ระบบบริหารจัดการเก็บและรักษาข้อมูลจราจรทางคอมพิวเตอร์ กรณีศึกษา สำนักงานบริการลูกค้า กสท เขตตะวันตก

โดย

นางทิพย์ศริน พรปิติเจริญ

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาเทคโนโลยีสารสนเทศ

ภาควิชาคอมพิวเตอร์

บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร

ปีการศึกษา 2553

ระบบบริหารจัดการเก็บและรักษาข้อมูลจราจรทางคอมพิวเตอร์ กรณีศึกษา สำนักงานบริการลูกค้า กสท เขตตะวันตก

โดย

นางทิพย์ศริน พรปิติเจริญ

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาเทคโนโลยีสารสนเทศ

ภาควิชาคอมพิวเตอร์

บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร

ปีการศึกษา 2553

NETWORK TRAFFIC DATA MANAGEMENT SYSTEM CASE STUDY CAT CUSTOMER SERVICE OFFICE - WESTERN REGION DEPARTMENT

By

Tipsrin Pornpiticharoen

An Independent Study Submitted in Partial Fulfillment of the Requirements for the Degree

MASTER OF SCIENCE

Department of Computing

Graduate School

SILPAKORN UNIVERSITY

2010

บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร อนุมัติให้การค้นคว้าอิสระเรื่อง “ ระบบบริหารจัดการเก็บและรักษาข้อมูลจราจรทางคอมพิวเตอร์ กรณีศึกษา สำนักงานบริการลูกค้า กสท เขตตะวันตก ” เสนอโดย นางทิพย์ศริน พรปิติเจริญ เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตร์มหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

…….....

(ผู้ช่วยศาสตราจารย์ ดร.ปานใจ ธารทัศนวงศ์)

คณบดีบัณฑิตวิทยาลัย

วันที่.....เดือน..... พ.ศ.....

อาจารย์ที่ปรึกษาการค้นคว้าอิสระ

รองศาสตราจารย์ ดร.จันทนา จันทราพรชัย

คณะกรรมการตรวจสอบการค้นคว้าอิสระ

..... ประธานกรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.ปานใจ ธารทัศนวงศ์)

...../...../.....

..... กรรมการ

(อาจารย์ ดร.ทัศนวรรณ ศูนย์กลาง)

...../...../.....

..... กรรมการ

(รองศาสตราจารย์ ดร.จันทนา จันทราพรชัย)

...../...../.....

49309314 : สาขาวิชาเทคโนโลยีสารสนเทศ
คำสำคัญ : ข้อมูลจราจรคอมพิวเตอร์/การพิสูจน์ตัวตน

ทิพย์ศริน พรปิติเจริญ : ระบบบริหารจัดการเก็บและรักษาข้อมูลจราจรทางคอมพิวเตอร์ กรณีศึกษา สำนักงานบริการลูกค้า กสท เขตตะวันตก. อาจารย์ที่ปรึกษาการค้นคว้าอิสระ : รศ.ดร.จันทนา จันทราพรชัย. 167 หน้า.

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อจัดทำระบบบริหารจัดการเก็บและรักษาข้อมูลจราจรทางคอมพิวเตอร์ให้รองรับตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร โดยใช้โปรแกรมรหัสเปิดมาประยุกต์เพื่อประหยัดงบประมาณและค่าใช้จ่ายในการต้องซื้อฮาร์ดแวร์หรือซอฟต์แวร์

ระบบที่ดำเนินการประกอบด้วย 3 ส่วน คือ ส่วนของผู้ใช้งาน ส่วนของผู้ดูแลระบบ และส่วนของผู้บริหาร ผู้วิจัยได้ติดตั้ง แก้ไข ปรับแต่ง เครื่องแม่ข่าย เพื่อกำหนดสิทธิ และอนุญาตให้ผู้มีสิทธิเข้าใช้งานระบบอินเทอร์เน็ตได้เท่านั้น กำหนดให้จัดเก็บข้อมูลการเข้าใช้งาน และส่งข้อมูลการเข้าใช้งานไปเก็บไว้ที่เครื่องแม่ข่ายอีกตัว เพื่อความปลอดภัยของข้อมูล โดยวิธีการส่งจะมีการรักษาความปลอดภัยของข้อมูล มีการปรับแต่งเวลาให้เป็นไปตามที่ประกาศกระทรวงฯ กำหนด ในส่วนของผู้ดูแลระบบ มีการจัดทำเป็นเว็บแอปพลิเคชั่น เพื่อให้ผู้ดูแลระบบง่ายต่อการใช้งาน นอกจากนี้ยังมีการนำข้อมูลการใช้งานมาจัดทำเป็นรายงานให้ผู้บริหาร สามารถดูรายงานการใช้งานต่าง ๆ

ผลการประเมินการทำงานของระบบ โดยประเมินจากผู้เข้าใช้งาน ผู้ดูแลระบบ ผู้บริหาร พบว่าคะแนนความพึงพอใจอยู่ระดับ 4.17 จากระดับ 5 ซึ่งอยู่ในระดับดีมาก ดังนั้นระบบที่พัฒนาขึ้นจึงสามารถช่วยให้สำนักงานฯ ดำเนินการได้ตามพระราชบัญญัติ และประกาศกระทรวงฯ โดยไม่ต้องจัดซื้อฮาร์ดแวร์และซอฟต์แวร์ใหม่ ทำให้ประหยัดค่าใช้จ่ายได้

ภาควิชาคอมพิวเตอร์ บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร ปีการศึกษา 2553

ลายมือชื่อนักศึกษา.....

ลายมือชื่ออาจารย์ที่ปรึกษาการค้นคว้าอิสระ .....

49309314 : MAJOR : INFORMATION TECHNOLOGY
KEY WORD : TRAFFIC DATA / IDENTIFICATION
TIPSRIN PORNPITICHAROEN : NETWORK TRAFFIC DATA MANAGEMENT SYSTEM CASE STUDY CAT CUSTOMER SERVICE OFFICE - WESTERN REGION DEPARTMENT. INDEPENDENT STUDY ADVISOR : ASSOC.PROF. CHANTANA CHANTRAPORNCHAI, Ph.D. 167 pp.

This research purpose is to develop the network traffic data management system. Support Act on Computer Crime 2007 according to the Announcement of Ministry of Information and Communication Technology. We applied the Open Source software for saving the budget.

The system includes three subsystems. The subsystems are the user subsystem, administration subsystem and executive subsystem. We had installed, edited and improved the server by setting the user privilege and authentication configuration and defining the accessed data and saving the data to another server following the security policy. The sending process has to encrypt the data and been improved to support the Announce of Ministry of Information and Communication Technology. The administrator uses the friendly user interface via the web application. The duties of administrators are to control the system, assign the privilege to users, and print the reports to the executives.

For evaluation, we have the users, administrators, and executives testing the usability of the system. It is found that satisfaction scores average level is 4.17 out of 5, which is very positive. Thus, the developed system can help the WEST CAT customer service office following this Act and Announcement of Ministry and help saving the budget by without purchasing the new hardware and software.

Department of Computing Graduate School, Silpakorn University Academic Year 2010
Student's signature .....
Independent Study Advisor's signature .....

กิตติกรรมประกาศ

การค้นคว้าอิสระฉบับนี้สำเร็จลงด้วยดี ด้วยความเมตตากรุณา ให้คำแนะนำ แนวทางในการทำการค้นคว้าอิสระ จากรองศาสตราจารย์ ดร.จันทนา จันทราพรชัย ซึ่งเป็นอาจารย์ที่ปรึกษา จึงขอกราบขอบพระคุณท่านไว้ ณ โอกาสนี้

ขอกราบขอบพระคุณ ประธานกรรมการสอบ ผู้ช่วยศาสตราจารย์ ดร.ปานใจ ธารทัศนวงศ์ กรรมการสอบ อาจารย์ ดร.ทัศนวรรณ ศูนย์กลาง

ขอขอบคุณ เพื่อนนักศึกษาปริญญาโท สาขาเทคโนโลยีสารสนเทศ รุ่นที่ 4 และผู้มีส่วนเกี่ยวข้องทุกท่าน ที่ให้ความช่วยเหลือในการจัดทำการค้นคว้าอิสระครั้งนี้

ขอขอบคุณ คุณศรนันท์ จันทร์หา คุณสหัส จวอรรถ คุณธิติมา ทองเวียงจันทร์ พนักงานสำนักงานบริการลูกค้า กสท เขตตะวันตก ที่ช่วยในการทดสอบระบบ ช่วยในการให้คำแนะนำ ต่าง ๆ

ขอขอบคุณผู้บริหาร พนักงานและลูกจ้าง สำนักงานบริการลูกค้า กสท เขตตะวันตก ที่ให้ความร่วมมือ อนุญาตให้ติดตั้ง และเข้าใช้งานระบบ

นอกจากนี้ผู้วิจัยขอขอบพระคุณ คุณพ่อ คุณแม่ และลูก ๆ ที่เป็นกำลังใจให้เสมอมา

สารบัญ

บทที่ หน้า

สารบัญตาราง

สารบัญภาพ

ภาพที่ หน้า

ภาพที่ หน้า

บทที่ 1
บทนำ

ความเป็นมาและความสำคัญของปัญหา

ตามที่ พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ประกาศในราชกิจจานุเบกษาเมื่อ 18 มิถุนายน 2550 มีผลบังคับใช้ตั้งแต่ 18 กรกฎาคม 2550 มีบทว่าด้วยการกระทำความผิด และบทกำหนดโทษในการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในมาตราต่าง ๆ แต่มีส่วนที่เกี่ยวข้องกับหน่วยงานสำนักงานบริการลูกค้า กสท เขตตะวันตก บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ดังต่อไปนี้

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กำหนดให้

ผู้ให้บริการ หมายความว่า ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

ตามความหมายข้างต้น ถือว่าสำนักงานบริการลูกค้า กสท เขตตะวันตก บริษัท กสท โทรคมนาคม จำกัด (มหาชน) เป็นผู้ให้บริการ เนื่องจากได้มีการให้บริการแก่พนักงานและลูกจ้างในการเข้าสู่อินเทอร์เน็ต จึงต้องดำเนินการตาม

มาตรา 26 ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ ผู้ให้บริการผู้ใด เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวัน แต่ไม่เกินหนึ่งปี เป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้ ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ต้องระวางโทษปรับไม่เกินห้าแสนบาท

มาตรา 27 ผู้ใดไม่ปฏิบัติตามคำสั่งของศาลหรือพนักงานเจ้าหน้าที่ที่สั่งตามมาตรา 18 หรือมาตรา 20 หรือไม่ปฏิบัติตามคำสั่งของศาลตามมาตรา 21 ต้องระวางโทษปรับไม่เกินสองแสนบาท และปรับเป็นรายวันอีกไม่เกินวันละห้าพันบาทจนกว่าจะปฏิบัติให้ถูกต้อง

นอกจากนี้ สำนักงานบริการลูกค้า กสท เขตตะวันตก ต้องมีการเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ ตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 ประกาศในราชกิจจานุเบกษา เมื่อ 23 สิงหาคม 2550 โดยมีรายละเอียดในส่วนที่ต้องเก็บตามประกาศฯ ดังนี้

ในการเก็บรักษาข้อมูลจราจรฯ ให้ผู้ให้บริการเก็บเพียงเฉพาะในส่วนที่เป็น ข้อมูลจราจร ที่เกิดจากส่วนที่เกี่ยวข้องกับบริการของตนเท่านั้น โดย

การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ผู้ให้บริการต้องใช้วิธีการที่มั่นคง ปลอดภัย ดังต่อไปนี้

1. เก็บในสื่อ (Media) ที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง (Integrity) และ ระบุตัวบุคคล (Identification) ที่เข้าถึงสื่อดังกล่าวได้

2. มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการ เข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เช่น การเก็บไว้ใน Centralized Log Server หรือการทำ Data Archiving หรือทำ Data Hashing เป็นต้น เว้นแต่ ผู้มีหน้าที่เกี่ยวข้องที่เจ้าของหรือ ผู้บริหารองค์กรกำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบระบบ สารสนเทศขององค์กร (IT Auditor) หรือบุคคลที่องค์กรมอบหมาย เป็นต้น รวมทั้ง พนักงาน เจ้าหน้าที่ตามพระราชบัญญัตินี้

3. จัดให้มีผู้มีหน้าที่ประสานงานและให้ข้อมูลกับพนักงานเจ้าหน้าที่ซึ่งได้รับการ แต่งตั้ง ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่อให้การส่งมอบข้อมูลนั้น เป็นไปด้วยความรวดเร็ว

4. ในการเก็บข้อมูลจราจรนั้น ต้องสามารถระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้ (Identification and Authentication) เช่น ลักษณะการใช้บริการ Proxy Server, Network Address Translation (NAT) หรือ Proxy Cache หรือ Cache Engine หรือบริการ Free Internet หรือ บริการ 1222 หรือ Wi-Fi Hotspot ต้องสามารถระบุตัวตนของผู้ใช้บริการเป็นรายบุคคลได้จริง

5. ในกรณีที่ผู้ให้บริการประเภทหนึ่งประเภทใด ในข้อ 1 ถึงข้อ 4 ข้างต้น ได้ให้บริการ ในนามตนเอง แต่บริการดังกล่าวเป็นบริการที่ใช้ระบบของผู้ให้บริการซึ่งเป็นบุคคลที่สาม เป็นเหตุให้ผู้ให้บริการในข้อ 1 ถึงข้อ 4 ไม่สามารถรู้ได้ว่า ผู้ใช้บริการที่เข้ามาในระบบนั้นเป็นใคร ผู้ให้บริการเช่นว่านั้นต้องดำเนินการให้มีวิธีการระบุ และยืนยันตัวบุคคล (Identification and Authentication) ของผู้ใช้บริการผ่านบริการของตนเองด้วย

เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริงผู้ให้บริการ ต้องตั้งนาฬิกา ของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดย ผิดพลาดไม่เกิน 10 มิลลิวินาที

จากพระราชบัญญัติฯ และประกาศกระทรวงฯ ข้างต้น ทำให้ สำนักงานบริการลูกค้า กสท เขตตะวันตก รวมถึงหน่วยงานและองค์กรต่าง ๆ ต้องปฏิบัติตาม ทั้งนี้ในการปฏิบัติตามนี้ หน่วยงานหรือองค์กร ต้องมีการซื้อ ฮาร์ดแวร์ หรือ ซอฟต์แวร์ ที่บริษัทเอกชนต่าง ๆ ผลิตขึ้นมาจำหน่าย ซึ่งมีราคาสูงมาก คือมีราคาตั้งแต่ สองแสน ถึงหลายล้านบาท แล้วแต่ Application ต่าง ๆ ที่จะนำเสนอ ปัญหาจึงเกิดขึ้นกับหน่วยงานที่ไม่มีงบประมาณดังกล่าว เนื่องจากผู้บริหารหน่วยงานไม่ทราบถึงความสำคัญและบทลงโทษของพระราชบัญญัติฯ และประกาศกระทรวงฯ ดังกล่าว หรือผู้บริหารบางหน่วยงานอาจจะทราบถึงความสำคัญและบทลงโทษ แต่ไม่สามารถหางบประมาณมาดำเนินการได้ ซึ่ง สำนักงานบริการลูกค้า กสท เขตตะวันตก ก็เป็นหน่วยงานหนึ่ง ที่ประสบปัญหา คือไม่มีงบประมาณเพียงพอที่จะซื้อ ฮาร์ดแวร์ หรือ ซอฟต์แวร์ ราคาหลักแสน และหลักล้าน ที่ บริษัทเอกชนต่าง ๆ มานำเสนอ อีกทั้งต้องการหาวิธีการที่จะสามารถจัดเก็บข้อมูลจราจรได้ตามพระราชบัญญัติ โดยใช้งบประมาณน้อยที่สุด เพื่อเป็นแนวทางหนึ่งในการให้คำแนะนำแก่ลูกค้าของสำนักงานบริการลูกค้า กสท เขตตะวันตก ได้

ผู้วิจัย จึงคิดศึกษาและหาวิธีการในการจัดเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ของสำนักงานบริการลูกค้า กสท เขตตะวันตก โดยใช้โปรแกรมรหัสเปิด เช่น Linux , Freeradius และ Chillispot มาประยุกต์ใช้งาน โดยจัดทำระบบ Identification and Authentication เพื่อให้สามารถระบุ รายละเอียดผู้ใช้บริการเป็นรายบุคคลได้ และจัดทำ Centralized Log Server เพื่อเก็บรักษา ความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูล เพื่อรักษาความน่าเชื่อถือ ของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้ ทั้งนี้โดยใช้ คอมพิวเตอร์ส่วนบุคคล หรือ เครื่องแม่ข่าย ที่มีอยู่ในสำนักงานบริการลูกค้า กสท เขตตะวันตก โดยไม่ต้อง เสียเงินซื้อ ฮาร์ดแวร์ หรือ ซอฟต์แวร์ ราคาแพง

วัตถุประสงค์การวิจัย

1. เพื่อปรับปรุงระบบการใช้งานอินเทอร์เน็ต ของ สำนักงานบริการลูกค้า กสท เขตตะวันตก ให้รองรับ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับ คอมพิวเตอร์ พ.ศ.2550 และประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

2. เพื่อประหยัดงบประมาณและค่าใช้จ่ายในการต้องซื้อ ฮาร์ดแวร์ หรือ ซอฟต์แวร์จากบริษัทเอกชน

3. เพื่อให้ผู้บริหารสามารถนำข้อมูลจราจรทางคอมพิวเตอร์ที่ได้มาใช้ประโยชน์ในการ วิเคราะห์การใช้งานอินเทอร์เน็ตของพนักงาน และลูกจ้าง โดยผู้ดูแลระบบสามารถ จัดทำรายงาน การใช้งานอินเทอร์เน็ตของผู้ใช้รายบุคคล และสามารถค้นหาเพื่อดูรายงานการใช้งานตามปฏิทิน

4. เพื่อให้ผู้บริหารมีข้อมูลในการปรับเพิ่มความเร็ว หรือปรับลดความเร็วในการให้บริการอินเทอร์เน็ตแก่พนักงานและลูกจ้าง โดยดูรายงานปริมาณการใช้งานจากกราฟ

5. สามารถกำหนดสิทธิในการใช้งานอินเทอร์เน็ตของพนักงานและลูกจ้างแต่ละคนได้ หรือสามารถกำหนดการใช้งานเป็นกลุ่มงานได้ อีกทั้งป้องกันการใช้งานโดยผู้ไม่ประสงค์ดี ระบบจะสั่งให้ตัดการใช้งานเมื่อไม่มีการใช้งานได้

สมมติฐานการวิจัย

ระบบพิสูจน์ตัวตนและควบคุมสิทธิการใช้บริการอินเทอร์เน็ต (Identification and Authentication) สามารถช่วยให้ผู้ให้บริการอินเทอร์เน็ต บริหารความมั่นคงปลอดภัยของระบบเครือข่าย งานวิจัยเชิงพัฒนานี้มุ่งเน้นที่จะพัฒนาซอฟต์แวร์จากซอฟต์แวร์โอเพนซอร์สซึ่งเป็นการพัฒนาต่อยอดหรือการนำฟรีซอฟต์แวร์หลาย ๆ ตัวมาใช้งานร่วมกันเพื่อให้เกิดประโยชน์แก่องค์กร

ระบบจัดเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ (Centralized Log Server) ปรับปรุงจาก ubuntu ทำงาน 2 หน้าที่ คือ Log และ Time Server ส่วน Time Server ใช้โปรแกรม NTP (Network Time Protocol)

ข้อมูลจราจรทางคอมพิวเตอร์ที่ได้จากการจัดเก็บ สามารถนำมาทำเป็น รายงานให้ผู้ผู้บริหาร ทราบได้ว่าพนักงานและลูกจ้าง มีการใช้งานอินเทอร์เน็ตเพื่อประโยชน์ขององค์กรมากน้อยเพียงใด ผู้บริหารสามารถแจ้งให้ ผู้ดูแลระบบกำหนดสิทธิว่าจะให้พนักงานและลูกจ้างคนใดใช้งาน อินเทอร์เน็ตได้จำนวนกี่ชั่วโมงต่อวัน ต่อเดือน หรือกำหนดสิทธิการใช้งานเป็นกลุ่ม/ส่วนงาน เพื่อประโยชน์ในการบริหารจัดการความเร็วอินเทอร์เน็ตที่มีอยู่ให้มีประสิทธิภาพสูงสุด

ประโยชน์ที่คาดว่าจะได้รับ

1. ได้ระบบ Login และควบคุมสิทธิการใช้งานอินเทอร์เน็ต ของพนักงานและลูกจ้าง ในสำนักงานบริการลูกค้า กสท เขตตะวันตก ระบุรายละเอียดได้ว่าผู้ใช้บริการเป็นใคร ทำอะไร ที่ไหน เมื่อไร อย่างไร

2. ช่วยประหยัดค่าใช้จ่ายและงบประมาณ ในการจัดซื้ออุปกรณ์ราคาแพง

3. สามารถถ่ายทอดความรู้ และแนะนำวิธีในการจัดทำระบบพิสูจน์ตัวตน และควบคุมสิทธิการใช้งานอินเทอร์เน็ต (Identification and Authentication) ระบบ Centralized Log Server และ Network Time Protocal Server (NTP Server) ให้แก่ลูกค้าของสำนักงานบริการลูกค้า กสท เขตตะวันตก เพื่อช่วยลูกค้าให้ปฏิบัติให้ถูกต้องตามพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และประกาศกระทรวงเทคโนโลยี สารสนเทศและการสื่อสาร เพื่อสร้างความสัมพันธ์ ที่ดีในการให้บริการแก่ลูกค้า

4. ผู้บริหารสามารถกำหนดให้พนักงาน/ลูกจ้าง ใช้งานอินเทอร์เน็ตให้เกิดประสิทธิภาพสูงสุด ผู้บริหารสามารถใช้รายงานเป็นข้อมูลในการของบประมาณเพื่อเพิ่มความเร็วอินเทอร์เน็ต ให้แก่พนักงาน/ลูกจ้าง

ขั้นตอนการศึกษา

1. ศึกษาและทำความเข้าใจเกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

2. ศึกษาและทดลองใช้โปรแกรมซอฟต์แวร์โอเพนซอร์ส ต่าง ๆ เช่น ubuntu , Freeradius และ Chillispot ที่คิดว่าจะสามารถนำมาจัดทำระบบพิสูจน์ตัวตน และควบคุมสิทธิการใช้งานอินเทอร์เน็ต ระบบ Centralized Log Server และ Network Time Protocal Server (NTP Server)

3. รวบรวมข้อมูลรายละเอียดการจัดทำระบบบริหารจัดการเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ ระบบพิสูจน์ตัวตนจากหนังสือ เอกสารและงานวิจัยที่เกี่ยวข้อง

4. หาข้อมูลเว็บแอปพลิเคชั่นฟรี เพื่อมาประยุกต์ทำหน้าเว็บสำหรับ Login และควบคุมสิทธิการใช้งานอินเทอร์เน็ตของพนักงานและลูกจ้างของสำนักงานบริการลูกค้า กสท เขตตะวันตก จัดเก็บข้อมูลการเข้าใช้ รายละเอียดการปิดเปิดพอร์ต การใช้งาน การจำกัดการใช้งาน ออกรายงานสรุปการใช้งานเครือข่าย

5. ขออนุญาตผู้บริหารสำนักงานบริการลูกค้า กสท เขตตะวันตก ติดตั้งระบบ และให้พนักงานและลูกจ้างใช้งานอินเทอร์เน็ตโดยผ่านระบบที่จัดทำขึ้น

6. ประเมินผลการใช้งานของพนักงานและลูกจ้างในสำนักงานบริการลูกค้า กสท เขตตะวันตก ว่าสามารถใช้งานอินเทอร์เน็ตได้ตามปกติ ไม่มีผลเสียต่อการใช้งานอินเทอร์เน็ตที่เคยใช้ โดยใช้แบบสอบถามกับพนักงานกลุ่มตัวอย่างและผู้บริหาร

ขอบเขตของการศึกษา

ออกแบบ พัฒนา ปรับปรุงระบบบริหารจัดการเก็บและรักษาข้อมูลจราจรทางคอมพิวเตอร์ของสำนักงานบริการลูกค้า กสท เขตตะวันตก ให้รองรับตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร โดยมีขอบเขตดังนี้

1. จัดทำระบบ Login และควบคุมสิทธิการใช้งานอินเทอร์เน็ต (Identification and Authentication) ในการเข้าใช้งานอินเทอร์เน็ตของพนักงานและลูกจ้างในสำนักงาน บริการลูกค้า กสท เขตตะวันตก ทำให้สามารถระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้ ทั้งนี้โดยทำเป็นเว็บแอปพลิเคชั่น และจัดทำระบบฐานข้อมูลเก็บข้อมูลการเข้าใช้งาน ในรายละเอียดพอร์ตการใช้งาน งานประยุกต์ที่ใช้จัดทำข้อมูลการใช้งานแต่ละเครื่อง การปิดเปิดพอร์ตการใช้งาน และจำกัดการใช้งาน

2. จัดทำ Centralized Log Server ใช้เก็บข้อมูลในการใช้งานของแต่ละบุคคล โดยสามารถบอกได้ว่า ใครเป็นผู้ใช้งาน เวลาที่ใช้งาน บริการที่ใช้งาน เช่น ดูเว็บ ส่งเมล์ ส่งไฟล์ สนทนา หมายเลข IP Address ของเครื่องคอมพิวเตอร์ที่ใช้งาน หมายเลข Port ที่ให้บริการ โดยข้อมูลต้องส่งไปเก็บไว้ที่ Centralized Log Server ทั้งนี้ ระบบ Centralized Log Server จะเป็นเครื่องแม่ข่ายที่เก็บข้อมูล Log จาก Identification and Authentication Server , Wifi , Hotspot ที่มีในระบบ และการเก็บ Log ของระบบ Centralized Log Server ต้องมีการ encrypt หรือวิธีการอื่นที่จะป้องกันไม่ให้ผู้อื่นเข้ามาเปลี่ยนแปลงแก้ไขข้อมูลใด ๆ ได้ เมื่อครบกำหนด 90 วัน จะต้องมีการจัดเก็บข้อมูลล็อกไว้ในสื่อบันทึกข้อมูลชนิดเขียนได้อย่างเดียว โดยไม่สามารถแก้ไขใด ๆ ได้ มีการตรวจสอบความถูกต้องครบถ้วนของข้อมูลในสื่อบันทึกข้อมูล กำหนดมาตรการป้องกันการเข้าถึงข้อมูลล็อกบน Centralized Log Server ให้รัดกุมและปลอดภัย โดยมีการบันทึกการเข้าถึงข้อมูลล็อกทุกครั้ง

3. จัดทำ Network Time Protocal Server (NTP Server) ในการตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน 10 มิลลิวินาที

4. เชื่อมต่อ ระบบ LOGIN (Identification and Authentication Server) , Centralized Log Server และ NTP Server เข้ากับระบบอินเทอร์เน็ตปัจจุบัน

5. นำข้อมูลจราจรทางคอมพิวเตอร์ที่ได้จากการจัดเก็บในแต่ละวันมาทำเป็นรายงานเสนอผู้บริหารแสดงการใช้งานของแต่ละคนเพื่อให้ผู้บริหารสามารถวิเคราะห์ได้ว่า ควรมีการปรับเพิ่มความเร็วในการใช้งาน หรือปรับลดความเร็วในการใช้งาน เพื่อประหยัดค่าใช้จ่ายขององค์กรหรือไม่

6. ประเมินผลการพัฒนาด้วยแบบสอบถามจากผู้ใช้งาน และผู้บริหาร

เครื่องมือที่ใช้ในการวิจัย

1. ฮาร์ดแวร์
   - 1.1 คอมพิวเตอร์
     - 1.1.1 Intel CPU Core 2 Duo
     - 1.1.2 Ram 1024 MB
     - 1.1.3 Hard disk 250 GB
     - 1.1.4 Gigabit Ethernet + 1 Cards 10/100 FastEthernet
   - 1.2 Router
   - 1.3 Switch
2. ซอฟต์แวร์
   - 2.1 ระบบปฏิบัติการ : ubuntu , Freeradius , Chillispot
   - 2.2 ระบบฐานข้อมูล : MySQL Version 5.0.67
   - 2.3 เครื่องมือในการพัฒนา : PHP Version 5

นิยามศัพท์เฉพาะ

1. Identification and Authentication Server เป็นเซิร์ฟเวอร์ให้บริการการพิสูจน์ตัวตน และการเข้าถึงข้อมูลผู้ใช้ด้วยโปรโตคอล Lightweight Directory Access Protocol หรือ LDAP เช่น Microsoft Active Directory หรือ Novell E-Directory เป็นต้น หรือความสามารถ

ทางด้าน Single Sign-on เพิ่มเติม รวมถึงการพิสูจน์ตัวตนด้วย โปรโตคอล RADIUS หรือ TACAT+ เช่น FreeRadius หรือ Funk ด้วย ข้อมูลล็อกที่พบได้ เช่นล็อกของการพิสูจน์ตัวตน ซึ่งบันทึกข้อมูล บัญชีผู้ใช้ รหัสผ่าน สถานะการ พิสูจน์ตัวตน วันเวลา เป็นต้น

2. ข้อมูลจราจร หรือ Traffic data หมายถึงข้อมูลที่เกิดขึ้นในระบบคอมพิวเตอร์ เช่น ข้อมูลในเครื่อง web server ที่เกิดจากการเข้าถึงข้อมูลโดยผู้เข้าเยี่ยมชมweb site เป็นต้น โดยปกติแล้วข้อมูลดังกล่าวนิยมเรียกกันโดยทั่วไปว่า log file ซึ่งระบบคอมพิวเตอร์ มักจะเก็บ log file ไว้ในเครื่องซึ่ง log file ดังกล่าวอาจถูกเขียนข้อมูลทับในระยะเวลา ไม่ถึง 90วัน ตามที่กฎหมายกำหนด และ log file อาจถูกแก้ไขโดย system admin หรือถูกลบโดยแฮกเกอร์ก็มีความเป็นไปได้สูง ดังนั้นประกาศกระทรวงฯ จึงมีข้อ กำหนดวิธีการเก็บ log file อย่างถูกต้อง

3. Centralized Log Server เป็นการเก็บบันทึก ล็อก แบบรวมศูนย์ โดยจัดทำล็อกเซิร์ฟเวอร์ เพื่อเก็บข้อมูลแบบ Secondary Logging เพื่อให้สามารถบริหารจัดการ และควบคุมการเข้าถึงข้อมูลล็อกที่ ล็อกเซิร์ฟเวอร์จากศูนย์กลาง และทำให้มี ความมั่นคงปลอดภัยมากยิ่งขึ้น ทั้งนี้การบันทึกข้อมูล ล็อกบนตัวระบบเองเรียกว่า Primary Logging หรือการบันทึกข้อมูลล็อกแบบปฐมภูมิ และการส่งข้อมูลล็อกไป บันทึก หรือจัดเก็บ ที่ล็อกเซิร์ฟเวอร์เรียกว่า Secondary Logging หรือการบันทึก ข้อมูลล็อก แบบทุติยภูมิ ทำหน้าที่หลักในการจัดเก็บข้อมูลล็อก สำรองข้อมูลล็อก มีระบบป้องกันการเข้าถึงหรือควบคุมการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต อาจมีความสามารถในการวิเคราะห์ข้อมูลล็อกรวมถึงบริหารจัดการข้อมูลล็อกชั้นสูงอื่น ๆ

4. Network Time Protocal (NTP) เป็นโพรโตคอลในระดับ Application Layer ของระบบเครือข่ายแบบ TCP/IP ที่ทำหน้าที่ในการเทียบเวลาระหว่างอุปกรณ์ คอมพิวเตอร์ ซึ่งอ้างอิงจาก RFC หมายเลข RFC 778, RFC 891, RFC 956, RFC 958, และ RFC 1305 การทำงานของโพรโตคอลชนิดนี้จะต้องอาศัย เครื่องให้บริการที่เปิด พอร์ตหมายเลข 123 ชนิด UDP ในการรอรับข้อมูลร้องขอการเทียบเวลาจากเครื่อง ลูกข่าย ลักษณะการแจกจ่ายเวลาของ NTP นั้นจะอยู่ในรูปแบบลำดับชั้น ที่เรียกว่า “Clock Strata” ดังภาพที่ 1 โดยแบ่งลำดับชั้นของการเทียบเวลาดังนี้

4.1 Stratum 0

เป็นอุปกรณ์ของแหล่งกำเนิดเวลา เช่น Atomic clocks, GPS เป็นต้น ซึ่งอุปกรณ์แต่ละ ชนิดมีข้อดีและข้อเสียแตกต่างกัน เช่น การประยุกต์ใช้ GPS จะมีต้นทุนที่ต่ำกว่า Atomic clock มาก แต่จะมีเสถียรภาพที่น้อยกว่า หากสภาพอากาศไม่เหมาะสม GPS จะไม่สามารถรับสัญญาณดาวเทียมได้ เป็นต้น

4.2 Stratum 1

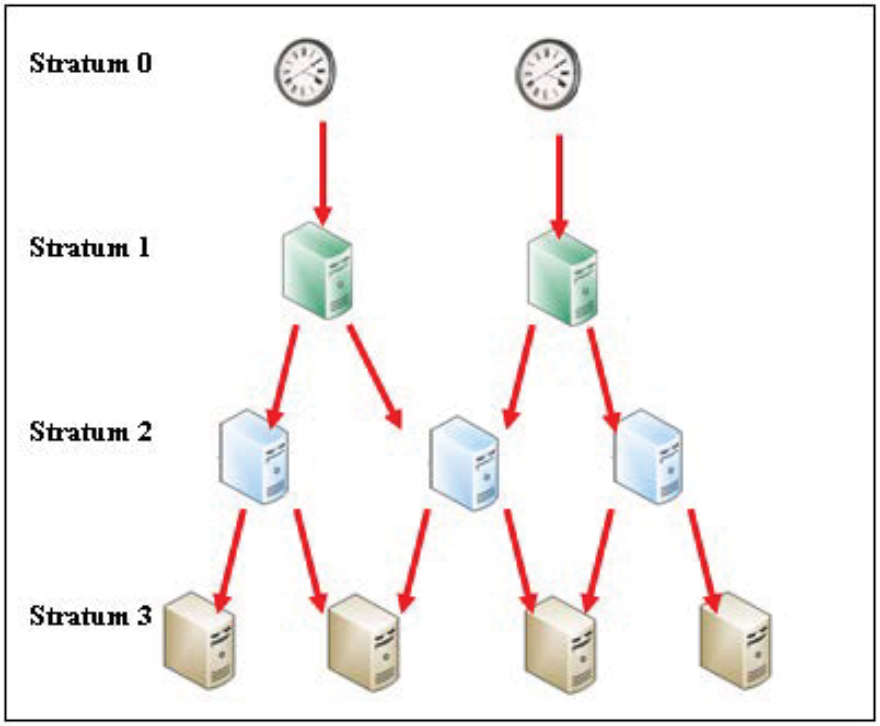
เป็นเครื่องคอมพิวเตอร์แม่ข่ายที่เชื่อมต่อกับ stratum 0 ได้รับค่าเวลามาจาก stratum 0 โดย ตรง ผ่านการเชื่อมต่อในระบบคอมพิวเตอร์ เช่น RS-232 เป็นต้น

4.3 Stratum 2

เป็นเครื่องคอมพิวเตอร์ที่ร้องขอการเทียบเวลาจากเครื่องคอมพิวเตอร์แม่ข่าย stratum 1 ผ่านระบบเครือข่าย TCP/IP ด้วยการใช้งาน NTP เครื่องคอมพิวเตอร์ในระดับนี้ อาจจะร้องขอการเทียบเวลาจาก stratum 1 ได้มากกว่า 1 แหล่งเพื่อรองรับการทำงานแบบ ทดแทน กัน เมื่อไม่สามารถเข้าถึง stratum 1 ตัวใดตัวหนึ่งก็จะสามารถร้องขอการเทียบเวลาจาก stratum 1 ตัวอื่นได้ต่อไป นอกจากนี้เครื่องคอมพิวเตอร์ใน stratum 2 สามารถ เทียบเคียง เวลาระหว่างกันแบบ peer-to-peer เพื่อรักษาเวลาให้เทียบเท่ากันในระดับเดียวกัน

4.4 Stratum 3

เป็นเครื่องคอมพิวเตอร์ที่ร้องขอการเทียบเวลาจากเครื่องคอมพิวเตอร์แม่ข่าย stratum 2 ผ่านระบบเครือข่าย TCP/IP ด้วยการใช้งาน NTP เครื่องคอมพิวเตอร์ในระดับนี้จะสามารถ อ้างอิง stratum 2 ได้มากกว่า 1 แหล่ง และสามารถทำงานในรูปแบบ peer-to-peer ได้เช่น เดียวกัน NTP นั้นสามารถรองรับระดับของการเทียบเวลาได้ถึง 16 ระดับ



ภาพที่ 1 ลำดับชั้นของการเทียบเวลาใน NTP

ที่มา : สถาบันมาตรวิทยาแห่งชาติ. NTP (Network Time Protocol) [ออนไลน์], เข้าถึงเมื่อ 28 กันยายน 2551. เข้าถึงได้จาก http://www.nimt.or.th/

4.5 การประยุกต์ใช้งาน NTP

รูปแบบการทำงานของ NTP จะอยู่ในลักษณะของ Server-Client ซึ่ง Server จะทำหน้าที่ แจกจ่ายเวลาให้กับ Client ที่อยู่ในระดับ stratum ที่ต่ำกว่า แนวทางการเทียบเวลาให้สอดคล้องกับ พรบ. คือการกำหนดให้ Client ภายในเครือข่ายขององค์กรขอเทียบเวลาจากเครื่องให้บริการ NTP ในระดับ stratum 1 ซึ่งในปัจจุบันมีเครื่องให้บริการขอเทียบเวลาในรูปแบบ NTP อยู่มากมาย เช่น NTP pool Project, Stratum One Time Server Project เป็นต้น

บทที่ 2
เอกสารและงานวิจัยที่เกี่ยวข้อง

การศึกษาเพื่อทำระบบบริหารจัดการ เก็บและรักษาข้อมูลจราจรทางคอมพิวเตอร์ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กรณีศึกษาสำนักงานบริการลูกค้า กสท เขตตะวันตก บริษัท กสท โทรคมนาคมจำกัด (มหาชน) นั้น ผู้วิจัยได้ศึกษาเอกสารและงานวิจัยที่เกี่ยวข้อง ซึ่งสรุปสาระสำคัญได้ ดังนี้

1. ที่มาของระบบบริหารจัดการ เก็บและรักษาข้อมูลจราจรทางคอมพิวเตอร์
2. ระบบอินเตอร์เน็ตของสำนักงานบริการลูกค้า กสท เขตตะวันตก
3. แนวคิดเกี่ยวกับระบบบริหารจัดการ เก็บและรักษาข้อมูลจราจรทางคอมพิวเตอร์
4. ทฤษฎีที่เกี่ยวข้อง
5. งานวิจัยที่เกี่ยวข้อง

1. ที่มาของระบบบริหารจัดการ เก็บและรักษาข้อมูลจราจรทางคอมพิวเตอร์

ที่ผ่านมาการติดตามและตรวจสอบพยานหลักฐานที่เกี่ยวข้องกับระบบคอมพิวเตอร์ในประเทศไทย หรือนำข้อมูลการบันทึกเหตุการณ์ที่เกิดขึ้นบนระบบคอมพิวเตอร์ไม่สามารถทำได้โดยตรง หรือไม่สามารถกำหนดให้ผู้ที่เกี่ยวข้องเก็บข้อมูลการเข้าถึงระบบคอมพิวเตอร์ที่จำเป็นได้ ยกตัวอย่าง เช่น เมื่อพบว่ามีผู้กระทำความผิดโดยใช้ระบบคอมพิวเตอร์ ผ่านร้านอินเทอร์เน็ตคาเฟ่ในการเข้าถึงระบบคอมพิวเตอร์เซิร์ฟเวอร์ของผู้อื่นโดยไม่ได้รับอนุญาต ซึ่งเมื่อมีการสอบสวนหรือต้องการหลักฐานเพิ่มเติมกลับพบว่าไม่สามารถติดตามข้อมูลการใช้งานอินเทอร์เน็ต ตั้งแต่ร้านอินเตอร์เน็ตคาเฟ่ ผู้ให้บริการอินเทอร์เน็ต หรือ Internet Service Provider (ISP) เพื่อนำข้อมูลมาวิเคราะห์ได้ ซึ่งเจ้าหน้าที่พนักงานจำเป็นต้องหามาตรการอื่นที่ไม่เกี่ยวข้องกับเทคโนโลยีในการสืบสวนพยานหลักฐาน

นอกจากนี้ยังพบว่าเมื่อมีคดีความที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทั้งที่ผู้กระทำความผิดใช้ระบบคอมพิวเตอร์โดยตรงเพื่อกระทำความผิด หรือทางอ้อม ยังไม่มีบทบัญญัติที่ชัดเจน

ว่าจะดำเนินคดีในลักษณะใด ซึ่งพนักงานเจ้าหน้าที่ที่เกี่ยวข้องจำเป็นต้องอ้างอิงด้วยกฎหมายฉบับอื่น เช่น กฎหมายลักษณะความอาญาเพื่อวิเคราะห์ประกอบพยานหลักฐาน เป็นต้น

ข้อมูลจากศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย (ThaiCERT) ภายใต้ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) ที่ผ่านมาเมื่อมีการรับมือเหตุการณ์ละเมิดความมั่นคงปลอดภัยคอมพิวเตอร์ภายในประเทศไทย การทำหน้าที่ประสานงาน ระหว่าง ผู้ที่แจ้งเหตุการณ์ละเมิดความมั่นคงปลอดภัยและผู้ที่เกี่ยวข้อง จำเป็นต้องใช้ข้อมูลที่บันทึกในระบบคอมพิวเตอร์เพื่อวิเคราะห์หาสาเหตุ ที่มาของผู้ละเมิดความมั่นคงปลอดภัย รวมถึงข้อมูลที่จำเป็นเพิ่มเติม ซึ่งบ่อยครั้งพบว่ามีข้อมูลที่ไม่เพียงพอ โดยเฉพาะเมื่อมีการติดตามข้อมูลเพิ่มเติมจากผู้ดูแลระบบเครือข่ายภายในองค์กร หรือผู้ให้บริการอินเตอร์เน็ตภายในประเทศ

จากการประกาศใช้ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งมีจุดมุ่งหมายเพื่อบัญญัติการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์ กำหนดแนวปฏิบัติในทิศทางเดียวกันสำหรับผู้ที่เกี่ยวข้องกับระบบสารสนเทศหรือระบบคอมพิวเตอร์ และกำหนดให้ ต้องมีการเก็บข้อมูลที่บันทึกเหตุการณ์ที่เกิดขึ้นบนระบบคอมพิวเตอร์ ข้อมูลดังกล่าวนี้ได้นิยามว่าเป็น “ข้อมูลจราจรคอมพิวเตอร์” และ “ข้อมูลผู้ใช้บริการ” และเพื่อกำหนดความชัดเจนเพิ่มเติม ได้ประกาศลงในราชกิจจานุเบกษาเรื่องประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 เมื่อวันที่ 23 สิงหาคม 2550 เพื่อขยายความหลักเกณฑ์ทางเทคนิคในการเก็บข้อมูลจราจรคอมพิวเตอร์ ทั้งนี้เพื่อให้ผู้ให้บริการในแต่ละประเภทได้เก็บข้อมูลดังกล่าวและสามารถนำมาใช้ต่อไปได้ (เลอศักดิ์ ลิ้มวิวัฒน์กุล, บรรจง หะรังษี และโกเมน พิบูลย์โรจน์ 2551 : 1-2)

ทั้งนี้คำว่า “ข้อมูลจราจรคอมพิวเตอร์” และ “ข้อมูลผู้ใช้บริการ” เป็นข้อมูลการบันทึกเหตุการณ์ที่เกิดขึ้นกับระบบคอมพิวเตอร์ ศัพท์ทางเทคนิคเรียกข้อมูลลักษณะนี้ว่า ข้อมูลล็อกหรือ Log ดังนั้นคำว่า “ข้อมูลล็อก” มีความหมายเดียวกันกับคำว่า “ข้อมูลจราจรคอมพิวเตอร์” และ “ข้อมูลผู้ใช้บริการ”

หน้าที่ของผู้ให้บริการที่ต้องปฏิบัติตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์คือ การปรับแต่งระบบคอมพิวเตอร์ให้สามารถเก็บ “ข้อมูลล็อก” ให้ได้อย่างน้อยตามที่ “ข้อมูลจราจรคอมพิวเตอร์” และ “ข้อมูลผู้ใช้บริการ” ได้กำหนดไว้ให้ดำเนินการเก็บ และที่สำคัญคือ

1.1 มีการรักษาความมั่นคงปลอดภัย ของข้อมูลล็อก เพื่อให้ข้อมูลล็อกมีความถูกต้องและเชื่อถือ มีการควบคุมการเข้าถึงข้อมูลล็อก กำหนดลำดับเวลาของการเก็บข้อมูลล็อกให้ถูกต้อง เพื่อให้ข้อมูลล็อกที่เก็บไว้นั้นใช้วิเคราะห์ตามความต้องการของพนักงานเจ้าหน้าที่หรือผู้ที่เกี่ยวข้องได้ รวมทั้งใช้เป็นพยานหลักฐานในชั้นศาลได้

1.2. มีการกำหนดวิธีการรักษาระยะเวลาการเก็บข้อมูลล็อก เพื่อให้มีข้อมูลล็อกที่นำมาวิเคราะห์สืบย้อนหลัง และติดตามเหตุการณ์ที่เกิดขึ้นมาแล้วได้

