

1.3 สมมุติฐานของการศึกษา

การศึกษาและการพัฒนาระบบในครั้งนี้นั้น คาดว่าจะประสบความสำเร็จในการพัฒนา เนื่องจากมีเอกสารอ้างอิงและคู่มือจำนวนมากพอสมควรที่สามารถใช้เพื่อประกอบการพัฒนาระบบ โดยที่การพัฒนาให้ระบบมีความปลอดภัยนั้น จะใช้เอกสาร UNIX top 20 security checklist ที่อยู่ในเว็ปไซต์ SANS.ORG และเอกสารจากเว็ปไซต์ DEFCON1.ORG ซึ่งเป็นเว็ปไซต์ที่เกี่ยวข้องกับการรักษาความปลอดภัยของระบบที่มีชื่อเสียง โดยที่ทาง THAICERT นำมาแปลเป็นภาษาไทยไว้ด้วย การพัฒนาระบบควบคุมการใช้งานเครือข่ายภายในห้องเรียนนี้จะใช้ภาษา PHP ในการพัฒนา ซึ่งเป็นภาษาที่เป็นที่นิยม รวมทั้งใช้ระบบฐานข้อมูล MYSQL ที่มีความสามารถสูงถึงแม้จะเป็นฟรีแวร์ แต่อย่างไรก็ตาม ระบบนี้จะมีข้อจำกัดบางประการซึ่งจะได้กล่าวถึงในภายหลังต่อไป

1.4 ทฤษฎีหรือแนวความคิดที่ใช้ในการวิจัย

การศึกษาและพัฒนาระบบควบคุมการใช้งานเครือข่ายในห้องเรียนนี้ จะอาศัยหลักการและทฤษฎีหลายประการ เริ่มตั้งแต่การวิเคราะห์และออกแบบระบบ โดยอาศัยการใช้หลักการการออกแบบฐานข้อมูลโดยใช้แผนภาพความสัมพันธ์ของข้อมูลหรือเอนติที (Entity-Relationship diagram) สำหรับการพัฒนาระบบนั้นจะใช้แบบจำลองแบบน้ำตก (Waterfall Model) ซึ่งเป็นแบบจำลองที่ใช้กันมากมาช่วยในการพัฒนาระบบ รวมทั้งยังต้องใช้หลักการของการทำงานของเครือข่าย TCP และ UDP รวมทั้ง IP ในการศึกษาและพัฒนาด้วย โดยที่เอกสารและข้อมูลส่วนใหญ่สามารถหาได้ในอินเตอร์เน็ต

1.5 ขอบเขตการวิจัย

ระบบที่ได้ทำการพัฒนาขึ้นมานี้ จะมีขอบเขตการทำงานและความสามารถดังต่อไปนี้

1. อาจารย์ผู้สอนสามารถกำหนดให้เครื่องคอมพิวเตอร์เครื่องใดเครื่องหนึ่งหรือกลุ่มของคอมพิวเตอร์หรือเครื่องคอมพิวเตอร์ทั้งหมด สามารถเข้าใช้งานระบบเครือข่ายภายในคณะหรือภายนอกคณะได้บ้าง
2. เครื่องคอมพิวเตอร์จากเครือข่ายอื่นๆ จะไม่สามารถเข้าใช้งานเครือข่ายภายในห้องเรียนในแต่ละห้องได้
3. จะต้องมีการกำหนดให้เครื่องคอมพิวเตอร์ของอาจารย์ในแต่ละห้องเท่านั้นที่จะสามารถเข้าใช้งานระบบนี้ผ่านทางเว็บบราวเซอร์ได้ เพื่อความปลอดภัยของระบบ
4. เจ้าหน้าที่ดูแลระบบ สามารถกำหนดนโยบายการเข้าใช้งานระบบเครือข่ายของห้องเรียน LAB ตามที่อาจารย์ต้องการได้ โดยดูจากตารางการเรียนการสอนที่ทางคณะหรืออาจารย์กำหนดขึ้น
5. ระบบนี้เป็นระบบที่ถูกพัฒนาขึ้นมาเพื่อใช้สำหรับห้องเรียน LAB 5 ห้อง
6. ระบบนี้ถูกพัฒนาขึ้นมาเพื่อรองรับการเรียนการสอนใน 2 ช่วงเวลาคือ ตั้งแต่ 9.00-12.00 และ 13.00-16.00 เท่านั้น
7. ระบบนี้มีผู้ใช้งานเพียง 2 คนคือแต่จะมีเพียง 1 รายชื่อผู้ใช้ซึ่งคือผู้ดูแลระบบ (ผู้ใช้ admin)
8. อาจารย์ผู้ใช้สามารถเข้าสู่ระบบเพื่อเลือกลักษณะของระบบเครือข่ายที่กำหนดไว้ล่วงหน้า หรือสามารถมอบหมายให้ผู้ดูแลระบบเป็นคนกำหนดตารางลักษณะของระบบเครือข่ายไว้ล่วงหน้าก่อนถึงเวลาการเรียนการสอนได้

แต่ระบบที่ได้ทำการพัฒนาขึ้นมานี้ จะมีไม่ครอบคลุมไปถึงหน้าที่การทำงานดังต่อไปนี้

1. ระบบที่พัฒนาขึ้นเป็นเพียงระบบที่ถูกจำลองขึ้นเท่านั้น ดังนั้นอาจทำให้การทำงานของระบบโดยรวมไม่ดีมากนัก เพราะพัฒนาอยู่บนเครื่องโน้ตบุ๊คที่มีประสิทธิภาพไม่สูง
2. ระบบที่ถูกพัฒนาขึ้นนี้จะรองรับห้องเรียน LAB ที่มีเครื่องคอมพิวเตอร์ห้องละไม่เกิน 252 เครื่องเท่านั้น
3. เนื่องจากระบบที่ถูกพัฒนาขึ้นเพื่อจำลองการทำงานภายในระบบเครือข่ายภายใน ดังนั้นความสัมพันธ์ระหว่าง interface จึงเป็นแบบ routed mode เท่านั้น ไม่มีการทำการเปลี่ยนแปลงหมายเลข ip address (ไม่มีการทำ NAT)
4. ระบบที่พัฒนาขึ้นจะตั้งอยู่บนสภาพแวดล้อมที่ผู้ดูแลระบบเป็นผู้กำหนดหมายเลข ip address เองเท่านั้น (อยู่ในสภาพแวดล้อมแบบคงที่ หรือ static) ไม่สามารถนำไปใช้กับสภาพแวดล้อมที่เครื่องแม่ข่ายเป็นผู้แจกหมายเลข ip address ได้ (อยู่ในสภาพแวดล้อมที่ไม่คงที่ หรือ dynamic)

1.6 ขั้นตอนของการศึกษา

ขั้นตอนในการการพัฒนาระบบงานจะประกอบด้วยขั้นตอนดังต่อไปนี้

1. เก็บรวบรวมข้อมูลที่จำเป็นในการที่จะทำการพัฒนาระบบ
2. ศึกษารายละเอียดของการพัฒนาเว็บแอพพลิเคชั่น
3. วิเคราะห์และออกแบบระบบควบคุมการใช้งานเครือข่ายในห้องเรียนด้วยไฟร์วอลล์ให้อยู่ในรูปแบบของเว็บแอพพลิเคชั่น
4. พัฒนาระบบควบคุมการใช้งานเครือข่ายในห้องเรียนด้วยไฟร์วอลล์
5. ทดสอบการใช้งานและปรับปรุงแก้ไขระบบที่พัฒนาแล้ว
6. สรุปผลการทดสอบจากการใช้งานที่เกิดขึ้น
7. จัดทำเอกสารคู่มือระบบ

บทที่ 2
ทฤษฎีและหลักการที่ใช้ในการพัฒนาระบบงาน

ในบทนี้จะกล่าวถึงทฤษฎีและหลักการต่าง ๆ รวมทั้งเครื่องมือที่ใช้ในการพัฒนาระบบงาน ซึ่งการพัฒนานั้นจะอยู่บนพื้นฐานของเว็บแอพพลิเคชั่น โดยทฤษฎีที่เกี่ยวข้องรวมทั้งรายละเอียดของโปรแกรมและเครื่องมือต่าง ๆ ที่ใช้ในการพัฒนาระบบงานมีดังต่อไปนี้

2.1 ทฤษฎีวงจรการพัฒนาระบบ

วงจรการพัฒนาระบบ (Systems Development Life Cycle: SDLC) เป็นเทคนิคการวิเคราะห์ระบบเชิงโครงสร้างลักษณะหนึ่ง เพื่อเตรียมการวางแผนและจัดการกระบวนการในการพัฒนาระบบอย่างเป็นขั้นเป็นตอน โดยแบ่งออกเป็น 5 ขั้นตอนดังนี้ (กิตติมา เจริญหิรัญ. 2546: 18)

1. การวางแผนระบบ คือ ขั้นตอนในการศึกษาปัญหาการทำงานของระบบเดิม กำหนดขอบเขตความต้องการของระบบ จัดทำแผนการดำเนินงานและประมาณระยะเวลารวมถึงงบประมาณ โดยการสำรวจเบื้องต้น หรืออาจเรียกว่าเป็นขั้นตอนในการศึกษาความเป็นไปได้ที่จะทำการพัฒนาระบบ ซึ่งเป็นขั้นตอนที่สำคัญเพราะจะมีผลกระทบต่อเนื่องกับกระบวนการพัฒนาระบบทั้งหมดต่อไปในอนาคต

2. การวิเคราะห์ระบบ คือ การทำความเข้าใจความต้องการขององค์กรและกำหนดรูปแบบความต้องการ ให้คำจำกัดความและบรรยายถึงการประมวลผล รวมถึงการสร้างแบบจำลองต่างๆ เพื่อใช้เป็นแนวทางในการพัฒนาระบบโดยสามารถเลือกใช้ได้หลายแบบจากเครื่องมือในการสร้างแบบจำลองต่างๆ

3. การออกแบบระบบ คือ การสร้างพิมพ์เขียวของระบบใหม่ขึ้นมาตามความต้องการของผู้ใช้ ทั้งนี้ไม่ว่าจะเป็นการพัฒนาระบบขึ้นมาใช้เองหรือการสั่งซื้อโปรแกรมสำเร็จรูปก็ตาม ในการออกแบบจำเป็นต้องกำหนดสิ่งที่จำเป็น เช่น อินพุต เอาท์พุต ส่วนต่อประสานงานผู้ใช้ และการประมวลผล เพื่อประกันความน่าเชื่อถือและความถูกต้องแม่นยำ การบำรุงรักษาได้ และความปลอดภัยของระบบ

4. การทำให้ระบบเกิดผล คือ การพัฒนาระบบงานใหม่ขึ้นมาตามที่ได้ทำการออกแบบไว้โดยจะประกอบด้วยหลายขั้นตอนคือ การเขียนโปรแกรม การทดสอบ การแก้ไขการทำงานที่ผิดพลาดของโปรแกรม การจัดทำเอกสาร การนำระบบไปติดตั้งเพื่อใช้งานจริง การจัดฝึกอบรมผู้ใช้ การประเมินผลระบบ โดยมีวัตถุประสงค์ในการที่จะส่งมอบระบบสาร สนเทศที่สามารถปฏิบัติงานได้อย่างสมบูรณ์พร้อมเอกสารระบบงาน

5. <u>การปฏิบัติงานและสนับสนุนระบบ</u> คือ การดูแลรักษาและเสริมสร้างระบบ โดยการดูแลรักษาคือการแก้ไขข้อผิดพลาดของระบบเมื่อนำไปใช้งานจริง และการปรับเปลี่ยนตามสภาพแวดล้อมของระบบ ส่วนการเสริมสร้างคือการเพิ่มลักษณะเฉพาะใหม่ๆ และสิ่งที่จะเป็นประโยชน์กับระบบ โดยมีวัตถุประสงค์ที่จะคืนผลของการลงทุนทางเทคโนโลยีให้มากที่สุด ระบบที่ออกแบบเป็นอย่างดีจะมีความเชื่อถือได้ สามารถบำรุงรักษาได้ง่าย และสามารถปรับเปลี่ยนขนาดตามความเหมาะสมได้

โดยวงจรการพัฒนาระบบแบบนี้จัดเป็นแนวคิดของการพัฒนาระบบแบบน้ำตก (Water Fall Model) คือเปรียบเสมือนน้ำตกไหลจากที่สูงลงสู่ที่ต่ำ โดยแต่ละขั้นตอนจะอาศัยผลลัพธ์ของการทำงานในขั้นตอนก่อนหน้า แต่การพัฒนาระบบจริงกระบวนการพัฒนาระบบจะไม่คงที่ และสามารถเกิดการเปลี่ยนแปลงได้เสมอ จึงต้องปรับให้มีความยืดหยุ่นเพิ่มขึ้นสามารถควบคุมความเปลี่ยนแปลงที่เกิดขึ้นให้ส่งผลกระทบต่องานที่ทำไปแล้วให้น้อยที่สุด

2.2 แผนภาพการไหลของข้อมูล

แผนภาพการไหลของข้อมูล (Data Flow Diagram) เป็นเครื่องมือที่ใช้ในการพัฒนาระบบและออกแบบระบบงาน โดยการเขียนแผนภาพที่แสดงถึงการไหลของข้อมูลต่าง ๆ ในระบบ รวมทั้งความสัมพันธ์ระหว่างโปรเซสกับข้อมูลที่เกี่ยวข้อง โดยข้อมูลในแผนภาพนั้น จะทำให้ทราบถึงรายละเอียดว่า ข้อมูลมาจากที่ใด ข้อมูลไปที่ใด และข้อมูลถูกจัดเก็บไว้ที่ใด ซึ่งแผนภาพกระแสข้อมูลจะแสดงให้เห็นถึงภาพรวมของระบบทั้งหมด สำหรับขั้นตอนของการวิเคราะห์เพื่อสร้างแผนภาพการไหลของข้อมูลมีดังนี้ (โอภาส เอี่ยมสิริวงศ์. 2545:55)

1. ศึกษารูปแบบการทำงานในลักษณะกายภาพของระบบงานเดิม
2. ดำเนินการวิเคราะห์เพื่อได้แบบจำลองเชิงตรรกะของระบบงานเดิม
3. เพิ่มเติมการทำงานใหม่ หรือปรับปรุงสิ่งที่ต้องการในแบบจำลองเชิงตรรกะ
4. พัฒนาระบบงานใหม่ในรูปแบบทางกายภาพ

2.3 โปรโตคอลทีซีพี

โปรโตคอล TCP (ย่อมาจาก Transmission Control Protocol) เป็นโปรโตคอลที่มีการรับส่งข้อมูลแบบ Stream oriented protocol หมายความว่า การรับส่งข้อมูลจะไม่คำนึงถึงปริมาณข้อมูลที่จะส่งไป แต่จะแบ่งข้อมูลเป็นส่วนย่อยๆก่อน แล้วจึงจะส่งไปยังปลายทางอย่างต่อเนื่องเป็นลำดับข้อมูล ในกรณีที่ข้อมูลส่วนใดส่วนหนึ่งสูญหายไป ก็จะส่งข้อมูลส่วนนั้นใหม่อีกครั้ง สำหรับปลายทางก็จะทำหน้าที่จัดเรียงส่วนของข้อมูลดาตาแกรมใหม่ให้ต่อเนื่องและประกอบกลับเป็นข้อมูลทั้งหมดได้ ซึ่งจะแยกข้อมูลส่วนที่ไม่ถูกต้องออก ดังนั้นแอพพลิเคชั่นหรือโปรเซสใดที่อาศัยการส่งผ่านข้อมูลโดยการใช้โปรโตคอลทีซีพี จะต้องใช้หน่วยความจำและขนาดของช่องสัญญาณ (bandwidth) มากกว่าโปรโตคอลยูดีพี

การติดต่อระหว่างกันจะต้องเป็นแบบ connection-oriented คือต้องมีการสร้างติดต่อกันเป็น session ทั้ง 2 ด้านเสียก่อน แล้วจึงจะรับส่งข้อมูลไปได้พร้อมกัน (full duplex) เหมือนกับการใช้โทรศัพท์ติดต่อกัน เมื่อผู้ติดต่อต้นทางเรียกให้ฝ่ายตรงข้ามรับสายแล้วจึงเริ่มการสนทนา เช่น พูดคำว่า "สวัสดี" หรือ "ฮัลโหล" กันก่อนเพื่อให้แน่ใจว่าฝ่ายตรงข้ามพร้อมจะติดต่อด้วย จากนั้นจึงเริ่มต้นสนทนากัน และเมื่อต้องการจะเลิกการติดต่อก็จะมีการพูดคำว่า "สวัสดี" ให้ฝ่ายตรงข้ามทราบว่าจะเลิกการติดต่อและวางสายไป ซึ่งในระหว่างการติดต่อกันนั้น แม้ว่าฝ่ายหนึ่งฝ่ายใดหรือทั้งสองฝ่ายจะเงียบไป คือไม่พูดอะไรเป็นเวลานานๆ แต่การเชื่อมโยงระหว่างสองด้านยังมีอยู่ไม่ขาดไปจนกว่าฝ่ายหนึ่งฝ่ายใดจะวางสาย เช่นเดียวกับการติดต่อกันด้วยโปรโตคอลทีซีพี เมื่อแอพพลิเคชั่นต้องการส่งผ่านข้อมูลจะใช้โปรโตคอลที่เหมาะสมในชั้น Application layer ติดต่อไปและมีการสร้างช่องส่งข้อมูลผ่านพอร์ตที่กำหนดเพื่อส่งผ่านข้อมูลไปยังโปรโตคอลทีซีพี

ในระหว่างการรับส่งข้อมูลนี้ โปรโตคอลทีซีพีจะเพิ่มกระบวนการตรวจสอบข้อมูลเพื่อให้ข้อมูลมีความถูกต้องไม่ผิดพลาดไปจากเดิม โดยที่จะมีการส่งสัญญาณตรวจสอบข้อมูล (acknowledgement) และส่งข้อมูลไปให้อีกครั้ง ถ้าปลายทางไม่ได้รับหรือข้อมูลเกิดความผิดพลาด

