ระบบยืนยันตัวตนบนระบบเครือข่ายแบบ Dual-Stack ผ่านเว็บบราวเซอร์ กรณีศึกษา: มหาวิทยาลัยศรีนครินทรวิโรฒ

DUAL-STACK AUTHENTICATION WITH CAPTIVE PORTAL IN SRINAKHARINWIROT UNIVERSITY CAMPUS NETWORK

โดย

ธัญย์ธรฐ์ พงษ์เฉลิม

TUNYATON PONGCHALERM

อาจารย์ที่ปรึกษา

รศ.ดร.โชติพัชร์ ภรณวลัย

รายงานนี้เป็นส่วนหนึ่งของวิชาศึกษาอิสระ 2

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ภาคเรียนที่ 2 ปีการศึกษา 2558

DUAL-STACK AUTHENTICATION WITH CAPTIVE PORTAL IN SRINAKHARINWIROT UNIVERSITY CAMPUS NETWORK

TUNYATON PONGCHALERM

A REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS OF THE COURSE
INDEPENDENT STUDY 2
MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG
2/2015

ใบรับรองการศึกษาอิสระ 2 (Independent Study 2)

เรื่อง

ระบบยืนยันตัวตนบนระบบเครือข่ายแบบ Dual-Stack ผ่านเว็บบราวเซอร์ กรณีศึกษา: มหาวิทยาลัยศรีนครินทรวิโรฒ

Dual-Stack Authentication with Captive Portal

in Srinakharinwirot University Campus Network

นางสาวธัญย์ธรฐ์ พงษ์เฉลิม

รหัสประจำตัว 57606062

ขอรับรองว่ารายงานฉบับนี้ ข้าพเจ้าไม่ได้คัดลอกมาจากที่ใด

รายงานฉบับนี้ได้รับการตรวจสอบและอนุมัติให้เป็นส่วนหนึ่งของ

การศึกษาวิชาการศึกษาอิสระ 2 หลักสูตรวิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศ)

ภาคเรียนที่ 2 ปีการศึกษา 2558

.....อาจารย์ที่ปรึกษา

(รศ.ดร.โชติพัชร์ ภรณวลัย)

.....กรรมการสอบ

(รศ.ดร.อาริต ธรรมโน)

.....กรรมการสอบ

(ผศ.ดร.ปานวิทย์ ธุวะนุติ)

หัวข้อ	ระบบยืนยันตัวตนบนระบบเครือข่ายแบบ Dual-Stack ผ่านเว็บบราวเซอร์ กรณีศึกษา: มหาวิทยาลัยศรีนครินทรวิโรฒ
นักศึกษา	นางสาวธัญย์ธรฐ์ พงษ์เฉลิม
รหัสนักศึกษา	57606062
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
แขนงวิชา	เทคโนโลยีเครือข่ายและระบบ
ปีการศึกษา	2558
อาจารย์ที่ปรึกษา	รศ.ดร.โชติพัชร์ ภรณวลัย

บทคัดย่อ

ประเทศไทยมีการผลักดันให้มีการใช้งาน IPv6 ตามแผนแม่บทของชาติ แต่การใช้งานนั้นยังไม่สามารถเกิดขึ้นได้อย่างเต็มที่ เนื่องจากองค์กรทั่วไปที่มีการใช้งาน IPv6 ไม่มีการจัดเก็บข้อมูลจราจรของ IPv6 ดังนั้นจึงได้มีการจัดทำระบบขึ้นมาเพื่อให้มหาวิทยาลัยที่มีการเปิดใช้งาน IPv6 สามารถใช้งาน IPv6 ได้และมีการจัดเก็บข้อมูลการจราจร ซึ่งในระบบนี้จะทำการจัดเก็บข้อมูล IPv4 และ IPv6 ที่เป็นแบบ Dual-stack โดยจับคู่กับรหัสผู้ใช้งาน เพื่อให้เป็นไปตามพระราชบัญญัติการกระทำความผิดทางคอมพิวเตอร์ ปี 2550 นอกจากนั้นระบบยังมีการปรับ IPv6 address ให้เป็นปัจจุบัน เพื่อป้องกันปัญหาที่ Temporary IPv6 address เปลี่ยนไปทำให้ระบบการจัดเก็บมีความถูกต้องสมบูรณ์ โดยระบบนี้จะทำการแสดงหน้าจอ Captive Portal เพื่อให้ผู้ใช้งานทำการยืนยันตัวตน ซึ่งเมื่อยืนยันตัวตนแล้วระบบจะนำค่าหมายเลข IPv4 และ IPv6 จากเครื่องลูกข่ายไปเปิดสิทธิอนุญาตให้ผ่านไฟร์วอลล์ ทำให้สามารถจัดเก็บข้อมูลการจราจร และสามารถใช้งานระบบเครือข่ายอินเทอร์เน็ตของมหาวิทยาลัยได้

Title	Dual-Stack Authentication with Captive Portal in Srinakharinwirot University Campus Network
Student	Miss.Tunyaton Pongchalerm
Student ID.	57606062
Degree	Master of Science
Program	Information Technology
Major	Network and Systems Technology
Academic Year	2015
Advisor	Assoc. Dr. Chotipat Pornavalai

ABSTRACT

In the national master plan of Thailand that pushing IPv6 usage. However, usability cannot be achieved fully. Because organizations are using IPv6 without storage traffic of IPv6. Thus, it had to be made to allow universities who enable IPv6 can use IPv6 connectivity and storage the traffic log. For Computer Crime Act B.E 2550 (2007), the system store IPv4 and IPv6 in Dual-stack that is matched with username. And, also update IPv6 address as in present to prevent the Temporary IPv6 address changing. It made the system complete accuracy. The system will display Captive Portal for user authentication. Once verified, it will bring IPv4 and IPv6 address of client to allow in the firewall. This system make it can store traffic data and can use the internet network of university.

กิตติกรรมประกาศ

การดำเนินโครงงานนี้ได้รับการให้คำแนะนำจาก รศ.ดร.โชติพัชร์ ภรณวลัย ซึ่งเป็นอาจารย์ที่ปรึกษาโครงงานนี้ ขอขอบพระคุณเป็นอย่างสูงที่อาจารย์ได้ให้มุมมองในการทดสอบต่างๆในแง่มุมที่ผู้ศึกษาไม่เคยนึกถึง สอนให้ได้คิดเองทำเอง เปิดโอกาสให้ได้แสดงความคิดเห็นของตัวเองอย่างไม่ปิดกั้นความคิด พร้อมให้คำแนะนำเพิ่มเติมกลับมาเพื่อใช้ในดำเนินการต่อ สิ่งเหล่านี้ช่วยให้ผู้ศึกษารู้สึกมีความมั่นใจในการทำโครงงานมากยิ่งขึ้น

ขอขอบคุณ คุณมหัทธวัฒน์ รักษาเกียรติศักดิ์ ซึ่งขณะนี้ดำรงตำแหน่งผู้ช่วยผู้อำนวยการสำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ ที่ให้คำปรึกษาทางด้านเทคนิคต่างๆที่สำคัญมากสำหรับโครงงาน อีกทั้งเป็นผู้กระตุ้นให้ผู้ศึกษามีความภาคภูมิใจในตนเอง ภูมิใจในสิ่งที่กำลังทำ ซึ่งเป็นตัวขับเคลื่อนให้ผู้ศึกษารู้สึกไม่ย่อท้อที่จะดำเนินการต่อจนเสร็จ

ขอบคุณเพื่อนร่วมงานทุกท่านที่ได้ให้ความช่วยเหลือในการพัฒนาและทดสอบระบบ คำแนะนำเล็กๆน้อยๆของทุกท่านได้เติมเต็มความสมบูรณ์ของโครงงานนี้ให้สำเร็จไปได้ด้วยดี

ขอบคุณครอบครัว พงษ์เฉลิมและเพื่อนๆทุกท่าน ที่เป็นกำลังใจและเป็นผู้ให้การสนับสนุนผู้ศึกษามาโดยตลอด

ขอบคุณความอนุเคราะห์จาก สำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ ที่ให้โอกาสผู้ศึกษาได้พัฒนาระบบนี้ขึ้นมา และสนับสนุนให้ผู้ศึกษาได้เข้าเรียนต่อในระดับปริญญาโท

โครงงานนี้สามารถสำเร็จได้ด้วยดี เนื่องมาจากได้รับความช่วยเหลือและคำแนะนำ จากบุคคลที่สำคัญหลายท่าน ผู้ศึกษามีความซาบซึ้งใจในความใจดี และมีน้ำใจของทุกท่านเป็นอย่างมาก ซึ่งหากจะกล่าวถึงทุกท่านคงจะต้องใช้กระดาษเป็นจำนวนหลายหน้า ท่านใดที่ไม่ได้ถูกกล่าวชื่อในกิตติกรรมประกาศนี้ ขอให้ท่านรับทราบว่าข้าพเจ้ารู้สึกเป็นเกียรติยิ่งที่ได้รับความช่วยเหลือจากท่านเช่นกัน

ผู้จัดทำ

นางสาวธัญย์ธรฐ์ พงษ์เฉลิม

กรกฎาคม 2559

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญรูป

รูปที่ หน้า

สารบัญรูป (ต่อ)

รูปที่ หน้า

สารบัญรูป (ต่อ)

รูปที่ หน้า

สารบัญตาราง

ตารางที่ หน้า

บทที่ 1

บทนำ

1.1 ความเป็นมาของโครงการ

ตามที่คณะรัฐมนตรีได้มีมติเห็นชอบแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของประเทศไทย (ฉบับที่ 2) และแผนปฏิบัติการเพื่อผลักดัน ส่งเสริม เร่งรัด และติดตามผลการดำเนินงานอินเทอร์เน็ตโพรโทคอลรุ่นที่ 6 (IPv6) ในประเทศไทย (พ.ศ. 2556- 2558) โดยได้กำหนดกรอบนโยบายระดับชาติในการส่งเสริมการใช้งานหมายเลขไอพีแอดเดรสที่เป็นอินเทอร์เน็ตโพรโทคอลรุ่นที่ 6 หรือ IPv6 เพื่อทดแทนหมายเลขไอพีแอดเดรสที่เป็นอินเทอร์เน็ตโพรโทคอลรุ่นที่ 4 หรือ IPv4 ซึ่งกำลังถูกใช้หมดไป และไม่เพียงพอกับการใช้งานอินเทอร์เน็ตในอนาคต

เนื่องจากในปัจจุบันอุปกรณ์ต่างๆมีการพัฒนาให้มีความสามารถในการเชื่อมต่อกับอินเทอร์เน็ตได้ ทำให้ไอพีแอดเดรสเป็นสิ่งจำเป็นอย่างยิ่งกับอุปกรณ์เหล่านี้เพื่อใช้ในการติดต่อสื่อสารผ่านเครือข่ายอินเทอร์เน็ต ในองค์กรการศึกษาอย่างเช่น มหาวิทยาลัย ก็เริ่มมีอัตราการใช้งานอุปกรณ์ที่มีความต้องการเชื่อมต่อกับเครือข่ายเพิ่มมากขึ้น เช่น โทรศัพท์ผ่านเครือข่าย (Voice Over IP : VoIP) คอมพิวเตอร์ และสมาร์ทโฟน เป็นต้น ทำให้มีปริมาณความต้องการไอพีแอดเดรสที่มากขึ้น ซึ่งในอนาคตอินเทอร์เน็ตโพรโทคอลรุ่นที่ 4 (IPv4) มีแนวโน้มว่าจะไม่เพียงพอต่อการใช้งานอีกต่อไป เพื่อรองรับความต้องการในอนาคต การนำอินเทอร์เน็ตโพรโทคอลรุ่นที่ 6 มาใช้จึงเป็นสิ่งที่จำเป็น ดังนั้นจึงควรดำเนินการให้ระบบเครือข่ายมีความสามารถที่จะนำอินเทอร์เน็ตโพรโทคอลรุ่นที่ 6 มาใช้งานได้อย่างเป็นรูปธรรม

การจะนำอินเทอร์เน็ตโพรโทคอลรุ่นที่ 6 มาใช้งานนั้น ไม่สามารถที่จะนำมาปรับใช้งานได้ทันที เนื่องมาจากหลายสาเหตุด้วยกัน เช่น อุปกรณ์ของผู้ใช้งาน อุปกรณ์เครือข่ายที่ไม่รองรับการใช้งาน IPv6 และสาเหตุหลักที่ทำให้ภาครัฐและเอกชนไม่สามารถดำเนินการติดตั้งและใช้งาน IPv6 ได้ก็คือ เรื่อง “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550” ที่ต้องมีการเก็บข้อมูลการใช้งานเครือข่าย ทั้ง IPv4 และ IPv6 โดยจะต้องสามารถระบุตัวตนผู้ใช้งานเครือข่าย และต้องจัดเก็บไว้อย่างน้อย 90 วัน

มหาวิทยาลัยศรีนครินทรวิโรฒปัจจุบันมีการจัดเก็บข้อมูลการใช้งานเครือข่ายตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เฉพาะการใช้งาน IPv4 เท่านั้น แต่การใช้งาน IPv6 ยังไม่มีการจัดเก็บข้อมูลผู้ใช้งาน ส่งผลให้เมื่อเกิดปัญหาจากการใช้งาน IPv6 ไม่สามารถติดตามหรือหาผู้กระทำความผิดมารับโทษได้ ดังนั้นจึงเห็นว่าการดำเนินการ

โครงการนี้จะก่อให้เกิดประโยชน์กับมหาวิทยาลัยศรีนครินทรวิโรฒ และหรือองค์กรอื่นๆที่สนใจนำระบบนี้ไปใช้งานเพื่อก่อให้เกิดการผลักดันการใช้งาน IPv6 ในประเทศไทยเพิ่มขึ้นตามกรอบนโยบายของชาติต่อไป

1.2 วัตถุประสงค์ของการพัฒนาระบบ

เพื่อให้สามารถตรวจสอบและเก็บข้อมูลล็อก (Log) การใช้งานเครือข่าย IPv4 และ IPv6 ภายในมหาวิทยาลัยได้ ซึ่งการออกแบบระบบการจัดเก็บล็อกของ IPv6 ตามพ.ร.บ 2550 ทำให้มหาวิทยาลัยมีระบบการยืนยันตัวตนตามกฎหมาย และยังสามารถที่จะนำไปใช้กับมหาวิทยาลัยอื่น และหรือองค์กรอื่นๆที่ต้องการระบบการยืนยันตัวตนที่ใช้งาน โอเพนซอร์ส (Opensource) เป็นหลัก โดยมีการใช้ Captive Portal ในการยืนยันตัวตนผู้เข้าใช้งานระบบเครือข่าย ซึ่งการใช้งานโดยใช้ Captive Portal ปกติแล้วเครื่องที่ใช้งานที่เป็น Dual-Stack ที่เป็น IPv4 และ IPv6 นั้น เครื่องคอมพิวเตอร์จะใช้งาน IPv6 ก่อนซึ่งถ้าไม่สามารถใช้งาน IPv6 ได้จึงจะใช้งาน IPv4 ดังนั้นการที่จะมีระบบที่ทำการยืนยันตัวตนนั้น โดยทั่วไปจะต้องดำเนินการ Login ผ่าน Captive Portal 2 ครั้ง ซึ่งเป็นการยืนยัน IPv4 และ IPv6 อย่างละครั้งทำให้ผู้ใช้งานเกิดความสับสน ดังนั้นเพื่อให้สามารถจัดเก็บข้อมูลตาม พ.ร.บ 2550 ได้ตามกฎหมายและผู้ใช้งานสามารถทำการยืนยันตัวตนเพียงครั้งเดียวได้ จึงทำการพัฒนาระบบนี้ขึ้นมาเพื่อให้มหาวิทยาลัยสามารถใช้งานเครือข่าย IPv6 ไปยังเครือข่ายอินเทอร์เน็ตได้และมีการจัดเก็บข้อมูลล็อกทั้ง IPv4 และ IPv6 จับคู่กับรหัสผู้ใช้ภายในมหาวิทยาลัย

1.3 ขอบเขตของการพัฒนาระบบ

1) ออกแบบการจัดแบ่ง IPv6 (IPv6 address Plan)
2) ดำเนินการติดตั้งและตั้งค่าอุปกรณ์เครือข่าย (Configuration)
   2.1) ตั้งค่าอุปกรณ์ Layer 3 switch เพื่อให้รองรับ IPv6
   2.2) ตั้งค่าอุปกรณ์ไฟร์วอลล์ (Firewall) เพื่อให้รองรับ IPv6
3) ดำเนินการจัดเตรียมเซิร์ฟเวอร์ (Server) สำหรับติดตั้งระบบยืนยันตัวตน (Dual-Stack authentication via Captive Portal)
   3.1) ติดตั้งระบบปฏิบัติการ CentOS
   3.2) ติดตั้งระบบรักษาความปลอดภัยไฟร์วอลล์
   3.3) ติดตั้งเว็บเซิร์ฟเวอร์ (Web Server) Apache หรือ NginX
   3.4) ติดตั้ง php เพื่อใช้ในการเชื่อมต่อกับ LDAP
4) ดำเนินการเขียนโปรแกรมเพื่อทำการเชื่อมต่อกับ LDAP
5) ดำเนินการเขียนโปรแกรมระบบยืนยันตัวตน
   5.1) เขียนโปรแกรมเพื่อทำการดึงค่า IPv4 กับ IPv6 จากเครื่องคอมพิวเตอร์ลูกข่าย

5.2) เขียนโปรแกรมเพื่อทำการส่งค่า IPv4 กับ IPv6 ที่ได้ให้กับ Firewall

5.3) ทำการจัดเก็บค่า IPv4 กับ IPv6 จับคู่กับ username เพื่อใช้ในการเก็บล็อกยืนยันตัวตน

5.4) ทำการจัดเก็บล็อกการใช้งาน IPv4 และ IPv6

5.5) เขียนโปรแกรมเพื่อ Monitor IP address ตามเวลาที่กำหนดถ้าไม่มีการต่อเวลา ก็จะต้องดำเนินการ Logout ออกจากระบบ

6) ตรวจสอบการใช้งานและทดสอบประสิทธิภาพการใช้งานระบบยืนยันตัวตน

7) ดำเนินการจัดเก็บข้อมูลสถิติการใช้งาน IPv4 และ IPv6 ภายในมหาวิทยาลัย

1.4 ขั้นตอนการพัฒนาระบบ

1) ออกแบบและการจัดแบ่ง IPv6 address Plan
2) ดำเนินการติดตั้งและจัดตั้งค่าอุปกรณ์เครือข่าย (Configuration)
3) ดำเนินการติดตั้งระบบยืนยันตัวตน (Dual stack authentication via Captive Portal)
4) ดำเนินการเขียนโปรแกรมเพื่อทำการเชื่อมต่อกับ LDAP
5) ดำเนินการเขียนโปรแกรมระบบยืนยันตัวตน
6) ตรวจสอบการใช้งานและทดสอบประสิทธิภาพการใช้งานระบบยืนยันตัวตน
7) ดำเนินการจัดเก็บข้อมูลสถิติการใช้งาน IPv4 และ IPv6 ภายในมหาวิทยาลัย

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1) ได้รับความรู้ความเข้าใจเกี่ยวกับ IPv6
2) ได้ระบบยืนยันตัวตนสำหรับ IPv4 และ IPv6
3) ได้ระบบจัดเก็บข้อมูลการยืนยันตัวตน ตาม พรบ.คอมพิวเตอร์
4) ได้ข้อมูลการใช้งาน IPv4 และ IPv6 ในรูปแบบกราฟิก
5) ได้มีส่วนร่วมในการผลักดันประเทศให้ก้าวไปสู่การใช้งาน IPv6

บทที่ 2
ทฤษฎีพื้นฐานและเทคโนโลยีที่เกี่ยวข้อง

2.1 IPv6

IP version 6 (IPv6) คือ รูปแบบใหม่ของ Internet Protocol (IP) ที่ถูกพัฒนาขึ้นมาเพื่อใช้แทนที่การใช้งาน IP version 4 (IPv4) โดยวัตถุประสงค์หนึ่งในการพัฒนา IPv6 ขึ้นมาเพื่อลดปัญหาการขาดแคลนไอพีแอดเดรส (IP Address) เนื่องจาก IPv6 นั้นสามารถนำมากำหนดเป็นไอพีแอดเดรสได้จำนวนมาก และถูกออกแบบให้ช่วยลดความยุ่งยากในการทำงานของโพรโทคอลให้น้อยลง

2.1.1 คุณลักษณะ (Feature) ของ IPv6

1) มีเฮดเดอร์ (header) รูปแบบใหม่ เนื่องจาก IPv6 มีขนาดแอดเดรสเป็น 4 เท่าของ IPv4

2) สามารถมีแอดเดรสที่มากขึ้น เนื่องจากการที่แอดเดรสของ IPv6 มี 128 บิต (bit) และสามารถทำ subnet เพื่อแบ่ง network และ host ได้อีกเป็นจำนวนมาก

3) มีการออกแบบในเรื่องของ addressing และ routing infrastructure ได้ดีขึ้น เนื่องจากในส่วนของ routing มีการรวบรวม (summarizable) และส่งไปที่แต่ละ level ของ ISP

4) สามารถกำหนด stateless และ stateful address ได้ ซึ่งการกำหนด stateful address จะถูกกำหนดผ่านเซิร์ฟเวอร์ DHCP ส่วนในกรณีของ stateless configuration นั้น host ที่อยู่บนลิงก์ (link) จะถูกตั้งค่าโดยอัตโนมัติซึ่งจะเรียกว่า link-local address และแอดเดรสที่ได้จะมาจาก prefix ที่เร้าเตอร์ (Router) ประกาศออกมา

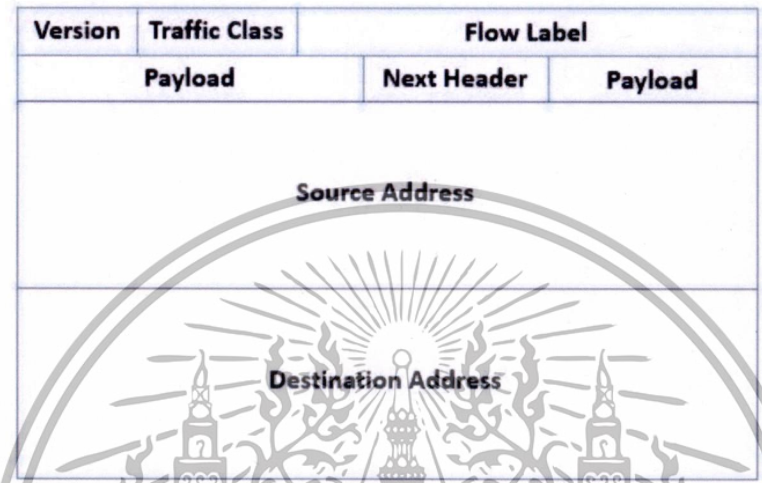
5) มีการรวมในเรื่องของความมั่นคงปลอดภัย (security) เข้าไป โดยการนำ IPSec รวมเข้าไปในโพรโทคอล IPv6 ด้วย

6) มีการรองรับ QOS (Quality of service) ที่ดีกว่า เนื่องจากในฟิลด์ (field) ของ IPv6 มีการกำหนดการจัดการเกี่ยวกับปริมาณการใช้งาน (traffic) ผ่านฟิลด์ flow label ทำให้ส่งข้อมูลระหว่างต้นทางและปลายทางได้อย่างมีประสิทธิภาพ และสามารถรองรับการทำ QOS ในกรณีที่มีการส่งแบบเข้ารหัสโดยใช้ IPSec ด้วย

7) มีโพรโทคอลใหม่ที่ใช้ในการติดต่อกับโหนด (node) ข้างเคียง คือ ICMPv6 (Internet Control Message Protocol v6) ซึ่งโพรโทคอลนี้จะมาแทนที่ Broadcast-based Address Resolution Protocol (ARP), ICMPv4 Router Discovery และ ICMPv

8) รองรับการเพิ่มคุณสมบัติ (feature) ใหม่ เนื่องจาก IPv6 สามารถเพิ่มเฮดเดอร์เข้าไปหลังจาก IPv6 header ได้ ซึ่งไม่เหมือนกับใน IPv4 ซึ่งมีได้เพียง 40 ไบต์ (byte) แต่ในส่วนของ IPv6 จะสามารถมีได้ตามจำนวนแพ็กเก็ตของ IPv6

2.1.2 IPv6 Header



รูปที่ 2.1 IPv6 header

รายละเอียดฟิลด์ของ IPv6 header มีดังต่อไปนี้

- **Version** จะใช้ 4 บิต เพื่อแสดงถึงเวอร์ชันของไอพี และถูกกำหนดเป็น 6
- **Traffic Class** จะแสดงถึงคลาส (class) และลำดับความสำคัญของ IPv6 packet ซึ่งขนาดของฟิลด์เท่ากับ 8 บิต ซึ่ง Traffic class จะคล้ายกับฟิลด์ Type of Service ใน IPv4 ตาม RFC 2460 จะไม่มีการกำหนดค่าของ Traffic class แต่อย่างไรก็ตามในส่วนของ IPv6 ก็ยังต้องการในเรื่องของคลาสเพื่อจะเป็นข้อมูลในการส่งไปยัง application layer
- **Flow Label** จะแสดงถึงลำดับของแพ็กเก็ตว่าเป็นลำดับใดของแพ็กเก็ตระหว่างต้นทางกับปลายทาง โดยจะใช้ใน IPv6 router ระหว่างทาง ซึ่งขนาดของฟิลด์จะเท่ากับ 20 บิต โดยปกติ flow label จะถูกกำหนดเป็น 0 ในกรณีข้อมูลไม่ต้องการให้ลำดับความสำคัญ ซึ่งถ้าข้อมูลที่ต้องการให้ลำดับความสำคัญสามารถกำหนดหลาย flow ได้ และในแต่ละ flow ต้องมีการกำหนดไม่ให้เป็น 0
- **Payload Length** จะแสดงถึงความยาวของ Payload โดยขนาดของฟิลด์จะเท่ากับ 16 บิต ฟิลด์ Payload Length นี้จะรวมถึง extension header และ upper layer PDU ซึ่งใน 16 บิตนั้น IPv6 payload จะสามารถขยายได้ถึง 65,535 ไบต์ ในกรณีของ payload ที่มากกว่า 65,535

ไบต์ สามารถกำหนด Payload length เป็น 0 และ เพิ่ม Jumbo Payload option เพื่อใช้ Hop-by-Hop options extension header ได้

- **Next Header** จะแสดงถึง extension header ลำดับแรก หรือโพรโทคอลใน upper layer protocol เช่น TCP, UDP หรือ ICMPv6 ซึ่งขนาดจะเท่ากับ 8 บิต
- **Hop Limit** จะแสดงถึงค่าที่มากที่สุด ที่ IPv6 packet จะเดินทางไปถึง ซึ่งขนาดของฟิลด์จะเท่ากับ 8 บิต โดย Hop Limit จะคล้ายกับ TTL ใน IPv4 ยกเว้นไม่มีความสัมพันธ์ของเวลาที่แพ็กเก็ตอยู่ในคิวของเร้าเตอร์เมื่อ Hop Limit เท่ากับ 0 ICMPv6 Time Exceeded message จะถูกส่งไปยังเครื่องต้นทาง และแพ็กเก็ตจะถูกยกเลิก
- **Source Address** จะเก็บ IPv6 ของเครื่องต้นทาง ซึ่งขนาดของฟิลด์จะเท่ากับ 128 bit
- **Destination Address** จะเก็บ IPv6 ของเครื่องปลายทาง ซึ่งขนาดของฟิลด์จะเท่ากับ 128 บิต โดยทั่วไป ถ้า routing extension header มีอยู่ แอดเดรสของเครื่องปลายทางจะถูกกำหนดเป็น next router interface ในรายการ route ของเครื่องต้นทาง

