

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

ผู้จัดทำที่ได้ลงนามทำยนี้ ขอรับรองว่ารายงานฉบับนี้เป็นรายงานที่มีความเป็นเอกลักษณ์ โดยที่ผู้จัดทำไม่ได้มีการคัดลอกมาจากที่ใดเลย เนื้อหาทั้งหมดถูกรวบรวมจากการพัฒนาในขั้นตอนต่าง ๆ ของการจัดทำโครงการ หากมีส่วนใดที่จำเป็นต้องนำเอาข้อความจากผลงานของผู้อื่น หรือบุคคลอื่นใดที่ไม่ใช่ตัวข้าพเจ้า ข้าพเจ้าได้ทำอ้างอิงถึงเอกสารเหล่านั้นไว้อย่างเหมาะสม และขอรับรองว่ารายงานฉบับนี้ไม่เคยเสนอต่อสถาบันใดมาก่อน

ผู้จัดทำ

.....

(นายจักรภูมิ มณีรัตน์)

โครงการนี้สำเร็จลงได้ด้วยความช่วยเหลือจาก อาจารย์ธัชชัย เอ็งฉ้วน อาจารย์ที่ปรึกษาโครงการที่ได้ให้แนวคิด คำปรึกษา คำแนะนำ และข้อเสนอแนะ ตลอดจนแนวทางในการแก้ปัญหาและอุปสรรค ตั้งแต่เริ่มต้นจนโครงการเล่มนี้เสร็จสมบูรณ์ ผู้จัดทำจึงขอกราบขอบพระคุณเป็นอย่างสูง

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

ขอบพระคุณคณาจารย์ภาควิชาวิศวกรรมคอมพิวเตอร์ และคณาจารย์ทุกท่านที่ได้ประสิทธิ์ประสาทวิชาความรู้ สามารถนำความรู้ที่มี ใช้ในการแก้ไขปัญหาจนสำเร็จลงเป็นอย่างดี

ขอบคุณเพื่อนๆ พี่ๆ น้อง ๆ ที่คอยให้ความช่วยเหลือ คำปรึกษา และกำลังใจเสมอมา

สุดท้ายนี้ ขอระลึกถึงพระคุณบิดามารดาที่ได้เลี้ยงดู อบรมสั่งสอนจนเติบโตใหญ่ ส่งเสริมสนับสนุน ให้คำแนะนำ คำปรึกษา และเป็นกำลังใจในการทำงานเสมอมา

นายจักรภูมิ มณีรัตน์

ผู้จัดทำ

ปัจจุบันการใช้งานและเข้าถึงอินเทอร์เน็ตสามารถกระทำได้อย่างอิสระและเสรีมากขึ้น จึงมีโอกาสดังกล่าวทำให้เกิดการกระทำผิดทางอินเทอร์เน็ตได้ทุกเมื่อไม่ว่าเจตนาหรือไม่ก็ตาม ดังนั้น จึงมีการออกกฎหมาย พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ขึ้น โดย ผู้ให้บริการ ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ไว้ไม่น้อยกว่า 90 วัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ ซึ่งระบบและเครื่องมือในส่วนของการระบุตัวตนในปัจจุบันบางระบบรองรับการทำงานในระบบ Internet Protocol version4 แต่ยังไม่รองรับระบบ Internet Protocol version6 โครงการนี้จึงคิดนำข้อมูล MAC Address (Physical Address) IPv4 และ IPv6 จาก Layer3 switch ซึ่ง Layer3 switch มีการเก็บไว้แล้วมาใช้ประโยชน์ ในการช่วยระบุตัวตน เพื่อทราบถึงชื่อผู้ใช้ และเก็บข้อมูลการใช้งานไว้เพื่อประโยชน์ในการระบุผู้กระทำความผิดได้ หากเกิดการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ต่อไป ขณะเดียวกันสามารถนำข้อมูลที่ได้ไปใช้ ทำสถิติ เพื่อวิเคราะห์ การใช้งานของผู้ใช้งานของผู้ใช้ได้

หนังสือรับรองความเป็นเอกลักษณ์.....	ii
กิตติกรรมประกาศ	iii
บทคัดย่อ.....	iv
Abstract.....	v
สารบัญ.....	vi
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)	3
2.2 ARP (Address Resolution Protocol)	3
2.3 IPv6 (Internet protocol version 6).....	3
2.4 Neighbor Discovery Protocol	4
2.5 Layer3 switch.....	4
2.6 SNMP	5
2.7 ภาษา PERL	5
2.8 Apache Webserver	6

2.9 SQL	6
2.10 mySQL	7
2.11 ภาษา PHP	7
2.12 RADIUS	8
2.13 Freeradius	9
2.14 หลักการทำงานเบื้องต้นของโครงการ	9
3. ระเบียบวิธีวิจัย.....	14
3.1 แนวคิดในการออกแบบระบบ	14
3.2 ระบบที่ได้ออกแบบ	16
3.3 การทดสอบระบบ.....	17
4. ผลและวิเคราะห์ผลการทดลอง	18
4.1 การทดสอบการจำลองระบบลงชื่อเข้าใช้	18
4.2 การทดสอบระบบส่วนเบื้องหลัง	18
4.3 การทดสอบระบบส่วนฐานข้อมูล.....	20
4.4 การทดสอบระบบในส่วนแสดงผล	22
5. สรุปผลและข้อเสนอแนะ	25
5.1 สรุปผล	25
5.2 ปัญหาและอุปสรรค.....	25
5.3 ข้อเสนอแนะ	25
6. เอกสารอ้างอิง.....	26

7. ภาคผนวก.....	1
-----------------	---

ภาพที่ 1 ตัวอย่างรูปภาพที่ไม่ชัดเจน.....ผิดพลาด! ไม่ได้กำหนดบุ๊กมาร์ก

ตารางที่ 1 ความแตกต่างของการเขียนทับศัพท์ของตัว A และ ตัว T.....ผิดพลาด! ไม่ได้กำหนดบุ๊กมาร์ก

1. บทนำ

1.1 ความสำคัญและที่มาของโครงการ

ปัจจุบันการใช้งานและเข้าถึงอินเทอร์เน็ตสามารถกระทำได้อย่างอิสระและเสรีมากขึ้น จึงมีโอกาสดังกล่าวทำให้เกิดทางอินเทอร์เน็ตได้ทุกเมื่อไม่ว่าเจตนาหรือไม่ก็ตาม ดังนั้น จึงมีการออกกฎหมาย พรบ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ขึ้น โดย ผู้ให้บริการ ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ไว้ไม่น้อยกว่า 90 วัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์

ซึ่งระบบและเครื่องมือในส่วนของการระบุตัวตนในปัจจุบันส่วนใหญ่รองรับการทำงานในระบบ Internet Protocol version4 แต่ยังไม่รองรับระบบ Internet Protocol version6 เนื่องจากมี Protocol ที่เกี่ยวข้องเปลี่ยนไป เช่น Neighbor Discovery Protocol ใน IPv6 เข้ามาทำงานแทน Address Resolution Protocol ใน IPv4 เป็นต้น นอกจากนั้นอุปกรณ์หนึ่งชิ้นสามารถมี IP Address ได้มากกว่าหนึ่งหมายเลข และยังมีส่วนที่เป็น Temporary Address เป็น IP Address ชั่วคราวซึ่งสามารถเกิดขึ้น และเปลี่ยนแปลงได้หลังจากการยืนยันตัวตนแล้ว ทำให้ไม่สามารถระบุได้ว่าผู้ใช้หมายเลขนั้นคือบุคคลใด เพราะหากเกิดการเปลี่ยนแปลงในส่วน Temporary Address ขึ้นการกระทำใดๆจากหมายเลขดังกล่าวจะไม่สามารถตรวจสอบได้ว่ามาจากผู้ใช้บุคคลใด

อุปกรณ์ Layer3 Switch เป็นอุปกรณ์เลือกเส้นทาง ซึ่งทำงานบน OSI Model ในระดับที่ 3 โดยทำงานระดับแพคเกจ ซึ่งจะมีการเก็บค่า IP Address และ MAC Address ทำให้สามารถนำข้อมูล MAC Address มาเปรียบเทียบกับเพื่อให้ทราบผู้ใช้ จากการยืนยันตัวตนจาก ระบบ IPv4 ได้ ซึ่ง อุปกรณ์ Layer3 Switch และอุปกรณ์อื่นๆในปัจจุบัน เช่น Routers, Layer2 switch, Servers, Workstations, Printers, UPS รองรับการทำงานสื่อสารผ่าน SNMP ทำให้สามารถ ส่งคำสั่งไปยัง Agent gets responses จาก Agents sets ค่าตัวแปรใน Agents และรับข้อมูลเหตุการณ์ต่างๆที่เกิดขึ้นจาก Agent ได้

ด้วยเหตุผลข้างต้น ผู้จัดทำโครงการจึงคิดที่จะนำข้อมูล MAC Address (Physical Address) IPv4 และ IPv6 จาก Layer3 switch ผ่านทาง SNMP Protocol มาใช้ในการช่วยระบุตัวตน และเก็บข้อมูล ในระบบ IPv6 ทำให้สามารถทราบได้ว่าอุปกรณ์นั้นได้รับ IP Address หมายเลขใดบ้าง ทราบถึงชื่อผู้ใช้ และเก็บข้อมูลการใช้งานไว้เพื่อประโยชน์ในการระบุผู้กระทำความผิดได้ หากเกิดการกระทำความผิดตาม พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ต่อไป ขณะเดียวกันสามารถนำข้อมูลที่ได้นำไปใช้ ทำสถิติ เพื่อวิเคราะห์ การใช้งานของผู้ใช้งานของผู้ใช้ได้

1.2 วัตถุประสงค์

1. เพื่อเก็บข้อมูลการได้รับหมายเลข IP Address ทั้ง IPv4 และ IPv6 ของแต่ละอุปกรณ์
2. เพื่อแสดงข้อมูล และช่วยจัดการ ผู้ใช้ในเครือข่าย
3. เพื่อแก้ไขปัญหาการไม่สามารถระบุตัวตนได้ของหมายเลข IP Address ในระบบ IPv6

