

คุณพร้อมหรือยัง สำหรับอินเทอร์เน็ตยุคหน้า ?

ตอนที่ 2 พร้อมลงมือ

กลับมาพบกันอีกแล้วในตอนที่สองของชุดบทความที่จะนำท่านเข้าสู่โลกของอินเทอร์เน็ตยุคหน้า ในตอนที่แล้ว (TechTrends: IT ฉบับที่ 64 เดือนมิถุนายน - กันยายน 2548) เราได้แนะนำท่านผู้อ่านเกี่ยวกับพื้นฐานของอินเทอร์เน็ตยุคหน้าว่าเป็นมาตรฐานของอินเทอร์เน็ตโพรโตคอลรุ่นใหม่ (Internet Protocol version 6; IPv6) ที่ถูกพัฒนาขึ้นมาเพื่อแก้ปัญหาความไม่เพียงพอของจำนวน IP address ในอินเทอร์เน็ตโพรโตคอลรุ่นปัจจุบัน (IPv4) โดยความสามารถหลักของ IPv6 คือการรองรับหมายเลข IP address ได้ถึง 2^{128} หมายเลข ซึ่งมากกว่าจำนวนหมายเลข IP address ในปัจจุบันถึง 2^{96} เท่า (IPv4 สามารถรองรับ IP address ได้เพียง 2^{32} หมายเลข) นอกจากนี้ IPv6 ยังมีคุณสมบัติพิเศษด้านอื่นๆ เช่น การสนับสนุนการติดตั้งระบบอัตโนมัติ การใช้งานอินเทอร์เน็ตแบบเคลื่อนที่ การรับประกันคุณภาพของบริการ ฯลฯ ดังที่ได้แนะนำไปในตอนที่แล้ว

ในฉบับนี้เราจะกล่าวถึงรายละเอียดเกี่ยวกับเทคนิคการปรับเปลี่ยนเครือข่ายในปัจจุบันให้เป็นเครือข่ายอินเทอร์เน็ตยุคหน้า เราจะแนะนำอุปกรณ์ที่จำเป็น และขั้นตอนการติดตั้งอุปกรณ์เหล่านี้ทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์ส่วนบุคคล (Desktop) สำหรับผู้ที่พร้อมที่จะทดลองใช้เครือข่าย IPv6 และกำลังสงสัยว่าจะต้องเริ่มอย่างไร บทความนี้จะช่วยท่านเลือกวิธีที่เหมาะสมในการเชื่อมต่อกับเครือข่าย IPv6 และรับรองว่าท่านจะได้สัมผัสกับโลกของอินเทอร์เน็ตยุคหน้าภายในอีกไม่กี่อึดใจข้างหน้า



การปรับเปลี่ยนระบบเครือข่าย จาก IPv4 สู่ IPv6



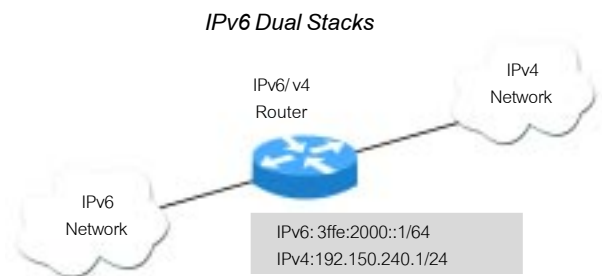
การปรับเปลี่ยนเครือข่ายจาก IPv4 สู่ IPv6 นั้นสามารถทำได้ทั้งสองระดับ ระดับแรกคือการปรับเปลี่ยนที่เครือข่าย เช่นการปรับเปลี่ยนที่อุปกรณ์เราเตอร์ หรือเครื่องเซิร์ฟเวอร์ วิธีนี้เหมาะสำหรับผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider; ISP) หรือผู้ดูแล เครือข่าย (Network operator) ที่ต้องการให้บริการ IPv6 บนเครือข่ายที่ตนดูแลอยู่ ระดับที่สองคือการปรับเปลี่ยนในส่วนของผู้ใช้ นั่นคือการเปลี่ยนแปลงที่คอมพิวเตอร์ส่วนบุคคล (Desktop, end host) วิธีนี้เหมาะสำหรับผู้ที่ต้องการทดลองใช้ IPv6 แต่เครือข่าย ISP ที่ใช้บริการอยู่ยังไม่พร้อมที่จะให้บริการ IPv6 นอกจากนี้ เราสามารถจำแนก วิธีการปรับเปลี่ยนเครือข่าย ตามเทคนิคที่ใช้ ซึ่งในปัจจุบันมีอยู่ 3 เทคนิคหลักด้วยกัน (ตามที่แนะนำไปในตอนที่แล้ว) หนึ่งคือ การใช้งาน IPv4 และ IPv6 ควบคู่กัน หรือที่เรียกว่า Dual stacks สองคือเทคนิคการทำอุโมงค์ (tunnel) เพื่อให้ข้อมูลในรูปแบบของ IPv6 สามารถส่งออกไปบนเครือข่าย IPv4 ได้ และสามารถคือเทคนิคการแปลงข้อมูล (translation) ระหว่างแพ็กเก็ต IPv6 และ IPv4 การเลือกใช้แต่ละเทคนิคต้องดูที่ความเหมาะสมของลักษณะ การใช้งานของเครือข่ายที่มีอยู่รวมถึงระดับของการปรับเปลี่ยน ที่เหมาะสมกับผู้ใช้ ซึ่งเราจะมาดูรายละเอียดของแต่ละเทคนิคกัน

