กรณีศึกษาการติดตั้ง IPv6 ภายในคณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

CASE STUDY OF IMPLEMENT IPv6 IN FACULTY OF INFORMATION TECHNOLOGY KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

โดย

ปาลิน รัตนพันธ์

PALIN RATTANAPAN

อาจารย์ที่ปรึกษา

รศ.ดร.โชติพัชร์ ภรณวลัย

รายงานนี้เป็นส่วนหนึ่งของวิชาการศึกษาอิสระ 2
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ภาคเรียนที่ 2 ปีการศึกษา 2554

CASE STUDY OF IMPLEMENT IPv6
IN FACULTY OF INFORMATION TECHNOLOGY
KING MONGKUT'S INSTITUTE
OF TECHNOLOGY LADKRABANG

PALIN RATTANAPAN

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/ 2011

หัวข้อ	กรณีศึกษาการติดตั้ง IPv6 ภายในคณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
นักศึกษา	นางสาวปาลิน รัตนพันธ์
รหัสนักศึกษา	52660532
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
แขนงวิชา	เทคโนโลยีระบบสารสนเทศ
ปีการศึกษา	2554
อาจารย์ที่ปรึกษา	รศ.ดร.โชติพัชร์ ภรณวลัย

บทคัดย่อ

กลไกการทำงานของอินเทอร์เน็ตที่สำคัญ คือ อินเทอร์เน็ตโพรโทคอล ทำหน้าที่จัดการเกี่ยวกับเลขที่อยู่ ซึ่งใช้ในการอ้างอิงเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายในการติดต่อสื่อสารกัน ปัจจุบันการขยายขนาดของเครือข่ายอินเทอร์เน็ตเป็นไปอย่างรวดเร็ว ทำให้จำนวนเลขที่อยู่ลดลง โดยปัจจุบันอินเทอร์เน็ตโพรโทคอลที่ใช้งานเป็นรุ่นที่ 4 (IPV4) กรณีศึกษานี้เสนอการติดตั้งอินเทอร์เน็ตโพรโทคอลรุ่นที่ 6 (IPv6) ภายในคณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ซึ่ง IPv6 ได้รับการออกแบบมาเพื่อรองรับปริมาณการใช้อินเทอร์เน็ตที่เพิ่มมากขึ้นในอนาคต รวมทั้งยังมีการปรับปรุงคุณลักษณะของโพรโทคอล ทั้งในด้านประสิทธิภาพและความปลอดภัยรองรับระบบแอปพลิเคชั่นใหม่ กรณีศึกษานี้นำเสนอวิธีการติดตั้ง IPv6 ให้สามารถทำงานร่วมกับเครือข่าย IPv4 ปัจจุบันและรองรับการทำงานร่วมกับเครือข่าย IPv6 ในอนาคตได้

Title	Case Study of Implement IPv6 In Faculty of Information Technology. King Mongkut's Institute of Technology Ladkrabung.
Student	Ms. Palin Rattanapan
Student ID.	52660532
Degree	Master of Science
Program	Information Technology
Major	Information System Technology
Academic Year	2011
Advisor	Assoc. Dr. Chotipat Pornwalai

ABSTRACT

The main mechanism behind the internet is the internet protocol (IP). It manages the address of the computers and network devices and allow them to communicate with each other. Nowadays the expansion of the internet is still rapidly increasing, therefore, the amount of available addresses is decreasing. At the moment, the internet protocol in used is an IPV4 (IP version 4). This case study detail how to put in use the IPV6 (IP version 6) in Faculty of Information Technology. King Mongkut's Institute of Technology Ladkrabung. IPV6 is designed to provided more addresses than IPV4, ensuring the availability of internet addresses in the future (even at the current rate of increase). In addition, it enhances the quality of the protocols both in efficiency and security as well as ensure the compatibility with new applications. This case study details how to install the IPV6 along the IPV4 and how to have them work smoothly with each other, as well as how to switch to a full IPV6 network in the future.

กิตติกรรมประกาศ

รายงานวิชาการศึกษาค้นคว้าอิสระ2 ฉบับนี้สำเร็จด้วยความอนุเคราะห์จากบุคคลหลายท่าน ซึ่งไม่สามารถนำมากล่าวได้ทั้งหมด ซึ่งผู้มีพระคุณท่านแรกที่ข้าพเจ้าใคร่ขอกราบขอบพระคุณคือ รศ.ดร. โชติพัชร์ ภรณวลัย ซึ่งเป็นอาจารย์ที่ปรึกษาวิชาการศึกษาอิสระ2 อาจารย์ผู้สอนที่ได้ให้ความรู้ คำแนะนำตรวจทาน และแก้ไขจุดบกพร่องต่างๆ ด้วยความเอาใจใส่ทุกขั้นตอนเพื่อให้การทำรายงานวิชาการศึกษาค้นคว้าอิสระ2 ฉบับนี้สมบูรณ์ที่สุด นอกจากนี้ข้าพเจ้าใคร่ขอกราบขอบพระคุณเจ้าหน้าที่และน้องนักศึกษาปริญญาตรี ที่ช่วยสนับสนุนและให้ข้อมูลส่งผลให้การทำงานราบรื่น ขอขอบคุณบริษัททริปเปิลทีบรอดแบนด์ในการสนับสนุนการทดสอบโครงการนี้ ขอขอบคุณคณาจารย์ คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังทุกท่านที่ได้ประสิทธิ์ประสาทวิชาให้แก่ข้าพเจ้า ขอบคุณเพื่อนร่วมรุ่นทุกท่านที่ช่วยเป็นกำลังใจในการศึกษา การทำงาน รวมถึงให้คำปรึกษาด้านต่างๆด้วยดีเสมอมา ขอขอบคุณเจ้าหน้าที่บัณฑิตศึกษา และเจ้าหน้าที่บัณฑิตวิทยาลัย รวมถึงเจ้าหน้าที่คณะเทคโนโลยีสารสนเทศที่ให้ความช่วยเหลือ ในเรื่องต่างๆด้วยดีเสมอมา สุดท้ายนี้ขอกล่าวขอบพระคุณบิดา มารดา ญาติพี่น้องของข้าพเจ้าที่คอยเป็นกำลังใจและสนับสนุนการตัดสินใจที่ดีของข้าพเจ้าเสมอมา ทำให้ข้าพเจ้าสามารถพัฒนาโครงการนี้สำเร็จลุล่วงไปด้วยดี

ปาลิน รัตนพันธ์

สารบัญ

หน้า

สารบัญ(ต่อ)

หน้า

สารบัญตาราง

ตารางที่ หน้า

สารบัญรูป

รูปที่ หน้า

สารบัญรูป(ต่อ)

รูปที่ หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันอินเทอร์เน็ตมีบทบาทสำคัญในการเชื่อมต่อกับเครือข่าย และยังมีเทคโนโลยีอีกมากมายที่จำเป็นต้องใช้อินเทอร์เน็ตในการเชื่อมต่อถึงกัน คอมพิวเตอร์และอุปกรณ์เครือข่ายจำเป็นต้องมีเลขที่อยู่เพื่อใช้ในการติดต่อสื่อสารระหว่างเครือข่าย โพรโทคอลอินเทอร์เน็ต เป็นเกณฑ์วิธีในการส่งข้อมูลแบบดิจิทัล ในรูปแบบกลุ่มข้อมูล (Packet) ผ่านเครือข่ายอินเทอร์เน็ตโดยโพรโทคอลจะระบุอุปกรณ์ต้นทางและอุปกรณ์ปลายทางของข้อมูลที่ส่ง ในปัจจุบันโพรโทคอลอินเตอร์เน็ตที่ใช้อยู่จะเป็นรุ่นที่ 4 (IPv4) ซึ่งใช้เลขฐานสองจำนวน 32 บิตในการกำหนดเลขที่อยู่ ทำให้สามารถรองรับอุปกรณ์ได้ประมาณ 4 พันล้านเครื่อง การขยายตัวอย่างรวดเร็วของเครือข่ายอินเทอร์เน็ต ทำให้เลขที่อยู่ของ IPv4 จะมีไม่เพียงพอในอนาคตที่ไม่ไกลนัก จึงได้มีการกำหนดโพรโทคอลขึ้นใหม่เป็นรุ่นที่ 6 (IPv6) ซึ่งจะใช้เลขฐานสองจำนวน 128 บิตในการกำหนดเลขที่อยู่ เมื่อนำระบบ IPv6 มาใช้งานจะให้ทำให้สามารถกำหนดเลขที่อยู่ให้กับอุปกรณ์ได้มากขึ้น

อินเตอร์เน็ตโพรโทคอลรุ่นที่ 6 (IPv6) ได้รับการพัฒนาเพื่อปรับปรุงโครงสร้างของตัวโพรโทคอล ให้รองรับเลขที่อยู่จำนวนมากและปรับปรุงลักษณะอื่นๆอีกหลายประการ รวมถึงการปรับปรุงด้านประสิทธิภาพและความปลอดภัยรองรับระบบแอปพลิเคชันใหม่ๆที่จะเกิดขึ้นในอนาคต และยังเพิ่มประสิทธิภาพในการประมวลผลการรับส่งข้อมูล (Packet) ให้ดียิ่งขึ้น ทำให้สามารถตอบสนองต่อการขยายตัวและความต้องการใช้งานเทคโนโลยีบนเครือข่ายอินเทอร์เน็ตในอนาคต ปัจจุบันคณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง มีการใช้งานโพรโทคอลรุ่นที่ 4 (IPv4) ภายในคณะและการเชื่อมต่อเครือข่ายอินเทอร์เน็ต

จากปัญหาดังกล่าว ทำให้เกิดแนวคิดการนำเทคโนโลยีอินเทอร์เน็ตโพรโทคอล รุ่นที่ 6 (IPv6) มาติดตั้งให้สามารถทำงานร่วมกับเครือข่าย IPv4 ปัจจุบันและรองรับการทำงานร่วมกับเครือข่าย IPv6 ในอนาคตได้และเพิ่มประสิทธิภาพการทำงานและความปลอดภัยยิ่งขึ้น

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

กรณีศึกษาการติดตั้ง IPv6 ภายในคณะเทคโนโลยีสารสนเทศ มีวัตถุประสงค์ดังต่อไปนี้

1. เพื่อศึกษาการหลักการทำงานของโพรโทคอลรุ่นที่ 6 (IPv6)
2. เพื่อศึกษาและวิเคราะห์ปัญหาที่เกิดขึ้นภายใต้การทำงานของโพรโทตอลเดิม (IPv4)
3. เพื่อศึกษาการติดตั้งการใช้งานของโพรโทโคอลรุ่นที่ 6 (IPv6) ภายในคณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
4. เพื่อศึกษาการทำงานของโพรโทคอลรุ่นที่ 6 (IPv6) ร่วมกับเครือข่ายปัจจุบัน(IPv4)

1.3 ขอบเขตของการศึกษา

กรณีศึกษาการติดตั้ง IPv6 มีขอบเขตการศึกษาดังต่อไปนี้

1. ศึกษาการหลักการทำงานของโพรโทคอลรุ่นที่ 6 (IPv6) กับเครือข่ายปัจจุบัน ที่มีการใช้งานโพรโทคอลรุ่นที่ 4 (IPv4)
2. ศึกษาการหลักการทำงานของโพรโทคอลรุ่นที่ 6 (IPv6) กับเครือข่ายที่มีการใช้งาน IPv6 ด้วยกันเอง
3. ศึกษาระบบเครือข่ายเดิมของคณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
4. ติดตั้งและทดสอบการใช้งานโพรโทคอลรุ่นที่ 6 (IPv6) ภายในคณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

1.4 ขั้นตอนของการศึกษา

ประกอบด้วยขั้นตอนต่างๆ ดังนี้

1.4.1 ศึกษาความเป็นไปได้ในการติดตั้ง

ศึกษาระบบเครือข่ายภายในคณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง โดยศึกษาภาพรวมการติดตั้ง เชื่อมต่อภายในคณะและการเชื่อมต่อไปยังผู้ให้บริการอินเทอร์เน็ต รวมทั้งศึกษาอุปกรณ์เครือข่าย เช่น เร้าเตอร์ สวิตซ์ ที่มีการใช้งาน

ในปัจจุบัน ด้านความสามารถในการรองรับการทำงาน IPv6 เพื่อประกอบการวิเคราห์และออกแบบเครือข่ายใหม่ที่มีกำหนดให้มีการทำงาน IPv6

1.4.2 การวิเคราะห์และออกแบบ

ศึกษาระบบเครือข่ายปัจจุบัน ด้านการติดตั้งและการเชื่อมต่อ นำข้อมูลที่ได้มาทำการวิเคราะห์และออกแบบเครือข่ายใหม่ให้มีการใช้งาน IPv6 โดยทำการออกแบบเครือข่ายใหม่ให้สามารถทำงานร่วมกับอุปกรณ์เดิมที่มีอยู่แล้ว ในการออกแบบคำนึงถึงประสิทธิภาพการทำงานและต้นทุนในการติดตั้งเครือข่ายใหม่เป็นหลัก

1.4.3 การติดตั้งและทดสอบ

ทำการติดตั้งอุปกรณ์โดยกำหนดให้มีการใช้งาน IPv6 ภายในเครือข่ายที่ต้องการทำการทดสอบ โดยทำการทดสอบดังนี้

1. ทดสอบการใช้งานผ่านเครือข่ายที่ใช้ IPv6 ภายในคณะเทคโนโลยีสารสนเทศ
2. ทดสอบการใช้งานระหว่างเครือข่ายที่ใช้ IPv6 และ IPV4 ภายในคณะเทคโนโลยีสารสนเทศ
3. ทดสอบการใช้งานอินเทอร์เน็ตและทดสอบแอปพลิเคชันต่างๆ จากเครือข่ายที่ใช้ IPv6 ภายในคณะเทคโนโลยีสารสนเทศ ผ่านผู้ให้บริการอินเทอร์เน็ต (ISP)

1.4.4 การทดลองใช้งานและปรับปรุงแก้ไข

ทดสอบการใช้งานผ่านเครือข่ายที่ใช้ IPv6 ในการสื่อสารกับเครือข่าย IPv6 และ IPV4 และทำการปรับปรุงแก้ไข เพื่อเพิ่มประสิทธิภาพการทำงานและความปลอดภัยในการใช้งาน โดยทดลองใช้งานภายในคณะเทคโนโลยีสารสนเทศ และทดลองใช้งานอินเทอร์เน็ตผ่านผู้ให้บริการอินเทอร์เน็ต

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1. พัฒนาความรู้ความเข้าใจการทำงานโพรโทคอลรุ่นที่ 6 (IPv6)
2. พัฒนาความรู้ความเข้าใจในหลักการทำงานภายในเครือข่ายที่ใช้งาน IPv6
3. พัฒนาความรู้ความเข้าใจในหลักการทำงานระหว่างเครือข่ายที่ใช้งาน IPv6 และ IPv4
4. สามารถติดตั้งการใช้งาน IPv6 ภายในคณะเทคโนโลยีสารสนเทศให้สามารถใช้งานภายในเครือข่าย IPv6 ด้วยกันเองและสามารถใช้งานระหว่างเครือข่าย IPv4 เดิมได้
5. สามารถปรับปรุงเพิ่มประสิทธิภาพการทำงานและความปลอดภัยได้

บทที่ 2
ทฤษฎีพื้นฐานในการพัฒนา

2.1 Internet Protocol

Internet Protocol (IP) เป็นโพรโทคอลในระดับชั้นเครือข่าย ทำหน้าที่จัดการเกี่ยวกับเลขที่อยู่ (IP Address) และข้อมูล และควบคุมการส่งข้อมูลบางอย่างที่ใช้ในการหาเส้นทางของกลุ่มข้อมูล (Packet) ซึ่งกลไกในการหาเส้นทางของ IP จะมีความสามารถในการหาเส้นทางที่ดีที่สุด และสามารถเปลี่ยนแปลงเส้นทางได้ในระหว่างการส่งข้อมูล มีระบบการแยกและประกอบดาต้าแกรม (Datagram) เพื่อรองรับการส่งข้อมูลระดับชั้นเชื่อมโยงข้อมูล ที่มีขนาด MTU (Maximum Transmission Unit) ที่แตกต่างกัน ทำให้สามารถนำ IP ไปใช้บนโพรโทคอลอื่นได้หลากหลาย เช่น Ethernet , Token Ring หรือ Apple Talk

การเชื่อมต่อของ IP เพื่อทำการส่งข้อมูล จะเป็นแบบ Connectionless หรือเกิดเส้นทางการเชื่อมต่อในทุกๆครั้งของการส่งข้อมูล 1 ดาต้าแกรม โดยจะไม่ทราบถึงข้อมูลดาต้าแกรมที่ส่งก่อนหน้าหรือส่งตามมา แต่การส่งข้อมูลใน 1 ดาต้าแกรม อาจจะเกิดการส่งได้หลายครั้งในกรณีที่มีการแบ่งข้อมูลออกเป็นส่วนย่อยๆ (fragmentation) และถูกนำไปรวมเป็นดาต้าแกรมเดิมเมื่อถึงปลายทาง

กลไกสำคัญในการทำงานของอินเทอร์เน็ต คือ อินเทอร์เน็ตโพรโทคอล ส่วนประกอบสำคัญของอินเทอร์เน็ตโพรโทคอลได้แก่ เลขที่อยู่ (IP Address) สำหรับใช้ในการอ้างอิงเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายต่างๆ ปัจจุบันมีการใช้เลขที่อยู่บนมาตราฐานของอินเทอร์เน็ตโพรโทคอลคือ Internet Protocol version 4 (IPv4) ซึ่งใช้เป็นมาตรฐานในการส่งข้อมูลในเครือข่ายอินเทอร์เน็ตตั้งแต่ปี ค.ศ. 1981 ทั้งนี้การขยายตัวของเครือข่ายอินเทอร์เน็ตในช่วงที่ผ่านมามีอัตราการเติบโตอย่างรวดเร็ว นักวิจัยเริ่มพบว่าจำนวนเลขที่อยู่ของ IPv4 กำลังจะถูกใช้หมดไป ไม่เพียงพอกับการใช้งานอินเทอร์เน็ตในอนาคต ดังนั้นคณะทำงาน IETF (The Internet Engineering Task Force) ซึ่งตระหนักถึงปัญหาสำคัญดังกล่าว จึงได้พัฒนาอินเทอร์เน็ตโพรโทคอลรุ่นที่หก คือ Internet Protocol version 6 (IPv6) เพื่อทดแทนอินเทอร์เน็ตโพรโทคอลรุ่นเดิม โดยมีวัตถุประสงค์ IPv6 เพื่อปรับปรุงโครงสร้างของตัวโพรโทคอล ให้รองรับเลขที่อยู่จำนวนมาก และปรับปรุง

คุณลักษณะอื่นๆ อีกหลายประการ ทั้งในแง่ของประสิทธิภาพและความปลอดภัยรองรับระบบแอปพลิเคชัน (Application) ใหม่ๆ ที่จะเกิดขึ้นในอนาคต และเพิ่มประสิทธิภาพในการประมวลผลการส่งข้อมูล (Packet) ให้ดีขึ้น ทำให้สามารถตอบสนองต่อการขยายตัวและความต้องการใช้งานเทคโนโลยีบนเครือข่ายอินเทอร์เน็ตในอนาคต

2.2 Internet Protocol version 4 (IPv4)

ปัจจุบันโพรโทคอลที่ใช้งานอยู่ในเครือข่ายอินเทอร์เน็ตจะเป็นรุ่นที่ 4 (IPv4) ซึ่งจะมีขนาดเลขที่อยู่ (IP Address) 32 บิต โดยเขียนให้อยู่ในรูปแบบด็อตเดซิมอล (Dotted Decimal Notation) รูปแบบการเขียนโดยแยกจัดกลุ่มเลขฐานสองเป็น 4 กลุ่ม กลุ่มละ 8 บิต ทำการแปลงจากเลขฐานสองของแต่ละกลุ่มให้เป็นเลขฐานสิบ เมื่อแปลงเสร็จให้นำเลขทั้งสี่ตัวมารวมกัน เลขที่อยู่เป็นเลขฐานสิบเป็นการแปลงมาจากเลขฐานสอง 8 บิต ดังนั้นเลขฐานสิบแต่ละตัวจะอยู่ระหว่าง 0 ถึง 255 ดังนั้นหมายเลขที่อยู่ของ IPv4 จะอยู่ระหว่าง 0.0.0.0 ถึง 255.255.255.255

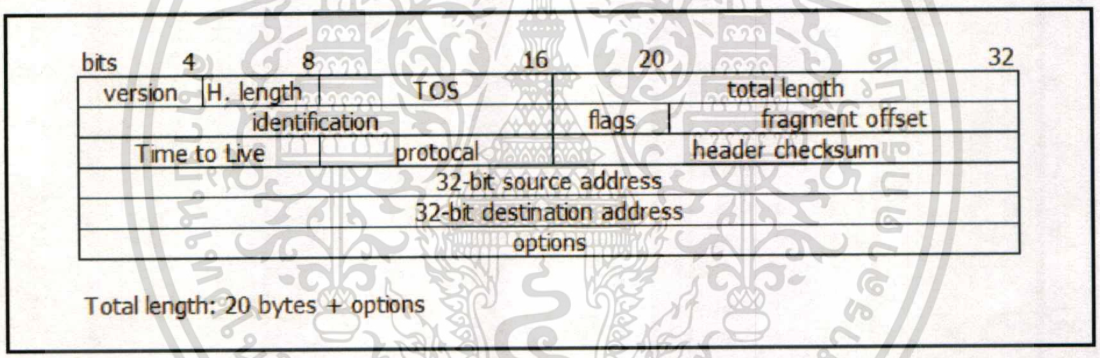
โพรโทคอลรุ่นที่ 4 (IPv4) ที่ใช้งานอยู่ในปัจจุบันจะแบ่งเลขที่อยู่ออกเป็น 5 ประเภท (Class) คือ A , B , C , D และ E โดยเลขที่อยู่ทั้ง 32 บิต จะถูกจัดให้เป็น 2 กลุ่มดังนี้ คือ กลุ่มแรกจะเป็นตัวเลขที่ใช้บอกหมายเลขเครือข่าย (Network ID) และกลุ่มที่สองจะเป็นตัวเลขที่ใช้บอกหมายเลขอุปกรณ์ที่อยู่ในเครือข่ายนั้น

ข้อกำหนดที่ใช้ในการแบ่งประเภทของเลขที่อยู่ ดังนี้

1. **Class A** : สำหรับเลขที่อยู่ประเภท A บิตแรกจะเป็นเลข 0 เท่านั้นและ 8 บิตแรกถัดมาเป็นส่วนที่บอกหมายเลขเครือข่าย เนื่องจากเครือข่ายมีจำนวนน้อยมากเมื่อเทียบกับจำนวนอุปกรณ์ ดังนั้นเลขที่อยู่ประเภทนี้จึงไม่เหมาะสำหรับเครือข่ายขนาดใหญ่ ซึ่งประกอบด้วยหลายเครือข่ายเชื่อมต่อกัน เช่น ระบบอินเทอร์เน็ต เพราะในการส่งข้อมูลระหว่างเครือข่ายนั้นเร้าเตอร์จะใช้เฉพาะหมายเลขเครือข่ายเท่านั้น ดังนั้นเครือข่ายประเภทนี้จึงเหมาะกับเครือข่ายส่วนบุคคล
2. **Class B** : สำหรับเลขที่อยู่ประเภท B นั้นสองบิตแรกจะเป็น 10 เท่านั้น ส่วนหมายเลขเครือข่ายจะใช้ 16 บิตแรก ดังนั้นจะมีจำนวนเครือข่ายได้ทั้งหมด 16,382 เครือข่าย ส่วนอีก 16 บิตที่เหลือเป็นหมายเลขอุปกรณ์ ซึ่งจะทำให้ในแต่ละเครือข่ายมีอุปกรณ์ได้ทั้งหมด 65,534 เครื่อง

3. **Class C** : สำหรับประเภท C จะมีบิตเริ่มต้นเป็น 110 และเมื่อรวมกับอีก 21 บิตต่อมาก็จะเป็นหมายเลขเครือข่าย ซึ่งจะได้ทั้งหมด 2,097,152 เครือข่าย ส่วน 8 บิตสุดท้ายเป็นหมายเลขอุปกรณ์ ซึ่งมีทั้งหมด 254 เครื่อง
4. **Class D** : สำหรับประเภท D จะมีบิตเริ่มต้นเป็น 1110 ซึ่งจะเป็นเลขที่อยู่ที่ใช้สำหรับการมัลติคาสก์ (Multicast) หรือสำหรับส่งข้อมูลแบบมีอุปกรณ์ปลายทางหลายเครื่องแต่อาจจะอยู่คนละเครือข่ายกัน
5. **Class E** : สำหรับประเภท E จะมีบิตเริ่มต้นเป็น 11110 เป็นหมายเลขที่สงวนไว้ใช้ในอนาคต หมายเลขเหล่านี้จะถูกกำหนดให้โดยศูนย์ข้อมูลเครือข่าย หรือ InterNIC (Internet Network Information Center)

โดยรูปแบบส่วนหัว (Header) ของกลุ่มข้อมูล (Packet) IPv4 ประกอบด้วยข้อมูลดังรูป 2.1



รูปที่ 2.1 แสดงรูปแบบ Header ของ IPv4 Packet

2.3 Internet Protocol version 6 (IPv6)

IETF ใช้เวลากว่าสามปีในการพัฒนาโพรโทคอล IPng (IP Next Generation) หรือ IPv6 โดยในช่วงปลายปี 1992 มีการยื่นข้อเสนอในการพัฒนาโพรโทคอลดังกล่าวทั้งหมด 4 ฉบับ อันได้แก่ CNAT, IP Encaps, Nimrod และSimple CLNP ต่อมาในเดือนธันวาคมปี 1992 มีการส่งข้อเสนอเพิ่มอีก 3 ฉบับคือ The P Internet Protocol (PIP), The Simple Internet Protocol (SIP) และ TP/IX หลังจากนั้นฤดูใบไม้ผลิในปี 1992 ข้อเสนอที่ชื่อว่า Simple CLNP ได้เปลี่ยนชื่อมาเป็น TCP and UDP with Bigger Addresses (TUBA) และ IP Encaps เปลี่ยนเป็น IP Address Encapsulation (IPAE) ในปี 1993 IPAE ได้รวมเข้ากับ SIP โดยยังคงใช้ชื่อว่า SIP ซึ่งต่อมากลุ่มนี้ได้รวมกับกลุ่ม

PIP กลายเป็นคณะทำงานที่เรียกตัวเองว่า Simple Internet Protocol Plus (SIPP) โดยในเวลาเดียวกันนั้นกลุ่มคณะทำงาน TP/IX ได้เปลี่ยนชื่อใหม่เป็น Common Architecture for the Internet (CATNIP) กล่าวได้ว่า ณ เวลานั้น มีข้อเสนอ 3 ชุดที่ถูกนำมาทำการคัดเลือกตามเกณฑ์ที่กำหนดไว้ในเอกสาร RFC1726 อันได้แก่ CATNIP,TUBA และ SIPP โดย

