สำนักงานคณะกรรมการกิจการโทรคมนาคมแห่งชาติ

รายงานระหว่างทาง

การศึกษากระบวนการเปลี่ยนแปลงโครงข่ายอินเตอร์เน็ต จาก IPv4 มาเป็น IPv6 และเสนอแนะแนวทางหรือมาตรการการกำกับดูแลการใช้งาน IPv6 ในประเทศไทย

A Study on Internet Network Migration from IPv4 to IPv6 and a Recommendation on Guideline or Regulation of IPv6 Usage in Thailand

สัญญาจ้างที่ สป 26/49
ลงวันที่ 30 พฤศจิกายน 2549

เสนอ
คณะกรรมการกิจการโทรคมนาคมแห่งชาติ

เสนอโดย
รศ. ดร.วาทิต เบญจพลกุล และคณะ

29 ธันวาคม 2549

สารบัญ

		หน้า
บทที่ 1	โพรโทคอล TCP/IP IPv4 และ IPv6	1
บทที่ 2	ความจำเป็นและแนวโน้มที่จะนำ IPv6 มาใช้ในประเทศไทย	17
บทที่ 3	ตัวอย่างการใช้งาน IPv6 ในต่างประเทศ	28
บทที่ 4	ผลกระทบการใช้งาน IPv6 ในเทคโนโลยีที่มีในปัจจุบันและเทคโนโลยีที่จะเกิดขึ้นในอนาคต	39
บทที่ 5	สรุปผลกระทบการใช้งาน IPv6 กับผู้ใช้งานอินเตอร์เน็ต ผู้ให้บริการอินเตอร์เน็ต หน่วยงานกำกับดูแล และผู้ผลิตอุปกรณ์และซอฟต์แวร์	50
บทที่ 6	สรุปรายงานระหว่างทาง	54
รายการอ้างอิง		55

บทที่ 1
โพรโทคอล TCP/IP IPv4 และ IPv6

คำว่าอินเตอร์เน็ต (Internet) หรือโครงข่ายอินเตอร์เน็ตเป็นระบบโครงข่ายสื่อสารข้อมูลระหว่างคอมพิวเตอร์ที่ใช้กันอย่างแพร่หลายทั่วโลก และรองรับการประยุกต์ใช้งานอย่างกว้างขวาง โครงข่ายอินเตอร์เน็ตมีจุดเริ่มต้นมาจากโครงการวิจัยและพัฒนาโครงข่าย packet-switching ของ Advanced Research Project Agency (ARPA) ซึ่งเป็นหน่วยงานของรัฐบาลกลางสหรัฐในปี พ.ศ. 2512 มีชื่อว่าโครงข่าย ARPANET มีวัตถุประสงค์เพื่อใช้ศึกษาเทคนิคในการสื่อสารข้อมูลที่ robust, เชื่อถือได้ (reliable), และไม่ขึ้นกับผู้ผลิต (Vendor) มีการทดลองตั้งโครงข่ายที่ให้เครื่องคอมพิวเตอร์สามารถติดต่อกับเครื่องคอมพิวเตอร์ของมหาวิทยาลัยอื่นได้ ความสำเร็จของ ARPANET ทำให้องค์กรต่าง ๆ หลายองค์กรเริ่มนำมาใช้เพื่อการสื่อสารข้อมูลในชีวิตประจำวัน ภายหลังมีการพัฒนาชุดโพรโทคอลที่ใช้ในการสื่อสารข้อมูลขึ้นมา ซึ่งในชุดโพรโทคอลนี้มีโพรโทคอลสองโพรโทคอลคือ Transmission Control Protocol (TCP) และ Internet Protocol (IP) ซึ่งเป็นโพรโทคอลที่มีความสำคัญและเป็นที่รู้จักมากที่สุด จึงเรียกชุดโพรโทคอลนี้ว่าโพรโทคอล TCP/IP โพรโทคอล TCP/IP ได้รับการพัฒนาอย่างต่อเนื่องเรื่อยมา มีการนำไปประยุกต์ใช้งานอย่างแพร่หลายไม่ว่าจะเป็นการใช้จดหมายอิเล็กทรอนิกส์หรือ e-mail การสนทนาด้วยการพิมพ์ข้อความผ่าน Internet และการใช้โทรศัพท์ผ่านอินเตอร์เน็ตหรือ VoIP (Voice over IP) รวมถึงการใช้ World Wide Web (www) ที่ได้รับความนิยมอย่างกว้างขวาง มีการนำไปใช้ในโครงข่ายทั้งแบบ Internet, Intranet, และ Extranet

ในปัจจุบันโพรโทคอล IP ที่ใช้อยู่คือ Internet Protocol version 4 (IPv4) ซึ่งใช้เป็นมาตรฐานในการส่งข้อมูลผ่านโครงข่าย TCP/IP ตั้งแต่ปี พ.ศ. 2524 เลขที่อยู่ไอพี (IP address) ของ IPv4 มีขนาด 32 บิตหรือมีจำนวนเลขที่อยู่ไอพีประมาณ 429 ล้านเลขที่อยู่ แต่อัตราการเติบโตของโครงข่ายอินเตอร์เน็ตที่ขยายตัวอย่างรวดเร็ว ทำให้จำนวนเลขที่อยู่ไอพีของ ชุดโพรโทคอล กำลังจะถูกใช้หมดไป ดังนั้นคณะทำงาน IETF (The Internet Engineering Task Force) จึงได้พัฒนา Internet Protocol version 6 (IPv6) เพื่อทดแทน IPv4 โดยมีวัตถุประสงค์ เพื่อปรับปรุงโครงสร้างของตัวโพรโทคอล ให้รองรับจำนวนเลขที่อยู่ไอพีจำนวนมาก มีการปรับปรุงโครงสร้างของเฮดเดอร์ (Header) โดยเฮดเดอร์ของข้อมูลแบบ IPv6 ออกแบบมาให้มีขนาดคงที่ (40 ไบต์) และมีรูปแบบที่เรียบง่ายที่สุด ถูกจัดสรรอย่างเป็นระบบมากขึ้น เพิ่มประสิทธิภาพในการประมวลผลแพ็กเกต (packet) ให้ดีขึ้น สามารถตอบสนองต่อการขยายตัวและความต้องการใช้งานเทคโนโลยีบนโครงข่ายอินเตอร์เน็ตในอนาคตได้เป็นอย่างดี

1.1 โครงข่ายอ้างอิง OSI

ในปี พ.ศ. 2520 องค์การมาตรฐานระหว่างประเทศ (International Standard Organization หรือ ISO) ได้จัดตั้งคณะกรรมการขึ้นกลุ่มหนึ่ง เพื่อศึกษาและกำหนดแบบจำลองแสดงหน้าที่การทำงานในการสื่อสาร และในปี พ.ศ. 2526 องค์กร ISO ก็ได้ออกประกาศรูปแบบของสถาปัตยกรรมโครงข่ายมาตรฐานเรียกว่า แบบจำลองอ้างอิง (reference model) หรือที่รู้จักกันในชื่อของ "แบบจำลอง OSI" (Open System Interconnection Model) สำหรับการสื่อสารข้อมูลระหว่างระบบคอมพิวเตอร์ด้วยกัน แบบจำลองนี้คือ แบบจำลองอ้างอิงการต่อถึงระหว่างกันของระบบแบบเปิด (Open Systems Interconnection (OSI) reference model) หมายถึงการที่คอมพิวเตอร์หรือระบบคอมพิวเตอร์หนึ่งสามารถ "เปิด" กว้างให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์อื่นที่ใช้มาตรฐาน OSI เหมือนกันสามารถติดต่อสื่อสารกันได้ แบบจำลองอ้างอิงนี้แบ่งโครงสร้างของสถาปัตยกรรมโครงข่ายออกเป็นชั้น ๆ โดยชั้นแต่ละชั้นจะกำหนดหน้าที่การทำงานและบริการต่าง ๆ ที่ต้องการ รวมถึงกำหนดรูปแบบการต่อระหว่างชั้นด้วย

OSI	
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

รูปที่ 1.1 แบบจำลอง OSI (Open System Interconnection Model)

แบบจำลอง OSI มีรูปแบบดังรูปที่ 1.1 มีการแบ่งโครงสร้างออกเป็น 7 ชั้น และในชั้นแต่ละชั้นได้มีการกำหนดหน้าที่การทำงานไว้ ดังต่อไปนี้

1. ชั้นกายภาพ (physical) เป็นชั้นล่างที่สุดของการติดต่อสื่อสาร รับผิดชอบเกี่ยวกับการส่งข้อมูลด้วยวิธีทางกายภาพผ่านช่องทางการสื่อสาร (สื่อกลาง) ระหว่างคอมพิวเตอร์เครื่องหนึ่งกับคอมพิวเตอร์เครื่องอื่น ๆ

2. ชั้นเชื่อมโยงข้อมูล (data link) มีหน้าที่ควบคุมการส่งข้อมูลไม่มีความผิดพลาดผ่านวงจรที่ต่อระหว่างคอมพิวเตอร์ที่อยู่ประชิดกัน และยังมีหน้าที่ป้องกันไม่ให้เครื่องส่ง ส่งข้อมูลเร็วจนเกินขีดความสามารถของเครื่องรับจะรับข้อมูลได้

3. ชั้นโครงข่าย (network) เป็นชั้นที่จัดเส้นทางปลายถึงปลายผ่านคอมพิวเตอร์ระหว่างทาง ออกแบบหรือกำหนดเส้นทางการเดินทางของข้อมูลที่จะส่งรับ ในการส่งผ่านข้อมูลระหว่างต้นทางและปลายทาง ทำหน้าที่เลือกเส้นทางที่ใช้เวลาในการสื่อสารน้อยที่สุด และระยะทางสั้นที่สุดด้วย

4. ชั้นเคลื่อนย้าย (transport) ทำหน้าที่กำหนดที่อยู่ของกระบวนการผู้ใช้ (user process) ที่ปลายทาง จัดหาช่องสัญญาณเพื่อส่งข่าวสารให้ตรงตามลำดับและไม่มีความผิดพลาดจากกระบวนการผู้ใช้หนึ่งไปยังกระบวนการผู้ใช้อื่น

5. ชั้นเซสชัน (session) ทำหน้าที่จัดการ (organize) และซิงโครไนซ์คาบเวลาหรือควบคุมจังหวะการสื่อสารโต้ตอบระหว่างกระบวนการผู้ใช้ของต้นทางกับปลายทาง รับผิดชอบเกี่ยวกับการสร้างเซสชันอนุญาตให้เกิดการต่อถึงกันในชั้นเคลื่อนย้ายระหว่างกระบวนการผู้ใช้ของต้นทางและปลายทาง ควบคุมการแลกเปลี่ยนข้อมูลให้การต่อถึงกันนั้นเป็นไปอย่างต่อเนื่องโดยไม่ขาดตอน รวมทั้งการยกเลิกเซสชันเมื่อการต่อถึงกันนั้นสิ้นสุดลง

6. ชั้นนำเสนอ (presentation) กำหนดรูปแบบ (format) ของการส่งข้อมูลหรือแปลงรูปแบบของข้อมูลให้เป็นรูปแบบการสื่อสารเดียวกัน กำหนดวิธีการแปลงข้อมูลให้อยู่ในฟอร์แมต (format) ที่เหมาะสมสำหรับการส่ง หรืออาจกำหนดวิธีอัดข้อมูลให้มีขนาดเล็กลงซึ่งจะทำให้อัตราข้อมูลสูงขึ้น หรือกำหนดวิธีเข้ารหัสลับ (encryption) เพื่อความปลอดภัยในการส่งข้อมูล

7. ชั้นประยุกต์ใช้งาน (application) หน้าที่ของชั้นประยุกต์ใช้งานคือ ให้บริการเฉพาะอย่างตามที่ผู้ใช้ต้องการ และให้บริการทั่วๆ ไปกับบริการเฉพาะอย่างทุกบริการ โดยใช้บริการของชั้นที่อยู่ต่ำกว่า สามารถนำเข้า หรือออกจากระบบโครงข่ายได้โดยไม่จำเป็นต้องสนใจว่ามีขั้นตอนการทำงานอย่างไร

1.2 โครงข่าย TCP/IP

ในปี พ.ศ. 2512 Advanced Research Project Agency (ARPA) ได้ก่อตั้งโครงการวิจัยและพัฒนาโครงข่าย packet-switching ที่มีชื่อว่า ARPANET ต่อมาในปี พ.ศ. 2518 ARPANET ได้เปลี่ยนจากโครงข่ายเพื่อการศึกษาทดลองมาเป็นโครงข่ายที่ใช้ในการปฏิบัติงาน (Operation network) โดยมี Defense Communication Agency (DCA) ซึ่งต่อมาภายหลังเปลี่ยนชื่อเป็น Defense Information Systems Agency (DISA) ทำหน้าที่เป็นผู้รับผิดชอบบริหารจัดการโครงข่าย ผลจากการออกแบบของ ARPANET เพื่อใช้ในการเชื่อมโยงคอมพิวเตอร์ที่มีความแตกต่างกัน และอยู่ห่างไกลกันให้สามารถติดต่อสื่อสารข้อมูลกันได้ สามารถทำให้ข้อมูลส่งผ่านเส้นทางหรือเปลี่ยนเส้นทางใหม่ได้มากกว่า 1 เส้นทาง และโครงข่ายยังสามารถทำงานต่อไปได้ แม้ว่าจะมีโครงข่ายบางส่วนถูกทำลายไป และผลการใช้งานก็เป็นที่น่าพอใจอย่างมาก โครงข่าย ARPANET ได้รับการ

พัฒนาอย่างต่อเนื่อง และได้ถูกนำมาใช้อย่างแพร่หลาย ซึ่งเทคนิคการสื่อสารข้อมูลในปัจจุบันหลายอย่างได้รับการพัฒนาโดย ARPANET ต่อมา ARPANET ได้มีการพัฒนาโพรโทคอล TCP/IP (Transmission Control Protocol และ Internet Protocol) ขึ้นมา โดยโพรโทคอล TCP/IP มีการแบ่งโครงสร้างออกเป็นชั้น (Layer) คล้ายกับแบบจำลองอ้างอิง Open System Interconnect (OSI) ทำให้ผู้ผลิตและพัฒนาอุปกรณ์ฮาร์ดแวร์และซอฟต์แวร์สามารถพัฒนาผลิตภัณฑ์ของตนเองให้สามารถทำงานร่วมกับส่วนอื่นได้ โดยไม่ต้องคำนึงถึงการออกแบบหรือพัฒนาส่วนอื่น ๆ แบบจำลอง OSI มีโครงสร้างในการทำงานที่ดีกว่า ดังนั้นส่วนใหญ่จึงนิยมใช้แบบจำลอง OSI เป็นแบบอ้างอิงสำหรับการสื่อสารข้อมูลระหว่างคอมพิวเตอร์ในโครงข่าย แต่การออกแบบโพรโทคอล TCP/IP เน้นไปที่การต่อกับโครงข่ายที่ใช้โพรโทคอลที่ต่างกันมากกว่าแบบจำลอง OSI ดังนั้นโพรโทคอล TCP/IP จึงนิยมใช้กับโครงข่ายในการทำงานจริงมากกว่า ปัจจุบันโพรโทคอล TCP/IP เป็นโพรโทคอลที่นิยมใช้ในโครงข่ายต่าง ๆ มากที่สุด โดยโพรโทคอล TCP/IP เป็นโพรโทคอลพื้นฐานที่ใช้ในโครงข่ายอินเตอร์เน็ต ซึ่งเป็นโครงข่ายที่ใหญ่ที่สุดในโลก

โครงข่าย TCP/IP แบ่งชุดของโพรโทคอลออกเป็น 4 ชั้นได้แก่ ชั้น Network Access, ชั้น Internet, ชั้น Host-to-Host, และชั้น Application (รูปที่ 1.2)

1. ชั้น Network Access จะประกอบด้วยโพรโทคอลสำหรับการควบคุมการสื่อสารผ่านช่องสัญญาณของโครงข่าย โพรโทคอลในชั้นนี้เป็นสิ่งที่ไม่มีการกำหนดรายละเอียดอย่างเป็นทางการ หน้าที่หลักคือการรับข้อมูลจากชั้น Internet จัดหาเส้นทางของข้อมูลให้ระหว่าง Host กับ Host ควบคุมการไหล ของข้อมูล และควบคุมความผิดพลาดของข้อมูล

2. ชั้น Internet ทำหน้าที่จัดเส้นทางให้ข้อมูลขนาดเล็กที่เรียกว่า แพ็กเกต (Packet) ซึ่งจะถูกส่งจากคอมพิวเตอร์ต้นทางไปตามโนดต่าง ๆ ในโครงข่ายจนถึงคอมพิวเตอร์ปลายทาง โพรโทคอลในชั้นนี้เป็นโพรโทคอลที่ให้บริการแบบ Connectionless คือไม่มีการสร้างการต่อถึงกันระหว่างคอมพิวเตอร์ต้นทางกับคอมพิวเตอร์ปลายทางก่อนการรับส่งข้อมูล ทำให้แพ็กเกตแต่ละแพ็กเกตถูกส่งอย่างอิสระต่อกัน ดังนั้นแพ็กเกตที่ส่งไปถึงคอมพิวเตอร์ปลายทางอาจจะไม่เป็นไปตามลำดับก็ได้

3. ชั้น Host-to-Host ประกอบด้วยโพรโทคอล 2 โพรโทคอลคือ Transmission Control Protocol (TCP) และ User Datagram Protocol (UDP) โพรโทคอล TCP ให้บริการแบบ connection-oriented มีการกำหนดการต่อถึงกันระหว่างคอมพิวเตอร์ต้นทางกับคอมพิวเตอร์ปลายทางตลอดระยะเวลาการสื่อสาร ทำให้การส่งข้อมูลเชื่อถือได้ ข้อมูลที่มีปริมาณมากจะถูกแบ่งออกเป็นส่วนเล็ก ๆ ก่อนที่จะถูกส่งผ่านโครงข่ายไปยังคอมพิวเตอร์ปลายทาง และจะมีกลไกที่จะนำข้อมูลมาเรียงต่อกันตามลำดับเป็นข้อมูลตัวเดิม TCP ยังมีความสามารถในการควบคุมการไหลของข้อมูลเพื่อป้องกันไม่ให้ผู้ส่ง ส่งข้อมูลเร็วเกินกว่าที่ผู้รับจะทำงานได้ทันอีกด้วย โพรโทคอลการนำส่งข้อมูลแบบที่สองเรียกว่า โพรโทคอล UDP ให้บริการแบบ connectionless ไม่มีการสร้างการต่อถึงกันก่อนทำการรับส่งข้อมูล ข้อมูลถูกส่งแบบไม่ต่อเนื่อง มีการตรวจสอบความถูกต้องของข้อมูล แต่จะไม่มีการแจ้งกลับไปยังผู้ส่ง จึงถือได้ว่าไม่มีการตรวจสอบความถูกต้องของข้อมูล

4. ชั้น Application ประกอบด้วยโพรโทคอลต่าง ๆ ที่ทำหน้าที่ให้บริการแลกเปลี่ยนข้อมูลระหว่างคอมพิวเตอร์ต้นทางกับคอมพิวเตอร์ปลายทาง เช่นโพรโทคอล FTP สำหรับการจัดการแฟ้มข้อมูล โพรโทคอล TELNET สำหรับสร้างจออุปกรณ์ปลายทางเสมือน (Virtual Terminal) โพรโทคอล SMTP สำหรับการให้บริการจดหมายอิเล็กทรอนิกส์ เป็นต้น

<table>
<tr><th colspan="2">OSI</th><th colspan="3">TCP/IP</th></tr>
<tr><td>7</td><td>Application</td><td rowspan="3">Application</td><td colspan="2" rowspan="3">FTP, Telnet, HTTP, SMTP, SNMP, DNS, etc.</td></tr>
<tr><td>6</td><td>Presentation</td></tr>
<tr><td>5</td><td>Session</td></tr>
<tr><td>4</td><td>Transport</td><td>Host-to-Host</td><td>TCP</td><td>UDP</td></tr>
<tr><td>3</td><td>Network</td><td>Internet</td><td>ICMP, IGMP
IP</td><td>ARP, RARP</td></tr>
<tr><td>2</td><td>Data Link</td><td rowspan="2">Network Access</td><td colspan="2" rowspan="2">Not Specified</td></tr>
<tr><td>1</td><td>Physical</td></tr>
</table>

รูปที่ 1.2 การเปรียบเทียบชั้นของโพรโทคอลระหว่าง OSI กับ TCP/IP

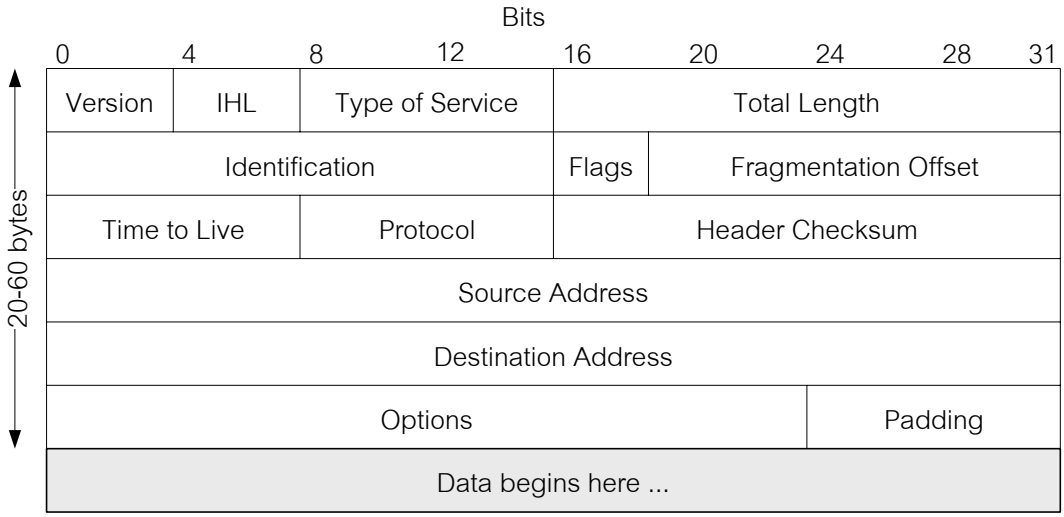
โดยการสื่อสารข้อมูลระหว่างเครื่องคอมพิวเตอร์จะเริ่มจากโปรแกรมประยุกต์ของผู้ใช้ส่งข้อมูลให้กับโพรโทคอลในชั้น Application ชั้น Application จะเพิ่มข้อมูลเกี่ยวกับชื่อของคอมพิวเตอร์ที่ต้องการสื่อสารด้วยและหมายเลขพอร์ตที่จะติดต่อกับเครื่องนั้นลงไปในเฮดเดอร์ของชั้น Application จากนั้นจะส่งข้อมูลให้กับชั้น Host-to-Host ซึ่งในชั้นนี้อาจใช้โพรโทคอล TCP หรือ UDP ก็ได้ ขึ้นอยู่กับรูปแบบของการประยุกต์ใช้งาน ในชั้นนี้จะแบ่งข้อมูลออกเป็นส่วนย่อย ๆ และมีการเพิ่มเฮดเดอร์ให้กับส่วนย่อยแต่ละส่วน ข้อมูลส่วนย่อยนี้เรียกว่าเซกเมนต์ โดยเฮดเดอร์ที่เพิ่มเข้าไปก็เพื่อทำหน้าที่ควบคุมการไหลของข้อมูล รวมทั้งควบคุมความผิดพลาดของข้อมูลด้วย หลังจากนั้นเซกเมนต์แต่ละเซกเมนต์จะถูกส่งต่อไปยังชั้น Internet และมีการเพิ่มเฮดเดอร์ที่มีข้อมูลสำคัญคือเลขที่อยู่ไอพีของเครื่องคอมพิวเตอร์ต้นทางและเครื่องคอมพิวเตอร์ปลายทาง ซึ่งจะถูกนำไปใช้ในการจัดเส้นทางการเดินทางของข้อมูลในโครงข่าย ชุดข้อมูลที่อยู่ในชั้นนี้เรียกว่าแพ็กเกต หลังจากนั้นจะส่งแพ็กเกตแต่ละแพ็กเกตไปยังชั้น Network Access เพื่อส่งแพ็กเกตผ่านช่องสัญญาณสื่อสารให้เดินทางไปยังเครื่องคอมพิวเตอร์ปลายทางต่อไป เมื่อข้อมูลเดินทางถึงเครื่องคอมพิวเตอร์ปลายทาง โพรโทคอลในชั้น