2.1.3 IPv6 Extension Header

IPv4 จะทำการรวม options ไว้ทั้งหมด ดังนั้นกระบวนการในการตรวจสอบต่างๆก่อนที่จะทำการ forward แพ็กเก็ตก็จะช้า ดังนั้นใน IPv6 จะทำการตัดส่วนต่างๆที่เป็น options ออก โดยนำส่วนนี้ไปไว้ในส่วนของ extension header ซึ่งจะทำที่เร้าเตอร์แต่ละตัวที่แพ็กเก็ตส่งออกไป โดยเฮดเดอร์นี้จะชื่อว่า Hop-by-Hop options extension header ซึ่งจะช่วยให้กระบวนการ forward แพ็กเก็ตดีขึ้น

RFC 2460 ได้มีการกำหนดว่าทุกโหนด IPv6 จะต้องรองรับเฮดเดอร์ต่างๆดังต่อไปนี้

- Hop-by-Hop Options header
- Destination Options header
- Routing header
- Fragment header
- Authentication header
- Encapsulating Security Payload header

2.1.4 การกำหนดแอดเดรสของ IPv6

- **IPv6 Address Space**

ระบบ IPv6 เป็นระบบที่รองรับเครือข่ายอินเทอร์เน็ตในอนาคตที่มากขึ้นทุกวัน โดยสามารถเปรียบเทียบกับจำนวนเครื่องที่ IPv4 รองรับได้ดังนี้

IPv4 address 4,294,967,296

IPv6 address ที่มี prefix /64 18,446,744,073,709,551,616 ซึ่งสามารถรองรับได้ทั้งหมด 2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456

- **IPv6 Address Syntax**

IPv6 address แบ่งออกเป็น 8 ส่วน ซึ่งแต่ละส่วนจะเป็น เลขฐานสิบหก 4 ตัว (0-F) เช่น 2001:03c8:1204:0000:0000:0000:0000:0001 อาจจะเขียนในอีกรูปแบบหนึ่งได้ดังนี้ 2001:3c8:1204::1 โดยในส่วนที่มีศูนย์อยู่ข้างหน้าสามารถย่อได้เพื่อความสะดวกในการจดจำ

- **IPv6 Prefix**

ส่วนของ Prefix หรือใน IPv4 จะเรียกเป็น subnet mask นั้นสามารถแจกแจงได้ดังตาราง 2.1

ตารางที่ 2.1 แสดงจำนวนหมายเลข IPv6 ตาม Prefix

Prefix	Number of IPv6 Ips	Space
127	2	none
120	256	Xx
64	18,446,744,073,709,551,616	xxxx:xxxx:xxxx:xxxx
48	1,208,925,819,614,629,174,706,176	xxxx:xxxx:xxxx:xxxx:xxxx
32	79,228,162,514,264,337,593,543,950,336	xxxx:xxxx:xxxx:xxxx:xxxx:xxxx

ในกรณีที่มีการกำหนด prefix เป็น /127 จะสามารถมี IPv6 address ได้เพียง 2 หมายเลขเท่านั้น แต่ถ้าในกรณีที่เป็น /48 เราสามารถกำหนดหมายเลข IPv6 ได้มากมายมหาศาล ตัวอย่างเช่น มหาวิทยาลัยศรีนครินทรวิโรฒ ได้หมายเลข IPv6 address มาเป็น 2001:3c8:1408::/48 สามารถแบ่ง subnet เป็น /64 ได้ เช่น

2001:3c8:1408:000a::/64

2001:3c8:1408:000b::/64

2001:3c8:1408:000c::/64 เป็นต้น

2.1.5 ชนิดของ IPv6 Address

ชนิดของ IPv6 Address มี 3 ชนิดคือ

1) Unicast address เป็นการกำหนด single interface ซึ่งในส่วนของ routing topology จะทำการส่ง unicast address ไปยัง single interface เท่านั้น

2) Multicast address ใช้ในการกำหนดหลาย interface ซึ่งในส่วนของ multicast address จะใช้ในกรณีที่เป็น one-to-many โดยจะสามารถส่งไปยัง หลาย interface ได้

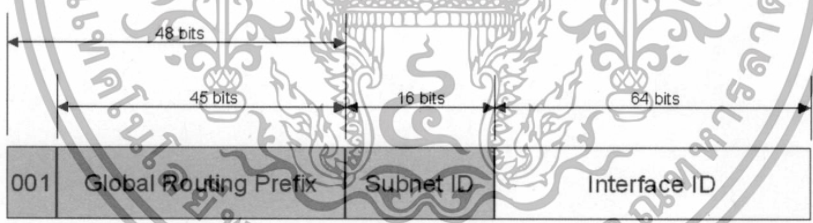
3) Anycast address ใช้ในการกำหนดหลาย interface เหมือนกับ multicast แต่แพ็กเก็ตที่ส่งไปยัง Anycast address จะส่งไปยัง single interface โดยมีการกำหนด nearest interface ซึ่ง nearest interface จะถูกกำหนดในรูปแบบของ routing distance ดังนั้น Anycast address นั้นจะใช้ในกรณีที่เป็น one-to-one-of-many โดยจะส่งไปยัง single interface

โดยทั่วไป IPv6 จะไม่มี extension header ยกเว้นในกรณีที่ต้องการจัดการพิเศษจึงจะมีการเพิ่ม extension headers เข้าไปที่เครื่องที่ส่ง โดยที่แต่ละ extension header จะต้องมี 64 บิต (8 ไบต์)

2.1.5.1 Unicast IPv6 Address

ชนิดของแอดเดรสที่เป็น Unicast IPv6 address มีดังนี้

- **Global Unicast address** จะเปรียบเสมือน Public IPv4 address ดังนั้น ขอบเขตของ Global Unicast address ก็คือ IPv6 address ทั้งหมดที่อยู่บนอินเทอร์เน็ต ซึ่งโครงสร้างของ Global Unicast address ที่ถูกกำหนดโดย IANA ตาม RFC 3587 เป็นดังรูปที่ 2.2



รูปที่ 2.2 The global unicast address as defined in RFC 3587

(ที่มา : Hagen S. 2006. IPv6 Essentials. [Ebook]. USA: O'Reilly Media.)

ในแต่ละฟิลด์จะประกอบด้วยส่วนต่างๆดังนี้

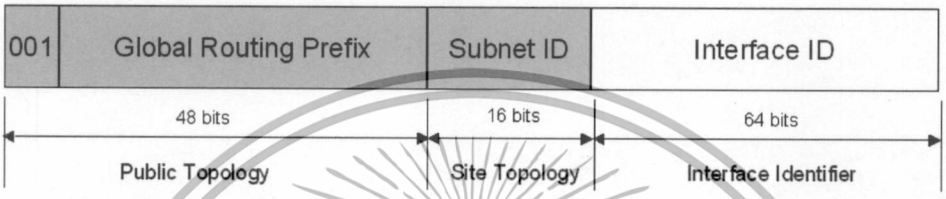
1) fixed portion จะถูกกำหนดเป็น 001 ปัจจุบันได้ถูกกำหนดให้เป็น global address ที่เป็น 2000::/3

2) Global Routing Prefix เป็นการกำหนด global routing prefix ขององค์กร ซึ่งจะใช้จำนวน 48 บิต prefix เกิดจาก 45 บิต รวมกับ 3 บิต ที่เป็น fix portion ในการ forward IPv6 packet มายังเร้าเตอร์ขององค์กร

3) Subnet ID จะถูกใช้ภายในองค์กรเพื่อใช้ในการกำหนด subnet โดยจะใช้ 16 บิต ในการแบ่งซึ่งจะสามารถแบ่งได้ถึง 65536 subnet หรือจะแบ่งเป็น level hierarchy เพื่อให้มีประสิทธิภาพในการ routing

4) Interface ID จะเป็น interface ที่ถูกกำหนด subnet ภายใน site นั้นๆ ซึ่งจะใช้ทั้งหมด 64 บิต

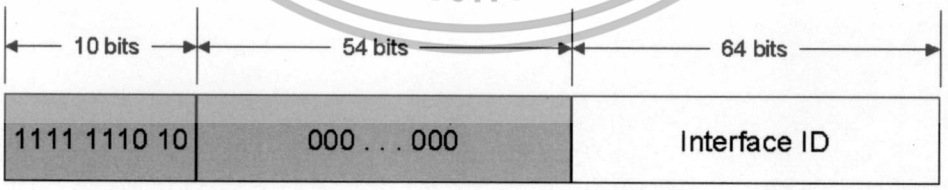
โดยฟิลด์ของ Unicast address สามารถแบ่งออกได้เป็น 3 level ดังรูปที่ 2.3



รูปที่ 2.3 The three-level structure of the global unicast address

(ที่มา : Hagen S. 2006. IPv6 Essentials. [Ebook]. USA: O'Reilly Media.)

- **Link-local address** จะถูกใช้ระหว่าง on-link neighbors ในกระบวนการหาเครื่องข้างเคียง (Neighbor Discovery processes) เช่น ในกรณีของเครื่องที่ทำการเชื่อมต่อกันโดยไม่ผ่านเร้าเตอร์แล้ว link-local address จะถูกใช้ในการติดต่อกัน ซึ่งถ้าเทียบกับ IPv4 จะหมายถึง Automatic Private IP Addressing (APIPA) IPv4 ซึ่งจะถูกกำหนดขึ้นโดย computer เช่น ในกรณีที่ใช้ OS เป็น Microsoft จะมีแอดเดรสเป็น 169.254.0.0/16 โดยโครงสร้างของ Link-local address นั้นจะเป็นดังรูปที่ 2.4

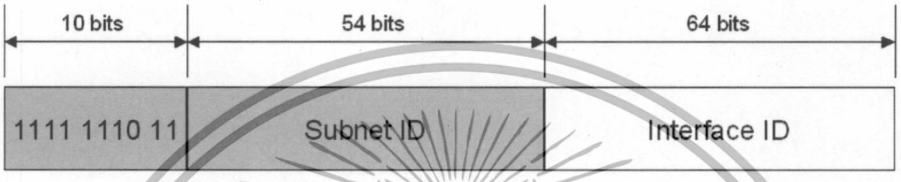


รูปที่ 2.4 The link-local address

(ที่มา : Hagen S. 2006. IPv6 Essentials. [Ebook]. USA: O'Reilly Media.)

ซึ่ง Link-local address จะมีค่าเริ่มต้นเป็น FE80 และจะใช้ 64 บิต ในการกำหนด interface ดังนั้น prefix ของ Link-local address จะเป็น FE80::/64 เสมอ

■ **Site-local address** จะถูกใช้ระหว่างโหนดหนึ่งกับอีกโหนดหนึ่งภายใน site เดียวกัน ซึ่งถ้าทำการเปรียบเทียบกับ IPv4 นั้น Site-local address จะเทียบได้กับ Private IPv4 address (10.0.0.0/8, 172.16.0.0/12 และ 192.168.0.0/16) โดยแอดเดรสนี้จะใช้ภายใน site ซึ่ง Site-local address จะไม่ถูกกำหนดโดยอัตโนมัติ ดังนั้นการกำหนดจะต้องใช้วิธี stateless หรือ stateful address configuration เท่านั้น โดยโครงสร้างของ Site-local address นั้นจะเป็นดังรูปที่ 2.5



รูปที่ 2.5 The site-local address

(ที่มา : Hagen S. 2006. IPv6 Essentials. [Ebook]. USA: O'Reilly Media.)

ซึ่ง 10 บิต แรกจะถูกกำหนดตายตัวสำหรับ Site-local address เป็น FEC0::/10 และหลังจาก fix 10 บิต แล้วจะเหลือ 54 บิต สำหรับ Subnet ID และหลังจากนั้นจะเป็น 64 บิต ในการกำหนด interface ภายใต้ subnet นั้นๆ

■ **Special IPv6 Address มีทั้งหมด 2 แบบ คือ**

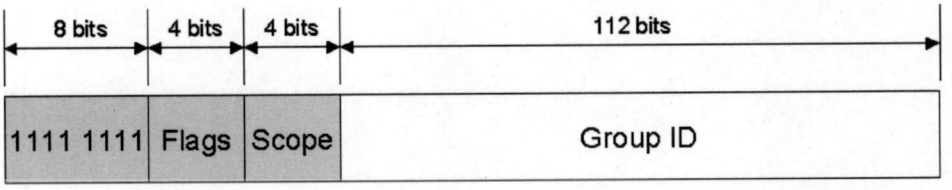
1) **Unspecified Address** (0:0:0:0:0:0:0:0 หรือ ::) เมื่อเทียบกับ IPv4 address จะเป็น 0.0.0.0 โดยทั่วไปจะใช้ในกรณีที่มีการกำหนดเป็นแอดเดรสต้นทางอะไรก็ได้ที่จะพยายามเข้าถึง host หรือจะใช้ในกรณีที่ไม่มีการกำหนดแอดเดรสบน interface หรือใช้กับแอดเดรสปลายทางก็ได้

2) **Loopback Address** (0:0:0:0:0:0:0:1 หรือ ::1) ใช้ในการกำหนด loopback interface หรือเมื่อเทียบกับ IPv4 จะเป็น 127.0.0.1

2.1.5.2 Multicast IPv6 Address

ในส่วนของ Multicast Address นั้นจะมีการทำงานเหมือนกันกับ IPv4 address โดยในเวลาหนึ่งๆ โหนดของ IPv6 สามารถอยู่ในกลุ่มได้หลาย multicast address ซึ่งในแต่ละโหนดสามารถเข้าร่วมหรือออกจากกลุ่มได้ตลอดเวลา

Multicast IPv6 address จะมี 8 บิต แรกถูกกำหนดให้เป็น 1111 1111 ซึ่งถ้าดูแล้ว Multicast IPv6 address จะขึ้นต้นด้วย FFFF โดยโครงสร้างของ Multicast IPv6 address จะเป็นดังรูปที่ 2.6



รูปที่ 2.6 The IPv6 multicast address

(ที่มา : Hagen S. 2006. IPv6 Essentials. [Ebook]. USA: O'Reilly Media.)

ฟิลด์ต่างๆ ใน Multicast IPv6 address มีดังนี้

1) Flags ขนาดของ Flags จะมีความยาว 4 บิต โดยในส่วนของ 3 บิต แรกจะเป็น 0 ส่วนบิตสุดท้ายจะเป็น T flags ซึ่งในกรณีที่ T เป็น 0 จะหมายถึง Mulitcast address ที่ถูกกำหนดอย่างถาวรโดย IANA (Internet Assigned Numbers Authority) ถ้า T เป็น 1 หมายถึง Multicast address นั้นเป็น Multicast address ชั่วคราว
2) Scope ขนาดของ Scope จะมีความยาว 4 บิต โดยเร้าเตอร์จะใช้ Multicast scope ในการตัดสินใจว่าจะให้ Multicast address ถูกส่งไปทางใด ซึ่งค่าต่างๆของฟิลด์ scope นั้นจะเป็นดังนี้
   (1) หมายถึง interface-local scope
   (2) หมายถึง link-local scope
   (5) หมายถึง site-local scope
3) Group ID ขนาดของ Group ID จะมีความยาว 112 บิต ซึ่งการกำหนด Group ID จะไม่ขึ้นอยู่กับ Scope โดยที่ Multicast address จะเริ่มต้นจาก FF01:: ถึง FF0F:: ซึ่งจะถูกจองไว้สำหรับแอดเดรสที่เป็นมาตรฐาน

ในการอ้างถึงทุกๆ โหนดสำหรับ interface-local และ link-local scopes นั้นมีการกำหนดดังนี้

FF01::1 (interface-local scope all-nodes multicast address)

FF02::1 (link-local scope all-nodes multicast address)

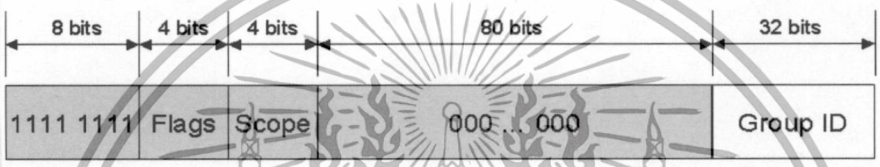
ในการอ้างถึงทุกๆเร้าเตอร์สำหรับ interface-local link-local และ site-local scopes นั้นมีการกำหนดดังนี้

FF01::2 (interface-local scope all-routers multicast address)

FF02::2 (link-local scope all-routers multicast address)

FF05::2 (site-local scope all-routers mulitcast address)

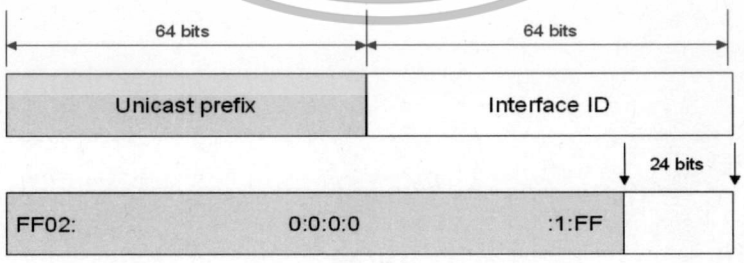
ใน 112 บิต สำหรับ Group ID ที่จะเป็นไปได้จะเท่ากับ 2112 Group ID ซึ่งการแปลง IPv6 Multicast address จะต้องถูกแปลงไปเป็น Ethernet multicast MAC address ซึ่งตาม RFC 3513 แนะนำว่าการกำหนด Group ID นั้นสามารถใช้เพียงแค่ 32 บิต ด้านหลัง มาเป็นตัวกำหนด Group ID ของ IPv6 Multicast address ได้ เนื่องจาก MAC address ก็จะไม่ซ้ำกันอยู่แล้ว



รูปที่ 2.7 The modified IPv6 multicast address using a 32-bit group ID

(ที่มา : Hagen S. 2006. IPv6 Essentials. [Ebook]. USA: O'Reilly Media.)

■ **Solicited node address** จะเป็นการช่วยให้การเข้าถึงในแต่ละโหนดได้ดีขึ้น เนื่องจากใน IPv4 จะใช้ ARP ส่งไปยัง MAC level และจะทำการ broadcast ไปยังโหนดทุกๆโหนด แต่ใน IPv6 จะใช้ Neighbor Solicitation message ในการทำ Address Resolution ทำให้ไม่ต้องส่งไปยังโหนด IPv6 ทุกๆโหนดซึ่งรูปแบบของ Solicited node address จะเป็นดังรูปที่ 2.8



รูปที่ 2.8 The solicited-node multicast address

(ที่มา : Hagen S. 2006. IPv6 Essentials. [Ebook]. USA: O'Reilly Media.)

2.1.5.3 Anycast IPv6 Address

Anycast Address สามารถกำหนดได้หลาย interface ซึ่งแพ็กเก็ตที่ส่งไปยัง Anycast address จะส่งไปตาม routing ของ interface ที่ใกล้ที่สุดที่ anycast address กำหนดไว้ ปัจจุบัน anycast address จะถูกใช้เป็นแอดเดรสปลายทางที่ถูกกำหนดโดยเร้าเตอร์เท่านั้น

สำหรับ Subnet-Router anycast address จะถูกกำหนดมาจาก subnet prefix ของ interface ซึ่งการสร้าง Subnet-Router anycast address นั้น สามารถทำได้โดยกำหนด บิตใน subnet prefix ที่เหมาะสมแล้วบิตที่เหลือจะถูกกำหนดให้เป็น 0 ทุกเร้าเตอร์ที่เกาะอยู่บน subnet นั้นจะถูกกำหนด Subnet-Router anycast address สำหรับ subnet นั้นๆ ซึ่ง Subnet-Router anycast address จะถูกใช้เมื่อมีการติดต่อกับเร้าเตอร์หนึ่งในหลายเร้าเตอร์ที่เกาะอยู่กับ subnet ปลายทาง

2.1.6 IPv6 Interface Identifiers

IPv6 จะใช้ 64 บิตหลังในการกำหนดตัว interface identifiers ซึ่งการกำหนดตัว interface identifiers นั้นสามารถกำหนดได้หลายรูปแบบดังนี้

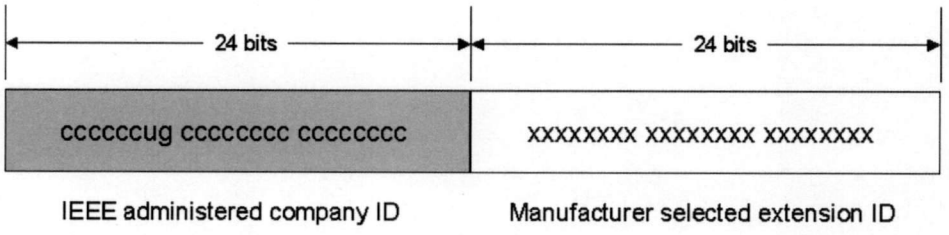
- 64 บิต interface identifiers ได้มาจาก Extended Unique Identifier (EUI)-64 address
- การสุ่มเลข (random) ที่ถูกสร้างขึ้นมาตามช่วงเวลาซึ่งไม่มีรูปแบบเฉพาะ
- การใช้เลข address ที่ถูกกำหนดขึ้นแบบ stateful address autoconfiguration เช่น ใช้ได้รับจาก DHCPv6

- **EUI-64 address-based interface identifiers**

ทุกๆ unicast address จะใช้ prefix ตั้งแต่ 001 ถึง 111 ซึ่ง 64 บิต EUI-address จะได้มาจาก network adapter card หรือ IEEE 802 address

- **IEEE 802 address**

ในรูปแบบเก่าจะใช้ 48 บิต interface identifiers ซึ่งเรียกว่า IEEE 802 address โดยประกอบด้วย 24 บิต company ID หรือ เรียกว่า ID ที่มาจากโรงงาน และ 24 บิต เป็น board ID โดยทั้ง 2 ID นี้จะต้องนำมารวมกัน ซึ่งในแต่ละส่วนก็จะไม่ซ้ำกันอยู่แล้ว ไม่ว่าจะเป็นในเรื่องของ company ID และ board ID ดังนั้น หมายเลข IEEE 802 address จึงไม่ซ้ำกัน และแต่ละ network adapter card เมื่อรวมกันเป็น 48 บิต จะเรียกว่า MAC (Media Access Control) address



รูปที่ 2.9 The 48-bit IEEE 802 address

(ที่มา : Hagen S. 2006. IPv6 Essentials. [Ebook]. USA: O'Reilly Media.)

การกำหนดบิตใน 802 address

Universal/Local (U/L) บิตรองสุดท้ายของไบต์แรกจะเป็นตัวกำหนดว่าเป็น Universal หรือ Local ถ้า U/L บิตถูกกำหนดให้เป็น 0 จะเป็นการกำหนดจากบริษัท แต่ถ้าเป็น 1 จะเป็น local เป็นผู้กำหนด ซึ่งผู้ดูแลระบบสามารถกำหนดบิตนี้ให้เป็นแอดเดรสใหม่ได้โดยสามารถกำหนด เป็น u ได้จากรูปที่ 2.9

Individual/Group (I/G) บิตสุดท้ายของไบต์แรกจะเป็นตัวกำหนดว่าจะเป็น individual address (unicast) หรือ group address (multicast) ถ้ากำหนดเป็น 0 จะเป็น unicast แต่ถ้ากำหนดเป็น 1 จะเป็น multicast address หรือ I/G บิตจะถูกกำหนดเป็น g ก็ได้ดังรูปที่ 2.9

- **IEEE EUI-64 Address**

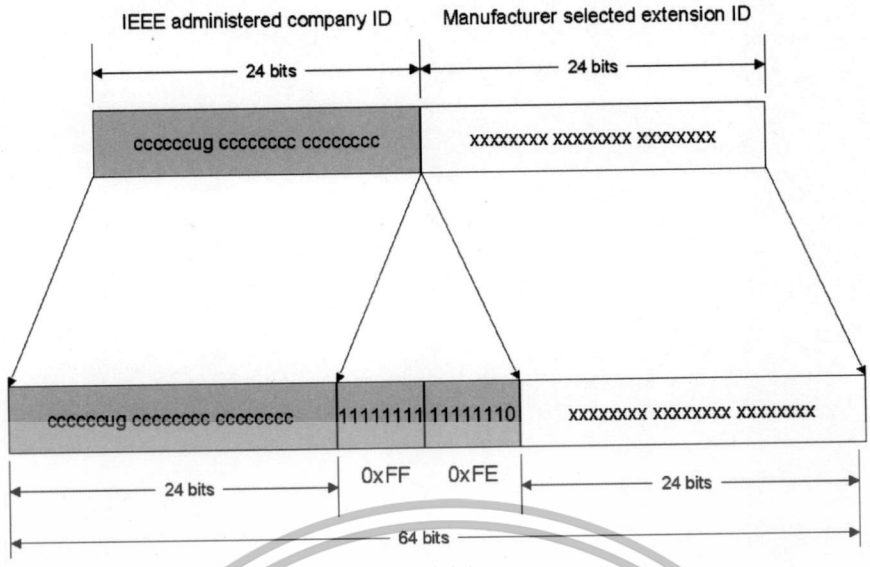
IEEE EUI-64 address เป็นการกำหนดมาตรฐานของแอดเดรสขึ้นมาใหม่ ซึ่งจะมี company ID เป็น 24 บิต และส่วนขยาย (extension) จะเป็น 40 บิต

รูปที่ 2.10 The EUI-64 address

(ที่มา : Hagen S. 2006. IPv6 Essentials. [Ebook]. USA: O'Reilly Media.)

- **Mapping IEEE 802 Address to EUI-64 Address**

การสร้าง EUI-64 address จาก IEEE 802 address จะใช้ 16 บิต คือ 11111111 11111110 (0xFFFE) แทรกเข้าไประหว่าง company ID และ extension ID ดังรูปที่ 2.11



รูปที่ 2.11 The conversion of an IEEE 802 address to an EUI-64 address

(ที่มา : Hagen S. 2006. IPv6 Essentials. [Ebook]. USA: O'Reilly Media.)

