

ชื่อโครงการ ระบบบันทึกและจัดการข้อมูลผู้ใช้เครือข่าย

Network Users Logging and Management System

ผู้จัดทำ นายจักรภูมิ มณีรัตน์ รหัส 5410110069

สาขาวิชา วิศวกรรมคอมพิวเตอร์

ปีการศึกษา 2559

อาจารย์ที่ปรึกษาโครงการ

.....

(อาจารย์รัชชัย เอ็งฉ้วน)

คณะกรรมการสอบ

.....

(รศ.ดร.สินชัย กมลวิวงศ์)

.....

(รศ.ทศพร กมลวิวงศ์)

.....

(อาจารย์สุธน แซ่ว่อง)

โครงการนี้เป็นส่วนหนึ่งของรายวิชา Computer Engineering Project I-II ตามหลักสูตรปริญญา
วิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมคอมพิวเตอร์ มหาวิทยาลัยสงขลานครินทร์

.....

(ผศ.ดร. วรณรัช สันติอมรทัต)

หัวหน้าภาควิชาวิศวกรรมคอมพิวเตอร์

หนังสือรับรองความเป็นเอกลักษณ์

ผู้จัดทำที่ได้ลงนามทำนี้ ขอรับรองว่ารายงานฉบับนี้เป็นรายงานที่มีความเป็นเอกลักษณ์ โดยที่ผู้จัดทำไม่ได้มีการคัดลอกมาจากที่ใดเลย เนื้อหาทั้งหมดถูกรวบรวมจากการพัฒนาในขั้นตอนต่าง ๆ ของการจัดทำโครงการ หากมีส่วนใดที่จำเป็นต้องนำเอาข้อความจากผลงานของผู้อื่น หรือบุคคลอื่นใดที่ไม่ใช่ตัวข้าพเจ้า ข้าพเจ้าได้ทำอ้างอิงถึงเอกสารเหล่านั้นไว้อย่างเหมาะสม และขอรับรองว่ารายงานฉบับนี้ไม่เคยเสนอต่อสถาบันใดมาก่อน

ผู้จัดทำ

(นายจักรภูมิ มณีรัตน์)

โครงการนี้สำเร็จลงได้ด้วยความช่วยเหลือจาก อาจารย์รัชชัย เอ็งฉ้วน อาจารย์ที่ปรึกษาโครงการที่ได้ให้แนวคิด คำปรึกษา คำแนะนำ และข้อเสนอแนะ ตลอดจนแนวทางในการแก้ปัญหาและอุปสรรค ตั้งแต่เริ่มต้นจนโครงการเล่มนี้เสร็จสมบูรณ์ ผู้จัดทำจึงขอกราบขอบพระคุณเป็นอย่างสูง

ขอขอบพระคุณ รศ.ดร.สินชัย กมลวิวงศ์ รศ.ทศพร กมลวิวงศ์ และอาจารย์สุธน แซ่ว่อง คณะกรรมการสอบโครงการที่กรุณาให้คำปรึกษา ข้อเสนอแนะ คำแนะนำ และตรวจทานโครงการให้ดำเนินไปอย่างสมบูรณ์

ขอบพระคุณคณาจารย์ภาควิชาวิศวกรรมคอมพิวเตอร์ และคณาจารย์ทุกท่านที่ได้ประสิทธิ์ประสาทวิชาความรู้ สามารถนำความรู้ที่มีไปใช้ในการแก้ไขปัญหาจนสำเร็จลงเป็นอย่างดี

ขอบคุณเพื่อนๆ พี่ๆ น้องๆ ที่คอยให้ความช่วยเหลือ คำปรึกษา และกำลังใจเสมอมา

สุดท้ายนี้ ขอระลึกถึงพระคุณบิดามารดาที่ได้เลี้ยงดูอบรมสั่งสอนจนเติบโตใหญ่ ส่งเสริมสนับสนุน ให้คำแนะนำ คำปรึกษา และเป็นกำลังใจในการดำเนินงานเสมอมา

นายจักรภูมิ มณีรัตน์

ผู้จัดทำ

ปัจจุบันการใช้งานและเข้าถึงอินเทอร์เน็ตสามารถกระทำได้อย่างอิสระและเสรีมากขึ้น จึงมีโอกาสเกิดการกระทำผิดทางอินเทอร์เน็ตได้ทุกเมื่อไม่ว่าเจตนาหรือไม่ก็ตาม ดังนั้นจึงมีการออกกฎหมาย พรบ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ขึ้น โดย ผู้ให้บริการ ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า 90 วันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกิน 90 วันแต่ไม่เกิน 1 ปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้ ซึ่งระบบและเครื่องมือในส่วนของการระบุตัวตนในปัจจุบันบางระบบรองรับการทำงานในระบบ IPv4 แต่ยังไม่รองรับระบบ IPv6 โครงการนี้จึงคิดนำข้อมูล MAC Address (Physical Address) IPv4 และ IPv6 จาก Layer3 Switch ซึ่ง Layer3 Switch มีการเก็บไว้แล้วมาใช้ประโยชน์ ในการช่วยระบุตัวตน เพื่อทราบถึงชื่อผู้ใช้ และเก็บข้อมูลการใช้งานไว้เพื่อประโยชน์ในการระบุผู้กระทำความผิดได้ หากเกิดการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ต่อไป ขณะเดียวกันสามารถนำข้อมูลที่ได้นำไปใช้ทำสถิติ เพื่อวิเคราะห์การใช้งานของผู้ใช้งานของผู้ใช้ได้

Nowadays, to access the Internet can be performed easier than the past. People also can make Internet crime both with or without intention. so Computer-related Crime Act B.E 2550 (2007) was legislated. in Section 26 that says “A service provider must store computer traffic data for at least ninety days from the date on which the data is input into a computer system. However, if necessary, a competent official may instruct a service provider to store data for a period of longer than ninety days but not exceeding one year on a special case by case basis or on a temporary basis.”.

At the present time, some system and tools in the part of identification support IPv4 system, but still not support in IPv6 So, this project trying to use MAC Address, IPv4 and IPv6 from Layer3 Switch with data of radius server to identify user for benefit of identify who make Internet crime, and also use data to analyses statistic of using data too.

1. บทนำ.....	1
1.1 ความสำคัญและที่มาของโครงการ.....	1
1.2 วัตถุประสงค์.....	2
1.3 ประโยชน์ที่คาดว่าจะได้รับ.....	2
1.4 ขอบเขตของโครงการ.....	2
2. ทฤษฎีและหลักการ.....	3
2.1 IP (Internet Protocol) [10]	3
2.2 ARP (Address Resolution Protocol) [9]	3
2.3 IPv6 (Internet protocol version 6) [1,7].....	3
2.4 Neighbor Discovery Protocol [7].....	4
2.5 Layer3 Switch [2,5,6].....	4
2.6 SNMP [4,8].....	5
2.7 ภาษา PERL [3].....	5
2.8 Apache Webserver [12].....	5
2.9 SQL [11].....	6
2.10 mySQL [11].....	6
2.11 ภาษา PHP [12]	7
2.12 RADIUS [15].....	8
2.13 FreeRADIUS [14].....	8
2.14 หลักการทำงานเบื้องต้นของโครงการ.....	8
3. ระเบียบวิธีวิจัย	12

3.1 แนวคิดในการออกแบบระบบ	12
3.2 ระบบที่ได้ออกแบบ.....	15
3.2.1 การทำงานของส่วนสรีปต์ สำหรับเรียกข้อมูลจาก Layer3 Switch	16
3.2.2 การออกแบบส่วนฐานข้อมูล	18
3.2.3 ส่วนของเว็บไซต์ที่แสดงข้อมูล.....	19
3.3 การทดสอบระบบ	19
4. ผลและวิเคราะห์ผลการทดลอง.....	20
4.1 การทดสอบการจำลองระบบลงชื่อเข้าใช้.....	20
4.2 การทดสอบระบบส่วนเบื้องหลัง.....	20
4.3 การทดสอบระบบส่วนฐานข้อมูล.....	22
4.4 การทดสอบระบบในส่วนแสดงผล	23
5. สรุปผลและข้อเสนอแนะ	26
5.1 สรุปผล.....	26
5.2 ปัญหาและอุปสรรคและวิธีแก้ไข	26
5.3 ข้อเสนอแนะ	27
6. เอกสารอ้างอิง	28
7. ภาคผนวก	I
7.1 วิธีการติดตั้ง.....	I
3.2.4 7.1.1 ติดตั้ง LAMP stack และ phpMyAdmin	I
3.2.5 7.1.2.สร้างฐานข้อมูล	IV
3.2.6 7.1.3.ติดตั้ง screen	VI
3.2.7 7.1.4.คัดลอกไฟล์ webservice	VI
3.2.8 7.1.5.การตั้งค่าเพื่อใช้งานโปรแกรม	VII

3.2.9	7.1.6.การสั่งรันโปรแกรม.....	VII
7.2	คู่มือการใช้งาน.....	VIII
3.2.10	7.2.1. การใช้งานของผู้ใช้ทั่วไป	VIII
3.2.11	7.1.2. การใช้งานของผู้ดูแลระบบ.....	XII

รูปที่ 2-1 หมายเลข IP Address ของเครื่องตัวอย่าง.....	9
รูปที่ 2-2 ข้อมูลบางส่วนจากรางงานสถิติการใช้งาน ของ firewall ของมหาวิทยาลัยสงขลานครินทร์ ในส่วน ของ Risky Users ประจำวันที่ 26 กันยายน พ.ศ.2557	9
รูปที่ 2-3 การเชื่อมต่อ Log Server กับเครือข่าย.....	10
รูปที่ 2-4 use case diagram ของผู้ใช้ทั่วไป	11
รูปที่ 2-5 use case diagram ของผู้ดูแลระบบ	11
รูปที่ 3-1 Layer3 Switch.....	12
รูปที่ 3-2 แนวคิดการทำงานของระบบระบุตัวตน.....	12
รูปที่ 3-3 ตัวอย่างข้อมูลที่ได้จาก ARP.....	13
รูปที่ 3-4 ตัวอย่างข้อมูลที่ได้จาก ND	13
รูปที่ 3-5 ตัวอย่างข้อมูลที่ได้จาก radius server.....	14
รูปที่ 3-6 แนวทางการเก็บข้อมูล	14
รูปที่ 3-7 ภาพรวมระบบที่ได้ออกแบบ	15
รูปที่ 3-8 ส่วนประกอบหลักของโครงงาน.....	15
รูปที่ 3-9 flowchart แสดงการทำงานของสคริปต์ สำหรับเรียกข้อมูลจาก Layer3 Switch	17
รูปที่ 3-10 ER-Diagram ของฐานข้อมูลที่ของระบบ.....	18
รูปที่ 4-1 การลงชื่อเข้าใช้ของระบบที่จำลองขึ้น	20
รูปที่ 4-2 ตัวอย่างไฟล์การตั้งค่าช่วงเวลาการตรวจสอบ.....	20
รูปที่ 4-3 ผลลัพธ์จากการทดสอบ โดยยังไม่ได้นำไปจับคู่กับข้อมูลผู้ใช้	21
รูปที่ 4-4 ตัวอย่าง log ของ RADIUS server ที่มาจากการยืนยันตัวตนในระบบ	22
รูปที่ 4-5 ข้อมูลที่ถูกเพิ่มจากสคริปต์จากการเรียกข้อมูลจาก L3 Switch.....	22

รูปที่ 4-6 แสดงส่วนของเว็บสำหรับการเข้าสู่ระบบ.....	24
รูปที่ 4-7 แสดงส่วนของเว็บสำหรับการดูบันทึกการใช้งานในมุมมองผู้ใช้ทั่วไป.....	24
รูปที่ 4-8 แสดงส่วนของเว็บสำหรับการดูบันทึกการใช้งานในมุมมองผู้ดูแลระบบ	25
รูปที่ 4-9 แสดงส่วนของเว็บสำหรับการสำรองข้อมูลผู้ใช้ในมุมมองผู้ดูแลระบบ	25
รูปที่ 7-1 ตัวอย่างการทดสอบการทำงานของ Apache.....	I
รูปที่ 7-2 การติดตั้ง mysql.....	II
รูปที่ 7-3 การทดสอบการทำงานของ php.....	III
รูปที่ 7-4 การติดตั้ง phpMyAdmin	V
รูปที่ 7-5 การติดตั้ง phpMyAdmin	V
รูปที่ 7-6 แสดงเว็บของ phpMyAdmin	VI
รูปที่ 7-7 แสดงเว็บในส่วนของการลงชื่อเข้าใช้ของระบบ	VII
รูปที่ 7-8 ส่วนการตั้งค่าการเชื่อมต่อฐานข้อมูล	VII
รูปที่ 7-9 ส่วนแสดงข้อมูลผู้ใช้ในมุมมองผู้ใช้ทั่วไป.....	VIII
รูปที่ 7-10 ผลลัพธ์การกรองข้อมูล	IX
รูปที่ 7-11 ตัวอย่างข้อมูลพร้อมพิมพ์ในรูปแบบนามสกุล .pdf	X
รูปที่ 7-12 ส่วนเลือกช่วงเวลาข้อมูลย้อนหลังที่ต้องการพิมพ์.....	XI
รูปที่ 7-13 ตัวอย่างรายงานพร้อมพิมพ์จากเมนู print report.....	XI
รูปที่ 7-14 ส่วนแสดงข้อมูลผู้ใช้ในมุมมองผู้ดูแลระบบ.....	XII
รูปที่ 7-15 ตัวอย่างข้อมูลพร้อมพิมพ์ในรูปแบบนามสกุล .pdf	XIII
รูปที่ 7-16 ส่วนสำหรับเลือกช่วงเวลาข้อมูลย้อนหลังที่ต้องการพิมพ์	XIV
รูปที่ 7-17 ตัวอย่างรายงานพร้อมพิมพ์จากเมนู print report.....	XIV
รูปที่ 7-18 ส่วนของเมนู backup and restore data	XV
รูปที่ 7-19 ตัวอย่างการสำรองข้อมูล	XV

รูปที่ 7-20 แสดงส่วนของเมนู clean old data.....	XVI
รูปที่ 7-21 แสดงส่วนยืนยันการลบข้อมูลที่มีอายุมากกว่า 2 ปี	XVII
รูปที่ 7-22 แสดงส่วนการยืนยันการลบข้อมูลที่มีอายุมากกว่า 90 วัน.....	XVII

ตารางที่ 4- 1 ตาราง permit จากฐานข้อมูล	23
ตารางที่ 4- 2 ตาราง ipRef จากฐานข้อมูล	23

1. บทนำ

1.1 ความสำคัญและที่มาของโครงการ

ปัจจุบันการใช้งานและเข้าถึงอินเทอร์เน็ตสามารถกระทำได้อย่างอิสระและเสรีมากขึ้น จึงมีโอกาสดังกล่าวทำให้เกิดทางอินเทอร์เน็ตได้ทุกเมื่อไม่ว่าเจตนาหรือไม่ก็ตาม ดังนั้นจึงมีการออกกฎหมาย พรบ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ขึ้น โดยผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า 90 วันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์

ซึ่งระบบและเครื่องมือในส่วนของการระบุตัวตนในปัจจุบันส่วนใหญ่รองรับการทำงานในระบบ Internet Protocol รุ่นที่ 4 (IPv4) แต่ยังไม่รองรับระบบ Internet Protocol รุ่นที่ 6 (IPv6) เนื่องจากมี Protocol ที่เกี่ยวข้องเปลี่ยนไป เช่น Neighbor Discovery Protocol ใน IPv6 เข้ามาทำงานแทน Address Resolution Protocol ใน IPv4 เป็นต้น นอกจากนี้อุปกรณ์หนึ่งชิ้นสามารถมี IP Address ได้มากกว่าหนึ่งหมายเลข และยังมีส่วนที่เป็น Temporary Address เป็น IP Address ชั่วคราวซึ่งสามารถเกิดขึ้นและเปลี่ยนแปลงได้หลังจากการยืนยันตัวตนแล้ว ทำให้ไม่สามารถระบุได้ว่าผู้ใช้หมายเลขนั้นคือบุคคลใด เพราะหากเกิดการเปลี่ยนแปลงในส่วน Temporary Address ขึ้นการกระทำใด ๆ จากหมายเลขดังกล่าวจะไม่สามารถตรวจสอบได้ว่ามาจากผู้ใช้บุคคลใด

อุปกรณ์ Layer3 Switch เป็นอุปกรณ์เลือกเส้นทาง ซึ่งทำงานบน OSI Model ในระดับที่ 3 โดยทำงานระดับแพ็กเก็ต ซึ่งจะมีการเก็บค่า IP Address และ MAC Address ทำให้สามารถนำข้อมูล MAC Address มาเปรียบเทียบกับเพื่อให้ทราบผู้ใช้จากการยืนยันตัวตนจากระบบ IPv4 ได้ ซึ่งอุปกรณ์ Layer3 Switch และอุปกรณ์อื่น ๆ ในปัจจุบัน เช่น Routers, Layer2 Switch, Servers, Workstations , Printers, UPS รองรับการทำงานผ่าน SNMP ทำให้สามารถ ส่งคำสั่งไปยัง Agent gets responses จาก Agents sets ค่าตัวแปรใน Agents และรับข้อมูลเหตุการณ์ต่าง ๆ ที่เกิดขึ้นจาก Agent ได้

ด้วยเหตุผลข้างต้น ผู้จัดทำโครงการจึงคิดที่จะนำข้อมูล MAC Address (Physical Address) IPv4 และ IPv6 จาก Layer3 Switch ผ่านทาง SNMP Protocol มาใช้ในการช่วยระบุตัวตนและเก็บข้อมูลในระบบ IPv6 ทำให้สามารถทราบได้ว่าอุปกรณ์นั้นได้รับ IP Address หมายเลขใดบ้าง ทราบถึงชื่อผู้ใช้ และเก็บข้อมูลการใช้งานไว้เพื่อประโยชน์ในการระบุผู้กระทำความผิดได้ หากเกิดการกระทำความผิดตาม พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ต่อไป ขณะเดียวกันสามารถนำข้อมูลที่ได้นำไปใช้ทำสถิติ เพื่อวิเคราะห์การใช้งานของผู้ใช้งานของผู้ใช้ได้

1.2 วัตถุประสงค์

1. เพื่อเก็บข้อมูลการได้รับ IP Address ทั้ง IPv4 และ IPv6 ของแต่ละอุปกรณ์
2. เพื่อแสดงข้อมูลและช่วยจัดการผู้ใช้ในเครือข่าย
3. เพื่อแก้ไขปัญหาการไม่สามารถระบุตัวตนได้ของ IP Address ในระบบ IPv6

1.3 ประโยชน์ที่คาดว่าจะได้รับ

1. สามารถระบุตัวตนผู้ใช้ในระบบ IPv6 เพื่อช่วยแก้ปัญหาไม่สามารถระบุผู้ใช้งานที่ใช้งานด้วย IPv6 ได้
2. ทำให้ทราบ IP Address ทั้งหมดที่ผู้ใช้แต่ละคนได้รับ เพื่อเป็นข้อมูลในการบริหารจัดการเครือข่าย

1.4 ขอบเขตของโครงการ

1. สามารถเก็บข้อมูล IP Address ของอุปกรณ์ที่ใช้งานผ่าน Layer3 Switch ที่ Log Server เชื่อมต่ออยู่ได้
2. สามารถแสดงข้อมูล IP Address และข้อมูลการลงชื่อเข้าใช้ของอุปกรณ์ ที่ใช้งานผ่าน Layer3 Switch ที่ Log Server เชื่อมต่ออยู่ได้
3. สามารถระบุตัวตนผู้ใช้ในระบบเครือข่ายได้ทั้ง IPv6 และ IPv4 ที่ใช้งานผ่าน Layer3 Switch ที่ Log Server เชื่อมต่ออยู่ได้