สาระสำคัญในแต่ละข้อเสนอมีดังต่อไปนี้

1. CATNIP (Common Architecture for Next Generation Internet Protocol) ได้ทำการสร้างความเป็นสามัญระหว่าง Internet (IPv4, TCP, UDP), OSI (CLNP, TP4, CLTP) และโพรโทคอล Novell (IPX, SPX)

2. TUBA (TCP and UDP with Bigger Addresses) ได้แทนที่เน็ตเวิร์คเลเยอร์ด้วย ISO's CNLP ซึ่งประกอบไปด้วยชุดหมายเลขแอดเดรสที่มีขนาดใหญ่กว่าในขณะที่ TCP/UDP สามารถใช้งานได้โดยไม่ต้องทำการปรับปรุงทั้งยังทำงานร่วมกับIDRP,IS-ISและES-IS ได้

3. SIPP (Simple Internet Protocol Plus) ได้นำคุณลักษณะบางอย่างใน IPv4 ที่คิดว่าไม่เหมาะสมออก และทำการปรับปรุงส่วนหัวของโพรโทคอลเสียใหม่ให้มีประสิทธิภาพมากยิ่งขึ้น และทำการเพิ่มขนาดของเลขที่อยู่จากเดิม 32 บิตเป็น 64 บิต ซึ่งต่อมาได้พัฒนาเป็นรุ่น128 บิต

2.3.1 ลักษณะ IPv6

IPv6 ได้มีการปรับปรุงจำนวนเลขที่อยู่เพิ่มขึ้นอย่างมากจาก IPv4 จากซึ่งมีขนาด 32 บิต เป็นมีขนาด 128 บิต ความแตกต่างของจำนวนทำให้เลขที่อยู่จึงมีจำนวนมาก ด้วยความยาวที่เพิ่มขึ้นของเลขที่อยู่ IPv6 ดังนั้นการอ้างอิงถึงเลขที่อยู่ IPv6 จึงใช้เลขฐานสิบหกเป็นหลัก โดยเขียนแบ่งเป็นลักษณะ 8 กลุ่มตัวเลข คั่นด้วยเครื่องหมาย “ : ” แต่ละกลุ่มตัวเลขจะประกอบไปด้วยเลขฐานสิบหกจำนวน 4 ตัว (ตัวละ 4 บิต รวมเป็น 16 บิต) นอกจากนี้ยังสามารถเขียนแบบย่อได้ โดยมีเงื่อนไขคือ

1. หากมีเลขศูนย์ด้านหน้าของกลุ่มใดสามารถจะละไว้ได้

2. หากกลุ่มใดเป็นเลขศูนย์ทั้ง 4 ตัว (0000) สามารถเขียนแทนด้วย “ 0 ”

3. หากกลุ่มใดกลุ่มหนึ่ง (หรือหลายๆกลุ่มที่ตำแหน่งติดกัน) เป็นเลขศูนย์ทั้งหมด สามารถจะละไว้ ได้โดยใช้เครื่องหมาย “ :: ” แต่จะสามารถทำลักษณะนี้ได้ตำแหน่งเดียวเท่านั้น เช่น

3fee:085b:1f1f:0000:0000:0000:00a9:1234 หรือ 3fee:085b:1f1f::a9:1234

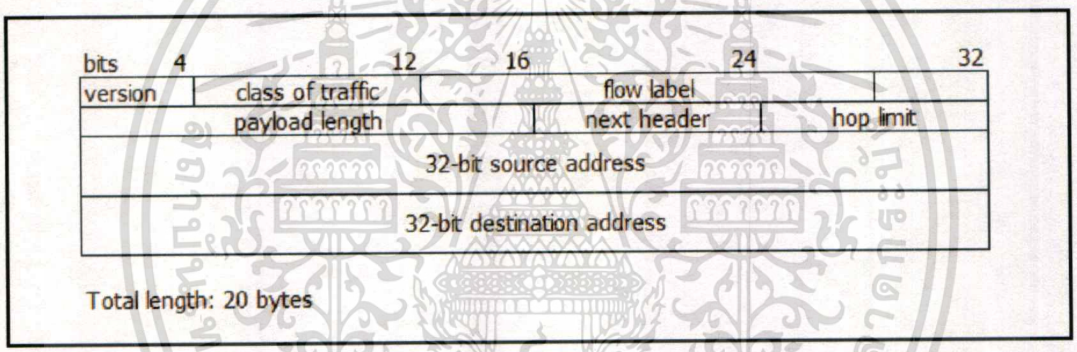
0000:0000:0000:0000:0000:0000:0000:0001 หรือ ::1

fec0:0000:0000:0000:0200:3cff:fec6:172e หรือ fec0::200:3cff:fec6:172e

2001:0000:0000:34fe:0000:0000:00ff:0321 2001::34fe:0:0:ff:321

2.3.2 Header IPv6 Packet

รูปแบบส่วนหัว (Header) ของกลุ่มข้อมูล (Packet) IPv6 ถูกออกแบบมาให้มีขนาดไม่คงที่ (40 ไบต์) ดังรูป 2.2 และมีรูปแบบที่ง่ายที่สุดเท่าที่จะทำได้โดยเฮดเดอร์ จะประกอบด้วยตำแหน่งต่างๆที่จำเป็นต้องใช้ในการประมวลผลกลุ่มข้อมูลที่เร้าเตอร์หรืออุปกรณ์เลือกเส้นทางทุกตัวเท่านั้น ส่วนตำแหน่งที่อาจจะถูกประมวลผลเฉพาะที่ต้นหรือปลายทางหรือที่เร้าเตอร์บางตัว จะถูกแยกออกมาไว้ที่ส่วนขยายของเฮดเดอร์ (Extended Header)



รูปที่ 2.2 แสดงรูปแบบ Header ของ IPv6 Packet

2.3.3 Extender Header IPv6

พิจารณารูปแบบ Header ของ IPV 6 เทียบกับของ IPV 4 จะสามารถเปรียบเทียบความแตกต่างได้ดังนี้

1. **ตำแหน่งข้อมูลที่ตัดออก**

Header length : ถูกตัดออกไป เพราะเฮดเดอร์ของ IPv6 มีขนาดไม่คงที่ (40 ไบต์) ทำให้ประสิทธิภาพโดยรวมของการประมวลผลแพ็กเก็ตดีขึ้น ไม่เสียเวลาในการคำนวณขนาดของเฮดเดอร์

Identification, Flag, Flag Offset, Protocol, Options, และ Padding : ถูกย้ายไปอยู่ใน ส่วนขยายของเฮดเดอร์(Extended Header) เพราะถือว่าเป็นส่วนที่ไม่จำเป็นต้องประมวลผลในทุกๆ เร้าเตอร์

Header Checksum : ถูกตัดออกเพราะว่าซ้ำซ้อนกับฟังก์ชันของโพรโทคอลในชั้นที่อยู่สูงกว่า อีกทั้งเป็นการเพิ่มประสิทธิภาพของการประมวลผลด้วย เพราะ Checksum จะต้องมีการคำนวณใหม่ที่เร้าเตอร์เสมอหากตัดออกก็จะลดภาระงานที่เร้าเตอร์ไปได้

2. ตำแหน่งข้อมูลที่ปรับเปลี่ยน

Total Length : เปลี่ยนมาเป็น Payload lengthเพื่อระบุขนาดของ Payload ในหน่วยไบต์ ดังนั้นขนาดของ Payload สูงสุดจะเป็น 65,535 ไบต์ Time-To-Live (TTL) ของ IPv4 เปลี่ยนมาเป็นHop Limit เพราะ TTL ระบุเวลาที่แพ็กเก็ตจะวนเวียนอยู่ในอินเทอร์เน็ต (หน่วยเป็นวินาที)โดยระบุว่าแต่ละเร้าเตอร์ต้องลด TTL ลงอย่างน้อย 1 วินาที เร้าเตอร์จึงลด TTL ครั้งละ 1 หน่วยเสมอแม้ว่าจะใช้เวลาประมวลผลแพ็กเก็ตน้อยกว่านั้น ทำให้ไม่ตรงกับความหมายของ TTLดังนั้นจึงถูกเปลี่ยนเป็น Hop Limit เพื่อให้ตรงกับความหมายจริงๆ ซึ่งเหมาะสมและง่ายต่อการประมวลผล

Protocol : เปลี่ยนมาเป็น Next Header ซึ่งใช้เป็นตัวบอกว่า Extended Header ตัวถัดไปเป็นเฮดเดอร์ ประเภทไหน เช่น ถ้าเป็น ExtendedHeader ชนิด IPsec จะมีค่า Next Header = 51

Type-of-Service (TOS) : เปลี่ยนมาเป็น TrafficClass ซึ่งมีจำนวนบิตมากกว่า สามารถแบ่งกลุ่มและระดับความสำคัญของแต่ละแพ็กเก็ตละเอียดมากขึ้น เพื่อที่เร้าเตอร์จะจัดลำดับขั้นการส่งแพ็กเก็ตให้เหมาะสม

3. ตำแหน่งข้อมูลที่เพิ่ม

Flow Label : ใช้ระบุลักษณะการไหลเวียนของทราฟฟิกระหว่างต้นทางกับปลายทาง เนื่องจากในแอปพลิเคชันหนึ่ง สามารถมีทราฟฟิกหลายประเภท (เช่น ภาพ เสียง ตัวอักษร ฯลฯ) และทราฟฟิกแต่ละประเภทมีความต้องการที่แตกต่างกัน Flow Label จึงมีไว้เพื่อแยกประเภทของทราฟฟิกและเพื่อให้เร้าเตอร์รู้ว่าควรปฏิบัติต่อทราฟฟิกแต่ละประเภทแตกต่างกัน

2.4 การทำงานระหว่างเครือข่าย IPv4 และ IPv6

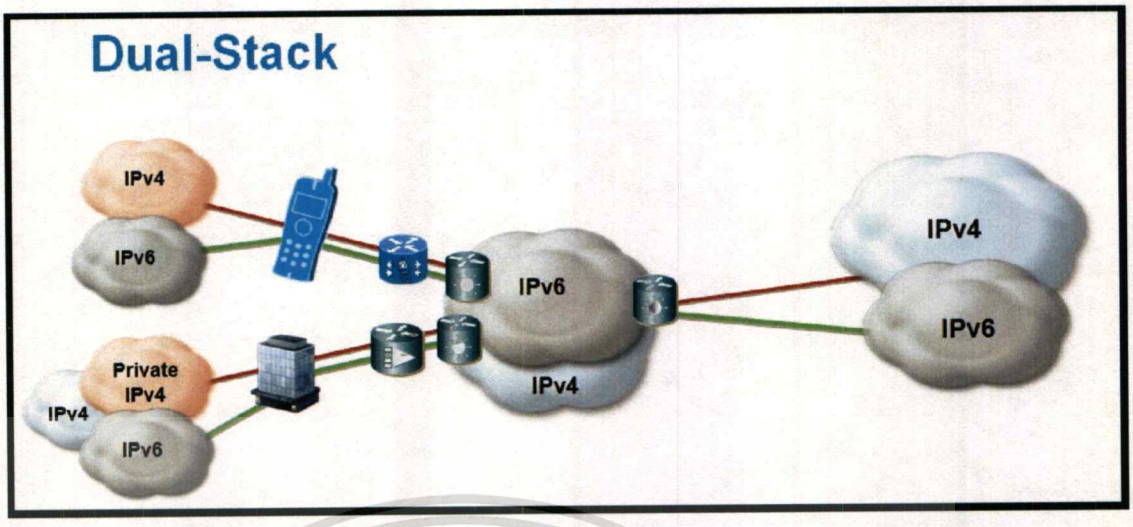
ในการนำ IPv6 มาใช้งานนั้น ทาง IETF ได้เสนอทางออกเพื่อช่วยในการทำงานร่วมกันระหว่าง IPv4 และ IPv6 ในระหว่างที่เครือข่าย บางแห่งเริ่มมีการปรับเปลี่ยน ในช่วงแรก การใช้งาน IPv6 อาจอยู่ในวงแคบ ดังนั้นจึงต้องอาศัยเทคนิคเพื่อเชื่อมต่อเครือข่ายที่เป็น IPv6 เข้ากับเครือข่าย IPv4 หรือเครือข่าย IPv6 อื่น เทคนิคการทำงานร่วมกันระหว่าง IPv4 และ IPv6 แบ่งออกเป็น 3 ประเภทด้วยกัน คือ

2.4.1 การทำ Dual Stack

เป็นวิธีพื้นฐานที่สุด ทำงานโดยใช้ IP stack สองอันคือ IPv4 stack และ IPv6 stack ทำงานควบคู่กัน ภายในอุปกรณ์ตัวเดียวกัน Dual stacks สามารถใช้ได้ทั้งที่อุปกรณ์ปลายทางที่เครื่องให้บริการ (Server) และที่อุปกรณ์เครือข่าย เช่น เร้าเตอร์ Dual stacks เป็นทางออกที่ง่ายที่สุดสำหรับเครือข่ายที่ต้องการเริ่มใช้งาน IPv6 และถูกใช้อย่างแพร่หลายมากที่สุด

ในปัจจุบัน Dual stacks เหมาะกับการติดต่อระหว่างสองสถานีเชื่อมต่อ (Node) ที่ใช้อินเทอร์เน็ตโพรโทคอลรุ่นเดียวกัน แต่ต้องผ่านเครือข่ายกลางทางที่ใช้ไอพีโพรโทคอลต่างรุ่น เช่น IPv4 - IPv4 ผ่านเครือข่าย IPv6 หรือ IPv6 - IPv6 ผ่านเครือข่าย IPv4 หรือในกรณีที่ บางโหนดต้องการปรับเปลี่ยนไปใช้โพรโทคอล IPv6 แต่หากเครือข่ายที่เชื่อมต่ออยู่ด้วยไม่สนับสนุน IPv6 โหนดเชื่อมต่อดังกล่าว สามารถใช้ Dual Stacks เพื่อรองรับทั้ง IPv4 และ IPv6 ดังรูป 2.3

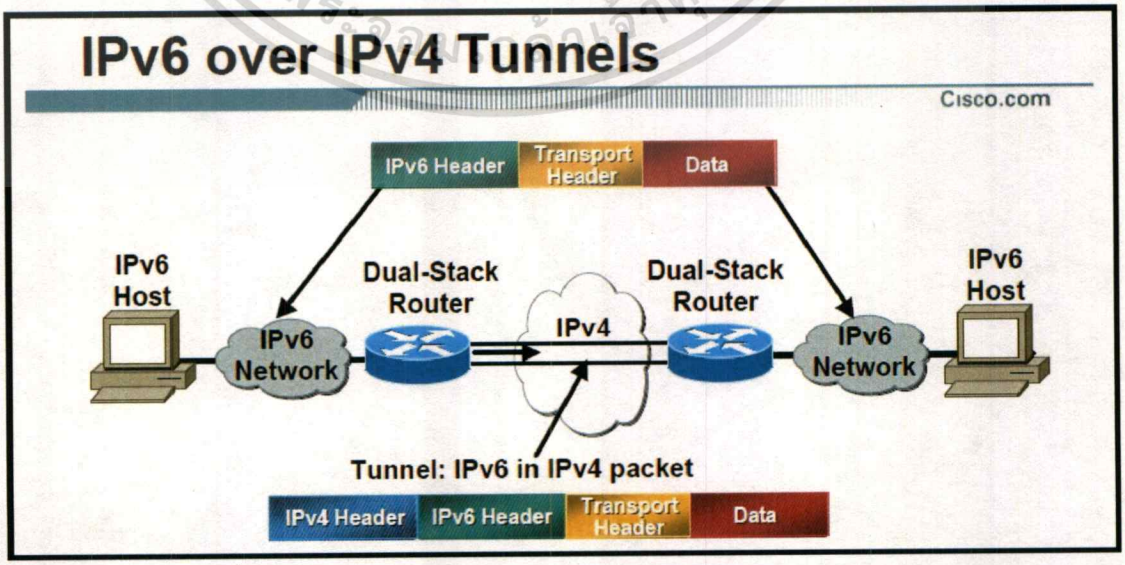
หลักการทำงานคือ IP stack ที่อยู่ภายในโหนดจะ แบ่งออกเป็น 2 Stacks ทำงานขนานกัน เช่นเมื่อโหนดได้รับ IPv6 Packet โหนดจะเลือก IPv6 Stack มาจัดการกับ กลุ่มข้อมูล (Packet) โดยตรวจสอบรุ่นของโพรโทคอลจากส่วนหัวของกลุ่มข้อมูล ในขณะเดียวกันโหนดสามารถติดต่อกับเครือข่าย IPv4 ผ่าน IPv4 Stack ได้เหมือนเดิมไม่ต้องเปลี่ยนแปลง โดยโหนดที่มี Dual Stack นี้จะต้องมีเลขที่อยู่สองหมายเลข คือ IPv4 Addressและ IPv6 Address



รูปที่ 2.3 แสดงวิธีการการทำงานร่วมกันระหว่าง IPv4 และ IPv6 แบบ Dual Stack

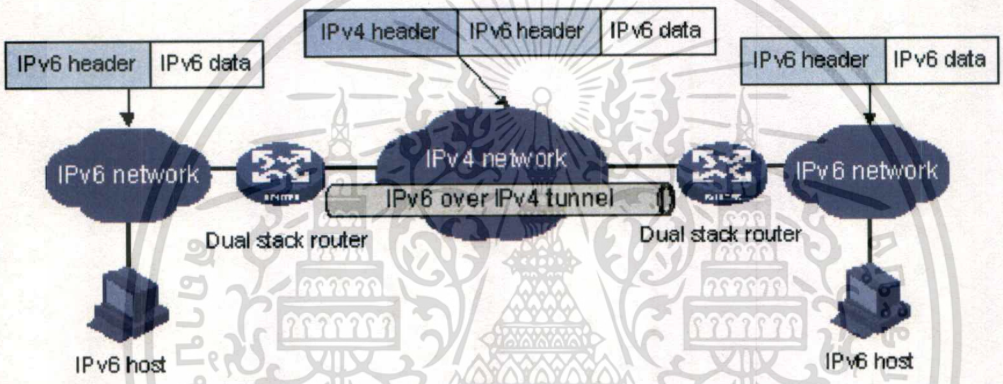
2.4.2 การทำ Tunneling

Tunnel หรือการทำอุโมงค์ เป็นอีกวิธีที่ใช้กันแพร่หลายเพราะเหมาะสมกับการสื่อสารระหว่างเครือข่าย IPv6 ผ่านเครือข่าย IPv4 การส่งข้อมูลทำได้โดยการห่อหุ้ม (Encapsulate) กลุ่มข้อมูล (Packet) ดังรูป 2.4 ที่ต้องการส่งไว้ในอีกกลุ่มข้อมูลหนึ่ง เนื่องจากกลุ่มข้อมูลที่อยู่ภายในไม่สามารถถูกส่งไปยังปลายทางได้ จึงต้องอาศัยการห่อหุ้มด้วยกลุ่มข้อมูลอื่น การทำอุโมงค์เพื่อใช้งาน IPv6 นั้นมีการใช้เมื่อเครือข่ายเชื่อมต่ออยู่ด้วยไม่สนับสนุน IPv6 จึงจำเป็นต้องหุ้มกลุ่มข้อมูล IPv6 ไว้ภายใต้กลุ่มข้อมูล IPv4 อีกชั้น



รูปที่ 2.4 แสดงการห่อหุ้ม (Encapsulate) IPv6 ด้วย IPv6

การทำอุโมงค์ สำหรับเครือข่าย IPv6 ต้องสร้างเส้นทางการติดต่อระหว่างอุปกรณ์ที่ใช้เลขที่อยู่ IPv6 ผ่านเครือข่ายที่ใช้เลขที่อยู่ IPv4 โดยเกตเวย์ (Gateway) ของเครือข่ายของเครื่องที่ใช้เลขที่อยู่ IPv6 จะทำหน้าที่ห่อหุ้มกลุ่มข้อมูล IPv6 ไว้ในกลุ่มข้อมูล IPv4 ก่อนจะส่งไปในเครือข่ายอินเทอร์เน็ตที่สนับสนุนการใช้เลขที่อยู่ IPv4 เท่านั้น โดยระหว่างทางจะมีการตรวจสอบเลขที่อยู่ต้นทางและปลายทางที่อยู่ในส่วนหัวของกลุ่มข้อมูล IPv4 เท่านั้น โดยไม่สนใจส่วนที่อยู่ภายใน เมื่อส่งไปถึงปลายทาง เกตเวย์จะทำการถอดกลุ่ม IPv4 ออกให้เหลือแต่กลุ่มข้อมูล IPv6 แล้วส่งไปยังอุปกรณ์ที่ใช้เลขที่อยู่ IPv6 ต่อไป ดังรูป 2.5



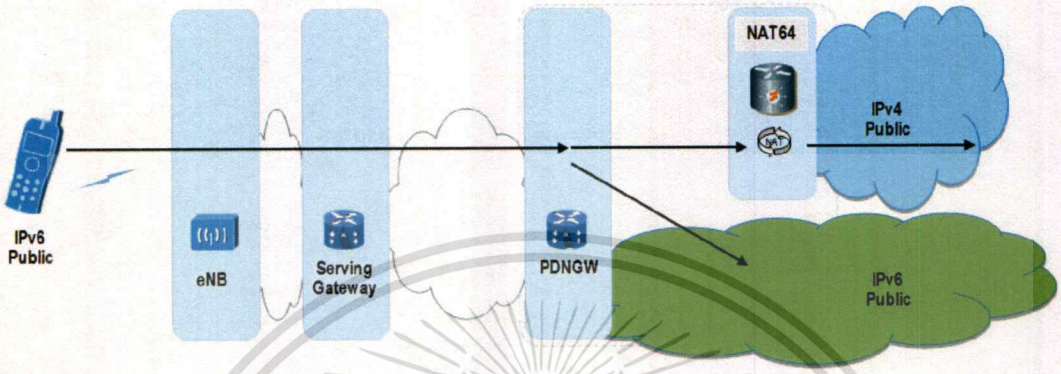
รูปที่ 2.5 แสดงวิธีการทำงานร่วมกันระหว่าง IPv4 และ IPv6 แบบ Tunneling

2.4.3 การทำ Translation

เทคนิคการทำ Translation เป็นวิธีที่ใช้กับการสื่อสารข้ามเครือข่าย เช่น สถานีเชื่อมต่อ (Node) จากเครือข่าย IPv4 ต้องการติดต่อกับเครื่องให้บริการ (Server)ในเครือข่าย IPv6 หรือโหนดที่เป็น IPv6 ต้องการคุยกับเครื่องให้บริการเป็น IPv4 ซึ่งจะเป็นกรณีที่ต่างไปจากการใช้งาน Dual Stacks และ Tunneling สำหรับการทำ Translation เป็นการแปลงข้อมูลไปมาระหว่างข้อมูลในรูปแบบของ IPv4และ IPv6 การแปลงข้อมูลนี้สามารถทำได้สองแบบ คือ

1. การแปลงที่อุปกรณ์ปลายทางโดยเพิ่มฟังก์ชันแปล เข้าไปในโพรโทคอล Stackโดยอาจอยู่ที่ชั้นเครือข่าย (Network Layer) หรือชั้นซ็อกเก็ต (Socket Layer)
2. การแปลงที่อุปกรณ์เครือข่ายโดยจะต้องใช้เกตเวย์ ทำหน้าที่เป็นตัวแปลง IPv6 - IPv4 และIPv4 - IPv6 อยู่ที่ทางออกที่มีการเชื่อมต่อระหว่างเครือข่าย IPv6 และ IPv4 สำหรับการแปลงข้อมูล องค์ประกอบสำคัญที่จำเป็นคือ ส่วนที่ทำหน้าที่แปลงเลขที่อยู่ ซึ่งการ

แปลงนี้สามารถทำได้โดยการจัดเก็บคู่เลขที่อยู่ IPv4 และ IPv6 ทุกคู่ในเครือข่าย โดยเรียกวิธีนี้ว่า Stateful Address Translation หรือจะทำการแปลงแบบอัตโนมัติที่เรียกว่า Stateless Address Translator



รูปที่ 2.6 แสดงเทคนิคการทำ NAT64

Models Comparison
Characteristics Summary

	CGN44	Dual Stack	Pure NAT64	6rd	DS Lite	SAM / 4rd	Stateless NAT64 Relay (dIVI)
Problem Addressed	IPv4 Exhaust in an IPv4 network	IPv6 Deployment/initial transition	IPv6 host to IPv4 Internet/Server	IPv6 Deployment/Initial transition	IPv4 services over IPv6	IPv4 services over IPv6	IPv4 services over IPv6 + IPv6 to IPv4
Technology	Translation	Pure IP Routing	Translation	Tunnel	Tunnel	Tunnel	Translation
SP IPv6 addressing constraints	No	No	No – Stateful Yes–Stateless	Some	No	Yes (IPv4 embedded IPv6 address)	Yes (IPv4 embedded IPv6 address)
Subscriber's IPv4 addressing constraints	Private	As today	Public IPv4 – Stateless	Stable Address	Private address w/ limited port range	Limited port range	Limited port range
SP State	NAT xlate state	IPv4+IPv6	NAT xlate state - Stateful	EID-to-RLOC map cache entry	NAT44 session, v6 tunnel binding	4over6 encap table, port range config	1:N NAT64, port range config
Dynamic CPE State	PNAT44	PNAT44	None	PNAT44	No (no NAT on B4)	PNAT44	PNAT44
Other State			None	MS/MR EID registration entry	Translation logging	None	None
SP NAT	Yes	Can be combined	Yes	Can be combined	Yes, limited ALG	No	No
CPE NAT	Yes	Yes	No	Yes	No	Yes	Yes
Operation and Provisioning Extensions	Logging	AAA, DHCPv6	AAA, DHCP6	DHCPv4, TR69	DHCPv6, TR69, Radius	(maybe DHCPv6)	(maybe DHCPv6)
Scalability	O(# of xlates on CGN)	IPv4 addresses	O(# of xlates on AFT)	IPv4 addresses (private or public)	O(# of xlates on CGN sessions)	O(#IPv4 addresses x port ration)	O(#IPv4 addresses x port ration)
Loadbalancing	Yes (per subscriber)	Yes (ECMP)	Yes (ECMP)	Yes (LISP TE)	Yes (per tunnel)	Yes (ECMP)	Yes (ECMP)
Inter-chassis Redundancy	No (IP xlate impacted)	Yes	Yes – stateless No- stateful	Yes	No (IP xlate impacted)	Yes	Yes
Topology	Hub & Spoke	P2P (Full Mesh)	P2P (Full Mesh)	P2P (Full Mesh)	Hub & Spoke	P2P (Full Mesh)	P2P (Full Mesh)