1. Dual stacks

ตามที่ได้เกริ่นไว้ในบทความตอนที่แล้ว Dual stacks หมายถึงการใช้งาน IPv4 และ IPv6 stack ควบคู่กันไปภายในอุปกรณ์ตัวเดียวกัน Dual stacks เป็นทางออกที่ง่ายที่สุดสำหรับเครือข่ายที่ต้องการเริ่มใช้งาน IPv6 และถูกใช้อย่างแพร่หลายมากที่สุดในปัจจุบัน หลักการทำงานของ Dual Stack คือการกำหนด IP stack ออกเป็น 2 Stacks ทำงานขนานกัน เช่น เมื่อโหนดได้รับ IPv6 packet โหนดจะเลือก IPv6 stack มาจัดการกับแพ็กเก็ต (โดยตรวจสอบ Protocol version จากส่วนหัวของแพ็กเก็ต) ในขณะที่เดียวกันโหนดสามารถติดต่อกับเครือข่าย IPv4 (ผ่าน IPv4 stack) ได้เหมือนเดิมไม่ต้องเปลี่ยนแปลง โดยโหนดที่มี dual stack นี้จะต้องมี IP address สองหมายเลข คือ IPv4 address และ IPv6 address (ตามรูปที่ 1) การติดตั้ง Dual stacks สามารถทำได้ทั้งที่โฮสต์ที่เซิร์ฟเวอร์ และที่อุปกรณ์เครือข่าย เช่น เราเตอร์ ซึ่งก่อนอื่นท่านต้องได้รับการจัดสรรหมายเลข IPv6 address ก่อนจึงจะสามารถใช้งาน Dual stacks ได้ ซึ่งท่านสามารถลงทะเบียนเพื่อขอรับ IPv6 address ได้กับศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติที่ http://www.ipv6.nectec.or.th/ipv6_delegation.php

ความต้องการเบื้องต้น (ระดับ Host และ Network)

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



รูปที่ 1 การใช้งาน Dual stacks ที่เราเตอร์

ขั้นตอนการติดตั้ง Dual Stacks ที่เครื่องคอมพิวเตอร์ (Host)

- ระบบปฏิบัติการ Windows XP ที่ command ให้ทำการพิมพ์ 'IPv6 Install'

```
C:\Documents and Settings>ipv6 install
Installing...
Succeeded.
```

จากนั้นกำหนด IPv6 ให้กับเครื่อง เช่น

```
C:\Documents and Settings>ipv6 add 4/ 3ffe:1234:1234::2
C:\Documents and Settings>ipv6 rtr ::0 4/ 3ffe:1234:1234::1
```

- ระบบปฏิบัติการ Linux หากยังไม่ support IPv6 ให้ทำการพิมพ์ modprobe ipv6

```
$ modprobe ipv6
```

จากนั้นกำหนด IPv6 ให้กับเครื่อง เช่น

```
$ ifconfig eth0 inet6 add 3ffe:1234:1234::2/64
$ route -A inet6 add ::0 gw 3ffe:1234:1234::1
$ route -A inet6 add ::0 dev eth0
```

ขั้นตอนการติดตั้ง Dual Stacks ที่เราเตอร์

หาก IOS Software บนเราเตอร์สนับสนุน IPv6 แล้ว ซึ่งตรวจสอบได้จากเว็บไซต์ของอุปกรณ์เครือข่ายที่ใช้งานทำการ config router ด้วยคำสั่ง

```
# configure terminal
# ipv6 unicast-routing
```

จากนั้นกำหนด IPv6 ให้กับเครื่อง เช่น

```
(config) #interface fastEthernet 0/0
(config-if) #ipv6 address 3ffe:1234:1234::1/64
(config-if) #ipv6 enable
```

ขั้นตอนการติดตั้ง Dual Stacks ที่เซิร์ฟเวอร์

ขั้นตอนการติดตั้งจะแตกต่างกันไปตามชนิดของเซิร์ฟเวอร์ เช่น DNS, Mail, WWW, FTP ขั้นตอนสำหรับเซิร์ฟเวอร์แต่ละชนิดสามารถดูได้ที่ <http://www.ipv6.nectec.or.th/server.php>

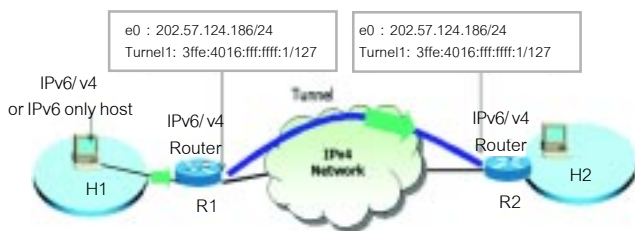
2. Tunnel

ในตอนที่เราได้แนะนำหลักการทำ Tunnel แบบคร่าวๆ ว่าต้องอาศัยเทคนิค IPv6-in-IPv4 packet encapsulation ในตอนนี้เราจะแนะนำหลักการทำ Tunnel สามประเภทพร้อมทั้งขั้นตอนการติดตั้ง