ต่าง ๆ ของเครื่องคอมพิวเตอร์ปลายทางก็จะทำงานในทางกลับกันกับโพรโทคอลของเครื่องคอมพิวเตอร์ต้นทาง

1.3 Internet Protocol version 4

IP (Internet Protocol) เป็นโพรโทคอลที่ใช้ในการส่งข้อมูลจากเครื่องคอมพิวเตอร์ต้นทางไปยังเครื่องคอมพิวเตอร์ปลายทางในโครงข่าย ไม่ว่าจะเป็นโครงข่าย Internet, Intranet, หรือ Extranetเครื่องคอมพิวเตอร์แต่ละเครื่องในโครงข่ายจะต้องมีเลขที่อยู่ไอพีอย่างน้อยหนึ่งที่อยู่ และต้องไม่ซ้ำกับเลขที่อยู่ไอพีของคอมพิวเตอร์เครื่องอื่นในโครงข่าย เมื่อมีการส่งและรับข้อมูล ข้อมูลจะถูกแบ่งเป็นชุดข้อมูล เรียกว่า แพ็กเกต (Packet) โดยแพ็กเกตแต่ละแพ็กเกตจะเก็บเลขที่อยู่ไอพีของเครื่องคอมพิวเตอร์ต้นทางและเครื่องคอมพิวเตอร์ปลายทางไว้ในเฮดเดอร์ โพรโทคอล IP จะทำหน้าที่จัดการเกี่ยวกับเลขที่อยู่ไอพี และควบคุมการการหาเส้นทางของแพ็กเกตให้ได้เส้นทางที่เหมาะที่สุด และสามารถเปลี่ยนแปลงเส้นทางได้ในระหว่างการส่งข้อมูล โพรโทคอล IP ใช้วิธีการต่อถึงกันแบบ connectionless โดยเครื่องคอมพิวเตอร์ต้นทางจะไม่ติดต่อกับเครื่องคอมพิวเตอร์ปลายทางเพื่อตกลงเกี่ยวกับการรับส่งข้อมูลก่อน แต่เครื่องคอมพิวเตอร์ต้นทางจะส่งแพ็กเกตออกไปทันที โดยคาดหวังว่าเครื่องคอมพิวเตอร์ปลายทางจะได้รับแพ็กเกตนั้น ดังนั้นความน่าเชื่อถือได้ในการส่งข้อมูลจึงน้อย เนื่องจากแพ็กเกตอาจสูญหายระหว่างทางได้

IP ที่ใช้อย่างกว้างขวางในปัจจุบันนี้คือ Internet Protocol version 4 (IPV4) ซึ่งรูปแบบของเฮดเดอร์ของ IP โดยปกติจะมีขนาด 20 bytes ยกเว้นในกรณีที่มีการเพิ่ม option หรือข้อมูลที่จำเป็นบางอย่าง ดังรูปที่ 1.3



รูปที่ 1.3 IPv4 Header

ข้อมูลในฟิลด์ของเฮดเดอร์ IP มีความหมายดังต่อไปนี้

- Version (4 บิต): ข้อมูล 4 บิตแรกที่บอกหมายเลขเวอร์ชันของโพรโทคอล IP ที่ใช้ ซึ่งในปัจจุบันคือเวอร์ชัน 4 (IPv4)
- Internet Header Length หรือ IHL (4 บิต): ตัวเลขที่บอกความยาวของเฮดเดอร์ โดยทั่วไปถ้าไม่มีส่วน option จะมีค่าเป็น 5 หรือ 20 bytes
- Type of Service หรือ TOS (8 บิต): ข้อมูลในฟิลด์นี้แต่ละบิตจะเป็น Flag บอกลำดับความสำคัญ, การประวิง, Throughput ใช้เป็นข้อมูลสำหรับเราเตอร์ในการตัดสินใจเลือกการจัดเส้นทางให้กับแพ็กเกตแต่ละแพ็กเกต (ในปัจจุบันไม่ได้มีการนำไปใช้งานแล้ว)
- Total Length (16 บิต): ความยาวทั้งหมดของแพ็กเกต มีหน่วยเป็นจำนวนไบต์ ขนาดของฟิลด์นี้มีขนาด 16 บิต ดังนั้นความยาวสูงสุดของแพ็กเกตที่เป็นไปได้ คือ 65536 bytes
- Identification (16 บิต): เป็นหมายเลขของดาต้าแกรมในกรณีที่มีการแยกดาต้าแกรมออกเป็นแพ็กเกตหลายแพ็กเกต เมื่อข้อมูลส่งถึงปลายทางจะนำแพ็กเกตที่มี identification เดียวกันมารวมกัน
- Flags (3 บิต): ใช้ในกรณีที่มีการแยกดาต้าแกรมออกเป็นแพ็กเกตหลายแพ็กเกต
- Fragment action offset (13 บิต): เป็นค่าบอกตำแหน่งของแพ็กเกตในดาตาแกรมที่มีการแยกส่วนเพื่อให้สามารถนำแพ็กเกตกลับมาเรียงต่อกันได้อย่างถูกต้อง
- Time to live หรือ TTL (8 บิต): บอกระยะเวลานานที่สุดที่แพ็กเกตจะสามารถอยู่ในโครงข่าย เพื่อป้องกันไม่ให้เกิดการส่งข้อมูลโดยไม่สิ้นสุด โดยเมื่อข้อมูลถูกส่งไป 1 hop จะเป็นการลดค่า TTL ลง 1 เมื่อค่าของ TTL เป็น 0 และข้อมูลยังไม่ถึงปลายทาง ข้อมูลนั้นจะถูกยกเลิก และเราเตอร์สุดท้ายจะส่งข้อมูล ICMP แจ้งกลับมายังต้นทางว่าเกิด time out ในระหว่างการส่งข้อมูล
- Protocol (8 บิต): ระบุโพรโทคอลของชั้นที่อยู่สูงกว่า เช่น TCP, UDP หรือ ICMP
- Header checksum (16 บิต): ใช้ในการตรวจวัดความผิดพลาดของข้อมูลในเฮดเดอร์
- Source IP address (32 บิต): เลขที่อยู่ไอพีของเครื่องคอมพิวเตอร์ต้นทาง
- Destination IP address (32 บิต): เลขที่อยู่ไอพีของเครื่องคอมพิวเตอร์ปลายทาง
- Data: ข้อมูลจากโพรโทคอลชั้นที่อยู่สูงกว่า ซึ่งมีความยาวไม่คงที่

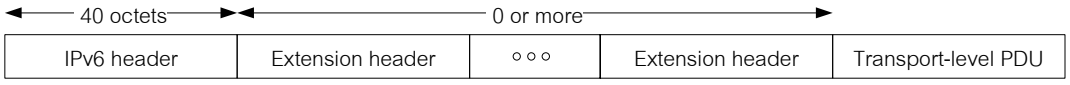
โพรโทคอล IPv4 ใช้เป็นมาตรฐานมาตั้งแต่ปี พ.ศ. 2524 แต่เนื่องจากอัตราการเติบโตของโครงข่ายอินเตอร์เน็ตที่ขยายตัวอย่างรวดเร็ว จำนวนเครื่องคอมพิวเตอร์ที่ต่อถึงกันกับโครงข่ายอินเตอร์เน็ตกำลังเพิ่มสูงขึ้นเรื่อย ๆ ทำให้จำนวนเลขที่อยู่ไอพีของ IPv4 กำลังจะถูกใช้หมดไป นอกจากนี้ IPv4 ยังมีปัญหาในการจัดเส้นทางที่ไม่มีประสิทธิภาพ และไม่รองรับรูปแบบการใช้งานโครงข่ายอินเตอร์เน็ตที่เปลี่ยนไป เนื่องจากในปัจจุบันมีความต้องการใช้งานในรูปแบบมัลติมีเดียมากขึ้น นอกจากนี้ยังมีความต้องการการรักษาความปลอดภัยของข้อมูลในชั้นโครงข่าย ทำให้มีความจำเป็นต้องพัฒนาโพรโทคอล IP เวอร์ชันใหม่ขึ้นมาเพื่อแก้ปัญหาและรองรับความต้องการใช้งานเทคโนโลยีบนโครงข่ายอินเตอร์เน็ตในอนาคตได้

1.4 Internet Protocol version 6

Internet Protocol version 6 หรือ IPv6 เป็นเวอร์ชันล่าสุดของ Internet Protocol บางครั้งถูกเรียกว่า Next Generation Internet Protocol หรือ IPng IPv6 ได้รับการพัฒนาโดย Internet Engineering Task Force (IETF) กำหนดในมาตรฐาน RFC 2460 “Internet Protocol Version 6 (IPv6) Specification” IPv6 ถูกพัฒนาขึ้นมาเพื่อทดแทน IPv4 มีการปรับปรุงแก้ไขข้อบกพร่องของ IPv4 หลายประการ IPv6 ปรับปรุงโครงสร้างของตัวโพรโทคอลให้มีประสิทธิภาพสูงขึ้น รองรับการทำงานของเทคโนโลยีใหม่ ๆ รองรับหมายเลขที่อยู่จำนวนมาก IPV6 มีการปรับปรุงโครงสร้างของเฮดเดอร์ โดยออกแบบให้มีขนาดคงที่ (40 ไบต์) และมีรูปแบบที่เรียบง่ายที่สุด ถูกจัดสรรอย่างเป็นระบบมากขึ้น เพิ่มประสิทธิภาพในการประมวลผลแพ็กเกต (packet) ให้ดีขึ้น สามารถตอบสนองต่อการขยายตัวและความต้องการใช้งานเทคโนโลยีบนโครงข่ายอินเตอร์เน็ตในอนาคตได้เป็นอย่างดี ความแตกต่างระหว่าง IPv6 และ IPv4 หลัก ๆ คือ ขนาดของเลขที่อยู่ไอพีที่เปลี่ยนจาก 32 บิตเป็น 128 บิต การเพิ่มขนาดของเลขที่อยู่ไอพีทำให้สามารถกำหนดเลขที่อยู่ไอพีให้กับเครื่องคอมพิวเตอร์หรืออุปกรณ์ต่าง ๆ ได้โดยไม่ต้องใช้เลขที่อยู่ไอพีซ้ำกัน รองรับการขยายตัวของโครงข่ายอินเตอร์เน็ตที่มีอัตราการเติบโตอย่างรวดเร็วได้ มีการออกแบบเลขที่อยู่ไอพีเป็นแบบลำดับชั้น กำหนดโครงสร้างการจัดเส้นทางได้ ทำให้การจัดเส้นทางทำได้ง่ายและมีประสิทธิภาพ รองรับการกำหนดเลขที่อยู่ไอพีแบบแจ้งค่าไว้ก่อน (Stateful) และแบบไม่แจ้งค่าไว้ก่อน (Stateless) นอกจากนี้ยังมีการปรับปรุงในเรื่องความปลอดภัย (Security) และรองรับการ Authentication โดยที่เราเตอร์และอุปกรณ์โครงข่ายทุกตัวในโครงข่าย IPv6 ถูกกำหนดให้รองรับการใช้งาน IPSec สนับสนุนการรับส่งข้อมูลที่ปลอดภัย

1.5 รูปแบบและหน้าที่การทำงานของ IPv6

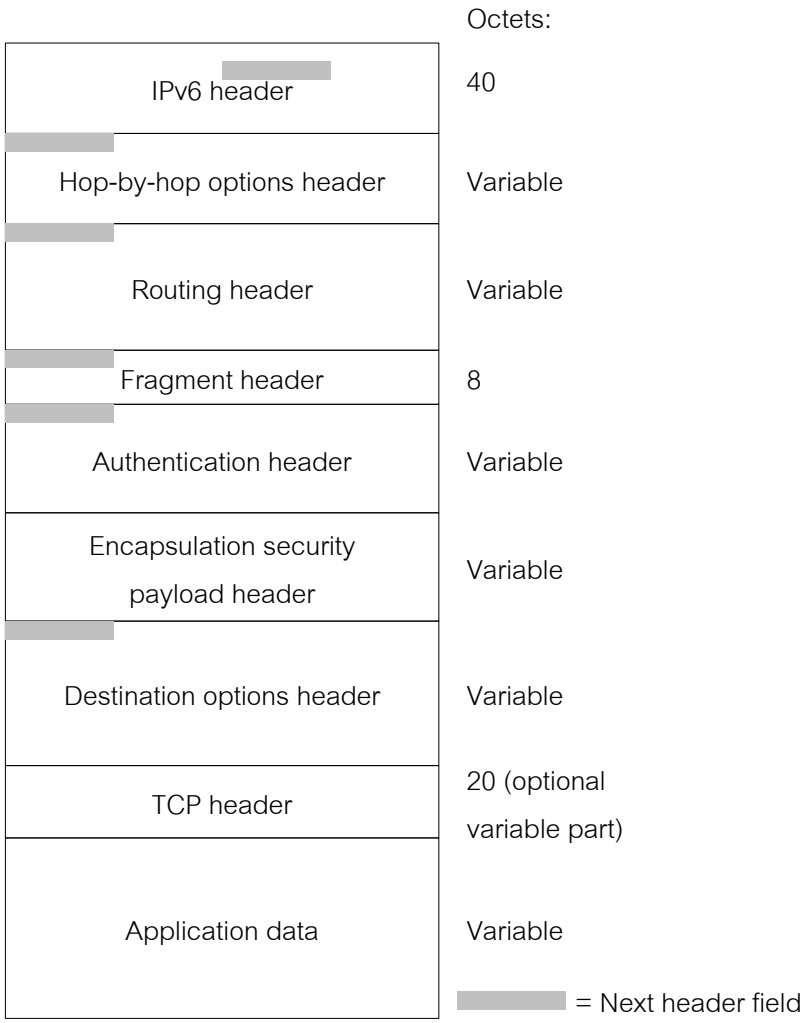
IPv6 Protocol Data Unit หรือที่เรียกว่าแพ็กเกต (packet) มีรูปแบบทั่วไปดังรูปที่ 1.4



รูปที่ 1.4 รูปแบบทั่วไปของ IPv6 Protocol Data Unit

IPv6 มีการปรับปรุงโครงสร้างของเฮดเดอร์ (Header) ให้มีรูปแบบที่เรียบง่ายที่สุด เฮดเดอร์ของข้อมูลแบบ IPv6 ออกแบบมาให้มีขนาดคงที่ (40 ไบต์) แตกต่างกับเฮดเดอร์ของ IPv4 ที่มีขนาดไม่คงที่ (เปลี่ยนแปลงตามขนาดของ option) การที่เฮดเดอร์มีขนาดคงที่ทำให้อุปกรณ์ในโครงข่ายสามารถประมวลผลเฮดเดอร์ได้ง่ายและเร็วขึ้นเพราะไม่ต้องเสียเวลาในการคำนวณขนาดของ header ส่วนฟิลด์บางฟิลด์ที่ยังมีความสำคัญหรือมี

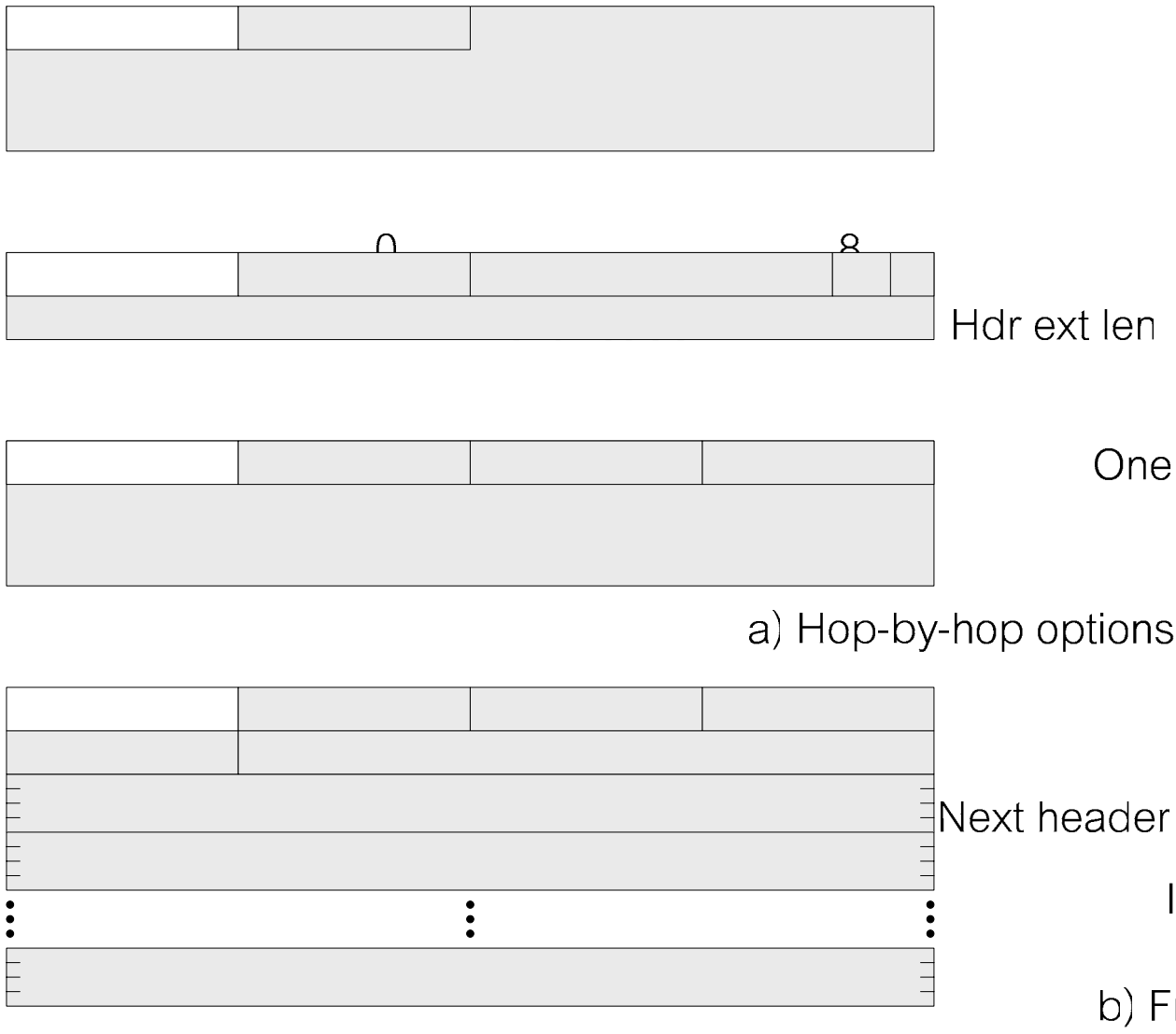
ประโยชน์ในการส่งแพ็กเกต แต่อาจถูกประมวลผลเฉพาะที่ต้นทางหรือปลายทางหรือที่เราเตอร์บางตัว จะถูกแยกออกมาไว้ที่ส่วนขยายของเฮดเดอร์ (Extended Header) ไม่ใส่ไว้ในเฮดเดอร์โดยตรง และใช้ฟิลด์ Next Header เป็นตัวบอกว่าส่วนขยายของเฮดเดอร์ที่อยู่ถัดไปทำหน้าที่อะไร โครงสร้างของแพ็กเกตจึงประกอบด้วยเฮดเดอร์ ส่วนขยายของเฮดเดอร์ และข้อมูล เรียงต่อกันตามลำดับ ดังรูปที่ 1.5



รูปที่ 1.5 การเรียงต่อกันของเฮดเดอร์และส่วนขยายของเฮดเดอร์ (รูปที่ 1.6)

ส่วนขยายของเฮดเดอร์สำหรับ IPv6 มีการกำหนดไว้ดังต่อไปนี้

- Hop-by-hop options header : ระบุ option พิเศษที่จำเป็นต่อการประมวลผลแบบ hop-by-hop ซึ่งกำหนดให้ทุก router ที่อยู่ในเส้นทางจากต้นทางถึงปลายทางจะต้องทำตาม
- Routing header : ให้ข้อมูลในการจัดเส้นทางเพิ่มเติม คล้ายกับการทำ Source routing ของ IPv4 คือต้นทางสามารถกำหนดเส้นทางที่ packet ต้องผ่านได้
- Fragment header : เก็บข้อมูลที่จำเป็นสำหรับการแบ่งข้อมูลออกเป็นข้อมูลชุดเล็ก ๆ เพื่อส่งผ่านโครงข่าย รวมทั้งข้อมูลที่จำเป็นสำหรับการรวบรวมข้อมูลที่ถูกแบ่ง
- Authentication header : เป็นเฮดเดอร์ที่รองรับความปลอดภัย ใช้สำหรับทำ authentication
- Encapsulation security payload header : ESP รองรับการเข้ารหัส สำหรับทำ encryption และ cryptography
- Destination options header : เก็บข้อมูลเพิ่มเติมที่จำเป็นสำหรับโนดปลายทาง

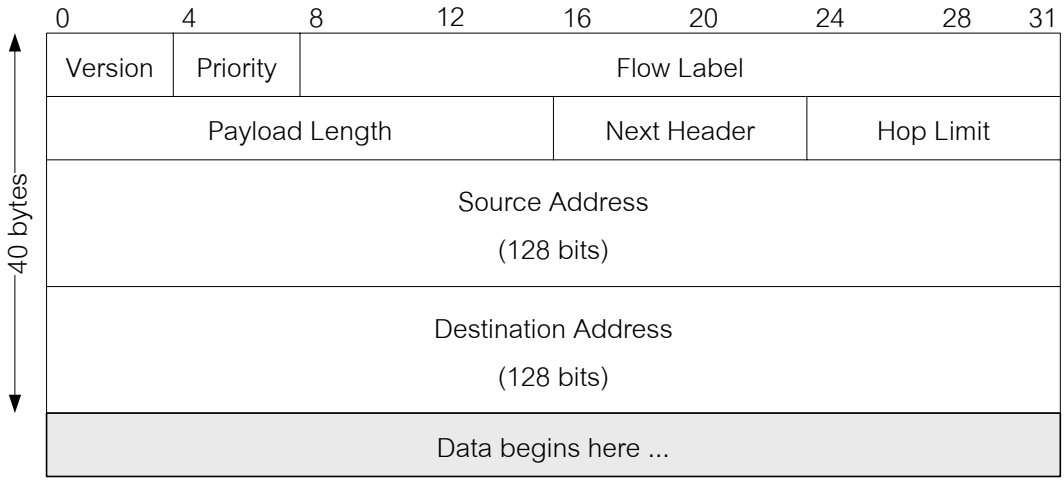


รูปที่ 1.6 ส่วนขยายของเฮดเดอร์ของ IPv6

นอกจากนี้เฮดเดอร์ของข้อมูลแบบ IPv6 ยังถูกจัดให้อยู่ในตำแหน่งที่ต่างกันออกไปเพื่อลดปัญหาเรื่องของการจัดเส้นทาง อย่างที่เคยเกิดกับ IPv4 โดยเฮดเดอร์จะประกอบด้วยตำแหน่งต่าง ๆ ที่จำเป็นต้องใช้ในการประมวลผลแพ็กเกตที่เราเตอร์ (router) หรืออุปกรณ์จัดเส้นทางทุกตัวเท่านั้น มีการตัดฟีลด์ที่ไม่จำเป็นทิ้งไป 6 ฟีลด์ ปรับปรุงฟีลด์ที่มีอยู่ให้มีประสิทธิภาพมากขึ้น 5 ฟีลด์ และมีการเพิ่มฟีลด์ใหม่อีก 2 ฟีลด์ ถึงแม้ว่าเฮดเดอร์ของ IPv6 จะมีจำนวนไบต์มากกว่าเฮดเดอร์ของIPv4 แต่ดูเรียบง่ายกว่าเฮดเดอร์ของ IPv4 มากเนื่องจากข้อมูลหลายตำแหน่งถูกตัดออกไป IPv6 มีการปรับปรุงให้สนับสนุนการประยุกต์ใช้งานแบบ Real Time ปรับปรุงการรับประกันคุณภาพของบริการ (Quality of service) โดยออกแบบมาให้สนับสนุนการรับประกัน