ความน่าเชื่อถือของการส่งผ่านข้อมูลโดยโปรโตคอลทีซีพีจะมีมากกว่า แต่ก็ต้องอาศัยทรัพยากรของระบบมากกว่าในการทำงานเช่นกัน

2.4 โปรโตคอลยูดีพี

ในชั้น host-to-host layer นอกจากจะมีโปรโตคอลทีซีพีทำงานแล้ว ก็ยังมีโปรโตคอลยูดีพี (ย่อมาจาก User Datagram Protocol) ที่มีคุณสมบัติแตกต่างกันอยู่ด้วย ในการรับส่งข้อมูลผ่านโปรโตคอลยูดีพี จะเป็นแบบที่ทั้งสองด้านไม่จำเป็นต้องอาศัยการสร้างช่องทางเชื่อมต่อกัน (connectionless) ระหว่างเครื่องเซิร์ฟเวอร์ที่ให้บริการกับเครื่องที่ขอใช้บริการ โดยไม่ต้องแจ้งให้ฝ่ายรับข้อมูลเตรียมรับข้อมูลเหมือนโปรโตคอลทีซีพี และไม่มีการตรวจสอบความถูกต้องครบถ้วนในการรับส่งข้อมูลนั้นๆด้วย เนื่องจากโปรโตคอลยูดีพีไม่มีกลไกในการตรวจสอบข้อมูลในการรับส่งข้อมูลแต่ละครั้ง และไม่มีการส่งข้อมูลใหม่อีกในกรณีที่เกิดความผิดพลาดของการส่งข้อมูล เมื่อเป็นเช่นนี้แอพพลิเคชั่นหรือโปรเซสใดที่ต้องอาศัยโปรโตคอลยูดีพีในการส่งผ่านข้อมูลก็อาจจะต้องสร้างกระบวนการตรวจสอบข้อมูลขึ้นมาเอง

ตัวอย่างของแอพพลิเคชั่นหรือโปรโตคอลที่ใช้บริการของโปรโตคอลยูดีพีเช่น โปรโตคอล SNMP (ใช้ควบคุมและจัดการอุปกรณ์เครือข่าย) และโปรโตคอล DHCP (ใช้สำหรับส่งพารามิเตอร์ของเครือข่ายให้กับเครื่องลูกข่าย) การส่งข้อมูลเหล่านี้ไม่จำเป็นต้องรับทราบหรือตรวจสอบว่าข้อมูลไปถึงปลายทางถูกต้องหรือไม่ แต่กลไกการตรวจสอบข้อมูลที่มีการรับส่งจะไปทำในขั้นตอนของโปรโตคอลในชั้นที่สูงกว่าแทน (เช่นในชั้นของ Application layer)

ตัวอย่างขั้นตอนกลไกการทำงานโดยใช้โปรโตคอลยูดีพี มีดังต่อไปนี้

1. ใน Application layer เมื่อโปรแกรมควบคุมอุปกรณ์เครือข่าย เช่น โปรแกรม Network Management ตัวหนึ่งต้องการส่งข้อมูลไปยังอุปกรณ์ที่ต้องการแอพพลิเคชั่นนั้นจะติดต่อผ่านโปรโตคอล SNMP ในชั้น Application layer
2. โปรโตคอล SNMP จะติดต่อกับโปรโตคอลยูดีพีที่อยู่ในชั้นถัดไป เพื่อขอติดต่อผ่านพอร์ตที่กำหนด
3. โปรโตคอล SNMP เตรียมข้อมูลที่จะส่ง รวมทั้งที่อยู่ปลายทาง
4. โปรโตคอล SNMP ส่งผ่านข้อมูลให้โปรโตคอลยูดีพีที่อยู่ในชั้นต่ำกว่า
5. โปรโตคอลยูดีพีจะทำหน้าที่ในการผนึกข้อมูลไปให้กับโปรโตคอลไอพีในชั้นถัดลงไปเพื่อส่งข้อมูลออกไป

ซึ่งจะเห็นได้ว่ามีกลไกที่ต่างจากการส่งข้อมูลด้วยโปรโตคอลทีซีพี ซึ่งจะต้องมีการติดต่อกันก่อนและทั้งสองฝ่ายรับทราบการรับส่งข้อมูลของช่องทางการส่งข้อมูลนั้น

2.5 โปรแกรม IPFIREWALL หรือ IPFW

IPFIREWALL หรือ IPFW นั้นเป็นโปรแกรมพื้นฐานที่มากับระบบปฏิบัติการ FreeBSD โดยที่ผู้ที่พัฒนาระบบปฏิบัติการ FreeBSD เป็นผู้พัฒนาขึ้น โดยมีการใช้งานที่ง่ายโดยอาศัยหลักการสร้างกฎแบบง่ายๆ

โปรแกรม IPFW นั้นประกอบไปด้วยส่วนประกอบทั้งหมด 7 ส่วนคือ

1. Kernel firewall filter rule processor and integrated packet accounting facility
2. The logging facility
3. The 'divert' rule which triggers the NAT facility and the advanced special purpose facility
4. The dummynet traffic shaper facility
5. The 'fwd rule' forward facility
6. The bridge facility
7. The ipstealth facility

2.5.1 การเรียกใช้งาน IPFW

ถ้าต้องการจะเรียกใช้โปรแกรม IPFW นั้น เพียงเพิ่มคำสั่ง firewall_enable="YES" ในไฟล์ /etc/rc.conf เท่านั้นเพราะโปรแกรม IPFW เป็นโปรแกรมพื้นฐานที่มากับระบบปฏิบัติการ FreeBSD อยู่แล้ว แต่ถ้าเรียกใช้แบบนี้จะไม่สามารถใช้ฟังก์ชั่นการทำงานของ Network Address Translation (NAT) ได้ ต้องมีการคอมไพล์ kernel ของ FreeBSD ใหม่

หลังจากเมื่อมีการเรียกใช้ตามคำสั่งข้างต้นแล้ว เมื่อเปิดเครื่องใหม่ขึ้นมา จะมีข้อความบอกว่า "ipfw2 initialized, divert disabled, rule-based forwarding disable, default to deny, logging disable" หมายความโมดูลอื่นๆ เช่นการทำ logging จะไม่มี เราสามารถเพิ่มได้โดยการเพิ่มคำสั่ง 2 บรรทัดลงในไฟล์ /etc/sysctl.conf ดังนี้

net.inet.ip.fw.verbose=1

net.inet.ip.fw.verbose_limit=5

2.5.2 ตัวเลือกหากต้องการคอมไพล์ kernel ใหม่

ถ้าหากต้องการใช้ฟังก์ชั่น NAT สำหรับโปรแกรม IPFW นั้น จำเป็นต้องเพิ่มคำสั่งบางคำสั่งลงในไฟล์ kernel ดังต่อไปนี้

options IPFIREWALL

หมายถึงการฝัง IPFIREWALL ลงใน kernel

options IPFIREWALL_VERBOSE

หมายถึงการให้มีการใช้งาน logging

options IPFIREWALL_VERBOSE_LIMIT=5

หมายถึงการจำกัดจำนวน packet/second ของ logging ให้เป็น 5 ถ้าหากมีค่ามากเกินไปอาจทำให้ SYSLOG Server ล่มได้

options IPFIREWALL_DEFAULT_TO_ACCEPT

หมายถึงการกำหนดให้ IPFIREWALL ยอมให้ packet ทั้งหมดผ่านไป โดยไม่จำเป็นต้องแก้ไขค่าใดๆ (โดยปกติ IPFIREWALL จะปฏิเสธ packet ทั้งหมด)

options IPDIVERT

หมายถึงการเรียกใช้ฟังก์ชั่น NAT บน IPFIREWALL

2.5.3 คำสั่งโดยทั่วไปของ IPFW

โดยปกติถ้าหากใช้คำสั่ง IPFW ในการสร้างเงื่อนไขของการอนุญาตหรือปฏิเสธ packet ใดๆ นั้น จะมีผลจนกระทั่งเครื่องที่รัน IPFW ต้องปิดไปหรือเสียหายไป แต่ถ้าหากเครื่องนั้นสามารถกลับมาทำงานได้อีกครั้ง เงื่อนไขต่างๆ ที่เคยสร้างไว้จะสูญหายไปด้วย ดังนั้นเราจึงจำเป็นต้องสร้างไฟล์ขึ้นมาเพื่อเก็บกฎเหล่านั้นไว้ และทำการโหลดไฟล์นี้เมื่อเปิดเครื่อง

คำสั่งของ IPFW นั้นมีประโยชน์มากในการเรียกดูกฎต่างๆ ที่มีผลบังคับใช้งานอยู่ในขณะนั้นๆ หรือ สามารถใช้เครื่องมือที่จะสามารถบอกได้ว่า packet ต่างๆ ที่วิ่งผ่านเข้าออกนั้น เข้ากับกฎข้อไหนบ้างหรือไม่ เป็นจำนวนเท่าใด โดยการใช้คำสั่งดังต่อไปนี้

ipfw list

หมายถึงการเรียกดูข้อมูลของกฎทั้งหมด

ipfw –t list

หมายถึงการเรียกดูข้อมูลของกฎที่มีข้อมูลเวลาอยู่ด้วย

ipfw –a list

หมายถึงการเรียกดูข้อมูลการนับจำนวน packet ที่ผ่านเข้าออกว่าเข้ากับกฎข้อไหนเป็นจำนวนเท่าใด

ipfw –d list

หมายถึงการเรียกดูกฎ dynamic ในปัจจุบัน

ipfw –d –e list

หมายถึงการเรียกดูกฎ dynamic ที่หมดอายุการใช้งานไปแล้ว

ipfw zero

หมายถึงการล้างการนับจำนวน packet ของกฎทั้งหมด

ipfw zero NUM

หมายถึงการล้างการนับจำนวน packet ของกฎที่ชื่อว่า “NUM”

2.5.4 ตัวอย่างกฎของ IPFW

1. This one disallows any connection from the entire crackers network to my host
   ipfw add deny ip from 123.45.67.0/24 to my.host.org
2. A first and efficient way to limit access (not using dynamic rules) is the use of the following rules:
   ipfw add allow tcp from any to any established
   ipfw add allow tcp from net1 portlist1 to net2 portlist2 setup
   ipfw add allow tcp from net1 portlist1 to net2 portlist2 setup
   …
   ipfw add deny tcp from any to any

2.6 MySQL

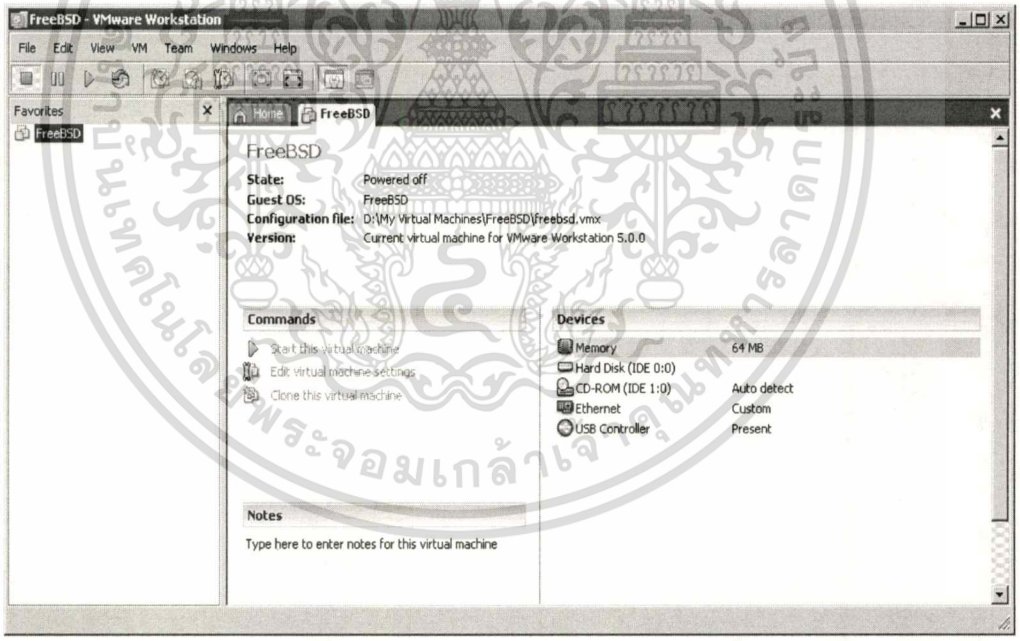
MySQL จัดเป็นระบบจัดการฐานข้อมูลเชิงสัมพันธ์ (หรือที่เรียกว่า RDBMS) ตัวหนึ่งซึ่งเป็นที่นิยมมากในปัจจุบัน เพราะว่าเป็นฟรีแวร์ทางด้านฐานข้อมูลซึ่งมีประสิทธิภาพสูง เป็นทางเลือกใหม่ของผลิตภัณฑ์ระบบจัดการฐานข้อมูลในปัจจุบัน นักพัฒนาระบบฐานข้อมูลที่เคยใช้ MySQL ต่างยอมรับในความสามารถ ความเร็ว การรองรับจำนวนผู้ใช้ และขนาดของข้อมูลจำนวนมหาศาล ทั้งยังสนับสนุนการใช้งานบนระบบปฏิบัติการมากมาย ไม่ว่าจะเป็น UNIX หรือ OS/2 หรือ Linux และ Microsoft Windows นอกจากนี้ยังสามารถใช้งานร่วมกับภาษาที่ใช้ในการพัฒนาระบบเว็บแอพพลิเคชั่นทั้งหลาย เช่น JAVA Perl PHP TCL หรือ ASP เป็นต้น ดังนั้น MySQL จึงเป็นที่นิยมมากในปัจจุบันและมีแนมโน้มที่จะมีผู้ใช้มากขึ้นในอนาคต (สงกรานต์ ทองสว่าง. 2544: 17)

MySQL จัดเป็น Open-Source Software สามารถดาวน์โหลดได้จากอินเตอร์เน็ต โดยไม่เสียค่าใช้จ่ายใดๆ การแก้ไขก็สามารถทำได้โดยอยู่ภายใต้เงื่อนไข GPL (ย่อมาจาก General Public License: GNU) ซึ่งเป็นข้อกำหนดของซอฟท์แวร์ประเภท Open-Source ส่วนใหญ่

MySQL ได้รับการยอมรับและทดสอบในเรื่องของความเร็วในการใช้งาน โดยจะมีการทดสอบเปรียบเทียบกับผลิตภัณฑ์อื่นอยู่เสมอ มีการพัฒนาอย่างต่อเนื่อง โดยเริ่มตั้งแต่เวอร์ชันแรกๆ ที่ไม่ค่อยมีความสามารถมากนัก จนกระทั่งปัจจุบันมีความสามารถสูงขึ้นมาก เช่น ความสามารถในการใช้งานผู้ใช้ได้หลายคน (Multi-user) มีการออกแบบให้สามารถแตกงานออกเป็นส่วนเพื่อช่วยให้การทำงานเร็วขึ้น (Multi-thread) วิธีและการเชื่อมต่อที่ดีขึ้น การกำหนดสิทธิและการรักษาความปลอดภัยของข้อมูลมีความรัดกุม เชื่อถือได้ เครื่องมือหรือโปรแกรมสนับสนุนมีมากขึ้น นอกจากนี้ยังสามารถใช้ภาษาในการเรียกดูข้อมูล ซึ่งเป็นมาตราฐานได้เช่นกัน

2.7 โปรแกรม VMWARE

โปรแกรม VMWARE เป็นซอฟท์แวร์ที่ถูกพัฒนาขึ้นเพื่อใช้ประโยชน์สำหรับการจำลองการทำงานของระบบปฏิบัติการหลายๆ ระบบให้ทำงานอยู่บนระบบปฏิบัติการของเครื่องที่ใช้พัฒนา (เครื่อง host) ในที่นี้คือระบบปฏิบัติการ Microsoft Windows XP Professional โดยที่มีการจำลองการทำงานของระบบปฏิบัติการ FreeBSD โดยที่มีหน้าจอในการทำงานดังรูป



ภาพที่ 2.1 หน้าจอโปรแกรม VMWARE Workstation

บทที่ 3
การวิเคราะห์ระบบงานในปัจจุบัน

3.1 การศึกษาระบบงานที่ใช้งานในปัจจุบัน

ในปัจจุบัน มักจะไม่ค่อยมีการควบคุมการใช้งานระบบเครือข่ายภายในห้องเรียน เนื่องจากผู้ดูแลระบบไม่สามารถที่จะกำหนดนโยบายให้กับเครื่องคอมพิวเตอร์ทุกๆ เครื่องได้ โดยส่วนใหญ่จะใช้การควบคุมในระดับภาพรวม แต่ไม่ค่อยมีประสิทธิภาพมากนัก เพราะในองค์กรหรือสถานศึกษาโดยทั่วไปจะมีไฟร์วอลล์เพียงตัวเดียวหรือไม่มีเลย จึงทำให้การกำหนดนโยบายต่างๆ ต้องกำหนดเป็นเครือข่ายขนาดใหญ่และทำให้ไม่สามารถกำหนดนโยบายตามห้องเรียนหรือเครื่องคอมพิวเตอร์แต่ละเครื่องได้ และไม่สามารถกำหนดนโยบายล่วงหน้าสำหรับห้องเรียนในแต่ละห้องได้ หรือถ้าหากอาจารย์หรือผู้สอนไม่ต้องการให้นักเรียนหรือนักศึกษาเข้าใช้งานระบบเครือข่าย จะทำได้เพียงแค่การปิดอุปกรณ์ระบบเครือข่ายเท่านั้น ซึ่งเป็นวิธีการที่ไม่เหมาะสมนัก

