พนิตา พงษ์ไพบูลย์
ฉัตรชัย จันทร์อินทร์
อดิศักดิ์ บุษรานันท์
เฉลิมพล ชาญศรีภิญโญ

คุณพร้อมหรือยัง สำหรับอินเทอร์เน็ตยุคหน้า

ตอนที่ 1 เตรียมความพร้อม

ปัจจุบันการใช้เทคโนโลยีเครือข่ายอินเทอร์เน็ตได้รับความนิยมอย่างแพร่หลายทั่วโลกและการเติบโตของเครือข่ายอินเทอร์เน็ตเป็นไปอย่างรวดเร็วทำให้จำนวนหมายเลขอินเทอร์เน็ตโพรโตคอล (IP address) ที่มีอยู่มีแนวโน้ม จะหมดไปในอนาคตอันใกล้อินเทอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol version 6; IPv6) จึงถูกพัฒนาขึ้นเพื่อแก้ปัญหาสำคัญดังกล่าว โดยมีการปรับปรุงโครงสร้างของตัวโพรโตคอลจากอินเทอร์เน็ตโพรโตคอลรุ่นที่ 4 (IPv4) ที่ใช้งานอยู่อย่างแพร่หลายในปัจจุบันให้มีจำนวน IP address มากยิ่งขึ้น เพื่อรองรับการขยายตัวของเครือข่ายอินเทอร์เน็ตในอนาคตได้อย่างพอเพียง นอกจากนี้ยังมีการปรับปรุงคุณลักษณะอื่นๆ อีกหลายประการ ทั้งในแง่ของประสิทธิภาพและความปลอดภัย เพื่อให้สามารถตอบสนองความต้องการในการใช้งานเทคโนโลยีเครือข่ายอินเทอร์เน็ต ในปัจจุบันและอนาคตหลายประเทศ ได้เริ่มนำอินเทอร์เน็ตโพรโตคอลรุ่นที่ 6 มาใช้งานจริง ในขณะที่ประเทศไทยยังมีความตื่นตัวกันค่อนข้างน้อยกับวิกฤตการณ์ การขาดแคลน IP address ดังกล่าวที่กำลังจะเกิดขึ้นในอนาคตซึ่งจะส่งผลกระทบโดยตรงต่ออัตราการขยายตัวของเครือข่ายในประเทศเป็นอย่างมาก บทความนี้ นำเสนอแนวทาง และวิธีการปรับเปลี่ยนระบบเครือข่ายคอมพิวเตอร์ที่ใช้อินเทอร์เน็ตโพรโตคอล รุ่นที่ 4 ในปัจจุบันให้เป็นอินเทอร์เน็ตโพรโตคอล รุ่นที่ 6 ในการเชื่อมโยงเข้าสู่เครือข่ายอินเทอร์เน็ตยุคหน้า เพื่อเป็นการเตรียมความพร้อมสำหรับการเปลี่ยนแปลงของเครือข่ายอินเทอร์เน็ตที่จะเกิดขึ้นในอนาคตอันใกล้ นอกจากนี้จะนำเสนอสถานะปัจจุบันของการเชื่อมต่อและการให้บริการเครือข่ายอินเทอร์เน็ตโพรโตคอลรุ่นที่ 6 ในประเทศไทย

1 อินเทอร์เน็ตโพรโตคอล

กลไกสำคัญในการทำงานของอินเทอร์เน็ต คือ อินเทอร์เน็ตโพรโตคอล (Internet Protocol) ซึ่งประกอบด้วยส่วนสำคัญคือ หมายเลขอินเทอร์เน็ตแอดเดรส หรือไอพีแอดเดรส (IP Address) ที่ใช้ในการอ้างอิงเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายต่างๆ บนอินเทอร์เน็ตทั่วโลกเปรียบเสมือนการใช้งานโทรศัพท์ในการติดต่อสื่อสารกัน จะต้องมีเลขหมายเบอร์โทรศัพท์เพื่อให้อ้างอิงผู้รับสายได้คอมพิวเตอร์ทุกเครื่องในอินเทอร์เน็ตก็ต้องมีหมายเลขไอพีแอดเดรสที่ไม่ซ้ำกับใคร ดังรูปที่ 1 การเชื่อมต่อเครือข่ายอินเทอร์เน็ตในปัจจุบันส่วนใหญ่อยู่บนพื้นฐานการทำงานของอินเทอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol version 4; IPv4) ซึ่งเป็นมาตรฐานในการสื่อสารบนเครือข่ายอินเทอร์เน็ตตั้งแต่ปี ค.ศ. 1981 ทั้งนี้การขยายตัวของเครือข่ายอินเทอร์เน็ตในช่วงที่ผ่านมามีอัตราการเติบโตอย่างรวดเร็ว นักวิจัยเริ่มพบว่าจำนวน หมายเลข IP address ของ IPv4 กำลังจะถูกใช้หมดไป ไม่เพียงพอกับการใช้งานอินเทอร์เน็ตในอนาคต และหากเกิดขึ้นก็หมายความว่าเราจะไม่สามารถเชื่อมต่อเครือข่ายเข้ากับระบบอินเทอร์เน็ตเพิ่มขึ้นได้อีก ดังนั้นคณะทำงาน IETF (The Internet Engineering Task Force) ซึ่งตระหนักถึงปัญหาสำคัญดังกล่าว จึงได้พัฒนาอินเทอร์เน็ตโพรโตคอลรุ่นใหม่ขึ้น คือ รุ่นที่หก (IPv6) เพื่อทดแทนอินเทอร์เน็ตโพรโตคอลรุ่นเดิม โดยมีวัตถุประสงค์เพื่อปรับปรุงโครงสร้างของตัวโพรโตคอล ให้รองรับหมายเลข IP address จำนวนมาก และเพื่อปรับปรุงคุณลักษณะอื่นๆ อีกหลายประการทั้งในแง่ของความปลอดภัย การรองรับแอปพลิเคชันใหม่ๆ ที่จะเกิดขึ้นในอนาคต และการเพิ่มประสิทธิภาพในการประมวลผลแพ็กเก็ตให้ดีขึ้น ทำให้สามารถตอบสนองต่อการขยายตัวและความต้องการใช้งานเทคโนโลยีบนเครือข่ายอินเทอร์เน็ตในอนาคตได้เป็นอย่างดี