คุณภาพของบริการตั้งแต่ตอนต้นของเฮดเดอร์ โดยจะเห็นได้จากตำแหน่ง Flow Label และ Traffic Class (หรือ Priority) ในเฮดเดอร์ ถึงแม้ว่าในเฮดเดอร์ของ IPv4 จะมีตำแหน่ง Type-of-Service แต่ไม่มีการใช้อย่างแพร่หลาย เนื่องจากไม่มีมาตรฐานในการกำหนดค่าและเราเตอร์บางตัวเท่านั้นที่สามารถประมวลผลตำแหน่ง ToS ได้ ที่ผ่านมา IPv4 มักปล่อยให้ Layer ข้างล่างจัดการเรื่อง QoS แทน

1.6 เฮดเดอร์ของ IPv6



รูปที่ 1.7 เฮดเดอร์ของ IPv6

ข้อมูลในฟิลด์ของเฮดเดอร์ IPv6 มีความหมายดังต่อไปนี้ (รูปที่ 1.7)

- Version (4 บิต): ระบุเวอร์ชันของโพรโทคอล ซึ่งในกรณี IPv6 ข้อมูลในฟิลด์นี้มีค่าเป็น 6
- Traffic Class หรือ Priority (8 บิต): ระบุชนิดหรือลำดับความสำคัญของข้อมูล
- Flow Label (20 บิต): กำหนดรูปแบบการสื่อสาร กำหนดลำดับของการไหลของข้อมูล
- Payload Length (16 บิต): ระบุขนาดของข้อมูล โดยไม่รวมส่วนที่เป็นเฮดเดอร์
- Next Header (8 บิต): ระบุชนิดของส่วนขยายเฮดเดอร์
- Hop Limit (8 บิต): ใช้กำหนดระยะทางที่แพ็กเกตสามารถเดินทางผ่านเราเตอร์ได้ กำหนดจำนวนการ hop ที่อนุญาตมีได้ โดยถ้า Hop Limit เป็น 0 ก็จะนำชุดข้อมูลนี้ทิ้ง
- Source Address (128 บิต): เลขที่อยู่ไอพีของเครื่องคอมพิวเตอร์ต้นทาง
- Destination Address (128 บิต): เลขที่อยู่ไอพีของเครื่องคอมพิวเตอร์ปลายทาง

จะเห็นว่าเฮดเดอร์ของ IPv6 มีขนาดคงที่ 40 ออกเตต ต่างกับเฮดเดอร์ของ IPv4 ที่มีขนาดไม่คงที่ นอกจากนี้เฮดเดอร์ของ IPv6 ยังดูเรียบง่ายกว่าเฮดเดอร์ของ IPv4 มาก การที่มีขนาดของเฮดเดอร์คงที่และมี

จำนวนฟิลด์น้อยกว่า (IPv6 มี 8 ฟิลด์ส่วน IPv4 มี 12 ฟิลด์) ทำให้ประสิทธิภาพโดยรวมของการประมวลผลแพ็กเกตดีขึ้น ทั้งนี้หากพิจารณาเฮดเดอร์ของ IPv6 เทียบกับของ IPv4 จะสามารถเปรียบเทียบความแตกต่างได้ดังนี้

<u>ฟิลด์ที่ถูกตัดออก</u>

- IHL: ถูกตัดออกไปเพราะเฮดเดอร์ของ IPv6 มีขนาดคงที่ 40 octets (bytes) ทำให้ประสิทธิภาพโดยรวมของการประมวลผลแพ็กเกตดีขึ้นเพราะไม่ต้องเสียเวลาในการคำนวณขนาดของ header ทำให้ไม่จำเป็นต้องใช้ฟิลด์ IHL อีกต่อไป
- Header Checksum: ถูกตัดออกเพราะว่าซ้ำซ้อนกับฟังก์ชันของโพรโทคอลในชั้นที่อยู่สูงกว่า นอกจากนี้การตัดฟิลด์ส่วนนี้ออกยังเป็นการเพิ่มประสิทธิภาพของการประมวลผลด้วย เพราะ checksum จะต้องมีการคำนวณใหม่ที่เราเตอร์เสมอ หากตัดออกก็จะลดภาระงานที่เราเตอร์ไปได้
- Identification, Flag, Segmentation, Protocol, Options, และ Padding: ถูกย้ายไปอยู่ในส่วนขยายของเฮดเดอร์ (extended header) เนื่องจากเป็นส่วนที่ไม่จำเป็นสำหรับเราเตอร์ทุก ๆ เราเตอร์ที่จะต้องใช้ในการประมวลผล
- TOS: เป็นฟิลด์กำหนดประเภทการให้บริการแต่ถูกตัดออกเพราะในทางปฏิบัติ การประยุกต์ใช้งานส่วนใหญ่ไม่ได้ใช้ฟิลด์นี้แต่อย่างใด

<u>ฟิลด์ที่ถูกปรับเปลี่ยน</u>

- Total Length: เปลี่ยนมาเป็น Payload Length ฟิลด์ Total Length เป็นฟิลด์ที่ใช้บอกความยาวของข้อมูลที่จะส่งรวมกับเฮดเดอร์ สำหรับ IPv6 ใช้ฟิลด์ Payload Length บอกเฉพาะขนาดข้อมูลเท่านั้น เนื่องจากเฮดเดอร์มีขนาดคงที่ 40 ไบต์
- Time-To-Live (TTL): เปลี่ยนมาเป็น Hop Limit เพราะ TTL ระบุเวลาที่ packet จะวนเวียนอยู่ในอินเตอร์เน็ต (หน่วยเป็นวินาที) โดยระบุว่าเราเตอร์แต่ละเราเตอร์ต้องลด TTL ลงอย่างน้อย 1 วินาที เราเตอร์จึงลด TTL ครั้งละ 1 หน่วยเสมอแม้ว่าจะใช้เวลาประมวลผลแพ็กเกตน้อยกว่านั้นทำให้ไม่ตรงกับความหมายของ TTL ดังนั้นจึงเปลี่ยนชื่อฟิลด์ให้สื่อความหมายคือ Hop Limit ให้ตรงกับความหมายจริง ๆ ซึ่งเหมาะสมและง่ายต่อการประมวลผลมากกว่า
- Protocol: เปลี่ยนมาเป็น Next Header ซึ่งใช้เป็นตัวบอกว่าส่วนที่อยู่ถัดจากเฮดเดอร์เป็นข้อมูลหรือส่วนขยายของเฮดเดอร์ (extended header) ประเภทใด

<u>ฟิลด์ที่เพิ่มขึ้นใหม่</u>

- Traffic class (Priority): ใช้ระบุว่าแพ็กเกตนี้อยู่ในกลุ่มใดและมีลำดับความสำคัญมากน้อยเพียงใด เพื่อที่เราเตอร์จะได้จัดลำดับขั้นการส่งแพ็กเกตให้เหมาะสม ออกแบบมาเพื่อสนับสนุนการทำงานแบบเวลาจริง โดยการกำหนดตามลำดับความสำคัญ งานที่เป็นประเภท real time จะมีความสำคัญมากกว่างานปกติ และยังช่วยแก้ปัญหาเกี่ยวกับ traffic ของ network ได้ ฟังก์ชัน traffic control ถ้า

แพ็กเกตใดกำหนดให้ใช้ traffic control เมื่อมี traffic เกิดขึ้น โดยใช้ฟังก์ชันนี้จะเข้าสู่ภาวะลดความเร็วของการส่งข้อมูลลงเพื่อลดความคับคั่งของโครงข่าย และเมื่อโครงข่ายเป็นปกติแล้ว ฟังก์ชันนี้ก็จะเพิ่มความเร็วในการส่งข้อมูลให้เท่าเดิม

- Flow Label: ใช้ระบุลักษณะการไหลเวียนของทราฟฟิกระหว่างต้นทางกับปลายทาง ทำให้สามารถประยุกต์ใช้งาน IPv6 เข้ากับทราฟฟิกหลายลักษณะ เช่น สามารถแยกการไหลของข้อมูลภาพและข้อมูลเสียงออกจากกันได้

1.7 การกำหนดเลขที่อยู่ไอพีของ IPv6

IPv6 มีขนาดเลขที่อยู่ไอพีขนาด 128 บิต มีการออกแบบเลขที่อยู่ไอพีแบบลำดับชั้น (Hierarchy) ทำให้การจัดเส้นทางมีประสิทธิภาพมากขึ้น นอกจากนี้ยังยกเลิกการจัดเลขที่อยู่ไอพีแบบ IPv4 ที่แบ่งออกเป็นคลาส (Class A-E) โดย IPv6 มีการจัดเลขที่อยู่ไอพีออกเป็น 3 กลุ่มดังต่อไปนี้

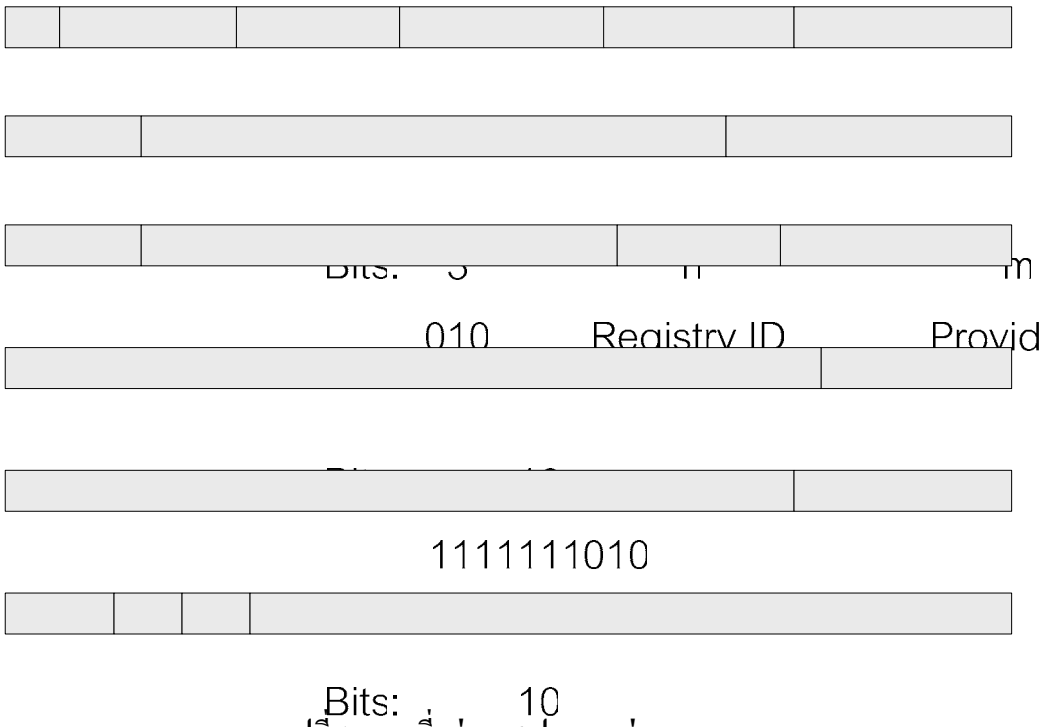
1. เลขที่อยู่ไอพีแบบ Unicast: เป็นเลขที่อยู่ไอพีที่กำหนดให้กับการต่อร่วม (interface), เลขที่อยู่ไอพีหนึ่งหมายเลขต่อการต่อร่วม แพ็กเกตที่มีเลขที่อยู่ไอพีปลายทางของการต่อร่วมหนึ่งจะถูกส่งไปยังการต่อร่วมนั้นเท่านั้น

2. เลขที่อยู่ไอพีแบบ Anycast: เป็นเลขที่อยู่ไอพีที่กำหนดให้กับกลุ่มของการต่อร่วม แพ็กเกตที่มีเลขที่อยู่ไอพีปลายทางแบบ Anycast หนึ่งหมายเลข จะถูกนำส่งไปยังการต่อร่วมหนึ่งการต่อร่วมที่มีเลขที่อยู่ไอพีแบบ Anycast นั้น ซึ่งโดยทั่วไปแพ็กเกตจะถูกนำส่งไปยังการต่อร่วมที่อยู่ใกล้ที่สุดตามการวัดจากโพรโทคอลจัดเส้นทาง

3. เลขที่อยู่ไอพีแบบ Multicast: เป็นเลขที่อยู่ไอพีที่กำหนดให้กับกลุ่มของการต่อร่วมคล้ายกับเลขที่อยู่ไอพีแบบ Anycast แต่แพ็กเกตที่มีเลขที่อยู่ไอพีปลายทางแบบ Multicast หนึ่งหมายเลข จะถูกนำส่งไปยังการต่อร่วมทุกการต่อร่วมที่มีเลขที่อยู่ไอพีแบบ Multicast นั้น

หมายเหตุ: IPv6 ไม่มีเลขที่อยู่ไอพีแบบ Broadcast แต่จะใช้เลขที่อยู่ไอพีแบบ Multicast แทน

IPv6 สามารถจัดสรรเลขที่อยู่ไอพีให้กับการต่อร่วมทุกการการต่อร่วมของอุปกรณ์ทุกอุปกรณ์ในโครงข่าย ไม่ว่าจะเป็น Host หรือ Router และการที่เลขที่อยู่ไอพีมีขนาดยาวขึ้นทำให้สามารถออกแบบเลขที่อยู่ไอพีแบบลำดับชั้นได้ โดยการกำหนดเลขที่อยู่ไอพีดูได้จากเอกสาร RFC 2373 “IP Version 6 Addressing Architecture” การทำเช่นนี้ทำให้เกิดความยืดหยุ่นในการออกแบบ และการจัดเส้นทางที่รวดเร็วและมีประสิทธิภาพมากขึ้น เนื่องจาก Routing table ของ Router มีขนาดเล็กลง ฟิลด์แรกสุดของเลขที่อยู่ไอพีคือ Format-prefix ที่มีความยาวไม่คงที่ ทำหน้าที่แบ่งเลขที่อยู่ไอพีออกเป็นประเภทต่าง ๆ ตามลักษณะการใช้งาน ดังรูปที่ 1.8



รูปที่ 1.8 เลขที่อยู่ IPv6 ประเภทต่าง ๆ

1.8 จุดเด่นอื่น ๆ ของ IPv6

นอกเหนือจากการขยายขนาดของเลขที่อยู่ไอพีแล้ว IPv6 ยังได้รับการออกแบบมาให้เหมาะสมกับสภาพการใช้งานอินเตอร์เน็ตในปัจจุบัน ตอบสนองต่อการขยายตัวและความต้องการใช้งานเทคโนโลยีบนโครงข่ายอินเตอร์เน็ตในอนาคต ไม่ว่าจะเป็นเรื่องการสนับสนุนการทำงานแบบ real time โดยใช้ Flow Label หรือการเพิ่มส่วนขยายของเฮดเดอร์ (Extended Header) และยังมีจุดเด่นที่สำคัญอีกสองประการคือ การติดตั้งที่อยู่แบบอัตโนมัติ และระบบรักษาความปลอดภัย

- การติดตั้งที่อยู่แบบอัตโนมัติ (Address Autoconfiguration): IPv6 มีความสามารถในการติดตั้งที่อยู่แบบอัตโนมัติ โดยไม่ต้องใช้โพรโทคอลที่กำหนดเป็น Stateful เช่น Dynamic Host Configuration Protocol (DHCP) การติดตั้งแบบอัตโนมัติใน IPv6 คือการต่อเครื่องเข้าสู่โครงข่าย โดยเครื่องจะกำหนดเลขที่อยู่ไอพีและพารามิเตอร์ที่จำเป็นแบบอัตโนมัติ โดยที่ผู้ใช้ไม่จำเป็นต้องทำอะไร นอกจากนี้ยังอำนวยความสะดวกให้กับการจัดสรรปรับเปลี่ยนเลขที่อยู่ไอพี (Address Renumbering) การเชื่อมต่อกับผู้ให้บริการหลายราย (Multihoming) เป็นต้น
- การรักษาความปลอดภัยของข้อมูล: อุปกรณ์ในโครงข่าย IPv6 ทุกตัวถูกกำหนดให้รองรับการใช้งาน IPSec ซึ่งมีระบบรักษาความปลอดภัยอยู่สองรูปแบบคือ การพิสูจน์ตัวจริง (authentication) และ การ

เข้ารหัสลับ (encryption) เพื่อสนับสนุนการรับส่งข้อมูลอย่างปลอดภัย ภายใต้การทำงานในชั้น Network แทนการทำงานในชั้น Application เหมือนอย่างในโครงข่าย IPv4

บทที่ 2
ความจำเป็นและแนวโน้มที่จะนำ IPv6 มาใช้งานในประเทศไทย

อินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol version 6; IPv6) ถูกพัฒนาขึ้นโดยการปรับปรุงโครงสร้างของตัวโพรโตคอลจากอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (IPv4) ที่ใช้งานอยู่อย่างแพร่หลายในปัจจุบันให้มีจำนวน IP address มากขึ้น เพื่อให้รองรับการขยายตัวของโครงข่ายอินเตอร์เน็ตในอนาคตได้อย่างพอเพียง นอกจากนี้ยังมีการปรับปรุงคุณลักษณะอื่นๆ อีกหลายประการ ทั้งในแง่ของประสิทธิภาพและความปลอดภัย เพื่อให้สามารถตอบสนองความต้องการในการใช้งานเทคโนโลยีโครงข่ายอินเตอร์เน็ต จำนวน IPv6 address มีขนาด 128 บิต ซึ่งเพิ่มขึ้นจาก IPv4 address เดิม ที่มีขนาดเพียง 32 บิต ความแตกต่างของจำนวน IP Address มีมากถึง 2^{96} เท่า ซึ่งจำนวน IP Address ที่เพิ่มขึ้นอย่างมากมายมหาศาลนี้ น่าจะมากเพียงพอสำหรับความต้องการการใช้งานในอนาคต นอกจากนี้ IPv6 ยังมีความสามารถพิเศษอื่นๆ ที่ถูกบรรจุอยู่ ได้แก่

- ความสามารถในการตั้งค่าและปรับแต่งโครงข่ายที่ง่ายกว่าในปัจจุบัน ทำให้ง่ายต่อการใช้งาน
- การรองรับการสื่อสารแบบ multicast ซึ่งเป็นการสื่อสารที่มีประสิทธิภาพมากกว่าการสื่อสารแบบ broadcast
- มีการจัดการด้านความปลอดภัยในโครงข่ายที่ดีขึ้น
- มีการออกแบบมาเพื่อให้รับประกันคุณภาพของบริการตั้งแต่เริ่ม ตั้งแต่ส่วนของ header และยังลดสัดส่วนของข้อมูล header ต่อข้อมูลทั้งหมด เพื่อเพิ่มประสิทธิภาพการส่งข้อมูลในระบบ

ในปัจจุบันหลายประเทศ ได้เริ่มนำอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 มาใช้งานจริง ในแถบประเทศในทวีปเอเชียนั้นประเทศที่ได้นำ IPv6 มาพัฒนาและใช้งานอย่างมากคือ ญี่ปุ่น เกาหลี และจีน เนื่องจากได้รับความร่วมมือที่ดีจากทั้งภาครัฐและเอกชน ในขณะที่ประเทศไทยยังมีความตื่นตัวกันค่อนข้างน้อยกับวิกฤตการณ์ การขาดแคลน IP Address ดังกล่าวที่กำลังจะเกิดขึ้นในอนาคต อาจจะเนื่องมาจากความไม่รู้หรือความคิดที่ว่าจำนวนหมายเลขที่ใช้อยู่ก็เพียงพอ ซึ่งจะส่งผลกระทบโดยตรงต่ออัตราการขยายตัวของโครงข่ายในประเทศในอนาคต และการเชื่อมต่อกับโครงข่ายภายนอกเป็นอย่างมาก

ปัจจุบันในประเทศไทยมีหน่วยงานภาครัฐและผู้ให้บริการอินเตอร์เน็ตหลายแห่งได้รับจัดสรรชุดหมายเลข IPv6 address จาก 6Bone และ APNIC และได้นำชุดหมายเลขเหล่านั้น มาจัดสรรต่อให้กับหน่วยงานอื่นที่ต้องการทดลองใช้และทดสอบการเชื่อมต่อบนโครงข่าย IPv6 อีกทั้งยังได้มีการก่อตั้งคณะทำงานระดับประเทศขึ้นภายใต้ชื่อ Thailand IPv6 Forum ซึ่งมี Logo แสดงได้ดังรูปที่ 2.1 หรือโครงการความร่วมมือพัฒนาและส่งเสริมการใช้โครงข่าย IPv6 ซึ่งเป็นความร่วมมือระหว่างหน่วยงานวิจัย ผู้ให้บริการอินเตอร์เน็ต

และผู้ผลิตหรือตัวแทนจำหน่ายฮาร์ดแวร์และซอฟต์แวร์ระบบโครงข่าย ซึ่งนับเป็นความตื่นตัวในขั้นแรกของประเทศไทยในการรองรับเทคโนโลยี IPv6 ที่จะมาถึงในอนาคตอันใกล้

รูปที่ 2.1 โลโก้ของ Thailand IPv6 Forum

องค์กรทั้งภาครัฐและเอกชนในประเทศไทยจำเป็นต้องร่วมกันเตรียมความพร้อมทั้งในด้านของบุคลากร และโครงสร้างหลักต่างๆ เพื่อรองรับการใช้งานโครงข่าย IPv6 ภายในประเทศ และการติดต่อกับโครงข่าย IPv6 ต่างประเทศ เพราะประเทศที่ให้ความสำคัญกับการปรับเปลี่ยนสู่ IPv6 ย่อมจะได้เปรียบและมีโอกาสที่จะนำ IPv6 มาพัฒนาโครงสร้างพื้นฐานของประเทศ เพื่อให้สามารถตอบสนองความต้องการในการใช้งานเทคโนโลยีบนโครงข่ายอินเตอร์เน็ตที่เพิ่มขึ้นอย่างรวดเร็ว

ในส่วนต่อไปจะสรุปและขยายความของเหตุผลความจำเป็นและแนวโน้มที่จะนำ IPv6 มาใช้งานในประเทศไทย