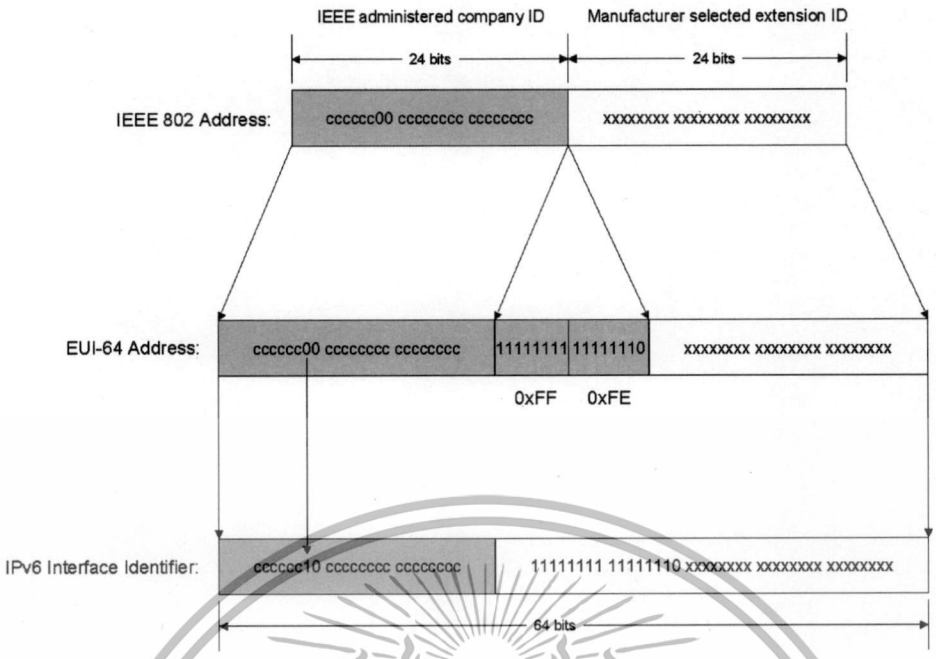
- **Mapping EUI-64 Address to IPv6 Interface Identifiers**

เพื่อให้ได้มาซึ่ง 64 บิต IPv6 unicast address ดังนั้นในส่วนของ U/L บิต ใน EUI-64 address จะถูก complement ซึ่งจะหมายถึงว่าถ้าบิตนั้นเป็น 1 จะถูกกำหนดให้เป็น 0 และถ้าบิตนั้นเป็น 0 จะถูกกำหนดให้เป็น 1 ดังรูปที่ 2.12

รูปที่ 2.12 Unicast EUI-64 address to an IPv6 interface identifiers

(ที่มา : Hagen S. 2006. IPv6 Essentials. [Ebook]. USA: O'Reilly Media.)

นอกจากการ complement แล้วกระบวนการ แปลงจาก IEEE 802 address เป็น IPv6 interface identifier จะต้องทำการแทรก 0xFF 0xFE เข้าไปด้วยดังรูปที่ 2.13



รูปที่ 2.13 Unicast IEEE 802 address to an IPv6 interface identifier

(ที่มา : Hagen S. 2006. IPv6 Essentials. [Ebook]. USA: O'Reilly Media.)

2.1.7 Temporary Address Interface Identifiers

ปัจจุบันการใช้งานอินเทอร์เน็ตเมื่อผู้ใช้งานทั่วไปเชื่อมต่อเข้ากับ ISP (Internet Service Provider) และได้รับ IPv4 ผ่านโพรโทคอล PPP (Point-to-Point Protocol) ซึ่งผู้ใช้จะได้รับ IPv4 ที่เปลี่ยนแปลงไปเรื่อยๆ ดังนั้นการที่ยากที่จะหาข้อมูลของผู้ใช้ว่าผู้ใช้คนนี้มีการใช้งานไอพีใด

สำหรับ IPv6 เมื่อผู้ใช้เชื่อมต่ออินเทอร์เน็ต เร้าเตอร์จะทำการแจก prefix และทำผ่านกระบวนการ stateless address auto configuration ถ้า interface identifier มีการกำหนดตาม EUI-64 address ก็จะช่วยให้สามารถที่จะติดตามและตรวจสอบว่า IPv6 นี้มีเครื่องใดได้รับ IP นี้ไป แต่ก็มีอีกทางเลือกหนึ่งก็คือ การใช้ random interface identifier ซึ่งแอดเดรสนี้จะเปลี่ยนไปเมื่อเวลาเปลี่ยนไป ซึ่งสามารถดูรายละเอียดได้ที่ RFC 3041

ค่าเริ่มต้นของ interface identifier จะถูก random ขึ้น ซึ่งในส่วนของ IPv6 จะไม่มีการเก็บค่าย้อนหลังเพื่อใช้ในการสร้างครั้งต่อไป ดังนั้นการสร้าง random interface identifier จะถูกสร้างขึ้นทุกครั้งที่ IPv6 เริ่มต้นขึ้น ซึ่งในกระบวนการเริ่มต้นสร้าง random interface identifier จะเป็นดังนี้

1) ทำการดึงค่าเก่าจากที่เก็บ (storage) จากนั้นต่อด้วย interface identifier ที่เป็น EUI-64 address

2) Message Digest - 5 (MD5) ทำการเข้ารหัสแบบทางเดียว (one-way hash encryption) เป็นขั้นตอนแรก

3) บันทึก 64 บิตสุดท้ายของกระบวนการ MD5 เพื่อเก็บเป็นค่าเก่าสำหรับกระบวนการสร้าง interface identifier ครั้งต่อไป

4) นำ 64 บิตแรกที่ได้จากกระบวนการ MD5 ในข้อ 2 และกำหนดให้บิตที่ 7 เป็น 0 ซึ่งบิตที่ 7 จะเป็น U/L บิตซึ่งเมื่อกำหนดเป็น 0 แล้วจะหมายถึง local administered interface identifier

ผลลัพธ์ของ IPv6 address ที่ได้จากกระบวนการ random interface identifier จะเรียกว่า Temporary address ซึ่ง Temporary address จะใช้เป็น public address prefix โดยที่แอดเดรสนี้จะมีช่วงเวลาในการใช้งานได้ ซึ่งช่วงเวลานี้จะอยู่ใน Prefix information option ใน Router Advertisement message โดยที่ค่า default ของ lifetime จะเป็น 1 สัปดาห์ แต่ส่วนมากจะมีการกำหนดเป็น 1 วัน หลังจาก lifetime หมดอายุแล้ว temporary address ก็จะถูกสร้างขึ้นมาใหม่

2.1.8 Type of Auto Configuration

การแจก IPv6 Address มีด้วยกัน 3 รูปแบบคือ

1) **Stateful Auto Configuration** จะแจกโดยใช้ DHCPv6 (Dynamic Host Configuration Protocol version 6) โดยเครื่อง DHCP ทำการแจกแอดเดรสที่ไม่ซ้ำกัน ซึ่งวิธีนี้นิยมใช้ใน IPv4

2) **Stateless Auto Configuration** (SLAAC : Stateless Address Auto Configuration) ทำการแจก Prefix เพียงอย่างเดียว

3) **ทำทั้ง 2 แบบ Stateful และ Stateless** การกำหนดค่าจะขึ้นอยู่กับการรับข้อความ (Message) จาก Router Advertisement ซึ่งประกอบด้วย Stateless Address Prefix และ Host นั้นต้องใช้โพรโทคอล Stateful Address configuration

2.1.9 เนเบอร์ดีสคัฟเวอรี (Neighbor Discovery)

กระบวนการของเนเบอร์ดีสคัฟเวอรีจะใช้ ICMP message และ Solicited-Node multicast address ในการกำหนด Link-Layer Address ของเนเบอร์ (Neighbor) ที่อยู่ในเน็ตเวิร์ค (Network) เดียวกัน ตรวจสอบการเชื่อมต่อของเนเบอร์ และติดตามอุปกรณ์ที่อยู่ใกล้เคียง

IPv6 Static cache ในการทำเนเบอร์ดีสคัฟเวอรีนั้นผู้ดูแลระบบจะต้องเข้าไปใส่ข้อมูล IPv6 addresses, Subnet masks, Gateways และ Media Access Control (MAC) addresses ในแต่ละ interface ของแต่ละอุปกรณ์ลงในตารางเส้นทาง (Routing table) เอง ซึ่งวิธีนี้ทำให้สามารถควบคุมเส้นทางได้ดี แต่ผู้ดูแลระบบก็ต้องทำงานมากขึ้น เนื่องจากต้องปรับปรุงตารางเส้นทางให้มีความเป็นปัจจุบันเสมอ

2.1.10 IPv6 Transition

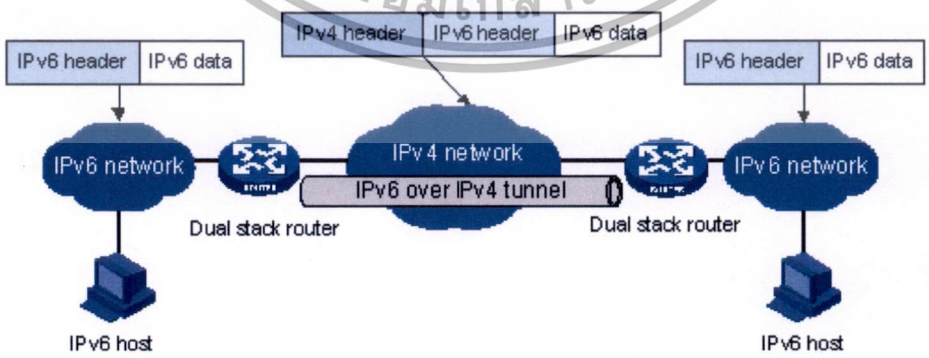
ในการที่จะปรับเปลี่ยนระบบเครือข่ายอินเทอร์เน็ตจาก IPv4 เป็น IPv6 นั้น ไม่สามารถทำได้ทันที เนื่องจากอุปกรณ์ต่างๆภายในองค์กรส่วนใหญ่แล้วไม่รองรับการใช้งาน IPv6 และหากจะเปลี่ยนอุปกรณ์ใหม่ทั้งหมดก็จะต้องใช้งบประมาณที่มาก ดังนั้นการทำ IPv6 Transition จึงเป็นเทคนิคที่จะทำให้สามารถใช้งาน IPv6 ได้บนระบบเครือข่ายที่ยังไม่มีความพร้อมทางด้านอุปกรณ์ทั้งหมด โดยมีเทคนิคหลักๆ ดังนี้

- **Dual Stacks**

เป็นวิธีที่ช่วยให้สามารถส่งข้อมูล IPv4 และ IPv6 ไปในเส้นทางเดียวกันได้ ซึ่งหากปลายทางรองรับการใช้งานทั้งสองแบบ ก็จะทำการเลือกใช้ IPv6 ก่อน แต่หากปลายทางไม่รองรับการใช้งาน IPv6 ก็จะทำการใช้งาน IPv4 แทน วิธีนี้จึงเป็นวิธีที่ทำให้เกิดการใช้งาน IPv6 ได้มากขึ้น และไม่กระทบการกับใช้งานหากปลายทางไม่มี IPv6 ก็ตาม

- **Tunneling**

เป็นหนึ่งวิธีที่ทำในกรณีที่ระบบเครือข่ายไม่รองรับ IPv6 ทั้งหมดซึ่งจะมีเพียงบางส่วนที่รองรับการใช้งาน IPv6 และต้องมีการส่งข้อมูลแพ็กเก็ตของ IPv6 เข้าไปในเครือข่ายที่เป็น IPv4 โดยหลักการแล้วเครื่องต้นทางและเร้าเตอร์ต้นทางจะต้องสามารถรองรับ IPv6 ซึ่งเป็นลักษณะที่เป็น Dual Stack จากนั้นทำการห่อหุ้มข้อมูล (Encapsulation) IPv6 datagrams เข้าไปใน IPv4 packet จากนั้นก็ทำการส่งข้อมูลผ่านเครือข่ายที่เป็น IPv4 เมื่อถึงเร้าเตอร์ปลายทาง IPv6 router ก็จะทำการถอด (Decapsulate) IPv6 datagrams ออกมาแล้วดำเนินการส่งต่อไปยัง IPv6 ปลายทาง

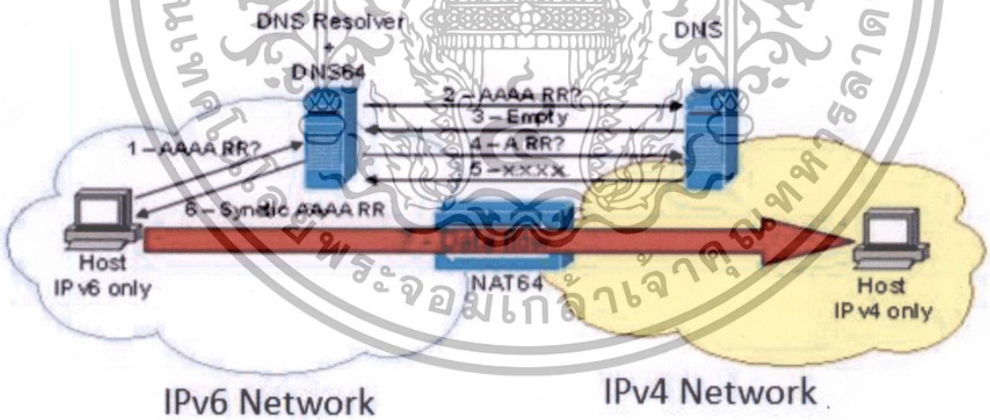


รูปที่ 2.14 ipv6 packet in ipv4 tunneling

(ที่มา : H3C Technologies. 2015. Tunneling Introduction. [Online] Available: http://www.h3c.com/portal/Products___Solutions/Technology/IPv4___IPv6_Services/Technology_Introduction/200702/201180_57_0.htm.)

- **Translation**

การเปลี่ยนเฮดเดอร์และชนิดของแอดเดรสแบบ Translation นั้นจะทำการแปลง IPv4 packet ไปเป็น IPv6 packet หรือจะทำการแปลง IPv6 packet ไปเป็น IPv4 packet ก็ได้โดยหลักการในการแปลงนั้นจะใช้เทคนิคที่เรียกว่า NAT64 โดยเทคนิคนี้จะทำการ mapไอพีแอดเดรสได้ทั้งแบบ Stateless และแบบ Stateful โดยกรณีที่เป็น Stateless จะต้องกำหนดการ map เป็นแบบ manual ส่วนกรณีที่เป็น Stateful นั้นจะทำการ map แบบอัตโนมัติ โดยสามารถดูรายละเอียดได้ดังรูปที่ xxx . เครื่องต้นทางจะมี IPv6 Address เท่านั้น เมื่อต้องการติดต่อกับเครื่องปลายทางก็จะทำการถาม DNS64 ว่าเครื่องปลายทางมี IPv6 Address อะไร ซึ่งเมื่อ DNS64 ถามไปพบว่าเครื่องปลายทางไม่มี AAAA Resource Records (RRs) ก็จะถามต่อว่ามี A RRs เป็นอะไร ซึ่งก็จะได้ IPv4 Address จากนั้น DNS64 ก็จะทำการแปลง A RRs ไปเป็น AAAA RRs ซึ่งเมื่อส่งค่า IPv6 Address ไปที่ NAT64 ก็จะทำให้รู้ว่าเครื่อง IPv6 Address นั้นต้องการติดต่อกับ IPv4 Address จากนั้น NAT64 ก็จะทำการ map IPv6 address กับ IPv4 Address และส่งไปยัง IPv4 Address ปลายทางได้



รูปที่ 2.15 NAT64/DNS64

(ที่มา : Maglione R., Moriondo C. 2015. IPv6 Transition Mechanisms. [Online] Available: http://www.ngnet.it/e/trans1/)

2.2 ความรู้เบื้องต้นเกี่ยวกับ IPTables

IPTables firewall เป็นส่วนสำคัญในการที่จะอนุญาติให้ข้อมูลต่างๆผ่านเข้าออกสู่ระบบเครือข่าย ถูกพัฒนามาจาก Netfilter Project ซึ่งเป็นส่วนหนึ่งของเคอร์เนล (Kernel) 2.4 เป็นต้นไป โดย IPTables นั้นเป็นไฟร์วอลล์ที่สามารถทำงานในลักษณะเหมือนกับอุปกรณ์ไฟร์วอลล์ทั่วไปเช่น การ Track protocol หรือการทำ Rate limit และส่วนที่สำคัญก็คือการกรองข้อมูล (Filtering) โดยในปัจจุบันลินุกซ์ (Linux) หลายๆค่ายก็ได้มี IPTables รวมมาอยู่ด้วยแล้วเมื่อมีการติดตั้งระบบปฏิบัติการ

กล่าวคือ IPTables เป็นเครื่องมือที่จะส่งค่าจาก Command line และทำการติดต่อกับ Firewall policy ไปที่เคอร์เนลซึ่งคำสั่งต่างๆ เช่น Tables, Chain, Match และ Target โดย IPTables นั้นจะทำงานตาม policy rule ที่มีการตั้งค่าว่าจะยอมให้แพ็กเก็ต (Packet) นั้นผ่านไปได้หรือไม่โดยทำการบอกไปที่เคอร์เนล และทำการ block หรือ allow เป็นต้น

Tables : จะแบ่งออกเป็นหมวดหมู่ โดยจะประกอบด้วย 4 หมวดหมู่ด้วยกัน คือ Filter , NAT, mangle และ raw ซึ่งแต่ละ rule จะถูกทำงานในแต่ละ Tables เช่น filter rules ก็จะทำงานที่ Filter tables NAT rules ก็จะทำงานที่ NAT Tables หรือ rule พิเศษอื่นๆจะทำงานที่ mangle tables และการทำ Connection tracking ก็จะทำงานที่ raw tables

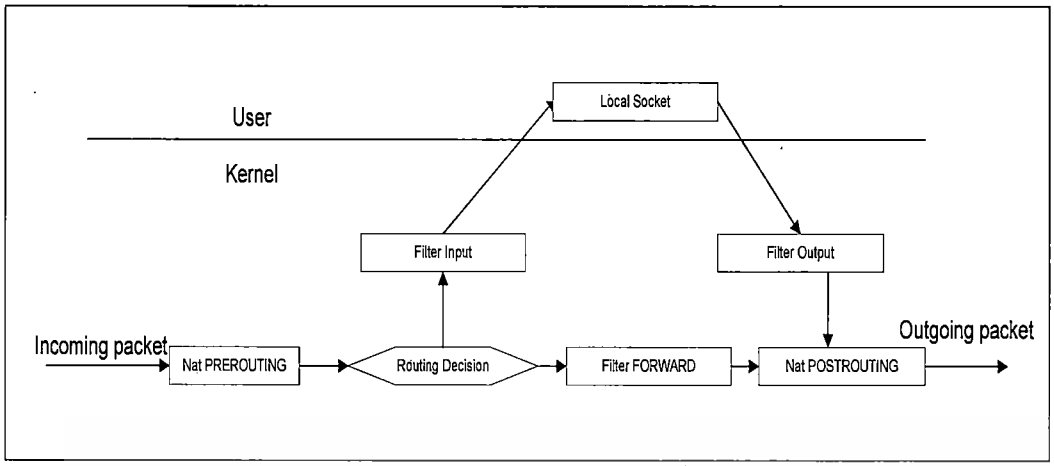
Chains : จะแบ่งออกเป็น Chains ที่เป็นผู้ใช้กำหนดเอง หรือ Chain ที่เป็นค่าเริ่มต้น (Default) ที่ถูกสร้างขึ้นมาแล้ว เช่น INPUT , FORWARD, OUTPUT chains เป็นต้น

INPUT Chain เป็น Chain ที่ทำการส่งข้อมูลมาที่ตัว Local

OUTPUT Chain เป็น Chain ที่ทำการส่งข้อมูลออกจากตัวลินุกซ์เครื่องนั้น

FORWARD Chain เป็น Chain ที่ข้อมูลถูกส่งผ่านตัวลินุกซ์ออกไป ซึ่งจะถูกส่งจากการ์ดหนึ่งไปยังอีกการ์ดหนึ่งโดยผ่านตัวมันออกไป

IPTables มี Default chain ที่สำคัญอีก 2 Chains คือ PREROUTING และ POSTROUTING ใน NAT Table ซึ่งใช้ในการเปลี่ยนแปลงข้อมูลเฮดเดอร์ (Header) ก่อนและหลังการทำการหาเส้นทาง (Routing) ตัวอย่างรูปที่ 2.16 แสดงถึงข้อมูลที่จะไหลผ่าน NAT และ Filter tables ภายในเคอร์เนล



รูปที่ 2.16 การไหลของข้อมูลใน IPTables

(ที่มา : Carter G. 2003. LDAP System Administration. [Ebook]. USA: O'Reilly Media.)

Matchs : ในทุกๆ rules จะต้องมีการ match target เพื่อที่จะบอกได้ว่าแพ็กเก็ตที่เข้าหรือออกนั้น จะ matchs กับอะไร และจะต้องไปทำอะไรต่อ ซึ่งโดยทั่วไปแล้ว จะกล่าวถึง match ที่ใช้บ่อยดังนี้

--source (-s)	match กับไอพีแอดเดรสต้นทาง หรือ network ต้นทาง
--destination (-d)	match กับไอพีแอดเดรสปลายทาง หรือ network ปลายทาง
--protocol (-p)	match กับ โพรโทคอล เช่น TCP , UDP หรือ ICMP เป็นต้น
--in-interface (-i)	match กับ input interface เช่น eth0
--out-interface (-o)	match กับ output interface
--state	match กับ connection states
--string	match กับ ลำดับของ application layer data bytes

Targets : เมื่อมีการ match แล้วก็จะต้องทำการ trigger action ว่าจะต้องทำอะไรต่อกับแพ็กเก็ตนั้นๆ โดยทั่วไปจะมีอยู่ด้วยกัน ดังนี้

Accept	อนุญาตให้แพ็กเก็ตนั้นผ่านได้
Drop	ไม่อนุญาตให้แพ็กเก็ตนั้นผ่าน เหมือนกับว่าแพ็กเก็ตนั้นไม่เคยส่งออก
Log	จัดส่งแพ็กเก็ตไปยัง Syslog
Reject	ไม่อนุญาตให้ผ่าน และ ทำการส่งแพ็กเก็ตตอบกลับไปยังต้นทางที่ส่งมา เช่น ICMP unreachable messages เป็นต้น

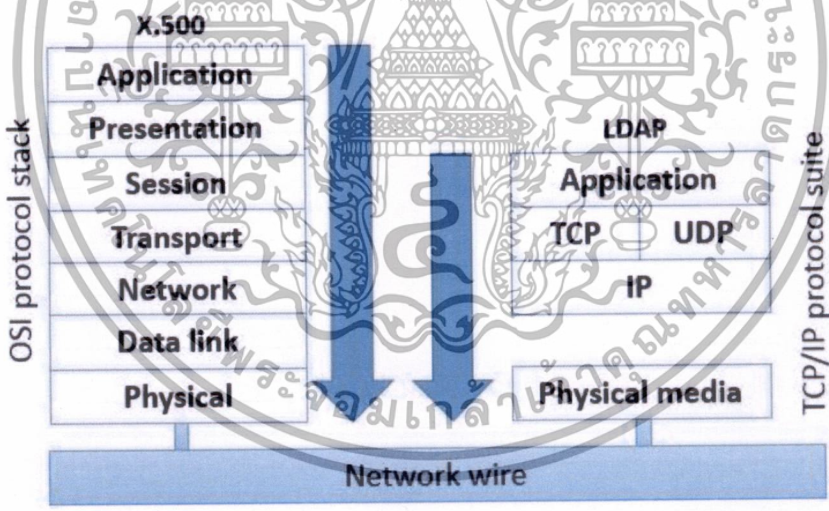
NAT (Network Address Translation) : การทำ NAT นี้จะทำใน 2 ลักษณะคือ inbound connection ซึ่งจะทำให้ external client สามารถเข้ามาใช้บริการ web และ DNS ได้ และ outbound connection หมายถึง ทำให้ internal network สามารถเชื่อมต่อไปยังภายนอกได้ ซึ่งการเชื่อมต่อจาก

ภายในจะเรียกว่า source NAT (SNAT) และ การเชื่อมต่อจากภายนอกจะเรียกว่า destination NAT (DNAT)

โดยทั่วไป NAT rules จะมีอยู่ด้วยกัน 2 Chains คือ PREROUTING และ POSTROUTING โดย PREROUTING นั้นจะถูก apply ก่อน routing algorithm ในเคอร์เนลซึ่งแพ็กเก็ตที่ถูกทำโดย NAT จะไม่ถูกทำโดย INPUT หรือ FORWARD Chain ส่วน POSTROUTING Chain นั้นจะทำหลังจากผ่านกระบวนการหาเส้นทาง มาแล้วในเคอร์เนลซึ่งแพ็กเก็ตที่ผ่านมาแล้วจะต้องผ่าน OUTPUT หรือ FORWARD Chain มาก่อน

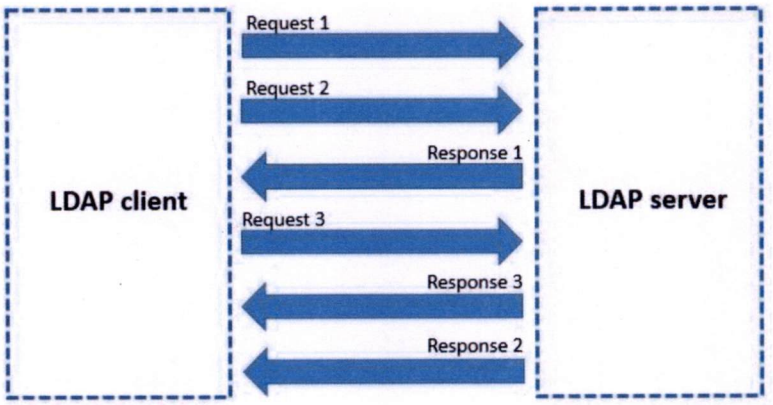
2.3 LDAP

LDAP (Lightweight Directory Access Protocol) โพรโทรคอล LDAP เริ่มมาจาก X.500 directory service โดย LDAP นั้นถูกออกแบบให้มีขนาดเล็กเพื่อที่จะได้ลดขนาดการเชื่อมต่อ (Overhead) ในการเรียกใช้งาน ซึ่ง LDAP จะทำการเชื่อมต่อไปยัง TCP Port 389



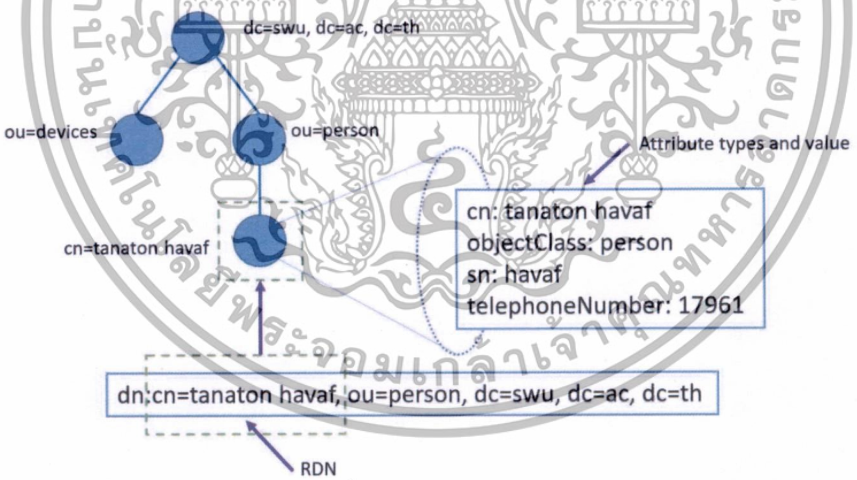
รูปที่ 2.17 เปรียบเทียบ LDAP กับ X.500 บน OSI

LDAP เป็นการเก็บข้อมูลรูปแบบหนึ่ง ซึ่งรายละเอียดในการเก็บจะเก็บในลักษณะที่เป็น object และเก็บในลักษณะของ Tree โดยจะต้องมีการเชื่อมต่อกันระหว่าง LDAP client กับ LDAP server แบบ asynchronous ทำให้ LDAP client สามารถร้องขอ (Request) ได้ทีละหลายๆการร้องขอมายัง LDAP server จากรูปข้างล่างนี้ LDAP client ส่งการร้องขอ 1 และการร้องขอ 2 ก่อนที่จะได้รับการตอบกลับ และการตอบกลับของการร้องขอ 3 จะมาก่อนการตอบกลับของการร้องขอ 2