2.1 Manually Configured Tunnel

Manually Configured Tunnel เป็นวิธีที่นิยมกันมากสำหรับการให้บริการเชื่อมต่อ กันระหว่างเครื่องที่ใช้และติดตั้งหมายเลข IPv6 เพียงอย่างเดียว โดยต้องมีเกตเวย์ที่ติดตั้งและใช้งานแบบ Dual stacks ซึ่งจะทำหน้าที่เป็นอุโมงค์ เครือข่ายทางเข้าและทางออกโดยแต่ละด้านจะต้องเก็บหมายเลข IP address ของอุโมงค์เครือข่ายของอีกด้านที่ต้องการเชื่อมต่อ ซึ่งผู้ดูแลระบบจะต้องใส่หมายเลข IP address ของปลายทางอุโมงค์เขาไปเอง

วิธีนี้จึงต้องการการดูแลในส่วนของการทำงาน เมื่อแพ็กเก็ต IPv6 มาถึงอุโมงค์ ก็จะถูกห่อหุ้มด้วยเฮดเดอร์ IPv4 โดยใช้หมายเลข IPv4 ของเครือข่ายต้นทาง หมายเลข IPv4 ของเครือข่ายปลายทาง และระบุชนิดโพรโตคอลของข้อมูลที่อยู่ภายในเป็น IPv6 เมื่อแพ็กเก็ตมาถึงปลายทางของอุโมงค์ เครือข่ายปลายทางจะทำการตรวจสอบเฮดเดอร์ ซึ่งจะทราบว่าภายในเป็นแพ็กเก็ตที่ใช้หมายเลข IPv6 ดังนั้น ตัวเกตเวย์จะเอาส่วนหัว IPv4 ออกไปให้เหลือแต่ส่วนที่เป็น IPv6 แพ็กเก็ตแล้วส่งต่อไปยังเครื่องปลายทางที่ใช้หมายเลข IPv6 ที่ระบุอยู่ในส่วน Destination ของเฮดเดอร์ IPv6



รูปที่ 2 การทำงานของ Manually Configured Tunnel

ความต้องการเบื้องต้น (ระดับ Network)

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

ขั้นตอนการติดตั้ง Manually Configured Tunnel บน Linux Gateway

ติดตั้ง Tunnel บนเครื่องเพื่อเป็น Local tunnel endpoint ด้วยการสร้าง Logical device interface ตั้งชื่อเป็น sit1 พร้อมทั้งกำหนดหมายเลข IPv4 address สำหรับ Local tunnel endpoint และระบุ Remote tunnel endpoint ด้วย IPv4 address ของเกตเวย์อีกฝั่งของอุโมงค์

```
$ /sbin/ip tunnel add sit1 mode sit ttl 3 remote 192.150.240.24 local 202.57.124.186
$ /sbin/ifconfig sit1 up
$ /sbin/route -A inet6 add ::/0 dev sit1
$ /sbin/ip -6 addr add 3ffe:4016:fff:ffff:1/127 dev sit1
#Forwarder เพื่อสามารถส่งต่อ IPv6 แพ็กเก็ตจากเครื่องโคลงตัวผ่านทาง sit1 ได้
$ /sbin/sysctl -w net.ipv6.conf.sit1.forwarding=1
$ /sbin/sysctl -w net.ipv6.conf.default.forwarding=1
$ /sbin/sysctl -w net.ipv6.conf.all.forwarding=1
$ /sbin/sysctl -w net.ipv6.conf.eth0.forwarding=1
$ /sbin/sysctl -w net.ipv6.conf.lo.forwarding=1
```

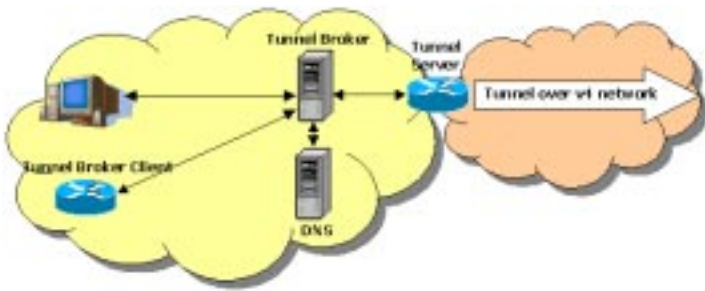
ขั้นตอนการติดตั้ง Manually Configured Tunnel บนเราเตอร์

```
!
ipv6 unicast-routing
interface Tunnel1
description Configured Tunnel to Tunnel2
no ip address
ipv6 address 3ffe:4016:fff:ffff:1/127
tunnel source Ethernet0/0
tunnel destination 192.150.240.24
tunnel mode ipv6ip
!
```

2.2 Semi Automatic Tunnel (Tunnel Broker)

การทำงานของ Semi Automatic Tunnel หรือที่รู้จักในชื่อ Tunnel Broker คือ การสร้างอุโมงค์อัตโนมัติโดยผู้ใช้ (end user) ต้องลงทะเบียนใช้บริการกับผู้ให้บริการ โดยผู้ให้บริการจะสร้าง Tunnel เพื่อเชื่อมต่อไปยังเครือข่าย IPv6 แทนผู้ที่มาลงทะเบียน ดังนั้นผู้ที่ให้บริการ Tunnel Broker จึงเป็นเสมือนผู้ให้บริการ IPv6 แก่ผู้ใช้ที่มีการเชื่อมต่อผ่านเครือข่าย IPv4 อยู่แล้ว ในปัจจุบันนี้มีผู้ให้บริการ 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 เหมาะกับเครือข่าย IPv6 เล็กๆ หรือโฮสต์จำนวนไม่มากที่ต้องการเชื่อมต่อกับเครือข่าย IPv6 ใหญ่แห่งอื่นอย่างง่าย การเชื่อมต่อด้วย Tunnel แบบอื่น จะเหมาะกับการติดต่อกันโดยตรงระหว่างเครือข่าย IPv6 ย่อยสองเครือข่าย โดยไม่ต้องพึ่งหรือรอการเชื่อมต่อที่ระดับ ISP