2.1 เหตุผลความจำเป็นและแนวโน้มในการนำ IPv6 มาใช้งานในประเทศไทย

1. หมายเลข IPv4 กำลังจะหมดไป

อินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol version 4 : IPv4) เป็นมาตรฐานในการสื่อสารบนโครงข่ายอินเตอร์เน็ตตั้งแต่ปี ค.ศ. 1981 แต่ในช่วงทีผ่านมาการขยายตัวของโครงข่ายอินเตอร์เน็ตมีอัตราการเติบโตอย่างรวดเร็ว นักวิจัยเริ่มพบว่า จำนวนหมายเลข IP Address ของ IPv4 กำลังจะถูกใช้หมดไป ไม่เพียงพอกับการใช้งานอินเตอร์เน็ตในอนาคต และมีการคาดคะเนว่าหมายเลข IPv4 address นั้น จะถูกจัดสรรหมดไปภายในปี พ.ศ. 2551 และหากเกิดขึ้นก็หมายความว่าเราจะไม่สามารถเชื่อมต่อโครงข่ายเข้ากับระบบอินเตอร์เน็ตเพิ่มขึ้นได้อีก

ตารางที่ 2.1 แสดงจำนวน IPv4 Address ซึ่งได้ถูกจัดสรรให้ประเทศทั่วโลกเรียงตามลำดับของปริมาณ IPv4 จากตารางที่ 1 แสดงให้เห็นว่าประเทศไทยได้รับการจัดสรรหมายเลข IPv4 เพียง 1,782,016 หมายเลข ซึ่ง

นับเป็นลำดับที่ 37 ของประเทศที่มีการใช้งานอินเตอร์เน็ต จากการที่ภาครัฐของประเทศไทยต้องการแพร่กระจายเทคโนโลยี IT รวมทั้งการสื่อสารผ่านโครงข่าย Internet สู่ทุกภาคส่วนและพื้นที่ พร้อมทั้งความสนใจของผู้คนส่วนใหญ่ที่จะสมัครเข้ารับบริการสื่อสารข้อมูล Internet ก็มีแนวโน้มเพิ่มขึ้นอย่างมาก บริการสื่อสารข้อมูลในอนาคตอันใกล้ ไม่ว่าจะเป็นโทรศัพท์ผ่านโครงข่าย Internet หรือ Voice over IP (VoIP), Mobile IP, และ IPTV นั้นล้วนแล้วแต่ต้องการใช้จำนวน IP address ปริมาณมากทั้งสิ้น ดังนั้นเป็นที่ชัดเจนว่าในอนาคตอันใกล้ ความต้องการใช้ IP address เพิ่มมากขึ้นจากการขยายตัวของบริการและการพัฒนาทางด้านต่างๆดังกล่าว และจำนวนหมายเลขที่มีอยู่ก็จะไม่เพียงพออย่างชัดเจน

ตารางที่ 2.1 จำนวน IPv4 Address ซึ่งได้ถูกจัดสรรให้ประเทศทั่วโลกเรียงตามลำดับ

ลำดับ	รหัสประเทศ	ชื่อประเทศ	IPv4 Address assigned	Share
1	US	สหรัฐอเมริกา	1,246,274,560	66.90%
2	JP	ญี่ปุ่น	103,830,16	5.57%
3	CA	แคนาดา	62,013,952	3.33%
4	GB	เกรทบริเทน	50,894,080	2.73%
5	DE	เยอรมัน	48,699,648	2.61%
6	FR	ฝรั่งเศส	37,210,112	2.00%
7	CN	จีน	30,719,744	1.65%
8	NL	เนเธอร์แลนด์	28,527,872	1.53%
9	KR	เกาหลี	26,208,768	1.41%
10	UK	อังกฤษ	26,112,000	1.40%
37	TH	ไทยแลนด์	1,782,016	0.10%

2. การเพิ่มความสามารถในการแจกจ่ายหมายเลข IP จริง ให้กับผู้ใช้

การใช้งานอินเตอร์เน็ตในอนาคตอันใกล้จะแปรเปลี่ยนเป็นแบบ Always-on คือพร้อมใช้และพร้อมบริการอยู่ตลอดเวลา ซึ่งการ Always-on นั้นต้องการ IP Address ที่สามารถอ้างอิงถึงได้อยู่ตลอดเวลา นอกจากนี้อุปกรณ์อีกหลายประเภท ไม่ใช่เฉพาะคอมพิวเตอร์ก็จะเชื่อมโยงเข้าสู่อินเตอร์เน็ตได้ ทั้งนี้ผู้ใช้จะเรียกร้อง IP Address จริง (Public IP Address) ที่อ้างอิงถึงได้จากทั่วโลกเสมือนบ้านเลขที่อยู่หรือหมายเลขหนังสือเดินทางซึ่งเฉพาะเจาะจงของแต่ละบุคคลเพื่อการติดต่อในลักษณะ peer-to-peer และเพื่อความเชื่อมั่น

ในความปลอดภัย ซึ่งไม่สามารถทำได้ในระบบปัจจุบันภายใต้ IPv4 ที่อาศัย Network Address Translation (NAT) เพื่อแปลง IP Address ระหว่าง Private IP Address กับ IP Address จริง นอกจากนี้การใช้ IP Address จริง ยังมีประโยชน์ต่อบริการที่ต้องอ้างอิงการใช้งานโดยตรงถึงผู้ใช้ เช่น ระบบโทรศัพท์ VoIP ระบบโทรศัพท์เคลื่อนที่ผ่านโครงข่ายอินเตอร์เน็ต Mobile IP ระบบการคิดค่าเช่า โครงข่าย หรือค่าบริการ VoIPVideo-on-Demand (VoD) เล่นเกมส์ต่างๆ รวมถึงระบบตรวจจับควบคุม Radio frequency identification (RFID) อีกด้วย

3. ความต้องการบริการหรือแอปพลิเคชั่นใหม่ที่ต้องใช้หมายเลข IPv6

ในอนาคตอันใกล้จะเกิดบริการหรือแอปพลิเคชั่นใหม่ที่หลากหลายและมากมาย ซึ่งต้องใช้หมายเลข IPv6 ในการอ้างอิงถึง ตัวอย่างเช่น

3.1 การขยายตัวของบริการโทรศัพท์เคลื่อนที่ Mobile IP และ Mobile Internet โทรศัพท์เคลื่อนที่ในปัจจุบันทำหน้าที่แลกเปลี่ยนข้อมูลได้หลายรูปแบบ ไม่เพียงแต่ข้อมูลเสียงพูดเท่านั้น ข้อมูลที่เป็นข้อความ รูปภาพ วีดิโอ ก็สามารถทำได้ด้วย ซึ่งการแลกเปลี่ยนข้อมูลเหล่านี้อาจเกิดขึ้นในรูปแบบของการรับ-ส่งอีเมล์ peer-to-peer หรือเปิดเว็บไซต์ ซึ่งต้องอาศัยเทคโนโลยี IP เข้ามาช่วย นั่นก็หมายความว่า โทรศัพท์เคลื่อนที่ในปัจจุบันมีความต้องการใช้ IP Address หากต้องการจ่าย IP address ให้กับโทรศัพท์เคลื่อนที่ในประเทศ ซึ่งปัจจุบันมีใช้งานอยู่ประมาณ 25 ล้านเครื่อง และมีแนวโน้มในการใช้ที่สูงขึ้นเรื่อยๆ หมายเลข IPv4 ย่อมไม่พอต่อความต้องการ และหากมีการจัดสรร IP Address ให้กับอุปกรณ์สื่อสารเคลื่อนที่ จะทำให้ปัญหาการขาดแคลนหมายเลข IP เกิดเร็วขึ้นอีก

3.2 เทคโนโลยีการรับ-ส่งสัญญาณเสียงบนระบบโครงข่าย Internet หรือ VoIP เพื่อความสะดวกและประหยัดค่าใช้จ่าย ซึ่งเทคโนโลยีนี้กำลังเป็นที่สนใจ เพื่อรองรับการใช้บริการที่เพียงพอจำเป็นต้องใช้ IP address เป็นจำนวนมาก จำนวน IPv4 address ที่มีอยู่ไม่น่าจะเพียงพอกับการรองรับการเจริญเติบโตของเทคโนโลยีนี้ในอนาคต

3.3 การพัฒนาแอปพลิเคชันแบบ peer-to-peer ที่ต้องการ IP address จริง เป็นจำนวนมาก เช่น การทำ File sharing, Instant messaging, และ Online gaming แอปพลิเคชันเหล่านี้มีข้อจำกัดภายใต้ IPv4 address เนื่องจากผู้ใช้บางส่วนที่ได้รับจัดสรร IP address ผ่าน NAT ไม่มี IP address จริงเนื่องจากจำนวน IP address มีไม่เพียง จึงไม่สามารถใช้แอปพลิเคชันเหล่านี้ได้

4. การรองรับการขยายตัวของบริการ Broadband Internet

โครงข่าย IPv6 จะช่วยรองรับการขยายตัวของบริการ Broadband Internet ได้เป็นอย่างดี เนื่องจากบริการ Broadband Internet มักจะหมายถึงการใช้งานอินเตอร์เน็ตในลักษณะ Always-on connection จึงมีความต้องการหมายเลข IP Address จำนวนมาก ตามนโยบายของกระทรวง ICT ที่ต้องการขยายการให้บริการ

Broadband Internet ภายในประเทศ อีกไม่น้อยกว่า 1,000,000 พอร์ท ทำให้ความต้องการหมายเลข IP ใหม่เพิ่มขึ้นอีกประมาณ 6,000,000 หมายเลข ซึ่งประเทศไทยไม่สามารถจัดสรรจำนวน IP Address ดังกล่าวได้จากโพรโตคอล IPv4 เพียง 1,782,016 หมายเลข ซึ่งนับเป็นลำดับที่ 37 ของประเทศที่มีการใช้งานอินเตอร์เน็ต

5. เครื่องใช้ไฟฟ้าภายในบ้านและอุปกรณ์อำนวยความสะดวกจำเป็นต้องมี IP ในอนาคต การจัดสรร IP Address ให้กับเครื่องใช้ไฟฟ้าชนิดต่างๆมีจุดประสงค์เพื่อให้แยกแยะ ระบุถึง และควบคุมได้ และสามารถทำให้เกิดเป็นโครงข่ายภายในบ้านหรือระหว่างบ้านได้ เช่น โทรทัศน์ในอนาคตจะสามารถโต้ตอบกับผู้ชมได้ สามารถสั่งเปิด ปิด ควบคุม หรือตรวจสอบสถานะของเครื่องใช้ไฟฟ้าในบ้านได้ นอกจากนี้เรายังสามารถใช้ IPv6 ร่วมกับเทคโนโลยี RFID (Radio Frequency Identification) เพื่อใช้ในระบบตรวจสอบทุกชนิดได้ ตัวอย่างเช่นในการตรวจสภาพแวดล้อม การวางอุปกรณ์ RFID ซึ่งมี IP Address ประจำตัวไว้ในภูมิภาคต่างๆ หรือติดไว้กับสัตว์หรือรถแท็กซี่สามารถส่งข้อมูลมาเพื่อตรวจสอบสภาพมลพิษในเมืองและระบุสถานที่ได้เป็นต้น

6. IPv6 มีความสามารถพิเศษที่เหนือกว่า IPv4

IPv6 มีมีความสามารถพิเศษต่างๆที่เหนือกว่า IPv4 อย่างชัดเจนซึ่งการนำ IPv6 มาใช้นั้นจะสามารถเพิ่มประสิทธิภาพของการสื่อสารภายในและนอกประเทศไทยได้ เช่น

- Management : IPv6 ถูกออกแบบมาให้สนับสนุนการติดตั้งและปรับแต่งระบบแบบอัตโนมัติ (auto configuration) เพื่ออำนวยความสะดวกให้กับการจัดสรรปรับเปลี่ยน IP Address (Address Renumbering) การเชื่อมต่อกับผู้ให้บริการหลายราย (Multihoming) และแม้แต่การจัดการโครงข่ายแบบ Plug-and-play

- Multicast/Anycast ใน IPv4 ได้มีการจัดสรร IP Address ส่วนหนึ่งเพื่อเป็น Broadcast Address แต่การสื่อสารแบบ Broadcast เป็นสิ่งที่ไม่มีความจำเป็นและสิ้นเปลือง Bandwidth โดยเปล่าประโยชน์ Multicast เป็นการสื่อสารที่มีประสิทธิภาพมากกว่าและเริ่มเป็นที่นิยม IPv6 จึงถูกออกแบบมาให้รองรับ Multicast group address และตัด Broadcast address ออก นอกจากนี้ IPv6 ยังเพิ่มความสามารถในการสื่อสารแบบ Anycast โดยอนุญาตให้อุปกรณ์มากกว่า 1 ชิ้น ได้รับการจัดสรร IP Address หมายเลขเดียวกัน ซึ่งหมายความว่าอุปกรณ์ชิ้นใดก็ได้สามารถตอบสนองต่อข้อมูลที่ส่งมาที่ Anycast address นั้นๆ

- Security เราเตอร์และอุปกรณ์โครงข่ายทุกตัวในโครงข่าย IPv6 ถูกกำหนดให้รองรับการใช้งาน IPSec นอกจากนี้ยังมีการกำหนด Security Payload สองประเภทคือ Authentication Payload และ Encrypted Security Payload เพื่อสนับสนุนการรับส่งข้อมูลที่มั่นคงปลอดภัย ภายใต้ Network Layer แทนที่จะพึ่ง Application Layer เหมือนในโครงข่าย IPv4 โครงข่าย IPv6 ทำให้ระบบโครงข่ายมีความปลอดภัยมากขึ้น โดยเฉพาะการติดต่อแบบ end-to-end อย่างแท้จริง สามารถทำให้ end-user สามารถ identify ระบบความปลอดภัยได้ด้วยตนเอง การตรวจสอบสามารถทำได้ง่ายเพราะไม่ผ่าน NAT (Network Address Translation)

การใช้งานแบบ IPv6 VPN จะทำให้มีความปลอดภัยและเสถียรขึ้นเนื่องจากไม่ผ่าน NAT ทำให้ผู้ให้บริการและผู้ใช้บริการมีความมั่นใจสูงขึ้น

7. เพิ่มคุณภาพชีวิตประชากรไทย

จากการพัฒนาบริการทางอิเล็กทรอนิกส์ (E-Services) เพื่อเพิ่มคุณภาพชีวิตของประชากรไทย และการพัฒนาประเทศไทยนั้น จำเป็นต้องอาศัยบริการพื้นฐาน อันได้แก่

- E-Health คือ บริการด้านสุขภาพทางอินเตอร์เนต สถานพยาบาลต่างๆ สามารถให้ความรู้ให้คำปรึกษา ตรวจและวิเคราะห์โรค แม้กระทั่งดำเนินการรักษาและผ่าตัดทางไกลผ่านโครงข่ายอินเตอร์เนตได้

- E-Government คือ บริการด้านราชการการปกครองผ่านโครงข่ายอินเตอร์เนต เช่น การขอเอกสารใบรับรอง การยื่นคำร้องติดต่อราชการกับกระทรวง ทบวง กรม โดยไม่จำเป็นต้องเดินทางไปยังต้นสังกัดที่ต้องการยื่นคำร้อง แต่ทั้งนี้ต้องอาศัยเทคโนโลยีการระบุตัวบุคคลควบคู่ไปด้วย ประชาชนที่ต้องการเข้าใช้บริการจะต้องสามารถเข้าใช้บริการจากที่ใดก็ได้ผ่านโครงข่ายอินเตอร์เนต

- E-Education คือ บริการเกี่ยวกับการศึกษาเรียนรู้ทางอินเตอร์เนต สามารถใช้ได้ในสถาบันการศึกษาและตามสถานที่ส่วนบุคคลของผู้ใช้บริการรายย่อย เพื่อให้ผู้ต้องการเรียนรู้สามารถติดต่อสถาบันที่ให้ความรู้หรือผู้สอนได้โดยไม่ต้องไปยังสถาบันนั้น

- E-Commerce คือ บริการทางการซื้อขาย ทำธุรกิจ และธุรกรรมทางการเงินผ่านโครงข่ายอินเตอร์เนต โดยไม่ต้องเข้าไปยังธนาคารหรือจุดซื้อขาย

บริการเหล่านี้จำเป็นต้องใช้ IP address เป็นจำนวนมากเพื่อให้เข้าถึงและรองรับการใช้บริการจากประชาชนได้

8. การเพิ่มขีดความสามารถในการแข่งขันของประเทศไทย

โครงข่าย IPv6 จะเป็นโครงข่ายหลักที่สำคัญสำหรับการให้บริการแบบบรอดแบนด์ของบริษัทโทรคมนาคมและผู้ให้บริการอินเตอร์เน็ตในประเทศไทยและการพัฒนาด้านอุตสาหกรรม IT ของประเทศ องค์กรต่างๆ ของไทยทั้งระบบรัฐวิสาหกิจและธุรกิจขนาดกลางและขนาดเล็ก (SMEs ต้องพร้อมที่จะรับการแข่งขันในเทคโนโลยีใหม่นี้ เพื่อไม่เสียเปรียบในการแข่งขันกับบริษัทต่างชาติ โดยเฉพาะอย่างยิ่งหลังจากรัฐบาลเปิดเสรีภาพทางด้านการให้บริการโทรคมนาคม

9. การลดความยุ่งยากและซับซ้อนในการเชื่อมต่อกับโครงข่ายต่างประเทศ

หลายประเทศทั่วโลกได้ออกนโยบายเกี่ยวกับการปรับเปลี่ยนระบบโครงข่ายภายในประเทศเพื่อรองรับการใช้งาน IPv6 ตัวอย่างเช่น กระทรวงกลาโหมของสหรัฐอเมริกาได้กำหนดไว้ว่าภายในสิ้นปี พ.ศ. 2551 โครงข่ายคอมพิวเตอร์ทั้งหมดต้องสามารถใช้งาน IPv6 ได้ ประเทศไต้หวันมีนโยบายว่าโครงข่ายภายในประเทศต้องสนับสนุนการใช้งานทั้ง IPv4 และ IPv6 ภายในปี พ.ศ. 2551 และประเทศสาธารณเกาหลีเริ่มให้บริการ IPv6 เชิงพาณิชย์แล้ว ตั้งแต่ปี พ.ศ. 2548 และกำหนดนโยบายที่ปรับโครงข่ายทั้งประเทศให้เป็น Native IPv6 ภายในปี พ.ศ. 2554 ประเทศญี่ปุ่น มี ISP กว่า 50 รายสามารถให้บริการ IPv6 ส่วน ISP รายใหม่ทั้งหมดสามารถให้บริการ IPv6 ได้ตั้งแต่ต้น โครงข่ายงานวิจัย เช่น Internet 2 ทำงานอยู่บนโครงข่าย IPv6 ดังนั้น การเตรียมความพร้อมด้าน IPv6 ของประเทศไทยจะช่วยลดความยุ่งยากและซับซ้อนในการเชื่อมต่อกับโครงข่ายต่างประเทศในอนาคต

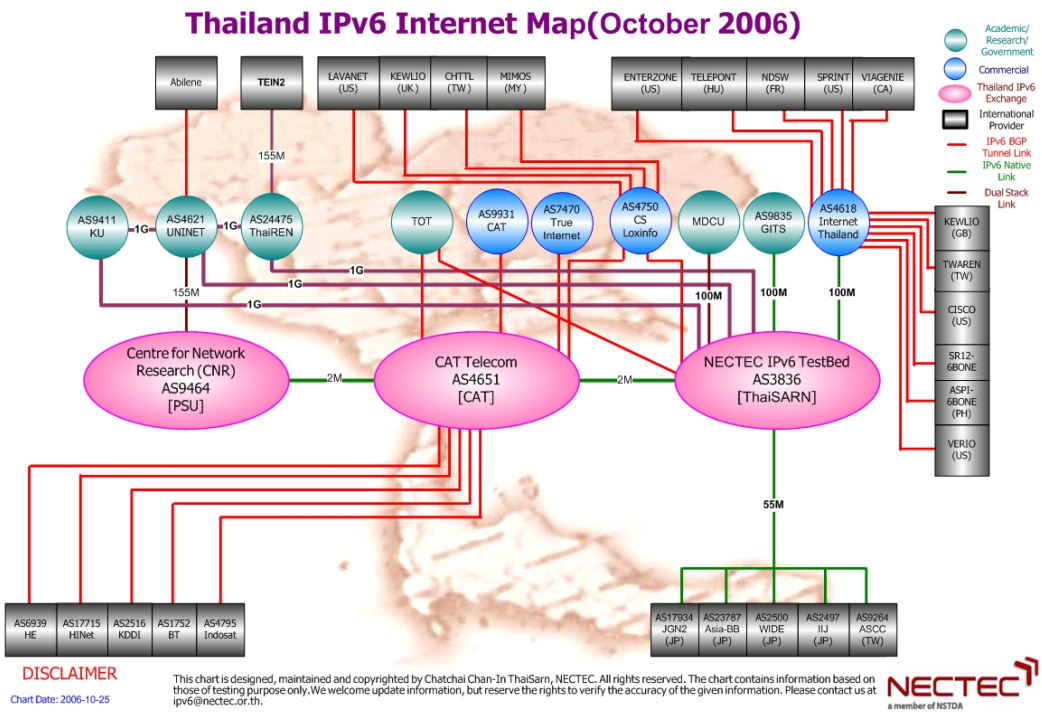
10. การส่งเสริมศักยภาพในการพัฒนาโปรแกรมซอฟแวร์เพื่อส่งออกของประเทศไทย และรองรับการใช้งานรูปแบบใหม่

หากประเทศไทยไม่มีโครงข่าย IPv6 เราจะไม่สามารถพัฒนาซอฟต์แวร์เพื่อให้ทำงานบนโครงข่ายดังกล่าวได้ ทำให้ขีดความสามารถในการส่งออกซอฟต์แวร์ลดลง เนื่องจากมีการบริการรี้ปแบบใหม่หลากหลายบนโครงข่าย IPv6 โดยเฉพาะทางด้าน Mobile Devices (เช่น โทรศัพท์มือคือ คอมพิวเตอร์มือถือ) Game on-line รุ่นใหม่จะใช้ความสามารถของโครงข่าย IPv65 การเชื่อมต่อกับอุปกรณ์ต่างๆ เช่น บริษัท Sony ประเทศญี่ปุ่น กำหนดไว้ว่าอุปกรณ์อิเล็กทรอนิกส์ของบริษัท จะสามารถเชื่อมต่อกับ IPv6 ได้อัตโนมัติ ภายในปี พ.ศ. 2549 เป็นต้น

11. การสร้างโครงสร้างพื้นฐานของประเทศไทยในการวิจัยพัฒนาและการศึกษา

โครงข่าย IPv6 จะเป็นโครงสร้างพื้นฐานที่สำคัญของประทศไทยในการวิจัยพัฒนาและการศึกษา เนื่องจากคุณลักษณะเด่นหลายประการ อาทิเช่น จำนวน IP Address ที่เพิ่มขึ้น การสนับสนุนคุณภาพการให้บริการ (Quality of Service) และความปลอดภัยของข้อมูล (Network Security) ตัวอย่างงานวิจัยซึ่งจะได้รับประโยชน์โดยตรง จากการใช้งานโครงข่าย IPv6 ได้แก่ งานวิจัย Grid Computing ซึ่งจะทำงานได้ดียิ่งขึ้นบนโครงข่าย IPv6 และงานวิจัยทางด้านมัลติมีเดีย เช่น Voice-over-IP, video conference, และ interactive distance learning

ตัวอย่างหน่วยงาน องค์กร และผู้ให้บริการอินเตอร์เน็ตที่เริ่มให้บริการเกี่ยวกับ IPv6 ในประเทศไทย