2. ทฤษฎีและหลักการ

2.1 IP (Internet Protocol) [10]

IP (Internet Protocol) คือข้อกำหนดซึ่งประกอบด้วยกฎต่าง ๆ สำหรับรูปแบบการสื่อสารที่ใช้ในการส่งข้อมูลจากเครื่องคอมพิวเตอร์เครื่องหนึ่งไปยังเครื่องอื่นในอินเทอร์เน็ต (Internet) คอมพิวเตอร์แต่ละเครื่อง บนอินเทอร์เน็ตต้องมีที่อยู่อย่างน้อยหนึ่งที่อยู่ (address) ซึ่งไม่ซ้ำกับคอมพิวเตอร์เครื่องอื่นในอินเทอร์เน็ต เมื่อมีการส่งและรับข้อมูล (เช่น อี-เมล) ข้อความจะถูกแบ่งเป็นชุดข้อมูลเรียกว่า แพ็กเก็ต (Packet) แต่ละชุดจะเก็บที่อยู่ของผู้ส่งและผู้รับ การส่งชุดข้อมูลจะส่งไปที่เครื่องคอมพิวเตอร์ที่เป็น Gateway เมื่อเครื่อง Gateway อ่านที่อยู่ของปลายทางแล้วจึงส่งต่อชุดข้อมูลไปยังเครือข่ายอินเทอร์เน็ตจนกระทั่งมีเครื่อง Gateway รู้ว่าชุดข้อมูลนั้น เป็นของคอมพิวเตอร์ ภายในกลุ่มใดจากนั้นเครื่อง Gateway จึงจะส่งชุดข้อมูลไปยังเครื่องคอมพิวเตอร์ที่มีอยู่ตามที่ระบุที่ระบุปัจจุบันคือรุ่นที่ 4 (IPv4) และกำลังอยู่ในช่วงผลักดันให้ใช้รุ่นที่ 6 (IPv6)

2.2 ARP (Address Resolution Protocol) [9]

ARP (Address Resolution Protocol) เป็นโปรโตคอลสำหรับการจับคู่ระหว่าง IP Address กับตำแหน่งของอุปกรณ์ในระบบเครือข่าย เช่น IPv4 ใช้การระบุตำแหน่งขนาด 32 บิต ซึ่งเสมือนเป็นชื่อเล่นให้อุปกรณ์จากใน Ethernet ของระบบ และใช้การระบุตำแหน่ง 48 บิต (การระบุตำแหน่งของอุปกรณ์รู้จักในชื่อของ Media Access Control หรือ MAC address) โดยใช้ตาราง ARP เพื่อรักษาการจับคู่ ระหว่าง MAC address กับ IP address โดย ARP ใช้กฎของการสร้างการจับคู่และแปลงตำแหน่งทั้งสองฝ่าย

2.3 IPv6 (Internet protocol version 6) [1,7]

IP Address ส่วนใหญ่ที่ใช้กันทุกวันนี้คือ IPv4 ซึ่งใช้เป็นมาตรฐานในการส่งข้อมูลในเครือข่ายอินเทอร์เน็ตตั้งแต่ปีค.ศ. 1981 ทั้งนี้การขยายตัวของเครือข่ายอินเทอร์เน็ตในช่วงที่ผ่านมา มีอัตราการเติบโตอย่างรวดเร็ว นักวิจัยเริ่มพบว่าจำนวน IP Address ของ IPv4 กำลังจะถูกใช้หมดไป ไม่เพียงพอกับการใช้งานอินเทอร์เน็ตในอนาคตและหากเกิดขึ้นก็หมายความว่าไม่สามารถเชื่อมต่อเครือข่ายเข้ากับระบบอินเทอร์เน็ตเพิ่มขึ้นได้อีก ดังนั้นคณะทำงาน IETF (The Internet Engineering Task Force) ซึ่งตระหนักถึงปัญหาดังกล่าว จึงได้พัฒนา IP รุ่นใหม่ขึ้นคือ IPv6 เพื่อทดแทน IP รุ่นเดิม โดยมีวัตถุประสงค์เพื่อปรับปรุงโครงสร้างของตัวโปรโตคอลให้รองรับหมายเลขแอดเดรสจำนวนมากและปรับปรุงคุณลักษณะอื่น ๆ อีกหลายประการทั้งในแง่ของประสิทธิภาพและความปลอดภัยของระบบแอปพลิเคชัน (application) ใหม่ ๆ ที่จะเกิดขึ้นในอนาคต และเพิ่มประสิทธิภาพในการประมวลผล

แพ็กเก็ต ให้ดีขึ้น ทำให้สามารถตอบสนองต่อการขยายตัวและความต้องการใช้งานเทคโนโลยีบนเครือข่าย อินเทอร์เน็ตในอนาคตได้เป็นอย่างดี

2.4 Neighbor Discovery Protocol [7]

ND อธิบายไว้ใน RFC 4861 ประกอบด้วยชุดของข้อความ ICMPv6 ตัวเลือกของข้อความและกำหนดกระบวนการที่ทำให้โหนดใกล้เคียงค้นพบโหนดอื่น ๆ การค้นพบเราเตอร์บนลิงค์และให้การรองรับสำหรับโฮสต์ที่เปลี่ยนเส้นทาง ND เป็นสิ่งอำนวยความสะดวกที่เข้ามาแทนใน IPv4

- Address Resolution Protocol (ARP)
- ICMP Router Discovery
- ICMP Redirect

2.5 Layer3 Switch [2,5,6]

Layer3 Switch เป็นอุปกรณ์ในการทำ Routing (หาเส้นทางการรับส่งข้อมูลระหว่างเน็ตเวิร์ก) เหมาะสมในการนำไปใช้ในระบบเน็ตเวิร์กที่มีการใช้งาน VLAN (VLAN เป็นการแบ่งพอร์ตต่าง ๆ ที่มีอยู่ใน Layer3 Switch ให้ดูเหมือนว่าแยกกันอยู่คนละเน็ตเวิร์ก) และต้องการให้อุปกรณ์ Computer ที่อยู่ในแต่ละ VLAN สามารถติดต่อกันได้ ซึ่ง Layer3 Switch จะสามารถทำงานได้ในทั้งระดับของ layer2 และ Layer3 แต่เรื่องของการส่งผ่านข้อมูลภายในหรือระหว่าง Switch ด้วยกันนั้นต้องดูว่าเจาะจงไปเฉพาะในส่วนการทำงานของ layer ไหน ซึ่งตรงนี้ก็อยู่ที่ Switch ตัวที่เชื่อมต่ออยู่และ mode ของการทำงานของ Switch ที่ได้ตั้งค่าเอาไว้ ถ้าเป็นการส่งข้อมูลกันในระดับ layer2 ยังคงพิจารณา MAC Address เหมือนเดิม แต่หากเป็นการติดต่อกันในระดับ Layer3 Switch จะพิจารณา IP Address เป็นหลักในด้านของข้อมูลที่ Layer3 Switch จะส่งต่อออกมานั้น ถ้าทำงานในระดับของ Layer2 ก็จะส่งข้อมูลออกมาเป็นเฟรม(Frame) แต่ถ้าทำงานในระดับ Layer3 จะส่งผ่านข้อมูลเป็นลักษณะของแพ็กเก็ตข้อมูล และนอกจากนี้ Layer3 Switch ยังมีความสามารถด้านการ Routing เหมือนกับ เราเตอร์ด้วย (แต่จะต่างกับเราเตอร์ คือ ไม่กันการส่ง broad cast ข้ามเครือข่าย) ซึ่งการส่งข้อมูลในระดับ Layer3 ที่ส่งผ่านข้อมูลเป็นแพ็กเก็ตนั้นจะมีการเก็บข้อมูลความสัมพันธ์ของ IP Address และ MAC Address ในเวลานั้น ๆ ด้วย หรือก็คือจะรองรับ ARP ใน IPv4 และ ND ใน IPv6

2.6 SNMP [4,8]

SNMP ย่อมาจาก Simple Network Management Protocol ซึ่งเป็นโปรโตคอลที่อยู่ระดับบนในชั้นการประยุกต์และเป็นส่วนหนึ่งของชุด Internet Protocol (IP) เครือข่ายอินเทอร์เน็ตที่ใช้โปรโตคอล IP มีอุปกรณ์เครือข่ายหลากหลายชนิดและหลายมาตรฐาน แต่มาตรฐานการจัดการเครือข่ายที่ใช้งานได้ดีและเป็นที่ยอมรับคือ SNMP ในการบริการและจัดการเครือข่ายต้องใช้อุปกรณ์ต่าง ๆ มีส่วนของการทำงานร่วมกับระบบจัดการเครือข่ายซึ่งเรียกว่า เอเจนต์ (Agent) เอเจนต์เป็นส่วนของซอฟต์แวร์ที่อยู่ในอุปกรณ์ต่าง ๆ ที่เชื่อมต่ออยู่ในเครือข่ายโดยมีคอมพิวเตอร์หลักในระบบหนึ่งเครื่องเป็นตัวจัดการและบริหารเครือข่ายหรือเรียกว่า NMS-Network Management System

โปรโตคอล SNMP ได้ถูกพัฒนาขึ้นในปี พ.ศ. 2531 เนื่องจากมีความเจริญเติบโตในการใช้อุปกรณ์ที่สนับสนุน IP อย่างสูง โปรโตคอล SNMP ถูกออกแบบให้มีฟังก์ชันและการทำงานแบบง่าย โดยมีจุดประสงค์หลักเพื่อให้ผู้ดูแลระบบเครือข่ายสามารถเข้ามาจัดการอุปกรณ์เครือข่ายได้จากระยะไกลโดยง่าย

ในโครงงานนี้ SNMP Protocol เป็นส่วนที่ใช้ในการติดต่อกันระหว่าง LOG Server และ Layer3 Switch และนำข้อมูลต่าง ๆ ที่ต้องการมาเก็บในส่วนของ Log Server เพื่อนำข้อมูลไปใช้ต่อไป

2.7 ภาษา PERL [3]

PERL (Practical Extraction and Report Language) เป็นภาษาโปรแกรมแบบไดนามิกพัฒนาโดยนายแลร์รี วอลล์ (Larry Wall) ในปี ค.ศ. 1987 เพื่อใช้งานกับระบบปฏิบัติการยูนิกซ์

ภาษาเพิร์ล นั้นถูกออกแบบมาให้ใช้งานได้ง่าย โครงสร้างของภาษาจึงไม่ซับซ้อน มีลักษณะคล้ายกับภาษาซี นอกจากนี้เพิร์ลยังได้แนวคิดบางอย่างมาจากเชลล์สคริปต์, ภาษา AWK, sed และ Lisp และเป็นภาษาที่ระบบปฏิบัติการ linux ส่วนใหญ่รองรับอยู่แล้ว

ซึ่งในโครงงานนี้จะใช้ภาษา PERL มาทำงานในการส่งข้อความ SNMP ไปหาอุปกรณ์ Layer3 Switch และนำข้อมูลที่ได้อีกเก็บในระบบฐานข้อมูล

2.8 Apache Webserver [12]

Apache คือ Web Server พัฒนามาจาก HTTPD Web Server โดย Apache นี้จะทำหน้าที่ในการจัดเก็บหน้าเว็บ (webpage) และส่งหน้าเว็บไปยัง Browser ที่มีการเรียกเข้ายัง Web server ที่เก็บหน้าเว็บนั้นอยู่ ซึ่งปัจจุบันจัดได้ว่าเป็น Web Server ที่มีความน่าเชื่อถือมาก เนื่องจากเป็นที่ยอมรับใช้กันทั่วโลก อีกทั้ง Apache ยังเป็นซอฟต์แวร์แบบโอเพ่นซอร์ส ที่เปิดให้บุคคลทั่วไปสามารถเข้ามาร่วมพัฒนาส่วนต่างๆ ของอาปาเช่ได้ ซึ่งทำให้เกิดเป็นโมดูลที่เกิดประโยชน์มากมาย เช่น mod PERL, mod python

หรือ mod php และทำงานร่วมกับภาษาอื่นได้ แทนที่จะเป็นเพียงเซิร์ฟเวอร์ที่ให้บริการเพียงแค่ HTML อย่างเดียว

นอกจากนี้อาปาเซเองยังมีความสามารถอื่น ๆ ด้วย เช่น การยืนยันตัวตนบุคคล (mod_auth , mod_access, mod_digest) หรือเพิ่มความปลอดภัยในการสื่อสารผ่านโปรโตคอล https (mod_ssl) และยังมีโมดูลอื่น ๆ ที่ได้รับความนิยมใช้ เช่น mod_vhost ทำให้สามารถสร้างโฮสต์เสมือนภายในเครื่องเดียวกันได้หรือ mod_rewrite ซึ่งเป็นเครื่องมือที่จะช่วยให้ url ของเว็บนั้นอ่านง่ายขึ้น ยกตัวอย่างเช่น จากเดิมต้องอ้างถึงเว็บไซต์แห่งหนึ่งด้วยการพิมพ์ `http://mydomain.com/board/question.php?qid=2xDffw&action=show&ttl=1187400` แต่หลังจากใช้ mod_rewrite จะทำให้สั้นลงกลายเป็น `http://mydomain.com/board/question/how_to_edit_wikipedia_content.html` ซึ่งที่อยู่เหล่านี้จะขึ้นอยู่กับว่าผู้ดูแลเว็บไซต์ว่าต้องการให้อยู่ในลักษณะใด

ในโครงการนี้จะนำ Apache มาใช้ในการทำ webserver สำหรับฝั่งการแสดงผลข้อมูล

2.9 SQL Structured Query Language [11]

SQL คือภาษาที่ใช้ในการเขียนโปรแกรมเพื่อจัดการกับฐานข้อมูลโดยเฉพาะ เป็นภาษามาตรฐานบนระบบฐานข้อมูลเชิงสัมพันธ์และเป็นระบบเปิด (open system) หมายถึงสามารถใช้คำสั่ง SQL กับฐานข้อมูลชนิดใดก็ได้ และคำสั่งงานเดียวกันเมื่อสั่งงานผ่านระบบฐานข้อมูลที่แตกต่างกันจะได้ผลลัพธ์เหมือนกัน ทำให้สามารถเลือกใช้ฐานข้อมูลชนิดใดก็ได้โดยไม่ติดขัดกับฐานข้อมูลใดฐานข้อมูลหนึ่ง นอกจากนี้แล้ว SQL ยังเป็นชื่อโปรแกรมฐานข้อมูล ซึ่งโปรแกรม SQL เป็นโปรแกรมฐานข้อมูลที่มีโครงสร้างของภาษาที่เข้าใจง่าย ไม่ซับซ้อน มีประสิทธิภาพการทำงานสูง สามารถทำงานที่ซับซ้อนได้โดยใช้คำสั่งเพียงไม่กี่คำสั่ง โปรแกรม SQL จึงเหมาะที่จะใช้กับระบบฐานข้อมูลเชิงสัมพันธ์ และเป็นภาษาหนึ่งซึ่งแบ่งการทำงานได้เป็น 4 ประเภท ดังนี้

1. Select query ใช้สำหรับดึงข้อมูลที่ต้องการ
2. Update query ใช้สำหรับแก้ไขข้อมูล
3. Insert query ใช้สำหรับการเพิ่มข้อมูล
4. Delete query ใช้สำหรับลบข้อมูลออกไป

ปัจจุบันมีซอฟต์แวร์ระบบจัดการฐานข้อมูล (DBMS) ที่สนับสนุนการใช้คำสั่ง SQL เช่น Oracle ,DB2 ,MS-SQL และ MS-Access นอกจากนี้ภาษา SQL ถูกนำมาใช้เขียนร่วมกับโปรแกรมภาษาต่าง ๆ เช่น ภาษา C/C++ , VisualBasic และ Java

2.10 mySQL [11]

mySQL เป็นโปรแกรมจัดการฐานข้อมูล Relational Database Management System (RDBMS) เป็นฐานข้อมูลที่สามารถจัดเก็บ ค้นหา เรียงข้อมูล และดึงข้อมูล mySQL มีความสามารถให้

ผู้ใช้งานเข้าถึงข้อมูลได้หลายคนในเวลาเดียวกันได้และมีการเข้าถึงข้อมูลที่รวดเร็ว มีการกำหนดการเข้าใช้งานของผู้ใช้ในแบบต่าง ๆ อย่างเหมาะสมปลอดภัย MySQL ถูกใช้งานเมื่อปี 1996 แต่โปรแกรมนี้พัฒนาดังแต่ปี 1979 และชนะรางวัล Linux Journal Reader's Choice Award 3ปีซ้อน

ปัจจุบัน MySQL ได้ใช้งานแพร่หลายโดยเป็นโปรแกรม Open Source License แต่ก็มีแบบ Commercial License ด้วยเช่นกัน โดยคุณสมบัติจะแตกต่างกันออกไป

2.11 ภาษา PHP [12]

PHP ย่อมาจาก PHP Hypertext Preprocessor แต่เดิมย่อมาจาก Personal Home Page Tools PHP คือภาษาคอมพิวเตอร์จำพวก scripting language ภาษาจำพวกนี้คำสั่งต่าง ๆ จะเก็บอยู่ในไฟล์ที่เรียกว่า script และเวลาใช้งานต้องอาศัยตัวแปลชุดคำสั่ง ตัวอย่างของภาษาสคริปต์ก็เช่น JavaScript, PERL เป็นต้น ลักษณะของ PHP ที่แตกต่างจากภาษาสคริปต์แบบอื่น ๆ คือ PHP ได้รับการพัฒนาและออกแบบมาเพื่อใช้งานในการสร้างเอกสารแบบ HTML โดยสามารถสอดแทรกหรือแก้ไขเนื้อหาได้โดยอัตโนมัติ ดังนั้นจึงกล่าวว่า PHP เป็นภาษาที่เรียกว่า server-side หรือ HTML-embedded scripting language นั่นคือในทุก ๆ ครั้งก่อนที่เครื่องคอมพิวเตอร์ซึ่งให้บริการเป็น Web Server จะส่งหน้าเว็บเพจที่เขียนด้วย PHP ให้ จะทำการประมวลผลตามคำสั่งที่มีอยู่ให้เสร็จเสียก่อน แล้วจึงค่อยส่งผลลัพธ์ที่ได้ให้ ผลลัพธ์ที่ได้นั้นก็คือเว็บเพจที่เห็นนั่นเอง ถือได้ว่า PHP เป็นเครื่องมือที่สำคัญชนิดหนึ่งที่จะช่วยให้สามารถสร้าง Dynamic Web pages (เว็บเพจที่มีการโต้ตอบกับผู้ใช้) ได้อย่างมีประสิทธิภาพและมีลูกเล่นมากขึ้น

PHP เป็นผลงานที่เติบโตมาจากกลุ่มของนักพัฒนาในเชิงเปิดเผยรหัสต้นฉบับ หรือ Open Source ดังนั้น PHP จึงมีการพัฒนาไปอย่างรวดเร็วและแพร่หลายโดยเฉพาะอย่างยิ่งเมื่อใช้ร่วมกับ Apache Web Server ระบบปฏิบัติการอย่างเช่น Linux หรือ FreeBSD เป็นต้น ในปัจจุบัน PHP สามารถใช้ร่วมกับ Web Server ได้หลายตัว ซึ่ง PHP มีลักษณะเด่นคือ

1. ใช้ได้ฟรี
2. PHP เป็นโปรแกรมวิ่งข้าง Sever ดังนั้นขีดความสามารถไม่จำกัด
3. Conlatfun นั่นคือ PHP วิ่งบนเครื่อง UNIX, Linux, Windows ได้หมด
4. เรียนรู้ง่าย เนื่องจาก PHP ผ่งเข้าไปใน HTML และใช้โครงสร้างและไวยากรณ์ภาษาง่ายๆ
5. เร็วและมีประสิทธิภาพ โดยเฉพาะเมื่อใช้กับ Apache Server เพราะไม่ต้องใช้โปรแกรมจาก