1.3 ประโยชน์ที่คาดว่าจะได้รับ

1. สามารถระบุตัวตนผู้ใช้ ในระบบ IPv6 เพื่อช่วยแก้ปัญหาไม่สามารถระบุผู้ใช้งานที่ใช้งานด้วย IPv6 ได้
2. ทำให้ทราบ IP Address ทั้งหมดที่ผู้ใช้แต่ละคนได้รับ เพื่อเป็นข้อมูลในการบริหารจัดการ เครือข่าย

1.4 ขอบเขตของโครงการ

1. สามารถเก็บข้อมูล IP Address ของอุปกรณ์ ที่ใช้งานผ่าน Layer3 switch ที่ Log Server เชื่อมต่ออยู่ได้
2. สามารถแสดงข้อมูล IP Address และข้อมูลการลงชื่อเข้าใช้ ของอุปกรณ์ 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)

IP [10] (Internet Protocol) เป็นวิธีการ (protocol) ที่ใช้ในการส่งข้อมูลจากเครื่องคอมพิวเตอร์เครื่องหนึ่งไปยังเครื่องอื่น ในอินเทอร์เน็ต (Internet) คอมพิวเตอร์แต่ละเครื่อง รู้จักกันในฐานะของ Host บน Internet ต้องมีที่อยู่อย่างน้อยหนึ่งที่อยู่ (address) ซึ่งไม่ซ้ำกับคอมพิวเตอร์เครื่องอื่นใน Internet เมื่อมีการส่งและรับข้อมูล (เช่น อี-เมล) ข้อความจะถูกแบ่งเป็นชุดข้อมูล เรียกว่า แพ็คเก็ต (Packet) แต่ละชุดจะเก็บที่อยู่ของผู้ส่งและผู้รับ การส่งชุดข้อมูลจะส่งไปที่เครื่องคอมพิวเตอร์ที่เป็น Gateway เมื่อเครื่อง Gateway อ่านที่อยู่ของปลายทางแล้ว จึงส่งต่อชุดข้อมูลไปยัง adjacent Gateway ซึ่งจะอ่านที่อยู่ปลายทาง และส่งอ่านเครือข่าย Internet จนกระทั่งมีเครื่อง gateway รู้ว่าชุดข้อมูลนั้น เป็นของคอมพิวเตอร์ ภายในกลุ่มใด จากนั้น เครื่อง Gateway จึงจะส่งชุดข้อมูลไปยังเครื่องคอมพิวเตอร์ที่มีอยู่ตามที่ระบุ

2.2 ARP (Address Resolution Protocol)

ARP [9] (Address Resolution Protocol) เป็นโปรโตคอลสำหรับการจับคู่ (map) ระหว่าง Internet Protocol address (IP address) กับตำแหน่งของอุปกรณ์ในระบบเครือข่าย เช่น IP เวอร์ชัน 4 ใช้การระบุตำแหน่งขนาด 32 บิต ใน Ethernet ของระบบใช้การระบุ ตำแหน่ง 48 บิต (การระบุตำแหน่งของอุปกรณ์รู้จักในชื่อของ Media Access Control หรือ MAC address) ตาราง ARP ซึ่งมักจะ เป็น cache จะรักษาการจับคู่ ระหว่าง MAC address กับ IP address โดย ARP ใช้กฎของโปรโตคอล สำหรับการสร้างการจับคู่ และแปลงตำแหน่งทั้งสองฝ่าย

2.3 IPv6 (Internet protocol version 6)

หมายเลข IP Address [1,7] ส่วนใหญ่ที่ใช้กันทุกวันนี้ คือ Internet Protocol version 4 (IPv4) ซึ่งเราใช้เป็นมาตรฐานในการส่งข้อมูลในเครือข่ายอินเทอร์เน็ตตั้งแต่ปีค.ศ. 1981 ทั้งนี้การขยายตัวของเครือข่ายอินเทอร์เน็ตในช่วงที่ผ่านมามีอัตราการเติบโตอย่างรวดเร็ว นักวิจัยเริ่มพบว่าจำนวนหมายเลข IP Address ของ IPv4 กำลังจะถูกใช้หมดไป ไม่เพียงพอกับการใช้งานอินเทอร์เน็ตในอนาคต และหากเกิดขึ้นก็หมายความว่าเราจะไม่สามารถเชื่อมต่อเครือข่ายเข้ากับระบบอินเทอร์เน็ตเพิ่มขึ้นได้อีก ดังนั้นคณะทำงาน IETF (The Internet Engineering Task Force) ซึ่งตระหนักถึงปัญหาสำคัญดังกล่าว จึงได้พัฒนาอินเทอร์เน็ตโปรโตคอลรุ่นใหม่ขึ้น คือ รุ่นที่หก (Internet Protocol version 6; IPv6) เพื่อทดแทนอินเทอร์เน็ตโปรโตคอลรุ่นเดิม โดยมีวัตถุประสงค์ เพื่อปรับปรุงโครงสร้างของตัวโปรโตคอล ให้รองรับหมายเลขแอดเดรสจำนวนมาก และปรับปรุงคุณลักษณะอื่น ๆ อีกหลายประการ

ทั้งในแง่ของประสิทธิภาพและความปลอดภัยรองรับระบบแอปพลิเคชัน (application) ใหม่ ๆ ที่จะเกิดขึ้นในอนาคต และเพิ่มประสิทธิภาพในการประมวลผลแพ็กเก็ต (packet) ให้ดีขึ้น ทำให้สามารถตอบสนองต่อการขยายตัวและความต้องการใช้งานเทคโนโลยีบนเครือข่ายอินเทอร์เน็ตในอนาคตได้เป็นอย่างดี

2.4 Neighbor Discovery Protocol

ND [7] อธิบายไว้ใน RFC 4861 ประกอบด้วยชุดของข้อความ ICMPv6 ตัวเลือกของข้อความ และกำหนดกระบวนการที่ทำให้โหนดใกล้เคียงค้นพบโหนดอื่น ๆ การค้นพบเราเตอร์บนลิงค์ และให้การรองรับ

สำหรับโหนดที่เปลี่ยนเส้นทาง ND เป็นสิ่งอำนวยความสะดวกที่เข้ามาแทนในIPv4

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

ND มี 5 ข้อความ มีดังต่อไปนี้

- Neighbor Solicitation
- Neighbor Advertisement
- Router Solicitation
- Router Advertisement
- Redirect

2.5 Layer3 switch

Layer3 switch [2,5,6] เป็นอุปกรณ์ในการทำ Routing (หาเส้นทางการรับส่งข้อมูลระหว่างเน็ตเวิร์ก) เหมาะสมในการนำไปใช้ในระบบเน็ตเวิร์กที่มีการใช้งาน VLAN (VLAN เป็นการแบ่งพอร์ตต่าง ๆ ที่มีอยู่ในสวิตช์ให้ดูเหมือนว่าแยกกันอยู่คนละเน็ตเวิร์ก) และต้องการให้อุปกรณ์ Computer ที่อยู่ในแต่ละ VLAN สามารถติดต่อกันได้ ซึ่ง Layer 3 switch จะสามารถทำงานได้ในทั้งระดับของ layer 2 และ layer 3 แต่เรื่องของการส่งผ่านข้อมูลภายใน หรือระหว่าง switch ด้วยกันนั้น ต้องดูว่าเราเจาะจงไปเฉพาะในส่วนการทำงานของ layer ไหน ซึ่งตรงนี้ก็อยู่ที่ switch ตัวที่เชื่อมต่ออยู่ และ mode ของการทำงานของ switch ที่ได้ตั้งค่าเอาไว้ ถ้าเป็นการส่งข้อมูลกันในระดับ layer 2 ยังคงพิจารณา MAC Address เหมือนเดิม แต่หากเป็นการติดต่อกันในระดับ Layer 3 Switch จะพิจารณา IP Address เป็นหลัก ในด้านของข้อมูล ที่ Layer 3 Switch จะส่งต่อออกมานั้น ถ้าทำงานในระดับของ Layer 2 ก็จะส่งข้อมูลออกมาเป็น Frame แต่ถ้าทำงานในระดับ Layer 3 จะส่งผ่านข้อมูลเป็นลักษณะของ Packet

ข้อมูล และ นอกจากนี้ Layer 3 Switch ยังมีความสามารถด้านการ Routing เหมือนกับพวก Router ด้วย (แต่จะต่างกับ Router คือ ไม่กันการส่ง broad cast ข้ามเครือข่าย)

ซึ่งในโครงงานนี้ จะนำข้อมูลในตาราง ARP table ซึ่งมีการเก็บ หมายเลข IP Address ทั้ง IPv4 ipv6 และ MAC Address ของทุกอุปกรณ์ในเครือข่ายมาใช้ในการเปรียบเทียบข้อมูลว่า อุปกรณ์แต่ละอุปกรณ์ได้ หมายเลข IP Address อะไรไปบ้างเพื่อการอ้างอิง ผู้ใช้ต่อไป

2.6 SNMP

SNMP[4][8] ย่อมาจาก Simple Network Management Protocol ซึ่งเป็นโพรโทคอลที่อยู่ระดับบนในชั้นการประยุกต์ และเป็นส่วนหนึ่งของชุดโพรโทคอล TCP/IP เครือข่ายอินเทอร์เน็ตที่ใช้โพรโทคอล TCP/IP มีอุปกรณ์เครือข่ายหลากหลายชนิดและหลายยี่ห้อ แต่มาตรฐานการจัดการเครือข่ายที่ใช้กันได้ดีคือ SNMP ในการบริการและการจัดการเครือข่ายต้องใช้อุปกรณ์ต่าง ๆ มีส่วนของการทำงานร่วมกับระบบจัดการเครือข่าย ซึ่งเราเรียกว่า เอเจนต์ (Agent) เอเจนต์เป็นส่วนของซอฟต์แวร์ที่อยู่ในอุปกรณ์ต่าง ๆ ที่เชื่อมต่ออยู่ในเครือข่ายโดยมีคอมพิวเตอร์หลักในระบบหนึ่งเครื่องเป็นตัวจัดการและบริหารเครือข่ายหรือเรียกว่า NMS-Network Management System

