การวิเคราะห์โครงสร้างการเชื่อมต่อบน IPv6 ภายในองค์กรและการประยุกต์ใช้งาน

STRUCTURAL CONNECTION ANALYSIS ON IPv6 IN ORGANIZATION AND ITS APPLICATIONS

สุริยา เจริญชุติธาร

SURIYA CHARCENCHUTITAVORN

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมโทรคมนาคม

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

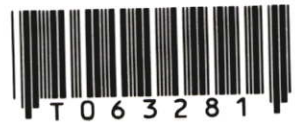
พ.ศ. 2549

ISBN 974-15-2253-3

สำนักหอสมุดกลาง พระจอมเกล้าลาดกระบัง

การวิเคราะห์โครงสร้างการเชื่อมต่อบน IPv6 ภายในองค์กรและการประยุกต์ใช้งาน

STRUCTURAL CONNECTION ANALYSIS ON IPv6 IN ORGANIZATION AND ITS APPLICATIONS



สุริยา เจริญชุติถาวร

SURIYA CHAROENCHUTITAVORN

เลขหมู่.....
เลขทะเบียน 63281
วัน,เดือน,ปี 25 ส.ค. 2549

.b.....
.i.....

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมโทรคมนาคม

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ.2549

ISBN 974-15-2253-3

STRUCTURAL CONNECTION ANALYSIS ON IPv6 IN ORGANIZATION AND ITS APPLICATIONS

SURIYA CHAROENCHUTITAVORN

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF ENGINEERING IN TELECOMMUNICATIONS ENGINEERING

SCHOOL OF GRADUATE STUDIES

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2006

ISBN 974-15-2253-3

COPYRIGHT 2006

SCHOOL OF GRADUATE STUDIES

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ใบรับรองวิทยานิพนธ์

หัวข้อวิทยานิพนธ์ การวิเคราะห์โครงสร้างการเชื่อมต่อบน IPv6 ภายในองค์กรและการประยุกต์ใช้งาน
STRUCTURAL CONNECTION ANALYSIS ON IPv6 IN ORGANIZATION AND ITS APPLICATIONS

นักศึกษา นายสุริยา เจริญชุติถาวร

รหัสประจำตัว 47061014

ปริญญา วิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชา วิศวกรรมโทรคมนาคม

อาจารย์ผู้ควบคุมวิทยานิพนธ์ รศ.ดร.กอบชัย เดชหาญ

คณะกรรมการสอบวิทยานิพนธ์		ลายมือชื่อ
ผศ.ดร.พิเชฐ	ม่วงนวล	
รศ.สมยศ	จุณณะปิยะ	
ดร.พิพัฒน์	พรหมมี	
รศ.ดร.ฟูศักดิ์	ชีวสุวิทย์	
รศ.ดร.กอบชัย	เดชหาญ	

วัน / เดือน/ ปี ที่สอบ 18 เมษายน 2549 เวลา 11.30 น. เป็นต้นไป

สถานที่สอบ ณ อาคาร 12 ชั้น ชั้น 4 (ห้อง E12-404)

บัณฑิตวิทยาลัยรับรองแล้ว

(ผศ.ดร.จารุวัตร เจริญสุข)

คณบดีบัณฑิตวิทยาลัย

วันที่.....๘.....**เดือน**...พฤษภาคม.....**พ.ศ**.....๒๕๔๙.....

หัวข้อวิทยานิพนธ์	การวิเคราะห์โครงสร้างการเชื่อมต่อบน IPv6 ภายในองค์กรและการประยุกต์ใช้งาน
นักศึกษา	นายสุริยา เจริญชุติถาวร
รหัสนักศึกษา	47061014
ปริญญา	วิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชา	วิศวกรรมโทรคมนาคม
พ.ศ.	2549
อาจารย์ผู้ควบคุมวิทยานิพนธ์	รศ.ดร. กอบชัย เดชหาญ

บทคัดย่อ

ปัจจุบันการใช้เทคโนโลยีเครือข่ายอินเตอร์เน็ตได้รับความนิยมอย่างแพร่หลายทั่วโลก และการเติบโตของเครือข่ายอินเตอร์เน็ตอย่างรวดเร็ว จึงทำให้จำนวนหมายเลขอินเตอร์เน็ตโพรโตคอลที่มีอยู่ไม่เพียงพอสำหรับความต้องการ ทำให้เกิดอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) ซึ่งถูกพัฒนามาจากอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) โดยในปัจจุบันได้เริ่มมีการใช้งานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) กันบ้างแล้ว ในบทความนี้จะเป็นการวิเคราะห์โครงสร้างการเชื่อมต่อบน IPv6 ภายในองค์กรและการประยุกต์การใช้งานโดยจะจำลองระบบเครือข่ายภายในองค์กร เพื่อทดสอบดูลักษณะการทำงานของอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) และการนำอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) มาเชื่อมต่อกับระบบอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 ว่าสามารถใช้งานร่วมกันได้หรือไม่ โดยการวิเคราะห์นี้จะเป็นการเตรียมระบบภายในองค์กรให้สามารถรองรับการใช้งานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) ให้มีประสิทธิภาพ

Thesis Title	Structural Connection Analysis on IPv6 in Organization and Its Applications
Student	Mr. Suriya Charoenchutitavorn
Student ID.	47061014
Degree	Mater of Engineering
Programme	Telecommuncations Engineering
Year	2006
Thesis Advisor	Assoc.Prof.Dr. Kobchai Dejhan

ABSTRACT

Internet technologies have become popular and widely used all over the world the growth of Internet effect to Internet protocol number that serve for Internet workstation. That's the reason to generate Internet protocol version 6 (IPv6) developed from Internet protocol version 4 (IPv4) and now it starts to use in some area. This paper uses the simulation of organization's network and analyze Internet protocol version 6 (IPv6) component. It uses Internet protocol version 6 (IPv6) to join with Internet protocol version 4 (IPv4) for testing, checking and analyzing its association between two versions. By analyzing in this paper, all organizations can prepare theirs networks for new version of Internet protocol version 6 (IPv6) with the previous version.

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุลวงได้อย่างดี ด้วยคำแนะนำเกี่ยวกับระบบเครือข่ายสื่อสารข้อมูล และคำปรึกษาที่มีประโยชน์อย่างสูงจากท่านรองศาสตราจาย์ ดร. กอบชัย เดชหาญ ที่ช่วยเหลือตลอดเวลา ซึ่งทำให้กระผมทีความรู้สึกซาบซึ้งในสิ่งต่างๆ ที่ท่านได้ให้ความอนุเคราะห์ ขอกราบขอบพระคุณเป็นอย่างสูง

ขอกราบขอบพระคุณ คุณพ่อ ย่งเกียง แซ่โง้ว และ คุณแม่ สุนัดดา พงศ์วิไล ที่กรุณามอบชีวิตความใฝ่รู้ และความมุมานะในด้านการศึกษาให้แก่ชีวิตกระผม

ขอขอบคุณอาจารย์รชา เพริศพิพัฒน์ ที่คอยให้คำชี้แนะ ตลอดจนให้ความรู้ทางด้านระบบเครือข่าย, สนับสนุนเครื่องมือตลอดจนข้อมูล และหนังสือต่างๆ ที่ใช้ในการทำวิจัย

ขอขอบคุณ คุณแสงนภา เชิดชิด ที่ให้กำลังใจและช่วยเหลือในเรื่องต่าง ๆ

สุดท้ายนี้ขอขอบคุณน้องๆ ที่ช่วยเหลือ และ ให้กำลังใจต่อผู้ทำวิจัยจนสำเร็จสมบูรณ์

คุณค่าและประโยชน์อันพึงมาจากวิทยานิพนธ์ฉบับนี้ ข้าพเจ้าขอมอบแด่ผู้มีพระคุณทุกท่าน

สุริยา เจริญชุติถาวร

สารบัญ

หน้า

บทคัดย่อภาษาไทย.....I

บทคัดย่อภาษาอังกฤษ.....II

กิตติกรรมประกาศ.....III

สารบัญ.....IV

สารบัญตาราง.....VII

สารบัญรูป.....VIII

บทที่ 1 บทนำ.....1

1.1 ความเป็นมาและความสำคัญของปัญหา.....1

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา.....1

1.3 หลักการใหม่ในวิทยานิพนธ์.....2

1.4 เปรียบเทียบกับหลักการเดิมที่มีอยู่.....2

1.5 ขอบเขตการทำวิทยานิพนธ์.....3

1.6 รายละเอียดในวิทยานิพนธ์.....3

บทที่ 2 ความรู้พื้นฐานเกี่ยวกับอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6.....4

2.1 คุณสมบัติอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6.....4

2.1.1 ขนาดแอดเดรส.....4

2.1.2 ระดับขนาดของแอดเดรส.....5

2.1.3 Autoconfiguration.....5

2.1.4 Renumbering.....6

2.1.5 Multicast Use.....7

2.1.6 ประสิทธิภาพของ Header.....8

2.1.7 Flow Label.....9

2.1.8 Extension Header.....10

2.1.9 Mobility.....10

2.1.10 Security.....10

สารบัญ (ต่อ)

หน้า

2.2 โครงสร้างอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6.....11

2.3 รูปแบบการเขียนหมายเลขแอดเดรสอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6.....12

2.4 ชนิดของอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6.....14

2.4.1 Limk-Local Address.....15

2.4.2 Site-Local Address.....16

2.4.3 Aggregable Global Unicast Address 17

2.4.4 Multicast Address.....18

2.4.5 Anycast Address.....19

2.4.6 Loopback Address.....19

2.5 เปรียบเทียบคุณสมบัติอินเทอร์เน็ตโพรโตคอลรุ่นที่ 6 กับคุณสมบัติเน็ตโพรโตคอลรุ่นที่ 4.....20

บทที่ 3 การเลือกเส้นทางอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6.....23

3.1 การเลือกเส้นทางแบบ Static Route.....23

3.2 การเลือกเส้นทางแบบ RIPng.....24

3.2.1 ขั้นตอนทำงานของ RIPng.....25

3.2.2 โครงสร้างของเมสเสจ RIPng.....26

บทที่ 4 ลักษณะการเชื่อมต่ออินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 29

4.1 Dual Stack 29

4.2 การทะลุผ่านข้อมูล (Tunneling).....31

4.2.1 Manually Configured Tunnel.....33

4.2.2 Fully Automatic Tunnel (6to4 Tunnel).....34

4.3 การแปลงข้อมูล (Translation).....35

4.3.1 NAT-PT (Network Address –Protocal Translation).....35

บทที่ 5 การเตรียมความพร้อมของอุปกรณ์.....38

5.1 เตรียมความพร้อมทางด้าน Hardware.....38

5.2 เตรียมความพร้อมทางด้าน Software.....38

สารบัญ (ต่อ)

หน้า

5.2.1 ระบบปฏิบัติการ (Operation System).....38
5.2.2 โปรแกรมประยุกต์ต่างๆ (Application).....39
5.2.3 การติดตั้งและการใช้คำสั่งอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 บน Windows XP...39

บทที่ 6 แบบจำลองและการวิเคราะห์ผลการทำงาน.....40
6.1 แบบจำลอง.....40
6.2 การกำหนดพารามิเตอร์ในระบบจำลอง.....42
6.3. ผลที่ได้การทดลองตามแบบจำลอง.....42
6.3.1 แบบจำลองระบบ LAN.....42
6.3.2 แบบจำลองระบบ WAN.....48
6.3.3 แบบจำลองลักษณะการเชื่อมต่อ IPv6 และ IPv4 แบบ 6to4 Tunneling....53

บทที่ 7 สรุปผลการวิจัยและข้อเสนอแนะ.....55

บรรณานุกรม.....57

ภาคผนวก.....58
ภาคผนวก ก. ตัวอย่าง Configuration ของ Router BRANCH แบบ IPv4 (Pure).....59
ภาคผนวก ข. ตัวอย่าง Configuration ของ Router BRANCH แบบ IPv6 (Pure)..... 63
ภาคผนวก ค. ตัวอย่าง Configuration ของ Router BRANCH แบบ Dual Stack.....67
ภาคผนวก ง. ตัวอย่าง Configuration ของ Router BRANCH แบบ 6to4 Tunneling.....71
ภาคผนวก จ. ตัวอย่าง Configuration ของ Router HQ แบบ IPv4 (Pure).....75
ภาคผนวก ฉ. ตัวอย่าง Configuration ของ Router HQ แบบ IPv6 (Pure).....79
ภาคผนวก ช. ตัวอย่าง Configuration ของ Router HQ แบบ Dual Stack.....83
ภาคผนวก ซ. ตัวอย่าง Configuration ของ Router HQ แบบ 6to4 Tunneling.....87
ภาคผนวก ฌ. ผลงานวิจัยที่ได้รับการตีพิมพ์เผยแพร่.....91

ประวัติผู้เขียน.....99

สารบัญตาราง

ตารางที่ หน้า

2.1 แสดงตัวอย่างหมายเลขแอดเดรสตัวอย่างที่ 1.....13

2.2 แสดงตัวอย่างหมายเลขแอดเดรสตัวอย่างที่ 2.....13

2.3 แสดงตัวอย่างหมายเลขแอดเดรสตัวอย่างที่ 3.....13

2.4 แสดงตัวอย่างหมายเลขแอดเดรสตัวอย่างที่ 4.....14

2.5 แสดงตัวอย่างหมายเลขแอดเดรสตัวอย่างที่ 5.....14

2.6 แสดงตัวอย่างหมายเลขแอดเดรสตัวอย่างที่ 6.....14

2.7 แสดงหมายเลขแอดเดรสของ Link-Local Address.....16

2.8 แสดงหมายเลขแอดเดรสของ Site-Local Address.....17

2.9 แสดงหมายเลขแอดเดรสของ Aggregatable Global Unicast Address.....17

2.10 แสดงหมายเลขแอดเดรสของ Multicast Address.....18

2.11 แสดงหมายของฟิลด์ Flag.....19

2.12 แสดงตัวอย่างของ Multicast Address.....19

2.13 แสดงหมายเลขแอดเดรสของ Loopback Address.....19

2.14 แสดงการเรียบเทียบคุณสมบัติอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 เทียบกับ
อินเตอร์เน็ตโพรโตคอลรุ่นที่ 4.....22

3.1 รายละเอียดการใช้งานฟิลด์.....28

5.1 แสดงคำสั่งอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 บน Windows XP.....39

6.1 แสดงข้อมูลทั้งหมดของ IPv4 (Pure) ของระบบ LAN.....43

6.2 แสดงข้อมูลทั้งหมดของ IPv6 (Pure) ของระบบ LAN.....44

6.3 แสดงข้อมูลทั้งหมดของ IPv4 (Dual Stack) ของระบบ LAN.....45

6.4 แสดงข้อมูลทั้งหมดของ IPv6 (Dual Stack) ของระบบ LAN.....46

6.5 แสดงข้อมูลทั้งหมดของ IPv4 (Pure) ของระบบ WAN.....48

6.6 แสดงข้อมูลทั้งหมดของ IPv6 (Pure) ของระบบ WAN.....49

6.7 แสดงข้อมูลทั้งหมดของ IPv4 (Dual Stack) ของระบบ WAN.....50

6.8 แสดงข้อมูลทั้งหมดของ IPv6 (Dual Stack) ของระบบ WAN.....51

6.9 แสดงข้อมูลทั้งหมดของ IPv6 (6to4 Tunneling).....53

สารบัญรูป

รูปที่ หน้า

2.1 แสดงระบบของขนาดแอดเดรส.....5

2.2 แสดงลักษณะการทำงาน Autoconfiguration.....6

2.3 แสดงลักษณะการทำงาน Renumbering.....7

2.4 แสดงลักษณะการทำงานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4.....7

2.5 แสดงลักษณะการทำงานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6.....8

2.6 เปรียบเทียบ Header ระหว่าง IPv4 และ IPv6.....9

2.7 แสดงฟิลด์ Flow Label.....9

2.8 แสดงโครงสร้างอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6.....11

2.9 แสดงสถาปัตยกรรมอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6.....15

2.10 แสดง Link-Local Address.....15

2.11 แสดง Site-Local Address.....16

2.12 แสดง Aggregatable Global Unicast Address.....17

2.13 แสดง Multicast Address.....18

2.14 เปรียบเทียบ Header ระหว่าง IPv4 และ IPv6.....20

3.1 แสดงการทำงานของโพรโตคอล RIPng ในช่วงเริ่มของการสร้างตารางเส้นทาง.....26

3.2 โครงสร้างเมสเสจของโพรโตคอล RIPng.....27

4.1 แสดงโครงสร้างของ Dual Stack.....30

4.2 แสดงลักษณะการทำงานของ Dual Stack.....30

4.3 แสดงการใช้งาน Dual Stack ของเราท์เตอร์.....31

4.4 IPv6 Packet Encapsulation.....32

4.5 การทำงานของ Manually Configured Tunnel.....33

4.6 การทำงานของ Fully Configured Tunnel.....34

4.7 การทำงานของ NAT-PT.....36

4.8 ขั้นตอนการเรียกดูเวบไซด์ IPv4 จากโหนด IPv6.....36

6.1 ระบบเครือข่ายภายในองค์กรแบบ LAN.....40

6.2 ระบบเครือข่ายภายในองค์กรแบบ WAN.....41

6.3 ลักษณะการเชื่อมต่อ IPv6 และ IPv4 แบบ Dual Stack.....41

6.4 ลักษณะการเชื่อมต่อ IPv6 และ IPv4 แบบ 6to4 Tunneling.....42

สารบัญรูป (ต่อ)

รูปที่ หน้า

6.5 กราฟแสดงความเร็วและระยะเวลาที่ทำการดึงข้อมูลของ IPv4 (Pure) ของระบบ LAN.....43
6.6 กราฟแสดงความเร็วและระยะเวลาที่ทำการดึงข้อมูลของ IPv6 (Pure) ของระบบ LAN.....44
6.7 กราฟแสดงความเร็วและระยะเวลาที่ทำการดึงข้อมูลของ IPv4 (Dual Stack) ของระบบ LAN 45
6.8 กราฟแสดงความเร็วและระยะเวลาที่ทำการดึงข้อมูลของ IPv6 (Dual Stack) ของระบบ LAN 46
6.9 กราฟแสดงความเร็วที่ทำการดึงข้อมูลของระบบ LAN ทั้งหมด.....47
6.10 กราฟแสดงระยะเวลาที่ทำการดึงข้อมูลของระบบ LAN ทั้งหมด.....47
6.11 กราฟแสดงความเร็วและระยะเวลาที่ทำการดึงข้อมูลของ IPv4 (Pure) ของระบบ WAN....48
6.12 กราฟแสดงความเร็วและระยะเวลาที่ทำการดึงข้อมูลของ IPv6 (Pure) ของระบบ WAN....49
6.13 กราฟแสดงความเร็วและระยะเวลาที่ทำการดึงข้อมูลของ IPv4 (Dual Stack) ของระบบ WAN.....50
6.14 กราฟแสดงความเร็วและระยะเวลาที่ทำการดึงข้อมูลของ IPv6 (Dual Stack) ของระบบ WAN.....51
6.15 กราฟแสดงความเร็วที่ทำการดึงข้อมูลของระบบ WAN ทั้งหมด.....52
6.16 กราฟแสดงระยะเวลาที่ทำการดึงข้อมูลของระบบ WAN ทั้งหมด.....52
6.17 กราฟแสดงความเร็วและระยะเวลาที่ทำการดึงข้อมูลของ IPv6 (6to4 Tunneling).....53
6.18 กราฟแสดงการเปรียบเทียบความเร็วระหว่างลักษณะการเชื่อมต่อ Dual Stack กับ 6to4 Tunneling.....54
6.19 กราฟแสดงการเปรียบเทียบระยะเวลาระหว่างลักษณะการเชื่อมต่อ Dual Stack กับ 6to4 Tunneling.....54

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

Internet และ Intranet ปัจจุบันมีการเติบโตและการใช้งานอย่างแพร่หลายมากขึ้น ดังนั้น ความต้องการที่จะใช้ระบบเครือข่ายที่มีศักยภาพสูง จึงเพิ่มขึ้นด้วยการเชื่อมต่อเครือข่ายอินเตอร์เน็ต ในปัจจุบันส่วนใหญ่อยู่บนพื้นฐานการทำงานของอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) ซึ่งทำให้การใช้งานจำนวนหมายเลข (IP Address) มีจำนวนมากขึ้นไม่เพียงพอต่อความต้องการในปัจจุบัน โดยการติดต่อสื่อสารกันนั้นจะต้องมีจำนวนหมายเลข (IP Address) ให้กับคอมพิวเตอร์ทุกเครื่องโดยที่ไม่ซ้ำกัน จึงได้มีการพัฒนาอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) เพื่อปรับปรุงโครงสร้างของอินเตอร์เน็ตให้สามารถรองรับหมายเลข (IP Address) จำนวนมากได้

อย่างไรก็ตามการใช้งานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) ก็ยังไม่แพร่หลาย ซึ่งภายในองค์กรปัจจุบันยังคงใช้อินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) จึงจำเป็นต้องทำการศึกษาโครงสร้าง และลักษณะการเชื่อมต่อของอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6)

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

วิทยานิพนธ์ฉบับนี้มุ่งหวังเพื่อศึกษาการใช้งานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) ภายในองค์กรว่าถ้าใช้งานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) จะทำให้ประสิทธิภาพในระบบเป็นอย่างไร ดังนั้นในวิทยานิพนธ์นี้จึงเสนอวิธีการเชื่อมต่ออินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) แบบต่างๆ เพื่อดูว่าการเชื่อมต่อแบบไหนมีประสิทธิภาพสูงสุด

โดยวัตถุประสงค์ของการศึกษา จะศึกษาถึงประสิทธิภาพในการใช้งานโดยทำการจำลองทดสอบดึงข้อมูลดังนี้

1. เทอมินอล (Terminal) โดยใช้อินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (IPv4) ส่งข้อมูลไปยังอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (IPv4) แบบ Pure

2. เทอมินอล (Terminal) โดยใช้อินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (IPv6) ส่งข้อมูลไปยังอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (IPv6) แบบ Pure

3. เทอมินอล (Terminal) โดยใช้อินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (IPv4) ส่งข้อมูลไปยังอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (IPv6) แบบ Dual Stack

4. เทอมินอล (Terminal) โดยใช้อินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (IPv6) ส่งข้อมูลไปยังอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (IPv4) แบบ Dual Stack

5. เทอมินอล (Terminal) โดยใช้อินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (IPv6) ส่งข้อมูลไปยังอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (IPv4) แบบ Tunneling (6to4)

จากนั้นจะนำผลลัพธ์ที่ได้มาเปรียบเทียบว่าแบบไหนทำให้ระบบเครือข่ายมีประสิทธิภาพเป็นอย่างไร ผลที่ได้นั้นสามารถเลือกลักษณะเชื่อมต่อให้เหมาะสมกับองค์กรและมีประสิทธิมากที่สุด

1.3 หลักการใหม่ในวิทยานิพนธ์

จะนำคุณสมบัติอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) นั้นมาทดสอบดูประสิทธิภาพ สมมุติว่าถ้านำอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) มาใช้งานภายในองค์กรกับโปรแกรมสำเร็จรูปต่างๆ จะทำให้ระบบมีประสิทธิภาพอย่างไร แล้วจะนำการเชื่อมต่ออย่างไรมาใช้งานให้ได้เหมาะสมกับองค์กรให้ได้ประสิทธิภาพสูงสุด

โดยลักษณะการเชื่อมต่อมีดังนี้

1. เทอมินอล (Terminal) โดยใช้อินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (IPv4) ส่งข้อมูลไปยังอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (IPv4) แบบ Pure

2. เทอมินอล (Terminal) โดยใช้อินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (IPv6) ส่งข้อมูลไปยังอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (IPv6) แบบ Pure

3. เทอมินอล (Terminal) โดยใช้อินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (IPv4) ส่งข้อมูลไปยังอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (IPv6) แบบ Dual Stack

4. เทอมินอล (Terminal) โดยใช้อินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (IPv6) ส่งข้อมูลไปยังอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (IPv4) แบบ Dual Stack

5. เทอมินอล (Terminal) โดยใช้อินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (IPv6) ส่งข้อมูลไปยังอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (IPv4) แบบ Tunneling (6to4)

1.4 เปรียบเทียบกับหลักการที่มีอยู่เดิม

โดยลักษณะการทดสอบอินเตอร์เน็ตอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) โดยทั่วไปจะทำการเซ็ตอุปกรณ์ให้สามารถใช้งานโปรแกรมประยุกต์ต่าง ๆ หรือไม่ก็เซ็ตให้ทำการเชื่อมต่อให้สามารถใช้งานได้ไม่สนใจประสิทธิภาพว่าแบบไหนที่มีประสิทธิภาพดีที่สุด

1.5 ขอบเขตการทำวิทยานิพนธ์

ขอบเขตในการทำวิทยานิพนธ์นี้เป็นการวิเคราะห์ โครงสร้างการเชื่อมต่ออินเตอร์เน็ต โพรโต คอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) กับ อินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) เพื่อตรวจสอบประสิทธิภาพภายในองค์กร

1.6 รายละเอียดในวิทยานิพนธ์

วิทยานิพนธ์ฉบับนี้ได้แบ่งเนื้อหาออกเป็น 7 บทด้วยกันคือ

บทที่ 1 กล่าวถึงความเป็นมาของงานวิจัย ความมุ่งหมายและวัตถุประสงค์ ทฤษฎีที่ใช้ ขอบเขตของการวิจัย

บทที่ 2 กล่าวถึงทฤษฎีพื้นฐานที่ใช้ในการวิจัย และพื้นฐานของอินเตอร์เน็ตโพรโตคอล รุ่นที่ 6 ซึ่งประกอบคุณสมบัติ, โครงสร้าง, ชนิด และการเปรียบเทียบคุณสมบัติอินเตอร์เน็ต โพร โตคอลรุ่นที่ 6 กับ คุณสมบัติอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4

บทที่ 3 กล่าวถึงการเลือกเส้นทางอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Routing on IPv6)

บทที่ 4 กล่าวถึงการลักษณะการเชื่อมต่ออินเตอร์เน็ตโพรโตคอลรุ่นที่ 6

บทที่ 5 กล่าวถึงการเตรียมความพร้อมของอุปกรณ์

บทที่ 6 กล่าวถึงแบบจำลองและการวิเคราะห์ผลการทำงาน

บทที่ 7 เป็นบทสรุปผลการวิจัยและข้อเสนอแนะ

บทที่ 2
ความรู้พื้นฐานเกี่ยวกับอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6

ในหัวข้อนี้จะกล่าวถึงทฤษฎีพื้นฐานต่างๆ ที่เกี่ยวข้องในการวิจัย และพื้นฐานของความรู้พื้นฐานเกี่ยวกับอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) ซึ่งเนื้อหาในบทนี้จะกล่าวถึงคุณสมบัติ, โครงสร้าง, ชนิดของอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 และเปรียบเทียบคุณสมบัติอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) กับ อินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) ซึ่งเนื้อหาทั้งหมดนี้จำเป็นสำหรับการศึกษา

2.1 คุณสมบัติอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6 Features)

กลไกสำคัญในการทำงานของอินเตอร์เน็ตคืออินเทอร์เน็ตโพรโตคอล (Internet Protocol) ซึ่งประกอบด้วยส่วนสำคัญ คือ หมายเลขอินเตอร์เน็ตแอดเดรส หรือ ไอพีแอดเดรส (IP Address) ที่ใช้ในการอ้างอิงเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายต่างๆ บนอินเทอร์เน็ตทั่วโลกเปรียบเสมือนการใช้งานโทรศัพท์ในการติดต่อสื่อสารกัน จะต้องมีเลขหมายเบอร์โทรศัพท์เพื่อให้อ้างอิงผู้รับสายได้ คอมพิวเตอร์ทุกเครื่องในอินเตอร์เน็ตก็ต้องมีหมายเลขไอพีแอดเดรสที่ไม่ซ้ำกับใคร

2.1.1 ขนาดแอดเดรส (Larger Address Space)

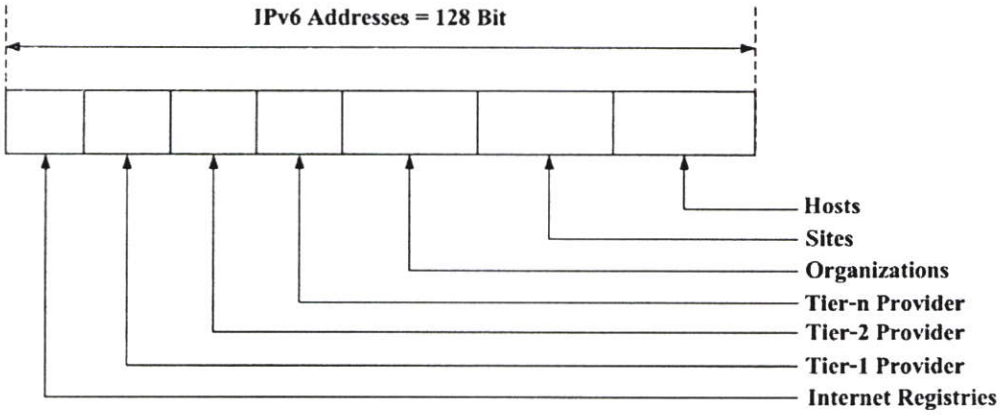
ขนาดแอดเดรสที่เพิ่มมากขึ้น ซึ่ง IPv4 มีแอดเดรสขนาด 32 Bit และเนื่องจากการใช้อินเทอร์เน็ตที่มีการเติบโตมากขึ้นจึงทำให้ IPv4 ไม่เพียงพอกับการใช้งาน องค์กรต้องมีการจัดสรรเกี่ยวกับ IPv4 ที่เริ่มขาดแคลนและมีค่าใช้จ่ายที่สูงขึ้น สิ่งที่มองเห็นได้ชัดของการเปลี่ยนแปลง IPv4 ไปเป็น IPv6 ก็คือ การเพิ่มขนาดของแอดเดรสจาก 32 Bit เป็น 128 Bit

IPv4 Address (32 Bit)	**IPv6 Address (128 Bit)**
ddd.ddd.ddd.ddd	**hhhh.hhhh.hhhh.hhhh.hhhh.hhhh.hhhh.hhhh**
d = Decimal (0-9)	**h = Hex (0-F)**

