การศึกษาการเชื่อมต่ออินเทอร์เน็ตโพรโทคอลรุ่นที่ 4 และรุ่นที่ 6

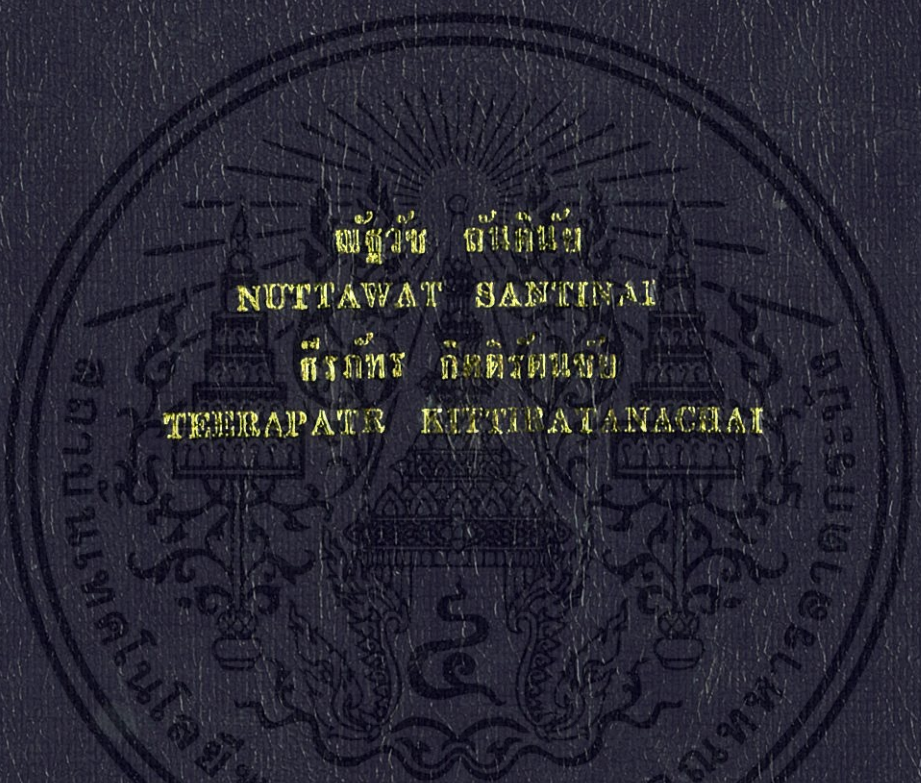
STUDY ON INTERNET PROTOCOL VERSION 4 AND 6 CONNECTIVITY

ณัฐวัช สันตินัย

NUTTAWAT SANTINAI

ธีรเดช กิตติรัตนชัย

TEERAPATR KITTIRATANACHAI



วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรดุษฎีบัณฑิต

สาขาวิชาวิศวกรรมสารสนเทศ

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2556

การศึกษาการเชื่อมต่ออินเทอร์เน็ตโพรโทคอลรุ่นที่ 4 และ รุ่นที่ 6
STUDY ON INTERNET PROTOCOL VERSION 4 AND 6 CONNECTIVITY

ณัฐวัช สันตินัย
NUTTAWAT SANTINAI

ธีรภัทร กิตติรัตนชัย
TEERAPATR KITTIRATANACHAI

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต
สาขาวิชาวิศวกรรมสารสนเทศ
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ปีการศึกษา 2556

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

STUDY ON INTERNET PROTOCOL VERSION 4 AND 6 CONNECTIVITY

NUTTAWAT SANTINAI

TEERAPATR KITTIRATANACHAI

THIS THESIS IS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENT FOR THE DEGREE OF
BACHELOR OF ENGINEERING IN INFORMATION ENGINEERING
FACULTY OF ENGINEERING
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG
ACADEMIC YEAR 2013

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หัวข้อปริญญานิพนธ์	การศึกษาการเชื่อมต่ออินเทอร์เน็ตโพรโทคอลรุ่นที่ 4 และ รุ่นที่ 6	
รายชื่อนักศึกษา	นายณัฐวัช สันตินัย	รหัสนักศึกษา 53010506
	นายธีรภัทร กิตติรัตนชัย	รหัสนักศึกษา 53010755
ปริญญา	วิศวกรรมศาสตรบัณฑิต	
สาขาวิชา	วิศวกรรมสารสนเทศ	
พ.ศ.	2556	
อาจารย์ที่ปรึกษาปริญญานิพนธ์	ผศ. มยุรี เลิศเวชกุล	

ปริญญานิพนธ์ฉบับนี้ ได้รับการอนุมัติให้เป็นส่วนหนึ่งของการศึกษา ตามหลักสูตรวิศวกรรมศาสตรบัณฑิต คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

.....

(ผศ. มยุรี เลิศเวชกุล)

อาจารย์ผู้ควบคุมปริญญานิพนธ์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หัวข้อปริญญานิพนธ์	การศึกษาการเชื่อมต่ออินเทอร์เน็ตโพรโทคอลรุ่นที่ 4 และ รุ่นที่ 6	
รายชื่อนักศึกษา	นายณัฐวัช สันตินัย	รหัสนักศึกษา 53010506
	นายธีรภัทร กิตติรัตนชัย	รหัสนักศึกษา 53010755
ปริญญา	วิศวกรรมศาสตรบัณฑิต	
สาขาวิชา	วิศวกรรมสารสนเทศ	
พ.ศ.	2556	
อาจารย์ที่ปรึกษาปริญญานิพนธ์	ผศ. มยุรี เลิศเวชกุล	

บทคัดย่อ

ปริญญานิพนธ์ฉบับนี้ นำเสนอการเชื่อมต่อระบบเครือข่ายที่มีการทำงานร่วมกันระหว่างมาตรฐานอินเทอร์เน็ตโพรโทคอลรุ่นที่ 4 (IPv4) และ รุ่นที่ 6 (IPv6) การนำ IPv6 มาใช้งานจริงบนระบบอินเทอร์เน็ตทั้งหมดต้องใช้เวลานาน เนื่องจากปัญหาในด้านต่างๆ เราจึงทดสอบอุโมงค์สื่อสาร (Tunneling) แบบต่างๆ ในระบบเครือข่ายแบบปิด ได้แก่ Manual Tunnel, GRE Tunnel, Automatic 6to4 Tunnel, IPv4-Compatible IPv6 Tunnel, 6RD Tunnel และ ISATAP Tunnel จากการทดสอบแบบจำลองระบบเครือข่ายทั้งหมดสามารถติดต่อสื่อสารกันได้ และได้มีการทดสอบการเชื่อมต่อไปยังเครือข่ายอินเทอร์เน็ตซึ่งทำงานบน IPv6 อีกด้วย สามารถแบ่งได้ 2 รูปแบบคือ เครื่องคอมพิวเตอร์เชื่อมต่อระบบเครือข่ายแบบ Dual Stack และเชื่อมต่อระบบเครือข่ายภายในไปยังระบบเครือข่าย IPv6 โดยทั้ง 2 รูปแบบเชื่อมต่อไปยังเครื่องแม่ข่ายที่ทำงานบน IPv6 ภายนอกผ่าน Tunnel Broker ที่ NECTEC ซึ่งจากการทดลองพบว่าสามารถทำงานได้ดี อีกทั้งได้จัดทำเว็บไซต์คู่มือแนะนำการตั้งค่าอุปกรณ์เครือข่ายเบื้องต้น เพื่อให้สามารถใช้บริการเครือข่าย IPv6 ได้ ซึ่งภายในคู่มือมีการให้ความรู้เกี่ยวกับการทำงานร่วมกันของทั้ง 2 โพรโทคอลรวมอยู่ด้วย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Thesis Title	Study on Internet Protocol version 4 and 6 Connectivity	
Student	Mr. Nuttawat Santinai	Student ID. 53010506
	Mr. Teerapatr Kittiratanachai	Student ID. 53010755
Degree Program	Bachelor of Engineering	
	Information Engineering	
Year	2014	
Thesis Advisor	Asst.Prof. Mayuree Lertwatechakul	

ABSTRACT

This thesis presents network connectivity which provides Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) Interoperation. Implementing IPv6 to all over the internet could take a long time caused by many problems. We made experiments of applying tunneling techniques; the experiments included Manual Tunnel, GRE Tunnel, Automatic 6to4 Tunnel, IPv4-Compatible IPv6 Tunnel, 6RD Tunnel, and ISATAP Tunnel. All of the experiments are successful establish the connections. As to try the experiments on the existing IPv6 public internet, we made up two scenarios, one is a local dual stack PC and another is a local IPv6 network. Both of them using the Global Unicast IPv6 address and connected the network to IPv6 server through IPv6 tunnel broker at NECTEC. These experiments also are successfully. We also develop the manual in web interface which suggest the basic configurations for network devices to provide IPv6 network and give you some information about interoperation of both protocols.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้ ได้รับคำแนะนำและคำปรึกษาเกี่ยวกับการค้นคว้าและวิเคราะห์เนื้อหาการวิจัยจากผู้ช่วยศาสตราจารย์มยุรี เลิศเวชกุล อาจารย์ที่ปรึกษาในการทำปริญญานิพนธ์ ซึ่งกลุ่มผู้วิจัยจะไม่สามารถทำวิจัยมาถึงจุดนี้ได้หากปราศจากคำแนะนำจากอาจารย์ กลุ่มผู้วิจัยจึงขอกราบขอบพระคุณอาจารย์เป็นอย่างสูง รวมถึงห้องทดลอง NGN สาขาวิศวกรรมสารสนเทศ ที่ได้สนับสนุนในส่วนของอุปกรณ์ประกอบการวิจัย และสนับสนุนสถานที่ในการทำวิจัยให้สำเร็จอย่างราบรื่นอีกด้วย

ขอกราบขอบพระคุณอาจารย์อัครเดช วัชระภูพงษ์ ที่คอยตอบข้อสงสัย และช่วยแก้ปัญหาในระหว่างการทำปริญญานิพนธ์ฉบับนี้จนสำเร็จได้ด้วยดี

ขอกราบขอบพระคุณคณาจารย์ท่านต่างๆ ทั้งในและนอกสาขาวิชาวิศวกรรมสารสนเทศ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ที่ได้ประสิทธิ์ประสาทวิชาความรู้ต่างๆ มากมายตลอดระยะเวลาทั้ง 4 ปี ในการศึกษามาประกอบรวมกันจนช่วยให้กลุ่มผู้วิจัยจัดทำปริญญานิพนธ์ฉบับนี้สำเร็จลงได้

ขอขอบคุณ Mr. Ross Chandler, Mr. Cameron Byrne, Mr. Lee Howard และสมาชิกทุกคนในกลุ่ม IPv6 (https://www.facebook.com/groups/2234775539) ที่ช่วยตอบข้อสงสัยในขณะทำวิจัย

ขอขอบพระคุณบิดา มารดา ครอบครัว ของกลุ่มผู้วิจัยที่คอยเป็นกำลังใจให้กับกลุ่มผู้วิจัย ในยามที่เผชิญกับปัญหาต่างๆ ในระหว่างการทำปริญญานิพนธ์ฉบับนี้

ขอขอบใจเพื่อนๆ ภาควิชาวิศวกรรมสารสนเทศ ที่อยู่เป็นกำลังใจให้กันและกันในยามดึกจนถึงเช้าของอีกวัน ขอบใจเพื่อนๆ ที่คอยช่วยเหลือกันในเรื่องต่างๆ มากมาย ร่วมกันฝ่าฟันอุปสรรคมาจนถึงจุดนี้ได้

และสุดท้ายนี้ กลุ่มผู้วิจัยหวังว่าปริญญานิพนธ์ฉบับนี้จะเป็นประโยชน์ต่อทุกท่าน และสามารถนำข้อมูลในปริญญานิพนธ์ฉบับนี้ไปประยุกต์ใช้ได้ในอนาคต

ณัฐวัช สันตินัย
ธีรภัทร กิตติรัตนชัย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ

หน้า

บทคัดย่อภาษาไทย I
บทคัดย่อภาษาอังกฤษ II
กิตติกรรมประกาศ III
สารบัญ IV
สารบัญตาราง VII
สารบัญรูป VIII
บทที่ 1 บทนำ 1
1.1 แนวคิดและที่มาของปัญหา 1
1.2 จุดประสงค์ 1
1.3 ขอบเขตของโครงงาน 2
1.4 ประโยชน์ที่คาดว่าจะได้รับ 2
บทที่ 2 ทฤษฎีพื้นฐาน 3
2.1 อินเทอร์เน็ตโพรโทคอลรุ่นที่ 6 3
2.1.1 คุณสมบัติของอินเทอร์เน็ตโพรโทคอลรุ่นที่ 6 3
2.1.2 หมายเลขอินเทอร์เน็ตโพรโทคอลรุ่นที่ 6 5
2.1.3 หมายเลขที่อยู่ Unicast 6
2.1.4 หมายเลขที่อยู่ Anycast 8
2.1.5 หมายเลขที่อยู่ Multicast 8
2.1.6 การสร้างหมายเลขอินเตอร์เฟสในรูปแบบ EUI-64 9
2.1.7 การตั้งค่าหมายเลขที่อยู่ IPv6 แบบอัตโนมัติ 10
2.1.8 การตั้งค่าหมายเลขที่อยู่ IPv6 11
2.2 การใช้งานร่วมกันระหว่าง IPv6 และ IPv4 11
2.2.1 ภาพรวมของเทคนิคการเปลี่ยนจาก IPv4 ไปยัง IPv6 (Transition Technology) 11
2.2.2 การทำอุโมงค์สื่อสาร (Tunneling) 13
2.2.3 ไอซาแทป 14
2.2.4 6to4 15
2.3 คำสั่งและการกำหนดค่า IPv6 บน IOS 15
2.3.1 User EXEC Mode 15
2.3.2 Privileged EXEC Mode 16
2.3.3 Global Configuration Mode 17

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ (ต่อ)

หน้า

2.3.4 การกำหนดค่าหมายเลขที่อยู่ IPv6 และทำ IPv6 Routing....18
2.4 ทฤษฎีพื้นฐานของภาษาที่ใช้ในการสร้างเว็บไซต์....28
2.4.1 HTML (Hypertext Markup Language)....28
2.4.2 PHP (Hypertext Preprocessor)....30
2.4.3 CSS (Cascading Style Sheets)....31
2.4.4 JavaScript....32
บทที่ 3 การออกแบบระบบ....33
3.1 กรณีที่เป็นไปได้ของ End-point....33
3.1.1 อุปกรณ์ที่ใช้ในการทดลอง....33
3.1.2 ขั้นตอนการทดลอง....33
3.1.3 ออกแบบการเชื่อมต่อ....33
3.2 ขั้นตอนการออกแบบคู่มือการตั้งค่า IPv6....43
3.2.1 ออกแบบรูปแบบเว็บเพจ....43
3.2.2 แผนภาพการทำงานของเว็บไซต์ (Sequence Diagram)....44
บทที่ 4 ผลการดำเนินงาน....46
4.1 ผลการจำลองการเชื่อมต่อเครือข่าย....46
4.1.1 การเชื่อมต่อแบบ Native IPv4....46
4.1.2 การเชื่อมต่อแบบ Native IPv6....47
4.1.3 การเชื่อมต่อแบบ Dual Stack....48
4.1.4 การเชื่อมต่อแบบ Manual Tunnel....49
4.1.5 การเชื่อมต่อแบบ GRE Tunnel (4over6)....49
4.1.6 การเชื่อมต่อแบบ GRE Tunnel (6over4)....50
4.1.7 การเชื่อมต่อแบบ Automatic 6to4 Tunnel....50
4.1.8 การเชื่อมต่อแบบ IPv4-Compatible IPv6 Tunnel (2 Routers)....51
4.1.9 การเชื่อมต่อแบบ IPv4-Compatible IPv6 Tunnel (3 Routers)....51
4.1.10 การเชื่อมต่อแบบ 6RD Tunnel....52
4.1.11 การเชื่อมต่อแบบ ISATAP Tunnel....52
4.2 การทดสอบการเชื่อมต่อไปยังเครือข่าย IPv6 ที่มีการใช้งานจริง....53
4.2.1 การเชื่อมต่อโดยสร้างอินเตอร์เฟสจำลองในเครื่องคอมพิวเตอร์....53

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ (ต่อ)

หน้า

4.2.2 การเชื่อมต่อผ่านอุโมงค์สื่อสารแบบ Manual Tunnel ที่เราท์เตอร์ 54
4.3 เว็บไซต์คู่มือการตั้งค่าอุปกรณ์สื่อสารที่ทำงานบน IPv6 56
4.3.1 หน้าหลักของเว็บไซต์ 56
4.3.2 หัวข้อต่างๆ ในแต่ละเมนู 56
4.3.3 โปรแกรมช่วยตั้งค่า 59
4.3.4 ผลการใช้งานโปรแกรมช่วยตั้งค่า 59
บทที่ 5 สรุปและวิจารณ์ผล 64
5.1 ผลการศึกษาโครงงาน 64
5.2 สรุปผลโครงงาน 65
5.3 ปัญหาที่เกิดระหว่างการทำโครงงาน 65
5.4 แนวทางในการพัฒนาโครงงานต่อ 66
บรรณานุกรม 67

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญตาราง

ตารางที่ หน้า
2.1 ตารางระบุ Header ของ IPv6 และรหัสประจำ Header....4
2.2 ตารางระบุค่าของ scope ในหมายเลขที่อยู่ Multicast....8
2.3 ตารางระบุคำสั่งที่ใช้งานบ่อยใน User EXEC Mode....15
2.4 ตารางระบุคำสั่งที่ใช้งานบ่อยใน Privileged EXEC Mode....16
2.5 ตารางระบุคำสั่งที่ใช้งานบ่อยใน Global Configuration Mode....17
2.6 ตารางระบุขั้นตอนการกำหนดค่า Native IPv6 Address....18
2.7 ตารางระบุขั้นตอนการกำหนดค่า IPv6 Dual IP Stack....20
2.8 ตารางระบุขั้นตอนการกำหนดค่า Manual IPv6 Tunnel....21
2.9 ตารางระบุขั้นตอนการกำหนดค่า GRE IPv6 Tunnel....22
2.10 ตารางระบุขั้นตอนการกำหนดค่า Automatic 6to4 Tunnel....23
2.11 ตารางระบุขั้นตอนการกำหนดค่า IPv4-Compatible IPv6 Tunnel....25
2.12 ตารางระบุขั้นตอนการกำหนดค่า 6RD Tunnel....26
2.13 ตารางระบุขั้นตอนการกำหนดค่า ISTAP Tunnel....27
3.1 ตารางแสดงการตั้งค่าให้กับเราท์เตอร์เพื่อสร้างการเชื่อมต่อแบบ Native IPv4....34
3.2 ตารางแสดงการตั้งค่าให้กับเราท์เตอร์เพื่อสร้างการเชื่อมต่อแบบ Native IPv6....34
3.3 ตารางแสดงการตั้งค่าให้กับเราท์เตอร์เพื่อสร้างการเชื่อมต่อแบบ Dual Stack....35
3.4 ตารางแสดงการตั้งค่าให้กับเราท์เตอร์เพื่อสร้างการเชื่อมต่อแบบ Manual Tunnel....36
3.5 ตารางแสดงการตั้งค่าให้กับเราท์เตอร์เพื่อสร้างการเชื่อมต่อแบบ GRE Tunnel (4over6)....37
3.6 ตารางแสดงการตั้งค่าให้กับเราท์เตอร์เพื่อสร้างการเชื่อมต่อแบบ GRE Tunnel (6over4)....37
3.7 ตารางแสดงการตั้งค่าให้กับเราท์เตอร์เพื่อสร้างการเชื่อมต่อแบบ Automatic 6to4 Tunnel....38
3.8 ตารางแสดงการตั้งค่าให้กับเราท์เตอร์เพื่อสร้างการเชื่อมต่อแบบ IPv4-Compatible IPv6 Tunnel (2 Routers)....39
3.9 ตารางแสดงการตั้งค่าให้กับเราท์เตอร์เพื่อสร้างการเชื่อมต่อแบบ IPv4-Compatible IPv6 Tunnel (3 Routers)....40
3.10 ตารางแสดงการตั้งค่าให้กับเราท์เตอร์เพื่อสร้างการเชื่อมต่อแบบ 6RD Tunnel....41
3.11 ตารางแสดงการตั้งค่าให้กับเราท์เตอร์เพื่อสร้างการเชื่อมต่อแบบ ISATAP Tunnel....42
5.1 ตารางแสดงการเปรียบเทียบคุณสมบัติของอุโมงค์สื่อสารแต่ละประเภท....65

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูป

รูปที่ หน้า

2.1 ข้อมูลส่วนหัวของอินเทอร์เน็ตโพรโทคอลรุ่นที่ 6 3
2.2 รูปแบบทั่วไปของหมายเลขที่อยู่ Global Unicast 7
2.3 รูปแบบทั่วไปของหมายเลขที่อยู่ Link-Local Unicast 7
2.4 รูปแบบทั่วไปของหมายเลขที่อยู่ Anycast 8
2.5 รูปแบบทั่วไปของหมายเลขที่อยู่ Multicast 8
2.6 การเปลี่ยนหมายเลข MAC-address ให้มีโครงสร้างแบบ EUI-64 10
2.7 การเชื่อมต่อแบบ Dual Stack 11
2.8 Dual IP Layer Architecture 12
2.9 Dual Stack Architecture 12
2.10 ภาพรวมของการทำงานแบบ NAT-PT 13
2.11 การห่อหุ้มแพ็กเก็ต IPv6 ด้วยแพ็กเก็ต IPv4 13
2.12 ภาพรวมของการทำงานแบบ Tunneling 14
2.13 ตัวอย่างหมายเลข ISATAP 14
2.14 โครงสร้างหมายเลข IPv6 ของ 6to4 15
2.15 ตัวอย่างการเชื่อมต่อ Native IPv6 19
2.16 ตัวอย่างการเชื่อมต่อแบบ Dual Stack 20
2.17 ตัวอย่างการเชื่อมต่อแบบ Manual IPv6 Tunnel 21
2.18 ตัวอย่างการเชื่อมต่อแบบ GRE IPv6 Tunnel 23
2.19 ตัวอย่างการเชื่อมต่อแบบ Automatic 6to4 Tunnel 24
2.20 ตัวอย่างการเชื่อมต่อแบบ IPv4-Compatible IPv6 Tunnel 25
2.21 ตัวอย่างการเชื่อมต่อแบบ 6RD Tunnel 26
2.22 ตัวอย่างการเชื่อมต่อแบบ ISATAP Tunnel 27
2.23 รูปแบบการเขียนคำสั่งภาษา HTML 29
2.24 โครงสร้างตารางในภาษา HTML 30
2.25 โครงสร้างภาษา CSS 31
3.1 การเชื่อมต่อแบบ Native IPv4 34
3.2 การเชื่อมต่อแบบ Native IPv6 34
3.3 การเชื่อมต่อแบบ Dual Stack 35
3.4 การเชื่อมต่อแบบ Manual Tunnel 36
3.5 การเชื่อมต่อแบบ GRE Tunnel (4over6) 36

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูป (ต่อ)

รูปที่ หน้า

3.6 การเชื่อมต่อแบบ GRE Tunnel (6over4) 37
3.7 การเชื่อมต่อแบบ Automatic 6to4 Tunnel 38
3.8 การเชื่อมต่อแบบ IPv4-Compatible IPv6 Tunnel (2 Routers) 39
3.9 การเชื่อมต่อแบบ IPv4-Compatible IPv6 Tunnel (3 Routers) 39
3.10 โครงสร้างหมายเลข IPv6 แบบ 6RD 40
3.11 การเชื่อมต่อแบบ 6RD Tunnel 41
3.12 โครงสร้างหมายเลข IPv6 แบบ ISATAP 42
3.13 การเชื่อมต่อแบบ ISATAP 42
3.14 ส่วนหัวของเว็บเพจ 43
3.15 ส่วนซ้ายของเว็บเพจ 43
3.16 ส่วนขวาของเว็บเพจ 43
3.17 ส่วนกลางของเว็บเพจ 44
3.18 แผนภาพแสดงการทำงานของเว็บไซต์ 44
3.19 แผนภาพแสดงการใช้งานตัวช่วยตั้งค่า IPv6 Tunnel 45
4.1 ผลการทดสอบการ Ping และแสดงเส้นทางการสื่อสารบนโทโพโลยีแบบ Native IPv4 47
4.2 ผลการทดสอบการ Ping และแสดงเส้นทางการสื่อสารบนโทโพโลยีแบบ Native IPv6 47
4.3 ผลการทดสอบการ Ping และแสดงเส้นทางการสื่อสารบนโทโพโลยีแบบ Dual Stack 48
4.4 ผลการทดสอบการ Ping และแสดงเส้นทางการสื่อสารบนโทโพโลยีแบบ Manual Tunnel 49
4.5 ผลการทดสอบการ Ping และแสดงเส้นทางการสื่อสารบนโทโพโลยีแบบ GRE Tunnel (4over6) 49
4.6 ผลการทดสอบการ Ping และแสดงเส้นทางการสื่อสารบนโทโพโลยีแบบ GRE Tunnel (6over4) 50
4.7 ผลการทดสอบการ Ping และแสดงเส้นทางการสื่อสารบนโทโพโลยีแบบ Automatic 6to4 Tunnel 50
4.8 ผลการทดสอบการ Ping และแสดงเส้นทางการสื่อสารบนโทโพโลยีแบบ IPv4-Compatible IPv6 Tunnel (2 Routers) 51
4.9 ผลการทดสอบการ Ping และแสดงเส้นทางการสื่อสารบนโทโพโลยีแบบ IPv4-Compatible IPv6 Tunnel (3 Routers) 51
4.10 ผลการทดสอบการ Ping และแสดงเส้นทางการสื่อสารบนโทโพโลยีแบบ 6RD Tunnel 52
4.11 ผลการทดสอบการ Ping และแสดงเส้นทางการสื่อสารบนโทโพโลยีแบบ ISATAP 52
4.12 การตั้งค่าการเชื่อมต่อโดยสร้างอินเตอร์เฟสจำลองในเครื่องคอมพิวเตอร์สำหรับระบบปฏิบัติการตระกูลวินโดวส์ 53

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูป (ต่อ)

รูปที่ หน้า

4.13 การตั้งค่าการเชื่อมต่อโดยสร้างอินเตอร์เฟสจำลองในเครื่องคอมพิวเตอร์สำหรับระบบปฏิบัติการตระกูลลินุกซ์ 53
4.14 การเชื่อมต่อไปยัง NECTEC โดยสร้างอินเตอร์เฟสจำลองในเครื่องคอมพิวเตอร์ 54
4.15 ผลการทดสอบการ Ping และแสดงเส้นทางการสื่อสารไปยังชื่อโดเมน google.com ผ่านทาง NECTEC โดยสร้างอินเตอร์เฟสจำลองในเครื่องคอมพิวเตอร์ 54
4.16 การเชื่อมต่อไปยัง NECTEC ผ่านอุโมงค์สื่อสารแบบ Manual Tunnel ที่เราท์เตอร์ 54
4.17 การตั้งค่าให้กับเราท์เตอร์เพื่อสร้างการเชื่อมต่อไปยัง NECTEC ผ่านอุโมงค์สื่อสารแบบ Manual Tunnel ที่เราท์เตอร์ 55
4.18 ผลการทดสอบการ Ping และแสดงเส้นทางการสื่อสารไปยังชื่อโดเมน google.com ผ่านทาง NECTEC ด้วยอุโมงค์สื่อสารแบบ Manual Tunnel ที่เราท์เตอร์ 55
4.19 หน้าแรกของเว็บไซต์คู่มือการตั้งค่าอุปกรณ์สื่อสารที่ทำงานบน IPv6 56
4.20 หัวข้อ IPv6 และหัวข้อย่อย 57
4.21 หัวข้อ IPv4 & IPv6 Technical และหัวข้อย่อย 57
4.22 หัวข้อ Cisco IOS และหัวข้อย่อย 58
4.23 หัวข้อ Connection & Configuration และหัวข้อย่อย 58
4.24 เมนูของโปรแกรมตัวช่วยตั้งค่า 59
4.25 ผลการใช้งานโปรแกรมตัวช่วยตั้งค่าแบบ Manual Tunnel 59
4.26 ผลการใช้งานโปรแกรมตัวช่วยตั้งค่าแบบ GRE IPv6 Tunnel 60
4.27 ผลการใช้งานโปรแกรมตัวช่วยตั้งค่าแบบ Automatic 6to4 Tunnel 60
4.28 ผลการใช้งานโปรแกรมตัวช่วยตั้งค่าแบบ IPv4–Compatible IPv6 Tunnel 61
4.29 ผลการใช้งานโปรแกรมตัวช่วยตั้งค่าแบบ 6RD Tunnel (ISP Border Router) 61
4.30 ผลการใช้งานโปรแกรมตัวช่วยตั้งค่าแบบ 6RD Tunnel (Client Edge) 62
4.31 ผลการใช้งานโปรแกรมตัวช่วยตั้งค่าแบบ ISATAP Tunnel (Router) 62
4.32 ผลการใช้งานโปรแกรมตัวช่วยตั้งค่าแบบ ISATAP Tunnel (Client) 63

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 1
บทนำ

1.1 แนวคิดและที่มาของปัญหา

ในปัจจุบันความต้องการในการใช้งานอินเทอร์เน็ตมีสูงมากขึ้น จึงทำให้หมายเลขที่อยู่ไอพี (IP Address) จากอินเทอร์เน็ตโพรโทคอลรุ่นที่ 4 (Internet Protocol Version 4; IPv4) ที่ใช้อยู่ไม่เพียงพอในการให้บริการ แม้จะมีการใช้วิธีการต่างๆ เพื่อขยายปริมาณการให้บริการแล้วก็ตาม ดังนั้นการย้ายไปใช้หมายเลขที่อยู่ไอพีภายใต้มาตรฐานใหม่คือ อินเทอร์เน็ตโพรโทคอลรุ่นที่ 6 (Internet Protocol Version 6; IPv6) เป็นทางเลือกที่ดีที่สุดในการแก้ไขปัญหาที่เกิดขึ้น

ถึงแม้มาตรฐาน IPv6 จะถูกประกาศใช้งานมาเป็นระยะเวลาหนึ่งแล้ว แต่ก็ยังไม่ถูกนำมาใช้งานจริงอย่างแพร่หลาย เนื่องจากระบบที่ใช้งานในปัจจุบันอยู่ภายใต้มาตรฐาน IPv4 เกือบทั้งหมด ปัจจุบันการใช้งาน IPv6 ส่วนใหญ่จะยังคงอยู่ในขั้นเตรียมการย้าย หรือระหว่างการทดสอบเท่านั้น แต่ก็มีบางองค์กรที่ได้นำ IPv6 มาใช้เป็นการภายในแล้วก็มี

การใช้งานทั้ง 2 โพรโทคอลได้พร้อมกันทำให้การเข้าถึงข่าวสารและบริการต่างๆ ขององค์กรไม่ถูกจำกัดอยู่เพียงกลุ่มผู้ให้บริการ หรือกลุ่มผู้ใช้บริการที่ใช้เทคโนโลยีของ IPv4 หรือ IPv6 เพียงกลุ่มเดียวแต่ก็ทำให้สิ้นเปลืองงบประมาณ ดังนั้นเพื่อให้ผู้ออกแบบเครือข่ายสามารถออกแบบเครือข่ายใหม่ หรือปรับปรุงแก้ไขระบบเครือข่ายในช่วงเปลี่ยนผ่านเทคโนโลยีนี้ได้อย่างมีประสิทธิภาพ ผู้ออกแบบจึงควรรู้ถึงขีดความสามารถ ข้อกำหนดและการทำงานของ IPv6 รวมถึงวิธีการย้ายระบบ (Migration) จากระบบปัจจุบันไปยังระบบใหม่โดยให้มีผลกระทบกับการใช้งานน้อยที่สุด

