สำนักหอสมุดกลาง พระจอมเกล้าลาดกระบัง

การนำเครือข่าย IP มาประยุกต์ใช้กับเครือข่าย SNA/SDLC และ X.25 กับระบบงาน ATM

AN APPLICATION OF IP NETWORK WITH SNA/SDLC AND X.25 PROTOCOLS OF ATMs SYSTEM

T045889

นพรัตน์ เจิดแจ่มจรัส

NOPARAT JERTJAMJARAT

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เลขหมู่.....
เลขทะเบียน 45889
วัน, เดือน, ปี 19 ก.พ. 2546

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

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมไฟฟ้า

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ.2546

ISBN 974-324-187-6

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

AN APPLICATION OF IP NETWORK WITH SNA/SDLC AND X.25 PROTOCOLS OF ATMs SYSTEM

NOPARAT JERTJAMJARAT

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF ENGINEERING IN ELECTRICAL ENGINEERING

SCHOOL OF GRADUATE STUDIES

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2003

ISBN 974-324-187-6

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

COPYRIGHT 2003

SCHOOL OF GRADUATE STUDIES

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หัวข้อวิทยานิพนธ์	การนำเครือข่าย IP มาประยุกต์ใช้กับเครือข่าย SNA/SDLC และ X.25 กับระบบ งาน ATM
นักศึกษา	นายนพรัตน์ เจิดแจ่มจรัส
รหัสประจำตัว	41061146
ปริญญา	วิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชา	วิศวกรรมไฟฟ้า
พ.ศ.	2546
อาจารย์ผู้ควบคุมวิทยานิพนธ์	รศ. ดร. กอบชัย เดชหาญ

บทคัดย่อ

วิทยานิพนธ์นี้เป็นการนำเสนอรูปแบบและวิธีการของการประยุกต์ใช้โพรโทคอล SNA/SDLC ที่ใช้อยู่กับระบบงาน ATM (Automatic Teller Machine) โดยมีระบบคอมพิวเตอร์หลักซึ่งทำงานเป็นแบบ PU type 4 และใช้โพรโทคอล X.25 ทำหน้าที่ควบคุมเครื่อง ATM ทั้งหมด โดยข้อมูลทั้งหมดจะถูกส่งผ่านเครือข่าย IP ที่ได้ถูกออกแบบไว้โดยการใช้ Routing Protocol แบบ Open Shortest Path First (OSPF) ซึ่งข้อมูลจากเครื่อง ATM เมื่อถูกส่งผ่านไปบนเครือข่าย IP จะถูกแปลงจากโพรโทคอล SNA/SDLC เป็นโพรโทคอล Data Link Switch (DLSw) หลังจากนั้นข้อมูลจะถูกแปลงเป็นแพ็กเก็ต X.25 และทำการเซ็ทบิท Q เป็น “1” ซึ่งเรียกว่า Qualified Logical Link Control (QLLC) เพื่อทำให้โพรโทคอล SNA/SDLC และ X.25 สามารถส่งผ่านข้อมูลกันได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Thesis Title An Application of IP Network with SNA/SDLC and X.25 Protocols of ATMs System

Student Mr. Noparat Jertjamjarat

Student ID. 41061146

Degree Master of Engineering

Programme Electrical Engineering

Year 2003

Thesis Advisor Assoc. Prof. Dr. Kobchai Dejhan

ABSTRACT

This thesis presents a method and application principle of SNA/SDLC protocol for using with ATMs (Automatic Teller Machine) system that have a host for controlling the whole ATM. The host works as PU type 4 and uses X.25 protocol. While the all ATM data are transferred via IP network, which is designed for using OSPF routing protocol, the data will be converted from SNA/SDLC to Data Link Switch (DLSw) protocol. After that, the data are converted to X.25 packet and Q bit will be set to "1" so called "Qualified Logical Link Control (QLLC)" in order to make data transferable between SNA/SDLC and X.25 protocol.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้อย่างดี ด้วยคำแนะนำเกี่ยวกับระบบเครือข่ายสื่อสารข้อมูล และคำปรึกษาที่มีประโยชน์อย่างสูงจากท่านรองศาสตราจารย์ ดร. กอบชัย เดชหาญ ที่ช่วยเหลือตลอดเวลา ซึ่งทำให้กระผมมีความรู้สึกซาบซึ้งในสิ่งต่าง ๆ ที่ท่านได้ให้ความอนุเคราะห์ ขอกราบขอบพระคุณเป็นอย่างสูง

ขอกราบขอบพระคุณ คุณพ่อ พิพัฒน์ และ คุณแม่ อุษณีษ์ เจิดแจ่มจรัส ที่กรุณามอบชีวิตความใฝ่รู้ และความมุมานะในด้านการศึกษาให้แก่ชีวิตกระผม

ขอขอบคุณ คุณชาลิน สุวรรณวงศ์ ที่คอยให้คำชี้แนะ ตลอดจนให้ความรู้ทางด้านระบบเครือข่ายและส่งเสริมสนับสนุนในด้านการศึกษา

ขอขอบคุณ คุณพุทธวรรณ และ ด.ช. อัณณ์ เจิดแจ่มจรัส ภรรยาและลูกชายที่คอยให้กำลังใจและเสียสละเวลาของครอบครัวเพื่อให้ผลงานวิจัยนี้เสร็จสิ้นได้ด้วยดี

ขอขอบคุณ ธนาคารสแตนดาร์ดชาร์เตอร์ดนครธน จำกัด (มหาชน) ที่ให้การสนับสนุนในเรื่องของการทำงานและอุปกรณ์ในการทำวิจัยนี้

ขอขอบคุณ บัณฑิตวิทยาลัย ที่ให้ทุนสนับสนุนการทำวิทยานิพนธ์ครั้งนี้

สุดท้ายนี้ขอขอบคุณ พี่ ๆ เพื่อน ๆ และน้อง ๆ ที่ช่วยเหลือ แนะนำ และให้กำลังใจต่อผู้ทำวิจัยจนสำเร็จสมบูรณ์

คุณค่าและประโยชน์อันพึงมีจากวิทยานิพนธ์ฉบับนี้ ผู้วิจัยขอมอบแด่ผู้มีพระคุณทุกท่าน

นพรัตน์ เจิดแจ่มจรัส

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ

หน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ(ต่อ)

หน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ(ต่อ)

หน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ(ต่อ)

หน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญตาราง

หน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูป

รูปที่ หน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูป(ต่อ)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูป(ต่อ)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 1
บทนำ

1.1 กล่าวนำ

ในปัจจุบันนี้ เทคโนโลยี IP ได้เข้ามามีบทบาทสำคัญอย่างมากในการส่งผ่านข้อมูลระยะไกล และมีระบบรักษาความปลอดภัยที่ดีขึ้น เช่น เครือข่าย VPN (Virtual Private Network) และเครือข่าย Internet เป็นต้น โดยมีรูปแบบของการเชื่อมต่อเป็นแบบ Connectionless ซึ่งไม่จำเป็นต้องมีการสร้างเส้นทางก่อนการส่งข้อมูล แต่จะอาศัยค่า IP Address เป็นตัวบ่งบอกถึงเส้นทางที่ข้อมูลควรจะผ่านไปในแต่ละ Hop แทน ซึ่งข้อมูลของหมายเลข IP และอินเทอร์เฟสที่ต่ออยู่จะถูกบันทึกลงในตาราง Routing ของอุปกรณ์แต่ละตัว ซึ่งจะทำให้อุปกรณ์ที่มีหมายเลข IP ทั้งหมดสามารถติดต่อกันได้โดยผ่านเครือข่ายชนิดนี้ได้

เนื่องจากโพรโทคอล SNA/SDLC เป็นโพรโทคอลที่ไม่มีคุณสมบัติในการสวิทช์ และรูปแบบของโทโปโลยีเป็นแบบจุดต่อจุด (Point-to-Point) จึงทำให้ไม่มีคุณสมบัติในการทำ Routing ได้ เช่น การทำ Alternative Routing หรือ Reroute แต่ในปัจจุบันโพรโทคอล SNA/SDLC ยังเป็นที่นิยมใช้กันอย่างแพร่หลายอย่างยิ่ง เช่น ในระบบ Mini Computer และ Mainframe เป็นต้น จึงทำให้เกิดแนวทางในการประยุกต์ใช้งานโพรโทคอล SNA/SDLC ร่วมกับเครือข่าย IP โดยมีโพรโทคอล X.25 ที่ทำหน้าที่ติดต่อกับ Host ในอีกด้านหนึ่ง ซึ่งโพรโทคอล X.25 มีข้อดีในเรื่องการตรวจเช็คความผิดพลาดของข้อมูล และใช้การเชื่อมต่อแบบ Connection Oriented ซึ่งจะมีการสร้างเส้นทางก่อนการส่งข้อมูล ซึ่งจะทำให้เกิดความน่าเชื่อถือ และมีความปลอดภัยมากยิ่งขึ้น

1.2 วัตถุประสงค์ของวิทยานิพนธ์

สืบเนื่องจากการดำเนินธุรกิจในปัจจุบันได้มีการนำเทคโนโลยีระบบคอมพิวเตอร์ Online ผ่านเครือข่ายมาประยุกต์ใช้ในองค์กร เพื่อนำมาซึ่งการให้การบริการที่สะดวก รวดเร็ว และทันสมัยแก่ลูกค้าโดยมีการตั้งเป้าหมายของประสิทธิภาพในการให้การบริการได้ถึง 99% ของเวลาที่ให้บริการนั้น ๆ รวมทั้งรูปแบบของข้อมูลในระบบการบริการมีความหลากหลาย และขนาดของข้อมูลในการส่งผ่านระบบเครือข่ายมีขนาดใหญ่ขึ้น

จากคุณสมบัติดังกล่าว วิทยานิพนธ์นี้จึงขอนำเสนอการออกแบบเครือข่าย IP ที่มีประสิทธิภาพ โดยนำเอาระบบบริการ Online ของเครื่องถอนเงินอัตโนมัติ (ATM) ที่มีรูปแบบโพรโทคอล SNA/SDLC ร่วมกับโพรโทคอล X.25 มาประยุกต์ใช้กับเครือข่าย IP ให้มีประสิทธิภาพและมีความเสถียรภาพ จึงทำให้เกิดแนวคิดในการออกแบบระบบเครือข่ายที่มีเสถียรภาพและมีความสามารถในการเปลี่ยนเส้นทาง (Reroute)ไปใช้ในอีกเส้นทางหนึ่งได้ในกรณีที่เกิดปัญหากับเส้นทางหลักขึ้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

และสามารถจัดสรรการส่งผ่านปริมาณข้อมูลให้กับเครือข่ายได้ ตลอดจนมีการประยุกต์ใช้โพรโทคอล SNA/SDLC ร่วมกับโพรโทคอล X.25 ซึ่งจะทำให้เกิดความน่าเชื่อถือ ให้กับระบบเครือข่าย IP ได้มากยิ่งขึ้น

1.3 หลักการใหม่ในวิทยานิพนธ์

การนำเสนอการออกแบบเครือข่าย IP อย่างมีเสถียรภาพและมีประสิทธิภาพ โดยนำอุปกรณ์เราท์เตอร์มาเป็นอุปกรณ์ในการสร้างเครือข่าย และส่งผ่านข้อมูลแบบแพ็กแก็ต ตลอดจนได้มีการนำระบบงาน ATM ที่มีอยู่เดิมกับโพรโทคอล SNA/SDLC และ X.25 มาประยุกต์ใช้งานร่วมกันกับเครือข่าย IP ที่ได้ออกแบบไว้แล้วดังกล่าว โดยใช้อุปกรณ์เราท์เตอร์เพื่อเชื่อมต่อกับเครื่อง ATM ซึ่งเราท์เตอร์จะทำการสร้างเส้นทางเสมือนผ่านเครือข่าย IP มายังระบบคอมพิวเตอร์หลัก (Host) ที่ใช้โพรโทคอล X.25 โดยที่ข้อมูลของเครื่อง ATM จะถูกส่งผ่านเครือข่าย IP โดยมีการบีบอัดข้อมูลด้วยฟังก์ชั่น DLSw+ (Data Link Switch+) ภายในเครือข่าย IP จากนั้นข้อมูลจะถูกบีบอัดด้วยโพรโทคอล X.25 เพื่อส่งผ่านมายังระบบคอมพิวเตอร์หลัก

1.4 เปรียบเทียบกับหลักการเดิม

ในหลักการเดิมนั้น การส่งผ่านข้อมูลจะเป็นแบบลักษณะจุดต่อจุด (Point-to-Point) โดยผ่านอุปกรณ์โมเด็ม ซึ่งทำให้การส่งผ่านข้อมูลมีข้อจำกัดต่าง ๆ เช่น ไม่สามารถสร้างเส้นทางสำรองให้แก่ข้อมูลได้ซึ่งเป็นผลให้ไม่สามารถแบ่งเบาโหลดให้กับอุปกรณ์เครือข่ายได้ และมีการใช้โพโทคอล SNA/SDLC กับ Host ทั้ง 2 ด้าน ทำให้การเชื่อมต่อ ATM เข้ากับ Host จำเป็นต้องให้อุปกรณ์แยกพอร์ท (Sharing equipments) ซึ่งเป็นผลให้ค่าความหน่วงของเวลา (Delay Time) มีค่ามากกว่าเครือข่ายในรูปแบบใหม่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 2

System Network Architecture

System Network Architecture (SNA) ถือกำเนิดขึ้นเมื่อปี ค.ศ. 1974 ซึ่งถูกคิดค้นโดยบริษัทไอบีเอ็ม ซึ่งรวบรวมการจัดการและโครงสร้างต่าง ๆ ที่เกี่ยวข้องกับ Networking System / 360 โดยผ่านระบบสถาปัตยกรรมเพียงระบบเดียวเพื่อการสื่อสารข้อมูล ทำให้การสื่อสารมีความยืดหยุ่นจากระบบการคำนวณหลักออกไปสู่สาขาที่ไกลออกไป โดยใช้โครงสร้างที่เป็นลำดับชั้นที่ประกอบด้วย 7 เลเยอร์ [4]

2.1 แนวคิดในการสร้าง SNA (Foundation SNA Concepts)

แนวคิดพื้นฐานต่าง ๆ เพื่อให้เข้าใจระบบ SNA มีดังนี้

- SNA เป็นเครือข่ายที่มีลำดับชั้น (hierarchical) คือมี master-slave
- SNA ใช้เส้นทางที่ได้เตรียมไว้ล่วงหน้าเพื่อขนถ่ายข้อมูลระหว่างต้นทางและปลายทาง
- ACF/VTAM เป็น master ของเครือข่าย SNA
- SNA เป็นสถาปัตยกรรมเครือข่ายที่ network-addressable unites สามารถติดต่อกันได้

2.1.1 องค์ประกอบของเครือข่าย

เครือข่าย SNA ถูกสร้างขึ้นจากองค์ประกอบพื้นฐานของ hardware และ software พื้นฐาน ใน เครือข่าย SNA ขั้นพื้นฐาน องค์ประกอบหลักของ hardware จะประกอบด้วย

- Mainframe CPU
- Communications controller และ Front-End Processor –37X5 (3725, 3745)
- Cluster controller –3X74 (3174, 3274)
- End-user workstation/printer

ความสัมพันธ์ของ master/slave เป็นรูปแบบที่เครือข่าย SNA ใช้ในการทำงาน ส่วนของ master ทำงานอยู่บน CPU ของระบบ mainframe เรียกว่า access method และ ส่วนของ slave ทำงานอยู่บนเครือข่าย ในช่วงเวลาต่อมาได้มีการเพิ่มหน้าที่ให้กับเครือข่ายทำให้องค์ประกอบของ hardware/software ตัวใหม่ถูกสร้างขึ้นเพื่อเป็น front-end ในการ process ของระบบ mainframe และเพื่อควบคุมเครือข่าย ดังนั้นจึงทำให้เกิดโปรแกรมในการควบคุมเครือข่ายขึ้น (Network Control Program) เพื่อรองรับ hardware ของเครือข่ายดังกล่าว จึงได้ทำการพัฒนา software ดังต่อไปนี้

- Advanced Communication Function/Communications Access Mtehod (VTAM)

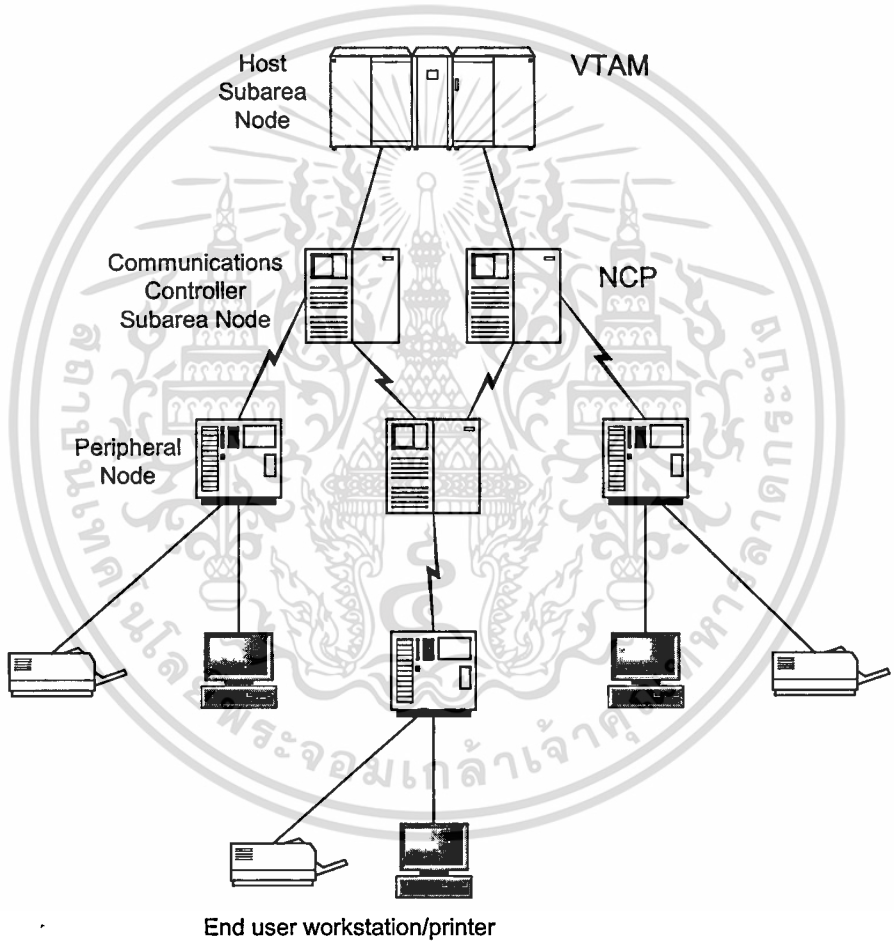
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- Advanced Communication Function/Network Control Program (NCP)

2.1.2 Nodes

กลุ่มของ hardware และ software ระบุถึงองค์ประกอบทางกายภาพและทางตรรกของเครือข่าย SNA ในรูปที่ 2.1 แสดงให้เห็นโนด 3 ชนิดคือ

- Host subarea nodes
- Communications controller subarea nodes
- Peripheral nodes



รูปที่ 2.1 รูปแบบโนดชนิดต่าง ๆ บนระบบเครือข่าย SNA

พิจารณาหน้าที่ของโนดในแต่ละโนดได้ดังนี้

- Host subarea node เป็นกลไกหลักสำหรับรับผิดชอบเครือข่าย ประกอบด้วย Hardware คือ mainframe CPU และมีองค์ประกอบของ Software คือ VTAM

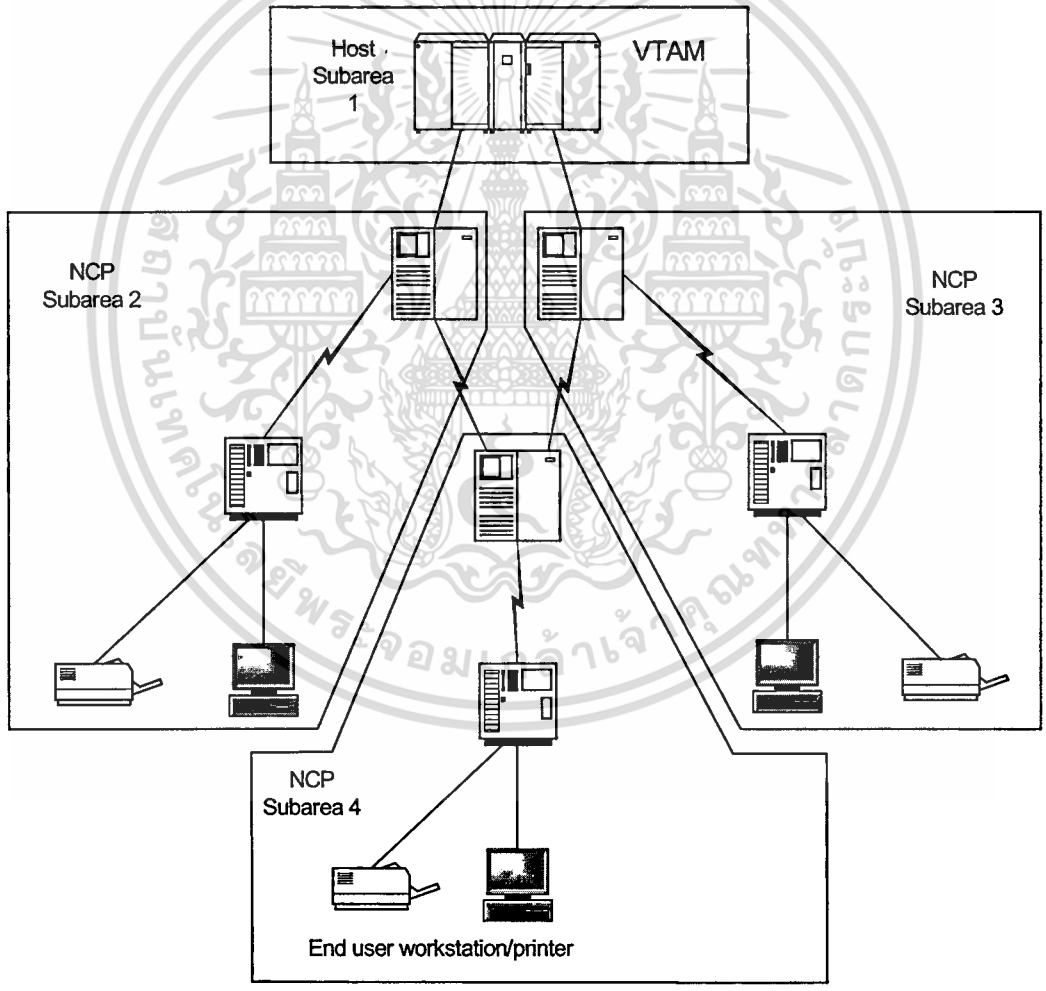
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- Communications Controller subarea node คือกลไกที่อยู่รอบนอกซึ่งส่งผ่านแพ็กเก็ตเครือข่ายออกไปสู่เครือข่าย Hardware คือ communications front-end processor และมีองค์ประกอบของ Software คือ Network Control Program

ส่วนที่เหลือขององค์ประกอบในเครือข่าย จะประกอบด้วย peripheral nodes ซึ่งรวมถึง Cluster controllers Distributed processors End-user workstations และ printers

2.1.3 แอเรียย่อย (Subareas)

ในระบบ SNA ส่วนต่าง ๆ ของเครือข่ายจะถูกแบ่งออกเป็นส่วนย่อย ๆ โดยมีกฎในการแบ่งออกเป็นส่วนย่อย ๆ หรือ subarea คือภายในเครือข่ายนั้นต้องเป็น VTAM หรือ NCP เพื่อไว้จัดการกับแอเรีย ในรูปที่ 2-2 แสดงถึง subareas ที่ประกอบด้วย VTAMs และ NCPs



รูปที่ 2.2 รูปแบบไดอะแกรมของเครือข่ายแอเรียย่อย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.1.4 การเชื่อมโยง (Links)

การเชื่อมโยง SNA เป็นการเชื่อมต่อใด ๆ ที่ใช้เพื่อเชื่อมแอเรียย่อย 2 แอเรียเข้าด้วยกัน การเชื่อมต่อทางกายภาพสามารถเป็น Fiber channel วงจรโทรคมนาคมขั้นพื้นฐาน หรือแม้แต่ดาวเทียม ในที่นี้สามารถมีการเชื่อมโยงระหว่างแอเรียย่อยได้มากกว่า 1 การเชื่อมโยงเพื่อเป็นเส้นทางสำรอง ในกรณีที่การเชื่อมโยงหลักล่มได้ ที่ด้านปลายของแต่ละด้านของ logical link คือ link station ทำหน้าที่ส่งข้อมูลไปบนข่ายเชื่อมโยงโดยใช้ data link control protocols ในรูปที่ 2.2 แสดงให้เห็นถึง links และ link stations ซึ่งในระบบ SNA สามารถรองรับ data link control protocols ดังนี้

- System/390 data channel
- SDLC
- BSC
- S/S
- X.25

2.1.5 Network-Addressable Units

ความพิศวงของเครือข่ายคอมพิวเตอร์ คือการที่มีรูปแบบที่เกาะติดกันโดยมีองค์ประกอบที่ต่างกันและพูดคุยกันได้ การติดต่อพูดคุยกันด้วยฟังก์ชั่นเหล่านี้ได้มาจากการแต่งตั้งของ Network Addressable Units (NAUs) โดยที่ NAUs เป็นองค์ประกอบหนึ่งของเครือข่าย SNA ซึ่งเป็น endpoints ของ sessions โดยที่ NAUs ต้องสามารถระบุแอดเดรสได้ตามเครือข่ายโดยใช้แอดเดรสที่เป็น unique ภายในเครือข่ายนั้น ๆ ในระบบ SNA มี NAUs อยู่ 3 แบบ คือ

- Logical Unit (LU)
- Physical Unit (PU)
- System Services Control Point (SSCP)

2.1.5.1 Logical Units

Logical Unit (LU) เป็น access point ที่อยู่นอกสุดภายในเครือข่าย โดยปกติแล้วพวกเราจะคิดว่า เทอร์มินัลหรือเครื่องพิมพ์เท่านั้นที่เป็น LU แต่จริง ๆ แล้วโปรแกรมแอพพลิเคชันยังเป็น LU ในเครือข่าย SNA ด้วย เป้าหมายสุดท้ายของเครือข่ายคือสร้างความสัมพันธ์ในการทำงานระหว่าง workstation และแอพพลิเคชัน ด้วยเหตุนี้จึงมีการสร้าง LU-LU session ขึ้น

จำนวน LU ระหว่าง workstation และแอพพลิเคชันไม่จำเป็นต้องถูกสร้างขึ้นให้มีจำนวนเท่ากัน เพราะโปรแกรมแอพพลิเคชันบางตัวสามารถมี session หลาย ๆ session ได้พร้อมกัน ซึ่งเรียกว่า parallel LU-LU session การแบ่งหมวดหมู่ของ LU สามารถแบ่งตามความสามารถได้ดังนี้

- LU type 1 : SNA Character String printer (SCS)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- LU type 2 : 3270 Interactive Terminals
- LU type 3 : Data Stream Compatible printer (DSC)
- LU type 6.2 : Applocation programs

2.1.5.2 Physical Units

LU session ต่าง ๆ สามารถถูกจัดการได้โดย Physical Unit (PU) โดยที่ Mainframe processor Communications controller หรือ Cluster controller แทนได้ด้วย PU หน้าที่ของ PU คือ เสนอ LU data ให้แก่ link เพื่อส่งข้อมูล PU สามารถแบ่งออกเป็นกลุ่มต่าง ๆ ดังนี้

- PU type 1 : Legacy distributed systems controller –S/3X
- PU type 2 : Cluster controllers
- PU type 2.1 : Advanced peer-to-peer networking nodes
- PU type 4 : Communication controllers
- PU type 5 : VTAMs

2.1.5.3 System Services Control Points

NAU ชนิดสุดท้าย คือ System Services Control Point (SSCP) หน้าที่ของ SSCP อยู่ภายใน access method ซึ่งอยู่บนระบบ mainframe เช่น VTAM ที่โนดแอเรียย่อยบน host เป็นองค์ประกอบของเครือข่ายอย่างเดียวที่สามารถ “activate” “control” หรือ “inactivate” ทรัพยากรเครือข่ายได้ ในภาษา SNA ภายใต้การควบคุมของ VTAM เรียกว่า “in its domain” เครือข่ายขนาดเล็กที่มีเพียง VTAM เดียวถูกเรียกว่า “single domain” และเครือข่ายที่มี VTAM มากกว่าหนึ่งจะถูกเรียกว่า “multidomain”

2.1.6 Network Addressing

แอดเดรสเครือข่ายระบุถึง NAUs ข่ายเชื่อมโยง และ link stations ในเครือข่าย subarea แอดเดรสเหล่านี้อนุญาตไว้สำหรับ routing ของข่าวสารระหว่าง subareas แอดเดรสเครือข่าย SNA ประกอบด้วยองค์ประกอบ 2 แบบ ดังนี้

- Subarea address
- Element address

Subarea address เป็นหมายเลขเฉพาะที่ถูกกำหนดและถูกแบ่งไว้สำหรับ subarea node ภายในแต่ละโนดที่อยู่ภายในเครือข่าย ซึ่ง VTAM และ NCP จะกำหนด Element address ในช่วงการสร้างระบบและการกระตุ้น (activation) เครือข่ายทำให้แอดเดรสเหล่านี้ไม่มีค่านัยสำคัญให้กับคนที่ทำหน้าที่เป็น operator หรือ user ที่ใช้ SNA ซึ่งยอมให้การกำหนดและการแบ่งชื่อให้แก่ NAU ที่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ถูกกำหนดไว้ด้วย VTAM ที่สัมพันธ์กับแอดเดรสในเครือข่าย SNA ในกรณีนี้ VTAM ทำหน้าที่คล้ายกับ domain name service (DNS)ในช่วงไม่นานมานี้ ความหมายของ subarea address ได้ถูกเปลี่ยนไปโดยถูกนำไปใช้เพื่ออธิบายเป็น network address ซึ่งการเปลี่ยนความหมายนี้ได้ทำให้เกิดความต้องการแอดเดรสของเครือข่ายที่แตกต่างกันซึ่งอยู่ใน Advanced Peer-to-Peer Networking (APPN)

เครือข่าย SNA ถูกสร้างและถูกอธิบายด้วยกระบวนการ offline โดยโปรแกรมที่ถูกสร้างขึ้นและโครงสร้างของคำสั่งจะถูกตรวจสอบก่อนการโหลดข้อมูล ซึ่งผู้เขียนโปรแกรมในระบบ SNA เรียกว่า perform gen ในช่วงเวลาของกระบวนการสร้าง SNA ค่า Network Definition Facility (NDF) ของ NCP จะจัดการกระบวนการแจกจ่ายแอดเดรสจำเพาะแก่ทุก ๆ element ดังอธิบายไว้ใน subarea ซึ่งภายใน 1 เครือข่าย SNA ประกอบด้วย element ต่าง ๆ ซึ่งไม่ใช่แค่ LU เช่น เราต้องระบุแอดเดรสในแต่ละ line ของ SDLC PU และ Token Ring ที่ยึดจับอยู่กับ Line PU และ LU หลังจากการสร้างอุปกรณ์เสร็จสมบูรณ์ การเปลี่ยนแปลงเครือข่ายยังคงถูกต้องการเป็นปกติ เช่นเดียวกับ NCP ก็ไม่สามารถถูกโหลดใหม่ได้โดยปราศจากการสร้างสภาพแวดล้อมที่แบ่งออกเป็นส่วนย่อย เมื่อ resource ต่าง ๆ ถูกผูกติดกับ mainframe VTAM จะทำหน้าที่แจกจ่ายแอดเดรสทั้งหมดให้กับอุปกรณ์ทางกายภาพเหล่านั้นตามจำนวนแอพพลิเคชั่นทั้งหมด เครือข่าย SNA จะทำการกระจายแอดเดรสเหล่านี้ในช่วงที่เครือข่าย SNA ทำการโหลดเครือข่าย ซึ่งเกิดขึ้นเมื่อ VTAM ถูก start ที่ Host และเมื่อสำเนาตัวใหม่ของ NCP ถูกโหลดเข้าไปยัง Front-End Processors (FEPs) ในเครือข่าย SNA มีฟิลด์แอดเดรสขนาด 31 บิท ส่วนแรกของแอดเดรสซึ่งมีขนาด 16 บิท ใช้แสดงหมายเลข subarea และ 15 บิทถัดไปถูกใช้สำหรับแสดง element ซึ่งจะทำให้เราสามารถมี 65,535 subarea และ 32,768 elements ภายใน 1 แอเรียย่อย ในปัจจุบัน VTAM V4 สามารถขยายแอดเดรส element ได้เป็น 1.6 ล้าน elements ต่อ 1 แอเรียย่อย

2.1.7 เส้นทาง (Routes)

เส้นทางเป็นความเชื่อทางตรรกของการเชื่อมต่อทางกายภาพในเครือข่าย เส้นทางในทางตรรกเหล่านี้จึงถูกกำหนดและถูกใช้กับคุณลักษณะที่สามารถบริการเวลาในการตอบสนองที่รวดเร็วและมีเส้นทางสำรองผ่านเครือข่าย เกี่ยวกับค่า priority ในการปิดกั้นในการสร้างและประสิทธิภาพที่จะเกิดขึ้น เส้นทางของ SNA จะยอมให้ session ของเทอร์มินัลมีเวลาในการตอบสนองที่เร็วกว่าเครื่องพิมพ์

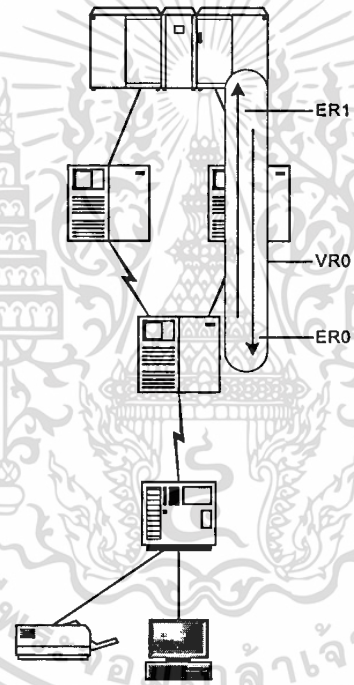
ในการเชื่อมต่อ NCP เข้าด้วยกันสามารถมีการเชื่อมต่อได้มากกว่า 1 การเชื่อมต่อ ถ้าใช้การเชื่อมโยงหลาย ๆ การเชื่อมโยงเรียกว่า การเชื่อมโยงขนาน (Parallel Links) เมื่อการเชื่อมโยงขนานถูกเชื่อมต่อเข้าด้วยกันจะถูกเรียกว่า Transmission Group (TG) ใน 1 TG สามารถมองได้เป็น 1 ข่ายเชื่อมโยง ข่ายเชื่อมโยงตรรก หรือข่ายเชื่อมโยงผสมสำหรับเส้นทาง ภายในเครือข่ายแอเรียย่อย โนด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

PU4 เท่านั้นที่สามารถกำหนดได้หลาย ๆ TG ในขณะที่โนดอื่น ๆ กำหนดได้เพียง TG เดียว ในการกำหนดข่ายเชื่อมโยงเหล่านี้แก่ระบบ เราต้องสร้าง PATH statements ซึ่ง PATH statements เป็นคำนิยามที่ใช้บอก VTAMs และ NCPs เพื่อให้ได้รับ hop ถัดไปในเครือข่าย ใน PATH statement ประกอบด้วยเส้นทางทั้งทางกายภาพและทางตรรก

2.1.7.1 เส้นทางที่แน่นอน (Explicit Routes)

เส้นทางที่แน่นอน (ER) เป็นคำนิยามของการเชื่อมต่อทางกายภาพระหว่าง 2 แอเรียย่อย การเชื่อมต่อทางกายภาพสามารถเป็น communications line หรือ channel ก็ได้ ใน ER นี้จะถูก map เป็น 1 TG ซึ่งสามารถมีหลาย ๆ ER ใน 1 TG โดยทำการแยกวงจรทางกายภาพออกเป็น 2 วงจรที่ประกอบอยู่ใน 1 TG สำหรับสำรองในกรณีที่วงจรใดวงจรหนึ่งเกิดเสียหายขึ้น (ดังรูปที่ 2.3)



รูปที่ 2.3 รูปแบบเส้นทางที่แน่นอนและเส้นทางเสมือน

กฎระเบียบที่เกี่ยวข้องเมื่อทำการกำหนด ER มีดังนี้

- ER ต้องมีช่องทางทั้งขาไปและขากลับ
- ER ต้องตัดผ่านกลุ่มของโนดแอเรียย่อยและ TG เดียวกัน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.1.7.2 เส้นทางเสมือน (Virtual Routes)

เส้นทางเสมือน (VR) หรือที่รู้จักกันว่า เส้นทางตรรก (Logical route) คือการเชื่อมต่อตรรกระหว่างแอเรียย่อย 2 แอเรีย ซึ่งใน 1 VR หรือมากกว่าสามารถถูกแมปเข้าไปใน 1 ER ความสัมพันธ์ระหว่าง VR จำนวนมากต่อ 1 ER นี้ทำให้เกิดความยืดหยุ่นสูงในการควบคุมการเคลื่อนที่ของข้อมูล ประโยชน์หลักของ 1 VR คือเพื่อแยกชนิดของทราฟฟิกชนิดหนึ่งออกจากทราฟฟิกชนิดอื่น ตัวอย่างเช่นการจัดลำดับความสำคัญของเทอร์มินัลไปบนทราฟฟิกของพรินท์เตอร์

2.1.7.3 ตารางระดับของการบริการ (Class of Service Table)

เนื่องจากเรามีเส้นทางมากมายซึ่งจัดหาวงจรตรรกหลาย ๆ วงจรไปบนตัวกลางกายภาพ (physical media) และมีความสามารถในการจัดลำดับความสำคัญของข้อมูลชนิดหนึ่งร่วมไปกับข้อมูลชนิดอื่น ๆ จึงทำให้เกิดคำถามขึ้นว่า ทำอย่างไรเราถึงสามารถระบุชนิดของทราฟฟิกได้ คำตอบที่ได้ก็คือ ตารางระดับของการบริการ (COS) COStab ถูกรวบรวมที่ VTAM และมี 3 ระดับที่สามารถถูกผูกติดกับข้อมูลได้ ได้แก่ ระดับสูง กลาง และต่ำ โดยผู้ใช้จะเป็นผู้กำหนดระดับเอง ในแต่ละ session ที่ถูกสร้างขึ้นจะมีคุณลักษณะผูกติดอยู่กับมัน ซึ่ง 1 ในนั้นคือ ชื่อของ COS

โดยทั่วไปแล้วใน SNA แอเรียย่อย เส้นทางจะเป็นแบบคงที่ซึ่งถูกกำหนดไว้ล่วงหน้าและบรรจุข้อมูลของเพื่อนบ้านที่อยู่ข้างเคียงกัน และถึงแม้ว่าไม่มีกลไกให้กับเครือข่ายของตัวเองทราบถึงการเปลี่ยนแปลงทางเดินและเผยแพร่เส้นทางได้อย่างอัตโนมัติ เราก็สามารถสร้างการเปลี่ยนแปลงและออกคำสั่งการทำงานของ VTAM เพื่ออัพเดตตารางของผู้ที่เกี่ยวข้องเองได้

2.1.8 ลำดับชั้น (Layers)

SNA ถูกสร้างขึ้นตามสถาปัตยกรรมแบบลำดับชั้น โดยในแต่ละลำดับชั้นได้ถูกออกแบบเป็นอิสระจากส่วนอื่น ๆ จนกระทั่งสามารถสื่อสารได้เป็นอิสระ ในรูปที่ 2.4 แสดงรูปแบบ SNA 7 ลำดับชั้น

SNA Stack

Transaction Services Layer
Presentation Services Layer
Data Flow Control Layer
Transmission Control Layer
Path Control Layer
Data Link Control Layer
Physical Control Layer

รูปที่ 2.4 โครงสร้างสถาปัตยกรรมของระบบ SNA

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.1.8.1 Physical Control Layer

ในส่วนนี้อธิบายถึงอินเทอร์เฟสทางกายภาพสำหรับตัวกลางในการส่งผ่านข้อมูลซึ่งกำหนดเป็นคุณลักษณะของสัญญาณทางไฟฟ้า

2.1.8.2 Data Link Control Layer

ในลำดับชั้นที่สองของ SNA แสดงให้เห็นถึงการทำงานของ software/firmware ที่จัดการกับองค์ประกอบทางตรรกของการสื่อสารข้อมูล ที่ Data Link Control Layer แผนการและการกู้ข้อมูลที่ผิดพลาดเกิดขึ้นในโพรโทคอล SDLC และโพรโทคอลในช่องสัญญาณของ OS/390

2.1.8.3 Path Control Layer

ข้อมูลเส้นทางและการเคลื่อนที่ของข้อมูลทั้งหมดถูกควบคุมภายใต้หลักการของช่องทางเดินที่เก็บอยู่ใน Path Control Layer ชนิดของ SNA session ที่แตกต่างกันทั้งหมดใช้หลักการพื้นฐานเหล่านี้เพื่อทำให้รับ-ส่งข้อมูลได้ Path Control Layer มีอยู่ 3 กลุ่มย่อย คือ

- กลุ่ม Transmission ทำหน้าที่จัดหาการเชื่อมต่อระหว่างโนดแอเรียย่อย
- เส้นทางที่แน่นอน ทำหน้าที่เลือก TG ที่จะใช้ระหว่างโนดแอเรียย่อย
- เส้นทางเสมือน ทำหน้าที่จัดหาช่องทางเดินกายภาพที่ซึ่ง session ทางตรรกจะนำพาไป ในขณะที่ session ทางตรรกทำงานอยู่ในเส้นทางของตัวเองผ่านเครือข่าย

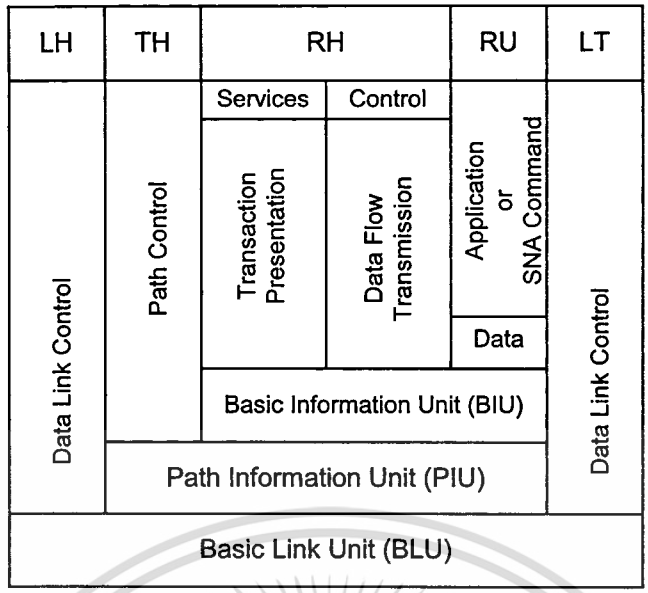
2.1.8.4 Transmission Control Layer

หน้าที่ของ layer นี้คือการส่งมอบข้อมูลที่สามารถนำไปใช้ได้ โดยใช้การตรวจสอบหมายเลขลำดับ (Sequence number checking)

2.1.8.5 Data Flow Control Layer

การเคลื่อนที่ของ session ทั้งหมดระหว่าง LU ถูกจัดการในลำดับชั้นนี้ โดยแพ็กเก็ตของข้อมูลที่ถูกส่งออกไปโดยแอพพลิเคชั่นจะถูกนำพาไปยัง VTAM เพื่อการส่งมอบ ในจุดนี้ VTAM ต้องรวบรวมการร้องขอและการตอบสนองที่เกี่ยวข้องเข้าไปในหน่วยร้องขอ/ตอบสนอง (RU) VTAM สร้างลูกโซ่เพื่อเชื่อมโยงแพ็กเก็ตของข้อมูลเข้าด้วยกันที่มีขนาดใหญ่มาก สำหรับขนาดบัฟเฟอร์ของข้อมูล VTAM จะใช้ bracket เพื่อรักษาสภาพของ session ระหว่าง แอพพลิเคชันกับ LU จนกระทั่งข้อมูลทั้งหมดถูกรับได้ ผลลัพธ์สุดท้ายของข้อมูลถูกเรียกว่า Path Information Unit (PIU) รูปที่ 2.5 แสดง SNA PIU

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 2.5 รูปแบบ SNA Path Information Unit

2.1.8.6 Presentation Services Layer

ในลำดับชั้นนี้ของรูปแบบจำลอง SNA เป็นที่ ๆ ซึ่งโปรแกรมแอพพลิเคชันจะทำการกำหนดคุณลักษณะสำหรับโปรแกรมแอพพลิเคชัน โดยที่คุณลักษณะจะเป็นตัวกำหนดการปรากฏของข้อมูลที่เอาท์พุทด้วยเทอร์มินัล พรินท์เตอร์ หรือแอพพลิเคชัน

2.1.8.7 Transaction Services Layer

Transaction Services Layer ประกอบด้วยกฎระเบียบทั้งหมดสำหรับผู้ใช้งานเพื่อเข้าถึงเครือข่าย และส่งการร้องขอไปยัง Presentation Layer หน้าที่ของการควบคุมและการทำงานยังถูกจัดไว้ในที่นี้ด้วย Session ของ SSCP-to-PU ถูกควบคุมที่ลำดับชั้นนี้และเป็นสิ่งจำเป็นสำหรับการทำงานของเครือข่าย Session ของ SSCP-to-PU ถูกใช้เพื่อกระตุ้นและยกเลิกการกระตุ้น (activate and deactivate) การเชื่อมโยง ใช้เพื่อโหลด software โดเมนเดียวกัน และกำหนดแอดเดรสที่ถูกสร้างขึ้นโดยอิสระ การบริการทางด้านการจัดการได้ถูกกระทำในลำดับชั้นนี้ ซึ่งการบริการเหล่านี้ได้แก่ การ monitor การทดสอบ และการบันทึกสถิติของ session ต่าง ๆ ทั้งหมด

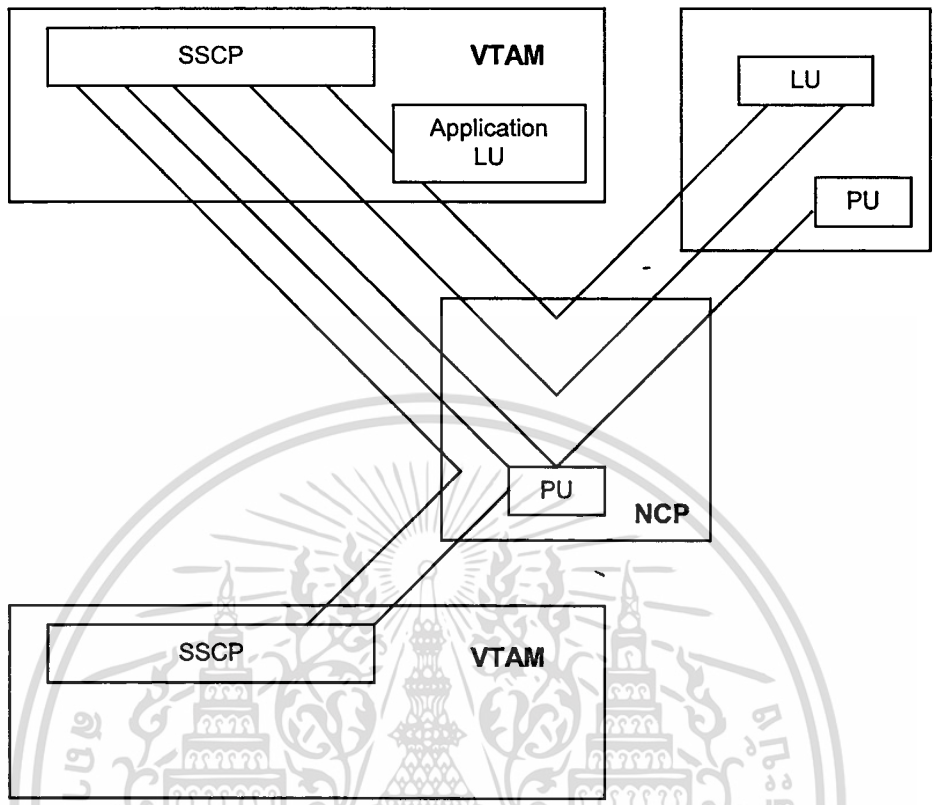
2.1.9 Sessions

Seesion ในโครงสร้างของ SNA มีอยู่ด้วยกัน 4 แบบ ซึ่งรูปที่ 2.6 แสดงตัวอย่างชนิดของ session เหล่านี้