รูปที่ 3 การทำงานของ Tunnel Broker

ความต้องการเบื้องต้น (ระดับ Network)

- เราเตอร์หรือเกตเวย์ (IPv4 หรือ Dual stacks ก็ได้) สำหรับ Tunnel Broker
- เราเตอร์หรือเกตเวย์ที่เป็น Dual stacks สำหรับ Tunnel Server (Tunnel Gateway)
- หมายเลข Public IPv4 address 1 หมายเลข สำหรับ Tunnel Broker
- หมายเลข Public IPv4 address 1 หมายเลข สำหรับ Tunnel Server

ความต้องการเบื้องต้น (ระดับ Host)

- 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
- ชื่อที่ต้องการลงทะเบียนในฐานะข้อมูล DNS คู่กับหมายเลข IPv6 address ที่ได้รับจัดสรรจาก Tunnel Broker
- ถ้า Tunnel Broker Client เป็นโฮสต์ไม่ควรอยู่หลัง NAT Gateway หรือถ้าหลีกเลี่ยงไม่ได้ ต้องเปิดพอร์ต 41 ที่ NAT Gateway
- ถ้า Tunnel Broker Client เป็นเราเตอร์ ต้องระบุจำนวน IPv6 address ที่ต้องการรับจัดสรรจาก Tunnel Broker

ขั้นตอนการติดตั้ง Tunnel Broker บนโฮสต์ส่วนใหญ่แล้วผู้ที่ให้บริการ Tunnel Broker จะเป็นผู้กำหนดขั้นตอนการติดตั้งค่าต่างๆ บนโฮสต์ที่ต้องการเป็น Tunnel Broker Client มาให้โดยหลักการแล้วเครื่องคอมพิวเตอร์ที่เป็น Tunnel Broker Client จะต้องทำการติดตั้ง Dual stacks ก่อน ให้ใช้งาน 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 คือวิธีที่เรียกว่า 6to4 Tunnel (ดู RFC3056) เครื่องข่ายที่เชื่อมต่อแบบ 6to4 Tunnel จะต้องกำหนดหมายเลข IPv6 Prefix พิเศษให้กับตัวเกตเวย์ทั้งสองฝั่งของ 6to4 Tunnel Prefix นี้จะขึ้นต้นด้วย 2002 และจะต้องมี IPv4 address ที่อยู่ในรูปเลขฐานสิบหก ตามมา เพราะฉะนั้น Prefix ต้องมีความยาวอย่างน้อย 48 บิต ตามรูปแบบ 2002:<IPv4 in hex>::/48 ตัวอย่างเช่น หาก IPv4 address ของเกตเวย์คือ 202.57.124.186 (แปลงเป็นเลขฐานสิบหกได้ CA39:7CBA) IPv6 address ของเกตเวย์อาจเป็น 2002:CA39:7CBA::1/48 การกำหนด Prefix วิธีนี้จะทำให้ทราบหมายเลข IPv4 ของเกตเวย์ปลายทางได้โดยอัตโนมัติ

ตามตัวอย่างในรูปที่ 4 เมื่อแพ็กเก็ต IPv6 มาถึงเกตเวย์ทางออกที่จะไปยังอินเทอร์เน็ตเกตเวย์ จะตรวจสอบหมายเลขปลายทาง พบหมายเลขปลายทางถูกกำหนดเป็น 2002:C096:F018::2/128 เกตเวย์สามารถทราบได้ว่า IPv4 address ของเกตเวย์ปลายทางจะต้องเป็น C096:F018 หรือ 192.150.240.24 จึงกำหนดหมายเลขนี้ใน Destination field ของ IPv4 packet header ที่นำมา encapsulate

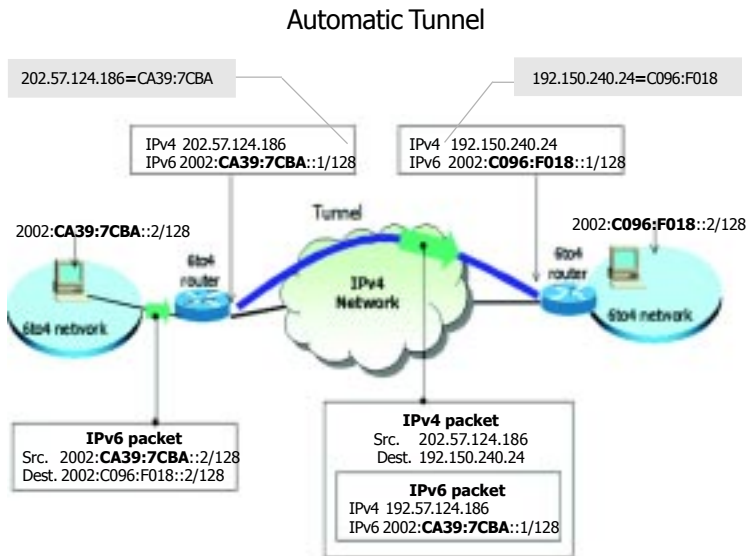
ในปัจจุบันท่านสามารถลงทะเบียนเพื่อขอใช้บริการ 6to4 tunnel ได้กับศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติที่ <http://www.ipv6.nectec.or.th>