โดยIPv4 จะมีจำนวนหมายเลข(IP Address) 2^{32}หรือ 4,294,967,296 ซึ่ง IPv6 จะมีจำนวนหมายเลข(IP Address) 3.4×10^{38}หรือ 340,282,366,920, 938,463,463,374,607,431,768,211,456

2.1.2 ระดับของขนาดแอดเดรส (Level Addressing Hierarchy)

โดยเมื่อขนาดแอดเดรสมีนาดเพิ่มมากขึ้นจะมีการใช้การแบ่งระดับของขนาดแอดเดรส ซึ่งแต่ระดับจะช่วยในการจัดขนาดแอดเดรส

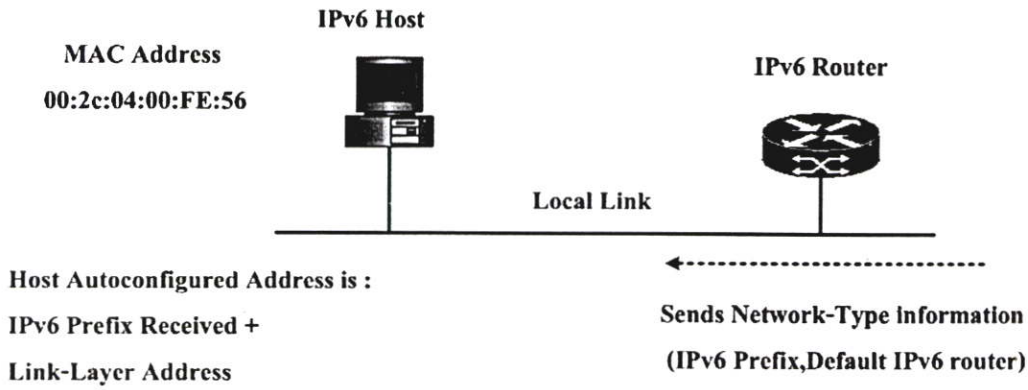


รูปที่ 2.1 แสดงระดับของขนาดแอดเดรส (Level Addressing Hierarchy)

2.1.3 Autoconfiguration

เครื่องโฮสต์หรือโหนดไม่ว่าจะเป็นระบบปฏิบัติการอะไรก็ตาม จำเป็นต้องมีการ Enable Featured ของ IPv6 คือ Autoconfiguration ขึ้นมาก่อนที่จะได้ไอพีแอดเดรสอย่างอัตโนมัติ ซึ่งปกติแล้วเมื่อเครื่องได้มีการ Enable IPv6 จะมีหมายเลข Link Local Address อยู่แล้ว สำหรับหมายเลขไอพีแอดเดรสแบบ Global จะได้หมายเลขเน็ตเวิร์คแอดเดรสจากเครื่องเราท์เตอร์ โดยเราท์เตอร์จะส่ง RA หรือ Router Advertisement Packet ซึ่งมี Prefix อยู่ออกไปให้เครื่องโฮสต์ในระบบเน็ตเวิร์ค แต่ถ้าระบบเครื่องที่เราใช้ไม่ได้อยู่ในองค์กรใหญ่ๆหรืออยู่ในระบบเน็ตเวิร์คใหญ่ๆ ก็ไม่จำเป็นที่จะมีเครื่องเราท์เตอร์อาจจะใช้หมายเลข Link Local Address ในการติดต่อกัน

เครื่องเราท์เตอร์จะส่ง RA ออกไปในเน็ตเวิร์คเป็นระยะๆ ซึ่งภายใน RA จะมีหมายเลข Prefix และมีข้อมูลอื่นๆที่เกี่ยวข้องอย่างเช่น ข้อมูลที่บอกเราท์เตอร์ตัวอื่นที่ติดต่อกันอยู่ว่า ถ้าหากต้องการจะออกไปในอินเตอร์เน็ตจะสามารถออกไปได้ยังไง อาจจะบอกว่าตัวมันเองเป็นเราท์เตอร์ที่ดีหรือไม่เป็นตัวจริงที่ ควรใช้งานหรือควรที่จะเราท์เตอร์ตัวอื่นในการติดต่ออินเตอร์เน็ต เป็นต้น ซึ่งการส่ง RA จะมีการทำงานเป็นช่วงๆ ของเวลา



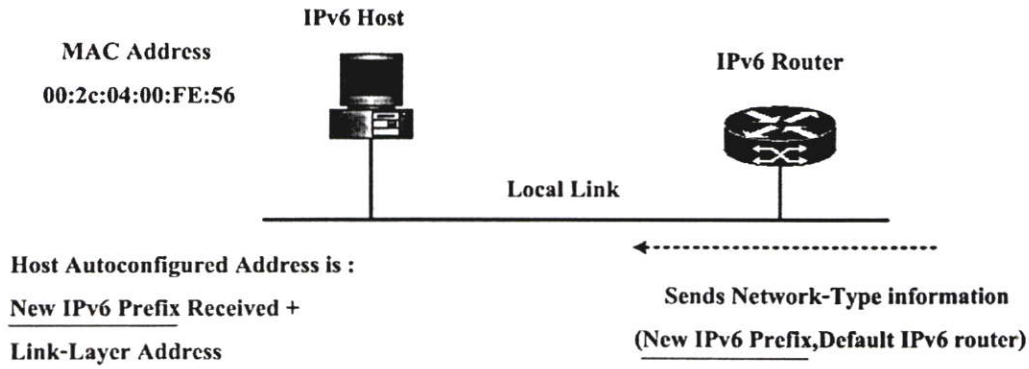
รูปที่ 2.2 แสดงลักษณะการทำงาน Autoconfiguration

อีก Mechanism ที่ต้องมีนอกจากเราท์เตอร์จะเป็นตัวส่งข้อมูลแล้ว เมื่อโหนดหรือโฮสต์ได้บูตขึ้นมาทุกเครื่องต้องการหมายเลขไอพีแอดเดรส วิธีการจัดการคือเครื่องโฮสต์จะมีระยะเวลาช่วงหนึ่งสำหรับรอรับ RA ที่เครื่องเราท์เตอร์จะต้องส่งออกมาแน่นอน แต่จะส่งออกเป็นช่วงๆ เวลาในกรณีที่แย่ที่สุดคือเราท์เตอร์พึ่งส่ง RA ออกมา สมมติว่าเราท์เตอร์ จะส่ง RA ทุกๆ 10 นาที เครื่องโฮสต์จะต้องรออีก 10 นาที ถึงจะได้รับหมายเลขไอพีแอดเดรส ซึ่งอาจจะช้าดังนั้นมีขบวนการโดยให้รอเป็นระยะเวลาสั้นๆ ถ้าหากเครื่องโฮสต์ยังไม่ได้รับหมายเลขไอพีแอด เดรสจะส่งข้อมูลไปร้องขอหมายเลขเน็ตเวิร์คแอดเดรสจากเครื่องเราท์เตอร์ ซึ่งแน่นอนเมื่อมีการร้องขอเครื่องเราท์เตอร์จะส่งข้อมูลตอบกลับไป แต่ถ้าไม่มีการร้องขอเราท์เตอร์ก็จะส่ง RA ตามช่วงเวลาของมัน

กรณีที่เครื่องในระบบเน็ตเวิร์คเปิดใช้งานพร้อมกัน ในการร้องขอหมายเลขเน็ตเวิร์คแอดเดรสนั้นจะไม่ส่งไปร้องขอพร้อมกัน แต่จะมีขบวนการจัดการเวลาสำหรับรอเพื่อร้องขอ RA โดยการสุ่มเวลาให้แต่ละเครื่องซึ่งจะไม่เท่ากัน เพราะจำเป็นต้องมีเครื่องใดเครื่องหนึ่งร้องขอไปก่อน เมื่อมีการร้องขอไปยังเราท์เตอร์ เราท์เตอร์ของ IPv6 จะมีการตอบกลับโดยการส่งข้อมูลออกไปแบบ Multicast ต่างจาก IPv4 ซึ่งเป็น Broadcast เพราะ IPv6 ไม่มีการส่งข้อมูลแบบ Broadcast เราท์เตอร์ส่ง RA ออกไปแบบ Multicast ทำให้เครื่องทุกเครื่องได้รับ RA ซึ่งมี Prefix พร้อมๆ กัน จึงทำให้เครื่องทุกเครื่องได้รับไอพีแอดเดรสอัตโนมัติพร้อมกัน

2.1.4 Renumbering

ในอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) นั้นจะมีระบบ Renumbering คือการเปลี่ยน IP Address โดยอัตโนมัติ ซึ่งในระบบอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4)ไม่มี ถ้าจะเปลี่ยนจำเป็นจะต้องเปลี่ยนเอง ซึ่งจะทำให้ยุ่งยากถ้าเน็ตเวอร์มีขนาดใหญ่

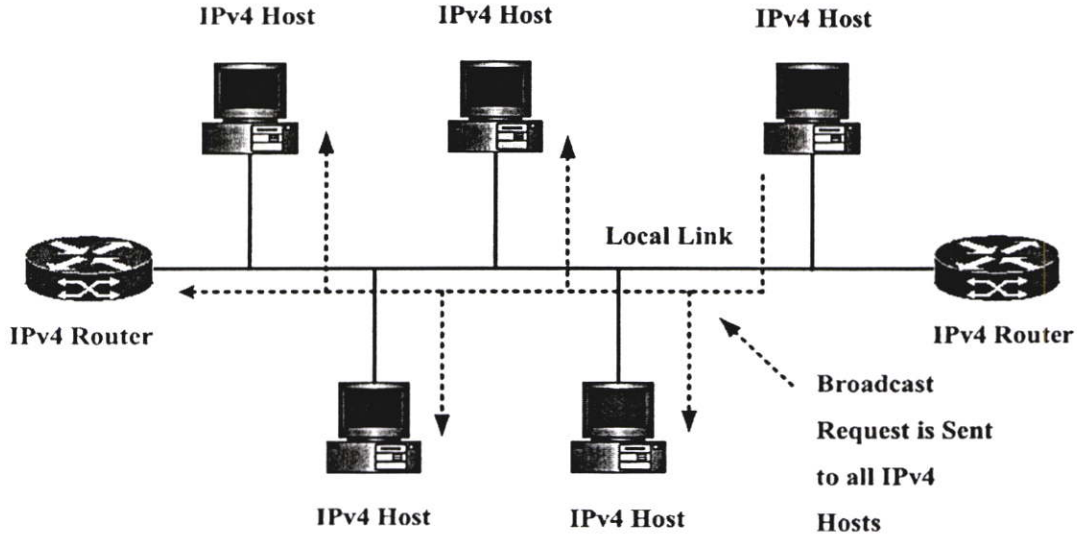


รูปที่ 2.3 แสดงลักษณะการทำงาน Renumbering

2.1.5 Multicast Use

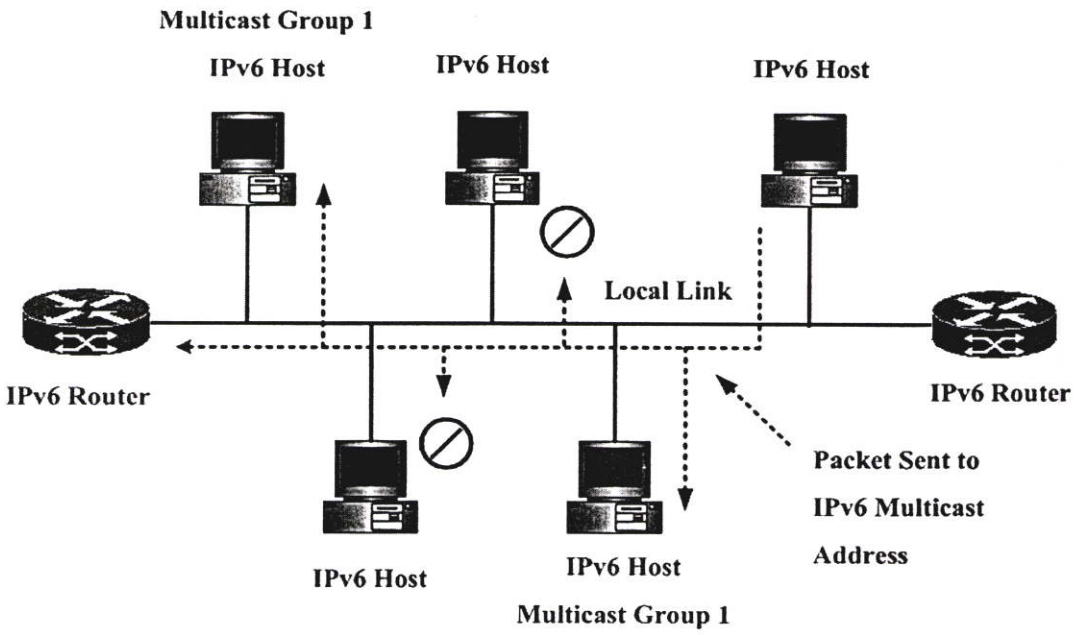
โดยในระบบระบบอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) นั้นจะใช้ระบบ Multicast ซึ่งในระบบอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; ;IPv4) ซึ่งใช้ระบบ Broadcast ซึ่งอธิบายแยกดังต่อไปนี้

ลักษณะการทำงานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) นั้นจะทำการส่ง ARP Request Broadcast ออกไปที่ Client ทุกๆ Client เพื่อสอบถามว่าใครรู้ IP Address นี้บ้าง โดยจะทำการส่งไปทั้งระบบเครือข่ายวงนั้นซึ่งจะทำให้เปลือง Bandwidth และจะทำการเก็บ MAC Address สัมพันธ์กับ IP Address ไว้ในเครื่องนั้น ดังนั้นการทำงานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4;IPv4) จะใช้ ARP และ Broadcast



รูปที่ 2.4 แสดงลักษณะการทำงานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (IPv4)

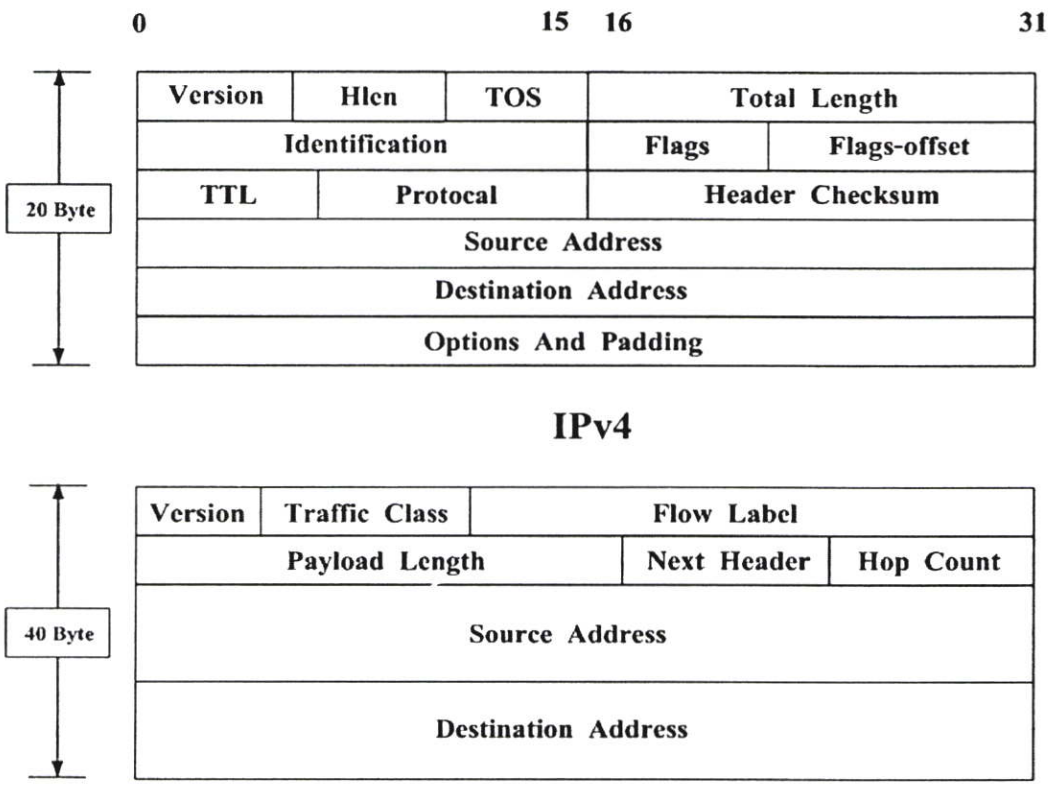
แต่ลักษณะการทำงานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6;IPv6) นั้นไม่ได้ใช้ ARP และ Broadcast แต่ใช้ ICMPv6 และ Multicast โดยจะทำการติดต่อสื่อสารระหว่าง Client ที่ต้องการติดต่อเท่านั้นซึ่งจะทำให้สามารถลด Bandwidth ได้



รูปที่ 2.5 แสดงลักษณะการทำงานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (IPv6)

2.1.6 ประสิทธิภาพของ Header (Efficient Header)

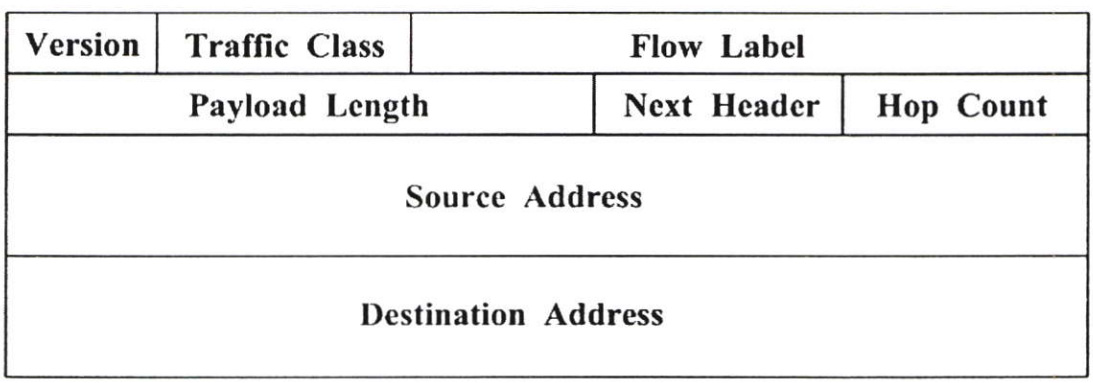
จากรูปที่ 2.6 จะเห็นว่าอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (IPv6) จะมี ขนาด Header ใหญ่กว่าอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (IPv4) ซึ่ง อินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (IPv6) จะมี Header 40 Byte แต่อินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (IPv4) มีขนาด Header 20 Byte



รูปที่ 2.6 เปรียบเทียบ Header ระหว่าง IPv4 และ IPv6

2.1.7 Flow Label

ในโครงสร้างอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) ดังรูปที่ 2.7 จะมีฟิลด์ Flow Label ซึ่งในอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) ไม่มี โดยส่วนมากฟิลด์นี้จะอยู่ใน MPLS



รูปที่ 2.7 แสดงฟิลด์ Flow Label

2.1.8 Extension Header

Extended Header ทำให้อินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) มี Extended Header หลายๆ แบบ แต่ละแบบก็เอาไว้ใช้ทำงานเฉพาะอย่างเพียงงานเดียว ใน 1 Packet เราสามารถใช้ Extended Header ได้มากกว่า 1 อัน ดังนั้น เราจึงขอ Service จาก อินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) ได้มากกว่า 1 อย่าง IPv6 Specification ล่าสุดกำหนดให้มี Extended Header อยู่ 6 แบบ ทุกแบบจะขึ้นต้นด้วยฟิลด์ "Next Header" เสมอ เพื่อระบุว่า Extended Header อันถัดเป็นชนิดไหน

2.1.7.1 Hop-by-Hop Options

2.1.7.2 Routing

2.1.7.3 Fragment

2.1.7.4 Authentication

2.1.7.5 Encapsulated Security Payload

2.1.9 Mobility

Mobility มีความสำคัญมาก ซึ่งถ้าใครต้องการใช้ Web, E-mail, และใช้เน็ตเวอร์นอกบ้านนั้น จำเป็นจะต้องใช้เทคโนโลยีไร้สาย เช่น 802.11b และ 3G การใช้อินเตอร์เน็ตโพรโตคอล รุ่นที่ 6 (Internet Protocol Version 6; IPv6) จะทำให้ IP Address สามารถจ่าย IP Address ได้เลย ซึ่งอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) ไม่สามารถทำได้เพราะติดว่าขนาด IP Address มีจำนวนจำกัด

2.1.10 Security

ในปัจจุบันมีการคำนึงถึง Security เป็นจำนวนมาก อินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) ก็เช่นเดียวกันมีการคำนึงเป็นจำนวนมาก ส่วนอินเตอร์เน็ตโพรโตคอล รุ่นที่ 6 (Internet Protocol Version 6; IPv6) นั้นก็มี Security พอสมควรก็เกี่ยวกับการใช้ IPSec ซึ่งเป็นโปรโตคอลในการรองรับความปลอดภัยที่จะส่งข้อมูลผ่านในระบบเครือข่าย ในส่วนต่างๆ ที่กล่าวมานั้น IPv6 กับ IPv4 นั้นยังคงไม่แตกต่างกันมากชัดเจน นอกจากเรื่องที่มีจำนวน IP Address ที่มีจำนวนมากขึ้น ตรงส่วนนี้นี่เอง IPSec ซึ่งเป็นโปรโตคอลที่แยกออกมาทำให้เห็นเป็นข้อแตกต่างที่ชัดเจนมากระหว่างอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) กับ อินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) ข้อแตกต่างก็คือมีตัว Security อยู่และจะต้องมีการ Implement อยู่บนอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) ซึ่งตรงจุดนี้นั่นเองทำให้การส่งผ่านข้อมูลระหว่างเครือข่ายมีความปลอดภัยในระดับสูง

ในปัจจุบันมีการนำ IPSec มาใช้มากขึ้นแล้ว ซึ่งระหว่างที่เราใช้อินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (IPv4) อยู่นั้นเราสามารถนำ อินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) ไป Implement ใน อินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) ได้ ปัญหาที่เกิดขึ้นก็คือการที่ต้องมีการ Encryption และกระบวนการอีกอย่างหนึ่งที่สำคัญไม่แพ้กัน คือในส่วนของ Key Management คือในการที่จะบอกว่าใน Key อะไรในการเข้ารหัส ซึ่งการใช้ Key นั้นมีหลายประเภทและมากเหลือเกิน ปัจจุบันยังไม่มีการตกลงกันอย่างชัดเจนในแต่ในระหว่างนี้จะให้ใช้ตัว IKE ไปก่อนในการที่จะจัดการเรื่อง Key ในการเข้ารหัสโปรโตคอลอีกตัวหนึ่งก็คือ SSL (Secure Socket Layer) ที่นำมาใช้เป็นการชั่วคราวเช่นเดียวกันบนอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (IPv4)

2.2 โครงสร้างอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6)

จากรูปที่ 2.8 แสดงโครงสร้างอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 ซึ่งมีส่วนประกอบหลักอยู่ 2 ส่วน คือ ส่วนของ (Header) และส่วนของข้อมูล (Data)

<table>
<tr><td>Version</td><td>Traffic Class</td><td colspan="2">Flow Label</td></tr>
<tr><td colspan="2">Payload Length</td><td>Next Header</td><td>Hop Count</td></tr>
<tr><td colspan="4">Source Address</td></tr>
<tr><td colspan="4">Destination Address</td></tr>
</table>

รูปที่ 2.8 แสดงโครงสร้างอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6)

- ฟิลด์ Version : ระบุเวอร์ชันของ IP ที่ใช้ในการสร้าง IP datagram ในฟิลด์นี้จะมีขนาด 4Bit ซึ่งปกติจะเซ็ทเป็น 0100 ในระบบของเลขฐานสอง ซึ่งแสดงถึงเวอร์ชั่น เช่น อินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) ซึ่งเป็นเวอร์ชันที่ใช้อยู่ในปัจจุบัน แสดงให้เห็นถึงเวอร์ชันในแบบต่างๆ ที่สัมพันธ์กันกับ RFC

- ฟิลด์ Type of Service (TOS) : มีขนาด 8 Bit ใช้สำหรับบ่งบอกถึงคุณลักษณะหรือรูปแบบการให้การบริการที่แพ็กเก็ต IP ต้องการ ในฟิลด์นี้สามารถแบ่งออกได้เป็น 2 ส่วน คือ ส่วนของ Precedence และส่วนของ TOS ส่วนของ Precedence นั้นมีจำนวน 3 Bit ใช้สำหรับจัดลำดับความสำคัญของแพ็กเก็ตซึ่งมีได้ 8 ระดับในส่วนของ TOS มีไว้เพื่อใช้ในการเลือกการบริการในการส่งมอบแพ็กเก็ตในรูปของDelay Throughput Reliability และ Monetary Cost

- Flow Label ใช้ระบุ End-to-end traffic flow ระหว่างต้นทางกับปลายทาง ใน Application นึงสามารถสร้าง Flow ได้หลายๆ อัน อย่างเช่น Video Conference เราสามารถแยก Flow ของภาพและเสียงออกจากกันได้ แม้ว่าจะเปิด Socket ในการทำงานเพียง Socket เดียว

- ฟิลด์ Total Length : มีขนาด 16 Bit ใช้สำหรับระบุขนาดของอินเตอร์เน็ตโพรโตคอลทั้งหมดซึ่งรวม Header ด้วย ขนาดของอินเตอร์เน็ตโพรโตคอลที่ใหญ่ที่สุดมีค่าเท่ากับ 65,535 Byte

- ฟิลด์ Hop Limit : มีขนาด 8 Bit มีหน้าที่กำหนดจำนวนเราท์เตอร์สูงสุดที่อินเตอร์เน็ตโพรโตคอล สามารถเดินทางผ่านได้ หรือ กล่าวในอีกนัยหนึ่งได้ว่าเป็นการกำหนดอายุของเส้นทางที่อนุญาตให้อยู่ในเครือข่ายได้ ขั้นตอนในการทำงาน คือ เมื่อ Host ต้นทางทำการส่ง ออกไปจะตั้งค่าเริ่มต้นให้กับฟิลด์ TTL ค่าหนึ่ง (โดยทั่วไปใช้ 32 หรือ 64) ทุกครั้งที่เดินทางผ่านเราท์เตอร์ตัวหนึ่งค่าของ TTL จะถูกปรับลดลงหนึ่งหน่วยหากเมื่อใดเราท์เตอร์พบที่ค่า TTL ลดลงจนเป็น 0 เราท์เตอร์จะตัดนั้นทิ้งไปพร้อมกับแจ้งให้ Host ต้นทางทราบการทำเช่น นี้จะทำให้สามารถป้องกันอินเตอร์ เน็ตโพรโตคอลที่รับส่งผิดพลาดได้

- ฟิลด์ Header Checksum : มีขนาด 16 Bitเป็นฟิลด์ที่ทำหน้าที่ตรวจสอบความถูกต้องของอินเตอร์เน็ตโพรโตคอล Header โดยมีลักษณะการทำงานดังนี้ เมื่อ Host ต้นทางทำการสร้างจะคำนวณค่า Header Checksum โดยนำ Header ทีละ16 Bit มาบวกกันแบบ One's component จากนั้นนำผลที่ได้มาทำ One's component อีกครั้ง จึงจะได้เป็นค่าที่บรรจุลงใน Header checksum โดยที่ด้านรับปลายทางจะตรวจสอบความผิดพลาดของ Header โดยนำ Header ทีละ 16 บิท มาบวกกับค่าในฟิลด์ Header checksum แบบ One's component หากผลลัพธ์ที่ได้มีค่าเป็นหนึ่งทั้งหมด แสดงว่าไม่มีความผิดพลาดเกิดขึ้น หากไม่ใช่ก็แสดงว่ามีความผิดพลาดเกิดขึ้นกับ header ในกรณีนี้อินเตอร์เน็ตโพรโตคอลจะถูกตัดทิ้งโดยไม่มีการแจ้งความผิดพลาดที่เกิดขึ้น ซึ่งโพรโทคอลในชั้นที่สูงกว่าต้องตรวจสอบปัญหาด้วยตัวเอง

- ฟิลด์ Source และ Destination Addresses : คือ IP address ของต้นทางและ IP address ของปลายทางมีขนาด 32 Bit

2.3 รูปแบบการเขียนหมายเลขแอดเดรสของอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Format of Internet Protocol Version 6; IPv6)

ขนาดแอดเดรสของ IPv6 มีขนาด 128 Bit ก็ประมาณ $3.4x10^{38}$ ซึ่งเยอะมากๆ แต่เราไม่สามารถใช้งานได้ทั้งหมด จะมีบางส่วนที่เสียไปเนื่องจากการจัดระเบียบของขนาดแอดเดรส นักวิจัยคำนวณออกมาได้ว่าขนาดแอดเดรสที่เราใช้ได้จริง ๆ จะอยู่ระหว่าง $8x10^{17}$ ถึง $2x10^{33}$ ซึ่งก็ยังมีขนาดใหญ่เพราะอย่างต่ำที่สุดเราจะมีขนาดแอดเดรส $8x10^{17}$ addresses ถ้าเอามาเฉลี่ยด้วยของพื้นที่ของโลกก็จะได้ประมาณ 1,546 addresses/sq.m เนื่องจากขนาดแอดเดรสมันยาวมากจะเขียนเป็น

dotted decimal notation เหมือน IPv4 ก็คงต้องคั่นด้วยจุดเป็นสิบๆ จุด แล้วก็คงไม่มีใครจะจำ IPv6 address กันอีกแล้ว ดังนั้น IPv6 จึงเขียนเป็นเลขฐานสิบหกโดยแบ่งเป็นส่วนๆ ละ 16-Bit (เท่ากับเลขฐานสิบหก 4 หลัก) Address นึงจึงมีทั้งหมด 8 กลุ่ม แต่ละกลุ่มคั่นด้วยเครื่องหมาย Colon อย่างเช่น

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

ซึ่งมีเงื่อนไขการเขียนย่อดังต่อไปนี้

- หากมีเลขศูนย์ด้านหน้าของกลุ่มใดสามารถละไว้ได้
- หากกลุ่มใดเป็นเลขศูนย์ทั้ง 4 ตัว (0000) สามารถเขียนแทนด้วย "0"
- หากกลุ่มใดกลุ่มหนึ่ง (หรือหลายกลุ่มที่ตำแหน่งติดกัน) เป็นเลขศูนย์ทั้งหมดสามารถละไว้ได้ โดยใช้เครื่องหมาย "::" แต่สามารถทำลักษณะนี้ได้ตำแหน่งเดียวเท่านั้น เพื่อไม่ให้เกิดความสับสน