- SSCP to SSCP
- SSCP to PU
- SSCP to LU

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- LU to LU



รูปที่ 2.6 รูปแบบชนิดของ Session ต่างบนระบบ SNA

2.1.9.1 SSCP to SSCP

SSCP to SSCP คือ จุดควบคุมการบริการของ session (Session Services Control Points : SSCP) ของ VTAM ที่สื่อสารกับ VTAM อื่น ๆ Session นี้ถูกใช้เพื่อส่งผ่านข้อมูลจาก VTAM หนึ่งไปยัง VTAM อื่น ๆ ซึ่งโดยปกติจะทำการสร้าง session แบบ LU to LU ในสภาพแวดล้อมแบบข้ามโดเมน ใน session แบบ SSCP to SSCP จะอยู่ในเครือข่ายเดียวกันหรืออยู่กันคนละเครือข่ายก็ได้

2.1.9.2 SSCP to PU

SSCP to PU เป็นการสนทนากันระหว่าง VTAM และตัวควบคุม(controller)รอง ซึ่งตัวควบคุมรองนี้อาจจะเป็นตัวควบคุมการสื่อสารขนาดใหญ่ (FEP-37X5) หรือตัวควบคุม cluster ขนาดเล็ก (3X74) Session นี้ถูกสร้างขึ้นในช่วงกระบวนการ activate ของการโหลดหรือสตาร์ท (Start) เครือข่าย จุดประสงค์หลักสำหรับ session นี้คือทำหน้าที่เป็นท่อนำสำหรับทรัพยากรรอง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในกรณีของ FEP (ทรัพยากรรองที่มีเป็นจำนวนมาก) จะประกอบด้วยส่วนของแอเรียย่อยทั้งหมดของอุปกรณ์ในเครือข่าย สำหรับตัวควบคุม cluster ขนาดเล็กซึ่งเป็นเพียงแค่ LU การร้องขอเกิดจากการ activate/deactivate LU หรือเกิดจากส่งผ่านข้อมูลการจัดการของเครือข่าย

2.1.9.3 SSCP to LU

Session แบบ SSCP to LU เกิดขึ้นในช่วงการ activate/load เครือข่ายเมื่อ LU ปลายทางรับรู้การร้องขอ ในกรณีของเทอร์มินัลหรือเครื่องพิมพ์ การ activate LU เกิดขึ้นเมื่ออุปกรณ์ระยะไกลตอบสนองกับการร้องขอ ACTLU ในกรณีของแอพพลิเคชัน Session นี้ถูกสร้างขึ้นเมื่อ Access Control Block (ACB) ถูก activate

2.1.9.4 LU to LU

การเชื่อมต่อ LU กับ LU เป็นสิ่งที่นิยมกันมากที่สุดและเกี่ยวข้องมากที่สุดกับกลุ่ม MIS ที่มีขนาดใหญ่ หลังจากที่ LU ได้รับการร้องขอจาก VTAM เพื่อเริ่มต้น seesion VTAM จะทำงานซึ่งเป็นงานประจำของตัวมันเองให้เสร็จสมบูรณ์ตามการร้องขอ VTAM จะค้นหาอุปกรณ์/แอพพลิเคชัน (การสร้าง session) ส่งมอบคุณลักษณะแก่กันสำหรับ session (BIND) และดำเนินการขั้นสุดท้ายในการส่งข้อมูลจาก “ที่นี่” ไปสู่ “ปลายทาง”

LU ต่าง ๆ ของแอพพลิเคชันสามารถมีได้มากกว่า 1 session ในเวลาหนึ่ง ๆ เรียกว่า parallel sessions ซึ่งในเหตุการณ์ต่าง ๆ สามารถมองแอพพลิเคชันเป็น LU หลัก (Primary LU :PLU) และเทอร์มินัลหรือเครื่องพิมพ์เป็น LU รอง (Secondary LU : SLU)

2.2 รูปแบบเฟรม SNA/SDLC

ในส่วนนี้กล่าวถึง รายละเอียดรูปแบบของข้อมูลที่ส่งผ่าน SNA กล่าวคือ Data Link Control Layer ซึ่งเป็นเลเยอร์ที่ 2 ของ SNA โดย Synchronous Data Link Control (SDLC) นั้นเป็นวิธีการส่งผ่านข้อมูลอย่างเป็นลำดับและควบคุมได้ สามารถตรวจสอบได้ว่าได้รับข้อมูลอย่างถูกต้องและสามารถส่งข้อมูลซ้ำเมื่อข้อมูลเกิดความผิดพลาด SDLC จะประกอบด้วย 3 รูปแบบ ดังนี้

1. เฟรม Information (I-Frame) ทำหน้าที่ส่งผ่านการร้องขอ และการตอบรับในระบบ SNA
2. เฟรม Supervisory ทำหน้าที่ตอบรับ I-Frame และตอบโต้สถานะของ NAU เช่น พร้อมรับข้อมูลเพิ่มเติม [Receiver Ready (RR)] หรือ ไม่พร้อมรับข้อมูลเพิ่มเติม [Receiver Not Ready (RNR)]
3. เฟรม Unnumbered ทำหน้าที่ส่งผ่านคำสั่ง SDLC เพื่อใช้สำหรับการจัดการเชื่อมโยงข้อมูล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.2.1 Message Unit Formats

ในระบบ SNA รูปแบบของ message unit สามารถแบ่งได้เป็น 3 แบบ ซึ่งขึ้นอยู่กับข้อมูลว่าเดินทางไปตามเส้นทางไหน จุดหมายของข้อมูลจะเป็นตัวบอกว่า message unit นั้นประกอบด้วยส่วนต่าง ๆ ดังนี้

1. Network-Addressable Units (NAUs) ใช้ Basic Information Unit (BIU) เพื่อส่งผ่านข้อมูลระหว่าง NAU อื่น ๆ BIU ถูกสร้างขึ้นจาก LU และ LU ยึดจับกับ Request Header (RH) ไปจนถึง Request Unit (RU) ซึ่ง NAU เท่านั้นที่ใช้ Request Header เมื่อสิ่งนี้ถูกประกอบกัน LU ก็จะส่งสิ่งนี้ไปบน Path Control Layer สำหรับข้อมูลเส้นทางที่เพิ่มขึ้น
2. Path Control Layer อยู่ต่อท้าย Transmission Header (TH) ไปจนถึง BIU ด้วย Transmission Header ที่ยึดจับอยู่ด้วยทำให้ BIU ถูกเลื่อนเป็นขั้นตอนของ Path Information Unit (PIU)
3. จากนั้น Path Control Layer จะส่งผ่านแพ็กเก็ตนี้ไปยังกลไกของ Data Link Control เพื่อการเตรียมส่ง PIU
4. Data Link Layer เพิ่ม Link Header (LH) และ Link Trailer (LT) ให้แก่ PIU
5. ในขั้นตอนนี้ แพ็กเก็ตของข้อมูลได้ถูกรวบรวมเข้าไปในเฟรม SDLC อย่างสมบูรณ์ ซึ่งเรียกว่า Basic Link Unit

2.2.2 Link Header

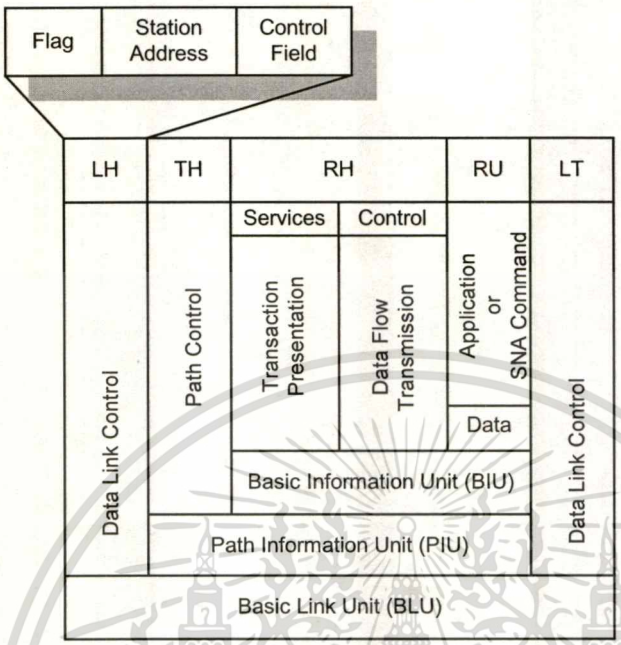
Link Header (LH) ประกอบด้วย 3 ฟิลด์ ดังรูปที่ 2.7 ดังนี้

1. ฟิลด์ Flag
2. ฟิลด์ SDLC station address
3. ฟิลด์ Link Header Control

- ฟิลด์ Flag มีค่าเป็น 7E ของเลขฐานสิบหก ค่านี้ใช้แสดงจุดเริ่มต้นของ SDLC เฟรม
- ฟิลด์ SDLC station address เป็นแอดเดรสของ station เดียว หรือกลุ่มของ station ในกรณีของการคอนฟิกแบบจุดต่อหลายจุดฟิลด์ SDLC station address ใช้แสดงถึงจุดหมายของเฟรม ค่าแอดเดรส FF เป็นค่าที่ใช้สำหรับ broadcast เพื่อแจ้งเตือนหรือใช้ส่งข้อมูลไปยังทุก ๆ station
- ฟิลด์ Link Header Control เป็นฟิลด์ที่สำคัญที่สุดใช้สำหรับอธิบายถึงเนื้อหาของฟิลด์ ซึ่งสามารถแบ่งรูปแบบของฟิลด์เป็น เฟรม unnumbered เฟรม supervisory และเฟรม information โดยที่เฟรม unnumbered เป็นคำสั่งที่ใช้ในการสร้างและยกเลิกการติดต่อ เช่น SNRM DISC และ UA เป็นต้น เฟรม supervisory จะคอยส่งผ่านสถานะของผู้รับ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เช่น RR RNR และ REJ เฟรม Information จะคอยเก็บบันทึกเฟรมที่ถูกส่งออกไปและรับเข้ามา



รูปที่ 2.7 Link header

2.2.3 Transmission Header

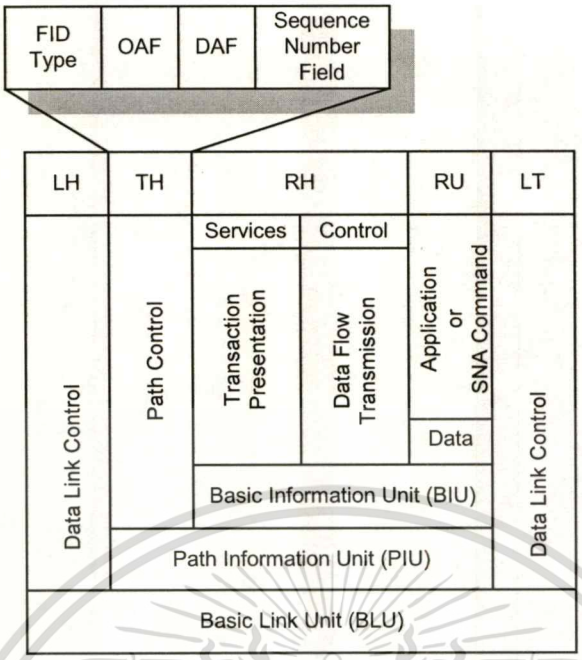
ฟิลด์ Transmission Header (TH) ประกอบด้วย ค่า Format Identifiers (FID) ซึ่งค่านี้สัมพันธ์กับชนิดของ session ที่ใช้ในการสื่อสารและสภาพแวดล้อม โดยสามารถแบ่งได้เป็น ดังนี้

1. Non-SNA FID แบบ Type 0 ใช้สำหรับทราฟฟิกระหว่างโนดข้างเคียงที่ไม่ใช่ SNA
2. PU4 and PU5 FID แบบ Type 1 ใช้กับทราฟฟิก SNA ที่อยู่ระหว่างโนดแอเรียย่อย
3. PU4, PU5, PU2 FID แบบ Type 2 ใช้กับทราฟฟิก SNA ที่อยู่ระหว่างโนดแอเรียย่อยและ PU2.1 ที่อยู่ข้างเคียงกับโนด peripheral
4. PU4 and PU1 FID แบบ Type 3 ใช้สำหรับทราฟฟิก SNA ที่อยู่ระหว่าง NCP กับโนด peripheral PU1
5. PU4 and PU4 FID แบบ Type 4 ใช้สำหรับทราฟฟิก SNA ที่อยู่ระหว่างโนดแอเรียย่อยที่รองรับโพรโทคอลเส้นทางเสมือน (vitrual route protocol)
6. PU4 and PU5 FID แบบ Type F ระบุคำสั่ง SNA ระหว่างโนดแอเรียย่อยที่รองรับโพรโทคอลเส้นทางเสมือนและเส้นทางที่แน่นอน (virtual and explicit route protocols)

โดยส่วนใหญ่แล้ว FID ที่นิยมใช้กันมากที่สุดคือ FID แบบ Type 2 และ 4 ในรูปที่ 2.8 แสดงถึงรูปแบบของ Transmission Header (TH)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สถาบันวิทยบริการ จุฬาลงกรณ์มหาวิทยาลัย



รูปที่ 2.8 รูปแบบเฟรม Transmission header

นอกจากนี้ฟิลด์ TH ยังประกอบด้วยฟิลด์ OAF (Origin Address Field) ฟิลด์ DAF (Destination Address Field) เพื่อบอกถึงจุดเริ่มต้นและจุดหมายของเฟรม และฟิลด์ Sequence number เพื่อแสดงถึงลำดับของ PIU ขนาดของ RU และบอกว่าเฟรมนี้เป็นเฟรมแรก เฟรมกลาง เฟรมสุดท้าย หรือเป็นเพียงแค่เฟรมเดียวของการส่งในครั้งนี้

2.2.4 Request/Response Header

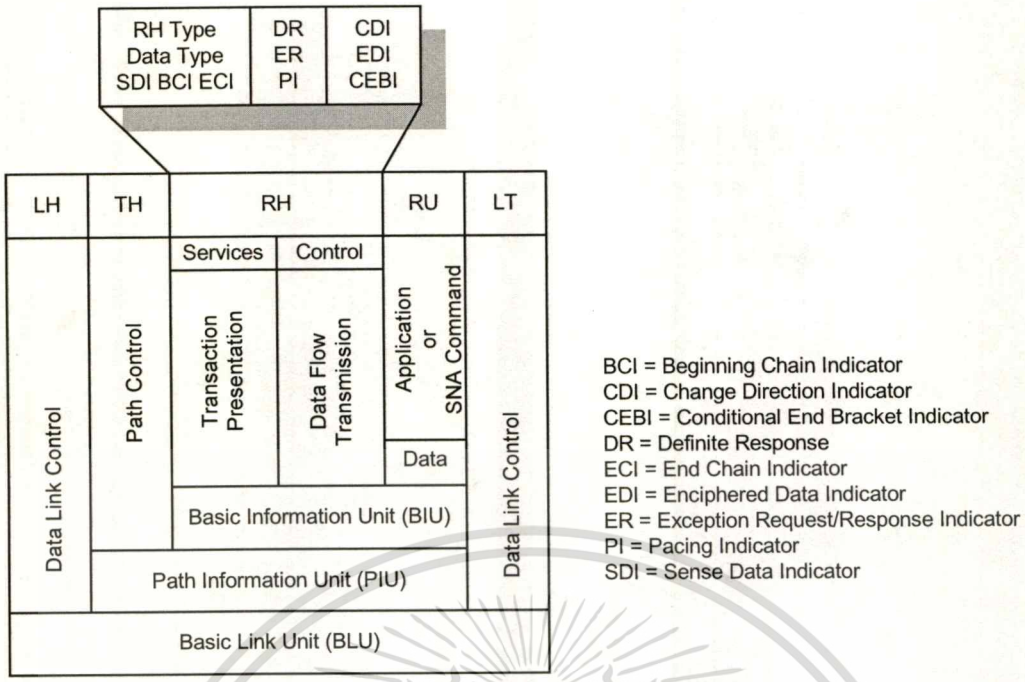
โดยปกติแล้ว TH คือ Header ที่มีขนาด 3 ไบท์ซึ่งแจ้งให้ทราบถึงชนิดของ information ที่ถูกส่งออกไป ชนิดของ header ถูกแสดงด้วยบิทแรก (บิทที่ 0) ถ้าบิท 0 เท่ากับ “0” จะเป็น request header ถ้าบิท 0 เท่ากับ “1” แสดงว่าเป็น response header

Request Header ทำหน้าที่ให้ข้อมูลแก่ PIU ถึงวิธีควบคุม session ซึ่งได้แก่ เวลาในการตอบสนอง การ pacing เครื่องหมาย bracket หรือตำแหน่งในแพ็กเก็ตที่ถูกต่อเป็นลูกโซ่

Response Header ถูกใช้เพื่อให้ข้อมูลที่เหมาะสมกลับไปยังโพรโทคอล SDLC ถ้ามีการตอบสนองเป็นลบเนื่องจากเกิดความผิดพลาดในการส่งข้อมูล Response Header จะบรรจุข้อมูลที่เกี่ยวข้องเกี่ยวกับสาเหตุของความผิดพลาด และทำให้บิท SDI เท่ากับ “1”

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

45889



รูปที่ 2.9 รูปแบบเฟรม Request/Response Header

2.2.5 Request/Response Unit

Request unit (RU) อยู่หลังจาก request header โดยที่ RU สามารถแปรเปลี่ยนความยาวและสามารถบรรจุข้อมูลของผู้ใช้งานหรือคำสั่งของ SNA ได้ โดยทางทฤษฎีแล้ว RU มีขนาดความยาวเป็นอนันต์ แต่ในทางปฏิบัติแล้ว จะต้องมีการจำกัดขนาดของ RU กับขนาดของบัฟเฟอร์ที่อุปกรณ์ปลายทาง โดยทั่วไปเครือข่าย SNA ที่ถูกประกอบด้วยคู่สายอนาลอกความเร็ว 9.6 Kbps กับ 3x74 controller ควรจะมี RU ขนาดเท่ากับ 256 ไบท์

2.2.6 Link Trailer

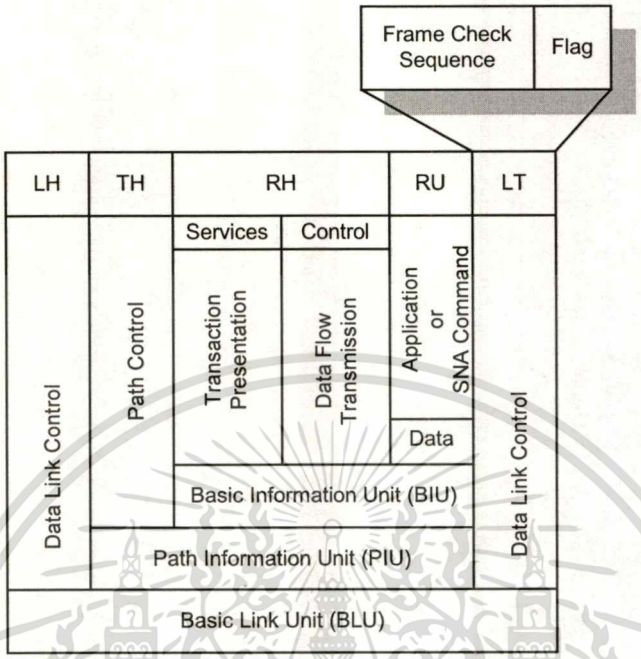
ฟิลด์สุดท้ายของเฟรม SDLC คือ Link Trailer (LT) ซึ่งประกอบด้วย 2 ฟิลด์ (ดังรูปที่ 2.10) ดังนี้

- ฟิลด์ Frame Check Sequence
- ฟิลด์ Link Trailer Flag

ฟิลด์ Frame Check Sequence (FCS) ถูกใช้เพื่อตรวจสอบความถูกต้องของแพ็กเก็ตที่ถูกส่งออกไปและรับเข้ามาในเครือข่าย โดยด้านส่งจะใช้อัลกอลิธึ่มแบบ Cyclic Redundancy Checking (CRC) เพื่อคำนวณหาค่า FCS ซึ่งข้อมูลที่ใช้ในการคำนวณคือ ฟิลด์ Link Header Address ไปจนถึงฟิลด์ RU ทางด้านรับก็จะใช้วิธีการคำนวณเดียวกันกับด้านส่งจากนั้นจะนำผลลัพธ์มาเปรียบเทียบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กับ FCS ถ้าผลลัพธ์ที่ได้ไม่ถูกต้อง ความผิดพลาดจากการส่งจะถูกส่งกลับไปยังผู้ส่งและส่งเฟรมนั้นซ้ำใหม่



รูปที่ 2.10 เฟรม Link Trailer

ฟิลด์ Flag ใช้จุดสิ้นสุดของเฟรม โดยมีค่าเป็น 7E

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 3
การทำงานของโพรโทคอล DLSw และ X.25

3.1 คำนิยามของ DLSw

DLSw [3] เป็นวิธีการส่งผ่านทราฟฟิกของระบบสถาปัตยกรรมเครือข่าย (System Network Architecture, SNA) และ NetBIOS ไปบนแคมปัส หรือเครือข่ายระยะไกล (WAN) โดยที่ปลายทางของระบบสามารถต่อกับเครือข่ายโดยผ่านทาง Token Ring Ethernet โพรโทคอล Synchronous Data Link Control (SDLC) Qualified Logical Link Control (QLLC), หรือ Fiber Distributed Data Interface (FDDI) DLSw+ ทำหน้าที่สวิตช์ระหว่างตัวกลางและสิ้นสุด Data links การ acknowledge ช่วงเวลาของ keepalives และ การ polling ออกจาก WAN ภายในโลคัล การสิ้นสุดภายในโลคัลของ data links ช่วยกำจัดการ timeouts ของ data-link control ที่สามารถเกิดขึ้นในช่วงที่เกิดการแออัดภายในเครือข่ายในช่วงเวลาหนึ่ง หรือเมื่อมีการเปลี่ยนเส้นทางเมื่อข่ายเชื่อมโยงเสียหาย ประการสุดท้าย DLSw+ ยังจัดเตรียมกลไกสำหรับค้นหาเครือข่ายสำหรับทรัพยากรแบบ SNA หรือ NetBIOS ไว้อย่างอิสระ รวมถึงอัลกอลิธึ่มแบบแคสที่ทำให้ทราฟฟิกแบบ broadcast มีน้อยลง

DLSw+ สามารถรองรับวงจรระหว่าง SNA physical units (PUs) หรือ ระหว่าง clients และ servers ของ NetBIOS การเชื่อมต่อที่สามารถรองรับได้ระหว่าง SNA PU ได้แก่ PU 2.0/2.1- to-PU 4, PU 1-to-PU 4, PU 4-to-PU 4 และ PU 2.1-to-PU 2.1

3.2 มาตรฐานของ DLSw

มาตรฐานของ DLSw อธิบายถึงโพรโทคอล Switch-to-Switch (SSP) ที่ใช้ระหว่างเราท์เตอร์ ซึ่งเรียกว่า data-link switches เพื่อสร้างการเชื่อมต่อของ DLSw ชี้ตำแหน่ง resources ส่งผ่านข้อมูล จัดการกับ flow control และกู้ข้อมูลในส่วนที่ผิดพลาด (error recovery) RFC1795 กำหนดไว้ว่าการเชื่อมต่อของ data-link ต้องสิ้นสุดที่ peer routers เช่น ใน Token Ring การเชื่อมต่อของ data-link ได้ถูก acknowledge ภายในโลคัลและฟิลด์ของข้อมูลในการสร้างเส้นทาง (Routing Information Field ; RIF) ซึ่งสิ้นสุดที่ virtual ring ใน peering router

ในการเชื่อมต่อของ Data-link control ที่มีการสิ้นสุดภายในโลคัล ทำให้ DLSw ไม่ต้องการ acknowledgment ที่ระดับ link layer และช่วงเวลาของ keepalive ที่ข้ามผ่าน WAN และนอกเหนือจากนี้ เพราะว่า เฟรมของ link-layer ถูก acknowledge ภายในโลคัลจึงทำให้ ไม่เกิดการ timeouts ในช่วงของ link-layer หน้าที่ของ DLSw routers คือการมัลติเพล็กซ์ทราฟฟิกของ data-link controls ต่าง ๆ เข้าไปในท่อ TCP ที่เหมาะสมและส่งผ่านข้อมูลอย่างเชื่อถือได้ไปบน IP backbone โดยก่อน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ที่การสื่อสารระหว่าง end-system ซึ่งข้ามผ่านด้วย DLSw ได้นั้น จะต้องเกิดขบวนการต่าง ๆ เหล่านี้ดังนี้

- สร้าง Peer Connections
- แลกเปลี่ยน Capabilities
- สร้างวงจร
-

3.3 การสร้าง Peer Connections

ก่อนที่เราท์เตอร์ 2 ตัวจะสามารถสวิทช์ SNA หรือ NetBIOS ทราฟฟิกได้นั้น เราท์เตอร์ทั้ง 2 ตัวจำเป็นต้องสร้างการเชื่อมต่อ TCP ระหว่างกันก่อน ซึ่งตามมาตรฐานแล้ว การเชื่อมต่อของ TCP ทุก ๆ TCP สามารถถูก drop ลงได้ถ้าหากไม่มีความจำเป็น และ DLSw ที่เป็นมาตรฐานยังยอมให้การเชื่อมต่อของ TCP ถูกสร้างขึ้นได้ตามระดับของค่า Priority

3.4 การแลกเปลี่ยน Capabilites

หลังจากที่การเชื่อมต่อของ TCP ถูกสร้างขึ้น เราท์เตอร์จะทำการแลกเปลี่ยนค่า Capability ต่าง ๆ ซึ่งได้แก่ ค่าเวอร์ชั่นของ DLSw ขนาดของ window การรองรับของ NetBIOS รายชื่อของ service access points (SAPs) และจำนวน session ของ TCP ที่รองรับได้ ตลอดจนรายชื่อ address ของ Media Access Control (MAC) และรายชื่อของ NetBIOS ยังสามารถถูกแลกเปลี่ยนได้ในช่วงเวลานี้ด้วย ในกรณีที่ต้องการ DLSw partner สามารถระบุว่าไม่ต้องการรับเฟรมที่เป็นเฟรมค้นหาได้ และเป็นไปได้ที่จะทำการ configure ค่า MAC address และ ชื่อของ NetBIOS ต่าง ๆ ของทุก ๆ resource ที่จะใช้ DLSw ซึ่งสามารถหลีกเลี่ยงการ broadcast ได้ หลังจากที่มีการแลกเปลี่ยน Capabilities แล้ว DLSw partner ก็พร้อมที่จะสร้างวงจรระหว่างระบบปลายทางของ SNA หรือ NetBIOS

3.5 การสร้างวงจร

การสร้างวงจรระหว่างระบบประกอบด้วย การชี้ตำแหน่งของ resource เป้าหมาย (ขึ้นอยู่กับ MAC address หรือชื่อของ NetBIOS ด้านปลายทางของตัวมันเอง) และการ setup การเชื่อมต่อของ data-link control ระหว่างระบบปลายทางกับ data-link switch ของตัวเอง (ภายในโลคัลเราท์เตอร์) ซึ่ง SNA และ NetBIOS มีการจัดการที่แตกต่างกัน อุปกรณ์ SNA ต่าง ๆ บน LAN หนึ่ง ๆ จะทำการค้นหาอุปกรณ์ SNA อื่น ๆ โดยการส่งเฟรมสำรวจ (เฟรม test หรือเฟรม exchange identification ; XID ไปกับ MAC address ของอุปกรณ์ SNA ที่เป็นเป้าหมาย เมื่อ DLSw เราท์เตอร์ได้รับเฟรมสำรวจแล้ว เราท์เตอร์จะส่งเฟรมซึ่งเรียกว่า เฟรม canureach (can-u-reach)ไปยังทุก ๆ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

DLSw partners ถ้า 1 ใน DLSw partner สามารถไปถึง MAC address ที่ระบุไว้ได้ Partner ก็จะตอบกลับด้วยเฟรมซึ่งเรียกว่า เฟรม icanreach (I-can-reach) ลำดับจำเพาะประกอบด้วย canureach ex (explorer) เพื่อหา resource และ canureach cs (circuit setup) เพื่อทริกให้ peering router สร้างวงจร

ในขณะนี้ DLSw partner ได้สร้างวงจรขึ้น 1 วงจร ซึ่งประกอบด้วยการเชื่อมต่อ 3 ชนิด คือ การเชื่อมต่อ 2 วงจรของ data-link control ระหว่างเราท์เตอร์แต่ละตัวกับระบบ SNA ที่ต่อกันภายใน และการเชื่อมต่อของ TCP ระหว่าง DLSw partner ด้วยกัน ซึ่งการเชื่อมต่อของ TCP กับ DLSw นี้ ถูกระบุโดย ID ของวงจรต้นทางและ ปลายทาง ซึ่งทั้งหมดจะถูกนำพาไปในรูปแบบของ data-link control address เช่น MAC address เป็นต้น ID ของวงจรในแต่ละวงจรถูกกำหนดขึ้นโดย MAC address ของปลายทางและ ต้นทาง Link service access points ของ ปลายทางและต้นทาง (LSAPs) และ Port ID ของ data-link control แนวความคิดของวงจรคือ ทำให้ง่ายต่อการจัดการ และมีกระบวนการในการกำจัดข้อผิดพลาด (error) ซึ่งหลังจากวงจรได้ถูกสร้างขึ้น เฟรมของข้อมูลก็จะสามารถเคลื่อนที่ผ่านไปในวงจรได้

การสร้างวงจร NetBIOS ก็คล้ายกับการสร้างวงจรของ SNA แต่แทนที่จะมีการส่งเฟรม canureach ที่ระบุ MAC address เราท์เตอร์ DLSW จะทำการส่งเฟรมซักถามชื่อ (NetBIOS NAME-QUERY) ที่ระบุ ชื่อของ NetBIOS และแทนที่จะส่งเฟรม icanreach ก็จะทำการส่งเฟรมรู้จักชื่อ (NetBIOS NAME-RECOGNIZED)

3.6 Flow Control

DLSw flow control เกี่ยวข้องกับการเคลื่อนที่ซึ่งสามารถปรับเปลี่ยนได้ (adaptive pacing) ระหว่างเราท์เตอร์ DLSw ด้วยกัน ในช่วงของกลไกการเจรจาของ flow control กลไกความอิสระ 2 แบบ กลไก flow control แบบทิศทางเดียวได้ถูกสร้างขึ้นระหว่าง DLSw partner กับ partner การเคลื่อนที่ซึ่งสามารถปรับเปลี่ยนได้ใช้กลไก window เพื่อปรับเปลี่ยน buffer ได้อย่างอิสระ Window สามารถเพิ่ม ลด แบ่งครึ่ง หรือรีเซ็ทเป็นศูนย์ ซึ่งจะทำให้ DLSw nodes สามารถควบคุมการเคลื่อนที่ของทราฟฟิกที่เคลื่อนที่ผ่านเครือข่าย เพื่อทำให้เกิดความน่าเชื่อถือและการส่งมอบข้อมูลได้ทั้งหมด

3.6.1 DLSw Flow Control Indicators

Granted units (คือจำนวนหน่วยที่ผู้ส่งมีสิทธิส่งได้) ได้ถูกเพิ่มขึ้นตามตัวบ่งชี้ของ flow control (ตัวบ่งชี้แบบหนึ่ง) จากผู้รับ ซึ่งตัวบ่งชี้สามารถแบ่งออกเป็นชนิดต่างๆ ได้ดังนี้

- Repeat : เพิ่ม granted units ตามขนาดของ window ปัจจุบัน
- Increment : เพิ่มขนาดของ window ขึ้น 1 ขนาด และเพิ่ม granted units ตามขนาดของ window ใหม่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

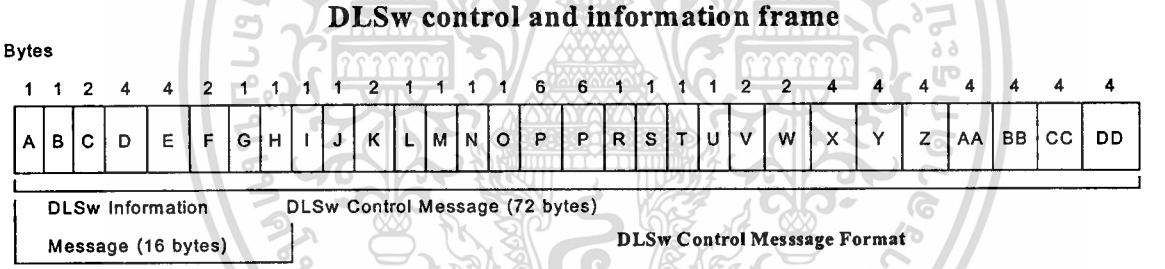
- Decrement : ลดขนาดของ window ลง 1 ขนาด และเพิ่ม granted units ตามขนาดของ window ใหม่
- Reset : ลด window เป็นศูนย์และเซ็ท granted units เป็นศูนย์ ซึ่งหยุดการส่งทั้งหมดใน 1 ทิศทาง จนกระทั่ง Increment indicator ถูกส่ง
- Half : ลดขนาดของ window ในปัจจุบันเหลือครึ่งหนึ่ง และเพิ่ม granted unit ตามขนาดของ window ใหม่

ตังบ่งชี้ Flow Control และการรับรู้ Flow Control สามารถถูกบรรทุกไปบนเฟรมข่าวสาร หรือถูกส่งเป็น flow control messages อิสระได้ แต่ตัวบ่งชี้ Reset ต้องถูกส่งเป็น message อิสระเสมอ

3.7 DLSw Message Formats

รูปแบบ header ของ message ที่ถูกแลกเปลี่ยนกันระหว่าง DLSw nodes มีอยู่ 2 รูปแบบดังนี้

- Control
- Information



DLSw Information Message (16 bytes)

A= Version number
B= Header length
C= Message length
D= Remote data-link correlator
E= Remote data-link control
F= Reserved
G= Message type
H= Flow-control byte

A= Version number
B= Header length
C= Message length
D= Remote data-link correlator
E= Remote data-link control (DLC) port ID
F= Reserved
G= Message type
H= Flow-control byte
I= Protocol ID
J= Header number
K= Reserved
L= Largest frame size
M= SSP flags
N= Circuit priority
Q= Message type

P= Target MAC address
Q= Origin MAC address
R= Origin link service access point (LSAP)
S= Target LSAP
T= Frame direction
U= Reserved
V= Reserved
W= Data-link-control (DLC) port ID
Y= Origin data-link-control (DLC) port ID
Z= Origin transport ID
AA= Target data-link correlator
CC= Target transport ID
DD= 2 reserved fields

รูปที่ 3.1 รูปแบบเฟรม DLSw Information Message และ DLSw Control Message

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Header ของ Control Message ถูกใช้กับทุก ๆ message ยกเว้น information frames (I frames) และ independent flow control messages (IFCMs) ซึ่งถูกส่งไปใน inframation header format ในรูปที่ 3.1 แสดงถึงรูปแบบของฟิลด์ DLSw Control และ Information

- Version Number : เมื่อเซ็ทเป็น 0x31 (ASCII 1) (มีค่าเท่ากับ 49 ในเลขฐานสิบ) ซึ่งระบุว่าอุปกรณ์นี้เป็น DLSw version 1
- Header Length : เมื่อเซ็ทเป็น 0x48 สำหรับ control messages (เท่ากับ 72 ไบท์ในเลขฐานสิบ) เมื่อค่านี้ถูกเซ็ทเป็น 0x10 สำหรับ information และ information flow control messages (เท่ากับ 16 ไบท์)
- Message Length : กำหนดจำนวนไบท์ภายในฟิลด์ข้อมูลที่ตามหลัง header
- Remote Data-Link Correlator : ทำงานควบคู่กับ Remote DLC Port ID ในรูป Circuit ID ขนาด 64 บิท ซึ่งระบุวงจร DLC ภายใน DLSw node เพียง node เดียว ID ของวงจรเป็นหมายเลขเฉพาะใน DLSw node และถูกกำหนดขึ้นภายใน วงจรระหว่างต้นทางถึงปลายทางถูกระบุโดยวงจร ID 1 คู่ที่ระบุหมายเลขเฉพาะให้กับวงจรต้นทางและปลายทาง ซึ่ง DLSw node ในแต่ละ node ต้องเก็บตารางที่บรรจุคู่ ID ของวงจรเหล่านี้ไว้ ค่าของ Remote data-link correlator ถูกเซ็ทให้เท่ากับค่า Target data-link correlator ก็ต่อเมื่อฟิลด์ของ Frame Direction ถูกเซ็ทเป็น 0x01 และค่าของ Remote data-link correlator มีค่าเท่ากับ Orioin data-link correlator ก็ต่อเมื่อฟิลด์ Frame Direction เป็น 0x02
- Remote DLC Port ID – ทำงานร่วมกับค่า Remote data-link correlator ในรูป Circuit ID ขนาด 64 บิท ซึ่งระบุวงจร DLC ไว้ภายใน DLSw node โดย ID วงจรเป็นหมายเลขเฉพาะใน DLSw node และถูกกำหนดอยู่ภายใน วงจรระหว่างต้นทางถึงปลายทางถูกระบุโดยวงจร ID 1 คู่ที่ระบุหมายเลขเฉพาะให้กับวงจรต้นทางและปลายทาง ซึ่ง DLSw node ในแต่ละ node ต้องเก็บตารางที่บรรจุคู่ ID ของวงจรเหล่านี้ไว้ ค่าของ Remote DLC Port ID ถูกเซ็ทให้เท่ากับค่า target DLC Port ID ก็ต่อเมื่อฟิลด์ Frame Direction ถูกเซ็ทเป็น 0x01 และค่าของ Remote DLC Port ID จะเท่ากับค่า origin DLC Port ID ก็ต่อเมื่อฟิลด์ Frame Direction ถูกเซ็ทเป็น 0x02
- Message Type : แสดงถึงชนิดของ DLSw message ค่านี้จะถูกกำหนดอยู่ในฟิลด์ที่ต่างกัน 2 ฟิลด์ (offset 14 และ 23 ในรูปของเลขฐานสิบ) ของ control message header ฟิลด์แรกถูกใช้ในการกระจาย SSP message ที่รับได้ ฟิลด์ที่สองถูกปล่อยละเลยไว้กับวิธีการตอบรับแบบใหม่แต่ถูกรักษาไว้เพื่อให้เข้ากันได้กับวิธีการของ RFC 1434 และสามารถนำมาใช้ได้กับเวอร์ชั่นในอนาคตได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- Flow-Control Byte : นำพาตัวบ่งชี้ flow-control การรับรู้ flow-control และบิท operator ของ flow-control
- Protocol ID : เมื่อเซ็ทเป็น 0x42 แสดงค่าเลขฐานสิบเท่ากับ 66
- Header Number : เมื่อเซ็ทเป็น 0x01 แสดงค่าเท่ากับ 1
- Largest Frame Size : นำพาบิทที่แสดงถึงขนาดของเฟรมที่ใหญ่ที่สุดข้ามผ่านการเชื่อมต่อ DLSw ฟิลด์นี้ถูกใช้เพื่อทำให้แน่ใจว่าสถานีปลายทาง 2 สถานีตกลงกันด้วยขนาดของเฟรมที่ใช้กับวงจรที่ไม่ต้องการ DLSw partners เพื่อการ resegment เฟรม
- SSP Flags : ประกอบด้วยข้อมูลเพิ่มเติมของ SSP ดังแสดงไว้ในตารางที่ 3.1 (บิทที่ 7 เป็นบิทที่มีค่านัยสำคัญที่มากที่สุด และบิท 0 เป็นบิทที่มีค่านัยสำคัญน้อยที่สุด)

ตารางที่ 3.1 ความหมายของแฟลก SSP

ตำแหน่งบิท	ชื่อ	ความหมาย
7	SSPex	1 = Explorer message (canureach หรือ icanreach)
6 ถึง 0	Reserved	ไม่มีความหมาย ฟิลด์ที่ถูกสำรองไว้จะถูกเซ็ทเป็น 0 สำหรับการส่งและเป็นค่าอะไรก็ได้ในการรับ

- Circuit Priority : ใช้จัดลำดับค่า priority ของวงจรว่าเป็นแบบไม่รองรับ (unsupport) แบบต่ำ แบบกลาง แบบสูง และแบบสูงที่สุด
- Target MAC Address : เป็นค่าที่รวบรวมมาจากค่า Target Link SAP ค่า Origin MAC address และค่า Origin SAP เพื่อกำหนดความสัมพันธ์ของการเชื่อมโยงจากต้นทางไปยังปลายทางในเชิงตรรก ซึ่งเรียกว่า Data-link ID
- Origin MAC Address : รองรับตามค่า MAC address ของสถานีที่กำเนิดแพ็กเก็ต
- Origin LSAP : รองรับตามค่า SAP ของอุปกรณ์ต้นทาง
- Target LSAP : รองรับตามค่า SAP ของอุปกรณ์ปลายทาง
- Frame Direction : บรรจุค่า 0x01 สำหรับเฟรมที่ส่งจาก DLSw ตัวต้นกำเนิดไปยังโนด DLSw เป้าหมาย หรือมีค่า 0x02 สำหรับเฟรมที่ส่งจาก DLSw เป้าหมายไปยังโนด DLSw ที่กำเนิดเฟรม
- DLC Header Length : มีค่าเป็น 0 สำหรับ SNA และมีค่าเป็น 0x23 สำหรับ NetBIOS ซึ่งมีความยาวเท่ากับ 35 ไบท์ Header ของ NetBIOS มีข้อมูลต่าง ๆ ดังนี้
    - ฟิลด์ Access Control (AC)
    - ฟิลด์ Frame Control (FC)
    - ค่า MAC Address ปลายทาง (DA)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- ค่า MAC Address ต้นทาง (SA)
- ฟิลด์ Routing Information (RI)
- Destination service access point (DSAP)
- Source SAP (SSAP)
- ฟิลด์ LLC control (UI)

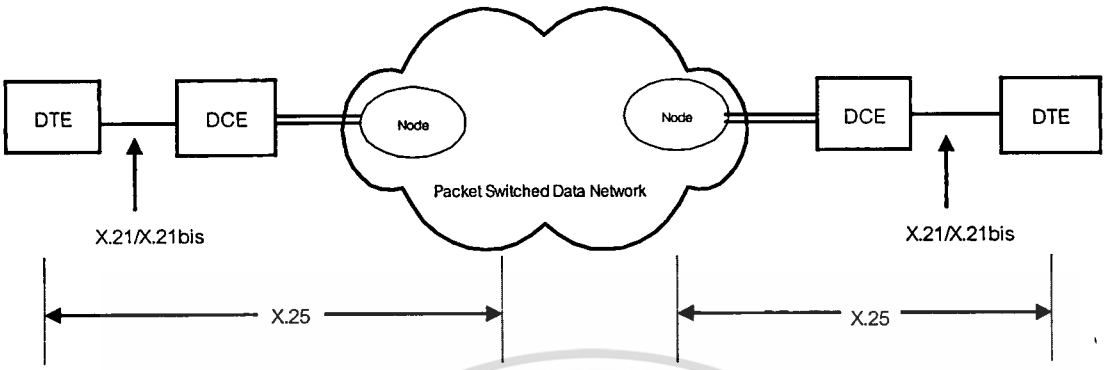
- Origin DLC Port ID : ทำงานควบคู่กับ origin data-link correlator ในรูปแบบ circuit ID ขนาด 64 บิท ซึ่งระบุวงจร DLC ภายในโนด DLSw โนดเดียว Circuit ID เป็นหมายเลขเฉพาะที่อยู่ในโนด DLSw โนดเดียวและถูกกำหนดไว้ภายในโลคัล วงจรระหว่างต้นทางถึงปลายทางถูกระบุโดย Circuit ID 1 คู่ ที่บ่งชี้วงจรต้นทางถึงปลายทาง 1 วงจร ภายในโนด DLSw แต่ละโนดต้องเก็บตารางของ Circuit ID ที่เป็นคู่ เหล่านี้ไว้ ซึ่งประกอบด้วยวงจรของต้นทาง และวงจรของปลายทาง
- Origin Data-Link Correlator : ทำงานร่วมกันกับ origin DLC port ID ในรูปแบบ circuit ID ขนาด 64 บิท ซึ่งระบุวงจร DLC ภายในโนด DLSw โนดเดียว Circuit ID เป็นหมายเลขเฉพาะที่อยู่ในโนด DLSw โนดเดียวและถูกกำหนดไว้ในโลคัล วงจรระหว่างต้นทางถึงปลายทางถูกระบุโดย Circuit ID 1 คู่ ที่บ่งชี้วงจรต้นทางถึงปลายทาง โนด DLSw ในแต่ละโนดต้องเก็บตารางของ Circuit ID ที่เป็นคู่ไว้ ซึ่งประกอบด้วยวงจรของต้นทาง และวงจรของปลายทาง
- Origin Transport ID : ระบุพอร์ท TCP/IP บนโนด DLSw
- Target Data-Link Correlator : ทำงานร่วมกันกับ Target DLC port ID ในรูปแบบ circuit ID ขนาด 64 บิท ซึ่งระบุวงจร DLC ภายในโนด DLSw โนดเดียว Circuit ID เป็นหมายเลขเฉพาะที่อยู่ในโนด DLSw โนดเดียวและถูกกำหนดไว้ในโลคัล วงจรระหว่างต้นทางถึงปลายทางถูกระบุโดย Circuit ID 1 คู่ ที่บ่งชี้วงจรต้นทางถึงปลายทาง โนด DLSw ในแต่ละโนดต้องเก็บตารางของ Circuit ID ที่เป็นคู่ไว้ ซึ่งประกอบด้วยวงจรของต้นทาง และวงจรของปลายทาง
- Transport ID : ระบุพอร์ท TCP/IP บนโนด DLSw

3.8 Protocol X.25

X.25 [2] เป็นมาตรฐานสากลเกี่ยวกับโพรโทคอลที่ใช้ในการติดต่อไปยังเครือข่ายการสวิตช์กลุ่มข้อมูล (Packet Switching Networks) เช่น การเริ่มต้นเรียกการติดต่อ การส่งผ่านข้อมูล และการยกเลิกการติดต่อเมื่อข้อมูลถูกส่งผ่านไปเรียบร้อย ซึ่งตามข้อกำหนดของ CCITT ได้ระบุเอาไว้ว่า “ เป็นการต่อประสาน (Interface) ระหว่าง Data Terminal Equipment (DTE) กับ Data

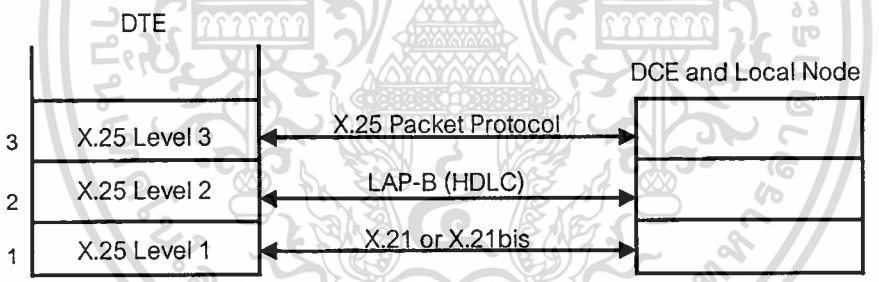
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Circuit-terminating Equipment (DCE) โดยที่อุปกรณ์ปลายทางทำงานแบบแพ็กเกต ภายในโครงข่ายข้อมูลสาธารณะ (Public Data Network)"



รูปที่ 3.2 การเชื่อมต่อ X.25

X.25 ถูกกำหนดรูปแบบของข้อมูลที่แลกเปลี่ยนข้ามระหว่าง DTE-DCE โดยเปรียบเทียบกับ OSI Model (Open System Interconnection) ไว้ที่ระดับ 1, 2 และ 3 หรือ ระดับ Physical, ระดับ Data Link และ ระดับ แพ็กเกต



รูปที่ 3.3 X.25 จำนวน 3 ระดับ เมื่อเปรียบเทียบกับ OSI Model

3.8.1 X.25 ระดับ 1 (Physical layer)

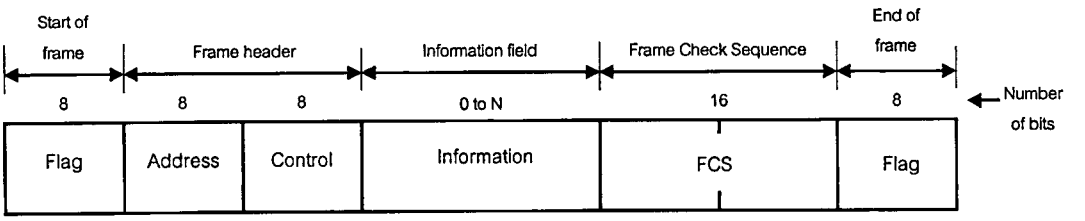
เป็นมาตรฐานที่กำหนดขึ้นเกี่ยวกับสัญญาณทางไฟฟ้าในการต่อประสาน (Interface) รวมถึงการกำหนด Pin ในการเชื่อมต่อระหว่าง DTE กับ DCE โดยใช้มาตรฐาน X.21 หรือ X.21 bis ซึ่งใช้ในโครงข่ายสื่อสารข้อมูลแบบดิจิตอล (Digital) และแอนะลอก (Analog) ตามลำดับ