รูปที่ 2.7 แสดงการเปรียบเทียบวิธีการทำงานระหว่าง IPv4 และ IPv6

2.5 คุณลักษณะเพิ่มเติมของ IPv6

IPv6 มีการปรับปรุงให้มีเลขที่อยู่พิ่มมากขึ้นแล้ว IPv6 ยังได้รับการออกแบบมาให้เหมาะสมกับสภาพการใช้งานอินเทอร์เน็ตในปัจจุบัน ความสามารถพิเศษต่างๆ ที่ถูกบรรจุอยู่ใน IPv6 ได้แก่

1. Management

การตั้งค่าและปรับแต่งระบบเครือข่าย ในปัจจุบันมีความซับซ้อนมาก IPv6 จึงถูกออกแบบมาให้สนับสนุนการติดตั้งและปรับแต่งระบบแบบอัตโนมัติ (Auto Configuration) เพื่ออำนวยความสะดวกให้กับการจัดสรรปรับเปลี่ยน IP address (Address Renumbering) การเชื่อมต่อกับผู้ให้บริการหลายราย (Multihoming) และแม้แต่การจัดการเครือข่ายแบบ Plug-and-play

2. Broadcast/Multicast/Anycast

ใน IPv4 ได้มีการจัดสรรเลขที่อยู่ส่วนหนึ่งเพื่อเป็นเลขที่อยู่แพร่กระจาย (Broadcast address) แต่ในความเป็นจริงแล้วการสื่อสารแบบ Broadcast เป็นสิ่งที่ไม่มีความจำเป็นและสิ้นเปลืองแบนด์วิดท์ (Bandwidth) โดยเปล่าประโยชน์ การส่งสัญญาณแบบหลาย (Multicast) เป็นการสื่อสารที่มีประสิทธิภาพมากกว่าและเริ่มเป็นที่นิยม IPv6 จึงถูกออกแบบมาให้รองรับกลุ่มเลขที่อยู่แบบ Multicastและตัดกลุ่มเลขที่อยู่แบบ Broadcast ออก

นอกจากนี้ IPv6 ยังเพิ่มความสามารถในการสื่อสารแบบ Anycast โดยอนุญาตให้อุปกรณ์มากกว่า 1ชิ้นได้รับการจัดสรร IP address เบอร์เดียวกันซึ่งหมายความว่าอุปกรณ์ชิ้นใดก็ได้สามารถตอบสนองต่อข้อมูลที่ส่งมาที่เลขที่อยู่ Anycast นั้นๆ

3. Security

เร้าเตอร์และอุปกรณ์เครือข่ายทุกตัวในเครือข่าย IPv6 ถูกกำหนดให้รองรับการใช้งาน IPSec นอกจากนี้ยังมีการกำหนดข้อมูลความปลอดภัย (Security Payload) สองประเภทคือ Authentication Payload และ Encrypted Security Payload เพื่อสนับสนุนการรับส่งข้อมูลที่มั่นคงปลอดภัย ภายใต้ชั้นเครือข่ายแทนที่จะพึ่งชั้นแอปพลิเคชั่นเหมือนในเครือข่าย IPv4

4. Virtual Private Network (VPN)

แต่เดิมในเครือข่ายIPv4 การให้บริการ VPN ทำได้โดยใช้ IPSec เพื่อเข้ารหัสข้อมูลใน Network Layer ทั้งหมด ซึ่งจะติดปัญหาหากเครือข่ายต้นทางหรือปลายทางมีการทำ Network Address Translation (NAT) เพราะการเข้ารหัสจะต้องสิ้นสุดก่อนถึงจุดหมายปลายทางสำหรับ

เครือข่าย IPv6 ไม่มีปัญหาดังกล่าว เพราะไม่มีความจำเป็นต้องใช้ NAT อีกต่อไป นอกจากนี้ยังสามารถใช้ Extended Hearder ที่เรียกว่า Authentication Header และ Encapsulated Security Payloadเพื่อรองรับการใช้งาน VPN แบบปลอดภัย

5. Quality-of-Service IPv6

ถูกออกแบบมาให้สนับสนุนการรับประกันคุณภาพของบริการตั้งแต่เริ่ม โดยจะเห็นได้จากตำแหน่ง Flow Label และ Traffic Classในเฮดเดอร์ ถึงแม้ว่าในเฮดเดอร์ของ IPv4 จะมีตำแหน่ง Type-of-Service แต่ไม่มีการใช้อย่างแพร่หลาย เนื่องจากไม่มีมาตรฐานในการกำหนดค่าและเราเตอร์บางตัวเท่านั้นที่สามารถประมวลผลตำแหน่งToS ได้ ที่ผ่านมา IPv4 มักปล่อยให้ Layer ข้างล่างจัดการเรื่อง QoS แทน เช่น ผ่านเทคโนโลยี MPLS

6. Maximum Transfer Unit (MTU)

MTU ขั้นต่ำในเครือข่าย IPv4 คือ 576 ไบต์ และถูกเพิ่มเป็น 1280ไบต์ในเครือข่าย IPv6 การเพิ่มความยาวขั้นต่ำของMTU นี้จะช่วยให้การส่งข้อมูลในเครือข่าย IPv6มีประสิทธิภาพมากขึ้น โดยช่วยลดสัดส่วนของข้อมูลเฮดเดอร์ต่อข้อมูลทั้งหมด

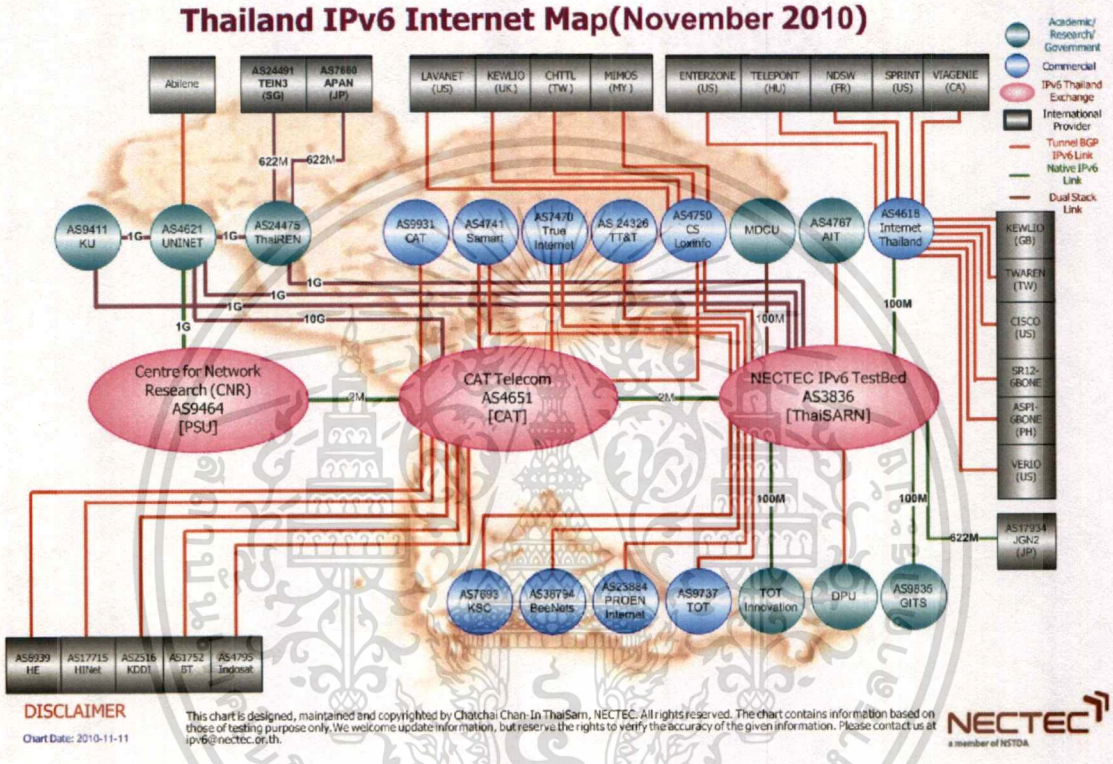
2.6 ผู้ให้บริการอินเทอร์เน็ตที่ให้บริการ IPv6

ปัจจุบัน ISP หลายรายได้รับการจัดสรรหมายเลข IPv6 address ซึ่งมีทั้งที่ให้บริการ IPv6 ในเชิงพาณิชย์กับลูกค้า และเพื่อการทดลองเชื่อมต่อเตรียมความพร้อมภายใน ตัวอย่างผู้ให้บริการ ดังรูปที่ 2.7

ลำดับที่	หน่วยงาน/องค์กร ผู้ให้บริการอินเทอร์เน็ต	IPv6 address from 6BONE	IPv6 address from APNIC
1.	CAT	-	2001:c38::/32
2.	TOT	-	2001:ec0::/32
3.	InternetThailand	3ffe:400B::/32	2001:c00::/32
4.	CS-Loxinfo	3ffe:4014::/32	-
5.	AsiaInfonet	-	2001:fb0::/32
6.	NECTEC	3ffe:4016::/32	2001:f00::/32
7.	UniNet	-	2001:3c8::/32

รูปที่ 2.8 แสดงผู้ให้บริการอินเทอร์เน็ตที่ให้บริการ IPv6

IPv6 address ที่ได้รับจัดสรรจาก 6Bone จะอยู่ในช่วง Prefix 3ffe::/16 เป็น IPv6 address ชั่วคราวสำหรับใช้งานในเครือข่ายทดสอบ ส่วน IPv6 address ที่ได้รับจัดสรรจาก APNIC จะเป็นหมายเลขที่สามารถนำไปให้บริการได้จริง สำหรับการใช้งานและให้บริการ IPv6 ในประเทศไทยนั้น แสดงดังรูปที่ 2.8



รูปที่ 2.9 แสดงแผนผังผู้ให้บริการอินเทอร์เน็ตบนเครือข่าย IPv6 ในประเทศไทย

บทที่ 3

วิเคราะห์ระบบงานเดิม

3.1 วิเคราะห์ระบบปัจจุบัน

ปัจจุบันการใช้งานอินเทอร์เน็ตและใช้งานทั่วไปในคณะเทคโนโลยีสารสนเทศ ลาดกระบัง และคณะเทคโนโลยีสารสนเทศ ตึกชินวัตร 3 มีการใช้งานแบบโพรโตคอล IPv4 ในการเข้าถึงโครงข่ายอินเทอร์เน็ตและโครงข่ายภายในคณะซึ่งโครงข่ายภายในคณะมีการติดตั้งอุปกรณ์ต่างๆ เพื่อรองรับการใช้งาน โดยอุปกรณ์แบ่งเป็น 4ส่วนหลักคือ

1. Untrustเป็นส่วนของอุปกรณ์ที่เชื่อมต่อตรงมาจากสำนักบริการคอมพิวเตอร์
2. Trust เป็นส่วนของอุปกรณ์ที่มีการเชื่อมต่อหลังจากไฟร์วอล์
3. Server Farm เป็นส่วนของกลุ่มเซิร์ฟเวอร์ที่ให้บริการในคณะ
4. DMZ เป็นส่วนของกลุ่มเซิร์ฟเวอร์ที่มีการติดต่อสื่อสารทั้งภายในและนอกคณะ

การใช้งานอินเทอร์เน็ตผ่านอุปกรณ์โครงข่ายภายในคณะ ผ่านไฟร์วอลล์ซึ่งเป็นเกตเวย์สำหรับ LAN ต่างๆ ควบคุมการเข้าออกข้อมูลภายในคณะ โดยไฟร์วอลล์ทำการส่งข้อมูลไปยังอุปกรณ์จัดเส้นทางของสถาบันฯ และถูกส่งข้อมูลต่อไปยังอุปกรณ์จัดเส้นทางของผู้ให้บริการอินเทอร์เน็ต (TRUE) โดยอุปกรณ์ในโครงข่ายของคณะดังตารางที่ 3.1-3.14

ตารางที่ 3.1 แสดงอุปกรณ์โครงข่าย1

ชนิดอุปกรณ์	Switch L2
ชื่ออุปกรณ์	SW-3COM-3824
รุ่น	3824
ผู้ขาย	3COM
OS	
หน้าที่การทำงาน	สวิตซ์ระดับเลเยอร์สองเชื่อมต่อใยแก้วนำแสง(Fiber Optic) จากสำนักบริการคอมพิวเตอร์เข้าสู่ระบบโครงข่ายของคณะแบบอีเทอร์เน็ตโดยมีการเชื่อมต่ออุปกรณ์ไร้สาย(Wireless) ของสำนักบริการคอมพิวเตอร์

ตารางที่ 3.2 แสดงอุปกรณ์โครงข่าย 2

ชนิดอุปกรณ์	Switch L2
ชื่ออุปกรณ์	SW-CISCO-3560G
รุ่น	Catalyst 3560
ผู้ขาย	CISCO
OS	IOS 12.0(5)WC10
หน้าที่การทำงาน	สวิตซ์ระดับเลเยอร์สองสำหรับต่อใช้งานอีเทอร์เน็ตในฝั่ง Untrust

ตารางที่ 3.3 แสดงอุปกรณ์โครงข่าย 3

ชนิดอุปกรณ์	Firewall
ชื่ออุปกรณ์	NSISG2000
รุ่น	ISG2000
ผู้ขาย	JUNIPER
OS	ScreenOS 6.2.0r4.0
หน้าที่การทำงาน	ไฟร์วอลล์สำหรับควบคุมการเข้าใช้งานในโครงข่ายของคณะโดยเป็นอุปกรณ์คั่นระหว่างโครงข่ายUntrustและ Trust ทั้งยังเป็นเกตเวย์สำหรับการจัดการควบคุมอุปกรณ์ตัวอื่นๆและเป็นเกตเวย์สำหรับ LAN และ Wireless LAN ในชั้นต่างๆ

ตารางที่ 3.4 แสดงอุปกรณ์โครงข่าย 4

ชนิดอุปกรณ์	Core Switch
ชื่ออุปกรณ์	Cat4506
รุ่น	Catalyst 4506
ผู้ขาย	CISCO
OS	IOS 12.1(13)EW2
หน้าที่การทำงาน	สวิตซ์ระดับเลเยอร์สามมีการเชื่อมต่อไปยังสวิตซ์ห้องชาร์ปในชั้นต่างๆเพื่อเชื่อมต่อ LAN ทุกห้องเข้าในโครงข่ายของคณะ โดยการเชื่อมต่อจะเป็นการเชื่อมต่อผ่านใยแก้วนำแสง (Fiber Optic)

ตารางที่ 3.5 แสดงอุปกรณ์โครงข่าย 5

ชนิดอุปกรณ์	Core Switch
ชื่ออุปกรณ์	C4506-Blade
รุ่น	Catalyst 4506
ผู้ขาย	CISCO
OS	IOS 12.1(13)EW2
หน้าที่การทำงาน	สวิตซ์ระดับเลเยอร์สามเชื่อมต่อไปยังเซิร์ฟเวอร์สองกลุ่ม ได้แก่ กลุ่มแรก DMZ เป็นกลุ่ม Server ที่สามารถเข้าโครงข่ายได้ทั้งขาที่เป็น Trust และ Untrustกลุ่มสอง Server Farm เป็นกลุ่มเซิร์ฟเวอร์ต่างๆภายในคณะเทคโนโลยีสารสนเทศ

ตารางที่ 3.6 แสดงอุปกรณ์โครงข่าย 6

ชนิดอุปกรณ์	Server Authentication
ชื่ออุปกรณ์	Server Authentication
รุ่น	HP Xenon
ผู้ขาย	HP
OS	Linux
หน้าที่การทำงาน	เซิร์ฟเวอร์สำหรับใช้ในการตรวจสอบสิทธิการใช้งานในการเข้าใช้งานผู้ใช้จะต้องทำการระบุตัวตนเพื่อแสดงสิทธิในการใช้งานผ่านเซิร์ฟเวอร์

ตารางที่ 3.7 แสดงอุปกรณ์โครงข่าย 7

ชนิดอุปกรณ์	Server Authentication
ชื่ออุปกรณ์	Consentry Authentication
รุ่น	CS2400
ผู้ขาย	CONSENTRY
หน้าที่การทำงาน	เซิร์ฟเวอร์สำหรับใช้ในการตรวจสอบสิทธิการใช้งานในการเข้าใช้งานผู้ใช้จะต้องทำการระบุตัวตนเพื่อแสดงสิทธิในการใช้งานผ่านเซิร์ฟเวอร์
ชนิดอุปกรณ์	Switch L2

ตารางที่ 3.8 แสดงอุปกรณ์โครงข่าย 8

ชนิดอุปกรณ์	SW-CISCO-3510
ชื่ออุปกรณ์	3510 Multipoint Control Unit
รุ่น	Catalyst 3560
ผู้ขาย	CISCO
OS	
หน้าที่การทำงาน	สวิตซ์ระดับเลเยอร์สองสำหรับต่อใช้งานโทรศัพท์ระบบ IP (IP Phone) โดยมีการเชื่อมแบบอีเทอร์เน็ตไปยังอุปกรณ์ปลายทาง

ตารางที่ 3.9 แสดงอุปกรณ์โครงข่าย9

ชนิดอุปกรณ์	Switch L2
ชื่ออุปกรณ์	SW-CISCO-3560#1-3
รุ่น	Catalyst 3560
ผู้ขาย	CISCO
OS	12.2(35)SE5
หน้าที่การทำงาน	สวิตซ์ระดับเลเยอร์สองสำหรับต่อไปยังเซิร์ฟเวอร์กลุ่ม DMZ และกลุ่ม Server Farm โดยมีการเชื่อมแบบอีเทอร์เน็ตไปยังอุปกรณ์ปลายทาง

ตารางที่ 3.10 แสดงอุปกรณ์โครงข่าย 10

ชนิดอุปกรณ์	Switch L2
ชื่ออุปกรณ์	Unmanage
รุ่น	1024D
ผู้ขาย	DLINK
OS	
หน้าที่การทำงาน	สวิตซ์ระดับเลเยอร์สองสำหรับต่อใช้งานระบบกล้องวงจรปิดโดยมีการเชื่อมแบบอีเทอร์เน็ตไปยังอุปกรณ์ปลายทาง

ตารางที่ 3.11 แสดงอุปกรณ์โครงข่าย 11

ชนิดอุปกรณ์	Switch L2
ชื่ออุปกรณ์	Router-Cisco-2800
รุ่น	2800
ผู้ขาย	CISCO
OS	IOS 12.4(11)T2
หน้าที่การทำงาน	สวิตซ์ระดับเลเยอร์สองสำหรับต่อใช้งานผ่าน Leaseline True

ตารางที่ 3.12 แสดงอุปกรณ์โครงข่าย 12

ชนิดอุปกรณ์	Switch L2
ชื่ออุปกรณ์	SW-Cisco-3400
รุ่น	3400
ผู้ขาย	CISCO
OS	IOS 12.0(5)WC10
หน้าที่การทำงาน	สวิตซ์ระดับเลเยอร์สองสำหรับต่อใช้งานผ่าน Leaseline True โดยเชื่อมต่อโครงข่ายคณะเทคโนโลยีสารสนเทศที่ลาดกระบังแบบอีเทอร์เน็ตและเชื่อมต่อไปยังโครงข่ายของคณะที่ตึกชินวัตร3 ผ่านใยแก้วนำแสง (Fiber Optic)

ตารางที่ 3.13 แสดงอุปกรณ์โครงข่าย 13

ชนิดอุปกรณ์	Switch L2
ชื่ออุปกรณ์	F3A1 - F6B
รุ่น	Catalyst 3524
ผู้ขาย	CISCO
OS	IOS 12.0(5)WC10
หน้าที่การทำงาน	สวิตซ์ระดับเลเยอร์สองโดยมีการวางสวิตซ์ทุกชั้น สำหรับการใช้งาน LAN และ WLAN ในชั้นดังกล่าว

ตารางที่ 3.14 แสดงอุปกรณ์โครงข่าย 14

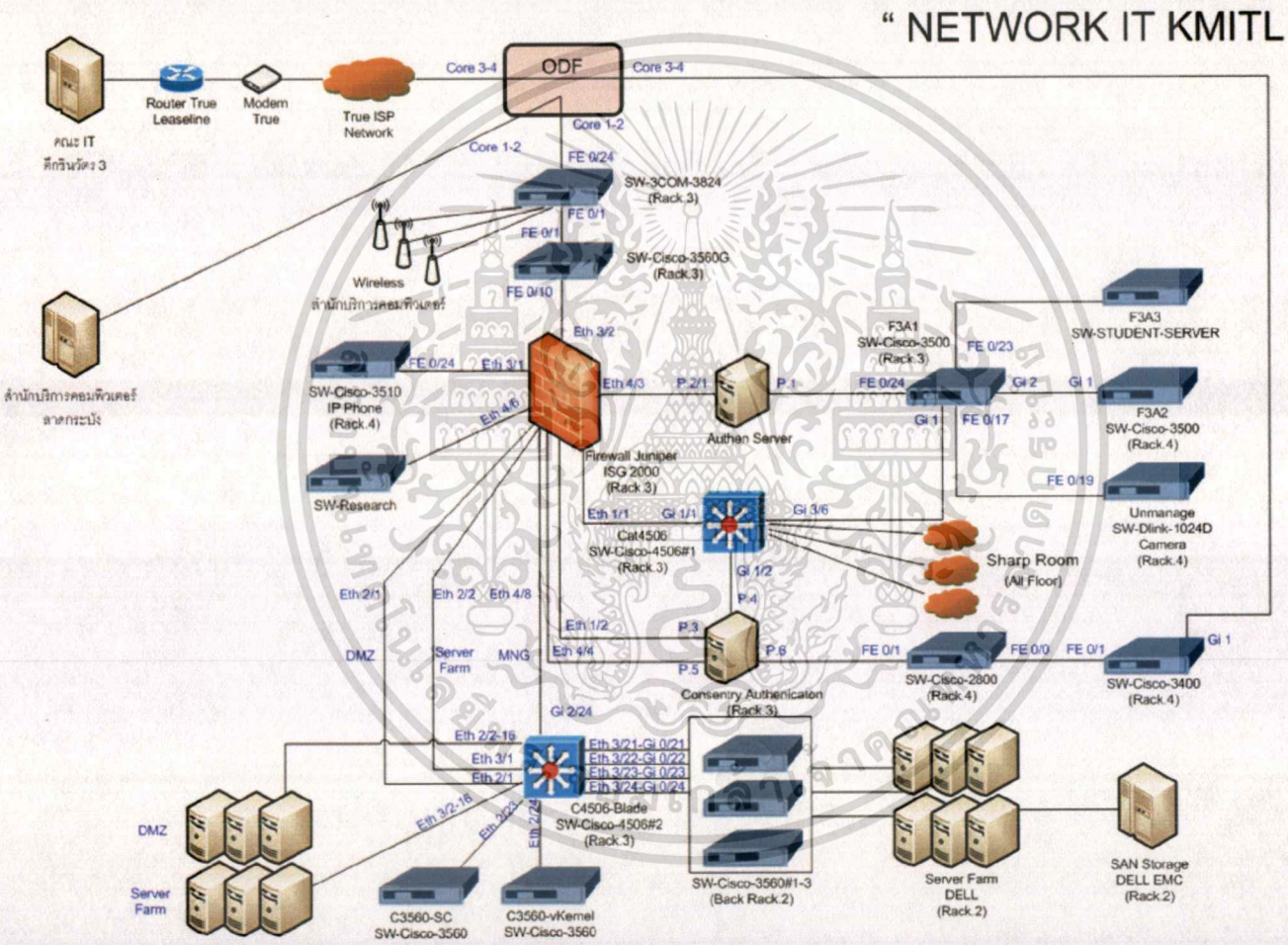
ชนิดอุปกรณ์	Switch L2
ชื่ออุปกรณ์	Research
รุ่น	Catalyst 3524
ผู้ขาย	CISCO
OS	IOS 12.0(5)WC10
หน้าที่การทำงาน	สวิตซ์ระดับเลเยอร์สองสำหรับให้นักศึกษาใช้ในงานวิจัย

นอกจากนั้นภายในคณะมีเครื่องให้บริการต่าง (Server) ภายในคณะ เพื่อบริการแก่นักศึกษา เจ้าหน้าที่และอาจารย์ โดยปัจจุบันเครื่องให้บริการเหล่านี้รองรับการใช้งาน IPv4 โดยมีเครื่องให้บริการดังตารางที่ 3.15

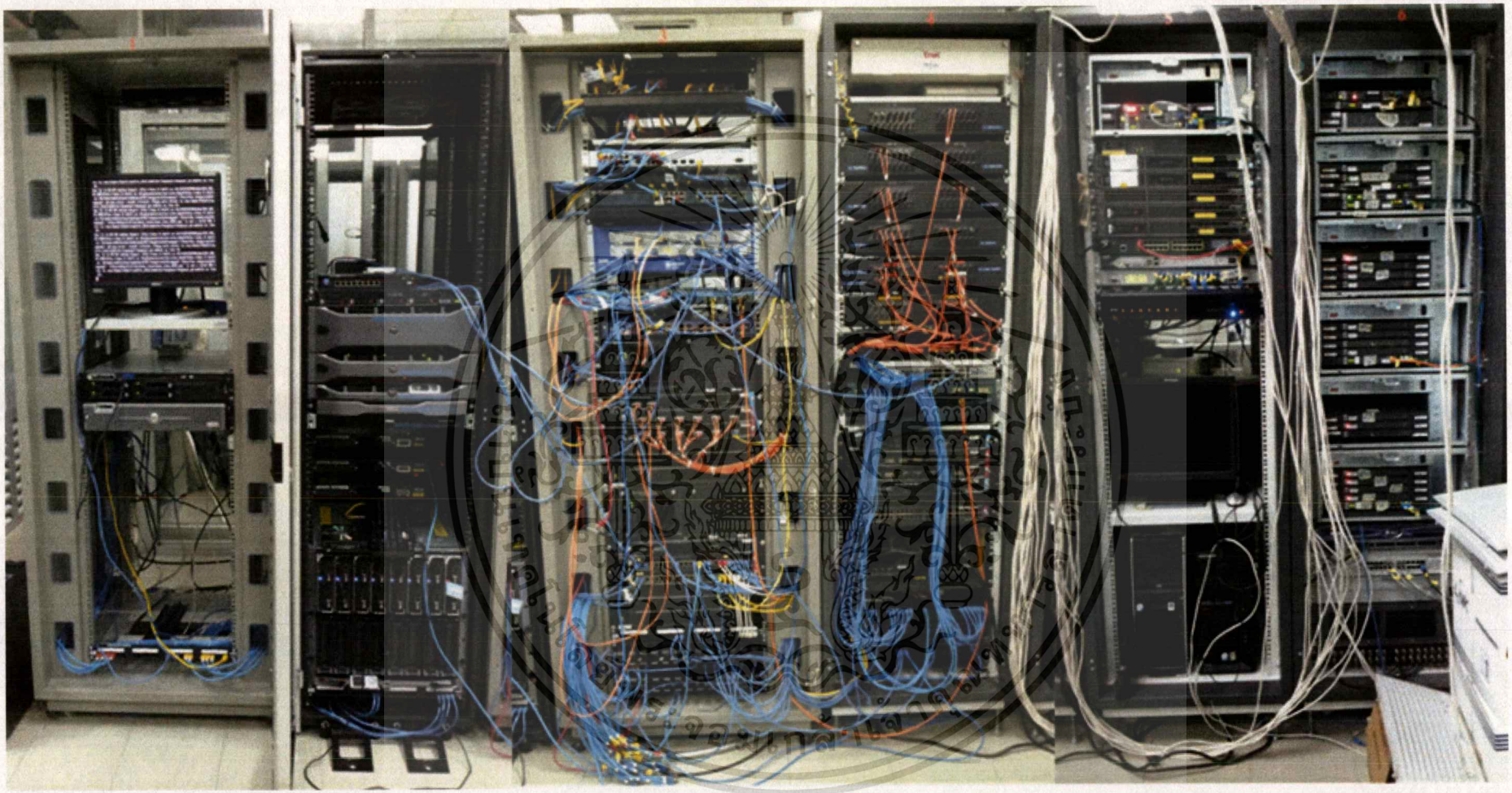
ตารางที่ 3.15 แสดงเครื่องให้บริการ

ชื่อ	**หน้าที่การทำงาน**
HTTP Server	บริการเว็บแก่ผู้ร้องขอด้วยโปรแกรมประเภทเว็บบราวเซอร์ (Web Browser) ที่ร้องขอข้อมูลผ่านโปรโตคอลเฮชทีทีพี ให้บริการข่าวสารข้อมูลภายในคณะ
Mail Server	บริการการรับส่งจดหมายอิเล็กทรอนิกส์(email) ภายในและภายในคณะ
Printer Server	บริการพิมพ์เอกสารสำหรับนักศึกษา เจ้าหน้าทีและอาจารย์ ภายในคณะ
DNS Server	บริการแปลงชื่อเว็บที่ให้บริการเป็นหมายเลขที่อยู่ (IP) เพื่อให้สามารถเข้าถึงเว็บทั้งภายในและภายนอกคณะได้
DHCP Server	บริการแจกหมายเลขที่อยู่ให้กับอุปกรณ์ปลายทาง เช่น คอมพิวเตอร์ ภายในคณะ
Authentication Server	ทำการพิสูจน์ตัวตนและตรวจสอบสิทธิการใช้งานของผู้ใช้งาน