รูปที่ 2.2 แผนผังแสดงการเชื่อมต่อกับโครงข่าย IPv6 ภายในและนอกประเทศ

ในประเทศไทย ปัจจุบันมีหน่วยงานองค์กรและผู้ให้บริการอินเตอร์เน็ตที่ทำการเชื่อมต่อกับโครงข่าย IPv6 ทั้งภายในประเทศและต่างประเทศ ดังแสดงในรูปที่ 2.2 การเชื่อมต่อไปยังโครงข่าย IPv6 ต่างประเทศและภายในประเทศ มีทั้งการเชื่อมต่อแบบ Tunnel แบบ Dual stacks และแบบ Native IPv6

หน่วยงาน องค์กร และผู้ให้บริการอินเตอร์เน็ตที่เริ่มให้บริการเกี่ยวกับ IPv6 มีดังต่อไปนี้

1. ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

- บริการการเชื่อมต่อโครงข่าย IPv6 ด้วย Tunnel ทั้งแบบ BGP routing และ Static routing สู่โครงข่าย IPv6 ภายในประเทศ และต่างประเทศ (6Bone)

- บริการ IPv6 Tunnel Broker เพื่อแจกจ่ายหมายเลข IPv6 ให้กับผู้ใช้งาน IPv6 ในประเทศไทย โดยไม่คิดมูลค่าในการใช้งาน ดังนั้นผู้มีสิทธิขอหมายเลข IPv6 จึงควรเป็นหน่วยงานภาครัฐ หรือเอกชน ที่มีวัตถุประสงค์เพื่อนำไปทำการทดลองใช้ วิจัย การศึกษา โดยห้ามนำไปเปิดบริการแบบคิดมูลค่า แต่สามารถใช้เพื่อเตรียมความพร้อมขององค์กรสำหรับการพัฒนาธุรกิจในอนาคต

- บริการ 6to4 Relay เพื่อช่วยให้โครงข่ายที่ใช้งานหมายเลข IP Address แบบ 6to4 สามารถทำการสื่อสารกับโหนดบนโครงข่ายอื่นที่ใช้หมายเลขแอดเดรสแบบ Native IPv6 ได้

- บริการจัดสรร IPv6 Address สำหรับทดสอบ

- บริการ DNS และ Reverse DNS delegation:

  ns1.ipv6.nectec.or.the

  ns2.ipv6.nectec.or.th

- บริการ IPv6 เว็บไซต์ โดยมีชื่อว่า http://www.ipv6.nectec.or.th/
- บริการ 6to4 prefix calculator ผ่านเว็บไซต์

  http://www.ipv6.nectec.or.th/

- บริการ IPv6 address divider ผ่านเว็บไซต์

  http://www.ipv6.nectec.or.th/

2. บริษัท กสท โทรคมนาคม จำกัด (มหาชน)
   - บริการการเชื่อมต่อโครงข่าย IPv6 ด้วย Tunnel ทั้งแบบ BGP routing และ Static routing
   - บริการ IPv6 Mail Server: mail6. IPv6.cattelcom.com
   - บริการ IPv6 DNS:

     dns6.ipv6.cattelecom.com

     andaman.cattelecom.com

   - บริการ IPv6 เว็บไซต์ โดยมีชื่อว่า http://web.ipv6.cattelecom.com/
3. บริษัท อินเตอร์เน็ตประเทศไทย จำกัด (มหาชน)
   - บริการการเชื่อมต่อโครงข่าย IPv6 ด้วย Tunnel ทั้งแบบ BGP routing และ Static routing
   - บริการ IPv6 เว็บไซต์ โดยมีชื่อว่า http://web.ipv6.cattelecom.com/
4. บริษัท ซีเอส ล็อกซอินโฟ จำกัด (มหาชน)
   - บริการการเชื่อมต่อโครงข่าย IPv6 ด้วย Tunnel ทั้งแบบ BGP routing และ Static routing
   - บริการ IPv6 เว็บไซต์ โดยมีชื่อว่า http://web.ipv6.cattelecom.com/
5. บริษัท Asia Infonet จำกัด
   - บริการการเชื่อมต่อโครงข่าย IPv6 ด้วย 6to4 Tunnel
   - บริการ 6to4 Relay เพื่อช่วยให้โครงข่ายที่ใช้งานหมายเลข IP Address แบบ 6to4 สามารถทำการสื่อสารกับโหนดบนโครงข่ายอื่นที่ใช้หมายเลขแอดเดรสแบบ Native IPv6 ได้
   - บริการ IPv6 เว็บไซต์ โดยมีชื่อว่า http://web.ipv6.cattelecom.com/
6. มหาวิทยาลัยสงขลานครินทร์
   - บริการ IPv6 Mail Server
   - บริการ IPv6 FTP Server
   - บริการ IPv6 SIP Proxy Server
   - บริการ IPv6 เว็บไซต์ โดยมีชื่อว่า http://web.ipv6.cattelecom.com/

2.2 หน่วยงาน องค์กร และผู้ให้บริการอินเตอร์เน็ตที่เริ่มให้บริการเกี่ยวกับ IPv6 ในประเทศไทย

ในปัจจุบันมีหน่วยงาน องค์กร และผู้ให้บริการอินเตอร์เน็ตที่เริ่มให้บริการเกี่ยวกับ IPv6 ในประเทศไทยแล้วอยู่จำนวนหนึ่งซึ่งยังเป็นส่วนน้อยอยู่ ซึ่งพอที่จะรวบรวมหน่วยงานสำคัญๆได้ดังนี้

1. ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

- บริการการเชื่อมต่อโครงข่าย IPv6 ด้วย Tunnel ทั้งแบบ BGP routing และ Static routing สู่โครงข่าย IPv6 ภายในประเทศ และต่างประเทศ (6Bone)
- บริการ IPv6 Tunnel Broker เพื่อแจกจ่ายหมายเลข IPv6 ให้กับผู้ใช้งาน IPv6 ในประเทศไทยโดยไม่คิดมูลค่าในการใช้งาน ดังนั้นผู้มีสิทธิขอหมายเลข IPv6 จึงควรเป็นหน่วยงานภาครัฐ หรือเอกชน ที่มีวัตถุประสงค์เพื่อนำไปทำการทดลองใช้ วิจัย การศึกษา โดยห้ามนำไปเปิดบริการแบบคิดมูลค่า แต่สามารถใช้เพื่อเตรียมความพร้อมขององค์กรสำหรับการพัฒนาธุรกิจในอนาคต
- บริการ 6to4 Relay เพื่อช่วยให้โครงข่ายที่ใช้งานหมายเลข IP Address แบบ 6to4 สามารถทำการสื่อสารกับโหนดบนโครงข่ายอื่นที่ใช้หมายเลขแอดเดรสแบบ Native IPv6 ได้
- บริการจัดสรร IPv6 Address สำหรับทดสอบ
- บริการ DNS และ Reverse DNS delegation:

  ns1.ipv6.nectec.or.the

  ns2.ipv6.nectec.or.th
- บริการ IPv6 เว็บไซต์ โดยมีชื่อว่า http://www.ipv6.nectec.or.th/
- บริการ 6to4 prefix calculator ผ่านเว็บไซต์

  http://www.ipv6.nectec.or.th/
- บริการ IPv6 address divider ผ่านเว็บไซต์

  http://www.ipv6.nectec.or.th/

2. บริษัท กสท โทรคมนาคม จำกัด (มหาชน)

- บริการการเชื่อมต่อโครงข่าย IPv6 ด้วย Tunnel ทั้งแบบ BGP routing และ Static routing
- บริการ IPv6 Mail Server: mail6. IPv6.cattelcom.com
- บริการ IPv6 DNS:

  dns6.ipv6.cattelecom.com

  andaman.cattelecom.com
- บริการ IPv6 เว็บไซต์ โดยมีชื่อว่า http://web.ipv6.cattelecom.com/

3. บริษัท อินเตอร์เน็ตประเทศไทย จำกัด (มหาชน)

- บริการการเชื่อมต่อโครงข่าย IPv6 ด้วย Tunnel ทั้งแบบ BGP routing และ Static routing
- บริการ IPv6 เว็บไซต์ โดยมีชื่อว่า http://web.ipv6.cattelecom.com/

4. บริษัท ซีเอส ล็อกซอินโฟ จำกัด (มหาชน)

- บริการการเชื่อมต่อโครงข่าย IPv6 ด้วย Tunnel ทั้งแบบ BGP routing และ Static routing
- บริการ IPv6 เว็บไซต์ โดยมีชื่อว่า http://web.ipv6.cattelecom.com/

5. บริษัท Asia Infonet จำกัด

- บริการการเชื่อมต่อโครงข่าย IPv6 ด้วย 6to4 Tunnel
- บริการ 6to4 Relay เพื่อช่วยให้โครงข่ายที่ใช้งานหมายเลข IP Address แบบ 6to4 สามารถทำการสื่อสารกับโหนดบนโครงข่ายอื่นที่ใช้หมายเลขแอดเดรสแบบ Native IPv6 ได้
- บริการ IPv6 เว็บไซต์ โดยมีชื่อว่า http://web.ipv6.cattelecom.com/

6. มหาวิทยาลัยสงขลานครินทร์

- บริการ IPv6 Mail Server
- บริการ IPv6 FTP Server
- บริการ IPv6 SIP Proxy Server
- บริการ IPv6 เว็บไซต์ โดยมีชื่อว่า http://web.ipv6.cattelecom.com/

บทที่ 3
ตัวอย่างการใช้งาน IPv6 ในต่างประเทศ

ในต่างประเทศนั้นมีความตื่นตัวกับ IPv6 อย่างพอสมควรโดยเฉพาะประเทศซึ่งได้รับจัดสรร IPv4 แต่มีการใช้ IP address จำนวนมากจนคาดว่าในอนาคตอันใกล้นั้นจำนวน IPv4 ซึ่งได้รับการจัดสรรนั้นจะหมดไป จึงต้องมีการเตรียมการเปลี่ยนไปสู่ IPv6 ประเทศดังกล่าวนี้ส่วนใหญ่อยู่ในแถบเอเชีย และยุโรป เช่น ประเทศญี่ปุ่น เกาหลีใต้ และ จีน ส่วนประเทศในแถบอเมริกาเหนือนั้น ได้รับการจัดสรร IPv4 อย่างพอเพียงดังได้แสดงตามตารางที่ 2.1

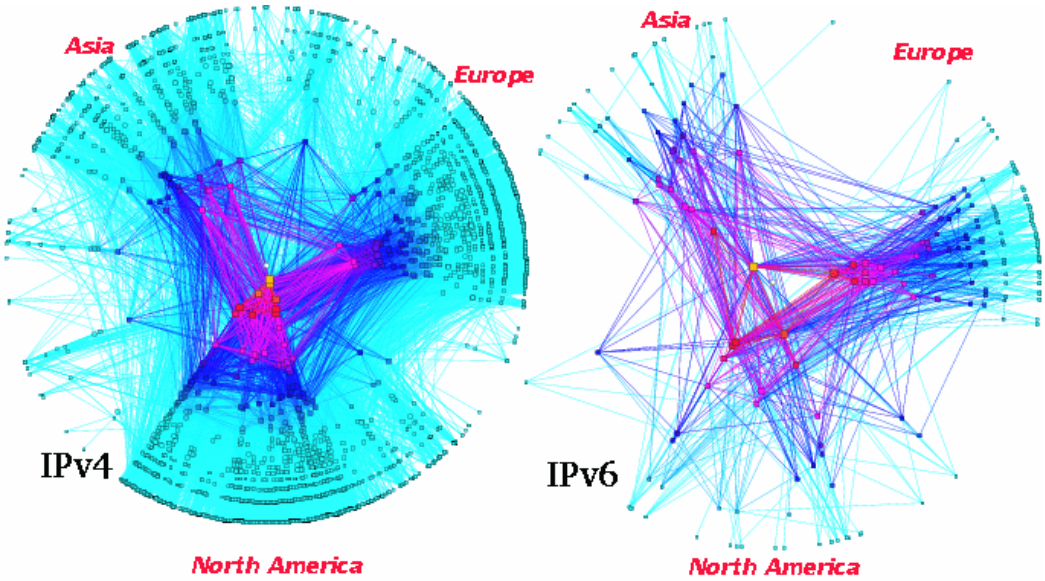
ตารางที่ 3.1 ลำดับของประเทศทั่วโลกที่ได้รับจัดสรร IPv6 address

Rank	Country Prefixes	Visible Prefixes	Allocated Percentage	Visible
1	United States	76	170	7.19%
2	Japan	77	99	7.28%
3	Germany	58	97	5.49%
4	The Great Britain	27	57	2.55%
5	Netherlands, The	29	51	2.74%
6	Italy	24	39	2.27%
7	Korea	16	36	1.51%
8	France	15	33	1.42%
9	Poland	18	26	1.70%
10	Switzerland	18	25	1.70%
24	**Thailand**	**8**	**10**	**0.76%**

จากตารางที่ 3.1 จะเห็นได้ชัดว่าศูนย์กลางการใช้งานโครงข่าย IPv6 อยู่ทวีปยุโรปและเอเชีย โดยประเทศไทยอยู่ในอันดับที่ 24 ของประเทศทั่วโลกที่ได้รับจัดสรร IPv6 address blocks

จากภาพรวมของการจัดสรร IPv6 การนำ IPv6 ไปใช้งานจริงจะอยู่ที่ทวีปยุโรปและเอเชียเป็นหลัก ส่วนทวีปอเมริกาเหนือนั้น ยังไม่เด่นชัดในเรื่องการนำไปใช้งาน สาเหตุที่สำคัญประการแรกคือ ในปัจจุบันทวีปอเมริกาเหนือมีส่วนแบ่งของ IPv4 address อยู่ถึงร้อยละ 62 ของ IP Address ทั้งหมดในโลก (จากตารางที่

2.1) ซึ่งน่าจะเป็นสาเหตุที่ทำให้ทวีปนี้ยังไม่เห็นความจำเป็นของ IPv6 ในทางตรงกันข้าม ทั้งยุโรปและเอเชียต่างพบปัญหาการมี IP Address ไม่พอกับจำนวนผู้ใช้อินเตอร์เน็ตเนื่องจากส่วนแบ่งของ IPv4 address มีน้อยกว่ามาก สาเหตุประการที่สองสืบเนื่องมาจากเทคโนโลยีโทรศัพท์เคลื่อนที่ยุคที่สาม (3G wireless technology) ทั้งในยุโรปและเอเชียต่างมีความต้องการสูงทางด้านเทคโนโลยี 3G ซึ่งเทคโนโลยีนี้ทำให้เกิดความต้องการ IP Address ที่เพิ่มขึ้น ดังนั้นจึงพบว่าในทวีปยุโรปและเอเชียเริ่มที่จะมีการแก้ปัญหาการขาดแคลน IP address หรืออีกนัยหนึ่งคือการสนใจต่อการเข้ามามีบทบาทในการใช้งานของ IPv6 อย่างจริงจัง ดังจะเห็นได้จากการที่บริษัทผู้นำทางด้านเทคโนโลยี IPv6 ล้วนตั้งอยู่ในภูมิภาคนี้ รัฐบาลประเทศญี่ปุ่นและสาธารณรัฐเกาหลี ต่างให้การสนับสนุนและผลักดันภาคเอกชนให้หันมาให้บริการ IPv6 ในเชิงพาณิชย์มากขึ้น อีกทั้งประเทศใหญ่ๆ อย่างเช่น จีน ก็คาดว่าจะเริ่มหันมาเอาจริงเอาจังในด้านนี้ ด้วยจำนวนประชากรและสถานะทางเศรษฐกิจที่บังคับนอกจากปัจจัยทางภูมิศาสตร์แล้ว



รูปที่ 3.1 การเปรียบเทียบการเชื่อมต่อระหว่าง AS ของโครงข่าย IPv4 และโครงข่าย IPv6

จากรูปที่ 3.1 ซึ่งแสดงการเปรียบเทียบแผนผังการเชื่อมต่อระหว่าง AS (Autonomous System) ภายในโครงข่าย IPv4 และภายในโครงข่าย IPv6 หนึ่ง AS เทียบได้กับ ISP หนึ่งราย จุดที่อยู่ใกล้ศูนย์กลางของวงกลมหมายถึง AS ที่มีปริมาณการเชื่อมต่อไปยัง AS อื่นๆ สูง จะเห็นว่าการเชื่อมต่อระหว่าง AS ในโครงข่าย IPv4 นั้นมีความหนาแน่นมากกว่าการเชื่อมต่อในโครงข่าย IPv6 มาก นอกจากนี้ ยังพบว่า AS ที่มีปริมาณการเชื่อมต่อภายในโครงข่าย IPv4 ส่วนใหญ่แล้วจะอยู่ในทวีปอเมริกาเหนือ ซึ่งต่างจากแผนผังของ IPv6 ซึ่งพบปริมาณการเชื่อมต่อมาก ในบริเวณทวีปยุโรปและเอเชีย

ในบทนี้จะทำการสรุปตัวอย่างการประยุกต์ใช้งานที่สำคัญและน่าสนใจของ IPv6

3.1 ตัวอย่างการใช้งาน IPv6 ในต่างประเทศ

1. ญี่ปุ่น (Japan IPv6 Promotion Council)

ญี่ปุ่นมีคณะกรรมการที่ชื่อว่า "Japanese IPv6 Promotion Council" ซึ่งแสดงความเป็นผู้นำอย่างเข้มแข็งในการส่งเสริม สนับสนุน ให้ IPv6 เป็นโครงสร้างพื้นฐานของประเทศ

รูปที่ 3.2 โลโก้ของ Japanese IPv6 Promotion Council

นอกจากนี้ รัฐบาลญี่ปุ่นได้จัดตั้งโครงการ "u-Japan" (Ubiquitous Japan) เพื่อให้ผู้ใช้บริการชาวญี่ปุ่นได้รับบริการในลักษณะดังนี้

- Ubiquitous access, connecting everyone and everything คือ ให้ผู้ใช้มีการติดต่อกันได้อย่างทั่วถึง
- Universal and user-friendly คือ ให้การติดต่อเป็นแบบสากล ใช้ได้ทั่วโลก
- User-Oriented คือ ผู้ใช้ต้องเชื่อมต่อกับระบบ
- Unique, be something special คือ ให้ความพิเศษกับผู้ใช้

รัฐบาลญี่ปุ่นยังเน้นในการทำให้เทคโนโลยีนี้แพร่หลายจาก Home network เป็น Space communication และจาก Sensor network เป็น RFID เป็นต้น

แผนการของรัฐบาลญี่ปุ่นไม่ใช่เพียงส่งเสริม สนับสนุน IPv6 ในญี่ปุ่นเท่านั้น แต่จะทำการส่งเสริมในต่างประเทศด้วย และจะเป็นผู้นำในการแสดงให้เห็นว่าจะนำ IPv6 มาใช้ในอุตสาหกรรมอย่างไรเพื่อสร้างโอกาสไปทั่วโลกและจะวาง IPv6 ไว้ที่ใดในระบบทั่วโลก

สำหรับผู้ที่ต้องการข้อมูลเพิ่มเติมสามารถหาดูได้จาก URL ต่อไปนี้

- IPv6 Promotion Council http://www.v6pc.jp/en/index.phtml
- BSD KAME http://www.kame.net/ code base and Linux USAGI http://www.linux-ipv6.org/ code base
- IPv6-based phone service FreeBit http://www.freebit.com/english/index.html
- Live E! project http://www.live-e.org
- InternetCAR Project http://www.sfc.wide.ad.jp/InternetCAR/

- IPv6-FIX http://v6fix.net/

2. สาธารณรัฐเกาหลี (South Korean IPv6 Forum)

ผู้เป็นอดีตรัฐมนตรีกระทรวงสารสนเทศและการสื่อสารและเป็นอดีต CEO ของบริษัทซัมซุงของเกาหลีใต้ผู้ซึ่งเปลี่ยนบริษัทซัมซุงจากเดิมที่เป็นบริษัทเพื่อความบันเทิงให้เป็นบริษัทเพื่อคอมพิวเตอร์ ได้มีการกำหนดกลยุทธ์เพื่อโปรโมทบริษัท เรียกว่า IT839 โดยเน้นที่จะนำ IPv6 มาใช้งาน และมีการประชุมร่วมกับ CEO ของ 30 บริษัท เพื่อให้ทราบถึงความก้าวหน้า หลังจากนั้น กระทรวงสารสนเทศและการสื่อสารได้มีการจัดตั้งโครงการ KOREAv6 ซึ่งเป็นโครงการนำร่องระยะที่หนึ่งขึ้นเมื่อปีที่ผ่านมาและมีแผนที่จะผลักดันให้โครงการระยะที่สองเกิดขึ้นภายในปีนี้ เพื่อสนับสนุนการนำเอาเทคโนโลยี IPv6 เข้ามาใช้งาน

รูปที่ 3.3 โลโก้ของ South Korean IPv6 Forum

ในภาคส่วนอื่นก็เริ่มมีการนำเทคโนโลยี IPv6 มาใช้งานเช่นกัน ตัวอย่างเช่น ในปี 2004 มีการใช้งานในระบบของ E-Government, กรมไปรษณีย์, มหาวิทยาลัย, โรงเรียน, กระทรวงกลาโหม เป็นต้น

ในส่วนของผู้ผลิตอุปกรณ์ทางการสื่อสาร อันได้แก่ Samsung Electronics, LG Electronics, Locus, iBIT, Mercury และ AddPac Technology ร่วมทั้งองค์กรที่ทำด้านการวิจัยเช่น Electronics and Telecommunication Research Institute (ETRI) ได้มีการผลิตอุปกรณ์ทางการสื่อสารต่างๆ เช่น router ทั้งขนาดเล็กและขนาดกลาง, home router, trunk gateways, access gateway, Voice over IP : VoIP, wireless access point เป็นต้น เพื่อรองรับการใช้งานเทคโนโลยี IPv6 ในอนาคต(http://www.ipv6.or.kr/english/index.new.htm)

3. เกาะไต้หวัน (Taiwan IPv6 Forum)

ไต้หวันมีนโยบายการจัดทำ E-Taiwan program ซึ่งประกอบไปด้วย e-Society, e- Commerce, e-Government และ e-Transportation เพื่อทำให้ไต้หวันเป็นประเทศที่มีความก้าวหน้าทางเทคโนโลยีอินเตอร์เน็ต ซึ่งนโยบายนี้จำเป็นต้องใช้เทคโนโลยี IPv6 โดยมีการวางแผนไว้ว่าจะให้มีผู้ใช้บริการ IPv6 ได้ถึง 6 ล้านคนได้ในปี 2551 และโครงข่ายของรัฐบาลต้องได้ใช้ IPv6 ภายในปี 2550 นี้ (http://www.ipv6.org.tw/)

รูปที่ 3.4 โลโก้ของ Taiwan IPv6 Forum

4. สาธารณรัฐประชาชนจีน (China IPv6 Council)

จีนมีการนำเอา IPv6 มาใช้งาน โดยการจัดตั้งโครงการ China Next Generation Internet (CNGI project) ขึ้น โดยกลุ่มผู้ริเริ่มที่ใช้ชื่อว่า 6TNET ซึ่งได้ทำการเสนอแนะให้มีการใช้ IPv6 ใน CNGI project แก รัฐบาลจีน เพื่อประโยชน์ทางการค้า การบริการและการวิจัย ทั้งยังมีการพิสูจน์ให้เห็นว่าผู้ที่ด้อยกว่าทางด้านเทคโนโลยีสามารถก้าวข้ามผู้นำได้ด้วยเทคโนโลยี IPv6 นี้ (http://www.ipv6.net.cn/)