ภายนอก

6. ใช้ร่วมกับ XML ได้ทันที
7. ใช้กับระบบแฟ้มข้อมูลได้
8. ใช้กับข้อมูลตัวอักษรได้อย่างมีประสิทธิภาพ
9. ใช้กับโครงสร้างข้อมูลแบบ Scalar ,Array ,Associative array
10. ใช้กับการประมวลผลภาพได้

ในโครงงานนี้ PHP จะเป็นภาษาที่ช่วยในการทำหน้าเว็บ ในการแสดงข้อมูลที่เก็บไว้ในฐานข้อมูล

2.12 RADIUS [15]

การเชื่อมต่อเพื่อพิสูจน์ตัวจริงระยะไกลในบริการของผู้ใช้หรือ RADIUS (Remote Authentication Dial In User Service) เป็นโปรโตคอลเครือข่ายที่ให้การตรวจสอบ อนุมัติ และการจัดการการบัญชี (AAA) จากส่วนกลาง สำหรับคอมพิวเตอร์ที่เชื่อมต่อและใช้บริการเครือข่าย RADIUS ได้รับการพัฒนาโดย Livingston Enterprises, Inc ในปี 1991 ในฐานะที่เป็นโปรโตคอลการตรวจสอบ และการบัญชีของเซิร์ฟเวอร์การเข้าถึง และภายหลังถูกนำมาเป็นมาตรฐานของ Internet Engineering Task Force (IETF) RADIUS เป็นโปรโตคอลแบบไคลเอนต์/เซิร์ฟเวอร์ที่ทำงานในชั้นแอปพลิเคชัน ใช้ UDP

2.13 FreeRADIUS [14]

FreeRADIUS เริ่มต้นในเดือนสิงหาคม 2542 โดย Alan DeKok และ Miquel van Smoorenburg โดย Miquel เคยพัฒนา Cistron RADIUS server ซึ่งเคยได้รับความนิยมเมื่อ Livingston server ไม่มีปรับปรุงดูแล จึงได้เริ่มสร้าง RADIUS Server ขึ้นมาใหม่ โดยใช้โมดูลการออกแบบที่จะให้ประชาชนมีส่วนร่วมมากขึ้น

รุ่นล่าสุดคือ FreeRADIUS 3 ซึ่ง FreeRADIUS 3 รวมการสนับสนุนสำหรับ RADIUS over TLS รวมทั้ง RadSec โมดูล rlm_ldap ที่เขียนขึ้นใหม่ และความเปลี่ยนแปลงอื่น ๆ ในรุ่นล่าสุดเพื่อความปลอดภัย และปรับปรุงประสิทธิภาพการใช้งานให้ดีกว่ารุ่นก่อน

FreeRADIUS เป็นซอฟต์แวร์ที่ทำหน้าที่เป็น Radius Server ซึ่งเป็น Server ในการจัดการการยืนยันตัวตนของผู้ใช้โดย FreeRADIUS เป็นฟรีซอฟต์แวร์ที่มีความสามารถสูง มีความยืดหยุ่นและได้รับความนิยมสูง

2.14 หลักการทำงานเบื้องต้นของโครงการ

จากปัญหาการไม่สามารถระบุตัวตนได้ในระบบ IPv6 เนื่องจากระบบการยืนยันตัวตนผู้ใช้ในรูปแบบเดิมที่ไม่ได้ออกแบบมารองรับกับรูปแบบของ IPv6 จึงทำให้ไม่สามารถระบุตัวตนผู้ใช้ได้ในกรณีที่ผู้ใช้ได้ใช้งานผ่านรูปแบบของ IPv6 เช่น ปัญหาของ IP Address ที่มีขนาดใหญ่ขึ้น และสามารถมีได้หลายค่าและ Temporary IP Address ซึ่งตรวจสอบได้ยากดังรูปที่ 2-1 IP Address ของเครื่องตัวอย่าง

```

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : coe.psu.ac.th
Description . . . . . : Realtek PCIe GBE Family Controller
Physical Address. . . . . : BC-EE-7B-53-4F-A0
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:3c8:9009:1e8:143: [redacted] (Preferred)
Lease Obtained. . . . . : 29, 2014 9:26:52 PM
Lease Expires . . . . . : 30, 2014 1:26:52 AM
IPv6 Address. . . . . : 2001:3c8:9009:1e8:98f: [redacted] (Preferred)
Temporary IPv6 Address. . . . . : 2001:3c8:9009:1e8:292: [redacted] (Preferred)
Link-local IPv6 Address . . . . . : fe80::98b3:730e:afc4: [redacted] (Preferred)
IPv4 Address. . . . . : 172.30.232.233 (Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 29, 2014 9:27:44 PM
Lease Expires . . . . . : 30, 2014 3:27:44 AM
Default Gateway . . . . . : fe80::1x18: [redacted]
                          172.30.232.1

```

รูปที่ 2-1 IP Address ของเครื่องตัวอย่าง

ทำให้หากเกิดการกระทำผิดเกี่ยวกับคอมพิวเตอร์ขึ้น จากที่อยู่ IPv6 จะไม่สามารถระบุผู้กระทำความผิดได้ เนื่องจากระบบยังไม่รองรับการใช้งานด้วย IPv6 อย่างสมบูรณ์ เช่น รูปที่ 2-2 ข้อมูลบางส่วนจากรางงานสถิติการใช้งาน ของ firewall ของมหาวิทยาลัยสงขลานครินทร์ ในส่วนของ Risky Users ประจำวันที่ 26 กันยายน พ.ศ.2557 จะเห็นว่าไม่สามารถระบุผู้ใช้ในระบบ IPv6 ได้

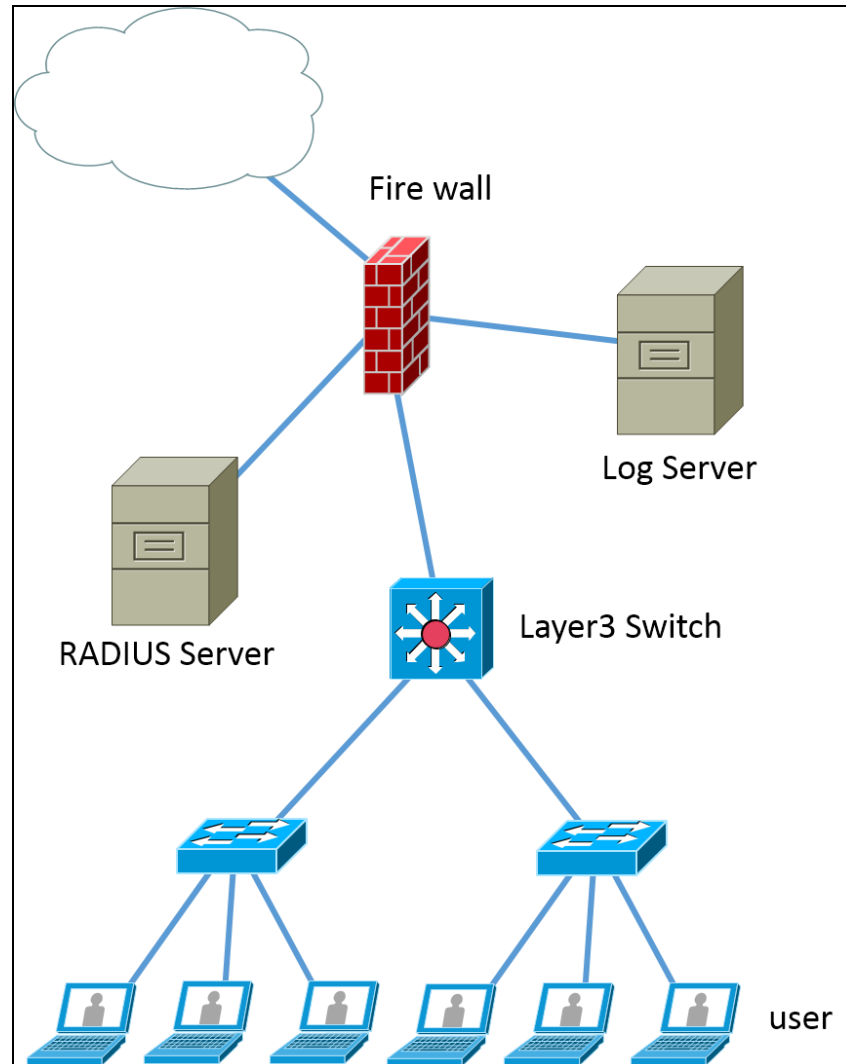
Virtual System	Source User	Source address	Source Host Name	Risk	Bytes	Sessions
vsys1	5540411112	172.21.148.182	172.21.148.182	4	553.60 M	323
vsys1	5411310071	172.24.5.14	172.24.5.14	4	552.52 M	23
vsys1	5610610363	172.22.116.120	172.22.116.120	4	542.35 M	98
vsys1	5630312007	172.19.131.155	172.19.131.155	4	532.77 M	50
vsys1	5620310056	172.18.40.106	172.18.40.106	4	515.05 M	83
vsys1		2001:3c8:9009:51c:a461:1f96:b28:6304	2001:3c8:9009:51c:a461:1f96:b28:6304	4	509.76 M	42

จะเห็นว่าไม่สามารถระบุผู้ใช้ในระบบ IPv6 ได้

รูปที่ 2-2 ข้อมูลบางส่วนจากรางงานสถิติการใช้งาน ของ firewall ของมหาวิทยาลัยสงขลานครินทร์ ในส่วนของ Risky Users ประจำวันที่ 26 กันยายน พ.ศ.2557

เนื่องด้วย Layer3 Switch จะมีการทำงานอยู่บน OSI model ในระดับที่ 3 โดยจะมีการเลือกเส้นทางจาก IP Address ซึ่งการทำงานดังกล่าวจะมีการเก็บตาราง IP Address เพื่อใช้ในการเลือกเส้นทาง ซึ่งจะมีการเก็บค่า IP Address และ MAC Address ใน ARP table ของระบบ IP Address v.4 และ ND table ในระบบ IP Address v.6 โดย Layer3 Switch ส่วนใหญ่จะมีการสนับสนุนการใช้งาน SNMP ซึ่งมีคำสั่งช่วยในการเรียกข้อมูลในส่วนดังกล่าวมาเพื่อใช้งานต่อได้ โดยจะมีการให้เครื่องคอมพิวเตอร์เครื่องหนึ่งทำการเรียกข้อมูลในส่วนดังกล่าวมาเปรียบเทียบกับโดยใช้ Mac Address เป็นตัวเชื่อมโยง และเก็บข้อมูลต่าง ๆ ในขณะเดียวกันก็ให้เครื่องดังกล่าวเป็น server ในการเข้าสู่ข้อมูลในส่วนที่เก็บได้ง่ายขึ้น ซึ่งผลได้ทำให้ได้ข้อมูลว่าปัจจุบันมีอุปกรณ์ใดที่ใช้งานบน IPv4 และ IPv6 ไปบ้างโดยมี

ข้อมูล IP Address และ MAC Address ของเครื่องต่าง ๆ ที่ใช้งานผ่าน Layer3 Switch เมื่อนำมาเปรียบเทียบกับข้อมูลจาก RADIUS Server จะทำให้ทราบถึงผู้ใช้ ของแต่ละ IP Address ได้

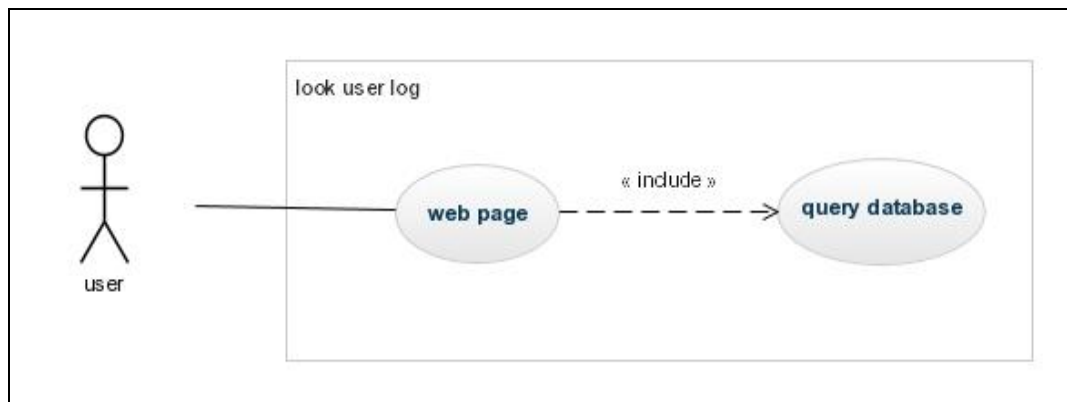


รูปที่ 2-3 การเชื่อมต่อ Log Server กับเครือข่าย

การเชื่อมต่อ Log Server จะต้องเชื่อมต่อ และสามารถติดต่อได้กับอุปกรณ์ Layer3 Switch และ RADIUS Server ดังรูปที่ 2-3 การเชื่อมต่อ Log Server กับเครือข่ายโดย Log Server จะมีการทำงานดังนี้

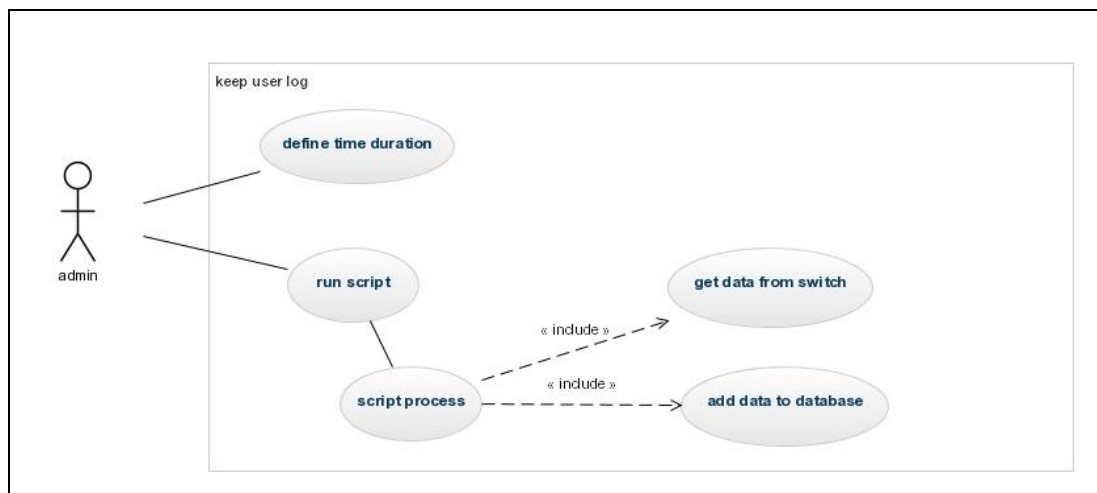
1. log sever ส่งข้อความร้องขอข้อมูลไปยัง Layer3 Switch ผ่านทาง SNMP Protocol เป็นระยะ
2. log sever ได้รับข้อมูลกลับมาประมวลผลและเก็บไว้ในระบบฐานข้อมูล
3. Web Server นำข้อมูลที่เก็บในฐานข้อมูลมาแสดงผ่านหน้า web

โดยผู้ใช้งานจะมี 2 กลุ่มโดยในกลุ่มแรกคือผู้ใช้ทั่วไปซึ่งจะสามารถเข้าสู่ข้อมูลประวัติของตนเองผ่านทางหน้าเว็บได้ดังรูปที่ 2-4 use case diagram ของผู้ใช้ทั่วไป



รูปที่ 2-4 use case diagram ของผู้ใช้ทั่วไป

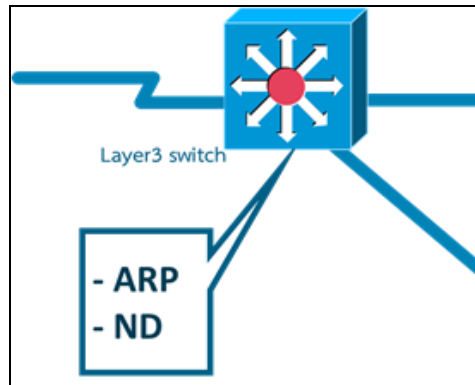
และผู้ใช้ที่เป็นผู้ดูแลระบบสามารถกำหนดความถี่ของการตรวจสอบข้อมูลของ Server ได้ดังรูปที่ 2-5 use case diagram ของผู้ดูแลระบบ



รูปที่ 2-5 use case diagram ของผู้ดูแลระบบ

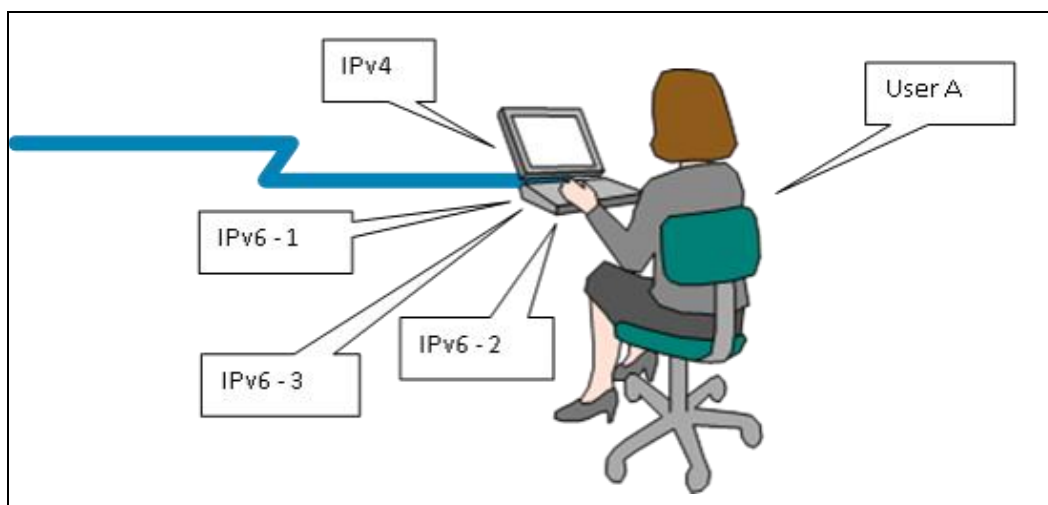
3. ระเบียบวิธีวิจัย

3.1 แนวคิดในการออกแบบระบบ



รูปที่ 3-1 Layer3 Switch

ใน Layer3 Switch ซึ่งทำงานบน Layer3 OSI model มีการเก็บตารางระหว่าง IP Address และ Physical Address ซึ่งก็คือ ตารางของ ARP ใน IPv4 และ ND ใน IPv6 ดังรูปที่ 3-1 Layer3 Switch ในส่วนของผู้ใช้ ทาง radius server จะมีการเก็บข้อมูลชื่อผู้ใช้ และ Physical Address อยู่แล้ว ดังนั้นจากสมมติฐานว่า “ในช่วงเวลาเดียวกันอุปกรณ์ที่มี IP Address ซึ่งมาจาก Physical Address เดียวกัน ย่อมเป็นอุปกรณ์เดียวกัน และย่อมเป็นผู้ใช้คนเดียวกัน” ดังรูปที่ 3-2 แนวคิดการทำงานของระบบระบุตัวตน