ความต้องการเบื้องต้น (ระดับ Network)

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

ความต้องการเบื้องต้น (ระดับ Host)

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



รูปที่ 4 การทำงานของ Fully Automatic Tunnel

ขั้นตอนการติดตั้ง Fully Automatic Tunnel บน เครื่องคอมพิวเตอร์ (Host)

- ระบบปฏิบัติการ Windows XP

```
C:\Documents and Settings>ipv6 rtu 2002:CA39:7CBA::1 pub
```

- ระบบปฏิบัติการ Linux

```
$ ifconfig eth0 add 2002:CA39:7CBA::2/128
$ route -A inet6 add ::/0 gw 2002:CA39:7CBA::1
$ route -A inet6 add ::/0 dev eth0
```

ขั้นตอนการติดตั้ง Fully Automatic Tunnel บนเราเตอร์

```
!
interface FastEthernet0/0
ip address 202.57.124.186 255.255.255.252
ipv6 address 2002:CA39:7CBA::1/64
ipv6 enable
!
```

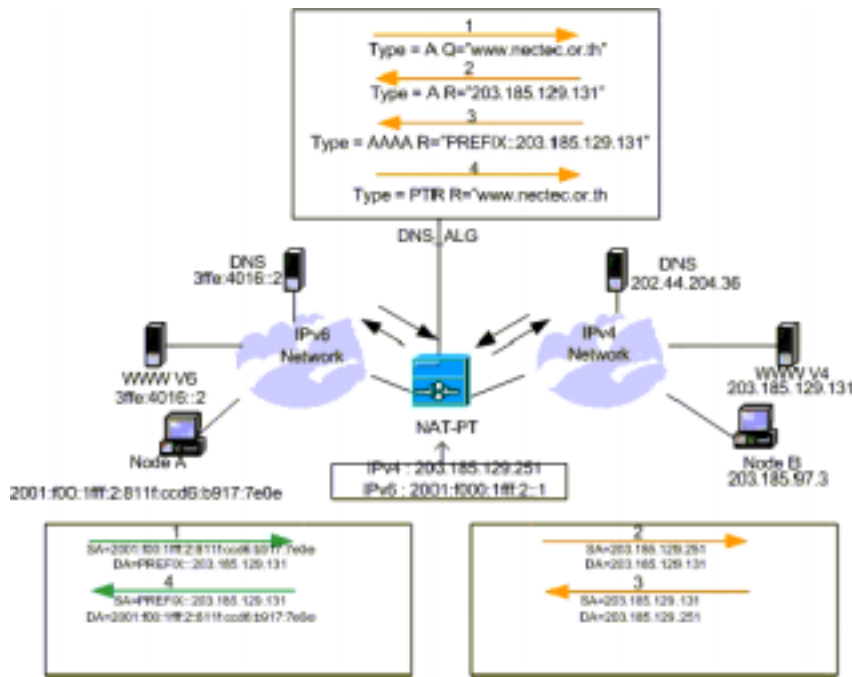
3. Translation

เทคนิคการทำ Translation เป็นวิธีที่ใช้กับการสื่อสารข้ามเครือข่าย เช่น โหนดจากเครือข่าย IPv4 ต้องการคุยกับเซิร์ฟเวอร์ในเครือข่าย IPv6 หรือโหนดที่เป็น IPv6 ต้องการคุยกับเซิร์ฟเวอร์ที่เป็น IPv4 ซึ่งจะเป็นกรณีที่ต่างไปจากการใช้งาน Dual stacks และ Tunnel การทำ Translation คือการแปลงข้อมูลไปมาระหว่างข้อมูลในรูปแบบของ IPv4 packet และ IPv6 packet 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

ในบทความนี้ เราจะยกตัวอย่างการทำ Translation ที่ Network device ได้แก่วิธีที่เรียกว่า 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 ในเครือข่าย IPv4 นั่นก็คือการแปลง IP address โดยเสมือนว่าคอมพิวเตอร์แต่ละเครื่องจะมีหมายเลข IP address สองตัว สำหรับติดต่อกับเครือข่ายภายในและสำหรับติดต่อกับเครือข่ายภายนอก สำหรับ NAT-PT จะเป็นการแปลงระหว่าง IPv4 address กับ IPv6 address เพื่อใช้ในการติดต่อสื่อสารกันระหว่างเครือข่ายที่ใช้อินเทอร์เน็ตโพรโตคอลคนละรุ่น ตัวอย่างเช่น ในรูปที่ 5 คอมพิวเตอร์