รูปที่ 2 การคาดคะเนการขาดแคลนหมายเลข IPv4 Address

ความจำเป็นที่จะต้องนำอินเทอร์เน็ตโพรโตคอลรุ่นที่ 6 มาใช้เริ่มมีมากขึ้น ดังจะเห็นได้จากรูปที่ 2 ว่าหมายเลขอินเทอร์เน็ตของ IPv4 ที่มีอยู่ในปัจจุบันเริ่ม ตอนที่ 1 เตรียมความพร้อมไม่เพียงพอกับความต้องการ และมีการคาดคะเนว่าหมายเลข IPv4 address นั้นจะถูกจัดสรรหมดไปภายในปี ค.ศ. 2008 ดังนั้นเพื่อเป็นการเตรียมความพร้อมรับมือกับการเปลี่ยนแปลงของระบบเครือข่ายอินเทอร์เน็ตที่จะเกิดขึ้นในอนาคตอันใกล้ บทความนี้จะนำเสนอข้อมูลเบื้องต้นเกี่ยวกับอินเทอร์เน็ตโพรโตคอลรุ่นใหม่ รวมถึงวิธีการต่างๆ ที่ได้ถูกพัฒนาขึ้นสำหรับช่วยในการปรับเปลี่ยนระบบเครือขาย IPv4 ที่มีอยู่เดิมไปสู่อินเทอร์เน็ตยุคหน้าบทความนี้เป็นอันดับแรกของชุดบทความที่จะแนะนำผู้อ่านเข้าสู่โลกของอินเทอร์-เน็ตยุคหน้าทั้งในมุมมองของผู้ใช้งานและมุมมองของผู้ดูแลระบบเครือข่าย

รูปที่ 1 แสดงการส่งข้อมูลบนอินเทอร์เน็ต โดยใช้อินเทอร์เน็ตโพรโตคอลรุ่นที่ 4

2 ความรู้พื้นฐานเกี่ยวกับอินเทอร์เน็ตโพรโตคอลรุ่นที่ 6 (IPv6)

องค์ประกอบพื้นฐานของ IPv6 ที่แตกต่างจาก IPv4 ได้แก่ ความยาวของหมายเลข IP address และรูปแบบของแพ็กเก็ตเฮดเดอร์ นอกจากนั้น IPv6 ยังมีความสามารถพิเศษต่างๆ ที่เพิ่มขึ้นมา ซึ่งเราจะกล่าวถึงในช่วงนี้

2.1 IPv6 Address Format

ประโยชน์หลักของ IPv6 และเหตุผลสำคัญของการเริ่มใช้ IPv6 ได้แก่ จำนวน IP address ที่เพิ่มขึ้นอย่างมากจากIPv4 address ซึ่งมีขนาด 32 บิต ในขณะที่ IPv6 address มีขนาด 128 บิต ความแตกต่างของจำนวน IP address มีมากถึง 296 เท่า มีผู้กล่าวว่าจำนวน IP address ที่เพิ่มขึ้นอย่างมากมายมหาศาลนี้มากเพียงพอที่จะจัดสรร IP address ให้ทุกสิ่งทุกอย่าง แม้แต่เม็ดทรายทุกเม็ดบนโลกนี้ ดังรูปที่ 3

IPv4 Address (32 bits)	IPv6 Address (128 bits)
ddd.ddd.ddd.ddd	hhhh : hhhh : hhhh : hhhh : hhhh : hhhh : hhhh : hhhh
d = เลขฐานสิบ (0-9)	h = เลขฐานสิบหก (O-F)
203.185.132.102	3fee:085b:1f1f:0000:0000:00a9:1234

รูปที่ 3 เปรียบเทียบรูปแบบของ IPv6 และ IPv4 address

รูปที่ 3 แสดงรูปแบบของ IPv6 address เปรียบเทียบกับ IPv4 address ด้วยความยาวที่เพิ่มขึ้นของ IPv6 address ทำให้ไม่สะดวกที่จะใช้ตัวเลขฐานสิบในการอ้างอิงถึง IP address อีกต่อไป (IPv4 address ใช้ตัวเลขฐานสิบจำนวนสี่ชุดในการแสดงค่า 32 บิต เช่น 202.127.3.254) การอ้างอิง ถึง IPv6 address จะใช้เลขฐานสิบหกเป็นหลัก โดยจะเขียนในลักษณะ 8 กลุ่มตัวเลข คั่นด้วยเครื่องหมาย ":" แต่ละกลุ่มตัวเลขจะประกอบไปด้วยเลขฐานสิบหกจำนวน 4 ตัว (ตัวละ 4 บิต รวมเป็น16 บิต) นอกจากนี้ยังสามารถเขียนแบบย่อได้ โดยมีเงื่อนไขคือ

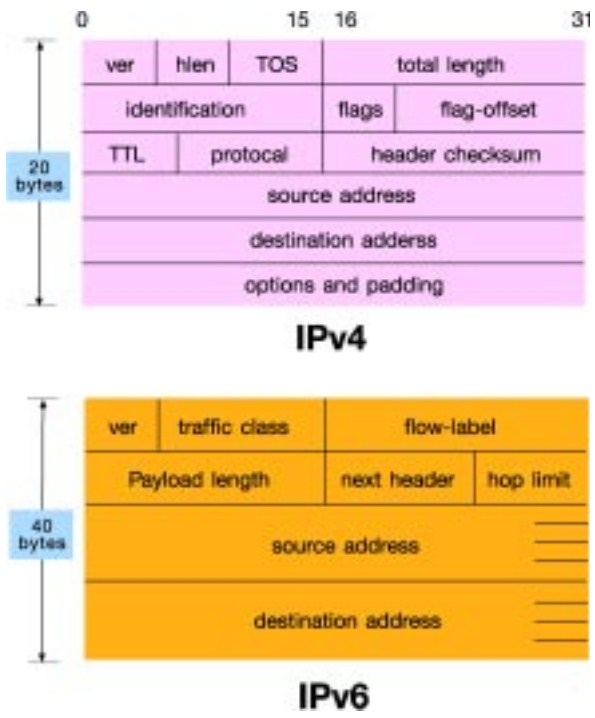
1. หากมีเลขศูนย์ด้านหน้าของกลุ่มใดสามารถจะละไว้ได้
2. หากกลุ่มใดเป็นเลขศูนย์ทั้ง 4 ตัว (0000) สามารถเขียนแทนด้วย "0"
3. หากกลุ่มใดกลุ่มหนึ่ง (หรือหลายกลุ่มที่ตำแหน่งติดกัน) เป็นเลขศูนย์ทั้งหมด สามารถจะละไว้ได้โดยใช้เครื่องหมาย "::" แต่จะสามารถทำลักษณะนี้ได้ในตำแหน่งเดียวเท่านั้น เพื่อไม่ให้เกิดความสับสน

   นอกจากนี้บางครั้ง IPv6 address อาจมี IPv4 address แทรกอยู่ ในกรณีนี้เราสามารถเขียนในลักษณะที่คงสภาพหมายเลข IPv4 อยู่ได้ จะเห็นได้ว่าเราสามารถเขียนหมายเลข IPv6 ได้หลายวิธี ดังตัวอย่างในรูปที่ 4

3fee:085b:1f1f:0000:0000:0000:00a9:1234	เขียนย่อได้เป็น	3fee:085b:1f1f:0:0:0:a9:123	หรือ 3fee:085b:1f1f::a9:1234
0000:0000:0000:0000:0000:0000:0000:0001	เขียนย่อได้เป็น	0:0:0:0:0:0:0:1	หรือ ::1
2001:0000:0000:34fe:0000:0000:00ff:0321	เขียนย่อได้เป็น	2001:0:0:0:34fe:0:0:ff:321	หรือ 2001::34fe:0:0:ff:321
0:0:0:0:0:0:192.168.1.1	เขียนย่อได้เป็น	::192.168.1.1	
0:0:0:0:0:0ffff192.168.1.1	เขียนย่อได้เป็น	::ffff:192.168.1.1	