3.8.2 X.25 ระดับ 2 (Data Link layer)

เป็นข้อกำหนดในการรับ-ส่งข้อมูล โดยมีการตรวจหาความผิดพลาดของข้อมูล (Error detection) และ การกู้ข้อมูลที่ผิดพลาด (Error correction) โดยใช้ขบวนการ Link Access Procedure

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Balanced (LAP-B) ซึ่งเป็นส่วนหนึ่งของ โพรโทคอลแบบ High-level Data Link Control (HDLC) ตามมาตรฐานของ International Standardization Organization (ISO)



รูปที่ 3.4 รูปแบบเฟรมของโพรโทคอล HDLC

- Flag : โดยปกติใช้ 7E (Hex) เป็น Synchronization Character เป็นส่วนที่บอกถึง จุดเริ่มต้นและจุดสิ้นสุดของเฟรม

- Address : ใน LAP-B ถูกใช้ในการชี้ทิศทางของ Command และ Response ที่ส่งมาจาก DTE และ DCE ตาม modulo 08 ดังตารางที่ 3.2

ตารางที่ 3.2 Address ของ Command และ Response

Direction	Address	
	Commands	Responses
DTE → DCE	01 Hex (B)	03 Hex (A)
DCE → DTE	03 Hex (A)	01 Hex (B)

จากตารางที่ 3.2 จะเห็นว่าถ้า Address มีค่า 01 จะทำให้ Command ถูกส่งโดย DTE และรอ Response จาก DCE

- Control : สามารถแบ่งรูปแบบ (Format) ได้เป็น 3 แบบ ดังนี้

1. Unnumbered frames จะใช้ในขั้นตอนของการ Setup และยกเลิกการติดต่อ ได้แก่ SABM (Set Asynchronous Balanced Mode), DISC (Disconnect), UA (Unnumbered Acknowledge), DM (Disconnect Mode), FRMR (Frame Reject)

2. Information frames ได้แก่ I - frame ซึ่งประกอบด้วย N(S) แสดงจำนวนเฟรมที่ส่ง และ N(R) ซึ่งแสดงจำนวนเฟรมที่ได้รับ มีค่าตั้งแต่ 0 - 7

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3. Supervisory frames ถูกใช้สำหรับควบคุมข้อผิดพลาด (Error control) และ ควบคุมปริมาณของเฟรม (Flow Control) ได้แก่ RR (Receiver Ready), RNR (Receiver Not Ready), REJ (Reject)

ตารางที่ 3.3 รูปแบบต่าง ๆ ใน Control field

Category	Commands	Responses	Control Field								Hex	
			7	6	5	4	3	2	1	0	P/F=1	P/F=0
I-Frame	I		r	r	r	P	s	s	s	0	even	even
S-Frame	RR	RR	r	r	r	P/F	0	0	0	1	x [1] 1	x [2] 1
	RNR	RNR	r	r	r	P/F	0	1	0	1	x [1] 5	x [2] 5
	REJ	REJ	r	r	r	P/F	1	0	0	1	x [1] 9	x [2] 9
U-Frame		DM	0	0	0	F	1	1	1	1	1F	0F
	SABM		0	0	1	P	1	1	1	1	3F	2F
	DISC		0	1	0	P	0	0	1	1	53	43
		UA	0	1	1	F	0	0	1	1	73	63
		FRMR	1	0	0	F	0	1	1	1	97	87

r = receive counter

s = send counter

F= final bit

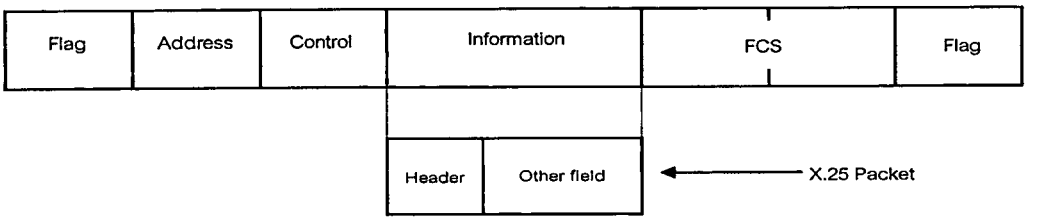
1) odd number

2) even number

P/F bit (Poll / Final bit) จะถูกเรียกว่า Poll bit เมื่อถูกใช้ใน Command frame (ส่งโดย Primary station) เมื่อถูก set จะชี้ว่า ผู้รับจะต้องตอบรับเฟรมนี้ เมื่อผู้รับตอบรับ Command frame แล้วจะตอบกลับด้วย Response frame (ส่งโดย Secondary station) ที่เหมาะสม ด้วยการ set P/F bit ซึ่งเรียกว่า Final bit

- Information : เป็นส่วนหนึ่งของ X.25 Packet และ ข้อมูลที่ต้องการส่ง
- FCS : เป็นส่วนที่ไว้ใช้ในการตรวจเช็คความผิดพลาดของข้อมูลภายในเฟรม

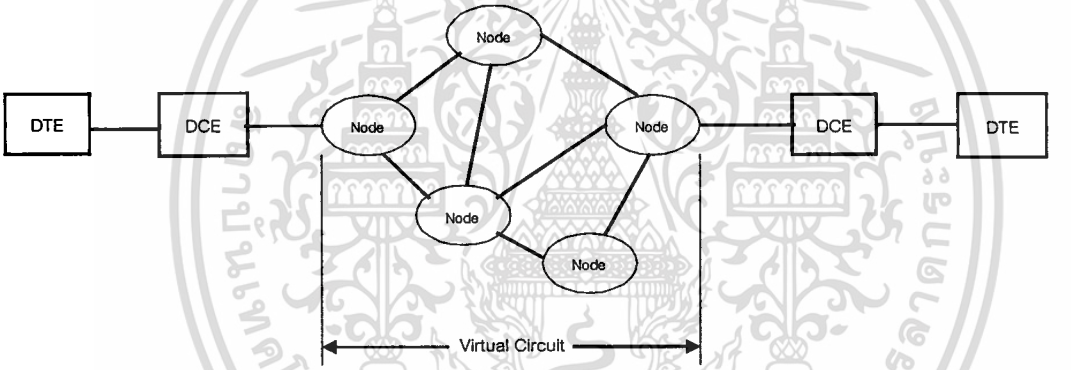
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.5 ตำแหน่งของ X.25 Packet ในเฟรม HDLC

3.8.3 X.25 ระดับ 3 (Packet Layer)

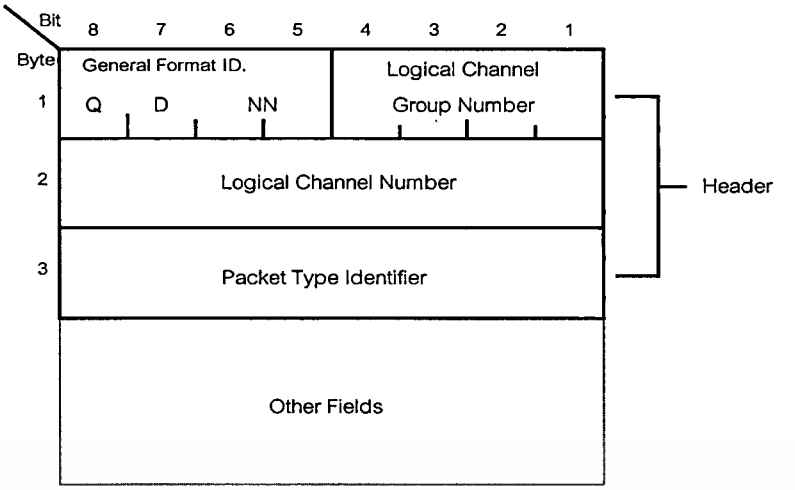
Packet Layer เทียบเท่าได้กับ Network Layer ตามมาตรฐาน OSI Model ทำหน้าที่รับข้อมูลจาก Data Link layer มาเพื่อจัดระบบเป็นวิถีเสมือน (Virtual path) ทำการแยก และควบคุมข้อมูลให้สามารถใช้ได้กับผู้เช่า (Subscriber) เช่น ขนาดของแพ็กเกต (Packet Size), การควบคุมการส่งผ่าน (Flow Control)



รูปที่ 3.6 วงจรเสมือน

ข้อมูลที่ถูกแบ่งออกเป็นแพ็กเกตจะถูกส่งผ่านไปบนวงจรเสมือน ซึ่งถูกสร้างโดย Packet Layer โดยสามารถแบ่งวงจรเสมือน ได้เป็น 2 ชนิด คือ Virtual Call (VC) หรือ Switch Virtual Circuit (SVC) และ Permanent Virtual Circuit (PVC), SVC นั้นเหมือนกับโครงข่ายการสวิตช์วงจร (Circuit Switched Network) เริ่มจาก สร้างทางเชื่อมต่อข้อมูล, ส่งข้อมูล และยกเลิกทางเชื่อมต่อข้อมูลเมื่อไม่มีการส่งข้อมูล ส่วน PVC นั้นจะคล้ายกับคู่สายเช่า (Leased Line) คือมีการเชื่อมต่อระหว่าง DTE 2 ด้านอยู่ตลอดเวลา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.7 โครงสร้างของ แพ็กเกต ทั่วไป

- Q bit (Qualifier bit) : เมื่อ Set เป็น " 1 " แล้ว DTE ทั้งสองจะทำการ qualify ค่าใน Data packet สำหรับกระบวนการเฉพาะ เช่น การเชื่อมต่อ QLLC ในระบบของ IBM โดยปกติ Q bit จะมีค่าเป็น " 0 "

- D bit (Delivery Confirmation bit) : โดยปกติ DTE ด้านท้องถิ่น จะได้รับ acknowledgment จาก DCE ซึ่งเรียกว่า " Local acknowledgment " แต่ในบางกรณี acknowledgment จะได้รับจาก DTE ด้านระยะไกล (Remote DTE) เรียกว่า "end-to-end acknowledgment " ในกรณีนี้ D bit จะถูก set ให้เป็น " 1 " ซึ่งจะถูกใช้ในช่วงของการ Call Setup และ Data packet โดยปกติ D bit จะมีค่าเป็น " 0 "

- NN : เป็น Packet Sequence Number ถ้าเป็น 01 จะใช้กับ Modulo 8 และ ถ้าเป็น 10 จะใช้กับ Modulo 128

- Logical Channel Group Number : มีขนาด 4 bits จะใช้เป็นกลุ่มของ Logical Channel Number โดยปกติจะมีค่าเป็น " 0 "

- Logical Channel Number (LCN) : เป็นหมายเลขของวงจรเสมือนระหว่าง DTE และ DCE มีค่ามากสุดถึง 255 หมายเลข

- Packet Type Identifier : เป็นการกำหนดชนิดของแพ็กเกต ตามตารางที่ 3.4

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 3.4 รูปแบบ Packet Type Identifier

From DCE to DTE	From DTE to DCE	Packet Type ID. (Hex)
Call set-up and clearing		
Incoming call	Call Request	0B
Call connected	Call Accepted	0F
Clear indication	Clear Request	13
DCE clear confirmation	DTE clear Confirmation	17
Data and interrupt		
DCE data	DTE data	even
DCE interrupt	DTE interrupt	23
DCE interrupt confirmation	DTE interrupt confirmation	27
Flow control and reset		
DCE RR (mod 8)	DTE RR (mod 8)	x1
DCE RNR (mod8)	DTE RNR (mod 8)	x5
Reset indication	Reset request	1B
DCE reset confirmation	DTE reset confirmation	1F
Restart		
Restart indication	Restart request	FB
DCE restart confirmation	DTE restart confirmation	FF
Diagnostic		
Diagnostic		F1

- Other Fields : ขึ้นอยู่กับการระบุชนิดของแพ็กเกต (Packet Type Identifier) เช่น ถ้าเป็น Restart Packet ส่วนนี้จะเป็น Restart Cause 1 byte และใน byte ที่ 2 จะเป็น Diagnostic Code เป็นต้น

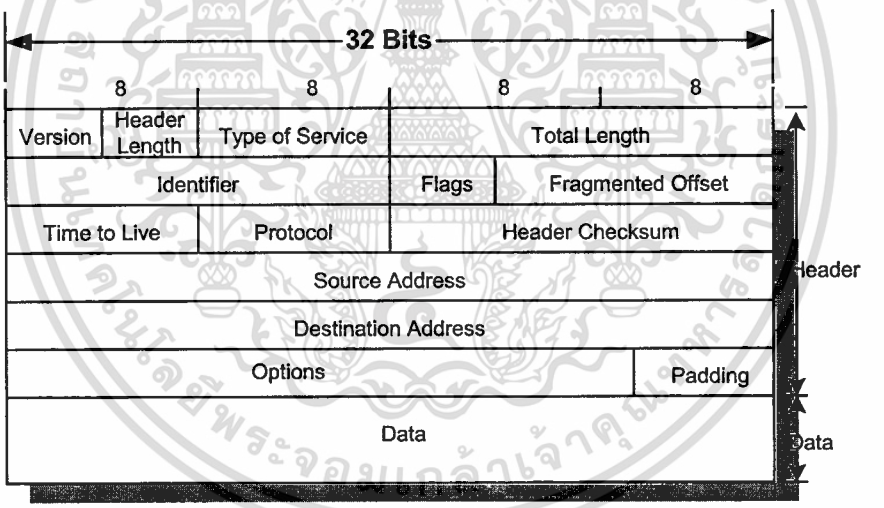
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 4
เครือข่าย TCP/IP

โพรโทคอล TCP/IP เป็นโพรโทคอลที่ทำงานอยู่ในชั้น network ซึ่งมีการเชื่อมต่อแบบ Connection oriented โดยมีอุปกรณ์การสื่อสารซึ่งเรียกว่า เราท์เตอร์ (router) ซึ่งทำหน้าที่ในการส่งผ่านข้อมูลของผู้ใช้ในรูปของ IP datagram กระบวนการในการตัดสินใจเลือกเส้นทางในการส่ง IP datagram ในแต่ละตัวจึงเป็นประเด็นหลักที่ต้องได้รับการพิจารณาและการออกแบบอย่างมีประสิทธิภาพ เพื่อให้การรับส่ง IP datagram มีความรวดเร็วและมีความผิดพลาดน้อยที่สุด [1]

4.1 โครงสร้างของ IP datagram

ในรูปที่ 4.1 แสดงถึงรูปแบบโครงสร้างของ IP datagram ซึ่งจะเห็นได้ว่า IP datagram มีองค์ประกอบหลักอยู่ 2 ส่วน คือ ส่วนของ Header และส่วนของข้อมูล (data)



รูปที่ 4.1 โครงสร้าง IP datagram

- ฟิลด์ Version : ระบุเวอร์ชันของ IP ที่ใช้ในการสร้าง IP datagram ในฟิลด์นี้จะมีขนาด 4 บิทซึ่งปกติจะเซ็ทเป็น 0100 ในระบบของเลขฐานสอง ซึ่งแสดงถึงเวอร์ชัน 4 (IPv4) ซึ่งเป็นเวอร์ชันที่ใช้อยู่ในปัจจุบัน ในตารางที่ 4.1 แสดงให้เห็นถึงเวอร์ชันในแบบต่าง ๆ ที่สัมพันธ์กันกับ RFC

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

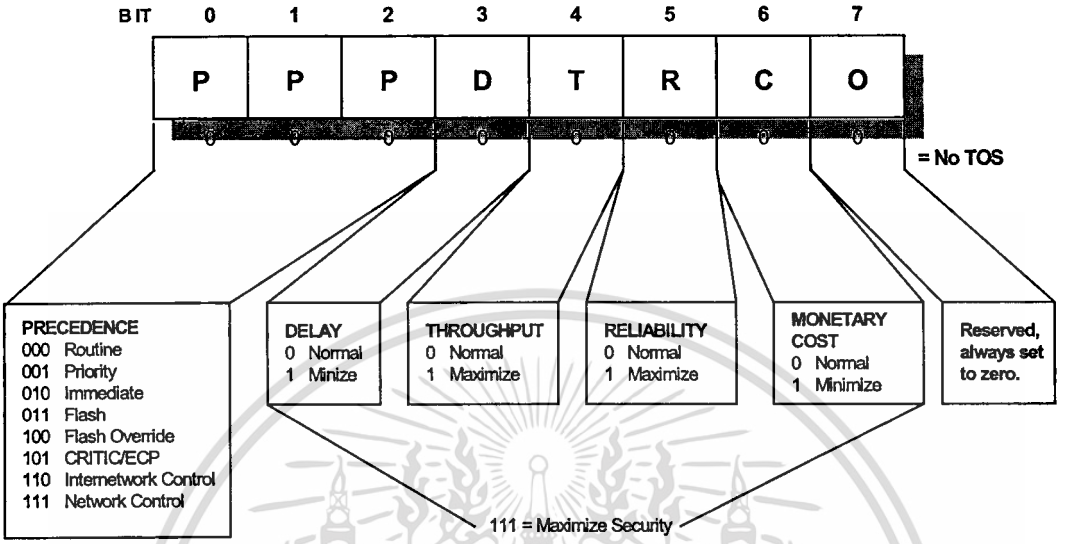
ตารางที่ 4.1 แสดงหมายเลขเวอร์ชันของ IP

Number	Version	RFC
0	Reserved	
1-3	Unassigned	
4	Internet Protocol (IP)	791
5	ST Datagram Mode	1190
6	Simple Internet Protocol (SIP)	
6	IPng	1883
7	TP/IX	1475
8	P Internet Protocol (PIP)	1621
9	TCP and UDP over Bigger Address (TUBA)	1347
10-14	Unassigned	
15	Reserved	

- ฟิลด์ Header Length : มีขนาด 4 บิทใช้บอกขนาด Header ของ IP โดยจะบอกในรูปของ word ขนาด 32 บิท ซึ่งปกติจะมีขนาดเท่ากับ 5 หรือเทียบเท่ากับ 20 ไบต์ และถ้าหากมีฟิลด์ Option เพิ่มเข้ามาจะทำให้ขนาดของ Header เท่ากับ 24 ไบต์
- ฟิลด์ Type of Service (TOS) : มีขนาด 8 บิท ใช้สำหรับบ่งบอกถึงคุณลักษณะหรือรูปแบบการให้การบริการที่แพ็กเก็ต IP ต้องการ ในฟิลด์นี้สามารถแบ่งออกได้เป็น 2 ส่วน คือ ส่วนของ Precedence และส่วนของ TOS ดังในรูปที่ 4.2 ส่วนของ Precedence นั้นมีจำนวน 3 บิทใช้สำหรับจัดลำดับความสำคัญของแพ็กเก็ตซึ่งมีได้ 8 ระดับ ในส่วนของ TOS มีไว้เพื่อใช้ในการเลือกการบริการในการส่งมอบแพ็กเก็ตในรูปของ Delay Throughput Reliability และ Monetary cost
- ฟิลด์ Total Length : มีขนาด 16 บิทใช้สำหรับระบุขนาดของ IP datagram ทั้งหมดซึ่งรวม Header ด้วย ขนาดของ IP datagram ที่ใหญ่ที่สุดมีค่าเท่ากับ 65,535 ไบท์
- ฟิลด์ Identifier : มีขนาด 16 บิทใช้ในการเชื่อมต่อฟิลด์ Flags และฟิลด์ Fragment Offset สำหรับการแบ่งแพ็กเก็ตออกเป็นแพ็กเก็ตย่อย ๆ ซึ่งแพ็กเก็ตจะถูกทำ fragment เพื่อทำให้เป็นแพ็กเก็ตย่อย ๆ ก็ต่อเมื่อความยาวของแพ็กเก็ตที่มาจากต้นทางมีความยาวมากเกินกว่าค่า Maximun Transmission Unit (MTU) ของ data link ในแต่ละเส้นทางที่แพ็กเก็ตนี้เดินทางผ่าน เช่น มีแพ็กเก็ตขนาด 5,000 ไบท์ที่จะต้องเดินทางผ่านเครือข่ายร่วมซึ่งมีค่า MTU เป็น 1,500 ไบท์ เพราะฉะนั้นภายในเฟรมหนึ่ง ๆ จะสามารถบรรจุขนาดของแพ็กเก็ตได้สูงสุด 1,500 ไบท์ ทำให้เราท์เตอร์ซึ่งบรรจุแพ็กเก็ตไปบน data link ทำการ fragment แพ็กเก็ต

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

แต่ละแพ็กเก็ตให้มีขนาดไม่เกิน 1,500 ไบท์ จากนั้นเราท์เตอร์จะทำการ mark แพ็กเก็ตซึ่งถูก fragment แล้วด้วยหมายเลขเดียวกันในฟิลด์ Identifier ซึ่งจะทำให้อุปกรณ์ทางด้านรับสามารถระบุได้ว่าแพ็กเก็ตที่ถูก fragment นั้นเป็นแพ็กเก็ตเดียวกัน



รูปที่ 4.2 ฟิลด์ Type of Service

- ฟิลด์ Flags : เป็นฟิลด์ที่มีขนาด 3 บิทโดยที่บิทแรกไม่มีการใช้งานและกำหนดให้เป็น 0 เสมอ บิทที่สองเรียกว่าบิท Don't Fragment (DF) มีไว้เพื่อกำหนดว่า IP datagram นี้อนุญาตให้ทำ fragment ได้หรือไม่ ถ้าHost ต้นทางกำหนดให้ DF=0 ก็หมายถึงอนุญาตให้เราท์เตอร์ระหว่างทางทำการ fragment ได้ถ้ามีความจำเป็น แต่ถ้าหากเซ็ท DF=1 หมายความว่าห้ามทำการ fragment ในกรณีนี้ถ้าหากเราท์เตอร์ไม่สามารถส่ง datagram ต่อไปได้หากไม่มีการทำ fragment เราท์เตอร์ก็จะทิ้ง datagram นั้นไป และส่งความผิดพลาดที่เกิดขึ้นกลับไปยัง Host ต้นทาง บิทที่สามเรียกว่าบิท More Fragments (MF) เป็นบิทที่ถูกเซ็ทโดยเราท์เตอร์เมื่อมีการทำ fragment กับ IP datagrtam นั้น โดยจะมีค่า MF=0 เพื่อแสดงว่า fragment นั้นเป็นส่วนสุดท้ายของ IP datagram และจะเซ็ทให้ MF=1 เพื่อแสดงว่ายังมี fragment อื่นตามมาอีก เพราะฉะนั้นฟิลด์ flag จึงเป็นตัวระบุให้ Host ปลายทางทราบจุสิ้นสุดของ IP datagram มีข้อสังเกตว่า เมื่อ fragment ในแต่ละส่วนอาจจะถูกส่งผ่านเครือข่ายด้วยเส้นทางที่แตกต่างกัน และ fragmnet เหล่านี้อาจเดินทางมาถึงจุดหมายในลำดับที่ผิดไปจากเดิมได้ ดังนั้นหาก Host ปลายทางได้รับ fragment ที่บอกว่าเป็น fragment สุดท้าย แต่แท้จริงแล้ว Host ปลายทางได้รับ fragment ของ IP datagram ยังไม่ครบถ้วนสมบูรณ์ ซึ่งจะเห็นได้ว่า การใช้เพียงฟิลด์ Identifier และ Flag จะไม่เพียงพอสำหรับ Host ปลายทางที่จะ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

นำ fragment มาประกอบกันได้อย่างถูกต้อง เพราะขาดข้อมูลที่บอกถึงลำดับการเรียงต่อของ fragment ปัญหานี้สามารถแก้ไขได้โดยอาศัยฟิลด์ Fragment Offset ที่จะได้กล่าวต่อไป

- ฟิลด์ Fragment Offset : ทำหน้าที่ชี้หรือระบุตำแหน่งเริ่มต้นของส่วนย่อยแต่ละส่วนภายใน IP datagram ฟิลด์นี้มีขนาด 13 บิท โดยค่าที่ใช้มีหน่วยเป็นจำนวนเท่าของ 8 ไบท์ เมื่อ Host ปลายทางอ่านค่าฟิลด์นี้ประกอบกับฟิลด์ Total length ของ fragment ที่ได้รับแต่ละตัว ก็จะทำให้สามารถตรวจสอบว่าได้รับ fragment ของ IP datagram ครบถ้วนหรือไม่
- ฟิลด์ Time to Live (TTL) : มีขนาด 8 บิทมีหน้าที่กำหนดจำนวนเราท์เตอร์สูงสุดที่ IP datagram สามารถเดินทางผ่านได้ หรือกล่าวในอีกนัยหนึ่งได้ว่าเป็นการกำหนดอายุของ datagram ที่อนุญาตให้อยู่ในเครือข่ายได้ ขั้นตอนในการทำงาน คือ เมื่อ Host ต้นทางทำการส่ง datagram ออกไปจะตั้งค่าเริ่มต้นให้กับฟิลด์ TTL ค่าหนึ่ง (โดยทั่วไปใช้ 32 หรือ 64) ทุกครั้งที่ datagram เดินทางผ่านเราท์เตอร์ตัวหนึ่งค่าของ TTL จะถูกปรับลดลงหนึ่งหน่วย หากเมื่อใดเราท์เตอร์พบ datagram ที่ค่า TTL ลดลงจนเป็น 0 เราท์เตอร์จะตัด datagram นั้นทิ้งไปพร้อมกับแจ้งให้ Host ต้นทางทราบ การทำเช่นนี้จะทำให้สามารถป้องกัน IP datagram ที่รับส่งผิดพลาดได้
- ฟิลด์ Protocol : เป็นฟิลด์ที่มีขนาด 8 บิท ใช้ระบุว่า datagram ที่ได้รับเป็นโพรโทคอลที่ใช้เชื่อม Host กับ Host หรือ Transport layer แบบใด ดังแสดงตัวอย่างของโพรโทคอลบางรูปแบบในตารางที่ 4.2
- ฟิลด์ Header Checksum : มีขนาด 16 บิทเป็นฟิลด์ที่ทำหน้าที่ตรวจสอบความถูกต้องของ IP header โดยมีลักษณะการทำงานดังนี้ เมื่อ Host ต้นทางทำการสร้าง datagram ขึ้นจะคำนวณค่า header checksum โดยนำ header ทีละ 16 บิทมาบวกกันแบบ one's component จากนั้นนำผลที่ได้มาทำ one's component อีกครั้ง จึงจะได้เป็นค่าที่บรรจุลงใน header checksum โดยที่ด้านรับปลายทางจะตรวจสอบความผิดพลาดของ header โดยนำ header ทีละ 16 บิทมาบวกกับค่าในฟิลด์ header checksum แบบ one's component หากผลลัพธ์ที่ได้มีค่าเป็นหนึ่งทั้งหมด แสดงว่าไม่มีความผิดพลาดเกิดขึ้น หากไม่ใช่ก็แสดงว่ามีความผิดพลาดเกิดขึ้นกับ header ในกรณีนี้ IP datagram จะถูกตัดทิ้งโดยไม่มีการแจ้งความผิดพลาดที่เกิดขึ้น ซึ่งโพรโทคอลในชั้นที่สูงกว่าต้องตรวจสอบปัญหาด้วยตัวเอง
- ฟิลด์ Source และ Destination Addresses : คือ IP address ของต้นทางและ IP address ของปลายทาง มีขนาด 32 บิท

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 4.2 ค่าภายในฟิลด์โพรโทคอลบางแบบที่รู้จักกันดี

Protocol Number	Host-to-Host Layer Protocol
1	Internet Control Message Protocol (ICMP)
2	Internet Group Management Protocol (IGMP)
3	Gateway to Gateway Protocol (GGP)
4	IP in IP
6	Transmission Control Protocol (TCP)
8	Exterior Gateway Protocol (EGP)
17	User Datagram Protocol (UDP)
35	Inter-Domain Policy Routing Protocol (IDPR)
45	Inter-Domain Routing Protocol (IDRP)
46	Resource Reservation Protocol (RSVP)
47	Generic Routing Encapsulation (GRE)
54	NBMA Next Hop Resolution Protocol (NHRP)
88	Cisco Internet Gateway Routing Protocol (IGRP)
89	Open Shortest Path First (OSPF)

- ฟิลด์ Option : เป็นส่วนที่เพิ่มเติมเมื่อมีการใช้งานบางอย่าง เช่น การทดสอบเครือข่าย และตรวจหาจุดผิดพลาดของระบบ ฟิลด์นี้จะมีขนาดไม่ตายตัวขึ้นอยู่กับชนิดของ option ที่เลือกใช้ เช่น Loose source routing Strict source routing Record route และ Timestamp เป็นต้น
- ฟิลด์ Padding : เป็นส่วนต่อท้ายฟิลด์ Option เพื่อทำให้มีขนาดครบ 32 บิท โดยทำการเติมศูนย์ต่อท้ายให้จนครบจำนวน 32 บิท

4.2 การทำงานพื้นฐานของโพรโทคอล TCP

ในขั้นตอนแรกข้อมูลของโปรแกรมแอพพลิเคชันจะถูกแบ่งออกเป็นองค์ประกอบย่อย ๆ เรียกว่า เซกเมนต์ (segment) เพื่อส่งผ่านไปในเครือข่ายโดยอาศัย IP datagram ขนาดของเซกเมนต์จะถูกกำหนดโดยโพรโทคอลในชั้น TCP เองและไม่ขึ้นกับขนาดของข้อมูลที่ส่งมาจากโปรแกรมแอพพลิเคชั่น

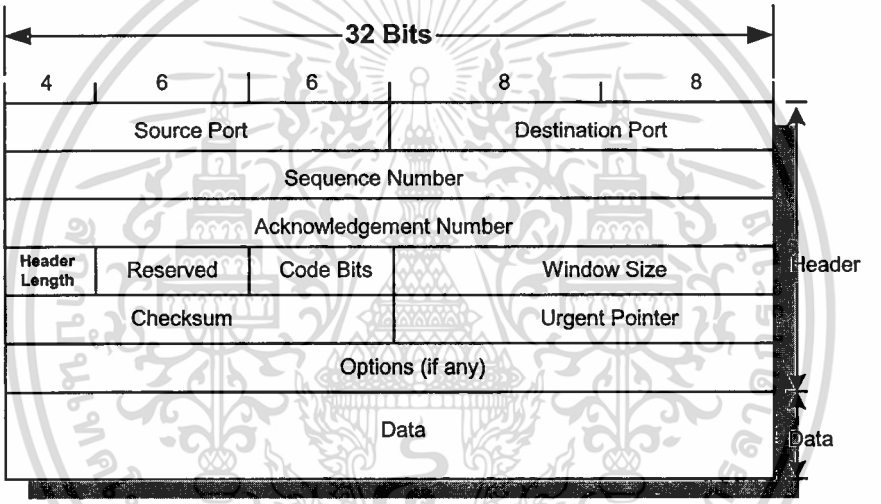
ทุกครั้งที่ Host ต้นทางส่งเซกเมนต์ออกไปหนึ่งเซกเมนต์ Host ต้นทางจะทำการจับเวลาและรอการตอบกลับจาก Host ปลายทางว่าได้รับเซกเมาต์ที่ส่งออกมาเรียบร้อยหรือไม่ การตอบรับจะอยู่ในรูปของเซกเมนต์ตอบรับที่ Host ปลายทางส่งกลับมา การทำเช่นนี้จะช่วยให้ Host ต้นทาง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

มั่นใจว่าเซกเมนต์ที่ตัวเองเป็นผู้ส่งออกไปจะถึง Host ปลายทางได้อย่างถูกต้อง สำหรับกรณีที่ Host ต้นทางยังไม่ได้รับเซกเมนต์ตอบรับจาก Host ปลายทางและช่วงเวลาที่จับเวลาไว้สิ้นสุดลง Host ต้นทางจะคิดเอาเองว่าการส่งเซกเมนต์ดังกล่าวล้มเหลว และจะทำการส่งเซกเมนต์เดิมออกไปซ้ำอีกครั้ง

4.3 โครงสร้างของ TCP

จากรูปที่ 4.3 แสดงให้เห็นถึงโครงสร้างของ TCP โดยที่ 2 ฟิลด์แรกคือ หมายเลขพอร์ท TCP ของ Host ต้นทาง (Source port) และหมายเลขพอร์ท TCP ของ Host ปลายทาง (Destination port) ฟิลด์ทั้งสองเป็นส่วนที่ทำหน้าที่ระบุหมายเลขพอร์ทหรือชนิดของโปรแกรมแอพพลิเคชัน



รูปที่ 4.3 โครงสร้างของ TCP

- ฟิลด์ sequence number และฟิลด์ acknowledgement number มีขนาดเท่ากันคือ 32 บิท กำหนดให้มีการทำงานร่วมกันสำหรับตรวจสอบความถูกต้องในการส่งผ่านข้อมูล ฟิลด์ sequence number ใช้ระบุหมายเลขไบท์ในสตรีมข้อมูลในขณะที่ Host ต้นทางกำลังส่งอยู่ เนื่องจากไบท์ทุกไบท์ในสตรีมของโพรโทคอล TCP จะมีการจัดสรรหมายเลขให้โดยเรียงลำดับจากค่าน้อยไปหามาก หมายเลขที่ใช้มีค่าอยู่ระหว่าง 0 ถึง 232-1 เมื่อใดที่ได้ใช้ถึงตัวเลขที่มีค่าสูงสุดแล้วก็จะวนกลับมาใช้เลขศูนย์ใหม่ ส่วนฟิลด์ ackhowledgement number ได้รับการกำหนดจาก Host ปลายทาง ค่าที่บรรจุอยู่ในฟิลด์นี้จะถูกกำหนดให้สอดคล้องกับหมายเลขของฟิลด์ sequence number ในเซกเมนต์ข้อมูลที่ส่งมาจาก Host ต้นทางเพื่อแสดงความหมายว่า Host ปลายทางกำลังรอรับหมายเลขของไบท์ถัดไปในสตรีมข้อมูลหมายเลข

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ใดอยู่ ทั้งนี้หมายเลขของไบท์สตรีมก่อนหน้านี้ทั้งหมดนั้นให้เข้าใจว่ารับได้ถูกต้องเรียบร้อยแล้ว

- ฟิลด์ header length มีขนาด 4 บิท ใช้บอกถึงขนาดของ Header ในเซกเมนต์ โดยตัวเลขที่ระบุเป็นจำนวนเท่าของ 4 ไบท์ ซึ่งปกติ Header จะมีขนาดคงที่เท่ากับ 20 ไบท์ หรือเท่ากับ 5 Header จะมีขนาดเพิ่มขึ้นเมื่อมีการใช้ฟิลด์ option ซึ่งมีขนาดไม่คงที่ขึ้นอยู่กับชนิดของ option ที่เลือกใช้ โดย Header จะมีขนาดสูงสุดไม่เกิน 60 ไบท์
- ฟิลด์ Reserved ถูกสำรองไว้สำรับใช้ในอนาคต
- ฟิลด์ Code Bits จะมีขนาด 6 บิท เป็นฟิลด์ที่ใช้บ่งบอกถึงชนิดของเซกเมนต์ที่ใช้งานอยู่ ซึ่งมีรายละเอียดและหน้าที่ ดังต่อไปนี้
- URG : บิทนี้จะถูกเซ็ทเพื่อแสดงว่า เซกเมนต์มีการใช้งานฟิลด์ urgent pointer อยู่ โดยจะใช้งานร่วมกัน เพื่อบอกให้โปรแกรมของ Host ปลายทางหยุดอ่านสตรีมข้อมูลที่อยู่ก่อนหน้านี้ทั้งหมดชั่วคราว และให้อ่านข้อมูลเร่งด่วนที่อยู่ในเซกเมนต์ส่วนนี่ก่อนที่จะทำกิจกรรมเดิมต่อไป การใช้งานของบิท URG เกิดขึ้นเฉพาะในกรณี เช่น ผู้ใช้อาจต้องการยกเลิกการติดต่อสื่อสารกลางคัน จึงทำการยกเลิก ข้อมูลการขอยกเลิกการสื่อสารจึงถูกส่งออกไปอย่างเร่งด่วนในเซกเมนต์ที่มีการเซ็ทบิท URG ทั้งนี้ฟิลด์ urgent pointer มีหน้าที่ระบุตำแหน่งจุดสิ้นสุดของข้อมูลเร่งด่วนภายในเซกเมนต์
- ACK : ใช้เพื่อบอกว่ามีการใช้งานฟิลด์ acknowledgement number ในการตอบรับเซกเมนต์
- PSH : บิทนี้จะถูกเซ็ทในกรณีที่ต้องการให้เลเยอร์ TCP ของ Host ปลายทางส่งข้อมูลต่อไปให้โปรแกรมแอพพลิเคชันทันที ทั้งนี้เพราะโดยปกติโพรโทคอล TCP จะสะสมและเก็บเซกเมนต์ไว้จนกว่าจะมีปริมาณมากพอจึงค่อยส่งต่อให้โปรแกรมแอพพลิเคชันเพื่อลดปริมาณงานการติดต่อลง บิท PSH นี้มีความสำคัญต่อโปรแกรมแอพพลิเคชันบางประเภทที่มีการส่งข้อมูลทีละอักขระและมีการโต้ตอบไปมาระหว่างสองฝ่าย
- RST : บิทนี้จะใช้งานเมื่อมีความผิดพลาดของการทำงานเกิดขึ้น และระบบไม่สามารถจัดการกับปัญหาเหล่านี้ได้อีกต่อไป การส่งเซกเมนต์ที่เซ็ทบิท RST จึงเป็นกลไกในการปิดการเชื่อมต่อหรือยกเลิกการเชื่อมต่อ
- SYN : บิทนี้ใช้งานเฉพาะสำหรับแสดงความต้องการในการขอเปิดการเชื่อมต่อระหว่าง Host เริ่มแรก Host ด้าหนึ่งจะส่งเซกเมนต์ที่มีการเซ็ทบิท SYN ออกไป หาก Host ปลายทางต้องการเปิดการเชื่อมต่อก็จะส่งเซกเมนต์ที่เซ็ทบิท SYN ตอบรับกลับไป
- FIN : บิทนี้มีหน้าที่กลับกันกับบิท SYN คือมีไว้สำหรับ Host เพื่อใช้แจ้งการขอยกเลิกการเชื่อมต่อ เนื่องจากไม่มีข้อมูลเหลือสำหรับส่งอีกต่อไป
- ฟิลด์ window size มีขนาด 16 บิท มีไว้สำหรับให้ Host ปลายทางใช้ในการประกาศขนาดของ window ที่ตัวเองอนุญาตให้ Host ต้นทางใช้งานได้ ขนาดของ window เป็นตัวกำหนด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จำนวนไบท์สตรีมที่ Host ต้นทางสามารถส่งออกอย่างต่อเนื่องโดยไม่ต้องรอการตอบกลับจาก Host ปลายทาง เพราะฉะนั้น Host ปลายทางจึงสามารถควบคุมปริมาณหรืออัตราการส่งเซกเมนต์ของ Host ต้นทางได้

- ฟิลด์ checksum มีขนาด 16 บิททำหน้าที่ตรวจสอบความถูกต้องขององค์ประกอบทุกส่วนในเซกเมนต์คือ ทั้ง Header และข้อมูล
- ฟิลด์ urgent pointer มีขนาด 16 บิท จะมีความหมายก็ต่อเมื่อบิท URG= 1 เท่านั้น เมื่อ Host ปลายทางได้รับเซกเมนต์ที่มีการเซ็ทบิท URG ก็จะทำการอ่านค่าฟิลด์ urgent pointer เพื่อให้ทราบถึงตำแหน่งไบท์สุดท้ายของข้อมูลเร่งด่วนในเซกเมนต์นั้น
- ฟิลด์ options ใน Header ของโพรโทคอล TCP มีขนาดที่เปลี่ยนแปลงได้ โดยขนาดที่แน่นอนของแต่ละเซกเมนต์สวามารถดูได้จากฟิลด์ Header length

4.4 การสร้างและการยกเลิกการเชื่อมต่อ TCP

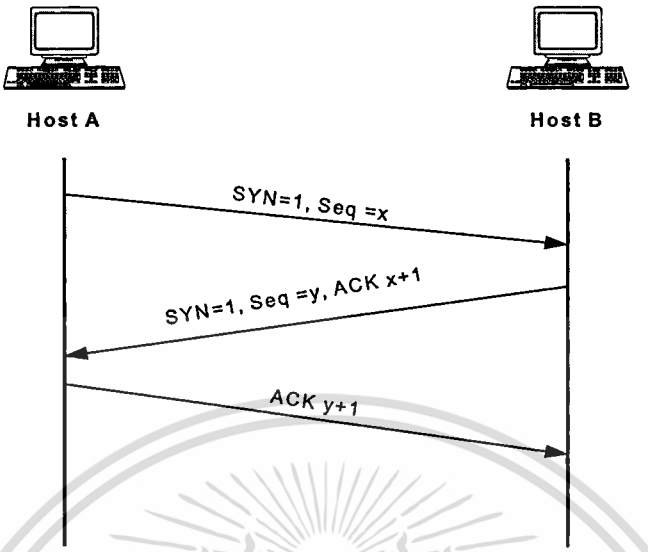
ในการติดต่อสื่อสารกันระหว่าง Host ต้นทางและปลายทาง จำเป็นต้องมีการสร้างการเชื่อมต่อกันก่อนและหลังจากที่ไม่มีความจำเป็นหรือไม่ต้องการการเชื่อมต่อนั้น ก็สามารถยกเลิกการเชื่อมต่อได้ โดยสามารถอธิบายได้ ดังนี้

4.4.1 การสร้างการเชื่อมต่อ TCP

กระบวนการในการสร้างการเชื่อมต่อของโพรโทคอล TCP ระหว่าง Host ต้นทางและปลายทาง สามารถแบ่งออกได้เป็น 3 ขั้น ดังรูปที่ 4.4 ดังนี้

- ขั้นตอนแรก เมื่อ Host A ต้องการเริ่มการติดต่อ ก็จะทำการส่งเซกเมนต์ที่เซ็ตบิท SYN ในฟิลด์ code ให้เป็น “1” พร้อมกับเลือกหมายเลข seq ขึ้นหนึ่งค่าเพื่อบรรจุลงในฟิลด์ sequence number ในตัวอย่างนี้คือ x ค่า seq ที่เลือกนี้จะใช้เป็นค่าเริ่มต้นสำหรับการติดต่อสื่อสารที่จะเกิดขึ้นในลำดับต่อไป
- ขั้นต่อมาเมื่อ Host B ตอบรับการขอเปิดการเชื่อมต่อด้วยเซกเมนตที่เซ็ทบิท SYN=1 และ ACK=1 ของฟิลด์ code พร้อมกับเลือกหมายเลข Seq ของตัวเองเพื่อบรรจุลงในฟิลด์ sequence number สำหรับใช้เป็นค่าเริ่มต้นของหมายเลขที่ใช้กำกับให้กับเซกเมนต์ที่จะส่งในลำดับถัดไป ในการตอบรับด้วยบิท ACK จะใช้ควบคุมกับฟิลด์ acknowledgement number ซึ่งจะบรรจุค่า x+1 สังเกตว่าเซกเมนต์ SYN จะใช้หมายเลข sequence number ไปหนึ่งหมายเลข
- ขั้นตอนสุดท้าย เมื่อ Host A ยืนยันการเปิดการเชื่อมต่อกับ Host B โดยการส่งเป็นเซกเมนต์ที่เซ็ทบิท ACK เท่านั้น ไม่ใช้บิท SYN อีกต่อไป ส่วนค่าในฟิลด์ ackhowledgement number ตั้งให้มีค่าเท่ากับ y+1

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

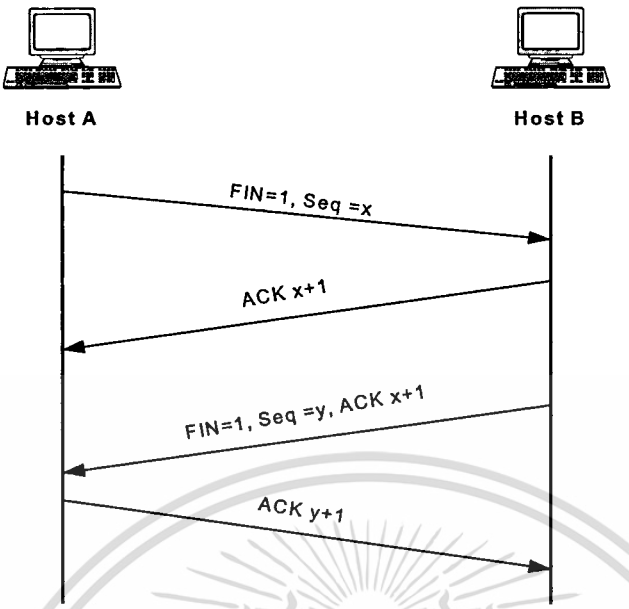


รูปที่ 4.4 ขั้นตอนการสร้างการเชื่อมต่อของโพรโทคอล TCP

4.4.2 การยกเลิกการเชื่อมต่อ TCP

เนื่องจากการเชื่อมต่อสื่อสารของโพรโทคอล TCP เป็นแบบ Full duplex คือสามารถรับส่งข้อมูลทั้งสองทิศทางได้พร้อมกันและไม่ขึ้นแก่กัน กระบวนการปิดการเชื่อมต่อเพื่อยกเลิกการเชื่อมต่อระหว่าง Host ในโพรโทคอล TCP จึงสามารถแยกทำแต่ละทิศทางอิสระจากกันได้ คือเมื่อ Host ด้านใดด้านหนึ่งไม่มีข้อมูลจะส่งอีกต่อไป Host ดังกล่าวสามารถขอปิดการเชื่อมต่อสำหรับทิศทางการส่งของตัวเองเพียงด้านเดียวได้โดยส่งเซกเมนต์ที่ได้เซ็ทบิท FIN = 1 ออกไปเพื่อแสดงความต้องการในการปิดการส่งของตัวเอง Host อีกด้านหนึ่งก็จะตอบกลับโดยส่งเซกเมนต์ที่เซ็ทบิท ACK = x+1 ในขณะเดียวกันก็แจ้งให้โปรแกรมแอพพลิเคชันของตัวเองให้รับทราบว่าจะไม่มีข้อมูลใหม่เข้ามาจากการเชื่อมต่อดังกล่าวอีกต่อไป ดังรูปที่ 4.5

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.5 ขั้นตอนการยกเลิกการเชื่อมต่อของโพรโทคอล TCP

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 5
รูปแบบโพรโทคอล OSPF

Open Shortest Path First (OSPF) [1] ได้ถูกพัฒนาขึ้นโดยองค์กร Internet Engineering Task Force (IEFT) ซึ่ง เป็นโพรโทคอลแบบ Link Stateที่ใช้อัลกอลิธึ่มแบบ Dijkstra's Shortest Path First และ เป็นแบบระบบเปิด (Open) ประโยชน์หลักของ OSPF คือ มีค่า reconvergence ที่เร็ว สามารถรองรับเครือข่ายที่มีขนาดใหญ่มากได้และมีความหวั่นไหวกับข้อมูลของเส้นทางเดิน (Routing information) น้อย คุณสมบัติอื่น ๆ ของ OSPF มีดังนี้

1. ใช้แอเรีย (Areas) ซึ่งลดผลกระทบของโพรโทคอลต่อ CPU และหน่วยความจำที่บรรจุการไหลเวียนของทราฟฟิกโพรโทคอลของเส้นทาง (routing protocol) และทำให้การสร้างโทโปโลยีของเครือข่ายเป็นไปตามลำดับชั้น (hierarchical) ได้
2. ไม่มีการแบ่งชนชั้น (classless) ซึ่งจะช่วยกำจัดปัญหาของ subnet ที่ไม่อยู่ติดกันได้
3. รองรับตารางเส้นทาง classless VLSM และ supernetting สำหรับการจัดการแอดเดรสได้อย่างมีประสิทธิภาพ
4. สามารถจัดโหลดให้สมดุลย์ได้เมื่อมีเส้นทางหลาย ๆ เส้นทาง
5. ใช้แอดเดรสแบบจุดต่อหลาย ๆ จุด (multicast address) ที่สำรองไว้ เพื่อลดผลกระทบที่เกิดจากอุปกรณ์ที่ไม่ใช้ OSPF
6. รองรับการรับรองตัวตน (authentication) เพื่อการจัดเส้นทางที่ปลอดภัย
7. ใช้ tag เพื่อการติดตามเส้นทางที่มาจากภายนอก