2. ระบบอินเทอร์เน็ตของสำนักงานบริการลูกค้า กสท เขตตะวันตก

ปัจจุบันการใช้บริการอินเทอร์เน็ตของพนักงานและลูกจ้างของสำนักงานบริการลูกค้า กสท เขตตะวันตก นั้น พนักงานและลูกจ้างจะใช้งานผ่านระบบอินทราเน็ต ซึ่งสามารถออกอินเทอร์เน็ตได้ หรืออาจใช้อินเทอร์เน็ตโดยตรง ทั้งนี้ในส่วนของการใช้งานอินเทอร์เน็ตผ่านระบบอินทราเน็ตนั้น การจัดเก็บและรักษาข้อมูลจราจรทางคอมพิวเตอร์นั้น ฝ่ายเทคโนโลยีสารสนเทศ ซึ่งตั้งอยู่ที่สำนักงานใหญ่ หลักสี่ กรุงเทพฯ จะเป็นผู้เก็บรักษาข้อมูล ความรับผิดชอบของสำนักงานบริการลูกค้า กสท เขตตะวันตก จึงเป็นส่วนที่อนุญาตให้พนักงานและลูกจ้างสามารถใช้งานอินเทอร์เน็ต โดยไม่ผ่านระบบอินทราเน็ต ซึ่งปัจจุบันพนักงานส่วนใหญ่จะใช้อินเทอร์เน็ตโดยไม่ผ่านระบบอินทราเน็ตเป็นหลัก เนื่องจากความเร็วและความสะดวกในการใช้งาน ดังนั้น สำนักงานบริการลูกค้า กสท เขตตะวันตกจึงต้องจัดทำระบบจัดเก็บและรักษาข้อมูลจราจรทางคอมพิวเตอร์ เพื่อจัดเก็บข้อมูลผู้ใช้บริการ และข้อมูลจราจรคอมพิวเตอร์ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

3. แนวคิดที่เกี่ยวข้อง

เมื่อมีการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร องค์กรต่าง ๆ สถาบันการศึกษา รวมถึงหน่วยงานภาคเอกชน ได้พยายามหาวิธีการจัดทำระบบจัดเก็บและรักษาข้อมูลจราจรทางคอมพิวเตอร์ ทั้งเพื่อไว้จำหน่าย รับติดตั้ง รับวางระบบ หรือเพื่อให้หน่วยงานของตนเองปฏิบัติได้ถูกต้องตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งนี้ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเอง ได้พยายามให้ข้อมูล และมีการจัดสัมมนา อบรม แก่เจ้าหน้าที่ที่เกี่ยวข้อง อาจารย์ ผู้ดูแลระบบของหน่วยงานราชการ โรงเรียนต่าง ๆ เพื่อให้สามารถจัดทำระบบให้รองรับตามพระราชบัญญัติดังกล่าวได้ แนวทางการอบรมของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร จะเป็นการใช้ฟรีซอฟต์แวร์ต่าง ๆ มาปรับปรุง แก้ไข เพิ่มเติมคำสั่งต่าง ๆ

ส่วนภาคเอกชนนั้น จะมีการตั้งทีมงานขึ้นมาวิเคราะห์ วิจัย เขียนและผลิต ซอฟต์แวร์ และ ฮาร์ดแวร์ มาเพื่อให้รองรับตามพระราชบัญญัติฯและประกาศกระทรวงฯ และ จำหน่ายแก่หน่วยงานต่าง ๆ ในราคาที่สูง

สำหรับแนวคิดหลักๆ ที่ต้องมีการดำเนินการให้ได้ตามประกาศกระทรวงฯ คือ

3.1. ต้องมีการตั้งเวลา ตามข้อ 9 ของประกาศกระทรวงฯ เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริงผู้ให้บริการต้องตั้งนาฬิกา ของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน 10 มิลลิวินาที

3.2. ต้องมีการจัดทำ Centralized Log Server ตามมาตรา 26 ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า เก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่ง ให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

3.3. ต้องมีการจัดทำ Authentication System ตามมาตรา 26 (วรรคสอง) ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง

4. ทฤษฎีที่เกี่ยวข้อง

4.1 Network Time Protocol (NTP)

NTP Protocol เป็นโปรโตคอลที่ใช้สำหรับปรับเทียบเวลา (Time Synchronization) ของ คอมพิวเตอร์ โดยอาศัยเครือข่ายอินเทอร์เน็ต 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 แค่เพียงมีคอมพิวเตอร์ที่สามารถเชื่อมต่อ เข้าระบบอินเทอร์เน็ต ได้ ผู้ใช้ก็สามารถที่จะ Synchronize เวลามาตรฐานผ่านระบบ NTP ได้ทันที

ในปัจจุบันคอมพิวเตอร์ มีบทบาทสำคัญต่อชีวิตประจำวันของมนุษย์ และมีแนวโน้มว่าจะมีความสำคัญเพิ่มมากขึ้น ในอีกมุมหนึ่งคอมพิวเตอร์ นั้นต้องการความถูกต้องแม่นยำของระบบเวลาในเรื่องของ Time stamp เพื่อเก็บบันทึก วัน เวลา และเหตุการณ์หรือกิจกรรมต่างๆ เช่น ระบบการเงินการธนาคาร การแพทย์ การส่งถ่ายข้อมูล เป็นต้น ในความเป็นจริงแล้ว ฐานเวลาที่คอมพิวเตอร์ ใช้ ยังมีความคลาดเคลื่อนอยู่ ไม่ถูกต้องแม่นยำมากนัก เนื่องจากคอมพิวเตอร์ใช้ตัวกำเนิดฐานเวลา (Time Base) เป็น Crystal Oscillator แบบธรรมดาซึ่งไม่มีการ

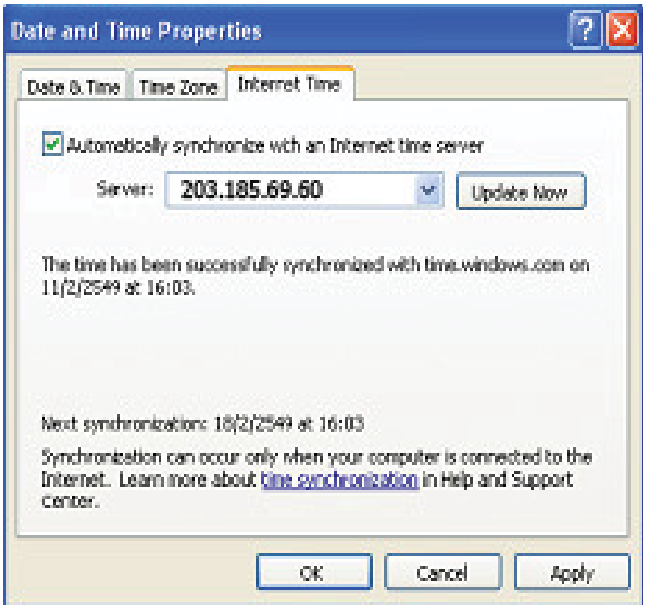
ควบคุมสภาวะแวดล้อมอย่างเข้มงวด เช่น อุณหภูมิ, ความชื้น ให้คงที่และเหมาะสม หมายความว่า เวลาของคอมพิวเตอร์ จะเปลี่ยนแปลงเนื่องจากผลกระทบจากสภาพแวดล้อมได้ง่าย ดังนั้นฐานเวลาที่อยู่ภายในตัวของคอมพิวเตอร์ จะมีการเปลี่ยนแปลงเนื่องมาจากความไม่คงที่ของสภาวะแวดล้อมได้หลายสิบวินาทีต่อสัปดาห์ จึงทำให้ผู้ใช้คอมพิวเตอร์ จำเป็นต้องทำการปรับเปลี่ยนเวลาที่คลาดเคลื่อนไปให้ถูกต้องด้วยตัวเอง ซึ่งอาจจะเปรียบเทียบจากแหล่งเวลาที่ทราบค่าและเชื่อถือได้หลาย ๆ แหล่งเช่น โทรศัพท์ (Speaking Clock), โทรทัศน์, วิทยุ เป็นต้น หลังจากนั้นเมื่อระบบโครงข่ายอินเทอร์เน็ต ได้ถือกำเนิดขึ้นและมีความนิยมในการใช้งานกันอย่างกว้างขวางในปัจจุบัน มีการพัฒนาขยายตัวออกไปอย่างไม่หยุดยั้งจึงส่งผลให้ มีการพัฒนาระบบ NTP ซึ่งสามารถใช้โครงข่ายพื้นฐานของอินเทอร์เน็ต เป็นตัวกลางในการถ่ายทอดเวลามาตรฐานได้ พบว่ามีความถูกต้องสูงและมีความรวดเร็วในการส่งข้อมูลด้วย

สถาบันมาตรวิทยาแห่งชาติ ส่วนห้องปฏิบัติการด้านเวลาและความถี่ได้จัดให้มีการติดตั้ง NTP Server ขึ้นเพื่อให้บริการถ่ายทอดเวลาผ่านระบบอินเทอร์เน็ต และสามารถเปิดให้บริการได้ในปัจจุบัน ผู้สนใจใช้บริการสามารถปรับเทียบเวลาได้โดยวิธีง่ายๆ ไม่สลับซับซ้อนมาก สามารถใช้โปรแกรมพื้นฐานที่ติดมากับ Windows Xp ได้ โดยให้ผู้ใช้ปฏิบัติตามขั้นตอนดังต่อไปนี้

กรณีใช้ Window Xp ขึ้นไปให้ double click ตรงตำแหน่งที่แสดงเวลาด้านล่างขวาของหน้าจอคอมพิวเตอร์ดังที่แสดงในภาพที่ 2

ภาพที่ 2 แสดงตำแหน่งที่ใช้ตั้งค่าการ Synchronize เวลา
ที่มา : สถาบันมาตรวิทยาแห่งชาติ. NTP (Network Time Protocol) [ออนไลน์], เข้าถึงเมื่อ 28 กันยายน 2551. เข้าถึงได้จาก http://www.nimt.or.th/

ที่ Tab Internet Time แล้วเลือก Check Box ที่ Automatically Synchronize with and internet time server และ ใส่ค่า IP Address ของ NTP Server ของสถาบันมาตรวิทยาแห่งชาติ ดังภาพที่ 3



ภาพที่ 3 แสดงวิธีการตั้งค่าการ Synchronize เวลา กับเครื่องแม่ข่าย

ที่มา : สถาบันมาตรวิทยาแห่งชาติ. NTP (Network Time Protocol) [ออนไลน์], เข้าถึงเมื่อ 28 กันยายน 2551. เข้าถึงได้จาก http://www.nimt.or.th/

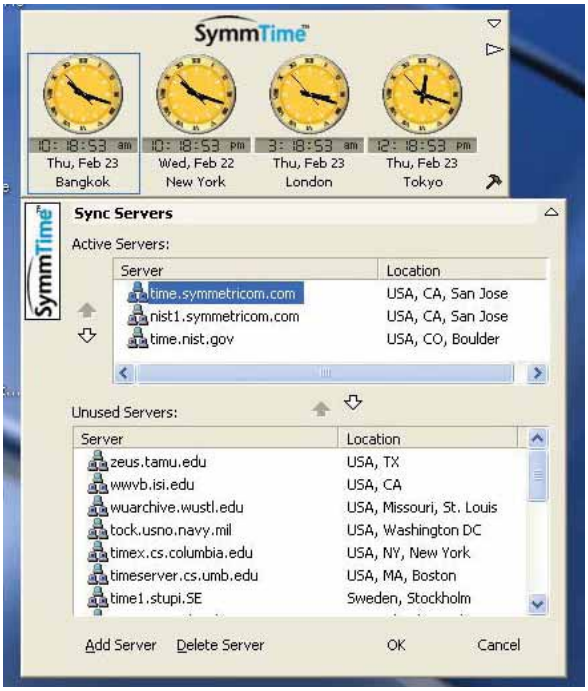
จากนั้นให้ Click ที่ปุ่ม Update Now และให้สังเกตบรรทัดล่างจะปรากฏคำว่า The time has been successfully synchronized with “IP 203.185.69.60” on 11/2/2549 at 16:03 หมายถึง สามารถที่จะ Synchronize เวลากับเครื่องแม่ข่ายได้เป็นที่เรียบร้อยแล้ว และ ถือเป็นอันเสร็จขั้นตอนการ Synchronize เวลาจากเครื่องแม่ข่าย

นอกจากเครื่องมือมาตรฐานที่ Windows Xp ให้มาแล้วยังสามารถที่จะใช้โปรแกรมประยุกต์อื่นๆ ที่รองรับการทำงานของระบบ NTP ได้ ในที่นี้ทาง ห้องปฏิบัติการด้านเวลาและความถี่ แนะนำ Software ที่ทำงานในลักษณะดังกล่าวอยู่ 2 ตัวได้แก่ SymmTime ดังภาพที่ 4 และ Dimension 4 ซึ่งมีความสามารถในการรองรับการใช้งานระบบ NTP ได้ ซึ่ง Software ดังกล่าวสามารถ Download ได้ทาง Internet ที่ www.symmetricom.com และ www.thinkman.com ตามลำดับ

ภาพที่ 4 แสดง User Interface ที่ได้มาจากโปรแกรม Symmtime

ที่มา : สถาบันมาตรวิทยาแห่งชาติ. NTP (Network Time Protocol) [ออนไลน์], เข้าถึงเมื่อ 28 กันยายน 2551. เข้าถึงได้จาก http://www.nimt.or.th/

จากภาพที่ 4 จะเห็นได้ว่า SymmTime สามารถเลือกแสดงเวลาของประเทศที่ต้องการได้มากกว่า 1 ประเทศ และ SymmTime ยังยอมให้สามารถเลือก Sync Server ที่เราต้องการจะ Synchronize เวลาได้เองอีกด้วยดังแสดงในภาพที่ 5



ภาพที่ 5 วิธีการตั้งค่า Sync Server ให้กับโปรแกรม SymmTime

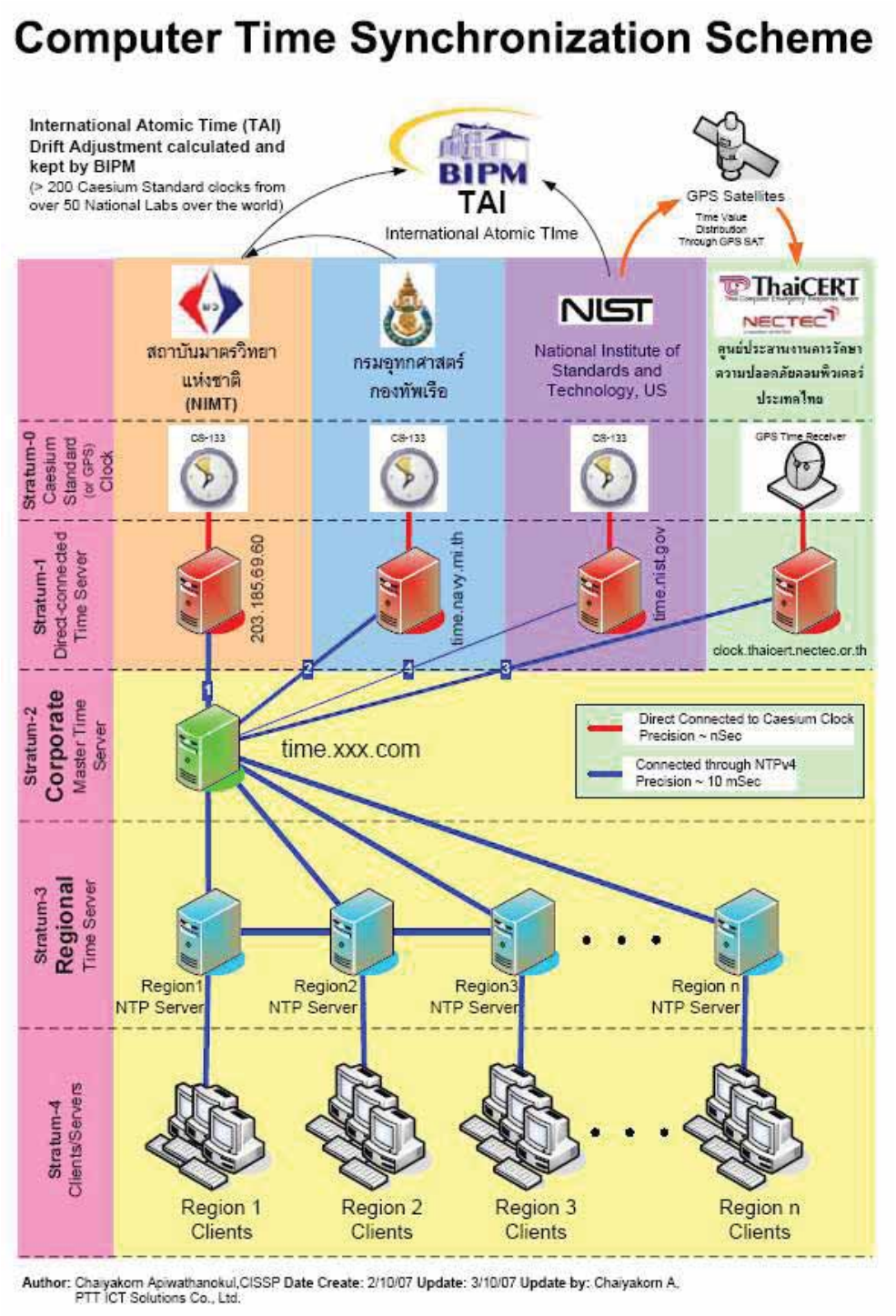
ที่มา : สถาบันมาตรวิทยาแห่งชาติ, NTP (Network Time Protocol) [ออนไลน์], เข้าถึงเมื่อ 28 กันยายน 2551. เข้าถึงได้จาก http://www.nimt.or.th/

โปรแกรมสำเร็จรูปอีกโปรแกรมหนึ่งที่ใช้ง่ายและมีความสามารถที่ดีได้แก่ โปรแกรม Dimension4 ซึ่งจะยอมให้สามารถ setup ค่าต่างๆได้อย่างละเอียดและ User Interface ดูแล้วไม่ยุ่งยากสำหรับผู้ใช้งานทั่วไปดังแสดงในภาพที่ 6

ภาพที่ 6 User Interface ของโปรแกรม Dimension4 ที่ยอมให้ใส่ค่ากำหนดค่าต่างๆได้อย่างละเอียด
ที่มา : สถาบันมาตรวิทยาแห่งชาติ. NTP (Network Time Protocol) [ออนไลน์], เข้าถึงเมื่อ 28 กันยายน 2551. เข้าถึงได้จาก http://www.nimt.or.th/

เนื่องจากที่ ห้องปฏิบัติการด้านเวลาและความถี่ ได้มีการจัดตั้ง NTP Server ขึ้นเพื่อให้บริการถ่ายทอดเวลามาตรฐานผ่านระบบ Internet ดังที่ได้กล่าวไปแล้วข้างต้นนั้น อย่างไรก็ตามจำเป็นอย่างยิ่งที่จะต้องมีการดูแลรักษาความปลอดภัยของระบบเครือข่าย คอมพิวเตอร์เป็นอย่างดีเพื่อป้องกันการเข้าใช้งานระบบโดยไม่ได้รับอนุญาตดังนั้น ณ ปัจจุบันทางห้องปฏิบัติการ จะมีระบบ Firewall เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตอยู่ด้วย (สถาบันมาตรวิทยาแห่งชาติ 2550 : 1-3)

สำหรับ Time server ที่ทางราชการแนะนำ สามารถเลือกใช้ Time Server ที่มีอยู่ในประเทศไทย แสดงได้ดังภาพที่ 7



ภาพที่ 7 Computer Time Synchronization Scheme

ที่มา : สถาบันมาตรวิทยาแห่งชาติ. NTP (Network Time Protocol) [ออนไลน์], เข้าถึงเมื่อ 28 กันยายน 2551. เข้าถึงได้จาก http://www.etcommission.go.thrver_v1_0.pdf

4.2 Syslog และ Syslog-ng (Syslog new generation)

syslogd เป็นกลไกที่ใช้ในการเก็บข้อมูลล็อกของ kernel และ application บนระบบยูนิกซ์และลินุกซ์ เป็น daemon ที่ถูกติดตั้งมาให้พร้อมกับระบบปฏิบัติการในเกือบทุกระบบ โดยผู้ดูแลระบบสามารถปรับแต่งไฟล์ configuration เพื่อควบคุมการทำงานของ syslogd ได้ เช่น ให้ syslogd เก็บข้อมูลไปไว้ที่ไฟล์ใด หรือให้ส่งข้อมูลล็อกนี้ไปเก็บไว้ยังเครื่องอื่นในเครือข่าย ข้อมูลล็อกที่ควบคุมโดย syslogd นั้น จะถูกกำหนดให้มีค่า facility และ priority โดยส่วนของ facility นั้น เป็นข้อมูลที่อธิบายถึงแหล่งกำเนิดของข้อมูลล็อกนั้นๆ เช่น ข้อมูลล็อกที่ส่งมาจากระบบเมล์ก็จะมี facility เป็น mail ส่วน priority นั้น จะแสดงถึงระดับความสำคัญของเหตุการณ์ที่เกิดสำหรับแต่ละ facility ทั้งนี้ข้อมูลล็อกทุกอันจำเป็นต้องมี facility และ priority เสมอ

syslog ถือได้ว่าเป็น log daemon ที่ใช้กันมาอย่างยาวนานและกลายเป็นมาตรฐานของการเก็บข้อมูลล็อกของระบบปฏิบัติการ *nix ในหลาย ๆ ตัว แต่อย่างไรก็ตาม syslog ก็มีข้อเสียบางอย่าง ที่ log daemon ตัวอื่น เช่น syslog-ng, msyslog สามารถแก้ไขข้อบกพร่องดังกล่าวได้ syslog-ng ซึ่งเป็น log daemon ตัวใหม่ที่กำลังเป็นที่นิยมกันมากขึ้น การสร้าง configuration แบบละเอียดเพื่อให้สามารถนำ syslog-ng ไปใช้งานได้จริง

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 มันจึงสามารถทำงานแทนที่ syslog ได้

syslog-ng สนับสนุน log forwarding ซึ่งทำให้สามารถทราบได้ว่า ต้นทางของล็อกถูกส่งมาจากเครื่องใด และผ่านเครื่องใดมาบ้าง

นอกจากนี้ syslog-ng ยังมีรูปแบบของไฟล์ configuration ที่ง่าย แต่มีความยืดหยุ่นสูง สามารถนำไปประยุกต์ใช้ให้ตรงความต้องการได้โดยง่าย

syslog-ng เป็นโปรแกรมที่มีความยืดหยุ่นในการทำงาน เหมาะสำหรับการนำมาใช้งานเป็น log server เป็นอย่างยิ่ง เพราะสามารถเก็บข้อมูลล็อกแยกตามเครื่องที่ส่งล็อกมาได้ นอกจากนี้ยังสามารถทำงานร่วมกับโปรแกรม sqlsyslogd เพื่อนำข้อมูลล็อกทั้งหมดบันทึกลงในฐานข้อมูลได้(ภูวดล ด่านระหาญ 2546 : 1-12)

4.3 การเข้ารหัสข้อมูล (Cryptography)

จุดประสงค์ที่สำคัญ 3 ประการของการเข้ารหัสข้อมูลประกอบด้วย

4.3.1 การทำให้ข้อมูลเป็นความลับ (Confidentiality) เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์ในการเข้าถึงข้อมูลสามารถเข้าถึงข้อมูลได้

4.3.2 การทำให้ข้อมูลสามารถตรวจสอบความสมบูรณ์ได้ (Integrity) เพื่อป้องกันข้อมูลให้อยู่ในสภาพเดิมอย่างสมบูรณ์ กล่าวคือ ในกระบวนการสื่อสารนั้นผู้รับ (Receiver) ได้รับข้อมูลที่ถูกต้องตามที่ผู้ส่ง (Sender) ส่งมาให้โดยข้อมูลจะต้องไม่มีการสูญหายหรือถูกเปลี่ยนแปลงแก้ไขใดๆ

4.3.3 การทำให้ สามารถพิสูจน์ตัวตน ของผู้ส่งข้อมูลได้ (Authentication/ Nonrepudiation) เพื่อให้ สามารถตรวจสอบได้ว่าใครคือผู้ส่งข้อมูล หรือในทางตรงกันข้าม ก็คือเพื่อป้องกันการแอบอ้างได้

การเข้ารหัสข้อมูลโดยพื้นฐานแล้ว จะเกี่ยวข้องกับวิธีการทางคณิตศาสตร์เพื่อใช้ในการป้องกันข้อมูลหรือข้อความตั้งต้นที่ต้องการส่งไปถึงผู้รับข้อมูลตั้งต้นจะถูกแปรเปลี่ยนไปสู่ข้อมูลหรือข้อความอีกรูปแบบหนึ่ง ที่ไม่สามารถอ่านเข้าใจได้ โดยใครก็ตามที่ไม่มีกุญแจ สำหรับเปิดดูข้อมูลนั้น เราเรียกกระบวนการในการแปรรูปของข้อมูลตั้งต้นว่า "การเข้ารหัสข้อมูล" (Encryption) และ กระบวนการในการแปลงข้อความ ที่ไม่สามารถอ่าน และทำความเข้าใจ ให้กลับไปสู่ข้อความดั้งเดิม ว่าการถอดรหัสข้อมูล (Decryption)

อัลกอริทึมในการเข้ารหัสข้อมูลมี 2 ประเภทหลัก คือ

4.3.3.1 อัลกอริทึมแบบสมมาตร (Symmetric key algorithms)

อัลกอริทึมแบบนี้จะใช้กุญแจที่เรียกว่า กุญแจลับ (Secret key) ซึ่งมีเพียงหนึ่งเดียวเพื่อใช้ในการเข้าและถอดรหัสข้อความที่ส่งไป อัลกอริทึมยังสามารถแบ่งย่อยออกเป็น 2 ประเภท ได้แก่ แบบบล็อค (Block Algorithms) ซึ่งจะทำการเข้ารหัสทีละบล็อค (1 บล็อคประกอบด้วยหลายไบต์ เช่น 64 ไบต์ เป็นต้น) และแบบสตรีม (Stream Algorithms) ซึ่งจะทำการเข้ารหัสทีละไบต์อัลกอริทึมแบบนี้จะใช้กุญแจที่เรียกว่า กุญแจลับ (Secret key) ซึ่งมีเพียงหนึ่งเดียวเพื่อใช้ในการเข้าและถอดรหัสข้อความที่ส่งไป

4.3.3.2 อัลกอริทึมแบบอสมมาตร (Asymmetric key algorithms)

อัลกอริทึมนี้จะใช้กุญแจสองตัวเพื่อทำงาน ตัวหนึ่งใช้ในการเข้ารหัสและอีกตัวหนึ่งใช้ในการถอดรหัสข้อมูลที่เข้ารหัสมาโดยกุญแจตัวแรกอัลกอริทึมกลุ่มสำคัญในแบบอสมมาตรนี้คือ อัลกอริทึมแบบกุญแจสาธารณะ (Public keys Algorithms) ซึ่งใช้กุญแจที่เรียกกันว่า กุญแจสาธารณะ (Public keys) ในการเข้ารหัสและใช้กุญแจที่เรียกกันว่า กุญแจส่วนตัว (Private keys) ในการถอดรหัสข้อมูลนั้น กุญแจสาธารณะนี้สามารถส่งมอบให้กับผู้อื่นได้ เช่น เพื่อนร่วมงานที่เราต้องการติดต่อด้วย หรือแม้กระทั่งวางไว้บนเว็บไซต์ เพื่อให้ผู้อื่นสามารถ

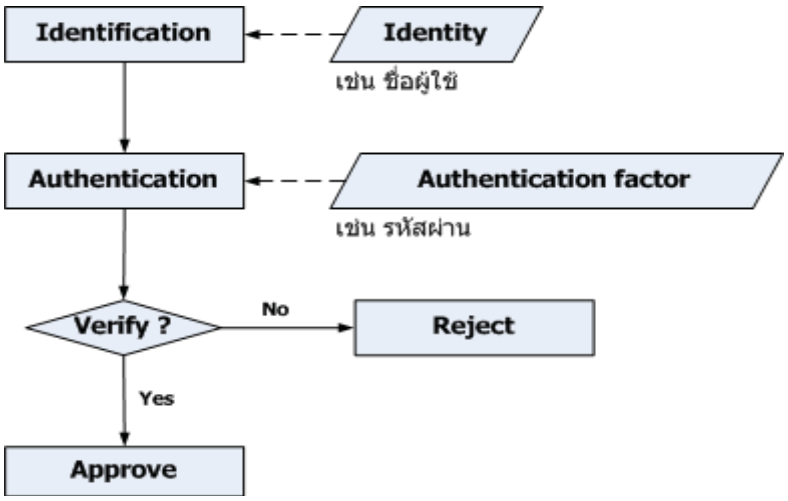
ดาวน์โหลดไปใช้งานได้ สำหรับกุญแจส่วนตัวนั้น ต้องเก็บไว้กับผู้เป็นเจ้าของกุญแจส่วนตัวเท่านั้น และห้ามเปิดเผยให้ผู้อื่นทราบโดยเด็ดขาด อัลกอริทึมแบบกุญแจสาธารณะ ยังสามารถประยุกต์ใช้ได้กับการลงลายมือชื่ออิเล็กทรอนิกส์ (ซึ่งเปรียบเสมือนการลงลายมือชื่อของเราที่ใช้กับเอกสารสำนักงานทั่วไป) การลงลายมือชื่อนี้จะเป็นการพิสูจน์ความเป็นเจ้าของและสามารถใช้ได้กับการทำธุรกรรมต่างๆ บนอินเทอร์เน็ต เช่น การซื้อสินค้า เป็นต้น วิธีการใช้งานคือ ผู้เป็นเจ้าของกุญแจส่วนตัวลงลายมือชื่อของตนกับข้อความที่ต้องการส่งไปด้วยกุญแจส่วนตัว แล้วจึงส่งข้อความนั้นไปให้กับผู้รับ เมื่อได้รับข้อความที่ลงลายมือชื่อมา ผู้รับสามารถใช้กุญแจสาธารณะ (ที่เป็นคู่ของกุญแจส่วนตัวนั้น) เพื่อตรวจสอบว่าเป็นข้อความที่มาจากผู้ส่งนั้นหรือไม่ (บรรจง หะรังษี 2547 : 1-3)

4.4 การพิสูจน์ตัวตน (Authentication)

การพิสูจน์ตัวตน คือขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง ในทางปฏิบัติจะแบ่งออกเป็น 2 ขั้นตอน คือ

การระบุตัวตน (Identification) คือขั้นตอนที่ผู้ใช้แสดงหลักฐานว่าตนเองคือใคร เช่น ชื่อผู้ใช้ (username)

การพิสูจน์ตัวตน (Authentication) คือขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลที่กล่าวอ้างจริง ดังแสดงในภาพที่ 8



ภาพที่ 8 แผนผังแสดงกระบวนการการพิสูจน์ตัวตน

ที่มา : สิริพร จิตต์เจริญธรรม, เสาวภา ปานจันทร์ และ เลอศักดิ์ ลิ้มวิวัฒน์กุล. ระบบพิสูจน์ตัวตน [ออนไลน์], เข้าถึงเมื่อ 5 ตุลาคม 2551. เข้าถึงได้จาก http://www.thaicert.nectec.or.th/

จากแผนผังแสดงกระบวนการพิสูจน์ตัวตน ในขั้นแรกผู้ใช้จะทำการแสดงหลักฐานที่ใช้ในการพิสูจน์ตัวตนต่อระบบ ซึ่งในขั้นนี้คือการระบุตัวตน และในขั้นตอนต่อมาระบบจะทำการตรวจสอบ หลักฐานที่ผู้ใช้นำมากล่าวอ้างซึ่งก็คือการพิสูจน์ตัวตน หลังจากระบบได้ทำการตรวจสอบหลักฐานเรียบร้อยแล้ว ถ้าหลักฐานที่นำมากล่าวอ้างถูกต้องจึงอนุญาตให้เข้าสู่ระบบได้ หากหลักฐานที่นำมากล่าวอ้างไม่ถูกต้อง ผู้ใช้จะถูกปฏิเสธจากระบบ หลักฐานที่ผู้ใช้นำมากล่าวอ้าง ที่เกี่ยวกับเรื่องของความปลอดภัยนั้นสามารถจำแนกได้ 2 ชนิด

Actual identity คือหลักฐานที่สามารถบ่งบอกได้ว่าในความเป็นจริงบุคคลที่กล่าวอ้างนั้นเป็นใคร

Electronic identity คือหลักฐานทางอิเล็กทรอนิกส์ซึ่งสามารถบ่งบอกข้อมูลของบุคคลนั้นได้ แต่ละบุคคลอาจมีหลักฐานทางอิเล็กทรอนิกส์ได้มากกว่า 1 หลักฐาน ตัวอย่างเช่น บัญชีชื่อผู้ใช้

กลไกของการพิสูจน์ตัวตน (Authentication mechanisms) สามารถแบ่งออกได้เป็น 3 คุณลักษณะคือ

สิ่งที่คุณมี (Possession factor) เช่น กุญแจหรือเครดิตการ์ด เป็นต้น

สิ่งที่คุณรู้ (Knowledge factor) เช่นรหัสผ่าน (passwords) หรือการใช้พิน (PINs) เป็นต้น

สิ่งที่คุณเป็น (Biometric factor) เช่น ลายนิ้วมือ รูปแบบเรตินา (retinal patterns) หรือใช้รูปแบบเสียง (voice patterns) เป็นต้น

กระบวนการพิสูจน์ตัวตนนั้นจะนำ 3 ลักษณะข้างต้นมาใช้ในการยืนยันหลักฐานที่นำมากล่าวอ้าง ทั้งนี้ขึ้นอยู่กับระบบ วิธีการที่นำมาใช้เพียงลักษณะอย่างใดอย่างหนึ่ง (Single-factor authentication) นั้นมีข้อจำกัดในการใช้ ตัวอย่างเช่น สิ่งที่คุณมี (Possession factor) นั้นอาจจะสูญหายหรือถูกขโมยได้ สิ่งที่คุณรู้ (Knowledge factor) อาจจะถูกดักฟัง เดา หรือขโมยจากเครื่องคอมพิวเตอร์ สิ่งที่คุณเป็น (Biometric factor) จัดได้ว่าเป็นวิธีที่มีความปลอดภัยสูงอย่างไรก็ตามการที่จะใช้เทคโนโลยีนี้ได้นั้นจำเป็นต้องมีการลงทุนที่สูง เป็นต้น

ดังนั้นจึงได้มีการนำ แต่ละคุณลักษณะมาใช้ร่วมกัน (multi-factor authentication) ตัวอย่างเช่น ใช้สิ่งที่คุณมีกับสิ่งที่คุณรู้มาใช้ร่วมกัน เช่น การใช้ลายมือชื่อร่วมกับการใช้บัตรเครดิต หรือการใช้รหัสผ่านร่วมกับการใช้บัตร ATM เป็นต้น การนำแต่ละลักษณะของการพิสูจน์ตัวตนมาใช้ร่วมกันมากกว่า 1 ลักษณะ จะช่วยเพิ่มประสิทธิภาพ ในการรักษาความปลอดภัย ของข้อมูล (สิริพร จิตต์เจริญธรรม, เสาวภา ปานจันทร์ และ เลอศักดิ์ ลิ้มวิวัฒน์กุล 2547 : 3-5)

5. งานวิจัยที่เกี่ยวข้อง

5.1 ระบบพิสูจน์ตัวตนและควบคุมสิทธิการใช้บริการอินเทอร์เน็ต บนวิถีโอเพนซอร์ส (Authentication and Authorization System for Internet Service based on Open Source Style)

ห้องปฏิบัติการวิจัยลีนุกซ์ คณะวิทยาศาสตร์ มหาวิทยาลัยบูรพา ช่วยให้ผู้ให้บริการอินเทอร์เน็ตบริหารความมั่นคงปลอดภัยของระบบเครือข่าย งานวิจัยเชิงพัฒนานี้มุ่งเน้นที่จะพัฒนาซอฟต์แวร์พร้อมสรรพ สามารถใช้งานได้ทันทีในวิถีโอเพนซอร์ส ซึ่งเป็นการพัฒนาต่อยอดจากซอฟต์แวร์ตั้งต้นเพื่อให้ได้ซอฟต์แวร์ ที่ดีขึ้น ในระยะแรกจะสามารถควบคุมการใช้งานเครือข่ายแบบใช้สายและแบบไร้สาย และจะพัฒนาให้สามารถควบคุมเครือข่ายในรูปแบบอื่นต่อไปในอนาคต ในการติดตั้งและใช้งานระบบนั้น ผู้ใช้งานสามารถกำหนดโครงสร้างของระบบให้สามารถควบคุมการทำงานของเครือข่ายทั้งหมดหรือเพียงบางส่วนได้ โมดูลของระบบประกอบด้วย ส่วนติดต่อผู้ใช้เพื่อควบคุมการเข้าใช้บริการ และส่วนควบคุมระบบสำหรับผู้ให้บริการ(ธวัชชัย เอี่ยมไพโรจน์, นวลศรี เด่นวัฒนา และ ณัฐวุฒิ จารุมาศ 2551 : 248)

แนวทางการจัดเก็บ ข้อมูลจราจรทางคอมพิวเตอร์ ตามพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

สำนักกำกับการใช้เทคโนโลยีสารสนเทศ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้ทำคู่มือการปฏิบัติ และแนวทางการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พร้อมชุดติดตั้ง (Software package), Slide บรรยายประกอบการฝึกอบรมปฏิบัติการ สำหรับใช้ทบทวนหรือศึกษาด้วยตนเองให้กับผู้ประกอบการและผู้ดูแลระบบของหน่วยงานภาครัฐ เพื่อให้หน่วยงานต่าง ๆ สามารถเก็บข้อมูลจราจรทางคอมพิวเตอร์(Traffic Data)ได้ถูกต้องและครบถ้วนตามที่กฎหมายกำหนด และสามารถประหยัดงบประมาณในการจัดซื้อซอฟต์แวร์จากต่างชาติ โดย การนำซอฟต์แวร์ Open Source ไปใช้ในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) (สำนักงานกำกับการใช้เทคโนโลยีสารสนเทศ 2551 : 1)

5.2 iPASSPORT (Internet Passport)

iPASSPORT (Internet Passport) หนังสือเดินทางบนอินเทอร์เน็ต เป็นระบบคอมพิวเตอร์ Centralized Log System ใช้เพื่อตรวจสอบสิทธิ์และเก็บข้อมูลการจราจรบนเครือข่ายอินเทอร์เน็ต ที่ออกแบบมาเพื่อรองรับกับ พรบฯ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ซึ่งออกแบบโดยกลุ่มนักคอมพิวเตอร์ และผู้เชี่ยวชาญด้านระบบเครือข่ายและความปลอดภัย ระบบนี้ได้พัฒนาขึ้นมาโดยนำเอา พรบฯ ฉบับนี้ และประกาศของกระทรวงเทคโนโลยี

สารสนเทศ มาเป็นต้นแบบในการพัฒนาระบบ จึงทำให้ระบบ iPASSPORT สามารถรองรับกับพรบฯ ฉบับนี้ได้ครบถ้วน และใช้โปรแกรมต่าง ๆ ที่มีชื่อเสียงระดับโลกมากกว่า 10 โปรแกรมมาทำการเขียนใหม่ และเขียนเพิ่มเติมเพื่อให้สามารถตอบโจทย์ของมาตรา ต่าง ๆ ได้โดยใช้ทีมพัฒนาคนไทยและผู้เชี่ยวชาญด้านเครือข่ายร่วมพัฒนา

ภาพที่ 9 โครงสร้างของระบบ iPassport

ที่มา : มหาวิทยาลัยราชภัฏมหาสารคาม. ipassport [ออนไลน์], เข้าถึงเมื่อ 5 เมษายน 2551. เข้าถึงได้จาก http:// www.thaibsd.com/ipassport/info/index.html

5.3 PROSPEROUS GATEWAY

เป็นระบบที่มีความสามารถในการจัดการด้าน Firewall สมบูรณ์แบบ ทำการกำหนดบัญชีรายชื่อผู้ใช้พร้อมทั้งตรวจสอบการเข้าใช้งานระบบ สามารถเชื่อมต่อเข้ากับระบบ Centralized log และ Gateway มีความสามารถในการทำหน้าที่เป็น web proxy, ftp proxy, smtp proxy และ instant messaging proxy ทำให้มั่นใจได้ว่าข้อมูลการใช้งานทั้งหมดของผู้ใช้งานจะถูกบันทึกอยู่ในระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่ตัวเกตเวย์ มีระบบตัวจัดการด้านเวลาในตัวเอง ทำหน้าที่เป็นทั้งเครื่องลูกข่ายและแม่ข่ายในตัว (ntp server) ทำให้สามารถตั้งค่าเวลาอ้างอิงจากเครื่องแม่ข่ายฐานเวลาจากทั่วโลก (บริษัท ไทย พรอสเพอรัส ไอที จำกัด 2551 : 2)

5.4 การสืบสวนผู้ใช้บริการด้วยวิชวลไลเซชันไทม์แมชชีน สำหรับนิติวิทยาศาสตร์สำหรับเครือข่าย (User Investigations with Visualization Time Machine for Network Forensic)

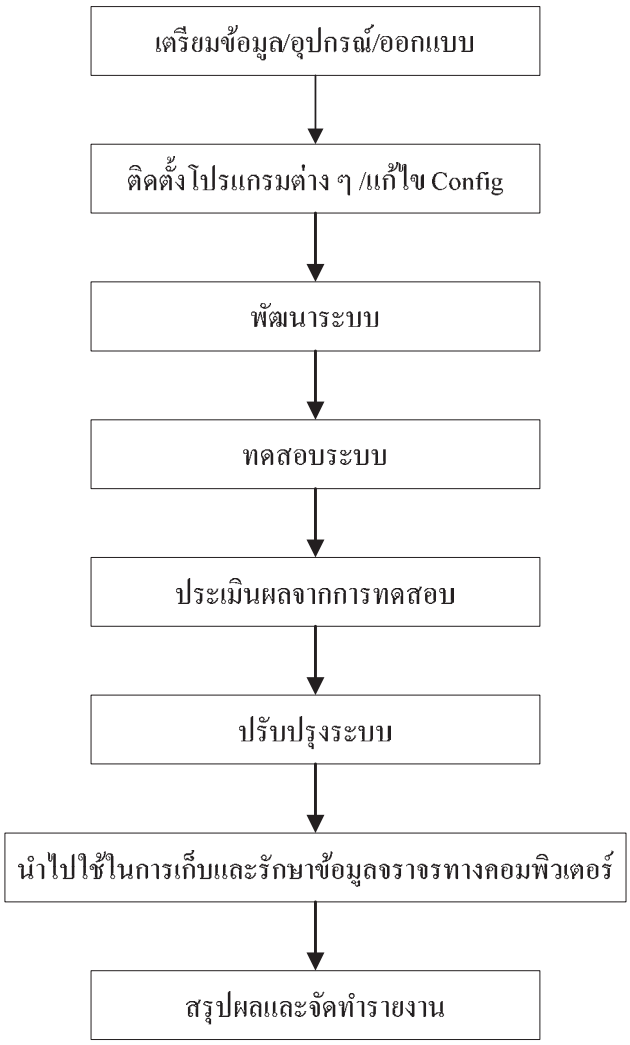
ข้อมูลจราจรทางคอมพิวเตอร์เป็นพยานหลักฐานสำคัญในการดำเนินคดีอันเป็นประโยชน์อย่างยิ่งต่อการสืบสวนสอบสวน เพื่อนำตัวผู้กระทำผิดมาลงโทษ ปัจจุบันยังไม่มีงานวิจัยที่สามารถใช้ประโยชน์จากข้อมูล Logs และ Network traffic เพื่อศึกษาและแสดงพฤติกรรมการใช้งานเครือข่าย และตรวจจับผู้ใช้งานที่มีการละเมิดนโยบายความปลอดภัย ผู้วิจัยจึงนำเสนอ Model เพื่อตรวจจับพฤติกรรมการใช้งานเครือข่ายโดยใช้เทคนิค Parallel coordinates ซึ่งแสดงความสัมพันธ์ด้วยตัวแปรต่าง ๆ ได้แก่ Users, Source IP Address, Time, Destination IP Address, Destination service และ Domain name โดยทำการแสดงพฤติกรรมการใช้งานเครือข่ายเป็นช่วงเวลา ซึ่งแต่ละแถวของ Timeline จะแสดงข้อมูลการใช้งานเครือข่ายของผู้ใช้งานปกติ ผู้ต้องสงสัย และ Host ที่เกี่ยวข้องตามช่วงเวลาที่กำหนด UIV Model สามารถรวบรวม จัดเก็บข้อมูล ตรวจจับผู้ต้องสงสัย สืบสวนเพื่อตอบคำถาม และแสดงผลในแบบ Visualization ประกอบด้วย Collector ทำหน้าที่รวบรวม Network traffic บนเครือข่าย และ Logs จาก Server logs Time Machine ทำหน้าที่ดึงข้อมูล Traffic และ Logs ตามช่วงเวลาที่ระบุ Flow generator ทำหน้าที่สร้าง Flow และ data จากข้อมูล Network traffic และ Logs ด้วยเทคนิค Parallel coordinates Detection analysis ทำหน้าที่วิเคราะห์พฤติกรรมการละเมินนโยบายความปลอดภัยของเครือข่ายจาก Flow data และ Attack signatures Parallel coordinates visualize แสดง Flow data ในรูปแบบกราฟิกด้วยเทคนิค Parallel coordinates Data cloud visualize แสดงผลการตรวจจับด้วย Data cloud Investigation interface แสดงการใช้งานเครือข่ายแบบ Timeline (ณัฐโชติ พรหมฤทธิ์ และอนิราช มิ่งขวัญ 2553 : 31)

5.5 ระบบตรวจจับและตรวจตราการส่งผ่านข้อมูลภายในเครือข่ายผ่านเว็บบราวเซอร์

เป็นการพัฒนาระบบตรวจจับและตรวจตราการส่งผ่านข้อมูลผ่านในเครือข่ายผ่านเว็บบราวเซอร์ โดยมีข้อมูลที่เกี่ยวข้องคือข้อมูลอุปกรณ์เครือข่าย ข้อมูลผู้ใช้งานระบบ ข้อมูลปริมาณการส่งผ่านข้อมูล และข้อมูลการตอบสนองต่อการติดต่อของอุปกรณ์เครือข่าย โดยระบบสามารถเก็บข้อมูล ค้นหา วิเคราะห์ แสดงผลรายงานข้อมูลระบบ และแสดงกราฟ รวมทั้งการแจ้งเตือนปริมาณการส่งข้อมูลที่ผิดปกติ โดยมีการใช้งานผ่านทางเว็บบราวเซอร์ ทำให้ผู้ใช้เกิดความสะดวกในการใช้งาน การใช้งานระบบไม่ยึดติดกับระบบปฏิบัติการ โดยพัฒนาบนระบบปฏิบัติการ Linux Fedora Core 3 ด้วยโปรแกรมภาษา PHP ภาษา PERL และให้ MySQL เป็นฐานข้อมูล โดยมีโปรแกรม MRTG เป็นส่วนช่วยติดต่อกับอุปกรณ์เครือข่าย และสร้างกราฟปริมาณการส่งผ่านข้อมูล (กฤดากร หิรัญพฤกษ์ 2549 : 13)