โพรโทคอล SNMP ได้ถูกพัฒนาขึ้นในปี พ.ศ. 2531 เนื่องจากมีความเจริญเติบโตในการใช้อุปกรณ์ที่สนับสนุนโพรโทคอล TCP/IP อย่างสูง โพรโทคอล SNMP ถูกออกแบบให้มีฟังก์ชันและการทำงานแบบง่าย เหมาะกับคำว่าซิมเปิล (Simple) โดยมีจุดประสงค์หลักเพื่อให้ผู้ดูแลระบบเครือข่ายสามารถเข้ามาจัดการอุปกรณ์เครือข่ายได้จากระยะไกลโดยง่าย

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

2.7 ภาษา PERL

PERL [3] (ย่อมาจาก Practical Extraction and Report Language) เป็นภาษาโปรแกรมแบบไดนามิก พัฒนาโดยนายแลร์รี วอลล์ (Larry Wall) ในปี ค.ศ. 1987 เพื่อใช้งานกับระบบปฏิบัติการยูนิกซ์

ภาษาเพิร์ล นั้นถูกออกแบบมาให้ใช้งานได้ง่าย โครงสร้างของภาษาจึงไม่ซับซ้อน มีลักษณะคล้ายกับภาษาซี นอกจากนี้เพิร์ลยังได้แนวคิดบางอย่างมาจากเชลล์สคริปต์, ภาษา AWK, sed และ Lisp ภาษาเพิร์ลมีตัวแปรอยู่ 4 ชนิด ได้แก่

สเกลาร์ สามารถเก็บข้อมูลได้ 1 อย่าง อาจจะเป็น ตัวเลข, สตริง หรือ รีเฟอเรนซ์ ก็ได้

อาเรย์ เป็นเหมือนกลุ่มของ สเกลาร์ที่ถูกเรียงไว้

แฮช หรืออีกชื่อหนึ่งคือแถวลำดับแบบจับคู่ เป็นเหมือนตู้ล็อกเกอร์สำหรับเก็บสเกลาร์ อนุญาตที่จะใช้ไขตู้ล็อกเกอร์จะเรียกว่า keys

ไฟล์แชนเดิล เป็นตัวแปรที่ใช้สำหรับ I/O โดยเฉพาะ อาจจะใช้สำหรับรับการสั่งงานจากผู้ใช้ผ่านทาง Standard Input หรือใช้สำหรับแสดงผลออกทาง Standard Output

2.8 Apache Webserver

Apache[12] คือ Web server พัฒนามาจาก HTTPD Web Server โดย Apache นี้จะทำหน้าที่ในการจัดเก็บ Homepage และส่ง Homepage ไปยัง Browser ที่มีการเรียกเข้า ยัง Web server ที่เก็บ Homepage นั้นอยู่ ซึ่งปัจจุบันจัดได้ว่าเป็น web server ที่มี ความน่าเชื่อถือมาก เนื่องจากเป็นที่นิยมใช้กันทั่วโลก อีกทั้งอาปาเช่ยังเป็นซอฟต์แวร์ แบบ โอเพ่นซอร์ส ที่เปิดให้บุคคลทั่วไปสามารถเข้ามาร่วมพัฒนาส่วนต่างๆ ของอาปาเช่ได้ ซึ่งทำให้เกิดเป็น โมดูล ที่เกิดประโยชน์มากมาย เช่น

mod_perl, mod_python หรือ mod_php และทำงานร่วมกับภาษาอื่นได้ แทนที่จะเป็นเพียงเซิร์ฟเวอร์ ที่ให้บริการเพียงแค่ HTML อย่างเดียว โดยสามารถหา Download ได้จาก website www.apache.org

นอกจากนี้อาปาเช่เองยังมีความสามารถอื่นๆ ด้วย เช่น การยืนยันตัวบุคคล

(mod_auth, mod_access, mod_digest) หรือเพิ่มความปลอดภัยในการสื่อสารผ่าน โพรโตคอล https (mod_ssl) และยังมีโมดูลอื่นๆ ที่ได้รับความนิยมใช้ เช่น mod_vhost ทำให้สามารถสร้างโฮสต์เสมือนภายในเครื่องเดียวกันได้ หรือ 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 ซึ่งที่อยู่เหล่านี้จะขึ้นอยู่กับว่าผู้ดูแลเว็บไซต์ ว่าต้องการให้อยู่ในลักษณะใด

2.9 SQL

SQL[11] ย่อมาจาก structured query language คือภาษาที่ใช้ในการเขียนโปรแกรม เพื่อจัดการกับฐานข้อมูลโดยเฉพาะ เป็นภาษามาตรฐานบนระบบฐานข้อมูลเชิงสัมพันธ์และเป็นระบบเปิด (open system) หมายถึงเราสามารถใส่คำสั่ง sql กับฐานข้อมูลชนิดใดก็ได้ และ คำสั่งงานเดียวกันเมื่อสั่งงานผ่าน ระบบฐานข้อมูลที่แตกต่างกันจะได้ ผลลัพธ์เหมือนกัน ทำให้เราสามารถเลือกใช้ฐานข้อมูลชนิดใดก็ได้โดยไม่ติดขัดกับฐานข้อมูลใดฐานข้อมูลหนึ่ง นอกจากนี้แล้ว SQL ยังเป็นชื่อโปรแกรมฐานข้อมูล ซึ่งโปรแกรม SQL เป็นโปรแกรมฐานข้อมูลที่มีโครงสร้างของภาษาที่เข้าใจง่าย ไม่ซับซ้อน มีประสิทธิภาพการทำงานสูง สามารถทำงานที่ซับซ้อนได้โดยใช้คำสั่งเพียงไม่กี่คำสั่ง โปรแกรม SQL จึงเหมาะที่จะใช้กับระบบฐานข้อมูลเชิงสัมพันธ์ และเป็นภาษาหนึ่ง ซึ่งแบ่งการทำงานได้เป็น 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, MS-Access

นอกจากนี้ภาษา SQL ถูกนำมาใช้เขียนร่วมกับโปรแกรมภาษาต่างๆ เช่น ภาษา c/C++ , VisualBasic และ Java

ประเภทของคำสั่งภาษา SQL

1. ภาษานิยามข้อมูล(Data Definition Language : DDL) เป็นคำสั่งที่ใช้ในการสร้างฐานข้อมูล กำหนดโครงสร้างข้อมูลว่ามี Attribute ใด ชนิดของข้อมูล รวมทั้งการเปลี่ยนแปลงตาราง และการสร้างดัชนี คำสั่ง : CREATE,DROP,ALTER
2. ภาษาจัดการข้อมูล (Data Manipulation Language :DML) เป็นคำสั่งที่ใช้ในการเรียกใช้ เพิ่ม ลบ และเปลี่ยนแปลงข้อมูลในตาราง คำสั่ง : SELECT,INSERT,UPDATE,DELETE
3. ภาษาควบคุมข้อมูล (Data Control Language : DCL) เป็นคำสั่งที่ใช้ในการกำหนดสิทธิการ อนุญาต หรือ ยกเลิก การเข้าถึงฐานข้อมูล เพื่อป้องกันความปลอดภัยของฐานข้อมูล คำสั่ง : GRANT,REVOKE

2.10 mySQL

MySQL [11] เป็นโปรแกรมจัดการฐานข้อมูล Relational Database Management System (RDBMS) เป็นฐานข้อมูลที่สามารถจัดเก็บ ค้นหา เรียงข้อมูล และดึงข้อมูล MySQL มีความสามารถให้ ผู้ใช้งานเข้าถึงข้อมูลได้หลายๆคนในเวลาเดียวกันได้และมีการเข้าถึงข้อมูลที่รวดเร็ว มีการกำหนดการเข้า ใช้งานของผู้ใช้ในแบบต่าง ๆ อย่างเหมาะสม ปลอดภัย MySQL ถูกใช้งานเมื่อปี 1996 แต่โปรแกรมนี้ พัฒนาคั้งแต่ปี 1979 และชนะรางวัล Linux Journal Reader 's Choice Award 3ปีซ้อน

ปัจจุบัน MySQL ได้ใช้งานแพร่หลายโดยเป็นโปรแกรม Open Source License แต่ก็มีแบบ Commercial License ให้ใช้ด้วย โดยคุณสมบัติจะแตกต่างกันออกไป

2.11 ภาษา PHP

PHP[12] ย่อมาจาก PHP Hypertext Preprocessor แต่เดิมนิยมาจก Personal Home Page Tools PHP คือภาษาคอมพิวเตอร์จำพวก scripting language ภาษาจำพวกนี้คำสั่งต่าง ๆ จะเก็บ

อยู่ในไฟล์ที่เรียกว่า script และเวลาใช้งานต้องอาศัยตัวแปรชุดคำสั่ง ตัวอย่างของภาษาสคริปก็ เช่น JavaScript , Perl เป็นต้น ลักษณะของ PHP ที่แตกต่างจากภาษาสคริปต์แบบอื่นๆ คือ PHP ได้รับการพัฒนาและออกแบบมา เพื่อใช้งานในการสร้างเอกสารแบบ HTML โดยสามารถสอดแทรกหรือแก้ไขเนื้อหาได้โดยอัตโนมัติ ดังนั้นจึงกล่าวว่า PHP เป็นภาษาที่เรียกว่า server-side หรือ HTML-embedded scripting language นั่นคือในทุก ๆ ครั้งก่อนที่เครื่องคอมพิวเตอร์ซึ่งให้บริการเป็น Web server จะส่งหน้าเว็บเพจที่เขียนด้วย PHP ให้เรา มันจะทำการประมวลผลตามคำสั่งที่มีอยู่ให้เสร็จเสียก่อน แล้วจึงค่อยส่งผลลัพธ์ที่ได้ให้เรา ผลลัพธ์ที่ได้นั้นก็คือเว็บเพจที่เราเห็นนั่นเอง ถือได้ว่า PHP เป็นเครื่องมือที่สำคัญชนิดหนึ่งที่ช่วยให้เราสามารถสร้าง Dynamic Web pages (เว็บเพจที่มีการโต้ตอบกับผู้ใช้) ได้อย่างมีประสิทธิภาพและมีลูกเล่นมากขึ้น