ดังตัวอย่างต่อไปนี้

ตารางที่ 2.1 แสดงตัวอย่างการเขียนหมายเลขแอดเดรสตัวอย่างที่ 1

รูปแบบ	หมายเลขแอดเดรส
รูปแบบปกติ	0000:0000:0000:0000:0000:0000:0000:0000
รูปแบบย่อแบบที่ 1	0:0:0:0:0:0:0:0
รูปแบบย่อแบบที่ 2	::

ตารางที่ 2.2 แสดงตัวอย่างการเขียนหมายเลขแอดเดรสตัวอย่างที่ 2

รูปแบบ	หมายเลขแอดเดรส
รูปแบบปกติ	3FFE:0000:0000:0000:1010:2AA0:0000:0001
รูปแบบย่อแบบที่ 1	3FFE:0:0:0:1010:2AA0:0:1
รูปแบบย่อแบบที่ 2	3FFE::1010:2AA0:0:1

ตารางที่ 2.3 แสดงตัวอย่างการเขียนหมายเลขแอดเดรสตัวอย่างที่ 3

รูปแบบ	หมายเลขแอดเดรส
รูปแบบปกติ	3FF0:0000:0000:0000:0000:0000:0000:0001
รูปแบบย่อแบบที่ 1	3FF0:0:0:0:0:0:0:1
รูปแบบย่อแบบที่ 2	3FF0::1

ตารางที่ 2.4 แสดงตัวอย่างการเขียนหมายเลขแอดเดรสตัวอย่างที่ 4

รูปแบบ	หมายเลขแอดเดรส
รูปแบบปกติ	FE80:0000:0000:0000:0001:0000:0000:0001
รูปแบบย่อแบบที่ 1	FE80:0:0:0:1:0:0:1
รูปแบบย่อแบบที่ 2	FE80::10:0:1

ตารางที่ 2.5 แสดงตัวอย่างการเขียนหมายเลขแอดเดรสตัวอย่างที่ 5

รูปแบบ	หมายเลขแอดเดรส
รูปแบบปกติ	2001:0002:000A:0008:1010:2AA0:0008:0001
รูปแบบย่อแบบที่ 1	2001:2:A:8:1010:2AA0:8:1
รูปแบบย่อแบบที่ 2	----

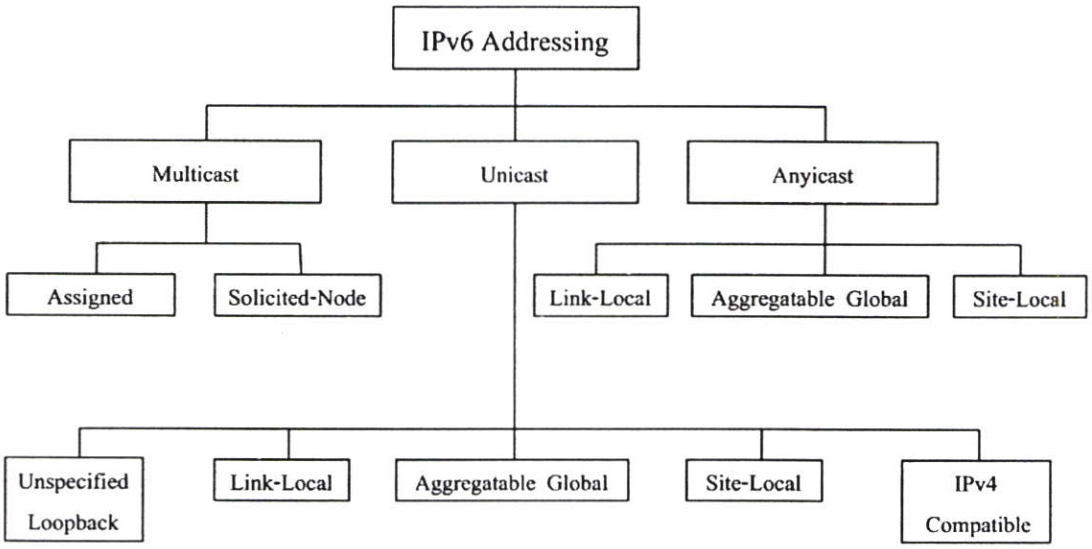
ตารางที่ 2.6 แสดงตัวอย่างการเขียนหมายเลขแอดเดรสตัวอย่างที่ 2

รูปแบบ	หมายเลขแอดเดรส
รูปแบบปกติ	FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
รูปแบบย่อแบบที่ 1	----
รูปแบบย่อแบบที่ 2	----

2.4 ชนิดของอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6 Address Types)

ในหัวข้อนี้จะกล่าวถึงชนิดของอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6 Address Types) ซึ่งจะถูกอธิบายมาตรฐาน RFC 2373

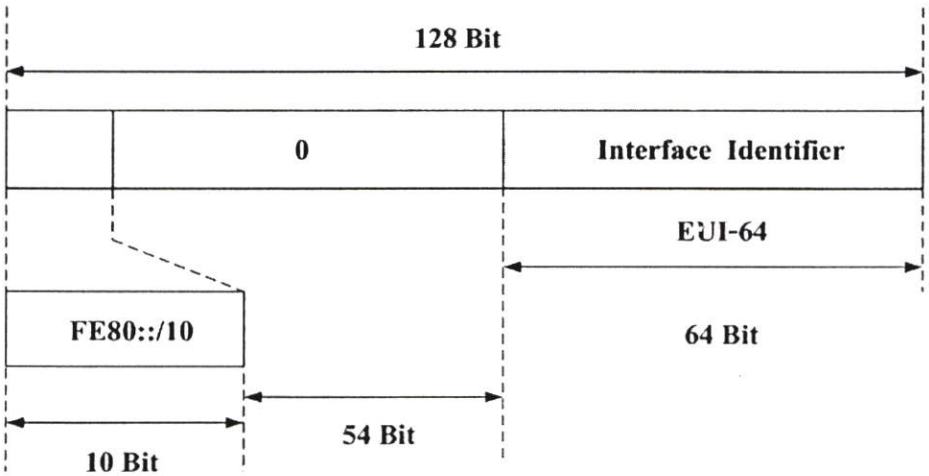
จากรูปที่ 2.9 ชนิดอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) จะถูกแบ่งเป็น 3 ส่วนใหญ่ คือ Multicast, Unicast และ Anycast



รูปที่ 2.9 แสดงสถาปัตยกรรมอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6 Architecture)

2.4.1 Link-Local Address

Link-Local Address เป็น Unicast เมื่อมีการเปิดใช้งานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) ที่ Client จะมี IP address อัตโนมัติ โดย Link-Local Address มี Prefix เป็น FE80::/10 ซึ่งจะใช้รวมกับ MAC Address ของ การ์ด LAN มีชื่อว่า (EUI–64) ดังรูปที่ 2.10



รูปที่ 2.10 แสดง Link-Local Address

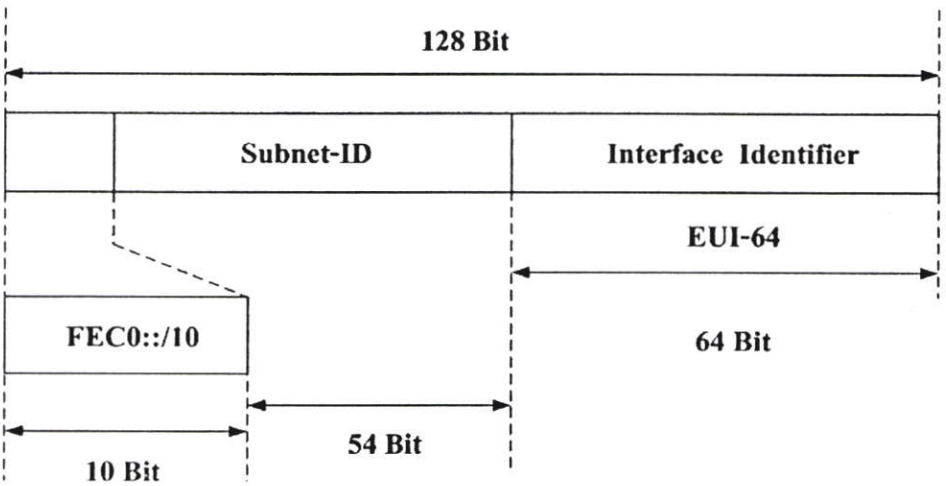
ตารางที่ 2.7 แสดงหมายเลขแอดเดรสของ Link-Local Address

รูปแบบ	หมายเลขแอดเดรส
รูปแบบปกติ	FE80:0000:0000:0000:0000:0000:0000:0000/10
รูปแบบย่อแบบที่ 1	FE80:0:0:0:0:0:0:0/10
รูปแบบย่อแบบที่ 2	FE80::/10

2.4.2 Site-Local Address

Site-Local Address เป็น Unicast เมื่อมีการเปิดใช้งานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) ที่ Client จะไม่มี IP address ซึ่งจำเป็นต้อง Assign

Site-Local Address เปรียบเสมือนเป็น Private Address ในอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) เช่น 10.0.0.0/8, 172.16.0.0/12 และ 192.168.0.0/16 โดย Site-Local Address มี Prefix เป็น FEC0::/10



รูปที่ 2.11 แสดง Site-Local Address

ตัวอย่าง Subnet ของ Site-Local Address ดังตัวอย่างต่อไปนี้

Subnet 1 → FEC0:0:0:0001::/64
Subnet 2 → FEC0:0:0:0002::/64
Subnet 3 → FEC0:0:0:0003::/64
Subnet 4 → FEC0:0:0:0004::/64
Subnet 5 → FEC0:0:0:0005::/64
Subnet 6 → FEC0:0:0:0006::/64
Subnet 7 → FEC0:0:0:0007::/64

สำนักหอสมุดกลาง พระจอมเกล้าลาดกระบัง

Subnet 8 → FEC0:0:0:0008::/64

Subnet 9 → FEC0:0:0:0009::/64

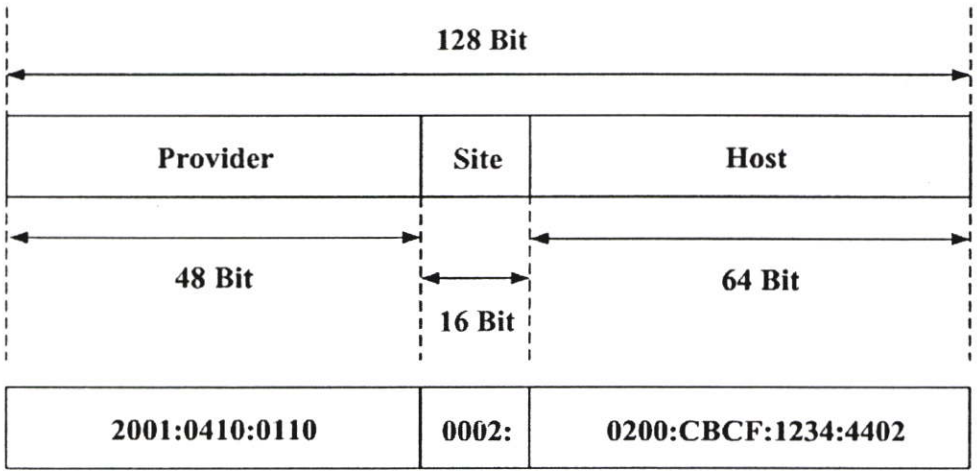
Subnet10 → FEC0:0:0:000A::/64

ตารางที่ 2.8 แสดงหมายเลขแอดเดรสของ Site-Local Address

รูปแบบ	หมายเลขแอดเดรส
รูปแบบปกติ	FEC0:0000:0000:0000:0000:0000:0000:0000/10
รูปแบบย่อแบบที่ 1	FEC0:0:0:0:0:0:0:0/10
รูปแบบย่อแบบที่ 2	FEC0::/10

2.4.3 Aggregatable Global Unicast Address

Aggregatable Global Unicast Address เป็น Unicast ซึ่งถ้าเปรียบเทียบกับอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) นั้นก็คือ Public Address โดย IP Address ชุดนี้จะถูกจัดสรรโดย IANA ซึ่งจะถูกแบ่งเป็นประเทศ ๆ ไป



รูปที่ 2.12 แสดง Aggregatable Global Unicast Address

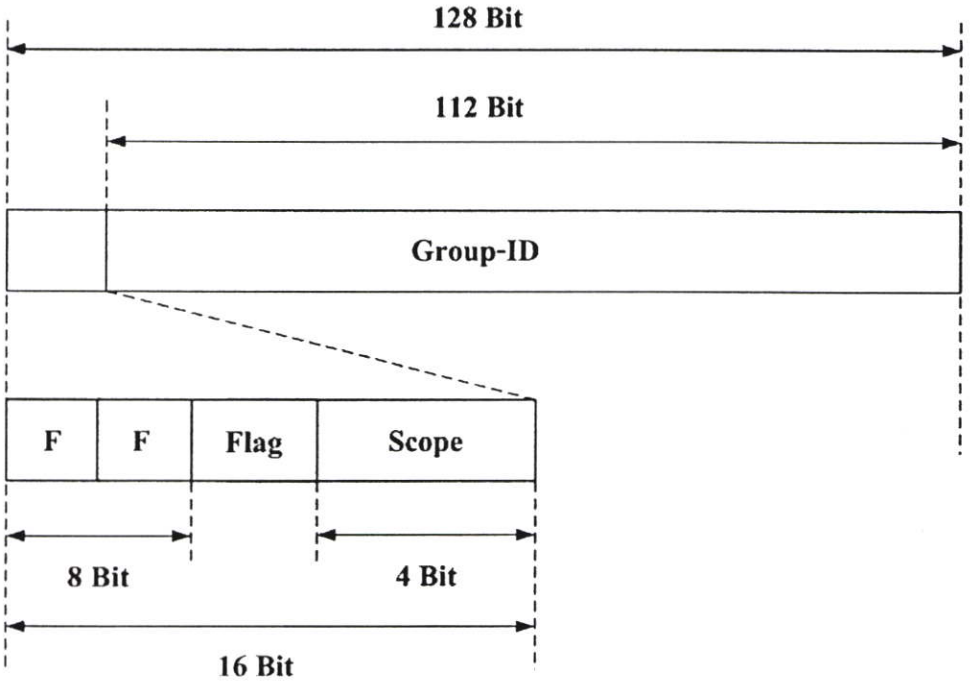
ตารางที่ 2.9 แสดงหมายเลขแอดเดรสของ Aggregatable Global Unicast Address

หมายเลขแอดเดรส	อธิบาย
2001::/16	ใช้ในอินเตอร์เน็ต IPv6
2002::/16	ใช้ในการทำ Tunnel 6to4
2003::/16 ถึง 3FFD::/16	ยังไม่ได้ระบุ
3FFE::/16	ใช้ใน 6bone

63281

2.4.4 Multicast Address

Multicast Address ใช้ในการ Routing แบบ Multicasting เป็นแบบ One-to-many (คล้ายๆ กับ Broadcast แต่ Broadcast จะเป็น One-to-all) ใน Multicasting เครื่องแต่ละเครื่องจะถูกกำหนดให้อยู่ใน Group (1 เครื่องอาจจะอยู่ได้มากกว่า 1 Group) แต่ละกลุ่มจะมี Multicast Address เป็นตัวกำหนด เครื่องที่มี Multicast Address เดียวกันก็จะหมายความว่าอยู่ในกลุ่มเดียวกัน เมื่อไหร่ก็ตามที่เราส่งข้อมูลไปยัง Multicast Address เครื่องทุกเครื่องในกลุ่ม นั้นก็จะได้รับข้อมูลของเรา การทำ Multicasting ทำให้ลดความซ้ำซ้อนในการส่งข้อมูลไปหาเครื่องหลายๆ เครื่อง ปัจจุบัน Multicast ใช้ในการ Update Routing และการส่งข้อมูลพวก Multimedia



รูปที่ 2.13 แสดง Multicast Address

ตารางที่ 2.10 แสดงหมายเลขแอดเดรสของ Multicast Address

รูปแบบ	หมายเลขแอดเดรส
รูปแบบปกติ	FF00:0000:0000:0000:0000:0000:0000:0000/8
รูปแบบย่อแบบที่ 1	FF00:0:0:0:0:0:0:0/8
รูปแบบย่อแบบที่ 2	FFC0::/8

ตารางที่ 2.11 แสดงความหมายของฟิลด์ Flag

เลขฐานสอง	ชนิดของ Multicast Address
0000	Permanent Multicast Address
0001	Temporary Multicast Address

ตารางที่ 2.12 แสดงตัวอย่างของ Multicast Address

หมายเลขแอดเดรส	อธิบาย
FF01::1	ทุก Node บน Interface-local
FF01::2	ทุก Router บน Interface-local
FF02::1	ทุก Node บน Link-local
FF02::2	ทุก Router บน Link-local
FF05::2	ทุก Router ใน Site

2.4.5 Anycast Address

Anycast Address อันนี้ก็จะคล้ายกับ Multicasting คือ มีแบ่งเป็นกลุ่มเหมือนกัน เรียกว่าเซ็ตแต่ละ เซ็ต จะกำหนดโดยใช้ Anycast Address ที่ต่างก็คือเมื่อเราส่งข้อมูลไปยัง Anycast Address เครื่องใดเครื่องหนึ่งในเซ็ตนั้นจะเป็นได้รับข้อมูล โดยทั่วไปจะเป็นเครื่องที่อยู่ใกล้ที่สุด Anycast Address อาจจะได้ใช้กับ DNS Server ในอนาคต DNS Server ทั้งโลกสามารถกำหนดให้เป็นเซ็ตเดียวกันได้ ผู้ใช้งานไม่ต้องตั้ง IP ของ DNS Server หลายเครื่อง เพราะไม่ว่าเน็ตเวอร์ไหนๆ ก็ใช้ IP Address ของ DNS Server เหมือนกัน หากว่า DNS Server ที่เราใช้ล่ม Anycast ก็จะหาเครื่องที่อยู่ใกล้ที่สุดที่ติดต่อได้เองโดยไม่ต้องเปลี่ยน Configuration

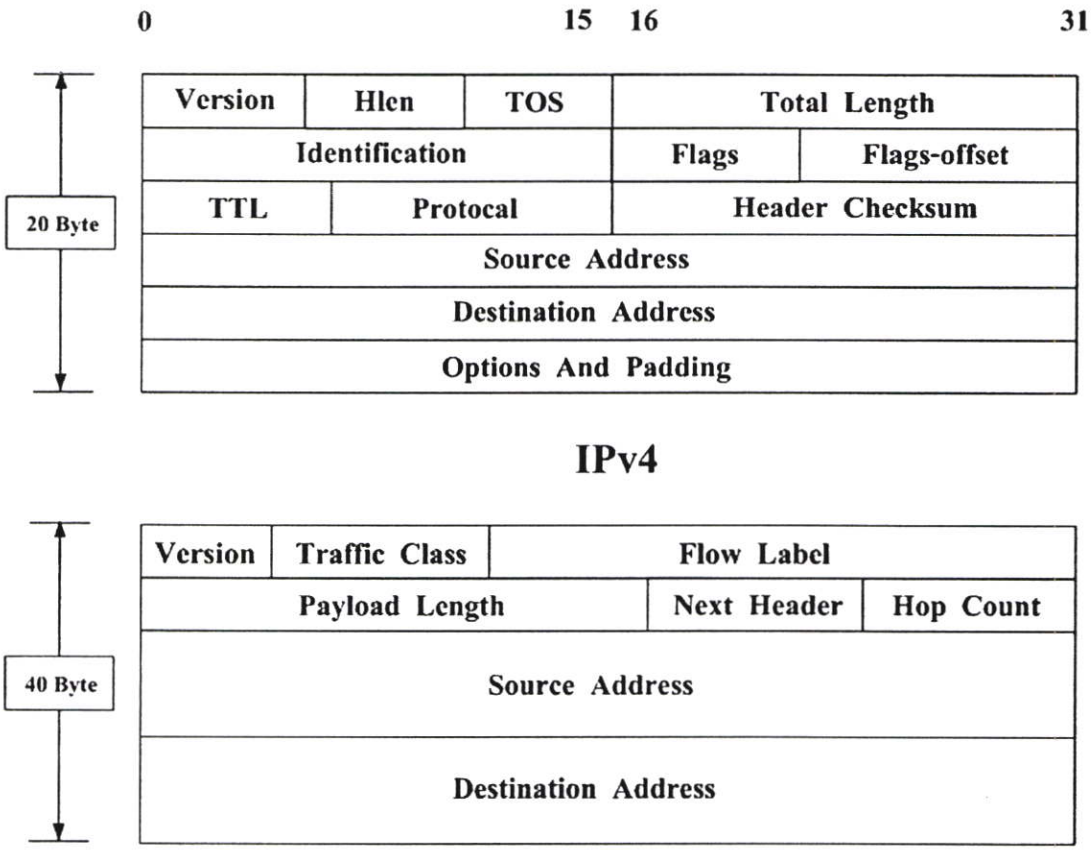
2.4.6 Loopback Address

Loopback Address ถ้าเปรียบเทียบกับอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) ก็คือ 127.0.0.1 แต่ของอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) คือ ::1

ตารางที่ 2.13 แสดงหมายเลขแอดเดรสของ Loopback Address

รูปแบบ	หมายเลขแอดเดรส
รูปแบบปกติ	0000:0000:0000:0000:0000:0000:0000:0001
รูปแบบย่อแบบที่ 1	0:0:0:0:0:0:0:1
รูปแบบย่อแบบที่ 2	::1

2.5 เปรียบเทียบคุณสมบัติอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 กับคุณสมบัติอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Compare Internet Protocol Version 6; IPv6 with Internet Protocol Version 4; IPv4)



รูปที่ 2.14 เปรียบเทียบ Header ระหว่าง IPv4 และ IPv6

จากรูปที่ 2.14 จะเห็นได้ว่า Header ของ IPv6 ถึงแม้ว่าจะมีความยาวกว่า IPv4 แต่จะดูเรียบง่ายกว่า Header ของ IPv4 มาก ทั้งนี้หากพิจารณา Header ของ IPv6 เทียบกับขอ IPv4 จะสามารถเปรียบเทียบความแตกต่างได้ดังนี้

ตำแหน่งที่ตัดออก :

- Header Length ถูกตัดออกไป เพราะ Header ของ IPv6 มีขนาดคงที่ที่ 40 Byte ทำให้ประสิทธิภาพโดยรวมของการประมวลผลแพ็กเก็ตดีขึ้นพราะไม่เสียเวลาใน การคำนวณขนาดของ Header

- Identification, Flag, Segmentation , Protocol , Options , และ Padding ถูกย้ายไปอยู่ในส่วนขยายของ Header (Extended Header) เพราะถือว่าเป็นส่วนที่ไม่จำเป็นต้องประมวลผลในทุกๆ เราเตอร์
- Header Checksum ถูกตัดออกเพราะว่าซ้ำซ้อนกับฟังก์ชันของโพรโตคอลในชั้นที่อยู่สูงกว่าอีกทั้งเป็นการเพิ่มประสิทธิภาพของการประมวลผลด้วย เพราะ Checksum จะต้องมีการคำนวณใหม่เราเตอร์เสมอ หากตัดออกก็จะลดภาระงานที่เราเตอร์ไปได้

ตำแหน่งที่ปรับเปลี่ยน :

- Total Length เปลี่ยนมาเป็น Payload Length เพื่อระบุขนาดของ Payload ในหน่วย octet (Byte) ดังนั้นขนาดของ Payload สูงสุดจะเป็น 65,535 octets
- Time-To-Live (TTL) ของ IPv4 เปลี่ยนมาเป็น Hop Limit เพราะ TTL ระบุเวลาที่ Packet จะวนเวียนอยู่ในอินเทอร์เน็ต (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 ตัวถัดไปเป็น Heade rประเภทไหน เช่น IPSec ซึ่งเป็น Extended Header ก็จะมีค่า Next Header = 51

ตำแหน่งที่เพิ่ม :

- Flow Label ใช้ระบุลักษณะการไหลเวียนของทราฟฟิก ระหว่างต้นทางกับปลายทาง เช่น ในแอปพลิเคชันแบบ Video Conference มีทราฟฟิกหลายลักษณะ (เช่น ภาพ เสียง ตัวอักษร ฯลฯ) ในแอปพลิเคชันหนึ่งจะสามารถสร้าง Flow Label ได้หลายลักษณะ และสามารถแยก Flow ของภาพและเสียงออกจากกันได้
- Traffic Class ใช้ระบุว่าแพ็กเก็ตนี้อยู่ในกลุ่มใดและมีระดับความสำคัญเท่าไหร่เพื่อที่เราเตอร์จะจัดลำดับขั้นการส่งแพ็กเก็ตให้เหมาะสม

ตารางที่ 2.14 แสดงการเปรียบเทียบคุณสมบัติอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 กับ คุณสมบัติอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4

คุณสมบัติ	IPv4	IPv6
ขนาดแอดเดรส	32 Bit	128 Bit
การควบคุม IP Address	Manual, DHCP	Stateless Autoconfiguration
Multicast	Multicast	กลุ่ม Multicast และ Anycast
ระบบอินเตอร์เน็ตไร้สาย	สนับสนุน	สนับสนุนมากกว่า และมีการพัฒนาสูงกว่า
ระบบ VPN	ใช้ IPSec Encrypt Packet ก่อนส่ง	สนับสนุนสำหรับ ESP/Ah Encrypt / Authenticate และสนับสนุน QoS
สนับสนุน IPSec	เป็น Option	จำเป็น
สนับสนุน QoS	สนับสนุนทั้ง Host และ Router	สนับสนุน Host เท่านั้น
Header Checksum	มี	ไม่มี
Linking-Layer	ใช้ ARP	ใช้ Multicast Neighbor Discovery Message
Broadcast	ใช้	ไม่ใช้
DNS	ใช้ A Record	ใช้ AAAA และ A6 Record
ค่า MTU ต่ำสุด	576 Byte	1280 Byte

บทที่ 3
การเลือกเส้นทางอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6

ในหัวข้อนี้จะกล่าวถึงทฤษฎีการเลือกเส้นทางอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Routing on IPv6) ซึ่งมีหลายวิธี เช่น การเลือกเส้นทางแบบ Static Route, การเลือกเส้นทางแบบ RIPng เป็นต้น

3.1 การเลือกเส้นทางแบบ Static Route

การเลือกเส้นทางแบบ Static Route คือ การบอกเส้นทางในการส่งแพ็กเก็ตไปยัง Subnet Address ต่างๆ โดยจะต้องส่งแพ็กเก็ตไปปลายทางที่ระบุ Nxet Hop Address หรือส่งไปที่ Interface ไหน กรณีที่มีจำนวน Subnet Address จำนวนมาก จะต้องใช้เวลามากในการระบุเลือกเส้นทางของแต่ละ Subnet Address

คำสั่งในการเลือกเส้นทางแบบ Static Route ดังนี้

Router(config)#ip route (destination subnet address) (destination subnet mask) (next hop router address)

ความหมายของคำสั่งข้างต้นก็คือ การบอกให้เราท์เตอร์ทราบว่าถ้าต้องการส่งแพ็กเก็ตไปหา Subnet Address ปลายทาง และมี Subnet Mask เท่ากับ Destination Subnet Mask มันจะต้องส่งไปยังเราท์เตอร์ตัวถัดไปที่มี IP Address เท่ากับ Next Hop Router Address

หรือ

Router(config)#ip route (destination subnet address) (destination subnet mask) (directly connected interface)

ความหมายของคำสั่งข้างต้นก็คือ การบอกให้เราท์เตอร์ส่งแพ็กเก็ตออกไปทาง Directly Connected Interface

ข้อแตกต่างก็คือ การทางออกไปยัง Next Hop Address กับชี้ไปยัง Directly Connected Interface ก็คือ การชี้ออกไปยัง Next Hop Address จะมีค่า Adminstrative Distance เท่ากับ 1 แต่ถ้าชี้ไปยัง Directly Connected Interface จะมีค่า Adminstrative Distance เท่ากับ 0

จากที่กล่าวมาข้างต้นเป็นการเลือกเส้นทางแบบ Static Routeของอินเตอร์เน็ตโพรโตคอล รุ่นที่ 4 (Internet Protocol Version 4; IPv4) แต่ถ้าเป็นอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) จะมีคำสั่งดังนี้

Router(config)#ipv6 route ipv6-prefix/prefix-length (next hop interface)

ความหมายของคำสั่งข้างต้นก็คือ การบอกให้เราท์เตอร์ส่งแพ็กเก็ตออกไปทาง Next Hop Interface โดย *ipv6-prefix/prefix-length* คือหมายเลข IP Address ของอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6)