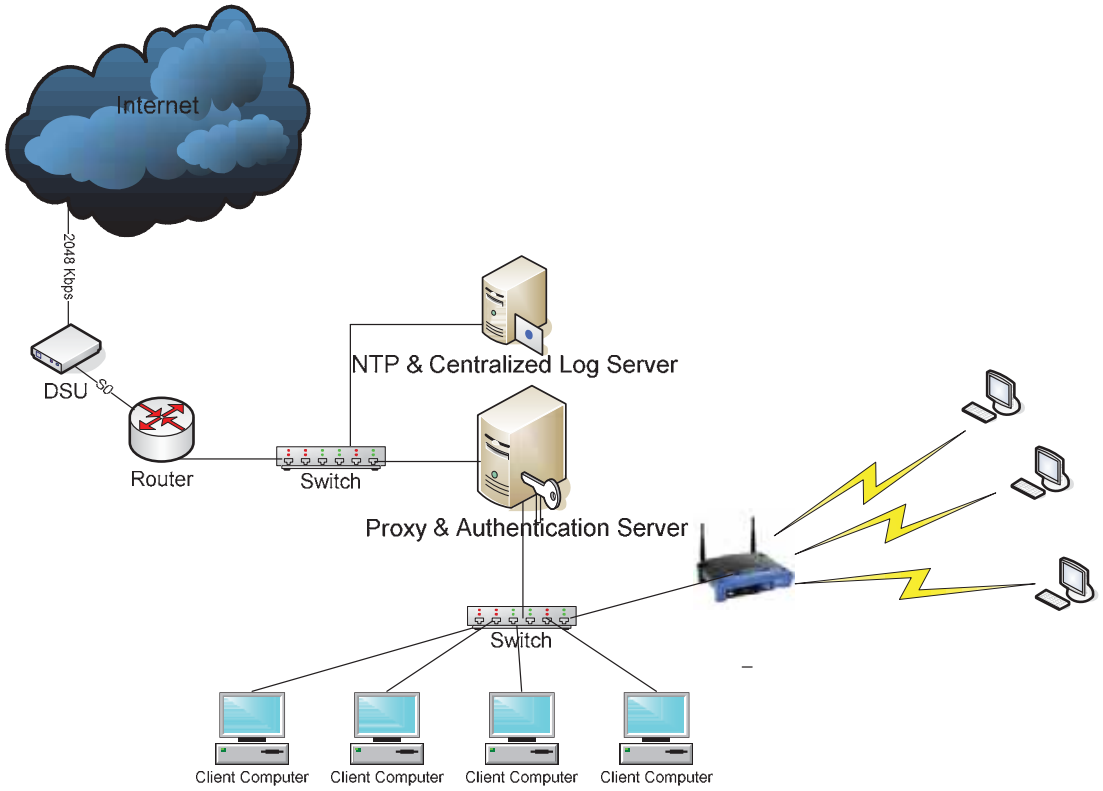
บทที่ 3
วิธีดำเนินการวิจัย

การจัดทำระบบบริหารจัดการเก็บและรักษาข้อมูลจราจรทางคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กรณีศึกษาสำนักงานบริการลูกค้า กสท เขตตะวันตก บริษัท กสท โทรคมนาคมจำกัด (มหาชน) นั้น มีขั้นตอนวิธีการดำเนินการ ดังภาพที่ 10



ภาพที่ 10 แผนผังการดำเนินงานวิจัย

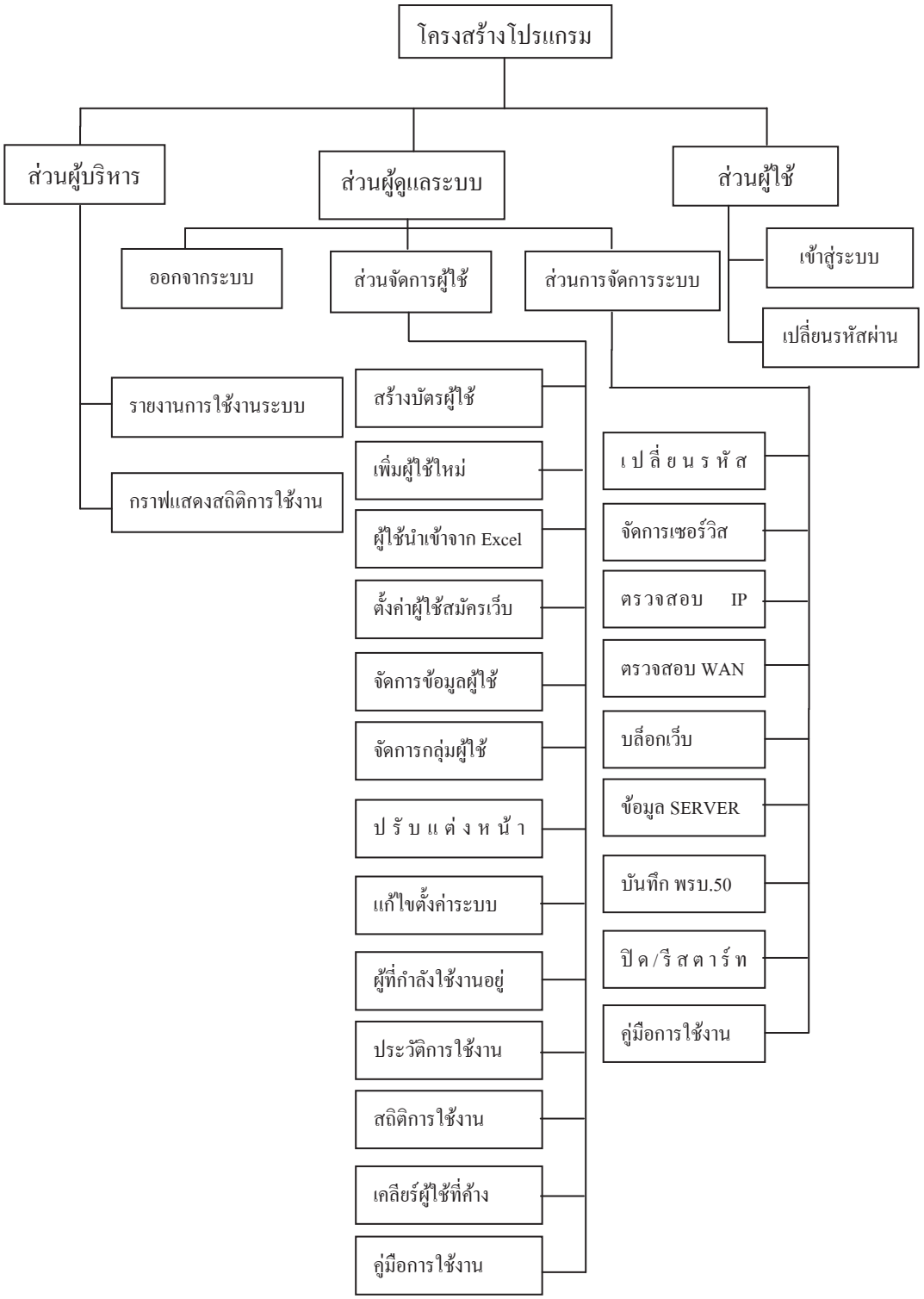
โครงสร้างของระบบ



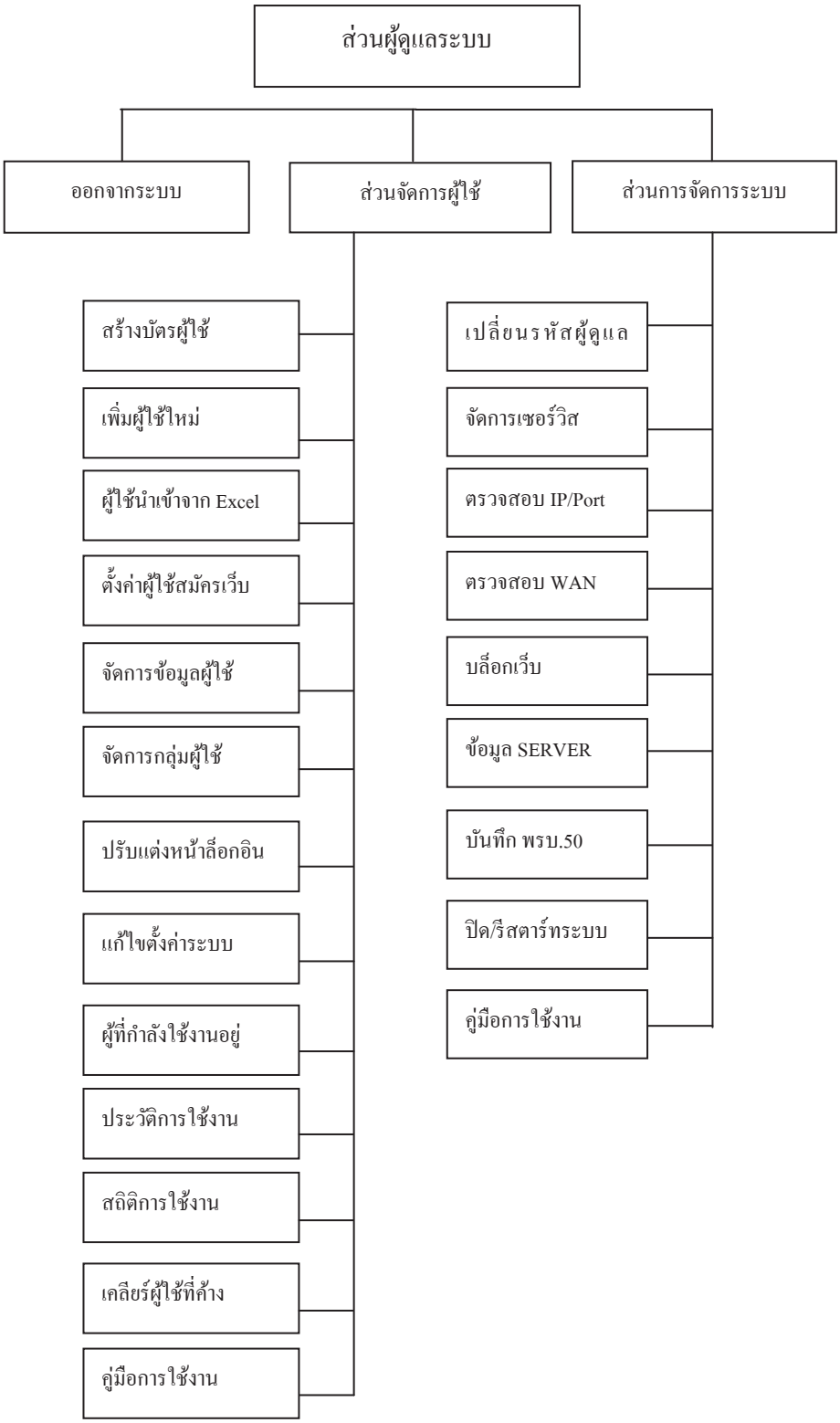
ระบบบริหารจัดการเก็บและรักษาข้อมูลจราจรทางคอมพิวเตอร์
สำนักงานบริการลูกค้า กสท เขตตะวันตก

ภาพที่ 11 โครงสร้างของระบบ

โครงสร้างโปรแกรม (Program Structure)



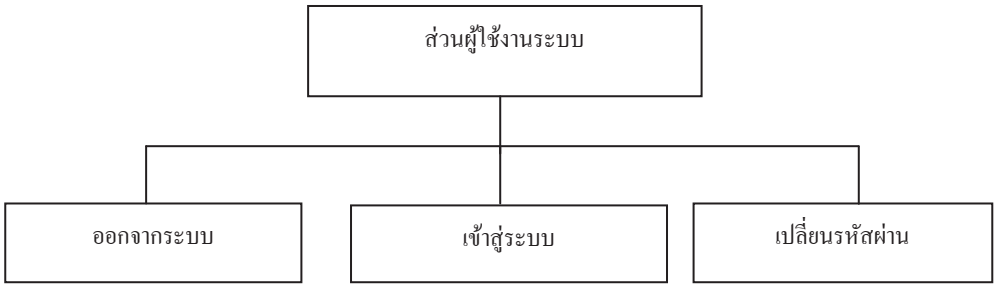
ภาพที่ 12 แสดงโครงสร้างโปรแกรมระบบบริหารจัดการเก็บและรักษาข้อมูลจราจรคอมพิวเตอร์



ภาพที่ 13 ผังเมนูระบบบริหารจัดการเก็บและรักษาข้อมูลจราจรทางคอมพิวเตอร์

สำหรับผู้ดูแลระบบ

ภาพที่ 14 ผังเมนูระบบบริหารจัดการเก็บและรักษาข้อมูลจราจรทางคอมพิวเตอร์สำหรับผู้บริหาร



ภาพที่ 15 ผังเมนูระบบบริหารจัดการเก็บและรักษาข้อมูลจราจรทางคอมพิวเตอร์สำหรับผู้ใช้งาน

จากโครงสร้างของโปรแกรม สามารถจำแนกลักษณะการทำงานได้ 3 ส่วน

1. ส่วนของผู้ใช้ จะทำงานโดยแบ่งเป็น 2 ส่วนคือ
   - 1.1 ส่วนของการ Login เข้าสู่ระบบเพื่อใช้งานอินเตอร์เน็ต
   - 1.2 ส่วนการเปลี่ยนรหัสผ่าน
2. ส่วนของผู้ดูแลระบบ จะทำงานโดยแบ่งเป็น 2 ส่วนคือ
   - 2.1 ส่วนจัดการผู้ใช้ จะประกอบด้วย
     - 2.1.1 สร้างบัตรผู้ใช้
     - 2.1.2 เพิ่มผู้ใช้ใหม่
     - 2.1.3 ผู้ใช้นำเข้าจาก Excel
     - 2.1.4 ตั้งค่าผู้ใช้สมัครเว็บ
     - 2.1.5 จัดการข้อมูลผู้ใช้
     - 2.1.6 จัดการกลุ่มผู้ใช้
     - 2.1.7 ปรับแต่งหน้าล็อกอิน

2.1.8 แก้ไขตั้งค่าระบบ

2.1.9 ผู้ที่กำลังใช้งานอยู่

2.1.10 ประวัติการใช้งาน

2.1.11 สถิติการใช้งาน

2.1.12 เคลียร์ผู้ใช้ที่ค้าง

2.1.13 คู่มือการใช้งาน

2.2 ส่วนการจัดการระบบ

2.1.1 เปลี่ยนรหัสผู้ดูแลระบบ

2.1.2 จัดการเซอร์วิส

2.1.3 ตรวจสอบ IP/Port

2.1.4 ตรวจสอบ WAN

2.1.5 บล็อกเว็บ

2.1.6 ข้อมูล Server

2.1.7 บันทึก พรบ.50

2.1.8 ปิด/รีสตาร์ทระบบ

2.1.9 คู่มือการใช้งานระบบ

2.3 ออกจากระบบ

3. ส่วนผู้บริหาร

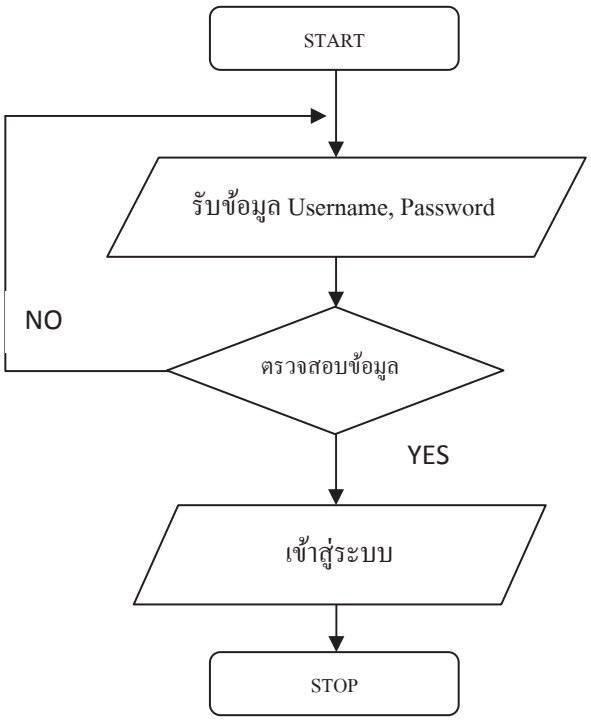
3.1 รายงานการใช้งานของผู้ใช้

3.2 กราฟแสดงสถิติการใช้งาน

ผังการทำงานของโปรแกรม

1. ผังการทำงานส่วนของผู้ใช้

1.1 ผังการทำงานของส่วน Login



ภาพที่ 16 ผังแสดงการทำงานของส่วน Login

อธิบายการทำงานของส่วน Login

1.1.1 รับข้อมูล Username, Password

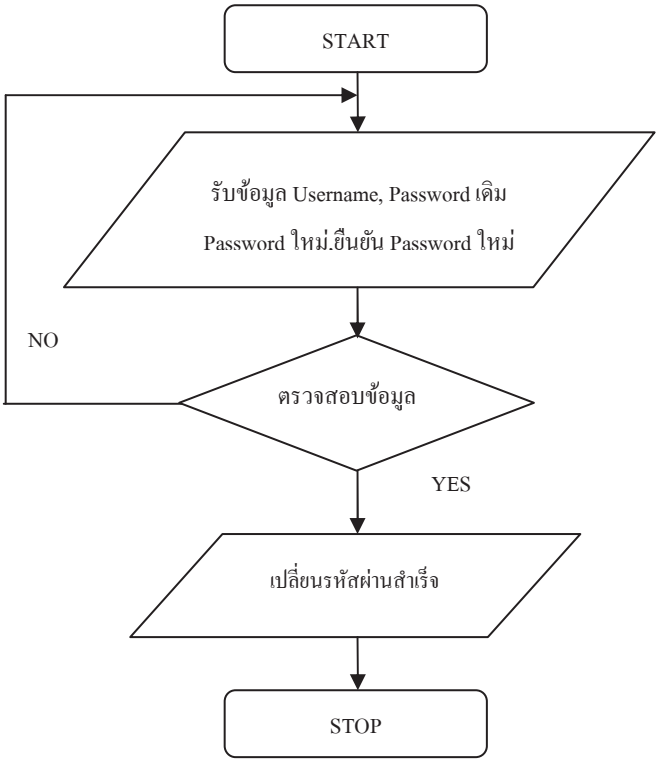
1.1.2 ตรวจสอบข้อมูล Username, Password ว่าตรงกับข้อมูลในแฟ้ม Login หรือไม่

1.1.3 หากข้อมูล Username, Password ไม่ตรง ก็จะให้กลับไปรับข้อมูลใหม่ พร้อมแจ้งรายละเอียดว่า Username หรือ Password ไม่ถูกต้อง

1.1.4 หากข้อมูล Username , Password ตรงกับข้อมูลในแฟ้มข้อมูล Login ก็สามารถเข้าสู่ระบบได้

1.1.5 จบการทำงาน

1.2 ผังการเปลี่ยนรหัสผ่าน



ภาพที่ 17 ผังแสดงการทำงานของการเปลี่ยนรหัสผ่าน

อธิบายการทำงานของส่วนการเปลี่ยนรหัสผ่าน

1.2.1 รับข้อมูล Username, Passwordเดิม,Password ใหม่,ยืนยัน Password ใหม่

1.2.2 ตรวจสอบข้อมูล Username, Passwordเดิม,Password ใหม่,ยืนยัน Password ใหม่ ว่าข้อมูลถูกต้องหรือไม่

1.2.3 หากข้อมูล Username, Password เดิม,Password ใหม่ , ยืนยัน Password ใหม่ ไม่ตรง ก็จะให้กลับไปรับข้อมูลใหม่

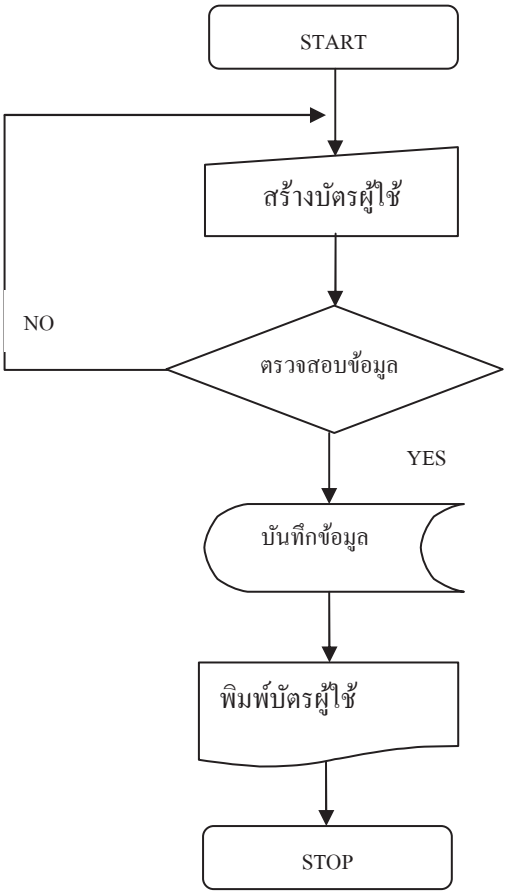
1.2.4 หากข้อมูล Username , Passwordเดิม , Password ใหม่ , ยืนยัน Password ใหม่ ถูกต้อง การเปลี่ยนรหัสผ่านสำเร็จ

1.2.5 จบการทำงาน

2. ส่วนของผู้ดูแลระบบ จะทำงานโดยแบ่งเป็น 2 ส่วนคือ

2.1 ส่วนจัดการผู้ใช้

2.1.1 การสร้างบัตรผู้ใช้



ภาพที่ 18 ผังแสดงการทำงานการสร้างบัตรผู้ใช้

อธิบายการทำงานของส่วนการสร้างบัตรผู้ใช้

2.1.1.1 สร้างบัตรผู้ใช้ ด้วยการกรอกข้อมูล คำขึ้นต้นชื่อผู้ใช้ , จำนวนที่ต้องการสร้าง , ราคา , วันที่บัตรหมดอายุ

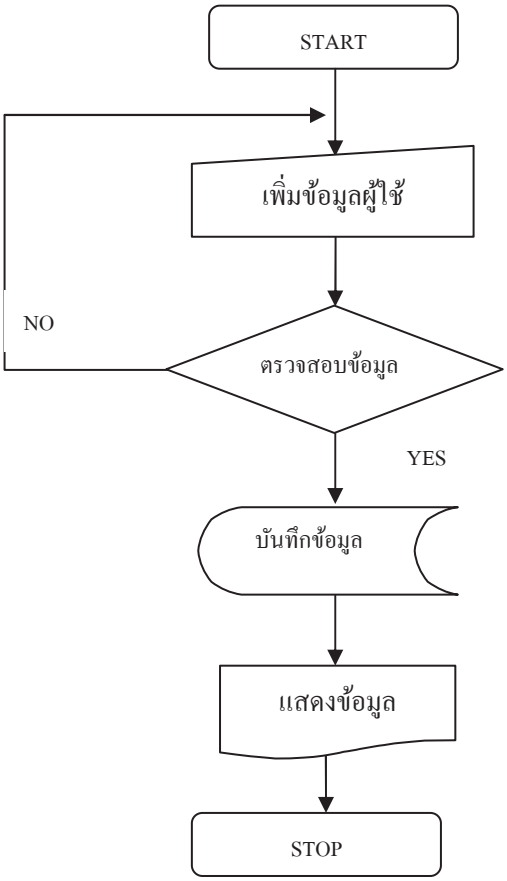
2.1.1.2 ตรวจสอบข้อมูลบัตรผู้ใช้

2.1.1.3 หากข้อมูลไม่ถูกต้องให้กลับไปสร้างบัตรผู้ใช้ใหม่

2.1.1.4 หากข้อมูลถูกต้องบันทึกบัตรผู้ใช้และพิมพ์บัตรผู้ใช้

2.1.1.5 จบการทำงาน

2.1.2 การเพิ่มผู้ใช้ใหม่



ภาพที่ 19 ผังแสดงการทำงานของการเพิ่มผู้ใช้เข้าสู่ระบบ

อธิบายการทำงานของส่วนเพิ่มผู้ใช้ใหม่

2.1.2.1 เพิ่มข้อมูลผู้ใช้ ประกอบด้วย เลือกกลุ่ม,เลขบัตรประชาชน ,ชื่อ,สกุล,ที่อยู่,เบอร์ติดต่อ,e-Mail, Username, รหัสผ่าน

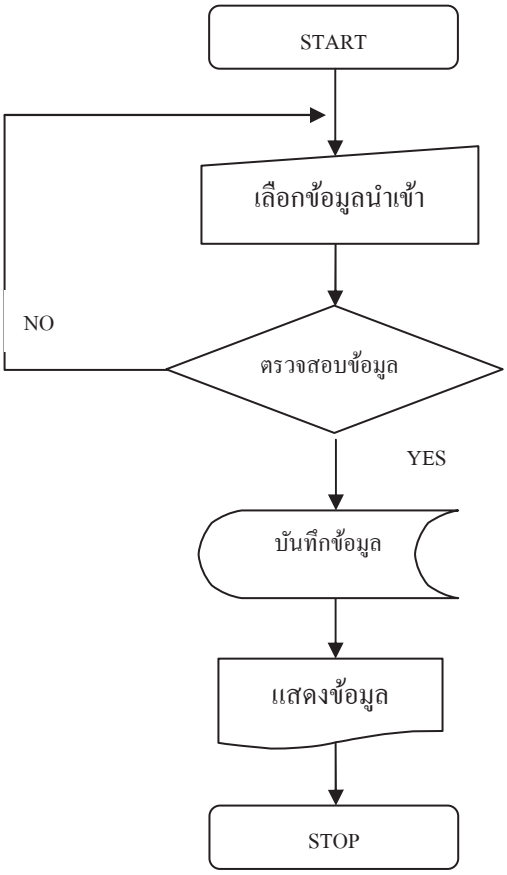
2.1.2.2 ตรวจสอบข้อมูลผู้ใช้

2.1.2.3 หากข้อมูลไม่ถูกต้องให้กลับไปเพิ่มผู้ใช้ใหม่

2.1.2.4 หากข้อมูลถูกต้องบันทึกข้อมูลและแสดงข้อมูลผู้ใช้

2.1.2.5 จบการทำงาน

2.1.3 ผู้ใช้นำเข้าจาก Excel



ภาพที่ 20 ผังแสดงการทำงานของการนำข้อมูลเข้าจาก Excel file

อธิบายการทำงานของส่วนผู้ใช้นำเข้าจาก Excel

2.1.3.1 เลือกแฟ้มข้อมูลนำเข้าจาก Excel ซึ่งประกอบด้วย Field : เลขบัตรประชาชน , ชื่อผู้ใช้, รหัสผ่าน,ชื่อ,สกุล,อีเมล์,ที่อยู่,เบอร์ติดต่อ

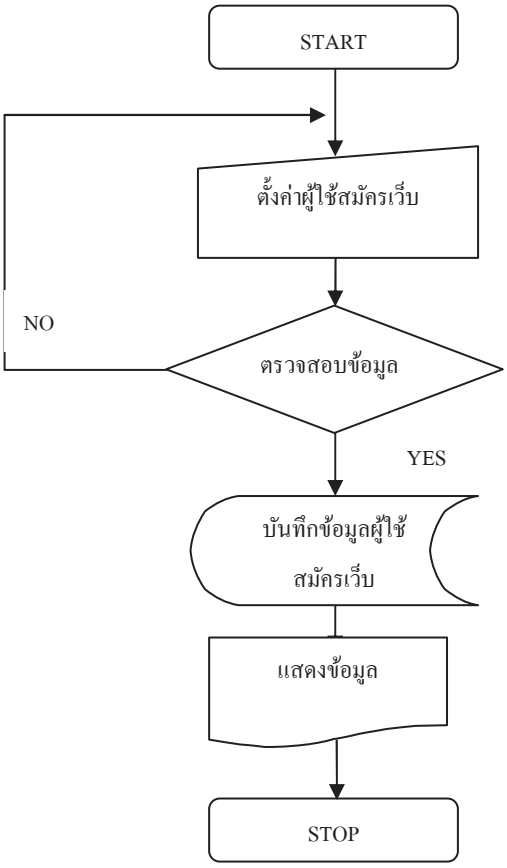
2.1.3.2 ตรวจสอบข้อมูลนำเข้า

2.1.3.3 หากข้อมูลไม่ต้องถูกต้องให้กลับไปนำเข้าข้อมูลจาก Excel ใหม่

2.1.3.4 หากข้อมูลถูกต้องบันทึกข้อมูลแสดงข้อมูลผู้ใช้

2.1.3.5 จบการทำงาน

2.1.4 การตั้งค่าผู้ใช้สมัครเว็บ



ภาพที่ 21 ผังแสดงการทำงานตั้งค่าผู้ใช้สมัครเว็บ

อธิบายการทำงานของส่วนตั้งค่าผู้ใช้สมัครเว็บ

2.1.4.1 ตั้งค่าผู้ใช้ที่ขอสมัครใช้งานผ่านเว็บ ประกอบด้วยความเร็วอินเทอร์เน็ต , ระยะเวลาหยุดการใช้งานอัตโนมัติ เมื่อไม่ได้ใช้งาน , ตรวจสอบการใช้งาน และเว็บไซต์ที่เริ่มใช้งาน

2.1.4.2 ตรวจสอบข้อมูลการตั้งค่า

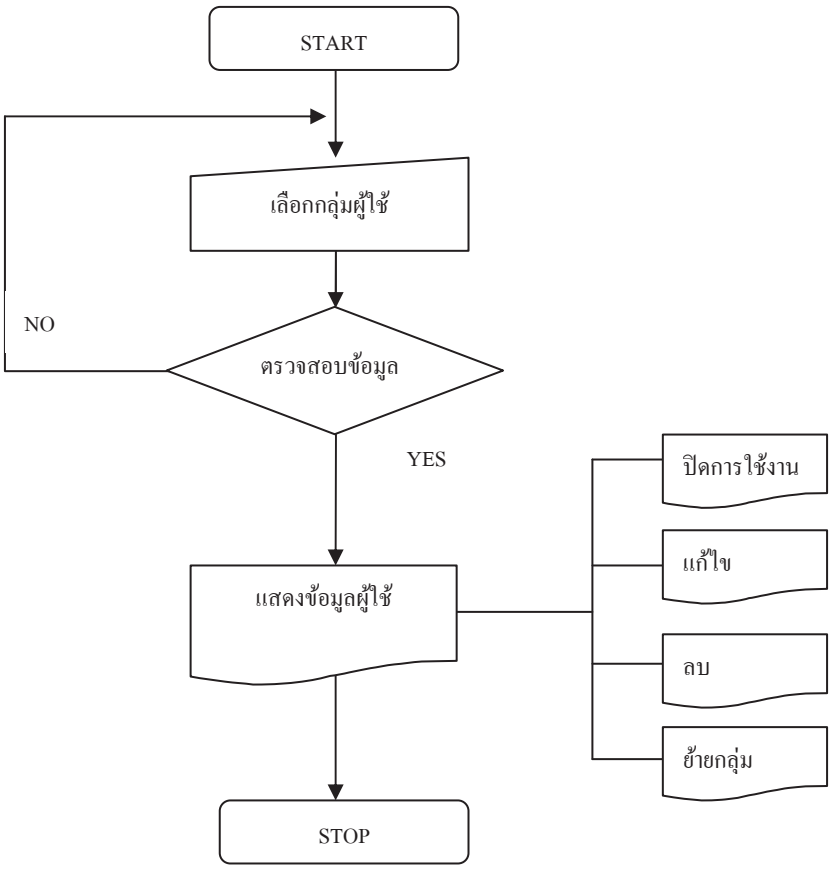
2.1.4.3 หากข้อมูลไม่ถูกต้องให้กลับไปตั้งค่าใหม่

2.1.4.4 หากข้อมูลถูกต้องบันทึกข้อมูลและแสดงข้อมูลการตั้งค่าผู้ใช้สมัครเว็บ

2.1.4.5 จบการทำงาน

2.2 ส่วนจัดการผู้ใช้

2.2.1 ส่วนจัดการข้อมูลผู้ใช้



ภาพที่ 22 ผังแสดงการทำงานของส่วนจัดการข้อมูลผู้ใช้

อธิบายการทำงานของส่วนจัดการข้อมูลผู้ใช้

2.2.1.1 เลือกกลุ่มผู้ใช้เพื่อแสดงข้อมูลผู้ใช้ในกลุ่มนั้น ๆ

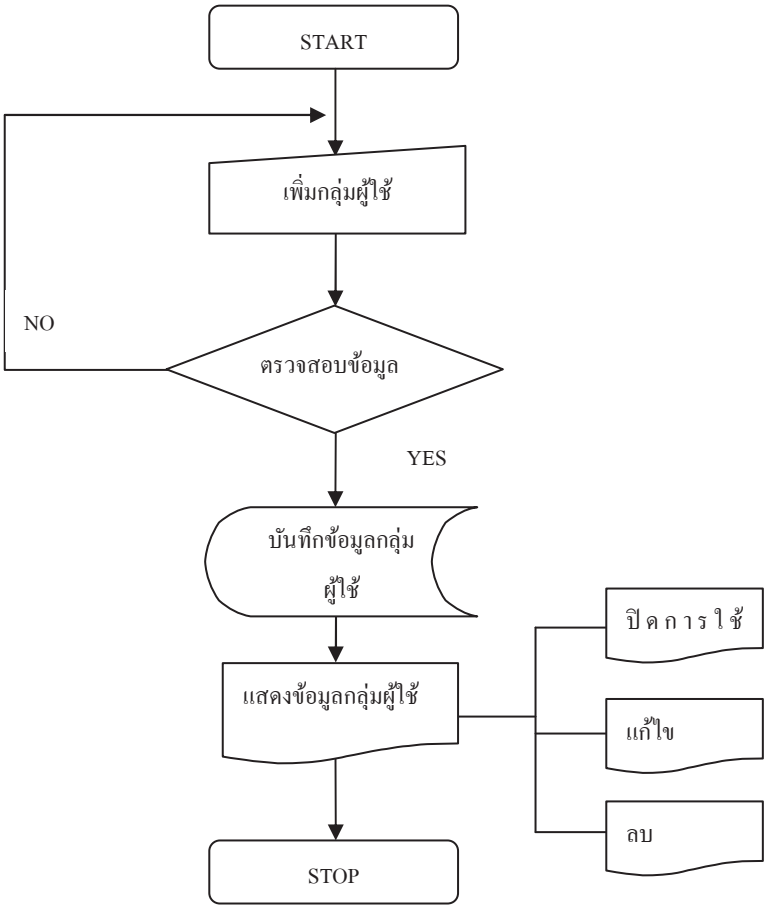
2.2.1.2 ตรวจสอบข้อมูลจากกลุ่มผู้ใช้ที่เลือก

2.2.1.3 หากข้อมูลไม่ถูกต้องให้กลับไปเลือกกลุ่มผู้ใช้ใหม่

2.2.1.4 หากข้อมูลถูกต้องแสดงข้อมูลผู้ใช้ ซึ่งสามารถดำเนินการปิดการใช้งาน ลบ แก้ไข และย้ายกลุ่มของผู้ใช้ได้

2.2.1.5 จบการทำงาน

2.2.2 ส่วนจัดการกลุ่มผู้ใช้



ภาพที่ 23 ผังแสดงการทำงานของส่วนจัดการกลุ่มผู้ใช้

อธิบายการทำงานของส่วนจัดการกลุ่มผู้ใช้

2.2.2.1 เพิ่มกลุ่มผู้ใช้ และกำหนดรายละเอียดเกี่ยวกับระยะเวลาในการใช้งานแต่ละครั้ง,ระยะเวลาในการใช้งานแต่ละวัน , หยุดการใช้งานอัตโนมัติ เมื่อไม่ได้ใช้งาน , ตรวจสอบสถานะ ,เมื่อเริ่มใช้งานให้เข้าเว็บไซต์

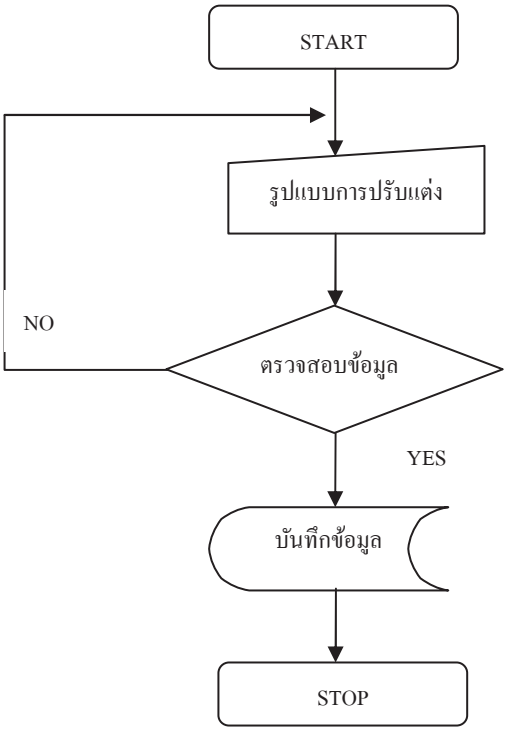
2.2.2.2 ตรวจสอบข้อมูลกลุ่มผู้ใช้ที่เพิ่ม

2.2.2.3 หากข้อมูลไม่ถูกต้องให้กลับไปเพิ่มกลุ่มผู้ใช้ใหม่

2.2.2.4 หากข้อมูลถูกต้องบันทึกข้อมูลและแสดงข้อมูลกลุ่มผู้ใช้ ซึ่งสามารถดำเนินการปิดการใช้งาน ลบ และแก้ไขได้

2.2.2.5 จบการทำงาน

2.2.3 ส่วนการปรับแต่งหน้าจอล็อกอิน



ภาพที่ 24 ผังแสดงการทำงานของส่วนการปรับแต่งหน้าจอล็อกอิน

อธิบายการทำงานของส่วนการปรับแต่งหน้าจอล็อกอิน

2.2.3.1 เลือกรูปแบบการปรับแต่ง ซึ่งประกอบ ธีมและข้อความอธิบาย

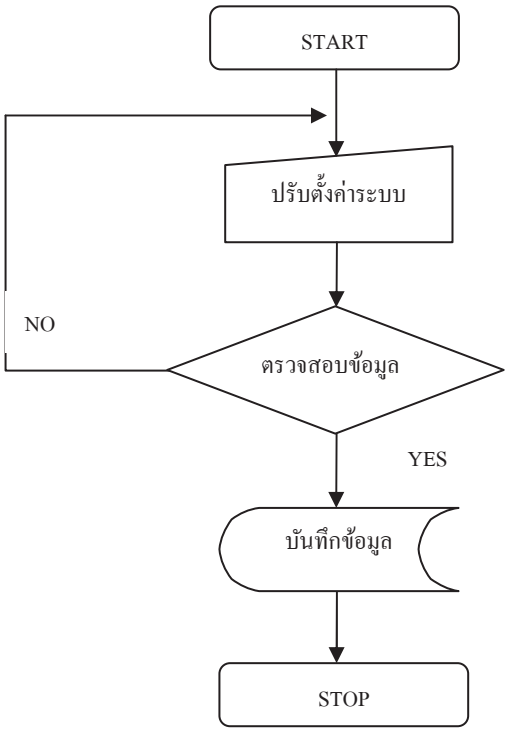
2.2.3.2 ตรวจสอบข้อมูลการปรับแต่ง

2.2.3.3 หากข้อมูลไม่ถูกต้องให้กลับไปปรับแต่งหน้าจอล็อกอินใหม่

2.2.3.4 หากข้อมูลถูกต้องบันทึกข้อมูล

2.2.3.5 จบการทำงาน

2.2.4 ส่วนการตั้งค่าระบบ



ภาพที่ 25 ผังแสดงการทำงานของส่วนการตั้งค่าระบบ

อธิบายการทำงานของส่วนการปรับตั้งค่าระบบ

2.2.4.1 ปรับตั้งค่าระบบ ประกอบด้วยชื่อหน่วยงาน , การเปิดระบบสมัครสมาชิกและเปลี่ยนรหัสผ่าน

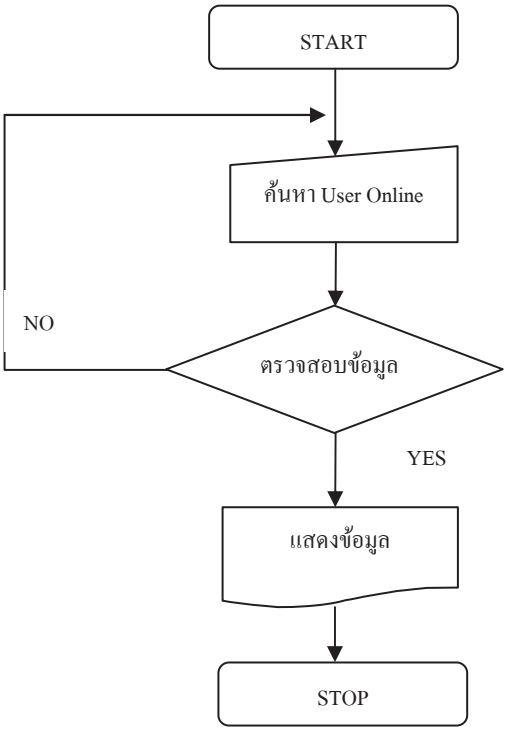
2.2.4.2 ตรวจสอบข้อมูลการปรับตั้งค่าระบบ

2.2.4.3 หากข้อมูลไม่ถูกต้องให้กลับไปปรับตั้งค่าระบบใหม่

2.2.4.4 หากข้อมูลถูกต้องบันทึกข้อมูล

2.2.4.5 จบการทำงาน

2.2.5 ผู้ที่กำลังใช้งานอยู่



ภาพที่ 26 ผังแสดงการทำงานของส่วนผู้ที่กำลังใช้งานอยู่

อธิบายการทำงานของส่วนผู้ที่กำลังใช้งานอยู่

2.2.5.1 ค้นหา User Online ในระบบ

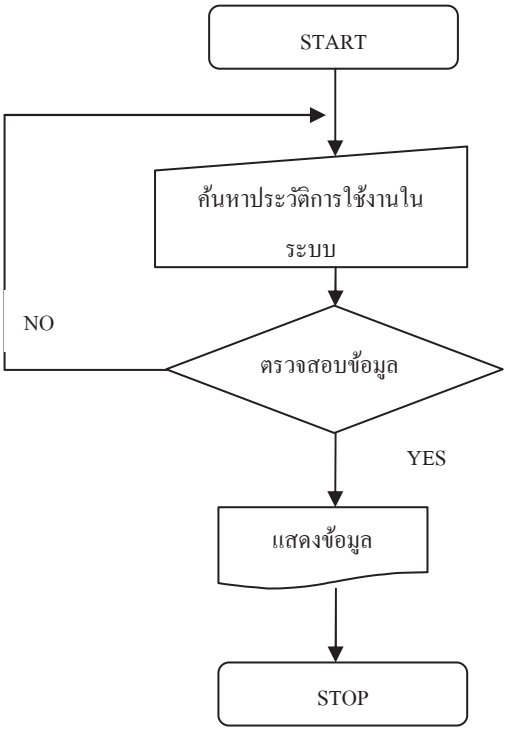
2.2.5.2 ตรวจสอบข้อมูล User Online

2.2.5.3 หากข้อมูลไม่ถูกต้องให้กลับไปค้นหาใหม่

2.2.5.4 หากข้อมูลถูกต้องแสดงข้อมูล User Online ในระบบ

2.2.5.5 จบการทำงาน

2.2.6 ประวัติการใช้งาน



ภาพที่ 27 ผังแสดงการทำงานของส่วนประวัติการใช้งาน

อธิบายการทำงานของส่วนประวัติการใช้งาน

2.2.6.1 ค้นหาประวัติข้อมูลผู้ใช้งานในระบบ โดยสามารถค้นหาได้จากวันที่เริ่มใช้งาน-วันที่สิ้นสุดใช้งานและUsername

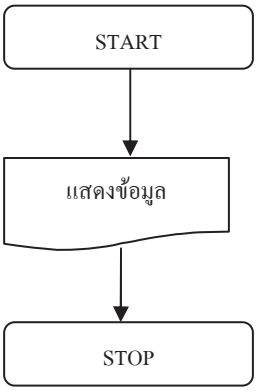
2.2.6.2 ตรวจสอบข้อมูลผู้ใช้งาน

2.2.6.3 หากข้อมูลไม่ถูกต้องให้กลับไปค้นหาใหม่

2.2.6.4 หากข้อมูลถูกต้องแสดงข้อมูลประวัติผู้ใช้งานในระบบ

2.2.6.5 จบการทำงาน

2.2.7 สถิติการใช้งาน



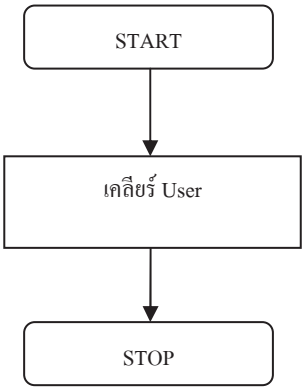
ภาพที่ 28 ผังแสดงการทำงานของส่วนสถิติการใช้งาน

อธิบายการทำงานของส่วนสถิติการใช้งาน

2.2.7.1 แสดงข้อมูลสถิติการใช้งาน โดยนับค่าการ Connect ของ User ในแต่ละเดือน

2.2.7.2 จบการทำงาน

2.2.8 เคลียร์ User ค้างในระบบ



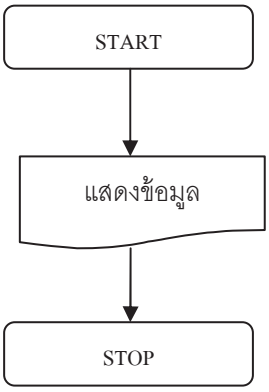
ภาพที่ 29 ผังแสดงการทำงานของส่วนเคลียร์ User ค้างในระบบ

อธิบายการทำงานของส่วนเคลียร์ User ค้างในระบบ

2.2.8.1 เมื่อพบว่ามี User ค้างในระบบเป็นจำนวนมาก ต้องการเคลียร์แบบครั้งเดียวหมด ให้เข้าสู่เมนูเคลียร์ User ค้างในระบบ แล้วดำเนินการลบข้อมูล