รูปที่ 6 ขั้นตอนการเรียกดูเว็บไซต์ IPv4 จากโหนด IPv6

ทางซ้ายมือใช้หมายเลข 172.16.1.1 ในการติดต่อกับเครื่องอื่นๆ ในเครือข่าย IPv4 ด้วยกัน แต่ถ้าหากมันต้องการติดต่อกับคอมพิวเตอร์อีกเครื่องในเครือข่าย 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 นี้จำเป็นต้องจำคู่หมายเลขนี้ไว้เพื่อที่ว่าเมื่อได้รับแพ็กเก็ตตอบจากเครื่องในเครือข่าย IPv6 โดยมีปลายทางที่ 2001:0420:1987:0:2E0:B0FF:FE6A:412C จะได้อัตโนมัติแปลงกลับเป็นหมายเลข 172.16.1.1

work layer จึงไม่มีความรู้ว่าแต่ละแพ็กเก็ตที่ผ่านเข้ามาเป็นของแอปพลิเคชันชนิดใด ดังนั้น จึงจำเป็นต้องมีอุปกรณ์อีกตัวที่ทำงานในระดับ Application layer สำหรับจัดการกับปัญหานี้ ซึ่งเรียกว่า Application Layer Gateway (ALG) โดยที่เกตเวย์ NAT-PT จะต้องคอยส่งแพ็กเก็ตต่อไปยัง ALG เพื่อตรวจสอบหาหมายเลข IP address ในส่วน payload และแปลงให้เป็น IP address ใหม่ที่ถูกต้อง

ตัวอย่าง ขั้นตอนการเรียกดูเว็บไซต์ IPv4 จากโหนด IPv6 มีดังนี้ (ดูรูปที่ 6 ประกอบ)

1. เมื่อ Node A ซึ่งมี Source Address (SA) = 2001:f00:1fff:2:811f:ccd6:b917 ต้องการเรียกเว็บ www.nectec.or.th ซึ่งเป็น IPv4 มันต้องไปถาม IP address ที่ DNS-ALG ซึ่ง DNS-ALG ก็จะมีทำการตรวจสอบไปยัง DNS ผ่านเกตเวย์ NAT-PT เซิร์ฟเวอร์ DNS v4 ตอบกลับมาว่า IPv4 address ของเว็บเซิร์ฟเวอร์ คือ 203.185.129.131 เกตเวย์ NAT-PT และ DNS_ALG ก็ต้องแปลง IPv4 address ของเว็บเซิร์ฟเวอร์นี้ให้ได้อยู่ในรูปแบบ IPv6 address คือ Destination Address (DA) = PREFIX::203.185.129.131 จะมีการใช้วิธีการแปลงจาก IPv4 ให้อยู่ในรูปแบบ IPv6 จะได้ 203.185.129.131 แปลงเป็นเลขฐาน 16 จะได้ cbb9:8183 เอามารวมกับ PREFIX เป็น 2001:f00:1fff::cbb9:8183 จะเป็น DA เพื่อใช้ในการคุยไปยังเครือข่าย IPv6



รูปที่ 5 การทำงานของ NAT-PT

เนื่องจากแอปพลิเคชันบางชนิด เช่น DNS มีการบรรจุหมายเลข IP address ในส่วนของ payload ด้วย ทำให้เกิดปัญหา เพราะว่าเกตเวย์ NAT-PT จะไม่สามารถแปลง IP address นอกเหนือจากส่วนที่อยู่ใน IP เฮดเดอร์ได้ เพราะว่าเกตเวย์ NAT-PT เป็นอุปกรณ์ที่ทำงานในระดับ Net-

- เมื่อได้ SA และ DA ในรูปแบบ IPv6 address แล้ว สามารถคุยกันได้ในเครือข่าย IPv6 เมื่อติดต่อกลับไป เครือข่าย IPv4 เกตเวย์ NAT-PT จะต้องแปลงจาก SAV6 ไปเป็น SAV4 = 203.185.129.251 (ซึ่งก็คือ IPv4 address ของตัวเกตเวย์ NAT-PT นั้นเอง) เพื่อไปคุยกับเว็บ เซิร์ฟเวอร์ (DAv4 = 203.185.129.131)
- เมื่อเว็บเซิร์ฟเวอร์ติดต่อกลับ ก็จะต้องผ่านเกตเวย์ NAT-PT อีก ซึ่งเกตเวย์จะได้รับแพ็กเก็ตที่มี SAV4 = 203.185.129.131 และ DAv4 = 203.185.129.251 เกตเวย์ NAT-PT จะต้องแปลงจาก SAV4 ไปเป็น SAV6 = Prefix::203.185.129.131
- เมื่อต้นทางกับปลายทางมีรูปแบบการสื่อสารเหมือนกันก็จะสามารถติดต่อกันได้ โดย SAV6 = Prefix::203.185.129.131 และ DAv6 = 2001:f00:1fff:2:811f:ccd6:b91

ความต้องการเบื้องต้น (ระดับ Network)

- เราเตอร์หรือเกตเวย์ที่เป็น Dual stacks สำหรับ NAT-PT Gateway
- เกตเวย์สำหรับ ALG (สามารถใช้เกตเวย์ตัวเดียวกันกับ NAT-PT Gateway ได้)
- DNS v6 เพื่อแปลงจากชื่อให้เป็นหมายเลข IPv6 address
- หมายเลข IPv4 address และ IPv6 address อย่างละ 1 หมายเลข สำหรับ NAT-PT Gateway