รูปที่ 3-2 แนวคิดการทำงานของระบบระบุตัวตน

ดังนั้นจึงสามารถระบุผู้ใช้ของ IP Address ใน IPv6 ได้ทางอ้อมจากการเทียบผู้ที่ใช้ที่มี Physical Address เดียวกันกับ IP Address ที่ต้องการทราบ โดยใช้ข้อมูลจากตาราง ARP ซึ่งสามารถระบุ IPv4 ของ Mac Address นั้นได้ดังรูปที่ 3-3 ตัวอย่างข้อมูลที่ได้จาก ARP, ตาราง ND ซึ่งสามารถระบุ IPv6 ของ Mac Address นั้นได้ดังรูปที่ 3-4 ตัวอย่างข้อมูลที่ได้จาก ND และข้อมูลจาก Radius Server ดังรูปที่ 3-5 ตัวอย่างข้อมูลที่ได้จาก radius server ซึ่งจะช่วยระบุ User ได้ ดังรูปที่ 3-6 แนวทางการเก็บข้อมูล

```
IP-MIB::ipNetToMediaPhysAddress.202.172.30.254.69 = STRING: 0:12:7f:17:a3:80
IP-MIB::ipNetToMediaPhysAddress.202.172.30.254.73 = STRING: 0:19:e7:e8:2:41
IP-MIB::ipNetToMediaPhysAddress.202.172.30.254.75 = STRING: c:85:25:c9:25:c1
IP-MIB::ipNetToMediaPhysAddress.202.172.30.254.77 = STRING: c:85:25:a3:fb:c1
IP-MIB::ipNetToMediaPhysAddress.202.172.30.254.79 = STRING: a4:56:30:54:bd:c1
IP-MIB::ipNetToMediaPhysAddress.202.172.30.254.80 = STRING: 0:12:43:bd:92:40
IP-MIB::ipNetToMediaPhysAddress.202.172.30.254.84 = STRING: 0:15:63:6:8e:40
IP-MIB::ipNetToMediaPhysAddress.202.172.30.254.85 = STRING: 0:19:e8:6c:40:42
IP-MIB::ipNetToMediaPhysAddress.202.172.30.254.88 = STRING: a4:56:30:56:68:41
IP-MIB::ipNetToMediaPhysAddress.202.172.30.254.89 = STRING: c:85:25:eb:e0:c1
IP-MIB::ipNetToMediaPhysAddress.202.172.30.254.109 = STRING: 34:62:88:77:c4:f2
IP-MIB::ipNetToMediaPhysAddress.202.172.30.254.201 = STRING: 0:c0:b7:d3:95:e8
IP-MIB::ipNetToMediaPhysAddress.202.172.30.254.202 = STRING: 0:c0:b7:84:6a:61
IP-MIB::ipNetToMediaPhysAddress.206.172.30.230.1 = STRING: 0:24:c4:6a:13:ff
IP-MIB::ipNetToMediaPhysAddress.206.172.30.230.101 = STRING: bc:5f:f4:fa:d6:77
IP-MIB::ipNetToMediaPhysAddress.206.172.30.230.143 = STRING: b8:88:e3:75:5:22
IP-MIB::ipNetToMediaPhysAddress.206.172.30.230.150 = STRING: 4:7d:7b:da:d2:b
IP-MIB::ipNetToMediaPhysAddress.206.172.30.230.151 = STRING: 0:c:29:6e:ca:8b
IP-MIB::ipNetToMediaPhysAddress.206.172.30.230.156 = STRING: 14:fe:b5:a7:b:f6
IP-MIB::ipNetToMediaPhysAddress.206.172.30.230.160 = STRING: 20:cf:30:90:4f:3c
IP-MIB::ipNetToMediaPhysAddress.206.172.30.230.162 = STRING: 44:8a:5b:45:8e:aa
IP-MIB::ipNetToMediaPhysAddress.206.172.30.230.163 = STRING: b8:27:eb:a6:61:79
IP-MIB::ipNetToMediaPhysAddress.208.172.30.224.1 = STRING: 0:24:c4:6a:13:ff
IP-MIB::ipNetToMediaPhysAddress.208.172.30.224.106 = STRING: 94:de:80:a2:ec:48
IP-MIB::ipNetToMediaPhysAddress.208.172.30.224.251 = STRING: f0:7d:68:c:57:f9
```

รูปที่ 3-3 ตัวอย่างข้อมูลที่ได้จาก ARP

```
IP-MIB::ipNetToPhysicalPhysAddress.103.ipv6."20:01:03:c8:90:09:01:f3:6d:0c:33:df:5c:53:3a:53" = STRING: 20:89:84:89:ff:7d
IP-MIB::ipNetToPhysicalPhysAddress.103.ipv6."20:01:03:c8:90:09:01:f3:a9:5f:ec:70:da:e1:50:86" = STRING: 14:da:e9:61:b0:1d
IP-MIB::ipNetToPhysicalPhysAddress.103.ipv6."20:01:03:c8:90:09:01:f3:cc:0c:d9:4a:6d:e9:ba:ac" = STRING: 44:8a:5b:a0:83:e6
IP-MIB::ipNetToPhysicalPhysAddress.103.ipv6."20:01:03:c8:90:09:01:f3:cc:49:8e:8d:4a:4e:29:cd" = STRING: e0:db:55:f7:69:fe
IP-MIB::ipNetToPhysicalPhysAddress.103.ipv6."20:01:03:c8:90:09:01:f3:f1:c6:b0:42:ff:a8:3a:d5" = STRING: 10:78:d2:47:f5:66
IP-MIB::ipNetToPhysicalPhysAddress.103.ipv6."fe:80:00:00:00:00:00:08:7f:c6:9a:1e:fe:4b:c7" = STRING: 20:89:84:89:ff:7d
IP-MIB::ipNetToPhysicalPhysAddress.103.ipv6."fe:80:00:00:00:00:00:71:35:0a:9d:c0:51:d2:63" = STRING: 14:da:e9:61:b0:1d
IP-MIB::ipNetToPhysicalPhysAddress.103.ipv6."fe:80:00:00:00:00:00:90:48:3e:96:da:3b:45:08" = STRING: e0:db:55:f7:69:fe
IP-MIB::ipNetToPhysicalPhysAddress.103.ipv6."fe:80:00:00:00:00:00:bc:b6:47:8d:ad:6e:50:fb" = STRING: f0:4d:a2:61:b7:22
IP-MIB::ipNetToPhysicalPhysAddress.103.ipv6."fe:80:00:00:00:00:00:00:f1:c6:b0:42:ff:a8:3a:d5" = STRING: 10:78:d2:47:f5:66
IP-MIB::ipNetToPhysicalPhysAddress.105.ipv6."20:01:03:c8:90:09:01:f5:39:c2:54:17:37:20:c4:8e" = STRING: 0:1c:c0:fa:64:44
IP-MIB::ipNetToPhysicalPhysAddress.105.ipv6."20:01:03:c8:90:09:01:f5:8c:16:c7:71:a2:6f:a2:cd" = STRING: 0:80:48:38:9:bc
IP-MIB::ipNetToPhysicalPhysAddress.105.ipv6."fe:80:00:00:00:00:00:02:1c:c0:ff:fe:fa:64:44" = STRING: 0:1c:c0:fa:64:44
IP-MIB::ipNetToPhysicalPhysAddress.106.ipv6."20:01:03:c8:90:09:01:f7:88:7f:49:fd:d5:4c:9f:46" = STRING: 4c:72:b9:b1:bb:ff
IP-MIB::ipNetToPhysicalPhysAddress.106.ipv6."fe:80:00:00:00:00:00:04:e7:b9:ff:fe:b1:bb:ff" = STRING: 4c:72:b9:b1:bb:ff
IP-MIB::ipNetToPhysicalPhysAddress.206.ipv6."20:01:03:c8:90:09:01:e6:20:5c:2e:3b:24:32:89:7c" = STRING: 44:8a:5b:45:8e:aa
IP-MIB::ipNetToPhysicalPhysAddress.206.ipv6."20:01:03:c8:90:09:01:e6:48:fb:49:f0:ac:b4:2a:25" = STRING: b8:88:e3:75:5:22
```

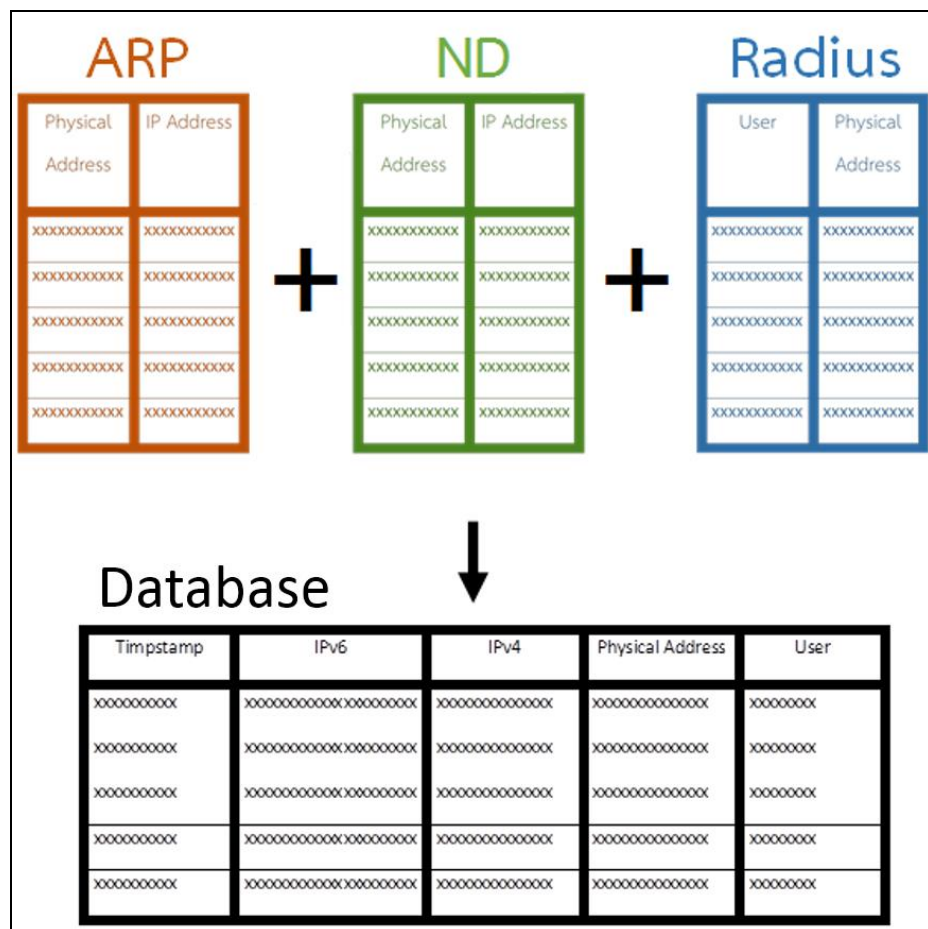
รูปที่ 3-4 ตัวอย่างข้อมูลที่ได้จาก ND

```

Wed Apr 15 23:44:45 2015
Acct-Status-Type = Start
NAS-Port-Type = Wireless-802.11
Calling-Station-Id = "BC:EE:7B:53:4F:A0"
Called-Station-Id = "hotspot1"
NAS-Port-Id = "ether3"
User-Name = "test"
NAS-Port = 2148532238
Acct-Session-Id = "8010000e"
Framed-IP-Address = 10.5.50.254
Mikrotik-Host-IP = 10.5.50.254
Event-Timestamp = "Apr 15 2015 23:44:38 ICT"
NAS-Identifier = "MikroTik"
Acct-Delay-Time = 0
NAS-IP-Address = 172.30.232.93
Acct-Unique-Session-Id = "138d0e2d0f8763e9"
Timestamp = 1429116285

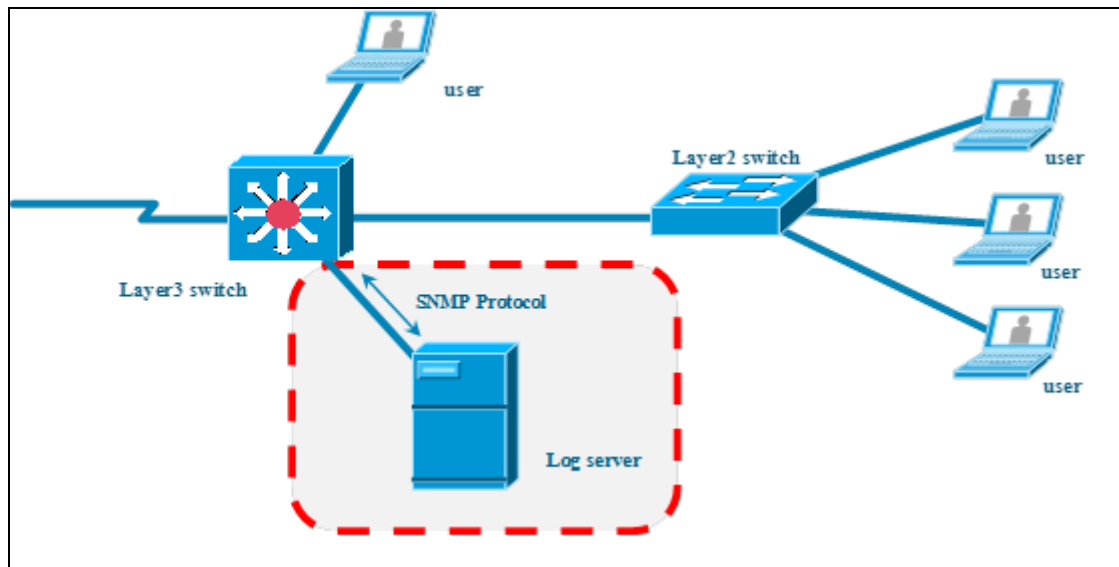
```

รูปที่ 3-5 ตัวอย่างข้อมูลที่ได้จาก radius server



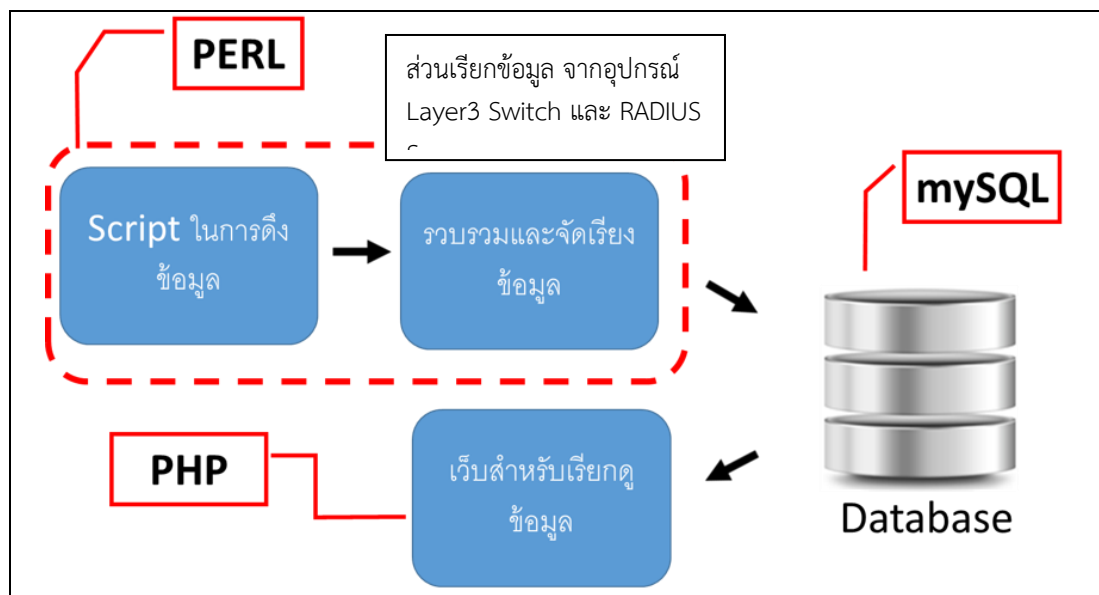
รูปที่ 3-6 แนวทางการเก็บข้อมูล

3.2 ระบบที่ได้ออกแบบ



รูปที่ 3-7 ภาพรวมระบบที่ได้ออกแบบ

ระบบที่ได้ออกแบบจะเป็น server ที่เชื่อมต่อกับเครือข่ายที่สามารถเข้าไปดึงค่าต่าง ๆ ของอุปกรณ์ Layer3 Switch ได้โดยการติดต่อจะใช้ SNMP ในการติดต่อสื่อสารกับอุปกรณ์ Layer3 Switch ได้ดังรูปที่ 3-7 ภาพรวมระบบที่ได้ออกแบบ



รูปที่ 3-8 ส่วนประกอบหลักของโครงการ

โดยการทำงานจะแบ่งออกเป็น 3 ส่วนใหญ่ๆ ดังนี้

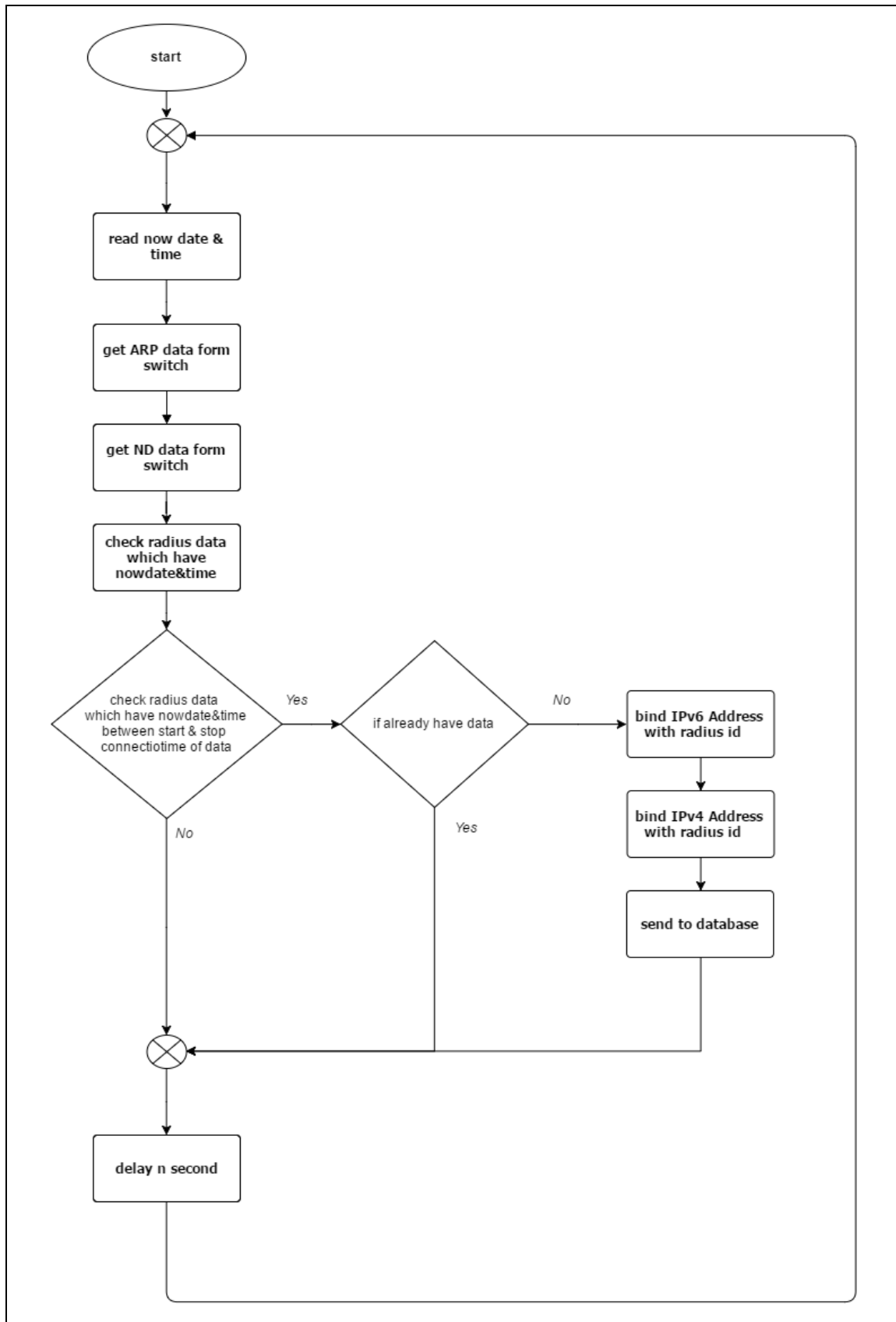
ส่วนที่ 1 จะเป็นสคริปต์ที่เขียนด้วยภาษา PERL ทำงานตลอดเวลาเพื่อรับค่าจากอุปกรณ์ Layer3 Switch และนำมาวิเคราะห์หาผู้ใช้ให้กับ IP Address ที่เป็น IPv6 และส่งต่อไปให้กับส่วนที่ 2