2.2.8.2 จบการทำงาน

2.2.9 คู่มือการใช้



ภาพที่ 30 ผังแสดงการทำงานของส่วนคู่มือการใช้

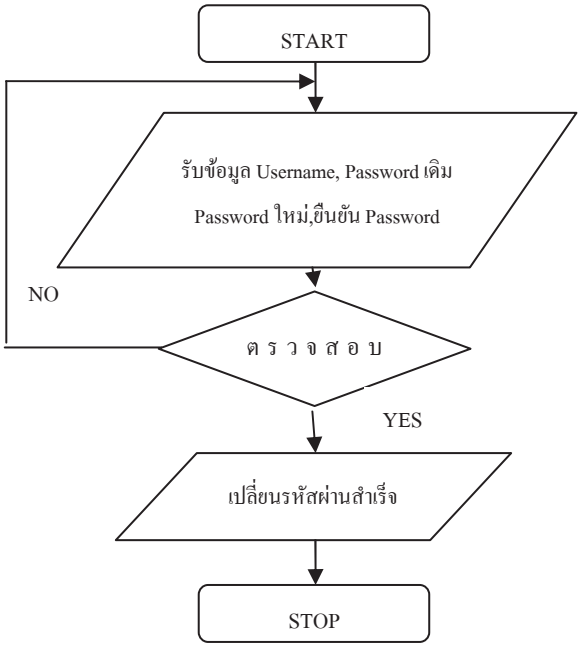
อธิบายการทำงานของส่วนคู่มือการใช้

2.2.9.1 แสดงข้อมูลคู่มือการใช้งานโปรแกรมส่วนของการจัดการผู้ใช้

2.2.9.2 จบการทำงาน

2.3 ส่วนจัดการระบบ

2.3.1 เปลี่ยนรหัสผู้ดูแลระบบ



ภาพที่ 31 ผังแสดงการทำงานของส่วนเปลี่ยนรหัสผู้ดูแลระบบ

อธิบายการทำงานของส่วนการเปลี่ยนรหัสผ่าน

2.3.1.1 รับข้อมูล Password เดิม,Password ใหม่,ยืนยัน Password ใหม่

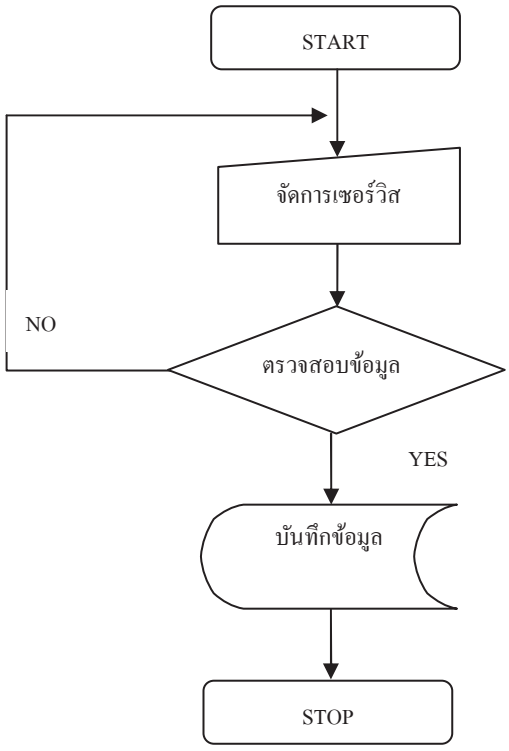
2.3.1.2 ตรวจสอบข้อมูล Password เดิม,Password ใหม่,ยืนยัน Password ใหม่ ว่าข้อมูลถูกต้องหรือไม่

2.3.1.3 หากข้อมูล Password เดิม,Password ใหม่ , ยืนยัน Password ใหม่ ไม่ตรง ก็จะให้กลับไปรับข้อมูลใหม่

2.3.1.4 หากข้อมูล Password เดิม , Password ใหม่ , ยืนยัน Password ใหม่ ถูกต้อง การเปลี่ยนรหัสผ่านสำเร็จ

2.3.1.5 จบการทำงาน

2.3.2 จัดการเซอร์วิส



ภาพที่ 32 ผังแสดงการทำงานของส่วนการจัดการเซอร์วิส

อธิบายการทำงานของส่วนการจัดการเซอร์วิส

2.3.2.1 จัดการเซอร์วิสในระบบ ประกอบด้วย service ดังนี้ HTTP, MYSQL , FREERADIUS, CHILLI, SQUID

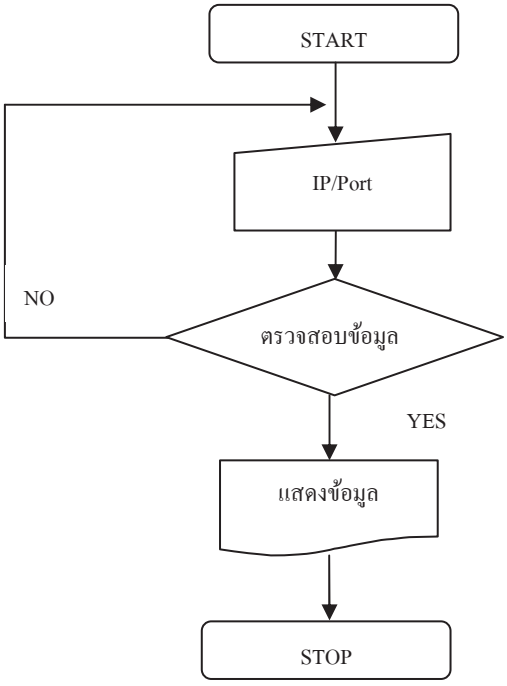
2.3.2.2 ตรวจสอบข้อมูลเซอร์วิส

2.3.2.3 หากสถานะเซอร์วิสไม่ถูกต้องให้กลับไปจัดการเซอร์วิสใหม่

2.3.2.4 หากสถานะเซอร์วิสถูกต้องบันทึกข้อมูล

2.3.2.5 จบการทำงาน

2.3.3 ตรวจสอบ IP/Port



ภาพที่ 33 ผังแสดงการทำงานของส่วนตรวจสอบ IP/Port

อธิบายการทำงานของส่วนตรวจสอบ IP/Port

2.3.3.1ใส่ IP หรือ Port ที่ต้องการตรวจสอบสถานะ

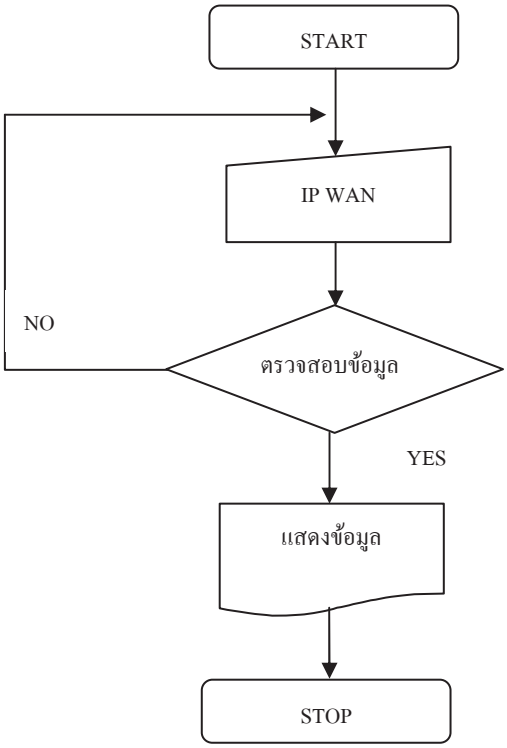
2.3.3.2 ตรวจสอบสถานะ IP หรือ Port

2.3.3.3 หากสถานะ IP หรือ Port ไม่ถูกต้องกลับไปตรวจสอบอีกครั้ง

2.3.3.4 หากสถานะ IP หรือ Port ที่ถูกต้อง แสดงข้อมูล

2.3.3.5 จบการทำงาน

2.3.4 ตรวจสอบ WAN



ภาพที่ 34 ผังแสดงการทำงานของส่วนตรวจสอบ WAN

อธิบายการทำงานของส่วนตรวจสอบ WAN

2.3.4.1 ใส่ IP ที่ต้องการตรวจสอบ WAN

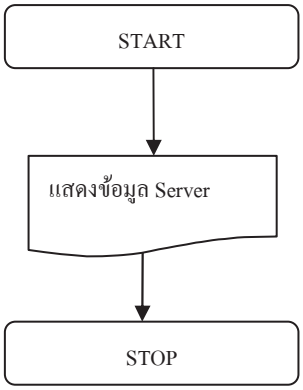
2.3.4.2 ตรวจสอบสถานะ WAN ของ IP

2.3.4.3 หากสถานะ WAN IP ไม่ถูกต้องกลับไปตรวจสอบอีกครั้ง

2.3.4.4 หากสถานะ WAN IP ถูกต้อง แสดงข้อมูล

2.3.4.5 จบการทำงาน

2.3.5 แสดงข้อมูล Server



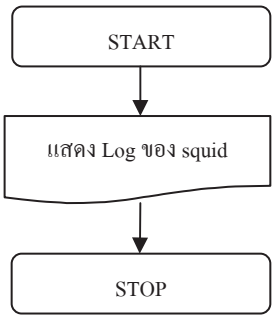
ภาพที่ 35 ผังแสดงการทำงานของส่วนแสดงข้อมูล Server

อธิบายการทำงานของส่วนแสดงข้อมูล Server

2.3.5.1 แสดงสถานะของ Server ประกอบด้วย System Virtal , Hardware Information, Memory Usage , Mounted File Systems , Network Usages

2.3.5.2 จบการทำงาน

2.3.6 บันทึก พรบ. 50



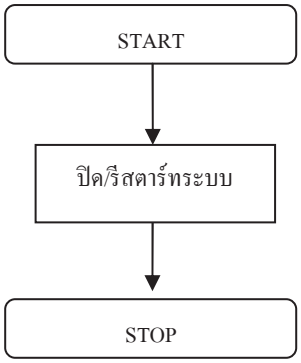
ภาพที่ 36 ผังแสดงการทำงานของส่วน บันทึก พรบ. 50

อธิบายการทำงานของส่วนบันทึก พรบ.50

2.3.6.1 แสดง Log ของ squid โดยตรวจสอบจาก IP

2.3.6.2 จบการทำงาน

2.3.7 ปิด/รีสตาร์ทระบบ



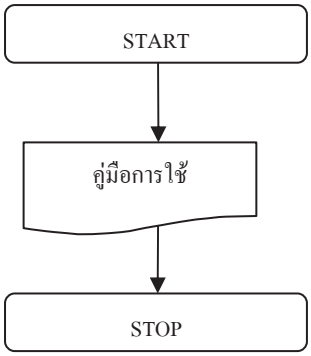
ภาพที่ 37 ผังแสดงการทำงานของส่วนปิด/รีสตาร์ทระบบ

อธิบายการทำงานของส่วนปิด/รีสตาร์ทระบบ

2.3.7.1 ปิดหรือรีสตาร์ทระบบของเครื่อง Server

2.3.7.2 จบการทำงาน

2.3.8 คู่มือการใช้



ภาพที่ 38 ผังแสดงการทำงานของส่วนคู่มือการใช้

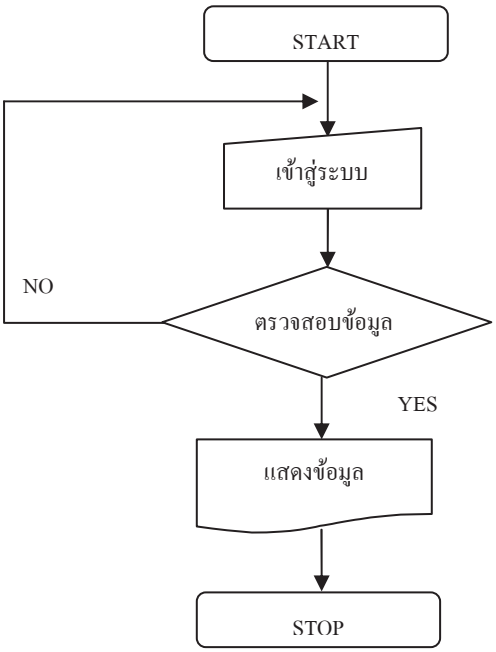
อธิบายการทำงานของส่วนคู่มือการใช้

2.3.8.1 แสดงคู่มือการใช้งานส่วนของเมนูการจัดการระบบ

2.3.8.2 จบการทำงาน

3. ส่วนผู้บริหาร

3.1 รายงานการใช้งานระบบ



ภาพที่ 39 ผังแสดงการทำงานของส่วนรายงานการใช้งานระบบ สำหรับผู้บริหาร

อธิบายการทำงานของรายงานการใช้งาน

3.1.1 ผู้บริหาร Login เข้าสู่ระบบ

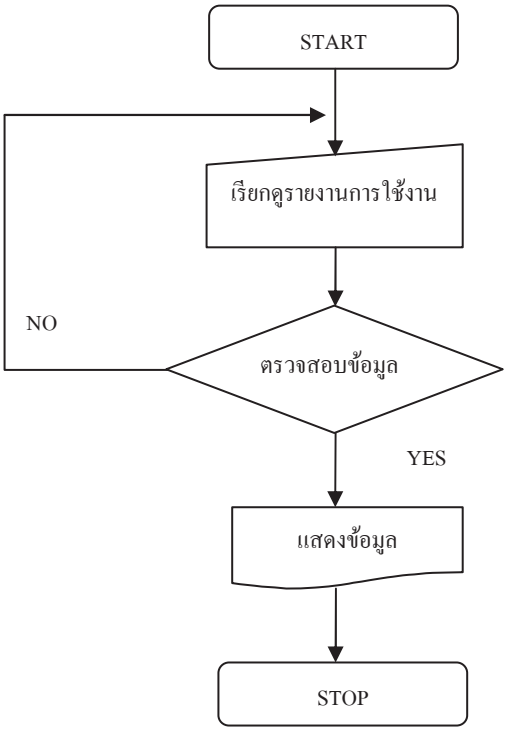
3.1.2 ตรวจสอบข้อมูลชื่อผู้ใช้และรหัสผ่าน

3.1.3 หากชื่อผู้ใช้และรหัสผ่านไม่ถูกต้อง ให้เข้าสู่ระบบใหม่

3.1.4 หากชื่อผู้ใช้และรหัสผ่านถูกต้อง เข้าสู่หน้าแสดงรายละเอียดข้อมูลการเข้าใช้งานเว็บไซต์ ซึ่งประกอบด้วยวันที่เข้าใช้งาน , ip address , เวลา และ url

3.1.5 จบการทำงาน

3.2 รายงานการใช้งานอินเทอร์เน็ต



ภาพที่ 40 ผังแสดงรายงานการใช้งานอินเทอร์เน็ต

อธิบายการทำงานของส่วนรายงานการใช้งานอินเทอร์เน็ต

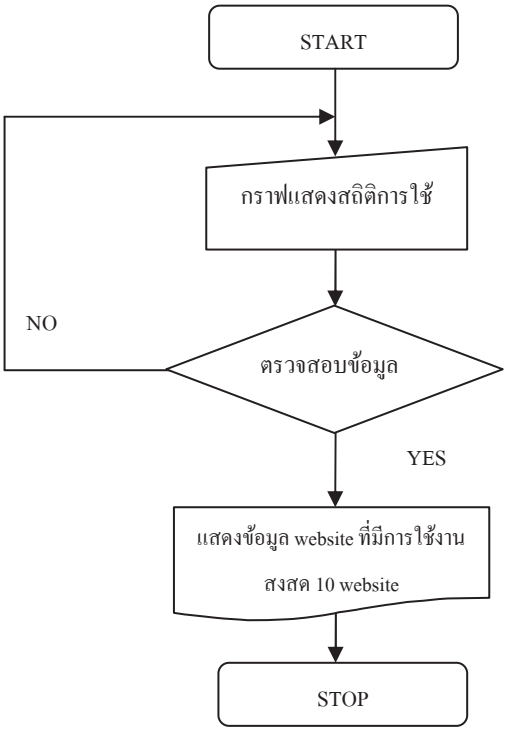
3.2.1 การเรียกดูรายงานการใช้งานอินเตอร์เน็ตของผู้ใช้งานสำหรับผู้บริหาร โดยเลือกจากวันที่และชื่อผู้ใช้ที่ผู้บริหารต้องการดูสถิติการใช้งานอินเทอร์เน็ต

3.2.2 ตรวจสอบข้อมูลการใช้อินเทอร์เน็ต

3.2.3 หากไม่พบข้อมูลให้กลับไปตรวจสอบอีกครั้ง กรณีที่พบข้อมูลให้แสดงผล

3.2.4 จบการทำงาน

3.3 กราฟแสดงสถิติการใช้งานอินเทอร์เน็ต



ภาพที่ 41 ผังกราฟแสดงสถิติการใช้งานอินเทอร์เน็ต

อธิบายการทำงานของส่วนกราฟแสดงสถิติการใช้งาน

3.3.1 กราฟแสดงสถิติการใช้งานสำหรับผู้บริหาร โดยระบบจะแสดงข้อมูล website ที่มีการใช้งานสูงสุด 10 website

3.3.2 ตรวจสอบข้อมูลการใช้งานสูงสุด 10 website

3.3.3 หากไม่พบข้อมูลให้กลับไปตรวจสอบอีกครั้ง กรณีที่พบข้อมูลให้แสดงผล

3.3.4 จบการทำงาน

โครงสร้างฐานข้อมูลระบบบริหารจัดการข้อมูลจราจรทางคอมพิวเตอร์

โครงสร้างฐานข้อมูลระบบบริหารจัดการข้อมูลจราจรทางคอมพิวเตอร์ ประกอบด้วย ระบบตรวจสอบสิทธิในการเข้าใช้งาน กำหนดผู้มีสิทธิใช้งาน การอนุญาตให้ใช้งาน ประกอบด้วย ตารางต่าง ๆ ซึ่งส่วนหนึ่งเป็นการ download โปรแกรมฟรีจาก http://www.linuxthai.org/forum/index.php?topic=3207.0 นำมาแก้ไข ดังนี้

ตารางที่ 1 โครงสร้างตาราง account

ชื่อตาราง : account				
รายละเอียดตาราง : เก็บข้อมูลรายละเอียดของผู้มีสิทธิใช้งานระบบ				
ชื่อรายการข้อมูล	**ประเภท**	**ขนาด**	**คำอธิบาย/ตัวอย่างข้อมูล**	**ตารางอ้างอิง**
Username	Varchar	20	ชื่อผู้ใช้	
Password	Varchar	32	รหัสผ่าน	
Firstname	Varchar	50	ชื่อผู้ใช้	
Lastname	Varchar	50	นามสกุลผู้ใช้	
Dateregis	Datetime	8	วันที่ลงทะเบียนใช้งาน	
Idn	Int	13	เลขบัตรประชาชน 13 หลัก	
Status	Int	1		
Mailaddr	Varchar	50	e-mail ผู้ใช้	
Addr	Varchar	100	ที่อยู่ผู้ใช้	
Tel	Varchar	25	โทรศัพท์ผู้ใช้	

ตารางที่ 2 โครงสร้างตาราง administrator

ชื่อตาราง : administrator				
รายละเอียดตาราง : เก็บข้อมูลรายละเอียดของผู้ดูแลระบบ				
ชื่อรายการข้อมูล	**ประเภท**	**ขนาด**	**คำอธิบาย/ตัวอย่างข้อมูล**	**ตารางอ้างอิง**
Username	Varchar	20	ชื่อผู้ดูแลระบบ	
Password	Varchar	32	รหัสผ่านผู้ดูแลระบบ	
Name	Varchar	50	ชื่อผู้ดูแลระบบ	
Lastlogin	Datetime	8	วันเวลาที่เข้าครั้งสุดท้าย	

ตารางที่ 3 โครงสร้างตาราง group

ชื่อตาราง : group				
รายละเอียดตาราง : เก็บข้อมูลรายละเอียดของกลุ่มผู้ใช้งาน				
ชื่อรายการข้อมูล	**ประเภท**	**ขนาด**	**คำอธิบาย/ตัวอย่างข้อมูล**	**ตารางอ้างอิง**
gid (PK)	Int	2		
Gname	Varchar	50	ชื่อกลุ่มที่ให้ใช้งาน	
Gdesc	Varchar	50	คำอธิบายชื่อกลุ่ม	
Gupload	Int	8	ความเร็วในการ upload	
Gdownloag	Int	8	ความเร็วในการ download	
Gexpire	Date	3	วันหมดอายุใช้งาน	
Glimited	Int	8		
Gstatus	Int	1		

ตารางที่ 4 โครงสร้างตาราง radacct

ชื่อตาราง : radacct				
รายละเอียดตาราง : เก็บข้อมูลรายละเอียดการใช้งานของ user				
ชื่อรายการข้อมูล	**ประเภท**	**ขนาด**	**คำอธิบาย/ตัวอย่างข้อมูล**	**ตารางอ้างอิง**
radacctid (PK)	bigint	5	รหัสการใช้งาน	
Acctsessionid	varchar	16	Session ที่เข้าใช้งาน	
Acctuniqueid	varchar	16		
Username	varchar	20	ชื่อผู้ใช้งาน	radcheck
Groupname	varchar	50	กลุ่มที่ใช้งาน	
Nasipaddress	varchar	15	Ip nas	
Nasportid	varchar	6	Port nas	
Nasporttype	varchar	32	ชนิดของ port nas	
Acctstarttime	datetime	8	เวลาที่เริ่มใช้งาน	
Acctstoptime	datetime	8	เวลาที่ออกจากระบบ	
Acctsessiontime	Int	12	จำนวนเวลาที่ใช้งานระบบ	

ตารางที่ 4 (ต่อ)

ชื่อรายการข้อมูล	ประเภท	ขนาด	คำอธิบาย/ตัวอย่างข้อมูล	ตารางอ้างอิง
Acctinputoctets	bigint	15		
acctoutputoctets	bigint	15		
Calledstationid	varchar	17		
Callingstationid	varchar	17	Mac Address ของเครื่องที่ใช้	
Acctterminatecause	varchar	20	เหตุของการออกจากระบบ	
Framedipaddress	varchar	15	IP ที่เข้าใช้งานระบบ	

ตารางที่ 5 โครงสร้างตาราง radcheck

ชื่อตาราง : radcheck				
รายละเอียดตาราง : เก็บข้อมูลชื่อผู้ใช้-รหัสผ่าน				
ชื่อรายการข้อมูล	**ประเภท**	**ขนาด**	**คำอธิบาย/ตัวอย่างข้อมูล**	**ตารางอ้างอิง**
id(PK)	Int	5	รหัส	
UserName	Varchar	20	ชื่อผู้ใช้	
Op	Char	2	= =	
Value	Varchar	32	Password ที่ใช้	

ตารางที่ 6 โครงสร้างตาราง radgroupcheck

ชื่อตาราง : radgroupcheck				
รายละเอียดตาราง : กำหนดคุณสมบัติการใช้งานของกลุ่มใช้งาน				
ชื่อรายการข้อมูล	**ประเภท**	**ขนาด**	**คำอธิบาย/ตัวอย่างข้อมูล**	**ตารางอ้างอิง**
id(PK)	Int	5	รหัส	
groupname	Varchar	50	ชื่อกลุ่ม	radcheck
Attribute	Varchar	25	ประเภทการใช้งาน	
Op	Char	2	: =	
Value	Varchar	10	ค่าที่กำหนด	

ตารางที่ 7 โครงสร้างตาราง radgroupreply

ชื่อตาราง : radgroupreply				
รายละเอียดตาราง : เก็บข้อมูลรายละเอียดการใช้งานของผู้ใช้				
ชื่อรายการข้อมูล	**ประเภท**	**ขนาด**	**คำอธิบาย/ตัวอย่างข้อมูล**	**ตารางอ้างอิง**
id(PK)	Int	5	รหัส	
groupname	Varchar	50	ชื่อกลุ่ม	radcheck
Attribute	Varchar	25	ประเภทการใช้งาน	
Op	Char	2	:=	
Value	Varchar	50	ค่าที่กำหนดให้	

ตารางที่ 8 โครงสร้างตาราง radusergroup

ชื่อตาราง : radusergroup				
รายละเอียดตาราง : เก็บข้อมูลรายละเอียดกลุ่มผู้ใช้				
ชื่อรายการข้อมูล	**ประเภท**	**ขนาด**	**คำอธิบาย/ตัวอย่างข้อมูล**	**ตารางอ้างอิง**
UserName	Varchar	50	ชื่อผู้ใช้	
GroupName	Varchar	50	กลุ่มที่ใช้	
Priority	Int	1	1	

โครงสร้างฐานข้อมูลที่นำมาจัดทำรายงาน

โครงสร้างฐานข้อมูลที่นำมาจัดทำรายงานสร้างขึ้นเพื่อเก็บรายละเอียดการใช้งานอินเตอร์เน็ตของผู้ใช้งานในระบบทั้งหมด

ตารางที่ 9 โครงสร้างตาราง config

ชื่อตาราง : config				
รายละเอียดตาราง : เก็บข้อมูลรายละเอียดของระบบ				
ชื่อรายการข้อมูล	**ประเภท**	**ขนาด**	**คำอธิบาย/ตัวอย่างข้อมูล**	**ตารางอ้างอิง**
Name	Varchar	50	ชื่อไฟล์ config	
Value	Varchar	20	ค่าไฟล์ config	

ตารางที่ 10 โครงสร้างตาราง hostnames

ชื่อตาราง : hostnames				
รายละเอียดตาราง : เก็บข้อมูลรายละเอียดของ IP Address ที่เข้าใช้งานระบบ				
ชื่อรายการข้อมูล	**ประเภท**	**ขนาด**	**คำอธิบาย/ตัวอย่างข้อมูล**	**ตารางอ้างอิง**
id(PK)	Bigint	5	รหัส hostname	
Ip	Int	15	รหัส ip address	
Description	Varchar	50	รายละเอียด	
isResolved	Tinyint	1		
Hostname	Varchar	15	หมายเลข IP	

ตารางที่ 11 โครงสร้างตาราง sites

ชื่อตาราง : sites				
รายละเอียดตาราง : เก็บข้อมูลรายละเอียดของเว็บไซต์ที่เข้าใช้งาน				
ชื่อรายการข้อมูล	**ประเภท**	**ขนาด**	**คำอธิบาย/ตัวอย่างข้อมูล**	**ตารางอ้างอิง**
id(PK)	Bigint	5	รหัส Sites	
Date	Date	3	วันที่เข้าใช้งานระบบ	
Site	Varchar	70	เว็บไซต์ที่เข้า	

ตารางที่ 12 โครงสร้างตาราง traffic

ชื่อตาราง : traffic				
รายละเอียดตาราง : เก็บข้อมูลรายละเอียดการใช้งานของ user				
ชื่อรายการข้อมูล	**ประเภท**	**ขนาด**	**คำอธิบาย/ตัวอย่างข้อมูล**	**ตารางอ้างอิง**
id(PK)	Bigint	5	ลำดับที่	
Date	Date	3	วันที่เข้าใช้งาน	
Time	Time	3	เวลาที่เข้าใช้งาน	
ip(FK)	Int	15	ip address	hostnames
resultCode	Varchar	25	Protocol	
Bytes	Bigint	15	ขนาดไฟล์ที่ใช้งาน	
url	Varchar	120	เว็บไซต์ที่เข้าใช้งานระบบ	
sitesID(FK)	Bigint	5	รหัสเว็บไซต์	sites
usersID(FK)	Bigint	4	รหัสผู้ใช้	users

ตารางที่ 13 โครงสร้างตาราง trafficsummaries

ชื่อตาราง : trafficesummaries				
รายละเอียดตาราง : สรุปรายละเอียดการใช้งานระบบ				
ชื่อรายการข้อมูล	**ประเภท**	**ขนาด**	**คำอธิบาย/ตัวอย่างข้อมูล**	**ตารางอ้างอิง**
id(PK)	Bigint	4	ลำดับที่	
Date	Date	3	วันที่	
ip(FK)	Int	15	ip address	hostnames
usersID(FK)	Bigint	4	รหัสผู้ใช้	users
inCache	Bigint	15		
outCache	Bigint	15		
sitesID(FK)	Bigint	5	รหัสเว็บไซต์	sites
summaryTime	Tinyint	4		

ตารางที่ 14 โครงสร้างตาราง users

ชื่อตาราง : users				
รายละเอียดตาราง : ตารางข้อมูลผู้ใช้งานระบบ				
ชื่อรายการข้อมูล	**ประเภท**	**ขนาด**	**คำอธิบาย/ตัวอย่างข้อมูล**	**ตารางอ้างอิง**
id(PK)	Bigint	4	รหัส	
Date	Date	3	วันที่เข้าใช้งานระบบ	

บทที่ 4
ผลการดำเนินการวิจัย

จากขั้นตอนการดำเนินการวิจัย สามารถอธิบายผลการดำเนินการ ได้ดังนี้

1. เตรียมข้อมูล/อุปกรณ์/ออกแบบ

เตรียมข้อมูล คือการให้ได้มาซึ่งข้อมูลที่ถูกต้องครบถ้วน ซึ่งจะเป็นข้อมูลชื่อพนักงาน ลูกจ้าง รหัสพนักงาน รหัสลูกจ้าง หมายเลขบัตรประจำตัวประชาชน ของพนักงาน ลูกจ้าง ในสังกัดสำนักงานบริการลูกค้า กสท เขตตะวันตก ทั้งหมด เพื่อใช้ในการตรวจสอบสิทธิในการเข้าใช้งานระบบ เตรียมอุปกรณ์ ขออนุญาตผู้บริหารใช้อุปกรณ์เครื่องแม่ข่ายและคอมพิวเตอร์ ที่มีอยู่มาลงโปรแกรม ubuntu และโปรแกรมอื่น ๆ ที่เกี่ยวข้องเพื่อให้สามารถทำงานได้ตามที่ออกแบบระบบไว้

ในการจัดเตรียมข้อมูล อุปกรณ์ ออกแบบนั้น ผู้วิจัยได้ใช้ซอร์ฟแวร์ที่ใช้ในการติดตั้งและออกแบบ ดังนี้

1.1 ดาวน์โหลด โปรแกรม ubuntu 9.04

1.2 ดาวน์โหลด โปรแกรม chillispot , Freeradius

1.3 จัดเตรียมเครื่องแม่ข่าย คอมพิวเตอร์ที่มีอยู่ โดยจัดหา Card Lan เพิ่ม

1.4 ออกแบบระบบ โดยใช้เครื่องแม่ข่ายที่มีอยู่ เพื่อทำระบบ Proxy &Authentication server และใช้คอมพิวเตอร์ที่มีทำเป็น NTP & Centralized log server

2. ติดตั้งโปรแกรม แก้ไข config

2.1 การติดตั้งเครื่อง Authentication Server โดยใช้ ubuntu และแก้ไข config ต่าง ๆ ลงโปรแกรม ubuntu และติดตั้งตามขั้นตอนของ ubuntu เมื่อติดตั้งสำเร็จ เข้าแก้ไขค่า config ต่าง ดังนี้

ตารางที่ 15 การแก้ไข config

ลำดับที่	ชื่อไฟล์	ตำแหน่ง	หน้าที่	รายละเอียดที่แก้ไข
1.	Interface	/etc/network/ Interface	เปิดใช้งาน internal lan card และปรับแต่ง network	กำหนด ip address ของ wan และ เปิด auto eth1
2.	resolv.conf	/etc/resolv.conf	กำหนดค่า DNS Server	ปรับแต่งค่า dns server ของ อินเทอร์เน็ต
3.	sysctl.conf	/etc/sysctl.conf	เปิด Forward IP	เปิด Forward IP จาก net.ipv4.ip_forward = 0 แก้เป็น 1
4.	Radiusd.conf	/etc/freeradius/ radiusd.conf	เป็นโปรแกรมที่ใช้ในการจัดการแอคเค้าท์และใช้ในการตรวจสอบสิทธิ ตามมาตรฐาน IEEE 802.1X ตามคอนเซ็ปคือ AAA คือ -Accounting คือการจัดการแอคเค้าท์ในด้านต่างๆทั้งการสร้างแอคเค้าท์ ลบ และเพิ่มแอคเค้าท์ ตลอดจนการเพิ่มเติมคุณสมบัติต่างๆของแต่ละแอคเค้าท์ Authentication สิทธิตามวิธีการ A แรกที่ได้กล่าวมา	กำหนดค่า directory ของ radius โดยเปลี่ยนค่าจาก radiusd เป็น freeradius

ตารางที่ 15 (ต่อ)

ลำดับที่	ชื่อไฟล์	ตำแหน่ง	หน้าที่	รายละเอียดที่แก้ไข
4 (ต่อ)			ในขั้นตอนนี้จะมีการแจ้งแมสเสจต่างๆว่าผ่านหรือไม่ผ่าน การตรวจสอบสิทธิและเมื่อผ่านกระบวนการนี้ได้สำเร็จก็จะเข้าสู่กระบวนการสุดท้าย นั่นคือ Authorize	
5.	Sql.conf	/etc/freeradius/ sql.conf	ไฟล์ปรับแต่งค่าเพื่อให้ freeradius ติดต่อกับฐานข้อมูล radius	บรรทัดที่36,37, 38, 41 ปรับแต่งค่าการเชื่อมต่อฐานข้อมูล
6.	Default	/etc/freeradius/sites-enabled/default	เปิดใช้งาน sql	บรรทัดที่ 152,346 เอาเครื่องหมาย # ออก เพื่อให้ freeradius สามารถใช้งาน sql ได้
7.	Chilli	/etc/default/chilli	ปิด-เปิดการทำงานของ chilli	START_CHILLI=0 แก้เป็น START_CHILLI=1
8.	Config	/etc/chilli/config	ปรับแต่งค่า network lan ของระบบหรือการสร้าง interfaces tun0 เพิ่มเข้ามาทำงาน	กำหนดค่า network ของ eth1

ตารางที่ 15 (ต่อ)

ลำดับที่	ชื่อไฟล์	ตำแหน่ง	หน้าที่	รายละเอียดที่แก้ไข
9.	chilli.iptables	/etc/init.d/chilli.iptables	การปรับแต่งค่า firewall เพื่อกำหนดให้เครื่อง client ออกอินเตอร์เน็ตโดยผ่าน proxy server	เป็นการปรับแต่งค่า network ของ eth0 และ eth1
10.	Default	/etc/apache2/sites-available/default	การสร้าง virtual host ของ hotspot	ปรับแต่ง ip ของ VirtualHost
11.	Apache2.conf	/etc/apache2/apache2.conf	ปรับแต่งโปรแกรม web server	กำหนด ServerName 10.23.51.254
12.	Hosts	/etc/hosts	การกำหนดพื้นที่ให้บริการ hosts	กำหนด ip ของเครื่องและตามด้วยชื่อเครื่อง
13.	squid.conf	/etc/squid/squid.conf	Squid มีคุณสมบัติในการจำกัด ควบคุมการแอกเซสเข้าสู่เว็บไซต์ภายนอกองค์กรได้เป็นอย่างดีและมีประสิทธิภาพ ที่เรียกว่า Access Control List	เป็นการกำหนดวงเครือข่ายอินเตอร์เน็ต การ block web และรูปแบบการส่ง log ของ squid
14.	Ntp.conf	/etc/ntp.conf	NTP เป็นโปรโตคอลที่ใช้ในการซิงโครไนซ์ เวลาของเครื่องบนเครือข่าย โดยมีกลไกรักษาและควบคุมเวลาได้ในระดับมิลลิวินาที	กำหนด IP server ที่จะอ้างอิง ntp

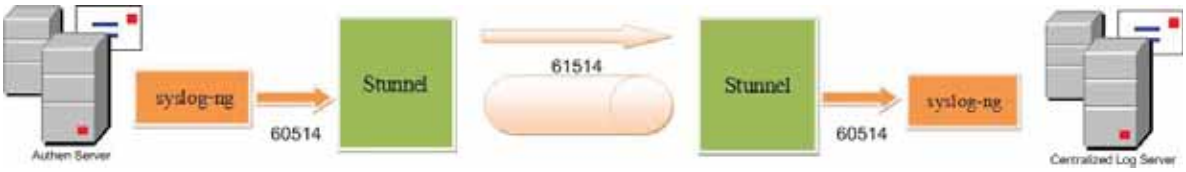
2.2 การติดตั้ง Centralized log Server

ตารางที่ 16 การแก้ไข config ใน Centralized log

ลำดับที่	ชื่อไฟล์	ตำแหน่ง	หน้าที่	รายละเอียดที่แก้ไข
1.	Syslog-ng.conf	/etc/syslog-ng/syslog-ng.conf	รองรับล็อกจากเครื่องลูกข่ายหรือเครื่องแม่ข่ายที่กำหนด	สร้าง source สำหรับใช้ในการรับข้อมูล โดยทำการเปิดพอร์ตทั้ง tcp/udp 60514 (เนื่องจากสร้าง tunnel จึงเปลี่ยน port จาก 514 เป็น 60514)
2.	Firewall.iptables	/etc/init.d/firewall.Iptables	เป็นไฟล์สำหรับการเปิด port จากภายนอกเพื่อส่ง Log มายังเครื่อง centralize log	ทำการเปิดพอร์ตในการทำงานทั้ง tcp/udp 60514 เพื่อส่ง log และ port 123 เพื่อส่ง log
3.	ntp.conf	/etc/ntp.conf	เป็นสื่อกลางในการส่งข้อมูลเวลามาตรฐานไปยังเครื่องลูกข่าย เพื่อปรับเทียบเวลาให้ตรงกับเวลามาตรฐาน	กำหนด NTP server เพื่อส่งเวลามาตรฐานไปยังเครื่องปลายทาง

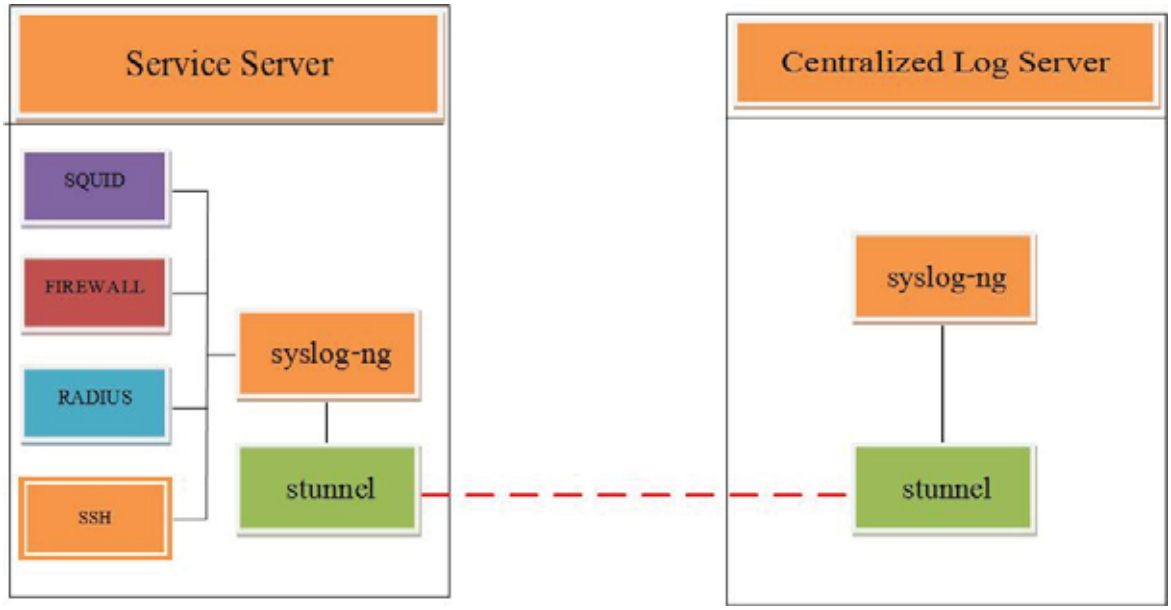
2.3 การทำ Stunnel เพื่อความปลอดภัยของการส่งข้อมูลระหว่างเครื่อง Authentication Server กับ Centralized log Server

ในการส่งข้อมูลจราจรคอมพิวเตอร์ใช้ syslog-ng ร่วมกับ Openssl และ Stunnel เข้ารหัสในระหว่างการส่ง เพื่อป้องกันการใช้โปรแกรมดักจับข้อมูลที่ส่งผ่านเครือข่าย ทำให้ข้อมูลที่จัดเก็บนั้นมีความน่าเชื่อถือเพิ่มมากขึ้น ดังภาพที่ 42



ภาพที่ 42 แสดงการส่งข้อมูล SSL Tunnel

ข้อมูลการใช้งานของผู้ใช้งานระบบไม่ว่าจะเป็นข้อมูลใน squid , firewall , radius และ ssh จากเครื่องแม่ข่าย จะถูกส่งผ่านไปยัง Centralized Log Server ดังภาพที่ 43



ภาพที่ 43 แสดงการเชื่อมโยง Centralized Log with SSL Tunnel

3. การพัฒนาระบบ

ผู้วิจัยได้มีการพัฒนาระบบ คือ ตามโครงสร้างของโปรแกรมส่วนที่เป็นของผู้ดูแลระบบ จะเป็นการ Download โปรแกรมฟรีจาก http://www.linuxthai.org/forum/index.php?topic=3207.0 นำมาแก้ไข และพัฒนาเพิ่มบางส่วนดังนี้

ตารางที่ 17 การแก้ไขไฟล์

File เดิม	File แก้ไข	รายละเอียดการแก้ไข
1. File : add_user.php วัตถุประสงค์ : เพื่อเก็บรายละเอียดข้อมูลเพิ่มมากขึ้น		
$username = $firstname = $lastname = $password = $password2 = "";	$username5 = $idn = $firstname = $lastname = $mailaddr = $addr = $tel = $password5 = $password2 = "";	เพิ่ม idn ,mailaddr,addr,tel และเปลี่ยนค่าตัวแปรจาก username เป็น username5

# check firstname 	
if(empty($firstname)) {
$error[0] = true;
}
# check lastname 	
if(empty($lastname)) {
$error[1] = true;
}
# check username 	
if(empty($username)) {
$error[2] = true;
}
	# check Group
	if(empty($group)) {
	$error[100] = true;
	}
	# check ID Number
	if(empty($idn)) {
	$error[10] = true;
	}
	# check firstname
	if(empty($firstname)) {
	$error[0] = true;
	}
	# check lastname
	if(empty($lastname)) {
	$error[1] = true;
	}
	# check mailaddr
	if(empty($mailaddr)) {
	$error[2] = true;
	}
		ตรวจสอบค่าว่างของฟิลด์ที่เพิ่มคือ Group,ID Number,Mail Address , Address ,Tel , username ว่าต้องไม่เป็นค่าว่างจึงสามารถเพิ่มข้อมูลได้

ตารางที่ 17 (ต่อ)

File เดิม	File แก้ไข	รายละเอียดการแก้ไข

	# check username
	if(empty($username5)) {
	$error[3] = true;
	}	

$sql = "INSERT INTO account VALUES " ."('$username','".substr(md5($passw ord),0,15)."'," . "'$firstname', '$lastname', '0',". "'0', '0', '0', '--'," . "'".date("Y-m-d H:i:s")."', 'md5','1')";	$sql = "INSERT INTO account VALUES " ."('$username5','".substr(md5($passw ord5),0,15)."'," . "'$firstname', '$lastname', '0'," . "'0', '0', '0', '--'," . "'".date("Y-m-d H:i:s")."', 'md5','1','".*$idn."','"* *.$mailaddr."','".$addr."','".$tel."'*)";	เพิ่มค่าฟิลด์ idn,mailaddr,addr,tel

	<tr>
	<td align="right">เลขบัตรประชาชน
	:</td><td><label>
	<input name="idn" type="text"
	class="inputbox-normal" id="idn"
	style="width:110px;background: <?
	if($error[10]) echo "#FFF0F0"; ?>"
	value="<?= $idn ?>" size="13"
	maxlength="13" />
	<? if($error[1]) {
	echo "« กรุณากรอกเลข
	ประชาชนด้วยครับ"; }
	?></label></td>
	</tr>** ช่องรับค่าเลขที่บัตรประชาชน
	---------- 	
	--
	<tr>
	<td align="right">ที่อยู่ :</td>
	<td><textarea name="addr"
		เพิ่มช่องสำหรับรับค่าใหม่
		คือ idn, addr,tel ,mailaddr

ตารางที่ 17 (ต่อ)

File เดิม	File แก้ไข	รายละเอียดการแก้ไข

	class="inputbox-normal" id="addr"
	style="width:250px;background:<?
	if($error[11]) echo "#FFF0F0";
	?>"><?= $addr ?>
	</textarea>
	<? if($error[1]) {
	echo "« กรุณากรอกที่อยู
	ผู้ใช้งานด้วยครับ"; }
	?></label></td>
	</tr>** ช่องรับค่าที่อยู่
	---------- 	
	--
	<tr>
	<td align="right">เบอร์ติดต่อ :</td>
	<td><input name="tel" type="text"
	class="inputbox-normal" id="tel"
	style="width:90px;background:<?
	if($error[12]) echo "#FFF0F0"; ?>"
	value="<?= $tel ?>" size="10"
	maxlength="10" />
	<? if($error[1]) {
	echo "« กรุณากรอกเบอร์ติดต่อ
	ด้วยครับ"; } ?></label></td>
	</tr> ** ช่องรับค่าเบอร์โทรศัพท์
	---------- 	
	<tr>
	<td align="right">Email :</td>
	<td>
	<input name="mailaddr" type="text"
	class="inputbox-normal"
	id="mailaddr"
	style="width:250px;background:<?	