3.2 การเลือกเส้นทางแบบ RIPng

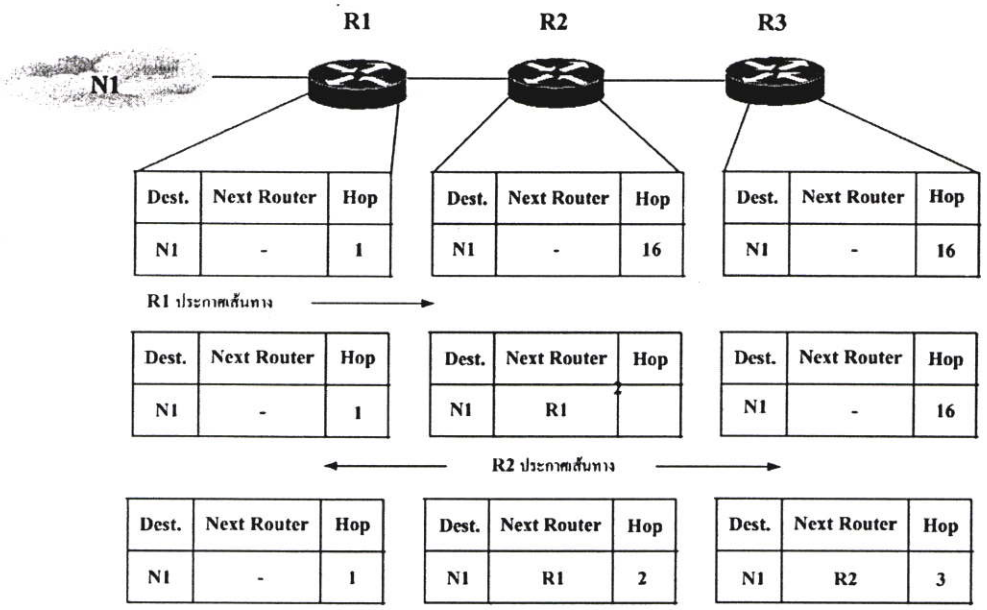
โพรโทคอล Routing Information Protocol Next Generation (RIPng) ได้รับการพัฒนาขึ้นเพื่อให้อุปกรณ์สื่อสารในระบบ สามารถแลกเปลี่ยนข้อมูลเกี่ยวกับตารางเส้นทางของตนกับอุปกรณ์ข้างเคียง พื้นฐานการทำงานของโพรโทคอล RIPng จัดอยู่ในประเภทที่เรียกว่าดิสแทนซ์เวกเตอร์ (Distance-Vector) การแลกเปลี่ยนข้อมูลตารางเส้นทางระหว่างอุปกรณ์สื่อสาร ประกอบด้วยหมายเลขโครงข่ายหรือโฮสต์ปลายทางและต้นทุนของเส้นทาง โดยจะแลกเปลี่ยนข้อมูลตารางเส้นทางเฉพาะกับอุปกรณ์ที่ติดกันเท่านั้น สำหรับโพรโทคอล RIPng วัดต้นทุนของเส้นทางโดยวิธีเรียบง่าย คือพิจารณาจากจำนวนฮอป (Hop Count) ในการส่งดาทาแกรมจากต้นทางถึงปลายทาง จำนวนฮอปหาได้จากจำนวนที่เราท์เตอร์ไอพีดาทาแกรมต้องผ่านบวกกับอีกหนึ่งฮอปสำหรับการเดินทางไปสู่จุดหมายปลายทาง โพรโทคอล RIPng กำหนดให้จำนวนฮอปมีค่าได้ไม่เกิน 15 ฮอป และจะกำหนดค่าเป็น 16 เพื่อแสดงว่าโครงข่ายนั้นไม่สามารถไปถึงได้ (Unreachable) อุปกรณ์สื่อสารหลักที่เกี่ยวข้องกับการแลกเปลี่ยนตารางเส้นทางได้แก่โฮสต์ และเราท์เตอร์สำหรับโฮสต์มีหน้าที่เป็นเพียงแค่ผู้รับข่าวสารของตารางเส้นทางเท่านั้น และทำการปรับตารางการเลือกเส้นทางของตนให้ทันสมัยอยู่เสมอ ในขณะที่เราท์เตอร์ทำหน้าที่สองอย่างคือ แจ้งหรือประกาศตารางเส้นทางของตนให้อุปกรณ์รอบตัว และในขณะเดียวกันก็รับข้อมูลตารางเส้นทางจากอุปกรณ์ข้างเคียงด้วย ในตารางเส้นทางของเราท์เตอร์ จะประกอบด้วยข้อมูลในการอธิบายเส้นทางและส่วนประกอบ ในการดูแลตรวจสอบเส้นทางให้ถูกต้องสอดคล้องกับสภาพของโครงข่ายที่อาจเปลี่ยนแปลงได้ตลอดเวลาสำหรับอุปกรณ์จุดหมายปลายทางแต่ละแห่ง ดังนี้ คือ

- หมายเลข IP Address ของจุดหมายปลายทาง
- ค่าต้นทุนในการส่งไอพีดาทาแกรมให้ถึงจุดหมาย (จำนวนฮอป)
- หมายเลข IP Address ของเราท์เตอร์ตัวถัดไปที่จะนำไปสู่จุดหมาย
- พารามิเตอร์ที่ใช้บ่งชี้ว่าเส้นทางเพิ่งจะได้รับการปรับเปลี่ยนใหม่
- นาฬิกาจับเวลา

ตามข้อกำหนดของโพรโทคอล RIPng เราท์เตอร์จะต้องประกาศข้อมูลตารางเส้นทางของตนให้อุปกรณ์ข้างเคียงทุกๆ 30 วินาที โดยอาศัยโพรโทคอล UDP กับพอร์ตหมายเลข 520 ข้อมูลที่ประกาศมีเพียง 2 ส่วน คือ หมายเลขอุปกรณ์ปลายทางและจำนวนฮอปที่ต้องใช้ในการไปให้ถึงจุดหมายถ้าส่งผ่านมาทางตน ฉะนั้นเราท์เตอร์ทุกตัวจึงคาดหวังได้ว่าจะมีข้อมูลตารางเส้นทางของอุปกรณ์รอบข้างเข้ามาใหม่อย่างสม่ำเสมอ ถ้าเมื่อใดพบว่ามีเส้นทางบางเส้นทางไม่ได้รับการปรับใหม่จากเราท์เตอร์ตัวใดตัวหนึ่งเป็นเวลานานเกิน 180 วินาที เราท์เตอร์จะตีความว่ามีเหตุการณ์ไม่ปกติเกิดขึ้นกับการเชื่อมต่อกับเราท์เตอร์นั้น และจากนั้นก็จะปรับค่าหาระยะห่างหรือจำนวนฮอปให้มีค่าเท่ากับ 16 เพื่อแสดงว่าไม่สามารถติดต่อไปยังโครงข่ายส่วนนั้น (Unreachable)

3.2.1 ขั้นตอนการทำงานของ RIPng

ในที่นี้จะอาศัยอย่างโครงข่ายเล็กๆ ในรูปที่ 3.1 สำหรับใช้ในการอธิบายการทำงานทั่วไปของโพรโทคอล RIPng เริ่มแรกตารางเส้นทางของเราท์เตอร์ทั้งหมดยังไม่มีข้อมูลใดๆ ยกเว้นก็แต่เราท์เตอร์ที่ต่อเชื่อมโดยตรงกับโครงข่าย สำหรับในที่นี้เราจะสนใจเฉพาะกับเส้นทางที่จะนำ ไปสู่โครงข่าย N1 เท่านั้น ส่วนเส้นทางไปสู่โครงข่ายอื่นๆ จะไม่แสดงในที่นี้เพราะมีหลักการเหมือนกันสำหรับตัวอย่างนี้จึงมีเพียงเราท์เตอร์ R1 เท่านั้นที่ทราบเส้นทางไปยังโครงข่าย N1 เพราะต่อเชื่อมโดยตรง ดังนั้นจำนวนฮอปจึงมีค่าเป็น 1 ส่วนเราท์เตอร์อื่นๆ ได้แก่ R2 และ R3 ยังไม่ทราบเส้นทางที่จะนำไปสู่โครงข่าย N1 จำนวนฮอปจึงตั้งไว้ที่ 16 ซึ่งเป็นค่าสูงสุดและแทนความหมายว่าเส้นทางเส้นนี้มีระยะทางเป็นอนันต์ ตามกระบวนการทำงานของโพรโตคอล RIPng เราท์เตอร์แต่ละตัวจะประกาศข้อมูลในตารางเส้นทางของตนให้กับเราท์เตอร์ข้างเคียงที่ติดกันเป็นระยะๆ ทุก 30 วินาที โดยที่จะบอกเป็นจำนวนฮอปสำหรับการไปถึงจุดหมายปลายทางแต่ละแห่งถ้าหากส่งผ่านดาทาแกรมผ่านมายังตน ดังนั้นเมื่อเราท์เตอร์หนึ่งๆ ได้รับข้อมูลเส้นทางจากเราท์เตอร์รอบข้าง ก็จะสามารถตัดสินใจเลือกส่งไอพีดาทาแกรมของตนไปให้กับเราท์เตอร์ข้างเคียงที่มีระยะห่างจากจุดหมายปลายทางที่สั้นที่สุด



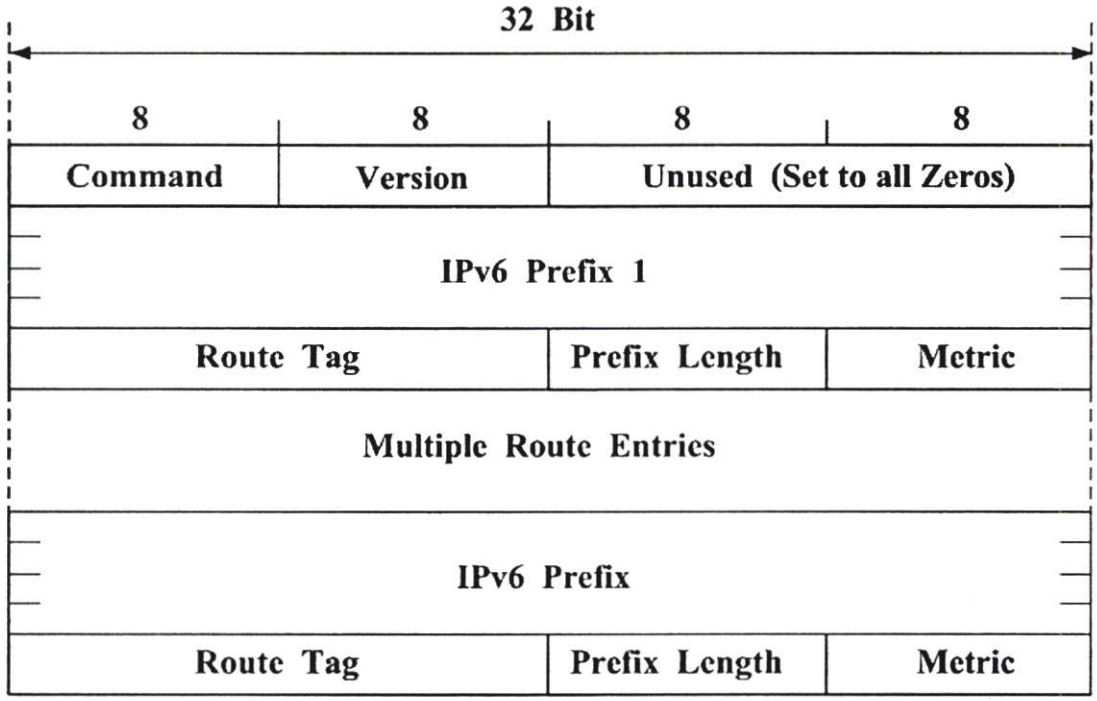
รูปที่ 3.1 แสดงการทำงานของโพรโทคอล RIPng ในช่วงเริ่มแรกของการสร้างตารางเส้นทาง

พิจารณาตัวอย่างในรูปที่ 3.1 สมมติว่าในช่วงเริ่มแรกเราท์เตอร์ R1 ประกาศตารางเส้นทางของตนไปให้เราท์เตอร์ข้างเคียง ซึ่งในขณะนี้มีเพียงเราท์เตอร์ R2 เท่านั้น เราท์เตอร์ R1 บอกเราท์เตอร์ R2 ว่าตนสามารถส่งต่อไอพีดาทาแกรมไปที่โครงข่าย N1 ได้ด้วยจำนวนฮอปเท่ากับ 1 เมื่อเราท์เตอร์ R 2 รับข้อมูลเข้ามาก็เปรียบเทียบกับเส้นทางเดิมที่มีค่าเป็นอนันต์ เราท์เตอร์ R2 จึงปรับตารางเส้นทางของตนใหม่ ซึ่งได้ระบุถ้าเมื่อใดมีดาทาแกรมจะส่งไปที่โครงข่าย N1 ให้ส่งต่อไปที่เราท์เตอร์ R1 เพราะเป็นเส้นทางที่สั้นที่สุดคือมีจำนวนฮอปเท่ากับ 2 สังเกตว่าที่จังหวะเวลานี้เราท์เตอร์ R3 ยังไม่มีข้อมูลเส้นทางการส่งไอพีดาทาแกรมของตนไปยังโครงข่าย N1 ในเวลาต่อมาเราท์เตอร์ R2 ได้ประกาศข้อมูลตารางเส้นทางของตนไปให้เราท์เตอร์รอบข้างได้แก่ R1 และ R3 ทันทีที่เราท์เตอร์ R3 ได้รับข้อมูลใหม่นี้ก็สามารถปรับตารางเส้นทางสำหรับไปโครงข่าย N1 ได้ เส้นทางดังกล่าวนี้มีจำนวนฮอปเท่ากับ 3 ฮอป โดยให้ส่งผ่านทางเราท์เตอร์ R2 สังเกตว่าข้อมูลเส้นทางที่เราท์เตอร์ R2 ส่งไปให้ R1 ไม่ส่งผลต่อตารางของเราท์เตอร์ R1 แต่อย่างใด เพราะเส้นทางเดิมที่เราท์เตอร์ R1 มีอยู่ใช้ระยะทางที่สั้นกว่าการส่งผ่านเราท์เตอร์ R2 จากตัวอย่างนี้ จะเห็นว่าการประกาศข้อมูลเส้นทางของเราท์เตอร์ภายในระบบอย่างสม่ำเสมอไปด้วยช่วงเวลาช่วงหนึ่ง เราท์เตอร์อื่นๆในระบบก็จะทราบถึงเส้นทางการเชื่อมต่อไปยังโครงข่าย N1 ได้อย่างถูกต้องสมบูรณ์

3.2.2 โครงสร้างของเมสเสจ RIPng

การส่งข้อมูลข่าวสารตารางเส้นทางโดยอาศัยโพรโตคอล RIPng จะมีโครงสร้างการจัดเรียงข้อมูลในแต่ละเมสเสจดังในรูปที่ 3.2 ข้อมูล RIPng นี้จะได้รับการส่งผ่านโครงข่ายโดยอาศัยดาทาแกรม UDP พิจารณาจากโครงสร้างของเมสเสจจะเห็นว่าส่วนต้นของเมสเสจจะเห็นว่าส่วนต้น

ของเมสเสจประกอบด้วยฟิลด์ Command และฟิลด์ Version ส่วนที่เหลือจะเป็นกลุ่มของฟิลด์ขนาด 40 Byte ซึ่งบรรจุข้อมูลของเส้นทางหนึ่งเส้น โดยจำนวนกลุ่มที่อนุญาตให้มีได้ไม่เกิน 25 กลุ่ม ฉะนั้นในการส่งเมสเสจหนึ่งครั้งสามารถประกาศเส้นทางได้มากถึง 25 เส้น ถ้าหากมีจำนวนเส้นทางที่ต้องประกาศมากกว่า 25 เส้นในเวลาเดียวกัน ก็ให้ส่งส่วนที่เหลือในเมสเสจใหม่ตามไป เนื่องจากเส้นทางแต่ละเส้นทางใช้เนื้อที่เท่ากับ 40 Byte



รูปที่ 3.2 โครงสร้างเมสเสจของโพรโตคอล RIPng

- ฟิลด์ Command คือใช้สำหรับระบุถึงความหมายของเมสเสจ ดูรายละเอียดการ ใช้งานในตารางที่ 3.1 ในปัจจุบันการใช้งานที่เป็นอยู่จะมีเพียง 2 คำสั่ง ได้แก่ Request และ Response เท่านั้น ซึ่งกำหนด Command ให้มีค่าเท่ากับ 1 และ 2 ตามลำดับ ส่วนคำสั่งอื่นคือ 3 และ 4 ไม่มีการใช้งาน ส่วนคำสั่ง Command = 5 สงวนไว้สำหรับใช้งานเฉพาะกับระบบของ Sun Microsystems
- ฟิลด์ Version มีค่าเท่ากับ 1 เพื่อแสดงว่าเป็นโพรโตคอล RIPng เวอร์ชั่น 1 และจะมีค่าเป็น 2 เมื่อเป็นโพรโตคอล RIPng เวอร์ชั่น 2
- ฟิลด์ IPv6 Prefix คือ IP Address ที่มีขนาด 128 Bit ของ IPv6 โดยเป็น IP Address ปลายทาง
- ฟิลด์ Route Tag ฟิลด์นี้จะทำหน้าที่คล้ายของ RIP เวอร์ชั่น 2
- ฟิลด์ Prefix Length ฟิลด์นี้เป็นฟิลด์พิเศษที่มีขนาด 8 Bit ซึ่งไว้ใส่ค่า IPv6 Prefix Filed

- ฟิลด์ Matric คือระยะทางที่นับจากตัวอุปกรณ์เองไปจนถึงอุปกรณ์ปลายทางการวัดระยะทางจะพิจารณาในหน่วยของจำนวนฮอป (Hop Count) Matric จะมีค่าอยู่ได้ระหว่าง 1-15 และถ้ากำหนด Matric=16 ให้หมายถึงไม่สามารถติดต่อไปยังปลาย ทางได้

ตารางที่ 3.1 รายละเอียดการใช้งานฟิลด์ Command

Command	ความหมาย
1. Request	คำสั่งสำหรับการร้องขอตารางเส้นทางที่มีต่ออุปกรณ์อื่น
2. Response	เมสเสจซึ่งแรรจุข้อมูลเส้นทางของตัวเองเพื่อตอบรับการร้องขอหรือเป็นการประกาศตารางตามปกติ
3. Traceon	ไม่มีการใช้งานต่อไป (Obsolete)
4. Traceoff	ไม่มีการใช้งานต่อไป (Obsolete)
5. Reserved	สงวนไว้ใช้งานเฉพาะกับระบบของ Sun Microsystem

บทที่ 4
ลักษณะการเชื่อมต่ออินเตอร์เน็ตโพรโตคอลรุ่นที่ 6

ในหัวข้อนี้จะกล่าวถึงทฤษฎีลักษณะการเชื่อมต่ออินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) กับ อินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) แบบต่างๆ ซึ่งการเชื่อมมีอยู่ 3 ชนิดด้วยกัน คือ การใช้งานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) และอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) ควบคู่กันหรือที่เรียกว่า Dual Stack, การทะลุผ่านข้อมูล (Tunneling), และการแปลงข้อมูล (Translation)

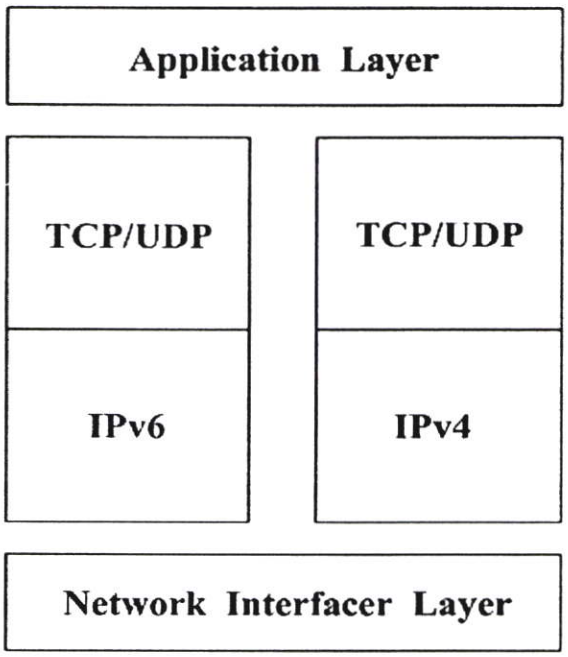
4.1 Dual Stack

Dual Stack คือ การใช้งานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) และ อินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) ควบคู่กันไปภายในอุปกรณ์ตัวเดียวกัน Dual Stack สามารถใช้ได้ทั้ง Host และ Server และอุปกรณ์เครือข่าย (Network Device) เช่น เราท์เตอร์ Dual Stack เป็นทางออกที่ง่ายที่สุดสำหรับเครือข่ายที่ต้องการเริ่มใช้งานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) และถูกใช้งานแพร่หลาย

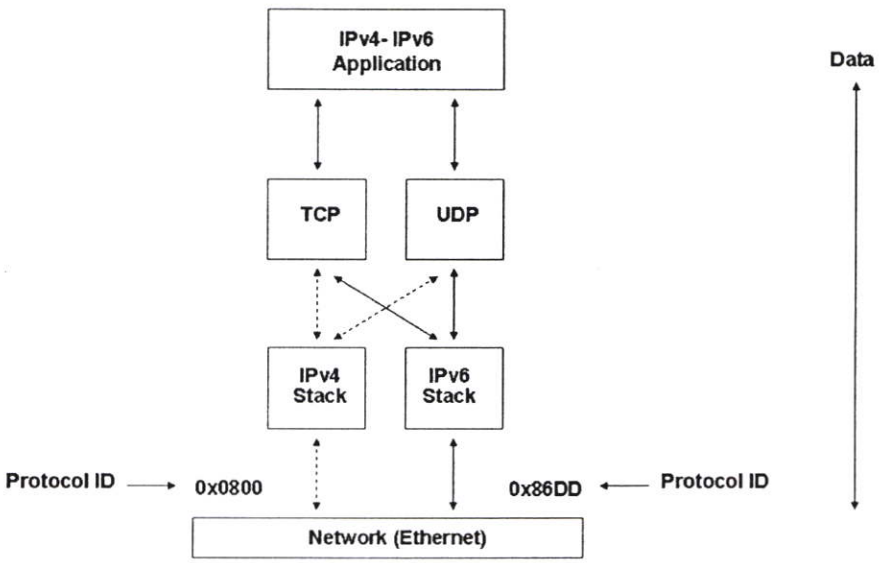
Dual Stack เหมาะกับการติดต่อระหว่าง 2 โหนด (Node) ที่ใช้อินเตอร์เน็ตโพรโตคอลเวอร์ชั่นเดียวกัน แต่ต้องผ่านเครือข่ายกลางทางที่ใช้ IP อินเตอร์เน็ตโพรโตคอลคนละเวอร์ชั่น เช่น อินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) - อินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) ผ่านเครือข่ายอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) หรือ อินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) - อินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) ผ่านเครือข่ายอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) หรือในกรณีที่บางโหนดต้องการปรับเปลี่ยนไปใช้อินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) แต่ว่าเครือข่ายที่เชื่อมต่ออยู่ด้วยไม่สนับสนุนอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) โหนดดังกล่าวสามารถใช้ Dual Stack เพื่อรองรับอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) และ อินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6)

หลักการทำงานคือ IP Stack ที่อยู่ภายในโหนดจะแบ่งออกเป็น 2 Stack ทำงานขนานกัน เช่น เมื่อโหนดอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) Packet โหนดจะเลือก IPv6 Stack มาจัดการกับแพ็กเก็ต (โดยตรวจสอบ Protocol Version จากส่วนหัวแพ็กเก็ต) ในขณะเดียวกันโหนดสามารถติดต่อกับเครือข่ายอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol

Version 4; IPv4)(ผ่าน IPv4 Stack) ได้เหมือนเดิมไม่ต้องเปลี่ยนแปลง โดยโหนดที่มี Dual Stack นี้จะต้องมี IP Address สองหมายเลข คือ IPv4 Address และ IPv6 Address



รูปที่ 4.1 แสดงโครงสร้างของ Dual Stack



รูปที่ 4.2 แสดงลักษณะการทำงานของ Dual Stack

ขั้นตอนการติดตั้ง Dual Stack บนเราท์เตอร์

หาก IOS Software สนับสนุน IPv6 แล้ว ซึ่งตรวจสอบได้จากเวบไซต์ของอุปกรณ์เครือข่ายที่ใช้งานทำการเซ็ทเราท์เตอร์ ด้วยคำสั่ง

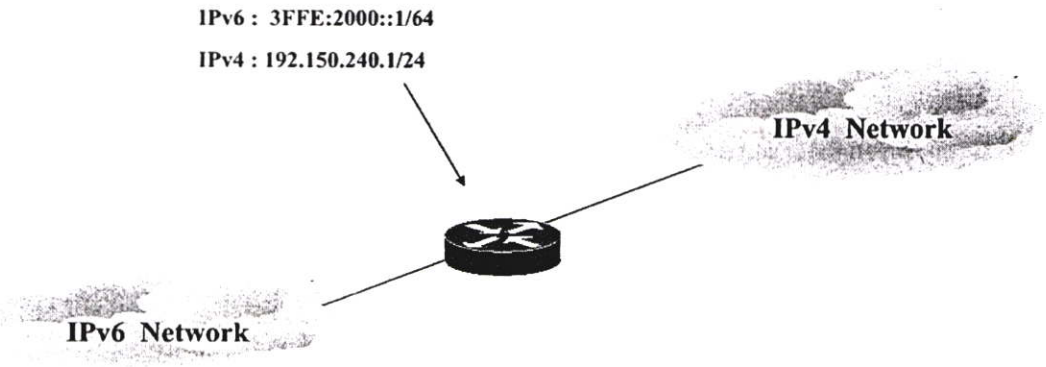
```
Router# configure terminal
Router# ipv6 unicast-routing
```

จากนั้นกำหนด IPv6 และ IPv4 ให้กับ Interface fastethernet 0/0 ให้แก่เราท์เตอร์

```
Router(config)#interface fastEthernet 0/0
Router(config-if)#ipv6 address 3FFE:2000::11/64
Router(config-if)#ipv6 enable

Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 192.150.240.1 255.255.255.0
Router(config-if)#no shutdown
```

ซึ่งเมื่อเรากำหนดได้แล้ว เราท์เตอร์ก็จะทำหน้าที่เป็น Dual Stack โดยทำการส่งแพ็กเก็ตไปตามเวอร์ชั่นของอินเตอร์เน็ตโพรโตคอลนั้น

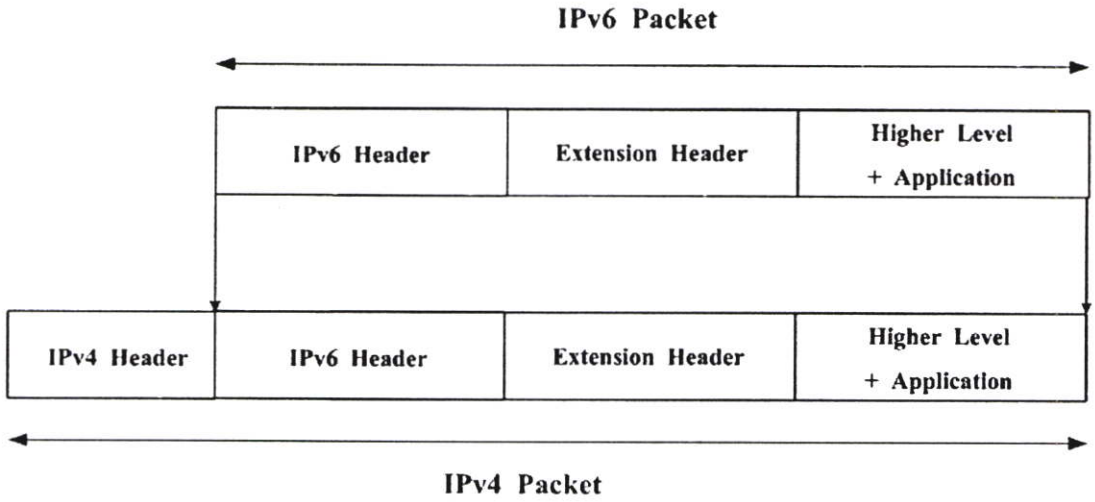


รูปที่ 4.3 แสดงการใช้งาน Dual Stack ของเราท์เตอร์

4.2 การทะลุผ่านข้อมูล (Tunneling)

การทะลุผ่านข้อมูล (Tunneling)โดยทั่วไปเป็นการ Encapsulate แพ็กเก็ตข้อมูลที่ต้องการส่งไว้ในอีกแพ็กเก็ตหนึ่ง เนื่องจากแพ็กเก็ตที่อยู่ภายในไม่สามารถถูกส่งไปยังปลายทางได้ จึงต้องอาศัยการห่อหุ้มด้วยแพ็กเก็ตอื่น การทำอุโมงค์เพื่อใช้งาน IPv6 นั้นก็เช่นกัน ใช้เมื่อเครือข่ายเชื่อมต่อ

อยู่ด้วยไม่สนับสนุน IPv6 จึงจำเป็นต้องหุ้มแพ็กเก็ต IPv6 ไว้ภายใต้แพ็กเก็ต IPv4 อีกที ดังรูปที่ 4.4

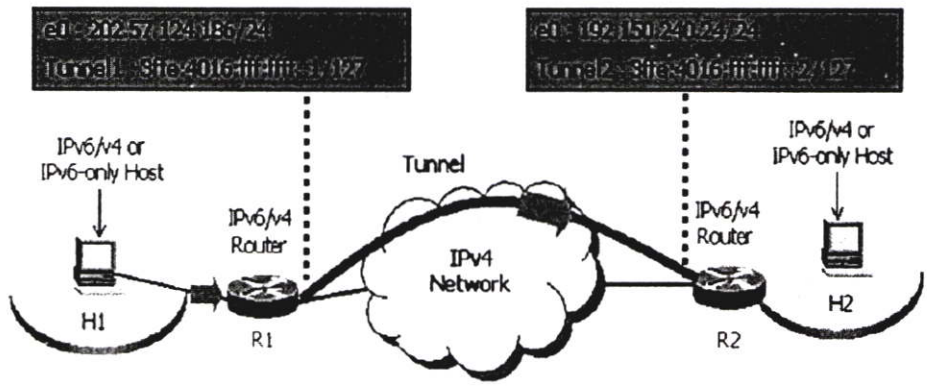


รูปที่ 4.4 IPv6 Packet Encapsulation

การทะลุผ่านข้อมูล (Tunneling) สำหรับเครือข่าย IPv6 ต้องสร้างเส้นทางการติดต่อระหว่างเครื่องที่ใช้หมายเลข IPv6 ผ่านเครือข่ายที่ใช้หมายเลข IPv4 โดยเกตเวย์ (Gateway) ของเครือข่ายของเครื่องที่ใช้หมายเลข IPv6 จะทำหน้าที่ห่อหุ้มแพ็กเก็ต IPv6 ไว้ใน IPv4 ก่อนจะส่งไปในเครือข่ายอินเทอร์เน็ตโพรโตคอลที่สนับสนุนการใช้หมายเลข IPv4 เท่านั้น โดยระหว่างทางจะดูหมายเลขต้นทางและปลายทางที่อยู่ในส่วนหัวของแพ็กเก็ต IPv4 เท่านั้นจะไม่สนใจส่วนที่อยู่ภายใน เมื่อส่งไปถึงปลายทางเกตเวย์จะถอดแพ็กเก็ต IPv4 ออกให้เหลือแต่แพ็กเก็ต IPv6 แล้วส่งไปยังเครื่องใช้หมายเลข IPv6 ต่อไป

ข้อเสียของวิธีนี้คือ Encapsulation ทำให้แพ็กเก็ตมีขนาดใหญ่ขึ้น เป็นผลให้เครือข่ายมี Overhead สูงขึ้น นอกจากนี้การทะลุผ่านข้อมูล (Tunneling) จำเป็นต้องใช้ Dual stack ที่ตัวเกตเวย์ทั้งสองด้านของอุโมงค์