PHP เป็นผลงานที่เติบโตมาจากกลุ่มของนักพัฒนาในเชิงเปิดเผยแพร่ให้ต้นฉบับ หรือ Open Source ดังนั้น PHP จึงมีการพัฒนาไปอย่างรวดเร็ว และแพร่หลายโดยเฉพาะอย่างยิ่งเมื่อใช้ร่วมกับ Apache Web server ระบบปฏิบัติการอย่างเช่น Linux หรือ FreeBSD เป็นต้น ในปัจจุบัน PHP สามารถใช้ร่วมกับ Web Server หลายๆตัวบนระบบปฏิบัติการอย่างเช่น Windows 95/98/NT เป็นต้น ซึ่ง PHP มีลักษณะเด่นคือ

- 1.ใช้ได้ฟรี
- 2.PHP เป็นโปรแกรมวิ่งข้าง Sever ดังนั้นขีดความสามารถไม่จำกัด
- 3.Conlatfun นั่นคือPHP วิ่งบนเครื่อง UNIX,Linux,Windows ได้หมด
- 4.เรียนรู้ง่าย เนื่องจาก PHP ผังเข้าไปใน HTML และใช้โครงสร้างและไวยากรณ์ภาษาง่ายๆ
- 5.เร็วและมีประสิทธิภาพ โดยเฉพาะเมื่อใช้กับ Apach Xerve เพราะไม่ต้องใช้โปรแกรมจากภายนอก
- 6.ใช้ร่วมกับ XML ได้ทันที
- 7.ใช้กับระบบแฟ้มข้อมูลได้
- 8.ใช้กับข้อมูลตัวอักษรได้อย่างมีประสิทธิภาพ
- 9.ใช้กับโครงสร้างข้อมูล แบบ Scalar,Array,Associative array
- 10.ใช้กับการประมวลผลภาพได้

ในโครงการนี้ PHP จะเป็นภาษาที่ช่วยในการทำ webpage ในการแสดงข้อมูลที่เก็บไว้

2.12 RADIUS

การเชื่อมต่อเพื่อพิสูจน์ตัวจริงระยะไกลในบริการของผู้ใช้ หรือ RADIUS (Remote Authentication Dial In User Service) เป็นโพรโทคอลเครือข่ายที่ให้การตรวจสอบ, อนุมัติ และการจัดการการบัญชี (AAA)จากส่วนกลาง สำหรับคอมพิวเตอร์ที่เชื่อมต่อและใช้บริการเครือข่าย. RADIUS

ได้รับการพัฒนาโดย Livingston Enterprises, Inc ในปี 1991 ในฐานะที่เป็นโพรโทคอลการตรวจสอบ และการบัญชีของเซิร์ฟเวอร์การเข้าถึง และภายหลังถูกนำมาเป็นมาตรฐานของ Internet Engineering Task Force (IETF).

เพราะการสนับสนุนในวงกว้างและธรรมชาติที่แพร่หลายของโพรโทคอล RADIUS มันมักจะถูกใช้ โดยผู้ให้บริการอินเทอร์เน็ตและผู้ประกอบการในการจัดการการเข้าถึงเครือข่ายอินเทอร์เน็ตหรือภายใน เครือข่ายไร้สาย และบริการอีเมลแบบบูรณาการ เครือข่ายเหล่านี้อาจประกอบด้วยโมเด็ม, DSL, access points, VPNs, พอร์ตเครือข่าย, เว็บเซิร์ฟเวอร์ ฯลฯ

RADIUS เป็นโพรโทคอลแบบไคลเอ็นต์/เซิร์ฟเวอร์ที่วิ่งในชั้นแอปพลิเคชัน ใช้ UDP เป็นตัวขนส่ง. Remote Access Server, Virtual Private Network server, the Network switch ที่มีการตรวจสอบพอร์ต และ Network Access Server (NAS) ทั้งหมดนี้เป็นเกตเวย์ที่ควบคุมการเข้าถึง เครือข่ายและทุกตัวมีส่วนลูกข่ายของ RADIUS ที่ติดต่อสื่อสารกับ RADIUS เซิร์ฟเวอร์. RADIUS เซิร์ฟเวอร์มักจะเป็นกระบวนการเบื้องหลัง ที่ทำงานบน UNIX หรือ Microsoft Windows Server.

2.13 Freeradius

Freeradius เป็นซอฟต์แวร์ที่ทำหน้าที่เป็น Radius Server ซึ่งเป็น server ในการจัดการการ ยืนยันตัวตนของผู้ใช้ โดย Freeradius เป็นฟรีซอฟต์แวร์ที่มีความสามารถสูงมีความยืดหยุ่นได้รับความนิยม สูง

2.14 หลักการทำงานเบื้องต้นของโครงการ

จากปัญหา การไม่สามารถระบุตัวตนได้ในระบบ IPv6 เนื่องจาก ระบบการยืนยันตัวตนผู้ใช้ใน แบบเดิมที่ไม่ได้ออกแบบมารองรับกับรูปแบบของ IPv6 จึงทำให้ไม่สามารถระบุตัวตนผู้ใช้ได้ในกรณีที่ผู้ใช้ได้ใช้งานผ่านรูปแบบของ IPv6 เช่น ปัญหาของ IP Address ที่สามารถมีได้หลายค่า และ Temporary IP Address ซึ่งตรวจสอบได้ยาก จาก รูปที่ 2-1


```

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:80:00:00:00:00:00:00:90:48:3e:96:da:3b:45:08" = STRING: e0:db:55:f7:69:fe
IP-MIB::ipNetToPhysicalPhysAddress.103.ipv6."fe:80:00:00:00:00:00:00: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:80:00:00:00:00:00:00:4e:72: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 2-3 ผลลัพธ์การเรียกดูข้อมูล IP Address จาก Layer3 Switch ผ่าน SNMP

ผลลัพธ์ที่ได้ทำให้ได้ข้อมูล ว่าปัจจุบันมีอุปกรณ์ใดที่ใช้งานบน IPv6 ไปบ้างโดยแสดง IP Address และ

MAC Address ของเครื่องต่าง ๆ ที่ใช้งานผ่าน Layer3 Switch

```

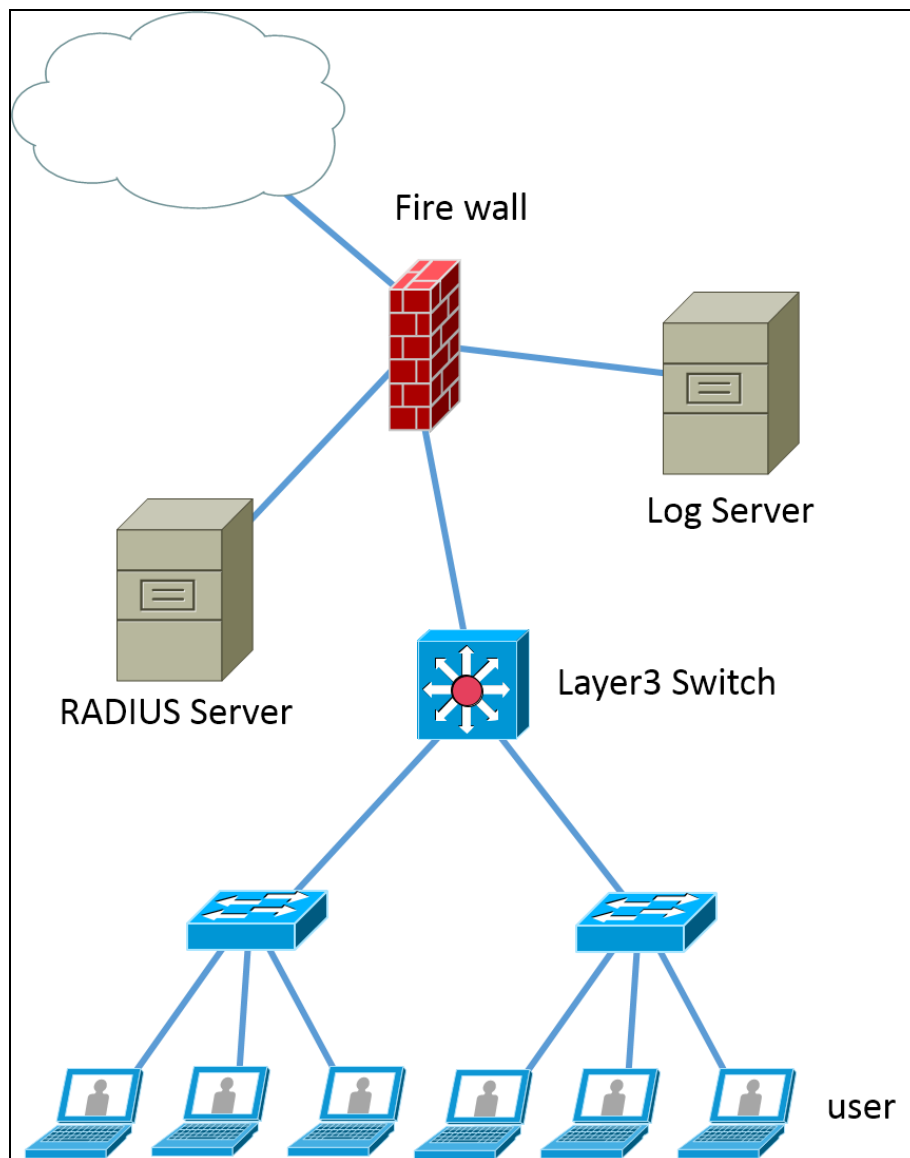
IP-MIB::ipNetToMediaPhysAddress.202.172.30.254.69 = STRING: 0:12:7f:17:a3:80
IP-MIB::ipNetToMediaPhysAddress.202.172.30.254.73 = STRING: 0:19:e7:e8:2:41
IP-MIB::ipNetToMediaPhysAddress.202.172.30.254.75 = STRING: c:85:25:c9:25:c1
IP-MIB::ipNetToMediaPhysAddress.202.172.30.254.77 = STRING: c:85:25:a3:fb:c1
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 2-4 ผลลัพธ์การเรียกดูข้อมูล IP Address จาก Layer3 Switch ผ่าน SNMP