ขั้นตอนการติดตั้ง NAT-PT Gateway บนระบบ

ปฏิบัติการ FreeBSD

ก่อนอื่นต้อง แก้ไข kernel ของ FreeBSD เพื่อให้ใช้งาน NAT-PT ได้ โดยการดาวน์โหลด snap kit ล่าสุดจาก <http://www.kame.net> หลังจากติดตั้ง snap kit แล้ว สามารถเช็ค ว่าสามารถใช้ NAT-PT ได้โดยใช้คำสั่ง

```
$ dmesg
NAT-PT initialized
```

แก้ไขไฟล์ /etc/natpt.conf ดังนี้

```
map flush
# set 96 bit natpt prefix
prefix 2001:0f00:1fff::
# [v6 -> v4] — seems outbound
map from any6 to 203.185.129.251 port 28672 -
32767
# [v4 -> v6]
# enable translation
map enable
```

แก้ไขไฟล์ /etc/rtdavd.conf ดังนี้

```
bfe0:\
:addr="2001:0f00:1fff:1::":prefixlen#64:
```

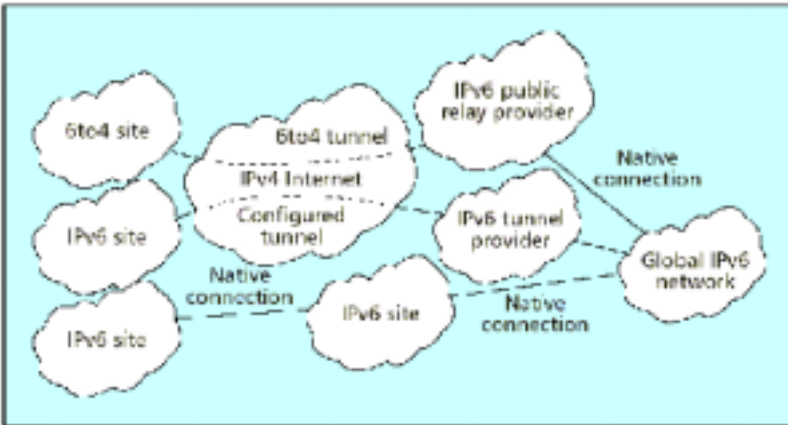
bfe0 คือ ชื่อของ Interface card ที่จะให้ทำการแจก IPv6 address ในฝั่ง Clientem0 คือ ชื่อของ Interface card ที่ต่อ IPv4 Address แก้ไขไฟล์ /etc/totd.conf ดังนี้

```
forwarder 202.44.204.36 port 53
forwarder 202.44.204.63 port 53
forwarder 203.185.132.132 port 53
forwarder 3ffe:4016::2 port 53
forwarder 203.185.97.253 port 53
forwarder 2001:0f00:1fff:2::1 port 53
prefix 2001:0f00:1fff::
port 53
```

การเลือกใช้เทคนิคการปรับเปลี่ยนที่เหมาะสม

การปรับเปลี่ยนเครือข่ายเพื่อให้ใช้งานกับเครือข่าย IPv6 ได้นั้นมีหลากหลายเทคนิค ซึ่งแต่ละเทคนิคสามารถใช้ควบคู่กันได้ (ดังแสดงในรูปที่ 7) การตัดสินใจเลือกที่จะใช้เทคนิคชนิดใดนั้น ขึ้นอยู่กับลักษณะของเครือข่าย และการเชื่อมต่อที่ต้องการเป็นสำคัญ ตัวอย่างเช่นถ้าผู้ใช้ต้องการติดต่อกับเครือข่าย IPv6 ในขณะที่ ISP ของตนยังไม่เปิดให้บริการเชื่อมต่อแบบ IPv6 สิ่งที่ใช้สามารถทำได้ก็คือ การลงทะเบียนกับ Tunnel broker หรือผู้ที่ให้บริการ tunnel แบบอื่นและตั้งค่าให้ คอมพิวเตอร์ ของตนเป็น Dual stacks แต่ถ้าหากว่า ISP นั้นมีบริการเชื่อมต่อกับเครือข่าย IPv6 อยู่แล้ว ผู้ใช้เพียงแค่อัปเดต Dual stacks ที่คอมพิวเตอร์ก็พอ

ตามที่กล่าวมาแล้วทั้งหมด จะเห็นได้ชัดว่า การใช้งานเครือข่าย IPv6 จะเป็นในลักษณะใช้งานควบคู่ไปกับ IPv4 อย่างค่อยเป็นค่อยไปมากกว่าที่จะเป็นการเปลี่ยนแปลงในทันที อย่างไรก็ตาม หลังจากการปรับเปลี่ยนเสร็จสมบูรณ์ เมื่อเครือข่ายต้นทาง กลางทาง และปลายทางเป็น IPv6 ทั้งหมด เราสามารถทำการสื่อสารโดยใช้โพรโตคอล IPv6 โดยตรง ซึ่งเราเรียกการสื่อสารลักษณะนี้ว่า Native IPv6 network



รูปที่ 7 การใช้เทคนิคการปรับเปลี่ยนเครือข่ายหลายชนิดควบคู่กัน [1]

ตารางที่ 1 เปรียบเทียบเทคนิคการปรับเปลี่ยนจาก IPv4 สู่ IPv6

Name	Connectivity	Type	Location
Dual stacks 6to6 over6	4to4 over4, 6to6 over6	Dual stacks	ในโฮสต์หรืออุปกรณ์เครือข่าย
Manual configured tunnel	6to6 over4	Tunnel	ระหว่างโฮสต์และอุปกรณ์เครือข่าย
Tunnel broker	6to6 over4	Tunnel	ระหว่างโฮสต์และอุปกรณ์เครือข่าย
6to4 tunnel	6to6 over4	Tunnel	ระหว่างโฮสต์และอุปกรณ์เครือข่าย
NAT-PT	6to4, 4to6	Translator	ในอุปกรณ์เครือข่าย