รูปที่ 4 แสดงตัวอย่างการเขียน IPv6 address แบบย่อ

2.2 IPv6 Header Format



รูปที่ 5 การเปรียบเทียบเฮดเดอร์ระหว่าง IPv4 และ IPv6

เฮดเดอร์ (Header) ของข้อมูลแบบ IPv6 แพ็กเก็ต (packet) ถูกออกแบบมาให้มีขนาดคงที่ (40 ไบต์) และมีรูปแบบที่ง่ายที่สุดเท่าที่จะทำได้ โดยเฮดเดอร์ จะประกอบด้วยตำแหน่งต่างๆ ที่จำเป็นต้องใช้ในการประมวลผลแพ็กเก็ตที่เราเตอร์ (router) หรืออุปกรณ์เลือกเส้นทางทุกตัวเท่านั้น ส่วนตำแหน่งที่อาจจะถูกประมวลผลเฉพาะที่ต้นหรือปลายทางหรือที่เราเตอร์บางตัว จะถูกแยกออกมาไว้ที่ส่วนขยายของเฮดเดอร์ (Extended Header)

จากรูปที่ 5 จะเห็นว่าเฮดเดอร์ของ IPv6 ถึงแม้จะมีจำนวนไบต์มากกว่าเฮดเดอร์ของ IPv4 แต่ดูเรียบง่ายกว่าเฮดเดอร์ของ IPv4 มาก เนื่องจากข้อมูลหลายตำแหน่งถูกตัดออกไป โดยสามารถสรุปความแตกต่างของเฮดเดอร์ทั้งสองชนิดได้ดังนี้

ตำแหน่งข้อมูลที่ตัดออก

- Header length ถูกตัดออกไป เพราะเฮดเดอร์ของ IPv6 มีขนาดคงที่ (40 ไบต์) ทำให้ประสิทธิภาพโดยรวมของการประมวลผลแพ็กเก็ตดีขึ้น ไม่เสียเวลาในการคำนวณขนาดของเฮดเดอร์
- Identification, Flag, Flag Offset, Protocol, Options, และ Padding ถูกย้ายไปอยู่ใน ส่วนขยายของเฮดเดอร์ (Extended Header) เพราะถือว่าเป็นส่วนที่ไม่จำเป็นต้องประมวลผลในทุกๆ เราเตอร์
- Header Checksum ถูกตัดออกเพราะว่าซ้ำซ้อนกับฟังก์ชันของโพรโตคอลในชั้นที่อยู่สูงกว่า อีกทั้งเป็นการเพิ่มประสิทธิภาพของการประมวลผลด้วย เพราะ Checksum จะต้องมีการคำนวณใหม่ที่เราเตอร์เสมอ หากตัดออกก็จะลดภาระงานที่เราเตอร์ไปได้

ตำแหน่งข้อมูลที่ปรับเปลี่ยน

- Total Length เปลี่ยนมาเป็น Payload length เพื่อระบุขนาดของ Payload ในหน่วยไบต์ ดังนั้นขนาดของ Payload สูงสุดจะเป็น 65,535 ไบต์
- Time-To-Live (TTL) ของ IPv4 เปลี่ยนมาเป็น Hop Limit เพราะ TTL ระบุเวลาที่แพ็กเก็ตจะวนเวียนอยู่ในอินเทอร์เน็ต (หน่วยเป็นวินาที) โดยระบุว่าแต่ละเราเตอร์ต้องลด TTL ลงอย่างน้อย 1 วินาที เราเตอร์จึงลด TTL ครั้งละ 1 หน่วยเสมอแม้ว่าจะใช้เวลาประมวลผลแพ็กเก็ตน้อยกว่านั้น ทำให้ไม่ตรงกับความหมายของ TTL ดังนั้นจึงถูกเปลี่ยนเป็น Hop Limit เพื่อให้ตรงกับความหมายจริงๆ ซึ่งเหมาะสมและง่ายต่อการประมวลผล
- Protocol เปลี่ยนมาเป็น Next Header ซึ่งใช้เป็นตัวบอกว่า Extended Header ตัวถัดไปเป็นเฮดเดอร์ประเภทไหน เช่น ถ้าเป็น Extended Header ชนิด IPsec จะมีค่า Next Header = 51

- Type-of-Service (TOS) เปลี่ยนมาเป็น Traffic Class ซึ่งมีจำนวนบิตมากกว่า สามารถแบ่งกลุ่มและระดับความสำคัญของแต่ละแพ็กเก็ตละเอียดมากขึ้น เพื่อที่เราเตอร์จะจัดลำดับขั้นการส่งแพ็กเก็ตให้เหมาะสม

ตำแหน่งข้อมูลที่เพิ่ม

- Flow Label ใช้ระบุลักษณะการไหลเวียนของทราฟฟิกระหว่างต้นทางกับปลายทาง เนื่องจากในแอปพลิเคชันหนึ่ง สามารถมีทราฟฟิกหลายประเภท (เช่น ภาพ เสียง ตัวอักษร ฯลฯ) และทราฟฟิกแต่ละประเภทมีความต้องการที่แตกต่างกัน Flow Label จึงมีไว้เพื่อแยกประเภทของทราฟฟิกและเพื่อให้เราเตอร์รู้ว่าควรปฏิบัติต่อทราฟฟิกแต่ละประเภทแตกต่างกัน

2.3 ความสามารถพิเศษของ IPv6 ที่เหนือกว่า IPv4

นอกเหนือไปจากจำนวน IP Address ที่เพิ่มมากขึ้น IPv6 ยังได้รับการออกแบบมาให้เหมาะสมกับสภาพการใช้งานอินเทอร์เน็ตในปัจจุบัน ความสามารถพิเศษต่างๆ ที่ถูกบรรจุอยู่ใน IPv6 ได้แก่