ส่วนที่ 2 จะเป็นฐานข้อมูลที่ใช้เก็บข้อมูลที่ผ่านกระบวนการจากส่วนที่หนึ่งมาแล้วโดยใช้ mySQL เป็นตัวจัดการฐานข้อมูล

ส่วนที่ 3 จะเป็นส่วนของเว็บแอปพลิเคชันที่นำข้อมูลจากฐานข้อมูลในส่วนที่ 2 มาจัดรูปแบบและแสดงผลตามที่ต้องการ โดยจะมีการวิเคราะห์ ทำสถิติจากข้อมูลที่มี และสามารถค้นหารายการตามที่น่าสนใจได้

3.2.1 การทำงานของส่วนสคริปต์ สำหรับเรียกข้อมูลจาก Layer3 Switch

ในส่วนนี้จะทำงานโดยใช้ SNMP เพื่อติดต่อกับอุปกรณ์ Layer3 Switch แล้วนำข้อมูลที่ได้มาเปรียบเทียบกับข้อมูลจาก RADIUS Server โดยเปรียบเทียบช่วงเวลาการเชื่อมต่อกับเวลาที่เรียกข้อมูลได้มา โดยใช้ MAC Address ในการจับคู่ แล้วส่งข้อมูลไปเก็บในฐานข้อมูล ดังรูปที่ 3-9 flowchart แสดงการทำงานของสคริปต์ สำหรับเรียกข้อมูลจาก Layer3 Switch



รูปที่ 3-9 flowchart แสดงการทำงานของสคริปต์ สำหรับเรียกข้อมูลจาก Layer3 Switch

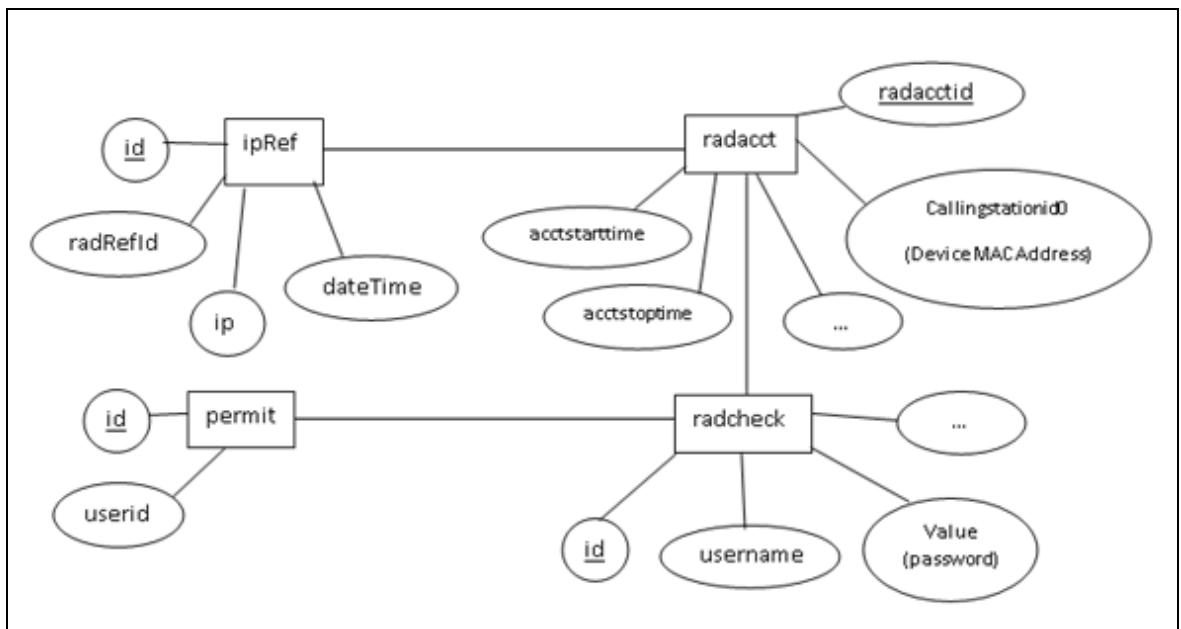
3.2.2 การออกแบบส่วนฐานข้อมูล

ฐานข้อมูลสำหรับการเก็บข้อมูลที่ได้มาจากตัวสคริปต์นั้นแบ่งเป็น 2 ตาราง คือ ตาราง ipRef และ ตาราง permit โดย

ตาราง ipRef เก็บหมายเลขอ้างอิงจากตาราง radacct (radRefId) ซึ่งก็คือตารางที่เก็บข้อมูลการลงชื่อใช้งานจาก radius server, IP Address และเวลาที่เก็บข้อมูล

ตาราง permit เป็นการกำหนดให้ผู้ใช้ใดบ้างที่ได้สิทธิ์ผู้ดูแลระบบโดยมีการเก็บหมายเลข id ของผู้ใช้ที่มีสิทธิ์เป็นผู้ดูแลระบบ

ซึ่งตาราง radacct และตาราง radcheck จะเป็นตารางที่ FreeRADIUS สร้างขึ้นมาอยู่แล้ว ดังรูปที่ 3-10 ER-Diagram ของฐานข้อมูลที่ของระบบ



รูปที่ 3-10 ER-Diagram ของฐานข้อมูลที่ของระบบ

3.2.3 ส่วนของเว็บไซต์ที่แสดงข้อมูล

ส่วนของเว็บไซต์เพื่อแสดงข้อมูลการเชื่อมต่อของผู้ใช้โดยเมื่อเข้าสู่หน้าแรกจะมีการลงชื่อเข้าใช้ และตรวจสอบสิทธิ์การใช้งาน ซึ่งจะแสดงรายการคำสั่งแตกต่างกันออกไปตามสิทธิ์ของผู้เข้าชม โดย

ผู้ใช้ทั่วไปสามารถเข้าถึงดังนี้

1. ดู และค้นหา ข้อมูลได้เฉพาะของตนเองเท่านั้น
2. พิมพ์รายงานข้อมูลได้เฉพาะของตนเองเท่านั้น

ผู้ใช้ที่มีสิทธิ์เป็นผู้ดูแลระบบจะสามารถเข้าถึงดังนี้

1. ดู และค้นหา ข้อมูลของผู้ใช้ทุกคนได้
2. พิมพ์รายงานข้อมูลของผู้ใช้ทุกคนได้
3. สำรองข้อมูล และนำเข้าข้อมูลสำรองได้

3.3 การทดสอบระบบ

เนื่องจากได้แบ่งเป็นส่วนๆอย่างชัดเจน การทดสอบระบบจึงสามารถทำได้โดยการทดสอบเป็นส่วนๆ และส่วนย่อยของแต่ละส่วน เช่น ค่าที่รับได้ออกมาเป็นอย่างไร ตีความหมายแล้วได้ผลลัพธ์อย่างไร ตรงกับสิ่งที่ต้องการหรือไม่ สามารถส่งต่อไปยังส่วนต่อไปหรือสามารถเรียกใช้จากส่วนก่อนหน้าได้ถูกต้องหรือไม่ และทดลองสุ่มผลลัพธ์เพื่อตรวจสอบค่าจากเครื่องตัวอย่าง ซึ่งผลลัพธ์มีความถูกต้องตามที่ออกแบบไว้

4. ผลและวิเคราะห์ผลการทดลอง

4.1 การทดสอบการจำลองระบบลงชื่อเข้าใช้

เป็นการจำลองสภาพแวดล้อมการลงชื่อเข้าใช้แบบ 802.1x โดยใช้อุปกรณ์ Switch เป็นเชื่อมต่อ กับ RADIUS Server ซึ่งใช้ FreeRADIUS เป็น RADIUS Server



รูปที่ 4-1 การลงชื่อเข้าใช้ของระบบที่จำลองขึ้น

4.2 การทดสอบระบบส่วนเบื้องหลัง

ในส่วนนี้ เป็นส่วนสคริปต์ที่มีการเรียกข้อมูลจากอุปกรณ์ Switch แล้วนำค่าที่ได้จากส่วนของ IPv6, IPv4, Mac Address และผู้ใช้จาก Radius Server มาเปรียบเทียบกันเป็นระยะ ๆ แล้วส่งข้อมูลไปยังส่วนที่ 2 ซึ่งคือส่วนของฐานข้อมูล โดยข้อมูลที่อยู่ของ Switch ตำแหน่งเครื่อง Server และข้อมูลเกี่ยวกับการเชื่อมต่อฐานข้อมูล ระยะของช่วงเวลาที่มีการเรียกข้อมูลจะนำมาจากข้อมูลที่กำหนดไว้ในไฟล์ ในส่วนการตั้งค่าของระบบโดยจะมีการกำหนดช่วงเวลาเป็นวินาที

```

11 ##### basic config #####
12 my $switch_v6address = "2001:3c8:9009:181::1";
13 my $interval = 60; # time interval between pooling round in second unit.
14
15 ##### MYSQL CONFIG VARIABLES #####
16 my $driver = "mysql";
17
18 my $radhost = "localhost"; # radius server ip address.
19 my $raduserid = "root"; # username to access database .
20 my $radpassword = "kks*5cyp768"; # password for access database.
21 my $raddatabase = "radius";
22
23
24 my $loghost = "localhost"; # Log server ip address.
25 my $loguserid = "root"; # username to access Logdatabase .
26 my $logpassword = "kks*5cyp768"; # password for access Logdatabase.
27 my $logdatabase = "proj"; # database name
28
29
30 #####

```

รูปที่ 4-2 ตัวอย่างไฟล์การตั้งค่าช่วงเวลาการตรวจสอบ

ซึ่งในการเรียกข้อมูลจากอุปกรณ์ Switch จะได้ลักษณะของข้อมูลดังรูปที่ 4-3 ผลลัพธ์จากการทดสอบ โดยยังไม่ได้นำไปจับคู่กับข้อมูลผู้ใช้แล้วจึงนำค่าที่ได้มาแยกข้อมูล และนำมาเปรียบเทียบกัน ซึ่งจะได้ข้อมูลของ IP Address ในส่วนของ IPv6 และ MAC Address ของอุปกรณ์ในเวลานั้น ๆ และเมื่อนำข้อมูลที่ได้ไปเปรียบเทียบกับข้อมูลการลงชื่อเข้าใช้ของ RADIUS server จะทำให้สามารถคาดเดาได้ว่า IPv6 ของอุปกรณ์ที่อยู่ในเครือข่ายนั้นเข้าใช้ด้วยชื่อผู้ใช้ใด และส่งข้อมูลที่ได้ไปยังฐานข้อมูลได้ โดยสามารถเข้าไปดูประวัติการลงชื่อเข้าใช้ของผู้ใช้ได้ดังรูปที่ 4-7 แสดงส่วนของเว็บสำหรับการดูข้อมูลการบันทึกการใช้งานในมุมมองผู้ใช้ทั่วไป และดังรูปที่ 4-8 แสดงของส่วนเว็บสำหรับการดูบันทึกการใช้งานในมุมมองผู้ดูแลระบบ

2001:03c8:9009:01f5:c868:d6a7:9d52:8a51	18:3:73:d5:70:7b	172.30.245.181	2015-6-25	15:54:39
fe80:0000:0000:0000:213b:2f9c:f226:d362	0:23:54:26:b4:34	172.30.245.176	2015-6-25	15:54:39
fe80:0000:0000:0000:4874:82fe:9b53:a715	18:3:73:d5:70:7b	172.30.245.181	2015-6-25	15:54:39
2001:03c8:9009:01f7:a870:93b4:51c6:fbcb	74:d0:2b:7:3c:a8	172.30.247.199	2015-6-25	15:54:39
2001:03c8:9009:01f7:b872:7894:b954:b613	4c:72:b9:b1:bb:ff	172.30.247.188	2015-6-25	15:54:39
fe80:0000:0000:0000:4e72:b9ff:feb1:bbff	4c:72:b9:b1:bb:ff	172.30.247.188	2015-6-25	15:54:39
fe80:0000:0000:0000:a870:93b4:51c6:fbcb	74:d0:2b:7:3c:a8	172.30.247.199	2015-6-25	15:54:39

รูปที่ 4-3 ผลลัพธ์จากการทดสอบ โดยยังไม่ได้นำไปจับคู่กับข้อมูลผู้ใช้

การนำข้อมูลชื่อผู้ใช้งานมาหาความสัมพันธ์กับข้อมูลการใช้นั้น นำมาจากข้อมูลในส่วนของ RADIUS server ซึ่งจะมีข้อมูลต่าง ๆ เช่น วัน เวลา ที่มีการเข้าสู่ระบบ ipaddress และอื่น ๆ ดังรูปที่ 4-4 ตัวอย่าง log ของ RADIUS server ที่มาจากการยืนยันตัวตนในระบบ

```

Wed Apr 15 23:44:45 2015
Acct-Status-Type = Start
NAS-Port-Type = Wireless-802.11
Calling-Station-Id = "BC:EE:7B:53:4F:A0"
Called-Station-Id = "hotspot1"
NAS-Port-Id = "ether3"
User-Name = "test"
NAS-Port = 2148532238
Acct-Session-Id = "8010000e"
Framed-IP-Address = 10.5.50.254
Mikrotik-Host-IP = 10.5.50.254
Event-Timestamp = "Apr 15 2015 23:44:38 ICT"
NAS-Identifier = "MikroTik"
Acct-Delay-Time = 0
NAS-IP-Address = 172.30.232.93
Acct-Unique-Session-Id = "138d0e2d0f8763e9"
Timestamp = 1429116285


































```

รูปที่ 4-4 ตัวอย่าง log ของ RADIUS server ที่มาจากการยืนยันตัวตนในระบบ

การระบุถึงผู้ใช้ในระบบ IPv6 จึงสามารถอ้างอิงจากข้อมูลการลงชื่อเข้าใช้ในระบบ IPv4 จาก RADIUS server ได้โดยการเทียบ MAC Address

4.3 การทดสอบระบบส่วนฐานข้อมูล

ในส่วนนี้เป็นส่วนที่ใช้เก็บข้อมูล ของระบบ โดยใช้ mySQL เป็นตัวจัดการฐานข้อมูลทดสอบการทำงานโดยการรันสคริปต์จากการเรียกข้อมูลจาก L3 Switch แล้วสามารถ เก็บข้อมูลจากส่วนของสคริปต์เรียกข้อมูลได้ ดังรูปรูปที่ 4-5 ข้อมูลที่ถูกเพิ่มจากสคริปต์จากการเรียกข้อมูลจาก L3 Switch

+ ตัวเลือก										
← T →		▼	id	radRefId	▼	ip	dateTime			
<input type="checkbox"/>		แก้ไข		คัดลอก		ลบ	200	148	FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB	2016-12-01 16:59:27
<input type="checkbox"/>		แก้ไข		คัดลอก		ลบ	199	148	2001:03C8:9009:01E7:C02C:ADCF:5057:07D1	2016-12-01 16:59:27
<input type="checkbox"/>		แก้ไข		คัดลอก		ลบ	198	148	172.30.231.17	2016-12-01 16:59:27
<input type="checkbox"/>		แก้ไข		คัดลอก		ลบ	197	147	FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB	2016-12-01 16:39:33
<input type="checkbox"/>		แก้ไข		คัดลอก		ลบ	196	147	2001:03C8:9009:01E7:4CB3:9FD0:4AB6:04C0	2016-12-01 16:39:33
<input type="checkbox"/>		แก้ไข		คัดลอก		ลบ	195	147	172.30.231.17	2016-12-01 16:39:33
<input type="checkbox"/>		แก้ไข		คัดลอก		ลบ	192	146	172.30.231.17	2016-12-01 13:54:24
<input type="checkbox"/>		แก้ไข		คัดลอก		ลบ	193	146	2001:03C8:9009:01E7:2DE4:3908:E5BE:6B5E	2016-12-01 13:54:24
<input type="checkbox"/>		แก้ไข		คัดลอก		ลบ	194	146	FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB	2016-12-01 13:54:24
<input type="checkbox"/>		แก้ไข		คัดลอก		ลบ	191	145	FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB	2016-12-01 08:42:31
<input type="checkbox"/>		แก้ไข		คัดลอก		ลบ	190	145	2001:03C8:9009:01E7:C8DD:39FB:A0B2:800A	2016-12-01 08:42:31

รูปที่ 4-5 ข้อมูลที่ถูกเพิ่มจากสคริปต์จากการเรียกข้อมูลจาก L3 Switch

ตาราง permit จะเป็นตารางในการกำหนดสิทธิ์ของผู้ใช้คนนั้น ๆ ว่าจะเป็นผู้ดูแลระบบหรือไม่ โดยจะเก็บ user id ของตารางผู้ใช้งานของ RADIUS server ดังตารางที่ 4-1 ตาราง permit จากฐานข้อมูล

id	userid
1	1

ตารางที่ 4-1 ตาราง permit จากฐานข้อมูล

ตาราง ipRef จะเก็บข้อมูล IP Address ของเครื่องที่เชื่อมต่ออยู่ และ id ที่อ้างอิงตารางการลงชื่อเข้าใช้ของ radius server ดังตารางที่ 4-2 ตาราง ipRef จากฐานข้อมูล

id	radRefId	ip	dateTime
1	29	FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB	2016-09-03 12:57:01
2	29	172.30.231.6	2016-09-03 12:57:01
3	29	2001:03C8:9009:01E7:0900:7AD7:4AD0:856C	2016-09-03 12:57:01

ตารางที่ 4-2 ตาราง ipRef จากฐานข้อมูล

4.4 การทดสอบระบบในส่วนแสดงผล

ในส่วนนี้เป็นส่วนของเว็บแอปพลิเคชันที่นำข้อมูลจากฐานข้อมูลมาแสดงผล ในส่วนนี้เขียนขึ้นด้วยภาษา php และ html โดยมีการให้สิทธิ์ผู้ใช้เป็น 2 ส่วน คือ

1. ผู้ใช้ทั่วไป สามารถดูบันทึกของระบบบนส่วนที่เป็นของตัวเองได้ และสามารถพิมพ์ข้อมูลของตัวเองได้
2. ผู้ดูแลระบบ สามารถดูบันทึกการใช้งานของผู้ใช้ทั้งหมด พิมพ์ข้อมูล และสำรองข้อมูลการใช้งานได้

หน้า login ใช้ในการเข้าสู่ระบบ โดยเมื่อกรอกชื่อผู้ใช้ และรหัสผ่านที่ถูกต้อง ก็สามารถใช้งานได้ ตามสิทธิ์ของผู้ใช้คนนั้นดังรูปที่ 4-6 แสดงส่วนของเว็บสำหรับการเข้าสู่ระบบ