ผลลัพธ์ที่ได้ทำให้ได้ข้อมูล ว่าปัจจุบันมีอุปกรณ์ใดที่ใช้งานบน IPv4 ไปบ้างโดยแสดง IP Address และ

MAC Address ของเครื่องต่าง ๆ ที่ใช้งานผ่าน Layer3 Switch

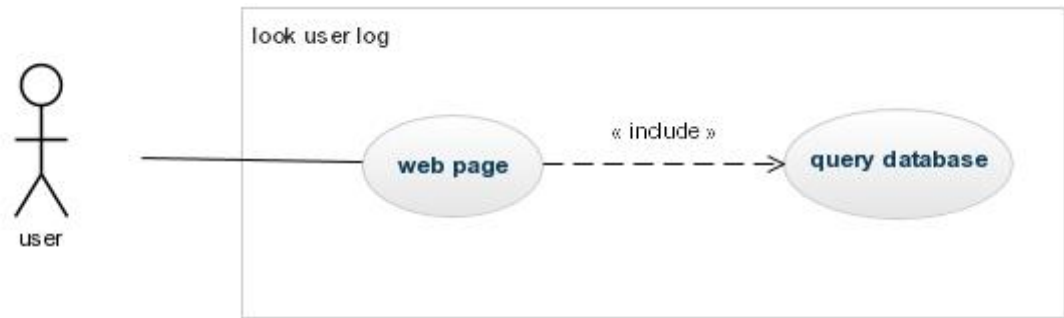


รูปที่ 2-5 การเชื่อมต่อ Log Server กับเครือข่าย

การเชื่อมต่อ Log Server จะต้องเชื่อมต่อและสามารถติดต่อได้กับอุปกรณ์สวิตช์ และ RADIUS Server เช่น รูปที่ 2-5 โดย Log Server จะมีการทำงานดังนี้

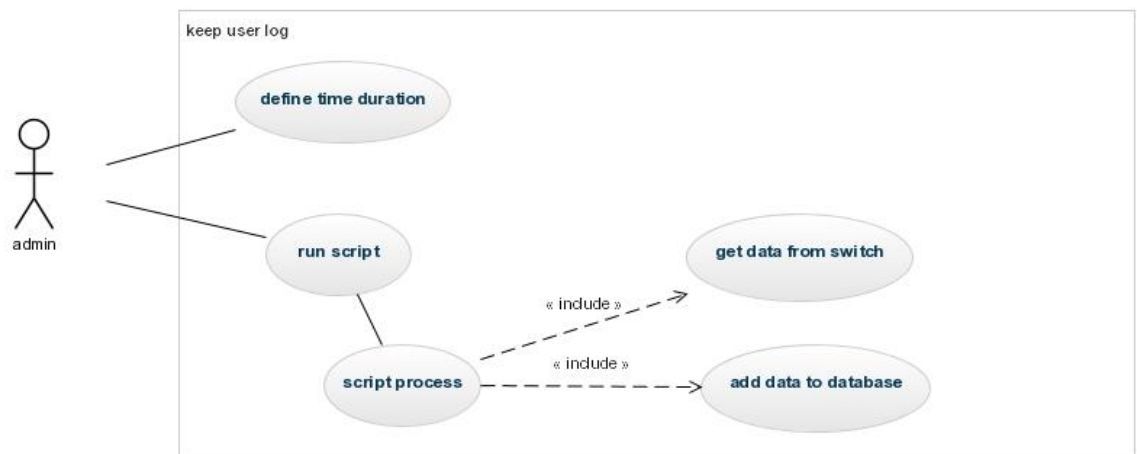
1. log sever ส่งข้อความร้องขอข้อมูลไปยัง layer3 switch ผ่านทาง SNMP Protocol เป็นระยะ
2. log sever ได้รับข้อมูลกลับมา ประมวลผลและเก็บไว้ในระบบฐานข้อมูล
3. web server นำข้อมูลที่เก็บในฐานข้อมูลมาแสดงผ่านหน้า web

โดยผู้ใช้งานจะมี 2 กลุ่มโดยในกลุ่มแรกคือผู้ใช้ทั่วไปซึ่งจะสามารถเข้าดูข้อมูลประวัติของตนเองผ่านทางหน้าเว็บได้ ดังรูปที่ 2-6



รูปที่ 2-6 use case diagram ของผู้ใช้ทั่วไป

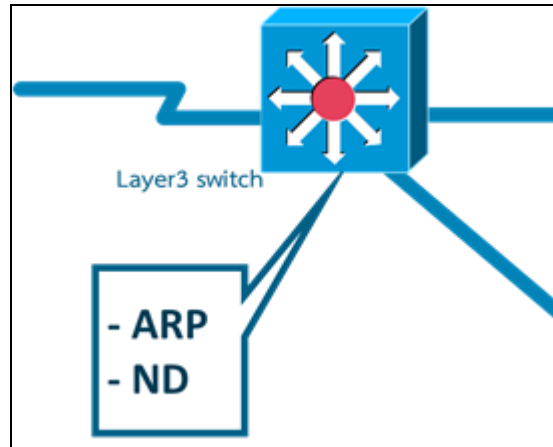
และผู้ใช้ที่เป็นผู้ดูแลระบบ สามารถกำหนดความถี่ของการตรวจสอบข้อมูลของ Server ได้ ดังรูปที่ 2-7