- **Management** การตั้งค่าและปรับแต่งระบบเครือข่าย ในปัจจุบันมีความซับซ้อนมาก IPv6 จึงถูกออกแบบมาให้สนับสนุนการติดตั้งและปรับแต่งระบบแบบอัตโนมัติ (autoconfiguration) เพื่ออำนวยความสะดวกให้กับการจัดสรรปรับเปลี่ยน IP address (Address Renumbering) การเชื่อมต่อกับผู้ให้บริการหลายราย (Multihoming) และแม้แต่การจัดการเครือข่ายแบบ Plug-and-play
- **Broadcast/Multicast/Anycast** ใน IPv4 ได้มีการจัดสรร IP Address ส่วนหนึ่งเพื่อเป็น Broadcast address แต่ในความเป็นจริงแล้วการสื่อสารแบบ Broadcast เป็นสิ่งที่ไม่มีความจำเป็นและสิ้นเปลือง Bandwidth โดยเปล่าประโยชน์ Multicast เป็นการสื่อสารที่มีประสิทธิภาพมากกว่าและเริ่มเป็นที่นิยม IPv6 จึงถูกออกแบบมาให้รองรับ Multicast group address และตัด Broadcast address ออก นอกจากนี้ IPv6 ยังเพิ่มความสามารถในการสื่อสารแบบ Anycast โดยอนุญาตให้อุปกรณ์มากกว่า 1 ชิ้นได้รับการจัดสรร IP address เบอร์เดียวกัน ซึ่งหมายความว่าอุปกรณ์ชิ้นใดก็ได้สามารถตอบสนองต่อข้อมูลที่ส่งมาที่ Anycast address นั้นๆ
- **Security** เราเตอร์และอุปกรณ์เครือข่ายทุกตัวในเครือข่าย IPv6 ถูกกำหนดให้รองรับการใช้งาน IPSec นอกจากนี้ยังมีการกำหนด Security Payload สองประเภทคือ Authentication Payload และ Encrypted Security Payload เพื่อสนับสนุนการรับส่งข้อมูลที่มั่นคงปลอดภัย ภายใต้ Network Layer แทนที่จะพึ่ง Application Layer เหมือนในเครือข่าย IPv4
- **Mobile IP** IPv6 สนับสนุนการใช้งานอินเทอร์เน็ตแบบเคลื่อนที่เช่นเดียวกับ IPv4 แต่ว่าการใช้งาน Mobile IPv6 นั้นมีประสิทธิภาพมากกว่า Mobile IPv4 ตรงที่สามารถส่งข้อมูลผ่านเส้นทางที่สั้นที่สุดโดยไม่ต้องพึ่งอุปกรณ์ตัวกลางในการส่งต่อข้อมูล (Route Optimization) และสามารถใช้ IPSec ในการป้องกันการโจรกรรมแพ็กเก็ตกลางทาง
- **Virtual Private Network (VPN)** แต่เดิมในเครือข่าย IPv4 การให้บริการ VPN ทำได้โดยใช้ IPSec เพื่อเข้ารหัสข้อมูลใน Network Layer ทั้งหมด ซึ่งจะติดปัญหาหากเครือข่ายต้นทางหรือปลายทางมีการทำ Network Address Translation (NAT) เพราะการเข้ารหัสจะต้องสิ้นสุดก่อนถึงจุดหมายปลายทาง สำหรับเครือข่าย IPv6 ไม่มีปัญหาดังกล่าว เพราะไม่มีความจำเป็นต้องใช้ NAT อีกต่อไป นอกจากนี้ยังสามารถใช้ Extended Hearder ที่เรียกว่า Authentication Header และ Encapsulated Security Payload เพื่อรองรับการใช้งาน VPN แบบปลอดภัย
- **Quality-of-Service** IPv6 ถูกออกแบบมาให้สนับสนุนการรับประกันคุณภาพของบริการตั้งแต่เริ่ม โดยจะเห็นได้จากตำแหน่ง Flow Label และ Traffic Class ในเฮดเดอร์ ถึงแม้ว่าในเฮดเดอร์ของ IPv4 จะมีตำแหน่ง Type-of-Service แต่ไม่มีการใช้อย่าง

แพร่หลาย เนื่องจากไม่มีมาตรฐานในการกำหนดค่าและเราเตอร์บางตัวเท่านั้นที่สามารถประมวลผลตำแหน่ง ToS ได้ ที่ผ่านมา IPv4 มักปล่อยให้ Layer ข้างล่างจัดการเรื่อง QoS แทน เช่น ผ่านเทคโนโลยี MPLS หรือ SONET/SDH

- Maximum Transfer Unit (MTU)-MTU ขั้นต่ำในเครือข่าย IPv4 คือ 576 ไบต์ และถูกเพิ่มเป็น 1280 ไบต์ในเครือข่าย IPv6 การเพิ่มความยาวขั้นต่ำของ MTU นี้จะช่วยให้การส่งข้อมูลในเครือข่าย IPv6 มีประสิทธิภาพมากขึ้น โดยช่วยลดสัดส่วนของข้อมูลเฮดเดอร์ต่อข้อมูลทั้งหมด

3 การปรับเปลี่ยนระบบเครือข่ายจาก IPv4 สู่ IPv6

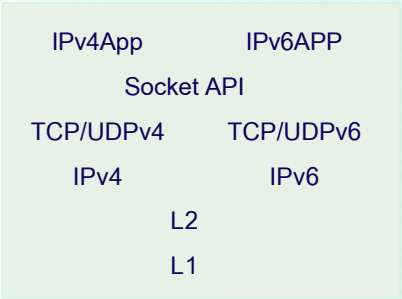
เทคนิคในการปรับเปลี่ยนเครือข่ายจาก IPv4 สู่ IPv6 (Transition technology) มีอยู่ 3 ชนิดหลักด้วยกัน คือการใช้งาน IPv4 และ IPv6 ควบคู่กัน หรือที่เรียกว่า Dual stacks, การทำอุโมงค์ (tunneling), และการแปลงข้อมูล (translation) ซึ่งการเลือกใช้แต่ละเทคนิคต้องดูที่ความเหมาะสม และลักษณะการใช้งานของเครือข่ายที่มีอยู่ในส่วนนี้เราจะแนะนำหลักเกณฑ์เบื้องต้นสำหรับแต่ละเทคนิค ส่วนขั้นตอนการติดตั้งอย่างละเอียดจะแนะนำในตอนต่อไป

3.1 Dual stacks

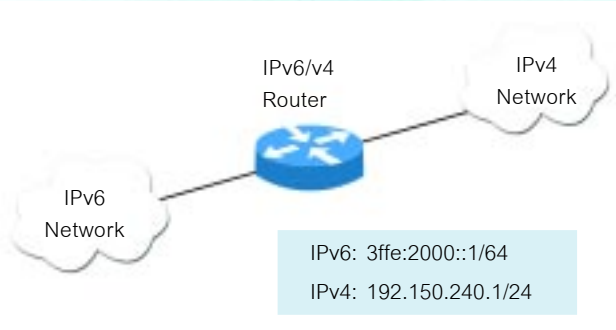
Dual stacks หมายถึงการใช้งาน IPv4 และ IPv6 stack ควบคู่กันไป ภายในอุปกรณ์ตัวเดียวกัน Dual stacks สามารถใช้ได้ทั้งที่ end host ที่เซิร์ฟเวอร์และที่อุปกรณ์เครือข่าย (network device) เช่น เราเตอร์