Please sign in

User Name

Password

Sign in

รูปที่ 4-6 แสดงส่วนของเว็บสำหรับการเข้าสู่ระบบ

สำหรับผู้ใช้งานทั่วไปเมื่อเข้ามาสู่ระบบแล้วจะสามารถดูข้อมูลการใช้ได้เฉพาะส่วนที่เป็นของตัวเอง โดยสามารถตัวกรองเพื่อกรองผลลัพธ์การแสดงผลได้ดังรูปที่ 4-7 แสดงส่วนของเว็บสำหรับการดูข้อมูลการบันทึกการใช้งานในมุมมองผู้ใช้งานทั่วไป

User Log Management System

User : IPv6 Permission : USER [logout](#)

User : IPv6
Permission : USER
[logout](#)

date time between and
 [Search](#) [Print](#)

Username	ACC time start	ACC time stop	Type	Device Vender	Physical Address	IP Address
IPv6	2016-12-01 16:38:47	2016-12-01 16:50:09	Ethernet	ASUSTek COMPUTER INC.	BC-EE-7B-53-4F-A0	172.30.231.17 2001:03C8:9009:01E7:4CB3:9FD0:4AB6:04C0 FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB
IPv6	2016-12-01 08:41:35	2016-12-01 08:44:06	Ethernet	ASUSTek COMPUTER INC.	BC-EE-7B-53-4F-A0	172.30.231.17 2001:03C8:9009:01E7:C8DD:39FB:A0B2:800A FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB

รูปที่ 4-7 แสดงส่วนของเว็บสำหรับการดูข้อมูลการบันทึกการใช้งานในมุมมองผู้ใช้งานทั่วไป

สำหรับผู้ดูแลระบบเมื่อเข้ามาสู่ระบบแล้วจะสามารถดูข้อมูลการใช้ได้ทั้งหมด โดยสามารถใช้ตัวกรองเพื่อกรองผลลัพธ์การแสดงผลได้ดังรูปที่ 4-8 แสดงของส่วนเว็บสำหรับการดูบันทึกการใช้งานในมุมมองผู้ดูแลระบบ

User Log Management System

User : tua Permission : ADMIN [logout](#)

User : tua
Permission : ADMIN
[logout](#)

userlog data
print report
backup / restore data
clean old data

date time between --:-- -- and --:-- --

[Search](#) [Print](#)

Username	ACC time start	ACC time stop	Type	Device Vender	Physical Address	IP Address
tua	2016-12-01 16:58:42	2016-12-01 18:06:06	Ethernet	ASUSTek COMPUTER INC.	BC-EE-7B-53-4F-A0	172.30.231.17 2001:03C8:9009:01E7:C02C:ADCF:5057:07D1 FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB
IPv6	2016-12-01 16:38:47	2016-12-01 16:50:09	Ethernet	ASUSTek COMPUTER INC.	BC-EE-7B-53-4F-A0	172.30.231.17 2001:03C8:9009:01E7:4CB3:9FD0:4AB6:04C0 FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB
tua	2016-12-01 13:53:32	2016-12-01 16:08:51	Ethernet	ASUSTek COMPUTER INC.	BC-EE-7B-53-4F-A0	172.30.231.17 2001:03C8:9009:01E7:2DE4:3908:E5BE:6B5E FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB
IPv6	2016-12-01	2016-12-01	Ethernet	ASUSTek	BC-EE-7B-	172.30.231.17

รูปที่ 4-8 แสดงของส่วนเว็บสำหรับการดูบันทึกการใช้งานในมุมมองผู้ดูแลระบบ

ผู้ดูแลระบบสามารถสำรองข้อมูลการลงชื่อเข้าใช้ หรือนำเข้าข้อมูลสำรองได้ โดยสามารถเลือกได้ ดังรูปที่ 4-9 แสดงส่วนของเว็บสำหรับการสำรองข้อมูลผู้ใช้ในมุมมองผู้ดูแลระบบ

User Log Management System

User : tua Permission : ADMIN [logout](#)

User : tua
Permission : ADMIN
[logout](#)

userlog data
print report
backup / restore data
clean old data

[สำรองข้อมูล](#)

หรือ

[Choose File](#) No file chosen

[นำเข้าข้อมูล](#)

รูปที่ 4-9 แสดงส่วนของเว็บสำหรับการสำรองข้อมูลผู้ใช้ในมุมมองผู้ดูแลระบบ

5. สรุปผลและข้อเสนอแนะ

5.1 สรุปผล

ในส่วนการทำงานของระบบในแต่ละส่วนสามารถทำงานได้ โดยส่วนเบื้องหลังโดยรวมสามารถทำงานได้โดยสามารถเรียกค่าจากตาราง ARP และตาราง ND โดยใช้ SNMP Protocol ได้และนำมาจับคู่กันตาม Physical Addressได้ และส่งข้อมูลไปยังฐานข้อมูลได้

ในส่วนของฐานข้อมูลก็ได้มีการออกแบบและทดลองใช้งานจากสคริปต์ที่เขียนขึ้นในส่วนแรกพบว่าสามารถทำงานได้สมบูรณ์ครบถ้วน

ในส่วนของเว็บแอปพลิเคชัน สามารถนำข้อมูลจากฐานข้อมูลมาแสดงผลได้ มีการแบ่งระดับสิทธิ์ผู้ใช้เป็น 2 ส่วนคือผู้ดูแลระบบ และผู้ใช้ทั่วไป โดยผู้ใช้ทั่วไปสามารถดูบันทึกของระบบบนส่วนที่เป็นของตัวเองได้เท่านั้น และผู้ดูแลระบบสามารถดูบันทึกการใช้งานของผู้ใช้ทั้งหมด สามารถสำรองข้อมูลหรือนำเข้าข้อมูลที่สำรองไว้ และสามารถลบข้อมูลการลงชื่อเข้าใช้ที่มีอายุเกินกว่าที่พบบ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์พ.ศ. 2550 กำหนดไว้ได้

5.2 ปัญหาและอุปสรรคและวิธีแก้ไข

1. การออกแบบวิธีการเรียกข้อมูลของหน้าเว็บทำได้ไม่ดีในครั้งแรก จึงทำให้ใช้เวลาในการเรียกหน้าการแสดงผลนานเกินไปจนไม่สามารถใช้งานได้อย่างสะดวก จึงต้องมีการแก้ไขรูปแบบวิธีการในภายหลังซึ่งทำให้เสียเวลาในการแก้ไขงานเพิ่มขึ้น

แนวทางแก้ไข วางแผนออกแบบให้รอบคอบขึ้น

2. ผู้เขียนไม่มีความรู้ในการตั้งค่าและปรับแต่งอุปกรณ์เพื่อการจำลองระบบสำหรับการทดสอบทำให้ใช้เวลามากในการเรียนรู้

แนวทางแก้ไข ศึกษาความรู้เพิ่มเติมในเรื่องที่เกี่ยวข้อง

3. ในช่วงแรกไม่มีการจัดการ source code ที่ดีทำให้มีการสูญหายไปบางส่วน จึงต้องมีการเขียนขึ้นมาใหม่

แนวทางแก้ไข ใช้ Git ช่วยในการจัดการ source code

4. ในส่วนของการพิมพ์รายงานเป็นไฟล์นามสกุล .pdf หากใช้ซอฟต์แวร์ช่วยดาวน์โหลด เช่น Internet Download Manager (IDM) อาจทำให้ไฟล์ที่ไม่สามารถเปิดดูได้อย่างถูกต้อง

แนวทางแก้ไข หากเกิดปัญหาให้ทำการดาวน์โหลดโดยไม่ผ่านซอฟต์แวร์ช่วยดาวน์โหลด

5.3 ข้อเสนอแนะ

1. เนื่องจากระบบที่ได้ออกแบบใช้วิธีการตรวจสอบแบบ polling คือการตรวจสอบเป็นรอบ ๆ จึงทำให้ความแม่นยำของข้อมูลขึ้นกับความถี่ของการตรวจสอบ
2. ในส่วนของสคริปต์เรียกข้อมูลจากอุปกรณ์ Layer3 Switch ควรทำให้สามารถทำงานเป็น daemon service และเริ่มทำงานเองได้เมื่อเปิดเครื่อง
3. Layer3 Switch ที่ใช้จำเป็นต้องสนับสนุน SNMP ในส่วนของ IP-MIB เพื่อใช้คำสั่ง IP-MIB::ipNetToPhysicalPhysAddress และ IP-MIB::ipNetToMediaPhysAddress

6. เอกสารอ้างอิง

- [1] “faq: ipv6.nectec.or.th,” [ออนไลน์]. Available:
<http://www.ipv6.nectec.or.th/faq.php#ans1>. (เข้าชมเมื่อ 25/11/2014)

- [2] “ข้อแตกต่างของ Hub, Switch Layer 2 และ 3,” [ออนไลน์]. Available:
http://www.greattelecom.co.th/article_detail.php?article_id=10.
 (เข้าชมเมื่อ 25/11/2014)

- [3] “แนะนำภาษา PERL,” [ออนไลน์]. Available:
<http://www.mindsind.s5.com/form/2Lenarning/web/w4/Untitled-1.htm>.
 (เข้าชมเมื่อ 25/11/2014)

- [4] “มารู้จักโปรโตคอล SNMP (ตอนที่ 1),” [ออนไลน์]. Available:
<http://www.thailandindustry.com/guru/view.php?id=14294§ion=9>.
 (เข้าชมเมื่อ 25/11/2014)

- [5] “CCNP Practical Studies: Layer3 Switching,” [ออนไลน์]. Available:
<http://www.ciscopress.com/articles/article.asp?p=102093>. (เข้าชมเมื่อ 25/11/2014)

- [6] “ข้อแตกต่างของ Hub, Switch Layer 2 และ 3,” [ออนไลน์]. Available:
<http://www.it-clever.com/%E0%B8%82%E0%B9%89%E0%B8%AD%E0%B9%81%E0%B8%95%E0%B8%81%E0%B8%95%E0%B9%88%E0%B8%B2%E0%B8%87%E0%B8%82%E0%B8%AD%E0%B8%87-hub-Switch-layer-2-%E0%B9%81%E0%B8%A5%E0%B8%B0-3/>. (เข้าชมเมื่อ 25/11/2014)

- [7] “ความรู้IPv6 พื้นฐานสำหรับผู้ดูแลระบบ,” [ออนไลน์]. Available:
<http://www.thailandipv6.net/ebook/IPv6book20140826.pdf>. (เข้าชมเมื่อ 25/11/2014)

- [8] “SNMPv1,” [ออนไลน์]. Available: <https://sites.google.com/site/snmphorus/snmpv1>.
 (เข้าชมเมื่อ 25/11/2014)

- [9] “ARP คืออะไร,” [ออนไลน์]. Available:
<http://www.com5dow.com/%E0%B9%84%E0%B8%82%E0%B8%9B%E0%B8%B1%E0%B8%8D%E0%B8%AB%E0%B8%B2%E0%B8%A8%E0%B8%B1%E0%B8%9E%E0%B8%97%E0%B9%8C-it/675-arp-%E0%B8%84%E0%B8%B7%E0%B8%AD%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3.html>. (เข้าชมเมื่อ 25/11/2014)

- [10] “IP คืออะไร,” [ออนไลน์]. Available:
<http://www.com5dow.com/%E0%B9%84%E0%B8%82%E0%B8%9B%E0%B8%B1%E0%B8%8D%E0%B8%AB%E0%B8%B2%E0%B8%A8%E0%B8%B1%E0%B8%9E%E0%B8%97%E0%B9%8C-it/1236-ip-%E0%B8%84%E0%B8%B7%E0%B8%AD%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3.html>. (เข้าชมเมื่อ 25/11/2014)
- [11] “SQL คืออะไร,” [ออนไลน์]. Available:
<http://www.mindphp.com/%E0%B8%84%E0%B8%B9%E0%B9%88%E0%B8%A1%E0%B8%B7%E0%B8%AD/73-%E0%B8%84%E0%B8%B7%E0%B8%AD%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3/2088-sql-%E0%B8%84%E0%B8%B7%E0%B8%AD%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3.html>. (เข้าชมเมื่อ 25/11/2014)
- [12] “PHP คืออะไร,” [ออนไลน์]. Available:
<http://www.mindphp.com/%E0%B8%84%E0%B8%B9%E0%B9%88%E0%B8%A1%E0%B8%B7%E0%B8%AD/73-%E0%B8%84%E0%B8%B7%E0%B8%AD%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3/2127-php-%E0%B8%84%E0%B8%B7%E0%B8%AD%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3.html>. (เข้าชมเมื่อ 25/11/2014)
- [13] “FreeRADIUS,” [ออนไลน์]. Available: <http://freeradius.org/> (เข้าชมเมื่อ 27/11/2014)
- [14] “Freeradius คืออะไร,” [ออนไลน์]. Available:
<https://beeooz.wordpress.com/2010/09/04/freeradius-%E0%B8%84%E0%B8%B7%E0%B8%AD%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3/>
 (เข้าชมเมื่อ 27/11/2014)
- [15] “RADIUS คือ อะไร,” [ออนไลน์]. Available: <http://www.thaiatl.com/blog/burin/5317/>
 (เข้าชมเมื่อ 27/11/2014)

7. ภาคผนวก

7.1 วิธีการติดตั้ง

3.2.4 7.1.1 ติดตั้ง LAMP stack และ phpMyAdmin

LAMP เป็นตัวอักษรย่อของโอเพ่นซอร์สซอฟต์แวร์ 4 ชนิดมารวมกันเพื่อทำหน้าที่เป็นเครื่องให้บริการเว็บ (Web Server) อันประกอบด้วย Linux, Apache, mySQL และ PHP

ติดตั้ง Apache

เปิด terminal แล้วใช้คำสั่ง

```
$sudo apt-get update
```

```
$sudo apt-get install apache2
```

ทดสอบหลังการติดตั้งเปิดโปรแกรมเว็บเบราว์เซอร์แล้วพิมพ์ IP Address ของเซิร์ฟเวอร์ เช่น <http://localhost> จะปรากฏหน้าจอดังรูปที่ 7-1 ตัวอย่างการทดสอบการทำงานของ Apache

It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

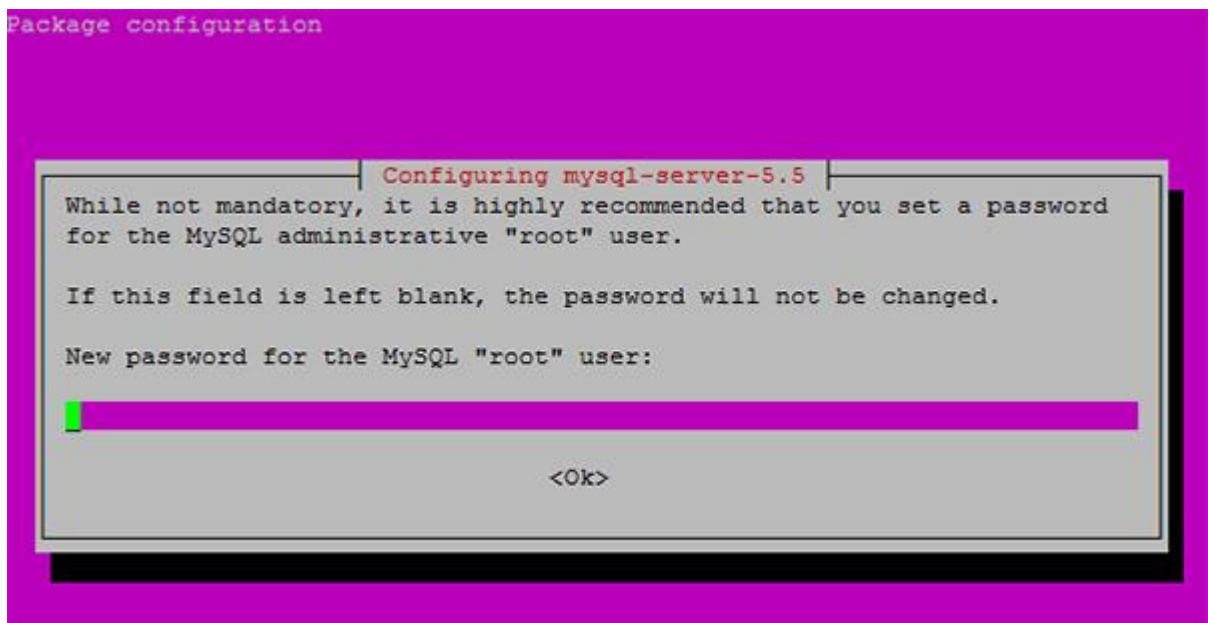
รูปที่ 7-1 ตัวอย่างการทดสอบการทำงานของ Apache

ติดตั้ง MySQL

เปิด terminal แล้วใช้คำสั่ง

```
$sudo apt-get install mysql -server mysql -client
```

ระหว่างการติดตั้งจะมีให้กรอกรหัสผ่านสำหรับ root ของ MySQL ให้ทำการกำหนดตามที่ต้องการดังรูปที่ 7-2 การติดตั้ง MySQL



รูปที่ 7-2 การติดตั้ง MySQL

ติดตั้ง PHP

เปิด terminal แล้วใช้คำสั่ง

```
$sudo apt-get install php5 libapache2-mod-php5
```

ทดสอบการติดตั้ง PHP

Restart Apache2

```
$service apache2 restart
```

สร้างไฟล์ทดสอบ โดยการเรียก php info ขึ้นมาแสดง

```
$nano var/www/phpinfo.php
```


จากนั้นพิมพ์คำสั่ง PHP ดังนี้

```
<?PHP

    phpinfo();

?>
```

บันทึกแล้วทดสอบโดยการเปิดโปรแกรมเว็บเบราว์เซอร์แล้วพิมพ์ IP Address ของเซิร์ฟเวอร์/phpinfo.php เช่น <http://localhost/phpinfo.php> จะปรากฏหน้าจอ ดังรูปที่ 7-3 การทดสอบการทำงานของ php

<div> PHP Version 5.3.10-1ubuntu3.9  </div>	
System	Linux demo 3.5.0-23-generic #35~precise1-Ubuntu SMP Fri Jan 25 17:15:33 UTC 2013 i686
Build Date	Dec 12 2013 04:06:44
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2

รูปที่ 7-3 การทดสอบการทำงานของ php

ติดตั้ง Packets อื่น ๆ เพื่อให้ PHP สนับสนุน MySQL รวมไปถึงส่วนประกอบอื่น ๆ ที่สำคัญสำหรับ PHP

เปิด terminal แล้วใช้คำสั่ง

```
$sudo apt-get install php5-mysql php5-curl php5-gd php5-intl php-pear php5-imagick php5-imap php5-mcryptphp5-memcache php5-ming php5-ps php5-pspell php5-recode php5-snmp php5-sqlite php5-tidy php5-xmlrpc php5-xsl
```

3.2.5 7.1.2.สร้างฐานข้อมูล

สร้างฐานข้อมูล และตารางโดยการ พิมพ์คำสั่ง

```
$mysql -u root -p

mysql > CREATE DATABASE ชื่อฐานข้อมูล

CREATE TABLE IF NOT EXISTS `ipRef` (

  `id` bigint(20) NOT NULL AUTO_INCREMENT,

  `radRefId` bigint(20) NOT NULL,

  `ip` varchar(50) NOT NULL,

  `dateTime` datetime DEFAULT NULL,

  PRIMARY KEY (`id`)

CREATE TABLE IF NOT EXISTS `permit` (

  `id` int(11) NOT NULL AUTO_INCREMENT,

  `userid` varchar(50) NOT NULL,

  PRIMARY KEY (`id`)

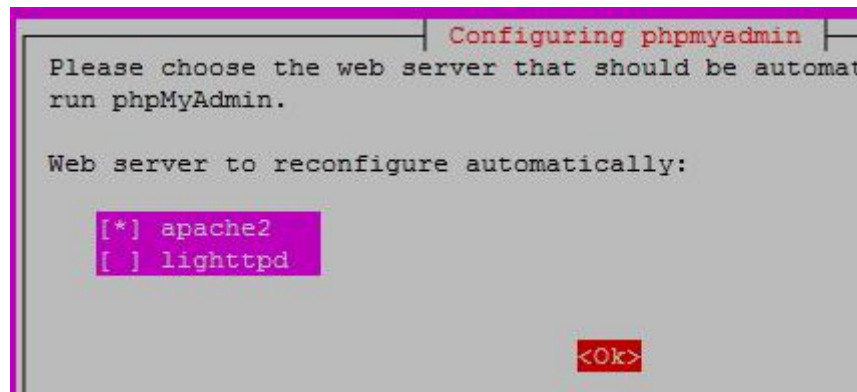
);
```