ตารางที่ 17 (ต่อ)

File เดิม	File แก้ไข	รายละเอียดการแก้ไข

	if($error[2]) echo "#FFF0F0"; ?>
	<td align="right">Email :</td>
	<td>
	<input name="mailaddr" type="text"
	class="inputbox-normal"
	id="mailaddr"
	style="width:250px;background:<?
	if($error[2]) echo "#FFF0F0"; ?>
	value="<?= $mailaddr ?>">
	<? if($error[1]) {
	echo "« กรุณากรอกอีเมล์
	ผู้ใช้งานด้วยครับ"; }
	?></label></td>
	</tr> ** เพิ่มช่องรับค่า e-Mail	

<input name="password2" type="password" class="inputbox- normal" id="password2" style="background: <? if($error[6] ‖ $error[7] ‖ $error[8]) echo "#FFF0F0"; ?>" value="<?= $password2 ?>">	<input name="password2" type="password" class="inputbox- normal" id="password2" style="background: <? if($error[7] ‖ $error[8] ‖ $error[9]) echo "#FFF0F0"; ?>" value="12345678">	การกำหนดค่า default รหัสผ่านของเดิมระบบ กำหนดให้ มีการ ปรับเปลี่ยนใหม่โดย กำหนดค่า default เป็น 12345678 และผู้ใช้ สามารถแก้ไขได้
2. File : add_multi_user.php เป็นไฟล์ที่จัดทำเพิ่มเติมประกอบด้วยไฟล์ PHPExcel และ folder upload เพื่อเก็บค่าข้อมูล มีวัตถุประสงค์เพื่อนำเข้าข้อมูลที่เป็นไฟล์ Excel		
3. File : manage_user.php วัตถุประสงค์เพื่อให้ผู้ดูแลระบบสามารถตรวจสอบรหัสผ่านของผู้ใช้ได้		
<td align="center" valign="top" bgcolor="<?= $bgcolor ?>"><?= substr($users->dateregis,0,10) ?>	<td align="center" valign="top" bgcolor="<?= $bgcolor ?>"><?=$users->password ?>	ปรับเปลี่ยนการแสดงค่า จากการแสดงค่าจากวันที่ สมัครปรับเปลี่ยนเป็น แสดงรหัสผ่าน
4. File : manage_interface.php ปรับเปลี่ยนรูปแบบธีมสำหรับหน้า login มีวัตถุประสงค์เพื่อเปลี่ยนรูปแบบธีมได้ตามต้องการ		
5. File : user_online.php มีวัตถุประสงค์เพื่อดูผู้ใช้งานระบบ		

ตารางที่ 17 (ต่อ)

File เดิม	File แก้ไข	รายละเอียดการแก้ไข
$shell_command=' /bin/echo "User-Name='.$_REQUEST['user'].'" | /usr/bin/radclient -x 127.0.0.1:3779 disconnect myradiussecret';	$shell_command=' /bin/echo "User-Name='.$_REQUEST['user'].'" | /usr/bin/radclient -x 127.0.0.1:3779 disconnect testing123';	มีการปรับเปลี่ยนค่า secretkey จากเดิม myradiussecretเป็น testing123
6. File : clearuser.php มีวัตถุประสงค์เพื่อเคลียร์ผู้ใช้งานที่ค้างในระบบ		
shell_exec("sudo /bin/bash /var/www/html/sam/admin/include/clearuser.sh");	shell_exec("sudo /bin/bash /var/www/hotspot/admin/include/clearuser.sh");	ปรับเปลี่ยน path จาก sam เป็น hotspot
shell_exec("sudo /bin/echo 'User-Name = $user' | /usr/local/bin/radclient -x localhost:3799 disconnect myradiussecret");	shell_exec("sudo /bin/echo 'User-Name = $user' | /usr/local/bin/radclient -x localhost:3799 disconnect testing123");	เปลี่ยน secret ket ตามที่ติดตั้งระบบ
7. File : user_history.php มีวัตถุประสงค์เพื่อดูประวัติการใช้งานระบบ		
<? $start = $end = date("Y-m-d"); if(isset($_REQUEST['submit'])) { $start = $_REQUEST['start']; $end = $_REQUEST['end']; } ?>	<? $start = $end = date("Y-m-d"); $user = ""; if(isset($_REQUEST['submit'])) { $start = $_REQUEST['start']; $end = $_REQUEST['end']; $user = $_REQUEST['user']; } ?>	กำหนดค่าตัวแปร $user = ""; เพิ่มเติม
	user id :<input name="user" type="text" class="inputbox" id="user" value="<?= $user ?>" style="width: 100px; text-align:center; padding-left:2px" />	เพิ่มช่องรับค่าจากของเดิม เป็นการแสดงข้อมูลจากวันที่เริ่มต้นและสิ้นสุดเท่านั้น จึงเพิ่มช่องค้นหาจากชื่อผู้ใช้ ด้วย

ตารางที่ 17 (ต่อ)

File เดิม	File แก้ไข	รายละเอียดการแก้ไข
	if($_REQUEST['user']==""){ $sql = "select * from radacct,account where radacct.acctstarttime >= '".$_REQUEST['start']." 00:00:00' and radacct.acctstarttime <= '".$_REQUEST['end']." 23:59:59' and radacct.username = account.username order by radacct.acctstarttime ";	เพิ่มการดึงข้อมูลจากชื่อผู้ใช้
<tr> <td width="69" height="30" align="center" class="key">ลำดับ </td> <td width="196" height="30" align="center" class="key">ชื่อ - นามสกุล</td> <td width="156" height="30" align="center" class="key">เริ่มต้น ใช้งาน</td> <td width="116" align="center" class="key">หมายเลข IP</td> <td width="92" height="30" align="center" class="key">เป็นเวลา </td> </tr>	<tr> <td width="52" height="30" align="center" class="key">NO.</td> <td width="300" height="30" align="center" class="key">ชื่อ - นามสกุล</td> <td width="120" align="center" class="key">ID</td> <td width="270" align="center" class="key">MAC Address</td> <td width="302" height="30" align="center" class="key">เริ่มต้นใช้ งาน</td> <td width="107" height="30" align="center" class="key">เป็นเวลา </td> </tr>	เพิ่มช่องแสดงค่า MAC Address , ID
	<td width="120" align="center" valign="top" bgcolor="<?= $bgcolor ?>"><?= $data->username ?></td> <td width="270" align="center" valign="top" bgcolor="<?= $bgcolor ?>"><?= $data->callingstationid ?> </td>	เพิ่มคำสั่งแสดงค่าข้อมูล username และ mac address

ตารางที่ 17 (ต่อ)

File เดิม	File แก้ไข	รายละเอียดการแก้ไข
8. File : manage_service.php มีวัตถุประสงค์เพื่อการดู status การทำงานของ Service ต่าง		
$radiusdstring = trim(shell_exec("sudo -u root ps -A | grep radiusd | awk {'print \$4'}"));	$radiusdstring = trim(shell_exec("sudo -u root ps -A | grep radius | awk {'print \$4'}"));	เปลี่ยนค่าจาก radiusd เป็น radius เพื่อดู status service
case 'firewallrestart' : shell_exec("sudo /sbin/service firewall restart"); break; case 'httpstart' :shell_exec("sudo /sbin/service httpd start"); echo "<meta http-equiv=refresh content='1;url=index3.php?option=manage_service'>"; break; case 'httpstop' : shell_exec("sudo /sbin/service httpd stop"); echo "<meta http-equiv=refresh content='1;url=index3.php?option=manage_service'>"; break; case 'httprestart' :shell_exec("sudo /sbin/service httpd restart"); echo "<meta http-equiv=refresh content='1;url=index3.php?option=manage_service'>"; break; case 'radiusstart' : shell_exec("sudo /sbin/service radiusd start"); echo "<meta http-equiv=refresh content='1;url=index3.php?option=manage_service'>"; break;	case 'firewallrestart' :shell_exec("sudo /etc/init.d/chilli.iptables"); break; case 'httpstart' : shell_exec("sudo /etc/init.d/apache2 start"); echo "<meta http-equiv=refresh content='1;url=index3.php?option=manage_service'>"; break; case 'httpstop' : shell_exec("sudo /etc/init.d/apache2 stop"); echo "<meta http-equiv=refresh content='1;url=index3.php?option=manage_service'>"; break; case 'httprestart' : shell_exec("sudo /etc/init.d/apache2 restart"); echo "<meta http-equiv=refresh content='1;url=index3.php?option=manage_service'>"; break; case 'radiusstart' : shell_exec("sudo /etc/init.d/ radius start"); echo "<meta http-equiv=refresh content='1;url=index3.php?option=manage_service'>"; break;	เปลี่ยนค่า service ของ firewall จาก firewall เป็น chilli.iptables , httpd เป็น apache2 และ radiusd เป็น radius

ตารางที่ 17 (ต่อ)

File เดิม	File แก้ไข	รายละเอียดการแก้ไข

case 'radiusstop' : shell_exec("sudo /sbin/service radiusd stop");
echo "<meta http-equiv=refresh content='1;url=index3.php?option=manage_service'>";
break;
case 'radiusrestart' :shell_exec("sudo /sbin/service radiusd restart");
echo "<meta http-equiv=refresh content='1;url=index3.php?option=manage_service'>"; break;
	case 'radiusstop' :shell_exec("sudo /etc/init.d/ radius stop");
	echo "<meta http-equiv=refresh content='1;url=index3.php?option=manage_service'>";
	break;
	case 'radiusrestart' :shell_exec("sudo /etc/init.d/radius restart");
	echo "<meta http-equiv=refresh content='1;url=index3.php?option=manage_service'>";
	break;	

$pos = strpos($httpdstring, "httpd");
if($task == "service httpd stop")
{
$httpdstart = false;
}
else if ($pos !== false || $task == "service httpd start")
{
$httpdstart = true;
}
	$pos = strpos($httpdstring, "apache2");
	if($task == "service httpd stop")
	{
	$httpdstart = false;
	}
	else if ($pos !== false || $task == "service apache2 start")
	{
	$httpdstart = true;
	}
		เปลี่ยนค่าจาก httpd เป็น apache2

$pos = strpos($httpdstring, "httpd");
if($task == "service httpd stop")
{
$httpdstart = false;
}
else if ($pos !== false || $task == "service httpd start")
	$pos = strpos($httpdstring, "apache2");
	if($task == "service httpd stop")
	{
	$httpdstart = false;
	}
		เปลี่ยนค่าจาก httpd เป็น apache2

ตารางที่ 17 (ต่อ)

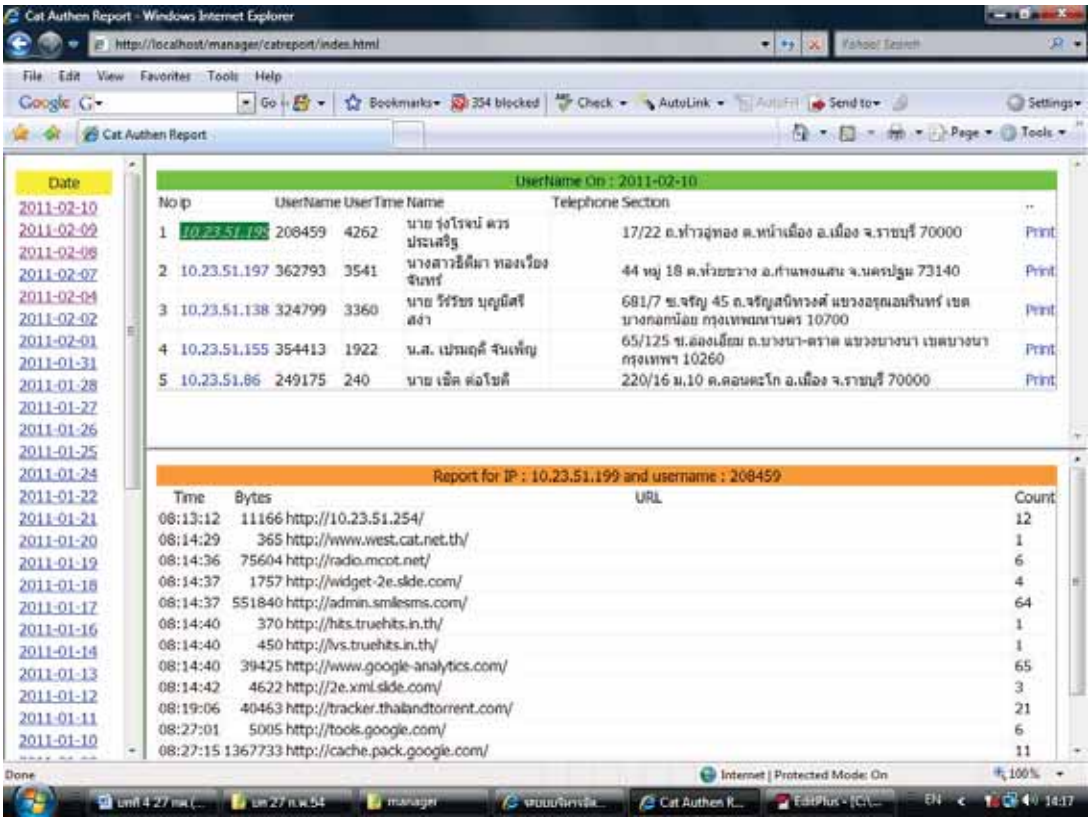
File เดิม	File แก้ไข	รายละเอียดการแก้ไข

{
$httpdstart = true;
}
	else if ($pos !== false || $task == "service apache2 start")
	{
	$httpdstart = true;
	}	

$pos = strpos($radiusdstring, "radiusd");
if($task == "service radiusd stop")
{
$radiusdstart = false;
}
else if ($pos !== false || $task == "service radiusd start")
{
$radiusdstart = true;
}
	$pos = strpos($radiusdstring, "radius");
	
	if($task == "service radius stop")
	{
	$radiusdstart = false;
	}
	else if ($pos !== false || $task == "service radius start")
	{
	$radiusdstart = true;
	}
		เปลี่ยนค่าจาก radiusd เป็น radius

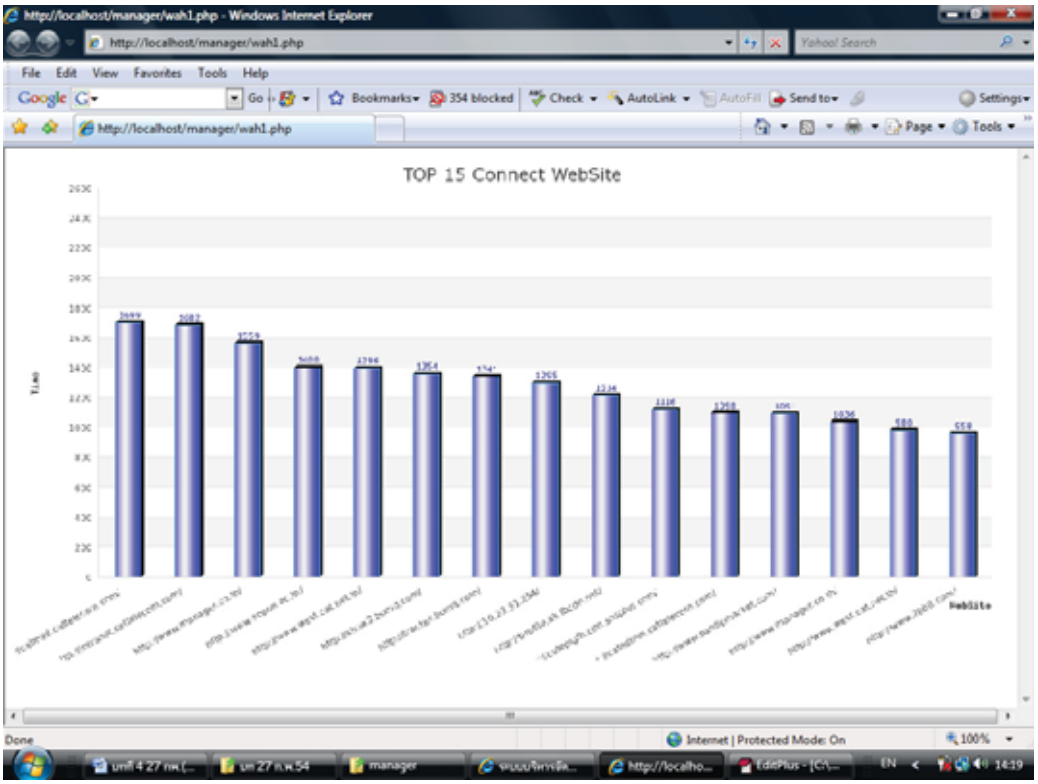
$result .= shell_exec("sudo -u root /var/www/html/authen/admin/include/checkwan.pl $checkporttext");	$result .= shell_exec("sudo -u root ping –c5 $checkporttext");	กำหนดรูปแบบการ check status wan ด้วยคำสั่ง ping
9. File : access_log.php เขียนไฟล์ขึ้นใหม่ มีวัตถุประสงค์เพื่อดู status การใช้งานอินเทอร์เน็ต		

ส่วนที่เป็นของผู้บริหารในการดูรายงาน ได้พัฒนาขึ้นเอง เพื่อให้ผู้บริหารสามารถดูรายงานการใช้งานผ่านอินเทอร์เน็ตได้ ดังภาพที่ 44



ภาพที่ 44 แสดงรายงานการใช้งานของผู้ใช้แต่ละคน

นอกจากนี้ผู้บริหารยังสามารถดูรายงานเว็บไซต์ ที่พนักงานส่วนใหญ่เข้าใช้งาน ดังภาพที่ 45



ภาพที่ 45 แสดงจำนวนเว็บไซต์ที่พนักงาน/ลูกจ้างเข้าใช้งาน เรียงลำดับจากมากมาน้อย 15 อันดับ

4. การประเมินผลจากการทดสอบ

ผู้พัฒนาระบบได้ทำแบบประเมินผลการทดสอบระบบ โดยให้พนักงาน ลูกจ้าง ผู้บริหารของสำนักงานบริการลูกค้า กสท เขตตะวันตก จำนวน 15 ท่าน ได้ประเมินผลการทำงานของระบบ ซึ่งมีหัวข้อที่ต้องประเมินดังนี้

1. การ Login เข้าสู่ระบบ
    1.1 ความง่ายและสะดวกในการใช้งาน
    1.2 ความถูกต้อง
2. การใช้งานระบบ
    2.1 ความเร็วของอินเทอร์เน็ตที่ใช้งาน
    2.2 ระยะเวลาของการใช้งานอินเทอร์เน็ตถูกต้องตามจริง
3. ส่วนการจัดการระบบ (สำหรับผู้ดูแลระบบเท่านั้น)
    3.1 การเรียกดูข้อมูลผู้ใช้งานระบบ
    3.2 การเพิ่มข้อมูลผู้ใช้
    3.3 การจัดการกลุ่มผู้ใช้
    3.4 การสร้างบัตรผู้ใช้
    3.5 การปรับแต่งหน้าล็อกอิน
    3.6 การแสดงสถานะผู้ใช้งานในระบบ
    3.7 การตรวจสอบข้อมูลการใช้งานระบบ
    3.8 การเคลียร์ User ค้างในระบบ
    3.9 การจัดการ Service
    3.10 การ Block Website
    3.11 การตรวจสอบ IP
    3.12 การดูข้อมล Log
4. ส่วนการดูรายงาน (สำหรับผู้บริหารเท่านั้น)
5. ความสมบูรณ์ของระบบ
6. มีประโยชน์ต่อหน่วยงาน

ตารางที่ 18 ข้อมูลผู้ประเมินตามหน้าที่รับผิดชอบ

ลำดับที่	หน้าที่รับผิดชอบ	จำนวน/คน	ร้อยละ
1	ผู้บริหาร	2	13
2	ช่างเทคนิค	7	47
3	เจ้าหน้าที่การตลาด	4	27
4	ผู้ดูแลระบบ	2	13

ตารางที่ 19 ข้อมูลผู้ประเมินตามตำแหน่ง / ระดับ

ลำดับที่	หน้าที่รับผิดชอบ	จำนวน/คน	ร้อยละ
1	ผู้จัดการส่วน	2	13
2	วิศวกร ระดับ 8	1	7
3	นายช่างโทรคมนาคม ระดับ 7	2	13
4	นายช่างโทรคมนาคม ระดับ 6	4	27
5	พนักงานปฏิบัติการโทรคมนาคม ระดับ 6	4	27
6	พนักงานโปรแกรมคอมพิวเตอร์ ระดับ 4	1	7
7	ลูกจ้างปฏิบัติการด้านโทรคมนาคม	1	7

ตารางที่ 20 แสดงระดับความพึงพอใจ ด้านความถูกต้องและสมบูรณ์

การใช้งานส่วนต่างๆ	ค่าเฉลี่ย (X)	ดีมาก	ดี	ปานกลาง	พอใช้	ปรับปรุง	ความพึงพอใจ
1 .การ Login เข้าสู่ระบบ							
1.1 ความง่าย	4.13	3	11	1	0	0	ดีมาก
1.2 ความถูกต้อง	4.20	4	10	1	0	0	ดีมาก
2. การใช้งานระบบ							
2.1 ความเร็ว	4.40	8	5	2	0	0	ดีมาก
2.2 ระยะเวลา	4.13	5	7	3	0	0	ดีมาก
3. ส่วนการจัดการระบบ							
3.1 การเรียกดู	4.00	0	2	0	0	0	ดี
3.2 การเพิ่มข้อมูล	4.00	0	2	0	0	0	ดี
3.3 การจัดการกลุ่ม	4.00	0	2	0	0	0	ดี
3.4 การสร้างบัตรผู้ใช้	4.50	1	1	0	0	0	ดีมาก
3.5 การปรับแต่งหน้า	4.50	1	1	0	0	0	ดีมาก
3.6 การแสดงสถานะผู้ใช้	4.50	1	1	0	0	0	ดีมาก
3.7 การตรวจสอบข้อมูล	3.50	0	1	1	0	0	ดี
3.8 การเคลียร์ User	3.50	0	1	1	0	0	ดี
3.9 การจัดการ Service	4.50	1	1	0	0	0	ดีมาก
3.10 การตรวจสอบ IP	4.50	1	1	0	0	0	ดีมาก
3.11 การ Block website	4.00	0	2	0	0	0	ดี
3.12 การดูข้อมูล Log	3.50	0	1	1	0	0	ดี

ตารางที่ 21 ความพึงพอใจส่วนการดูรายงาน(สำหรับผู้บริหารเท่านั้น)

การใช้งานส่วนต่างๆ	ค่าเฉลี่ย (X)	ดีมาก	ดี	ปานกลาง	พอใช้	ปรับปรุง	ความพึงพอใจ
1 .ความครบถ้วนสมบูรณ์รายงาน	4.50	1	1	0	0	0	ดีมาก

ตารางที่ 22 ความพึงพอใจความสมบูรณ์และประโยชน์ของระบบ

การใช้งานส่วนต่างๆ	ค่าเฉลี่ย (X)	ดีมาก	ดี	ปานกลาง	พอใช้	ปรับปรุง	ความพึงพอใจ
1 .ความสมบูรณ์ของระบบ	4.40	6	9	0	0	0	ดีมาก
2. ความมีประโยชน์ของหน่วยงาน	4.47	7	8	0	0	0	ดีมาก

คะแนนเฉลี่ย 4.01 – 5.00 หมายความว่าระดับความพึงพอใจในระบบมีคุณภาพดีมาก

คะแนนเฉลี่ย 3.01 – 4.00 หมายความว่าระดับความพึงพอใจในระบบมีคุณภาพดี

คะแนนเฉลี่ย 2.01 – 3.00 หมายความว่าระดับความพึงพอใจในระบบมีคุณภาพปานกลาง

คะแนนเฉลี่ย 1.01 – 2.00 หมายความว่าระดับความพึงพอใจในระบบมีคุณภาพพอใช้

คะแนนเฉลี่ย 0 – 1.00 หมายความว่าระดับความพึงพอใจในระบบมีคุณภาพควรปรับปรุง

บทที่ 5
สรุปผลการศึกษา และข้อเสนอแนะ

การค้นคว้าอิสระเรื่องระบบบริหารจัดการเก็บและรักษาข้อมูลจราจรทางคอมพิวเตอร์ กรณีศึกษาสำนักงานบริการลูกค้า กสท เขตตะวันตก ผู้วิจัยได้ทำการพัฒนาระบบเพื่อให้การใช้งานอินเทอร์เน็ตของพนักงานและลูกจ้างในสำนักงาน เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร สิ่งที่พัฒนาขึ้นคือการให้ผู้ดูแลระบบสามารถตรวจสอบการใช้งาน จัดการการใช้งานของผู้ใช้แต่ละคน เพิ่มผู้ใช้งาน ผู้บริหารสามารถดูรายงานการใช้งานอินเทอร์เน็ต

1. สรุปผลการศึกษา

หลังจากได้พัฒนาระบบบริหารจัดการเก็บและรักษาข้อมูลจราจรทางคอมพิวเตอร์ กรณีศึกษา สำนักงานบริการลูกค้า กสท เขตตะวันตก และได้ทดสอบการใช้งานเป็นระยะเวลา 3 เดือน สามารถสรุปผลการศึกษาวิจัย ดังนี้

1.1 ได้ระบบบริหารจัดการเก็บและรักษาข้อมูลจราจรทางคอมพิวเตอร์ เพื่อรองรับตามพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

1.2 สามารถให้ผู้บริหาร ดูข้อมูลการใช้งานอินเทอร์เน็ตของพนักงานและลูกจ้าง ว่าใช้งานในทางที่เป็นประโยชน์มากน้อยเพียงใด

1.3 ผู้บริหารต้องการให้พัฒนาต่อ และใช้เป็นต้นแบบ เพื่อจัดทำระบบให้แก่ลูกค้าของสำนักงานบริการลูกค้า กสท เขตตะวันตก เช่น โรงเรียนระดับมัธยม ประถม องค์กรปกครองส่วนท้องถิ่น หอพัก เป็นต้น ที่มีงบประมาณจำกัด และไม่มีบุคลากรที่จะจัดทำระบบได้ โดยนำเสนอเป็นบริการร่วมกับการให้บริการอินเทอร์เน็ต เพื่อสร้างความแตกต่างจากคู่แข่ง จึงได้พัฒนาระบบให้สามารถสร้าง user และ password และสร้างจำนวนชั่วโมงในการใช้งาน อีกทั้งสามารถสร้างบัตรรายชั่วโมง รายวัน รายเดือน ต่าง ๆ เพื่อให้บุคคลภายนอกใช้งานได้

1.4 ประหยัดทรัพยากรของหน่วยงาน ทำให้สำนักงานบริการลูกค้า กสท เขตตะวันตก ไม่ต้องจัดซื้อฮาร์ดแวร์ ที่จะรองรับการให้บริการอินเทอร์เน็ต ให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งบริษัทเอกชนนำเสนอในราคาประมาณ 300,000.- บาท

2. ปัญหาและแนวทางแก้ไข

ปัญหาในการทำความเข้าใจกับพนักงาน ลูกจ้าง ที่ต้องมีการจัดเก็บและรักษาข้อมูลจราจรทางคอมพิวเตอร์ และขอความร่วมมือในการใช้งานผ่านระบบ เมื่อติดตั้งระบบระยะแรก พนักงานและลูกจ้างจะกังวลว่าผู้บริหารและผู้ดูแลระบบ จะรู้รายละเอียดต่างๆ ตลอดจนข้อความ คำพูด รูปภาพ ที่ส่งผ่านอินเทอร์เน็ต ซึ่งต้องสร้างความเข้าใจแก่พนักงานและลูกจ้าง แสดงให้เห็นว่าผู้ดูแลระบบหรือผู้บริหารไม่สามารถดูข้อมูลต่าง ๆ ที่เป็นส่วนตัวได้ ยกเว้นข้อมูลที่ต้องเก็บตามพระราชบัญญัติฯ และประกาศกระทรวงฯ

3. ข้อเสนอแนะ

3.1 จากการศึกษาระบบบริหารจัดการ เก็บ และ รักษาข้อมูลจราจร ทางคอมพิวเตอร์ กรณีศึกษา สำนักงานบริการลูกค้า กสท เขตตะวันตก พบว่าการจัดเก็บและรักษาข้อมูลจราจรทางคอมพิวเตอร์สามารถดำเนินการได้ โดยไม่ต้องจัดซื้ออุปกรณ์ ฮาร์ดแวร์ ราคาแพง เพียงแต่บุคลากรของหน่วยงานจะต้องมีการเรียนรู้และพัฒนา ทั้งนี้ในส่วนของสำนักงานบริการลูกค้า กสท เขตตะวันตก ผู้วิจัยได้นำเสนอให้ผู้บริหารจัดตั้งทีมงานเพื่อเรียนรู้และศึกษา พัฒนาต่อยอด เพื่อใช้เป็นโอกาสในการสร้างความแตกต่างจากคู่แข่ง ในการนำเสนอบริการอินเทอร์เน็ต แก่กลุ่มลูกค้าที่มีงบประมาณจำกัด อีกทั้งจะได้มีทีมงานที่จะจัดอบรมให้แก่กลุ่มลูกค้า เพื่อสร้างความสัมพันธ์ที่ดี และเป็นการถ่ายทอดความรู้แก่หน่วยงานราชการ องค์กรปกครองส่วนท้องถิ่นที่มีบุคคลกรด้าน IT จำกัด

3.2 การพัฒนาเพื่อให้เกิดประโยชน์และใช้งานง่าย ควรพัฒนาโปรแกรมให้สามารถติดตั้งและใช้งานได้ทันที โดยไม่ต้องใช้คำสั่งต่าง ๆ ในการแก้ไขเปลี่ยนแปลง

3.3 การพัฒนาระบบ เพื่อให้มีประโยชน์ยิ่งขึ้น หากมีปริมาณการใช้งานอินเตอร์เน็ตมาก ระบบควรจะมีการจำกัด ปริมาณการใช้งานสำหรับโปรแกรมดาวน์โหลดที่ใช้แบนด์วิชสูงได้ทันที

บรรณานุกรม

กฤดากร หิรัญพฤกษ์. ระบบตรวจจับและตรวจตราการส่งผ่านข้อมูลภายในเครือข่ายผ่านเว็บเบราเซอร์ [ออนไลน์]. เข้าถึงเมื่อ กุมภาพันธ์ 2554. เข้าถึงได้จาก http://tdc.thailis.or.th/tdc/basic.php

การติดตั้ง mysar บน ubuntu เพื่อแสดงผล squid [ออนไลน์]. เข้าถึงเมื่อ ตุลาคม 2553. เข้าถึงได้จาก http://www.oknation.net/blog/sniperthai/2009/09/04/entry-2

"คู่มือการปฏิบัติและแนวทางการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550." สำนักกำกับการใช้เทคโนโลยีสารสนเทศ กระทรวงเทคโนโลยีสารสนเทศ, 2551. (อัดสำเนา)

ธวัชชัย เอี่ยมไพโรจน์ , นวลศรี เด่นวัฒนา และ ณัฐวุฒิ จารุมาศ. ระบบพิสูจน์ตัวตนและควบคุมสิทธิการใช้บริการอินเทอร์เน็ต บนวิถีโอเพนซอร์ส [ออนไลน์], เข้าถึงเมื่อ 5 ตุลาคม 2551. เข้าถึงได้จาก http://www.thaicert.nectec.or.th

ณัฐโชติ พรหมฤทธิ์ และอนิราช มิ่งขวัญ, "การสืบสวนผู้ใช้บริการด้วยวิชวลไลเซชันไทม์แมชชีนสำหรับนิติวิทยาศาสตร์สำหรับเครือข่าย," วารสารเทคโนโลยีสารสนเทศ 6, 11 (มกราคม-มิถุนายน 2553) : 31-36.

บุญลือ อยู่คง. ติดตั้ง Log Server ด้วย Linux. กรุงเทพฯ : โฟกัสมาสเตอร์พรินต์ , 2550.

บุญลือ อยู่คง. Internet Server กับ Linux Server 3. กรุงเทพฯ : ทองใบ อยู่คง, 2550.

บรรจง หะรังษี, "ความรู้เบื้องต้นของการเข้ารหัสข้อมูล (Introduction to Cryptography)," วารสารเทคโนโลยีสารสนเทศ ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย , (สิงหาคม 2547)

ภูวดล ด่านระหาญ. Syslog-ng (Syslog new generation) [ออนไลน์], เข้าถึงเมื่อ 5 ตุลาคม 2551. เข้าถึงได้จาก http://www.thaicert.nectec.or.th

มหาวิทยาลัยราชภัฏมหาสารคาม. ipassport [ออนไลน์]. เข้าถึงเมื่อ 5 เมษายน 2551 . เข้าถึงได้จาก http://www.thaibsd.com/ipassport/info/index.html

สิริพร จิตต์เจริญธรรม, เสาวภา ปานจันทร์ และ เลอศักดิ์ ลิ้มวิวัฒน์กุล. ระบบพิสูจน์ตัวตน [ออนไลน์], เข้าถึงเมื่อ 5 ตุลาคม 2551. เข้าถึงได้จาก http://www.thaicert.nectec.or.th

สถาบันมาตรวิทยาแห่งชาติ. NTP (Network Time Protocol) [ออนไลน์]. เข้าถึงเมื่อ 28 กันยายน 2551. เข้าถึงได้จาก http://www.nimt.or.th/

อสมาภรณ์ ฉัตรัตติกรณ์ และชวลิต ทินกรสูติบุตร. การเทียบเวลาด้วย Network Time Protocol ให้สอดคล้องกับ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 [ออนไลน์]. เข้าถึงเมื่อ 27 กุมภาพันธ์ 2551. เข้าถึงได้จาก http://www.thaicert.nectec.or.th

phpsysinfo [ออนไลน์]. เข้าถึงเมื่อ เมษายน 2553. เข้าถึงได้จาก http://phpsysinfo.sourceforge.net/

Prosperous Gateway 1.0 [ออนไลน์]. เข้าถึงเมื่อ 5 ตุลาคม 2551. เข้าถึงได้จาก http:// www.tpit.co.th/public/

Smile Authentication Server [ออนไลน์]. เข้าถึงเมื่อ กรกฎาคม 2553. เข้าถึงได้จาก http://www.linuxthai.org/forum/index.php?topic=3207.0

Ubuntu 9.04 [ออนไลน์]. เข้าถึงเมื่อ เมษายน 2553. เข้าถึงได้จาก http://www.ubuntu.com/desktop/get-ubuntu/download

ภาคผนวก

ภาคผนวก ก

คู่มือการใช้งาน

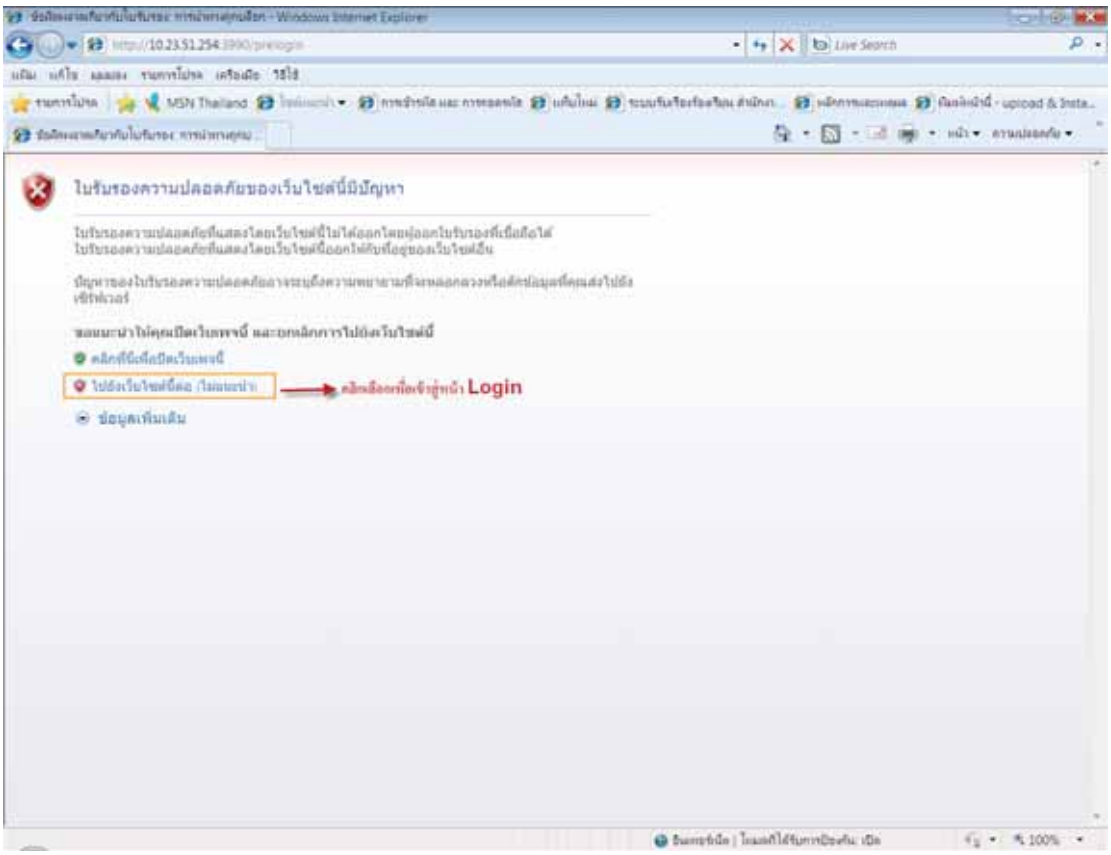
คู่มือการใช้งานโปรแกรม ระบบบริหารจัดการเก็บ และรักษาข้อมูลจราจรทางคอมพิวเตอร์

ส่วนของผู้ใช้งานระบบ

การเข้าสู่ระบบ เมื่อผู้ใช้งานต้องการเข้าใช้งานอินเทอร์เน็ต ดับเบิลคลิกที่ internet explorer จะปรากฏดังภาพที่ 46 ให้คลิกที่ เข้าสู่ระบบ

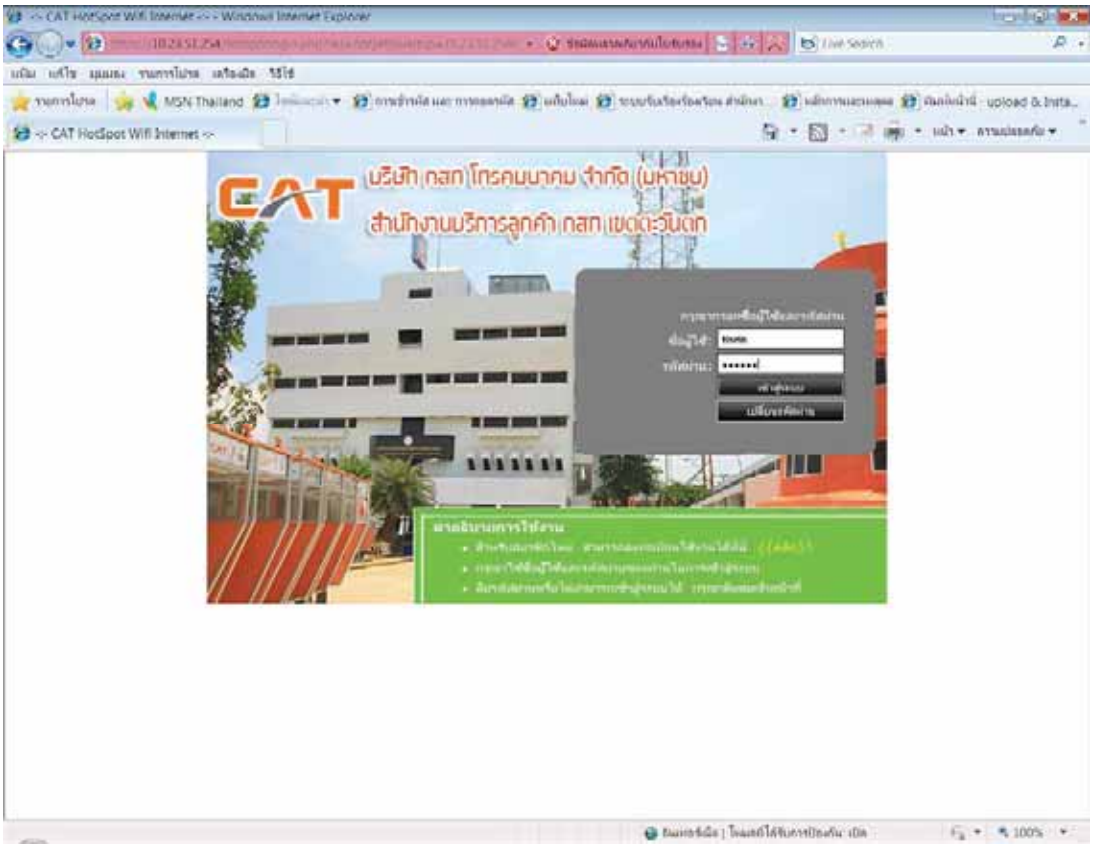
ภาพที่ 46 หน้า เว็บเพจ สำหรับเข้าใช้งานระบบ

เมื่อคลิกเข้าสู่ระบบจะปรากฏดังภาพที่ 47 ให้คลิกที่ ไปยังเว็บนี้ต่อ (ไม่แนะนำ) การปรากฏหน้าดังกล่าว เป็นการแสดงความปลอดภัยของระบบ



ภาพที่ 47 แสดงความปลอดภัยของระบบ

เมื่อขึ้นหน้าเว็บดังภาพที่ 48 ให้ผู้ใช้งานใส่ชื่อผู้ใช้งาน ที่กำหนดให้ คือรหัสพนักงาน 6 หลัก และรหัสผ่าน เป็นหมายเลขประจำตัวประชาชน 13 หลัก จากนั้นคลิกเข้าสู่ระบบ เพื่อเข้าสู่ระบบ หรือคลิกที่เปลี่ยนรหัสผ่าน เพื่อเปลี่ยนรหัสผ่าน



ภาพที่ 48 แสดงหน้าเว็บสำหรับใส่ชื่อผู้ใช้งานและรหัสผ่านเพื่อเข้าสู่ระบบ

เมื่อผู้ใช้งานใส่ชื่อผู้ใช้งานและรหัสผ่านได้ถูกต้อง จะปรากฏ pop up ดังภาพที่ 49 แสดงเวลาที่สามารถใช้งานได้ ซึ่งเวลาจะนับถอยหลัง ผู้ใช้งานไม่ต้องปิดหน้าต่างนี้ เพียงคลิกย่อให้เล็กก็สามารถใช้งานอินเทอร์เน็ตได้ และเมื่อต้องการออกจากอินเทอร์เน็ต ให้คลิกที่ออกจากระบบ

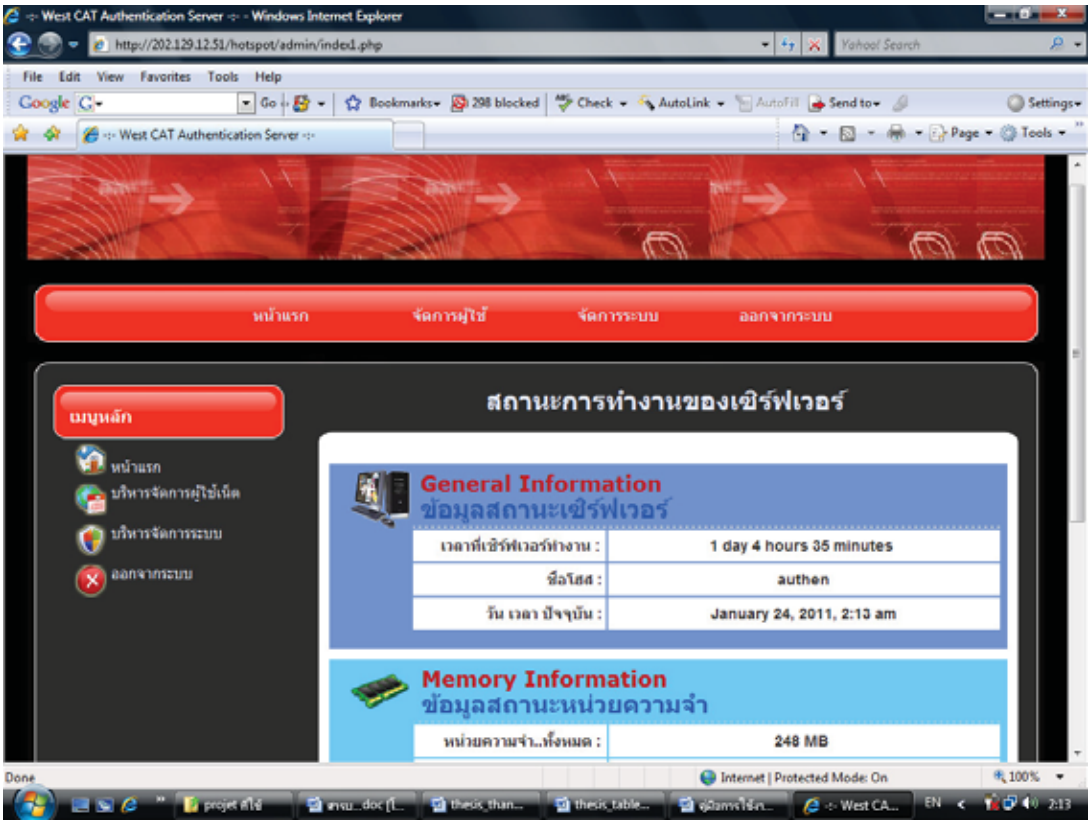
ภาพที่ 49 popup แสดงเวลาที่สามารถอยู่ในระบบ และมีเมนูให้คลิกออกจากระบบ

ส่วนของผู้ดูแลระบบ

โปรแกรมบริหารจัดการผู้ใช้งานอินเทอร์เน็ต สำหรับผู้ดูแลระบบ การเข้าใช้งานของผู้ดูแลระบบ จะต้องเข้าโดย http://202.129.12.51/hotspot/admin จะปรากฏหน้าต่างของผู้ดูแลระบบดังภาพที่ 50 ผู้ดูแลระบบสามารถใส่ชื่อผู้ใช้งาน รหัสผ่าน และคลิกเข้าสู่ระบบ

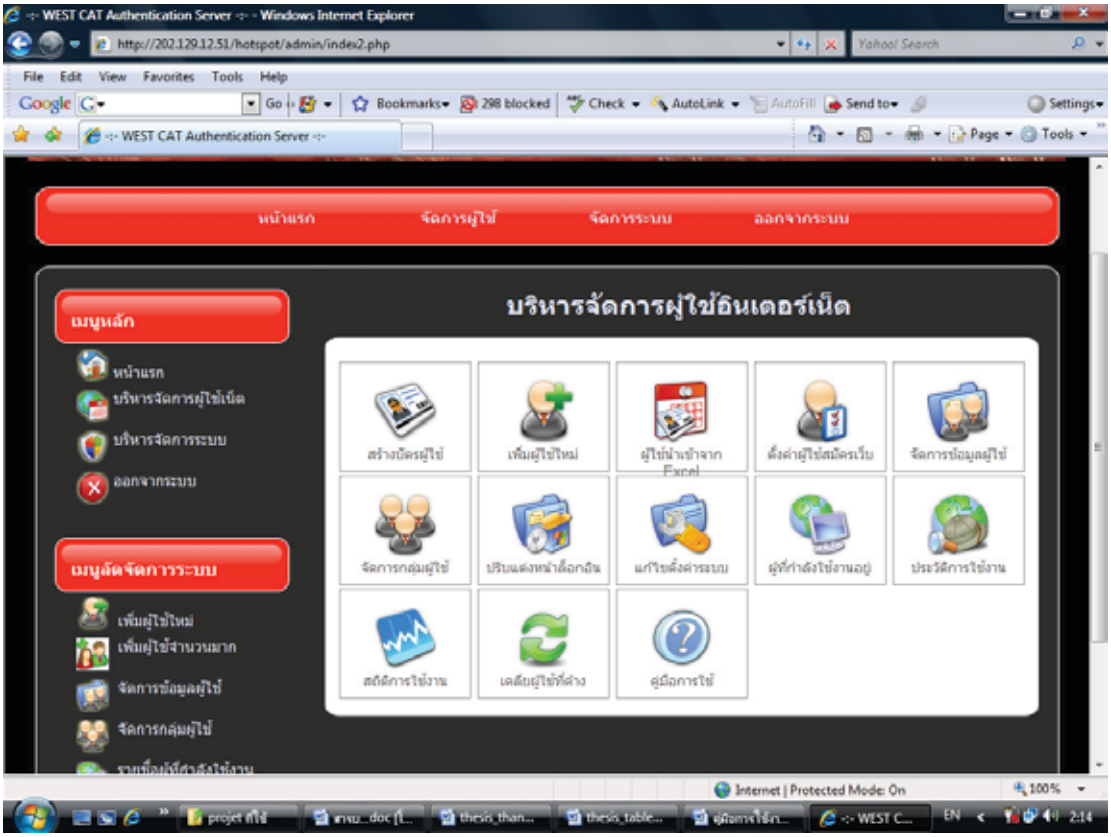
ภาพที่ 50 แสดงหน้าเว็บเพจแรกของผู้ดูแลระบบ