จากแนวคิดดังกล่าว ทำให้เกิดความสนใจในการศึกษาเรื่องนี้และมีความต้องการทดสอบการทำงานของ IPv6 ให้รู้ถึงความสามารถและการนำไปใช้งานในเครือข่ายภายในและภายนอกได้อย่างมีประสิทธิภาพ

1.2 จุดประสงค์

- เพื่อศึกษาการทำงานของ IPv6 และการตั้งค่าอุปกรณ์เครือข่ายให้สามารถสื่อสารได้ทั้งในโพรโตคอล IPv4 และ IPv6
- เพื่อให้เครือข่ายของสถาบันฯ และสาขาวิชาฯ สามารถใช้งานบน IPv6 ได้อย่างมีประสิทธิภาพ
- เพื่อทดสอบการเชื่อมต่อไปยังเครือข่ายอินเทอร์เน็ตปัจจุบันที่ทำงานภายใต้ IPv6 ผ่านระบบ Tunnel
- เพื่อให้สามารถนำความรู้ความเข้าใจไปใช้ในการออกแบบเครือข่ายได้อย่างมีประสิทธิภาพ
- เพื่อจัดทำคู่มือการตั้งค่าอุปกรณ์สื่อสารที่ทำงานบน IPv6
- เพื่อส่งเสริมให้องค์กรต่างๆ นำ IPv6 ไปใช้งานมากขึ้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1.3 ขอบเขตของโครงงาน

- ทดสอบการเชื่อมต่อภายใต้โทโพโลยีแบบ Native IPv4
- ทดสอบการเชื่อมต่อภายใต้โทโพโลยีแบบ Native IPv6
- ทดสอบการเชื่อมต่อภายใต้โทโพโลยีแบบ Dual Stack
- ทดสอบการเชื่อมต่อภายใต้โทโพโลยีแบบ Manual Tunnel
- ทดสอบการเชื่อมต่อภายใต้โทโพโลยีแบบ GRE Tunnel (4over6)
- ทดสอบการเชื่อมต่อภายใต้โทโพโลยีแบบ GRE Tunnel (6over4)
- ทดสอบการเชื่อมต่อภายใต้โทโพโลยีแบบ Automatic 6to4 Tunnel
- ทดสอบการเชื่อมต่อภายใต้โทโพโลยีแบบ IPv4-Compatible Tunnel (2 Routers)
- ทดสอบการเชื่อมต่อภายใต้โทโพโลยีแบบ IPv4-Compatible Tunnel (3 Routers)
- ทดสอบการเชื่อมต่อภายใต้โทโพโลยีแบบ 6RD Tunnel
- ทดสอบการเชื่อมต่อภายใต้โทโพโลยีแบบ ISATAP Tunnel
- ทดสอบการเชื่อมต่อไปยังเครือข่ายอินเทอร์เน็ตที่ทำงานบน IPv6
- จัดทำเว็บไซต์คู่มือแนะนำและการตั้งค่าอุปกรณ์สื่อสารที่ทำงานบน IPv6

1.4 ประโยชน์ที่คาดว่าจะได้รับ

- เรียนรู้หลักการทำงานของ IPv6
- เรียนรู้ประสิทธิภาพการทำงานของ IPv6 บนโทโพโลยีต่างๆ
- สามารถทำเว็บไซต์คู่มือการตั้งค่าและใช้งานอุปกรณ์เครือข่ายบนเครือข่าย IPv6 ได้
- สามารถนำไปปรับปรุงเครือข่ายของสาขาวิชาฯ ได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 2
ทฤษฎีพื้นฐาน

ในหัวข้อนี้จะกล่าวถึงทฤษฎีพื้นฐานต่างๆ ที่เกี่ยวข้องในการทำโครงงาน โดยในบทนี้จะกล่าวถึง พื้นฐานของอินเทอร์เน็ตโพรโทคอลรุ่นที่ 6 (Internet Protocol version 6: IPv6), การใช้งานร่วมกันระหว่าง IPv6 และ IPv4 (IPv6 Transition and Integration), ระบบปฏิบัติการเครือข่าย (Internetwork Operating System: IOS) ของ บริษัท ซิสโก้ ซีสเต็มส์ จำกัด และทฤษฎีพื้นฐานของภาษา HTML, PHP, CSS และ JavaScript ในการสร้างเว็บไซต์คู่มือการตั้งค่าอุปกรณ์สื่อสารบน IPv6

2.1 อินเทอร์เน็ตโพรโทคอลรุ่นที่ 6 [1], [5], [6], [7], [8], [9], [10]

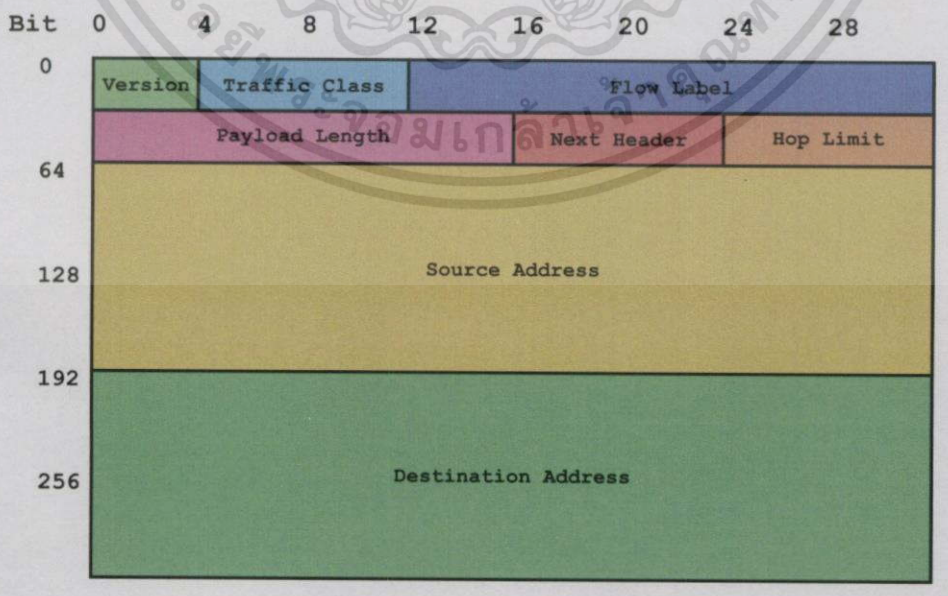
2.1.1 คุณสมบัติของอินเทอร์เน็ตโพรโทคอลรุ่นที่ 6

ระบบอินเทอร์เน็ตจะไม่สามารถทำงานได้เลย หากขาดส่วนประกอบที่สำคัญไป นั่นคือ "อินเทอร์เน็ตโพรโทคอล (Internet Protocol: IP)" IP เป็นส่วนสำคัญที่จัดการการสื่อสารและส่งข้อมูลทั้งภายในเครือข่ายและข้ามระบบเครือข่าย ภายใต้การอ้างอิงด้วย "หมายเลขที่อยู่อินเทอร์เน็ตโพรโทคอล (IP Address)" อีกทั้งยังกำหมดมาตรฐานต่างๆ ในการติดต่อสื่อสาร ตั้งแต่วิธีการจัดเรียงข้อมูลก่อนนำส่งตลอดจนการนำส่งข้อมูลเสร็จสิ้น

2.1.1.1 ข้อมูลส่วนหัว

ข้อมูลส่วนหัว (Packet Header) ของ IPv6 ถูกกำหนดไว้รองรับความต้องการขั้นต่ำ (Minimum Requirement) ที่ต้องใช้ในการนำส่งข้อมูล โดยอาจจะมีข้อมูลส่วนหัวเพิ่มเติม (Extension Header) ตามมาหรือไม่ก็ได้

สำหรับ IPv6 กำหนดให้ข้อมูลส่วนหัว มีความยาวคงที่ขนาด 320 บิต ดังรูปที่ 2.1



รูปที่ 2.1 ข้อมูลส่วนหัวของอินเทอร์เน็ตโพรโทคอลรุ่นที่ 6 [13]

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

โดยแต่ละเขตข้อมูล (field) มีความหมายดังนี้

- Version: หมายถึงรุ่นของอินเทอร์เน็ตโพรโทคอลที่ใช้งาน สำหรับ IPv6 เขตข้อมูลนี้จะมีค่าเท่ากับ 0110 ในเลขฐาน 2 หรือ 6 ในเลขฐาน 10

- Traffic Class: สามารถแยกย่อยได้อีก 2 ค่า โดย 6 บิตแรก แสดงถึงบริการชนิดต่างๆ ซึ่งให้บริการ ทั้งนี้เพื่อควบคุมรักษาคุณภาพการให้บริการ (Quality of Service; QoS) และอีก 2 บิตใช้แลกเปลี่ยนสภาพความคับคั่งของข้อมูล (Congestion) ระหว่างอุปกรณ์สื่อสาร

- Flow Label: สำหรับควบคุมปริมาณการใช้งานประเภทเวลาจริง (Real Time) เพื่อให้สามารถควบคุมและจัดการปริมาณการใช้งานประเภทต่อเนื่องและต้องการการตอบสนองที่รวดเร็วได้อย่างเหมาะสม

- Payload Length: ขนาดของข้อมูลรวมไปถึงข้อมูลเพิ่มเติมส่วนหัว ในหน่วยไบต์ (Byte)

- Next Header: บอกประเภทของส่วนหัวที่อยู่ถัดไปว่าเป็นข้อมูลส่วนหัวเพิ่มเติม หรือส่วนหัวของโพรโทคอลชั้นที่สูงกว่า

- Hop Limit: ใช้กำหนดจำนวนอุปกรณ์เครือข่ายสูงสุดที่แพ็กเก็ตสามารถเดินทางผ่านได้

- Source Address: หมายเลขที่อยู่ IP ต้นทาง

- Destination Address: หมายเลขที่อยู่ IP ปลายทาง

2.1.1.2 ข้อมูลส่วนหัวเพิ่มเติม

ข้อมูลส่วนหัวเพิ่มเติม (Extension Header) คือส่วนหัวที่บรรจุข้อมูลที่เป็นตัวเลือก (Optional) ของชั้นอินเทอร์เน็ต (Internet Layer) ข้อมูลส่วนหัวเพิ่มเติมจะถูกบรรจุระหว่างข้อมูลส่วนหัวและส่วนหัวของโพรโทคอลชั้นที่สูงกว่า มีประเภทต่างๆ ที่สำคัญดังนี้

- Hop-by-Hop Options: เพื่อให้อุปกรณ์เครือข่ายที่อยู่ในเส้นทางทำตามเงื่อนไข เช่น เพิ่มขนาดข้อมูลให้สามารถบรรจุได้มากกว่า 65,535 ไบต์

- Routing: เพื่อกำหนดเส้นทางในการนำส่งข้อมูล

- Fragment: ใช้แบ่งข้อมูลออกเป็นส่วนๆ โดยมีการหาค่าของขนาดขนส่งสูงสุดของเส้นทางนั้นๆ (Path Maximum Transfer Unit: PMTU) ไว้ก่อนแล้ว ดังนั้นข้อมูลจะถูกแบ่งที่ต้นทางเท่านั้น แล้วจึงถูกนำส่งออกไป

- Authentication Header (AH): เพื่อยืนยันตัวตนของแหล่งต้นกำเนิด

- Encapsulating Security Payload (ESP): เพื่อควบคุมและกำหนดการเข้ารหัสสำหรับช่องทางการสื่อสารที่มีความปลอดภัย

- Destination Options: เพื่อให้อุปกรณ์สื่อสารปลายทางทำตามเงื่อนไขที่กำหนด

ตารางที่ 2.1 ตารางระบุ Header ของ IPv6 และรหัสประจำ Header

Header Type	Next Header Code
Basic IPv6 Header	-
Hop-by-Hop Options	0

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 2.1(ต่อ) ตารางระบุ Header ของ IPv6 และรหัสประจำ Header

Header Type	Next Header Code
Destination Options (with Routing Options)	60
Routing Header	43
Fragment Header	44
Authentication Header	51
Encapsulation Security Payload Header	50
Destination Options	60
Mobility Header	135
No next header	59
TCP	6
UDP	17
ICMPv6	58

2.1.2 หมายเลขอินเทอร์เน็ตโพรโทคอลรุ่นที่ 6

2.1.2.1 ประเภทของหมายเลขที่อยู่ IPv6

หมายเลขที่อยู่ IPv6 สามารถแบ่งได้ 3 ประเภทตามรูปแบบการใช้งานดังนี้

- หมายเลขที่อยู่ Unicast ใช้สำหรับระบุอุปกรณ์สื่อสารเพียงอุปกรณ์เดียว ข้อมูลที่ถูกส่งไปยังหมายเลขที่อยู่ Unicast จะถูกส่งไปยังอุปกรณ์นั้นๆ
- หมายเลขที่อยู่ Anycast ใช้สำหรับระบุกลุ่มของอุปกรณ์สื่อสาร ข้อมูลที่ถูกส่งไปยังหมายเลขที่อยู่ Anycast จะถูกส่งไปยังอุปกรณ์ที่ใกล้ที่สุด โดยขึ้นอยู่กับการประเมินค่าระยะทาง (cost) ของโพรโทคอลเลือกเส้นทาง (Routing Protocol) ที่ใช้งาน
- หมายเลขที่อยู่ Multicast ใช้สำหรับระบุกลุ่มของอุปกรณ์สื่อสาร ข้อมูลที่ถูกส่งไปยังหมายเลขที่อยู่ Multicast จะถูกส่งไปยังทุกๆ อุปกรณ์

2.1.2.2 รูปแบบของ IPv6 Address

หมายเลข IPv6 มีความยาวขนาด 128 บิต จะถูกเขียนแบ่งออกเป็น 8 กลุ่ม กลุ่มละ 16 บิต ตัวเลขในแต่ละกลุ่มจะถูกเขียนด้วยเลขฐาน 16 และแต่ละกลุ่มจะถูกแยกกันด้วยเครื่องหมายทวิภาค (:) เช่น 2001:0db8:017e:000d:0e49:0000:0000:0001

หมายเลข IPv6 สามารถแบ่งได้ 2 ส่วนหลักๆ ได้แก่ หมายเลขเครือข่าย (Network Prefix) และหมายเลขโฮสหรือหมายเลขอินเตอร์เฟส (Host ID/Interface ID) ซึ่งมีความยาวส่วนละ 64 บิต โดยยังสามารถแยก Network Prefix ออกได้เป็น 2 องค์ประกอบย่อยคือ เราท์ติ้งพรีฟิกซ์ (Routing Prefix) และ ซับเน็ตไอดี (Subnet ID)

2.1.2.3 การเขียน IPv6 Address

เพื่อให้การเขียนหมายเลข IPv6 เป็นมาตรฐานเหมือนกันทั่วโลก "คณะทำงานเฉพาะกิจด้านวิศวกรรมอินเทอร์เน็ต (Internet Engineering Task Force; IETF)" จึงกำหนดการเขียนหมายเลข IPv6 เพิ่มเติมไว้ดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- ตัวอักษรโรมันที่ถูกใช้ในเลขฐาน 16 (A - F) ให้ใช้ตัวพิมพ์เล็กทั้งหมด (a, b, c, d, e, f)

- หากมีกลุ่มของเลขศูนย์ติดกันตั้งแต่ 2 กลุ่มเป็นต้นไป ให้ลดรูปด้วยเครื่องหมาย "::" ได้เพียง 1 ครั้งและต้องลดรูปให้มากที่สุด เช่น 2001:db8:0:0:0:0:2:1 เขียนแทนด้วย 2001:db8::2:1 ไม่ใช่ 2001:db8::0:2:1

- หากมีกลุ่มที่สามารถลดรูปได้ 2 กลุ่มที่แยกออกจากกัน ให้ลดรูปในกลุ่มที่มีขนาดใหญ่กว่า เช่น 2001:0:0:1:0:0:0:1 เขียนแทนด้วย 2001:0:0:1::1 ไม่ใช่ 2001::1:0:0:0:1

- หากมีกลุ่มที่สามารถลดรูปได้ 2 กลุ่มที่แยกออกจากกันและมีขนาดเท่ากัน ให้ลดรูปในกลุ่มที่พบเป็นลำดับแรกจากทางซ้ายมือ เช่น 2001:db8:0:0:1:0:0:1 เขียนแทนด้วย 2001:db8::1:0:0:1

- หากกลุ่มใดมีเลขศูนย์นำหน้า ให้ลดรูปโดยการตัดเลขศูนย์ที่นำหน้าในกลุ่มนั้นออกทั้งหมด เว้นแต่ถ้ากลุ่มนั้นมีค่าเป็น 0000 ฐาน 16 ให้คงเลขศูนย์ไว้ 1 ตำแหน่ง เช่น 2001:0db8:0000:0001::0001 เขียนแทนด้วย 2001:db8:0:1::1

2.1.3 หมายเลขที่อยู่ Unicast

หมายเลขที่อยู่ Unicast ของ IPv6 ทำงานร่วมกับหมายเลขเครือข่ายส่วนหน้า (Prefix) เช่นเดียวกับ IPv4 ภายใต้ "การจัดสรรหมายเลขที่อยู่ IP แบบไม่ตามคลาส (Classless Inter-Domain Routing; CIDR)"

2.1.3.1 หมายเลขที่ไม่นิยาม (Unspecified Address)

หมายเลข 0:0:0:0:0:0:0:0 (::) ใช้สำหรับเป็นหมายเลขที่อยู่ต้นทางของแพ็กเก็ตในการเริ่มต้นร้องขอหมายเลขที่อยู่ IPv6 เท่านั้น และห้ามใช้เป็นหมายเลขปลายทาง แพ็กเก็ตใดๆ ที่มีหมายเลขต้นทางเป็น :: จะไม่ถูกส่งต่อ (forward) โดยเราท์เตอร์ (Router)

2.1.3.2 หมายเลขวนกลับ (Loopback Address)

หมายเลข 0:0:0:0:0:0:0:1 (::1) ใช้สำหรับทดสอบการทำงานของโพรโทคอลบนโฮสต์หรืออุปกรณ์นั้นๆ โดยเป็นการส่งแพ็กเก็ตหาตัวเอง หมายเลขนี้เป็นหมายเลขที่อยู่สำหรับอินเทอร์เฟสจำลอง (Virtual interface) ทำงานในลักษณะของ Link-Local Scope

2.1.3.3 หมายเลขที่อยู่ Global Unicast

ในส่วนของ Global Routing Prefix ซึ่งถูกแจกจ่ายโดยผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider; ISP) และ Subnet ID ของหมายเลขที่อยู่ Global Unicast สามารถแบ่งองค์ประกอบย่อยดังนี้

- Format Prefix (FP) มีขนาด 3 บิต ใช้สำหรับกำหนดประเภทของ IPv6 โดยปัจจุบันใช้เพียงหมายเลข 001 (2000::/3) เพื่อระบุว่าเป็นหมายเลขที่อยู่ Global Unicast

- Top-Level Aggregation Identifier (TLA ID) มีขนาด 13 บิต ใช้สำหรับกำหนดหมายเลขเครือข่ายระดับบนสุด มักใช้ในการกำหนดจาก IANA (Internet Assigned Numbers Authority) ให้กับ RIR (Regional Internet Registry) เช่น APNIC, ARIN, RIPE NCC เป็นต้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- Sub-TLA Aggregation Identifier (Sub-TLA ID) มีขนาด 13 บิต ใช้สำหรับแจกจ่ายให้แต่ละองค์กร มักใช้ในการกำหนดจาก RIR สู่ LIR (Local Internet Registry)

- Next-Level Aggregation Identifier (NLA ID) มีขนาด 19 บิต ใช้สำหรับแจกจ่ายภายในแต่ละองค์กร

n bits	m bits	128-n-m bits
global routing prefix	subnet ID	interface ID

รูปที่ 2.2 รูปแบบทั่วไปของหมายเลขที่อยู่ Global Unicast

โดยส่วนของ global routing prefix แสดงถึงแหล่งที่ตั้งระบบเครือข่าย (site) ส่วนของ subnet ID แสดงหมายเลขประจำซับเน็ต/ลิงค์ในแหล่งที่ตั้งนั้นๆ และ interface ID แสดงหมายเลขประจำอินเตอร์เฟสนั้นๆ ในซับเน็ต โดยอาจมาจากการใช้ EUI-64 หรือการตั้งค่าด้วยตนเอง

2.1.3.4 หมายเลขที่อยู่ Link-Local Unicast

หมายเลขที่อยู่ Link-Local Unicast ใช้สำหรับ 1 ลิงค์อินเตอร์เฟส ในการตั้งค่าหมายเลขต่างๆ และการค้นพบเพื่อนบ้าน (Neighbor Discovery) เมื่อไม่มีเราท์เตอร์ ซึ่งจะขึ้นต้นด้วย fe80::/10 มีโครงสร้างดังรูปที่ 2.3

10 bits	54 bits	64 bits
1111111010	0	interface ID

รูปที่ 2.3 รูปแบบทั่วไปของหมายเลขที่อยู่ Link-Local Unicast

โดยเราท์เตอร์จะไม่นำส่งแพ็กเก็ตที่มีที่อยู่ปลายทางกลุ่มนี้ออกไป

2.1.3.5 หมายเลขที่อยู่ Site-Local Unicast

หมายเลขที่อยู่ Site-Local Unicast ถูกออกแบบสำหรับใช้งานภายในองค์กร/หน่วยงานนั้นๆ

หมายเลขที่อยู่ Site-Local Unicast จะขึ้นต้นด้วย fec0::/10 ปัจจุบันหมายเลขประเภทนี้ไม่มีการใช้งานแล้วตามเอกสาร RFC 3879

2.1.3.6 หมายเลข IPv6 ที่ผนวก IPv4 ไว้ด้วย (IPv6 Address with Embedded IPv4 Addresses)

หมายเลข IPv6 ที่ผนวก IPv4 ไว้ด้วยสามารถแยกได้ 2 ประเภท ดังนี้

- IPv4-Compatible IPv6 Address ใช้สำหรับการแปลง (transition) ระหว่าง IPv4 และ IPv6 ซึ่งปัจจุบันไม่ได้ใช้งานแล้ว มีรูปแบบคือ IPv4: “192.168.1.1” จะได้ IPv6: “::192.168.1.1”

- IPv4-Mapped IPv6 Address ใช้สำหรับการแทน (represent) IPv4 ในรูปของ IPv6 โดยมีรูปแบบคือ IPv4: “192.168.1.1” จะได้ IPv6: “::ffff:192.168.1.1”

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.1.4 หมายเลขที่อยู่ Anycast

หมายเลขที่อยู่ Anycast ถูกกำหนดให้กับหลายๆ อินเตอร์เฟส (มักจะเป็นของแต่ละอุปกรณ์) ข้อมูลจะถูกส่งไปยังอุปกรณ์ที่อยู่ใกล้อุปกรณ์ต้นทางมากที่สุด โดยวัดค่าระยะทางจากโพรโทคอลเลือกเส้นทางที่ใช้งานอยู่

หมายเลขที่อยู่ Anycast มีโครงสร้างเหมือนกับหมายเลขที่อยู่ Unicast ดังนั้นเมื่อหมายเลขที่อยู่ Unicast ถูกกำหนดให้กับอุปกรณ์มากกว่า 1 อุปกรณ์ ก็จะกลายเป็น หมายเลขที่อยู่ Anycast

หมายเลขที่อยู่ Anycast ถูกใช้เพื่อยืนยันตัวตนในกลุ่มของอุปกรณ์เครือข่ายต่างๆ ที่เป็นขององค์กรใด องค์กรหนึ่ง เพื่อความสะดวกในการจัดการ

n bits	128-n bits
subnet prefix	0...0

รูปที่ 2.4 รูปแบบทั่วไปของหมายเลขที่อยู่ Anycast

รูปที่ 2.4 แสดงโครงสร้างของหมายเลขเอนี่คาส โดยส่วนของ subnet prefix จะต้องระบุลิงค์ที่แตกต่างกันได้ คือ routing prefix รวมกับ subnet ID นั่นเอง

2.1.5 หมายเลขที่อยู่ Multicast

หมายเลขที่อยู่ Multicast ถูกกำหนดให้กับหลายๆ อินเตอร์เฟสเช่นเดียวกับ หมายเลขที่อยู่ Anycast แต่ข้อมูลจะถูกส่งไปยังทุกๆ อุปกรณ์ภายในมัลติคาสนั้น

8 bits	4 bits	4 bits	112 bits
11111111	flags	scope	group ID

รูปที่ 2.5 รูปแบบทั่วไปของหมายเลขที่อยู่ Multicast

โครงสร้างส่วนของ flag คือ 0RPT โดย

- 0 เป็นส่วนที่ถูกสงวนไว้ (reserved) สำหรับใช้ในอนาคต
- T มีค่าเป็น “0” เมื่อเป็นหมายเลขมัลติคาสแบบถาวร (permanently-assigned) ซึ่งถูกกำหนดโดย Internet Assigned Numbers Authority (IANA) และมีค่าเป็น “1” เมื่อเป็นหมายเลขมัลติคาสแบบไม่ถาวร/ชั่วคราว (non-permanently-assigned/transient/dynamically)
- R, P เป็นส่วนเพิ่มเติมตามเอกสาร RFC 3956 และ RFC 3306 ตามลำดับ

โครงสร้างส่วนของ scope ใช้สำหรับกำหนดขอบเขตของการมัลติคาส มีค่าดังตารางที่ 2.2

ตารางที่ 2.2 ตารางระบุค่าของ scope ในหมายเลขที่อยู่ Multicast

Scope value	Meaning
0	reserved
1	Interface-Local scope
2	Link-Local scope

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 2.2(ต่อ) ตารางระบุค่าของ scope ในหมายเลขที่อยู่ Multicast

Scope value	Meaning
3	reserved
4	Admin-Local scope
5	Site-Local scope
6	unassigned
7	unassigned
8	Organization-Local scope
9	unassigned
A	unassigned
B	unassigned
C	unassigned
D	unassigned
E	Global scope
F	reserved

ตัวอย่างการใช้งาน เช่น interface-local สำหรับ 1 อินเตอร์เฟสบนลูปแบ็ค, link-local สำหรับติดต่อในยูนิคาสซับเน็ตเดียวกัน, organization-local สำหรับจัดการหลายๆ ไซต์ซึ่งอยู่ภายใต้หน่วยงานเดียวกัน และ unassigned scope สำหรับให้ผู้ดูแลระบบเครือข่าย (network administrator) ประกาศขอบเขตเพิ่มเติมเอง

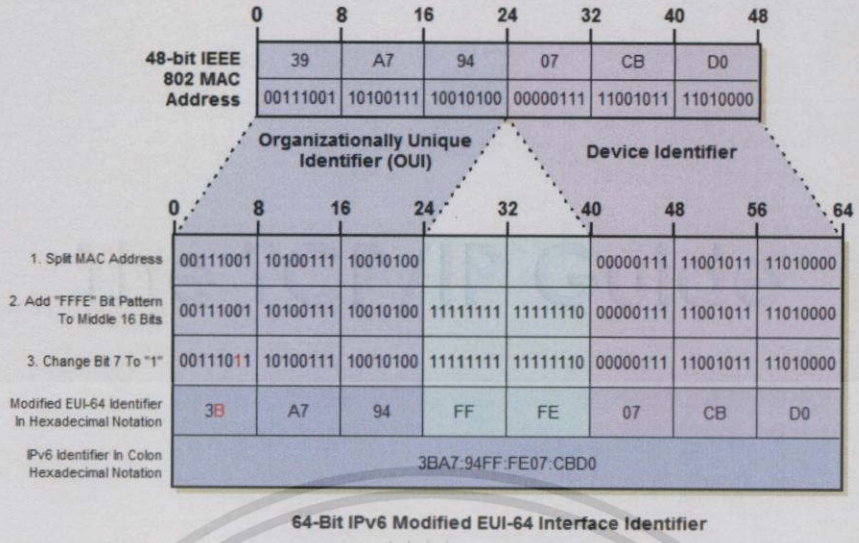
2.1.6 การสร้างหมายเลขอินเตอร์เฟสในรูปแบบ EUI-64

การสร้างหมายเลขอินเตอร์เฟสเพื่อให้สามารถระบุอินเตอร์เฟสได้อย่างถูกต้องสามารถทำได้หลายวิธี โดยขึ้นอยู่กับประเภทของอินเตอร์เฟสนั้นๆ เช่น

2.1.6.1 ลิงค์/โหนดที่มี EUI-64 อยู่แล้ว (IEEE EUI-64 Identifiers)
สำหรับอินเตอร์เฟสประเภทนี้ ให้กลับค่าบิตของบิตที่ 7 เพียงค่าเดียว

2.1.6.2 ลิงค์/โหนดที่มี MAC-address (IEEE 802 48-bit MACs)
อินเตอร์เฟส MACs ให้เพิ่ม 0xFFFE เข้าตรงกลางของ MAC-address (ระหว่างหมายเลขบริษัทและหมายเลขผู้ผลิต) และให้กลับค่าของบิตที่ 7 ดังรูปที่ 2.6

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 2.6 การเปลี่ยนหมายเลข MAC-address ให้มีโครงสร้างแบบ EUI-64 [14]

2.1.6.3 ลิงค์ที่ใช้หมายเลขประเภทอื่นๆ

ให้ใช้หมายเลขเดิมของอินเตอร์เฟสนั้นๆ แล้วเติมบิตศูนย์เข้าไปด้านหน้าจนครบ 64 บิต

2.1.6.4 ลิงค์ที่ไม่มีหมายเลขระบุใดๆ

ลิงค์ประเภทนี้มักเป็นลิงค์อนุกรม (Serial Link) ให้ใช้การกำหนดค่าด้วยตนเอง โดยจะต้องตรวจสอบให้แน่ใจว่าไม่ซ้ำกับอินเตอร์เฟสอื่นๆ ภายในลิงค์เดียวกัน

2.1.7 การตั้งค่าหมายเลขที่อยู่ IPv6 แบบอัตโนมัติ [12]

การตั้งค่าแบบอัตโนมัติของหมายเลข IPv6 สามารถแบ่งได้ 2 ประเภทคือ

2.1.7.1 การตั้งค่าแบบสเตทเลท (Stateless)

การตั้งค่าประเภทนี้ ใช้หมายเลขอินเตอร์เฟสในการตั้งค่าร่วมด้วย โดยใช้โพรโทคอลใหม่ของ IPv6 ที่ชื่อ "โพรโทคอลค้นพบเพื่อนบ้าน (Neighbor Discovery Protocol: NDP)" เพื่อระบุ Network Prefix ร่วมกับ Interface ID ที่ได้จากการสร้าง EUI-64 Identifier รวมเป็นหมายเลขที่อยู่ IPv6 (มักพบในหมายเลขที่อยู่ไอพีประเภท Link-local) ร่วมกับโพรโทคอลดีเอชซีพีสำหรับ IPv6 (DHCPv6) แต่ DHCPv6 จะแจกเฉพาะหมายเลขที่อยู่ไอพีของเครื่องแม่ข่ายที่ให้บริการพื้นฐานเท่านั้น เช่น บริการโดเมนเนม (Domain Name System: DNS) หรือ บริการเทียบเวลาบนอินเตอร์เน็ต (Network Time Protocol: NTP) รวมไปถึงชี้เกตเวย์ (Gateway) ให้กับโฮสต์ด้วย

2.1.7.2 การตั้งค่าแบบสเตทฟูล (Stateful)