รูปที่ 3.5 โลโกของ China IPv6 Council

5. ทวีปยุโรป (European IPv6 Task Force)

รูปที่ 3.6 โลโก้ของ European IPv6 Task Force

คณะกรรมาธิการของสหภาพยุโรปเป็นผู้นำและแบบอย่างที่ดี ได้มีการจัดตั้งโครงการต่างๆ ขึ้น เช่น 6INIT, 6WINIT, 6NET, Euro6ix เป็นต้น และตระหนักถึงความจำเป็นในการใช้งาน IPv6

ในปี 2001 IPv6 Forum ได้เสนอกับ Dr.Joao Da Silva ซึ่งเป็นผู้ก่อตั้ง The European IPv6 Task Force ให้พยายามทำให้ยุโรปมีการตระหนัก รับรู้และเผยแพร่ เรื่องเกี่ยวกับ IPv6

รัฐบาลของประเทศต่างๆ ในทวีปยุโรปที่สนใจและเห็นพ้องด้วย ก็มีการจัดตั้งก็ทุนหรืออะไรก็ตามที่เกี่ยวข้องเพื่อทำการส่งเสริม สนับสนุน IPv6 :

- รัฐบาลฝรั่งเศส ได้ทำการจัดตั้ง French IPv6 Task Force (http://www.fr.ipv6tf.org/) ซึ่งมีการร่วมมือกันกับหลายฝ่าย ได้แก่ G6 และ CN6 นับเป็นกลุ่มความร่วมมือที่ใหญ่ที่สุดในทวีปยุโรป เมื่อไม่นานมานี้ได้มีการจัดตั้ง IPv6 Competence และ IPv6 Task Force ใน มลฑลบริททานี (http://www.point6.net/) ของฝรั่งเศสด้วย

รูปที่ 3.7 โลโก้ของ French IPv6 Task Force

- รัฐบาลออสเตรีย สนับสนุนให้มีการจัดตั้ง Austrian IPv6 Task Force (http://www.at.ipv6tf.org/)
- รัฐบาลฟินิช สนับสนุนให้มีการจัดตั้ง Finish IPv6 Task Force (http://www.fi.ipv6tf.org/)
- กระทรวงกลาโหมของเยอรมันเป็นแรงจูงใจให้เกิดองค์กร German IPv6 Summit ในปี 2004 เพื่อสนับสนุนการนำ IPv6 ไปสู่ผู้ให้บริการ (http://www.ipv6tf.de/tiki-index.php)

6. ทวีปอเมริกาเหนือ (North American IPv6 Task Force NAv6TF)

North American IPv6 Task Force (NAv6TF) เป็นคณะกรรมการที่จัดตั้งขึ้นเพื่อทำการสนับสนุน ส่งเสริม ให้คำปรึกษา เป็นศูนย์กลางทางเทคนิค ให้การช่วยเหลือทางด้านธุรกิจการค้าและการศึกษา และให้คำแนะนำแก่ประเทศทางทวีปอเมริกาเหนือที่จะนำเทคโนโลยี IPv6 ไปใช้ โดย NAv6TF มีการทำงานร่วมกับคณะกรรมการอื่นๆ ที่เกี่ยวกับ IPv6 ทั่วโลกเพื่อให้ความช่วยเหลือแก่ผู้ที่จะนำเทคโนโลยี IPv6 ไปใช้งาน ในส่วนอื่นๆ ของโลกด้วย (http://www.nav6tf.org/, http://www.moonv6.org/)

รูปที่ 3.8 โลโก้ของ North American IPv6 Task Force

3.2 ผู้ผลิตและผู้ให้บริการ IPv6 ในต่างประเทศ

- Router จากผู้ผลิตดังต่อไปนี้สามารถรองรับเทคโนโลยี IPv6 ได้แก่
  - Cisco
  - Juniper
  - Hitachi
  - NEC
  - Fujitsu
  - Extreme
  - Foundry
  - NOKIA
  - etc,

รูปที่ 3.9 Router ที่สามารถใช้งาน IPv6 ได้

- ผู้ผลิต gateway ที่รองรับ IPv6 ได้แก่
  - Panasonic
  - NEC
  - NTT Communication
  - etc,

รูปที่ 3.10 IPv6 gateway

3.3 ระบบปฏิบัติการ (Operating System) ที่สามารถใช้ IPv6 ได้ในปัจจุบัน

ปัจจุบันระบบปฏิบัติการส่วนใหญ่พร้อมสนับสนุนการใช้งาน IPv6 (IPv6 Ready) ตัวอย่าง เช่น Digital UNIX, HP-UX, AIX, BSDi, *BSD, Linux, MS Windows 2000, XP, 9X, NT, Solaris, MAC OS X, Open-VMS โดยในส่วนของ Linux ผู้ใช้สามารถดาวน์โหลดโปรแกรมประยุกต์และ service ต่างๆ ได้จาก URL ต่อไปนี้

- http://www.kame.net/
- http://www.deepspace6.net/docs/ipv6_status_page_apps.html
- http://www.bieringer.de/linux/IPv6/index.html

สำหรับ Microsoft Windows เวอร์ชันต่างๆ สามารถใช้งานได้ โดย

- Windows9X มี Trumpet Winsock ซึ่ง version ล่าสุดใช้ IPv6 ได้
- Windows 2000 ถ้าติดตั้ง SP1 ขึ้นไป แล้วจะสามารถดาวน์โหลด TCP/ IPv6 มาลง ก็จะใช้งาน IPv6 ได้
- Windows 2003 และ Windows XP สามารถใช้งาน IPv6 ได้อยู่แล้ว (IPv6 Ready)

3.4 ตัวอย่างเครื่องใช้ไฟฟ้าและอุปกรณ์ที่มีแนวโน้มจะถูกแจกจ่าย IPv6 ให้ในอนาคต

- **Internet refrigerator** เมื่อทำการกำหนด IP ให้กับตู้เย็น ผู้ใช้ก็สามารถสั่งงานให้ตู้เย็นทำงานต่างๆ ผ่านโครงข่ายอินเตอร์เน็ตได้ เช่น สั่งให้ทำการละลายน้ำแข็งสำหรับตู้เย็นที่ไม่มีระบบละลายน้ำแข็งเอง เป็นต้น

รูปที่ 3.11 Internet refrigerator

- **Internet car** ในปัจจบันมีระบบที่เรียกว่า Intelligent Transport Systems (ITS) เป็นระบบที่ช่วยในการเดินทาง เพิ่มประสิทธิภาพการจราจร โดยการรวมเอาทั้งรถ ผู้ขับและถนนเป็นระบบเดียวกัน มีอุปกรณ์เสริมต่างๆ เช่น Car Navigation, Vehicle Information และCommunication System เพื่อช่วยในการตัดสินใจเลือกเส้นทาง และการติดต่อกับรถคันอื่นๆ

Internet car จะคิดว่ารถเป็นโหนดหนึ่งในอินเตอร์เน็ต ผู้ใช้สามารถทำการติดต่อกับรถ หรือสอบถามข้อมูลเกี่ยวกับรถผ่านทางอินเตอร์เน็ตได้

รูปที่ 3.12 Internet car

- **IP TV, HDTV over IP** โทรทัศน์ที่เราใช้กันอยู่ในปัจจุบัน แผนผังรายการผู้ผลิตจะเป็นผู้กำหนด แต่ถ้าหากมีการใส่ IP ให้กับโทรทัศน์ ผู้ชมก็จะสามารถเลือกรายการที่อยากดู เมื่อใด เวลาใดก็ได้ ทางสถานีก็จะทำการกระจายข้อมูลแบบ multicast มายังผู้รับได้

รูปที่ 3.13 IP TV

- **IP Phone** เครื่องโทรศัพท์ที่มี IP เป็นของตัวเอง จะสามารถเชื่อมต่อเข้ากับระบบอินเตอร์เน็ตได้ ก็จะสามารถทำการสื่อสารผ่านอินเตอร์เน็ตได้ ทั้งยังเป็นการลดค่าใช้จ่ายในการสื่อสารเพราะระบบอินเตอร์เน็ตเชื่อมต่อกันได้ทั่วโลกอยู่แล้ว ผู้ให้บริการจึงไม่ต้องมีการสร้างโครงข่ายและระบบใหม่ ผู้ใช้จึงไม่ต้องเสียค่าบริการในด้านนี้

รูปที่ 3.14 VoIP Phone

- **RFID** เป็นผลิตภัณฑ์ที่มีการจัดเก็บข้อมูลลงในรูปแบบของบัตรหรือเหรียญขนาดเล็กซึ่งสามารถอ่านและเขียนข้อมูลลงไปใน Tag ได้หลายครั้งโดยการใช้คลื่นความถี่ในการอ่านและเขียนข้อมูล ถ้ามีการใส่ IP เข้าไปใน card เมื่อต้องการอ่านหรือเขียนก็จะสามารถทำผ่านระบบอินเตอร์เน็ตได้ เช่น เมื่อมีการอ่านค่าจาก card หนึ่งก็สามารถส่งไปยังที่ต่างๆ ตามต้องการได้

รูปที่ 3.15 RFID

บทที่ 4
ผลกระทบการใช้งาน IPv6 ในเทคโนโลยีที่มีในปัจจุบันและเทคโนโลยีที่จะเกิดขึ้นในอนาคต

ตามที่ได้กล่าวมาในบทก่อนหน้านี้แล้วว่า ความสำคัญของการมี IP address ที่ไม่ซ้ำกันและสารมารถเห็นกันได้ทั่วโลกจะช่วยผลักดันการพัฒนาแอปพลิเคชั่นแบบ peer-to-peer ที่ต้องการ IP address จริงเป็นจำนวนมาก ซึ่งปัจจุบัน IPv4 กำลังจะหมดไป ไม่เพียงพอต่อความต้องการที่เพิ่มมากขึ้นเรื่อยๆ จึงจำเป็นต้องมีการเปลี่ยนแปลง และการเปลี่ยนแปลง IPv4 เป็น IPv6 ยังทำให้เกิดการพัฒนาในหลายๆ ด้าน เช่น สามารถรองรับการขยายตัวของการบริการ Broadband Internet รองรับการขยายตัวของบริการโทรศัพท์เคลื่อนที่ Mobile Internet และ Voice over IP และยังสามารถลดความยุ่งยากและซับซ้อนในการเชื่อมต่อกับต่างประเทศ และเพิ่ม Network Security ขึ้นมากกว่า IPv4 อีกด้วย

นอกจาก IPv6 จะทำให้ให้เกิดการพัฒนาด้านต่างๆ แล้ว IPv6 ยังมีความสามารถมากกว่า IPv4 หลายๆ ด้านด้วย เช่น ความสามารถในการจัดการโครงข่ายซึ่ง IPv6 สามารถติดตั้งระบบได้อัตโนมัติ (autoconfiguration) รองรับ Broadcast Multicast Anycast ทำให้ช่วยลด Traffic ในโครงข่ายลงได้ และยังมี Security ดีกว่า IPv4 รองรับการใช้งาน IPSec และรองรับการใช้งาน Mobile IP IPv6 , VPN (Virtual Private Network) และได้พัฒนา QOS (Quality of Service) ให้ดีขึ้นด้วย

จากสาเหตุที่จำเป็นต้องเปลี่ยนแปลงจาก IPv4 เป็น IPv6 และข้อดีต่างๆ ที่เพิ่มขึ้น ดังนั้นเราจึงจำเป็นต้องเปลี่ยนจาก IPv4 เป็น IPv6 อย่างแน่นอน ดังนั้นเราจึงต้องมีการปรับเปลี่ยนระบบโครงข่ายจาก IPv4 เป็น IPv6

4.1 การปรับเปลี่ยนระบบโครงข่ายจาก IPv4 เป็น Ipv6

การปรับเปลี่ยนโครงข่ายจาก IPv4 สู่ IPv6 นั้น สามารถทำได้ที่สองระดับ ระดับแรกคือการปรับเปลี่ยนที่โครงข่าย เช่น การปรับเปลี่ยนที่อุปกรณ์เราเตอร์ หรือเครื่องเซิร์ฟเวอร์ วิธีนี้เหมาะสำหรับผู้ให้บริการอินเตอร์เน็ต (Internet Service Provider, ISP) หรือผู้ดูแลโครงข่าย (Network Operator) ที่ต้องการให้บริการ IPv6 บนโครงข่ายที่ตนดูแลอยู่ ระดับที่สองคือการปรับเปลี่ยนในส่วนของผู้ใช้ นั่นคือ การเปลี่ยนแปลงที่คอมพิวเตอร์ส่วนบุคคล (Desktop, end host) วิธีนี้เหมาะสำหรับผู้ที่ต้องการทดลองใช้ IPv6 แต่โครงข่าย ISP ที่ใช้บริการอยู่ยังไม่พร้อมที่จะให้บริการ IPv6 นอกจากนี้ เราสามารถจำแนกวิธีการปรับเปลี่ยนโครงข่าย ตามเทคนิคที่ใช้ ซึ่งในปัจจุบันมีอยู่ 3 เทคนิคหลักด้วยกัน หนึ่งคือ การใช้งาน IPv4 และ IPv6 ควบคู่กัน หรือที่เรียกว่า Dual stacks สองคือเทคนิคการทำอุโมงค์ (tunnel) เพื่อให้ข้อมูลในรูปแบบของ IPv6 สามารถส่งออกไปบนโครงข่าย IPv4 ได้ และสามคือ เทคนิคการแปลงข้อมูล (translation) ระหว่างแพ็กเก็ต IPv6 และ IPv4 การ

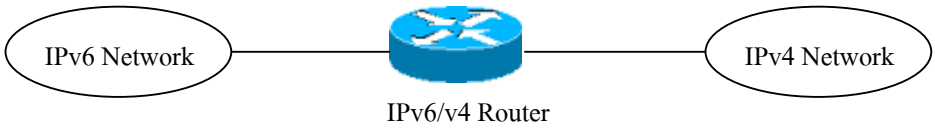
เลือกใช้แต่ละเทคนิคต้องดูที่ความเหมาะสมของลักษณะการใช้งานของโครงข่ายที่มีอยู่รวมถึงระดับของการปรับเปลี่ยนที่เหมาะกับผู้ใช้

1. Dual stacks

Dual stacks หมายถึง การใช้งาน IPv4 และ IPv6 stack ควบคู่กันไป ภายในอุปกรณ์ตัวเดียวกัน Dual stacks เป็นทางออกที่ง่ายที่สุดสำหรับโครงข่ายที่ต้องการเริ่มใช้งาน IPv6 และถูกใช้อย่างแพร่หลายมากที่สุดในปัจจุบัน หลักการทำงานของ Dual Stack คือการกำหนด IP stack ออกเป็น 2 Stacks ทำงานขนานกัน เช่น เมื่อโหนดได้รับ IPv6 packet โหนดจะเลือก IPv6 stack มาจัดการกับแพ็กเก็ต (โดยตรวจสอบ Protocol version จากส่วนหัวของแพ็กเก็ต) ในขณะเดียวกันโหนดสามารถติดต่อกับโครงข่าย IPv4 (ผ่าน IPv4 stack) ได้เหมือนเดิมไม่ต้องเปลี่ยนแปลง โดยโหนดที่มี Dual stack นี้จะต้องมี IP Address สองหมายเลข คือ IPv4 Address และ IPv6 Address การติดตั้ง Dual stacks สามารถทำได้ทั้งที่โฮสต์ที่เซิร์ฟเวอร์และที่อุปกรณ์โครงข่าย เช่น เราเตอร์ ซึ่งก่อนอื่นท่านต้องได้รับการจัดสรรหมายเลข IPv6 Address ก่อนจึงจะสามารถใช้งาน Dual stacks ได้ ซึ่งเราสามารถลงทะเบียนเพื่อขอรับ IPv6 Address ได้กับศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติที่ http://www.ipv6.nectec.or.th/ipv6_delegation.php

<u>ความต้องการเบื้องต้น (ระดับ Host และ Network)</u>

- หมายเลข Public IPv4 Address และ IPv6 Address อย่างละ 1 หมายเลข สำหรับแต่ละอุปกรณ์ที่ต้องการติดตั้ง Dual stacks
- โฮสต์หรืออุปกรณ์ที่จะใช้งาน dual-stack ต้องรองรับ IPv6



รูปที่ 4.1 การใช้งาน Dual Stacks ที่เราเตอร์

2. Tunnel

หลักการทำ Tunnel สามประเภท คือ

2.1 Manually Configured Tunnel

Manually Configured Tunnel เป็นวิธีที่นิยมกันมาก สำหรับการให้บริการเชื่อมต่อ กันระหว่างเครื่องที่ใช้และติดตั้งหมายเลข IPv6 เพียงอย่างเดียว โดยต้องมีเกตเวย์ที่ติดตั้งและใช้งาน

แบบ Dual stacks ซึ่งจะทำหน้าที่เป็นอุโมงค์ โครงข่ายทางเข้าและทางออก โดยแต่ละด้านจะต้องเก็บหมายเลข IP Address ของอุโมงค์โครงข่ายของอีกด้านหนึ่งที่ต้องการเชื่อมต่อ ซึ่งผู้ดูแลระบบจะต้องใส่หมายเลข IP Address ของปลายทางอุโมงค์เข้าไปเอง วิธีนี้จึงต้องการการดูแลสูงในส่วนของการทำงาน เมื่อแพ็กเก็ต IPv6 มาถึงอุโมงค์ ก็จะถูกห่อหุ้มด้วยเฮดเดอร์ IPv4 โดยใช้หมายเลข IPv4 ของโครงข่ายต้นทาง หมายเลข IPv4 ของโครงข่ายปลายทาง และระบุชนิดโพรโทคอลของข้อมูลที่อยู่ภายในเป็น IPv6 เมื่อแพ็กเก็ตมาถึงปลายทางของอุโมงค์โครงข่ายปลายทางจะทำการตรวจสอบเฮดเดอร์ ซึ่งจะทราบว่าภายในเป็นแพ็กเก็ตที่ใช้หมายเลข IPv6 ดังนั้น ตัวเกตเวย์จะเอาส่วนหัว IPv4 ออไปให้เหลือแต่ส่วนที่เป็น IPv6 แพ็กเก็ตแล้วส่งต่อไปยังเครื่องปลายทางที่ใช้หมายเลข IPv6 ที่ระบุอยู่ในส่วน Destination ของเฮดเดอร์ IPv6

<u>ความต้องการเบื้องต้น (ระดับ Network)</u>

- เราเตอร์หรือเกตเวย์ที่เป็น Dual stacks สำหรับ Tunnel Geteway
- หมายเลข Public IPv4 Address และ IPv6 Address อย่างละ 1 หมายเลข สำหรับ Tunnel Geteway
- ต้องทราบหมายเลข Public IPv4 Address และ IPv6 Address ของ Tunnel Gateway อีกฝั่ง

2.2 Semi Automatic Tunnel (Tunnel Broker)

การทำงานของ Semi Automatic Tunnel หรือที่รู้จักในชื่อ Tunnel Broker คือ การสร้างอุโมงค์อัตโนมัติโดยผู้ใช้ (end user) ต้องลงทะเบียนใช้บริการกับผู้ให้บริการ โดยผู้ให้บริการจะสร้าง Tunnel เพื่อเชื่อมต่อไปยังโครงข่าย IPv6 แทนผู้ที่มาลงทะเบียน ดังนั้น ผู้ที่ให้บริการ Tunnel Broker จึงเป็นเสมือนผู้ให้บริการ IPv6 แก่ผู้ใช้ที่มีการเชื่อมต่อผ่านโครงข่าย IPv4 อยู่แล้ว ในปัจจุบันมีผู้ให้บริการ Tunnel Broker หลายราย ตัวอย่างเช่น http://www.freenet6.net และ http://ipv6.he.net ในประเทศไทยยังไม่มีผู้ให้บริการ Tunnel Broker (สำหรับรายชื่อผู้ให้บริการต่างประเทศทั้งหมดสามารถดูได้ที่ http://www.ipv6.org)

ตามมุมมองของผู้ใช้ การเลือกใช้งาน Tunnel Broker จะต่างจากการเชื่อมต่อแบบ Manually Configured Tunnel และ Fully Automatic Tunnel ตรงที่ Tunnel Broker เหมาะกับโครงข่าย IPv6 เล็กๆ หรือโฮสต์จำนวนไม่มาก ที่ต้องการเชื่อมต่อโครงข่าย IPv6 ใหญ่แห่งอื่นอย่างง่ายๆ การเชื่อมต่อด้วย Tunnel แบบอื่น จะเหมาะกับการติดต่อกันโดยตรงระหว่างโครงข่าย IPv6 ย่อยสองโครงข่าย โดยไม่ต้องพึ่งหรือรอการเชื่อมต่อที่ระดับ ISP

<u>ความต้องการเบื้องต้น (ระดับ Network)</u>

- เราเตอร์หรือเกตเวย์ (IPv4 หรือ Dual stacks ก็ได้) สำหรับ Tunnel Broker

- เราเตอร์หรือเกตเวย์ที่เป็น Dual stacks สำหรับ Tunnel Server (Tunnel Geteway)
- หมายเลข Public IPv4 address 1 หมายเลข สำหรับ Tunnel Broker
- หมายเลข Public IPv4 address 1 หมายเลข สำหรับ Tunnel Server

<u>ความต้องการเบื้องต้น (ระดับ Host)</u>

- ผู้ที่เรียกใช้บริการจาก Tunnel Broker อาจเป็นโฮสต์หรือเราเตอร์ก็ได้ ซึ่งเราจะเรียกอุปกรณ์นี้ว่า Tunnel Broker Client
- อุปกรณ์โฮสต์หรือเราเตอร์ที่เป็น Dual stacks สำหรับ Tunnel Broker Client
- หมายเลข Public IPv4 address สำหรับ Tunnel Broker Client 1 หมายเลข
- ชื่อที่ต้องการลงทะเบียนในฐานข้อมูล DNS คู่กับหมายเลข IPv6 address ที่ได้รับจัดสรรจาก Tunnel Broker
- ถ้า Tunnel Broker Client เป็นโฮสต์ ไม่ควรอยู่หลัง NAT Gateway หรือถ้าหลีกเลี่ยงไม่ได้ ต้องเปิดพอร์ต 41 ที่ NAT Gateway
- ถ้า Tunnel Broker Client เป็นเราเตอร์ ต้องระบุจำนวน IPv6 address ที่ต้องการรับจัดสรรจาก Tunnel Broker

ขั้นตอนการติดตั้ง Tunnel Broker บนโฮสต์ส่วนใหญ่แล้ว ผู้ที่ให้บริการ Tunnel Broker จะเป็นผู้กำหนดขั้นตอนการติดตั้งค่าต่างๆ บนโฮสต์ที่ต้องการเป็น Tunnel Broker Client มาให้ โดยหลักการแล้วเครื่องคอมพิวเตอร์ที่เป็น Tunnel Broker Client จะต้องทำการติดตั้ง Dual stacks ก่อนให้ใช้งาน IPv6 ได้ จากนั้นผู้ใช้จะต้องไปลงทะเบียนขอใช้ Tunnel Broker ที่เว็บไซต์ของผู้ให้บริการ Tunnel Broker และทางผู้ให้บริการจะส่งซอฟต์แวร์เพื่อใช้ในการติดต่อกับ Tunnel Broker มาให้ลงที่เครื่องโฮสต์