Dual stacks เป็นทางออกที่ง่ายที่สุดสำหรับเครือข่ายที่ต้องการเริ่มใช้งาน IPv6 และถูกใช้อย่างแพร่หลายมากที่สุดในปัจจุบัน Dual stacks เหมาะกับการติดต่อระหว่างสองโหนด (node) ที่ใช้อินเทอร์เน็ตโพรโตคอลเวอร์ชันเดียวกัน แต่ต้องผ่านเครือข่ายกลางทางที่ใช้ไอพีโพรโตคอลคนละเวอร์ชัน เช่น IPv4-IPv4 ผ่านเครือข่าย IPv6 หรือ IPv6-IPv6 ผ่านเครือข่าย IPv4 หรือในกรณีที่บางโหนดต้องการปรับเปลี่ยนไปใช้โพโตคอล IPv6 แต่ว่าเครือข่ายที่เชื่อมต่ออยู่ด้วยไม่สนับสนุน IPv6 โหนดดังกล่าว สามารถใช้ Dual stacks เพื่อรองรับทั้ง IPv4 และ IPv6

หลักการทำงานคือ IP stack ที่อยู่ภายในโหนดจะ แบ่งออกเป็น 2 Stacks ทำงานขนานกัน เช่น เมื่อโหนดได้รับ IPv6 packet โหนดจะเลือก IPv6 stack มาจัดการกับแพ็กเก็ต (โดยตรวจสอบProtocol version จากส่วนหัวของแพ็กเก็ต) ในขณะเดียวกันโหนดสามารถติดต่อกับเครือข่าย IPv4 (ผ่าน IPv4 stack) ได้เหมือนเดิมไม่ต้องเปลี่ยนแปลง โดยโหนดที่มี dual stack นี้จะต้องมี IP address สองหมายเลข คือ IPv4 address และ IPv6 address (ดังรูปที่ 6-7)



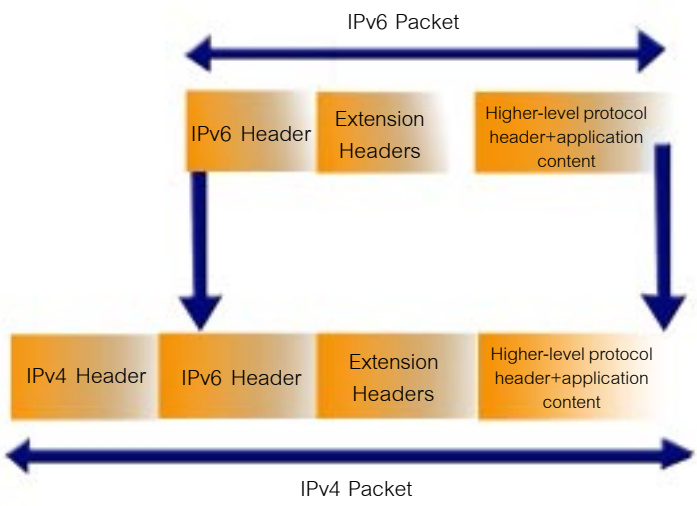
รูปที่ 6 โครงสร้างของ Dual IP stacks



รูปที่ 7 การใช้งาน Dual stacks ที่เราเตอร์

3.2 Tunnel

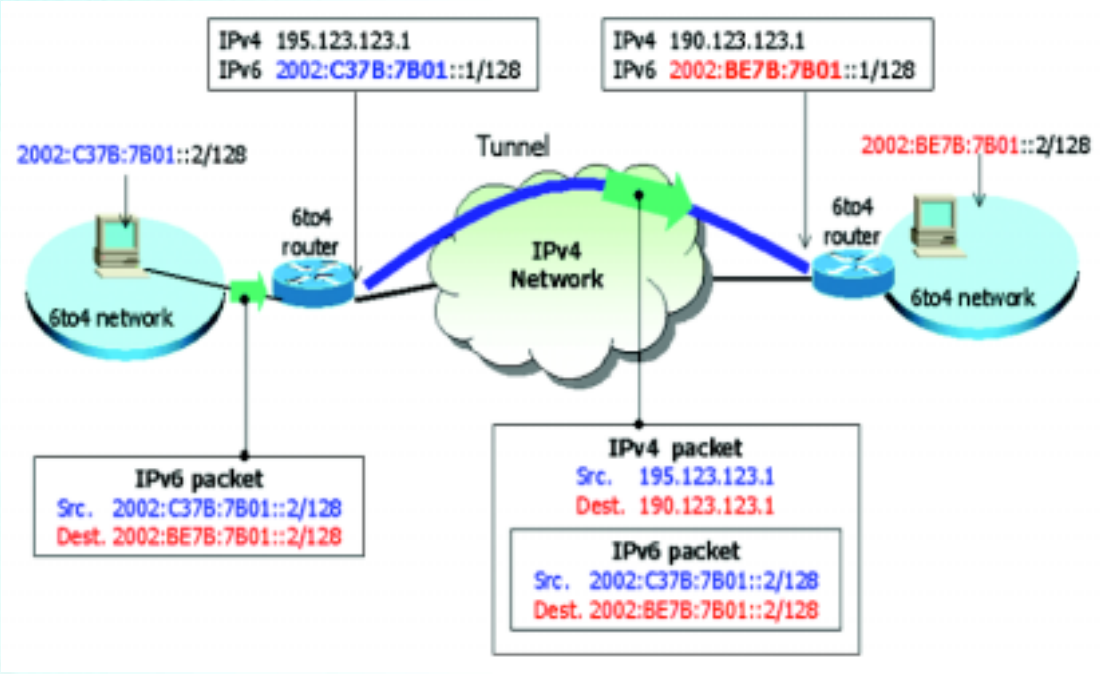
Tunnel หรือการทำอุโมงค์ โดยทั่วไปเป็นการ encapsulate แพ็กเก็ตข้อมูลที่ต้องการส่งไว้ในอีกแพ็กเก็ตหนึ่ง เนื่องจากแพ็กเก็ตที่อยู่ภายในไม่สามารถถูกส่งไปยังปลายทางได้ จึงต้องอาศัยการห่อหุ้มด้วยแพ็กเก็ตอื่น การทำอุโมงค์เพื่อใช้งาน IPv6 นั้นก็เช่นกัน ใช้เมื่อเครือข่ายเชื่อมต่ออยู่ด้วยไม่สนับสนุน IPv6 จึงจำเป็นต้องหุ้มแพ็กเก็ต IPv6 ไว้ภายใต้แพ็กเก็ต IPv4 อีกที ดังรูปที่ 8



รูปที่ 8 การทำ IPv6-in-IPv4 packet encapsulation

การทำ Tunnel สำหรับเครือข่าย IPv6 ต้องสร้างเส้นทางการติดต่อระหว่างเครื่องที่ใช้หมายเลข IPv6 ผ่านเครือข่ายที่ใช้หมายเลข IPv4 โดยเกตเวย์ (Gateway) ของเครือข่ายของเครื่องที่ใช้หมายเลข IPv6 จะทำหน้าที่ห่อหุ้มแพ็กเก็ต IPv6 ไว้ใน IPv4 ก่อนจะส่งไปในเครือข่ายอินเทอร์เน็ตที่สนับสนุนการใช้หมายเลข IPv4 เท่านั้น โดยระหว่างทางจะดูหมายเลขต้นทางและปลายทางที่อยู่ในส่วนหัวของแพ็กเก็ต IPv4 เท่านั้นจะไม่สนใจส่วนที่อยู่ภายในเมื่อส่งไปถึงปลายทางเกตเวย์จะถอดแพ็กเก็ต IPv4 ออกให้เหลือแต่แพ็กเก็ต IPv6 แล้วส่งไปยังเครื่องที่ใช้หมายเลข IPv6 ต่อไป