รูปที่ 2.18 การร้องขอและตอบกลับของ LDAP

รูปแบบของการร้องขอนั้นจะเป็นการตรวจสอบสิทธิในการเข้าใช้งาน โดยจะทำการส่งข้อมูลที่เป็นรหัสผู้ใช้และรหัสผ่านเข้ามาเพื่อทำการตรวจสอบข้อมูล ซึ่งในข้อมูลของ LDAP ในแต่ละ object จะมี Attributes ต่างที่สามารถใช้ในการตรวจสอบ เช่น uid ก็จะเป็น username และ userPassword ก็จะเป็นรหัสผ่าน โดยรูปแบบของ Tree ใน LDAP จะเป็นดังรูป



รูปที่ 2.19 ตัวอย่างโครงสร้างของ LDAP

โดยรูปแบบของ Tree จะมี DIT (Directory Information Tree) จะมีการแบ่งเป็น base dn ซึ่งในตัวอย่างจะเป็น dc=swu ,dc=ac, dc=th จากนั้นจะมีการแบ่งย่อยออกเป็น OU (Organization Unit) โดยจะเป็นการแบ่งประเภทเช่น ประเภทคน หรืออุปกรณ์ ซึ่งในบางกรณีการแบ่ง OU อาจจะแบ่งตามแผนกหรือส่วนงานก็ได้ จากนั้นก็จะถึงส่วนของ cn (Common Name) จะเป็นการบอกถึงชื่อ โดยในชื่อแต่ละชื่อเปรียบเสมือน 1 record ในฐานข้อมูลโดยในแต่ละ record นั้นจะมี attributed

โดยแต่ละ attributed นั้นก็จะมีค่าเช่น sn (surname) หรือหมายเลขโทรศัพท์ telephoneNumber และรหัสผ่าน (userPassword) เป็นต้น

2.4 Captive Portal

Captive Portal เป็นเว็บเพจที่ให้ผู้ใช้งานเข้าถึงจากภายนอก หรือภายในองค์กรก่อนที่ได้รับสิทธิในการเข้าใช้งานทรัพยากรขององค์กรนั้นๆ เช่น การใช้งานเครือข่ายอินเทอร์เน็ต โดยปกติแล้วการใช้งาน Captive Portal นั้นจะมีการประกาศในเรื่องของนโยบายการเข้าใช้งานเครือข่าย (Accept Use Policy) เพื่อให้ผู้ใช้ได้ตระหนักถึงการใช้งาน ว่าระบบจะมีการจัดเก็บข้อมูลของผู้ใช้งานนั้นๆ ซึ่งผู้ใช้งานจะต้องยอมรับเงื่อนไขในการใช้งาน จึงจะสามารถใช้งานได้

โดยปกติหน้า Captive Portal จะเป็นหน้าเว็บเพจที่ให้ผู้ใช้ใส่รหัสผู้ใช้ และรหัสผ่าน เพื่อพิสูจน์สิทธิในการเข้าใช้งาน ซึ่งหลักการทำงานของ Captive Portal นั้นจะต้องทำการดักจับแพ็กเก็ต (intercept packet) ที่ผ่านเข้ามาโดยปกติแล้วการทำ Captive สามารถทำได้ที่ firewall ให้ทำการ redirect แพ็กเก็ตไปยัง port 80 หรือ 443 เพื่อแสดงหน้าเว็บเพจที่ใช้ในการยืนยันตัวตน หรือในกรณีที่ไม่ได้มีการใช้ firewall ในการ redirect แพ็กเก็ตก็สามารถใช้คุณสมบัติของ switch L3-L4 ก็สามารถทำการ redirect ได้เช่นกัน

2.5 Log File

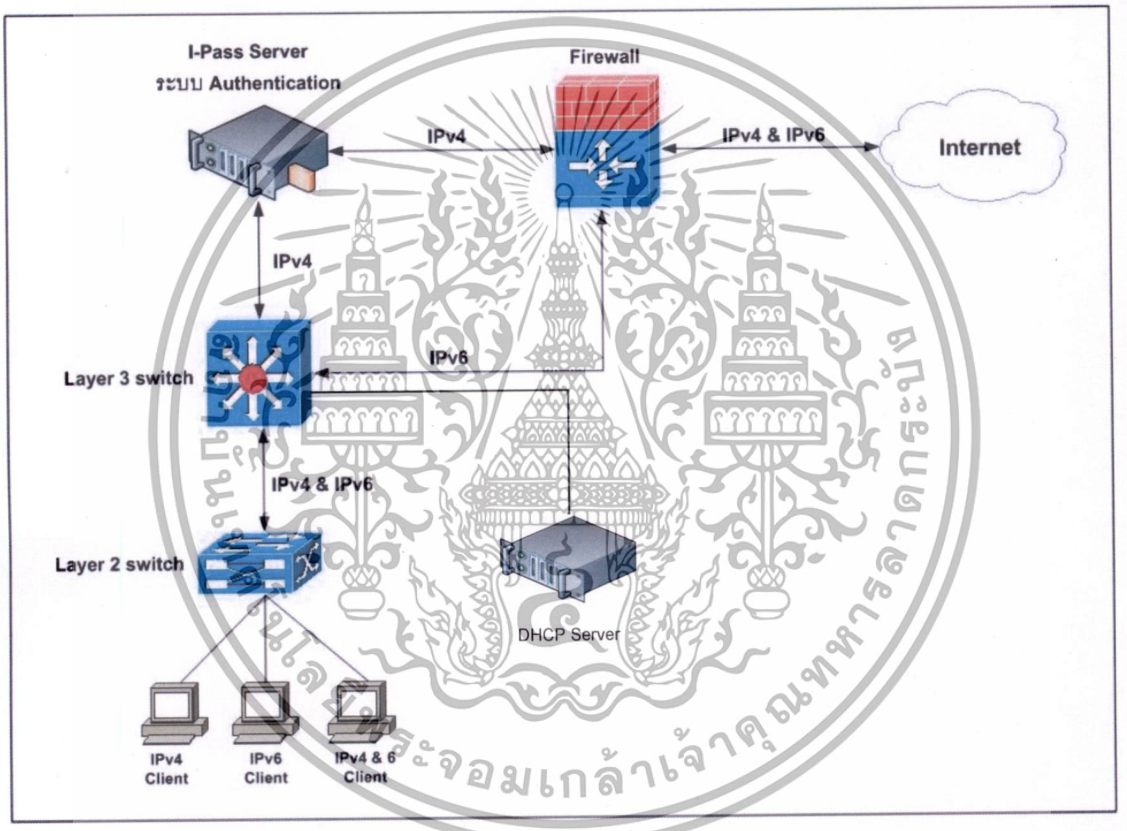
Log File คือไฟล์ที่ประกอบไปด้วยรายการเหตุการณ์ต่างๆที่เกิดขึ้น ถูกบันทึกโดยคอมพิวเตอร์รูปแบบของไฟล์ส่วนใหญ่จะถูกบันทึกอยู่ในรูปแบบ text ซึ่งช่วยลดขนาดของไฟล์ได้ และสามารถเรียกดูได้ในโปรแกรม text editor ทั่วไป ข้อมูลที่ได้จาก Log File สามารถนำมาใช้ได้หลายวัตถุประสงค์ โดยทั่วไปแล้วการเก็บ Log File จะทำการเก็บตาม Application หรือเก็บตามการเข้าใช้งานของระบบปฏิบัติการ (Operating System) ซึ่ง Log File จะเป็นไฟล์ข้อมูลที่ใช้ในการตรวจสอบเหตุการณ์ต่างของ Application หรือระบบใดระบบหนึ่งที่ต้องการจะจัดเก็บ ในกรณีอย่างเช่นระบบรักษาความปลอดภัย เช่น Firewall นั้นก็จะต้องมีการเก็บข้อมูลการจราจร (Traffic Log) หรือข้อมูลการใช้งานว่ามีไอพีแอดเดรสใดภายในระบบเครือข่ายติดต่อไปยังไอพีแอดเดรสใดในเครือข่ายภายนอก หรือไอพีแอดเดรสภายนอกใดที่มาติดต่อกับไอพีแอดเดรสใดในเครือข่ายหรือติดต่อผ่าน Application ใด ยิ่งไปกว่านั้นระบบการจัดเก็บ Log File ที่ดีนั้นยังต้องสามารถหาผู้ที่ใช้งานใน Application นั้นๆหรือระบบนั้นได้ เพื่อใช้ในการตรวจสอบปัญหา

โดยการใช้งาน Log File จะมีประโยชน์นั้นเครื่องคอมพิวเตอร์แม่ข่าย (Server) ทุกเครื่องจะต้องมีการตั้งเวลาให้ตรงกัน โดยมากจะนิยมใช้งานผ่านโปรโตคลอ NTP (Network Time Protocol) เพื่อให้การบันทึกเหตุการณ์ต่างๆที่เกิดขึ้นตรงกันและสามารถตรวจสอบได้ ถ้าการใช้งานไม่ได้มีการติดตั้ง NTP แล้วอาจจะทำให้การบันทึก Log File เกิดความคลาดเคลื่อน ยิ่งในองค์กรที่มีขนาดใหญ่มีการบันทึกเหตุการณ์ต่างๆเป็นจำนวนมาก เวลาเพียงเสี้ยววินาที ก็จะมีความหมายมากซึ่งถ้าผิดไปก็จะทำให้ข้อมูลนั้นไม่ถูกต้อง

บทที่ 3
การทำงานของระบบปัจจุบัน

ศึกษาระบบโครงสร้างการทำงานของระบบการยืนยันตัวตนในปัจจุบัน โดยจะศึกษาถึงรูปแบบการเชื่อมต่อ และการทำงานของระบบ โดยจะใช้ข้อจำกัดของระบบปัจจุบันมาเป็นข้อมูลในการพัฒนาระบบ

3.1 ภาพรวมและการทำงานของระบบปัจจุบัน



รูปที่ 3.1 แผนผังแสดงการเชื่อมต่อ IPv4 และ IPv6

จากรูปที่ 3.1 การทำงานของระบบยืนยันตัวตนของมหาวิทยาลัยนั้นมีการเปิดให้มีการใช้งาน IPv6 ขึ้น โดยดำเนินการแบบ Dual Stack ซึ่งเครื่องคอมพิวเตอร์ลูกข่ายจะได้รับทั้ง IPv4 และ IPv6 โดยอัตโนมัติ ซึ่งในระบบ IPv4 จะได้รับการแจกอัตโนมัติผ่านระบบ DHCP ของมหาวิทยาลัย ส่วน IPv6 จะทำการแจกจาก Layer3 switch แบบ SLAAC (Stateless Auto configuration) โดยทุกๆ เครื่องเมื่อมีการใช้งานเครือข่ายอินเทอร์เน็ต ระบบจะทำการตรวจสอบว่าปลายทางที่ต้องการติดต่อ

สามารถติดต่อผ่าน IPv6 ได้หรือไม่ถ้าสามารถติดต่อได้ ก็จะเลือกที่จะไปสู่ปลายทางด้วย IPv6 หากกรณีที่เครื่องปลายทางไม่มีหมายเลข IPv6 ก็จะทำการติดต่อผ่านหมายเลข IPv4

กลไกการทำงานจะใช้รูปแบบการค้นหาเส้นทางบน Layer 3 Switch ซึ่งที่ Layer 3 Switch นั้นจะมีตารางค้นหาเส้นทาง (Routing Tables) อยู่ 2 ตารางคือ ตารางค้นหาเส้นทางที่เป็น IPv4 และตารางค้นหาเส้นทางที่เป็น IPv6 ถ้าปลายทางมีหมายเลข IPv6 ก็จะทำการส่งไปยัง Firewall ของมหาวิทยาลัยเพื่อทำการยืนยันตัวตน ส่วนกรณีที่เครื่องปลายทางไม่มี IPv6 ก็จะส่งไปที่ระบบ I-Pass โดยระบบ I-Pass นั้นจะทำการยืนยันตัวตนเฉพาะเครื่องที่เป็น IPv4 เท่านั้น ซึ่งรูปแบบการยืนยันตัวตนของทั้ง IPv4 และ IPv6 นั้นจะเป็นการยืนยันตัวตนแบบ Captive Portal เป็นการ redirect ไปยังหน้า web site แล้วให้ผู้ใช้ดำเนินการใส่รหัสผู้ใช้และรหัสผ่านของมหาวิทยาลัย เพื่อออกสู่เครือข่ายอินเทอร์เน็ต

3.2 ปัญหาและข้อจำกัดที่พบในระบบปัจจุบัน

ในปัจจุบันระบบที่ทำการยืนยันตัวตนของมหาวิทยาลัยที่เป็น I-Pass นั้นเป็น Opensource ดำเนินการติดตั้งบนระบบปฏิบัติการ Linux และใช้การควบคุมการเข้าออกเพื่อใช้งานผ่านโปรแกรม IPTables ส่วนการยืนยันตัวตนของ IPv6 นั้นเป็นการทำผ่านอุปกรณ์ Firewall ที่เป็นอุปกรณ์ทางการค้า (Commercial Product) ซึ่งระบบทั้ง 2 นั้นเป็นคนละระบบโดยจะมีหน้าจอที่ติดต่อกับผู้ใช้ไม่เหมือนกัน ซึ่งหน้าจอที่เป็นอุปกรณ์ทาง การค้า ไม่สามารถที่จะปรับแต่งได้ตามที่ต้องการ เหมือนกับระบบที่เป็น Opensource ที่มหาวิทยาลัยทำการพัฒนาขึ้น ดังนั้นปัญหาที่เกิดขึ้นกับผู้ใช้ คือ ผู้ใช้จะต้องทำการยืนยันตัวตน 2 ครั้ง จึงทำให้เกิดความสับสน เพราะในปัจจุบันเครื่องปลายทางไม่ว่าจะเป็น Google, Facebook หรือ web site ชั้นนำในต่างประเทศก็มีหมายเลข IPv6 เป็นที่เรียบร้อยแล้ว ดังนั้นเมื่อเครื่องลูกข่ายเข้าเว็บไซต์เหล่านั้น ก็จะขึ้นหน้าจอให้ยืนยันตัวตน ซึ่งถ้าในกรณีที่ผู้ใช้เข้าเว็บไซต์ในประเทศไทยส่วนมากยังไม่มีหมายเลข IPv6 ก็จะต้องผ่านหน้าจอยืนยันตัวตนอีกครั้งผ่านระบบ I-Pass ทำให้ผู้ใช้งานต้องทำการยืนยันตัวตนถึง 2 ครั้ง และหน้าจอการยืนยันตัวตนยังแตกต่างกันอีกด้วย ซึ่งผู้ใช้ไม่ต้องการให้เกิดเหตุการณ์ดังกล่าว เพราะผู้ใช้ไม่ได้ให้ความสนใจว่าเครื่องผู้ใช้จะออกอินเทอร์เน็ตเป็น IPv4 หรือ IPv6 เพียงแต่ขอให้สามารถใช้งานเครือข่ายอินเทอร์เน็ตได้ก็พอ

ประเด็นต่อไปก็คือ การใช้งานหมายเลข IPv6 นั้นทุกๆครั้งที่เครื่องผู้ใช้ได้รับหมายเลข IPv6 ไปแล้ว เครื่องผู้ใช้จะได้หมายเลข IPv6 ชั่วคราว (Temporary IPv6 Address) ด้วย ซึ่งประเด็นของหมายเลข IPv6 ชั่วคราวนั้นจะมีการเปลี่ยนแปลง ซึ่งในกรณีที่หมายเลข IPv6 ชั่วคราวมีการ

เปลี่ยนแปลงไป ผู้ใช้ที่เคยทำการยืนยันตัวตนไปแล้วก็จะต้องทำการยืนยันตัวตนใหม่อีกครั้ง ซึ่งทำให้ผู้ใช้เกิดความสับสนมาก ว่าทำไมระบบถึงต้องให้ผู้ใช้ทำการ login ซ้ำหลายรอบ นอกจากประเด็นการ Login แล้วในการจัดเก็บข้อมูลที่เป็น Log การใช้งานเครือข่ายอินเทอร์เน็ตนั้นก็จะต้องดำเนินการเก็บแยกออกจากกัน เนื่องจากว่าระบบที่ใช้ในการยืนยันตัวตนของระบบ I-Pass กับระบบ Firewall ที่เป็นอุปกรณ์ทางการค้านั้นเป็นคนละระบบกัน ทำให้การค้นหาข้อมูลการใช้งานจะต้องไปค้นหาคนละระบบ นอกจากนั้นในระบบปัจจุบันเมื่อทำการ Login เป็นที่เรียบร้อยแล้วจะขึ้นหน้าจอที่แสดงเวลานับถอยหลังเป็นแบบ Popup ซึ่งปัญหาของระบบ Popup นั้นส่วนมากเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่างๆจะทำการ Block Popup ซึ่งทำให้ไม่สามารถใช้ระบบได้ ดังนั้นเครื่องทุกเครื่องภายในมหาวิทยาลัยต้องทำการปลด Block Popup ของบราวเซอร์ที่เว็บไซต์นี้ และปัญหาที่ตามมาก็คือ อุปกรณ์บางชนิด เช่น Windows phone ไม่สามารถแสดง Popup ได้ดังนั้นเมื่อใช้อุปกรณ์ชนิดนี้ก็จะไม่สามารถใช้งานระบบของมหาวิทยาลัยได้

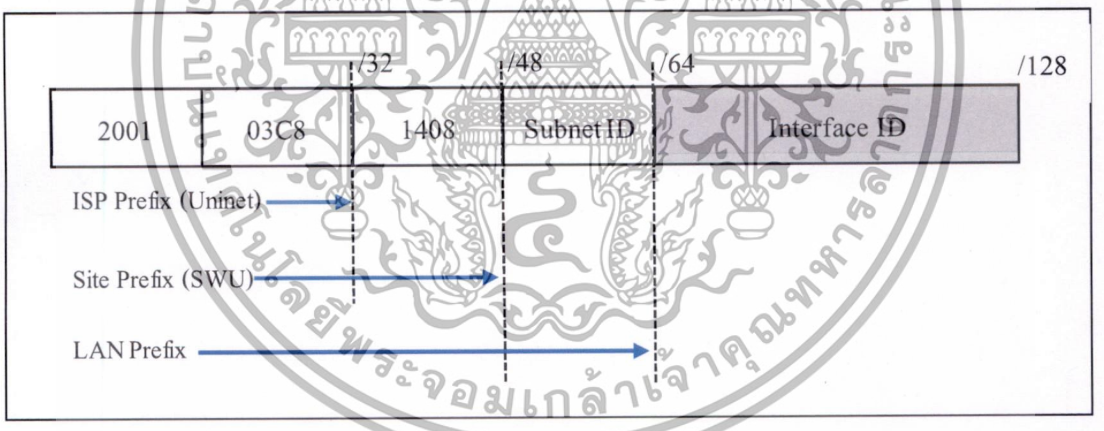
บทที่ 4

การวิเคราะห์และออกแบบระบบงาน

4.1 ออกแบบการจัดแบ่ง IPv6 (IPv6 address Plan)

การจัดสรรหมายเลข IPv6 ให้กับเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่าย เครื่องแต่ละเครื่องจะต้องได้รับหมายเลข IPv6 ที่ไม่ซ้ำกัน โดยหมายเลขทั้งหมดนั้นมีหน่วยงานกลางที่รับผิดชอบในการจัดการคือ IANA (Internet Assigned Number Authority) องค์กรนี้จะมีหน้าที่ในการออกไอพีแอดเดรสซึ่งการแบ่งไอพีแอดเดรสจะถูกแบ่งไปที่ RIR (Regional Registry) และในประเทศไทยได้รับการดูแลไอพีแอดเดรสจาก APNIC (Asia-Pacific Network Information Centre)

มหาวิทยาลัยศรีนครินทรวิโรฒได้มีการเชื่อมต่อเครือข่ายอินเทอร์เน็ตกับ Uninet ซึ่งไอพีแอดเดรสของ Uninet ที่ได้รับจัดสรรจาก APNIC ในฐานะที่เป็นผู้ให้บริการอินเทอร์เน็ต (ISP) โดยมี ISP Prefix เป็น 2001:3c8::/32 และทาง Uninet ได้จัดสรรให้กับทางมหาวิทยาลัยโดยมี Site Prefix เป็น 2001:3c8:1408::/48 ดังรูปที่ 3.1



รูปที่ 4.1 การแบ่ง Global IPv6 Address

แนวทางในการจัดสรรหมายเลข IPv6 Address ของมหาวิทยาลัย จะใช้การอ้างอิงกับ Private IPv4 Address ที่ใช้อยู่ภายในมหาวิทยาลัย เพื่ออำนวยความสะดวกให้กับผู้ดูแลระบบ สามารถจดจำหมายเลข IPv6 Address ที่เป็น Subnet ได้ง่ายขึ้น โดยมีการแบ่งตามวิทยาเขต ดังนี้

1) ประสานมิตร เป็น 2001:3c8:1408:1::/52
2) องครักษ์ เป็น 2001:3c8:1408:2::/52

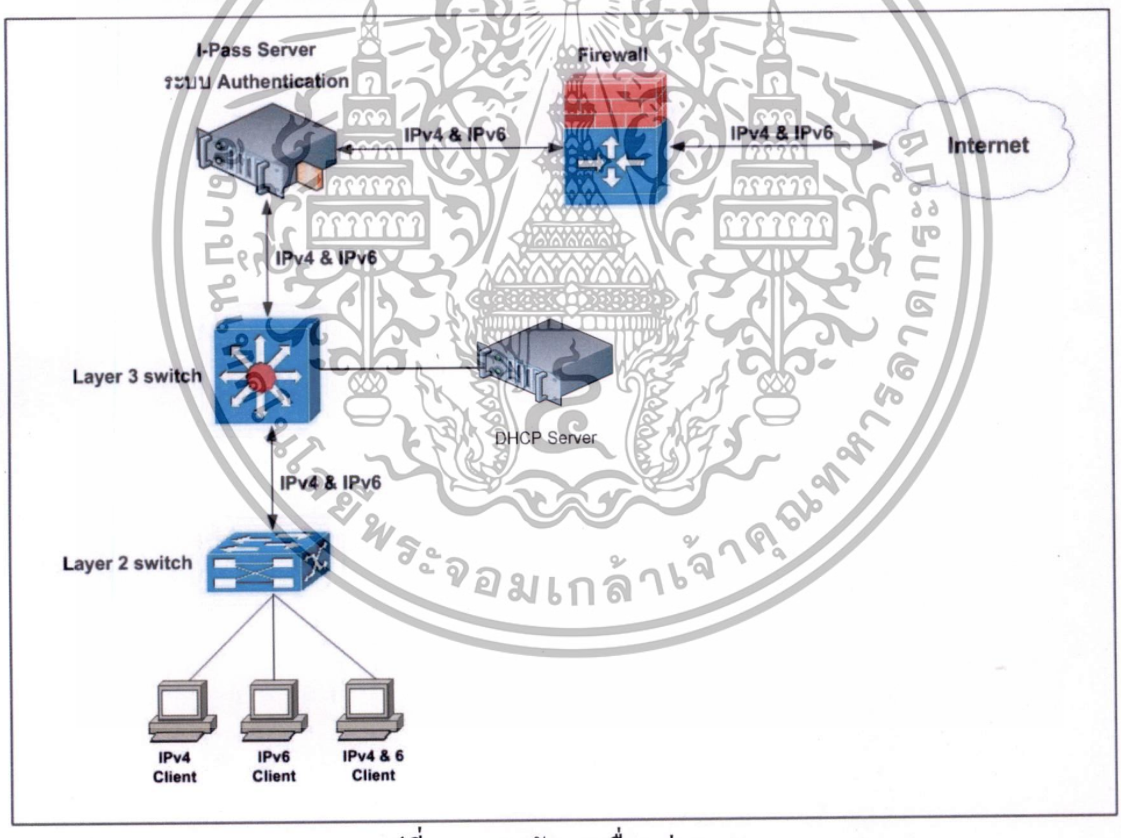
จากนั้นรูปแบบของการแบ่ง Subnet ในหลักถัดไป (/64) จะเป็นดังตารางที่ 4.1 โดยมีการอ้างอิงถึง Subnet ของ IPv4 Address ที่มีอยู่ ในปัจจุบันมีการแบ่งเป็น Class C

ตารางที่ 4.1 ตัวอย่างรูปแบบการจัดสรร IPv6 และ IPv4 Address

Private IPv4				IPv6			
8 Bits	8 Bits	8 Bits	8 Bits	Site Prefix /48 (48 Bits)	Subnet /52 (4 Bits)	Subnet /64 (12 Bits)	Interface ID /128 (64 Bits)
10	1	1	0	2001:3c8:1408	1	001	::
10	1	171	0	2001:3c8:1408	1	171	::
10	1	172	0	2001:3c8:1408	1	172	::
10	2	1	0	2001:3c8:1408	2	001	::
10	2	254	0	2001:3c8:1408	2	254	::

4.2 ดำเนินการติดตั้งและตั้งค่าอุปกรณ์เครือข่าย (Configuration)

4.2.1 แผนผังการเชื่อมต่อระบบใหม่



รูปที่ 4.2 แผนผังการเชื่อมต่อระบบ

จากรูปที่ 4.2 แสดงถึงแผนผังการเชื่อมต่อระบบโดยข้อมูลจากเครื่องลูกข่าย (Client) จะได้รับ IPv6 จากอุปกรณ์ Layer 3 switch แบบ SLAAC จากนั้นเมื่อเครื่องลูกข่ายต้องการใช้งานอินเทอร์เน็ต จะถูกส่งต่อไปที่ IPASS server เพื่อทำการพิสูจน์ตัวตน (Authentication) เมื่อผ่าน

การพิสูจน์ตัวตนเรียบร้อย ระบบจะทำการจัดเก็บข้อมูลรหัสผู้ใช้ IPv4 และ IPv6 Address จากนั้นจะทำการ Routing ไปยังไฟร์วอลล์ และออกสู่อินเทอร์เน็ตต่อไป

4.2.2 ตั้งค่าอุปกรณ์ Layer 3 switch เพื่อให้รองรับ IPv6

ระบบเครือข่ายของมหาวิทยาลัยศรีนครินทรวิโรฒมี Layer 3 switch โดยต้องมีการตั้งค่า (Configuration) เพื่อให้สามารถส่งผ่านข้อมูล (Traffic) ของ IPv6 และสามารถแจก IPv6 ที่เป็นแบบ SLAAC ดังต่อไปนี้

```
# vlan 171 enable name "Client-FL12"
# vlan 171 port default 9/24
# ip interface "GW-Client-FL12" address 10.1.171.1 mask 255.255.255.0 vlan 171

# ipv6 interface "v6if-v171" vlan 171
# ipv6 address 2001:3c8:1408:1171::1/64 "v6if-v171"
# ipv6 static-route ::/0 gateway 2001:3c8:1408:1153::63 v6if-v153
```

4.2.3 ตั้งค่าอุปกรณ์ไฟร์วอลล์ (Firewall) เพื่อให้รองรับ IPv6

การตั้งค่า IPv6 สำหรับอุปกรณ์ไฟร์วอลล์ (Firewall) จะต้องมีการตั้งค่า Routing และกำหนด Policy ที่อนุญาตให้แพ็กเก็ตของ IPv6 ผ่านได้ตาม Service ที่ต้องการ ดังต่อไปนี้