2.3 Fully Automatic Tunnel (6to4 Tunnel)

การทำงานแบบ Fully Automatic Tunnel มีขั้นตอนการทำงานเหมือนกับ Manually Configured Tunnel แต่จะแตกต่างกันตรงที่ Tunnel Gateway แต่ละด้านไม่ต้องเก็บหมายเลข IP address ของเกตเวย์ปลายทางที่ต้องการเชื่อมต่อ แต่เกตเวย์จะตรวจสอบหมายเลขเครื่องปลายทางโดยพิจารณาจากหมายเลขปลายทางของแพ็กเก็ตที่ถูกห่อหุ้มอยู่

วิธีหนึ่งในการทำ Fully Automatic Tunnel คือ วิธีที่เรียกว่า 6to4 Tunnel โครงข่ายที่เชื่อมต่อแบบ 6to4 Tunnel จะต้องกำหนดหมายเลข IPv6 Prefix พิเศษให้กับตัวเกตเวย์ทั้งสองฝั่งของ 6to4 Tunnel

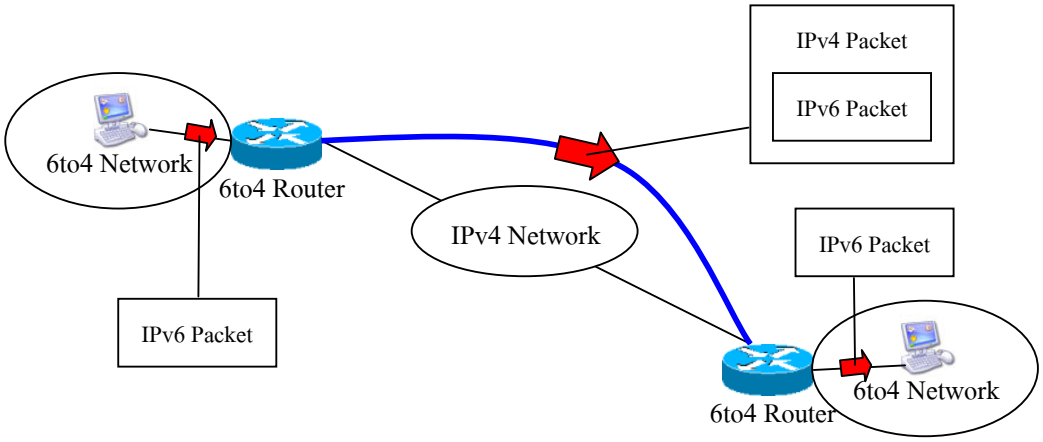
ในปัจจุบันเราสามารถลงทะเบียนเพื่อขอใช้บริการ 6to4 tunnel ได้กับศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติที่ http://www.ipv6.nectec.or.th

<u>ความต้องการเบื้องต้น (ระดับ Network)</u>

- เราเตอร์หรือเกตเวย์ที่เป็น Dual stacks สำหรับ Tunnel Gateway
- หมายเลข Public IPv4 address 1 หมายเลข สำหรับ Tunnel Gateway

<u>ความต้องการเบื้องต้น (ระดับ Host)</u>

- หมายเลข Public IPv4 address สำหรับโฮสต์ 1 หมายเลข
- โฮสต์ไม่ควรอยู่หลัง NAT Gateway หรือ ถ้าหลีกเลี่ยงไม่ได้ต้องเปิดพอร์ต 41 ที่ NAT Gateway



รูปที่ 4.2 การเชื่อมต่อโครงข่ายแบบอุโมงค์ IPv6-over-IPv4 Tunnel

3. Translation

เทคนิคการทำ Translation เป็นวิธีที่ใช้กับการสื่อสารข้ามโครงข่าย เช่น โหนดจากโครงข่าย IPv4 ต้องการคุยกับเซิร์ฟเวอร์ ในโครงข่าย IPv6 หรือโหนดที่เป็น IPv6 ต้องการคุยกับเซิร์ฟเวอร์ที่เป็น IPv4 ซึ่งจะเป็นกรณีที่ต่างไปจากการใช้งาน Dual stacks และ Tunnel การทำ Translation คือการแปลงข้อมูลไปมาระหว่างข้อมูลในรูปแบบของ IPv4 packet และ IPv6 packet การแปลงข้อมูลนี้สามารถทำได้สองแบบ แบบแรกคือ การแปลงที่ end host โดยเพิ่ม Translator function เข้าไปใน protocol stack โดยอาจอยู่ที่ network layer หรือ socket layer ก็ได้ แบบที่สองคือการแปลงที่ Network device โดยจะต้องใช้ gateway ทำหน้าที่เป็น IPv6- IPv4 และ IPv4- IPv6 translator อยู่ที่ทางออกที่มีการเชื่อมต่อระหว่างโครงข่าย IPv6 และ IPv4

ในบทความนี้ เราจะยกตัวอย่างการทำ Translation ที่ Network device ได้แก่ วิธีที่เรียกว่า NAT-PT (Network Address Translation-Protocol Translation) ซึ่งเป็นการทำ Translation ที่แพร่หลายมากวิธีหนึ่งรายละเอียดของการทำ NAT-PT มีดังนี้

3.1 NAT-PT (Network Address Translation – Protocol Translation)

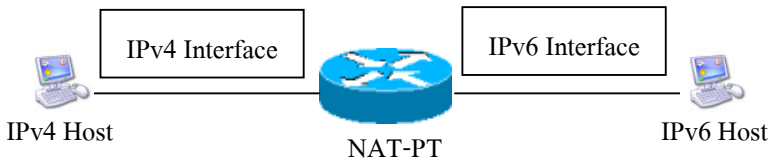
NAT-PT มีพื้นฐานเช่นเดียวกับการทำ NAT ในโครงข่าย IPv4 นั่นก็คือ การแปลง IP Address โดยเสมือนว่าคอมพิวเตอร์แต่ละเครื่องจะมีหมายเลข IP Address สองตัว สำหรับติดต่อกับโครงข่ายภายในและสำหรับติดต่อกับโครงข่ายภายนอก สำหรับ NAT-PT จะเป็นการแปลงระหว่าง IPv4 address กับ IPv6 address เพื่อใช้ในการติดต่อสื่อสารกันระหว่างโครงข่ายที่ใช้อินเตอร์เน็ตโพรโทคอลคนรุ่น ตัวอย่างเช่น คอมพิวเตอร์ทางซ้ายมือใช้หมายเลข 172.16.1.1 ในการติดต่อกับเครื่องอื่นๆ ในโครงข่าย IPv4 ด้วยกัน แต่ถ้าหากมันต้องการติดต่อกับคอมพิวเตอร์อีกเครื่องในโครงข่าย IPv6 มันจำเป็นต้องส่งแพ็กเก็ตข้อมูลผ่านเกตเวย์ NAT-PT เพื่อแปลงหมายเลขต้นทางจาก 172.16.1.1 ให้เป็นรูปแบบ ของ IPv6 address เช่น 2001:0420:1987:0:2E0:B0FF:FE6A:412C จะได้ติดต่อกับ IPv6 ได้ ตัวเกตเวย์ NAT-PT นี้จำเป็นต้องจำคู่หมายเลขนี้ไว้ เพื่อที่ว่าเมื่อได้รับแพ็กเก็ตตอบจากเครื่องในโครงข่าย IPv6 โดยมีปลายทางที่ 2001:0420:1987:0:2E0:B0FF:FE6A:412C จะได้รู้ว่าควรแปลงกลับเป็นหมายเลข 172.16.1.1

เนื่องจากแอปพลิเคชันบางชนิด เช่น DNS มีการบรรจุหมายเลข IP Address ในส่วนของ payload ด้วย ทำให้เกิดปัญหา เพราะว่าเกตเวย์ NAT-PT จะไม่สามารถแปลง IP Address นอกเหนือจากส่วนที่อยู่ใน IP เฮดเดอร์ได้ เพราะเกตเวย์ NAT-PT เป็นอุปกรณ์ที่ทำงานในระดับ Network layer จึงไม่มีความรู้ว่าแต่ละแพ็กเก็ตที่ผ่านเข้ามาเป็นของแอปพลิเคชันชนิดใด ดังนั้น จึงจำเป็นต้องมีอุปกรณ์อีกตัวที่ทำงานในระดับ Application layer สำหรับจัดการกับปัญหานี้ ซึ่งเรียกว่า Application Layer Getaway (ALG) โดยที่เกตเวย์ NAT-PT จะต้องคอยส่งแพ็กเก็ตต่อไปยัง ALG เพื่อตรวจสอบหาหมายเลข IP address ส่วนใน payload และแปลงให้เป็น IP address ใหม่ที่ถูกต้อง

<u>ความต้องการเบื้องต้น (ระดับ Network)</u>

- เราเตอร์หรือเกตเวย์ที่เป็น Dual stacks สำหรับ NAT-PT Gateway
- เกตเวย์สำหรับ ALG (สามารถใช้เกตเวย์ตัวเดียวกันกับ NAT-PT Gateway ได้)
- DNSv6 เพื่อแปลงจากชื่อให้เป็นหมายเลข IPv6 address

- หมายเลข IPv4 address และ IPv6 address อย่างละ 1 หมายเลข สำหรับ NAT-PT Gateway



รูปที่ 4.3 การทำงานของ NAT-PT

4.2 สรุปผลกระทบกับเทคโนโลยีปัจจุบัน

ในการเปลี่ยนแปลง IPv4 เป็น IPv6 ในปัจจุบัน ไม่ได้มีผลกระทบมากนัก เนื่องจากการเปลี่ยนแปลงจาก IPv4 เป็น IPv6 มีวิธีการชัดเจนดังที่ได้กล่าวมาแล้ว พร้อมทั้งมีขั้นตอนที่มีลักษณะค่อยเป็นค่อยไป รวมทั้งอุปกรณ์ที่ใช้งานในโครงข่ายส่วนใหญ่ได้รองรับการใช้งานอยู่แล้ว มีองค์กรหรือหน่วยงานดูแลและจัดสรร IPv6 แล้ว ซึ่งสามารถขอใช้บริการ เพื่อเตรียมความพร้อมในการเปลี่ยนแปลงได้ทันที จึงไม่ใช่เรื่องยากที่จะเปลี่ยนแปลงในปัจจุบัน อย่างไรก็ตาม จะพอสรุปผลกระทบกับ และปัจจัยที่จะสร้างผลกระทบกับเทคโนโลยีปัจจุบันได้ดังต่อไปนี้

1. การเลือกใช้เทคนิคการปรับเปลี่ยนที่เหมาะสม

การปรับเปลี่ยนโครงข่ายเพื่อให้ใช้งานกับโครงข่าย IPv6 ได้นั้น มีหลากหลายเทคนิค ซึ่งแต่ละเทคนิคสามารถใช้ควบคู่กันได้ การตัดสินใจเลือกที่จะใช้เทคนิคชนิดใดนั้น ขึ้นอยู่กับลักษณะของโครงข่ายและการเชื่อมต่อที่ต้องการเป็นสำคัญ ตัวอย่าง เช่น ถ้าผู้ใช้ต้องการติดต่อกับโครงข่าย IPv6 ในขณะที่ ISP ของตน ยังไม่เปิดให้บริการเชื่อมต่อแบบ IPv6 สิ่งที่ผู้ใช้สามารถทำได้ก็คือ การลงทะเบียนกับ Tunnel broker หรือ ผู้ที่ให้บริการ tunnel แบบอื่นและตั้งค่าให้ คอมพิวเตอร์ ของตนเป็น Dual stacks แต่ถ้าหากว่า ISP นั้นมีบริการเชื่อมต่อกับโครงข่าย IPv6 อยู่แล้ว ผู้ใช้เพียงแค่ติดตั้ง Dual stacks ที่คอมพิวเตอร์ก็พอ

ตามที่กล่าวมาแล้วทั้งหมด จะเห็นได้ชัดว่า การใช้งานโครงข่าย IPv6 จะเป็นในลักษณะใช้งานควบคู่ไปกับ IPv4 อย่างค่อยเป็นค่อยไป มากกว่าที่จะเป็นการเปลี่ยนแปลงในทันที อย่างไรก็ตาม หลังจากการปรับเปลี่ยนเสร็จสมบูรณ์ เมื่อโครงข่ายต้นทาง กลางทาง และปลายทาง เป็น IPv6 ทั้งหมด เราสามารถทำการสื่อสารโดยใช้โพรโทคอล IPv6 โดยตรง ซึ่งเราเรียกการสื่อสารลักษณะนี้ว่า Native IPv6 network

ตาราง 4.1 เปรียบเทียบเทคนิคการปรับเปลี่ยนจาก IPv4 สู่ IPv6

Name	Connectivity	Type	Location
Dual stacks 6to6 over6	4to4 over4,	Dual stacks	ในโฮสต์หรืออุปกรณ์โครงข่าย
Manual Configured Tunnel	6to6 over4	Tunnel	ระหว่างโฮสต์และอุกรณ์โครงข่าย
Tunnel broker	6to6 over4	Tunnel	ระหว่างโฮสต์และอุปกรณ์โครงข่าย
6to4 tunnel	6to6 over4	Tunnel	ระหว่างโฮสต์และอุปกรณ์โครงข่าย
NAT-PT	6to4, 4to6	Translator	ในอุปกรณ์โครงข่าย

2. อุปกรณ์และแอปพลิเคชันที่สนับสนุน IPv6

- **อุปกรณ์โครงข่าย (Network Device)**

อุปกรณ์หรือผลิตภัณฑ์ในท้องตลาดที่สนับสนุน การใช้งาน IPv6 ขณะนี้เริ่มมีจำนวนมากขึ้น ยกตัวอย่างเช่น อุปกรณ์ของบริษัท Cisco, Juniper, Nortel, Fujitsu, Hitachi และอื่นๆ ทั้งนี้หากอุปกรณ์โครงข่าย เช่น Router ที่ใช้งานอยู่ยังไม่สนับสนุนการใช้งาน IPv6 เราสามารถแก้ไขได้โดยการเปลี่ยน firmware หรือ ระบบปฏิบัติการของ Router นั้นๆ

- **การขอหมายเลข IPv6 address ในประเทศ**

ปัจจุบันมีหน่วยงานภาครัฐและผู้ให้บริการอินเตอร์เน็ตหลายแห่งได้รับจัดสรรชุดหมายเลข IPv6 address จาก 6Bone และ APNIC และได้นำชุดหมายเลขเหล่านั้น มาจัดสรรต่อให้แก่หน่วยงานอื่นที่ต้องการ ทดลองใช้และทดสอบการเชื่อมต่อบนโครงข่าย IPv6 เราสามารถลงทะเบียนเพื่อขอรับ IPv6 address ได้ จาก ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติที่ http://www.ipv6.nectec.or.th/ipv6_delegation.php และที่บริษัท กสท โทรคมนาคมที่ http://web.ipv6.cattelecom.com/addressallocation.html

4.3 สรุปผลกระทบกับเทคโนโลยีในอนาคต

การเปลี่ยนแปลงจากยุคของ IPv4 ไปสู่ IPv6 อย่างเต็มรูปแบบนั้นก่อให้เกิดบริการใหม่ๆทางการสื่อสารข้อมูลมากมายซึ่งไม่สามารถเกิดขึ้นได้ถ้าใช้ IPv4 ซึ่งมีจำนวนจำกัด รวมทั้งการอินทีเกรทอุปกรณ์เครื่องใช้ไฟฟ้าอื่นเข้ากับระบบโครงข่ายอินเตอร์เน็ต ซึ่งจะส่งผลทำให้เกิดอุตสาหกรรมต่างๆทางการสื่อสารอีกมากมายเหลือคณานับ ทั้งทางด้าน Hardware Software และบริการ นอกจากนี้

1. ทำให้เกิดอุปกรณ์ เครื่องใช้ไฟฟ้า ที่สามารถเชื่อมโยงเข้ากับโครงข่ายอินเตอร์เน็ต พร้อมทั้งสามารถสื่อสารข้อมูลได้ โดยมี IP address เป็นของตัวเอง

การที่อุปกรณ์และเครื่องใช้ไฟฟ้าสามารถมี IP เป็นของตัวเองได้จะทำให้ อุปกรณ์และเครื่องใช้ไฟฟ้าเหล่านั้นมีความสามารถเพิ่มขึ้นและทำให้ผู้ใช้งานเกิดความสะดวกสบายขึ้นอย่างมาก ตัวอย่างอุปกรณ์เครื่องใช้ไฟฟ้าที่กำลังจะมาพร้อม IPv6 เช่น Internet Refrigerator ทำเราสามารถสั่งงานตู้เย็นให้ละลายน้ำแข็ง ทำความเย็น เปิด ปิด ได้ทุกที่ทุกเวลา, IPTV HDTV over IP ทำให้การส่งข้อมูลของ TV ไม่จำเป็นต้องเป็น Broadcast อีกต่อไป เราสามารถระบุเครื่องรับได้ว่าเป็นเครื่องใดบ้างและสามารถดูช่องใดได้บ้าง, IP DVD Recorder ทำให้เราสามารถบันทึกรายการ TV ที่เราไม่สามารถชมได้ ด้วยการสั่งงานผ่าน IP จึงสามารถสั่งงานได้ทุกที่ทุกเวลา และอุปกรณ์ใหม่ๆ อีกมากมาย เพราะการมี IP เป็นของตัวเองเสมือนการมีชื่อเรียกอุปกรณ์ทำให้เราสามารถสั่งงานถูกต้องตามที่ต้องการ

2. เพิ่มความสามารถในการแจกจ่ายหมายเลข IP จริง ให้กับผู้ใช้ในอนาคต

การใช้งานอินเตอร์เน็ตจะแปรเปลี่ยนเป็นแบบ always-on คือพร้อมใช้และพร้อมบริการ โดยที่อุปกรณ์อีกหลายประเภท ไม่ใช่เฉพาะคอมพิวเตอร์ก็จะเชื่อมโยงเข้าสู่อินเตอร์เน็ตได้ ทั้งนี้ผู้ใช้จะเรียกร้อง IP Address จริง (Public IP Address) ที่อ้างอิงถึงได้จากทั่วโลก เพื่อการติดต่อในลักษณะ peer-to-peer และเพื่อความเชื่อมั่นในความปลอดภัย ซึ่งไม่สามารถทำได้ในระบบปัจจุบันที่อาศัย NAT (Network Address Translation) เพื่อแปลง IP Address ระหว่าง Private IP Address กับ IP Address จริง นอกจากนี้การใช้ IP Address จริง ยังมีประโยชน์ต่อการอ้างอิงการใช้งานโดยตรงถึงผู้ใช้ เช่น ระบบการคิดค่าเช่า โครงข่าย หรือค่าบริการเล่นเกมส์ต่างๆ

3. สามารถรองรับการขยายตัวของบริการ Broadband Internet ในอนาคต

โครงข่าย IPv6 จะช่วยรองรับการขยายตัวของบริการ Broadband Internet ได้เป็นอย่างดี เนื่องจากบริการ Broadband Internet มักจะหมายถึงการใช้งานอินเตอร์เน็ตในลักษณะ always-on connection จึงมีความต้องการหมายเลข IP Address จำนวนมาก ตามนโยบายของกระทรวง ICT ที่ต้องการขยายการให้บริการ Broadband Internet ภายในประเทศ อีกไม่น้อยกว่า 1,000,000 พอร์ท ทำให้ความต้องการหมายเลข IP ใหม่

เพิ่มขึ้นอีกประมาณ 6,000,000 หมายเลข ซึ่งประเทศไทยไม่สามารถจัดสรรจำนวน IP Address ดังกล่าวได้จากโพรโทคอล IPv4 เพียง 1,782,016 หมายเลข ซึ่งนับเป็นลำดับที่ 37 ของประเทศที่มีการใช้งานอินเตอร์เน็ต

4. เกิดเทคโนโลยี และบริการโทรศัพท์เคลื่อนที่ และ Mobile Internet ในอนาคต

โทรศัพท์เคลื่อนที่ในปัจจุบันไม่เพียงแต่ทำหน้าที่แลกเปลี่ยนข้อมูล เสียงพูดเท่านั้น ยังสามารถแลกเปลี่ยนข้อมูลที่เป็นสื่อประสมชนิดอื่นๆ เช่น ข้อความ รูปภาพ วีดิโอ ซึ่งการแลกเปลี่ยนข้อมูลเหล่านี้อาจเกิดขึ้นในรูปแบบของการรับ-ส่งอีเมล์ peer-to-peer หรือเปิดเว็บไซต์ ซึ่งต่างก็อาศัยเทคโนโลยี IP เข้ามาช่วย นั่นก็แปลว่า โทรศัพท์เคลื่อนที่ในปัจจุบันมีความต้องการใช้ IP Address แม้ว่าในปัจจุบันทางออกในการจัดสรร IP Address ให้แก่โทรศัพท์เคลื่อนที่คือการจัดสรร IP Address ชั่วคราวโดยใช้เทคโนโลยี NAT ในอนาคต หากโทรศัพท์เคลื่อนที่ได้วิวัฒนาการไปสู่ยุคที่ 3 มาตรฐานการใช้งาน 3GPP Release 5 กำหนดให้ ผู้ให้บริการโทรศัพท์เคลื่อนที่จัดสรร IP Address ถาวรให้กับโทรศัพท์เคลื่อนที่แต่ละเครื่อง หากต้องการจ่ายหมายเลข IP ให้กับโทรศัพท์เคลื่อนที่ในประเทศ ซึ่งปัจจุบันมีใช้งานอยู่ประมาณ 25 ล้านเครื่อง ย่อมเป็นไปไม่ได้ที่จะใช้หมายเลข IPv4 หากมีการจัดสรร IP Address ให้กับอุปกรณ์สื่อสารเคลื่อนที่ จะทำให้ปัญหาการขาดแคลนหมายเลข IP เกิดเร็วขึ้นในอีกปี

5. ความยุ่งยากและซับซ้อนในการเชื่อมต่อกับโครงข่ายต่างประเทศจะลดลงในอนาคต

หลายประเทศทั่วโลกได้ออกนโยบายเกี่ยวกับการปรับเปลี่ยนระบบโครงข่ายภายในประเทศเพื่อรองรับการใช้งาน IPv6 ตัวอย่างเช่น กระทรวงกลาโหมของสหรัฐอเมริกาได้กำหนดไว้ว่าภายในสิ้นปี พ.ศ. 2551 โครงข่ายคอมพิวเตอร์ทั้งหมดต้องสามารถใช้งาน IPv6 ได้ ประเทศไต้หวันมีนโยบายว่าโครงข่ายภายในประเทศต้องสนับสนุนการใช้งานทั้ง IPv4 และ IPv6 ภายในปี พ.ศ. 2551 และประเทศสาธารณเกาหลีจะเริ่มให้บริการ IPv6 เชิงพาณิชย์ ตั้งแต่ปี พ.ศ. 2548 และกำหนดนโยบายที่ปรับโครงข่ายทั้งประเทศให้เป็น Native IPv6 ภายในปี พ.ศ. 2554 ประเทศญี่ปุ่น มี ISP กว่า 50 รายสามารถให้บริการ IPv6 ส่วน ISP รายใหม่ทั้งหมดสามารถให้บริการ IPv6 ได้ตั้งแต่ต้น โครงข่ายงานวิจัย เช่น Internet 2 ทำงานอยู่บนโครงข่าย IPv6 ดังนั้น การเตรียมความพร้อมด้าน IPv6 ของประเทศไทยจะช่วยลดความยุ่งยากและซับซ้อนในการเชื่อมต่อกับโครงข่ายต่างประเทศในอนาคต