3.2 ปัญหาที่พบในระบบปัจจุบัน

ปัญหาที่พบในการใช้งานปัจจุบันนั้น ถ้าหากองค์กรหรือสถานศึกษานั้นๆ ไม่มีไฟร์วอลล์ที่ใช้ในการควบคุมการใช้งานของผู้ใช้ภายใน จะมีปัญหาเช่นผู้ใช้จากภายนอกอาจจะเข้ามาใช้งานเครือข่ายภายในได้ อาจทำให้ข้อมูลรั่วไหลออกไปยังภายนอก หรืออาจโดนโจมตีทำให้เครื่องไม่สามารถทำงานต่อไปได้ และทำให้ไม่สามารถควบคุมพฤติกรรมการใช้งานระบบเครือข่ายได้เลย แต่ถ้าหากองค์กรหรือสถานศึกษาใดๆ มีการใช้งานไฟร์วอลล์อยู่เพียงตัวเดียว จะทำให้การใช้งานดีขึ้นในระดับหนึ่ง แต่จะไม่สามารถควบคุมการใช้งานภายในระบบเครือข่าย เช่นระหว่างห้องเรียนหรือห้องปฏิบัติการ และถ้าหากระบบเครือข่ายขององค์กรหรือสถานศึกษานั้นๆ มีขนาดใหญ่ จะทำให้การควบคุมเป็นไปได้ยาก และไม่คล่องตัว แต่ถ้าหากมีไฟร์วอลล์ตัวที่สองเพิ่มมา จะช่วยให้ประสิทธิภาพโดยรวมของระบบดีขึ้น

บทที่ 4

การออกแบบระบบงาน

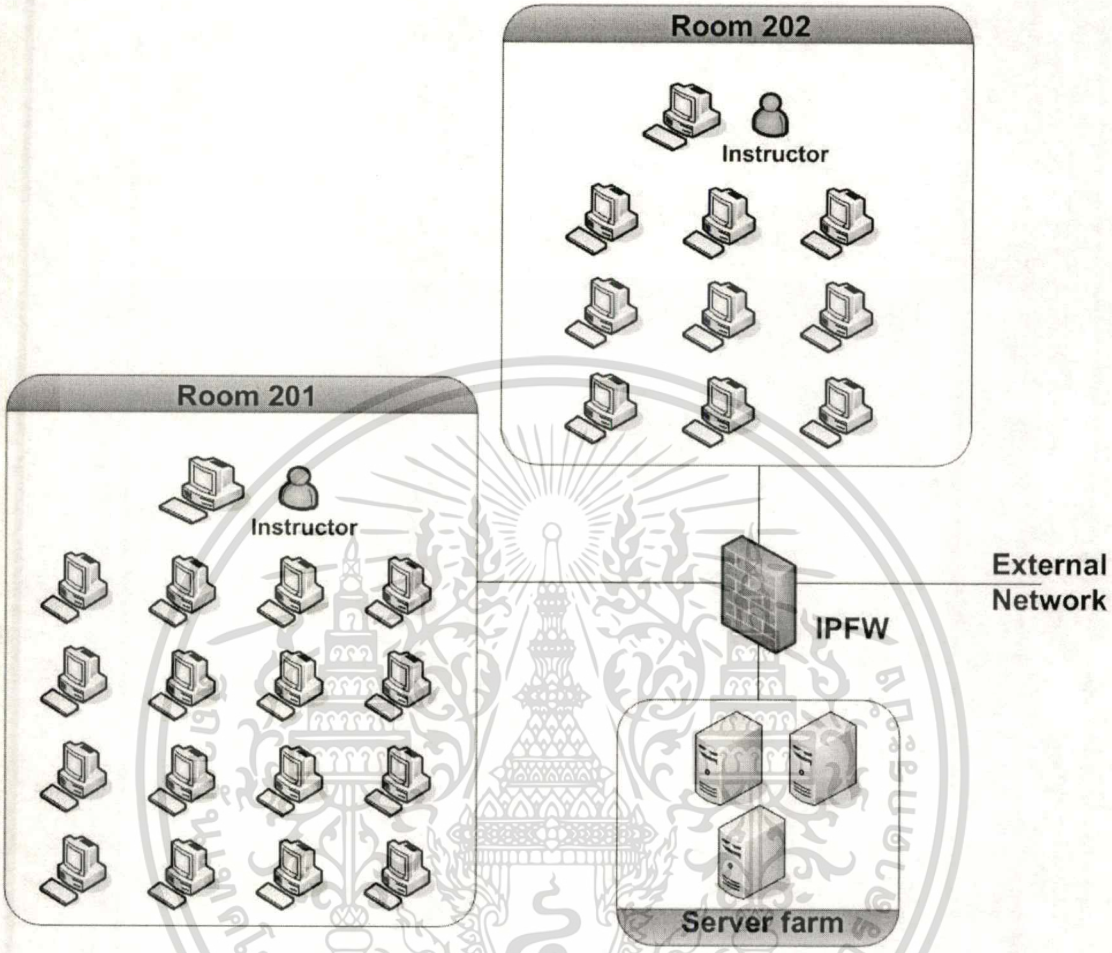
ในบทนี้จะกล่าวถึงการออกแบบระบบควบคุมการใช้งานเครือข่ายในห้องเรียนโดยใช้ไฟร์วอลล์ ซึ่งในการออกแบบจะเน้นถึงความต้องการของผู้ใช้เป็นหลัก โดยเริ่มจากการศึกษาความต้องการและขอบเขตของระบบงาน ส่วนประกอบของระบบงาน โดยแสดงรายละเอียดของขั้นตอนการทำงานจากการหาความสัมพันธ์ของระบบงานกับผู้เกี่ยวข้องในการทำงาน โดยจะแสดงด้วยคอนเท็กซ์ไดอะแกรม และแสดงขั้นตอนการทำงานและการไหลเวียนของข้อมูลด้วยดาต้าโฟล์วไดอะแกรม จากนั้นจึงทำการออกแบบพจนานุกรมข้อมูลของข้อมูลภายในฐานข้อมูลที่พัฒนาขึ้น

3.1 ความต้องการของระบบ

ระบบควบคุมการใช้งานเครือข่ายในห้องเรียนโดยใช้ไฟร์วอลล์ จะมีการออกแบบให้ตรงกับความต้องการของผู้ใช้ ซึ่งมีรายละเอียดดังต่อไปนี้

- ระบบดังกล่าวจะทำงานบนระบบปฏิบัติการ FreeBSD ซึ่งจะมีการติดตั้งซอฟท์แวร์ Apache Web Server และฐานข้อมูล MySQL โดยใช้ภาษา PHP ในการพัฒนาระบบ
- ระบบจะต้องใช้งานง่าย ไม่ซับซ้อน ผู้ใช้สามารถใช้งานระบบได้ง่าย
- ระบบจะสามารถรับเงื่อนไขที่ผู้ใช้เป็นผู้เลือก แล้วระบบจะแปลงให้เป็น Script ของคำสั่ง IPFW เพื่อใช้ในการสร้างกฎ และจะทำการบันทึกลงฐานข้อมูล
- ระบบจะต้องรองรับการลบกฎออกทีละกฎ หรือหลายๆ กฎได้
- ระบบจะต้องนำ Log จากโปรแกรม IPFW มาแสดงได้
- ระบบที่ถูกพัฒนาขึ้นจะต้องมีความปลอดภัย โดยที่จะต้องทำงานผ่าน Protocol HTTPS โดยอาศัย SSL (หรือ Secure Socket Layer) บน Apache Web Server
- ระบบจะต้องให้ผู้ใช้กำหนดได้ว่า คอมพิวเตอร์เครื่องใดสามารถเข้าใช้งานระบบเครือข่ายได้บ้าง โดยสามารถระบุได้ว่าให้เข้าใช้งานเฉพาะเครือข่ายภายในคณะ หรือเข้าใช้งานเครือข่ายภายนอกได้

ในระบบควบคุมการใช้งานเครือข่ายในห้องเรียนโดยใช้ไฟร์วอลล์นั้นจะอาศัยการออกแบบระบบอยู่บนพื้นฐานของแผนภาพในภาพที่ 3.1



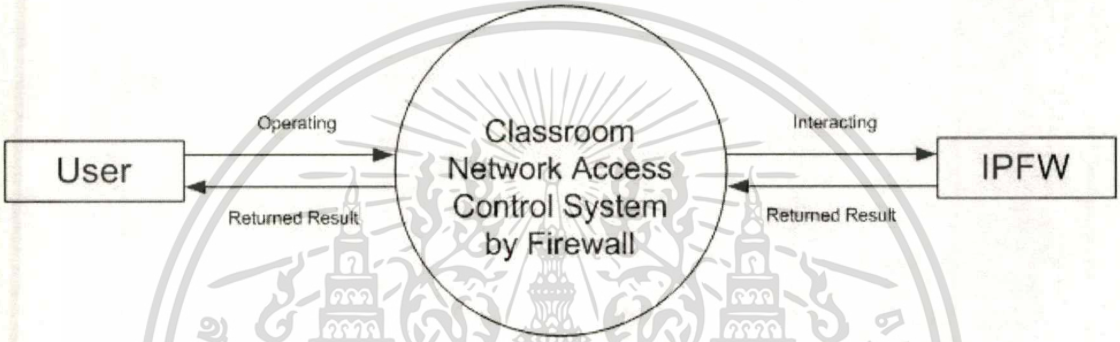
ภาพที่ 3.1 Network diagram ของระบบควบคุมการใช้งานเครือข่ายในห้องเรียนโดยใช้ไฟร์วอลล์

3.2 การออกแบบการทำงานของระบบโดยการจำลองแบบกระบวนการ

ในการออกแบบระบบงานของระบบนี้ จะทำได้โดยการพิจารณาจากส่วนประกอบของระบบงานมาสรุปเป็นคอนเท็กซ์ไดอะแกรม แผนภาพการไหลของข้อมูล และพจนานุกรมของข้อมูล

3.2.1 คอนเท็กซ์ไดอะแกรม

คอนเท็กซ์ไดอะแกรม จะแสดงให้เห็นถึงภาพรวมทั้งหมดของระบบงาน โดยจะแสดงให้เห็นถึงสิ่งที่อยู่ภายนอกระบบ ซึ่งเกี่ยวกับระบบควบคุมการใช้งานเครือข่ายในห้องเรียนโดยใช้ไฟร์วอลล์ ซึ่งสามารถแสดงได้ดังนี้



ภาพที่ 3.2 คอนเท็กซ์ไดอะแกรมของระบบ

จากภาพคอนเท็กซ์ไดอะแกรมของระบบ แสดงให้เห็นถึงการทำงานโดยรวมของระบบว่าประกอบด้วยเอนทิตีใดบ้าง และมีการแลกเปลี่ยนข้อความอะไรกันบ้างดังนี้

เอนทิตี User

เป็นผู้ใช้งานระบบ มีหน้าที่กำหนดนโยบายให้กับระบบ หรือเรียกดูข้อมูลต่างๆ ของระบบ

เอนทิตี Classroom Network Access Control System

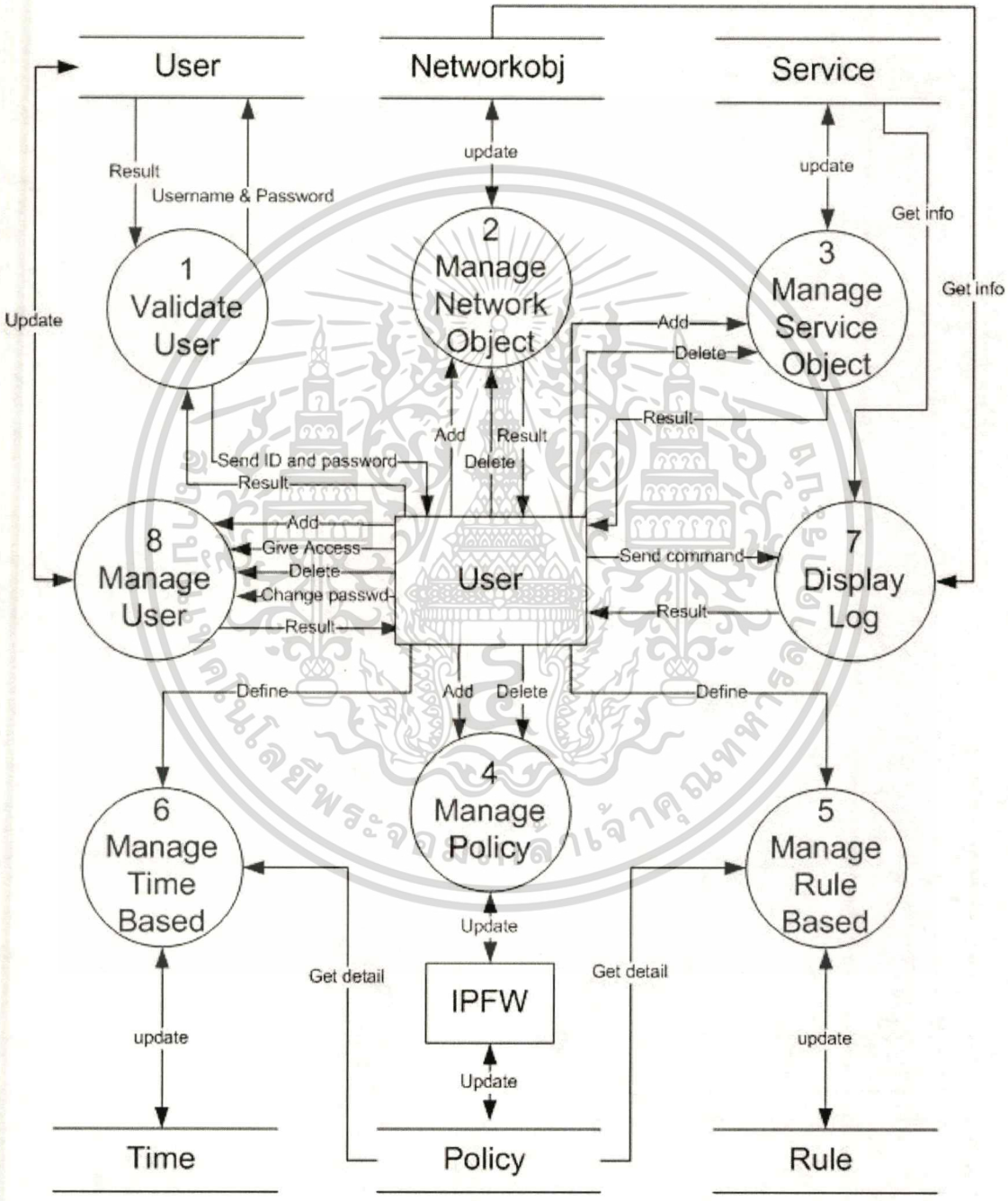
จะทำหน้าที่ในการนำคำสั่งที่ได้รับจากผู้ใช้งานมาเปลี่ยนเป็นคำสั่งที่ระบบรู้จัก เพื่อส่งต่อให้ เอนทิตี IPFW ทำงานต่อและรอรับผลที่ได้จากการทำงานของเอนทิตี IPFW มาแสดงต่อผู้ใช้งานและนำผลที่ได้ไปทำการบังคับใช้กับเครื่องคอมพิวเตอร์ตามเงื่อนไขที่กำหนด

เอนทิตี IPFW

ทำหน้าที่นำคำสั่งที่ได้จากระบบไปประมวลผล และทำการคืนค่าหรือผลที่ได้กลับไปยังระบบเพื่อบันทึกลงในฐานข้อมูลต่อไป และทำการติดต่อสื่อสารกับระบบเพื่อให้ระบบนำคำสั่งไปใช้ได้อย่างถูกต้อง และจะทำการแจ้งเตือนหากระบบทำงานไม่ถูกต้อง

3.2.2 แผนภาพการไหลของข้อมูล

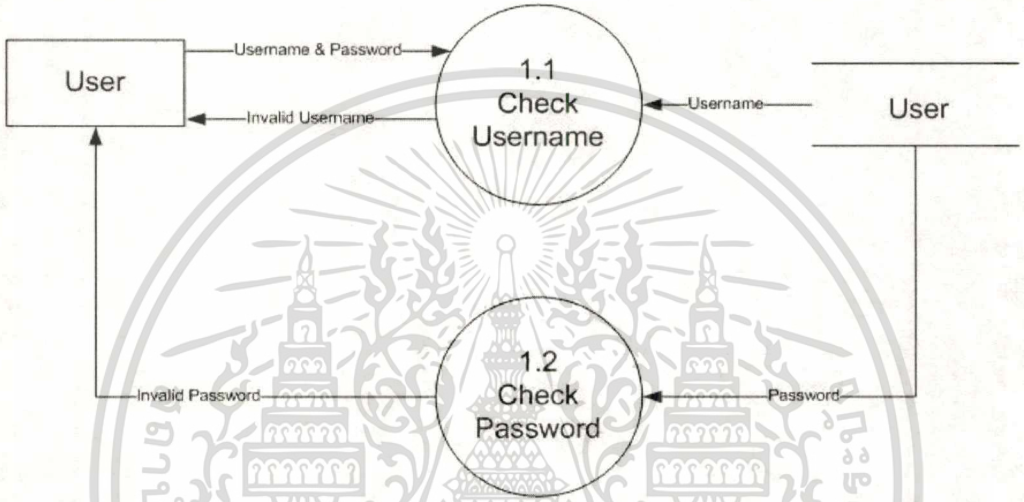
เมื่อได้แสดงให้เห็นถึงภาพรวมทั้งหมดของระบบงานและสิ่งที่อยู่ภายนอกระบบ ซึ่งเกี่ยวข้องกับระบบงานโดยคอนเท็กซ์ไดอะแกรมแล้ว จากนั้นจึงต้องแสดงขั้นตอนการทำงานของแผนภาพการไหลของข้อมูล ซึ่งระบบควบคุมการใช้งานเครือข่ายในห้องเรียนด้วยไฟร์วอลล์สามารถแบ่งออกเป็นระบบย่อยได้ดังนี้



ภาพที่ 3.3 แผนภาพการไหลของข้อมูลของระบบ

จากแผนภาพการไหลของข้อมูลของระบบ จะแสดงให้เห็นว่าระบบควบคุมการใช้งานเครือข่ายในห้องเรียนโดยใช้ไฟร์วอลล์นั้น มีการแบ่งส่วนการทำงานเป็นอย่างไร มีการติดต่อกับเอนทิตี และตารางข้อมูลอย่างไร และมีการส่งข้อความอะไรกันบ้าง ซึ่งแบ่งการทำงานออกได้เป็น 8 ระบบย่อย ซึ่งได้แก่