จากการใช้ DHCPv6 ร่วมกับการตั้งค่าแบบ Stateless หมายเลขที่อยู่ไอพี ที่ได้เมื่อมองในมุมมองของผู้บริหารเครือข่าย (Network Administrator) จะพบว่าไม่มีความเป็นระเบียบ เนื่องจาก Interface ID ขึ้นอยู่กับหมายเลข EUI-64 ของอินเตอร์เฟสที่ใช้งานอยู่ ดังนั้นการตั้งค่าแบบ Stateful จึงเป็นการกำหนดหมายเลขที่อยู่ IPv6 ให้ทั้งชุด โดยไม่อ้างอิงตามหมายเลขประจำอินเตอร์เฟสของโฮสต์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.1.8 การตั้งค่าหมายเลขที่อยู่ IPv6

ในยุคของ IPv4 นั้น ในช่วงแรกแต่ละอินเตอร์เฟสสามารถมีได้หมายเลขที่อยู่ไอพี ได้เพียง 1 หมายเลขเท่านั้น แต่หลังการปรับปรุงมีการอนุญาตให้ใช้งาน "หมายเลขที่อยู่ไอพีรอง (Secondary IP Address)" หากต้องการใช้หมายเลขที่อยู่ไอพีเพิ่มเติมจะต้องสร้าง "เอเลียสไอพี (Alias IP)" หรือ "อินเตอร์เฟสเสมือน (Virtual Interface)" ซึ่งมักพบบนระบบปฏิบัติการลินุกซ์มากกว่าวินโดวส์

แต่สำหรับ IPv6 นั้น อนุญาตให้ 1 อินเตอร์เฟสสามารถมีได้หลายหมายเลขที่อยู่ไอพีได้ ซึ่งมีข้อดีคือถึงแม้ในเครือข่ายจะไม่มีอุปกรณ์พื้นฐาน (เช่น เราท์เตอร์) อุปกรณ์สื่อสารก็สามารถค้นหากันได้ (Discoverable) โดยใช้ หมายเลขที่อยู่ใน Link-local Scope และเมื่อมีการเพิ่มเราท์เตอร์เพื่อต่อออกไปยังอินเตอร์เน็ต ก็จะเพิ่ม Global Scope Address เข้ามาโดยไม่มีการเปลี่ยนแปลง Link-local Address ทำให้การสื่อสารที่กำลังเกิดขึ้นขณะเพิ่มการเชื่อมต่ออินเตอร์เน็ตไม่ขัดข้อง

ดังนั้น การใช้งาน IPv6 แต่ละอินเตอร์เฟสจำเป็นต้องมีอย่างน้อย 1 Link-local Address และหากมีการออกสู่อินเตอร์เน็ตด้วย ก็จะเพิ่ม Global Scope Address เข้ามา

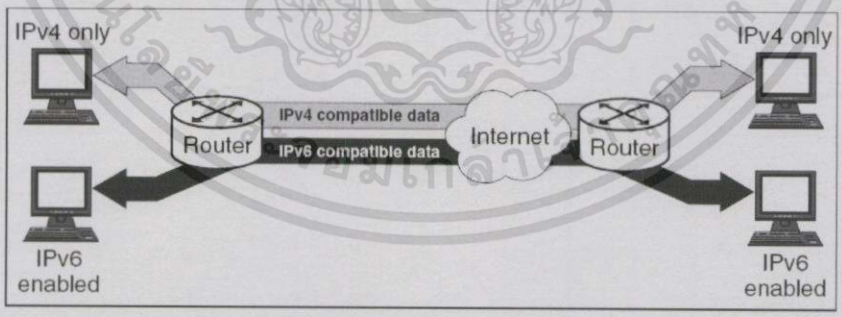
2.2 การใช้งานร่วมกันระหว่าง IPv6 และ IPv4

2.2.1 ภาพรวมของเทคนิคการเปลี่ยนจาก IPv4 ไปยัง IPv6 (Transition Technology)

การเปลี่ยนแปลงจาก IPv4 ไปยัง IPv6 จะต้องทำแบบค่อยเป็นค่อยไป เนื่องจากระบบเดิมยังคงถูกใช้งานอยู่ และระบบใหม่ก็มีความจำเป็นที่จะต้องเข้ามาแทนที่

2.2.1.1 Dual Stacks

คือระบบที่สามารถใช้งานได้ทั้ง IPv4 และ IPv6 โดยสามารถแยกได้เป็น 2 ประเภท

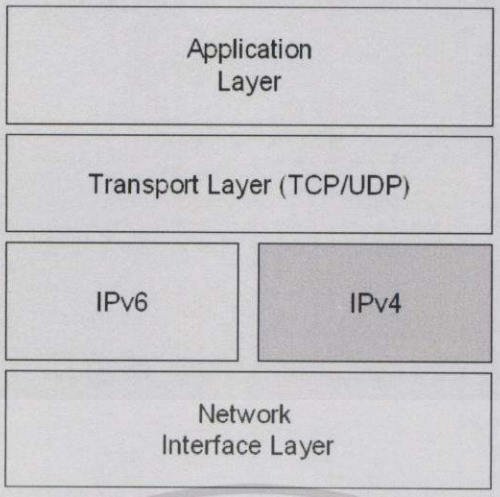


รูปที่ 2.7 การเชื่อมต่อแบบ Dual Stack [15]

- Dual IP Layer Architecture

เป็นการพัฒนาโพรโทคอลใน Network Layer ให้ทำงานแยกกันระหว่าง IPv4 และ IPv6 ดังรูปที่ 2.8

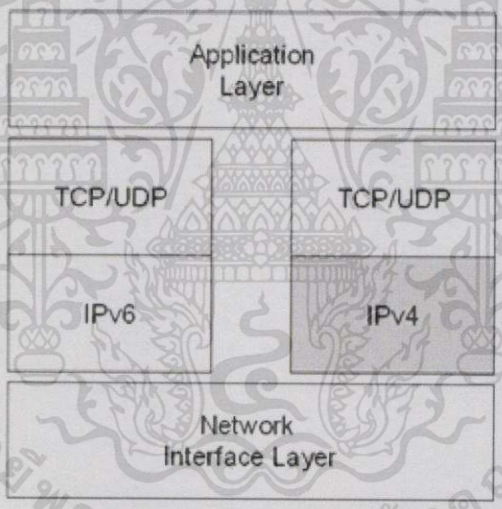
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 2.8 Dual IP Layer Architecture

- Dual Stack Architecture

เป็นการพัฒนาโพรโทคอลใน Transport Layer ให้ทำงานแยกกันระหว่าง IPv4 และ IPv6 ดังรูปที่ 2.9



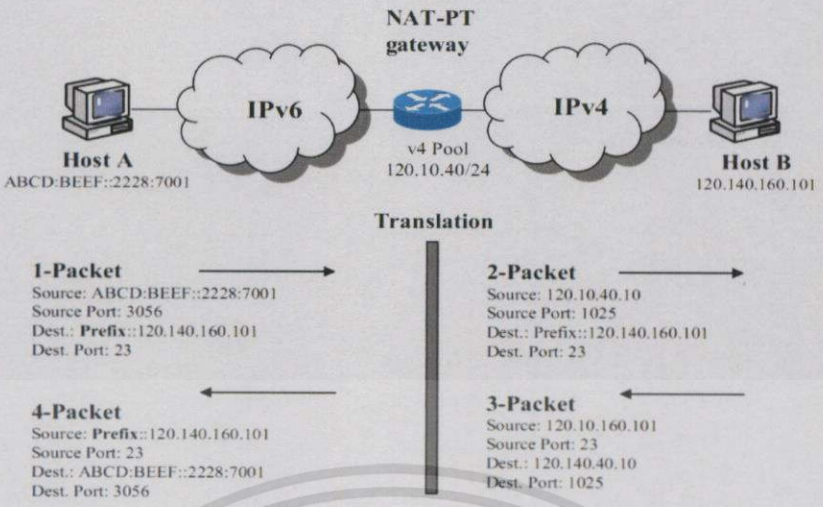
รูปที่ 2.9 Dual Stack Architecture

การทำงานแบบ Dual Stack มีข้อดีคือสามารถสื่อสารได้กับทั้ง 2 โพรโทคอล

2.2.1.2 Header Translation

Header Translation หรือ Network Address Translation-Protocol Translation (NAT-PT) เป็นการแปลงหมายเลขที่อยู่ IPv4 ให้อยู่ในรูปแบบ IPv6 ด้วยวิธี IPv4-Mapped IPv6 Address ในหัวข้อ 2.1.3.6 มักใช้ในกรณีที่เครือข่ายส่วนใหญ่เปลี่ยนเป็นระบบ IPv6 แล้วทำให้ไม่ต้อง Encapsulate ซึ่งทำให้แพ็กเก็ตมีขนาดใหญ่ขึ้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

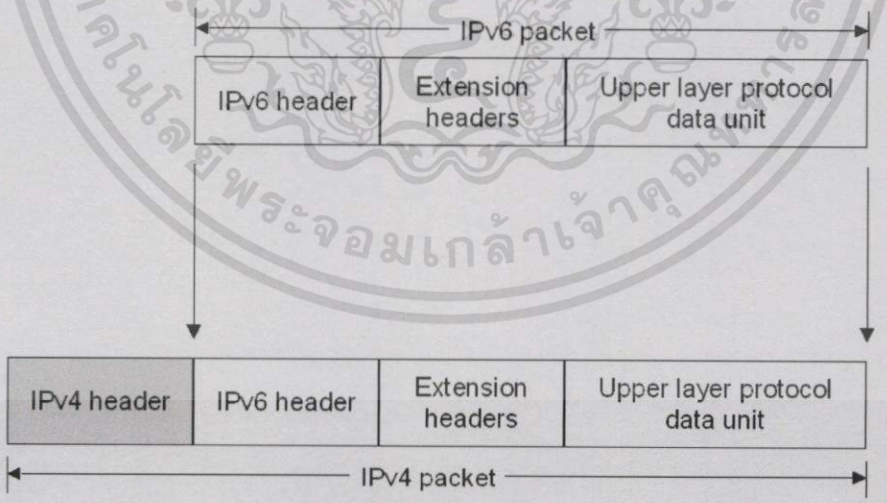


รูปที่ 2.10 ภาพรวมของการทำงานแบบ NAT-PT [4]

Header Translation สามารถทำได้ทั้งใน Network Layer, Transport Layer และ Application Layer

2.2.1.3 Tunneling

คือการบรรจุแพ็กเก็ต IPv6 ให้อยู่ในแพ็กเก็ต IPv4 (encapsulation) ที่ต้นทางของอุโมงค์สื่อสารแล้วจึงส่งออกไปโดยผ่านเครือข่ายของ IPv4 และถอดแพ็กเก็ต IPv6 ออกจากแพ็กเก็ต IPv4 (decapsulation) ที่ปลายอุโมงค์สื่อสาร หรือในทางกลับกัน เราสามารถเอาแพ็กเก็ต IPv6 ห่อหุ้มแพ็กเก็ต IPv4 ได้ด้วยเช่นกัน

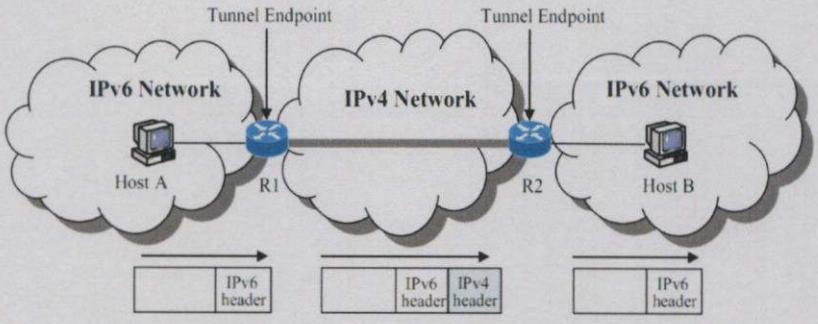


รูปที่ 2.11 การห่อหุ้มแพ็กเก็ต IPv6 ด้วยแพ็กเก็ต IPv4

2.2.2 การทำอุโมงค์สื่อสาร (Tunneling)

อุโมงค์สื่อสารเป็นวิธีที่มีความยืดหยุ่นสูง สามารถทำงานได้หลายรูปแบบ เช่น ใช้ อุโมงค์สื่อสารเพียงวิธีเดียว, ใช้อุโมงค์สื่อสารร่วมกับ Dual Stack, ใช้อุโมงค์สื่อสารร่วมกับ Header Translation

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 2.12 ภาพรวมของการทำงานแบบ Tunneling [4]

2.2.2.1 อุโมงค์แบบตั้งค่า (Configured Tunnels)

การใช้งาน Configured Tunnel จำเป็นต้องตั้งค่าปลายทางการเชื่อมต่อทั้ง 2 ด้านให้เรียบร้อยก่อน ซึ่งการที่จะตั้งค่าอุปกรณ์ที่อยู่นอกความดูแลทำให้ไม่สะดวก

2.2.2.2 อุโมงค์แบบอัตโนมัติ (Automatic Tunnels)

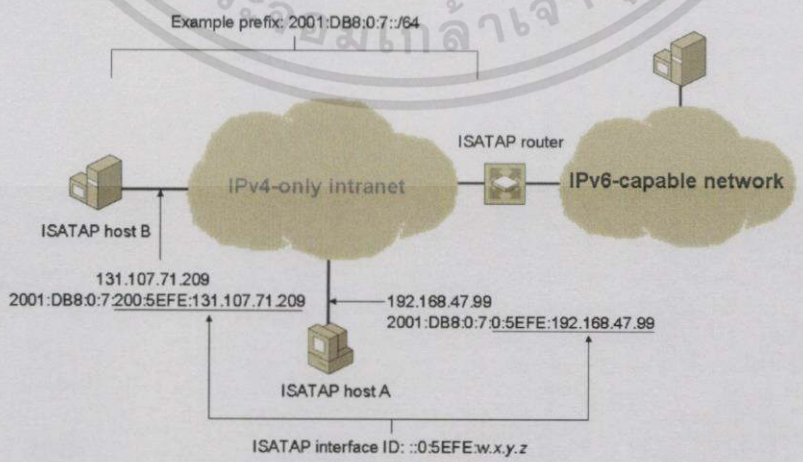
Automatic Tunnel จะเลือกเส้นทางจากหมายเลขที่อยู่ IPv6 ปลายทาง (Destination IPv6 Address) และเงื่อนไขอื่นๆ ของแต่ละอินเตอร์เฟส มีวิธีที่นิยมใช้ 2 วิธีได้แก่ ไอซาแทป (ISATAP) และ 6ทู4 (6to4)

2.2.3 ไอซาแทป

ไอซาแทป (Intra-Site Automatic Tunnel Addressing Protocol; ISATAP) ใช้หมายเลขที่อยู่ IPv6 ที่เกิดจากวิธีการฝังหมายเลขที่อยู่ IPv4 ลงใน IPv6 โดยมีเงื่อนไขว่า

- Interface ID ของ IPv6 จะมีค่าเป็น ::5EFE:w.x.y.z เมื่อ w.x.y.z คือหมายเลขที่อยู่ Private IPv4
- Interface ID ของ IPv6 จะมีค่าเป็น ::200:5EFE:w.x.y.z เมื่อ w.x.y.z คือหมายเลขที่อยู่ Public IPv4

หมายเลข ISATAP ที่ได้สามารถนำไปใช้กับหมายเลขที่อยู่ Unicast ใดๆ ก็ได้ ที่มีความยาว Prefix เท่ากับ 64 บิต (/64)

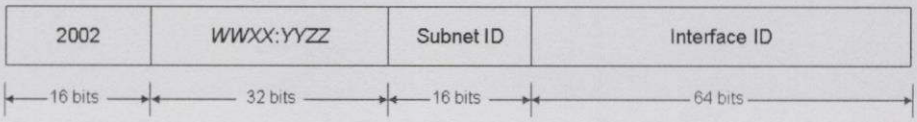


รูปที่ 2.13 ตัวอย่างหมายเลข ISATAP [11]

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.2.4 6to4

6to4 ใช้หมายเลขที่อยู่ IPv6 ที่เกิดจากการฝังหมายเลขที่อยู่ IPv4 ลงในหมายเลขที่อยู่ IPv6 เช่นเดียวกับ ISATAP แต่มีโครงสร้างต่างกัน โดยหมายเลขที่อยู่ IPv6 ของ 6to4 มีโครงสร้าง คือ 2002:WWXX:YYZZ::/48 เมื่อ WWXX:YYZZ คือการเขียน IPv4 Address w.x.y.z ให้อยู่ในรูปของหมายเลขที่อยู่ IPv6 (colon-hexadecimal representation)



รูปที่ 2.14 โครงสร้างหมายเลข IPv6 ของ 6to4

แต่ 6to4 มีข้อเสียคือ หมายเลขที่อยู่ IPv4 ที่ใช้งานได้ จะต้องเป็นหมายเลขที่อยู่ Public IPv4 เท่านั้น ดังนั้นหากมีการใช้ "การแปลงหมายเลขเครือข่าย (Network Address Translation; NAT)" เครื่องแม่ข่าย NAT (มักเป็นเราท์เตอร์) จะต้องรองรับการทำ 6to4 และต้องใช้ 6to4 Relay ก่อนออกสู่เครือข่าย IPv6

2.3 คำสั่งและการกำหนดค่า IPv6 บน IOS [2], [3]

Cisco มีระบบปฏิบัติการที่ควบคุมการทำงาน คล้ายกับระบบปฏิบัติการที่ใช้กับเครื่องพีซีทั่วไป ระบบปฏิบัติการดังกล่าวมีชื่อว่า Cisco IOS (Internetwork Operating System) ซึ่งเป็นระบบปฏิบัติการที่จะทำให้สามารถตั้งค่าการทำงาน รวมถึงการบริหารจัดการเราท์เตอร์และอุปกรณ์เชื่อมต่อกับเราท์เตอร์ของ Cisco ได้โดยสะดวก ซึ่งในระบบปฏิบัติการ IOS ของ Cisco นี้ มีคำสั่งที่ทำงานในโหมดต่างๆ หลายโหมดดังต่อไปนี้

- User EXEC Mode
- Privileged EXEC Mode
- Global Configuration Mode

2.3.1 User EXEC Mode

User EXEC Mode เป็นโหมดแรกที่พบเมื่อเชื่อมต่อเข้ากับเราท์เตอร์ วิธีสังเกตว่าได้เข้าสู่ User EXEC Mode คือสังเกตจาก Prompt ของเราท์เตอร์ที่แสดงบนหน้าจอ ได้แก่ ชื่อของเราท์เตอร์แล้วตามด้วยเครื่องหมาย > เช่น

```
Router_name>
```

ตารางที่ 2.3 ตารางระบุคำสั่งที่ใช้งานบ่อยใน User EXEC Mode

คำสั่ง	การทำงาน
access-enable	สร้าง Access List entry ชั่วคราว
clear	ล้างการทำงานที่ตั้งค่าไว้
connect	เปิดการเชื่อมต่อ Terminal
disable	ปิดหรือยกเลิกคำสั่งที่อยู่ใน Privileged EXEC Mode
enable	เข้าสู่ Privileged EXEC Mode

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 2.3(ต่อ) ตารางระบุคำสั่งที่ใช้งานบ่อยใน User EXEC Mode

คำสั่ง	การทำงาน
exit	ออกจากการใช้ User EXEC Mode
help	ใช้เพื่อแสดงรายการช่วยเหลือ
login	เข้าสู่ระบบเข้ามาเป็น user
logout	ออกจาก EXEC
ping	ใช้เพื่อทดสอบการเชื่อมต่อ (ส่ง ICMP Echo-request Packet)
show	แสดงข้อมูลต่างๆ ของเราท์เตอร์ในปัจจุบัน
ssh	เปิดการเชื่อมต่อทาง Secure Shell
telnet	เปิดการเชื่อมต่อทาง Telnet
traceroute	เป็นการใช้ Traceroute เพื่อหาเส้นทางการเชื่อมต่อไปยังปลายทาง
tunnel	เปิดการเชื่อมต่อแบบ Tunnel

2.3.2 Privileged EXEC Mode

เป็นโหมดที่สามารถดูการตั้งค่าในตัวเราท์เตอร์ได้ทั้งหมด โหมดนี้จะสามารถเข้าสู่การทำงานของโหมดย่อยอื่นๆ เพื่อการเปลี่ยนค่า Configuration รวมทั้งขอบข่ายการทำงานของเราท์เตอร์ได้

วิธีการเข้าสู่ Privileged EXEC Mode ได้แก่การใช้คำสั่ง enable ขณะยังอยู่ใน User EXEC Mode เมื่อเข้าโหมดนี้ ส่วนใหญ่มักจะมีการร้องขอรหัสผ่าน (หากมีการตั้งค่าไว้) เมื่อรหัสผ่านถูกต้อง จะพบว่า Prompt จะเปลี่ยนจาก > เป็น # เช่น

```
Router#
```

ตารางที่ 2.4 ตารางระบุคำสั่งที่ใช้งานบ่อยใน Privileged EXEC Mode

คำสั่ง	การทำงาน
clock	จัดการระบบนาฬิกาของระบบ
configure	เข้าสู่ Configure Mode
copy	เป็นการคัดสำเนาการตั้งค่าและข้อมูล
debug	เป็นการใช้คำสั่ง debug
delete	เป็นคำสั่งลบไฟล์
dir	ดูรายชื่อไฟล์ในระบบ
disable	เป็นการยกเลิก Privileged EXEC Mode
enable	ใช้เพื่อเปิดการเข้าสู่ Privileged EXEC mode
erase	ใช้เพื่อการลบข้อมูลในหน่วยความจำแฟลชหรือหน่วยความจำที่เก็บการตั้งค่าในเราท์เตอร์
exit	ใช้เพื่อออกจาก EXEC mode
help	คำสั่งการช่วยเหลือ
logout	ใช้เพื่อออกจาก EXEC mode
mkdir	สร้างไดเร็กทอรี่ใหม่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 2.4(ต่อ) ตารางระบุคำสั่งที่ใช้งานบ่อยใน Privileged EXEC Mode

คำสั่ง	การทำงาน
more	แสดงเนื้อหาของไฟล์
no	ยกเลิกการทำงานของคำสั่ง debugging
reload	ใช้เพื่อ Restart แบบ Cold Restart (Reset ตัวเองแล้วเริ่มทำงานใหม่)
rmdir	ลบไดเร็กทอรี่
setup	เรียกตัวช่วยตั้งค่า
test	ทดสอบระบบภายใน รวมทั้งหน่วยความจำและอินเตอร์เฟส
undebug	ยกเลิกการใช้ debug
verify	ใช้เพื่อตรวจสอบความถูกต้องของไฟล์ที่อยู่ในหน่วยความจำแฟลช
vlan	ตั้งค่า VLAN พารามิเตอร์
write	ใช้เพื่อบันทึกการตั้งค่าไปที่หน่วยความจำเครือข่ายหรือ Terminal

2.3.3 Global Configuration Mode

Global Configuration Mode เป็นโหมดที่สามารถกำหนดการทำงาน หรือปรับเปลี่ยนการตั้งค่าทั้งหมดในเราท์เตอร์ เมื่อใดที่เข้าสู่โหมดนี้ไปแล้ว จะสามารถเข้าสู่การทำงานของโหมดการทำงานย่อยอื่นๆ (Sub-configuration Mode) เพื่อการเปลี่ยนการตั้งค่าของอินเตอร์เฟสต่างๆ จนถึงการกำหนดลักษณะการทำงานของเราท์เตอร์ได้ Prompt ของเราท์เตอร์ที่แสดงบนหน้าจอเป็นดังนี้

```
Router(config)#
```

ตารางที่ 2.5 ตารางระบุคำสั่งที่ใช้งานบ่อยใน Global Configuration Mode

คำสั่ง	การทำงาน
access-list	กำหนด Access List
banner	กำหนด Banner ต่างๆ
boot	เปลี่ยนการตั้งค่าของการเริ่มการทำงาน
cdp	คำสั่งย่อยของการตั้งค่า CDP
class-map	กำหนดค่าแมพคลาส
clock	จัดการเกี่ยวกับเวลาของเราท์เตอร์
config-register	เปลี่ยนค่ารีจิสเตอร์ที่ใช้เริ่มต้นการทำงาน
crypto	เข้ารหัสโมดูล
do	ใช้เพื่อรันคำสั่งของ EXEC Mode ใน Configuration Mode
default	ล้างการตั้งค่าให้กลับไปเหมือนค่าเริ่มต้น
enable	เปลี่ยนการตั้งค่าเกี่ยวกับรหัสผ่าน
end	ออกจาก Global Configuration Mode
exit	ออกจาก Global Configuration Mode
help	แสดง Help Menu
hostname	เปลี่ยนชื่อเราท์เตอร์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 2.5(ต่อ) ตารางระบุคำสั่งที่ใช้งานบ่อยใน Global Configuration Mode

คำสั่ง	การทำงาน
interface	เลือกอินเตอร์เฟสที่ต้องการจะตั้งค่า
ip	คำสั่งย่อยของการตั้งค่า IP
ipv6	คำสั่งย่อยของการตั้งค่า IPv6
line	ใช้เพื่อการตั้งค่าสำหรับ Terminal Line
login	บังคับให้มีการเข้าสู่ระบบ
mac-address-table	กำหนดค่าตารางหมายเลข MAC
no	ยกเลิกคำสั่งเดิมที่สั่งไว้ หรือกำหนดเป็นค่าเริ่มต้น
router	คำสั่งย่อยของการตั้งค่าโพรโทคอลการเลือกเส้นทาง (Routing Protocol)

2.3.4 การกำหนดค่าหมายเลขที่อยู่ IPv6 และทำ IPv6 Routing

การทำงานนี้ทำเพื่อกำหนดหมายเลข IPv6 เพื่อให้เชื่อมต่อกับเราท์เตอร์อื่นๆ และเปิดการส่งต่อ IPv6 บนเส้นทางการเชื่อมต่อทั่วโลก โดยค่าเริ่มต้นนั้นภายในเราท์เตอร์จะยังไม่ได้ถูกกำหนดค่าใดๆ และ โพรโทคอลเลือกเส้นทางของ IPv6 นั้นก็ยังไม่ได้ถูกเปิดการใช้งาน เพื่อให้เราท์เตอร์ทำงานบน IPv6 ได้อย่างมีประสิทธิภาพ จึงเสนอวิธีการตั้งค่าต่างๆ ดังนี้

- Native IPv6 Address
- Dual IP Stack
- IPv6 Tunneling ซึ่งสามารถแยกย่อยได้หลายวิธีดังนี้
  - Manual IPv6 Tunnel
  - GRE IPv6 Tunnel
  - Automatic 6to4 Tunnel
  - IPv4-Compatible IPv6 Tunnel
  - 6RD Tunnel
  - ISATAP

2.3.4.1 IPv6 Address and Routing

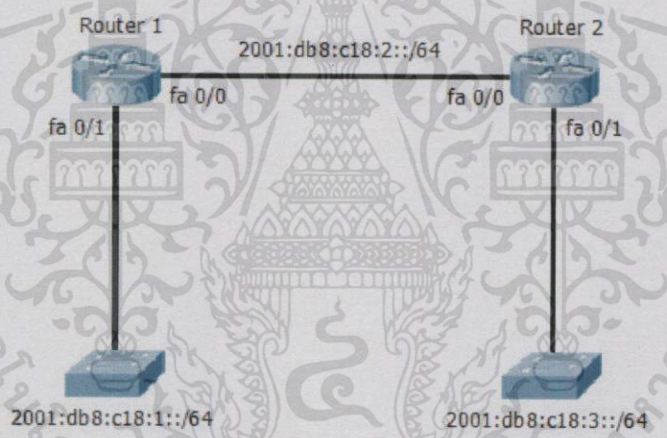
ตารางที่ 2.6 ตารางระบุขั้นตอนการกำหนดค่า Native IPv6 Address

	คำสั่ง	คำอธิบาย
ขั้นที่ 1	enable	เข้า privileged mode
ขั้นที่ 2	configure terminal	เข้า configuration mode.
ขั้นที่ 3	ipv6 unicast-routing	เปิดใช้การส่งต่อข้อมูล (forwarding) IPv6 บนเราท์เตอร์
ขั้นที่ 4	interface *type number*	ระบุชนิดและหมายเลข interface เพื่อเข้า interface configuration mode

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 2.6(ต่อ) ตารางระบุขั้นตอนการกำหนดค่า Native IPv6 Address

	คำสั่ง	คำอธิบาย
ขั้นที่ 5	ipv6 address *ipv6-prefix/prefix length* eui-64 หรือ ipv6 address *ipv6-address* link-local หรือ ipv6 address *ipv6-address* anycast หรือ ipv6 enable	ระบุหมายเลข IPv6 ที่ interface และใช้งานการประมวลผล IPv6 -ระบุหมายเลข IPv6 โดยใช้การกำหนดโดย eui-64 -ระบุหมายเลข IPv6 โดยใช้การกำหนดโดย link-local -ระบุหมายเลข IPv6 โดยใช้การกำหนดโดย Anycast
ขั้นที่ 6	no shutdown	เป็นการ Activate interface



รูปที่ 2.15 ตัวอย่างการเชื่อมต่อ Native IPv6

ตัวอย่างการตั้งค่า Router 1 ในรูปที่ 2.11 มีคำสั่งดังนี้

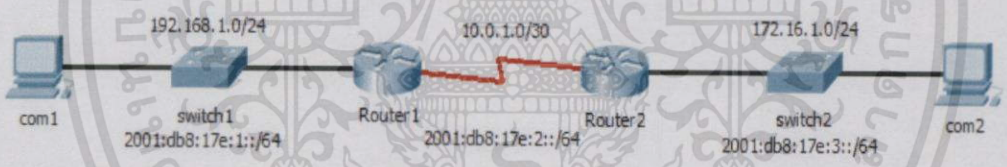
```
Router1>enable
Router1#configure terminal
Router1(config)#ipv6 unicast-routing
Router1(config)#interface fastethernet 0/0
Router1(config-if)#ipv6 address 2001:db8:c18:2::/64 eui-64
Router1(config-if)#no shutdown
Router1(config-if)#interface fastethernet 0/1
Router1(config-if)#ipv6 address 2001:db8:c18:1::/64 eui-64
Router1(config-if)#no shutdown
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.3.4.2 IPv6 Dual IP Stack

ตารางที่ 2.7 ตารางระบุขั้นตอนการกำหนดค่า IPv6 Dual IP Stack

	คำสั่ง	คำอธิบาย
ขั้นที่ 1	enable	เข้า privileged mode
ขั้นที่ 2	configure terminal	เข้า configuration mode.
ขั้นที่ 3	ipv6 unicast-routing	เปิดใช้การส่งต่อข้อมูล (forwarding) IPv6 บนเราท์เตอร์
ขั้นที่ 4	interface *type number*	ระบุชนิดและหมายเลข interface เพื่อเข้า interface configuration mode
ขั้นที่ 5	ip address ip-address mask [secondary [vrf vrf-name]]	กำหนดหมายเลข IPv4 ให้กับ interface
ขั้นที่ 6	ipv6 address {*ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length*}	ระบุ IPv6 network เพื่อกำหนดให้กับ interface
ขั้นที่ 7	no shutdown	เป็นการ Activate interface



รูปที่ 2.16 ตัวอย่างการเชื่อมต่อแบบ Dual Stack

ตัวอย่างการตั้งค่า Dual Stack บน Router