4.2.1 Manually Configured Tunnel



รูปที่ 4.5 การทำงานของ Manually Configured Tunnel

Manually Configured Tunnel เป็นวิธีที่นิยมกันมากสำหรับการให้บริการเชื่อมต่อกันระหว่างเครื่องที่ใช้และติดตั้งหมายเลข IPv6 เพียงอย่างเดียว โดยต้องมีเกตเวย์ที่ติดตั้งและใช้งานแบบ Dual Stack ซึ่งจะทำหน้าที่เป็นอุโมงค์เครือข่ายทางเข้าและทางออก โดยแต่ละด้านจะต้องเก็บหมายเลขไอพีของอุโมงค์เครือข่ายของอีกด้านที่ต้องการเชื่อมต่อ ซึ่งผู้ดูแลระบบจะต้องใส่หมายเลข IP Address ของปลายทางอุโมงค์เข้าไปเอง วิธีนี้จึงต้องการดูแลสูง

ในส่วนของการทำงาน เมื่อแพ็กเก็ต IPv6 มาถึงอุโมงค์ก็จะถูกห่อหุ้มด้วยเฮดเดอร์ IPv4 โดยใช้หมายเลข IPv4 ของเครือข่ายต้นทาง หมายเลข IPv4 ของเครือข่ายปลายทาง และระบุชนิดโพรโตคอลของข้อมูลที่อยู่ภายในเป็น IPv6 เมื่อแพ็กเก็ตมาถึงปลายทางของอุโมงค์ เครือข่าย ปลายทางจะทำการตรวจสอบเฮดเดอร์ ซึ่งจะทราบว่าภายในเป็นแพ็กเก็ตที่ใช้หมายเลข IPv6 ดังนั้น ตัวเกตเวย์จะเอาส่วนหัน IPv4 ออกไปให้เหลือแต่ส่วนที่เป็น IPv6 แพ็กเก็ต แล้วส่งต่อไปยังเครื่องปลายทางที่ใช้หมายเลข IPv6 ที่ระบุอยู่ในส่วน Destination ของเฮดเดอร์ IPv6

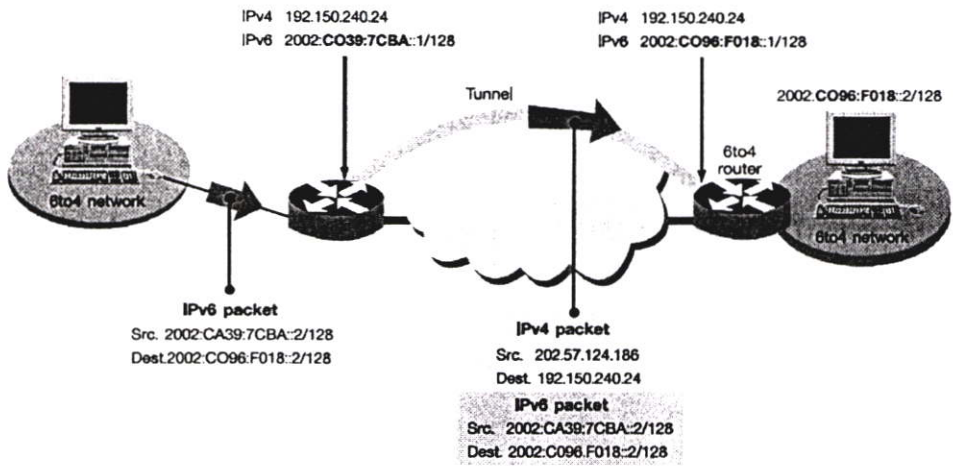
ขั้นตอนการติดตั้ง Manually Configured Tunnel บนเราท์เตอร์

```
Router(config)#ipv6 unicast-routing
Router(config)#interface Tunnel1
Router(config)#description Configured Tunnel to Tunnel2
Router(config)#no ip address
Router(config)#ipv6 address ffe:1234:1234::2/127
Router(config)tunnel source Ethernet0/0
Router(config)tunnel destination 202.100.100.1
Router(config)#tunnel mode ipv6ip
```

4.2.2 Fully Automatic Tunnel (6to4 Tunnel)

การทำงานแบบ Fully Automatic Tunnel มีขั้นตอนการทำงานเหมือนกับ Manually Configured Tunnel แต่จะแตกต่างกันตรงที่ Tunnel แต่ละด้านไม่ต้องเก็บหมายเลขไอพีของเกตเวย์ปลายทางที่ต้องการเชื่อมต่อแต่เกตเวย์ จะตรวจสอบหมายเลขเครื่องปลายทางโดยพิจารณาจากหมายเลขปลายทางของแพ็กเก็ตที่ห่อหุ้มอยู่

หนึ่งในการทำ Fully Automatic Tunnel คือวิธีที่เรียกว่า 6to4 Tunnel (ดูRFC3056) เครือ ข่ายที่เชื่อมต่อแบบ 6to4 Tunnel จะต้องกำหนดหมายเลข IPv6 Prefix พิเศษให้กับตัวเกตเวย์ทั้งสองฝั่งของ 6to4 Tunnel Prefix นี้จะขึ้นต้นด้วย 2002 และจะต้องมี IPv4 Address ที่อยู่ในรูปเลขฐานสิบหกตามมา เพราะฉะนั้น Prefix ต้องมีความยาวอย่างน้อย 48 บิตตามรูปแบบ 2002 :<IPv4 in hex>::/48 ตัวอย่างเช่น หาก 202.57.124.186 (แปลงเป็นเลขฐานสิบหกได้ CA39:7CBA) IPv6 address ของเกตเวย์อาจเป็น 2002 : CA39:7CBA ::1/48 การกำหนด Prefix วิธีนี้จะทำให้ทราบหมายเลข IPv4 ของเกตเวย์ปลายทางได้อัตโนมัติ



รูปที่ 4.6 การทำงานของ Fully Automatic Tunnel

ตามตัวอย่างในรูปที่ 4.6 เมื่อแพ็กเก็ต IPv6 มาถึงเกตเวย์ทางออกที่จะไปยังอินเทอร์เน็ต เกตเวย์จะตรวจสอบหมายเลขปลายทาง พบหมายเลขปลายทางถูกกำหนดเป็น 2002 :C096: F018 ::/128 เกตเวย์สามารถทราบได้ว่า IPv4 Address ของเกตเวย์ปลายทางจะต้องเป็น C096: F018 หรือ 192.150.240.24 จึงกำหนดหมายเลขนี้ใน Destination Field ของ IPv4 Packet Header ที่นำมา Encapsulate

ขั้นตอนการติดตั้ง Manually Configured Tunnel บนเราท์เตอร์

```
Router(config)#interface FastEthernet0/0
    Router(config-if)#ip address 202.57.124.186 255.255.255.252
    Router(config-if)#ipv6 address 2002:CA39:7CBA::1/64
    Router(config-if)#ipv6 enable
```

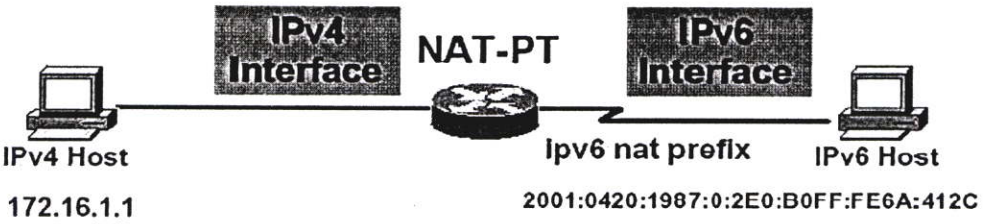
4.3 การแปลงข้อมูล (Translation)

เทคนิคการทำแปลงข้อมูล (Translation) เป็นวิธีที่ใช้กับการสื่อสารข้ามเครือข่าย เช่น โหนดจากเครือข่าย IPv4 ต้องการคุยกับเซิร์ฟเวอร์ ในเครือข่าย IPv6 หรือ โหนดที่เป็น IPv6 ต้องการคุยเซิร์ฟเวอร์ที่เป็น IPv4 ซึ่งจะเป็นกรณีที่ต่างไปจากการใช้งาน Dual Stack และการทะลุผ่านข้อมูล (Tunneling), การทำแปลงข้อมูล (Translation) พูดง่ายๆก็คือการแปลงข้อมูลไปมาระหว่างข้อมูลในรูปแบบของ IPv4 และ IPv6 การแปลงข้อมูลนี้สามารถทำได้ที่หลายระดับ เช่น Network Layer ,Socket Layer หรือ Application Layer

ไม่ว่าจะทำการแปลงข้อมูลที่ระดับไหน องค์ประกอบสำคัญที่จำเป็นคือส่วนที่ทำหน้าที่แปลงหมายเลข IP Address หรือ Address Translator ซึ่งการแปลงเลขนี่สามารถทำได้โดยการจัดเก็บคู่หมายเลข IPv4 และ IPv6 Address ทุกคู่ในเครือข่าย เราเรียกวิธีนี้ว่า Stateful Address Translation หรือจะทำการแปลงแบบอัตโนมัติ ที่เรียกว่า Stateless Address Translator ก็ได้

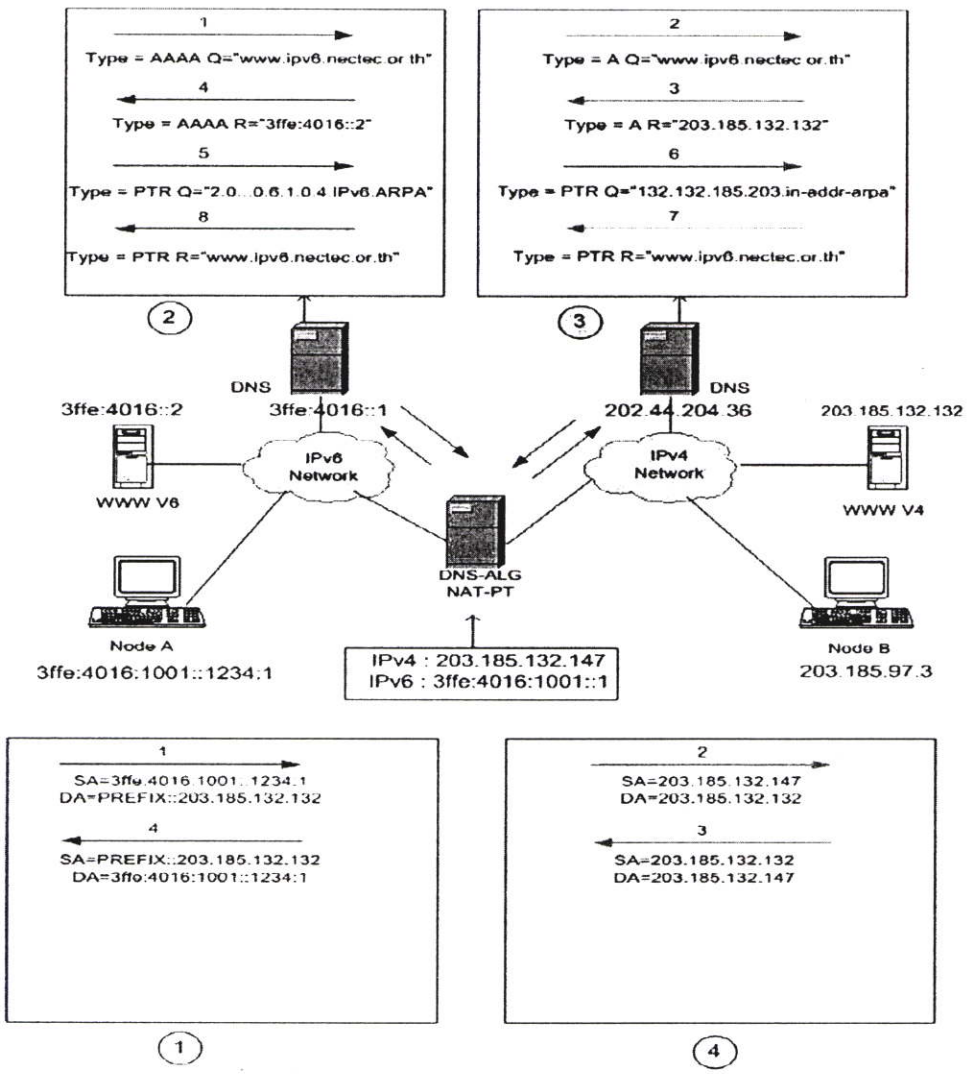
4.3.1 NAT-PT (Network Address Translation-Protocal Translation)

NAT-PT มีพื้นฐานเดียวกับการทำ NAT ในเครือข่าย IPv4 นั่นก็คือการแปลง IP Address โดยเสมือนว่าคอมพิวเตอร์แต่ละเครื่องจะมีหมายเลข IP Address สองตัวสำหรับติดต่อกับเครือข่ายภายในและสำหรับติดต่อกับเครือข่ายภายนอก สำหรับ NAT-PT จะเป็นการแปลงระหว่าง IPv4 Address กับ IPv6 Address เพื่อใช้ในการติดต่อสื่อสารกันระหว่างเครือข่ายที่ใช้อินเทอร์เน็ตโพรโทคอลคนละรุ่น ตัวอย่างเช่น ในรูปที่ 4.7 คอมพิวเตอร์ทางซ้ายมือใช้หมายเลข 172.16.1.1 ในการติดต่อกับเครื่องอื่นๆในเครือข่าย IPv4 ด้วยกัน แต่ถ้าหากมันต้องการติดต่อกับเครื่องคอมพิวเตอร์อีกเครื่องในเครือข่าย IPv6 มันจำเป็นต้องส่งแพ็กเก็ตข้อมูลผ่านเกตเวย์ NAT-PT เพื่อแปลงหมายเลขต้นทางจาก 172.16.1.1 ให้เป็นรูปแบบของ IPv6 Address เช่น 2001:0420:1987:02E0:B0FF:FE6A:412 มันจะได้รู้ว่าควรแปลงกลับเป็นหมายเลข 172.16.1.1



รูปที่ 4.7 การทำงานของ NAT-PT

เนื่องจากแอพพลิเคชั่นบางชนิด เช่น DNS มีการบรรจุหมายเลข IP Address ในส่วนของ Payload ด้วยทำให้เกิดปัญหา เพราะว่าเกตเวย์ NAT-PT จะไม่สามารถแปลง IP Address นอกเหนือจากส่วนที่อยู่ในเฮดเดอร์ได้ เพราะเกตเวย์ NAT-PT เป็นอุปกรณ์ที่ทำงานในระดับ



รูปที่ 4.8 ขั้นตอนการเรียกดูเวบไซต์ IPv4 จากโหนด IPv6

Network Layer จึงไม่มีความรู้ว่าแต่ละแพ็กเก็ตที่ผ่านเข้ามาเป็นของแอพพลิเคชั่นชนิดใด ดังนั้นจึงจำเป็นต้องมีอุปกรณ์อีกตัว ที่ทำงานในระดับ Application Layer สำหรับจัดการกับปัญหานี้ซึ่งเรียกว่า Application Layer Gateway (ALG) โดยที่เกตเวย์ NAT-PT จะต้องคอยส่งแพ็กเก็ตต่อไปยัง ALG เพื่อตรวจสอบหาหมายเลข IP Address ในส่วน Payload และแปลงให้เป็น IP Address ใหม่ให้ถูกต้อง

ตัวอย่างขั้นตอนการเรียกดูเวบไซต์ IPv4 จากโหนด IPv6 มีดังนี้ (ดูที่รูปที่ 4.8 ประกอบ)

1. เมื่อ Node A ซึ่งมี Source Address (SA) = 3ffe:4016:1001:1234:1 ต้องการเรียกเวบ www.ipv6.nectec.or.th ซึ่งเป็น IPv4 มันต้องไปถาม IP Address ที่เซิร์ฟเวอร์ DNS v6 ซึ่งถ้าไม่มีจะต้องติดต่อเซิร์ฟเวอร์ DNS v4 ผ่านเกตเวย์ NAT-PT ซึ่งจะมีส่วนที่ทำหน้าที่เป็น Proxy DNS_ALG ช่วยในการแปลงข้อมูล สมมติว่าเซิร์ฟเวอร์ DNS v4 ตอบกลับมาว่า IPv4 Address ของเวบเซิร์ฟเวอร์คือ 203.185.132.132 เกตเวย์ NAT-PT และ DNS_ALG ก็ต้องแปลง IPv4 Address ของเวบเซิร์ฟเวอร์นี้ให้ได้อยู่ในรูป IPv6 Address คือ Destination Address (DA = Prefix 203:185.132.133

2. เมื่อได้ SA และ DA ในรูปแบบ IPv6 Address แล้วเกตเวย์ NAT-PT จะต้องแปลงจาก SAv6 ไปเป็น SAv4 = 203.185.132.147 (ซึ่งก็คือ IPv4 Address ของตัวเกตเวย์ NAT-PT นั่นเอง) เพื่อไปคุยกับเซิร์ฟเวอร์ DAv4 = 203.185.132.132

3. เมื่อเวบเซิร์ฟเวอร์ติดต่อกลับ ก็จะต้องผ่านเกตเวย์ NAT-PT อีก ซึ่งเกตเวย์จะได้รับแพ็กเก็ตที่มี SAv4 = 203.185.132.132 และ DAv4 = 203.185.132.147 เกตเวย์ NAT-PT จะต้องแปลงจาก SAv4 ไปเป็น SAv6 = Prefix ::203.185.132.132

4. เมื่อต้นทางกับปลายทางมีรูปแบบการสื่อสารเหมือนกันก็จะสามารถติดต่อกันได้โดย SAv6 = Prefix::203.185.132.132 และ DAv6 = 3ffe:4016:1001:1234:1

บทที่ 5
การเตรียมความพร้อมของอุปกรณ์

ในหัวข้อนี้จะกล่าวถึงการจัดเตรียมอุปกรณ์นั้นจะต้องเตรียมความพร้อมของอุปกรณ์ที่จะใช้งานกับอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) ซึ่งต้องดูจากข้อมูลของผู้ผลิตของอุปกรณ์นั้น เช่น เราท์เตอร์(Router), สวิตซ์(Switch), ระบบปฏิบัติการ(Operation System), โปรแกรมประยุกต์ต่างๆ เป็นต้น ซึ่งเนื้อหาทั้งหมดนี้จำเป็นสำหรับการศึกษา

5.1 เตรียมความพร้อมทางด้าน Hardware

เราท์เตอร์(Router), สวิตซ์(Switch)

การจำลองระบบเครือข่ายนี้ใช้อุปกรณ์ยี่ห้อ Cisco ทั้งเราท์เตอร์ (Router) และ สวิตซ์ (Switch) ดังนั้นเราจะต้องหา IOS (Software) ของเราท์เตอร์ (Router) และ สวิตซ์ (Switch) ที่สนับสนุนอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) ซึ่งได้ IOS (Software) ดังนี้ 12.0(22)S, 12.0(22)S, 12.2(2)T, 12.2(14)S, 12.3, 12.3(2)T, 12.4, และ 12.4(2)T

5.2 เตรียมความพร้อมทางด้าน Software

5.2.1 ระบบปฏิบัติการ (Operation System)

ส่วนมากระบบปฏิบัติการ (Operation System) นั้นถ้าเป็นระบบปฏิบัติการ (Operation System) ใหม่ จะสนับสนุนอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) แต่ถ้าเป็นระบบปฏิบัติการ (Operation System) เวอร์ชั่นเก่าจำเป็นจะต้องทำการ Update Software เพิ่ม

Window 9x จะต้องมี Trumpet Winsock ซึ่งสนับสนุนอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6)

Window 2000 จะต้องติดตั้ง Service Pack 1 (SP1) ขึ้นไป

Window XP, Window 2003 สามารถใช้งานกับสนับสนุนอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (IPv6) ได้

Linux ต้องดาวน์โหลดโปรแกรมประยุกต์ จาก URL ต่อไปนี้

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

5.2.2 โปรแกรมประยุกต์ต่างๆ (Application)

โปรแกรมประยุกต์ที่ใช้งานบนเครือข่ายอินเตอร์เน็ตโพรโตคอลรุ่นที่6 (Internet Protocol Version 6; IPv6) ได้ เช่น WWW, DNS, Mail, FTP, Telnet และอื่นๆ

5.2.3 การติดตั้งและการใช้คำสั่งอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 บน Windows XP

เข้าสู่ Mode Dos บน Windows XP แล้วพิมพ์คำสั่ง "ipv6 install" เมื่อเสร็จแล้วก็สามารถใช้งานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 ได้

C:\Documents and Settings>ipv6 install

Installing...

Succeeded.

กรณีจะนำอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 ออก ก็ให้เข้าสู่ Mode Dos แล้วพิมพ์คำสั่ง "uninstall ipv6"

C:\Documents and Settings>ipv6 install

Uninstalling...

Succeeded.

สามารถใช้คำสั่งในการตรวจสอบได้ ดังตารางที่ 5.1

ตารางที่ 5.1 แสดงคำสั่งอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 บน Windows XP

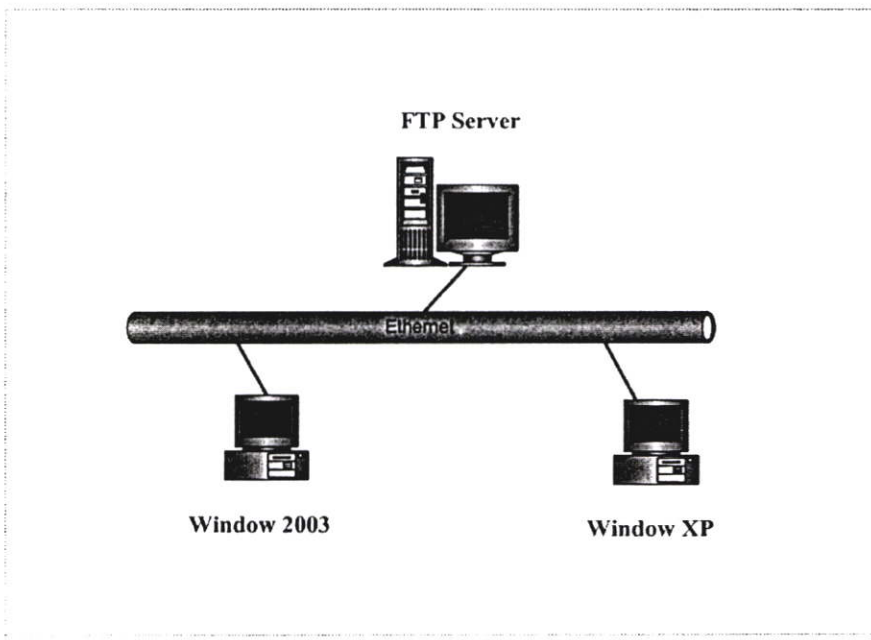
คำสั่ง		อธิบาย
C:\ipv6 if	C:\netsh interface ipv6 show interface	คำสั่งแสดง Pseudo-interface
C:\ipv6 adu	C:\netsh interface ipv6 add address	คำสั่งใช้ routing table ของ IPv6 ที่ Pseudo-interface
C:\ipv6 rt	C:\netsh interface ipv6 show rt	คำสั่งแสดง local routing ของ IPv6
C:\ipv6 rtu	C:\netsh interface ipv6 add rtu	คำสั่งใช้เพิ่ม local routing table ของ IPv6
C:\tracert6	----	เป็นคำสั่งเพื่อหาทิศทางแพ็กเก็ตที่จะวิ่งไป
C:\ping6	C:\ping	เป็นคำสั่งเพื่อเช็คการตอบสนอง

บทที่ 6
แบบจำลองและการวิเคราะห์ผลการทำงาน

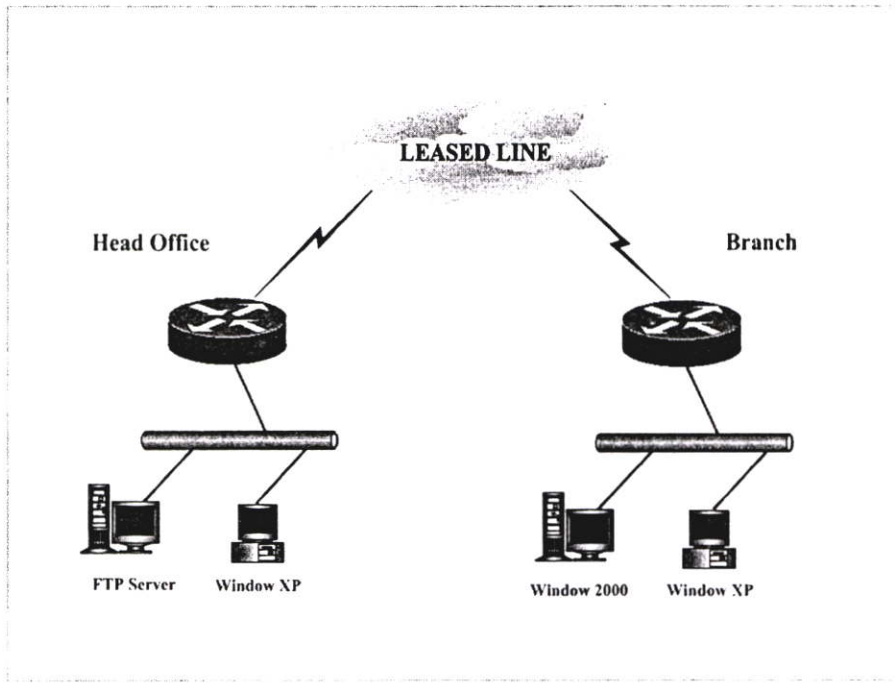
ในบทนี้จะกล่าวถึงการจำลองระบบและผลที่ได้จากการจำลองระบบโดยผลที่ได้จะแสดงให้เห็นประสิทธิภาพของระบบเมื่อนำอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) มาเชื่อมต่ออินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) โดยนำผลการทดสอบมาเปรียบเทียบ

6.1 แบบจำลอง

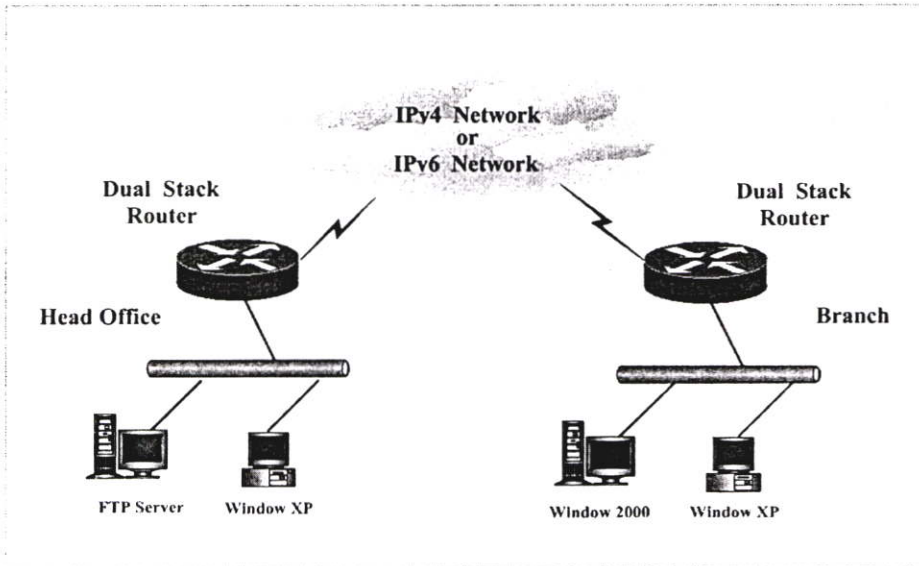
ในวิทยานิพนธ์นี้จะวิเคราะห์ระบบ โดยใช้ระบบจำลองซึ่งทำการทดสอบ 2 ระบบ คือ ระบบ LAN และ ระบบ WAN และ ลักษณะการเชื่อมต่อ 2 แบบ คือ Dual Stack และ 6to4 Tunneling



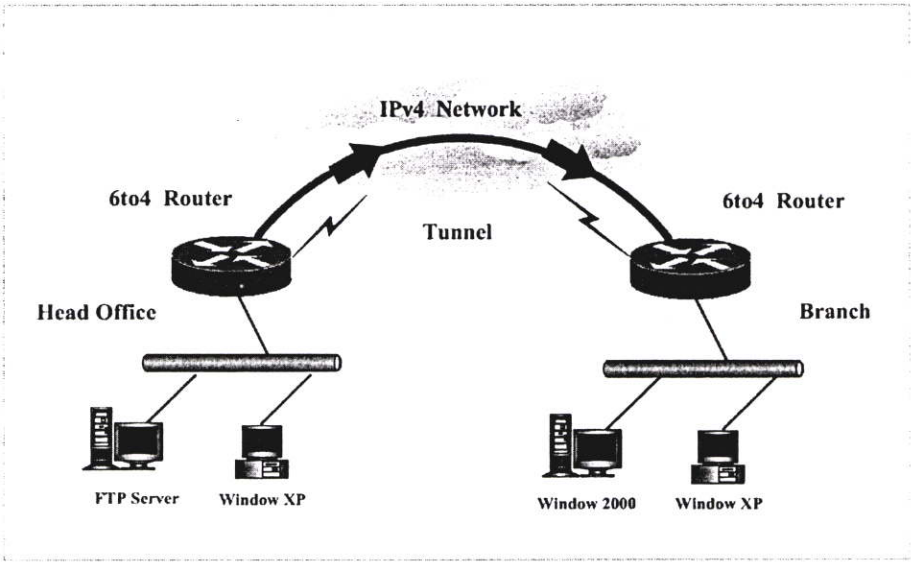
รูปที่ 6.1 ระบบเครือข่ายภายในองค์กรแบบ LAN



รูปที่ 6.2 ระบบเครือข่ายภายในองค์กรแบบ WAN



รูปที่ 6.3 ลักษณะการเชื่อมต่อ IPv6 และ IPv4 แบบ Dual Stack



รูปที่ 6.4 ลักษณะการเชื่อมต่อ IPv6 และ IPv4 แบบ 6to4 Tunneling

6.2 การกำหนดพารามิเตอร์ในระบบจำลอง

ค่าพารามิเตอร์ต่างๆ ที่ใช้กับแบบจำลองนี้สามารถแบ่งออกเป็น 3 ค่าหลัก คือ

6.2.1 ค่าพารามิเตอร์ของโทรโพโลยีการเชื่อมต่อ

6.2.2 ค่าพารามิเตอร์ลักษณะการใช้งานอินเตอร์เน็ตโพรโตคอลเวอร์ชั่นต่างๆ

6.2.3 ค่าพารามิเตอร์ลักษณะการเชื่อมต่อ IPv6 และ IPv4

โดยทำการจัดตั้ง FTP Server โดยทำการให้เครื่อง Client ทำการดึงข้อมูลจาก FTP Server ซึ่งได้ทำการทดสอบทั้งระบบ LAN และ ระบบ WAN ซึ่งทั้งสองระบบจะทดสอบทั้ง 4 แบบ