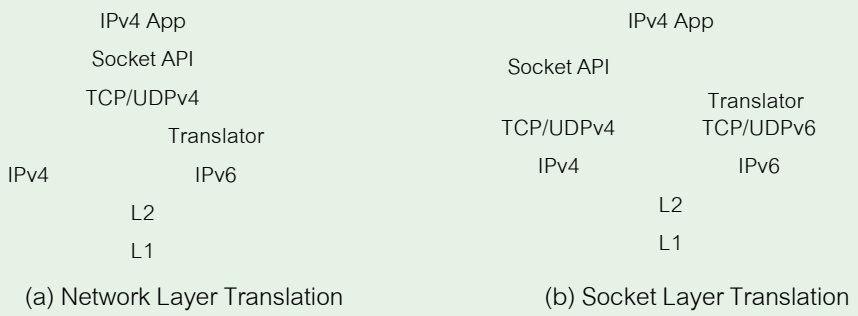
ข้อเสียของวิธีนี้คือ การ encapsulation ทำให้แพ็กเก็ต มีขนาดใหญ่ขึ้นเป็นผลให้เครือข่ายมี overhead สูงขึ้น นอกจากนี้ การทำ Tunnel จำเป็น ต้องใช้ Dual stacks ที่ตัวเกตเวย์ทั้งสองด้านของอุโมงค์



รูปที่ 9 การเชื่อมต่อเครือข่ายแบบอุโมงค์ IPv6-over-IPv4 Tunnel

3.3 Translation

เทคนิคการทำ Translation เป็นวิธีที่ใช้กับการสื่อสารข้ามเครือข่าย เช่น โหนดจากเครือข่าย IPv4 ต้องการคุยกับเซิร์ฟเวอร์ในเครือข่าย IPv6 หรือโหนดที่เป็น IPv6 ต้องการคุยกับเซิร์ฟเวอร์ที่เป็น IPv4 ซึ่งจะเป็นกรณีที่ต่างไปจากการใช้งาน Dual stacks และ Tunnel การทำ Translation พูดง่ายๆ ก็คือ การแปลงข้อมูลไปมาระหว่างข้อมูลในรูปแบบของ IPv4 และ IPv6 การแปลงข้อมูลนี้สามารถทำได้สองแบบ แบบแรกคือการแปลงที่ 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 อยู่ที่ทางออกที่มีการเชื่อมต่อระหว่างเครือข่าย IPv6 และ IPv4



รูปที่ 10 โครงสร้างของ Network Stacks เพื่อการแปลงข้อมูลระหว่าง IPv6 และ IPv4

ไม่ว่าจะทำการแปลงข้อมูลที่แบบไหน องค์ประกอบสำคัญที่จำเป็นคือส่วนที่ทำหน้าที่แปลงหมายเลข IP address หรือ Address translator ซึ่งการแปลงหมายเลขนี้สามารถทำได้โดยการจัดเก็บคู่หมายเลข IPv4 และ IPv6 address ทุกคู่ในเครือข่าย เราเรียกวิธีนี้ว่า Stateful address translation หรือจะทำการแปลงแบบอัตโนมัติ ที่เรียกว่า Stateless address translator ก็ได้

สรุป

ในปัจจุบันความตื่นตัวในการปรับเปลี่ยนระบบเครือข่ายจาก IPv4 เป็น IPv6 ได้เกิดขึ้นช้ากว่าที่คาดหมายกันไว้ สาเหตุสำคัญอาจเนื่องมาจากทัศนคติที่ว่า ตราบใดที่อินเทอร์เน็ตยังไม่ขาดแคลน IP address การใช้ IPv6 ก็ยังคงเป็นสิ่งฟุ่มเฟือยและยังไม่จำเป็นมากนัก บทความนี้ได้นำเสนอวิธีการต่างๆ ในปรับเปลี่ยนระบบเครือข่ายที่ใช้ IPv4 ให้สามารถสื่อสารกับเครือข่ายอินเทอร์เน็ตในอนาคตที่ใช้ IPv6 ได้ โดยใช้แบบที่ค่อยเป็นค่อยไปโดยไม่ต้องลงทุนเปลี่ยนแปลงระบบเครือข่ายใหม่ทั้งระบบในทันที การเลือกใช้แต่ละเทคนิคต้องดูที่ความเหมาะสม และลักษณะการใช้งานของเครือข่ายที่มีอยู่เพื่อให้เกิดผลกระทบต่อการใช้งานให้น้อยที่สุด ถึงแม้ว่าความจำเป็นในการปรับเปลี่ยนระบบเครือข่ายจาก IPv4 เป็น IPv6 จะไม่มีกำหนดเวลาที่แน่นอน ซึ่งต่างจากการปรับเปลี่ยนระบบคอมพิวเตอร์และโปรแกรมให้สามารถรองรับการใช้งานในช่วง ค.ศ. 2000 แต่เป็นที่ยอมรับกันโดยทั่วไปว่าสักวันหนึ่งอินเทอร์เน็ตจะต้องปรับเปลี่ยนไปใช้ IPv6 เพราะไม่ช้าก็เร็วปัญหาการขาดแคลน IP address จะต้องมาถึง และเมื่อถึงเวลานั้นผู้ที่มีความพร้อมมากกว่าจะเป็นผู้ได้เปรียบ นอกจากนั้น IPv6 ยังเป็นทางออกที่ถาวรทางเดียวในการแก้ปัญหานี้ ในตอนต่อไปเราจะกล่าวถึงรายละเอียดในการลงมือปรับเปลี่ยนเครือข่ายจาก IPv4 สู่ IPv6 ว่าต้องใช้อุปกรณ์ชนิดใด และมีขั้นตอนการปฏิบัติอย่างไรบ้าง หากท่านคิดว่าพร้อมแล้วที่จะก้าวเข้าสู่อินเทอร์เน็ตยุคหน้า โปรดติดตามตอนต่อไป

อะไร:

IPv6 คืออะไร

IPv6 คืออินเทอร์เน็ตโพรโตคอลรุ่นใหม่ที่ได้รับการพัฒนาขึ้นมาแทนที่อินเทอร์เน็ตโพรโตคอลรุ่นปัจจุบัน (IPv4) โดยมีวัตถุประสงค์หลักคือการปรับปรุงโครงสร้างอินเทอร์เน็ตโพรโตคอลให้รองรับหมายเลข IP address จำนวนมาก เพื่อให้ทันกับการเจริญเติบโตอย่างรวดเร็วของเครือข่ายอินเทอร์เน็ตในปัจจุบัน หมายเลข IP address ของ IPv6 มีความยาวถึง 128 บิต และรูปแบบโครงสร้างของ IPv6 packet header ก็มีความเรียบง่ายขึ้นกว่าเฮดเดอร์ของ IPv4