เมื่อผู้ดูแลระบบเข้าสู่ระบบ ระบบจะแสดงสถานะการทำงานของเซิร์ฟเวอร์ และเมนูหลัก ดังภาพที่ 51 ซึ่งประกอบด้วย หน้าแรก เมนูบริหารจัดการผู้ใช้เน็ต เมนูบริหารจัดการระบบ เมนูออกจากระบบ



ภาพที่ 51 แสดงสถานะการทำงานของเซิร์ฟเวอร์ และเมนูต่าง ๆ

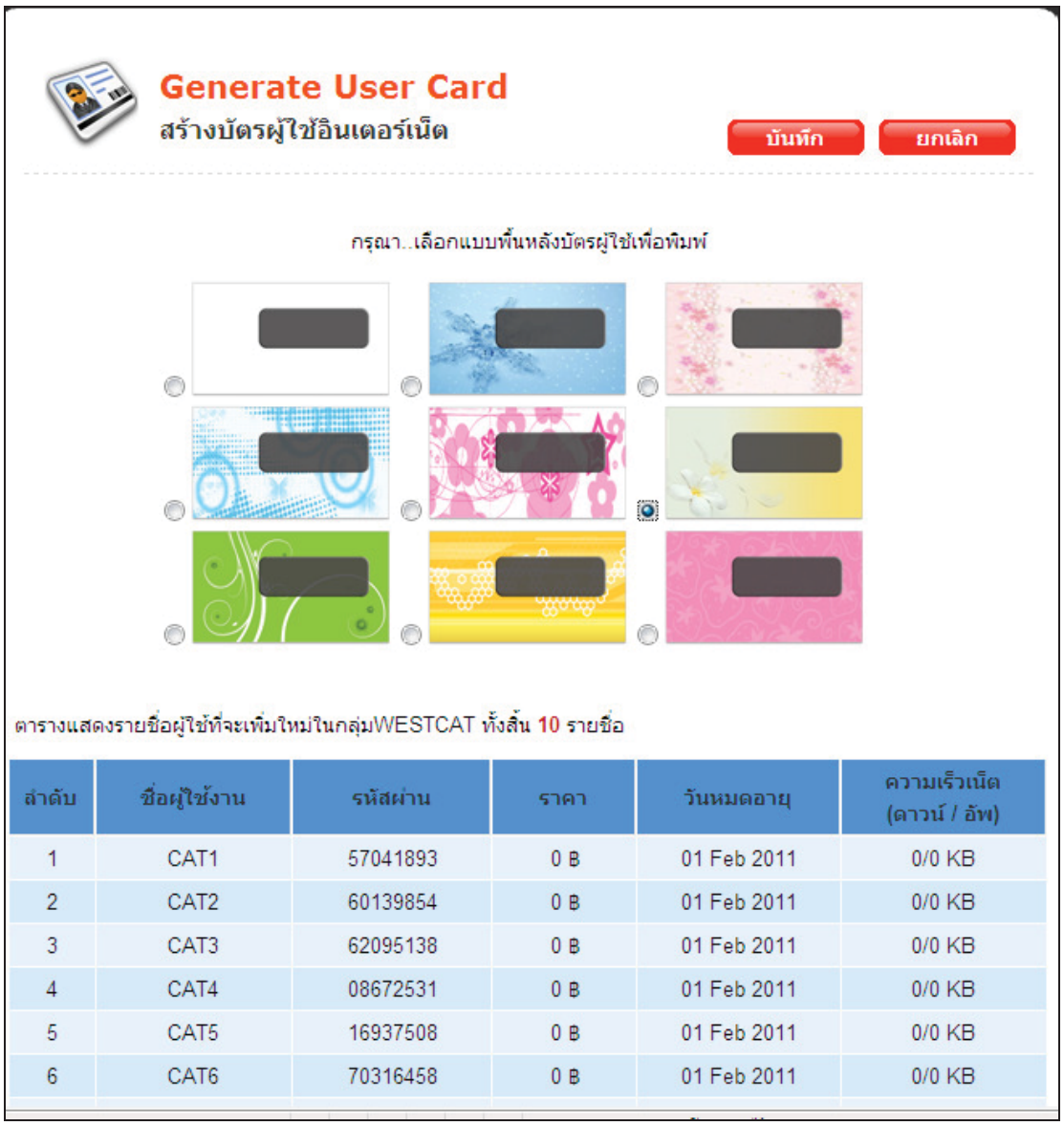
เมื่อคลิกเมนูบริหารจัดการผู้ใช้ จะปรากฏเมนูย่อยต่าง ๆ ที่เกี่ยวข้องกับการบริหารจัดการผู้ใช้ ดังภาพที่ 52 ประกอบด้วย เมนูสร้างบัตรผู้ใช้ เพิ่มผู้ใช้ใหม่ ผู้ใช้นำเข้าจาก Excel ตั้งค่าผู้ใช้ผ่านเว็บ จัดการกลุ่มผู้ใช้ ปรับแต่งหน้าล็อกอิน แก้ไขตั้งค่าระบบ ผู้ที่กำลังใช้งานอยู่ ประวัติการใช้งาน สถิติการใช้งาน เคลียร์ผู้ใช้งาน คู่มือการใช้งาน



ภาพที่ 52 แสดงเมนูบริหารจัดการผู้ใช้อินเทอร์เน็ต

เมนู  สร้างบัตรผู้ใช้งาน เป็นเมนูสำหรับสร้าง ผลิตบัตรให้ผู้ใช้งานที่มาจากที่อื่น และต้องการใช้งานอินเทอร์เน็ต ผู้ดูแลระบบสามารถกำหนดกลุ่มที่จะให้ใช้งาน และจำนวนผู้ที่จะให้ใช้งาน ตลอดจนสามารถกำหนดราคา ดังแสดงในภาพที่ 53 เมื่อกรอกข้อมูลเรียบร้อยแล้ว คลิก ประมวลผล จะปรากฏ ดังภาพที่ 54 แสดงตัวอย่างรูปหน้าบัตร ผู้ดูแลระบบสามารถคลิกเลือกรูปแบบบัตรที่ต้องการ และคลิกบันทึก เมื่อตกลงให้ระบบสั่งพิมพ์บัตร คลิกยกเลิกหากต้องการยกเลิกที่ดำเนินการมา

ภาพที่ 53 แสดงเมนูสร้างบัตรผู้ใช้อินเทอร์เน็ต



ภาพที่ 54 แสดงรูปแบบบัตร และรายละเอียดที่จะสั่งพิมพ์บัตร

เมนู 

เป็นการเพิ่มผู้ใช้งานใหม่ที่ยังไม่มีข้อมูลในระบบใช้สร้างรหัสผู้ใช้อินเทอร์เน็ต ให้กับผู้ใช้ในกลุ่มต่างๆ ที่ผู้ดูแลระบบได้สร้างกลุ่มไว้ใน Group Manager โดยสามารถระบุกลุ่ม ,ระบุชื่อผู้ใช้ ,ระบุรหัสผ่านได้ รายละเอียดการกรอกข้อมูลดังภาพที่ 55

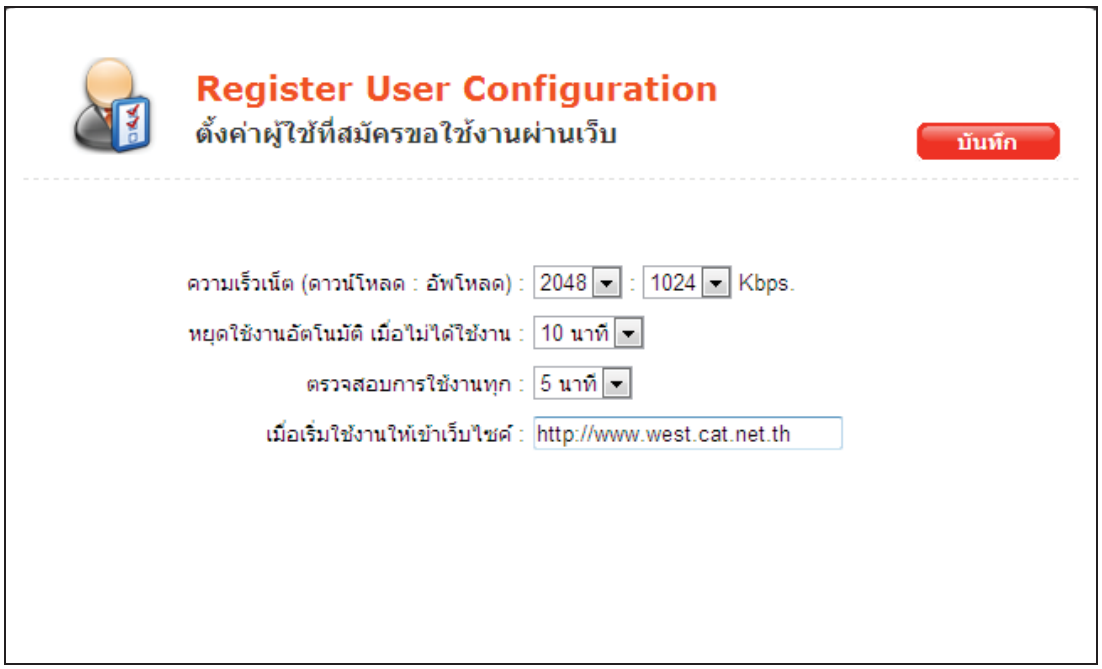
ภาพที่ 55 เมนูเพิ่มผู้ใช้รายบุคคล

เมนู  ผู้ใช้นำเข้าจาก Excel ใช้สำหรับผู้ดูแลระบบที่ต้องการนำข้อมูลรายละเอียดทั้งหมดของผู้ใช้งานเข้าไว้ในระบบ โดยไม่ต้องกรอกข้อมูลที่ละราย เมื่อคลิกเลือกเมนูจะปรากฏดังภาพที่ 56 ให้เลือกไฟล์ที่ต้องการนำเข้าข้อมูล และคลิก บันทึก

ภาพที่ 56 แสดงระบบเพิ่มจำนวนผู้ใช้งานทีละมาก ๆ

เมนู ตั้งค่าผู้ใช้สมัครเว็บ 

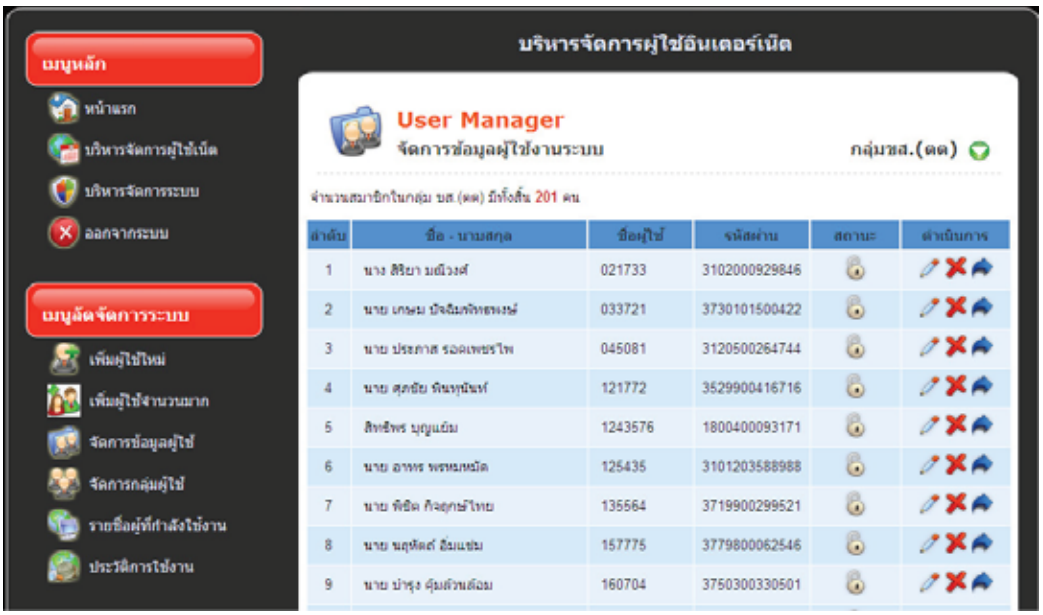
ใช้สำหรับตั้งค่าผู้ใช้ที่สมัครใช้งานผ่านหน้าเว็บไซต์ โดยสามารถกำหนดความเร็วในการใช้งาน กำหนดให้ออกจากระบบอัตโนมัติเมื่อไม่มีการใช้งานในเวลาที่กำหนด กำหนดให้ระบบตรวจสอบการใช้งาน ดังแสดงในภาพที่ 57 เมื่อกรอกข้อมูลเรียบร้อยให้คลิกที่บันทึก



ภาพที่ 57 แสดงการตั้งค่าผู้ใช้ที่สมัครของใช้งานผ่านเว็บ

เมนู 

ใช้บริหารจัดการผู้ใช้อินเทอร์เน็ต โดยสามารถ ลบผู้ใช้ ย้ายกลุ่มผู้ใช้ ระงับการใช้งานอินเทอร์เน็ต และแก้ไขข้อมูลผู้ใช้ได้ ดังภาพที่ 58



ภาพที่ 58 แสดงหน้าเว็บสำหรับการจัดการผู้ใช้อินเทอร์เน็ต

เมนู 

ใช้บริหารจัดการกลุ่มผู้ใช้อินเทอร์เน็ต โดยสามารถ สร้างกลุ่มผู้ใช้ ลบกลุ่มผู้ใช้ กำหนดค่าของกลุ่มผู้ใช้ได้ ดังภาพที่ 59

ภาพที่ 59 แสดงรายละเอียดการจัดการกลุ่มผู้ใช้อินเทอร์เน็ต

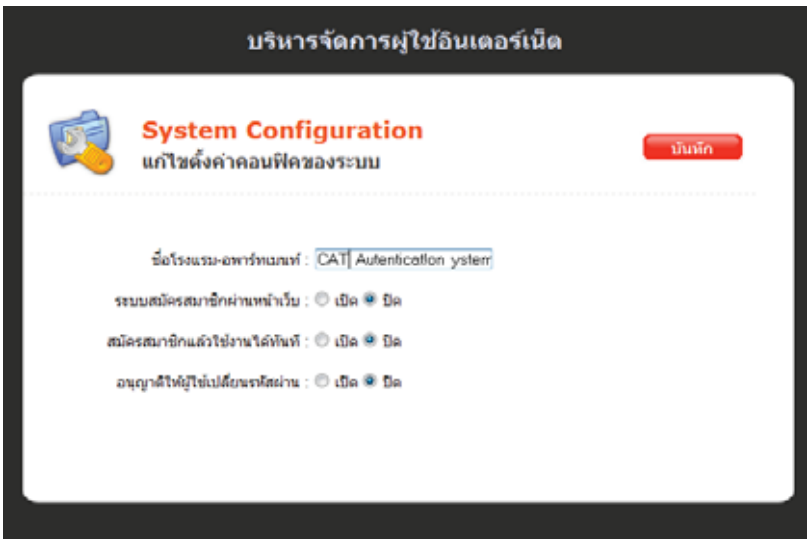
เมนู 

ใช้ปรับแต่งหน้าล็อกอิน สำหรับผู้ใช้อินเทอร์เน็ต โดยสามารถเลือก ชุดรูปแบบของหน้าล็อกอิน และหน้าป๊อปอัพ ได้ถึง 14 แบบ สามารถแก้ไข ข้อความหน้าล็อกอิน และหน้าป๊อปอัพได้ ดังแสดงในภาพที่ 60

ภาพที่ 60 แสดงหน้าปรับแต่งหน้าจอล็อกอิน

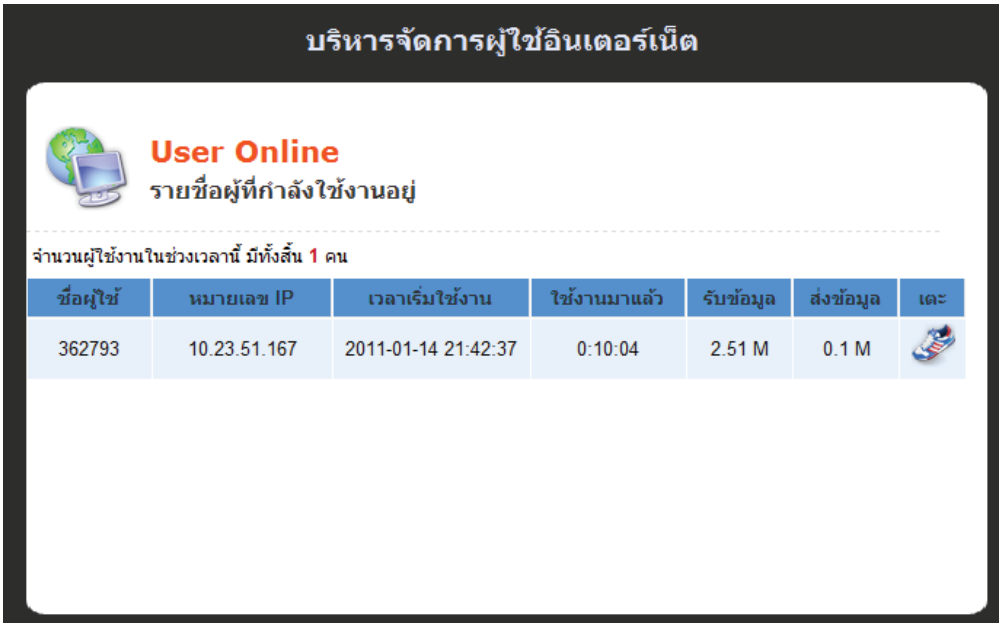
เมนู 

ใช้แก้ไขค่า และตั้งค่าระบบ เช่น ชื่อองค์กร การอนุญาตให้ลงทะเบียนขอใช้ อินเทอร์เน็ต การอนุญาตให้ใช้งานได้ทันทีหลังการลงทะเบียนเสร็จ และ การอนุญาตให้ผู้ใช้เปลี่ยนรหัสผ่านเองได้ ดังแสดงในภาพที่ 61



ภาพที่ 61 แสดงหน้าแก้ไขตั้งค่าคอนฟิตของระบบ

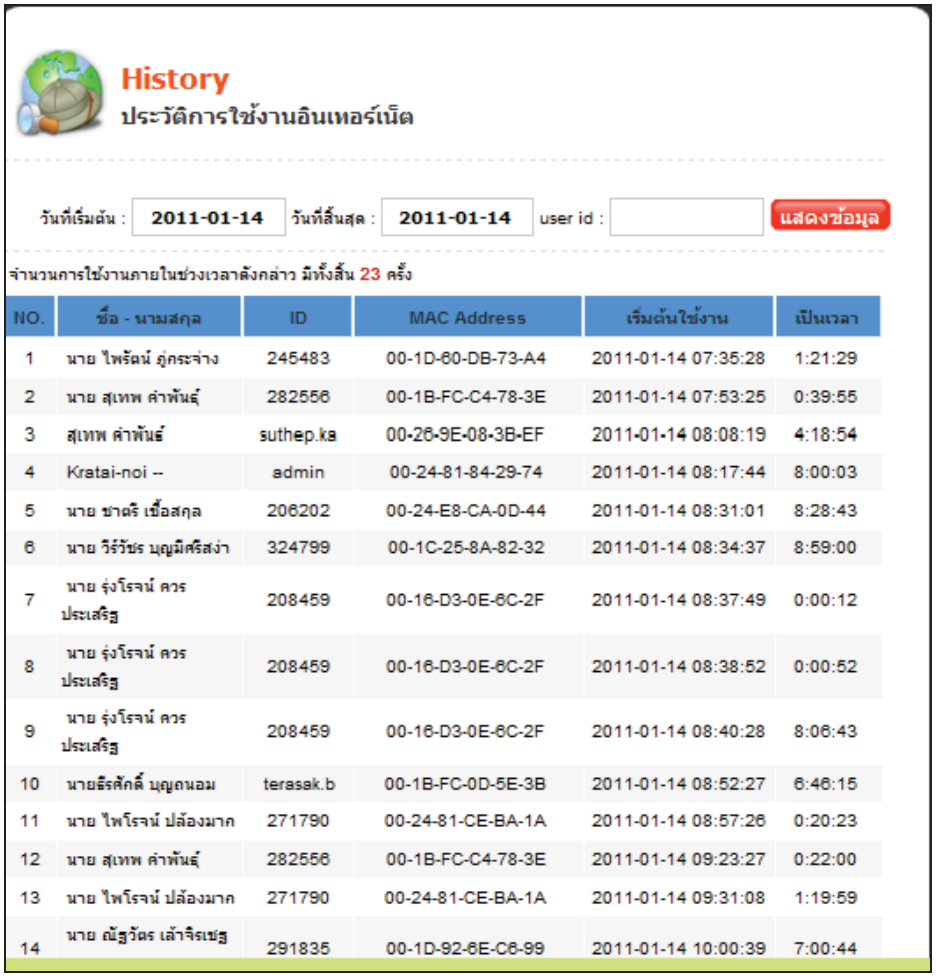
เมนู  แสดงรายชื่อผู้ที่กำลังใช้งานในระบบทั้งหมด ซึ่งจะประกอบด้วยชื่อผู้ใช้ หมายเลข IP เวลาเริ่มใช้งาน ใช้งานมาแล้ว การรับข้อมูล การส่งข้อมูล และสามารถนำผู้ใช้งานที่ค้างออกจากระบบ ดังแสดงในภาพที่ 62



ภาพที่ 62 แสดงรายชื่อผู้ที่กำลังใช้งาน

เมนู 

จะแสดงประวัติการใช้งานอินเทอร์เน็ต สามารถดูกำหนดวันที่เริ่มและวันที่สิ้นสุดการใช้งาน ชื่อผู้ใช้ โดยระบบจะแสดงชื่อ-สกุลผู้ใช้ Username MAC Address วันที่และเวลาเริ่มใช้งาน และรวมเวลาที่ใช้งาน ดังแสดงในภาพที่ 63



History

ประวัติการใช้งานอินเทอร์เน็ต

วันที่เริ่มต้น : 2011-01-14 วันที่สิ้นสุด : 2011-01-14 user id : แสดงข้อมูล

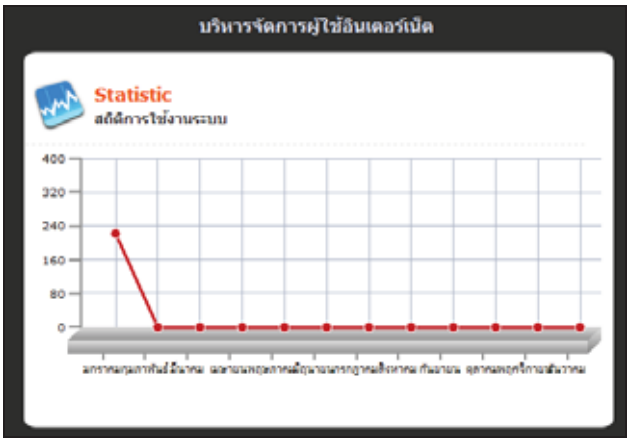
จำนวนการใช้งานภายในช่วงเวลาดังกล่าว มีทั้งสิ้น 23 ครั้ง

NO.	ชื่อ - นามสกุล	ID	MAC Address	เริ่มต้นใช้งาน	เป็นเวลา
1	นาย ไพรัฒน์ ภู่กระจ่าง	245483	00-1D-60-DB-73-A4	2011-01-14 07:35:28	1:21:29
2	นาย สุเทพ ค่าพันธุ์	282556	00-1B-FC-C4-78-3E	2011-01-14 07:53:25	0:39:55
3	สุเทพ ค่าพันธ์	suthep.ka	00-26-9E-08-3B-EF	2011-01-14 08:08:19	4:18:54
4	Kratai-noi --	admin	00-24-81-84-29-74	2011-01-14 08:17:44	8:00:03
5	นาย ชาคริ เชื้อสกุล	206202	00-24-E8-CA-0D-44	2011-01-14 08:31:01	8:28:43
6	นาย วิร์วัชร บุญมีศรีสง่า	324799	00-1C-25-8A-82-32	2011-01-14 08:34:37	8:59:00
7	นาย รุ่งโรจน์ ควรประเสริฐ	208459	00-16-D3-0E-6C-2F	2011-01-14 08:37:49	0:00:12
8	นาย รุ่งโรจน์ ควรประเสริฐ	208459	00-16-D3-0E-6C-2F	2011-01-14 08:38:52	0:00:52
9	นาย รุ่งโรจน์ ควรประเสริฐ	208459	00-16-D3-0E-6C-2F	2011-01-14 08:40:28	8:06:43
10	นายธีรศักดิ์ บุญถนอม	terasak.b	00-1B-FC-0D-5E-3B	2011-01-14 08:52:27	6:46:15
11	นาย ไพโรจน์ ปล้องมาก	271790	00-24-81-CE-BA-1A	2011-01-14 08:57:26	0:20:23
12	นาย สุเทพ ค่าพันธุ์	282556	00-1B-FC-C4-78-3E	2011-01-14 09:23:27	0:22:00
13	นาย ไพโรจน์ ปล้องมาก	271790	00-24-81-CE-BA-1A	2011-01-14 09:31:08	1:19:59
14	นาย ณัฐวัตร เล้าจิรเชฐ	291835	00-1D-92-6E-C6-99	2011-01-14 10:00:39	7:00:44

ภาพที่ 63 แสดงประวัติการใช้งาน

เมนู 

ใช้แสดงกราฟสถิติปริมาณการเข้าใช้งานในแต่ละเดือน ดังภาพที่ 64



ภาพที่ 64 แสดงสถิติการใช้งาน

ส่วนบริหารจัดการระบบ ประกอบด้วย เมนูเปลี่ยนรหัสผู้ดูแล จัดการเซอร์วิส ตรวจสอบ IP/Port ตรวจสอบ Wan บล็อกเว็บ ข้อมูลเซิร์ฟเวอร์ บันทึก พรบ 50 ปิด/รีสตาร์ทระบบ คู่มือการใช้ ดังภาพที่ 65

ภาพที่ 65 แสดงส่วนบริหารจัดการระบบ

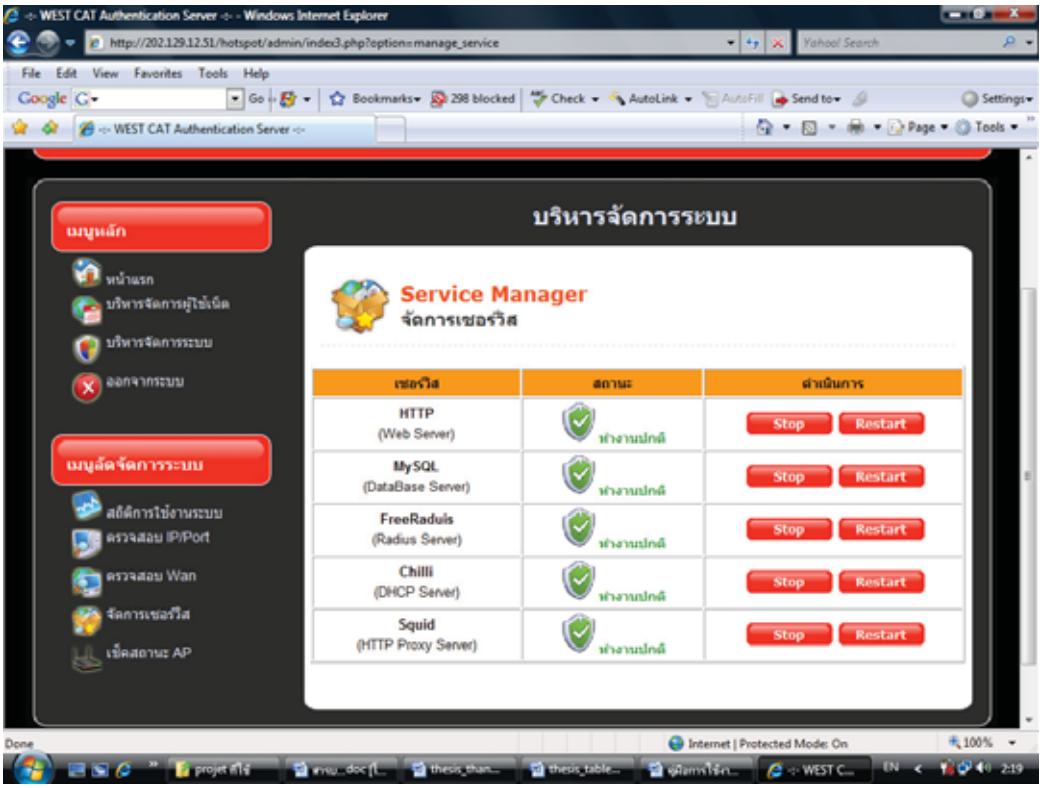
เมนู 

ใช้สำหรับการเปลี่ยนรหัสผ่านของผู้ดูแลระบบ เมื่อคลิกจะปรากฏดังภาพที่ 66 ให้ดำเนินการกรอกข้อมูล และคลิกบันทึก ระบบจะทำการเปลี่ยนรหัสผ่านให้ผู้ดูแลระบบ

ภาพที่ 66 แสดงหน้าสำหรับเปลี่ยนรหัสผ่านของผู้ดูแลระบบ

เมนู 

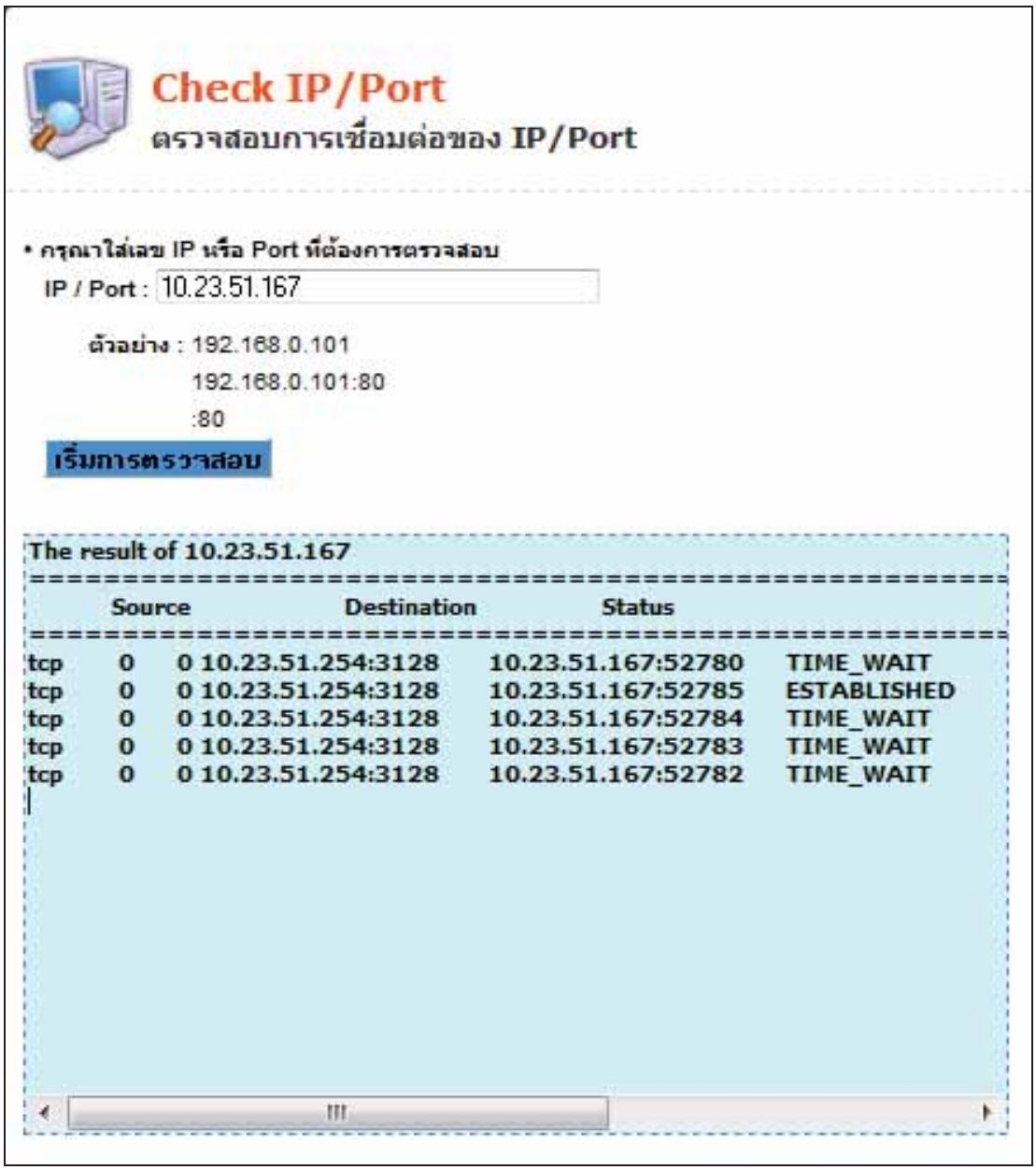
ใช้สำหรับดูสถานะบริการ และใช้สำหรับเปิดปิดระบบบริการต่าง ๆ ดังรายละเอียดตามภาพที่ 67



ภาพที่ 67 แสดงสถานะบริการ

เมนู 

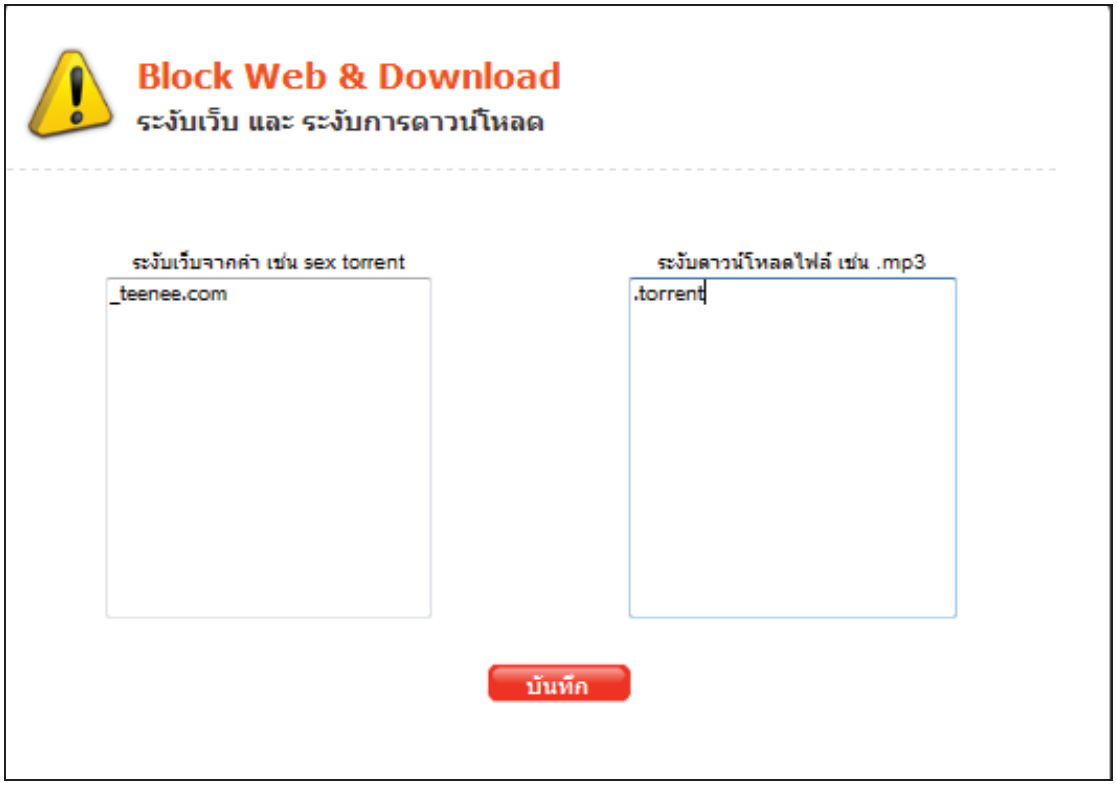
ใช้สำหรับผู้ดูแลระบบตรวจสอบการเชื่อมต่อ IP/Port ในเน็ตเวิร์ค โดยผู้ดูแลระบบจะต้องกรอกหมายเลข IP ที่ต้องการตรวจสอบ และคลิกที่เริ่มการตรวจสอบ ระบบจะแสดงรายละเอียดดังภาพที่ 68



ภาพที่ 68 แสดงสถานะ IP ที่ต้องการตรวจสอบ

เมนู 

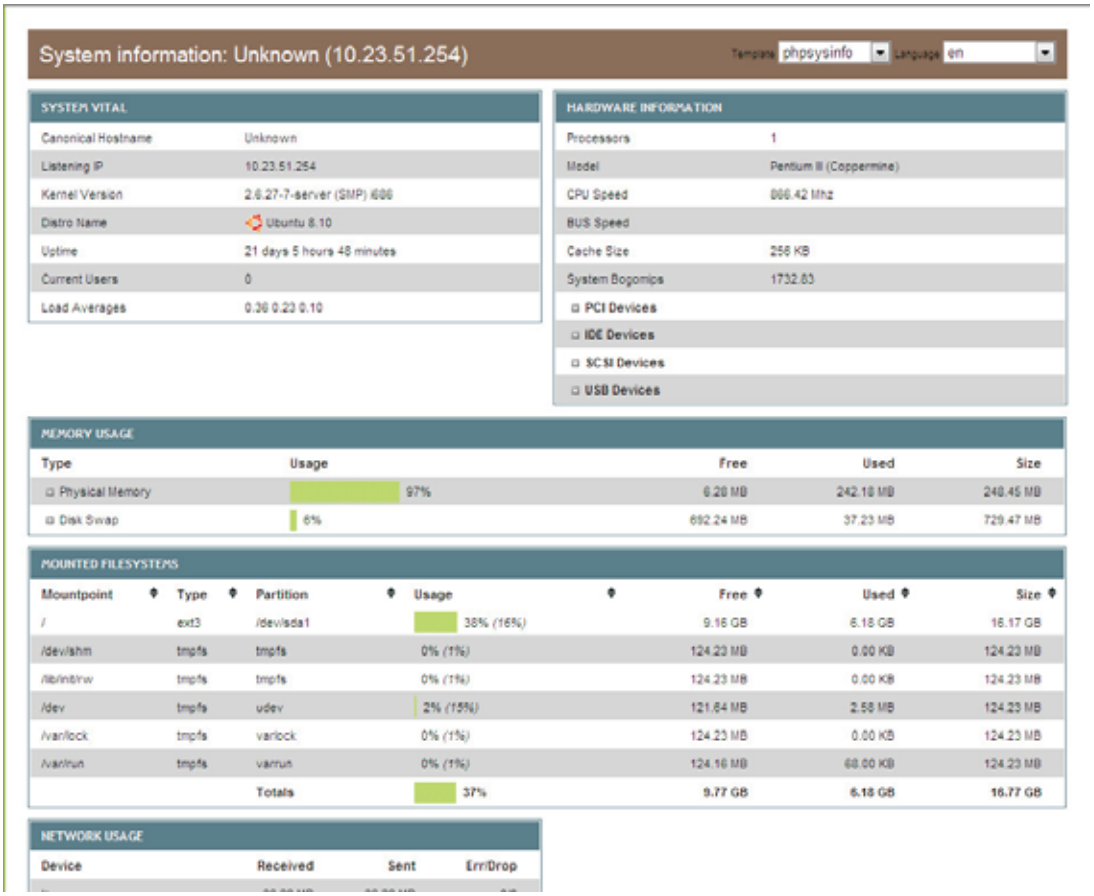
ใช้บล็อกเว็บหรือระงับการดาวน์โหลด ใช้สำหรับกรณีต้องการบล็อคการใช้งานเว็บไซต์ที่ไม่เหมาะสม หรือนโยบายของหน่วยงานไม่ต้องการให้ใช้งานการดาวน์โหลดไฟล์ข้อมูลที่ใช้งานแบนด์วิชสูง ผู้ดูแลระบบสามารถคลิกที่เมนูบล็อกเว็บ จะปรากฏดังภาพที่ 69 และพิมพ์เว็บไซต์ที่ต้องการให้บล็อก จากนั้นคลิกบันทึก ระบบก็จะทำการบล็อคเว็บไซต์ดังกล่าวให้



ภาพที่ 69 แสดงรายชื่อเว็บไซต์ที่บล็อก และไฟล์ที่ไม่ต้องการให้ดาวน์โหลด

เมนู 

ใช้สำหรับตรวจสอบสถานะของ Server เมื่อคลิกจะปรากฏดังภาพที่ 70



ภาพที่ 70 แสดงสถานะของเซิร์ฟเวอร์

เมนู 

ใช้สำหรับตรวจสอบดู Log ของ squid เมื่อคลิกจะปรากฏดังภาพที่ 71 ซึ่งแสดงข้อมูลการใช้งานต่าง ๆ ของผู้ใช้งานอินเทอร์เน็ตในระบบ

ภาพที่ 71 แสดง Log ของ Squid

เมนู 

ใช้สำหรับการปิดหรือรีสตาร์ทระบบ เมื่อคลิกจะปรากฏดังภาพที่ 72 เพื่อให้ผู้ดูและระบบคลิกเลือกปิดระบบ หรือรีสตาร์ทระบบ

ภาพที่ 72 แสดงเมนูการปิด/รีสตาร์ทระบบ

ภาคผนวก ข

แบบสอบถาม

วัตถุประสงค์ของแบบสอบถาม

1. เพื่อศึกษาวิจัยผลกระทบ ปัญหาอุปสรรคและข้อบกพร่องต่าง ๆ ของระบบ
2. เพื่อนำไปใช้ในการแก้ไขปัญหาที่จะเกิดขึ้นกับระบบได้ตรงจุด เพื่อนำผลการประเมินมาปรับปรุงระบบงานให้มีประสิทธิภาพมากยิ่งขึ้น
3. เพื่อประเมินการใช้งานและความครบถ้วนของระบบ

คำชี้แจง โปรดทำเครื่องหมาย ☑ หน้าข้อความและในช่องระดับความสำคัญที่ตรงกับความจริง และโปรดเติมข้อมูลต่าง ๆ ในช่องว่างตามความเหมาะสม

ส่วนที่ 1 ข้อมูลทั่วไป

1. เพศ ☐ ชาย ☐ หญิง
2. อายุ.....ปี
3. อายุการทำงาน.....ปี
4. ระดับ
   - ☐ 1-4 ☐ 5-7
   - ☐ ตั้งแต่ 8 ขึ้นไป ☐ ลูกจ้างไม่กำหนดระยะเวลา
   - ☐ ลูกจ้างประจำ ☐ อื่น ๆ (ระบุ).....
5. ระดับการศึกษา
   - ☐ ต่ำกว่าปริญญาตรี ☐ ปริญญาตรี
   - ☐ ปริญญาโท ☐ สูงกว่าปริญญาโท
   - ☐ อื่น ๆ (ระบุ).....
6. ปัจจุบันดำรงตำแหน่ง
   - ☐ สูงกว่า ผส.,ผสค. ☐ ผส.,ผสค.
   - ☐ นทค.,ชทค. ☐ พพฒ.,พกค
   - ☐ พปค.,พคค. ☐ อื่น ๆ (ระบุ).....
7. หน้าที่ความรับผิดชอบ
   - ☐ ผู้บริหาร ☐ ช่างเทคนิค
   - ☐ เจ้าหน้าที่การตลาด ☐ ผู้ดูแลระบบ
   - ☐ อื่น ๆ (ระบุ).....