```
Router>enable
Router#configure terminal
Router(config)#ipv6 unicast-routing
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.1.0 255.255.255.0
Router(config-if)#ipv6 address 2001:db8:17e:1::/64 eui-64
Router(config-if)#no shutdown
```

2.3.4.3 Manual IPv6 Tunnel

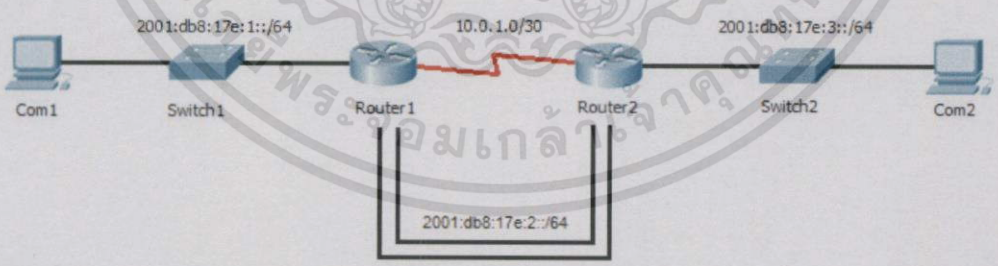
การกำหนดค่าการทำอุโมงค์ด้วยตนเองนั้นเทียบเท่ากับการเชื่อมต่อถาวรระหว่างระบบเครือข่าย IPv6 สองระบบผ่านระบบเครือข่าย IPv4 การกำหนดค่าการทำอุโมงค์สื่อสารด้วยตนเองหรือ Manual IPv6 จะต้องมีการกำหนดค่าหมายเลขที่อยู่ IPv6 ในอุปกรณ์เครือข่ายและ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กำหนดหมายเลขที่อยู่ IPv4 ที่ให้เป็นอุโมงค์ต้นทางและอุโมงค์ปลายทางด้วยตนเองทั้งหมด โฮสต์และเราท์เตอร์ที่จะกำหนดค่าแบบอุโมงค์สื่อสารนั้นต้องรองรับโปรโตคอล IPv4 และ IPv6 สแต็กด้วย

ตารางที่ 2.8 ตารางระบุขั้นตอนการกำหนดค่า Manual IPv6 Tunnel

	คำสั่ง	คำอธิบาย
ขั้นที่ 1	enable	เข้า privileged mode
ขั้นที่ 2	configure terminal	เข้า configuration mode.
ขั้นที่ 3	interface tunnel *tunnel-number*	ระบุชนิดและหมายเลข tunnel เพื่อเข้า interface configuration mode
ขั้นที่ 4	ipv6 address ipv6-prefix/prefix length eui-64	ระบุหมายเลข IPv6 ที่ interface และใช้งานการประมวลผล IPv6 ระบุหมายเลข IPv6 โดยใช้การกำหนดโดย eui-64
ขั้นที่ 5	tunnel source {ip-address | interface-type interface-number}	กำหนดชนิดและหมายเลขที่อยู่ IPv4 ของ source interface ของ tunnel interface
ขั้นที่ 6	tunnel destination ip-address	กำหนดหมายเลข IPv4 หรือ hostname สำหรับ tunnel interface
ขั้นที่ 7	tunnel mode ipv6ip	ระบุว่าเป็น manual IPv6 tunnel ปล. คำสั่ง tunnel mode ipv6ip เป็นคำสั่งที่ทำให้โปรโตคอลของ IPv6 และ IPv4 มีการห่อหุ้มและส่งผ่าน อุโมงค์ IPv6



รูปที่ 2.17 ตัวอย่างการเชื่อมต่อแบบ Manual IPv6 Tunnel

ตัวอย่างการตั้งค่าแบบ Manual IPv6 Tunnel

```
Router1>enable
Router1#configure terminal
Router1(config)#interface tunnel0
Router1(config-if)#ipv6 address 2001:db8:17e::2/64
Router1(config-if)#tunnel source serial 0/0
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
Router1(config-if)#tunnel destination 10.0.1.0
Router1(config-if)#tunnel mode ipv6ip
```

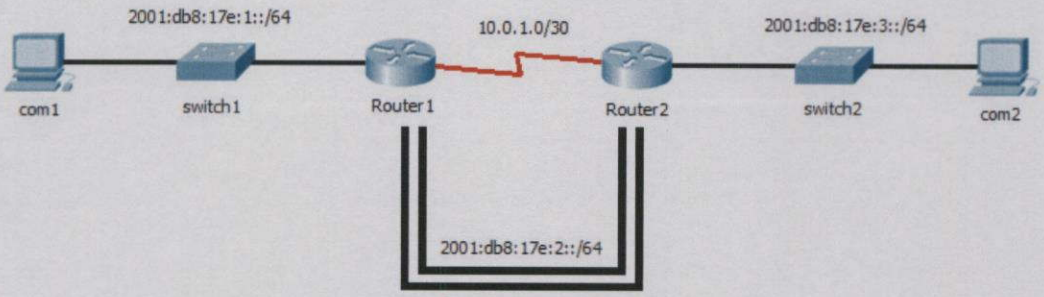
2.3.4.4 GRE IPv6 Tunnel

การใช้งานหลักๆของอุโมงค์สื่อสารแบบ GRE คือใช้สำหรับการเชื่อมต่อที่มีเสถียรภาพ ต้องมีความปลอดภัยระหว่างเราท์เตอร์ที่อยู่ขอบนอกทั้งสอง หรือระหว่างระบบกับเราท์เตอร์ที่อยู่ขอบนอก การทำอุโมงค์สื่อสารแบบ GRE สามารถกำหนดค่าให้ทำงานอยู่ชั้นเครือข่าย IPv6 รวมถึงการส่งแพ็กเก็ต IPv6 ในอุโมงค์ IPv6 หรือในอุโมงค์ IPv4 และแพ็กเก็ต IPv4 ในอุโมงค์ IPv6

ตารางที่ 2.9 ตารางระบุขั้นตอนการกำหนดค่า GRE IPv6 Tunnel

	คำสั่ง	**คำอธิบาย**
ขั้นที่ 1	enable	เข้า privileged mode
ขั้นที่ 2	configure terminal	เข้า configuration mode.
ขั้นที่ 3	interface tunnel *tunnel-number*	ระบุชนิดและหมายเลข tunnel เพื่อเข้า interface configuration mode
ขั้นที่ 4	ipv6 address *ipv6-prefix/prefix length* eui-64	ระบุหมายเลข IPv6 ที่ interface และใช้งานการประมวลผล IPv6 ระบุหมายเลข IPv6 โดยใช้การกำหนดโดย eui-64
ขั้นที่ 5	tunnel source *{ip-address | interface-type interface-number}*	กำหนดชนิดและหมายเลขที่อยู่ IPv4 ของ source interface ของ tunnel interface -อุปกรณ์เครือข่ายที่ระบุจะต้องเป็นการกำหนดแบบหมายเลขที่อยู่ IPv4
ขั้นที่ 6	tunnel destination *{host-name | ip-address | ipv6-address}*	กำหนดหมายเลขที่อยู่ IPv6 ปลายทางหรือ hostname สำหรับ tunnel interface
ขั้นที่ 7	tunnel mode {aurp | cayman | dvmrp | eon | gre| gre multipoint | gre ipv6 | ipip [decapsulate-any] | iptalk | ipv6 | mpls | nos	ระบุว่าเป็น GRE IPv6 tunnel

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 2.18 ตัวอย่างการเชื่อมต่อแบบ GRE IPv6 Tunnel

ตัวอย่างการตั้งค่าแบบ GRE IPv6 Tunnel

```
Router>enable
Router#configure terminal
Router(config)#interface tunnel0
Router(config-if)#ipv6 address 2001:db8:17e:2::/64
Router(config-if)#tunnel source ethernet 0
Router(config-if)#tunnel destination 2001:db8:17e:1::/64
Router(config-if)#tunnel mode gre ipv6
```

2.3.4.5 Automatic 6to4 Tunnel

การทำงานในวิธีนี้จะคล้ายกับการทำงานแบบกำหนดค่าด้วยตนเอง ต่างกันที่แบบกำหนดค่าด้วยตนเองเป็นแบบจุดต่อจุด (Point-to-point) และต้องกำหนดหมายเลขที่อยู่ปลายทางที่ต้องการเชื่อมต่อด้วยตนเอง แต่แบบ 6to4 เป็นแบบจุดหนึ่งไปยังหลายจุด (Point-to-multipoint) และกำหนดค่าหมายเลขที่อยู่ปลายทางโดยอัตโนมัติ ในแบบ 6to4 อุโมงค์สื่อสารปลายทางจะถูกกำหนดโดยหมายเลขที่อยู่ IPv4 ของเราท์เตอร์ขอบนอก และถูกใส่หมายเลขส่วนหน้าเครือข่ายเป็น 2002::/16 เป็นไปตามรูปแบบ 2002:border-router-IPv4-address::/48

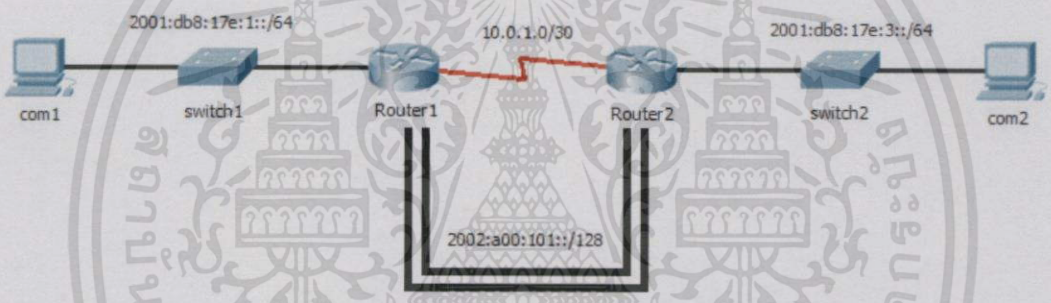
ตารางที่ 2.10 ตารางระบุขั้นตอนการกำหนดค่า Automatic 6to4 Tunnel

	คำสั่ง	คำอธิบาย
ขั้นที่ 1	enable	เข้า privileged mode
ขั้นที่ 2	configure terminal	เข้า configuration mode.
ขั้นที่ 3	interface tunnel *tunnel-number*	ระบุชนิดและหมายเลข tunnel เพื่อเข้า interface configuration mode
ขั้นที่ 4	ipv6 address *ipv6-prefix/prefix length* eui-64	ระบุหมายเลข IPv6 ที่ interface และใช้งานการประมวลผล IPv6 32 บิตจะขึ้นต้นด้วย 2002::/16

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 2.10(ต่อ) ตารางระบุขั้นตอนการกำหนดค่า Automatic 6to4 Tunnel

	คำสั่ง	คำอธิบาย
ขั้นที่ 5	tunnel source *{ip-address | interface-type interface-number}*	กำหนดชนิดและหมายเลขของ source interface ของ tunnel interface -อุปกรณ์เครือข่ายที่ระบุจะต้องเป็นการกำหนดแบบหมายเลขที่อยู่ IPv4
ขั้นที่ 6	tunnel mode ipv6ip 6to4	ระบุว่า IPv6 tunnel ใช้แบบ 6to4 address
ขั้นที่ 7	exit	กลับไปยัง configuration mode
ขั้นที่ 8	ipv6 route *ipv6-prefix / prefix-length* tunnel *tunnel-number*	กำหนดเส้นที่คงที่สำหรับ IPv6 6to4 Prefix 2002::/16 ไปที่ tunnel interface หมายเลขอุโมงค์ที่ระบบในคำสั่ง ipv6 route ต้องเหมือนกับหมายเลขอุโมงค์ในคำสั่ง interface tuunel



รูปที่ 2.19 ตัวอย่างการเชื่อมต่อแบบ Automatic 6to4 Tunnel

ตัวอย่างการตั้งค่าแบบ Automatic 6to4 Tunnel

```
Router>enable
Router#configure terminal
Router(config)#interface tunnel0
Router(config-if)#ipv6 address 2002:a00:101::/128
Router(config-if)#tunnel source ethernet 0
Router(config-if)#tunnel mode ipv6ip 6to4
Router(config-if)#exit
Router(config)#ipv6 route 2002::/16 tunnel 0
```

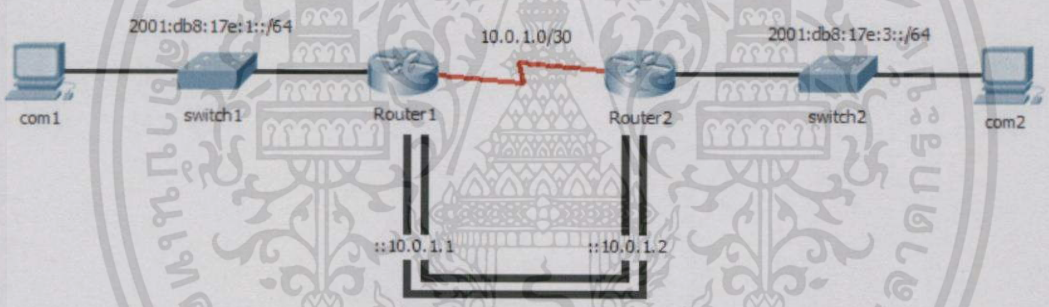
2.3.4.6 IPv4-Compatible IPv6 Tunnel

หมายที่อยู่ของ IPv4-Compatible IPv6 คือหมายเลขที่มี “0” อยู่ใน 96 บิตแรกของหมายที่อยู่และหมายเลขที่อยู่ IPv4 ใน 32 บิตหลัง สามารถเขียนได้ เช่น 0:0:0:0:0:0:A.B.C.D หรือ ::A.B.C.D อุโมงค์สื่อสารปลายทางจะถูกกำหนดโดยอัตโนมัติโดยหมายเลขที่อยู่ IPv4 ที่อยู่ใน 32 บิตหลังของหมายเลขที่อยู่ IPv4-Compatible IPv6

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 2.11 ตารางระบุขั้นตอนการกำหนดค่า IPv4-Compatible IPv6 Tunnel

	คำสั่ง	คำอธิบาย
ขั้นที่ 1	enable	เข้า privileged mode
ขั้นที่ 2	configure terminal	เข้า configuration mode.
ขั้นที่ 3	interface tunnel *tunnel-number*	ระบุชนิดและหมายเลข tunnel เพื่อเข้า interface configuration mode
ขั้นที่ 4	tunnel source *{ip-address | interface-type interface-number}*	กำหนดชนิดและหมายเลขของ source interface ของ tunnel interface -อุปกรณ์เครือข่ายที่ระบุจะต้องเป็นการกำหนดแบบหมายเลขที่อยู่ IPv4
ขั้นที่ 5	tunnel mode ipv6ip auto-tunnel	ระบุว่า IPv4-compatible tunnel ใช้แบบ IPv4-compatible IPv6 address



รูปที่ 2.20 ตัวอย่างการเชื่อมต่อแบบ IPv4-Compatible IPv6 Tunnel

ตัวอย่างการตั้งค่าแบบ IPv4-Compatible IPv6 Tunnel

```
Router>enable
Router#configure terminal
Router(config)#interface tunnel0
Router(config-if)#tunnel source ethernet 0
Router(config-if)#tunnel mode ipv6ip auto-tunnel
```

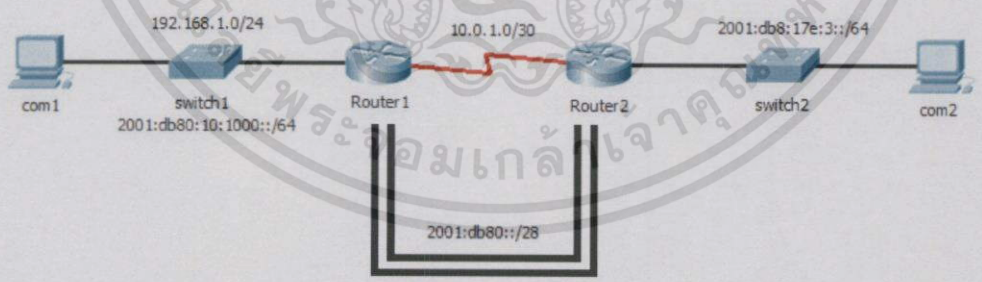
2.3.4.7 6RD Tunnel

6RD มีลักษณะเป็นส่วนขยายของ 6to4 ซึ่งช่วยให้ผู้ให้บริการสามารถให้บริการ IPv6 Unicast ให้กับลูกค้าผ่านเครือข่าย IPv4 โดยนำหมายเลข IPv4 ที่ได้รับจากบริการ DHCP มาใช้เป็นส่วนหนึ่งของหมายเลข IPv6 ด้วย ทำให้การทำอุโมงค์สื่อสารแบบ 6RD นั้นไม่จำเป็นต้องมีหมายเลขเครือข่ายส่วนหน้าเป็น 2002::/16

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 2.12 ตารางระบุขั้นตอนการกำหนดค่า 6RD Tunnel

	คำสั่ง	คำอธิบาย
ขั้นที่ 1	enable	เข้า privileged mode
ขั้นที่ 2	configure terminal	เข้า configuration mode.
ขั้นที่ 3	interface tunnel *tunnel-number*	ระบุชนิดและหมายเลข tunnel เพื่อเข้า interface configuration mode
ขั้นที่ 4	tunnel source *{ip-address | interface-type interface-number}*	กำหนดชนิดและหมายเลขของ source interface ของ tunnel interface
ขั้นที่ 5	tunnel mode ipv6ip [6rd | 6to4 | auto-tunnel | isatap]	กำหนด static IPv6 interface
ขั้นที่ 6	tunnel 6rd prefix *ipv6-prefix / prefix-length*	ระบุ Prefix ของ IPv6 ที่ใช้ร่วมกันบน IPv6 rapid 6RD tunnel
ขั้นที่ 7	tunnel 6rd ipv4 {prefix-length *length*} {suffix-length *length*	กำหนดความยาวของ Prefix หรือ Suffix ของ IPv4
ขั้นที่ 8	tunnel 6rd br *ipv4-address*	กำหนดเราท์เตอร์ขอบนอกของระบบที่ทำหน้าที่แจกหมายเลขส่วนหน้าของที่อยู่ IPv6 (เฉพาะเราท์เตอร์ลูกข่าย)



รูปที่ 2.21 ตัวอย่างการเชื่อมต่อแบบ 6RD Tunnel

ตัวอย่างการตั้งค่าแบบ 6RD Tunnel

```
Router>enable
Router#configure terminal
Router(config)#interface tunnel0
Router(config-if)#tunnel source Ethernet2/0
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

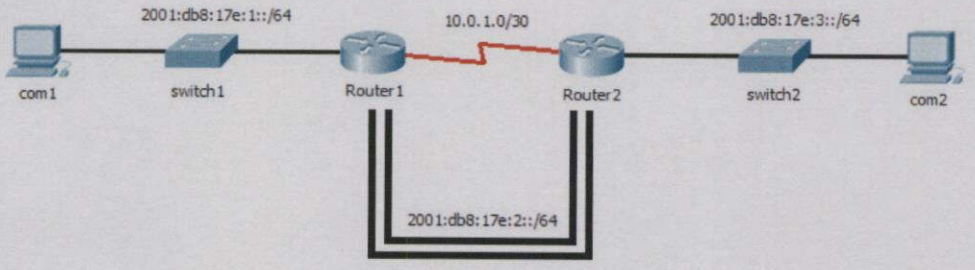
```
Router(config-if)#tunnel mode ipv6ip 6rd
Router(config-if)#tunnel 6rd prefix 2001:db80::/28
Router(config-if)#tunnel 6rd ipv4 prefix-length 16 suffix 8
```

2.3.4.8 ISATAP

ISATAP เป็นการทำอุโมงค์สื่อสารอัตโนมัติภายใต้ระบบเครือข่าย IPv4 พื้นฐาน ISATAP ถูกออกแบบมาสำหรับการขนส่งแพ็กเกจ IPv6 ถายใต้ที่ที่ยังไม่รองรับ IPv6 ทั้งหมด เราท์เตอร์ที่กำหนดค่าแบบ ISATAP นั้นสามารถทำให้ไคล์แอนแจกหมายเลขที่อยู่ IP ได้อัตโนมัติ ISATAP สามารถใช้ได้ดีกับหมายเลขที่อยู่ในรูปแบบ Unicast IPv6 Prefix (/64)

ตารางที่ 2.13 ตารางระบุขั้นตอนการกำหนดค่า ISTAP Tunnel

	คำสั่ง	คำอธิบาย
ขั้นที่ 1	enable	เข้า privileged mode
ขั้นที่ 2	configure terminal	เข้า configuration mode.
ขั้นที่ 3	interface tunnel *tunnel-number*	ระบุชนิดและหมายเลข tunnel เพื่อเข้า interface configuration mode
ขั้นที่ 4	ipv6 address *ipv6-prefix/prefix length* eui-64	ระบุหมายเลข IPv6 ที่ interface และใช้งานการประมวลผล IPv6
ขั้นที่ 5	no ipv6 nd ra suppress	คำสั่งนี้จะทำให้เราท์เตอร์สามารถ ทำการแจกหมายเลขที่อยู่ IPv6 แบบอัตโนมัติ
ขั้นที่ 6	tunnel source *{ip-address | interface-type interface-number}*	กำหนดชนิดและหมายเลขของ source interface ของ tunnel interface ประเภทและหมายเลขของอุปกรณ์เครือข่ายที่ระบุใน tunnel source จะต้องกำหนดเป็นหมายเลข IPv4
ขั้นที่ 7	tunnel mode ipv6ip isatap	ระบุว่า IPv6 overlay tunnel ใช้แบบ ISATAP address
ขั้นที่ 8	tunnel destination ip-address	กำหนดหมายเลขที่อยู่ IPv6 ปลายทางหรือ hostname สำหรับ tunnel interface



รูปที่ 2.22 ตัวอย่างการเชื่อมต่อแบบ ISATAP Tunnel

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตัวอย่างการตั้งค่าแบบ ISTAP Tunnel

```
Router>enable
Router#configure terminal
Router(config)#interface tunnel0
Router(config-if)#ipv6 address 2001:db8:17e:2::/64 eui-64
Router(config-if)#no ipv6 nd ra suppress
Router(config-if)#tunnel source ethernet 1/0
Router(config-if)#tunnel mode ipv6ip isatap
```

2.4 ทฤษฎีพื้นฐานของภาษาที่ใช้ในการสร้างเว็บไซต์ [16], [17], [18]

2.4.1 HTML (Hypertext Markup Language)

HTML เป็นภาษาที่ใช้แสดงผลในเว็บเบราว์เซอร์ (Browser) ซึ่งมีนามสกุลเป็น .htm หรือ .html ภายในไฟล์ HTML นี้จะเป็นรหัส HTML หรือเรียกอีกอย่างหนึ่งว่าแท็ก (Tag) ภาษา HTML สามารถนำไปเปิดด้วยโปรแกรมเว็บเบราว์เซอร์ต่างๆ เช่น Google Chrome, Mozilla Firefox, Internet Explorer ฯลฯ ได้ แล้วแสดงออกมาในรูปแบบเว็บเพจ

รูปแบบการเขียนโค้ด HTML นั้นจะเขียนเป็นแฟ้มข้อความ (Text file) ในปัจจุบันโปรแกรมช่วยสร้างเว็บเพจต่างๆ พยายามทำให้การเขียนภาษา HTML ทำได้ง่ายขึ้น โดยใช้การแก้ไขแบบเสมือนจริง (What You See Is What You Get; WYSIWYG) เช่น Dreamweaver เป็นต้น

2.4.1.1 รูปแบบคำสั่ง HTML

รูปแบบคำสั่งมีอยู่ 2 แบบ คือ

- แท็กที่มีจุดเริ่มต้นและจุดสิ้นสุด เช่น ... เป็นการทำให้ตัวอักษรเป็นตัวหนา หากไม่มีการปิดแท็กจะทำให้การแสดงผลผิดพลาด
- แท็กเดี่ยว คือแท็กที่เขียนไปแล้วไม่ต้องมีจุดสิ้นสุด เช่น <p> เป็นการขึ้นย่อหน้าใหม่

2.4.1.2 โครงสร้างของเอกสาร HTML

แบ่งเป็น 2 ส่วน คือ ส่วน head และส่วน body

- HEAD ใช้บอกรายละเอียดเกี่ยวกับเว็บเพจ ซึ่งจะไม่แสดงผลออกมาแต่ใช้อธิบายเกี่ยวกับข้อมูลเฉพาะของเว็บเพจนั้นๆ เช่น ชื่อเรื่อง (Title) เป็นต้น
- BODY ใช้ในการจัดรูปแบบตัวอักษร, จัดหน้า, ใส่รูปภาพ ซึ่งเนื้อหาในส่วนนี้จะแสดงที่เว็บเพจ ซึ่งการแสดงผลจะต้องใช้แท็กจำนวนมาก ขึ้นอยู่กับลักษณะของข้อมูล เช่น ข้อความ, รูปภาพ, เสียง, วีดิโอ หรือไฟล์ต่างๆ การเขียนแท็กในส่วนนี้ ไม่มีข้อจำกัดทางด้านรูปแบบ สามารถป้อนติดกัน หรือ 1 บรรทัดต่อ 1 คำสั่งก็ได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ทั้ง 2 ส่วนจะมีการวางรูปแบบแท็กดังรูปที่ 2.23

```
<html>
        <head>
                ... คำสั่งในส่วน HEAD Tag ...
        </head>
        <body>
                ... คำสั่งในส่วน BODY Tag ...
        </body>
</html>
```

รูปที่ 2.23 รูปแบบการเขียนคำสั่งภาษา HTML

2.4.1.3 คำสั่งต่างๆของ HTML

คำสั่งในส่วนหัวของเอกสาร HTML (HEAD)

1) <TITLE> ข้อความที่ใช้เป็น TITLE ไม่ควรยาวเกิน 64 ตัวอักษร, ไม่ต้องใส่ลักษณะพิเศษ เช่น ตัวหนา, เอียง หรือสี โดยข้อความในส่วนนี้จะแสดงผลในแถบชื่อ (Title Bar) ของเว็บเบราว์เซอร์

2) <META> Tag META จะไม่แสดงผลบนเว็บเบราว์เซอร์ แต่จะเป็นส่วนสำคัญ ในการบอกข้อมูลเกี่ยวกับเว็บเพจสำหรับผู้ให้บริการสืบค้นเว็บ และใช้บอกว่าใช้ชุดตัวอักษรแบบใดในการแสดงผล (Character Encoding)

คำสั่งในส่วนเนื้อหาของเอกสาร HTML (BODY)

1) กลุ่มคำสั่งเกี่ยวกับการจัดรูปแบบเอกสาร

- <p> ใช้จัดย่อหน้า เพื่อเพิ่มบรรทัดว่างก่อนและหลังข้อความ
-
 ใช้ขึ้นบรรทัดใหม่ การตัดบรรทัดใหม่นั้น โดยปกติแล้วเว็บเบราว์เซอร์จะทำการตัดบรรทัดให้เอง เมื่อไม่สามารถแสดงผลได้ครบทั้งบรรทัด แต่การแทรกแท็ก
 เข้าไป เว็บเบราว์เซอร์จะตัดบรรทัดใหม่ให้ทันที
- <h...> ใช้กับข้อความที่เป็นหัวเรื่อง แท็ก <h> จะมีทั้งหมด 6 ลำดับด้วยกัน ตั้งแต่ h1, h2, h3, h4, h5, และ h6 ซึ่งขนาดของ h1 จะใหญ่ที่สุด
- <hr> ใช้ขีดเส้นคั่น เพื่อขีดเส้นคั่นระหว่างบรรทัด
- <align=...> ใช้ในการจัดข้อความชิดซ้าย กลาง ขวา โดยระบุคือ <align='left'> ให้ชิดซ้าย, <align='right'> ชิดขวา, และ <align='center'> จัดกึ่งกลาง
- <body bgcolor=...> bgcolor ใช้กำหนดสีพื้นหลัง โดยกำหนดเป็นชื่อสี หรือรหัสสีก็ได้

2) กลุ่มคำสั่งจัดแต่งและควบคุมรูปแบบตัวอักษร

- <b> จัดรูปแบบตัวอักษรเป็นแบบตัวหนา
- <I> จัดรูปแบบตัวอักษรเป็นแบบตัวเอียง
- <s> จัดรูปแบบตัวอักษรให้มีตัวขีดฆ่า
- <sub> จัดรูปแบบตัวอักษรเป็นแบบตัวห้อย
- <sup> จัดรูปแบบตัวอักษรเป็นแบบตัวยก
- <u> จัดรูปแบบตัวอักษรเป็นแบบขีดเส้นใต้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3) กลุ่มคำกลุ่มคำสั่งเกี่ยวกับการเชื่อมโยง

การเชื่อมโยง (Link) หรือ การเชื่อมโยงหลายมิติ (Hyperlink) คือการเชื่อมโยงเว็บเพจแต่ละหน้าเข้าด้วยกันรวมถึงการเชื่อมโยงเว็บไซต์ภายนอก สร้างการเชื่อมโยงโดยใช้แท็ก <a href=link>

4) กลุ่มคำสั่งจัดการรูปภาพ

- <img src=รูปภาพ> ใช้ใส่รูป โดยอ้างอิงจากที่อยู่ของรูปในคุณลักษณะ (attribute) src

- <body background=รูปภาพ> ใช้ใส่รูปพื้นหลังในเว็บเพจ โดยอ้างอิงจากที่อยู่ของรูปในคุณลักษณะ background

5) กลุ่มคำสั่งจัดการตาราง

ในหน้าเว็บเพจประกอบด้วยข้อมูลจำนวนมาก จึงจำเป็นจะต้องจัดเรียงข้อมูลให้เป็นระเบียบเพื่อให้อ่านง่าย โดยการเขียนตารางมีโครงสร้างดังรูปที่ 2.24 โดยแท็ก tr เป็นการสร้างแถว ส่วนแท็ก td เป็นการสร้างสดมภ์ (column)

```
<table>
    <tr>
        <td></td>
    </tr>
    <tr>
        <td></td>
    </tr>
</table>
```

รูปที่ 2.24 โครงสร้างตารางในภาษา HTML

6) กลุ่มคำสั่งควบคุมเฟรม

ใช้แสดงเว็บเพจหลายๆ เว็บเพจในหน้าเดียว โดยจะแบ่งหน้าของเว็บเบราว์เซอร์ออกเป็นส่วนๆ

- <frameset cols=ขนาดเฟรม1,...> ใช้กำหนดขนาดของเฟรมในแนวตั้ง สามารถกำหนดเป็นจุดภาพ (pixel) หรือเปอร์เซ็นต์ก็ได้

- <frameset rows=ขนาดเฟรม1,...> ใช้กำหนดขนาดของเฟรมในแนวนอน สามารถกำหนดเป็นจุดภาพหรือเปอร์เซ็นต์ก็ได้

- <frame src=เว็บเพจ> นำเว็บเพจมาแสดงผลในเฟรม

- <iframe src=เว็บเพจ> แตกต่างจากเฟรมคือสามารถแทรกในเว็บเพจอื่นๆ ได้ โดยสามารถกำหนดได้ทั้งความกว้างและความยาว

2.4.2 PHP (Hypertext Preprocessor)

PHP (Hypertext Preprocessor) เป็นภาษาสคริปต์ (Script Language) ประเภท SSI (Sever Side Include) ซึ่งมีโปรแกรมที่ใช้แปล (compile) ภาษา PHP ให้อยู่ในรูปแบบเอกสาร HTML เมื่อถูกร้องข้อจากผู้ใช้บริการ

ลักษณะของ PHP ที่แตกต่างจากภาษาสคริปต์แบบอื่นๆ คือ PHP ได้รับการพัฒนาและออกแบบมา เพื่อใช้งานในการสร้างเอกสารแบบ HTML โดยสามารถสอดแทรกหรือแก้ไขเนื้อหาได้โดยอัตโนมัติ ดังนั้นจึงสามารถเรียกภาษา PHP ว่า HTML-embedded ได้เช่นเดียวกัน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.4.2.1 ข้อดีที่สำคัญของ PHP