1) กำหนดหมายเลข IPv6 Address ให้กับ Interface ที่เชื่อมต่อกับ IPASS Server
2) กำหนด Routing ที่จะออกสู่อินเทอร์เน็ต และเครือข่ายภายใน
3) กำหนด Policy ที่จะอนุญาต (Allow) หรือปฏิเสธ (Deny) การให้บริการ

4.3 ดำเนินการติดตั้งระบบยืนยันตัวตน

4.3.1 ติดตั้งระบบปฏิบัติการ CentOS 6.6

เครื่องคอมพิวเตอร์แม่ข่ายที่นำมาติดตั้งระบบยืนยันตัวตน จะต้องมี Network card อย่างน้อย 2 อัน เพื่อใช้ติดต่อกับ Layer 3 switch และอุปกรณ์ไฟร์วอลล์ โดยมีการตั้งค่าเป็นแบบบริดจ์ (Bridge) เพื่อที่จะไม่ต้องกำหนดไอพีแอดเดรสของทั้ง 2 การ์ด แต่จะกำหนดไอพีแอดเดรสของบริดจ์เพื่อใช้ในการเข้าถึง Captive Portal แทน

4.3.2 ติดตั้งระบบรักษาความปลอดภัย (Firewall)

เมื่อติดตั้งระบบปฏิบัติการเป็นที่เรียบร้อยแล้ว จะมีโปรแกรม IPTables และ IP6Tables ซึ่งเป็นโปรแกรมไฟร์วอลล์ที่ทำงานอยู่ใน Kernel ใช้สำหรับการกำหนดกฎ (Rules) ที่จะอนุญาต

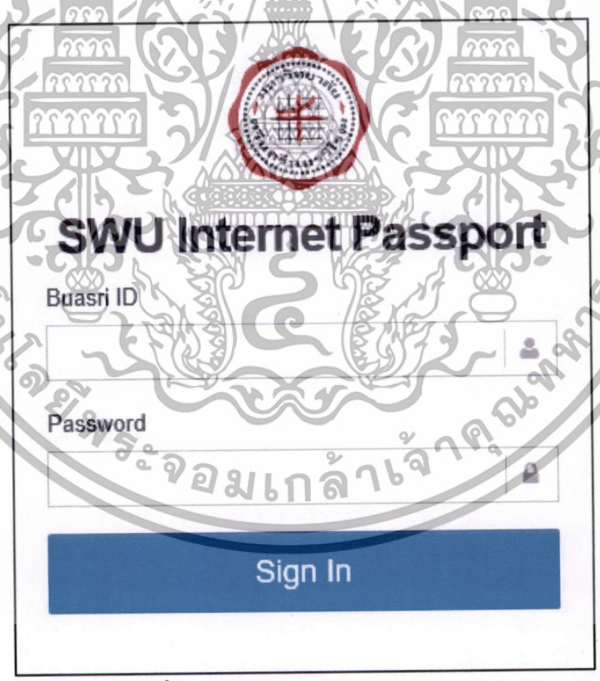
ว่าไอพีแอดเดรสใดสามารถผ่านเข้า-ออกได้บ้าง โดยโปรแกรมนี้จะมีหน้าที่ในการ Redirect แพ็กเก็ตที่เข้ามาผ่านเครื่อง IPASS Server ให้ไปที่ Captive Portal โดยในหน้า Captive Portal จะให้ใส่รหัสผู้ใช้ และรหัสผ่าน กรณีที่ใส่ถูกต้องก็จะนำไอพีแอดเดรสของเครื่องลูกข่าย (Client) ไปใส่ยัง Rules ของ IPTables เพื่ออนุญาตให้แพ็กเก็ตนั้นผ่านได้ กรณีที่ผู้ใช้ออกจากระบบ (Logout) ระบบจะทำการส่งค่าไอพีแอดเดรสเพื่อนำออกจากกฎของ IPTables

4.3.3 ติดตั้ง Web Server (Apache หรือ NginX)

Web Server จะเป็นหน้า Captive Portal ให้ผู้ใช้ทำการ login เพื่อเข้าสู่การใช้งานเครือข่ายอินเทอร์เน็ต

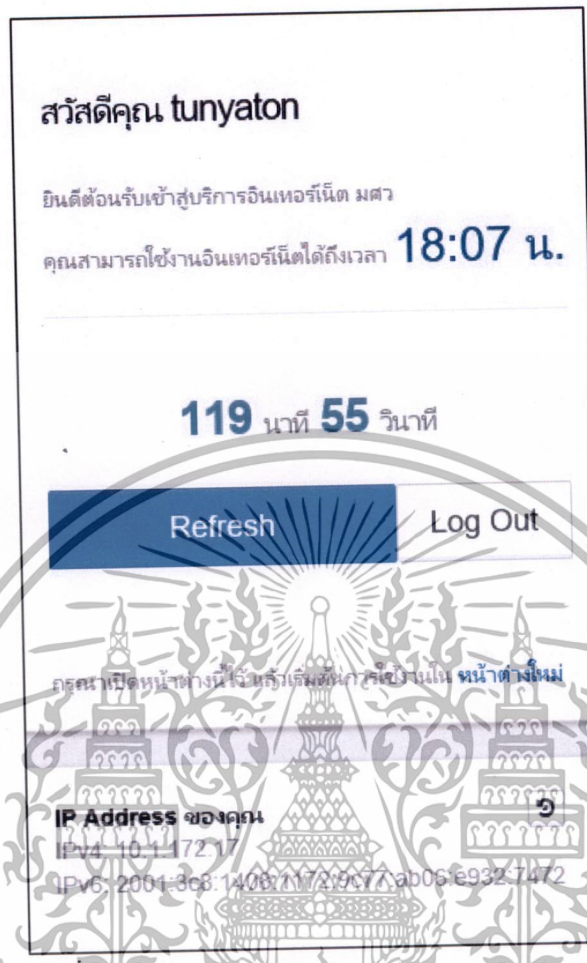
4.4 การออกแบบหน้าจอการทำงานของโปรแกรม

รูปแบบของหน้าจอการทำงาน โดยหลักการแล้วเมื่อผู้ใช้งานจะเข้าสู่ระบบอินเทอร์เน็ตจะถูกโปรแกรม firewall redirect มาที่ Captive Portal เพื่อให้ผู้ใช้ทำการยืนยันตัวตน โดยลักษณะหน้าจอจะเป็นดังรูปที่ 4.3



รูปที่ 4.3 ฟอร์มสำหรับ Login

เมื่อทำการ Login โดยใส่รหัสผู้ใช้ที่อยู่บน LDAP ที่ถูกต้องจะปรากฏหน้าจอนับเวลาดังรูปที่ 4.4



รูปที่ 4.4 หน้าจอแสดงการนับเวลา และ IP Address

โดยในหน้าจอนี้จะแสดงรายละเอียดดังนี้

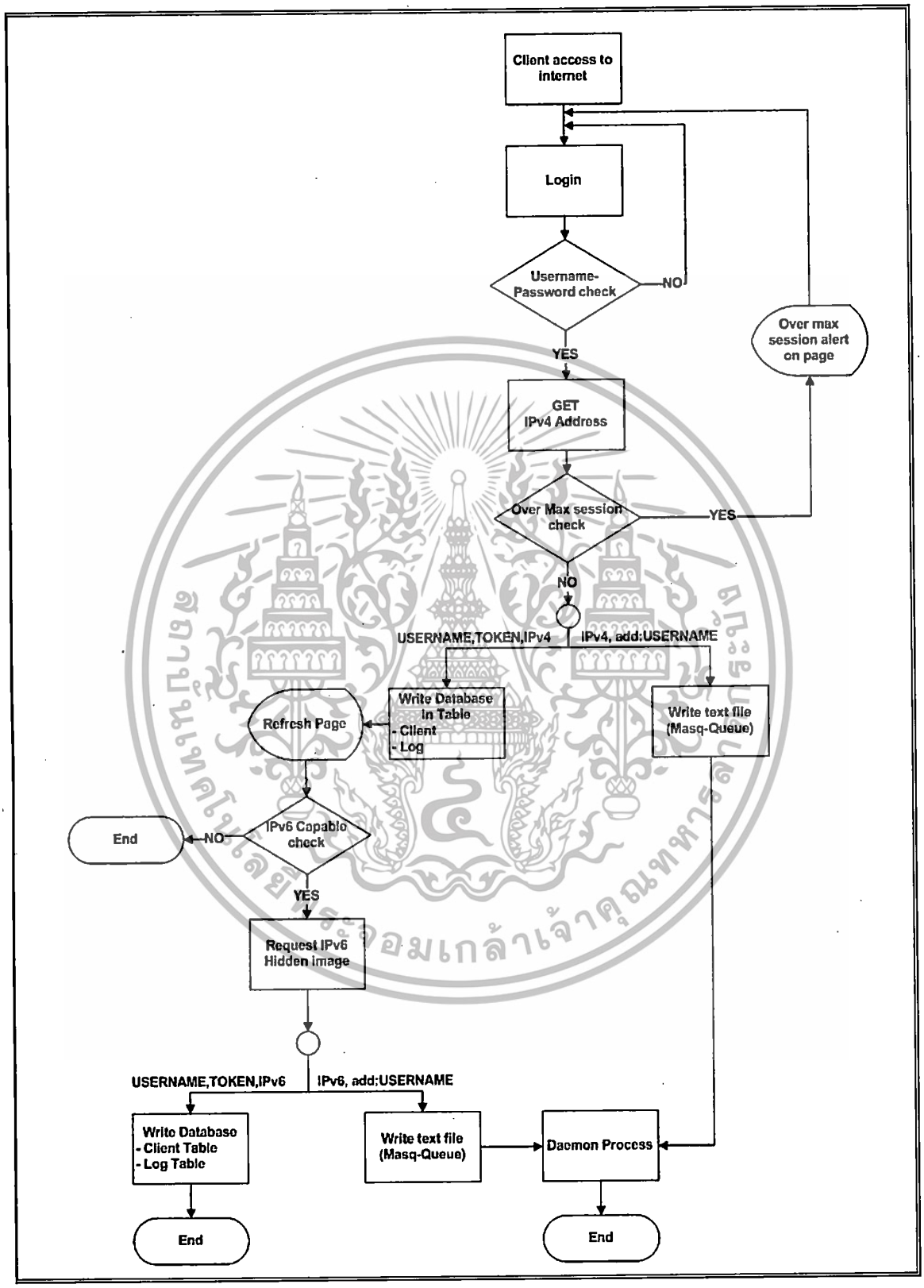
1) ชื่อบัญชีผู้ใช้งานที่ Login เข้ามาในระบบ
2) เวลาที่ผู้ใช้จะสามารถใช้งานได้ถึงเวลาเท่าไร โดยโปรแกรมจะตั้งไว้ 2 ชั่วโมง
3) เวลานับถอยหลังโดยเริ่มต้นที่ 120 นาที 00 วินาที
4) ปุ่ม Refresh ใช้ในกรณีที่ผู้ใช้งานต้องการต่อเวลาใช้งานเพิ่ม
5) ปุ่ม Log out ใช้สำหรับ Log out ออกจากระบบ
6) แสดงไอพีแอดเดรสของผู้ใช้ที่เข้ามาในระบบ ซึ่งจะมีหมายเลข IPv4 และ IPv6 Address ถ้าเครื่องนั้นมีหมายเลข IPv6 Address ผู้ใช้สามารถเข้าใช้งานได้ถึงเวลาเท่าไร ซึ่งในระบบเบื้องต้นจะตั้งค่าไว้ที่ 2 ชมแล้วจะมีโปแกรมที่เป็น java script ในการนับเวลาถอยหลัง

4.5 การทำงานของระบบยืนยันตัวตน

4.5.1 การ Login

1) เครื่องลูกข่ายต้องการออกสู่เครือข่ายอินเทอร์เน็ต
2) ระบบจะทำการ redirect ไปยังหน้า Captive Portal เพื่อทำการยืนยันตัวตน
3) ทำการตรวจสอบรหัสผู้ใช้และรหัสผ่าน
   - ถ้าถูกต้องทำการ get IPv4 Address
   - ถ้าไม่ถูกต้องก็ทำการกลับไปหน้า Login ใหม่
4) ทำการตรวจสอบ Max Session ว่าเกินค่า Max Session หรือไม่
   - ถ้าเกินก็ให้กลับไปหน้า Login ใหม่แล้วแสดงข้อความแจ้งเตือน
   - ถ้าไม่เกินก็ดำเนินการต่อ
5) ในขั้นตอนนี้จะดำเนินการ 2 ส่วนคือส่วนที่เก็บลง Database และส่วนที่ทำการ write text file ใน queue folder เพื่อให้ Daemon Process (hupnet) ไปทำงานต่อ
6) หลังจากที่เก็บลง Database แล้วจะทำการแสดงหน้า refresh page ขึ้นมา
7) จากนั้นทำการ check ว่าเครื่องลูกข่ายมี IPv6 หรือไม่โดยการ request hidden image ไปยัง IPv6 Address
   - ถ้ามี IPv6 Address ก็ทำการเก็บ IPv6 Address ลง Database และทำการ write text file ใน queue folder เพื่อให้ Daemon Process ไปทำงานต่อ
   - ถ้าไม่มี IPv6 Address ก็จบการทำงานในส่วนนี้

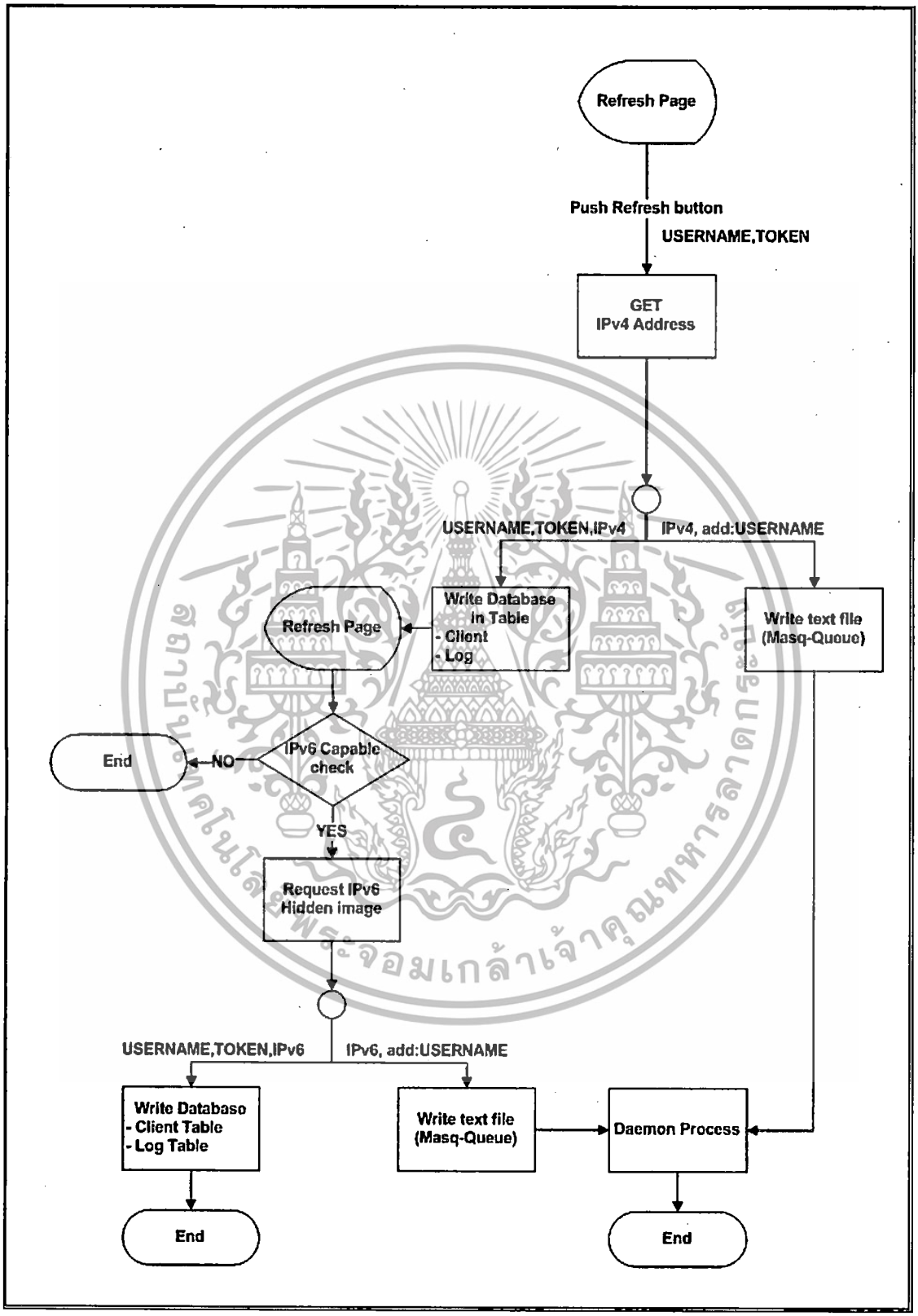
Flow Chart การ Login



4.5.2 การกดปุ่ม Refresh

1) หน้า Refresh page เมื่อผู้ใช้ทำการกด Refresh ก็จะทำการ Get IPv4 Address
2) ในขั้นตอนนี้จะดำเนินการ 2 ส่วนคือส่วนที่เก็บลง Database และส่วนที่ทำการ write text file ใน queue folder เพื่อให้ Daemon Process (hupnet) ไปทำงานต่อ
3) หลังจากที่เก็บลง Database แล้วจะทำการแสดงหน้า refresh page ขึ้นมา
4) จากนั้นทำการ check ว่าเครื่องลูกข่ายมี IPv6 หรือไม่โดยการ request hidden image ไปยัง IPv6 Address
5) ถ้ามี IPv6 Address ก็ทำการเก็บ IPv6 Address ลง Database และทำการ write text file ใน queue folder เพื่อให้ Daemon Process ไปทำงานต่อ
6) ถ้าไม่มี IPv6 Address ก็จบการทำงานในส่วนนี้

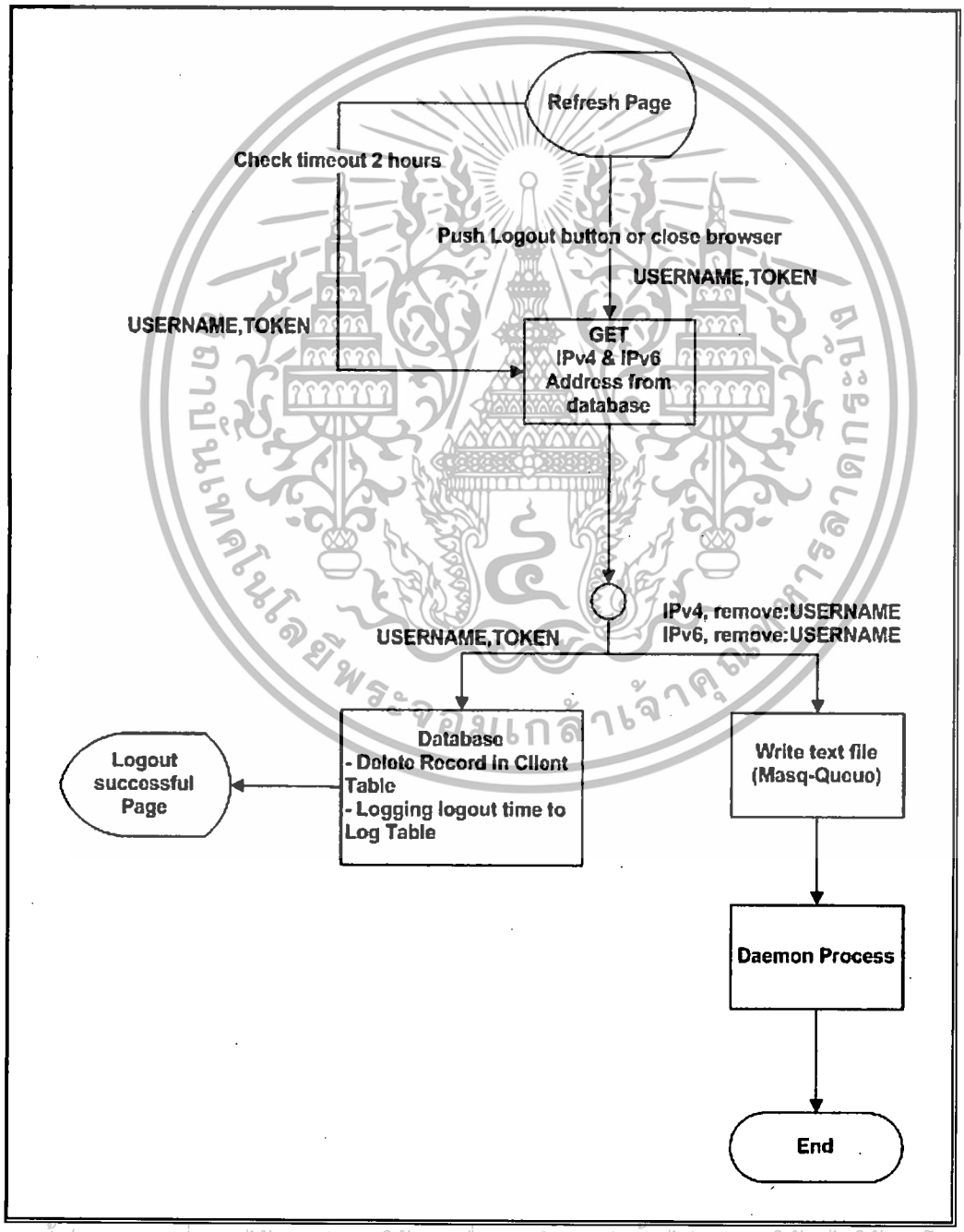
Flow Chart การกดปุ่ม Refresh



4.5.3 การกดปุ่ม Logout และหมดเวลา 2 ชั่วโมงตามที่กำหนด

1) เมื่อมีการกดปุ่ม Logout หรือปิด browser จะทำการ Get ค่า IPv4 และ IPv6 Address
2) ในขั้นตอนนี้จะดำเนินการ 2 ส่วนคือ ทำการ delete record ใน Client Table และ logging logout time ใน Log Table และแสดงหน้า logout สำเร็จ และทำการ Write text file ใน queue folder ใน ว่าทำการ Remove
3) จากนั้น Daemon Process ก็มาดำเนินการต่อ

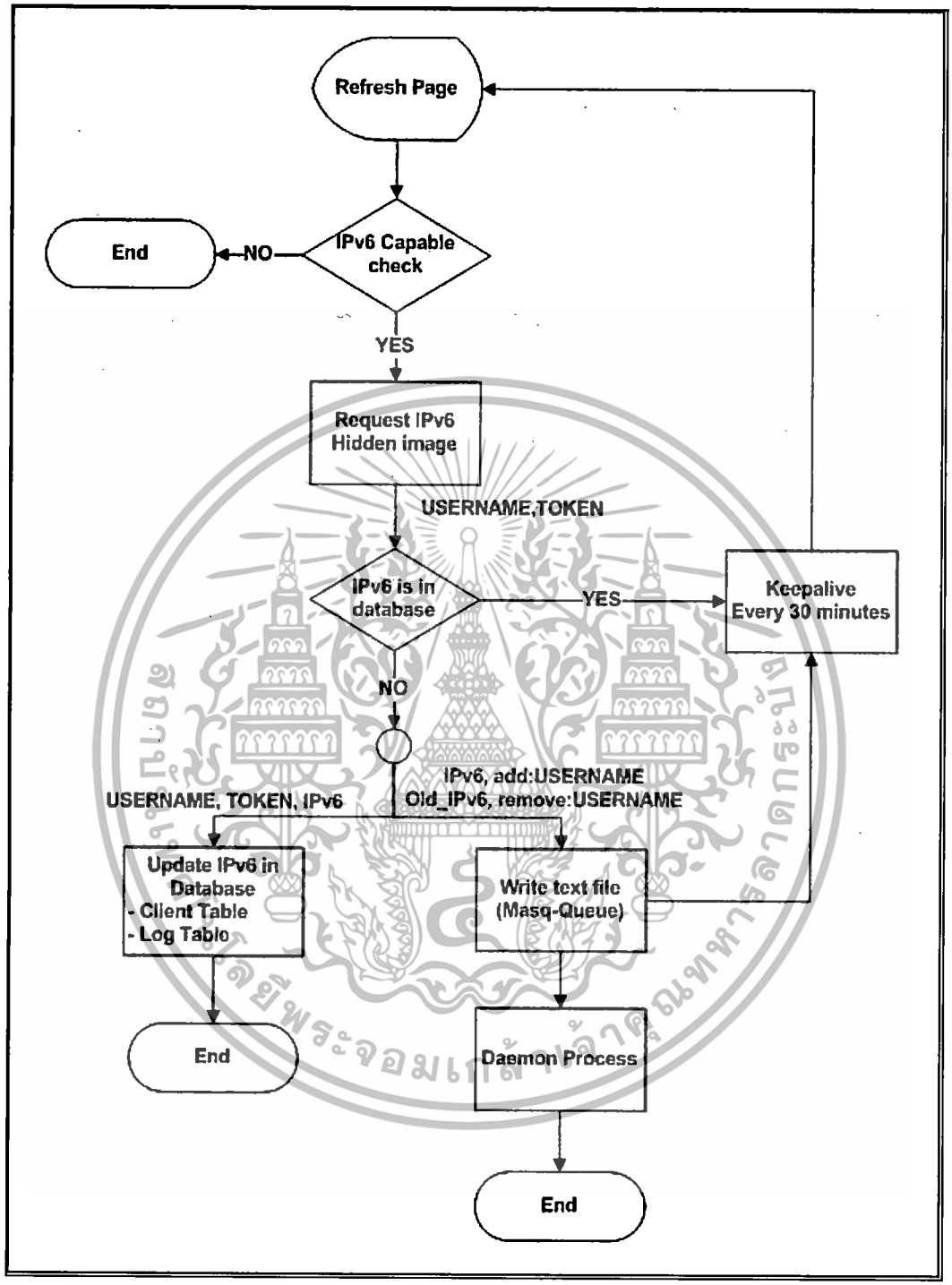
Flow Chart การกดปุ่ม Logout และหมดเวลา 2 ชั่วโมงตามที่กำหนด



4.5.4 การตรวจสอบการเปลี่ยนแปลง IPv6 Address

1) หน้า Refresh Page นั้นจะทำการตรวจสอบว่าเครื่องลูกข่ายมี IPv6 หรือไม่
   - ถ้ามี IPv6 Address ก็ทำการตรวจสอบใน Database ว่า username นี้กับ IPv6 Address ยังเป็นค่าเดิมไหม ถ้าเป็นค่าเดิมก็ไม่ทำอะไร ซึ่งระบบจะทำการตรวจสอบทุก 30 นาที
   - ถ้ามี IPv6 Address แต่ทำการตรวจสอบใน Database กับค่า IPv6 Address ที่ get ได้ไม่เหมือนกันแสดงว่า IPv6 Address มีการเปลี่ยนแปลง ก็ให้ทำการ update ipv6 ใน Database และทำการ write text file ใน queue folder โดยทำการ ส่ง IPv6 เก่าไปลบทิ้ง และส่ง IPv6 ใหม่ไปทำการ add
   - ถ้าไม่มี IPv6 Address ก็จบการทำงาน
2) จากนั้น Daemon Process ก็มาดำเนินการต่อ