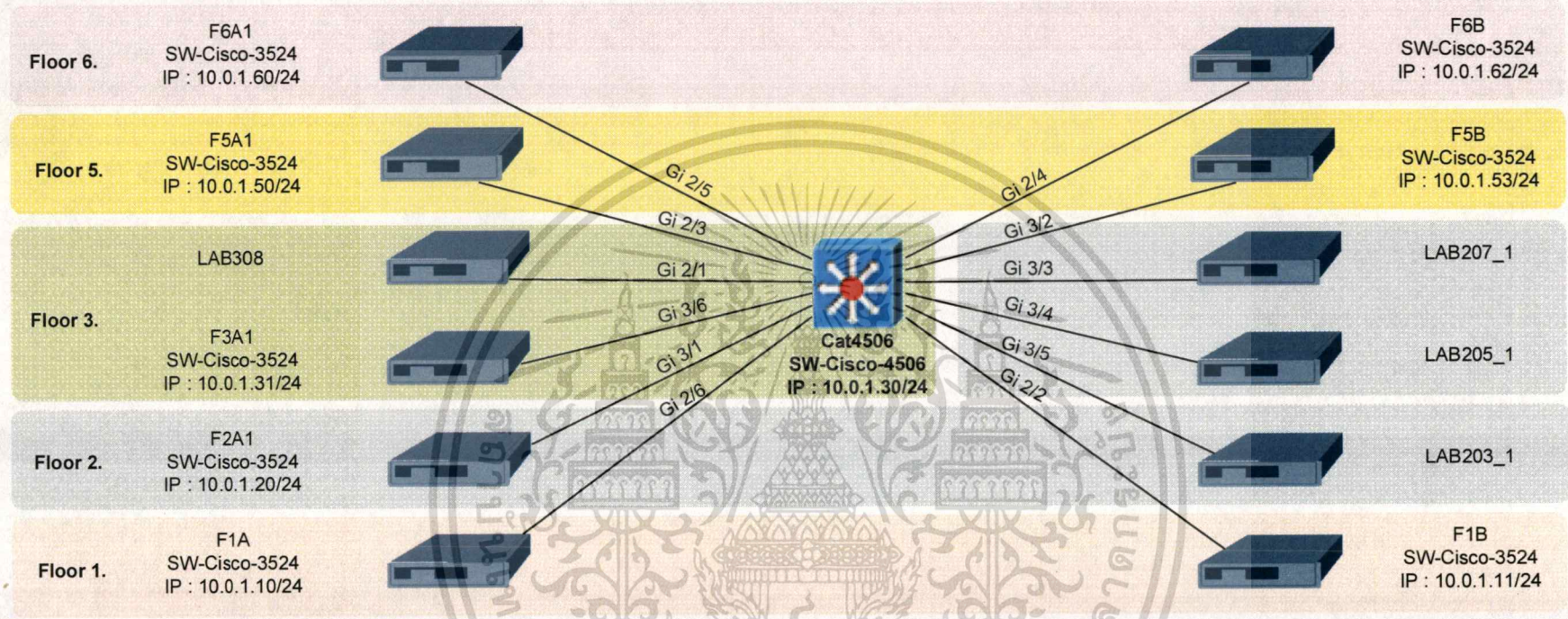
3.2 โครงข่ายคณะเทคโนโลยีสารสนเทศ



รูปที่ 3.1 แสดงระบบโครงข่ายคณะเทคโนโลยีสารสนเทศ



รูปที่ 3.2 แสดงอุปกรณ์ห้องเซิร์ฟเวอร์ชั้น 3



รูปที่ 3.3 แสดงการเชื่อมต่อจากห้องเซิร์ฟเวอร์ไปยังห้องชาร์ปชั้นต่างๆ

บทที่ 4

การออกแบบระบบงานใหม่

4.1 การออกแบบระบบโครงข่าย IPv6

4.1.1 ความต้องการของระบบ

ระบบโครงข่ายใหม่รองรับการใช้งาน IPv6 ได้ สามารถติดต่อสื่อสารกับโครงข่ายเดิมที่มีการใช้งาน IPv4 อุปกรณ์และเครื่องให้บริการ (Server) ภายในคณะซึ่งการใช้งาน IPv4 สามารถรองรับตอบสนองการใช้งานร่วมกับโครงข่าย IPv6 ใหม่ได้ โดยสามารถใช้งานโครงข่ายใหม่ได้ทั้งภายในและภายนอกคณะได้

4.1.2 กลุ่มระบบเป้าหมายสำหรับรองรับโครงข่าย IPv6

ภายในคณะเทคโนโลยีสารสนเทศ มีการให้บริการการเชื่อมโยงเครือข่ายดังนี้

1. LAN ระบบเครือข่ายติดต่อสื่อสารโดยใช้สายเคเบิลเชื่อมต่อถึงกัน
2. Wireless LAN ระบบเครือข่ายติดต่อสื่อสารโดยใช้คลื่นความถี่เชื่อมต่อถึงกัน โดยส่งข้อมูลผ่าน Access Point

การใช้บริการต่างๆ ผ่านเครื่องให้บริการ(Server) ปัจจุบันมีการใช้งาน IPv4 ดังนั้นเพื่อรองรับการใช้ผ่านโครงข่าย IPv6 ให้สามารถใช้งานได้ครอบคลุมทุกการให้บริการ กลุ่มเป้าหมายในการพัฒนา คือ ระบบการเชื่อมโยงเครือข่ายแบบ LAN, Wireless และเครื่องให้บริการดังนี้

1. เครื่องให้บริการเว็บ (Web Server)
2. เครื่องให้แจกหมายเลขที่อยู่(DHCP Server)
3. เครื่องให้บริการ โอนถ่ายข้อมูล (FTP Server)
4. เครื่องให้บริการแปลงชื่อเป็นหมายเลขที่อยู่ (DNS Server)

4.1.3 ทฤษฎีที่เลือกใช้ในการออกแบบ

ทฤษฎีสำหรับการออกแบบโครงข่าย IPv6 ที่นำมาใช้ในการพัฒนามีดังนี้

1. กลวิธีการใช้งาน IPv4 ควบคู่กับ IPv6 (Dual Stack)

การทำงานแบบ Dual Stack ใช้สำหรับการติดต่อสื่อสารระหว่างเครือข่ายที่มีการใช้งาน

อินเทอร์เน็ตโพรโทคอลแบบเดียวกันผ่านเครือข่ายหลักที่มีการใช้อินเทอร์เน็ตโพรโทคอลอีกแบบ โดยอุปกรณ์ที่ขอบของเครือข่าย (Router) จะต้องรองรับการทำงานอินเทอร์เน็ตโพรโทคอลแบบ IPv4 และ IPv6 ในการรับส่งข้อมูล เมื่ออุปกรณ์ได้รับกลุ่มข้อมูลแบบ IPv6 จากต้นทาง จะทำการเพิ่มในส่วนหัวแบบ IPv4 ในกลุ่มข้อมูลเพื่อทำการส่งกลุ่มข้อมูลดังกล่าวผ่านเครือข่ายหลักที่มีการใช้งานอินเทอร์เน็ตโพรโทคอลแบบ IPv4 โดยกำหนดให้อุปกรณ์แต่ละตัวมีหมายเลขที่อยู่ IPv4 และ IPv6 อย่างน้อยละ 1 หมายเลข

2. กลวิธีการทำอุโมงค์ (Tunneling)

การทำงานโดยการสร้างอุโมงค์ เป็นการห่อหุ้มกลุ่มข้อมูลหนึ่งภายในของกลุ่มข้อมูลอีกกลุ่มหนึ่ง เนื่องจากกลุ่มข้อมูลที่ถูกห่อหุ้มภายในไม่สามารถส่งโดยตรงผ่านเครือข่ายไปยังปลายทางได้ เมื่อต้นทางส่วนกลุ่มข้อมูลแบบ IPv6 ไปยังอุปกรณ์เกตเวย์ (Router Gateway) กลุ่มข้อมูลดังกล่าวจะถูกห่อหุ้มด้วยกลุ่มข้อมูลแบบ IPv4 เพื่อทำการส่งข้อมูลผ่านเครือข่ายหลักที่มีการใช้งานอินเทอร์เน็ตโพรโทคอลแบบ IPv4 เมื่อกลุ่มข้อมูลส่งไปถึงอุปกรณ์เกตเวย์อีกฝั่ง จะทำการถอดกลุ่มข้อมูลภายในออกมาเพื่อส่งกลุ่มข้อมูล IPv6 ไปยังปลายทางที่มีการใช้งานผ่านเครือข่าย IPv6

3. กลวิธีการเปลี่ยนแปลงข้อมูล (Translation)

การทำงานโดยการใช้กลวิธีการเปลี่ยนแปลงข้อมูล เป็นวิธีการเปลี่ยนแปลงหมายเลขที่อยู่เสมือนอุปกรณ์หรือคอมพิวเตอร์ปลายทางมีเลขที่อยู่ทั้งแบบ IPv4 และ IPv6 เพื่อใช้สำหรับติดต่อสื่อสารกับเครือข่ายทั้งสองแบบ โดยอุปกรณ์เกตเวย์จะมีการทำ NAT-TP เพื่อแปลงหมายเลขที่อยู่แบบ IPv4 เป็น IPv6 โดยจะมีการบันทึกข้อมูลเลขหมายที่อยู่ที่มีการใช้สำหรับอ้างอิงในการรับส่งข้อมูลข้ามเครือข่ายหลักที่มีการใช้งานอินเทอร์เน็ตโพรโทคอลที่แตกต่างกัน

ตารางที่ 4.1 แสดงกลวิธีที่ใช้ในการออกแบบระบบ

กลวิธีการทำงาน	การเชื่อมต่ออินเทอร์เน็ตโพรโทคอล	ตำแหน่งติดตั้ง
Dual Stack	ระหว่างเครือข่าย IPv4 และ IPv4 ผ่าน IPv6 ระหว่างเครือข่าย IPv6 และ IPv6 ผ่าน IPv4	ในโฮสต์หรืออุปกรณ์เครือข่าย
Tunneling	ระหว่างเครือข่าย IPv6 และ IPv6 ผ่านเครือข่าย IPv4	ระหว่างโฮสต์และอุปกรณ์เครือข่าย
Translation	ระหว่าง IPv4 และ IPv6	ในอุปกรณ์เครือข่าย

ระบบใหม่ : เลือกการเทคนิคทำงานแบบ Tunneling, Dual Stack ในการทำงานร่วมกัน โดยใช้กลวิธี Dual Stack เพื่อให้เครือข่ายเดิมที่มีการใช้งานแบบ IPv4 ยังคงสามารถใช้งานได้เช่นเดิมและเครือข่ายใหม่ที่มีการใช้งานแบบ IPv6 และสามารถใช้งานภายในเครือข่าย IPv6 เองได้ สำหรับเครือข่ายภายในที่มีการใช้งาน IPv6 ที่ต้องการติดต่อสื่อสารร่วมกับเครือข่ายภายนอกแบบ IPv6 นั้นใช้วิธีการทำอุโมงค์ (Tunneling) เพื่อส่งกลุ่มข้อมูลแบบ IPv6 ผ่านเครือข่ายแบบ IPv4 ส่วนกลวิธีการทำงาน Translation รองรับการใช้งานของเครือข่าย IPv6 ที่ต้องการติดต่อสื่อสารร่วมกับเครือข่ายแบบ IPv4

4.1.4 รูปแบบการทำงานแบบอุโมงค์ (Tunneling) ที่เลือกใช้ในการออกแบบ

กลุ่มข้อมูล(Packet) ที่ใช้งานแบบ IPv6 จะถูกทำการห่อหุ้ม (Encapsulate) ภายในกลุ่มของข้อมูลแบบ IPv4 และทำการส่งข้อมูลผ่านระบบโครงข่ายโครงสร้างแบบ IPv4 ในการทำ Tunneling สามารถติดต่อสื่อสารแยกระบบเครือข่ายแบบ IPv6 ออกจากระบบเครือข่ายแบบ IPv4 โดยไม่ต้องทำการเปลี่ยนแปลงโครงสร้างระบบ การทำ Tunnel สามารถสร้างได้ระหว่าง Router แต่ละเครือข่าย ซึ่ง Router ที่ทำการสร้าง Tunnel จะต้องสามารถรองรับการทำงานของโปรโตคอล IPv4 และ IPv6 โดยมีวิธีการสร้าง Tunnel มีดังนี้

1. Manaul

การสร้าง Tunnel โดยระบุอย่างชัดเจนระหว่างเครือข่ายแบบ IPv4 และ IPv6 โดยทำการสร้างเส้นทางระหว่างทั้งสองเครือข่าย การสร้าง Tunnel ทำการสร้างบน Router ที่อยู่ขอบของแต่ละเครือข่ายโดย Router ทั้งสองจะต้องรองรับการทำงานแบบ IPv4 และ IPv6 โดยทำการระบุหมายเลขที่อยู่(IP Address) ทั้งชนิด IPv4 และ IPv6 บน Router ทั้ง 2 ตัว โดยหมายเลขที่อยู่บน Router ทั้งสองตัวจะเป็นเป็นเลขที่อยู่ในวงเดียวและ Router แต่ละตัวจะต้องทราบเลขที่อยู่ของอีกด้าน เพื่อให้สามารถติดต่อกันได้ เมื่อมีการส่งกลุ่มข้อมูล(Packet)แบบ IPv6 ผ่านมายัง Router ที่มีการสร้าง Tunnel กลุ่มข้อมูลเหล่านั้นจะถูกทำการห้อหุ้มด้วยส่วนหัวของ IPv4 และจะถูกส่งผ่านเครือข่าย IPv4 ไปยัง Router ปลายทาง เมื่อ Router ปลายทางได้รับจึงทำการถอดห่อหุ้มเหล่านั้นออก และส่งข้อมูลไปยังเครือข่าย IPv6 ปลายทาง

2. Generic routing encapsulation (GRE)

การส่งข้อมูล IPv6 สามารถส่งผ่าน GRE Tunnel แบบ IPv4 ได้โดยการใช้วิธีมาตรฐานใน

การสร้าง GRE Tunnel ซึ่งได้ออกแบบให้สามารถดำเนินการโครงสร้างการทำงานแบบ point to point ทั่วไปได้การทำ GRE Tunnel สามารถระบุโพรโทคอลในการส่ง ได้เช่น โพรโทคอล IS-IS หรือ IPv6 ที่มีการระบุโพรโทคอลอื่นๆ โดย Router ทั้งสองจะต้องรองรับการทำงานแบบ IPv4 และ IPv6 และการระบุหมายเลขที่อยู่ (IP Address) ทั้งชนิด IPv4 และ IPv6 บน Router

3. 6 to 4 Tunnel

การสร้าง Tunnel 6to4 จะอนุญาตให้สามารถใช้โพรโทคอล IPv6 ผ่านระบบเครือข่าย IPv6 เผื่อติดต่อสื่อสารกับระบบเครือข่าย IPv6 อีกด้าน โดยการทำวิธีนี้เป็นแบบ point to multipoint ซึ่งต่างกับวิธี Manual ที่เป็นแบบ point to point นั่นคือ Router ไม่จำเป็นต้องกำหนดเลขที่อยู่ IPv4 และ IPv6 บน Router ทั้งสอง เนื่องด้วยวิธีนี้จะปฏิบัติโครงสร้าง IPv4 ให้เสมือน NBMA นั้นคือ เลขที่อยู่ IPv4 ถูกฝังอยู่ในเลขที่อยู่ IPv6 โดยจะใช้ในการหาปลายทางของ Tunnel ในการสร้าง Tunnel ที่ Router จะทำการสร้างหมายเลขที่อยู่ IPv6 แบบพิเศษขึ้นมา โดยกำหนดให้ขึ้นต้นด้วย 2002 และตัวด้วยหมายเลขที่อยู่ของ IPv4 ที่แปลงเป็น IPv6 แล้ว โดย Router ที่อยู่ขอบของเครือข่าย จะต้องรองรับการทำงานทั้งแบบ IPv4 และ IPv6

ตารางที่ 4.2 แสดงรูปแบบการทำงานแบบอุโมงค์ (Tunneling)

รูปแบบ Tunneling	ลักษณะการใช้งาน	หมายเหตุ
Manual Configure Tunnel	เป็นแบบ Point to Point เหมาะกับการใช้งานภายในเครือข่าย และใช้งานระหว่างเครือข่าย	สามารถส่งผ่านกลุ่มข้อมูล IPv6 เท่านั้น
GRE Tunnel	เป็นแบบ Point to Point เหมาะกับการใช้งานภายในเครือข่าย และใช้งานระหว่างเครือข่าย	สามารถส่งผ่านกลุ่มข้อมูล IPv6 บริการการส่งผ่านการเชื่อมต่อระหว่างเครือข่าย และสามารถส่งกลุ่มข้อมูลอื่นได้
6 to 4 Tunnel	เป็นแบบ Point to Multi-point ซึ่งแต่ละเครือข่ายมีการใช้งานแบบ IPv6	ต้องระบุ IPv6 แบบพิเศษ ซึ่งกำหนดให้ขึ้นต้นด้วย 2002 และตัวด้วยหมายเลขที่อยู่ของ IPv4 ที่แปลงเป็น IPv6

ระบบใหม่ : เลือกวิธีการสร้าง Tunneling แบบ Manual กำหนดให้อุปกรณ์เกตเวย์มีหมายเลขที่อยู่แบบ IPv4 และ IPv6 อย่างละ 1 หมายเลข โดยสร้างอุโมงค์ระหว่างอุปกรณ์เกตเวย์ของคณะและอุปกรณ์เกตเวย์ของผู้ให้บริการอินเทอร์เน็ต เนื่องด้วยการทำงานของอุปกรณ์เกตเวย์ในคณะเป็นลักษณะแบบ Point to Point ดังนั้นกลวิธีแบบอุโมงค์โดยใช้รูปแบบ Manual จะมีความซับซ้อนและยุ่งยากน้อยกว่าแบบ 6 to 4 ซึ่งมีลักษณะการทำงานแบบ Point to Multipoint และการส่งข้อมูลไปยังผู้ให้บริการอินเทอร์เน็ตมีการใช้งานโพรโทคอลการจัดเส้นทางแบบระบุชัดเจน (Static) ไม่ได้มีการใช้งานโพรโทคอลอื่นๆ จึงไม่จำเป็นต้องใช้รูปแบบ GRE แต่ข้อจำกัดของการทำอุโมงค์ คือ จะไม่สามารถกำหนดขนาดของกลุ่มข้อมูล (MTU) ในเครือข่ายหลัก IPv4 ที่ส่งข้อมูลผ่านได้

ตารางที่ 4.3 แสดงการเปรียบเทียบวิธีการออกแบบ

วิธีการ	ข้อดี	ข้อเสีย
Dual Stack	- การปรับปรุงระบบสามารถดำเนินการได้โดยไม่จำเป็นต้องเปลี่ยนแปลงแก้ไขเครือข่ายทั้งหมด	- ต้นทุนและทรัพยากรด้านฮาร์ดแวร์และซอฟต์แวร์ที่มีประสิทธิภาพเพิ่มขึ้น
	- การใช้งานโดยส่วนใหญ่มีการใช้งานทั้ง IPv4 และ IPv6 รวมกัน จึงสามารถตอบความตอบความต้องการได้	- อุปกรณ์ทุกตัวที่ทำจะต้องรองรับทั้ง IPv6 และ IPv4 ในกรณีที่อุปกรณ์ไม่รองรับจำเป็นต้องอัพเกรด
		- ไม่สามารถปรับขนาดได้
Tunneling	- ไม่จำเป็นต้องมีการปรับปรุงระบบโครงสร้างเดิมที่มีอยู่	- การจัดการผ่าน Tunneling เท่านั้น
	- ไม่กระทบต่อการใช้งาน IPv4	- ไม่สามารถปรับขนาดได้
	- การเชื่อมต่อโครงข่าย IPv6 จะดำเนินการผ่านโครงสร้างระบบ IPv4 เดิม	- ต้องการอุปกรณ์ Router ที่มีประสิทธิภาพ รองรับปริมาณการใช้งานได้สูง
Translation	- รองรับการสื่อสารระหว่าง IPv6 และ IPv4 ได้ในกรณีที่ไม่สามารถใช้วิธี Dual Stack และ Tunneling ได้	- จำเป็นต้องมีเซิร์ฟเวอร์ NAT
		- ไม่สามารถปรับขนาดได้

4.1.5 แนวทางและวิธีการการพัฒนาระบบ

ในการออกแบบระบบโครงข่ายได้ออกแบบ 2 แผน ดังนี้

1. การทำ Tunneling และ Dual Stack ไปยังผู้ให้บริการ

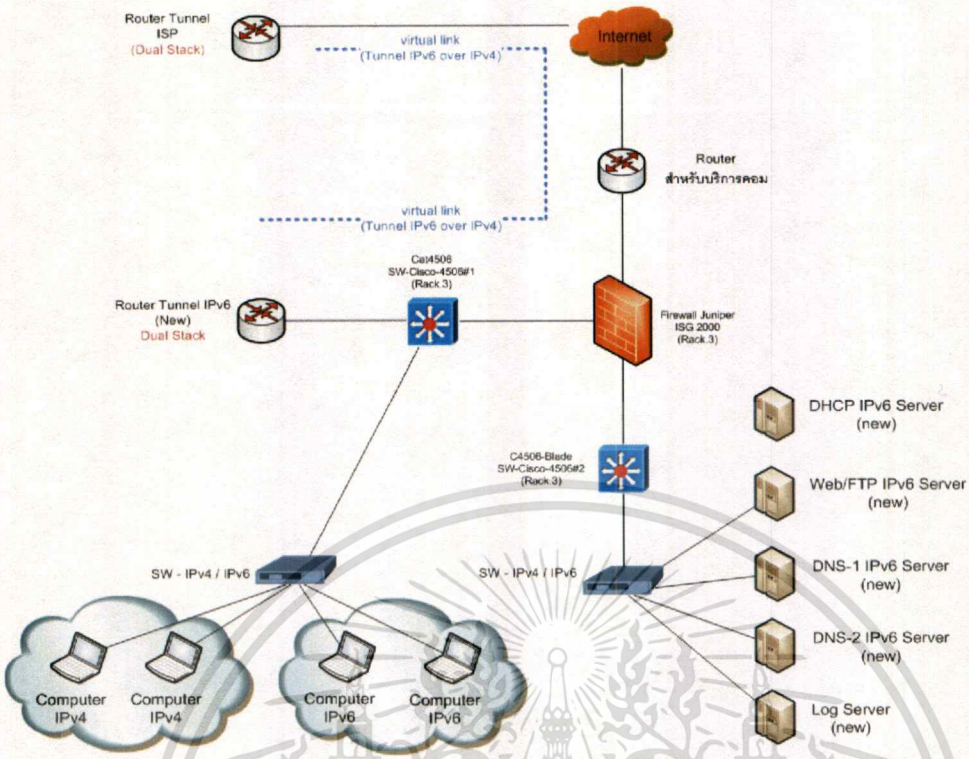
2. การทำ Dual Stack ไปยังผู้ให้บริการ

วิธีที่ 1 การทำ Tunneling และ Dual Stack ไปยังผู้ให้บริการ

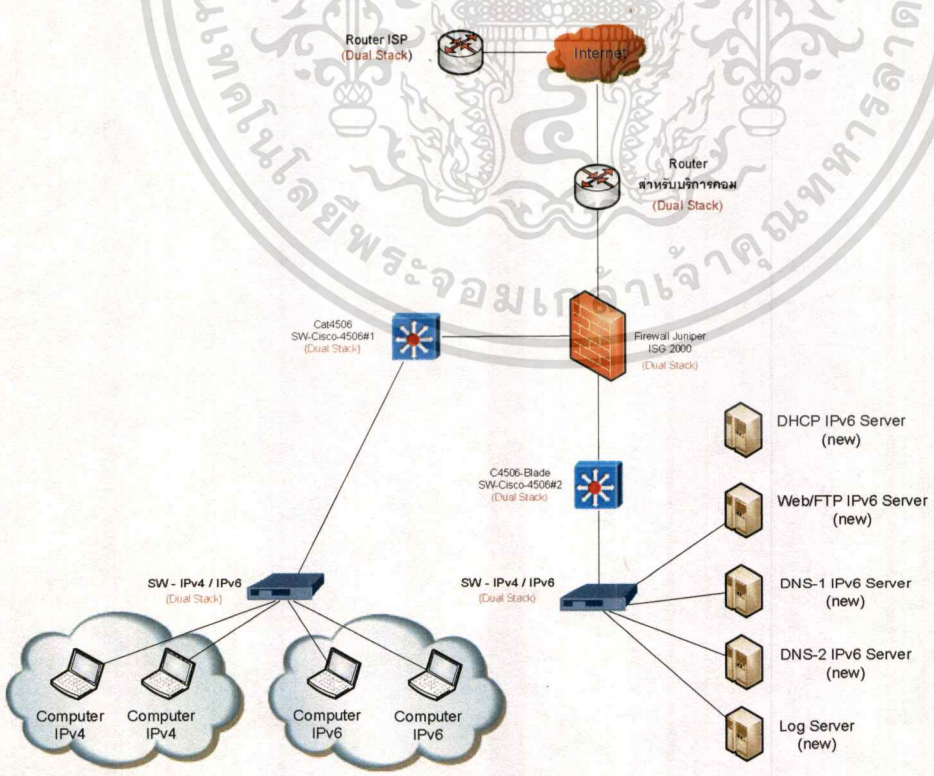
ระบบโครงข่ายใหม่ออกแบบให้รองรับการใช้งานโพรโทคอล IPv6 เพิ่มขึ้น โดยยังคงให้สามารถใช้งานโพรโทคอลเดิม IPv4 ได้ โดยทำการติดตั้งอุปกรณ์เพิ่มคือ เร้าเตอร์ CISCO รุ่น 2811 เพื่อทำหน้าที่เป็นเร้าเตอร์ที่ทำการสร้างท่อ (Tunnel) ไปยังผู้ให้บริการที่รองรับการใช้งาน IPv6 เช่น NECTEC , 3BB และทำการส่งเส้นทาง(Routing) เพื่อแลกข้อมูลสื่อสารกัน และทำให้สามารถใช้งานอินเทอร์เน็ตโพรโทคอล IPv6 ได้ โดยกลุ่มข้อมูลจากโครงข่าย IPv6 ต้นทางจะสามารถส่งไปยังโครงข่าย IPv6 ปลายทาง โดยผ่านท่อ (Tunnel) ที่มีการใช้งานโพรโตคอล IPv4