- PHP ทำงานได้บนระบบปฏิบัติการทุกตระกูล
- เรียนรู้ได้ง่าย
- ทำงานรวดเร็วและมีประสิทธิภาพ
- ทำงานร่วมกับระบบฐานข้อมูลได้
- ใช้โครงสร้างข้อมูลแบบต่างๆ ได้

2.4.2.2 การเขียน PHP

เมื่อเขียน PHP รวมกับ HTML จะใช้สัญลักษณ์พิเศษแยก PHP ออกจาก HTML โดยมีรูปแบบคือเปิดด้วยแท็ก <?php และปิดด้วยแท็ก ?>

2.4.3 CSS (Cascading Style Sheets)

CSS เป็นคำสั่งที่ใช้คู่กับ HTML เพื่อจัดและแก้ไขรูปแบบของเว็บเพจได้ง่ายขึ้น

2.4.3.1 ข้อดีของการใช้ CSS

- ช่วยลดการใช้ HTML ในการจัดรูปแบบเหลือแต่เนื้อหา ทำให้เข้าใจง่าย สามารถแก้ไขเนื้อหาได้ง่ายและรวดเร็ว
- ขนาดไฟล์เล็กลง
- สามารถนำไปใช้กับเว็บเพจหลายๆ หน้าได้
- มีความยืดหยุ่นสูงในการปรับแต่งแก้ไข

2.4.3.2 รูปแบบคำสั่งของ CSS

รูปแบบคำสั่ง CSS มีองค์ประกอบดังนี้ และมีโครงสร้างดังรูปที่ 2.25

- selector คือส่วนที่เราต้องการจะให้แสดงผล
- property คือส่วนของคุณสมบัติที่เราต้องการให้แสดง เช่น สีตัวอักษร, ชนิดตัวอักษร, ขนาดตัวอักษร
- value คือค่าที่เราต้องการให้แสดง เช่น ตัวอักษรสีแดง, ตัวอักษรหนา, ตัวอักษรขนาด 12 pt

```
selector {
        property1: value1;
        property2: value2;
        …
        propertyN: valueN;
}
```

รูปที่ 2.25 โครงสร้างภาษา CSS

2.4.3.3 การสร้าง CSS เพื่อใช้ในเอกสาร HTML

- เขียนในเอกสาร HTML คือการเขียน CSS ในส่วน HEAD หรือในแต่ละแท็กที่ต้องการให้แสดงผล การใช้งานลักษณะนี้มักไม่นิยมเนื่องจากแก้ไขได้ยาก
- เขียนในเอกสาร CSS คือการเขียน CSS ในไฟล์ใหม่ แล้วจึงนำเข้า (import) มาในเอกสาร HTML ด้วยแท็ก <link>

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.4.3.4 การกำหนด CSS selector แบบ Class และ ID

- Class สามารถนำไปใช้งานกับส่วนต่างๆ ซ้ำได้หลายครั้ง ในการสร้าง Class จะใช้ "." นำหน้า selector

- ID สามารถนำไปใช้งานกับส่วนต่างๆ ได้เพียง 1 ครั้งต่อ 1 เว็บเพจเท่านั้น ในการสร้าง ID จะใช้ "#" นำหน้า selector

2.4.4 JavaScript

JavaScript เป็นภาษาโปรแกรมที่เรียกว่าสคริปต์ (Script) ซึ่งมีวิธีการทำงานโดยใช้ตัวแปลคำสั่งครั้งละ 1 บรรทัด (Interpreter) เดิมภาษานี้ชื่อว่า LiveScript ได้รับการพัฒนาขึ้นโดย Netscape เพื่อช่วยให้เว็บเพจสามารถแสดงเนื้อหาที่มีการเปลี่ยนแปลงไปตามเงื่อนไขได้ (Dynamic content)

เนื่องจาก JavaScript ช่วยให้ผู้พัฒนาสร้างเว็บเพจได้ตรงกับความต้องการและน่าสนใจมากขึ้น และเป็นภาษาเปิดจึงได้รับความนิยมสูง รวมทั้งได้ถูกกำหนดให้เป็นมาตรฐานโดย ECMA อีกด้วย

2.4.4.1 การทำงานของ JavaScript

การทำงานของ JavaScript เกิดขึ้นบนเว็บเบราว์เซอร์ (Client-side Script) จึงแตกต่างกับภาษาสคริปต์อื่น เช่น Perl, PHP, ASP ซึ่งต้องแปลคำสั่งและทำงานที่เครื่องแม่ข่าย จากลักษณะดังกล่าวทำให้ JavaScript มีข้อจำกัด คือไม่สามารถรับและส่งข้อมูลต่างๆ กับเครื่องแม่ข่ายได้โดยตรง เช่น การอ่านไฟล์, การสอบถามจากฐานข้อมูล เป็นต้น

การทำงานของ JavaScript จะมีประสิทธิภาพ หากสามารถดัดแปลงคุณสมบัติขององค์ประกอบต่างๆ บนเว็บเพจ และสามารถรับรู้เหตุการณ์ที่ผู้ชมเว็บเพจโต้ตอบกับองค์ประกอบเหล่านั้นได้ เช่น การคลิกหรือเลื่อนเมาส์ ดังนั้นภาษา HTML รุ่นใหม่ๆ จึงมีการพัฒนาให้มีคุณสมบัติบางอย่างเพิ่มขึ้น และมีลักษณะเป็นวัตถุ (object) มากขึ้น การทำงานร่วมกันระหว่างคุณสมบัติใหม่ของ HTML กับ JavaScript ทำให้เกิดภาษาที่เรียกว่า Dynamic HTML คือภาษา HTML ที่สามารถสร้างเว็บเพจแบบพลวัตรได้นั่นเอง

นอกจากนี้ JavaScript ยังสามารถดัดแปลงคุณสมบัติของ CSS ได้เช่นกัน จึงช่วยให้เราปรับเปลี่ยนเว็บเพจได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 3
การออกแบบระบบ

3.1 การออกแบบการทดลอง

จากการศึกษาการทำงานของ IPv6 และการตั้งค่าอุปกรณ์ของ Cisco จึงทำให้ได้แนวคิดในการออกแบบการทดลองเพื่อทดสอบการเชื่อมต่อระหว่าง IPv4 และ IPv6 บนอุปกรณ์ของ Cisco ดังนี้

3.1.1 อุปกรณ์ที่ใช้ในการทดลอง

1) คอมพิวเตอร์ส่วนบุคคล (PC)
2) เราท์เตอร์ Cisco 3925
3) สวิตช์ Cisco Catalyst 2960
4) สาย UTP ที่เข้าหัวด้วยพอร์ท RJ45

3.1.2 ขั้นตอนการทดลอง

1) สำรวจความพร้อมของอุปกรณ์ที่ใช้ทดลอง ว่าระบบปฏิบัติการรองรับการใช้งาน IPv6 หรือไม่ หากไม่รองรับให้อัพเดทระบบปฏิบัติการให้เป็นรุ่นที่สูงกว่า
2) จำลองการเชื่อมต่อในเครือข่ายปิดเพื่อทดสอบโทโพโลยีแบบต่างๆ ดังนี้
   - แบบ Native IPv4
   - แบบ Native IPv6
   - แบบ Dual Stack
   - แบบ Manual Tunnel
   - แบบ GRE Tunnel (6over4)
   - แบบ GRE Tunnel (4over6)
   - แบบ Automatic 6to4 Tunnel
   - แบบ IPv4-Compatible IPv6 Tunnel (2 Routers)
   - แบบ IPv4-Compatible IPv6 Tunnel (3 Routers)
   - แบบ 6RD Tunnel
   - แบบ ISATAP Tunnel
3) ทดลองเชื่อมต่อไปยังเครือข่าย IPv6 ที่มีการใช้งานจริง
4) ใช้คำสั่ง Ping และ Trace Route เพื่อทดสอบการเชื่อมต่อแต่ละแบบ

3.1.3 ออกแบบการเชื่อมต่อในเครือข่ายแบบปิด

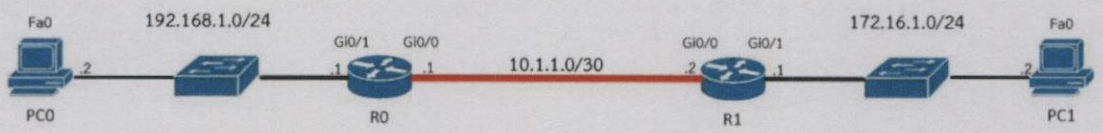
บนเราท์เตอร์ทุกตัว จะต้องเปิดโหมดการทำงานของ IPv6 โดยใช้คำสั่ง ipv6 unicast-routing

เส้นแสดงการเชื่อมต่อในรูปมีความหมายคือ เส้นสีดำหมายถึงเครือข่ายภายในองค์กร เส้นสีแดงหมายถึงเครือข่ายภายนอกองค์กร และเส้นสีฟ้าหมายถึงอุโมงค์สื่อสาร

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1) การเชื่อมต่อแบบ Native IPv4

การเชื่อมต่อแบบ Native IPv4 คือการเชื่อมต่อที่อุปกรณ์สื่อสารทั้งหมดโดยใช้โพรโทคอล IPv4 ในการสื่อสาร โดยออกแบบให้มีการเชื่อมต่ออุปกรณ์และการกำหนดค่าดังรูปที่ 3.1



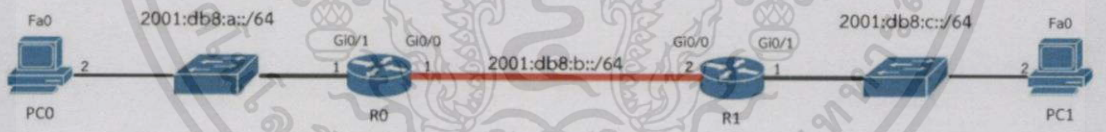
รูปที่ 3.1 การเชื่อมต่อแบบ Native IPv4

ตารางที่ 3.1 ตารางแสดงการตั้งค่าให้กับเราท์เตอร์เพื่อสร้างการเชื่อมต่อแบบ Native IPv4

R0	R1
! interface GigabitEthernet0/0 ip address 10.1.1.1 255.255.255.252 duplex auto speed auto ! interface GigabitEthernet0/1 ip address 192.168.1.1 255.255.255.0 duplex auto speed auto ! ip route 172.16.1.0 255.255.255.0 GigabitEthernet0/0	! interface GigabitEthernet0/0 ip address 10.1.1.2 255.255.255.252 duplex auto speed auto ! interface GigabitEthernet0/1 ip address 172.16.1.1 255.255.255.0 duplex auto speed auto ! ip route 192.168.1.0 255.255.255.0 GigabitEthernet0/0

2) การเชื่อมต่อแบบ Native IPv6

การเชื่อมต่อแบบ Native IPv6 คือการเชื่อมต่อที่อุปกรณ์สื่อสารทั้งหมดโดยใช้โพรโทคอล IPv6 ในการสื่อสาร โดยมีการเชื่อมต่ออุปกรณ์และมีการกำหนดค่าดังรูปที่ 3.2



รูปที่ 3.2 การเชื่อมต่อแบบ Native IPv6

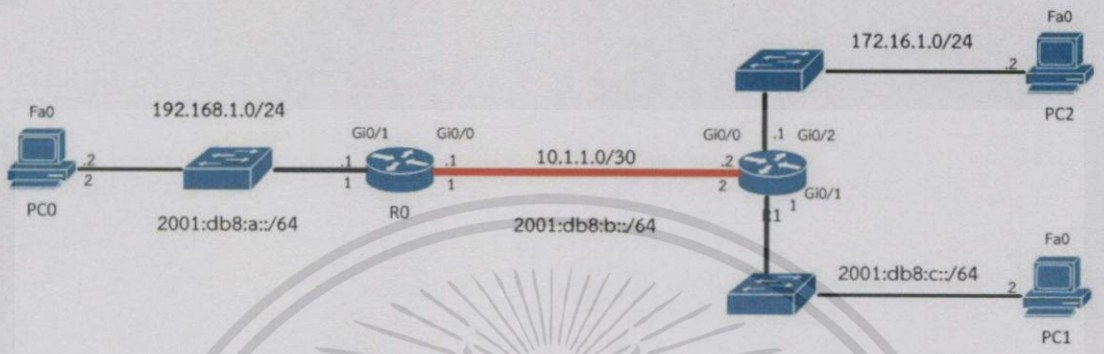
ตารางที่ 3.2 ตารางแสดงการตั้งค่าให้กับเราท์เตอร์เพื่อสร้างการเชื่อมต่อแบบ Native IPv6

R0	R1
! interface GigabitEthernet0/0 no ip address duplex auto speed auto ipv6 address 2001:DB8:B::1/64 ! interface GigabitEthernet0/1 no ip address duplex auto speed auto ipv6 address 2001:DB8:A::1/64 ! ipv6 route 2001:DB8:C::/64 2001:DB8:B::2	! interface GigabitEthernet0/0 no ip address duplex auto speed auto ipv6 address 2001:DB8:B::2/64 ! interface GigabitEthernet0/1 no ip address duplex auto speed auto ipv6 address 2001:DB8:C::1/64 ! ipv6 route 2001:DB8:A::/64 2001:DB8:B::1

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3) การเชื่อมต่อแบบ Dual Stack

การเชื่อมต่อแบบ Dual Stack คือการเชื่อมต่อที่อุปกรณ์สื่อสารสามารถรองรับการทำงานทั้งแบบ IPv4 และ IPv6 ในระบบเครือข่าย คือเมื่อใดที่มีการส่งแพ็กเก็ต IPv4 แพ็กเก็ตนั้นจะถูกส่งผ่าน IPv4 Stack และเมื่อมีการส่งแพ็กเก็ต IPv6 แพ็กเก็ตนั้นจะถูกส่งผ่าน IPv6 Stack โดยมีการเชื่อมต่ออุปกรณ์ดังรูปที่ 3.3



รูปที่ 3.3 การเชื่อมต่อแบบ Dual Stack

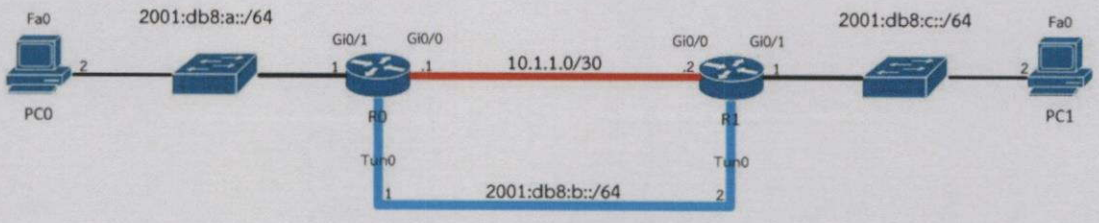
ตารางที่ 3.3 ตารางแสดงการตั้งค่าให้กับเราท์เตอร์เพื่อสร้างการเชื่อมต่อแบบ Dual Stack

R0	R1
! interface GigabitEthernet0/0 ip address 10.1.1.1 255.255.255.252 duplex auto speed auto ipv6 address 2001:DB8:B::1/64 ! interface GigabitEthernet0/1 ip address 192.168.1.1 255.255.255.0 duplex auto speed auto ipv6 address 2001:DB8:A::1/64 ! ip route 172.16.1.0 255.255.255.0 GigabitEthernet0/0 ! ipv6 route 2001:DB8:C::/64 2001:DB8:B::2	! interface GigabitEthernet0/0 ip address 10.1.1.2 255.255.255.0 duplex auto speed auto ipv6 address 2001:DB8:B::2/64 ! interface GigabitEthernet0/1 no ip address duplex auto speed auto ipv6 address 2001:DB8:C::1/64 ! interface GigabitEthernet0/2 ip address 172.16.1.1 255.255.255.0 duplex auto speed auto ! ip route 192.168.1.0 255.255.255.0 GigabitEthernet0/0 ! ipv6 route 2001:DB8:A::/64 2001:DB8:B::1

4) การเชื่อมต่อแบบ Manual Tunnel

การเชื่อมต่อแบบ Manual Tunnel คือการทำอุโมงค์สื่อสาร โดยให้แพ็กเก็ต IPv6 ถูกห่อหุ้มอยู่ภายในแพ็กเก็ต IPv4 แล้วจึงส่งแพ็กเก็ตออกไป ที่ปลายอุโมงค์สื่อสารเราท์เตอร์จะทำการแยกส่วนแพ็กเก็ต IPv6 ออกมาเพื่อส่งเข้าเกตเวย์ IPv6 และมีการเชื่อมต่ออุปกรณ์ดังรูปที่ 3.4

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



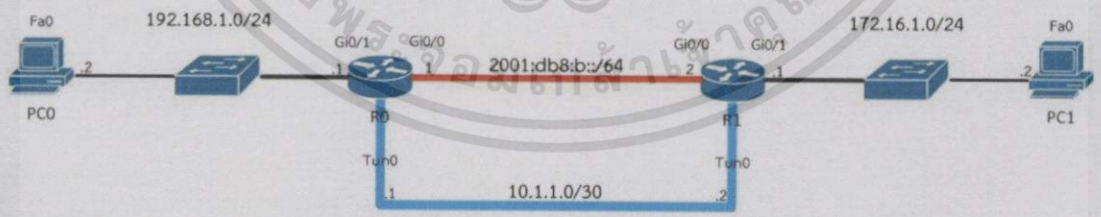
รูปที่ 3.4 การเชื่อมต่อแบบ Manual Tunnel

ตารางที่ 3.4 ตารางแสดงการตั้งค่าให้กับเราท์เตอร์เพื่อสร้างการเชื่อมต่อแบบ Manual Tunnel

R0	R1
! interface Tunnel0 no ip address ipv6 address 2001:DB8:B::1/64 tunnel source 10.1.1.1 tunnel mode ipv6ip tunnel destination 10.1.1.2 ! interface GigabitEthernet0/0 ip address 10.1.1.1 255.255.255.252 duplex auto speed auto ! interface GigabitEthernet0/1 no ip address duplex auto speed auto ipv6 address 2001:DB8:A::1/64 ! ipv6 route 2001:DB8:C::/64 2001:DB8:B::2	! interface Tunnel0 no ip address ipv6 address 2001:DB8:B::2/64 tunnel source 10.1.1.2 tunnel mode ipv6ip tunnel destination 10.1.1.1 ! interface GigabitEthernet0/0 ip address 10.1.1.2 255.255.255.252 duplex auto speed auto ! interface GigabitEthernet0/1 no ip address duplex auto speed auto ipv6 address 2001:DB8:C::2/64 ! ipv6 route 2001:DB8:A::/64 2001:DB8:B::1

5) การเชื่อมต่อแบบ GRE Tunnel (4over6)

การเชื่อมต่อแบบ GRE Tunnel คือการเชื่อมต่อแบบอุโมงค์สื่อสารซึ่งมีลักษณะคล้ายกับ Manual Tunnel แต่การกำหนดค่าแบบ GRE Tunnel สามารถกำหนดหมายเลขต้นทางและปลายทางเป็นได้ทั้ง IPv4 หรือ IPv6 และสามารถส่งโพรโทคอลในชั้นเครือข่ายใดๆ ก็ได้ ผ่านอุโมงค์สื่อสาร โดยมีการเชื่อมต่ออุปกรณ์ GRE Tunnel แบบ IPv4 อยู่ภายใน IPv6 ดังรูปที่ 3.5



รูปที่ 3.5 การเชื่อมต่อแบบ GRE Tunnel (4over6)

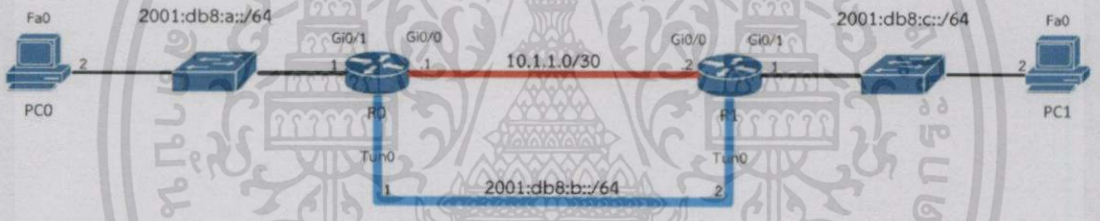
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 3.5 ตารางแสดงการตั้งค่าให้กับเราท์เตอร์เพื่อสร้างการเชื่อมต่อแบบ GRE Tunnel (4over6)

R0	R1
! interface Tunnel0 ip address 10.1.1.1 255.255.255.252 tunnel source 2001:DB8:B::1 tunnel mode gre ipv6 tunnel destination 2001:DB8:B::2 interface GigabitEthernet0/0 no ip address duplex auto speed auto ipv6 address 2001:DB8:B::1/64 ! interface GigabitEthernet0/1 ip address 192.168.1.1 255.255.255.0 duplex auto speed auto ! ip route 172.16.1.0 255.255.255.0 Tunnel0	! interface Tunnel0 ip address 10.1.1.2 255.255.255.252 tunnel source 2001:DB8:B::2 tunnel mode gre ipv6 tunnel destination 2001:DB8:B::1 ! interface GigabitEthernet0/0 no ip address duplex auto speed auto ipv6 address 2001:DB8:B::2/64 ! interface GigabitEthernet0/1 ip address 172.16.1.1 255.255.255.0 duplex auto speed auto ! ip route 192.168.1.0 255.255.255.0 Tunnel0

6) การเชื่อมต่อแบบ GRE Tunnel (6over4)

การเชื่อมต่อแบบ GRE Tunnel โดย IPv6 อยู่ภายใน IPv4 ดังรูปที่ 3.6



รูปที่ 3.6 การเชื่อมต่อแบบ GRE Tunnel (6over4)

ตารางที่ 3.6 ตารางแสดงการตั้งค่าให้กับเราท์เตอร์เพื่อสร้างการเชื่อมต่อแบบ GRE Tunnel (6over4)

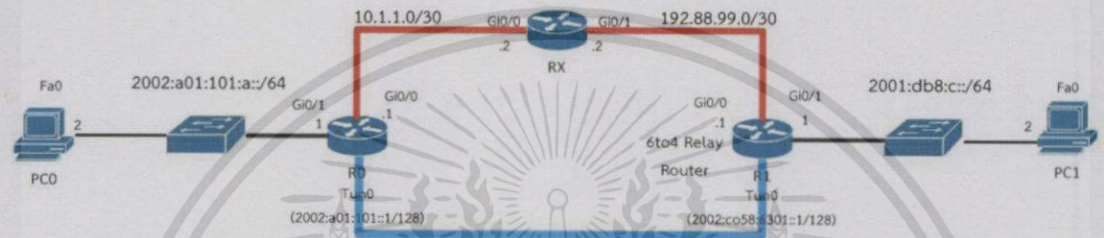
R0	R1
! interface Tunnel0 ipv6 address 2001:DB8:B::1/64 tunnel source 10.1.1.1 tunnel mode gre ipv6 tunnel destination 10.1.1.2 ! interface GigabitEthernet0/0 ip address 10.1.1.1 255.255.255.252 duplex auto speed auto ! interface GigabitEthernet0/1 no ip address duplex auto speed auto ipv6 address 2001:db8:a::1/64 ! ipv6 route 2001:db8:a::/64 Tunnel0	! interface Tunnel0 ipv6 address 2001:DB8:B::2/64 tunnel source 10.1.1.2 tunnel mode gre ipv6 tunnel destination 10.1.1.1 ! interface GigabitEthernet0/0 ip address 10.1.1.2 255.255.255.252 duplex auto speed auto ! interface GigabitEthernet0/1 no ip address duplex auto speed auto ipv6 address 2001:db8:c::1/64 ! ipv6 route 2001:db8:a::/64 Tunnel0

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

7) การเชื่อมต่อแบบ Automatic 6to4 Tunnel

การเชื่อมต่อแบบ Automatic 6to4 Tunnel คือการเชื่อมต่อแบบอุโมงค์สื่อสาร ซึ่งมีลักษณะคล้ายกับ Manual Tunnel แต่ไม่ต้องกำหนดหมายเลขที่อยู่ปลายทางของอุโมงค์สื่อสาร เหมาะสำหรับเราท์เตอร์ที่อยู่ขอบนอกขององค์กร (Border Router) เพราะต้องใช้หมายเลขที่อยู่ Public IPv4 ในการสร้างอุโมงค์สื่อสาร โดยต้องมี รีเลย์เราท์เตอร์ (Relay Router)

รีเลย์เราท์เตอร์ ทำหน้าที่เชื่อมต่อระหว่างระบบเครือข่ายที่ใช้หมายเลข IPv6 แบบ 6to4 และระบบเครือข่ายที่ใช้หมายเลข IPv6 แบบ Native รีเลย์เราท์เตอร์จะถอดแพ็กเก็ต IPv6 ออกจากแพ็กเก็ต IPv4 เพื่อส่งแพ็กเก็ตไปยังเครือข่าย IPv6 ปลายทาง และมีการเชื่อมต่อดังรูปที่ 3.7 โดยเราท์เตอร์ R1 ทำหน้าที่เป็นรีเลย์เราท์เตอร์



รูปที่ 3.7 การเชื่อมต่อแบบ Automatic 6to4 Tunnel

ตารางที่ 3.7 ตารางแสดงการตั้งค่าให้กับเราท์เตอร์เพื่อสร้างการเชื่อมต่อแบบ Automatic 6to4 Tunnel

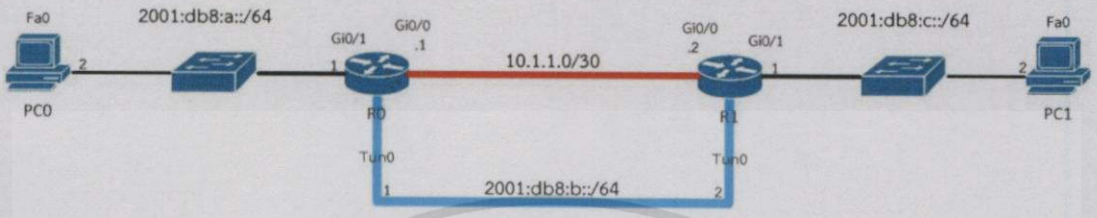
R0	R1
! interface Tunnel0 no ip address no ip redirects ipv6 address 2002:A01:101::1/128 tunnel source 10.1.1.1 tunnel mode ipv6ip 6to4 ! interface GigabitEthernet0/0 ip address 10.1.1.1 255.255.255.252 duplex auto speed auto ! interface GigabitEthernet0/1 no ip address duplex auto speed auto ipv6 address 2002:A01:101:A::1/64 ! ip route 192.88.99.0 255.255.255.252 GigabitEthernet0/0 ! ipv6 route ::/0 Tunnel0 2002:C058:6301::	! interface Tunnel0 no ip address no ip redirects ipv6 address 2002:C058:6301::/128 anycast tunnel source 192.88.99.1 tunnel mode ipv6ip 6to4 ! interface GigabitEthernet0/0 ip address 192.88.99.1 255.255.255.252 duplex auto speed auto ! interface GigabitEthernet0/1 no ip address duplex auto speed auto ipv6 address 2001:DB8:C::1/64 ! ip route 10.1.1.0 255.255.255.252 GigabitEthernet0/0 ! ipv6 route 2002::/16 Tunnel0

RX
! interface GigabitEthernet0/0 ip address 10.1.1.2 255.255.255.252 duplex auto speed auto ! interface GigabitEthernet0/1 ip address 192.88.99.2 255.255.255.252 duplex auto speed auto

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

8) การเชื่อมต่อแบบ IPv4-Compatible IPv6 Tunnel (2 Routers)

การเชื่อมต่อแบบ IPv4-Compatible IPv6 Tunnel คือการเชื่อมต่อแบบอุโมงค์สื่อสารซึ่งมีลักษณะคล้ายกับการเชื่อมต่อแบบ Automatic 6to4 Tunnel แต่มีกำหนดหมายเลขที่อยู่ต้นทางและปลายทางโดยใช้หลักการแบบ IPv4-Compatible IPv6 (ตามที่อธิบายไว้ในหัวข้อที่ 2.1.3.6) และมีการเชื่อมต่อดังรูปที่ 3.8



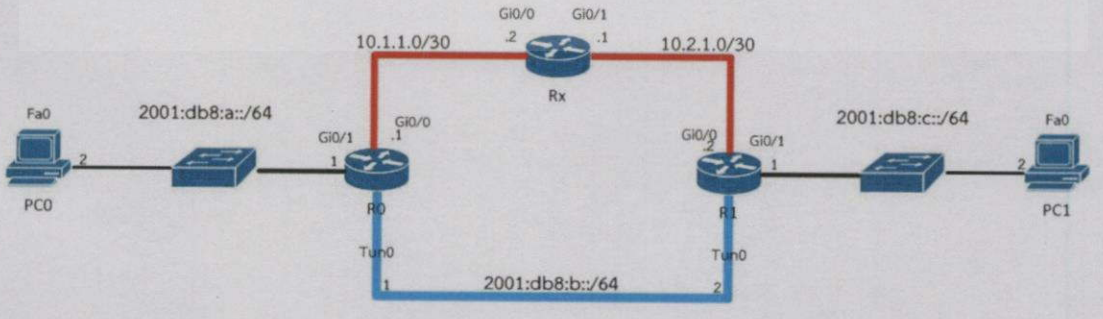
รูปที่ 3.8 การเชื่อมต่อแบบ IPv4-Compatible IPv6 Tunnel (2 Routers)

ตารางที่ 3.8 ตารางแสดงการตั้งค่าให้กับเราท์เตอร์เพื่อสร้างการเชื่อมต่อแบบ IPv4-Compatible IPv6 Tunnel (2 Routers)

R0	R1
! interface Tunnel0 no ip address no ip redirects ipv6 enable tunnel source GigabitEthernet0/0 tunnel mode ipv6ip auto-tunnel ! interface GigabitEthernet0/0 ip address 10.1.1.1 255.255.255.252 duplex auto speed auto ! interface GigabitEthernet0/1 no ip address duplex auto speed auto ipv6 address 2001:DB8:A::1/64 ! ipv6 route ::/0 ::10.1.1.2	! interface Tunnel0 no ip address no ip redirects ipv6 enable tunnel source GigabitEthernet0/0 tunnel mode ipv6ip auto-tunnel ! interface GigabitEthernet0/0 ip address 10.1.1.2 255.255.255.252 duplex auto speed auto ! interface GigabitEthernet0/1 no ip address duplex auto speed auto ipv6 address 2001:DB8:C::1/64 ! ipv6 route ::/0 ::10.1.1.1

9) การเชื่อมต่อแบบ IPv4-Compatible IPv6 Tunnel (3 Routers)

การเชื่อมต่อแบบ IPv4-Compatible IPv6 Tunnel แบบ (3 Routers)



รูปที่ 3.9 การเชื่อมต่อแบบ IPv4-Compatible IPv6 Tunnel (3 Routers)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 3.9 ตารางแสดงการตั้งค่าให้กับเราท์เตอร์เพื่อสร้างการเชื่อมต่อแบบ IPv4-Compatible IPv6 Tunnel (3 Routers)

R0	R1
! interface Tunnel0 no ip address no ip redirects ipv6 enable tunnel source GigabitEthernet0/0 tunnel mode ipv6ip auto-tunnel ! interface GigabitEthernet0/0 ip address 10.1.1.1 255.255.255.252 duplex auto speed auto ! interface GigabitEthernet0/1 no ip address duplex auto speed auto ipv6 address 2001:DB8:A::1/64 ! ip route 10.2.1.0 255.255.255.252 GigabitEthernet0/0 ! ipv6 route ::/0 ::10.2.1.2	! interface Tunnel0 no ip address no ip redirects ipv6 enable tunnel source GigabitEthernet0/0 tunnel mode ipv6ip auto-tunnel ! interface GigabitEthernet0/0 ip address 10.2.1.2 255.255.255.252 duplex auto speed auto ! interface GigabitEthernet0/1 no ip address duplex auto speed auto ipv6 address 2001:DB8:C::1/64 ! ip route 10.1.1.0 255.255.255.252 GigabitEthernet0/0 ! ipv6 route ::/0 ::10.1.1.1