Flow Chart การตรวจสอบการเปลี่ยนแปลง IPv6 Address



4.5.5 การทำงานของ Daemon Process

1) Daemon Process จะทำการอ่าน queue folder

2) ระบบก็จะทำการตรวจสอบว่าเป็น Add หรือ Remove

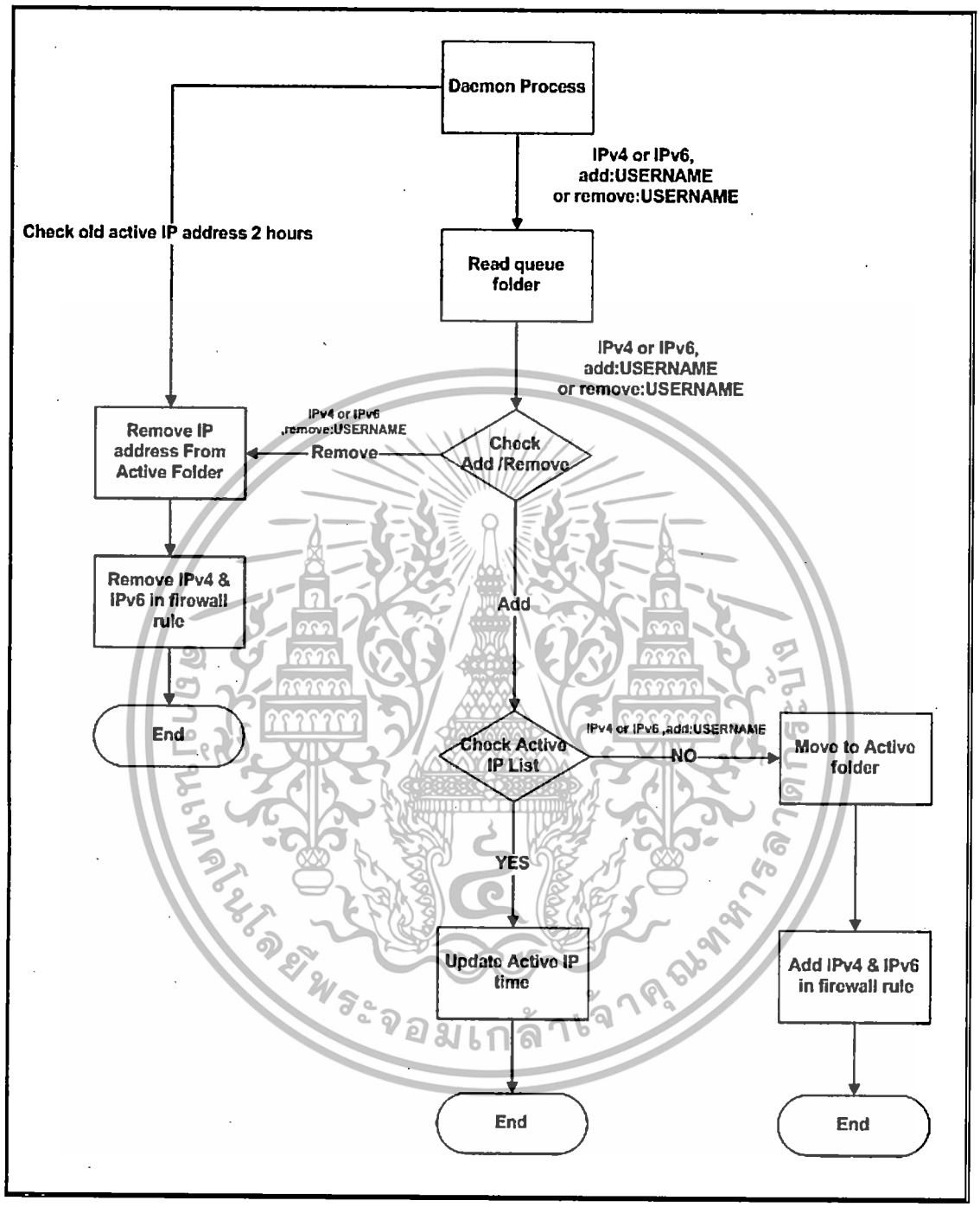
2.1) ถ้าเป็น Add ก็ทำการตรวจสอบว่ามี IP อยู่ใน active folder หรือไม่

- ถ้ามี IP อยู่แล้วก็จะทำการ update Active IP time
- ถ้าไม่มี IP อยู่ก็จะทำการ move จาก queue folder ไปยัง active folder
- จากนั้นก็ทำการ เขียน firewall rule ให้ allow ip address นั้น

2.2) ถ้าเป็น Remove

- ก็จะทำการ Remove IP Address จาก Active Folder
- จากนั้นทำการเขียน firewall rule เพื่อลบ IPv4 & IPv6 ทิ้งไป

Flow Chart การทำงานของ Daemon Process



บทที่ 5

การทำงานของระบบ

จากการดำเนินการออกแบบและติดตั้งระบบยืนยันตัวตน จากบทที่ 4 ได้มีการติดตั้งระบบปฏิบัติการ CentOS 6.6 โปรแกรมส่วนประกอบอื่นๆ เช่น Nginx และดำเนินการโปรแกรมตามขั้นตอนใน Flowchart เป็นที่เรียบร้อยแล้วนั้น การทำงานของระบบจะขอกล่าวในบทนี้

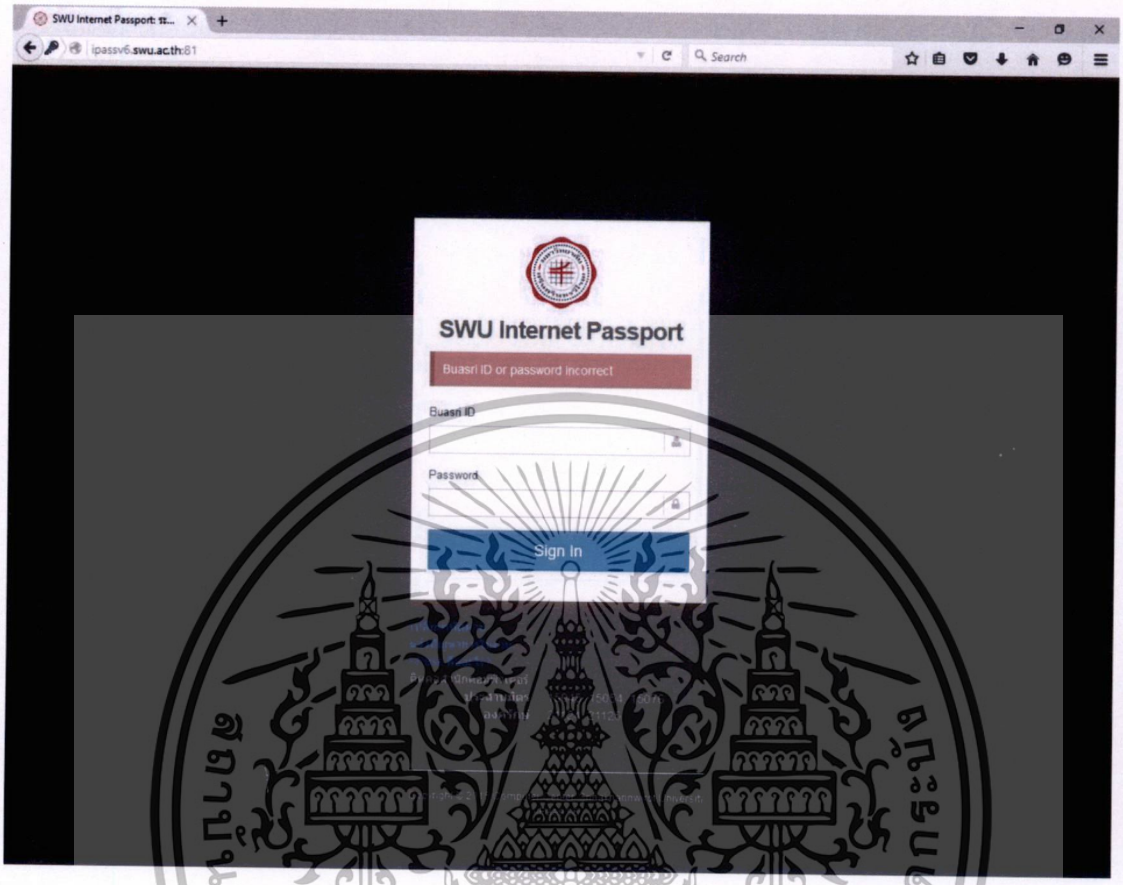
5.1 การใช้งานระบบยืนยันตัวตน

5.1.1 การ Sign In เข้าใช้

เมื่อเข้าสู่หน้าจอหลักในการ Sign In เข้าระบบจะปรากฏหน้าจอดังรูปที่ 5.1 โดยทำการกรอกชื่อผู้ใช้งาน และรหัสผ่าน ลงในกล่องข้อความ จากนั้นกดปุ่ม Sign In เพื่อเข้าสู่ระบบ

รูปที่ 5.1 หน้าจอระบบยืนยันตัวตน

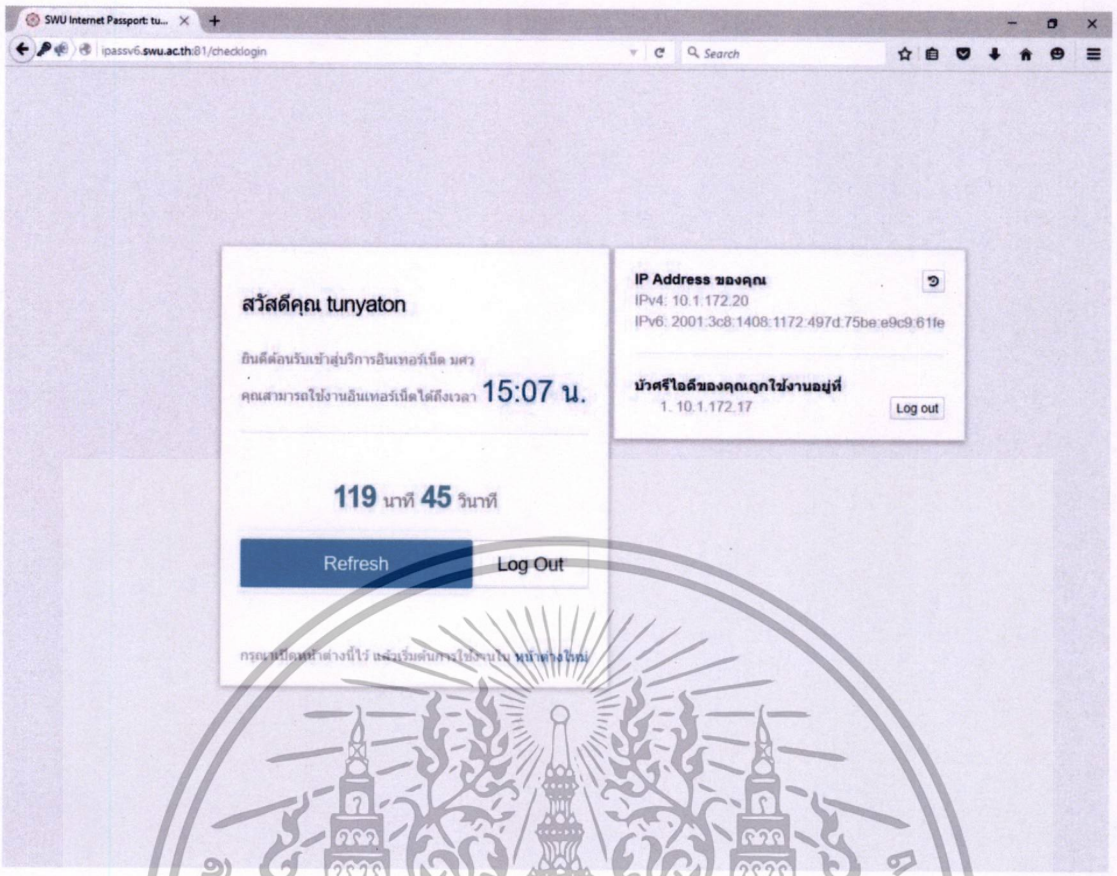
หากใส่ชื่อผู้ใช้งาน หรือรหัสผ่านไม่ถูกต้อง จะปรากฏข้อความ “Buasri ID or password incorrect” ดังรูปที่ 5.2 และให้ทำการกรอกข้อมูลอีกครั้ง



รูปที่ 5.2 หน้าจอเมื่อกรอกข้อมูลไม่ถูกต้อง

เมื่อกรอกข้อมูลถูกต้อง จะปรากฏหน้าจอดังรูปที่ 5.3 โดยข้อมูลที่ปรากฏมีดังต่อไปนี้

- ข้อความต้อนรับ และชื่อผู้ใช้งานที่ใช้ในการ Sign In
- เวลาสิ้นสุดการใช้งานอินเทอร์เน็ตที่สามารถใช้ได้
- นับเวลาถอยหลัง 120 นาที (2 ชั่วโมง) เนื่องจากมีการกำหนดการใช้งานให้สามารถใช้งานได้นานสูงสุด 2 ชั่วโมง ต่อการ Sign In 1 ครั้ง
- ข้อมูล IPv4 และ IPv6 Address ของเครื่องที่ใช้ในการ Sign In
- แสดง IPv4 Address ว่าชื่อผู้ใช้งานนี้ใช้งานอยู่ที่เครื่องใดบ้างในขณะนั้น (เฉพาะเมื่อมีการ Sign In ตั้งแต่ 2 เครื่องขึ้นไป)



รูปที่ 5.3 หน้าจอนับเวลาถอยหลัง

5.1.2 การต่อเวลาการใช้งาน

หากยังไม่ครบกำหนดเวลา 2 ชั่วโมง สามารถทำการต่อเวลาได้โดยไม่ต้อง Sign In ใหม่ โดยการกดปุ่ม Refresh ที่หน้าจอนับเวลาถอยหลัง กรณีที่หมดเวลา 2 ชั่วโมง จะต้องทำการ Sign in ใหม่อีกครั้ง

5.1.3 การยกเลิกหรือออกจากการใช้งาน

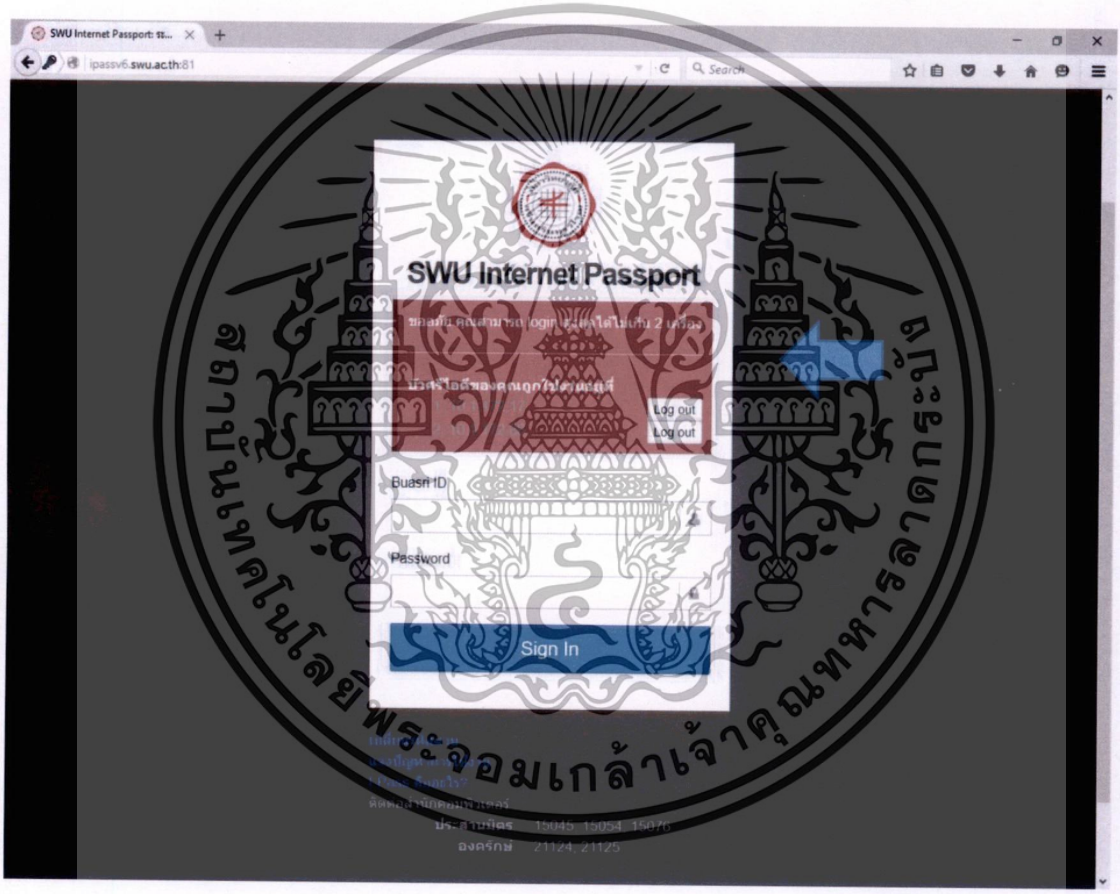
กดปุ่ม Log Out ที่หน้าจอนับเวลาถอยหลัง ระบบจะทำการออกจากระบบให้ทันที โดยทำการลบ IPv4 และ IPv6 Address ของเครื่องนั้นๆออกจาก Firewall Rule

5.1.4 การยกเลิกหรือออกจากการใช้งานในกรณี Sign In หลายเครื่อง

ในกรณีที่มีการ Sign In อยู่ที่เครื่องอื่นด้วยในขณะนั้น ในหน้าจอนับเวลาจะแสดงข้อมูล IP Address ของเครื่องก่อนหน้านี้ที่ทำการ Sign In เอาไว้และสามารถกด Log Out เพื่อยกเลิกการใช้งานของเครื่องที่มี IP Address นั้นได้

5.1.5 การจำกัดจำนวนเครื่องใช้งาน

หากมีการ Sign In ด้วยชื่อผู้ใช้งานเดียวกันในเวลาเดียวกันเกินจากที่กำหนดไว้ คือ 2 เครื่อง จะมีข้อความเตือน “ขออภัย คุณสามารถ Login สูงสุดได้ไม่เกิน 2 เครื่อง” ปรากฏขึ้น พร้อมทั้งแสดง IPv4 Address ของเครื่องที่มีการใช้งานอยู่ ผู้ใช้งานสามารถเลือก Log out ออกจากเครื่องเหล่านั้นได้โดยการกดปุ่ม Log out ด้านหลัง IPv4 Address ของเครื่องที่ต้องการยกเลิกการใช้งานในขณะนั้น ดังรูปที่ 5.4 และหลังจากทำการ Log Out แล้ว จะสามารถทำการ Sign In เข้าใช้บริการได้ตามปกติ



รูปที่ 5.4 หน้าจอแจ้งเตือน Session เกินกำหนด

5.2 การทดสอบการทำงานของระบบ

เนื่องจากภายในมหาวิทยาลัยเครื่องที่เป็นเครื่องลูกข่ายที่จะใช้งานระบบนั้นมีความหลากหลาย ซึ่งจำเป็นต้องมีการทดสอบการทำงานของบราวเซอร์และระบบปฏิบัติการต่างๆให้รองรับความต้องการของผู้ใช้ให้ได้มากที่สุด ซึ่งโดยรวมผู้ใช้งานภายในมหาวิทยาลัยจะมีการใช้ระบบปฏิบัติการอยู่ด้วยกัน 4 ระบบปฏิบัติการ คือ Microsoft Windows MacOS ที่เป็นอุปกรณ์คอมพิวเตอร์แบบตั้งโต๊ะ ส่วนอุปกรณ์ที่เป็นโทรศัพท์มือถือก็จะทำการทดสอบระบบปฏิบัติการที่เป็น iOS และ Android ในส่วนของบราวเซอร์ที่นิยมใช้ภายในมหาวิทยาลัยมีอยู่ 4 บราวเซอร์คือ Internet Explorer (IE) Chrome Safari และ Firefox ซึ่งทั้งหมดนี้ได้ทำการทดสอบผลการทำงานในแง่มุมต่างของระบบ โดยมีผลที่ได้ดังตารางที่ 5.1

ตารางที่ 5.1 การทดสอบการทำงานของระบบบนระบบปฏิบัติการและบราวเซอร์ที่แตกต่าง

รายการ	Windows (10)			MacOS X (10.11.4)			iOS (9.3.1)		Android (6.0.1)	
	IE (11)	Chrome (49.0.2623.112 m)	Firefox (48.0.1)	Safari (9.1)	Chrome (49.0.2623.112)	Firefox (45.0.2)	Safari	Chrome (50.0.2661.77)	Browser (4)	Chrome (49.0.2623.105)
การ Sign In เข้าใช้	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
การต่อเวลาการใช้งาน	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
การยกเลิกหรือออกจากการใช้งาน	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
การยกเลิกหรือออกจากการใช้งานในกรณี Sign In หลายเครื่อง	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
การจำกัดจำนวนเครื่องใช้งาน	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

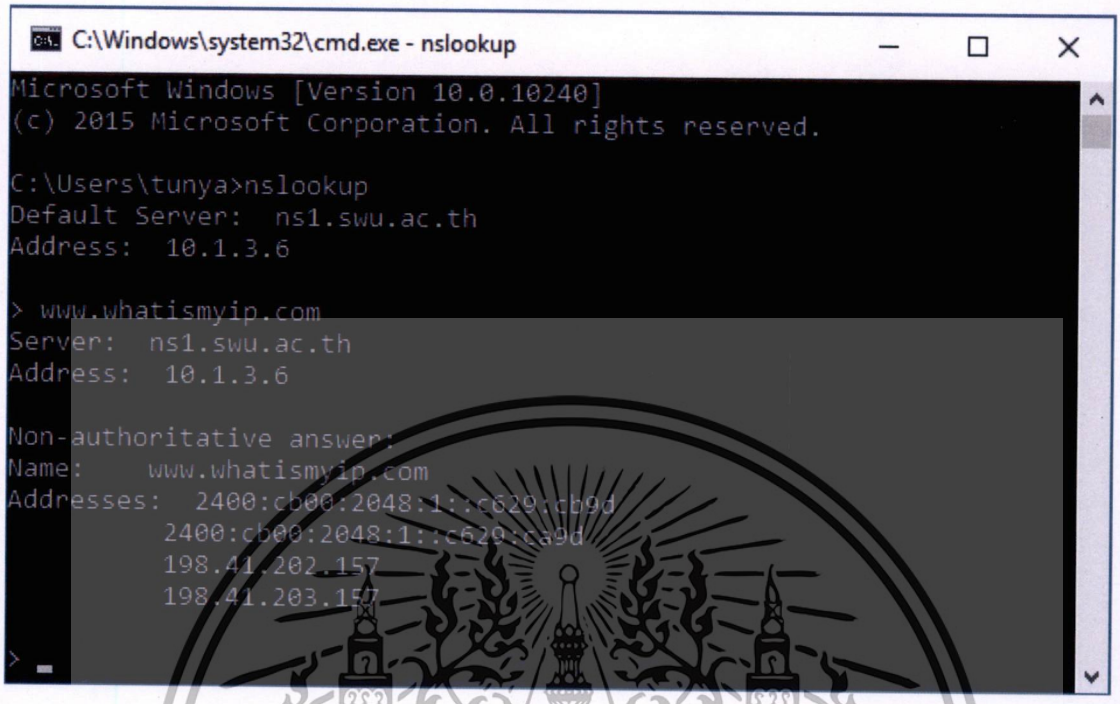
☑ = สามารถใช้งานได้ ☐ = ไม่สามารถใช้งานได้

จากผลการทดสอบจะเห็นว่าสามารถใช้งานได้ทุกบราวเซอร์และทุกระบบปฏิบัติการที่ครอบคลุมการใช้งานภายในมหาวิทยาลัย ซึ่งการทดสอบในแต่ละรายการจะดำเนินการทดสอบดังนี้

1) การ Sign In เข้าใช้ ดำเนินการโดยทำการทดสอบการ login ผิดซ้ำๆกันหลายครั้งและทำการ login ถูกและลองทำการ login โดยการใส่ค่าที่ไม่ใช่ character หรือการทดสอบเรื่องความปลอดภัยโดยการใส่รหัสผู้ใช้ เป็น hi' or 1=1 -- และรหัสผ่าน เป็น hi' or 1=1 – ซึ่งเป็นการทดสอบ sql injection ก็ปรากฏว่าไม่สามารถ login เข้าระบบได้ และทำการทดสอบโดยการใส่ character ที่เป็นค่ามากๆระบบก็สามารถทำงานได้ถูกต้อง
2) การต่อเวลาการใช้งาน ดำเนินการทดสอบโดยทำการกดปุ่ม refresh หลายๆครั้งและทำการเข้าไปดูในระบบก็พบว่ามีการปรับเปลี่ยนค่าที่จะหมดเวลาไปอีก 2 ชั่วโมงซึ่งทำให้การหมดเวลาการทำงานถูกต้อง
3) การยกเลิกหรือออกจากการใช้งาน ดำเนินการทดสอบโดยกดปุ่ม Logout และทำการตรวจสอบดูใน IPtables ซึ่งเป็น Firewall ซึ่งจะพบว่า IP Address ที่ทำการ Logout แล้วจะไม่ปรากฏใน List ของ IPtables ที่อนุญาตให้ใช้งาน และมีข้อมูลเวลาที่ IP Address และผู้ใช้ทำการ Logout เก็บลงฐานข้อมูล
4) การยกเลิกหรือออกจากการใช้งานในกรณี Sign In หลายเครื่อง ดำเนินการทดสอบโดยการ Sign In โดยใช้รหัสผู้ใช้รหัสเดียวกันหลายๆเครื่อง ซึ่งระบบก็แจ้งเตือนว่ามีการใช้งานอยู่อีกเครื่องและแสดงหมายเลข IP Address ที่ Sign In อยู่ที่เครื่องอื่นด้วย เมื่อทำการสั่ง Logout IP Address นั้นแล้ว เมื่อเข้าไปตรวจสอบ IPtables ที่เป็น Firewall ก็พบว่า IP ดังกล่าวไม่ปรากฏอยู่ใน List ของ IPtables ที่อนุญาตให้ใช้งาน และมีข้อมูลเวลาที่ IP Address และผู้ใช้ทำการ Logout เก็บลงฐานข้อมูล
5) การจำกัดจำนวนเครื่องใช้งาน ดำเนินการทดสอบโดยทำการ Sign In โดยใช้รหัสผู้ใช้เดียวกันจำนวน 3 เครื่องปรากฏว่าเครื่องที่ 3 ไม่สามารถจะทำการ Sign In ได้ซึ่งทำการตรวจสอบแล้วเครื่องที่ 3 กรณีที่ยังไม่ Logout IP Address ของเครื่องที่ 1 หรือเครื่องที่ 2 ก็จะไม่สามารถออกอินเทอร์เน็ตได้ และทำการทดสอบโดยการ Logout เครื่องที่ 1 จากนั้นเครื่องที่ 3 จึงจะสามารถ Sign In เพื่อเข้าใช้งานได้ตามปกติ