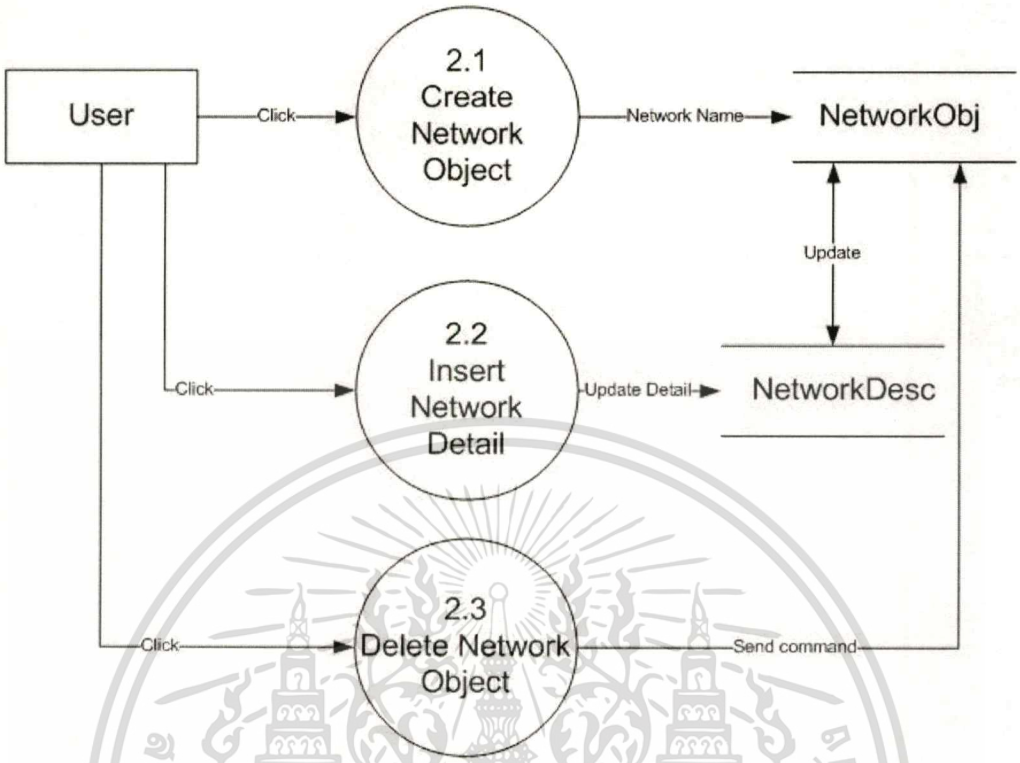
1. การตรวจสอบผู้ใช้งานระบบ



ภาพที่ 3.4 แผนภาพการไหลของข้อมูลของการตรวจสอบผู้ใช้งานระบบ

ผู้ใช้งานระบบจะทำการเข้าใช้งานระบบด้วยการใส่ชื่อผู้ใช้และรหัสผ่านของผู้ใช้ในฟอร์มของหน้าแรกของหน้าเว็บเพจ โดยที่กระบวนการแรก 1.1 จะมีการตรวจสอบว่าชื่อผู้ใช้ที่ใส่เข้ามามีอยู่ในระบบหรือไม่ ถ้าไม่มีจะมีข้อความเตือนว่าชื่อผู้ใช้งานไม่ถูกต้องให้ทำการใส่ใหม่อีกครั้ง และถ้ามีข้อมูลผู้ใช้อยู่จะเข้าสู่กระบวนการที่ 1.2 คือการตรวจสอบรหัสผ่าน ถ้าใส่รหัสผ่านผิดก็จะมีข้อความเตือนให้ใส่รหัสผ่านให้ถูกต้อง แต่ถ้าใส่รหัสผ่านถูกต้อง ผู้ใช้งานก็จะสามารถเข้าใช้งานระบบได้ต่อไป

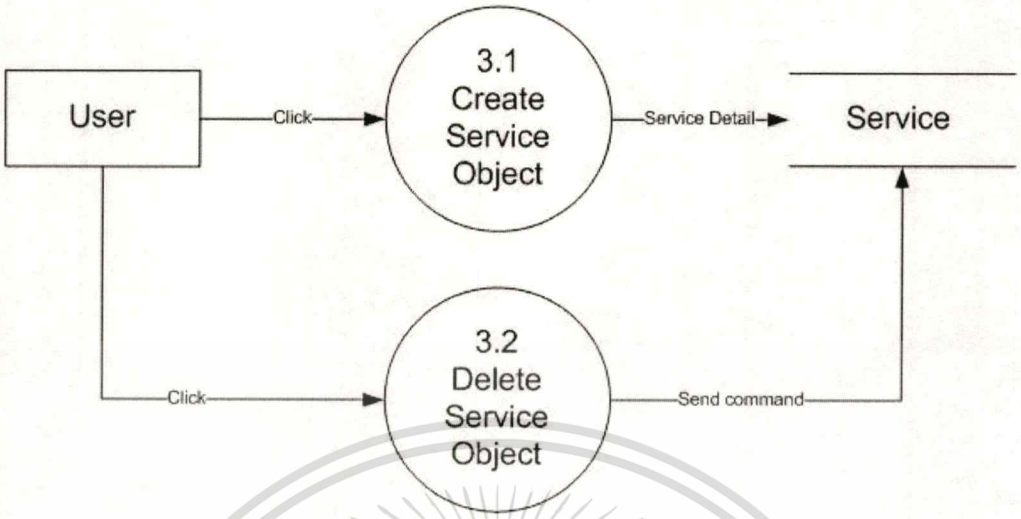
2. การบริหารจัดการกับ Network Object



ภาพที่ 3.5 แผนภาพการไหลของข้อมูลของระบบการบริหารจัดการกับ Network Object

ผู้ใช้งานระบบสามารถที่จะสร้าง Network Object ใหม่ขึ้นมาและสามารถลบ Network Object ที่มีอยู่ทิ้งไปได้ โดยที่ถ้าหากต้องการที่จะสร้าง Network Object ขึ้นมาใหม่นั้น ต้องเริ่มด้วยการใส่ชื่อของ Network Object นั้นก่อน แล้วจึงค่อยใส่รายละเอียดคือ หมายเลข ip address และ subnet mask และถ้าหากต้องการจะลบ Network Object ใดๆ ก็สามารถทำได้ด้วยการเลือก Network Object ที่ต้องการแล้วกดปุ่ม Delete Network Object นั้นก็จะถูกลบไป

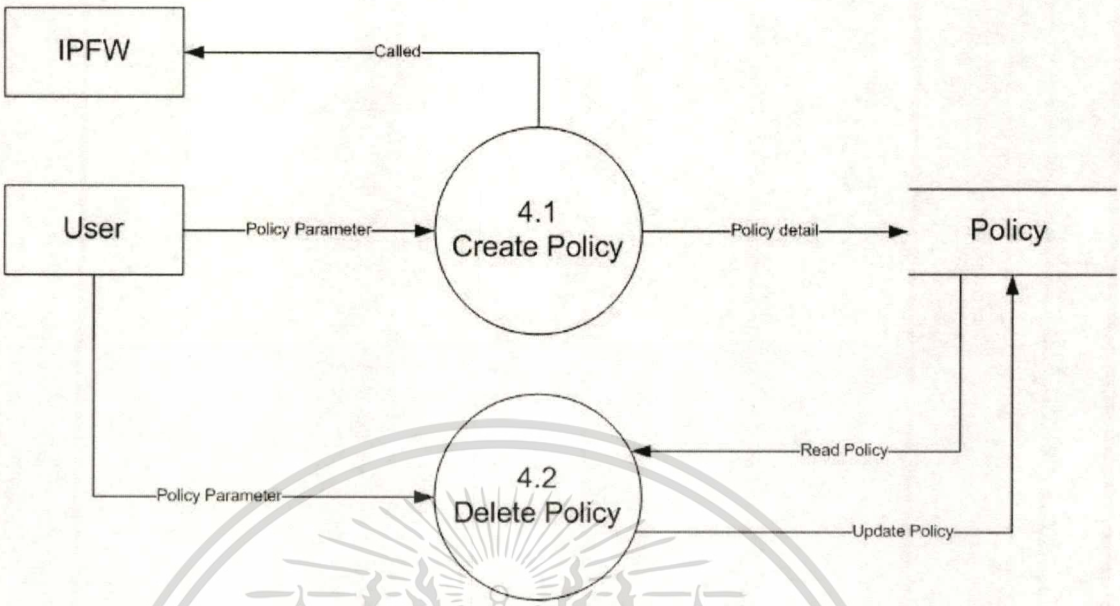
3. การบริหารจัดการกับ Service Object



ภาพที่ 3.6 แผนภาพการไหลของข้อมูลของระบบบริหารจัดการกับ Service Object

ผู้ใช้งานระบบสามารถที่จะสร้าง Service Object ใหม่ขึ้นมาและสามารถลบ Service Object ที่มีอยู่ทิ้งไปได้ โดยที่ถ้าหากต้องการที่จะสร้าง Service Object ขึ้นมาใหม่นั้น ต้องเริ่มด้วยการใส่ชื่อของ Service Object นั้นก่อน แล้วเลือก Protocol ว่าเป็น Protocol อะไร ระหว่าง TCP หรือ UDP และใส่หมายเลข Port ของ Service Object นั้น และถ้าหากต้องการจะลบ Service Object ใดๆ ก็สามารถทำได้ด้วยการเลือก Service Object ที่ต้องการแล้วกดปุ่ม Delete Service Object นั้นก็จะถูกลบไป

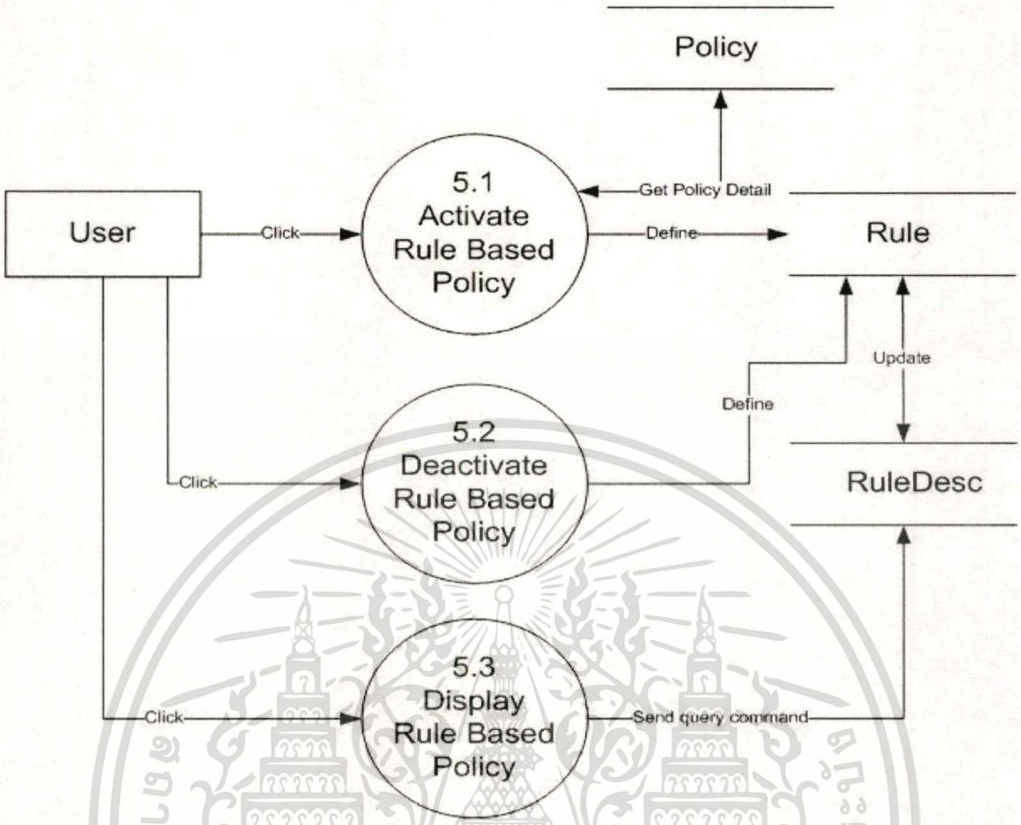
4. การบริหารจัดการกับ Policy



ภาพที่ 3.7 แผนภาพการไหลของข้อมูลของระบบบริหารจัดการกับ Policy

ผู้ใช้งานระบบสามารถที่จะสร้าง Policy ใหม่ขึ้นมาและสามารถลบ Policy ที่มีอยู่ทิ้งไปได้ โดยที่ถ้าหากต้องการที่จะสร้าง Policy ขึ้นมาใหม่นั้น ต้องเริ่มด้วยการเลือก Type ของ Policy ว่าจะเป็น Policy ให้อนุญาตหรือไม่อนุญาต หลังจากนั้นเลือก Service Object และ Network Object ต้นทางและ Network Object ปลายทาง และถ้าหากต้องการจะลบ Policy ใดๆ ก็สามารถทำได้ด้วยการเลือก Policy ที่ต้องการแล้วกดปุ่ม Delete Policy นั้นก็จะหายไป

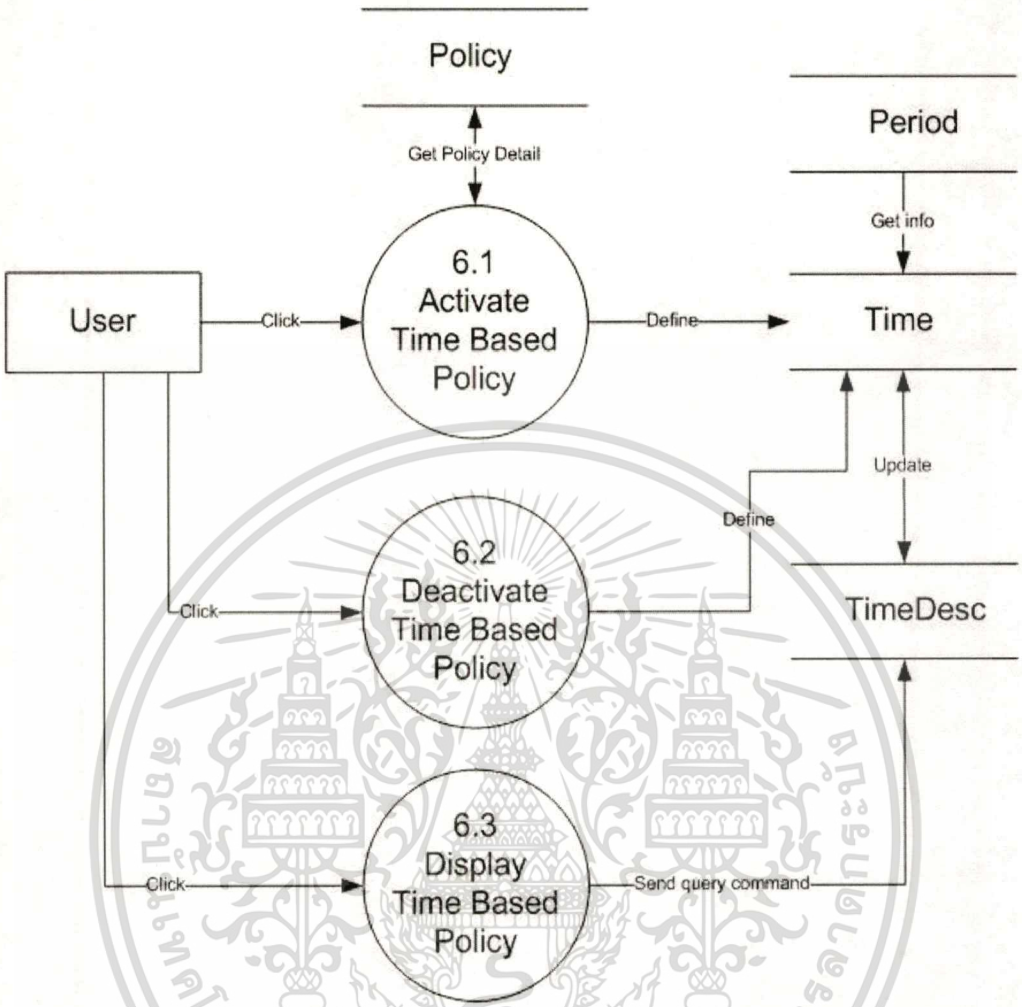
5. การบริหารจัดการกับ Rule Based Policy



ภาพที่ 3.8 แผนภาพการไหลของข้อมูลของระบบบริหารจัดการกับ Rule Based Policy

ผู้ใช้งานระบบสามารถที่จะกำหนด Rule Based Policy ขึ้นมาและเอา Rule Based Policy ออกไปจากระบบได้ โดยที่ถ้าหากต้องการที่จะกำหนด Rule Based Policy ขึ้นมาใหม่นั้น ทำได้ด้วยการเลือก Policy ที่มีอยู่แล้วมาใช้ ด้วยการ Activate Policy ที่มีอยู่ แต่ถ้าหากไม่ต้องการใช้ Rule Based Policy ใด ก็สามารถ Deactivate Policy นั้นๆ ได้

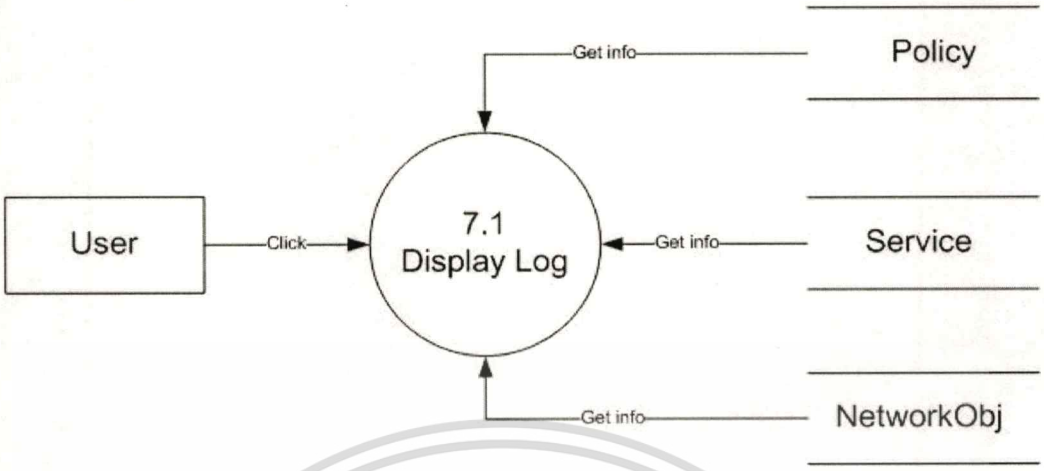
6. การบริหารจัดการกับ Time Based Policy



ภาพที่ 3.9 แผนภาพการไหลของข้อมูลของระบบบริหารจัดการกับ Time Based Policy

ผู้ใช้งานระบบสามารถที่จะกำหนด Time Based Policy ขึ้นมาและเอา Time Based Policy ออกไปจากระบบได้ โดยที่ถ้าหากต้องการที่จะกำหนด Time Based Policy ขึ้นมาใหม่นั้น ทำได้ด้วยการเลือก Policy ที่มีอยู่แล้วมาใช้ ด้วยการเลือกช่วงเวลาที่ต้องการให้ policy นั้นทำงาน แต่ถ้าหากไม่ต้องการใช้ Time Based Policy ใด ก็สามารถ Deactivate Policy นั้นๆ ได้ และถ้าหากผ่านพ้นช่วงเวลาที่เรากำหนดไว้ Policy นั้นจะถูกลบออกจาก Time Based Policy โดยอัตโนมัติ