1. FTP Server (IPv4 Pure)
2. FTP Server (IPv6 Pure)
3. FTP Server (IPv4 แบบ Dual Stack)
4. FTP Server (IPv6 แบบ Dual Stack)

6.3 ผลที่ได้การทดลองตามแบบจำลอง

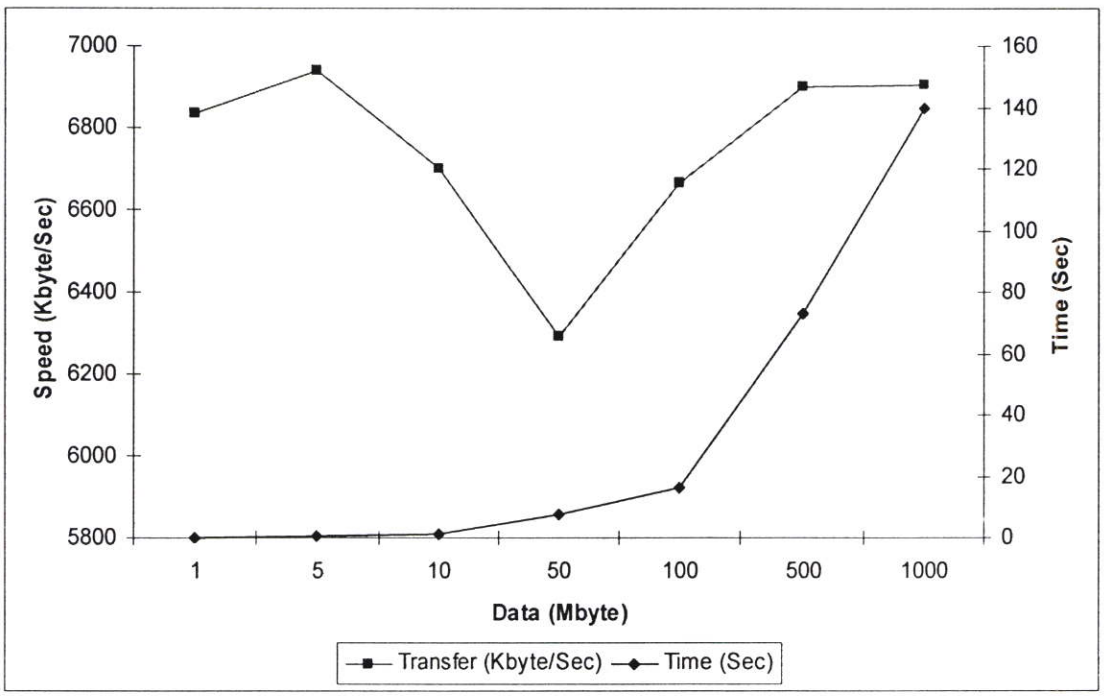
6.3.1 แบบจำลองระบบ LAN

1. FTP Server (IPv4 Pure) ทำการตั้ง FTP Server โดยใช้ IPv4 อย่างเดียว โดยให้เครื่อง Client ทำการดึงข้อมูล ซึ่งข้อมูลมีขนาดเพิ่มขึ้นเรื่อยจาก 1 Mbyte จนถึง 1 Gbyte ซึ่งได้ข้อมูลดังตารางที่ 6.1

ตารางที่ 6.1 แสดงข้อมูลทั้งหมดของ IPv4 (Pure) ของระบบ LAN

FTP IPv4 (Pure)		
Data (Mbyte)	Speed (Kbyte/Sec)	Time (Sec)
1	6834.98	0.16
5	6950.29	0.75
10	6698.02	1.4
50	6291.47	7.25
100	6663.87	15.97
500	6900.19	73
1000	6905.52	140

ลักษณะกราฟที่ได้



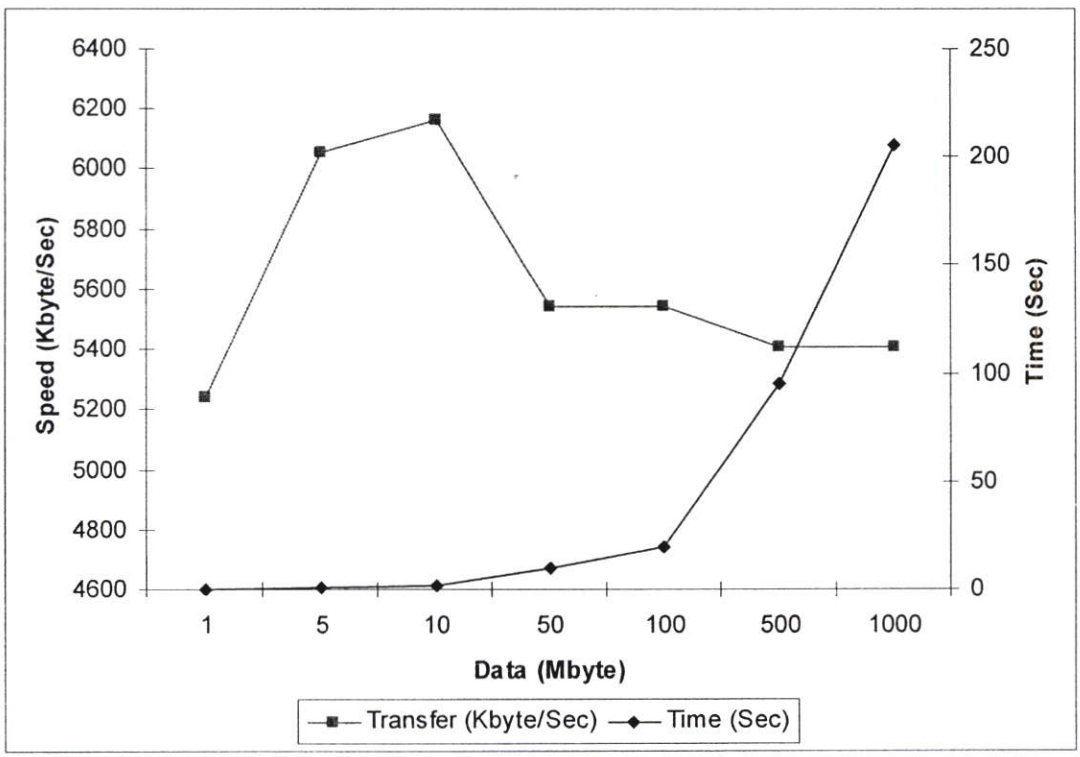
รูปที่ 6.5 กราฟแสดงความเร็วและระยะเวลาที่ทำการดึงข้อมูลของ IPv4 (Pure) ของระบบ LAN

2. FTP Server (IPv6 Pure) ทำการตั้ง FTP Server โดยใช้ IPv6 อย่างเดียว โดยให้เครื่อง Client ทำการดึงข้อมูล ซึ่งข้อมูลมีขนาดเพิ่มขึ้นเรื่อยจาก 1 Mbyte จนถึง 1 Gbyte ซึ่งได้ข้อมูลดังตารางที่ 6.2

ตารางที่ 6.2 แสดงข้อมูลทั้งหมดของ IPv6 (Pure) ของระบบ LAN

FTP IPv6 (Pure)		
Data (Mbyte)	Speed (Kbyte/Sec)	Time (Sec)
1	5240.15	0.21
5	6053.61	0.86
10	6163.56	1.74
50	5544.34	9.36
100	5541.54	19.21
500	5405.13	95.1
1000	5408.25	205.44

ลักษณะกราฟที่ได้



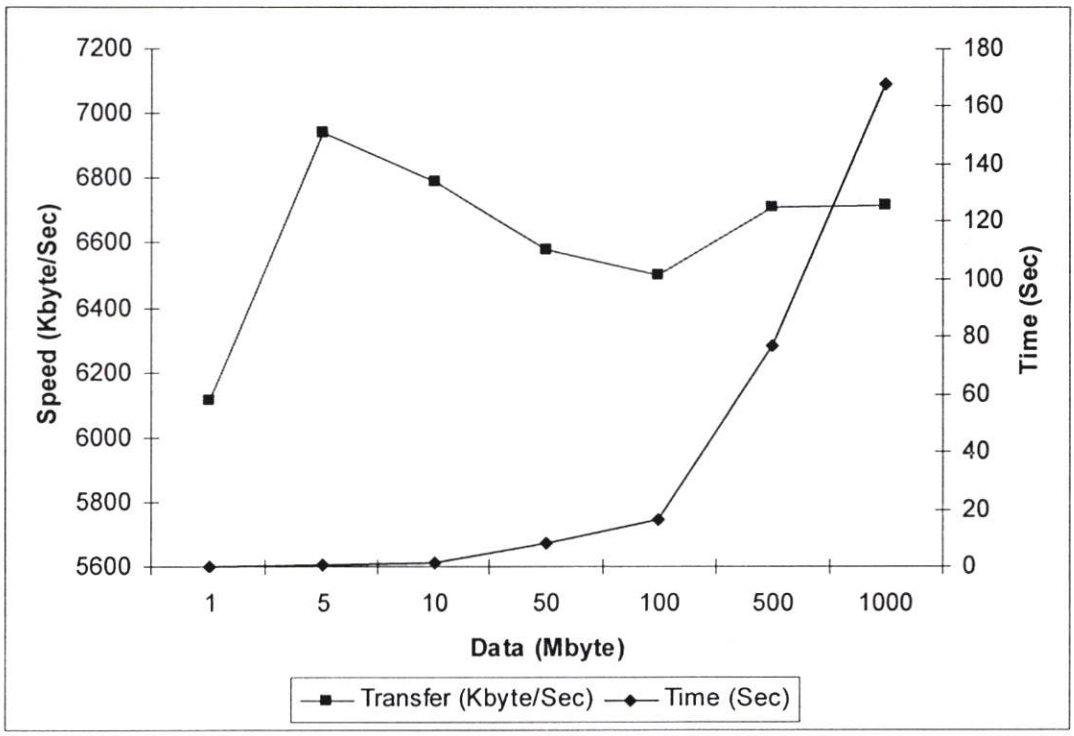
รูปที่ 6.6 กราฟแสดงความเร็วและระยะเวลาที่ทำการดึงข้อมูลของ IPv6 (Pure) ของระบบ LAN

3. FTP Server (IPv4 แบบ Dual Stack) ทำการตั้ง FTP Server โดยใช้ IPv4 แต่อยู่ในรูปแบบที่มีทั้ง IPv4 และ IPv6 ในการ์ดแลนเดียวกัน โดยใช้เครื่อง Client ทำการดึงข้อมูล ซึ่งข้อมูลมีขนาดเพิ่มขึ้นเรื่อยจาก 1 Mbyte จนถึง 1 Gbyte ซึ่งได้ข้อมูลดังตารางที่ 6.3

ตารางที่ 6.3 แสดงข้อมูลทั้งหมดของ IPv4 (Dual Stack) ของระบบ LAN

FTP IPv4 (Dual Stack)		
Data (Mbyte)	Speed (Kbyte/Sec)	Time (Sec)
1	6113.51	0.18
5	6940.29	0.75
10	6786.93	1.58
50	6579.3	7.898
100	6500.67	16.37
500	6713.84	76.56
1000	6716.1	167.67

ลักษณะกราฟที่ได้



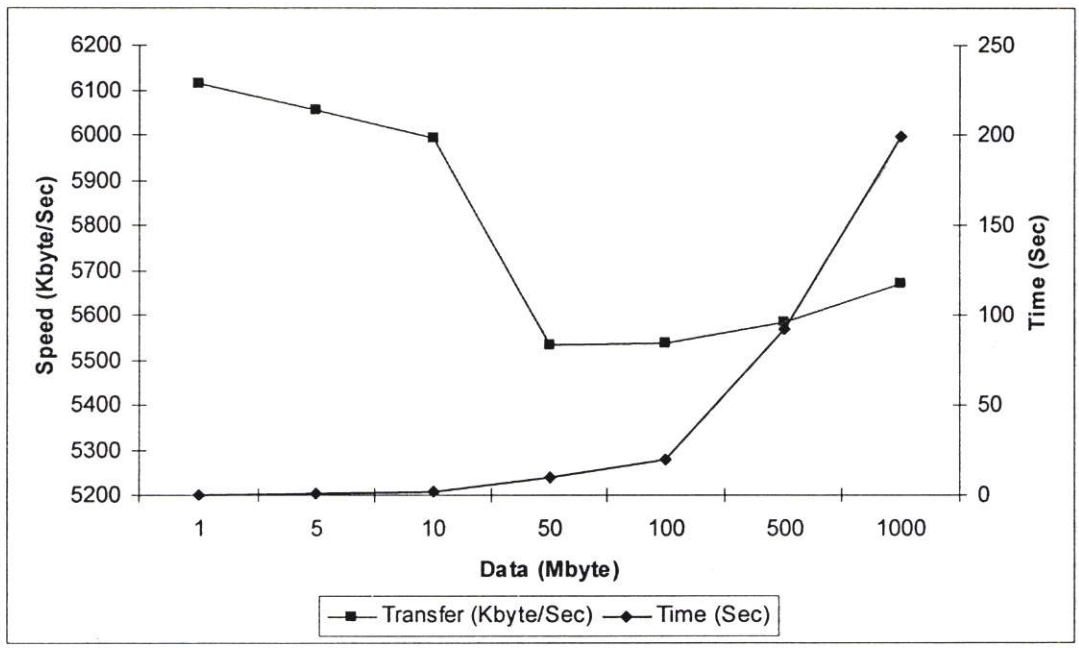
รูปที่ 6.7 กราฟแสดงความเร็วและระยะเวลาที่ทำการดึงข้อมูลของ IPv4 (Dual Stack) ของระบบ LAN

4. FTP Server (IPv6 แบบ Dual Stack) ทำการตั้ง FTP Server โดยใช้ IPv6 แต่อยู่ในรูปแบบที่มีทั้ง IPv4 และ IPv6 ในการ์ดแลนเดียวกัน โดยใช้เครื่อง Client ทำการดึงข้อมูล ซึ่งข้อมูลมีขนาดเพิ่มขึ้นเรื่อยจาก 1 Mbyte จนถึง 1 Gbyte ซึ่งได้ข้อมูลดังตารางที่ 6.4

ตารางที่ 6.4 แสดงข้อมูลทั้งหมดของ IPv6 (Dual Stack) ของระบบ LAN

FTP IPv6 (Dual Stack)		
Data (Mbyte)	Speed (Kbyte/Sec)	Time (Sec)
1	6113.51	0.18
5	6053.61	0.86
10	5991.59	1.79
50	5533.12	9.38
100	5538.66	19.22
500	5582.71	92.07
1000	5669.42	198.63

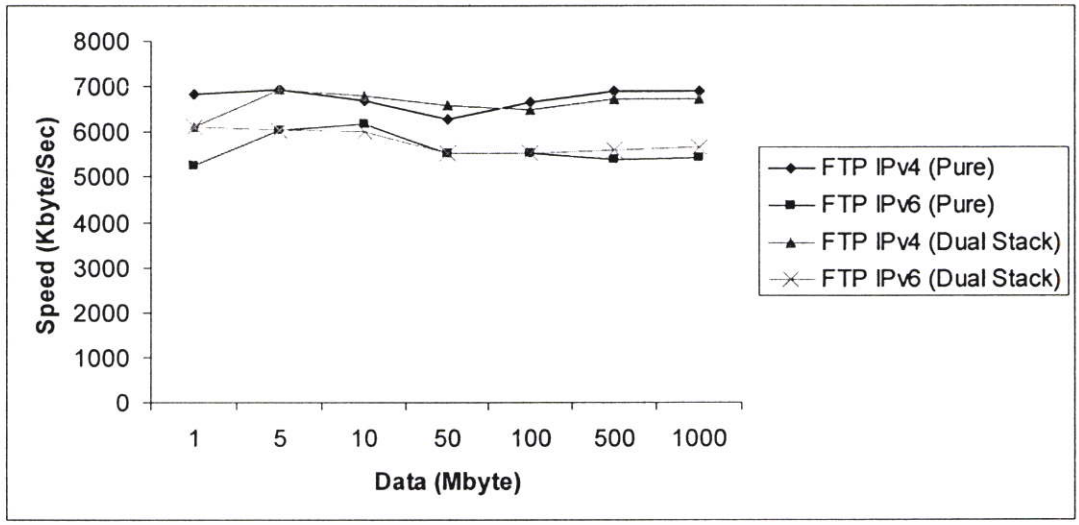
ลักษณะกราฟที่ได้



รูปที่ 6.8 กราฟแสดงความเร็วและระยะเวลาที่ทำการดึงข้อมูลของ IPv6 (Dual Stack) ของระบบ LAN

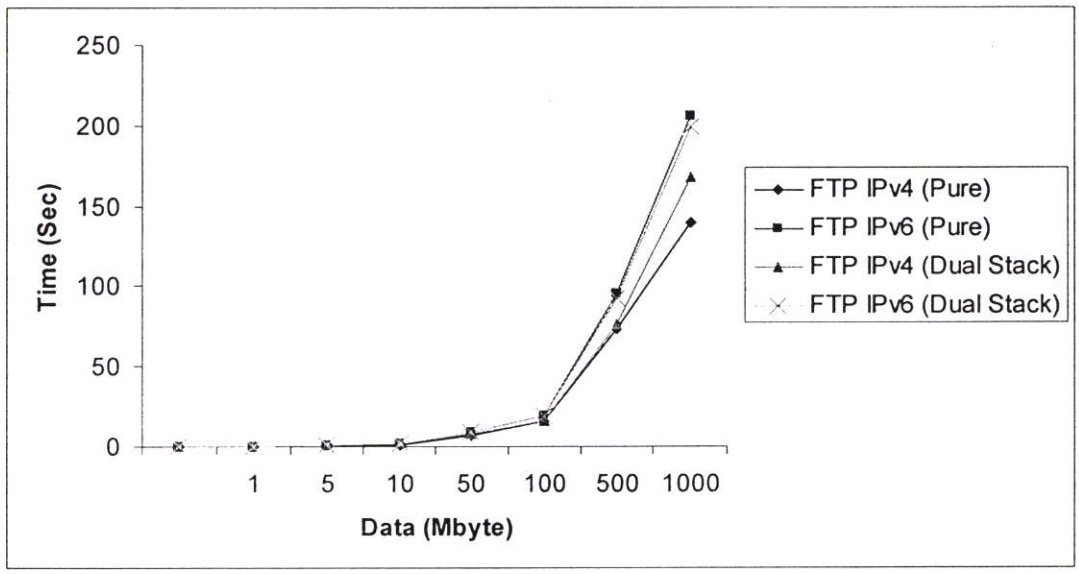
ซึ่งจากการที่ทดสอบโดยทำการดึงข้อมูลจาก FTP Server ทั้ง 4 แบบนั้น เราสามารถนำข้อมูลมาเทียบเพื่อดูความเร็ว (Speed) หรือ เวลา (Time) ได้

- เมื่อเทียบกับความเร็ว



รูปที่ 6.9 กราฟแสดงความเร็วที่ทำการดึงข้อมูลของระบบ LAN ทั้งหมด

- เมื่อเทียบกับระยะเวลา



รูปที่ 6.10 กราฟแสดงระยะเวลาที่ทำการดึงข้อมูลของระบบ LAN ทั้งหมด

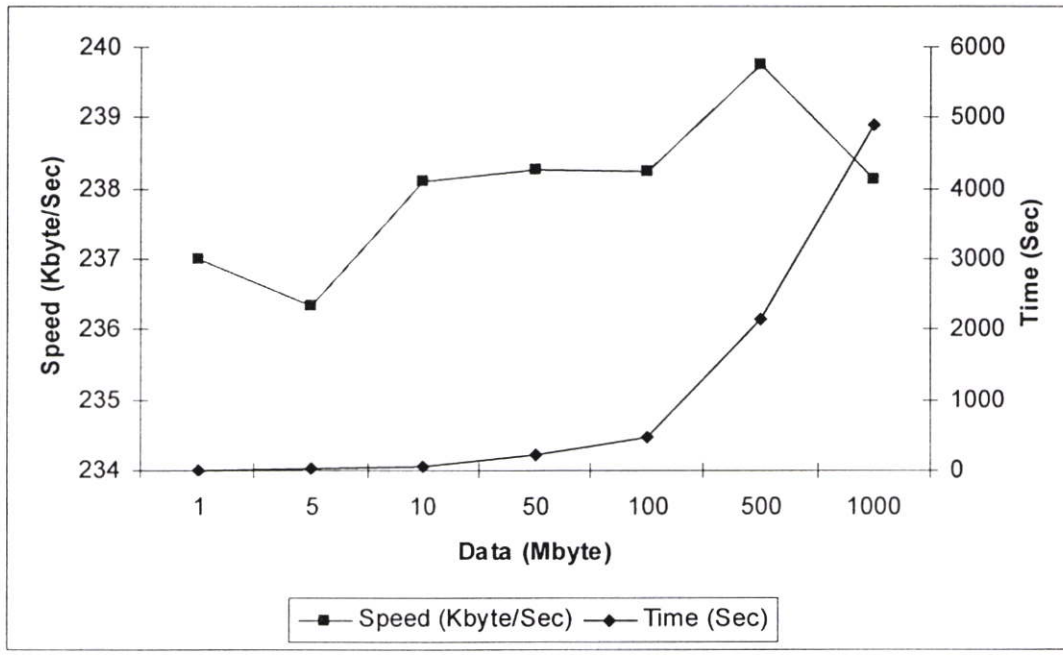
6.3.2 แบบจำลองระบบ WAN

1. FTP Server (IPv4 Pure) ทำการตั้ง FTP Server โดยใช้ IPv4 อย่างเดียว โดยให้เครื่อง Client ทำการดึงข้อมูล ซึ่งข้อมูลมีขนาดเพิ่มขึ้นเรื่อยจาก 1 Mbyte จนถึง 1 Gbyte ซึ่งได้ข้อมูลดังตารางที่ 6.5

ตารางที่ 6.5 แสดงข้อมูลทั้งหมดของ IPv4 (Pure) ของระบบ WAN

FTP IPv4 (Pure)		
Data (Mbyte)	Speed (Kbyte/Sec)	Time (Sec)
1	237	5.04
5	236.35	27.91
10	238.09	44.69
50	238.27	227.14
100	238.23	477.47
500	239.74	2144.06
1000	238.13	4892.35

ลักษณะกราฟที่ได้



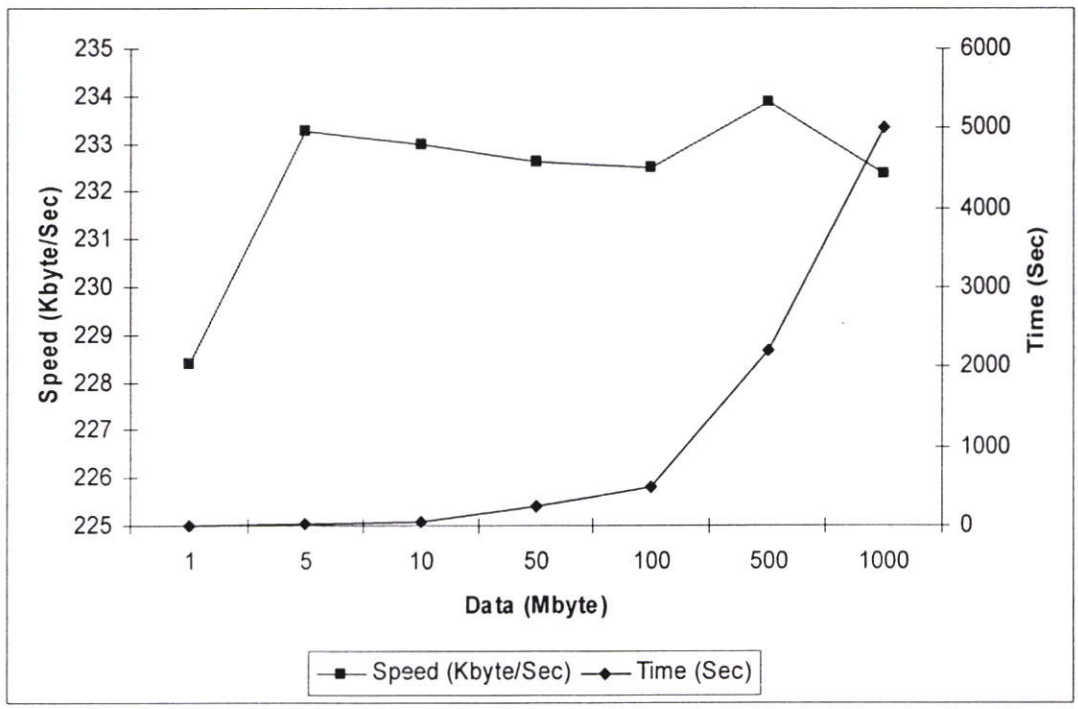
รูปที่ 6.11 กราฟแสดงความเร็วและระยะเวลาการที่ทำการดึงข้อมูลของ IPv4 (Pure) ของระบบ WAN

2. FTP Server (IPv6 Pure) ทำการตั้ง FTP Server โดยใช้ IPv6 อย่างเดียว โดยให้เครื่อง Client ทำการดึงข้อมูล ซึ่งข้อมูลมีขนาดเพิ่มขึ้นเรื่อยจาก 1 Mbyte จนถึง 1 Gbyte ซึ่งได้ข้อมูลดังตารางที่ 6.6

ตารางที่ 6.6 แสดงข้อมูลทั้งหมดของ IPv6 (Pure) ของระบบ WAN

FTP IPv6 (Pure)		
Data (Mbyte)	Speed (Kbyte/Sec)	Time (Sec)
1	228.39	5.23
5	233.25	28.28
10	232.98	45.67
50	232.61	232.66
100	232.50	489.24
500	233.87	2197.86
1000	232.39	5013.12

ลักษณะกราฟที่ได้



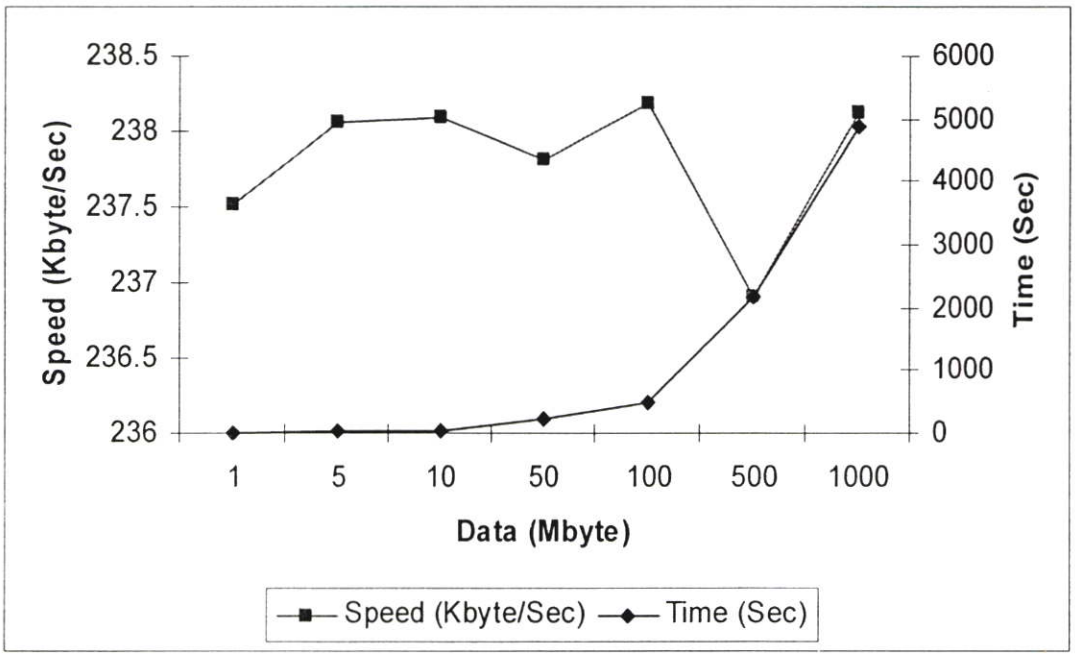
รูปที่ 6.12 กราฟแสดงความเร็วและระยะเวลาการที่ทำการดึงข้อมูลของ IPv6 (Pure) ของระบบ WAN

3. FTP Server (IPv4 แบบ Dual Stack) ทำการตั้ง FTP Server โดยใช้ IPv4 แต่อยู่ในรูปแบบที่มีทั้ง IPv4 และ IPv6 ในการ์ดแลนเดียวกัน โดยใช้เครื่อง Client ทำการดึงข้อมูล ซึ่งข้อมูลมีขนาดเพิ่มขึ้นเรื่อยจาก 1 Mbyte จนถึง 1 Gbyte ซึ่งได้ข้อมูลดังตารางที่ 6.7

ตารางที่ 6.7 แสดงข้อมูลทั้งหมดของ IPv4 (Dual Stack) ของระบบ WAN

FTP IPv4 (Dual Stack)		
Data (Mbyte)	Speed (Kbyte/Sec)	Time (Sec)
1	237.52	5.03
5	238.07	27.71
10	238.09	44.70
50	237.82	227.57
100	238.19	477.55
500	236.90	2169
1000	238.13	4892.35