ส่วนที่ 2 ความสมบูรณ์ของระบบ

รายการ	เกณฑ์/ระดับ					ข้อเสนอแนะ หมายเหตุ
	มากที่สุด	มาก	ปานกลาง	น้อย	น้อยที่สุด	
1.การ Login เข้าสู่ระบบ						
-ความง่ายและสะดวกในการใช้งาน						
-ความถูกต้องของข้อมูลหน้า Login						
2. การใช้งานระบบ						
- ความเร็วของอินเทอร์เน็ตที่ใช้งาน						
-ระยะเวลาการใช้งานอินเทอร์เน็ตถูกต้องตามจริง						
3. ส่วนการจัดการระบบ (สำหรับผู้ดูแลระบบเท่านั้น)						
-การเรียกดูข้อมูลผู้ใช้งานระบบ						
-การเพิ่มข้อมูลผู้ใช้						
-การจัดการกลุ่มผู้ใช้						
-การสร้างบัตรผู้ใช้						
-การปรับแต่งหน้าล็อกอิน						
-การแสดงสถานะผู้ใช้งานในระบบ						
-การตรวจสอบข้อมูลการใช้งานระบบ						
-การเคลียร์ User ค้างในระบบ						
-การจัดการ Service						
-การตรวจสอบ IP						
-การ block website						
-การดูข้อมูล Log						

รายการ	เกณฑ์/ระดับ					ข้อเสนอแนะ หมายเหตุ
	มากที่สุด	มาก	ปานกลาง	น้อย	น้อยที่สุด	
4. ส่วนการดูรายงาน (สำหรับผู้บริหารเท่านั้น)						
5.ความสมบูรณ์ของระบบ						
6.มีประโยชน์ต่อหน่วยงาน						

หมายเหตุ 5=มากที่สุด , 4 = มาก , 3 = ปานกลาง , 2 = น้อย , 1 = น้อยที่สุด

ส่วนที่ 3 ข้อคิดเห็นและข้อเสนอแนะ (อยากต้องการให้ระบุ เพื่อประโยชน์สำหรับการพัฒนาระบบให้เหมาะสมและพร้อมสำหรับการใช้งานในหน่วยงาน)

……

……

……

……

……

……

……

……

……

……

……

……

ขอขอบคุณทุกท่านที่ให้ความร่วมมือในการตอบแบบสอบถาม ทางผู้วิจัยหวังเป็นอย่างยิ่งว่าข้อมูลที่ได้รับจะเป็นประโยชน์สำหรับการพัฒนาระบบให้เหมาะสมกับหน่วยงานยิ่งขึ้นไป

ภาคผนวก ค
รายละเอียดขั้นตอนการปรับแก้ไฟล์ต่าง ๆ ของระบบ

รายละเอียดขั้นตอนการปรับแก้ไฟล์ต่าง ๆ ของระบบ

Login ด้วย user ที่ใช้ตอนติดตั้ง

เปิดใช้งาน root

$sudo passwd

[sudo] password for tipsrin : [ป้อนพาสเวิร์ด user]

Enter new UNIX password: [ตั้ง password root]

Retype new UNIX password: [พิมพ์ password root อีกครั้ง]

passwd: password update successfully;

$exit

Login ใหม่ด้วย user root

เปิดใช้งาน Internal LAN card (ต้องมี LAN Card 2 ใบ)

#vim /etc/network/interfaces

auto lo

iface lo inet loopback

auto eth0 # การ์ด WAN

iface eth0 inet static

address 202.129.12.51 # ใส่ค่า IP Address Card WAN

netmask 255.255.255.0

network 202.129.12.0

broadcast 202.129.12.255

gateway 202.129.12.1 # ใส่ค่า IP ของ Router

dns-nameservers 61.19.245.245 # ใส่ค่า DNS ของ CAT

dns-search west.cat.net.th

auto eth1 #เพิ่มบรรทัดนี้ เข้าไป เพื่อเป็น Card LAN

:wq! # กด ESC ตามด้วย :wq! หมายถึงบันทึกและออก

แก้ไขไฟล์ /etc/resolv.conf

#vim /etc/resolv.conf

nameserver 61.19.245.245 #ใส่ค่า DNS ของ ISP

nameserver 61.19.245.246 #ใส่ค่า DNS ของ ISP

:wq! # กด ESC ตามด้วย :wq! หมายถึงบันทึกและออก

เปิด Forward IP

#vim /etc/sysctl.conf

net.ipv4.ip_forward=1 # บรรทัดที่ 28 นำเครื่องหมาย # ออกจากหน้าบรรทัดที่ 28

:wq! # กด ESC ตามด้วย :wq! หมายถึงบันทึกและออก

สั่งให้มีผลทันที โดยไม่ต้อง Reboot เครื่อง

echo 1 | tee /proc/sys/net/ipv4/ip_forward

รีสตาร์ท Network ใหม่

/etc/init.d/networking restart

ทดสอบสถานะการเชื่อมต่อ (โดยเสียบสายแลนเส้นเดียว คือ สายที่มาจาก Router) ก่อน

#mii-tool

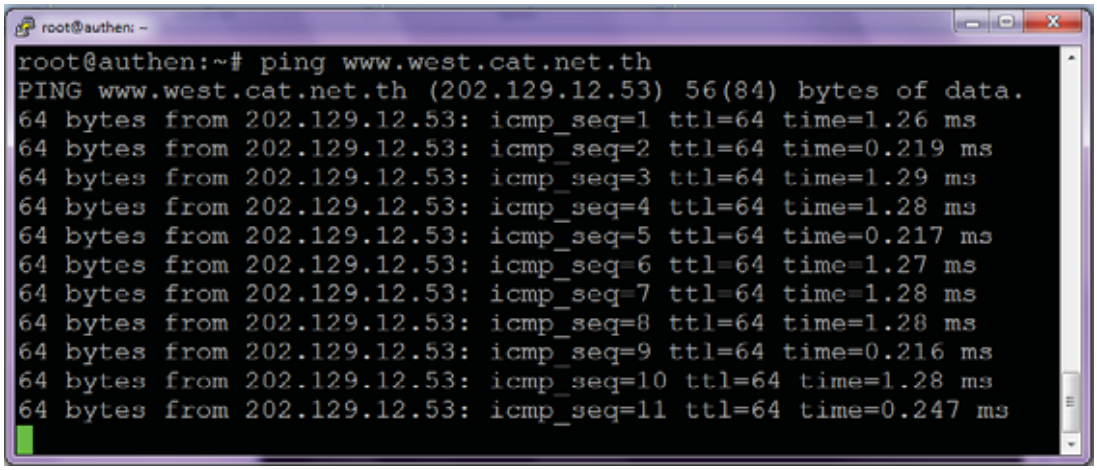
eth0 : negotiated 100baseTxFD flow-control, link ok #แสดงว่าสายเสียบอยู่ที่ eth0 แล้ว

.....

ทดสอบว่าเครื่อง Server ออกเน็ตได้หรือยัง

#ping www.yahoo.com

ถ้าเครื่อง Server ออกอินเตอร์เน็ตได้แล้ว จะเป็นเหมือนดังภาพที่ 73



ภาพที่ 73 แสดงค่าที่ได้จากการ ping www.yahoo.com

ทำการ Update

apt-get update (รอจนมาอยู่ที่ #)

การติดตั้ง Freeradius และ ปรับแต่ง

apt-get install –y freeradius freeradius-mysql #ติดตั้ง freeradius , freeradius-mysql

#vim /etc/freeradius/radiusd.conf #เข้าปรับแต่งค่า radiusd.conf

บรรทัดที่ 65

run_dir = ${localstatedir}/run/radiusd

แก้เป็น

run_dir = ${localstatedir}/run/freeradius

บรรทัดที่ 113

pidfile = ${run_dir}/radiusd.pid

แก้เป็น

pidfile = ${run_dir}/freeradius.pid

:wq! # กด ESC ตามด้วย :wq! หมายถึงบันทึกและออก

เสร็จแล้ว restart freeradius ใหม่

/etc/init.d/freeradius restart

ตั้งค่าการ Authen โดยใช้ฐานข้อมูล Mysql แทนการ Authen ผ่านไฟล์ user ในระบบ

#mysql -uroot –pmysqlsecret

สร้าง database ชื่อ radius ดังนี้

CREATE DATABASE radius;

สร้าง user ที่มีสิทธิใน database ดังนี้

GRANT ALL PRIVILEGES ON radius.* to 'radius'@'localhost' IDENTIFIED BY

'mysql@cattelecom';

FLUSH PRIVILEGES;

ออกจาก mysql ด้วยคำสั่ง

quit;

นำเข้าโครงสร้างฐานข้อมูล

#mysql -uroot –pmysqlsecret radius < /etc/freeradius/sql/mysql/ippool.sql

#mysql -uroot –pmysqlsecret radius < /etc/freeradius/sql/mysql/nas.sql

#mysql -uroot –pmysqlsecret radius < /etc/freeradius/sql/mysql/schema.sql

Add user ในฐานข้อมูล mysql และ ทดสอบ

echo “INSERT INTO radcheck (username,attribute,value) VALUES

(‘tipsrin’,’pasword’,’tipsrin’);” | mysql –uroot –pmysql@cattelecom radius

แก้ไขไฟล์ /etc/freeradius/sql.conf เพื่อให้ freeradius ติดต่อกับฐานข้อมูล radius

vim /etc/freeradius/sql.conf

บรรทัดที่ 36,37,38 และ 41

Connection info:

36 server = "localhost"

37 login = "radius"

38 password = "mysql@cattelecom"

39

40 # Database table configuration for everything except Oracle

41 radius_db = "radius"

:wq! # กด ESC ตามด้วย :wq! หมายถึงบันทึกและออก

แก้ไขไฟล์ /etc/freeradius/sites-enabled/default

vim /etc/freeradius/sites-enabled/default

บรรทัดที่ 152

151# See "Authorization Queries" in sql.conf

152 sql # นำ # หน้าบรรทัดนี้ออก

บรรทัดที่ 197 – 202

195 # Autz-Type Status-Server {

196 #

197 # }

198 noresetcounter # เพิ่มบรรทัดนี้

100 dailycounter # เพิ่มบรรทัดนี้

200 monthlycounter # เพิ่มบรรทัดนี้

201

202 }

บรรทัดที่ 346

345 # See "Accounting queries" in sql.conf

346 sql #นำ # ออกจากหน้าบรรทัดนี้

บรรทัดที่ 377

376 # See "Simultaneous Use Checking Queries" in sql.conf

377 sql #นำ # ออกจากหน้าบรรทัดนี้

378 }

:wq! # กด ESC ตามด้วย :wq! หมายถึงบันทึกและออก

รีสตาร์ท radius

/etc/init.d/freeradius restart

ขั้นตอนการติดตั้ง Coova-Chilli

ติดตั้ง Coova-Chilli

โดยการ Download Coova-Chilli จาก web ดังนี้

wget http://ap.coova.org/chilli/coova-chilli_1.0.12-1_i386.deb

dpkg –i coova-chilli_1.0.12-1_i386.deb

แก้ไขไฟล์ /etc/default/chilli

vim /etc/default/chilli

START_CHILLI=0

แก้เป็น

START_CHILLI=1

:wq! # กด ESC ตามด้วย : wq! หมายถึงบันทึกและออก

แก้ไขไฟล์ config ของ coova-chilli ดังนี้

cp /etc/chilli/defaults /etc/chilli/config

vim /etc/chilli/config

13 # HS_WANIF=eth0 # WAN Interface toward the Internet

14 HS_LANIF=eth1 # Subscriber Interface for client devices

15 HS_NETWORK=**10.23.51.0** # HotSpot Network (must include HS_UAMLISTEN)

16 HS_NETMASK=**255.255.255.0** # HotSpot Network Netmask

17 HS_UAMLISTEN=**10.23.51.254** # HotSpot IP Address (on subscriber network)

18 HS_UAMPORT=**3990** # HotSpot Port (on subscriber network)

19

20 #HS_DYNIP=10.23.51.200/24:10.23.51.201/24

21 #HS_DYNIP_MASK=255.255.255.0

22 HS_STATIP=**10.23.51.0**

23 HS_STATIP_MASK=**255.255.255.0**

24 # HS_DNS_DOMAIN=

25 HS_DNS1=**61.19.245.245**

26 HS_DNS2=**61.19.245.246**

27

28 ###

29 # HotSpot settings for simple Captive Portal

30 #

```
31      HS_NASID=nas01
32      HS_UAMSECRET=uamsecret          #เหมือนกับไฟล์ /var/www/hotspotlogin.php
33      HS_RADIUS=127.0.0.1
34      HS_RADIUS2=127.0.0.1
35      HS_RADSECRET=testing123
36      HS_UAMALLOW=10.23.51.0/24,202.129.12.51
……….

48      #  create the final chilli 'uamserver' url configuration.
49      HS_UAMSERVER=10.23.51.254
50
51      #  Use HS_UAMFORMAT to define the actual captive portal url.
52      #  Shell variable replacement takes place when evaluated, so here
53      #  HS_UAMSERVER is escaped and later replaced by the pre-defined
54      #  HS_UAMSERVER to form the actual "--uamserver" option in chilli.
55      HS_UAMFORMAT=https://10.23.51.254/hotspotlogin.php
56
57      #  Same principal goes for HS_UAMHOMEPAGE.
58      #HS_UAMHOMEPAGE=http://10.23.51.254:3990/prelogin
59      HS_UAMHOMEPAGE=http://10.23.51.254/welcome.html
60
61      #  This option will be configured to be the WISPr LoginURL as well
62      #  as provide "uamService" to the ChilliController. The UAM Service is
63      #  described in: http://coova.org/wiki/index.php/CoovaChilli/UAMService
64      #
65      HS_UAMSERVICE=https://10.23.51.254/hotspotlogin.php
```

:wq! # กด ESC ตามด้วย :wq! หมายถึงบันทึกและออก

Restart Coova-chilli

/etc/init.d/chilli restart

ทดสอบว่า chilli ทำงานหรือยัง

ifconfig

สังเกตดูว่าจะต้องมี interfaces tun0 เพิ่มเข้ามา (ได้ IP เป็น 10.23.51.254) แสดงว่าพร้อมทำงานแล้ว สามารถนำ Access Point มาเชื่อมต่อกับ ช่อง LAN Card eth1 ได้เลย (ต้องปิดโหมด DHCP ของ Access Point)

การปรับแต่ง Firewall สำหรับทำ Transparent Proxy

การทำ Transparent proxy คือ การบังคับให้เครื่อง client ออกอินเตอร์เน็ต โดยผ่าน Proxy Server (port 3128) ประโยชน์คือเครื่อง client ไม่ต้องไปกำหนดหมายเลขไอพีและหมายเลขพอร์ตของ Proxy Server

chmod +x /etc/init.d/chilli.iptables

ln –s /etc/init.d/chilli.iptables /etc/rcS.d/S41/chilli.iptables

ดูเนื้อหาของไฟล์

vim /etc/init.d/chilli.iptables

#!/bin/sh

Firewall script for ChilliSpot

A Wireless LAN Access Point Controller

Uses $EXTIF (eth0) as the external interface (Internet or intranet) and

$INTIF (eth1) as the internal interface (access points).

SUMMARY

```
# * All connections originating from chilli are allowed.
# * Only ssh is allowed in on external interface.
# * Nothing is allowed in on internal interface.
# * Forwarding is allowed to and from the external interface, but disallowed
#   to and from the internal interface.
# * NAT is enabled on the external interface.

IPTABLES="/sbin/iptables"
EXTIF1="eth0"
INTIF="eth1"

$IPTABLES -F
$IPTABLES -t nat -F

$IPTABLES -P INPUT DROP
$IPTABLES -P FORWARD ACCEPT
$IPTABLES -P OUTPUT ACCEPT

#Allow related and established on all interfaces (input)
$IPTABLES -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

#Allow releated, established and ssh on $EXTIF. Reject everything else.
$IPTABLES -A INPUT -i $EXTIF1 -p tcp -m tcp --dport 22 --syn -j ACCEPT
$IPTABLES -A INPUT -i $EXTIF1 -j REJECT

#Allow ssh tun0
```

```
$IPTABLES -A INPUT -i tun0 -p tcp -m tcp --dport 22 --syn -j ACCEPT
$IPTABLES -A INPUT -i tun0 -p tcp -m tcp --dport 3306 --syn -j ACCEPT

#Allow related and established from $INTIF. Drop everything else.
$IPTABLES -A INPUT -i $INTIF -j DROP

#Allow http and https on other interfaces (input).
#This is only needed if authentication server is on same server as chilli
$IPTABLES -A INPUT -p tcp -m tcp --dport 80 --syn -j ACCEPT
$IPTABLES -A INPUT -p tcp -m tcp --dport 443 --syn -j ACCEPT
$IPTABLES -A INPUT -p udp --dport 53 -j ACCEPT

#Allow for Network Time Protocol
$IPTABLES -A INPUT -p udp --dport 123 -j ACCEPT
$IPTABLES -A OUTPUT -p udp --sport 123 -j ACCEPT

#Allow 3990 on other interfaces (input).
$IPTABLES -A INPUT -p tcp -m tcp --dport 3990 --syn -j ACCEPT

#Allow transparent proxy 1/2
$IPTABLES -A INPUT -p tcp -m tcp --dport 3128 --syn -j ACCEPT

#Allow everything on loopback interface.
$IPTABLES -A INPUT -i lo -j ACCEPT

#Allow transparent proxy 2/2
```

```
$IPTABLES -t mangle -A PREROUTING -i tun0 -p tcp -m tcp --dport 3128 --syn -j DROP
$IPTABLES -t nat -A PREROUTING -i tun0 -p tcp -m tcp -d 10.0.0.0/24 --dport 80 -j RETURN
$IPTABLES -t nat -A PREROUTING -i tun0 -p tcp -m tcp --dport 80 -j REDIRECT --to-ports
3128

# Drop everything to and from $INTIF (forward)
# This means that access points can only be managed from ChilliSpot
$IPTABLES -A FORWARD -i $INTIF -j DROP
$IPTABLES -A FORWARD -o $INTIF -j DROP

#MSN Service

$IPTABLES -t mangle -A PREROUTING -i $EXTIF1 -p tcp -m tcp --dport 1683 -j MARK --set-
mark 1
$IPTABLES -t mangle -A PREROUTING -i $EXTIF1 -p udp -m udp --dport 1683 -j MARK --
set-mark 1

#Enable NAT on output device
$IPTABLES -t nat -A POSTROUTING -o $EXTIF1 -j MASQUERADE
:q!                                    # กด ESC ตามด้วย : q! หมายถึงออกจากระบบ
```

Run Script chilli.iptables

```
# /etc/init.d/chilli.iptables
```

การปรับแต่ง Apache Web Server และ SSL

สร้าง Virtualhost

vim /etc/apache2/sites-available/hotspot

NameVirtualHost **10.23.51.254:443**

<VirtualHost **10.23.51.254:443**>

ServerAdmin webmaster@pt-lmr.com

DocumentRoot "/var/www/hotspot"

ServerName **"10.23.51.254"**

<Directory "/var/www/hotspot/">

Options Indexes FollowSymLinks MultiViews

AllowOverride None

Order allow,deny

allow from all

</Directory>

Alias "/dialupadmin/" "/usr/share/freeradius-dialupadmin/htdocs/"

<Directory "/usr/share/freeradius-dialupadmin/htdocs/">

Options Indexes FollowSymLinks MultiViews

AllowOverride None

Order allow,deny

allow from all

</Directory>

ScriptAlias /cgi-bin/ /var/www/hotspot/cgi-bin/

<Directory "/var/www/hotspot/cgi-bin/">

AllowOverride None

```
                Options ExecCGI -MultiViews +SymLinksIfOwnerMatch
                Order allow,deny
                Allow from all
        </Directory>

        ErrorLog /var/log/apache2/hotspot-error.log

        LogLevel warn

        CustomLog /var/log/apache2/hotspot-access.log combined

        ServerSignature On
        SSLEngine on
        SSLCertificateFile /etc/apache2/ssl/apache.pem
</VirtualHost>
```

เปิด SSL virtualhost

```
# a2ensite hotspot
# /etc/init.d/apache2 reload
```

สร้าง Listen port

```
# vim /etc/apache2/ports.conf
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
```

/etc/apache2/sites-enabled/000-default

NameVirtualHost *:80 # เอา # ออก

Listen 80 # เอา # ออก

Listen 443 # เอา # ออก

#<IfModule mod_ssl.c>

SSL name based virtual hosts are not yet supported, therefore no

NameVirtualHost statement here

Listen 443

#</IfModule>

:wq! # กด ESC ตามด้วย :wq! หมายถึงบันทึกและออก

แก้ไขไฟล์

vim /etc/apache2/sites-available/default

<VirtualHost *:80>

เพิ่ม Server Name 10.23.51.254 บรรทัดบนสุด

vim /etc/apache2/apache2.conf

ServerName **10.23.51.254**

แก้ไขไฟล์ hosts

vim /etc/hosts

10.23.51.254 hotspot.domain.org hotspot # ใส่ชื่อ Host และ domain name ของเรา

Restart apache

/etc/init.d/apache2 restart

Reboot Server 1 รอบ

shutdown –r now

ขั้นตอนการติดตั้ง Squid Proxy Server

ติดตั้ง Squid Proxy Server

apt-get install squid

แก้ไขไฟล์ squid.conf

---- NETWORK OPTIONS

http_port 0.0.0.0:3128 transparent no-connection-auth

hierarchy_stoplist cgi-bin ? \.info$ \.ini$ \.dll$ \.inf$ \.php$ \.html$ \.htm$ \.cgi$ \.jsp$ \.js$ \.asp$ \.aspx$ \.phtml$ \.ctf$ \.cfg$ \.txt$ \.xml$ \.xtp$ \.ver$ version \.md5$ \.config$ update.ver \.css$ 10\.0\.1\.1 \.php

---- ACL CONTROLS

acl all src 0.0.0.0/0.0.0.0

acl net src 10.23.51.0/24

acl 2blockweb url_regex -i "/etc/squid/website.txt"

acl 2download url_regex -i "/etc/squid/filename.txt"

http_access deny 2blockweb

http_access deny 2download

deny_info http://10.23.51.254/deny.html 2blockweb

deny_info http://10.23.51.254/deny.html 2download

acl QUERY url_regex cgi-bin [^z]\? photos[1-9] \.D$ \.ini$ \.dll$ \.inf$ \.Xt \.xtp Loader\.exe 1st$ update.cfg\? urlinfo\.ini$ updatelist notice_popup ProjectG.exe.zip$ start/ucg \.php UCG\.DAT$ UCGA?\.exe$ version\.cfg$ 10\.0\.1\.1

cache deny QUERY

```
http_access allow net

# ---- DNS OPTIONS
ipcache_size 3072

# ---- MEMORY CACHE OPTIONS
cache_mem 700 MB
maximum_object_size_in_memory 8 MB
memory_replacement_policy heap GDSF
ipcache_high 98
ipcache_low 93

# ---- DISK CACHE OPTIONS
cache_dir aufs /var/spool/squid 6144 16 256
maximum_object_size 32 MB
cache_replacement_policy heap GDSF
store_dir_select_algorithm round-robin
cache_swap_high 98
cache_swap_low 93
cache_dir null /dev/null

# ---- HTTP OPTIONS
ie_refresh on
vary_ignore_expire on

# ----- Log Format
```

```
logformat squid %ts.%03tu %6tr %>a %Ss/%03Hs %<st %rm %ru %un %Sh/%<A %mt
logformat squidmime %ts.%03tu %6tr %>a %Ss/%03Hs %<st %rm %ru %un %Sh/%<A %mt
[%>h] [%<h]
logformat common %>a %ui %un [%tl] "%rm %ru HTTP/%rv" %Hs %<st %Ss:%Sh
logformat combined %>a %ui %un [%tl] "%rm %ru HTTP/%rv" %Hs %<st "%{Referer}>h"
"%{User-Agent}>h" %Ss:%Sh

# ---- LOGFILE OPTIONS
# cache_access_log /var/log/squid/access.log
access_log /var/log/squid/access.log
access_log syslog:local0.notice combined
cache_log /var/log/squid/cache.log
cache_store_log none
logfile_rotate 90
pid_filename /var/run/squid.pid
buffered_logs off
strip_query_terms off

# ---- MISCELLANEOUS
pipeline_prefetch on

# OPTIONS FOR FTP GATEWAYING
ftp_passive on
ftp_sanitycheck on

# ---- OPTIONS FOR TUNING THE CACHE
```

```
quick_abort_min 0 KB
quick_abort_max 0 KB
refresh_pattern -i .(class|pdf|rtf|doc|wp|wp5|ps|prn)$ 1440 80% 1440 override-lastmod override-expire reload-into-ims ignore-reload
refresh_pattern -i .(mov|avi|mpg|wav|au|mid|mp3)$ 1440 100% 1440 override-lastmod override-expire reload-into-ims ignore-reload
refresh_pattern -i .(zip|gz|pkg|arj|lha|lzh|dat|rar|tgz|tar|Z)$ 1440 100% 1440 override-lastmod override-expire reload-into-ims ignore-reload
refresh_pattern -i .(jpg|gif|jpeg|png|css|js)$ 1440 100% 1440 override-lastmod override-expire reload-into-ims ignore-reload
refresh_pattern -i .(bmp|tif|tiff|xbm)$ 1440 100% 1440 override-lastmod override-expire reload-into-ims ignore-reload
refresh_pattern -i .(png|swf)$ 1440 18000% 1440 override-lastmod override-expire reload-into-ims ignore-reload
refresh_pattern -i .(exe|db|daf|pak|fsh|dll)$ 1440 100% 1440 override-lastmod override-expire reload-into-ims ignore-reload
refresh_pattern ^http://.*\.*$ 0 20% 1440
refresh_pattern ^ftp://.*\.*$ 0 20% 1440
refresh_pattern ^ftp: 0 20% 1440
refresh_pattern ^gopher: 0 0% 1440
refresh_pattern . 0 20% 1440

# ---- OPTIONS INFLUENCING REQUEST FORWARDING
prefer_direct on

# ---- TIMEOUTS
```

half_closed_clients off

---- ADMINISTRATIVE PARAMETERS

cache_mgr tipsrin.p@cattelecom.com

visible_hostname www.west.cat.net.th

start squid

/etc/init.d/squid restart

ติดตั้ง NTP

#apt-get install ntp

#ls –l /etc/localtime

#ln –sf /usr/share/zoneinfo/Asia/Bangkok /etc/localtime

แก้ไขไฟล์ /etc/ntp.conf โดยก่อนจะแก้ไข ต้องเลือกว่าจะใช้อ้างอิงเวลาของที่ไหน ตรวจสอบเวลาโดยใช้คำสั่ง

#ntpdate time1.nimt.or.th

#ntpdate time.navy.mi.th

#ntpdate clock.nectec.or.th

ก่อนที่จะตรวจสอบเวลา ต้องสั่ง stop ntp ในเครื่องก่อน โดยใช้คำสั่ง

#/etc/init.d/ntp stop

เมื่อเลือกได้ว่าจะเทียบเวลากับ server ของหน่วยงานใด ก็เพิ่ม server นั้นใน ntp.conf โดย

vim /etc/ntp.conf

เพิ่ม

server time1.nimt.or.th

server time.navy.mi.th

server clock.nectec.or.th

:wq! # กด ESC ตามด้วย : wq! หมายถึงการบันทึกออกจากระบบ

รีสตาร์ท NTP ด้วยคำสั่ง

/etc/init.d/ntp restart

ตรวจสอบการทำงานของ ntpd โดยใช้คำสั่ง

#ntptrace

รายละเอียดการแก้ไข File ต่าง ๆ สำหรับเครื่อง Centralized log Server หลังการติดตั้งโปรแกรม ubuntu

 # apt-get install syslog-ng

จะปรากฏข้อความ ดังต่อไปนี้

Reading package lists... Done

Building dependency tree

Reading state information... Done

The following packages will be REMOVED:

klogd sysklogd ubuntu-minimal

The following NEW packages will be installed:

syslog-ng

0 upgraded, 1 newly installed, 3 to remove and 4 not upgraded.

Need to get 209kB of archives.

After this operation, 188kB of additional disk space will be used.

Do you want to continue [Y/n]? Y //เลือก Y เพื่อทำการยืนยันถึงการติดตั้ง

Get:1 http://th.archive.ubuntu.com hardy/universe syslog-ng 2.0.9-1ubuntu1 [209kB]

Fetched 209kB in 0s (1724kB/s)

(Reading database ... 124401 files and directories currently installed.)

Removing ubuntu-minimal ...

Removing klogd ...

* Stopping kernel log daemon...

...done.

Removing sysklogd ...

* Stopping system log daemon...

...done.

Selecting previously deselected package syslog-ng.

(Reading database ... 124377 files and directories currently installed.)

Unpacking syslog-ng (from .../syslog-ng_2.0.9-1ubuntu1_i386.deb) ...

Setting up syslog-ng (2.0.9-1ubuntu1) ...

* Starting system logging syslog-ng

...done.

ทำการทดสอบการทำงานของ Syslog-ng โดยคำสั่ง

 # /etc/init.d/syslog-ng restart

และตามด้วย

 # logger -i -t logtest -- "logtest"

ทำการตรวจสอบการเขียน log ของ Syslog-ng ด้วยคำสั่งดังต่อไปนี้

 # tail /var/log/syslog

ผลที่ได้จะปรากฏ ดังต่อไปนี้

Nov 15 01mail syslog-ng[]: Termination requested via signal, terminating;

Nov 15 01mail syslog-ng[]: syslog-ng shutting down; version='0'

Nov 15 01mail syslog-ng[]: syslog-ng starting up; version='0'

Nov 0145 mail logtest[9302]: logtest

แสดงว่า Syslog-ng สามารถทำงานได้แล้ว

ขั้นตอนในการแก้ไขเพื่อให้ syslog-ng รองรับ log จากเครื่องอื่น โดยทั่วไปนั้น เครื่องที่จะทำงานเป็น Centralized log Server นั้นจะใช้งานพอร์ตมาตรฐานคือ udp 514(สำหรับ syslogd) แต่สำหรับ Syslog-ng สามารถทำงานได้ทั้ง udp/tcp 514 และยังสามารถปรับแต่งให้ทำงานที่พอร์ตอื่นได้อีก โดยปกติ syslog-ng จะไม่รองรับการทำงานเป็น Centralized log Server จะต้องมีการแก้ไข ดังนี้

ไฟล์ที่จะเข้าไปทำการแก้ไขคือ “syslog-ng.conf” ซึ่งโดยทั่วไปจะอยู่ที่ “/etc/syslog-ng/syslog-ng.conf” ในที่นี้จะทำการเปิดพอร์ตในการทำงานทั้ง tcp/udp 514

แก้ไขไฟล์ syslog-ng.conf โดยเพิ่ม port 514 บรรทัดที่ 88 - 91

87 # Source from remote client

88 source s_client {

89 tcp(ip(0.0.0.0) port(514) keep-alive(yes) max-connections(300));

90 udp(ip(0.0.0.0) port(514));

91 };

……..

บรรทัดที่ 103 – 107 กำหนดรูปแบบ File Log ของ squid ที่จะส่ง Log

103 destination d_squid {

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

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

106 create_dirs(yes) dir_perm(0775));

107 };

:wq! # กด ESC ตามด้วย :wq! หมายถึงบันทึกและออก

หลังจากที่ได้มีการเพิ่ม Port 514 และกำหนดรูปแบบการส่ง Log เข้าไปแล้วให้ทำการ restart syslog-ng ด้วยคำสั่ง

 # /etc/init.d/syslog-ng restart

ทำการตรวจสอบการทำงานของพอร์ตที่เปิดขึ้น

 # netstat -an |grep 514

tcp 0 0 0.0.0.0:514 0.0.0.0:* LISTEN //พอร์ตที่เปิดขึ้นมา

udp 0 0 0.0.0.0:514 0.0.0.0:* //พอร์ตที่เปิดขึ้นมา

udp 0 0 10.23.51.197:45918 10.23.51.254:514 ESTABLISHED //มีการเชื่อมต่อ

แสดงว่า syslog-ng รองรับการทำงานเป็น Centralized log server แล้ว

การปรับแต่ง Firewall เพื่อเปิด port สำหรับการส่ง Log

vim /etc/init.d/firewall.iptables

ดูเนื้อหาของไฟล์

#!/bin/sh

a simple iptables ruleset

```
iptables="/sbin/iptables"

# flush any existing chains and set default policies
$iptables -F INPUT
$iptables -F OUTPUT
$iptables -F FORWARD

# set default parameters
$iptables -P INPUT DROP
$iptables -P OUTPUT ACCEPT
$iptables -P FORWARD DROP

# this is our main rule, to allow established connections in
$iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# allow all packets on the loopback interface (so that gnome can function)
$iptables -A INPUT -i lo -j ACCEPT
$iptables -A OUTPUT -o lo -j ACCEPT

$iptables -A INPUT -p tcp --dport 22 -j ACCEPT
$iptables -A INPUT -p tcp --dport 514 -j ACCEPT
$iptables -A INPUT -p udp --dport 514 -j ACCEPT

$iptables -A INPUT -p udp --dport 123 -j ACCEPT
$iptables -A INPUT -p tcp --dport 123 -j ACCEPT
$iptables -A OUTPUT -p udp --sport 123 -j ACCEPT
```

:wq! # กด ESC ตามด้วย : wq! หมายถึงบันทึกและออก

รีสตาร์ท firewall ใหม่

/etc/init.d/firewall.iptables

รายละเอียดการทำ Stunnel เพื่อความปลอดภัยของการส่งข้อมูลระหว่างเครื่อง Authentication Server กับ Centralized log Server

สร้าง Certificate โดยคำสั่ง

root@Log-ntp:/etc/stunnel# openssl req -new -x509 -days 3650 -nodes -out stunnel.pem -keyout stunnel.pem

Generating a 1024 bit RSA private key

writing new private key to 'stunnel.pem'

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:**th**

State or Province Name (full name) [Some-State]:**ratchaburi**

Locality Name (eg, city) []:**moung**

Organization Name (eg, company) [Internet Widgits Pty Ltd]:**cattelecom Ltd**

Organizational Unit Name (eg, section) []:**marketing**

Common Name (eg, YOUR name) []:**tipsrin**

Email Address []:**tipsrin.p@cattelecom.com**

แสดง stunnel.pem

root@Log-ntp:/etc/stunnel# cat stunnel.pem

-----BEGIN RSA PRIVATE KEY-----

MIICXQIBAAKBgQDKPeYrFbpwgymo/v6hk7LEi/W++kHRwSpSIUD5+L1aG6c5B0ff

JPUmltWcZsmNIMYDUmPvcnFAkg80znfGYpG644gwA9rtIPZ2F7LQiiGXkLFFcNDw

Ah8FXgQHbGkoqgvl1J0uSBWVa8rLA6BqjsMePQNTYjOwa5HYHalOseBLvQIDAQAB

AoGBAMBEoqp5SLsoZxXL/oXb5ctnh+TdBHAGZVaZWK2NJW8h9ROJcXGaMBpUsZW0

Po8WBkooLOv6b+LEOQKp+0K2ePV0JvGU96SSzi5b2cWZdV5FtOYzvMZssARVd7t9

fgFKa1m4BGobKz9u0lQu7MdqxnMPUb3Dd/vLf+Va0IM0MwohAkEA5pY6khyblyp8

l4XdUUm2a9Zz72YfLJAUWxCrEbOU5a26KXdnJazXLS/5ju151oPi6XzN32soRy78

sY56ILJidQJBAOCH8bBwYVSqqN1u1DyKleDYSag5ovpWtUNga9wvMvx2grqTXRqa

5JZ3/vS0jsq8u3G/JRN1wz3M7DuPRSVViykCQEm6gVHUud8044+jaueh9SU39ev3

MEKUcx3HD5viWtqxmNPHbQC76jV1oIsV3Z48n2Je2Ij2f3N7T6sKTnyD7T0CQQDT

EtlBHZRSDJDsgSihtUJKeelcbLpqjiKesUEUX4aV0S76CFiJDz1+ulWCY06tBhlM

R/2pupYNPdyB7SB6hV1pAkA+caWtyS/SVL1yWXVvx1+v1gLVMn1gIIZtsYz+7g6+

HrRUAB2cKLDYV7U3xEOO0Tcmp2Uipc2+3KtqradyU2mF

-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----

MIIDuDCCAyGgAwIBAgIJAP6y18k+a9YzMA0GCSqGSIb3DQEBBQUAMIGaMQswCQYD

VQQGEwJUSDETMBEGA1UECBMKUmF0Y2hhYnVyaTEOMAwGA1UEBxMFbW91bmcxF

zAV

BgNVBAoTDmNhdHRlbGVjb20gTHRkMRIwEAYDVQQLEwltYXJrZXRpbmcxEDAOBgNV

BAMTB3RpcHNyaW4xJzAlBgkqhkiG9w0BCQEWGHRpcHNyaW4ucEBjYXR0ZWxlY29t

LmNvbTAeFw0xMTAxMjQwODMxMjhaFw0yMTAxMjEwODMxMjhaMIGaMQswCQYDVQ

QG

EwJUSDETMBEGA1UECBMKUmF0Y2hhYnVyaTEOMAwGA1UEBxMFbW91bmcxFzAVB
gNV
BAoTDmNhdHRlbGVjb20gTHRkMRIwEAYDVQQLEwltYXJrZXRpbmcxEDAOBgNVBAMT
B3RpcHNyaW4xJzAlBgkqhkiG9w0BCQEWGHRpcHNyaW4ucEBjYXR0ZWxlY29tLmNv
bTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAyj3mKxW6cIMpqP7+oZOyxIv1
vvpB0cEqUiFA+fi9WhunOQdH3yT1JpbVnGbJjSDGA1Jj73JxQJIPNM53xmKRuuOI
MAPa7SD2dhey0Iohl5CxRXDQ8AIfBV4EB2xpKKoL5dSdLkgVlWvKywOgao7DHj0D
U2IzsGuR2B2pTrHgS70CAwEAAaOCAQIwgf8wHQYDVR0OBBYEFN+HZawsg5SJTK8g
3XjRdHYRgVvJMIHPBgNVHSMEgccwgcSAFN+HZawsg5SJTK8g3XjRdHYRgVvJoYGg
pIGdMIGaMQswCQYDVQQGEwJUSDETMBEGA1UECBMKUmF0Y2hhYnVyaTEOMAwGA1UE
BxMFbW91bmcxFzAVBgNVBAoTDmNhdHRlbGVjb20gTHRkMRIwEAYDVQQLEwltYXJr
ZXRpbmcxEDAOBgNVBAMTB3RpcHNyaW4xJzAlBgkqhkiG9w0BCQEWGHRpcHNyaW4u
cEBjYXR0ZWxlY29tLmNvbYIJAP6y18k+a9YzMAwGA1UdEwQFMAMBAf8wDQYJKoZI
hvcNAQEFBQADgYEAxKaP93SEZipZgUXOf6z1hHXWp9I2HrgmWKi0m77cCuu+yAUU
og390ttaO9jQ0HUc5H73oFZ5fpdu7svT3RBZMt4kVeRY70q3UQUbSP0PhL8fVE4F
KRgVOpsbdp0q0kydbSUWJB1X4jgU9VW0MgDM8sKU6PVsZE1VdI7gaOeTFBs=
-----END CERTIFICATE-----

START SSL TUNNEL Server

root@Log-ntp:~# /etc/init.d/stunnel4 start

Starting SSL tunnels: [Started: /etc/stunnel/syslog-server.conf] stunnel.

root@Log-ntp:~# netstat -an | grep 514

tcp 0 0 0.0.0.0:60514 0.0.0.0:* LISTEN

tcp 0 0 0.0.0.0:61514 0.0.0.0:* LISTEN

tcp 0 0 61.19.42.172:60514 202.129.12.51:48892 ESTABLISHED

udp 0 0 0.0.0.0:60514 0.0.0.0:*

unix 2 [ ] STREAM CONNECTED 5514

START SSL TUNNEL Authentication Server

root@authen:~# /etc/init.d/stunnel4 start

Starting SSL tunnels: [Already running: /etc/stunnel/syslog-client.conf] stunnel

root@authen:~# netstat -an | grep 60514

tcp 0 0 127.0.0.1:60514 0.0.0.0:* LISTEN

tcp 0 0 192.168.1.11:57148 61.19.42.172:60514 ESTABLISHED

ในการส่งข้อมูลจราจรคอมพิวเตอร์ใช้ syslog-ng ร่วมกับ Openssl และ Stunnel เพื่อเข้ารหัสในระหว่างการส่ง เพื่อป้องกันการใช้โปรแกรมดักจับข้อมูลที่ส่งผ่านเครือข่าย ทำให้ข้อมูลที่จัดเก็บนั้นมีความน่าเชื่อถือเพิ่มมากขึ้น

ติดตั้ง syslog-ng เครื่อง Authentication Server

apt-get install syslog-ng

/etc/init.d/syslog-ng restart เพื่อรีสตาร์ท syslog-ng ก่อนใช้งาน

ติดตั้ง openssl และ stunnel

apt-get install openssl stunnel

สร้างคอนฟิกไฟล์สำหรับ stunnel

#vim /etc/stunnel/syslog-client.conf

#ModLoad imuxsock

debug = 7

client = yes

[syslog-ng]

accept = 127.0.0.1:60514

connect = [61.19.42.172]:61514

แก้ไขไฟล์ /etc/default/stunnel4

vim /etc/default/stunnel4

ENABLED=1

FILES=”/etc/stunnel/syslog-client.conf”

เริ่มโพรเซส stunnel

#/etc/init.d/stunnel4 start

ทดสอบ

#netstat -an |grep61514

tcp0 0 127.0.0.1:61514 0.0.0.0:* LISTEN

แก้ไขไฟล์ /etc/rsyslog.conf แล้วเพิ่ม

.@@127.0.0.1:61514

เริ่ม rsyslog ใหม่

/etc/init.d/rsyslog restart

ที่เครื่อง Centralized log server

ติดตั้ง openssl และ stunnel

#vim apt-get install openssl stunnel

สร้าง Certificate

#cd/etc/stunnel

opensslreq-new-x509 -days 3650 -nodes -out stunnel.pem-keyoutstunnel.pem

สร้างคอนฟิกไฟล์สำหรับ stunnel

vim /etc/stunnel/syslog-server.conf

/etc/init.d/stunnel4 start

cert = /etc/stunnel/stunnel.pem

debug = 7

[syslog-ng]

accept = 61514

connect = 60514

แก้ไฟล์ /etc/default/stunnel4

ENABLED=1

FILES=”/etc/stunnel/syslog-server.conf”