อุปกรณ์และแอปพลิเคชันที่สนับสนุน IPv6

ก่อนที่ท่านผู้อ่านจะเริ่มลงมือปฏิบัติตามขั้นตอนการติดตั้งต่างๆ ที่เรานำเสนอไปแล้วนั้น ลองสำรวจดูสักนิดว่าเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายของท่านพร้อมที่จะรับมือกับเครือข่าย IPv6 หรือไม่

ระบบปฏิบัติการ (Operating System)

ปัจจุบันระบบปฏิบัติการส่วนใหญ่พร้อมสนับสนุนการใช้งาน IPv6 (IPv6 Ready) ตัวอย่างเช่น 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 สามารถใช้งานได้โดย

- Windows9x มี Trumpet Winsock ซึ่ง version ล่าสุดใช้ IPv6 ได้
- Windows 2000 ถ้าติดตั้ง SP1 ขึ้นไป แล้วจะสามารถดาวน์โหลด TCP/IPv6 มาลง ก็จะใช้ IPv6 ได้
- Windows 2003 และ Windows XP สามารถใช้งาน IPv6 ได้อยู่แล้ว (IPv6 Ready)

อุปกรณ์เครือข่าย (Network Device)

อุปกรณ์หรือผลิตภัณฑ์ในท้องตลาดที่สนับสนุน การใช้งาน IPv6 ขณะนี้เริ่มมีจำนวนมากขึ้น ยกตัวอย่าง เช่น อุปกรณ์ของบริษัท Cisco, Juniper, Nortel, Fujitsu, Hitachi และอื่นๆ ทั้งนี้หากอุปกรณ์เครือข่าย เช่น เราเตอร์ ที่ท่านมีอยู่ยังไม่สนับสนุนการใช้งาน IPv6 ท่านสามารถแก้ไขได้โดยการเปลี่ยน firmware หรือระบบปฏิบัติการของเราเตอร์นั้นๆ

การขอหมายเลข IPv6 Address ในประเทศไทย

ปัจจุบันมีหน่วยงานภาครัฐและผู้ให้บริการอินเทอร์เน็ตหลายแห่งได้รับจัดสรรชุดหมายเลข IPv6 address จาก 6Bone และ APNIC และได้้นำชุดหมายเลขเหล่านั้น มาจัดสรรต่อให้แก่หน่วยงานอื่นที่ต้องการทดลองใช้และทดสอบการเชื่อมต่อบนเครือข่าย IPv6 ท่านสามารถลงทะเบียน เพื่อขอรับ IPv6 address ได้จากศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติที่ http://www.ipv6.nectec.or.th/ipv6_delegation.php และที่บริษัท กสท โทรคมนาคมที่ <http://web.ipv6.cattelecom.com/addressallocation.html>

สรุป

หวังว่าบทความนี้จะช่วยนำท่านผู้อ่านให้เข้าใจโลกอินเทอร์เน็ตยุคหน้ามากขึ้นไปอีก ความเข้าใจในตัวเทคโนโลยีเป็นก้าวแรกของการเตรียมความพร้อม สำหรับรายละเอียดเพิ่มเติม ท่านสามารถหาดูได้จากเว็บไซต์NECTEC IPv6 Testbed (<http://www.ipv6.nectec.or.th>) ในตอนต่อไป เราจะกล่าวถึงสภาพโดยรวมของเครือข่าย IPv6 ในประเทศไทยว่าในปัจจุบันมี ISP ที่รายที่ได้เริ่มเชื่อมต่อกับเครือข่าย IPv6 บ้างแล้ว และมีการให้บริการอะไรบ้าง และประเทศไทยมีความก้าวหน้าในระดับใดเมื่อเทียบกับประเทศอื่นๆ อย่าลืมติดตามนะคะ



เอกสารอ้างอิง

1. D. Waddington and F. Chang, "Realizing the Transition to IPv6," IEEE Communications Magazine, June 2002.
2. B. Carpenter and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds," RFC 3056, February 2001.
3. A. Durand, P. Fassano, I. Guardini, and D. Lento, "IPv6 Tunnel Broker," RFC 3053, January 2001.
4. G. Tsirtsis and P. Srisuresh "Network Address Translation - Protocol Translation (NAT-PT)", RFC 2766, February 2000.
5. Benoit Lourdelet, "Cisco IOS NAT-PT for IPv6," White Paper, May 2003.
6. P. Srisuresh, G. Tsirtsis, P. Akkiraju. and A. Heffernan, "DNS extensions to Network Address Translator (DNS_ALG)," RFC 2694, September 1999.
7. <http://www.kame.net>
8. <http://www.cisco.njut.edu.cn/UploadFiles/200452692750734.gif>
9. <http://www.ripe.net/rs/ipv6/stats/apnic.html>
10. <http://www.ipv6.nectec.or.th/>
11. <http://web.ipv6.catttelecom.com>
12. <http://www.6bone.net>
13. <http://www.apnic.org>