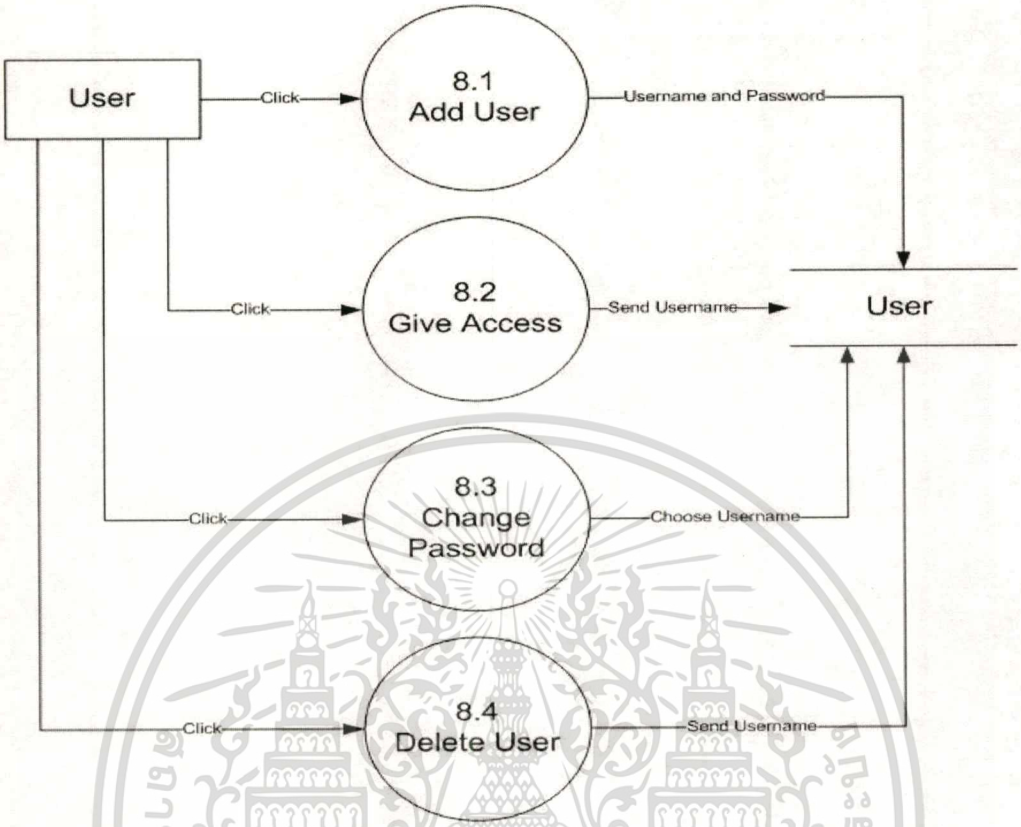
7. การแสดง Log



ภาพที่ 3.10 แผนภาพการไหลของข้อมูลของระบบการแสดง Log

ผู้ใช้งานระบบสามารถที่จะดู Log ของ Policy ต่างๆ ที่ถูกเรียกใช้ได้ โดยที่จะสามารถดูในขณะที่ Policy นั้นๆ มีผลทำงานอยู่เท่านั้น

8. การบริหารจัดการผู้ใช้

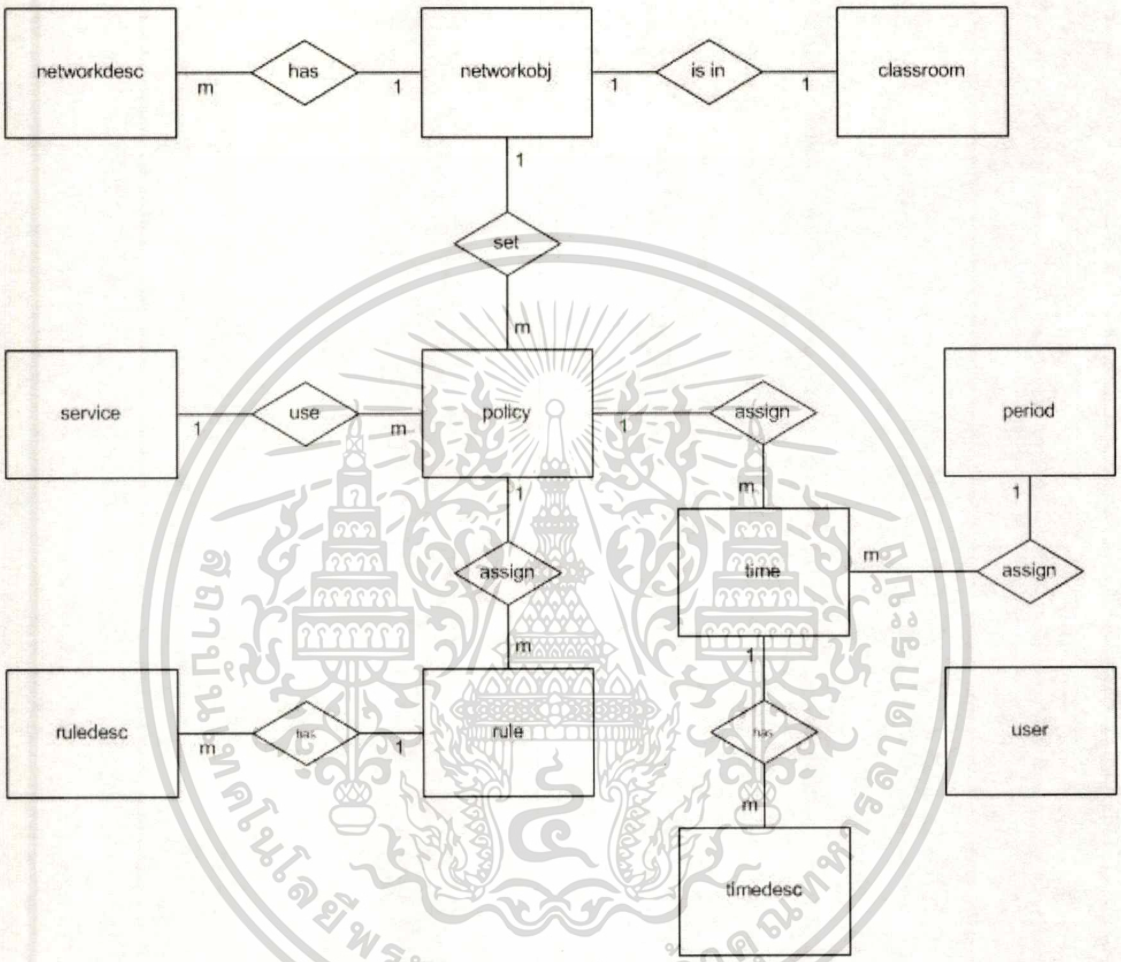


ภาพที่ 3.11 แผนภาพการไหลของข้อมูลของระบบบริหารจัดการผู้ใช้

ผู้ใช้งานระบบสามารถที่จะสร้างผู้ใช้ใหม่ขึ้นมา ลบผู้ใช้ที่มีอยู่ออกไป (แต่จะไม่สามารถลบผู้ใช้ admin ออกไปได้) สามารถกำหนดสิทธิ์ให้ผู้ใช้ได้ สามารถแก้ไข Password ของตนเองได้ (ผู้ใช้ admin สามารถแก้ไข Password ของผู้ใช้อื่นได้ด้วย)

3.3 การออกแบบระบบงานโดยการจำลองแบบข้อมูล

ในหัวข้อนี้จะอธิบายการออกแบบระบบงานเกี่ยวกับกลุ่มของข้อมูลที่สัมพันธ์กัน ด้วยแบบจำลองข้อมูล สำหรับเครื่องมือที่จะนำมาใช้ในการวิเคราะห์คือแผนภาพแสดงความสัมพันธ์ระหว่างเอนทิตี (Entity Relationship Diagram) ดังภาพที่ 3.6



ภาพที่ 3.12 อีอาร์ไดอะแกรมของระบบควบคุมการใช้งานเครือข่ายในห้องเรียนโดยใช้ไฟร์วอลล์

จะเห็นว่าในฐานข้อมูลประกอบด้วย 11 ตาราง คือ

1. ตาราง classroom คือ ตารางที่ใช้จัดเก็บข้อมูลห้องปฏิบัติการ โดยจะจัดเก็บข้อมูลจำนวนแถวและสดมภ์ของเครื่องคอมพิวเตอร์ที่มีในแต่ละห้องปฏิบัติการ
2. ตาราง networkobj คือ ตารางที่ใช้จัดเก็บข้อมูลเครื่องให้บริการในเครือข่ายของระบบ
3. ตาราง networkdesc คือ ตารางที่ใช้จัดเก็บข้อมูลรายละเอียดเครือข่ายที่มีในระบบ
4. ตาราง service คือ ตารางที่ใช้จัดเก็บข้อมูลของงานบริการที่มีให้ของระบบ
5. ตาราง policy คือ ตารางที่ใช้จัดเก็บข้อมูลนโยบายที่ผู้ใช้งานระบบกำหนดขึ้น
6. ตาราง rule คือ ตารางที่ใช้จัดเก็บข้อมูลของการทำงานแบบ Rule Based
7. ตาราง ruledesc คือ ตารางที่ใช้จัดเก็บข้อมูลรายละเอียดของการทำงานแบบ Rule Based
8. ตาราง time คือ ตารางที่ใช้จัดเก็บข้อมูลของการทำงานแบบ Time Based
9. ตาราง timedesc คือ ตารางที่ใช้จัดเก็บข้อมูลรายละเอียดของการทำงานแบบ Time Based
10. ตาราง period คือ ตารางที่ใช้จัดเก็บข้อมูลช่วงเวลา
11. ตาราง user คือ ตารางที่ใช้จัดเก็บข้อมูลผู้ใช้งานระบบ

ตารางต่างๆในฐานข้อมูลมีรายละเอียดของข้อมูล ซึ่งสามารถอธิบายด้วยพจนานุกรมข้อมูลดังต่อไปนี้

ตารางที่ 3.1 classroom: ตารางห้องปฏิบัติการ

ชื่อแอตทริบิวต์	ประเภท	ความหมาย	คีย์	ตารางที่อ้างถึง
roomid	VarChar(5)	รหัสห้องปฏิบัติการ	PK	
roomdesc	VarChar(80)	ชื่อห้องปฏิบัติการ		
col	Integer	จำนวนcolumn ในห้องปฏิบัติการ		
row	Integer	จำนวน row ในห้องปฏิบัติการ		
networkid	Integer	รหัสเครือข่ายของห้องปฏิบัติการ	FK	networkobj

ตารางที่ 3.2 networkobj: ตารางข้อมูล object ของเครือข่าย

ชื่อแอตทริบิวต์	ประเภท	ความหมาย	คีย์	ตารางที่อ้างถึง
networkid	Integer	รหัสเครือข่าย	PK	
descript	Varchar(255)	ชื่อเครือข่าย		
used	Boolean	สถานะ 1=used, 0= not used		

ตารางที่ 3.3 networkdesc : ตารางรายละเอียดเครือข่าย

ชื่อแอตทริบิวต์	ประเภท	ความหมาย	คีย์	ตารางที่อ้างถึง
networkid	Integer	รหัสเครือข่าย	PK FK	networkobj
ip	VarChar(20)	IP Address	PK	
netmask	Integer	SubnetMask		

ตารางที่ 3.4 service: ตารางข้อมูลงานบริการ

ชื่อแอตทริบิวต์	ประเภท	ความหมาย	คีย์	ตารางที่อ้างถึง
serviceid	Integer	รหัสงานบริการ	PK	
servicename	Varchar(80)	ชื่องานบริการ		
protocol	VarChar(8)	ชื่อโปรโตคอลที่ใช้		
port	Integer	หมายเลข Port		
used	Boolean	สถานะ 1=used, 0= not used		

ตารางที่ 3.5 policy: ตารางข้อมูลนโยบายการให้บริการ

ชื่อแอตทริบิวต์	ประเภท	ความหมาย	คีย์	ตารางที่อ้างถึง
id	Integer	รหัสนโยบาย	PK	
type	Boolean	ประเภทนโยบาย 0=allow,1=deny		
service	Integer	รูปแบบการให้บริการ	FK	service
source	Integer	รหัสเครือข่ายต้นทาง	FK	networkobj
destination	Integer	รหัสเครือข่ายปลายทาง	FK	networkobj
used	Boolean	สถานะ 1=used, 0= not used		

ตารางที่ 3.6 rule: ตารางข้อมูลของการทำงานแบบ Rule Based

ชื่อแอตทริบิวต์	ประเภท	ความหมาย	คีย์	ตารางที่อ้างถึง
ruleid	Integer	รหัสการทำงานของ Rule Based	PK	
policyid	Integer	รหัสนโยบาย	FK	policy
date	datetime	วันที่กำหนดนโยบาย		

ตารางที่ 3.7 ruledesc: ตารางข้อมูลรายละเอียดของการทำงานแบบ Rule Based

ชื่อแอตทริบิวต์	ประเภท	ความหมาย	คีย์	ตารางที่อ้างถึง
ruleid	Integer	รหัสการทำงานของ Rule Based	PK FK	rule
ruleorder	Integer	ลำดับการทำงาน		
source	varchar(20)	ข้อมูล ip address/subnetmask ของเครือข่ายต้นทาง		
destination	varchar(20)	ข้อมูล ip address/subnetmask ของเครือข่ายปลายทาง		

ตารางที่ 3.8 time: ตารางข้อมูลของการทำงานแบบ Time Based

ชื่อแอตทริบิวต์	ประเภท	ความหมาย	คีย์	ตารางที่อ้างถึง
ruleid	Integer	รหัสการทำงานของ Time Based	PK	
policyid	Integer	รหัสนโยบาย	FK	policy
date	datetime	วันที่กำหนดให้มีการทำงาน		
period	Integer	รหัสช่วงเวลา	FK	period
used	Boolean	สถานะ 1=used, 0= not used		

ตารางที่ 3.9 timedesc: ตารางข้อมูลรายละเอียดของการทำงานแบบ Time Based

ชื่อแอตทริบิวต์	ประเภท	ความหมาย	คีย์	ตารางที่อ้างถึง
ruleid	Integer	รหัสการทำงานของ Time Based	PK FK	time
ruleorder	Integer	ลำดับการทำงาน		
source	varchar(20)	ข้อมูล ip address/subnet mask ของเครือข่ายต้นทาง		
destination	varchar(20)	ข้อมูล ip address/subnet mask ของเครือข่ายปลายทาง		

ตารางที่ 3.10 period: ตารางข้อมูลช่วงเวลา

ชื่อแอตทริบิวต์	ประเภท	ความหมาย	คีย์	ตารางที่อ้างถึง
id	Integer	รหัสการทำงานของ Time Based	PK	
name	varchar(10)	ชื่อช่วงเวลา		
start_h	varchar(2)	ข้อมูลเวลาชั่วโมงเริ่มต้น		
start_m	varchar(2)	ข้อมูลเวลานาทีเริ่มต้น		
stop_h	varchar(2)	ข้อมูลเวลาชั่วโมงสิ้นสุด		
stop_m	varchar(2)	ข้อมูลเวลานาทีสิ้นสุด		

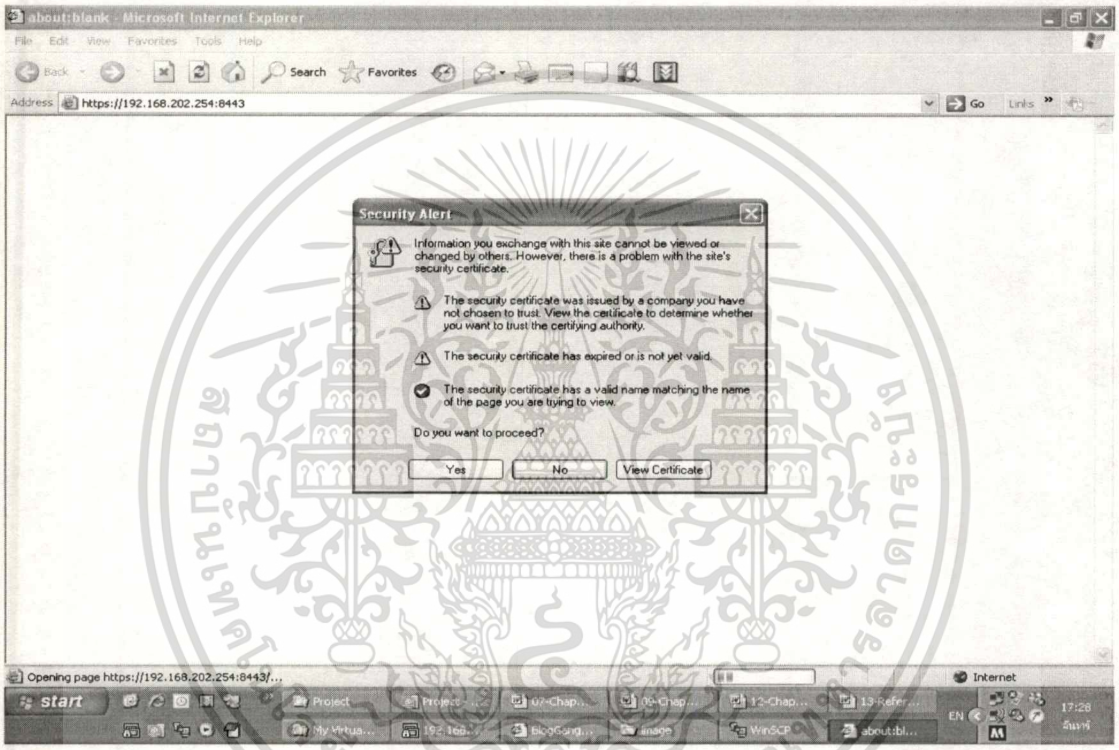
ตารางที่ 3.11 user : ตารางผู้ใช้งานระบบ

ชื่อแอตทริบิวต์	ประเภท	ความหมาย	คีย์	ตารางที่อ้างถึง
num	Integer	ลำดับที่ผู้ใช้	PK	
userid	VarChar(5)	รหัสผู้ใช้		
userpw	Varchar(10)	รหัสผ่าน		
enable	Boolean	สถานะผู้ใช้งาน 1=enable, 0=disable		