วิธีที่ 2 การทำ Dual Stack ไปยังผู้ให้บริการ

ระบบโครงข่ายใหม่ออกแบบให้รองรับการใช้งานโพรโทคอล IPv6 เพิ่มขึ้น โดยยังคงให้สามารถใช้งานโพรโทคอลเดิม IPv4 ได้ โดยทำการติดตั้งอุปกรณ์เพิ่มคือ เร้าเตอร์ CISCO รุ่น 2811 สำหรับแผนที่ 2 ออกแบบให้มีการทำ Dual Stack ตลอดเส้นทาง ได้แก่เร้าเตอร์ของคณะฯ เร้าเตอร์ของสำนักบริการคอมพิวเตอร์ และเร้าเตอร์ของผู้ให้บริการ ดังนั้นเร้าเตอร์ทั้งหมดจะต้องมีเลขที่อยู่ทั้ง IPv4 และ IPv6 เพื่อให้สามารถใช้งานอินเทอร์เน็ตได้ โดยระบบที่ใช้งาน IPv4 สามารถใช้งานผ่านโครงข่าย IPv4 ได้และระบบที่ใช้งาน IPv6 สามารถใช้งานผ่านโครงข่าย IPv6 ได้เช่นกัน



รูปที่ 4.1 การออกแบบระบบโครงข่ายใหม่สนับสนุน IPv6 วิธีที่ 1



รูปที่ 4.2 การออกแบบระบบโครงข่ายใหม่สนับสนุน IPv6 วิธีที่ 2

ในการพัฒนาเพื่อปรับปรุงโครงข่ายเดิมที่มีการใช้งานเครือข่ายแบบ IPv4 ให้มีการสามารถใช้งานเครือข่ายแบบ IPv6 และสามารถติดต่อสื่อสารระหว่างเครือข่ายทั้งสองแบบได้ จำเป็นต้องติดตั้งอุปกรณ์เกตเวย์ที่รองรับการทำงานเครือข่ายแบบ IPv6 โดยอุปกรณ์จะรองรับการทำงานต่างๆดังนี้

1. กำหนดเกตเวย์ให้กับเครือข่ายย่อย

ทำหน้าที่แบ่งเครือข่ายย่อย IPv6 สำหรับใช้งานในคณะ โดยแบ่งตามเครือข่ายของห้องต่างๆ เช่น ห้องเรียน ห้องทำงาน ห้องแลป และกำหนดให้เกตเวย์ของเครือข่ายย่อมดังกล่าวอยู่บนอุปกรณ์เกตเวย์ ปัจจุบันเกตเวย์ของเครือข่าย IPv4 เหล่านี้กำหนดไว้บน Firewall ISG2000

2. สร้างอุโมงค์ (Tunnel) เชื่อมต่อกับผู้ให้บริการ

เพื่อสร้างการเชื่อมต่อระหว่างเครือข่ายของคณะและเครือข่ายของผู้ให้บริการอินเทอร์เน็ตรองรับการติดต่อสื่อสารระหว่างเครือข่าย IPv6 ภายในคณะกับเครือข่าย IPv6 ภายนอก และยังรองรับการติดต่อสื่อสารระหว่างเครือข่าย IPv6 ภายในคณะกับเครือข่าย IPv4 ภายนอก

3. จัดการและควบคุมเส้นทางการรับส่งข้อมูล

ทำหน้าที่จัดการและควบคุมเส้นทางในตารางข้อมูล (Routing Table) ระหว่างอุปกรณ์เครือข่ายต่างๆที่ทำงานในระดับชั้นเครือข่าย เพื่อให้อุปกรณ์เหล่านี้สามารถส่งข้อมูลไปยังคอมพิวเตอร์หรืออุปกรณ์ปลายทางได้อย่างถูกต้อง

4. จัดการควบคุมความปลอดภัย IPv6 จากเครือข่ายภายนอก (Security)

5. จัดการควบคุมกฎการเข้าถึงและการกรองการรับส่งข้อมูล (Filter/Access List)

ควบคุมสิทธิการเข้าถึงกลุ่มเครือข่ายย่อยต่างๆ โดยสามารถควบคุมได้จากหมายเลขที่อยู่ หมายเลขพอร์ต โพรโทคอล

6. สร้างวิธีการNAT64

ทำหน้าที่ในการแปลงหมายเลขที่อยู่แบบ IPv4 และ IPv6 ให้เครือข่ายทั้งสองสามารถติดต่อสารข้ามเครือข่ายได้ โดยให้อุปกรณ์เกตเวย์ที่มีการเชื่อมต่อระหว่างเครือข่าย IPv4 และ IPv6 ทำหน้าในการแปลงหมายเลขที่อยู่ ทำให้ต้นทางจากเครือข่าย IPv46 สามารถส่งข้อมูลติดต่อสื่อสารกับเครือข่าย IPv4 ได้

7. สร้างวิธีการ DNS64 (Domain Name Server 6 to 4)

กำหนดให้มี DNS64 เพื่อรองรับการทำงานของเครือข่าย IPv6 เมื่อต้องการเข้าเว็บที่มีการ

ใช้งานแบบ IPv4 โดย DNS64 จะบันทึกข้อมูลหมายเลขที่อยู่เว็บแบบ IPv4 เพื่อตอบกลับไปยังผู้ใช้งานในเครือข่าย IPv6 ที่มีการร้องขอหมายเลขที่อยู่ว่าจะต้องติดต่อไปยังหมายเลขที่อยู่ใดเพื่อให้สามารถรับการใช้งานเว็บนั้นได้

การทำงานของอุปกรณ์เกตเวย์ข้างต้น กำหนดให้มีการทำงานบนอุปกรณ์จัดเส้นทาง (Router Cisco) สำหรับการทำงานทั้งหมดสามารถแบ่งแยกทำงานบนอุปกรณ์จัดเส้นทางคนละตัวหรือใช้อุปกรณ์จัดเส้นทางเพียงตัวเดียวในการทำหน้าที่ทั้งหมด ซึ่งได้ทำการเปรียบเทียบข้อดีข้อเสียการทำงานบนอุปกรณ์จัดเส้นทาง 2 ตัวและ 1 ตัว ตามตารางที่ 4.3

ระบบใหม่ได้แบ่งหน้าที่การทำงานของ Router ดังนี้

1. Router 1 : Router Tunnel
   - สร้างอุโมงค์ (Tunnel) เชื่อมต่อกับผู้ให้บริการ
   - จัดการควบคุมความปลอดภัย IPv6 จากเครือข่ายภายนอก (Security)
   - สร้างวิธีการNAT64
2. Router 2 : Router Gateway
   - กำหนดเกตเวย์ให้กับเครือข่ายย่อย
   - จัดการและควบคุมเส้นทางการรับส่งข้อมูลในคณะ
   - จัดการควบคุมกฎการเข้าถึงและการกรองการรับส่งข้อมูล (Filter/Access List)

ตารางที่ 4.4 แสดงการเปรียบเทียบข้อดีข้อเสียการทำงานบนอุปกรณ์จัดเส้นทาง 2 ตัวและ 1 ตัว

หัวข้อ	การทำงานบน Router 1 ตัว	การทำงานบน Router 2 ตัว
ต้นทุน (Cost)	ต้นทุนต่ำกว่า	ต้นทุนสูงด้วยจำนวน Router ที่และการ์ด Interface มากกว่า
การเชื่อมโยง (Link)	ลดการเชื่อมโยงไปยังอุปกรณ์ด้วยใยแสงนำแก้วหรือสายแลน	การเชื่อมโยงไปยังอุปกรณ์เพิ่มขึ้นหากปริมาณการใช้งานเพิ่มขึ้นต้องเพิ่มมากกว่ากรณีใช้ Router 1 ตัวถึงสองเท่า

ตารางที่ 4.4 (ต่อ)

หัวข้อ	การทำงานบน Router 1 ตัว	การทำงานบน Router 2 ตัว
ภาระการทำงาน (Load)	- ภาระการทำงานเพิ่มขึ้น	- แบ่งแยกหน้าที่การทำงานอย่างชัดเจน
	- หน้าที่การทำงานที่เพิ่มขึ้น	- ลดภาระการทำงาน เช่น การประมวลผล คำนวณเส้นทาง
	- จำนวน Routing ที่มาก ใช้เวลาในการคำนวณและประมวลผลเส้นทางมากขึ้น ตารางเส้นทางมีขนาดใหญ่มีผลต่อการประมวลผล	- ลดการใช้งานทรัพยากรที่มีอยู่ เช่น หน่วยประมวลผล (CPU) หน่วยความจำ (RAM)
	- การทำงานส่วนห่อหุ้มกลุ่มข้อมูล (Encapsulation) และการถอดส่วนที่ห่อหุ้มกลุ่มข้อมูลที่ได้รับมา (De-encapsulation) ส่งผลต่อการทำงานของหน่วยประมวลผล (CPU) ที่เพิ่มขึ้น และจำเป็นต้องใช้ทรัพยากรที่มีเพิ่มขึ้นด้วย เช่น หน่วยความจำ (RAM)	
ปริมาณ MAC - Address	มีปริมาณมาก เก็บข้อมูลจำนวน MAC-Address ทั้งหมดที่ใช้งาน	มีปริมาณน้อยกว่า Router อีกตัวที่ไม่ได้ทำหน้าที่เป็นเกตเวย์ มีการเก็บข้อมูล MAC-Address เฉพาะอุปกรณ์ที่มีติดต่อกันโดยตรงเท่านั้น
วิเคราะห์ปัญหา/แก้ไขเหตุเสีย	การกำหนด Configuration ทั้งหมดอยู่บน Router เพียงตัวเดียว หากเกิดปัญหาจะกระทบต่อหน้าที่การทำงานทั้งหมด	- มีการทำงานที่แบ่งแยกชัดเจน สามารถตรวจสอบปัญหาที่เกิดขึ้นได้เร็วกว่า
		- ลดผลกระทบจากปัญหาที่เกิดขึ้น หากหน้าที่การทำงานบางอย่างผิดพลาด จะไม่กระทบต่อหน้าที่อีกส่วนที่อยู่บน Router

4.2 ความเสี่ยงและผลกระทบ

การพัฒนาระบบเครือข่ายให้สามารถรองรับการทำงานโดยใช้อินเทอร์เน็ตโพรโทคอลรุ่นที่ 6 (IPv6) สามารถติดตั้งเพิ่มเติมเพื่อทดสอบภายในเครือข่าย IPv6 ได้และสามารถติดตั้งเชื่อมต่อกับระบบเดิมที่มีการใช้งานโดยใช้อินเทอร์เน็ตโพรโทคอลรุ่นที่ 4 (IPv4) ในการติดตั้งระบบใหม่จะไม่ส่งผลกระทบต่อการใช้งานเดิมในเครือข่าย IPv4 เนื่องด้วยได้แยกอุปกรณ์เกตเวย์ของเครือข่าย IPv6 ออกมาต่างหาก และทำการสร้างอุโมงค์ (Tunnel) สำหรับเป็นท่อเพื่อออกไปให้ผู้ให้บริการ เสมือนเป็นเส้นทางตรงของเครือข่าย IPv6 ออกสู่เครือข่ายภายนอก

สำหรับการติดตั้งหรือแก้ไขการกำหนดค่าต่างๆของIPv6 สามารถกระทำได้โดยไม่กระทบเครือข่าย IPv4 เดิม สำหรับการกำหนดค่าเพิ่มเติมในอุปกรณ์เดิม (Switch) ในเครือข่าย IPv4 ที่เชื่อมต่อไปยังเครือข่ายย่อยต่างๆ เพื่อให้สามารถใช้งานเครือข่าย IPv6 ผ่านอุปกรณ์ได้นั้น สามารถกระทำได้โดยไม่กระทบผู้ใช้งานในเครือข่ายเดิมเช่นกัน

อุปกรณ์ไฟร์วอลล์ของคณะและ Router ของสำนักบริการคอมพิวเตอร์ยังคงใช้งาน IPv4 เช่นเดิม ซึ่งเป็นการส่งกลุ่มข้อมูลแบบ IPv6 ผ่านโครงข่ายเดิมที่มีการใช้งาน IPv4 ดังนั้นการพัฒนาระบบเครือข่ายให้สามารถรองรับการทำงานแบบ IPv6 นั้นสามารถกระทำได้ ไม่กระทบต่อระบบเครือข่าย IPv4 เดิม หากมีการแก้ไขหรือทดสอบการทำงานของ IPv6 จะกระทบเฉพาะผู้ที่ใช้งานเครือข่าย IPv6 เท่านั้น

บทที่ 5

การพัฒนาและการทำงานของระบบ

5.1 การเตรียมความพร้อมระบบ

5.1.1 สำรวจความพร้อมอุปกรณ์และโครงข่ายเดิม

การตรวจสอบความพร้อมในระบบโครงข่าย IPv4 เดิม ทำการตรวจสอบความพร้อมของอุปกรณ์ทั้งหมด ทั้งในส่วนของสวิตซ์ เร้าเตอร์และไฟร์วอลล์ โดยทำการตรวจสอบด้านฮาร์ดแวร์และซอฟต์แวร์ เพื่อเก็บข้อมูลการรองรับการใช้งาน IPv6 รวบรวมข้อมูลใช้สำหรับการออกแบบระบบโครงข่าย IPv6 ใหม่ ดังนี้

ตารางที่ 5.1 แสดงความพร้อมด้านฮาร์ดแวร์และซอฟต์แวร์ของอุปกรณ์

ข้อมูลอุปกรณ์				รองรับ IPv6		
ชนิดอุปกรณ์	ผู้จำหน่าย	ฮาร์ดแวร์	ซอฟต์แวร์	ฮาร์ดแวร์	ซอฟต์แวร์	อัพเกรดเพื่อรองรับ
Firewall	Juniper	NSISG2000	ScreenOS 6.2.0r4.0	ไม่รองรับ	ไม่รองรับ	
Core Switch	Cisco	Catalyst 4506	IOS 12.1(13)EW2	รองรับ	ไม่รองรับ Dual Stack	IOS 12.2(20)EW
Switch L2	Cisco	S3560	IOS 12.2(35)SE5	รองรับ	ไม่รองรับ Dual Stack	IOS 12.4
Switch L2	Cisco	S3524	IOS 12.0(5)WC10	รองรับ	ไม่รองรับ Dual Stack	IOS 12.4
Switch L2	Cisco	S2800	IOS 12.4(11)T2	รองรับ	รองรับ	

5.1.2 สำรวจอุปกรณ์ที่ติดตั้งเพิ่ม

ในการวางระบบโครงข่ายใหม่มีการติดตั้งอุปกรณ์เร้าเตอร์เพิ่มเพื่อให้สามารถรองรับการใช้งาน IPv6 เพื่อสำหรับเป็นเกตเวย์ IPv6 ให้กับเครือข่ายย่อยทั้งแบบ LAN และ Wireless LAN อุปกรณ์เร้าเตอร์ทำการสร้างอุโมงค์ไปยังผู้ให้บริการอินเทอร์เน็ต (ISP) ทำหน้าที่การจัดการเส้นทางการรับส่งข้อมูล ทั้งยังดูแลความปลอดภัย การเข้าถึงสิทธิเครือข่ายและอุปกรณ์ต่างๆ โดยอุปกรณ์เร้าเตอร์ติดตั้งเพิ่ม ดังนี้

ตารางที่ 5.2 แสดงข้อมูลเร้าเตอร์ในการติดตั้งเพิ่ม

รุ่น	CISCO 2811
หน่วยความจำภายใน	256 MB
หน่วยความจำภายนอก	64M
ข้อมูลซอฟต์แวร์	Cisco IOS Software, 2800 Software (C2800NM-ADVENTERPRISEK9-M)
	Version 12.4(11)T2, RELEASE SOFTWARE (fc4)
	ROM: Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M)
	Version 12.4(12), RELEASE SOFTWARE (fc1)

นอกจากนั้นทำการติดตั้งอุปกรณ์ให้บริการ (Server) เพิ่ม เพื่อทดสอบและให้บริการต่างๆ เช่น บริการเว็บ บริการรับส่งอีเมล์ บริการเครื่องพิมพ์เอกสาร บริการแปลงข้อมูลชื่อเป็นหมายเลขที่อยู่ ทำหน้าที่บริการต่างๆให้กับระบบโครงข่าย IPv6 ใหม่ โดยมีการติดตั้งเพิ่มดังนี้

ตารางที่ 5.3 แสดงข้อมูลเซิร์ฟเวอร์ในการทดสอบ

ผู้ขาย	Dell
รุ่น	PowerEdge R410
หน่วยประมวลผลกลาง	Intel(R) CPU E5620 @2.40GHz
หน่วยประมวลผล	8 Core
หน่วยความจำภายใน	16G
หน่วยเก็บข้อมูล	750G

5.2 ข้อจำกัดในการพัฒนาระบบ

1. การพัฒนาระบบโครงข่าย IPv6 บนระบบโครงข่ายปัจจุบัน IPv4 ซึ่งมีการใช้งานอยู่ ซึ่งอุปกรณ์ปัจจุบันมีอายุการใช้งานสูง ในส่วนของฮาร์ดแวร์และซอฟต์แวร์ในบางอุปกรณ์ไม่รองรับการใช้งาน IPv6 เช่น ไฟร์วอลล์ซึ่งเป็นอุปกรณ์หลักในการใช้งานเครือข่ายปัจจุบัน และในบางอุปกรณ์ เช่น สวิตซ์ ทั้งที่สำหรับเป็นอุปกรณ์กลางเชื่อมต่อไปยังอุปกรณ์ปลายทางอื่นๆ และสวิตซ์

ปลายทางที่เชื่อมต่อเครือข่ายย่อยของห้องต่างๆ มีความสามารถในรองรับ IPv6 เพียงแค่พื้นฐานเท่านั้น ดังนี้จึงจำเป็นต้องติดตั้งอุปกรณ์เพิ่มที่มีความสามารถในการรองรับการทำงาน IPv6 มากขึ้น

2. ในการพัฒนาระบบเพิ่มการใช้งาน IPv6 กับระบบปัจจุบัน สำหรับในส่วนของเครื่องให้บริการ (Server) ต่างๆภายในคณะเช่น บริการเว็บ บริการรับส่งอีเมล์ บริการเครื่องพิมพ์เอกสาร บริการแปลงข้อมูลชื่อเป็นหมายเลขที่อยู่ เพื่อให้การบริการเหล่านี้สามารถรองรับการใช้งาน IPv6 ได้ จะต้องทำการแก้ไขและเพิ่มหมายเลขที่อยู่ IPv6 เพื่อตอบสนองความต้องการการใช้งานบริการได้ทั้งในเครือข่าย IPv4 และ IPv6

3. การพัฒนาระบบเพื่อให้สามารถใช้งาน IPv6 ได้จะต้องได้รับการจัดสรรหมายเลขที่อยู่ IPv6 จากผู้ให้บริการอินเทอร์เน็ต ซึ่งสถาบันเทคโนโลยีพระจอมเกล้า เจ้าคุณทหารลาดกระบัง ได้มีการใช้บริการอินเทอร์เน็ตผ่านผู้ให้บริการชื่อทรู (True) โดยสถาบันฯจะได้รับหมายเลขการจัดสรร IPv6 จากทรู และจะจัดสรรแก่คณะต่างๆ ภายในสถาบัน

เนื่องด้วยการจัดสรรหมายเลขที่อยู่ IPv6 จากสถาบันล่าช้า ทางผู้จัดทำได้ขอความร่วมมือจากผู้ให้บริการอินเทอร์เน็ตชื่อสามบีบี (3BB) เพื่อขอทดสอบการใช้งาน IPv6 ภายในคณะซึ่งได้รับการจัดสรรดังนี้

หมายเลข IPv6 สำหรับการทดสอบ 2403:6200:FFF1::/48

สำหรับเครือข่ายย่อยภายในคณะทั้งแบบ LAN และ wireless เพื่อให้สามารถใช้งาน IPv6 ได้ จึงมีการกำหนดเครือข่ายย่อยต่างๆ โดยทำการแบ่งหมายเลขที่อยู่ IPv6 ที่ได้รับการจัดสรรมา ดังนี้

ตารางที่ 5.4 แสดงการแบ่งหมายเลขที่อยู่ IPv6

Floor	VLAN	Subnet IPv4	Subnet IPv6
			2403:6200:FFF1::/48
FL. 1	103	10.10.3.1/24	2403:6200:FFF1:67::/64
FL. 1	106	10.10.6.1/24	2403:6200:FFF1:6A::/64
FL. 1	111	10.10.11.1/24	2403:6200:FFF1:6F::/64
FL. 1	114	10.10.14.1/24	2403:6200:FFF1:72::/64
FL. 2	203	10.20.3.1/24	2403:6200:FFF1:CB::/64
FL. 2	205	10.20.5.1/24	2403:6200:FFF1:CD::/64
FL. 2	207	10.20.7.1/24	2403:6200:FFF1:CF::/64
FL. 2	209	10.20.9.1/24	2403:6200:FFF1:D1::/64

ตารางที่ 5.4 (ต่อ)

Floor	VLAN	Subnet IPv4	Subnet IPv6
			2403:6200:FFF1::/48
FL. 2	218	10.20.18.1/24	2403:6200:FFF1:DA::/64
FL. 2	219	10.20.19.1/24	2403:6200:FFF1:DB::/64
FL. 2	220	10.20.20.1/24	2403:6200:FFF1:DC::/64
FL. 2	221	10.20.21.1/24	2403:6200:FFF1:DD::/64
FL. 2	222	10.20.22.1/24	2403:6200:FFF1:DE::/64
FL. 2	223	10.20.23.1/24	2403:6200:FFF1:DF::/64
FL. 2	224	10.20.24.1/24	2403:6200:FFF1:E0::/64
FL. 2	225	10.20.25.1/24	2403:6200:FFF1:E1::/64
FL. 2	226	10.20.26.1/24	2403:6200:FFF1:E2::/64
FL. 2	231	10.20.31.1/24	2403:6200:FFF1:E7::/64
FL. 2	232	10.20.32.1/24	2403:6200:FFF1:E8::/64
FL. 3	304	10.30.4.1/24	2403:6200:FFF1:130::/64
FL. 3	306	10.30.6.1/24	2403:6200:FFF1:132::/64
FL. 3	308	10.30.8.1/24	2403:6200:FFF1:134::/64
FL. 3	310	10.30.10.1/24	2403:6200:FFF1:136::/64
FL. 3	316	10.30.16.1/24	2403:6200:FFF1:13C::/64
FL. 3	317	10.30.17.1/24	2403:6200:FFF1:13D::/64
FL. 3	323	10.30.23.1/24	2403:6200:FFF1:143::/64
FL. 3	324	10.30.24.1/24	2403:6200:FFF1:144::/64
FL. 3	325	10.30.25.1/24	2403:6200:FFF1:145::/64
FL. 3	326	10.30.26.1/24	2403:6200:FFF1:146::/64
FL. 3	328	10.30.28.1/24	2403:6200:FFF1:148::/64
FL. 3	329	10.30.29.1/24	2403:6200:FFF1:149::/64
FL. 3	330	10.30.30.1/24	2403:6200:FFF1:14A::/64
FL. 3	331	10.30.31.1/24	2403:6200:FFF1:14B::/64
FL. 3	332	10.30.32.1/24	2403:6200:FFF1:14C::/64

ตารางที่ 5.4 (ต่อ)

Floor	VLAN	Subnet IPv4	Subnet IPv6
			2403:6200:FFF1::/48
FL. 3	333	10.30.33.1/24	2403:6200:FFF1:14D::/64
FL. 3	334	10.30.34.1/24	2403:6200:FFF1:14E::/64
FL. 3	335	10.30.35.1/24	2403:6200:FFF1:14F::/64
FL. 3	336	10.30.36.1/24	2403:6200:FFF1:150::/64
FL. 5	503	10.50.3.1/24	2403:6200:FFF1:1F7::/64
FL. 5	504	10.50.4.1/24	2403:6200:FFF1:1F8::/64
FL. 5	505	10.50.5.1/24	2403:6200:FFF1:1F9::/64
FL. 5	506	10.50.6.1/24	2403:6200:FFF1:1FA::/64
FL. 5	507	10.50.7.1/24	2403:6200:FFF1:1FB::/64
FL. 5	508	10.50.8.1/24	2403:6200:FFF1:1FC::/64
FL. 5	509	10.50.9.1/24	2403:6200:FFF1:1FD::/64
FL. 5	510	10.50.10.1/24	2403:6200:FFF1:1FE::/64
FL. 5	511	10.50.11.1/24	2403:6200:FFF1:1FF::/64
FL. 5	517	10.50.17.1/24	2403:6200:FFF1:205::/64
FL. 5	518	10.50.18.1/24	2403:6200:FFF1:206::/64
FL. 5	519	10.50.19.1/24	2403:6200:FFF1:207::/64
FL. 5	520	10.50.20.1/24	2403:6200:FFF1:208::/64
FL. 5	521	10.50.21.1/24	2403:6200:FFF1:209::/64
FL. 5	522	10.50.22.1/24	2403:6200:FFF1:20A::/64
FL. 5	523	10.50.23.1/24	2403:6200:FFF1:20B::/64
FL. 5	524	10.50.24.1/24	2403:6200:FFF1:20C::/64
FL. 5	525	10.50.25.1/24	2403:6200:FFF1:20D::/64
FL. 5	528	10.50.28.1/24	2403:6200:FFF1:210::/64
FL. 5	529	10.50.29.1/24	2403:6200:FFF1:211::/64
FL. 5	530	10.50.30.1/24	2403:6200:FFF1:212::/64
FL. 5	531	10.50.31.1/24	2403:6200:FFF1:213::/64