ติดตั้ง phpMyAdmin

เปิด terminal แล้วใช้คำสั่ง

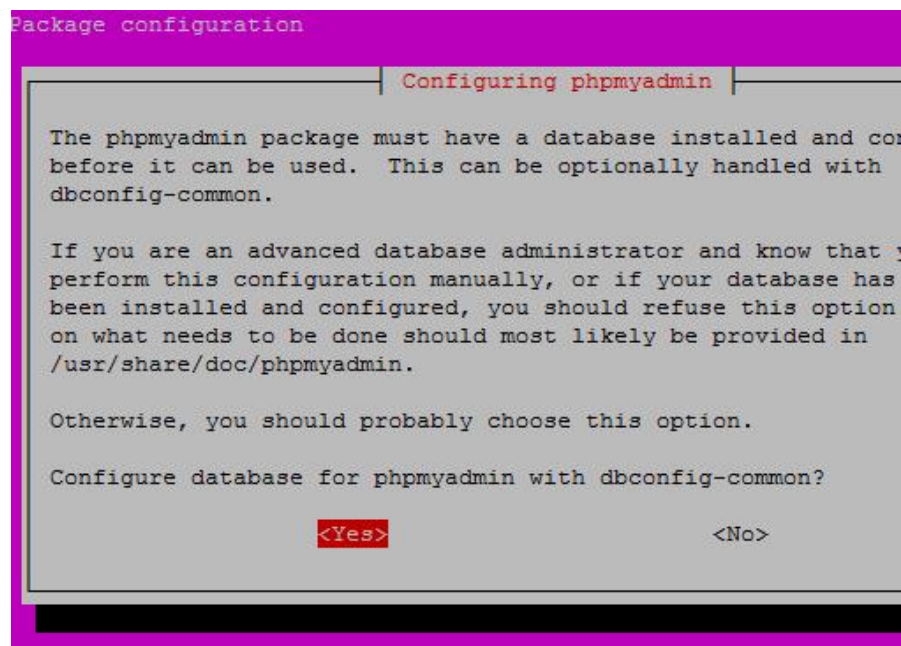
```
$sudo apt-get install phpmyadmin
```

เลือก Apache2 ดังรูปที่ 7-4 การติดตั้ง phpMyAdmin



รูปที่ 7-4 การติดตั้ง phpMyAdmin

เลือก YES จากนั้นกำหนด Password ให้กับ Account สำหรับ mySQL ตามที่ต้องการ ดังรูปที่ 7-5 การติดตั้ง phpMyAdmin



รูปที่ 7-5 การติดตั้ง phpMyAdmin

Restart Apache โดยการพิมพ์คำสั่ง

```
$sudo service apache2 restart
```

ทดสอบการติดตั้ง phpmyadmin เปิดโปรแกรมเว็บเบราว์เซอร์แล้วพิมพ์ IP Address ของเซิร์ฟเวอร์ /phpmyadmin เช่น <http://localhost/phpmyadmin> จะปรากฏหน้าจอตั้งรูปที่ 7-6 แสดงเว็บของ phpMyAdmin



รูปที่ 7-6 แสดงเว็บของ phpMyAdmin

3.2.6 7.1.3.ติดตั้ง screen

Screen เป็นเครื่องมือที่ช่วยในการสั่งให้โปรแกรมทำงานอยู่ โดยไม่ต้องเปิดหน้าต่าง terminal หรือ session ค้างไว้ได้

```
$sudo apt-get update
$sudo apt-get install screen
```

3.2.7 7.1.4.คัดลอกไฟล์ websize

คัดลอกไฟล์ webpage ต่าง ๆ ไปที่ /var/www/

ทดสอบหลังการติดตั้งเปิดโปรแกรมเว็บเบราว์เซอร์แล้วพิมพ์ IP Address ของเซิร์ฟเวอร์ เช่น <http://localhost> จะปรากฏหน้าจอตั้งรูปที่ 7-7 แสดงเว็บในส่วนของการลงชื่อเข้าใช้ของระบบ

รูปที่ 7-7 แสดงเว็บในส่วนของลงชื่อเข้าใช้ของระบบ

3.2.8 7.1.5.การตั้งค่าเพื่อสั่งงานโปรแกรม

แก้ไขไฟล์ psulog ข้อมูลการเชื่อมต่อให้ถูกต้อง

```

11 ##### basic config #####
12 my $switch_v6address = "2001:3c8:9009:181::1";
13 my $interval = 60; # time interval between pooling round in second unit.
14
15
16 ##### MYSQL CONFIG VARIABLES #####
17 my $driver = "mysql";
18
19 my $radhost = "localhost"; # radius server ip address.
20 my $raduserid = "root"; # username to access database .
21 my $radpassword = "kks*5cvp768"; # password for access database.
22 my $raddatabase = "radius";
23
24
25 my $loghost = "localhost"; # log server ip address.
26 my $loguserid = "root"; # username to access logdatabase .
27 my $logpassword = "kks*5cvp768"; # password for access logdatabase.
28 my $logdatabase = "proj";
29
30 #####

```

รูปที่ 7-8 ส่วนการตั้งค่าการเชื่อมต่อฐานข้อมูล

3.2.9 7.1.6.การสั่งรันโปรแกรม

ที่ตำแหน่งที่อยู่ ไฟล์ psulog ใช้คำสั่ง

\$screen

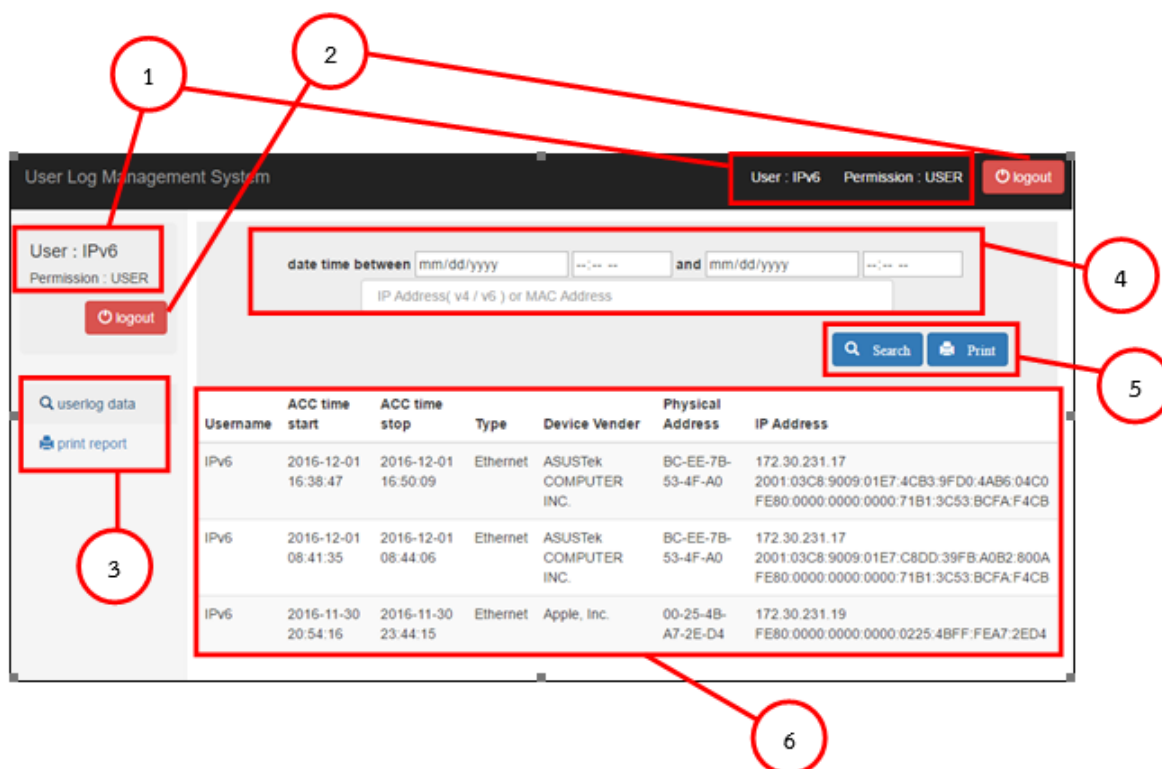
\$/psulog

กด Ctrl+A แล้วกด D

7.2 คู่มือการใช้งาน

3.2.10 7.2.1. การใช้งานของผู้ใช้ทั่วไป

เมื่อเปิดหน้า web page ขึ้นมาจะพบกับหน้า login ให้ทำการกรอกชื่อผู้ใช้ และรหัสผ่านให้ถูกต้อง จากนั้นคลิกที่ปุ่ม Sign in หลังจากทำการ Sign in แล้ว หากมีสิทธิ์การใช้งานเป็น user จะพบกับหน้าต่าง ดังรูปที่ 7-9 ส่วนแสดงข้อมูลผู้ใช้ในมุมมองผู้ใช้ทั่วไป



รูปที่ 7-9 ส่วนแสดงข้อมูลผู้ใช้ในมุมมองผู้ใช้ทั่วไป

โดยแต่ละส่วนคือ

หมายเลข 1 คือ ข้อมูลผู้ใช้ที่กำลังใช้งานหน้าเว็บในปัจจุบัน

หมายเลข 2 คือ ปุ่มการลงชื่อออก

หมายเลข 3 คือ เมนูคำสั่ง

หมายเลข 4 คือ ช่องตัวกรองข้อมูล

หมายเลข 5 คือ ปุ่มสำหรับการกรองข้อมูล และพิมพ์ข้อมูล

หมายเลข 6 คือ ช่องแสดงข้อมูลการลงชื่อเข้าใช้

ดูข้อมูลการใช้ของตนเอง

หลังจากทำการ Sign in แล้ว หากมีสิทธิ์การใช้งานเป็น user จะพบกับหน้าต่างดังรูปที่ 7-9 ส่วนแสดงข้อมูลผู้ใช้ในมุมมองผู้ใช้ทั่วไป หรือหากอยู่ที่เมนูอื่นสามารถเข้าเมนูได้โดยการเลือก userlog data จากเมนูหมายเลข 3

ผู้ใช้สามารถดูข้อมูลการเชื่อมต่อของตนเอง และสามารถกรองข้อมูลได้ด้วยส่วนของตัวกรองข้อมูลในหมายเลข 4 โดยการกรอกข้อมูลตัวกรอง แล้วคลิกที่ปุ่ม Search จากหมายเลข 5

The screenshot displays the 'User Log Management System' interface. At the top, it shows 'User : IPv6' and 'Permission : USER' with a 'logout' button. The main area contains a search filter for 'date time between' with input fields for 'mm/dd/yyyy' and a time range '172.30.231.17'. Below the filter is a table of user login data.

Username	ACC time start	ACC time stop	Type	Device Vender	Physical Address	IP Address
IPv6	2016-12-01 16:38:47	2016-12-01 16:50:09	Ethernet	ASUSTek COMPUTER INC.	BC-EE-7B-53-4F-A0	172.30.231.17 2001:03C8:9009:01E7:4CB3:9FD0:4AB6:04C0 FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB
IPv6	2016-12-01 08:41:35	2016-12-01 08:44:06	Ethernet	ASUSTek COMPUTER INC.	BC-EE-7B-53-4F-A0	172.30.231.17 2001:03C8:9009:01E7:C8DD:39FB:A0B2:800A FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB

รูปที่ 7-10 ผลลัพธ์การกรองข้อมูล

การพิมพ์ข้อมูลการใช้ของตนเอง

หากผู้ใช้ต้องการพิมพ์ข้อมูลการใช้ของตนเอง สามารถกรองข้อมูลได้ด้วยส่วนตัวกรองข้อมูลใน หมายเลข 4 จากนั้นคลิกที่ปุ่ม Print หมายเลข 5

printnow.php 1 / 1

ข้อมูลการเชื่อมต่อ และหมายเลข IP Address
ของผู้ใช้ IPv6
พิมพ์ข้อมูลเมื่อ : 2016-12-18 17:25:36

Username	ACC time start	ACC time stop	Type	Device Vender	Physical Address	IP Address
IPv6	2016-12-01 16:38:47	2016-12-01 16:50:09	Ethernet	ASUSTek COMPUTER INC.	BC-EE-7B-53-4F-A0	172.30.231.17 2001:03C8:9009:01E7:4CB3:9FD0:4AB6:04C0 FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB
IPv6	2016-12-01 08:41:35	2016-12-01 08:44:06	Ethernet	ASUSTek COMPUTER INC.	BC-EE-7B-53-4F-A0	172.30.231.17 2001:03C8:9009:01E7:C8DD:39FB:A0B2:800A FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB
IPv6	2016-11-30 20:54:16	2016-11-30 23:44:15	Ethernet	Apple, Inc.	00-25-4B-A7-2E-D4	172.30.231.19 FE80:0000:0000:0000:0225:4BFF:FEA7:2ED4

+
-

รูปที่ 7-11 ตัวอย่างข้อมูลพร้อมพิมพ์ในรูปแบบนามสกุล .pdf

เมื่อผู้ใช้พิมพ์ข้อมูลของตนเอง จะได้ข้อมูลดังรูปที่ 7-11 ตัวอย่างข้อมูลพร้อมพิมพ์ในรูปแบบนามสกุล .pdf ซึ่งแสดงข้อมูลการเชื่อมต่อและ IP Address ของผู้ใช้งาน

การพิมพ์ข้อมูลของตัวเองย้อนหลังตามจำนวน วัน/เดือน/ปี

ผู้ใช้งานสามารถพิมพ์ข้อมูลย้อนหลังตามจำนวน วัน/เดือน/ปี ได้โดยการคลิกที่เมนู print report จากส่วนหมายเลข 3 จะพบกับหน้าต่างดังรูปที่ 7-12 ส่วนเลือกช่วงเวลาข้อมูลย้อนหลังที่ต้องการพิมพ์

The screenshot shows the 'User Log Management System' interface. At the top, it displays 'User : IPv6' and 'Permission : USER' with a 'logout' button. On the left sidebar, there are options for 'userlog data' and 'print report'. The main area contains a form for selecting a time range. It has radio buttons for '1 วันที่ผ่านมา', '1 สัปดาห์ที่ผ่านมา', '1 เดือนที่ผ่านมา', '1 ปีที่ผ่านมา', and '2 ปีที่ผ่านมา'. There is also a 'ระหว่างวันที่' (from) and 'ถึง' (to) section with input fields for 'mm/dd/yyyy'. A 'Print' button is located at the bottom right of the form.

รูปที่ 7-12 ส่วนเลือกช่วงเวลาข้อมูลย้อนหลังที่ต้องการพิมพ์

ผู้ใช้งานสามารถเลือกระยะเวลาการเข้าใช้งาน หรือเลือก วัน/เดือน/ปี ที่กำหนดเอง จากนั้นคลิกที่ปุ่ม Print เพื่อทำการพิมพ์ข้อมูลที่ต้องการ

The screenshot shows the 'report.php' page with a title 'รายงานการเชื่อมต่อ และหมายเลข IP Address' (Connection Report and IP Address Number). Below the title, it specifies 'ของผู้ใช้ IPv6 ระหว่างวันที่ 1916-12-18 ถึง 2016-12-18' (for IPv6 user from 1916-12-18 to 2016-12-18) and 'พิมพ์ข้อมูลเมื่อ : 2016-12-18 10:35:39' (print data at: 2016-12-18 10:35:39). The table below contains the following data:

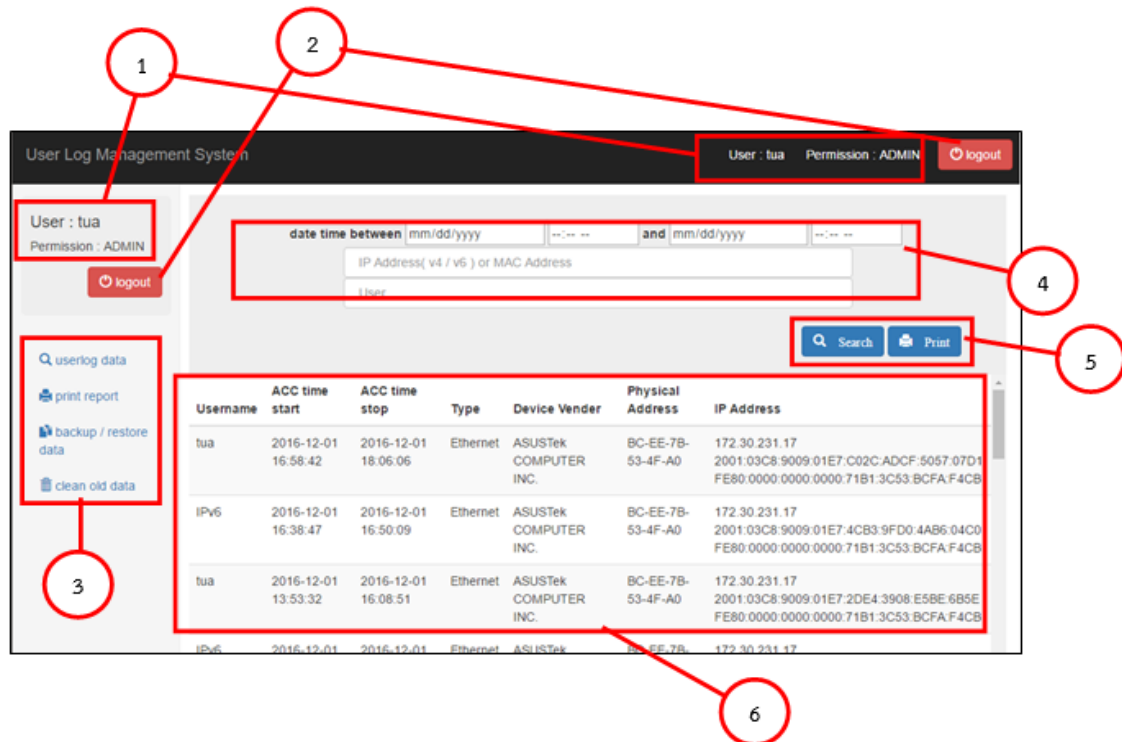
Username	ACC time start	ACC time stop	Type	Device Vender	Physical Address	IP Address
IPv6	2016-11-30 20:54:16	2016-11-30 23:44:15	Ethernet	Apple, Inc.	00-25-4B-A7-2E-D4	172.30.231.19 FE80:0000:0000:0000:0225:4BFF:FEA7:2ED4
IPv6	2016-12-01 08:41:35	2016-12-01 08:44:06	Ethernet	ASUSTek COMPUTER INC.	BC-EE-7B-53-4F-A0	172.30.231.17 2001:03C8:9009:01E7:C8DD:39FB:A0B2:800A FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB
IPv6	2016-12-01 16:38:47	2016-12-01 16:50:09	Ethernet	ASUSTek COMPUTER INC.	BC-EE-7B-53-4F-A0	172.30.231.17 2001:03C8:9009:01E7:4CB3:9FD0:4AB6:04C0 FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB

รูปที่ 7-13 ตัวอย่างรายงานพร้อมพิมพ์จากเมนู print report

เมื่อผู้ใช้พิมพ์ข้อมูลของตนเองย้อนหลัง จะได้ข้อมูลดังรูปที่ 7-13 ตัวอย่างรายงานพร้อมพิมพ์จากเมนู print report ซึ่งแสดงข้อมูลการใช้งานตามระยะเวลาที่ผู้ใช้เลือก วัน/เดือน/ปี

3.2.11 7.1.2. การใช้งานของผู้ดูแลระบบ

เมื่อผู้ดูแลระบบเปิดหน้า web page จะพบกับหน้า login ให้ทำการกรอกชื่อผู้ใช้ และรหัสผ่านให้ถูกต้องจากนั้นคลิกที่ปุ่ม Sign in



รูปที่ 7-14 ส่วนแสดงข้อมูลผู้ใช้ในมุมมองผู้ดูแลระบบ

โดยแต่ละส่วนคือ

หมายเลข 1 คือ ข้อมูลผู้ใช้ที่กำลังใช้งานหน้าเว็บในปัจจุบัน

หมายเลข 2 คือ ปุ่มการลงชื่อออก

หมายเลข 3 คือ เมนูคำสั่ง

หมายเลข 4 คือ ช่องตัวกรองข้อมูล

หมายเลข 5 คือ ปุ่มสำหรับการกรองข้อมูล และพิมพ์ข้อมูล

หมายเลข 6 คือ ช่องแสดงข้อมูลการลงชื่อเข้าใช้

ดูข้อมูลการใช้ของผู้ใช้

หลังจากทำการ Sign in แล้ว จะพบกับหน้าต่างดังรูปที่ 7-14 ส่วนแสดงข้อมูลผู้ใช้ในมุมมองผู้ดูแลระบบ หรือหากอยู่ที่เมนูอื่นสามารถเข้าเมนูได้โดยการเลือก userlog data จากเมนูหมายเลข 3

ผู้ดูแลระบบสามารถดูข้อมูลการเชื่อมต่อของผู้ใช้และสามารถกรองข้อมูลได้ด้วยส่วนของตัวกรองข้อมูลในหมายเลข 4 โดยการกรอกข้อมูลตัวกรอง แล้วคลิกที่ปุ่ม Search จากหมายเลข 5

การพิมพ์ข้อมูล

ผู้ดูแลระบบสามารถพิมพ์ข้อมูลการเชื่อมต่อของผู้ใช้และสามารถกรองข้อมูลได้ด้วยส่วนของตัวกรองข้อมูลหมายเลข 4 และพิมพ์ข้อมูลด้วยการคลิกปุ่ม Print จากส่วนหมายเลข 5

printnow.php 1 / 3

ข้อมูลการเชื่อมต่อ และหมายเลข IP Address
พิมพ์ข้อมูลเมื่อ : 2016-12-18 17:49:46

Username	ACC time start	ACC time stop	Type	Device Vender	Physical Address	IP Address
tua	2016-12-01 16:58:42	2016-12-01 18:06:06	Ethernet	ASUSTek COMPUTER INC.	BC-EE-7B-53-4F-A0	172.30.231.17 2001:03C8:9009:01E7:C02C:ADCF:5057:07D1 FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB
IPv6	2016-12-01 16:38:47	2016-12-01 16:50:09	Ethernet	ASUSTek COMPUTER INC.	BC-EE-7B-53-4F-A0	172.30.231.17 2001:03C8:9009:01E7:4CB3:9FD0:4AB6:04C0 FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB
tua	2016-12-01 13:53:32	2016-12-01 16:08:51	Ethernet	ASUSTek COMPUTER INC.	BC-EE-7B-53-4F-A0	172.30.231.17 2001:03C8:9009:01E7:2DE4:3908:E5BE:6B5E FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB
IPv6	2016-12-01 08:41:35	2016-12-01 08:44:06	Ethernet	ASUSTek COMPUTER INC.	BC-EE-7B-53-4F-A0	172.30.231.17 2001:03C8:9009:01E7:C8DD:39FB:A0B2:800A FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB
tua	2016-12-01 03:54:18	2016-12-16 17:52:55	Ethernet	Apple, Inc.	00-25-4B-A7-2E-D4	172.30.231.19 FE80:0000:0000:0000:0225:4BFF:FEA7:2ED4

รูปที่ 7-15 ตัวอย่างข้อมูลพร้อมพิมพ์ในรูปแบบนามสกุล .pdf

เมื่อผู้ดูแลระบบพิมพ์ข้อมูลการเชื่อมต่อ จะได้ข้อมูลดังรูปที่ 7-15 ตัวอย่างข้อมูลพร้อมพิมพ์ในรูปแบบนามสกุล .pdf ซึ่งจะแสดงข้อมูลการเชื่อมต่อของผู้ใช้ตามตัวกรองที่เลือก

การพิมพ์ข้อมูลย้อนหลังตามจำนวน วัน/เดือน/ปี

ผู้ใช้งานสามารถพิมพ์ข้อมูลย้อนหลังตามจำนวน วัน/เดือน/ปี ได้โดยการคลิกที่เมนู print report จากส่วนหมายเลข 3 จะพบกับหน้าต่างดังรูปที่ 7-16 ส่วนสำหรับเลือกช่วงเวลาข้อมูลย้อนหลังที่ต้องการพิมพ์

รูปที่ 7-16 ส่วนสำหรับเลือกช่วงเวลาข้อมูลย้อนหลังที่ต้องการพิมพ์

ผู้ดูแลระบบสามารถเลือกระยะเวลาการเชื่อมต่อ โดยการคลิกที่ช่องระยะเวลาหรือเลือก วัน/เดือน/ปี ที่กำหนดเอง จากนั้นคลิกที่ปุ่ม Print หมายเลข 5 เพื่อทำการพิมพ์ข้อมูลการเชื่อมต่อที่ต้องการ

Username	ACC time start	ACC time stop	Type	Device Vender	Physical Address	IP Address
tua	2016-11-28 15:51:16	2016-11-30 16:43:36	Ethernet	ASUSTek COMPUTER INC.	BC-EE-7B-53-4F-A0	172.30.231.17 2001:03C8:9009:01E7:D421:C472:D16C:4F27 FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB
tua	2016-11-30 20:01:28	2016-11-30 20:03:43	Ethernet	ASUSTek COMPUTER INC.	BC-EE-7B-53-4F-A0	172.30.231.17 2001:03C8:9009:01E7:71B1:3C53:BCFA:F4CB 2001:03C8:9009:01E7:EC9C:C6A7:6A8E:3456 FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB
tua	2016-11-30 20:04:37	2016-11-30 20:27:53	Ethernet	ASUSTek COMPUTER INC.	BC-EE-7B-53-4F-A0	172.30.231.17 2001:03C8:9009:01E7:3516:D942:4530:0760 2001:03C8:9009:01E7:71B1:3C53:BCFA:F4CB FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB
tua	2016-11-30 20:42:20	2016-12-01 08:41:00	Ethernet	ASUSTek COMPUTER INC.	BC-EE-7B-53-4F-A0	172.30.231.17 2001:03C8:9009:01E7:2D2F:FB08:6629:15E9 2001:03C8:9009:01E7:71B1:3C53:BCFA:F4CB

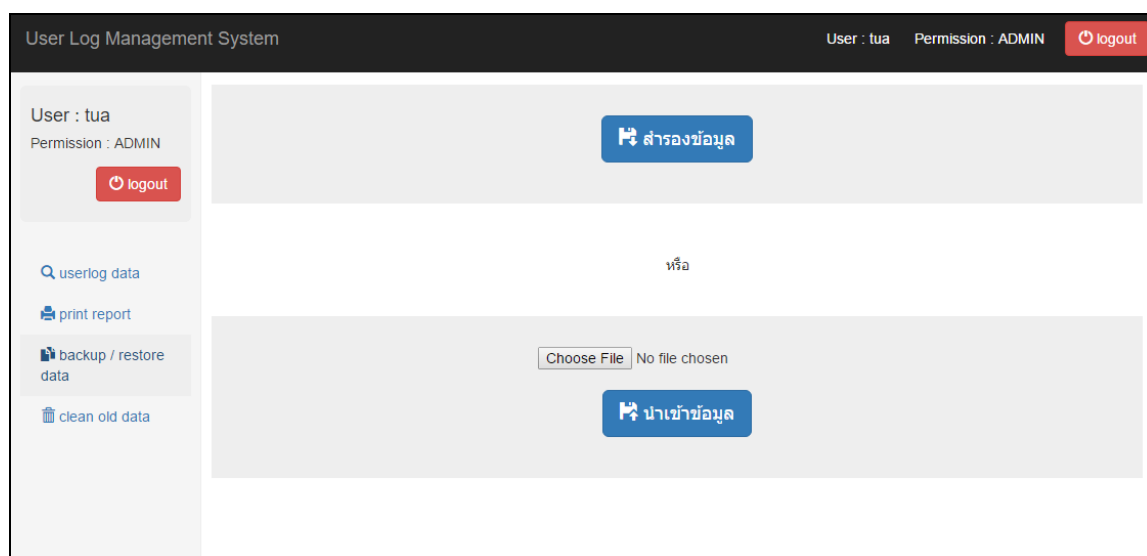
รูปที่ 7-17 ตัวอย่างรายงานพร้อมพิมพ์จากเมนู print report

เมื่อผู้ดูแลระบบพิมพ์ข้อมูลการเชื่อมต่อ จะได้ข้อมูลดังรูปที่ 7-17 ตัวอย่างรายงานพร้อมพิมพ์จากเมนู print report ซึ่งแสดงข้อมูลการเชื่อมต่อตามระยะเวลาหรือวัน/เดือน/ปี ที่กำหนด

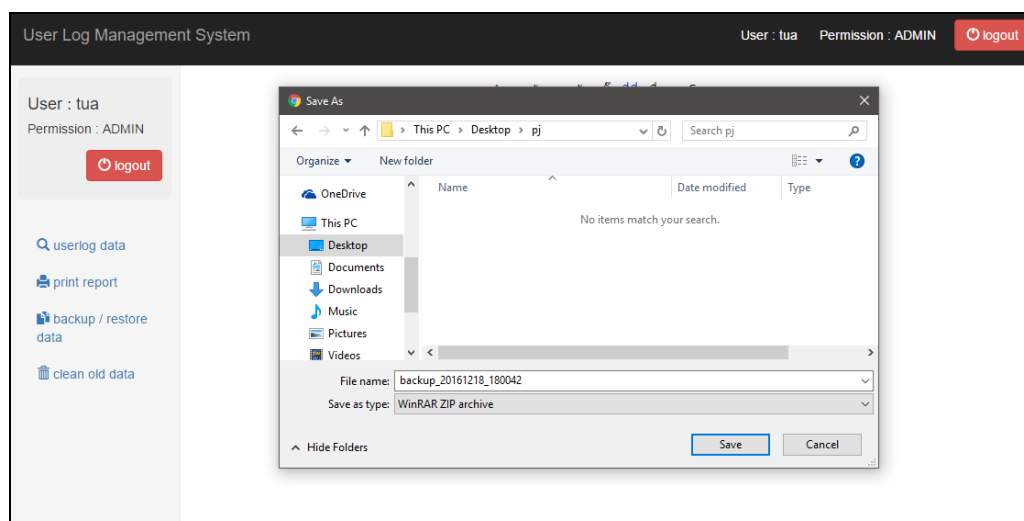
การสำรองข้อมูล และ การนำเข้าข้อมูลสำรอง

ผู้ดูแลระบบสามารถคลิกที่ปุ่ม backup/restore data จากเมนูในส่วนของหมายเลข 3 จะพบหน้าต่างดังรูปที่ 7-18 ส่วนของเมนู backup and restore data

ผู้ดูแลระบบสามารถเก็บสำรองข้อมูลการเชื่อมต่อของผู้ใช้งาน โดยการคลิกที่ปุ่มสำรองข้อมูล เลือกตำแหน่งเก็บไฟล์และกดปุ่ม save เพื่อยืนยันการเก็บสำรองข้อมูล



รูปที่ 7-18 ส่วนของเมนู backup and restore data

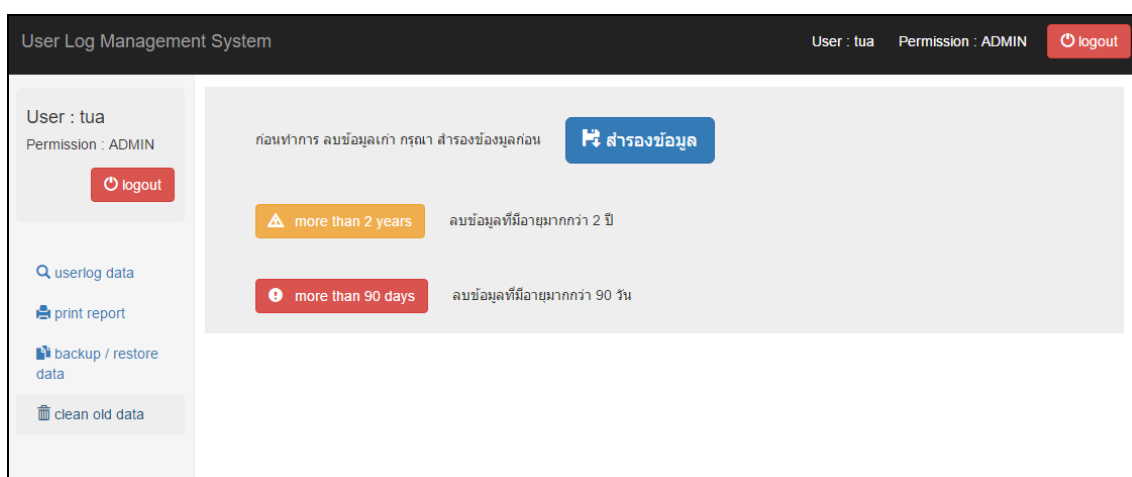


รูปที่ 7-19 ตัวอย่างการสำรองข้อมูล

ผู้ดูแลระบบสามารถสำรองข้อมูลและนำเข้าข้อมูลที่เคยมีการสำรองไว้จากเมนูสำรองข้อมูลได้ในกรณี
ที่จำเป็น โดยการคลิกที่ปุ่ม Choose File แล้วเลือกไฟล์ข้อมูลสำรอง จากนั้นกดปุ่มนำเข้าข้อมูล

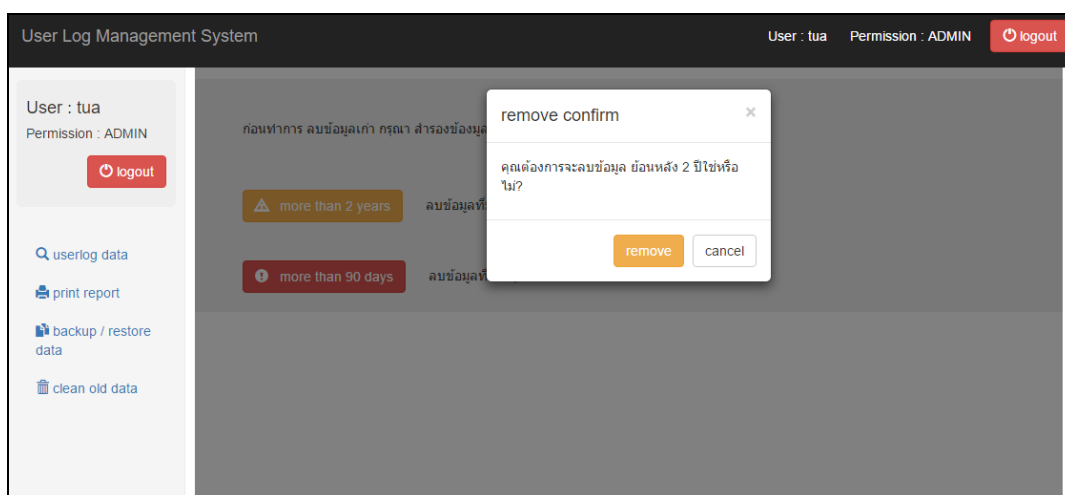
การล้างข้อมูลเก่า

ผู้ดูแลระบบสามารถลบข้อมูลการเชื่อมต่อของผู้ใช้งานที่มีการเก็บข้อมูลที่มีอายุมากกว่า 90 วัน หรือ
2 ปี ได้โดยการเข้าไปที่เมนู clean old data ในส่วนของหมายเลข 3 จะพบหน้าต่างดังรูปที่ 7-20 แสดงส่วน
ของเมนู clean old data



รูปที่ 7-20 แสดงส่วนของเมนู clean old data

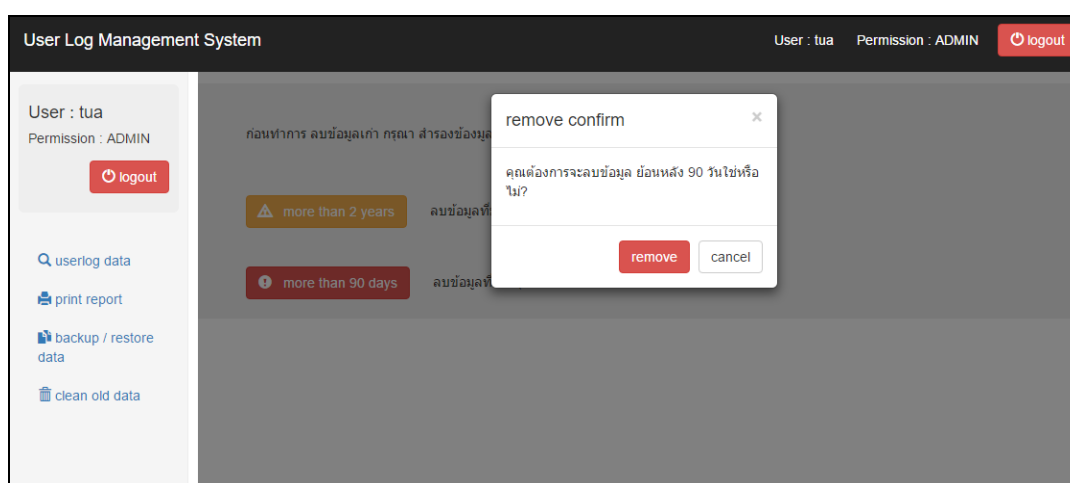
เมื่อผู้ดูแลระบบเข้าสู่เมนู clean old data คลิกที่ปุ่ม more than 2 years เพื่อลบข้อมูลที่มีอายุ
มากกว่า 2 ปี จะปรากฏหน้าต่าง remove confirm เพื่อเป็นการยืนยันก่อนการลบข้อมูลอีกครั้ง
ดังรูปที่ 7-21 แสดงส่วนยืนยันการลบข้อมูลที่มีอายุมากกว่า 2 ปี



รูปที่ 7-21 แสดงส่วนยืนยันการลบข้อมูลที่มีอายุมากกว่า 2 ปี

และผู้ดูแลระบบสามารถลบข้อมูลการเชื่อมต่อของผู้ใช้งานที่มีการเก็บข้อมูลเกิน 90 วัน โดยการเข้าไปที่เมนู clean old data ในส่วนของหมายเลข 3 จะพบหน้าต่างดังรูปที่ 7-22 แสดงส่วนการยืนยันการลบข้อมูลที่มีอายุมากกว่า 90 วัน

เมื่อผู้ดูแลพบหน้าต่างนี้ หากต้องการลบข้อมูลให้คลิกที่ปุ่ม more than 90 days และจะปรากฏหน้าต่างยืนยันการลบข้อมูลขึ้นมา เพื่อเป็นการยืนยันก่อนการลบข้อมูลอีกครั้งโดยคลิกปุ่ม confirm หรือหากไม่ต้องการลบให้กดปุ่ม cancel



รูปที่ 7-22 แสดงส่วนการยืนยันการลบข้อมูลที่มีอายุมากกว่า 90 วัน