รูปที่ 2-7 use case diagram ของผู้ดูแลระบบ

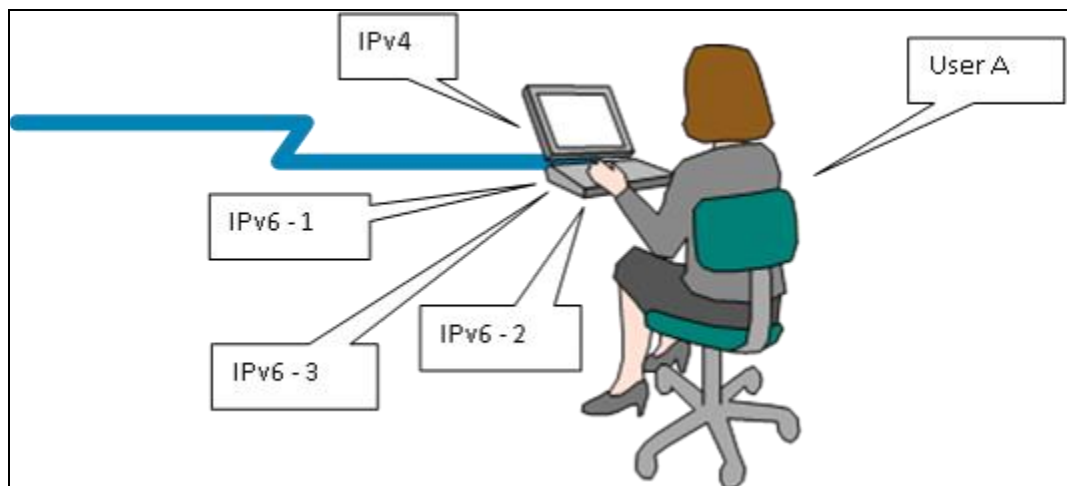
3. เปรียบวิธีวิจัย

3.1 แนวคิดในการออกแบบระบบ



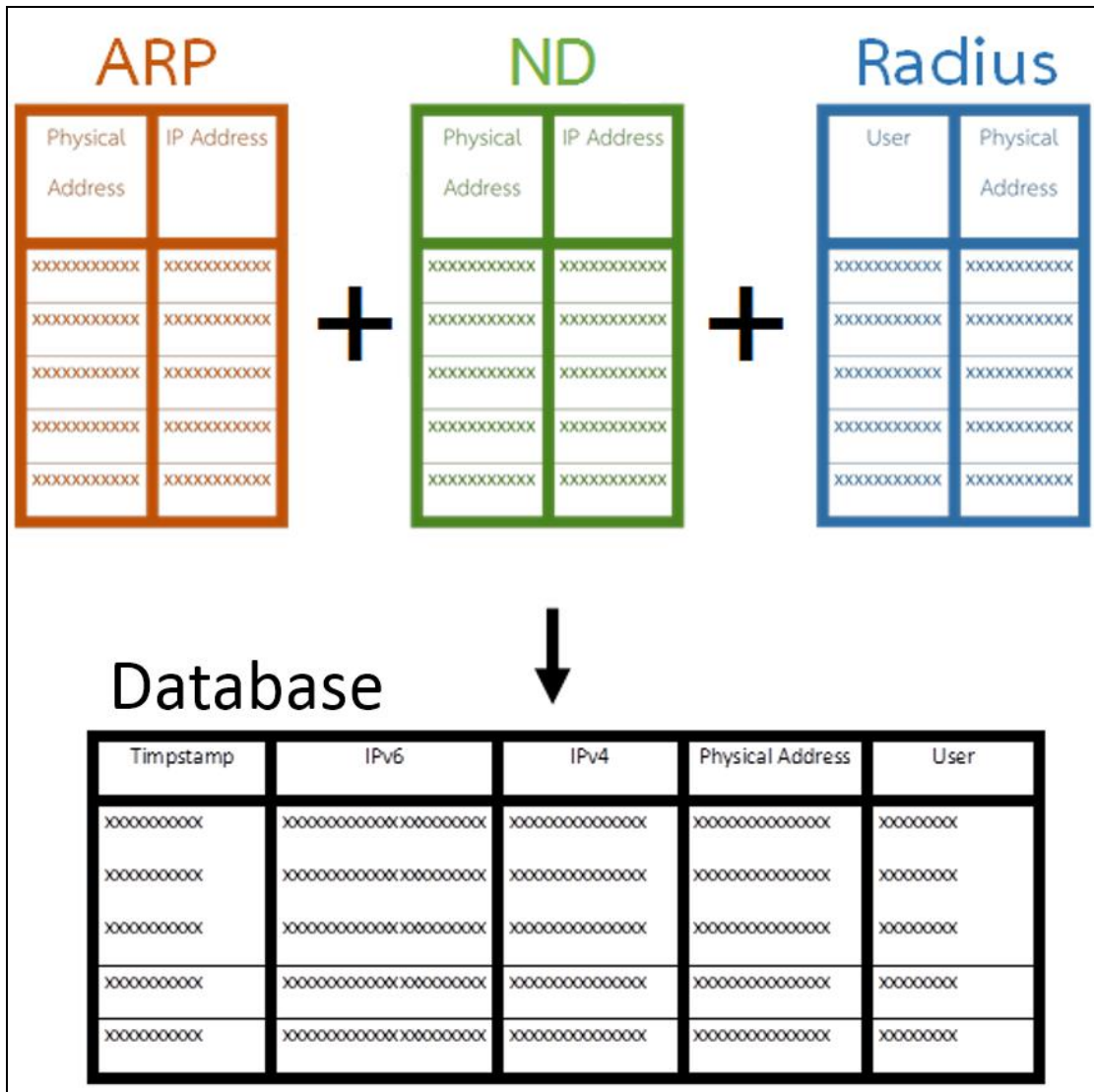
รูปที่ 3-1 Layer3 switch

ใน Layer3 switch ซึ่งทำงานบน Layer3 OSI model มีการเก็บ ตารางระหว่าง IP Address และ Physical Address ซึ่งก็คือ ตาราง ARP ใน IPv4 และ ND ใน IPv6 ในส่วนของผู้ใช้ ทาง radius server จะมีการเก็บข้อมูลชื่อผู้ใช้ และ Physical Address อยู่แล้ว ดังนั้นจากสมมติฐานว่า “ในช่วงเวลาเดียวกันอุปกรณ์ที่มี IP Address ซึ่งมาจาก Physical Address เดียวกัน ย่อมเป็นอุปกรณ์เดียวกัน และ ย่อมเป็น ผู้ใช้คนเดียวกัน” ดังรูปที่



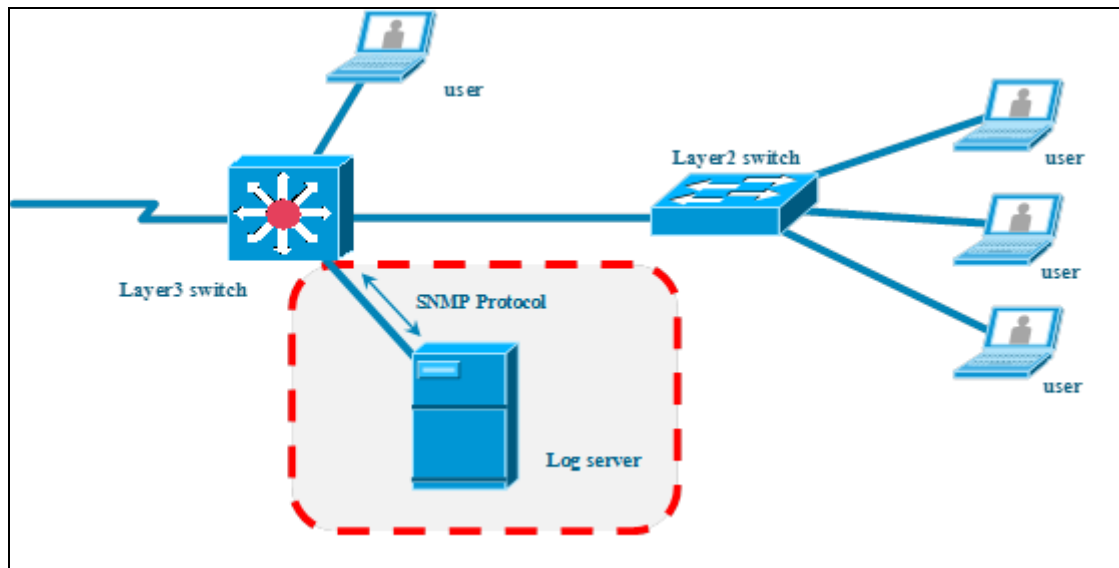
รูปที่ 3-2 แนวคิดการทำงานของการระบุตัวตน

ดังนั้นเราจึงสามารถระบุผู้ใช้ของ IP Address ใน IPv6 ได้ทางอ้อมจากการเทียบผู้ใช้ที่มี Physical Address เดียวกันกับ IP Address ที่ต้องการทราบ โดยใช้ข้อมูลจากตาราง ARP ซึ่งสามารถระบุ IPv4 ของ Mac Address นั้นได้, ตาราง ND ซึ่งสามารถระบุ IPv6 ของ Mac Address นั้นได้และข้อมูลจาก Radius Server ซึ่งจะช่วยระบุ User ได้ ดังรูปที่ 3-38



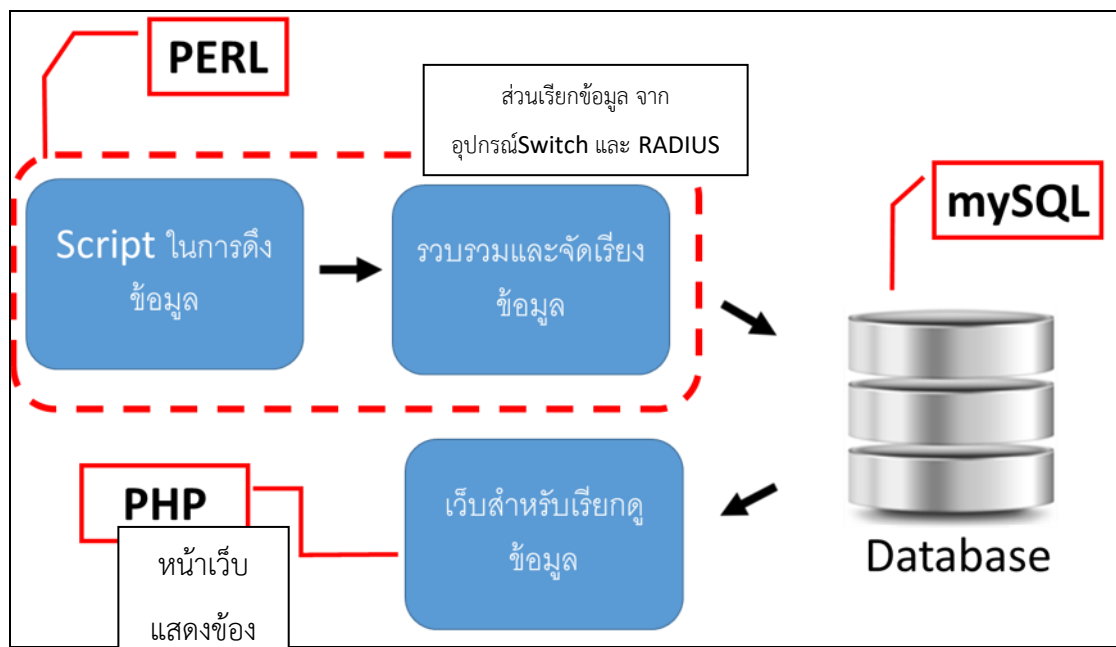
รูปที่ 3-38 แนวทางการเก็บข้อมูล

3.2 ระบบที่ได้ออกแบบ



รูปที่ 9 ภาพรวมระบบที่ได้ออกแบบ

ระบบที่ได้ออกแบบจะเป็น server ที่เชื่อมต่อกับเครือข่ายที่สามารถเข้าไปดึงค่าต่าง ๆ ของอุปกรณ์ switch ได้โดยการติดต่อจะใช้ SNMP Protocol ในการติดต่อสื่อสารกับอุปกรณ์ switch ได้ดังรูปที่ 9



รูป 3-5 ส่วนประกอบหลักของโครงการ

โดยการทำงานจะแบ่งออกเป็น 3 ส่วนใหญ่ๆ ดัง โดย

ส่วนที่ 1 จะเป็นสคริปต์ที่ทำงานตลอดเวลาเพื่อรับค่าจากอุปกรณ์ switch และนำมาวิเคราะห์หาผู้ใช้ให้กับ หมายเลข IP Address ที่เป็น IPv6 และส่งต่อไปให้กับส่วนที่ 2

ส่วนที่ 2 จะเป็นฐานข้อมูลที่ใช้เก็บข้อมูลที่ผ่านมากระบวนการจากส่วนที่หนึ่งมาแล้ว

ส่วนที่ 3 จะเป็นส่วนของเว็บแอปพลิเคชันที่นำข้อมูลจาก ฐานข้อมูลในส่วนที่ 2 มาจัดรูปแบบและแสดงผลตามที่ต้องการ โดยจะมีการวิเคราะห์ ทำสถิติจากข้อมูลที่มี และสามารถค้นหารายการตามที่สนใจได้

3.3 การทดสอบระบบ

เนื่องจากได้แบ่งเป็นส่วนๆอย่างชัดเจน การทดสอบระบบจึงสามารถทำได้โดยการทดสอบเป็นส่วนๆ และส่วนย่อยของแต่ละส่วน เช่น ค่าที่รับได้ออกมาเป็นอย่างไร ตีความหมายแล้วได้ผลลัพธ์อย่างไร ตรงกับสิ่งที่ต้องการหรือไม่ สามารถส่งต่อไปยังส่วนต่อไปหรือสามารถเรียกใช้จากส่วนก่อนหน้าได้ถูกต้องหรือไม่หรือไม่ และทดลองสุ่มผลลัพธ์ เพื่อตรวจสอบค่าจากเครื่องตัวอย่าง