5.3 การทดสอบการใช้งานเข้าเว็บไซต์

5.3.1 ทดสอบการเข้าเว็บไซต์ที่เป็น IPv4 และ IPv6 Address

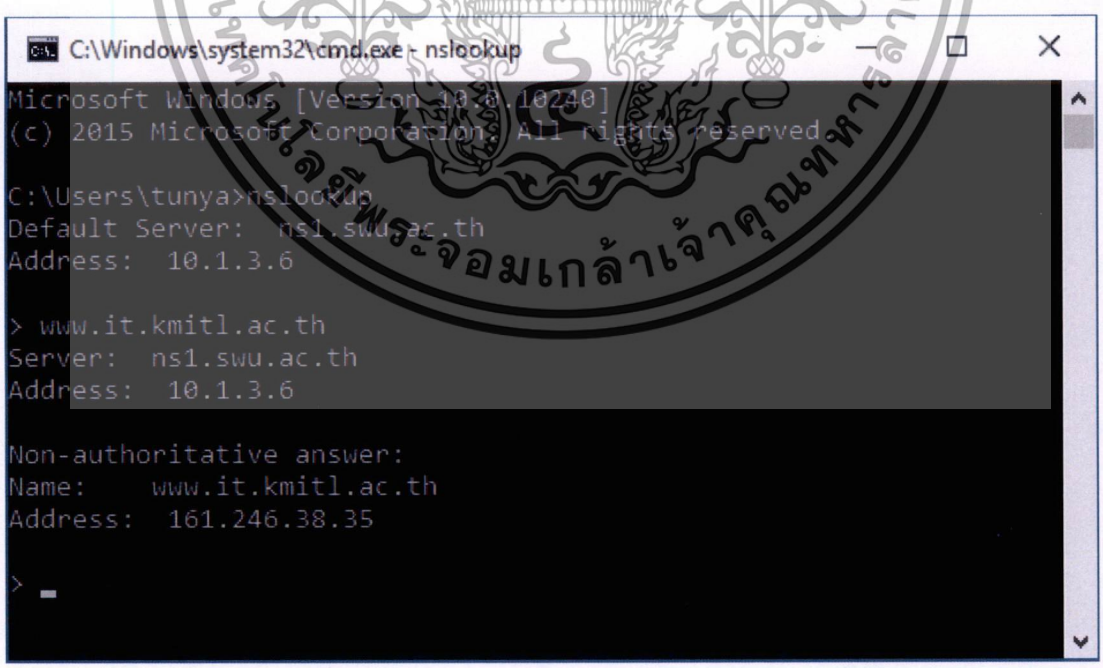


รูปที่ 5.5 การแปลงชื่อเป็น IPv4 และ IPv6 Address

ทำการทดสอบการโดยเข้าเว็บไซต์ที่มีทั้ง IPv4 และ IPv6 Address ตัวอย่างเช่น www.whatismyip.com จากรูปที่ 5.5 เป็นการแปลงชื่อเป็น IP Address ด้วยคำสั่ง nslookup ผ่านโปรแกรม cmd บนระบบปฏิบัติการ Windows จะเห็นได้ว่าเว็บไซต์ดังกล่าวมีการใช้งาน IP Address ทั้งสองแบบ หลังจากที่เราทำการ Sign In เรียบร้อยแล้ว ระบบจะทำการอนุญาต (Allow) บนไฟร์วอลให้ IPv4 และ IPv6 Address ของเครื่องไคลเอนต์สามารถออกไปใช้งานเว็บไซต์ภายนอกได้ ตามหลักการของ IPv6 แบบ Dual-stack ในกรณีที่เว็บไซต์มีทั้ง IPv4 และ IPv6 ระบบปฏิบัติการจะทำการเลือกไปที่เว็บไซต์ด้วย IPv6 Address ก่อน IPv4 Address เสมอ ผลที่ได้จากการเข้าเว็บไซต์ www.whatismyip.com เป็นดังรูปที่ 5.6 ซึ่งเว็บไซต์นี้จะแสดงข้อมูล IP Address ของเครื่องที่เข้าไป จะเห็นได้ว่า IP Address ที่ปรากฏนั้น เป็น IPv6 Address ของเครื่องไคลเอนต์

รูปที่ 5.6 หน้าจอแสดงการเข้าเว็บไซต์ด้วย IPv6 Address

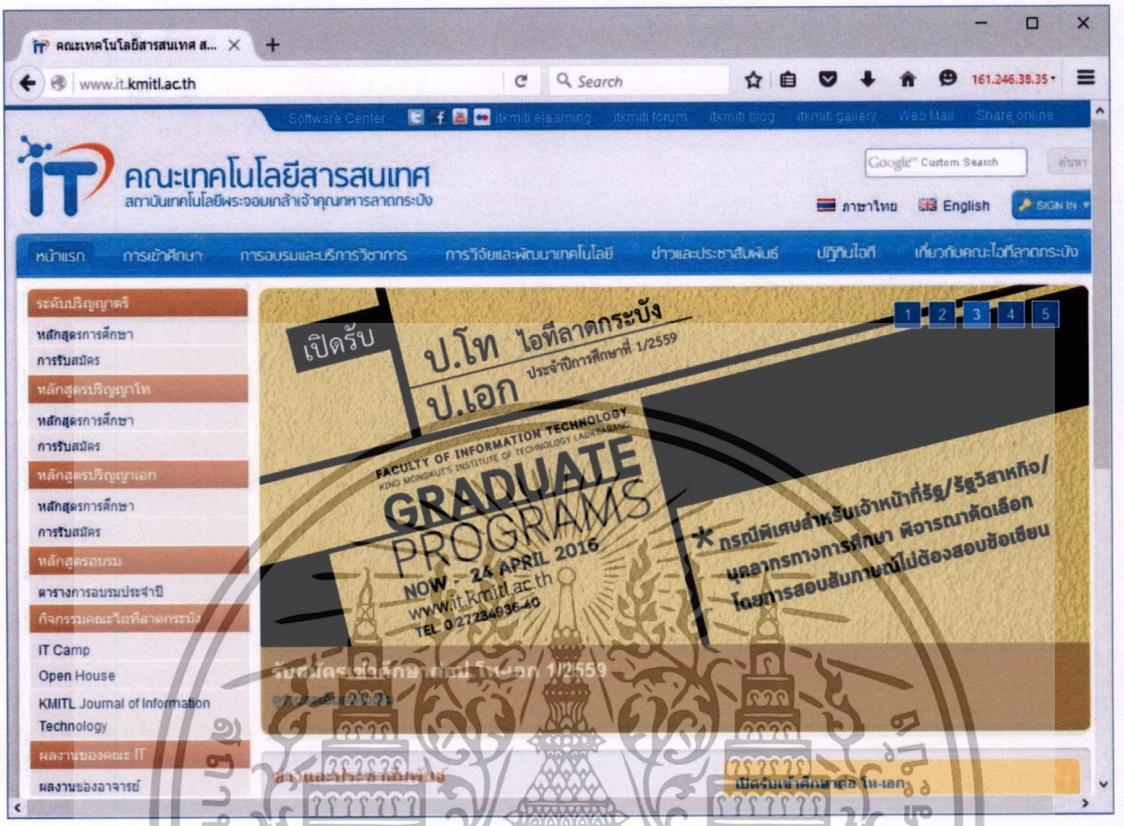
5.3.2 ทดสอบการเข้าเว็บไซต์ที่เป็น IPv4 Address



รูปที่ 5.7 การแปลงชื่อเป็น IPv4 Address

ทำการทดสอบโดยการเว็บไซต์ที่มี IPv4 Address เท่านั้น เช่น www.it.kmitl.ac.th จากรูปที่ 5.7 ทำการแปลงชื่อเป็น IP Address จะเห็นได้ว่าเว็บไซต์นี้มีการใช้งาน IPv4 Address เพียง

อย่างเดียว ซึ่งระบบยืนยันตัวตัวได้ทำการอนุญาต IPv4 Address ของเครื่องนี้แล้ว ทำให้สามารถออกไปใช้งานเว็บไซต์ www.it.kmilt.ac.th ซึ่งเป็นเว็บไซต์ภายนอกได้ ดังรูปที่ 5.8

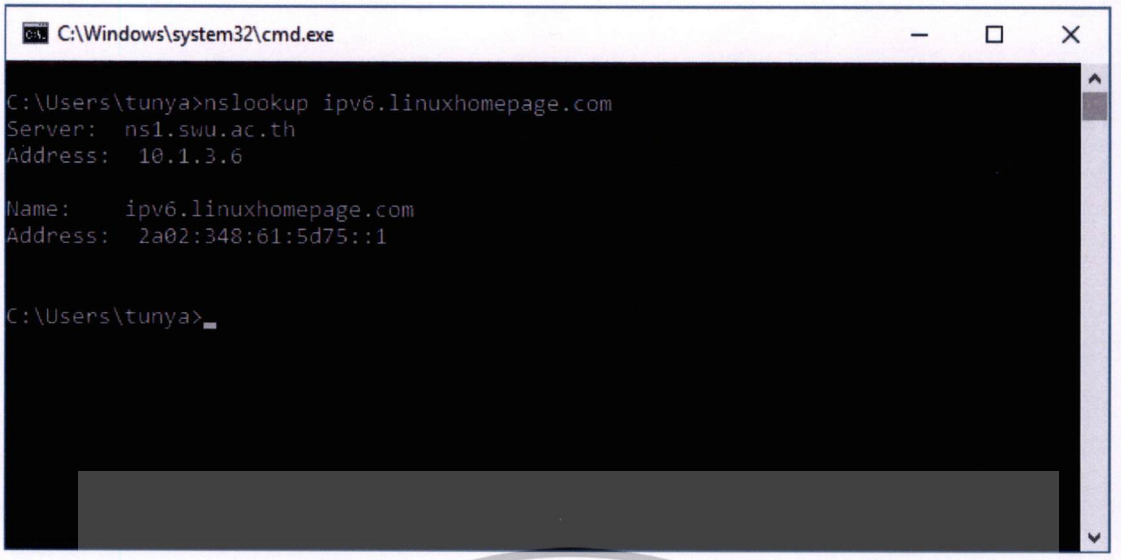


รูปที่ 5.8 หน้าจอแสดงการเข้าเว็บไซต์ด้วย IPv4 Address

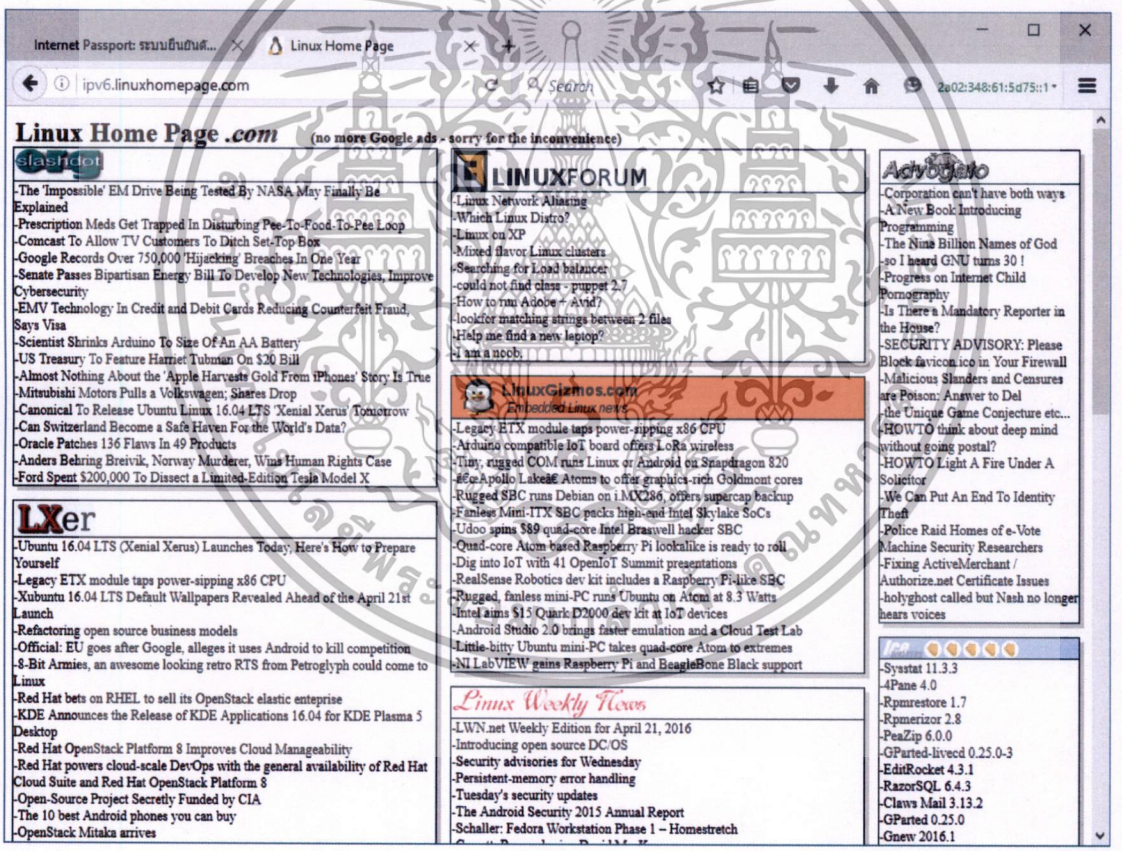
การตรวจสอบว่าขณะนั้นกำลังเข้าเว็บไซต์ที่เป็น IPv4 หรือ IPv6 Address สามารถทำได้โดยการติดตั้งส่วนขยาย (Extension) บนบราวเซอร์ เช่น Extension ชื่อ ShowIP บนบราวเซอร์ Firefox เป็นต้น

5.3.3 ทดสอบการเข้าเว็บไซต์ที่เป็น IPv6 Address เท่านั้น

ทำการทดสอบโดยการเข้าเว็บไซต์ http://ipv6.linuxhomepage.com ซึ่งเป็นเว็บไซต์ที่มีแต่ IPv6 Address เท่านั้น ดังรูปที่ 5.9 ผลปรากฏว่าสามารถใช้งานได้ตามปกติดังรูปที่ 5.10



รูปที่ 5.9 การแปลงชื่อเป็น IPv6 Address

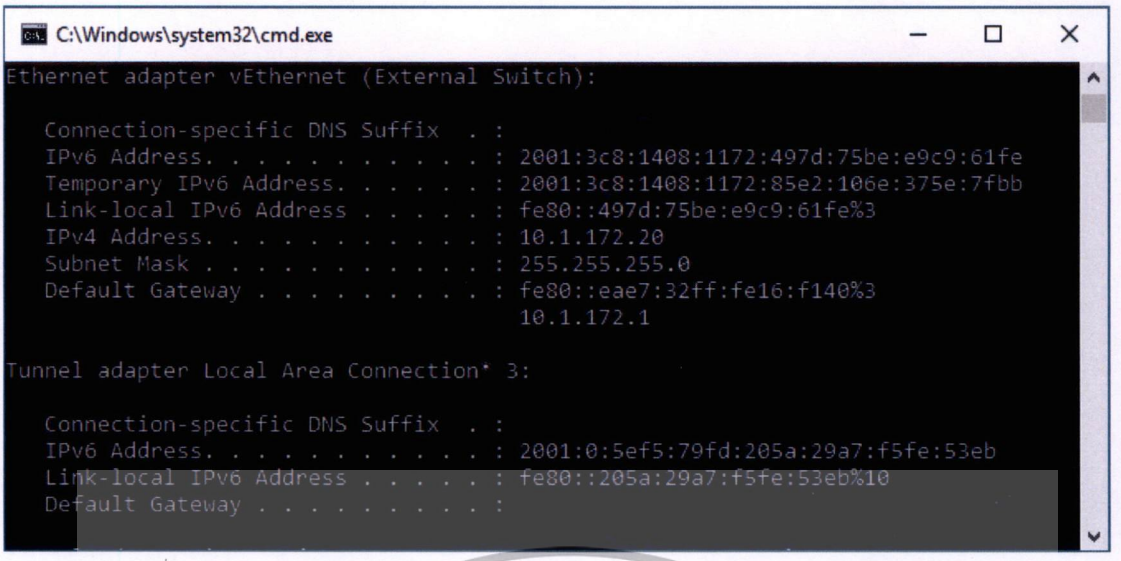


รูปที่ 5.10 หน้าจอแสดงการเข้าเว็บไซต์ที่เป็น IPv6 Address เท่านั้น

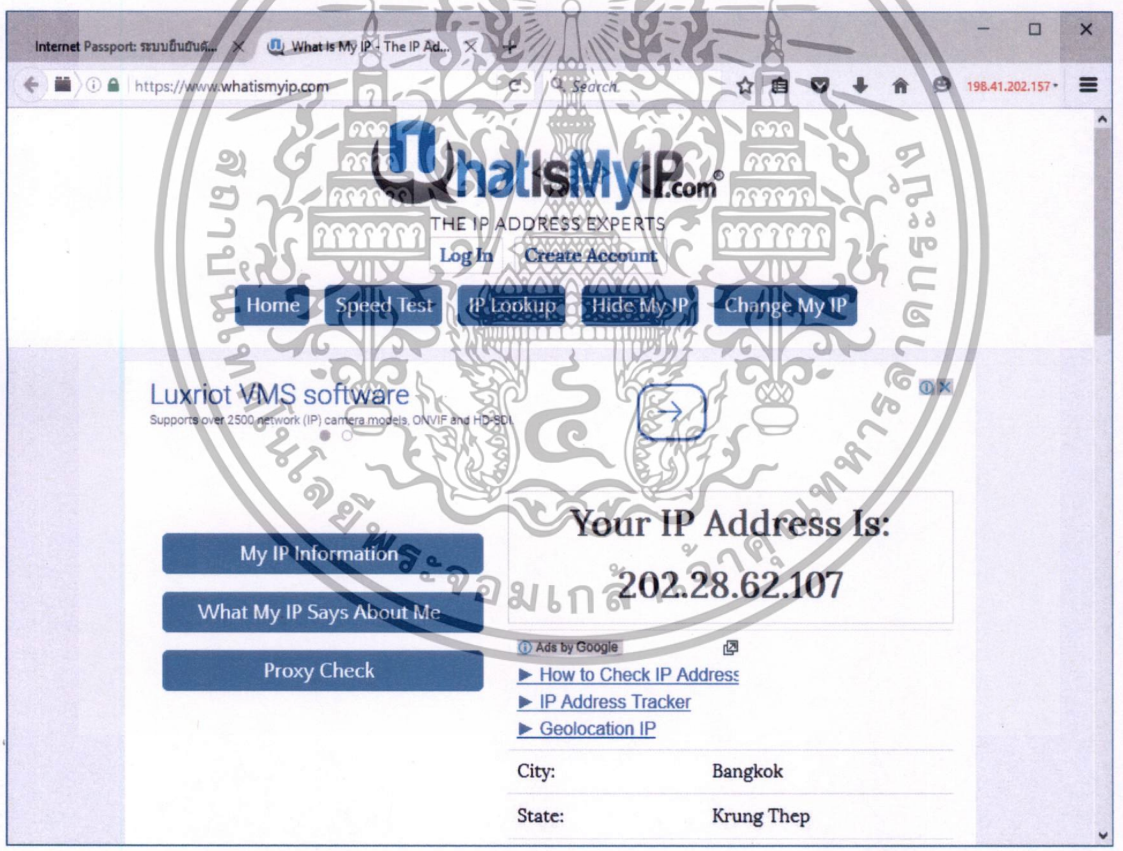
5.3.4 ทดสอบการเข้าเว็บไซต์ที่เป็น IPv4 และ IPv6 Address กรณี Temporary IPv6 Address เปลี่ยนระหว่างใช้งาน

เมื่อทำการ Log-in ระบบยืนยันตัวตนเรียบร้อยแล้ว ระบบจะทำการ Allow Rule บน Firewall ให้ IPv4 และ IPv6 Address ณ เวลานั้นของเครื่องไคลเอนต์ให้ออกอินเทอร์เน็ตได้ ดังรูปที่ 5.11 ในกรณีที่ Temporary IPv6 Address มีการเปลี่ยนแปลงระหว่างการใช้งานอินเทอร์เน็ต ดังรูปที่ 5.12 เครื่องไคลเอนต์จะทำการเปลี่ยนไปใช้ IPv4 Address เพื่อทำการออกอินเทอร์เน็ตแทน ดังรูปที่ 5.13 ทำให้สามารถใช้งานอินเทอร์เน็ตได้อย่างต่อเนื่อง และเมื่อครบกำหนดเวลา 30 นาที หรือกดปุ่ม Refresh ระบบจะทำการตรวจสอบการเปลี่ยนแปลงของ IPv6 Address หากพบว่ามีการเปลี่ยนแปลง จะทำการลบ IPv6 Address เก่า และ Allow ให้ IPv6 Address ใหม่นี้สามารถออกอินเทอร์เน็ต จากนั้นเมื่อได้รับการ Allow Rule แล้ว หากไปเว็บไซต์ที่เป็น IPv6 Address ก็จะสามารถใช้งาน IPv6 Address ได้ตามปกติ

รูปที่ 5.11 หน้าจอแสดง IP Address ของเครื่องไคลเอนต์ที่ Allow บน Firewall



รูปที่ 5.12 แสดง Temporary IPv6 Address ของเครื่องไคลเอนต์ที่มีการเปลี่ยนแปลง

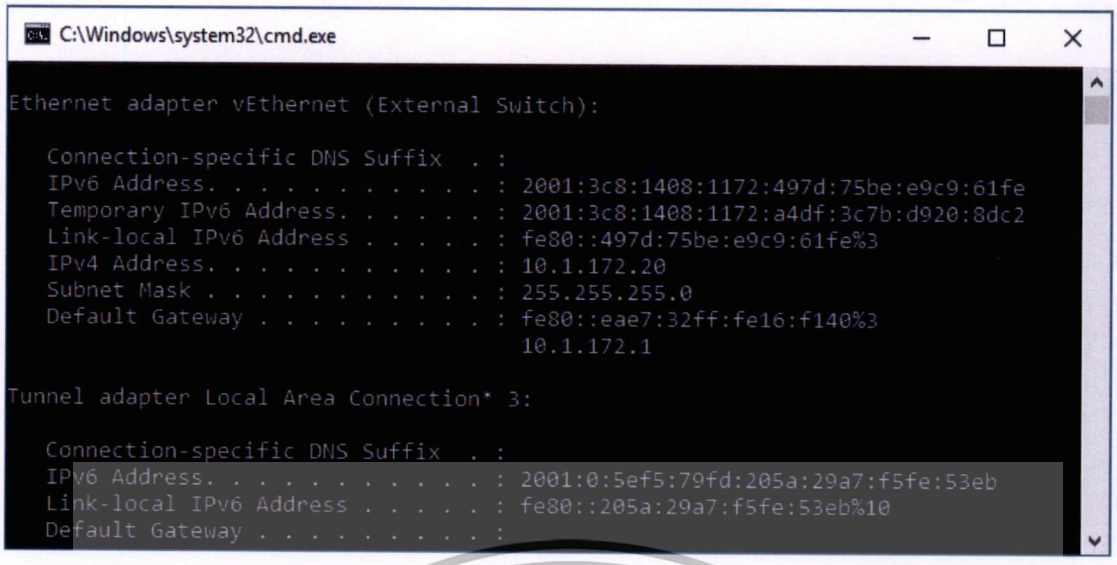


รูปที่ 5.13 แสดงการเข้าเว็บไซต์เมื่อ Temporaary IPv6 Address เปลี่ยนระหว่างใช้งาน

5.3.5 ทดสอบการเข้าเว็บไซต์ที่เป็น IPv6 Address เท่านั้น กรณี Temporary IPv6 Address เปลี่ยนระหว่างการใช้งาน

ทำการทดสอบโดยเข้าเว็บไซต์ที่เป็น IPv6 Address เพียงอย่างเดียวนั้น เช่น http://ipv6.linuxhomepage.com เมื่อมีทำการยืนยันตัวตนเรียบร้อยแล้ว ดังรูปที่ 5.14 หาก Temporary IPv6 Address เปลี่ยนระหว่างที่ใช้งาน ดังรูปที่ 5.15 จะส่งผลให้ไม่สามารถเข้าใช้เว็บไซต์ที่มี IPv6 Address เพียงอย่างเดียวได้ ดังรูปที่ 5.16 โดยจะสามารถกลับมาใช้งานได้เมื่อครบกำหนดเวลา 30 นาที หรือกดปุ่ม Refresh ที่ระบบจะทำการตรวจสอบการเปลี่ยนแปลงและปรับปรุง IPv6 Address ให้เป็นปัจจุบันอีกครั้ง

รูปที่ 5.14 หน้าจอแสดง IP Address ของเครื่องไคลเอนต์ที่ Allow บน Firewall



รูปที่ 5.15 แสดง Temporary IPv6 Address ของเครื่องไคลเอนต์ที่มีการเปลี่ยนแปลง

รูปที่ 5.16 หน้าจอแสดงการเข้าเว็บไซต์เมื่อ Temporary IPv6 Address เปลี่ยนระหว่างใช้งานเว็บไซต์ที่มีแต่ IPv6 Address เท่านั้น

5.4 การจัดเก็บข้อมูลผู้ใช้งาน (Log)

จากการติดตั้งระบบยืนยันตัวตน ทำให้สามารถจัดเก็บข้อมูลตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยมีการจัดเก็บข้อมูลของผู้ใช้งาน หมายเลข IPv4 Address และ IPv6 Address ซึ่งการจัดเก็บข้อมูลตาม พรบ.คอมพิวเตอร์ นั้นจะดำเนินการจัดเก็บที่ /var/log/masq.log โดยมีรูปแบบการจัดเก็บดังนี้

```
Fri Mar 11 10:05:51 2016 10.1.128.181:suwitta added
Fri Mar 11 10:05:53 2016 2001:3c8:1408:1189:d0d3:e5c3:ebed:5973:prisaha renewed
Fri Mar 11 10:05:54 2016 10.1.213.247:co571010367 added
Fri Mar 11 10:05:55 2016 2001:3c8:1408:1116:85c:9351:c89a:8f2:kamnug renewed
Fri Mar 11 10:05:55 2016 10.1.149.59:supkanate renewed
Fri Mar 11 10:05:59 2016 2001:3c8:1408:1196:f0d7:160c:a044:f143:janpensi renewed
Fri Mar 11 10:06:01 2016 2001:3c8:1408:1121:5918:d9b:f24f:14bf:patcharapornd renewed
Fri Mar 11 10:06:01 2016 2001:3c8:1408:1121:3820:8c31:7864:5fc1:siripatc renewed
Fri Mar 11 10:06:01 2016 removing IPv6 2001:3c8:1408:1189:5d7b:882b:99d6:ff1f
Fri Mar 11 10:06:01 2016 removing IPv4 10.44.10.208
Fri Mar 11 10:06:02 2016 10.1.111.56: onchuma added
Fri Mar 11 10:06:04 2016 2001:3c8:1408:1121:705e:e371:8900:67b3:thatsaporn renewed
Fri Mar 11 10:06:05 2016 2001:3c8:1408:1121:4c07:c33f:8fc5:e2d8:Niponr renewed
Fri Mar 11 10:06:05 2016 10.44.10.242:narisarawo renewed
Fri Mar 11 10:06:05 2016 2001:3c8:1408:1116:b073:17a2:7be2:e3cf:nipatpu renewed
Fri Mar 11 10:06:06 2016 2001:3c8:1408:1115:a96e:2118:ca9:d7b2:supatrak renewed
Fri Mar 11 10:06:07 2016 2001:3c8:1408:1121:202b:6638:105d:1767:sirikuns renewed
Fri Mar 11 10:06:11 2016 2001:3c8:1408:1117:8d1b:e019:b97a:760b:phapada renewed
```

```
Fri Mar 11 10:06:12 2016 2001:3c8:1408:1138:418e:e811:c1e7:e021:anchalej renewed

Fri Mar 11 10:06:12 2016 removing IPv4 10.44.5.65

Fri Mar 11 10:06:12 2016 removing IPv4 10.44.5.169

Fri Mar 11 10:06:15 2016 2001:3c8:1408:1170:ec19:7014:262:f5c0:ss551010670 renewed

Fri Mar 11 10:06:17 2016 2001:3c8:1408:1121:549b:872c:628b:9993:nilobonm renewed

Fri Mar 11 10:06:18 2016 2001:3c8:1408:1117:1506:f1bf:bcad:26b7:natthaya renewed

Fri Mar 11 10:06:21 2016 2001:3c8:1408:1184:8405:3626:6f44:973c:guest240 renewed

Fri Mar 11 10:06:21 2016 2001:3c8:1408:1121:983b:7b53:bdbd:9667:thitapha renewed

Fri Mar 11 10:06:22 2016 2001:3c8:1408:1121:a072:266e:b91d:4b79:koshwaris renewed

Fri Mar 11 10:06:23 2016 removing IPv4 10.1.13.57

Fri Mar 11 10:06:23 2016 removing IPv4 10.1.184.26

Fri Mar 11 10:06:24 2016 2001:3c8:1408:1113:8d89:11da:443c:84a3:ss551010880 logout

Fri Mar 11 10:06:24 2016 removing IPv6 2001:3c8:1408:1113:8d89:11da:443c:84a3

Fri Mar 11 10:06:24 2016 10.1.113.124:ss551010880 logout

Fri Mar 11 10:06:24 2016 removing IPv4 10.1.113.124
```