ตารางที่ 5.4 (ต่อ)

Floor	VLAN	Subnet IPv4	Subnet IPv6
			2403:6200:FFF1::/48
FL. 5	532	10.50.32.1/24	2403:6200:FFF1:214::/64
FL. 5	533	10.50.33.1/24	2403:6200:FFF1:215::/64
FL. 5	534	10.50.34.1/24	2403:6200:FFF1:216::/64
FL. 5	535	10.50.35.1/24	2403:6200:FFF1:217::/64
FL. 5	536	10.50.36.1/24	2403:6200:FFF1:218::/64
FL. 5	537	10.50.37.1/24	2403:6200:FFF1:219::/64
FL. 5	538	10.50.38.1/24	2403:6200:FFF1:21A::/64
FL. 5	539	10.50.39.1/24	2403:6200:FFF1:21B::/64
FL. 5	540	10.50.40.1/24	2403:6200:FFF1:21C::/64
FL. 5	541	10.50.41.1/24	2403:6200:FFF1:21D::/64
FL. 5	542	10.50.42.1/24	2403:6200:FFF1:21E::/64
FL. 6	606	10.60.6.1/24	2403:6200:FFF1:25E::/64
FL. 6	607	10.60.7.1/24	2403:6200:FFF1:25F::/64
FL. 6	608	10.60.8.1/24	2403:6200:FFF1:260::/64
FL. 6	609	10.60.9.1/24	2403:6200:FFF1:260::/64
FL. 6	610	10.60.10.1/24	2403:6200:FFF1:261::/64
FL. 6	611	10.60.11.1/24	2403:6200:FFF1:262::/64
FL. 6	612	10.60.12.1/24	2403:6200:FFF1:263::/64
FL. 6	613	10.60.13.1/24	2403:6200:FFF1:264::/64
FL. 6	616	10.60.16.1/24	2403:6200:FFF1:268::/64
FL. 6	617	10.60.17.1/24	2403:6200:FFF1:269::/64
FL. 6	622	10.60.22.1/24	2403:6200:FFF1:26E::/64
FL. 6	623	10.60.23.1/24	2403:6200:FFF1:26F::/64
FL. 6	624	10.60.24.1/24	2403:6200:FFF1:270::/64
FL. 6	625	10.60.25.1/24	2403:6200:FFF1:271::/64
FL. 6	626	10.60.26.1/24	2403:6200:FFF1:272::/64

ตารางที่ 5.4 (ต่อ)

Floor	VLAN	Subnet IPv4	Subnet IPv6
			2403:6200:FFF1::/48
FL. 6	627	10.60.27.1/24	2403:6200:FFF1:273::/64
FL. 6	628	10.60.28.1/24	2403:6200:FFF1:274::/64
FL. 6	629	10.60.29.1/24	2403:6200:FFF1:275::/64
FL. 6	630	10.60.30.1/24	2403:6200:FFF1:276::/64
FL. 6	631	10.60.31.1/24	2403:6200:FFF1:277::/64
FL. 6	632	10.60.32.1/24	2403:6200:FFF1:278::/64
FL. 6	633	10.60.33.1/24	2403:6200:FFF1:279::/64
FL. 6	640	10.60.40.1/24	2403:6200:FFF1:280::/64
FL. 6	641	10.60.41.1/24	2403:6200:FFF1:281::/64
FL. 6	642	10.60.42.1/24	2403:6200:FFF1:282::/64
FL. 6	643	10.60.43.1/24	2403:6200:FFF1:283::/64
FL. 6	644	10.60.44.1/24	2403:6200:FFF1:284::/64
FL. 6	645	10.60.45.1/24	2403:6200:FFF1:285::/64
FL. 6	646	10.60.46.1/24	2403:6200:FFF1:286::/64
FL. 6	647	10.60.47.1/24	2403:6200:FFF1:287::/64
FL. 6	649	10.60.49.1/24	2403:6200:FFF1:289::/64
FL. 6	650	10.60.50.1/24	2403:6200:FFF1:28A::/64
FL. 6	651	10.60.51.1/24	2403:6200:FFF1:28B::/64
FL. 6	652	10.60.52.1/24	2403:6200:FFF1:28C::/64
Other	703	10.15.3.1/24	2403:6200:FFF1:2BF::/64
Other	704	10.15.4.1/24	2403:6200:FFF1:2C0::/64
Other	705	10.15.5.1/24	2403:6200:FFF1:2C1::/64
Other	712	10.15.12.1/24	2403:6200:FFF1:2C8::/64
Other	713	10.15.13.1/24	2403:6200:FFF1:2C9::/64
Other	714	10.15.14.1/24	2403:6200:FFF1:2CA::/64
Other	715	10.15.15.1/24	2403:6200:FFF1:2CB::/64

ตารางที่ 5.4 (ต่อ)

Floor	VLAN	Subnet IPv4	Subnet IPv6
			2403:6200:FFF1::/48
Other	716	10.15.16.1/24	2403:6200:FFF1:2CC::/64
Other	717	10.15.17.1/24	2403:6200:FFF1:2CD::/64
Other	718	10.15.18.1/24	2403:6200:FFF1:2CE::/64
Other	721	10.15.21.1/24	2403:6200:FFF1:2D1::/64
Other	722	10.15.22.1/24	2403:6200:FFF1:2D2::/64
Other	723	10.15.23.1/24	2403:6200:FFF1:2D3::/64
Other	725	10.15.25.1/24	2403:6200:FFF1:2D5::/64
Other	825	10.5.25.1/24	2403:6200:FFF1:339::/64

5.3 การกำหนดกลุ่มในการพัฒนาระบบ

ในการพัฒนาระบบมีการจัดกลุ่มเพื่อพัฒนาเป็นลำดับ โดยคำนึงถึงความเสี่ยงและผลกระทบต่อการใช้งานระบบโครงข่าย IPv4 เดิม โดยแบ่งตามลำดับความสำคัญและความยุ่งยากในการพัฒนาระบบ แบ่งกลุ่มเป้าหมายเป็น 3 กลุ่มคือ

กลุ่มที่ 1 เครื่องให้บริการที่มีการใช้งานภายในคณะเท่านั้น

กลุ่มนี้เป็นกลุ่มของเครื่องให้บริการที่มีการให้บริการนักศึกษา เจ้าหน้าที่และอาจารย์ภายในคณะเท่านั้น ได้แก่ เครื่องให้บริการพิมพ์เอกสาร (Printer Server) เครื่องให้บริการแบ่งข้อมูล (FTP Server , File Sharing Server)

กลุ่มที่ 2 เครื่องให้บริการที่มีการใช้งานภายในคณะ เพื่อบริการการเข้าถึงข้อมูลภายนอกคณะ

กลุ่มนี้เป็นกลุ่มของเครื่องให้บริการที่มีการให้บริการนักศึกษา เจ้าหน้าที่และอาจารย์ภายในคณะ แต่มีการติดต่อสื่อสารภายนอกคณะ ได้แก่ เครื่องให้บริการเว็บ (Web Server) เครื่องให้บริการสิทธิการเข้าใช้งานอินเทอร์เน็ต (Authentications Server)

กลุ่มที่ 3 เครื่องให้บริการที่มีการใช้งานภายในและภายนอกคณะ

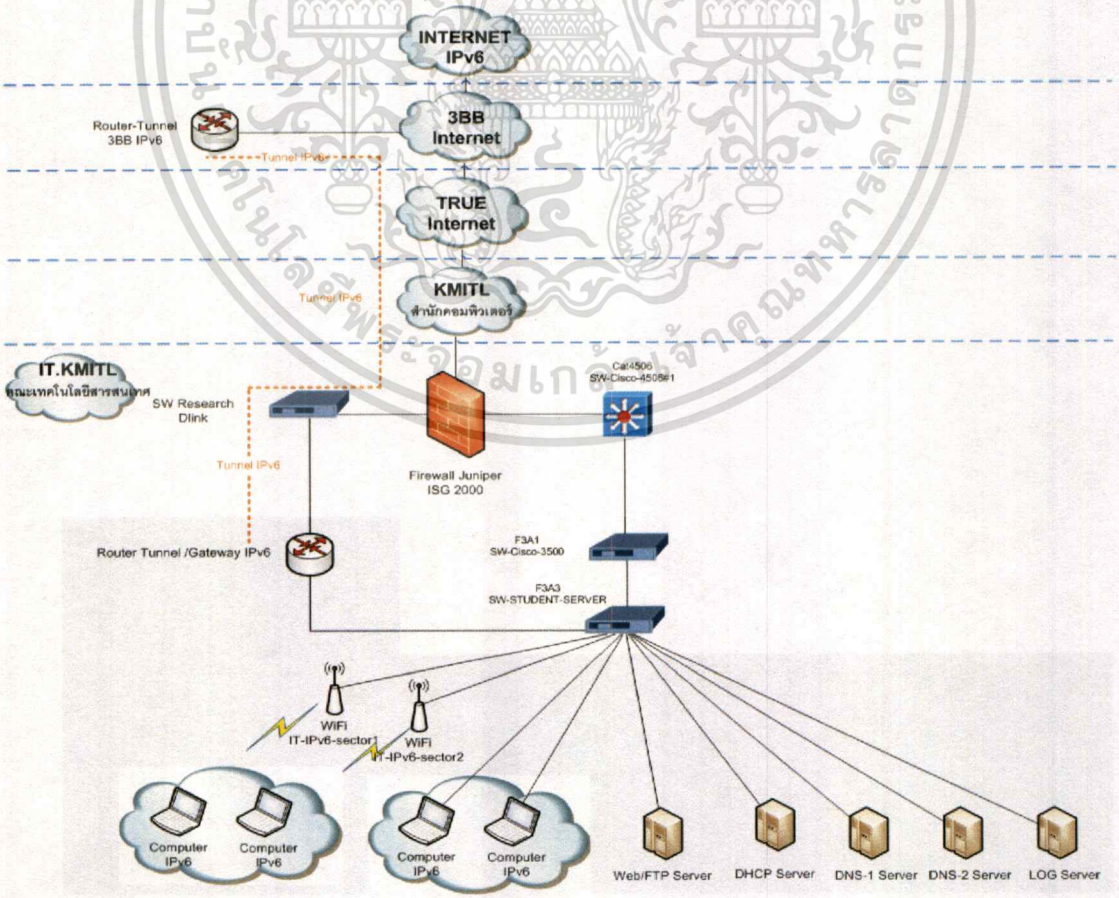
กลุ่มนี้เป็นกลุ่มของเครื่องให้บริการที่มีการให้บริการนักศึกษา เจ้าหน้าที่และอาจารย์ ทั้งภายในและภายนอกคณะ ได้แก่ เครื่องให้บริการเว็บ (WebServer) เครื่องให้บริการแปลงหมายเลขที่อยู่ (DNS Server)

5.4 การพัฒนาระบบ

การจัดลำดับในการพัฒนาระบบแบ่งเป็น 3 ขั้นตอน ในการพัฒนาระบบเริ่มจากการทดสอบภายในห้องทดสอบ และหลังจากนั้นจึงนำมาพัฒนาบนโครงข่ายปัจจุบัน โดยแบ่งขั้นตอนการทำงาน เพื่อลดความเสี่ยงและผลกระทบต่อการใช้งาน โดยการแบ่งลำดับการพัฒนามีดังนี้

5.4.1 Phase 1 การทดสอบภายในห้องทดสอบ

ขั้นตอนที่ 1 เป็นการทดสอบภายในห้องทดสอบ ก่อนการทดสอบมีการเตรียมเครือข่าย IPv6 ซึ่งภายในแต่ละเครือข่ายประกอบด้วยคอมพิวเตอร์ซึ่งใช้งานโพรโทคอล IPv6 และทำการติดตั้งเครื่องให้บริการ (Server) ได้แก่ Web Server , FTP Server , DNS Server , DHCP Server , Log Server ทำการติดตั้ง Router 2811 เพื่อเชื่อมไปยังผู้ให้บริการอินเทอร์เน็ต 3BB เพื่อไปยังโครงข่ายอินเทอร์เน็ต IPv6 โดยผ่านโครงข่ายอินเทอร์เน็ต IPv4 ของผู้ให้บริการ True และดำเนินการติดตั้ง WiFi เพื่อทดสอบการใช้งานการ Wireless

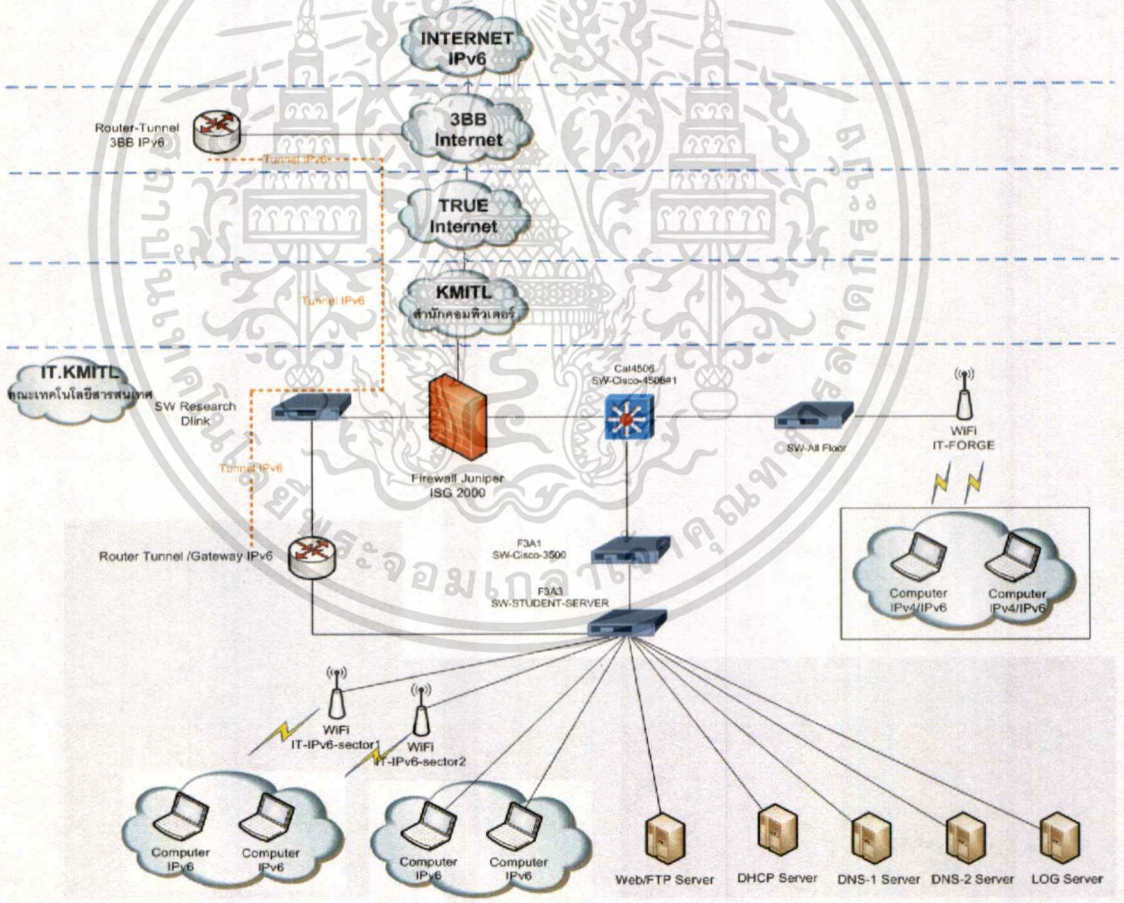


รูปที่ 5.1 แสดงเครือข่ายภายในห้องทดสอบ

5.4.2 Phase 2 การทดสอบกับระบบโครงข่ายจริง

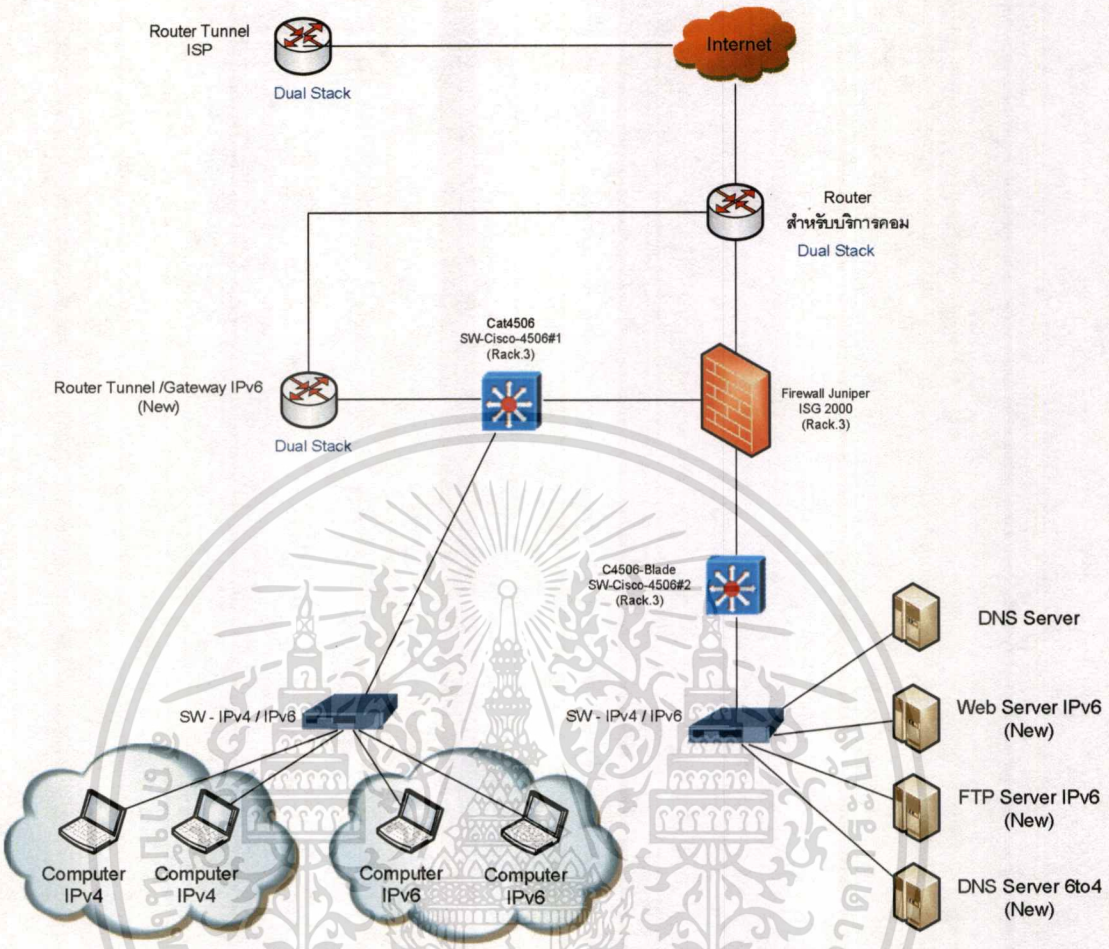
การทดสอบร่วมกับเครือข่ายจริง เร้าเตอร์มีการทำอุโมงค์ (Tunnel) เชื่อมต่อไปยังเร้าเตอร์ผู้ให้บริการอินเทอร์เน็ต เครือข่าย IPv6 สามารถใช้งานอินเทอร์เน็ตผ่านอุโมงค์นี้ ไปยังภายนอกคณะเมื่อมีการเชื่อมต่อกับเครือข่ายจริง เครื่องให้บริการต่างๆจะต้องทำการแก้ไขหมายเลขที่อยู่เพื่อให้สามารถรองรับการใช้งานเครือข่าย IPv6 ได้ โดยการดำเนินการตามกลุ่มกำหนดเป้าหมาย โดยจะเลือกกลุ่มที่มีความเสี่ยงน้อยก่อน เพื่อลดผลกระทบและปัญหาที่จะเกิดขึ้น

โดยกลุ่มที่เลือกคือ กลุ่ม WiFi IT-FORGE ซึ่งเป็น WiFi ของคณะมีผู้ใช้งานทั่วไป ติดตั้งภายในตึกคณะเทคโนโลยีสารสนเทศ



รูปที่ 5.2 แสดงการทดสอบร่วมกับเครือข่ายจริง

5.4.3 Phase 3 การพัฒนาเพื่อใช้งานจริง

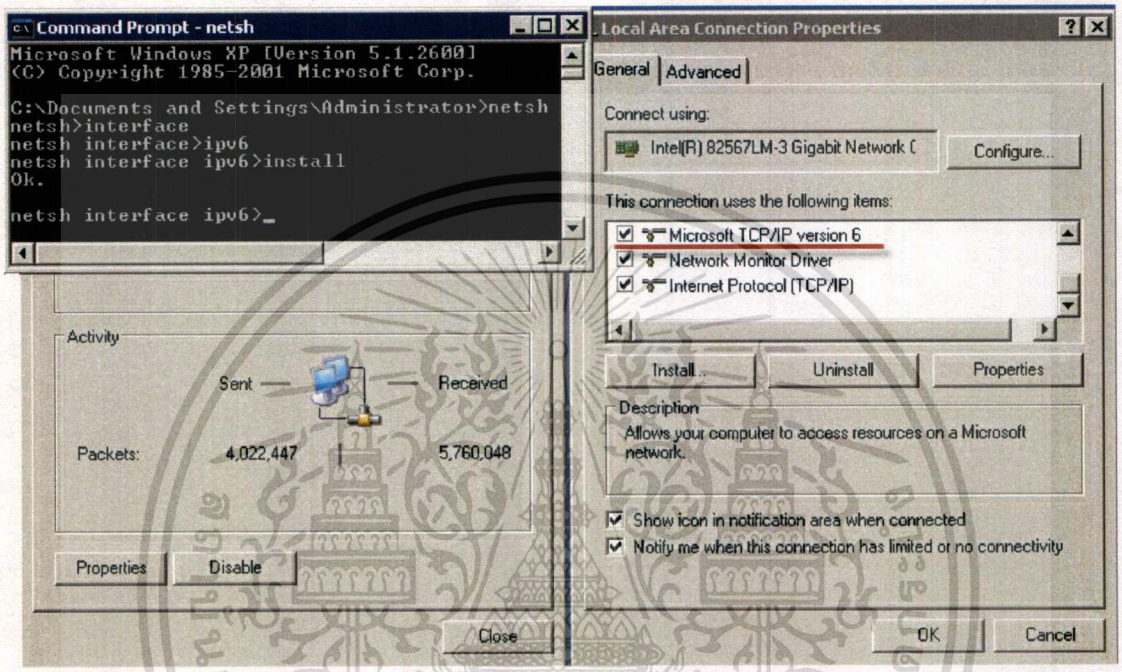


รูปที่ 5.3 แสดงการพัฒนาเพื่อใช้งานจริง

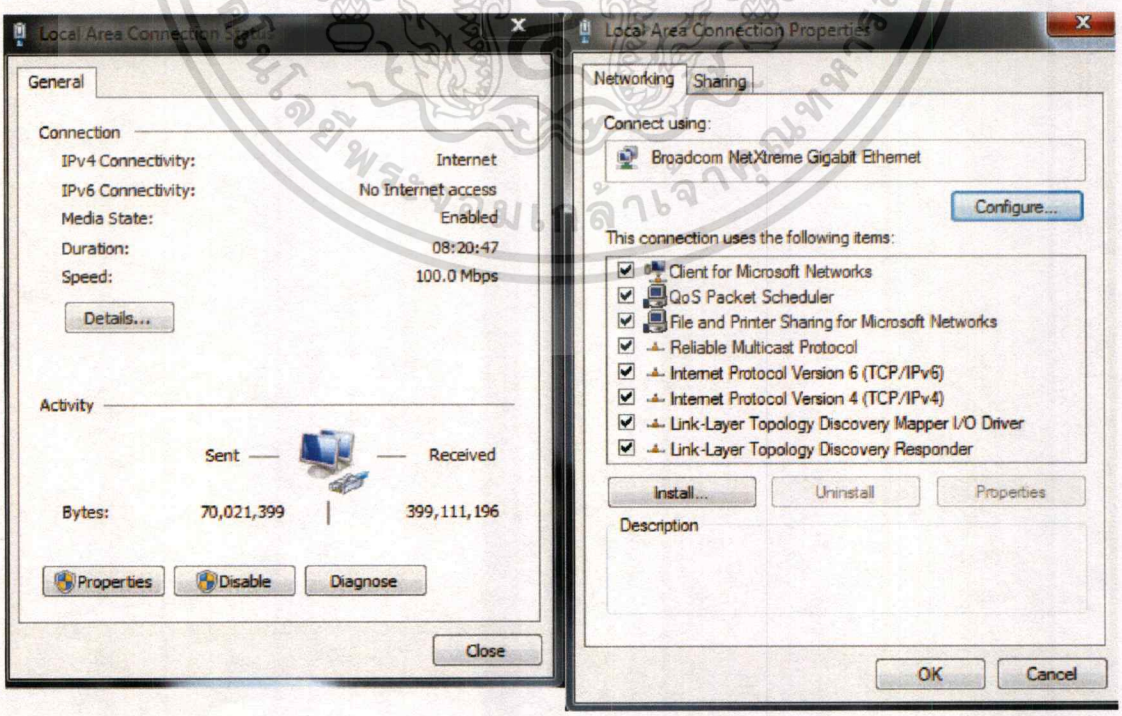
การทดสอบการใช้งาน IPv6 ผ่านอุโมงค์ (Tunnel) ไปยังผู้ให้บริการอินเทอร์เน็ต นั้นสามารถใช้งานได้ แต่จะมีข้อจำกัดของ MTU เนื่องจากผ่านอุปกรณ์ในโครงข่ายมากมาย ซึ่งแต่ละเส้นทางอาจจะมีแค่ MTU ไม่เท่ากัน ซึ่งส่งผลต่อการใช้งาน IPv6 ดังนั้นในการพัฒนามาใช้งานจริงควรใช้วิธีการทำ Dual Stack ตลอดเส้นทาง แต่การทำวิธีจะต้องมีการปรับเปลี่ยนแก้ไขตลอดเส้นทาง นั้นคืออุปกรณ์เหล่านั้นจะต้องรองรับการทำงานแบบ Dual Stack คือรองรับทั้ง IPv4 และ IPv6

5.5 ผลการทดสอบการใช้งาน

ดำเนินการเตรียมพร้อมการรองรับการใช้งาน IPv6 ให้กับคอมพิวเตอร์ อุปกรณ์เร้าเตอร์ เซิร์ฟเวอร์ ในการเปิดใช้งาน IPv6 สำหรับคอมพิวเตอร์ ได้ทำการทดสอบกับ Windows XP และ Windows 7 โดยทำการเปิดการใช้งานดังรูป ที่ 5.4 และ 5.5