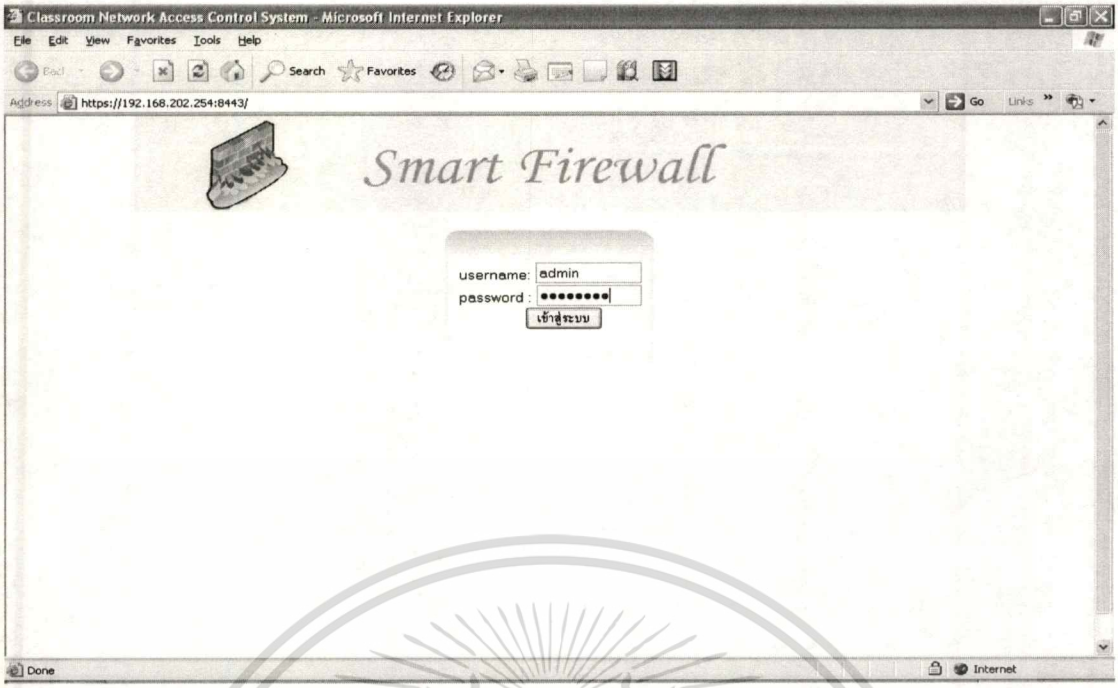
หลังจากที่ได้ทำการออกแบบในส่วนต่าง ๆ เรียบร้อยแล้ว ก็จะเข้าสู่ขั้นตอนของการพัฒนาระบบให้ตรงตามที่ออกแบบไว้ ซึ่งการพัฒนาระบบนั้นจะกล่าวในบทต่อไป

บทที่ 5
การออกแบบส่วนติดต่อของผู้ใช้

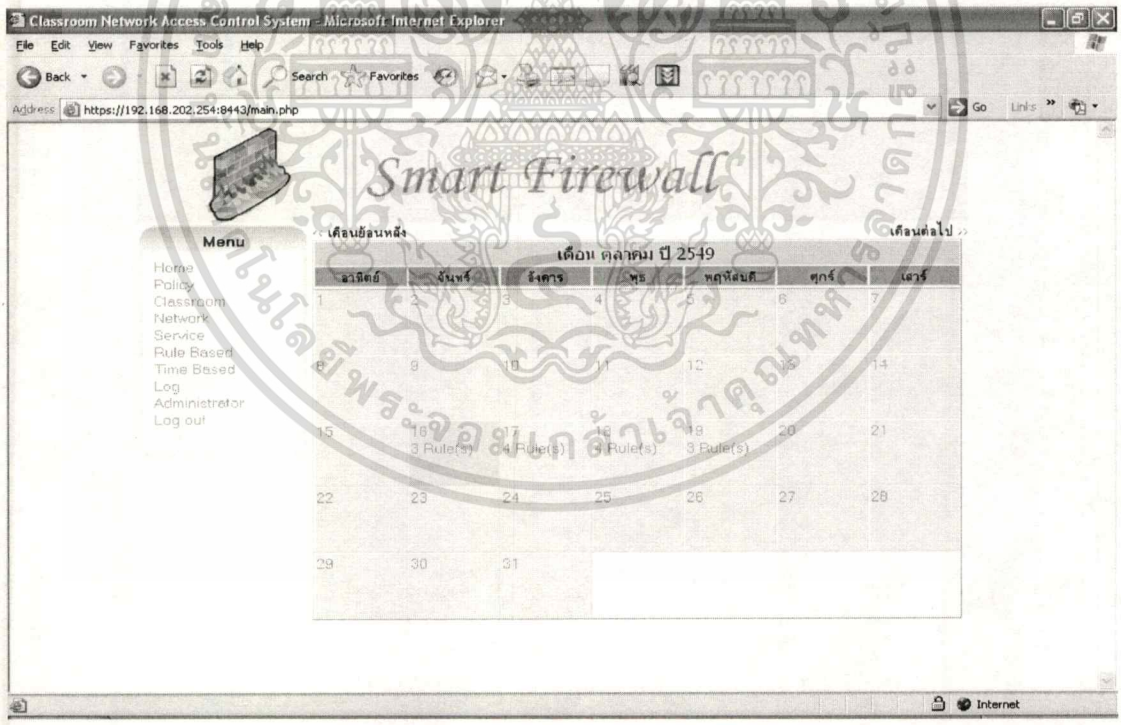
เมื่อได้ทำการออกแบบระบบตามรายละเอียดในบทที่ 3 แล้ว ขั้นตอนต่อไปคือการพัฒนาระบบควบคุมการใช้งานเครือข่ายในห้องเรียนโดยใช้ไฟร์วอลล์ให้เป็นไปตามที่ได้ออกแบบไว้ โดยในบทนี้จะกล่าวถึงหน้าจอในการรับข้อมูลเข้า (Input) และการแสดงผล (Output)



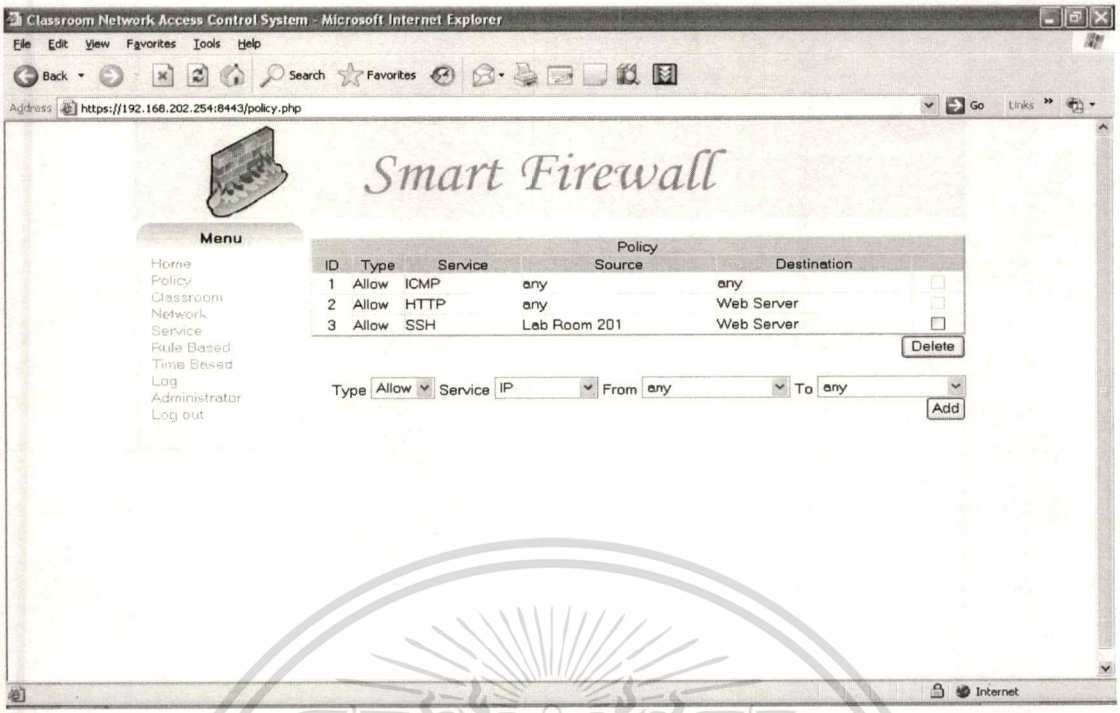
ภาพที่ 4.1 หน้าจอแสดงถึงการยืนยันการเข้าใช้งานแบบ SSL



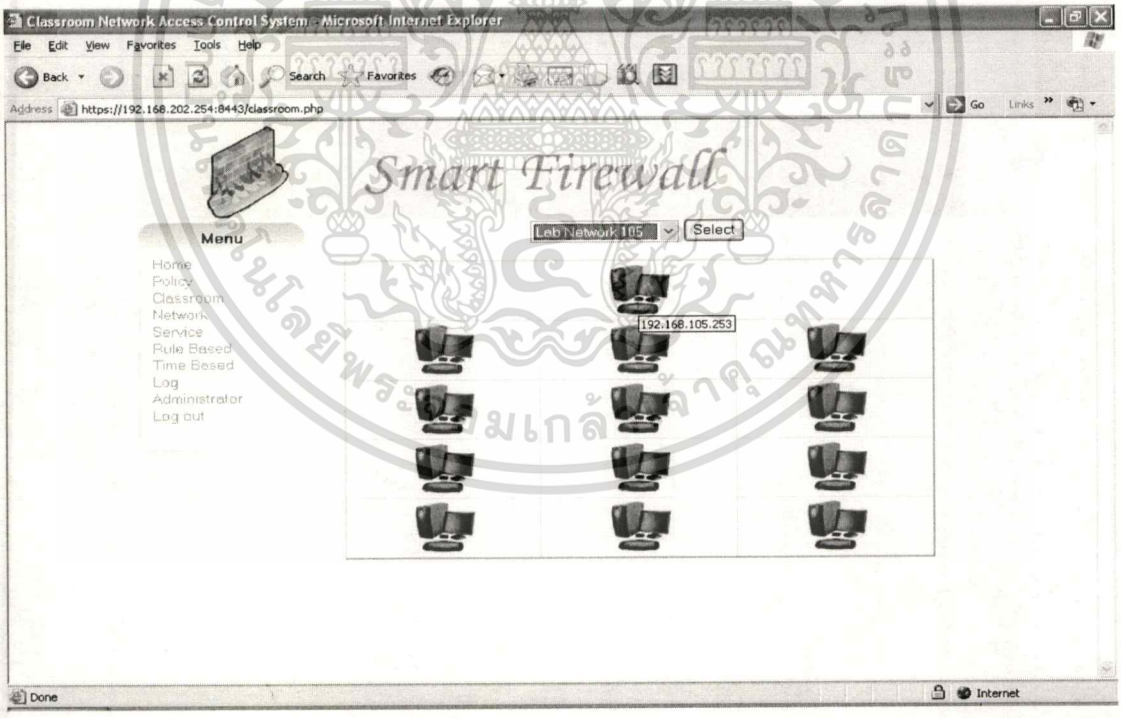
ภาพที่ 4.2 หน้าจอการล็อกอินเข้าสู่ระบบ



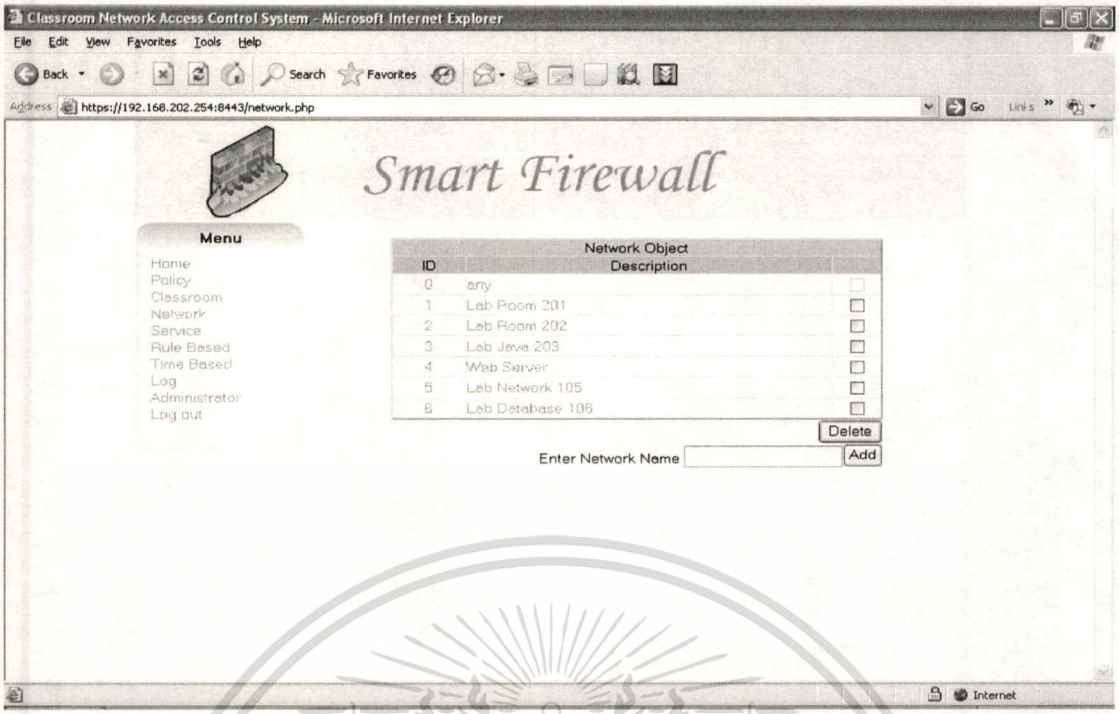
ภาพที่ 4.3 หน้าจอหลัก



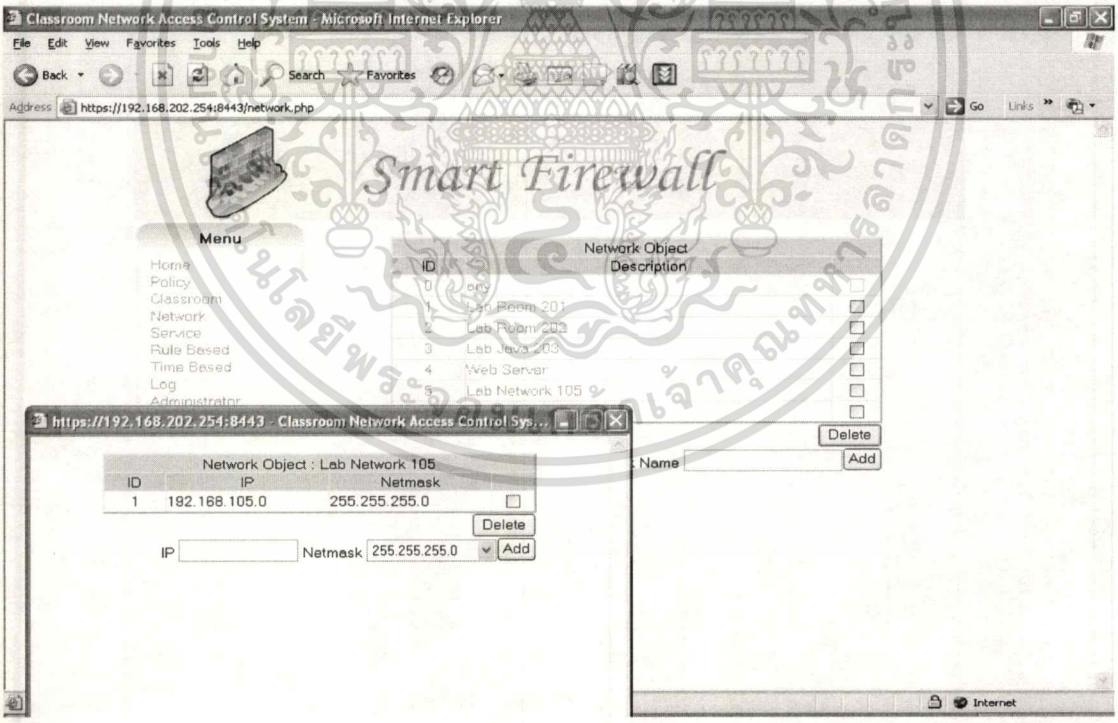
ภาพที่ 4.4 หน้าจอนโยบายที่มีในปัจจุบันของระบบ