ลักษณะกราฟที่ได้



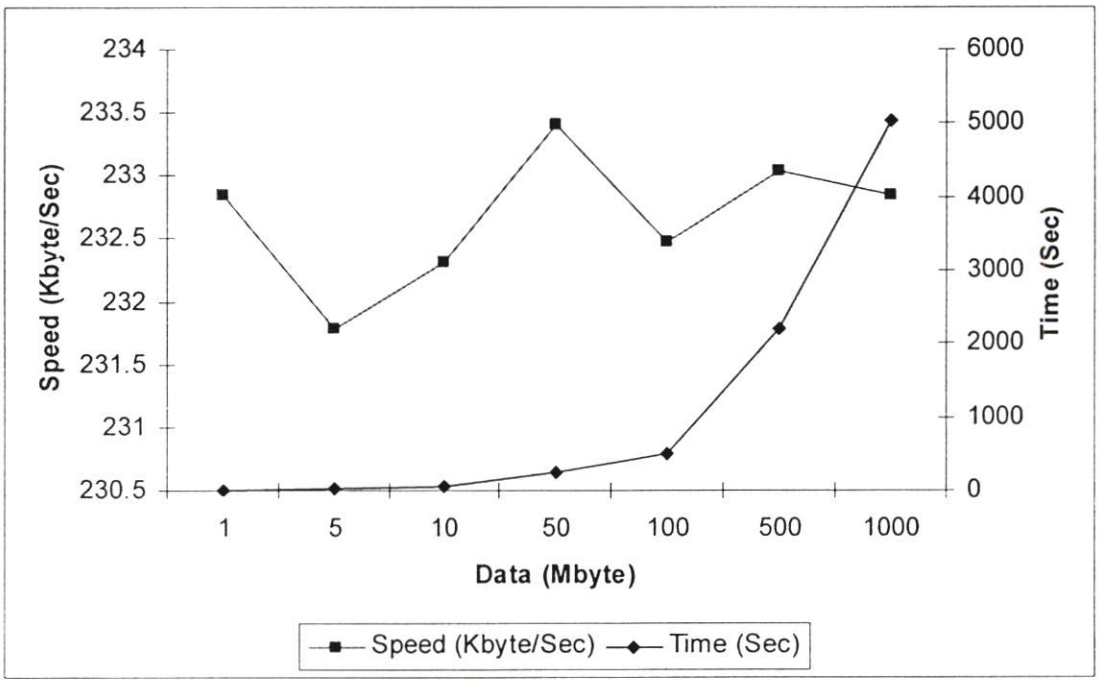
รูปที่ 6.13 กราฟแสดงความเร็วและระยะเวลาการที่ทำการดึงข้อมูลของ IPv4 (Dual Stack) ของระบบ WAN

4. FTP Server (IPv6 แบบ Dual Stack) ทำการตั้ง FTP Server โดยใช้ IPv4 แต่อยู่ในรูปแบบที่มีทั้ง IPv4 และ IPv6 ในการ์ดแลนเดียวกัน โดยใช้เครื่อง Client ทำการดึงข้อมูล ซึ่งข้อมูลมีขนาดเพิ่มขึ้นเรื่อยจาก 1 Mbyte จนถึง 1 Gbyte ซึ่งได้ข้อมูลดังตารางที่ 6.8

ตารางที่ 6.8 แสดงข้อมูลทั้งหมดของ IPv6 (Dual Stack) ของระบบ WAN

FTP IPv6 (Dual Stack)		
Data (Mbyte)	Speed (Kbyte/Sec)	Time (Sec)
1	232.84	5.13
5	231.78	28.46
10	232.31	45.81
50	233.41	242.24
100	232.47	489.31
500	233.04	2205.64
1000	232.84	5024.95

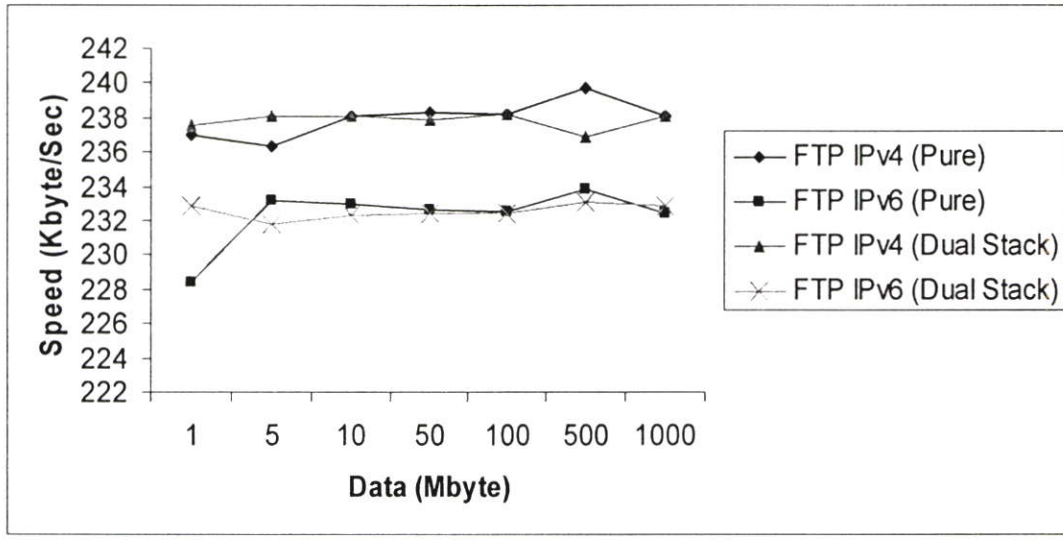
ลักษณะกราฟที่ได้



รูปที่ 6.14 กราฟแสดงความเร็วและระยะเวลาการที่ทำการดึงข้อมูลของ IPv6 (Dual Stack) ของระบบ WAN

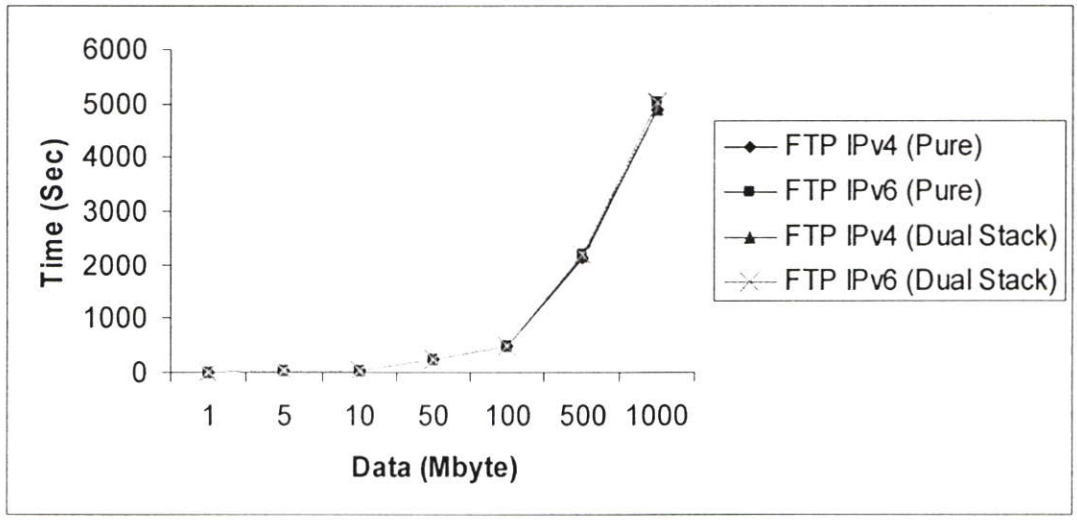
ซึ่งจากการที่ทดสอบโดยทำการดึงข้อมูลจาก FTP Server ทั้ง 4 แบบนั้น เราสามารถนำข้อมูลมาเทียบเพื่อดูความเร็ว (Speed) หรือ เวลา (Time) ได้

- เมื่อเทียบความเร็ว



รูปที่ 6.15 กราฟแสดงความเร็วสูงสุดที่ทำการดึงข้อมูลได้ของระบบ WAN ทั้งหมด

- เมื่อเทียบกับระยะเวลา



รูปที่ 6.16 กราฟแสดงระยะเวลาที่ทำการดึงข้อมูลได้ของระบบ WAN ทั้งหมด

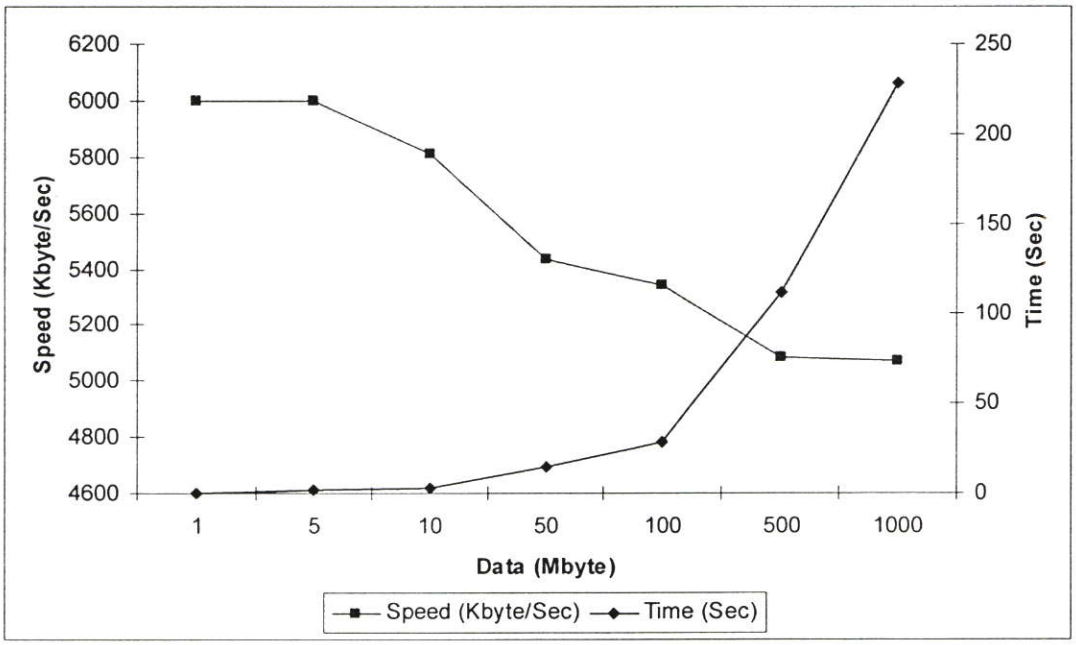
6.3.3 แบบจำลองลักษณะการเชื่อมต่อ IPv6 และ IPv4 แบบ 6to4 Tunneling

FTP Server (IPv6 แบบ 6to4 Tunneling) ทำการตั้ง FTP Server โดยใช้ IPv4 แต่อยู่ในรูปแบบที่มีทั้ง IPv4 และ IPv6 ในการ์ดแลนเดียวกัน โดยใช้เครื่อง Client ทำการดึงข้อมูล ซึ่งข้อมูลมีขนาดเพิ่มขึ้นเรื่อยจาก 1 Mbyte จนถึง 1 Gbyte ซึ่งได้ข้อมูลดังตารางที่ 6.9

ตารางที่ 6.9 แสดงข้อมูลทั้งหมดของ IPv6 (6to4Tunneling)

FTP IPv6 (6to4Tunneling)		
Data (Mbyte)	Speed (Kbyte/Sec)	Time (Sec)
1	6000.51	0.4
5	5999.61	1.9
10	5811.59	2.64
50	5433.12	14.59
100	5338.66	28.22
500	5082.71	112.07
1000	5069.42	228.63

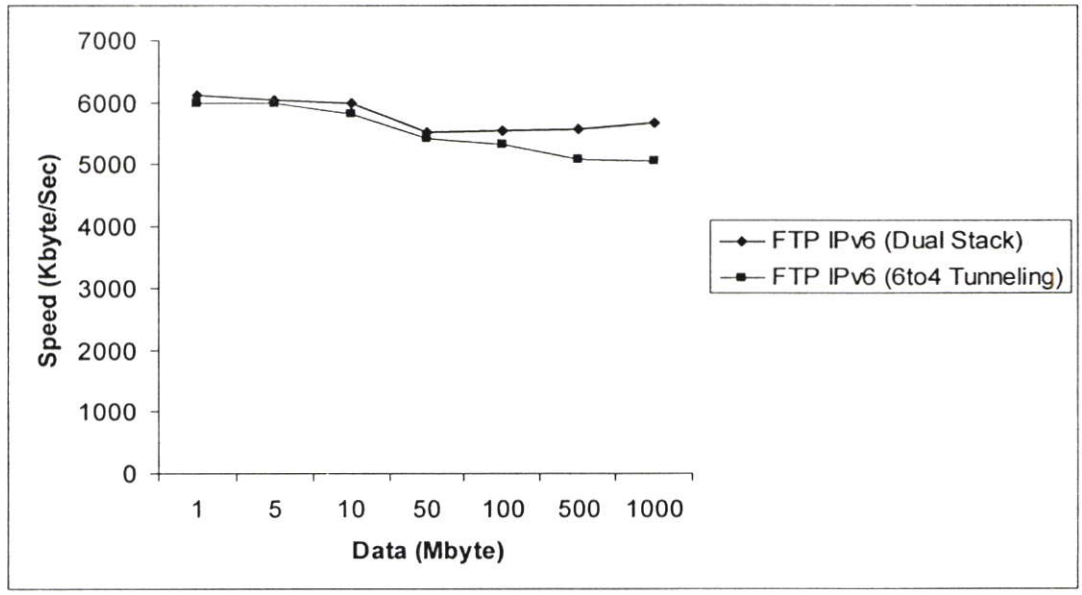
ลักษณะกราฟที่ได้



รูปที่ 6.17 กราฟแสดงความเร็วและระยะเวลาการที่ทำการดึงข้อมูลของ IPv6 (6to4 Tunneling)

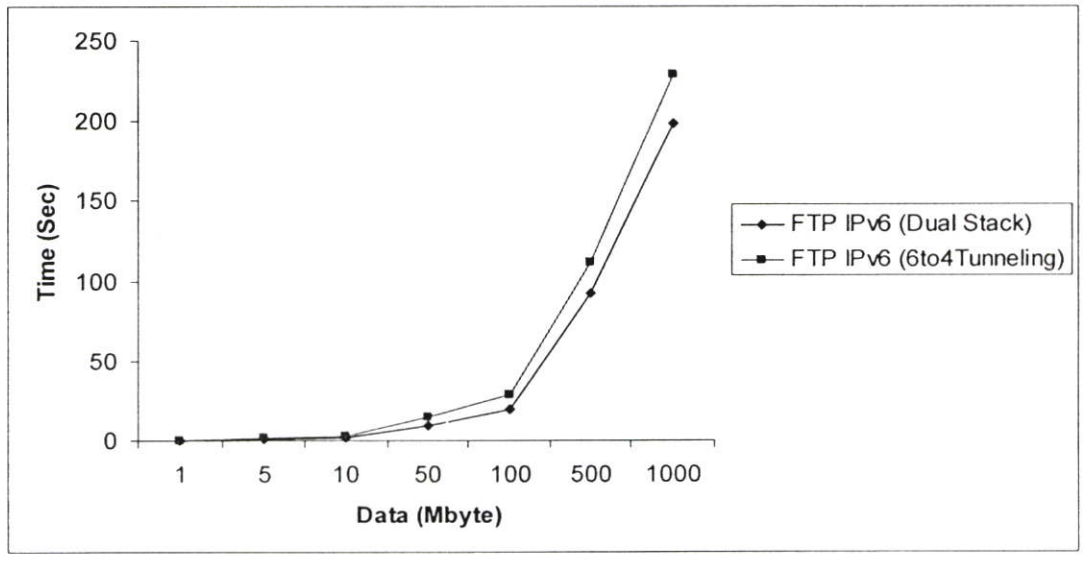
ซึ่งจากการที่ทดสอบโดยทำการดึงข้อมูลจาก FTP Server โดยมีลักษณะการเชื่อมต่อ IPv6 กับ IPv4 ทั้งแบบ Dual Stack กับ Tunneling 6to4 เราสามารถนำข้อมูลมาเทียบเพื่อดูความเร็ว (Speed) หรือ เวลา (Time) ได้

- เมื่อเทียบความเร็ว



รูปที่ 6.18 กราฟแสดงการเปรียบเทียบความเร็วระหว่างลักษณะการเชื่อมต่อ Dual Stack กับ 6to4 Tunneling

- เมื่อเทียบกับระยะเวลา



รูปที่ 6.19 กราฟแสดงการเปรียบเทียบระยะเวลาของลักษณะการเชื่อมต่อ Dual Stack กับ 6to4 Tunneling

บทที่ 7
สรุปผลการวิจัยและข้อเสนอแนะ

ความต้องการใช้เทคโนโลยีอินเตอร์เน็ตมีการเพิ่มขึ้นอย่างรวดเร็ว ดังจะเห็นได้จากการเพิ่มขึ้นของความต้องการอินเตอร์เน็ต จึงทำให้มีการผลักดันให้เริ่มมีการใช้งานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) ถึงแม้จะเป็นที่ยอมรับกันโดยทั่วไปว่าสักวันหนึ่งอินเทอร์เน็ตจะต้องเปลี่ยนไปใช้อินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) แต่ความตื่นตัวในการปรับเปลี่ยนได้เกิดขึ้นช้ากว่าที่คาดหมายกันไว้ สาเหตุสำคัญอาจเนื่องมาจากทัศนคติที่ว่าตราบใดที่อินเทอร์เน็ตยังไม่ขาดแคลนไอพีแอดเดรสอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) ยังคงเป็นสิ่งฟุ่มเฟือยและยังไม่จำเป็นมากนัก ถึงกระนั้นก็ตามอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (IPv6) เริ่มได้รับการยอมรับเพิ่มมากขึ้นเพราะผู้ให้บริการอินเทอร์เน็ตต่างตระหนักดีว่าไม่ช้าก็เร็ว ปัญหาการขาดแคลนไอพีแอดเดรสจะต้องมาถึงและเมื่อถึงเวลานั้นผู้ที่มีความพร้อมมากกว่าจะเป็นผู้ได้เปรียบ นอกจาก นั้น IPv6 ยังเป็นทางออกที่ถาวรทางเดียวในการแก้ปัญหานี้

การใช้งานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) นั้นยังสามารถนำไปใช้งานกับการใช้งานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) ได้โดยใช้เทคนิคการเชื่อมต่อได้ 3 ชนิดด้วยกัน คือ การใช้งานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (IPv6) และ อินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) ควบคู่กันหรือที่เรียกว่า Dual Stack, การทะลุผ่านข้อมูล (Tunneling), และการแปลงข้อมูล (Translation) ขึ้นกับความเหมาะสมของแต่ละองค์กร

วิทยานิพนธ์ฉบับนี้ได้นำเสนอวิธีการทดสอบประสิทธิภาพของระบบเมื่อนำอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) มาทดสอบเปรียบเทียบกับอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) ทำการจัดตั้ง FTP Server โดยทำการให้เครื่อง Client ทำการดึงข้อมูลจาก FTP Server ซึ่งได้ทำการทดสอบทั้งระบบ LAN และ ระบบ WAN ซึ่งทั้งสองระบบจะทดสอบทั้ง 4 แบบ

1. FTP Server (IPv4 Pure)
2. FTP Server (IPv6 Pure)
3. FTP Server (IPv4 แบบ Dual Stack)
4. FTP Server (IPv6 แบบ Dual Stack)

และทำการดึงข้อมูล ซึ่งขนาดของข้อมูลมี 1, 5, 10, 50, 100, 500, 1000 Mbyte แล้วนำผลมาเปรียบเทียบว่าการดึงข้อมูลจาก FTP Server จะมีประสิทธิภาพของระบบเป็นอย่างไร

วิธีการที่นำเสนอในวิทยานิพนธ์ จะพบว่าการใช้งานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) เมื่อเทียบกับอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (IPv4) จะพบว่าการใช้งานของระบบมีประสิทธิภาพต่ำลง อาจจะขึ้นอยู่กับขนาดของ Header โดยอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) มีขนาด 40 Byte แต่อินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) มีขนาด 20 Byte ซึ่งในอนาคตอาจจะมีการพัฒนาทางด้านฮาร์แวร์ (Hardware) และ ทางด้านซอฟท์แวร์ (Software) มากขึ้น

บรรณานุกรม

[1] D. Régis, 2003. **Cisco Self-Study : Implementing Cisco IPv6 Networks (IPv6).** Indianapolis : Cisco Press.

[2] Y.M. Yussoff, M. Samad, **Implementation of native IPv6 test-bed for network link quality and performance analysis.** IEEE Internet Computing, pp. 453 – 455, July 2002.

[3] G.H. Yong, K.S. Myung, J.K. Hyoung, **Application translation for IPv6 at NAT-PT.** The 9th Asia-Pacific Conference, vol. 1, pp. 203 – 207, Sep 2003.

[4] T. Yazaki, T. Kanetake, S. Akahane, Y. Sakata, K. Sugai, H. Yano, **High-speed IPv6 router/switch architecture.** IEEE Internet Computing, pp. 153-158, Jan 2004.

[5] ภาสกร ประถมบุตร พนิตา พงษ์ไพบูลย์ ธีรีสา มัทวพันธุ์ ฉัตรชัย จันทร์อินทร์ **ความรู้ - เบื้องต้นเกี่ยวกับ IPv6 สำหรับผู้ใช้งานทั่วไป** ศูนย์เทคโนโลยีอิเล็กทรอนิกส์ และคอมพิวเตอร์แห่งชาติ มีนาคม 2548.

[6] พนิตา พงษ์ไพบูลย์ เฉลิมพล ชาญศรีภิญโญ ฉัตรชัย จันทร์อินทร์ อดิศักดิ์ บุศรานันท์ **การเตรียมความพร้อมในการเชื่อมต่อเข้าสู่อินเทอร์เน็ตยุคหน้า** มีนาคม 2548.

ภาคผนวก

ภาคผนวก ก. ตัวอย่าง Configuration ของ Router BRANCH แบบ IPv4 (Pure)

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname BRANCH
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$L4jX$RZCizqMkuF8bhfVA6/lXE1
!
no aaa new-model
ip subnet-zero
!
hub ether 0 1
link-test
auto-polarity
!
hub ether 0 2
link-test
auto-polarity
!
hub ether 0 3
link-test
auto-polarity
!
hub ether 0 4
link-test
auto-polarity
!
```

```
hub ether 0 5
link-test
auto-polarity
!
hub ether 0 6
link-test
auto-polarity
!
hub ether 0 7
link-test
auto-polarity
!
hub ether 0 8
link-test
auto-polarity
!
hub ether 0 9
link-test
auto-polarity
!
hub ether 0 10
link-test
auto-polarity
!
hub ether 0 11
link-test
auto-polarity
!
hub ether 0 12
link-test
auto-polarity
!
hub ether 0 13
```

```
link-test
auto-polarity
!
hub ether 0 14
link-test
auto-polarity
!
hub ether 0 15
link-test
auto-polarity
!
hub ether 0 16
link-test
auto-polarity
!
interface Ethernet0
ip address 192.168.2.1 255.255.255.0

interface Serial0
ip address 10.10.10.2 255.255.255.252
clock rate 2000000
no fair-queue
!
interface Serial1
no ip address
shutdown
!
router rip
version 2
network 10.0.0.0
network 192.168.2.0
!
ip http server
```

```
ip classless
!
line con 0
line aux 0
line vty 0 4
password cisco
login
!
end
```

ภาคผนวก ข. ตัวอย่าง Configuration ของ Router BRANCH แบบ IPv6 (Pure)

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname BRANCH
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$sHrp$lc.BCpTuL2aQ3PfEmeFkw1
!
no aaa new-model
ip subnet-zero
!
ipv6 unicast-routing
!
hub ether 0 1
link-test
auto-polarity
!
hub ether 0 2
link-test
auto-polarity
!
hub ether 0 3
link-test
auto-polarity
!
hub ether 0 4
link-test
```

```
auto-polarity
!
hub ether 0 5
link-test
auto-polarity
!
hub ether 0 6
link-test
auto-polarity
!
hub ether 0 7
link-test
auto-polarity
!
hub ether 0 8
link-test
auto-polarity
!
hub ether 0 9
link-test
auto-polarity
!
hub ether 0 10
link-test
auto-polarity
!
hub ether 0 11
link-test
auto-polarity
!
hub ether 0 12
link-test
auto-polarity
```

```
!
hub ether 0 13
link-test
auto-polarity
!
hub ether 0 14
link-test
auto-polarity
!
hub ether 0 15
link-test
auto-polarity
!
hub ether 0 16
link-test
auto-polarity
!
interface Ethernet0
ipv6 address 3FFE:B00:FFFF:2::/64 eui-64
ipv6 enable
ipv6 rip thsis enable
!
interface Serial0
ipv6 address 3FFE:B00:FFFF:4::/64
ipv6 enable
ipv6 rip thsis enable
clock rate 2000000
no fair-queue
!
interface Serial1
no ip address
shutdown
```

```
ip http server
ip classless
!
ipv6 router rip thsis
!
line con 0
line aux 0
line vty 0 4
password cisco
login
!
end
```

ภาคผนวก ค. ตัวอย่าง Configuration ของ Router BRANCH แบบ Dual Stack

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname BRANCH
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$sHrp$lc.BCpTuL2aQ3PfEmeFkw1
!
no aaa new-model
ip subnet-zero
!
ipv6 unicast-routing
!
hub ether 0 1
link-test
auto-polarity
!
hub ether 0 2
link-test
auto-polarity
!
hub ether 0 3
link-test
auto-polarity
!
hub ether 0 4
link-test
```

```
auto-polarity
!
hub ether 0 5
link-test
auto-polarity
!
hub ether 0 6
link-test
auto-polarity
!
hub ether 0 7
link-test
auto-polarity
!
hub ether 0 8
link-test
auto-polarity
!
hub ether 0 9
link-test
auto-polarity
!
hub ether 0 10
link-test
auto-polarity
!
hub ether 0 11
link-test
auto-polarity
!
hub ether 0 12
link-test
auto-polarity
```

```
!
hub ether 0 13
link-test
auto-polarity
!
hub ether 0 14
link-test
auto-polarity
!
hub ether 0 15
link-test
auto-polarity
!
hub ether 0 16
link-test
auto-polarity
!
interface Ethernet0
ip address 192.168.2.1 255.255.255.0
ipv6 address 3FFE:B00:FFFF:2::/64 eui-64
ipv6 enable
ipv6 rip thsis enable
!
interface Serial0
ip address 10.10.10.2 255.255.255.252
ipv6 address 3FFE:B00:FFFF:4::/64
ipv6 enable
ipv6 rip thsis enable
clock rate 2000000
no fair-queue
!
interface Serial1
no ip address
```

```
shutdown
!
router rip
version 2
network 10.0.0.0
network i92.168.2.0
!
ip http server
ip classless
!
ipv6 router rip thsis
!
line con 0
line aux 0
line vty 0 4
password cisco
login
!
end
```

ภาคผนวก ง. ตัวอย่าง Configuration ของ Router BRANCH แบบ 6to4 Tunneling

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname BRANCH
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$h7KC$yAhUuATwfSMbaaVZUt1W41
!
no aaa new-model
ip subnet-zero
!
ipv6 unicast-routing
!
hub ether 0 1
link-test
auto-polarity
!
hub ether 0 2
link-test
auto-polarity
!
hub ether 0 3
link-test
auto-polarity
!
hub ether 0 4
link-test
```

```
auto-polarity
!
hub ether 0 5
link-test
auto-polarity
!
hub ether 0 6
link-test
auto-polarity
!
hub ether 0 7
link-test
auto-polarity
!
hub ether 0 8
link-test
auto-polarity
!
hub ether 0 9
link-test
auto-polarity
!
hub ether 0 10
link-test
auto-polarity
!
hub ether 0 11
link-test
auto-polarity
!
hub ether 0 12
link-test
auto-polarity
```

```
hub ether 0 13
link-test
auto-polarity
!
hub ether 0 14
link-test
auto-polarity
!
hub ether 0 15
link-test
auto-polarity
!
hub ether 0 16
link-test
auto-polarity
!
interface Tunnel1
no ip address
no ip redirects
ipv6 unnumbered Ethernet0
tunnel source Serial0
tunnel mode ipv6ip 6to4
!
interface Ethernet0
no ip address
ipv6 address 2002:C0A8:12::/64 eui-64
ipv6 enable
ipv6 nd prefix 2002:C0A8:12::/64 300 300
!
interface Serial0
ip address 192.168.1.2 255.255.255.0
!
interface Serial1
```

```
no ip address
shutdown
!
ip http server
ip classless
!
ipv6 route 2002::/16 Tunnel1
!
line con 0
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

ภาคผนวก จ. ตัวอย่าง Configuration ของ Router HQ แบบ IPv4 (Pure)

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$sHrp$lc.BCpTuL2aQ3PfEmeFkw1
!
no aaa new-model
ip subnet-zero
!
hub ether 0 1
link-test
auto-polarity
!
hub ether 0 2
link-test
auto-polarity
!
hub ether 0 3
link-test
auto-polarity
!
hub ether 0 4
link-test
auto-polarity
!
```

```
hub ether 0 5
link-test
auto-polarity
!
hub ether 0 6
link-test
auto-polarity
!
hub ether 0 7
link-test
auto-polarity
!
hub ether 0 8
link-test
auto-polarity
!
hub ether 0 9
link-test
auto-polarity
!
hub ether 0 10
link-test
auto-polarity
!
hub ether 0 11
link-test
auto-polarity
!
hub ether 0 12
link-test
auto-polarity
!
hub ether 0 13
```

```
link-test
auto-polarity
!
hub ether 0 14
link-test
auto-polarity
!
interface Ethernet0
ip address 192.168.1.1 255.255.255.0

interface Serial0
ip address 10.10.10.1 255.255.255.252

no fair-queue
!
interface Serial1
no ip address
shutdown
!
interface BRI0
no ip address
shutdown
!
router rip
version 2
network 10.0.0.0
network 192.168.1.0
!
ip http server
ip classless
!
line con 0
line aux 0
```

```
line vty 0 4
password cisco
login
!
end
```

ภาคผนวก ฉ. ตัวอย่าง Configuration ของ Router HQ แบบ IPv6 (Pure)

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$sHrp$lc.BCpTuL2aQ3PfEmeFkw1
!
no aaa new-model
ip subnet-zero
!
ipv6 unicast-routing
!
hub ether 0 1
link-test
auto-polarity
!
hub ether 0 2
link-test
auto-polarity
!
hub ether 0 3
link-test
auto-polarity
!
hub ether 0 4
link-test
```

```
auto-polarity
!
hub ether 0 5
link-test
auto-polarity
!
hub ether 0 6
link-test
auto-polarity
!
hub ether 0 7
link-test
auto-polarity
!
hub ether 0 8
link-test
auto-polarity
!
hub ether 0 9
link-test
auto-polarity
!
hub ether 0 10
link-test
auto-polarity
!
hub ether 0 11
link-test
auto-polarity
!
hub ether 0 12
link-test
auto-polarity
```