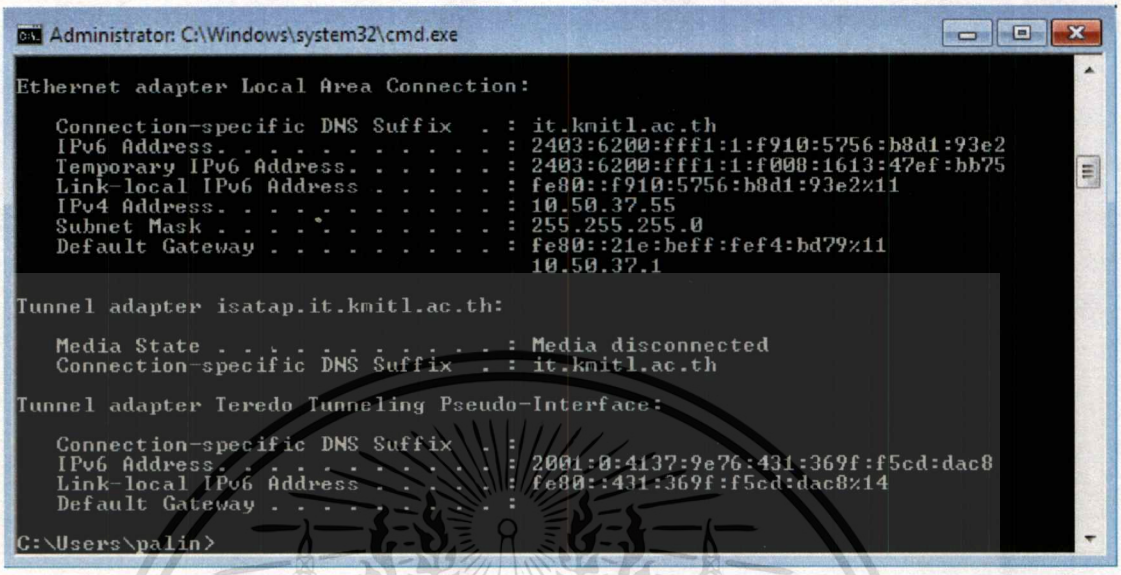


รูปที่ 5.4 แสดงการเปิดใช้งานสำหรับ Windows XP



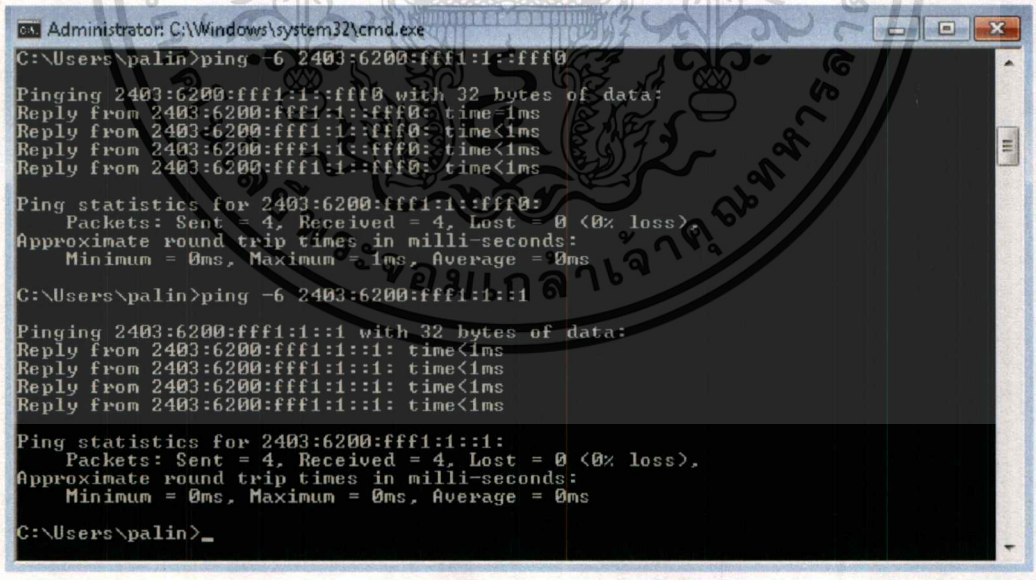
รูปที่ 5.5 แสดงการเปิดใช้งานสำหรับ Windows 7

ทำการทดสอบรับหมายเลขที่อยู่โดยสามารถระบุได้โดยวิธี stateless, stateful และแบบกำหนดหมายเลขที่อยู่ IPv6 ดังรูปที่ 5.6



รูปที่ 5.6 แสดงการกำหนดหมายเลขที่อยู่อัตโนมัติของคอมพิวเตอร์แบบ Stateless

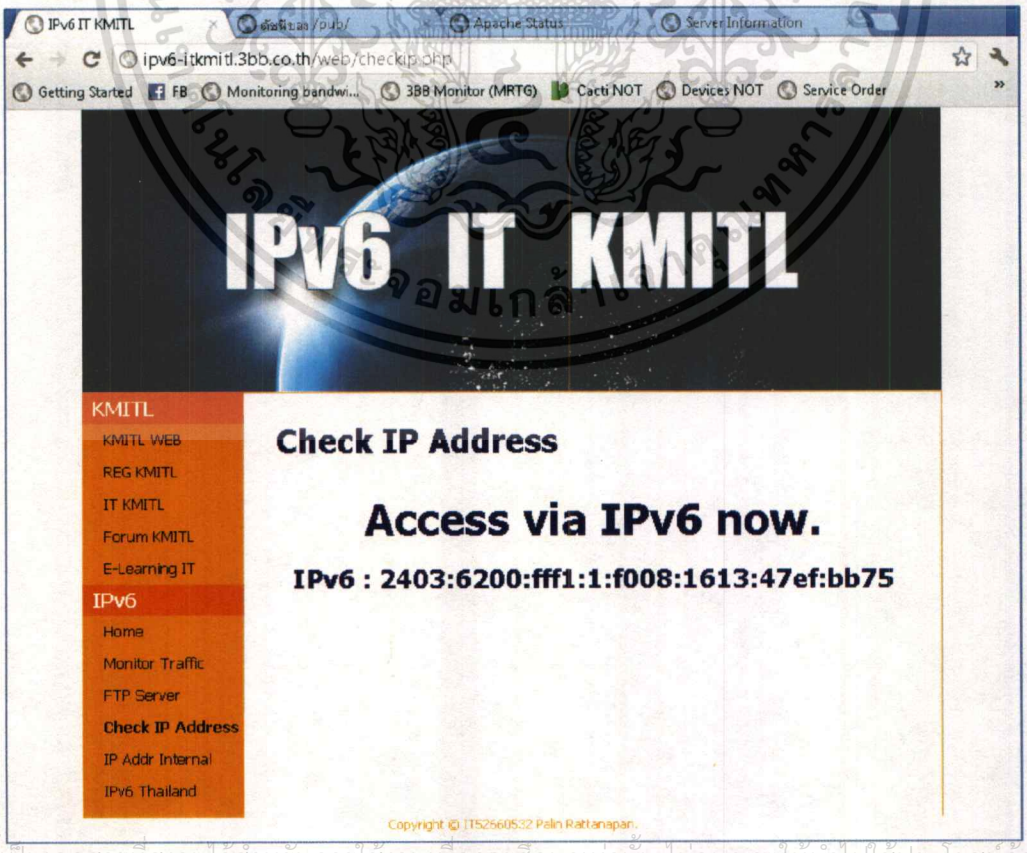
ทำการทดสอบการติดต่อภายในเครือข่าย IPv6 โดยการทดสอบ Ping ไปยังเร้าเตอร์และเซิร์ฟเวอร์ ดังรูปที่ 5.7



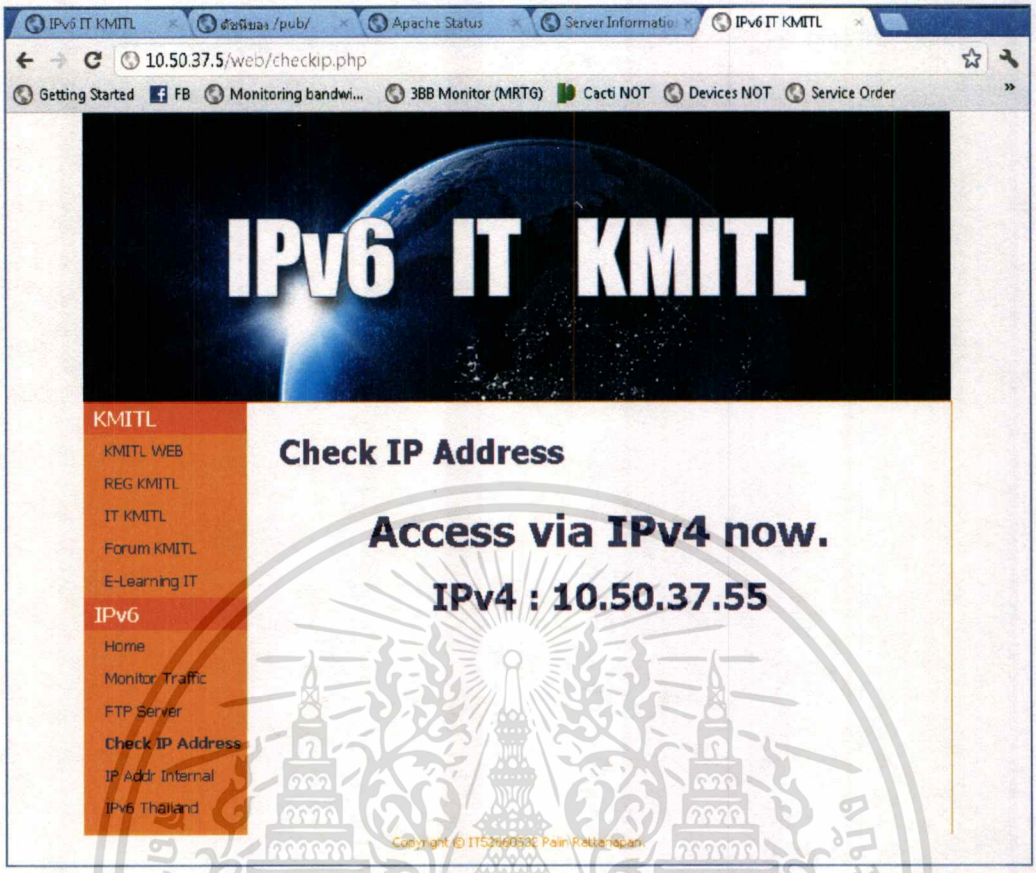
รูปที่ 5.7 แสดงผลการติดต่อภายในเครือข่าย IPv6

ทดสอบการเข้าถึงเว็บเซิร์ฟเวอร์ โดยทำการติดตั้งแต่เซิร์ฟเวอร์และเปิดให้สามารถใช้งานผ่านโพรโทคอล HTTP โดยสามารถให้บริการได้ทั้งเครือข่าย IPv4 และ IPv6 ซึ่งสามารถเข้าถึงและได้รับข้อมูลเหมือนกัน ดังรูปที่ 5.8, 5.9 และ 5.10

รูปที่ 5.8 แสดงการเข้าถึงเว็บผ่านเครือข่าย IPv6

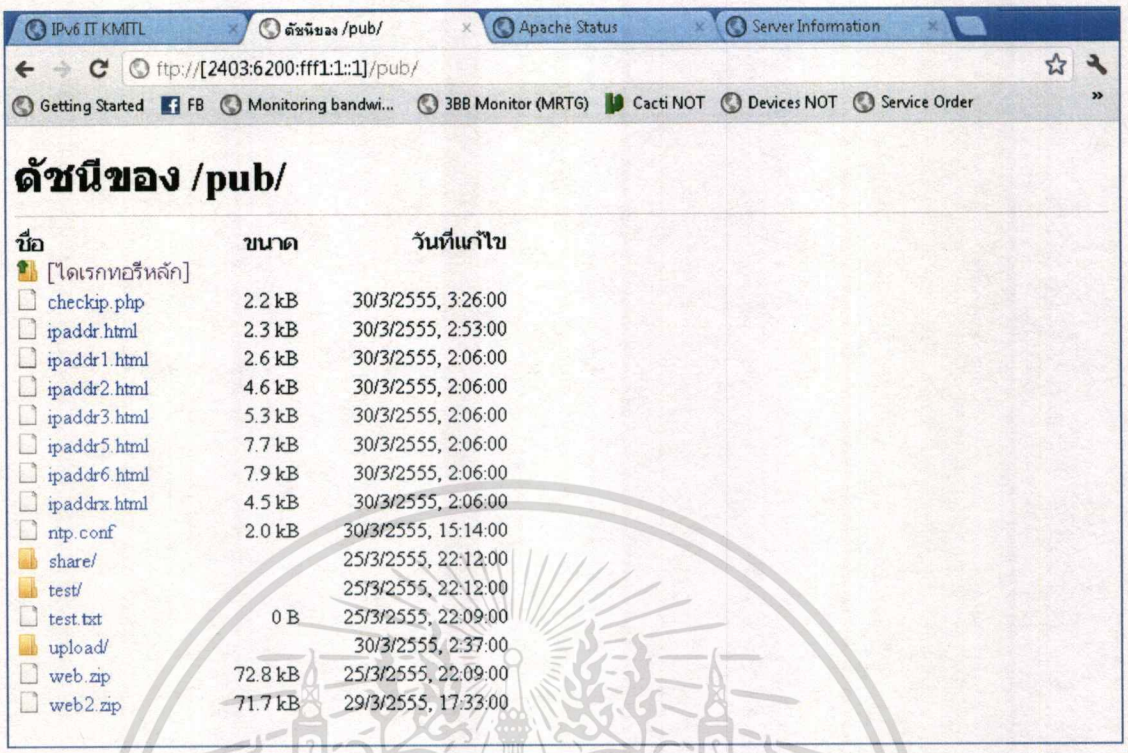


รูปที่ 5.9 แสดงการเข้าถึงเว็บผ่านเครือข่าย IPv6

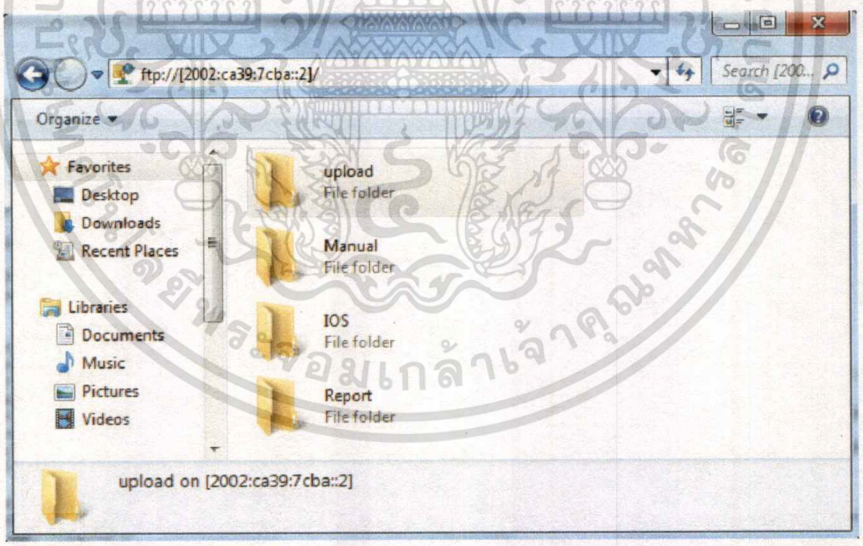


รูปที่ 5.10 แสดงการเข้าถึงเว็บผ่านเครือข่าย IPv4

ทดสอบการโอนถ่ายข้อมูลจากเครื่องให้บริการโอนถ่ายข้อมูล(FTP) โดยทำการติดตั้งและเปิดให้ใช้งาน VSFTPD สามารถอัพโหลดและดาวน์โหลดข้อมูลจากเซิร์ฟเวอร์ได้ผ่านเว็บและผ่าน Path ในคอมพิวเตอร์ ดังรูปที่ 5.11 และ 5.12

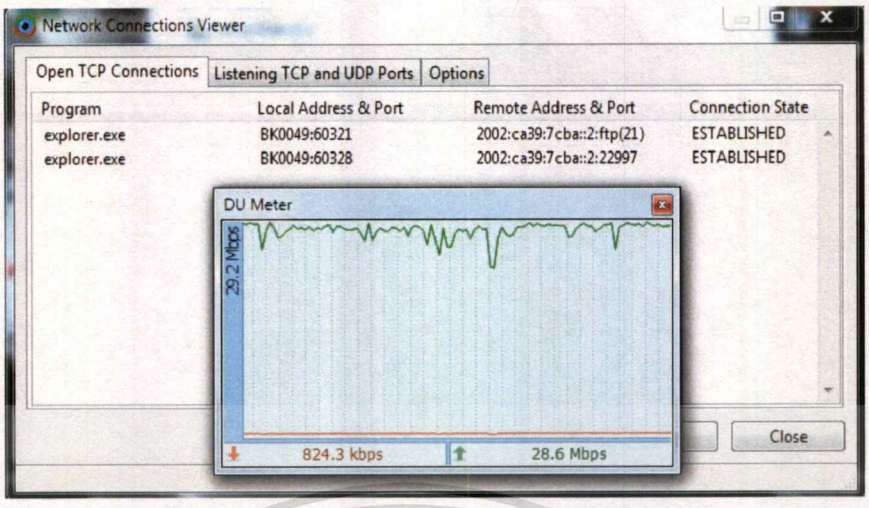


รูปที่ 5.11 แสดงการเข้าถึงเซิร์ฟเวอร์โอนถ่ายข้อมูลผ่านเครือข่าย IPv6 ผ่านเว็บ

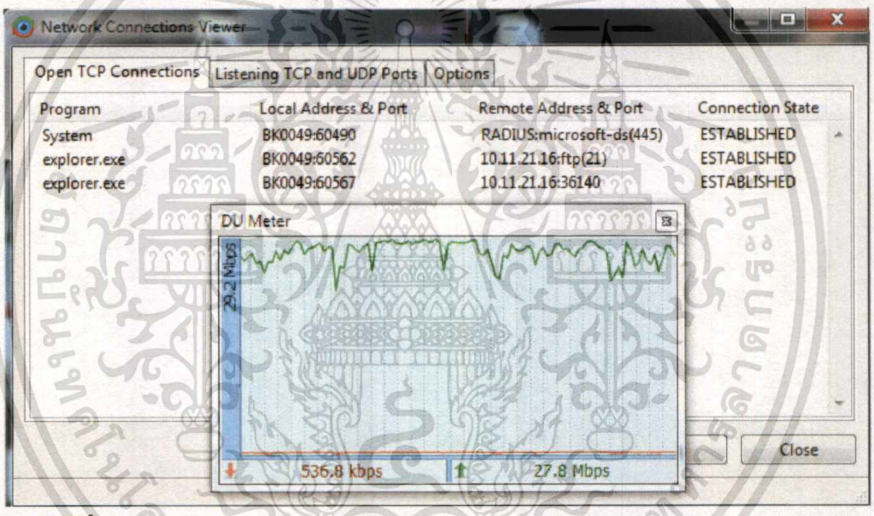


รูปที่ 5.12 แสดงการเข้าถึงเซิร์ฟเวอร์โอนถ่ายข้อมูลผ่านเครือข่าย IPv6 ผ่าน Path คอมพิวเตอร์

ทดสอบใช้งาน FTP สามารถให้บริการได้ทั้งเครือข่าย IPv4 และ IPv6 ซึ่งสามารถเข้าถึงและสามารถรับส่งข้อมูลได้เหมือนกัน ดังรูปที่ 5.13 และ 5.14

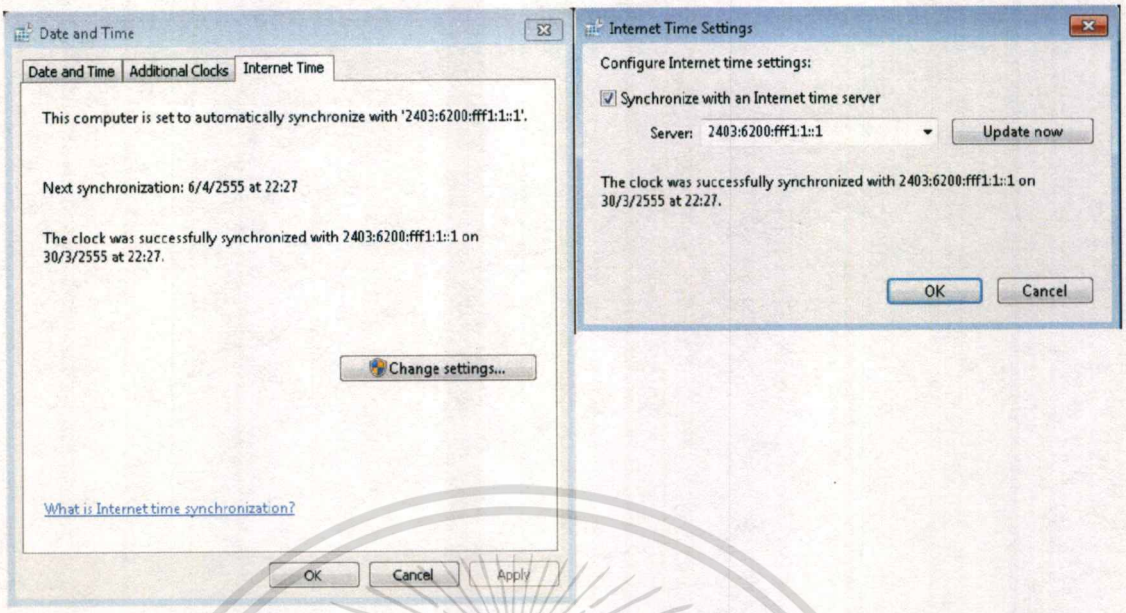


รูปที่ 5.13 แสดงการเข้าถึงเซิร์ฟเวอร์โอนถ่ายข้อมูลผ่านเครือข่าย IPv6



รูปที่ 5.14 แสดงการเข้าถึงเซิร์ฟเวอร์โอนถ่ายข้อมูลผ่านเครือข่าย IPv4

ทดสอบการSynchronize ข้อมูลเวลากับ NTP Server เพื่อให้คอมพิวเตอร์และอุปกรณ์ในโครงข่ายมีเวลาที่ตรงกันทั้งหมด โดยอุปกรณ์ต่างๆจะต้องดำเนินการมาติดต่อเซิร์ฟเวอร์เพื่อร้องขอข้อมูล โดยทำการทดสอบให้เครื่องคอมพิวเตอร์มา sync เวลากับเซิร์ฟเวอร์ดังรูปที่ 5.15

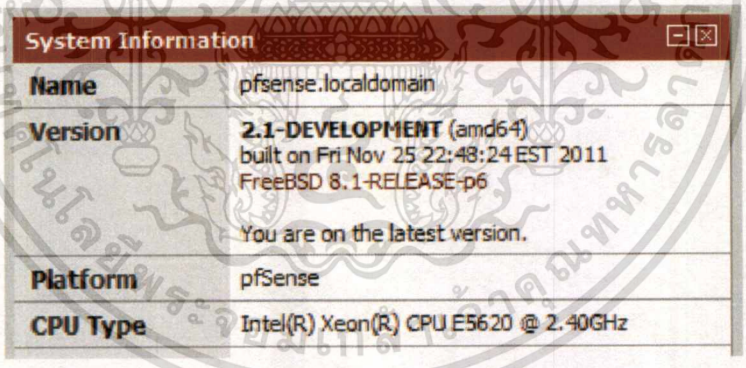


รูปที่ 5.15 แสดงการ Synchronize เวลากับ NTP Server

ดำเนินการติดตั้ง DHCP Server เพื่อรองรับการใช้งาน IPv6 โดยมีรายละเอียดดังนี้

ระบบปฏิบัติการ CentOS 6.2

ซอฟต์แวร์ : Pfsense 2.1 Deveplopment



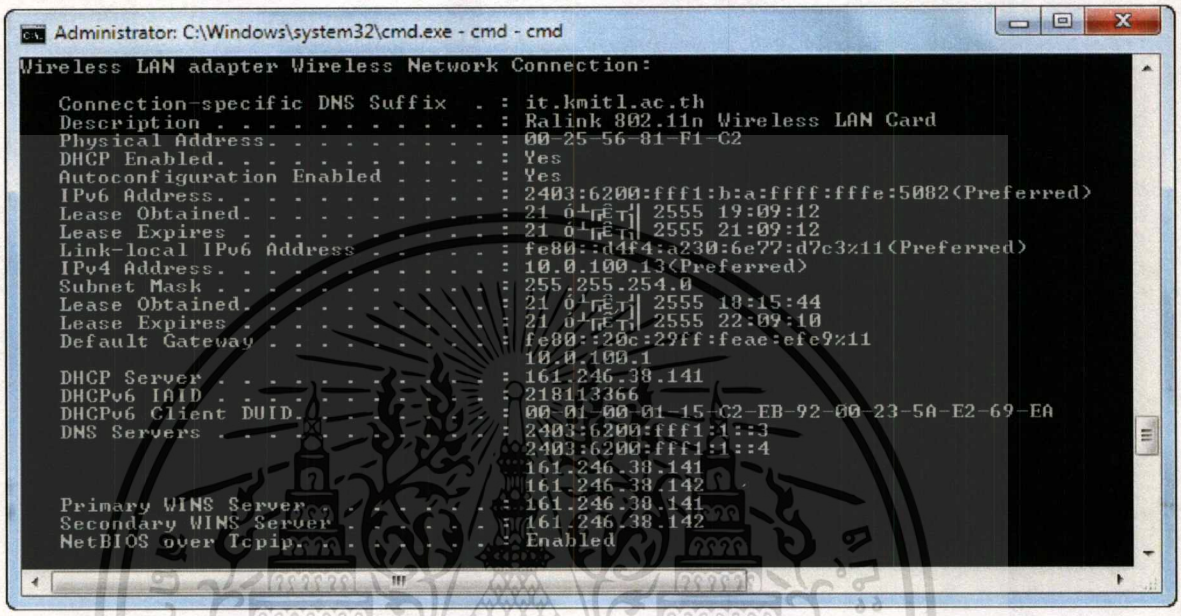
รูปที่ 5.16 แสดงซอฟต์แวร์สำหรับเซิร์ฟเวอร์ DHCP

ดำเนินการติดตั้ง WiFi จำนวน 2 ตัว เพื่อทดสอบการแจกหมายเลข IPv6

		ชื่อ WiFi		
		IT-Kmitl-Sector1	IT-Kmitl-Sector2	IT-FORGE
IPv4	รองรับ DHCPv4	ไม่	ไม่	รองรับ
	ชื่อ DHCP			nitrogen server
	Address v4			10.0.100.0/23
IPv6	รองรับ DHCPv6	รองรับ	รองรับ	รองรับ
	ชื่อ DHCPv6	Pfsense Server	Pfsense Server	Pfsense Server
	Address v6	2403:6200:fff1:a:a:a:a:1-2403:6200:fff1:a:a:ffff:ffff:1	2403:6200:fff1:c:a:a:a:1-2403:6200:fff1:c:a:ffff:ffff:1	2403:6200:fff1:b:a:a:a:1-2403:6200:fff1:b:a:ffff:ffff:1