5.1 การทำงานของ OSPF

การทำงานของ OSPF สามารถอธิบายได้ ดังนี้

1. เราท์เตอร์ต่าง ๆ ที่ติดต่อกันด้วย OSPF (OSPF-speaking) จะทำการส่งแพ็คเก็ต Hello
2. ไปยังทุก ๆ interface ที่รองรับ OSPF ถ้าเราท์เตอร์ 2 ตัวมีการแบ่ง data link ร่วมกันตามค่าพารามิเตอร์ที่ตกลงไว้ในแพ็กเก็ต Hello ต่าง ๆ โดยลำดับ เราท์เตอร์ทั้ง 2 ตัวจะกลายเป็นเพื่อนบ้านกัน (Neighbor)
3. การอยู่ติดกัน (Adjacency) ซึ่งอาจจะถูกคิดได้ตามการเชื่อมต่อแบบจุดต่อจุดเสมือน ได้ถูกจัดรูปแบบไว้ระหว่างเพื่อนบ้านกับเพื่อนบ้าน OSPF ได้กำหนดชนิดของเครือข่ายและชนิดของเราท์เตอร์ไว้มากมาย การสร้างการอยู่ติดกันในรูปแบบหนึ่งได้ถูกกำหนดตามชนิดของการแลกเปลี่ยน Hello ของเราท์เตอร์ และตามชนิดของเครือข่ายที่ Hello ได้ถูกแลกเปลี่ยนกัน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4. เราท์เตอร์แต่ละตัวส่ง Link State Advertisements (LSAs) ให้กับเราท์เตอร์ที่อยู่ติดกัน LSAs จะอธิบายถึงการเชื่อมต่อของเราท์เตอร์ทุก ๆ ตัวหรือทุก ๆ interface และสถานะของการเชื่อมต่อ การเชื่อมต่อเหล่านี้อาจจะเป็น เครือข่าย Stub (เครือข่ายที่ไม่มีเราท์เตอร์ต่ออยู่) เราท์เตอร์อื่น ๆ ที่ใช้ OSPF เครือข่ายในแอเรียอื่น หรือเครือข่ายจากภายนอก (เครือข่ายที่เรียนรู้จากกระบวนการของเส้นทางอื่น)
5. เราท์เตอร์แต่ละตัวที่ได้รับ LSA มาจากเพื่อนบ้านจะทำการบันทึก LSA ลงในฐานข้อมูล link state ในตัวมันเอง และส่งสำเนาของ LSA ไปยังเพื่อนบ้านอื่น ๆ ของตัวมันเองทั้งหมด
6. เนื่องจากการไหลเวียนของ LSA กระจายครอบคลุมทั่วแอเรีย เราท์เตอร์ทั้งหมดจะทำการสร้างฐานข้อมูล link state ที่เหมือนกัน
7. เมื่อฐานข้อมูลเสร็จสมบูรณ์ เราท์เตอร์แต่ละตัวจะใช้อัลกอริธึ่ม SPF เพื่อคำนวณหากราฟที่ไม่มีการลูป (loop) ที่บ่งบอกถึงเส้นทางที่สั้นที่สุด (มีค่า cost ต่ำที่สุด) กับทุก ๆ ปลายทางที่รู้จักด้วยตัวของมันเอง นั่นคือ root กราฟนี้เรียกว่า SPF tree
8. เราท์เตอร์แต่ละตัวจะทำการสร้างตารางเส้นทางของตัวเองจาก SPF tree

เมื่อข้อมูล link state ทั้งหมดถูกแพร่กระจายไปยังเราท์เตอร์ทุกตัวในแอเรีย นั่นคือ ฐานข้อมูล link state ซิงค์โครไนซ์กัน และตารางเส้นทางถูกสร้างขึ้น OSPF ก็จะเสร็จสิ้น แพ็กเก็ต Hello จะถูกแลกเปลี่ยนกันระหว่างเพื่อนบ้านตามค่า keepalive และ LSAs จะถูกส่งซ้ำ ๆ กัน ทุก ๆ 30 นาที ถ้าหากว่า โทโปโลยีของเครือข่ายมีเสียรภาพก็จะไม่มีกิจกรรมใด ๆ เกิดขึ้น

5.2 เพื่อนบ้านและการอยู่ติดกัน (Neighbors and Adjacencies)

ก่อนที่จะมีการส่ง LSAs เราท์เตอร์ OSPF ต้องค้นพบเพื่อนบ้านและสร้างการอยู่ติดกัน จากนั้นเพื่อนบ้านจะถูกบันทึกลงในตารางเพื่อนบ้าน (neighbor table) ตามด้วยข่ายเชื่อมโยง หรืออินเทอร์เฟส (interface) ที่ซึ่งเพื่อนบ้านแต่ละตัวตั้งอยู่ และข้อมูลอื่น ๆ ที่จำเป็น ดังรูปที่ 5.1

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
Monet#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.30.70     1   FULL/DR         00:00:34    192.168.17.73   Ethernet0
192.168.30.254    1   FULL/DR         00:00:34    192.168.32.2    Ethernet1
192.168.30.70     1   FULL/BDR        00:00:34    192.168.32.4    Ethernet1
192.168.30.30     1   FULL/ -         00:00:33    192.168.17.50   Serial0.23
192.168.30.10     1   FULL/ -         00:00:32    192.168.17.9    Serial1
192.168.30.68     1   FULL/ -         00:00:39    192.168.21.134  Serial2.824
192.168.30.18     1   FULL/ -         00:00:30    192.168.21.142  Serial2.826
192.168.30.78     1   FULL/ -         00:00:36    192.168.21.170  Serial2.836
```

รูปที่ 5.1 รูปแบบตารางเพื่อนบ้านซึ่งติดต่อกันด้วย OSPF

เพื่อการติดตามเราท์เตอร์ OSPF ตัวอื่น ๆ เราท์เตอร์แต่ละตัวจะมี router ID เพียง 1 ID และ 1 IP address ตามที่เราท์เตอร์ถูกจำแนกออกเป็นลักษณะเฉพาะภายในโดเมนOSPF เราท์เตอร์สามารถรับเราท์เตอร์ ID ได้ดังนี้

1. เราท์เตอร์จะเลือกจากค่าไอพีแอดเดรสที่มีค่าสูงที่สุดจากอินเทอร์เฟส loopback ต่าง ๆ ของตัวเอง
2. ถ้าอินเทอร์เฟส loopback ไม่ได้ถูกกำหนดไอพีแอดเดรสไว้ เราท์เตอร์จะทำการเลือกจากไอพีแอดเดรสที่มีค่าสูงที่สุดจากอินเทอร์เฟสต่างในตัวมันเอง ซึ่งไม่จำเป็นต้องรัน OSPF

การใช้แอดเดรสจากอินเทอร์เฟส loopback มีประโยชน์อยู่ 2 ประการ

1. อินเทอร์เฟส loopback มีเสถียรภาพมากกว่าอินเทอร์เฟสอื่น ๆ ซึ่งจะทำงานเมื่อเราท์เตอร์ถูกบูต และจะใช้งานไม่ได้เมื่อเราท์เตอร์ล่ม
2. เราท์เตอร์ที่ใช้ OSPF จะเริ่มต้นด้วยความสัมพันธ์ของเพื่อนบ้านโดยการประกาศ ID ของเราท์เตอร์ของตัวเองภายในแพ็กเก็ต Hello

5.2.1 โพรโทคอล Hello (Hello Packet)

โพรโทคอล Hello ใช้เพื่อรองรับวัตถุประสงค์ต่าง ๆ ดังนี้

1. เป็นวิธีการที่ใช้ค้นหาเพื่อนบ้าน
2. ทำหน้าที่ประกาศค่าพารามิเตอร์ต่าง ๆ ให้กับเราท์เตอร์ 2 ตัวก่อนที่เราท์เตอร์ทั้ง 2 ตัวจะกลายเป็นเพื่อนบ้านกัน
3. แพ็กเก็ต Hello ทำหน้าที่ keepalives ระหว่างเพื่อนบ้าน
4. รับรองการสื่อสาร 2 ทางระหว่างเพื่อนบ้าน
5. ทำหน้าที่เลือก Designated Routers (DRs) และ Backup Designated Routers (BDRs) บนเครือข่าย Broadcast และ Nonbroadcast Multiaccess (NBMA)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เราท์เตอร์ที่มีการติดต่อกันด้วย OSPF จะส่งแพ็กเก็ต Hello ออกไปยังแต่ละอินเทอร์เฟสที่ใช้งาน OSPF เป็นช่วงเวลา ซึ่งช่วงเวลานี้เรียกว่า Hello Interval โดยมีค่า default อยู่ที่ 30 วินาที ถ้าหากว่าเราท์เตอร์ไม่ได้ยิน Hello จากเพื่อนบ้านภายในเวลาที่กำหนด เราเรียกว่า Router Dead Interval เราท์เตอร์จะบอกสถานะว่า เพื่อนบ้านหาย

5.2.2 องค์ประกอบของแพ็กเก็ต Hello

แพ็กเก็ต Hello ประกอบด้วยข้อมูลดังต่อไปนี้

1. ID เราท์เตอร์ของเราท์เตอร์ตัวต้นทาง
2. ID แอเรียของอินเทอร์เฟสเราท์เตอร์ตัวต้นทาง
3. แอดเดรสมาร์คของอินเทอร์เฟสด้านต้นทาง
4. ชนิดและข้อมูลของการแสดงการมีตัวตน (authentication) สำหรับอินเทอร์เฟสด้านต้นทาง
5. Hello Interval และ Router Dead Interval ของอินเทอร์เฟสด้านต้นทาง
6. ลำดับความสำคัญของเราท์เตอร์
7. DR และ BDR
8. บิท flag 5 บิท ที่แสดงถึงความจุ
9. เราท์เตอร์ ID ของเพื่อนบ้านของเราท์เตอร์ด้านต้นทาง

เมื่อเราท์เตอร์ได้รับ Hello จากเพื่อนบ้าน ก็จะทำการพิสูจน์ว่าค่า แอเรีย ID การรับรองตัวตน network mask HelloInterval RouterDeadInterval และออปชั่นมีค่าตรงกันกับอินเทอร์เฟสด้านรับหรือไม่ ถ้าหากว่าไม่ตรงกัน แพ็กเก็ตจะถูกตัดทิ้งและไม่มีการสร้างการอยู่ติดกันขึ้น แต่ถ้าหากว่าค่าทุก ๆ ค่าที่กล่าวถึงมีค่าตรงกัน แพ็กเก็ต Hello จะถูกประกาศให้มีผลใช้งานได้ และถ้าหากว่า ID ของเราท์เตอร์ด้านต้นทางถูกเก็บรายชื่อไว้ในตารางเพื่อนบ้านสำหรับอินเทอร์เฟสด้านรับแล้ว เวลาของ RouterDeadInterval ก็จะถูกรีเซ็ท ถ้าหากเราท์เตอร์ ID ยังไม่มีอยู่ในตาราง เราท์เตอร์ ID ก็จะถูกเพิ่มเข้าไปในตารางเพื่อนบ้าน

5.3 ชนิดของเครือข่าย (Network Types)

OSPF ได้กำหนดชนิดของเครือข่ายไว้ 5 ชนิด ดังนี้

1. เครือข่ายแบบ จุดต่อจุด (Point-to-Point networks)
2. เครือข่ายแบบบรอดคลาส์ (Broadcast networks)
3. เครือข่ายแบบ การเข้าถึงได้หลายช่องทางชนิดไม่บรอดคลาส์ (Non-broadcast Multi-access [NBMA])

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4. เครือข่ายแบบ จุดต่อหลาย ๆ จุด (Point-to-multipoint networks)
5. การเชื่อมโยงเสมือน (Virtual links)

เครือข่ายทั้ง 5 แบบสามารถจัดแบ่งออกได้เป็น 2 ชนิดใหญ่ ๆ ดังนี้

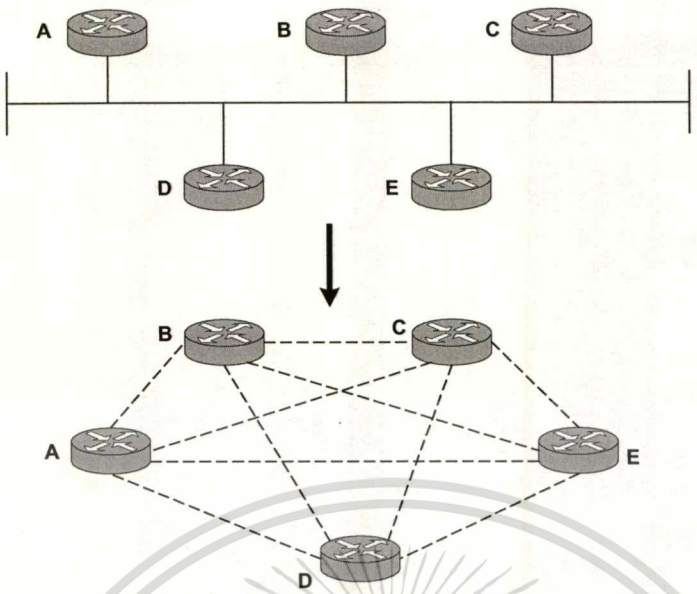
1. เครือข่ายส่งผ่าน (Transit networks) มีเราท์เตอร์ถูกต่ออยู่ 2 ตัวหรือมากกว่า ซึ่งนำพาแพ็กเก็ต "just passing through" ที่เกิดขึ้นและถูกกำหนดไว้สำหรับเครือข่าย ๆ หนึ่ง
2. เครือข่าย Stub มีเพียงเราท์เตอร์ที่ต่ออยู่เพียงตัวเดียว แพ็กเก็ตบนเครือข่าย stub จะมีแอดเดรสของต้นกำเนิดหรือไม่ก็แอดเดรสของปลายทางที่เป็นของเครือข่ายนั้น นั่นคือทุกๆแพ็กเก็ตเกิดขึ้นโดยอุปกรณ์ตัวหนึ่งบนเครือข่ายหรือถูกกำหนดไว้สำหรับอุปกรณ์ตัวหนึ่งบนเครือข่าย

5.4 Designated Routers และ Backup Designated Routers

เครือข่ายแบบเข้าถึงหลายช่องทางแสดงให้เห็นถึงปัญหาสำหรับ OSPF 2 อย่างซึ่งสัมพันธ์กับการแพร่กระจายของ LSAs ดังนี้

1. การสร้างการอยู่ติดกันระหว่างเราท์เตอร์ที่ต่อกันทุก ๆ ตัวจะสร้าง LSAs ที่ไม่จำเป็นจำนวนมาก ถ้า n คือจำนวนของเราท์เตอร์บนเครือข่ายแบบเข้าถึงหลายช่องทาง เพราะฉะนั้นจะมีการอยู่ติดกันเท่ากับ $n(n-1)/2$ (ดังรูปที่ 5.2) เราท์เตอร์แต่ละตัวจะกระจาย LSAs เป็นจำนวน n-1 สำหรับเพื่อนบ้านที่อยู่ติดกันกับตัวมันเอง บวกด้วย 1 LSA สำหรับเครือข่าย ได้ผลลัพธ์เท่ากับ n^2 ที่เกิดจากเครือข่าย
2. การแพร่กระจายของเครือข่ายด้วยตัวเองจะสับสน เราท์เตอร์ตัวหนึ่งจะกระจาย LSA หนึ่ง ๆ ไปยังเพื่อนบ้านที่อยู่ติดกันกับตัวมันทั้งหมด ซึ่งโดยรอบแล้ว LSA นั้นจะแพร่กระจายไปยังเพื่อนบ้านที่อยู่ติดกันของพวกมันทั้งหมด ทำให้เกิดการสร้างสำเนาของ LSA เดียวกันบนเครือข่ายเดียวกันเป็นจำนวนมาก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



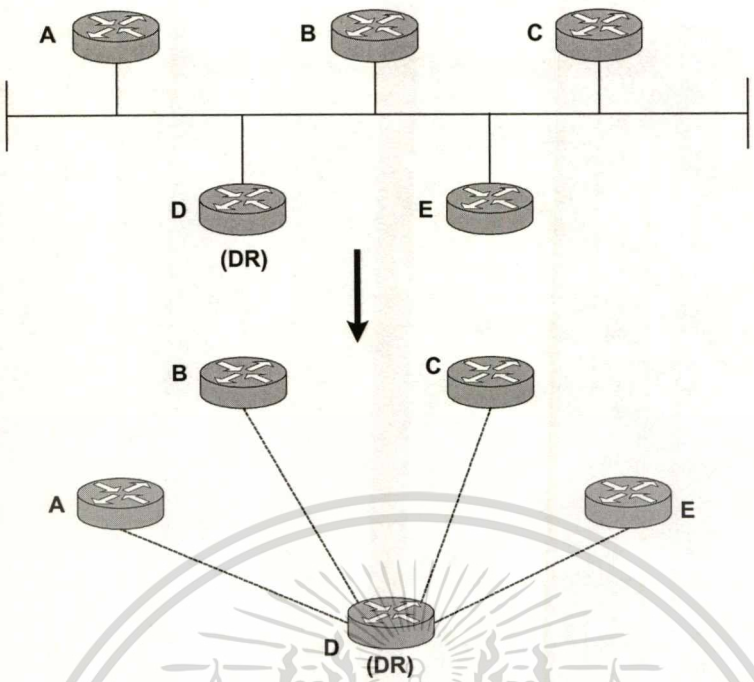
รูปที่ 5.2 รูปแบบการอยู่ติดกันทั้ง 10 เส้นทางสำหรับเราท์เตอร์ 5 เครื่องบนเครือข่าย OSPF ที่มี 25 LSAs

ในเครือข่ายการเข้าถึงหลายช่องทางจึงได้เลือก Designated Router ขึ้นมาเพื่อป้องกันปัญหาดังกล่าวข้างต้น โดยที่ DR มีหน้าที่ดังนี้

1. แทนเครือข่ายการเข้าถึงหลายช่องทางและเราท์เตอร์ที่ต่ออยู่ของตัวมันเองเพื่อเป็นที่พักของเครือข่ายที่เชื่อมต่อกัน
2. เพื่อการจัดการขบวนการในการแพร่กระจายบนเครือข่ายการเข้าถึงหลายช่องทาง

เราท์เตอร์แต่ละตัวบนเครือข่ายจัดรูปแบบการอยู่ติดกันด้วย DR (ดังรูปที่ 5.3) ซึ่ง DR เท่านั้นที่จะส่ง LSAs ไปยังจุดพักของเครือข่ายที่เชื่อมต่อกัน และเพื่อป้องกันปัญหาที่จะทำให้เครือข่ายไม่สามารถส่งผ่านแพ็กเก็ตได้เมื่อ DR เสียหายหรือพังลง คือจะมีการเลือก Backup Designated Router ซึ่งจะทำให้ DR และ BDR กลายเป็นตัวที่อยู่ติดกันเอง ซึ่งถ้าหากว่า DR พัง BDR ก็จะกลายเป็น DR ตัวใหม่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 5.3 รูปแบบการเชื่อมต่อและหน้าที่ของ Designated Router ซึ่งทำให้เราท์เตอร์ตัวอื่น ๆ อยู่ติดกันได้โดยผ่าน DR

กระบวนการในการเลือก DR และ BDR มีดังนี้

1. หลังจากการสื่อสาร 2 ทางได้ถูกสร้างขึ้นกับเพื่อนบ้าน ตรวจสอบสิทธิพิเศษ DR และ BDR ของ Hello แต่ละตัวจากเพื่อนบ้านแล้ว รายชื่อของเราท์เตอร์ทุกตัวมีสิทธิที่จะได้รับเลือก (นั่นคือ เราท์เตอร์ที่มีสิทธิพิเศษที่มากกว่า 0 และมีสถานะของเพื่อนบ้านไม่น้อยกว่า 2 ทาง) เราท์เตอร์ทั้งหมดก็จะประกาศตัวของมันให้เป็น DR และ BDR (แอดเดรสของอินเทอร์เฟสของตัวพวกมันเองที่อยู่ในฟิลด์ DR และ BDR ของแพ็กเก็ต Hello) การคำนวณของเราท์เตอร์ได้รวมถึงตัวมันเองที่อยู่ในรายชื่อนี้ ยกเว้นว่าตัวมันเองไม่มีสิทธิในการรับเลือก
2. จากรายชื่อของเราท์เตอร์ที่มีสิทธิได้รับเลือกจะมีการแบ่ง subset ของเราท์เตอร์ที่ประสงค์จะไม่อ้างสิทธิเป็น DR ออก (เราท์เตอร์ที่ประกาศตัวของพวกมันเองที่เป็น DR จะไม่สามารถถูกเลือกให้เป็น BDR ได้)
3. ถ้าเพื่อนบ้าน 1 ตัวหรือมากกว่าที่อยู่ใน subset นี้รวมถึงแอดเดรสของอินเทอร์เฟสของตัวมันเองในฟิลด์ BDR จะทำให้เพื่อนบ้านที่มีค่าสิทธิพิเศษสูงที่สุดถูกประกาศให้เป็น BDR ในทางพันธะ เราท์เตอร์ที่มี ID เราท์เตอร์สูงที่สุดจะถูกเลือก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4. ถ้าไม่มีเราท์เตอร์ใน subset อ้างสิทธิเป็น BDR เพื่อนบ้านที่มีค่าสิทธิพิเศษสูงที่สุดจะกลายเป็น BDR ในทางพันธะ เพื่อนบ้านที่มี ID เราท์เตอร์สูงที่สุดจะถูกเลือก
5. ถ้ามีเราท์เตอร์ 1 ตัวที่มีสิทธิเข้ารับเลือกหรือมากกว่ารวมทั้งแอดเดรสอินเทอร์เฟสของตัวพวกมันเองในฟิลด์ DR เพื่อนบ้านที่ค่าสิทธิพิเศษสูงที่สุดจะถูกประกาศให้เป็น DR ในทางพันธะ เพื่อนบ้านที่มี ID เราท์เตอร์สูงที่สุดจะถูกเลือก
6. ถ้าไม่มีเราท์เตอร์ประกาศตัวเองเป็น DR BDR ที่ถูกเลือกใหม่จะกลายเป็น DR
7. ถ้าเราท์เตอร์ที่กระทำการคำนวณคือ DR หรือ BDR ที่ถูกเลือกขึ้นใหม่ หรือไม่มี DR หรือ BDR อยู่เลย กระบวนที่ 2 ถึง 6 ก็จะเกิดขึ้นซ้ำ

ถ้ากล่าวโดยง่ายคือ เมื่อเราท์เตอร์ OSPF เริ่มทำงานมันก็จะทำการค้นหาเพื่อนบ้าน โดยจะทำการตรวจสอบ DR และ BDR ที่ทำงานอยู่ ถ้าหากว่ามี DR และ BDR อยู่ก่อนแล้ว เราท์เตอร์ก็จะยอมรับ DR และ BDR ถ้าหากไม่มี BDR เราท์เตอร์ตัวที่มีค่าสิทธิพิเศษสูงที่สุดจะถูกเลือกเป็น BDR แต่ถ้าหากมีเราท์เตอร์มากกว่า 1 ตัวมีค่าสิทธิพิเศษเท่ากัน เราท์เตอร์ตัวที่มี ID เราท์เตอร์สูงที่สุดก็จะได้รับเลือก ถ้าหากไม่มี DR แอกทีฟ BDR ก็จะถูกเลื่อนให้เป็น DR และทำการเลือก BDR ขึ้นใหม่

5.5 OSPF Interfaces

ส่วนประกอบสำคัญของโพรโทคอล link state คือการเชื่อมโยงและสถานะของการเชื่อมโยง ซึ่งก่อนที่จะมีการส่ง Hello ก่อนที่การอยู่ติดกันจะถูกสร้างขึ้น และก่อนที่ LSAs ได้ถูกส่งออกไป เราท์เตอร์ OSPF ต้องเข้าใจการเชื่อมโยงของตัวมันเองก่อน ในหัวข้อนี้อธิบายถึงโครงสร้างข้อมูล OSPF ที่เกี่ยวข้องกับอินเทอร์เฟสและสถานะต่าง ๆ ของอินเทอร์เฟส OSPF

5.5.1 โครงสร้างข้อมูลอินเทอร์เฟส (Interface Data Structure)

เราท์เตอร์ OSPF มีโครงสร้างข้อมูลสำหรับอินเทอร์เฟสที่ใช้งาน OSPF ไว้ ดังรูปที่ 5.4 ซึ่งองค์ประกอบของโครงสร้างข้อมูลอินเทอร์เฟสมีดังนี้

- IP Address และ Mask : องค์ประกอบนี้คือแอดเดรสและมาส์คของอินเทอร์เฟสที่ถูกคอนฟิกไว้ แพ็กเก็ต OSPF ที่เกิดจากอินเทอร์เฟสนี้จะมีแอดเดรสนี้เป็นแอดเดรสต้นกำเนิด (Source Address) ในรูปที่ 5.4 แอดเดรสและมาส์คคือ 192.168.21.21/30
- แอเรีย ID : แอเรียที่อินเทอร์เฟสและเครือข่ายต่ออยู่ ในรูปที่ 5.4 แอเรีย ID เท่ากับ 7
- Process ID : คุณสมบัติพิเศษของ Cisco นี้ไม่ใช่มาตรฐาน แต่เนื่องจากเราท์เตอร์ Cisco มีความสามารถที่จะรันได้หลาย ๆ Process OSPF จึงใช้ Process ID เพื่อแยกความแตกต่าง ในรูปที่ 5.4 Process ID เป็น 1
- Router ID : ในรูปที่ 5.4 Router ID คือ 192.168.30.70

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
Renoir#show ip ospf interface Ethernet0
Ethernet0 is up, line protocol is up
  Internet Address 192.168.17.73/29, Area 0
  Process ID 1, Router ID 192.168.30.70, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.30.70, Interface address 192.168.17.73
  Backup Designated router (ID) 192.168.30.80, Interface address
192.168.17.74
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.30.80  (Backup Designated Router)
  Message digest authentication enabled
    Youngest key id is 10
```

รูปที่ 5.4 ข้อมูลบนอินเทอร์เฟสและชนิดของเครือข่ายแบบ point-to-point

- ชนิดของเครือข่าย : ชนิดของเครือข่ายที่อินเทอร์เฟสถูกต่ออยู่ เช่น broadcast point-to-point NBMA point-to-multipoint หรือ virtual link ในรูปที่ 5.4 ชนิดของเครือข่ายคือ point-to-point
- Cost : ค่า Cost ขาออกสำหรับแพ็กเก็ตที่ถูกส่งออกจากอินเทอร์เฟสนี้ ค่า Cost คือ OSPF metric แสดงได้ด้วย เลขจำนวนเต็ม 16 บิทซึ่งอยู่ในช่วง 1 ถึง 65535 ค่า default เท่ากับ 10^8/BW โดยที่ BW คือค่าแบนด์วิดส์ของอินเทอร์เฟสที่ถูกคอนฟิกไว้ และ 10^8 เป็นแแบนด์วิดส์อ้างอิง ในรูปที่ 5.4 ค่าแบนด์วิดส์ที่ถูกคอนฟิกไว้มีค่าเท่ากับ 128K (ไม่ได้แสดงไว้ในรูป) เพราะฉะนั้นค่า Cost จะเท่ากับ 10^8/128K = 781
- InfTransDelay : เวลาในการปรากฏ LSA
- State : สถานะหน้าที่ของอินเทอร์เฟส
- ค่าสิทธิพิเศษเราท์เตอร์ : จำนวนเต็ม 8 บิทที่อยู่ในช่วง 0 ถึง 255 เพื่อเลือก DR และ BDR ค่าสิทธิพิเศษนี้ไม่ได้ถูกแสดงไว้ในรูปที่ 5.4 เพราะชนิดของเครือข่ายเป็นแบบจุดต่อจุด จึงทำให้ไม่มี DR หรือ BDR ในเครือข่ายชนิดนี้ ในรูปที่ 5.5 แสดงอินเทอร์เฟส OSPF อื่นในเราท์เตอร์ตัวเดียวกัน อินเทอร์เฟสนี้แสดงให้เห็นถึงชนิดของเครือข่ายที่ต่ออยู่เป็นแบบ broadcast ดังนั้น DR และ BDR จะถูกเลือก ค่าสิทธิพิเศษที่แสดงในรูปมีค่าเป็น 1
- Designated Router : DR สำหรับเครือข่ายที่ซึ่งอินเทอร์เฟสถูกต่ออยู่ได้ถูกบันทึกไว้ทั้งเราท์เตอร์ ID ของตัวเอง และแอดเดรสของอินเทอร์ที่ต่ออยู่กับเครือข่าย ในรูปที่ 5.5 DR คือ 192.168.30.70 และแอดเดรสของอินเทอร์เฟสเป็น 192.168.17.73
- Backup Designated Router : BDR สำหรับเครือข่ายที่ซึ่งอินเทอร์เฟสถูกต่ออยู่ได้ถูกบันทึกไว้ทั้งเราท์เตอร์ ID ของตัวมันเอง และแอดเดรสของอินเทอร์เฟสที่ต่ออยู่ ในรูปที่ 5.5 BDR คือ 192.168.30.80 และแอดเดรสอินเทอร์เฟสคือ 192.168.17.74

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
Renoir#show ip ospf interface Serial1.738
Serial1.738 is up, line protocol is up
  Internet Address 192.168.21.21/30, Area 7
  Process ID 1, Router ID 192.168.30.70, Network Type Point_To_Point, Cost:
781
  Transmit Delay is 1 sec, State Point_To_Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.30.77
  Message digest authentication enabled
    Youngest key id is 10
```

รูปที่ 5.5 อินเทอร์เฟสที่มีชนิดของเครือข่ายแบบ broadcast และเราท์เตอร์เป็น DR

- HelloInterval : คาบเวลา (มีหน่วยเป็นวินาที) ระหว่างการส่งแพ็กเก็ต Hello บนอินเทอร์เฟส คาบเวลานี้ถูกประกาศในแพ็กเก็ต Hello ที่ถูกส่งจากอินเทอร์เฟส ค่า Default เท่ากับ 10 วินาที
- RouterDeadInterval : คาบเวลา (หน่วยเป็นวินาที) ที่เราท์เตอร์จะคอยรับ Hello จากเพื่อนบ้านบนเครือข่าย ซึ่งอินเทอร์เฟสถูกเชื่อมต่อก่อนการแจ้งว่าเพื่อนบ้านหายไป RouterDeadInterval ได้ถูกประกาศอยู่ในแพ็กเก็ต Hello ที่ส่งจากอินเทอร์เฟส ค่า Default เท่ากับ 4 เท่าของ HelloInterval
- Wait Timer : ช่วงเวลาที่เราท์เตอร์ใช้คอย DR และ BDR เพื่อการประกาศไปในแพ็กเก็ต Hello ของเพื่อนบ้านก่อนการเริ่มต้นเลือก DR และ BDR ช่วงเวลาของ Wait Timer เท่ากับ RouterDeadInterval
- RxmtInterval : คาบเวลา (หน่วยเป็นวินาที) ที่เราท์เตอร์จะคอยการส่งแพ็กเก็ต OSPF ซ้ำเมื่อไม่มีการตอบรับ (acknowledge) ค่า Default เป็น 5 วินาที
- Hello Timer : เวลาที่ถูกตั้งให้กับ HelloInterval แพ็กเก็ต Hello ได้ถูกส่งจากอินเทอร์เฟสเมื่อ Hello Timer หมดลง
- Neighboring Routers : รายชื่อเพื่อนบ้านทั้งหมดบนเครือข่ายที่ต่ออยู่ รูปที่ 5.6 แสดงถึงอินเทอร์เฟสอื่นบนเราท์เตอร์ตัวเดียวกัน มี 5 เพื่อนบ้านที่เป็นที่รู้จักบนเครือข่าย แต่มีเพียงการอยู่ติดกันเท่ากับ 2 ตัว (เราท์เตอร์ ID ของเพื่อนบ้านเท่านั้นที่ถูกแสดง) เราท์เตอร์ได้สร้างการอยู่ติดกันกับ DR และ BDR เท่านั้น
- Au Type : ชนิดของการแสดงการมีตัวตน (Authentication) ที่ใช้กับเครือข่าย ชนิดของการแสดงการมีตัวตนอาจจะเป็น Null (ไม่มีการแสดงการมีตัวตน) รหัสผ่านแบบง่าย (Simple Password) หรือ Cryptographic (Message Digest)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- Authentication Key : ใช้รหัสผ่านขนาด 64 บิท ถ้าหากการแสดงการมีตัวตนอย่างง่ายถูกใช้งานกับอินเทอร์เฟส หรือใช้ message digest key ถ้าใช้การแสดงการมีตัวตนแบบ Cryptographic

```
Renoir#show ip ospf interface Ethernet1
Ethernet1 is up, line protocol is up
  Internet Address 192.168.32.4/24, Area 78
  Process ID 1, Router ID 192.168.30.70, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 192.168.30.254, Interface address 192.168.32.2
  Backup Designated router (ID) 192.168.30.80, Interface address
192.168.32.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Neighbor Count is 5, Adjacent neighbor count is 2
    Adjacent with neighbor 192.168.30.80  (Backup Designated Router)
    Adjacent with neighbor 192.168.30.254  (Designated Router)
  Message digest authentication enabled
    Youngest key id is 10
```

รูปที่ 5.6 รูปแบบเราท์เตอร์ที่สามารถมองเห็นเพื่อนบ้านได้ 5 เครื่องด้วยรูปแบบการอยู่ติดกันโดยผ่าน DR และ BDR

ในรูปที่ 5.7 แสดงให้เห็นถึงอินเทอร์เฟสที่ถูกเชื่อมต่อกับเครือข่าย NBMA สังเกตว่าค่า Default ของ HelloInterval เท่ากับ 30 วินาที และค่า Default ของ RouterDeadInterval เท่ากับ 4 เท่าของ HelloInterval