6. เพิ่ม Network Security ให้กับทุกเทคโนโลยีการสื่อสารที่จะเกิดในอนาคต

โครงข่าย IPv6 ทำให้ระบบโครงข่ายมีความปลอดภัยมากขึ้น โดยเฉพาะการติดต่อแบบ end-to-end อย่างแท้จริง สามารถทำให้ end-user สามารถ identify ระบบความปลอดภัยได้ด้วยตนเอง การตรวจสอบสามารถทำได้ง่ายเพราะไม่ผ่าน NAT การใช้งานแบบ IPv6 VPN จะทำให้มีความปลอดภัยและเสถียรขึ้น เนื่องจากไม่ผ่าน Nat ทำให้ผู้ให้บริการและผู้ใช้บริการมีความมั่นใจสูงขึ้น

7. เกิด Software และโปรแกรมที่ถูกพัฒนาขึ้นเพื่อรองรับ IPv6

เนื่องจากมีการบริการรูปแบบใหม่หลากหลายบนโครงข่าย IPv6 โดยเฉพาะทางด้าน Mobile Devices จึงจะมีการพัฒนา Software ขึ้นใหม่อย่างหลากหลายและมากมาย

8. จะเกิดความคับคั่งของข้อมูลในโครงข่ายอย่างมาก

เนื่องจากข้อมูลต่างๆซึ่งเคยอยู่บน Platform ที่ต่างกันจะถูกอินทิเกรตลงบนโครงข่าย Internet ทั้งหมด ไม่ว่าจะเป็น Mobile IP IPTV VoIP และข้อมูลอื่นๆ ดังนั้นผู้ให้บริการจำเป็นต้องลงทุนเพิ่มสมรรถนะ หรืออัตราข้อมูลที่โครงข่ายให้บริการได้ เนื่องจากจะมีข้อมูลจำนวนมหาศาลกว่ายุคของ IPv4 หลายเท่า ซึ่งจะถูกสื่อสารบนโครงข่าย

บทที่ 5
สรุปผลกระทบการใช้งาน IPv6 กับผู้ใช้งานอินเตอร์เน็ต ผู้ให้บริการอินเตอร์เน็ต หน่วยงานกำกับดูแล และผู้ผลิตอุปกรณ์และซอฟต์แวร์

จากที่ได้กล่าวมาพอสมควรในบทต่างๆที่แล้ว เนื่องจาก IP Address ในปัจจุบันมีจำนวนไม่เพียงพอกับปริมาณผู้ใช้งานอินเตอร์เน็ตที่มากขึ้น จึงต้องมีการเปลี่ยนแปลงจาก IPv4 เป็น IPv6 ซึ่งมีจำนวนมากกว่าหลายเท่า ซึ่งการเปลี่ยนแปลงนี้ทำให้เกิดผลกระทบกับหลายๆ ฝ่าย ทั้งผู้ใช้บริการ ผู้ให้บริการ หน่วยงานกำกับดูแล และผู้ผลิตอุปกรณ์และซอฟต์แวร์ แต่อย่างไรก็ตาม เราจำเป็นที่จะต้องเปลี่ยนแปลงอย่างแน่นอน ดังนั้นทุกฝ่าย จึงจำเป็นต้องเข้าใจการเปลี่ยนแปลงและดำเนินการเปลี่ยนแปลงด้วยกันทุกๆ ฝ่าย เพื่อให้เป็นไปตามแนวทางเดียวกัน

แต่จากบทที่ผ่านมาก็จะเห็นได้ว่า ข้อดีของ IPv6 มีมากมายและไม่ได้ยุ่งยากในการตั้งค่าสำหรับการใช้งานรวมถึงการที่จะต้องลงทุนเพิ่มเติมแต่อย่างใด ทำให้ไม่มีผลกระทบที่รุนแรงกับผู้ใช้บริการอินเตอร์เน็ต ผู้ใช้บริการอินเตอร์เน็ต หน่วยงานที่กำกับดูแล และผู้ผลิตอุปกรณ์และซอฟต์แวร์ แต่จะเห็นได้ว่ามีประโยชน์ที่ได้รับจากการเปลี่ยนแปลงจาก IPv4 เป็น IPv6 มากกว่าผลเสียอย่างชัดเจน ในบทนี้จะสรุปผลกระทบกับผู้ใช้บริการ ผู้ให้บริการ หน่วยงานกำกับดูแล และผู้ผลิตอุปกรณ์และซอฟต์แวร์

5.1 ผลกระทบกับผู้ใช้บริการ Internet

ในช่วง Transition จาก IPv4 เป็น IPv6 ผู้ใช้บริการจะมีผลกระทบเล็กน้อย คือ ผู้ใช้บริการ จำเป็นต้องมีความรู้เกี่ยวกับ IPv6 เบื้องต้นบ้าง ว่าผู้ให้บริการใช้การ Transition ประเภทใด และผู้ใช้บริการสามารถเข้าใช้งานโครงข่ายได้อย่างไร แต่ทางผู้ให้บริการจะมีการประกาศและอธิบายการใช้งานให้กับผู้ใช้บริการและคิดว่าถ้าทางผู้ใช้บริการที่ไม่มีความรู้เพียงพอ ทางผู้ให้บริการอาจจะจัดการติดตั้งให้ถึงบ้านผู้ใช้บริการแต่อาจจะมีค่าใช้จ่ายเล็กน้อย

แต่เมื่อโครงข่ายทั้งหมดเป็น IPv6 เรียบร้อยแล้ว จะทำให้ไม่มีผลกระทบกับผู้ใช้งานมากนัก เพียงแค่ติดตั้ง IPv6 เพิ่มขึ้น และการติดตั้ง IPv6 ไม่ได้มีขั้นตอนยุ่งยาก เนื่องจากระบบปฏิบัติการเกือบทั้งหมดได้สนับสนุนการทำงานของ IPv6 อยู่แล้ว เช่น Windows Xp, Windows 2000, Linux เพียงแค่ให้ผู้ใช้งานลงเพิ่มเติมเท่านั้นเอง ไม่จำเป็นตั้งอัพเกรดระบบปฏิบัติการใหม่ทั้งหมด ยิ่งไปกว่านั้นระบบปฏิบัติการใหม่ๆที่เกิดขึ้นได้สนับสนุนการทำงานของ IPv6 เรียบร้อยแล้ว เช่น Windows Vista ทำให้ผู้ใช้งานไม่มีผลกระทบใดๆเลยทั้งสิ้น ผู้ใช้งานอาจจะไม่รู้ด้วยซ้ำว่าขณะนี้ผู้ใช้งานได้ใช้งาน IPv6 เรียบร้อยแล้ว

5.2 ผลกระทบกับผู้ให้บริการ

1. ส่วนใหญ่อุปกรณ์ในโครงข่ายจะสามารถรองรับ IPv6 อยู่แล้ว เพียงแค่ตัว Function นั้นไม่ได้เปิดใช้งานเท่านั้นเอง จึงไม่จำเป็นต้องเสียค่าใช้จ่ายในเปลี่ยนตัวอุปกรณ์ ยกเว้นในกรณีที่อุปกรณ์ในโครงข่ายที่ให้บริการไม่รองรับ IPv6 ผู้ให้บริการจำเป็นต้องลงทุนเพิ่มเพื่อปรับปรุงเปลี่ยนแปลงอุปกรณ์นั้น แต่คาดว่ากรณีดังกล่าวจะเป็นเพียงส่วนน้อย
2. ถ้าอุปกรณ์ในโครงข่ายไม่รองรับt IPv6 ส่วนใหญ่จะสามารถอัพเกรดให้รองรับได้โดยทำการ Update ตัว Firmware ของอุปกรณ์ชิ้นนั้นให้รองรับ IPv6 ได้เท่านั้นก็เพียงพอ จึงไม่จำเป็นต้องเสียค่าใช้จ่ายในเปลี่ยนตัวอุปกรณ์
3. จำเป็นต้องเพิ่มความรู้บุคลากรในการ Configure หรือดูแลระบบ IPv6 เนื่องจากเป็นระบบใหม่ จึงมีบางส่วนที่ไม่เหมือน IPv4 ซึ่งในสถานการณ์ปัจจุบันยังขาดแคลนผู้เชี่ยวชาญเกี่ยวกับ IPv6 อีกจำนวนมาก
4. จำเป็นทำการ Promote ให้ทางลูกค้าได้รับรู้ถึงการเปลี่ยนจาก IPv4 มาเป็น IPv6 และอธิบายถึงข้อดีของ IPv6 และเหตุผลในการเปลี่ยนแปลง
5. ทำให้ผู้ให้บริการสามารถสร้างรายได้เพิ่มเติมได้จากบริการ Content ใหม่ๆ ที่จะมาพร้อมกับ IPv6 และความสามารถของ Application เพิ่มขึ้น เป็นช่องทางในการทำรายได้ให้กับผู้ประกอบการได้
6. ผู้ให้บริการจำเป็นต้องลงทุนเพิ่มสมรรถนะ หรืออัตราข้อมูลที่โครงข่ายให้บริการได้ เนื่องจากจะมีข้อมูลจำนวนมหาศาลกว่ายุคของ IPv4 หลายเท่า ซึ่งจะถูกสื่อสารบนโครงข่าย

5.3 ผลกระทบกับหน่วยงานกำกับดูแล

1. หน่วยงานกำกับดูแลจำเป็นต้องตระหนักว่าไม่สามารถหลีกเลี่ยงการพัฒนาจาก IPv4 ไปสู่ IPv6 ในอนาคตอันใกล้ได้
2. หน่วยงานกำกับดูแลต้องทราบว่ามีอำนาจหน้าที่ในระดับไหนกับการควบคุมดูแลการเปลี่ยนแปลงไปสู่เทคโนโลยี IPv6
3. หน่วยงานกำกับดูแลจำเป็นต้องมีความรู้พื้นฐานเป็นอย่างดีเกี่ยวกับ IPv6
4. เนื่องจากกระบวนการเปลี่ยนไปยัง IPv6 ได้เกิดขึ้นแล้วในหลายประเทศ รวมทั้งอุปกรณ์ที่รองรับ IPv6 ทั้ง Hardware และ Software ก็ได้มีจำหน่ายอย่างมากมายแล้วในปัจจุบัน หน่วยงานกำกับดูแลจำเป็นต้องสร้าง Roadmap เพื่อให้การเปลี่ยนแปลงไปสู่ IPv6 ของประเทศเป็นไปในทางเดียวกันและเป็นไปพร้อมกันของทั้งผู้ให้บริการและผู้ใช้บริการ ถ้าปล่อยไว้ให้ผู้ให้บริการแต่ละรายทำการเปลี่ยนแปลงหรือนำ IPv6 มาใช้เอง จะทำให้กระบวนการเปลี่ยนแปลงเป็น IPv6 เป็นไปอย่างสะเปะสะปะ ซึ่งอาจก่อให้เกิดความไม่เท่าเทียมกันระหว่างผู้ให้บริการ และรากฐานของระบบที่ไม่มั่นคงและไม่เป็นระเบียบในอนาคต

5. ต้องศึกษาขบวนการเปลี่ยนแปลง และ Roadmap พร้อมกับนโยบายของแต่ละประเทศ โดยเฉพาะประเทศผู้นำทางด้าน IPv6 อย่างประเทศญี่ปุ่น เพื่อสร้าง Roadmap ของการเปลี่ยนแปลงไปสู่ IPv6 ของประเทศไทยที่สอดคล้องกับการเปลี่ยนแปลงของประเทศอื่น
6. ต้องจัดให้มีการรับฟังความคิดเห็นจากผู้ให้บริการ ผู้ใช้บริการเพื่อนำไปจัดทำ Roadmap ที่เหมาะสมและเป็นกลางกับทุกฝ่าย และต้องเผยแพร่สู่สาธารณะเพื่อให้ทุกภาคส่วนนำไปปฏิบัติได้พร้อมเพรียงกัน
7. ต้องกำกับดูแลการเปลี่ยนแปลงไปสู่ IPv6 เป็นระยะ ว่าตรงไปตาม Roadmap ที่ได้วางไว้หรือไม่ พร้อมทั้ง อาจจัดตั้งหน่วยงาน หรือคณะกรรมการกำกับดูแลโดยเฉพาะ เพื่อบริหารงานให้บรรลุจุดประสงค์
8. IPv6 เป็นเทคโนโลยีที่จะสามารถสร้างมูลค่าทางเศรษฐกิจได้อย่างเหลือคณานับในอนาคตอันใกล้ เพียงแค่กำไรที่จะได้จากบริการ Mobile IP นั้นก็แทบจะไมสามารถคาดเดาถึงมูลค่าได้แล้ว ดังนั้น หน่วยงานกำกับดูแลจำเป็นต้องควบคุมการจัดสรร IP address ให้แต่ละผู้ให้บริการให้เป็นไปอย่างยุติธรรมและเท่าเทียมกัน IP address อาจมีมูลค่าเทียบได้เท่ากับคลื่นความถี่ซึ่งเป็นสมบัติสาธารณะของชาติ ดังนั้นการจัดสรร IP address อาจอยู่ในรูปของการให้สัมปทาน หรือการเช่า ทั้งนี้ต้องดูขอบเขตอำนาจว่า หน่วยงานกำกับดูแลมีอำนาจจัดสรร IP address หรือไม่ในทางกฎหมาย
9. หน่วยงานกำกับดูแลจำเป็นต้องสร้างความร่วมมือกับองค์กรต่างๆซึ่งเกี่ยวข้องกับ IPv6 เพื่อให้ความรู้ และสร้างความเข้าใจกับผู้ให้บริการ ผู้ใช้บริการ และสาธารณะถึงเทคโนโลยี IPv6 ความจำเป็น และประโยชน์ รวมถึงการโฆษณาประชาสัมพันธ์
10. ประชาสัมพันธ์องค์กร หรือหน่วยงานที่ให้บริการ IPv6
11. เพื่อส่งเสริมให้การเปลี่ยนแปลงไปสู่ IPv6 เป็นไปอย่างรวดเร็วและสร้างแรงจูงใจกับผู้ให้บริการซึ่งยังมิได้เริ่มให้บริการ IPv6 หน่วยงานกำกับดูแลอาจสร้างมาตรการส่งเสริมการใช้งาน IPv6 เช่นลดภาษีนำเข้าอุปกรณ์โทรคมนาคมที่รองรับ IPv6 ลดภาษีของผู้ให้บริการถ้าผู้ให้บริการนั้นสามารถให้บริการ IPv6 ได้
12. หน่วยงานกำกับดูแลต้องออกมาตรฐานเกี่ยวกับการใช้งาน Application ต่างๆเช่น VoIP Mobile IP และ RFID บน IPv6 เพื่อส่งเสริมการเปลี่ยนแปลงและการนำ IPv6 มาใช้งาน
13. หน่วยงานกำกับดูแลต้องออกมาตรฐานต่างๆเกี่ยวกับการสื่อสารข้อมูลต่างๆด้วย IPv6 หรือการใช้งาน รวมทั้งระดับของ Security ใน Application ที่นอกเหนือจากข้อที่แล้ว เนื่องจากดังที่ได้กล่าวมาแล้วว่า ในอนาคตอุปกรณ์เครื่องใช้ไฟฟ้าทั้งหลายจะสามารถสื่อสารข้อมูลโดยมี IPv6 address เป็นของตัวเอง

5.4 ผลกระทบกับผู้ผลิตอุปกรณ์และ Software

1. ทำให้เกิดอุตสาหกรรมผลิตอุปกรณ์ใหม่ๆรองรับเทคโนโลยี IPv6 อย่างมากมาย โดยเฉพาะอุปกรณ์ที่รองรับระบบ VoIP Mobile IP และ RFID
2. เกิดอุตสาหกรรมการผลิตอุปกรณ์ไฟฟ้าทั่วไปซึ่งอินทีเกรทเทคโนโลยี IP เข้าไปด้วย และสามารถสื่อสารข้อมูล หรือถูกควบคุมผ่านโครงข่าย Internet โดยมี IP address เป็นของตัวเอง
3. อุปกรณ์เครื่องใช้ไฟฟ้าทั้งหมด รวมทั้งเทคโนโลยีการสื่อสารทั้งหมดข้อมูลจะถูกสร้างขึ้นมาบน Platform เดียวกันคือ เทคโนโลยีของ IP
4. ทางด้านซอฟต์แวร์ที่มีอยู่เดิมนั้นอาจจะต้องมีการพัฒนาให้รองรับ IPv6 ได้ ด้วยการอัพเกรด หรือการติดตั้งใหม่ เพื่อให้ผู้ใช้บริการสามารถใช้งาน IPv6 ได้ และเกิดความเชื่อมั่นใน บริษัทซอฟต์แวร์ที่ใช้งานอยู่
5. ทางด้านซอฟต์แวร์ ที่จะเกิดขึ้นมาใหม่จะต้องสนับสนุนการทำงานของ IPv6 เรียบร้อยแล้ว ถ้าหากไม่ผลิตซอฟต์แวร์ที่สนับสนุนการทำงานของ IPv6 อาจจะแพ้คู่แข่งซึ่งมีความพร้อมกับ IPv6 มากกว่า
6. เกิดแรงจูงใจเพื่อสร้างสรรค์ Software บริการสื่อสารข้อมูลแบบใหม่ๆที่หลากหลาย รวมทั้งสามารถพัฒนาเป็นอุตสาหกรรม Software ได้
7. สามารถส่งออกซอฟต์แวร์ที่สนับสนุนการทำงานของ IPv6 ออกไปยังต่างประเทศได้

บทที่ 6
สรุปรายงานระหว่างทาง

ปัจจุบันการใช้เทคโนโลยีโครงข่ายอินเตอร์เน็ตได้รับความนิยมอย่างแพร่หลายทั่วโลกและการเติบโตของโครงข่ายอินเตอร์เน็ตเป็นไปอย่างรวดเร็ว ทำให้จำนวนหมายเลขอินเตอร์เน็ตโพรโทคอล (IP address) ที่มีอยู่ มีแนวโน้มจะหมดไปในอนาคตอันใกล้ อินเตอร์เน็ตโพรโทคอลรุ่นที่ 6 (Internet Protocol version 6; IPv6) จึงถูกพัฒนาขึ้นเพื่อแก้ปัญหาสำคัญดังกล่าวโดยมีการปรับปรุงโครงสร้างของตัวโพรโทคอลจากอินเตอร์เน็ตโพรโทคอลรุ่นที่ 4 (IPv4) ที่ใช้งานอยู่อย่างแพร่หลายในปัจจุบัน ให้มีจำนวน IP address มากยิ่งขึ้น เพื่อรองรับการขยายตัวของโครงข่ายอินเตอร์เน็ตในอนาคตได้อย่างพอเพียง นอกจากนี้ยังมีการปรับปรุงคุณลักษณะอื่นๆ อีกหลายประการ ทั้งในแง่ของประสิทธิภาพและความปลอดภัย เพื่อให้สามารถตอบสนองความต้องการในการใช้งานเทคโนโลยีโครงข่ายอินเตอร์เน็ตในปัจจุบันและอนาคต นอกจากนี้ Application หรือบริการหลายชนิดก็ต้องอาศัยจำนวน IP address อย่างมากมาย เช่น VoIP Mobile IP และ RFID การเกิดขึ้นของบริการดังกล่าวนั้นต้องอาศัย IPv6 ทั้งสิ้นแม้แต่อุปกรณ์เครื่องใช้ไฟฟ้าทั่วไปก็มีแนวโน้มที่จะต้องมี IP address เป็นของตัวเองในอนาคต

หลายประเทศเช่น ญี่ปุ่น จีน และเกาหลีใต้ ได้เริ่มนำ IPv6 มาใช้งานจริง รวมทั้งมีการวาง Roadmap การเปลี่ยนแปลงไปสู่ IPv6 อย่างเต็มรูปแบบ สำหรับประเทศไทยนั้นก็เริ่มมีการนำ IPv6 มาทดลองใช้ในหน่วยงานต่างๆ แล้ว นอกจากการนำ IPv6 มาใช้งานแล้วยังมีการจัดตั้งองค์กรความร่วมมือต่างๆ ที่ทำการส่งเสริม สนับสนุน ให้ความรู้ในเรื่องเกี่ยวกับ IPv6 อีกด้วย จะเห็นได้ว่า ยังไงก็ตามเทคโนโลยีจะต้องเปลี่ยนแปลงจาก IPv4 เป็น IPv6 อย่างแน่นอน การเปลี่ยนแปลงไปสู่ IPv6 อย่างเต็มรูปแบบนั้นย่อมมีผลกระทบเกิดขึ้นกับทั้งผู้ให้บริการ ผู้ใช้บริการ และหน่วยงานที่กำกับดูแล แม้ว่าผลกระทบที่เกิดขึ้นจะมีทั้งผลดีและผลเสีย โดยรวมจากการวิเคราะห์นั้นจะเห็นได้ว่ามีผลดีมากกว่าผลเสีย และจะก่อให้เกิดประโยชน์อย่างมากมาย ทั้งทางด้านอุตสาหกรรม Hardware และ Software รวมทั้งบริการทางการสื่อสารข้อมูลรูปแบบใหม่ที่ต้องอาศัย IP address จำนวนมากและเกิดการพัฒนาคุณภาพชีวิต และความสะดวกสบายในชีวิตประจำวันมากขึ้น

รายการอ้างอิง

1. William Stalling, “IPv6: The New Internet Protocol,” IEEE Communications Magazine, June 1996, pp. 96-108.
2. พนิตา พงษ์ไพบูลย์ ฉัตรชัย จันทร์อินทร์ อดิศักดิ์ บุษรานันท์ และ เฉลิมพล ชาญศรีภิญโญ “คุณพร้อมหรือยังสำหรับอินเทอร์เน็ตยุคหน้า: ตอนที่ 1 เตรียมความพร้อม” สาร NECTEC, พฤษภาคม-มิถุนายน, หน้า 6-16 (2548)
3. พนิตา พงษ์ไพบูลย์ ฉัตรชัย จันทร์อินทร์ อดิศักดิ์ บุษรานันท์ และ เฉลิมพล ชาญศรีภิญโญ “คุณพร้อมหรือยังสำหรับอินเทอร์เน็ตยุคหน้า: ตอนที่ 2 พร้อมลงมือ” สาร NECTEC, สิงหาคม, หน้า 48-57 (2548)
4. พนิตา พงษ์ไพบูลย์ ฉัตรชัย จันทร์อินทร์ อดิศักดิ์ บุษรานันท์ และ เฉลิมพล ชาญศรีภิญโญ “คุณพร้อมหรือยังสำหรับอินเทอร์เน็ตยุคหน้า: ตอนที่ 3 ความจำเป็นของ IPv6 กับการพัฒนาประเทศไทย” สาร NECTEC, พฤศจิกายน-ธันวาคม, หน้า 20-28 (2548)
5. http://www.sfc.wide.ad.jp/InternetCAR/
6. http://www.v6pc.jp/en/index.phtml
7. http://www.kame.net/
8. http://www.linux-ipv6.org/
9. http://www.freebit.com/english/index.html
10. http://v6fix.net
11. http://hdtv.nm.gist.ac.kr/
12. http://totoro.cs.nthu.edu.tw/
13. www.ipv6.org.tw
14. www.v6pc.jp
15. http://www.ipv6forum.org/
16. http://www.thailandipv6.net/
17. www.ipv6-taskforce.nl
18. www.pe.ipv6tf.org
19. www.corega.co.jp
20. www.4ukphones.com
21. www.ist-daidalos.org

22. www.linux-ipv6.org
23. www.sfc.wide.ad.jp
24. www.cav6tf.org
25. www.ipv6.nectec.or.th
26. www.apnic.net
27. http://web.ipv6.cattelecom.com/
28. http://ipv6.coe.psu.ac.th/news.php
29. http://iir.ngi.nectec.or.th
30. http://www.veritecinc.com/
31. http://rfidusa.com/
32. http://www.rfidjournal.com/
33. http://www.rfidproductnews.com/