ทำไม:

ทำไมจึงต้องเริ่มใช้ IPv6

ประโยชน์หลักของ IPv6 และเป็นเหตุผลสำคัญของการเริ่มใช้ IPv6 ได้แก่ จำนวน IP address ที่เพิ่มขึ้นอย่างมากมายมหาศาลเมื่อเปรียบเทียบกับจำนวน IP address เดิมภายใต้ IPv4 IPv4 address มี 32 บิต ในขณะที่ IPv6 address มี 128 บิต ความแตกต่างของจำนวน IP address มีมากถึง 2^{96} เท่า

ความสำคัญของการมี IP address ที่ไม่ซ้ำกันและสามารถเห็นกันได้ทั่วโลก จะช่วยผลักดันการพัฒนาแอปพลิเคชันแบบ peer-to-peer ที่ต้องการ IP address จริงเป็นจำนวนมาก เช่น การทำ file sharing, instant messaging, และ online gaming แอปพลิเคชันเหล่านี้มีข้อจำกัดภายใต้ IPv4 address เนื่องจากผู้ใช้บางส่วนที่ได้รับจัดสรร IP address ผ่าน NAT (Network Address Translation) ไม่มี IP address จริง จึงไม่สามารถใช้แอปพลิเคชันเหล่านี้ได้

สำหรับองค์กรหรือบริษัทห้างร้านต่างๆ การมี IP address จริงอาจไม่ใช่ประเด็นสำคัญ อย่างไรก็ตามหน่วยงานเหล่านี้ ควรมีความเข้าใจถึงข้อจำกัดของการใช้ NAT นั่นก็คือ การใช้ IP address ปลอม อาจทำให้เกิดความยุ่งยากในอนาคต หากต้องมีการรวมเครือข่ายสองเครือข่ายที่ใช้ IP address ปลอมทั้งคู่ อีกทั้งการใช้ IP address ปลอม เป็นการปิดโอกาสที่จะใช้แอปพลิเคชันหรือบริการแบบ peer-to-peer เช่น IPsec ในอนาคต

เมื่อไหร่:

เมื่อไหร่เราจะต้องเริ่มใช้ IPv6

ความจริงแล้วส่วนประกอบหลักๆ ของโพรโตคอล IPv6 ได้ถูกกำหนดขึ้นเรียบร้อยและออกเป็น RFC (Request For Comments) อย่างสมบูรณ์ตั้งแต่ปี ค.ศ. 1998 แล้ว ยังคงเหลือในส่วนความสามารถ และคุณลักษณะปลีกย่อย เช่น การจัดสรรชุดหมายเลข IPv6 การทำ multi-homing หรือการทำ network management ที่ยังต้องรอการกำหนดมาตรฐาน แต่ในส่วนนี้ไม่น่าจะทำให้เกิดการเปลี่ยนแปลงในฮาร์ดแวร์หรือซอฟต์แวร์มากนัก

จะว่าไปแล้ว IPv6 ถูกเริ่มใช้มาเป็นเวลาหลายปีแล้ว เพียงแต่ไม่ได้ใช้กันอย่างแพร่หลายในต่างประเทศ เช่น เกาหลี และญี่ปุ่น ได้มีการใช้ IPv6 ในเครือข่าย ISP หลายแห่งในประเทศไทยยังไม่มีการใช้ IPv6 ในเชิงพาณิชย์ มีแต่ในเครือข่ายทดสอบของหน่วยงานวิจัยและมหาวิทยาลัยต่างๆ

หากจะถามว่าเมื่อไหร่จึงจะต้องเริ่มใช้ IPv6 คำตอบนั้นขึ้นอยู่กับความจำเป็นในด้านต่างๆ ของ

เมื่อไหร่:

ผู้ใช้และผู้ให้บริการเอง ความจำเป็นประการแรกคือการขาดแคลนหมายเลข IP address สิ่งนี้น่าจะเป็นองค์ประกอบสำคัญสำหรับประเทศในเอเชียเช่น เกาหลี และญี่ปุ่น ซึ่งมีจำนวนผู้ใช้อินเทอร์เน็ตสูงกว่าหมายเลข IPv4 address ที่ได้รับจัดสรรมาก สำหรับประเทศในทวีปอเมริกาเหนือ ความจำเป็นด้านนี้ยังไม่สูงมาก เนื่องจากยังมีหมายเลข IPv4 address เหลืออยู่อีกเป็นจำนวนมาก ความจำเป็นประการที่สอง ได้แก่ ความต้องการบริการหรือแอปพลิเคชันชนิดใหม่ที่ต้องใช้หมายเลข IPv6 address ตัวอย่างเช่น การให้บริการโทรศัพท์เคลื่อนที่ยุคที่ 3 (Third Generation Mobile Phone) หรือการใช้แอปพลิเคชันแบบ peer-to-peer อย่างไรก็ตาม ในส่วนของผู้ให้บริการ การรอจนกระทั่งความจำเป็นดังกล่าวมาถึง โดยไม่ได้มีการวางแผนการปรับเปลี่ยนเครือข่ายล่วงหน้า อาจทำให้สิ้นเปลืองค่าใช้จ่ายและเสียโอกาสการแข่งขันทางธุรกิจได้

อย่างไร: เราควรนำ IPv6 มาใช้อย่างไร

อย่างไร:

การนำ IPv6 มาใช้ ควรจะเป็นไปอย่างค่อยเป็นค่อยไป เนื่องจากการปรับเปลี่ยนอินเทอร์เน็ตโพรโตคอล จะส่งผลกระทบต่อเครือข่ายทั่วโลกที่เชื่อมต่อกันอยู่ ดังนั้นการปรับเปลี่ยนไปสู่เครือข่าย IPv6 ล้วนอาจใช้ระยะเวลาเป็นปี เพราะเหตุนี้ ทาง IETF จึงเสนอทางออกเพื่อช่วยในการทำงานร่วมกันระหว่าง IPv4 และ IPv6 ในระหว่างที่เครือข่ายบางแห่งเริ่มมีการปรับเปลี่ยนในช่วงแรก การใช้งาน IPv6 อาจอยู่ในวงแคบ ดังนั้นเราต้องการเทคนิคเพื่อเชื่อมต่อเครือข่ายที่เป็น IPv6 เข้ากับเครือข่าย IPv4 หรือเครือข่าย IPv6 อื่น เทคนิคการทำงานร่วมกันระหว่าง IPv4 และ IPv6 แบ่งออกเป็น 3 ประเภทด้วยกันคือ