เริ่มโพรเซส stunnel

/etc/init.d/stunnel4 start

แก้ไขไฟล์ /etc/default/syslog-ng

SYSLOG_NG_OPTIONS=”-m 0-r -t 61514“

เริ่ม syslog-ng

/etc/init.d/syslog-ng restart

ทดสอบ

netstat-an| grep 514

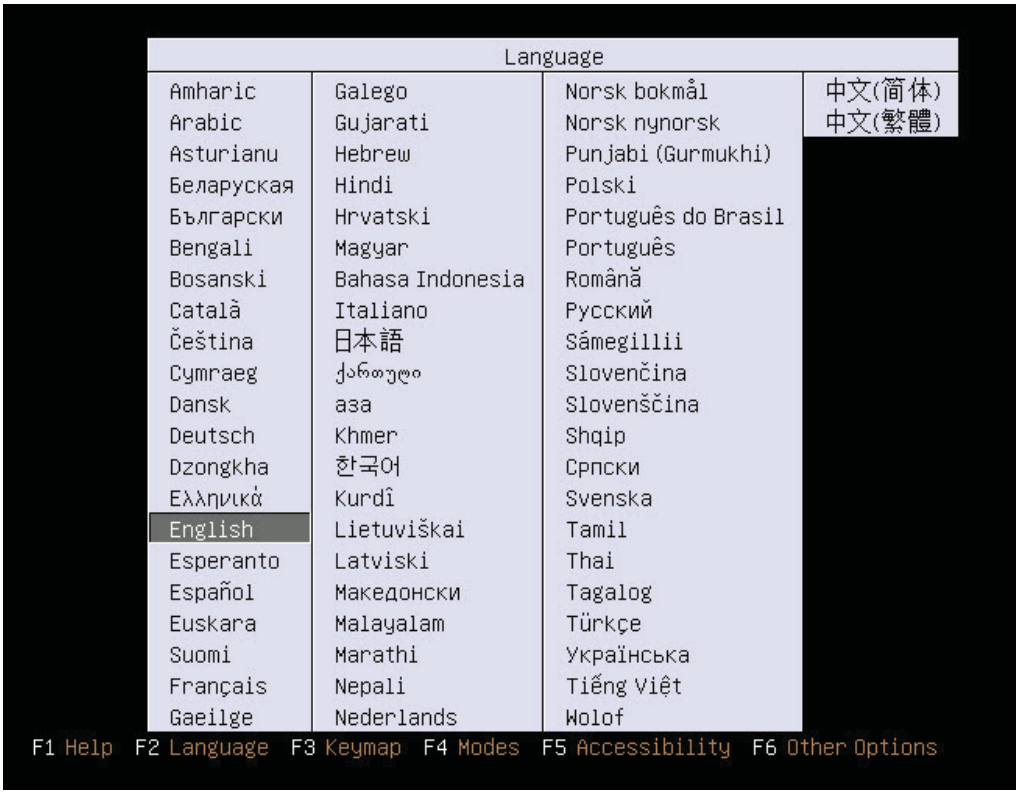
tcp0 0 0.0.0.0:60514 0.0.0.0:* LISTEN

tcp0 0 0.0.0.0:61514 0.0.0.0:* LISTEN

ภาคผนวก ง
ขั้นตอนการติดตั้ง ubuntu

ขั้นตอนการติดตั้ง Ubuntu 9.10

1. ใส่แผ่นซีดี เลือกบูทจาก CDROM เลือกภาษาเป็น English ดังภาพที่ 74

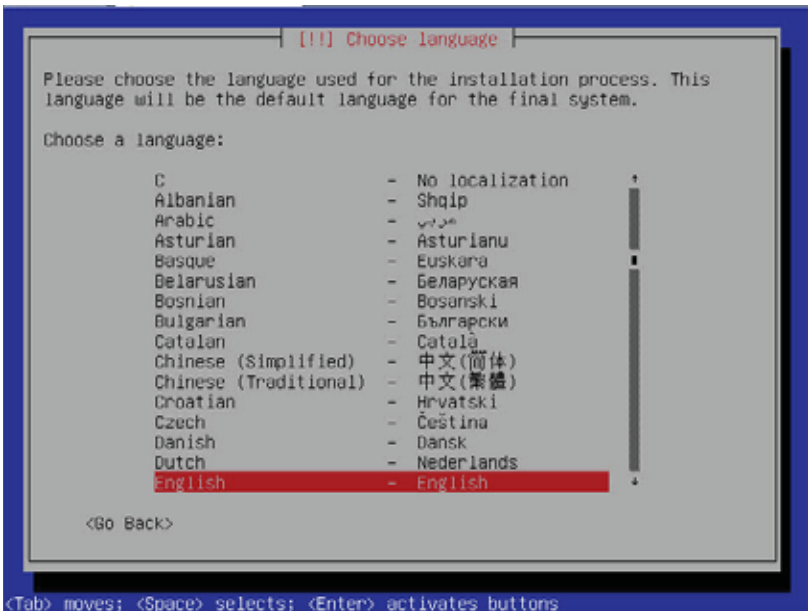


ภาพที่ 74 การบูทจาก CDROM

2. เลือกประเภทการติดตั้งเป็น Install Ubuntu Server ดังภาพที่ 75

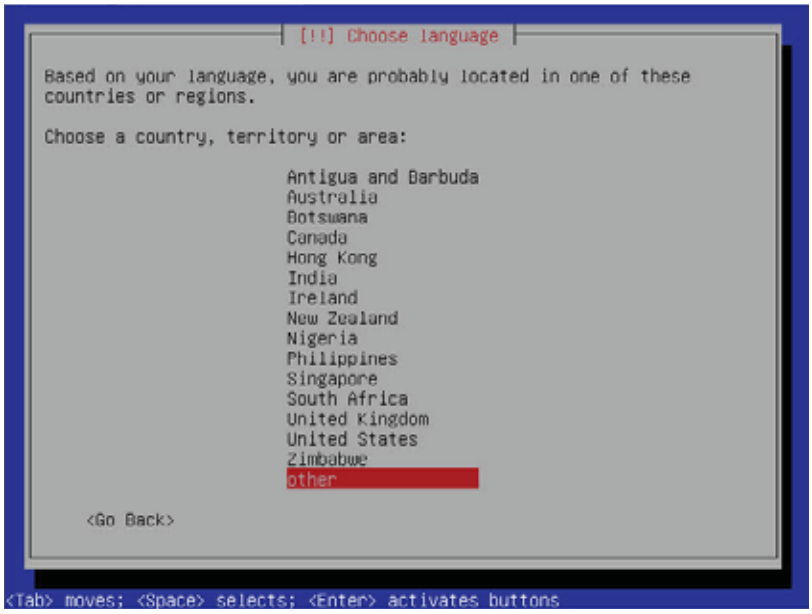
ภาพที่ 75 เลือกประเภทการติดตั้ง

3. เป็นการเลือกภาษาที่ใช้สำหรับการติดตั้ง เป็น English ดังภาพที่ 76



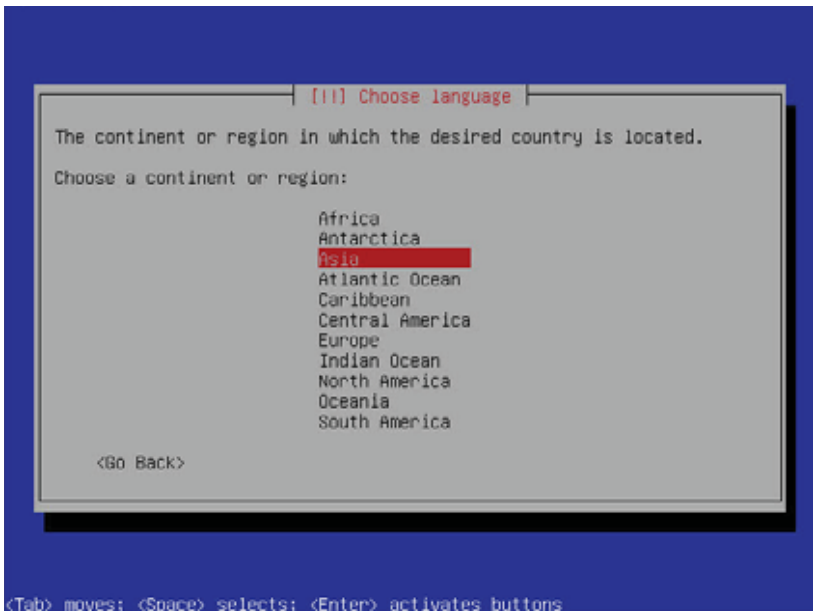
ภาพที่ 76 แสดงภาษาที่เลือก

4. เลือก ประเทศ สำหรับติดตั้งเป็น Other ดังภาพที่ 77 เนื่องจากไม่มี Thailand



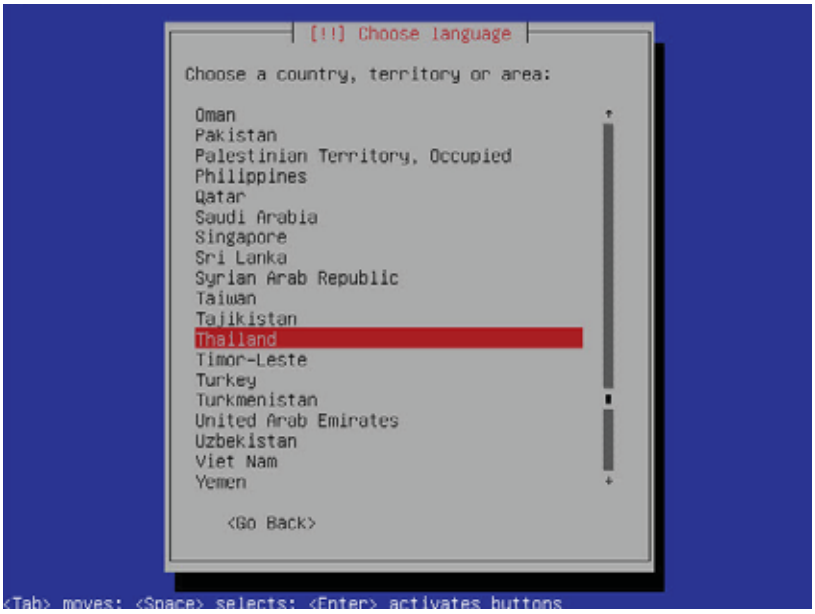
ภาพที่ 77 แสดงประเทศที่เลือก

5. เลือก Region เป็น Asia ดังภาพที่ 78



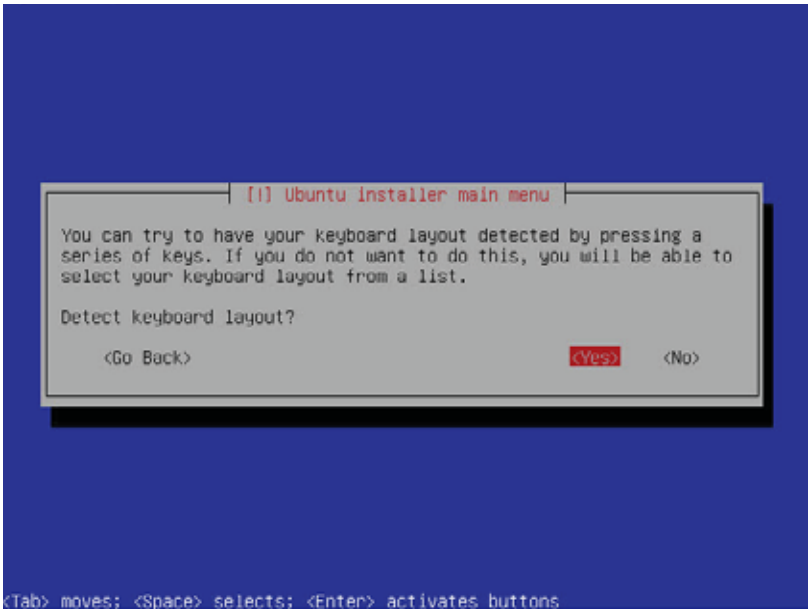
ภาพที่ 78 แสดงการเลือก Region เป็น Asia

6. เมื่อเลือก Region เป็น Asia จะปรากฏ country ให้เลือก Thailand ดังภาพที่ 79



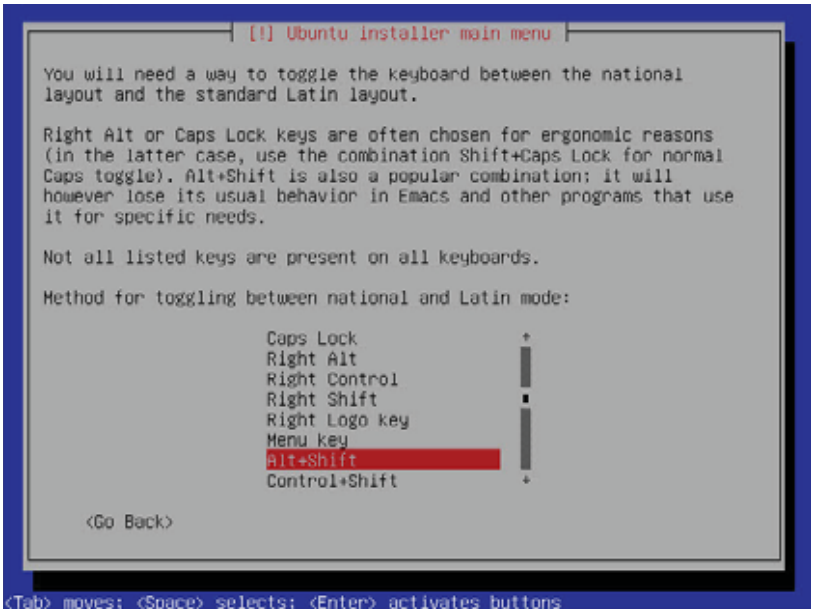
ภาพที่ 79 แสดงการเลือกประเทศไทย

7. ระบบติดตั้งจะตรวจสอบ keyboard layout เลือก Yes ดังภาพที่ 80



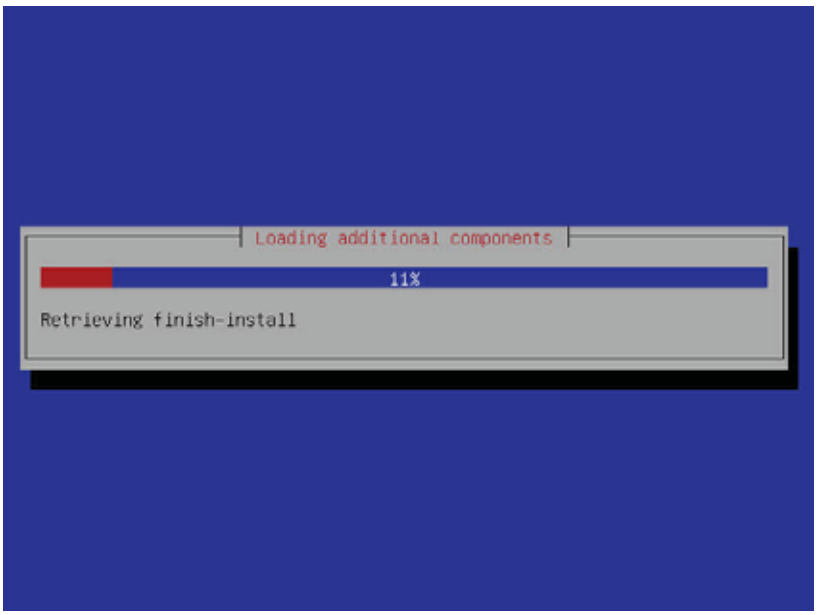
ภาพที่ 80 แสดงการกำหนดการทำงานของคีย์บอร์ด

8. กำหนดให้เลือกปุ่มสลับภาษา กด Alt+Shift ดังภาพที่ 81



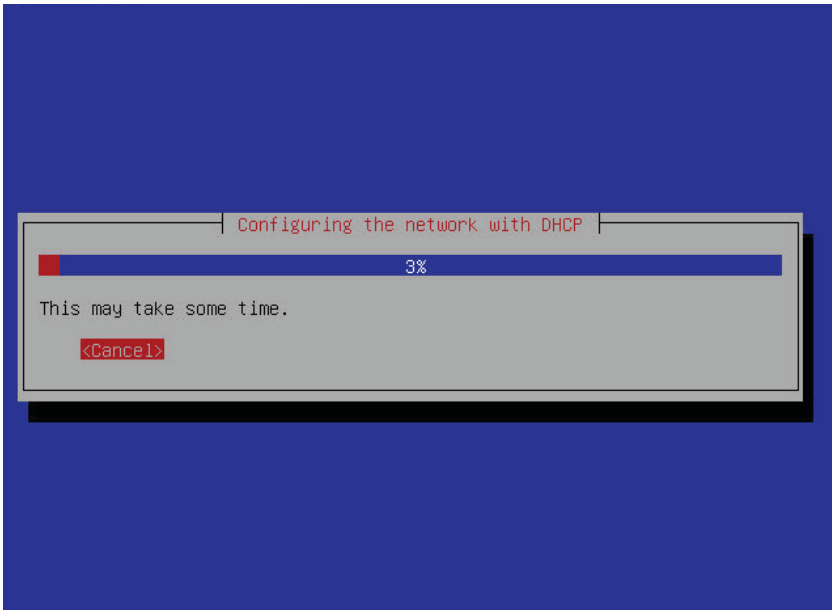
ภาพที่ 81 แสดงการเลือกปุ่มสลับภาษา

9. ระบบจะดำเนินการติดตั้ง Component ดังภาพที่ 82



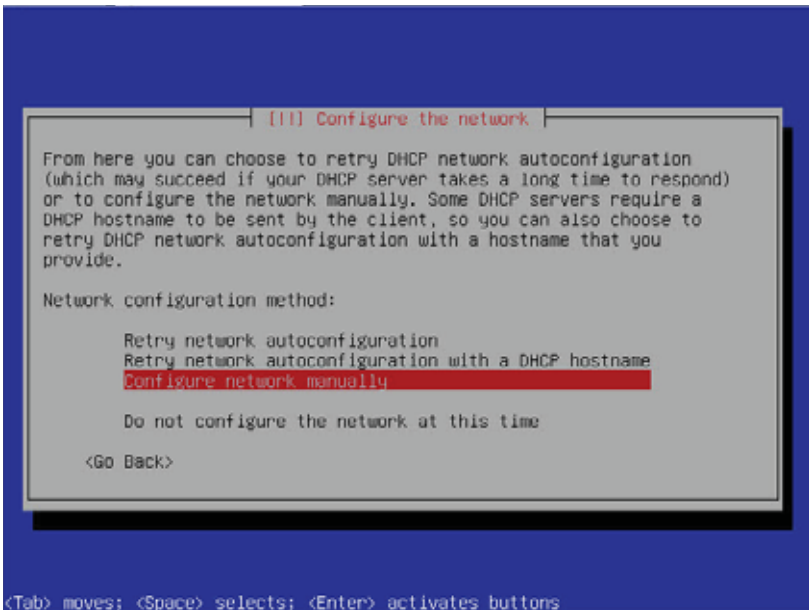
ภาพที่ 82 แสดงเปอร์เซ็นต์การติดตั้ง

10. ระบบจะดำเนินการติดตั้ง โดยค้นหา DHCP ให้เลือก Cancel ดังภาพที่ 83



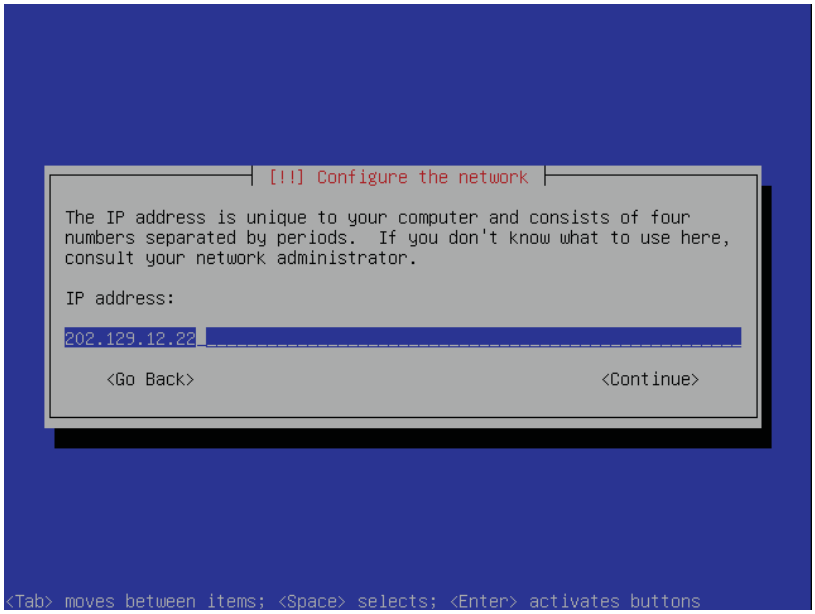
ภาพที่ 83 แสดงการยกเลิกการติดตั้ง DHCP

12. เลือก Configure network manually ดังภาพที่ 84



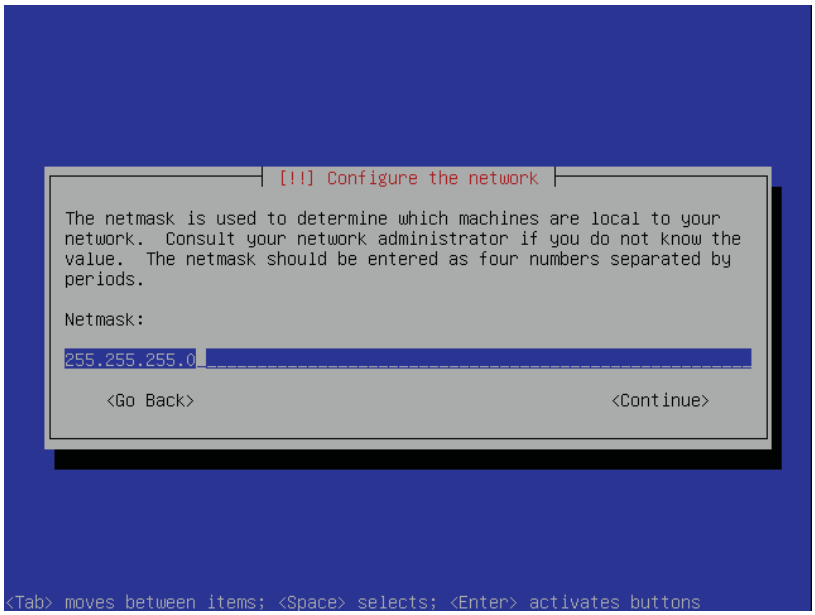
ภาพที่ 84 แสดงการเลือกตั้งค่าระบบแบบกำหนดเอง

13. ใส่หมายเลขไอพีแอดเดรส เครื่องเซิร์ฟเวอร์ ดังภาพที่ 85



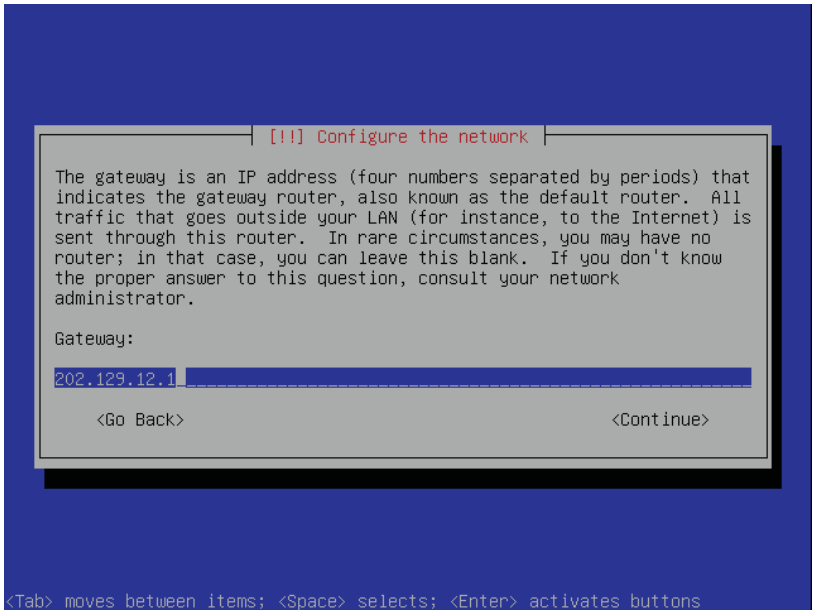
ภาพที่ 85 กำหนดค่าไอพีแอดเดรส สำหรับเครื่องเซิร์ฟเวอร์

14. ใส่หมายเลข Netmask IP ของ Network ดังภาพที่ 86



ภาพที่ 86 แสดงการใส่หมายเลข Netmask IP

15. ใส่หมายเลข IP ที่เป็น Gateway ของ Network ดังภาพที่ 87

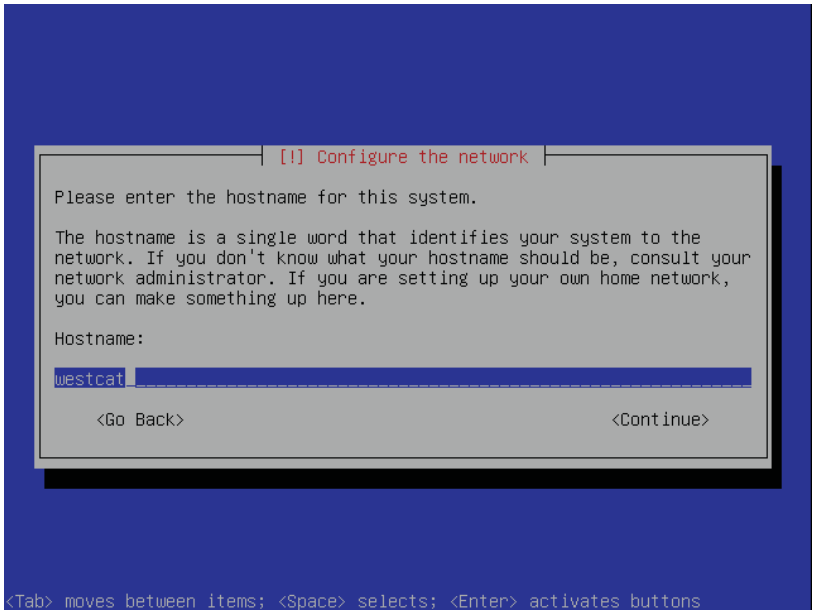


ภาพที่ 87 แสดงการใส่หมายเลข Gateway IP

16. ใส่หมายเลข IP ที่เป็น DNS Server ของ Network ดังภาพที่ 88

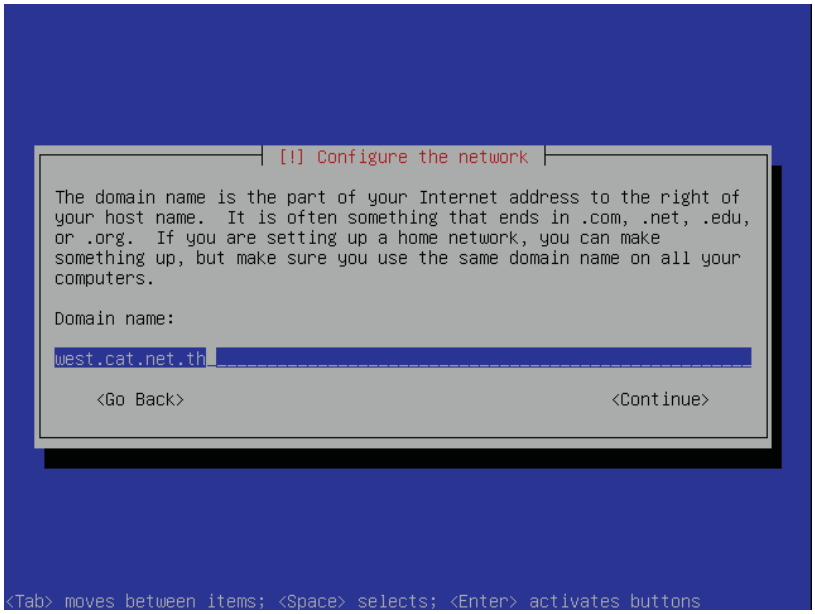
ภาพที่ 88 แสดงการใส่หมายเลข IP ของ DNS Server

17. ใส่ชื่อ Hostname ของ Server ดังภาพที่ 89



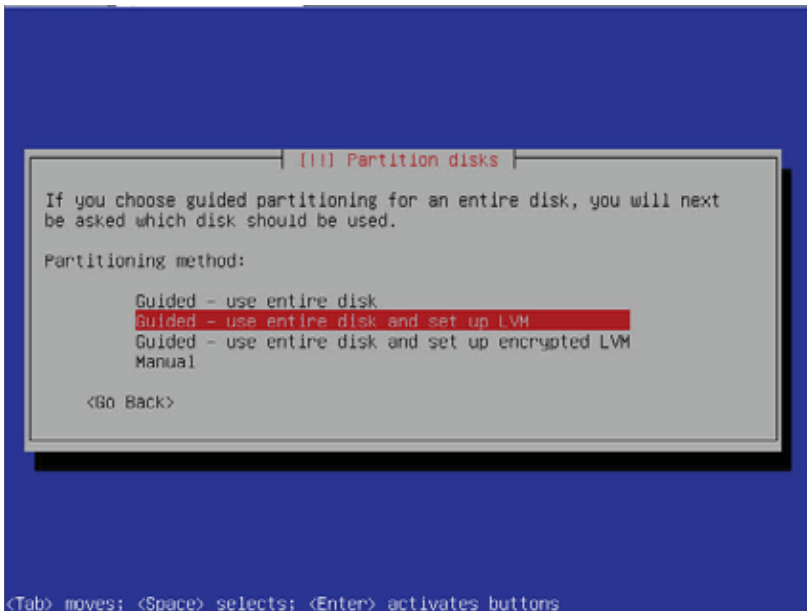
ภาพที่ 89 แสดงการใส่ชื่อ Hostname ของ Server

18. ใส่ชื่อ Domain name ของ Server ดังภาพที่ 90



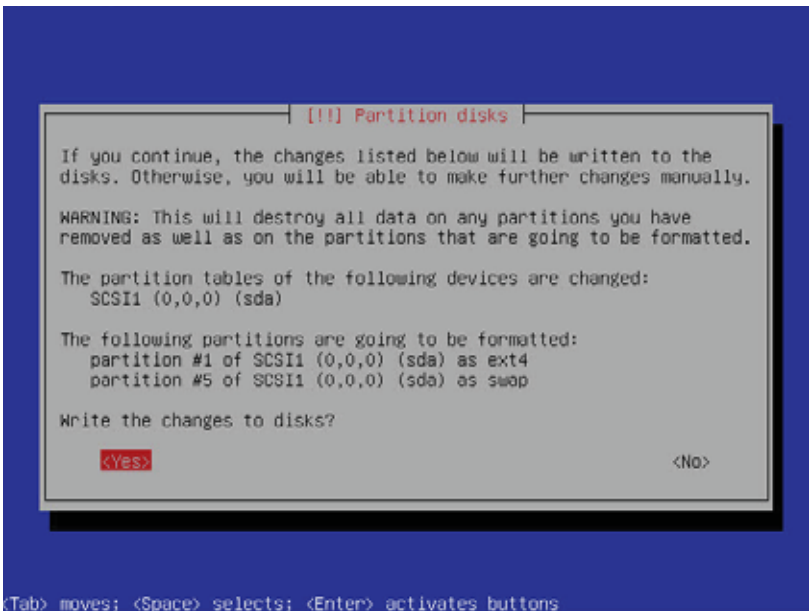
ภาพที่ 90 แสดงการใส่ชื่อ Domain name ของ Server

19. Partition disks กำหนดตามค่า default เลือก Guided-use entire disk and set up LVM ดังภาพที่ 91



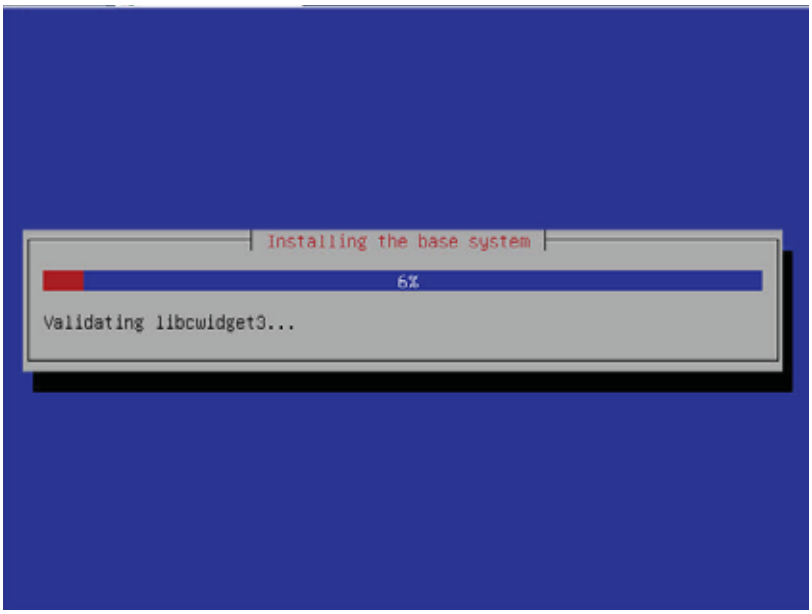
ภาพที่ 91 แสดงการเลือกการแบ่ง Partition

20. เมื่อระบบทำการแบ่ง Partition disks เรียบร้อยแล้ว เลือก Yes บันทึกการเปลี่ยนแปลง Partition disks ดังภาพที่ 92



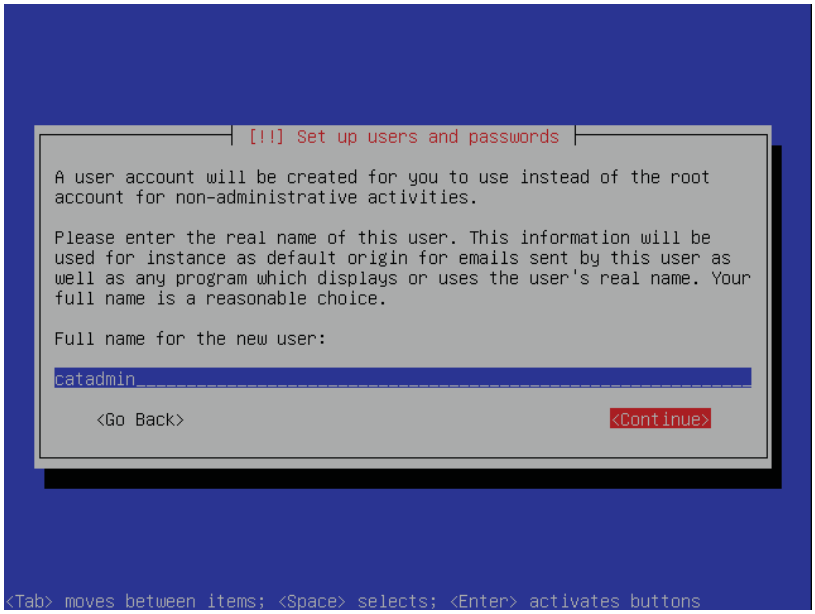
ภาพที่ 92 แสดงการเลือกเพื่อให้บันทึกข้อมูล

21. เมื่อคลิกบันทึกข้อมูล ระบบจะดำเนินการ Install ดังภาพที่ 93



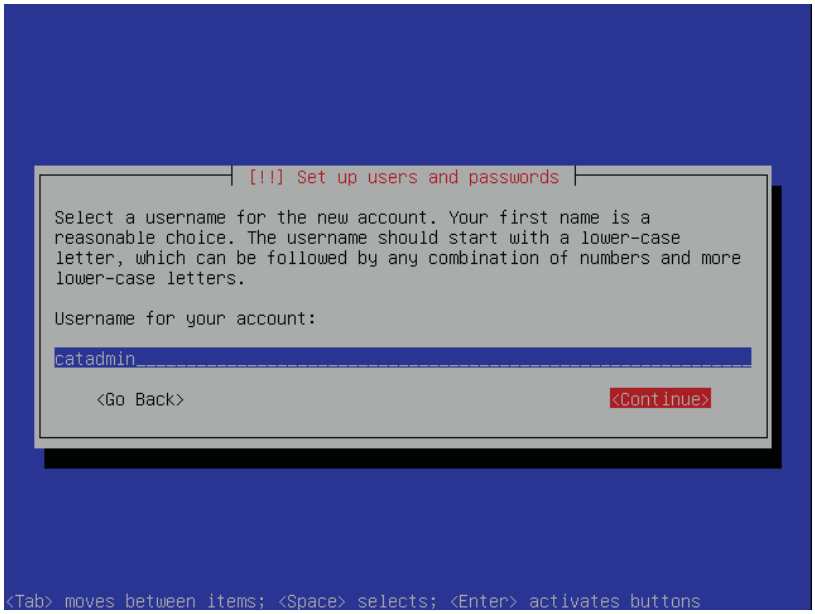
ภาพที่ 93 แสดงสถานะ การติดตั้งระบบ

22. กำหนดชื่อ Full name for new user ดังภาพที่ 94



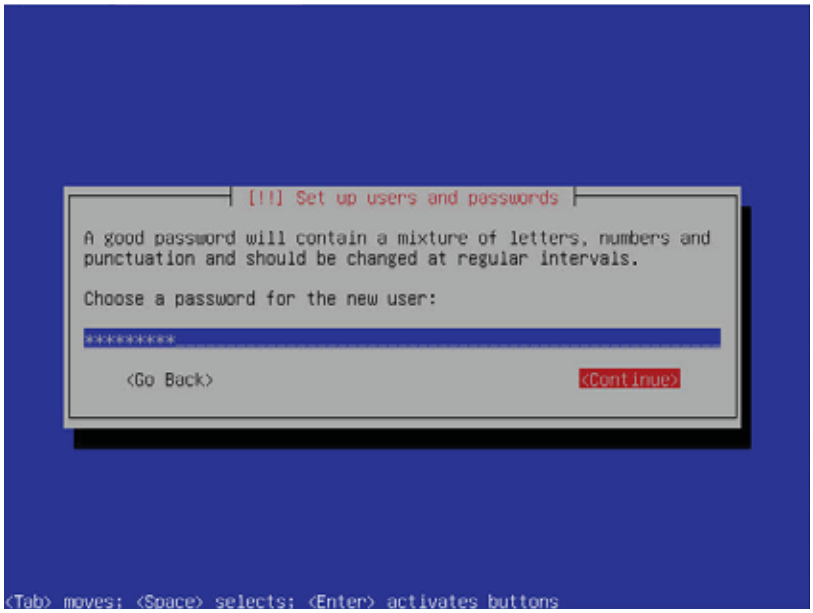
ภาพที่ 94 แสดงการกำหนดชื่อผู้ที่จะเข้าใช้ระบบ

23. กำหนด Username เพื่อเข้าระบบ ดังภาพที่ 95



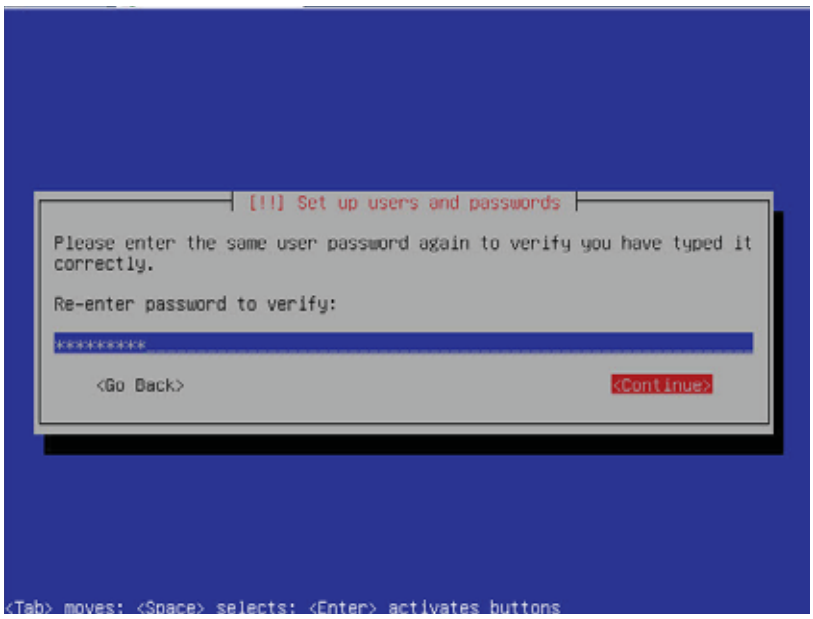
ภาพที่ 95 แสดงการกำหนด Username

24. กำหนด Password สำหรับ User ดังภาพที่ 96



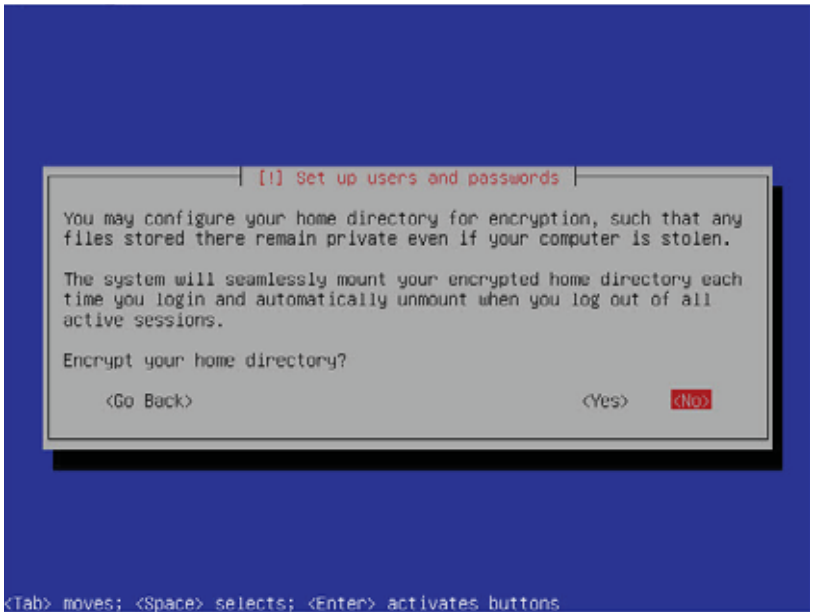
ภาพที่ 96 แสดงการกำหนด Password

25. ยืนยัน Password อีกครั้ง ดังภาพที่ 97



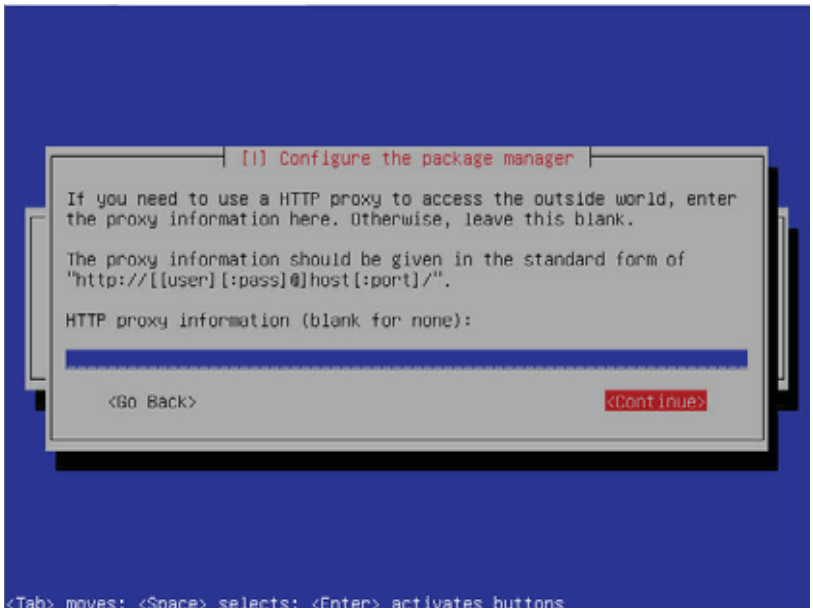
ภาพที่ 97 แสดงการยืนยัน Password อีกครั้ง

26. ระบบจะสอบถามยืนยันการ Encrypt ให้เลือก No ดังภาพที่ 98



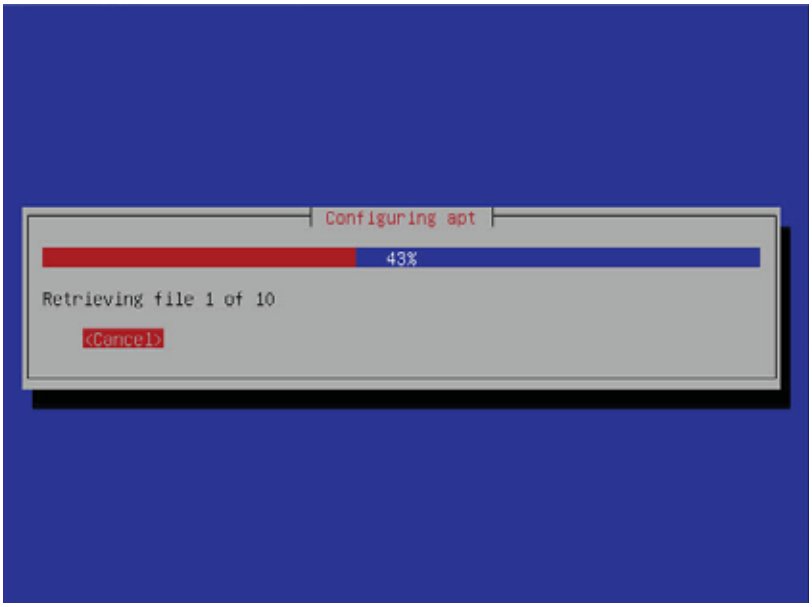
ภาพที่ 98 กำหนดค่าไม่ต้องเข้ารหัส

27. HTTP Proxy คลิกเลือก Continue ดังภาพที่ 99



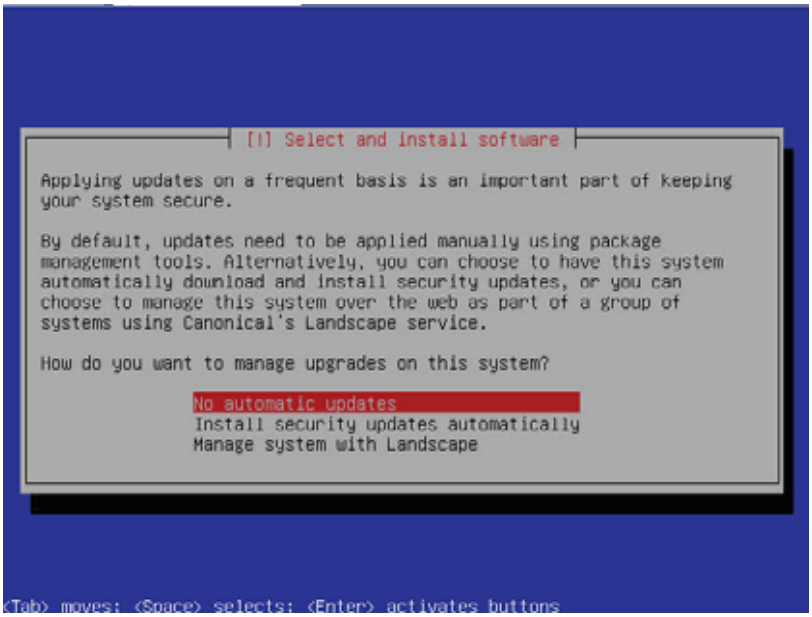
ภาพที่ 99 แสดงการให้ระบบติดตั้ง Proxy

28. ระบบจะติดตั้งค่า config ต่าง ๆ ดังภาพที่ 100



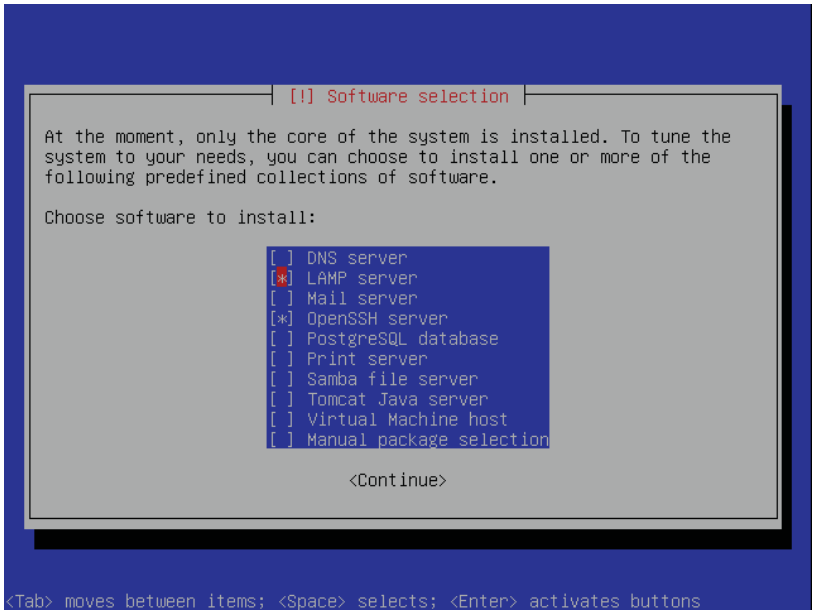
ภาพที่ 100 แสดงเปอร์เซ็นต์การติดตั้งค่า config

29. เลือก No automatic updates เพื่อต้องการปรับปรุงเอง ดังภาพที่ 101



ภาพที่ 101 แสดงการเลือกคำสั่ง No automatic updates

30. เลือก software install เป็น LAMP server , OpenSSH server ดังภาพที่ 102

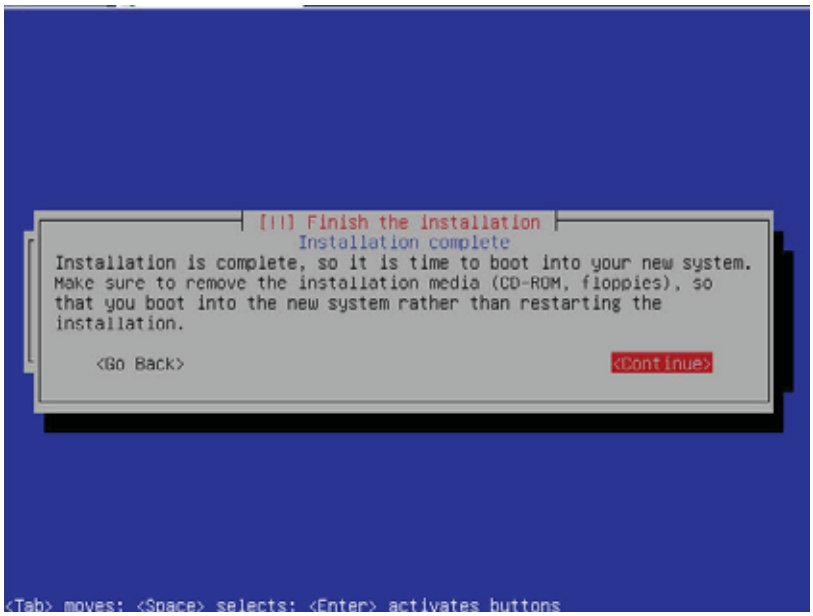


ภาพที่ 102 แสดงการเลือกซอต์ฟแวร์ที่จะติดตั้ง

31. ระบบจะติดตั้ง software ที่เลือกลง Server ดังภาพที่ 103

ภาพที่ 103 แสดงเปอร์เซ็นต์การติดตั้งซอร์ฟแวร์

32. เมื่อติดตั้งเสร็จสิ้น ระบบจะแจ้งให้นำแผ่น CD-ROM ออกและคลิก Continue เพื่อ Reboot เครื่อง ดังภาพที่ 104



ภาพที่ 104 แสดงการติดตั้งแล้วเสร็จ และให้ Reboot

ประวัติผู้วิจัย

ชื่อ-สกุล	นางทิพย์ศริน พรปิติเจริญ
ที่อยู่	70 ถ.ริมคลองวัดพระงาม ต.พระปฐมเจดีย์ อ.เมือง จ.นครปฐม 73000
ที่ทำงาน	สำนักงานบริการลูกค้า กสท เขตตะวันตก
	บริษัท กสท โทรคมนาคมจำกัด (มหาชน)
	162 หมู่ 4 ถ.เพชรเกษม ต.โคกหม้อ อ.เมือง จ.ราชบุรี 70000

ประวัติการศึกษา

พ.ศ. 2530	สำเร็จการศึกษาระดับปริญญาตรี คณะบริหารธุรกิจ
	วิทยาลัยเทคโนโลยีและอาชีวศึกษา
พ.ศ. 2549	ศึกษาต่อระดับปริญญามหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
	มหาวิทยาลัยศิลปากร

ประวัติการทำงาน

พ.ศ. 2530	พนักงานปฏิบัติการโทรคมนาคมระดับ 2 การสื่อสารแห่งประเทศไทย
พ.ศ. 2540	พนักงานปฏิบัติการโทรคมนาคม ระดับ 7
	สำนักงานบริการลูกค้า กสท นครปฐม
พ.ศ. 2549	ผู้บริหารระดับ 8 ส่วนการตลาด
	สำนักงานบริการลูกค้า กสท เขตตะวันตก