RX
! interface GigabitEthernet0/0 ip address 10.1.1.2 255.255.255.252 duplex auto speed auto ! interface GigabitEthernet0/1 ip address 10.2.1.1 255.255.255.252 duplex auto speed auto

10) การเชื่อมต่อแบบ 6RD Tunnel

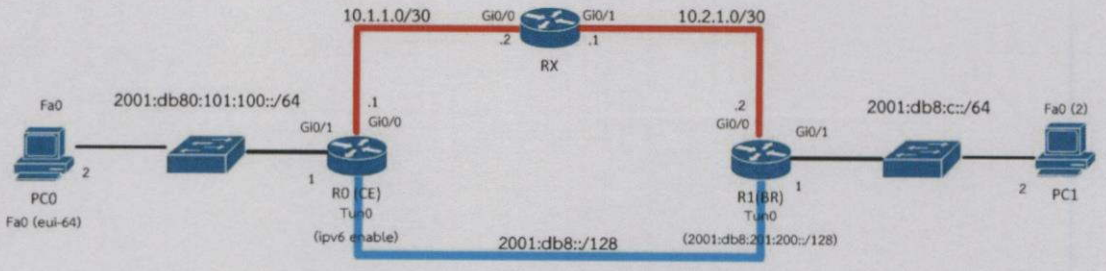
การเชื่อมต่อแบบ 6RD คืออุโมงค์สื่อสารซึ่งมีลักษณะการเชื่อมต่อที่เหมาะสำหรับสร้างการเชื่อมต่อภายในเครือข่ายของผู้ให้บริการอินเทอร์เน็ตที่มีเครือข่ายภายในเป็นเครือข่าย IPv4 ทั้งหมด โดยหมายเลขเครือข่ายส่วนหน้าจะถูกกำหนดให้โดยผู้ให้บริการอินเทอร์เน็ต และเมื่อเราท์เตอร์ของผู้ใช้บริการได้รับหมายเลขที่อยู่ IPv4 จะนำหมายเลข IPv4 นั้นมาเพิ่มหลังหมายเลขหมายเลขเครือข่ายส่วนหน้า ซึ่งส่วนของหมายเลขที่อยู่ IPv4 ที่นำมาใช้จะเป็นส่วนที่เหลือจากการประกาศความยาวส่วนหน้าของ IPv4 ในการตั้งค่าอุโมงค์ โดยมีการเชื่อมต่อดังรูปที่ 3.11

n bits	x bits	m bits	128-n-x-m bit
6rd prefix	IPv4 prefix	Subnet ID	Interface ID

รูปที่ 3.10 โครงสร้างหมายเลข IPv6 แบบ 6RD

โดย n บิตแรกได้รับจากผู้ให้บริการอินเทอร์เน็ต และ x บิตถัดมาเป็นหมายเลขที่อยู่ IPv4 ในรูปแบบเลขฐานสิบหก เช่น 10.2.1.2 เมื่อกำหนดหมายเลขส่วนหน้าเป็น 8 (tunnel 6rd ipv4 prefix-len 8) จะใช้เฉพาะส่วน 3 ไบต์หลังคือ 2.1.2 ซึ่งเขียนในรูปแบบของหมายเลขที่อยู่ IPv6 ได้เป็น 202:200

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.11 การเชื่อมต่อแบบ 6RD Tunnel

ตารางที่ 3.10 ตารางแสดงการตั้งค่าให้กับเราท์เตอร์เพื่อสร้างการเชื่อมต่อแบบ 6RD Tunnel

R0	R1
ipv6 general-prefix pre6rd 6rd Tunnel0 ! interface Tunnel0 no ip address no ip redirects ipv6 enable tunnel source 10.1.1.1 tunnel mode ipv6ip 6rd tunnel 6rd ipv4 prefix-len 8 tunnel 6rd prefix 2001:DB8::/32 tunnel 6rd br 10.2.1.2 ! interface GigabitEthernet0/0 ip address 10.1.1.1 255.255.255.252 duplex auto speed auto ! interface GigabitEthernet0/1 no ip address duplex auto speed auto ipv6 address pre6rd ::/64 eui-64 ! ip route 10.2.1.0 255.255.255.252 GigabitEthernet0/0 ! ipv6 route ::/0 Tunnel0 2001:DB8:201:200::	ipv6 general-prefix pre6rd 6rd Tunnel0 ! interface Tunnel0 no ip address no ip redirects ipv6 address pre6rd ::/128 anycast tunnel source 10.2.1.2 tunnel mode ipv6ip 6rd tunnel 6rd ipv4 prefix-len 8 tunnel 6rd prefix 2001:DB8::/32 ! interface GigabitEthernet0/0 ip address 10.2.1.2 255.255.255.252 duplex auto speed auto ! interface GigabitEthernet0/1 no ip address duplex auto speed auto ipv6 address 2001:DB8:C::1/64 ! ! ip route 10.1.1.0 255.255.255.252 GigabitEthernet0/0 ! ipv6 route 2001:DB8:101:100::/64 Tunnel0

RX
! interface GigabitEthernet0/0 ip address 10.1.1.2 255.255.255.252 duplex auto speed auto ! interface GigabitEthernet0/1 ip address 10.2.1.1 255.255.255.252 duplex auto speed auto

11) การเชื่อมต่อแบบ ISATAP Tunnel

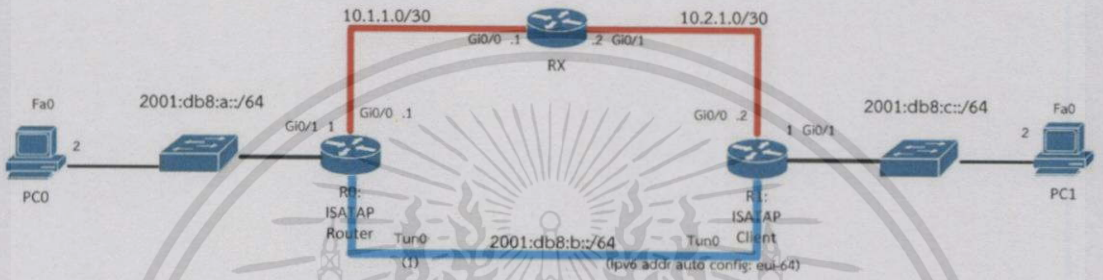
การเชื่อมต่อแบบ ISATAP คืออุโมงค์สื่อสารซึ่งมีลักษณะการเชื่อมต่อคล้ายกับ Manual Tunnel แต่ใช้งานได้ภายในองค์กรเท่านั้น และมีการกำหนดค่าเพิ่มเติมที่เราท์เตอร์ของ ISATAP ทำให้เราท์เตอร์ลูกข่ายของ ISATAP ได้รับหมายเลขที่อยู่แบบอัตโนมัติ โดยมีการเชื่อมต่อดังรูปที่ 3.13

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

48 bits	16 bits	32 bits	32 bits
หมายเลขเครือข่ายส่วนหน้าขององค์กร	Subnet ID	0000:0000	IPv4 Address

รูปที่ 3.12 โครงสร้างหมายเลข IPv6 แบบ ISATAP

โดย 48 บิตแรกเป็นหมายเลขเครือข่ายส่วนหน้าขององค์กรที่ได้มาจาก ISP และ 16 บิตถัดมาเป็นหมายเลขเครือข่ายย่อย เช่น 10:2:1:2 เมื่อกำหนดหมายเลขเครือข่ายส่วนหน้าเป็น 2001:db8:b::/64 จะได้หมายเลขที่อยู่ IPv6 คือ 2001:DB8:B::A02:102



รูปที่ 3.13 การเชื่อมต่อแบบ ISATAP Tunnel

ตารางที่ 3.11 ตารางแสดงการตั้งค่าให้กับเราท์เตอร์เพื่อสร้างการเชื่อมต่อแบบ ISATAP Tunnel

R0	R1
! interface Tunnel0 no ip address no ip redirects ipv6 address 2001:DB8:B::1/64 no ipv6 nd ra suppress tunnel source 10.1.1.1 tunnel mode ipv6ip isatap ! interface GigabitEthernet0/0 ip address 10.1.1.1 255.255.255.252 duplex auto speed auto ! interface GigabitEthernet0/1 no ip address duplex auto speed auto ipv6 address 2001:DB8:A::1/64 ! ip route 10.2.1.0 255.255.255.252 GigabitEthernet0/0 ! ipv6 route 2001:DB8:C::/64 2001:DB8:B::A02:102	! interface Tunnel0 no ip address ipv6 address autoconfig ipv6 enable tunnel source 10.2.1.2 tunnel mode ipv6ip tunnel destination 10.1.1.1 ! interface GigabitEthernet0/0 ip address 10.2.1.2 255.255.255.252 duplex auto speed auto ! interface GigabitEthernet0/1 no ip address duplex auto speed auto ipv6 address 2001:DB8:C::1/64 ! ip route 10.1.1.0 255.255.255.252 GigabitEthernet0/0 ! ipv6 route ::/0 Tunnel0

RX
! interface GigabitEthernet0/0 ip address 10.1.1.2 255.255.255.252 duplex auto speed auto ! interface GigabitEthernet0/1 ip address 10.2.1.1 255.255.255.252 duplex auto speed auto

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.2 ขั้นตอนการออกแบบคู่มือการตั้งค่า IPv6

3.2.1 ออกแบบรูปแบบเว็บเพจ

ใช้โปรแกรมประเภทกราฟฟิกและรูปภาพในการออกแบบส่วนหน้าเว็บเพจตามแบบที่ต้องการ ได้แก่ โปรแกรมอะโดบี โฟโต้ช็อป (Adobe Photoshop CC) โดยโครงสร้างของหน้าจะแบ่งได้เป็น 4 ส่วน ได้แก่

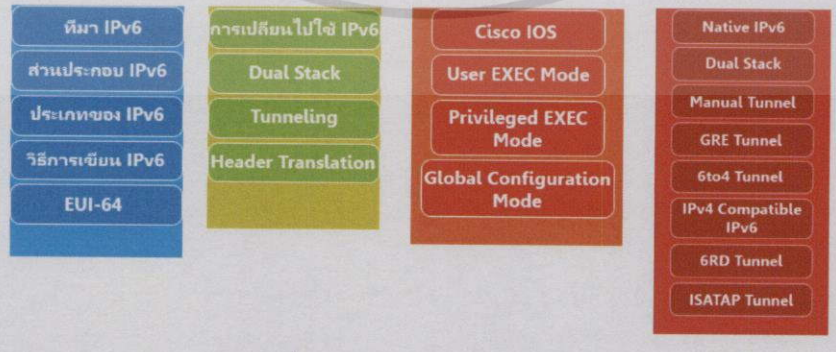
1) ส่วนหัว หรือ Top มีเมนูย่อย ได้แก่ Home และ Contact us

รูปที่ 3.14 ส่วนหัวของเว็บเพจ

2) ส่วนซ้าย หรือ Left เป็นส่วนของเมนูหลัก ได้แก่ IPv6, IPv4 & IPv6 Technical, Cisco IOS และ Connection & Configuration เมื่อคลิกเข้าไป เมนูย่อยในส่วนทางด้านขวาจะเปลี่ยนไปตามหัวข้อต่างๆ

รูปที่ 3.15 ส่วนซ้ายของเว็บเพจ

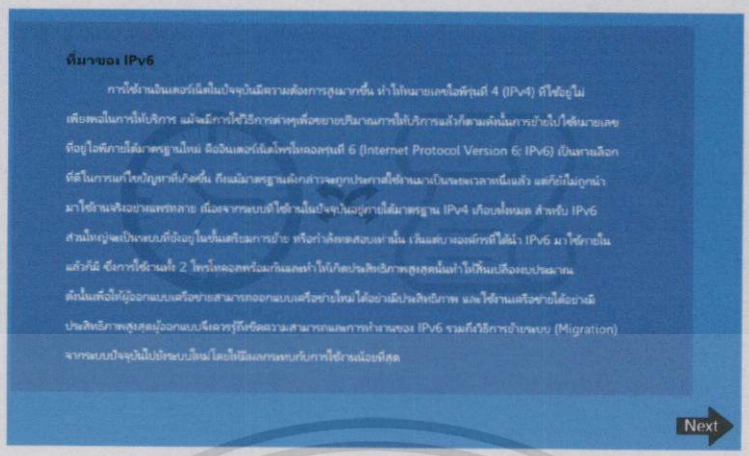
3) ส่วนขวา หรือ Right เป็นเมนูย่อยของส่วนทางด้านซ้าย



รูปที่ 3.16 ส่วนขวาของเว็บเพจ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4) ส่วนกลาง หรือ Center คือส่วนที่แสดงเนื้อหารายละเอียดของหัวข้อต่างๆ



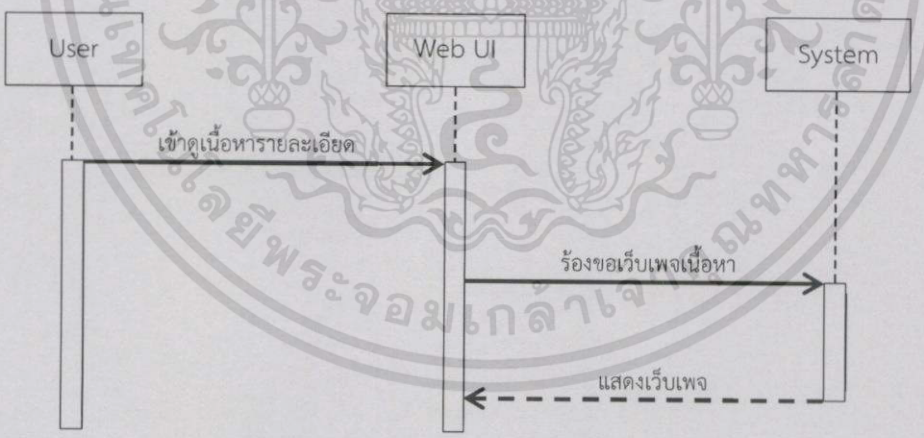
รูปที่ 3.17 ส่วนกลางของเว็บเพจ

นำเว็บเพจที่ได้จากการออกแบบมาใส่ข้อมูล, รายละเอียดและเนื้อหาต่างๆ ในแต่ละหัวข้อ ตกแต่งรูปแบบภายในเว็บเพจด้วย CSS และสร้างการเชื่อมโยงเว็บเพจ HTML และ PHP โดยใช้โปรแกรมอะโดบีดรีมวีฟเวอร์ (Adobe Dreamwaever CS6)

3.2.2 แผนภาพการทำงานของเว็บไซต์ (Sequence Diagram)

1) แผนภาพการดูเนื้อหาของเว็บไซต์

รูปที่ 3.2 แสดงการทำงานของระบบเมื่อมี User เข้ามาใช้งาน

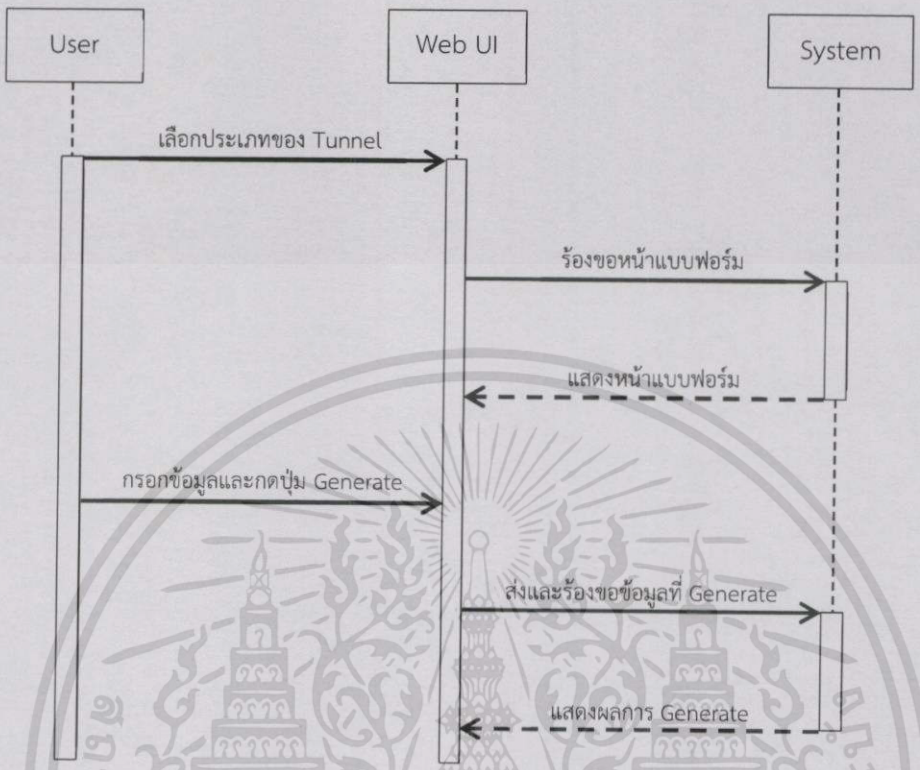


รูปที่ 3.18 แผนภาพแสดงการทำงานของเว็บไซต์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2) แผนภาพการใช้งานตัวช่วยตั้งค่า IPv6 Tunnel

รูปที่ 3.7 แสดงการทำงานเมื่อมี User เข้าไปหน้าเว็บเพจตัวช่วยตั้งค่า IPv6 Tunnel



รูปที่ 3.19 แผนภาพแสดงการใช้งานตัวช่วยตั้งค่า IPv6 Tunnel

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 4
ผลการดำเนินงาน

ในบทนี้จะกล่าวถึงผลการเชื่อมต่อระบบเครือข่าย ทั้งการจำลองการเชื่อมต่อในระบบปิดและการเชื่อมต่อไปยังเครือข่าย IPv6 ที่มีการใช้งานจริง รวมไปถึงผลที่ได้จากการเชื่อมต่อระบบโดยผลที่ได้แสดงให้เห็นการสื่อสารภายใต้ทั้ง 2 โพรโทคอล คือทั้ง IPv4 และ IPv6 ในโทโพโลยีแบบต่างๆ อีกทั้งยังมีการจัดทำเว็บไซต์เพื่อให้ความรู้เกี่ยวกับ IPv6 อีกด้วย

4.1 ผลการจำลองการเชื่อมต่อเครือข่าย

การจำลองการเชื่อมต่อเครือข่ายเป็นการจำลองการเชื่อมต่อเครือข่ายที่สมมติขึ้น โดยใช้อุปกรณ์ที่มีอยู่แล้วจำลองการเชื่อมต่อ เพื่อทดสอบโทโพโลยีแบบต่างๆ ดังนี้

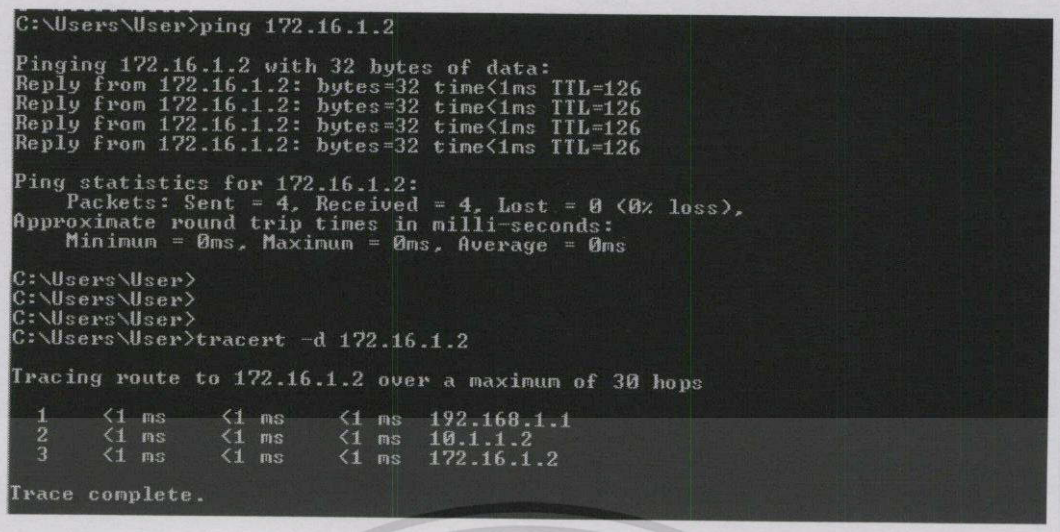
1. แบบ Native IPv4
2. แบบ Native IPv6
3. แบบ Dual Stack
4. แบบ Manual Tunnel
5. แบบ GRE Tunnel (6over4)
6. แบบ GRE Tunnel (4over6)
7. แบบ Automatic 6to4 Tunnel
8. แบบ IPv4-Compatible IPv6 Tunnel (2 Routers)
9. แบบ IPv4-Compatible IPv6 Tunnel (3 Routers)
10. แบบ 6RD Tunnel
11. แบบ ISATAP Tunnel

เมื่อมีการกำหนดค่าหมายเลขที่อยู่และค่าพารามิเตอร์ต่างๆ ให้แก่โพรโตคอลอุโมงค์สื่อสารให้กับเราท์เตอร์ จะทำให้อุปกรณ์สื่อสารที่อยู่ในระบบเครือข่ายต้นทางสามารถสื่อสารกับอุปกรณ์สื่อสารที่ติดตั้งอยู่ในระบบเครือข่ายปลายทางได้ โดยสามารถทดสอบได้จากการใช้คำสั่ง Ping จากคอมพิวเตอร์เครื่องหนึ่ง (PC0) ในระบบเครือข่ายต้นทางไปยังคอมพิวเตอร์อีกเครื่องหนึ่ง (PC1) ในระบบเครือข่ายปลายทาง

4.1.1 การเชื่อมต่อแบบ Native IPv4

มีการเชื่อมต่อและตั้งค่าโดยอ้างอิงจากรูปที่ 3.1 และตารางที่ 3.1 ได้ผลการทดสอบการเชื่อมต่อดังรูปที่ 4.1

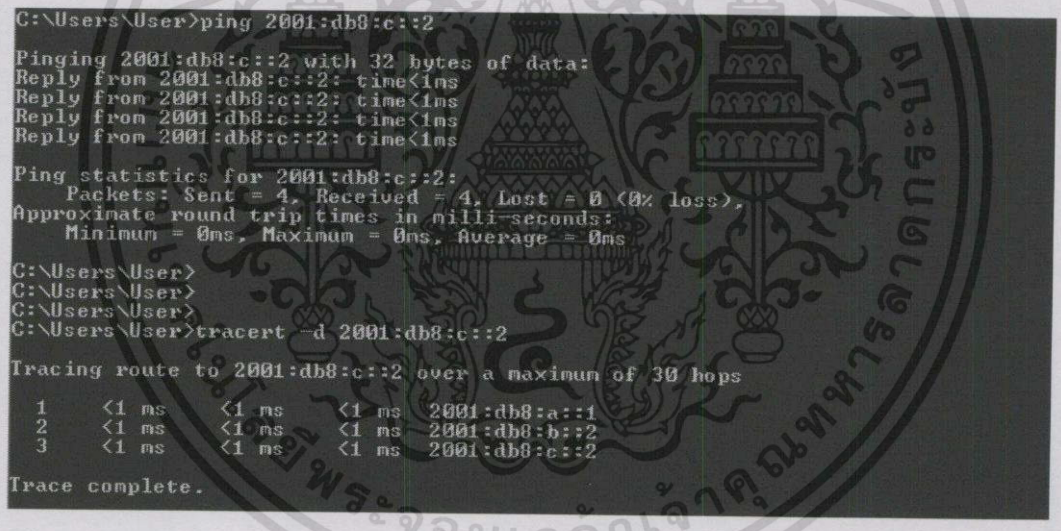
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.1 ผลการทดสอบการ Ping และแสดงเส้นทางการสื่อสารบนโทโพโลยีแบบ Native IPv4

4.1.2 การเชื่อมต่อแบบ Native IPv6

มีการเชื่อมต่อและตั้งค่าโดยอ้างอิงจากรูปที่ 3.2 และตารางที่ 3.2 ได้ผลการทดสอบการเชื่อมต่อดังรูปที่ 4.2

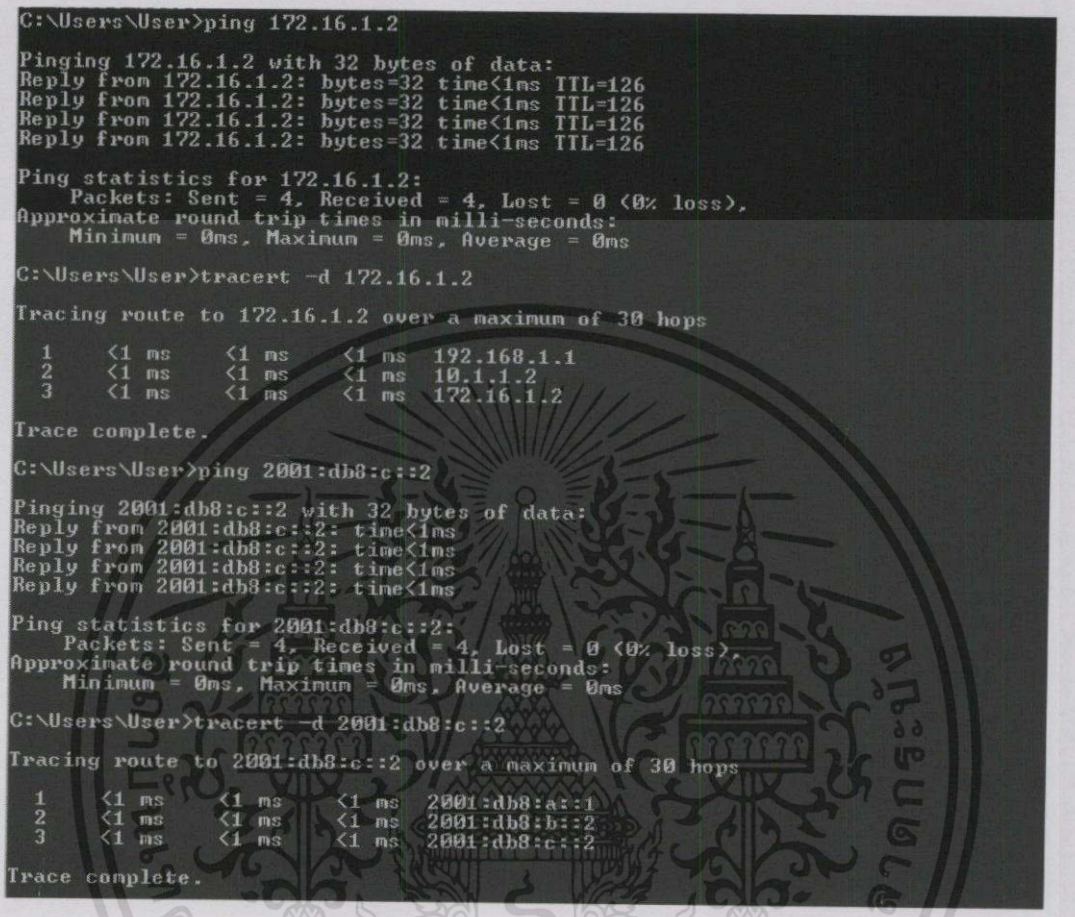


รูปที่ 4.2 ผลการทดสอบการ Ping และแสดงเส้นทางการสื่อสารบนโทโพโลยีแบบ Native IPv6

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.1.3 การเชื่อมต่อแบบ Dual Stack

มีการเชื่อมต่อและตั้งค่าโดยอ้างอิงจากรูปที่ 3.3 และตารางที่ 3.3 ได้ผลการทดสอบการเชื่อมต่อดังรูปที่ 4.3

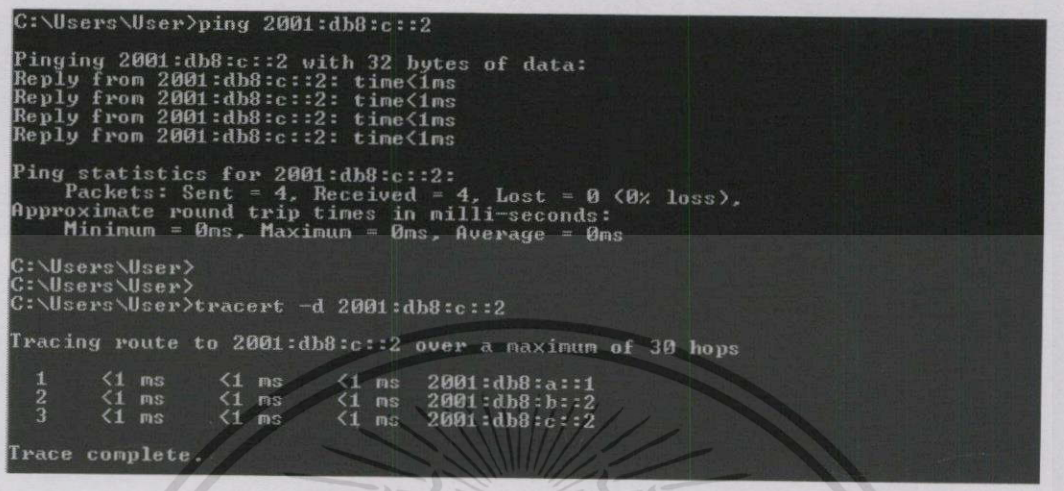


รูปที่ 4.3 ผลการทดสอบการ Ping และแสดงเส้นทางการสื่อสารบนโทโพโลยีแบบ Dual Stack

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.1.4 การเชื่อมต่อแบบ Manual Tunnel

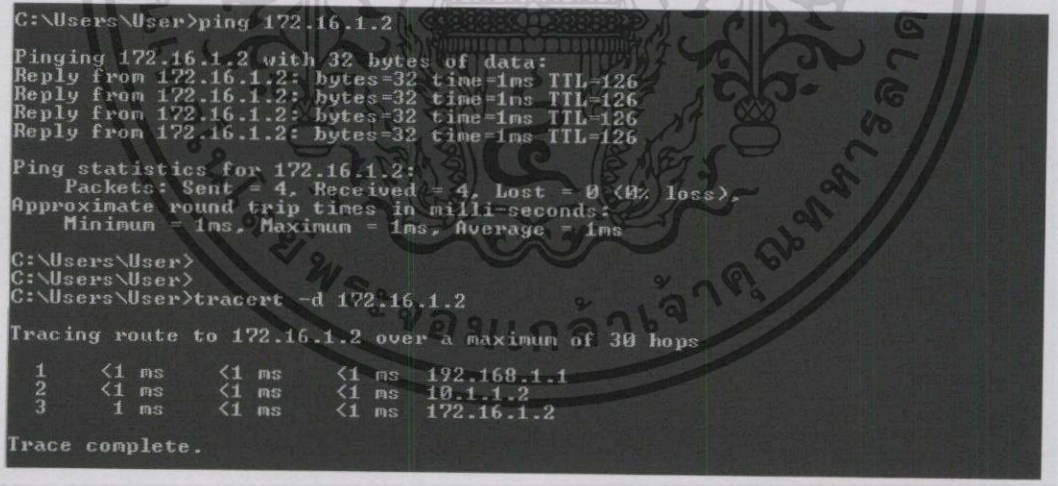
มีการเชื่อมต่อและตั้งค่าโดยอ้างอิงจากรูปที่ 3.4 และตารางที่ 3.4 ได้ผลการทดสอบการเชื่อมต่อดังรูปที่ 4.4