จากตัวอย่างจะเห็นว่ามีข้อมูลที่ประกอบไปด้วย วัน เดือน วันที่ เวลา ปี IPv4 Address หรือ IPv6 Address เครื่องหมาย ":" รหัสผู้ใช้ และ Action ซึ่งในส่วนของ Action นั้นจะมีอยู่ 3 รูปแบบ คือ added renewed และ logout

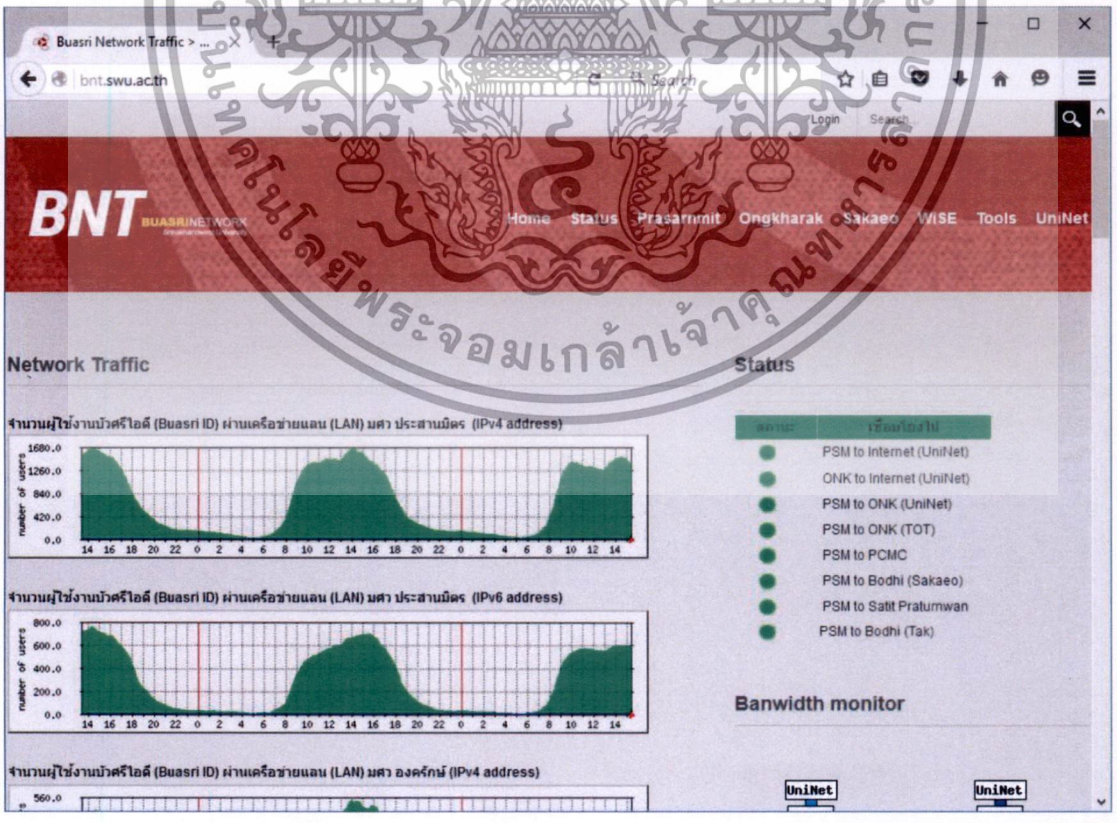
เมื่อทำการ login ระบบจะทำการบันทึกข้อมูลข้างต้น โดย Action จะเป็น "added" กรณีที่ login เข้ามาและยังไม่หมดเวลาแต่ต้องการต่อเวลาโดยการกดปุ่ม Refresh ระบบจะบันทึก Action ว่าเป็น "renewed" ในกรณีที่มีการกดปุ่ม Logout ระบบจะบันทึก Action ว่า "logout" และทำการบันทึก Log ให้ด้วยว่า "Removing IPv4" และ "Removing IPv6" ขึ้นอยู่กับเครื่องนั้นว่ามี IPv6 Address หรือไม่ซึ่งถ้าเครื่องไคลเอนต์มีหมายเลข IPv6 Address ก็จะทำการลบทั้ง IPv4 Address และ IPv6

Address ออกจาก Rule ของไฟร์วอล หรือในกรณีที่ผู้ใช้ไม่ได้ทำการกดปุ่ม Logout แต่มีการใช้งานจนครบ 2 ชั่วโมงระบบก็จะทำการ Removing IPv4 และ IPv6 Address ออกจากระบบเช่นกัน

5.5 การจัดเก็บสถิติข้อมูลการใช้งาน

การจัดเก็บข้อมูลสถิติการใช้งานตามช่วงเวลา ซึ่งการจัดเก็บข้อมูลตามช่วงเวลานั้น ได้มีการใช้งานโปรแกรม Mrtg ซึ่งเป็นโปรแกรมที่ใช้ในการจัดเก็บข้อมูลตามช่วงเวลา แต่โดยทั่วไปของโปรแกรม Mrtg นั้นส่วนใหญ่จะดำเนินการจัดเก็บแบนด์วิดท์ หรือปริมาณการเข้าออกของข้อมูล แต่ในที่นี้ระบบต้องการที่จะนำโปรแกรม Mrtg มาประยุกต์ โดยทำการปรับปรุงระบบ Mrtg โดยเขียนโปรแกรมเพื่อตรวจสอบข้อมูลปริมาณการใช้งานของผู้ใช้ โดยทำการนับจำนวนผู้ใช้งาน IPv4 และ IPv6 Address ทุกๆ 5 นาทีจากระบบ I-Pass แล้วส่งค่าไปยังระบบ Mrtg เพื่อนำมาสร้างกราฟแสดงจำนวนผู้ใช้งานในรูปแบบกราฟิก

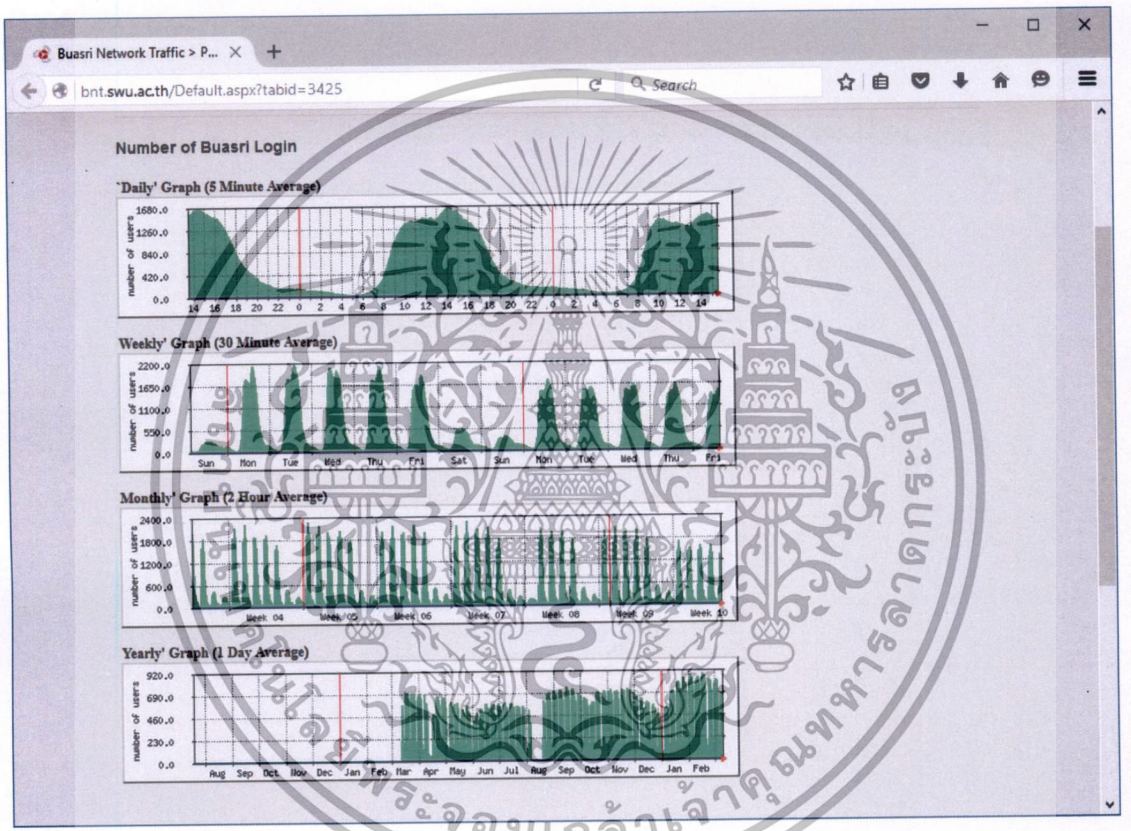
โดยรูปแบบของกราฟจะแสดงจำนวนผู้ใช้งาน IPv4 Address และ IPv6 Address จากรูปที่ 5.8 จะเห็นว่า ณ เวลาหนึ่งจำนวนผู้ใช้งานภายในมหาวิทยาลัยจะมีจำนวนผู้ใช้งาน IPv4 Address มากกว่า IPv6 Address ซึ่งเป็นเพราะการใช้งาน IPv6 Address นั้นจะสามารถใช้งานได้ก็ต่อเมื่อเครื่องไคลเอนต์นั้นรองรับการใช้งาน IPv6 ด้วยเท่านั้น



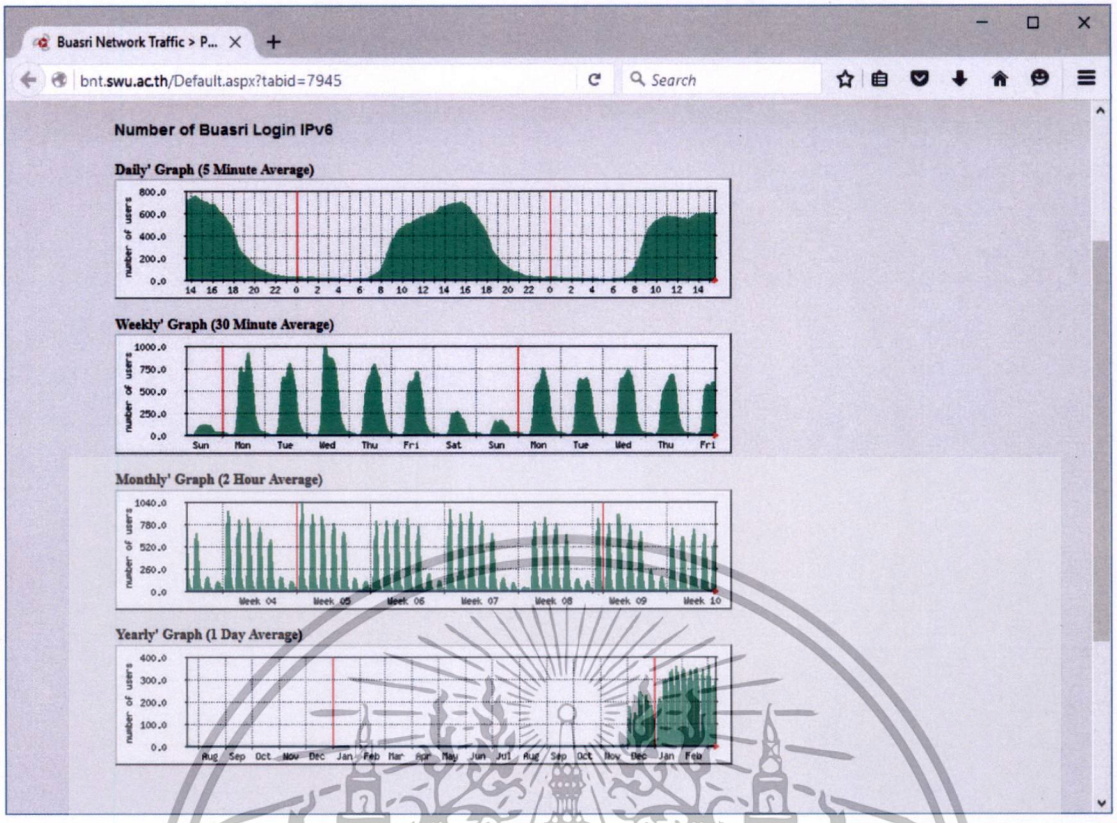
รูปที่ 5.17 หน้าจอแสดงจำนวนผู้ใช้งานระบบยืนยันตัวตนรายชั่วโมง

ซึ่งผู้ใช้งานที่มีทั้ง IPv4 และ IPv6 Address นั้นมีประมาณ 50% นอกนั้นจะเป็น IPv4 only ซึ่งในอนาคต เมื่อเครื่องไคลเอนต์รองรับ IPv6 Address มากขึ้นก็จะทำให้จำนวนผู้ใช้งานระบบยืนยันตัวตนทั้ง IPv4 และ IPv6 มีค่าใกล้เคียงกันหรือเท่ากัน

เมื่อทำการกดที่กราฟแสดงจำนวนผู้ใช้งาน IPv4 Address จะนำมาที่หน้าเว็บไซต์ดังรูปที่ 5.9 ซึ่งจะแสดงจำนวนการ Login ด้วย IPv4 Address ของมหาวิทยาลัยตามช่วงเวลา ซึ่งจะประกอบด้วยปริมาณการ Login รายวัน รายสัปดาห์ รายเดือน และ รายปี



รูปที่ 5.18 กราฟแสดงปริมาณการใช้งานระบบยืนยันตัวตนด้วย IPv4 Address



รูปที่ 5.19 กราฟแสดงปริมาณการใช้งานระบบยืนยันตัวตนด้วย IPv6 Address

จากรูปที่ 5.8 เมื่อทำการกดที่กราฟแสดงจำนวนผู้ใช้งานระบบยืนยันตัวตนด้วย IPv6 Address จะปรากฏหน้าจอดังภาพที่ 5.10 ซึ่งจะแสดงถึงจำนวนผู้ใช้งานด้วย IPv6 Address ของมหาวิทยาลัย ตามช่วงเวลา ซึ่งจะประกอบด้วย ปริมาณการ Login รายวัน รายสัปดาห์ รายเดือน และ รายปี จาก กราฟของ IPv6 จะสอดคล้องกับการ Login ด้วย IPv4 แต่จำนวนเครื่องที่ Login ด้วย IPv6 Address จะมีจำนวนที่น้อยกว่า IPv4 Address

บทที่ 6

สรุปผลการดำเนินงานและข้อเสนอแนะ

6.1 สรุปผลการวิเคราะห์และออกแบบ

จากการดำเนินการทดลองใช้งานระบบยืนยันตัวตนบนระบบเครือข่ายแบบ Dual-Stack ผ่านเว็บบราวเซอร์แล้วนั้น ทำให้สามารถแก้ปัญหาเรื่องการจัดเก็บข้อมูลตาม "พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550" ได้เป็นผลสำเร็จ โดยการจัดเก็บข้อมูลผู้ใช้ หมายเลข IPv4 Address และ IPv6 Address ในแต่ละช่วงเวลาบันทึกลงในล็อกไฟล์ได้ ระบบนี้สามารถแก้ปัญหาเรื่องการใช้งานเครื่องไคลเอนต์ที่มีการใช้งาน IPv4 Address และ IPv6 Address แบบ Dual Stack ได้ เพราะสามารถจัดเก็บข้อมูล IPv4 และ IPv6 Address ได้พร้อมกัน รวมถึงได้มีการแก้ปัญหาหลักของการใช้งาน IPv6 บนเครื่องไคลเอนต์ที่ Temporary IPv6 Address มีการเปลี่ยนแปลง ซึ่งระบบสามารถทำการ Login เพียงครั้งเดียว แล้วจัดการจัดเก็บ IPv6 Address ที่มีการเปลี่ยนแปลงได้แบบอัตโนมัติ โดยที่ผู้ใช้ไม่ต้องยุ่งยากในการ Log In หลายครั้งเมื่อระบบมีการเปลี่ยนแปลง Temporary IPv6 Address นอกจากการแก้ปัญหาต่างๆข้างต้นแล้ว ระบบยังสามารถแก้ปัญหาการใช้งานชื่อผู้ใช้งาน 1 คนแต่มีการ Log In หลายเครื่อง เนื่องจากระบบได้มีการตั้งค่ากำหนดจำนวนเครื่องที่สามารถใช้งานพร้อมกันได้ ทำให้ผู้ใช้งานมีความปลอดภัยมากยิ่งขึ้น ลดปัญหาการแจกจ่ายชื่อผู้ใช้งาน และรหัสผ่าน ให้กับคนอื่น เนื่องจากระบบจะทำการจำกัดการใช้งานได้เพียง 2 เครื่องต่อ 1 ชื่อผู้ใช้งานเท่านั้น

6.2 ปัญหาและข้อจำกัด

1) ระบบระบบยืนยันตัวตนบนระบบเครือข่ายแบบ Dual-Stack ผ่านเว็บบราวเซอร์เป็นระบบที่ต้องนำมาวางขวางในระบบเครือข่าย ซึ่งจะต้องวางระหว่าง Layer 3 Switch กับ Firewall ในกรณีนี้ถ้าระบบยืนยันตัวตนมีปัญหาก็จะทำให้เกิด Single point of failure ทำให้ไม่สามารถใช้งานได้ ซึ่งปัญหานี้ในเบื้องต้นได้มีการแก้ปัญหาแล้วในโครงงานนี้ โดยทำการตั้งค่าให้ระบบยืนยันตัวตนเป็น Bridge ซึ่งจะไม่มี IP Address ดังนั้นถ้าระบบมีปัญหาก็สามารถนำระบบนี้ออก แล้วนำสายจาก Layer3 Switch ต่อเข้าโดยตรงกับ Firewall โดยไม่ต้องทำการเปลี่ยนแปลงค่าใดๆ

2) การใช้งานบนระบบปฏิบัติการ MacOS และ iOS โดยเชื่อมต่ออินเทอร์เน็ตผ่านระบบเครือข่ายไร้สาย (Wireless) หากไม่ทำการปิด Auto-Login ของ WiFi จะมี Pop-up แสดงหน้าจอระบบยืนยันตัวตนขึ้นมาให้ทำการ Login ซึ่งหน้าต่างนี้จะไม่สามารถย่อและขยายได้

3) กรณีที่เครื่องไคลเอนต์ได้ทำการยืนยันตัวตนแล้ว ซึ่งหมายถึง IPv4 และ IPv6 Address ได้รับอนุญาตให้ออกอินเทอร์เน็ตได้ เมื่อเข้าเว็บไซต์ที่เป็น IPv6 Address เพียงอย่างเดียว จะสามารถเข้าใช้งานได้ แต่เมื่อมีการเปลี่ยน Temporary IPv6 Address ในระหว่างที่ใช้งานอยู่นั้น จะไม่สามารถเข้าเว็บไซต์ที่เป็น IPv6 Address เพียงอย่างเดียวได้ เนื่องจาก IPv6 Address ใหม่นี้ ยังไม่ได้รับการอนุญาตบนไฟร์วอลให้ออกสู่อินเทอร์เน็ตได้ และด้วยเว็บไซต์ไม่มี IPv4 Address ทำให้ไม่สามารถเปลี่ยนไปใช้ IPv4 Address ของเครื่องไคลเอนต์ได้ โดยจะสามารถเข้าใช้งานได้ก็ต่อเมื่อมีการกดปุ่ม Refresh ที่หน้าจอนับเวลาของระบบ หรือเมื่อครบกำหนด 30 นาทีตามที่ได้ตั้งไว้

4) กรณีที่เครื่องไคลเอนต์ภายในมหาวิทยาลัยมีจำนวนเพิ่มมากขึ้น และมีความต้องการใช้งานพร้อมๆกัน (Concurrent) เป็นจำนวนมาก อาจจะต้องมีการเพิ่มขนาดของเครื่องคอมพิวเตอร์แม่ข่ายให้ใหญ่ขึ้น หรือมีทรัพยากร เช่น CPU Memory ที่มากขึ้น

6.3 ข้อเสนอแนะ

จากผลการดำเนินการสังเกตุเห็นว่าระบบนั้นมีการใช้งาน Memory ค่อนข้างมาก ประกอบกับถ้านำระบบนี้ทำการจัดเก็บข้อมูล Traffic log ด้วยจะต้องมี IO ที่มี IOPS (Input/Output Operation Per Second) มากขึ้น ซึ่งอาจจะต้องทำการเชื่อมต่อกับ Storage ที่รองรับการใช้งานที่มี IOPS สูงหรือติดตั้งบนเครื่องที่มีฮาร์ดดิสก์เป็นแบบ SSD (Solid State Disk) เพื่อให้ระบบสามารถทำงานได้ไม่ติดขัด ในส่วนของระบบยืนยันตัวตนนั้น กรณีที่มีผู้ใช้งานเป็นจำนวนมาก ซึ่งอาจจะทำให้เกิดปัญหาทรัพยากรไม่เพียงพอ หากสามารถเพิ่มขนาดของเครื่องแม่ข่ายได้ก็จะช่วยแก้ปัญหาได้ แต่หากเพิ่มขนาดของเครื่องแม่ข่ายแล้วระบบยังไม่สามารถรองรับกับปริมาณการใช้งานได้ อาจจะต้องมีการติดตั้ง Load balance web server ที่ทำหน้าที่เป็น Reverse proxy เพื่อทำการกระจายงานมาที่หน้า Captive Portal เมื่อทำการ Login เสร็จเรียบร้อย จึงทำการส่งมาให้กับเครื่องที่ทำหน้าที่เป็น Firewall ในการอนุญาตให้ใช้งาน หรือหากดำเนินการเพิ่มในส่วนของ Captive portal แล้วยังไม่สามารถรองรับได้ก็อาจจะต้องทำการตรวจสอบที่เครื่อง Firewall ว่าสามารถรองรับได้หรือไม่ ถ้าไม่สามารถรองรับได้ ควรจะทำการแยกเครือข่ายออกมา แล้วแบ่งเครือข่ายว่าเครือข่ายนี้จะดำเนินการออกผ่านระบบยืนยันตัวตนเครื่องไหน ซึ่งอาจจะมีหลาย Firewall หลาย Captive Portal ในกระบวนการแยกนี้อาจจะนำเรื่องของ Source routing เข้ามาช่วยในการแก้ปัญหาเพื่อกระจายงานให้สามารถรองรับกับผู้ใช้ในปริมาณมากๆได้

ระบบนี้เป็นเพียงระบบเพื่อใช้ในการยืนยันตัวตนและจัดเก็บข้อมูลการยืนยันตัวตน โดยทำการจับคู่รหัสผู้ใช้งานกับ IP Address เท่านั้น ซึ่งไม่สามารถป้องกันการปลอมแปลง IP Address ได้

หากต้องการเพิ่มความปลอดภัยของระบบเครือข่ายให้มากขึ้น เห็นควรที่จะมีการพัฒนาให้มีการตรวจสอบการปลอมแปลง IP Address ต่อไป

บรรณานุกรม

โกสัลล์ ถีถะแก้ว. 2556. **"การเปรียบเทียบประสิทธิภาพ ไอพีวีซิกส์ทรานซิชัน."** สารนิพนธ์วิทยาศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมเครือข่าย คณะวิทยาการและเทคโนโลยีสารสนเทศ, มหาวิทยาลัยเทคโนโลยีมหานคร.

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. 2557. **ความรู้ IPv6 พื้นฐานสำหรับผู้ดูแลระบบ Basic IPv6 for System Administrators**. [ออนไลน์]. เข้าถึงได้จาก: http://www.thailandipv6.net/ebook/IPv6book20140826.pdf.

Butcher, M. 2007. **Mastering OpenLDAP**. [Ebook]. UK: Packt Publishing Ltd.

Carter, G. 2003. **LDAP System Administration**. [Ebook]. USA: O'Reilly Media.

Cicileo,G. 2015. **Transition Mechanism**. [Online]. Available: http://portalipv6.lacnic.net/en/transition-mechanisms.

Cisco. 2015. **IPv6 Configuration Guide, Cisco IOS Release 15.2M&T**. [Online]. Available: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-15-2mt-book/ip6-neighb-disc.html.

Gheorghe, L. 2006. **Designing and Implementing Linux Firewalls and QoS using netfilter, iproute2, NAT, and L7-filter**. [Ebook]. UK: Packt Publishing Ltd.

Gregor, N, P. 2005. **Linux iptables Pocket Reference**. [Ebook]. USA: O'Reilly Media.

H3C Technologies. 2015. **Tunneling Introduction**. [Online]. Available: http://www.h3c.com/portal/Products___Solutions/Technology/IPv4___IPv6_Services/Technology_Introduction/200702/201180_57_0.htm.

Hagen, S. 2006. **IPv6 Essentials**. [Ebook]. USA: O'Reilly Media.

Maglione, R and Moriondo, C. 2015. **IPv6 Transition Mechanisms**. [Online]. Available: http://www.ngnet.it/e/trans1.

บรรณานุกรม (ต่อ)

Microsoft Corporation. 2015. **IPv6 Concept**. [Online]. Available: https://technet.microsoft.com/en-us/library/cc778502%28v=ws.10%29.aspx.

Rash, M. 2007. **Linux Firewalls**. [Ebook]. USA: William Pollock.

Rouse, M. 2016. **Captive Portal**. [Online]. Available: http://searchmobilecomputing.techtarget.com/definition/captive-portal.

Rouse, M. 2016. **Log (Log file)**. [Online]. Available: http://whatis.techtarget.com/definition/log-log-file.

Untangle, Inc. 2016. **Captive Portal**. [Online]. Available: https://www.untangle.com/shop/captive-portal.

ประวัติผู้เขียน

ชื่อผู้เขียน	นางสาวธัญย์ธรฐ์ พงษ์เฉลิม
วันเดือนปีเกิด	15 กุมภาพันธ์ 2531
สถานที่เกิด	กรุงเทพมหานคร
วุฒิการศึกษาระดับปริญญาตรี	วิทยาศาสตรบัณฑิต (วิทยาการคอมพิวเตอร์)
สถานที่สำเร็จการศึกษา	มหาวิทยาลัยศรีนครินทรวิโรฒ
ปีการศึกษา	2553
การทำงาน	นักวิชาการคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