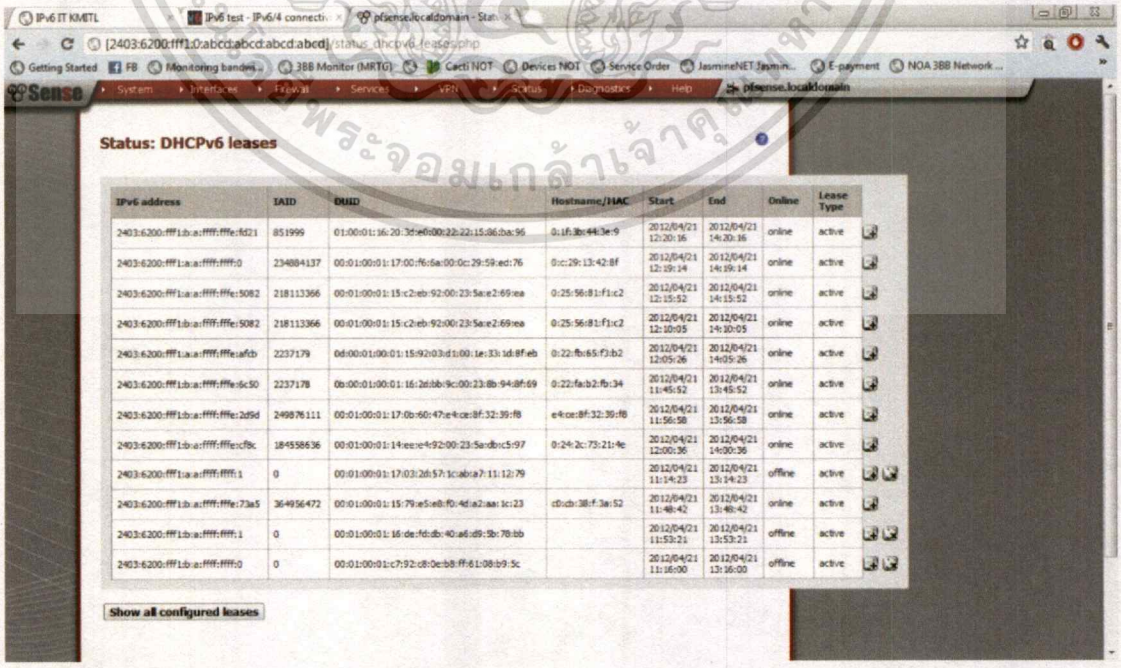
รูปที่ 5.17 แสดง WiFi ที่รองรับการทำงาน IPv6

ทดสอบให้คอมพิวเตอร์รับ IPv6 จาก DHCP Server โดยทำการรับ IPv6 จาก WiFi IT-FORGE ซึ่งสามารถรับหมายเลขได้ทั้ง IPv4 และ IPv6 โดย IPv4 ได้รับจาก DHCP Server เดิมในปัจจุบัน และสำหรับ IPv6 จะได้รับจาก PFsense Server ทั้งนี้จะได้รับหมายเลข DNS อีกด้วย ดังรูป



รูปที่ 5.18 แสดงการรับ IPv6 จาก WiFi IT-FORGE

ในส่วนของเซิร์ฟเวอร์ DHCP สามารถตรวจสอบ หมายเลขกับ MAC Address ได้ ดังรูป



รูปที่ 5.19 แสดงการตรวจสอบหมายเลข IPv6 และ MAC Address ได้ที่รับ

ดำเนินการติดตั้ง DNS Server รองรับการใช้งาน IPv6 และดำเนินการทดสอบ ดำเนินการทดสอบเรียกโดเมน IPv6 โดยมีรายละเอียดเซิร์ฟเวอร์ดังนี้ดังนี้

ระบบปฏิบัติการ CentOS 6.2

ซอฟต์แวร์ : Bind 0.9.9

หมายเลข IPv6 : 2403:6200:fff1:1::3 ; 2403:6200:fff1:1::4

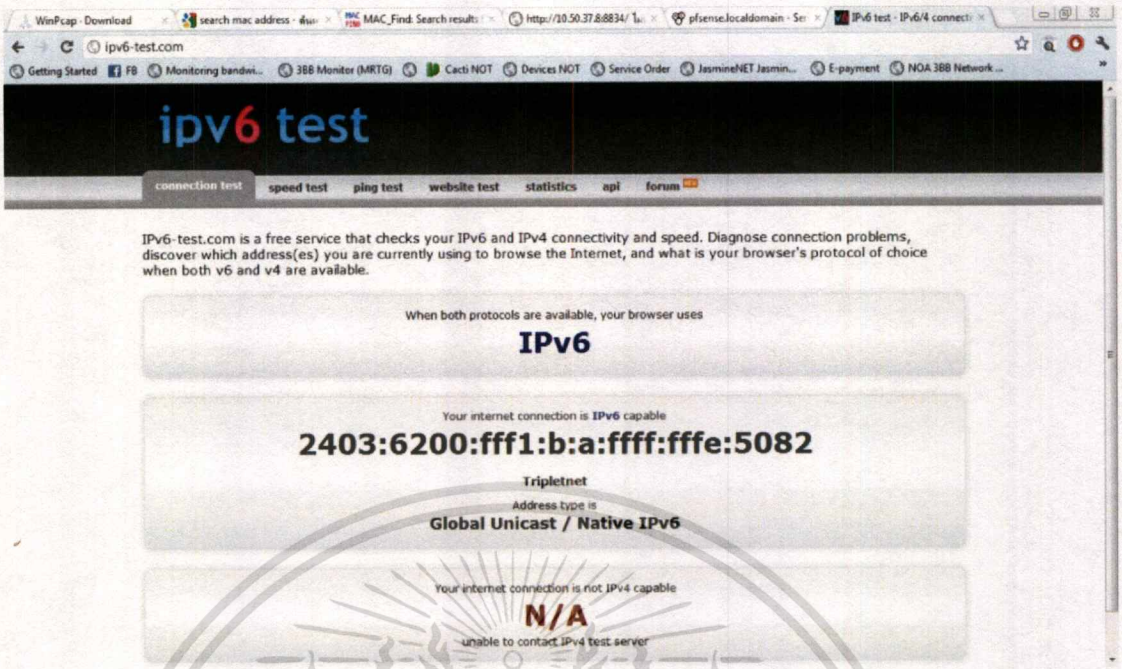
ดำเนินการทดสอบเรียกโดเมน IPv6 พบว่า DNS สามารถตอบหมายเลขที่อยู่ของโดเมนดังกล่าวได้ ดังรูป

รูปที่ 5.20 แสดงการทดสอบ lookup domain

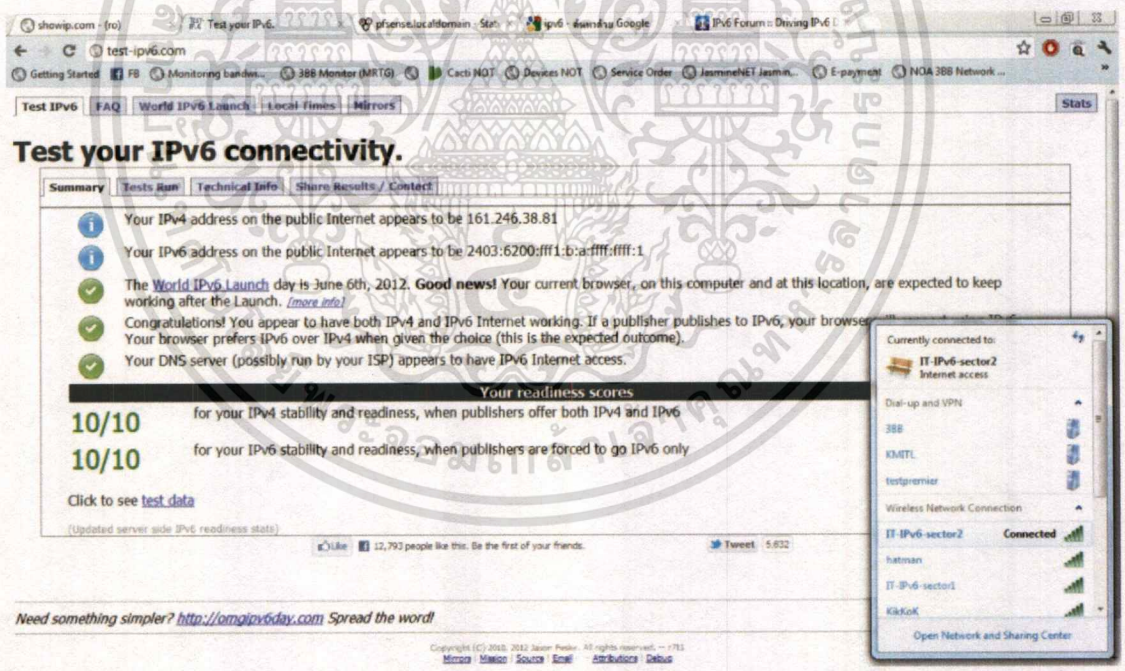
ชนิด DNS ของ Internet protocol

- DNS IPv4 type = A
- DNS IPv6 type = AAAA

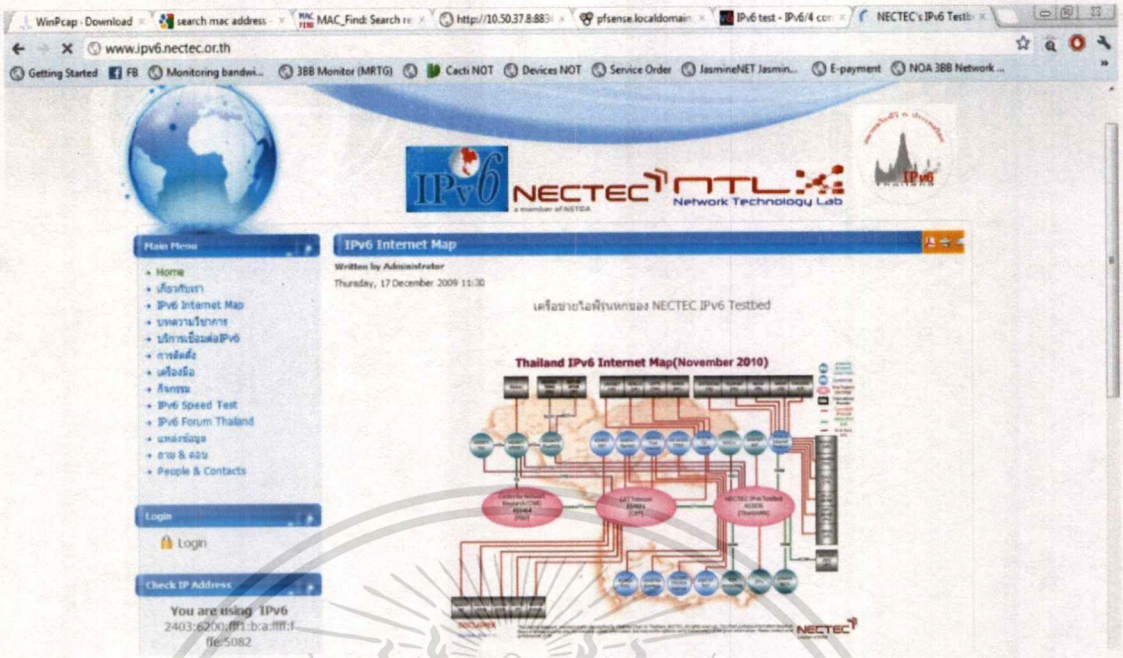
การทำ DNS Forward เมื่อมีการเชื่อมต่อไปยัง domain kmitl.ac.th โดยทำการส่งต่อไป DNS IPv4 ของคณะ ตัวอย่างการทดสอบเว็บ IPv6 ภายในนอกคณะ ดังรูป



รูปที่ 5.21 แสดงการทดสอบเว็บ IPv6 ภายนอกคณะ



รูปที่ 5.22 แสดงการทดสอบเว็บ IPv6 ภายนอกคณะ



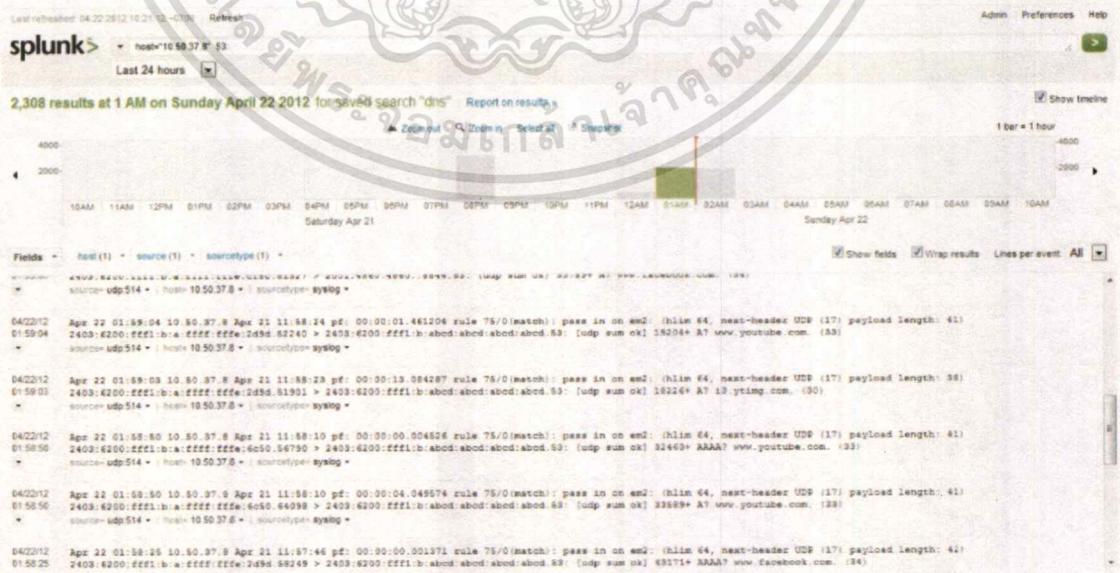
รูปที่ 5.23 แสดงการทดสอบเว็บ IPv6 ภายนอกคณะ

ดำเนินการติดตั้ง Log Server รองรับการใช้งาน IPv6

ระบบปฏิบัติการ CentOS 6.2

ซอฟต์แวร์ : Splunk

กำหนดให้ DNS Server และ Pfsense Server ส่ง Log มายัง Log Server ตัวอย่าง Log ดังรูป



รูปที่ 5.24 แสดงการตรวจสอบ Log IPv6

ดำเนินการทดสอบการใช้เว็บ ipv6-itkmitl.3bb.co.th จากภายนอกคณะ โดยจะต้องแจ้งไปยังเจ้าของ Domain เพื่อให้ดำเนินการจดโดเมนย่อย ให้สามารถใช้งานจากอินเทอร์เน็ตได้

รูปที่ 5.25 แสดงการเข้าถึงเว็บโดยผ่านเครือข่าย IPv6 ภายนอกสถาบัน

5.6 การเตรียมคอนฟิกกูเรชัน

การเตรียมคอนฟิกกูเรชันสำหรับเร้าเตอร์ CISCO ดังนี้

ตารางที่ 5.5 แสดงการเตรียมคอนฟิกกูเรชั่นเร้าเตอร์

คำสั่ง	รายละเอียด
interface FastEthernet0/0 description Research ip address 161.246.38.80 255.255.255.192 no ip redirects no ip unreachables no ip proxy-arp ip nat outside ip virtual-reassembly load-interval 30 duplex auto speed auto ipv6 address 2403:6200:FFF1::FFF0/64	Fa 0/0 เชื่อมต่อกับสวิตซ์ Research เพื่อเชื่อมต่อเครือข่าย IPv6 ภายนอกสถาบันฯ ทำงานแบบ Dual Stack คือกำหนด IPv4 และ IPv6
interface FastEthernet0/1 ip address 10.50.37.2 255.255.255.0 ip nat outside ip virtual-reassembly load-interval 30 duplex auto speed auto ipv6 address 2403:6200:FFF1:1::FFF0/64	Fa 0/0 เชื่อมต่อกับสวิตซ์ Research เพื่อเชื่อมต่อเครือข่าย IPv6 และ IPv4เข้าด้วยกัน กำหนด IPv6 เพื่อเป็น Gateway ให้กับ LAN ต่างๆ

ตารางที่ 5.5 แสดงการเตรียมคอนฟิกกูเรชั่นเร้าเตอร์ (ต่อ)

คำสั่ง	รายละเอียด
interface Tunnel100 description "===TO 3BB IPv6 Tunneling==" no ip address load-interval 30 ipv6 address 2403:6200:FFF1:4::FFF0/64 ipv6 traffic-filter acl_ipv6_inbound in tunnel source 161.246.38.80 tunnel destination 110.164.252.251 tunnel mode ipv6ip tunnel path-mtu-discovery	Tunnel 100 สำหรับเป็นอุโมงค์เชื่อมต่อไปยังเครือข่ายภายนอก ทำงานแบบ Dual Stack คือกำหนด IPv4 และ IPv6 โดยทำการเชื่อมต่อไปยังผู้ให้บริการ 3BB แบบ IPv6 over IPv4
ipv6 route ::/0 Tunnel100 2403:6200:FFF1:4::FFF1	ประกาศเส้นทาง IPv6 ที่ไม่ได้กำหนดไว้ให้ออกทาง Tunnel 100 เพื่อให้ใช้งานภายนอกสถาบันฯ
ipv6 access-list acl_vty_ipv6_in deny ipv6 any any	กำหนด ACL เพื่อกำหนดสิทธิการเข้าถึงโดยกำหนดให้หมายเลขที่อยู่ IPv6 เท่านั้น
ipv6 access-list acl_ipv6_inbound permit tcp any 2403:6200:FFF1::/48 eq www sequence 1000000 deny ipv6 any any	กำหนด ACL เพื่อกำหนดสิทธิการเข้าถึงโดยกำหนดให้หมายเลขที่อยู่ IPv6 ของคณะสามารถเข้าใช้งานเว็บได้
line vty 0 4 access-class 10 in exec-timeout 15 0 ipv6 access-class acl_vty_ipv6_in in logging synchronous login local transport input telnet ssh	กำหนดสิทธิการเข้าถึงเร้าเตอร์ โดยให้สิทธิการเข้าถึงตาม ACL ที่ระบุไว้และสามารถเข้าได้โดย telnet และ ssh

บทที่ 6

สรุปการพัฒนาระบบ

6.1 ผลการพัฒนา

การพัฒนาระบบโครงข่ายภายในคณะเทคโนโลยีสารสนเทศ สถาบันพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ให้สามารถรองรับการใช้งานอินเทอร์เน็ตโปรโทคอลรุ่นที่ 6 (IPv6) ร่วมกับโครงข่ายเดิมที่มีการใช้งานอินเทอร์เน็ตโปรโทคอลรุ่นที่ 4 (IPv4) สามารถรองรับการใช้งานทั้งสองโปรโทคอลได้ โดยการเพิ่มอุปกรณ์การจัดการเส้นทาง (Router) เพิ่มเพื่อทำหน้าที่เป็นอุโมงค์ให้เครือข่าย IPv6 สามารถรับส่งข้อมูลผ่านโครงข่าย IPv4 ของผู้ให้บริการอินเทอร์เน็ตได้ พร้อมทั้งจัดการดูแลด้านความปลอดภัยให้การโครงข่ายภายในของคณะ

ระบบสามารถใช้งานภายในเครือข่าย IPv4 และ IPv6 เองได้ สามารถรับบริการจากเครื่องให้บริการ (Server) ภายในคณะได้ ซึ่งเครื่องให้บริการเหล่านี้ เพื่อให้สามารถรองรับการใช้งานจากเครือข่าย IPv6 จำเป็นต้องทำการแก้ไขและเพิ่มเลขที่อยู่ IPv6 ดังนั้นเครื่องให้บริการต่างเมื่อทำการแก้ไขแล้ว จะสามารถรองรับการทำงานได้ทั้งเครือข่าย IPv4 และ IPv6 พร้อมๆกัน

ทั้งนี้เครือข่าย IPv4 และ IPv6 ภายในคณะยังสามารถติดต่อสื่อสารกันได้ โดยผ่านการควบคุมของเร้าเตอร์โดยกลวิธีการเปลี่ยนแปลงข้อมูล เป็นวิธีการเปลี่ยนแปลงหมายเลขที่อยู่เสมือนอุปกรณ์หรือคอมพิวเตอร์ปลายทางมีเลขที่อยู่ทั้งแบบ IPv4 และ IPv6 เพื่อใช้สำหรับติดต่อสื่อสารกับเครือข่ายทั้งสองแบบ โดยอุปกรณ์เกตเวย์จะมีการทำ NAT-TP เพื่อแปลงหมายเลขที่อยู่แบบ IPv4 เป็น IPv6 โดยจะมีการบันทึกข้อมูลเลขหมายที่อยู่ที่มีการใช้สำหรับอ้างอิงในการรับส่งข้อมูลข้ามเครือข่ายหลักที่มีการใช้งานอินเทอร์เน็ตโพรโทคอลที่แตกต่างกัน

IPv6 รองรับการเพิ่มขยายขนาดของเครือข่าย สามารถรองรับหมายเลขที่อยู่ได้มากกว่าเครือข่าย IPV4 นอกจากนั้นแล้ว IPv6 ยังมีความปลอดภัยมากกว่าการใช้งานในเครือข่าย IPv4 เพราะ IPv6 IPSec ถูกกำหนดตามมาตรฐาน ให้เป็นสิ่งที่ต้องใช้เพื่อเพิ่มความปลอดภัยของเครือข่าย นอกจากนั้น IPv6 สนับสนุนการปรับแต่งระบบให้เป็นแบบอัตโนมัติ (Automatically configuration) ซึ่งไม่จำเป็นต้องกำหนดเลขที่อยู่แน่นอน (Static Address) หรือ การรับจากผู้แจกหมายเลขที่อยู่ (DHCP)

6.2 อุปสรรคในการพัฒนา

ในการพัฒนาระบบโครงข่ายใหม่ IPv6 บนโครงข่ายเดิม IPv4 พบอุปสรรคทั้งในด้านอุปกรณ์และข้อมูลในการเตรียมพร้อมสำหรับโครงข่ายใหม่ ดังนี้

1. หมายเลขที่อยู่ IPv6 ซึ่งจะได้รับการจัดสรรจากผู้ให้บริการอินเทอร์เน็ต โดยจะจัดสรรให้กับทางสถาบัน และทางสถาบันจะเป็นผู้จัดสรรให้กับคณะต่างๆ ขั้นตอนการขอข้อมูลเลขที่อยู่ใช้เวลานาน เนื่องจากต้องข้อมูลผ่านสถาบัน ดังนั้นจึงแก้ไขโดยการขอความร่วมมือกับผู้ให้บริการอินเทอร์เน็ตสามบีบี เพื่อขอทดสอบร่วมกัน ดังนั้นหมายเลขที่อยู่ IPv6 ที่ได้รับมา จะใช้เพียงในการทดสอบเท่านั้น

2. อุปกรณ์ในโครงข่ายเดิมมีอายุการใช้งานนาน ดังนั้นฮาร์ดแวร์และซอฟต์แวร์ของบางอุปกรณ์ ไม่รองรับการใช้งาน IPv6 ในขณะเดียวกันอุปกรณ์ที่รองรับการใช้มีซอฟต์แวร์ที่รองรับบางฟังก์ชันเท่านั้น ดังนั้นจึงการมีการเพิ่มอุปกรณ์เพื่อให้สามารถรองรับการใช้งาน IPv6 ได้

3. เครื่องให้บริการ (Server) ภายในคณะ เพื่อให้สามารถรองรับการใช้งานเครือข่าย IPv6 จำเป็นต้องแก้ไขและเพิ่มหมายเลขที่อยู่ IPv6 ซึ่งเครื่องให้บริการเหล่านี้มีการใช้งานอยู่ในระบบโครงข่ายปัจจุบัน ในการพัฒนาจึงมีความเสี่ยงที่อาจเกิดผลกระทบหรือปัญหาได้

6.3 ปัญหาข้อจำกัดและข้อเสนอแนะ

1. ข้อจำกัดในการพัฒนาโครงข่าย IPv6 โดยวิธีการทำอุโมงค์ไปยังผู้ให้บริการ เป็นการขอความร่วมมือในการทดสอบการผู้ให้บริการอินเทอร์เน็ตสามบีบีเท่านั้น ดังนั้นหากพัฒนาให้มีการใช้งานจริงจะต้องได้รับจัดสรรหมายเลขที่อยู่ที่ถูกต้อง

2. ข้อจำกัดในทดสอบแบบอุโมงค์ คือ MTU ขนาดของข้อมูลที่มีการรับส่งการ มีการรับส่งผ่านโครงข่ายมากมาย ซึ่งขนาด MTU แตกต่างมีผลต่อการใช้งาน

3. ในพัฒนาเครื่องให้บริการ (Server) ควรมีการทดสอบก่อนใช้งานจริง เพราะมีความเสี่ยงที่อาจผิดพลาดส่งผลกระทบต่อการใช้งานระบบโครงข่ายเดิมได้

บรรณานุกรม

โครงการอินเทอร์เน็ตยุคหน้า ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ. 2548. **ความรู้เบื้องต้นเกี่ยวกับ IPv6 สำหรับผู้ใช้งานทั่วไป.**[Online]. เข้าถึงได้จาก: http://www.ipv6.nectec.or.th/document/The_simple_guide_IPv6final.pdf

Baskaran Boobathiraj. 2011. **IDA IPv6 Technology Pilot.** เข้าถึงได้จาก: http://www.ipv6.com.sg/presentation/D202_IDA-IPv6-Transition-test_bed_Baskaran_Boobathiraj.pdf

Cisco Systems. 2008. **Cisco IOS IPv6 Configuration Guide.** [Online]. เข้าถึงได้จาก: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/12_4/ipv6_12_4_book.pdf

Cisco Systems. 2011. **Implementing Tunneling for IPv6.** [Online]. เข้าถึงได้จาก: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-tunnel.pdf

Cisco Systems. 2010. **Transitioning to IPv6 and beyond in SP Broadband Networks.** [Slide]. Cisco Public.

Salman Asadullah. **IPv6 Network Design & Operation(Session 1).** [Slide]. Thailand: Cisco Systems,Inc.

ประวัติผู้เขียน

ชื่อผู้จัดทำโครงการ	นางสาวปาลิน รัตนพันธ์
วันเดือนปีเกิด	15 มกราคม 2527
สถานที่เกิด	นครศรีธรรมราช

ประวัติการศึกษา

มัธยมศึกษาตอนต้น	โรงเรียนจุฬาภรณราชวิทยาลัย นครศรีธรรมราช
มัธยมศึกษาตอนปลาย	โรงเรียนจุฬาภรณราชวิทยาลัย นครศรีธรรมราช
อุดมศึกษา	มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตภูเก็ต

ประวัติการทำงาน

พ.ศ.2549-2551	วิศวกร โครงข่าย บริษัท ทีทีแอนด์ที จำกัด มหาชน
พ.ศ.2552-2555	วิศวกร โครงข่าย บริษัท ทริปเปิลที บรอดแบนด์ จำกัด มหาชน