รูปที่ 4.4 ผลการทดสอบการ Ping และแสดงเส้นทางการสื่อสารบนโทโพโลยีแบบ Manual Tunnel

4.1.5 การเชื่อมต่อแบบ GRE Tunnel (4over6)

มีการเชื่อมต่อและตั้งค่าโดยอ้างอิงจากรูปที่ 3.5 และตารางที่ 3.5 ได้ผลการทดสอบการเชื่อมต่อดังรูปที่ 4.5

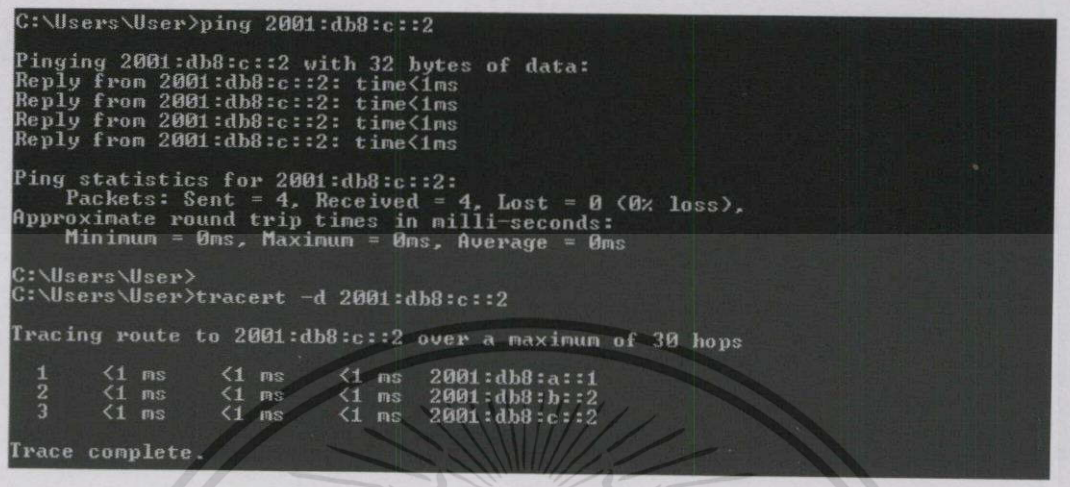


รูปที่ 4.5 ผลการทดสอบการ Ping และแสดงเส้นทางการสื่อสารบนโทโพโลยีแบบ GRE Tunnel (4over6)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.1.6 การเชื่อมต่อแบบ GRE Tunnel (6over4)

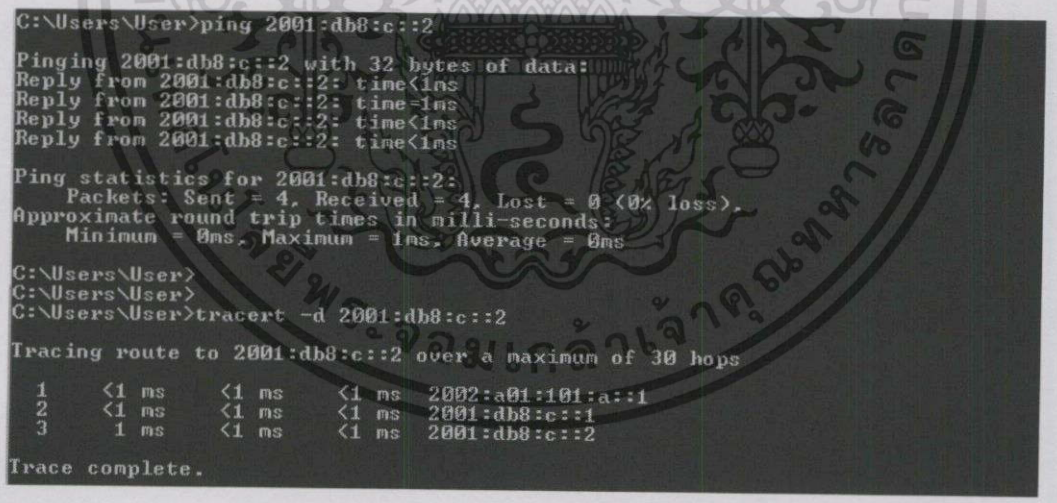
มีการเชื่อมต่อและตั้งค่าโดยอ้างอิงจากรูปที่ 3.6 และตารางที่ 3.6 ได้ผลการทดสอบการเชื่อมต่อดังรูปที่ 4.6



รูปที่ 4.6 ผลการทดสอบการ Ping และแสดงเส้นทางการสื่อสารบนโทโพโลยีแบบ GRE Tunnel (6over4)

4.1.7 การเชื่อมต่อแบบ Automatic 6to4 Tunnel

มีการเชื่อมต่อและตั้งค่าโดยอ้างอิงจากรูปที่ 3.7 และตารางที่ 3.7 ได้ผลการทดสอบการเชื่อมต่อดังรูปที่ 4.7

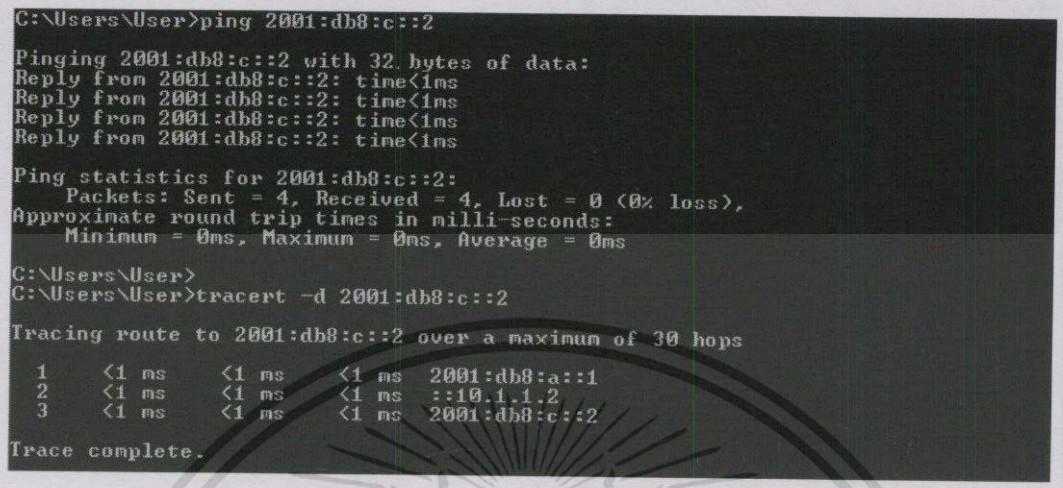


รูปที่ 4.7 ผลการทดสอบการ Ping และแสดงเส้นทางการสื่อสารบนโทโพโลยีแบบ Automatic 6to4 Tunnel

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.1.8 การเชื่อมต่อแบบ IPv4-Compatible IPv6 Tunnel (2 Router)

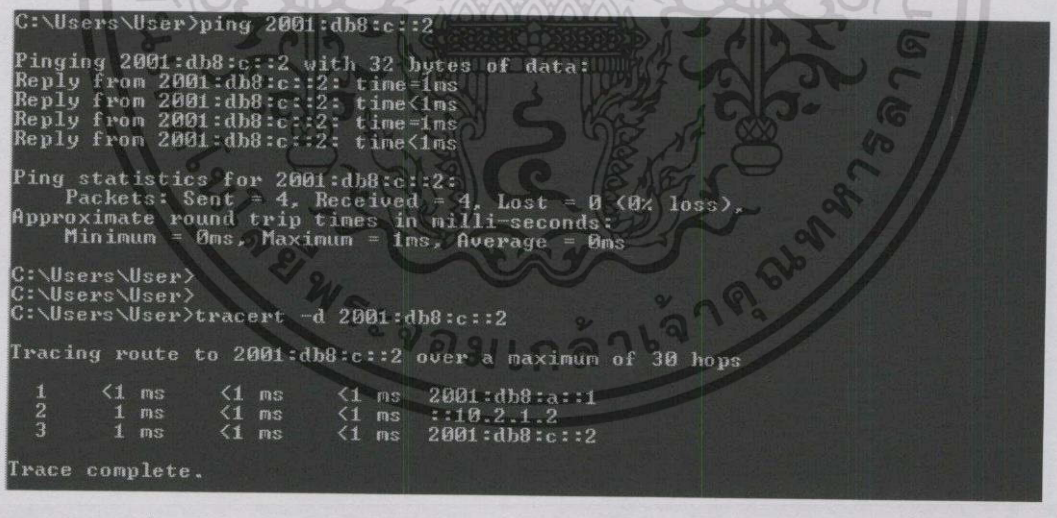
มีการเชื่อมต่อและตั้งค่าโดยอ้างอิงจากรูปที่ 3.8 และตารางที่ 3.8 ได้ผลการทดสอบการเชื่อมต่อดังรูปที่ 4.8



รูปที่ 4.8 ผลการทดสอบการ Ping และแสดงเส้นทางการสื่อสารบนโทโพโลยีแบบ IPv4-Compatible IPv6 Tunnel (2 Router)

4.1.9 การเชื่อมต่อแบบ IPv4-Compatible IPv6 Tunnel (3 Router)

มีการเชื่อมต่อและตั้งค่าโดยอ้างอิงจากรูปที่ 3.9 และตารางที่ 3.9 ได้ผลการทดสอบการเชื่อมต่อดังรูปที่ 4.9



รูปที่ 4.9 ผลการทดสอบการ Ping และแสดงเส้นทางการสื่อสารบนโทโพโลยีแบบ IPv4-Compatible IPv6 Tunnel (3 Router)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.1.10 การเชื่อมต่อแบบ 6RD Tunnel

มีการเชื่อมต่อและตั้งค่าโดยอ้างอิงจากรูปที่ 3.10 และตารางที่ 3.10 ได้ผลการทดสอบการเชื่อมต่อดังรูปที่ 4.10

```
C:\Users\User>ping 2001:db8:c::2

Pinging 2001:db8:c::2 with 32 bytes of data:
Reply from 2001:db8:c::2: time=1ms
Reply from 2001:db8:c::2: time<1ms
Reply from 2001:db8:c::2: time=1ms
Reply from 2001:db8:c::2: time=1ms

Ping statistics for 2001:db8:c::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\User>
C:\Users\User>tracert -d 2001:db8:c::2

Tracing route to 2001:db8:c::2 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  2001:db8:101:100:aef2:c5ff:fe49:5481
  2    <1 ms    <1 ms    <1 ms  2001:db8:c::1
  3     1 ms    <1 ms    <1 ms  2001:db8:c::2

Trace complete.
```

รูปที่ 4.10 ผลการทดสอบการ Ping และแสดงเส้นทางการสื่อสารบนโทโพโลยีแบบ 6RD Tunnel

4.1.11 การเชื่อมต่อแบบ ISATAP Tunnel

มีการเชื่อมต่อและตั้งค่าโดยอ้างอิงจากรูปที่ 3.11 และตารางที่ 3.11 ได้ผลการทดสอบการเชื่อมต่อดังรูปที่ 4.11

```
C:\Users\User>ping 2001:db8:c::2

Pinging 2001:db8:c::2 with 32 bytes of data:
Reply from 2001:db8:c::2: time=1ms
Reply from 2001:db8:c::2: time<1ms
Reply from 2001:db8:c::2: time=1ms
Reply from 2001:db8:c::2: time=1ms

Ping statistics for 2001:db8:c::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\User>
C:\Users\User>
C:\Users\User>tracert -d 2001:db8:c::2

Tracing route to 2001:db8:c::2 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  2001:db8:a::1
  2    <1 ms    <1 ms    <1 ms  2001:db8:b::a02:102
  3     1 ms    <1 ms     1 ms  2001:db8:c::2

Trace complete.
```

รูปที่ 4.11 ผลการทดสอบการ Ping และแสดงเส้นทางการสื่อสารบนโทโพโลยีแบบ ISATAP Tunnel

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.2 การทดสอบการเชื่อมต่อไปยังเครือข่าย IPv6 ที่มีการใช้งานจริง

การเชื่อมต่อไปยังเครือข่าย IPv6 ที่มีการใช้งานจริงมีข้อจำกัดค่อนข้างมาก เนื่องจากระบบส่วนใหญ่ยังคงเป็นระบบที่อยู่ในระหว่างการทดสอบ หรือหากเป็นระบบที่มีการใช้งานแล้ว ก็มักจะเป็นระบบที่มีการใช้งานเชิงธุรกิจซึ่งไม่เปิดโอกาสให้ทำการทดสอบการเชื่อมต่อ อีกทั้งเครือข่ายที่เปิดให้มีการทดสอบการเชื่อมต่อมักใช้อุโมงค์สื่อสารที่เป็นที่นิยม จึงทำให้มีตัวอย่างการเชื่อมต่อไม่มากนัก โดยการเชื่อมต่อที่ทดสอบเป็นการเชื่อมต่อผ่าน Tunnel Broker ของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (National Electronics and Computer Technology Center) หรือ เนคเทค (NECTEC)

4.2.1 การเชื่อมต่อโดยสร้างอินเตอร์เฟสจำลองในเครื่องคอมพิวเตอร์

การเชื่อมต่อโดยสร้างอินเตอร์เฟสจำลองในเครื่องคอมพิวเตอร์ คือการสร้างอุโมงค์สื่อสารจากเครื่องคอมพิวเตอร์ไปยังเราท์เตอร์ปลายทางของผู้ให้บริการ ทำให้เครื่องคอมพิวเตอร์สามารถติดต่อสื่อสารกับเครือข่าย IPv6 ได้โดยอุปกรณ์เครือข่ายอื่นๆ ไม่จำเป็นต้องรองรับ IPv6 ในรูปที่ 4.19 เป็นการตั้งค่าสำหรับระบบปฏิบัติการตระกูลวินโดวส์ (Windows) และรูปที่ 4.20 สำหรับระบบปฏิบัติการตระกูลลินุกซ์ (Linux)

```
cls
ipv6 install
netsh interface ipv6 install
netsh interface ipv6 add v6v4tunnel tbNTv6 161.246.56.214 203.185.93.4
netsh interface ipv6 add address tbNTv6 2001:f00:3836:1:0:feb5:0:2
netsh interface ipv6 add route ::/0 tbNTv6 2001:f00:3836:1:0:feb5:0:1
netsh interface ipv6 set interface tbNTv6 forwarding=enabled
pause
```

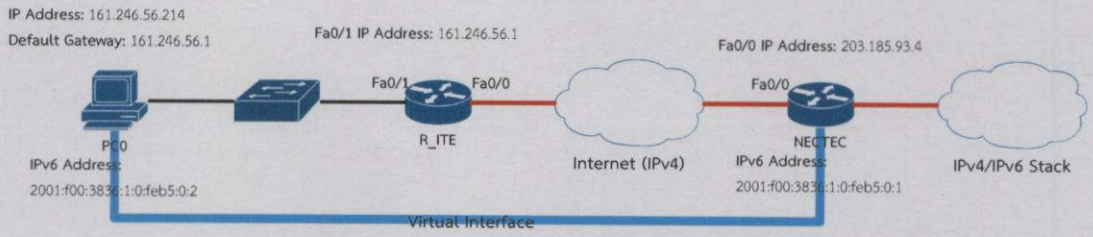
รูปที่ 4.12 การตั้งค่าการเชื่อมต่อโดยสร้างอินเตอร์เฟสจำลองในเครื่องคอมพิวเตอร์สำหรับระบบปฏิบัติการตระกูลวินโดวส์

```
#!/usr/bin/perl
modprobe ipv6
sudo /sbin/ip tunnel add tbNTv6 mode sit ttl 255 remote 203.185.93.4 local 161.246.73.214
sudo /sbin/ifconfig tbNTv6 up
sudo /sbin/route -A inet6 add ::/0 dev tbNTv6
sudo /sbin/ip -6 addr add 2001:f00:3836:1:0:feb5:0:2/96 dev tbNTv6
sudo /sbin/route -A inet6 add 2000::/3 dev tbNTv6
sudo /sbin/sysctl -w net.ipv6.conf.default.forwarding=1
sudo /sbin/sysctl -w net.ipv6.conf.tbNTv6.forwarding=1
```

รูปที่ 4.13 การตั้งค่าการเชื่อมต่อโดยสร้างอินเตอร์เฟสจำลองในเครื่องคอมพิวเตอร์สำหรับระบบปฏิบัติการตระกูลลินุกซ์

มีรูปแบบการเชื่อมต่อดังรูปที่ 4.14 และผลการเชื่อมต่อไปยังชื่อโดเมน google.com ผ่านเครือข่าย IPv6 ดังรูปที่ 4.15 ตามลำดับ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



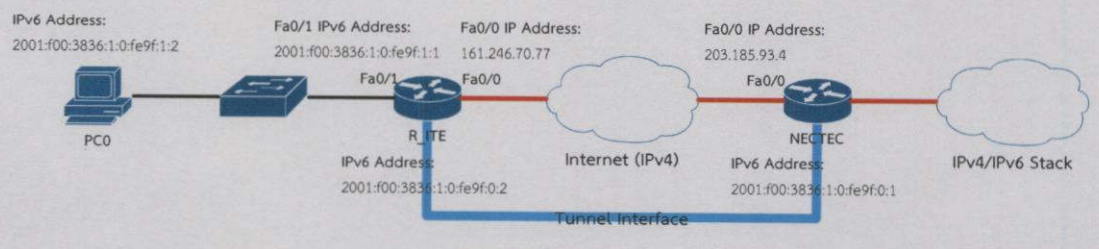
รูปที่ 4.14 การเชื่อมต่อไปยัง NECTEC โดยสร้างอินเตอร์เฟสจำลองในเครื่องคอมพิวเตอร์

```
C:\Users\Te>ping -6 google.com

Pinging google.com [2404:6800:4001:c01::8b] with 32 bytes of data:
Reply from 2404:6800:4001:c01::8b: time=205ms
Reply from 2404:6800:4001:c01::8b: time=199ms
Reply from 2404:6800:4001:c01::8b: time=201ms
Reply from 2404:6800:4001:c01::8b: time=217ms

Ping statistics for 2404:6800:4001:c01::8b:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 199ms, Maximum = 217ms, Average = 205ms

C:\Users\Te>
C:\Users\Te>tracert -d -6 google.com

Tracing route to google.com [2404:6800:4001:c01::8b]
over a maximum of 30 hops:

  1     5 ms     4 ms     4 ms  2001:f00:3836:1:0:feb5:0:1
  2     7 ms     4 ms     5 ms  2001:f00:1ffe:ffff::1
  3     *      120 ms     *     2001:200:e000:281::7660:1
  4   115 ms   119 ms   115 ms  2001:200:e000:1372::1600
  5   117 ms   116 ms   115 ms  2001:200:e000:7::b8
  6   118 ms   127 ms   117 ms  2001:200:0:fe00::3b41:0
  7   115 ms   118 ms   122 ms  2001:4860::3:0:11f1
  8   120 ms   119 ms   117 ms  2001:4860::1:0:6631
  9   127 ms   120 ms   127 ms  2001:4860::1:0:26ff
 10   195 ms   196 ms   193 ms  2001:4860::1:0:518d
 11   253 ms   252 ms   207 ms  2001:4860::1:0:9d0
 12   204 ms   211 ms   198 ms  2001:4860::2:0:3c7
 13     *        *        *     Request timed out.
 14   199 ms   198 ms   201 ms  2404:6800:4001:c01::8b

Trace complete.

C:\Users\Te>
```

รูปที่ 4.15 ผลการทดสอบการ Ping และแสดงเส้นทางการสื่อสารไปยังชื่อโดเมน google.com ผ่านทาง NECTEC โดยสร้างอินเตอร์เฟสจำลองในเครื่องคอมพิวเตอร์

4.2.2 การเชื่อมต่อผ่านอุโมงค์สื่อสารแบบ Manual Tunnel ที่เราท์เตอร์

การเชื่อมต่อผ่านอุโมงค์สื่อสารที่เราท์เตอร์ คือสร้างอุโมงค์สื่อสารที่เราท์เตอร์ซึ่งรองรับการทำงานทั้ง IPv4 และ IPv6 และทำหน้าที่เป็นเกตเวย์ของเครือข่าย IPv6 โดยมีรูปแบบการเชื่อมต่อดังรูปที่ 4.16



รูปที่ 4.16 การเชื่อมต่อไปยัง NECTEC ผ่านอุโมงค์สื่อสารแบบ Manual Tunnel ที่เราท์เตอร์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

มีการกำหนดค่าอุปกรณ์เราท์เตอร์ดังรูปที่ 4.17 และได้ผลการทดสอบการเชื่อมต่อไปยังชื่อโดเมน google.com ดังรูปที่ 4.18

```
!
ipv6 unicast-routing
!
interface Tunnel0
 no ip address
 ipv6 address 2001:F00:3836:1:0:FE9F:0:2/112
 tunnel source FastEthernet0/0
 tunnel mode ipv6ip
 tunnel destination 203.185.93.4
!
interface FastEthernet0/0
 ip address 161.246.73.77 255.255.255.0
!
interface FastEthernet0/1
 no ip address
 ipv6 address 2001:F00:3836:1:0:FE9F:1:1/112
!
ipv6 route ::/0 Tunnel0
!
```

รูปที่ 4.17 การตั้งค่าให้กับเราท์เตอร์เพื่อสร้างการเชื่อมต่อไปยัง NECTEC ผ่านอุโมงค์สื่อสารแบบ Manual Tunnel ที่เราท์เตอร์

```
C:\Users\User>ping -6 google.com

Pinging google.com [2404:6800:4001:c01::8a] with 32 bytes of data:
Reply from 2404:6800:4001:c01::8a: time=196ms
Reply from 2404:6800:4001:c01::8a: time=194ms
Reply from 2404:6800:4001:c01::8a: time=193ms
Reply from 2404:6800:4001:c01::8a: time=193ms

Ping statistics for 2404:6800:4001:c01::8a:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 193ms, Maximum = 196ms, Average = 194ms

C:\Users\User>
C:\Users\User>
C:\Users\User>tracert -6 -d google.com

Tracing route to google.com [2404:6800:4001:c01::8a]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  2001:f00:3836:1:0:fe9f:1:1
  2    11 ms     4 ms     4 ms  2001:f00:3836:1:0:fe9f:0:1
  3     *        5 ms     4 ms  2001:f00:1ffe:ffff::1
  4   118 ms   115 ms   115 ms  2001:200:e000:281::7660:1
  5   114 ms   114 ms   114 ms  2001:200:e000:1372::1600
  6   114 ms   114 ms   114 ms  2001:200:e000:7::b8
  7   115 ms   114 ms   114 ms  2001:200:0:fe00::3b41:0
  8   115 ms   114 ms   115 ms  2001:4860::3:0:11f1
  9   115 ms   114 ms   119 ms  2001:4860::1:0:6631
 10   119 ms   118 ms   118 ms  2001:4860::1:0:26fc
 11   192 ms   191 ms   191 ms  2001:4860::1:0:518d
 12   195 ms   193 ms   196 ms  2001:4860::1:0:3c0
 13   193 ms   195 ms   195 ms  2001:4860::2:0:3c7
 14     *        *        *     Request timed out.
 15   193 ms   196 ms   194 ms  2404:6800:4001:c01::8a

Trace complete.

C:\Users\User>_
```

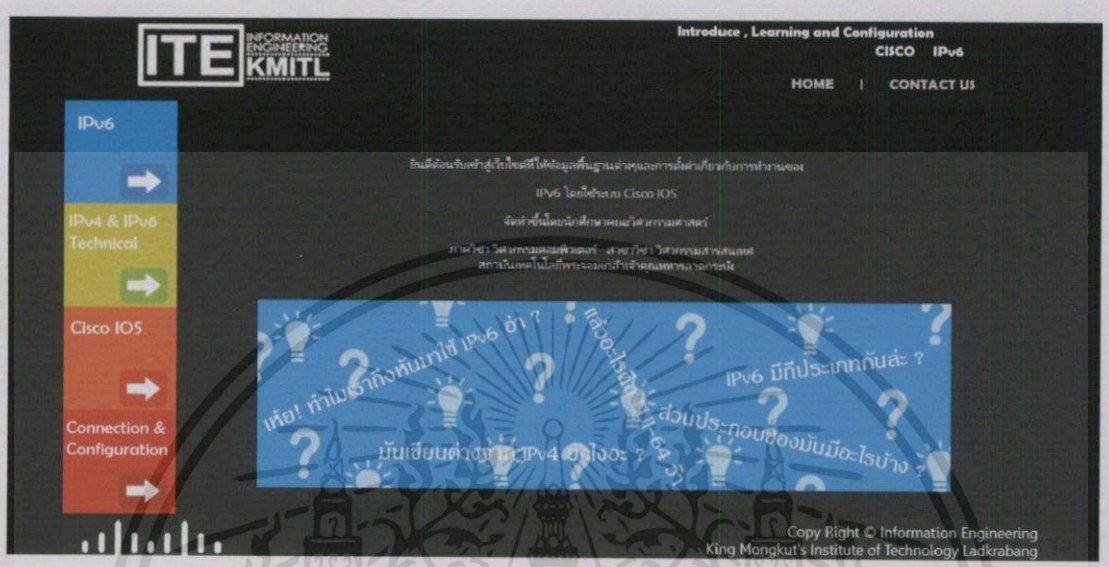
รูปที่ 4.18 ผลการทดสอบการ Ping และแสดงเส้นทางการสื่อสารไปยังชื่อโดเมน google.com ผ่านทาง NECTEC ด้วยอุโมงค์สื่อสารแบบ Manual Tunnel ที่เราท์เตอร์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.3 เว็บไซต์คู่มือการตั้งค่าอุปกรณ์สื่อสารที่ทำงานบน IPv6

4.3.1 หน้าหลักของเว็บไซต์

เมื่อเข้าสู่เว็บไซต์ ในหน้าแรกของคู่มือการตั้งค่าอุปกรณ์สื่อสารที่ทำงานบน IPv6 จะมีข้อความต้อนรับและทางด้านซ้ายจะมีเมนูเพื่อเข้าดูเนื้อหาตามหัวข้อนั้นๆ



รูปที่ 4.19 หน้าแรกของเว็บไซต์คู่มือการตั้งค่าอุปกรณ์สื่อสารที่ทำงานบน IPv6

4.3.2 หัวข้อต่างๆ ในแต่ละเมนู

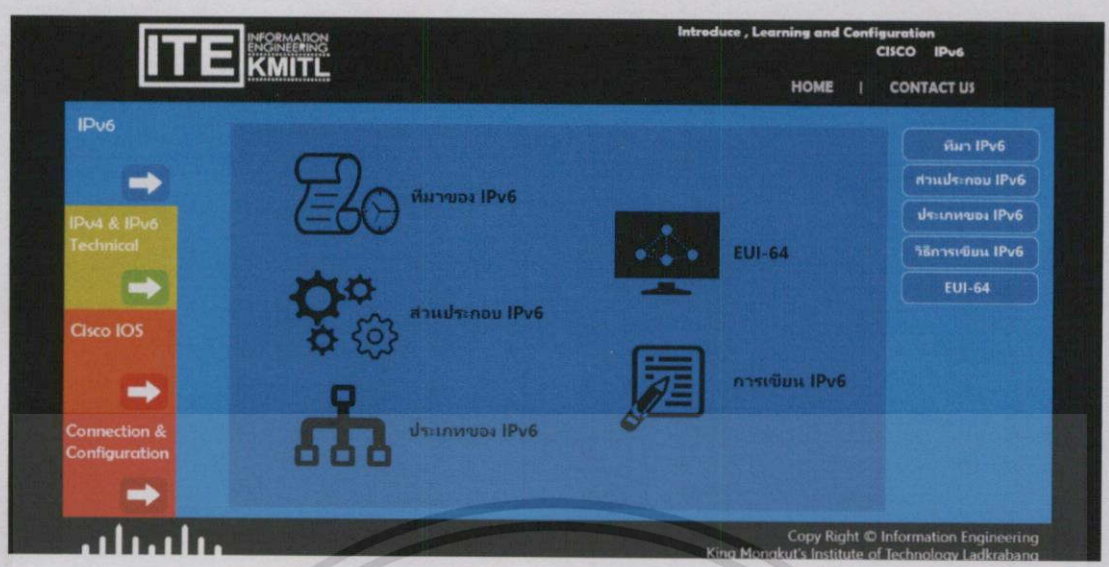
เมื่อเลือกไปที่เมนูทางด้านซ้าย ในแต่ละหัวข้อนั้นจะมีหัวข้อย่อยภายในแตกต่างกันไปตามหัวข้อหลัก ซึ่งจะแบ่งได้ดังนี้

4.3.2.1 หัวข้อ IPv6

เป็นหัวข้อที่อธิบายถึงทฤษฎีพื้นฐานต่างๆของ IPv6 ซึ่งแบ่งเป็นหัวข้อย่อยได้ดังนี้

- ที่มาของ IPv6
- ส่วนประกอบของ IPv6
- ประเภทของ IPv6
- การเขียนหมายเลข IPv6
- EUI-64

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

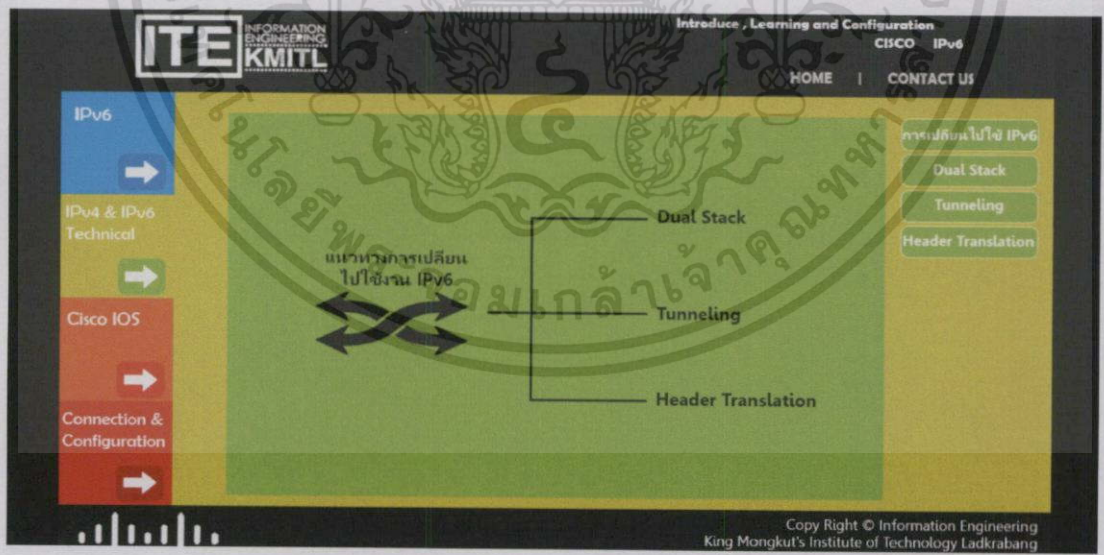


รูปที่ 4.20 หัวข้อ IPv6 และหัวข้อย่อย

4.3.2.2 หัวข้อ IPv4 & IPv6 Technical

เป็นหัวข้อที่อธิบายเกี่ยวกับรูปแบบที่จะเปลี่ยนไปใช้ IPv6 โดยใช้เทคนิคการใช้งานร่วมกันของ IPv4 และ IPv6 แบ่งเป็นหัวข้อย่อยดังนี้