```
Renoir#show ip ospf interface Serial3
Serial3 is up, line protocol is up
  Internet Address 192.168.16.41/30, Area 0
  Process ID 1, Router ID 192.168.30.105, Network Type NON_BROADCAST, Cost:
64
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 192.168.30.210, Interface address 192.168.16.42
  Backup Designated router (ID) 192.168.30.105, Interface address
192.168.16.41
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    Hello due in 00:00:08
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.30.210  (Designated Router)
```

รูปที่ 5.7 รูปแสดงอินเทอร์เฟสที่ถูกต่อกับเครือข่ายเฟรมรีเลย์ NBMA และทำหน้าที่เป็น BDR

5.5.2 The Interface State Machine

อินเทอร์เฟสที่ใช้ OSPF จะผ่านสถานะหลายอย่างก่อนที่อินเทอร์เฟสนั้นจะทำงานได้อย่างเต็มที่ สถานะเหล่านั้นได้แก่ การลง (Down) การเชื่อมต่อจุดต่อจุด (Point-to-Point) การรอคอย (Waiting) DR การสำรอง (Backup) Drother และ Loopback

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Down : เป็นสถานะเริ่มต้นของอินเทอร์เฟส ซึ่งเป็นสถานะที่อินเทอร์เฟสไม่สามารถทำงานได้และไม่มีทราฟฟิกถูกส่งหรือรับผ่านอินเทอร์เฟส

Point-to-Point : สถานะนี้เหมาะสมกับอินเทอร์เฟสที่เชื่อมต่อกับเครือข่ายแบบจุดต่อจุด จุดต่อหลายจุด และการเชื่อมโยงเสมือน เท่านั้น เมื่ออินเทอร์เฟสเข้าสู่สถานะนี้ มันจะเริ่มต้นส่งแพ็กเก็ต Hello ไปยังทุก ๆ ช่วงเวลา HelloInterval และจะพยายามสร้างการอยู่ติดกันกับเพื่อนบ้านที่ปลายทางของการเชื่อมโยง

Waiting : สถานะนี้เหมาะสมกับอินเทอร์เฟสที่เชื่อมต่อกับเครือข่ายแบบ broadcast และ NBMA เท่านั้น เมื่ออินเทอร์เฟสเข้าสู่สถานะนี้ มันจะเริ่มส่งและรับแพ็กเก็ต Hello และเซ็ทค่า wait timer เราท์เตอร์จะพยายามระบุ DR และ BDR ของเครือข่ายขณะที่อยู่ในสถานะนี้

DR : ในสถานะนี้ เราท์เตอร์ที่เป็น DR จะสร้างการอยู่ติดกันกับเราท์เตอร์ตัวอื่น ๆ ที่อยู่บนเครือข่ายแบบเข้าถึงได้หลายช่องทาง

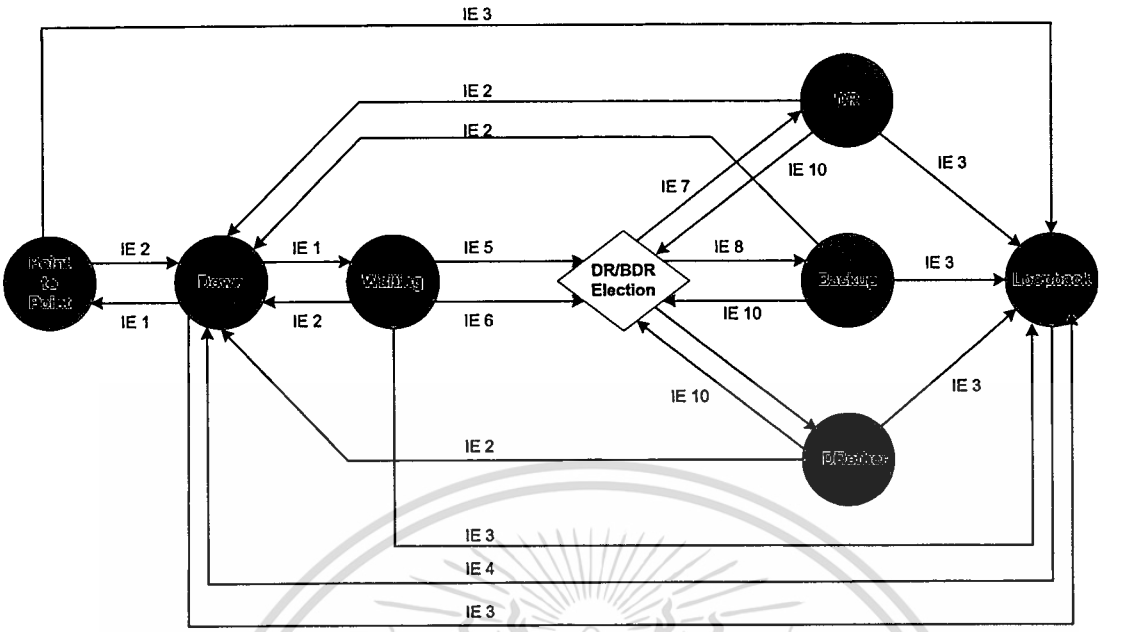
Backup : ในสถานะนี้ เราท์เตอร์ที่เป็น BDR จะสร้างการอยู่ติดกันกับเราท์เตอร์ตัวอื่น ๆ ที่อยู่บนเครือข่ายแบบเข้าถึงได้หลายช่องทาง

DRother : ในสถานะนี้ เราท์เตอร์ที่ไม่ใช่ทั้ง DR และ BDR จะสร้างการอยู่ติดกันกับ DR และ BDR เท่านั้น

Loopback : ในสถานะนี้ อินเทอร์เฟสได้ถูกลูปกลับโดยผ่านทาง software หรือ hardware ถึงแม้ว่าแพ็กเก็ตไม่สามารถส่งผ่านด้วยอินเทอร์เฟสนี้ ค่าแอดเดรสของอินเทอร์เฟสก็ยังคงถูกประกาศไปใน LSAs เราท์เตอร์ได้ เพื่อที่ว่าแพ็กเก็ต Test สามารถค้นหาเส้นทางของพวกมันเองได้

จากรูปที่ 5.8 แสดงให้เห็นถึงสถานะอินเทอร์เฟส OSPF และเหตุการณ์ด้านอินพุทที่จะเกิดจากการส่งผ่านในแต่ละขั้นตอน เหตุการณ์ด้านอินพุทได้ถูกอธิบายไว้ในตารางที่ 5.1

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 5.8 รูปแบบกลไกของ OSPF interface state machine

5.6 OSPF Neighbors

ในหัวข้อนี้อธิบายนี้ถึงความสัมพันธ์ของเราท์เตอร์กับเพื่อนบ้านที่อยู่บนเครือข่าย จุดประสงค์สุดท้ายของความสัมพันธ์ของเพื่อนบ้านคือการสร้างการอยู่ติดกันด้วยข้อมูลเส้นทาง (Routing Information) การอยู่ติดกันได้ถูกสร้างขึ้นโดยผ่านขั้นตอนทั่วไป 4 อย่าง คือ

1. การค้นพบเพื่อนบ้าน
2. การสื่อสารแบบ 2 ทิศทาง : การสื่อสารนี้สำเร็จลงได้ต่อเมื่อเพื่อนบ้าน 2 ตัวลงรายชื่อ Router ID ซึ่งกันและกันลงในแพ็กเก็ต Hello ของพวกมัน
3. การจัดทำฐานข้อมูลให้ตรงกัน : รายละเอียดของฐานข้อมูล การร้องขอสถานะการเชื่อมโยง และแพ็กเก็ตที่อัพเดตสถานะการเชื่อมโยง ได้ถูกแลกเปลี่ยนกันเพื่อให้แน่ใจว่าเพื่อนบ้านทั้งคู่มีข้อมูลเหมือนกัน จุดประสงค์สำหรับกระบวนการนี้คือ เพื่อให้เพื่อนบ้านตัวหนึ่งเป็น master และอีกตัวเป็น slave ซึ่งตัว master จะทำหน้าที่ควบคุมการแลกเปลี่ยนแพ็กเก็ตที่เกี่ยวกับรายละเอียดของฐานข้อมูล
4. การอยู่ติดกันอย่างสมบูรณ์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 5.1 เหตุการณ์อินพุทสำหรับกลไกที่บ่งบอกถึงสถานะของอินเทอร์เฟส

เหตุการณ์อินพุท	รายละเอียด
IE 1	โพรโทคอลระดับล่างบ่งบอกว่าอินเทอร์เฟสของเครือข่ายมีการทำงาน
IE 2	โพรโทคอลระดับล่างบ่งบอกว่าอินเทอร์เฟสของเครือข่ายไม่มีการทำงาน
IE 3	ตัวจัดการเครือข่าย หรือโพรโทคอลระดับล่างบ่งบอกว่าอินเทอร์เฟสมีการลูปเกิดขึ้น
IE 4	ตัวจัดการเครือข่าย หรือโพรโทคอลระดับล่างบ่งบอกว่าอินเทอร์เฟสไม่มีการลูป
IE 5	ได้รับแพ็กเก็ต Hello ในกรณีที่เพื่อนบ้านตัวต้นกำเนิดแสดงรายชื่อของตัวเองเป็น BDR หรือไม่ก็ได้รับแพ็กเก็ต Hello ในกรณีที่เพื่อนบ้านตัวต้นกำเนิดแสดงรายชื่อของตัวเองเป็น DR และบ่งบอกว่าไม่มี BDR
IE 6	เวลาในการคอย (wait timer) สิ้นสุดลง
IE 7	เราท์เตอร์ถูกเลือกเป็น DR สำหรับเครือข่ายนี้
IE 8	เราท์เตอร์ถูกเลือกเป็น BDR สำหรับเครือข่ายนี้
IE 9	เราท์เตอร์ไม่ถูกเลือกให้เป็น DR หรือ BDR สำหรับเครือข่ายนี้
IE 10	การเปลี่ยนแปลงเกิดขึ้นกับกลุ่มเพื่อนบ้านบนเครือข่ายนี้ การเปลี่ยนแปลงนี้อาจเกิดได้จาก (1) มีการสร้างการสื่อสาร 2 ทางกับเพื่อนบ้าน (2) สูญเสียการสื่อสาร 2 ทางกับเพื่อนบ้าน (3) ได้รับ Hello ในกรณีที่เพื่อนบ้านตัวต้นกำเนิดแสดงรายชื่อรายใหม่ของตัวเองเป็น DR หรือ BDR (4) ได้รับ Hello จาก DR ในกรณีที่เราท์เตอร์ถูกแสดงรายชื่อว่าสูญหาย (5) ได้รับ Hello จาก BDR ในกรณีที่เราท์เตอร์ถูกแสดงรายชื่อว่าสูญหาย (6) การสิ้นสุดของ RouterDeadInterval โดยไม่ได้รับ Hello จาก DR หรือ BDR หรือทั้งคู่

ตามที่ได้อธิบายไว้ก่อนหน้านี้ว่า ความสัมพันธ์ของเพื่อนบ้านได้ถูกสร้างขึ้นและถูกรักษาไว้โดยการแลกเปลี่ยนแพ็กเก็ต Hello บนเครือข่ายแบบ broadcast และ point-to-point แพ็กเก็ต Helloใช้การ multicast ไปยังเราท์เตอร์ทุกตัว (224.0.0.5) บนเครือข่ายแบบ NBMA point-to-multipoint และ virtual link แพ็กเก็ต Hello ใช้การ unicast ไปยังเพื่อนบ้านเป็นราย ๆ ไป ความสัมพันธ์ของการ unicast คือเราท์เตอร์ต้องมีการเรียนรู้ความเป็นอยู่ของเพื่อนบ้านของตัวเองก่อนโดยวิธีการคอนฟิกด้วยมือ หรือด้วยกลไก เช่น Inverse ARP

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5.6.1 Neighbor State Machine

เราท์เตอร์ OSPF จะมีการส่งมอบเพื่อนบ้านผ่านกระบวนต่าง ๆ ก่อนที่เพื่อนบ้านจะถูกพิจารณาให้เป็นการอยู่ติดกันอย่างสมบูรณ์

Down : สถานะเริ่มต้นของการสนทนากันของเพื่อนบ้านซึ่งชี้ว่า ไม่มี Hello ได้ยินเพื่อนบ้านในช่วงเวลา RouterDeadInterval ครั้งสุดท้าย Hello จะไม่ถูกส่งไปยังเพื่อนบ้านที่ down ยกเว้นว่าเพื่อนบ้านเหล่านั้นอยู่บนเครือข่าย NBMA ซึ่งในกรณีนี้ Hello จะถูกส่งทุก ๆ PollInterval ถ้าเพื่อนบ้านมีการส่งผ่านไปถึงสถานะที่ down จากสถานะที่สูงกว่า รายการของการส่งสถานะการเชื่อมโยงซ้ำ รายการผลรวมของฐานข้อมูล และรายการร้องขอสถานะการเชื่อมโยงจะถูกลบทิ้ง

Attempt : สถานะนี้ใช้กับเพื่อนบ้านที่อยู่บนเครือข่าย NBMA เท่านั้น โดยที่เพื่อนบ้านถูกคอนฟิกด้วยมือ เราท์เตอร์ซึ่งได้รับเลือกเป็น DR จะส่งผ่านเพื่อนบ้านไปยังสถานะ Attempt เมื่ออินเทอร์เฟสกับเพื่อนบ้านครั้งแรกแล้วแอกทีฟ หรือเมื่อเราท์เตอร์เป็น DR หรือ BDR เราท์เตอร์จะส่งแพ็กเก็ตไปยังเพื่อนบ้านในสถานะ Attempt ที่เวลา HelloInterval

Init : สถานะนี้ชี้ว่าแพ็กเก็ต Hello ได้ถูกมองเห็นจากเพื่อนบ้านในช่วง RouterDeadInterval สุดท้าย แต่การสื่อสาร 2 ทางยังไม่ได้ถูกสร้างขึ้น เราท์เตอร์จะรวมเอา Router ID ของเพื่อนบ้านทั้งหมดเข้าไปในสถานะนี้หรือสูงกว่าสถานะนี้เข้าไปในฟิลด์เพื่อนบ้านของแพ็กเก็ต Hello

2-Way : สถานะนี้แสดงให้เห็นว่าเราท์เตอร์ได้เห็น Router ID ของตัวมันเองในฟิลด์เพื่อนบ้านของแพ็กเก็ต Hello ที่มาจากเพื่อนบ้าน ซึ่งหมายความว่าการสนทนา 2 ทิศทางได้ถูกสร้างขึ้นแล้ว บนเครือข่ายแบบเข้าถึงได้ปลายช่องทาง เพื่อนบ้านต้องอยู่ในสถานะนี้หรือสูงหว่านี้เพื่อมีสิทธิเข้ารับเลือกเป็น DR หรือ BDR การต้อนรับแพ็กเก็ตที่บอกถึงรายละเอียดของฐานข้อมูลจากเพื่อนบ้านในสถานะ Init จะทำให้เกิดการส่งผ่านแบบ 2 ทางด้วย

ExStart : ในสถานะนี้ เราท์เตอร์และเพื่อนบ้านของมันสร้างความสัมพันธ์กับ master/slave และกำหนดลำดับเลขหมาย DD เริ่มต้น ในการเตรียมการสำหรับการแลกเปลี่ยนแพ็กเก็ตที่บอกถึงรายละเอียดของฐานข้อมูล เพื่อนบ้านที่มีแอดเดรสอินเทอร์เฟสสูงที่สุดจะได้เป็น master

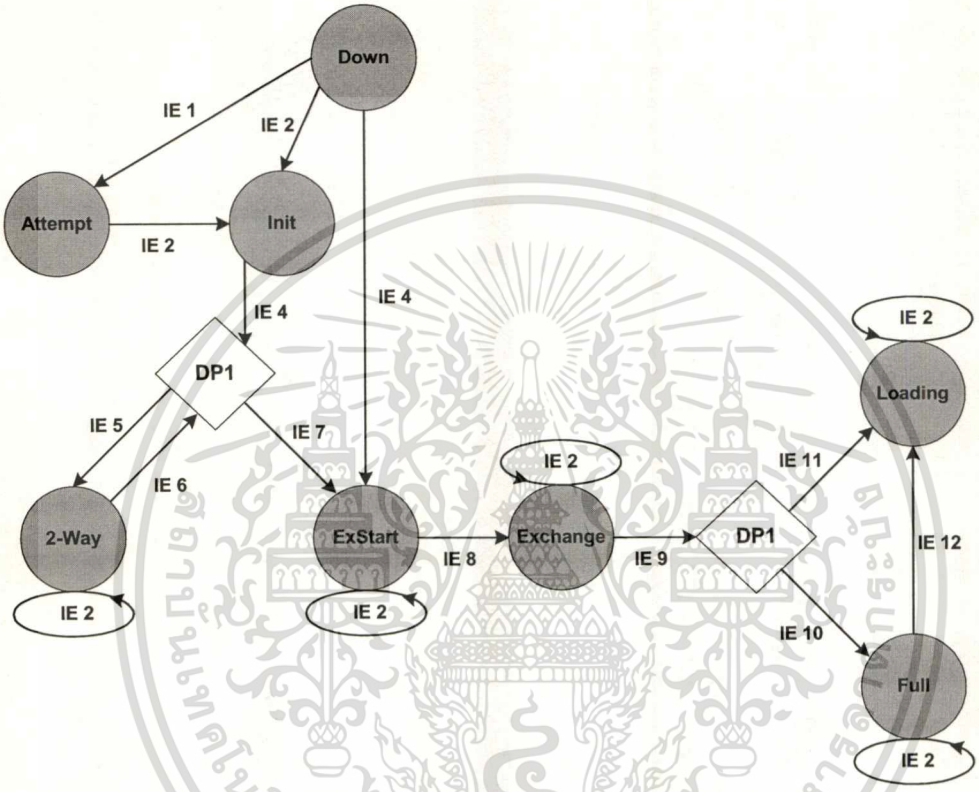
Exchange : เราท์เตอร์ส่งแพ็กเก็ตที่บอกถึงรายละเอียดของฐานข้อมูลที่อธิบายถึงฐานข้อมูลของสถานะการเชื่อมโยงทั้งหมดของตัวเองแกเพื่อนบ้านที่อยู่ในสถานะ Exchange เราท์เตอร์สามารถส่งแพ็กเก็ตการร้องขอสถานะการเชื่อมโยง (การร้องขอ LSAs เพิ่ม) แก่เพื่อนบ้านในสถานะนี้ได้ด้วย

Loading : เราท์เตอร์จะส่งแพ็กเก็ตการร้องขอสถานะการเชื่อมโยงแก่เพื่อนบ้านที่อยู่ในสถานะ Loading การร้องขอ LSAs เพิ่มท่ได้ถูกค้นพบในสถานะ Exchange แต่ยังไม่ได้รับ

Full : เพื่อนบ้านในสถานะนี้คือการอยู่ติดกันอย่างสมบูรณ์ และการอยู่ติดกันจะปรากฏอยู่ใน Router LSAs และ Network LSAs

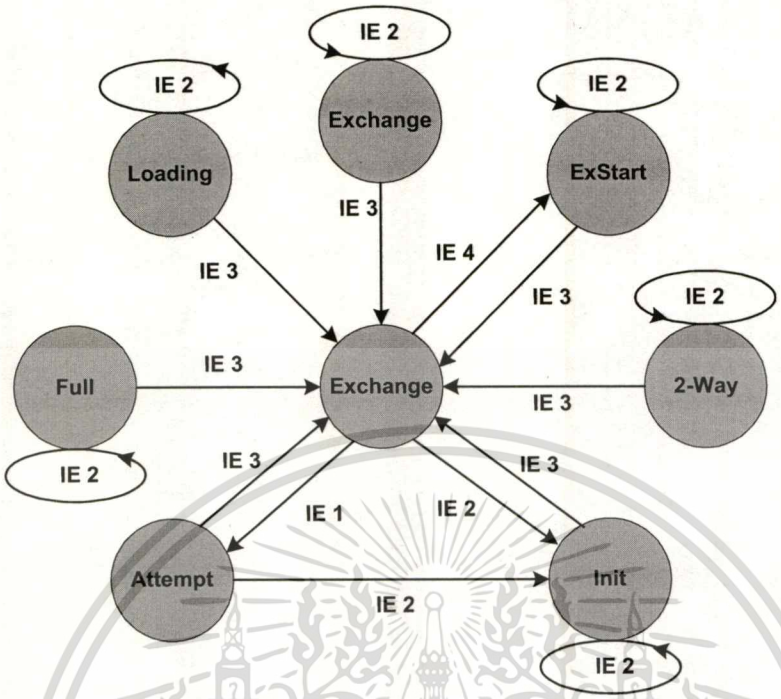
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในรูปที่ 5.10 ถึง 5.12 แสดงถึงสถานะเพื่อนบ้าน OSPF และเหตุการณ์ของอินพุทที่จะทำให้เกิดสถานะการส่งผ่าน เหตุการณ์ของอินพุทได้ถูกอธิบายไว้ในตารางที่ 5.2 และจุดในการตัดสินใจได้ถูกกำหนดในตารางที่ 5.3 รูปที่ 5.9 แสดงขบวนการแบบปกติจากสถานะการทำงานที่น้อยที่สุดไปยังสถานะที่สมบูรณ์แบบ รูปที่ 5.10 และ 5.11 แสดงกลไกของสถานะเพื่อนบ้าน OSPF ที่สมบูรณ์

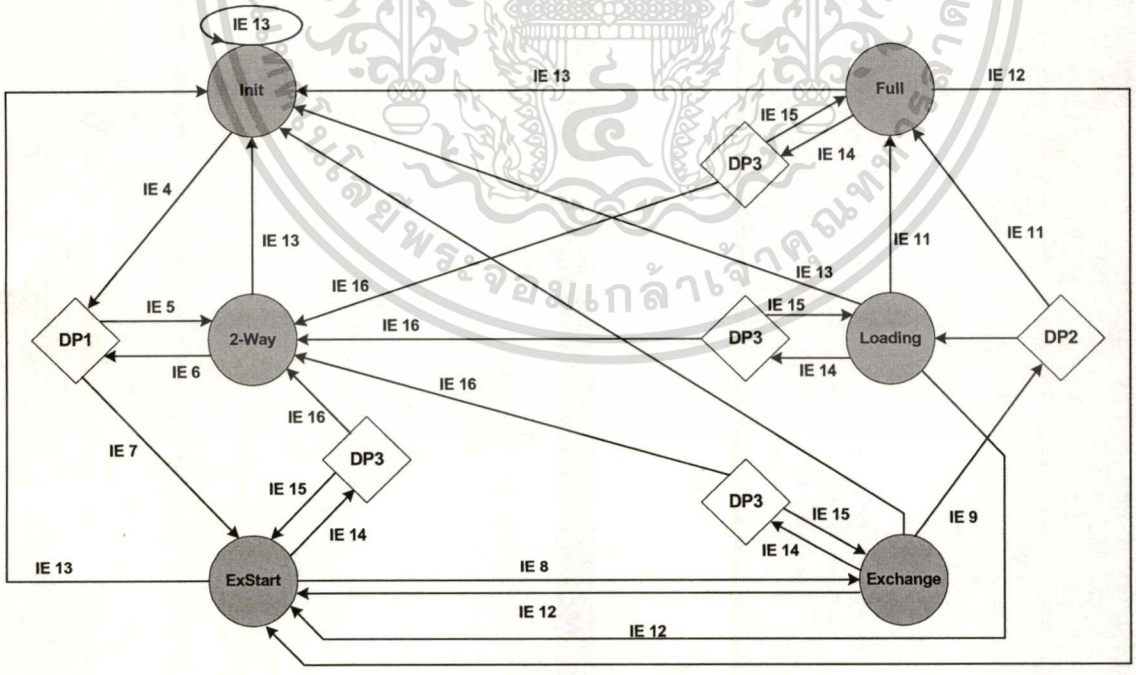


รูปที่ 5.9 รูปแบบกลไก OSPF ในการมองหาเพื่อนบ้านจากสภาวะ Down เป็น Full

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 5.10 รูปแบบกลไกในการจัดหาเพื่อนบ้านจากสภาวะ Down เป็น Init



รูปที่ 5.11 รูปแบบกลไกการจัดหาเพื่อนบ้านจากสภาวะ Init เป็น Full

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 5.2 เหตุการณ์ที่เกิดขึ้นในรูปที่ 5.9 5.10 และ 5.11

เหตุการณ์อินพุท	รายละเอียด
IE 1	เหตุการณ์นี้เกิดขึ้นกับเพื่อนบ้านที่เชื่อมต่อแบบ NBMA เท่านั้น เหตุการณ์อินพุทจะถูกทริกภายใต้เงื่อนไข ดังนี้ (1) อินเทอร์เฟสที่ต่อกับเครือข่าย NBMA เป็น active และเพื่อนบ้านมีสิทธิเหมาะสมกับการเข้ารับเลือกเป็น DR (2) เราท์เตอร์กลายเป็น DR หรือ BDR และเพื่อนบ้านไม่เหมาะสมที่จะได้รับการคัดเลือกเป็น DR
IE 2	ได้รับแพ็กเก็ต Hello จากเพื่อนบ้าน
IE 3	เพื่อนบ้านไม่สามารถมาถึงได้ตามที่กำหนดไว้โดยโพรโทคอลระดับล่าง โดยคำแนะนำที่แน่นอนจากกระบวนการ OSPF ในตัวเอง หรือโดยการสิ้นสุดของเวลา
IE 4	เราท์เตอร์ตัวแรกพบ Router ID ของตัวมันเองในรายชื่อที่อยู่ในฟิลด์ Neighbor ของแพ็กเก็ต Hello ของเพื่อนบ้าน หรือได้รับแพ็กเก็ต Database Description จากเพื่อนบ้าน
IE 5	เพื่อนบ้านจะไม่กลายเป็นการอยู่ติดกัน
IE 6	เหตุการณ์อินพุทเกิดขึ้นภายใต้เงื่อนไข ดังนี้ (1) สถานะเพื่อนบ้านตัวแรกส่งมอบเป็น 2 ทาง (2) สถานะอินเทอร์เฟสเปลี่ยนแปลง
IE 7	การอยู่ติดกันควรจะถูกจัดอยู่ในรูปเพื่อนบ้าน
IE 8	ความสัมพันธ์ master/slave ได้ถูกสร้างขึ้น และแลกเปลี่ยนหมายเลขลำดับ DD ระหว่างกัน
IE 9	การแลกเปลี่ยนแพ็กเก็ต Database Description เสร็จสมบูรณ์
IE 10	แพ็กเก็ต Database Description ปรากฏอยู่ในรายชื่อของ Link State Request
IE 11	รายชื่อของ Link State Request ว่างเปล่า
IE 12	การอยู่ติดกันควรจะถูกทำลายและเริ่มต้นใหม่ เหตุการณ์อินพุทอาจจะถูกทริกโดยสิ่งต่าง ๆ ดังนี้ (1) การได้รับแพ็กเก็ต Database Description ด้วยหมายเลขลำดับ DD ที่ไม่ได้คาดหวังไว้ (2) การได้รับแพ็กเก็ต Database Description ด้วยฟิลด์ option ที่เซ็ทไว้แตกต่างกว่าฟิลด์ option ของแพ็กเก็ต DD สุดท้าย (3) การได้รับแพ็กเก็ต Database Description ในกรณีที่บิท Init ถูกเซ็ท

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

	(4) การได้รับแพ็กเก็ต Link State Request สำหรับ LSA ที่ไม่อยู่ในฐานข้อมูล
IE 13	แพ็กเก็ต Hello ถูกรับมาจากเพื่อนบ้าน ซึ่ง Router ID ของเราท์เตอร์ด้านรับข้อมูลไม่ถูกเก็บรายชื่อในฟิลด์เพื่อนบ้าน
IE 14	เหตุการณ์นี้เกิดขึ้นเมื่อสถานะอินเทอร์เฟสเปลี่ยน
IE 15	การปรากฏหรือการประกอบการอยู่ติดกันด้วยเพื่อนบ้าน จะดำเนินต่อไป
IE 16	การปรากฏหรือการประกอบการอยู่ติดกันด้วยเพื่อน จะไม่ดำเนินต่อไป

ตารางที่ 5.3 จุดตัดสินใจสำหรับรูปที่ 5.9 และ 5.11

การตัดสินใจ	รายละเอียด
DP1	การอยู่ติดกันควรจะถูกสร้างด้วยเพื่อนบ้านหรือไม่ การอยู่ติดกันควรจะถูกประกอบขึ้นถ้าเงื่อนไขข้อใดข้อหนึ่งเป็นจริง ดังนี้ (1) ชนิดเครือข่ายเป็นแบบจุดต่อจุด (2) ชนิดเครือข่ายเป็นแบบจุดต่อหลายจุด (3) ชนิดเครือข่ายเป็นแบบการเชื่อมโยงเสมือน (4) เราท์เตอร์เป็น DR ของเครือข่ายที่ซึ่งเพื่อนบ้านตั้งอยู่ (5) เราท์เตอร์เป็น BDR ของเครือข่ายที่ซึ่งเพื่อนบ้านตั้งอยู่ (6) เพื่อนบ้านคือ DR (7) เพื่อนบ้านคือ BDR
DP2	รายชื่อ Link State Request ของเพื่อนบ้านนี้ว่างเปล่าหรือไม่
DP3	การปรากฏหรือการประกอบการอยู่ติดกันกับเพื่อนบ้านควรดำเนินต่อไปหรือไม่

5.7 การสร้างการอยู่ติดกัน (Building an Adjacency)

เพื่อนบ้านที่อยู่บนเครือข่ายแบบจุดต่อจุด จุดต่อหลายจุด และการเชื่อมโยงเสมือนจะกลายเป็นเพื่อนบ้านกันเสมอ ยกเว้นว่าค่าพารามิเตอร์ของ Hello ไม่ตรงกัน บนเครือข่ายแบบ broadcast และ NBMA DR และ BDR จะกลายเป็นการอยู่ติดกันกับเพื่อนบ้านทั้งหมด แต่การอยู่ติดกันจะไม่มีอยู่ระหว่าง Drothers ด้วยกัน

กระบวนการสร้างการอยู่ติดกันใช้แพ็กเก็ต OSPF อยู่ 3 ชนิด ดังนี้

1. แพ็กเก็ต Database Description (Type 2)
2. แพ็กเก็ต Link State Request (Type 3)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3. แพ็กเก็ต Link State Update (Type 4)

แพ็กเก็ต Database Description มีความสำคัญอย่างยิ่งต่อกระบวนการสร้างการอยู่ติดกัน แพ็กเก็ตนี้ทำหน้าที่นำพารายละเอียดผลสรุปของ LSA แต่ละตัวเข้าไปในฐานข้อมูลสถานะการเชื่อมโยงของเราท์เตอร์ตัวกำเนิด รายละเอียดเหล่านี้ไม่ใช่ LSAs ที่สมบูรณ์ แต่เป็นข้อมูลที่เพียงพอสำหรับเราท์เตอร์ด้านรับเพื่อตัดสินใจว่ามันมีสำเนาล่าสุดของ LSA อยู่ในฐานข้อมูลของตัวมันเองหรือไม่ นอกจากนี้ แฟลก (Flag) 3 ตัวในแพ็กเก็ต DD ถูกใช้สำหรับจัดการกระบวนการสร้างการอยู่ติดกัน ดังนี้

1. บิท I หรือบิทเริ่มแรก (Initial bit) เมื่อถูกเซ็ทจะชี้ให้เห็นว่า แพ็กเก็ต DD แพ็กเก็ตแรกได้ส่งออกไป
2. บิท M หรือบิท More ซึ่งเมื่อถูกเซ็ท จะชี้ให้เห็นว่าแพ็กเก็ต DD ไม่ใช่แพ็กเก็ตสุดท้ายที่ส่งออกไป
3. บิท MS หรือบิท Master/Slave ซึ่งถูกเซ็ทในแพ็กเก็ต DD ที่เกิดจาก master

เมื่อการเจรจาของ master/slave เริ่มขึ้นในสถานะ ExStart เพื่อนบ้านทั้งคู่จะเรียกร้องสิทธิเพื่อเป็น master โดยการส่งแพ็กเก็ต DD ที่ว่างเปล่าด้วยบิท MS ที่เซ็ทเป็น 1 หมายเลขลำดับของ DD ใน 2 แพ็กเก็ตนี้จะถูกเซ็ทตามความคิดของเราท์เตอร์ด้านต้นกำเนิดตามที่มันควรจะเป็น เพื่อนบ้านที่มี Router ID ต่ำที่สุดจะกลายเป็น slave และจะตอบกลับด้วยแพ็กเก็ต DD ที่มีบิท MS เป็น 0 และมีหมายเลขลำดับ DD ที่ถูกเซ็ทตามหมายเลขลำดับของ master แพ็กเก็ต DD นี้จะเป็นแพ็กเก็ตแรกที่อาศัยอยู่กับผลรวมของ LSA เมื่อการเจรจาของ master/slave เสร็จสิ้น สถานะเพื่อนบ้านจะส่งต่อไปยัง Exchange

ในสถานะ Exchange เพื่อนบ้านจะทำให้ฐานข้อมูลสถานะการเชื่อมโยงสอดคล้องกันโดยการพิจารณาค่าที่มีอยู่ทั้งหมดในฐานข้อมูลสถานะการเชื่อมโยงโดยลำดับ รายการผลรวมของฐานข้อมูลได้ถูกรวมกับ Header ของ LSAs ทั้งหมดที่มีอยู่ในฐานข้อมูลของเราท์เตอร์ แพ็กเก็ตรายละเอียดของฐานข้อมูลที่บรรจุอยู่ใน Header ของ LSA ที่ถูกขึ้นรายการไว้จะถูกส่งไปยังเพื่อนบ้าน

ถ้าเราท์เตอร์เห็นว่าเพื่อนบ้านของมันมี LSA ที่ไม่ได้อยู่ในฐานข้อมูลของตัวเอง หรือไม่ก็เพื่อนบ้านมีสำเนาของ LSA ที่รู้จักก่อนหน้านี้ เราท์เตอร์จะจัดวาง LSA เข้าไปในรายการร้องขอสถานะการเชื่อมโยง หลังจากนั้นเราท์เตอร์ส่งแพ็กเก็ตร้องขอสถานะการเชื่อมโยงเพื่อขอสำเนา LSA ที่สมบูรณ์ แพ็กเก็ต update สถานะการเชื่อมโยงก็จะพา LSA ที่ถูกร้องขอมาให้ ขณะที่ได้รับ LSA ที่ถูกร้องขอ พวกมันจะถูกลบออกจากรายการร้องขอสถานะการเชื่อมโยง

LSAs ทั้งหมดที่ส่งไปในแพ็กเก็ต update ต้องถูกรับรอง (acknowledge) เป็นรายตัว เพราะฉะนั้น LSA ที่ถูกส่งออกไปซึ่งได้เข้าไปอยู่ในรายการการส่งสถานะการเชื่อมโยงซ้ำ เมื่อ LSA ถูกรับรองก็จะถูกลบออกจากรายการ LSA อาจจะถูกรับรองได้ด้วย 1 ใน 2 วิธี ดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- Explicit Acknowledgment :ได้รับแพ็กเก็ตการรับรองสถานะการเชื่อมโยงที่บรรจุ LSA header
- Implicit Acknowledgment : ได้รับแพ็กเก็ต update ที่บรรจุตัวอย่างเดียวกันกับ LSA

Master ทำหน้าที่ควบคุมกระบวนการที่ทำให้เกิดความสอดคล้องกัน และรับรองว่ามีแพ็กเก็ต DD เพียงแพ็กเก็ตเดียวที่สำคัญในช่วงเวลาหนึ่ง เมื่อ Slave ได้รับแพ็กเก็ต DD จาก Master Slave จะทำการรับรองแพ็กเก็ตนั้นโดยการส่งแพ็กเก็ต DD ที่มีหมายเลขลำดับเดียวกัน ถ้า Master ไม่ได้รับการรับรองของแพ็กเก็ต DD ภายในช่วง RxmtInterval Master จะส่งสำเนาของแพ็กเก็ตใหม่ออกไป

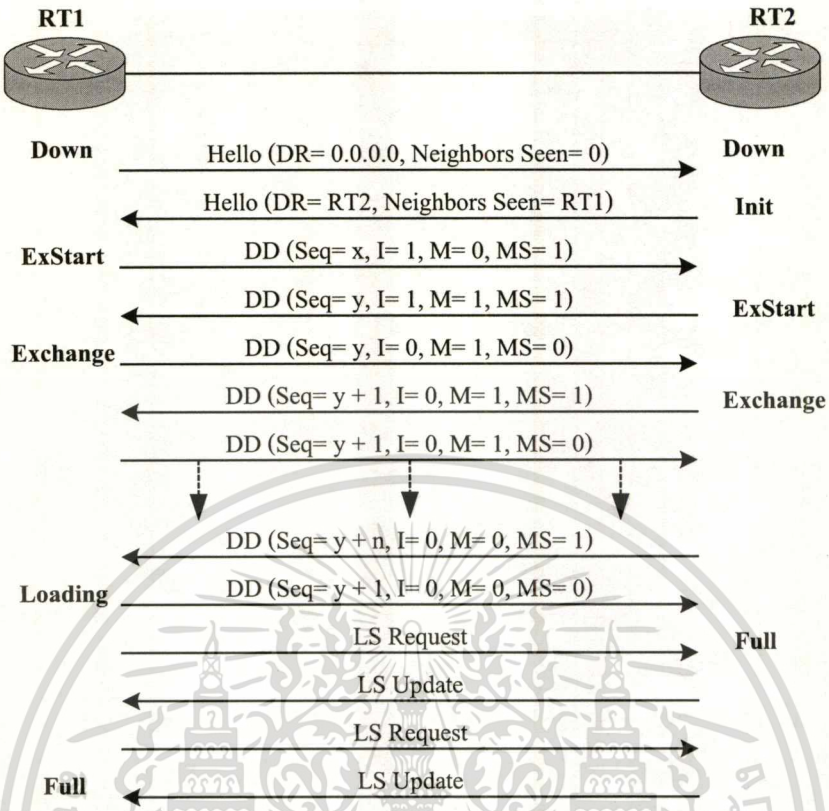
Slave จะทำการส่งแพ็กเก็ต DD เท่านั้นในการตอบสนองกับแพ็กเก็ต DD ที่ได้รับจาก Master ถ้าแพ็กเก็ตที่ได้รับมีหมายเลขลำดับใหม่ Slave จะส่งแพ็กเก็ต DD ด้วยหมายเลขลำดับเดียวกัน ถ้าหากว่าหมายเลขลำดับที่ได้รับเหมือนกันกับแพ็กเก็ต DD ที่ได้รับรองไปก่อนหน้านี้ แพ็กเก็ตการรับรองก็จะถูกส่งออกไปใหม่

เมื่อกระบวนการที่ทำให้ฐานข้อมูลมีความสอดคล้องกันเสร็จสมบูรณ์ สถานะการส่งมอบอย่างใดอย่างหนึ่งนี้ก็จะเกิดขึ้น ดังนี้

- ถ้ายังคงมีรายการร้องขอสถานะการเชื่อมโยงอยู่ทั้งหมด เราท์เตอร์จะทำการส่งมอบจากสถานะเพื่อนบ้านไปเป็น Loading
- ถ้ารายการร้องขอสถานะการเชื่อมโยงว่างเปล่า เราท์เตอร์จะส่งผ่านจากสถานะเพื่อนบ้านไปเป็น Full

เมื่อ Master รู้ว่ากระบวนการทำให้เกิดความสอดคล้องเสร็จสมบูรณ์ Master จะทำการส่งแพ็กเก็ต DD ทั้งหมดแก่ฐานข้อมูลสถานะการเชื่อมโยงของตัวเอง และรับแพ็กเก็ต DD ที่มีบิท M เป็นศูนย์ และ Slave จะรู้ว่ากระบวนการเสร็จสมบูรณ์เมื่อ Slave ได้รับแพ็กเก็ต DD ที่มีบิท M เป็นศูนย์ และส่งแพ็กเก็ต DD รับรองซึ่งมีบิท M ศูนย์ด้วย Slave จะต้องรู้เป็นคนแรกว่ากระบวนการที่ทำให้เกิดความสอดคล้องเสร็จสมบูรณ์ เพราะว่า Slave ต้องรับรองแพ็กเก็ตที่ได้รับในแต่ละแพ็กเก็ตในรูปที่ 5.12 แสดงถึงกระบวนการสร้างการอยู่ติดกัน ตัวอย่างนี้ถูกนำมาจาก RFC 2328

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 5.12 กระบวนการซิงโครไนซ์ฐานข้อมูล Link State และสถานะของเพื่อนบ้าน

ขั้นตอนที่แสดงในรูปที่ 5.12 สามารถอธิบายได้ ดังนี้

1. เมื่อ RT1 เริ่มแอกทีฟบนเครือข่ายที่มีการถึงเข้าได้หลายช่องทางและส่งแพ็กเก็ต Hello RT1 จะยังไม่ได้ยินอะไรเลยจากเพื่อนบ้านตัวใด ๆ ดังนั้นแพ็กเก็ตในฟิลด์เพื่อนบ้านจะว่างเปล่า และฟิลด์ DR และ BDR ถูกเซ็ทเป็น 0.0.0.0
2. เมื่อ RT2 ได้รับ Hello จาก RT1 RT2 จะสร้างโครงสร้างข้อมูลของเพื่อนบ้านสำหรับ RT1 และเซ็ทสถานะของ RT1 เป็น Init RT2 จะส่งแพ็กเก็ต Hello ด้วย Router ID ของ RT1 ไปในฟิลด์เพื่อนบ้านในฐานะที่เป็น DR RT2 ยังรวมแอดเดรสอินเทอร์เฟสของตัวมันเองเข้าไปในฟิลด์ DR ด้วย
3. การมองเห็น Router ID ของตัวมันเองในแพ็กเก็ต Hello ที่ได้รับ (IE4 ในตารางที่ 5.2) RT1 ได้สร้างโครงสร้างข้อมูลเพื่อนบ้านสำหรับ RT2 และเซ็ทสถานะ RT2 เป็น ExStart เพื่อการเจรจา mater/slave จากนั้น RT1 จะสร้างแพ็กเก็ตรายละเอียดของฐานข้อมูลที่ว่างเปล่า (ไม่มีผลรวม LSA) หมายเลขลำดับ DD ถูกเซ็ทเป็น x บิท I ถูกเซ็ทขึ้นเพื่อชี้ว่าแพ็กเก็ตนี้เป็นแพ็กเก็ต DD เริ่มแรกของ RT1 บิท M ถูกเซ็ทขึ้นเพื่อชี้ว่า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

แพ็กเก็ตนี้ไม่ใช่แพ็กเก็ต DD สุดท้าย และบิท MS ถูกเซ็ทขึ้นเพื่อชี้ว่า RT1 กำลังอ้างสิทธิให้ตัวมันเองเป็น master

4. RT2 ส่งมอบสถานะของ RT1 ด้วย Exstart ในโอกาสที่ได้รับแพ็กเก็ต DD จากนั้นมันจึงส่งแพ็กเก็ต DD ตอบสนองด้วยหมายเลขลำดับ DD ด้วย y ซึ่ง RT2 มี Router ID สูงกว่า RT1 ดังนั้น RT2 จึงเซ็ทบิท MS เป็น 1 แพ็กเก็ต DD นี้เหมือนกับแพ็กเก็ต DD แรกที่ถูกใช้สำหรับการเจรจา master/slave ด้วยเหตุนี้มันจึงว่าง
5. เมื่อตกลงได้ว่า RT2 เป็น master RT1 จึงส่งมอบสถานะของ RT2 ด้วย Exchange RT1 จะสร้างแพ็กเก็ต DD ด้วยหมายเลขลำดับ DD ของ RT2 เป็น y และ MS = 0 ซึ่งเป็นการชี้ว่า RT1 เป็น slave แพ็กเก็ตนี้จะถูกอาศัยอยู่กับ LSA header จากรายการสรุปสถานะการเชื่อมโยงของ RT1
6. RT2 ส่งมอบสถานะเพื่อนบ้านของมันด้วย Exchange ที่ระบุว่าได้รับแพ็กเก็ต DD ของ RT1 RT2 จะส่งแพ็กเก็ต DD ที่บรรจุด้วย LSA header จากรายการสรุปสถานะการเชื่อมโยงของตัว RT2 เอง และจะเพิ่มหมายเลขลำดับ DD เป็น y+1
7. RT1 ส่งแพ็กเก็ตรับรองที่บรรจุหมายเลขลำดับเดียวกันตามแพ็กเก็ต DD ที่ เพิ่งได้รับจาก RT2 กระบวนการยังคงดำเนินต่อไป ด้วย RT2 ส่งแพ็กเก็ต DD แพ็กเก็ตเดียวและรอคอยแพ็กเก็ตรับรองจาก RT1 ที่บรรจุหมายเลขลำดับเดียวกันก่อนการส่งแพ็กเก็ตถัดไป เมื่อ RT2 ส่งแพ็กเก็ต DD ด้วยผลรวม LSA ของตัวเองเป็นแพ็กเก็ตสุดท้าย RT2 จะเซ็ท M = 0
8. การรับแพ็กเก็ตนี้และการรับรู้ว่าแพ็กเก็ตการรับรองที่มันจะส่งไปประกอบด้วยผลรวม LSA ของตัวมันเองเป็นผลรวมสุดท้าย RT1 จึงรับรู้ว่ากระบวนการ Exchange เสร็จสิ้นแล้ว อย่างไรก็ตาม RT1มี entires อยู่ในรายการร้องขอสถานะการเชื่อมโยงของตัวมันเอง เพราะฉะนั้น RT1 จะส่งผ่านไปยัง Loading
9. เมื่อ RT2 รับแพ็กเก็ต DD สุดท้ายของ RT1 RT2 จะส่งมอบสถานะของ RT1 เป็น Full เพราะ RT2 ไม่มี entires อยู่ในรายการร้องขอสถานะการเชื่อมโยงของตัวเองอยู่
10. RT1 ส่งแพ็กเก็ตร้องขอสถานะการเชื่อมโยง และ RT2 ส่ง LSA ที่ถูกร้องขอไปในแพ็กเก็ต update สถานะการเชื่อมโยง จนกระทั่งรายการร้องขอการเชื่อมโยงของ RT1 ว่าง RT1 จึงจะส่งมอบสถานะของ RT2 เป็น Full

สังเกตว่าถ้าเราท์เตอร์มี entires อยู่ในรายการร้องขอสถานะการเชื่อมโยง เราท์เตอร์ไม่จำเป็นต้องคอยสถานะ Loading เพื่อส่งแพ็กเก็ตร้องขอสถานะการเชื่อมโยงก็ได้ เราท์เตอร์อาจจะไม่รอคอยในขณะที่เพื่อนบ้านยังคงอยู่ในสถานะ Exchange ผลที่สุดกระบวนการที่ทำให้เกิดความสอดคล้องกันก็จะไม่เรียบร้อยเท่ากับที่แสดงไว้ในรูปที่ 5.13 แต่จะมีประสิทธิภาพมาก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5.8 แอเรีย (Areas)

แอเรียเป็นกลุ่มตรรก (logical) ของเราท์เตอร์ OSPF และการเชื่อมโยง ซึ่งแบ่งโดเมน OSPF ออกเป็นโดเมนย่อย ๆ (sub-domain) ดังรูปที่ 5.13 เราท์เตอร์ในแอเรียหนึ่งจะไม่มีการรับรู้ในรายละเอียดของโทโปโลยีจากภายนอกของแอเรียของพวกมัน เพราะว่าเงื่อนไขเหล่านี้

- เราท์เตอร์ ต้องแบ่งฐานข้อมูลสถานะการเชื่อมโยงเฉพาะกับเราท์เตอร์ตัวอื่นที่อยู่ในแอเรียของมันเองเท่านั้น ไม่ใช่กับเครือข่ายที่เชื่อมต่อกันทั้งหมด ขนาดของฐานข้อมูลที่ลดลงช่วยลดผลกระทบที่จะเกิดขึ้นกับหน่วยความจำของเราท์เตอร์
- ฐานข้อมูลสถานะการเชื่อมโยงที่มีขนาดเล็กหมายความว่า LSA มีขนาดน้อยเพื่อผ่านกรรมวิธีการทำงาน เพราะฉะนั้นผลกระทบต่อ CPU จึงน้อย
- เพราะว่าฐานข้อมูลสถานะการเชื่อมโยงต้องถูกรักษาอยู่ภายในแอเรียเท่านั้น การแพร่กระจาย (flooding) โดยส่วนใหญ่จึงถูกจำกัดอยู่ในแอเรีย

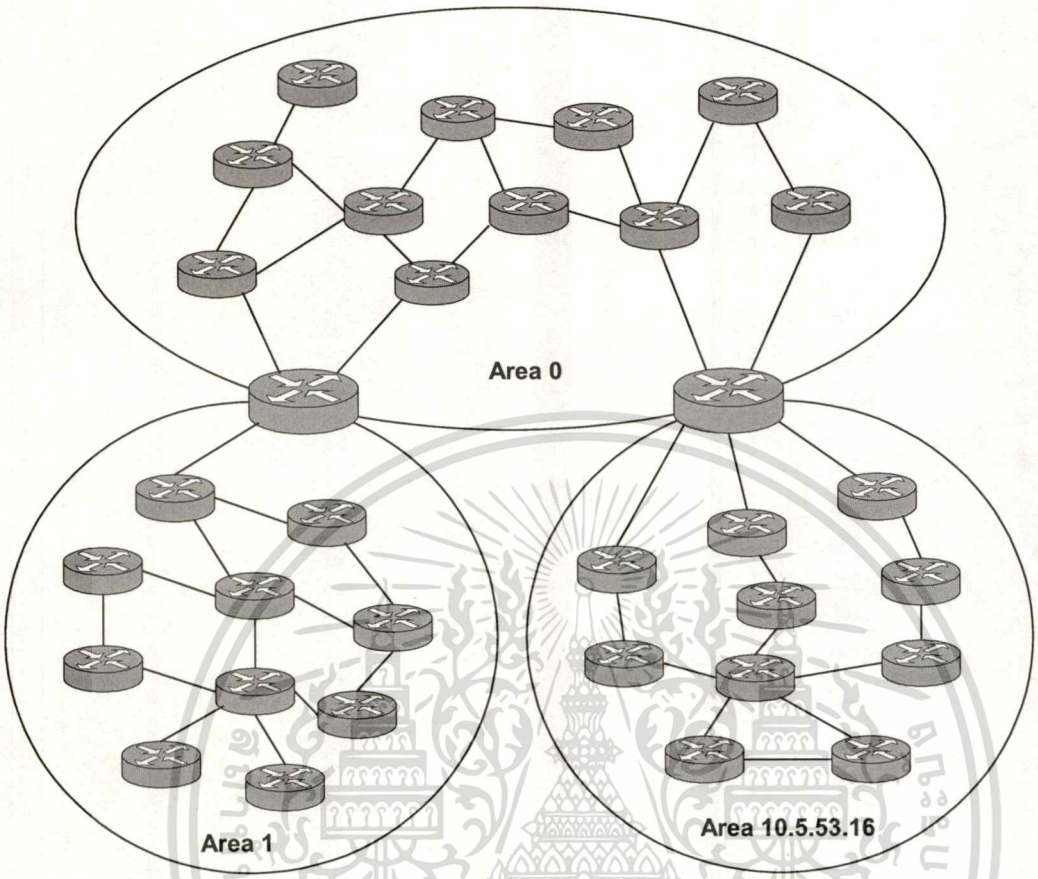
แอเรียได้ถูกแบ่งแยกด้วย Area ID ซึ่งมีขนาด 32 บิท ดังรูปที่ 5.13 แสดงถึง Area ID ที่อาจจะแสดงได้ด้วยเลขฐานสิบ หรือเลขฐานสิบที่มีจุด และรูปแบบของทั้งสองแบบสามารถใช้ร่วมกันได้ ตัวอย่างเช่น แอเรีย 0 และแอเรีย 0.0.0.0 มีค่าเท่ากัน แอเรีย 16 เท่ากับ 0.0.0.16 และแอเรีย 271 เท่ากับ 0.0.0.15 เป็นต้น

ทราฟฟิก 3 ชนิดที่ถูกกำหนดขึ้นตามความสัมพันธ์ของแอเรีย มีดังนี้

- Intra-area : เป็นทราฟฟิกที่ประกอบด้วยแพ็กเก็ตที่ถูกส่งผ่านกันระหว่างเราท์เตอร์ที่อยู่ภายในแอเรียเดียวกัน
- Inter-area : เป็นทราฟฟิกที่ประกอบด้วยแพ็กเก็ตที่ถูกส่งผ่านกันระหว่างเราท์เตอร์ที่อยู่ในแอเรียต่างกัน
- External-area : เป็นทราฟฟิกที่ถูกส่งผ่านระหว่างเราท์เตอร์ที่อยู่ภายในโดเมน OSPF กับเราท์เตอร์ที่อยู่ภายในระบบ autonomous อื่น

แอเรีย 0 (หรือ 0.0.0.0) ได้ถูกสำรองไว้สำหรับ backbone ซึ่ง backbone ทำหน้าที่รวบรวม topography ต่าง ๆ ของแต่ละแอเรียกับแอเรียอื่น ๆ ทุกแอเรีย เหตุผลคือเพื่อให้ทราฟฟิกของ inter-area ทั้งหมดต้องผ่านทะลุ backbone แอเรียที่ไม่ใช่ backbone ไม่สามารถแลกเปลี่ยนแพ็กเก็ตได้โดยตรง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 5.13 กลุ่มเราท์เตอร์ในเชิงตรรกที่ถูกจัดแบ่งเป็นแอเรียต่าง ๆ

5.9 ชนิดของเราท์เตอร์ (Router Types)

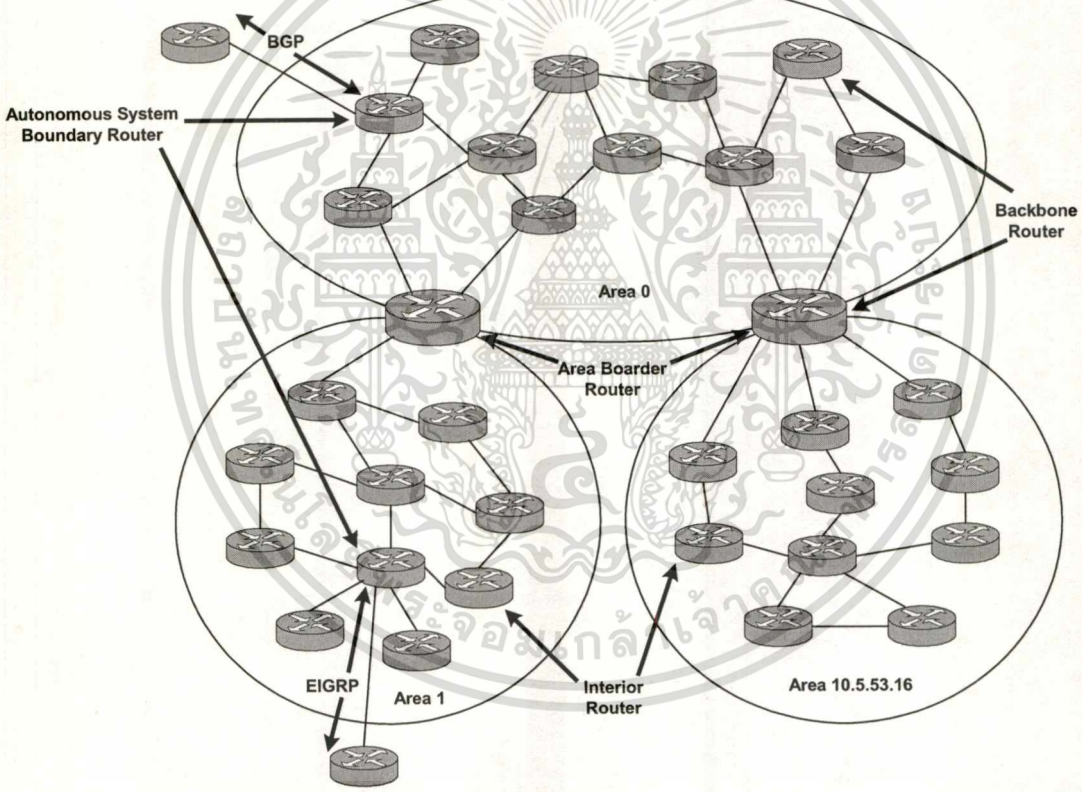
เราท์เตอร์ก็เหมือนกับทราฟฟิกที่สามารถจัดแบ่งเป็นกลุ่มตามความสัมพันธ์กับแอเรีย เราท์เตอร์ OSPF ทั้งหมดจะถูกแบ่งออกเป็น 4 แบบ ดังรูปที่ 5.14

- Internal Router : คือ เราท์เตอร์ที่มีอินเทอร์เฟสทั้งหมดอยู่ในแอเรียเดียวกัน เราท์เตอร์เหล่านี้มีฐานข้อมูลสถานะการเชื่อมโยงเดียว
- Area Border Routers (ABRs) : คือเราท์เตอร์ที่เชื่อมต่อกับ 1 แอเรียหรือมากกว่ากับ backbone และทำหน้าที่เป็น gateway สำหรับทราฟฟิกแบบ inter-area ABR ต้องมีอย่างน้อยหนึ่งอินเทอร์เฟสเสมอที่เป็นของ backbone และต้องรักษาฐานข้อมูลสถานะการเชื่อมโยงแยกกันสำหรับแอเรียแต่ละแอเรียที่ถูกต่ออยู่ เพราะว่า ABR มีหน่วยความจำและมีหน่วยประมวลผลที่มีความสามารถสูงกว่า Internal Router ABR จะสรุปข้อมูล topological ของแอเรียของมันเองที่ถูกต่ออยู่เข้าไปใน backbone จากนั้นจึงแพร่กระจายข้อมูลสรุปให้แก่แอเรียอื่น ๆ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- Backbone Routers : เป็นเราท์เตอร์ที่มีอย่างน้อยหนึ่งอินเทอร์เฟสต่ออยู่กับ backbone ถึงแม้ว่าความต้องการนี้หมายความว่า ABR ก็เป็น Backbone Router ด้วย ซึ่งในรูปที่ 5.15 แสดงให้เห็นว่า Backbone Routers ทั้งหมดไม่ใช่ ABR Internal Router ที่มีอินเทอร์เฟสทั้งหมดเป็นของแอเรีย 0 ยังเป็น Backbone Router ด้วย

Autonomous System Boundary Routers (ASBRs) คือ gateway สำหรับทราฟฟิกที่มาจากภายนอก การปล่อยเส้นทางเข้าไปในโดเมน OSPF ที่ได้เรียนรู้จากโพโทคอลชนิดอื่น เช่น BGP และ EIGRP ดังแสดงในรูปที่ 5.14 ASBR สามารถวางไว้ที่ไหนก็ได้ภายใน autonomous system ของ OSPF ซึ่งอาจจะเป็น Internal Backbone หรือ ABR ก็ได้

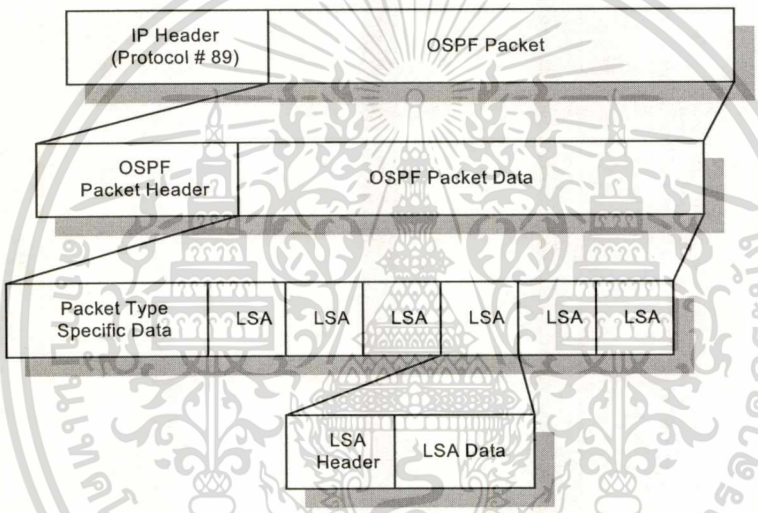


รูปที่ 5.14 การจัดแบ่งเราท์เตอร์เป็น Internal Router Backbone Router Area Border Router(ABR) หรือ Autonomous System Boundary Router (ASBR)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5.10 รูปแบบแพ็กเก็ต OSPF (OPSF Packet Formats)

แพ็กเก็ต OSPF ประกอบด้วยการบีบอัดข้อมูล (encapsulation) หลาย ๆ ครั้ง ดังแสดงในรูปที่ 5.16 การบีบอัดข้อมูลภายใน IP header เป็น 1 ใน 5 ชนิดของแพ็กเก็ต OSPF แพ็กเก็ตแต่ละชนิดเริ่มด้วย header ของแพ็กเก็ต OSPF ส่วนข้อมูลของแพ็กเก็ต OSPF ที่ตามหลัง header จะแปรเปลี่ยนเพื่อให้สอดคล้องตามชนิดของแพ็กเก็ต ชนิดของแพ็กเก็ตในแต่ละชนิดจะมีหมายเลขฟิลด์ตามชนิดที่ระบุไว้ตามด้วยข้อมูลเป็นจำนวนมาก ข้อมูลที่บรรจุอยู่ในแพ็กเก็ต Hello จะเป็นรายชื่อของเพื่อนบ้าน แพ็กเก็ตร้องของ LS จะบรรจุ series ของฟิลด์ แพ็กเก็ต update LS จะบรรจุรายชื่อของ LSA ดังแสดงในรูปที่ 5.15 LSA พวกนี้ก็มี header และฟิลด์ ข้อมูลตามชนิดที่ระบุไว้เป็นของตัวเอง แพ็กเก็ตที่เป็นรายละเอียดข้อมูลและการรับรอง LS จะบรรจุรายชื่อ header ของ LSA

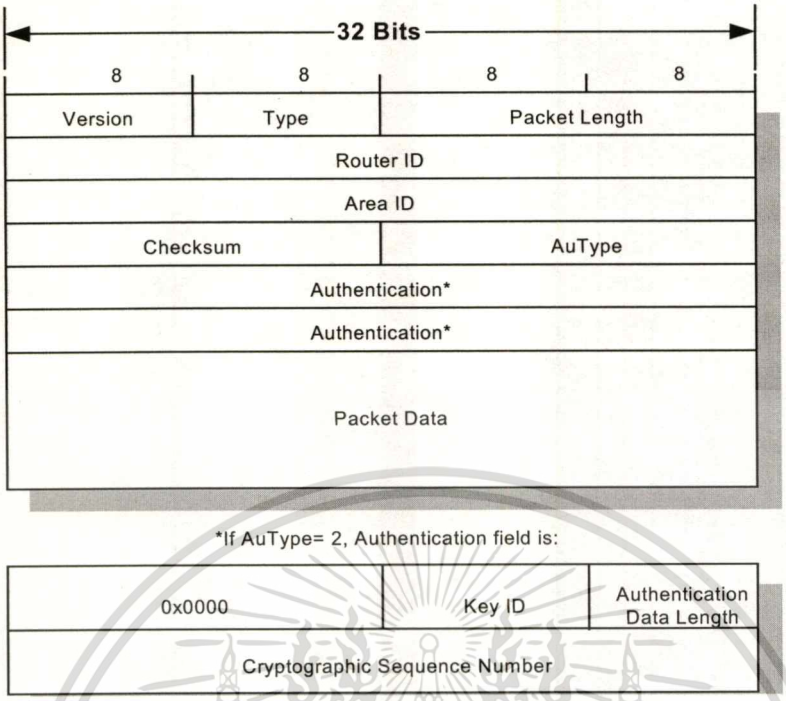


รูปที่ 5.15 โครงสร้างแพ็กเก็ต OSPF ในรูปของการบีบอัด

5.10.1 Header ของแพ็กเก็ต (Packet Header)

แพ็กเก็ต OSPFทั้งหมดเริ่มต้นด้วย header ขนาด 24 octet ดังรูปที่ 5.16

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 5.16 รูปแบบแพ็กเก็ต Header ของ OSPF

ตารางที่ 5.4 ชนิดของแพ็กเก็ต OSPF

Type Code	รายละเอียด
1	Hello
2	Database Description
3	Link State Request
4	Link State Update
5	Link State Acknowledgment

- Version คือหมายเลขเวอร์ชั่น OSPF โดยส่วนใหญ่มีค่าเวอร์ชั่นเป็น 2
- Type ระบุชนิดของแพ็กเก็ตตาม header ตารางที่ 5.4 แสดงชนิดของแพ็กเก็ตมีอยู่ 5 ชนิด ตามหมายเลขที่ปรากฏในฟิลด์ type
- Packet length คือความยาวของแพ็กเก็ต OSPF (อยู่ในรูป octets) ซึ่งรวม header ด้วย
- Router ID คือ ID ของเราท์เตอร์ตัวต้นกำเนิด
- Area ID คือ แอเรียที่ได้จากแพ็กเก็ตที่เกิดขึ้นมา ถ้าแพ็กเก็ตถูกส่งผ่านไปบนการเชื่อมโยงเสมือน Area จะเป็น 0.0.0.0 (backbone area ID) เพราะว่าการเชื่อมโยงเสมือนถือเป็นส่วนหนึ่งของ backbone

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- Checksum คือ การตรวจสอบผลรวม IP มาตรฐานของแพ็กเก็ตทั้งหมดรวมถึง header ด้วย
- Au Type คือโหมดที่ใช้ในการรับรองการมีตัวตน ตารางที่ 5.5 เป็นรายชื่อโหมดของการรับรองการมีตัวตนที่เป็นไปได้
- Authentication คือ ข้อมูลที่มีความจำเป็นต่อแพ็กเก็ตที่ถูกรับรองการมีตัวตนด้วยโหมดที่ถูกระบุไว้ในฟิลด์ AuType ถ้า Au Type = 0 ฟิลด์จะไม่ถูกตรวจสอบเพราะฉะนั้นภายในฟิลด์จะบรรจุอะไรก็ได้ ถ้า Au Type = 1 ภายในฟิลด์จะบรรจุด้วยรหัสผ่านขนาด 64 บิท ถ้า Au Type = 2 ภายในฟิลด์ Authentication จะบรรจุ Key ID ความยาวข้อมูลการรับรองการมีตัวตน และหมายเลขลำดับของ Cryptographic ที่ไม่มีการลดจำนวน สาระสำคัญของข่าวสาร (message digest) จะถูกใส่เพิ่มไว้ท้ายสุดของแพ็กเก็ต OSPF และจะไม่ถูกพิจารณาว่าเป็นส่วนหนึ่งของแพ็กเก็ตของตัวมันเอง

ตารางที่ 5.5 ชนิด authentication ของ OSPF

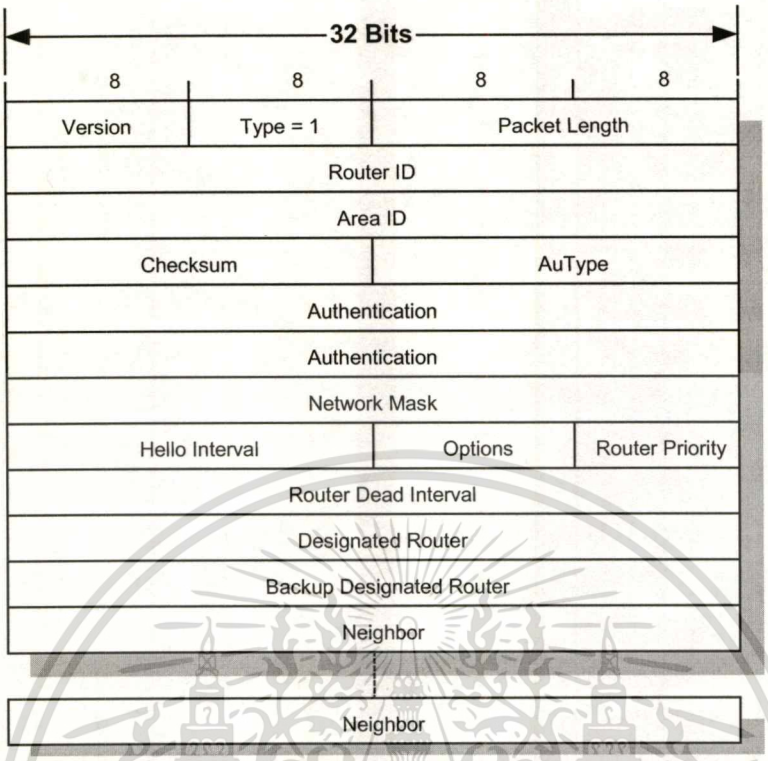
AuType	Authentication Type
0	Null (ไม่มีการทำ authentication)
1	Simple (clear text) Password Authentication
2	Crytographic (MD5) Checksum

- Key ID บ่งบอกถึงอัลกอริธึ่มของการรับรองการมีตัวตน และ secret key ที่ใช้สร้างสาระสำคัญของข่าวสาร (message digest)
- Authentication Data Length ระบุถึงความยาว (หน่วยเป็น octets) ของสาระสำคัญของข่าวสารที่ถูกใส่เพิ่มไว้ท้ายสุดของแพ็กเก็ต
- Cryptographic Sequence Number คือหมายเลขที่ไม่ลดจำนวนใช้เพื่อป้องกันการพยายามเล่นซ้ำ

5.10.2 Hello Packet

Hello packet (รูปที่ 5.17) ทำหน้าที่สร้างและรักษาการอยู่ติดกัน Hello จะนำเอาค่าพารามิเตอร์ที่เพื่อนบ้านต้องตกลงกันเพื่อจัดรูปแบบการอยู่ติดกัน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 5.17 รูปแบบแพ็กเก็ต Hello ของ OSPF

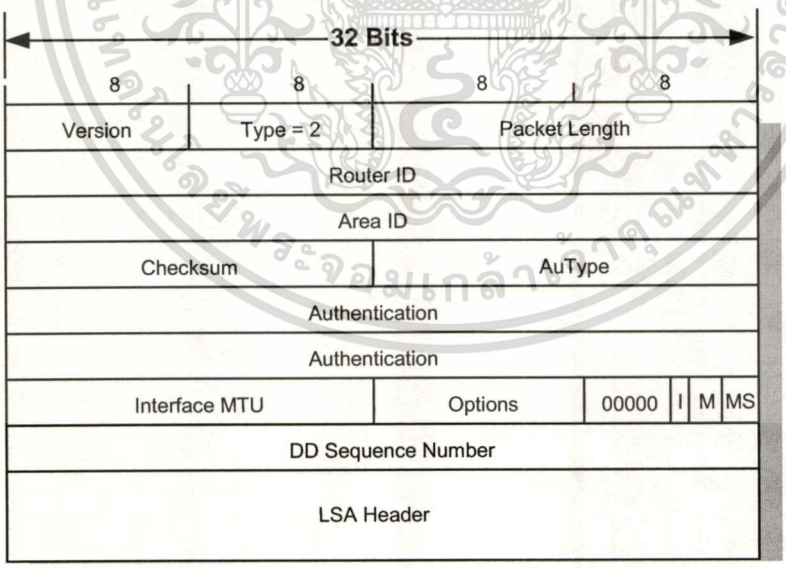
- Network Mask คือแอดเดรสมาส์คของอินเทอร์เฟสที่มีแพ็กเก็ตส่งออกไป ถ้ามาส์คนี้ไม่ตรงกับมาส์คของอินเทอร์เฟสที่รับแพ็กเก็ตเข้ามา แพ็กเก็ตจะถูกตัดทิ้ง เทคนิคนี้รับรองว่าเราท์เตอร์จะกลายเป็นเพื่อนบ้านกันได้ ถ้าเราท์เตอร์สามารถตกลงกันด้วยแอดเดรสที่แน่นอนของเครือข่ายร่วม
- Hello Interval คือคาบเวลา (หน่วยเป็นวินาที) ระหว่างการส่งแพ็กเก็ต Hello บนอินเทอร์เฟส ถ้าเราท์เตอร์ตัวส่งและตัวรับมีค่าพารามิเตอร์นี้ต่างกัน เราท์เตอร์ทั้งสองจะไม่สร้างความสัมพันธ์การเป็นเพื่อนบ้าน
- Options ฟิลด์นี้ถูกรวมอยู่ในแพ็กเก็ต Hello เพื่อทำให้แน่ใจว่าเพื่อนบ้านมีความสามารถที่สามารถเข้ากันได้ เราท์เตอร์สามารถปฏิเสธการเป็นเพื่อนบ้านเพราะว่ามีความสามารถไม่ตรงกัน
- Router Priority ถูกใช้ในการเลือก DR และ BDR ถ้าหากเซ็ทเป็น 0 เราท์เตอร์ตัวต้นกำเนิดจะไม่ได้รับเลือกให้เป็น DR หรือ BDR

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- Router Dead Interval คือเวลามีหน่วยเป็นวินาทีที่เราท์เตอร์ตัวต้นกำเนิดจะคอย Hello จากเพื่อนบ้านก่อนประกาศว่าเพื่อนบ้านตายไป (dead) ถ้าได้รับ Hello ในช่วงเวลาที่ไม่ตรงกันกับ RouterDeadInterval ของอินเทอร์เฟสด้านรับ แพ็กเก็ตจะถูกตัดทิ้ง
- Designated Router คือแอดเดรส IP ของอินเทอร์เฟสของ DR ที่อยู่บนเครือข่าย (ไม่ใช่ Router ID ของตัวมันเอง)
- Backup DR คือแอดเดรส IP ของอินเทอร์เฟสของ BDR ที่อยู่บนเครือข่าย
- Neighbor คือฟิลด์ที่เกิดขึ้นซ้ำซึ่งแสดงรายชื่อเพื่อนบ้านทั้งหมดที่อยู่บนเครือข่ายจากที่ๆ ซึ่งเราท์เตอร์ตัวต้นกำเนิดได้รับ Hello ในช่วง past RouterDeadInterval

5.10.3 Database Description Packet

แพ็กเก็ต Database Description (ดังรูปที่ 5.18) ถูกใช้เมื่อการอยู่ติดกันกำลังถูกสร้างขึ้น จุดประสงค์หลักของแพ็กเก็ต DD คือใช้เพื่ออธิบาย LSA บางส่วนหรือทั้งหมดที่อยู่ในฐานข้อมูลของตัวกำเนิด เพื่อที่ว่าตัวรับสามารถกำหนดได้ว่ามันมี LSA ที่เหมาะสมกับฐานข้อมูลของตัวมันเองหรือไม่ สิ่งนี้ถูกกระทำโดยการตรวจสอบรายชื่อ header ของ LSA เท่านั้น เนื่องจากว่าแพ็กเก็ต DD หลาย ๆ แพ็กเก็ตอาจจะถูกแลกเปลี่ยนกันในช่วงกระบวนการนี้ flags จึงได้ถูกใส่รวมไว้เพื่อทำการจัดการแลกเปลี่ยนโดยผ่านทางความสัมพันธ์ที่ใช้ในการโพล master/slave



รูปที่ 5.18 รูปแบบแพ็กเก็ต Database Description ของ OSPF

- Interface MTU : คือขนาด (หน่วยเป็น octets) ของแพ็กเก็ต IP ที่ใหญ่ที่สุดที่สามารถส่งออกไปยังอินเทอร์เฟสของตัวต้นกำเนิดโดยปราศจากการแบ่งเป็นส่วนย่อยๆ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

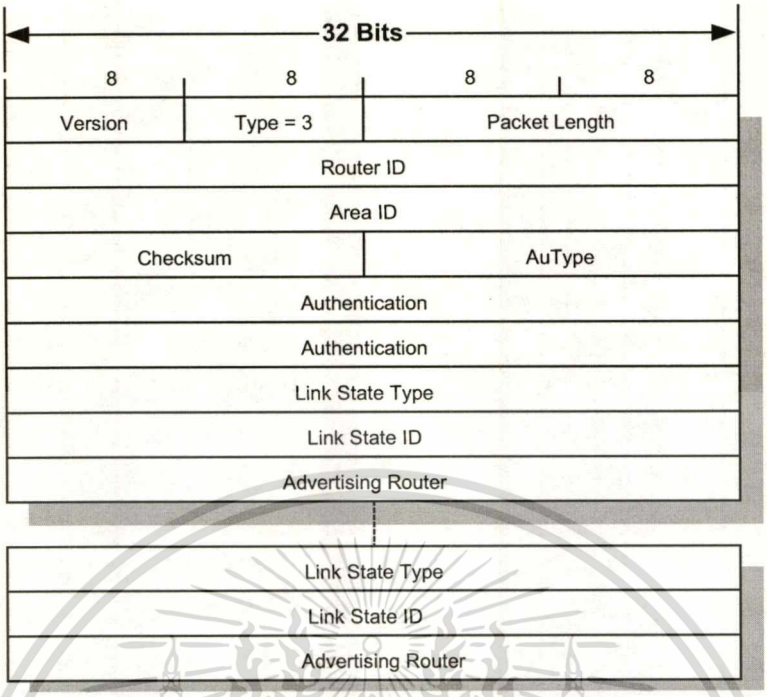
(fragmentation) ฟิลด์นี้จะถูกเซ็ทเป็น 0x0000 เมื่อแพ็กเก็ตถูกส่งออกไปบนการเชื่อมโยงเสมือน

- Options : ฟิลด์นี้ถูกรวมเข้าไปแพ็กเก็ตรายละเอียดฐานข้อมูล เพื่อให้เราท์เตอร์เลือกหรือไม่ก็ส่ง LSA ที่แน่นอนแก่เพื่อนบ้านที่ไม่รองรับความสามารถที่จำเป็น
- 5 บิทแรกของ octet ถัดไปไม่ได้ใช้ และถูกเซ็ทให้มีค่า 00000b เสมอ
- I-bit หรือ Initial bit จะถูกเซ็ทเป็น 1 เมื่อแพ็กเก็ตเป็นแพ็กเก็ตเริ่มแรก (Initial) ใน series ของแพ็กเก็ต DD โดยที่แพ็กเก็ต DD ถัดไปจะมี I-bit = 0
- M-bit หรือ More bit จะถูกเซ็ทเป็น 1 เพื่อชี้ว่าแพ็กเก็ตนี้ไม่ใช่แพ็กเก็ต DD แพ็กเก็ตสุดท้ายใน series แพ็กเก็ต DD โดยที่แพ็กเก็ตสุดท้ายจะมี M-bit = 0
- MS-bit หรือ Master/Slave bit ถูกเซ็ทเป็น 1 เพื่อชี้ว่าตัวกำเนิดเป็น master (นั่นคืออยู่ในความควบคุมของขั้นตอนการโพล) ในช่วงเวลาการทำให้ฐานข้อมูลมีความสอดคล้องกัน Slave จะมี MS-bit = 0
- DD Sequence Number ทำให้แน่ใจว่าลำดับของแพ็กเก็ต DD ทั้งหมดถูกรับได้ในขั้นตอนการทำให้ฐานข้อมูลมีความสอดคล้องกัน หมายเลขลำดับจะถูกเซ็ทโดย master ซึ่งเป็นค่าเฉพาะในแพ็กเก็ต DD แรก และลำดับจะถูกเพิ่มขึ้นในแพ็กเก็ตลำดับถัดไป
- LSA Headers รายชื่อ header ของ LSAs ทั้งหมดหรือเพียงบางส่วนในฐานข้อมูลสถานะการเชื่อมโยงของตัวกำเนิด

5.10.4 Link State Request Packet

เนื่องจากแพ็กเก็ตรายละเอียดฐานข้อมูลถูกรับได้ในช่วงกระบวนการที่ทำให้ฐานข้อมูลมีค่าตรงกัน เพราะฉะนั้นเราท์เตอร์จะทำการเก็บ LSAs ไว้บางส่วนซึ่งไม่มีอยู่ในฐานข้อมูลของมันเอง LSA เหล่านี้ได้ถูกบันทึกอยู่ในรายการร้องขอสถานะการเชื่อมโยง จากนั้นเราท์เตอร์จะส่งแพ็กเก็ตการร้องขอสถานะการเชื่อมโยง (ดังรูปที่ 5.19) ไป 1 แพ็กเก็ตหรือมากกว่า เพื่อขอสำเนาของ LSA จากเพื่อนบ้าน สังเกตว่าแพ็กเก็ตบ่งชี้ LSA ที่มีเอกลักษณ์เฉพาะโดยฟิลด์ชนิด (Type) ฟิลด์ ID และฟิลด์การประกาศของเรท์เตอร์ แต่ไม่ได้ร้องขอตัวอย่างชี้เฉพาะของ LSA

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 5.19 รูปแบบแพ็กเก็ต Link State Request ของ OSPF

- Link State Type คือ หมายเลขชนิดของ LSA ซึ่งแสดงถึง LSA ที่เป็น LSA เราท์เตอร์ LSA เครือข่าย และอื่น ๆ หมายเลขชนิดถูกแสดงไว้ในตารางที่ 5.6
- Link State ID คือ ฟิลด์ type-dependent ของ LSA header และ ส่วนของ LSA-specfic สำหรับรายละเอียดทั้งหมดของวิธีที่ LSA หลาย ๆ แบบใช้อยู่
- Advertisting Router คือ Router ID ของเราท์เตอร์ที่กำเนิด LSA

ตารางที่ 5.6 ชนิดของ LSA

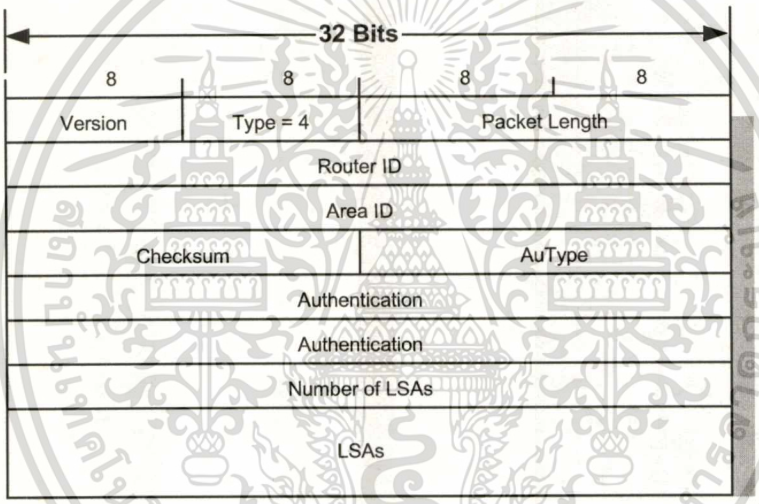
Type Code	รายละเอียด
1	Router LSA
2	Network LSA
3	Network Summary LSA
4	ASBR Summary LSA
5	AS External LSA
6	Group Menbership LSA
7	NSSA External LSA
8	External Attributes LSA

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

9	Opaque LSA (link-local scope)
10	Opaque LSA (area-local scope)
11	Opaque LSA (AS scope)

5.10.5 Link State Update Packet

Link State Update Packet (ดังรูปที่ 5.20) ที่ถูกใช้ในการกระจาย LSAs และส่ง LSA ในการตอบสนองการร้องขอสถานะการเชื่อมโยง ระลึกไว้ว่าแพ็กเก็ตไม่ได้ทิ้งเครือข่ายไว้กับที่ ๆ ซึ่งแพ็กเก็ตกำเนิดขึ้น ดังนั้นแพ็กเก็ต Link State Update นำพา LSAs เท่านั้นเพียง 1 hop จากเราท์เตอร์ตัวต้นกำเนิดของพวกมัน เพื่อนบ้านด้านรับมีหน้าที่ re-encapsulate LSA ที่เหมาะสมลงในแพ็กเก็ต update LSA แพ็กเก็ตใหม่เพื่อการแพร่กระจายต่อ ๆ ไป



รูปที่ 5.20 รูปแบบแพ็กเก็ต Link State Update ของ OSPF

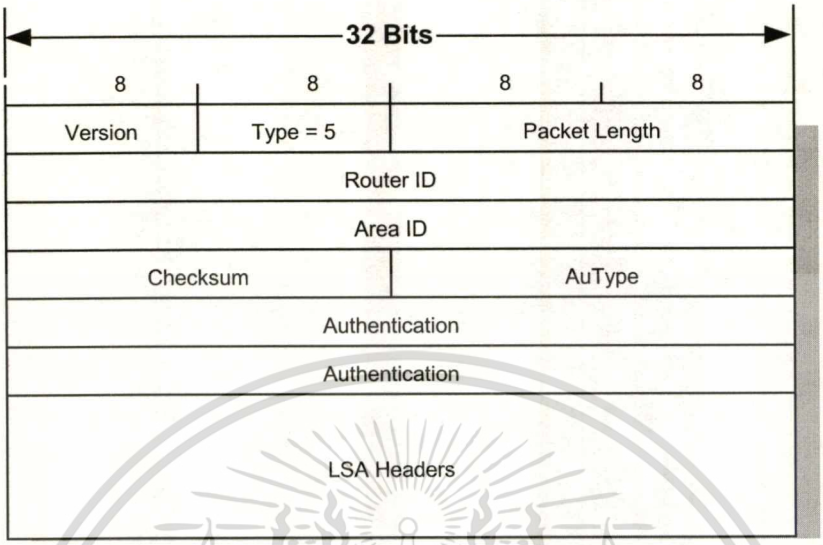
- Number of LSAs ระบุหมายเลขของ LSA ที่รวมอยู่ในแพ็กเก็ตนี้
- LSAs คือ LSAs ที่สมบูรณ์ ในการ update แต่ละครั้งอาจจะนำพาได้หลาย ๆ LSAs ซึ่งขึ้นอยู่กับขนาดแพ็กเก็ตที่มากที่สุดที่ยอมรับได้ในข่ายเชื่อมโยง

5.10.6 Link State Acknowledgment Packet

Link State Acknowledgment packet ถูกใช้เพื่อสร้างความน่าเชื่อถือให้กับการแพร่กระจาย LSAs ในแต่ละ LSA ที่รับได้โดยเราท์เตอร์จากเพื่อนบ้านที่ต้องรับรู้อย่างแท้จริงในแพ็กเก็ต Link State Acknowledgment ใน LSA ที่ถูกรับรู้ได้ถูกระบุโดยการรวม header ของตัวมันเองเข้าไปในใน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

แพ็กเก็ต LS ACK และหลาย ๆ LSAs อาจจะถูกรับรู้ในแพ็กเก็ตเดียวได้ ดังรูปที่ 5.21 แสดงถึงแพ็กเก็ต LS ACK ประกอบด้วย OSPF header และ LSA headers



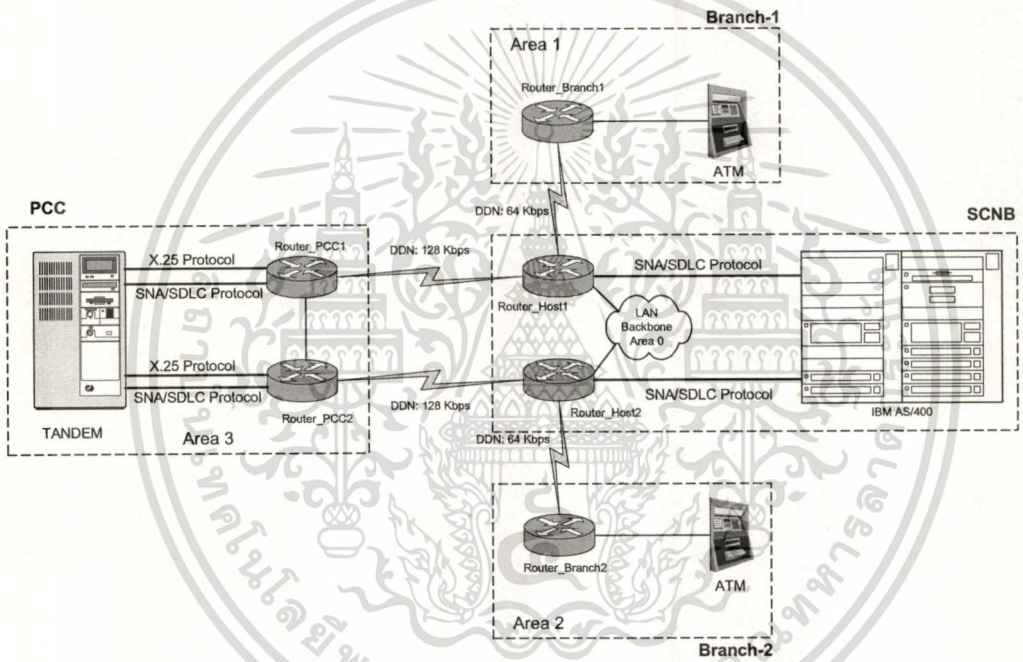
รูปที่ 5.21 รูปแบบแพ็กเก็ต Link State Acknowledgment ของ OSPF

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 6
แบบจำลองการทดสอบเพื่อศึกษาการทำงานของระบบเครือข่าย

6.1 การออกแบบการเชื่อมโยงเพื่อใช้ในการทดสอบ

ในการเลือกใช้อุปกรณ์เพื่อนำมาทำการทดสอบนั้นจำเป็นจะต้องคำนึงถึงความาสามารถในการรองรับรูปแบบโพรโทคอลชนิดต่าง ๆ ซึ่งในที่จะต้องสามารถรองรับ โพรโทคอล SNA/SDLC X.25 QLLC และ TCP/IP จากนั้นจึงจะเป็นรูปแบบของการเชื่อมต่อ (Topology) เพื่อการรองรับปริมาณข้อมูลในเครือข่ายให้มีประสิทธิภาพมากที่สุด ดังรูปที่ 6.1



รูปที่ 6.1 รูปแบบจำลองในการส่งผ่านโพรโทคอล SNA/SDLC และ X.25 ผ่านเครือข่าย IP

จากรูปการทดลองด้วยแบบจำลองประกอบด้วยอุปกรณ์หลัก ๆ 3 อย่างด้วยกัน ดังนี้

1. อุปกรณ์การสื่อสารข้อมูล ในที่นี้ใช้เราท์เตอร์เป็นอุปกรณ์ในการส่งผ่านข้อมูล ซึ่งรองรับโพรโทคอล SNA/SDLC เพื่อใช้ในการติดต่อกับ เครื่อง Automatic Teller Machine (ATM) และ Subarea Node (AS/400) โพรโทคอล TCP/IP ใช้เพื่อเชื่อมโยงเราท์เตอร์ให้เป็นเครือข่ายเดียวกันตลอดจนใช้ Routing Protocol แบบ OSPF เพื่อเพิ่มประสิทธิภาพให้แก่เครือข่าย และโพรโทคอล X.25 เพื่อใช้ในการติดต่อกับ Tandem

2. ระบบคอมพิวเตอร์หลัก (Host) ซึ่งแบ่งออกเป็น 2 ระบบ ระบบแรกใช้ SNA Subarea

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Node ใช้อุปกรณ์ AS/400 ที่รัน platform ด้วย OS400 เป็นระบบประมวลผลกลางและเก็บข้อมูลด้านระบบบัญชีของลูกค้าโดยใช้โพรโทคอล SNA/SDLC ในการส่งผ่านข้อมูล ซึ่งทำหน้าที่ควบคุม และตรวจสอบระบบบัญชีของลูกค้าในแต่ละรายในขณะที่ทำธุรกรรมผ่านเครื่อง ATM และระบบที่สอง คือ ระบบ Tandem กับแอพพลิเคชันที่มีชื่อว่า BASE24 ทำหน้าที่เป็นระบบ Front-End-Processor (FEP) สำหรับตรวจสอบข้อมูลบนบัตร ATM กับการเข้ารหัส และเป็นระบบฐานข้อมูลบัตรของลูกค้าทั้งหมด ซึ่งใช้การบีบอัดโพรโทรคอล X.25 ไปบนโพรโทคอล SNA/SDLC ในการควบคุมการทำงานของเครื่อง ATM ทั้งหมด

3. เครื่อง Automatic Teller Machine (ATM) เป็นอุปกรณ์ SNA Peripheral Node PU Type 2.0 ใช้โพรโทคอล SNA/SDLC เป็นโพรโทคอลที่ใช้ในการส่งผ่านข้อมูล โดยมีการกำหนดแอดเดรสให้กับ ATM ในแต่ละตู้ โดยมีค่าแอดเดรสที่ต่างกัน

จากรูปที่ 6.1 สามารถแบ่งการเชื่อมโยงอุปกรณ์ต่าง ๆ เข้าด้วยกันได้เป็น 4 ส่วน โดยในแต่ละส่วนแบ่งจำแนกตามสถานที่ ที่ใช้ติดตั้งอุปกรณ์ และเพื่อเพิ่มประสิทธิภาพให้กับเครือข่าย ซึ่งมีรายละเอียดต่าง ๆ ดังนี้

1. SCNB Site เป็นสถานที่ที่ติดตั้งอุปกรณ์สื่อสารหลัก (Backbone Routers) และ AS/400 ซึ่งในที่นี้จะประกอบด้วย Router_Host1 และ Router_Host2 โดยใช้ Routing Protocol แบบ OSPF เพื่อใช้สำหรับการเรียนรู้เส้นทางในการติดต่อกับอุปกรณ์เราท์เตอร์ทั้งหมดภายในเครือข่าย ซึ่ง Routing Protocol ชนิดนี้คุณสมบัติที่สามารถแบ่งลำดับชั้น (Hierarchy) ของเครือข่ายได้ ซึ่งจะทำให้การส่ง LSAs (Link State Advertisements) เพื่อใช้ในการ Update ตาราง Routing ของเราท์เตอร์เมื่อเกิดการเปลี่ยนแปลงของโทโปโลยีภายในเครือข่าย IP เช่น การเชื่อมโยงของเราท์เตอร์เมื่อเกิดขาดจากกัน เป็นต้น การ Update Routing ก็จะทำเฉพาะในแอเรียของตัวเองเท่านั้น เพราะฉะนั้นจึงกำหนดให้ Router_Host1 และ Router_Host2 จะทำหน้าที่เป็น ABR (Area Border Router) โดยมีอินเทอร์เฟสข้างหนึ่งต่ออยู่กับ LAN Backbone ซึ่งมีแอเรียเป็น “0” หรือเรียกว่า Backbone area และมีอินเทอร์เฟสอีกข้างหนึ่งต่ออยู่กับ Router_Branch1 และ Router_Branch2 โดยมีแอเรียเป็น “1” และ “2” ตามลำดับ

2. PCC Site เป็นสถานที่ติดตั้ง Router_PCC1 Router_PCC2 และระบบ Tandem ซึ่งในที่นี้ได้จำลองให้ Host ไม่ได้ตั้งอยู่ในอาคารเดียวกัน ทำให้การออกแบบจำลองต้องคำนึงถึงระบบเชื่อมต่อที่จะทำให้การแลกเปลี่ยนข้อมูลระหว่างกันสามารถติดต่อกันได้ ในแบบจำลองนี้อาศัยการจำลองการเชื่อมต่อ Host ด้วยเราท์เตอร์ โดยใช้โพรโทคอล TCP/IP เพื่อเชื่อมโยง Router_PCC1 กับ Router_Host1 และ Router_PCC2 กับ Router_Host2 โดยสร้างการเชื่อมโยง (Link) แยกจากกันด้วย DDN ที่ความเร็ว 128Kbps และกำหนดแอเรียเป็น แอเรีย “3”

3. Branch-1 ถูกจำลองเป็นพื้นที่ของสาขา ซึ่งติดตั้ง Router_Branch1 และ ATM โดย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เชื่อมโยง Router_Branch1 กับ Router_Host1 ด้วย DDN ที่ความเร็ว 64Kbps และให้เป็นแอเรีย “1”

4. Branch-2 ถูกจำลองเป็นพื้นที่ของสาขา ซึ่งติดตั้ง Router_Branch2 และ ATM โดยเชื่อมโยง Router_Branch2 กับ Router_Host2 ด้วย DDN ที่ความเร็ว 64Kbps และมีแอเรียเป็น “2”

6.2 การกำหนดพารามิเตอร์ในแบบจำลอง

ค่าพารามิเตอร์ต่าง ๆ ที่ใช้กับแบบจำลองนี้สามารถแบ่งออกเป็น 2 ค่าหลัก ๆ คือ

6.2.1. ค่าพารามิเตอร์ที่ใช้ในการเชื่อมโยงเราท์เตอร์ และ Routing Protocol

6.2.2. ค่าพารามิเตอร์ที่ใช้ในการเชื่อมต่อกับ Host และ ATM

6.2.1 ค่าพารามิเตอร์ที่ใช้ในการเชื่อมต่อโยงเราท์เตอร์ และ Routing Protocol

ลำดับแรกของการเชื่อมโยงเราท์เตอร์ 2 ตัวเข้าด้วยกัน จำเป็นต้องทำการกำหนดค่า IP แอดเดรสให้กับอินเทอร์เฟสก่อน ซึ่งในที่นี้ใช้ Serial Interface ของเราท์เตอร์ตัวหนึ่งต่อเข้ากับ Serial Interface ของเราท์เตอร์อีกตัวหนึ่ง ซึ่งจะเห็นได้ว่า ค่า IP แอดเดรสจะถูกใช้เพียง 2 IP แอดเดรสเท่านั้น ทำให้สามารถกำหนดค่า Subnet Mask เป็น 255.255.255.252 จากนั้นเลือกใช้โพรโทคอล HDLC ในการเชื่อมโยงเราท์เตอร์เข้าหากัน กำหนด Network ID ภายใต้ Routing Protocol เพื่อให้เราท์เตอร์ที่อยู่ภายในเครือข่ายทั้งหมดรู้จักกันด้วย Routing Protocol แบบ OSPF ดังตารางที่ 6.1 ถึง 6.4 ซึ่งแสดงให้เห็นถึงค่าพารามิเตอร์ของเราท์เตอร์ทั้งหมดในการเชื่อมโยงซึ่งอ้างอิงจากแบบจำลองดังรูป

ตารางที่ 6.1 ค่าพารามิเตอร์ในการเชื่อมโยงของ Router_Host1 และ Router_PCC1

Router_Host1	Router_PCC1
interface Serial1/0	interface Serial1/0
description To Router_PCC1	description To Router_Host1
ip address 172.21.188.1 255.255.255.252	ip address 172.21.188.2 255.255.255.252
encapsulation HDLC	encapsulation HDLC
interface FastEthernet0/0	router ospf 1
description To LAN BackBone	network 172.21.188.0 0.0.0.3 area 3
ip address 172.21.103.249 255.255.255.0	
router ospf 1	
network 172.21.103.0 0.0.0.255 area 0	
network 172.21.188.0 0.0.0.3 area 3	

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 6.2 ค่าพารามิเตอร์ในการเชื่อมโยงของ Router_Host2 และ Router_PCC2

Router_Host2	Router_PCC2
interface Serial1/0	interface Serial0/0
description To Router_PCC2	description To Router_Host1
ip address 172.21.188.9 255.255.255.252	ip address 172.21.188.10 255.255.255.252
encapsulation HDLC	encapsulation HDLC
interface FastEthernet0/0	router ospf 1
description To LAN BackBone	network 172.21.188.8 0.0.0.3 area 3
ip address 172.21.103.248 255.255.255.0	
router ospf 1	
network 172.21.103.0 0.0.0.255 area 0	
network 172.21.188.8 0.0.0.3 area 3	

ตารางที่ 6.3 ค่าพารามิเตอร์ในการเชื่อมโยงของ Router_Host1 และ Router_Branch1

Router_Host1	Router_Branch1
interface Serial2/5	interface Serial0/0
description To Router_Branch1	description To Router_Host1
ip address 172.21.137.1 255.255.255.252	ip address 172.21.137.2 255.255.255.252
encapsulation HDLC	encapsulation HDLC
router ospf 1	router ospf 1
network 172.21.137.0 0.0.0.3 area 1	network 172.21.137.0 0.0.0.3 area 1

ตารางที่ 6.4 ค่าพารามิเตอร์ในการเชื่อมโยงของ Router_Host2 และ Router_Branch2

Router_Host2	Router_Branch2
interface Serial5/0	interface Serial0/0
description To Router_Branch2	description To Router_Host2
ip address 172.21.148.1 255.255.255.252	ip address 172.21.148.2 255.255.255.252
encapsulation HDLC	encapsulation HDLC
router ospf 1	router ospf 1
network 172.21.148.0 0.0.0.3 area 2	network 172.21.148.0 0.0.0.3 area 2

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

6.2.2 ค่าพารามิเตอร์ที่ใช้ในการเชื่อมต่อกับ Host และ ATM

ค่าพารามิเตอร์ในส่วนนี้เป็นการกำหนดรูปแบบโพรโทคอลและฟังก์ชั่นการทำงานระหว่างเราท์เตอร์กับอุปกรณ์ซึ่งเป็น Host และเครื่อง ATM โดยเน้นถึงความสามารถในการตรวจเช็คความผิดพลาด (Error) ของข้อมูล การแก้ไขให้ปราศจากความผิดพลาด (Error Correction) และเน้นถึงความประหยัดโดยการใช้ฟังก์ชั่นที่มีอยู่นำมาปรับแต่งให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

จากตารางที่ 6.5 แสดงถึงค่าพารามิเตอร์เพื่อทำให้เครื่อง AS/400 และ Tandem สามารถติดต่อกันได้โดยผ่านโพรโทคอล SNA/SDLC ซึ่งในที่นี้ใช้ฟังก์ชั่น STUN (Serial line Tunneling) ซึ่งเป็นหลักการบีบอัดข้อมูล SNA/SDLC โดยครอบด้วยแพ็กเก็ต IP ผ่านไปบนช่องทางสื่อสารที่ถูกสร้างขึ้นระหว่างเราท์เตอร์ต้นทางและเราท์เตอร์ปลายทาง ซึ่งเป็นรูปแบบเฉพาะของ Cisco Router ในตารางที่ 6.6 แสดงถึงค่าพารามิเตอร์ที่ใช้ในการควบคุมเครื่อง ATM ซึ่งมี Tandem เป็นตัวควบคุมการทำงาน ซึ่งในที่นี้ใช้โพรโทคอล SNA/SDLC ในการติดต่อกับเครื่อง ATM โดยที่ระบบ Tandem ใช้โพรโทคอล X.25 ซึ่งมีการเซ็ทค่าบิท Q เป็น “1” ซึ่งเรียกว่า QLLC โดยจะมีการสร้างวงจรเสมือน (Virtual circuit) 1 วงจรต่อการควบคุมเครื่อง ATM 1 เครื่อง

ตารางที่ 6.5 ค่าพารามิเตอร์ STUN ที่ใช้ในการติดต่อกันระหว่าง Router_Host1 และ Router_PCC1

Router_Host1	Router_PCC1
stun peer-name 172.21.119.1	stun peer-name 172.21.188.5
stun protocol-group 1 basic	stun protocol-group 1 basic
interface Loopback0	interface Loopback0
ip address 172.21.119.1 255.255.255.255	ip address 172.21.188.5 255.255.255.255
interface Serial2/1	interface Serial1/4
description ### Link to AS/400 ###	description ### Link to Tandem ###
no ip address	no ip address
encapsulation stun	encapsulation stun
no ip mroute-cache	clockrate 64000
clockrate 64000	stun group 1
stun group 1	stun route all tcp 172.21.119.1
stun route all tcp 172.21.188.5	router ospf 1
router ospf 1	network 172.21.188.5 0.0.0.0 area 3
network 172.21.119.1 0.0.0.0 area 1	

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 6.6 ค่าพารามิเตอร์ที่ใช้ในการควบคุมเครื่อง ATM ด้วย Tandem ผ่าน Router_Host1 และ Router_PCC1 แหล่งอ้างอิง

Router_PCC1	Router_Branch1
dlsw local-peer peer-id 172.21.188.5	dlsw local-peer peer-id 172.21.137.5
dlsw remote-peer 0 tcp 172.21.137.5	dlsw remote-peer 0 tcp 172.21.188.5
interface Serial1/5	interface Serial0/1
description ATM GROUP 1	no ip address
no ip address	encapsulation sdlc
encapsulation x25 dce	no ip mroute-cache
x25 address 500010002	no keepalive
x25 htc 100	sdlc role primary
x25 win 7	sdlc vmac 5000.0001.0200
x25 wout 7	sdlc address 07
x25 ips 1024	sdlc xid 0A 0A100217
x25 ops 1024	sdlc partner 4900.0001.0207 07
x25 map qllc 4900.0001.0207 49001000207	sdlc dlsw 7
clockrate 64000	
qllc dlsw subaddress 07 vmacaddr 4900.0001.0207 partner 5000.0001.0207 npsi-poll	

6.3 ผลที่ได้การทดลองตามแบบจำลอง

จากรูปที่ 6.1 และตารางที่ 6.1 ถึง 6.4 ซึ่งแสดงแบบจำลองและค่าพารามิเตอร์ที่ใช้ในการเชื่อมต่อเราท์เตอร์นั้น สามารถแสดงให้เห็นถึงสถานะการเชื่อมต่อของเราท์เตอร์ตลอดจนตาราง Routing ที่ทำให้เราสามารถรู้ได้ว่ามีเครือข่ายย่อย (Sub-network) ใดบ้างที่ต่อผ่านอยู่กับอินเทอร์เฟสที่ทำหน้าที่เป็น Gateway ให้กับแต่ละเครือข่ายย่อย ดังรูปที่ 6.2 ซึ่งแสดงให้เห็นถึงสถานะของอินเทอร์เฟสใน Layer 1 (Serial) และ Layer 2 (Line Protocol) ตามมาตรฐาน OSI Model ของ Router_Host1 รูปที่ 6.3 แสดงสภาวะของ OSPF ซึ่งแสดงค่า Router ID ชนิดของเครือข่าย (Network Type) และ Adjacentcy เป็นต้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
Serial1/0 is up, line protocol is up
  Hardware is CD2430 in sync mode
  Description: To Router_PCC1_3660
  Internet address is 172.21.188.1/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
```