```
!
hub ether 0 13
link-test
auto-polarity
!
hub ether 0 14
link-test
auto-polarity
!
interface Ethernet0
ipv6 address 3FFE:B00:FFFF:1::/64 eui-64
ipv6 enable
ipv6 rip thsis enable
!
interface Serial0
ipv6 address 3FFE:B00:FFFF:3::/64
ipv6 enable
ipv6 rip thsis enable
no fair-queue
!
interface Serial1
no ip address
shutdown
!
interface BRI0
no ip address
shutdown
!
ip http server
ip classless
!
ipv6 router rip thsis
!
```

```
line con 0
line aux 0
line vty 0 4
password cisco
login
!
end
```

ภาคผนวก ช. ตัวอย่าง Configuration ของ Router HQ แบบ Dual Stack

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$sHrp$lc.BCpTuL2aQ3PfEmeFkw1
!
no aaa new-model
ip subnet-zero
!
ipv6 unicast-routing
!
hub ether 0 1
link-test
auto-polarity
!
hub ether 0 2
link-test
auto-polarity
!
hub ether 0 3
link-test
auto-polarity
!
hub ether 0 4
link-test
```

```
auto-polarity
!
hub ether 0 5
link-test
auto-polarity
!
hub ether 0 6
link-test
auto-polarity
!
hub ether 0 7
link-test
auto-polarity
!
hub ether 0 8
link-test
auto-polarity
!
hub ether 0 9
link-test
auto-polarity
!
hub ether 0 10
link-test
auto-polarity
!
hub ether 0 11
link-test
auto-polarity
!
hub ether 0 12
link-test
auto-polarity
```

```
!
hub ether 0 13
link-test
auto-polarity
!
hub ether 0 14
link-test
auto-polarity
!
interface Ethernet0
ip address 192.168.1.1 255.255.255.0
ipv6 address 3FFE:B00:FFFF:1::/64 eui-64
ipv6 enable
ipv6 rip thsis enable
!
interface Serial0
ip address 10.10.10.1 255.255.255.252
ipv6 address 3FFE:B00:FFFF:3::/64
ipv6 enable
ipv6 rip thsis enable
no fair-queue
!
interface Serial1
no ip address
shutdown
!
interface BRI0
no ip address
shutdown
!
router rip
version 2
network 10.0.0.0
```

```
network 192.168.1.0
!
ip http server
ip classless
!
ipv6 router rip thsis
!
line con 0
line aux 0
line vty 0 4
password cisco
login
!
end
```

ภาคผนวก ซ. ตัวอย่าง Configuration ของ Router HQ แบบ 6to4 Tunneling

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$69/l$R9bh8wN7.aTL391wLajjb1
!
no aaa new-model
ip subnet-zero
!
ipv6 unicast-routing
!
hub ether 0 1
link-test
auto-polarity
!
hub ether 0 2
link-test
auto-polarity
!
hub ether 0 3
link-test
auto-polarity
!
hub ether 0 4
link-test
```

```
auto-polarity
!
hub ether 0 5
link-test
auto-polarity
!
hub ether 0 6
link-test
auto-polarity
!
hub ether 0 7
link-test
auto-polarity
!
hub ether 0 8
link-test
auto-polarity
!
hub ether 0 9
link-test
auto-polarity
!
hub ether 0 10
link-test
auto-polarity
!
hub ether 0 11
link-test
auto-polarity
!
hub ether 0 12
link-test
auto-polarity
```

```
!
hub ether 0 13
link-test
auto-polarity
!
hub ether 0 14
link-test
auto-polarity
!
interface Tunnel1
no ip address
no ip redirects
ipv6 unnumbered Ethernet0
tunnel source Serial0
tunnel mode ipv6ip 6to4
!
interface Ethernet0
no ip address
ipv6 address 2002:C0A8:11::/64 eui-64
ipv6 enable
ipv6 nd prefix 2002:C0A8:11::/64 300 300
!
interface Serial0
ip address 192.168.1.1 255.255.255.0
clock rate 2000000
no fair-queue
!
interface Serial1
no ip address
shutdown
!
interface BRI0
no ip address
```

```
shutdown
!
ip http server
ip classless
!
ipv6 route 2002::/16 Tunnel1
!
line con 0
line aux 0
line vty 0 4
login
!
end
```

ภาคผนวก ณ. ผลงานวิจัยที่ได้รับการตีพิมพ์เผยแพร่

[1] สุริยา เจริญชุติถาวร, กอบชัย เดชหาญ "การวิเคราะห์โครงสร้างการเชื่อมต่อบน IPv6 ภายในองค์กรและการประยุกต์ใช้งาน" วิศวสารลาดกระบัง ปีที่ 22 ฉบับที่ 4 หน้า 13 - 18 ธันวาคม 2548

ISSN 0125-1724

วิศวสาร

ลาดกระบัง

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

LADKRABANG ENGINEERING JOURNAL

ปีที่ 22 ฉบับที่ 4 ธันวาคม 2548

1. Self-Organizing Map หลายลำดับชั้นสำหรับการตรวจจับการบุกรุก 1
สุรพล โรจนประดิษฐ เอื้อน ปิ่นเงิน

2. การจัดกลุ่มโหนดใน Self-Organizing Map โดยใช้เจเนติกอัลกอริทึม 7
กสานต์ ศรีกุลนาถ พรเทพ โรจนวสุ ไพฑูรย์ ศรีนิล เอื้อน ปิ่นเงิน

3. การวิเคราะห์โครงสร้างการเชื่อมต่อบน IPv6 ภายในองค์กรและการประยุกต์ใช้งาน 13
สุริยา เจริญชุติถาวร กอบชัย เดชหาญ

4. การออกแบบและสร้างหม้อแปลงไฟฟ้าแรงสูงความถี่สูงขนาด 20 kV 2 mA 19
กิตติพงษ์ ตันมิตร อำนาจ สุขศรี ชัยพร อัดโดดตร

5. การออกแบบและวิเคราะห์วงจรเรียงกระแสเอซี/ดีซี 6 พัลส์คอนเวอร์เตอร์ที่มีการปรับปรุงรูปคลื่นแรงดันเอาท์พุท และกระแสอินพุท 25
สกล กลิ่นหรั่น วิจิตร กิณเรศ

6. ผลกระทบของน้ำยาเคมี และน้ำ DI ที่มีต่อคุณสมบัติทางไฟฟ้าและแม่เหล็กของหัวอ่าน-เขียนข้อมูล 31
สมเกียรติ ปรารภ วิสุทธิ์ ฐิติรุ่งเรือง ลัดดาวัลย์ สุภาดี

7. การสังเคราะห์คาร์บอนนาโนทิวบ์ด้วยวิธี CVD แบบขดลวดความร้อนที่ความดัน 1 บรรยากาศ โดยใช้แอลกอฮอร์และไนโตรเจนเป็นก๊าซพาหะ 36
ณธวรรษ กสิกรรุ่งโรจน์ ปฏิคม ศรีชมพล สุธิชัย ชัยสิทธิศักดิ์

8. วงจรกำเนิดฟังก์ชันเอ็กซ์โพเนนเชียลทำงานในโหมดกระแสใช้แรงดันต่ำด้วยเทคโนโลยีซีมอส 42
มนตรี คำเงิน รัฐพล บุญมา กอบชัย เดชหาญ

9. วงจรบวกทางเวกเตอร์หลายหน้าที่ด้วยซีมอส 46
มนตรี คำเงิน คมกฤช โกมลเจิดศิริ กอบชัย เดชหาญ

10. ผลกระทบของเครือข่ายที่ใช้ชุดควบคุมหลักสั่งการชุดควบคุมย่อยเพียงชุดควบคุมเดียวของระบบแจ้งเหตุเพลิงไหม้ 52
วิจิตต์ แก้วไทรเทียม กอบชัย เดชหาญ

11. การวิเคราะห์สมรรถนะของระบบ DS-QPSK CDMA โดยใช้ช่องสัญญาณการจางแบบนาคากามิ 57
เกรียงวุฒิ จรภักดี กอบชัย เดชหาญ

การวิเคราะห์โครงสร้างการเชื่อมต่อบน IPv6 ภายในองค์กรและการประยุกต์ใช้งาน

Structural Connection Analysis on IPv6 in Organization and Its Applications

สุริยา เจริญชุติถาวร กอบชัย เดชหาญ

คณะวิศวกรรมศาสตร์และสำนักงานวิจัยการสื่อสารและเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

บทคัดย่อ

บทความนี้ได้เสนอหลักการทำงานร่วมกันระหว่างอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) กับอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) ภายในองค์กร โดยมีการวิเคราะห์ตรวจสอบลักษณะการทำงานของอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 และทดสอบประสิทธิภาพจากการทำงานจากการเชื่อมต่ออินเตอร์เน็ตโพรโตคอลทั้งสองรุ่น ซึ่งสามารถนำผลที่ได้จากการทดสอบไปวิเคราะห์โดยเปรียบเทียบได้จากความเร็วและเวลาเพื่อทำการสรุปผลว่าลักษณะการเชื่อมต่ออินเตอร์เน็ตโพรโตคอลแบบใดเหมาะสมกับองค์กรและให้ประสิทธิภาพดีที่สุด

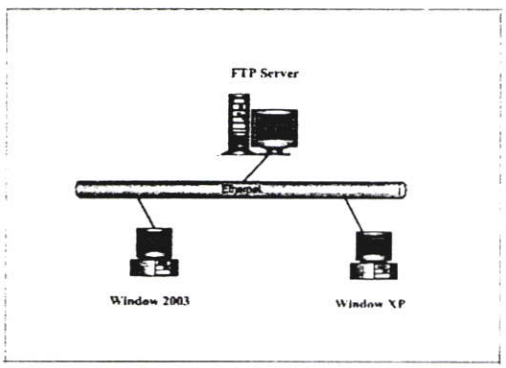
Abstract

This paper presents the use to Internet Protocol Version 6 (IPv6) to work with Internet Protocol Version 4 (IPv4) in any organization which analyzed the characteristic of IPv6 and testing performance from the connection between two Internet protocols. All results from testing are analyzed and concluded which type of connection between two protocols is the most suitable for organization with the best performance.

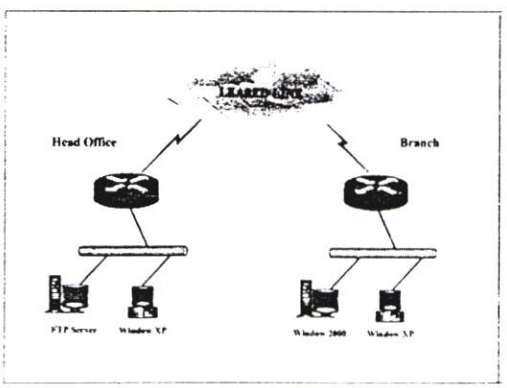
1. บทนำ

Internet และ Intranet ปัจจุบันมีการเติบโตและ การใช้งานอย่างแพร่หลายมากขึ้นดังนั้นความต้องการที่จะใช้ระบบเครือข่ายที่มีศักยภาพสูง จึงเพิ่มขึ้นด้วย การเชื่อมต่อเครือข่ายอินเตอร์เน็ตในปัจจุบันส่วนใหญ่อยู่บนพื้นฐานการทำงานของอินเตอร์เน็ตโพรโตคอลรุ่นที่4 ซึ่งทำให้การใช้งานจำนวนหมายเลข IP Address มีจำนวนมากขึ้นไม่เพียงพอต่อความต้องการ ในปัจจุบันโดยการติดต่อสื่อสารกันนั้น จะต้องมีจำนวนหมายเลข (IP Address) ให้กับคอมพิวเตอร์ทุกเครื่องโดยที่ไม่ซ้ำกัน เนื่องจากจำนวนหมายเลข (IP Address) อินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 นั้นมีจำนวนจำกัด และ ผลจากการใช้งานระบบอินเตอร์เน็ตซึ่งมี การใช้งานเพิ่มขึ้น ทำให้จำนวนหมายเลข (IP Address) กำลังจะหมดไปจึงได้มีการพัฒนาอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 เพื่อปรับปรุงโครงสร้างของอินเตอร์เน็ต ให้สามารถรองรับหมายเลข (IP Address) จำนวนมากได้ เพิ่มประสิทธิภาพและความปลอดภัยรองรับระบบการประยุกต์ใช้งาน (application) ใหม่ๆที่จะเกิด ขึ้นในอนาคต

ปัจจุบันการใช้งานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 นั้นในประเทศไทยยังมีใช้งานไม่แพร่หลายนักส่วนใหญ่การใช้งานจะอยู่ในกลุ่มผู้ให้บริการอินเตอร์เน็ต (Internet Service Provider) และ ในองค์กรบางองค์กร โดยในการจะใช้งานนั้น จะต้องทำการเตรียมความพร้อมให้กับอุปกรณ์ และลักษณะการเชื่อมต่อแบบต่างๆ โดยลักษณะการเชื่อมต่อนั้นมีอยู่ 3 ชนิดด้วยกันคือการใช้งานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 และอินเตอร์ เน็ตโพรโตคอลรุ่นที่ 4 ควบคู่กันหรือที่เรียกว่า Dual Stack การทะลุผ่านข้อมูล (Tunneling) และการแปลงข้อมูล (Translation) ซึ่งการเลือกใช้แต่ละเทคนิคต้องดูที่ความเหมาะสม และลักษณะการใช้งานของเครือข่ายที่มีอยู่



รูปที่ 1 ระบบเครือข่ายภายในองค์กรแบบ LAN



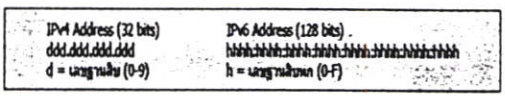
รูปที่ 2 ระบบเครือข่ายภายในองค์กรแบบ WAN

2. ทฤษฎีและหลักการ

ในหัวข้อนี้จะกล่าวถึงคุณสมบัติและการเปรียบเทียบของอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 กับอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 โดยมีหัวข้อต่างๆ ดังนี้

2.1 โครงสร้าง

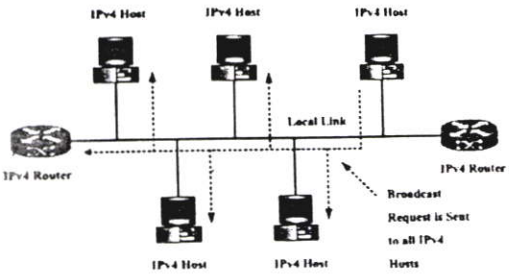
หลักการอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 มีจำนวน IP Address ที่เพิ่มขึ้นจากอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 ซึ่งมีขนาดเพียง 32 บิต ในขณะที่อินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 ซึ่งมีขนาดถึง 128 บิต



เฮดเดอร์ (Header) ของข้อมูลแบบอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 แพ็กเก็ตถูกออกแบบให้มีขนาดคงที่ 40 ไบต์ และ มีรูปแบบที่ง่ายที่สุดเท่าที่จะทำได้ โดยเฮดเดอร์ (Header) จะประกอบด้วยตำแหน่งต่างๆ ที่จำเป็นต้องใช้ในการประมวลผลแพ็กเก็ตของเราเตอร์ หรืออุปกรณ์เลือกเส้นทางทุกตัวเท่านั้น ส่วนตำแหน่งที่อาจจะถูกประมวลผลเฉพาะที่ต้นหรือปลายทาง หรือที่เราเตอร์บางตัว จะถูกยอกมาไว้ที่ส่วนขยายของเฮดเดอร์ (Extended Header)

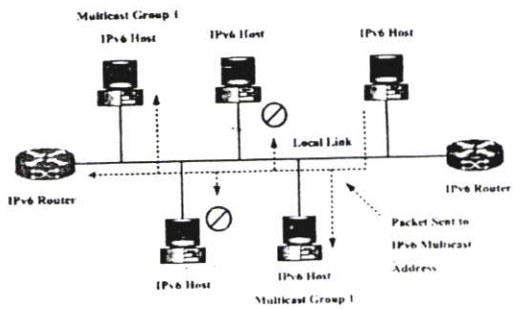
2.2 ลักษณะการทำงาน

ลักษณะการทำงานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 นั้นจะทำการส่ง ARP Request Broadcast ออกไปที่ Client ทุกๆ Client เพื่อสอบถามว่าใครรู้ IP Address นี้บ้าง โดยจะทำการส่งไปทั้งระบบเครือข่ายวงนั้นซึ่งจะทำให้เปลือง Bandwidth และ จะทำการเก็บ MAC Address สัมพันธ์กับ IP Address ไว้ในเครื่องนั้น ดังนั้นการทำงานของอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 จะใช้ ARP และการ Broadcast



รูปที่ 3 การทำงานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4

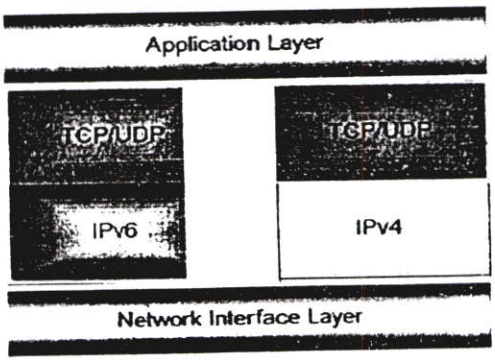
ลักษณะการทำงานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 นั้นไม่ได้ใช้ ARP และ Broadcast แต่ใช้ ICMPv6 (Internet Control Message Protocol Version 6) และ Multicast โดยจะทำการติดต่อสื่อสารระหว่าง Client ที่ต้องการติดต่อเท่านั้นซึ่งจะทำให้สามารถลด Bandwidth ได้



รูปที่ 4 การทำงานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6

2.3 ลักษณะการเชื่อม

ซึ่งลักษณะการเชื่อมต่อการใช้งานภายในองค์กรสามารถใช้งานได้หลายแบบ แต่ในบทความนี้กล่าวแบบ Dual Stack โดย Dual Stack คือการใช้งานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 และ อินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 ควบคู่กันไปภายในอุปกรณ์ตัวเดียวกัน สามารถใช้ได้ทั้ง Host และ Server และอุปกรณ์เครือข่าย ซึ่ง Dual Stack เป็นทางออกที่ง่ายที่สุดสำหรับเครือข่ายที่ต้องการเริ่มใช้งานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 และเหมาะกับการติดต่อระหว่าง 2 โหนด (Node) ที่ใช้อินเตอร์เน็ตโพรโตคอลเวอร์ชั่นเดียวกันแต่ต้องผ่านเครือข่ายกลางทางที่ใช้ IP อินเตอร์เน็ตโพรโตคอลคนละเวอร์ชั่น เช่น อินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 อินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 ผ่านเครือข่ายอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 หรือ อินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 อินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 ผ่านเครือข่ายอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 หรือ ในกรณีที่บางโหนดต้องการปรับเปลี่ยนไปใช้อินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 แต่ว่าเครือข่ายที่เชื่อมต่ออยู่ด้วยไม่สนับสนุนอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 โหนดดังกล่าวสามารถใช้ Dual Stack เพื่อรองรับอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 และ อินเตอร์เน็ตโพรโตคอลรุ่นที่ 6



รูปที่ 5 โครงสร้างของ Dual Stack

3. การทดลองและผลการทดลอง

การทดลองจะทำการดึงข้อมูลโดยตั้ง FTP Server และให้ Client ทำการดึงข้อมูล ซึ่งจะทำการทดสอบทั้งระบบ LAN ดังรูปที่ 1 และระบบ WAN ดังรูปที่ 2 โดยแต่ละระบบจะมีการทดสอบ 4 แบบ ดังนี้

1. FTP Server (IPv4 Pure)
2. FTP Server (IPv6 Pure)
3. FTP Server (IPv4 แบบ Dual Stack)
4. FTP Server (IPv6 แบบ Dual Stack)

โดยมีผลการทดลองดังต่อไปนี้

<u>ระบบ LAN</u>

จากการที่ทดสอบโดยทำการดึงข้อมูลทั้ง 4 แบบได้ข้อมูลดังต่อไปนี้

FTP IPv4 (Pure)		
Data (Mbyte)	Speed (Kbyte/Sec)	Time (Sec)
1	6834.98	0.16
5	6950.29	0.75
10	6698.02	1.4
50	6291.47	7.25
100	6663.87	15.97
500	6900.19	73
1000	6905.52	140

ตารางที่ 1 ข้อมูลทั้งหมดของ IPv4 (Pure)

FTP IPv6 (Pure)		
Data (Mbyte)	Speed (Kbyte/Sec)	Time (Sec)
1	5240.15	0.21
5	6053.61	0.86
10	6163.56	1.74
50	5544.34	9.36
100	5541.54	19.21
500	5405.13	95.1
1000	5408.25	205.44

ตารางที่ 2 ข้อมูลทั้งหมดของ IPv6 (Pure)

FTP IPv4 (Dual Stack)		
Data (Mbyte)	Speed (Kbyte/Sec)	Time (Sec)
1	6113.51	0.18
5	6940.29	0.75
10	6786.93	1.58
50	6579.3	7.898
100	6500.67	16.27
500	6713.84	76.56
1000	6716.1	167.67

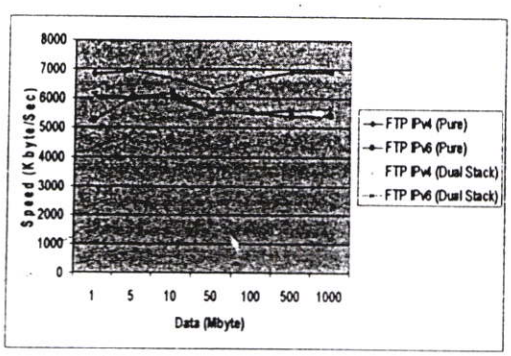
ตารางที่ 3 ข้อมูลทั้งหมดของ IPv4 (Dual Stack)

FTP IPv6 (Dual Stack)		
Data (Mbyte)	Speed (Kbyte/Sec)	Time (Sec)
1	6113.51	0.18
5	6053.61	0.86
10	5991.59	1.79
50	5533.12	9.38
100	5538.66	19.22
500	5582.71	92.07
1000	5669.42	198.63

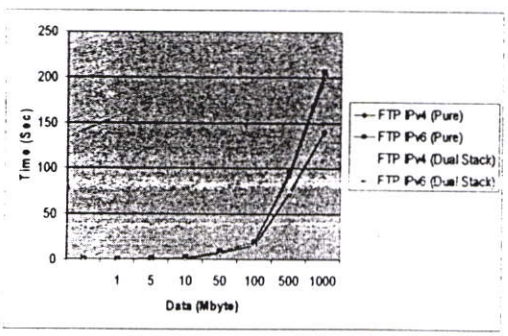
ตารางที่ 4 ข้อมูลทั้งหมดของ IPv6 (Dual Stack)

จากข้อมูลข้างต้น สามารถนำข้อมูลมาเปรียบเทียบเพื่อดูความเร็ว (Speed) หรือ เวลา (Time) ได้ลักษณะกราฟที่ได้

- เมื่อเทียบกับความเร็วและระยะเวลา



รูปที่ 6 ความเร็วที่ทำการดึงข้อมูล



รูปที่ 7 ระยะเวลาที่ทำการดึงข้อมูล

จากการทดสอบในระบบ LAN โดยนำข้อมูลที่ได้ทั้งทางความเร็วและระยะเวลา มาเปรียบเทียบจะเห็นว่าอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 ทั้งแบบ Pure และ Dual Stack นั้นจะใช้ความเร็วสูงและระยะเวลาในการดึงข้อมูลต่ำ

ระบบ WAN

จากการที่ทดสอบโดยทำการดึงข้อมูลทั้ง 4 แบบได้ข้อมูลดังต่อไปนี้

FTP IPv4 (Pure)		
Data (Mbyte)	Speed (Kbyte/Sec)	Time (Sec)
1	237	5.04
5	236.35	27.91
10	238.09	44.69
50	238.27	227.14
100	238.23	477.47
500	239.74	2144.06
1000	238.13	4892.35

ตารางที่ 5 ข้อมูลทั้งหมดของ IPv4 (Pure)

FTP IPv6 (Pure)		
Data (Mbyte)	Speed (Kbyte/Sec)	Time (Sec)
1	228.39	5.23
5	233.25	28.28
10	232.98	45.67
50	232.61	232.66
100	232.5	489.24
500	233.87	2197.86
1000	232.39	5013.12

ตารางที่ 6 ข้อมูลทั้งหมดของ IPv6 (Pure)

FTP IPv4 (Dual Stack)		
Data (Mbyte)	Speed (Kbyte/Sec)	Time (Sec)
1	237.52	5.03
5	238.07	27.71
10	238.09	44.7
50	237.82	227.57
100	238.19	477.55
500	236.9	2169
1000	238.13	4892.35

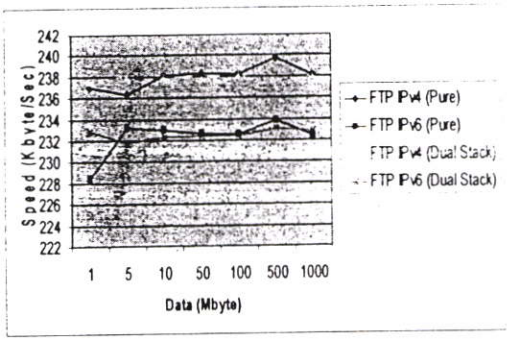
ตารางที่ 7 ข้อมูลทั้งหมดของ IPv4 (Dual Stack)

FTP IPv6 (Dual Stack)		
Data (Mbyte)	Speed (Kbyte/Sec)	Time (Sec)
1	232.84	5.13
5	231.78	28.46
10	232.31	45.81
50	233.41	242.24
100	232.47	489.31
500	233.04	2205.64
1000	232.84	5024.95

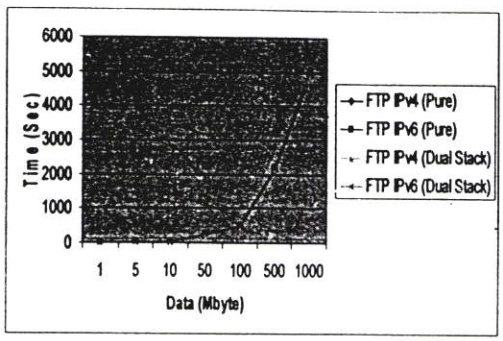
ตารางที่ 8 ข้อมูลทั้งหมดของ IPv6 (Dual Stack)

จากข้อมูลข้างต้น สามารถนำข้อมูลมาเปรียบเทียบเพื่อดูความเร็ว (Speed) หรือ เวลา (Time) ได้โดยลักษณะกราฟที่ได้เป็นดังนี้

- เมื่อเทียบกับความเร็วและระยะเวลา



รูปที่ 8 ความเร็วที่ทำการดึงข้อมูล



รูปที่ 9 ระยะเวลาที่ทำการดึงข้อมูล

จากการทดสอบในระบบ WAN โดยนำข้อมูลที่ได้ทั้งทางความเร็วและระยะเวลามาเปรียบเทียบ จะพบว่าทั้งอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 และอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 นั้น จะใช้ความเร็วและระยะเวลาในการดึงข้อมูลใกล้เคียงกัน เพราะถูกกำหนดความเร็วทางด้าน WAN

4. บทสรุป

จากการทดสอบข้างต้นจะพบว่าการใช้งานอินเตอร์เน็ตโพรโตคอลรุ่นที่ 6 เมื่อเทียบกับอินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 จะพบว่าการใช้งานของระบบมีประสิทธิภาพต่ำลง อาจจะขึ้นอยู่กับขนาดของ Header โดยโพรโตคอลรุ่นที่ 6 มีขนาด 40 Byte แต่อินเตอร์เน็ตโพรโตคอลรุ่นที่ 4 มีขนาด 20 Byte ซึ่งในอนาคตอาจจะมีการพัฒนาทางด้านฮาร์แวร์และทางด้านซอฟท์แวร์มากขึ้น

5. เอกสารอ้างอิง

[1] D. Régis, Cisco Self-Study : Implementing Cisco IPv6 Networks (IPv6). Indianapolis : Cisco Press. 2003.

[2] Y.M. Yussoff, M. Samad, Implementation of Native IPv6 test-bed for network link quality and performance analysis. IEEE Internet Computing, pp. 453-455, July 2002.

[3] G.H. Yong, K.S. Myung, J.K. Hyoung, Application translation for IPv6 at NAT-PT. Proc. 9th Asia-Pacific Conference, pp.203-207, Sept., 2003.

[4] T. Yazaki, T. Kanetake, S. Akahane, Y. Sakata, K. Sugai, H. Yano, High-speed IPv6 router/switch architecture. IEEE Internet Computing, pp. 153-158, Jan., 2004.

[5] ภาสกร ประถมบุตร พนิตา พงษ์ไพบูลย์ ธีรีสา มัทวพันธุ์ ฉัตรชัย จันทร์อินทร์ ปวีณา ทองแม้น ความรู้เบื้องต้นเกี่ยวกับ IPv6 สำหรับผู้ใช้งานทั่วไป ศูนย์เทคโนโลยีอิเล็กทรอนิกส์ และ คอมพิวเตอร์แห่งชาติ มีนาคม 2548.

[6] พนิตา พงษ์ไพบูลย์ เฉลิมพล ชาญศรีภิญโญ ฉัตรชัย จันทร์อินทร์ อดิศักดิ์ บุศรานันท์ การเตรียมความพร้อมในการเชื่อมต่อเข้าสู่อินเทอร์เน็ตยุคหน้า 2005 NSTDA Annual Conference มีนาคม 2548.

ประวัติผู้เขียน

นายสุริยา เจริญติถาวร เกิดเมื่อวันที่ 12 ตุลาคม พ.ศ.2518 ที่จังหวัดกรุงเทพมหานคร สำเร็จการศึกษาปริญญาตรีวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมอิเล็กทรอนิกส์ จากคณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษมบัณฑิต ในปีการศึกษา 2544 และเข้าศึกษาต่อในระดับปริญญาโท หลักสูตรวิศวกรรมศาสตรมหาบัณฑิต สาขาวิศวกรรมโทรคมนาคม ภาควิชาวิศวกรรมโทรคมนาคม คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ในปีการศึกษา 2547 ได้เข้าทำงานในตำแหน่งวิศวกร บริษัท จีเนียสคอมมูนิเคชั่นซิสเต็ม จำกัด ปี 2544–2545 ปัจจุบันเข้าทำงานในตำแหน่ง Network Specialist บริษัท จักรวาลคอมมูนิเคชั่นซิสเต็ม จำกัด