- แนวทางการเปลี่ยนไปใช้ IPv6
- Dual Stack
- Tunneling
- Header Translation

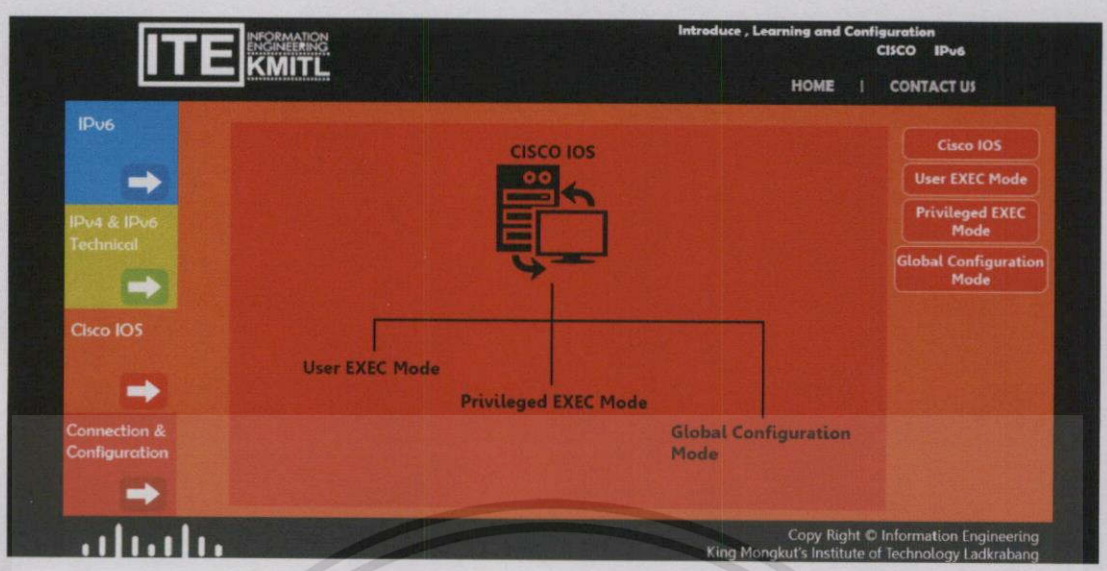


รูปที่ 4.21 หัวข้อ IPv4 & IPv6 Technical และหัวข้อย่อย

4.3.2.3 หัวข้อ Cisco IOS

เป็นหัวข้อที่อธิบายเกี่ยวกับระบบปฏิบัติการที่ควบคุมการทำงานของ Cisco แบ่งเป็นหัวข้อย่อยดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

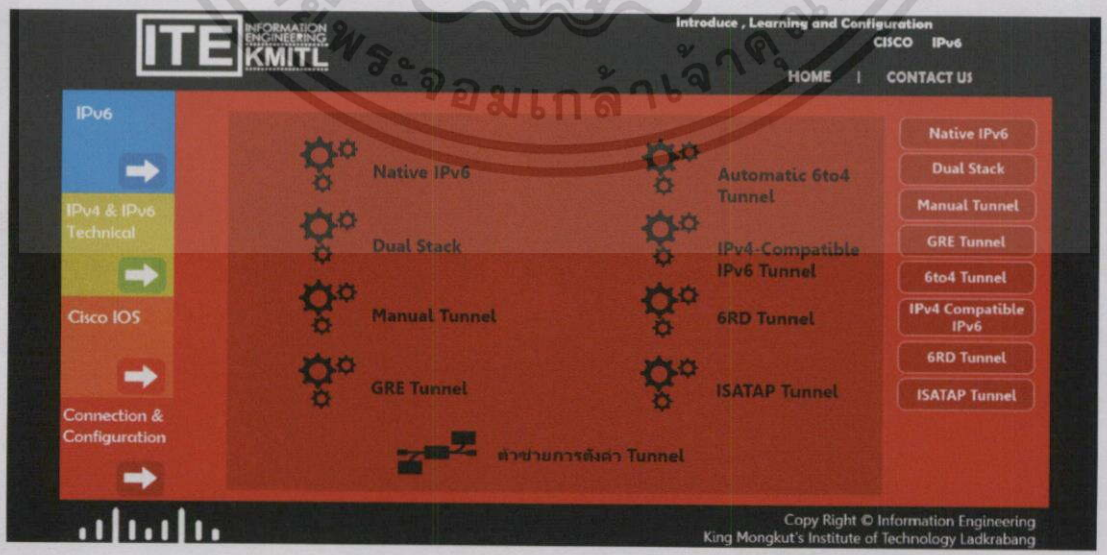


รูปที่ 4.22 หัวข้อ Cisco IOS และหัวข้อย่อย

4.3.2.4 หัวข้อ Connection & Configuration

เป็นหัวข้อที่อธิบายเกี่ยวกับการเชื่อมต่อและการตั้งค่าให้เราท์เตอร์ให้ทำงานภายใต้เครือข่าย IPv6 ด้วยรูปแบบต่างๆ และมีโปรแกรมตัวช่วยการตั้งค่า แบ่งเป็นหัวข้อย่อยดังนี้

- Native IPv6
- Dual Stack
- Manual Tunnel
- GRE Tunnel
- Automatic 6to4 Tunnel
- IPv4-Compatible IPv6 Tunnel
- 6RD Tunnel
- ISATAP Tunnel
- ตัวช่วยตั้งค่า IPv6

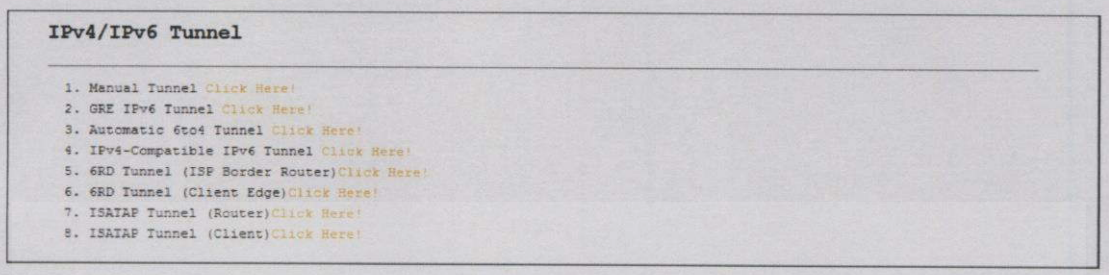


รูปที่ 4.23 หัวข้อ Connection & Configuration และหัวข้อย่อย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.3.3 โปรแกรมช่วยตั้งค่า

โปรแกรมตัวช่วยตั้งค่านี้จะอยู่ในหัวข้อ Connection & Configuration เมื่อเข้าไปจะเป็นการเปิดเว็บเพจใหม่ และมีเมนูในการตั้งค่าของ อุโมงค์สื่อสารแบบต่างๆ ดังรูปที่ 4.31

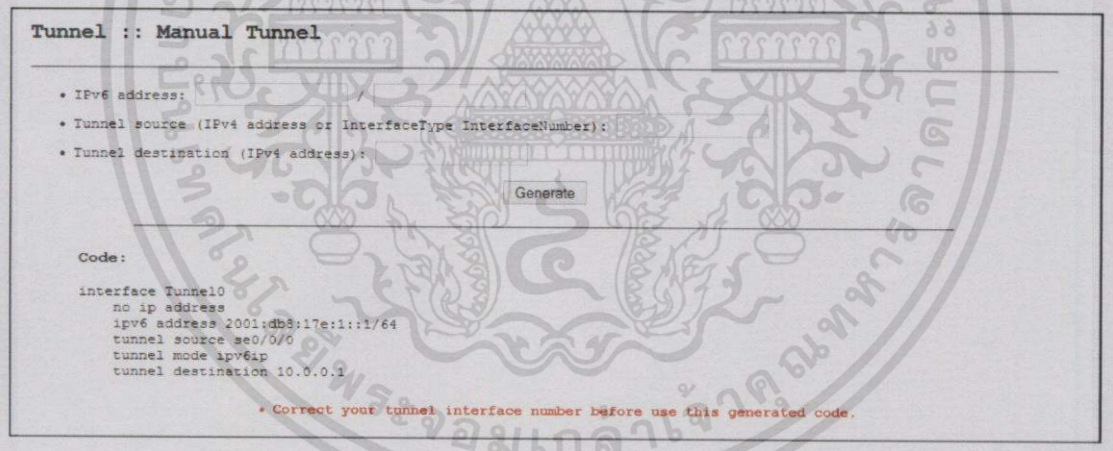


รูปที่ 4.24 เมนูของโปรแกรมตัวช่วยตั้งค่า

4.3.4 ผลการใช้งานโปรแกรมช่วยตั้งค่า

เมื่อเลือกรูปแบบที่ต้องการในโปรแกรม โปรแกรมจะแสดงเว็บเพจขึ้นมา โดยให้ใส่ข้อมูลตามแบบฟอร์มที่แสดงขึ้นมา และเมื่อกด Generate โปรแกรมจะแสดงวิธีการตั้งค่านั้นขึ้นมาตามรูปแบบต่างๆ ดังนี้

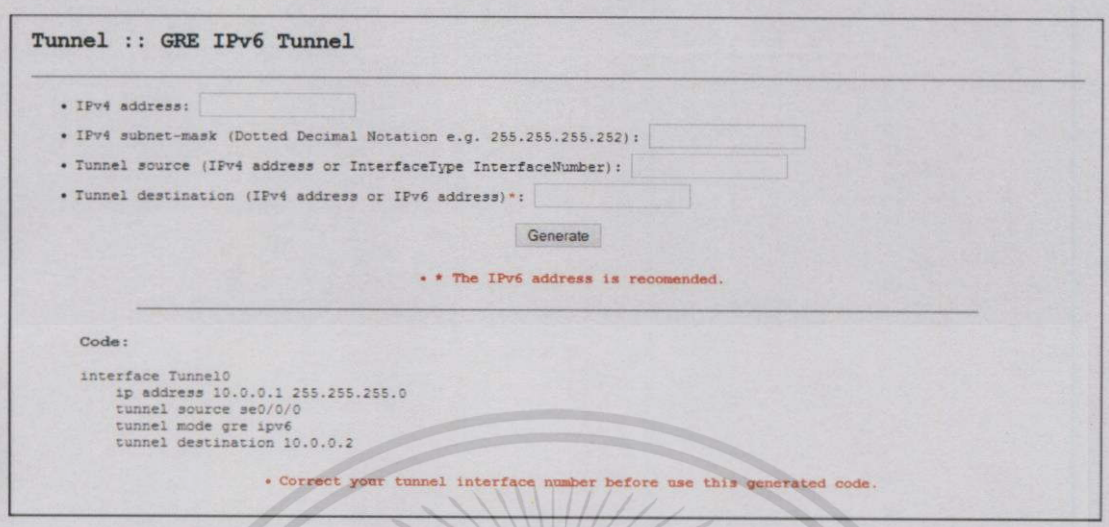
4.3.4.1 Manual Tunnel



รูปที่ 4.25 ผลการใช้งานโปรแกรมตัวช่วยตั้งค่าแบบ Manual Tunnel

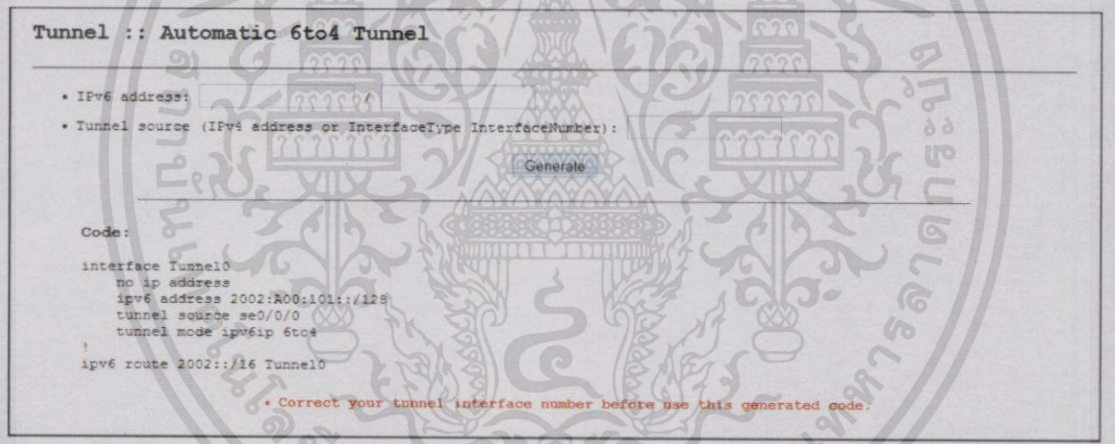
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.3.4.2 GRE IPv6 Tunnel



รูปที่ 4.26 ผลการใช้งานโปรแกรมตัวช่วยตั้งค่าแบบ GRE IPv6 Tunnel

4.3.4.3 Automatic 6to4 Tunnel



รูปที่ 4.27 ผลการใช้งานโปรแกรมตัวช่วยตั้งค่าแบบ Automatic 6to4 Tunnel

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.3.4.4 IPv4–Compatible IPv6 Tunnel

Tunnel :: IPv4-Compatible IPv6 Tunnel

• Tunnel source (IPv4 address or InterfaceType InterfaceNumber):

Generate

Code:

```
interface Tunnel0
    no ip address
    ipv6 enable
    tunnel source se0/0/0
    tunnel mode ipv6ip auto-tunnel
!
ipv6 route <ipv6-network-address> <IPv4-Compatible-IPv6 e.g ::10.0.1.2>
```

• Correct your tunnel interface number before use this generated code.

รูปที่ 4.28 ผลการใช้งานโปรแกรมตัวช่วยตั้งค่าแบบ IPv4–Compatible IPv6 Tunnel

4.3.4.5 6RD Tunnel (ISP Border Router)

Tunnel :: 6RD Tunnel (ISP Border Router)

• 6RD prefix name:

• Tunnel source (IPv4 address or InterfaceType InterfaceNumber):

• Tunnel IPv4 Prefix Lenght:

• Tunnel IPv6 address Prefix: /

Generate

Code:

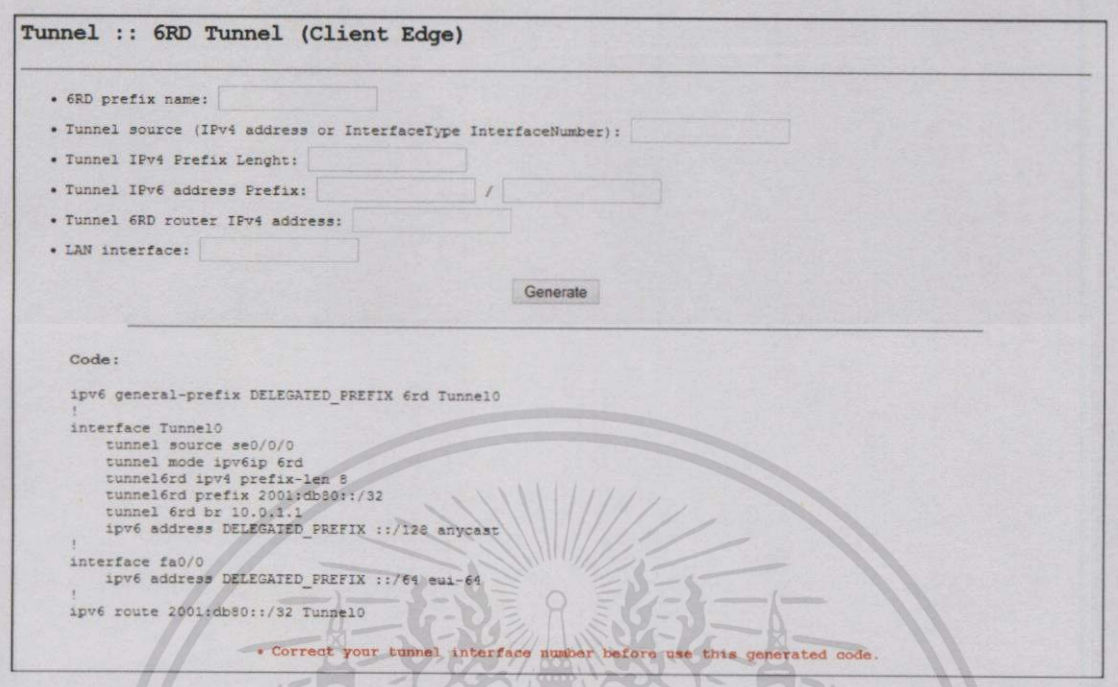
```
ipv6 general-prefix DELEGATED_PREFIX 6rd Tunnel0
!
interface Tunnel0
    tunnel source se0/0/0
    tunnel mode ipv6ip 6rd
    tunnel6rd ipv4 prefix-len 8
    tunnel6rd prefix 2001:db80::/32
    ipv6 address DELEGATED_PREFIX ::/128 anycast
!
ipv6 route 2001:db80::/32 Tunnel0
```

• Correct your tunnel interface number before use this generated code.
• Correct your loopback interface number before use this generated code.

รูปที่ 4.29 ผลการใช้งานโปรแกรมตัวช่วยตั้งค่าแบบ 6RD Tunnel (ISP Border Router)

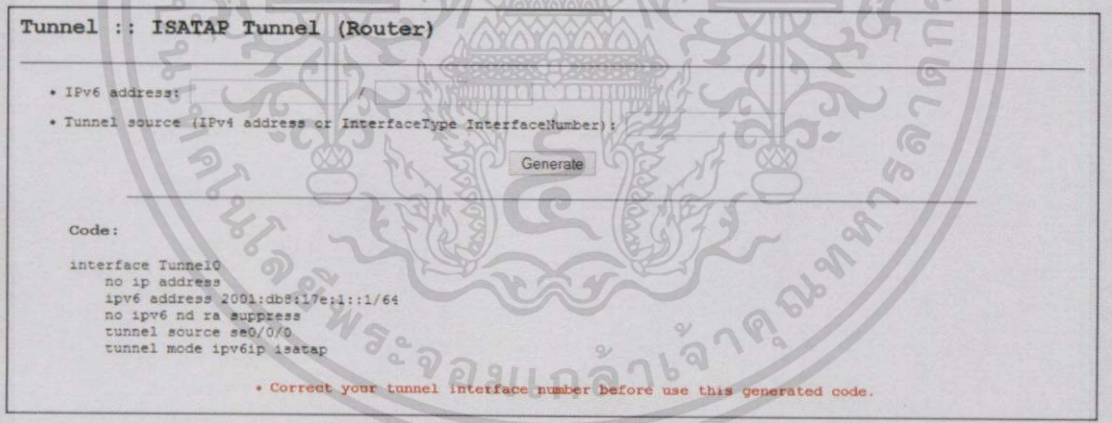
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.3.4.6 6RD Tunnel (Client Edge)



รูปที่ 4.30 ผลการใช้งานโปรแกรมตัวช่วยตั้งค่าแบบ 6RD Tunnel (Client Edge)

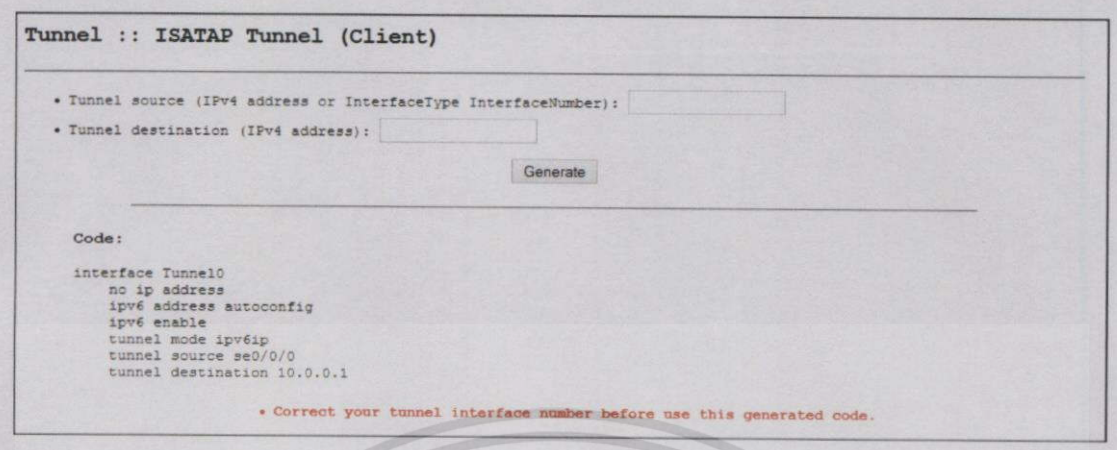
4.3.4.7 ISATAP Tunnel (Router)



รูปที่ 4.31 ผลการใช้งานโปรแกรมตัวช่วยตั้งค่าแบบ ISATAP Tunnel (Router)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.3.4.8 ISATAP Tunnel (Client)



รูปที่ 4.32 ผลการใช้งานโปรแกรมตัวช่วยตั้งค่าแบบ ISATAP Tunnel (Client)

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 5
สรุปและวิจารณ์ผล

5.1 ผลการศึกษาโครงงาน

จากการศึกษาและทดลองการเชื่อมต่อพบว่าการสร้างอุโมงค์สื่อสารแต่ละประเภทมีคุณสมบัติดังต่อไปนี้ และเปรียบเทียบได้ดังตารางที่ 5.1

- Manual Tunnel

เป็นอุโมงค์สื่อสารที่มีการใช้งานมานานที่สุดและนิยมใช้งานมากที่สุด โดยถูกประกาศใช้งานใน RFC 1993 มีรูปแบบการเชื่อมต่อแบบจุดต่อจุด (point-to-point) การตั้งค่าต้องทำโดยผู้ดูแลระบบหรือผู้ที่มีความรู้ แต่เนื่องจากมีการตั้งค่าที่แน่นอนทำให้สามารถคาดเดาประสิทธิภาพได้ (predictable) และวิเคราะห์ปัญหาได้ง่าย (debug)

- GRE Tunnel

เป็นอุโมงค์สื่อสารแบบจุดต่อจุดที่สามารถห่อหุ้มโพรโทคอลบนชั้นเครือข่ายได้หลายประเภท ซึ่งทำให้มี overhead สูงกว่าอุโมงค์สื่อสารแบบอื่นๆ โดยขนาดของ overhead จะขึ้นอยู่กับตัวเลือก (option) ต่างๆ ที่เลือกใช้

- Automatic 6to4 Tunnel

เป็นอุโมงค์สื่อสารที่สร้างหมายเลข IPv6 จากหมายเลข IPv4 แบบสาธารณะ โดยมีหมายเลขเครือข่ายส่วนหน้าเป็น 2002::/16 โดยสามารถติดต่อสื่อสารได้เฉพาะในเครือข่าย 6to4 ด้วยกันเท่านั้น หากต้องการติดต่อสื่อสารกับเครือข่าย IPv6 แบบ Native จะต้องมีอุปกรณ์ที่ชื่อว่า 6to4 รีเลย์ (6to4 Relay)

- IPv4-Compatible IPv6 Tunnel

อุโมงค์สื่อสารประเภทนี้ถูกประกาศใช้ใน RFC 2893 และถูกยกเลิกใช้ใน RFC 4213 เนื่องจากมีข้อจำกัดจำนวนมาก เช่นไม่สามารถสื่อสารกับเครือข่าย IPv6 แบบ Native ได้

- 6RD Tunnel

เป็นอุโมงค์สื่อสารที่ถูกใช้โดยผู้ให้บริการอินเทอร์เน็ต (ISP) ที่มีเครือข่ายภายในเป็นเครือข่าย IPv4 เพื่อให้บริการ IPv6 แก่ผู้ใช้บริการ โดยมีลักษณะการทำงานคล้าย Automatic 6to4 Tunnel แต่แตกต่างกันที่ 6RD ใช้เฉพาะในเครือข่ายของ ISP และ 6to4 ใช้รีเลย์สาธารณะ แต่ 6RD ใช้รีเลย์ของ ISP

- ISATAP Tunnel

เป็นอุโมงค์สื่อสารที่มีการออกแบบไว้สำหรับการใช้งานภายในองค์กร โดยมีการติดต่อสื่อสารแบบ NBMA (Non-Broadcast Multiple Access)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 5.1 ตารางแสดงการเปรียบเทียบคุณสมบัติของอุโมงค์สื่อสารแต่ละประเภท

อุโมงค์สื่อสาร	Manual	GRE	Automatic 6to4	IPv4-Compatible IPv6	6RD	ISATAP
6over4	✓	✓	✓	✓	✓	✓
4over6	✗	✓	✗	✗	✗	✗
6over6	✗	✓	✗	✗	✗	✗
ขนาดของ overhead (byte)	20	28 - 36	20	20	20	20
Multicast	✓	✓	✗	✗	✓	✗
Prefix delegate	✓	✓	/48	/96	✓	✗
Protocol number	41	47	41	41	41	41
Cross-site implement	✓	✓	✓	✓	Inside ISP	✗

✓ หมายถึง มีคุณสมบัติ (Support)

✗ หมายถึง ไม่มีคุณสมบัติ (Not Support)

5.2 สรุปผลโครงงาน

- ได้รับความรู้เรื่องการทำงานของ IPv6
- เครือข่ายทดสอบสามารถติดต่อสื่อสารผ่าน IPv4 ในโทโพโลยีแบบต่างๆ ได้
- สามารถติดต่อสื่อสารด้วย IPv6 ผ่านระบบอินเทอร์เน็ตได้
- ได้จัดทำเว็บไซต์คู่มือแนะนำและการตั้งค่าอุปกรณ์เครือข่ายของ IPv6
- ปัจจุบันผู้ให้บริการมักให้บริการการเชื่อมต่อแบบ Manual Tunnel เนื่องจากสามารถวิเคราะห์ปัญหาได้ง่าย และนิยมใช้งานแพร่หลายมากกว่าการทำอุโมงค์สื่อสารแบบอื่นๆ

5.3 ปัญหาที่เกิดระหว่างการทำโครงงาน

- IPv6 เป็นความรู้ใหม่ทำให้ผู้จัดทำใช้เวลานานในการศึกษา
- คู่มือการตั้งค่าอุปกรณ์มีน้อยมากและไม่ละเอียด จึงทำให้ใช้เวลานานในการเรียนรู้
- แม้ว่าเครื่องคอมพิวเตอร์/อุปกรณ์เครือข่ายจะรองรับมาตรฐาน IPv6 เรียบร้อยแล้ว แต่โปรแกรมที่รองรับการทำงานบน IPv6 ยังมีจำนวนน้อยมาก
- IPv6 Tunnel Broker ที่ใช้งานจริงและอนุญาตให้สร้างการเชื่อมต่อด้วยมีน้อย จึงทำให้มีตัวอย่างการทดสอบน้อย
- IPv6 Tunnel Broker ส่วนใหญ่ตรวจสอบการมีอยู่จริงของอุปกรณ์ที่ร้องขอการสร้างอุโมงค์สื่อสาร (check alive) ด้วยการ ping ซึ่งระบบเครือข่ายในสถาบันฯ และ คณะฯ ซึ่งดูแลโดย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สำนักบริการคอมพิวเตอร์ไม่ได้มีการอนุญาตให้มีการ ping จากเครือข่ายภายนอกจึงมี IPv6 Tunnel Broker ให้เลือกสามารถใช้บริการได้น้อยราย

- ไม่สามารถทดสอบการให้บริการ IPv6 ด้วยการแปลงหมายเลขที่อยู่ได้ เนื่องจากต้องใช้อุปกรณ์ Carrier Grade NAT ซึ่งเป็นอุปกรณ์เฉพาะของผู้ให้บริการอินเทอร์เน็ต

5.4 แนวทางในการพัฒนาโครงงานต่อ

- ทดสอบระบบเมื่อเครือข่าย IPv4 จำนวน 2 เครือข่ายต้องการติดต่อกันผ่านเครือข่าย IPv6
- ทำให้ระบบช่วยสร้างการตั้งค่าสามารถตรวจสอบข้อมูลหมายเลขที่อยู่ IPv6 ที่ป้อนเข้ามาได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บรรณานุกรม

[1] Bao, C., Huitema, C., Bagnulo, M., Boucadair, M. และ X. Li, "IPv6 Addressing of IPv4/IPv6 Translators," RFC 6052, October 2010.

[2] Cisco Systems, Inc., "Cisco IOS IP Configuration Guide Release 12.2," CA, USA, August 2006.

[3] Cisco Systems, Inc., "IPv6 Configuration Guide, Cisco IOS Release 15.2MT," CA, USA, July 2012.

[4] DATACOMM. Dept., "รูปแบบการเชื่อมต่อกับโครงข่ายระบบ IPv6 ของ กสท.," CAT TELECOM, March 2011.

[5] Deering, S. และ R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," RFC 2460, December 1998.

[6] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., และ M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," RFC 3315, July 2003.

[7] Hinden, R. และ S. Deering, "IP Version 6 Addressing Architecture," RFC 4291, February 2006.

[8] Hinden, R., Deering, S., Fink, R., และ T. Hain, "Initial IPv6 Sub-TLA ID Assignments," RFC 2928, September 2000.

[9] Huston, G., Lord, A. และ P. Smith, "IPv6 Address Prefix Reserved for Documentation," RFC 3849, July 2004.

[10]Kawamura, S. และ M. Kawashima, "A Recommendation for IPv6 Address Text Representation," RFC 5952, August 2010.

[11]Microsoft Corporation, "Microsoft® Windows Server® 2008 White Paper: IPv6 Transition Technologies," February 2008.

[12]Thomson, S., Narten, T. และ T. Jinmei, "IPv6 Stateless Address Autoconfiguration," RFC 4862, September 2007.

[13]Wikimedia Commons. "File:IPv6 header rv1.png," July 2013, https://commons.wikimedia.org/wiki/File:IPv6_header_rv1.png.

[14]Kozierok, C. M., "The TCP/IP Guide - IPv6 Interface Identifiers and Physical Address Mapping," September 2005, http://www.tcpipguide.com/free/t_IPv6InterfaceIdentifiersandPhysicalAddressMapping-2.htm.

[15]Cybertelecom, "Cybertelecom :: IPv6 Transition," June 2013, http://www.cybertelecom.org/dns/ipv6_transition.htm

[16]Hellomyweb, "โครงสร้างคำสั่งของ HTML," 16 May 2010, http://www.hellomyweb.com/index.php/main/content/12

[17]Doesystem, "HTML Basic," 14 Dec 2011, http://www.doesystem.com/43d214aa6605b7783eb7e778821e3552/HTML-Basic.htm

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

[18]วิกิตำรา contributors, "ภาษาพีเอชพี/เริ่มต้นกับ PHP/คู่มือพื้นฐาน/เริ่มเขียนเว็บด้วย PHP," 14 Jan 2013, http://th.wikibooks.org/w/index.php?title=%E0%B8%A0%E0%B8%B2%E0%B8%A9%E0%B8%B2%E0%B8%9E%E0%B8%B5%E0%B9%80%E0%B8%AD%E0%B8%8A%E0%B8%9E%E0%B8%B5/%E0%B9%80%E0%B8%A3%E0%B8%B4%E0%B9%88%E0%B8%A1%E0%B8%95%E0%B9%89%E0%B8%99%E0%B8%81%E0%B8%B1%E0%B8%9A_PHP/%E0%B8%84%E0%B8%B9%E0%B9%88%E0%B8%A1%E0%B8%B7%E0%B8%AD%E0%B8%9E%E0%B8%B7%E0%B9%89%E0%B8%99%E0%B8%90%E0%B8%B2%E0%B8%99/%E0%B9%80%E0%B8%A3%E0%B8%B4%E0%B9%88%E0%B8%A1%E0%B9%80%E0%B8%82%E0%B8%B5%E0%B8%A2%E0%B8%99%E0%B9%80%E0%B8%A7%E0%B9%87%E0%B8%9A%E0%B8%94%E0%B9%89%E0%B8%A7%E0%B8%A2_PHP&oldid=23551

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้