4. ผลและวิเคราะห์ผลการทดลอง

4.1 การทดสอบการจำลองระบบลงชื่อเข้าใช้

เป็นการจำลองสภาพแวดล้อมการลงชื่อเข้าใช้แบบ 802.1x โดยใช้อุปกรณ์ switch เป็นเชื่อมต่อ กับ radius server ซึ่งใช้ free radius เป็น radius server



รูปที่ 4-1 รูปตัวอย่างการลงชื่อเข้าใช้ของระบบที่จำลองขึ้น

4.2 การทดสอบระบบส่วนเบื้องหลัง

ในส่วนนี้ เป็นส่วนสคริปต์ที่มีการเรียกข้อมูลจากอุปกรณ์ switch แล้วนำค่าที่ได้จากส่วนของ IPv6, IPv4, Mac Address และ ผู้ใช้ จาก Radius Server มาเปรียบเทียบกันเป็นระยะ ๆ แล้วส่งข้อมูลไปยังส่วนที่ 2 ซึ่งก็คือส่วนของฐานข้อมูล โดยข้อมูลที่อยู่ของ switch ตำแหน่งเครื่อง server และข้อมูลเกี่ยวกับการเชื่อมต่อฐานข้อมูล ระยะของช่วงเวลาที่มีการเรียกข้อมูลจะนำมาจากข้อมูลที่กำหนดไว้ในไฟล์ ในส่วนการตั้งค่า ของระบบโดยจะมีการกำหนดช่วงเวลเป็นวินาที

```

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*5cyp768"; # 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*5cyp768"; # password for access logdatabase.
28 my $logdatabase = "proj"; # database name
29 |
30 #####

```

รูปที่ 4-2 ตัวอย่างไฟล์การตั้งค่าช่วงเวลาการตรวจสอบ

ซึ่งในการเรียกข้อมูลจากอุปกรณ์ switch จะได้ลักษณะของข้อมูลตาม รูปที่ 2-3 และ รูปที่ 2-4 แล้วจึงนำค่าที่ได้มาแยกข้อมูล และนำมาเปรียบเทียบกัน ซึ่งจะได้ข้อมูลของ IP Address ทั้งในส่วนของ IPv6 IPv4 และ MAC Address ของอุปกรณ์ในเวลานั้น ๆ และเมื่อนำข้อมูลที่ได้ไปเปรียบเทียบกับข้อมูลการลงชื่อเข้าใช้ของ radius server จะทำให้สามารถคาดเดาได้ว่า IPv6 ของอุปกรณ์ที่อยู่ในเครือข่ายนั้น เข้าใช้ด้วยชื่อผู้ใด และส่งข้อมูลที่ไปยังฐานข้อมูลได้ โดยสามารถเข้าไปดูประวัติการ ลงชื่อเข้าใช้ของผู้ใช้ได้ ดังรูปที่ 4-8

```

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

การนำข้อมูลชื่อผู้เข้ามาหาความสัมพันธ์กับข้อมูลการใช้นั้น นำมาจากข้อมูล ในส่วนของ radius server ซึ่งจะมีข้อมูลต่างๆ เช่น วัน เวลา ที่มีการเข้าสู่ระบบ ipaddress และอื่นๆ ดังรูปที่ 4-4