รูปที่ 6.2 รูปแสดงสถานะอินเทอร์เฟส Serial 1/0 ของ Router_Host1

```
Serial1/0 is up, line protocol is up
  Internet Address 172.21.188.1/30, Area 3
  Process ID 1, Router ID 172.21.119.1, Network Type POINT_TO_POINT,
Cost: 781
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  Index 1/29, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 11, maximum is 49
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.21.188.5
  Suppress hello for 0 neighbor(s)
```

รูปที่ 6.3 รูปแสดงสภาวะของ OSPF ภายใต้อินเทอร์เฟส Serial 1/0 ของ Router_Host1

ในรูปที่ 6.4 แสดงถึงตาราง Routing ที่เกิดจากการเชื่อมต่อเราท์เตอร์เข้าไปกับเครือข่ายด้วย OSPF Protocol ซึ่งจะทำให้ทราบถึง Gateway หรืออินเทอร์เฟสที่จะต้องผ่านในการที่จะติดต่อกับเครือข่ายย่อย (Sub-network) ที่ต้องการได้ โดยที่สัญญลักษณ์ "O" แทน OSPF สัญลักษณ์ "IA" แทน OSPF Inter area และ "C" แทนด้วย Connected และค่าที่อยู่ภายในเครื่องหมาย "[ ]" หมายถึงค่า Administrative Distance ซึ่งเป็นค่า Default ของ OSPF มีค่าเท่ากับ 110 และตามหลังด้วยค่า Cost โดยสามารถคำนวณหาได้จาก 10^8/Bandwidth

```
O       172.21.188.5/32 [110/782] via 172.21.188.2, 1d01h, Serial1/0
C       172.21.188.0/30 is directly connected, Serial1/0
O       172.21.188.13/32 [110/792] via 172.21.188.2, 1d01h, Serial1/0
O       172.21.188.8/30 [110/1572] via 172.21.188.2, 1d01h, Serial1/0
C       172.21.137.0/30 is directly connected, Serial2/5
C       172.21.137.5/32 is directly connected, Serial2/5
O IA    172.21.148.0/30 [110/1563] via 172.21.103.248, 08:48:20, FastEthernet0/0
O IA    172.21.148.5/32 [110/782] via 172.21.103.248, 08:48:20, FastEthernet0/0
C       172.21.103.0/24 is directly connected, FastEthernet0/0
```

รูปที่ 6.4 ตาราง Routing หลังจากที่มีการเชื่อมต่อเราท์เตอร์ทั้งหมดเข้าด้วยกัน

ในการแลกเปลี่ยนข้อมูลกันระหว่าง AS/400 กับระบบ Tandem ผ่านเราท์เตอร์ Router_Host1 และ Router_PCC1 ซึ่งใช้โพรทคอล SNA/SDLC ในที่นี้ใช้ฟังก์ชัน STUN เพื่อสร้าง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ช่องทางสำหรับการส่งผ่านข้อมูล SNA/SDLC โดยมีการกำหนดกลุ่ม (group) ให้กับพอร์ทที่ต้องการใช้งาน เพื่อแบ่งแยกช่องทางของข้อมูลได้อย่างชัดเจนทำให้ข้อมูลในแต่ละพอร์ทเป็นอิสระจากกัน โดยเนื้อข้อมูลที่ส่งผ่านฟังก์ชันนี้ยังคงความเป็นโพรโทคอล SNA/SDLC อยู่ นั่นคือยังคงมีกาใช้เฟรม unnumbered เพื่อขอสร้างหรือยกเลิกการติดต่อระหว่างคอมพิวเตอร์หลัก ใช้เฟรม information สำหรับเฟรมข้อมูล และใช้เฟรม supervisory เพื่อควบคุมความถูกต้องและปริมาณของเฟรม จากตารางที่ 6.5 เป็นรูปแบบการส่งผ่านข้อมูล SNA/SDLC ผ่านฟังก์ชั่น STUN ซึ่งเป็น proprietary ของ Cisco ทำให้การตรวจจับแพ็กเก็ตสามารถตรวจจับได้เฉพาะแพ็กเก็ต SNA/SDLC เท่านั้น ซึ่งในรูปที่ 6.5 จะแสดงให้เห็นถึงแพ็กเก็ต SNA/SDLC ที่ปรากฏอยู่ใน Tunnel ที่ถูกสร้างขึ้นระหว่าง Router_Host1 และ Router_PCC1 โดยที่

NDI : หมายถึง ข้อมูลที่ได้รับมาจากเครือข่าย (Network) ในที่นี้คือ Router_PCC1

SDI : หมายถึงข้อมูลที่ส่งจากอินเทอร์เฟสที่ถูก encapsulate ด้วย STUN ในที่นี้คืออินเทอร์เฟส Serial 2/1 ของ Router_Host1

Data : หมายถึงข้อมูลซึ่งประกอบด้วยเฟรมของ SNA/SDLC นั่นคือ ค่าแอดเดรส ค่า Control และข้อมูล

```
1w3d: STUN basic: 00:00:00 Serial2/1        NDI:   Data: c1b1
1w3d: STUN basic: 00:00:00 Serial2/1        SDI:   Data: c1d1
1w3d: STUN basic: 00:00:00 Serial2/1        NDI:   Data: c1ac2c000101008e0390
1w3d: STUN basic: 00:00:00 Serial2/1        NDI:   Data: c1b1
1w3d: STUN basic: 00:00:00 Serial2/1        SDI:   Data: c1f1
1w3d: STUN basic: 00:00:00 Serial2/1        NDI:   Data: c1b1
1w3d: STUN basic: 00:00:00 Serial2/1        SDI:   Data: c1f1
1w3d: STUN basic: 00:00:00 Serial2/1        NDI:   Data: c1b1
1w3d: STUN basic: 00:00:00 Serial2/1        SDI:   Data: c1fa2c000101008c0390
1w3d: STUN basic: 00:00:00 Serial2/1        NDI:   Data: c1d1
```