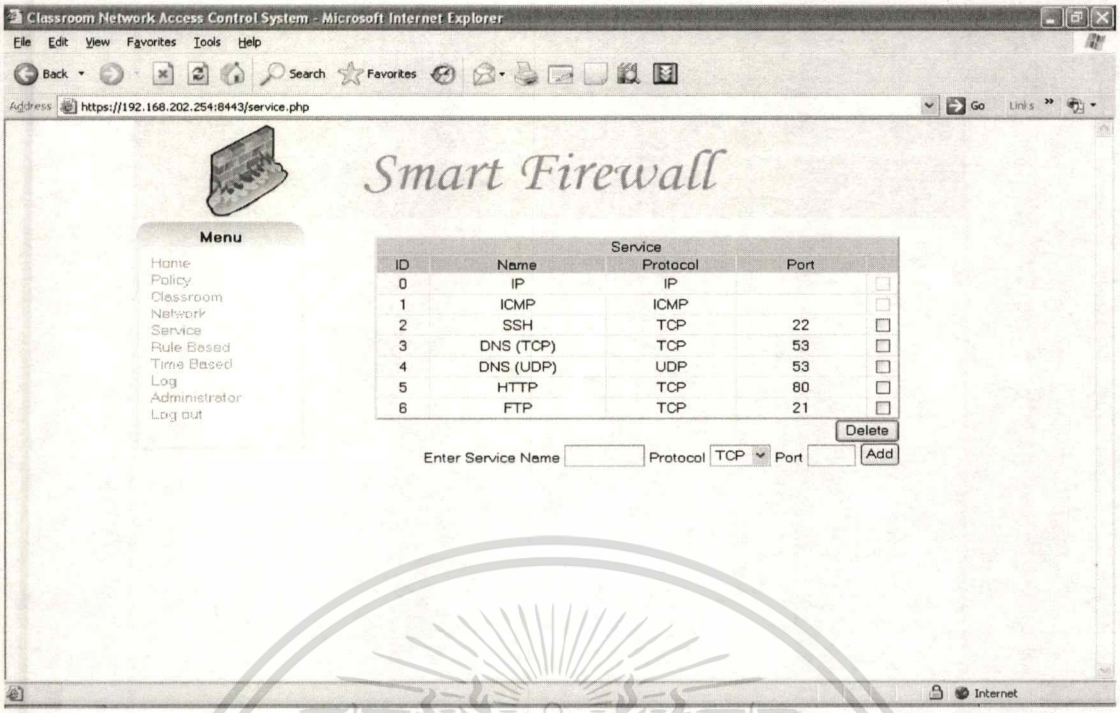
ภาพที่ 4.5 หน้าจอการเลือกห้องเรียน



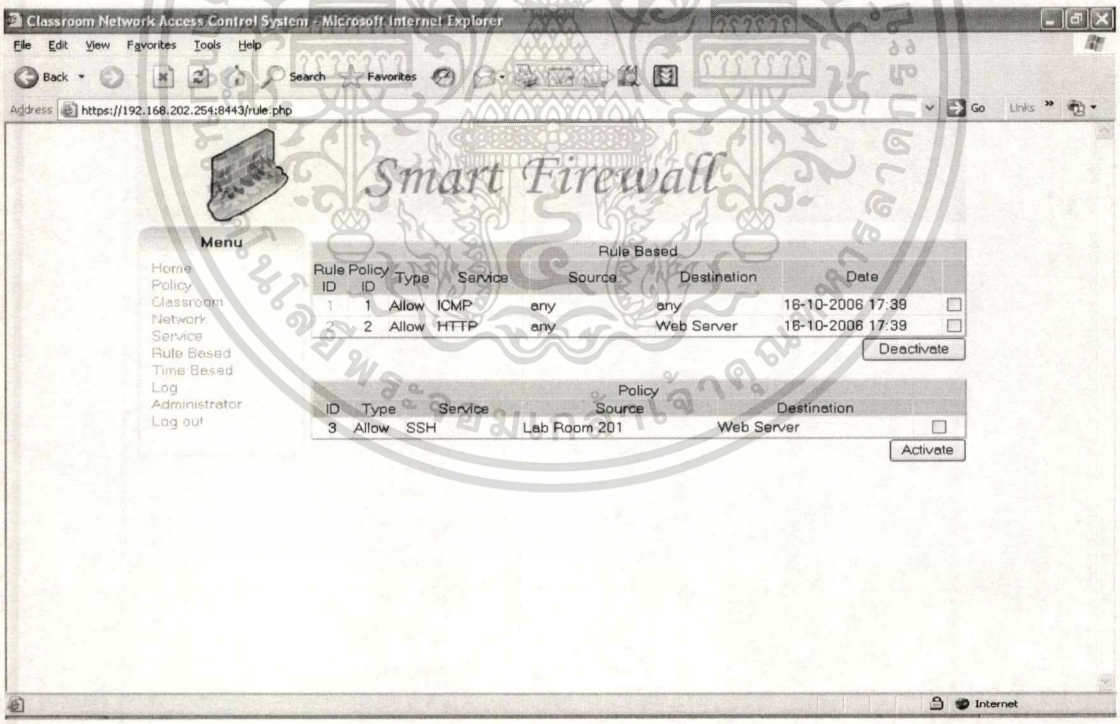
ภาพที่ 4.6 หน้าจอ Network Object ที่มีในระบบ



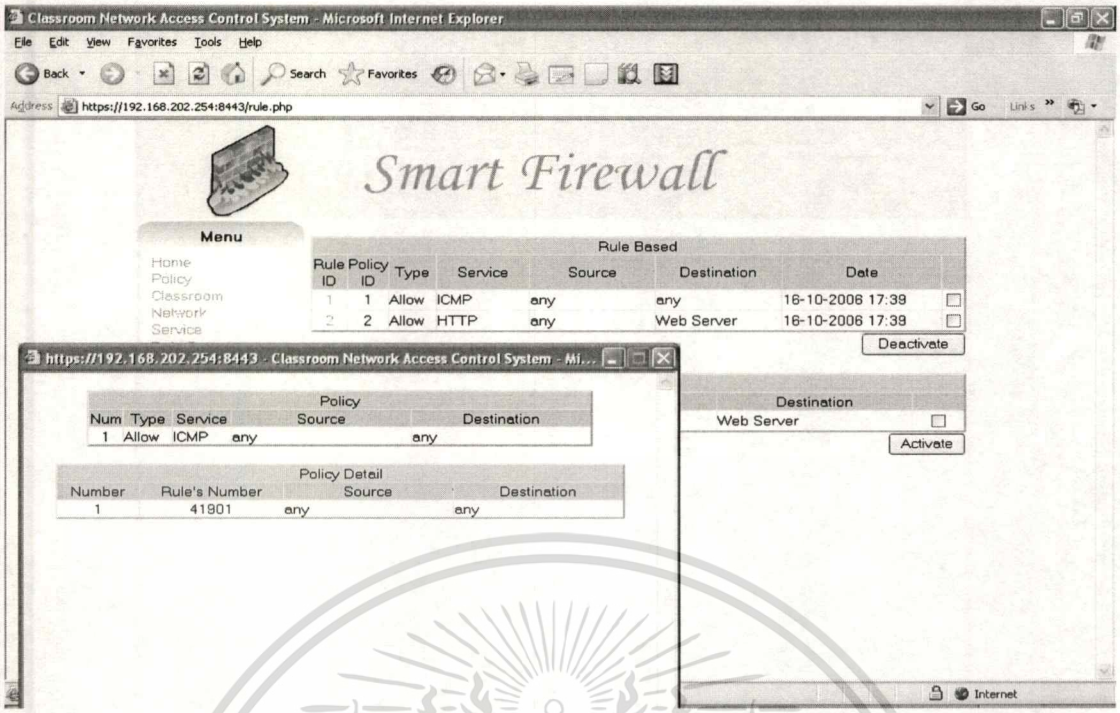
ภาพที่ 4.7 หน้าจอรายละเอียดของ Network Object



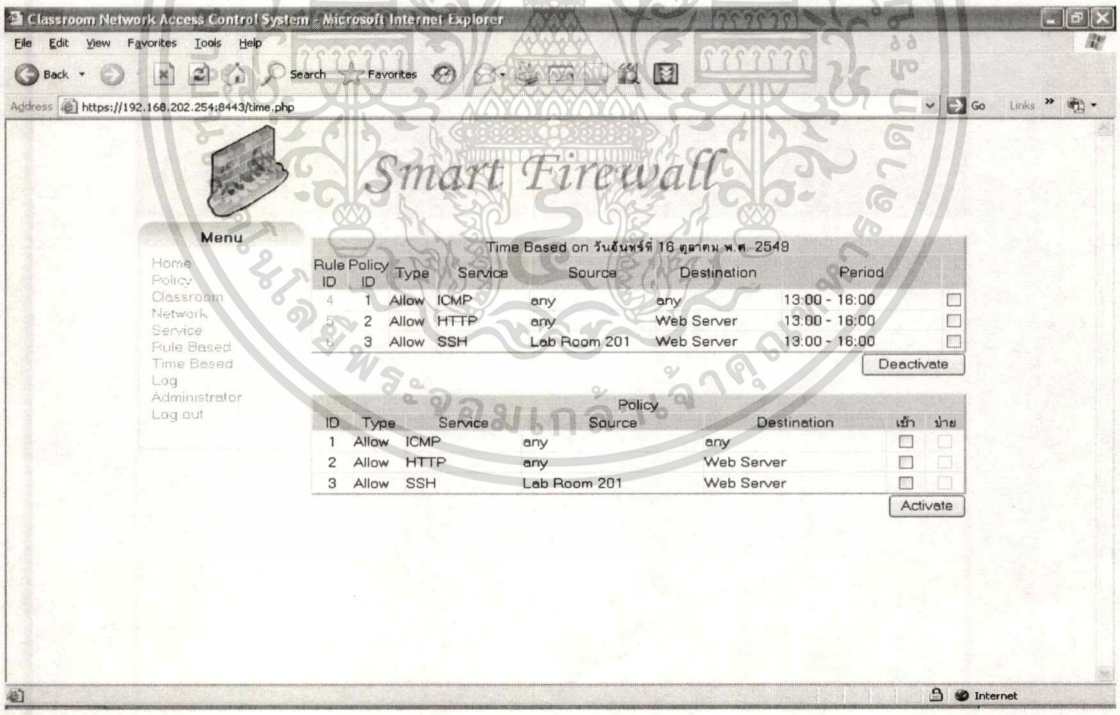
ภาพที่ 4.8 หน้าจอรายละเอียดของ Service ต่างๆ ที่มีอยู่ในระบบ



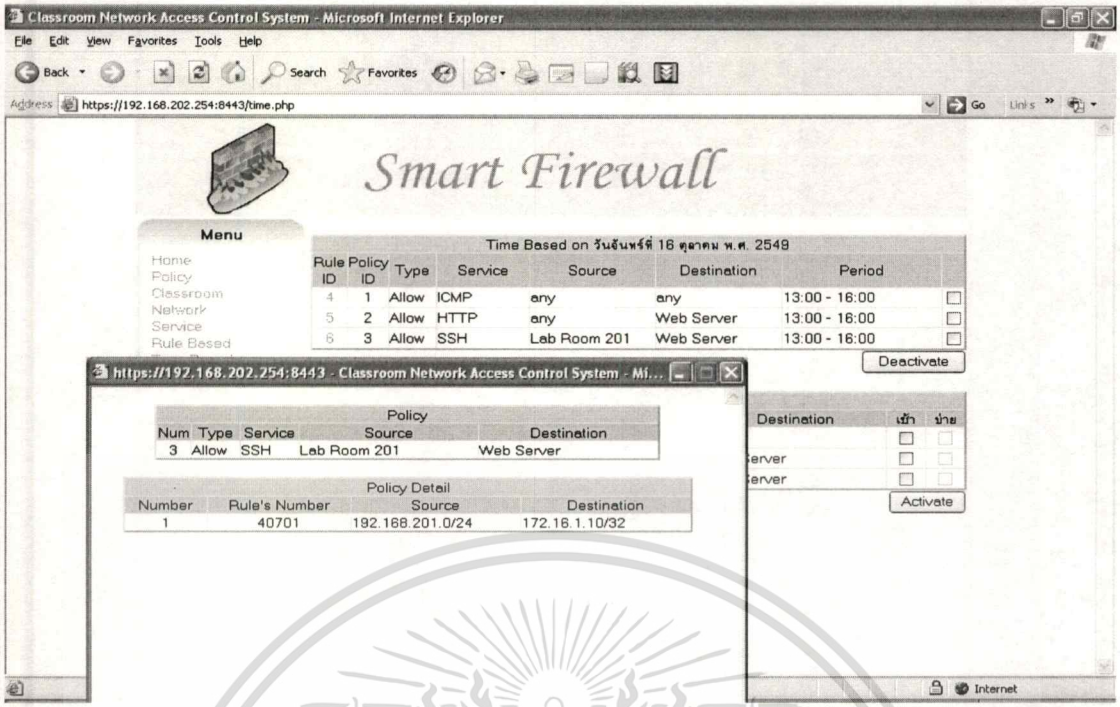
ภาพที่ 4.9 หน้าจอของกฎที่ใช้ในปัจจุบัน



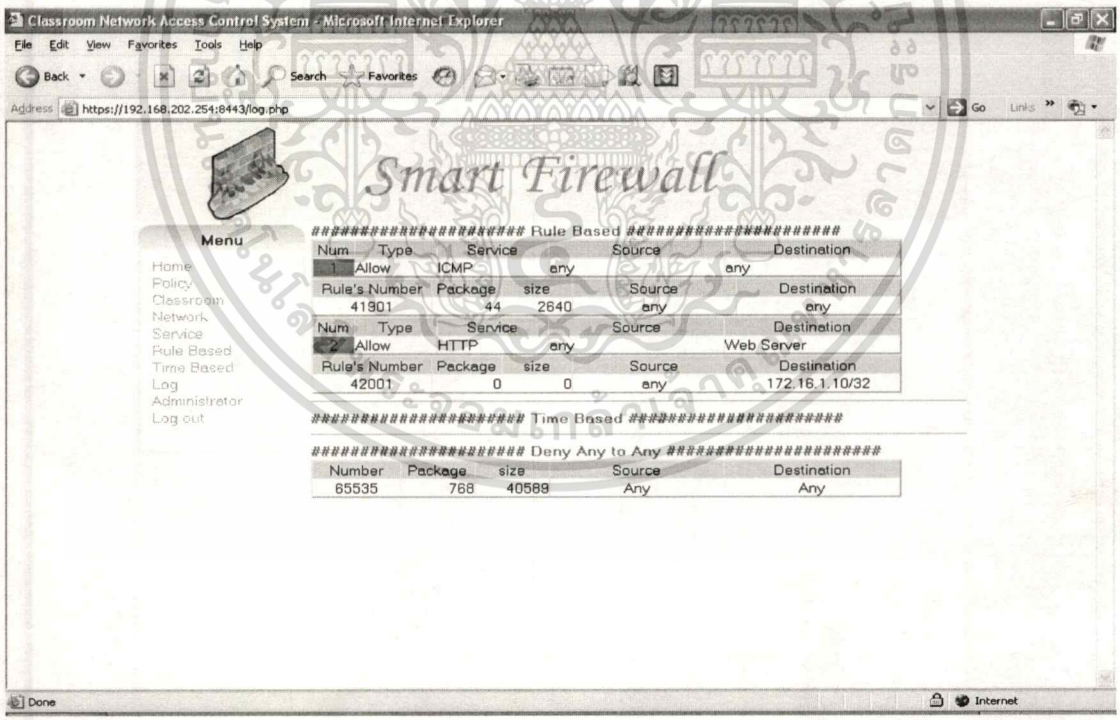
ภาพที่ 4.10 หน้าจอรายละเอียดของกฎที่ใช้ในปัจจุบัน



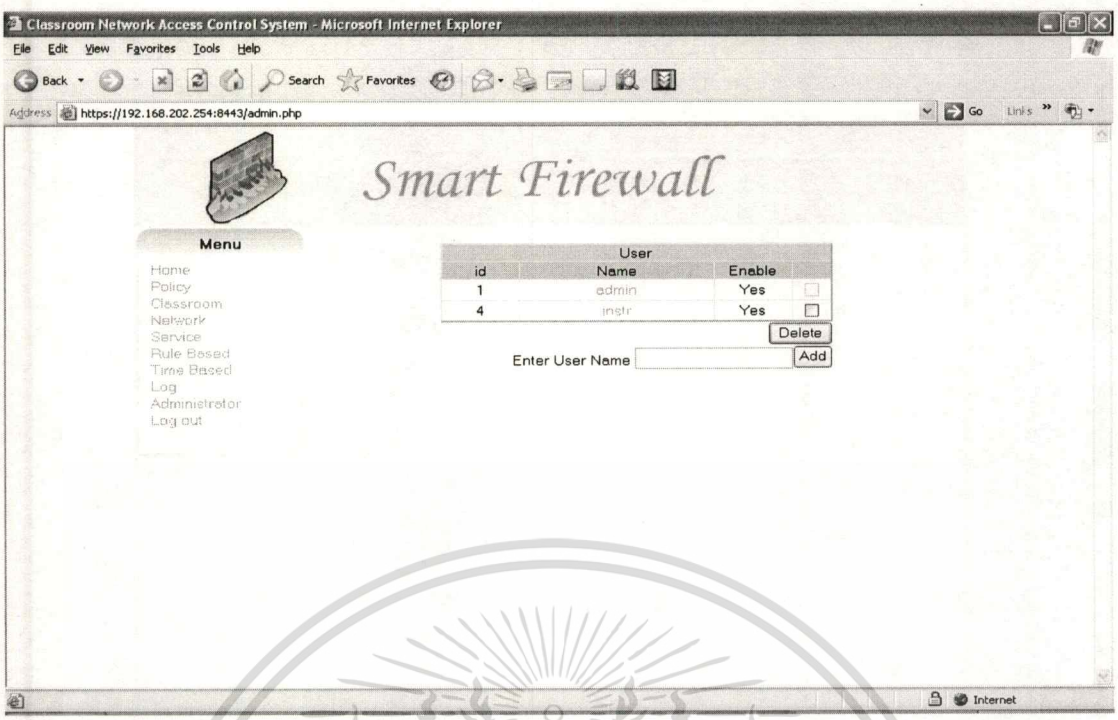
ภาพที่ 4.11 หน้าจอของกฎที่มีการกำหนดไว้ในแต่ละวัน