```

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

```

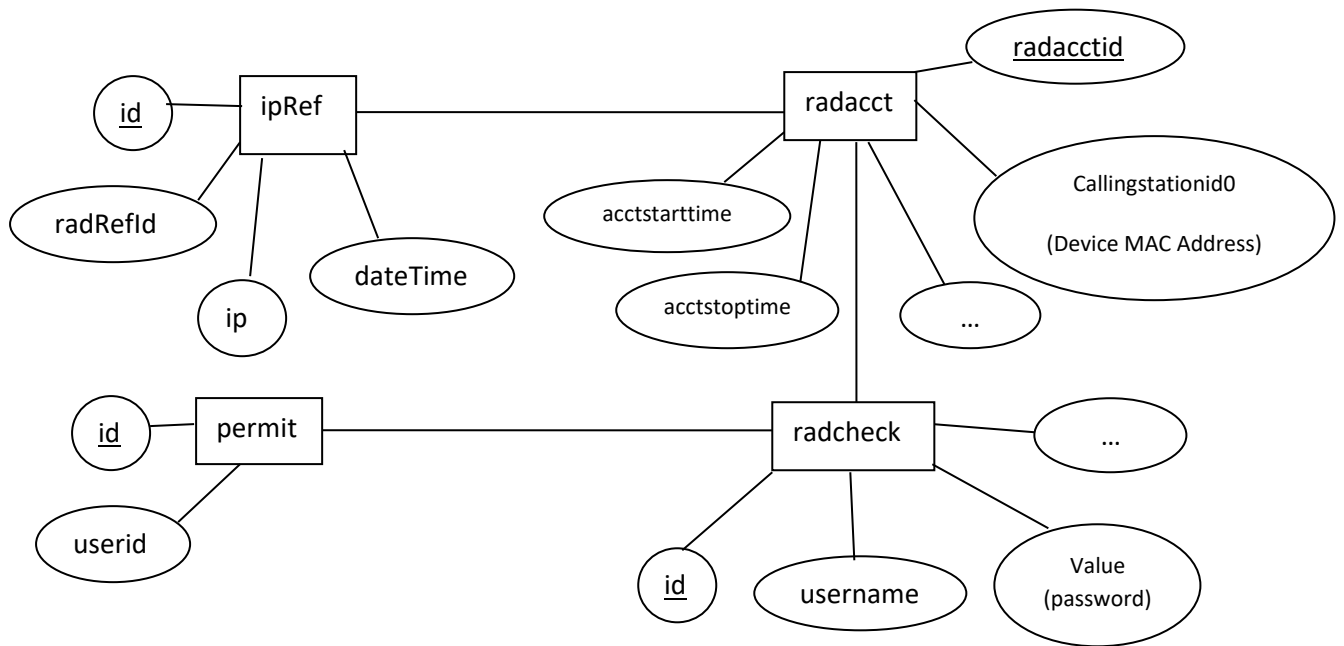
รูปที่ 4-4 ตัวอย่าง log ของ radius server ที่มาจากการยืนยันตัวตนในระบบ

การคาดเดาถึงผู้ใช้ในระบบ IPv6 จึงสามารถอ้างอิงจากข้อมูลการลงชื่อเข้าใช้ในระบบ IPv4 จาก radius server ได้โดยการเทียบ MAC Address

4.3 การทดสอบระบบส่วนฐานข้อมูล

ออกแบบฐานข้อมูล และสร้างฐานข้อมูลเพื่อเก็บข้อมูลจากส่วนเบื้องหลัง โดยจะมีการแยกเป็นตารางย่อย ๆ 2 ตารางได้แก่ ตาราง permit และตาราง ipRef โดยใช้งานร่วมกับตาราง radacct และ radcheck ของ freeradius ที่มีให้ใช้อยู่แล้ว

และตาราง ipRef จะเก็บ ข้อมูล IP Address ของเครื่องที่เชื่อมต่ออยู่ และ id ที่อ้างอิงตารางการลงชื่อเข้าใช้ ของ radius server



รูปที่ 4-5 ER-Diagram ของฐานข้อมูล

ซึ่ง ตาราง permit จะเป็นตารางในการกำหนดสิทธิ์ของ user คนนั้น ๆ ว่าจะเป็นผู้ดูแลระบบหรือไม่ โดยจะเก็บ user id ของตาราง ผู้ใช้ของ radius server

<u>id</u>	userid
1	1

และตาราง ipRef จะเก็บ ข้อมูล IP Address ของเครื่องที่เชื่อมต่ออยู่ และ id ที่อ้างอิงตารางการลงชื่อเข้าใช้ ของ radius server

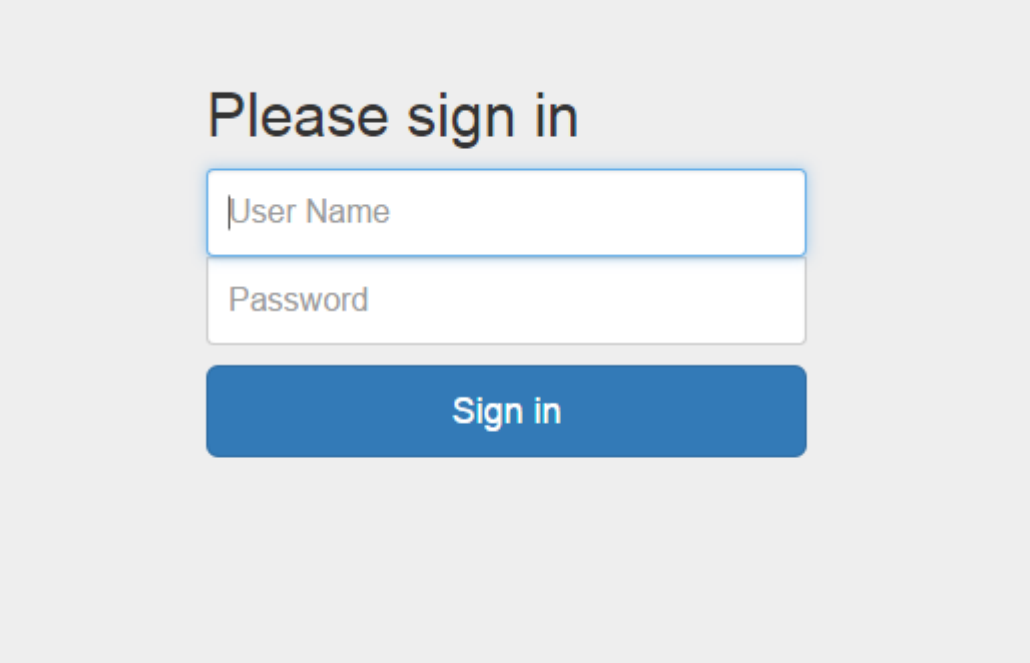
<u>id</u>	radRefId	ip	dateTime
1	29	FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB	2016-09-03 12:57:01
2	29	172.30.231.6	2016-09-03 12:57:01
3	29	2001:03C8:9009:01E7:0900:7AD7:4AD0:856C	2016-09-03 12:57:01

4.4 การทดสอบระบบในส่วนแสดงผล

ในส่วนนี้เป็นส่วนของเว็บแอปพลิเคชันที่นำข้อมูลจากฐานข้อมูลมาแสดงผล ในส่วนนี้เขียนขึ้นด้วย ภาษา php และ html โดยมีการให้สิทธิ์ผู้ใช้เป็น 2 ส่วน คือ

1. ผู้ใช้ทั่วไป สามารถดูบันทึกของระบบส่วนที่เป็นของตัวเองได้
2. ผู้ดูแลระบบ สามารถดูบันทึกการใช้งานของผู้ใช้ทั้งหมด และ แก้ไข ลบ หรือเพิ่มผู้ใช้ใหม่ได้

หน้า login ใช้ในการเข้าสู่ระบบ โดยเมื่อกรอก ชื่อผู้ใช้ และรหัสผ่านที่ถูกต้อง ก็จะเข้าใช้งานได้ ตามสิทธิ์ของผู้ใช้คนนั้น



The image shows a login interface with a light gray background. At the top, the text 'Please sign in' is displayed in a large, bold, black font. Below this, there are two white input fields with blue borders. The first field is labeled 'User Name' and the second is labeled 'Password'. Both labels are in a light gray font. Below the input fields is a blue button with the text 'Sign in' in white. The entire form is centered on the page.

รูปที่ 4-6 หน้าเว็บสำหรับการเข้าสู่ระบบ ดูบันทึกการใช้งาน

สำหรับผู้ทั่วไปเมื่อเข้ามาสู่ระบบแล้วจะสามารถดูข้อมูลการใช้ได้เฉพาะส่วนที่เป็ของตัวผู้ใช้งาน
โดยสามารถตัวกรอง เพื่อกรองผลลัพธ์การแสดงผลได้

User Log Management System

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

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

IP Address(v4 / v6) or MAC Address

[Search](#)

Username	ACC time start	ACC time stop	Device Vender	Physical Address	IP Address
IPv6	2016-04-22 02:00:36	2016-04-22 02:01:00	Apple, Inc.	00-25-4B-A7-2E-D4	172.30.231.6 2001:03C8:9009:01E7:0900:7AD7:4AD0:856C FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB
IPv6	2016-04-22 01:06:18	2016-04-22 01:06:43	Apple, Inc.	00-25-4B-A7-2E-D4	172.30.231.6 2001:03C8:9009:01E7:0900:7AD7:4AD0:856C FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB

รูปที่ 4-7 หน้าเว็บสำหรับการ ดูบันทึกการใช้งาน ในมุมมองผู้ทั่วไป

สำหรับผู้ดูแลระบบเมื่อเข้ามาสู่ระบบแล้วจะสามารถดูข้อมูลการใช้ได้ทั้งหมด โดยสามารถตัว
กรอง เพื่อกรองผลลัพธ์การแสดงผลได้เช่นกัน

User Log Management System

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

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

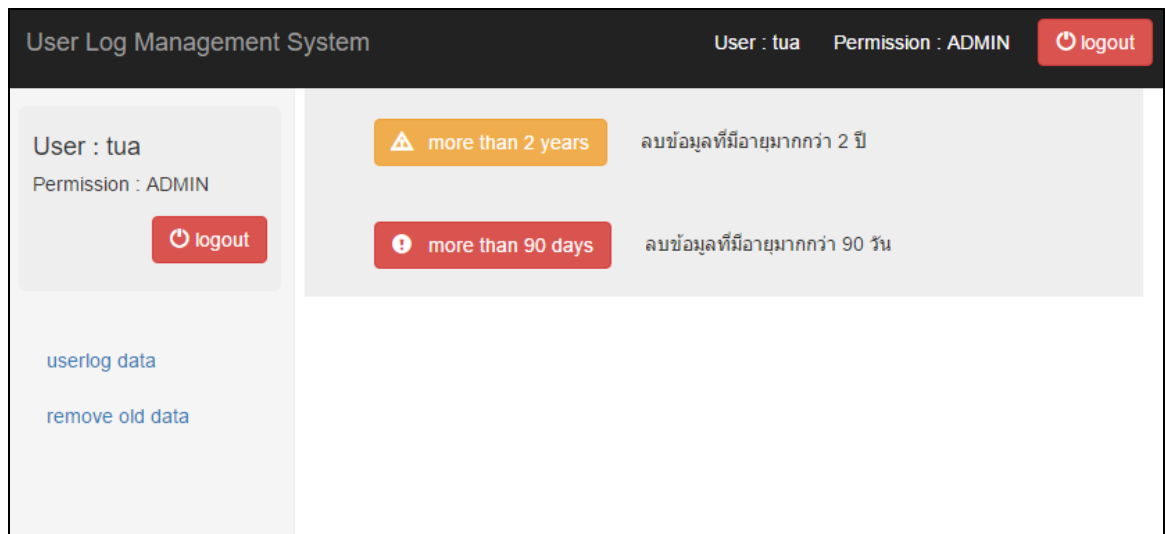
IP Address(v4 / v6) or MAC Address

[Search](#)

Username	ACC time start	ACC time stop	Device Vender	Physical Address	IP Address
tua	2016-11-15 16:04:19	connect until now	ASUSTek COMPUTER INC.	BC-EE-7B-53- 4F-A0	172.30.231.17 2001:03C8:9009:01E7:71B1:3C53:BCFA:F4CB FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB
tua	2016-10-04 16:38:51	2016-10-05 06:21:47	ASUSTek COMPUTER INC.	BC-EE-7B-53- 4F-A0	172.30.231.15 2001:03C8:9009:01E7:50F8:8439:99C0:DD70 FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB
tua	2016-09-30 23:25:50	2016-10-02 17:38:14	ASUSTek COMPUTER INC.	BC-EE-7B-53- 4F-A0	172.30.231.14 2001:03C8:9009:01E7:A572:2D13:C27D:2F46 FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB 2001:03C8:9009:01E7:71B1:3C53:BCFA:F4CB
tua	2016-09-27 18:12:21	2016-09-30 23:22:16	ASUSTek COMPUTER INC.	BC-EE-7B-53- 4F-A0	172.30.231.14 2001:03C8:9009:01E7:11A3:2149:521A:BEE3

รูปที่ 4-8 หน้าเว็บสำหรับการ ดูบันทึกการใช้งาน ในมุมมองผู้ดูแลระบบ

ผู้ดูแลระบบ สามารถ ลบข้อมูลการลงชื่อเข้าใช้ได้ โดยสามารถเลือกได้ว่าจะลบข้อมูลที่มีอายุมากกว่า 2 ปี หรือข้อมูลที่มีอายุมากกว่า 90 วัน ได้



รูปที่ 4-9 หน้าเว็บสำหรับการ แก้ไขผู้ใช้งาน ในมุมมองผู้ดูแลระบบ

5. สรุปผลและข้อเสนอแนะ

5.1 สรุปผล

ในส่วนการทำงานของระบบในแต่ละส่วนสามารถทำงานได้ โดยส่วนเบื้องหลังโดยรวมสามารถทำงานได้โดยสามารถเรียกค่าจากตาราง ARP และตาราง ND โดยใช้ SNMP Protocol ได้และนำมาจับคู่กันตาม Physical Address ได้ และส่งข้อมูลไปยัง ฐานข้อมูลได้

ในส่วนของฐานข้อมูลก็ได้มีการออกแบบและทดลองใช้งานจากสคริปต์ที่เขียนขึ้นในส่วนแรกพบว่าสามารถทำงานได้สมบูรณ์ครบถ้วน

ในส่วนของเว็บแอปพลิเคชัน สามารถนำข้อมูลจากฐานข้อมูลมาแสดงผลได้ มีการแบ่งระดับสิทธิ์ผู้ใช้เป็น 2 ส่วนคือผู้ดูแลระบบ และผู้ทั่วไป โดย ผู้ใช้ทั่วไป สามารถดูบันทึกของระบบบนส่วนที่เป็นของตัวเองได้เท่านั้น และ ผู้ดูแลระบบสามารถดูบันทึกการใช้งานของผู้ใช้ทั้งหมด และสามารถ ลบข้อมูลการลงชื่อเข้าใช้ ที่มากกว่า 2 ปี หรือมากกว่า 90 วันได้

5.2 ปัญหาและอุปสรรค

เนื่องจากการออกแบบวิธีการเรียกข้อมูล ของหน้าเว็บทำได้ไม่ดี จึงทำให้ใช้เวลาในการเรียกหน้าการแสดงผลนานเกินไป การมาแก้รูปแบบวิธีการในภายหลังทำให้เสียเวลาในการแก้ไขงานเพิ่มขึ้น

5.3 ข้อเสนอแนะ

เนื่องจากระบบที่ได้ออกแบบใช้วิธีการตรวจสอบแบบ pooling คือการตรวจสอบเป็นรอบ ๆ จึงทำให้ความแม่นยำของข้อมูลขึ้นกับความถี่ของการตรวจสอบ

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: Layer 3 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/snmpthorus/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)

7. ภาคผนวก

ส่วนนี้อาจจะมีหรือไม่มีก็ได้ ควรจะเป็นข้อมูลที่ไม่อยู่ในส่วนอื่น ๆ เป็นข้อมูลโดยละเอียด เช่น data sheet ของอุปกรณ์ที่คุณใช้ (สอบถามอาจารย์ที่ปรึกษาก่อนว่าต้องใส่หรือไม่ อย่างไร) คนที่ทำโครงการในการพัฒนาซอฟต์แวร์ ควรจะใส่คู่มือการใช้งาน และ technical manual หรือ source code (หากอาจารย์ที่ปรึกษาเห็นสมควร)

โดยภาคผนวกอาจจะแบ่งเป็นหมวดย่อย ๆ ออกไปอีกก็ได้ ตามสมควร