รูปที่ 6.5 รูปแบบแพ็กเก็ต SNA/SDLC จาก Router_Host1

ในส่วนถัดมา เป็นส่วนของการสร้างการเชื่อมต่อระหว่างระบบ Tandem กับเครื่อง ATM ซึ่งในที่นี้สามารถแบ่งการอธิบายได้ออกเป็น 2 ส่วน ในส่วนแรกนี้เป็นส่วนของการ setup ในเลเยอร์ 2 (data link) ซึ่งใช้กระบวนการ LAPB ระหว่าง Router_PCC1 กับระบบ Tandem โดยที่ฟิลด์ EQ เป็นข้อมูลที่มาจาก Router_PCC1 และฟิลด์ LN เป็นข้อมูลที่มาจากระบบ Tandem

```
(EQ) 8          15:07:09.6252679    LAPB: Addr=001 Type=SABM    P/F=1(F) FCS=Good
 Record #8        (EQ) Captured on 07.12.01 at 15:07:09.625267956 Length =     4
LAPB:
  Address               = 001
  Frame Type            = 0x3f (SABM)
  Control Information = 0x3F
    ...1 .... P/F Bit = 1 (Final)
  FCS                   = 0xeb-df (Good)
(LN) 9          15:07:09.6296947    LAPB: Addr=001 Type=UA      P/F=1(F) FCS=Good
 Record #9        (LN) Captured on 07.12.01 at 15:07:09.629694756 Length =     4
LAPB:
  Address               = 001
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
  Frame Type          = 0x73 (UA)
  Control Information = 0x73
    ...1 .... P/F Bit = 1 (Final)
  FCS                 = 0x83-57 (Good)
(LN) 10       15:07:09.6321948    LAPB: Addr=003 Type=Info    P/F=0(P) N(S)=0     N(R)=0
FCS=Good X25: Mod=8   LCN=0     Type=Restart Indication/Request
 Record #10      (LN) Captured on 07.12.01 at 15:07:09.632194856 Length =     9
LAPB:
  Address             = 003
  Frame Type          = 0x00 (Information)
  Control Information = 0x00
    000. .... N(R) = 0
    ...0 .... P/F Bit = 0 (Poll)
    .... 000. N(S) = 0
  FCS                 = 0xc4-78 (Good)
X25:
  Header Information              = 0x10
    ..01 .... Modulo = 1 (8  )
    .... 0000 Logical Channel Group Number = 0
  Combined LCN                    = 0
  Logical Channel Number          = 0
  Cause Code                      = 7 (Network operational)
  Diagnostic Code                 = 0(No additional info)
  Diagnostic Explanation          = (none)
  Packet Type                     = 0xfb (Restart Indication/Request)
(EQ) 11       15:07:09.6461535    LAPB: Addr=003 Type=RR      P/F=0(P) N(R)=1     FCS=Good
 Record #11      (EQ) Captured on 07.12.01 at 15:07:09.646153556 Length =     4
LAPB:
  Address             = 003
  Frame Type          = 0x21 (RR)
  Control Information = 0x21
    001. .... N(R) = 1
    ...0 .... P/F Bit = 0 (Poll)
  FCS                 = 0xa4-15 (Good)
(EQ) 12       15:07:09.6674037    LAPB: Addr=001 Type=Info    P/F=0(P) N(S)=0     N(R)=1
FCS=Good X25: Mod=8   LCN=0     Type=Restart Indication/Request
 Record #12      (EQ) Captured on 07.12.01 at 15:07:09.667403755 Length =     9
LAPB:
  Address             = 001
  Frame Type          = 0x20 (Information)
  Control Information = 0x20
    001. .... N(R) = 1
    ...0 .... P/F Bit = 0 (Poll)
    .... 000. N(S) = 0
  FCS                 = 0x17-87 (Good)
X25:
  Header Information              = 0x10
    ..01 .... Modulo = 1 (8  )
    .... 0000 Logical Channel Group Number = 0
  Combined LCN                    = 0
  Logical Channel Number          = 0
  Cause Code                      = 0 (DTE originated)
  Diagnostic Code                 = 0(No additional info)
  Diagnostic Explanation          = (none)
  Packet Type                     = 0xfb (Restart Indication/Request)
(LN) 13       15:07:09.6776640    LAPB: Addr=001 Type=RR      P/F=0(P) N(R)=1     FCS=Good
 Record #13      (LN) Captured on 07.12.01 at 15:07:09.677664055 Length =     4
LAPB:
  Address             = 001
  Frame Type          = 0x21 (RR)
  Control Information = 0x21
    001. .... N(R) = 1
    ...0 .... P/F Bit = 0 (Poll)
  FCS                 = 0x14-26 (Good)
(EQ) 14       15:07:24.6759438    LAPB: Addr=003 Type=RR      P/F=0(P) N(R)=1     FCS=Good
 Record #14      (EQ) Captured on 07.12.01 at 15:07:24.675943876 Length =     4
LAPB:
  Address             = 003
  Frame Type          = 0x21 (RR)
  Control Information = 0x21
    001. .... N(R) = 1
    ...0 .... P/F Bit = 0 (Poll)
  FCS                 = 0xa4-15 (Good)
(LN) 15       15:07:27.2528451    LAPB: Addr=003 Type=Info    P/F=0(P) N(S)=1     N(R)=1
FCS=Good X25: Mod=8   LCN=1     Type=Call Incoming/Request
 Record #15      (LN) Captured on 07.12.01 at 15:07:27.252845111 Length =    24
LAPB:
  Address             = 003
  Frame Type          = 0x22 (Information)
  Control Information = 0x22
    001. .... N(R) = 1
    ...0 .... P/F Bit = 0 (Poll)
    .... 001. N(S) = 1
  FCS                 = 0x83-f2 (Good)
X25:
  Header Information              = 0x10
    .0.. .... D Bit = 0
    ..01 .... Modulo = 1 (8  )
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
    .... 0000 Logical Channel Group Number = 0
  Combined LCN                    = 1
  Logical Channel Number          = 1
  Called Address                  = 49008000555
  Calling Address                 = 50008000555
  Packet Type                     = 0x0b (Call Incoming/Request)
(EQ) 16       15:07:27.2659705    LAPB: Addr=003 Type=RR      P/F=0(P) N(R)=2     FCS=Good
 Record #16      (EQ) Captured on 07.12.01 at 15:07:27.265970511 Length =      4
LAPB:
  Address                 = 003
  Frame Type              = 0x41 (RR)
  Control Information = 0x41
    010. .... N(R) = 2
    ...0 .... P/F Bit = 0 (Poll)
  FCS                     = 0xa2-76 (Good)
(EQ) 17       15:07:27.2988875    LAPB: Addr=001 Type=Info    P/F=0(P) N(S)=1     N(R)=2
FCS=Good X25: Mod=8   LCN=1     Type=Call Connect/Accept
 Record #17      (EQ) Captured on 07.12.01 at 15:07:27.298887510 Length =      9
LAPB:
  Address                 = 001
  Frame Type              = 0x42 (Information)
  Control Information = 0x42
    010. .... N(R) = 2
    ...0 .... P/F Bit = 0 (Poll)
    .... 001. N(S) = 1
  FCS                     = 0x1e-fb (Good)
X25:
  Header Information              = 0x10
    .0.. .... D Bit = 0
    ..01 .... Modulo = 1 (8  )
    .... 0000 Logical Channel Group Number = 0
  Combined LCN                    = 1
  Logical Channel Number          = 1
  Called Address                  = (None)
  Calling Address                 = (None)
  Packet Type                     = 0x0f (Call Connect/Accept)
(EQ) 18       15:07:27.3056063    LAPB: Addr=001 Type=Info    P/F=0(P) N(S)=2     N(R)=2
FCS=Good X25: Mod=8   LCN=1     Type=Data
 Record #18      (EQ) Captured on 07.12.01 at 15:07:27.305606310 Length =      9
LAPB:
  Address                 = 001
  Frame Type              = 0x44 (Information)
  Control Information = 0x44
    010. .... N(R) = 2
    ...0 .... P/F Bit = 0 (Poll)
    .... 010. N(S) = 2
  FCS                     = 0xca-91 (Good)
X25:
  Header Information              = 0x90
    1... .... Q Bit = 1
    .0.. .... D Bit = 0
    ..01 .... Modulo = 1 (8  )
    .... 0000 Logical Channel Group Number = 0
  Combined LCN                    = 1
  Logical Channel Number          = 1
  P(R)/P(S) Fields                = 0x00
    000. .... P(R) = 0
    ...0 .... M bit = 0
    .... 000. P(S) = 0
  Packet Type                     = 0x00 (Data)
```

รูปที่ 6.6 รูปแบบการสร้างวงจรเสมือนระหว่าง Tandem กับ Router_PCC1 ด้วยโพรโทคอล X.25

ขั้นตอนเริ่มแรกนั้น Router_PCC1 จะเป็นตัวเริ่มต้นส่งเฟรม SABM (Set Asynchronous Balance Mode) เพื่อขอสร้างการเชื่อมต่อกับระบบ Tandem เมื่อ Tandem ได้รับเฟรมนี้ก็จะทำการตอบกลับด้วยเฟรม UA (Unnumbered Acknowledgement) เพื่อตอบรับการขอสร้างการเชื่อมต่อพร้อมกับส่งเฟรม Restart Request จากนั้น Router_PCC1 จะทำการส่งเฟรม Restart Request ออกไปให้ Tandem และ Tandem จะทำการส่งเฟรม Call Request โดย Router_PCC1 ตอบกลับด้วยเฟรม Call Confirm ซึ่งเป็นอันสิ้นสุดกระบวนการ LAPB

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในกระบวนการถัดมาเป็นการสร้างวงจรเสมือนระหว่างเครื่อง ATM กับ Tandem ซึ่งกระบวนการนี้จะถูกแยกกระทำเป็น 2 กระบวนการ คือกระบวนการแรกเป็นส่วนของเครื่อง ATM กับ Router_Branch1 ซึ่งอยู่ภายในพื้นที่ของ Branch1 ซึ่งจะต้องกระทำการในขั้นตอนของ SNA/SDLC ให้เสร็จสิ้นก่อน ซึ่งหมายความว่า เครื่อง ATM จะต้องสามารถส่ง polling โต้ตอบกับเราท์เตอร์ได้ก่อน หลังจากนั้นข้อมูลจึงจะถูกส่งผ่าน Router_Branch1 ไปยัง Router_PCC1 และผ่านเข้าไปสู่ Tandem Host ซึ่งเป็นกระบวนการที่สอง ซึ่งเป็นส่วนของโพรโทคอล X.25 ดังรูปที่ 6.7

```
(EQ) 45       14:16:29.2405977    HDLC: Addr=007 Type=SNRM    P/F=1(F) FCS=Good
 Record #45      (EQ) Captured on 07.20.01 at 14:16:29.240597766 Length =     4
HDLC:
  Address             = 007
  Frame Type          = 0x93 (SNRM)
  Control Information = 0x93
    ...1 .... P/F Bit = 1 (Final)
  FCS                 = 0x5d-e4 (Good)
 Record #45      (EQ) Captured on 07.20.01 at 14:16:29.240597766 Length =     4

    07 93 5d e4                                              ..].
(LN) 46       14:16:29.4157702    HDLC: Addr=007 Type=UA      P/F=1(F) FCS=Good
 Record #46      (LN) Captured on 07.20.01 at 14:16:29.415770262 Length =     4
HDLC:
  Address             = 007
  Frame Type          = 0x73 (UA)
  Control Information = 0x73
    ...1 .... P/F Bit = 1 (Final)
  FCS                 = 0x53-03 (Good)
 Record #46      (LN) Captured on 07.20.01 at 14:16:29.415770262 Length =     4

    07 73 53 03                                              .sS.
(EQ) 47       14:16:29.4406012    HDLC: Addr=007 Type=RNR     P/F=1(F) N(R)=0     FCS=Good
 Record #47      (EQ) Captured on 07.20.01 at 14:16:29.440601261 Length =     4
HDLC:
  Address             = 007
  Frame Type          = 0x15 (RNR)
  Control Information = 0x15
    000. .... N(R) = 0
    ...1 .... P/F Bit = 1 (Final)
  FCS                 = 0x63-05 (Good)
 Record #47      (EQ) Captured on 07.20.01 at 14:16:29.440601261 Length =     4

    07 15 63 05                                              ..c.
(LN) 48       14:16:29.6034808    HDLC: Addr=007 Type=RR      P/F=1(F) N(R)=0     FCS=Good
 Record #48      (LN) Captured on 07.20.01 at 14:16:29.603480857 Length =     4
HDLC:
  Address             = 007
  Frame Type          = 0x11 (RR)
  Control Information = 0x11
    000. .... N(R) = 0
    ...1 .... P/F Bit = 1 (Final)
  FCS                 = 0x47-43 (Good)
 Record #48      (LN) Captured on 07.20.01 at 14:16:29.603480857 Length =     4

    07 11 47 43                                              ..GC
(EQ) 49       14:16:29.6289378    HDLC: Addr=007 Type=RNR     P/F=1(F) N(R)=0     FCS=Good
 Record #49      (EQ) Captured on 07.20.01 at 14:16:29.628937856 Length =     4
HDLC:
  Address             = 007
  Frame Type          = 0x15 (RNR)
  Control Information = 0x15
    000. .... N(R) = 0
    ...1 .... P/F Bit = 1 (Final)
  FCS                 = 0x63-05 (Good)
 Record #49      (EQ) Captured on 07.20.01 at 14:16:29.628937856 Length =     4

    07 15 63 05                                              ..c.
(LN) 50       14:16:29.7909862    HDLC: Addr=007 Type=RR      P/F=1(F) N(R)=0     FCS=Good
 Record #50      (LN) Captured on 07.20.01 at 14:16:29.790986252 Length =     4
HDLC:
  Address             = 007
  Frame Type          = 0x11 (RR)
  Control Information = 0x11
    000. .... N(R) = 0
    ...1 .... P/F Bit = 1 (Final)
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
  FCS                 = 0x47-43 (Good)
 Record #50      (LN) Captured on 07.20.01 at 14:16:29.790986252 Length =     4

    07 11 47 43                                              ..GC
 (EQ) 147        14:16:39.4407746      HDLC: Addr=007 Type=Info      P/F=1(F) N(S)=0       N(R)=0
FCS=Good Auto LAN over WAN Recognition: >>> NOTICE >>> Unrecognized data.
 Record #147     (EQ) Captured on 07.20.01 at 14:16:39.440774608 Length =    22
HDLC:
  Address             = 007
  Frame Type          = 0x10 (Information)
  Control Information = 0x10
    000. .... N(R) = 0
    ...1 .... P/F Bit = 1 (Final)
    .... 000. N(S) = 0
  FCS                 = 0x8b-03 (Good)
Auto LAN over WAN Recognition: >>> NOTICE >>> Unrecognized data.
 Record #147     (EQ) Captured on 07.20.01 at 14:16:39.440774608 Length =    22

    07 10 2d 00 00 00 00 4e    6b 80 00 11 01 01 05 00    ..-....N k.......
    00 00 00 00 8b 03                                     ......
(LN) 148      14:16:39.6349079    HDLC: Addr=007 Type=RR      P/F=1(F) N(R)=1     FCS=Good
 Record #148     (LN) Captured on 07.20.01 at 14:16:39.634907903 Length =     4
HDLC:
  Address             = 007
  Frame Type          = 0x31 (RR)
  Control Information = 0x31
    001. .... N(R) = 1
    ...1 .... P/F Bit = 1 (Final)
  FCS                 = 0x45-62 (Good)
 Record #148     (LN) Captured on 07.20.01 at 14:16:39.634907903 Length =     4

    07 31 45 62                                              .1Eb
(EQ) 149      14:16:39.6607784    HDLC: Addr=007 Type=RR      P/F=1(F) N(R)=0     FCS=Good
 Record #149     (EQ) Captured on 07.20.01 at 14:16:39.660778403 Length =     4
HDLC:
  Address             = 007
  Frame Type          = 0x11 (RR)
  Control Information = 0x11
    000. .... N(R) = 0
    ...1 .... P/F Bit = 1 (Final)
  FCS                 = 0x47-43 (Good)
 Record #149     (EQ) Captured on 07.20.01 at 14:16:39.660778403 Length =     4

    07 11 47 43                                              ..GC
(LN) 150        14:16:39.8534533      HDLC: Addr=007 Type=Info      P/F=1(F) N(S)=0       N(R)=1
FCS=Good Auto LAN over WAN Recognition: >>> NOTICE >>> Unrecognized data.
 Record #150     (LN) Captured on 07.20.01 at 14:16:39.853453398 Length =    23
HDLC:
  Address             = 007
  Frame Type          = 0x30 (Information)
  Control Information = 0x30
    001. .... N(R) = 1
    ...1 .... P/F Bit = 1 (Final)
    .... 000. N(S) = 0
  FCS                 = 0xd2-3b (Good)
Auto LAN over WAN Recognition: >>> NOTICE >>> Unrecognized data.
 Record #150     (LN) Captured on 07.20.01 at 14:16:39.853453398 Length =    23

    07 30 2d 00 00 00 00 4e    eb 80 00 11 01 40 40 40    .0-....N .....@@@
    40 40 40 40 40 40 d2 3b                               @@@@@@.;
(EQ) 151      14:16:39.9141160    HDLC: Addr=007 Type=RR      P/F=1(F) N(R)=1     FCS=Good
 Record #151     (EQ) Captured on 07.20.01 at 14:16:39.914116096 Length =     4
HDLC:
  Address             = 007
  Frame Type          = 0x31 (RR)
  Control Information = 0x31
    001. .... N(R) = 1
    ...1 .... P/F Bit = 1 (Final)
  FCS                 = 0x45-62 (Good)
 Record #151     (EQ) Captured on 07.20.01 at 14:16:39.914116096 Length =     4

    07 31 45 62                                              .1Eb
(LN) 152      14:16:40.1036670    HDLC: Addr=007 Type=RR      P/F=1(F) N(R)=1     FCS=Good
 Record #152     (LN) Captured on 07.20.01 at 14:16:40.103667092 Length =     4
HDLC:
  Address             = 007
  Frame Type          = 0x31 (RR)
  Control Information = 0x31
    001. .... N(R) = 1
    ...1 .... P/F Bit = 1 (Final)
  FCS                 = 0x45-62 (Good)
```

รูปที่ 6.7 กระบวนการของเครื่อง ATM ในการติดต่อกับ Router_Branch1

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

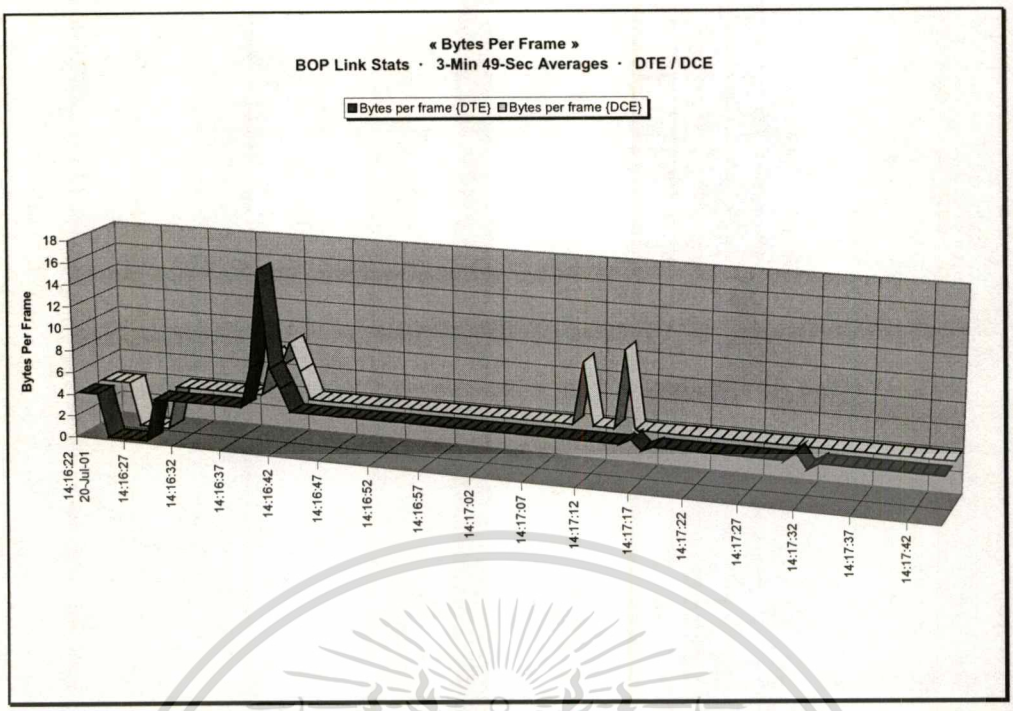
จากรูปจะเห็นว่า เมื่อ Router_Branch1 ส่งเฟรม SNRM ให้แก่เครื่อง ATM โดยที่เครื่อง ATM อยู่ในสภาวะพร้อมรับข้อมูล เครื่อง ATM จะทำการตอบกลับด้วยเฟรม UA หลังจากนั้นเราท์เตอร์จะตอบกลับด้วยเฟรม RNR ซึ่งแสดงให้เห็นว่า เราท์เตอร์อยู่ในสภาวะที่ยังไม่พร้อมรับข้อมูล โดยเกิดจากเราท์เตอร์ Router_Branch1 เองที่จะต้องสร้างการเชื่อมต่อกับเราท์เตอร์ Router_PCC1 ด้วยโพรโทคอล DLSw และกระบวนการที่เราท์เตอร์ Router_PCC1 ซึ่งจะต้องสร้างการเชื่อมต่อกับ Tandem ด้วยโพรโทคอล X.25 ให้เสร็จสมบูรณ์ก่อน ซึ่งหลังจากที่ Tandem สามารถสร้างวงจรเสมือนเชื่อมต่อกับ Router_PCC1 ได้ และเราท์เตอร์ Router_PCC1 และ Router_Branch1 สร้างวงจร DLSw ได้ก็จะทำให้ Router_Branch1 ส่งเฟรม Info ให้แก่เครื่อง ATM และเครื่อง ATM ตอบกลับด้วยเฟรม RR ซึ่งเป็นผลให้เครื่อง ATM สามารถสื่อสารกันกับ Tandem ได้ โดยในรูปที่ 6.8 แสดงให้เห็นถึงกระบวนการในการสร้างวงจรเสมือนระหว่าง Tandem กับเราท์เตอร์ Router_PCC1 ซึ่งเราท์เตอร์เป็นตัวส่ง Call Request และ Tandem ตอบรับด้วยเฟรม Call Confirm โดยที่ค่าที่อยู่ภายในเครื่องหมายวงเล็บหมายถึง ความยาวของแพ็กเก็ต มีหน่วยเป็นไบท์ และใช้ modulo “8”

```
8w6d: Serial1/1: X.25 O R1 Call (20) 8 lci 21
8w6d:   From (11): 50002000262 To (11): 49002000262
8w6d:   Facilities: (0)
8w6d:   Call User Data (4): 0xC3000000 (qllc)
8w6d: Serial1/1: X.25 I R1 Call Confirm (5) 8 lci 21
8w6d:   From (0): To (0):
8w6d:   Facilities: (0)
8w6d: Serial1/1: X.25 I D1 Data (5) Q 8 lci 21 PS 0 PR 0
8w6d: Serial1/1: X.25 O D1 Data (11) Q 8 lci 21 PS 0 PR 1
8w6d: Serial1/1: X.25 I D1 Data (5) Q 8 lci 21 PS 1 PR 1
8w6d: Serial1/1: X.25 O D1 Data (5) Q 8 lci 21 PS 1 PR 2
8w6d: Serial1/1: X.25 I D1 Data (21) 8 lci 21 PS 2 PR 2
8w6d: Serial1/1: X.25 O D1 Data (22) 8 lci 21 PS 2 PR 3
8w6d: Serial1/1: X.25 I D1 Data (15) 8 lci 21 PS 3 PR 3
8w6d: Serial1/1: X.25 O D1 Data (14) 8 lci 21 PS 3 PR 4
8w6d: Serial1/1: X.25 I R1 Clear (5) 8 lci 21
```

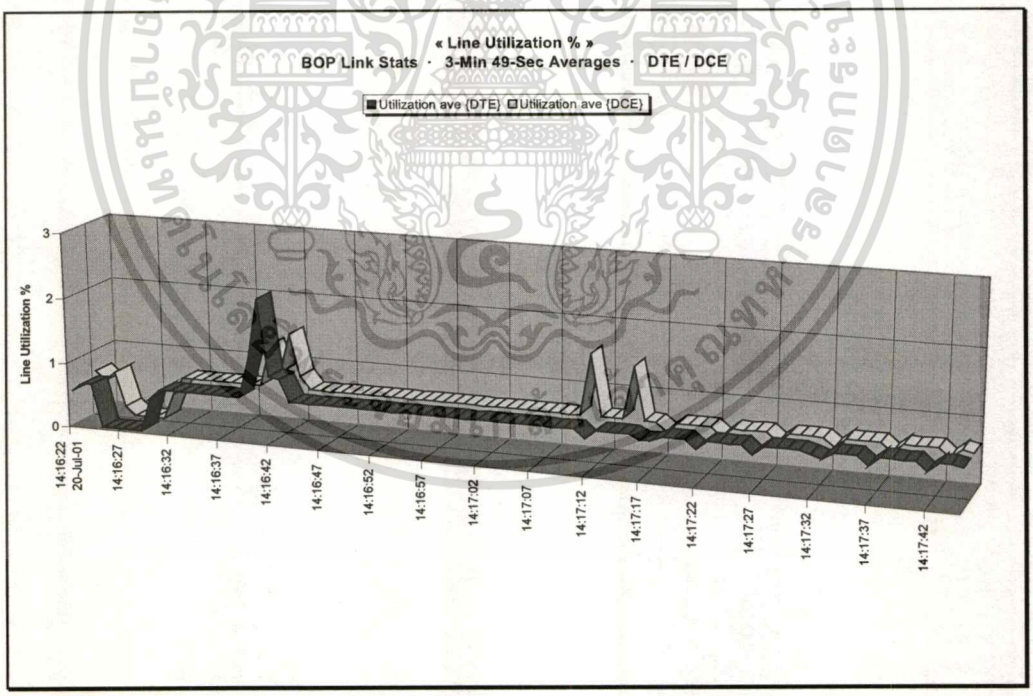
รูปที่ 6.8 กระบวนการในการสร้างวงจรเสมือนระหว่าง Tandem และ Router_PCC1

ในรูปที่ 6.9 และ 6.10 แสดงให้เห็นถึงค่า Throughput ในรูปของจำนวนไบท์ต่อเฟรม และค่า Utilization เทียบจากแบนด์วิดท์ 9.6 Kbps ในช่วงที่ ATM กำลังอยู่ในสภาวะที่เพิ่งเริ่มติดต่อกับ Router_Branch1 จนกระทั่งสามารถติดต่อกับ Tandem ในขณะที่ยังไม่มีรายการถอน โดยมีค่าเฉลี่ยของ Throughput เท่ากับ 5 เฟรมต่อวินาที และมีค่า Utilization เฉลี่ยอยู่ที่ 10 bps

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



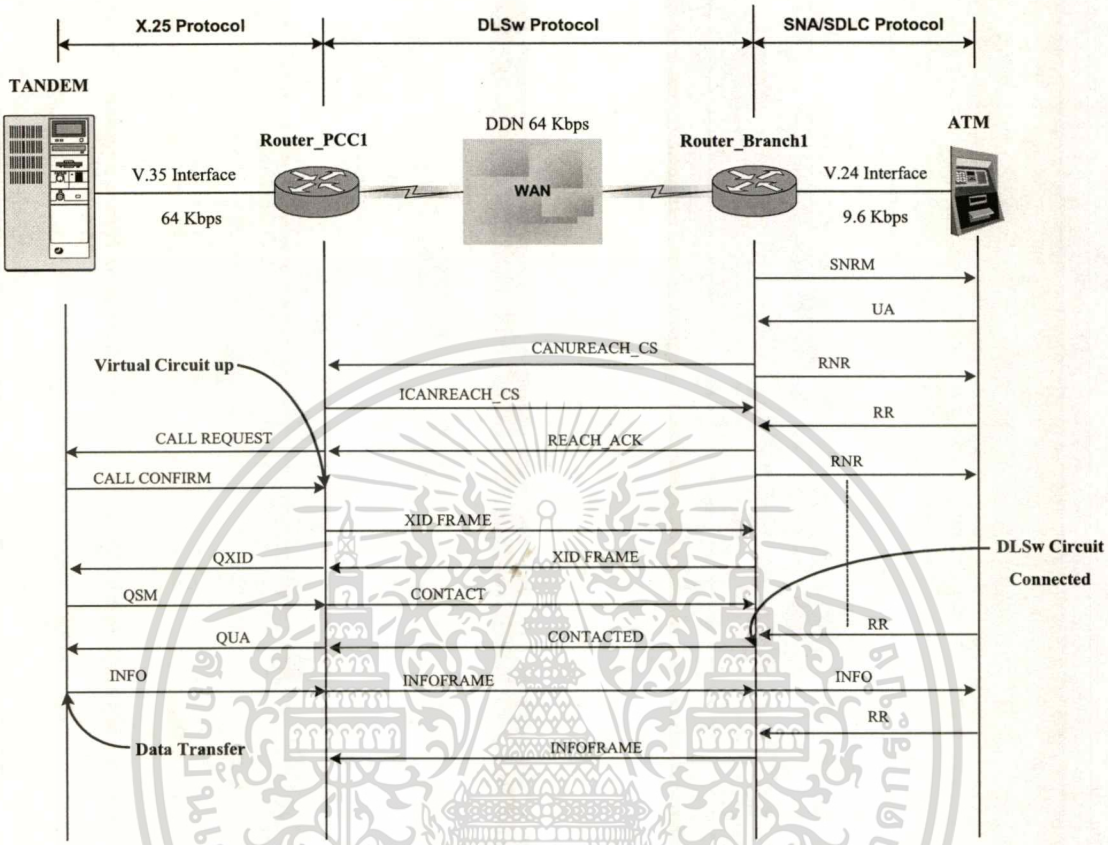
รูปที่ 6.9 จำนวนไบท์ต่อเฟรมระหว่าง Router_Branch1 กับเครื่อง ATM ในขณะสร้างการเชื่อมต่อ



รูปที่ 6.10 ค่า Utilization ระหว่าง Router_Branch1 กับเครื่อง ATM ในขณะสร้างการเชื่อมต่อ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากกระบวนการต่าง ๆ ที่กล่าวมาข้างต้นสามารถนำมาเขียนให้อยู่ในรูปไดอะแกรมเพื่อให้เข้าใจหลักการทำงานของอุปกรณ์ในและส่วน และการทำงานของโพรโทคอลในแต่ละขั้นตอนได้ง่ายขึ้น ซึ่งในที่นี้สามารถแบ่งการทำงานได้เป็น 3 ส่วนตามรูปแบบโพรโทคอลที่ใช้งานดังรูปที่6.11



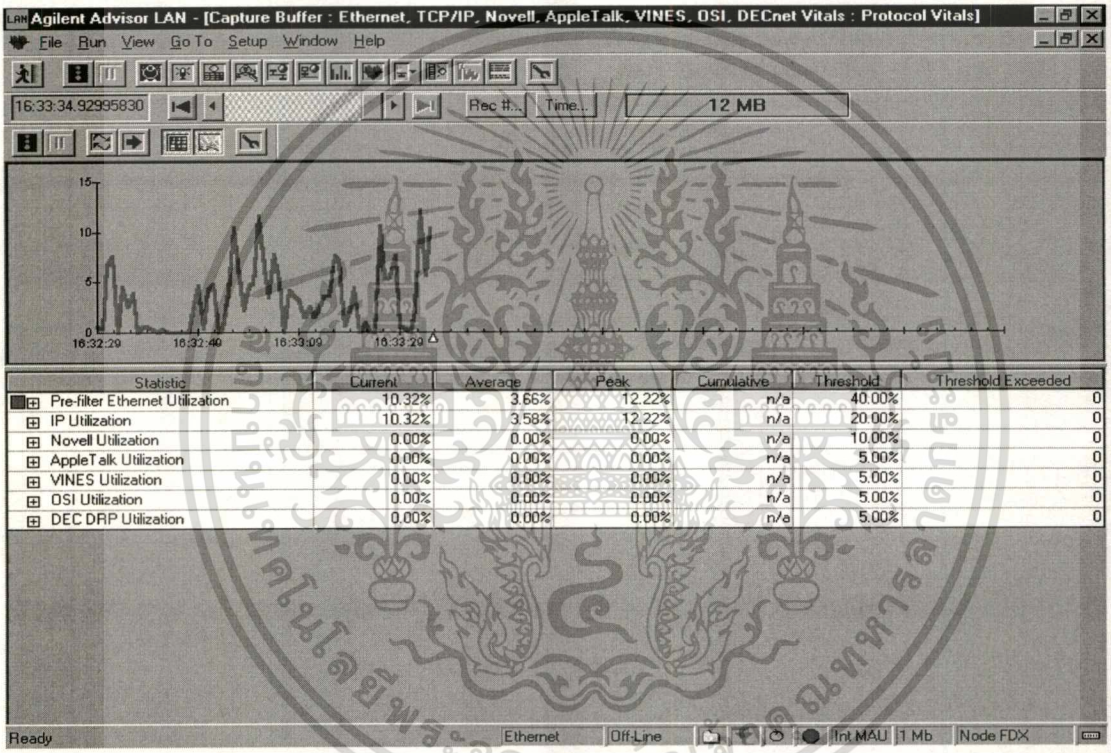
รูปที่ 6.11 ขั้นตอนของกระบวนการส่งผ่านข้อมูลของโพรโทคอล SNA/SDLC และ X.25 บนเครือข่าย IP โดยละเอียด

ขั้นตอนของกระบวนการต่าง ๆ สามารถสรุปได้เป็นดังนี้

1. Router_Branch1 ส่งเฟรม SNRM ให้แก่เครื่อง ATM และได้รับเฟรม UA ตอบกลับจากเครื่อง ATM
2. Router_Branch1 ใช้กระบวนการของ DLSw เพื่อส่งเฟรม CANUREACH_CS (Can U Reach Station-circuit start) ให้กับ Router_PCC1 และได้รับเฟรมที่ตอบกลับด้วยเฟรม ICANREACH_CS (I Can Reach Station-circuit start) และทำการส่งเฟรมตอบกลับไปยัง Router_PCC1 ด้วย REACH_ACK (Reach Acknowledgment)
3. จากนั้น Router_PCC1 จะทำการส่งเฟรมในกระบวนการของ X.25 ด้วยเฟรม Call Request เพื่อสร้างวงจรเสมือนไปยัง Tandem และได้รับเฟรมตอบกลับด้วยเฟรม Call Confirm ซึ่งในขณะนี้จะทำให้วงจรเสมือนเกิดขึ้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4. Router_PCC1 ส่งเฟรม XID ไปยัง Router_Branch1 โดยที่ Router_Branch1 ตอบกลับด้วยเฟรม XID เช่นกันทำให้ Router_PCC1 ส่งเฟรม QXID ไปยัง Tandem และตอบกลับด้วยเฟรม QSM
5. Router_PCC1 ส่งเฟรม CONTACT เพื่อสร้างวงจร DLSw ระหว่าง Router_PCC1 กับ Router_Branch1 ซึ่งหลังจาก Router_Branch1 ตอบกลับด้วยเฟรม CANTACTED จะทำให้วงจร DLSw เป็น Connected
6. Router_PCC1 ส่งเฟรม QUA ให้แก่ Tandem หลังจากนั้นจะเป็นเฟสที่ข้อมูลสามารถส่งผ่านถึงกันได้ ซึ่งเป็นอันเสร็จสิ้นกระบวนการ



รูปที่ 6.12 รูปแสดง Utilization ของเครื่อง ATM ซึ่งผ่าน WAN ในขณะใช้งานปกติ

จากรูปที่ 6.12 เป็นค่า Utilization ผ่านเครือข่าย WAN ที่มีค่าแบนด์วิดท์เท่ากับ 64 Kbps จะเห็นได้ว่าค่าเฉลี่ยอยู่ที่ 3.58% หรือเท่ากับ 2.29 Kbps

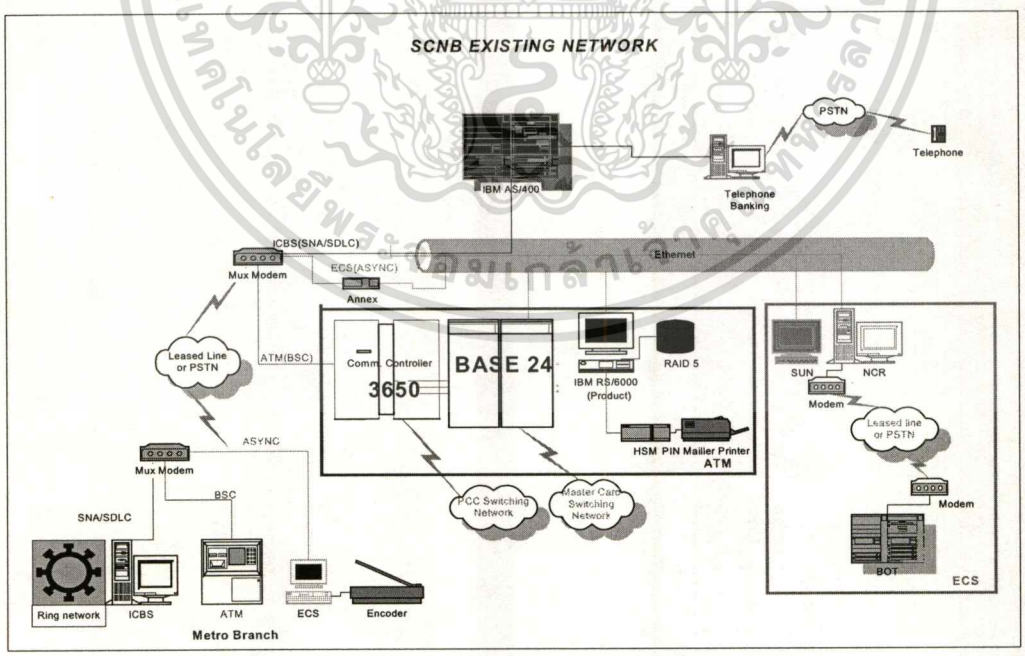
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 7
การประยุกต์ใช้งาน

7.1 การนำมาประยุกต์ใช้งานกับเครือข่าย

ในปัจจุบันองค์กรต่าง ๆ ไม่ว่าจะเป็นทางภาครัฐบาลและภาคเอกชนได้มีการสร้างระบบเครือข่ายคอมพิวเตอร์ทั้งระยะใกล้และระยะไกลเป็นของตัวเอง (LAN and WAN) โดยที่เครือข่ายระยะใกล้ (LAN) เป็นรูปแบบการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์ด้วยกันเองหรือไม่ก็ระหว่างเครื่องคอมพิวเตอร์กับระบบโฮลต์ (Host) ภายในอาคารเดียวกัน ส่วนรูปแบบของเครือข่ายระยะไกล (WAN) จะเป็นรูปแบบที่มีการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์กับระบบโฮลต์ที่อยู่ห่างไกลกันมากซึ่งในที่นี้อาจหมายถึงสาขาก็ได้ ทั้งนี้รูปแบบเครือข่ายระยะไกลจำเป็นต้องอาศัย carrier (เช่น TOT TA และ TT&T) เป็นผู้ดำเนินการจัดสร้างคู่สายระหว่างต้นทางและปลายทางที่ต้องการเพื่อใช้ในการเชื่อมต่อระบบเครือข่ายเข้าด้วยกันโดยใช้โพรโทคอล HDLC X.25 หรือ Frame Relay ในการสื่อสารระหว่างกัน

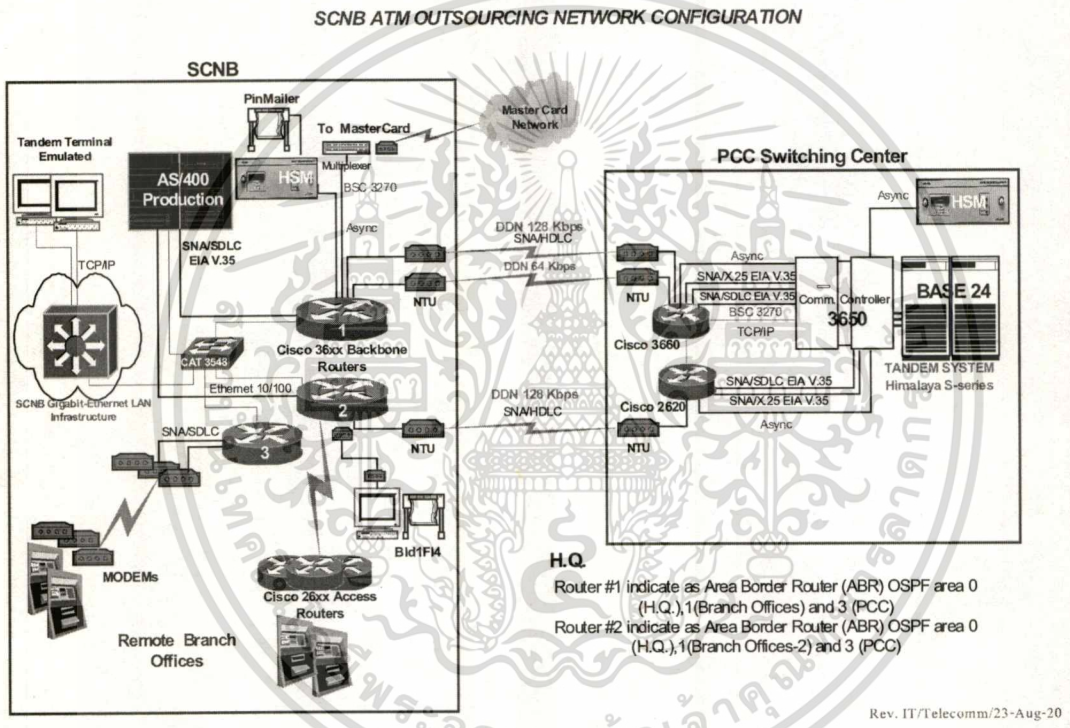
จากหลักการเชื่อมโยงดังกล่าวข้างต้น ผู้จัดทำวิทยานิพนธ์จึงได้ออกแบบระบบเครือข่ายสื่อสารข้อมูลเพื่อนำมาประยุกต์ใช้งานกับเครือข่ายที่มีอยู่เดิม เพื่อเพิ่มประสิทธิภาพการทำงานของเครือข่าย และความน่าเชื่อถือระหว่างเครื่อง ATM กับระบบโฮลต์ ดังรูปที่ 7.1



รูปที่ 7.1 ระบบเครือข่ายที่มีอยู่เดิมของธนาคารสแตนดาร์ดชาร์เตอร์ดนครธน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากรูปที่ 7.1 แสดงให้เห็นถึงระบบเครือข่ายที่มีอยู่เดิมของธนาคารสแตนดาร์ดชาร์เตอร์ด นครธน ซึ่งมีทั้งระบบ LAN ที่ใช้ในการติดต่อสื่อสารกันภายในอาคารสำนักงานใหญ่ และมีระบบ WAN เพื่อเชื่อมโยงไปยังสาขาต่าง ๆ ประมาณ 40 สาขา โดยมีระบบงาน On-line อยู่ 3 ระบบด้วยกันคือ ระบบฝาก-ถอน ระบบงาน ATM และระบบเช็คเคลียร์ริ่ง โดยใช้รูปแบบโพรโทคอล SNA/SDLC Bisync และ Asyncronous ตามลำดับ โดยมี AS/400 เป็น Main Database และมี Tandem เป็น Host สำหรับระบบ ATM และใช้โมเด็ม multiplexer เชื่อมต่อกับคู่สายวงจรเช่าอนาลอกความเร็ว 19.2 Kbps ไปยังสาขาเพื่อเชื่อมต่อกับ Branch server เครื่อง ATM และคอมพิวเตอร์ตามลำดับ



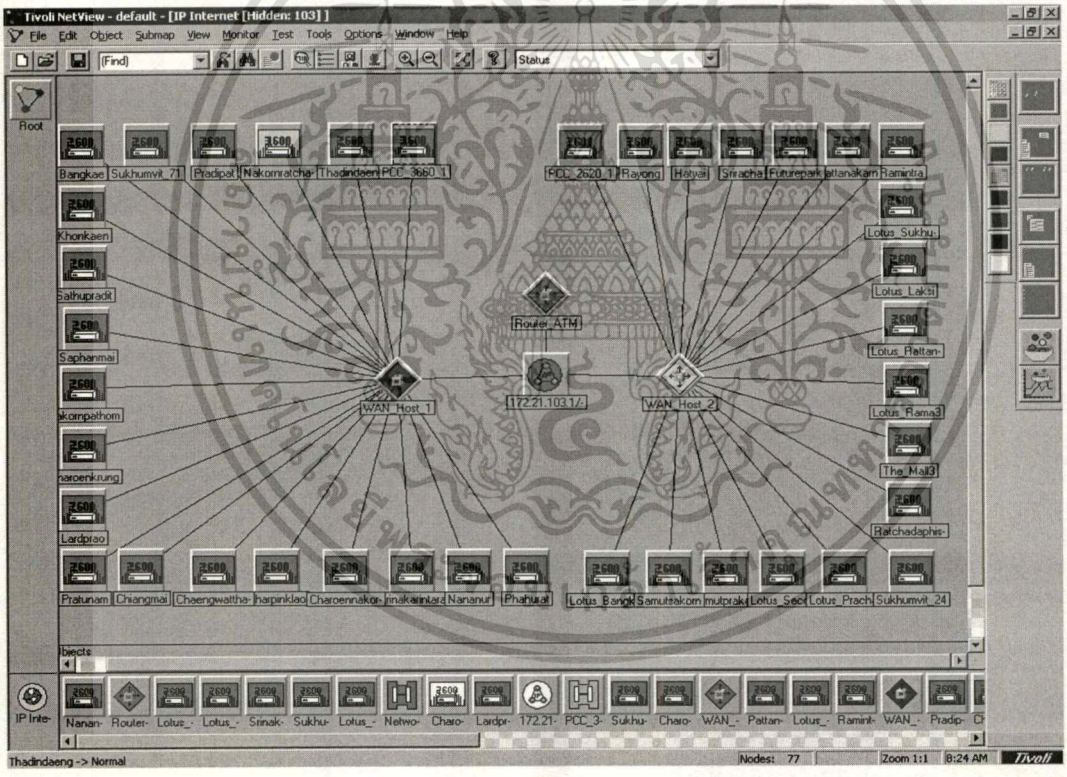
รูปที่ 7.2 รูปแบบการนำเครือข่ายจากแบบจำลองทดสอบมาประยุกต์ใช้งานกับเครือข่ายของธนาคารสแตนดาร์ดชาร์เตอร์นครธน

จากรูปที่ 7.2 เป็นการนำเครือข่าย IP มาประยุกต์ใช้งานโดยมีขั้นตอนในการประยุกต์พอสังเขป ดังนี้

1. เปลี่ยนอุปกรณ์การเชื่อมโยงจากคู่สายเช่าแบบอนาลอกเป็นคู่สายเช่าแบบดิจิตอล (DDN) ที่ความเร็ว 64 Kbps ที่สาขา ส่วนสำนักงานใหญ่ใช้วงจรเช่าแบบ Channelized E1 ซึ่งสามารถแบ่งเป็นวงจรย่อยได้ 30 วงจรทำให้สามารถรองรับสาขาได้ถึง 30 สาขา

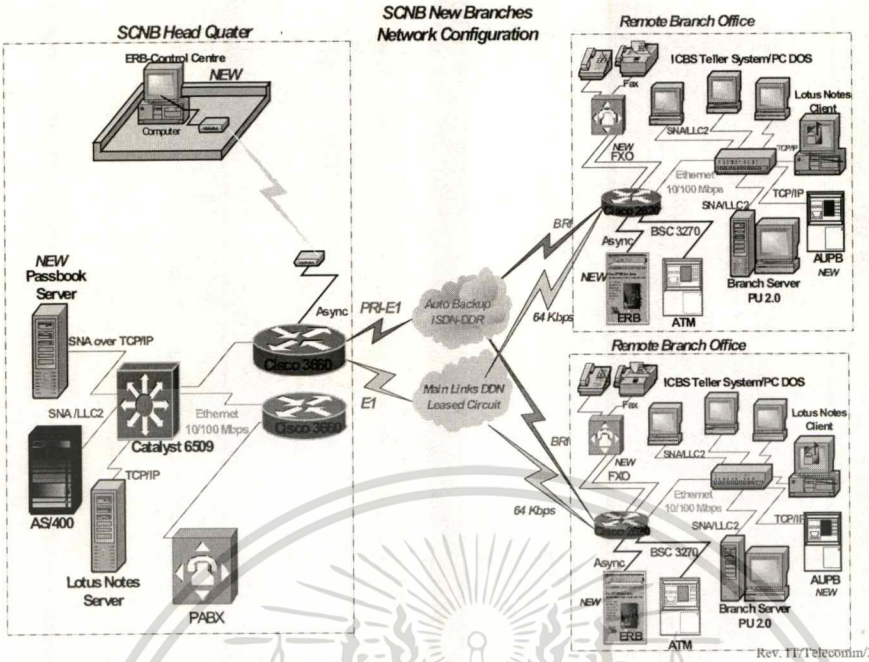
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2. ติดตั้งอุปกรณ์เราท์เตอร์ที่อาคารสำนักงานใหญ่ สาขา และศูนย์ประมวลผล (PCC) โดยติดตั้งเราท์เตอร์ขนาดกลาง 2 ตัวที่สำนักงานใหญ่เพื่อทำหน้าที่เป็น Backbone WAN สำหรับเชื่อมต่อไปยังสาขาต่าง ๆ โดยจัดแบ่งแอเรียออกเป็น 2 แอเรียคือ WAN_Host_1 เป็นแอเรีย "1" และ WAN_Host_2 เป็นแอเรีย "2" สำหรับเราท์เตอร์ที่ PCC จะมีแอเรียเป็น "3" และมี LAN Backbone เป็นแอเรีย "0" ดังรูปที่ 7.3
3. เปลี่ยนรูปแบบโพรโทคอลของ ATM จากเดิม Bisync เป็น SNA/SDLC ซึ่งจะทำให้สามารถตรวจสอบความถูกต้องของข้อมูลได้ และทำให้ข้อมูลเกิดความน่าเชื่อถือ
4. คงรูปแบบโพรโทคอล SNA/SDLC และ Asyncronous สำหรับระบบงานฝาก-ถอน และระบบเช็คเคลียร์ริ่งตามลำดับ
5. เปลี่ยนรูปแบบระบบ LAN ในสาขาจากเดิมที่ใช้ Token Ring มาเป็น Ethernet เพื่อเพิ่มความเร็วและความมีประสิทธิให้มากยิ่งขึ้น



รูปที่ 7.3 รูปแบบการเชื่อมโยงและการจัดแบ่งกลุ่มตามแอเรีย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 7.4 รูปแบบแอพพลิเคชันของสาขาและการเชื่อมโยงระบบเครือข่ายเข้าด้วยกัน

ในรูปที่ 7.4 แสดงให้เห็นถึงรูปแบบการเชื่อมโยงระหว่างสำนักงานใหญ่กับสาขาโดยใช้ DDN ความเร็ว 64 Kbps เป็นข่ายสื่อสารหลักและใช้เครือข่าย ISDN แบบ BRI เป็นเครือข่ายสำรองในกรณีที่ DDN หลักล่ม หรือใช้ส่งข้อมูลในกรณีที่ DDN หลักเกิดความแออัดของข้อมูล เพื่อแบ่งเบาโหลด และแสดงให้เห็นถึงแอพพลิเคชันต่าง ๆ ที่สาขาโดยผ่านเครือข่าย IP ได้แก่ ระบบฝาก-ถอนเงิน หรือระบบ Teller ระบบ ATM ระบบโทรศัพท์แบบ VoIP และบอร์ดแสดงอัตราแลกเปลี่ยนเงินตราต่างประเทศแบบ On-line

7.2 สรุปผลการทดสอบและข้อเสนอแนะ

วิทยานิพนธ์ฉบับนี้ได้นำเสนอผลงานวิจัยเพื่อพัฒนาประสิทธิภาพเครือข่ายที่ให้บริการ ATM แก่ลูกค้า โดยคาดหวังว่าเครื่อง ATM จะสามารถทำงานได้อย่างมีประสิทธิภาพ และมีความน่าเชื่อถือ ทั้งนี้จึงได้นำเสนอการใช้งานโพรโทคอล SNA/SDLC ร่วมกับโพรโทคอล X.25 ผ่านเครือข่ายที่ได้สร้างขึ้นใหม่โดยใช้ IP เป็นสื่อกลางในการเชื่อมโยง โดยที่ IP มีข้อดีตรงที่ไม่ต้องมีการสร้างการเชื่อมต่อก่อนการส่งข้อมูล ซึ่งลดความยุ่งยากในการ setup ค่าพารามิเตอร์ต่าง ๆ และยังสามารถเชื่อมต่ออุปกรณ์เครือข่ายตัวใหม่เข้าไปในเครือข่ายที่มีอยู่เดิมได้ง่าย โดยใช้ Routing Protocol แบบ OSPF ซึ่งจะทำให้อุปกรณ์ทุก ๆ ตัวที่อยู่บนเครือข่ายสามารถส่งผ่านข้อมูลระหว่างกันได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากการแบ่งแยกกลุ่มของเราท์เตอร์เป็น 3 แอเรียทำให้การอัพเดท Routing Table ในกรณีที่โทโปโลยีเปลี่ยนแปลง เช่น เราท์เตอร์ล่ม หรือมีการเพิ่มเราท์เตอร์เข้าไปในเครือข่ายในแต่ละแอเรียเป็นไปอย่างอิสระจากกัน ทำให้กระบวนการของ CPU ในการที่จะต้องคำนวณหา Routing Table ใหม่ลดลง แต่จะมีข้อเสียในเรื่องการสื่อสารข้ามผ่านระหว่างแอเรียที่จะต้องผ่านแอเรีย Backbone (แอเรีย 0) ก่อน ในส่วนของโพรโทคอล SNA/SDLC และ X.25 นั้นเป็นโพรโทคอลที่มีความน่าเชื่อถือสูงอยู่แล้ว กล่าวคือจะมีการตรวจสอบเฟรมที่มีความผิดพลาดของข้อมูลในทุกเฟรมในลำดับชั้นของ Data Link อีกทั้งยังทำให้จำนวนพอร์ทต่อจำนวนตู้ ATM ที่จะต้องใช้ในการควบคุมเครื่อง ATM ในด้าน Host ลดลงโดยการใช้โพรโทคอล X.25 ซึ่งมีข้อดีตรงที่สามารถสร้างวงจรเสมือนได้ตั้งแต่ 1 ถึง 255 วงจรต่อ 1 physical port โดยที่ 1 วงจรเสมือนทำหน้าที่ควบคุมเครื่อง ATM 1 เครื่องซึ่งจะเป็นหลักประกันให้ว่าข้อมูลจะไม่สามารถส่งไปยังจุดปลายทางที่ผิดพลาดได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บรรณานุกรม

[1] J. Doyle, 1998. **CCIE Professional Development : Routing TCP/IP.** Indianapolis : Cisco Press.