1. การทำ dual stack-เป็นวิธีพื้นฐานที่สุด ทำงานโดยใช้ IP stack สองอันคือ IPv4 stack และ IPv6 stack ทำงานควบคู่กัน เมื่อใดที่แอปพลิเคชันที่ใช้เป็น IPv4 ข้อมูลแพ็กเก็ตก็จะถูกส่งออกผ่านทาง IPv4 stack เมื่อใดที่แอปพลิเคชันที่ใช้เป็น IPv6 ข้อมูลแพ็กเก็ตก็จะถูกส่งออกผ่านทาง IPv6 stack การทำ dual stack เป็นทางออกที่ง่ายที่สุดแต่ไม่ใช่ long term solution เนื่องจากยังจำเป็นต้องใช้ IPv4 address ที่โฮสต์หรือเราเตอร์ที่ใช้ dual stack นั้น

2. การทำ tunneling-เป็นอีกวิธีที่ใช้กันแพร่หลายเพราะเหมาะสมกับการสื่อสารระหว่างเครือข่าย IPv6 ผ่านเครือข่าย IPv4 การส่งข้อมูลทำได้โดยการ encapsulate IPv6 packet ภายใน IPv4 packet ที่ tunneling gateway ก่อนออกไปยังเครือข่าย IPv4 ที่ปลายทาง ก่อนเข้าไปสู่เครือข่าย IPv6 ก็จะต้องผ่าน tunneling gateway อีกตัวซึ่งทำหน้าที่ decapsulate IPv6 packet และส่งต่อไปยังจุดหมายปลายทาง จะเห็นได้ว่าการทำ tunneling นี้จะใช้ไม่ได้สำหรับการสื่อสารโดยตรงระหว่างเครื่องในเครือข่าย IPv6 และเครื่องในเครือข่าย IPv4

3. การทำ translation-การทำ translation จะช่วยในการสื่อสารระหว่างเครือข่าย IPv6 และ IPv4 เทคนิคการทำ translation มีสองแบบ แบบแรกคือการแปลที่ end host โดยเพิ่ม translator function เข้าไปใน protocol stack โดยอาจอยู่ที่ network layer, TCP layer, หรือ socket layer ก็ได้ แบบที่สองคือการแปลที่ network device โดยจะต้องใช้ gateway ทำหน้าที่เป็น IPv6-IPv4 และ IPv4-IPv6 translator อยู่ที่ทางออกที่มีการเชื่อมต่อระหว่างเครือข่าย IPv6 และ IPv4

ทั้งนี้หลังจากการปรับเปลี่ยนเสร็จสมบูรณ์ เมื่อเครือข่ายต้นทาง กลางทาง และปลายทาง เป็น IPv6 ทั้งหมด เราสามารถทำการสื่อสารโดยใช้โพรโตคอล IPv6 โดยตรง ซึ่งเราเรียกการสื่อสารลักษณะนี้ว่า native IPv6 network

IPv6 จะถูกเริ่มใช้ที่ไหนก่อน

ที่ไหน:

ประเทศในทวีปเอเชีย และยุโรป มีความตื่นตัวในการปรับเปลี่ยนเครือข่ายมากกว่าประเทศในทวีปอเมริกาเหนือ เนื่องมาจากปัญหาการขาดแคลน IPv4 address บริษัทผู้นำทางด้านเทคโนโลยี IPv6 ล้วนตั้งอยู่ในภูมิภาคนี้ รัฐบาลประเทศญี่ปุ่นและสาธารณรัฐเกาหลี ต่างให้การสนับสนุนและผลักดันภาคเอกชนให้หันมาให้บริการ IPv6 ในเชิงพาณิชย์มากขึ้น อีกทั้งประเทศใหญ่ๆ อย่างเช่น จีน ก็คาดว่าจะเริ่มหันมาเอาจริงเอาจังในด้านนี้ ด้วยจำนวนประชากรและสถานะทางเศรษฐกิจที่บังคับนอกจากปัจจัยทางภูมิศาสตร์แล้ว บริการทางเครือข่ายที่จำเป็นต้องใช้ IPv6 อย่างเช่นบริการโทรศัพท์เคลื่อนที่ยุคที่ 3 ก็อาจเป็นจุดแรกของการเริ่มนำ IPv6 มาใช้ หรือการพัฒนาเครือข่ายภายในบ้านสำหรับติดต่อสื่อสารระหว่างอุปกรณ์เครื่องใช้ไฟฟ้าต่างๆ ก็อาจเป็นแรงผลักดันสำคัญสำหรับการนำ IPv6 มาใช้ การสำรวจพบว่าบริษัทผู้ผลิตเครื่องใช้ไฟฟ้าต่างให้ความสนใจที่จะผนวกหมายเลข IPv6 address เข้ากับอุปกรณ์ไฟฟ้าของตน

เท่าไหร่:

การลงทุนปรับเปลี่ยนเครือข่ายไปสู่เครือข่าย IPv6 มีค่าใช้จ่ายเท่าไร

การปรับเปลี่ยนเครือข่ายไปสู่เครือข่าย IPv6 ไม่จำเป็นต้องลงทุนสูง ผู้ผลิตอุปกรณ์ฮาร์ดแวร์ เช่น เราเตอร์ และสวิตช์ ในปัจจุบัน รองรับเทคโนโลยี IPv6 อยู่แล้ว เพียงแต่ผู้ใช้อาจยังไม่ได้เลือกใช้ option นี้ สำหรับอุปกรณ์รุ่นเก่าที่อาจไม่ได้รองรับเทคโนโลยี IPv6 ตั้งแต่แรกนั้น ผู้ใช้สามารถ upgrade firmware หรือ software ระบบได้ไม่ยาก ดังนั้นการปรับเปลี่ยนเครือข่ายไปสู่เครือข่าย IPv6 จึงไม่ได้หมายความว่าจะต้องกำจัดอุปกรณ์ เก่าทิ้งและซื้ออุปกรณ์ใหม่หมดอย่างไรก็ตาม การลงทุนที่สำคัญและหลีกเลี่ยงไม่ได้ เห็นจะเป็นการลงทุน พัฒนาทรัพยากรบุคคลให้มีความรู้ความชำนาญในการดูแลและจัดการระบบเครือข่าย IPv6 แต่ในท้ายที่สุดแล้ว การลงทุนเหล่านี้จะช่วยประหยัดค่าใช้จ่ายในระยะยาว เนื่องจาก IPv6 จะช่วยลดการใช้แรงงานคน ในการบริหารจัดการเครือข่าย ช่วยลดความผิดพลาดที่อาจเกิดขึ้น และยังช่วยเพิ่มรายได้จากการให้บริการชนิดใหม่ๆ เช่น QoS IPSec และ multicast บนเครือข่ายได้อีกด้วย

เอกสารอ้างอิง

1. Robert Elz, “Note on IPv6 Fundamental,” Handbook of IPv6 Workshop, 2004.
2. S. Hagen, IPv6 essentials, O’Reilly, July 2002.
3. D. Waddington and F. Chang, “Realizing the Transition to IPv6,” IEEE Communications Magazine, June 2002.
4. B. Carpenter and K. Moore, “Connection of IPv6 Domains via IPv4 Clouds,” RFC 3056, February 2001.