ภาพที่ 4.12 หน้าจอรายละเอียดของกฎที่มีการกำหนดไว้ในแต่ละวัน



ภาพที่ 4.13 หน้าจอรายละเอียดของ log ทั้งหมดที่มีในระบบ



ภาพที่ 4.14 หน้าจอรายละเอียดของผู้ใช้ทั้งหมดที่มีในระบบ

บทที่ 6
สรุปผลการพัฒนาระบบและข้อเสนอแนะ

การพัฒนาระบบควบคุมการใช้งานเครือข่ายภายในห้องเรียนโดยใช้ไฟร์วอลล์นี้ มีจุดประสงค์ทางหนึ่งเพื่อช่วยควบคุมดูแลให้การเรียนการสอนเป็นไปอย่างมีประสิทธิภาพสูงสุด และอีกทางหนึ่งเพื่อเป็นการอำนวยความสะดวกในการทำงานของผู้ดูแลระบบและอาจารย์ผู้สอน ในการควบคุมการเข้าใช้งานระบบเครือข่ายของนักเรียนหรือนักศึกษาโดยอาศัยเว็ปเพจที่ใช้งานง่าย ไม่ซับซ้อน

5.1 ประโยชน์ที่ได้รับจากโครงการ

1. ประโยชน์ต่อผู้พัฒนาระบบ
   - เป็นการนำความรู้ที่ได้จากการศึกษามาประยุกต์ใช้ในการวิเคราะห์ระบบ ออกแบบระบบ และทำการพัฒนาระบบ เพื่อให้สามารถใช้งานได้จริง
   - เป็นการศึกษาเรียนรู้และประยุกต์ใช้เทคโนโลยีที่มีอยู่ในปัจจุบันมาใช้ในการพัฒนาระบบให้มีประสิทธิภาพ
   - รู้จักวิธีการวางแผนการพัฒนา การแก้ปัญหาต่างๆ ที่เกิดขึ้นในการพัฒนาระบบในแต่ละขั้นตอน
2. ประโยชน์ต่อองค์กรหรือสถาบันการศึกษาที่จะนำระบบไปใช้งาน
   - เป็นโปรแกรมต้นแบบเพื่อที่นำไปใช้ในการพัฒนาระบบให้มีประสิทธิภาพมากขึ้นต่อไป
   - เป็นการเพิ่มประสิทธิภาพในการเรียนการสอนในห้องเรียน LAB ให้มากขึ้น
   - ช่วยอำนวยความสะดวกให้การบริหารจัดการเครือข่ายภายในห้องเรียน LAB เป็นไปด้วยความเป็นระเบียบ
3. ประโยชน์ต่อผู้ใช้งานระบบ
   - สามารถกำหนดสิทธิ์ของเครื่องแต่ละเครื่องได้ หากต้องการให้เครื่องใดสามารถเข้าใช้งานเครือข่ายได้
   - ผู้ใช้งานระบบไม่จำเป็นต้องจำคำสั่งในการกำหนดค่าต่างๆ โดยระบบจะมีหน้าจอที่ง่ายสำหรับใช้งาน
   - สามารถกำหนดเวลาการเข้าใช้งานระบบเครือข่ายล่วงหน้าได้

5.2 ข้อจำกัดของระบบที่พัฒนาขึ้น

ระบบที่ได้ทำการพัฒนาขึ้นมานี้ จะมีไม่ครอบคลุมไปถึงหน้าที่การทำงานดังต่อไปนี้

1. ระบบที่พัฒนาขึ้นเป็นเพียงระบบที่ถูกจำลองขึ้นเท่านั้น ดังนั้นอาจทำให้การทำงานของระบบโดยรวมไม่ดีมากนัก เพราะพัฒนาอยู่บนเครื่องโน้ตบุ๊คที่มีประสิทธิภาพไม่สูง
2. ระบบที่ถูกพัฒนาขึ้นนี้จะรองรับห้องเรียน LAB ที่มีเครื่องคอมพิวเตอร์ห้องละไม่เกิน 252 เครื่องเท่านั้น
3. เนื่องจากระบบที่ถูกพัฒนาขึ้นเพื่อจำลองการทำงานภายในระบบเครือข่ายภายใน ดังนั้น ความสัมพันธ์ระหว่าง interface จึงเป็นแบบ routed mode เท่านั้น ไม่มีการทำการเปลี่ยนแปลงหมายเลข ip address (ไม่มีการทำ NAT)
4. ระบบที่พัฒนาขึ้นจะตั้งอยู่บนสภาพแวดล้อมที่ผู้ดูแลระบบเป็นผู้กำหนดหมายเลข ip address เองเท่านั้น (อยู่ในสภาพแวดล้อมแบบคงที่ หรือ static) ไม่สามารถนำไปใช้กับสภาพแวดล้อมที่เครื่องแม่ข่ายเป็นผู้แจกหมายเลข ip address ได้ (อยู่ในสภาพแวดล้อมที่ไม่คงที่ หรือ dynamic)

5.3 ปัญหาและอุปสรรคระหว่างการพัฒนาระบบ

- ปัญหาด้านการเขียนโปรแกรม

เนื่องจากผู้พัฒนาไม่มีประสบการณ์ในการเขียนโปรแกรมภาษา PHP มาก่อน ทำให้ต้องใช้เวลามากเป็นพิเศษในการศึกษาวิธีการเขียนโปรแกรม การใช้งานฟังก์ชันต่าง ๆ และเทคนิคในการผสมผสานกันระหว่าง PHP, Java Script และ Shell script

- ปัญหาด้านข้อจำกัดทางด้านเวลา

เนื่องจากผู้พัฒนาต้องทำงานไปด้วยและเรียนไปด้วย และในระหว่างที่ผู้พัฒนาได้ทำการพัฒนาระบบงานนี้ งานประจำที่ที่ผู้พัฒนาดูแลอยู่มีเพิ่มมากขึ้น และต้องเดินทางออกต่างจังหวัดบ่อยครั้ง ทำให้มีเวลาในการพัฒนาระบบน้อยลง ประกอบกับความเหนื่อยล้าจากงานประจำที่ทำอยู่ส่งผลทำให้ไม่สามารถพัฒนาระบบให้เสร็จได้ทันตามที่ได้ตั้งใจไว้

5.4 ข้อเสนอแนะ

ระบบที่พัฒนาขึ้นใหม่นี้ถือได้ว่าเสร็จสมบูรณ์ในระดับที่น่าพอใจ แต่ก็ยังมีบางส่วนที่สามารถพัฒนาต่อเพื่อให้ระบบมีประสิทธิภาพมากขึ้นได้ ตัวอย่างเช่น

- การปรับแต่ง ความสามารถของระบบฐานข้อมูล MYSQL เพราะจะช่วยเพิ่มประสิทธิภาพในการทำงาน หรือการค้นหาข้อมูลในฐานข้อมูลได้เร็วมากขึ้น
- การปรับแต่ง Apache Web Server ให้มีประสิทธิภาพมากขึ้น ทำให้ระบบการแสดงผลบน Web มีประสิทธิภาพมากขึ้น
- การออกแบบ Web Page และการจัดรูปแบบการนำเสนอข้อมูลใหม่ ทำให้ระบบมีความน่าใช้มากขึ้น และใช้งานสะดวกมากยิ่งขึ้น
- การปรับแต่งโปรแกรม เนื่องจากผู้เขียนไม่มีประสบการณ์ในการเขียนโปรแกรมภาษา PHP มาก่อนทำให้โปรแกรมบางฟังก์ชันการทำงาน อาจมีการทำงานที่ยุ่งยากซับซ้อน ซึ่งการปรับแต่ง จะทำให้ระบบมีความรวดเร็วในการประมวลผลมากขึ้น
- การเพิ่มฟังก์ชันการทำงานให้มากขึ้น เช่นการพัฒนาระบบให้สนับสนุนระบบเครือข่ายแบบ Dynamic (สนับสนุน DHCP)

บรรณานุกรม

กิตติมา เจริญหิรัญ .2546. **การวิเคราะห์และออกแบบระบบ.** กรุงเทพฯ : สำนักพิมพ์ท้อป.

กิติศักดิ์ เจริญโภคานนท์ . 2537. **คัมภีร์การสร้าง E-Commerce Application PHP 4.** กรุงเทพ: ซัคเซส มีเดีย.

สงกรานต์ ทองสว่าง .2544. **MySQL ระบบฐานข้อมูลสำหรับอินเทอร์เน็ต.** กรุงเทพฯ: ซีเอ็ดยูเคชั่น.

สมประสงค์ ธิตินิลนิธิ .2547. **เรียนลัด PHP 4 ครอบคลุม PHP เวอร์ชั่น 4.2.** กรุงเทพ: โปรวิชั่น.

DEFCON1 .2549. **IPFW How-to.** [Online].

Available: http://www.defcon1.org/htmll/NATD-config/firewall-setup/ipfw.html

ภาคผนวก ก

การติดตั้ง Apache Web Server version 2.2.3+mod ssl+Openssl-0.9.8b บน ระบบปฏิบัติการ FreeBSD

1. ทำการ Download Openssl จาก http://www.ssl.org/source/ หลังจากนั้นก็ทำการ อัพโหลดไปไว้ที่ Server โดยไว้ที่โฟลเดอร์ /temp/ เพื่อเก็บไฟล์

เมื่ออัปโหลดไปไว้เรียบร้อย ทำการขยายไฟล์ออกโดยใช้คำสั่ง ดังนี้

```
# gunzip openssl-0.9.8b.tar.gz
# tar -xvf openssl-0.9.8b.tar
```

หลังจากขยายไฟล์เรียบร้อย ในระบบจะสร้างโฟลเดอร์ชื่อ openssl-0.9.8b ให้เข้าไปที่โฟลเดอร์ openssl-0.9.8b เพื่อทำการ Config โดยจะใช้เวลาประมาณหนึ่งชั่วโมงขึ้นไป โดยใช้คำสั่ง

```
#cd openssl-0.9.8b
# ./config --prefix=/usr/local/ssl
# make
# make install
```

ถ้าทุกอย่างเรียบร้อยและไม่ติดปัญหาหรือ Error ใดๆ ก็ให้ไปแก้ไขที่ .profile ดังนี้

```
#vi .profile
export PATH=/usr/local/bin
export SSL_BASE=/usr/local/ssl
```

จากนั้นบันทึกแล้วเข้าไปที่โฟลเดอร์ ssl

```
#cd /usr/local/ssl
```

แล้ว copy ไฟล์ openssl ไปไว้ที่โฟลเดอร์ bin

```
#cp openssl /usr/local/bin
```

จากนั้นทำการทดสอบ openssl ว่าถูกต้องหรือไม่ โดยใช้คำสั่ง

#openssl

OpenSSL> version

OpenSSL 0.9.8b 04 May 2006

OpenSSL>exit

#

ถ้าแสดง Version ออกมาตามนี้ก็หมายความว่า ใช้งานได้ครับ

2. การติดตั้ง Apache Web Server version 2.2.3

ให้ไป Download Apache Web Server httpd-2.2.3.tar.gz จากเว็บ

http://httpd.apache.org/download.cgi

จากนั้นให้ทำการอัพโหลดไปไว้ที่ Server ในโฟลเดอร์ /temp/ หลังจากนั้นให้แตกไฟล์ออก โดยใช้คำสั่ง

gunzip -d httpd-2.2.2.tar.gz

tar -xvf httpd-2.2.2.tar

จากนั้นระบบจะสร้างโฟลเดอร์ httpd-2.2.3 หลังจากนั้น เริ่มทำการติดตั้งโดยการใช้คำสั่งดังต่อไปนี้

#cd httpd-2.2.3

#./configure --prefix=/usr/local/apache

--enable-ssl --enable-ssl=shared --with-ssl=/usr/local/ssl

--enable-status --enable-status=shared

--enable-module=so --enable-dso

--enable-info --enable-info=shared

--enable-module=so --enable-dso

พอเสร็จเรียบร้อยแล้วก็ใช้คำสั่ง

#make

ขั้นตอนสุดท้ายก็ใช้คำสั่ง

#make install

หลังจากติดตั้งและไม่มีข้อผิดพลาดใดๆ ก็ให้เข้าไปตรวจเช็ค Modules ว่ามีหรือไม่ที่

#cd /usr/local/apache/module

ls

httpd.exp mod_info.so mod_jk.so mod_ssl.so mod_status.so

หลังจากนั้นก็ให้เข้าแก้ไขไฟล์ httpd.conf ของ Apache Web Server

#cd /usr/local/apache/conf

#cp httpd.conf httpd.conf.org

#vi httpd.conf

เริ่มหาและตรวจเช็คพร้อมแก้ไขตามนี้ครับ

Listen 192.168.202.254:80

user nobody

Group nobody

ServerName 192.168.202.254:80

LoadModule ssl_module modules/mod_ssl.so

LoadModule status_module modules/mod_status.so

LoadModule info_module modules/mod_info.so

เสร็จเรียบร้อยแล้วก็บันทึกและทดสอบการทำงานของ Apache Web Server เช่น version และ configuration file ถ้าหากเรียบร้อยแล้วก็เริ่ม start apache

#./apachectl -version

Server version: Apache/2.2.3

Server built: Jul 26 2006 12:34:23

./apachectl configtest

Syntax OK

จากนั้นลองทำการ Start apache

#cd /usr/local/apache/bin

#./apachectl start

ในการตรวจสอบว่า Apache ทำงานได้หรือไม่ ถ้าได้ตามนี้

ps -ef|grep httpd

nobody 15762 49206 0 15:11:22 - 0:00 /usr/local/apache/bin/httpd -k start

nobody 29750 49206 0 15:11:21 - 0:00 /usr/local/apache/bin/httpd -k start

nobody 37110 49206 0 15:11:22 - 0:00 /usr/local/apache/bin/httpd -k start

root 49206 1 0 15:11:06 - 0:00 /usr/local/apache/bin/httpd -k start

nobody 50458 49206 0 15:11:51 - 0:00 /usr/local/apache/bin/httpd -k start

หลังจากนั้นทดสอบ โดยใช้ web browser ไปที่ http://192.168.202.254 ถ้าผ่านจะขึ้น It Work แสดงว่าใช้งานได้

การสร้าง Certificate เพื่อรับรองความปลอดภัย ต้องเริ่มด้วยการหยุด Apache Web Server ก่อนโดยใช้คำสั่ง

#cd /usr/local/apache/bin

#./apachectl stop

3. การสร้าง self-signed certificate ให้กับเว็บไซต์

เริ่มจากการสร้างโฟลเดอร์ให้เก็บไฟล์ certificate ให้อยู่ภายใต้โฟลเดอร์ของ Apache Web Server ดังนี้

#cd /usr/local/apache/conf/

#mv ssl

#cd ssl

#pwd

/usr/local/apache/conf/ssl

จากนั้นก็ใช้คำสั่ง openssl เพื่อทำการสร้าง certificate

#openssl

openssl> genrsa -des3 -out server.key 1024

openssl> rsa -in server.key -out server.key

openssl>openssl req -new -key server.key -out server.csr

ในขั้นตอนนี้จะมีการถามให้ใส่รายละเอียด เช่น ชื่อ ที่อยู่ อีเมล ที่อยู่เว็บ ซึ่งเป็นสิ่งสำคัญที่จะต้องตรงกับชื่อ hostname ที่เราตั้งตอนแรก

Common Name (eg, your name or your server's hostname) []: 192.168.202.254

openssl> x509 -req -days 365 -in server.csr -signkey server.key -out server.crt

เมื่อสร้างเรียบร้อยก็ใช้คำสั่ง exit ออกไปและลองตรวจสอบดูว่ามีไฟล์ที่ชื่อ server.csr server.key server.crt อยู่หรือไม่ถ้ามีอยู่ก็ถูกต้องและสามารถใช้งานได้

4. การ Config Apache Web Server ให้สนับสนุน SSL

เริ่มต้นจากการเข้าไปแก้ไฟล์ httpd.conf ใน Apache Web Server อีกครั้งหนึ่ง โดยใช้คำสั่ง

#cd /usr/local/apache/conf

#vi httpd.conf

แก้ไขข้อมูลในไฟล์ httpd.conf ให้เป็นดังนี้

Listen 192.168.202.254:443

ServerName 192.168.202.254:443

SSLEngine On

SSLCertificateFile /usr/local/apache/conf/ssl/server.crt

SSLCertificateKeyFile /usr/local/apache/conf/ssl/server.key

หลังจากที่ใส่และตรวจเช็คเรียบร้อยแล้วก็บันทึกและทำการทดสอบการทำงานของ certificate โดยการเริ่มบริการ Apache Web Server ใหม่

#cd /usr/local/apache/bin

#./apachectl start

จากนั้นก็ใช้เครื่อง Client เข้าไปที่ https://192.168.202.254 เพื่อตรวจสอบว่าใช้ได้หรือไม่ ถ้าหากไม่มีข้อผิดพลาดจะสามารถเข้าสู่หน้า Web Site ได้ตามปกติ และจะมีรูปกุญแจอยู่ด้านล่างขวาของจอ

ประวัติผู้เขียน

ชื่อ-นามสกุล	นายโอภาส ปัญญาชัยรักษา
วัน เดือน ปีเกิด	3 กันยายน 2522 ที่จังหวัดราชบุรี
ที่อยู่	80/377 ซ.ลาดพร้าว 58/1 ถ.ลาดพร้าว แขวงวังทองหลาง เขตวังทองหลาง กรุงเทพฯ 10310
ประวัติการศึกษา	2543. วิทยาศาสตรบัณฑิต สาขาวิชาคณิตศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ความชำนาญเฉพาะด้าน	1.) ระบบเครือข่าย 2.) ระบบความปลอดภัยข้อมูลสารสนเทศ
ประสบการณ์การทำงานและผลงานวิจัย	
พ.ศ. 2543	ตำแหน่งผู้ดูแลระบบบริษัท SolutionOne Telecom จำกัด
พ.ศ. 2544-2547	ตำแหน่งวิศวกรระบบเครือข่ายและข้อมูล บริษัท ทีเอชนิค จำกัด
พ.ศ. 2547-ปัจจุบัน	ตำแหน่งที่ปรึกษาด้านเทคนิคระบบความปลอดภัยของข้อมูล บริษัท เทลินคุส (ไทยแลนด์) จำกัด