[2] F. Halsall, 1995. **Data Communications Computer Networks and Open Systems.** New York : Addison-Wesley.

[3] http://cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/dlsw.htm

[4] G. Sackert and N. Sackert, 1999. **Internetworking SNA with CISCO Solutions.** Indianapolis : Cisco Press.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภาคผนวก

ตัวอย่างค่าพารามิเตอร์ของ WAN_Host_1 ซึ่งเชื่อมต่อไปยังสาขาต่าง ๆ ด้วย Channelized E1 โดยใช้ Interface serial 5/0:0 ถึง 5/0:30 .

WAN_Host_1#sh running-config

Building configuration...

Current configuration : 17192 bytes

!

! Last configuration change at 09:30:03 UTC Sun Mar 24 2002

! NVRAM config last updated at 09:30:06 UTC Sun Mar 24 2002

!

version 12.1

no service single-slot-reload-enable

service timestamps debug uptime

service timestamps log datetime msec

service password-encryption

!

hostname WAN_Host_1

!

logging buffered 10248 debugging

logging rate-limit console 10 except errors

enable secret 5 1h4LE$xgO4LUfHb8VZXGGyv0VRq1

!

username scnbtelecom privilege 10 password xxxx

username scnbadmin privilege 15 password xxxx

!

ip subnet-zero

!

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
!
no ip finger
no ip domain-lookup
ip host CALLED_1 4040 172.21.188.5
!
virtual-profile virtual-template 1
isdn switch-type primary-net5
call rsvp-sync
cns event-service server
!
!
!
!
!
stun peer-name 172.21.119.1
stun protocol-group 1 basic
stun protocol-group 3 basic
dlsw local-peer peer-id 172.21.119.1
dlsw remote-peer 0 tcp 172.21.188.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.137.133 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.136.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.138.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.138.133 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.135.133 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.133.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.129.133 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.136.133 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.132.133 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.140.133 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.137.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.188.37 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.133.133 lsap-output-list 200
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
dlsw remote-peer 0 tcp 172.21.128.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.135.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.140.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.132.5 lsap-output-list 200
dlsw bridge-group 1
!
bstun peer-name 172.21.119.1
bstun protocol-group 1 bsc
bstun protocol-group 2 bsc
bstun protocol-group 3 bsc
!
controller E1 5/0
 framing NO-CRC4
 channel-group 0 timeslots 1
 channel-group 1 timeslots 2
 channel-group 2 timeslots 3
 channel-group 3 timeslots 4
 channel-group 4 timeslots 5
 channel-group 5 timeslots 6
 channel-group 6 timeslots 7
 channel-group 7 timeslots 8
 channel-group 8 timeslots 9
 channel-group 9 timeslots 10
 channel-group 10 timeslots 11
 channel-group 11 timeslots 12
 channel-group 12 timeslots 13
 channel-group 13 timeslots 14
 channel-group 14 timeslots 15
 channel-group 15 timeslots 16
 channel-group 16 timeslots 17
 channel-group 17 timeslots 18
 channel-group 18 timeslots 19
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
 channel-group 19 timeslots 20
 channel-group 20 timeslots 21
 channel-group 21 timeslots 22
 channel-group 22 timeslots 23
 channel-group 23 timeslots 24
 channel-group 24 timeslots 25
 channel-group 25 timeslots 26
 channel-group 26 timeslots 27
 channel-group 27 timeslots 28
 channel-group 28 timeslots 29
 channel-group 29 timeslots 30
 channel-group 30 timeslots 31
!
controller E1 5/1
 pri-group timeslots 1-31
!
!
interface Loopback0
 ip address 172.21.119.1 255.255.255.255
!
interface FastEthernet0/0
 description Ethernet 0/0 LAN BB
 ip address 172.21.103.249 255.255.255.0
 no ip mroute-cache
 ip policy route-map 64only
 duplex auto
 speed auto
 no cdp enable
 bridge-group 1
!
interface FastEthernet0/1
 no ip address
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
 no ip mroute-cache
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
interface Serial1/0
 description ### TA-Link to PCC 128Kbps  ###
 ip address 172.21.188.1 255.255.255.252
 ip access-group 101 in
 no ip mroute-cache
!
interface Serial1/1
 description ############  To PCC with 64K Link  ################
 bandwidth 64
 ip address 172.21.188.21 255.255.255.252
 ip access-group 101 in
!
interface Serial1/2
 description ## MASTER CARD ##
 mtu 512
 no ip address
 encapsulation bstun
 no keepalive
 bstun group 1
 bsc contention 1
 bstun route all tcp 172.21.188.5
!
interface Serial1/3
 no ip address
 no keepalive
!
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
interface Serial1/4
 description ### Master Card Test ###
 no ip address
 encapsulation bstun
 no keepalive
 bstun group 2
 bsc contention 2
 bstun route all tcp 172.21.188.37
!
interface Serial1/5
 description ### Link to Empire ###
 ip address 172.21.188.33 255.255.255.252
 no ip mroute-cache
!
interface Serial1/6
 description ### ATM Test PCC T202 ###
 no ip address
 encapsulation sdlc
 no ip mroute-cache
 no keepalive
 sdlc role primary
 sdlc vmac 5000.0008.0500
 sdlc address C2
 sdlc xid C2 0A800101
 sdlc partner 4900.0008.0502 C2
 sdlc dlsw C2
!
interface Serial1/7
 description ### ATM Test PCC T207 ###
 no ip address
 encapsulation sdlc
 no ip mroute-cache
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
 no keepalive
 sdlc role primary
 sdlc vmac 5000.0008.0500
 sdlc address C7
 sdlc xid C7 0A800204
 sdlc partner 4900.0008.0507 C7
 sdlc dlsw C7
!
interface Serial2/0
 description ### AS/400 Test to PCC_Empire Test ###
 no ip address
 encapsulation stun
 no ip mroute-cache
 clockrate 9600
 stun group 3
 stun route all tcp 172.21.188.37
!
interface Serial2/1
 description ### Link to AS/400 ###
 no ip address
 encapsulation stun
 no ip mroute-cache
 clockrate 128000
 stun group 1
 stun route all tcp 172.21.188.5
!
interface Serial2/2
 description ### ATM TEST SCNB ST3FL6 ###
 no ip address
 encapsulation sdlc
 no ip mroute-cache
 no keepalive
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
 sdlc role primary
 sdlc vmac 5000.0008.0500
 sdlc address 20
 sdlc xid 20 0A800555
 sdlc partner 4900.0008.0555 20
 sdlc dlsw 20
!
interface Serial2/3
no ip address
 no ip mroute-cache
!
interface Serial2/4
 no ip address
 no ip mroute-cache
!
interface Serial2/5
 description ### Bangkae-WAN Interface CCT: 0-2238-4898 ###
 mtu 500
 bandwidth 64
 ip address 172.21.137.1 255.255.255.252
 no ip mroute-cache
 no cdp enable
!
interface Serial2/6
 no ip address
!
interface Serial2/7
 no ip address
 shutdown
!
interface Serial5/0:0
 description ### Nakornratchasima-WAN Interface CCT: B03600 ###
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
 mtu 500
 ip address 172.21.128.1 255.255.255.252
 ip rtp header-compression
 ip rtp compression-connections 25
!
interface Serial5/0:1
 description ### Chonburi-WAN Interface CCT: B03633 ###
 mtu 500
 ip address 172.21.129.129 255.255.255.252
 ip rtp header-compression
 ip rtp compression-connections 25
!
interface Serial5/0:2
 description ### Udornthani-WAN Interface CLOSED ###
 mtu 500
 ip address 172.21.132.1 255.255.255.252
 ip rtp header-compression
 ip rtp compression-connections 25
!
interface Serial5/0:3
 description ### Charoenkrung-WAN Interface CCT: B03507 ###
 mtu 500
 ip address 172.21.132.129 255.255.255.252
 ip rtp header-compression
 ip rtp compression-connections 25
!
interface Serial5/0:4
 description ### Lardprao-WAN Interface CCT: B03659 ###
 mtu 500
 ip address 172.21.133.1 255.255.255.252
 ip rtp header-compression
 ip rtp compression-connections 25
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
!
interface Serial5/0:5
 description ### Chiangmai-WAN Interface CCT: B03436 ###
 mtu 500
 ip address 172.21.133.129 255.255.255.252
 ip rtp header-compression
 ip rtp compression-connections 25
!
interface Serial5/0:6
 description ### Pratunam-WAN Interface CCT: B03596 ###
 mtu 500
 ip address 172.21.135.1 255.255.255.252
 ip rtp header-compression
 ip rtp compression-connections 25
!
interface Serial5/0:7
 description ### Chaengwatthana-WAN Interface CCT: B03337 ###
 mtu 500
 ip address 172.21.135.129 255.255.255.252
 ip rtp header-compression
 ip rtp compression-connections 25
!
interface Serial5/0:8
 description ### Charoennakorn-Wan Interface CCT: B03510 ###
 mtu 500
 ip address 172.21.136.1 255.255.255.252
 ip rtp header-compression
 ip rtp compression-connections 25
!
interface Serial5/0:9
 description ### Thadindaeng-WAN Interface CCT: B02243 ###
 mtu 500
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
 ip address 172.21.136.129 255.255.255.252
 ip rtp header-compression
 ip rtp compression-connections 25
!
interface Serial5/0:10
 description ### Rama IV-WAN Interface CCT: B00315 ###
 mtu 500
 ip address 172.21.137.129 255.255.255.252
 ip rtp header-compression
 ip rtp compression-connections 25
!
interface Serial5/0:11
 description ### Sathupradit-WAN Interface CCT: B03554 ###
 mtu 500
 ip address 172.21.138.1 255.255.255.252
 ip rtp header-compression
 ip rtp compression-connections 25
!
interface Serial5/0:12
 description ### Saphanmai-WAN Interface CCT: B03511 ###
 mtu 500
 ip address 172.21.138.129 255.255.255.252
 ip rtp header-compression
 ip rtp compression-connections 25
!
interface Serial5/0:13
 description ### Nananur-WAN Interface CCT: B03339 ###
 mtu 500
 ip address 172.21.140.1 255.255.255.252
 ip rtp header-compression
 ip rtp compression-connections 25
!
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
interface Serial5/0:14
 description ### Phahurat-WAN Interface CCT: B03513 ###
 mtu 500
 ip address 172.21.140.129 255.255.255.252
 ip rtp header-compression
 ip rtp compression-connections 25
!
interface Serial5/0:15
 no ip address
!
interface Serial5/0:16
 no ip address
!
interface Serial5/0:17
 no ip address
!
interface Serial5/0:18
 no ip address
!
interface Serial5/0:19
 no ip address
!
interface Serial5/0:20
 no ip address
!
interface Serial5/0:21
 no ip address
!
interface Serial5/0:22
 no ip address
!
interface Serial5/0:23
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
 no ip address
!
interface Serial5/0:24
 no ip address
!
interface Serial5/0:25
 no ip address
!
interface Serial5/0:26
 no ip address
!
interface Serial5/0:27
 no ip address
!
interface Serial5/0:28
 no ip address
!
interface Serial5/0:29
 no ip address
!
interface Serial5/0:30
 no ip address
!
interface Serial5/1:15
 ip unnumbered Loopback0
 encapsulation ppp
 dialer idle-timeout 2000000
 dialer-group 1
 isdn switch-type primary-net5
 ppp multilink
!
interface Virtual-Template1
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
 ip unnumbered Loopback0
!
router ospf 1
 log-adjacency-changes
 area 1 range 172.21.128.0 255.255.240.0
 area 3 range 172.21.188.0 255.255.255.224
 network 172.21.103.0 0.0.0.255 area 0
 network 172.21.119.1 0.0.0.0 area 1
 network 172.21.128.0 0.0.0.3 area 1
 network 172.21.129.128 0.0.0.3 area 1
 network 172.21.132.0 0.0.0.3 area 1
 network 172.21.132.128 0.0.0.3 area 1
 network 172.21.133.0 0.0.0.3 area 1
 network 172.21.133.128 0.0.0.3 area 1
 network 172.21.135.0 0.0.0.3 area 1
 network 172.21.135.128 0.0.0.3 area 1
 network 172.21.136.0 0.0.0.3 area 1
 network 172.21.136.128 0.0.0.3 area 1
 network 172.21.137.0 0.0.0.3 area 1
 network 172.21.137.8 0.0.0.3 area 1
 network 172.21.137.128 0.0.0.3 area 1
 network 172.21.138.0 0.0.0.3 area 1
 network 172.21.138.128 0.0.0.3 area 1
 network 172.21.140.0 0.0.0.3 area 1
 network 172.21.140.128 0.0.0.3 area 1
 network 172.21.188.0 0.0.0.3 area 3
 network 172.21.188.20 0.0.0.3 area 3
 network 172.21.188.32 0.0.0.3 area 3
!
 ip kerberos source-interface any
 ip classless
 ip route 0.0.0.0 0.0.0.0 172.21.103.1
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
ip route 172.30.0.3 255.255.255.255 172.21.188.2
ip route 192.168.0.8 255.255.255.255 172.21.188.2
no ip http server
!
logging trap debugging
logging 11.10.1.101
access-list 11 permit 11.10.0.0 0.0.255.255
access-list 11 permit 172.21.101.0 0.0.0.255
access-list 101 deny   tcp any any eq telnet
access-list 101 deny   tcp any any eq ftp
access-list 101 permit ip any any
access-list 110 permit ip any 192.168.0.0 0.0.255.255
access-list 200 permit 0x0000 0x0D0D
access-list 200 deny   0x0000 0xFFFF
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
route-map 64only permit 10
 match ip address 110
 set ip next-hop 172.21.188.22
!
!
bridge 1 protocol ieee
!
!
privilege exec level 10 show startup-config
!
line con 0
 exec-timeout 0 0
 password xxxx
 transport input none
line aux 0
 no motd-banner
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
no exec-banner
exec-timeout 0 0
no flush-at-activation
no activation-character
no vacant-message
modem InOut
autocommand  telnet CALLED_1 /stream
transport preferred telnet
transport output pad v120 telnet rlogin
escape-character NONE
databits 7
parity even
stopbits 1
flowcontrol hardware
line vty 0 4
 password xxxx
 login
!
ntp clock-period 17180317
ntp server 11.10.1.1 prefer
end
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตัวอย่างค่าพารามิเตอร์ของสาขาท่าดินแดง โดยใช้ Interface serial 0/0 เป็น Main Link และ ใช้ Interface serial 0/1 เชื่อมต่อกับเครื่อง ATM

Thadindaeng#sh running-startup

Building configuration...

Current configuration : 3187 bytes

!

version 12.1

service timestamps debug uptime

service timestamps log datetime

service password-encryption

!

hostname Thadindaeng

!

logging buffered 65535 debugging

aaa new-model

aaa authentication login default local

aaa authorization exec default local

enable secret 5 1TaAC$NIHrt.U.33PqGW5l82h5O.

enable password xxxx

!

username scnbadmin privilege 15 password xxxx

username scnbtelecom privilege 10 password xxxx

username WAN_Host_1 password xxxx

!

!

!

!

ip subnet-zero

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
!
isdn switch-type basic-net3
!
dlsw local-peer peer-id 172.21.136.133
dlsw remote-peer 0 tcp 172.21.188.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.119.1 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.139.5 lsap-output-list 200
dlsw bridge-group 1
!
!
voice-port 1/0/0
!
voice-port 1/0/1
!
!
interface Loopback0
 ip address 172.21.136.133 255.255.255.255
!
interface FastEthernet0/0
 ip address 172.21.136.193 255.255.255.192
 duplex auto
 speed 100
 bridge-group 1
!
interface Serial0/0
 mtu 500
 bandwidth 64
 backup delay 300 120
 backup interface Dialer1
 backup load 99 5
 ip address 172.21.136.130 255.255.255.252
 no ip mroute-cache
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
 no fair-queue
 ip rtp header-compression
 ip rtp compression-connections 25
!
interface BRI0/0
 no ip address
 encapsulation ppp
 no ip mroute-cache
 dialer pool-member 1
 isdn switch-type basic-net3
 ppp multilink
!
interface Serial0/1
 no ip address
 encapsulation sdlc
 no ip mroute-cache
 no keepalive
 sdlc role primary
 sdlc vmac 5000.0001.0200
 sdlc address 0B
 sdlc xid 0B 0A100211
 sdlc partner 4900.0001.0211 0B
 sdlc dlsw B
!
interface Dialer1
 ip unnumbered Loopback0
 encapsulation ppp
 dialer pool 1
 dialer string 022069940
 dialer load-threshold 99 outbound
 dialer-group 1
 ppp multilink
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
!
router ospf 1
 log-adjacency-changes
 network 172.21.136.128 0.0.0.3 area 1
 network 172.21.136.133 0.0.0.0 area 1
 network 172.21.136.192 0.0.0.63 area 1
!
ip classless
no ip http server
!
logging trap debugging
logging 11.10.1.101
access-list 200 permit 0x0000 0x0D0D
access-list 200 deny   0x0000 0xFFFF
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
bridge 1 protocol ieee
privilege exec level 10 show startup-config
privilege exec level 10 show
!
line con 0
 transport input none
line aux 0
line vty 0 4
 password xxxx
!
end
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตัวอย่างการกำหนดค่าพารามิเตอร์ของเราท์เตอร์ PCC_3660_1 ซึ่งติดตั้งอยู่ที่ศูนย์ประมวลผล โดยใช้ Interface serial 1/0 เชื่อมโยงกับเราท์เตอร์ WAN_Host_1 ด้วยความเร็ว 128 Kbps และใช้ Interface serial 1/5 เชื่อต่อเข้ากับ Tandem

```
PCC_3660_1#sh run
Building configuration...

Current configuration : 10059 bytes
!
! Last configuration change at 08:23:47 UTC Wed Jan 9 2002
! NVRAM config last updated at 08:24:10 UTC Wed Jan 9 2002
!
version 12.1
no service single-slot-reload-enable
service tcp-keepalives-in
service timestamps debug uptime
service timestamps log datetime
service password-encryption
!
hostname PCC_3660_1
!
logging buffered 65535 debugging
logging rate-limit console 10 except errors
enable secret 5 $1$H7S.$2pkRiBtZtQWi2HBEVRRFP/
!
ip subnet-zero
!
!
no ip finger
no ip domain-lookup
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
!
x25 routing
call rsvp-sync
!
!
stun peer-name 172.21.188.5
stun protocol-group 1 basic
dlsw local-peer peer-id 172.21.188.5
dlsw remote-peer 0 tcp 172.21.119.1 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.119.3 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.137.133 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.138.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.136.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.138.133 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.135.133 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.133.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.136.133 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.140.133 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.137.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.146.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.145.133 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.144.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.135.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.140.5 lsap-output-list 200
dlsw remote-peer 0 tcp 172.21.132.5 lsap-output-list 200
!
bstun peer-name 172.21.188.5
bstun protocol-group 1 bsc
bstun protocol-group 2 bsc
!
!
interface Loopback0
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
 ip address 172.21.188.5 255.255.255.255
!
interface FastEthernet0/0
 ip address 172.21.188.17 255.255.255.252
 ip ospf cost 10
 ip ospf priority 2
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.221.253 255.255.255.0
 ip access-group 101 in
 duplex auto
 speed auto
 no cdp enable
!
interface Serial1/0
 description SCNB-PCC 128Kbps
 bandwidth 128
 ip address 172.21.188.2 255.255.255.252
!
interface Serial1/1
 description SCNB-PCC 64Kbps
 bandwidth 64
 ip address 172.21.188.22 255.255.255.252
!
interface Serial1/2
 description MasterCard
 mtu 512
 no ip address
 encapsulation bstun
 no keepalive
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
 clockrate 19200
 bstun group 1
 bsc contention 1
 bstun route all tcp 172.21.119.1
!
interface Serial1/3
 no ip address
!
interface Serial1/4
 description ### Link to AS/400 ###
 no ip address
 encapsulation stun
 clockrate 64000
 stun group 1
 stun route all tcp 172.21.119.1
!
interface Serial1/5
 description ##### SCNB ATM GROUP 1 ####
 no ip address
 encapsulation x25 dce
 x25 address 500010002
 x25 htc 100
 x25 win 7
 x25 wout 7
 x25 ips 1024
 x25 ops 1024
 x25 map qllc 4900.0001.0201 49001000201
 x25 map qllc 4900.0001.0202 49001000202
 x25 map qllc 4900.0001.0203 49001000203
 x25 map qllc 4900.0001.0204 49001000204
 x25 map qllc 4900.0001.0205 49001000205
 x25 map qllc 4900.0001.0206 49001000206
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

x25 map qllc 4900.0001.0207 49001000207

x25 map qllc 4900.0001.0208 49001000208

x25 map qllc 4900.0001.0209 49001000209

x25 map qllc 4900.0001.0210 49001000210

x25 map qllc 4900.0001.0211 49001000211

x25 map qllc 4900.0001.0212 49001000212

x25 map qllc 4900.0001.0213 49001000213

x25 map qllc 4900.0001.0214 49001000214

x25 map qllc 4900.0001.0215 49001000215

x25 map qllc 4900.0001.0216 49001000216

x25 map qllc 4900.0001.0217 49001000217

x25 map qllc 4900.0001.0218 49001000218

x25 map qllc 4900.0001.0219 49001000219

x25 map qllc 4900.0001.0220 49001000220

x25 map qllc 4900.0001.0221 49001000221

x25 map qllc 4900.0001.0222 49001000222

x25 map qllc 4900.0001.0224 49001000224

x25 map qllc 4900.0001.0225 49001000225

x25 map qllc 4900.0001.0226 49001000226

x25 map qllc 4900.0001.0227 49001000227

x25 map qllc 4900.0001.0228 49001000228

x25 map qllc 4900.0001.0229 49001000229

x25 map qllc 4900.0001.0230 49001000230

x25 map qllc 4900.0001.0231 49001000231

x25 map qllc 4900.0001.0232 49001000232

x25 map qllc 4900.0001.0233 49001000233

x25 map qllc 4900.0001.0234 49001000234

x25 map qllc 4900.0001.0235 49001000235

x25 map qllc 4900.0001.0236 49001000236

x25 map qllc 4900.0001.0237 49001000237

x25 map qllc 4900.0001.0238 49001000238

x25 map qllc 4900.0001.0239 49001000239

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

clockrate 64000

qllc dlsw subaddress 01 vmacaddr 4900.0001.0201 partner 5000.0001.0201 npsi-poll

qllc dlsw subaddress 02 vmacaddr 4900.0001.0202 partner 5000.0001.0202 npsi-poll

qllc dlsw subaddress 03 vmacaddr 4900.0001.0203 partner 5000.0001.0203 npsi-poll

qllc dlsw subaddress 04 vmacaddr 4900.0001.0204 partner 5000.0001.0204 npsi-poll

qllc dlsw subaddress 05 vmacaddr 4900.0001.0205 partner 5000.0001.0205 npsi-poll

qllc dlsw subaddress 06 vmacaddr 4900.0001.0206 partner 5000.0001.0206 npsi-poll

qllc dlsw subaddress 07 vmacaddr 4900.0001.0207 partner 5000.0001.0207 npsi-poll

qllc dlsw subaddress 08 vmacaddr 4900.0001.0208 partner 5000.0001.0208 npsi-poll

qllc dlsw subaddress 09 vmacaddr 4900.0001.0209 partner 5000.0001.0209 npsi-poll

qllc dlsw subaddress 10 vmacaddr 4900.0001.0210 partner 5000.0001.020a npsi-poll

qllc dlsw subaddress 11 vmacaddr 4900.0001.0211 partner 5000.0001.020b npsi-poll

qllc dlsw subaddress 12 vmacaddr 4900.0001.0212 partner 5000.0001.020c npsi-poll

qllc dlsw subaddress 13 vmacaddr 4900.0001.0213 partner 5000.0001.020d npsi-poll

qllc dlsw subaddress 14 vmacaddr 4900.0001.0214 partner 5000.0001.020e npsi-poll

qllc dlsw subaddress 15 vmacaddr 4900.0001.0215 partner 5000.0001.020f npsi-poll

qllc dlsw subaddress 16 vmacaddr 4900.0001.0216 partner 5000.0001.0210 npsi-poll

qllc dlsw subaddress 17 vmacaddr 4900.0001.0217 partner 5000.0001.0211 npsi-poll

qllc dlsw subaddress 18 vmacaddr 4900.0001.0218 partner 5000.0001.0212 npsi-poll

qllc dlsw subaddress 19 vmacaddr 4900.0001.0219 partner 5000.0001.0213 npsi-poll

qllc dlsw subaddress 20 vmacaddr 4900.0001.0220 partner 5000.0001.0214 npsi-poll

qllc dlsw subaddress 21 vmacaddr 4900.0001.0221 partner 5000.0001.0215 npsi-poll

qllc dlsw subaddress 22 vmacaddr 4900.0001.0222 partner 5000.0001.0216 npsi-poll

qllc dlsw subaddress 24 vmacaddr 4900.0001.0224 partner 5000.0001.0217 npsi-poll

qllc dlsw subaddress 25 vmacaddr 4900.0001.0225 partner 5000.0001.0218 npsi-poll

qllc dlsw subaddress 26 vmacaddr 4900.0001.0226 partner 5000.0001.0219 npsi-poll

qllc dlsw subaddress 27 vmacaddr 4900.0001.0227 partner 5000.0001.021a npsi-poll

qllc dlsw subaddress 28 vmacaddr 4900.0001.0228 partner 5000.0001.021b npsi-poll

qllc dlsw subaddress 29 vmacaddr 4900.0001.0229 partner 5000.0001.021c npsi-poll

qllc dlsw subaddress 30 vmacaddr 4900.0001.0230 partner 5000.0001.021d npsi-poll

qllc dlsw subaddress 31 vmacaddr 4900.0001.0231 partner 5000.0001.021e npsi-poll

qllc dlsw subaddress 32 vmacaddr 4900.0001.0232 partner 5000.0001.021f npsi-poll

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
qllc dlsw subaddress 33 vmacaddr 4900.0001.0233 partner 5000.0001.0220 npsi-poll
qllc dlsw subaddress 34 vmacaddr 4900.0001.0234 partner 5000.0001.0221 npsi-poll
qllc dlsw subaddress 35 vmacaddr 4900.0001.0235 partner 5000.0001.0222 npsi-poll
qllc dlsw subaddress 36 vmacaddr 4900.0001.0236 partner 5000.0001.0223 npsi-poll
qllc dlsw subaddress 37 vmacaddr 4900.0001.0237 partner 5000.0001.0224 npsi-poll
qllc dlsw subaddress 38 vmacaddr 4900.0001.0238 partner 5000.0001.0225 npsi-poll
qllc dlsw subaddress 39 vmacaddr 4900.0001.0239 partner 5000.0001.0226 npsi-poll
!
interface Serial1/6
 no ip address
!
interface Serial1/7
 physical-layer async
 description ### Tandem for HSM ###
 bandwidth 9
 no ip address
!
router ospf 1
 log-adjacency-changes
 redistribute static
 network 172.21.188.0 0.0.0.3 area 3
 network 172.21.188.5 0.0.0.0 area 3
 network 172.21.188.16 0.0.0.3 area 3
 network 172.21.188.20 0.0.0.3 area 3
 network 172.21.188.24 0.0.0.3 area 3
 network 192.168.3.0 0.0.0.255 area 3
 network 192.168.221.0 0.0.0.255 area 3
!
ip classless
ip route 172.30.0.3 255.255.255.255 172.21.188.26
ip route 192.168.0.8 255.255.255.255 172.21.188.26
ip route 192.168.3.0 255.255.255.0 192.168.221.221
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
no ip http server
!
logging trap debugging
logging 11.10.1.101
access-list 11 permit 11.10.0.0 0.0.255.255
access-list 11 permit 172.21.101.0 0.0.0.255
access-list 101 permit tcp host 192.168.3.61 host 172.21.103.35 eq ftp
access-list 101 deny   tcp any any eq ftp
access-list 101 deny   tcp any any eq telnet
access-list 101 deny   icmp any any
access-list 101 deny   udp any any eq snmp log
access-list 101 permit ip any any
access-list 200 permit 0x0000 0x0D0D
access-list 200 deny   0x0000 0xFFFF
route-map 64only permit 10
 match ip address 101
 set ip next-hop 172.21.188.21
!
bridge 1 protocol ieee
!
dial-peer cor custom
!
!
!
privilege exec level 10 show startup-config
!
line con 0
 password xxxx
 login
 transport input none
line 40
 no exec
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
no exec-banner
no vacant-message
modem InOut
transport preferred telnet
transport input all
databits 7
parity even
stopbits 1
flowcontrol hardware
line aux 0
line vty 0 4
 password xxxx
 login
line vty 5 39
 login
!
end
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตัวอย่างการกำหนดค่าพารามิเตอร์ TANDEM ที่เชื่อมต่อกับเราท์เตอร์ PCC_3660_1 เพื่อใช้ควบคุมเครื่อง ATM ทั้งหมด

```
LIST SCNBSOX
Comment   Production Config.
Comment   SNA over X.25 Config
Comment
Comment   Date: 19 April 2001
Comment

Comment ========================ADD X25 PHYSICAL LINE ========================
Comment X25 Line : $SCNB25A
Comment ========================= 2 LINES OF X25 PHYSICAL LINE ==================
Comment X25 Line : $SCNB25A
Comment X25 Line : $SCNB25B
Comment ========================================================================
ALLOW ALL ERRORS
ASSUME LINE $SCNB25A
ABORT, SUB ALL
DELETE, SUB ONLY

ALTER, PVCRANGE RESET, SVCRANGE (1,64),L3WINDOW 7
ALTER, CHARACTERSET ASCII, SRCADDR "490010002", INTERFACE RS422

ADD SU #SD1 , PROTOCOL QLLC, DEVTYPE (58,20), RECSIZE 512, PORT 1,& DESTADDR
        "50001000201"
ADD SU #SD2 ,LIKE #SD1 ,PORT 2, DESTADDR "50001000202"
ADD SU #SD3 ,LIKE #SD1 ,PORT 3, DESTADDR "50001000203"
ADD SU #SD4 ,LIKE #SD1 ,PORT 4, DESTADDR "50001000204"
ADD SU #SD5 ,LIKE #SD1 ,PORT 5, DESTADDR "50001000205"
ADD SU #SD6 ,LIKE #SD1 ,PORT 6, DESTADDR "50001000206"
ADD SU #SD7 ,LIKE #SD1 ,PORT 7, DESTADDR "50001000207"
ADD SU #SD8 ,LIKE #SD1 ,PORT 8, DESTADDR "50001000208"
ADD SU #SD9 ,LIKE #SD1 ,PORT 9, DESTADDR "50001000209"
ADD SU #SD10 ,LIKE #SD1 ,PORT 10, DESTADDR "50001000210"
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ADD SU #SD11 ,LIKE #SD1 ,PORT 11, DESTADDR "50001000211"

ADD SU #SD12 ,LIKE #SD1 ,PORT 12, DESTADDR "50001000212"

ADD SU #SD13 ,LIKE #SD1 ,PORT 13, DESTADDR "50001000213"

ADD SU #SD14 ,LIKE #SD1 ,PORT 14, DESTADDR "50001000214"

ADD SU #SD15 ,LIKE #SD1 ,PORT 15, DESTADDR "50001000215"

ADD SU #SD16 ,LIKE #SD1 ,PORT 16, DESTADDR "50001000216"

ADD SU #SD17 ,LIKE #SD1 ,PORT 17, DESTADDR "50001000217"

ADD SU #SD18 ,LIKE #SD1 ,PORT 18, DESTADDR "50001000218"

ADD SU #SD19 ,LIKE #SD1 ,PORT 19, DESTADDR "50001000219"

ADD SU #SD20 ,LIKE #SD1 ,PORT 20, DESTADDR "50001000220"

ADD SU #SD21 ,LIKE #SD1 ,PORT 21, DESTADDR "50001000221"

ADD SU #SD22 ,LIKE #SD1 ,PORT 22, DESTADDR "50001000222"

ADD SU #SD24 ,LIKE #SD1 ,PORT 24, DESTADDR "50001000224"

ADD SU #SD25 ,LIKE #SD1 ,PORT 25, DESTADDR "50001000225"

ADD SU #SD26 ,LIKE #SD1 ,PORT 26, DESTADDR "50001000226"

ADD SU #SD27 ,LIKE #SD1 ,PORT 27, DESTADDR "50001000227"

ADD SU #SD28 ,LIKE #SD1 ,PORT 28, DESTADDR "50001000228"

ADD SU #SD29 ,LIKE #SD1 ,PORT 29, DESTADDR "50001000229"

ADD SU #SD30 ,LIKE #SD1 ,PORT 30, DESTADDR "50001000230"

ADD SU #SD31 ,LIKE #SD1 ,PORT 31, DESTADDR "50001000231"

ADD SU #SD32 ,LIKE #SD1 ,PORT 32, DESTADDR "50001000232"

ADD SU #SD33 ,LIKE #SD1 ,PORT 33, DESTADDR "50001000233"

ADD SU #SD34 ,LIKE #SD1 ,PORT 34, DESTADDR "50001000234"

ADD SU #SD35 ,LIKE #SD1 ,PORT 35, DESTADDR "50001000235"

ADD SU #SD36 ,LIKE #SD1 ,PORT 36, DESTADDR "50001000236"

ADD SU #SD37 ,LIKE #SD1 ,PORT 37, DESTADDR "50001000237"

ADD SU #SD38 ,LIKE #SD1 ,PORT 38, DESTADDR "50001000238"

ADD SU #SD39 ,LIKE #SD1 ,PORT 39, DESTADDR "50001000239"

Comment ==========ADD X25 LOGICAL LINE (SOX) ==========

Comment Line Name : $SCNBSX1

Comment ========== 2 LINES OF X25 LOGICAL LINE (SOX) ==========

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
Comment Line Name : $SCNBSX1
Comment Line Name : $SCNBSX2
Comment
Comment PU Name :
Comment   PUIDBLK %H0A1
Comment ═══════════════════════════════════════════════════════

ASSUME LINE $SCNBSX1
ABORT, SUB ALL
DELETE

ADD LINE, DUPLEX FULL, CHARACTERSET ASCII, STATION PRIMARY, & RECSIZE 512,
      SPXID ON, CONNECT APPL ANY, SWITCHED ON, & IOPAGES 0, XPAGES 0, MAXPUS 80,
      MAXLUS 160

ADD PU #PU201, ADDRESS %H01,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD1, &
      TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00201
ADD PU #PU202, ADDRESS %H02,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD2, &
      TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00202
ADD PU #PU203, ADDRESS %H03,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD3, &
      TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00203
ADD PU #PU204, ADDRESS %H04,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD4, &
      TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00204
ADD PU #PU205, ADDRESS %H05,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD5, &
      TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00205
ADD PU #PU206, ADDRESS %H06,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD6, &
      TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00206
ADD PU #PU207, ADDRESS %H07,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD7, &
      TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00207
ADD PU #PU208, ADDRESS %H08,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD8, &
      TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00208
ADD PU #PU209, ADDRESS %H09,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD9, &
      TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00209
ADD PU #PU210, ADDRESS %H0A,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD10, &
      TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00210
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
ADD PU #PU211, ADDRESS %H0B,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD11, &
    TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00211
ADD PU #PU212, ADDRESS %H0C,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD12, &
    TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00212
ADD PU #PU213, ADDRESS %H0D,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD13, &
    TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00213
ADD PU #PU214, ADDRESS %H0E,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD14, &
    TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00214
ADD PU #PU215, ADDRESS %H0F,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD15, &
    TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00215
ADD PU #PU216, ADDRESS %H10,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD16, &
    TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00216
ADD PU #PU217, ADDRESS %H11,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD17, &
    TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00217
ADD PU #PU218, ADDRESS %H12,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD18, &
    TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00218
ADD PU #PU219, ADDRESS %H13,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD19, &
    TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00219
ADD PU #PU220, ADDRESS %H14,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD20, &
    TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00220

ADD PU #PU221, ADDRESS %H15,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD21, &
    TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00221
ADD PU #PU222, ADDRESS %H16,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD22, &
    TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00222
ADD PU #PU224, ADDRESS %H17,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD24, &
    TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00224
ADD PU #PU225, ADDRESS %H18,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD25, &
    TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00225
ADD PU #PU226, ADDRESS %H19,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD26, &
    TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00226
ADD PU #PU227, ADDRESS %H1A,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD27, &
    TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00227
ADD PU #PU228, ADDRESS %H1B,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD28, &
    TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00228
ADD PU #PU229, ADDRESS %H1C,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD29, &
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
        TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00229
ADD PU #PU230, ADDRESS %H1D,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD30, &
        TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00230
ADD PU #PU231, ADDRESS %H1E,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD31, &
        TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00231

ADD PU #PU232, ADDRESS %H1F,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD32, &
        TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00232
ADD PU #PU233, ADDRESS %H20,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD33, &
        TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00233
ADD PU #PU234, ADDRESS %H21,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD34, &
        TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00234
ADD PU #PU235, ADDRESS %H22,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD35, &
        TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00235
ADD PU #PU236, ADDRESS %H23,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD36, &
        TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00236
ADD PU #PU237, ADDRESS %H24,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD37, &
        TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00237
ADD PU #PU238, ADDRESS %H25,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD38, &
        TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00238
ADD PU #PU239, ADDRESS %H26,MAXLUS 2,ASSOCIATESUBDEV $SCNB25A.#SD39, &
        TYPE (13,2), RECSIZE 256, PUIDBLK %H0A1, PUIDNUM %H00239



ADD LU #LU275, ADDRESS 1, PUNAME #PU201, TYPE (14,0), PROTOCOL SNALU, &
        RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU276, ADDRESS 1, PUNAME #PU202, TYPE (14,0), PROTOCOL SNALU, &
        RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU203, ADDRESS 1, PUNAME #PU203, TYPE (14,0), PROTOCOL SNALU, &
        RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU204, ADDRESS 1, PUNAME #PU204, TYPE (14,0), PROTOCOL SNALU, &
        RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU205, ADDRESS 1, PUNAME #PU205, TYPE (14,0), PROTOCOL SNALU, &
        RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU206, ADDRESS 1, PUNAME #PU206, TYPE (14,0), PROTOCOL SNALU, &
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
    RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU207, ADDRESS 1, PUNAME #PU207, TYPE (14,0), PROTOCOL SNALU, &
    RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU208, ADDRESS 1, PUNAME #PU208, TYPE (14,0), PROTOCOL SNALU, &
    RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU209, ADDRESS 1, PUNAME #PU209, TYPE (14,0), PROTOCOL SNALU, &
    RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU210, ADDRESS 1, PUNAME #PU210, TYPE (14,0), PROTOCOL SNALU, &
    RECSIZE 1024, CHARACTERSET EBCDIC

ADD LU #LU211, ADDRESS 1, PUNAME #PU211, TYPE (14,0), PROTOCOL SNALU, &
    RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU212, ADDRESS 1, PUNAME #PU212, TYPE (14,0), PROTOCOL SNALU, &
    RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU213, ADDRESS 1, PUNAME #PU213, TYPE (14,0), PROTOCOL SNALU, &
    RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU214, ADDRESS 1, PUNAME #PU214, TYPE (14,0), PROTOCOL SNALU, &
    RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU215, ADDRESS 1, PUNAME #PU215, TYPE (14,0), PROTOCOL SNALU, &
    RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU216, ADDRESS 1, PUNAME #PU216, TYPE (14,0), PROTOCOL SNALU, &
    RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU217, ADDRESS 1, PUNAME #PU217, TYPE (14,0), PROTOCOL SNALU, &
    RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU218, ADDRESS 1, PUNAME #PU218, TYPE (14,0), PROTOCOL SNALU, &
    RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU219, ADDRESS 1, PUNAME #PU219, TYPE (14,0), PROTOCOL SNALU, &
    RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU220, ADDRESS 1, PUNAME #PU220, TYPE (14,0), PROTOCOL SNALU, &
    RECSIZE 1024, CHARACTERSET EBCDIC

ADD LU #LU221, ADDRESS 1, PUNAME #PU221, TYPE (14,0), PROTOCOL SNALU, &
    RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU222, ADDRESS 1, PUNAME #PU222, TYPE (14,0), PROTOCOL SNALU, &
    RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU224, ADDRESS 1, PUNAME #PU224, TYPE (14,0), PROTOCOL SNALU, &
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
        RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU225, ADDRESS 1, PUNAME #PU225, TYPE (14,0), PROTOCOL SNALU, &
        RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU226, ADDRESS 1, PUNAME #PU226, TYPE (14,0), PROTOCOL SNALU, &
        RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU227, ADDRESS 1, PUNAME #PU227, TYPE (14,0), PROTOCOL SNALU, &
        RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU228, ADDRESS 1, PUNAME #PU228, TYPE (14,0), PROTOCOL SNALU, &
        RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU229, ADDRESS 1, PUNAME #PU229, TYPE (14,0), PROTOCOL SNALU, &
        RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU230, ADDRESS 1, PUNAME #PU230, TYPE (14,0), PROTOCOL SNALU, &
        RECSIZE 1024, CHARACTERSET EBCDIC

ADD LU #LU231, ADDRESS 1, PUNAME #PU231, TYPE (14,0), PROTOCOL SNALU, &
        RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU232, ADDRESS 1, PUNAME #PU232, TYPE (14,0), PROTOCOL SNALU, &
        RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU233, ADDRESS 1, PUNAME #PU233, TYPE (14,0), PROTOCOL SNALU, &
        RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU234, ADDRESS 1, PUNAME #PU234, TYPE (14,0), PROTOCOL SNALU, &
        RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU235, ADDRESS 1, PUNAME #PU235, TYPE (14,0), PROTOCOL SNALU, &
        RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU236, ADDRESS 1, PUNAME #PU236, TYPE (14,0), PROTOCOL SNALU, &
        RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU237, ADDRESS 1, PUNAME #PU237, TYPE (14,0), PROTOCOL SNALU, &
        RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU238, ADDRESS 1, PUNAME #PU238, TYPE (14,0), PROTOCOL SNALU, &
        RECSIZE 1024, CHARACTERSET EBCDIC
ADD LU #LU239, ADDRESS 1, PUNAME #PU239, TYPE (14,0), PROTOCOL SNALU, &
        RECSIZE 1024, CHARACTERSET EBCDIC
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ผลงานที่ได้รับการตีพิมพ์

1. นพรัตน์ เจิดแจ่มจรัส กอบชัย เดชหาญ และ ชาลิน สุวรรณวงศ์, "การประยุกต์ใช้งานโพรโทคอล SNA บนโพรโทคอล X.25 ในโครงข่ายย่อย," วิศวกรรมสารฉบับวิจัยและพัฒนา ปีที่ 10 ฉบับที่ 2 พ.ศ. 2542
2. นพรัตน์ เจิดแจ่มจรัส กอบชัย เดชหาญ และ ชาลิน สุวรรณวงศ์, "การนำเครือข่าย IP มาประยุกต์ใช้กับเครือข่าย SNA/SDLC และ X.25 กับระบบงาน ATMs," วิศวสารลาดกระบัง ปีที่ 18 ฉบับที่ 4 เดือนธันวาคม 2544

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ประวัติผู้เขียน

นายนพรัตน์ เจิดแจ่มจรัส เกิดเมื่อวันที่ 27 สิงหาคม พ.ศ. 2513 ที่จังหวัดกรุงเทพมหานคร สำเร็จการศึกษาอุตสาหกรรมศาสตรบัณฑิต คณะวิศวกรรมศาสตร์ สาขาวิชาวิศวกรรมอิเล็กทรอนิกส์ มหาวิทยาลัย เอเชียอาคเนย์ ปีการศึกษา 2535 เข้าทำงานตำแหน่งวิศวกรข่ายสื่อสารข้อมูล ธนาคารกรุงเทพ จำกัด (มหาชน) ปี พ.ศ. 2536 – 2540 ปัจจุบัน ตำแหน่ง Technical Specialist ธนาคาร สแตนดาร์ดชาร์เตอร์ดนครธน จำกัด (มหาชน)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้